Пограничные контроллеры сессий

SBC-1000, SBC-2000, SBC-3000

Руководство по эксплуатации, версия ПО 1.10.3 (15.09.2021)

Версия ПО: 1.10.3		
Версия документа	Дата выпуска	Содержание изменений
Версия 1.13	15.09.2021	Обновлена документация
Версия 1.12	30.03.2021	Изменено: – прекращена поддержка резерва на SBC-1000. Добавлено: – работа в режиме облегчённого резерва по схеме 1+1 для SBC-3000; – опция «Использовать DIGEST User-name в запросах авторизации».
Версия 1.11	12.11.2020	Изменено: – переупорядочено дерево меню по функциональному признаку; – лимиты защитного таймаута для вызовов без media. Добавлено: – опция автоматического ответа на OPTIONS; – опция формирования логов по запросу; – поддержка ограничения CPS на SIP-Destination; – опция «Передавать символ '#' без кодирования»; – опция «Передавать домен из заголовков FROM и TO»; – опция «Не отправлять заблокированные адреса в черный список»; – возможность задавать больше SIP-транспортов, SIP-Destination, SIP-Users, SBC Trunk, Rules в конфигурации (при наличии лицензии); – авария о превышении максимального количества одновременных запросов INVITE, SUBSCRIBE, OTHER; – поддержка передачи заголовков RPI и PAI для SIP-Users.
Версия 1.10	10.07.2020	Добавлено: – описание нового устройства SBC-3000.
Версия 1.9	23.04.2020	Синхронизация с версией ПО 1.9.4
Версия 1.8	04.10.2019	Добавлено: – доработан механизм согласования медии для абонентов за NAT; – обновлены базы GeoIP; – работа динамического брэндмауэра с telnet; – игнорирование порта по-умолчанию для устройств, которые регистрируют контакт без указания порта, но совершают вызов с указанием его.
Версия 1.7	29.10.2018	Обновлена документация
Версия 1.6	08.09.2017	Изменено: – переименован раздел "fail2ban" в "динамический брандмауэр"; – переименован раздел "профили firewall" в "статический брандмауэр"; – разделены правила блокировок в динамическом брандмауэре для различных сервисов; – переименован раздел "MTR" в "TRACEROUTE". Добавлено: – манипулирование SIP заголовками; – управление счётчиками статистик вызовов; – опция контроля источника RTP; – поддержка 3000 одновременных вызовов на SBC2000; – обнаружение атаки RTP flood; – назначение сетевых маршрутов на интерфейс VPN-клиента; – сбор статистики вызовов по SNMP.
Версия 1.5	08.06.2017	Изменено: – базовый SNMP OID изменён на 1.3.6.1.4.1.35265.1.49. Добавлено: – защита от DoS-атак — ICMP flood, port scan, SIP flood; – новый тип правила firewall — GeoIP; – новый тип правила firewall — String; – возможность фильтрации по User-Agent; – ограничение по времени в правилах rule set; – конфигурирование SBC через CLI; – групповая очистка правил fail2ban;

		– число VLAN-интерфейсов на SBC-2000 увеличено до 500 (при наличии лицензии); – установка минимального времени регистрации на SIP Users; – опция игнорирования порта-источника при входящих вызовах через SIP Destination; – актуальные для текущей версии ПО SNMP MIB-файлы можно скачать прямо с устройства; – счётчики статистики по вызовам; – расширено количество отображаемой информации о зарегистрированных абонентах.
Версия 1.4	27.02.2017	Добавлено: – работа в режиме облегчённого резерва по схеме 1+1.
Версия 1.3	20.06.2016	Изменено: – разнесены транковые и абонентские направления; – транки могут объединять различные направления для целей резервирования/балансировки нагрузки; – расширен функционал fail2ban. Добавлено: – мониторинг активных сессий; – адаптации для ZTE Softswitch и MTA M-200; – обработка переадресаций в SIP-ответах 302; – новые более гибкие правила коммутации вызовов; – возможность задавать больше SIP-транспортов и направлений в конфигурации; – опционирование формата заголовков SIP.
Версия 1.2	21.01.2016	Добавлено: – авария о заполнении внешних накопителей; – различные режимы создания файлов CDR; – использование директорий для файлов CDR; – единый диапазон RTP-портов.
Версия 1.1	12.08.2015	Добавлено: – защитный таймаут для отбоя вызовов без проключенных медиапотоков; – мониторинг количества вызовов (на графике максимальное, текущее и минимальное значения); – выбор сетевого интерфейса, для которого выделяется медиа ресурс; – резервирование SIP-направления; – балансировка нагрузки; – контроль доступности взаимодействующего SIP-сервера; – регистрация по SIP-транку; – журнал заблокированных адресов.
Версия 1.0	11.11.14	Первая публикация

ЦЕЛЕВАЯ АУДИТОРИЯ

Данное руководство по эксплуатации предназначено для технического персонала, выполняющего настройку и мониторинг устройства посредством Web-конфигуратора, а также процедуры по установке и обслуживанию устройства. Квалификация технического персонала предполагает знание основ работы стеков протоколов TCP/IP, UDP/IP и принципов построения Ethernet-сетей.

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ....7
2 ОПИСАНИЕ ИЗДЕЛИЯ....7
2.1 Назначение....7
2.2 Типовые схемы применения....9
2.2.1 Межоператорское взаимодействие....9
2.2.2 Взаимодействие между оператором и корпоративным клиентом....9
2.2.3 Взаимодействие между оператором и частным пользователем....10
2.3 Основные технические параметры....10
2.4 Конструктивное исполнение....12
2.4.1 SBC-1000....12
2.4.2 SBC-2000....13
2.4.3 SBC-3000....14
2.5 Световая индикация....17
2.5.1 Световая индикация устройства в рабочем состоянии....17
2.5.2 Световая индикация интерфейсов Ethernet 1000/100....19
2.5.3 Световая индикация при загрузке и сбросе к заводским настройкам....19
2.5.4 Световая индикация аварий....20
2.6 Использование функциональной кнопки «F»....21
2.7 Сохранение заводской конфигурации....21
2.8 Восстановление пароля....22
2.8.1 Восстановление пароля CLI....22
2.8.2 Восстановление пароля Web....23
2.9 Комплект поставки....24
2.10 Инструкции по технике безопасности....24
2.10.1 Общие указания....24
2.10.2 Требования электробезопасности....24
2.10.3 Меры безопасности при наличии статического электричества....25
2.10.4 Требования к электропитанию....25
2.11 Установка SBC....26
2.11.1 Порядок включения....26
2.11.2 Крепление кронштейнов....27
2.11.3 Установка устройства в стойку....27
2.11.4 Установка модулей питания....28
2.11.5 Вскрытие корпуса....29
2.11.6 Установка блоков вентиляции....32
2.11.7 Установка SSD-накопителей для SBC-1000....33
2.11.8 Установка SATA-дисков для SBC-2000 и SBC-3000....34
2.11.9 Замена батарейки часов реального времени....35
3 ОБЩИЕ РЕКОМЕНДАЦИИ ПРИ РАБОТЕ С УСТРОЙСТВОМ....38
4 КОНФИГУРИРОВАНИЕ УСТРОЙСТВА....40
4.1 Настройка SBC через Web-конфигуратор....40
4.1.1 Системные параметры....43
4.1.2 Мониторинг....47
4.1.3 Конфигурация SBC....58
4.1.4 Конфигурация интерфейсов. Сетевая подсистема....78
4.1.5 Сетевые сервисы....83
4.1.6 Коммутатор....88
4.1.7 Сетевые утилиты....95
4.1.8 Безопасность....97
4.1.9 Настройка RADIUS....108
4.1.10 Трассировки....110
4.1.11 Работа с объектами и меню «Объекты»....114

4.1.12 Сохранение конфигурации и меню «Сервис» ... 114
4.1.13 Настройка даты и времени ... 115
4.1.14 Обновление ПО через web-интерфейс ... 115
4.1.15 Лицензии ... 115
4.1.16 Меню «Помощь» ... 116
4.1.17 Просмотр заводских параметров и информации о системе ... 116
4.1.18 Выход из конфигуратора ... 116
4.2 Настройка SBC через Telnet, SSH или RS-232 ... 117
4.2.1 Перечень команд CLI ... 117
4.2.2 Смена пароля для доступа к устройству ... 118
4.2.3 Режим просмотра активных сессий ... 119
4.2.4 Просмотр активных регистраций ... 119
4.2.5 Управление регистрациями ... 119
4.2.6 Работа со статистикой SIP ... 119
4.2.7 Режим конфигурирования ... 120
4.3 Настройка коммутатора SBC-2000/SBC-3000 ... 159
4.3.1 Структура коммутатора ... 159
4.3.2 Команды управления интерфейсами коммутатора SBC-2000/SBC-3000 ... 161
4.3.3 Команды настройки групп агрегации ... 167
4.3.4 Команды управления интерфейсами VLAN ... 169
4.3.5 Команды настройки STP/RSTP ... 169
4.3.6 Команды настройки MAC-таблицы ... 172
4.3.7 Команды для настройки зеркалирования портов ... 173
4.3.8 Команды для настройки функции SELECTIVE Q-IN-Q ... 176
4.3.9 Настройка протокола DUAL HOMING ... 179
4.3.10 Настройка протокола LLDP ... 181
4.3.11 Настройка QOS ... 187
4.3.12 Команды работы с конфигурацией ... 190
4.3.13 Команды применения и подтверждения конфигурации ... 191
4.3.14 Прочие команды ... 191
ПРИЛОЖЕНИЕ А. РЕЗЕРВНОЕ ОБНОВЛЕНИЕ ВСТРОЕННОГО ПО УСТРОЙСТВА ... 193
ПРИЛОЖЕНИЕ Б. ПРИМЕРЫ НАСТРОЙКИ SBC ... 196
ПРИЛОЖЕНИЕ В. ОБЕСПЕЧЕНИЕ ФУНКЦИИ РЕЗЕРВИРОВАНИЯ SBC ... 206
ПРИЛОЖЕНИЕ Г. УПРАВЛЕНИЕ И МОНИТОРИНГ ПО ПРОТОКОЛУ SNMP ... 212
ПРИЛОЖЕНИЕ Д. ОГРАНИЧЕНИЕ РЕСУРСОВ SBC ... 225
ТЕХНИЧЕСКАЯ ПОДДЕРЖКА ... 228

1 ВВЕДЕНИЕ

Пограничный контроллер сессий SBC (Session Border Controller) предназначен для решения задач сопряжения разнородных VoIP сетей, обеспечивая совместную работу терминалов с различными протоколами сигнализации и наборами используемых кодеков. Кроме того, за счет функциональности Firewall, NAT и проксирования сигнального и медиа трафика он защищает корпоративную сеть от атак и скрывает ее внутреннюю структуру. SBC всегда устанавливается на границе корпоративной или операторской VoIP сети и выполняет те функции, которые не целесообразно возлагать на устройства оператора (например, гибкий коммутатор Softswitch).

Основные функции SBC

- защита сети и других устройств от внешних атак (например, DoS-атак);
- выполняет функции межсетевого экрана Firewall;
- позволяет скрыть топологию сети оператора;
- позволяет согласовать различные протоколы сигнализаций и кодеки;
- позволяет предоставить услуги QoS и приоритезацию потоков;
- позволяет взаимодействовать с устройствами, подключенными через NAT (Network Address Translation);
- сбор статистики вызовов, обслуженных через SBC.

2 ОПИСАНИЕ ИЗДЕЛИЯ

2.1 Назначение

Eltex SBC — компонент программно-аппаратного комплекса ECSS-10, участвующий в процессе обслуживания вызова в качестве пограничного контроллера сессий. Устройство обеспечивает нормализацию реализаций сигнального протокола, установленный SLA уровень качества, защиту сети оператора от несанкционированного доступа и различных атак, сбор статистики.

Основные характеристики SBC:

- количество одновременных сессий:
  - для SBC-3000: 2000;
  - для SBC-2000: 2000;
  - для SBC-1000: 500.
- количество зарегистрированных абонентов:
  - для SBC-3000: 16000;
  - для SBC-2000: 16000;
  - для SBC-1000: 4000.
- количество вызовов/секунду (CPS):
  - для SBC-3000: 100;
  - для SBC-2000: 100;
  - для SBC-1000: 30.
- количество Ethernet-портов:
  - для SBC-3000:
    - 4 порта 10/100/1000BASE-T;
    - 2 комбо-порта 1000-BASE-X (SFP).
  - для SBC-2000:
    - 4 порта 10/100/1000BASE-T;
    - 2 комбо-порта 1000-BASE-X (SFP).
  - для SBC-1000:
    - 3 порта 10/100/1000BASE-T;
    - 2 порта 1000-BASE-X (SFP).

- поддержка статического адреса и DHCP;
- протоколы IP-телефонии SIP, SIP-T, SIP-I;
- поддержка NTP;
- поддержка DNS;
- поддержка SNMP;
- ограничение полосы и QoS;
- ToS и CoS для RTP и сигнализации[1];
- VLAN для RTP, сигнализации и управления;
- аварийное логирование;
- поддержка RADIUS;
- запись биллинговой информации;
- аппаратное резервирование по схеме облегчённого резерва 1+1[2]:
    - время переключения на резерв при отключении внешнего линка основного устройства 2-4 секунды;
    - время переключения на резерв при полном отключении основного устройства — 4-5 секунд;
- обновление ПО: через Web-интерфейс, CLI (Telnet, SSH, консоль (RS-232));
- конфигурирование и настройка (в том числе удаленно):
    - Web-интерфейс;
    - CLI[3] (Telnet, консоль (RS-232));
- удаленный мониторинг:
    - Web-интерфейс;
    - CLI;
    - SNMP.

Функционал SIP/SIP-T/SIP-I:

- 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).

Передача факса

- T.38;
- G.711

[1] В текущей версии ПО не поддерживается
[2] Функционал не поддержан для SBC-1000
[3] В текущей версии ПО поддерживается частично

2.2 Типовые схемы применения

В данном руководстве предлагается несколько схем построения сети с использованием SBC.

2.2.1 *Межоператорское взаимодействие*

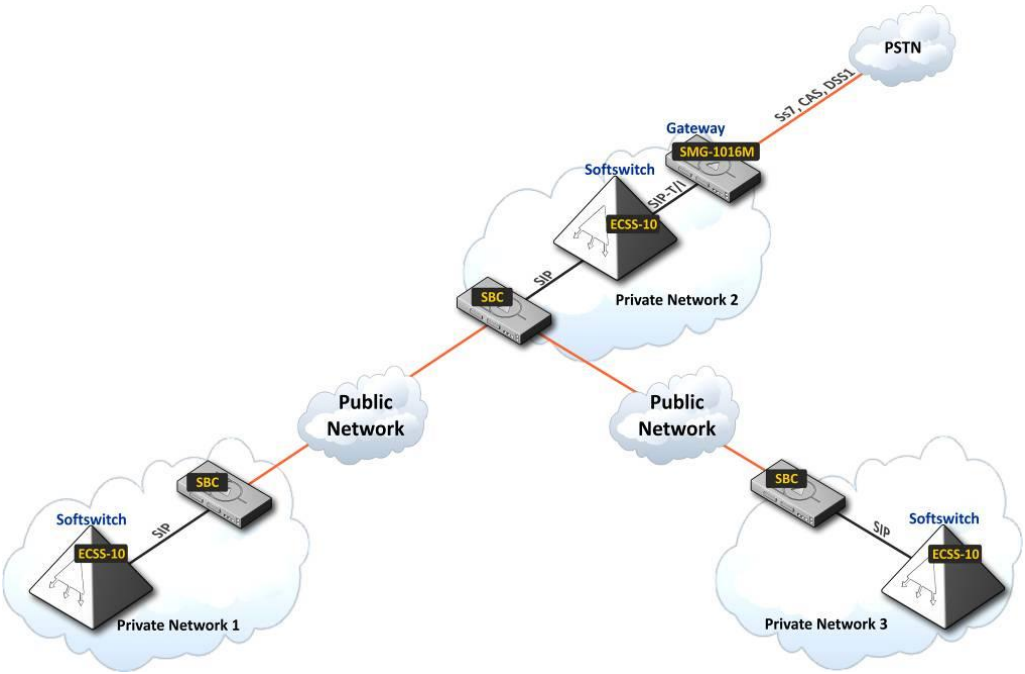


Рисунок 1 — Схема применения «Межоператорское взаимодействие»

2.2.2 *Взаимодействие между оператором и корпоративным клиентом*

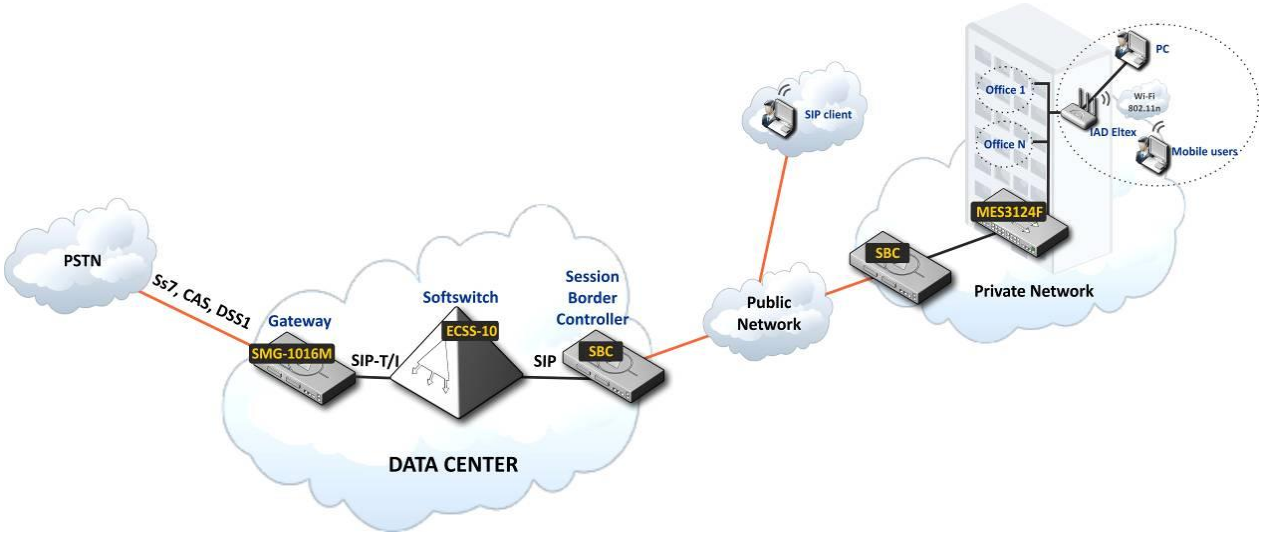


Рисунок 2 — Схема применения «Оператор – корпоративный клиент»

2.2.3 *Взаимодействие между оператором и частным пользователем*

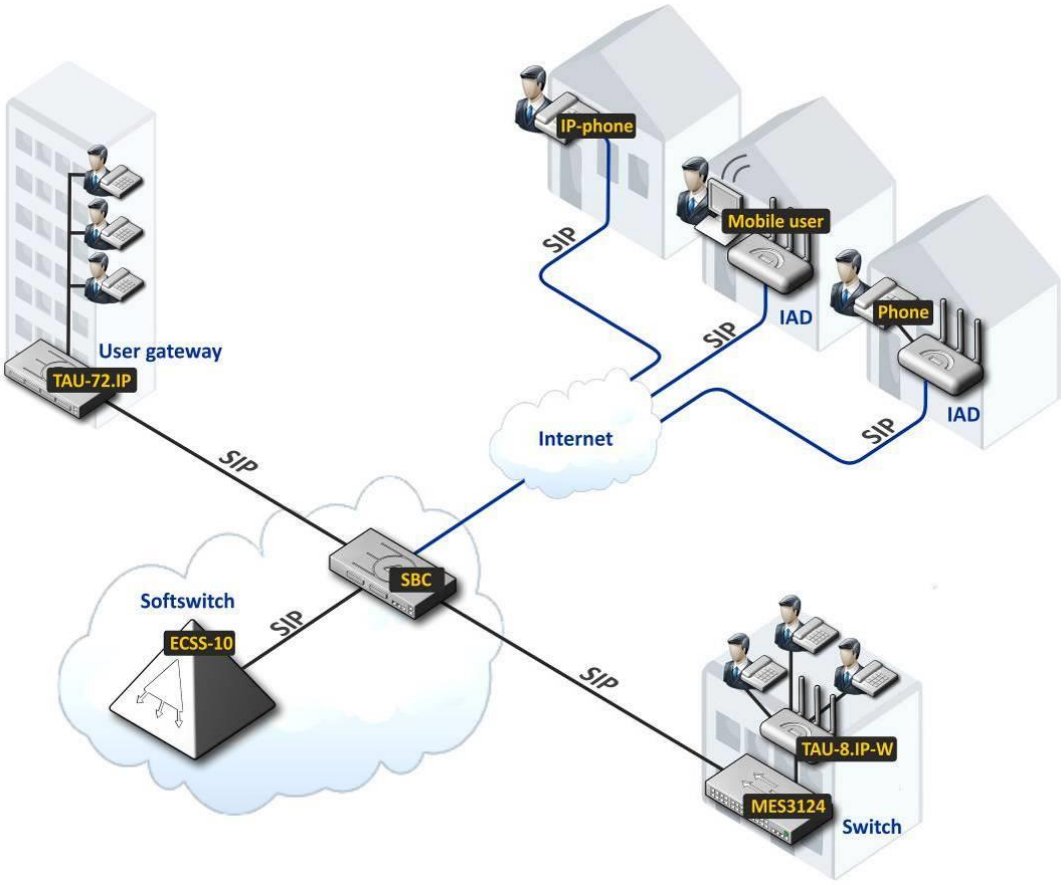


Рисунок 3 — Схема применения «Оператор – частный клиент»

2.3 Основные технические параметры

Основные технические параметры приведены в таблице 1.

Таблица 1 — Основные технические параметры

Протоколы VoIP

Поддерживаемые протоколы	SIP-T/SIP-I SIP T.38

Поддерживаемые кодеки

Аудиокодеки	G.711 a-law (в тексте G711A) G.711 µ-law (в тексте G.711U) G.729 A/B G.723.1 (6.3 Kbps, 5.3 Kbps) G.726 (32 Kbps)
Видеокодеки	H.263 H.263-1998 H.264

Параметры электрического интерфейса Ethernet

Количество интерфейсов	SBC-1000	SBC-2000	SBC-3000
	3	4	4
Электрический разъем	RJ-45		
Скорость передачи, Мбит/с	Автоопределение, 10/100/1000Мбит/с, дуплекс		
Поддержка стандартов	10/100/1000BASE-T		

Параметры оптического интерфейса Ethernet

Количество интерфейсов	2 combo-порта
Оптический разъем	Mini-Gbic (SFP): 1) дуплексные, двухволоконные с длинной волны 1310 нм (Single-Mode), 1000BASE-LX (коннектор LC), дальность — до 10 км, напряжение питания — 3,3 В 2) дуплексные, одноволоконные с длинами волн на прием/передачу 1310/1550 нм, 1000BASE-LX (коннектор SC), дальность — до 10 км, напряжение питания — 3,3 В
Скорость передачи, Мбит/с	1000Мбит/с, дуплекс
Поддержка стандартов	1000BASE-X

Параметры консоли

Последовательный порт RS-232	
Скорость передачи данных, бит/сек	115200
Электрические параметры сигналов	По рекомендации МСЭ-Т V.28

Прочие интерфейсы

Интерфейс	Количество
USB	1 — для SBC-1000/2000; 2 — для SBC-3000
e-SATA	2

Общие параметры

Рабочий диапазон температур		от 0 до +40°С		
Относительная влажность		до 80%		
Варианты питания		- один источник питания постоянного или переменного тока; - два источника питания постоянного или переменного тока.		
Источники питания		Сеть переменного тока	Сеть постоянного тока	
Напряжение питания		220В+-20%, 50 Гц	-48В+30-20%	
	Обозначение ИП	РМ160-220/12	РМ100-48/12	
	Мощность ИП	160Вт	100Вт	
Потребляемая мощность		не более 50Вт		
Габариты (ширина, высота, глубина)		SBC-1000	SBC-2000	SBC-3000
		430x45x260 мм	430x45x340 мм	430x45x340 мм
Конструктив		19" конструктив, типоразмер 1U		
Вес нетто	Устройство в полной комплектации	SBC-1000	SBC-2000	SBC-3000
		3,2 кг	5,3 кг	5,3 кг
	БП	0,5 кг		
	Вентпанель	0,1 кг		
	SATA-накопитель[1]	0,1 кг		

[1] Только для SBC-2000 и SBC-3000

2.4 Конструктивное исполнение

2.4.1 *SBC-1000*

Пограничный контроллер сессий SBC-1000 выполнен в металлическом корпусе с возможностью установки в 19″ каркас типоразмером 1U.

Внешний вид передней панели устройства приведен на рисунке 4.

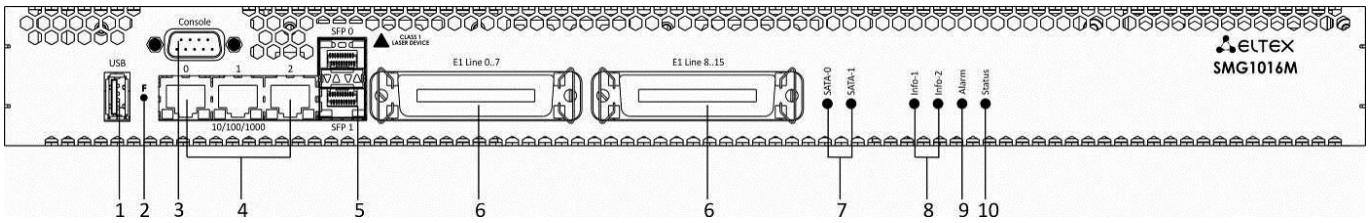


Рисунок 4 — Внешний вид передней панели SBC-1000 (на базе SMG-1016M)

На передней панели устройства расположены следующие разъемы, световые индикаторы и органы управления, Таблица 2.

Таблица 2 — Описание разъемов, индикаторов и органов управления передней панели

№	Элемент передней панели	Описание
1	***USB***	USB-порт для подключения внешнего накопителя
2	***F***	Функциональная кнопка
3	***Console***	Консольный порт RS-232 для локального управления устройством
4	***10/100/1000 0..2***	3 разъема RJ-45 интерфейсов Ethernet 10/100/1000 BASE-T
5	***SFP 0, SFP 1***	2 шасси для оптических SFP модулей 1000BASE-X Gigabit uplink интерфейса для выхода в IP-сеть
6	***E1 Line 0..7, E1 Line 8..15***	2 разъема CENC-36M для подключения потоков E1[1]
7	***SATA-0, SATA-1***	Индикаторы работы интерфейсов SATA[2]
8	***Info1, Info2***	Индикаторы работы оптических интерфейсов SFP
9	***Alarm***	Индикатор аварии устройства
10	***Status***	Индикатор работы устройства

[1] Для устройства в конфигурации SBC-1000 не используется
[2] В данной версии не используется

Внешний вид задней панели устройства приведён на рисунке ниже.

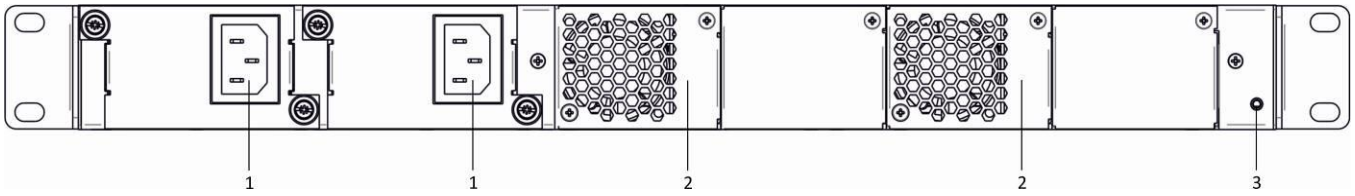


Рисунок 5 — Внешний вид задней панели SBC-1000 (на базе SMG-1016M)

В таблице ниже приведен перечень разъемов, расположенных на задней панели устройства.

Таблица 3 — Описание разъемов задней панели коммутатора

№	Элемент задней панели	Описание
1	Разъем питания	Разъем для подключения к источнику электропитания
2	Съемные вентиляторы	Съемные вентиляционные модули с возможностью горячей замены
3	Клемма заземления ⏚	Клемма для заземления устройства

2.4.2 *SBC-2000*

Пограничный контроллер сессий SBC-2000 выполнен в металлическом корпусе с возможностью установки в 19” каркас типоразмером 1U.

Внешний вид передней панели устройства приведен на рисунке 6.

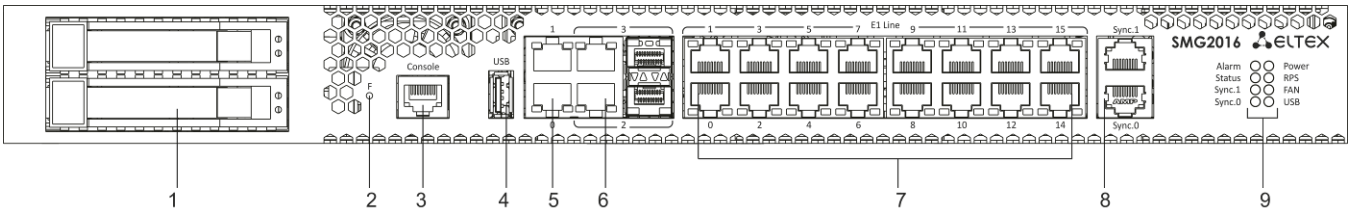


Рисунок 6 — Внешний вид передней панели SBC-2000 (на базе SMG-2016)

На передней панели устройства расположены следующие разъемы, световые индикаторы и органы управления, Таблица 4.

Таблица 4 — Описание разъемов, индикаторов и органов управления передней панели

№	Элемент передней панели	Описание
1	***Разъемы SATA-дисков***	Разъемы для установки SATA-дисков
2	***F***	Функциональная кнопка
3	***Console***	Консольный порт для локального управления устройством
4	***USB***	USB-порт для подключения внешнего накопителя
5	***0, 1***	2 разъема RJ-45 Ethernet 10/100/1000 BASE-T Gigabit uplink для выхода в IP-сеть
6	***2,3***	2 шасси для установки SFP модулей 1000 BASE-X uplink интерфейса для выхода в IP-сеть

		2 разъема RJ-45 10/100/1000 BASE-T Gigabit uplink интерфейса для выхода в IP-сеть
7	***E1 Line 0..15***	16 разъемов RJ-48 для подключения потоков E1[1]
8	***Sync.0, Sync.1***	2 разъема RJ-45 для подключения источников внешней синхронизации[1]
Индикаторы		
9	***Alarm***	Индикатор аварии устройства
	Status	Индикатор работы устройства
	Sync.1	Индикатор работы интерфейса внешней синхронизации ***Sync.1***[1]
	Sync.0	Индикатор работы интерфейса внешней синхронизации ***Sync.2***[1]
	Power	Индикатор питания устройства
	RPS	Индикатор дополнительного питания устройства
	FAN	Индикатор работы вентиляторов
	USB	Индикатор работы USB

Внешний вид задней панели устройства приведен на рисунке 7.

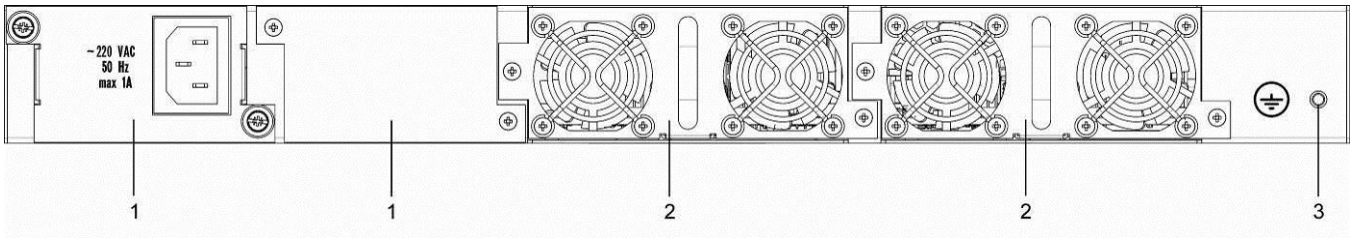


Рисунок 7 — Внешний вид задней панели SBC-2000 (на базе SMG-2016)

В таблице ниже приведен перечень разъемов, расположенных на задней панели устройства.

Таблица 5 — Описание разъемов задней панели коммутатора

№	Элемент задней панели	Описание
1	Модули питания	Модули с разъемом для подключения к источнику электропитания
2	Панели вентиляторов	Съемные вентиляционные модули с возможностью горячей замены
3	Клемма заземления ⏚	Клемма для заземления устройства

2.4.3 *SBC-3000*

Пограничный контроллер сессий SBC-3000 выполнен в металлическом корпусе с возможностью установки в 19” каркас типоразмером 1U.

[1] Для устройства в конфигурации SBC-2000 не используется

Внешний вид передней панели устройства приведен на рисунке ниже.

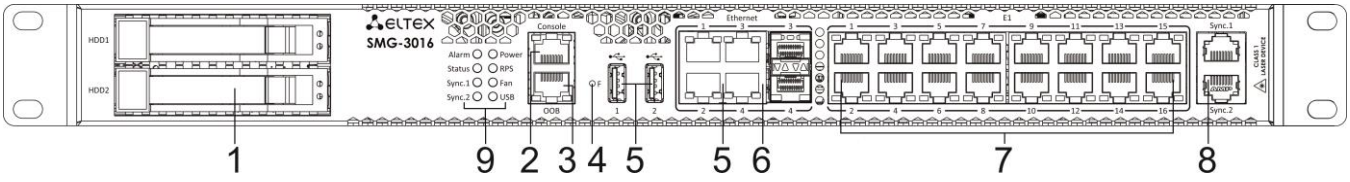


Рисунок 8 — Внешний вид передней панели SBC-3000 (на базе SMG-3016)

На передней панели устройства расположены следующие разъемы, световые индикаторы и органы управления, Таблица 6.

Таблица 6 — Описание разъемов, индикаторов и органов управления передней панели

№	Элемент передней панели	Описание
1	***Разъемы SATA-дисков***	Разъемы с салазками для установки SATA-дисков
2	***Console***	Консольный порт для локального управления устройством
3	***OOB***	Выделенный порт Ethernet для конфигурирования устройства[1]. Порт не имеет возможности коммутации с прочими портами SMG
4	***F***	Функциональная кнопка
5	***USB***	USB-порты для подключения внешних накопителей
5	***1, 2***	2 разъема RJ-45 Ethernet 10/100/1000 BASE-T Gigabit uplink для выхода в IP-сеть
6	***3, 4***	2 шасси для установки SFP модулей 1000 BASE-X uplink интерфейса для выхода в IP-сеть
		2 разъема RJ-45 10/100/1000 BASE-T Gigabit uplink интерфейса для выхода в IP-сеть
7	***E1 Line 0..15***	16 разъемов RJ-48 для подключения потоков E1[2]
8	***Sync.1, Sync.2***	2 разъема RJ-45 для подключения источников внешней синхронизации[2]
	Индикаторы	
9	***Alarm***	Индикатор аварии устройства
	Status	Индикатор работы устройства
	Sync.1	Индикатор работы интерфейса внешней синхронизации ***Sync.2***[2]
	Sync.0	Индикатор работы интерфейса внешней синхронизации ***Sync.1***[2]
	Power	Индикатор питания устройства
	RPS	Индикатор дополнительного питания устройства
	FAN	Индикатор работы вентиляторов

[1] В данной версии не поддерживается
[2] Для устройства в конфигурации SBC-3000 не используется

	USB	Индикатор работы USB

Внешний вид задней панели устройства приведен на рисунке 9.

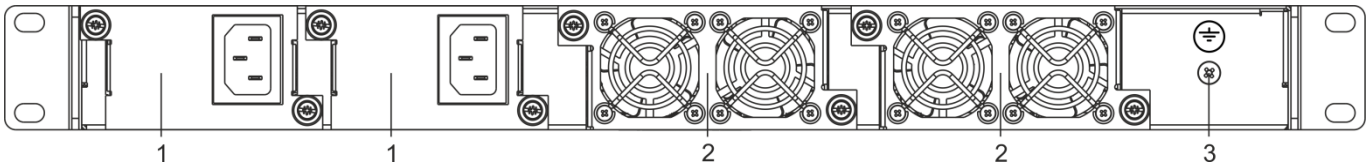


Рисунок 9 — Внешний вид задней панели SBC-3000 (на базе SMG-3016)

В таблице ниже приведен перечень разъемов, расположенных на задней панели устройства.

Таблица 7 — Описание разъемов задней панели коммутатора

№	**Элемент задней панели**	**Описание**
1	Модули питания	Модули с разъемом для подключения к источнику электропитания
2	Панели вентиляторов	Съемные вентиляционные модули с возможностью горячей замены
3	Клемма заземления	Клемма для заземления устройства

2.5 Световая индикация

Текущее состояние устройства отображается при помощи индикаторов, расположенных на передней панели.

2.5.1 *Световая индикация устройства в рабочем состоянии*

2.5.1.1 SBC-1000

Световая индикация устройства в рабочем состоянии приведена в таблице 8 — Световая индикация состояния устройства в рабочем состоянии.

