# Session border controllers

## SBC-1000, SBC-2000, SBC-3000

User Manual, Firmware Version 1.10.0

## Firmware version: 1.10.0

| Document version | Issue date | Revisions |
|---|---|---|
| Version 1.11 | 12.11.2020 | Changed:<br>– the menu tree is reordered by function;<br>– protection timeout limits for calls without media.<br>Added:<br>– the option for automatic response to OPTIONS;<br>– the option for generating logs on request;<br>– support for CPS restriction on SIP-Destination;<br>– the option «Pass the '#' character without encoding»;<br>– the option «Pass the domain from FROM and TO headers»;<br>– the option «Do not send blocked addresses to blacklist»;<br>– the ability to specify more SIP Transports, SIP Destinations, SIP Users, SBC Trunks, Rules in the configuration (if licensed);<br>– an alarm about exceeding the maximum number of simultaneous INVITE, SUBSCRIBE, OTHER requests;<br>– support for RPI and PAI header transmission for SIP-Users. |
| Version 1.10 | 10.07.2020 | Added:<br>– a description of the new SBC-3000 device. |
| Version 1.9 | 23.04.2020 | Synchronization with firmware version 1.9.4 |
| Version 1.8 | 04.10.2019 | Added:<br>– improved media negotiation mechanism for subscribers behind NAT;<br>– GeoIP databases updated;<br>– dynamic firewall operation with telnet;<br>– default port ignore for devices that register a contact without specifying a port, but make a call specifying one. |
| Version 1.7 | 29.10.2018 | Documentation updated |
| Version 1.6 | 08.09.2017 | Changed:<br>– the «fail2ban» section renamed «Dynamic firewall»;<br>– the «firewall profiles» section renamed «Static firewall»;<br>– blocking rules in a dynamic firewall are separated for different services;<br>– the «MTR» section renamed «TRACEROUTE».<br>Added:<br>– SIP header manipulation;<br>– management of call statistics counters;<br>– RTP source control option;<br>– support for 3000 simultaneous calls on SBC2000;<br>– RTP flood attack detection;<br>– assigning network routes to a VPN client interface;<br>– gathering call statistics via SNMP. |
| Version 1.5 | 08.06.2017 | Changed:<br>– base SNMP OID changed to 1.3.6.1.4.1.35265.1.49.<br>Added:<br>– protection against DoS attacks — ICMP flood, port scan, SIP flood;<br>– a new type of firewall rule — GeoIP;<br>– a new type of firewall rule — String;<br>– the ability to filter by User-Agent;<br>– the time limit in rule set;<br>– SBC configuration via the CLI;<br>– group fail2ban rule clearing;<br>– the number of VLAN interfaces on SBC-2000 is increased to 500 (if licensed);<br>– setting a minimum registration time for SIP Users;<br>– option to ignore the source port on incoming calls via SIP Destination;<br>– the SNMP MIB files for the current software version can be downloaded directly from the device;<br>– view call statistics;<br>– the amount of information about registered subscribers displayed has been expanded. |
| Version 1.4 | 27.02.2017 | Added:<br>– 1+1 redundancy. |

| | | |
|---|---|---|
| Version 1.3 | 20.06.2016 | Changed:<br>– trunk and subscriber destinations are separated;<br>– trunks can combine different destinations for redundancy/load balancing purposes;<br>– fail2ban functionality has been extended.<br>Added:<br>– active sessions monitoring;<br>– adaptations for ZTE Softswitch and MTA M-200;<br>– handling redirections in SIP 302 responses;<br>– new more flexible call-switching rules;<br>– the ability to specify more SIP transports and destinations in the configuration;<br>– optioning of the SIP header format. |
| Version 1.2 | 21.01.2016 | Added:<br>– an alarm about full external storage devices;<br>– different modes for creating CDR files;<br>– the use of directories for CDR files;<br>– single RTP port range. |
| Version 1.1 | 12.08.2015 | Added:<br>– a safety timeout to reject calls without media streams switching through;<br>– monitoring the number of calls (maximum, current and minimum values on the graph);<br>– select the network interface for which the media resource is allocated;<br>– SIP destination redundancy;<br>– load balancing;<br>– monitoring the availability of the opposite SIP server;<br>– registration via a SIP trunk;<br>– blocked addresses list. |
| Version 1.0 | 11.11.14 | First issue |

## TARGET AUDIENCE

This operation manual is intended for technical personnel that performs device installation, configuration, monitoring, and maintenance using a web configurator. Qualified technical personnel should be familiar with the operation basics of TCP/IP & UDP/IP protocol stacks and Ethernet networks design concepts.

## CONTENTS

# 1 INTRODUCTION

Session Border Controller (SBC) is designed for heterogeneous VoIP network interfacing tasks, ensuring interoperability of terminals with different signaling protocols and codec sets in use. In addition, due to the functionality of Firewall, NAT and proxying signal and media traffic, it protects the corporate network from attacks and hides its internal structure. SBC is always installed at the edge of the corporate or carrier VoIP network and performs those functions that it is not reasonable to entrust to the operator's devices (for example, a flexible Softswitch).

***Main SBC functions***

- protecting the network and other devices from external attacks (e.g. DoS attacks);
- Firewall functions;
- hiding carrier's network topology;
- negotiating different alarm protocols and codecs;
- providing QoS services and stream prioritization;
- communicating with devices connected via NAT (Network Address Translation);
- collecting statistics on the calls served through SBC.

# 2 DEVICE DESCRIPTION

## 2.1 Purpose

Eltex SBC is a component of the ECSS-10 hardware and software complex, which participates in the call service process as a session border controller. The device provides normalization of the signal protocol implementations, the set SLA level of quality, protection of the carrier's network from unauthorized access and various attacks, collection of statistics.

***SBC main specifications:***

- number of simultaneous sessions:
  - for SBC-3000: 2000[1];
  - for SBC-2000: 2000[1];
  - for SBC-1000: 500.
- number of registered subscribers:
  - for SBC-3000: 16000;
  - for SBC-2000: 16000;
  - for SBC-1000: 4000.
- number of calls per second (CPS):
  - for SBC-3000: 100;
  - for SBC-2000: 100;
  - for SBC-1000: 30.
- number of Ethernet ports:
  - for SBC-3000:
    - 4 ports of 10/100/1000BASE-T;
    - 2 combo ports of 1000-BASE-X (SFP).
  - for SBC-2000:
    - 4 ports of 10/100/1000BASE-T;
    - 2 combo ports of 1000-BASE-X (SFP).
  - for SBC-1000:
    - 3 ports of 10/100/1000BASE-T;
    - 2 ports of 1000-BASE-X (SFP).

[1] For firmware versions starting from 1.4.1 — 2000 calls, starting from 1.9.1 — 3000 calls.

- static address and DHCP support;
- SIP, SIP-T, SIP-I IP protocols;
- NTP support;
- DNS support;
- SNMP support;
- bandwidth limit and QoS;
- ToS and CoS for RTP and signalling[1];
- VLAN for RTP, signalling and management;
- alarm logging;
- RADIUS support;
- billing information recording;
- 1+1 redundancy[2]:
  - switching time to reserve when the main unit's external link is disconnected is 2-4 seconds;
  - switching time to reserve when the main device is completely disconnected is 4-5 seconds;
- firmware update: via web configurator, CLI (Telnet, SSH, console (RS-232));
- configuration and setup (also remotely):
  - Web interface;
  - CLI[3] (Telnet, console (RS-232));
- remote monitoring:
  - web interface;
  - CLI;
  - SNMP.

**SIP/SIP-T/SIP-I functionality:**

- SIP L5 NAT/Topology hiding;
- SIP dialogue transparency;
- SIP transit of unrecognized headers;
- B2BUA as defined in RFC 3261;
- RFC 2833 (Telephone Event);
- RFC 3264 (Offer/Answer);
- RFC 3204 (MIME Support);
- RFC 4028 (Session Timers);
- RFC 3326 (Reason Field);
- RFC 3262 (PRACK);
- RFC 3372 (SIP-T);
- B2BUA peering;
- B2BUA access;
- RFC 1889 (RTP);
- RFC 4566 (SDP);
- RFC 3261;
- RFC 3581;
- SIP OPTIONS Keep-Alive (SIP Busy Out);
- NAT support (comedia mode).

**Fax transmission**

- T.38;
- G.711

[1] Not supported in the current firmware version

[2] This functionality is not supported for SBC with the current firmware version 1.10.0

[3] Not fully supported in the current firmware version

## 2.2 Typical Application Diagrams

This manual proposes several network layouts using SBC.

### 2.2.1 *Interaction between operators*

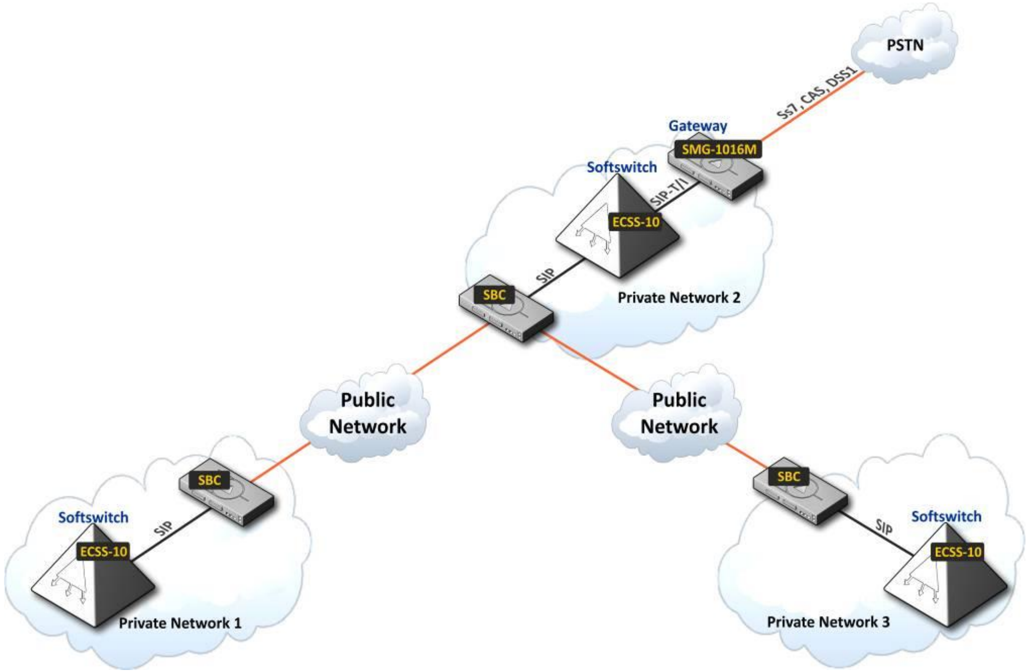


Figure 1 — Use case "Interaction between operators"

### 2.2.2 *Interaction between operator and corporate client*

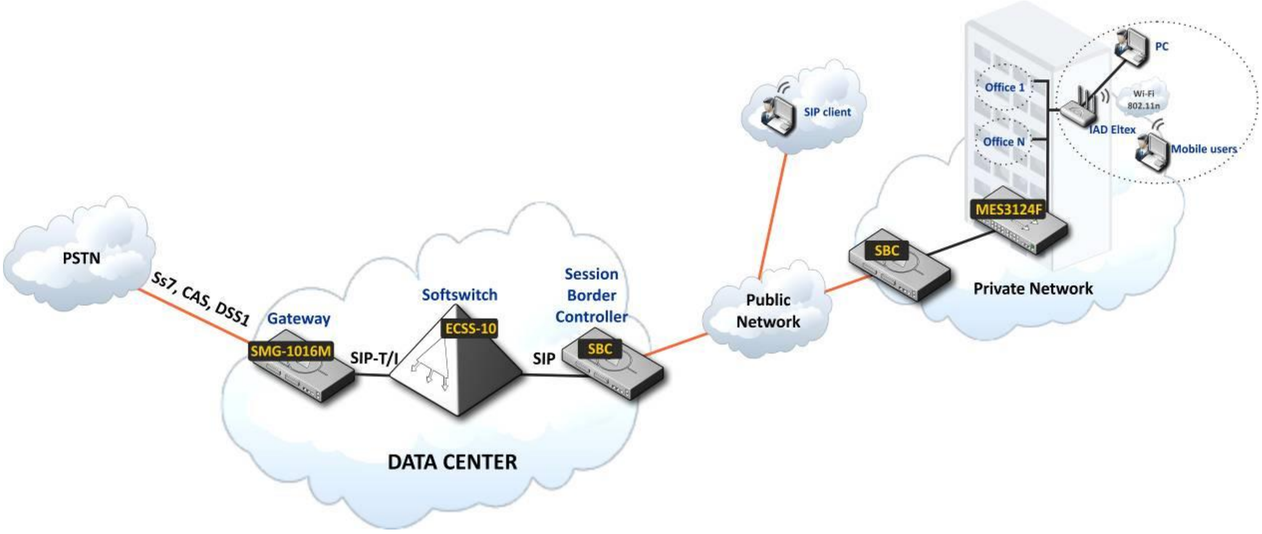


Figure 2 — Use case "Operator — corporate client"

### 2.2.3 *Interaction between operator and private customer*

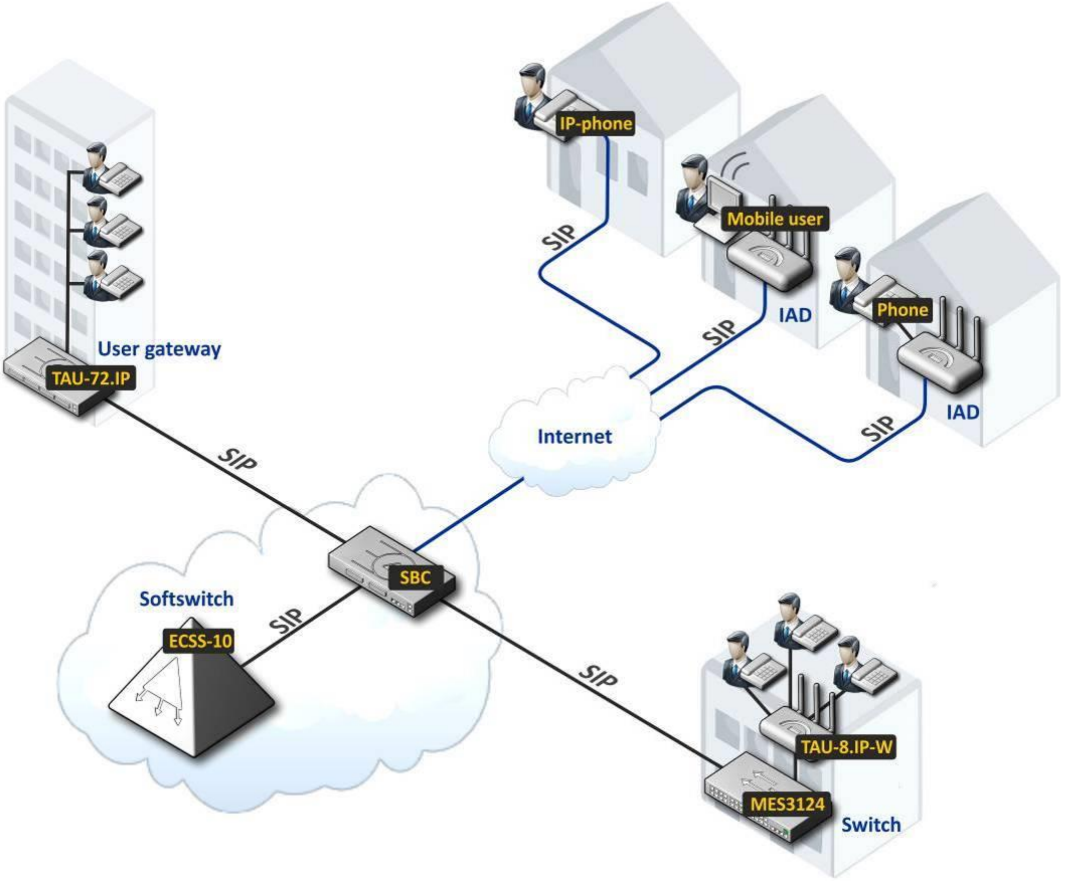


Figure 3 — Use case "Operator — private customer"

## 2.3 Main Specifications

Table 1 shows main specifications of the device.

Table 1 — Main specifications

**VoIP protocols**

| | |
|---|---|
| Supported protocols | SIP-T/SIP-I<br>SIP<br>T.38 |

**Supported codecs**

| | |
|---|---|
| Audio codecs | G.711 a-law (G.711A in text)<br>G.711 µ-law (G.711U in text)<br>G.729 A/B<br>G.723.1 (6.3 Kbps, 5.3 Kbps)<br>G.726 (32 Kbps) |
| Video codecs | H.263<br>H.263-1998<br>H.264 |

**Electrical Ethernet interface specifications**

| | | | |
|---|---|---|---|
| No. of interfaces | SBC-1000 | SBC-2000 | SBC-3000 |
| | 3 | 4 | 4 |
| Electric port | RJ-45 | | |
| Data rate, Mbps | Autodetection, 10/100/1000Mbps duplex | | |
| Standards | 10/100/1000BASE-T | | |

### Optical Ethernet interface specifications

| | |
|---|---|
| No. of interfaces | 2 combo ports |
| Optical port | Mini-Gbic (SFP):<br>1) duplex, double fibre, wave length 1310nm (Single-Mode), 1000BASE-LX (LC connector), distance — up to 10km, supply voltage — 3.3V<br>2) duplex, single fibre, reception/transmission wave lengths 1310/1550nm, 1000BASE-LX (SC connector), distance — up to 10km, supply voltage — 3.3V |
| Data rate, Mbps | 1000Mbps, duplex |
| Standards | 1000BASE-X |

### Console parameters

| RS-232 serial port | |
|---|---|
| Data transfer rate, baud | 115200 |
| Electric signal parameters | According to ITU-T V.28 guidelines |

### Other interfaces

| Interface | Quantity |
|---|---|
| USB | 1 — for SBC-1000/2000; 2 — for SBC-3000 |
| e-SATA | 2 |

### General parameters

| | | | | |
|---|---|---|---|---|
| Operating temperature range | | From 0 to 40°C | | |
| Relative humidity | | Up to 80% | | |
| Power options | | - single AC or DC power supply;<br>- two AC or DC power supplies. | | |
| Power supply | | AC: | DC: | |
| Power supply voltage | | 220V+–20%, 50 Hz | -48V+30–20% | |
| | PM designation | PM160-220/12 | PM100-48/12 | |
| | PM rated power | 160 W | 100 W | |
| Power consumption | | no more than 50 W | | |
| Dimensions (W x H x D) | | SBC-1000 | SBC-2000 | SBC-3000 |
| | | 430x45x260mm | 430x45x340mm | 430x45x340mm |
| Form-factor | | 19" form-factor, 1U size | | |
| Net weight | Complete device package | SBC-1000 | SBC-2000 | SBC-3000 |
| | | 3.2 kg | 5.3 kg | 5.3 kg |
| | Power supply | 0.5 kg | | |
| | Vent panel | 0.1 kg | | |
| | SATA drive[1] | 0.1 kg | | |

[1] Only for SBC-2000 and SBC-3000

## 2.4 Design

### 2.4.1 *SBC-1000*

Session border controller SBC-1000 has a metal case available for 19” form-factor rack-mount 1U shelf installation.

The front panel of the device is shown in Figure 4.

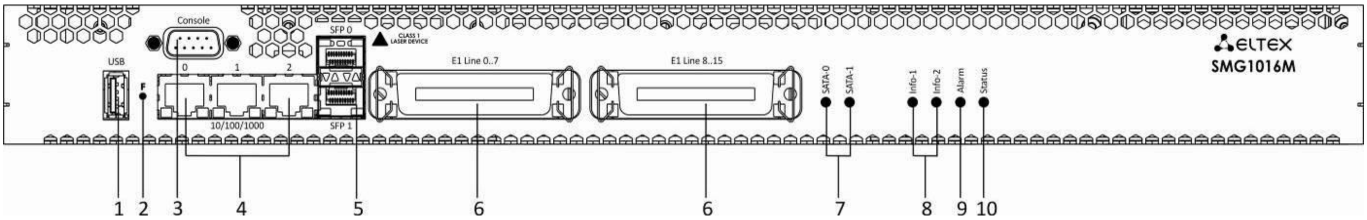


Figure 4 — The front panel of SBC-1000 (based on SMG-1016M)

Connectors, LEDs and controls located on the front panel of the device are listed in Table 2.

Table 2 — Description of connectors, LEDs, and controls located on the front panel

| № | Front panel elements | Description |
|---|---|---|
| 1 | ***USB*** | USB port for external storage device connection |
| 2 | ***F*** | Function button |
| 3 | ***Console*** | RS-232 console port for local control of the device |
| 4 | ***10/100/1000 0..2*** | 3 x RJ-45 ports of Ethernet 10/100/1000 Base-T interfaces |
| 5 | ***SFP 0, SFP 1*** | 2 chassis for 1000Base-X Gigabit uplink interface optical SFP modules used for IP network connection |
| 6 | ***E1 Line 0..7, E1 Line 8..15*** | 2 x CENC-36M connectors for E1 streams[1] |
| 7 | ***SATA-0, SATA-1*** | Indicators of SATA interfaces[2] |
| 8 | ***Info1, Info2*** | SFP optical interface activity indicator |
| 9 | ***Alarm*** | Device alarm indicator |
| 10 | ***Status*** | Device operation indicator |

[1] Not used for configuration SBC-1000

[2] Not used in the current version

The rear panel of the device is shown in Figure 5.

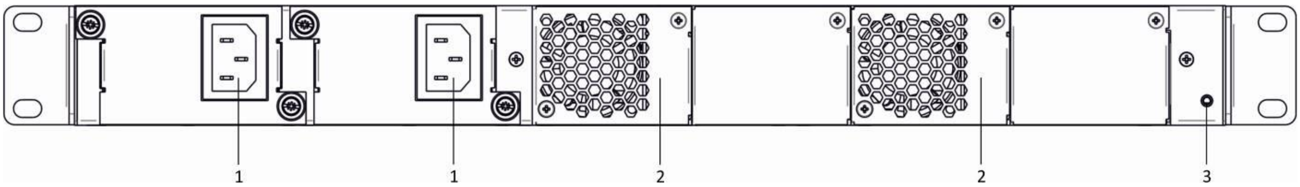


Figure 5 — The rear panel of SBC-1000 (based on SMG-1016M)

The Table below lists rear panel connectors of the device.

Table 3 — Description of rear panel connectors of the switch

| № | Rear panel element | Description |
|---|---|---|
| 1 | Power supply connector | Connector for power supply |
| 2 | Removable fans | Removable ventilation modules with hot-swapping |
| 3 | Earth bonding point ⏚ | Earth bonding point of the device |

### 2.4.2 *SBC-2000*

Session border controller SBC-2000 has a metal case available for 19” form-factor rack-mount 1U shelf installation.

The front panel of device is shown in Figure 6.

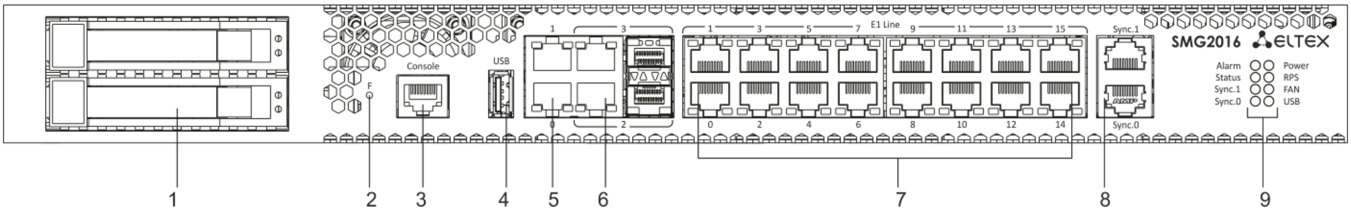


Figure 6 — The front panel of SBC-2000 (based on SMG-2016)

Connectors, LEDs and controls located on the front panel of the device are listed in Table 4.

Table 4 — Description of connectors, LEDs, and controls located on the front panel

| № | Front panel elements | Description |
|---|---|---|
| 1 | ***SATA disk ports*** | Cradle connectors for SATA drive installation |
| 2 | ***F*** | Function button |
| 3 | ***Console*** | Console port for local management of the device |
| 4 | ***USB*** | USB port for external storage device connection |
| 5 | ***0, 1*** | 2 x 10/100/1000BASE-T Gigabit uplink interface RJ-45 connectors used for IP network connection |
| 6 | ***2, 3*** | 2 chassis for 1000BASE-X uplink interface SFP modules used for IP network connection |
| | | 2 x 10/100/1000BASE-T Gigabit uplink interface RJ-45 connectors used for IP network connection |

| | | |
|---|---|---|
| 7 | ***E1 Line 0..15*** | 16 x RJ-48 connectors for E1 streams[1] |
| 8 | ***Sync.0, Sync.1*** | 2 x RJ-45 ports for connection of external synchronization sources[1] |
| Indicators | | |
| 9 | ***Alarm*** | Device alarm indicator |
| | ***Status*** | Device operation indicator |
| | ***Sync.1*** | ***Sync.1*** external synchronization interface operation indicator[1] |
| | ***Sync.0*** | ***Sync.2*** external synchronization interface operation indicator[1] |
| | ***Power*** | Device power indicator |
| | ***RPS*** | Device aux power indicator |
| | ***FAN*** | Fan operation indicator |
| | ***USB*** | USB operation indicator |

The rear panel of the device is shown in Figure 7.

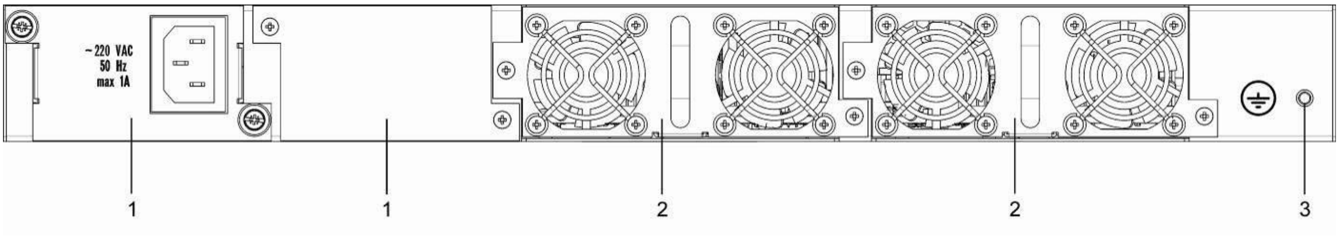


Figure 7 — The rear panel of SBC-2000 (based on SMG-2016)

The Table below lists rear panel connectors of the device.

Table 5 — Description of rear panel connectors of the switch

| № | Rear panel element | Description |
|---|---|---|
| 1 | Power modules | Modules with connector for power supply |
| 2 | Fan panels | Removable ventilation modules with hot-swapping |
| 3 | Earth bonding point ⏚ | Earth bonding point of the device |

[1] Not used for configuration SBC-2000

### 2.4.3 *SBC-3000*

Session border controller SBC-3000 has a metal case available for 19” form-factor rack-mount 1U shelf installation.

The front panel of device is shown in the Figure below.

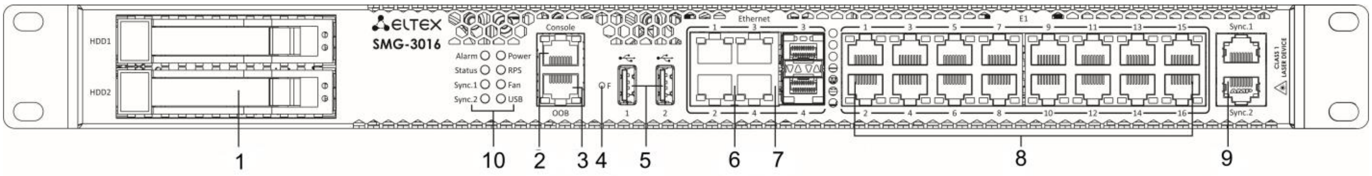


Figure 8 — The front panel of SBC-3000 (based on SMG-3016)

Connectors, LEDs and controls located on the front panel of the device are listed in Table 6.

Table 6 — Description of connectors, LEDs, and controls located on the front panel

| № | Front panel elements | Description |
|---|---|---|
| 1 | ***SATA disk ports*** | Cradle connectors for SATA drive installation |
| 2 | ***Console*** | Console port for local management of the device |
| 3 | ***OOB*** | Dedicated Ethernet port for device configuration[1]. The port does not have the ability to switch with other SMG ports |
| 4 | ***F*** | Function button |
| 5 | ***USB*** | USB ports for external storage devices connection |
| 6 | ***1, 2*** | 2 x 10/100/1000BASE-T Gigabit uplink interface RJ-45 connectors used for IP network connection |
| 7 | ***3, 4*** | 2 chassis for 1000BASE-X uplink interface SFP modules used for IP network connection |
| | | 2 x 10/100/1000BASE-T Gigabit uplink interface RJ-45 connectors used for IP network connection |
| 8 | ***E1 Line 0..15*** | 16 x RJ-48 connectors for E1 streams[2] |
| 9 | ***Sync.1, Sync.2*** | 2 x RJ-45 ports for connection of external synchronization sources[2] |
| | Indicators | |
| 10 | ***Alarm*** | Device alarm indicator |
| | ***Status*** | Device operation indicator |
| | ***Sync.1*** | ***Sync.2*** external synchronization interface operation indicator[2] |
| | ***Sync.0*** | ***Sync.1*** external synchronization interface operation indicator[2] |
| | ***Power*** | Device power indicator |
| | ***RPS*** | Device aux power indicator |

[1] Not supported in the current firmware version

[2] Not used for configuration SBC-3000

| | | |
|---|---|---|
| | ***FAN*** | Fan operation indicator |
| | ***USB*** | USB operation indicator |

The rear panel of the device is shown in Figure 9.

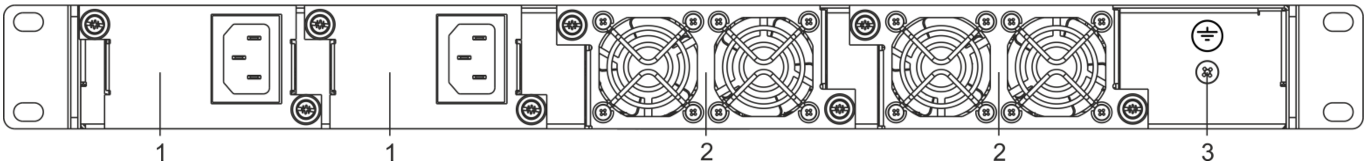


Figure 9 — The rear panel of SBC-3000 (based on SMG-3016)

The table below lists rear panel connectors of the device.

Table 7 — Description of rear panel connectors of the switch

| **№** | **Rear panel element** | **Description** |
|---|---|---|
| 1 | Power modules | Modules with connector for power supply |
| 2 | Fan panels | Removable ventilation modules with hot-swapping |
| 3 | Earth bonding point ⏚ | Earth bonding point of the device |

## 2.5 LED Indication

LED indicators located on the front panel represent the current state of the device.

### 2.5.1 *Device light indication in operation*

#### *2.5.1.1 SBC-1000*

Light indication of the device in operation is shown in Table 8.

Table 8 — Light indication of the device operational status

| **Indicator** | **Indicator State** | **Device Status** |
|---|---|---|
| ***Info1*** | off | SFP0 link lost |
| | solid green | SFP0 link in operation |
| ***Info2*** | off | SFP1 link lost |
| | solid green | SFP1 link in operation |
| | solid red | the device is loading |
| ***Alarm*** | flashes red | critical device failure |
| | solid red | non-critical device failure |
| | solid yellow | no failures, non-critical warnings |
| | solid green | normal operation |
| ***Status*** | solid green | normal operation |
| | off | device power lost |

#### 2.5.1.2 SBC-2000

Light indication of the device in operation is shown in Table  9.

Table 9 — Light indication of the device in operation

| Indicator | Indicator State | Device Status |
|---|---|---|
| ***Alarm*** | flashes red | critical device failure |
| | solid red | non-critical device failure |
| | solid yellow | no failures, non-critical warnings |
| | solid green | normal operation |
| ***Status*** | solid green | normal operation |
| | off | device power lost |
| ***Sync.0, Sync.1*** | solid green | synchronization with an external source |
| | off | external synchronization source disconnected |
| ***Power*** | solid green | powered by power supply unit #1 |
| | solid orange | power supply unit #1 is installed, not supplied with power |
| ***RPS*** | solid green | power supply unit #2 is installed, supplied with power |
| | solid red | power supply unit #2 is installed, not supplied with power |
| | off | power supply unit #2 is not installed |
| ***FAN*** | solid green | all removable fan modules are installed, all fans are operational |
| | solid orange | all removable fan modules are installed, some fans are down |
| | solid red | one or both removable fan modules are not installed |
| ***USB*** | solid green | USB flash is installed |
| | off | USB flash is not installed |

#### 2.5.1.3 SBC-3000

Light indication of the device in operation is shown in Table 10.

Table 10 — Light indication of the device in operation

| Indicator | Indicator State | Device Status |
|---|---|---|
| ***Alarm*** | Flashes red | Critical device failure |
| | Solid red | Non-critical device failure |
| | Solid yellow | No failures, non-critical warnings |
| | Solid green | Normal operation |
| ***Status*** | Solid green | Normal operation |
| | Off | Device power lost |
| ***Sync.1, Sync.2*** | Solid green | Synchronization with an external source |
| | Off | External synchronization source disconnected |
| ***Power*** | Solid green | Powered by power supply unit #1 |
| | Solid orange | Power supply #1 is installed, not supplied with power |
| ***RPS*** | Solid green | Power supply unit #2 is installed, supplied with power |
| | Solid red | Power supply unit #2 is installed, not supplied with power |
| | Off | Power supply unit #2 is not installed |
| ***FAN*** | Solid green | All removable fan modules are installed, all fans are operational |
| | Solid orange | All removable fan modules are installed, some fans are down |
| | Solid red | One or both removable fan modules are not installed |
| ***USB*** | Solid green | USB flash is installed |
| | Off | USB flash is not installed |

### 2.5.2 *Light indication of Ethernet 1000/100 interfaces*

Ethernet interfaces state is shown by LED indicators built into 1000/100 connectors. Possible states are listed in the Table below.

Table 11 — Light indication of Ethernet 1000/100 interfaces

| **Device Status** | **LED/Status** | |
|---|---|---|
| | **Yellow LED 1000/100** | **Green LED 1000/100** |
| A port runs in 1000BASE-T mode, no data transfer | always on | always on |
| A port runs in 1000BASE-T mode, data transfer available | always on | flashes |
| A port runs in 10/100BASE-TX mode, no data transfer | off | always on |
| A port runs in 10/100BASE-TX mode, data transfer available | off | flashes |

### 2.5.3 *Light indication during device boot and reset to factory defaults*

#### ***2.5.3.1 SBC-1000***

For light indication during device boot and reset to factory defaults, see Table 12.

Table 12 — Light indication during device boot and reset to factory defaults

| **№** | **Indication** | | | | **Reset to factory defaults procedure** |
|---|---|---|---|---|---|
| | **Info1** | **Info1** | **Alarm** | **Status** | **(device in operation)** |
| 1 | yellow | yellow | yellow | yellow | Press and hold the F button for 1 second until the following pattern appears. The device will be rebooted in 3 seconds |
| 2 | green | red | yellow | red | Reset to factory defaults has been initiated. This LED pattern will appear only when the device boot begins |
| 3 | yellow | yellow | yellow | yellow | At this step, LED functionality check will be performed: all LEDs including SATA-0 and SATA-1 will light up yellow. |
| 4 | off | off | green | green | At this step, the gateway operating system boot will be performed. To change network parameters and to reset the device configuration to factory defaults, press and hold the F button for 40-45 seconds when the pattern appears (when you hold the button, pattern 2 may appear shortly; ignore it and continue holding the button until the pattern 4 appears). |
| 5 | yellow | yellow | yellow | yellow | When the pattern appears, release the F button.<br>After a while, the following message will be displayed in the console.<br><<<BOOTING IN SAFE-MODE.RESTORING DEFAULT PARAMETERS>>><br>Reset to the factory settings complete |

✓ **It is not recommended to hold down the "F" button while resetting the device: this will bring it to a complete stop. Resumption of operation will only be possible after a power reset.**

! **It is also possible to reset to factory settings on the device being switched on.**
**In this case, skip the 1st step.**

### 2.5.3.2 SBC-2000

For light indication during device boot and reset to factory defaults, see Table 13.

Table 13 — Light indication during device boot and reset to factory defaults

| № | Indication | | | | Reset to factory defaults procedure (device in operation) |
|---|---|---|---|---|---|
| | Alarm | Status | Sync.1 | Sync.2 | |
| 1 | yellow | yellow | yellow | yellow | Press and hold the F button for 1 second until the following pattern appears. The device will be rebooted in 3 seconds |
| 2 | yellow | red | yellow | yellow | Reset to factory defaults has been initiated. This LED pattern will appear only when the device boot begins |
| 3 | - | - | - | - | At this step, the gateway operating system boot will be performed. To change network parameters and restore the device configuration to factory defaults, when the pattern appears press and hold the F button for 40-45 seconds |
| 4 | yellow | yellow | - | - | When the pattern appears, release the F button.<br>After a while, the following message will be displayed in the console.<br><<<BOOTING IN SAFE-MODE.RESTORING DEFAULT PARAMETERS>>><br>Reset to the factory settings complete |

**State of POWER, RPS, FAN, and USB LEDs during reset procedure can be ignored.**
**It is also possible to reset to factory settings on the device being switched on.**
**In this case, skip the 1st step.**

### 2.5.3.3 SBC-3000

Light indication when resetting SBC-3000 to factory settings is the same as for SBC-2000 (see section 2.5.3.2).

## 2.5.4 *Light indication of alarms*

Table 14 contains detailed description of alarms represented by the status of the Alarm LED.

**Indication of CDR files saving**

**If the FTP server is unavailable, CDR entries are saved into device RAM. 30 MB are allocated for CDR file storage. When the memory is full within certain limits, an alarm will be indicated.**

Table 14 — Alarm indication

| Alarm LED State | Fault level | Fault description |
|---|---|---|
| flashes red | critical | Configuration error |
| | | SIP module loss |
| | | Alarm of the SS7 line group (when the *Alarm indication* flag is set in the *«Routing/SS7 line groups»* menu) |
| | | Stream alarm (when the *Alarm indication* flag is set in the menu *"E1 streams/Physical parameters"*) |
| | | FTP server unavailable, CDR file storage RAM is over 50% (15–30 MB) full |
| | | Redundant: slave is disconnected |
| solid red | non-critical (errors) | Alarm of the SS7 line group (when the *Alarm indication* flag is set in the *«Routing/SS7 line groups***»** menu) |
| | | VoIP submodule (MSP) loss |
| | | Synchronization fault (free-run mode operation) |
| | | FTP server unavailable, CDR file storage RAM is to 50% (15–30 MB) full |
| | | Redundant: slave is not connected via one of the links |

| | | |
|---|---|---|
| solid yellow | warnings | Stream remote alarm |
| | | Synchronization from the lower priority source (the one with the higher priority is not available) |
| | | FTP server unavailable, CDR file storage RAM is full up to 5 MB |
| | | Redundant: slave has another firmware version |

## 2.6 'F' Function Button Operation

The F button allows you to reboot the device, restore the factory configuration and to reset the password.

For resetting to factory settings when the device is switched on, see Tables 13 and 14 in Section 2.5.3.

When the factory configuration is restored, you can access the device by IP address 192.168.1.2 (mask 255.255.255.0):

- via Telnet/SSH or console with login **admin**, password **rootpasswd**;
- via web interface with login **admin**, password **rootpasswd**;

Next, you may save the factory configuration, restore password or reboot the device.

## 2.7 Saving factory configuration

To save the factory configuration:

- reset the device to factory settings (Section 2.5.3);
- connect via telnet or console with login **admin**, password **rootpasswd**;
- Enter the ***sh*** command (the device will exit the CLI mode and enter the SHELL mode);
- enter the ***save*** command;
- reboot the device using the ***reboot*** command.

The gateway will be restarted with the factory configuration.

```
*********************************************
*        Welcome to SBC-1000                *
*********************************************

smg login: admin
Password: rootpasswd

********************************************
*           Welcome to  SBC-1000           *
********************************************


Welcome! It is Wed Mar 11 08:45:20 NOVT 2015
SBC> sh
/home/admin # save
tar: removing leading '/' from member names
**********
**********
***Saved successful
New image 1
Restored successful
/home/admin # reboot
```

## 2.8 Password recovery

### 2.8.1 *CLI password recovery*

To recover the password:

- reset the device to factory settings (Section 2.5.3);
- connect via Telnet, SSH, or Console;
- enter the ***sh*** command (the device will exit the cli mode and enter the shell mode);
- enter the ***restore*** command (current configuration will be restored);
- Enter the ***passwd*** command (the device will ask for a new password and its confirmation);
- enter the ***save*** command;
- reboot the device using the ***reboot*** command.

The gateway will be restarted with the current configuration and a new password.

If the device is rebooted without any further actions, the current configuration will be restored on the device without password recovery. The gateway will be restarted with the current configuration and an old password.

```
*********************************************
*        Welcome to SBC-1000                *
*********************************************

smg login: admin
Password: rootpasswd

********************************************
*           Welcome to  SBC-1000           *
********************************************

Welcome! It is Fri Jul  2 12:57:56 UTC 2010
SBC> sh
/home/admin # restore
New image 1
Restored successful
/home/admin # passwd admin
Changing password for admin
New password: 1q2w3e4r5t6y
Retype password: 1q2w3e4r5t6y
Password for admin changed by root
/home/admin # save
tar: removing leading '/' from member names
**********
**********
***Saved successful
New image 0
Restored successful

# reboot
```

### 2.8.2 *WEB password recovery*

To recover the password:

- reset the device to factory settings (Section 2.5.3);
- connect via Telnet, SSH, or Console;
- enter the ***sh*** command (the device will exit the cli mode and enter the shell mode);
- enter the ***restore*** command (current configuration will be restored);

- Connect to the web interface of the device via 192.168.1.2;
- go to «Users: Management»;
- change a password for admin user;
- in the console, enter the ***save*** command;
- reboot the device using the ***reboot*** command.

**It is not recommended to save the configuration from the WEB when restoring the password, as this may result in the loss of the saved gateway configuration. Use the `save` command from the shell mode.**

The gateway will be restarted with the current configuration and a new password.

If the device is rebooted without any further actions, the current configuration will be restored on the device without password recovery. The gateway will be restarted with the current configuration and an old password.

```
*********************************************
*        Welcome to SBC-1000               *
*********************************************

smg login: admin
Password: rootpasswd

********************************************
*           Welcome to  SBC-1000           *
********************************************

Welcome! It is Fri Jul  2 12:57:56 UTC 2010
SBC> sh
/home/admin # restore
New image 1
Restored successful
```

This step is used to change the password from the WEB.

```
/home/admin # save
tar: removing leading '/' from member names
**********
**********
***Saved successful
New image 0
Restored successful

# reboot
```

## 2.9 Delivery Package

SBC standard delivery package includes:

- SBC session border controller;
- A mounting set for 19'' rack;
- The means to connect to the console:
  - for SBC-2000: RJ45-DB9 console port adapter;
  - for SBC-1000: DB9(F) — DB9(F) connection cable;
- 2 x support brackets;
- Operating manual on a CD (optional).

If ordered, delivery package may also include:

- Mini-Gbic (SFP).

## 2.10 Safety instructions

### 2.10.1 *General guidelines*

Any operations with the equipment should comply to the Safety Rules for Operation of Customers' Electrical Installations.

**Operations with the equipment should be carried out only by personnel authorised in accordance with the safety requirements.**

Before operating the device, all engineers should undergo special training.

The device should be connected only to properly functioning supplementary equipment.

SBC can be permanently used provided the following requirements are met:

– Ambient temperature from 0 to +40°C.
– Relative humidity up to 80% at +25°C.
– Atmosphere pressure from 6.0x10*4 to 10.7x10*4 Pa (from 450 to 800 mm Hg).

The device should be not be exposed to mechanical shock, vibration, smoke, dust, water, and chemicals.

To avoid components overheating that may result in device malfunction, do not block air vents or place objects on the equipment.

### 2.10.2 *Electrical Safety Requirements*

Prior to connecting the device to a power source, ensure that the equipment case is grounded with an earth bonding point. The earthing wire should be securely connected to the earth bonding point. The resistance between the protective earth terminal and the earth bus must not exceed 0.1 Ohms.

PC and measurement instruments should be grounded prior to connection to the device. The potential difference between the equipment case and the cases of the instruments must not exceed 1 V.

Prior to turning the device on, ensure that all cables are undamaged and securely connected.

Make sure the device is off, when installing or removing the case.

### 2.10.3 *Electrostatic discharge safety measures*

In order to avoid failures caused by electrostatic discharge, we strongly recommend

– to wear ESD belt, shoes and wrist strap which prevent electrostatic charge accumulation (for wrist strap, make sure that it has a secure fit against the skin) and connect the cable to earthing prior to operation.

### 2.10.4 *Power supply requirements*

#### *2.10.4.1 Power supply type requirements*

The power supply must be from a DC source with an earthed positive potential with a voltage of 48 V, or from an AC remote power supply with a voltage of up to 220 V.

#### *2.10.4.2 Permissible voltage variation requirements for DC power supply*

The voltage of a 48 V power supply can vary between 40.5 V and 57 V.

When the power supply voltage is restored after being below the permissible threshold, the device specifications will be restored automatically.

#### *2.10.4.3 Permissible interference requirements for DC power supply*

The equipment must function properly with power supply interference not exceeding that shown in Table 15.

Table 15 — Permissible interference requirements for DC power supply

| Interference type | Value |
|---|---|
| Permissible voltage deviation from rated value, %<br>duration 50 ms<br>duration 5 ms | <br>-20<br>40 |
| Harmonical component voltage ripple, mV eff.<br>up to 300 Hz<br>from 300 Hz to 150 kHz | <br>50<br>7 |

#### *2.10.4.4 Requirements to interference produced by equipment in power supply circuit*

Voltage values of interference produced by the equipment in the power supply circuit should not exceed the values listed in Table 16.

Table 16 — Requirements to interference produced by equipment in power supply circuit

| Interference type | Value |
|---|---|
| Total interference in the range of 25 Hz to 150 Hz, mV eff. | 50 |
| Selective interference in the range of 300 Hz to 150 kHz, mV eff. | 7 |
| Weighted (psophometric) interference, mV psoph. | 2 |

#### *2.10.4.5 AC power supply requirements*

AC power supply parameters should be as follows:

- Maximum allowed voltage — 220 V.
- Power supply should feature residual current device (RCD).
- Insulation strength of AC power supply circuits against the housing should withstand at least 1000 V peak (in normal conditions).

## 2.11 SBC installation

Check the device for visible mechanical damage before installing and turning it on. In case of any damage, stop the installation, fill in a corresponding document and contact your supplier.

If the device was exposed to low temperatures for a long time before installation, leave it for 2 hours at ambient temperature prior to operation. If the device was exposed to high humidity for a long time, leave it for at least 12 hours in normal conditions prior to turning it on.

Mount the device. The device is intended to be installed into a 19" rack using the mounting set or mounted to the horizontally oriented perforated shelf.

Ground the case of the device after installation. This should be done prior to connecting the device to the power supply. An insulated multiconductor wire should be used for earthing. The device grounding and the earthing wire section should comply with Electric Installation Code. The earth bonding point is located at the right bottom corner of the rear panel, see Figures 5, 7 and 9.

### 2.11.1 *Startup procedure*

1. Connect optical and electrical Ethernet cables to corresponding connectors.
2. Connect the power supply cable to the device. To connect the device to DC power supply, use the cable with cross-section not less than $1mm^2$.
3. If a PC is supposed to be connected to the SBC console port, connect the SBC console port to a PC COM port. PC should be powered off and grounded at the same point with SBC.
4. Ensure that all cables are undamaged and securely connected.
5. Turn the device on and check the front panel LEDs to make sure the terminal is in normal operating conditions.

### 2.11.2 *Support brackets mounting*

The delivery package includes support brackets for rack installation and mounting screws to fix the device case on the brackets.

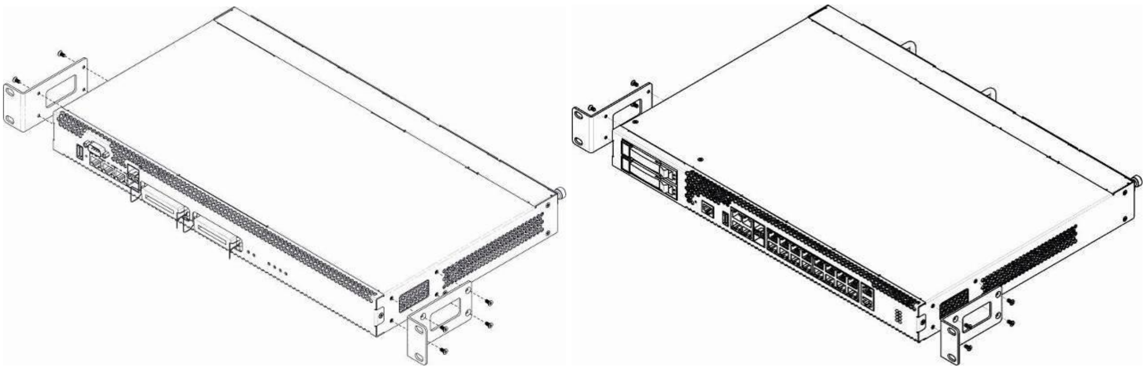


Figure 10 — Mounting brackets for SBC-1000 (left) and SBC-2000 (right)

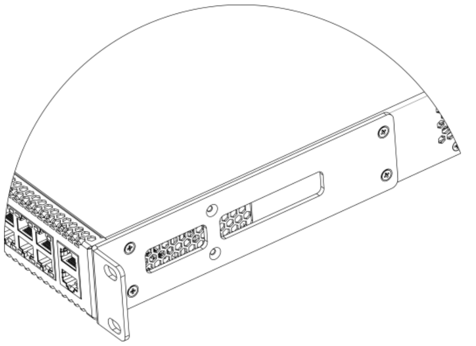


Figure 11 — Mounting brackets for SBC-3000

To install the support brackets:

1. Align four mounting holes in the support bracket with the corresponding holes in the side panel of the device, see Figures 10 and 11.
2. Use a screwdriver to screw the support bracket to the case.

Repeat steps 1 and 2 for the second support bracket.

### 2.11.3 *Device rack installation*

To install the device to the rack:

1. Attach the device to the vertical guides of the rack.
2. Align mounting holes in the support bracket with the corresponding holes in the rack guides. Use the holes of the same level on both sides of the guides to ensure the device horizontal installation.
3. Use a screwdriver to mount the device to the rack.
4. To dismount the device, disconnect cables and remove support bracket screws from the rack. Remove the device from the rack.

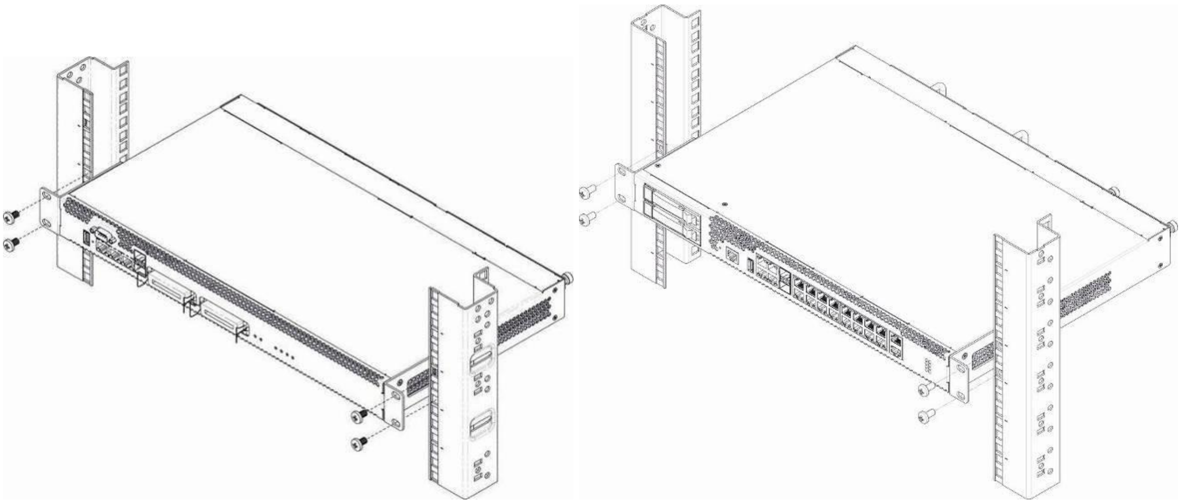


Figure 12 — Rack mounting of SBC-1000 (left) and SBC-2000 (right)

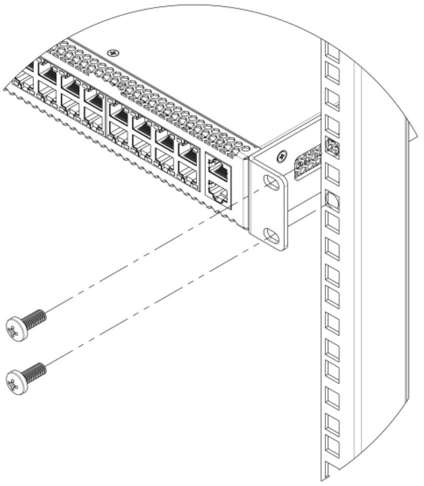


Figure 13 — Rack mounting of SBC-3000

### 2.11.4 *Power module installation*

Device can operate with one or two power modules. The second power module installation is necessary when the device operates under strict reliability requirements.

From the electric point of view, both places for power module installation are identical. In the context of device operation, the power module located closer to the edge is considered as the main module, and the one closer to the centre — as the redundant module. Power modules can be inserted and removed without powering the device off. When additional power module is inserted or removed, the device continues operation without reboot.

SBC has 2 power supply circuit breakers with nominal current 3.15 A. Circuit breakers are not user-serviceable. They should be replaced by qualified service specialists in the manufacturer's service center. The installation of the power modules is shown in the Figure below.

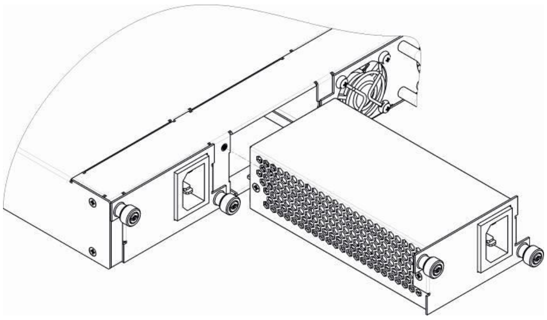


Figure 14 — Power module installation

### 2.11.5 *Removing the housing*

First, disconnect the device from the power supply, disconnect all the cables and remove the device from the rack if necessary (see Section 2.11.3 Device rack installation).

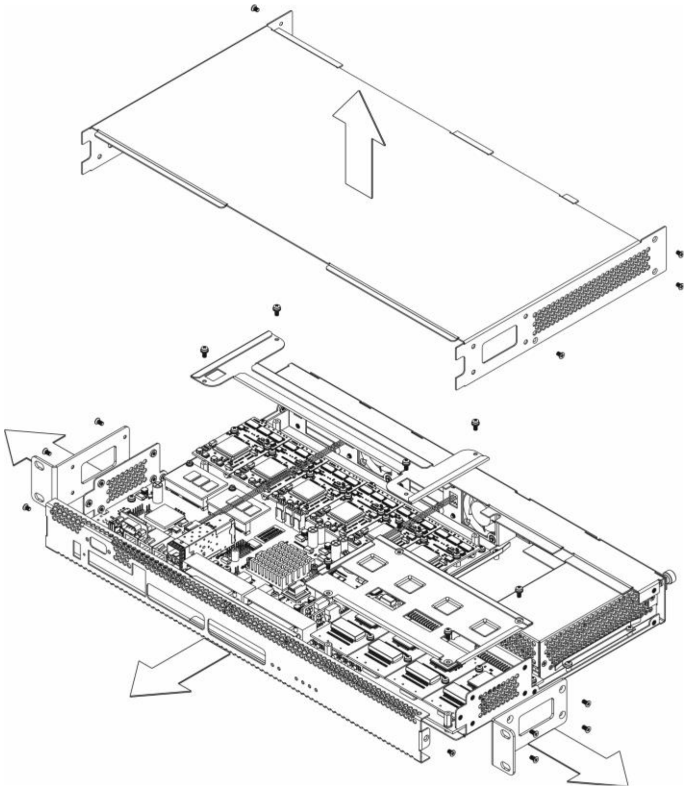


Figure 15 — Case opening procedure of SBC-1000 (based on SMG-1016M)

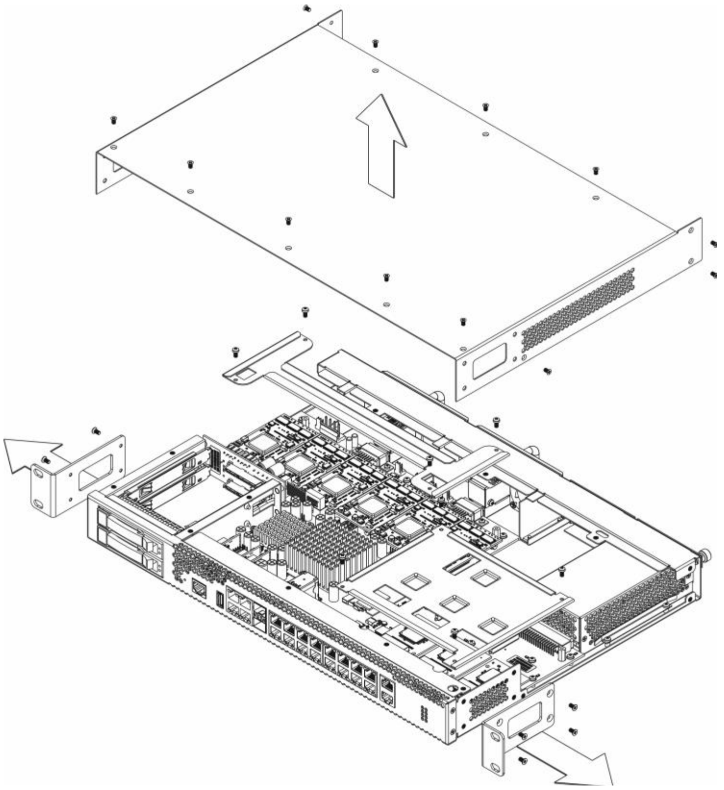


Figure 16 — Case opening procedure of SBC-2000 (based on SMG-2016)

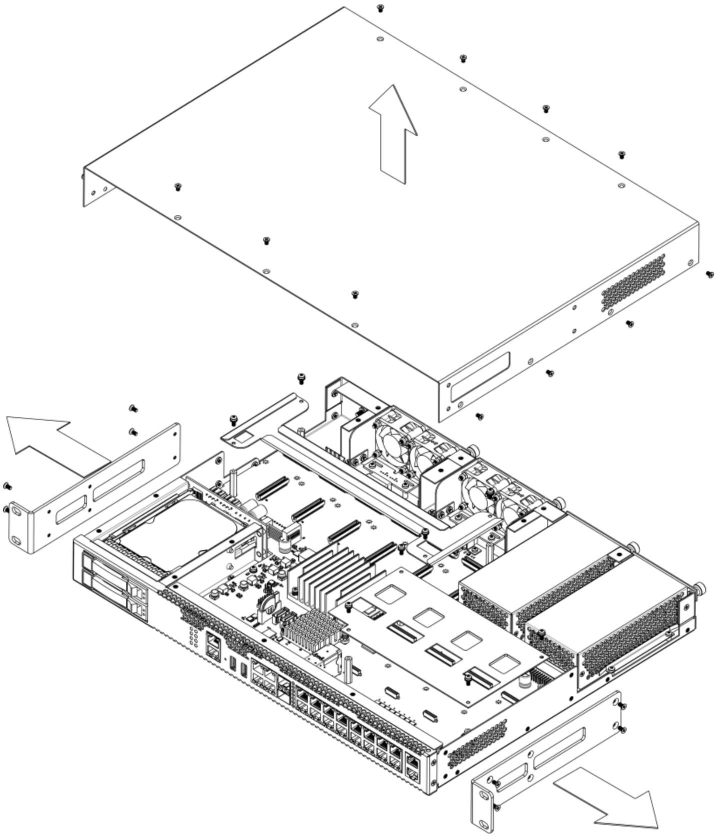


Figure 17 — Case opening procedure of SBC-3000 (based on SMG-3016)

1. Use a screwdriver to remove support brackets from the device housing.
2. **For SBC-1000 only**, the front panel retaining screws must be unscrewed, then pulled to separate from the top and side panels (Figure 15).

3. Remove the screws on the top panel of the device
4. Pull the top panel (cover) of the device to remove it.

For the device assembly, repeat all mentioned steps in the reverse order.

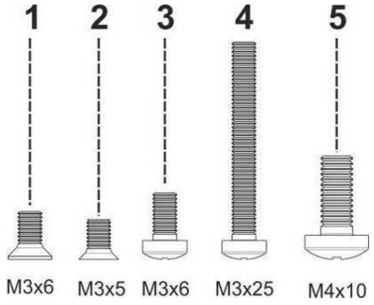


Figure 18 — Screw types for SBC assembly (based on SMG)

Fig. 18 shows screw types, used for assembling the device into case:

1. Support brackets mounting for rack installation.
2. Housing parts mounting.
3. Board, ventilation unit, covers, guides mounting.
4. Fan mounting screw.
5. Earthing screw.

**During the device assembly, avoid using inappropriate screw type for the operations specified. Changing screw type may cause the device failure.**

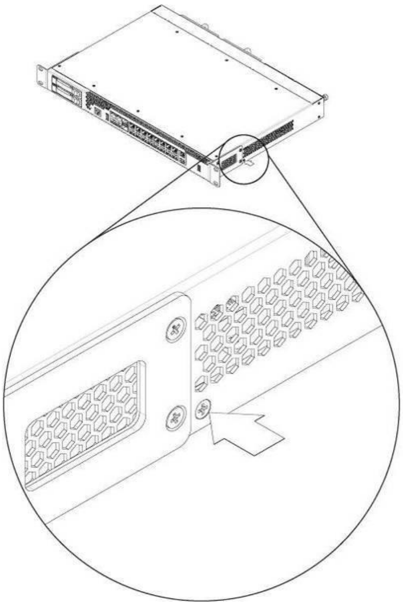


Figure 19 — Assembly into housing

**During SBC assembly, fit the manufacturer-provided screw at the position shown in the Figure above. Changing screw type may cause the device failure.**

### 2.11.6 *Installation of ventilation units*

The device design allows ventilation units replacement even when the terminal is on.

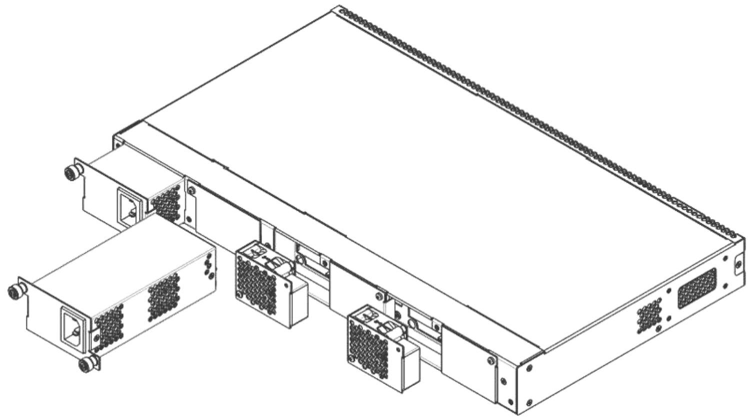


Figure 20 — Ventilation unit in SBC-1000 based on SMG-1016M. Case mounting

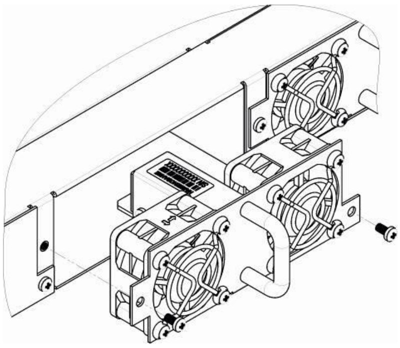


Figure 21 — Ventilation unit in SBC-2000 based on SMG-2016. Case mounting

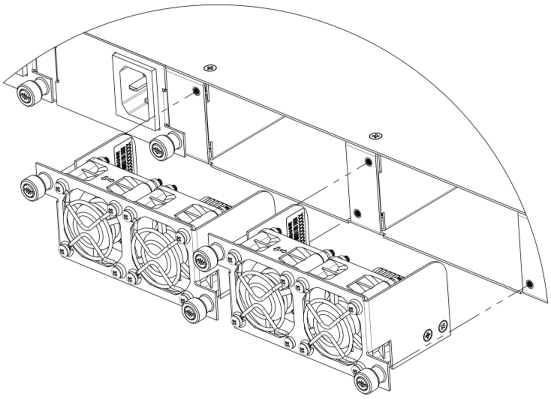


Figure 22 — Ventilation unit in SBC-3000 based on SMG-3016. Case mounting

To remove a ventilation unit, perform the following actions:

1. Use a screwdriver to remove the screws fixing the ventilation unit to the rear panel.
2. Carefully pull the unit until it is removed from the case.
3. Disconnect the unit from the device socket, Figure 23.

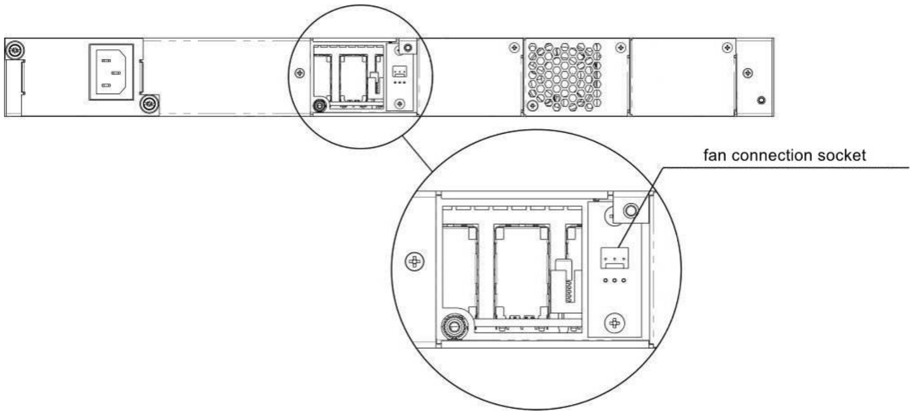


Figure 23 — Fan connection socket in SBC-1000 based on SMG-1016M

To install a ventilation unit, perform the following actions:

1. Connect the unit to the socket.
2. Insert the unit into the case.
3. Screw the ventilation unit to the rear panel.

### 2.11.7 *SSD installation for SBC-1000*

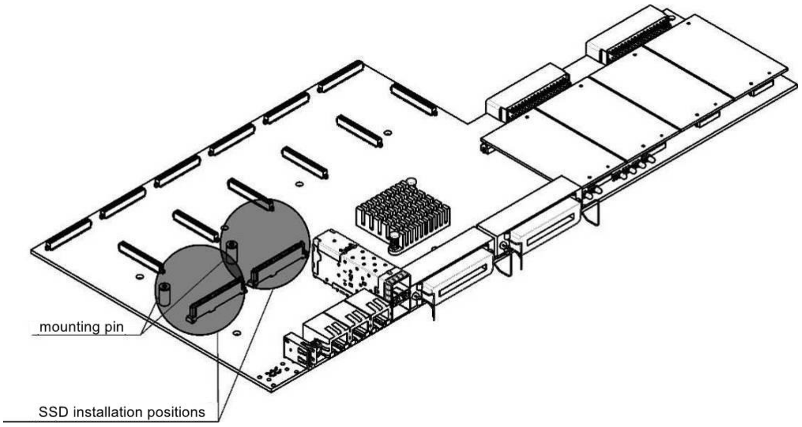


Figure 24 — SSD installation procedure

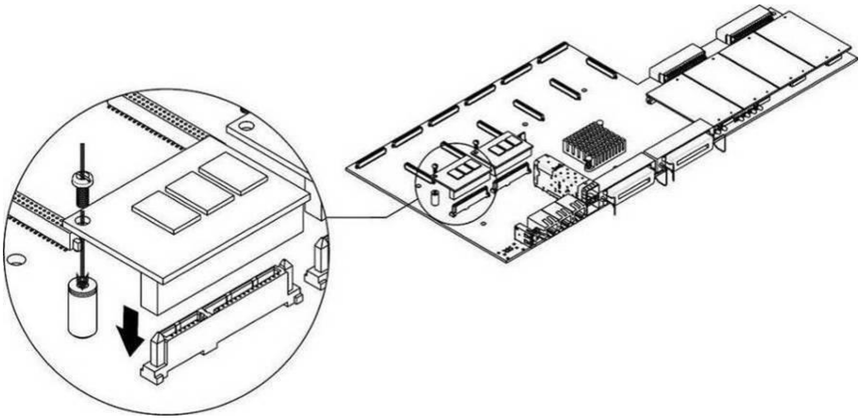
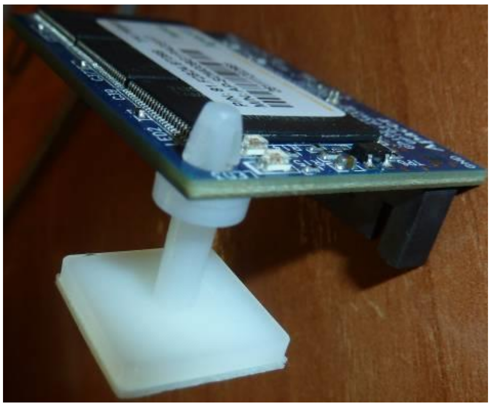


Figure 25— SSD mounting procedure

1. Check if the device is supplied with power.
2. If yes, disconnect the power supply.
3. Remove the device from the rack if necessary (see Section 2.11.3).



4. Open the casing of the device (more information in Section 2.11.5).
5. If the mounting sleeve (see Figure 24) is missing from the device board, use the removable stand:
   a. mount the SSD onto the fixing stand;
   b. Remove the top protective layer from the adhesive surface of the fixing stand;
6. Install the drive into a vacant slot (2 slots are available in total — see Figure 24), and if the mounting sleeve is present on the board, fasten the drive with a screw as shown in Figure 25.

For the SSD removal, repeat all mentioned steps in the reverse order.

### 2.11.8 *SATA drive installation for SBC-2000 and SBC-3000*

SATA drives may be additionally included in the device delivery package. A drive slot is designed to accomodate 2.5'' for factor drives up to 12.5 mm thick.

Installation of SATA drives:

1. Remove the cradle from the device housing (Figure 6, Element 1). To do this, press the button on the right until the ejector knob is released, pull the knob to remove the cradle from the housing.
2. Remove the mounting kit located under the ejector knob, Figure 26.
3. Secure the drive in the cradle tray, Figure 27.
4. Insert the cradle with the SATA drive installed back into slot and push the ejector knob until it fits with a click.

For the SATA drive removal, repeat all mentioned steps in the reverse order.

You may also install and/or remove SATA drives when the device in energized.

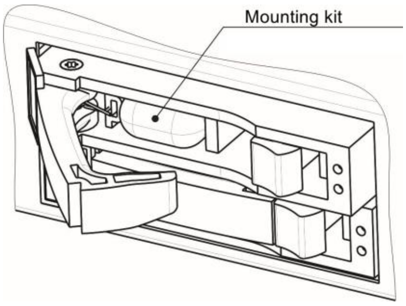


Figure 26 — Mounting kit location on delivery

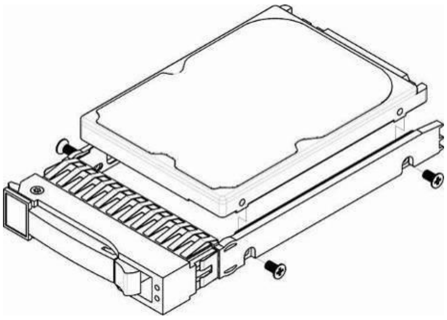


Figure 27 — Mounting SATA drive into cradle tray

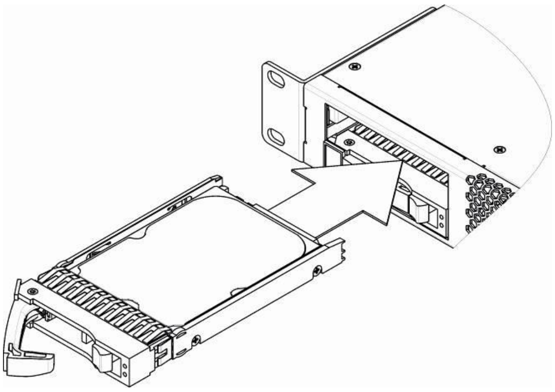


Figure 28 — Installation of SATA drive in the device housing

### 2.11.9 *RTC battery replacement*

RTC (electric circuit designed for automatic chronometric data metering — current time, date, day of the week, etc.) located on the device board features a battery which specifications are listed in the Table below.

| | |
|---|---|
| Battery type | Lithium |
| Form-factor | CR2032 (CR2024 installation is possible) |
| Voltage | 3V |
| Capacity | 225mAh |
| Diameter | 20 mm |
| Thickness | 3.2mm |
| Shelf life / expiration date | 5 years |
| Storage conditions | from -20 to +35°C |

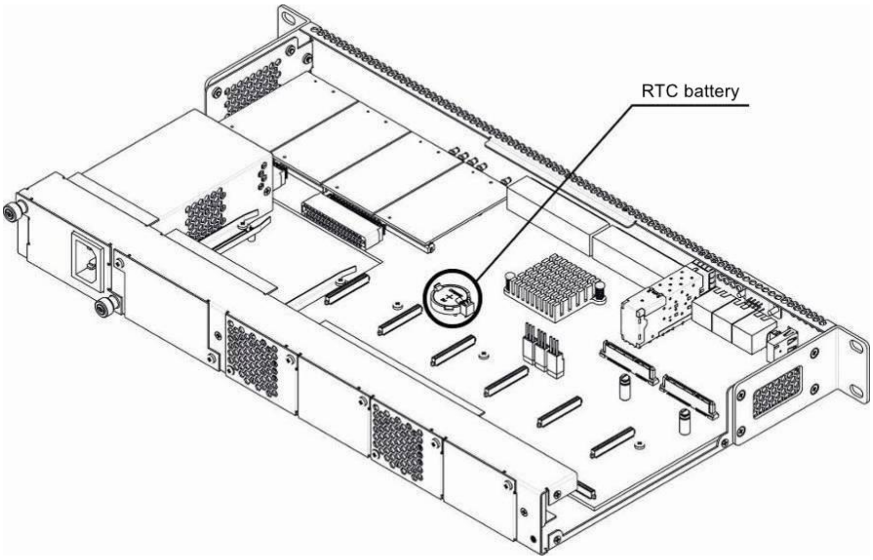


Figure 29 — RTC battery position for SBC-1000 (based on SMG-1016M)

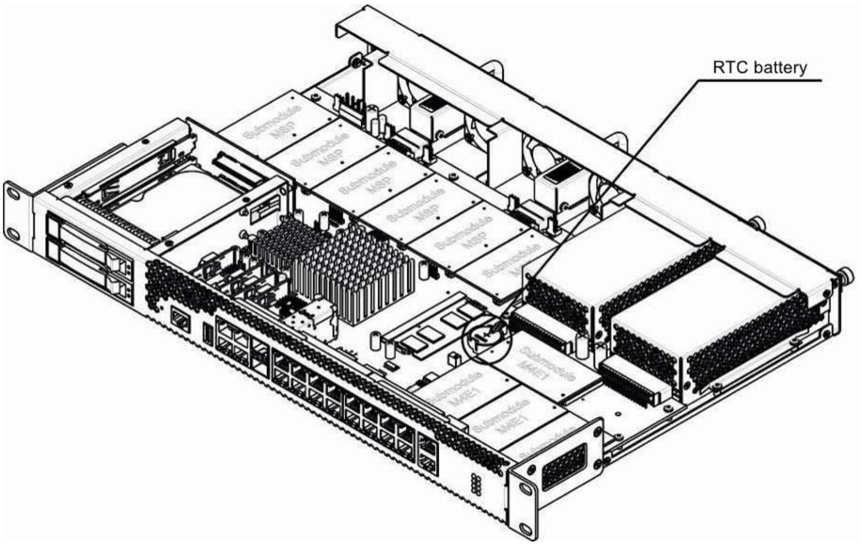


Figure 30 — RTC battery position for SBC-2000 (based on SMG-2016)

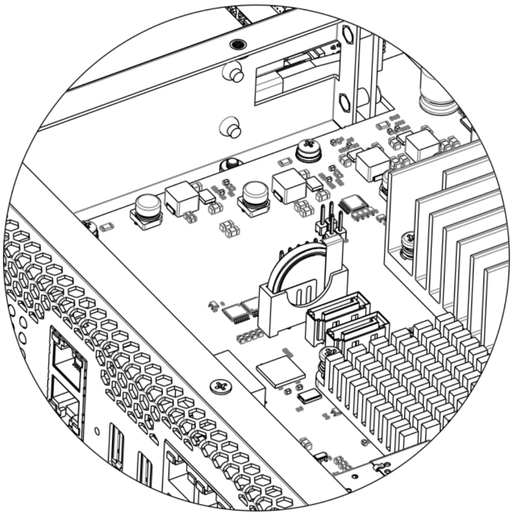


Figure 31 — RTC battery position for SBC-3000 (based on SMG-3016)

If the battery shelf life is expired, replace it with a new one to ensure correct and continuous operation. The replacement procedure as follows:

1. Check if the device is supplied with power.
2. If yes, disconnect the power supply.
3. Remove the device from the rack if necessary (see Section 2.11.3).
4. Open the casing of the device (more information in Section 2.11.5).
5. Remove the used battery (Figure 29, Figure 30 and Figure 31) and install a new one into the same position.