Таблица 8 — Световая индикация состояния устройства в рабочем состоянии

Индикатор	Состояние индикатора	Состояние устройства
Info1	не горит	отсутствует линк SFP0
	горит зеленым светом	линк SFP0 в работе
Info2	не горит	отсутствует линк SFP1
	горит зеленым светом	линк SFP1 в работе
	горит красным светом	загрузка устройства
Alarm	мигает красным светом	критическая авария на устройстве
	горит красным светом	не критическая авария на устройстве
	горит желтым светом	нет аварий, есть некритические замечания
	горит зеленым светом	нормальная работа
Status	горит зеленым светом	нормальная работа
	не горит	нет питания устройства

2.5.1.2 SBC-2000

Световая индикация устройства в рабочем состоянии приведена в таблице 9 — Световая индикация устройства в рабочем состоянии.

Таблица 9 — Световая индикация устройства в рабочем состоянии

Индикатор	Состояние индикатора	Состояние устройства
Alarm	мигает красным светом	критическая авария на устройстве
	горит красным светом	не критическая авария на устройстве
	горит желтым светом	нет аварий, есть некритические замечания
	горит зеленым светом	нормальная работа
Status	горит зеленым светом	нормальная работа
	не горит	нет питания устройства
Sync.0, Sync.1	горит зеленым цветом	синхронизация от внешнего источника
	не горит	внешний источник синхронизации не подключен
Power	горит зеленым цветом	питание от блока питания #1
	горит оранжевым цветом	блок питания #1 установлен, питание на него нет
RPS	горит зеленым цветом	блок питания #2 установлен, на него подается питание
	горит красным цветом	блок питания #2, питание на него не подается
	не горит	блок питания #2 не установлен
FAN	горит зеленым цветом	все модули съемных вентиляторов установлены, все вентиляторы в работе
	горит оранжевым цветом	все модули съемных вентиляторов установлены, присутствуют нерабочие вентиляторы
	горит красным цветом	один или оба модуля съемных вентиляторов не установлены
USB	горит зеленым цветом	USB-flash установлена
	не горит	USB-flash не установлена

2.5.1.3 SBC-3000

Световая индикация устройства в рабочем состоянии приведена в таблице 10.

Таблица 10 — Световая индикация устройства в рабочем состоянии

Индикатор	Состояние индикатора	Состояние устройства
Alarm	Мигает красным светом	Критическая авария на устройстве
	Горит красным светом	Не критическая авария на устройстве
	Горит желтым светом	Нет аварий, есть некритические замечания
	Горит зеленым светом	Нормальная работа
Status	Горит зеленым светом	Нормальная работа
	Не горит	Нет питания устройства
Sync.1, Sync.2	Горит зеленым цветом	Синхронизация от внешнего источника
	Не горит	Внешний источник синхронизации не подключен
Power	Горит зеленым цветом	Питание от Блока питания #1
	Горит оранжевым цветом	Блок питания #1 установлен, питание на него не подается
RPS	Горит зеленым цветом	Блок питания #2 установлен, на него подается питание
	Горит красным цветом	Блок питания #2, питание на него не подается
	Не горит	Блок питания #2 не установлен
FAN	Горит зеленым цветом	Все модули съемных вентиляторов установлены, все вентиляторы в работе
	Горит оранжевым цветом	Все модули съемных вентиляторов установлены, присутствуют нерабочие вентиляторы
	Горит красным цветом	Один или оба модуля съемных вентиляторов не установлены
USB	Горит зеленым цветом	USB-flash установлена
	Не горит	USB-flash не установлена

2.5.2 *Световая индикация интерфейсов Ethernet 1000/100*

Состояние интерфейсов Ethernet отображается светодиодными индикаторами, встроенными в разъем 1000/100 и приведено в таблице ниже.

Таблица 11 — Световая индикация интерфейсов Ethernet 1000/100

Состояние устройства	**Индикатор/Состояние**	
	Желтый индикатор 1000/100	**Зеленый индикатор 1000/100**
Порт работает в режиме 1000BASE-T, нет передачи данных	горит постоянно	горит постоянно
Порт работает в режиме 1000BASE-T, есть передача данных	горит постоянно	мигает
Порт работает в режиме 10/100BASE-TX, нет передачи данных	не горит	горит постоянно
Порт работает в режиме 10/100BASE-TX, есть передача данных	не горит	мигает

2.5.3 *Световая индикация при загрузке и сбросе к заводским настройкам*

2.5.3.1 SBC-1000

Световая индикация при загрузке и сбросе к заводским настройкам приведена в таблице 12.

Таблица 12 — Световая индикация при загрузке и сбросе к заводским настройкам

№	**Индикация**				**Порядок сброса к настройкам по умолчанию (устройство включено)**
	Info1	**Info1**	**Alarm**	**Status**	
1	желтый	желтый	желтый	желтый	Нажать и удерживать кнопку «F» в течение 1 секунды до появления данной комбинации, затем отпустить кнопку. Через 3 секунды начнется перезагрузка устройства
2	зеленый	красный	желтый	красный	Начало сброса настроек к заводским. Данная комбинация светодиодов загорится в начале загрузки устройства
3	желтый	желтый	желтый	желтый	На данном этапе происходит проверка работоспособности светодиодов, желтым должны загореться все светодиоды, включая SATA-0 и SATA-1
4	не горит	не горит	зеленый	зеленый	На данном этапе происходит загрузка операционной системы шлюза. Для изменения сетевых параметров и возврата конфигурации устройства к заводским настройкам после появления комбинации нажать и удерживать кнопку «F» в течение 40-45 сек (во время удерживания кнопки кратковременно загорится комбинация 2, не обращая на нее внимания, продолжайте удерживать до появления комбинации 4)
5	желтый	желтый	желтый	желтый	При появлении комбинации отпустить кнопку «F». Через некоторое время в консоль будет выведено сообщение: <<<BOOTING IN SAFE-MODE.RESTORING DEFAULT PARAMETERS>>> Сброс к заводским настройкам завершен

Не рекомендуется удерживать нажатой кнопку «F» во время сброса устройства — это приведет к полной остановке устройства. Возобновление работы будет возможно только после сброса по питанию.

Возможен сброс к заводским настройкам на включаемом устройстве.
В этом случае пункт 1 необходимо пропустить.

2.5.3.2 SBC-2000

Световая индикация при загрузке и сбросе к заводским настройкам приведена в таблице 13.

Таблица 13 — Световая индикация при загрузке и сбросе к заводским настройкам

№	Индикация				Порядок сброса к настройкам по умолчанию (устройство включено)
	Alarm	Status	Sync.1	Sync.2	
1	желтый	желтый	желтый	желтый	Нажать и удерживать кнопку «F» в течение 1 секунды до появления данной комбинации. Через 3 секунды начнется перезагрузка устройства
2	желтый	красный	желтый	желтый	Начало сброса настроек к заводским. Данная комбинация светодиодов загорится в начале загрузки устройства
4	-	-	-	-	На данном этапе происходит загрузка операционной системы шлюза. Для изменения сетевых параметров и возврата конфигурации устройства к заводским настройкам после появления комбинации нажать и удерживать кнопку «F» в течение 40-45 сек
5	желтый	желтый	-	-	При появлении комбинации отпустить кнопку «F». Через некоторое время в консоль будет выведено сообщение: <<<BOOTING IN SAFE-MODE.RESTORING DEFAULT PARAMETERS>>> Сброс к заводским настройкам завершен

Состоянием диодов POWER, RPS, FAN, USB при сбросе можно пренебречь.
Возможен сброс к заводским настройкам на включаемом устройстве.
В этом случае пункт 1 необходимо пропустить.

2.5.3.3 SBC-3000

Световая индикация при сбросе к заводским настройкам SBC-3000 аналогична SBC-2000 (см. раздел выше).

2.5.4 *Световая индикация аварий*

В таблице 14 приведено подробное описание аварий, отображаемых в состоянии индикатора Alarm.

Индикация сохранения CDR-файлов

В случае если FTP сервер недоступен, CDR-записи сохраняются в оперативной памяти устройства, на хранение CDR-файлов выделено 30 MB. При заполнении памяти в определенных границах будет индицироваться авария.

Таблица 14 — Индикация аварий

Состояние индикатора Alarm	Уровень аварии	Описание аварии
мигает красным светом	критическая (critical)	Ошибка конфигурации
		Потеря sip-модуля
		Авария группы линий ОКС-7 (при установленном флаге *Индикация аварии* в меню *«Маршрутизация/Группы линий ОКС»*)
		Авария потока (при установленном флаге *Индикация Alarm* в меню *«Потоки E1/Физические параметры»*)
		FTP-сервер недоступен, оперативная память для хранения CDR-файлов заполнена свыше 50% (15 - 30 MB)
		Резерв — ведомый не подключен

горит красным светом	не критическая (errors)	Авария линка ОКС-7 (при установленном флаге *Индикация аварии* в меню *«Маршрутизация/Группы линий ОКС»*)
		Потеря VoIP субмодуля (MSP)
		Авария синхронизации (работа в режиме free-run)
		FTP-сервер недоступен, оперативная память для хранения CDR-файлов заполнена до 50 % (5 - 15 MB)
		Резерв — ведомый не подключен по одному из линков
горит желтым светом	предупреждения (warning)	Удаленная авария потока
		Синхронизация от менее приоритетного источника (более приоритетный недоступен)
		FTP-сервер недоступен, оперативная память для хранения CDR-файлов заполнена до 5 MB
		Резерв — на ведомом установлена другая версия ПО

2.6 Использование функциональной кнопки «F»

Функциональная кнопка «F» используется для перезагрузки устройства, восстановления заводской конфигурации, а также для восстановления пароля.

Порядок сброса к заводским настройкам на включенном устройстве приведен в таблицах 13 и 14 в разделе 2.5.3.

После восстановления заводской конфигурации к устройству можно будет обратиться по IP-адресу 192.168.1.2 (маска 255.255.255.0):

- через Telnet/SSH либо console: логин **admin**, пароль **rootpasswd**;
- через Web-интерфейс: логин **admin**, пароль **rootpasswd**;

Далее можно сохранить заводскую конфигурацию, восстановить пароль или перезагрузить устройство.

2.7 Сохранение заводской конфигурации

Для сохранения заводской конфигурации:

- произведите сброс устройства к заводским настройкам (раздел 2.5.3);
- подключитесь через telnet либо console, используя логин **admin**, пароль **rootpasswd**;
- введите команду ***sh*** (устройство выйдет из режима CLI в режим SHELL);
- введите команду ***save***;
- перезагрузите устройство командой ***reboot***.

Шлюз загрузится с заводской конфигурацией.

```
*********************************************
*        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 Восстановление пароля

2.8.1 *Восстановление пароля CLI*

Для восстановления пароля:

- произведите сброс устройства к заводским настройкам (раздел 2.5.3);
- подключитесь через Telnet, SSH либо Console;
- введите команду ***sh*** (устройство выйдет из режима cli в режим shell);
- введите команду ***restore*** (восстановится текущая конфигурация);
- введите команду ***passwd*** (устройство потребует ввести новый пароль и его подтверждение);
- введите команду ***save***;
- перезагрузите устройство командой ***reboot***.

Шлюз загрузится с текущей конфигурацией и новым паролем.

В случае перезагрузки без выполнения каких-либо действий, на устройстве восстановится текущая конфигурация без восстановления пароля. Шлюз загрузится с текущей конфигурацией и старым паролем.

```
*********************************************
*        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 *Восстановление пароля Web*

Для восстановления пароля:

- произведите сброс устройства к заводским настройкам (раздел 2.5.3);
- подключитесь через Telnet, SSH либо Console;
- введите команду ***sh*** (устройство выйдет из режима cli в режим shell);
- введите команду ***restore*** (восстановится текущая конфигурация);
- подключитесь к web-интерфейсу устройства по адресу 192.168.1.2;
- зайдите в раздел "Пользователи: Управление";
- смените пароль для пользователя admin;
- в консоли введите команду ***save***;
- перезагрузите устройство командой ***reboot***.

Сохранять конфигурацию из WEB при восстановлении пароля не рекомендуется, т.к. это может привести к потере сохранённой конфигурации шлюза. Используйте команду `save` из режима shell.

Шлюз загрузится с текущей конфигурацией и новым паролем.

В случае перезагрузки без выполнения каких-либо действий, на устройстве восстановится текущая конфигурация без восстановления пароля. Шлюз загрузится с текущей конфигурацией и старым паролем.

```
*********************************************
*        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
```

На этом этапе производится смена пароля из WEB.

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

# reboot
```

2.9 Комплект поставки

В базовый комплект поставки устройства SBC входят:

- Пограничный контроллер сессий SBC;
- Комплект крепления в 19” стойку;
- Средства для подключения к консоли:
  - для SBC-2000: адаптер консольного порта RJ45-DB9;
  - для SBC-1000: кабель соединительный DB9(F) — DB9(F);
- Кронштейн — 2шт.;
- Памятка о документации;
- Сертификат соответствия;
- Руководство по эксплуатации (поставляется на CD-диске);
- Паспорт.

При наличии в заказе также могут быть поставлены:

- Mini-Gbic (SFP).

2.10 Инструкции по технике безопасности

2.10.1 *Общие указания*

При работе с оборудованием необходимо соблюдение требований «Правил техники безопасности при эксплуатации электроустановок потребителей».

Запрещается работать с оборудованием лицам, не допущенным к работе в соответствии с требованиями техники безопасности в установленном порядке.

Эксплуатация устройства должна производиться инженерно-техническим персоналом, прошедшим специальную подготовку.

Подключать к устройству только годное к применению вспомогательное оборудование.

Устройство SBC предназначено для круглосуточной эксплуатации при следующих условиях:

- температура окружающей среды от 0 до +40 ˚С;
- относительная влажность воздуха до 80% при температуре 25 ˚С;
- атмосферное давление от 6,0х10*4 до 10,7х10*4 Па (от 450 до 800 мм рт.ст.).

Не подвергать устройство воздействию механических ударов и колебаний, а также дыма, пыли, воды, химических реагентов.

Во избежание перегрева компонентов устройства и нарушения его работы запрещается закрывать вентиляционные отверстия посторонними предметами и размещать предметы на поверхности оборудования.

2.10.2 *Требования электробезопасности*

Перед подключением устройства к источнику питания необходимо предварительно заземлить корпус оборудования, используя клемму заземления. Крепление заземляющего провода к клемме заземления должно быть надежно зафиксировано. Величина сопротивления между клеммой защитного заземления и земляной шиной не должна превышать 0,1 Ом.

Перед подключением к устройству измерительных приборов и компьютера, их необходимо

предварительно заземлить. Разность потенциалов между корпусами оборудования и измерительных приборов не должна превышать 1В.

Перед включением устройства убедиться в целостности кабелей и их надежном креплении к разъемам.

При установке или снятии кожуха необходимо убедиться, что электропитание устройства отключено.

2.10.3 *Меры безопасности при наличии статического электричества*

Во избежание поломок электростатического характера настоятельно рекомендуется:

– надеть специальный пояс, обувь или браслет для предотвращения накопления статического электричества (в случае браслета убедиться, что он плотно примыкает к коже) и заземлить шнур перед началом работы с оборудованием.

2.10.4 *Требования к электропитанию*

2.10.4.1 Требования к виду источника электропитания

Электропитание должно осуществляться от источника постоянного тока с заземленным положительным потенциалом с напряжением 48, либо от источника дистанционного питания постоянного тока напряжением до 220 В.

2.10.4.2 Требования к допустимым изменениям напряжения источника питания постоянного тока

Изменения напряжения источника питания с напряжением 48 В допускаются в пределах от 40,5 до 57 В.

В случае снижения напряжения источника электропитания ниже допустимых пределов и при последующем восстановлении напряжения характеристики средства связи восстанавливаются автоматически.

2.10.4.3 Требования к допустимым помехам источника электропитания постоянного тока

Оборудование должно нормально функционировать при помехах источника электропитания, не превышающих приведенных в таблице 15.

Таблица 15 — Требования к допустимым помехам источника электропитания постоянного тока

Вид помехи	Значение
Допустимое отклонение напряжения от номинального значения, %: длительностью 50 мс длительностью 5 мс	 -20 40
Пульсации напряжения гармонических составляющих, мВэфф в диапазоне до 300 Гц в диапазоне выше 300 Гц до 150 кГц	 50 7

2.10.4.4 Требования к помехам, создаваемым оборудованием в цепи источника электропитания

Напряжения помех, создаваемых оборудованием в цепи источника электропитания, не должны превышать значений, приведённых в таблице Таблица 16.

Таблица 16 — Требования к помехам, создаваемым оборудованием в цепи источника электропитания

Вид помехи	Значение
Суммарные помехи в диапазоне от 25 Гц до 150 Гц, мВэфф	50
Селективные помехи в диапазоне от 300 Гц до 150 кГц	7
Взвешенное (псофометрическое) значение помех, мВпсоф	2

2.10.4.5 Требования к источнику питания переменного тока

Параметры источника питания переменного тока:

- Максимально допустимое напряжение — не более 220 В.
- Источник питания переменного тока оснащается устройством защитного отключения (УЗО).
- Прочность изоляции цепей источника питания переменного тока относительно корпуса выдерживает (в нормальных условиях) не менее 1000 В пик.

2.11 Установка SBC

Перед установкой и включением устройства необходимо проверить устройство на наличие видимых механических повреждений. В случае наличия повреждений следует прекратить установку устройства, составить соответствующий акт и обратиться к поставщику.

Если устройство находилось длительное время при низкой температуре, перед началом работы следует выдержать его в течение двух часов при комнатной температуре. После длительного пребывания устройства в условиях повышенной влажности перед включением выдержать в нормальных условиях не менее 12 часов.

Смонтировать устройство. Устройство может быть закреплено на 19" несущих стойках при помощи комплекта крепежа, либо установлено на горизонтальной перфорированной полке.

После установки устройства требуется заземлить его корпус. Это необходимо выполнить прежде, чем к устройству будет подключена питающая сеть. Заземление выполнять изолированным многожильным проводом. Правила устройства заземления и сечение заземляющего провода должны соответствовать требованиями ПУЭ. Клемма заземления находится в правом нижнем углу задней панели, рисунки 5, 7 и 9.

2.11.1 *Порядок включения*

1. Подключить оптический и электрический Ethernet-кабели к соответствующим разъемам шлюза.
2. Подключить к устройству кабель питания. Для подключения к сети постоянного тока использовать провод сечением не менее 1 мм^2.
3. Если предполагается подключение компьютера к консольному порту SBC, соединить консольный порт SBC с COM-портом ПК, при этом ПК должен быть выключен и заземлен в одной точке с SBC.
4. Убедиться в целостности кабелей и их надежном креплении к разъемам.
5. Включить питание устройства и убедиться в отсутствии аварий по состоянию индикаторов на передней панели.

2.11.2 *Крепление кронштейнов*

В комплект поставки устройства входят кронштейны для установки в стойку и винты для крепления кронштейнов к корпусу устройства.

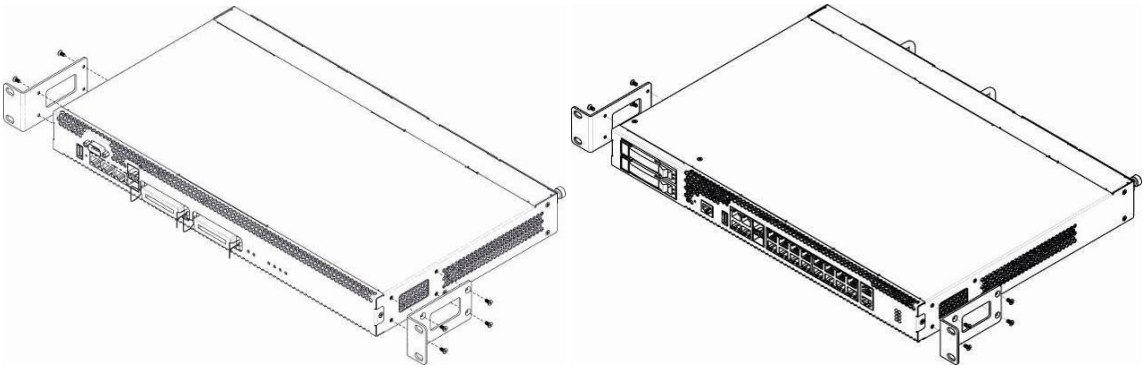


Рисунок 10 — Крепление кронштейнов для SBC-1000 (слева) и SBC-2000 (справа)

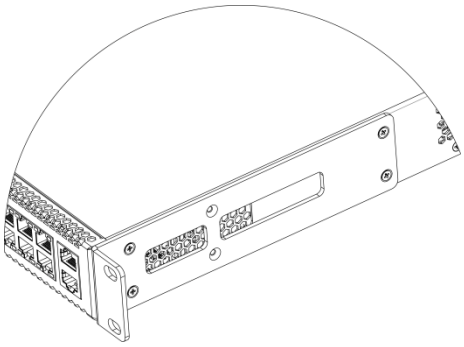


Рисунок 11 — Крепление кронштейнов для SBC-3000

Для установки кронштейнов:

1. Совместите четыре отверстия для винтов на кронштейне с такими же отверстиями на боковой панели устройства, Рисунок 10 и Рисунок 11.
2. С помощью отвертки прикрепите кронштейн винтами к корпусу.

Повторите действия 1, 2 для второго кронштейна.

2.11.3 *Установка устройства в стойку*

Для установки устройства в стойку:

1. Приложите устройство к вертикальным направляющим стойки.
2. Совместите отверстия кронштейнов с отверстиями на направляющих стойки. Используйте отверстия в направляющих на одном уровне с обеих сторон стойки, для того чтобы устройство располагалось горизонтально.
3. С помощью отвертки прикрепите устройство к стойке винтами.
4. Для демонтажа устройства отсоединить подключенные кабели и винты крепления кронштейнов к стойке. Вынуть устройство из стойки.

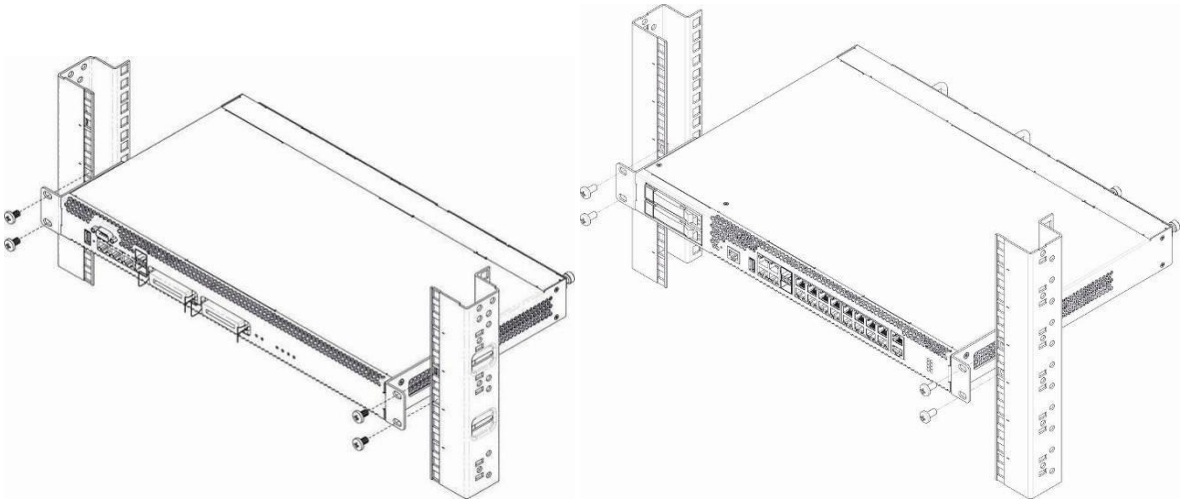


Рисунок 12 — Установка устройства в стойку SBC-1000 (слева) и SBC-2000 (справа)

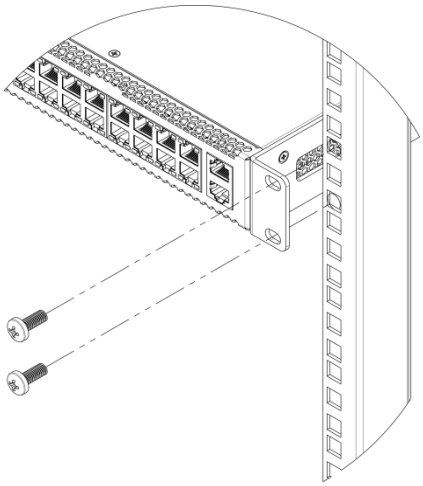


Рисунок 13 — Установка устройства в стойку SBC-3000

2.11.4 *Установка модулей питания*

Устройство может работать с одним или двумя модулями питания. Установка второго модуля питания необходима в случае использования устройства в условиях, требующих повышенной надежности.

Места для установки модулей питания с электрической точки зрения равноценны. С точки зрения использования устройства, модуль питания, находящийся ближе к краю, считается основным, ближе к центру — резервным. Модули питания могут устанавливаться и извлекаться без выключения устройства. При установке или извлечении дополнительного модуля питания устройство продолжает работу без перезапуска.

В устройстве SBC установлено 2 предохранителя блоков питания номиналом 3,15 А. Самостоятельная замена предохранителей невозможна и осуществляется только квалифицированными специалистами в сервисном центре завода-изготовителя. Установка модулей питания показана на рисунке ниже.

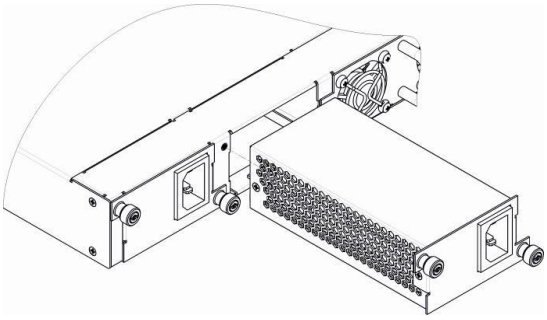


Рисунок 14 — Установка модулей питания

2.11.5 *Вскрытие корпуса*

Предварительно надлежит отключить питание устройства, отсоединить все кабели и, если требуется, демонтировать устройство из стойки (подробнее в разделе 2.11.3 Установка устройства в стойку).

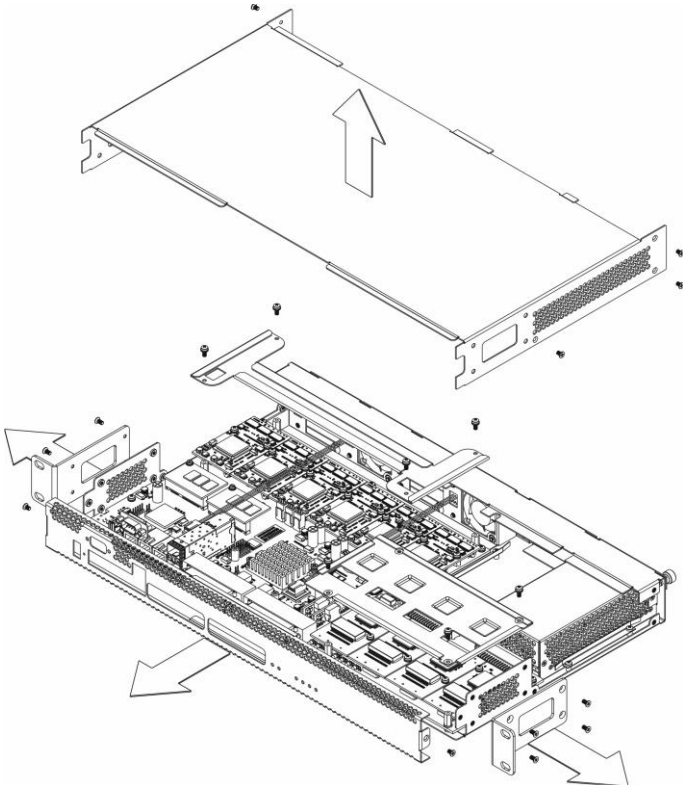


Рисунок 15 — Порядок вскрытия корпуса SBC-1000 (на базе SMG-1016M)

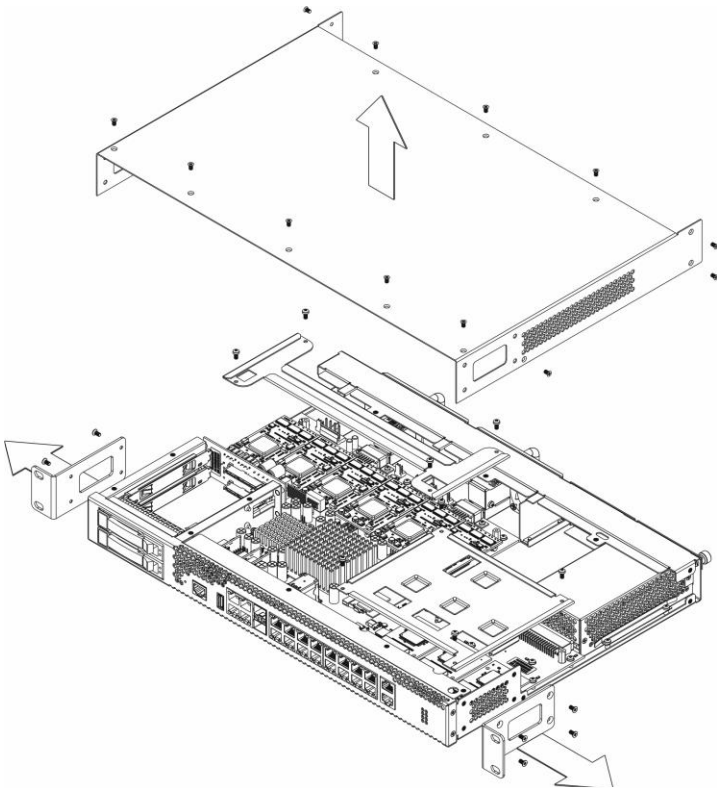


Рисунок 16 — Порядок вскрытия корпуса SBC-2000 (на базе SMG-2016)

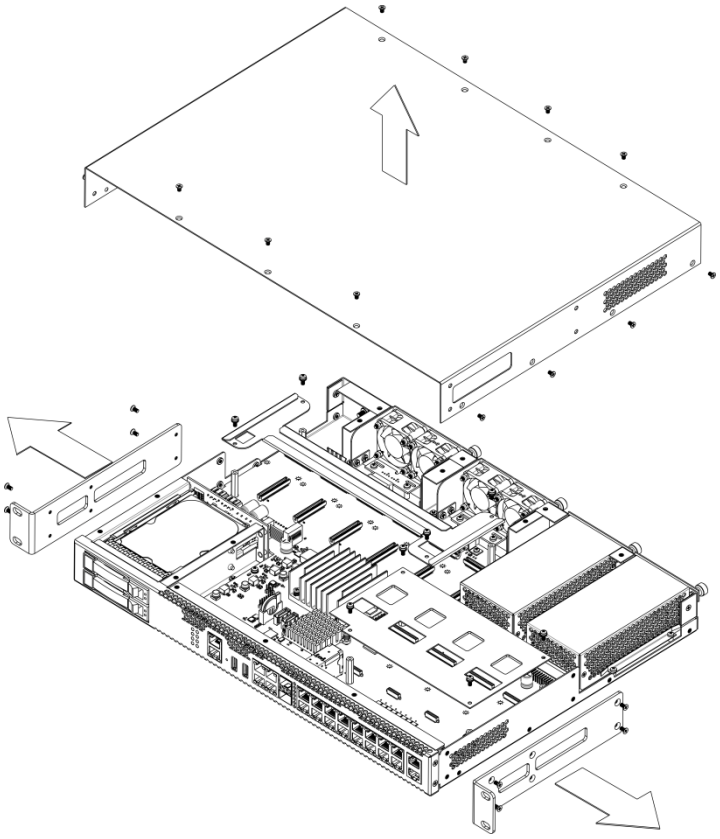


Рисунок 17 — Порядок вскрытия корпуса на SBC-3000 (на базе SMG-3016)

1. С помощью отвертки отсоединить кронштейны от корпуса устройства.
2. **Только для SBC-1000** необходимо открутить фиксирующие винты передней панели, затем потянуть её на себя до отделения от верхней и боковых панелей (Рисунок 15).

3. Открутить винты верхней панели устройства.
4. Снять верхнюю панель (крышку) устройства, потянув ее наверх.

При сборе устройства в корпус выполнить вышеперечисленные действия в обратном порядке.

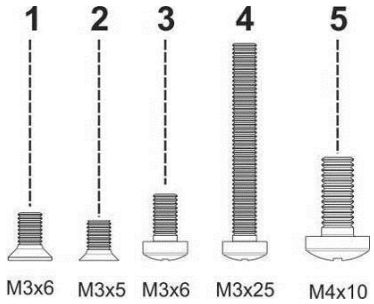


Рисунок 18 — Типы болтов для сборки SBC (на базе SMG)

На рисунке 18 представлены типы болтов, используемые для сборки устройства в корпус:

1. Крепление кронштейнов для установки в стойку.
2. Крепление корпусных деталей.
3. Крепление плат, вентиляционный блоков, заглушек, направляющих.
4. Винт крепления вентиляторов.
5. Винт заземления.

При сборке устройства запрещается использовать ненадлежащий тип болтов для указанных операций. Изменение типа винта может привести к выходу устройства из строя.

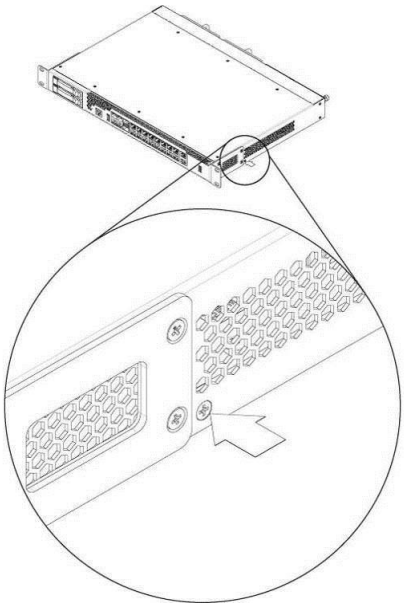


Рисунок 19 — Сборка в корпус

При сборке устройства SBC в место, указанное на рисунке выше, требуется установить винт, заложенный при производстве. Изменение типа винта может привести к выходу устройства из строя.

2.11.6 *Установка блоков вентиляции*

Конструкция устройства предусматривает возможность замены блоков вентиляции без отключения питания.

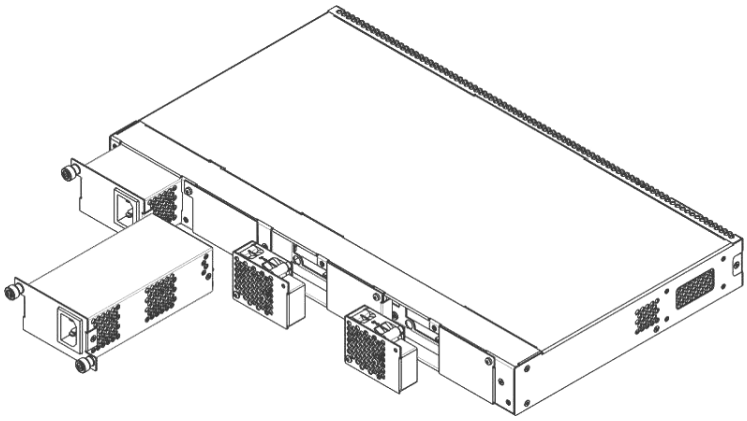


Рисунок 20 — Блок вентиляции в SBC-1000 на базе SMG-1016M. Крепление в корпус

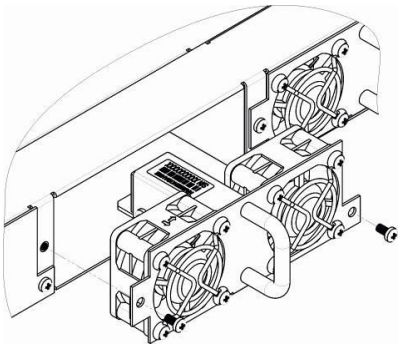


Рисунок 21 — Блок вентиляции в SBC-2000 на базе SMG-2016. Крепление в корпус

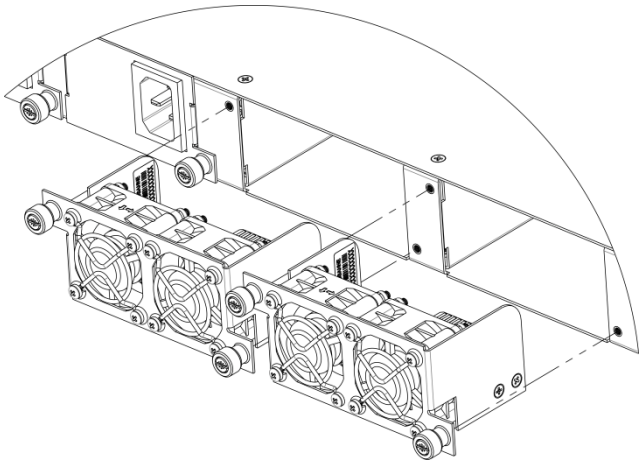


Рисунок 22 — Блок вентиляции в SBC-3000 на базе SMG-3016. Крепление в корпус

Для удаления блока необходимо:

1. С помощью отвертки отсоединить винты крепления блока вентиляции на задней панели.
2. Осторожно потянуть блок на себя до извлечения из корпуса.
3. Отсоединить контакты блока от разъема в устройстве, Рисунок 23.

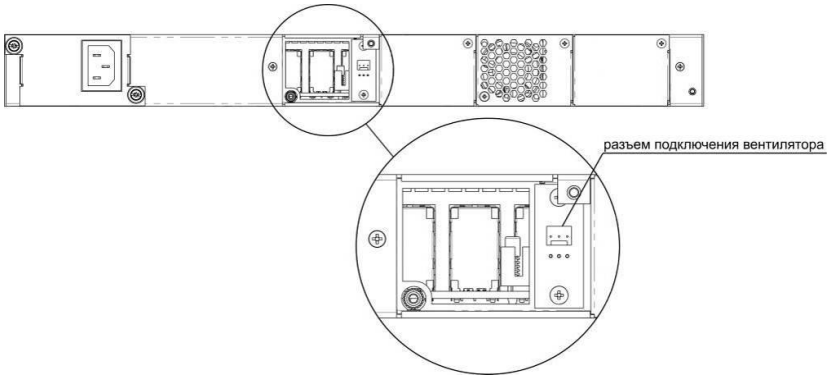


Рисунок 23 — Разъем для подключения вентилятора в SBC-1000 на базе SMG-1016M

Для установки блока необходимо:

1. Соединить контакты блока с разъемом в устройстве.
2. Вставить блок в корпус устройства.
3. Закрепить винтами блок вентиляции на задней панели.

2.11.7 *Установка SSD-накопителей для SBC-1000*

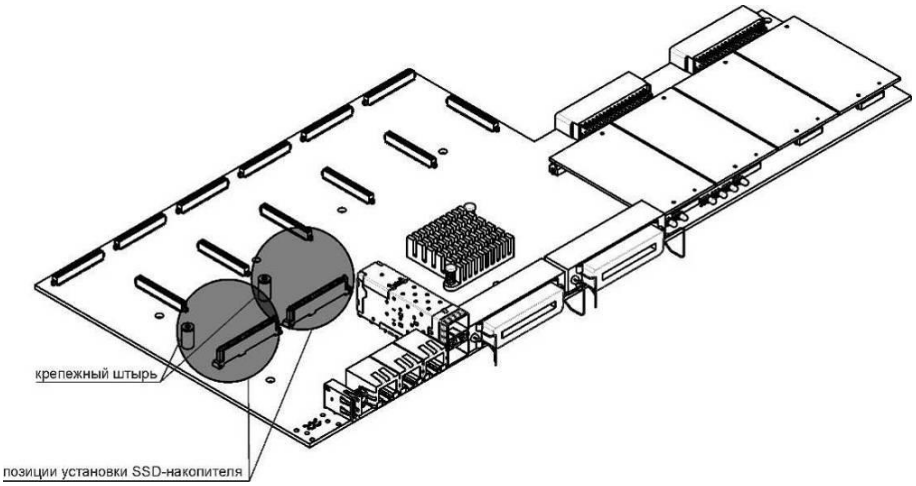


Рисунок 24 — Установка SSD-накопителя

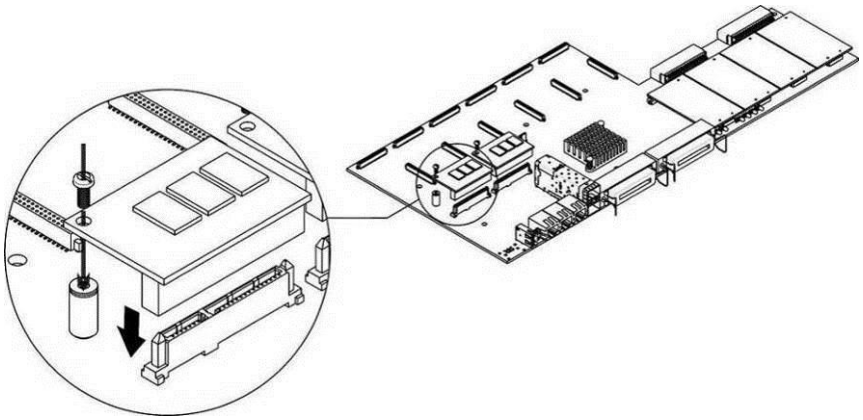


Рисунок 25 — Монтаж SSD-накопителя

1. Проверить наличие питания сети на устройстве.
2. В случае наличия напряжения — отключить питание.
3. Если требуется, демонтировать устройство из стойки (подробнее в разделе 2.11.3).

4. Вскрыть корпус устройства (подробнее в разделе 2.11.5).
5. Если на плате устройства отсутствует крепежный штырь (Рисунок 24), необходимо использовать съемную стойку:
   a. прикрепить стойку-фиксатор к SSD-накопителю;
   b. снять верхний защитный слой с клеевой поверхности стойки-фикса тора;
6. Установить накопитель в свободную позицию — всего доступно 2 позиции (Рисунок 24), и, если на плате присутствует крепежный штырь, закрепить винтом, как показано на рисунке 25.

При удалении SSD-накопителя выполнить вышеперечисленные действия в обратном порядке.

2.11.8 *Установка SATA-дисков для SBC-2000 и SBC-3000*

При заказе с устройством могут быть дополнительно поставлены SATA-диски. Слот для подключения дисков рассчитан на накопители форм-фактора 2,5" толщиной до 12,5 мм".

При монтаже SATA-дисков необходимо:

1. Извлечь направляющие салазки из корпуса устройства (Рисунок 6, элемент 1), для этого нажать на кнопку справа до отхождения ручки выталкивателя, затем потянуть ручку на себя до извлечения салазок из корпуса.
2. Извлечь комплект крепежа, расположенный под ручкой выталкивателя, Рисунок 26.
3. Закрепить диск в лотке направляющих салазок, Рисунок 27.
4. Вставить салазки с установленным SATA-диском обратно в разъем и прижать ручку выталкивателя до характерного щелчка.

При удалении SATA-диска выполнить вышеперечисленные действия в обратном порядке.

Установка и удаления SATA-дисков могут быть произведены при включенном питании устройства.

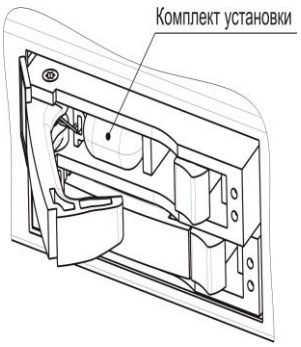


Рисунок 26 — Расположение комплекта крепежных элементов при поставке

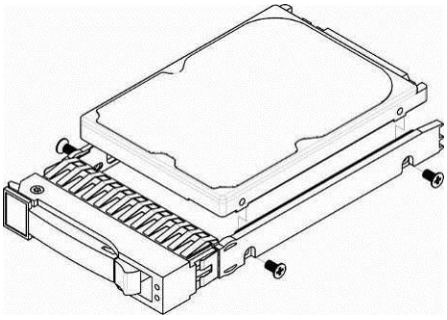


Рисунок 27 — Крепление SATA-диска в лоток направляющих салазок

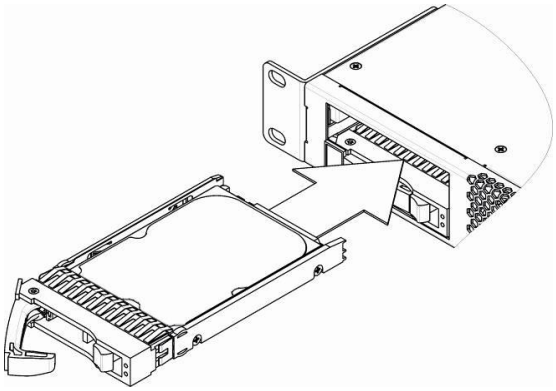


Рисунок 28 — Монтаж SATA-диска в корпус устройства

2.11.9 *Замена батарейки часов реального времени*

В RTC — электронной схеме, предназначенной для автономного учёта хронометрических данных (текущее время, дата, день недели и др.) на плате устройства установлен элемент питания (батарейка), имеющий следующие характеристики:

Тип батареи	литиевая
Типоразмер	CR2032 (возможна установка CR2024)
Напряжение	3 В
Емкость	225 мА
Диаметр	20 мм
Толщина	3,2 мм
Срок службы или срок годности	5 лет
Условия хранения	от -20 до +35 С

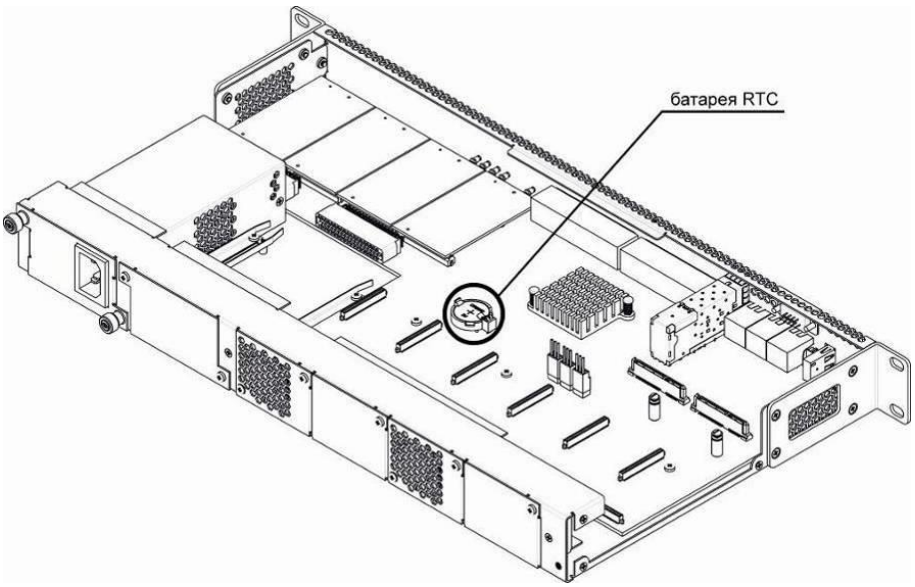


Рисунок 29 — Положение батареи RTC для SBC-1000 (на базе SMG-1016M)

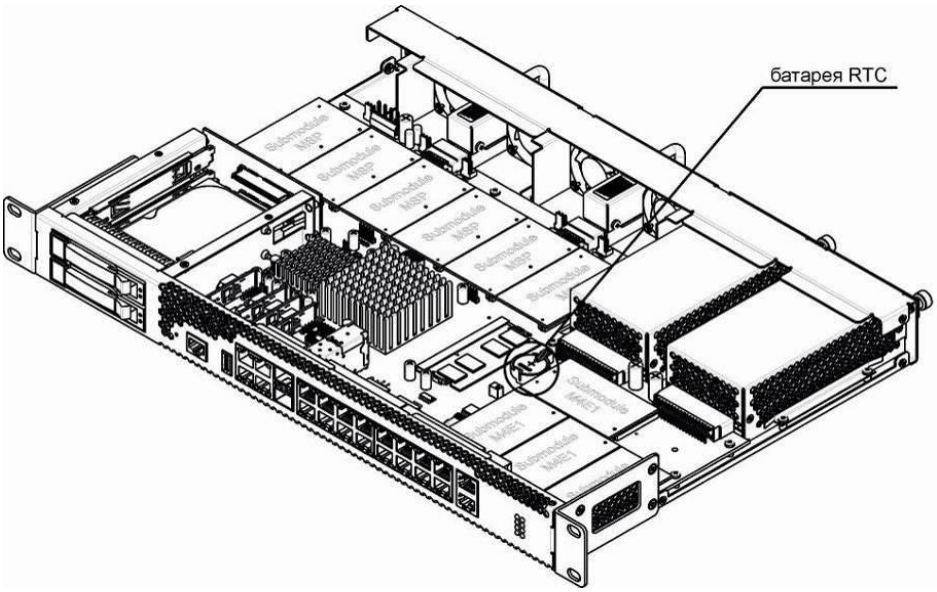


Рисунок 30 — Положение батареи RTC для SBC-2000 (на базе SMG-2016)

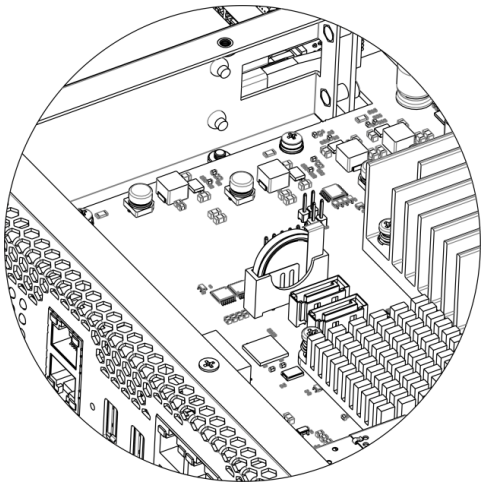


Рисунок 31 — Положение батареи RTC для SBC-3000 (на базе SMG-3016)

В случае если срок работы батарейки истек, для корректной и бесперебойной работы оборудования необходимо заменить ее на новую, выполнив следующие действия:

1. Проверить наличие питания сети на устройстве.
2. В случае наличия напряжения — отключить питание.
3. Если требуется, демонтировать устройство из стойки (подробнее в разделе 2.11.3).
4. Вскрыть корпус устройства (подробнее в разделе 2.11.5).
5. Извлечь отработавшую батарейку (Рисунок 29, Рисунок 30 и Рисунок 31) и в аналогичной позиции установить новую.

При сборе устройства в корпус выполнить вышеперечисленные действия в обратном порядке.

При отключенной синхронизации NTP после замены батарейки RTC необходимо заново установить системную дату и время на устройстве.

Использованные батарейки подлежат специальной утилизации.

3 ОБЩИЕ РЕКОМЕНДАЦИИ ПРИ РАБОТЕ С УСТРОЙСТВОМ

Самым простым способом конфигурирования и мониторинга устройства является Web-конфигуратор, поэтому для этих целей рекомендуется использовать его.

Во избежание несанкционированного доступа к устройству рекомендуем сменить пароль на доступ через Telnet, SSH и консоль (по умолчанию пользователь **admin**, пароль **rootpasswd**), а также сменить пароль для администратора на доступ через Web-конфигуратор. Установка пароля для доступа через Telnet и консоль описана в разделе 4.2. Рекомендуется записать и сохранить установленные пароли в надежном месте, недоступном для злоумышленников. Также настоятельно рекомендуем не открывать доступ к устройству через Telnet, SSH и WEB из публичной сети.

В локальной сети для доступа к Web-конфигуратору лучше использовать соединение по протоколу HTTPS вместо HTTP (настройка описана в разделе Настройка SSL/TLS). Для доступа к CLI лучше использовать протокол SSH вместо Telnet. Выбор протоколов доступа осуществляется в настройках сетевого интерфейса (описание в разделе 4.1.4.3). Также рекомендуется выделить на SBC отдельный интерфейс для управления в выделенном VLAN. Для ограничения доступа к администрированию SBC с отдельных узлов можно использовать так же белый список адресов, с которых может осуществляться управление (подробнее в разделе 4.1.8.6).

Во избежание потери данных настройки устройства, например, после сброса к заводским установкам, рекомендуем сохранять резервную копию конфигурации на компьютере каждый раз после внесения в нее существенных изменений.

В сети следует использовать доверенные и защищённые DNS и NTP-серверы. Желательно разместить оборудование за сетевым экраном, на котором настроен ingress filtering.

3.1 Обеспечение безопасности вызовов

SBC имеет несколько механизмов, обеспечивающих безопасность вызовов:

- Встроенный firewall, который обеспечивает следующие функции (подробнее в разделе 4.1.8.5 Статический брандмауэр):
  - Фильтрация по IP-адресам, портам и протоколам;
  - Фильтрация пользователей по географическому признаку (GeoIP);
  - Фильтрация по строкам, содержащимся в сообщениях.
- Ограничения вызовов в правилах Rule Set (подробнее в разделе 4.1.3.5):
  - Действие "reject" — позволяет запретить прохождение вызовов по условиям, подпадающим под правило. Например, можно использовать правило для запрета прохождения международных вызовов "Имя из заголовка To" с маской имени "^\+*[78]10.+";
  - Действие "send to..." с использованием фильтров. Например, можно установить ограничение вызовов только по России, используя правило "Имя из заголовка To" в виде маски "^7[3489].{9}$";
  - Ограничение по времени действия правила. Таким образом можно ограничить время действия услуги связи или запретов связи, комбинируя ограничение по времени действия и правила "reject" и "send to...".
- Защита от DoS-атак (подробнее в разделе 4.1.8.7):
  - Защита от ICMP-флуда. В этом режиме SBC не будет откликаться на запросы ICMP type 8 и type 13;

- Обнаружение port scan. SBC будет анализировать попытки доступа и при обнаружении сканирования портов заблокирует нарушителя;
- Список запрещённых клиентских приложений. SBC будет блокировать SIP-запросы по обнаружению в User-Agent заданных шаблонов, которые соответствуют популярным SIP-сканерам и утилитам для совершения различных атак;
- Защита от SIP-флуда. SBC анализирует активность как сетевых хостов, так и отдельных абонентов на предмет действий, рассматриваемых как флуд или попытки подбора паролей. Также SBC начинает заменять ответы 404 на 403 для затруднения сканирования распределения номеров.

4 КОНФИГУРИРОВАНИЕ УСТРОЙСТВА

К устройству можно подключиться четырьмя способами: через Web-конфигуратор, с помощью протокола Telnet, SSH либо кабелем через разъем RS-232 (при доступе через RS-232, SSH либо Telnet используется командная консоль CLI).

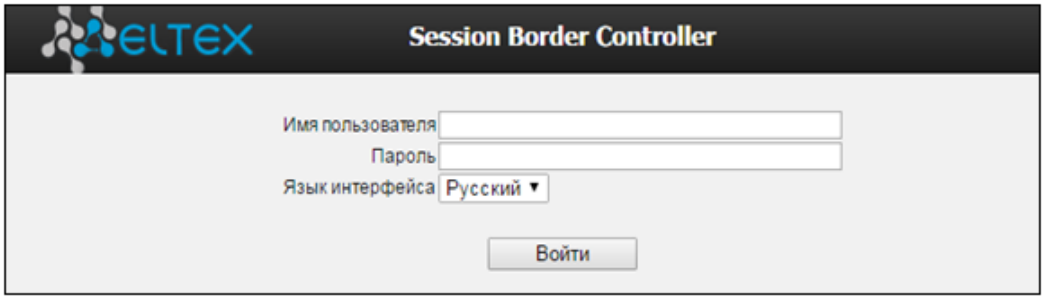
Для сохранения измененной конфигурации в энергонезависимую память используйте меню «Сервис/Сохранить конфигурацию во Flash» в Web-конфигураторе, либо команду `copy running to startup save` в командной консоли CLI.

4.1 Настройка SBC через Web-конфигуратор

Для того чтобы произвести конфигурирование устройства, необходимо подключиться к нему через web-браузер (программу-просмотрщик гипертекстовых документов), например: Google, Firefox, Internet Explorer и т.д. Ввести в строке браузера IP-адрес устройства:

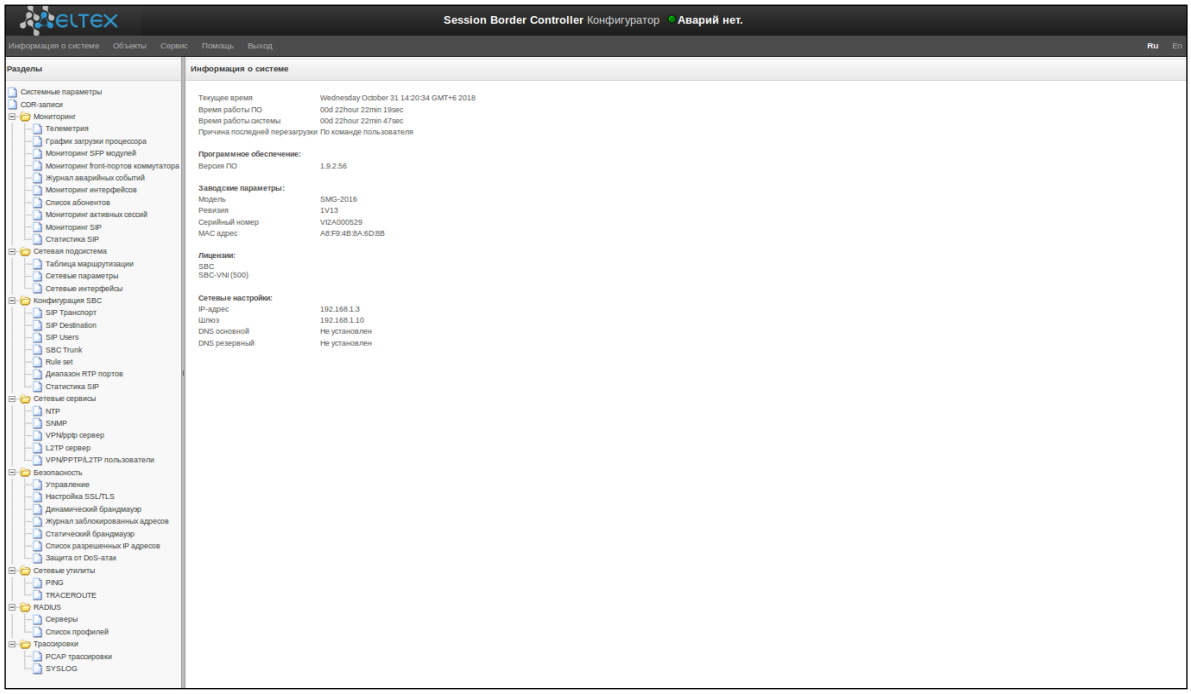
Заводской IP-адрес устройства SBC 192.168.1.2, маска сети 255.255.255.0

После ввода IP-адреса устройство запросит имя пользователя и пароль. Также здесь можно выбрать язык, который будет использоваться в интерфейсе.



При первом запуске имя пользователя: *admin*, пароль: *rootpasswd*.

После получения доступа к Web-конфигуратору откроется меню *«Информация о системе».*



На рисунке ниже представлены элементы навигации Web-конфигуратора.

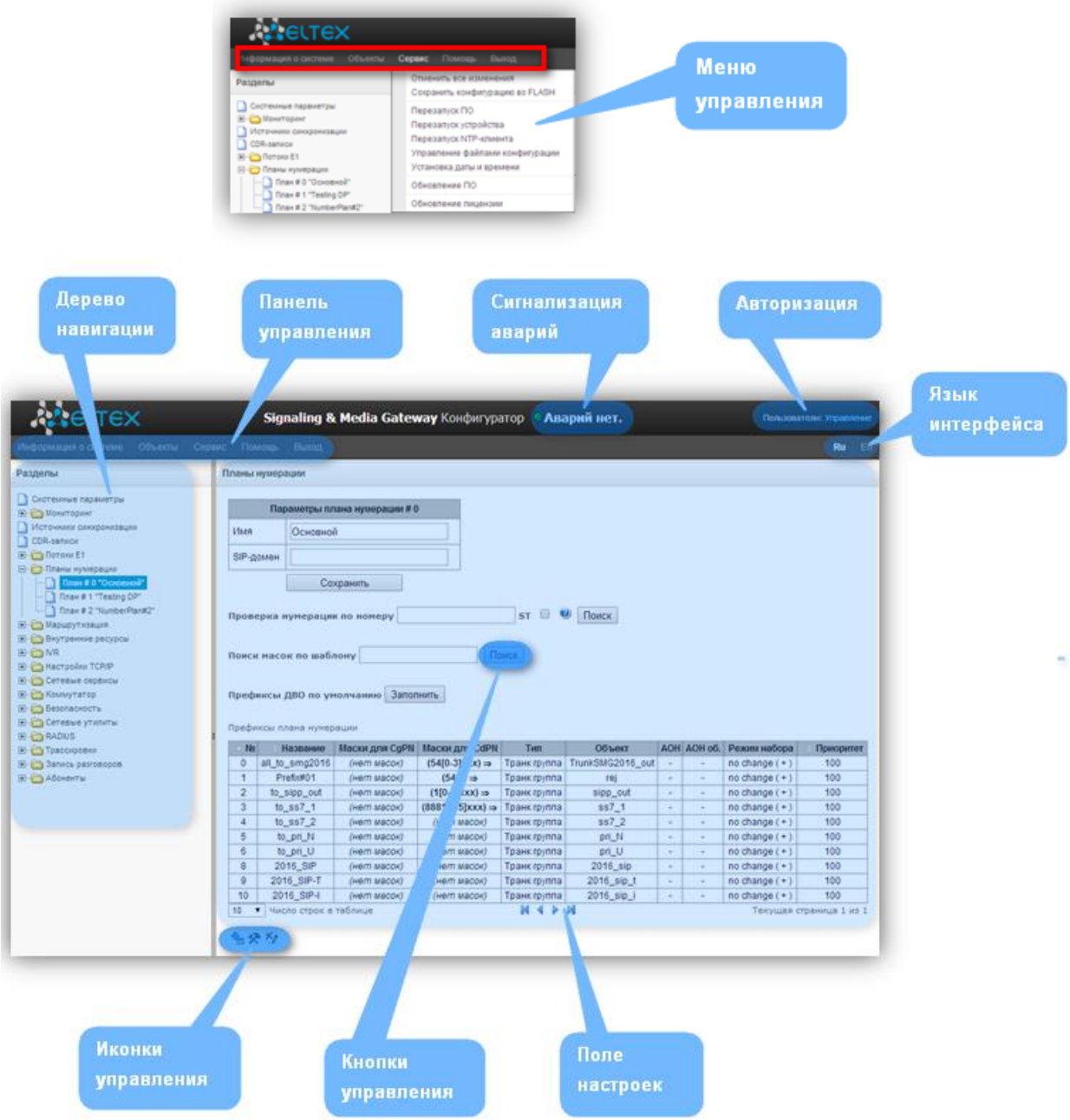


Рисунок 32 — Элементы навигации Web-конфигуратора

Окно пользовательского интерфейса разделено на несколько областей:

Дерево навигации – служит для управления полем настроек. В дереве навигации иерархически отображены разделы управления и меню, находящиеся в них.

Поле настроек – базируется на выборе пользователя. Предназначено для просмотра настроек устройства и ввода конфигурационных данных.

Панель управления – панель для управления полем настроек и состоянием ПО устройства.

Меню управления – выпадающие меню панели управления полем настроек и состоянием ПО устройства

Сигнализация аварий – служит для отображения текущей приоритетной аварии, также является ссылкой для работы с журналом аварийных событий.

Авторизация – ссылка для работы с паролями доступа к устройству через web-конфигуратор.

Язык интерфейса – кнопки для переключения языка интерфейса.

Иконки управления – элементы управления для работы с объектами поля настроек, дублируют меню «Объекты» на панели управления:

— *Добавить объект;*
— *Редактировать объект;*
— *Удалить объект;*
— *Посмотреть объект.*

Кнопки управления – элементы управления для работы с полем настроек.

Во избежание несанкционированного доступа при дальнейшей работе с устройством рекомендуется изменить пароль (раздел 4.1.8.1).

Кнопка («Подсказка») рядом с элементом редактирования позволяет получить пояснения по данному параметру.

4.1.1 *Системные параметры*

В данном разделе производится настройка системных параметров и ограничений обработки запросов.

Системные параметры	
Имя устройства	SBC1000
Путь к диску для хранения трассировок	default
Устройство для аварийного логирования	Нет
Индикация аварий	
Работа вентиляторов	☑
Загруженность процессора	☑
Использование оперативной памяти	☑
Заполнение внешних накопителей	☑
Аварии резервирующего устройства	☑
Отсутствие связи с ведомым	☐
Ограничение обработки запросов INVITE	☐
Ограничение обработки запросов SUBSCRIBE	☐
Ограничение обработки остальных запросов	☐
Ограничение обработки запросов SBC	
Запросы INVITE, ед/3 сек	15
Запросы SUBSCRIBE, ед/3 сек	15
Остальные запросы, ед/3 сек	15
Защитный таймаут для отбоя вызовов без media, мин	30
Настройки SIP	
Включить статистику SIP вызовов	☐
Передавать символ '#' без кодирования	☐

Сохранить Отменить

Автоматическое конфигурирование	
Включить автообновление	☐
Источник	Static
Протокол	TFTP
Аутентификация	☐
Имя	
Пароль	
Сервер	update.local
Обновлять конфигурацию	☐
Имя файла конфигурации	a8.f9.4b.88.70.a6.cfg
Период обновления конфигурации, мин	30
Обновлять ПО	☐
Имя файла версий ПО	SBC1000.manifest
Период обновления ПО, мин	30

Сохранить Отменить

Системные параметры

- *Имя устройства* — наименование устройства, выводимое в заголовке web-конфигуратора (в данной версии ПО не используется);
- *Путь к диску для хранения трассировок* — на устройстве существует возможность сохранения отладочной информации (трассировок) в оперативной памяти (RAM), либо на установленном SSD накопителе:
  - *default* — отладочная информация сохраняется в оперативную память;
  - */mnt/sdX* — путь к локальному SSD-диску, настройка отображается при установленном SSD-диске. При выборе SSD-диска на нем будет создан каталог logs, в котором будут храниться файлы трассировок;

Сохранение трассировок доступно только для SSD-диска, хранение на USB-flash невозможно.

- *Устройство для аварийного логирования* — выбор SSD-диска для записи критических аварийных сообщений в энергонезависимую память. Данная опция может быть необходима при выяснении причин перезапуска или выхода из строя оборудования.
  - */mnt/sdX* — выбор пути к локальному SSD-диску**.** При включении данной опции на SSD-диске создается файл alarm.txt, в которой заносится информация об авариях.

Пример файла alarm.txt

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

Описание формата файла:
0, 1, 2… — порядковый номер события;
24/09/13 — дата возникновения события;
20:03:22 — время возникновения события;
ALARM/OK — текущее состояние события (OK — авария нормализована, ALARM — авария активна).

Таблица 17 — Примеры выводимых сообщений об авариях

Аварийное сообщение	**Расшифровка**
Конфигурация не прочитана	Ошибка файла конфигурации
Высокая загрузка процессора	Авария высокой загрузки процессора
Port Scan Detector выключен	Информационное сообщение о выключенной защите от Port Scan в конфигурации
Динамический брандмауэр заблокировал новый адрес	Предупреждение о блокировке нового адреса с указанием причины в описании
Регистрация абонента запрещена	Поступил запрос регистрации, обслуживание которого запрещено
Звонок запрещен	Поступил вызов, обслуживание которого запрещено
Запуск ПО V.1.X.X.X	Программное обеспечение запущено
На ведомом устройстве установлена другая версия ПО	Устройства в резерве имеют разные версии ПО

Отсутствует подключение с ведомым	Отсутствует подключение с резервным устройством либо полностью, либо на одном из линков. Во втором случае в параметрах будет указано, на каком линке потеряна связь
Смена состояния в группе резерва	Произошло пересогласование устройств в резерве
Оперативная память заканчивается	Оперативная память заканчивается. Возможны 3 уровня аварии — предупреждение (осталось менее 25% свободной памяти), авария (менее 10%), критическая авария (менее 5%)
Не удалось отправить CDR-файлы по FTP	Проблема отправки файла CDR на FTP — сервер
Запуск ПО устройства	Запуск ПО устройства

Индикация аварий

- *Работа вентиляторов* — при установленном флаге в систему управления будет выдаваться авария о неисправности вентиляторов;
- *Загруженность процессора* — при установленном флаге в систему управления будет выдаваться авария о высокой загрузке процессора;
- *Использование оперативной памяти* — при установленном флаге в систему управления будет выдаваться авария о заканчивающейся свободной оперативной памяти;
- *Заполнение внешних накопителей* — при установленном флаге в систему управления будет выдаваться авария о заканчивающемся свободном дисковом пространстве на внешних накопителей;
- *Аварии резервирующего устройства* — при установленном флаге в систему управления будут выдаваться вышеперечисленные аварии с резервирующего устройства;
- Отсутствие связи с ведомым — при установленном флаге в систему управления будут выдаваться аварии об отсутствии связи с резервирующим устройством на локальном и глобальном линках;
- Ограничение обработки запросов INVITE — при установленном флаге в систему управления будут выдаваться аварии о превышении максимально разрешенного количества одновременных запросов INVITE, заданное в разделе «Ограничение обработки запросов SBC»;
- Ограничение обработки запросов SUBSCRIBE — при установленном флаге в систему управления будут выдаваться аварии о превышении максимально разрешенного количества одновременных запросов SUBSCRIBE, заданное в разделе «Ограничение обработки запросов»;
- Ограничение обработки остальных запросов — при установленном флаге в систему управления будут выдаваться аварии о превышении максимально разрешенного количества одновременных запросов, отличных от INVITE и SUBSCRIBE.

Ограничение обработки запросов SBC

- *Запросы INVITE, ед/3 сек* — количество запросов INVITE, обрабатываемых в течение трех секунд. Если за три секунды поступит большее количество запросов, то превысившие порог запросы не будут обслужены;
- *Запросы SUBSCRIBE, ед/3 сек* — количество запросов SUBSCRIBE, обрабатываемых в течение трех секунд. Если за три секунды поступит большее количество запросов, то превысившие порог запросы не будут обслужены;
- *Остальные запросы, ед/3 сек* — количество запросов, отличных от INVITE и SUBSCRIBE, обрабатываемых в течение трех секунд. Если за три секунды поступит большее количество запросов, то превысившие порог запросы не будут обслужены;
- *Защитный таймаут для отбоя вызовов без media, мин* — интервал времени, по истечении которого вызов, установленный между устройствами, будет отклонен в случае, если между ними по разговорному каналу не передаются RTP-пакеты.

Настройки SIP

- *Включить статистику SIP вызовов* — включает ведение статистики вызовов. Статистика отображается в разделе мониторинга "Статистика SIP";

- Передавать символ '#' без кодирования — при включенной опции SBC в исходящее плечо символ '#' отправляет как '#', при выключенной опции отправляет как '%23'.

Автоматическое конфигурирование

SBC может автоматически получать конфигурацию и файлы с версиями ПО с сервера автоконфигурирования (далее — «сервер») с заданным периодом.

После скачивания конфигурации, SBC будет ожидать завершения всех активных вызовов, после чего применит новую конфигурацию. Либо конфигурация применится вместе с новым ПО перед перезагрузкой.

Файл с описанием версий ПО содержит в себе информацию об имеющемся на сервере ПО — версии и имена файлов. Там же можно задать разрешённое для обновления время. Формат файла должен быть следующим:

<номер версии ПО>;<имя файла с ПО>;<разрешённое время обновления, час>

- *Номер версии ПО* — задаётся полностью до версии сборки;
- *Имя файла с ПО* должно иметь расширение .bin;
- *Разрешённое время обновления может отсутствовать.* В этом случае SBC обновится в ближайшее время, когда не будет активных вызовов. Если же указан интервал времени, то SBC будет обновляться только в заданный интервал времени.

Пример файла описания версий ПО:
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

- *Включить автообновление* — включить автоматическое обновление конфигурации и ПО;
- *Источник* — выбор источника информации о сервере:
  - *Static* — информация о сервере заносится и сохраняется на SBC в соответствующем поле;
  - *DHCP (имя интерфейса)* — информация о сервере будет получена на выбранном интерфейсе по протоколу DHCP из опции 66, информация об имени файла версий и файла конфигурации будет получена из опции 67;
- *Протокол* — выбор протокола для соединения с сервером;
- *Аутентификация* — использовать аутентификацию для доступа на сервер (для протоколов FTP, HTTP, HTTPS);
- *Имя* — имя (логин) для доступа на сервер;
- *Пароль* — пароль для доступа на сервер;
- *Сервер* — IP-адрес или доменное имя сервера. Используется при выбранном источнике Static;
- *Обновлять конфигурацию* — разрешает обновление конфигурации с сервера;
- *Имя файла конфигурации* — имя файла конфигурации. Имя должно быть с расширением .cfg и иметь длину не более 64 символов;
- *Период обновления конфигурации, м* — периодичность проверки сервера на наличие конфигурации;
- *Обновлять ПО* — разрешает обновление ПО с сервера;
- *Имя файла версий ПО* — имя файла с версиями ПО. Имя должно быть с расширением .manifest и иметь длину не более 64 символов;
- *Период обновления ПО, м* — периодичность проверки сервера на наличие нового ПО.

Выгрузка конфигураций

SBC может автоматически выгружать конфигурацию на внешний FTP/TFTP сервер при каждом её сохранении в энергонезависимую память.

- *Включить* — включает функцию выгрузки конфигурации;
- *Протокол* — выбор протокола, по которому будет производиться выгрузка. Поддерживается FTP или TFTP;
- *Сервер* — IP-адрес сервера, на который будет производиться выгрузка;
- *Порт* — порт сервера, на который будет производиться выгрузка;
- *Путь к файлу* — директория на сервере, в которую будет сохраняться конфигурация;
- *Имя* — имя для аутентификации при использовании протокола FTP;
- *Пароль* — пароль для аутентификации при использовании протокола FTP.

4.1.2 *Мониторинг*

4.1.2.1 Телеметрия

В разделе отображается информация о показаниях датчиков системы телеметрии, установленных на устройстве, а также информация об установленных блоках питания и вентиляторах процессора.

Мониторинг –> Телеметрия

Температурные датчики

Для SBC-1000:

- *Датчик #0* — температура процессора;
- *Датчик #1* — температура коммутатора.

Для SBC-2000:

- *Температура CPU* — температура процессора.

Блоки питания

- *Блок питания #0* — состояние блока питания в нулевой позиции;
- *Блок питания #1* — состояние блока питания в первой позиции).

Возможные состояния блоков питания:

- *Установлен* — блок питания установлен.
- *Не установлен* — блок питания не установлен.
- *Работает* — на блок питания подается питающее напряжение.
- *Не работает* — на блок питания не подается питающее напряжение.

Вентиляторы

- *Вентилятор #N* — информация о состоянии вентилятора N и о его скорости вращения (например, 9600 rpm).

В устройстве SBC-1000 установлено 2 вентилятора, в SBC-2000 — 4 вентилятора, в SBC-3000 — 4 вентилятора.

Напряжение[1]:

– *Внутреннее напряжение (+12В)* — информация о состоянии датчика напряжения 12В.

Текущие напряжения[2]:

– *+12.0 В* — информация о состоянии датчика напряжения 12В;
– *+5.0 В* — информация о состоянии датчика напряжения 5В;
– *+3.3 В* — информация о состоянии датчика напряжения 3.3В;
– *+2.5 В* — информация о состоянии датчика напряжения 2.5В;