For the device assembly, repeat all mentioned steps in the reverse order.

**If NTP synchronization is disabled, you should set the system date and time after RTC battery replacement.**

**Used batteries should be recycled accordingly.**

# 3 GENERAL SWITCH OPERATION GUIDELINES

The easiest way to configure and monitor a device is to use the web configurator, so we recommend you to use it for these purposes.

In order to prevent an unauthorized access to the device, we recommend changing the password for Telnet, SSH and console access (default username: **admin**, password: **rootpasswd**) and administrator password for web configurator access. For setting a password for access through Telnet and console, see Section 4.2. We recommend to write down and store defined passwords in a safe place, inaccessible by intruders. We also strongly recommend not to open access to the device via Telnet, SSH and web from a public network.

On a local network, it is better to use an HTTPS connection to access the web configurator instead of an HTTP connection (configuration process is described in Section SSL/TLS configuration). It is better to use SSH instead of Telnet to access the CLI. Access protocols are selected in the network interface settings (described in Section 4.1.4.3). It is also recommended to allocate a separate interface on SBC for management in a dedicated VLAN. To restrict access to SBC administration from individual nodes, you can also use a whitelist of addresses from which SBC can be managed (more details in Section 4.1.8.6).

In order to prevent device configuration data loss, e.g. after reset to factory settings, we recommend making configuration backup copies and storing them on a PC each time significant changes are made.

It is recommended to use trusted and protected DNS and NTP servers on the network. It is better to place the equipment behind a firewall with ingress filtering configured on it.

## 3.1 Ensuring call security

SBC has several mechanisms for call security:

- A built-in firewall that provides the following functions (more details in section 4.1.8.5 Static firewall):
  - Filtering by IP address, port and protocol;
  - Filtering of users by geographical area (GeoIP);
  - Filtering by strings contained in messages.
- Call restrictions in Rule Set rules (see Section 4.1.3.5):
  - The "reject" action prevents passing of calls under conditions covered by the rule. For example, you can use a rule to forbid international calls "Name from To header" with the name mask "^\+*[78]10.+";
  - Action "send to..." using filters. For example, you can set a restriction on calls to Russia only, using the rule «Name from To header» as a mask «^7[3489].{9}$»;
  - A time limit on the validity of the rule. In this way, it is possible to limit the validity of the communication service or communication restrictions by combining the validity time limit and the "reject" and "send to..." rules.
- DoS attacks prevention (see Section 4.1.8.7):
  - ICMP flood protection. In this mode SBC will not respond to ICMP type 8 and type 13 requests;
  - Port scan detection. SBC will analyze access attempts and, if port scanning is detected, will block the intruder;
  - List of forbidden client applications. SBC will block SIP requests by detecting specified patterns in the User-Agent, which correspond to popular SIP scanners and utilities to carry out various attacks;
  - SIP flood protection. SBC analyses both network hosts and individual subscribers for activities considered as flooding or attempts at password brute-forcing. SBC is also starting to replace 404 responses with 403 to make it more difficult to scan number allocation.

# 4 DEVICE CONFIGURATION

There are four ways to connect to the device: via web configurator, Telnet, SSH or via cable via RS-232 (access via RS-232, SSH or Telnet uses the CLI command console).

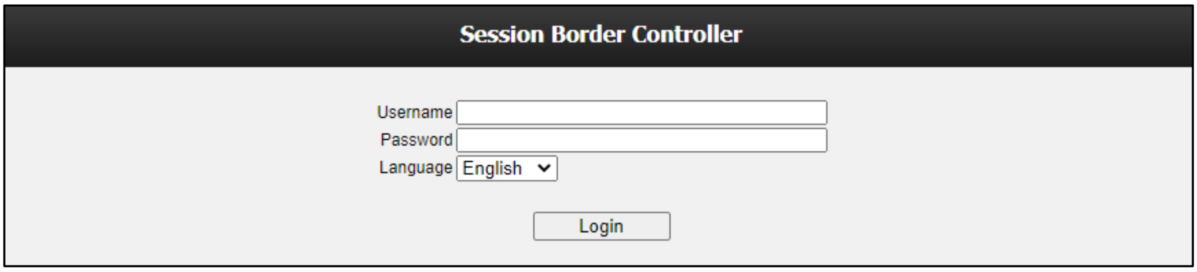
**To save changes made to configuration into the non-volatile memory, use «Service/Save configuration to flash» menu in the web configurator or the `copy running to startup save` command of CLI.**

## 4.1 SBC configuration via web configurator

To configure the device, establish connection using a web browser (hypertext viewer), e.g. Google, Firefox, Internet Explorer, etc. Enter the device IP address in the browser address bar:

**SBC factory default IP address — 192.168.1.2, network mask—255.255.255.0**

After entering IP address the device will request username and password. You can also select an interface language.



Session Border Controller

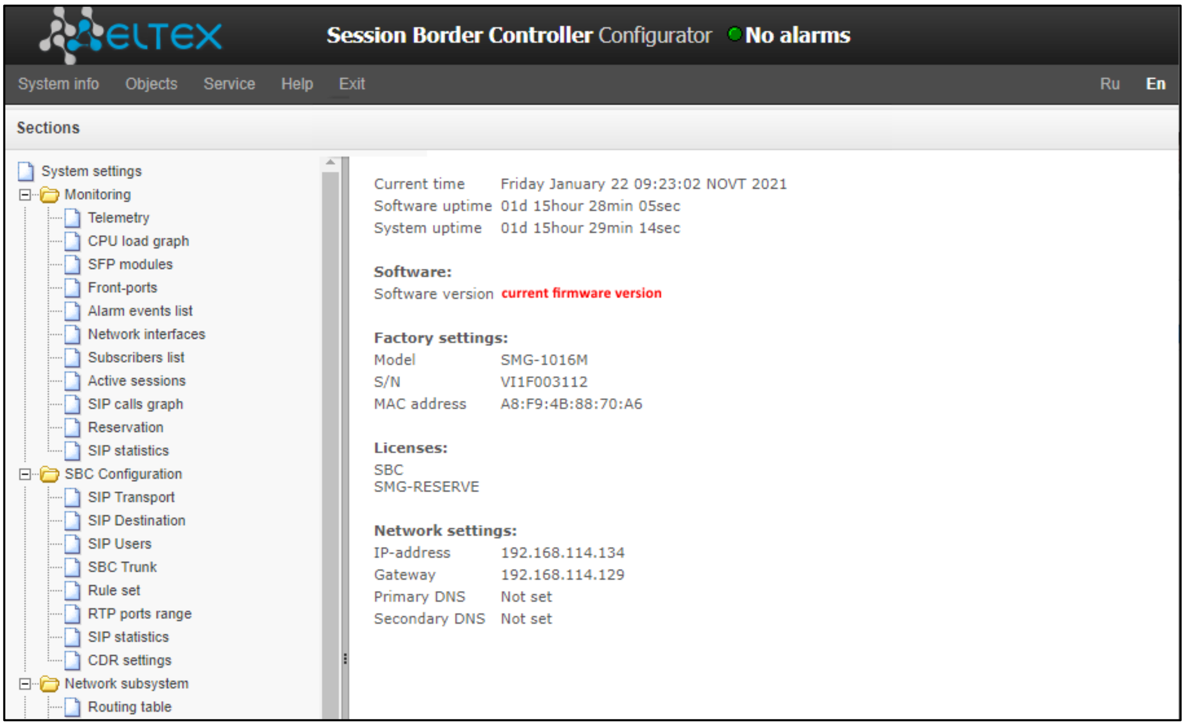
Username

Password

Language English

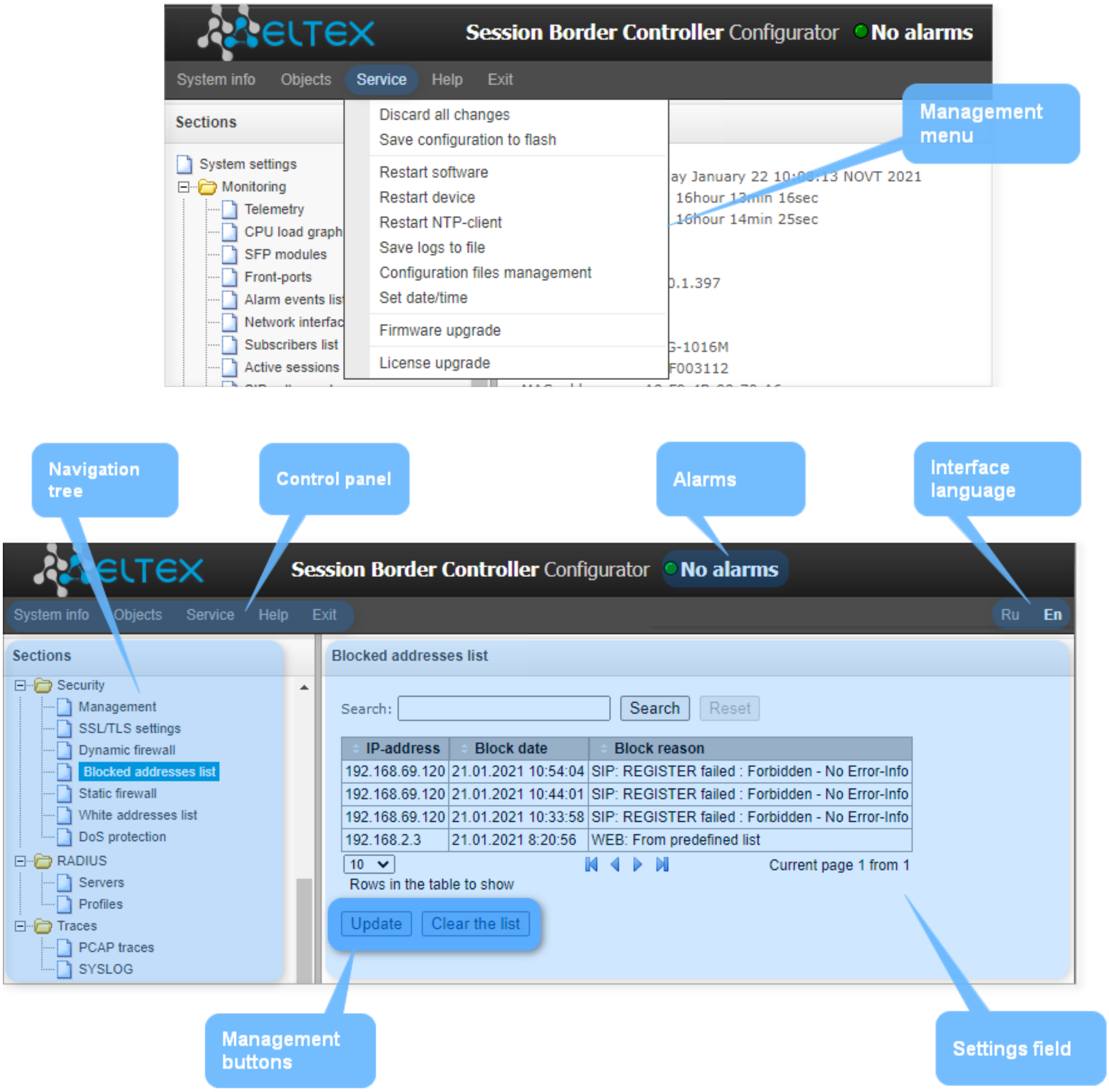
**When starting up for the first time, use username: *admin*, password: *rootpasswd*.**

After accessing the Web Configurator, the *'System info'* menu will open.



```
Current time      Friday January 22 09:23:02 NOVT 2021
Software uptime   01d 15hour 28min 05sec
System uptime     01d 15hour 29min 14sec

Software:
Software version  current firmware version

Factory settings:
Model             SMG-1016M
S/N               VI1F003112
MAC address       A8:F9:4B:88:70:A6

Licenses:
SBC
SMG-RESERVE

Network settings:
IP-address        192.168.114.134
Gateway           192.168.114.129
Primary DNS       Not set
Secondary DNS     Not set
```

The Figure below shows web configurator navigation elements.



Blocked addresses list

| IP-address | Block date | Block reason |
|---|---|---|
| 192.168.69.120 | 21.01.2021 10:54:04 | SIP: REGISTER failed : Forbidden - No Error-Info |
| 192.168.69.120 | 21.01.2021 10:44:01 | SIP: REGISTER failed : Forbidden - No Error-Info |
| 192.168.69.120 | 21.01.2021 10:33:58 | SIP: REGISTER failed : Forbidden - No Error-Info |
| 192.168.2.3 | 21.01.2021 8:20:56 | WEB: From predefined list |

Figure 32 — Web configurator navigation elements

User interface window is divided into several areas.

*Navigation tree* — is used to control the settings field. Navigation tree contains the hierarchy of management sections and nested menus.

*Settings field* — based on user's choice. Allows viewing device settings and enter configuration data.

*Control panel* — panel for controlling the settings field and device firmware status.

*Management menu* — drop down menus for the settings field and device firmware status management.

*Alarms* — displays the current highest-priority alarm and serves as a link for the fault events log operations.

*Authorization* — link for passwords used for web configurator access.

*Interface language* — buttons for interface language switching.

*Management icons* — controls for working with the settings field objects' management. They duplicate the 'Objects' menu on the control panel:

- *— Add an object;*
- *— Edit object;*
- *— Delete an object;*
- *— View object.*

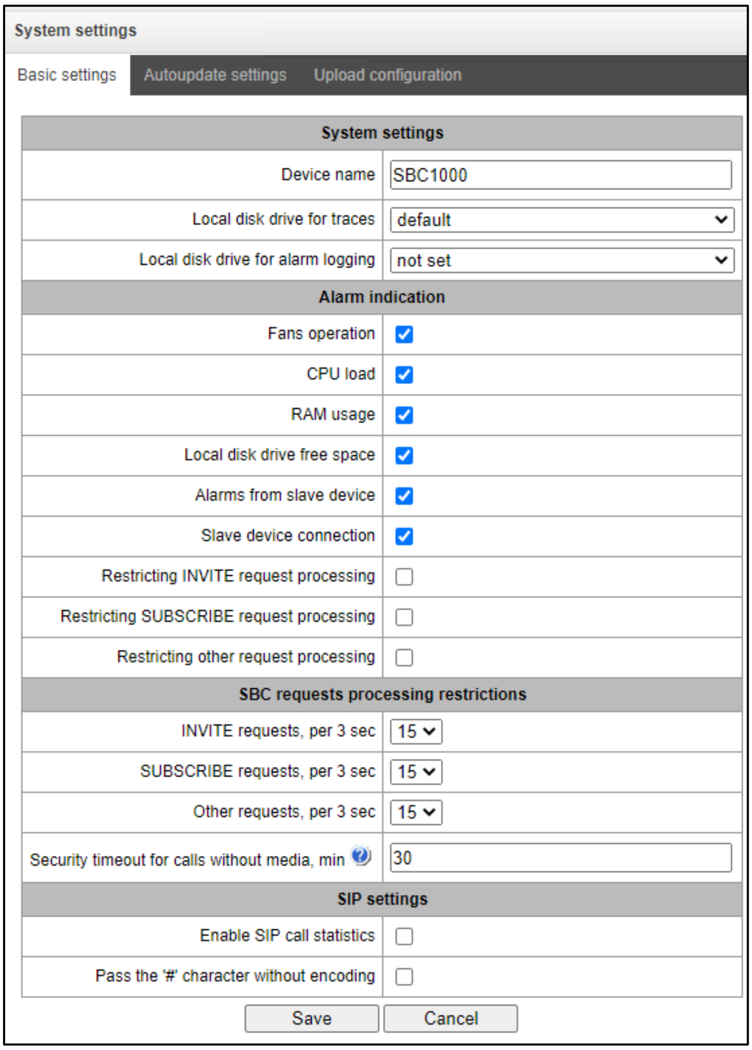
*Management buttons* — controls for working with settings the field.

To prevent unauthorized access to device in the future, it is recommended to change password (see Section 4.1.8.1).

✓ **The button ('Tooltip') next to an edit item provides an explanation of the parameter.**

### 4.1.1 *System settings*

This section is used to configure system parameters and request processing limits.



System settings

Basic settings | Autoupdate settings | Upload configuration

| | |
|---|---|
| **System settings** | |
| Device name | SBC1000 |
| Local disk drive for traces | default |
| Local disk drive for alarm logging | not set |
| **Alarm indication** | |
| Fans operation | ☑ |
| CPU load | ☑ |
| RAM usage | ☑ |
| Local disk drive free space | ☑ |
| Alarms from slave device | ☑ |
| Slave device connection | ☑ |
| Restricting INVITE request processing | □ |
| Restricting SUBSCRIBE request processing | □ |
| Restricting other request processing | □ |
| **SBC requests processing restrictions** | |
| INVITE requests, per 3 sec | 15 |
| SUBSCRIBE requests, per 3 sec | 15 |
| Other requests, per 3 sec | 15 |
| Security timeout for calls without media, min | 30 |
| **SIP settings** | |
| Enable SIP call statistics | □ |
| Pass the '#' character without encoding | □ |

***Basic settings***

- *Device name* — the device name displayed in the web configurator header (not used in this software version);
- *Local disk drive for traces* — it is possible to save debugging information (traces) to RAM or to an installed SSD:
  - *default* — debugging information (traces) is saved to RAM;
  - */mnt/sdX* — a path to a local SSD drive, the setting is displayed when a SSD drive is installed. When you select a drive, a logs directory will be created to store the trace files;

**Tracing file storage is available for SSD/SATA drives only; this function is not available for USB storage devices.**

- *Local disk drive for alarm logging* — selection of an SSD drive for saving critical alarm messages to non-volatile memory. This option may be required for troubleshooting device restart or failure issues.
  - */mnt/sdX* — select a path to a local storage device**.** When this option is enabled, the file 'alarm.txt' containing alarm data will be created on the storage device.

***Example of alarm.txt file:***

```
0. 24/09/13 20:03:22. Software started.
1. 24/09/13 20:03:22. state ALARM. Sync from local source, but sync source table not empty
2. 24/09/13 20:03:22. state OK. PowerModule#1. Unit ok! or absent
3. 24/09/13 20:03:31. state OK. MSP-module lost: 1
4. 24/09/13 20:03:34. state OK. MSP-module lost: 2
5. 24/09/13 20:03:38. state OK. MSP-module lost: 3
6. 24/09/13 20:03:42. state OK. MSP-module lost: 4
```

File format description:
0, 1, 2… — event ordinal number;
24/09/13 — event occurrence date;
20:03:22 — event occurrence time;
ALARM/OK — event current state (OK— alarm is resolved, ALARM — alarm is active).

Table 17 — Alarm message examples

| **Alarm message** | **Meaning** |
|---|---|
| Configuration has not been read | Configuration file error |
| High CPU utilization | High CPU load alarm |
| Port Scan Detector disabled | Information message about disabled Port Scan protection in the configuration |
| The dynamic firewall blocked the new address | A warning about blocking a new address with the reason in the description |
| Subscriber registration is restricted | Registration request received, the service of which is restricted |
| Call is restricted | A call came in that is not allowed to be serviced |
| Running firmware V.1.X.X.X | Firmware is running |
| Slave device has another firmware version | Reserve devices have different firmware versions |
| No connection with slave | No connection with the reserve device either completely or on one of the links. In the second case, the parameters will indicate on which link the connection is lost |
| Change of state in the reserve group | Renegotiation of the devices in the reserve |

| | |
|---|---|
| Operating memory is low | Operating memory is low. 3 levels of alarm possible — warning (less than 25% of free memory left), alarm (less than 10%), critical alarm (less than 5%) |
| Failed to send CDR files via FTP | Problem with sending a CDR file to an FTP server |
| Device software startup | Device software startup |

***Alarm Indication***

- *Fans operation* — when the flag is set, a fan failure alarm will be generated in the control system;
- *CPU load* — when the flag is set, a high CPU load alarm will be generated in the control system;
- *RAM usage* — when the flag is set, an alarm on running out of free RAM will be generated in the control system;
- *Local disk drive free space* — when the flag is set, an alarm on running out of free space on external drives will be generated in the control system;
- *Alarms from slave device* — when the flag is set, the above alarms will be sent to the control system from a redundant device;
- Slave device connection — when the flag is set, alarms on no communication with a redundant device on the local and global links will be sent to the control system;
- Restricting INVITE request processing — when the flag is set, alarms on exceeding the maximum number of simultaneous INVITE requests set under "SBC requests processing restrictions" will be sent to the control system;
- Restricting SUBSCRIBE request processing — when the flag is set, alarms on exceeding the maximum number of simultaneous SUBSCRIBE requests set under "SBC requests processing restrictions" will be sent to the control system;
- Restricting other request processing — when the flag is set, alarms on exceeding the maximum number of simultaneous requests other than INVITE and SUBSCRIBE will be sent to the control system.

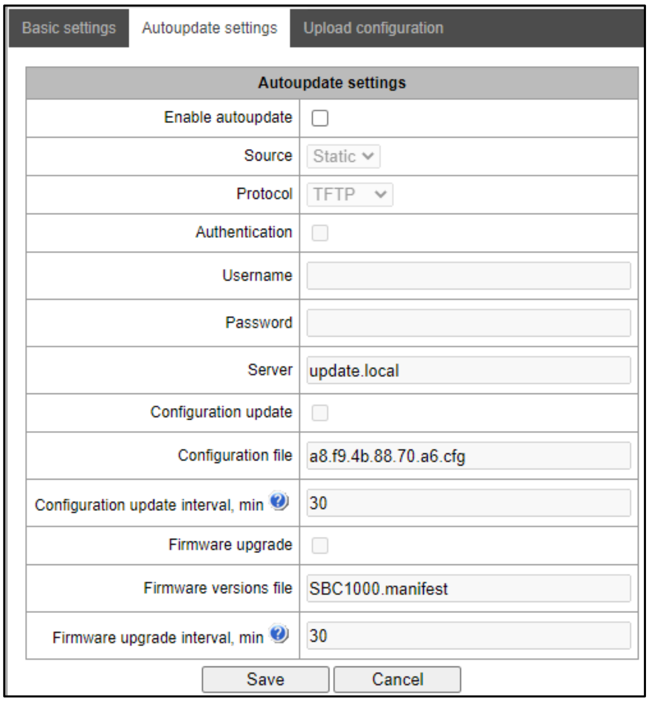
***SBC requests processing restrictions***

- *INVITE requests, per 3 sec* — the number of INVITE requests processed within three seconds. If more requests are received, those exceeding the threshold will not be processed;
- *SUBSCRIBE requests, per 3 sec* — the number of SUBSCRIBE requests processed within three seconds. If more requests are received, those exceeding the threshold will not be processed;
- *Other requests, per 3 sec* — the number of requests other than INVITE and SUBSCRIBE processed within three seconds. If more requests are received, those exceeding the threshold will not be processed;
- *Security timeout for calls without media, min* — the time interval after which a call established between the devices will be rejected if no RTP packets are transmitted between them over the speaking channel.

***SIP settings***

- *Enable SIP call statistics* — enables the maintenance of call statistics. Statistics are displayed in the "SIP Statistics" monitoring section;

- *Pass the '#' character without encoding* — when enabled, SBC sends the '#' character as '#' to the outgoing leg and when disabled it sends it as '%23'.



| Autoupdate settings | |
|---|---|
| Enable autoupdate | □ |
| Source | Static |
| Protocol | TFTP |
| Authentication | □ |
| Username | |
| Password | |
| Server | update.local |
| Configuration update | □ |
| Configuration file | a8.f9.4b.88.70.a6.cfg |
| Configuration update interval, min | 30 |
| Firmware upgrade | □ |
| Firmware versions file | SBC1000.manifest |
| Firmware upgrade interval, min | 30 |

***Autoupdate settings***

SBC can automatically retrieve configuration and software version files from the Auto-configuration server (hereinafter referred to as "server") with a set period of time.

After downloading a configuration, SBC will wait for completion of all active calls before applying the new configuration. Either the configuration will be applied with the new firmware before rebooting.

The firmware version description file contains information about the firmware available on the server (versions and file names). There the time for updating can also be set. The file format should be as follows:

*<FIRMWARE version number>;<FIRMWARE file name>;<allowed update time, hour>*

- *Number of firmware version* — defines completely, including assembling version;
- *Firmware file name* must have .bin extension;
- *It is not necessary to assign permitted update time.*

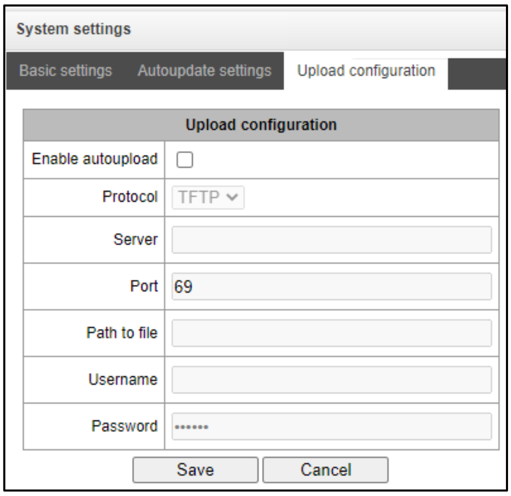
  SBC will be updated as soon as active calls are finished. If you specify the time, SBC will be updated only within this time range.

**Example of firmware description file:**

1.8.0.99; smg2016_firmware_sbc_1.8.0.99.bin
1.8.0.100; smg2016_firmware_sbc_1.8.0.100.bin;9-13

- *Enable autoupdate* — enable automatic configuration and firmware updates;
- *Source* — selecting a source of information about the server:
  - *Static* — server information is entered in the appropriate field and stored on SBC;
  - *DHCP (interface name)* — server information will be obtained on the selected interface via DHCP from option 66, version and configuration file name information will be obtained from option 67;
- *Protocol* — select a protocol for connecting to the server;
- *Authentication* — use authentication to access the server (for FTP, HTTP, HTTPS protocols);
- *Username* — name (login) for server access;
- *Password* — password for server access;
- *Server* — server IP address or domain name. Used with the 'Static' source selected;
- *Configuration update* — enables a configuration update from the server;
- *Configuration file* — configuration file name. The name must have '.cfg' extension with maximum length of 64 characters;
- *Configuration update interval, min* — the interval at which the server is checked for configuration;
- *Firmware upgrade* — allows firmware updates from the server;

- *Firmware versions file* — firmware version file name. The name mast have '.manifest' extension with maximum length of 64 characters;
- *Firmware upgrade interval, min* — the interval at which the server is checked for new firmware.



System settings

| Upload configuration | |
|---|---|
| Enable autoupload | □ |
| Protocol | TFTP |
| Server | |
| Port | 69 |
| Path to file | |
| Username | |
| Password | •••••• |

***Upload configuration***

SBC can automatically upload the configuration to an external FTP/TFTP server whenever it is saved to non-volatile memory.

- *Enable autoupload* — enables the configuration upload function;
- *Protocol* — select a protocol according to which the upload will be performed. FTP or TFTP is supported;
- *Server* — the IP address of the server to which the upload will be made;
- *Port* — the server port to which the upload will be made;
- *Path to file* — the directory on the server where the configuration will be saved;
- *Username* — the name for authentication when using the FTP protocol;
- *Password* — the password for authentication when using the FTP protocol.

## 4.1.2 *Monitoring*

### *4.1.2.1 Telemetry*

This section contains information on the device telemetric sensor readings as well as the information on power supplies and fans installed.

***Temperature sensors***

***For SBC-1000:***

- *TempSensor #0* — CPU temperature;
- *TempSensor #1* — switch temperature.

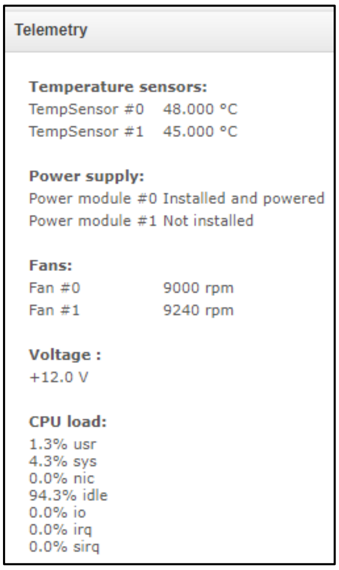
***For SBC-2000:***

- *CPU temperature* — temperature of the processor.

***Power supply***

- *Power module #0* — the status of the power supply in the zero position;
- *Power module #1* — the status of the power supply in the first position.

***Monitoring –> Telemetry***



```
Telemetry

Temperature sensors:
TempSensor #0   48.000 °C
TempSensor #1   45.000 °C

Power supply:
Power module #0 Installed and powered
Power module #1 Not installed

Fans:
Fan #0          9000 rpm
Fan #1          9240 rpm

Voltage :
+12.0 V

CPU load:
1.3% usr
4.3% sys
0.0% nic
94.3% idle
0.0% io
0.0% irq
0.0% sirq
```

Possible power supply states:

- *Installed* — power supply is installed.
- *Not installed* — power supply is not installed.
- *Powered* — voltage is applied.
- *Not powered* — voltage is not applied.

***Fans***

- *Fan #N* — information on the status of the N fan and its speed (e.g. 9600 rpm).

✓ **SBC-1000 has 2 fans, SBC-2000 has 4 fans and SBC-3000 has 4 fans.**

***Voltage[1]:***

- *Internal voltage (+12V)* — 12V voltage sensor status details.

***Current voltage[2]:***

- *+12.0 V* — information on the status of the 12 V voltage sensor;
- *+5.0 V* — information on the status of the 5 V voltage sensor;
- *+3.3 V* — information on the status of the 3.3 V voltage sensor;
- *+2.5 V* — information on the status of the 2.5 V voltage sensor;
- *+1.8 V* — information on the status of the 1.8 V voltage sensor;
- *+1.5 V* — information on the status of the 1.5 V voltage sensor;
- *+1.2 V* — information on the status of the 1.2 V voltage sensor;
- *+1.0 V* — information on the status of the 1 V voltage sensor;
- *CPU* — information on the supply voltage status of the CPU;
- *CPU Vcore* — information on the supply voltage status of the CPU core;
- *RTC battery* — real-time clock battery voltage status details.

***CPU load:***

- *USR* — the percentage of CPU time used by user programs;
- *SYS* — the percentage of CPU time used by kernel processes;
- *NIC* — the percentage of CPU time used by programs with a changed priority;
- *IDLE* — the percentage of idle CPU resources;
- *IO* — the percentage of CPU time spent on I/O operations;
- *IRQ* — the percentage of CPU time spent on hardware interrupts processing;
- *SIRQ* — the percentage of CPU time spent on software interrupts processing.

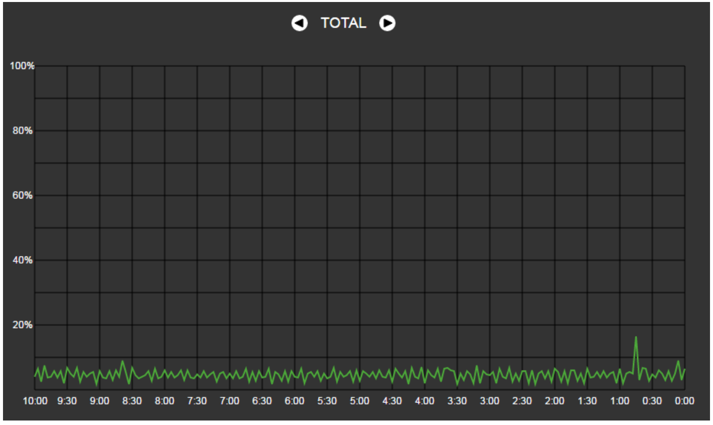
#### *4.1.2.2 CPU load graph*

This section contains information on CPU utilization in real time (10-minute interval). Statistics charts are based on average data for each 3-second device operation interval.

[1] Only for SBC-1000

[2] Only for SBC-2000 and SBC-3000

*Monitoring –> CPU load graph*



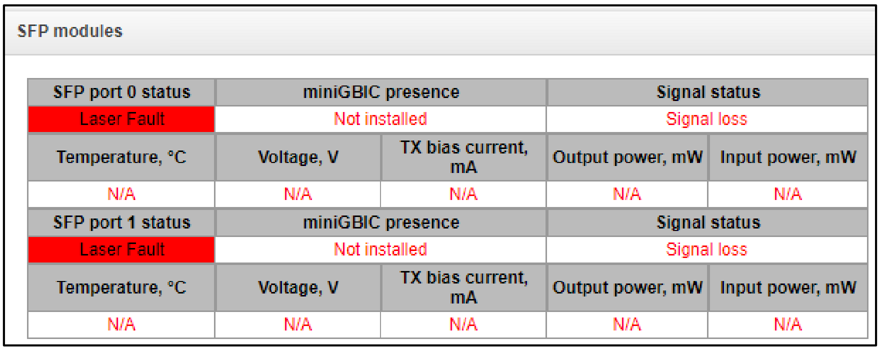
To navigate between specific parameters in monitoring charts, use the buttons ◀ and ▶. To facilitate visual identification, all charts have different colors.

- *TOTAL* — the total percentage of CPU load;
- *IO* — the percentage of CPU time spent on I/O operations;
- *IRQ* — the percentage of CPU time spent on hardware interrupts processing;
- *SIRQ* — the percentage of CPU time spent on software interrupts processing;
- *USR* — the percentage of CPU time used by user programs;
- *SYS* — the percentage of CPU time used by kernel processes;
- *NIC* — the percentage of CPU time used by programs with a changed priority.

### 4.1.2.3 SFP modules monitoring

This section contains status indication and optical line parameters.

*Monitoring –> SFP modules*



SFP modules

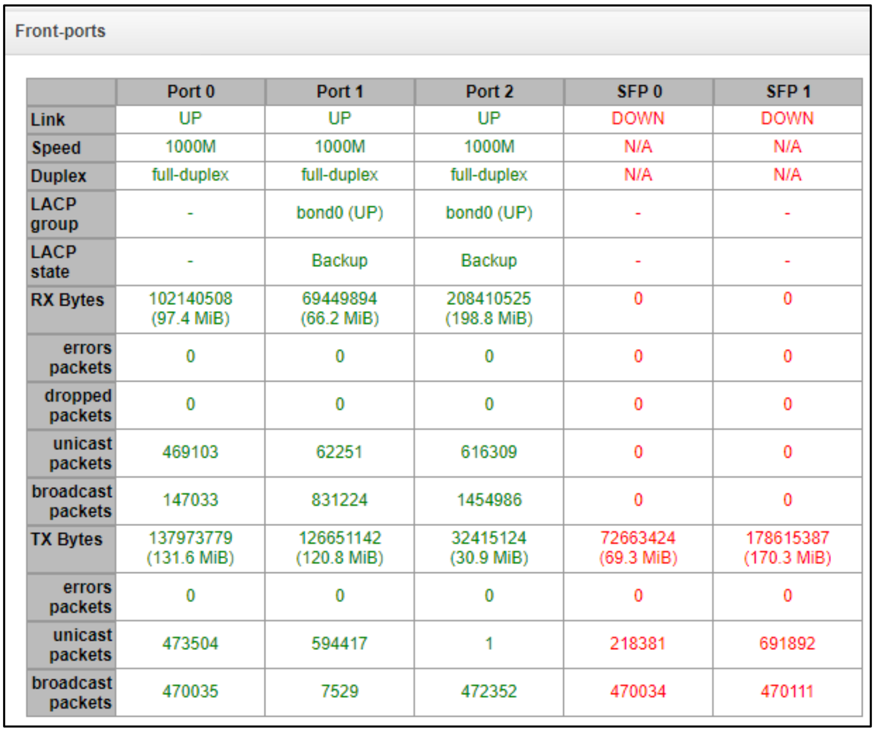
| | | | | |
|---|---|---|---|---|
| SFP port 0 status | miniGBIC presence | | Signal status | |
| Laser Fault | Not installed | | Signal loss | |
| Temperature, °C | Voltage, V | TX bias current, mA | Output power, mW | Input power, mW |
| N/A | N/A | N/A | N/A | N/A |
| SFP port 1 status | miniGBIC presence | | Signal status | |
| Laser Fault | Not installed | | Signal loss | |
| Temperature, °C | Voltage, V | TX bias current, mA | Output power, mW | Input power, mW |
| N/A | N/A | N/A | N/A | N/A |

- *SFP port 0 status, SFP port 1 status* — optical module status:
  - *miniGBIC presence* — module installation indication (module installed, module not installed);
  - *Signal status* — indication of signal loss (signal lost, in operation);
  - *Temperature, °C* — optical module temperature;
  - *Voltage, V* — optical module power supply voltage, V;
  - *TX bias current, mA* — bias current during transmission, mA;
  - *Input power, mW* — signal power at reception, mW;
  - *Output power, mW* — signal strength at transmission, mW.

### 4.1.2.4 Switch front port monitoring

The section displays information on the physical state of the switch ports: link availability, committed rate on the port and transmission mode. If the port is a combo port (copper and optical connectors), the port number will be marked "(SFP)". It disappears if the dual port is active and connected with a copper cable.

***Monitoring –> Front-ports***



Front-ports

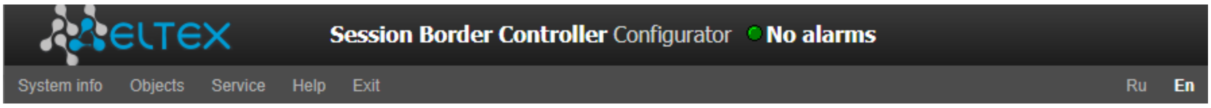
| | Port 0 | Port 1 | Port 2 | SFP 0 | SFP 1 |
|---|---|---|---|---|---|
| Link | UP | UP | UP | DOWN | DOWN |
| Speed | 1000M | 1000M | 1000M | N/A | N/A |
| Duplex | full-duplex | full-duplex | full-duplex | N/A | N/A |
| LACP group | - | bond0 (UP) | bond0 (UP) | - | - |
| LACP state | - | Backup | Backup | - | - |
| RX Bytes | 102140508<br>(97.4 MiB) | 69449894<br>(66.2 MiB) | 208410525<br>(198.8 MiB) | 0 | 0 |
| errors packets | 0 | 0 | 0 | 0 | 0 |
| dropped packets | 0 | 0 | 0 | 0 | 0 |
| unicast packets | 469103 | 62251 | 616309 | 0 | 0 |
| broadcast packets | 147033 | 831224 | 1454986 | 0 | 0 |
| TX Bytes | 137973779<br>(131.6 MiB) | 126651142<br>(120.8 MiB) | 32415124<br>(30.9 MiB) | 72663424<br>(69.3 MiB) | 178615387<br>(170.3 MiB) |
| errors packets | 0 | 0 | 0 | 0 | 0 |
| unicast packets | 473504 | 594417 | 1 | 218381 | 691892 |
| broadcast packets | 470035 | 7529 | 472352 | 470034 | 470111 |

- *Link* — the status of the cable connection on the port (UP/DOWN);
- *Speed* — committed rate on the port;
- *Duplex* — data transmission mode (half-full-duplex);
- *LACP group* — the LACP channel the port is included in and its status (UP/DOWN)
- *LACP state* — the mode in which the port is operating (active/backup)
- *RX Bytes* — a storage counter of received bytes, including the different types of received packets;
- *TX Bytes* — a storage counter of transmitted bytes, including the different types of transmitted packets.

### 4.1.2.5 Alarm events list

When an alarm occurs, information about it is displayed in the header of the Web Configurator. If there are several active alarms, the web configurator header will display the most critical one at the time.

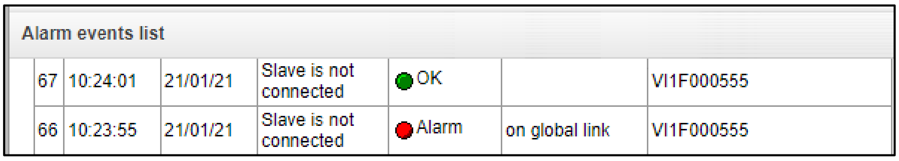
When there are no alarms, the message «*No alarms*» will be shown.



**Session Border Controller** Configurator ● **No alarms**

In the *Alarm events list* menu, the list of alarm events, ranked by date and time is displayed. There is also the *"Clear"* button that removes all information messages and resolved alarms from the current list.

***Monitoring — Alarm events list***



Alarm events list

| | | | | | | |
|---|---|---|---|---|---|---|
| 67 | 10:24:01 | 21/01/21 | Slave is not connected | ● OK | | VI1F000555 |
| 66 | 10:23:55 | 21/01/21 | Slave is not connected | ● Alarm | on global link | VI1F000555 |

***Alarm table***

- *№* — alarm sequence number;
- *Time* — alarm occurrence time in HH:MM:SS format;
- *Date* — alarm occurrence date in DD/MM/YY format;
- *Type* — alarm types are given in Table 18.

Table 18 — Alarm types

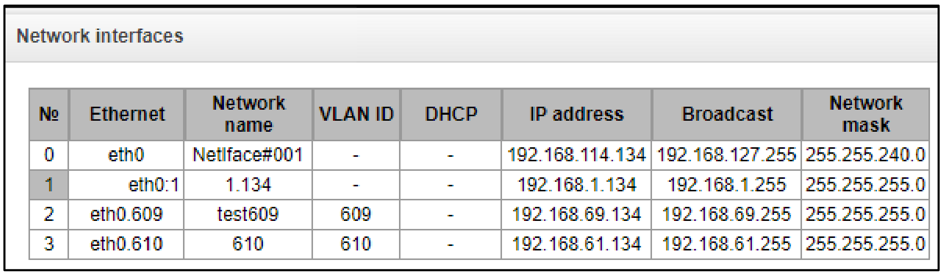
| Type | Meaning |
|---|---|
| Configuration has not been read | Configuration file read error |
| MSP-module lost | MSP module connection loss |
| CDR-FTP | Error in transferring CDR files to the FTP server. There are 3 levels of failure — warning (5 MB of data accumulated), alarm (5-15 MB), critical alarm (15-30 MB) |
| Operating memory is low | Operating memory is low. 3 levels of alarm possible — warning (less than 25% of free memory left), alarm (less than 10%), critical alarm (less than 5%) |
| Subscriber registration expired | Subscriber registration expired |
| SBC subsystem overload | One of SBC subsystems is overloaded |
| Call is restricted | A call came in that is not allowed to be serviced |
| Subscriber registration is restricted | Registration request received, the service of which is restricted |
| Running firmware V.1.X.X.X | Firmware is running |
| Slave device has another firmware version | Reserve devices have different firmware versions |
| No connection with slave | No connection with the reserve device either completely or on one of the links. In the second case, the parameters will indicate on which link the connection is lost |
| Change of state in the reserve group | Renegotiation of the devices in the reserve |

- *State* — fault state status:
  - *critical alarm, flashing red LED* — fault requires immediate intervention of the service personnel, affects device operation and provisioning of communication services;
  - *alarm, red LED* — non-critical fault, also requires intervention of the service personnel;
  - *warning, yellow LED* — fault does not affect provisioning of communication services;
  - *information message, gray indicator* — not alarm, is intended to inform about the event that occurred;
  - *OK, green LED* — fault is resolved.
- *Parameters* — code for the alarm localization. For a crash «Operating memory is low» has the following form:
  - [00:XX:YY], where XX — free memory, YY — total memory.
- *Description* — text description of the problem. For example, the amount of remaining RAM, the number of the subscriber who ran out of registration.

### 4.1.2.6 *Network interfaces*

This section allows monitoring of network interfaces (tagged/untagged/VPN) and viewing VPN users connected to the device.

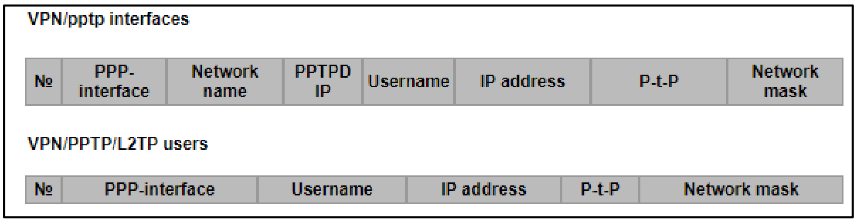
***Monitoring –> Network interfaces***



Network interfaces

| № | Ethernet | Network name | VLAN ID | DHCP | IP address | Broadcast | Network mask |
|---|---|---|---|---|---|---|---|
| 0 | eth0 | NetIface#001 | - | - | 192.168.114.134 | 192.168.127.255 | 255.255.240.0 |
| 1 | eth0:1 | 1.134 | - | - | 192.168.1.134 | 192.168.1.255 | 255.255.255.0 |
| 2 | eth0.609 | test609 | 609 | - | 192.168.69.134 | 192.168.69.255 | 255.255.255.0 |
| 3 | eth0.610 | 610 | 610 | - | 192.168.61.134 | 192.168.61.255 | 255.255.255.0 |

- *Ethernet* — Ethernet interface name;
- *Network name* — the name to which the specified network settings are associated;
- *VLAN ID* — a virtual network identifier (for a tagged interface);
- *DHCP* — the status of using DHCP to obtain network settings automatically (requires a DHCP server in the operator's network);
- *IP address, Broadcast, Network mask* — network settings of the interface (if DHCP is not used).



VPN/pptp interfaces

| № | PPP-interface | Network name | PPTPD IP | Username | IP address | P-t-P | Network mask |
|---|---|---|---|---|---|---|---|

VPN/PPTP/L2TP users

| № | PPP-interface | Username | IP address | P-t-P | Network mask |
|---|---|---|---|---|---|

### *VPN/pptp interfaces*

- *PPP-interface* — the interface name;
- *Network name* — the name to which the specified network settings are associated;
- *PPTPD IP* — the IP address of the PPTP server for connection;
- *Username* — user identifier;
- *IP address, P-t-P, Network mask* — network settings of the interface.

### *VPN/PPTP/L2TP users*

- *PPP-interface* — the interface name;
- *Username* — user identifier;
- *IP address, P-t-P, Network mask* — network settings of the interface.

### *4.1.2.7 Subscribers list*

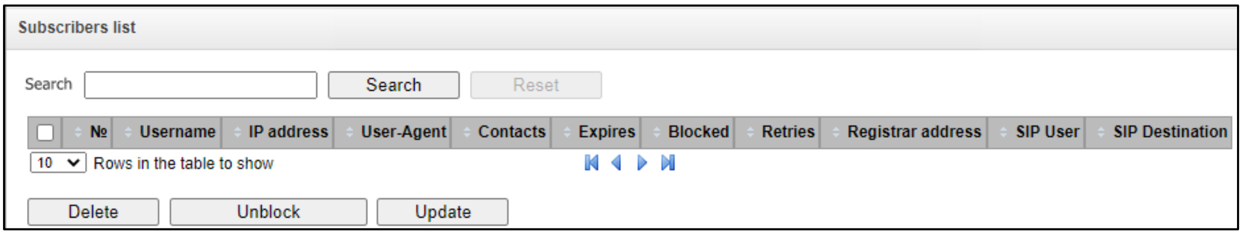
This submenu displays subscribers registered via SBC-2000.

In the field *"Rows in the table to show"* the number of entries to be displayed on the page is specified. The table on the right contains the current page number and the total number of pages. To navigate between pages, the arrows ⏮ ◀ ▶ ⏭ under the table are used. A single arrow is for moving to the next/previous page, a double one is to display the first/the last page.

The entries may have different colours depending on the status of the subscriber:

- black — standard subscriber who works normally;
- red — the subscriber is blocked by the DoS security system;
- orange — the subscriber has been blocked but is now unblocked manually or when the DoS protection timer expires.

***Monitoring –> Subscribers list***



Subscribers list

Search [ ] Search Reset

| □ | № | Username | IP address | User-Agent | Contacts | Expires | Blocked | Retries | Registrar address | SIP User | SIP Destination |
|---|---|---|---|---|---|---|---|---|---|---|---|

10 Rows in the table to show ⏮ ◀ ▶ ⏭

Delete Unblock Update

- *Search* — check the list of registered SIP subscribers for the subscriber number;
- № — subscriber sequence number;
- *Username* — a public number of a registered subscriber, a value passed in the header To of the request REGISTER;
- *IP address* — an IP address from which SBC received a subscriber registration request;

- *User-Agent* — a SIP client of a subscriber, a value passed in the header User-Agent header of the request REGISTER;
- *Contacts* — private addresses of a registered subscriber, values passed in Contact headers of the request REGISTER;
- *Expires* — the time remaining until the end of the registration period. For a subscriber who has been unblocked, the forgiveness time is displayed, after which the blocking counters for that caller will be reset;
- *Blocked* — a subscriber blocking status. If the subscriber is blocked, requests from the subscriber will be answered with a 403 response without processing it;
- *Retries* — a number of access attempts a subscriber has made before being blocked;
- *Registrar address* — an address and a port of a device that approved a subscriber's registration. This is usually a Softswitch address and port;
- *SIP User* — the name of the SIP User via which the subscriber has registered;
- *SIP Destination* — the name of the SIP Destination to which the subscriber registration request has gone and from where it has been approved.

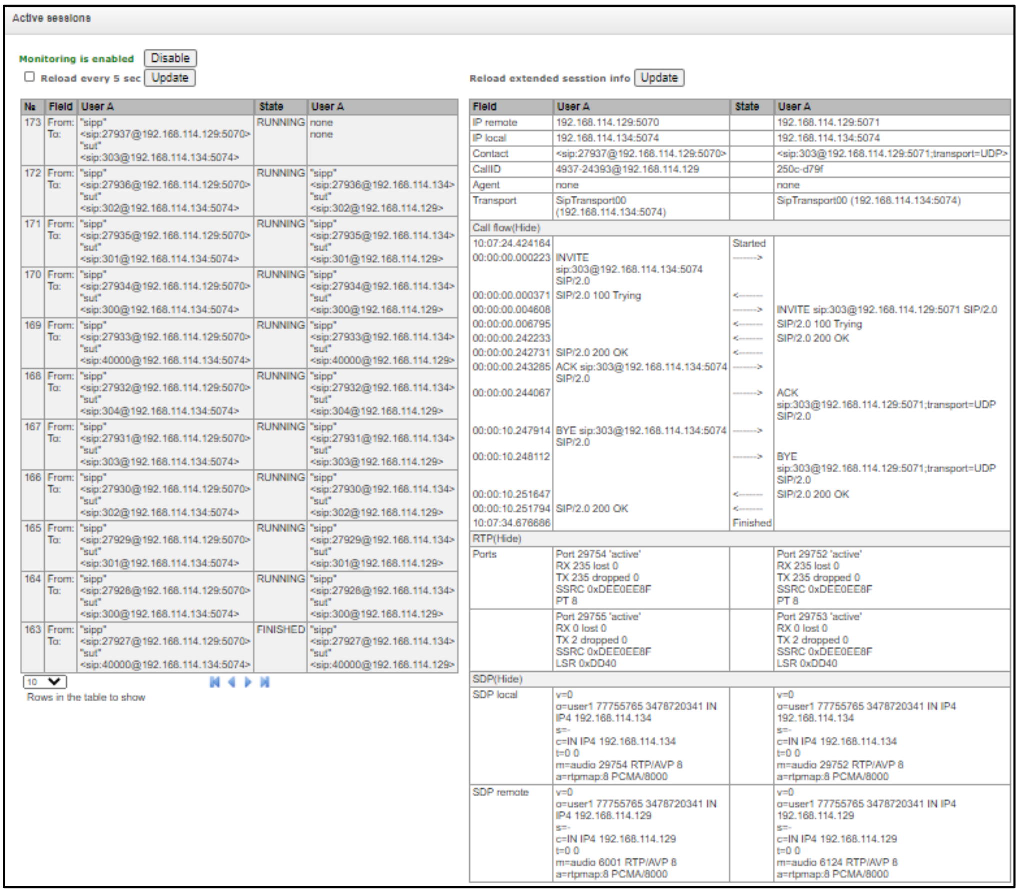
Below the table, there are the following buttons:

- *Delete* — allows removing a subscriber or a group of subscribers from a database of registered subscribers. To delete subscribers, check the box next to a corresponding entry and press the *"Delete"* button;
- *Unblock* — allows taking a subscriber out of the blocked state;
- *Update* — allows updating the list of registered subscribers.

### *4.1.2.8 Active sessions*

The active call sessions established via SBC are displayed here. Signal messages for each call and a media flow can be viewed. Completed calls are stored in the monitor for one minute.

***Monitoring –> Active sessions***



Active sessions

Monitoring is enabled

□ Reload every 5 sec

| № | Field | User A | State | User A |
|---|---|---|---|---|
| 173 | From:<br>To: | "sipp"<br><sip:27937@192.168.114.129:5070><br>"sut"<br><sip:303@192.168.114.134:5074> | RUNNING | none<br>none |
| 172 | From:<br>To: | "sipp"<br><sip:27936@192.168.114.129:5070><br>"sut"<br><sip:302@192.168.114.134:5074> | RUNNING | "sipp"<br><sip:27936@192.168.114.134><br>"sut"<br><sip:302@192.168.114.129> |
| 171 | From:<br>To: | "sipp"<br><sip:27935@192.168.114.129:5070><br>"sut"<br><sip:301@192.168.114.134:5074> | RUNNING | "sipp"<br><sip:27935@192.168.114.134><br>"sut"<br><sip:301@192.168.114.129> |
| 170 | From:<br>To: | "sipp"<br><sip:27934@192.168.114.129:5070><br>"sut"<br><sip:300@192.168.114.134:5074> | RUNNING | "sipp"<br><sip:27934@192.168.114.134><br>"sut"<br><sip:300@192.168.114.129> |
| 169 | From:<br>To: | "sipp"<br><sip:27933@192.168.114.129:5070><br>"sut"<br><sip:40000@192.168.114.134:5074> | RUNNING | "sipp"<br><sip:27933@192.168.114.134><br>"sut"<br><sip:40000@192.168.114.129> |
| 168 | From:<br>To: | "sipp"<br><sip:27932@192.168.114.129:5070><br>"sut"<br><sip:304@192.168.114.134:5074> | RUNNING | "sipp"<br><sip:27932@192.168.114.134><br>"sut"<br><sip:304@192.168.114.129> |
| 167 | From:<br>To: | "sipp"<br><sip:27931@192.168.114.129:5070><br>"sut"<br><sip:303@192.168.114.134:5074> | RUNNING | "sipp"<br><sip:27931@192.168.114.134><br>"sut"<br><sip:303@192.168.114.129> |
| 166 | From:<br>To: | "sipp"<br><sip:27930@192.168.114.129:5070><br>"sut"<br><sip:302@192.168.114.134:5074> | RUNNING | "sipp"<br><sip:27930@192.168.114.134><br>"sut"<br><sip:302@192.168.114.129> |
| 165 | From:<br>To: | "sipp"<br><sip:27929@192.168.114.129:5070><br>"sut"<br><sip:301@192.168.114.134:5074> | RUNNING | "sipp"<br><sip:27929@192.168.114.134><br>"sut"<br><sip:301@192.168.114.129> |
| 164 | From:<br>To: | "sipp"<br><sip:27928@192.168.114.129:5070><br>"sut"<br><sip:300@192.168.114.134:5074> | RUNNING | "sipp"<br><sip:27928@192.168.114.134><br>"sut"<br><sip:300@192.168.114.129> |
| 163 | From:<br>To: | "sipp"<br><sip:27927@192.168.114.129:5070><br>"sut"<br><sip:40000@192.168.114.134:5074> | FINISHED | "sipp"<br><sip:27927@192.168.114.134><br>"sut"<br><sip:40000@192.168.114.129> |

10

Rows in the table to show

Reload extended sesstion info

| Field | User A | State | User A |
|---|---|---|---|
| IP remote | 192.168.114.129:5070 | | 192.168.114.129:5071 |
| IP local | 192.168.114.134:5074 | | 192.168.114.134:5074 |
| Contact | <sip:27937@192.168.114.129:5070> | | <sip:303@192.168.114.129:5071;transport=UDP> |
| CallID | 4937-24393@192.168.114.129 | | 250c-d79f |
| Agent | none | | none |
| Transport | SipTransport00<br>(192.168.114.134:5074) | | SipTransport00 (192.168.114.134:5074) |
| Call flow(Hide) | | | |
| 10:07:24.424164 | | Started | |
| 00:00:00.000223 | INVITE sip:303@192.168.114.134:5074 SIP/2.0 | -------> | |
| 00:00:00.000371 | SIP/2.0 100 Trying | <------- | |
| 00:00:00.004608 | | -------> | INVITE sip:303@192.168.114.129:5071 SIP/2.0 |
| 00:00:00.006795 | | <------- | SIP/2.0 100 Trying |
| 00:00:00.242233 | | <------- | SIP/2.0 200 OK |
| 00:00:00.242731 | SIP/2.0 200 OK | <------- | |
| 00:00:00.243285 | ACK sip:303@192.168.114.134:5074 SIP/2.0 | -------> | |
| 00:00:00.244067 | | -------> | ACK sip:303@192.168.114.129:5071;transport=UDP SIP/2.0 |
| 00:00:10.247914 | BYE sip:303@192.168.114.134:5074 SIP/2.0 | -------> | |
| 00:00:10.248112 | | -------> | BYE sip:303@192.168.114.129:5071;transport=UDP SIP/2.0 |
| 00:00:10.251647 | | <------- | SIP/2.0 200 OK |
| 00:00:10.251794 | SIP/2.0 200 OK | <------- | |
| 10:07:34.676686 | | Finished | |
| RTP(Hide) | | | |
| Ports | Port 29754 'active'<br>RX 235 lost 0<br>TX 235 dropped 0<br>SSRC 0xDEE0EE8F<br>PT 8 | | Port 29752 'active'<br>RX 235 lost 0<br>TX 235 dropped 0<br>SSRC 0xDEE0EE8F<br>PT 8 |
| | Port 29755 'active'<br>RX 0 lost 0<br>TX 2 dropped 0<br>SSRC 0xDEE0EE8F<br>LSR 0xDD40 | | Port 29753 'active'<br>RX 0 lost 0<br>TX 2 dropped 0<br>SSRC 0xDEE0EE8F<br>LSR 0xDD40 |
| SDP(Hide) | | | |
| SDP local | v=0<br>o=user1 77755765 3478720341 IN IP4 192.168.114.134<br>s=-<br>c=IN IP4 192.168.114.134<br>t=0 0<br>m=audio 29754 RTP/AVP 8<br>a=rtpmap:8 PCMA/8000 | | v=0<br>o=user1 77755765 3478720341 IN IP4 192.168.114.134<br>s=-<br>c=IN IP4 192.168.114.134<br>t=0 0<br>m=audio 29752 RTP/AVP 8<br>a=rtpmap:8 PCMA/8000 |
| SDP remote | v=0<br>o=user1 77755765 3478720341 IN IP4 192.168.114.129<br>s=-<br>c=IN IP4 192.168.114.129<br>t=0 0<br>m=audio 6001 RTP/AVP 8<br>a=rtpmap:8 PCMA/8000 | | v=0<br>o=user1 77755765 3478720341 IN IP4 192.168.114.129<br>s=-<br>c=IN IP4 192.168.114.129<br>t=0 0<br>m=audio 6124 RTP/AVP 8<br>a=rtpmap:8 PCMA/8000 |

- *Monitoring is enabled/disabled* — monitoring current status. The *Enable/Disable* button can be used to control the monitor's status.

✓ **When monitoring is enabled, calls already established will not be displayed, only new calls will be displayed.**

There are two monitoring tables in the menu. The left table contains general information on all active sessions.

In the field *"Rows in the table to show",* the number of entries to be displayed on the page is specified. The table on the right contains the current page number and the total number of pages. To navigate between pages, the arrows under the table are used. A single arrow is for moving to the next/previous page, a double one is to display the first/the last page.

**Information on active sessions (table on the left)**

- *Reload every 5 sec* — when checked, the call list in the monitor window is automatically updated;
- *Update* — the button to manually update the call list in the monitor window when the button is clicked;
- *Field* — the headers of the main fields (e.g. From and To), which are transmitted during the call;
- *User A* — field values for subscriber A;
- *State* — the current status of the session:
  - *RUNNING* — the session is active and is currently being processed;
  - *FINISHED* — session processing is complete (such sessions are deleted from monitoring after a while);
- *User B* — field values for subscriber B;

The right table contains details of the call. To display it, left-click on the corresponding entry in the left table.

**Information on active sessions (table on the right)**

- *Reload extended session info* — clicking the *"Update"* button updates the current status of the session in the monitor;
- *Field* — the headers of the main fields (e.g. From and To), which are transmitted during the call;
- *User A* — field values for subscriber A;
- *State* — the current status of the session:
  - *RUNNING* — the session is active and is currently being processed;
  - *FINISHED* — session processing is complete (such sessions are deleted from monitoring after a while);
- *User B* — field values for subscriber B;

List of fields:

- *IP remote* — the IP address of the subscriber from or to which the call was routed;
- *IP local* — the local IP address where the call came from or was sent to (IP local);
- *Contact* — Contact fields values;
- *CallID* — the dialogue identifier from the Call-ID field;
- *Agent* — the name of the subscriber's SIP client from the User-Agent field;
- *Transport* — the transport protocol used for transmission.

The **Call Flow** block in the table displays the call signalling to both legs, indicating the total start time of the call and the time each message was sent relative to the start time.

The **RTP** block in the table displays information about media streams between subscribers.

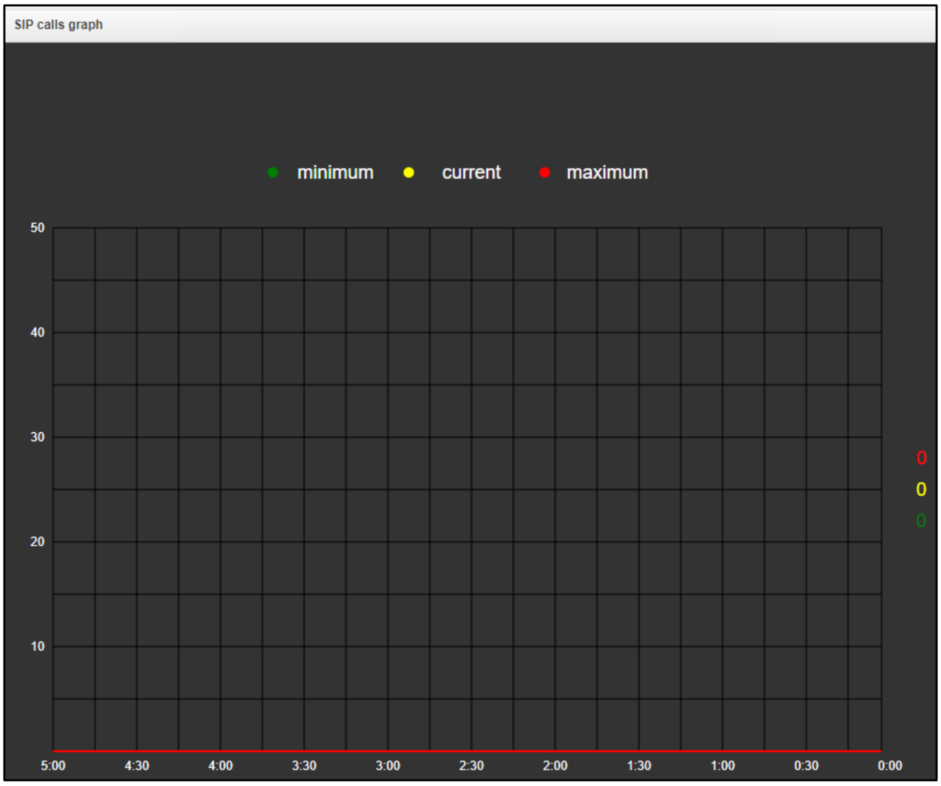
The **SDP** block in the table shows which SDP messages have been exchanged between the calling parties. SDP local — SDP sent from SBC to the subscriber; SDP remote — SDP received from the subscriber.

**The information in the blocks can be hidden/expanded by left-clicking on the relevant subtitle.**

### *4.1.2.9 SIP calls graph*

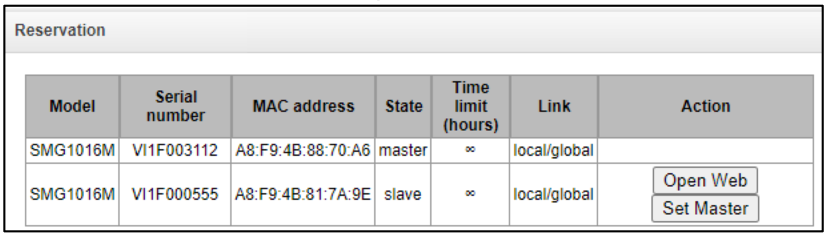
This submenu displays the maximum, current and minimum number of calls made in the last five minutes on the graph. The graph is updated every three seconds.

***Monitoring –> Reservation***



### *4.1.2.10 Reservation*

***Monitoring –> Reservation***



Reservation

| Model | Serial number | MAC address | State | Time limit (hours) | Link | Action |
|---|---|---|---|---|---|---|
| SMG1016M | VI1F003112 | A8:F9:4B:88:70:A6 | master | ∞ | local/global | |
| SMG1016M | VI1F000555 | A8:F9:4B:81:7A:9E | slave | ∞ | local/global | Open Web<br>Set Master |

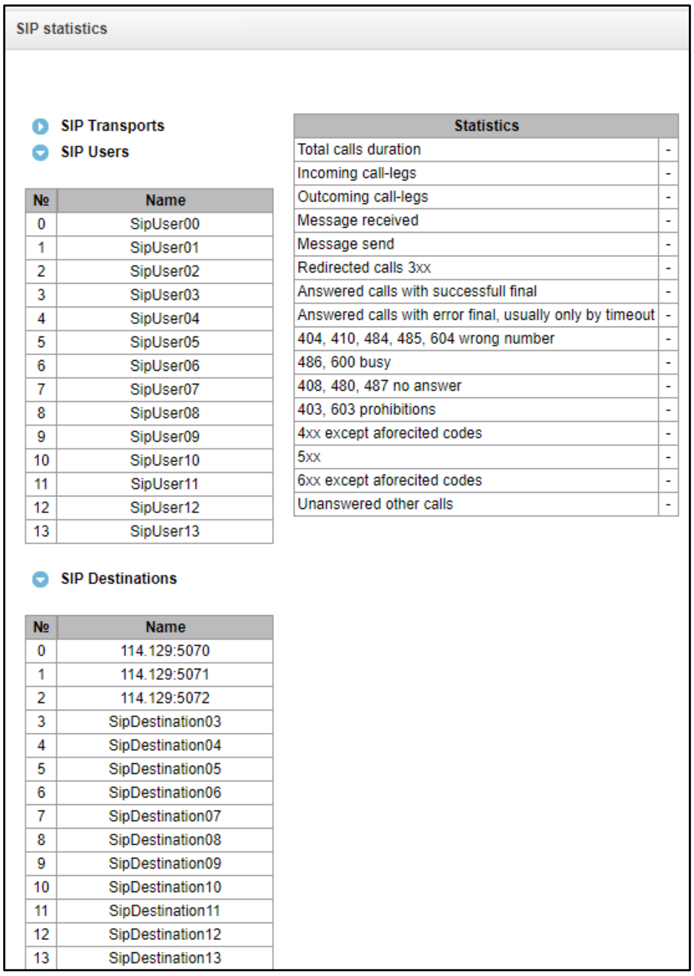
- *Model* — device model*;*
- *Serial number* — device serial number;
- *MAC address* — device MAC address;
- *State*:
  - master — the device is a master;
  - slave — the device is a slave.
- *Link*:
  - local — the device is available via a local link;
  - global — the device is available via a global link.
- *Open Web* — open the web interface of the slave device.

More about reservation in the APPENDIX C. SBC RESERVATION FUNCTION PROVISION.

#### 4.1.2.11 *SIP statistics*

The section contains the call statistics accumulated by SBC. If statistics are disabled, they can be switched on in the section 4.1.1 System settings. On the left is a list of all SIP Transports, SIP Destinations and SIP Users configured on SBC. On the right is a table showing the statistics counters. To view the statistics, select an entry on the left and then the table on the right will display the statistics for the entry selected. The total statistics for the entire SBC can be viewed by selecting the entry "The sum of all transports" in the list of transports. Any list of elements can be collapsed or expanded by clicking on the arrow next to its name.

***Monitoring –> SIP statistics***



SIP statistics

SIP Transports

SIP Users

| № | Name |
|---|---|
| 0 | SipUser00 |
| 1 | SipUser01 |
| 2 | SipUser02 |
| 3 | SipUser03 |
| 4 | SipUser04 |
| 5 | SipUser05 |
| 6 | SipUser06 |
| 7 | SipUser07 |
| 8 | SipUser08 |
| 9 | SipUser09 |
| 10 | SipUser10 |
| 11 | SipUser11 |
| 12 | SipUser12 |
| 13 | SipUser13 |

SIP Destinations

| № | Name |
|---|---|
| 0 | 114.129:5070 |
| 1 | 114.129:5071 |
| 2 | 114.129:5072 |
| 3 | SipDestination03 |
| 4 | SipDestination04 |
| 5 | SipDestination05 |
| 6 | SipDestination06 |
| 7 | SipDestination07 |
| 8 | SipDestination08 |
| 9 | SipDestination09 |
| 10 | SipDestination10 |
| 11 | SipDestination11 |
| 12 | SipDestination12 |
| 13 | SipDestination13 |

| Statistics | |
|---|---|
| Total calls duration | - |
| Incoming call-legs | - |
| Outcoming call-legs | - |
| Message received | - |
| Message send | - |
| Redirected calls 3xx | - |
| Answered calls with successfull final | - |
| Answered calls with error final, usually only by timeout | - |
| 404, 410, 484, 485, 604 wrong number | - |
| 486, 600 busy | - |
| 408, 480, 487 no answer | - |
| 403, 603 prohibitions | - |
| 4xx except aforecited codes | - |
| 5xx | - |
| 6xx except aforecited codes | - |
| Unanswered other calls | - |

**The table on the right shows the following information:**

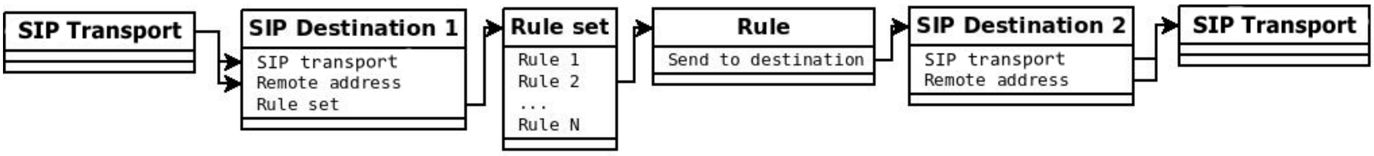
- *Total calls duration* — the total time of all calls that have passed through the selected item;
- *Incoming call-legs* — the total and current number of incoming calls;
- *Outcoming call-legs* — — the total and current number of outcoming calls;
- *Message received* — how many SIP messages were received by the item (all dialogue messages, both requests and replies, are counted);
- *Message send* — how many SIP messages have been sent (all dialogue messages, both requests and replies, are counted);
- *Answered calls with successful final* — calls that were ended in a proper way after the call;
- *Answered calls with error final, usually only by timeout* — calls that ended prematurely with an error during the call;
- *404,410,484,485,604 wrong number* — calls that have been answered with information about a wrong or non-existent number;
- *486,600 busy* — calls that are answered "busy";
- *408, 480, 487 no answer* — calls that have not been answered and have been ended by the initiator of the call or by timeout;

- *403, 603 prohibitions* — the call was rejected with the reason "call prohibition";
- *4xx except aforecited codes* — other calls with SIP responses 400-499 received on them that do not fall into the categories above;
- *5xx system failure* — calls with SIP responses 500-599 received on them;
- *6xx except aforecited codes* — calls with SIP responses 600-699 received on them

### 4.1.3 *SBC Configuration*

Functionally, SBC can be described as a set of tunnels between different (or within the same) subnets that allow both signalling and speech (or other) information to be transmitted between users. The tunnel is terminated on each side by an SBC SIP server, the exit point for which is a SIP transport. SBC switches messages between SBC SIP servers in accordance with the specified rules. In general, several SBC SIP servers can be created in the same subnet (e.g. tunnels from the same subnet to different subnets). The speech information can either be transmitted in the same subnet as the signalling one (where SBC SIP server is located) or in a separate subnet. To transmit speech information, a range of ports is allocated.

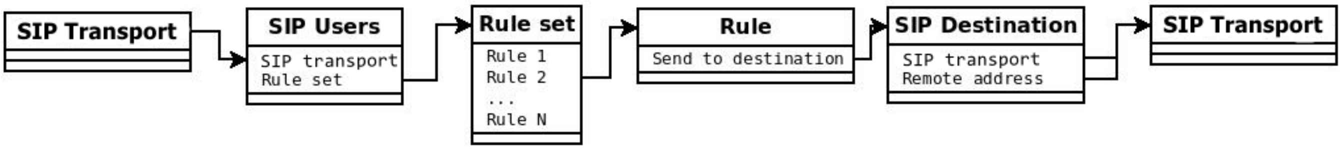
**General algorithm for signalling passing through SBC**



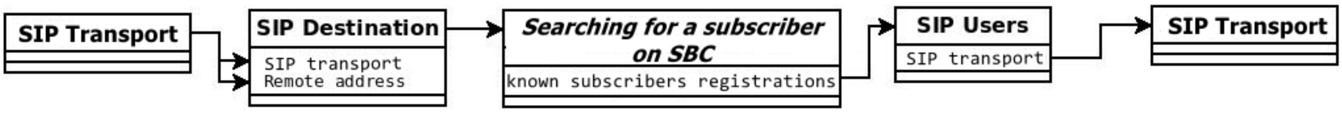
Consider the call passing through SBC for two terminal nodes. Incoming signalling is received on one of the SBC interfaces. An available incoming destination is searched by transport, which is linked to the interface and IP address of the call source. Then a corresponding set of rules is checked according to the destination setting. If the signalling matches any of the rules in the set where the action *"send to destination"* or *"send to trunk"* is specified, the call is passed to the destination specified in the rule. The destination selected as outgoing indicates the transport through which the signalling is to be sent next and the remote address of the node to which the signalling is to be sent.

The one-way call has been considered above. In order to ensure that calls go both ways, the destinations used together should be set symmetrically. Two sets of rules to be used for call direction should be created and appropriate sets of rules should be specified in each destination.

**Signalling passing for subscribers registered via SBC**



When subscribers are registered via SBC, signalling is carried out in the same way as described above, except that calls must go through the destinations configured under *"SIP Users".* In this case, the incoming destination is only searched by the SIP transport that is bound to it. The outgoing direction in this case will be that behind which the register-sender is located.



Note that when calling towards a registered subscriber it is not necessary to link rule sets to the destination where the register-sender's address is specified. SBC will remember the directions used for registrations that have passed through it and will use this as a basis for sending a signalling to the subscriber coming from the register-sender.

### General SBC configuration algorithm

1. Create a SIP transport in those subnets between which the switching will take place.

2. Create SIP destinations and users, link transports to them. For destinations, specify addresses of terminal nodes.

3. Create rule sets according to the desired call-switching scheme between the terminal nodes.

4. Bind rule sets to incoming destinations.

For more information, see APPENDIX B. SBC CONFIGURATION EXAMPLES.

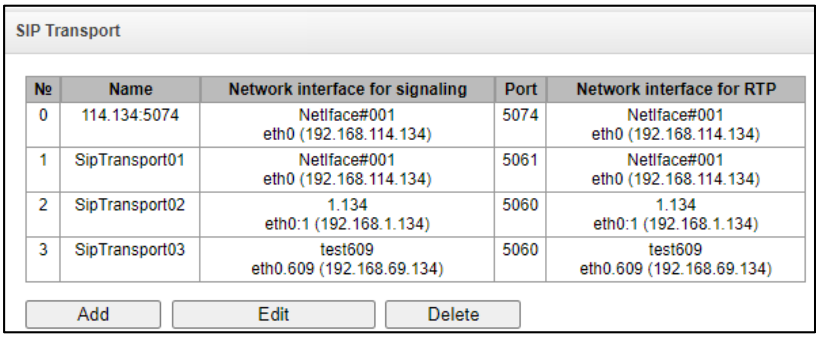
### *4.1.3.1 SIP Transport*

This submenu allows editing the list of transport that will serve as entry points into the tunnels. Up to 256 transports can be created.

To create, edit or remove interfaces, use *'Objects'* — *'Add an object'*, *'Objects'* — *'Edit an object'* and *'Objects'* — *'Remove an object'* and the following buttons:

- *«Add»;*
- *«Edit»;*
- *«Delete»*.

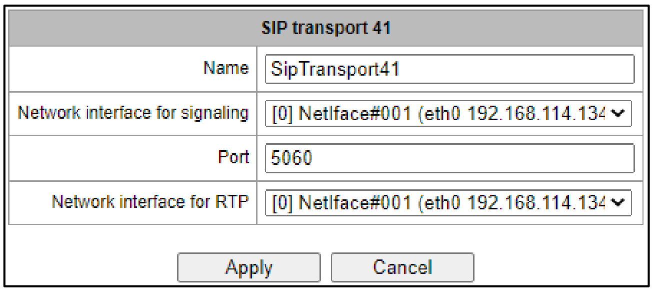
***SBC Configuration –> SIP Transport***



SIP Transport

| № | Name | Network interface for signaling | Port | Network interface for RTP |
|---|---|---|---|---|
| 0 | 114.134:5074 | NetIface#001<br>eth0 (192.168.114.134) | 5074 | NetIface#001<br>eth0 (192.168.114.134) |
| 1 | SipTransport01 | NetIface#001<br>eth0 (192.168.114.134) | 5061 | NetIface#001<br>eth0 (192.168.114.134) |
| 2 | SipTransport02 | 1.134<br>eth0:1 (192.168.1.134) | 5060 | 1.134<br>eth0:1 (192.168.1.134) |
| 3 | SipTransport03 | test609<br>eth0.609 (192.168.69.134) | 5060 | test609<br>eth0.609 (192.168.69.134) |

***SBC Configuration –> SIP Destination –> "Add" or "Edit"***



SIP transport 41

| | |
|---|---|
| Name | SipTransport41 |
| Network interface for signaling | [0] NetIface#001 (eth0 192.168.114.134 |
| Port | 5060 |
| Network interface for RTP | [0] NetIface#001 (eth0 192.168.114.134 |

**Transport parameters**

- *Name* — an arbitrary name for identification, convenient for the operator;
- *Network interface for signalling* — network interface for receiving signalling;
- *Port* — port for receiving signalling;
- *Network interface for RTP* — the network interface on which media streams will be transmitted.

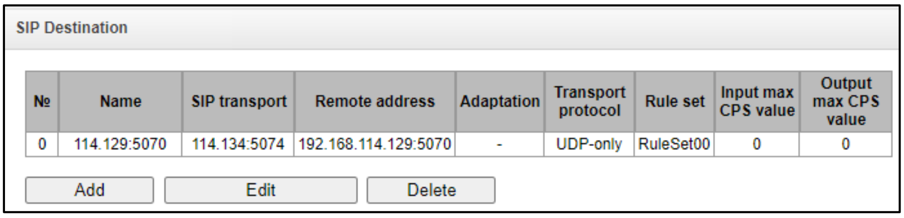
### 4.1.3.2 SIP Destination

This submenu allows editing the list of destinations for receiving and sending calls to end nodes. Up to 256 destinations can be created.

To create, edit or remove interfaces, use *'Objects' — 'Add an object', 'Objects' — 'Edit an object'* and *'Objects' — 'Remove an object'* and the following buttons:

- *"Add";*
- *«Edit»;*
- *«Delete».*

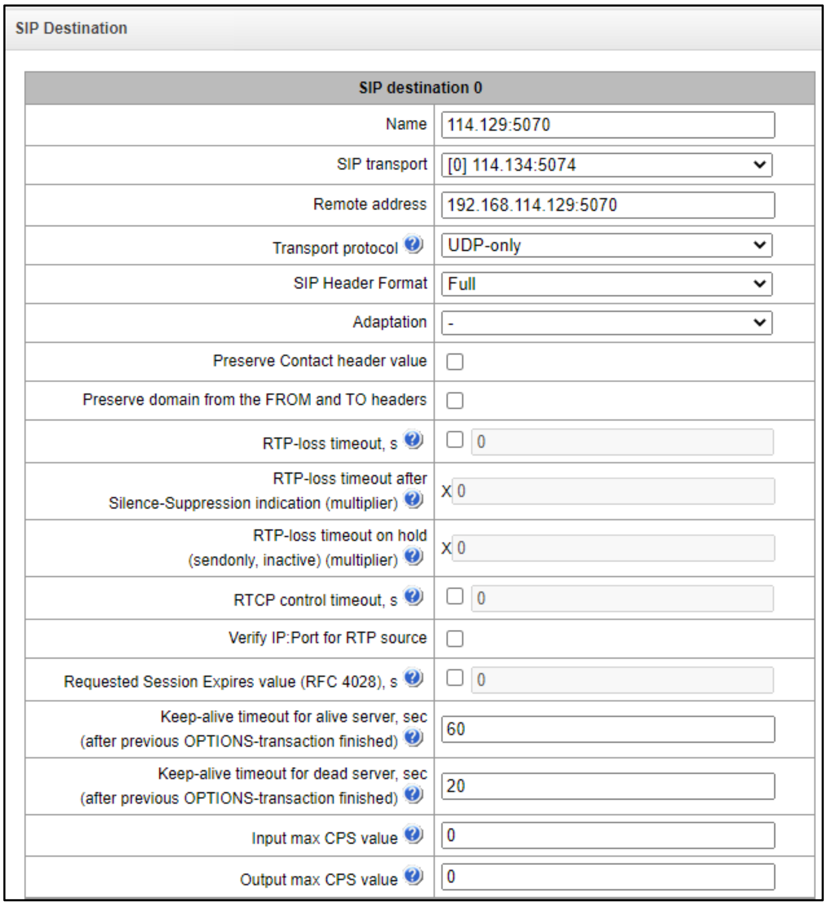
***SBC Configuration –> SIP Destination***



SIP Destination

| № | Name | SIP transport | Remote address | Adaptation | Transport protocol | Rule set | Input max CPS value | Output max CPS value |
|---|---|---|---|---|---|---|---|---|
| 0 | 114.129:5070 | 114.134:5074 | 192.168.114.129:5070 | - | UDP-only | RuleSet00 | 0 | 0 |

***SBC Configuration –> SIP Destination –> "Add" or "Delete"***



SIP Destination

| SIP destination 0 | |
|---|---|
| Name | 114.129:5070 |
| SIP transport | [0] 114.134:5074 |
| Remote address | 192.168.114.129:5070 |
| Transport protocol | UDP-only |
| SIP Header Format | Full |
| Adaptation | - |
| Preserve Contact header value | □ |
| Preserve domain from the FROM and TO headers | □ |
| RTP-loss timeout, s | □ 0 |
| RTP-loss timeout after Silence-Suppression indication (multiplier) | x 0 |
| RTP-loss timeout on hold (sendonly, inactive) (multiplier) | x 0 |
| RTCP control timeout, s | □ 0 |
| Verify IP:Port for RTP source | □ |
| Requested Session Expires value (RFC 4028), s | □ 0 |
| Keep-alive timeout for alive server, sec (after previous OPTIONS-transaction finished) | 60 |
| Keep-alive timeout for dead server, sec (after previous OPTIONS-transaction finished) | 20 |
| Input max CPS value | 0 |
| Output max CPS value | 0 |

**Destination parameters**

- *Name* — an arbitrary name for identification, convenient for the operator;
- *SIP transport* — transport to be used to receive calls to and from the destination.
- *Remote Address* — the address of the remote node which is associated with this destination. Calls to the destination from an IP address other than the one specified in this field will be rejected. Calls from the destination will be sent to the address specified in this field.

- *Transport protocol* — selection of the transport layer protocol used to receive and transmit SIP messages:
    - *TCP-prefer* — reception via UDP and TCP. Transmission via TCP. If connection is not established via TCP, the transmission will be performed via UDP;
    - *UDP-prefer* — reception via UDP and TCP. Sending packets over 1300 bytes via TCP, under 1300 bytes via UDP;
    - *UDP-only* — use only UDP protocol;
    - *TCP-only* — use only TCP protocol;

- *SIP header format* — defines the format for SIP headers transmission:
    - *full* — use a normal (long) header format;
    - *compact* — use a short header format;

- *Adaptation* — the setting is intended to adapt the interaction of gateways from different manufacturers with the ESCC-10 softswitch via SBC.
    - *HUAWEI-EchoLife* — this adaptation allows receiving a Flash signal from a gateway using the re-INVITE method and transmitting it towards a softswitch using the SIP INFO method;
    - *Iskratel SI3000* — when using this adaptation, SBC does not substitute the contact field in requests sent towards a softswitch. When calling a subscriber in Request-URI the URI-parameters are not analysed. Only a subscriber's number and address are analysed;
    - *HUAWEI-SoftX3000* — when using this adaptation, SBC does not substitute the contact field in requests sent towards a softswitch. In the 200OK response to the REGISTER request, the URI containing the default port 5060 is assumed to be equal to the URI not containing it;
    - *ZTE Softswitch* — when using this adaptation, SBC does not substitute the *"contact"* field in requests sent towards a softswitch. When calling a subscriber in Request-URI, URI-parameters are not analysed. Only a subscriber's number and address are analysed; Origin version sequence violations in the SDP are also ignored;
    - *Nortel* — when using this adaptation, SBC ignores the origin sequence inconsistencies in SDP.
    - *MTA M-200* — when using this adaptation, SBC does not check the port specified in the Request URI when incoming calls are received.

- *Preserve Contact header value* — when using this option, SBC does not substitute the 'contact' field in requests sent to the second leg;

- *Preserve domain from the FROM and TO headers* — When using this option, SBC will drop the domain that came in the FROM, TO fields into the outgoing leg. If an IP address is received, SBC will replace it with its own IP address;

- *RTP-loss timeout* — voice frequency path status control function that monitors the presence of RTP traffic from the communicating device. The range of available values is from 10 to 300 seconds. When flag is unchecked, RTP control is disabled, otherwise enabled. If there are no RTP packets coming from the opposite device for the duration of the timeout and the last packet was not a silence suppression packet, the call will be rejected;

- *RTP-loss timeout after Silence-Suppression indication (multiplier)* — RTP packet timeout for the silence suppression option utilization. Permitted value range is from 1 to 30. Coefficient is a multiplier and determines how many times the value of this timeout is greater than the "*RTP-loss timeout*". If there are no RTP packets coming from the opposite device for the duration of the timeout and the last packet was a silence suppression packet, the call will be rejected;

- *RTP-loss timeout on hold (sendonly, inactive) (multiplier)* — RTP packets timeout for SBC communicating with the SIP server in modes where the voice frequency path is transmitting only or is inactive. Permitted value range is from 1 to 30. Coefficient is a multiplier and determines how many times the value of this timeout is greater than the "*RTP-loss timeout*". If there are no RTP packets coming from the opposite device for the duration of the timeout and the voice frequency path is transmitting only or inactive, the call will be rejected;

– *RTCP control timeout, s* — the voice frequency path monitor function, takes on values from 10-300 c. Defines the period of time, during which the opposite side will wait for RTCP protocol packets. If no packets are received within a given time period, if at least one RTCP packet has previously been sent by the opposite party, the established connection is terminated;

– *Verify IP:Port for RTP source* — when enabled, SBC ensures that the media stream from the opposite side is routed exactly from the IP and the port specified in the SDP. Otherwise the media stream will be rejected;

– *Requested Session Expires value (RFC 4028), s* — when checked, SIP session timers are supported (RFC 4028). Session update is supported by transmitting re-INVITE requests during the session. This parameter defines the time period, in seconds, after which a session will be forcibly terminated if the session is not updated in time (from 90 to 64800 s, the recommended value is 1800 s);

**The RTP, RTCP packet waiting control and the use of RFC 4028 are designed to ensure that conversational sessions established via an SBC do not hang up if there are problems with packet transmission on the operator's network. All inactive sessions will be closed after appropriate timeouts.**

– *Keep-alive timeout for alive server, sec (after previous OPTIONS-transaction finished)* — the time interval after which an OPTIONS control request will be sent to the SIP server if the previous OPTIONS request was confirmed;

– *Keep-alive timeout for dead server, sec (after previous OPTIONS-transaction finished)* — the time interval after which an OPTIONS control request will be sent to the SIP server if the previous OPTIONS request was not confirmed;

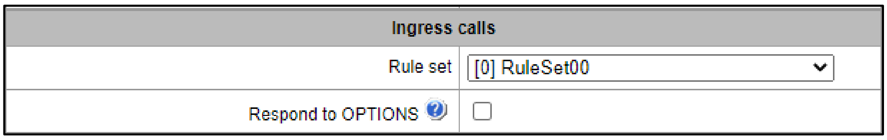
– *Input max CPS value* — the number of calls per second that can be received by SIP Destination. The permissible value range is from 0 to 100, 0 — option deactivation;

– *Output max CPS value* — the number of calls per second that can be sent by SIP Destination. The permissible value range is from 0 to 100, 0 — option deactivation.

**Ingress calls**

– *Rule set*— apply the rule set created in the "Rule set" menu to the incoming signalling (more information in section  4.1.3.5 Rule set);

– *Respond to OPTIONS* — when enabled, SBC will respond to OPTIONS on its own if the Rule in not present in the Rule set responsible for sending OPTIONS.



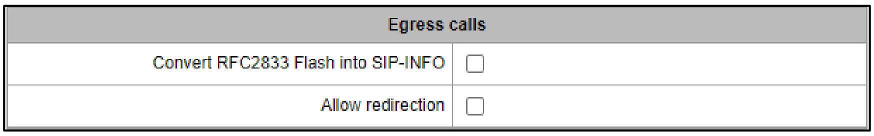
| Ingress calls | |
|---|---|
| Rule set | [0] RuleSet00 |
| Respond to OPTIONS | □ |

**Egress calls**

– *Convert RFC2833 Flash into SIP INFO* — converts the Flash signal received using RFC 2833 method to a SIP INFO application/hook-flash request and transmits it to the communicating channel;

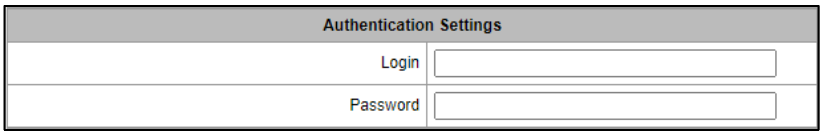
– *Allow redirection* — allows 302 responses processing. When disabled, SBC will end the call when 302 response is received from B. When enabled, SBC will process 302 responses as follows: after receiving a subscriber C contact, SBC will try to send the call to him, notifying side A that the call has been redirected by 181 response. If the contact contains the address of SBC itself, it will transparently route the 302 message to side A by specifying the address of side A in the Contact field;

**When enabled, the setting will disable built-in firewall rules for the SIP transport bound to the SIP destination on which the option is enabled to ensure that redirects work correctly! If the transport is used on other SIP destinations, built-in Firewall rules will also be disabled for them. It is recommended to allocate a separate SIP transport for those SIP destinations from which redirects are allowed to be processed, or restrict access manually if necessary (more details in section 4.1.8.5).**



| Egress calls | |
|---|---|
| Convert RFC2833 Flash into SIP-INFO | ☐ |
| Allow redirection | ☐ |

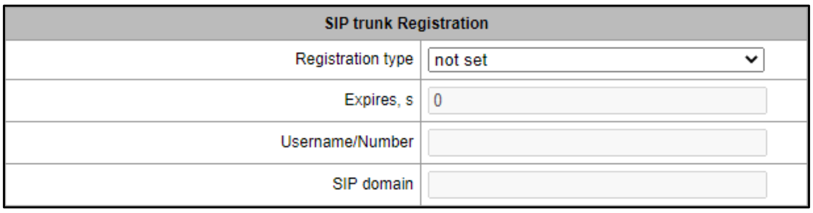
*Authentication settings*



| Authentication Settings | |
|---|---|
| Login | |
| Password | |

- *Login* — login to authenticate to the upstream SIP server;
- *Password* — password to authenticate to the upstream SIP server. Authentication data is only used to authorise requests generated by SBC itself, e.g. re-INVITE requests generated by SBC when using RFC 4028 timer function, authentication on the interacting server, registration on the interacting server (with UAC registration type), authentication of requests from the interacting server (with UAS registration type).

*SIP trunk Registration*



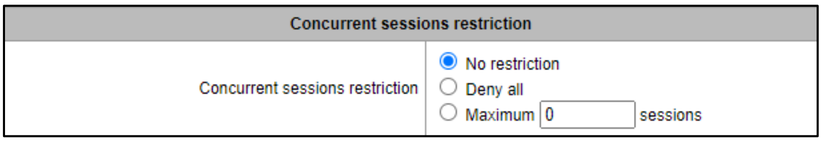
| SIP trunk Registration | |
|---|---|
| Registration type | not set |
| Expires, s | 0 |
| Username/Number | |
| SIP domain | |

- *Registration type* — this setting specifies the direction of registration:
  - *UAC* — in this case, SBC will register on the cooperating registration server via a trunk. If there is no registration, the destination will be considered unavailable and no calls will be sent to it (but they will always be received);
  - *UAS* — in this case, the device interacting over the trunk will register on SBC, provided that the registration confirmation is received from the selected by *Rule set* server. SBC will also authenticate all requests from the interacting server. The setting in the *Remote Address* field does not apply, the address obtained in the contact during registration is used.

**If there is no registration, the destination will be considered unavailable and no calls will be sent from it (but they will always be received);**

- *Expires, s* — update period for registration on the server (used for UAC registration type);
- *Username/Number* — name/number with which SBC trunk registers on the registration server (for UAC registration type);
- *SIP domain* — the domain name with which the SBC trunk is registered to the registration server (for UAC registration type), or the domain name with which the opposite device is authenticated to the SBC via the trunk (for UAS registration type);

### *Concurrent sessions restriction*

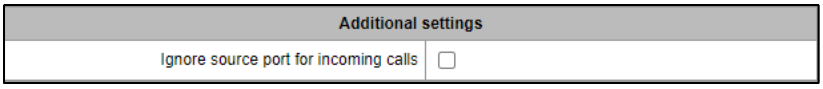


Concurrent sessions restriction

| | |
|---|---|
| Concurrent sessions restriction | ● No restriction<br>○ Deny all<br>○ Maximum 0 sessions |

- *No restriction* — the number of sessions is not limited;
- *Deny all* — total prohibition of sessions;
- *Maximum N sessions,* where N is the number of simultaneous sessions.

### *Additional settings*



Additional settings

| | |
|---|---|
| Ignore source port for incoming calls | □ |

- *Ignore source port for incoming calls* — do not check the address of the port from which the request came for incoming calls. When disabled, for incoming calls it is strictly checked that the call came from the address and the port specified in the 'Remote address' field. If the option is enabled, SIP Destination is first searched and selected from those destinations where the option is not present. Then one of those destinations where the option is enabled and which suit the IP/hostname parameter in the 'Remote address' field is selected.

**Example:**

Four SIP Destinations are configured on the SBC with these remote address parameters:

| Name | remote address | Option state |
|---|---|---|
| Dest1 | 192.0.2.1:5060 | disabled |
| Dest2 | 192.0.2.1:5061 | disabled |
| Dest3 | 192.0.2.1:5062 | enabled |

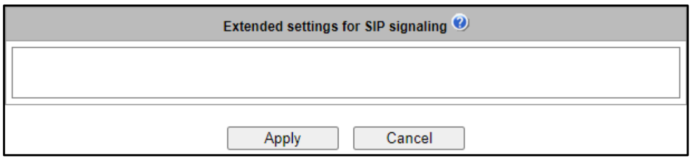
Requests from 192.0.2.1:5060...192.0.2.1:5062 will be handled by destination Dest1...Dest3 according to their addresses, since they match exactly what is configured in the remote address.

*The request from 192.0.2.1:5090 will get to Dest3 because the request does not fit any remote address setting, but Dest3 ignores the port. Similarly, all requests from ports other than 5060...5062 will also go to Dest3.*

**It is not recommended to create several SIP Destinations with the same IP addresses and activated ignore port settings, as it is impossible to predict which one of them will eventually process the request.**

### *Extended settings for SIP signaling*

This field contains advanced SIP settings. With these settings, you can adjust the fields of SIP messages according to the specified rules.



Extended settings for SIP signaling

### *Field filling format*

[sipheader:HEADER_NAME=operation],[sipheader:...],...

where:

- *Operations — disable, insert or modification rule;*
- *HEADER_name — non case-sensitive parameter, for example, Accept = accept = ACCEPT. In other parameters, the case does matter.*

***Modification rules***

Modification rules are described by symbols:

- *$ — leave the following text;*
- *! — remove the following text;*
- *+(ABC) — add the specified text;*
- *-(ABC) — remove the specified text.*

Examples of operation rules implementation are shown in the Table below.

Table 19 — Examples of operation rules implementation

| **Operation** | **Original header** | **Expressions** | **Result** |
|---|---|---|---|
| Do not send header | Accept: application/SDP | [sipheader:accept=disable] | |
| Pass the header from the first leg unchanged | Additional headers on the first leg:<br>P-Asserted-Identity: username@domain<br>Subject: Test call | [sipheader:[MESSAGE_LIST]:[HEADER_MASK]=transit]<br>[sipheader:[HEADER_MASK]=transit]<br>In INVITE and 200 messages: [sipheader:INVITE,200:Subject=transit]<br>In any messages: [sipheader:Subject=transit] | The specified header appears on the second leg:<br>Subject: Test call |
| Pass the header group from the first leg unchanged | Additional headers on the first leg:<br>P-Asserted-Identity: sip:username@domain<br>P-Called-Party-ID: sip:username@domain<br>Privacy: id<br>Subject: Test call | [sipheader:P-*=transit]<br>Note that the following rule: [sipheader:*=transit] will not work as the * character can only replace part of the name. | The specified headers appear on the second leg:<br>P-Asserted-Identity: sip:username@domain<br>P-Called-Party-ID: sip:username@domain |
| Insert header | | [sipheader:insert[HEADER_LIST]:RemoteIp=+(TEXT)]<br>In all requests: [sipheader:insert:RemoteIp=+(example.SBC)]<br>In INVITE request only: [sipheader:insert,INVITE:RemoteIp=+( example.SBC)]<br>Only in specified requests (e.g., INVITE and ACK): [sipheader:insert,INVITE,ACK:RemoteIp=+( example.SBC)] | RemoteIp:example.SBC |
| Add text at the beginning | Accept: application/SDP | [sipheader:accept=+(application/ISUP,)$] | Accept: application/ISUP,application/SDP |
| Add text in the end | Accept: application/SDP | [sipheader:accept=$+(,application/ISUP)] | Accept: application/SDP,application/ISUP |

| | | | |
|---|---|---|---|
| Remove text | Accept: application/SDP,application/ISUP | [sipheader:accept=-(application/SDP,)$] | Accept: application/ISUP |
| Remove, starting from the specified text | Accept: application/SDP,text/plain | [sipheader:accept=-(,text)!] | Accept: application/SDP |
| Replace the text completely | Accept: application/SDP | [sipheader:accept=+(application/ISUP)!] | Accept: application/ISUP |
| Replace the text | Accept: application/SDP,text/plain | [sipheader:accept=-(SDP)+(ISUP)$] | Accept: application/ISUP,text/plain |
| Replace the text by discarding the data at the end | Accept: application/SDP,text/plain | [sipheader:accept=-(SDP)+(ISUP)!] | Accept: application/ISUP |
| Complex modification example | From: <sip:who@host>;tag=aBc | [sipheader:from=+(DISPLAY )-(who)+(12345)-(>)+(;user=phone>)$+(;line=abc)] | From: DISPLAY <sip:12345@host;user=phone>;tag=aBc;line=abc |

**Example**

[sipheader:Accept=disable],[sipheader:user-agent=disable]

In this example all SIP messages sent via this SIP interface will not have the fields*Accept* and *user-agent.*

**List of mandatory SIP message fields that cannot be modified: via, from, to, call-id, cseq, contact, content-type, content-length.**

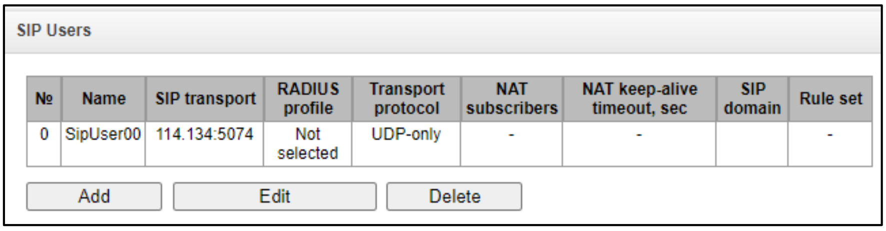
### *4.1.3.3 SIP Users*

This menu configures destinations for receiving and routing calls for SIP users who will send calls and registrations via SBC. Up to 256 users can be created.

To create, edit or remove interfaces, use *'Objects'* — *'Add an object', 'Objects'* — *'Edit an object'* and *'Objects'* — *'Remove an object'* and the following buttons:

– *«Add»;*
– *«Edit»;*
– *«Delete»*.

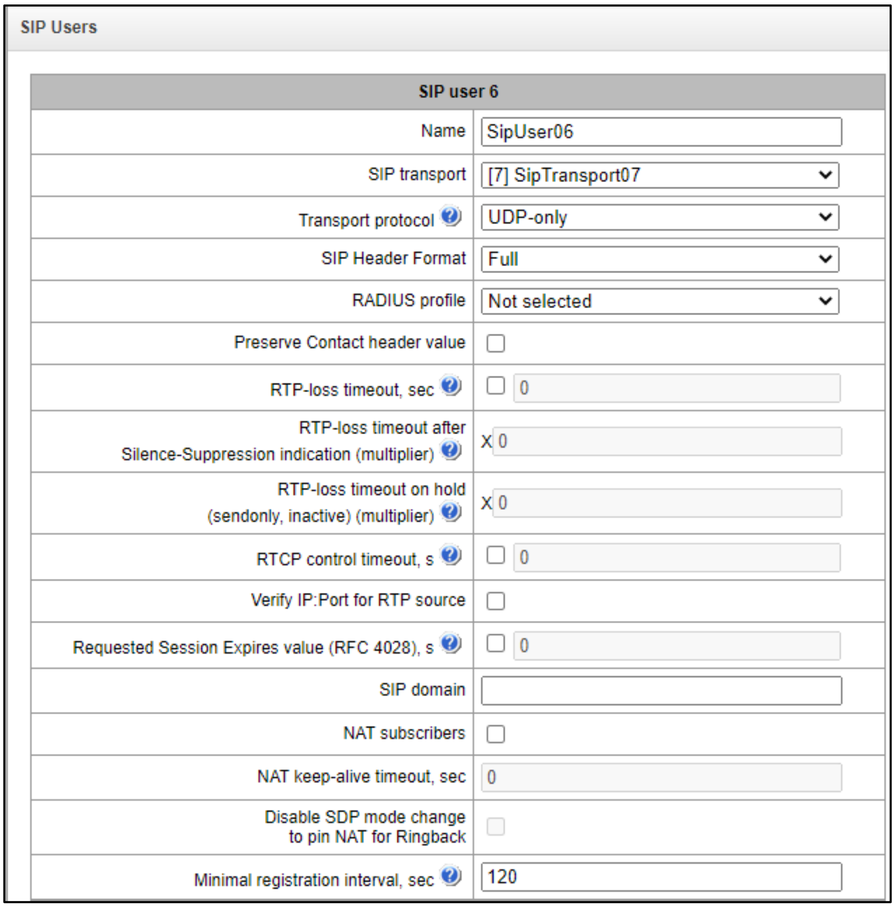
***SBC Configuration –> SIP Users***



SIP Users

| № | Name | SIP transport | RADIUS profile | Transport protocol | NAT subscribers | NAT keep-alive timeout, sec | SIP domain | Rule set |
|---|---|---|---|---|---|---|---|---|
| 0 | SipUser00 | 114.134:5074 | Not selected | UDP-only | - | - | | - |

***SBC Configuration –> SIP Users –> "Add" or "Edit"***



SIP Users

SIP user 6

| | |
|---|---|
| Name | SipUser06 |
| SIP transport | [7] SipTransport07 |
| Transport protocol | UDP-only |
| SIP Header Format | Full |
| RADIUS profile | Not selected |
| Preserve Contact header value | □ |
| RTP-loss timeout, sec | □ 0 |
| RTP-loss timeout after Silence-Suppression indication (multiplier) | X 0 |
| RTP-loss timeout on hold (sendonly, inactive) (multiplier) | X 0 |
| RTCP control timeout, s | □ 0 |
| Verify IP:Port for RTP source | □ |
| Requested Session Expires value (RFC 4028), s | □ 0 |
| SIP domain | |
| NAT subscribers | □ |
| NAT keep-alive timeout, sec | 0 |
| Disable SDP mode change to pin NAT for Ringback | □ |
| Minimal registration interval, sec | 120 |

***User direction parameters***

- *Name* — an arbitrary name for identification, convenient for the operator;

- *SIP transport* — transport to be used to receive calls to and from the destination;

- *Transport protocol* — selection of the transport layer protocol used to receive and transmit SIP messages:
  - *TCP-prefer* — reception via UDP and TCP. Transmission via TCP. If connection is not established via TCP, the transmission will be performed via UDP;
  - *UDP-prefer* — reception via UDP and TCP. Sending packets over 1300 bytes via TCP, under 1300 bytes via UDP;
  - *UDP-only* — use only UDP protocol;
  - *TCP-only* — use only TCP protocol;

- *SIP header format* — defines the format for SIP headers transmission:
  - *full* — use a normal (long) header format;
  - *compact* — use a short header format;

- *RADIUS profile* — RADIUS profile for incoming calls authentication and authorization (more information in section 4.1.9);

- *Preserve Contact header value* — when using this option, SBC does not substitute the 'contact' field in requests sent to the softswitch;

- *RTP packet timeout*— voice frequency path status control function that monitors the presence of RTP traffic from the communicating device. The range of available values is from 10 to 300 seconds. When flag is unchecked, RTP control is disabled, otherwise enabled. If there are no RTP packets coming from the opposite device for the duration of the timeout and the last packet was not a silence suppression packet, the call will be rejected;

- *RTP-loss timeout after Silence-Suppression indication (multiplier)* — RTP packet timeout for the silence suppression option utilization. Permitted value range is from 1 to 30. Coefficient is a multiplier and determines how many times the value of this timeout is greater than the "*RTP-loss timeout*". If there are no RTP packets coming from the opposite device for the duration of the timeout and the last packet was a silence suppression packet, the call will be rejected;

- *RTP-loss timeout on hold (sendonly, inactive) (multiplier)* — RTP packets timeout for SBC communicating with the SIP server in modes where the voice frequency path is transmitting only or is inactive. Permitted value range is from 1 to 30. Coefficient is a multiplier and determines how many times the value of this timeout is greater than the "*RTP-loss timeout*". If there are no RTP packets coming from the opposite device for the duration of the timeout and the voice frequency path is transmitting only or inactive, the call will be rejected;

- *RTCP control timeout, s* — the voice frequency path monitor function, takes on values from 10-300 c. Defines the period of time, during which the opposite side will wait for RTCP protocol packets. If no packets are received within a given time period, if at least one RTCP packet has previously been sent by the opposite party, the established connection is terminated;

- *Verify IP:Port for RTP source* — when enabled, SBC ensures that a media stream from the opposite side is routed exactly from the IP and port specified in SDP. Otherwise the media stream will be rejected;

- *Requested Session Expires value (RFC 4028), s* — when checked, SIP session timers are supported (RFC 4028). Session update is supported by transmitting re-INVITE requests during the session. This parameter defines the time period, in seconds, after which a session will be forcibly terminated if the session is not updated in time (from 90 to 64800 s, the recommended value is 1800 s);

**The RTP, RTCP packet waiting control and the use of RFC 4028 are designed to ensure that conversational sessions established via an SBC do not hang up if there are problems with packet transmission on the operator's network. All inactive sessions will be closed after appropriate timeouts.**

- *SIP domain* — the domain name with which the SBC trunk is registered to the registration server (for UAC registration type), or the domain name with which the opposite device is authenticated to SBC via the trunk (for UAS registration type);

- *NAT subscribers* — set a flag if it is necessary to connect subscribers who are in a private network (behind NAT). This setting also allows SIP messages to be sent symmetrically (to the port from which the request was received) if the client did not use the RPORT parameter in the initiating request;

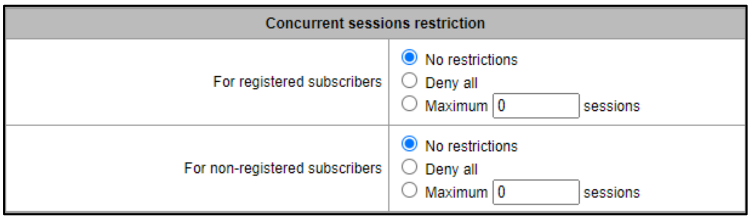
- *NAT keep-alive timeout, sec* — storage time of port matching for signalling traffic. Also limits the 'expires' parameter for SIP subscribers registration;

- *Disable SDP mode change to pin NAT for Ringback* — by default, starting from software version 1.9.2, SBC will declare sendrecv mode in SDP,  even if the opposite side has accepted sendonly or recvonly, to ensure correct preanswering media connection (PDA, voice messages) for clients behind NAT. The option allows disabling this behaviour and announce to the SDP what the opposite side has stated;

- *Minimal registration interval, sec* — the minimum registration time allowed for the subscriber. Can take values from 60 to 65535 seconds. Note that values less than 120s can affect performance.

***Concurrent sessions restriction***

- *For registered subscribers* — limit the number of simultaneous sessions for registered subscribers:
  - *No restriction* — the number of sessions is not limited;
  - *Deny all* — total prohibition of sessions;
  - *Maximum N sessions, where N is* the number of simultaneous sessions;



| Concurrent sessions restriction | |
|---|---|
| For registered subscribers | ● No restrictions<br>○ Deny all<br>○ Maximum 0 sessions |
| For non-registered subscribers | ● No restrictions<br>○ Deny all<br>○ Maximum 0 sessions |

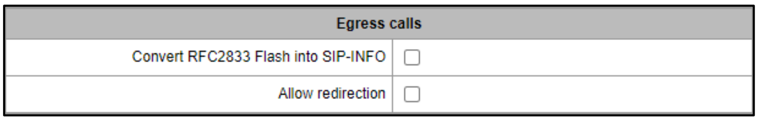
- *For non-registered subscribers* — limit the number of simultaneous sessions for non-registered subscribers:
  - *No restriction* — the number of sessions is not limited;
  - *Deny all* — total prohibition of sessions;
  - *Maximum N sessions, where N is* the number of simultaneous sessions.

**Ingress calls**

- Rule set — apply the rule set created in the *"Rule set"* menu to the incoming signalling (more information in section 4.1.3.5 Rule set);

**Egress calls**

- *Convert RFC2833 Flash into SIP INFO* — converts the Flash signal received using RFC 2833 method to a SIP INFO application/hook-flash request and transmits it to the communicating channel;



| Egress calls | |
|---|---|
| Convert RFC2833 Flash into SIP-INFO | ☐ |
| Allow redirection | ☐ |

- *Allow redirection* — allows 302 responses processing. When disabled, SBC will end the call when 302 response is received from B. When enabled, SBC will process 302 responses as follows: after receiving a subscriber C contact, SBC will try to send the call to him, notifying side A that the call has been redirected by 181 response. If the contact contains the address of SBC itself, it will transparently route the 302 message to side A by specifying the address of side A in the 'Contact' field.

***Extended settings for SIP signaling***

Operate similarly to SIP Destination settings; see SIP protocol settings in Section 4.1.3.2.

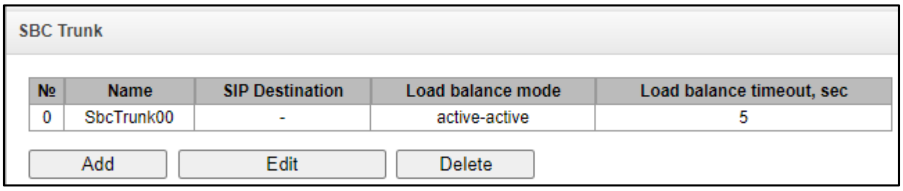
### *4.1.3.4 SBC Trunk*

This submenu is used to configure trunks for load balancing or link redundancy purposes. Up to 256 trunks can be created.

To create, edit or remove interfaces, use *'Objects'* — *'Add an object'*, *'Objects'* — *'Edit an object'* and *'Objects'* — *'Remove an object'* and the following buttons:

- *«Add»;*
- *«Edit»;*
- *"Delete"*.

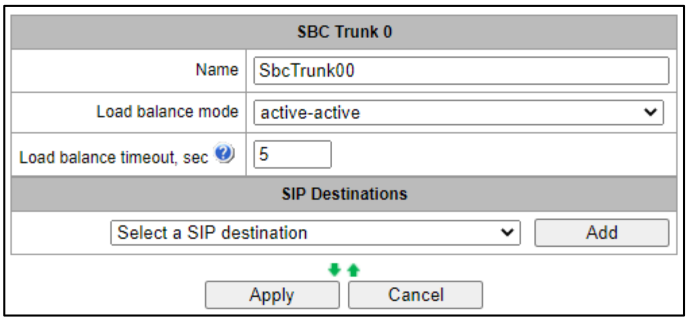
***SBC Configuration –> SBC Trunk***



SBC Trunk

| № | Name | SIP Destination | Load balance mode | Load balance timeout, sec |
|---|---|---|---|---|
| 0 | SbcTrunk00 | - | active-active | 5 |

***SBC Configuration –> SBC Trunk –> "Add" or "Delete"***



| SBC Trunk 0 | |
|---|---|
| Name | SbcTrunk00 |
| Load balance mode | active-active |
| Load balance timeout, sec | 5 |

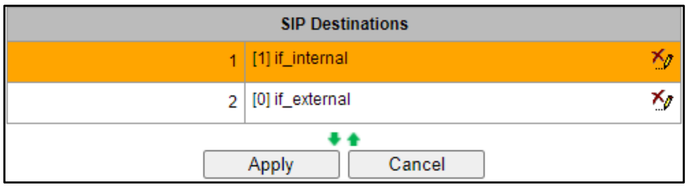
SIP Destinations

Select a SIP destination

***Trunk parameters***

- *Name* — an arbitrary name for identification, convenient for the operator;
- *Load balance mode* — type of load balancing between SIP servers:
  - *Active-active* — the load is balanced between SIP servers in a 50/50 ratio;
  - *Active-backup* — all load is transmitted via the first SIP server. If the first SIP server is unavailable, the load will be directed to the second SIP server;
- *Load balance timeout, sec* — the time after which the call will be routed to a backup SIP server if the server to which the call has already been routed is unavailable;

In the section ***SIP Destinations,*** destinations to be added to the trunk are selected. It is also possible to delete a destination from the trunk by clicking the icon ✗ *("Delete")* in the selected row. The green arrows below the list allow moving the highlighted entries in the table, adjusting the order (priority) of the destinations created.



| SIP Destinations | |
|---|---|
| 1 | [1] if_internal |
| 2 | [0] if_external |

### 4.1.3.5 Rule set

In this section, the rules for switching calls via SBC are configured. Up to 512 rule sets can be created in total, in which up to 1000 rules can be distributed. The limit on the number of rules is common to the whole SBC, one set of rules can contain up to 1000 rules. Thus, for example, one rule set with 1000 rules or 512 rule sets with two rules in each can be created on SBC.

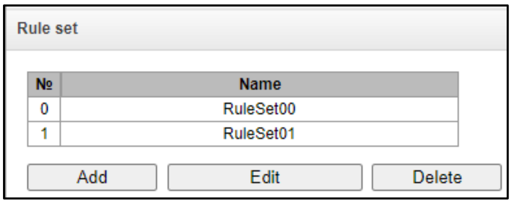
To create, edit or remove interfaces, use *'Objects'* — *'Add an object'*, *'Objects'* — *'Edit an object'* and *'Objects'* — *'Remove an object'* and the following buttons:

- *«Add»;*
- *«Edit»;*
- *"Delete"*.

***SBC Configuration –> Rule set***

***Rule sets configuration***

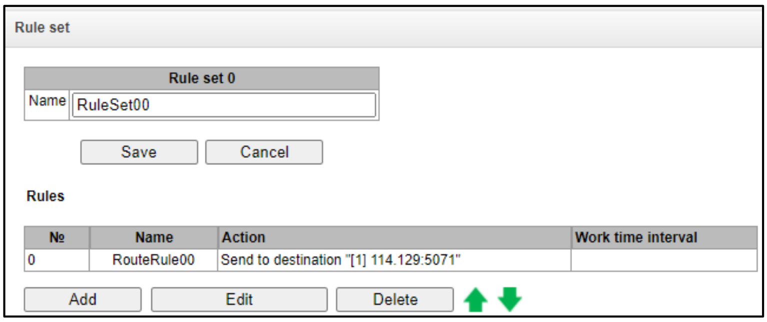
- *Name* — an arbitrary name for identification, convenient for the operator;



Rule set

| № | Name |
|---|---|
| 0 | RuleSet00 |
| 1 | RuleSet01 |

Each set of rules can contain several rules that define under which conditions and to which destination calls are to be sent.


Rule set

Rule set 0

| | |
|---|---|
| Name | RuleSet00 |

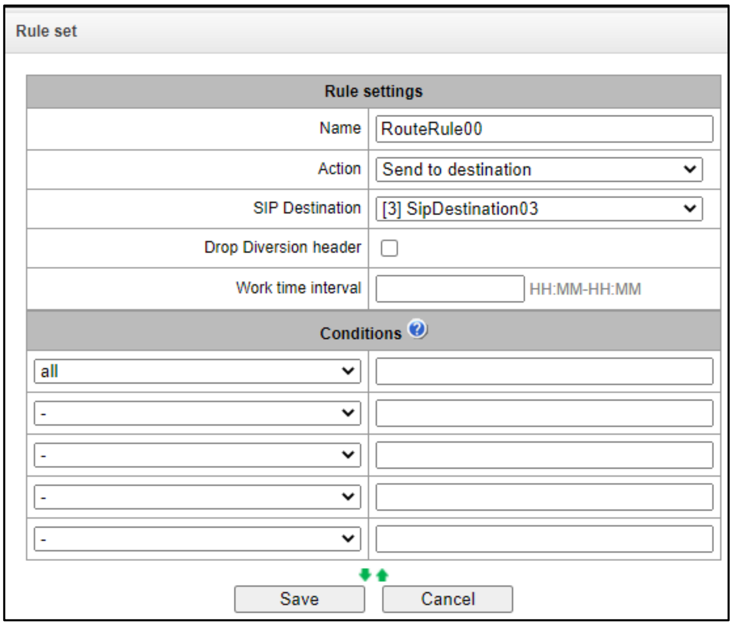
Rules

| № | Name | Action | Work time interval |
|---|---|---|---|
| 0 | RouteRule00 | Send to destination "[1] 114.129:5071" | |

***Rules configuration***

To create, edit and delete rules, the buttons *"Add", "Edit" and "Delete" are used.* The green arrows next to the edit buttons allow moving the highlighted entries in the table, adjusting the order of the rules created.

***SBC Configuration –> Rule set –> "Edit"***


Rule set

Rule settings

| | |
|---|---|
| Name | RouteRule00 |
| Action | Send to destination |
| SIP Destination | [3] SipDestination03 |
| Drop Diversion header | □ |
| Work time interval | HH:MM-HH:MM |

Conditions

| | |
|---|---|
| all | |
| - | |
| - | |
| - | |
| - | |

- *Name* — an arbitrary name for identification, convenient for the operator;
- *Action* — the action to be taken on messages that are subject to the conditions of the rule:
  - *Reject* — the message will be rejected;
  - *Send to destination* — the message will be sent to one of the destinations;
  - *Send to trunk* — the message will be sent to one of the trunks;
- *SIP Destination/SBC Trunk* — a field for selecting a destination or a trunk, appears when selecting an action other than Reject;
- *Drop Diversion header* — when enabled, the Diversion field will not be transmitted towards the selected SIP Destination/SBC Trunk;
- *Work time interval* — the time interval during which the rule will be enabled. Outside this interval, the rule will not work. The setting format is a time range written as "HH:MM-HH:MM".

***Conditions***

The *"Conditions"* section is used to set the conditions for determining whether a message falls under the rule or not. The left column contains a list of conditions and the right column contains their values. The rule must contain at least one condition and all conditions must be true for it to work.

Conditions:

- *All* — no further checks are made, the messages are processed according to the *"Action"* field;
- *From address User Part* — the name from the From header is checked, it is possible to check via a regular expression;
- *From address Host Part* — the domain from the From header is checked, it is possible to check via a regular expression;
- *From address URI* — the URI from the From header is checked, it is possible to check via a regular expression;
- *To address User Part* — the name from the To header is checked, it is possible to check via a regular expression;
- *To address Host Part* — the domain from the To header is checked, it is possible to check via a regular expression;

- *To address URI* — the URI from the To header is checked, it is possible to check via a regular expression;
- *Request-URI User Part* — the name from the Request-URI header is checked, it is possible to check via a regular expression;
- *Request-URI Host Part* — the domain from the Request-URI header is checked, it is possible to check via a regular expression;
- *Request-URI* — the Request-URI is checked, it is possible to check via a regular expression;
- *Source IP* — the source IP address is checked, either a single IP or a subnet in CIDR notation: 192.0.2.0/24 is allowed;
- *User-Agent* — the User-Agent is checked, it is possible to check via a regular expression.

It is possible to change the order of conditions by selecting a condition by clicking on a field and moving it up or down using the green arrows below the list of conditions.

***Syntax of regular expressions for making conditions***

1. A regular expression is described by a combination of Latin letters, numbers and special characters.

*Example:* **12345@my\.domain** — string containing "**12345@my.domain".** The symbol "." (dot) in this entry is special and has been escaped, see paragraph 11 for details.

2. Digit sequence enclosed in square brackets corresponds to any of the characters enclosed in brackets;

*Example:* **[01459]** corresponds to one of the digits 0, 1, 4, 5 or 9

3. A range of characters can be specified in square brackets, separated by a dash;

*Example:* **[4-9]** — corresponds to one of the numbers from 4 to 9;

*Example:* **[a-d4-97]** — a combination of the previous options. Corresponds to any letter from 'a' to 'd', one of the numbers from 4 to 9 or the number 7.

4. The symbol "^" marks the beginning of a line;

*Example:* **^7383** — a string that starts with 7383.

5. The "$" symbol marks the end of a line;

*Example:* **100$** — a string that ends with 100.

*Example:* **^40000$** — a string that corresponds exactly to «40000»

6. The symbol "." (dot) stands for any character;

*Example:* **^7383....... —** a string that starts with 7383 and then contains seven any characters. The string may be longer in this case. To definitely limit the string, add a "$" at the end: **^7383.......$**;

*Example:* **^…..$ —** a string that contains exactly five any characters;

*Example:* **…..** — a string that contains five any characters; Longer strings also fit this condition.

7. The symbol "*" represents the repetition of the previous character zero or more times

*Example:* **45*** — strings that contain the sequence: 4, 45, 455 etc.

8. The symbol "+" represents the repetition of the previous character one or more times

*Example:* **45+** — strings that contain the sequence: 45, 455 etc;

*Example:* **^2.+** — a string that begins with two and continues with one or more of any number of characters.

9. Curly braces may indicate the exact range of character repetitions:

- {k, m} — repetition of the previous character from k to m times;
- {k,} — repetition of a character k times or more;
- {,m} — repetition of a character no more than m times;
- {n} — repetition of a character exactly n times. It is similar to {n,n}.

*Example:* **^7{0,1}38329[0-5][0-9]{4}$** — any line that does or does not contain a seven at the beginning, then the sequence 38329, followed by one any digit from zero to five, followed by four any digits.

10. Expressions can be grouped together in parentheses. Usually used with the symbol "|" (vertical slash), which stands for logical OR;

*Example:* **(^9000$|^10000$)** — a string corresponds to 9000 or 10000;

*Example:* **^(7|8)[0-9]{10}$** — a string starts with a seven or eight and then contains 10 digits;

*Example:* **^(4[0-4]|5[3-4])** — a string that starts with 40, 41, 42, 43, 44, 53 or 54.

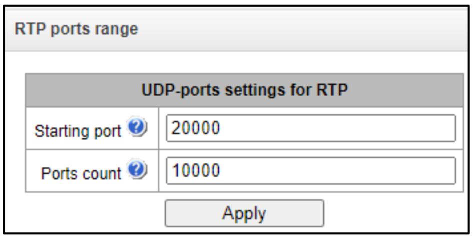
11. To match special characters used in a regular expression, escape them with a "\" (backslash).

*Example:* **^\+7.*** — a string that starts with +7.

#### *4.1.3.6 RTP ports range*

In this section, you may configure UDP port range for voice RTP packets transmission. It is possible to specify from 1 to 32000 ports.

***SBC Configuration –> RTP ports range***



RTP ports range

| UDP-ports settings for RTP | |
|---|---|
| Starting port | 20000 |
| Ports count | 10000 |

***UDP ports settings for RTP***

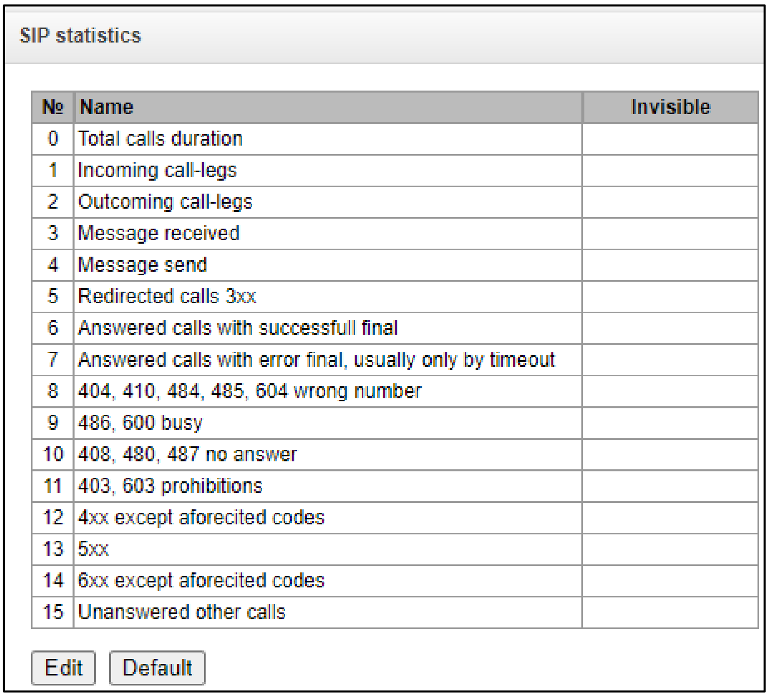
- *Starting port* — the number of the initial UDP port used for transmitting voice traffic (RTP) and data using the T.38 protocol;
- *Ports count* — the range (number) of UDP ports used for transmitting voice traffic (RTP) and T.38 data.

**To avoid collisions, the ports used for RTP and T.38 transmission must not overlap with the ports used for SIP signalling (default port 5060).**

#### *4.1.3.7 SIP statistics*

This section configures the display and structure of groups of statistics. Any group can be hidden from the *«Monitoring - SIP statistics»* menu. In groups 8 to 11 inclusive, you can configure the SIP response codes to be counted in them and the name of the counters to be displayed.

***SBC Configuration –> SIP statistics***

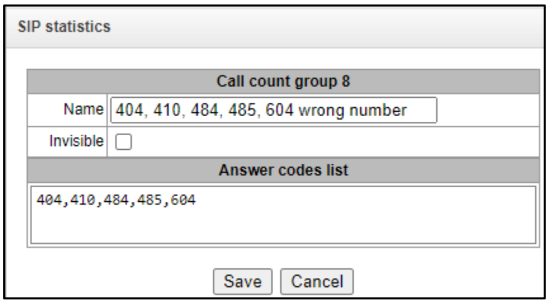


SIP statistics

| № | Name | Invisible |
|---|---|---|
| 0 | Total calls duration | |
| 1 | Incoming call-legs | |
| 2 | Outcoming call-legs | |
| 3 | Message received | |
| 4 | Message send | |
| 5 | Redirected calls 3xx | |
| 6 | Answered calls with successfull final | |
| 7 | Answered calls with error final, usually only by timeout | |
| 8 | 404, 410, 484, 485, 604 wrong number | |
| 9 | 486, 600 busy | |
| 10 | 408, 480, 487 no answer | |
| 11 | 403, 603 prohibitions | |
| 12 | 4xx except aforecited codes | |
| 13 | 5xx | |
| 14 | 6xx except aforecited codes | |
| 15 | Unanswered other calls | |

To configure a group, select it in the table and click the *«Edit»* button. To reset the group to its default state, select it and click the *«Default»* button.

When editing, the following window will open depending on the type of group: with visibility editing only and with full editing.



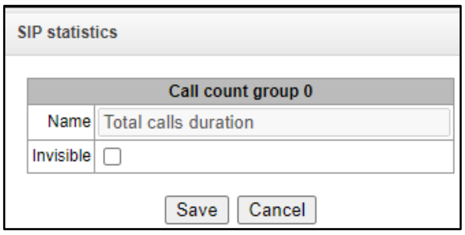
SIP statistics

Call count group 8

| | |
|---|---|
| Name | 404, 410, 484, 485, 604 wrong number |
| Invisible | □ |

Answer codes list

```
404,410,484,485,604
```



SIP statistics

Call count group 0

| | |
|---|---|
| Name | Total calls duration |
| Invisible | □ |

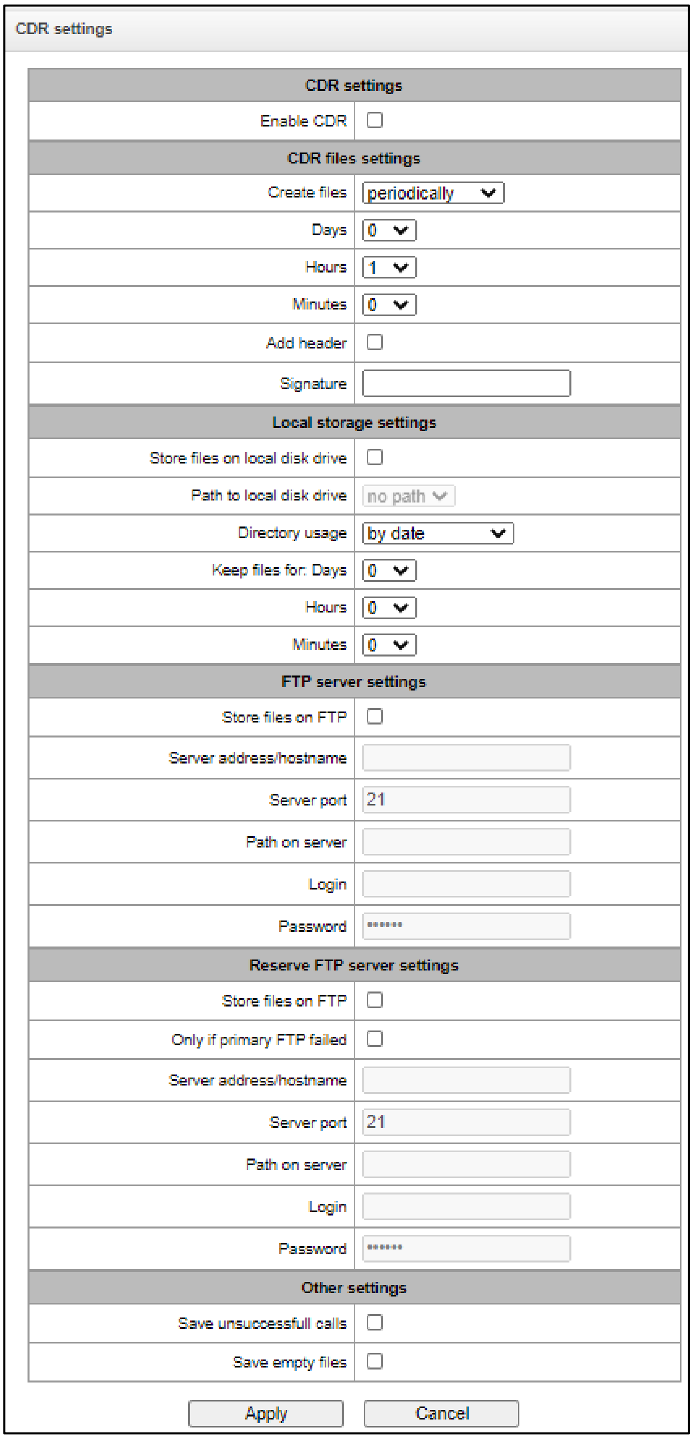
Available for configuration:

- *Name* — displayed statistics group name;
- *Invisible* — when checked, the group will not be displayed in the statistics view;
- *Answer codes list* — here the SIP codes of responses are entered to account for the selected group of statistics.  Codes between 400 and 699 in numeric form separated by spaces, commas, tabs, or line breaks are allowed.

### *4.1.3.8 CDR settings*

This section is used to configure the parameters for saving detailed call records.

**CDR** — detailed call records, allow to store the history of calls made through the SBC gateway.



CDR settings

| | |
|---|---|
| **CDR settings** | |
| Enable CDR | □ |
| **CDR files settings** | |
| Create files | periodically |
| Days | 0 |
| Hours | 1 |
| Minutes | 0 |
| Add header | □ |
| Signature | |
| **Local storage settings** | |
| Store files on local disk drive | □ |
| Path to local disk drive | no path |
| Directory usage | by date |
| Keep files for: Days | 0 |
| Hours | 0 |
| Minutes | 0 |
| **FTP server settings** | |
| Store files on FTP | □ |
| Server address/hostname | |
| Server port | 21 |
| Path on server | |
| Login | |
| Password | •••••• |
| **Reserve FTP server settings** | |
| Store files on FTP | □ |
| Only if primary FTP failed | □ |
| Server address/hostname | |
| Server port | 21 |
| Path on server | |
| Login | |
| Password | •••••• |
| **Other settings** | |
| Save unsuccessfull calls | □ |
| Save empty files | □ |

***Parameters for saving CDR records***

- *Enable CDR* — when checked the gateway will generate CDR records;

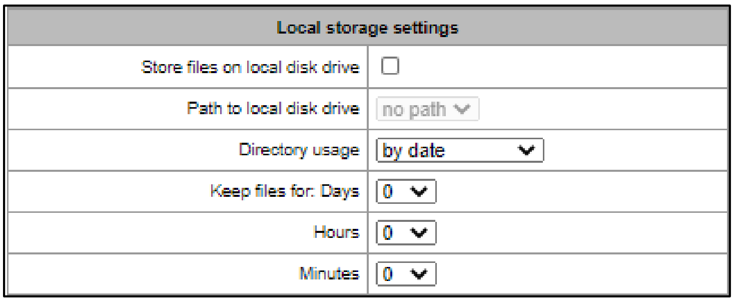
***CDR files settings***

- *Create files* — select CDR file creation mode:
  - *periodically* — CDR file is created after a specified period of time since the device was booted.
  - *once per day* — CDR file is created once a day at a specified time*;*
  - *once per hour* — CDR file is created once an hour at a specified time;
- *Saving period: Days, Hours, Minutes* — period of CDR records formation; during this period CDR-records are stored in the main memory, after that they are saved to the local storage source;

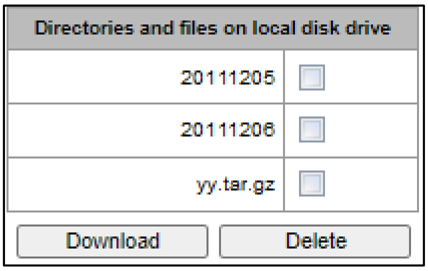
- *Add header* — when checked, the header of the CDR file is written to the beginning of the CDR file in the form of: SBC-1000. CDR. File started at 'YYYYMMDDhhmmss', where 'YYYYMMDDhhmmss' — the time to start saving the records to the file;
- *Signature* — sets a signature that can be used to identify the device that created the record.

***Local storage settings***

- *Store files on local disk drive* — when checked, CDR records are saved on the local drive;
- *Path to local disk drive* — path to local drive. When you specify the path to the local drive, the menu will display a list of folders and files on that drive. To download the data to your computer, check the box next to the desired entries and click *«Download».* In this case, the folder with the records will be placed in the archive, which is recommended to delete after loading to avoid disk overflow. To delete already irrelevant data, check the box next to the desired entries and click *«Delete»*.



| Local storage settings | |
|---|---|
| Store files on local disk drive | □ |
| Path to local disk drive | no path |
| Directory usage | by date |
| Keep files for: Days | 0 |
| Hours | 0 |
| Minutes | 0 |



| Directories and files on local disk drive | |
|---|---|
| 20111205 | □ |
| 20111206 | □ |
| yy.tar.gz | □ |

- *Directory usage* — select directories for storing CDR data:
  - *by date* — CDR records are saved in separate directories, the directory name corresponds to the date of creation of the CDR file, the format of the name is «cdrYYYYMMDD», for example, cdr20150818;
  - *single directory* — all CDR records are saved in a single *«cdr_all»* directory on the selected drive;
- *Keep file for*: *Days, Hours, Minutes* — storage period of CDR records on the local disk drive;

**The device has 30MB in RAM for storing CDR records.**

**If the volume of received CDRs exceeds the 30MB threshold before the retention period expires, all further billing data coming in during that time period will be lost.**

***FTP server settings***

- *Store files on FTP* — when checked, the CDR records will be transferred to the FTP server;
- *Server address/hostname* — FTP server IP address;
- *Server port* — FTP port TCP port;
- *Path on server* — specifies the path to the folder on the FTP server, where the CDR records will be saved;
- *Login* — user name for accessing the FTP server;
- *Password* — password for accessing the FTP server.

***Reserve FTP server settings***

- *Store files on FTP* — when checked, the CDR records will be transferred to the reserve FTP server;
- *Only if primary FTP failed* — if this option is set, then saving CDR to the backup FTP server will be done only if writing to the primary FTP server fails. Otherwise, CDRs will be written simultaneously to the primary and reserve servers.
- *Server address/hostname* — reserve FTP server IP address;

- *Server port* — reserve FTP port TCP port;
- *Path on server* — specifies the path to the folder on the reserve FTP server, where the CDR records will be saved;
- *Login* — user name for accessing the reserve FTP server;
- *Password* — password for accessing the reserve FTP server.

***Other settings***

- *Save unsuccessful calls* — when checked, save unsuccessful calls (that did not end the conversation) to CDR files;
- *Save empty files* — when checked, save CDR-files that do not contain records.

##### 4.1.3.8.1 CDR record format

- the header common to the whole CDR file (the parameter is present if the corresponding setting is enabled);
- signature (present if the setting is enabled) (SIGNATURE);
- time the connection was established in the format YYYY-MM-DD hh:mm:ss (DATATIME);
- information about the caller:
  - caller number (KOD_A);
  - caller trunk number (not implemented in the current version) (N_TR_GR_A);
  - caller category (not implemented in the current version) (CATEG_A);
  - IP address of the caller gateway (SRC_IP);
  - list of IP addresses from the Record-Route headers when a connection is established in the direction from the caller (SRC_R_ROUTE);
  - list of IP addresses from the Via headers when a connection is established in the direction from the caller (SRC_VIA);
  - IP address from the Contact header of the caller (SRC_CONTACT);
- information about the callee:
  - callee number (KOD_B);
  - callee trunk number (not implemented in the current version) (N_TR_GR_B);
  - IP address of the callee gateway (DST_IP);
  - IP address from the Contact header of the callee (DST_CONTACT);
- call duration, sec (T_ECD);
- disconnection reason according to ITU-T Q.850 (CAUSE);
- successful call indicator (with caller answer) (COMPLETEIND);
- disconnect initiator side (PLACE);
- internal reason for disconnection (in the current version it is the same as CAUSE) (TREATMENT);
- call identifier (CONN_ID);
- Caller ID number when forwarding (not implemented in the current version) (REDIRECTED).

##### 4.1.3.8.2 CDR file example

Example of a CDR file containing two records (header and signature saving is enabled):

```
    <SBC>. CDR. File started at '20120726112449'
    SIGNATURE;DATATIME;KOD_A;KOD_B;N_TR_GR_A;N_TR_GR_B;T_ECD;CAUSE;COMPLETEIND;CATEG
_A;PLACE;TREATMENT;CONN_ID;REDIRECTED;SRC_IP;DST_IP;SRC_R_ROUTE;SRC_VIA;SRC_CONTACT;D
ST_CONTACT;
    label;2012-07-26
11:24:39;6502;6501;;;0;16;0;;A;16;zBRyfChAr9mfhIPRI.3xjn4w2X.ui8ap;;192.168.23.170;19
2.168.23.212;;;192.168.23.170;192.168.23.170;
label;2012-07-26 11:24:40;6502;6501;;;0;16;0;;A;16;1343-276680-166831-sip3-
sip3@ecss3;;192.168.23.212;192.168.23.170;;;192.168.23.170;192.168.23.170;
```

### 4.1.4 *Network subsystem*

This section specifies the network settings of the device and the IP packet routing table.

**DHCP** — protocol that allows automatically obtaining IP address and other settings required for operation in TCP/IP network. Allows the gateway to obtain all necessary network settings from DHCP server.

**DNS** — protocol that allows obtaining domain information. Allows the gateway to obtain IP address of the communicating device by its network name (hostname). It may be necessary, e.g. when specifying hosts in the routing plan or using network name of the SIP server as its address.

**TELNET** — protocol that allows establishing mechanisms of control over the network. Allows you to remotely connect to the gateway from a computer for configuration and management purposes. For TELNET protocol operation, the data transfer process is not encrypted.

**SSH** — protocol that allows establishing mechanisms of control over the network. Unlike the TELNET, this protocol implies encryption of all data transferred through the network, including passwords.

**VPN** — technology that allows one or more network connections (a logical network) on top of another network (e.g., the Internet).

**PPTP** — point-to-point tunneling protocol that allows a computer to establish secure connection with a server by creating a special tunnel in a common unsecured network. One of VPN forms.

#### *4.1.4.1 Routing table*

In this submenu, you may configure static routes. A total of up to 255 routes can be configured.

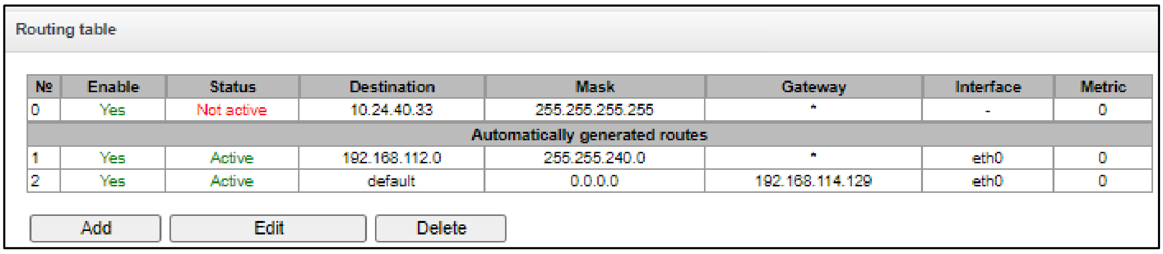
*Static routing* allows you to route packets to defined IP networks or IP addresses through the specified gateways. Packets sent to IP addresses not belonging to the gateway IP network and falling outside the scope of static routing rules will be sent to the default gateway.

Routing table is separated into 2 parts — manually configured routes that are displayed in the top part of the table and automatically created routes.

Automatically created routes cannot be changed as they are created automatically when the network and VPN/PPTP interfaces are established and required for their normal operation.

The table shows the routes used at the time of the request (*«Active»* in the status field), as well as unused (*«Inactive»* in the status field), if the routes were set manually by the operator. Manually created routes, unlike automatically created routes, are not deleted by the system when the corresponding interface is disabled and will be reapplied when the interface is restored to serviceability.

***Network subsystem –> Routing table***



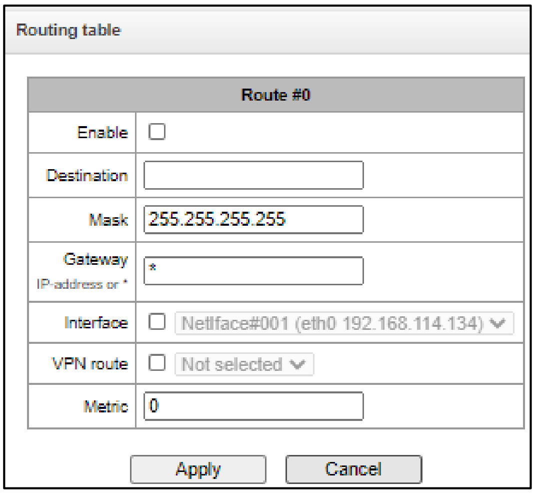
Routing table

| № | Enable | Status | Destination | Mask | Gateway | Interface | Metric |
|---|---|---|---|---|---|---|---|
| 0 | Yes | Not active | 10.24.40.33 | 255.255.255.255 | * | - | 0 |
| Automatically generated routes | | | | | | | |
| 1 | Yes | Active | 192.168.112.0 | 255.255.240.0 | * | eth0 | 0 |
| 2 | Yes | Active | default | 0.0.0.0 | 192.168.114.129 | eth0 | 0 |

To create, edit or remove a route, use *«Objects» — «Add object», «Objects» — «Edit object»* and *«Objects» — «Remove object»* menus and the following buttons:

– *«Add»;*
– *«Edit»;*
– *«Delete»*.

***Network subsystem –> Routing table –> «Add»***



Routing table

| Route #0 | |
|---|---|
| Enable | □ |
| Destination | |
| Mask | 255.255.255.255 |
| Gateway<br>IP-address or * | * |
| Interface | □ NetIface#001 (eth0 192.168.114.134) |
| VPN route | □ Not selected |
| Metric | 0 |

To add a new route, set the following parameters:

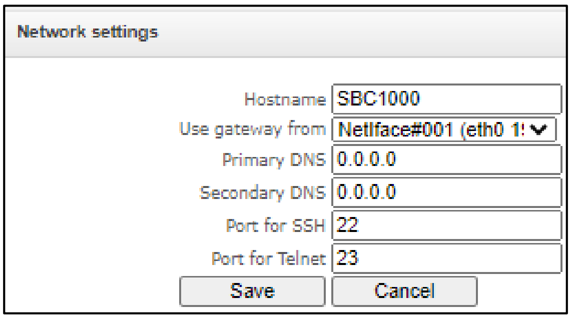
- *Enable* — when checked, the route is available for use;
- *Destination* — IP network, IP address or default (to set the «default» gateway);
- *Mask* — specify a network mask for the defined IP network (use mask 255.255.255.255 for IP address).
- *Gateway* — define IP address of route gateway.
- *Interface* — select the network transmission interface (if not checked, the most appropriate interface will be selected based on the gateway address);
- *VPN route* — transmission interface associated with the VPN client account. The route and address will be automatically set through the associated network interface when the VPN client establish the connection;
- Metric — route metric.

*«Apply»* and *«Cancel»* buttons, are used to save and reset parameters respectively.

### 4.1.4.2 *Network Settings*

In this submenu, you may specify the device name, change the network gateway address, DNS server address and SSH/Telnet access ports.

***Network subsystem –> Network settings***



Network settings

| | |
|---|---|
| Hostname | SBC1000 |
| Use gateway from | NetIface#001 (eth0 1! |
| Primary DNS | 0.0.0.0 |
| Secondary DNS | 0.0.0.0 |
| Port for SSH | 22 |
| Port for Telnet | 23 |

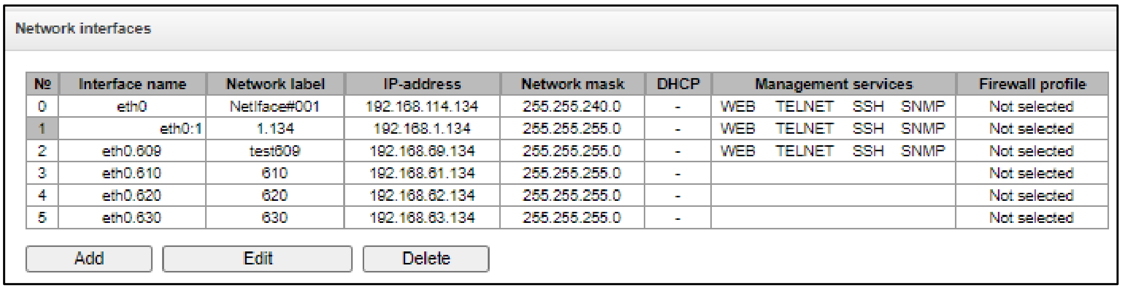
- *Hostname* — network name of the device;
- *Use gateway from* — select network interface that the gateway will consider as a primary for the device;
- *Primary DNS* — primary DNS server;
- *Secondary DNS* — secondary DNS server;
- *Port for SSH* — TCP port for the device access via SSH protocol, default value is 22;
- *Port for Telnet* — TCP port for the device access via Telnet protocol, default value is 23.

### 4.1.4.3 *Network interfaces*

The device allows you to configure 1 primary network interface eth0 and up to 9 additional interfaces; these interfaces may include VLAN interfaces as well as Aliases for primary interface eth0 or VLAN interface.

*Alias* — additional network interface based on the existing primary network interface eth0 or VLAN interface.

***Network subsystem –> Network interfaces***



Network interfaces

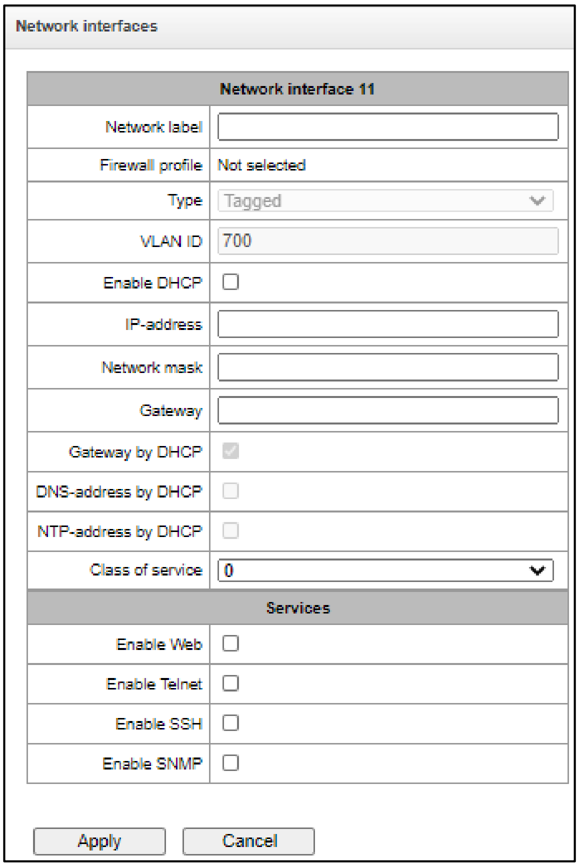
| № | Interface name | Network label | IP-address | Network mask | DHCP | Management services | Firewall profile |
|---|---|---|---|---|---|---|---|
| 0 | eth0 | NetIface#001 | 192.168.114.134 | 255.255.240.0 | - | WEB TELNET SSH SNMP | Not selected |
| 1 | eth0:1 | 1.134 | 192.168.1.134 | 255.255.255.0 | - | WEB TELNET SSH SNMP | Not selected |
| 2 | eth0.609 | test609 | 192.168.69.134 | 255.255.255.0 | - | WEB TELNET SSH SNMP | Not selected |
| 3 | eth0.610 | 610 | 192.168.61.134 | 255.255.255.0 | - | | Not selected |
| 4 | eth0.620 | 620 | 192.168.62.134 | 255.255.255.0 | - | | Not selected |
| 5 | eth0.630 | 630 | 192.168.63.134 | 255.255.255.0 | - | | Not selected |

To create, edit or remove interfaces, use *'Objects' — 'Add an object', 'Objects' — 'Edit an object'* and *'Objects' — 'Remove an object'* and the following buttons:

- *«Add»;*
- *«Edit»;*
- *«Delete»*.

To add a network interface, click the *«Add»* button and fill in the parameters:

***Network subsystem –> Network interfaces –> «Add»***
***(window when selecting the «Tagged» type)***



Network interfaces

| Network interface 11 | |
|---|---|
| Network label | |
| Firewall profile | Not selected |
| Type | Tagged |
| VLAN ID | 700 |
| Enable DHCP | □ |
| IP-address | |
| Network mask | |
| Gateway | |
| Gateway by DHCP | ☑ |
| DNS-address by DHCP | □ |
| NTP-address by DHCP | □ |
| Class of service | 0 |
| **Services** | |
| Enable Web | □ |
| Enable Telnet | □ |
| Enable SSH | □ |
| Enable SNMP | □ |

***Basic settings:***

- *Network label* — arbitrary name (for the carrier convenience), with which the specified network settings will be associated;
- *Firewall profile* — show the selected firewall profile for the current interface;
- *Type* — interface type (always untagged for eth0 interface).
  - *untagged* — untagged interface (without VLAN);
  - *tagged* — tagged interface (with VLAN);
  - *VPN/pptp client* — client interface for connecting VPN to a remote server via PPTP;
- *VLAN ID* — VLAN identifier (1–4095) (only for tagged type interfaces);
- *Enable DHCP* — obtain an IP address dynamically from a DHCP server (requires a DHCP server in the carrier network);
- *IP-address* — device network address;
- *Network mask* — network mask for device;
- *Gateway* — default gateway;
- *Gateway by DHCP* — obtain the gateway address from the DHCP server;
- *DNS-address by DHCP* — obtain DNS server IP address dynamically from DHCP server;
- *NTP-address by DHCP* — obtain NTP server IP address dynamically from DHCP server;
- *Class of service* — set the traffic priority tag according to the IEEE 802.1p standard.