– *+1.8 В* — информация о состоянии датчика напряжения 1.8В;
– *+1.5 В* — информация о состоянии датчика напряжения 1.5В;
– *+1.2 В* — информация о состоянии датчика напряжения 1.2В;
– *+1.0 В* — информация о состоянии датчика напряжения 1В;
– *CPU* — информация о состоянии напряжения питания центрального процессора;
– *CPU Vcore* — информация о состоянии напряжения питания ядра центрального процессора;
– *Батарея RTC* — информация о состоянии напряжения батареи часов реального времени.

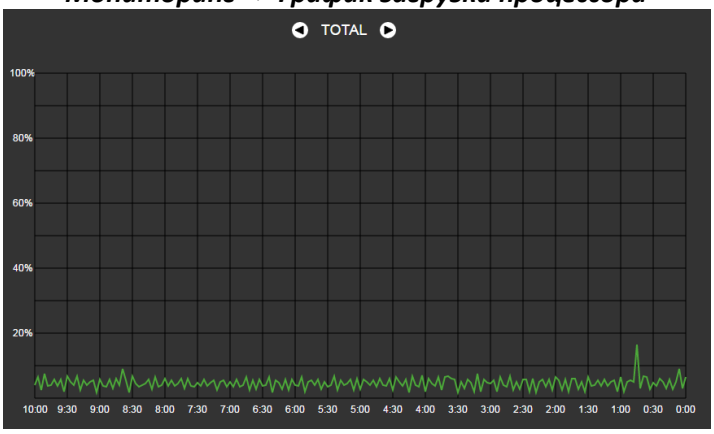
Текущая загрузка процессора:

– *USR* — процент использования процессорного времени пользовательскими программами;
– *SYS* — процент использования процессорного времени процессами ядра;
– *NIC* — процент использования процессорного времени программами с измененным приоритетом;
– *IDLE* — процент незадействованных процессорных ресурсов;
– *IO* — процент процессорного времени, потраченного на операции ввода/вывода;
– *IRQ* — процент процессорного времени, потраченного на обработку аппаратных прерываний;
– *SIRQ* — процент процессорного времени, потраченного на обработку программных прерываний.

4.1.2.2 График загрузки процессора

В разделе отображается информация о загрузке процессора в реальном времени (10 минутный интервал). Графики статистики строятся на основании усредненных данных за каждые 3 секунды работы устройства.

Мониторинг –> График загрузки процессора



Навигация между графиками мониторинга по отдельным параметрам осуществляется с помощью кнопок ◀ и ▶. Для облегчения визуальной идентификации все графики имеют различную цветовую

[1] Только для SBC-1000
[2] Только для SBC-2000 и SBC-3000

окраску.

- *TOTAL* — общий процент загрузки процессора;
- *IO* — процент процессорного времени, потраченного на операции ввода/вывода;
- *IRQ* — процент процессорного времени, потраченного на обработку аппаратных прерываний;
- *SIRQ* — процент процессорного времени, потраченного на обработку программных прерываний;
- *USR* — процент использования процессорного времени пользовательскими программами;
- *SYS* — процент использования процессорного времени процессами ядра;
- *NIC* — процент использования процессорного времени программами с измененным приоритетом.

4.1.2.3 Мониторинг SFP-модулей

В разделе отображаются индикация состояния и параметры оптической линии.

Мониторинг –> Мониторинг SFP-модулей

Мониторинг SFP модулей

SFP порт 0 статус	Наличие SFP модуля		Состояние сигнала	
	Модуль установлен		Сигнал установлен	
Температура, °C	Напряжение, В	Ток смещения TX, мА	Исходящая мощность, мВт	Входящая мощность, мВт
55.250	3.2936	12.184	0.2520	0.2152
SFP порт 1 статус	Наличие SFP модуля		Состояние сигнала	
Laser Fault	Модуль не установлен		Сигнал потерян	
Температура, °C	Напряжение, В	Ток смещения TX, мА	Исходящая мощность, мВт	Входящая мощность, мВт
N/A	N/A	N/A	N/A	N/A

- *SFP порт 0 статус, SFP порт 1 статус* — состояние оптического модуля:
  - *Наличие и SFP модуля* — индикация установки модуля (модуль установлен, модуль не установлен);
  - *Состояние сигнала* — индикация потери сигнала (сигнал потерян, в работе);
  - *Температура, °C* — температура оптического модуля;
  - *Напряжение, В* — напряжение питания оптического модуля, В;
  - *Ток смещения Tx, мА* — ток смещения при передаче, мА;
  - *Входящая мощность, мВт* — мощность сигнала на приеме, мВт;
  - *Исходящая мощность, мВт* — мощность сигнала на передачу, мВт.

4.1.2.4 Мониторинг front-портов коммутатора

В разделе отображается информация о физическом состоянии портов коммутатора — наличие линка, согласованная скорость на порту и режим передачи. Если порт сдвоеный (медный и оптический разъёмы), то рядом с номером порта будет указана пометка «(SFP)». Она пропадает, если сдвоенный порт активен и подключен медным кабелем.

Мониторинг –> Мониторинг front-портов коммутатора

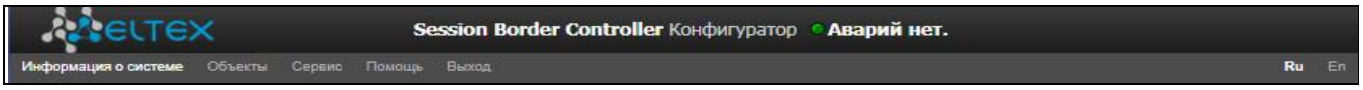
	Port 0	Port 1	Port 2	SFP 0	SFP 1
Состояние линка	DOWN	UP	UP	DOWN	DOWN
Скорость	N/A	1000M	1000M	N/A	N/A
Режим передачи	N/A	full-duplex	full-duplex	N/A	N/A
LACP группа	-	bond0 (UP)	bond0 (UP)	-	-
Статус порта LACP	-	Backup	Active	-	-
Принято байт	875955482 (835.4 MiB)	320 (0.0 MiB)	263649 (0.3 MiB)	0	0
ошибочных пакетов	0	0	0	0	0
отброшено пакетов	0	0	0	0	0
одноадресных пакетов	3488867	0	1669	0	0
широковещательных пакетов	1608922	5	1303	0	0
Передано байт	33413154 (31.9 MiB)	0	1872410 (1.8 MiB)	1018 (0.0 MiB)	1018 (0.0 MiB)
ошибочных пакетов	0	0	0	0	0
отброшено пакетов	0	0	0	0	0
одноадресных пакетов	240133	0	2420	0	0
широковещательных пакетов	12	0	0	15	15

- *Состояние линка* — состояние кабельного подключения на порту (активно/неактивно);
- *Скорость* — согласованная скорость на порту;
- *Режим передачи* — режим, используемый для передачи данных (half-/full-duplex);
- *LACP-группа* — здесь отображается LACP канал, в который входит порт и его статус (UP/DOWN)
- *Статус порта LACP* — режим, в котором находится порт (active/backup)
- *Принято байт* — накопительный счётчик принятых байт, включая различные виды принятых пакетов;
- *Передано байт* — накопительный счётчик переданных байт, включая различные виды переданных пакетов.

4.1.2.5 Сигнализация об авариях. Журнал аварийных событий

При возникновении аварии информация о ней выводится в заголовке Web-конфигуратора. Если активных аварий несколько, в заголовке web-конфигуратора выводится наиболее критичная в текущий момент авария.

При отсутствии аварий выводится сообщение *«Аварий нет».*



В меню *«Журнал аварийных событий»* выводится список аварийных событий, ранжированных по дате и времени. Также присутствует кнопка *«Очистить»*, которая удаляет из текущего журнала все информационные сообщения и нормализованные аварии.

Мониторинг –> Журнал аварийных событий

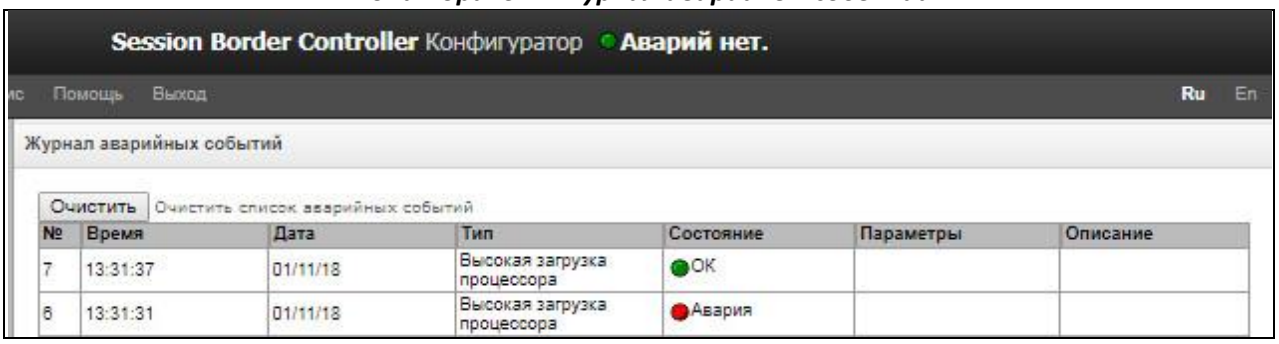


Таблица аварий

- *Очистить* — удалить существующую таблицу аварийных событий;
- *№* — порядковый номер аварии;
- *Время* — время возникновения аварии в формате ЧЧ:ММ:СС;
- *Дата* — дата возникновения аварии в формате ДД/ММ/ГГ;
- *Тип* — типы аварий приведены в таблице 18.

Таблица 18 — Типы аварий

Тип	**Расшифровка**
Конфигурация не прочитана	Ошибка чтения файла конфигурации
MSP-module lost	Потеря связи с модулем MSP
CDR-FTP	Ошибка передачи CDR файлов на FTP сервер. Возможны 3 уровня аварии — предупреждении, (накоплено 5 MB данных), авария (5-15 MB), критическая авария (15-30 MB)
Оперативная память заканчивается	Оперативная память заканчивается. Возможны 3 уровня аварии — предупреждение (осталось менее 25% свободной памяти), авария (менее 10%), критическая авария (менее 5%)
Регистрация абонента истекла	Регистрация абонента истекла
Перегрузка подсистемы sbc	Одна из подсистем SBC перегружена
Звонок запрещен	Поступил вызов, обслуживание которого запрещено
Регистрация абонента запрещена	Поступил запрос регистрации, обслуживание которого запрещено
Запуск ПО V.1.X.X.X	Программное обеспечение запущено
На ведомом устройстве установлена другая версия ПО	Устройства в резерве имеют разные версии ПО
Отсутствует подключение с ведомым	Отсутствует подключение с резервным устройством либо полностью, либо на одном из линков. Во втором случае в параметрах будет указано, на каком линке потеряна связь
Смена состояния в группе резерва	Произошло пересогласование устройств в резерве

- *Состояние* — статус аварийного состояния:
  - *критическая авария, мигающий красный индикатор* — авария, требующая незамедлительного вмешательства обслуживающего персонала, влияющие на работу устройства и оказания услуг связи;
  - *авария, красный индикатор* — некритическая авария, так же требуется вмешательство персонала;
  - *предупреждение, желтый индикатор* — авария, которая не влияет на оказание услуг связи;

- *информационное сообщение, серый индикатор* — не является аварией, предназначено для информирования о произошедшем событии;
- *ОК, зеленый индикатор* — авария устранена.

– *Параметры* — кодовое обозначение локализации аварии. Для аварии «Оперативная память заканчивается» имеет следующий вид:
  - [00:XX:YY], где XX — количество свободной памяти, YY — общее количество памяти.

– *Описание* — текстовое описание проблемы. Например, количество оставшейся оперативной памяти, номер абонента, у которого закончилась регистрация.

4.1.2.6 Мониторинг интерфейсов

Данный раздел предназначен для мониторинга состояния сетевых тегированных/нетегированных/VPN интерфейсов, а также просмотра подключенных к устройству VPN-пользователей.

Мониторинг –> Мониторинг интерфейсов

Сетевые интерфейсы

№	Ethernet	Имя сети	VLAN ID	DHCP	IP адрес	Broadcast	Маска сети
1	eth0	1	-	-	92.125.153.131	92.125.153.135	255.255.255.248
2	eth0:1	18	-	-	192.168.18.213	192.168.18.255	255.255.255.0
3	eth0:2	110	-	-	192.168.1.10	192.168.1.255	255.255.255.0

VPN/pptp интерфейсы

№	PPP-интерфейс	Имя сети	PPTPD IP	Имя пользователя	IP адрес	P-t-P	Маска сети

VPN/PPTP/L2TP пользователи

№	PPP-интерфейс	Имя пользователя	IP адрес	P-t-P	Маска сети

– *Ethernet* — имя интерфейса Ethernet;
– *Имя сети* — имя, с которым ассоциированы заданные сетевые настройки;
– *VLAN ID* — идентификатор виртуальной сети (для тегированного интерфейса);
– *DHCP* — статус использования протокола DHCP для получения сетевых настроек автоматически (требуется наличие DHCP сервера в сети оператора);
– *IP адрес, Маска сети, Broadcast* — сетевые настройки интерфейса (если не используется DHCP).

VPN/pptp интерфейсы

– *PPP-интерфейс* — имя интерфейса;
– *Имя сети* — имя, с которым ассоциированы заданные сетевые настройки;
– *PPTPD IP* — IP-адрес PPTP сервера для подключения;
– *Имя пользователя* — идентификатор пользователя;
– *IP адрес, P-t-P, Маска сети* — сетевые настройки интерфейса.

VPN/PPTP/L2TP пользователи

– *PPP-интерфейс* — имя интерфейса;
– *Имя пользователя* — идентификатор пользователя;
– *IP адрес, P-t-P, Маска сети* — сетевые настройки интерфейса.

4.1.2.7 Список абонентов

В данном подменю отображаются зарегистрированные через SBC-2000 абоненты.

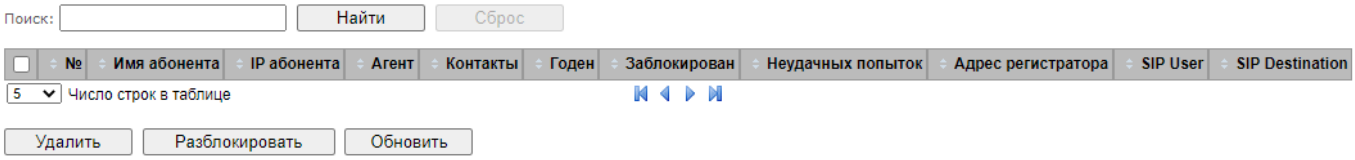
В поле *«Число строк в таблице»* производится настройка количества записей, выводимых на страницу. Информация о номере текущей страницы и общем количестве страниц выводится под таблицей с правой стороны. Для навигации используются стрелки , расположенные под таблицей, одинарная стрелка производит переход на одну страницу вперед/назад, двойная стрелка — в конец/начало массива

записей.

Записи могут иметь различные цвета в зависимости от состояния абонента:

- чёрный — обычный абонент, который нормально работает;
- красный — абонент заблокирован системой защиты от DoS;
- оранжевый — абонент был заблокирован, но сейчас разблокирован вручную, либо по истечении таймера защиты от DoS.

Мониторинг –> Список абонентов



- *Поиск* — проверка наличия номера абонента в списке зарегистрированных SIP-абонентов;
- № — порядковый номер абонента;
- *Имя абонента* — публичный номер зарегистрированного абонента, значение, переданное в заголовке To запроса REGISTER;
- *IP абонента* — IP-адрес, с которого на SBC пришёл запрос на регистрацию абонента;
- *Агент* — SIP-клиент абонента, значение, переданное в заголовке User-Agent запроса REGISTER;
- *Контакты* — частные адреса зарегистрированного абонента, значения, переданные в заголовках Contact запроса REGISTER;
- *Годен* — время, оставшееся до окончания действия регистрации. Для абонента, который был разблокирован, отображается время прощения, после которого будут сброшены счётчики блокировок для этого абонента;
- *Заблокирован* — состояние блокировки абонента. Если абонент заблокирован, то на запросы от него будет отправлен ответ 403 без обработки запроса;
- *Неудачных попыток* — количество попыток доступа, которые совершил абонент перед тем, как попасть в блокировку;
- *Адрес регистратора* — адрес и порт устройства, которое одобрило регистрацию абонента. Как правило, это адрес и порт Softswitch;
- *SIP User* — название SIP User, через который зарегистрировался абонент;
- *SIP Destination* — название SIP Destination, куда ушёл и откуда был одобрен запрос на регистрацию абонента.

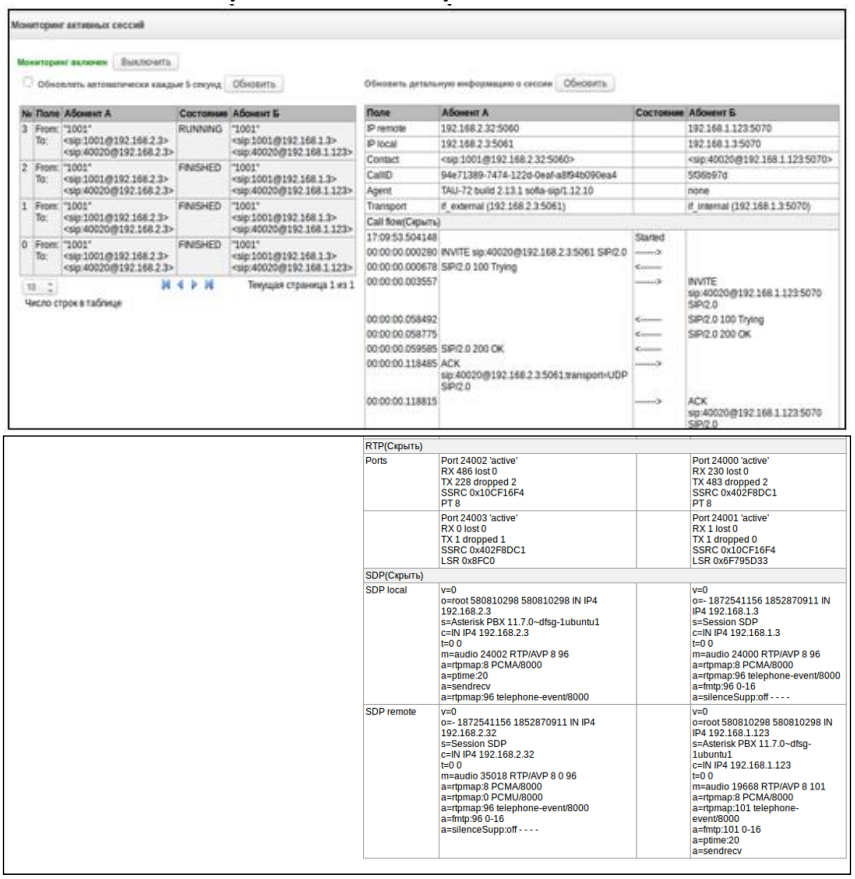
Под таблицей имеются следующие кнопки:

- *Удалить* — позволяет удалить абонента или группу абонентов из базы зарегистрированных абонентов. Для удаления абонентов необходимо установить флаг напротив нужной строки и нажать кнопку *«Удалить»;*
- *Разблокировать* — позволяет вывести абонента из состояния блокировки;
- *Обновить* — позволяет обновить список зарегистрированных абонентов.

4.1.2.8 Мониторинг активных сессий

Здесь отображаются активные сессии вызовов, установленные через SBC. Можно просмотреть сообщения сигнализации по каждому вызову и прохождение медиапотоков. Завершённые вызовы хранятся в мониторе в течение одной минуты.

Мониторинг –> Мониторинг активных сессий



– *Мониторинг включен/выключен* — текущий статус мониторинга. Кнопкой *«Включить/Выключить»* можно управлять состоянием монитора.

При включении мониторинга уже установившиеся вызовы не отобразятся, будут отображены только новые вызовы.

В меню расположены две таблицы мониторинга. В таблице слева отображается общая информация обо всех активных сессиях.

В поле *«Число строк в таблице»* производится настройка количества записей, выводимых на страницу. Информация о номере текущей страницы и общем количестве страниц выводится под таблицей с правой стороны. Для навигации используются стрелки, расположенные под таблицей, одинарная стрелка производит переход на одну страницу вперед/назад, двойная стрелка — в конец/начало массива записей.

Информация об активных сессиях (таблица слева)

– *Обновлять автоматически каждые 5 секунд* — при установленном флаге производится автоматическое обновление списка вызовов в окне монитора;
– *Обновить* — кнопка для ручного обновления списка вызовов в окне монитора при нажатии на кнопку;
– *Поле* — заголовки основных полей (например, From и To), которые передаются в ходе вызова;
– *Абонент А* — значения полей для абонента А;
– *Состояние* — текущее состояние сессии:
  - *RUNNING* — сессия активна и обрабатывается в данный момент;
  - *FINISHED* — обработка сессии завершена (такие сессии через некоторое время удаляются из мониторинга);
– *Абонент Б* — значения полей для абонента Б.

В правой таблице приводится детальная информация по вызову. Для её отображения необходимо нажать левой кнопкой мыши на записи об интересующем вызове в левой таблице.

Информация об активных сессиях (таблица справа)

- *Обновить детальную информацию о сессии* — по нажатию на кнопку *«Обновить»* обновляется текущее состояние сессии в мониторе;

- *Поле* — заголовки основных полей (например, From и To), которые передаются в ходе вызова;
- *Абонент А* — значения полей для абонента А;
- *Состояние* — текущее состояние сессии:
  - *RUNNING* — сессия активна и обрабатывается в данный момент;
  - *FINISHED* — обработка сессии завершена (такие сессии через некоторое время удаляются из мониторинга);
- *Абонент Б* — значения полей для абонента Б.

Список полей:

- *IP remote* — IP-адрес абонента, откуда или куда был направлен вызов;
- *IP local* — локальный IP-адрес, куда пришёл или откуда был отправлен вызов (IP local);
- *Contact* — значения полей Contact;
- *CallID* — идентификатор диалога из поля Call-ID;
- *Agent* — название SIP-клиента абонента из поля User-Agent;
- *Transport* — транспортный протокол, используемый при передаче.

Блок **Call Flow** в таблице отображает сигнализацию вызова на оба плеча с указанием общего времени начала вызова и времени отправки каждого сообщения относительно начала.

Блок **RTP** в таблице отображает информацию о медиапотоках между абонентами.

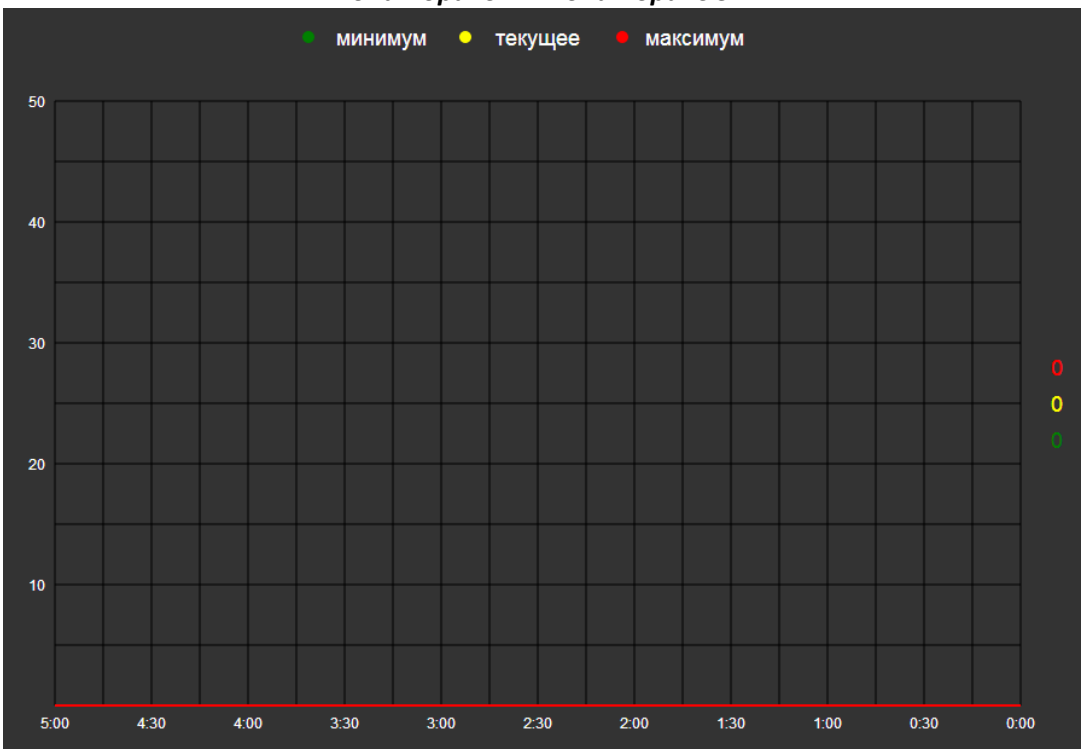
Блок **SDP в таблице** показывает, какими сообщениями SDP обменялись стороны вызова. SDP local — SDP, отправленный от SBC к абоненту; SDP remote — SDP, полученный от абонента.

Информацию в блоках возможно скрыть/развернуть, нажав левой кнопкой мыши на соответствующем подзаголовке.

4.1.2.9 Мониторинг SIP

В данном подменю на графике отображается максимальное, текущее и минимальное количество вызовов, совершенных за последние пять минут. График обновляется каждые три секунды.

Мониторинг –> Мониторинг SIP



4.1.2.10 Резервирование

Мониторинг –> Мониторинг SIP

Резервирование

Модель	Серийный номер	MAC-адрес	Состояние	Доступ	Действие	
SBC-2000	VI2A000409	A8:F9:4B:8A:64:97	master	local/global		
SBC-2000	VI2A000529	A8:F9:4B:8A:6D:8B	slave	local/global	Открыть Веб	Сделать мастером

- *Модель* — модель устройства;
- *Серийный номер* — серийный номер устройства;
- *MAC-адрес* — MAC-адрес устройства;
- *Состояние*:
  - master — устройство является ведущим;
  - slave — устройство является ведомым.
- *Доступ*:
  - local — устройство доступно по локальному линку;
  - global — устройство доступно по глобальному линку.
- *Открыть Веб* — открыть web-интерфейс ведомого устройства.

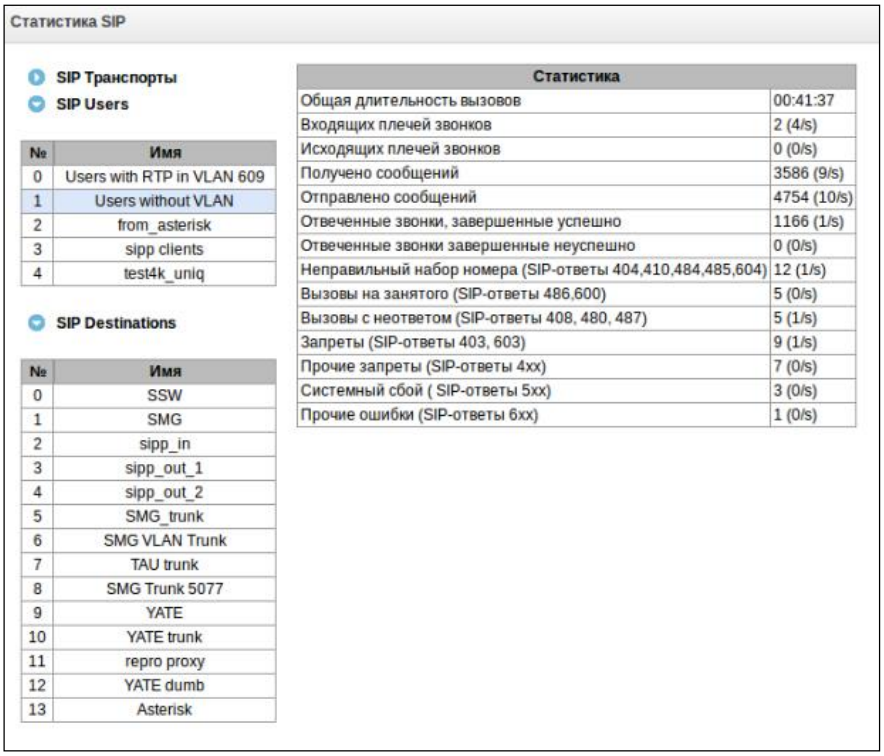
Подробнее о резервировании в ПРИЛОЖЕНИЕ В. ОБЕСПЕЧЕНИЕ ФУНКЦИИ РЕЗЕРВИРОВАНИЯ SBC.

4.1.2.11 Статистика SIP

В этом разделе отображается статистика по вызовам, накопленная SBC. Если статистика отключена, то включить её можно в разделе 4.1.1 Системные параметры. Слева находится список всех SIP транспортов, SIP Destination и SIP User, которые сконфигурированы на SBC. Справа находится таблица, в которой отображаются счётчики статистики. Для просмотра статистики следует слева выбрать интересующий

элемент и тогда в таблице справа будет отображена статистика по нему. Общую статистику по всей SBC можно посмотреть, выбрав в списке транспортов элемент "Сумма по всем транспортам". Любой список элементов можно свернуть или развернуть, кликнув на стрелку рядом с его названием.

Мониторинг –> Статистика SIP



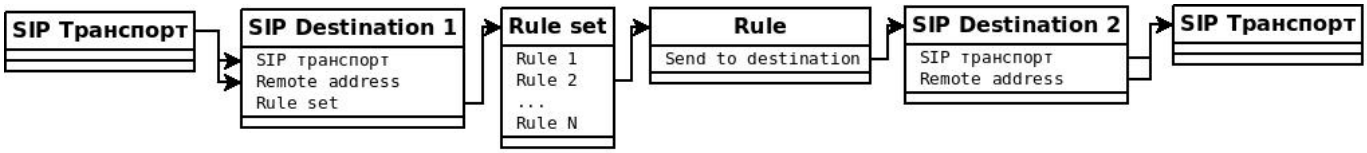
В таблице справа отображаются следующая информация:

- *Общая длительность вызовов* — общее время всех вызовов, которые прошли через выбранный элемент;
- *Входящих плечей звонков* — общее и текущее число входящих вызовов;
- *Исходящих плечей звонков* — общее и текущее число исходящих вызовов;
- *Получено сообщений* — сколько сообщений SIP пришло на элемент (учитываются все сообщения в диалогах, как запросы, так и ответы);
- *Отправлено сообщений* — сколько сообщений SIP отправлено (учитываются все сообщения в диалогах, как запросы, так и ответы);
- *Отвеченные звонки, завершенные успешно* — звонки, которые после разговора были завершены нормальным образом;
- *Отвеченные звонки, завершенные неуспешно* — звонки, которые завершились преждевременно с ошибкой в ходе разговора;
- *Неправильный набор номера (SIP-ответы 404,410,484,485,604)* — звонки, на которые был получен ответ, свидетельствующий о неверном или несуществующем номере;
- *Вызовы на занятого (SIP-ответы 486,600)* — звонки с ответом "занято";
- *Вызовы с неответом (SIP-ответы 408, 480, 487)* — вызовы, которые не были отвечены и завершились инициатором вызова или по таймауту;
- *Запреты (SIP-ответы 403, 603)* — вызов был отбит с причиной "запрет вызова";
- *Прочие запреты (SIP-ответы 4xx)* — другие вызовы с полученными на них SIP-ответами 400-499, не попавшие в категории выше;
- *Системный сбой (SIP-ответы 5xx)* — вызовы с полученными на них SIP-ответами 500-599;
- *Прочие ошибки (SIP-ответы 6xx)* — вызовы с полученными на них SIP-ответами 600-699

4.1.3 *Конфигурация SBC*

Функционально SBC можно описать как набор туннелей между различными (а может и внутри одной) подсетями, которые позволяют передавать как сигнальную, так и речевую (или иного рода) информацию между пользователями. Туннель с каждой стороны оканчивается SBC SIP-сервером, точкой выхода наружу для которого является SIP-транспорт. SBC осуществляет коммутацию сообщений между SBC SIP-серверами в соответствии с указанными правилами. В общем случае в одной подсети может быть создано несколько SBC SIP-серверов (например, туннели из одной подсети в разные). Речевая информация при этом может идти как в той же подсети, что и сигнальная (в которой находится SBC SIP-сервер), так и в отдельной. Для передачи речевой информации выделяется диапазон портов.

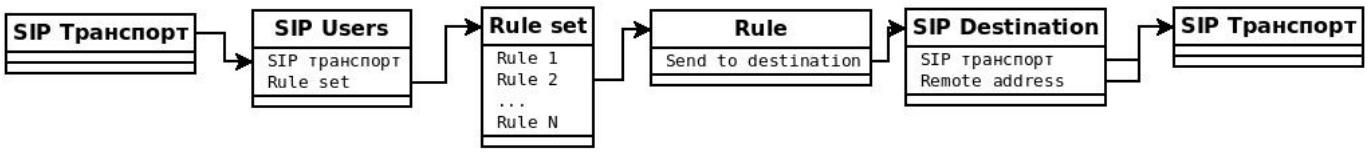
Общий алгоритм прохождения сигнализации через SBC



Рассмотрим прохождение вызова через SBC для двух оконечных узлов. Входящая сигнализация поступает на один из интерфейсов SBC. Производится поиск доступного входящего направления по транспорту, который привязан к интерфейсу и IP-адресу источника вызова. Далее согласно настройке направления, проверяется соответствующий набор правил. Если сигнализация соответствует хоть одному правилу из набора, где указано действие *«send to destination»* или *«send to trunk»,* вызов передаётся на направление, которое указано в правиле. В направлении, выбранном как исходящее, указывается транспорт, через который следует отправить сигнализацию дальше и remote address узла, куда следует отправлять сигнализацию.

Выше было рассмотрено прохождение вызова в одну сторону. Для обеспечения прохождения вызовов в обе стороны следует симметрично настроить направления, которые используются вместе — создать для них два набора правил, которые будут использоваться для направления вызовов, и указать соответствующие наборы в каждом направлении.

Прохождение сигнализации для абонентов, которые регистрируются через SBC



Когда абоненты регистрируются на регистраторе через SBC, прохождение сигнализации осуществляется аналогично описанному выше, за исключением того, что вызовы должны проходить через направления, настраиваемые в разделе *«SIP Users».* В этом случае поиск входящего направления производится только по привязанному к нему SIP-транспорту. Исходящим в этом случае будет направление, за которым находится регистратор.

Заметим, что при вызовах в сторону зарегистрированного абонента не требуется привязывать наборы правил к направлению, где указан адрес регистратора. SBC запомнит использовавшиеся направления для прошедших через него регистраций и будет на этом основании направлять пришедшую со стороны регистратора сигнализацию на абонента.

Общий алгоритм настройки SBC

1. Создать SIP-транспорт в тех подсетях, между которыми будет осуществляться коммутация.

2. Создать SIP-направления и пользователей, привязав к ним транспорты. Для направлений указать адреса оконечных узлов.

3. Создать наборы правил в соответствии с желаемой схемой коммутации вызовов между оконечными узлами.

4. Привязать наборы правил к входящим направлениям.

Для получения дополнительной информации рекомендуется к изучению ПРИЛОЖЕНИЕ Б. ПРИМЕРЫ НАСТРОЙКИ SBC.

4.1.3.1 SIP Транспорт

В данном подменю редактируется список транспорта, который будет служить точками входа в туннели. Может быть создано до 256 транспортов.

Для создания, редактирования и удаления интерфейсов используется меню *«Объекты» - «Добавить объект», «Объекты» - «Редактировать объект»* и *«Объекты» - «Удалить объект»*, а также кнопки:

- *«Добавить»;*
- *«Редактировать»;*
- *«Удалить»*.

Конфигурация SBC –> SIP-транспорт

SIP Транспорт

№	Имя	Сетевой интерфейс для сигнализации	Порт	Сетевой интерфейс для RTP
0	SipTransport00	Netlface#001 eth0 (192.168.114.134)	5060	Netlface#001 eth0 (192.168.114.134)

Добавить | Редактировать | Удалить

Конфигурация SBC –> SIP-транспорт –> «Добавить» или «Редактировать»

SIP transport 0	
Имя	SipTransport00
Сетевой интерфейс для сигнализации	[0] Netlface#001 (eth0 192.168.114.134
Порт	5060
Сетевой интерфейс для RTP	[0] Netlface#001 (eth0 192.168.114.134

Применить | Отменить

Параметры транспорта

- *Имя* — произвольное имя для идентификации, удобное для оператора;
- *Сетевой интерфейс для сигнализации* — сетевой интерфейс для приёма сигнализации;
- *Порт* — порт для приёма сигнализации;
- *Сетевой интерфейс для RTP* — сетевой интерфейс, на котором будет осуществляться передача медиапотоков.

4.1.3.2 SIP Destination

В этом подменю редактируется список направлений для приёма и отправки вызовов на конечные узлы. Может быть создано до 256 направлений.

Для создания, редактирования и удаления интерфейсов используется меню *«Объекты» - «Добавить объект», «Объекты» - «Редактировать объект»* и *«Объекты» - «Удалить объект»*, а также кнопки:

- *«Добавить»;*
- *«Редактировать»;*
- *«Удалить».*

Конфигурация SBC –> SIP-Destination

SIP Destination

№	Имя	SIP транспорт	Remote address	Адаптация	Транспортный протокол	Rule set
0	SipDestination00	SipTransport00		-	UDP-only	-

Добавить | Редактировать | Удалить

Конфигурация SBC –> SIP- Destination –> «Добавить» или «Редактировать»

SIP destination 2	
Имя	SipDestination02
SIP транспорт	Не выбран
Remote address	
Транспортный протокол	UDP-only
Формат заголовков SIP	Full
Адаптация	-
Передавать контакт без изменения	☐
Передавать домен из заголовков FROM и TO	☐
Таймаут ожидания RTP-пакетов, с	☐ 0
Таймаут ожидания RTP-пакетов после получения Silence-Suppression (множитель)	X 0
Таймаут ожидания RTP-пакетов в режиме удержания вызова (sendonly, inactive) (множитель)	X 0
Таймаут ожидания RTCP-пакетов, с	☐ 0
Контроль IP:Port источника RTP	☐
Запрашиваемый период контроля сессии (Session Expires, RFC 4028), с	☐ 0
Период проверки рабочего сервера, с (после завершения предыдущей транзакции OPTIONS)	60
Период проверки нерабочего сервера, с (после завершения предыдущей транзакции OPTIONS)	20
Входящее максимальное значение CPS	0
Исходящее максимальное значение CPS	0

Параметры направления

- *Имя* — произвольное имя для идентификации (удобное для оператора);
- *SIP Транспорт* — транспорт, который будет использоваться для приёма вызовов на направление и отправки вызовов с направления.
- *Remote Address* — адрес удалённого узла, который связан с данным направлением. Вызовы на направление с IP-адреса, отличного от указанного в этом поле, будут отвергнуты. Вызовы с направления будут отправляться на адрес, указанный в этом поле.
- *Транспортный протокол* — выбор протокола транспортного уровня, используемого для приема и передачи сообщений SIP:
  - *TCP-prefer* — прием по UDP и TCP. Отправка по TCP. В случае если не удалось установить соединение по TCP, отправка производится по UDP;
  - *UDP-prefer* — прием по UDP и TCP. Отправка пакетов более 1300 байт по TCP, менее 1300 байт — по UDP;
  - *UDP-only* — использовать только UDP протокол;
  - *TCP-only* — использовать только TCP протокол;
- *Формат заголовков SIP* — определяет, в каком формате передавать заголовки SIP:
  - *full* — использовать обычный (длинный) формат заголовков;
  - *compact* — использовать короткий формат заголовков;
- *Адаптация* — настройка предназначена для адаптации взаимодействия через SBC шлюзов различных производителей с программным коммутатором ESCC-10.
  - *HUAWEI-EchoLife* — данная адаптация позволяет принять сигнал Flash от шлюза методом re-INVITE и передать его в сторону программного коммутатора методом SIP INFO;
  - *Iskratel SI3000* — при использовании данной адаптации SBC не подменяет поле contact в запросах, передаваемых в сторону программного коммутатора. При вызове на абонента в Request-URI URI-parameters не анализируются, анализируются только номер абонента и его адрес;

- *HUAWEI-SoftX3000* — при использовании данной адаптации SBC не подменяет поле contact в запросах, передаваемых в сторону программного коммутатора. В ответе 200OK на запрос REGISTER считается, что URI, содержащий дефолтный порт 5060, равен URI, не содержащему его;
- *ZTE Softswitch* — при использовании данной адаптации SBC не подменяет поле *«contact»* в запросах, передаваемых в сторону программного коммутатора. При вызове на абонента в Request-URI URI-parameters не анализируются, анализируются только номер абонента и его адрес. Также игнорируются нарушения последовательности origin version в SDP;
- *Nortel* — при использовании данной адаптации SBC игнорирует нарушения последовательности origin version в SDP.
- *MTA M-200* — при использовании данной адаптации SBC при поступлении входящих вызовов не проверяет порт, указанный в Request URI.

- *Передавать контакт без изменения* — при использовании данной опции SBC не подменяет поле contact в запросах, передаваемых на второе плечо;

- *Передавать домен из заголовков FROM и TO* — при использовании данной опции SBC в исходящее плечо прокидывает домен, который пришел в полях FROM, TO. В случае, если пришел IP-адрес, SBC подменяет его на свой IP;

- *Таймаут ожидания RTP-пакетов* — функция контроля состояния разговорного тракта по наличию RTP-трафика от взаимодействующего устройства. Диапазон допустимых значений от 10 до 300 секунд. При снятом флаге контроль RTP выключен, при установленном — включен. Контроль осуществляется следующим образом: если в течение данного таймаута от встречного устройства не поступает ни одного RTP-пакета и последний пакет не был пакетом подавления пауз, то вызов отбивается;

- *Таймаут ожидания RTP-пакетов после получения Silence-Suppression (множитель)* — таймаут ожидания RTP-пакетов при использовании опции подавления пауз. Диапазон допустимых значений от 1 до 30. Коэффициент является множителем и определяет, во сколько раз значение данного таймаута больше, чем «*Таймаут ожидания RTP-пакетов»*. Контроль осуществляется следующим образом: если в течение данного времени от встречного устройства не поступает ни одного RTP пакета и последний пакет был пакетом подавления пауз, то вызов отбивается;

- *Таймаут ожидания RTP-пакетов в режиме удержания вызова (множитель)* — таймаут ожидания RTP-пакетов от взаимодействующего с данным SIP-сервером SBC в режимах, когда разговорный канал работает только на передачу либо неактивен. Диапазон допустимых значений от 1 до 30. Коэффициент является множителем и определяет, во сколько раз значение данного таймаута больше, чем «*Таймаут ожидания RTP-пакетов»*. Контроль осуществляется следующим образом: если в течение данного времени от встречного устройства не поступает ни одного RTP пакета и разговорный канал работает только на передачу либо неактивен, то вызов отбивается;

- *Таймаут ожидания RTCP пакетов* — функция контроля состояния разговорного тракта, принимает значения из диапазона 10-300 с. Время, в течение которого ожидаются пакеты протокола RTCP со встречной стороны. При отсутствии пакетов в заданном периоде времени, в случае, если встречной стороной ранее был отправлен хотя бы один RTCP пакет, установленное соединение разрушается;

- *Контроль IP:Port источника RTP* — при включении опции, SBC следит, чтобы прохождение медиа-потока от встречной стороны осуществлялось именно с тех IP и порта, которые указаны в SDP. Медиа-поток, пришедший не с указанного IP или порта, будет отброшен;

- *Запрашиваемый период контроля сессии (Session Expires, RFC 4028), с* — при установленном флаге поддерживаются таймеры SIP-сессий (RFC 4028). Обновление сессии поддерживается путем передачи запросов re-INVITE в течение сессии. Данный параметр определяет период времени в секундах, по истечении которого произойдет принудительное завершение сессии, в случае, если сессия не будет вовремя обновлена (от 90 до 64800 с, рекомендуемое значение — 1800 с);

Контроль ожидания RTP, RTCP пакетов, а также использование RFC 4028 предназначено для того, чтобы исключить зависание разговорных сессий, установленных через SBC, в случае возникновения проблем с прохождением пакетов на сети оператора. Все неактивные сессии через соответствующие таймауты будут закрыты.

– *Период проверки рабочего сервера, с (после завершения предыдущей транзакции OPTIONS)* — интервал времени, через который контрольный запрос OPTIONS будет отправлен на SIP-сервер в случае, если на предыдущий запрос OPTIONS было получено подтверждение;

– *Период проверки нерабочего сервера, с (после завершения предыдущей транзакции OPTIONS)* — интервал времени, через который контрольный запрос OPTIONS будет отправлен на SIP-сервер в случае, если на предыдущий запрос OPTIONS не было получено подтверждение;

– Входящее максимальное значение CPS — количество вызовов в секунду, которое может быть принято на SIP Destination. Диапазон допустимых значений от 0 до 100, 0 — отключение опции;

– Исходящее максимальное значение CPS — количество вызовов в секунду, которое может быть отправлено на SIP Destination. Диапазон допустимых значений от 0 до 100, 0 — отключение опции.

Входящая связь

– *Rule set*— применить для входящей сигнализации набор правил, созданный в меню «Rule set» (подробнее в разделе 4.1.3.5 Rule set);

– Ответить на OPTIONS — при использовании данной опции SBC самостоятельно отвечает на запрос OPTIONS в случае, если Rule в Rule set, отвечающий за отправку OPTIONS, отсутствует.

Входящая связь	
Rule set	Нет
Ответить на OPTIONS	☐

Исходящая связь

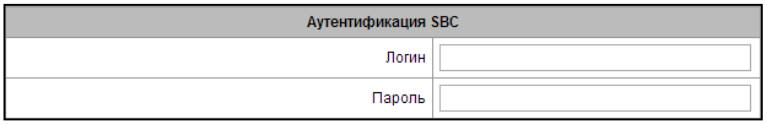
– *Конвертировать RFC2833 Flash в SIP INFO* — преобразовывает сигнал Flash, принятый методом RFC 2833, в запрос INFO application/hook-flash протокола SIP и передает его во взаимодействующий канал;

– *Разрешить перенаправление* — разрешает обработку ответов 302. При отключенной настройке при получении со стороны Б ответа 302 SBC завершит вызов. При включении опции SBC будет обрабатывать ответы 302 следующим образом: получив контакт абонента С, SBC попытается отправить вызов ему, уведомив сторону А о перенаправлении вызова ответом 181. Если же в контакте содержится адрес самого SBC, то он прозрачно пробросит сообщение 302 на сторону А, указав в поле Contact адрес стороны А;

Исходящая связь	
Конвертировать RFC2833 Flash в SIP INFO	☐
Разрешить перенаправление	☐

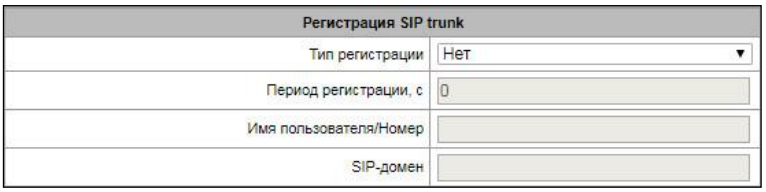