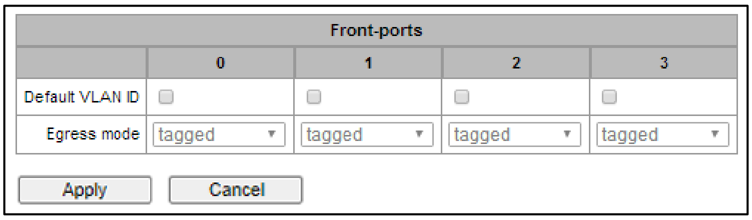
***Services*** — configuration menu for services enabled the current interface:

- *Enable Web* — enables access to configurator through the interface;
- *Enable Telnet* — enables access via telnet protocol through the interface;
- *Enable SSH* — enables access via ssh protocol through the interface;
- *Enable SNMP* — enables SNMP utilization through the interface.

**If an IP address or network mask has been changed, or web configurator management has been disabled for the network interface, confirm these settings by logging into the web configurator to prevent the loss of access to the device; otherwise, the previous configuration will be restored when two-minute timeout expires.**

**Front-ports[1] — external front port configuration**

This setting is only available for tagged VLAN interfaces (the *«Type»* parameter is set to *«Tagged»*).



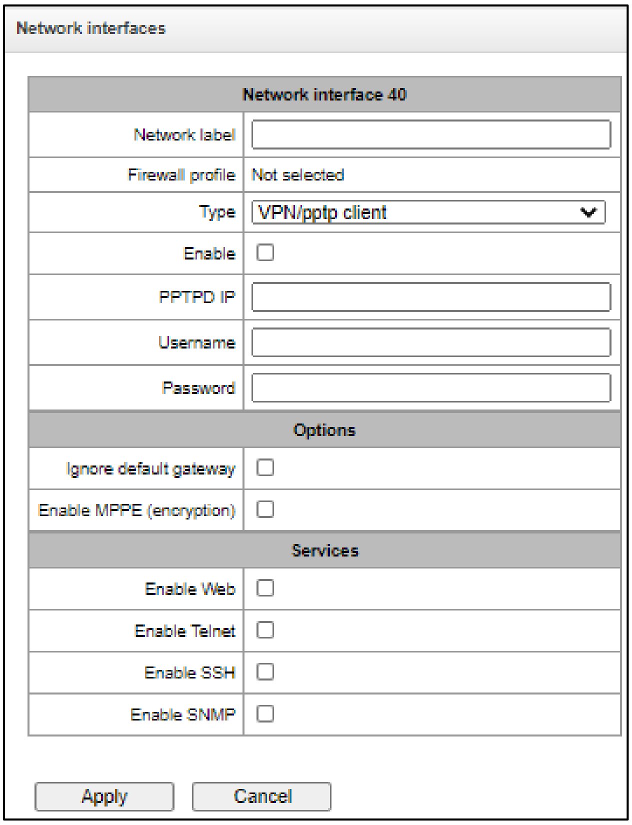
| Front-ports | | | | |
|---|---|---|---|---|
| | 0 | 1 | 2 | 3 |
| Default VLAN ID | □ | □ | □ | □ |
| Egress mode | tagged ▾ | tagged ▾ | tagged ▾ | tagged ▾ |

Apply Cancel

- *Default VLAN ID* — when a packet without VLAN ID tag comes to the port, this packet will be tagged with VLAN ID tag of the selected network interface, if the packet is received with VLAN ID tag, this tag remains unchanged;
- *Egress mode* — VLAN tag operation rules during packet transfer from the port:
  - *tagged* — send packet with the selected interface VLAN ID;
  - *untagged* — send packet without VLAN ID.

***Network subsystem –> Network interfaces –> «Add»***
***(window when selecting the «VPN/pptp client» type)***

If you select VPN/pptp client in the *«Type»* field, special settings will become available*:*



Network interfaces

| Network interface 40 | |
|---|---|
| Network label | |
| Firewall profile | Not selected |
| Type | VPN/pptp client ▾ |
| Enable | □ |
| PPTPD IP | |
| Username | |
| Password | |
| **Options** | |
| Ignore default gateway | □ |
| Enable MPPE (encryption) | □ |
| **Services** | |
| Enable Web | □ |
| Enable Telnet | □ |
| Enable SSH | □ |
| Enable SNMP | □ |

Apply Cancel

- *Network label* — network name;
- *Firewall profile* — show the selected firewall profile for the current interface;
- *Type* — VPN/pptp client;
- *Enable* — enable VPN/PPP interface;
- *PPTPD IP* — PPTP server IP address;
- *Username* — username (login) used by the device for the network connection;
- *Password* — VPN connection password.

***Options:***

- *Ignore default gateway* — ignore the gateway setting in the *«Network parameters»* section;
- *Enable MPPE (encryption)* — enable encryption.

***Services*** — configuration menu for services enabled the current interface:

- *Enable Web* — enables access to configurator through the interface;
- *Enable Telnet* — enables access via telnet protocol through the interface;
- *Enable SSH* — enables access via ssh protocol through the interface;
- *Enable SNMP* — enables SNMP utilization through the interface.

[1] Only for SBC-2000

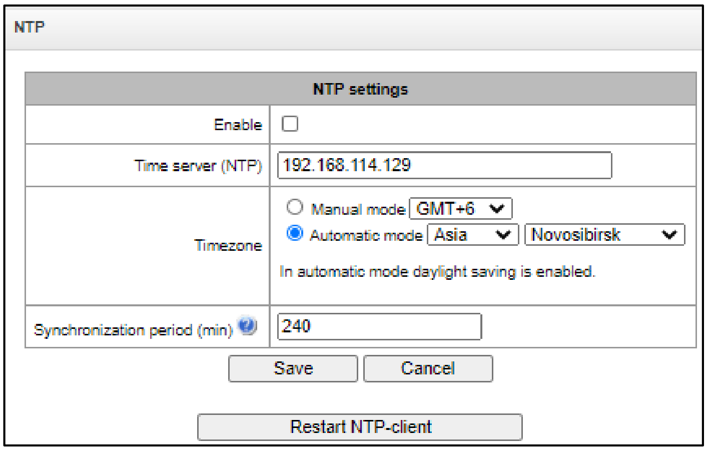
## 4.1.5 *Network services*

### *4.1.5.1 NTP*

This submenu configures the time synchronization service.

**NTP** — protocol designed for synchronization of real-time clock of the device. Allows synchronising date and time used by the gateway against their reference values.

***Network services –> NTP***



NTP

| NTP settings | |
|---|---|
| Enable | □ |
| Time server (NTP) | 192.168.114.129 |
| Timezone | ○ Manual mode GMT+6<br>● Automatic mode Asia Novosibirsk<br>In automatic mode daylight saving is enabled. |
| Synchronization period (min) | 240 |

- *Enable* — enable NTP client;
- *Time server (NTP)* — time server from which the device will synchronize the date and time;
- *Timezone* — timezone and GMT (Greenwich Mean Time) offset configuration:
  - *Manual mode* — define GMT offset;
  - *Automatic mode* — in this mode, you may select the device location, GMT offset will be defined automatically, also this mode enables automatic daylight saving change;
- *Synchronization period (min)* — time synchronization request transmission period.

The *«Save»* and *«Cancel»* buttons are used to save and discard changes. To perform forced time synchronization with the server, click *«Restart NTP client»* button (NTP client will be restarted).

### *4.1.5.2 SNMP*

**SNMP** — Simple network management protocol. It allows the device to send real-time messages on occurred failures to controlling SNMP manager. In addition, device SNMP agent supports monitoring of gateway sensors' status on request from SNMP manager.

SNMP monitoring functions are able to request the following parameters from the gateway:

- Gateway name
- Device type
- Firmware version
- IP address
- IP submodule statistics
- Linkset state
- IP channel state (statistics for the current calls via IP)

Statistics for the current calls performed via IP channels contains the following data:

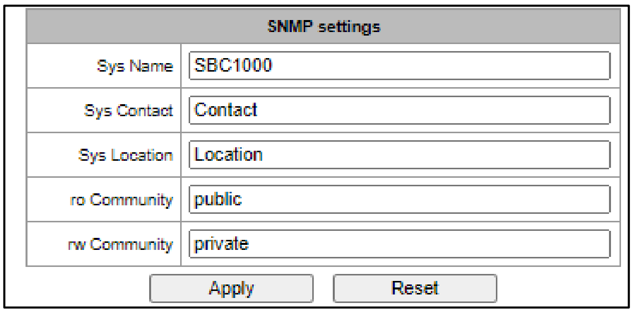
- Channel number
- Channel state
- Call identifier
- Caller MAC address

- Caller IP address
- Caller number
- Callee MAC address
- Callee IP address
- Callee number
- Channel engagement duration

#### 4.1.5.2.1 SNMP settings

***Network services –> SNMP***

- *Sys Name* — device system name;
- *Sys Contact* — device manufacturer contacts;
- *Sys Location* — device location;
- *ro Community* — password for parameter reading (common: public);
- *rw Community* — password for parameter writing (common: private).



| SNMP settings | |
|---|---|
| Sys Name | SBC1000 |
| Sys Contact | Contact |
| Sys Location | Location |
| ro Community | public |
| rw Community | private |

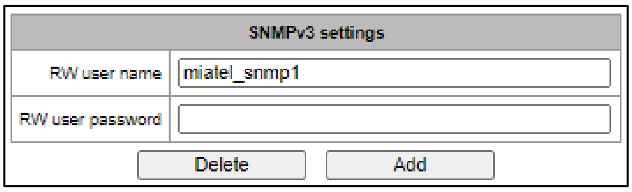
#### 4.1.5.2.2 SNMPv3 settings

***Network services –> SNMP (SNMPv3 settings)***

**SNMPv3 configuration:**

The system uses a single SNMPv3 user.

- *RW user name* — username;
- *RW user password* — password (password should contain 8 characters or more).



| SNMPv3 settings | |
|---|---|
| RW user name | miatel_snmp1 |
| RW user password | |

To apply SNMPv3 user configuration, click *'Add'* button (settings will be applied immediately). To remove an entry, click *'Delete'* button.

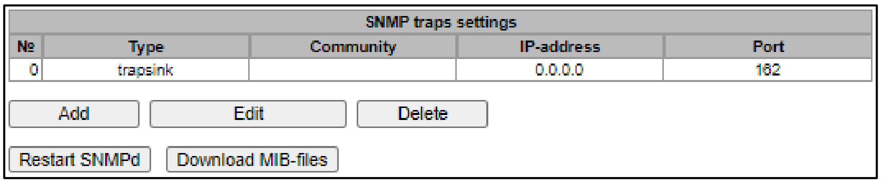
#### 4.1.5.2.3 SNMP trap configuration

**For detailed monitoring parameters and Traps description, see MIB files on disk shipped with firmware.**

SNMP agent sends SNMPv2-trap message, when the following events occur:

- Configuration error
- subscriber registration is restricted;
- call is restricted;
- dynamic firewall blocked the new address;
- high CPU load;
- fan operation problem;
- Configuration error corrected
- FTP server unavailable, CDR file storage RAM is over 50% (15–30 MB) full;
- FTP server unavailable, CDR file storage RAM is to 50% (5–15 MB) full;
- FTP server unavailable, CDR file storage RAM is full up to 5 MB;
- Software update or configuration file upload/download status.

*Network services –> SNMP (SNMP traps settings)*

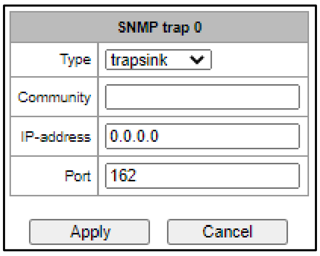


SNMP traps settings

| № | Type | Community | IP-address | Port |
|---|---|---|---|---|
| 0 | trapsink | | 0.0.0.0 | 162 |

- *Restart SNMPd* — SNMP client restarts when the button is clicked;

*Network services –> SNMP (SNMP traps settings) –> «Add»*



SNMP trap 0

| | |
|---|---|
| Type | trapsink |
| Community | |
| IP-address | 0.0.0.0 |
| Port | 162 |

Up to 16 traps can be created. To create, edit or remove trap parameters, use the following buttons:

- *"Add";*
- *«Edit»;*
- *«Delete».*

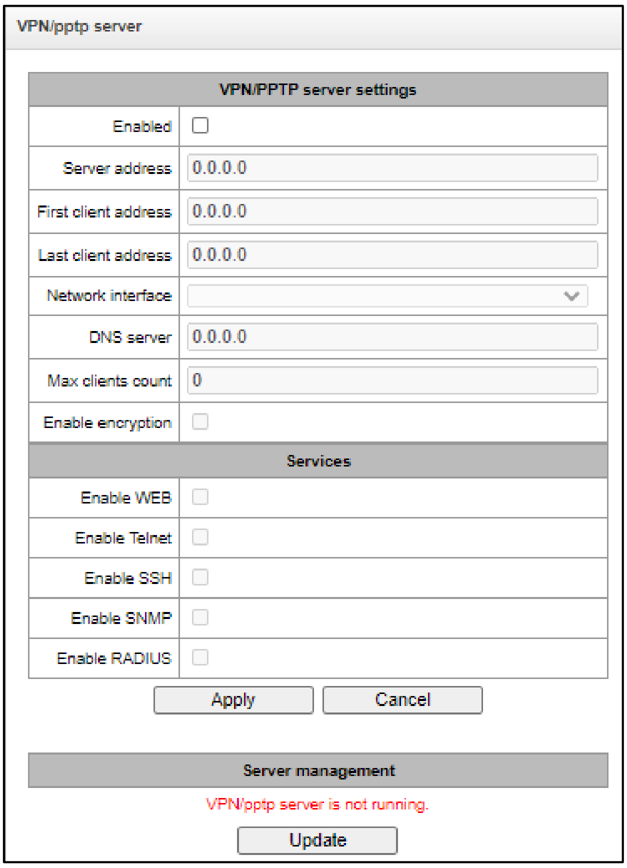
- *Type* — SNMP message type (TRAPv1, TRAPv2, INFORM);
- *Community* — password contained in traps;
- *IP-address* — trap recipient IP address;
- *Port* — trap receiver UDP port.

#### 4.1.5.2.4 Retrieving MIB files

In the current firmware version, you can download the current MIB files directly from the device by clicking the *«Download MIB-files»* button.

### *4.1.5.3 VPN/PPTP server*

*Network services –> VPN/PPTP server*



VPN/pptp server

VPN/PPTP server settings

| | |
|---|---|
| Enabled | ☐ |
| Server address | 0.0.0.0 |
| First client address | 0.0.0.0 |
| Last client address | 0.0.0.0 |
| Network interface | |
| DNS server | 0.0.0.0 |
| Max clients count | 0 |
| Enable encryption | ☐ |
| **Services** | |
| Enable WEB | ☐ |
| Enable Telnet | ☐ |
| Enable SSH | ☐ |
| Enable SNMP | ☐ |
| Enable RADIUS | ☐ |

Server management

VPN/pptp server is not running.

*VPN/PPTP server settings*

- *Enabled* — start the service at startup/reboot;
- *Server address* — IP address that will be reported as the server address to all connecting PPTP clients;
- *First client address*, *Last client address* — range of IP addresses assigned to PPTP clients;
- *Network interface* — select the interface to connect to the VPN/PPTP server;
- *DNS server* — address of the DNS server, which will be reported to clients;
- *Max clients count* — number of simultaneous client connections;
- *Enable encryption* — encryption of transmitted data (must also be enabled on the client);

- *Enable Web, Enable Telnet, Enable SSH* — when checked, the corresponding management service is available at the specified interface address;
- *Enable SNMP* — enables SNMP utilization through the interface;
- *Enable RADIUS* — enables RADIUS protocol utilization through the interface.

The *«Start»* and *«Stop»* buttons are used to control the PPTP server. When stopped, new client connections will not be created, but those already created will continue to work. Server status information is updated by clicking the *«Update»* button next to the header.

### *4.1.5.4 L2TP server*

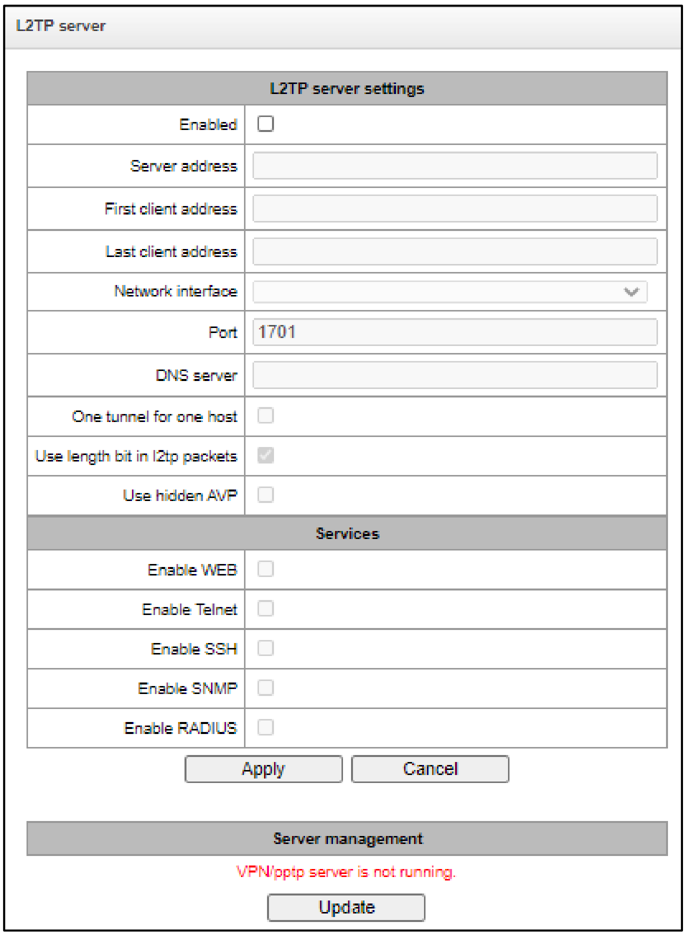
***L2TP server settings***

- *Enabled* — start the service at startup/reboot;
- *Server address* — IP address that will be reported as the server address to all connecting L2TP clients;
- *First client address, Last client address* — range of IP addresses assigned to L2TP clients;
- *Network interface* — select the interface to connect to the L2TP server;
- *Port* — number of port used for connection;
- *DNS server* — address of the DNS server, which will be reported to clients;
- *One tunnel for one host* — limit the number of tunnels to one per host;
- *Use length bit in l2tp packets* — using the length bit represented in the L2TP packet load;
- *Use hidden AVP* — use of hidden AVPs (more details in RFC 2661);

- *Enable Web, Enable Telnet, Enable SSH* — the availability of the corresponding management service at the specified address;
- *Enable SNMP, Enable RADIUS* — flag to enable the corresponding client at the specified address.

Server status information is updated by clicking the *«Update»* button next to the header.

***Network services –> L2TP server***



L2TP server

| L2TP server settings | |
|---|---|
| Enabled | ☐ |
| Server address | |
| First client address | |
| Last client address | |
| Network interface | |
| Port | 1701 |
| DNS server | |
| One tunnel for one host | ☐ |
| Use length bit in l2tp packets | ☑ |
| Use hidden AVP | ☐ |
| **Services** | |
| Enable WEB | ☐ |
| Enable Telnet | ☐ |
| Enable SSH | ☐ |
| Enable SNMP | ☐ |
| Enable RADIUS | ☐ |

Server management

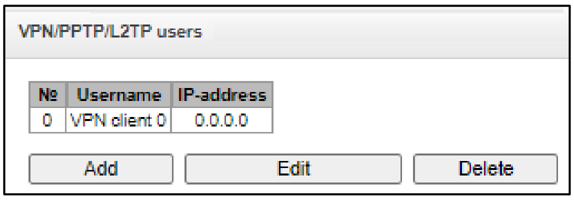
VPN/pptp server is not running.

### *4.1.5.5 VPN/PPTP/L2TP users*

This table shows a list of VPN/PPTP/L2TP clients that are allowed to connect to this server.

The client can be assigned a permanent IP address from the configured range (*Client address*). If 0.0.0.0 is set, the client will get a free IP address from the range each time a new connection is made.

***Network services –> L2TP server***

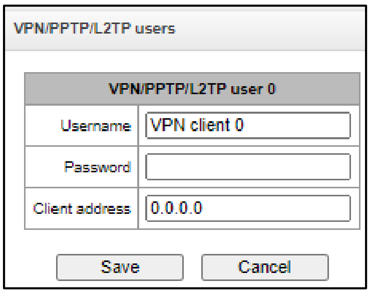


VPN/PPTP/L2TP users

| № | Username | IP-address |
|---|---|---|
| 0 | VPN client 0 | 0.0.0.0 |

To add a user, you need to fill the following fields:

- *Username* — the name with which the user will connect to the server;
- *Password* — the password with which the user will connect to the server;
- *Client address* — address to be given to the client inside the tunnel. If you want to output the address dynamically, you must leave the field blank or with the address 0.0.0.0.



VPN/PPTP/L2TP users

| VPN/PPTP/L2TP user 0 | |
|---|---|
| Username | VPN client 0 |
| Password | |
| Client address | 0.0.0.0 |

### 4.1.6 *Network switch*[1]

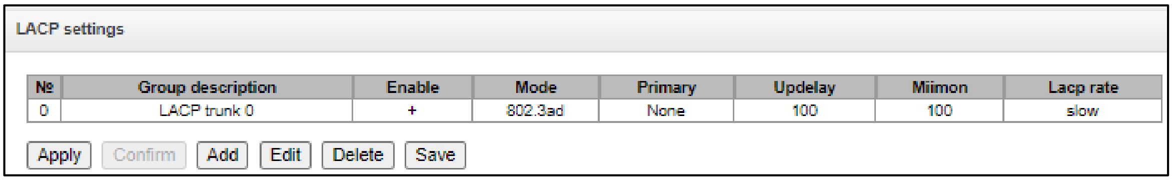
The *«Network switch»* menu is intended to configure switch ports.

#### 4.1.6.1.1 LACP settings

In this section, you may configure LACP groups. You can set up to 5 groups for SBC-1000.

**Link Aggregation Control Protocol (LACP)** — protocol, designed for combining multiple physical channels into one logical channel.

***Network switch –> LACP settings***



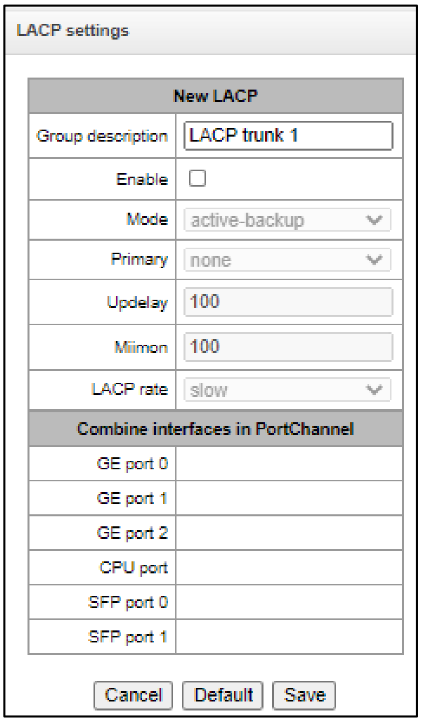
LACP settings

| № | Group description | Enable | Mode | Primary | Updelay | Miimon | Lacp rate |
|---|---|---|---|---|---|---|---|
| 0 | LACP trunk 0 | + | 802.3ad | None | 100 | 100 | slow |

To edit, delete and apply changes to the LACP group, use the *«Edit», «Delete»* and *«Apply»* buttons. To set new LACP group, click the *«Add»* button and fill the following fields:

***Network switch –> LACP settings –> «Add»***

- *Group description* — LACP group name;
- *Enable* — when checked, LACP will be enabled;
- *Mode* — LACP operation mode:
  - *active-backup* — one interface operates in active mode, while others in standby mode. If an active interface goes out of service, the control will be transferred to one of the standby interfaces. This function doesn't have to be supported by the switch.
  - *balance-xor* — packet transmission is allocated among the interfaces merged according to the formula: ((source MAC address) XOR (destination MAC address)) % number of interfaces. A certain interface operates with a specific recipient. This mode allows balancing the load and increasing the robustness;
  - *802.3ad* — dynamic port aggregation. This mode enables significant boost of the incoming and outgoing traffic bandwidth through utilization of every single aggregated interface. This function must be supported by the switch, and in some cases it requires an additional switch setting;
- *Primary* — primary interface configuration;
- *Updelay* — interface change time if the primary interface is unavailable;
- *Miimon* — MII monitoring time, frequency in milliseconds;
- *LACP rate* — the transmission interval of the LACPDU control packets:
  - *fast* — transmission interval is 1 second;
  - *slow* — transmission interval is 30 seconds.
- *Combine interfaces in PortChannel* — list of ports added to LACP group.



LACP settings

New LACP

| | |
|---|---|
| Group description | LACP trunk 1 |
| Enable | □ |
| Mode | active-backup |
| Primary | none |
| Updelay | 100 |
| Miimon | 100 |
| LACP rate | slow |

Combine interfaces in PortChannel

| | |
|---|---|
| GE port 0 | |
| GE port 1 | |
| GE port 2 | |
| CPU port | |
| SFP port 0 | |
| SFP port 1 | |

[1] This menu is available for SBC-1000 only

### 4.1.6.2 *Configuration of switch ports*

The switch can operate in four modes:

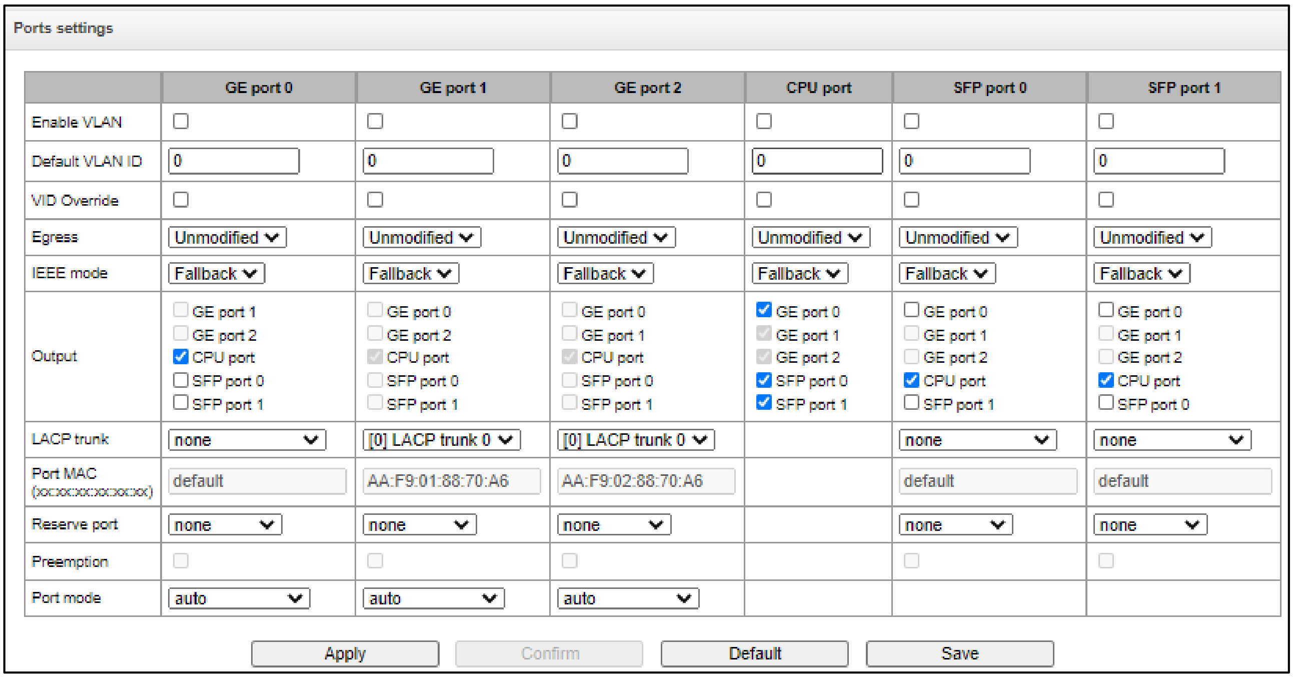
1. ***Without VLAN settings*** — to use this mode, *«Enable VLAN»* checkboxes should be deselected for all ports, *«IEEE Mode»* value should be set to *«Fallback»* for all ports, mutual availability of data ports should be set to *«Output»* with the respective checkboxes. *«802.1q»* routing table in *«802.1q»* tab should not contain any entries.

2. ***Port based VLAN* —** to use this mode, *«IEEE Mode»* value should be set to *«Fallback»* for all ports, mutual availability of data ports should be set to *«Output»* with the respective checkboxes. For VLAN operation, use *«Enable VLAN», «Default VLAN ID», «Egress»* and *«Override» settings. «802.1q»* routing table in *«802.1q»* tab should not contain any entries.

*3.* ***802.1q*** — to use this mode, *«IEEE Mode»* value should be set to *«Check»* or *«Secure» for all ports.* For VLAN operation, use *«Enable VLAN», «Default VLAN ID», and «Override» settings.* Also, routing rules described in *«802.1q»* routing table in *«802.1q»* tab will apply.

*4.* ***802.1q + Port based VLAN.*** 802.1q mode may be used in combination with 'Port based VLAN'. In this case, *«IEEE Mode»* value should be set to *«Fallback»* for all ports, mutual availability of data ports should be set to *«Output»* with the respective checkboxes. For VLAN operation, use *«Enable VLAN», «Default VLAN ID», «Egress» and «Override» settings.* Also, routing rules described in *«802.1q»* routing table in *«802.1q»* tab will apply.

***Network switch –> Ports settings***



Ports settings

| | GE port 0 | GE port 1 | GE port 2 | CPU port | SFP port 0 | SFP port 1 |
|---|---|---|---|---|---|---|
| Enable VLAN | □ | □ | □ | □ | □ | □ |
| Default VLAN ID | 0 | 0 | 0 | 0 | 0 | 0 |
| VID Override | □ | □ | □ | □ | □ | □ |
| Egress | Unmodified | Unmodified | Unmodified | Unmodified | Unmodified | Unmodified |
| IEEE mode | Fallback | Fallback | Fallback | Fallback | Fallback | Fallback |
| Output | □ GE port 1<br>□ GE port 2<br>☑ CPU port<br>□ SFP port 0<br>□ SFP port 1 | □ GE port 0<br>□ GE port 2<br>☑ CPU port<br>□ SFP port 0<br>□ SFP port 1 | □ GE port 0<br>□ GE port 1<br>☑ CPU port<br>□ SFP port 0<br>□ SFP port 1 | ☑ GE port 0<br>☑ GE port 1<br>☑ GE port 2<br>☑ SFP port 0<br>☑ SFP port 1 | □ GE port 0<br>□ GE port 1<br>□ GE port 2<br>☑ CPU port<br>□ SFP port 1 | □ GE port 0<br>□ GE port 1<br>□ GE port 2<br>☑ CPU port<br>□ SFP port 0 |
| LACP trunk | none | [0] LACP trunk 0 | [0] LACP trunk 0 | | none | none |
| Port MAC (xx:xx:xx:xx:xx:xx) | default | AA:F9:01:88:70:A6 | AA:F9:02:88:70:A6 | | default | default |
| Reserve port | none | none | none | | none | none |
| Preemption | □ | □ | □ | | □ | □ |
| Port mode | auto | auto | auto | | | |

**In factory configuration, switch ports may not access each other.**

SBC-1000 switch is equipped with 3 electrical Ethernet ports, 2 optic ports and 1 port for CPU interactions:

- *GE port 0, port 1, port 2* — electrical Ethernet ports of the device;
- *SFP port (0, 1)* — optical Ethernet ports of the device;
- *CPU port* — an internal port connected to the device's CPU.

**All ports of the device are independent; SBC-1000 does not use combo ports.**

***Switch settings***

- *Enable VLAN* — when checked, enable «Default VLAN ID», «Override» and «Egress» settings for this port, otherwise they will be disabled;
- *Default VLAN ID* — when an untagged packet is received at the port, this will be its VID; when a tagged packet is received at that port, its VID is considered to be specified in its VLAN tag.
- *VID Override* — when checked, any received packet is considered to have a VID specified in the *default VLAN ID line.* This is true both for untagged and tagged packets;
- *Egress*:
  - *unmodified* — packets are transmitted by this port unchanged (i.e. in the same form as they came to the other port of the switch);
  - *untagged* — packets will always be sent without VLAN tag by this port;
  - *tagged* — packets will always be sent with VLAN tag by this port;
  - *double tag* — each packet will be sent with two VLAN tags — if received packet was tagged and came with one VLAN tag — if the received packet was untagged;
- *IEEE mode* — sets security modes when processing received tagged frames*:*
  - *fallback* — frame is received on the incoming port regardless of its 802.1q tag in the «802.1q» routing table.

▪ If the 802.1q tag is not contained in the «802.1q» routing table, the frame is transmitted to the outgoing port as long as it is allowed in the «output» section of the incoming port settings.

▪ If the 802.1q tag is contained in the «802.1q» routing table, the frame is transmitted to the outgoing port as long as it is a VLAN member in the «802.1q» table and the port is allowed in the «output» section of the incoming port settings.

  - *check* — frame is received by incoming port if its 802.1q tag is contained in the «802.1q» routing table (the incoming port does not have to be a VLAN member in the «802.1q» table).

▪ The frame is transmitted to the outgoing port if this port is the VLAN member in the «802.1q» table and is allowed in the «output» section of the incoming port settings.

  - *secure* — frame is received by incoming port if its 802.1q tag is contained in the «802.1q» routing table and the incoming port is the VLAN member in the «802.1q» table.

▪ The frame is transmitted to the outgoing port if this port is the VLAN member in the «802.1q» table and is allowed in the «output» section of the incoming port settings.

  - *Output* — mutual availability of data ports. Defines privileges that allow packets received by this port to be transferred to flagged ports.
  - *LACP trunk* — select the LACP group to which the specified switch port belongs;
  - *Port MAC* — change the port MAC address. The option is editable when the LACP group on the port is selected. Ports belonging to the same LACP group must have different MAC addresses;
  - *Reserve port* — select the port that will receive the traffic when abnormal situation occurs (i.e. line interruption). This setting is required for provisioning of Dual Homing redundancy.
  - *Preemption* — when checked, return to master port when it becomes available.

✓ **This firmware version supports the global dual homing only.**

- *Port mode* — select port operation mode (auto, 10/100 Mbps Half, 10/100 Mbps Full, 1 Gbps). Mode configuration is possible for electric Ethernet ports only (*GE port 0, GE port 1, GE port 2*).

! **Click '*Confirm*' button in 1-minute interval to confirm settings, or the previous values will be restored.**

To apply settings, click *«Apply»* button; to confirm applied settings, click *«Confirm»* button.

Use the *«Default»* button to set default parameters (the figure below shows default values).

To save settings to the configuration file without applying them, click *«Save»* button.

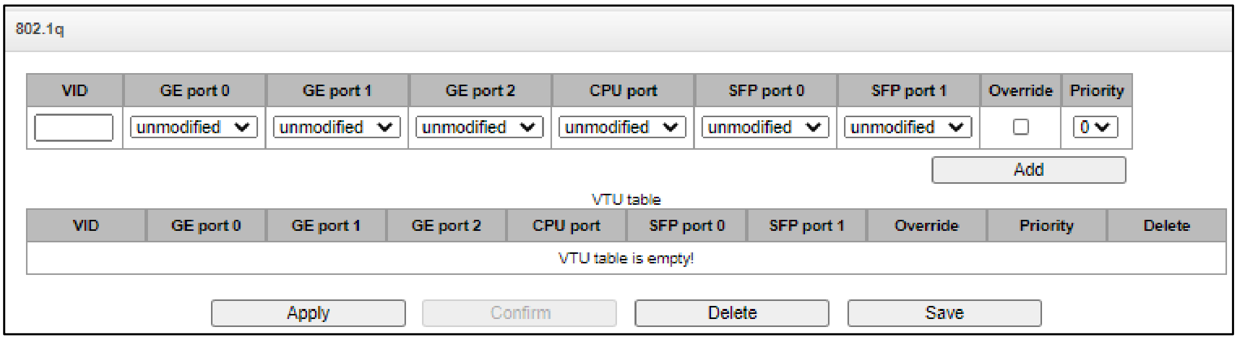
### 4.1.6.3 802.1q

In *'802.1q'* submenu, you may define the configuration of packet routing rules for switch operation in 802.1q mode. The table may contain up to 1024 characters.

Gateway switch is equipped with 3 electrical Ethernet ports, 2 optical ports and 1 port for CPU interactions:

- *GE port 0, port 1, port 2* — electrical Ethernet ports of the device;
- *CPU port* — an internal port connected to the device's CPU;
- *SFP port (0, 1)* — optical Ethernet ports of the device.

***Network switch –> 802.1q***



802.1q

| VID | GE port 0 | GE port 1 | GE port 2 | CPU port | SFP port 0 | SFP port 1 | Override | Priority |
|---|---|---|---|---|---|---|---|---|
|  | unmodified | unmodified | unmodified | unmodified | unmodified | unmodified | □ | 0 |

VTU table

| VID | GE port 0 | GE port 1 | GE port 2 | CPU port | SFP port 0 | SFP port 1 | Override | Priority | Delete |
|---|---|---|---|---|---|---|---|---|---|
| VTU table is empty! |  |  |  |  |  |  |  |  |  |

***Adding records to the packet routing table***

- *VID* — enter the ID of the VLAN group for which the routing rule is being created and for each port assign the actions it performs when transmitting a packet with the specified VID.
  - *unmodified* — packets are transmitted with no changes (i.e. in the same form as they were received);
  - *untagged* — packets will always be sent without VLAN tag by this port;
  - *tagged* — packets will always be sent with VLAN tag by this port;
  - *not member* — packets with specified VID are not transmitted by this port, i.e. the port is not a member of this VLAN group.

Then, click *«Add» button.* To apply the configuration, click the *«Apply»* button, then confirm the settings with the *«Confirm»* button.

**Click *'Confirm'* button in 1-minute interval to confirm settings, or the previous values will be restored.**

It is possible to save the settings to the Flash memory of the device without using the *«Save»* button.

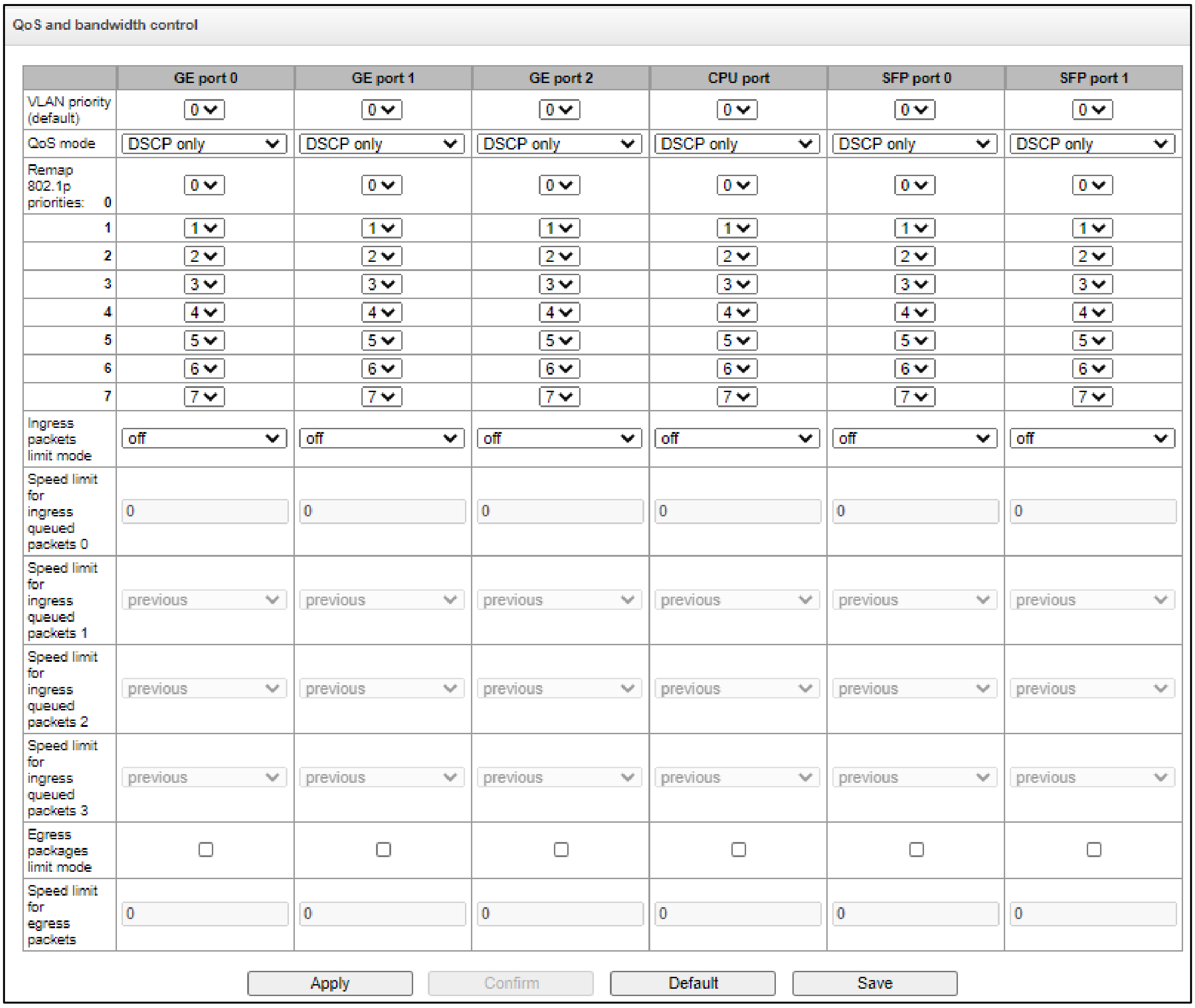
***Removing records from the packet routing table***

To remove records, select checkboxes for the rows to be removed and click *«Remove selected»* button.

#### 4.1.6.4 QoS and bandwidth control

In the section *"QoS and bandwidth control",* Quality of Service (QoS) functions are configured.

***Ethernet switch –> QoS and bandwidth control***



QoS and bandwidth control

| | GE port 0 | GE port 1 | GE port 2 | CPU port | SFP port 0 | SFP port 1 |
|---|---|---|---|---|---|---|
| VLAN priority (default) | 0 | 0 | 0 | 0 | 0 | 0 |
| QoS mode | DSCP only | DSCP only | DSCP only | DSCP only | DSCP only | DSCP only |
| Remap 802.1p priorities: 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 7 | 7 | 7 | 7 | 7 | 7 | 7 |
| Ingress packets limit mode | off | off | off | off | off | off |
| Speed limit for ingress queued packets 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Speed limit for ingress queued packets 1 | previous | previous | previous | previous | previous | previous |
| Speed limit for ingress queued packets 2 | previous | previous | previous | previous | previous | previous |
| Speed limit for ingress queued packets 3 | previous | previous | previous | previous | previous | previous |
| Egress packages limit mode | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Speed limit for egress packets | 0 | 0 | 0 | 0 | 0 | 0 |

- *VLAN priority (default)* — 802.1p priority assigned to untagged packets, received by this port. If *802.1p* or *IP diffserv* priority is already assigned to the packet, this setting will not be used ('default vlan priority' will not be applied to packets containing IP header, when one of the QoS modes is in use: *DSCP only, DSCP preferred, 802.1p preferred*, and also to untagged packets;
- *QoS mode* — QoS operation mode:
  - *DSCP only* — distribute packets into queues based on IP diffserv priority only;
  - *802.1p only* — distribute packets into queues based on 802.1p priority only;
  - *DSCP, 802.1p* — distribute packets into queues based on IP diffserv and 802.1p priorities, if both priorities are present in the packet, IP diffserv priority is used for queuing purposes;
  - *802.1p, DSCP* — distribute packets into queues based on IP diffserv and 802.1p priorities, if both priorities are present in the packet, 802.1p priority is used for queuing purposes;
- *Remap 802.1p priority* — remap 802.1p priorities for untagged packets. Thus, a new value may be assigned for each priority received in VLAN packet.
- *Ingress packets limit mode* — restriction mode for traffic coming to the port:
  - *Off* — no limit;
  - *All packets* — restrict all traffic;
  - *BroadMultFlood* — multicast, broadcast, and flooded unicast traffic will be restricted;
  - *BroadMult* — multicast and broadcast traffic will be restricted;
  - *Broad* — only broadcast traffic will be restricted;

- *Speed limit for ingress queued packets 0* — bandwidth restriction for traffic incoming to a queue 0 port. Permitted values—from 70 to 250000kbps.
- *Speed limit for ingress queued packets 1* — bandwidth restriction for traffic incoming to a queue 1 port. You can double the bandwidth (prev prio *2) of priority 0, or leave it unchanged (same as prev prio).
- *Speed limit for ingress queued packets 2* — bandwidth restriction for traffic incoming to a queue 2 port. You can double the bandwidth (prev prio *2) of priority 1, or leave it unchanged (same as prev prio).
- *Speed limit for ingress queued packets 3* — bandwidth restriction for traffic incoming to a queue 3 port. You can double the bandwidth (prev prio *2) of priority 2, or leave it unchanged (same as prev prio).
- *Egress packets limit mode* — when this flag is checked, bandwidth limitation for outgoing traffic from the port is allowed;
- *Speed limit for egress packets* — bandwidth limitation for outgoing traffic from the port. Permitted values — from 70 to 250000kbps.

- *Apply* — apply defined settings;
- *Confirm* — confirm modified settings;

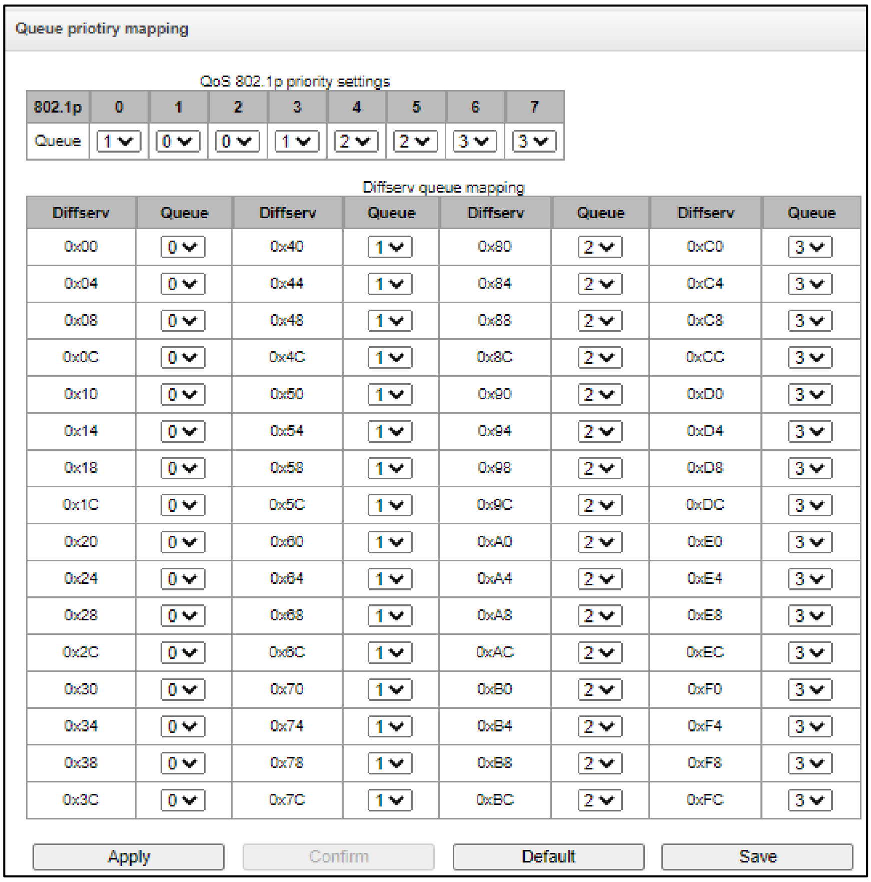
**Click *'Confirm'* button in 1-minute interval to confirm settings, or the previous values will be restored.**

- *Default* — set default settings;
- *Save* — save settings into the device flash memory without applying them.

### 4.1.6.5 *Queue priority mapping*

In the section *"QoS and bandwidth control",* Quality of Service (QoS) functions are configured.

***Network switch –> Queue priority mapping***



Queue priotiry mapping

QoS 802.1p priority settings

| 802.1p | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| Queue | 1 | 0 | 0 | 1 | 2 | 2 | 3 | 3 |

Diffserv queue mapping

| Diffserv | Queue | Diffserv | Queue | Diffserv | Queue | Diffserv | Queue |
|---|---|---|---|---|---|---|---|
| 0x00 | 0 | 0x40 | 1 | 0x80 | 2 | 0xC0 | 3 |
| 0x04 | 0 | 0x44 | 1 | 0x84 | 2 | 0xC4 | 3 |
| 0x08 | 0 | 0x48 | 1 | 0x88 | 2 | 0xC8 | 3 |
| 0x0C | 0 | 0x4C | 1 | 0x8C | 2 | 0xCC | 3 |
| 0x10 | 0 | 0x50 | 1 | 0x90 | 2 | 0xD0 | 3 |
| 0x14 | 0 | 0x54 | 1 | 0x94 | 2 | 0xD4 | 3 |
| 0x18 | 0 | 0x58 | 1 | 0x98 | 2 | 0xD8 | 3 |
| 0x1C | 0 | 0x5C | 1 | 0x9C | 2 | 0xDC | 3 |
| 0x20 | 0 | 0x60 | 1 | 0xA0 | 2 | 0xE0 | 3 |
| 0x24 | 0 | 0x64 | 1 | 0xA4 | 2 | 0xE4 | 3 |
| 0x28 | 0 | 0x68 | 1 | 0xA8 | 2 | 0xE8 | 3 |
| 0x2C | 0 | 0x6C | 1 | 0xAC | 2 | 0xEC | 3 |
| 0x30 | 0 | 0x70 | 1 | 0xB0 | 2 | 0xF0 | 3 |
| 0x34 | 0 | 0x74 | 1 | 0xB4 | 2 | 0xF4 | 3 |
| 0x38 | 0 | 0x78 | 1 | 0xB8 | 2 | 0xF8 | 3 |
| 0x3C | 0 | 0x7C | 1 | 0xBC | 2 | 0xFC | 3 |

- *QoS 802.1p priority settings*—allows distributing packets into queues depending on the 802.1p priority.
    - *802.1p* — 802.1p priority value;
    - *Queue* — egress queue number.
- *Diffserv queue mapping* — allows distributing packets into queues depending on the IP diffserv priority.
    - *diffserv* — IP diffserv priority value;
    - *Queue* — egress queue number.

- *Apply* — apply defined settings;
- *Confirm* — confirm modified settings;

**Click *'Confirm'* button in 1-minute interval to confirm settings, or the previous values will be restored.**

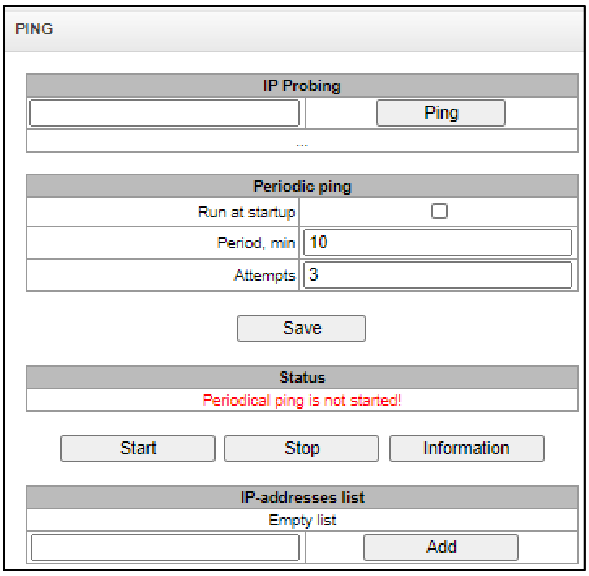
- *Default* — set default settings;
- *Save* — save settings into the device flash memory without applying them.

### 4.1.7 ***Network utilities:***

#### ***4.1.7.1 PING***

This utility is used for device network connection (route presence) check.

***Network utilities –> PING***



Run at startup □

Period, min 10

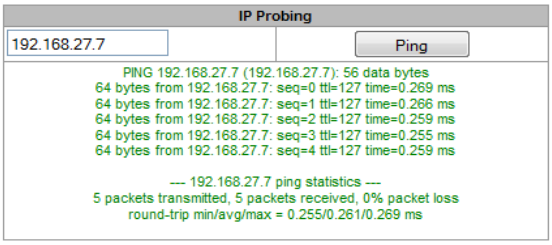
Attempts 3

Periodical ping is not started!

Empty list

***IP Probing —*** used for a single-time device network connection control.

To send an echo request (*Ping),* enter host IP address or network name in the *'IP probing'* field and click the *'Ping' button.* Command execution result will be shown in the lower part of the page. The result contains the quantity of transmitted packets, quantity of received responses to those packets, percentage of lost packets, and reception/transmission time (minimum/average/maximum) in milliseconds.



192.168.27.7

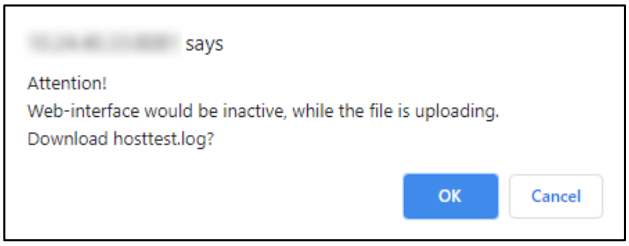
```
PING 192.168.27.7 (192.168.27.7): 56 data bytes
64 bytes from 192.168.27.7: seq=0 ttl=127 time=0.269 ms
64 bytes from 192.168.27.7: seq=1 ttl=127 time=0.266 ms
64 bytes from 192.168.27.7: seq=2 ttl=127 time=0.259 ms
64 bytes from 192.168.27.7: seq=3 ttl=127 time=0.255 ms
64 bytes from 192.168.27.7: seq=4 ttl=127 time=0.259 ms

--- 192.168.27.7 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.255/0.261/0.269 ms
```

***Periodic ping*** **—** used for periodic device network connection control.

- *Run at startup* — when set, ping requests to the addresses in the host list will be activated immediately after the device is started;
- *Period, min* — a time interval between requests in minutes;
- *Attempts* — a number of attempts to send a ping request.

***Status***

- *Start* — launch/restart periodic ping;
- *Stop*— forcibly stop periodic ping.
- *Information* — click this button to view the log file '/tmp/log/hosttest.log'that contains data on the last periodic ping attempt.



[redacted] says

Attention!
Web-interface would be inactive, while the file is uploading.
Download hosttest.log?

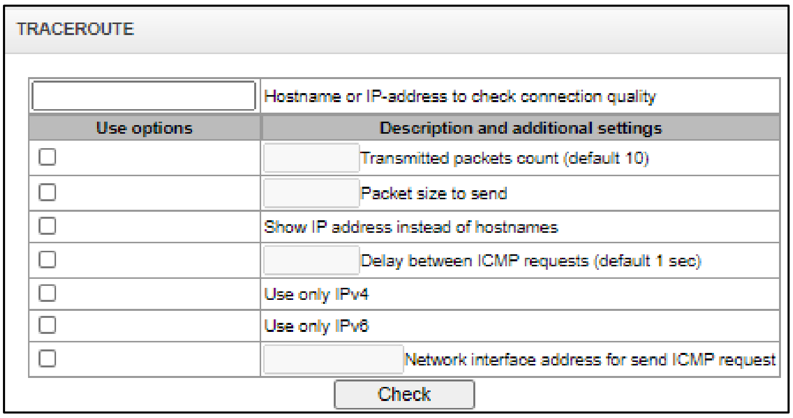
***IP-addresses list*** **—** a list of IP addresses that periodic ping requests will be sent to.

To add a new address to the list, select it in the entry field and click the *'Add' button.* To remove an address, click *«Remove»* button next to the required address.

### *4.1.7.2 TRACEROUTE*

The **TRACEROUTE** utility performs the route tracing function and ping tests to monitor the network. This function allows evaluating the connection quality for the tested node.

***Network utilities –> TRACEROUTE***



TRACEROUTE

| | |
|---|---|
| | Hostname or IP-address to check connection quality |
| **Use options** | **Description and additional settings** |
| □ | Transmitted packets count (default 10) |
| □ | Packet size to send |
| □ | Show IP address instead of hostnames |
| □ | Delay between ICMP requests (default 1 sec) |
| □ | Use only IPv4 |
| □ | Use only IPv6 |
| □ | Network interface address for send ICMP request |

In the *«Host name or IP address to test connection quality»* field, enter the IP address of the network device to test the connection quality. To use the options, select the checkboxes in the corresponding line.

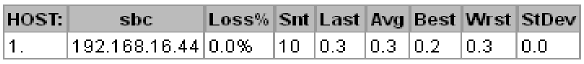
**Options:**

- *Transmitted packets count* — the number of the ICMP request transfer cycles;
- *Packet size to send* — the ICMP packet size in bytes;
- *Show IP address instead of host names* — do not use DNS. Display the IP address without trying to obtain their network names;
- *Delay between ICMP requests (default 1 sec)* — polling interval;
- *Use only IPv4* — use only IPv4 protocol;
- *Use IPv6 only* — use only IPv6 protocol;
- *Network interface address to send ICMP request* — IP address of the network interface from which ICMP requests will be sent.

After entering the IP address of the network device for which the connection quality and setting the options are evaluated, click the *«Check»* button.

As a result, the utility displays a table containing:

- *the node number and its IP address (or network name)*
- *the percentage of packets lost (Loss%)*
- *the number of packets sent (Snt)*
- *the round-trip time of the last packet (Last)*
- *average round-trip time of the packet (Avg)*
- *the best round-trip time of the packet (Best)*
- *the worst time round-trip time of the packet (Wrst)*
- *the standard deviation of delays for each node (StDev)*



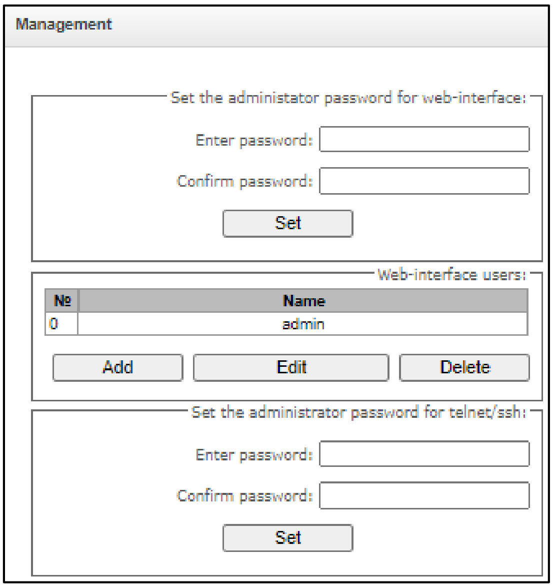
| HOST: | sbc | Loss% | Snt | Last | Avg | Best | Wrst | StDev |
|---|---|---|---|---|---|---|---|---|
| 1. | 192.168.16.44 | 0.0% | 10 | 0.3 | 0.3 | 0.2 | 0.3 | 0.0 |

## 4.1.8 *Security*

### ***4.1.8.1 Management***

In this submenu, the passwords for access to SBC configuration tools are changed.

***Security –> Management***



| № | Name |
|---|---|
| 0 | admin |

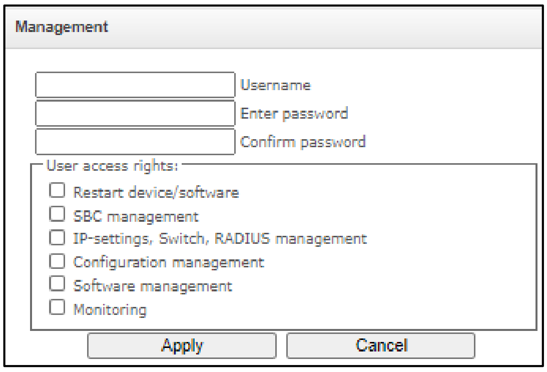
In the section *«Set the administrator password for web interface»,* a password to access the web interface of the *admin* user is set.

**By default, the login *admin* and password *rootpasswd* are used to access the web interface.**

**The password for *admin* user access via the web interface may not be the same as the password for Telnet, SSH access.**

In the section *«Web interface users»,* web interface users are created and their rights are assigned. Up to 10 users can be created.

To create a user, click *«Add»*. In the window (on the right), select a username, a password and confirm the password. Then specify user rights and click *«Apply»*. To edit, select a user from the list and press the *«Edit»* button. Deletion is done by selecting the user and pressing the *«Delete»* button.



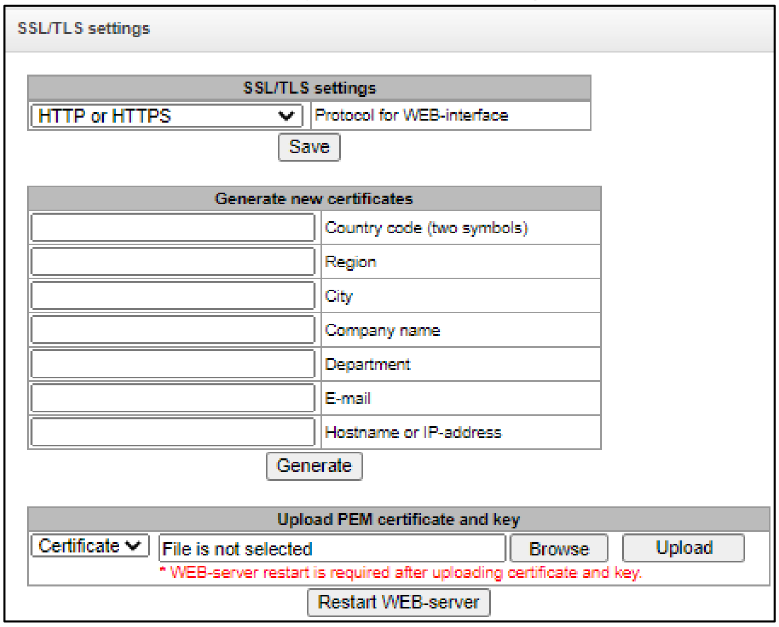
**Unable to delete or change *admin* user rights.**

In the section *«Set the administrator password for telnet/ssh»*, the *admin* user password for CLI access is set.

#### 4.1.8.2 SSL/TLS configuration

This section is intended for downloading or creating a self-signed SSL/TLS certificate that allows using an encrypted connection to the gateway and uploading/downloading configuration files via HTTPS.

***Security –> SSL/TLS settings***



SSL/TLS settings

| SSL/TLS settings | |
|---|---|
| HTTP or HTTPS | Protocol for WEB-interface |

Save

| Generate new certificates | |
|---|---|
| | Country code (two symbols) |
| | Region |
| | City |
| | Company name |
| | Department |
| | E-mail |
| | Hostname or IP-address |

Generate

Upload PEM certificate and key

Certificate | File is not selected | Browse | Upload

* WEB-server restart is required after uploading certificate and key.

Restart WEB-server

– *Protocol for WEB-interface* — the mode for connection to the web configurator:

- *HTTP or HTTPS* — both unencrypted HTTP and encrypted HTTPS connections are allowed. At that, connection via HTTPS is possible only when a generated certificate is present.
- *HTTPS only* — only encrypted connection via HTTPS is allowed. Connection via HTTPS is possible only when a generated certificate is present*;*

***Generate new certificates***

**These parameters should contain Latin characters only.**

– *Country code* — country code (for Russia — RU);
– *Region* — the name of a region, province, territory, republic, etc;
– *City* — city name;
– *Company name* — organization name;
– *Department* — the name of the unit or department;
– *E-mail* — e-mail address;
– *Hostname or IP address* — the IP address of the gateway.

***Upload PEM certificate and key***

The section allows you to download a pre-generated and signed PEM certificate and key. To upload, select the type of file to upload from the drop-down menu. Press the *«Browse»* button and select the required file. Then press the *«Download»* button.

**Once the certificate and key have been downloaded, the web server will need to be restarted using the «Restart web server» button.**

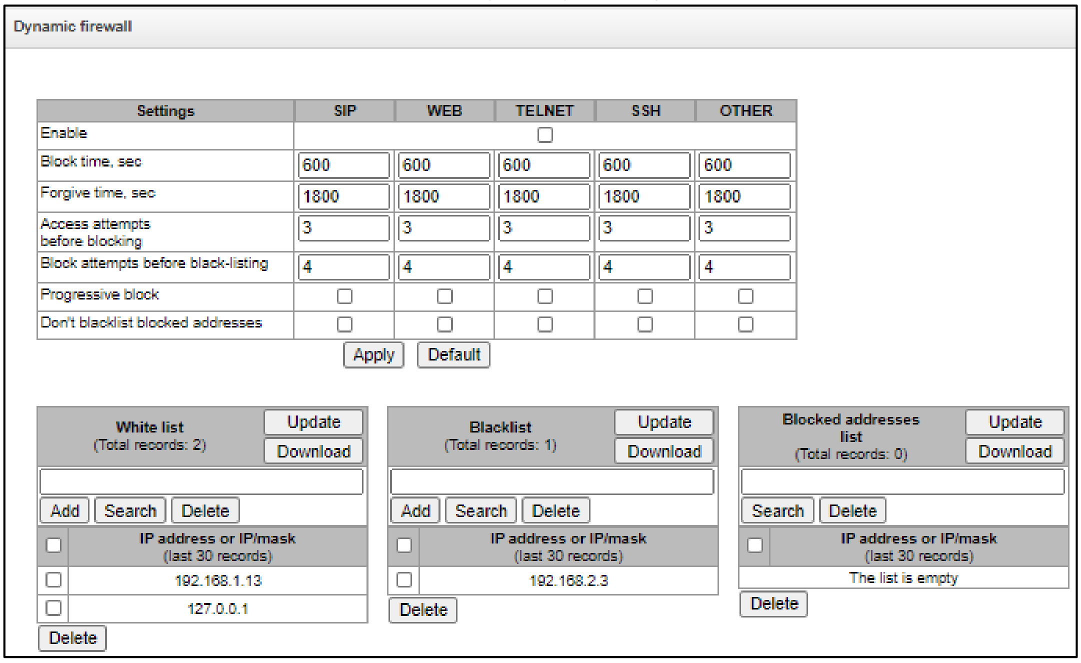
#### 4.1.8.3 Dynamic firewall

**Dynamic firewall** — a utility that tracks attempts of access to various services. When constantly repeated unsuccessful access attempts from the same IP address/host are discovered, the dynamic firewall blocks all further access attempts from this IP address/host.

The following actions may be identified as an unsuccessful access attempt:

- bruteforcing web interface or SSH authentication data, i.e. attempts to log in to the management interface using a wrong login or password;
- authentication data matching — accepting REGISTER requests from a known IP address, but with incorrect authentication data;
- receiving requests (REGISTER, INIVITE, SUBSCRIBE, etc.) from an unknown IP address;
- accepting unknown requests via a SIP port;
- the call falls under a rule with reject policy.

***Security –> Dynamic firewall***



| Settings | SIP | WEB | TELNET | SSH | OTHER |
|---|---|---|---|---|---|
| Enable | | | ☐ | | |
| Block time, sec | 600 | 600 | 600 | 600 | 600 |
| Forgive time, sec | 1800 | 1800 | 1800 | 1800 | 1800 |
| Access attempts before blocking | 3 | 3 | 3 | 3 | 3 |
| Block attempts before black-listing | 4 | 4 | 4 | 4 | 4 |
| Progressive block | ☐ | ☐ | ☐ | ☐ | ☐ |
| Don't blacklist blocked addresses | ☐ | ☐ | ☐ | ☐ | ☐ |

White list (Total records: 2)

| ☐ | IP address or IP/mask (last 30 records) |
|---|---|
| ☐ | 192.168.1.13 |
| ☐ | 127.0.0.1 |

Blacklist (Total records: 1)

| ☐ | IP address or IP/mask (last 30 records) |
|---|---|
| ☐ | 192.168.2.3 |

Blocked addresses list (Total records: 0)

| ☐ | IP address or IP/mask (last 30 records) |
|---|---|
| | The list is empty |

***Dynamic firewall parameters***

- *Enable* — enable a firewall;

The following parameters can be configured separately for different services. All these parameters can be reset to default values using the «Default» button.

- *Block time, sec* — time in seconds during which access from the suspicious address will be blocked;
- *Forgive time, sec* — time after which the address from which a suspicious request came will be forgotten if it has never been blocked;
- *Access attempts before blocking* — the maximum number of unsuccessful attempts to access the service before the host is blocked;
- *Block attempts before black-listing* — the number of blockages after which a problem address will be forcibly blacklisted;
- *Progressive block* — when this flag is set, each subsequent address block will be twice as large as the previous one, twice as few access attempts will be used to block the address. For example, the first time the address was blocked for 30 seconds after 16 attempts, the second time – for 60 seconds after 8 attempts, the third time – for 120 seconds after 4 attempts and so on;
- *Don't blacklist blocked addresses* — when set, SBC does not send blocked addresses to the blacklist, the «Progressive Block» option is ignored.

**White list (last 30 entries) —** a list of IP addresses and subnets that cannot be blocked by the dynamic firewall. Up to 4096 entries can be created.

**Blacklist (last 30 entries) —** a list of permanently blocked addresses. Up to 8192 records can be created for SBC-1000 and 16384 records for SBC-2000.

To add/search/remove an address from the list, select it in the input field and click *«Add»/«Search»/«Delete»* button.

**The black list takes precedence over the white list.**

**Blocked addresses list** — a list of addresses banned by a dynamic firewall. Up to 8192 records can be created for SBC-1000 and 16384 records for SBC-2000.

In the header of the lists, there are two buttons for downloading and updating them:

- *Download* — the web interface only displays the last 30 entries of the file. Clicking this button allows downloading full lists to your computer;
- *Update* — update a displayed list.

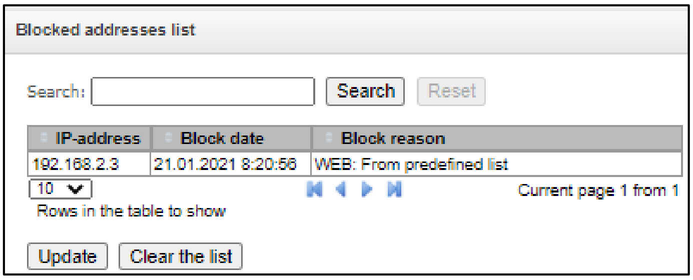
To add/search for an address in the list, enter it in the input field and press the *«Add»/«Search»* button; to delete it, press the *«Delete»* button. It is allowed to specify both single IP address and subnet in CIDR notation: 192.0.2.0/24. When a subnet is deleted, single addresses and subnets included in that subnet will also be deleted.

To delete addresses, you can also select the required addresses using the checkboxes and click the *«Delete»* button below the list.

### *4.1.8.4 Blocked addresses list*

The submenu is used to view the log of addresses blocked by the dynamic firewall. In the menu, it is also possible to unblock certain addresses by deleting them from the list. The list contains up to 10000 entries.

***Security –> Blocked addresses list***



Blocked addresses list

Search: [ ] Search Reset

| IP-address | Block date | Block reason |
|---|---|---|
| 192.168.2.3 | 21.01.2021 8:20:56 | WEB: From predefined list |

10 Rows in the table to show    Current page 1 from 1

Update  Clear the list

- *Search* — in the field a filter to search for addresses is specified;
- *Search* — a button for selecting addresses from the list according to the filter;
- *Reset* — a button for filter reset;
- *Update* — update the information in the list;
- *Clear the list* — delete all entries from the blocked addresses list. This will clear the list, but will not remove addresses from the blocking; this must be done in the dynamic firewall configuration menu.

The list contains the following information:

- *IP address* — IP address that was blocked;
- *Block date* — date and time of IP address block;
- *Block reason* — an explanation of which service and why the address was blocked;

The Table below shows a list of blocking messages and the reasons for them.

Table 20 — Blocking messages

| Message in the list | Reason for the occurrence | SIP message |
|---|---|---|
| Request error: REGISTER failed : Resource limit overflow | Dynamic user registration limit reached | Response 403 |
| Request error: REGISTER failed : Unknown user or registration domain | Requesting the registration of an unknown user | Response 403 |
| Request error: REGISTER failed : Server doesn't allow a third party registration | Registration request with different To and From headings | Response 403 |
| Request error: REGISTER failed : Authentication is wrong | Incorrect login/password | Response 403 |
| Request error: REGISTER failed : Wrong de-registration | Attempted deregistration of an unregistered contact by a user | Response 200 |
| Request error: REGISTER failed : Request from disallowed IP | Attempting to register from an address other than an allowed address | Response 403 |
| Request error: INVITE failed : No registration before | A call attempt from a user who is known but whose contact has not been registered | Response 403 |
| Request error: INVITE failed : Registration is expired | A call attempt from a user who is known but whose contact registration has expired | Response 403 |
| Request error: INVITE failed : Authentication is wrong | Incoming call or registration failed to be authenticated | Response 403 |
| Request error: INVITE failed : Unknown original address | A call from an unknown destination | The call is forwarded to the mgapp, where a decision is made whether to allow or reject it |
| Request error: INVITE failed : RURI not for me | Unknown host name or address in RURI | Response 404 |
| Request error: BYE failed : Call/Transaction Does Not Exist | No dialogue found to accept the request | Response 481 |
| SIP: INVITE rejected by the rule id:name (%d:%s) : Forbidden — Blocked by SB | The call falls under a rule with reject policy | - |
| SSH: Too many requests from address | Failed SSH authentication attempts | - |
| WEB: Unknown user <%s> attempted to access : password '%s' | Failed WEB authentication attempts | - |
| ANY: Manually by cmd from other module or administrator | Blocking added via CLI or WEB by an administrator | - |

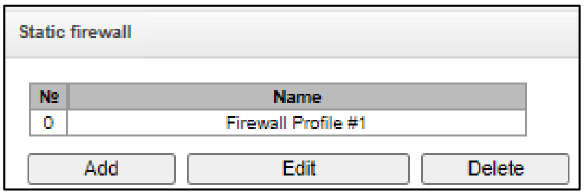
#### *4.1.8.5 Static firewall*

***Firewall*** is a package of software tools that allows for control and filtering of transmitted network packets in accordance with the defined rules in order to protect the device from unauthorised access. A device may have up to 32 profiles.

**Firewall rules will not work to restrict access via HTTP/HTTPS, SSH, Telnet, SNMP, FTP. To restrict access to these protocols, use the list of allowed IP addresses (section 4.1.8.6) and the settings for activating services on network interfaces (section 4.1.4.3).**

### Firewall profiles

***Security –> Static firewall***



Static firewall

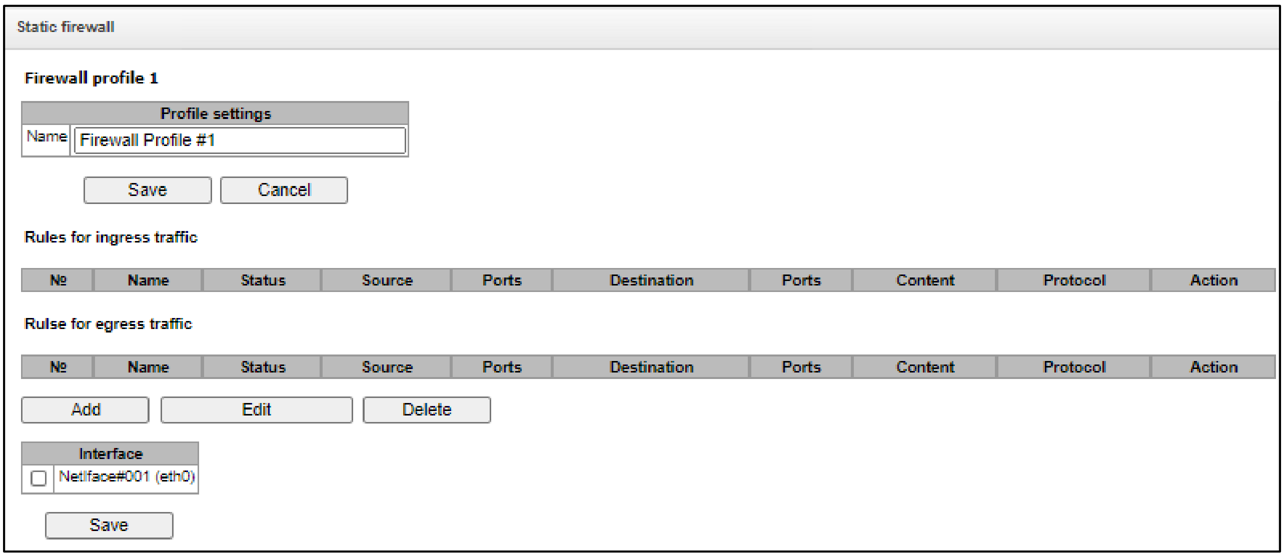
| № | Name |
|---|---|
| 0 | Firewall Profile #1 |

To create, edit or remove a firewall profile, use *«Objects» — «Add object», «Objects» — «Edit object»* and *«Objects» — «Remove object»* menus and the following buttons:

- *«Add»;*
- *«Edit»;*
- *"Delete"*.