При активации настройки для обеспечения корректности работы перенаправлений будут отключены встроенные правила firewall для SIP transport, привязанного к SIP destination, на котором включается опция! Если транспорт используется на других SIP destination, то для них встроенные правила Firewall них тоже будут отключены. Рекомендуется выделять отдельный SIP transport для тех SIP destination, с которых разрешена обработка перенаправлений, либо, при необходимости, ограничить доступ вручную (подробнее в разделе 4.1.8.5).

Аутентификация SBC



- *Логин* — логин для аутентификации на вышестоящем SIP-сервере;
- *Пароль* — пароль для аутентификации на вышестоящем SIP-сервере. Данные аутентификации используются только для авторизации запросов, формируемых самим SBC, например, это могут быть запросы re-INVITE, формируемые SBC при использовании функции timer RFC 4028, аутентификация на взаимодействующем сервере, регистрация на взаимодействующем сервере (при типе регистрации UAC), аутентификации запросов от взаимодействующего сервера (при типе регистрации UAS).

Регистрация SIP trunk

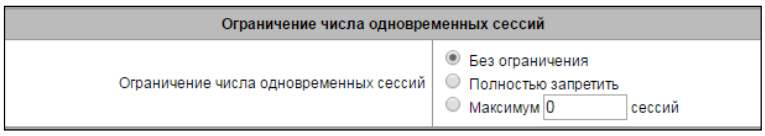


- *Тип регистрации* — данная настройка задает направление регистрации:
  - *UAC* — в данном случае SBC по транку будет регистрироваться на взаимодействующем сервере регистрации. При этом при отсутствии регистрации направление будет считаться недоступным, и в него не будут отправляться вызовы (но приниматься будут всегда);
  - *UAS* — в данном случае взаимодействующее по транку устройство будет регистрироваться на SBC при условии, что будет получено подтверждение регистрации от выбранного по *Rule set* сервера. Также SBC будет аутентифицировать все запросы от взаимодействующего сервера. Настройка в поле *Remote Address* при этом не применяется, используется адрес, полученный в контакте при регистрации.

При отсутствии регистрации в любом режиме направление будет считаться недоступным, и с него не будут отправляться вызовы (но приниматься будут всегда);

- *Период регистрации, с* — период обновления регистрации на сервере (используется при типе регистрации UAC);
- *Имя пользователя/Номер* — имя/номер, с которым транк SBC регистрируется на сервере регистрации (при типе регистрации UAC);
- *SIP-домен* — доменное имя, с которым транк SBC регистрируется на сервере регистрации (при типе регистрации UAC), либо доменное имя, с которым встречное устройство аутентифицируется на SBC через транк (при типе регистрации UAS);

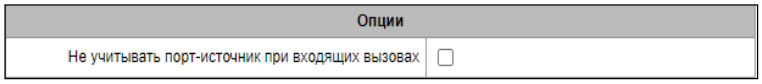
Ограничение числа одновременных сессий



- *Без ограничения* — количество сессий не ограничено;
- *Полностью запретить* — полный запрет сессий;
- *Максимум N сессий,* где N — количество одновременных сессий.

Опции

– *Не учитывать порт-источник при входящих вызовах* — не проверять для входящих вызовов адрес порта, с которого пришёл запрос. Если опция не активна, то для входящих вызовов строго проверяется, что вызов пришёл с адреса и порта, указанных в настройке remote address. Если опция активна, то поиск и выбор SIP Destination производится сначала по тем destination, где опции нет, а затем будет выбираться один из тех, где опция активирована и которые проходят по параметру IP/hostname в настройке remote address.



Пример:

На SBC сконфигурировано четыре SIP Destination с такими параметрами remote address:

Имя	remote address	Состояние опции
Dest1	192.0.2.1:5060	отключена
Dest2	192.0.2.1:5061	отключена
Dest3	192.0.2.1:5062	включена

Запросы с адресов 192.0.2.1:5060..192.0.2.1:5062 будут обработаны в destination Dest1..Dest3 соответственно своим адресам, поскольку они точно совпадают с тем, что настроено в remote address.

Запрос с адреса 192.0.2.1:5090 попадёт в Dest3, поскольку запрос не подходят ни под одну настройку remote address, но на Dest3 игнорируется порт. Аналогично все запросы с портов, не входящих в 5060..5062 попадут также в Dest3.

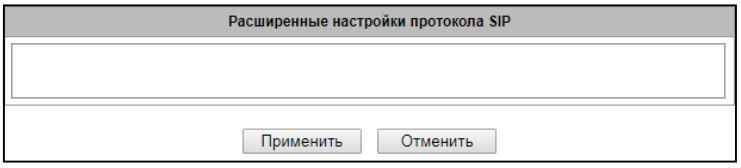
Не рекомендуется создавать несколько SIP Destination с одинаковыми IP-адресами и активированными настройками игнорирования порта, т.к. нельзя предсказать, в каком из них будет в итоге обработан запрос.

Расширенные настройки протокола SIP

В поле находятся расширенные настройки протокола SIP. При помощи данных настроек можно корректировать поля сообщений SIP по заданным правилам.

Формат заполнения поля

[sipheader:ИМЯ_ЗАГОЛОВКА=операция],[sipheader:...],...



Где:

– *Операции — disable, insert или правило модификации;*
– *ИМЯ_ЗАГОЛОВКА — регистронезависимый параметр, например, Accept = accept = ACCEPT. В иных параметрах регистр имеет значение.*

Правила модификации

Правила модификации описываются символами:

– *$ — оставить последующий текст;*
– *! — удалить оставшийся текст;*
– *+(АБВ) — добавить указанный текст;*
– *-(АБВ) — удалить указанный текст.*

Примеры реализации правил операции приведены в таблице ниже.

Таблица 19 — Примеры реализации правил операции

Операция	Исходный заголовок	Правило	Результат
Не отправлять заголовок	Accept: application/SDP	[sipheader:accept=disable]	
Передать без изменений заголовок из первого плеча	Дополнительные заголовки на первом плече: P-Asserted-Identity: username@domain Subject: Test call	[sipheader:[СПИСОК_СООБЩЕНИЙ]: [МАСКА_ЗАГОЛОВКА]=transit] [sipheader:[МАСКА_ЗАГОЛОВКА]=transit] В сообщениях INVITE и 200: [sipheader:INVITE,200:Subject=transit] В любых сообщениях: [sipheader:Subject=transit]	На втором плече появится заданный заголовок: Subject: Test call
Передать без изменений группу заголовков из первого плеча	Дополнительные заголовки на первом плече: P-Asserted-Identity: sip:username@domain P-Called-Party-ID: sip:username@domain Privacy: id Subject: Test call	[sipheader:P-*=transit] Обратите внимание, что такое правило: [sipheader:*=transit] работать не будет, поскольку символ * может заменять только часть имени.	На втором плече появятся заданные заголовки: P-Asserted-Identity: sip:username@domain P-Called-Party-ID: sip:username@domain
Вставить заготовок		[sipheader:insert[СПИСОК_ЗАГОЛОВКОВ]: RemoteIp=+(ТЕКСТ)] Во всех запросах: [sipheader:insert:RemoteIp=+(example.SBC)] Только в запросе INVITE: [sipheader:insert,INVITE:RemoteIp=+(example.SBC)] Только в указанные запросы (например, INVITE и ACK): [sipheader:insert,INVITE,ACK:RemoteIp=+(example.SBC)]	RemoteIp:example.SBC
Добавить текст в начало	Accept: application/SDP	[sipheader:accept=+(application/ISUP,)$]	Accept: application/ISUP,application/SDP
Добавить текст в конец	Accept: application/SDP	[sipheader:accept=$+(,application/ISUP)]	Accept: application/SDP,application/ISUP
Удалить текст	Accept: application/SDP,application/ISUP	[sipheader:accept=-(application/SDP,)$]	Accept: application/ISUP
Удалить, начиная с указанного текста	Accept: application/SDP,text/plain	[sipheader:accept=-(,text)!]	Accept: application/SDP
Заменить текст полностью	Accept: application/SDP	[sipheader:accept=+(application/ISUP)!]	Accept: application/ISUP

Заменить текст	Accept: application/SDP,text/plain	[sipheader:accept=-(SDP)+(ISUP)$]	Accept: application/ISUP,text/plain
Заменить текст, отбросив данные в конце	Accept: application/SDP,text/plain	[sipheader:accept=-(SDP)+(ISUP)!]	Accept: application/ISUP
Пример комплексной модификации	From: <sip:who@host>;tag=aBc	[sipheader:from=+(DISPLAY)-(who)+(12345)-(>)+(;user=phone>)$+(;line=abc)]	From: DISPLAY <sip:12345@host;user=phone>;tag=aBc;line=abc

Пример

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

В данном примере все сообщения SIP, отправляемые устройством через данный SIP-интерфейс, будут следовать без полей *Accept* и *user-agent.*

Список обязательных полей сообщений SIP, которые не могут быть модифицированы: via, from, to, call-id, cseq, contact, content-type, content-length.

4.1.3.3 SIP Users

В данном меню настраиваются направления для приёма и маршрутизации вызовов для SIP-пользователей, которые будут отправлять вызовы и регистрации через SBC. Может быть создано до 256 users.

Для создания, редактирования и удаления интерфейсов используется меню *«Объекты» - «Добавить объект», «Объекты» - «Редактировать объект»* и *«Объекты» - «Удалить объект»*, а также кнопки:

- *«Добавить»;*
- *«Редактировать»;*
- *«Удалить»*.

Конфигурация SBC –> SIP-Users

SIP Users

№	Имя	SIP транспорт	Профиль RADIUS	Транспортный протокол	Абоненты за NAT	Время хранения соединения на NAT, с	SIP домен	Rule set
0	SipUser00	SipTransport00	Не выбран	UDP-only	-	-		-

Добавить | Редактировать | Удалить

Конфигурация SBC –> SIP- Users –> «Добавить» или «Редактировать»

SIP user 6

Имя	SipUser06
SIP транспорт	Не выбран
Rule set	Нет
Транспортный протокол	UDP-only
Формат заголовков SIP	Full
Профиль RADIUS	Не выбран
Передавать контакт без изменения	
Таймаут ожидания RTP-пакетов, с	0
Таймаут ожидания RTP-пакетов после получения Silence-Suppression (множитель)	x0
Таймаут ожидания RTP-пакетов в режиме удержания вызова (sendonly, inactive) (множитель)	x0
Таймаут ожидания RTCP-пакетов, с	0
Контроль IP:Port источника RTP	
Запрашиваемый период контроля сессии (Session Expires, RFC 4028), с	0
SIP домен	
Абоненты за NAT	
Время хранения соединения на NAT, с	0
Не использовать подмену SDP mode для пробоев КПВ через NAT	
Минимальное время регистрации, с	120

Параметры пользовательского направления

- *Имя* — произвольное имя для идентификации (удобное для оператора);
- *SIP Транспорт* — транспорт, который будет использоваться для приёма вызовов на направление и отправки вызовов с направления;
- *Транспортный протокол* — выбор протокола транспортного уровня, используемого для приема и передачи сообщений SIP:
  - *TCP-prefer* — прием по UDP и TCP. Отправка по TCP. В случае если не удалось установить соединение по TCP, отправка производится по UDP;
  - *UDP-prefer* — прием по UDP и TCP. Отправка пакетов более 1300 байт по TCP, менее 1300 байт — по UDP;
  - *UDP-only* — использовать только UDP протокол;
  - *TCP-only* — использовать только TCP протокол;
- *Формат заголовков SIP* — определяет, в каком формате передавать заголовки SIP:
  - *full* — использовать обычный (длинный) формат заголовков;
  - *compact* — использовать короткий формат заголовков;
- *Профиль RADIUS* — профиль RADIUS для аутентификации и авторизации входящих вызовов (подробнее в разделе 4.1.9);

- *Передавать контакт без изменения* — при использовании данной опции SBC не подменяет поле contact в запросах, передаваемых в сторону программного коммутатора;

- *Таймаут ожидания RTP-пакетов* — функция контроля состояния разговорного тракта по наличию RTP-трафика от взаимодействующего устройства. Диапазон допустимых значений от 10 до 300 секунд. При снятом флаге контроль RTP выключен, при установленном — включен. Контроль осуществляется следующим образом: если в течение данного таймаута от встречного устройства не поступает ни одного RTP-пакета и последний пакет не был пакетом подавления пауз, то вызов отбивается;

- *Таймаут ожидания RTP-пакетов после получения Silence-Suppression (множитель)* — таймаут ожидания RTP-пакетов при использовании опции подавления пауз. Диапазон допустимых значений от 1 до 30. Коэффициент является множителем и определяет, во сколько раз значение данного таймаута больше, чем «*Таймаут ожидания RTP-пакетов»*. Контроль осуществляется следующим образом: если в течение данного времени от встречного устройства не поступает ни одного RTP пакета и последний пакет был пакетом подавления пауз, то вызов отбивается;

- *Таймаут ожидания RTP-пакетов в режиме удержания вызова (множитель)* — таймаут ожидания RTP-пакетов от взаимодействующего с данным SIP-сервером SBC в режимах, когда разговорный канал работает только на передачу либо неактивен. Диапазон допустимых значений от 1 до 30. Коэффициент является множителем и определяет, во сколько раз значение данного таймаута больше, чем «*Таймаут ожидания RTP-пакетов»*. Контроль осуществляется следующим образом: если в течение данного времени от встречного устройства не поступает ни одного RTP пакета и разговорный канал работает только на передачу либо неактивен, то вызов отбивается;

- *Таймаут ожидания RTCP пакетов* — функция контроля состояния разговорного тракта, принимает значения из диапазона 10-300 с. Время, в течение которого ожидаются пакеты протокола RTCP со встречной стороны. При отсутствии пакетов в заданном периоде времени, в случае, если встречной стороной ранее был отправлен хотя бы один RTCP пакет, установленное соединение разрушается;

- *Контроль IP:Port источника RTP* — при включении опции, SBC следит, чтобы прохождение медиа-потока от встречной стороны осуществлялось именно с тех IP и порта, которые указаны в SDP. Медиа-поток, пришедший не с указанного IP или порта, будет отброшен;

- *Запрашиваемый период контроля сессии (Session Expires, RFC 4028), с* — при установленном флаге поддерживаются таймеры SIP-сессий (RFC 4028). Обновление сессии поддерживается путем передачи запросов re-INVITE в течение сессии. Данный параметр определяет период времени в секундах, по истечении которого произойдет принудительное завершение сессии, в случае если сессия не будет вовремя обновлена (от 90 до 64800 с, рекомендуемое значение — 1800 с);

Контроль ожидания RTP, RTCP пакетов, а также использование RFC 4028 предназначено для того, чтобы исключить зависание разговорных сессий, установленных через SBC, в случае возникновения проблем с прохождением пакетов на сети оператора. Все неактивные сессии через соответствующие таймауты будут закрыты.

- *SIP-домен* — доменное имя, с которым транк SBC регистрируется на сервере регистрации (при типе регистрации UAC), либо доменное имя, с которым встречное устройство регистрируется на SBC через транк (при типе регистрации UAS);

- *Абоненты за NAT* — установить флаг, если необходимо подключение абонентов, находящихся в частной сети (находящихся за NAT). Также данная настройка позволяет передавать сообщения протокола SIP симметрично (на порт, с которого был принят запрос) в случае, если клиент в инициирующем запросе не использовал параметр RPORT;

– *Время хранения соединения на NAT, с* — время хранения соответствия портов для сигнального трафика, также ограничивает параметр expires для регистрации SIP-абонентов;

– *Не использовать подмену SDP mode для проброса КПВ через NAT* — по умолчанию, начиная с версии ПО 1.9.2, SBC для обеспечения корректного проключения медии в предответном состоянии (КПВ, голосовые сообщения) для клиентов за NAT будет заявлять в SDP режим sendrecv, даже если встречная сторона согласовала sendonly или recvonly. Опция позволяет отключить такое поведение и анонсировать в SDP то, что заявила встречная сторона;

– *Минимальное время регистрации, с* — минимальное время регистрации, допустимое для абонента. Может принимать значения от 60 до 65535 секунд. Обратите внимание, что значения менее 120 с могут повлиять на производительность.

Ограничение числа одновременных сессий

– *От зарегистрированных абонентов* — ограничение числа одновременных сессий для зарегистрированных абонентов:
  – *Без ограничения* — количество сессий не ограничено;
  – *Полностью запретить* — полный запрет сессий;
  – *Максимум N сессий, где N* — количество одновременных сессий;

Ограничение числа одновременных сессий	
От зарегистрированных абонентов	(•) Без ограничения ( ) Полностью запретить ( ) Максимум 0 сессий
От незарегистрированных абонентов	(•) Без ограничения ( ) Полностью запретить ( ) Максимум 0 сессий

– *От незарегистрированных абонентов* — ограничение числа одновременных сессий для незарегистрированных абонентов:
  – *Без ограничения* — количество сессий не ограничено;
  – *Полностью запретить* — полный запрет сессий;
  – *Максимум N сессий, где N* — количество одновременных сессий.

Входящая связь

– Rule set — применить для входящей сигнализации набор правил, созданный в меню *«Rule set»* (подробнее в разделе 4.1.3.5 Rule set);

Исходящая связь

– *Конвертировать RFC2833 Flash в SIP INFO* — преобразовывает сигнал Flash, принятый методом RFC2833, в запрос INFO application/hook-flash протокола SIP и передает его во взаимодействующий канал;

Исходящая связь	
Конвертировать RFC2833 Flash в SIP INFO	☐
Разрешить перенаправление	☐

– *Разрешить перенаправление* — разрешает обработку ответов 302. При отключенной настройке при получении со стороны Б ответа 302 SBC завершит вызов. При включении опции SBC будет обрабатывать ответы 302 следующим образом: получив контакт абонента С, SBC попытается отправить вызов ему, уведомив сторону А о перенаправлении вызова ответом 181. Если же в контакте содержится адрес самого SBC, то он прозрачно пробросит сообщение 302 на сторону А, указав в поле Contact адрес стороны А.

Расширенные настройки протокола SIP

Работают аналогично настройкам в SIP Destination, смотрите настройки протокола SIP в разделе 4.1.3.2.

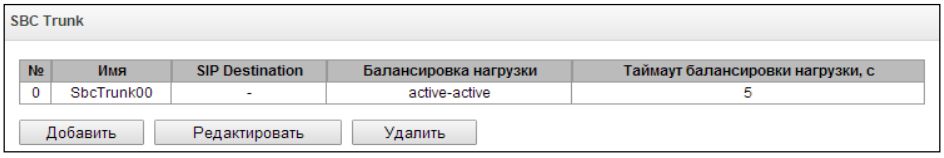
4.1.3.4 SBC Trunk

В данном подменю производится настройка транков для целей распределения нагрузки или резервирования каналов. Может быть создано до 256 транков.

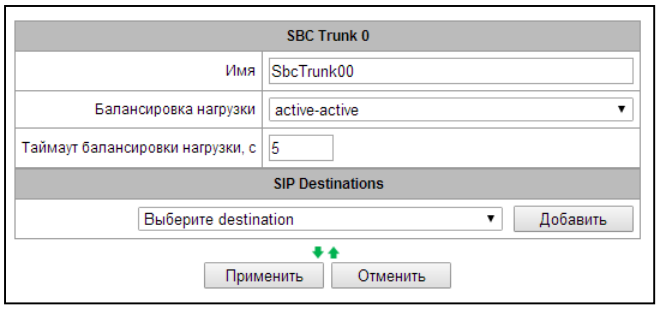
Для создания, редактирования и удаления записей используется меню *«Объекты» - «Добавить объект», «Объекты» - «Редактировать объект»* и *«Объекты» - «Удалить объект»*, а также кнопки:

- *«Добавить»;*
- *«Редактировать»;*
- *«Удалить»*.

Конфигурация SBC –> SBC Trunk



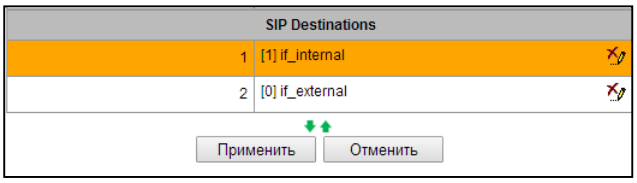
Конфигурация SBC –> SBC Trunk –> «Добавить» или «Редактировать»



Параметры транков

- *Имя* — произвольное имя для идентификации (удобное для оператора);
- *Балансировка нагрузки* — тип разделения нагрузки между SIP-серверами:
  - *Active-active* — нагрузка балансирует между SIP-серверами в процентном соотношении 50/50;
  - *Active-backup* — вся нагрузка передается через первый SIP-сервер. При недоступности первого SIP-сервера нагрузка будет направлена на второй SIP-сервер;
- *Таймаут балансировки нагрузки, с* — время, через которое вызов будет направлен на резервный SIP-сервер в случае, если сервер, на который вызов уже был направлен, оказался недоступен;

В блоке ***SIP Destinations*** выбираются направления для добавления в транк. Также возможно удалить направление из транка, нажав иконку (*«Удалить»*) в выбранной строке. Зеленые стрелки под списком позволяют перемещать выделенные записи в таблице, настраивая порядок (приоритет) созданных направлений.



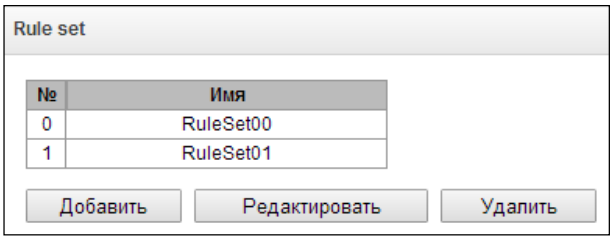
4.1.3.5 Rule set

В данном разделе настраиваются правила коммутации вызовов через SBC. Всего может быть создано до 512 наборов правил, в которых могут быть распределены до 1000 правил. Ограничение на число правил общее для всего SBC, один набор правил может содержать до 1000 правил. Таким образом, например, на SBC можно создать один набор правил с 1000 правил, либо 512 наборов с двумя правилами в каждом.

Для создания, редактирования и удаления записей используется меню *«Объекты» - «Добавить объект», «Объекты» - «Редактировать объект»* и *«Объекты» - «Удалить объект»*, а также кнопки:

- *«Добавить»;*
- *«Редактировать»;*
- *«Удалить»*.

Конфигурация SBC –> Rule set

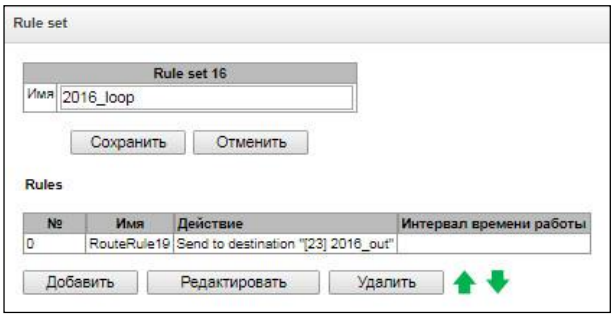


Настройка наборов правил

- *Имя* — произвольное имя для идентификации (удобное для оператора).

Каждый набор правил может содержать несколько правил, которые определяют, при каких условиях и в какое направление требуется отправлять вызовы.

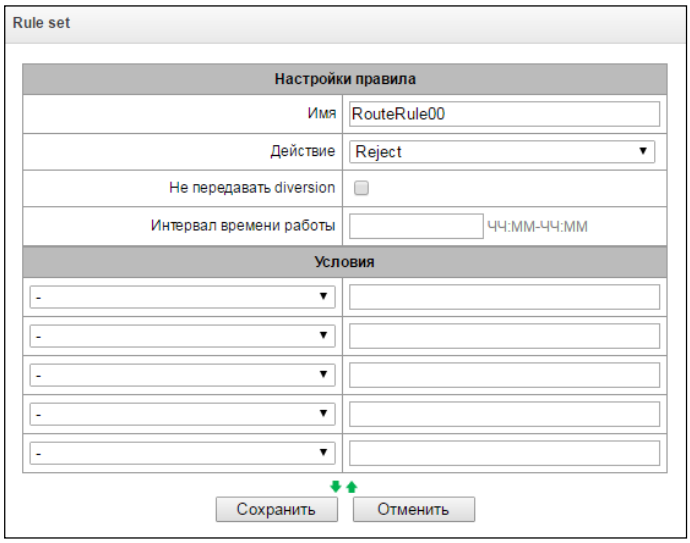
Конфигурация SBC –> Rule set–> «Редактировать»



Настройки правил

Для создания, редактирования и удаления правил служат кнопки *«Добавить», «Редактировать» и «Удалить»*. Зеленые стрелки рядом с кнопками редактирования позволяют перемещать выделенные записи в таблице, настраивая порядок расположения созданных правил.

Конфигурация SBC –> Rule set–> «Редактировать»



- *Имя* — произвольное имя для идентификации (удобное для оператора);
- *Действие* — действие, которое требуется произвести над сообщениями, попавшими под условия правила:
  - *Reject* — сообщение будет отброшено;
  - *Send to destination* — сообщение будет отправлено в одно из направлений;
  - *Send to trunk* — сообщение будет направлено в один из транков;
- *SIP Destination/SBC Trunk* — поле для выбора направления или транка, появляется при выборе действия, отличного от Reject;
- *Не передавать diversion* — при включенной опции поле Diversion не будет передаваться в сторону выбранного SIP Destination/SBC Trunk;
- *Интервал времени работы* — интервал времени, в течении которого правило будет работать. Вне этого интервала правило отрабатываться не будет. Формат настройки — диапазон времени, записанный как "ЧЧ:ММ-ЧЧ:ММ".

Условия

В блоке *«Условия»* производится настройка условий для определения того, попадает ли сообщение под правило. В левом столбце настраивается перечень параметров проверки, в правом — значения параметров. Для срабатывания правило должно содержать хотя бы одно условие, и все условия должны быть истинными.

Параметры проверки:

- *Все* — не производится никаких дополнительных проверок, сообщения обрабатываются согласно полю *«Действие»;*
- *Имя из заголовка From* — проверяется имя из заголовка From, допускается проверка через регулярное выражение;
- *Домен из заголовка From* — проверяется домен из заголовка From, допускается проверка через регулярное выражение;
- *URI из заголовка From* — проверяется URI из заголовка From, допускается проверка через регулярное выражение;
- *Имя из заголовка To* — проверяется имя из заголовка To, допускается проверка через регулярное выражение;
- *Домен из заголовка To* — проверяется домен из заголовка To, допускается проверка через регулярное выражение;
- *URI из заголовка To* — проверяется URI из заголовка To, допускается проверка через регулярное выражение;
- *Имя из Request-URI* — проверяется имя из Request-URI, допускается проверка через регулярное выражение;
- *Домен из Request-URI* — проверяется домен из Request-URI, допускается проверка через регулярное выражение;
- *Request-URI* — проверяется Request-URI, допускается проверка через регулярное выражение;
- *IP источника* — проверяется IP-адрес источника, допускается указание как отдельного IP, так и подсети в нотации CIDR: 192.0.2.0/24;
- *User-Agent* — проверяется User-Agent, допускается проверка через регулярное выражение.

Возможно изменить порядок условий, выбрав условие кликом по полю и переместить его выше или ниже зелёными стрелками, которые находятся под списком условий.

Синтаксис регулярных выражений для составления условий

1. Регулярное выражение описывается комбинацией букв латинского алфавита, цифрами и специальными символами.

Пример: **12345@my\.domain** — строка, содержащая «**12345@my.domain».** Символ «.» (точка) в данной записи является специальным и был экранирован, подробнее в пункте 11.

2. Последовательность символов, заключённая в квадратные скобки, соответствует любому из заключённых в скобки символов;

Пример: **[01459]** — соответствует одной из цифр 0, 1, 4, 5 или 9

3. В квадратных скобках может быть указан диапазон символов через тире;

Пример: **[4-9]** — соответствует одному из чисел от 4 до 9;

Пример: **[a-d4-97]** — комбинация предыдущих вариантов записи. Соответствует любой букве от «a» до «d», одному из чисел от 4 до 9 или числу 7.

4. Символ «^» обозначает начало строки;

Пример: **^7383** — строка, которая начинается на 7383.

5. Символ «$» обозначает конец строки;

Пример: **100$** — строка, которая заканчивается на 100.

Пример: **^40000$** — строка, которая точно соответствует «40000»

6. Символ «.» (точка) означает любой символ;

Пример: **^7383.....** — строка, которая начинается на 7383 и далее содержит семь любых символов. При этом строка может быть длиннее. Чтобы точно ограничить строку, в конце следует добавить символ «$»: **^7383.....$**;

Пример: **^.....$** — строка, которая содержит ровно пять любых символов;

Пример: **.....** — строка, которая содержит любые пять символов. Более длинные строки тоже попадают сюда.

7. Символ «*» означает повторение предыдущего символа ноль и более раз

Пример: **45*** — строки, которые содержат последовательность: 4, 45, 455 и т.д.

8. Символ «+» означает повторение предыдущего символа один и более раз

Пример: **45+** — строки, которые содержат последовательность: 45, 455 и т. д.;

Пример: **^2.+** — строка, которая начинается на два и продолжается одним и более количеством любых символов.

9. В фигурных скобках может указываться точный диапазон повторений символов:

- {k, m} — повторение предыдущего символа от k до m раз;
- {k,} — повторение символа k раз и более;
- {,m} — повторение символа не более m раз;
- {n} — повторение символа точно n раз. Аналогично {n,n}.

Пример: **^7{0,1}38329[0-5][0-9]{4}$** — любая строка, в начале которой содержится или не содержится семёрка, затем последовательность 38329, затем одна любая цифра от нуля до пяти и следом четыре любые цифры.

10. В круглых скобках можно группировать выражения. Обычно используется с символом «|» (вертикальная черта), который означает логическое ИЛИ;

Пример: **(^9000$|^10000$)** — строка соответствует числу 9000 или 10000;

Пример: **^(7|8)[0-9]{10}$** — строка начинается с семёрки или восьмёрки и затем содержит 10 цифр;

Пример: **^(4[0-4]|5[3-4])** — строка начинается на 40, 41, 42, 43, 44, 53 или 54.

11. Для сравнения со специальными символами, используемыми в регулярном выражении,

требуется экранировать их символом «\» (обратный слэш).

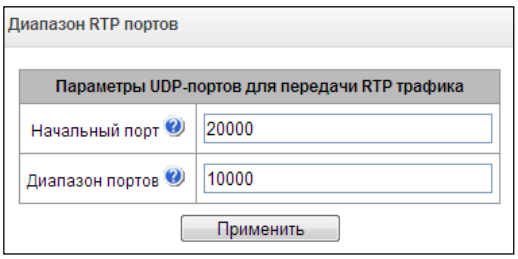
Пример: **^\+7.*** — строка, которая начинается на +7.

4.1.3.6 Диапазон RTP портов

В данном разделе конфигурируется диапазон портов UDP для передачи голосовых RTP пакетов. Может быть задано от 1 до 32000 портов.

Конфигурация SBC –> Диапозон RTP портов

Параметры UDP-портов:



- *Начальный порт* — номер начального UDP-порта, используемого для передачи разговорного трафика (RTP) и данных по протоколу T.38;
- *Диапазон портов* — диапазон (количество) UDP-портов, используемых для передачи разговорного трафика (RTP) и данных по протоколу T.38.

Во избежание конфликтов, порты, используемые для передачи RTP и T.38, не должны пересекаться с портами, используемыми под сигнализацию SIP (по умолчанию порт 5060).

4.1.3.7 Статистика SIP

В этом разделе настраивается отображение и состав групп статистик. Любая группа может быть скрыта из меню *«Мониторинг - Статистика SIP»*. В группах с 8 по 11 включительно могут быть настроены учитываемые в них коды ответов SIP и отображаемое наименование счётчиков.

Конфигурация SBC –> Статистика SIP

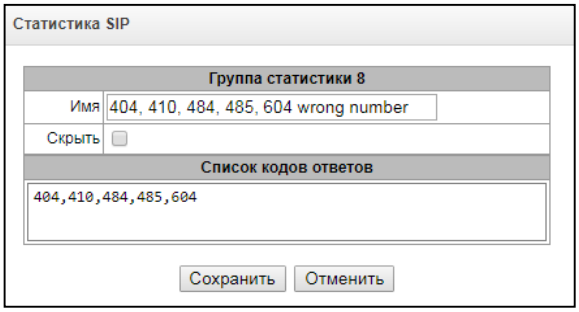
Статистика SIP

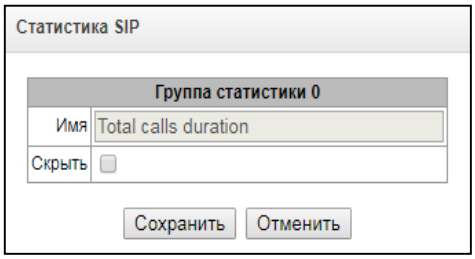
№	Имя	Скрыть
0	Total calls duration	
1	Incoming call-legs	
2	Outcoming call-legs	
3	Message received	
4	Message send	
5	Redirected calls 3xx	
6	Answered calls with successfull final	
7	Answered calls with error final, usually only by timeout	
8	404, 410, 484, 485, 604 wrong number	
9	486, 600 busy	
10	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	

Редактировать | По умолчанию

Для настройки группы надо выделить её в таблице и нажать кнопку *«Редактировать»*. Для сброса параметров группы к стандартному состоянию надо выделить его и нажать кнопку *«По умолчанию»*.

При редактировании откроется следующее окно в зависимости от типа группы: с редактированием только видимости и с полным редактированием.





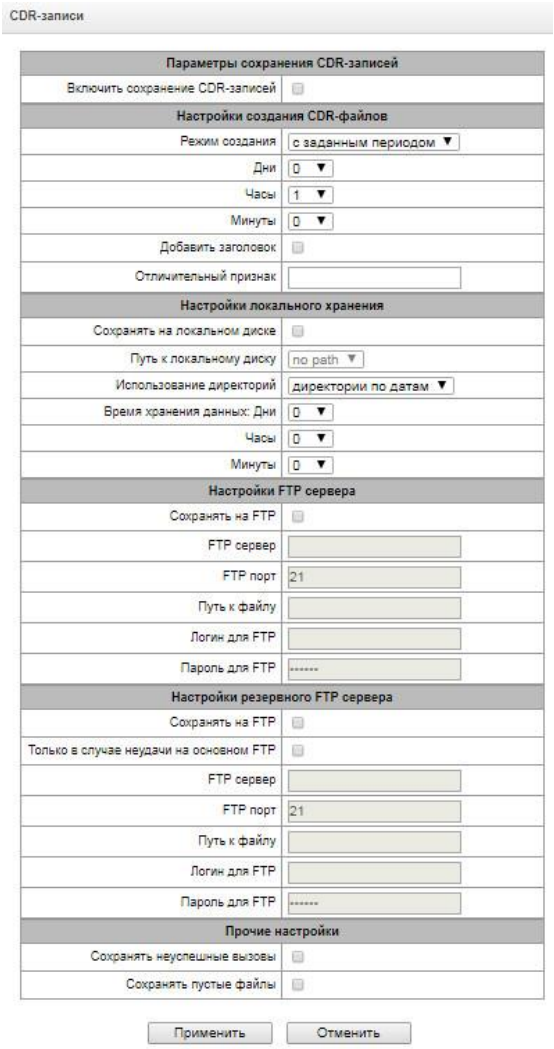
Для настройки доступны:

- *Имя* — отображаемое имя группы статистик;
- *Скрыть* — при установленном флаге группа не будет отображаться в просмотре статистик;
- *Список кодов ответов* — сюда заносятся SIP коды ответов для учёта в выбранной группе статистик. Допускаются коды в числовом виде от 400 до 699, разделённые пробелом, запятой, знаком табуляции или переносом строк.

4.1.3.8 CDR-записи

В данном разделе производится настройка параметров для сохранения детализированных записей о вызовах.

CDR — детализированные записи о вызовах, позволяют сохранить историю о совершенных через шлюз SBC вызовах.



Параметры сохранения CDR-записей

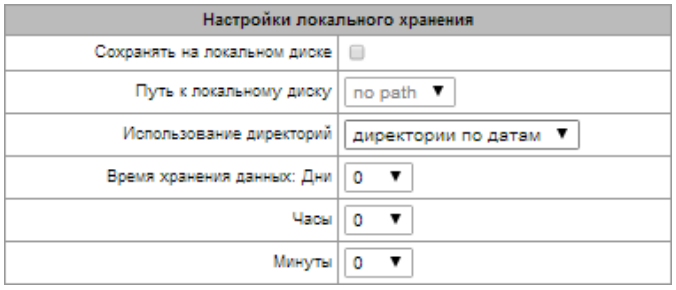
- *Включить сохранение CDR записей* — при установленном флаге шлюз будет формировать CDR-записи;

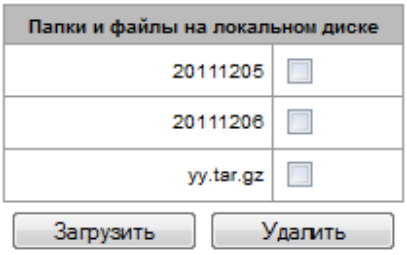
Настройки создания CDR-файлов

- *Режим создания* — выбор режима создания файлов CDR:
  - *с заданным периодом* — CDR-файл создается по истечении указанного периода с момента загрузки устройства.
  - *один раз в сутки* — CDR-файл создается один раз в сутки в указанное время;
  - *один раз в час* — CDR-файл создает один раз в час в указанное время;
- *Период сохранения: Дни, Часы, Минуты* — период формирования CDR-записей, в течение данного периода CDR-записи хранятся в оперативной памяти, после — сохранятся на локальный источник хранения;
- *Добавить заголовок* — при установленном флаге в начало CDR-файла записывается заголовок вида: SBC-1000. CDR. File started at 'YYYYMMDDhhmmss', где 'YYYYMMDDhhmmss' — время начала сохранения записей в файл;
- *Отличительный признак* — задает отличительный признак, по которому можно идентифицировать устройство, создавшее запись.

Настройки локального хранения

- *Сохранять на локальном диске* — при установленном флаге CDR-записи сохраняются на локальном накопителе;
- *Путь к локальному диску* — путь к локальному накопителю. При указании пути к локальному диску в меню отобразится список папок и файлов на данном диске. Для загрузки данных на компьютер необходимо установить флаг напротив требуемых записей и нажать *«Загрузить»*. При этом папка с записями будет помещена в архив, который во избежание переполнения диска рекомендуется после загрузки удалить. Для удаления уже неактуальных данных необходимо установить флаг напротив требуемых записей и нажать *«Удалить»*.





- *Использование директорий* — выбор директорий для хранения данных CDR:
  - *директории по датам* — CDR-записи сохраняются в отдельных директориях, имя директории соответствует дате создания файла CDR, формат имени «cdrYYYYMMDD», например, cdr20150818;
  - *Единая директория* — все CDR-записи сохраняются в единый каталог *«cdr_all»* на выбранном накопителе;
- *Время хранения данных*: *Дни, Часы, Минуты* — период хранения CDR-записей на локальном накопителе диске;

В оперативной памяти устройства выделено 30MB для хранения CDR-записей.

Если объем полученных CDR-записей превысит порог 30MB до истечения периода хранения, все дальнейшие биллинговые данные, поступающие в этом промежутке времени, будут утеряны.

Настройки FTP-сервера

- *Сохранять на FTP* — при установленном флаге CDR-записи будут передаваться на FTP-сервер;
- *FTP сервер* — IP-адрес FTP-сервера;
- *FTP порт* — TCP-порт FTP-сервера;
- *Путь к файлу* — указывает путь к папке на FTP-сервере, в которую будут сохраняться CDR-записи;
- *Логин для FTP* — имя пользователя для доступа к FTP-серверу;
- *Пароль для FTP* — пароль пользователя для доступа к FTP-серверу.

Настройки резервного FTP сервера

- *Сохранять на FTP* — при установленном флаге CDR-записи будут передаваться на резервный FTP-сервер;
- *Только в случае неудачи на основном FTP* — если опция задана, то сохранение CDR на резервный FTP сервер будет производиться только при неудаче записи на основной FTP сервер. В противном случае CDR будут записываться одновременно на основной и резервный серверы.
- *FTP сервер* — IP-адрес резервного FTP-сервера;
- *FTP порт* — TCP-порт резервного FTP-сервера;
- *Путь к файлу* — указывает путь к папке на резервном FTP-сервере, в которую будут сохраняться CDR-записи;
- *Логин для FTP* — имя пользователя для доступа к резервному FTP-серверу;
- *Пароль для FTP* — пароль пользователя для доступа к резервному FTP-серверу.

Прочие настройки

- *Сохранять неуспешные вызовы* — при установленном флаге записывать в CDR-файлы неуспешные вызовы (не окончившиеся разговором);
- *Сохранять пустые файлы* — при установленном флаге сохранять не содержащие записей CDR-файлы.

4.1.3.8.1 Формат CDR-записи

- заголовок, общий для всего CDR-файла (параметр присутствует, если установлена соответствующая настройка);
- отличительный признак (параметр присутствует, если установлена соответствующая настройка) (SIGNATURE);
- время установления соединения в формате YYYY-MM-DD hh:mm:ss (DATATIME);
- информация о вызывающем абоненте:
    - номер вызывающего абонента (KOD_A);
    - номер транка вызывающего абонента (не реализовано в текущей версии) (N_TR_GR_A);
    - категория вызывающего абонента (не реализовано в текущей версии) (CATEG_A);
    - IP-адрес шлюза вызывающего абонента (SRC_IP);
    - список IP-адресов из заголовков Record-Route при установлении соединения в направлении от вызывающего абонента (SRC_R_ROUTE);
    - список IP-адресов из заголовков Via при установлении соединения в направлении от вызывающего абонента (SRC_VIA);
    - IP-адрес из заголовка Contact вызывающего абонента (SRC_CONTACT);
- информация о вызываемом абоненте:
    - номер вызываемого абонента (KOD_B);

- номер транка вызываемого абонента (не реализовано в текущей версии) (N_TR_GR_B);
- IP-адрес шлюза вызываемого абонента (DST_IP);
- IP-адрес из заголовка Contact вызываемого абонента (DST_CONTACT);

– длительность вызова, сек (T_ECD);
– причина разъединения согласно ITU-T Q.850 (CAUSE);
– индикатор успешного вызова (с ответом вызываемого абонента) (COMPLETEIND);
– сторона-инициатор разъединения (PLACE);
– внутренняя причина разъединения (в текущей версии совпадает с CAUSE) (TREATMENT);
– идентификатор вызова (CONN_ID);
– номер абонента при переадресации (не реализовано в текущей версии) (REDIRECTED).

4.1.3.8.2 Пример CDR-файла

Пример CDR-файла, содержащего две записи (включено сохранение заголовка и отличительного признака):