Software allows you to configure firewall rules for incoming, outgoing and transit traffic as well as for specific network interfaces. The total number of firewall rules is the same for all profiles and is 1000 rules.

***Security –> Static firewall –> «Add»***



Static firewall

Firewall profile 1

| Profile settings | |
|---|---|
| Name | Firewall Profile #1 |

Rules for ingress traffic

| № | Name | Status | Source | Ports | Destination | Ports | Content | Protocol | Action |
|---|---|---|---|---|---|---|---|---|---|

Rulse for egress traffic

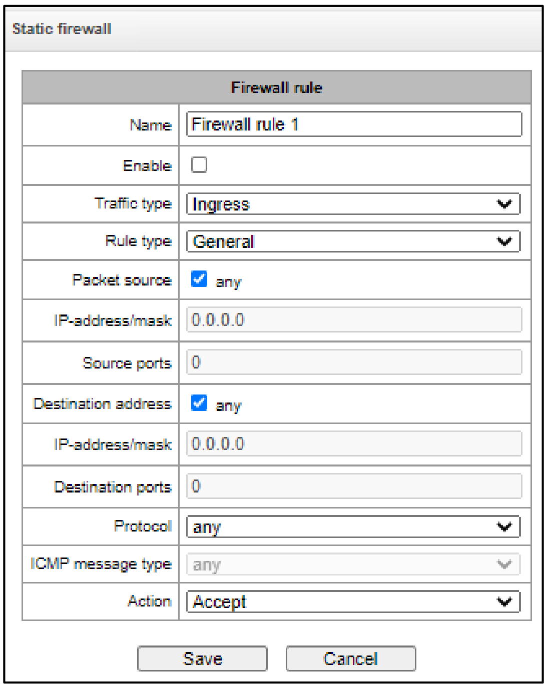
| № | Name | Status | Source | Ports | Destination | Ports | Content | Protocol | Action |
|---|---|---|---|---|---|---|---|---|---|

| Interface | |
|---|---|
| ☐ | Netiface#001 (eth0) |

When a rule is created, you should configure the following parameters:

- *Name* — rule name;
- *Enable* — defines whether the rule will be used. When unchecked, the rule will be inactive.
- *Traffic type* — type of traffic for the rule being created:
  - *Ingress* — intended for SBC;
  - *Egress* — transmitted by SBC;
- *Rule type* — may take values:
  - *General* — rule with IP and port verification;
  - *GeoIP* — rule with GeoIP address verification;
  - *String* — rule with a string occurrence in the package verification.

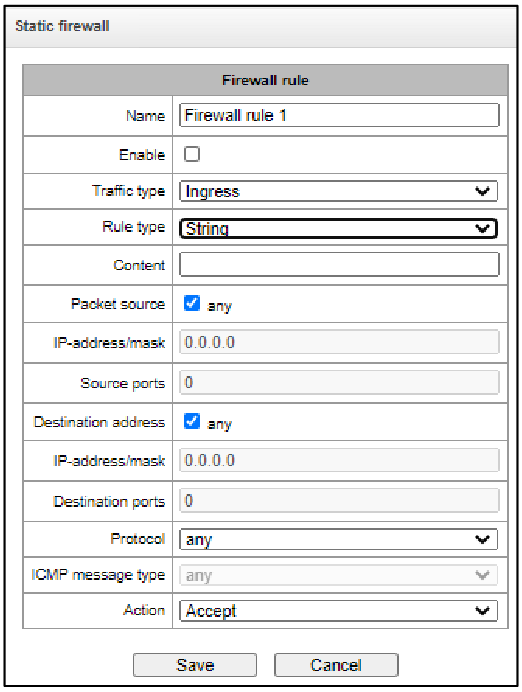
***Firewall rule menu depending on the type of rule selected***



Static firewall

Firewall rule

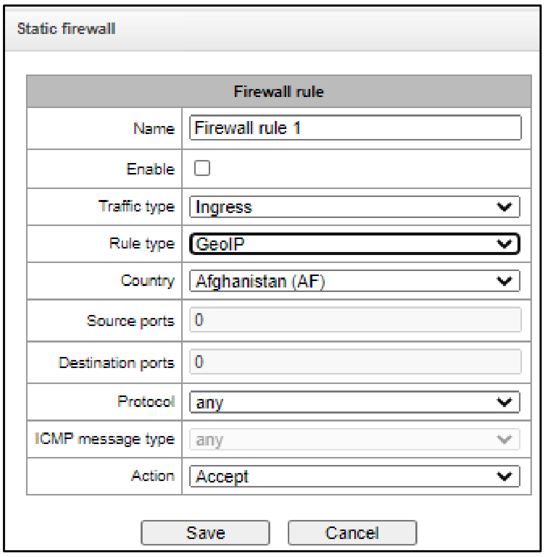
| | |
|---|---|
| Name | Firewall rule 1 |
| Enable | ☐ |
| Traffic type | Ingress |
| Rule type | General |
| Packet source | ☑ any |
| IP-address/mask | 0.0.0.0 |
| Source ports | 0 |
| Destination address | ☑ any |
| IP-address/mask | 0.0.0.0 |
| Destination ports | 0 |
| Protocol | any |
| ICMP message type | any |
| Action | Accept |



Static firewall

Firewall rule

| | |
|---|---|
| Name | Firewall rule 1 |
| Enable | ☐ |
| Traffic type | Ingress |
| Rule type | String |
| Content | |
| Packet source | ☑ any |
| IP-address/mask | 0.0.0.0 |
| Source ports | 0 |
| Destination address | ☑ any |
| IP-address/mask | 0.0.0.0 |
| Destination ports | 0 |
| Protocol | any |
| ICMP message type | any |
| Action | Accept |



Static firewall

Firewall rule

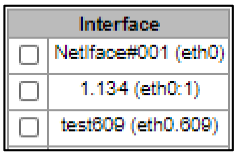
| | |
|---|---|
| Name | Firewall rule 1 |
| Enable | ☐ |
| Traffic type | Ingress |
| Rule type | GeoIP |
| Country | Afghanistan (AF) |
| Source ports | 0 |
| Destination ports | 0 |
| Protocol | any |
| ICMP message type | any |
| Action | Accept |

- *Packet source* — defines the packet source network address either for all addresses or a particular IP address or network:
  - *any* — for all addresses (checkbox is selected).
  - *IP address/mask* — for a particular IP address or network. Field is active when «any» checkbox is deselected. For a network, the mask is mandatory; for IP address, the mask is optional.
  - *Source ports* — packet source TCP/UDP port or port range (defined with a hyphen «-»). This parameter is used for TCP and UDP only; thus, select UDP, TCP, or TCP/UDP in the field in order to make this field active.
- *Destination address* — defines the packet recipient network address either for all addresses or a particular IP address or network:
  - *any* — for all addresses (checkbox is selected).
  - *IP address/mask* — for a particular IP address or network. Field is active when «any» checkbox is deselected. For a network, the mask is mandatory; for IP address, the mask is optional.
  - *Destination ports* — packet recipient TCP/UDP port or port range (defined with a hyphen «-»). This parameter is used for TCP and UDP only; thus, select UDP, TCP, or TCP/UDP in the field in order to make this field active.
- *Protocol* — protocol for which the rule will be used: UDP, TCP, ICMP or TCP/UDP;

- *ICMP message type* — ICMP message type that the rule will be used for. This field is active, when ICMP is selected in the *«Protocol»* field;
- *Action* — action executed by this rule:
  - *Accept* — packets falling under this rule will be accepted by the firewall;
  - *Drop* — packets falling under this rule will be rejected by the firewall without informing the party that has sent these packets;
  - *Reject* — packets falling under this rule will be rejected by the firewall; the party that has sent the packet will receive either TCP RST packet or «ICMP destination unreachable»;
- *Country* — country to which the address belongs. The field is displayed only for the «GeoIP» rule type;
- *Content* — text string that should be in the packet. The string will be searched by the contents of the packet, case-sensitive. The field is displayed only for the «String» rule type;

The created rule will be placed in the corresponding section: *«Rules for ingress traffic», «Rules for egress traffic»* or *«Rules for transit traffic»*.

Also, in the *firewall profile*, you may specify network interfaces that these profile rules will be applied to.



| | Interface |
|---|---|
| ☐ | NetIface#001 (eth0) |
| ☐ | 1.134 (eth0:1) |
| ☐ | test609 (eth0.609) |

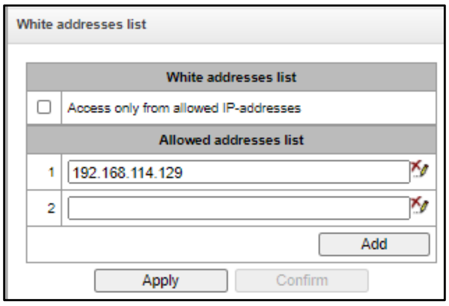
**Each network interface may be used only in a single firewall profile at a time. If you attempt to assign a network interface to a new profile, it will be removed from the previous one.**

To apply the rules, click *«Apply»* button that will appear when the changes are made into the firewall settings.

### *4.1.8.6 White addresses list*

In this section, you may configure the list of allowed IP addresses that the administrator may use for connection to the device via web configurator and Telnet/SSH protocol. By default, all addresses are allowed. Up to 255 addresses can be specified.

***Security –> White addresses list***



White addresses list

White addresses list

☐ Access only from allowed IP-addresses

Allowed addresses list

| | |
|---|---|
| 1 | 192.168.114.129 |
| 2 | |

- *Access only from allowed IP-addresses* — when checked, only addresses from the whitelist are allowed to access the device.

To add an address to the *«Allowed addresses list»* table, click *«Add»* and in the field that appears, specify the required value. After filling the list, click *«Apply»*.

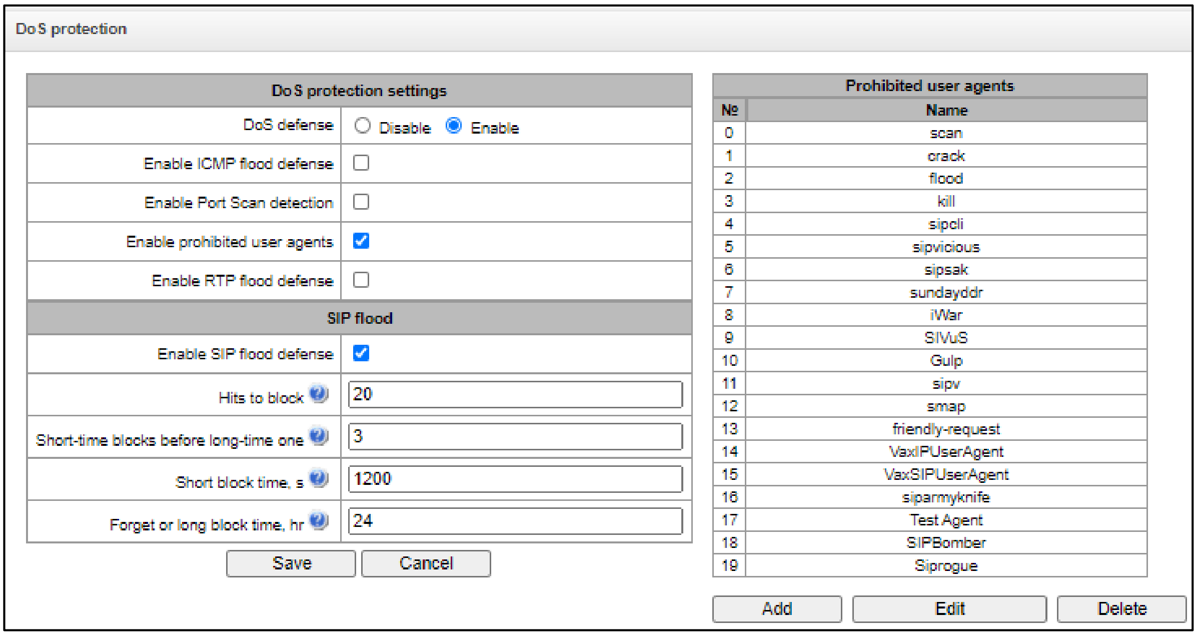
You can remove addresses from the list by clicking the icon (*«Delete»*) in the selected line.

**If you enable access only for allowed IP addresses without whitelisting your own IP address, access to the device will be lost.**

### 4.1.8.7 DoS protection

This menu is used to configure DoS protection settings.

***Security –> DoS protection***



DoS protection

| DoS protection settings | |
|---|---|
| DoS defense | ○ Disable ● Enable |
| Enable ICMP flood defense | □ |
| Enable Port Scan detection | □ |
| Enable prohibited user agents | ☑ |
| Enable RTP flood defense | □ |
| **SIP flood** | |
| Enable SIP flood defense | ☑ |
| Hits to block | 20 |
| Short-time blocks before long-time one | 3 |
| Short block time, s | 1200 |
| Forget or long block time, hr | 24 |

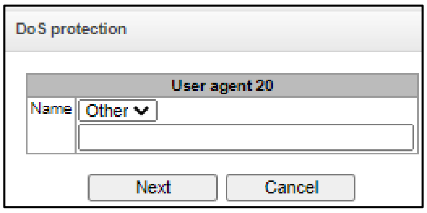
| Prohibited user agents | |
|---|---|
| № | Name |
| 0 | scan |
| 1 | crack |
| 2 | flood |
| 3 | kill |
| 4 | sipcli |
| 5 | sipvicious |
| 6 | sipsak |
| 7 | sundayddr |
| 8 | iWar |
| 9 | SIVuS |
| 10 | Gulp |
| 11 | sipv |
| 12 | smap |
| 13 | friendly-request |
| 14 | VaxIPUserAgent |
| 15 | VaxSIPUserAgent |
| 16 | siparmyknife |
| 17 | Test Agent |
| 18 | SIPBomber |
| 19 | Siprogue |

On SBC, the following attacks are countered:

- *ICMP flood* — attack with multiple ICMP requests;
- *Port Scan* — port scanning;
- *SIP flood* — attacks via SIP in order to brute-force user passwords, flooding with requests to forbidden direction, protection against scanning actual numbers;
- *RTP flood* — flooding on ports used to transmit media data in order to degrade the quality of service;
- *User-Agent filtering* — SBC contains a forbidden list of standard User-Agents of different utilities, which can be used for SIP attacks. Search by User-Agent is not case-sensitive.

DoS protection settings:

- *DoS defense* — general setting that activates all other protections;
- *Enable ICMP flood defense* — when activated, the SBC will not respond to ICMP type 8 (echo) and ICMP type 13 (timestamp) requests;
- *Enable Port Scan detection* — this mode checks for too frequent requests to different ports from the same address;
- *Enable prohibited user agents* — filtering SIP requests by User-Agent. When you activate this option, a list of banned User-Agents will appear on the right. On this list you can:
  - Add a new User-Agent with the «Add» button. A window will appear where you can select either one of the preset options or enter your own by selecting «other» from the drop-down list;
  - Change any position in the list. To do this, select the position and click «Edit»;
  - Remove any position from the list. To do this, select the position and click «Delete».



DoS protection

User agent 20

Name: Other

- *Enable RTP flood defense* — activates detection of hosts sending voice traffic to inactive media ports, or to media ports that are already in use for voice communications. A host is considered a flooder if it sends unwanted traffic for more than five seconds.

**SIP flood**

- *Enable SIP flood defense* — protection against brute-forcing user passwords and flooding with requests to the forbidden direction.
- *Hits to block* — after exceeding the number of attempts, the user will be blocked. You can set from 1 to 32 attempts;
- *Short-time blocks before long-time one* — the number of temporary blocks that will be applied to the user. Once this limit is exceeded, long-time blocking will be applied. You can set from 1 to 10 blocks;
- *Short block time, s* — subscriber blocking time, can be from 600 to 3600 seconds;
- *Forget or long block time, hr* — long block time. This is also the forgiveness time — after which the access attempts counter will be reset. You can set from 12 to 48 hours.

### *4.1.8.8 SBC network protection operation scheme*

The following order of dynamic and static firewall rules, list of forbidden addresses and access restriction from network interfaces works on SMG:

1. The dynamic firewall rules are worked out (section 4.1.8.3). This step resets requests from addresses that are on the blacklist and temporary block list;

2. The access restrictions configured in the Network interfaces -> Services4.1.4.3 and White addresses list4.1.8.6 sections are worked out. When the list of allowed IP addresses is inactive, rules are generated that allow management access to the addresses of SMG network interfaces that have access permission in the «Services» block. When the list of allowed IP addresses is active, the rules are complemented by the source IP address control — only connections from addresses specified in the list are allowed;

3. The rules of SIP destination protection are worked out (section 4.1.3.2). Protection rules for SIP destination are formed automatically. By default, it is checked that the UDP can only be accessed from a specified remote address and port. For TCP (and for UDP with the «Ignore source port for incoming calls» option) only the remote address is checked. If the «Allow redirection» option is set, the remote address is not controlled — you should use a static firewall to limit access;

4. Allow other access to network interfaces that do not have static firewall rules bound to them;

5. The static firewall rules (section 4.1.8.5) are worked out on those network interfaces to which the rules are bound.

**If one of the list rules worked, the remaining rules will not be applied to the request.**

### *4.1.8.9 Providing typical SBC network protection tasks*

**Restrict management access via WEB/Telnet/SSH/SNMP protocols.**

To restrict management access, use the settings in Network Interfaces -> Services 4.1.4.3 and White addresses list 4.1.8.6. First, on the network interfaces where it is necessary to grant access, you set the flags of the protocols that you want to grant access. This will expose the destination address restriction. After that, the list of allowed IP addresses is configured, which will additionally limit the source address to the addresses from the list.

**Restrict access to SIP interfaces to specific addresses and/or geographic locations.**

By default, SIP destination security rules are created automatically. However, when the «Allow redirects» option is checked, no rules will be created. In addition, rules are not automatically created for a SIP trunk. To protect a SIP trunk, you need to configure static firewall (section 4.1.8.5).

Example of configuring access with these restrictions:

- Allow access from Russia;
- Allow access from subnet 34.192.128.128/28;
- Restrict access from other addresses.

To do this, create three static firewall rules in the following order:

1. A rule for ingress traffic with «GeoIP» type and «Russian Federation (RU)» country. Action — Accept;
2. A rule for ingress traffic with «Normal» type and IP address and source mask «34.92.128.128/255.255.255.240». Action — Accept;
3. A rule for ingress traffic with «Normal» type and packet source «Any». Action — Drop;

After that, select the desired network interfaces in the list of interfaces and save the settings.

**Full restriction of access to SMG from a certain address or subnet.**

Such a restriction can be implemented by activating the dynamic firewall (section 4.1.3.2) and blacklisting the address or subnet. Note — if there are too many addresses, it is better to go backwards and create static firewall rules (section 4.1.8.5) on the principle of «allow connections to trusted nodes first, then discard everything» and restrict access through the list of allowed IP addresses (section 4.1.8.6);

**Automatic blocking of unsuccessful requests/authorizations**

Performed by the dynamic firewall (section 4.1.3.2). You should enable the dynamic firewall and configure the triggering conditions. It is also recommended to whitelist those addresses and subnets to which the automatic blocking rules should not be applied.

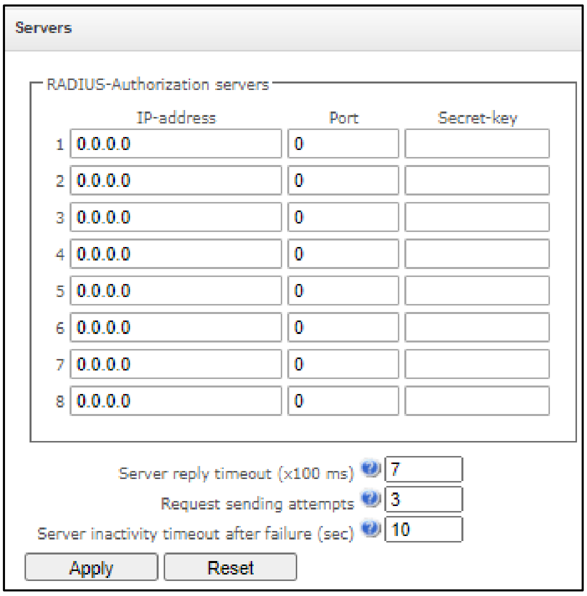
## 4.1.9 *RADIUS configuration*

The gateway supports authentication of subscribers registering through it and call authorization using a RADIUS server. When using RFC5090 parameters for digest authentication (in the ACCESS-CHALLENGE message) the gateway receives from the RADIUS server and forwards them to the subscriber. When using RFC5090-no-challenge or Draft Sterman, the gateway sends parameters for digest authentication to the subscriber, then these parameters and the digest response received from the subscriber, passes to the RADIUS server for verification.

To use authorization using RADIUS server, you must set the desired RADIUS profile in the direction settings for SIP-users (section SIP Destination).

### *4.1.9.1 Servers*

***RADIUS –> Servers***



Servers

RADIUS-Authorization servers

| | IP-address | Port | Secret-key |
|---|---|---|---|
| 1 | 0.0.0.0 | 0 | |
| 2 | 0.0.0.0 | 0 | |
| 3 | 0.0.0.0 | 0 | |
| 4 | 0.0.0.0 | 0 | |
| 5 | 0.0.0.0 | 0 | |
| 6 | 0.0.0.0 | 0 | |
| 7 | 0.0.0.0 | 0 | |
| 8 | 0.0.0.0 | 0 | |

Server reply timeout (x100 ms) 7
Request sending attempts 3
Server inactivity timeout after failure (sec) 10

The device supports up to 8 authorization servers.

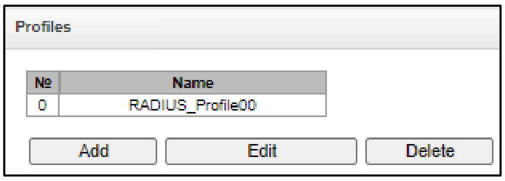
- *Server reply timeout* — the time for which the server is expected to respond;
- *Request sending attempts* — the number of times the request to the server is repeated. If all attempts are unsuccessful, the server is considered inactive and the request is redirected to another server, if specified, otherwise an error is detected;
- *Server inactivity timeout after failure* — time during which the server is considered inactive (no requests are sent to it).

#### *4.1.9.2 Profiles*

***RADIUS –> Profiles***

Up to 32 profiles can be created. To create, edit or remove a RADIUS profile, use *«Objects» — «Add object», «Objects» — «Edit object»* and *«Objects» — «Remove object»* menus and the following buttons:

- *«Add»;*
- *«Edit»;*
- *"Delete*".



| № | Name |
|---|---|
| 0 | RADIUS_Profile00 |

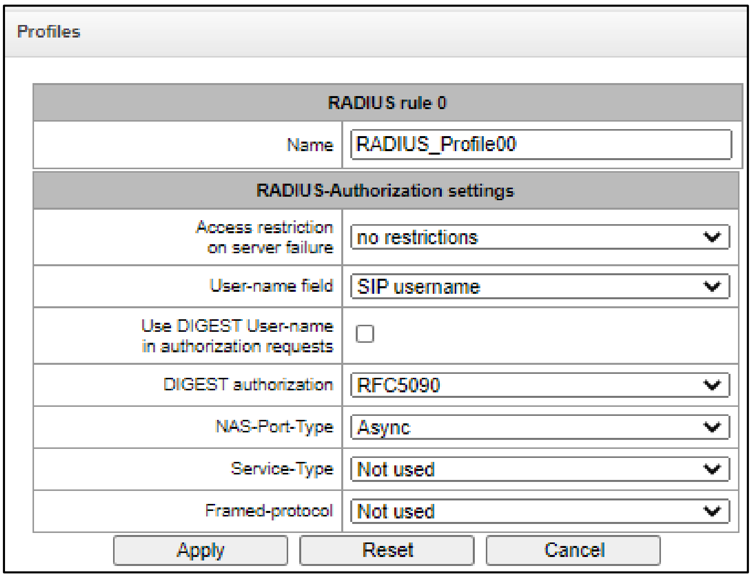
***RADIUS –> Profiles –> «Add»***

**RADIUS rule N**

- *Name* — profile name;

**RADIUS- Authorization settings:**

- *Access restriction on server failure* — If the server fails (no response from the server), it is possible to set restrictions on egress communication:
  - *no restrictions* — allow all calls;
  - *deny all* — deny all calls.
- *User-name field* — select the value of the User-Name attribute in the corresponding Access Request (RADIUS-Authorization) package:
  - *SIP username* — use the caller phone number (username from the from field) as the value;
  - *IP address* — use the caller IP address as the value;
  - *SIP interface name* — use the name of the SIP-server through which the incoming occupation is performed as the value.
- *Use DIGEST User-name in authorization requests* — select the algorithm of subscriber authorization through the RADIUS server. With digest authentication, the password is not transmitted in plaintext, as with basic authentication, but as a hash code and cannot be intercepted when traffic is scanned*:*
  - *RFC5090* — full RFC5090 recommendation implementation;
  - *RFC5090-no-challenge* — operate with the server not transmitting the Access Challenge;
  - *Draft-sterman (NetUp, FreeRadius)* — draft operation, on the basis of which recommendation RFC5090 was written);
- *NAS-Port-Type* — type of physical NAS port (the server where the user is authenticated), Async is default;
- *Service-Type* — service type, not used by default;
- *Framed-protocol* — protocol, specified when using packet access, not used by default.



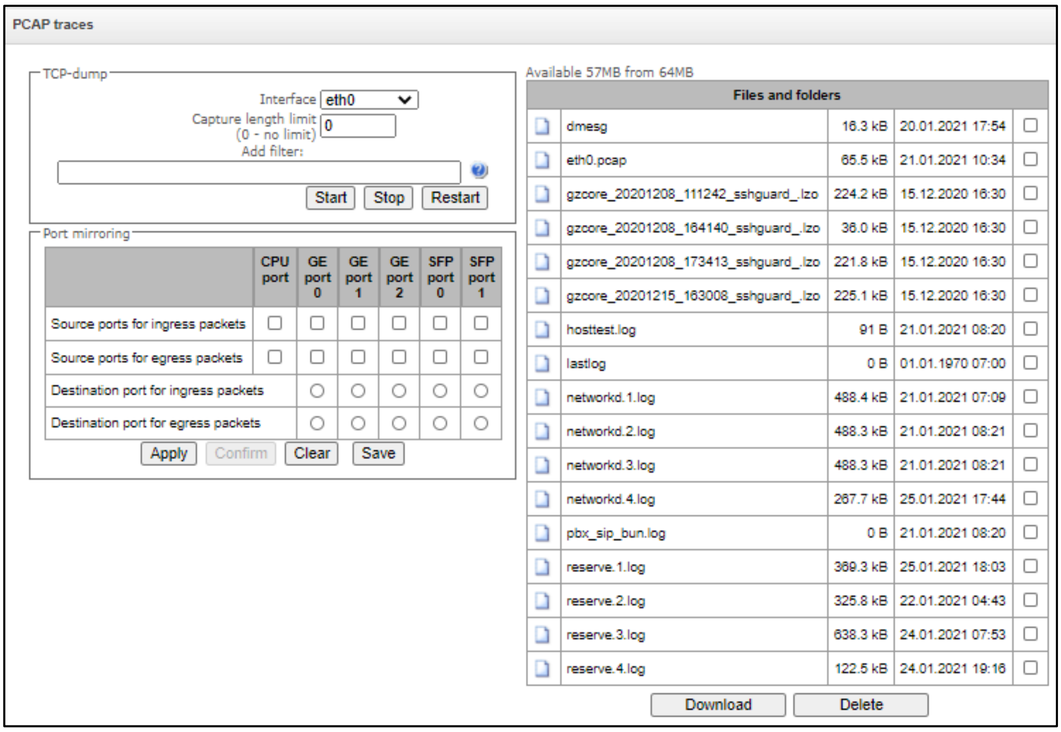
| RADIUS rule 0 | |
|---|---|
| Name | RADIUS_Profile00 |
| **RADIUS-Authorization settings** | |
| Access restriction on server failure | no restrictions |
| User-name field | SIP username |
| Use DIGEST User-name in authorization requests | □ |
| DIGEST authorization | RFC5090 |
| NAS-Port-Type | Async |
| Service-Type | Not used |
| Framed-protocol | Not used |

## 4.1.10 *Traces*

### *4.1.10.1 PCAP traces*

The menu is used to configure parameters for network traffic analysis and TDM network protocols.

***Traces –> PCAP traces***



PCAP traces

TCP-dump

Interface: eth0

Capture length limit (0 - no limit): 0

Add filter:

Port mirroring

| | CPU port | GE port 0 | GE port 1 | GE port 2 | SFP port 0 | SFP port 1 |
|---|---|---|---|---|---|---|
| Source ports for ingress packets | □ | □ | □ | □ | □ | □ |
| Source ports for egress packets | □ | □ | □ | □ | □ | □ |
| Destination port for ingress packets | | ○ | ○ | ○ | ○ | ○ |
| Destination port for egress packets | | ○ | ○ | ○ | ○ | ○ |

Available 57MB from 64MB

| Files and folders | | | |
|---|---|---|---|
| dmesg | 16.3 kB | 20.01.2021 17:54 | □ |
| eth0.pcap | 65.5 kB | 21.01.2021 10:34 | □ |
| gzcore_20201208_111242_sshguard_.lzo | 224.2 kB | 15.12.2020 16:30 | □ |
| gzcore_20201208_164140_sshguard_.lzo | 36.0 kB | 15.12.2020 16:30 | □ |
| gzcore_20201208_173413_sshguard_.lzo | 221.8 kB | 15.12.2020 16:30 | □ |
| gzcore_20201215_163008_sshguard_.lzo | 225.1 kB | 15.12.2020 16:30 | □ |
| hosttest.log | 91 B | 21.01.2021 08:20 | □ |
| lastlog | 0 B | 01.01.1970 07:00 | □ |
| networkd.1.log | 488.4 kB | 21.01.2021 07:09 | □ |
| networkd.2.log | 488.3 kB | 21.01.2021 08:21 | □ |
| networkd.3.log | 488.3 kB | 21.01.2021 08:21 | □ |
| networkd.4.log | 267.7 kB | 25.01.2021 17:44 | □ |
| pbx_sip_bun.log | 0 B | 21.01.2021 08:20 | □ |
| reserve.1.log | 369.3 kB | 25.01.2021 18:03 | □ |
| reserve.2.log | 325.8 kB | 22.01.2021 04:43 | □ |
| reserve.3.log | 638.3 kB | 24.01.2021 07:53 | □ |
| reserve.4.log | 122.5 kB | 24.01.2021 19:16 | □ |

***TCP-dump — TCP–dump utility settings:***

– *Interface* — interface for network traffic capture;
– *Capture length limit (0 — no limit)* — size limit for captured packets, in bytes;
– *Add filter* — packet filter for tcpdump utility.

***Structure of filter expressions***

Each expression that defines the filter includes a single or multiple primitives containing a single or multiple object identifiers and preceding qualifiers. Object identifier may be represented by its name or number.

***Object qualifiers***

1. **type** — indicates the object type specified by identifier. Object type may be represented by the following values:
   - **host**,
   - **net**,
   - **port**.

   If object type is not defined, **host** value will be assumed.

2. **dir** — defines the direction towards the object. The following values are supported:
   - **src** (the object is a sender),
   - **dst** (the object is a recipient),
   - **src or dst** (a sender or a recipient),
   - **src and dst** (a sender and a recipient).

   If **dir** qualifier is not defined, **src or dst** value will be assumed.

   For traffic interception from artificial interface **any**, qualifiers **inbound** and **outbound** may be used.

3. **proto** — defines the protocol that packets should belong to. This qualifier may take values: **ether**, **fddi1**, **tr2**, **wlan3**, **ip**, **ip6**, **arp**, **rarp**, **decnet**, **tcp** and **udp**.

   If the primitive does not contain protocol qualifier, it is assumed that all protocols compatible with object type comply with this filter.

In addition to objects and qualifiers, primitives may contain arithmetic expressions and keywords:

- **gateway**,
- **broadcast**,
- **less**,
- **greater**.

Complex filters may contain numerous primitives interconnected with logical operators **and**, **or**, and **not**. To reduce the expressions that define the filters, identical qualifier lists may be omitted.

**Filter examples**:

- **dst foo** — filters packets which IPv4/v6 recipient address field contains foo host address;
- **src net 128.3.0.0/16** — filters all Ipv4/v6 packets sent from the specific network;
- **ether broadcast** — enables filtering of all Ethernet broadcasting frames. Keyword 'ether' may be omitted.
- **ip6 multicast** — filters packets with IPv6 group addresses.

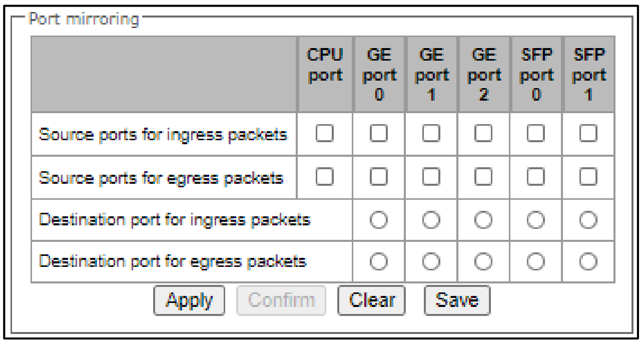
For detailed information on packet filtering, see specialized resources.

- *Start* — begin data collection;
- *Stop* — finish data collection;
- *Restart* — restart data collection.

**After stopping the packet capture, the right side of the file list will allow you to select to download the dump from the specified interface to the local computer.**

***Port mirroring*[1] *— traffic mirroring settings:***

Port mirroring enables copying of sent and received frames from the gateway switch ports and their forwarding to another port.



Port mirroring

| | CPU port | GE port 0 | GE port 1 | GE port 2 | SFP port 0 | SFP port 1 |
|---|---|---|---|---|---|---|
| Source ports for ingress packets | □ | □ | □ | □ | □ | □ |
| Source ports for egress packets | □ | □ | □ | □ | □ | □ |
| Destination port for ingress packets | | ○ | ○ | ○ | ○ | ○ |
| Destination port for egress packets | | ○ | ○ | ○ | ○ | ○ |

For device ports, available operations are as follows:

- *Source ports for ingress packets* — copy frames received from this port (source port);
- *Source ports for egress packets* — copy frames sent by this port (source port);
- *Destination port for ingress packets* — destination port for copied frames received by selected source ports;
- *Destination port for egress packets* — destination port for copied frames sent by selected source ports;

[1] Only for SBC-1000

*Apply* — apply mirroring setting parameters;
*Confirm* — confirm applied mirroring setting parameters;
*Clear* — reset mirroring settings;
*Save* — save mirroring setting parameters.

**Click *«Confirm»* button in 1-minute interval to confirm settings, or the previous values will be restored.**

The **«Files and folders»** block features the list of tracing files in the corresponding directory. SSD or RAM of the device can be used to save traces. If RAM is used, the recording is performed to the ***/tmp/log*** directory.

To download it to a local PC, select the checkboxes located next to the required filenames and click *«Download» button.* To delete the specific files from the directory, click *«Delete».*

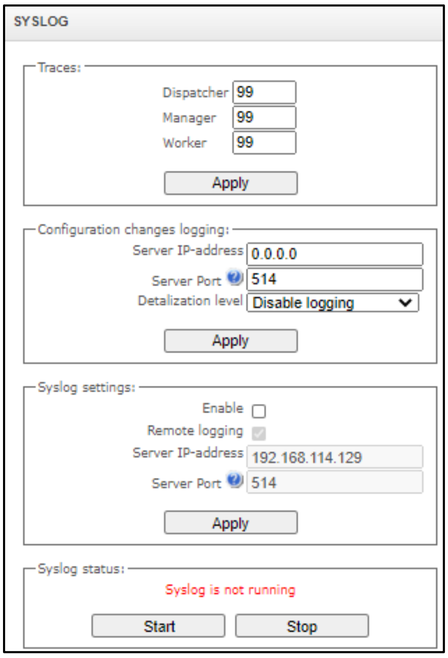
### *4.1.10.2 SYSLOG*

In *'SYSLOG'* menu, you may configure system log settings.

**SYSLOG** is a protocol designed for transmission of messages on current system events. Gateway software generates system data logs on operation of system applications and signalling protocols, as well as occurred failures and sends them to SYSLOG server.

**High debug levels may cause delays in operation of the device.**
**IT IS NOT RECOMMENDED to use system log without due cause.**

**System log should be used only when problems in gateway operation occur, and you have to identify the reason. To define the necessary debug levels, consult a Eltex Service Centre Specialist.**



SYSLOG

Traces:
Dispatcher 99
Manager 99
Worker 99
Apply

Configuration changes logging:
Server IP-address 0.0.0.0
Server Port 514
Detalization level Disable logging
Apply

Syslog settings:
Enable □
Remote logging ☑
Server IP-address 192.168.114.129
Server Port 514
Apply

Syslog status:
Syslog is not running
Start Stop

***Traces*** — allows saving the log of device components operation and interaction, as well as message exchange via various protocols.

In tracing parameters, you may configure tracing level for various events and protocols. Possible levels: 0 — off, 1-99 — on. 1 — minimum 99 — maximum level of debug.

- *Dispatcher* — process manager logging;
- *Manager* — logging of the connection manager and registrations, RTP traffic management;
- *Worker* — SIP adapter operation logging;

***Configuration changes logging —*** allows saving the history of the gateway setting changes.

- *Server IP-address* — server address to save the log of the entered commands;
- *Server Port* — the server port to save the log of the entered commands;
- *Detalization level* — verbosity level of the entered commands log:
  - *Disable logging* — disable entered commands logs generation;
  - *Standard* — messages contain the name of modified parameter;
  - *Extended* — messages contain the name of modified parameter as well as parameter values before and after the modification.

***Syslog settings*** — system log configuration settings for transmission of the device access events.

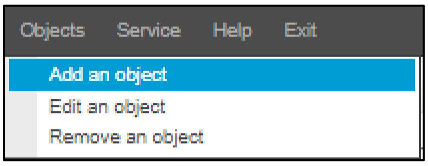
The syslog parameters configure the IP address of the syslog server, the UDP port on which the syslog server receives messages.

- *Enable* — enable event logging;
- *Remote logging* — when checked, the log will be saved on the server whose IP address is set below, otherwise the log will be saved to RAM (the size of the log is limited to 5 MB, in addition, log entries are saved only until you reboot the device). Saving the log to RAM is not recommended for use.
- *Server IP-address* — server address to save the event log;
- *Server Port* — the server port to save the event log;

The *«Start»* and *«Stop»* buttons allow you to start and stop the log transfer to the server respectively.

### 4.1.11 *Working with objects and 'Objects' menu*

In addition to create, edit and remove icons, you may use the corresponding 'Objects' menu items to perform different operations with objects.



### 4.1.12 *Saving configuration and 'Service' menu*

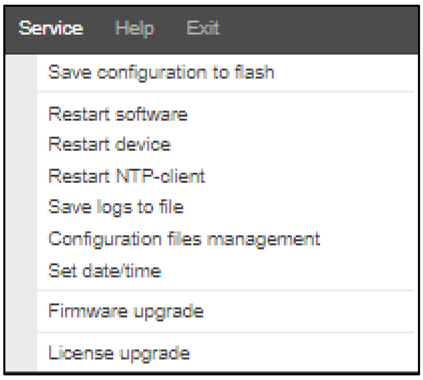
To discard all changes, select *«Service»—«Discard all changes»* menu.

To write the current configuration into non-volatile memory of the the device, select *«Service»—«Save configuration into flash»* menu.

To restart the device software, select *«Service»—«Restart software»* menu.

To restart the device completely, select *«Service»—«Restart device»* menu.

To perform forced time re-synchronization with NTP server, select *«Service»—«Restart NTP client»* menu.



To generate and save logs on the device, select the «Service»—«Save logs to file» menu. The archive with logs can be found under PCAP traces — files and folders in the tracing directory.

An example of the name of the archive:

*sbc_logs_current_calls_20201111_165508.tar.gz*

To forcibly restart the SSHD, select the menu *«Service» - «Restart SSHD[1]»*.

To read/write the main device configuration file, select the «*Service*» - *«Configuration files management»* menu.

To reset the device configuration, select the menu «*Service*» - *«Configuration files management»* and press the *«Reset»* button. This will reset all settings except for network parameters, network interfaces, network routes, firewall profiles and rules, white list and time server (NTP). For a complete factory reset, refer to the section 2.6.

To configure the device local date and time manually, select the *«Service» - «Set date/time»* menu; see Section 4.1.13 Time and date configuration.

To update the software via the web interface, select the menu *«Service» - «Firmware upgrade»*, see Section 4.1.14 Firmware update via web interface.

To update/add licenses, select *«Service»—«License update»* menu; see Section 4.1.15 Licenses.

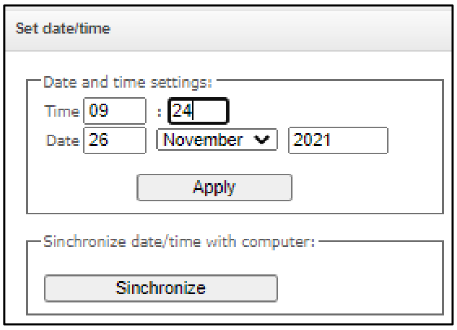
[1] Only for SBC-1000

### 4.1.13 *Time and date configuration*

In the respective fields, you may define the system time in HH:MM format and the date in DD.month.YYYY format.

To save settings, use «*Apply*» button.

Click «*Synchronize*» button to synchronize the device system time with the current time on a local PC.



Set date/time

Date and time settings:

Time 09 : 24

Date 26 November 2021

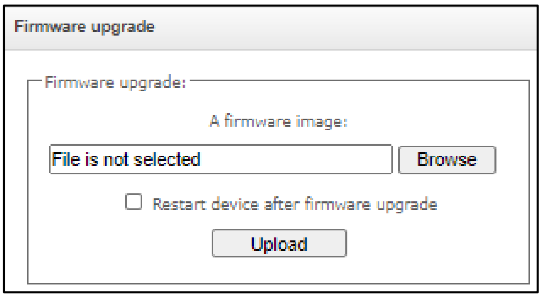
### 4.1.14 *Firmware update via web interface*

To update the device firmware, use *«Service» - «Firmware update»* menu.

A firmware file upload form will open.

– *Firmware upgrade* — update firmware and/or Linux kernel.

To update the firmware, specify the update file name in *«A firmware image»* field using *«Browse»* button and click *«Upload»*. When the operation is completed, restart the device using *«Service» - «Device restart»* menu.



Firmware upgrade

Firmware upgrade:

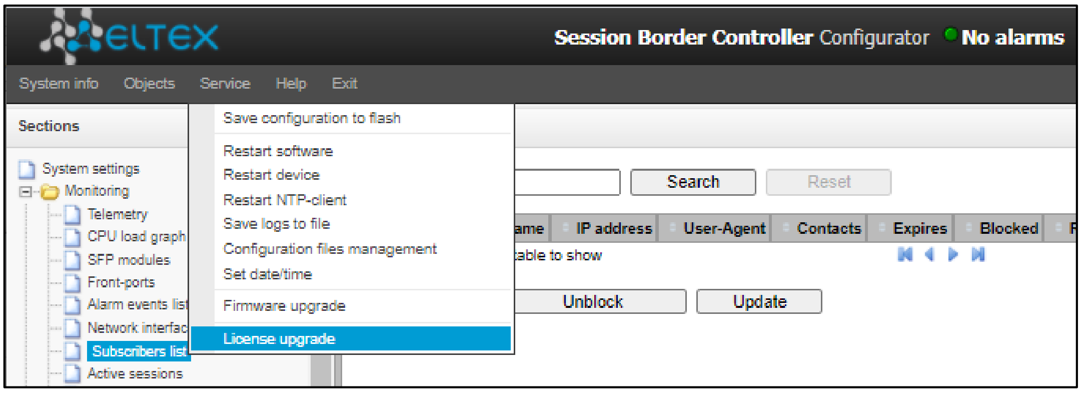
A firmware image: File is not selected

□ Restart device after firmware upgrade

### 4.1.15 *Licenses*

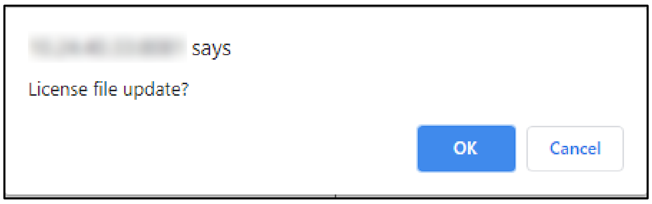
To update/add licenses, you should obtain a license file. Contact Eltex marketing department by email eltex@eltex-co.ru or phone +7 (383) 274-48-48 and provide device serial number and MAC address (see Section 4.1.17).

Next, select *«License upgrade»* parameter from the *«Service»* menu.



Specify a path to the license file obtained from the manufacturer using *«Select file»* button, and update it by clicking *«Update»*.

Confirmation is required for the license file update.



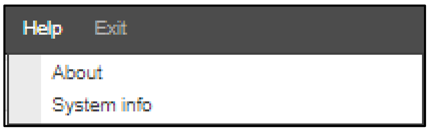
[redacted] says

License file update?

When the operation is completed, you will be prompted to restart the device, or you should do this manually using *«Service» - «Restart device »* menu.

### 4.1.16 *The «Help» menu*

The menu provides information on the current firmware version, factory defaults and other system information, as well as the ability to retrieve the latest documentation from http://eltex.org.

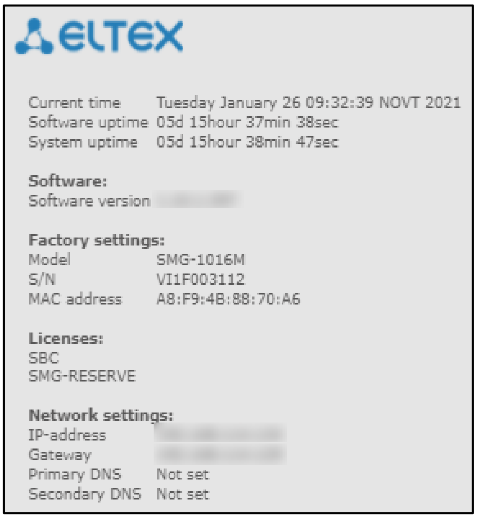


### 4.1.17 *View factory settings and system information*

To view it, use the menu *«Help» - «System info»*.

Factory settings (Serial number and MAC address) are also listed on the label located in the lower part of the device housing.

To view the detailed system information (factory settings, SIP adapter version, current date and time, uptime, network settings, internal temperature), click *«System info»* link in the control panel.



| | |
|---|---|
| Current time | Tuesday January 26 09:32:39 NOVT 2021 |
| Software uptime | 05d 15hour 37min 38sec |
| System uptime | 05d 15hour 38min 47sec |

**Software:**

| | |
|---|---|
| Software version | [redacted] |

**Factory settings:**

| | |
|---|---|
| Model | SMG-1016M |
| S/N | VI1F003112 |
| MAC address | A8:F9:4B:88:70:A6 |

**Licenses:**

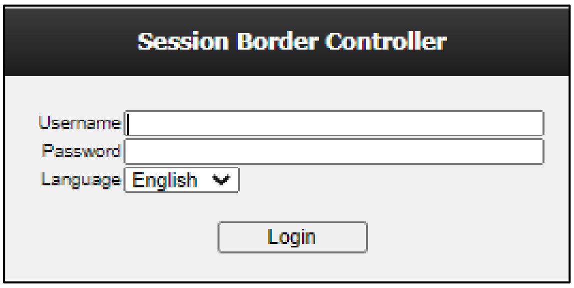
SBC
SMG-RESERVE

**Network settings:**

| | |
|---|---|
| IP-address | [redacted] |
| Gateway | [redacted] |
| Primary DNS | Not set |
| Secondary DNS | Not set |

### 4.1.18 *Exit the configurator*

When you click the *«Exit»* link on the panel, the following window will be displayed:



**Session Border Controller**

Username
Password
Language English

To resume the access, you should specify the defined username and password and click *«Login» button.*

## 4.2 SBC configuration via Telnet, SSH, or RS-232

To configure the device, you should connect to it via Telnet or SSH protocol, or by the RS-232 cable (for access via console). At factory defaults address: **192.168.1.2**, mask: **255.255.255.0**.

Configuration is stored in text files located in the ***/etc/config*** directory (to exit execute the ***sh*** command) that you can edit with the integrated text editor 'joe' (these changes will take effect after the device is restarted).

To save configuration into the device non-volatile memory, execute the **`save`** command.

When starting up for the first time, use username: ***admin***, password: ***rootpasswd*.**

### 4.2.1 *List of CLI commands*

| Command | Parameter | Value | Action |
|---|---|---|---|
| `?` | | | Show the list of available commands. |
| `alarm global` | | | Show the current alarm information |
| `alarm list clear` | | | Clear fault events log |
| `alarm list show` | | | Show fault events log with identification of fault type and status, occurrence time and localization parameters. |
| `config` | | | Enter the device parameter configuration mode |
| `CPU load statistic` | | | Show CPU load for the last minute |
| `date` | `<DAY>`<br>`<MONTH>`<br>`<YEAR>`<br>`<HOURS>`<br>`<MINS>` | `1-31`<br>`1-12`<br>`2011-2037`<br>`00-23`<br>`00-59` | Set the local date and time on the device. |
| `firmware update tftp` | `<FILE>`<br>`<SERVERIP>` | `firmware file name`<br>`IP address in AAA.BBB.CCC.DDD format` | Firmware update without gateway restart<br>FILE — firmware file name<br>SERVERIP — TFTP server IP address |
| `firmware update ftp` | `<FILE>`<br>`<SERVERIP>` | `firmware file name`<br>`IP address in AAA.BBB.CCC.DDD format` | Firmware update without gateway restart<br>FILE — firmware file name<br>SERVERIP — FTP server IP address |
| `firmware update usb` | `<FILE>` | `firmware file name` | Firmware update without gateway restart<br>FILE — firmware file name |
| `firmware update_and_reboot tftp` | `<FILE>`<br>`<SERVERIP>` | `firmware file name`<br>`IP address in AAA.BBB.CCC.DDD format` | Firmware update with gateway restart<br>FILE — firmware file name<br>SERVERIP — TFTP server IP address |
| `firmware update_and_reboot ftp` | `<FILE>`<br>`<SERVERIP>` | `firmware file name`<br>`IP address in AAA.BBB.CCC.DDD format` | Firmware update with gateway restart<br>FILE — firmware file name<br>SERVERIP — FTP server IP address |
| `firmware update_and_reboot usb` | `<FILE>` | `firmware file name` | Firmware update with gateway restart<br>FILE — firmware file name |
| `get_logs` | | | Generating and saving logs on the device |
| `history` | | | View history of entered commands. |
| `license download` | `<FILE>`<br>`<SERVERIP>` | `License file name` | Download licenses from the address specified |

| | | | |
|---|---|---|---|
| | | Server IP address in AAA.BBB.CCC.DDD format | |
| license update | | | Update the licence |
| license reset | no/yes | | Delete all installed licenses |
| password | | | Change access password via CLI |
| quit | | | Terminate this CLI session |
| reboot | <YES_NO> | yes/no | Reboot device |
| sh | | | Go to Linux Shell from CLI |
| show environment | | | Viewing hardware status information |
| show system info | | | Viewing firmware status information |
| sntp retry | | | Send SNTP request to the server for time synchronization |
| space hint | <SPACE> | yes/no | Enable or disable the tooltip when you press the «space» key |
| tcpdump | <DEVICE><br><FILE><br><SNAPLEN> | eth0/eth1/local<br>string<br>0-65535 | Capture packets from the Ethernet device<br>DEVICE — interface for monitoring;<br>FILE — file for packet writing;<br>SNAPLEN — byte quantity captured from each packet (0—full packet capture). |
| tftp get | <REMOTE_FILE><br><LOCAL_FILE><br><SERVERIP> | string<br>string<br>IP address in AAA.BBB.CCC.DDD format | Upload a file to the SBC via TFTP. |
| tftp put | <LOCAL_FILE><br><REMOTE_FILE><br><SERVERIP> | string<br>string<br>IP address in AAA.BBB.CCC.DDD format | Upload a file to TFTP. The command is used to download traces taken by the tcpdump and pcmdump commands. |

### 4.2.2 *Change device access password*

Given that you may connect to the gateway remotely via Telnet, we recommend changing the password for ***admin*** user in order to avoid unauthorized access.

To do this, you should do as follows:

1) Connect to the gateway, authorize using login/password, enter **`password`** command and press **<Enter>**.
2) Enter a new password:
   New password:
3) Retype entered password:
   Retype password:
   Password changed (Password for admin changed by root)
4) Save configuration to Flash: enter the **`save`** command and press **<Enter>**.

### 4.2.3 *Active sessions viewing mode*

This mode allows viewing detailed information on the connections established through the SBC, including RTP statistics, information from the SDP and the signaling trace in the call.

#### ***4.2.3.1 Enable/disable mode***

| Command | Action |
|---|---|
| statistics call_sessions enable | Enabling active sessions monitoring |
| statistics call_sessions disable | Disabling active session monitoring |

#### 4.2.3.2 *Viewing active sessions*

To work with these commands, it is necessary to enable monitoring of active sessions (section 4.2.3.1).

| Command | Parameter | Value | Action |
|---|---|---|---|
| `show call list` | | | View list of active connections |
| `show call info` | `CALL_ID` | `0-65520.0-5` | View general information about the selected call |
| `show call info detailed` | `CALL_ID` | `0-65520.0-5` | View detailed information about the selected call |
| `show call info RTP` | `CALL_ID` | `0-65520.0-5` | View RTP statistics for the selected call |
| `show call info SDP` | `CALL_ID` | `0-65520.0-5` | View SDP information for the selected call |

### 4.2.4 *View active registrations*

| Command | Parameter | Value | Action |
|---|---|---|---|
| `show registration list` | | | Show active registrations and blockages |
| `show registration info` | `SEARCH_LINE` | `string` | Search through active registrations and blockages |
| `registration show json` | | | Show all active registrations in json format |
| `registration show info` | `<REG_INDEX>` | `integer` | Show registration details |

### 4.2.5 *Registration management*

| Command | Parameter | Value | Action |
|---|---|---|---|
| `registration del` | `<REG_INDEX>` | `0-4095/all` | Delete subscriber registration |
| `registration unblock` | `<REG_INDEX>` | `0-4095` | Unblock subscriber |

### 4.2.6 *Operations with SIP statistics*

#### 4.2.6.1 *Enable/disable mode*

| Command | Action |
|---|---|
| `statistics sip_counters enable` | Enabling SIP statistics counters |
| `statistics sip_counters disable` | Disabling SIP statistics counters |

#### 4.2.6.2 *View statistics*

| Command | Parameter | Value | Action |
|---|---|---|---|
| `show counters list transport` | | | Show list of configured SIP transports |
| `show counters list destination` | | | Show list of configured SIP destinations |
| `show counters list users` | | | Show list of configured SIP users |
| `show counters total` | | | Show statistic counters for the entire SBC |
| `show counters transport` | `<TRANSPORT_IDX>` | `0-255` | Show statistic counters for the SIP transport |
| `show counters destinations` | `<DESTINATIONS_IDX>` | `0-255` | Show statistic counters for the SIP destination |
| `show counters users` | `<USERS_IDX>` | `0-255` | Show statistic counters for the SIP users |

### 4.2.7 *Configuration mode*

#### *4.2.7.1 General device parameter configuration mode*

To proceed to device parameter configurations/monitoring, execute **`config`** command.

```
SBC> config
Entering configuration mode.
SBC-[CONFIG]>
```

| Command | Parameter | Value | Action |
|---|---|---|---|
| `?` | | | Show the list of available commands. |
| `alarm show` | | | View alarm display settings |
| `alarm set cps` | `invite/other/subscribe` | `yes/no` | Change the INVITE/OTHER/SUBSCRIBE request processing limit alarm display mode |
| `alarm set cpu` | `<set>` | `yes/no` | Change the high CPU load alarm display mode |
| `alarm set fans` | `<set>` | `yes/no` | Change the fan alarm display mode |
| `alarm set ram` | `<set>` | `yes/no` | Change the RAM occupancy alarm display mode |
| `alarm set rom` | `<set>` | `yes/no` | Change the ROM occupancy alarm display mode |
| `alarm set reserve` | `<set>` | `yes/no` | Change the reserve alarm display mode |
| `autoupdate` | | | Switching to the configuration mode of automatic firmware and configuration updates |
| `copy running_to_startup` | | | Write the current configuration into non-volatile memory of the the device (into start configuration) |
| `copy startup_to_running` | | | Restore the current configuration from the start configuration |
| `dos-protection` | | | Enter the DoS protection configuration mode |
| `firewall dynamic` | | | Enter the dynamic firewall configuration mode |
| `firewall static` | | | Enter the static firewall configuration mode |
| `global set` | `Invite-per-3-sec/other-per-3-sec/subscribe-per-3-sec <INVITE/OTHER/SUBSCRIBE_RESTRICT>` | `60-300` | INVITE/OTHER/SUBSCRIBE requests processing restriction |
| `global set media-security-timeout` | `<SECURITY_TIMEOUT>` | `1-10080` | Protective timeout for rejection of calls without media, min |
| `global set not-encode-hash` | | `yes/no` | Enable the option to pass the «#» character without encoding |
| `history` | | | View history of entered commands. |
| `hostping` | | | Switching into the ping utility operation mode |
| `log path` | `<apply>`<br>`<set>`<br>`<show>` | `local`<br>`/mnt/sd[abc][1-7]*` | Apply settings of path to trace storage.<br>Configuration of path to trace storage: local — local storage in RAM; /mnt/sd[abc][1-7]* — path to the trace storage drive<br>View settings of path to trace storage |
| `network` | | | Enter the network parameter configuration mode |

| | | | |
|---|---|---|---|
| ports start | START_PORT | 1024-65535 | Set the start port for RTP |
| ports range | RANGE_PORT | 1-65535 | Set number of ports for RTP |
| ports show | | | View configuration of ports for RTP |
| quit | | | Terminate this CLI session |
| radius | | | Enter the RADIUS configuration mode |
| reserve | | | Enter the reserve management mode |
| route | | | Enter the static route configuration mode |
| rule set | | | Enter the rule set configuration mode |
| switch | | | Enter the switch configuration mode (only for SBC-2000 and SBC-3000) |
| show running main by_step | | | Show the current main configuration in steps |
| show running main whole | | | Show the current main configuration in full |
| show running network | | | Show current network configuration |
| show running radius_servers | | | Show the current RADIUS server configuration |
| show running snmp | | | Show current SNMP configuration |
| show startup main by_step | | | Show the initial main configuration in steps |
| show startup main whole | | | Show the initial main configuration in full |
| show startup network | | | Show initial network configuration |
| show startup radius_servers | | | Show the initial RADIUS server configuration |
| sip destination | | | Enter the SIP destination configuration mode |
| sip transport | | | Enter the SIP transport configuration mode |
| sip users | | | Enter the SIP users configuration mode |
| snmp | | | Enter the SNMP configuration mode |
| switch | | | Enter the internal switch configuration mode |
| syslog | | | Enter the syslog parameter configuration mode |
| top | | | Return to level back. |
| trunk | | | Enter the trunk configuration mode |
| user agent | | | Enter the mode of editing the list of banned client applications |

#### *4.2.7.2 Configuration mode of automatic firmware and configuration updates*

To switch to the configuration mode, you need to execute the **autoupdate** command.

```
SBC-[CONFIG]> autoupdate
Entering auto-update mode.
SBC-[CONFIG]-[AUTO-UPDATE]>
```

| Command | Parameter | Value | Action |
|---|---|---|---|
| ? | | | Show the list of available commands. |
| exit | | | Return from this configuration submenu to the upper level. |
| quit | | | Terminate this CLI session |
| set auth-name | AUTH_NAME | String, 63 characters max. | Set authentication name |
| set auth-pass | AUTH_PASS | String, 63 characters max. | Set authentication password |
| set authentication | AUTH | on/off | Enable authentication on autoupdate server |
| set config-name | CFG_NAME | String, 63 characters max. | Set configuration file name. The name must be in «. cfg» format |

| | | | |
|---|---|---|---|
| set enable | EN | on/off | Enable autoupdate |
| set manifest-name | MANIFEST_NAME | String, 63 characters max. | Set firmware versions file. The name must be in «.manifest» format |
| set protocol | PROTO | tftp<br>ftp<br>http<br>https | Specify the protocol to be used for the update |
| set source | NET_IFACE_IDX<br>static | 0-39 | Set the interface from which the server address (DHCP option 66) and the names of configuration files and firmware versions (DHCP option 57)<br>If you set static, the server information and file names will be taken from the SBC configuration |
| set static-server | ST_SERVER | String, 63 characters max. | Set the address of the auto update server |
| set update-config | UCONF | on/off | Enable configuration autoupdate |
| set update-firmware | UFIRM | on/off | Enable firmware autoupdate |
| set updating-period config | UPD_CONFIG | 1-263520 | Set the period for configuration update, in minutes |
| set updating-period manifest | UPD_MANIFEST | 1-263520 | Set the period for firmware update, in minutes |
| show auto-update-config | | | Show autoupdate configuration |
| show net-interfaces | | | Show the list of network interfaces with DHCP enabled |

#### *4.2.7.3 DoS protection configuration mode*

To enter this mode, execute **`dos-protection`** command in the configuration mode.

```
SBC2000-[CONFIG]> dos-protection
Entering dos-protection mode.
SBC2000-[CONFIG]-[DOS-PROTECTION]>
```

| Command | Parameter | Value | Action |
|---|---|---|---|
| ? | | | Show the list of available commands. |
| exit | | | Return from this configuration submenu to the upper level. |
| quit | | | Terminate this CLI session |
| set enable ICMP_flood | ENABLE | true/false | Activate ICMP flood protection |
| set enable PortScan | ENABLE | true/false | Activate port scanning protection |
| set enable protection | ENABLE | true/false | The option manages the global enabling of DoS protection functions |
| set enable RTP_flood | ENABLE | true/false | Activate RTP flood protection |
| set enable SIP_flood | ENABLE | true/false | Activate SIP flood protection |
| set enable User_Agent_filter | ENABLE | true/false | Activate filtering by User-Agent |
| set SIP_flood block time | BLOCKTIME | 600-3600 | Set the time of short subscriber blocking, seconds |
| set SIP_flood blocks | BLOCKS | 1-10 | Set the number of hits to the short block before hitting the long block |
| set SIP_flood forget_time | FORGETTIME | 12-48 | Set the long blocking time and the forget time of the subscriber caught in the short blocking, hours |
| set SIP_flood | HITS | 1-32 | Set the number of violations before hitting a short block |
| show | | | Show DoS protection settings |

### 4.2.7.4 *Dynamic firewall parameters configuration mode*

To enter this mode, execute **firewall dynamic** command in the configuration mode.

```
SBC-[CONFIG]> firewall dynamic
Entering dynamic firewall mode.
SBC-[CONFIG]-[DYN-FIREWALL]>
```

| Command | Parameter | Value | Action |
|---|---|---|---|
| ? | | | Show the list of available commands. |
| blacklist add | &lt;BLACKIP&gt; | IP address in AAA.BBB.CCC.DDD format or subnet in CIDR AAA.BBB.CCC.DDD/FF notation | Add an address to the list of blocked addresses |
| blacklist remove by addr | &lt;BLACKIP&gt; | IP address in AAA.BBB.CCC.DDD format or subnet in CIDR AAA.BBB.CCC.DDD/FF notation | Remove an address to the list of blocked addresses |
| blacklist remove by pos | &lt;POSITION&gt; | 0-65635 | Remove an address to the list of blocked addresses by its position in the list |
| blacklist show all | | | Show the list of blocked addresses |
| blacklist show count | | | Show the number of entries in the list of addresses blocked by the dynamic firewall |
| blacklist show address | &lt;BLACKIP&gt; | IP address in AAA.BBB.CCC.DDD format or subnet in CIDR AAA.BBB.CCC.DDD/FF notation | Find the specified address in the list of blocked addresses |
| blacklist show first | &lt;COUNT&gt; | 0-4095 | Show the specified number from the beginning of the list of blocked addresses |
| blacklist show last | &lt;COUNT&gt; | 0-4095 | Show the specified number from the end of the list of blocked addresses |
| blacklist show position | &lt;POSITION&gt; | 0-65635 | Show the entry in the specified position of the list of blocked addresses |
| blacklist subnet | &lt;BLACKIP&gt; | subnet in CIDR AAA.BBB.CCC.DDD/FF notation | Add a subnet to the list of blocked addresses and remove addresses and subnets included in the added subnet |
| block history show all | | | View a log of blocked addresses |
| block show count | | | Show the number of entries in the log of blocked addresses |
| block show address | &lt;BLACKIP&gt; | IP address in AAA.BBB.CCC.DDD format or subnet in CIDR AAA.BBB.CCC.DDD/FF notation | Find the specified address in the log of blocked addresses |
| block show first | &lt;COUNT&gt; | 0-4095 | Show the specified number from the beginning of the log of blocked addresses |
| block show last | &lt;COUNT&gt; | 0-4095 | Show the specified number from the end of the log of blocked addresses |
| block show position | &lt;POSITION&gt; | 0-65635 | Show the entry in the specified position of the log of blocked addresses |
| blocklist remove by addr | &lt;BLACKIP&gt; | IP address in AAA.BBB.CCC.DDD format or subnet in CIDR AAA.BBB.CCC.DDD/FF notation | Remove an address to the list of automatically blocked addresses |
| blocklist remove by pos | &lt;POSITION&gt; | 0-65635 | Remove an address to the list of automatically blocked addresses by its position in the list |

|  |  |  |  |
|---|---|---|---|
| blocklist show all |  |  | Show the list of automatically blocked addresses |
| blocklist show count |  |  | Show the number of entries in the list of automatically blocked addresses |
| blocklist show address | <BLACKIP> | IP address in AAA.BBB.CCC.DDD format or subnet in CIDR AAA.BBB.CCC.DDD/FF notation | Find the specified address in the list of automatically blocked addresses |
| blocklist show first | <COUNT> | 0-4095 | Show the specified number from the beginning of the list of automatically blocked addresses |
| blocklist show last | <COUNT> | 0-4095 | Show the specified number from the end of the list of automatically blocked addresses |
| blocklist show position | <POSITION> | 0-65635 | Show the entry in the specified position of the list of automatically blocked addresses |
| exit |  |  | Return from this configuration submenu to the upper level. |
| history |  |  | View history of entered commands. |
| quit |  |  | Terminate this CLI session |
| set block_time | <SERVICE><br><BLCKTIME> | SIP/WEB/TELNET/SSH/OTHER<br>60-352800 | Set the time in seconds for the service, during which access from a suspicious address will be blocked |
| set enable | <ENA> | on/off | Enable/disable dynamic firewall |
| set tries | <SERVICE><br><TRIES> | SIP/WEB/TELNET/SSH/OTHER<br>1-10 | Set the maximum number of fault attempts to access the service before the host is blocked |
| set forgive_time | <SERVICE><br><FORGIVETIME> | SIP/WEB/TELNET/SSH/OTHER<br>60-352800 | Set the forgiveness time for the service |
| set increment | <SERVICE><br><INCREMENT_FLG> | SIP/WEB/TELNET/SSH/OTHER<br>no/yes | Enable progressive blocking for the service |
| set only block | <SERVICE><br><ONLY_BLOCK_FLG> | SIP/WEB/TELNET/SSH/OTHER<br>no/yes | Enable the «Do not send blocked addresses to blacklist» option for the service |
| show |  |  | Show dynamic firewall settings |
| whitelist add | <WHITEIP> | IP address in AAA.BBB.CCC.DDD format or subnet in CIDR AAA.BBB.CCC.DDD/FF notation | Add an IP address to the list of addresses banned for automatic blocking |
| whitelist remove by addr | <WHITEIP> | IP address in AAA.BBB.CCC.DDD format or subnet in CIDR AAA.BBB.CCC.DDD/FF notation | Remove an IP address from the list of addresses banned for automatic blocking |
| whitelist remove by pos | <POSITION> | 0-65635 | Remove an IP address from the list of addresses banned for automatic blocking by its position in the list |
| whitelist show all |  |  | Show the list of addresses banned for automatic blocking |
| whitelist show count |  |  | Show the number of entries in the list of addresses banned for automatic blocking |
| whitelist show address | <WHITEIP> | IP address in AAA.BBB.CCC.DDD format or subnet in CIDR AAA.BBB.CCC.DDD/FF notation | Find the specified address in the list of addresses banned for automatic blocking |
| whitelist show first | <COUNT> | 0-4095 | Show the specified number from the beginning of the list of addresses banned for automatic blocking |
| whitelist show last | <COUNT> | 0-4095 | Show the specified number from the end of the list of addresses banned for automatic blocking |
| whitelist show position | <POSITION> | 0-65635 | Show the entry in the specified position of the list of addresses banned for automatic blocking |

|  |  |  |  |
|---|---|---|---|
| whitelist subnet | <WHITEIP> | subnet in CIDR AAA.BBB.CCC.DDD/FF notation | Add a subnet to the list of addresses banned for automatic blocking and remove addresses and subnets included in the added subnet |

### *4.2.7.5 Static firewall parameters configuration mode*

To enter this mode, execute **`firewall static`** command in the configuration mode.

```
SBC-[CONFIG]> firewall static
Entering static firewall mode
SBC-[CONFIG]-[FIREWALL]>
```

| Command | Parameter | Value | Action |
|---|---|---|---|
| ? |  |  | Show the list of available commands. |
| add profile | <PROF_NAME> | you may use letters, numbers, '_' character, 63 characters max. | Add firewall profile |
| add rule default | <direction> | input<br>output | Add firewall rule<br>Rule direction |
|  | <ENABLE> | enable/disable | Enable/disable rule |
|  | <RULE_NAME> | Text, 63 characters max. | Rule name |
|  | <S_IP> | AAA.BBB.CCC.DDD | Source IP address |
|  | <S_MASK> | AAA.BBB.CCC.DDD | Source subnet mask |
|  | <R_IP> | AAA.BBB.CCC.DDD | Destination IP address |
|  | <R_MASK> | AAA.BBB.CCC.DDD | Destination subnet mask |
|  | <PROTO> | any<br>tcp<br>udp<br>icmp<br>tcp+udp | Protocol type |
|  | <S_PORT_START> | 1-65535 | Source starting port |
|  | <S_PORT_END> | 1-65535 | Source ending port |
|  | <D_PORT_START> | 1-65535 | Destination starting port |
|  | <D_PORT_END> | 1-65535 | Destination ending port |
|  | <ICMP_TYPE> | none<br>any<br>echo-reply<br>destination-unreachable<br>network-unreachable<br>host-unreachable<br>protocol-unreachable<br>port-unreachable<br>fragmentation-needed<br>source-route-failed<br>network-unknown<br>host-unknown<br>network-prohibited<br>host-prohibited<br>TOS-network-unreachable TOS-host-unreachable<br>communication-prohibited | ICMP packet type |

| | | | |
|---|---|---|---|
| | | host-precedence-violation<br>precedence-cutoff<br>source-quench<br>redirect<br>network-redirect<br>host-redirect<br>TOS-network-redirect<br>TOS-host-redirect<br>echo-request<br>router-advertisement<br>router-solicitation<br>time-exceeded<br>ttl-zero-during-transit<br>ttl-zero-during-reassembly<br>parameter-problem<br>ip-header-bad<br>required-option-missing<br>timestamp-request<br>timestamp-reply<br>address-mask-request<br>address-mask-reply | |
| | <ACTION> | accept, drop, reject | Action — action executed by this rule:<br>— ACCEPT — packets falling under this rule will be accepted by the firewall;<br>— DROP — packets falling under this rule will be rejected by the firewall without informing the party that has sent these packets;<br>— DROP — packets falling under this rule will be rejected by the firewall; the party that has sent the packet will receive either TCP RST packet or 'ICMP destination unreachable'. |
| | <P_IDX> | 1-65535 | Firewall profile number |
| add rule geoip | <direction> | input<br>output | Add firewall GeoIP-rule<br>Rule direction |
| | <ENABLE> | enable/disable | Enable/disable rule |
| | <RULE_NAME> | Text, 63 characters max. | Rule name |
| | <COUNTRY> | Country name | The country to which the address belongs |
| | <PROTO> | any<br>tcp<br>udp<br>icmp<br>tcp+udp | Protocol type |
| | <S_PORT_START> | 1-65535 | Source starting port |
| | <S_PORT_END> | 1-65535 | Source ending port |
| | <D_PORT_START> | 1-65535 | Destination starting port |
| | <D_PORT_END> | 1-65535 | Destination ending port |
| | <ICMP_TYPE> | | ICMP packet type |

| | | | |
|---|---|---|---|
| | | none<br>any<br>echo-reply<br>destination-unreachable<br>network-unreachable<br>host-unreachable<br>protocol-unreachable<br>port-unreachable<br>fragmentation-needed<br>source-route-failed<br>network-unknown<br>host-unknown<br>network-prohibited<br>host-prohibited<br>TOS-network-unreachable<br>TOS-host-unreachable<br>communication-prohibited<br>host-precedence-violation<br>precedence-cutoff<br>source-quench<br>redirect<br>network-redirect<br>host-redirect<br>TOS-network-redirect<br>TOS-host-redirect<br>echo-request<br>router-advertisement<br>router-solicitation<br>time-exceeded<br>ttl-zero-during-transit<br>ttl-zero-during-reassembly<br>parameter-problem<br>ip-header-bad<br>required-option-missing<br>timestamp-request<br>timestamp-reply<br>address-mask-request<br>address-mask-reply | |
| | <ACTION> | accept, drop, reject | Action — action executed by this rule:<br>— ACCEPT — packets falling under this rule will be accepted by the firewall;<br>— DROP — packets falling under this rule will be rejected by the firewall without informing the party that has sent these packets;<br>— DROP — packets falling under this rule will be rejected by the firewall; the party that has sent the packet will receive either TCP RST packet or 'ICMP destination unreachable'. |
| | <P_IDX> | 1-65535 | Firewall profile number |
| add rule string | | | Add firewall rule — string check. |
| | <direction> | input<br>output | Rule direction |
| | <ENABLE> | enable/disable | Enable/disable rule |
| | | | Rule name |

| | | | |
|---|---|---|---|
| | <RULE_NAME> | Text, 63 characters max. | |
| | <CONTENT> | Text, 127 characters max. | The text string that should be in the packet |
| | <S_IP> | AAA.BBB.CCC.DDD | Source IP address |
| | <S_MASK> | AAA.BBB.CCC.DDD | Source subnet mask |
| | <R_IP> | AAA.BBB.CCC.DDD | Destination IP address |
| | <R_MASK> | AAA.BBB.CCC.DDD | Destination subnet mask |
| | <PROTO> | any<br>tcp<br>udp<br>icmp<br>tcp+udp | Protocol type |
| | <S_PORT_START> | 1-65535 | Source starting port |
| | <S_PORT_END> | 1-65535 | Source ending port |
| | <D_PORT_START> | 1-65535 | Destination starting port |
| | <D_PORT_END> | 1-65535 | Destination ending port |
| | <ICMP_TYPE> | none<br>any<br>echo-reply<br>destination-unreachable<br>network-unreachable<br>host-unreachable<br>protocol-unreachable<br>port-unreachable<br>fragmentation-needed<br>source-route-failed<br>network-unknown<br>host-unknown<br>network-prohibited<br>host-prohibited<br>TOS-network-unreachable<br>TOS-host-unreachable<br>communication-prohibited<br>host-precedence-violation<br>precedence-cutoff<br>source-quench<br>redirect<br>network-redirect<br>host-redirect<br>TOS-network-redirect<br>TOS-host-redirect<br>echo-request<br>router-advertisement<br>router-solicitation<br>time-exceeded<br>ttl-zero-during-transit<br>ttl-zero-during-reassembly<br>parameter-problem<br>ip-header-bad<br>required-option-missing | ICMP packet type |

| | | | |
|---|---|---|---|
| | <ACTION><br><P_IDX> | timestamp-request<br>timestamp-reply<br>address-mask-request<br>address-mask-reply<br>accept, drop, reject<br>1-65535 | Action — action executed by this rule:<br>– ACCEPT — packets falling under this rule will be accepted by the firewall;<br>– DROP — packets falling under this rule will be rejected by the firewall without informing the party that has sent these packets;<br>– DROP — packets falling under this rule will be rejected by the firewall; the party that has sent the packet will receive either TCP RST packet or 'ICMP destination unreachable'.<br>Firewall profile number |
| apply | | | Apply firewall settings |
| config | | | Return to Configuration menu. |
| del profile | <ID> | 1-65535 | Remove firewall profile |
| del rule | <ID> | 1-65535 | Remove firewall rule |
| exit | | | Exit from this configuration submenu to the upper level. |
| modify profile | <ID><br><NAME> | 1-65535<br>allowed using letters, numbers, character'_'. 63 characters max. | Firewall profile index<br>Enter a new name for the device |
| modify rule | <TYPE><br><ID><br><param> | action<br>dport_end<br>dport_start  enable<br>icmp-type<br>name<br>prof_id<br>proto<br>r_ip  r_mask<br>s_ip  s_mask<br>sport_end<br>sport_start<br>traffic-type<br>1-65535<br>New value according to this parameter type | Modify the firewall rule specified (one of the parameters) |
| move down | <ID> | 1-65535 | Move the rule one position down |
| move up | <ID> | 1-65535 | Move the rule one position up |
| quit | | | Terminate this CLI session |
| set interface | <IFACE_NAME><br><PROFILE ID> | Interface name | Assign the rule to the network interface<br>PROFILE ID = 0 means that profile will not be used |
| show config | | | Show configuration |
| show net-interfaces | | | Show interface parameters: |
| show system | | | Show system parameters |

#### 4.2.7.6 Configuration and operation with the PING utility

To enter this mode, execute **`hostping`** command in the configuration mode.

SBC1000-[CONFIG]> hostping
Entering hostping mode.
SBC1000-[CONFIG]-[HOSTPING]>

| Command | Parameter | Value | Action |
|---|---|---|---|
| ? | | | Show the list of available commands. |
| | | | |
| exit | | | Return from this configuration submenu to the upper level. |
| host add | ADDR | AAA.BBB.CCC.DDD | Add a host to the ping list |
| host remove | ADDR | AAA.BBB.CCC.DDD | Remove a host from the ping list |
| host show | | | Show operation result |
| set onboot | ONBOOT | yes/no | Start onboot check |
| set period | PINGTIME | 1-255 | Ping period, minutes |
| set tries | TRIES | 1-7 | Number of requests to each host |
| show | | | Display the PING utility settings |
| start | | | Run a periodic ping |
| stop | | | Stop a periodic ping |
| quit | | | Terminate this CLI session |

#### 4.2.7.7 Network parameters configuration mode

To enter this mode, execute **`network`** command in the configuration mode.

SBC-[CONFIG]> network
Entering Network mode.
SBC-[CONFIG]-NETWORK>

| Command | Parameter | Value | Action |
|---|---|---|---|
| ? | | | Show the list of available commands. |
| add interface pptpVPNclient | &lt;LABEL&gt;<br>&lt;IPADDR&gt;<br>&lt;USER&gt;<br>&lt;PASS&gt; | you may use letters, numbers, '_', '.', '-', ':' characters, 255 characters max.<br>IP address in AAA.BBB.CCC.DDD format<br>you may use letters, numbers, '_', '.', '-' characters, 63 characters max.<br>you may use letters, numbers, '_', '.', '-' characters, 63 characters max. | Add new VPN/PPTP client<br>LABEL — interface name;<br>IPADDR — PPTP server IP address;<br>USER — user name;<br>PASS — password |
| add interface tagged | dynamic/static<br>&lt;LABEL&gt;<br>&lt;VID&gt;<br>&lt;IPADDR&gt;<br>&lt;NETMASK&gt; | you may use letters, numbers, '_', '.', '-', ':' characters, 255 characters max.<br>1-4095<br>IP address in AAA.BBB.CCC.DDD format<br>network mask in format of AAA.BBB.CCC.DDD | Add a new network interface<br>LABEL — interface name;<br>VID — VLAN ID;<br>IPADDR — PPTP server IP address;<br>NETMASK — network mask |

| | | | |
|---|---|---|---|
| add interface untagged | dynamic/static<br><LABEL><br><IPADDR><br><NETMASK> | you may use letters, numbers, '_', '.', '-', ':' characters, 255 characters max.<br>IP address in AAA.BBB.CCC.DDD format<br>network mask in format of AAA.BBB.CCC.DDD | Add a new network interface<br>LABEL — interface name;<br>IPADDR — PPTP server IP address;<br>NETMASK — network |
| config | | | Return to Configuration menu. |
| confirm | | | Confirm changed network and VLAN settings without rebooting the gateway. If the applied network settings are not confirmed within a minute, their values will return to the initial |
| exit | | | Exit from this configuration submenu to the upper level. |
| history | | | View history of entered commands. |
| ntp | | | Enter the NTP configuration mode |
| quit | | | Terminate this CLI session |
| remove interface | <NET_IFACE_IDX> | 0-39 | Remove the specified interface |
| rollback | | | Discard changes |
| set interface COS | <NET_IFACE_IDX><br><COS> | 0-39<br>0-7 | Assign 802.1p priority for the specified interface |
| set interface dhcp | <NET_IFACE_IDX><br><ON_OFF> | 0-39<br>on/off | Obtain network configuration dynamically from the DHCP server for the specified interface |
| set interface dhcp_dns | <NET_IFACE_IDX><br><ON_OFF> | 0-39<br>on/off | Obtain DNS server IP address dynamically from the DHCP server for the specified interface |
| set interface dhcp_no_gw | <NET_IFACE_IDX><br><ON_OFF> | 0-39<br>on/off | Do not obtain gateway configuration dynamically from the DHCP server for the specified interface |
| set interface gateway | <NET_IFACE_IDX><br><IPADDR> | 0-39<br>IP address in AAA.BBB.CCC.DDD format | Set the default gateway for the interface |
| set interface dhcp_ntp | <NET_IFACE_IDX><br><ON_OFF> | 0-39<br>on/off | Obtain NTP configuration dynamically from the DHCP server for the specified interface |
| set interface gw_ignore | <NET_IFACE_IDX><br><ON_OFF> | 0-39<br>on/off | Ignore gateway configuration for the specified interface |
| set interface ipaddr | <NET_IFACE_IDX><br><IPADDR><br><NETMASK> | 0-39<br>IP address in AAA.BBB.CCC.DDD format<br>network mask in format of AAA.BBB.CCC.DDD | Set the IP address and netmask for the specified interface |
| set interface network-label | <NET_IFACE_IDX><br><LABEL> | 0-39<br>digits, '_', '.', '-', ':' characters, 255 characters max. | Set the name for the given interface |
| set interface run_at_startup | <NET_IFACE_IDX><br><STARTUP> | 0-39<br>on/off | Automatically start the interface at startup (only for the VPN interface) |
| set interface serverip | <NET_IFACE_IDX><br><IPADDR> | 0-39<br>IP address in AAA.BBB.CCC.DDD format | Set the PPTP server IP address |
| set interface snmp | <NET_IFACE_IDX><br><ON_OFF> | 0-39<br>on/off | Allow SNMP packet transmission via interface |

| | | | |
|---|---|---|---|
| set interface ssh | <NET_IFACE_IDX><br><ON_OFF> | 0-39<br>on/off | Allow ssh session via interface |
| set interface telnet | <NET_IFACE_IDX><br><ON_OFF> | 0-39<br>on/off | Allow telnet session via interface |
| set interface use_mppe | <NET_IFACE_IDX><br><ON_OFF> | 0-39<br>on/off | Enable/disable encryption (VPN interface only) |
| set interface user_name | <NET_IFACE_IDX><br><USER> | 0-39<br>you may use letters, numbers, '_', '.', '-' characters, 63 characters max. | Set user name (VPN interface only) |
| set interface user_pass | <NET_IFACE_IDX><br><PASS> | 0-39<br>you may use letters, numbers, '_', '.', '-' characters, 63 characters max. | Set password (VPN interface only) |
| set interface VID | <NET_IFACE_IDX><br><VID> | 0-39<br>1-4095 | Assign VID for the interface |
| set interface web | <NET_IFACE_IDX><br><ON_OFF> | 0-39<br>on/off | Allow the access via web interface |
| set settings dns primary | <IPADDR> | IP address in AAA.BBB.CCC.DDD format | Set main DNS server IP address |
| set settings dns secondary | <IPADDR> | IP address in AAA.BBB.CCC.DDD format | Set redundant DNS server IP address |
| set settings gateway_iface | <NET_IFACE_NAME> | | Name of the interface whose gateway will be the default gateway |
| set settings hostname | <HOSTNAME> | you may use letters, numbers, '_', '.', '-' characters, 63 characters max. | Set the host name |
| set settings ssh | <PORT> | 1-65535 | Set the TCP port for SSH access to the device, the default is 22 |
| set settings telnet | <PORT> | 1-65535 | Set the TCP port for Telnet access to the device, the default is 23 |
| set settings web | <PORT> | 1-65535 | Set the TCP port for web configurator, default is 80 |
| show interface by_index | <NET_IFACE_IDX> | 0-39 | Show the settings of the specified network interface |
| show interface list | | | Show the list of available network interfaces |
| show settings | | | Show network parameters |
| snmp | | | Enter the SNMP configuration mode |
| ssh restart | | | SSH restart process |

#### 4.2.7.8 NTP configuration mode

To enter this mode, execute **ntp** command in the network parameters configuration mode.

```
SBC-[CONFIG]-NETWORK> ntp
Entering NTP mode.
SBC-[CONFIG]-[NETWORK]-NTP>
```

| Command | Parameter | Value | Action |
|---|---|---|---|
| ? | | | Show the list of available commands. |
| apply | | no/yes | Apply NTP settings |
| config | | | Return to Configuration menu. |
| exit | | | Exit from this configuration submenu to the upper level. |
| quit | | | Terminate this CLI session |

|  |  |  |  |
|---|---|---|---|
| restart ntp |  | no/yes | Restart NTP process |
| set ntp | dhcp<br>period<br>server<br>usage | off/on<br>10-1440<br>IP address in AAA.BBB.CCC.DDD format<br>off/on | Obtain NTP settings via DHCP<br>Set synchronization period<br>Set NTP server<br>Do not use/use NTP |
| show config |  |  | Show |
| timezone set |  | GMT/GMT+1/GMT-1/GMT+2/GMT-2/GMT+3/GMT-3/GMT+4/GMT-4/GMT+5/GMT-5/GMT+6/GMT-6/GMT+7/GMT-7/GMT+8/GMT-8/GMT+9/GMT-9/GMT+10/GMT-10/GMT+11/GMT-11/GMT+12<br>Asia<br>Europe | Set the time zone in relation to universal time coordinates<br>Choosing a location city in Asia.<br>Choosing a location city in Europe |

#### *4.2.7.9 SNMP configuration mode*

To enter this mode, execute **snmp** command in the configuration mode.

```
SBC-[CONFIG]-NETWORK> snmp
Entering SNMP mode.
SBC-[CONFIG]-SNMP>
```

| Command | Parameter | Value | Action |
|---|---|---|---|
| ? |  |  | Show the list of available commands. |
| add | <TYPE><br><IP><br><COMM><br><PORT> | trapsink/ trap2sink/ informsink<br>IP address in AAA.BBB.CCC.DDD format<br>string of up to 31 characters<br>1-65535 | Add SNMP trap transmission rule:<br>TYPE — SNMP message type<br>IP — trap receiver IP address;<br>COMM — password contained in traps.<br>PORT — trap receiver UDP port |
| config |  |  | Return to Configuration menu. |
| create user | <LOGIN><br><PASSWD> | string of up to 31 characters<br>password from 8 to 31 characters | Create a user (assign a login and password for access) |
| exit |  |  | Exit from this configuration submenu to the upper level. |
| history |  |  | View history of entered commands. |
| modify community | <IDX><br><COMM> | 0-15<br>string of up to 31 characters | Change the SNMP traps transmission rule (the password contained in the traps) |
| modify ip | <IDX><br><IP> | 0-15<br>IP address in AAA.BBB.CCC.DDD format | Change the SNMP trap transmission rule (trap receiver address) |
| modify port | <IDX><br><PORT> | 0-15<br>1-65535 | Change the SNMP trap transmission rule (trap receiver port) |

| | | | |
|---|---|---|---|
| modify type | <IDX><br><TYPE> | 0-15<br>trapsink/ trap2sink/ informsink | Change the SNMP trap transmission rule (SNMP message type) |
| quit | | | Terminate this CLI session |
| remove | <IDX> | 0-15 | Remove SNMP trap transmission rule |
| restart snmpd | Yes/no | | Restart SNMP client |
| ro | <RO> | string, 63 characters max. | Set the password for reading the parameters |
| rw | <RW> | string, 63 characters max. | Set the password for reading and recording the parameters |
| show | | | Show SNMP configuration |
| syscontact | <SYSCONTACT> | string, 63 characters max. | Specify contact information |
| syslocation | <SYSLOC> | string, 63 characters max. | Specify device location |
| sysname | <SYSNAME> | string, 63 characters max. | Specify device name |

### *4.2.7.10 Radius configuration mode*

To enter this mode, execute **radius** command in the configuration mode.

```
SBC-[CONFIG]> radius
Entering RADIUS mode.
SBC-[CONFIG]-RADIUS>
```

| Command | Parameter | Value | Action |
|---|---|---|---|
| ? | | | Show the list of available commands. |
| auth ipaddr | <IP_ADDR><br><SRV_IDX> | IP address in AAA.BBB.CCC.DDD format<br>0-8 | Set authorization server IP address.<br>IP_ADDR — IP address;<br>SRV_IDX — server number |
| auth port | <PORT><br><SRV_IDX> | 0-65535<br>0-8 | Set authorization server port<br>PORT — port number;<br>SRV_IDX — server number |
| auth secret | <SECRET><br><SRV_IDX> | string, 31 characters max.<br>0-8 | Set the password for authorization server<br>SECRET — password;<br>SRV_IDX — server number |
| config | | | Return to Configuration menu. |
| deadtime | <DEADTIME> | 5-60 | Server downtime in case of failure — time during which the server is considered inactive |
| exit | | | Exit from this configuration submenu to the upper level. |
| history | | | View history of entered commands. |
| profile | <PROFILE_INDEX> | 0-31 | Go to the RADIUS profile parameters configuration |
| quit | | | Terminate this CLI session |
| retries | <RETRIES> | 2-5 | Set the number of attempts to send a request |
| show config | | | Show information on RADIUS server configuration |
| timeout | <TIMEOUT> | 3-10 | Set the time for which the server is expected to respond (x100ms) |
| | | | |

### *4.2.7.11 RADIUS profile parameters configuration mode*

To enter this mode, in the RADIUS configuration mode, run the **profile <PROFILE_INDEX>** command, where **<PROFILE_INDEX>** is the RADIUS profile number.

```
SBC-[CONFIG]-RADIUS> profile 0
Entering RADIUS-Profile-mode.
SBC-[CONFIG]-RADIUS-PROFILE[0]>
```

| Command | Parameter | Value | Action |
|---|---|---|---|
| `?` | | | Show the list of available commands. |
| `auth digestauth` | `<DIGESTAUTH>` | `rfc5090/`<br>`rfc5090-no-challenge/`<br>`draft-sterman` | Select the algorithm of subscriber authorization with dynamic registration through the RADIUS server.  With digest authentication, the password is transmitted as a hash code and cannot be intercepted when traffic is scanned |
| `auth framedprotocol` | `<FRAMED_PROTOCOL>` | `none/PPP/`<br>`SLIP/ARAP/`<br>`Gandalf/Xylogics/`<br>`X75_Sync` | Assign a protocol when using packet access for RADIUS authentication requests<br><br>*none* — packet access is not used |
| `auth nas port type` | `<PORT_TYPE>` | `Async/`<br>`Sync/`<br>`ISDN_Sync/`<br>`ISDN_Async_v120/`<br>`ISDN_Async_v110/`<br>`Virtual/`<br>`PIAFS/`<br>`HDLC_Channel/`<br>`X25/`<br>`X75/`<br>`G3_Fax/`<br>`SDSL/`<br>`ADSL_CAP/`<br>`ADSL_DMT/`<br>`IDSL/`<br>`Ethernet/`<br>`xDSL/`<br>`Cable/`<br>`Wireless/`<br>`Wireless_IEEE_802.1` | Assign the type of the physical NAS port (the server where the user is authenticated), Async is default |
| `auth restrict` | `<RESTRICT>` | `none/`<br>`restrict-all` | Set a limit on outgoing communication when the server fails (no response from the server):<br><br>*none* — allow all calls;<br><br>*restrict-all* — restrict all calls |
| `auth service type` | `<SERVICE_TYPE>` | `none/`<br>`Login/`<br>`Framed/`<br>`Callback_Login/`<br>`Callback_Framed/`<br>`Outbound/`<br>`Administrative/`<br>`NAS_Promt/`<br>`Authenticate_Only/`<br>`Callback_NAS_Prompt/`<br>`Call_Check/`<br>`Callback_Administrative` | Set the type of service, by default it is none |
| `auth user_name originate` | `<USERNAME_MODE>` | `sip_username/`<br>`ip/`<br>`sip_iface_name` | Set the User-Name attribute in Access-Request packages:<br><br>*cgpn* — use the telephone number of the calling party as the value;<br><br>*ip_or_stream* — use the IP address of the calling party or the number of the stream on which the incoming connection is made as the value; |

| | | | |
|---|---|---|---|
| | | | *trunk* — use the name of the trunk over which the incoming connection is made as a value |
| config | | | Return to Configuration menu. |
| exit | | | Exit from this configuration submenu to the upper level. |
| history | | | View history of entered commands. |
| name | <PRF_NAME> | String, 63 characters max. | Set profile name |
| quit | | | Terminate this CLI session |
| show | | | Show RADIUS profile configuration |

### 4.2.7.12 Reserve operation mode

To enter this mode, execute '**reserve**' command in the configuration mode.

```
SBC1000-[CONFIG]> reserve
Entering reserve mode.
SBC1000-[CONFIG]-[RESERVE]>
```

| Command | Parameter | Value | Action |
|---|---|---|---|
| ? | | | Show the list of available commands. |
| config | | | Return to Configuration menu. |
| exit | | | Exit from this configuration submenu to the upper level. |
| history | | | View history of entered commands. |
| set master | SERIAL_NUMBER | String, 10 characters | Make the device with the specified serial number a master |
| show | | | Show reserve status information |
| quit | | | Terminate this CLI session |
| show | | | Show RADIUS profile configuration |

### 4.2.7.13 Static route configuration mode

To enter this mode, execute '**route**' command in the configuration mode.

```
SBC-[CONFIG]> route
Entering route mode.
SBC-[CONFIG]-ROUTE>
```

| Command | Parameter | Value | Action |
|---|---|---|---|
| ? | | | Show the list of available commands. |
| config | | | Return to Configuration menu. |
| exit | | | Exit from this configuration submenu to the upper level. |
| history | | | View history of entered commands. |
| quit | | | Terminate this CLI session |
| route default add | <DESTINATION><br><MASK><br><GATEWAY><br><METRIC><br><IFACE_NAME> | IP address in AAA.BBB.CCC.DDD format<br>mask in format of AAA.BBB.CCC.DDD<br>gateway in format of AAA.BBB.CCC.DDD<br>unsigned integer<br>string, 255 characters max. | Add static route:<br>DESTINATION — IP address of the destination;<br>MASK — network mask for the specified IP address;<br>GATEWAY — gateway IP address;<br>METRIC — metric |

| | | | |
|---|---|---|---|
| | <ENABLE> | disable/enable | IFACE_NAME — network interface<br>ENABLE — enable/disable network route |
| route del | <IDX> | 0-4095 | Delete route:<br>IDX — network route index |
| route modify destination | <IDX><br><DESTINATION> | 0-4095 | Change the destination address |
| route modify dev | <IDX><br><IFACE_NAME> | 0-4095<br>network interface name | Change the network interface |
| route modify enable | <IDX><br><EN> | 0-4095<br>enable/disable | Enable or disable the route |
| route modify gateway | <IDX><br><GATEWAY> | 0-4095<br>IP address in AAA.BBB.CCC.DDD format | Change the gateway |
| route modify metric | <IDX><br><METRIC> | 0-4095<br>0-2147483647 | Change the metric |
| route modify netmask | <IDX><br><NETMASK> | 0-4095<br>mask in format of AAA.BBB.CCC.DDD | Change network mask |
| route modify vpn-client | <IDX><br><VPN_CLIENT> | 0-4095<br>VPN client name | Change VPN client |
| route VPN add | <DESTINATION><br><MASK><br><METRIC><br><VPN_CLIENT><br><ENABLE> | IP address in AAA.BBB.CCC.DDD format<br>mask in format of AAA.BBB.CCC.DDD<br>unsigned integer<br>string, 255 characters max.<br>disable/enable | Add a route via VPN client:<br>DESTINATION — IP address of the destination;<br>MASK — network mask for the specified IP address;<br>METRIC — metric<br>VPN_CLIENT — VPN client name<br>ENABLE — enable/disable network route |
| show config | | | Show information on route configuration |
| show net-interfaces | | | Show the list of network interfaces |
| show system | | | Show active routes |
| show vpn-clients | | | Show list of VPN clients |

#### *4.2.7.14 Configuring a list of rule sets*

To enter this mode, execute '**rule set**' command in the configuration mode.

```
SBC1000-[CONFIG]> rule set
Entering SBC rule set mode.
SBC1000-[CONFIG]-RULE-SET>
```

| Command | Parameter | Value | Action |
|---|---|---|---|
| ? | | | Show the list of available commands. |
| add rule set | SBC_RULE_SET_NAME | String, 63 characters max. | Add the rule set |

|  |  |  |  |
|---|---|---|---|
| edit rule set id | PREFIX_SIGN | 1-65535 | Edit a rule set with a specified ID |
| edit rule set index | PREFIX_SIGN | 0-65534 | Edit a rule set with a specified index |
| exit |  |  | Exit from this configuration submenu to the upper level. |
| quit |  |  | Terminate this CLI session |
| remove by id rule set | SBC_RULE_SET_ID | 1-65535 | Remove a rule set with a specified ID |
| show |  |  | Display a list of all rule sets |

### *4.2.7.15 Configuring a rule set*

To switch to this mode, execute the **edit rule set id <ID>** or **edit rule set index <INDEX>** command in the **rule set** list configuration mode, where **<ID>** and **<INDEX>** are the ID or index of the rule being edited.

```
SBC1000-[CONFIG]-RULE-SET> edit rule set id 1
Entering SBC rule set edit mode.
SBC1000-[CONFIG]-RULE-SET-ID[1>

SBC1000-[CONFIG]-RULE-SET> edit rule set index 0
Entering SBC rule set edit mode.
SBC1000-[CONFIG]-RULE-SET-INDEX[0]>
```

| Command | Parameter | Value | Action |
|---|---|---|---|
| ? |  |  | Show the list of available commands. |
| add rule | SBC_RULE_NAME | String, 63 characters max. | Add a rule with the specified name to the set |
| edit rule | SBC_RULE_ID | 1-65535 | Edit a rule with a specified ID |
| exit |  |  | Exit from this configuration submenu to the upper level. |
| quit |  |  | Terminate this CLI session |
| remove rule | SBC_RULE_ID | 1-65535 | Remove the rule with the specified ID |
| show info |  |  | Display a list of all rule sets |
| swap rules | <SBC_RULE_ID_CURRENT><br><SBC_RULE_ID_TARGET> | 1-65535<br>1-65535 | Swap CURRENT and TARGET rules |

### *4.2.7.16 Configuring rule sets*

To enter this mode, in the **rule set** configuration mode, execute the **edit rule <ID>** command, where **<ID>** is the ID of the rule to be edited.

```
SBC1000-[CONFIG]-RULE-SET-INDEX[13]> edit rule 16
Entering SBC rule edit mode.
SBC1000-[CONFIG]-RULE-SET-INDEX[13]-RULE-ID[16]>
```

| Command | Parameter | Value | Action |
|---|---|---|---|
| ? |  |  | Show the list of available commands. |
| exit |  |  | Exit from this configuration submenu to the upper level. |
| quit |  |  | Terminate this CLI session |
| set action reject | reject |  | Set rule type — reject call |
| set action send to destination | <DESTINATION_ID> | 1-65535 | Set rule type — send call to SIP destination with specified ID |
| set action send to trunk | <SBC_TRUNK_ID> | 1-65535 | Set rule type — send call to SBC trunk with specified ID |
| set condition all | <CONDITION> | 1-5 | Set condition with CONDITION number — all |
| set condition none | <CONDITION> | 1-5 | Clear condition with number CONDITION — all |

| | | | |
|---|---|---|---|
| `set condition type` | `<CONDITION_TYPE>`<br>`<CONDITION>`<br>`<CONDITION_MASK>` | `from-address-user-part/ from-address-host-part/ from-address-URI/ to-address-user-part/ to-address-host-part/ to-address-URI/ request-URI-user-part/ request-URI-host-part/ request-URI/ source-IP/ user-agent`<br>`1-5`<br>`String, 63 characters max.` | Set a condition of a certain type<br>from-address-user-part — name from the From header<br>from-address-host-part — domain from the From header<br>from-address-URI — URI from the From header<br>to-address-user-part — name from the To header<br>to-address-host-part — domain from the To header<br>to-address-URI — URI from the To header<br>request-URI-user-part — name from the request-URI<br>request-URI-host-part — domain from the request-URI<br>request-URI — URI from the request-URI<br>source-IP — source IP<br>user-agent — User-Agent header value<br>Rule number<br>Regular expression or IP address |
| `set drop diversion header` | `<ON_OFF>` | `on/off` | If this option is enabled, the Diversion header will not be sent to the destination |
| `set name` | `<SBC_RULE_NAME>` | `String, 63 characters max.` | Rule name |
| `set work time interval` | `<WORK_TIME_INTERVAL>` | `HH:MM-HH:MM where`<br>`HH = [00-23]`<br>`MM = [00-59]` | Set the time interval of the rule |
| `show info` | | | Show all rule settings |
| `show sip destination list` | | | Show all available SIP destination |
| `show trunk list` | | | Show available SBC trunk |

### *4.2.7.17 SIP destination list configuration*

To enter this mode, execute '**`sip destination`**' command in the configuration mode.

```
SBC1000-[CONFIG]> sip destination
Entering SBC SIP destination mode.
SBC1000-[CONFIG]-SIP-DESTINATION>
```

| Command | Parameter | Value | Action |
|---|---|---|---|
| `?` | | | Show the list of available commands. |
| `add destination with hostname` | `SIP_DESTINATION_NAME`<br>`SIP_TRANSPORT_ID`<br>`SIP_REMOTE_HOSTNAME` | `String, 63 characters max.`<br>`1-65535`<br>`String, 63 characters max. in format of: hostname/ hostname:port where port = 1-65535` | Add new SIP destination.<br>Set the name.<br>Set ID for the used SIP transport<br>Oncoming side domain and port. If no port is specified, port 5060 will be used. |
| `add destination with ip address` | | | Add new SIP destination. |

| | | | |
|---|---|---|---|
| | SIP_DESTINATION_NAME<br>SIP_TRANSPORT_ID<br>SIP_REMOTE_IP_ADDR | String, 63 characters max.<br>1-65535<br>AAA.BBB.CCC.DDD/ AAA.BBB.CCC.DDD:port where port = 1-65535 | Set the name.<br>Set ID for the used SIP transport<br>Oncoming side IP address and port. If no port is specified, port 5060 will be used. |
| edit destination id | PREFIX_SIGN | 0-65534 | Edit destination with selection by ID |
| edit destination index | PREFIX_SIGN | 1-65535 | Edit destination with selection by index |
| exit | | | Exit from this configuration submenu to the upper level. |
| quit | | | Terminate this CLI session |
| remove destination | SIP_DESTINATION_INDEX | 0-254 | Remove destination by index |
| remove by id destination | SIP_DESTINATION_ID | 1-65535 | Remove destination by ID |
| show info | | | Show list of all destination |
| show sip transport list | | | Show list of transports |

#### *4.2.7.18 SIP destination configuration*

To enter this mode, in the **`SIP destination`** list configuration mode, execute the **`edit destination <ID>`** or **`edit destination index <INDEX>`** command, where **`<ID>`** and **`<INDEX>`** — ID or index of the edited destination.

```
SBC1000-[CONFIG]-SIP-DESTINATION> edit destination id 12
Entering SBC SIP destination edit mode.
SBC1000-[CONFIG]-SIP-DESTINATION-ID[12]>
```

| Command | Parameter | Value | Action |
|---|---|---|---|
| ? | | | Show the list of available commands. |
| exit | | | Exit from this configuration submenu to the upper level. |
| quit | | | Terminate this CLI session |
| set adaptation | ADAPTATION | none/<br>HUAWEI-EchoLife/<br>Iskratel-SI3000/<br>HUAWEI-SoftX3000/<br>ZTE-Softswitch/<br>Nortel/<br>MTA-M-200 | Set the adaptation for this direction |
| set allow redirection | ON_OFF | on/off | Management of permissions for handling redirects |
| set auth login | AUTH_LOGIN | String, 63 characters max. | Authentication login |
| set auth password | AUTH_LOGIN | String, 63 characters max. | Authentication password |
| set auth remove | | | Clear authentication settings |
| set command line | CMDLINE | String | Set the advanced SIP settings rules |
| set const fromto domain | ON_OFF | on/off | Managing the «Pass the domain from FROM and TO headers» option |
| set convert flash | ON_OFF | on/off | Enable or disable conversion of Flash from RFC2833 to SIP INFO |
| set cps in | <MAX_CPS_IN> | 0-100 | Incoming maximum CPS value; 0 — option disabled |
| set cps out | <MAX_CPS_OUT> | 0-100 | Outgoing maximum CPS value; 0 — option disabled |

| | | | |
|---|---|---|---|
| set ignore source port | ON_OFF | on/off | Enable ignoring source port |
| set keep-alive server | KEEP_ALIVE_TIMEOUT_0_1000 | 0-1000 | Period of checking the operating server by OPTIONS messages |
| set keep-dead server | KEEP_ALIVE_TIMEOUT_5_1000 | 5-1000 | Period of checking the non-operating server by OPTIONS messages |
| set name | SIP_DESTINATION_NAME | String, 63 characters max. | Set SIP destination name |
| set preserve contact header | ON_OFF | on/off | Enable unchanged contact transmission |
| set remote address as hostname | SIP_REMOTE_HOSTNAME | String, 63 characters max. in format of:<br>hostname/<br>hostname:port<br>where<br>port = 1-65535 | Set the address of the counterparty as a domain. If no port is specified, port 5060 will be used |
| set remote address as ip | SIP_REMOTE_IP_ADDRESS | AAA.BBB.CCC.DDD/<br>AAA.BBB.CCC.DDD:port<br>where<br>port = 1-65535 | Set the address of the counterparty as an IP address. If no port is specified, port 5060 will be used. |
| set restriction deny-all | | | Set call restrictions — everything is restricted |
| set restriction maximum-sessions | MAXIMUM_SESSIONS | 1-65535 | Set call restrictions — maximum session number |
| set restriction no-restriction | | | Set call restrictions — without restriction |
| set rtcp timeout | TIMEOUT | 10-300/off | Set the RTCP waiting timeout from the counterparty.<br>off — disable RTCP waiting. |
| set rtp-loss timeout | TIMEOUT | 10-300/off | Set the RTP waiting timeout from the counterparty.<br>off — disable RTP waiting. |
| set rtp-loss multiplier on hold | TIMEOUT_MULTIPLIER | 1-30 | Set the RTP waiting multiplier in the on hold mode. |
| set rtp-loss multiplier silence-suppression | TIMEOUT_MULTIPLIER | 1-30 | Set the RTP waiting multiplier in the on silence suppression mode. |
| set rule set id | RULE_SET_ID | 1-65535 | Assign rule set |
| set rule set none | | | Remove rule set |
| set session-expires | SESSION_EXPIRES_OR_OFF | 90-64800/off | Requested period of session control according to RFC4028, seconds.<br>off — disables session control |
| set sip header format | SIP_HEADER_FORMAT | full/compact | Set SIP header format.<br>full — full format;<br>compact — compact format |
| set sip transport | SIP_TRANSPORT_ID | 1-65535 | Assign SIP transport |
| set transport protocol | SIP_TRANSPORT | UDP-only/<br>UDP-prefer/<br>TCP-prefer/<br>TCP-only | Assign transport protocol<br>UDP-only — UDP only;<br>UDP-prefer — UDP/TCP with UDP priority;<br>TCP-prefer — UDP/TCP with TCP priority;<br>TCP-only — TCP only |
| set trunk expires | EXPIRES | 0-65535 | Time of re-registration when using trunk registration |
| set trunk registration type | REGISTRATION_TYPE | none/<br>uac/<br>uas | Select trunk registration type<br>none — do not use trunk registration;<br>uac — register on counter device;<br>uas — receive registration from a counter device |
| set trunk sip domain | SIP_DOMAIN | String, 63 characters max. | SIP domain used for trunk registration |

|  |  |  |  |
|---|---|---|---|
| set trunk username/number | USERNAME_NUMBER | String, 63 characters max. | The user name used for registration |
| set verify media remote address | ON_OFF | on/off | Enable the RTP source IP and port control option |
| show info |  |  | Show settings |
| show rule set list |  |  | Show list of configured rule set |
| show sip transport list |  |  | Show list of available SIP transports |

#### *4.2.7.19 SIP transport configuration*

To enter this mode, execute '**sip transport**' command in the SIP transport list configuration mode.

```
SBC1000-[CONFIG]> sip transport
Entering SBC SIP transport mode.
SBC1000-[CONFIG]-SIP-TRANSPORT>
```

| Command | Parameter | Value | Action |
|---|---|---|---|
| ? |  |  | Show the list of available commands. |
| add transport | <br>SBC_SIP_TRANSPORT_NAME<br>IFACE_ID<br>PORT<br>RTP_IFACE_ID | <br>String, 63 characters max.<br>1-65535<br>1-65535<br>1-65535 | Add new SIP transport.<br>Set the name.<br>Set the ID of the interface used for SIP signaling<br>Set the port for signalling<br>Set the ID of the interface used for RTP |
| exit |  |  | Exit from this configuration submenu to the upper level. |
| quit |  |  | Terminate this CLI session |
| remove transport | SBC_SIP_TRANSPORT_INDEX | 0-254 | Remove destination by index |
| remove by id transport | SBC_SIP_TRANSPORT_ID | 1-65535 | Remove destination by ID |
| set by id name | <br>SBC_SIP_TRANSPORT_ID<br>SBC_SIP_TRANSPORT_NAME | <br>1-65535<br>String, 63 characters max. | Change the name of the transport by its ID<br>Transport ID<br>New transport name |
| set by id netiface | <br>SBC_SIP_TRANSPORT_ID<br>IFACE_ID | <br>1-65535<br>1-65535 | Change the network interface for SIP signalling<br>Transport ID<br>Network interface ID |
| set by id port | <br>SBC_SIP_TRANSPORT_ID<br>PORT | <br>1-65535<br>1-65535 | Change the port for signalling<br>Transport ID<br>Port for signalling |
| set by id rtp | <br>SBC_SIP_TRANSPORT_ID<br>RTP_IFACE_ID | <br>1-65535<br>1-65535 | Change the network interface for RTP<br>Transport ID<br>Network interface ID |
| set name |  |  | Change the name of the transport by its ID |

| | | | |
|---|---|---|---|
| | SBC_SIP_TRANSPORT_INDEX<br>SBC_SIP_TRANSPORT_NAME | 1-65535<br>String, 63 characters max. | Transport index<br>New transport name |
| set netiface | SBC_SIP_TRANSPORT_INDEX<br>IFACE_ID | 1-65535<br>1-65535 | Change the network interface for SIP signalling<br>Transport index<br>Network interface ID |
| set port | SBC_SIP_TRANSPORT_INDEX<br>PORT | 1-65535<br>1-65535 | Change the port for signalling<br>Transport index<br>Port for signalling |
| set rtp | SBC_SIP_TRANSPORT_INDEX<br>RTP_IFACE_ID | 1-65535<br>1-65535 | Change the network interface for RTP<br>Transport index<br>Network interface ID |
| show info | | | Show list of all transports |
| show net-ifaces | | | Show the list of network interfaces |

#### *4.2.7.20 SIP users list configuration*

To enter this mode, execute '**sip users**' command in the configuration mode.

```
SBC1000-[CONFIG]> sip users
Entering SBC SIP users mode.
SBC1000-[CONFIG]-SIP-USERS>
```

| Command | Parameter | Value | Action |
|---|---|---|---|
| ? | | | Show the list of available commands. |
| add user | SIP_USER_NAME<br>SIP_TRANSPORT_ID | String, 63 characters max.<br>1-65535 | Add new SIP users.<br>Set the name.<br>Set ID for the used SIP transport |
| edit user id | PREFIX_SIGN | 0-65534 | Edit user with selection by ID |
| edit user index | PREFIX_SIGN | 1-65535 | Edit user with selection by index |
| exit | | | Exit from this configuration submenu to the upper level. |
| quit | | | Terminate this CLI session |
| remove user | SIP_USER_INDEX | 0-254 | Remove user by index |
| remove by id user | SIP_USER_ID | 1-65535 | Remove user by ID |
| show info | | | Show list of all user |
| show sip transport list | | | Show list of transports |

#### *4.2.7.21 SIP users configuration*

To enter this mode, in the **SIP destination** list configuration mode, execute the **edit user <ID>** or **edit user index <INDEX>** command, where **<ID>** and **<INDEX>** — ID or index of the edited user.

```
SBC1000-[CONFIG]-SIP-USERS> edit user id 1
Entering SBC SIP user edit mode.
SBC1000-[CONFIG]-SIP-USER-ID[1]>

SBC1000-[CONFIG]-SIP-USERS> edit user index 0
Entering SBC SIP user edit mode.
SBC1000-[CONFIG]-SIP-USER-INDEX[0]>
```

| Command | Parameter | Value | Action |
|---|---|---|---|
| ? | | | Show the list of available commands. |
| exit | | | Exit from this configuration submenu to the upper level. |
| quit | | | Terminate this CLI session |
| set allow redirection | ON_OFF | on/off | Management of permissions for handling redirects |
| set command line | CMDLINE | String | Set the advanced SIP settings rules |
| set convert flash | ON_OFF | on/off | Enable or disable conversion of Flash from RFC2833 to SIP INFO |
| set name | SIP_USER_NAME | String, 63 characters max. | Set SIP user name |
| set nat keep-alive | KEEP_ALIVE | 0-65535 | Connection behind NAT storage time, sec |
| set nat subscribers | ON_OFF | on/off | Enables «subscriber behind NAT» mode |
| set preserve contact header | ON_OFF | on/off | Enable unchanged contact transmission |
| set radius profile id | RADIUS_PROFILE_ID | 1-65535 | Assign RADIUS profile |
| set radius profile none | | | Unassign RADIUS profile |
| set registration interval | REG_INTERVAL | 60-65535 | Set the permissible re-registration interval for users, sec |
| set restrictions non-registered deny-all | | | Set call restriction for unregistered users — everything is restricted |
| set restrictions non-registered maximum-sessions | MAXIMUM_SESSIONS | 1-65535 | Set call restriction for unregistered users — maximum session number |
| set restrictions non-registered no-restriction | | | Set call restriction for unregistered users — no restriction |
| set restrictions registered deny-all | | | Set call restriction for registered users — everything is restricted |
| set restrictions registered maximum-sessions | MAXIMUM_SESSIONS | 1-65535 | Set call restriction for registered users — maximum session number |
| set restrictions registered no-restriction | | | Set call restriction for registered users — no restriction |
| set rtcp timeout | TIMEOUT | 10-300/off | Set the RTCP waiting timeout from the counterparty.<br>off — disable RTCP waiting. |
| set rtp-loss timeout | TIMEOUT | 10-300/off | Set the RTP waiting timeout from the counterparty.<br>off — disable RTP waiting. |
| set rtp-loss multiplier on hold | TIMEOUT_MULTIPLIER | 1-30 | Set the RTP waiting multiplier in the on hold mode. |

| | | | |
|---|---|---|---|
| set rtp-loss multiplier silence-suppression | TIMEOUT_MULTIPLIER | 1-30 | Set the RTP waiting multiplier in the on silence suppression mode. |
| set rule set id | RULE_SET_ID | 1-65535 | Assign rule set |
| set rule set none | | | Remove rule set |
| set session-expires | SESSION_EXPIRES_OR_OFF | 90-64800/off | Requested period of session control according to RFC4028, seconds.<br>off — disables session control. |
| set sip domain | SIP_DOMAIN | String, 63 characters max. | Set the SIP domain with which to register |
| set sip header format | SIP_HEADER_FORMAT | full/compact | Set SIP header format.<br>full — full format;<br>compact — compact format. |
| set sip transport | SIP_TRANSPORT_ID | 1-65535 | Assign SIP transport |
| set transport protocol | SIP_TRANSPORT | UDP-only/<br>UDP-prefer/<br>TCP-prefer/<br>TCP-only | Assign transport protocol<br>UDP-only — UDP only;<br>UDP-prefer — UDP/TCP with UDP priority;<br>TCP-prefer — UDP/TCP with TCP priority;<br>TCP-only — TCP only. |
| set verify media remote address | ON_OFF | on/off | Enable the RTP source IP and port control option |
| show info | | | Show settings |
| show radius profile list | | | Show list of all configured RADIUS profiles |
| show rule set list | | | Show list of configured rule set |
| show sip transport list | | | Show list of available SIP transports |

#### 4.2.7.22 SNMP configuration mode

To enter this mode, you must execute the **snmp** command in the general configuration mode or in the network configuration mode.

```
SBC-[CONFIG]> snmp
Entering SNMP mode.
SBC-[CONFIG]-[NETWORK]-SNMP>

SBC-[CONFIG]-NETWORK> snmp
Entering SNMP mode.
SBC-[CONFIG]-[NETWORK]-SNMP> exit
```

| Command | Parameter | Value | Action |
|---|---|---|---|
| ? | | | Show the list of available commands. |
| add | &lt;TYPE&gt;<br>&lt;IP&gt;<br>&lt;COMM&gt;<br>&lt;PORT&gt; | trapsink/<br>trap2sink/<br>informsink<br>IP address in AAA.BBB.CCC.DDD format<br>string of up to 31 characters<br>1-65535 | Add SNMP trap transmission rule:<br>TYPE — SNMP message type<br>IP — trap receiver IP address;<br>COMM — password contained in traps;<br>PORT — trap receiver UDP port |
| config | | | Return to Configuration menu. |
| create user | &lt;LOGIN&gt; | string of up to 31 characters | Create a user (assign a login and password for access) |

| | | | |
|---|---|---|---|
| | <PASSWD> | password from 8 to 31 characters | |
| exit | | | Exit from this configuration submenu to the upper level. |
| history | | | View history of entered commands. |
| modify community | <IDX><br><COMM> | 0-15<br>string of up to 31 characters | Change the SNMP traps transmission rule (the password contained in the traps) |
| modify ip | <IDX><br><IP> | 0-15<br>IP address in AAA.BBB.CCC.DDD format | Change the SNMP trap transmission rule (trap receiver address) |
| modify port | <IDX><br><PORT> | 0-15<br>1-65535 | Change the SNMP trap transmission rule (trap receiver port) |
| modify type | <IDX><br><TYPE> | 0-15<br>trapsink/ trap2sink/ informsink | Change the SNMP trap transmission rule (SNMP message type) |
| quit | | | Terminate this CLI session |
| remove | <IDX> | 0-15 | Remove SNMP trap transmission rule |
| restart snmpd | Yes/no | | Restart SNMP client |
| ro | <RO> | string, 63 characters max. | Set the password for reading the parameters |
| rw | <RW> | string, 63 characters max. | Set the password for reading and recording the parameters |
| show | | | Show SNMP configuration |
| syscontact | <SYSCONTACT> | string, 63 characters max. | Specify contact information |
| syslocation | <SYSLOC> | string, 63 characters max. | Specify device location |
| sysname | <SYSNAME> | string, 63 characters max. | Specify device name |

#### *4.2.7.23 Switch parameter configuration mode*

To enter this mode, [1]execute '**switch**' command in the configuration mode.

```
SBC-[CONFIG]> switch
Entering switch control mode.
SBC-[CONFIG]-[SWITCH]>
```

| Command | Parameter | Value | Action |
|---|---|---|---|
| ? | | | Show the list of available commands. |
| 802.1q | | | Go to the 802.1q configuration mode. |
| apply mirroring settings | | no/yes | Apply mirroring settings |
| apply port settings | | no/yes | Apply port settings |
| confirm mirroring settings | | | Confirm mirroring settings You have 1 minute to confirm settings, or the previous values will be restored. |
| confirm port settings | | | Confirm port settings. You have 1 minute to confirm settings, or the previous values will be restored. |
| exit | | | Exit from this configuration submenu to the upper level. |
| history | | | View history of entered commands. |
| LACP[2] | | | Enter the LACP parameter configuration mode |

[1] Only for SBC-1000

[2] Not supported in the current firmware version

|  |  |  |  |
|---|---|---|---|
| QoS_control |  |  | Enter the QoS parameter configuration mode |
| quit |  |  | Terminate this CLI session |
| save mirroring |  |  | Save mirroring settings without applying |
| save vlan |  |  | Save VLAN settings without applying |
| set mirroring | &lt;PORT&gt;<br>&lt;NAME&gt;<br>&lt;ACT&gt; | GE_PORT0(0)/ GE_PORT1(1)/ GE_PORT2(2)/ CPU(4)/ SFP0(6)/ SFP1(7)<br>src_in/ src_out/ dst_in/ dst_out<br>on/off | Configure port mirroring:<br>PORT — port type;<br>NAME — port designation:<br>- *src_in* — incoming packet source port — copy frames received from this port (source port);<br>- *src_out* — outgoing packet source port — copy frames transmitted by this port (source port);<br>- *dst_in* — incoming packet destination port — receiver port for the copied frames received by the selected source ports;<br>- *dst_out* — outgoing packet destination port — receiver port for the copied frames transmitted by the selected source ports; |
| set port backup | &lt;ON_OFF&gt;<br>&lt;B_MASTER&gt;<br>B_SLAVE | on/off<br>GE_PORT0/GE_PORT1/ GE_PORT2/SFP0/SFP1<br>GE_PORT0/GE_PORT1/ GE_PORT2/SFP0/SFP1 | Enable Dual Homing redundancy<br>B_MASTER — main port<br>B_SLAVE — redundant port<br>PREEMPTION — enable/disable return to the main port when it is restored |
| set port default vlan id | &lt;PORT&gt;<br>&lt;VLANID&gt; | GE_PORT0(0)/ GE_PORT1(1)/ GE_PORT2(2)/ CPU(4)/ SFP0(6)/ SFP1(7)<br>0-4095 | Assign VLAN ID to this port. |
| set port egress | &lt;PORT&gt;<br>&lt;EGRESS&gt; | GE_PORT0(0)/ GE_PORT1(1)/ GE_PORT2(2)/ CPU(4)/ SFP0(6)/ SFP1(7)<br>unmodified/ untagged/ tagged/ double-tag | Set the packet transmission mode on this port.<br>EGRESS – packet transmission mode:<br>– *unmodified* — packets are transmitted by this port unchanged (i.e. in the same form as they came to the other port of the switch);<br>– *untagged* — packets will always be sent without VLAN tag by this port;<br>– *tagged* — packets will always be sent with VLAN tag by this port;<br>– *Double tag* — each packet will be sent with two VLAN tags — if received packet was tagged and came with one VLAN tag — if the received packet was untagged. |
| set port ieee mode | &lt;PORT&gt; | GE_PORT0(0)/ GE_PORT1(1)/ | Set the received tagged packet control mode for this port. |

| | | | |
|---|---|---|---|
| | | GE_PORT2(2)/<br>CPU(4)/<br>SFP0(6)/<br>SFP1(7) | |
| | <IEEE> | fallback/<br>check/<br>secure | IEEE — packet control mode:<br>— *Fallback* — if a packet with VLAN tag is received through this port, and there is a record in a routing table for this packet, then it falls within a scope of routing rules, specified in the record of this table; otherwise, routing rules specified in «egress» and «output» will be applied to it;<br>— *Check* — if a packet with VID is received through the port, and there is a record in a «802.1q» routing table for this packet, then it falls within a scope of routing rules, specified in the current record of this table, even if this port does not belong to the group of this VID. Routing rules specified in «egress» and «output» will not apply to this port;<br>— *Secure* — if a packet with VID is received through the port, and there is a record in a «802.1q» routing table for this packet, then it falls within a scope of routing rules, specified in the current record of this table; otherwise, it is rejected. Routing rules specified in «egress» and «output» will not apply to this port. |
| set port LACP_trunk[1] | <PORT> | CPU/<br>GE_PORT0/<br>GE_PORT1/<br>GE_PORT2/<br>SFP0/<br>SFP1 | Assign LACP trunk for the specified port. |
| | <LACP> | 0-4 | |
| set port MAC GE_PORT0 | <MACADDR> | MAC address in format of XX:XX:XX:XX:XX:XX | Specify MAC address for port |
| set port output | <PORT> | GE_PORT0/<br>GE_PORT1/<br>GE_PORT2/<br>CPU/<br>SFP0/<br>SFP1 | Setting permissible ports for sending packets<br>PORT — configurable port<br>P_DEST — permitted sending port |
| | <P_DEST> | GE_PORT0/<br>GE_PORT1/<br>GE_PORT2/<br>CPU/<br>SFP0/<br>SFP1 | |
| | <ENABLE> | on/off | |
| set port speed | <SPEED> | 1000M<br>100M (full-duplex/ half-duplex)<br>10M(full-duplex/ half-duplex)<br>auto | Set port operation mode |

[1] Not supported in the current firmware version

| | | | |
|---|---|---|---|
| | <PORT> | GE_PORT0/GE_PORT1/<br>GE_PORT2 | |
| set port vlan enabling | <PORT><br><ENABLE> | CPU/<br>GE_PORT0/<br>GE_PORT1/<br>GE_PORT2/<br>SFP0/<br>SFP1<br>on/off | Enable/disable VLAN on this port |
| set port vlan override | <PORT><br><OVER> | CPU/<br>GE_PORT0/<br>GE_PORT1/<br>GE_PORT2/<br>SFP0/<br>SFP1<br>on/off | Set the VLAN ID override mode for this port to standard |
| show mirror settings | | | Show port mirroring parameters |
| show port settings | | | Show port configuration parameters |

#### 4.2.7.23.1 802.1q parameter configuration mode

To enter this mode, execute '**802.1q**' command in the switch configuration mode.

```
SBC-[CONFIG]-[SWITCH]> 802.1q
Entering 802.1q_control mode.
SBC-[CONFIG]-[SWITCH]-[802.1q]>
```

| Command | Parameter | Value | Action |
|---|---|---|---|
| ? | | | Show the list of available commands. |
| add VTU element | <VID><br><PRIO><br><OVER><br><GE_PORT0><br><GE_PORT1><br><GE_PORT2><br><CPU><br><SFP0><br><SFP1> | 0-4095<br>0-7<br>on/off<br>unmodified/ untagged/ tagged/ not_member<br>unmodified/ untagged/ tagged/ not_member<br>unmodified/ untagged/ tagged/ not_member<br>unmodified/ untagged/ tagged/ not_member<br>unmodified/ untagged/ tagged/ not_member<br>unmodified/ untagged/ tagged/ not_member | Add new element to VTU table:<br>VID — VLAN identifier;<br>PRIO — 802.1p priority, assigned to packets in the given VLAN, if the *OVER* parameter is active (on);<br>OVER — overwrite 802.1p priority for the given VLAN (yes/no);<br>PORT — actions performed by this port when transmitting a packet with the specified VID:<br>– *Unmodified* — packets will be sent by the port without any changes;<br>– *Untagged* — packets will always be sent without VLAN tag by this port;<br>– *Tagged* — packets will always be sent with VLAN tag by this port;<br>– *Not member* — packets with specified VID will not be sent by this port (i.e. the port is not the member of VLAN) |
| apply | <YES_NO> | yes/no | Apply VTU settings |

| | | | |
|---|---|---|---|
| confirm | | | Confirm VTU settings. You have 1 minute to confirm settings, or the previous values will be restored. |
| exit | | | Return from this configuration submenu to the upper level. |
| QoS_control | | | Go to the QoS configuration mode |
| quit | | | Terminate this CLI session |
| remove VTU element | <NUMBER> | 0-4095 | Remove the given VTU table element |
| save | | | Save VTU settings without applying |
| set VTU override | <NUMBER><br><OVER> | 0-4095<br>on/off | Overwrite/ not overwrite 802.1p priority for the given VLAN (yes/no) |
| set VTU priority | <NUMBER><br><PRIO> | 0-4095<br>0-7 | Set the 802.1p priority assigned to packets on this VLAN if the «set VTU override» parameter is active |
| set VTU settings_CPU | <NUMBER><br><CPU> | 0-4095<br>unmodified/ untagged/ tagged/ not_member | Assign actions performed by this port when transmitting a packet with the specified VID<br>– *Unmodified* — packets will be sent by the port without any changes;<br>– *untagged* — packets will always be sent without VLAN tag by this port;<br>– *tagged* — packets will always be sent with VLAN tag by this port;<br>– *Not member* — packets with specified VID will not be sent by this port (i.e. the port is not the member of VLAN) |
| settings_GE_PORT0 | <NUMBER><br><CPU> | 0-4095<br>unmodified/ untagged/ tagged/ not_member | Assign actions performed by this port when transmitting a packet with the specified VID<br>– *Unmodified* — packets will be sent by the port without any changes;<br>– *untagged* — packets will always be sent without VLAN tag by this port;<br>– *tagged* — packets will always be sent with VLAN tag by this port;<br>– *Not member* — packets with specified VID will not be sent by this port (i.e. the port is not the member of VLAN) |
| settings_GE_PORT1 | <NUMBER><br><CPU> | 0-4095<br>unmodified/ untagged/ tagged/ not_member | Assign actions performed by this port when transmitting a packet with the specified VID:<br>– *Unmodified* — packets will be sent by the port without any changes;<br>– *untagged* — packets will always be sent without VLAN tag by this port;<br>– *tagged* — packets will always be sent with VLAN tag by this port;<br>– *Not member* — packets with specified VID will not be sent by this port (i.e. the port is not the member of VLAN) |
| settings_GE_PORT2 | <NUMBER><br><CPU> | 0-4095<br>unmodified/ | Assign actions performed by this port when transmitting a packet with the specified VID: |

| | | | |
|---|---|---|---|
| | | untagged/<br>tagged/<br>not_member | — *Unmodified* — packets will be sent by the port without any changes;<br>— *untagged* — packets will always be sent without VLAN tag by this port;<br>— *tagged* — packets will always be sent with VLAN tag by this port;<br>— *Not member* — packets with specified VID will not be sent by this port (i.e. the port is not the member of VLAN) |
| settings_SFP0 | <NUMBER><br><CPU> | 0-4095<br>unmodified/<br>untagged/<br>tagged/<br>not_member | Assign actions performed by this port when transmitting a packet with the specified VID:<br>— *Unmodified* — packets will be sent by the port without any changes;<br>— *untagged* — packets will always be sent without VLAN tag by this port;<br>— *tagged* — packets will always be sent with VLAN tag by this port;<br>— *Not member* — packets with specified VID will not be sent by this port (i.e. the port is not the member of VLAN) |
| settings_SFP1 | <NUMBER><br><CPU> | 0-4095<br>unmodified/<br>untagged/<br>tagged/<br>not_member | Assign actions performed by this port when transmitting a packet with the specified VID:<br>— *Unmodified* — packets will be sent by the port without any changes;<br>— *untagged* — packets will always be sent without VLAN tag by this port;<br>— *tagged* — packets will always be sent with VLAN tag by this port;<br>— *Not member* — packets with specified VID will not be sent by this port (i.e. the port is not the member of VLAN) |
| show list | | | Show list of item in VTU table |
| show one | <NUMBER> | 0-4095 | Show information about the given VTU table item |
| show table | | | Show VTU table |

#### 4.2.7.23.2 QoS parameter configuration mode

To enter this mode, execute '**`QoS_control`**' command in the switch or 802.1q configuration mode.

```
SBC-[CONFIG]-[SWITCH]> QoS_control
Entering QoS_control mode.
SBC-[CONFIG]-[SWITCH]-[QoS]>
```

| Command | Parameter | Value | Action |
|---|---|---|---|
| ? | | | Show the list of available commands. |
| 802.1q | | | Return to the 802.1q parameter configuration mode |
| apply | <YES_NO> | yes/no | Apply QoS settings |

|  |  |  |  |
|---|---|---|---|
| confirm | | | Confirm QoS settings. You have 1 minute to confirm settings, or the previous values will be restored. |
| exit | | | Return from this configuration submenu to the upper level. |
| quit | | | Terminate this CLI session |
| save | | | Save QoS settings without applying |
| set 802.1p_prio_mapping | <PRIO><br><QUEUE> | 0-7<br>0-3 | Distribute packets into queues depending on the 802.1p priority.<br>PRIO — 802.1p priority number;<br>QUEUE — queue number |
| set default_VLAN_priority | <PORT><br><DEFPRIO> | GE_PORT0(0)/<br>GE_PORT1(1)/<br>GE_PORT2(2)/<br>CPU(4)/<br>SFP0(6)/<br>SFP1(7)<br>0-7 | Assign 802.1p priority to untagged packets received on this port. If 802.1p or IP diffserv priority is already assigned to the packet, this setting will not be used ('default vlan priority' will not be applied to packets containing IP header, when one of the QoS modes is in use: DSCP only, DSCP preferred, 802.1p preferred, and also to untagged packets) |
| set diffserv_prio_mapping | <NUMBER><br><QUEUE> | *1<br>0-3 | Distribute packets into queues depending on the IP diffserv priority.<br>NUMBER — IP diffserv priority number;<br>QUEUE — queue number |
| set egress_limit | <PORT><br><EGRLIM> | GE_PORT0(0)/<br>GE_PORT1(1)/<br>GE_PORT2(2)/<br>CPU(4)/<br>SFP0(6)/<br>SFP1(7)<br>on/off | Enable/disable bandwidth limit for outgoing traffic from this port |
| set egress_rate_limit | <PORT><br><EGRRATE> | GE_PORT0(0)/<br>GE_PORT1(1)/<br>GE_PORT2(2)/<br>CPU(4)/<br>SFP0(6)/<br>SFP1(7)<br>0-250000 | Set the bandwidth limit (kbit/s) for outgoing traffic from this port |
| set ingress_limit_mode | <PORT><br><INGRMODE> | GE_PORT0(0)/<br>GE_PORT1(1)/<br>GE_PORT2(2)/<br>CPU(4)/<br>SFP0(6)/<br>SFP1(7)<br>off/<br>all/<br>mult_flood_broad/<br>mult_broad/<br>broad | Set restriction mode for traffic coming to the port<br>INGRMODE — restriction mode:<br>– *off* — no restriction;<br>– *all* — all traffic is restricted;<br>– *mult_flood_broad* — multicast, broadcast, and flooded unicast traffic will be restricted;<br>– *mult_broad* — multicast and broadcast traffic will be restricted;<br>– *broad* — only broadcast traffic will be restricted |
| set ingress_rate_ prio_0/1/2/3 | <PORT> | GE_PORT0(0)/<br>GE_PORT1(1)/<br>GE_PORT2(2)/<br>CPU(4)/<br>SFP0(6)/ | Set a bandwidth limit (kbps) for traffic arriving on this port for zero/first/second/third queue. |

|  |  |  |  |
|---|---|---|---|
|  | <INGPRIO> | SFP1(7)<br>0-250000 |  |
| set QoS_mode | <PORT><br><QOSMODE> | GE_PORT0(0)/<br>GE_PORT1(1)/<br>GE_PORT2(2)/<br>CPU(4)/<br>SFP0(6)/<br>SFP1(7)<br>DSCP_only/<br>802.1p_only/<br>DSCP_preferred/<br>802.1p_preferred | Set QoS usage mode.<br>QOSMODE — usage mode:<br>– *DSCP only* — distribute packets into queues based on IP diffserv priority only;<br>– *802.1p only* — distribute packets into queues based on 802.1p priority only;<br>– *DSCP preferred* — distribute packets into queues based on IP diffserv and 802.1p priorities, if both priorities are present in the packet, IP diffserv priority is used for queuing purposes;<br>– *802.1p preferred* — distribute packets into queues based on IP diffserv and 802.1p priorities, if both priorities are present in the packet, 802.1p priority is used for queuing purposes. |
| set remapping_priority | <PORT><br><NUM><br><REMAP> | GE_PORT0(0)/<br>GE_PORT1(1)/<br>GE_PORT2(2)/<br>CPU(4)/<br>SFP0(6)/<br>SFP1(7)<br>0-7<br>0-7 | Remap 802.1p priorities for tagged packets<br>PORT — configurable port;<br>NUM — current priority value;<br>REMAP — new value. |
| show QOS | <PORT> | GE_PORT0(0)/<br>GE_PORT1(1)/<br>GE_PORT2(2)/<br>CPU(4)/SFP0(6)/<br>SFP1(7) | Show QoS configuration parameters for the given port |
| show QOS_diffserv |  |  | Show parameters for distribution of packets into queues depending on the IP diffserv priority |
| show QOS_priomap |  |  | Show parameters for distribution of packets into queues depending on the 802.1p priority |

#### *4.2.7.24 Syslog parameter configuration mode*

To enter this mode, execute '**`syslog`**' command in the configuration mode.

```
SBC-[CONFIG]> syslog
Entering syslog mode.
SBC-[CONFIG]-SYSLOG>
```

| Command | Parameter | Value | Action |
|---|---|---|---|
| ? |  |  | Show the list of available commands. |
| authlog set | IP<br>PORT<br>ONOFF<br>LOCREM | IP address in AAA.BBB.CCC.DDD format<br>1-65535<br>off/on<br>local/remote | Set the address of the server to send syslog messages, as well as operation mode.<br>on/off — enable/disable logging;<br>local/remote — if set to remote, send logs to the syslog server. |
| authlog show |  |  | Show current logging parameters |
| config |  |  | Return to Configuration menu. |

| | | | |
|---|---|---|---|
| dispatcher | DISPATCHER | 0-99 | Enable Dispatcher tracing |
| exit | | | Return from this configuration submenu to the upper level. |
| manager | MANAGER | 0-99 | Enable Manager tracing |
| quit | | | Terminate this CLI session |
| show | | | Show information on Syslog configuration |
| start | | | Enable data transmission to the syslog server |
| stop | | | Disable data transmission to the syslog server |
| userlog | <IPADDR><br><PORT><br><MODE> | IP address in AAA.BBB.CCC.DDD format<br>1-65535<br>off/standart/full | Enable output of the history of entered commands<br>IPADDR — syslog server IP address<br>PORT — Syslog server port<br>MODE — detail level of the entered commands log<br>*off* — disable entered commands logs generation;<br>Standart — messages contain the name of modified parameter;<br>*Full* — messages contain the name of modified parameter as well as parameter values before and after the modification. |
| worker | WORKER | 0-99 | Enable Worker tracing |

### *4.2.7.25 SBC Trunk configuration mode*

To enter this mode, execute '**trunk**' command in the configuration mode.

SBC1000-[CONFIG]> trunk
Entering SBC trunk mode.
SBC1000-[CONFIG]-TRUNK>

| Command | Parameter | Value | Action |
|---|---|---|---|
| ? | | | Show the list of available commands. |
| add trunk | SBC_TRUNK_NAME<br>LOAD_BALANCE_MODE<br>LOAD_BALANCE_TIMEOUT | String, 63 characters max.<br>active-active/ active-backup<br>5-65535 | Add new SBC Trunk<br>Trunk name<br>Balancing mode<br>Balancing timeout, sec |
| exit | | | Return from this configuration submenu to the upper level. |
| quit | | | Terminate this CLI session |
| remove by id destination primary | SBC_TRUNK_ID | 1-65535 | Remove main destination from trunk by ID |
| remove by id destination secondary | SBC_TRUNK_ID | 1-65535 | Remove redundant destination from trunk by ID |
| remove by id trunk | SBC_TRUNK_ID | 1-65535 | Remove SBC trunk by its ID |
| remove destination primary | SBC_TRUNK_ID | 0-65534 | Remove main destination from trunk by index |
| remove destination secondary | SBC_TRUNK_ID | 0-65534 | Remove redundant destination from trunk by index |
| remove trunk | SBC_TRUNK_ID | 0-65534 | Remove SBC trunk by its index |
| set by id destination primary | SBC_TRUNK_ID<br>SBC_SIP_DESTINATION_ID | 1-65535<br>1-65535 | Assign main destination to trunk by ID |

| | | | |
|---|---|---|---|
| set by id destination secondary | SBC_TRUNK_ID<br>SBC_SIP_DESTINATION_ID | 1-65535<br>1-65535 | Assign redundant destination to trunk by ID |
| set by id load balance mode | SBC_TRUNK_ID<br>LOAD_BALANCE_MODE | 1-65535<br>active-active/ active-backup | Assign balancing mode by trunk ID |
| set by id load balance timeout | SBC_TRUNK_ID<br>LOAD_BALANCE_TIMEOUT | 1-65535<br>5-65535 | Assign balancing timeout by trunk ID, sec |
| set by id name | SBC_TRUNK_ID<br>SBC_TRUNK_NAME | 1-65535<br>String, 63 characters max. | Assign name to trunk by its ID |
| set destination primary | SBC_TRUNK_INDEX<br>SBC_SIP_DESTINATION_ID | 0-65534<br>1-65535 | Assign main destination to trunk by index |
| set destination secondary | SBC_TRUNK_INDEX<br>SBC_SIP_DESTINATION_ID | 0-65534<br>1-65535 | Assign redundant destination to trunk by index |
| set load balance mode | SBC_TRUNK_INDEX<br>LOAD_BALANCE_MODE | 0-65534<br>active-active/ active-backup | Assign balancing mode by trunk index |
| set load balance timeout | SBC_TRUNK_INDEX<br>LOAD_BALANCE_TIMEOUT | 0-65534<br>5-65535 | Assign balancing timeout by trunk index, sec |
| set name | SBC_TRUNK_INDEX<br>SBC_TRUNK_NAME | 0-65534<br>String, 63 characters max. | Assign name to trunk by its index |
| show info | | | Show settings |
| show sip destination list | | | Show list of available SIP destination |
| swap by id destination | SIP_TRUNK_ID | 1-65535 | Swap main and redundant destination in the specified trunk |
| swap destination | SIP_TRUNK_INDEX | 0-65534 | Swap main and redundant destination in the specified trunk |

#### *4.2.7.26 Configuring the list of restricted client applications*

To enter this mode, execute '**user agent**' command in the configuration mode.

```
SBC1000-[CONFIG]> user agent
Entering SBC user agent mode.
SBC1000-[CONFIG]-USER-AGENT>
```

| Command | Parameter | Value | Action |
|---|---|---|---|
| ? | | | Show the list of available commands. |
| add | USER_AGENT | scan/<br>crack/<br>flood/<br>kill/<br>sipcli/<br>sipvicious/<br>sipsak/<br>sundayddr/<br>iWar/<br>SIVuS/<br>Gulp/<br>sipv/<br>smap/ | Add one of the preset User-Agents to the block list |

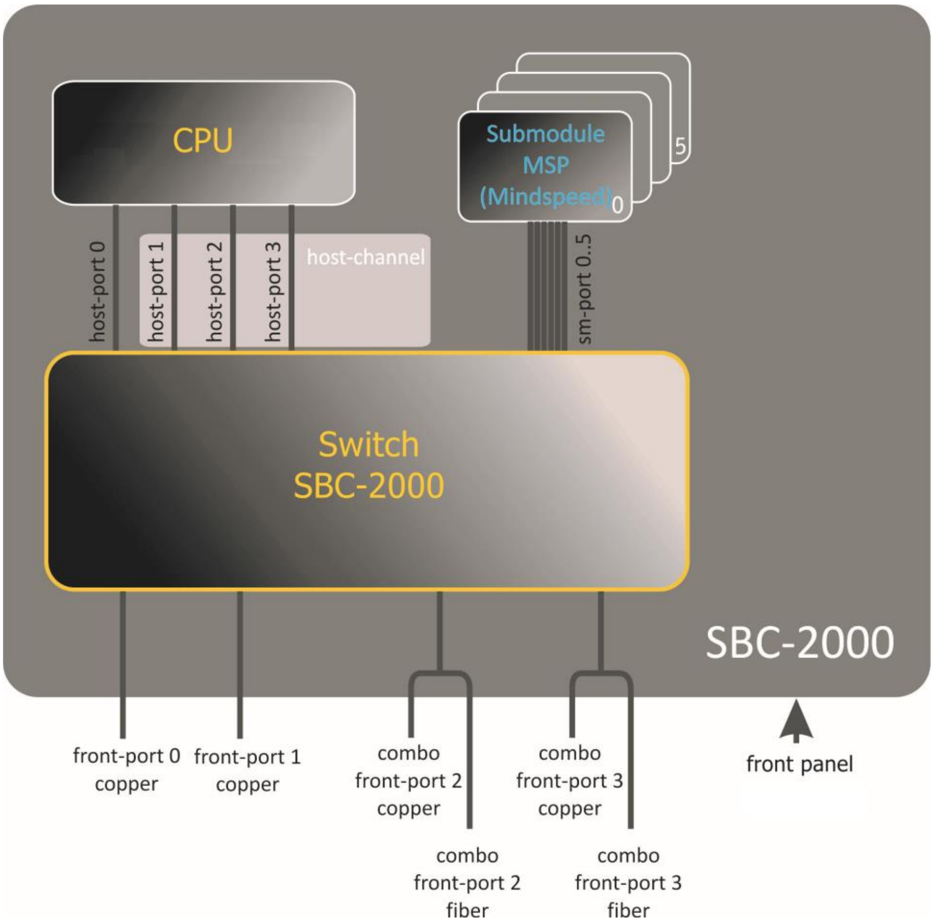
| | | | |
|---|---|---|---|
| | | friendly-request/<br>VaxIPUserAgent/<br>VaxSIPUserAgent/<br>siparmyknife/<br>Test_Agent/<br>SIPBomber/<br>Siprogue | |
| add other | USER_AGENT_NAME | String, 31 characters max. | Add your User-Agent mask to the list |
| exit | | | Return from this configuration submenu to the upper level. |
| quit | | | Terminate this CLI session |
| remove by id user agent | USER_AGENT_ID | 1-65535 | Remove User-Agent from list by its ID |
| remove user agent | USER_AGENT_INDEX | 0-65534 | Remove User-Agent from list by its index |
| show | | | Show configured list |

## 4.3 SBC-2000 switch configuration

The configuration is performed from the switch configuration mode.

```
SBC2000> config
Entering configuration mode.
SBC2000-[CONFIG]> switch
SBC2000-[CONFIG]-[SWITCH]>
```

### 4.3.1 *Switch structure*



SBC-2000 switch has the following interfaces:

- *front-port* — external ethernet ports of the switch, which are brought out on the front panel.

  Possible values: 0 - 3.

  - ports 0 .. 1 — copper ports
  - ports 2 .. 3 — optical and copper combo ports.

- *port-channel* — LAG aggregation groups of switch front-port interfaces, used when multiple front-ports are combined into a LACP group.

  Possible values: 1 — 4.

- *host-port* — internal ports of the SMG-2016 switch intended for communication with the SMG-2016 processor (CPU).

  Possible values: 0 - 2.

- *host-channel* — LAG host-channel interface aggregation group of the switch, this group is always active.

Possible value: 1.

- *sm-port* — internal ports of the SBC-2000 switch designed to communicate with SM-VP submodules.

  Possible values: 0 – 5.

When working with the switch, a unit number value of 1 is used.

### 4.3.2 *SBC-2000 switch interface management commands*

#### *interface*

This command allows entering the configuration mode of the SBC-2000 switch interfaces.

**Syntax**

interface <interface> <number>

**Parameters**

<interface> — interface type:

- front-port — external switch interfaces;
- host-channel — LAG host-channel interfaces aggregation groups of the switch;
- port-channel — LAG aggregation groups of the switch's external interfaces;

<number> — port number:

- for front-port: <unit/port>, where
  - unit — SBC-2000 module number, always is 1;
  - port — port number, may take values: [0 .. 3];
- for host-channel: 1;
- for port-channel: [1 .. 4].

The <number> parameter can take the 'all' value to configure all ports of the same interface type at once.

#### *shutdown*

This command disables an interface being configured.

The use of a negative form of the command enables the interface being configured.

**Syntax**

[no] shutdown

**Parameters**

Command contains no arguments.

**Example**

```
SBC2000-[CONFIG]-[SWITCH]-[if]> shutdown
```

The configurable interface disabled

#### *bridging to*

This command sets permission for traffic transfer between interfaces.

The use of the negative form of the command sets prohibition for traffic transfer between interfaces.

**Syntax**

[no] bridging to <interface> <range>

**Parameters**

<interface> — interface type:

- cpu-port;
- front-port — external uplink interfaces;
- host-channel;
- host-port;
- port-channel — LAG uplink interface aggregation groups;
- sm-port.

<range> — number of the port/ports with which traffic exchange is allowed:

- for cpu-port: <1/0>, where:
- for front-port: <unit/port>, where:
  - unit — module number, may take value [1],
  - port — port number, may take values: [0 .. 3];
- for host-channel: [1];
- for host-port:
  - unit — module number, may take value [1],
  - port — port number, may take values: [0 .. 2];
- for port-channel: [0 .. 4];
- for sm-port: [0 .. 15].
  - unit — module number, may take value [1],
  - port — port number, may take values: [0 .. 5].

**Example**

```
SBC2000-[CONFIG]-[SWITCH]-[if]> bridging to front-port all
```

### *flow-control*

This command enables/disables the flow control mechanism on the interface to be configured. The flow control mechanism makes it possible to compensate for differences in transmitter and receiver speeds. If the traffic amount exceeds a certain level, the receiver will transmit frames informing the transmitter of the need to reduce the amount of traffic to reduce the number of lost packets. To implement this mechanism, it is necessary that the remote device also supports this function.

**Syntax**

flow-control <act>

**Parameters**

<act> — allocated action:

- on — enable;
- off — disable.

**Default value**

off

#### Example

```
SBC2000-[CONFIG]-[SWITCH]-[if]> flow-control on
```

### *frame-types*

The command allows assigning specific rules for receiving packets for the interface:

- receive tagged and untagged packages;
- receive only packets with VLAN tag.

#### Syntax

frame-types <act>

#### Parameters

<act> — allocated action:

- all — receive tagged and untagged packages;
- tagged — receive only packets with VLAN tag.

#### Default value

receive all packets (tagged and untagged)

#### Example

```
SBC2000-[CONFIG]-[SWITCH]-[if]> frame-types all
```

Untagged traffic is allowed on configured ports.

### *speed*

The command sets speed value for interface being configured.

The command set the following modes: 10 Mbps, 100 Mbps, 1000 Mbps. When setting 10 Mbps, 100 Mbps, you must specify the mode of the transceiver: duplex, half-duplex.

#### Syntax

speed <rate> [<mode>]

#### Parameters

<rate> — rate value: 10M; 100M; 1000 Mbps;

<mode> — mode of the transceiver:

- full-duplex — duplex;
- half-duplex — half-duplex.

#### Example

```
SBC2000-[CONFIG]-[SWITCH]-[if]> speed 10M full-duplex
```

10 Mbps speed limit is set, duplex.

### *speed auto*

The command sets speed value for interface being configured automatically.

**Syntax**

speed auto

**Parameters**

Command contains no arguments.

**Example**

```
SBC2000-[CONFIG]-[SWITCH]-[if]> speed auto
```

The speed for the port will be set automatically.

### *show interfaces configuration*

This command is used to view the configuration of the SBC-2000 switch interfaces

**Syntax**

show interfaces configuration <interface> <number>

**Parameters**

<interface> — interface type:

- front-port — external uplink interfaces;
- host-channel;
- host-port;
- port-channel — external LAG uplink interface aggregation groups;
- sm-port.

<number> — port number:

- all — all ports of the selected interface;
- for front port: <unit/port>, where:
  - unit — module number, may take value [1],
  - port — port number, may take values: [0 .. 3];
- for host-channel: [1];
- for host-port:
  - unit — module number, may take value [1],
  - port — port number, may take values: [0 .. 2];
- for port-channel: [0 .. 4].
- for sm-port: [0 .. 15].
  - unit — module number, may take value [1],
  - port — port number, may take values: [0 .. 5].

**Example**

```
SBC2000-[CONFIG]-[SWITCH]> show interfaces configuration front-port all
Port                 Duplex   Speed      Neg        Flow      Admin
                                                    control   State
------------------   ------   --------   --------   -------   -----
front-port   1/0     Full     10 Mbps    Enabled    Off       Up
front-port   1/1     Full     10 Mbps    Disabled   Off       Up
front-port   1/2     Full     10 Mbps    Enabled    Off       Up
front-port   1/3     Full     10 Mbps    Enabled    Off       Up
SBC2000-[CONFIG]-[SWITCH]>
```

### *show interfaces status*

This command allows viewing information about the status of an interface, a group of interfaces.

**Syntax**

show interfaces status <interface> <number>

**Parameters**

<interface> — interface type:

- front-port — external uplink interfaces;
- host-channel
- host-port    ;
- port-channel — external LAG uplink interface aggregation groups;
- sm-port

<number> — port number:

- all — all ports of the selected interface;
- for front port: <unit/port>, where:
  - unit — module number, may take value [1],
  - port — port number, may take values: [0 .. 3];
- for host-channel: [1];
- for host-port:
  - unit — module number, may take value [1],
  - port — port number, may take values: [0 .. 2];
- for port-channel: [0 .. 4].
- for sm-port:
  - unit — module number, may take value [1],
  - port —  port number, may take values: [0 .. 5].