```
<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 *Конфигурация интерфейсов. Сетевая подсистема*

В данном разделе задаются сетевые настройки устройства, таблица маршрутизации IP-пакетов.

DHCP — протокол, предназначенный для автоматического получения IP-адреса и других параметров, необходимых для работы в сети TCP/IP. Позволяет шлюзу автоматически получить все необходимые сетевые настройки от DHCP-сервера.

DNS — протокол, предназначенный для получения информации о доменах. Позволяет шлюзу получить IP-адрес взаимодействующего устройства по его сетевому имени (хосту). Это может быть необходимо, например, при указании хостов в плане маршрутизации, либо использовании в качестве адреса SIP-сервера его сетевого имени.

TELNET — протокол, предназначенный для организации управления по сети. Позволяет удаленно подключиться к шлюзу с компьютера для настройки и управления. При использовании протокола TELNET данные передаются по сети нешифрованными.

SSH — протокол, предназначенный для организации управления по сети. При использовании данного протокола, в отличие от TELNET, вся информация, включая пароли, передается по сети в зашифрованном виде.

VPN — технология, позволяющая обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет).

PPTP — туннельный протокол типа точка-точка, позволяющий компьютеру устанавливать защищённое соединение с сервером за счёт создания специального туннеля в стандартной, незащищённой сети. Одна из разновидностей VPN.

4.1.4.1 Таблица маршрутизации

В данном подменю пользователь может настроить статические маршруты. Всего можно настроить до 255 маршрутов.

Статическая маршрутизация позволяет маршрутизировать пакеты к указанным IP-сетям, либо IP-адресам через заданные шлюзы. Пакеты, передаваемые на IP-адреса, не принадлежащие IP-сети шлюза и не попадающие под статические правила маршрутизации, будут отправлены на шлюз по умолчанию.

Таблица маршрутизации делится на 2 части, это сконфигурированные маршруты, которые отображаются в верхней части таблицы, и маршруты, созданные автоматически.

Маршруты, созданные автоматически, невозможно изменить, они создаются автоматически при поднятии сетевых и VPN/PPTP интерфейсов, и необходимы для нормальной работы этих интерфейсов.

В таблице показаны используемые на момент запроса маршруты (*«Активен»* в поле статус), а также неиспользуемые (*«Неактивен»* в поле статус), если маршруты были заданы вручную оператором. Созданные вручную маршруты, в отличие от созданных автоматически, не удаляются системой при отключении соответствующего интерфейса и будут заново применены при восстановлении работоспособности интерфейса.

Сетевая подсистема –> Таблица маршрутизации

Таблица маршрутизации

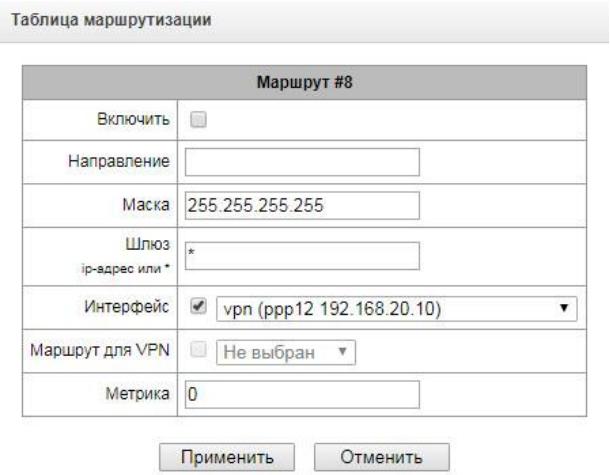
№	Включен	Статус	Направление	Маска	Шлюз	Интерфейс	Метрика
0	Да	Активен	1.2.3.10	255.255.255.255	192.168.1.123	-	99
1	Да	Неактивен	1.2.3.11	255.255.255.255	192.168.69.123	if_609_dhcp (eth0.609)	2
2	Да	Неактивен	1.6.8.4	255.255.255.0	*	-	0
3	Да	Неактивен	10.20.32.0	255.255.255.0	*	-	0
4	Да	Неактивен	10.20.33.1	255.255.255.255	*	-	2
5	Да	Неактивен	10.20.34.1	255.255.255.255	*	-	0
6	Да	Неактивен	10.20.35.1	255.255.255.255	*	-	0
7	Да	Неактивен	10.20.31.0	255.255.255.0	*	-	0
Маршруты, созданные автоматически							
8	Да	Активен	192.168.20.1	255.255.255.255	*	ppp12	0
9	Да	Активен	99.99.99.0	255.255.255.0	*	eth0.999	0
10	Да	Активен	192.168.69.0	255.255.255.0	*	eth0.609	0
11	Да	Активен	192.168.118.0	255.255.255.0	*	eth0.118	0
12	Да	Активен	192.168.2.0	255.255.255.0	*	eth0	0
13	Да	Активен	192.168.1.0	255.255.255.0	*	eth0	0
14	Да	Активен	192.168.0.0	255.255.255.0	*	eth0	0
15	Да	Активен	172.1.0.0	255.255.0.0	*	eth0	0
16	Да	Активен	default	0.0.0.0	192.168.1.123	eth0	0

Добавить Редактировать Удалить

Для создания, редактирования и удаления маршрута используется меню *«Объекты» - «Добавить объект», «Объекты» - «Редактировать объект»* и *«Объекты» - «Удалить объект»*, а также кнопки:

- «*Добавить»;*
- *«Редактировать»;*
- *«Удалить»*.

Сетевая подсистема –> Таблица маршрутизации –> «Добавить»



Для добавления нового маршрута необходимо задать следующие параметры:

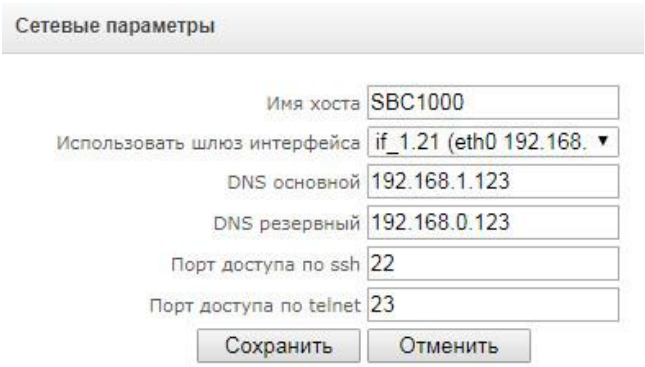
– *Включить* — при установленном флаге маршрут доступен для использования;
– *Направление* — IP-сеть, IP-адрес или значение default (для задания шлюза «по умолчанию»);
– *Маска* — задает маску сети для заданной IP-сети (для IP-адреса используйте маску 255.255.255.255);
– *Шлюз* — задает IP-адрес шлюза для маршрута;
– *Интерфейс* — выбор сетевого интерфейса передачи (если флаг не установлен, то будет выбран наиболее подходящий интерфейс исходя из адреса шлюза);
– *Маршрут для VPN* — интерфейс передачи, связанный с учётной записью VPN-клиента. Маршрут и адрес будут автоматически установлены через связанный с клиентом сетевой интерфейс, когда VPN-клиент произведёт подключение;
– Метрика — метрика маршрута.

Кнопки *«Применить»* и *«Отменить»,* для сохранения и сброса параметров соответственно.

4.1.4.2 Сетевые параметры

В данном подменю пользователь может указать имя устройства, изменить адрес сетевого шлюза, адрес DNS-сервера и порты доступа по SSH и Telnet.

Сетевая подсистема –> Сетевые параметры



– *Имя хоста* — сетевое имя устройства;
– *Использовать шлюз интерфейса* — выбор сетевого интерфейса, шлюз которого будет считаться основным на устройствах;
– *DNS основной* — основной DNS-сервер;
– *DNS резервный* — резервный DNS-сервер;
– *Порт доступа по ssh* — TCP-порт для доступа к устройству по протоколу SSH, по умолчанию 22;
– *Порт доступа по Telnet* — TCP-порт для доступа к устройству по протоколу Telnet, по умолчанию 23.

4.1.4.3 Сетевые интерфейсы

На устройстве есть возможность сконфигурировать 1 основной сетевой интерфейс eth0 и до 9-ти дополнительных интерфейсов, этими интерфейсами могут быть интерфейсы VLAN и Alias основного интерфейса eth0, либо Alias интерфейса VLAN.

Alias — это дополнительный сетевой интерфейс, который создается на базе существующего основного интерфейса eth0, либо на базе существующего VLAN-интерфейса.

Сетевая подсистема –> Сетевые интерфейсы

Сетевые интерфейсы

№	Имя интерфейса	Имя сети	IP адрес	Маска сети	DHCP	Сервисы управления				Профиль firewall
0	eth0	ssw	192.168.118.90	255.255.255.0	-	WEB		SSH	SNMP	Firewall Profile #8
1	eth0:1	alias1	192.168.116.90	255.255.255.0	-	WEB	TELNET	SSH	SNMP	Не выбран
2	eth0:2	alias2	192.168.117.90	255.255.255.0	-	WEB	TELNET			Не выбран
3	eth0.20	localnet	192.168.16.199	255.255.255.0	-	WEB			SNMP	Не выбран
4	VPN/pptp client (ppp3)	345uu	-	-	-		TELNET	SSH	SNMP	Не выбран
5	eth0.40	119	192.168.119.90	255.255.255.0	-	WEB	TELNET	SSH		Не выбран

Добавить | Редактировать | Удалить

Для создания, редактирования и удаления интерфейсов используется меню *«Объекты» - «Добавить объект», «Объекты» - «Редактировать объект»* и *«Объекты» - «Удалить объект»*, а также кнопки:

- *«Добавить»;*
- *«Редактировать»;*
- *«Удалить»*.

Для добавления сетевого интерфейса необходимо нажать кнопку *«Добавить»* и заполнить параметры:

Сетевая подсистема –> Сетевые интерфейсы –> «Добавить» (окно при выборе типа «Tagged»)

Сетевые интерфейсы

Сетевой интерфейс 11	
Имя сети	
Профиль firewall	Не выбран
Тип	Tagged
VLAN ID	
Использовать DHCP	☐
IP адрес	
Маска сети	
Broadcast	
Шлюз	
Получить шлюз автоматически	☐
Получить DNS автоматически	☐
Получить NTP автоматически	☐
Class of service	0
Сервисы	
Управление через Web	☐
Управление по Telnet	☐
Управление по SSH	☐
Использовать SNMP	☐

Применить | Отменить

Основные настройки:

- *Имя сети* — произвольное наименование (для удобства оператора), с которым будут ассоциированы заданные сетевые настройки;
- *Профиль firewall* — отображение выбранного профиля firewall для данного интерфейса;
- *Тип* — тип интерфейса (для интерфейса eth0 всегда untagged).
  - *untagged* — нетегированный интерфейс (без VLAN);
  - *tagged* — тегированный интерфейс (с VLAN);
  - *VPN/pptp client* — клиентский интерфейс для подключения VPN к удалённому серверу по протоколу PPTP;
- *VLAN ID* — идентификатор виртуальной сети (1-4095) (только для интерфейсов с типом tagged);
- *Использовать DHCP* — получить IP-адрес динамически от DHCP сервера (требуется наличие DHCP сервера в сети оператора);
- *IP-адрес* — сетевой адрес устройства;
- *Маска сети* — маска сети для устройства;
- *Шлюз* — сетевой шлюз по умолчанию;
- *Получить шлюз автоматически* — получение адреса шлюза от DHCP-сервера.
- *Получить DNS автоматически* — получить IP-адрес DNS-сервера динамически от DHCP-сервера;
- *Получить NTP автоматически* — получить IP-адрес NTP-сервера динамически от DHCP-сервера;
- *Class of service* — установка метки приоритета трафика в соответствии со стандартом IEEE 802.1p.

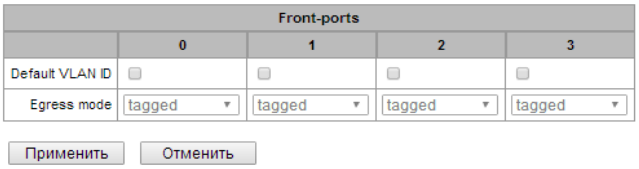
Сервисы — меню управления разрешенных сервисов для данного интерфейса:

- *Управление через Web* — разрешает доступ к конфигуратору через интерфейс;
- *Управление по Telnet* — разрешает доступ по протоколу telnet через интерфейс;
- *Управление по SSH* –разрешает доступ по протоколу SSH через интерфейс;
- *Использовать SNMP* — разрешает использования протокола SNMP через интерфейс.

После изменения IP-адреса или маски сети, либо при отключении управления через web-конфигуратор на сетевом интерфейсе, во избежание потери доступа к устройству необходимо подтвердить данные настройки, подключившись к web-конфигуратору, иначе по истечении двухминутного таймера произойдет откат к предыдущей конфигурации.

Front-ports[1] — настройка внешних front-портов

Данная настройка доступна только для тегированных интерфейсов VLAN (в параметре *«Тип»* установлено значение *«Tagged»).*

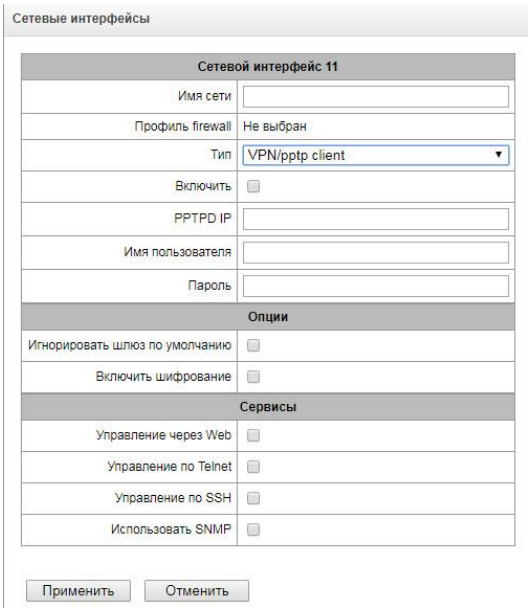


– *Default VLAN ID* — при поступлении на порт пакета без тега VLAN ID этот пакет помечается тегом VLAN ID выбранного сетевого интерфейса, если пакет принят с тегом VLAN ID, то принятый тег не изменяется;
– *Egress mode* — правила работы с тегом VLAN при отправке пакета с порта:

- *tagget* — отправлять пакет с VLAN ID выбранного сетевого интерфейса;
- *untagget* — отправлять пакет без VLAN ID.

Сетевая подсистема –> Сетевые интерфейсы –> «Добавить» (окно при выборе типа «VPN/ pptp client»)

При выборе в поле *«Тип интерфейса»* значения VPN/ pptp client станут доступны специальные настройки*:*



– *Имя сети* — наименование сети;
– *Профиль firewall* — отображение выбранного профиля firewall для данного интерфейса;
– *Тип* — VPN/pptp client;
– *Включить* — включение VPN/PPP интерфейса;
– *PPTPD IP* — IP-адрес PPTP сервера;
– *Имя пользователя* — имя пользователя (login), под которым устройство присоединяется к сети;
– *Пароль* — пароль для VPN–соединения.

Опции:

– *Игнорировать шлюз по умолчанию* — игнорировать настройку шлюза в разделе *«Сетевые параметры»*;
– *Включить шифрование* — включает шифрование.

Сервисы — меню управления разрешенных сервисов для данного интерфейса:

– *Управление через Web* — разрешает доступ к конфигуратору через интерфейс;
– *Управление по Telnet* — разрешает доступ по протоколу telnet через интерфейс;
– *Управление по SSH* –разрешает доступ по протоколу SSH через интерфейс;

[1] Только для SBC-2000

– *Использовать SNMP* — разрешает использования протокола SNMP через интерфейс.

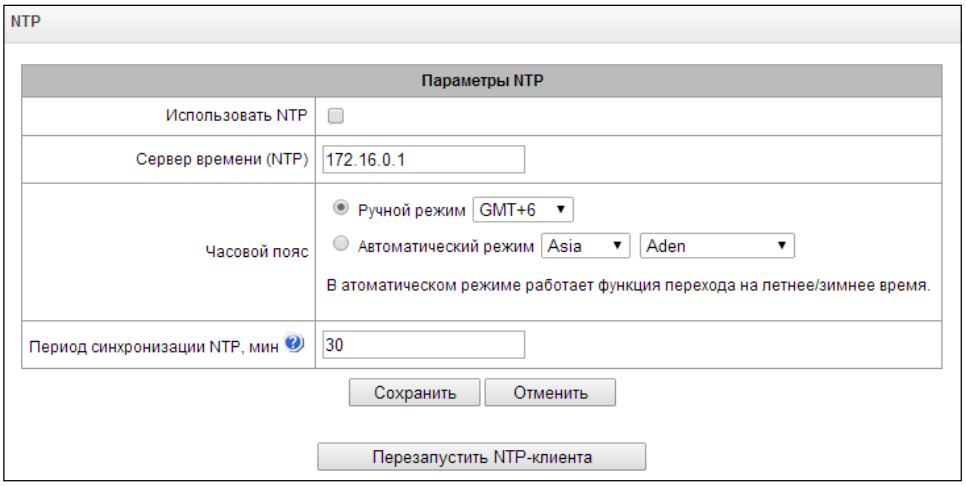
4.1.5 *Сетевые сервисы*

4.1.5.1 NTP

В данном подменю настраивается служба синхронизации времени.

NTP — протокол, предназначенный для синхронизации внутренних часов устройства. Позволяет синхронизировать время и дату, используемую шлюзом, с их эталонными значениями.

Сетевые сервисы –> NTP



– *Использовать NTP* — включить NTP-клиента;
– *Сервер времени (NTP)* — сервер времени, с которого устройство будет синхронизировать дату и время;
  – *Часовой пояс* — настройка часового пояса и отклонения текущего времени относительно GMT (Greenwich Mean Time):
    – *Ручной режим* — выбор отклонения времени относительно GMT;
    – *Автоматический режим* — в данном режиме предоставлена возможность выбора местонахождения устройства, отклонение от GMT будет настроено автоматически, также в данном режиме работает автоматический переход на летнее и зимнее время;
– *Период синхронизации NTP, мин* — период отправки запросов на синхронизацию времени.

Для сохранения и отмены изменений используются кнопки «*Сохранить*» и «*Отменить*». Для принудительной синхронизации времени от сервера необходимо нажать кнопку «*Перезапустить NTP-клиента*» (происходит перезапуск NTP–клиента).

4.1.5.2 SNMP

SNMP — протокол простого управления сетью. Позволяет устройству в реальном времени передавать сообщения о произошедших авариях контролирующему SNMP-менеджеру. Также SNMP-агент устройства поддерживает мониторинг состояний датчиков шлюза по запросу от SNMP-менеджера.

Функции мониторинга по SNMP позволяют запросить у шлюза следующие параметры:

– имя шлюза;
– тип устройства;
– версия программного обеспечения;
– IP-адрес;
– статистика субмодулей IP;

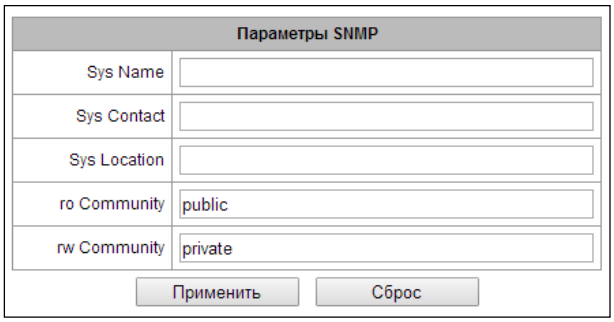
– состояние линксетов;
– состояние каналов IP (статистика по текущим вызовам через IP).

В статистике текущих вызовов по IP-каналам передаются следующие данные:

– номер канала;
– состояние канала;
– идентификатор вызова;
– MAC-адрес вызывающего абонента;
– IP-адрес вызывающего абонента;
– номер вызывающего абонента;
– MAC-адрес вызываемого абонента;
– IP-адрес вызываемого абонента;
– номер вызываемого абонента;
– продолжительность занятия канала.

4.1.5.2.1 Параметры SNMP

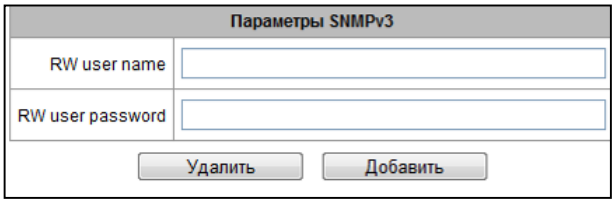
Сетевые сервисы –> SNMP



– *Sys Name* — системное имя устройства;
– *Sys Contact* — контактная информация производителя устройства;
– *Sys Location* — место расположения устройства;
– *roCommunity* — пароль на чтение параметров (общепринятый: public);
– *rwCommunity* — пароль на запись параметров (общепринятый: private).

4.1.5.2.2 Параметры SNMPv3

Сетевые сервисы –> SNMP (Параметры SNMPv3)



Конфигурация SNMPv3:

В системе используется только один пользователь SNMPv3.

– *RW User name* — имя пользователя;
– *RW User password* — пароль (пароль должен содержать более 8 символов).