**Example**

```
SBC2000-[CONFIG]-[SWITCH]> show interfaces status front-port all
Port                Media     Duplex   Speed      Neg        Flow      Link    Back
                                                             control   State   Pressure
------------------  -------   ------   --------   --------   -------   -----   --------
front-port   1/0    N/A       N/A      N/A        N/A        N/A       Down    N/A
front-port   1/1    copper    Full     10 Mbps    Disabled   Off       Up      Disabled
front-port   1/2    copper    Full     100 Mbps   Enabled    Off       Up      Disabled
front-port   1/3    N/A       N/A      N/A        N/A        N/A       Down    N/A
SBC2000-[CONFIG]-[SWITCH]>
```

### *show interfaces counters*

This command allows viewing the counters of an interface or group of interfaces.

**Syntax**

show interfaces counters <interface> <number>

**Parameters**

<interface> — interface type:

- cpu-port;
- front-port — external uplink interfaces;
- host-channel;
- host-port;
- port-channel — LAG uplink interface aggregation groups;
- sm-port.

<range> — number of the port/ports with which traffic exchange is allowed:

- for cpu-port: <1/0>, where:
- for front-port: <unit/port>, where:
  - unit — module number, may take value [1],
  - port — port number, may take values: [0 .. 3];
- for host-channel: [1];
- for host-port:
  - unit — module number, may take value [1],
  - port — port number, may take values: [0 .. 2];
- for port-channel: [0 .. 4].
- for sm-port:
  - unit — module number, may take value [1],
  - port — port number, may take values: [0 .. 5].

**Example**

```
SBC2000-[CONFIG]-[SWITCH]> show interfaces counters front-port all

   MAC MIB counters receive
   ~~~~~~~~~~~~~~~~~~~~~~~~
Port            UC recv           MC recv          BC recv           Octets recv
---------------------------------------------------------------------------------
front-port 1/0         0              0               0                     0
front-port 1/1    436940           6297            9289              65685375
front-port 1/2   1422764           6077           41999             210652881
front-port 1/3         0              0               0                     0

   MAC MIB counters sent
   ~~~~~~~~~~~~~~~~~~~~~
Port            UC sent           MC sent           BC sent           Octets sent
---------------------------------------------------------------------------------
front-port 1/0        0                 0                 0                   0
front-port 1/1   455819              6087             42006            96955149
front-port 1/2   148842              6280              9296            17450454
front-port 1/3        0                 0                 0                   0
```

### 4.3.3 *Aggregation group configuration commands*

#### *channel-group*

This command adds FRONT-PORT interfaces to the aggregation group.

The use of the negative form of the command (no) removes FRONT-PORT interface from the aggregation group.

**Syntax**

channel-group <id> [force]

no channel-group

**Parameters**

<id> — sequence number of the aggregation group, to which the port will be added, takes values [1 ... 4];

- [force] — optional parameter, may take value;
- force — means being compatible with the rest of the group.

**Example**

```
SBC2000-[CONFIG]-[SWITCH]-[if]> channel-group 1
```

All uplink ports are combined in group 1.

#### *lacp mode*

This command allows you to select the channel aggregation mode:

- Passive — switch does not initiate creation of a logical link, but processes incoming LACP packets;
- Active — in this mode it is necessary to form an aggregated communication line and initiate negotiation.

Connection of communication lines is formed if the other side works in LACP active or passive modes.

The use of the negative form of the command (no) sets the default channel aggregation mode.

**Syntax**

lacp mode <name>

no lacp mode

**Parameters**

<name> — mode:

- active;
- passive.

**Default value**

active

**Example**

```
SBC2000-[CONFIG]-[SWITCH]-[if]> lacp mode active
```

The channel aggregation mode «active» is enabled on the configurable ports.

### *lacp port-priority*

This command sets the priority for the configurable port. The priority is set in the range [1 .. 65535]. 1 is the highest priority.

The use of a negative form (no) of the command sets the default priority value.

**Syntax**

lacp port-priority <priority>

no lacp port-priority

**Parameters**

<PRIORITY> — the priority for this port is [0 .. 65535].

**Default value**

all ports are set to priority 32768

**Command mode**

INTERFACE FRONT-PORT

**Example**

```
SBC2000-[CONFIG]-[SWITCH]-[if]> lacp port-priority 256
```

Port 256 priority is set on the configurable ports.

### *lacp rate*

This command sets the transmission interval of control packets of LACPDU protocol.

The use of the negative form of the command (no) sets the transmission interval of control packets of the LACPDU protocol by default.

**Syntax**

lacp rate <rate>

no lacp rate

**Parameters**

<rate> — transmission interval:

- fast — transmission interval is 1 second;
- slow — transmission interval is 1 second.

**Default value**

1 seconds (fast)

**Command mode**

INTERFACE FRONT-PORT

**Example**

```
SBC2000-[CONFIG]-[SWITCH]-[if]> lacp rate slow
```

LACPDU control packets transmission interval is set to 30 seconds.

## 4.3.4 *VLAN interface management commands*

### *pvid*

This command sets the default VID value for packets received by the port.

When an untagged packet or a packet with VID value in the VLAN tag equal to 0 is received, the packet is assigned a VID value equal to PVID.

**Syntax**

pvid <num>Parameters

<num> — VLAN port ID number, specified in the range [1 ... 4094].

**Default value**

PVID = 1

**Command mode**

INTERFACE FRONT-PORT

INTERFACE PORT-CHANNEL

**Example**

```
SBC-2000-[CONFIG]-[SWITCH]-[if]> pvid 5
```

PVID 5 is assigned to the configured port.

## 4.3.5 *STP/RSTP configuartion commands*

### *spanning-tree enable*

This command enables the STP function on the interface to be configured.

The use of the negative form of the command (no) forbids STP on interface.

**Syntax**

[no] spanning-tree enable

**Parameters**

Command contains no arguments.

**Command mode**

INTERFACE FRONT-PORT

INTERFACE PORT-CHANNEL

**Example**

```
SBC2000-[CONFIG]-[SWITCH]-[if]> spanning-tree enable
```

The STP feature is enabled for all front-port.

### *spanning-tree pathcost*

This command sets the value of the STP path for the configurable interface.

The use of a negative form (no) of the command sets the default path cost value.

The default value is 0.

**Syntax**

spanning-tree pathcost <pathcost>

no spanning-tree pathcost

**Parameters**

<pathcost> — path cost, may take values [0.. 200000000].

**Default value**

path cost value = 0

**Command mode**

INTERFACE FRONT-PORT

INTERFACE PORT-CHANNEL

**Example**

```
SBC2000-[CONFIG]-[SWITCH]-[if]> spanning-tree pathcost 1
```

Path cost 1 is set.

### *spanning-tree priority*

This command sets the STP priority for the configurable port.

The use of a negative form (no) of the command sets the default STP operation priority. 128 is set by default.

**Syntax**

spanning-tree priority <priority>

no spanning-tree priority

**Parameters**

<priority> — priority, takes values in multiples of 16 [0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240].

**Default value**

128

**Command mode**

INTERFACE FRONT-PORT

INTERFACE PORT-CHANNEL

**Example**

```
SBC2000-[CONFIG]-[SWITCH]-[if]> spanning-tree priority 144
```

Priority 144 is set.

### *spanning-tree admin-edge*

This command sets the connection type as an edge link to the host. In this case, data transmission is enabled automatically for the interface, when the link is established.

The use of a negative form (no) of the command restores the default value.

**Syntax**

[no] spanning-tree admin-edge

**Parameters**

Command contains no arguments.

**Default value**

off

**Command mode**

INTERFACE FRONT-PORT

INTERFACE PORT-CHANNEL

**Example**

```
SBC2000-[CONFIG]-[SWITCH]-[if]> spanning-tree admin-edge
```

For the configured port, the type of edge-link connection is enabled.

### *spanning-tree admin-p2p*

This command defines the type of p2p connection definition.

The use of a negative form (no) of the command sets the default p2p connection definition type.

**Syntax**

spanning-tree admin-p2p <type>
no spanning-tree admin-p2p

**Parameters**

<type> — connection definition type:

- auto — the definition is based on BPDU;
- force-false — forced link as a non p2p;
- force-true — forced link as a p2p.

**Default value**

p2p connection type is determined based on BPDU

**Command mode**

INTERFACE FRONT-PORT
INTERFACE PORT-CHANNEL

**Example**

```
SBC2000-[CONFIG]-[SWITCH]-[if]> spanning-tree admin-p2p auto
```

For the configured port, the connection type p2p is defined on the basis of BPDU.

### *spanning-tree auto-edge*

This command sets the automatic bridge detection on the configured interface.

The use of a negative form (no) of the disables automatic bridge detection on the configured interface.

The automatic bridge detection feature is enabled by default.

**Syntax**

[no] spanning-tree auto-edge

**Parameters**

Command contains no arguments.

**Command mode**

INTERFACE FRONT-PORT
INTERFACE PORT-CHANNEL

**Example**

```
SBC2000-[CONFIG]-[SWITCH]-[if]> spanning-tree auto-edge
```

The automatic bridge detection feature is enabled.

### 4.3.6 *MAC table configuration commands*

#### *mac-address-table aging-time*

The command sets MAC address lifetime in the table globally.

The use of the negative form of the command (no) sets the default MAC address lifetime.

**Syntax**

[no] mac-address-table aging time <aging time>

no mac-address-table aging time

**Parameters**

<aging time> — MAC address life time, may take values [10 .. 630] seconds.

**Default value**

300 seconds

**Command mode**

CONFIG-SWITCH

**Example**

```
SBC2000-[CONFIG]-[SWITCH]> mac-address-table aging-time 100
```

#### *show mac address-table count*

This command allows viewing the number of MAC address entries on all front-port interfaces, port-channel interfaces, slot-channel interfaces.

**Syntax**

show mac address-table count

**Parameters**

Command contains no arguments.

**Command mode**

CONFIG-SWITCH

**Example**

```
SBC2000-[CONFIG]-[SWITCH]> show mac address-table count
17 valid mac entries
```

#### *show mac address-table include/exclude interface*

This command allows viewing the MAC table according to the specified interface:

**Syntax**

show mac address-table include/exclude interface <interface> <number>

**Parameters**

<interface> — interface type:

- front-port — external uplink interfaces;
- host-channel;
- port-channel — external LAG uplink interface aggregation groups;

<number> — port number:

- all — all ports of the selected interface;
- for front port: <unit/port>, where:
  - unit — module number, may take value [1],
  - port — port number, may take values: [0 .. 3];
- for host-channel: [1];
- for port-channel: [0 .. 4].

**Command mode**

CONFIG-SWITCH

### 4.3.7 *Port mirroring configuration commands*

#### *mirror <rx|tx> interface*

This command enables the mirroring operation on the switch ports for incoming and outgoing traffic.

Interface mirroring allows you to copy traffic going from one port to another for external analysis.

The use of the negative form of the command (no) disables the mirroring operation.

**Syntax**

[no] mirror <rx|tx> interface <port> <num>

**Parameters**

<rx|tx> — traffic type:

- rx — incoming;
- tx — outgoing.

<port> — interface type:

- front-port — external uplink interfaces;
- host-channel — interfaces for connecting interface modules;
- host-port;
- port-channel — logical association of external uplink interfaces;
- sm-port.

<num> — the sequential number of the port of a given group (you can specify several ports by enumerating with «,» or a range of ports with «-»):

- «all» — all ports of this group;

<interface> — interface type:

- front-port — external uplink interfaces;
- host-channel;
- host-port;
- port-channel — external LAG uplink interface aggregation groups;
- sm-port.

<number> — port number:

- all — all ports of the selected interface;
- for front port: <unit/port>, where:
  - unit — module number, may take value [1],
  - port — port number, may take values: [0 .. 3];
- for host-channel: [1];
- for host-port:
  - unit — module number, may take value [1],
  - port — port number, may take values: [0 .. 2];
- for port-channel: [0 .. 4].
- for sm-port:
  - ▪ unit — module number, may take value [1],
  - ▪ port — port number, may take values: [0 .. 5].

**Command mode**

CONFIG-SWITCH

**Example**

```
SBC2000-[CONFIG]-[SWITCH]> mirror rx interface front-port 1/3
```

For incoming traffic coming to front-port 1/3 interfaces, «port mirroring»

operation is enabled. Traffic is copied from the slot-port to the port-analyzer set by the «mirror rx analyzer» command.

### *mirror <rx|tx> analyzer*

This command allows you to install a port to which packets will be duplicated to analyze incoming/outgoing traffic from the ports set by the mirror rx port/mirror tx port command.

The use of the negative form of the command (no) disables analysis of transmitted incoming/outgoing traffic.

**Syntax**

[no] mirror <rx|tx> analyzer <interface> <port>

**Parameters**

<rx|tx> — traffic type:

- rx — incoming;
- tx — outgoing.

<interface> — interface type. Only front-port, port-channel interfaces can be used as a port-analyzer;

<port> — sequential number of the port of the front-port group in the format <unit/port>, where:

- for front port: <unit/port>, where:
  - unit — module number, may take value [1],
  - port — port number, may take values: [0 .. 3];
- for port-channel: [0 .. 4].

**Command mode**

CONFIG-SWITCH

**Example**

```
SBC2000-[CONFIG]-[SWITCH]> mirror rx analyzer front-port 1/2
```

Data for external analysis will be duplicated to the front-port 1/2 from the port/ports where the option «mirror incoming traffic» is set.

### *mirror add-tag*

This command adds the 802.1q mark to the traffic being analyzed. Setting the tag value can be done by the command **mirror <rx/tx> added-tag-config**.

The use of the negative form of the command (no) removes the tag.

**Syntax**

[no] mirror add-tag

**Parameters**

Command contains no arguments.

**Command mode**

CONFIG-SWITCH

**Example**

```
SBC2000-[CONFIG]-[SWITCH]> mirror add-tag
```

### *mirror <rx|tx> added-tag-config*

This command allows you to set a tag value that can be added to the analyzed incoming/outgoing traffic.

**Syntax**

mirror <rx|tx>  added-tag-config vlan <vid> [user-prio <user-prio>]

**Parameters**

<vid> — VLAN ID, may take values [1 .. 4094];

<user-prio> — COS priority, takes values from [0 .. 7].

**Command mode**

CONFIG-SWITCH

**Example**

```
SBC2000-[CONFIG]-[SWITCH]> mirror rx added-tag-config vlan 77 user-prio 5
```

#### *mirror <rx|tx> vlan*

The command specifies the VLAN ID to be used in the mirroring operation when transmitting incoming/outgoing traffic.

**Syntax**

[no] mirror <rx|tx> vlan <vid>

**Parameters**

<rx|tx> — traffic type:

- rx — incoming;
- tx — outgoing.

<vid> — VLAN ID, takes values of [1..4094].

**Command mode**

CONFIG-SWITCH

**Example**

```
SBC2000-[CONFIG]-[SWITCH]> mirror rx vlan 56
```

### 4.3.8 *SELECTIVE Q-IN-Q feature configuration commands*

For general settings of the Selective Q-in-Q feature the **SELECTIVE Q-IN-Q COMMON** command mode is intended. The **SELECTIVE Q-IN-Q LIST** command mode is used to configuration the Selective Q-in-Q rule list.

The SELECTIVE Q-IN-Q functionality allows adding an external SPVLAN (Service Provider's VLAN), replace the Customer VLAN, and deny traffic based on configurable filtering rules by internal VLAN (Customer VLAN) numbers.

#### *add-tag*

This command adds an outer tag based on the inner tag.

The use of a negative form (no) of the command removes the set rule.

**Syntax**

[no] add-tag svlan <s-vlan> cvlan <c-vlan>

**Parameters**

<s-vlan> — outer tag number, may take values [1..4095];

<c-vlan> — inner tag number(s), may take values 1-4094. The C-VLAN list is defined with «,».

**Command mode**

SELECTIVE Q-IN-Q

#### *overwrite-tag*

This command is used to substitute SVLAN in the required direction.

The use of a negative form (no) of the command removes the set rule.

**Syntax**

[no] overwrite-tag new-vlan <new-vlan> old-vlan <old-vlan> <rule_direction>

**Parameters**

<new-vlan> — new VLAN number, may take values [1 ..4095];

<old-vlan> — number of VLAN, which should be substituted, may take values [1 .. 4094].

<rule_direction> — traffic direction:

- Ingress — incoming;
- Egress — outgoing.

**Command mode**

SELECTIVE Q-IN-Q

### ***remove***

This command removes the Selective Q-in-Q rule by the specified number.

**Syntax**

remove <rule_index>

**Parameters**

<rule_index> — rule number, may take values [0 .. 511].

**Command mode**

SELECTIVE Q-IN-Q

### ***clear***

This command removes all Selective Q-in-Q rules.

**Syntax**

clear

**Parameters**

Command contains no arguments.

**Command mode**

SELECTIVE Q-IN-Q

### ***selective-qinq enable***

This command enables the Selective Q-in-Q feature on the configured SMG-2-16 switch Interface. The use of a negative form (no) of the command disables the SELECTIVE Q-in-Q feature on the interface.

**Syntax**

[no] selective-qinq enable

**Parameters**

Command contains no arguments.

**Command mode**

INTERFACE FRONT-PORT

INTERFACE PORT-CHANNEL

### *selective-qinq list*

This command assigns the Selective Q-in-Q rule list to the configurable interface of the SMG-2016 switch.

The use of the negative form of the command (no) removes the assignment.

**Syntax**

selective-qinq list <name>

no selective-qinq list

**Parameters**

<name> — Selective Q-in-Q rule list name

**Command mode**

INTERFACE FRONT-PORT

INTERFACE PORT-CHANNEL

### *show interfaces selective-qinq lists*

This command displays information about the status of the «Selective Q-in-Q» feature on the interfaces of the switch.

**Syntax**

show interfaces selective-qinq lists

## 4.3.9 *DUAL HOMING protocol configuration*

### *backup interface*

This command specifies a redundant interface to which the switching will occur when the connection is lost on a primary one: Redundancy is enabled only on those interfaces on which the SPANNING TREE protocol is disabled.

The use of a negative form (no) of the command removes interface configuration.

**Syntax**

[no] backup interface <INTERFACE> <INDEX> vlan <VLAN_ID_RANGE>

**Parameters**

<interface> — interface type:

- front-port — external interfaces;
- port-channel — external LAG uplink interface aggregation groups.

<INDEX> — port number:

- for front port: <unit/port>, where:
  - unit — SMG-2016 board number, may take value [1];
  - port — port number, may take values: [0 .. 3].
- for port-channel: [1 .. 4].

<VLAN_ID_RANGE> **—** can take the following values:

- [1..4094] — specified VLAN (VLAN range) identifier, for which the redundancy must be enabled.
- Ignore — enable redundancy regardless of existing VLANs on the port.

**Command mode**

INTERFACE FRONT-PORT

INTERFACE PORT-CHANNEL

**Example**

Global redundancy

```
SBC2000-[CONFIG]-[SWITCH]-[if]> no backup interface vlan ignore
SBC2000-[CONFIG]-[SWITCH]-[if]> backup interface front-port 1/1 vlan ignore
```

Redundancy in a specific VLAN

```
SBC2000-[CONFIG]-[SWITCH]-[if]> no backup interface vlan 10
SBC2000-[CONFIG]-[SWITCH]-[if]> backup interface port-channel 1 vlan 10
```

### ***backup-interface mac-duplicate***

This command specifies the number of packets copies with the same MAC address that will be sent to an active interface when switching.

The use of a negative form (no) of the command restores the default value (1 packet).

**Syntax**

[no] backup-interface mac-duplicate <COUNT>

**Parameters**

<COUNT> — amount of packets copies, takes values of [1..4].

**Default value**

1 packet

**Command mode**

CONFIG SWITCH

**Example**

```
SBC2000-[CONFIG]-[SWITCH]> backup-interface mac-duplicate 4
```

### ***backup-interface preemption***

This command specifies that it is necessary to switch traffic to the main interface when restoring communication. If the primary interface is configured to recover when the redundant interface is active, then when the link is up on the primary interface, the traffic will be switched to it. The use of a negative form (no) of the command restores the default setting.

**Syntax**

[no] backup-interface preemption

**Parameters**

Command contains no arguments.

**Default value**

Switching disabled.

**Command mode**

CONFIG SWITCH

**Example**

```
SBC2000-[CONFIG]-[SWITCH]> backup-interface preemption
```

### *show interfaces backup*

This command allows viewing interface redundancy settings.

**Syntax**

show interfaces backup

**Parameters**

Command contains no arguments.

**Command mode**

CONFIG SWITCH

**Example**

```
SBC2000-[CONFIG]-[SWITCH]> show interfaces backup
   Backup Interface Options:
      Preemption is disabled.
      MAC recovery packets rate 400 pps.
      Recovery packets repeats count 1.

   Backup Interface Pairs
   ~~~~~~~~~~~~~~~~~~~~~~
VID    Master Interface            Backup Interface            State
----   -------------------------   -------------------------   ------------------------------
30     front-port 1/0              front-port 2/0              Master Up/Backup Standby
----   -------------------------   -------------------------   ------------------------------
150    front-port 1/0              front-port 2/0              Master Up/Backup Standby
```

## 4.3.10 *LLDP configuration*

### *lldp enable*

This command allows the switch to work over the LLDP.

The use of a negative form (no) of the command disables LLDP protocol usage by switch.

**Syntax**

[no] lldp enable

**Parameters**

Command contains no arguments.

**Command mode**

CONFIG SWITCH

**Example**

```
SBC2000-[CONFIG]-[SWITCH]> lldp enable
```

### *lldp hold-multiplier*

This command specifies the amount of time for the receiver to keep LLDP packets before dropping them.

This value will be transmitted to the receiving side in the LLDP update packets; and should be an increment for the LLDP timer. Thus, the lifetime of LLDP packets is calculated by the formula: TTL = min(65535, LLDP-Timer * LLDP-HoldMultiplier).

The use of a negative form (no) of the command sets the default value.

**Syntax**

lldp hold-multiplier <hold>

no lldp hold-multiplier

**Parameters**

<hold> — time, may take values [2 .. 10] seconds.

**Default value**

The default value is 4 seconds.

**Command mode**

CONFIG SWITCH

**Example**

```
SBC2000-[CONFIG]-[SWITCH]> lldp hold-multiplier 5
```

### *lldp reinit*

This command sets ninimum amount of time for the LLDP port to wait before LLDP reinitialization.

The use of a negative form (no) of the command sets the default value.

**Syntax**

lldp reinit <reinit>

no lldp reinit

**Parameters**

<reinit> — time, may take values [1 .. 10] seconds.

**Default value**

The default value is 2 seconds.

**Command mode**

CONFIG SWITCH

**Example**

```
SBC2000-[CONFIG]-[SWITCH]> lldp reinit 3
```

### *lldp timer*

This command specifies how frequently the device will send LLDP information updates.

The use of a negative form (no) of the command sets the default value.

**Syntax**

lldp timer <timer>

no lldp timer

**Parameters**

<timer> — time, may take values [5..32768] seconds.

**Default value**

The default value is 30 seconds.

**Command mode**

CONFIG SWITCH

**Example**

```
SBC2000-[CONFIG]-[SWITCH]> lldp timer 60
```

### *lldp tx-delay*

This commans specifies the delay between the subsequent LLDP packet transmissions caused by the changes of values or status in the local LLDP MIB database.

It is recommended that this delay be less than 0.25* LLDP-Timer.

The use of a negative form (no) of the command sets the default value.

**Syntax**

lldp tx-delay  <txdelay>

no lldp tx-delay

**Parameters**

<txdelay> – time, may take values [1..8192] seconds.

**Default value**

The default value is 2 seconds.

**Command mode**

CONFIG SWITCH

**Example**

```
SBC2000-[CONFIG]-[SWITCH]> lldp tx-delay 3
```

### *lldp lldpdu*

This command sets the LLDP packet processing mode when LLDP is disabled.

The use of a negative form (no) of the command sets the default value (filtering).

**Syntax**

lldp lldpdu [mode]

no lldp lldpdu

**Parameters**

<mode> — LLDP packets processing mode:

- filtering — LLDP packets are filtered if LLDP is disabled on the switch;
- flooding — LLDP packets are transmitted if LLDP is disabled on the switch.

**Command mode**

CONFIG SWITCH

**Example**

```
SBC2000-[CONFIG]-[SWITCH]> lldp lldpdu flooding
```

### *show lldp configuration*

This command allows viewing the LLDP configuration of all physical interfaces of the device or specified interfaces.

**Syntax**

show lldp configuration [<interface>< number >]

**Parameters**

Optional parameters, if you omit them, the display will show information for all ports.

[interface] — interface type:

- front-port — external uplink interfaces;
- port-channel — external LAG uplink interface aggregation groups.

[number] — port number (you can specify several ports separated by commas «,» or you can specify the range of ports with «-»).

- for front port: <unit/port>, where:
  - unit — module number, may take value [1],
  - port — port number, may take values: [0 .. 3];
- for port-channel: [0 .. 4].

**Default value**

The display will show information for all ports.

**Command mode**

CONFIG SWITCH

**Example**

```
SBC2000-[CONFIG]-[SWITCH]> show lldp configuration

   LLDP configuration
   ~~~~~~~~~~~~~~~~~~
Interface         Status               Timer (sec)  Hold multiplier  Reinit delay (sec)  Tx delay (sec)
-------------   ----------------- ------     ----------    -------------    ----------
front-port 1/0  transmit-receive   30           4            2              2
front-port 1/1  transmit-receive   30           4            2              2
front-port 1/2  transmit-receive   30           4            2              2
front-port 1/3  transmit-receive   30           4            2              2
```

### *show lldp neighbor*

This command allows viewing information on the neighbour devices on which LLDP is enabled.

**Syntax**

show lldp neighbor  [<interface>< number >]

**Parameters**

Optional parameters, if you omit them, the display will show information for all ports.

[interface] — interface type:

- front-port — external uplink interfaces;
- port-channel — external LAG uplink interface aggregation groups.

[number] — port number (you can specify several ports separated by commas «,» or you can specify the range of ports with «-»).

- for front port: <unit/port>, where:
  - unit — module number, may take value [1],
  - port — port number, may take values: [0 .. 3];
- for port-channel: [0 .. 4].

**Default value**

The display will show information for all ports.

**Command mode**

CONFIG SWITCH

**Example**

```
SBC2000-[CONFIG]-[SWITCH]> show lldp neighbor

   LLDP neighbors
   ~~~~~~~~~~~~~~
Interface           Device ID                Port ID                  TTL
----------------   ----------------------   -----------------------   ----------
front-port 1/1     02:00:2a:00:07:15           g15                    115/120
front-port 1/2     02:00:04:88:7e:             front-port 1/3         105/120
SBC2000-[CONFIG]-[SWITCH]>
```

### *show lldp local*

This command allows viewing the LLDP information announced by this port.

**Syntax**

show lldp local [<interface>< number >]

**Parameters**

Optional parameters, if you omit them, the display will show information for all ports.

[interface] — interface type:

- front-port — external uplink interfaces;
- port-channel — external LAG uplink interface aggregation groups.

[number] — port number (you can specify several ports separated by commas «,» or you can specify the range of ports with «-»).

- for front port: <unit/port>, where:
  - unit — module number, may take value [1],
  - port — port number, may take values: [0 .. 3];
- for port-channel: [0 .. 4].

**Default value**

The display will show information for all ports.

**Command mode**

CONFIG SWITCH

**Example**

```
SBC2000-[CONFIG]-[SWITCH]> show lldp local

   LLDP local TLVs
   ~~~~~~~~~~~~~~~
Interface           Device ID                Port ID                   TTL
----------------   ----------------------   -----------------------   ----------
front-port 1/1     02:00:04:88:7c:0a        front-port 1/1             120
front-port 1/2     02:00:04:88:7c:0a        front-port 1/2             120
```

### ***show lldp statistics***

This command allows viewing LLDP statistics for front-port, port-channel interfaces.

**Syntax**

show lldp statistics [<interface>< number >]

**Parameters**

Optional parameters, if you omit them, the display will show information for all ports.

[interface] — interface type:

- front-port — external uplink interfaces;
- port-channel — external LAG uplink interface aggregation groups.

[number] — port number (you can specify several ports separated by commas «,» or you can specify the range of ports with «-»).

- for front port: <unit/port>, where:
  - unit — module number, may take value [1],
  - port — port number, may take values: [0 .. 3];
- for port-channel: [0 .. 4];
- for slot-channel: [0 .. 15].

**Default value**

The display will show information for all ports.

**Command mode**

CONFIG SWITCH

**Example**

```
SBC2000-[CONFIG]-[SWITCH]> show lldp statistics

Tables Last Change Time: 0:0:4:28
Tables Inserts: 3
Tables Deletes: 1
Tables Dropped: 0
Tables Ageouts: 0

   LLDP statistics
   ~~~~~~~~~~~~~~~
Interface         Tx total Rx total Rx errors Rx discarded TLVs discarded TLVs unrecognized Agouts total
front-port 1/0       0           0          0            0              0            0              0
front-port 1/1      6134       6159         0            0              0            0              0
front-port 1/2      6141       6136         0            0              0            0              0
front-port 1/3       0           0          0            0              0            0              0
```

### *show lldp lldpdu*

This command is used to view the way LLDPDU packets are processed for interfaces where LLDP function is disabled.

**Syntax**

show lldp lldpdu

**Parameters**

Command contains no arguments.

**Command mode**

CONFIG SWITCH

**Example**

```
SBC2000-[CONFIG]-[SWITCH]> show lldp lldpdu
Global: flooding
```

## 4.3.11 *QoS configuration*

### *qos default*

This command defines the queue, that will be used for packets without any preconfigured rules. The queue with the value of 7 is considered the highest priority.

**Syntax**

qos default <queue>

**Parameters**

< queue > – priority queue number, may take values [0 .. 7].

**Default value**

The default is queue 0.

**Command mode**

CONFIG SWITCH

**Example**

```
qos default 6
```

Packets for which no other rules are set are queued with priority 6.

### *qos type*

This command allows you to set a rule by which to select the priority field for the package.

The traffic prioritization method will be chosen depending on the configured system rules (IEEE 802.1p/DSCP).

- The system distinguishes the following traffic prioritization methods:
- All the priorities are equal;
- Packet selection according to IEEE 802.1p;
- Packet selection only according to IP ToS (Type of Service) on 3 level — support for Differentiated Services Codepoint (DSCP);
- Interaction according to either 802.1p or DSCP/TOS;

**Syntax**

qos type <type>

**Parameters**

<type> — traffic prioritization method:

- 0 — all the priorities are equal;
- 1 — packet selection only by 802.1p only (Priority field in 802.1Q tag);
- 2 — packet selection only by DSCP/TOS (field Differentiated Services IP packet header, senior 6 bits);
- 3 — interaction either via 802.1p or DSCP/ToS.

**Default value**

By default all priorities are equal.

**Command mode**

CONFIG SWITCH

**Example**

```
qos type 2
```

Traffic prioritization will be done only via DSCP/ToS.

### *qos map*

This command sets the parameters for the priority queue:

- specifies the value of the field Differentiated Services IP packet header, senior 6 bits,
- value of the Priority field in 802.1Q tag.

Based on the rules set by the qos type command and the specified priority values, packages are selected for this priority queue.

The use of the negative form of the command (no) allows you to remove the entry from the queue settings table.

**Syntax**

[no] qos map <type> <field values> to <queue>

**Parameters**

<type> — traffic prioritization method:

- 0 — by the 802.1p standard (used on level 2);
- 1 — by the DSCP/TOS standard (used on level 3).

<field values> – value of the field by which the packets are selected is set according to <parameter 1> (the values of the fields are entered with a comma or as a range with «-»):

- if <type> = 0, then the Priority field value is set to 802.1Q Tag: [0 ... 7];
- if <type> = 1, then set the values of the fields *Differentiated Services* of the IP packet header, the highest 6 bits. The value is entered in decimal format: [0 .. 63].

<queue> – priority queue number, may take values [0 .. 7].

**Command mode**

CONFIG SWITCH

**Example**

```
qos map 0 7 7
```

For the 7th priority queue the value of the field priority = 7 in 802.1Q tag.

### *cntrset*

This command assigns the queue statistics collector to the queues with specified criteria.

**Syntax**

cntrset <PORT>  <UNIT> <SET> <VLAN> <QUEUE> <DROP PRECEDENCE>

**Parameters**

<PORT> — type of the port for counting, may take values:

- all — all ports;
- cpu — CPU port;
- front-port — counting front-port;
- host-port;
- sm-port.

<UNIT> — port sequential number:

- for cpu: may take value [1];
- for front port: <unit/port>, where:
    - unit — module number, may take value [1];
    - port — port number, may take values: [0 .. 3].
- for host-port: <unit/port>, where:
    - unit — module number, may take value [1];
    - port — port number, may take values: [0 .. 2].
- for sm-port: <unit/port>, where:
    - unit — module number, may take value [1];
    - port —  port number, may take values: [0 .. 5].
- <SET> — statistics collector number, may take values [0 .. 1];
- < VLAN > — VLAN ID, may take values [1 .. 4094] or all;
- < QUEUE > — queue number, may take values [0 .. 7] or all;
- < DROP PRECEDENCE > — drop precedence value [0 .. 1] or all.

**Command mode**

CONFIG – SWITCH

**Example**

```
cntrset sm-port 1/2 1 22 2 1
```

#### *show cntrset*

This command is used to view the queue collector information.

**Syntax**

show cntrset <SET>

**Parameters**

<SET> — counter number [0 .. 1].

**Command mode**

CONFIG – SWITCH

#### *show qos*

This command is used to view the priorities assigned to the queues. By default queue priority is 0. The priority value for the queue is set in the range [0 .. 7], the queue with a priority value of 7 is considered the highest priority.

**Syntax**

show qos

**Parameters**

Command contains no arguments.

**Command mode**

CONFIG – SWITCH

### 4.3.12 *Configuration operation commands*

SBC-2000 switch has 2 configuration types:

- running-config — configuration that is currently active on the device;
- candidate-config — configuration in which any changes have been made, it will become running-config after it is applied with the apply command.

**View configuration**

#### *show running-config*

**Syntax**

show running-config

**Parameters**

Command contains no arguments.

**Command mode**

CONFIG – SWITCH

#### *show candidate-config*

**Syntax**

show candidate-config

**Parameters**

Command contains no arguments.

**Command mode**

CONFIG – SWITCH

### 4.3.13 *Configuration application and confirmation commands*

Once the SBC-2000 switch has been configured, you must apply the configuration (apply) to make it active on the device and confirm the application (confirm) to protect against the changes that have been made causing loss of access to the device. If no confirmation is performed within 60 seconds, the configuration is rolled back to the previous running-config.

*Configuration application command.*

**Syntax**

apply

**Parameters**

Command contains no arguments.

**Command mode**

CONFIG – SWITCH

*Confirmation command.*

**Syntax**

confirm

**Parameters**

Command contains no arguments.

**Command mode**

CONFIG – SWITCH

### 4.3.14 *Other commands*

#### *config*

Command to return to the Configuration menu.

**Syntax**

config

**Parameters**

Command contains no arguments.

**Command mode**

CONFIG – SWITCH

### *exit*

Command is used to exit from this configuration submenu to the upper level.

**Syntax**

exit

**Parameters**

Command contains no arguments.

**Command mode**

CONFIG – SWITCH

### *history*

Command is used to view history of entered commands.

**Syntax**

history

**Parameters**

Command contains no arguments.

**Command mode**

CONFIG – SWITCH

# APPENDIX A. ALTERNATIVE FIRMWARE UPDATE METHOD

When you cannot update the firmware via web configurator or console (telnet, RS-232), you may use an alternative firmware update method via RS-232.

To update the device firmware, you will need the following programs:

- terminal program (for example, TERATERM);
- TFTP server program.

Firmware update procedure:

*1.* Connect to Ethernet port of the device.

*2.* Connect PC console port to the device console port using a crossed cable;

*3.* Run the terminal application.

*4.* Configure data rate: 115200, data format: 8bit w/o parity, 1 stop bit, w/o flow control:

*5.* Run *tftp* server program and specify the path to *smg_files* folder. In this folder, create *smg2016* subfolder, and place *smg2016_kernel, smg2016_initrd* files *for SBC-2000* (*smg1016M_kernel, smg1016M_initrd for SBC-1000*) in it (computer that runs TFTP server and the device should be located in the same network);

*6.* Turn the device on and stop the startup sequence by entering «**`stop`**» command in the terminal program window:

For SBC-2000:

```
U-Boot 2011.12 (Nov 18 2013 - 12:56:19) Marvell version: 2012_Q4.0p17

…
Init Switch of the board
Switch. Initialization
Switch. Initialization Ok, Vendor Id: 000011ab
Switch. Phy 4: id 0141-0dc0
Switch. Phy 5: id 0141-0dc0
Switch. Phy 6: id 0141-0dc0
Switch. Phy 7: id 0141-0dc0
Switch. QSGMII 0: 0a800050 = 00000001. Sync not ok
Switch. QSGMII 3: 0a803050 = 00000003. Sync ok
Switch: cpu link 0: 0000ac0f. Sync not ok
Switch: cpu link 1: 0000ac0f. Sync not ok
Switch: cpu link 2: 0000ac0f. Sync not ok
Switch: cpu link 3: 0000ac0f. Sync not ok
Net:   egiga0 [PRIME]
Warning: failed to set MAC address
, egiga1, egiga2, egiga3
Type 'stop' to stop autoboot:  3
SMG2016>>
```

For SBC-1000:

```
U-Boot 2009.06 (Feb 09 2010 - 20:57:21)

CPU:   AMCC PowerPC 460GT Rev. A at 800 MHz (PLB=200, OPB=100, EBC=100 MHz)
       Security/Kasumi support
       Bootstrap Option B - Boot ROM Location EBC (16 bits)
       32 kB I-Cache 32 kB D-Cache
```

```
Board: <SBC-1000>v2 board, AMCC PPC460GT Glacier based, 2*PCIe, Rev. FF
I2C:   ready
DRAM:  512 MB
SDRAM test phase 1:
SDRAM test phase 2:
SDRAM test passed. Ok!
FLASH: 64 MB
NAND:  128 MiB
DTT:   1 FAILED INIT
Net:   ppc_4xx_eth0, ppc_4xx_eth1

Type run flash_nfs to mount root filesystem over NFS

Autobooting in 3 seconds, press 'stop' for stop
=>
```

*7.* Enter **`set ipaddr`** <device ip address> <ENTER>;

Example: `set ipaddr 192.168.2.2`

*8.* Enter **`set netmask`** <device network mask> <ENTER>;

Example: `set netmask 255.255.255.0`

*9.* Enter **`set serverip`** <IP address of a computer, that runs TFTP server><ENTER>;

Example: `set serverip 192.168.2.5`

*10.* For SBC-1000, enter **`mii si`** <ENTER> to activate the network interface:

```
=> mii si
Init switch 0: ..Ok!
Init switch 1: ..Ok!
Init phy 1: ..Ok!
Init phy 2: ..Ok!
=>
```

*11.* Update the Linux kernel using **`run flash_kern`** command*:*

For SBC-2000:

```
SMG2016>> run flash_kern
…
TFTP from server 192.168.2.5; our IP address is 192.168.2.2
Filename ' smg2016/smg2016_kernel'.
Loading: #################################################################
         ###################################
done
…
Copy to Flash... done
SMG2016>>
```

For SBC-1000:

```
=> run flash_kern
About preceeding transfer (eth0):
- Sent packet number 0
- Received packet number 0
- Handled packet number 0
ENET Speed is 1000 Mbps - FULL duplex connection (EMAC0)
Using ppc_4xx_eth0 device
TFTP from server 192.168.2.5; our IP address is 192.168.2.2
Filename ' smg/smg1016M_kernel'.
Load address: 0x400000
```

```
Loading: #################################################################
         ###################################
done
Bytes transferred = 1455525 (1635a5 hex)
Un-Protected 15 sectors

............... done
Erased 15 sectors
Copy to Flash... 9....8....7....6....5....4....3....2....1....done
=>
```

12. Update the file system using **`run flash_initrd`** command:

For SBC-2000:

```
SMG2016>>  run flash_initrd
…
TFTP from server 192.168.2.5; our IP address is 192.168.2.2
Filename ' smg2016/smg2016_initrd'.
Loading: #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         ####################
done
…
Copy to Flash... done
SMG2016>>
```

For SBC-1000:

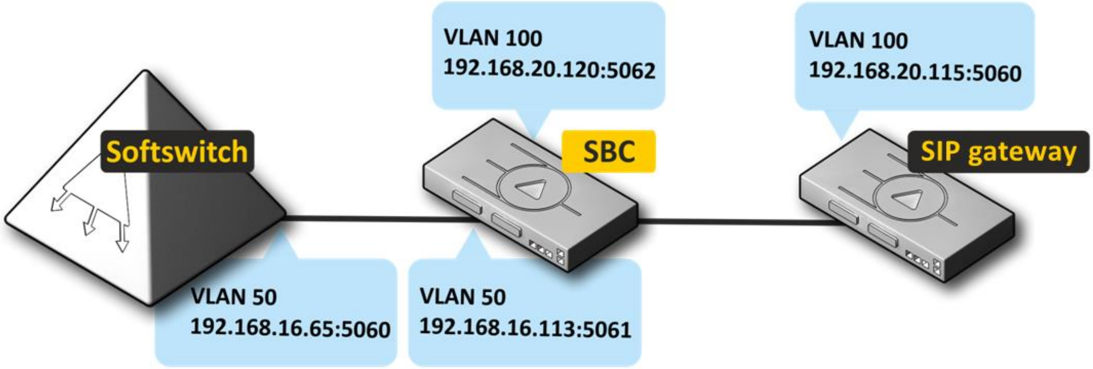
```
=> run flash_initrd
Using ppc_4xx_eth0 device
TFTP from server 192.168.2.5; our IP address is 192.168.2.2
Filename ' smg/smg1016M_initrd'.
Load address: 0x400000
Loading: #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         ####################
done
Bytes transferred = 25430113 (1840861 hex)
Erase Flash Sectors 56-183 in Bank # 2
Un-Protected 256 sectors
........................................................... done
Erased 256 sectors
Copy to Flash... 9....8....7....6....5....4....3....2....1....done=>
```

13. Start up the device using **`run bootcmd`** command.

# APPENDIX B. SBC CONFIGURATION EXAMPLES

## 1. Configuration of SBC for SIP subscribers

### Use Case



### Operation algorithm

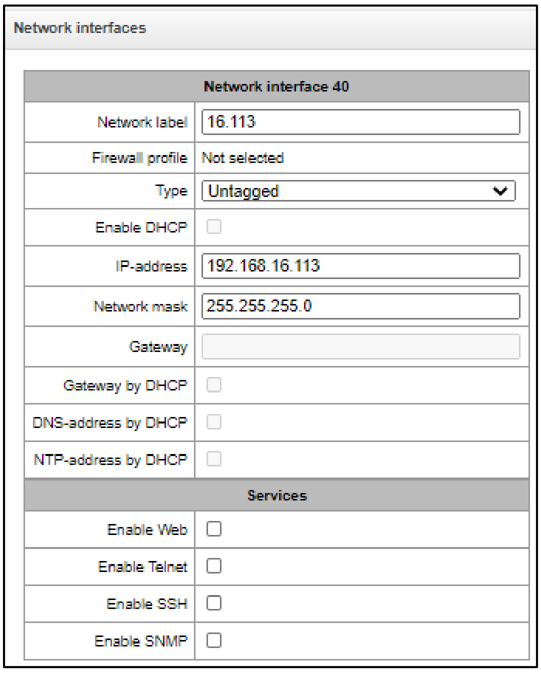
The subscriber gateway sends a message to IP-address 192.168.20.120 port 5062, SBC-2000 forwards this traffic from IP address 192.168.16.113 port 5061 to Softswitch 192.168.16.65 port 5060.

### SBC configuration procedure

1. Interface configuration (menu **Network subsystem/Network interfaces, section 4.1.4.3**).

   a. Create an interface in the Softswitch direction.

Interface parameters: *192.168.16.113.*

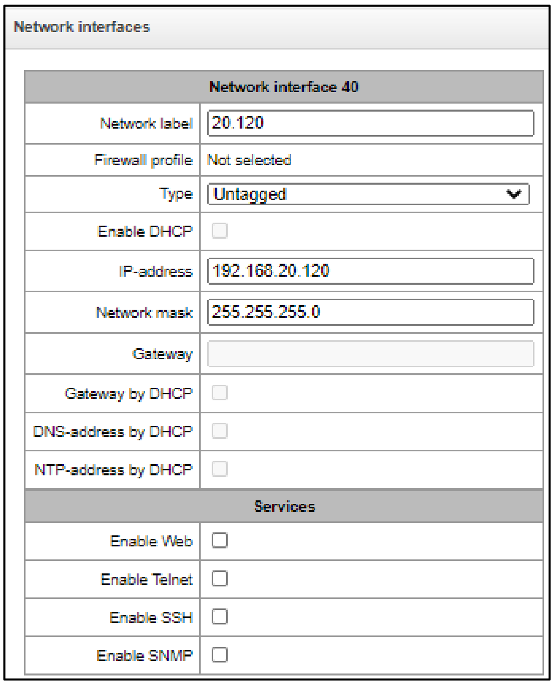


Network interfaces

| Network interface 40 | |
|---|---|
| Network label | 16.113 |
| Firewall profile | Not selected |
| Type | Untagged |
| Enable DHCP | □ |
| IP-address | 192.168.16.113 |
| Network mask | 255.255.255.0 |
| Gateway | |
| Gateway by DHCP | □ |
| DNS-address by DHCP | □ |
| NTP-address by DHCP | □ |
| **Services** | |
| Enable Web | □ |
| Enable Telnet | □ |
| Enable SSH | □ |
| Enable SNMP | □ |

b. Create an interface in the subscriber gateway direction.

Interface parameters: *192.168.20.120.*

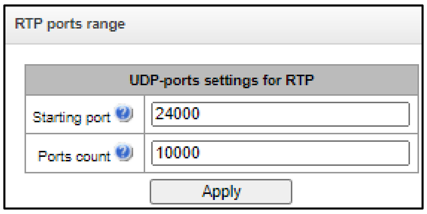


Network interfaces

| Network interface 40 | |
|---|---|
| Network label | 20.120 |
| Firewall profile | Not selected |
| Type | Untagged |
| Enable DHCP | □ |
| IP-address | 192.168.20.120 |
| Network mask | 255.255.255.0 |
| Gateway | |
| Gateway by DHCP | □ |
| DNS-address by DHCP | □ |
| NTP-address by DHCP | □ |
| **Services** | |
| Enable Web | □ |
| Enable Telnet | □ |
| Enable SSH | □ |
| Enable SNMP | □ |

2. Configuration of media for SIP (menu **SBC Configuration/RTP ports range, section 4.1.3.6**).

It is necessary to set the ranges of ports used for RTP.



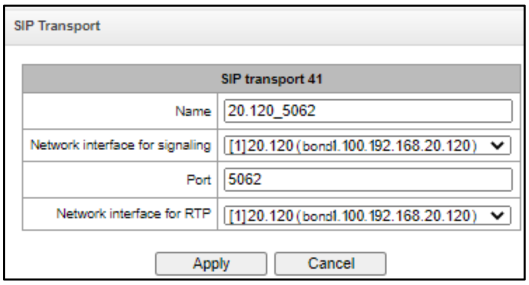
RTP ports range

| UDP-ports settings for RTP | |
|---|---|
| Starting port | 24000 |
| Ports count | 10000 |

3. SIP transport configuration (menu **SBC configuration/SIP transport, section 4.1.3.1**).

a. Add a SIP transport in the subscriber gateway direction.

Interface parameters:
*network interface 20.120;*
*signalling port — 5062;*
*media — 20.120.*

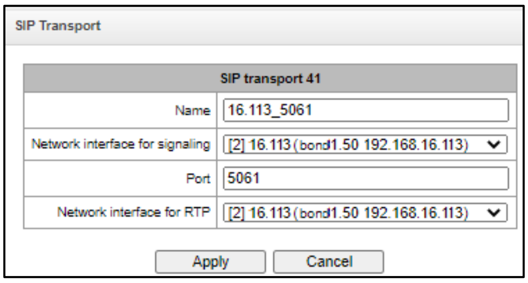


SIP Transport

| SIP transport 41 | |
|---|---|
| Name | 20.120_5062 |
| Network interface for signaling | [1]20.120 (bond1.100 192.168.20.120) |
| Port | 5062 |
| Network interface for RTP | [1]20.120 (bond1.100 192.168.20.120) |

b. Add a SIP transport in the Softswitch destination.

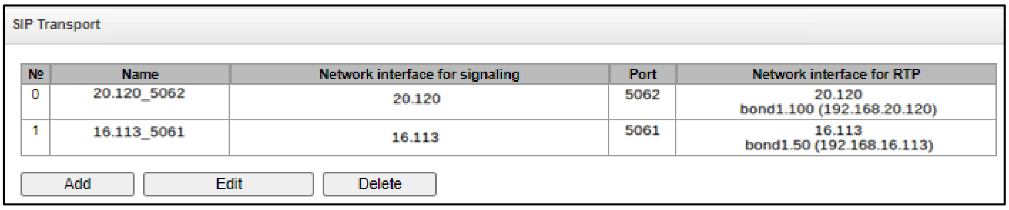
Interface parameters:
*network interface 16.113;*
*signalling port — 5061;*
*media — 16.113.*



SIP Transport

| SIP transport 41 | |
|---|---|
| Name | 16.113_5061 |
| Network interface for signaling | [2] 16.113 (bond1.50 192.168.16.113) |
| Port | 5061 |
| Network interface for RTP | [2] 16.113 (bond1.50 192.168.16.113) |

c. The SIP transport table will be as follows:



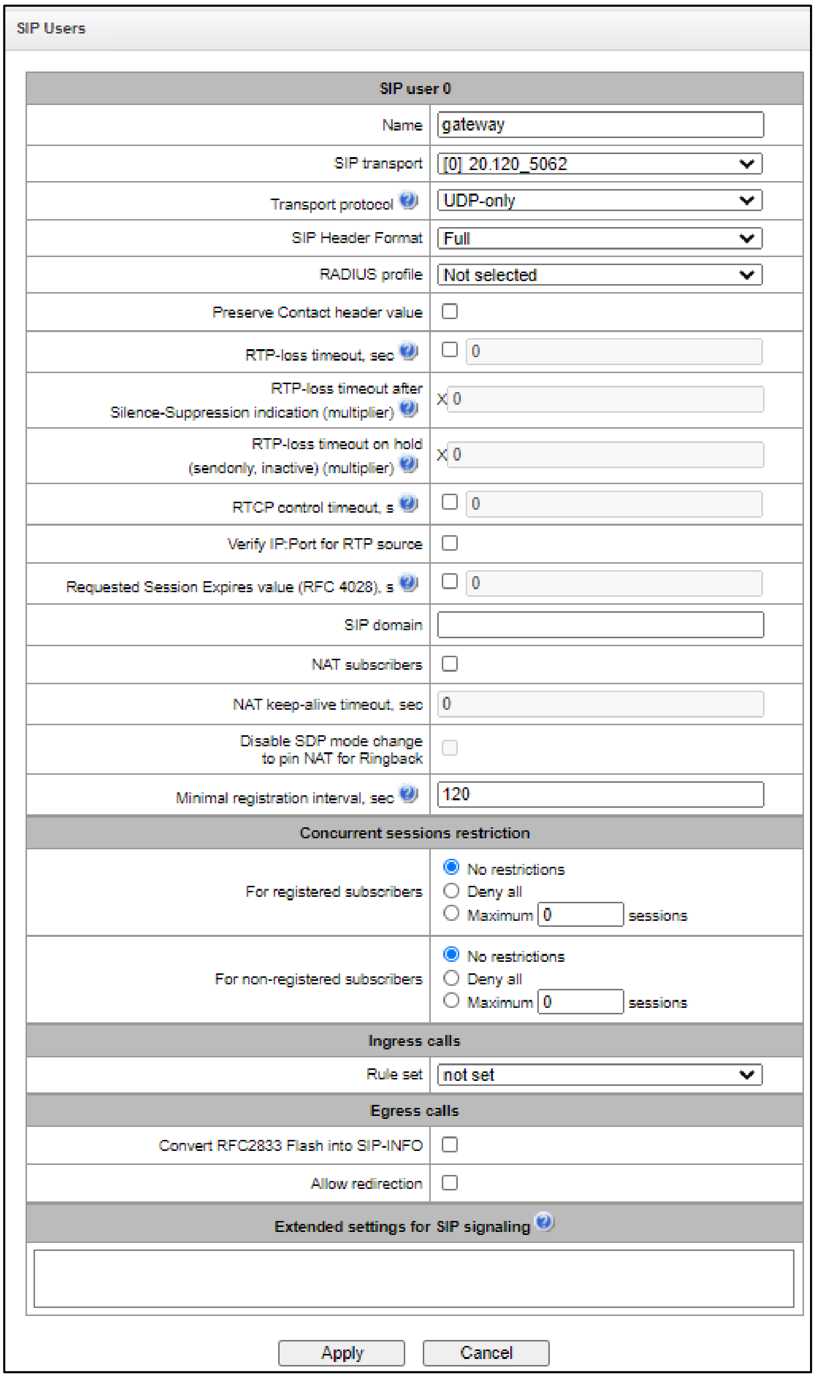
SIP Transport

| № | Name | Network interface for signaling | Port | Network interface for RTP |
|---|---|---|---|---|
| 0 | 20.120_5062 | 20.120 | 5062 | 20.120<br>bond1.100 (192.168.20.120) |
| 1 | 16.113_5061 | 16.113 | 5061 | 16.113<br>bond1.50 (192.168.16.113) |

4. SIP user configuration (menu **SBC Configuration/SIP Users, section 4.1.3.3**).

a. Add SIP Users.

In the *«SIP transport»* field, select the transport in the subscriber destination (*20.120_50 62*), if the subscribers are behind NAT, set the *«NAT subscribers»* flag and specify the connection storage time on NAT.



SIP Users

SIP user 0

| | |
|---|---|
| Name | gateway |
| SIP transport | [0] 20.120_5062 |
| Transport protocol | UDP-only |
| SIP Header Format | Full |
| RADIUS profile | Not selected |
| Preserve Contact header value | ☐ |
| RTP-loss timeout, sec | ☐ 0 |
| RTP-loss timeout after Silence-Suppression indication (multiplier) | X 0 |
| RTP-loss timeout on hold (sendonly, inactive) (multiplier) | X 0 |
| RTCP control timeout, s | ☐ 0 |
| Verify IP:Port for RTP source | ☐ |
| Requested Session Expires value (RFC 4028), s | ☐ 0 |
| SIP domain | |
| NAT subscribers | ☐ |
| NAT keep-alive timeout, sec | 0 |
| Disable SDP mode change to pin NAT for Ringback | ☐ |
| Minimal registration interval, sec | 120 |

Concurrent sessions restriction

| | |
|---|---|
| For registered subscribers | ● No restrictions<br>○ Deny all<br>○ Maximum 0 sessions |
| For non-registered subscribers | ● No restrictions<br>○ Deny all<br>○ Maximum 0 sessions |

Ingress calls

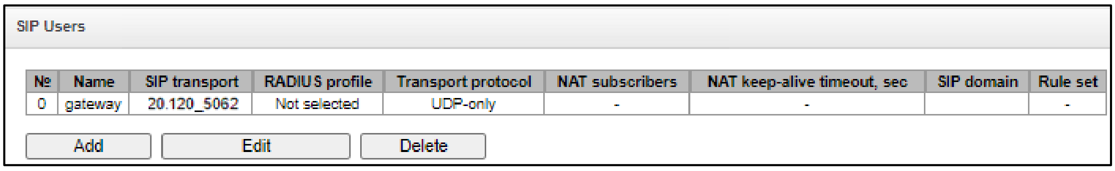
| | |
|---|---|
| Rule set | not set |

Egress calls

| | |
|---|---|
| Convert RFC2833 Flash into SIP-INFO | ☐ |
| Allow redirection | ☐ |

Extended settings for SIP signaling

b. The SIP user table will be as follows:



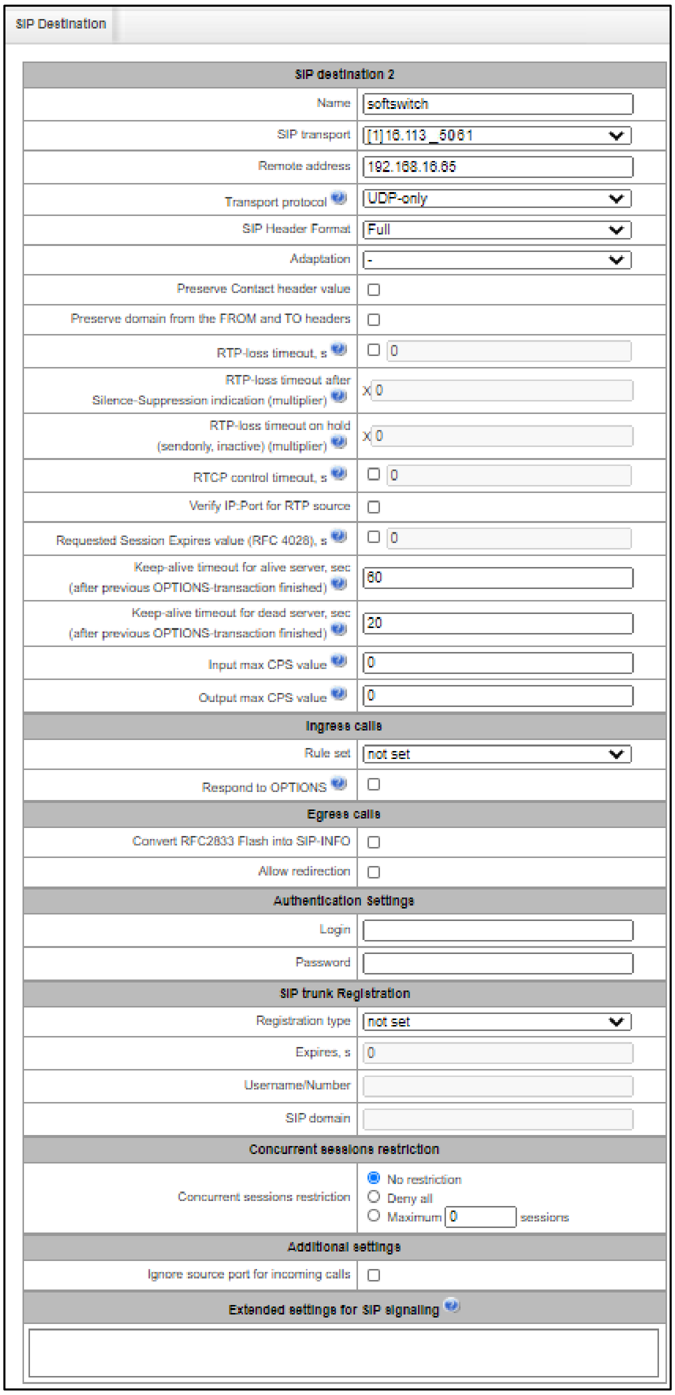
SIP Users

| № | Name | SIP transport | RADIUS profile | Transport protocol | NAT subscribers | NAT keep-alive timeout, sec | SIP domain | Rule set |
|---|---|---|---|---|---|---|---|---|
| 0 | gateway | 20.120_5062 | Not selected | UDP-only | - | - |  | - |

5. SIP destination configuration (menu **SBC Configuration/SIP Destination, section 4.1.3.2**).

a. Add a SIP Destination.

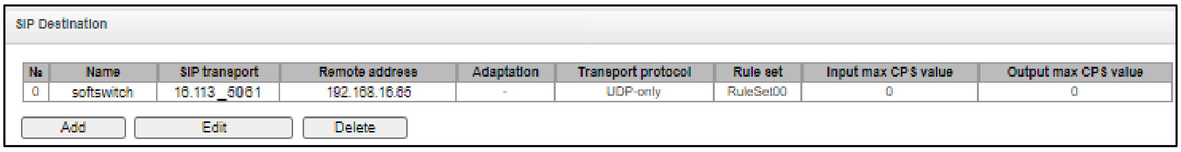
In the *«SIP transport»* field select the transport in the Softswitch destination (*16.113_5061*), in the *«Remote address»* field specify the IP address of Softswitch.



SIP Destination

|  |  |
|---|---|
| **SIP destination 2** |  |
| Name | softswitch |
| SIP transport | [1] 16.113_5061 |
| Remote address | 192.168.16.65 |
| Transport protocol | UDP-only |
| SIP Header Format | Full |
| Adaptation | - |
| Preserve Contact header value | □ |
| Preserve domain from the FROM and TO headers | □ |
| RTP-loss timeout, s | □ 0 |
| RTP-loss timeout after Silence-Suppression indication (multiplier) | x 0 |
| RTP-loss timeout on hold (sendonly, inactive) (multiplier) | x 0 |
| RTCP control timeout, s | □ 0 |
| Verify IP:Port for RTP source | □ |
| Requested Session Expires value (RFC 4028), s | □ 0 |
| Keep-alive timeout for alive server, sec (after previous OPTIONS-transaction finished) | 60 |
| Keep-alive timeout for dead server, sec (after previous OPTIONS-transaction finished) | 20 |
| Input max CPS value | 0 |
| Output max CPS value | 0 |
| **Ingress calls** |  |
| Rule set | not set |
| Respond to OPTIONS | □ |
| **Egress calls** |  |
| Convert RFC2833 Flash into SIP-INFO | □ |
| Allow redirection | □ |
| **Authentication settings** |  |
| Login |  |
| Password |  |
| **SIP trunk Registration** |  |
| Registration type | not set |
| Expires, s | 0 |
| Username/Number |  |
| SIP domain |  |
| **Concurrent sessions restriction** |  |
| Concurrent sessions restriction | ● No restriction<br>○ Deny all<br>○ Maximum 0 sessions |
| **Additional settings** |  |
| Ignore source port for incoming calls | □ |
| **Extended settings for SIP signaling** |  |

b. The SIP destination table will be as follows:

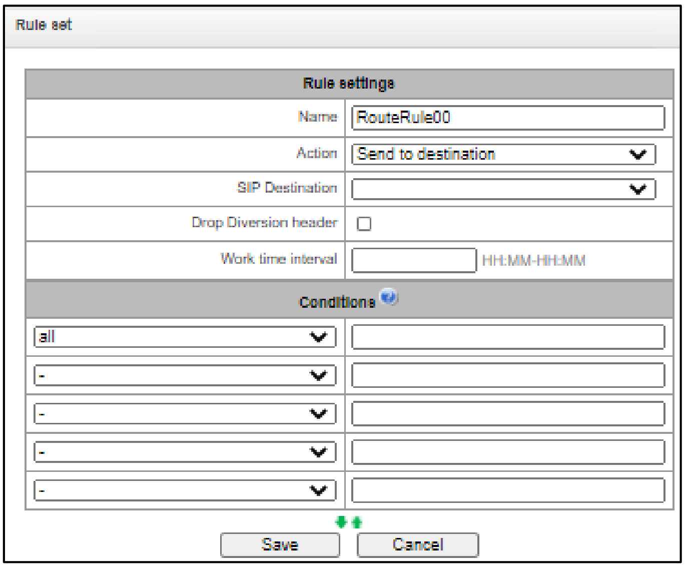


SIP Destination

| № | Name | SIP transport | Remote address | Adaptation | Transport protocol | Rule set | Input max CPS value | Output max CPS value |
|---|---|---|---|---|---|---|---|---|
| 0 | softswitch | 16.113_5061 | 192.168.16.65 | - | UDP-only | RuleSet00 | 0 | 0 |

6. Rule set configuration (menu **SBC Configuration/Rule set, section 4.1.3.5**).

Create rule set, specify its name, add a rule to the set. In the *«Action»* field select *«Send to destination»*, in the *«SIP Destination»* field specify the destination that was configured for Softswitch. Set the condition to *«All»*, save the rule and the rule set.



Rule set

Rule settings

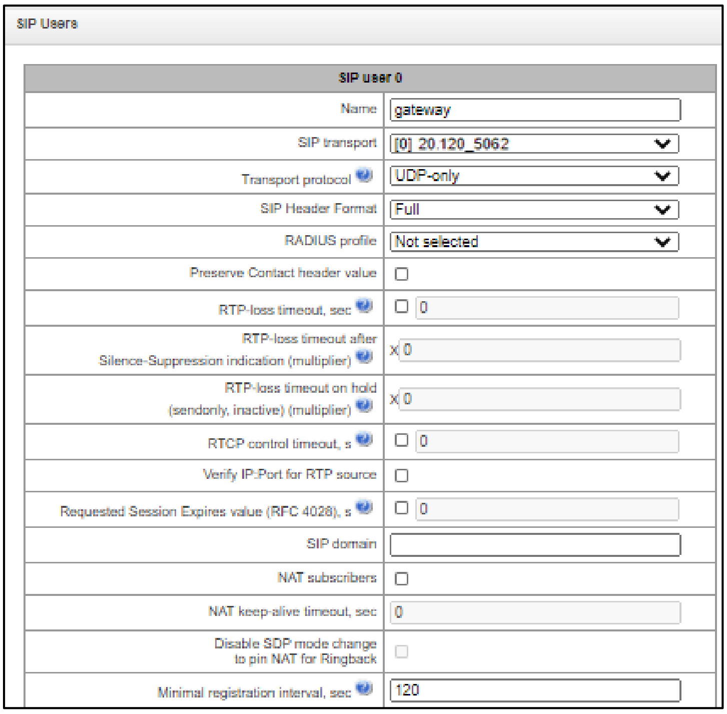
| | |
|---|---|
| Name | RouteRule00 |
| Action | Send to destination |
| SIP Destination | |
| Drop Diversion header | □ |
| Work time interval | HH:MM-HH:MM |

Conditions

| | |
|---|---|
| all | |
| - | |
| - | |
| - | |
| - | |

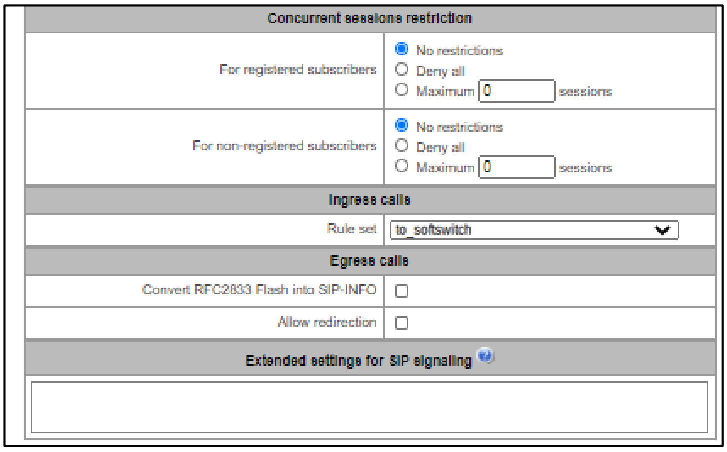
7. Binding a rule to a destination for subscribers.

a. Go to the *«SIP Users»* section, select the previously created destination and in the *«Rule set»* select the created rule set.



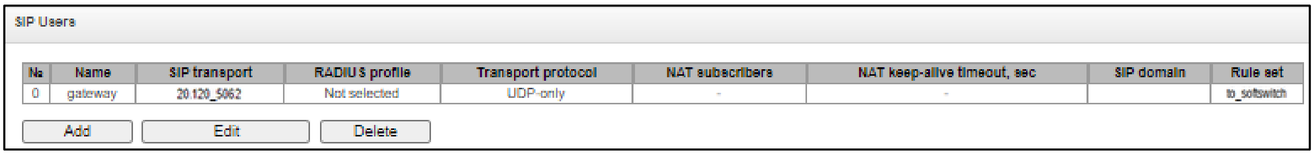
SIP Users

| SIP user 0 | |
|---|---|
| Name | gateway |
| SIP transport | [0] 20.120_5062 |
| Transport protocol | UDP-only |
| SIP Header Format | Full |
| RADIUS profile | Not selected |
| Preserve Contact header value | □ |
| RTP-loss timeout, sec | □ 0 |
| RTP-loss timeout after Silence-Suppression indication (multiplier) | x 0 |
| RTP-loss timeout on hold (sendonly, inactive) (multiplier) | x 0 |
| RTCP control timeout, s | □ 0 |
| Verify IP:Port for RTP source | □ |
| Requested Session Expires value (RFC 4028), s | □ 0 |
| SIP domain | |
| NAT subscribers | □ |
| NAT keep-alive timeout, sec | 0 |
| Disable SDP mode change to pin NAT for Ringback | □ |
| Minimal registration interval, sec | 120 |



| Concurrent sessions restriction | |
|---|---|
| For registered subscribers | ● No restrictions<br>○ Deny all<br>○ Maximum 0 sessions |
| For non-registered subscribers | ● No restrictions<br>○ Deny all<br>○ Maximum 0 sessions |
| **Ingress calls** | |
| Rule set | to_softswitch |
| **Egress calls** | |
| Convert RFC2833 Flash into SIP-INFO | □ |
| Allow redirection | □ |
| **Extended settings for SIP signaling** | |

b. The SIP user table will be as follows:



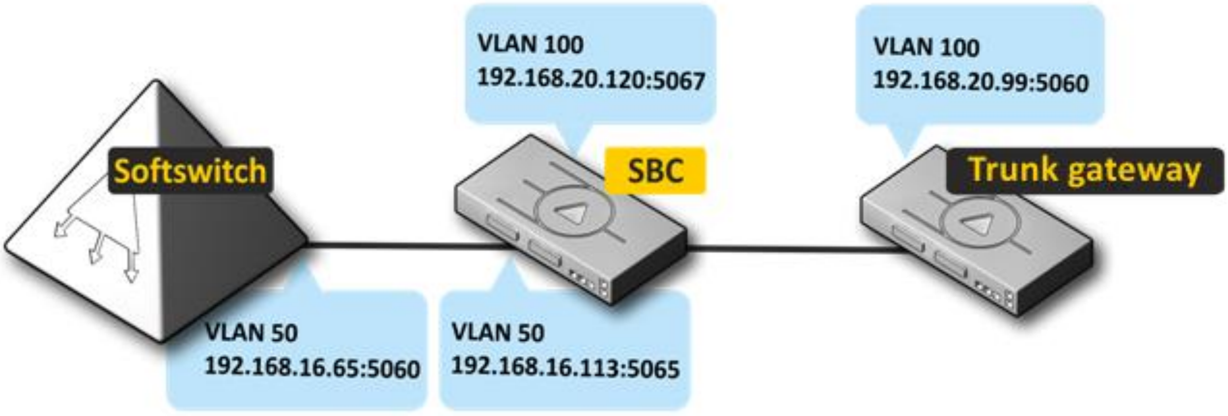
SIP Users

| № | Name | SIP transport | RADIUS profile | Transport protocol | NAT subscribers | NAT keep-alive timeout, sec | SIP domain | Rule set |
|---|---|---|---|---|---|---|---|---|
| 0 | gateway | 20.120_5062 | Not selected | UDP-only | - | - | | to_softswitch |

8. To apply the settings, save the configuration to Flash (menu **Service/Save configuration to flash, section 4.1.12**).

## 2. Configuration of SBC for SIP trunks

### Use Case



**SBC does not analyze the types of traffic (subscriber or sip trunk); you must use different ports for different traffic.**

### SBC configuration procedure

1. Interface configuration.

See section 1 **Configuration of SBC for SIP subscribers** of this Appendix.

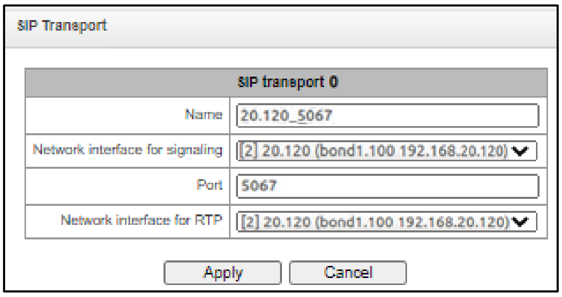
2. Configuration of media for SIP.

See section 1 **Configuration of SBC for SIP subscribers** of this Appendix.

3. SIP transport configuration (menu **SBC Configuration/SIP transport, section 4.1.3.1**).

   a. Add a SIP transport in the trunk gateway destination.

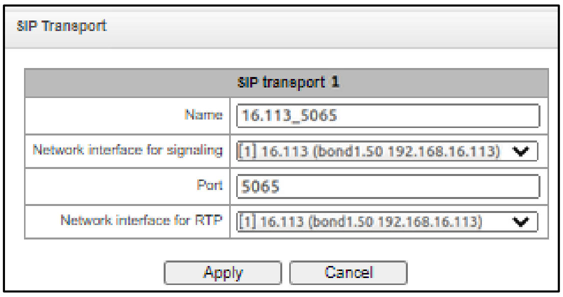
Interface parameters:
*network interface 20.120;*
*signalling port — 5067;*
*media — 20.120.*


SIP Transport

| SIP transport 0 | |
|---|---|
| Name | 20.120_5067 |
| Network interface for signaling | [2] 20.120 (bond1.100 192.168.20.120) |
| Port | 5067 |
| Network interface for RTP | [2] 20.120 (bond1.100 192.168.20.120) |

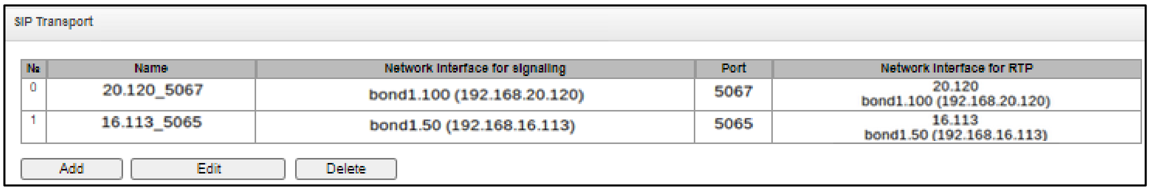
   b. Add a SIP transport in the Softswitch destination.

Interface parameters:
*network interface 16.113;*
*signalling port — 5065;*
*media — 16.113.*


SIP Transport

| SIP transport 1 | |
|---|---|
| Name | 16.113_5065 |
| Network interface for signaling | [1] 16.113 (bond1.50 192.168.16.113) |
| Port | 5065 |
| Network interface for RTP | [1] 16.113 (bond1.50 192.168.16.113) |

c. The SIP transport table will be as follows:

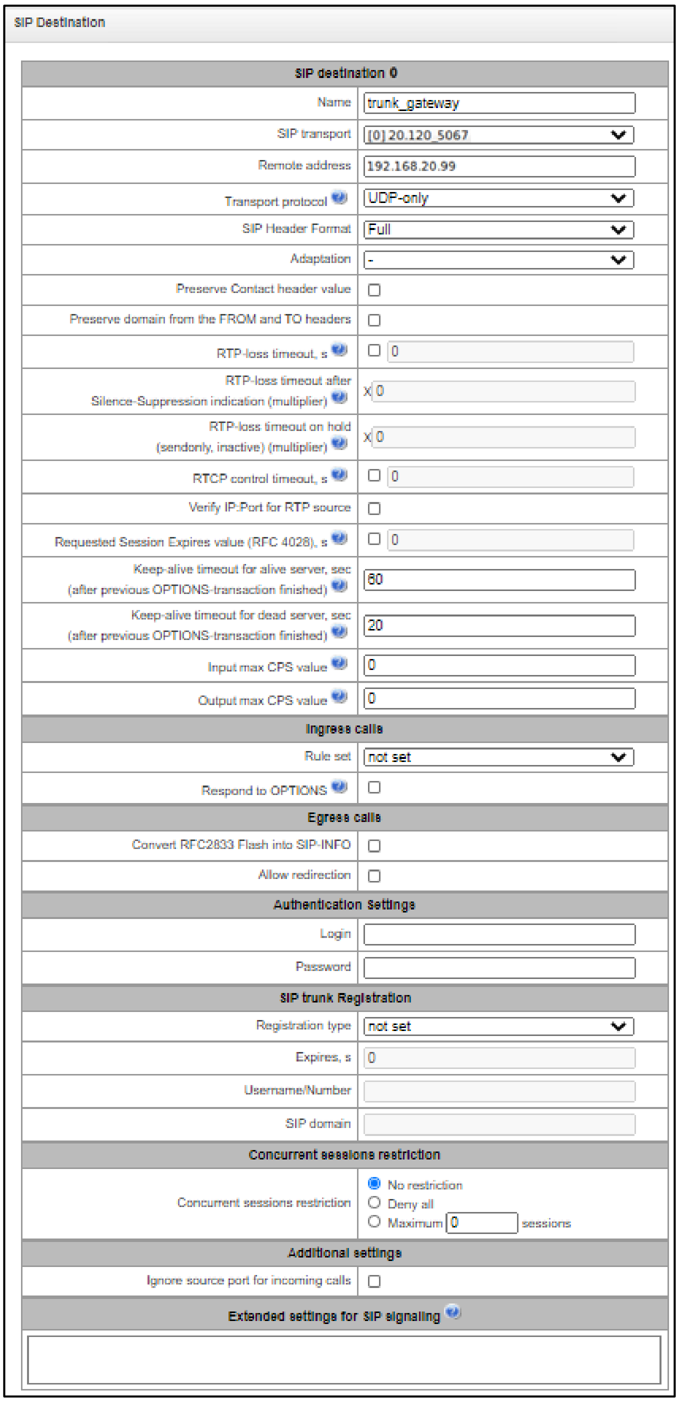


SIP Transport

| № | Name | Network interface for signaling | Port | Network interface for RTP |
|---|---|---|---|---|
| 0 | 20.120_5067 | bond1.100 (192.168.20.120) | 5067 | 20.120<br>bond1.100 (192.168.20.120) |
| 1 | 16.113_5065 | bond1.50 (192.168.16.113) | 5065 | 16.113<br>bond1.50 (192.168.16.113) |

4. SIP destination configuration (menu **SBC Configuration/SIP Destination, section 4.1.3.2**).

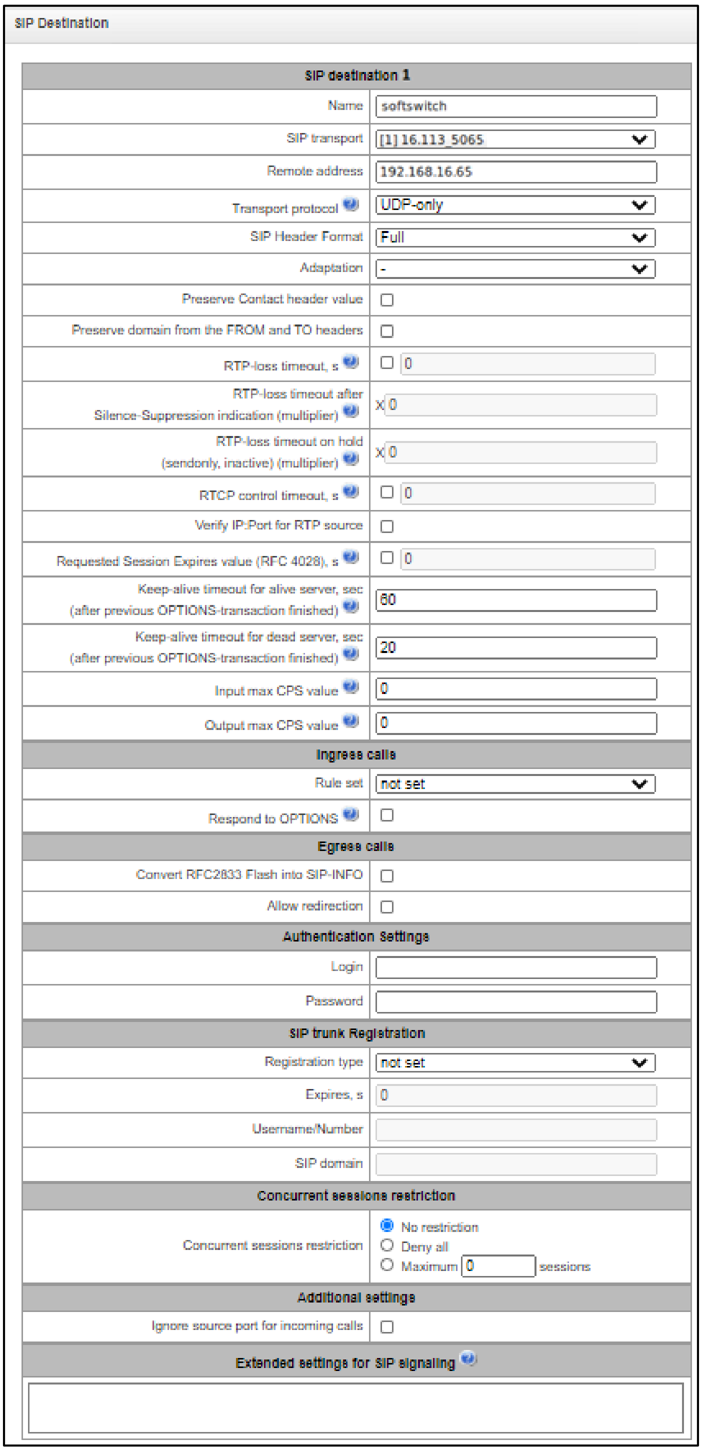
a. Add a SIP destination in the trunk gateway destination (the *«Rule set»* field does not need to be filled in at this point).



SIP Destination

| | |
|---|---|
| **SIP destination 0** | |
| Name | trunk_gateway |
| SIP transport | [0] 20.120_5067 |
| Remote address | 192.168.20.99 |
| Transport protocol | UDP-only |
| SIP Header Format | Full |
| Adaptation | - |
| Preserve Contact header value | □ |
| Preserve domain from the FROM and TO headers | □ |
| RTP-loss timeout, s | □ 0 |
| RTP-loss timeout after Silence-Suppression indication (multiplier) | x 0 |
| RTP-loss timeout on hold (sendonly, inactive) (multiplier) | x 0 |
| RTCP control timeout, s | □ 0 |
| Verify IP:Port for RTP source | □ |
| Requested Session Expires value (RFC 4028), s | □ 0 |
| Keep-alive timeout for alive server, sec (after previous OPTIONS-transaction finished) | 60 |
| Keep-alive timeout for dead server, sec (after previous OPTIONS-transaction finished) | 20 |
| Input max CPS value | 0 |
| Output max CPS value | 0 |
| **Ingress calls** | |
| Rule set | not set |
| Respond to OPTIONS | □ |
| **Egress calls** | |
| Convert RFC2833 Flash into SIP-INFO | □ |
| Allow redirection | □ |
| **Authentication Settings** | |
| Login | |
| Password | |
| **SIP trunk Registration** | |
| Registration type | not set |
| Expires, s | 0 |
| Username/Number | |
| SIP domain | |
| **Concurrent sessions restriction** | |
| Concurrent sessions restriction | ● No restriction<br>○ Deny all<br>○ Maximum 0 sessions |
| **Additional settings** | |
| Ignore source port for incoming calls | □ |
| **Extended settings for SIP signaling** | |

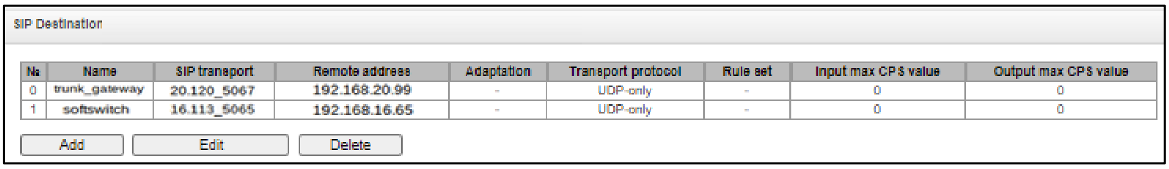
b. Add a SIP destination in the Softswitch destination (the *«Rule set»* field does not need to be filled in at this point).



SIP Destination

| SIP destination 1 | |
|---|---|
| Name | softswitch |
| SIP transport | [1] 16.113_5065 |
| Remote address | 192.168.16.65 |
| Transport protocol | UDP-only |
| SIP Header Format | Full |
| Adaptation | - |
| Preserve Contact header value | □ |
| Preserve domain from the FROM and TO headers | □ |
| RTP-loss timeout, s | □ 0 |
| RTP-loss timeout after Silence-Suppression indication (multiplier) | x 0 |
| RTP-loss timeout on hold (sendonly, inactive) (multiplier) | x 0 |
| RTCP control timeout, s | □ 0 |
| Verify IP:Port for RTP source | □ |
| Requested Session Expires value (RFC 4028), s | □ 0 |
| Keep-alive timeout for alive server, sec (after previous OPTIONS-transaction finished) | 60 |
| Keep-alive timeout for dead server, sec (after previous OPTIONS-transaction finished) | 20 |
| Input max CPS value | 0 |
| Output max CPS value | 0 |
| **Ingress calls** | |
| Rule set | not set |
| Respond to OPTIONS | □ |
| **Egress calls** | |
| Convert RFC2833 Flash into SIP-INFO | □ |
| Allow redirection | □ |
| **Authentication Settings** | |
| Login | |
| Password | |
| **SIP trunk Registration** | |
| Registration type | not set |
| Expires, s | 0 |
| Username/Number | |
| SIP domain | |
| **Concurrent sessions restriction** | |
| Concurrent sessions restriction | ● No restriction<br>○ Deny all<br>○ Maximum 0 sessions |
| **Additional settings** | |
| Ignore source port for incoming calls | □ |
| **Extended settings for SIP signaling** | |

c. The SIP destination table will be as follows:

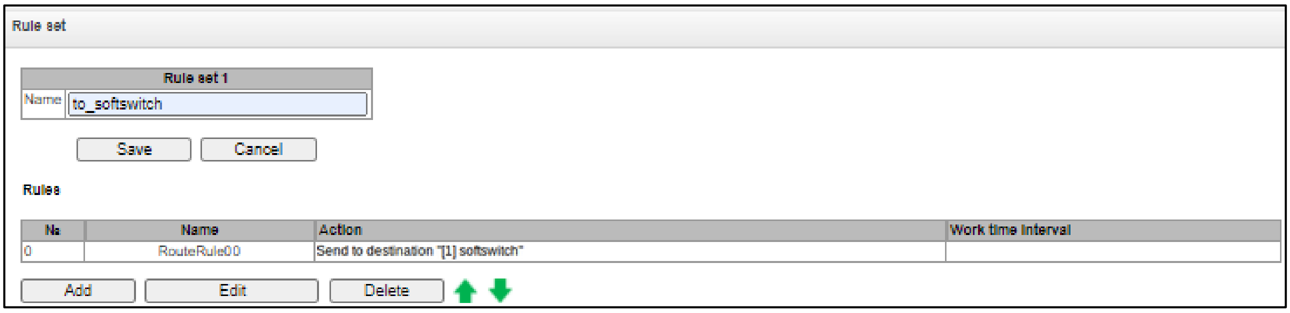


SIP Destination

| № | Name | SIP transport | Remote address | Adaptation | Transport protocol | Rule set | Input max CPS value | Output max CPS value |
|---|---|---|---|---|---|---|---|---|
| 0 | trunk_gateway | 20.120_5067 | 192.168.20.99 | - | UDP-only | - | 0 | 0 |
| 1 | softswitch | 16.113_5065 | 192.168.16.65 | - | UDP-only | - | 0 | 0 |

5. Rule set configuration (menu **SBC Configuration/Rule set, section 4.1.3.5**).

Create two rule sets. In the first *«SIP Destination»* field, specify the destination that was configured for Softswitch. In the second, specify the trunk gateway destination.

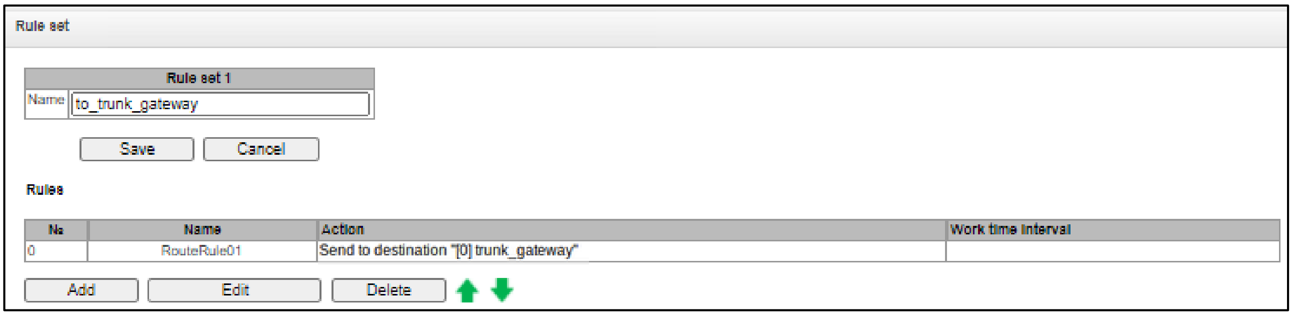


Rule set

| Rule set 1 | |
|---|---|
| Name | to_softswitch |

Rules

| № | Name | Action | Work time interval |
|---|---|---|---|
| 0 | RouteRule00 | Send to destination "[1] softswitch" | |



Rule set

| Rule set 1 | |
|---|---|
| Name | to_trunk_gateway |

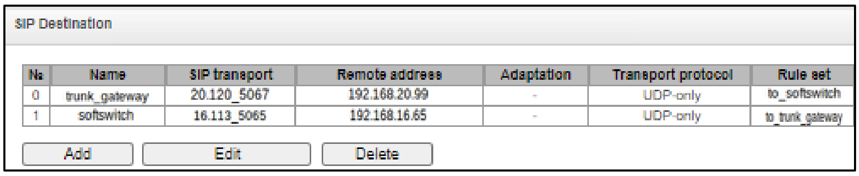
Rules

| № | Name | Action | Work time interval |
|---|---|---|---|
| 0 | RouteRule01 | Send to destination "[0] trunk_gateway" | |

6. Bind the rule to destinations.

To bind in the destination settings for Softswitch in the *«SIP Users»* section select a rule set, where in the field *«SIP destination»* specified the trunk gateway destination. Accordingly, in the destination settings for the trunk gateway, select a different set of rules, directing everything to Softswitch.

The SIP destination table will be as follows:



SIP Destination

| № | Name | SIP transport | Remote address | Adaptation | Transport protocol | Rule set |
|---|---|---|---|---|---|---|
| 0 | trunk_gateway | 20.120_5067 | 192.168.20.99 | - | UDP-only | to_softswitch |
| 1 | softswitch | 16.113_5065 | 192.168.16.65 | - | UDP-only | to_trunk_gateway |

7. To apply the settings, save the configuration to Flash (menu **Service/Save configuration to flash, section 4.1.12**).

# APPENDIX C. SBC RESERVATION FUNCTION PROVISION

Starting from firmware version 1.7.0 the redundancy feature is implemented. This feature is automatically activated by installing an additional SBC-RESERVE license. The principle of operation is that the redundant device is in sleep mode (SLAVE), without any features and without its IP address in the network, constantly watching the primary device (MASTER) and, as soon as MASTER fails SLAVE takes over all functions, completely replacing the failed MASTER. In order to fully duplicate the function, the redundant device constantly receives from the master the current configuration, subscriber database and other necessary files for work.

✓ **Only single-type SBC-1000 or SBC-2000 devices are used to provide redundancy functions.**

Consider the connection schemes:

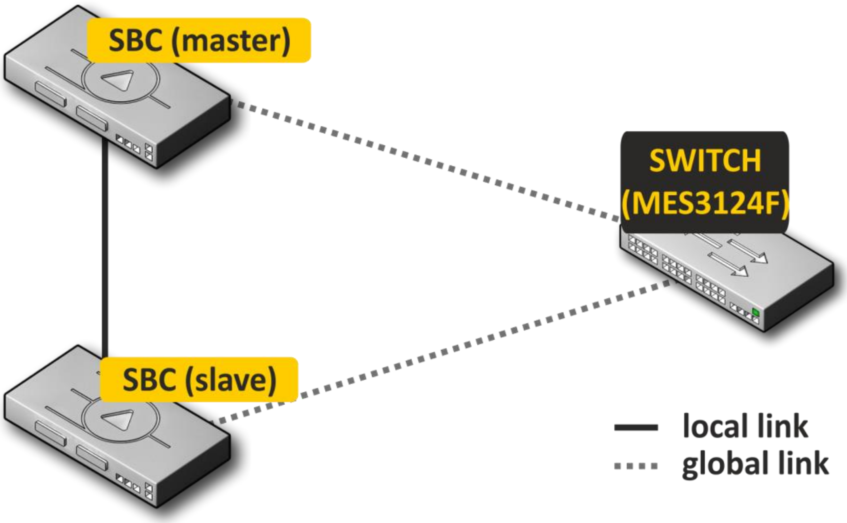


Figure 33 — Redundancy scheme with one switch

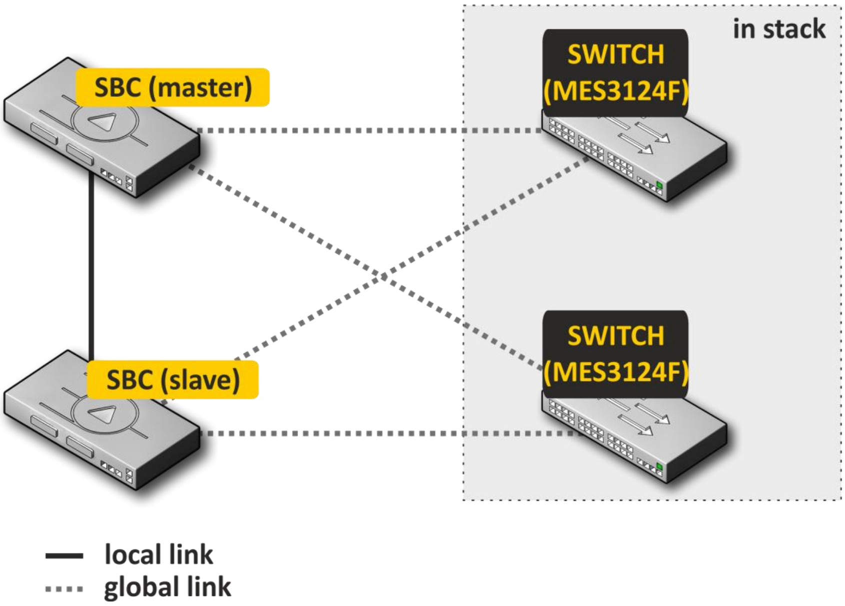


Figure 34 — Redundancy scheme with two switches in stack

During redundancy, 2 types of front-port are allocated on the device, these are local and global. On SBC-1000, the local port is 0, the global ports are 1 and 2, on the SBC-2000 the local ports are 0 and 1, the global ports are 2 and 3. When connecting devices, you need to communicate simultaneously on a local and global link. The redundancy scheme works over IPv6, during which the devices exchange configuration and other files necessary to maintain up-to-date information. The local link uses 4091 VLAN, the global 4092 VLAN. In the case of a break in the local link, the devices exchange operating files on the global link.

If one of the links is disconnected, the device initiates an alarm.

**Reserve connection and configuration procedure**

Consider the case of connecting to two MES switches in a stack (Figure 35). Initial state: two SBC of the same type with a reserve license, two MES switches in the stack. The stack on the switches should be configured according to the switch documentation.

First, you should configure the service VLAN pass-through on the switches. On the ports where the global SBC links will be connected, VLAN 4092 must be allowed to pass through. The ports must also pass through other VLANs configured on the SBC. In addition, the ports to which the SBC will connect should be combined into a port-channel. The final scheme at this stage will look as follows:

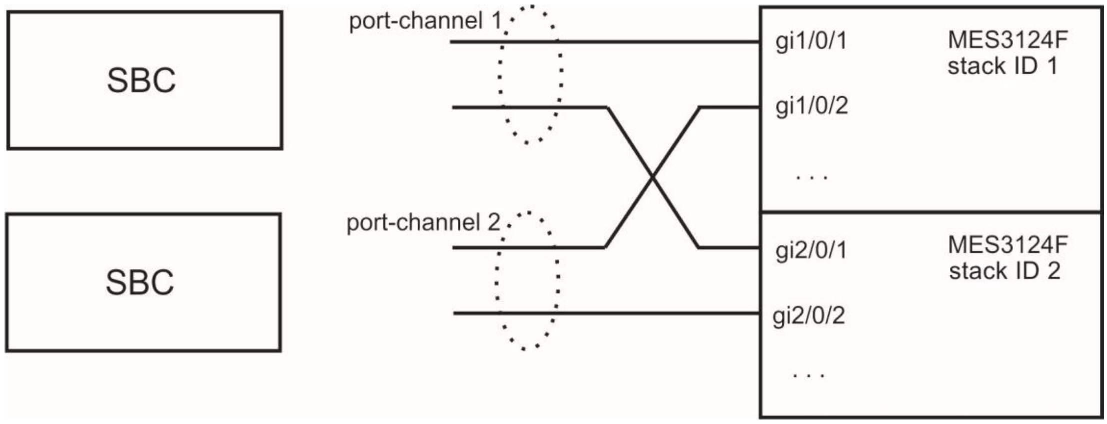


Figure 35 — Scheme of the ports association in the port-chanel

The next step is to connect the master SBC. At this stage, only the global links are connected. The SBC is then started and becomes the master. The scheme at this stage will look as follows:

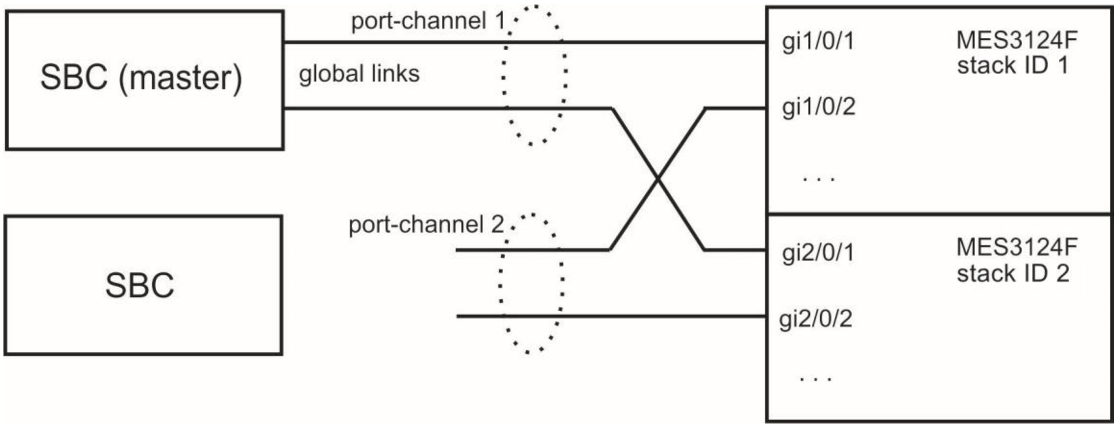


Figure 36 — Master SBC connection scheme

After that, the slave SBC is connected to the master SBC by a local link. At this point, wait until the devices have detected each other and are operating as a slave-master pair (see Monitoring - Reservation). The scheme at this stage will look as follows:

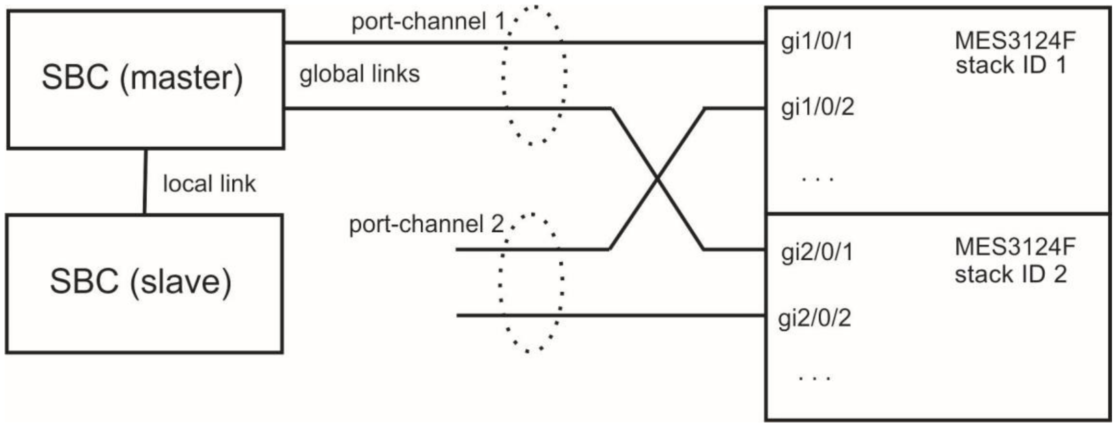


Figure 37 — Slave SBC connection scheme

After the slave-master pair has been formed, you can connect global links to the slave device:

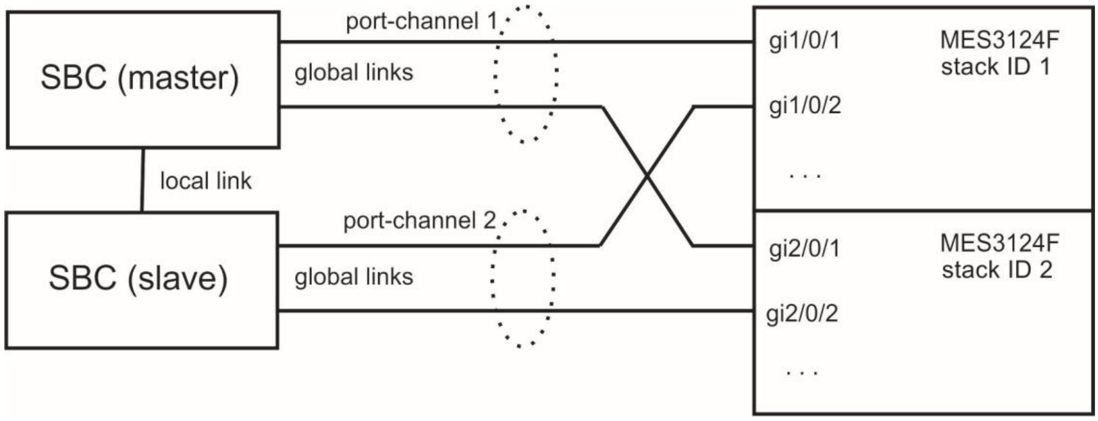


Figure 38 — Global links connection scheme

This completes the assembly of the reserve. In monitoring, make sure that both SBC see each other on both the local and global links.

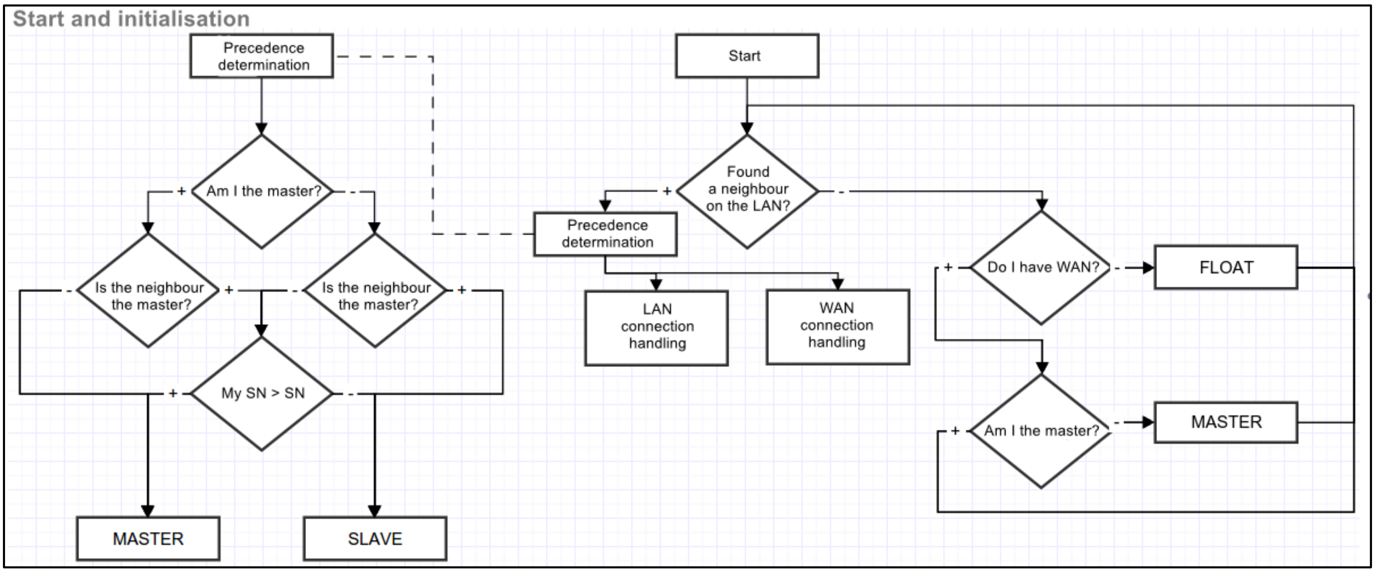
If there are problems with the master-slave relationship or lack of visibility over the local and global links, check that all configuration steps have been completed correctly.

**Seniority determination**

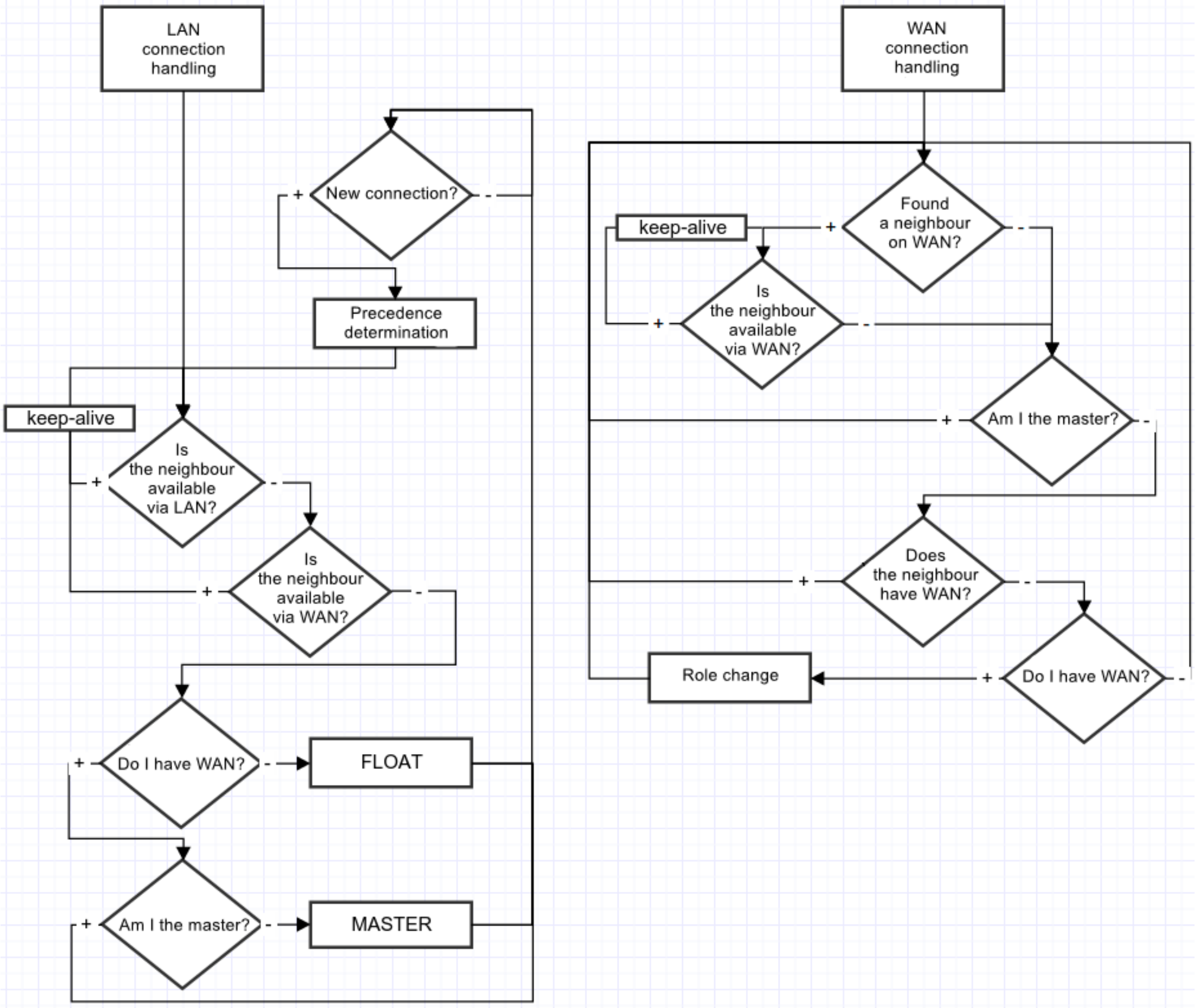
The following algorithm is used to determine which device is MASTER or SLAVE:

- If no local links are active when the device is turned on, the device becomes MASTER.
- If no local links are active when the device is turned on, the device becomes SLAVE.
- If you connect SLAVE to a device that is MASTER during operation, the seniority will not change.
- If you connect a MASTER to a device that is a MASTER in the process, the seniority will be determined based on the serial number, whoever has a larger serial number will become a MASTER.

The block scheme for determining seniority:



Handling of connection via global or local link.



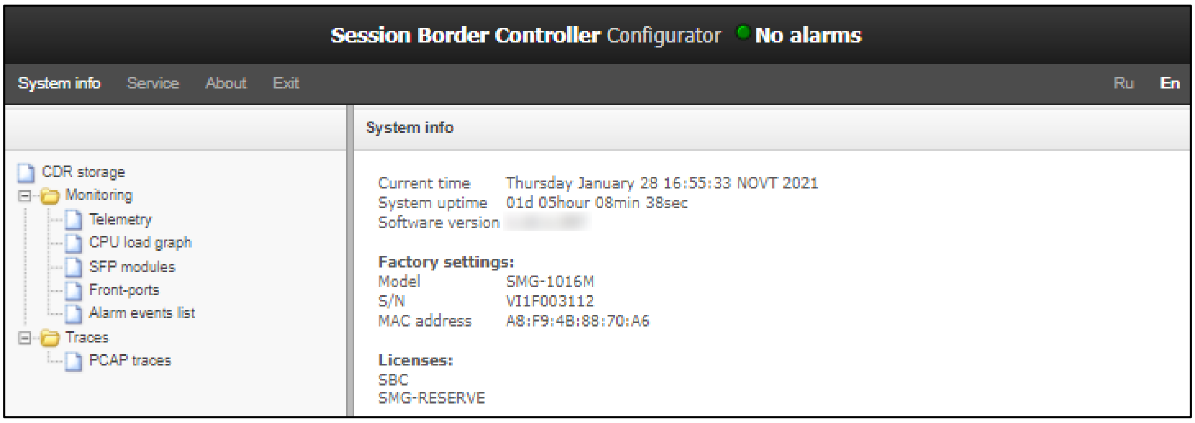
**When connecting a device to an already operating device, you must disconnect all WAN links on the device to be connected, connect the LAN link to an operating (MASTER) SBC, wait for negotiation, connect the WAN links to SLAVE, otherwise the newly connected device may be detected as MASTER and transfer its irrelevant Operation files.**

Operation files are transferred immediately after connecting to MASTER, each time after writing the configuration to flash, 10 seconds after each configuration change, and periodically once every 180 seconds.

List of transferred files:

- file of configuration recorded to flash;
- Current running configuration file;
- keys for creating ssh-tunnels;
- registered subscribers database;
- linux user files;
- Web interface and CLI user password files;
- all dynamic firewall address lists;
- https keys and certificates;
- all CDR files.

During operation, the user can access the SLAVE Web interface by going to the «Monitoring» - «Reservation» - «Open Web» tab, or by the following link: http://192.168.0.100:8080/login, where instead of 192.168.0.100 enter the MASTER IP address.



System info

Current time Thursday January 28 16:55:33 NOVT 2021
System uptime 01d 05hour 08min 38sec
Software version [redacted]

Factory settings:
Model SMG-1016M
S/N VI1F003112
MAC address A8:F9:4B:88:70:A6

Licenses:
SBC
SMG-RESERVE

# APPENDIX D. MANAGEMENT AND MONITORING VIA SNMP

SBC supports monitoring and configuration via Simple Network Management Protocol (SNMP).

Monitoring functions:

- Collection data on device, established sensors and software;
- SIP interface state;
- SIP statistics collection

Management functions:

- Firmware version updating;
- Firmware version updating;
- device reboot;
- SIP subscribers management.

The following format of the description will be accepted for the 'Inquiry description' column of OID description tables:

- Get — an object or tree value can be displayed by sending 'GetRequest'.
- Set — an object value can be set by sending 'SetRequest' (Please pay attention if you set value by SET inquiry, you need to specify OID in 'OID.0' form);
- {} — object name or OID;
- N — integer type of numeric parameter is used in the command;
- U — unsigned integer  type of numeric parameter is used in the command;
- S — string parameter is used in the command;
- A — IP address is used in the command (Please pay attention, some commands, using IP address as argument, have string type of data – 's').

Table D.1 — Command examples

| Request description | Command |
|---|---|
| Get {} | snmpwalk -v2c -c public -m +ELTEX-SBC $ip_sbc activeCallCount |
| Get {}.x | snmpwalk -v2c -c public -m +ELTEX-SBC $ip_sbc pmExist.1<br>snmpwalk -v2c -c public -m +ELTEX-SBC $ip_sbc pmExist.2<br>etc. |
| Set {} N | snmpset -v2c -c public -m +ELTEX-SBC $ip_sbc \\<br>sbcSyslogHistoryPort.0 i 514 |
| Set {} 1 | snmpset -v2c -c private -m +ELTEX-SBC $ip_sbc sbcReboot.0 i 1 |
| Set {} U111 | snmpset -v2c -c public -m +ELTEX-SBC $ip_sbc \\<br>getGroupUserByID.0 u 2 |
| Set {} S | snmpset -v2c -c private -m +ELTEX-SBC $ip_sbc \\<br>sbcUpdateFw.0 s \\<br>"smg1016m_firmware_sbc_1.9.0.51.bin 192.0.2.2" |
| Set {} "NULL"111 | snmpset -v2c -c private -m +ELTEX-SBC $ip_sbc \\<br>getUserByNumber.0 s "NULL" |
| Set {} A111 | snmpset -v2c -c private -m +ELTEX-SBC $ip_sbc \\<br>sbcSyslogTracesAddress.0 a 192.0.2.44 |

**Examples of query execution:**

The following queries are equivalent. An example request of sbcActiveCallsCount object, which displays the number of current calls to the SBC.