Для применения конфигурации пользователя SNMPv3 используется кнопка *«Добавить»* (настройки применяются сразу после нажатия). Для удаления записи нажать кнопку *«Удалить».*

4.1.5.2.3 Настройка трапов (SNMP trap)

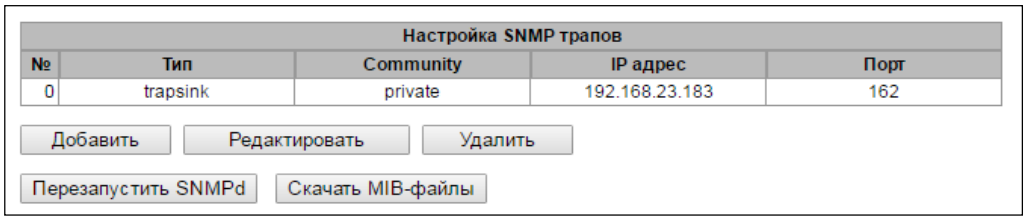
Подробное описание параметров мониторинга и сообщений Trap приведено в MIB-файлах, поставляемых на диске вместе с программным обеспечением.

SNMP-агент посылает сообщение SNMPv2-trap при возникновении следующих событий:

– ошибка конфигурации;
– регистрация абонента запрещена;
– вызов запрещен;
– динамический брандмаузер заблокировал новый адрес;
– высокая загрузка процессора;
– проблема в работе вентилятора;

- исправлена ошибка конфигурации;
- FTP-сервер недоступен, оперативная память для хранения CDR-файлов заполнена свыше 50% (15 — 30 MB);
- FTP-сервер недоступен, оперативная память для хранения CDR-файлов заполнена менее чем на 50% (5 — 15 MB);
- FTP-сервер недоступен, оперативная память для хранения CDR-файлов заполнена до 5MB;
- Статус обновления программного обеспечения и загрузки/выгрузки файла конфигурации.

Сетевые сервисы –> SNMP (Настройка SNMP трапов)



Настройка SNMP трапов

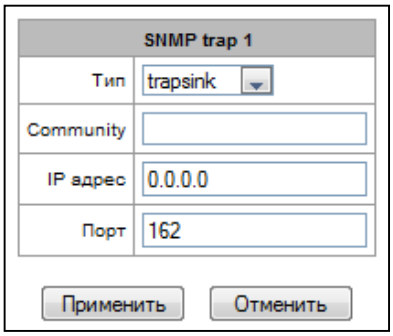
№	Тип	Community	IP адрес	Порт
0	trapsink	private	192.168.23.183	162

Добавить | Редактировать | Удалить

Перезапустить SNMPd | Скачать MIB-файлы

- *Перезапустить SNMPd* — по нажатию на кнопку осуществляется перезапуск SNMP клиента;

Сетевые сервисы –> SNMP (Настройка SNMP трапов) –> «Добавить»



SNMP trap 1

Тип	trapsink
Community	
IP адрес	0.0.0.0
Порт	162

Применить | Отменить

Могут быть созданы до 16 трапов. Для создания, редактирования и удаления параметров трапов используется кнопки:

- *«Добавить»;*
- *«Редактировать»;*
- *«Удалить».*

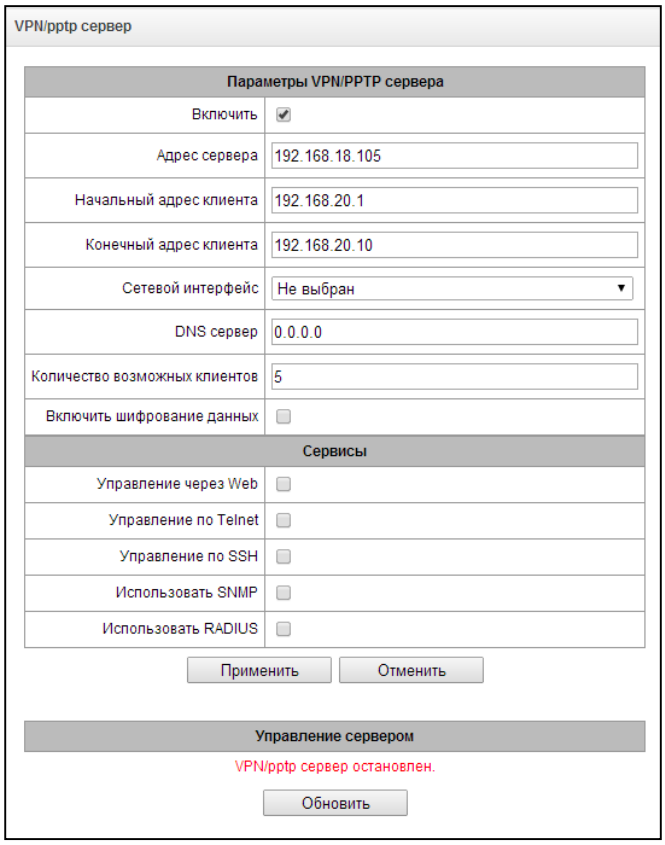
- *Тип* — тип SNMP сообщения (TRAPv1, TRAPv2, INFORM);
- *Community* — пароль, содержащийся в трапах;
- *IP адрес* — IP-адрес приемника трапов;
- *Порт* — UDP-порт приемника трапов.

4.1.5.2.4 Получение MIB-файлов

Для текущей версии ПО можно скачать актуальные MIB-файлы прямо с устройства, для этого необходимо нажать кнопку *«Скачать MIB-файлы»*.

4.1.5.3 VPN/PPTP сервер

Сетевые сервисы –> VPN/PPTP сервер



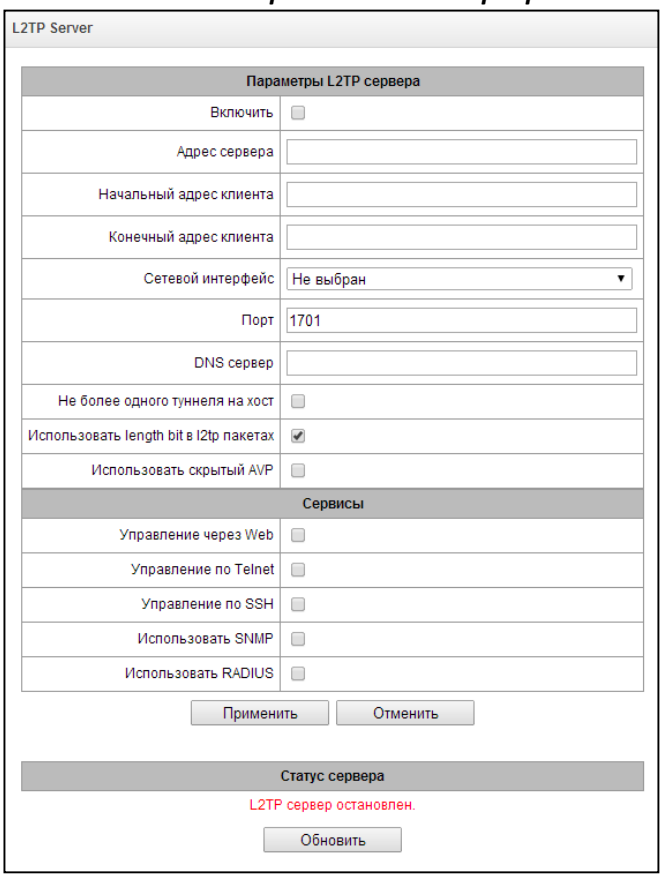
Параметры VPN/PPTP сервера

- *Включить* — запускать службу при старте/перезагрузке;
- *Адрес сервера* — IP-адрес, который будет сообщен в качестве адреса сервера всем подключающимся PPTP клиентам;
- *Начальный адрес клиента*, *Конечный адрес клиента* — границы диапазона IP-адресов, назначаемых PPTP клиентам;
- *Сетевой интерфейс* — выбор интерфейса для подключения к VPN/PPTP серверу;
- *DNS сервер* — адрес DNS сервера, который будет сообщаться клиентам;
- *Количество возможных клиентов* — число одновременных подключений клиентов;
- *Включить шифрование данных* — шифрование передаваемых данных (должно также быть включено у клиента);
- *Управление через Web, Управление по Telnet, Управление по SSH* — при установленном флаге соответствующий сервис управления доступен по заданному адресу интерфейса;
- *Использовать SNMP* — разрешает использования протокола SNMP через интерфейс;
- *Использовать RADIUS* — разрешает использование протокола RADIUS через интерфейс.

Для управления PPTP сервером используются кнопки *«Запустить»* и *«Остановить»*. При остановке новые соединения клиентов не будут создаваться, однако уже созданные будут продолжать работать. Обновление информации о статусе сервера происходит по нажатию кнопки *«Обновить»* напротив заголовка.

4.1.5.4 L2TP сервер

Сетевые сервисы –> L2TP сервер



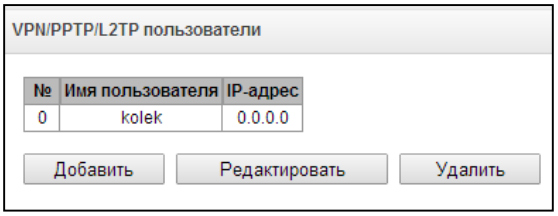
Параметры L2TP сервера

- *Включить* — запускать службу при старте/перезагрузке;
- *Адрес сервера* — IP-адрес, который будет сообщен в качестве адреса сервера всем подключающимся L2TP клиентам;
- *Начальный адрес клиента, Конечный адрес клиента* — границы диапазона IP-адресов, назначаемых PPTP клиентам;
- *Сетевой интерфейс* — выбор интерфейса для подключения к L2TP серверу;
- *Порт* — номер порта для подключения;
- *DNS сервер* — адрес DNS сервера, который будет сообщаться клиентам;
- *Не более одного туннеля на хост* — ограничение количества туннелей до одного для хоста;
- *Использовать length bit в l2tp пакетах* — использование бита длины представленного в нагрузке L2TP пакетов;
- *Использовать скрытый AVP* — использование скрытых AVP (подробнее в RFC 2661);
- *Управление через Web, Управление по Telnet, Управление по SSH* — доступность соответствующего сервиса управления по заданному адресу;
- *Использовать SNMP, использовать RADIUS* — флаг для включения соответствующего клиента по заданному адресу.

Обновление информации о статусе сервера происходит по нажатию кнопки *«Обновить»* напротив заголовка.

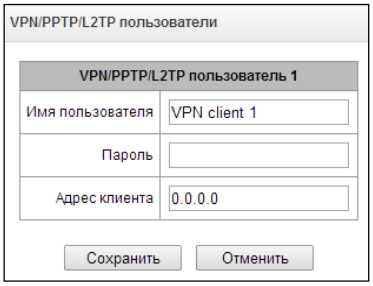
4.1.5.5 VPN/PPTP/L2TP пользователи

Сетевые сервисы –> L2TP сервер



В таблице показывается список VPN/PPTP/L2TP клиентов, которым разрешено подключаться к данному серверу.

За клиентом может быть закреплен постоянный IP-адрес из настроенного диапазона (*Адрес клиента*). Если настроено значение 0.0.0.0, то при каждом новом подключении клиенту будет выдаваться свободный IP-адрес из диапазона.



Для добавления пользователя необходимо заполнить следующие поля:

- *Имя пользователя* — имя, с которым пользователь будет подключаться к серверу;
- *Пароль* — пароль, с которым пользователь будет подключаться к серверу;
- *Адрес клиента* — адрес, который будет выдан клиенту внутри тоннеля. Если требуется выдавать адрес динамически, надо оставить поле пустым или с адресом 0.0.0.0.

4.1.6 *Коммутатор*[1]

Меню *«Коммутатор»* предназначено для настройки портов коммутатора.

4.1.6.1.1 Настройки LACP

В данном разделе производится настройка групп LACP. Можно задать до 5 групп для SBC-1000.

Link Aggregation Control Protocol (LACP) — протокол для объединения нескольких физических каналов в один логический.

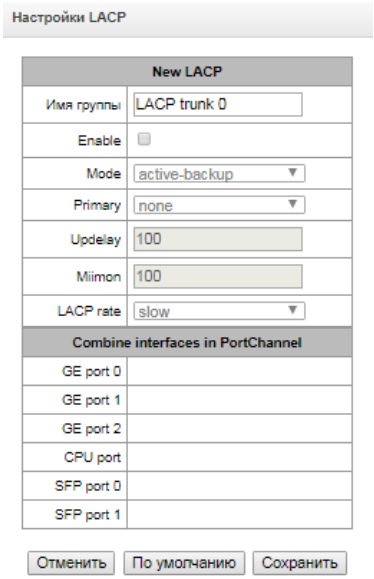
Коммутатор –> Настройки LACP

№	Имя группы	Enable	Mode	Primary	Updelay	Miimon	Lacp rate
0	LACP trunk 0	+	Active-backup	None	100	100	slow

Применить | Подтвердить | Добавить | Редактировать | Удалить | Сохранить

Для редактирования, удаления и применения изменений группы LACP используется кнопки: *«Редактировать», «Удалить»* и *«Применить»*. Для добавления новой группы LACP нажмите кнопку *«Добавить»* и заполните следующие поля:

Коммутатор –> Настройки LACP –> «Добавить»



- *Имя группы* — имя группы LACP;
- *Enable* — при установленном флаге разрешено использовать протокол LACP;
- *Mode* — режим работы протокола LACP:
  - *active-backup* — один интерфейс работает в активном режиме, остальные в ожидающем. Если активный интерфейс выходит из обслуживания, управление передается одному из ожидающих. Не требует поддержки данного функционала от коммутатора;
  - *balance-xor* — передача пакетов распределяется между объединенными интерфейсами по формуле: ((MAC-адрес источника) XOR (MAC-адрес получателя)) % число интерфейсов. Один и тот же интерфейс работает с определённым получателем. Данный режим позволяет сбалансировать нагрузку и повысить отказоустойчивость;
  - *802.3ad* — динамическое объединение портов. В данном режиме можно получить значительное увеличение пропускной способности как входящего, так и исходящего трафика, используя все объединенные интерфейсы. Требует поддержки данного функционала от коммутатора, а в ряде случаев — дополнительную настройку коммутатора;
- *Primary* — настройка ведущего интерфейса;
- *Updelay* — период смены интерфейса при недоступности ведущего интерфейса;
- *Miimon* — период проверки MII, частота в миллисекундах;
- *LACP rate* — интервал передачи управляющих пакетов протокола LACPDU:
  - *fast* — интервал передачи 1 секунда;
  - *slow* — интервал передачи 30 секунд.
- *Combine interfaces in PortChannel* — список портов, добавленных в группу LACP.

[1] Меню доступно только для SBC-1000

4.1.6.2 Настройка портов коммутатора

Коммутатор может работать в четырех режимах:

1. ***Без использования настроек VLAN*** — для использования режима на всех портах флаги *«Enable VLAN»* должны быть не установлены, значение *«IEEE Mode»* на всех портах должно быть установлено в «*Fallback*», взаимодоступность портов для передачи данных необходимо определить флагами «*Output*». Таблица маршрутизации *«802.1q»* в закладке «*802.1q»* не должна содержать записей.

2. ***Port based VLAN*** — для использования режима значение *«IEEE Mode»* на всех портах должно быть установлено в «*Fallback*», взаимодоступность портов для передачи данных необходимо определить флагами «*Output*». Для работы с VLAN необходимо использовать настройки *«Enable VLAN»*, «*Default VLAN ID», «Egress» и «Override».* Таблица маршрутизации *«802.1q»* в закладке «*802.1q»* не должна содержать записей.

3. ***802.1q*** — для использования режима значение *«IEEE Mode»* на всех портах должно быть установлено в *«Check»* либо *«Secure».* Для работы с VLAN используются настройки — *«Enable VLAN», «Default VLAN ID», «Override».* А также используются правила маршрутизации, описанные в таблице маршрутизации *«802.1q»* закладки «*802.1q».*

4. ***802.1q + Port based VLAN.*** Режим 802.1q может использоваться совместно с Port based VLAN. В этом случае значение *«IEEE Mode»* на всех портах должно быть установлено в «*Fallback*», взаимодоступность портов для передачи данных необходимо определить флагами «*Output*». Для работы с VLAN необходимо использовать настройки *«Enable VLAN», «Default VLAN ID», «Egress и Override».* А также используются правила маршрутизации, описанные в таблице маршрутизации *«802.1q»* закладки «*802.1q».*

Коммутатор –> Настройки портов коммутатора

Настройки портов коммутатора

	GE порт 0	GE порт 1	GE порт 2	CPU порт	SFP порт 0	SFP порт 1
Использовать 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 порт 1 ☐ GE порт 2 ☑ CPU порт ☑ SFP порт 0 ☐ SFP порт 1	☑ GE порт 0 ☐ GE порт 2 ☑ CPU порт ☑ SFP порт 0 ☐ SFP порт 1	☑ GE порт 0 ☑ GE порт 1 ☑ CPU порт ☐ SFP порт 0 ☐ SFP порт 1	☑ GE порт 0 ☑ GE порт 1 ☑ GE порт 2 ☑ SFP порт 0 ☑ SFP порт 1	☑ GE порт 0 ☑ GE порт 1 ☐ GE порт 2 ☑ CPU порт ☐ SFP порт 1	☐ GE порт 0 ☐ GE порт 1 ☐ GE порт 2 ☑ CPU порт ☐ SFP порт 0
LACP trunk	none	none	none		none	[0] LACP trunk 0
Port MAC (xx:xx:xx:xx:xx:xx)	A8:F9:4B:81:79:F5	A8:F9:4B:81:79:F5	A8:F9:4B:81:79:F5		A8:F9:4B:81:79:F5	A8:F9:4B:81:79:F5
Резервный порт	none	none	none		none	none
Возврат на master-порт	☐	☐	☐		☐	☐
Режим работы порта	auto	auto	auto			

Применить | Подтвердить | По умолчанию | Сохранить

В заводской конфигурации порты коммутатора недоступны между собой.

Коммутатор устройства SBC-1000 имеет 3 электрических порта Ethernet, 2 оптических и 1 порт для взаимодействия с процессором:

- *GE порт (0, 1, 2)* — электрические Ethernet-порты устройства;
- *SFP порт (0, 1)* — оптические Ethernet-порты устройства;
- *CPU порт* — внутренний порт, подключенный к центральному процессору устройства.

Все порты устройства являются самостоятельными, в SBC-1000 не используются combo порты.

Настройки коммутатора

- *Использовать VLAN* — при установленном флаге использовать настройки Default VLAN ID, Override и Egress на данном порту, иначе не использовать;
- *Default VLAN ID* — при поступлении на порт нетегированного пакета считается, что он имеет данный VID, при поступлении тегированного пакета считается, что пакет имеет VID, который указан в его теге VLAN;
- *VID Override* — при установленном флаге считается, что любой поступивший пакет имеет VID, указанный в строке *default VLAN ID.* Справедливо как для нетегированных, так и для тегированных пакетов;
- Egress:
  - *unmodified* — пакеты передаются данным портом без изменений (т.е. в том же виде, в каком поступили на другой порт коммутатора);
  - *untagged* — пакеты передаются данным портом всегда без тега VLAN;
  - *tagged* — пакеты передаются данным портом всегда с тегом VLAN;
  - *double tag* — пакеты передаются данным портом с двумя тегами VLAN — если принятый пакет был тегированным и с одним тегом VLAN — если принятый пакет был не тегированным;
- *IEEE mode* — устанавливает режимы безопасности при обработке принятых тегированных фреймов*:*
  - *fallback* — фрейм принимается на входящем порту независимо от наличия его 802.1q-тега в таблице маршрутизации «802.1q».
  - Если 802.1q-тег не содержится в таблице маршрутизации «802.1q», то фрейм передаётся на исходящий порт при условии, что он разрешён в секции «output» в настройках входящего порта.
  - Если 802.1q-тег содержится в таблице маршрутизации «802.1q», то фрейм передаётся на исходящий порт при условии, что исходящий порт является членом VLAN в таблице «802.1q» и разрешён в секции «output» в настройках входящего порта;
    - *check* — фрейм принимается на входящем порту если его 802.1q-тег содержится в таблице маршрутизации «802.1q» (входящий порт не обязан быть членом VLAN в таблице «802.1q»).
  - Фрейм передаётся на исходящий порт если исходящий порт является членом VLAN в таблице «802.1q» и разрешён в секции «output» в настройках входящего порт;
    - *secure* — фрейм принимается на входящем порту если его 802.1q-тег содержится в таблице маршрутизации «802.1q» и входящий порт является членом VLAN в таблице «802.1q».
  - Фрейм передаётся на исходящий порт если исходящий порт является членом VLAN в таблице «802.1q» и разрешён в секции «output» в настройках входящего порта.
    - *Output* — взаимодоступность портов для передачи данных. Устанавливаются разрешения отправки пакетов, принятых данным портом, в порты, отмеченные флагом;
    - *LACP trunk* — выбор группы LACP, к которой принадлежит указанный порт коммутатора;
    - *Port MAC* — смена MAC-адреса порта. Опция доступна для редактирования при выборе группы LACP на порту. Порты, входящие в одну группу LACP, должны иметь различные MAC-адреса;
    - *Резервный порт* — выбор порта, на который будет переключен трафик в случае возникновения нештатной ситуации (например, разрыв линии). Данная настройка необходима для обеспечения резервирования Dual Homing;
    - *Возврат на master-порт* — при установленном флаге будет осуществлен переход на

основной порт после его восстановления;

В текущей версии ПО поддерживается только global dual homing.

– *Режим работы порта* — выбор режима работы порта (auto, 10/100 Mbps Half, 10/100 Mbps Full, 1 Gbps). Настройка режима возможна только для электрических Ethernet-портов (*GE порт 0, GE порт 1, GE порт 2*).

Если в течение одной минуты настройки не подтверждены нажатием на кнопку *«Подтвердить»*, то они возвращаются к предыдущим значениям.

Для применения настроек необходимо нажать кнопку *«Применить»*, для подтверждения примененных настроек — кнопку *«Подтвердить»*.

При помощи кнопки «*По умолчанию*» можно установить параметры по умолчанию (значения, устанавливаемые по умолчанию, приведены на рисунке выше).

Для сохранения настроек в файл конфигурации без применения необходимо нажать кнопку «*Сохранить*».

4.1.6.3 802.1q

В подменю *«802.1q»* устанавливаются правила маршрутизации пакетов при работе коммутатора в режиме 802.1q. Таблица может содержать до 1024 записей.

Коммутатор шлюза имеет 3 электрических порта Ethernet, два оптических и один порт для взаимодействия с процессором:

– *GE порт (0, 1, 2)* — электрические Ethernet-порты устройства;
– *CPU порт* — внутренний порт, подключенный к центральному процессору устройства;
– *SFP порт (0, 1)* — оптические Ethernet-порты устройства.

Коммутатор –> 802.1q

802.1q

VID	GE порт 0	GE порт 1	GE порт 2	CPU порт	SFP порт 0	SFP порт 1	Override	Приоритет
	unmodified	unmodified	unmodified	unmodified	unmodified	unmodified		0

Добавить

VTU table

VID	GE порт 0	GE порт 1	GE порт 2	CPU порт	SFP порт 0	SFP порт 1	Override	Приоритет	Удалить
VTU table is empty!									

Применить | Подтвердить | Удалить | Сохранить

Добавление записи в таблицу маршрутизации пакетов

– *VID* — в поле необходимо ввести идентификатор группы VLAN, для которой создается правило маршрутизации, и для каждого порта назначить действия, выполняемые им при передаче пакета, имеющего указанный VID.
  – *unmodified* — пакеты передаются данным портом без изменений (т.е. в том же виде, в каком были приняты);
  – *untagged* — пакеты передаются данным портом всегда без тега VLAN;
  – *tagged* — пакеты передаются данным портом всегда с тегом VLAN;
  – *not member* — пакеты с указанным VID не передаются данным портом, т.е. порт не является членом этой группы VLAN.

Затем необходимо нажать кнопку *«Добавить»*. Для применения установленных настроек необходимо нажать кнопку *«Применить»*, затем подтвердить настройки кнопкой *«Подтвердить»*.

Если в течение одной минуты настройки не подтверждены нажатием на кнопку *«Подтвердить»*, то они возвращаются к предыдущим значениям.

Сохранить настройки во Flash-память устройства без применения возможно с помощью кнопки *«Сохранить»*.

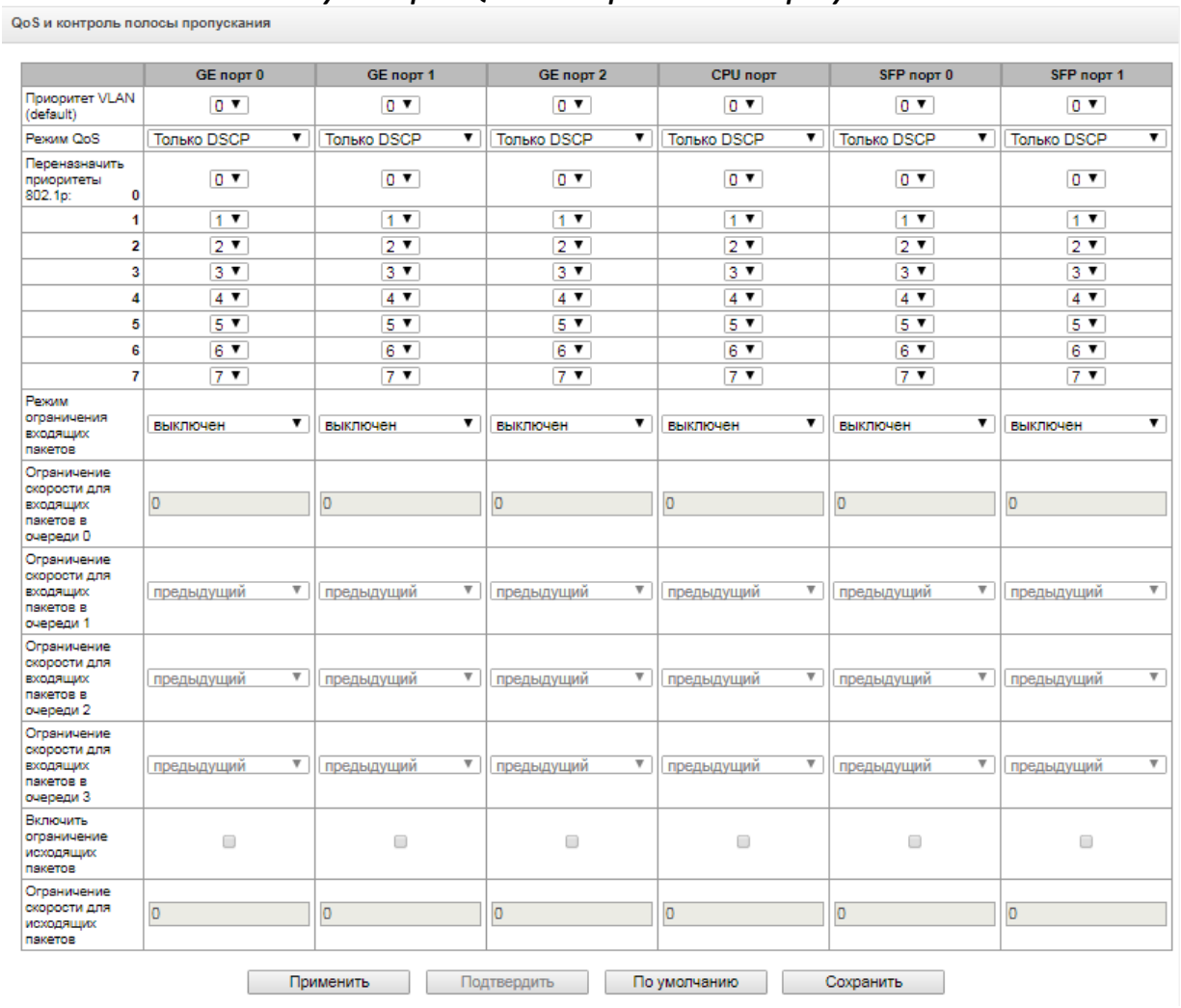
Удаление записи из таблицы маршрутизации пакетов

Для удаления записей необходимо установить флаги напротив удаляемых строк и нажать кнопку «*Удалить выделенные*».

4.1.6.4 QoS и контроль полосы пропускания

В разделе *«QoS и контроль полосы пропускания»* настраиваются функции обеспечения качества обслуживания (Quality of Service).

Коммутатор –> QoS и контроль полосы пропускания



– *Приоритет VLAN (default)* — приоритет 802.1p, назначаемый нетегированным пакетам, принятым данным портом. Если пакет уже имеет приоритет *802.1p* либо *IP diffserv* приоритет, то данный параметр не используется (default vlan priority не будет применяться к пакетам, содержащим заголовок IP, в случае использования одного из режимов QoS: *DSCP only, DSCP preferred, 802.1p preferre*d, а также к уже тегированным пакетам;
– *Режим QoS* — режим использования QoS:

  - *Только DSCP* — распределять пакеты по очередям только на основании приоритета IP diffserv;
  - *Только 802.1p* — распределять пакеты по очередям только на основании приоритета 802.1p;
  - *DSCP, 802.1p* — распределять пакеты по очередям на основании приоритетов IP diffserv и 802.1p, при этом при наличии обоих приоритетов в пакете, распределение по очередям осуществляется на основании IP diffserv;
  - *802.1p, DSCP* — распределять пакеты по очередям на основании приоритетов IP diffserv и 802.1p, при этом при наличии обоих приоритетов в пакете, распределение по очередям осуществляется на основании 802.1p;
- *Переназначить приоритеты 802.1p* — переназначение приоритетов 802.1p для тегированных пакетов. Каждому приоритету, принятому в пакете VLAN, можно таким образом назначить новое значение;
- *Режим ограничения входящих пакетов* — режим ограничения трафика, поступающего на порт:
  - *Выключен* — нет ограничения;
  - *Все пакеты* — ограничивается весь трафик;
  - *BroadMultFlood* — ограничивается многоадресный (multicast), широковещательный (broadcast) и лавинный одноадресный (flooded unicast) трафик;
  - *BroadMult* — ограничивается многоадресный (multicast) и широковещательный (broadcast) трафик;
  - *Broad* — ограничивается только широковещательный (broadcast) трафик;
- *Ограничение скорости для входящих пакетов в очереди 0* — ограничение полосы пропускания трафика, поступающего на порт для нулевой очереди. Допустимые значения в пределах от 70 до 250000 килобит в секунду;
- *Ограничение скорости для входящих пакетов в очереди 1* — ограничение полосы пропускания трафика, поступающего на порт для первой очереди. Полосу пропускания можно либо увеличить в два раза (prev prio *2) относительно нулевой очереди, либо оставить такой же (same as prev prio);
- *Ограничение скорости для входящих пакетов в очереди 2* — ограничение полосы пропускания трафика, поступающего на порт для второй очереди. Полосу пропускания можно либо увеличить в два раза (prev prio *2) относительно первой очереди, либо оставить такой же (same as prev prio);
- *Ограничение скорости для входящих пакетов в очереди 3* — ограничение полосы пропускания трафика, поступающего на порт для третьей очереди. Полосу пропускания можно либо увеличить в два раза (prev prio *2) относительно второй очереди, либо оставить такой же (same as prev prio);
- *Включить ограничение исходящих пакетов* — при установленном флаге разрешено ограничение полосы пропускания для исходящего с порта трафика;
- *Ограничение скорости для исходящих пакетов* — ограничение полосы пропускания для исходящего с порта трафика. Допустимые значения в пределах от 70 до 250000 килобит в секунду.

- *Применить* — применить установленные настройки;
- *Подтвердить* — подтвердить измененные настройки;

Если в течение одной минуты настройки не подтверждены нажатием на кнопку *«Подтвердить»*, то они возвращаются к предыдущим значениям.

- *По умолчанию* — установить настройки по умолчанию;
- *Сохранить* — сохранить настройки во Flash-память устройства без применения.

4.1.6.5 Распределение приоритетов по очереди

В разделе *«QoS и контроль полосы пропускания»* настраиваются функции обеспечения качества обслуживания (Quality of Service).

Коммутатор –> Распределение приоритетов по очереди

Распределение приоритетов по очередям

Распределение приоритетов 802.1p по очередям

802.1p	0	1	2	3	4	5	6	7
Очередь	1	0	0	1	2	2	3	3

Распределение приоритетов IP diffserv по очередям

Diffserv	Очередь	Diffserv	Очередь	Diffserv	Очередь	Diffserv	Очередь
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

Применить | Подтвердить | По умолчанию | Сохранить

- *Распределение приоритетов 802.1p по очередям* — позволяет распределить пакеты по очередям в зависимости от приоритета 802.1p.
  - *802.1p* — значение приоритета 802.1p;
  - *Очередь* — номер исходящей очереди.
- *Распределение приоритетов IP diffserv по очередям* — позволяет распределить пакеты по очередям в зависимости от приоритета IP diffserv.
  - *diffserv* — значение приоритета IP diffserv;
  - *Очередь* — номер исходящей очереди.

- *Применить* — применить установленные настройки;
- *Подтвердить* — подтвердить измененные настройки;

Если в течение одной минуты настройки не подтверждены нажатием на кнопку *«Подтвердить»*, то они возвращаются к предыдущим значениям.

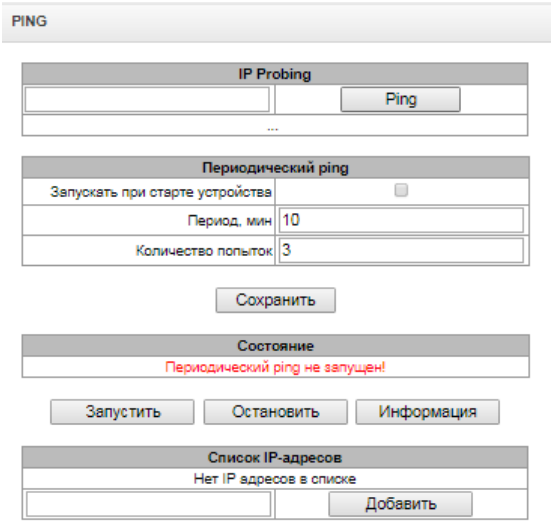
- *По умолчанию* — установить настройки по умолчанию;
- *Сохранить* — сохранить настройки во Flash-память устройства без применения.

4.1.7 *Сетевые утилиты*

4.1.7.1 PING

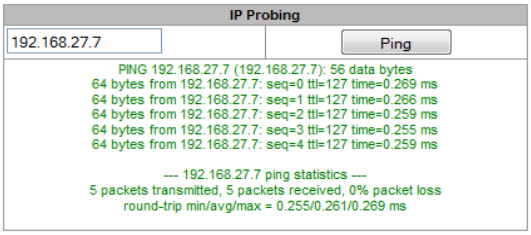
Утилита используется для проверки соединения (наличия маршрута) до устройства в сети.

Сетевые утилиты –> PING



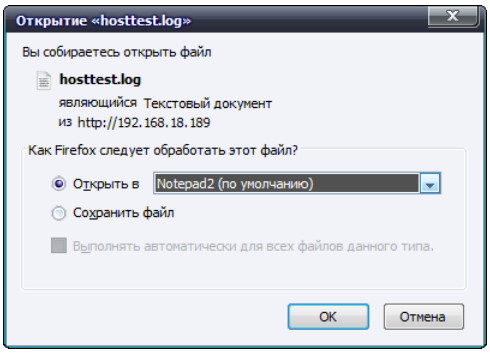
IP Probing **—** используется для однократного контроля соединения до устройства в сети.

Для эхо-теста (посыла *Ping-запроса)* необходимо ввести IP-адрес либо сетевое имя узла в поле *«IP probing»* и нажать кнопку *«Ping».* Результат выполнения команды будет выведен в нижней части страницы. В результате указывается количество переданных пакетов, количество полученных на них ответов, процент потерь, а также время приема-передачи (минимальное/среднее/максимальное) в миллисекундах.



Периодический ping **—** используется для периодического контроля соединений до устройств в сети.

- *Запускать при старте устройства* — при установленном флаге посылать ping-запросы на адреса, указанные в списке хостов будет активироваться сразу после запуска устройства;
- *Период, мин* — интервал между запросами в минутах;
- *Количество попыток* — число попыток отправить ping-запрос.



Состояние

- *Перезапустить* — запуск/перезапуск периодического ping;
- *Остановить* — принудительная остановка периодического ping;
- *Информация* — по нажатию данной кнопки для просмотра станет доступен лог-файл '/tmp/log/hosttest.log' с данными о последней попытке периодического ping-запроса.

Список хостов — список IP-адресов, на которые будут отправляться периодические ping-запросы.

Для добавления нового адреса в список необходимо указать его в поле ввода и нажать кнопку *«Добавить»*. Для удаления — нажать кнопку *«Удалить»* напротив требуемого адреса.

4.1.7.2 TRACEROUTE

Утилита **TRACEROUTE** выполняет функции трассировки маршрута и эхо-тестов (передачи ping-запросов) для диагностики работы сети. Данная функция позволяет оценить качество соединения до проверяемого узла.

Сетевые утилиты –> TRACEROUTE

TRACEROUTE

	Имя хоста или IP адрес для проверки качества соединения
Использовать опции	**Описание и дополнительные параметры**
☐	Число передаваемых пакетов (по умолчанию 10)
☐	Размер пакетов для отправки
☐	Отображать IP-адреса вместо имен хостов
☐	Задержка между ICMP запросами (по умолчанию 1 сек)
☐	Использовать только IPv4
☐	Использовать только IPv6
☐	Адрес сетевого интерфейса для отправки ICMP запросов

Проверить

В поле *«Имя хоста или IP-адрес для проверки качества соединения»* вводится IP-адрес сетевого устройства, до которого оценивается качество соединения. Для использования опций необходимо установить флаг в соответствующей строке.