```
$ snmpwalk -v2c -c public -m +ELTEX-SBC 192.0.2.1 sbcActiveCallCount
ELTEX-SBC::sbcActiveCallCount.0 = INTEGER: 22

$ snmpwalk -v2c -c public -m +ELTEX-SBC 192.0.2.1 sbc.42.1
ELTEX-SBC::sbcActiveCallCount.0 = INTEGER: 22

$ snmpwalk -v2c -c public -m +ELTEX-SBC 192.0.2.1 1.3.6.1.4.1.35265.1.49.42.1
ELTEX-SBC::sbcActiveCallCount.0 = INTEGER: 22

$ snmpwalk -v2c -c public 192.0.2.1 1.3.6.1.4.1.35265.1.49.42.1
SNMPv2-SMI::enterprises.35265.1.49.42.1.0 = INTEGER: 22
```

**OID Description of the ELTEX-SMG MIB**

Table D.2 – Common information and sensors

| Name | OID | Requests | Description |
|---|---|---|---|
| sbc | 1.3.6.1.4.1.35265.1.49 | `Get {}` | Root object of OID tree |
| sbcDevName | 1.3.6.1.4.1.35265.1.49.1 | `Get {}` | Device name |
| sbcDevType | 1.3.6.1.4.1.35265.1.49.2 | `Get {}` | Device type<br>(always 49) |
| sbcFwVersion | 1.3.6.1.4.1.35265.1.49.3 | `Get {}` | Firmware version |
| sbcUptime | 1.3.6.1.4.1.35265.1.49.5 | `Get {}` | Firmware operation time |
| sbcUpdateFw | 1.3.6.1.4.1.35265.1.49.25 | `Set {} S` | Firmware update. Send a Set inquiry with space-separated parameters:<br>- the name of the file without spaces;<br>- TFTP server address |
| sbcReboot | 1.3.6.1.4.1.35265.1.49.27 | `Set {} 1` | Reboot of the device |
| sbcSave | 1.3.6.1.4.1.35265.1.49.29 | `Set {} 1` | Saving the configuration |
| sbcFreeSpace | 1.3.6.1.4.1.35265.1.49.32 | `Get {}` | Free space on embedded flash memory |
| sbcFreeRam | 1.3.6.1.4.1.35265.1.49.33 | `Get {}` | The value of free RAM |
| sbcMonitoring | 1.3.6.1.4.1.35265.1.49.35 | `Get {}` | Display temperature sensors and fan rate, root object |
| sbcTemperature1 | 1.3.6.1.4.1.35265.1.49.35.1 | `Get {}` | Temperature sensor 1 |
| sbcTemperature2 | 1.3.6.1.4.1.35265.1.49.35.2 | `Get {}` | Temperature sensor 2 |
| sbcFan0 | 1.3.6.1.4.1.35265.1.49.35.3 | `Get {}` | Fan speed sensor 1 |
| sbcFan1 | 1.3.6.1.4.1.35265.1.49.35.4 | `Get {}` | Fan speed sensor 2 |
| sbcFan2 | 1.3.6.1.4.1.35265.1.49.35.5 | `Get {}` | Fan speed sensor 3 |
| sbcFan3 | 1.3.6.1.4.1.35265.1.49.35.6 | `Get {}` | Fan speed sensor 4 |
| sbcPowerModuleTable | 1.3.6.1.4.1.35265.1.49.36 | `Get {}` | Information on sate of a power supply unit, root object. |

| Name | OID | Requests | Description |
|---|---|---|---|
| | | | For subordinate object, 1 or 2 is specified as number of power supply unit. |
| sbcPowerModuleEntry | 1.3.6.1.4.1.35265.1.49.36.1 | `Get {}` | see sbcPowerModuleTable |
| pmExist | 1.3.6.1.4.1.35265.1.49.36.1.2.x | `Get {}.x` | Status of the battery installation<br>1 — installed<br>2 — not installed |
| pmPower | 1.3.6.1.4.1.35265.1.49.36.1.3.x | `Get {}.x` | Power units are<br>1 — enabled<br>2 — disabled |
| pmType | 1.3.6.1.4.1.35265.1.49.36.1.4.x | `Get {}.x` | Type of the installed PSU<br>1 — PM48/12<br>2 — PM220/12<br>3 — PM220/12V<br>4 — PM150-220/12 |
| sbcCpuLoadTable | 1.3.6.1.4.1.35265.1.49.37 | `Get {}` | CPU load, root object. Shows the percentage of CPU usage by task type. For child objects, specify the CPU number:<br>sbc1016M — 1<br>sbc2016 — 1..4 |
| sbcCpuLoadEntry | 1.3.6.1.4.1.35265.1.49.37.1 | `Get {}` | see sbcCpuLoadTable |
| cpuUsr | 1.3.6.1.4.1.35265.1.49.37.1.2.x | `Get {}.x` | % CPU, user applications |
| cpuSys | 1.3.6.1.4.1.35265.1.49.37.1.3.x | `Get {}.x` | % CPU, kernel applications |
| cpuNic | 1.3.6.1.4.1.35265.1.49.37.1.4.x | `Get {}.x` | % CPU, applications with changed priority |
| cpuIdle | 1.3.6.1.4.1.35265.1.49.37.1.5. | `Get {}.x` | % CPU idle |
| cpuIo | 1.3.6.1.4.1.35265.1.49.37.1.6.x | `Get {}.x` | % CPU, I/o operations |
| cpuIrq | 1.3.6.1.4.1.35265.1.49.37.1.7.x | `Get {}.x` | % CPU, hardware interrupt processing |
| cpuSirq | 1.3.6.1.4.1.35265.1.49.37.1.8.x | `Get {}.x` | % CPU, the processing of firmware interrupts |
| cpuUsage | 1.3.6.1.4.1.35265.1.49.37.1.9.x | `Get {}.x` | % CPU, total utilization |
| activeCallCount | 1.3.6.1.4.1.35265.1.49.42.1 | `Get {}` | Number of current active calls |
| registrationCount | 1.3.6.1.4.1.35265.1.49.42.2 | `Get {}` | Current number registrations |

Table D. 3 – Syslog settings

| Name | OID | Requests | Description |
|---|---|---|---|
| sbcSyslog | 1.3.6.1.4.1.35265.1.49.34 | `Get {}` | Syslog settings, root object |
| sbcSyslogHistory | 1.3.6.1.4.1.35265.1.49.34.2 | `Get {}` | Set up logging the command history to syslog, root object |
| sbcSyslogHistoryAddress | 1.3.6.1.4.1.35265.1.49.34.2.1 | `Get {}`<br>`Set {} S` | IP address of syslog to receive the command history |
| sbcSyslogHistoryPort | 1.3.6.1.4.1.35265.1.49.34.2.2 | `Get {}`<br>`Set {} N` | The syslog server port to receive the command history |

| Name | OID | Requests | Description |
|---|---|---|---|
| sbcSyslogHistoryLVL | 1.3.6.1.4.1.35265.1.49.34.2.3 | Get {}<br>Set {} N | Log verbosity level<br>0 — disable logging;<br>1 — standard;<br>2 — full |
| sbcSyslogHistoryRowStatus | 1.3.6.1.4.1.35265.1.49.34.2.4 | Get {}<br>Set {} 1 | To apply changes to the logging history commands |
| sbcSyslogConfig | 1.3.6.1.4.1.35265.1.49.34.3 | Get {} | System log settings |
| sbcSyslogConfigLogsEnabled | 1.3.6.1.4.1.35265.1.49.34.3.1 | Get {}<br>Set {} N | Enable logging<br>1 — enable;<br>2 — disable |
| sbcSyslogConfigSendToServer | 1.3.6.1.4.1.35265.1.49.34.3.2 | Get {}<br>Set {} N | Send messages to syslog server<br>1 — enable;<br>2 — disable |
| sbcSyslogConfigAddress | 1.3.6.1.4.1.35265.1.49.34.3.3 | Get {}<br>Set {} S | The IP address of the syslog server |
| sbcSyslogConfigPort | 1.3.6.1.4.1.35265.1.49.34.3.4 | Get {}<br>Set {} N | Syslog server port |
| sbcSyslogConfigRowStatus | 1.3.6.1.4.1.35265.1.49.34.3.5 | Get {}<br>Set {} 1 | Apply changes in the system log settings |

**View information on registered users**

In this description, the SNMP utility invocation commands will be represented by the following scripts for brevity and clarity:

**Swalk** script implements reading values:

```
#!/bin/bash
/usr/bin/snmpwalk -v2c -c public -m +ELTEX-SBC 192.0.2.1 "$@"
```

**Sset** script implements value setting:

```
#!/bin/bash
/usr/bin/snmpset -v2c -c private -m +ELTEX-SBC 192.0.2.1 "$@"
```

The following steps are required for viewing:

1) Reset search status;
2) Set the search criteria (optional);
3) Display information.

**An example of searching for a subscriber by number**

```
sset sbcSubResetSearch.0 i 1                  # reset search
sset getSbcSubBySubstring.0 s 40012           # set criteria
swalk tableOfSbcSubscribers                   # display results
```

**Result:**

```
ELTEX-SBC::subName.0 = STRING: 40012@tau.domain:5060

ELTEX-SBC::subUserAgent.0 = STRING: TAU-72 build 2.13.1 sofia-sip/1.12.10

ELTEX-SBC::subUserAddr.0 = STRING: 192.0.2.32:5060

ELTEX-SBC::subContacts.0 = STRING: <sip:40012@192.0.2.32:5060>;expires=119
```

ELTEX-SBC::subRegAddr.0 = STRING: 192.0.1.22:5080

ELTEX-SBC::subSipUser.0 = STRING: Users with RTP in VLAN 609

ELTEX-SBC::subSipDest.0 = STRING: SMG

ELTEX-SBC::subBloked.0 = INTEGER: 0

ELTEX-SBC::subRetries.0 = Gauge32: 0

ELTEX-SBC::subExpires.0 = Gauge32: 0

Table D.4 — View information on registered users

| Name | OID | Requests | Description |
|---|---|---|---|
| sbcSubSearchStatus | 1.3.6.1.4.1.35265.1.49.44.1 | `Get {}` | Status of search by criteria.<br>Without search — search is not performed;<br>Search by substring — substring search mode |
| sbcSubResetSearch | 1.3.6.1.4.1.35265.1.49.44.2 | `Set {} N` | Resets the search to the «without search» state. To reset, set any numeric value. |
| sbcSubCount | 1.3.6.1.4.1.35265.1.49.44.3 | `Get {}` | Total number of subscribers registered through SBC |
| getSbcSubBySubstring | 1.3.6.1.4.1.35265.1.49.44.4 | `Get {}`<br>`Set {} S` | Specifies a substring to search for in the registration list and sets the search to «search by substring» mode |
| tableOfSbcSubscribers | 1.3.6.1.4.1.35265.1.49.44.5 | `Get {}` | List of registered subscribers.<br>In the «without search» mode displays all subscribers.<br>In the «search by substring» mode displays all subscribers whose description contains the specified substring. |
| subName | 1.3.6.1.4.1.35265.1.49.44.5.1.2 | `Get {}` | Subscriber name (SIP URI) |
| subUserAgent | 1.3.6.1.4.1.35265.1.49.44.5.1.3 | `Get {}` | user-agent |
| subUserAddr | 1.3.6.1.4.1.35265.1.49.44.5.1.4 | `Get {}` | IP address and port from which the subscriber was registered |
| subContacts | 1.3.6.1.4.1.35265.1.49.44.5.1.5 | `Get {}` | Subscriber contact IP address and port |
| subRegAddr | 1.3.6.1.4.1.35265.1.49.44.5.1.6 | `Get {}` | Address of the registrar who approved the registration |
| subSipUser | 1.3.6.1.4.1.35265.1.49.44.5.1.7 | `Get {}` | Name of SIP Users from which the subscriber registered |
| subSipDest | 1.3.6.1.4.1.35265.1.49.44.5.1.8 | `Get {}` | Name of SIP Destination from which the registration was approved |
| subBloked | 1.3.6.1.4.1.35265.1.49.44.5.1.9 | `Get {}` | Subscriber blocking status |
| subRetries | 1.3.6.1.4.1.35265.1.49.44.5.1.10 | `Get {}` | Amount of failed access attempts |
| subExpires | 1.3.6.1.4.1.35265.1.49.44.5.1.11 | `Get {}` | Time after which registration will expire |

**View SIP statistics**

In this description, the SNMP utility invocation commands will be represented by the following scripts for brevity and clarity:

**Swalk** script implements reading values:

```
#!/bin/bash
/usr/bin/snmpwalk -v2c -c public -m +ELTEX-SBC 192.0.2.1 "$@"
```

**Sset** script implements value setting:

```
#!/bin/bash
/usr/bin/snmpset -v2c -c private -m +ELTEX-SBC 192.0.2.1 "$@"
```

The statistics are grouped into six groups by type:

1. Cumulative counters by SIP Users
2. Instant counters by SIP Users
3. Cumulative counters by SIP Transport
4. Instant counters by SIP Transport
5. Cumulative counters by SIP Destination
6. Instant counters by SIP Destination

The counter OID is formed as follows:

1.3.6.1.4.1.35265.1.49.43.<TYPE>.1.<COUNTER>.<ID>, where

TYPE — one of six counter types;

COUNTER — counter ID;

ID — ID of the object that the counter points to.

You can get the object ID from the ID column in the CLI. To do this, in SIP destination edit mode, give SIP users or SIP transport the show info command. The second way is to request an SNMP counter with COUNTER = 3 without specifying an ID.

**Examples:**

Requesting the names of all SIP Transports, note that in the response the next digit after the name requested by OID is the transport identifier, which can be further used in the queries:

```
swalk 1.3.6.1.4.1.35265.1.49.43.3.1.3

ELTEX-SBC::countStatTransportName.4 = STRING: 1.21_5068_rtp_69.121

ELTEX-SBC::countStatTransportName.5 = STRING: 118.164_5068

ELTEX-SBC::countStatTransportName.6 = STRING: user_0.21_5060_rtp_69_21

ELTEX-SBC::countStatTransportName.7 = STRING: user_0.21_5062

ELTEX-SBC::countStatTransportName.8 = STRING: trunk_1.21_5069

ELTEX-SBC::countStatTransportName.9 = STRING: trunk_0.21_5069

ELTEX-SBC::countStatTransportName.10 = STRING: 0.21_5066

ELTEX-SBC::countStatTransportName.12 = STRING: 2.21_5060

ELTEX-SBC::countStatTransportName.13 = STRING: 2.21_5065

ELTEX-SBC::countStatTransportName.14 = STRING: 2.21:5069
```

ELTEX-SBC::countStatTransportName.15 = STRING: 1.21_5061

ELTEX-SBC::countStatTransportName.16 = STRING: 172.30.0.1:5062

ELTEX-SBC::countStatTransportName.18 = STRING: test

ELTEX-SBC::countStatTransportName.19 = STRING: vlan609_dhcp

Requests by counters:

1.3.6.1.4.1.35265.1.49.43.3.1.9.20

TYPE = 3 — Cumulative counter by SIP Transport;

COUNTER = 9 — unsuccessful calls terminated with SIP codes 4xx;

ID = 20 — counter by SIP Transport with identifier 20.

ELTEX-SBC::countStatTransportAnswSuccessCalls.20 = Gauge32: 21946

1.3.6.1.4.1.35265.1.49.43.5.1.408.14

TYPE = 3 — Cumulative counter by SIP Destination;

COUNTER = 408 — unsuccessful calls terminated with SIP code 408;

ID = 14 — counter by SIP Destination with identifier 14.

ELTEX-SBC::countStatDestUnansw408.14 = Gauge32: 33

Table D.5 — View SIP statistics

| Name | OID | Requests | Description |
|---|---|---|---|
| sbcCallStatistics | 1.3.6.1.4.1.35265.1.49.43 | `Get {}` | Table with all SIP counters |
| tableOfCallCountStatUsers | 1.3.6.1.4.1.35265.1.49.43.1 | `Get {}` | Table with all cumulative SIP Users counters |
| countStatUserIndex | 1.3.6.1.4.1.35265.1.49.43.1.1.2 | `Get {}` | SIP Users indexes |
| countStatUserName | 1.3.6.1.4.1.35265.1.49.43.1.1.3 | `Get {}` | SIP Users names |
| countStatUserElapsedTime | 1.3.6.1.4.1.35265.1.49.43.1.1.4 | `Get {}` | Total time of active calls |
| countStatUserIncCalls | 1.3.6.1.4.1.35265.1.49.43.1.1.5 | `Get {}` | Number of incoming calls |
| countStatUserOutCallLegs | 1.3.6.1.4.1.35265.1.49.43.1.1.6 | `Get {}` | Number of outgoing calls |
| countStatUserMsgRcv | 1.3.6.1.4.1.35265.1.49.43.1.1.7 | `Get {}` | Number of incoming SIP messages |
| countStatUserMsgSend | 1.3.6.1.4.1.35265.1.49.43.1.1.8 | `Get {}` | Number of outgoing SIP messages |
| countStatUserAnswSuccessCalls | 1.3.6.1.4.1.35265.1.49.43.1.1.9 | `Get {}` | Number of successfully received calls |
| countStatUserAnswFinalErrCalls | 1.3.6.1.4.1.35265.1.49.43.1.1.10 | `Get {}` | Number of rejected calls |
| countStatUserUnanswOther4xx | 1.3.6.1.4.1.35265.1.49.43.1.1.11 | `Get {}` | Number of unanswered calls with SIP codes 4xx |
| countStatUserUnanswOther5xx | 1.3.6.1.4.1.35265.1.49.43.1.1.12 | `Get {}` | Number of unanswered calls with SIP codes 5xx |
| countStatUserUnanswOther6xx | 1.3.6.1.4.1.35265.1.49.43.1.1.13 | `Get {}` | Number of unanswered calls with SIP codes 6xx |
| countStatUserUnanswOtherUndef | 1.3.6.1.4.1.35265.1.49.43.1.1.14 | `Get {}` | Number of unanswered calls with SIP codes that are not included in other counters. |

| Name | OID | Requests | Description |
|---|---|---|---|
| countStatUserRedirectCalls<CODE><br>where CODE — one of values:<br>300, 301, 302, 305, 308 | 1.3.6.1.4.1.35265.1.49.43.1.1.300<br>...<br>1.3.6.1.4.1.35265.1.49.43.1.1.308 | Get {} | Individual counters by codes — number of forwarded calls (completed by SIP codes 3xx) |
| countStatUserUnansw<CODE><br>where CODE — one of values:<br>400, 401, 402, 403, 404, 405, 406, 407, 408, 410, 413, 414, 415, 416, 420, 421, 422, 423, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 493, 500, 501, 502, 503, 504, 505, 513, 580, 600, 603, 604, 606 | 1.3.6.1.4.1.35265.1.49.43.1.1.400<br>...<br>1.3.6.1.4.1.35265.1.49.43.1.1.606 | Get {} | Individual counters by codes — number of forwarded calls (completed by SIP codes 4xx-6xx) |
| tableOfCallPerSecStatUsers | 1.3.6.1.4.1.35265.1.49.43.2 | Get {} | Table with all instant SIP Users counters |
| perSecStatUserIndex | 1.3.6.1.4.1.35265.1.49.43.2.1.2 | Get {} | SIP Users indexes |
| perSecStatUserName | 1.3.6.1.4.1.35265.1.49.43.2.1.3 | Get {} | SIP Users names |
| perSecStatUserElapsedTime | 1.3.6.1.4.1.35265.1.49.43.2.1.4 | Get {} | Total time of active calls |
| perSecStatUserIncCalls | 1.3.6.1.4.1.35265.1.49.43.2.1.5 | Get {} | Number of incoming calls |
| perSecStatUserOutCallLegs | 1.3.6.1.4.1.35265.1.49.43.2.1.6 | Get {} | Number of outgoing calls |
| perSecStatUserMsgRcv | 1.3.6.1.4.1.35265.1.49.43.2.1.7 | Get {} | Number of incoming SIP messages |
| perSecStatUserMsgSend | 1.3.6.1.4.1.35265.1.49.43.2.1.8 | Get {} | Number of outgoing SIP messages |
| perSecStatUserAnswSuccessCalls | 1.3.6.1.4.1.35265.1.49.43.2.1.9 | Get {} | Number of successfully received calls |
| perSecStatUserAnswFinalErrCalls | 1.3.6.1.4.1.35265.1.49.43.2.1.10 | Get {} | Number of rejected calls |
| perSecStatUserUnanswOther4xx | 1.3.6.1.4.1.35265.1.49.43.2.1.11 | Get {} | Number of unanswered calls with SIP codes 4xx |
| perSecStatUserUnanswOther5xx | 1.3.6.1.4.1.35265.1.49.43.2.1.12 | Get {} | Number of unanswered calls with SIP codes 5xx |
| perSecStatUserUnanswOther6xx | 1.3.6.1.4.1.35265.1.49.43.2.1.13 | Get {} | Number of unanswered calls with SIP codes 6xx |
| perSecStatUserUnanswOtherUndef | 1.3.6.1.4.1.35265.1.49.43.2.1.14 | Get {} | Number of unanswered calls with SIP codes that are not included in other counters. |
| perSecStatUserRedirectCalls<CODE><br>where CODE — one of values:<br>300, 301, 302, 305, 308 | 1.3.6.1.4.1.35265.1.49.43.2.1.300<br>...<br>1.3.6.1.4.1.35265.1.49.43.2.1.308 | Get {} | Individual counters by codes — number of forwarded calls (completed by SIP codes 3xx) |
| perSecStatUserUnansw<CODE> | 1.3.6.1.4.1.35265.1.49.43.2.1.400<br>...<br>1.3.6.1.4.1.35265.1.49.43.2.1.606 | Get {} | Individual counters by codes — number of forwarded calls (completed by SIP codes 4xx-6xx) |

| Name | OID | Requests | Description |
|---|---|---|---|
| where CODE — one of values:<br>400, 401, 402, 403, 404, 405, 406, 407, 408, 410, 413, 414, 415, 416, 420, 421, 422, 423, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 493, 500, 501, 502, 503, 504, 505, 513, 580, 600, 603, 604, 606 | | | |
| tableOfCallCountStatTransport | 1.3.6.1.4.1.35265.1.49.43.3 | `Get {}` | Table with all cumulative SIP Transport counters |
| countStatTransportIndex | 1.3.6.1.4.1.35265.1.49.43.3.1.2 | `Get {}` | SIP Transport indexes |
| countStatTransportName | 1.3.6.1.4.1.35265.1.49.43.3.1.3 | `Get {}` | SIP Transport names |
| countStatTransportElapsedTime | 1.3.6.1.4.1.35265.1.49.43.3.1.4 | `Get {}` | Total time of active calls |
| countStatTransportIncCalls | 1.3.6.1.4.1.35265.1.49.43.3.1.5 | `Get {}` | Number of incoming calls |
| countStatTransportOutCallLegs | 1.3.6.1.4.1.35265.1.49.43.3.1.6 | `Get {}` | Number of outgoing calls |
| countStatTransportMsgRcv | 1.3.6.1.4.1.35265.1.49.43.3.1.7 | `Get {}` | Number of incoming SIP messages |
| countStatTransportMsgSend | 1.3.6.1.4.1.35265.1.49.43.3.1.8 | `Get {}` | Number of outgoing SIP messages |
| countStatTransportAnswSuccessCalls | 1.3.6.1.4.1.35265.1.49.43.3.1.9 | `Get {}` | Number of successfully received calls |
| countStatTransportAnswFinalErrCalls | 1.3.6.1.4.1.35265.1.49.43.3.1.10 | `Get {}` | Number of rejected calls |
| countStatTransportUnanswOther4xx | 1.3.6.1.4.1.35265.1.49.43.3.1.11 | `Get {}` | Number of unanswered calls with SIP codes 4xx |
| countStatTransportUnanswOther5xx | 1.3.6.1.4.1.35265.1.49.43.3.1.12 | `Get {}` | Number of unanswered calls with SIP codes 5xx |
| countStatTransportUnanswOther6xx | 1.3.6.1.4.1.35265.1.49.43.3.1.13 | `Get {}` | Number of unanswered calls with SIP codes 6xx |
| countStatTransportUnanswOtherUndef | 1.3.6.1.4.1.35265.1.49.43.3.1.14 | `Get {}` | Number of unanswered calls with SIP codes that are not included in other counters. |
| countStatTransportRedirectCalls<CODE><br>where CODE — one of values:<br>300, 301, 302, 305, 308 | 1.3.6.1.4.1.35265.1.49.43.3.1.300<br>...<br>1.3.6.1.4.1.35265.1.49.43.3.1.308 | `Get {}` | Individual counters by codes — number of forwarded calls (completed by SIP codes 3xx) |
| countStatTransportUnansw<CODE><br>where CODE — one of values:<br>400, 401, 402, 403, 404, 405, 406, 407, 408, 410, 413, 414, 415, 416, 420, 421, 422, 423, 480, 481, 482, 483, 484, 485, 486, | 1.3.6.1.4.1.35265.1.49.43.3.1.400<br>...<br>1.3.6.1.4.1.35265.1.49.43.3.1.606 | `Get {}` | Individual counters by codes — number of forwarded calls (completed by SIP codes 4xx-6xx) |

| Name | OID | Requests | Description |
|---|---|---|---|
| 487, 488, 489, 490, 491, 493, 500, 501, 502, 503, 504, 505, 513, 580, 600, 603, 604, 606 | | | |
| tableOfCallPerSecStatTransport | 1.3.6.1.4.1.35265.1.49.43.4 | Get {} | Table with all instant SIP Transport counters |
| perSecStatTransportIndex | 1.3.6.1.4.1.35265.1.49.43.4.1.2 | Get {} | SIP Transport indexes |
| perSecStatTransportName | 1.3.6.1.4.1.35265.1.49.43.4.1.3 | Get {} | SIP Transport names |
| perSecStatTransportElapsedTime | 1.3.6.1.4.1.35265.1.49.43.4.1.4 | Get {} | Total time of active calls |
| perSecStatTransportIncCalls | 1.3.6.1.4.1.35265.1.49.43.4.1.5 | Get {} | Number of incoming calls |
| perSecStatTransportOutCallLegs | 1.3.6.1.4.1.35265.1.49.43.4.1.6 | Get {} | Number of outgoing calls |
| perSecStatTransportMsgRcv | 1.3.6.1.4.1.35265.1.49.43.4.1.7 | Get {} | Number of incoming SIP messages |
| perSecStatTransportMsgSend | 1.3.6.1.4.1.35265.1.49.43.4.1.8 | Get {} | Number of outgoing SIP messages |
| perSecStatTransportAnswSuccessCalls | 1.3.6.1.4.1.35265.1.49.43.4.1.9 | Get {} | Number of successfully received calls |
| perSecStatTransportAnswFinalErrCalls | 1.3.6.1.4.1.35265.1.49.43.4.1.10 | Get {} | Number of rejected calls |
| perSecStatTransportUnanswOther4xx | 1.3.6.1.4.1.35265.1.49.43.4.1.11 | Get {} | Number of unanswered calls with SIP codes 4xx |
| perSecStatTransportUnanswOther5xx | 1.3.6.1.4.1.35265.1.49.43.4.1.12 | Get {} | Number of unanswered calls with SIP codes 5xx |
| perSecStatTransportUnanswOther6xx | 1.3.6.1.4.1.35265.1.49.43.4.1.13 | Get {} | Number of unanswered calls with SIP codes 6xx |
| perSecStatTransportUnanswOtherUndef | 1.3.6.1.4.1.35265.1.49.43.4.1.14 | Get {} | Number of unanswered calls with SIP codes that are not included in other counters. |
| perSecStatTransportRedirectCalls<CODE><br>where CODE — one of values:<br>300, 301, 302, 305, 308 | 1.3.6.1.4.1.35265.1.49.43.4.1.300<br>...<br>1.3.6.1.4.1.35265.1.49.43.4.1.308 | Get {} | Individual counters by codes — number of forwarded calls (completed by SIP codes 3xx) |
| perSecStatTransportUnansw<CODE><br>where CODE — one of values:<br>400, 401, 402, 403, 404, 405, 406, 407, 408, 410, 413, 414, 415, 416, 420, 421, 422, 423, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 493, 500, 501, 502, 503, 504, 505, 513, 580, 600, 603, 604, 606 | 1.3.6.1.4.1.35265.1.49.43.4.1.400<br>...<br>1.3.6.1.4.1.35265.1.49.43.4.1.606 | Get {} | Individual counters by codes — number of forwarded calls (completed by SIP codes 4xx-6xx) |

| Name | OID | Requests | Description |
|---|---|---|---|
| tableOfCallCountStatDest | 1.3.6.1.4.1.35265.1.49.43.5 | Get {} | Table with all cumulative SIP Destination counters |
| countStatDestIndex | 1.3.6.1.4.1.35265.1.49.43.5.1.2 | Get {} | SIP Destination indexes |
| countStatDestName | 1.3.6.1.4.1.35265.1.49.43.5.1.3 | Get {} | SIP Destination names |
| countStatDestElapsedTime | 1.3.6.1.4.1.35265.1.49.43.5.1.4 | Get {} | Total time of active calls |
| countStatDestIncCalls | 1.3.6.1.4.1.35265.1.49.43.5.1.5 | Get {} | Number of incoming calls |
| countStatDestOutCallLegs | 1.3.6.1.4.1.35265.1.49.43.5.1.6 | Get {} | Number of outgoing calls |
| countStatDestMsgRcv | 1.3.6.1.4.1.35265.1.49.43.5.1.7 | Get {} | Number of incoming SIP messages |
| countStatDestMsgSend | 1.3.6.1.4.1.35265.1.49.43.5.1.8 | Get {} | Number of outgoing SIP messages |
| countStatDestAnswSuccessCalls | 1.3.6.1.4.1.35265.1.49.43.5.1.9 | Get {} | Number of successfully received calls |
| countStatDestAnswFinalErrCalls | 1.3.6.1.4.1.35265.1.49.43.5.1.10 | Get {} | Number of rejected calls |
| countStatDestUnanswOther4xx | 1.3.6.1.4.1.35265.1.49.43.5.1.11 | Get {} | Number of unanswered calls with SIP codes 4xx |
| countStatDestUnanswOther5xx | 1.3.6.1.4.1.35265.1.49.43.5.1.12 | Get {} | Number of unanswered calls with SIP codes 5xx |
| countStatDestUnanswOther6xx | 1.3.6.1.4.1.35265.1.49.43.5.1.13 | Get {} | Number of unanswered calls with SIP codes 6xx |
| countStatDestUnanswOtherUndef | 1.3.6.1.4.1.35265.1.49.43.5.1.14 | Get {} | Number of unanswered calls with SIP codes that are not included in other counters. |
| countStatDestRedirectCalls<CODE><br>where CODE — one of values:<br>300, 301, 302, 305, 308 | 1.3.6.1.4.1.35265.1.49.43.5.1.300<br>...<br>1.3.6.1.4.1.35265.1.49.43.5.1.308 | Get {} | Individual counters by codes — number of forwarded calls (completed by SIP codes 3xx) |
| countStatDestUnansw<CODE><br>where CODE — one of values:<br>400, 401, 402, 403, 404, 405, 406, 407, 408, 410, 413, 414, 415, 416, 420, 421, 422, 423, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 493, 500, 501, 502, 503, 504, 505, 513, 580, 600, 603, 604, 606 | 1.3.6.1.4.1.35265.1.49.43.5.1.400<br>...<br>1.3.6.1.4.1.35265.1.49.43.5.1.606 | Get {} | Individual counters by codes — number of forwarded calls (completed by SIP codes 4xx-6xx) |
| tableOfCallPerSecStatDest | 1.3.6.1.4.1.35265.1.49.43.6 | Get {} | Table with all instant SIP Destination counters |
| perSecStatDestIndex | 1.3.6.1.4.1.35265.1.49.43.6.1.2 | Get {} | SIP Destination indexes |
| perSecStatDestName | 1.3.6.1.4.1.35265.1.49.43.6.1.3 | Get {} | SIP Destination names |
| perSecStatDestElapsedTime | 1.3.6.1.4.1.35265.1.49.43.6.1.4 | Get {} | Total time of active calls |
| perSecStatDestIncCalls | 1.3.6.1.4.1.35265.1.49.43.6.1.5 | Get {} | Number of incoming calls |
| perSecStatDestOutCallLegs | 1.3.6.1.4.1.35265.1.49.43.6.1.6 | Get {} | Number of outgoing calls |

| Name | OID | Requests | Description |
|---|---|---|---|
| perSecStatDestMsgRcv | 1.3.6.1.4.1.35265.1.49.43.6.1.7 | `Get {}` | Number of incoming SIP messages |
| perSecStatDestMsgSend | 1.3.6.1.4.1.35265.1.49.43.6.1.8 | `Get {}` | Number of outgoing SIP messages |
| perSecStatDestAnswSuccessCalls | 1.3.6.1.4.1.35265.1.49.43.6.1.9 | `Get {}` | Number of successfully received calls |
| perSecStatDestAnswFinalErrCalls | 1.3.6.1.4.1.35265.1.49.43.6.1.10 | `Get {}` | Number of rejected calls |
| perSecStatDestUnanswOther4xx | 1.3.6.1.4.1.35265.1.49.43.6.1.11 | `Get {}` | Number of unanswered calls with SIP codes 4xx |
| perSecStatDestUnanswOther5xx | 1.3.6.1.4.1.35265.1.49.43.6.1.12 | `Get {}` | Number of unanswered calls with SIP codes 5xx |
| perSecStatDestUnanswOther6xx | 1.3.6.1.4.1.35265.1.49.43.6.1.13 | `Get {}` | Number of unanswered calls with SIP codes 6xx |
| perSecStatDestUnanswOtherUndef | 1.3.6.1.4.1.35265.1.49.43.6.1.14 | `Get {}` | Number of unanswered calls with SIP codes that are not included in other counters. |
| perSecStatDestRedirectCalls<CODE><br>where CODE — one of values:<br>300, 301, 302, 305, 308 | 1.3.6.1.4.1.35265.1.49.43.6.1.300<br>...<br>1.3.6.1.4.1.35265.1.49.43.6.1.308 | `Get {}` | Individual counters by codes — number of forwarded calls (completed by SIP codes 3xx) |
| perSecStatDestUnansw<CODE><br>where CODE — one of values:<br>400, 401, 402, 403, 404, 405, 406, 407, 408, 410, 413, 414, 415, 416, 420, 421, 422, 423, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 493, 500, 501, 502, 503, 504, 505, 513, 580, 600, 603, 604, 606 | 1.3.6.1.4.1.35265.1.49.43.6.1.400<br>...<br>1.3.6.1.4.1.35265.1.49.43.6.1.606 | `Get {}` | Individual counters by codes — number of forwarded calls (completed by SIP codes 4xx-6xx) |

**Outdated OIDs**

Some OID have been changed and in future releases old branches may be removed or replaced by new assignments. It is recommended to reconfigure monitoring systems and scripts to use the new OIDs.

Table D.6 — Outdated OID

| Name | OID | Requests | Description |
|---|---|---|---|
| sbcCpuLoad | 1.3.6.1.4.1.35265.1.49.17 | `Get {}` | Changed on smgCpuLoadTable (1.3.6.1.4.1.35265.1.49.37) |
| sbcTopCpuUsr | 1.3.6.1.4.1.35265.1.49.17.1.x | `Get {}.x` | Changed on cpuUsr (1.3.6.1.4.1.35265.1.49.37.1.2.x) |
| sbcTopCpuSys | 1.3.6.1.4.1.35265.1.49.17.2.x | `Get {}.x` | Changed on cpuSys (1.3.6.1.4.1.35265.1.49.37.1.3.x) |
| sbcTopCpuNic | 1.3.6.1.4.1.35265.1.49.17.3.x | `Get {}.x` | Changed on cpuNic (1.3.6.1.4.1.35265.1.49.37.1.4.x) |
| sbcTopCpuIdle | 1.3.6.1.4.1.35265.1.49.17.4.x | `Get {}.x` | Changed on cpuIdle (1.3.6.1.4.1.35265.1.49.37.1.5.x) |
| sbcTopCpuIo | 1.3.6.1.4.1.35265.1.49.17.5.x | `Get {}.x` | Changed on cpuIo (1.3.6.1.4.1.35265.1.49.37.1.6.x) |
| sbcTopCpuIrq | 1.3.6.1.4.1.35265.1.49.17.6.x | `Get {}.x` | Changed on cpuIrq (1.3.6.1.4.1.35265.1.49.37.1.7.x) |
| sbcTopCpuSirq | 1.3.6.1.4.1.35265.1.49.17.7.x | `Get {}.x` | Changed on cpuSirq (1.3.6.1.4.1.35265.1.49.37.1.8.x) |
| sbcTopCpuUsage | 1.3.6.1.4.1.35265.1.49.17.8.x | `Get {}.x` | Changed on cpuUsage (1.3.6.1.4.1.35265.1.49.37.1.9.x) |

**Support for OID MIB-2 (1.3.6.1.2.1)**

SMG supports the following MIB-2 branches:

- system (1.3.6.1.2.1.1) — general information on the system;
- interfaces (1.3.6.1.2.1.2) — information on network interfaces;
- snmp (1.3.6.1.2.1.11) — information on SNMP operation.

# APPENDIX E. SBC RESOURCE RESTRICTION

| Parameter | SBC-3000 | SBC-2000 | SBC-1000 | Note |
|---|---|---|---|---|
| LACP groups | 4 | 4 | 5 | |
| 802.1q table entries | NA | NA | 1024 | |
| Static routes in routing table (switch) | 255 | 255 | 255 | |
| Network interfaces | 40 | 40 | 40 | For SBC-2000 and SBC-3000 can be expanded to 500 with a 500VNI license |
| SIP Transports | 256 | 256 | 256 | For SBC-2000 and SBC-3000 can be expanded to 500 with a 500VNI license |
| sip destination | 256 | 256 | 256 | For SBC-2000 and SBC-3000 can be expanded to 500 with a 500VNI license |
| SIP Users | 256 | 256 | 256 | For SBC-2000 and SBC-3000 can be expanded to 500 with a 500VNI license |
| SBC Trunk | 256 | 256 | 256 | For SBC-2000 and SBC-3000 can be expanded to 500 with a 500VNI license |
| Rule set | 1000 | 1000 | 512 | |
| Rule for each Rule set | 1500 | 1500 | 1000 | There is no limit per profile, only a general limit |
| Rule set rules per device | 1500 | 1500 | 1000 | |
| Ports for RTP | range for starting port:<br>10000-65535<br>number of ports: 1-32000 | range for starting port:<br>10000-65535<br>number of ports: 1-32000 | range for starting por<br>10000-65535<br>number of ports: 1-32000 | |
| SNMP trap | 16 | 16 | 16 | |
| Client addresses for VPN/PPTP server | 5 | 5 | 5 | SBC is a client — VPN/pptp client |
| Client addresses for L2TP server | - | - | - | SBC cannot act as an L2TP client, only as a server |
| VPN/PPTP/L2TP users | 255 | 255 | 255 | |
| WEB interface users (tab | 10 | 10 | 10 | |

| | | | | |
|---|---|---|---|---|
| Security/Management) | | | | |
| Entries in Fail2ban whitelist | ND | ND | ND | |
| Entries in Fail2ban blacklist | 16384 | 16384 | 8192 | |
| Entries in Fail2ban blocked list | 16384 | 16384 | 8192 | |
| Entries in log of blocked addresses | 10000 | 10000 | 10000 | |
| Firewall profiles | 32 | 32 | 32 | |
| Rules for incoming/outgoing/transit traffic branches, in the profile and everything for the device | 1000 | 1000 | 1000 | |
| Entries in the list of allowed IP addresses (access to the control from certain addresses) | 255 | 255 | 255 | |
| RADIUS profiles | 32 | 32 | 32 | |

NA — not applicable;

ND — not defined.

## TECHNICAL SUPPORT

Contact ELTEX Service Centre to receive technical support regarding our products:

Feedback form on the site: **http://eltex-co.com/support/**
Servicedesk: **https://servicedesk.eltex-co.com**

Visit ELTEX official website to get the relevant technical documentation and software, send us an online request or consult a Service Centre Specialist.

Official website: **http://eltex-co.com/**
Download center: **http://eltex-co.com/support/downloads**