Опции:

- *Число передаваемых пакетов* — количество циклов передачи ICMP-запросов;
- *Размер пакетов для отправки* — размер ICMP-пакета в байтах;
- *Отображать IP адреса вместо имен хостов* — не использовать DNS. Отображать IP-адреса без попыток получения их сетевых имен;
- *Задержка между ICMP запросами (по умолчанию 1сек)* — интервал опроса;
- *Использовать только IPv4* — использовать только протокол IPv4;
- *Использовать только IPv6* — использовать только протокол IPv6;
- *Адрес сетевого интерфейса для отправки ICMP запросов* — IP-адрес сетевого интерфейса, с которого будут отправлены ICMP запросы.

После ввода IP-адреса сетевого устройства, до которого оценивается качество соединения и установки опций нужно нажать кнопку *«Проверить»*.

В результате работы утилиты выводится таблица, содержащая:

- *номер узла и его IP-адрес (либо сетевое имя),*
- *процент потерянных пакетов (Loss%),*
- *количество отправленных пакетов (Snt),*
- *время кругового обращения последнего пакета (Last),*
- *среднее время кругового обращения пакета (Avg),*
- *лучшее время кругового обращения пакета (Best),*
- *худшее время кругового обращения пакета (Wrst),*

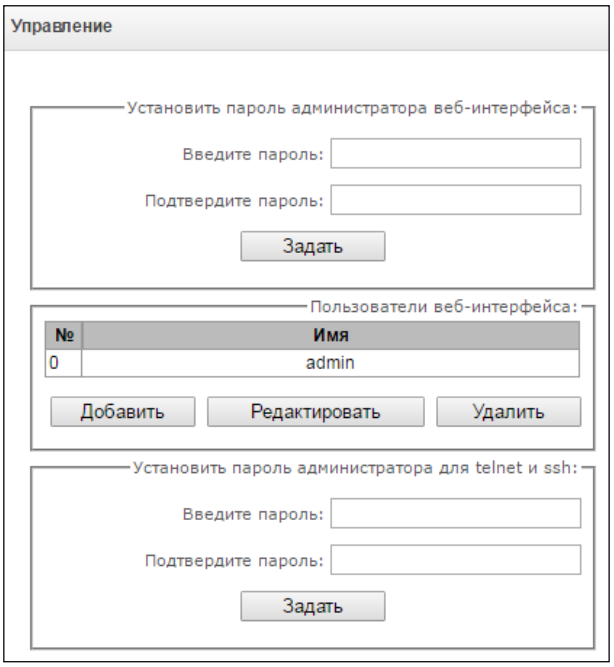
– *среднеквадратичное отклонение задержек для каждого узла (StDev).*

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 *Безопасность*

4.1.8.1 Управление

Безопасность –> Управление



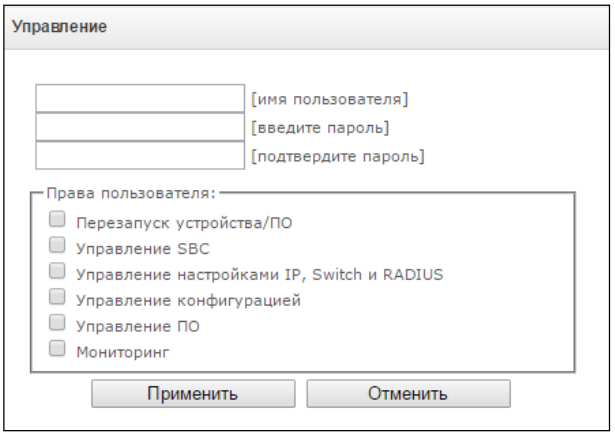
В этом подменю изменяются пароли доступа к средствам конфигурирования SBC.

В разделе *«Установить пароль администратора web-интерфейса»* устанавливается пароль для доступа к web-интерфейсу пользователя *admin*.

По умолчанию для доступа к web-интерфейсу используется логин *admin* пароль *rootpasswd*.

Пароль для доступа пользователя *admin* через web-интерфейс может не совпадать с паролем для доступа по протоколам Telnet, SSH.

В разделе *«Пользователи web-интерфейса»* создаются пользователи web-интерфейса и назначаются их права. Всего может быть создано до 10 пользователей.



Для создания пользователя следует нажать кнопку *«Добавить»*. В появившемся окне (справа) выбрать имя пользователя, пароль для входа и подтвердить пароль. Затем задать права пользователя и нажать *«Применить»*. Для редактирования надо выбрать пользователя из списка и нажать кнопку *«Редактировать»*. Удаление осуществляется выбором пользователя и нажатием кнопки *«Удалить»*.

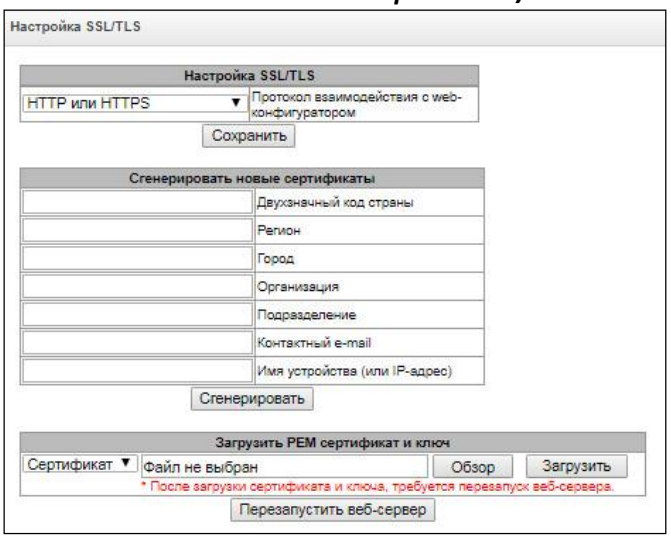
Невозможно удалить или изменить права пользователя *admin*.

В разделе *«Установить пароль администратора для telnet и ssh»* устанавливается пароль пользователя *admin* для доступа к CLI.

4.1.8.2 Настройка SSL/TLS

Раздел предназначен для загрузки или создания самоподписанного сертификата SSL/TLS, который позволяет использовать шифрованное подключение к шлюзу и загрузку/выгрузку файлов конфигурации по протоколу HTTPS.

Безопасность –> Настройка SSL/TLS



– *Протокол взаимодействия с web-конфигуратором* — режим подключения к Web-конфигуратору:

- *HTTP или HTTPS* — разрешено как нешифрованное подключение — по HTTP, так и шифрованное — по HTTPS. При этом подключение по HTTPS возможно только при наличии сгенерированного сертификата;
- *только HTTPS* — разрешено только шифрованное подключение по HTTPS. Подключение по HTTPS возможно только при наличии сгенерированного сертификата*;*

Сгенерировать новые сертификаты

Данные параметры необходимо вводить латинскими буквами.

– *Двухзначный код страны* — код страны (для России — RU);
– *Регион* — название региона, области, края, республики и т.п.;
– *Город* — название города;
– *Организация* — название организации;
– *Подразделение* — название подразделения или отдела;
– *Контактный e-mail* — адрес электронной почты;
– *Имя устройства (или IP-адрес)* — IP-адрес шлюза.

Загрузить PEM сертификат и ключ

Раздел позволяет загрузить заранее сгенерированный и подписанный PEM сертификат и ключ. Для загрузки следует выбрать в выпадающем меню тип загружаемого файла. Нажать кнопку *«Обзор»* и выбрать требуемый файл. После чего нажать кнопку *«Загрузить».*

После загрузки сертификата и ключа необходимо будет перезапустить веб-сервер кнопкой «Перезапустить веб-сервер».

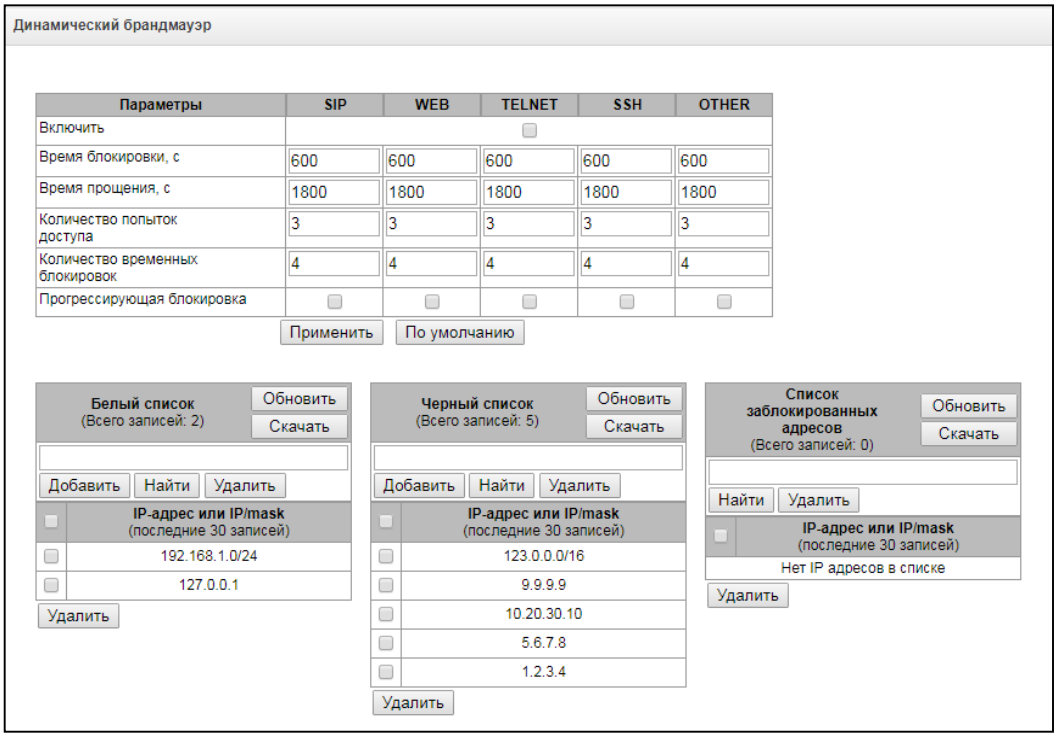
4.1.8.3 Динамический брандмауэр

Динамический брандмауэр — это утилита, которая отслеживает попытки обращения к различным сервисам. При обнаружении постоянно повторяющихся неудачных попыток обращения с одного и того же IP-адреса или хоста, динамический брандмауэр блокирует дальнейшие попытки с этого IP-адреса/хоста.

В качестве неудачных попыток могут быть идентифицированы:

- подбор аутентификационных данных для web-интерфейса или по протоколу SSH, то есть попытки зайти в интерфейс управления с неверным логином или паролем;
- подбор аутентификационных данных — прием запросов REGISTER с известного IP-адреса, но с неверными аутентификационными данными;
- прием запросов (REGISTER, INIVITE, SUBSCRIBE, и других) с неизвестного IP-адреса;
- прием неизвестных запросов по SIP-порту;
- попадание вызова в правило с политикой reject.

Безопасность –> Динамический брандмауэр



Параметры динамического брандмауэра

- *Включить* — запустить брандмауэр;

Следующие параметры могут настраиваться отдельно для различных сервисов. Все эти параметры могут быть сброшены в предустановленные значения кнопкой "По умолчанию".

- *Время блокировки, с* — время в секундах, на протяжении которого доступ с подозрительного адреса будет блокирован;
- *Время прощения, с* — время, через которое адрес, с которого пришел проблемный запрос, будет забыт, если ни разу не был заблокирован;
- *Количество попыток доступа* — максимальное число неудачных попыток доступа к сервису, прежде чем хост будет заблокирован;
- *Количество временных блокировок* — количество блокировок, после которых проблемный адрес будет принудительно занесен в черный список;
- *Прогрессирующая блокировка* — при установленном флаге каждая очередная блокировка адреса будет вдвое больше предыдущей, для блокировки адреса будет использоваться вдвое меньше

попыток доступа. Например, в первый раз адрес был заблокирован на 30 секунд после 16 попыток, во второй раз — на 60 секунд после 8 попыток, в третий раз — на 120 секунд после 4 попыток и так далее;

- Не отправлять заблокированные адреса в черный список — при установленном флаге SBC не отправляет заблокированные адреса в черный список, опция "Прогрессирующая блокировка" игнорируется.

Белый список (последние 30 записей) — список IP-адресов, которые не могут быть блокированы динамическим брандмауэром. Всего может быть создано до 4096 записей.

Черный список (последние 30 записей) — список запрещенных адресов, доступ с которых будет всегда заблокирован. Всего может быть создано до 8192 записи для SBC-1000 и 16384 записи для SBC-2000.

Для добавления/поиска/удаления адреса в списке необходимо указать его в поле ввода и нажать кнопку *«Добавить»/ «Найти» /«Удалить».*

Чёрный список имеет приоритет над белым.

Список заблокированных адресов — перечень адресов, заблокированных в ходе работы динамического брандмауэра. Всего в списке может быть 8192 записи для SBC-1000 и 16384 записи для SBC-2000.

В заголовке списков присутствуют две кнопки для их скачивания и обновления:

- *Скачать* — в Web-интерфейсе отображается только 30 последних записей в файле. Нажатие на данную кнопку позволяет скачать полные списки на компьютер;
- *Обновить* — обновить отображаемый список.

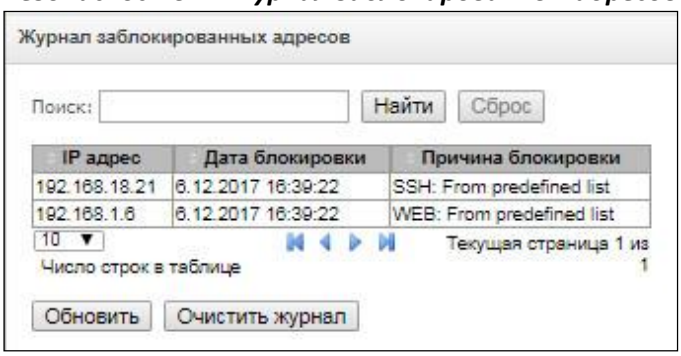
Для добавления/поиска адреса в списке необходимо указать его в поле ввода и нажать кнопку *«Добавить»/ «Найти»*, для удаления — нажать *«Удалить»*. Допускается указание как отдельного IP-адреса, так и подсети в нотации CIDR: 192.0.2.0/24. При удалении подсети будут также удалены одиночные адреса и подсети, входящие в эту подсеть.

Также для удаления адресов можно выбрать необходимые адреса с помочью флажков напротив и нажать кнопку *«Удалить»*, которая находится под списком.

4.1.8.4 Журнал заблокированных адресов

Данное подменю предназначено для просмотра журнала заблокированных динамическим брандмауэром адресов. Также в подменю возможно разблокировать определенные адреса путем удаления их из журнала. Журнал содержит до 10000 записей.

Безопасность –> Журнал заблокированных адресов



- *Поиск* — в поле указывается фильтр для поиска адресов;
- *Найти* — выборка адресов из журнала согласно фильтру;

- *Сброс* — очистка фильтра;
- *Обновить* — обновить информацию в журнале;
- *Очистить журнал* — удалить все записи из журнала заблокированных адресов. При этом будет произведена очистка журнала, но из блокировки адреса удалены не будут, это надлежит сделать в меню настройки динамического брандмауэра.

Журнал содержит информацию:

- *IP-адрес* — IP-адрес, который попадал в блокировку;
- *Дата блокировки* — дата и время попадания IP-адреса в блокировку;
- *Причина блокировки* — пояснение, каким сервисом и за что произведена блокировка;

В таблице ниже приведен список сообщений о блокировке и причины их возникновения.

Таблица 20 — Сообщения блокировки

Сообщение в журнале	Причина возникновения	Сообщение SIP
Request error: REGISTER failed : Resource limit overflow	Достигнут лимит регистраций динамических пользователей	Ответ 403
Request error: REGISTER failed : Unknown user or registration domain	Запрос регистрации неизвестного пользователя	Ответ 403
Request error: REGISTER failed : Server doesn’t allow a third party registration	Запрос регистрации, в котором заголовки To и From различны	Ответ 403
Request error: REGISTER failed : Authentication is wrong	Неверный логин/пароль	Ответ 403
Request error: REGISTER failed : Wrong de-registration	Попытка дерегистрации пользователем незарегистрированного контакта	Ответ 200
Request error: REGISTER failed : Request from disallowed IP	Попытка регистрации с адреса, отличного от разрешенного	Ответ 403
Request error: INVITE failed : No registration before	Попытка звонка от пользователя, который известен, но его контакт не был зарегистрирован	Ответ 403
Request error: INVITE failed : Registration is expired	Попытка звонка от пользователя, который известен, но регистрация его контакта истекла	Ответ 403
Request error: INVITE failed : Authentication is wrong	Входящий звонок или регистрация не прошли аутентификацию	Ответ 403
Request error: INVITE failed : Unknown original address	Звонок с неизвестного направления	Звонок направляется на mgapp, где принимается решение о его пропуске или отклонении
Request error: INVITE failed : RURI not for me	Неизвестное имя хоста или адрес в RURI	Ответ 404
Request error: BYE failed : Call/Transaction Does Not Exist	Не найден диалог для принятия запроса	Ответ 481
SIP: INVITE rejected by the rule id:name (%d:%s) : Forbidden — Blocked by SB	Запрос попал в правило с политикой reject	-
SSH: Too many requests from address	Неудачные попытки аутентификаций по SSH	-

Сообщение в журнале	Причина возникновения	Сообщение SIP
WEB: Unknown user <%s> attempted to access : password '%s'	Неудачные попытки аутентификации через WEB	-
ANY: Manually by cmd from other module or administrator	Блокировка добавлена через CLI или WEB администратором	-

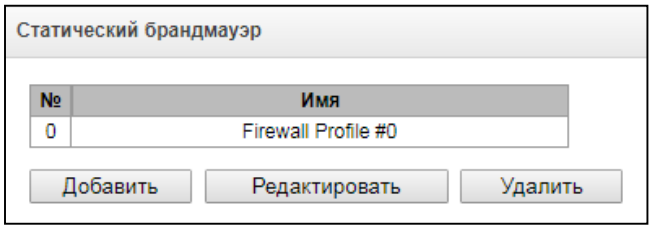
4.1.8.5 Статический брандмауэр

Firewall или ***сетевой экран*** — комплекс программных средств, осуществляющих контроль и фильтрацию передаваемых через него сетевых пакетов в соответствии с заданными правилами, что необходимо для защиты устройства от несанкционированного доступа. На устройстве может быть до 32 профилей.

Правила брандмауэра не будут работать на ограничение доступа по протоколам HTTP/HTTPS, SSH, Telnet, SNMP, FTP. Для ограничения доступа по этим протоколам воспользуйтесь списком разрешённых IP адресов (раздел 4.1.8.6) и настройками активации сервисов на сетевых интерфейсах (раздел 4.1.4.3).

Профили firewall

Безопасность –> Статический брандмауэр

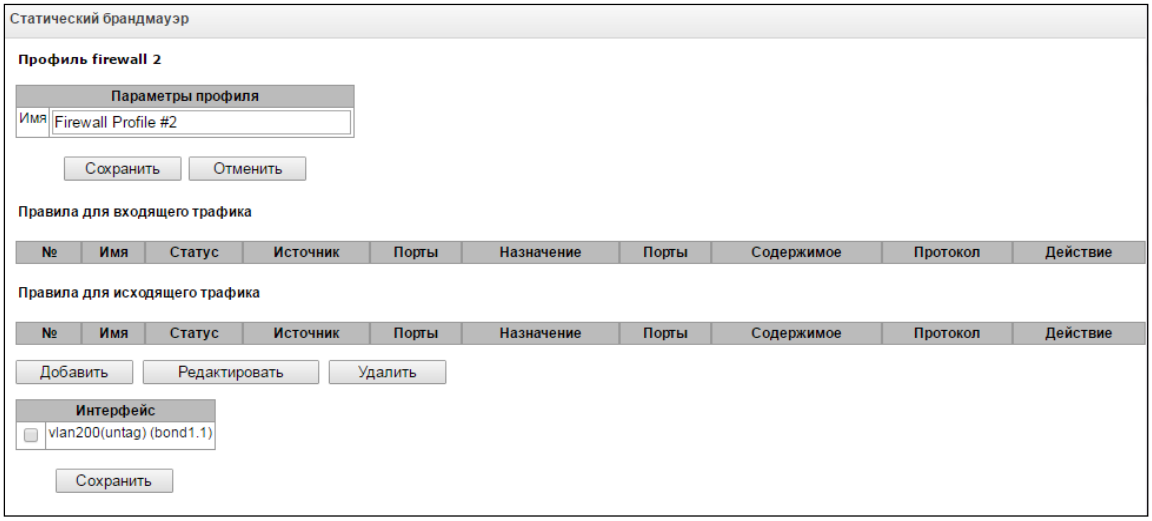


Для создания, редактирования и удаления профилей firewall используется меню *«Объекты» - «Добавить объект»*, *«Объекты» - «Редактировать объект»* и *«Объекты» - «Удалить объект»*, а также кнопки:

- *«Добавить»;*
- *«Редактировать»;*
- *«Удалить»*.

Программное обеспечение позволяет настроить правила firewall для входящего, исходящего и транзитного трафика, а также для определенных сетевых интерфейсов. Общее количество правил firewall едино на все профили и составляет 1000 правил.

Безопасность –> Статический брандмауэр –> «Добавить»

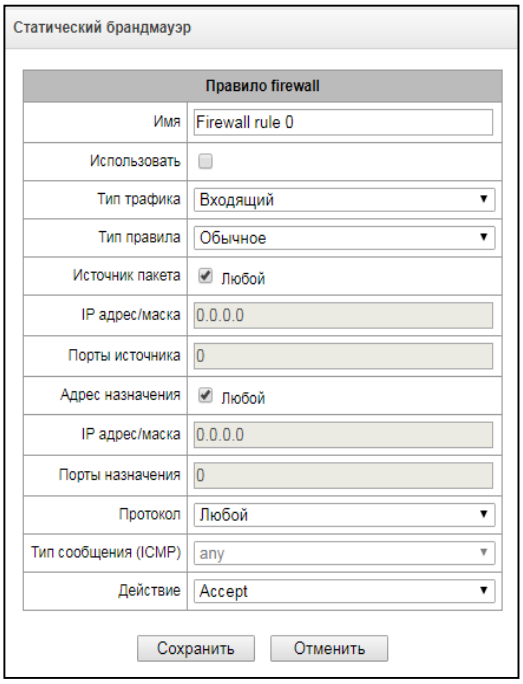


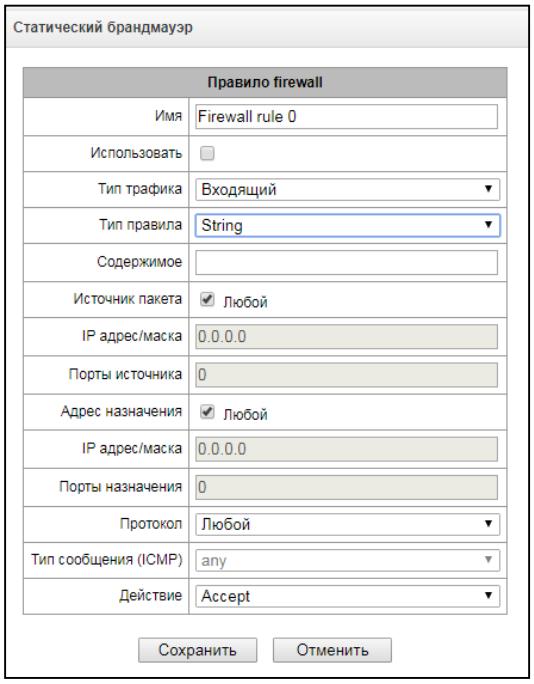
При создании правила настраиваются следующие параметры:

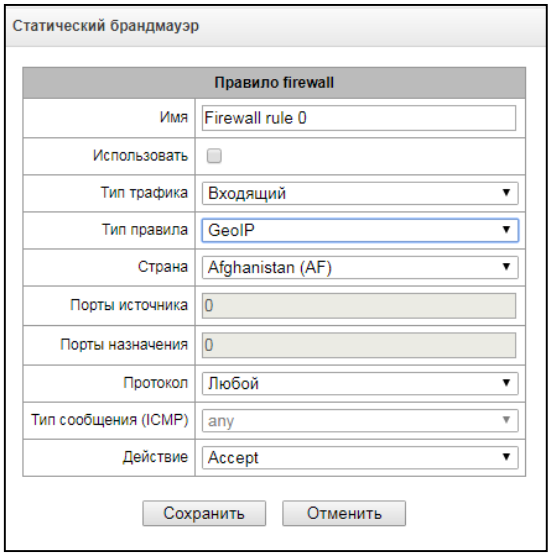
- *Имя* — имя правила;
- *Использовать* — определяет, будет ли использоваться правило. Если флаг не установлен, то правило будет неактивно;
- *Тип трафика* — тип трафика, для которого создается правило:
  - *входящий* — предназначенный для SBC;

  - *исходящий* — отправляемый SBC;
- *Тип правила* — может принимать значения:
  - *Обычное* — правило с проверкой IP-адресов и портов;
  - *GeoIP* — правило с проверкой адреса по базе GeoIP;
  - *String* — правило с проверкой вхождения строки в пакет;

Меню правила firewall в зависимости выбора типа правила



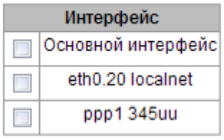




- *Источник пакета* — определяет сетевой адрес источника пакетов, либо для всех адресов, либо для конкретного IP-адреса или сети:
  - *любой* — для всех адресов (флаг установлен);
  - *IP адрес/маска* — для конкретного IP-адреса или сети. Поле активно при снятом флаге «любой». Для сети обязательно указывается маска, для IP-адреса указание маски не обязательно;
  - *Порты источника* — TCP/UDP порт или диапазон портов (указывается через тире «-») источника пакетов. Данный параметр используется только для протоколов TCP и UDP, поэтому, чтобы данное поле стало активным, необходимо выбрать в поле протокол UDP, TCP, либо TCP/UDP;
- *Адрес назначения* — определяет сетевой адрес приемника пакетов, либо для всех адресов, либо для конкретного IP-адреса или сети:

  - *любой* — для всех адресов (флаг установлен);
  - *IP адрес/маска* — для конкретного IP-адреса или сети. Поле активно при снятом флаге «любой». Для сети обязательно указывается маска, для IP-адреса указание маски не обязательно;
  - *Порты назначения* — TCP/UDP порт или диапазон портов (указывается через тире «-») приемника пакетов. Данный параметр используется только для протоколов TCP и UDP, поэтому, чтобы данное поле стало активным, необходимо выбрать в поле протокол UDP, TCP, либо TCP/UDP;
- *Протокол* — протокол, для которого будет использоваться правило: UDP, TCP, ICMP, либо TCP/UDP;
- *Тип сообщения (ICMP)* — тип сообщения протокола ICMP, для которого используется правило. Данное поле активно, если в поле *«Протокол»* выбран ICMP;
- *Действие* — действие, выполняемое данным правилом:
  - *ACCEPT* — пакеты, попадающие под данное правило, будут пропущены сетевым экраном firewall
  - *DROP* — пакеты, попадающие под данное правило, будут отброшены сетевым экраном firewall без какого либо информирования стороны передавшей пакет
  - *REJECT* — пакеты, попадающие под данное правило, будут отброшены сетевым экраном firewall, стороне, передавшей пакет, будет отправлен либо пакет TCP RST либо ICMP destination unreachable;
- *Страна* — выбор страны, к которой принадлежит адрес. Поле отображается только для правила типа "GeoIP";
- *Содержимое* — строка, которая должна содержаться в пакете. Строка будет искаться по содержимому пакета с учётом регистра. Поле отображается только для правила типа "String".

Созданное правило попадет в соответствующий раздел: *«Правила для входящего трафика», «Правила для исходящего трафика»* либо *«Правила для транзитного трафика»*.



Также в *профиле firewall* возможно указать сетевые интерфейсы, для которых будут использоваться правила данного профиля.

Каждый сетевой интерфейс может одновременно использоваться только в одном профиле firewall. При попытке назначения сетевого интерфейса в новый профиль из старого он будет удален.

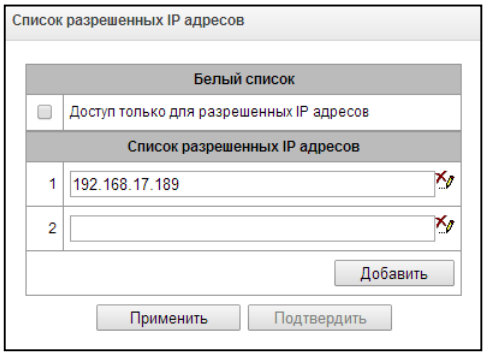
Для применения правил необходимо нажать на кнопку *«Применить»,* которая появится, если в настройках firewall были сделаны изменения.

4.1.8.6 Список разрешенных IP адресов

В данном разделе конфигурируется список разрешенных IP-адресов, с которых администратор может подключаться к устройству через web-конфигуратор, а также по протоколу Telnet и SSH. По умолчанию разрешены все адреса. Может быть указано до 255 адресов.

Безопасность –> Список разрешенных IP-адресов

- *Доступ только для разрешенных IP-адресов* — при установленном флаге доступ к устройству разрешен только с адресов из белого списка.



Для добавления адреса в таблицу «*Список разрешенных адресов»* необходимо нажать кнопку *«Добавить»* и в появившемся поле указать требуемое значение. После заполнения списка следует нажать кнопку *«Применить».*

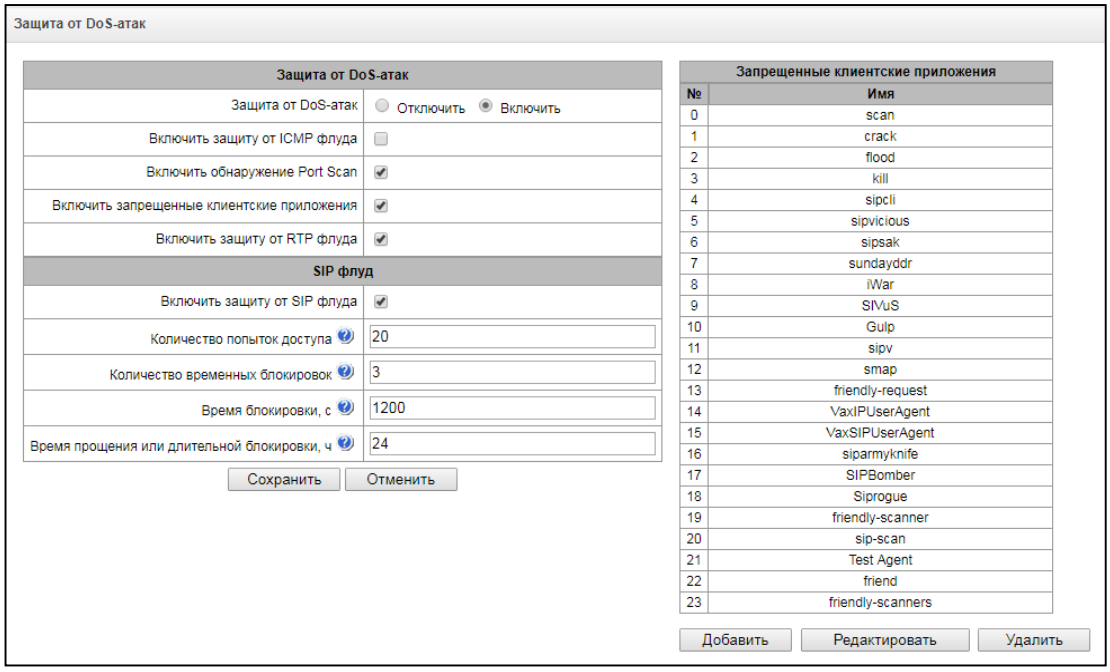
Удалить адреса из списка возможно, нажав иконку (*«Удалить»)* в выбранной строке.

При активации доступа только для разрешенных IP-адресов без занесения собственного IP-адреса в белый список доступ к устройству будет потерян.

4.1.8.7 Защита от DoS-атак

В этом меню конфигурируются опции защиты от DoS-атак.

Безопасность –> Защита от DOS-атак

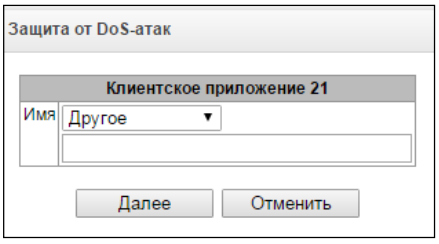


На SBC реализовано противодействие следующим атакам:

- *ICMP flood* — атака многочисленными ICMP-запросами;
- *Port Scan* — сканирование портов;
- *SIP flood* — атаки через SIP с целью подбора пароля пользователя, флуд запросами на запрещённое направление, защита от сканирования актуальных номеров;
- *RTP flood* — флуд на порты, используемые для передачи медиаданных с целью ухудшения качества услуг;
- *Фильтрация User-Agent* — SBC содержит запрещённый список стандартных User-Agent различных утилит, которые могут использоваться для организации атак по протоколу SIP. Поиск по User-Agent не зависит от регистра.

Настройка опций защиты:

- *Защита от DoS-атак* — общая настройка, активирующая все прочие защиты;
- *Включить защиту от ICMP флуда* — при активации SBC не будет отвечать на запросы ICMP тип 8 (echo) и ICMP тип 13 (timestamp);
- *Включить обнаружение Port Scan* — в этом режиме проверяется наличие слишком частых запросов к разным портам с одного адреса;
- *Включить запрещенные клиентские приложения* — фильтрация SIP запросов по User-Agent. При активации этой опции справа появится список запрещённых User-Agent. В этом списке можно:
  - Добавить новый User-Agent кнопкой "Добавить". Появится окно, где можно выбрать либо один из предустановленных вариантов, либо ввести свой, выбрав в выпадающем списке "другое";



  - Изменить любую позицию в списке. Для этого надо выделить позицию и нажать кнопку "Редактировать";
  - Удалить любую позицию в списке. Для этого надо выделить позицию и нажать кнопку "Удалить".
- *Включить защиту от RTP флуда* — активирует обнаружение хостов, отправляющих голосовой трафик на неактивные медиапорты, либо на медиапорты, которые уже используются для обмена голосовой информацией. Хост считается флудером, если производит посылку не ожидаемого трафика в течении более чем пяти секунд.

SIP флуд

- *Включить защиту от SIP флуда* — защита от подбора паролей пользователей и флуда запросами на запрещённое направление.
- *Количество попыток доступа* — по превышении какого числа попыток пользователь будет заблокирован. Можно задать от 1 до 32 попыток;
- *Количество временных блокировок* — количество временных блокировок, которые будут применены к пользователю. По превышении этого лимита будут применяться длительные блокировки. Можно задать от 1 до 10 блокировок;
- *Время блокировки, с* — время блокировки абонента, можно задать от 600 до 3600 секунд;
- *Время прощения или длительной блокировки, ч* — время длительной блокировки. Это же время прощения — по проишествии которого, будет сброшен счётчик попыток доступа. Можно задать от 12 до 48 часов.

4.1.8.8 Схема работы сетевой защиты SBC

На SMG работает следующий порядок отработки правил динамического и статического брандмауэра, списка запрещённых адресов и ограничения доступа с сетевых интерфейсов:

1. Производится отработка правил динамического брандмауэра (раздел 4.1.8.3). На этом этапе происходит сброс запросов от адресов, находящихся в чёрном списке и списке временных блокировок;

2. Отрабатываются ограничения доступа, настраиваемые в разделах 4.1.4.3 Сетевые интерфейсы -> Сервисы и 4.1.8.6 Список разрешённых IP-адресов. При неактивном списке разрешённых IP-адресов формируются правила, разрешающие доступ к управлению на адреса сетевых интерфейсов SMG, у которых есть разрешение на доступ в блоке "Сервисы". При активном списке разрешённых IP-адресов правила дополняются контролем IP-адреса источника — разрешено подключение только с адресов, указанных в списке;

3. Отрабатываются правила защиты SIP destination (раздел 4.1.3.2). Правила защиты для SIP destination формируются автоматически. По-умолчанию проверяется, что для протокола UDP доступ возможен только с указанного удалённого адреса и порта. Для протокола TCP (и для UDP при наличии опции "Не учитывать порт-источник при входящих вызовах") проверяется только удалённый адрес. В случае, если выставлена опция "Разрешить перенаправление", удалённый адрес не контроллируется — для ограничения доступа следует воспользоваться статическим брандмауэром;

4. Разрешается прочий доступ к сетевым интерфейсам, на которые нет привязки правил статического брэндмауэра;

5. Отрабатываются правила статического брандмауэра (раздел 4.1.8.5) на тех сетевых интерфейсах, к которым правила привязаны.

Если отработало одно из правил списка, то оставшиеся правила к запросу применяться не будут.

4.1.8.9 Обеспечение типовых задач сетевой защиты SBC

Ограничение доступа к управлению по протоколам WEB/Telnet/SSH/SNMP.

Для ограничения доступа к управлению следует воспользоваться настройками в разделах 4.1.4.3 Сетевые интерфейсы -> Сервисы и 4.1.8.6 Список разрешённых IP-адресов. Сначала на сетевых интерфейсах, куда необходимо разрешить доступ, выставляются флаги протоколов, по которым необходимо разрешить доступ. Таким образом будет выставлено ограничение по адресу назначения. После этого настраивается список разрешённых IP адресов, который дополнительно выставит ограничение по адресу источника по адресам из списка.

Ограничение доступа к интерфейсам SIP определёнными адресами и/ли географическими локациями.

По-умолчанию для SIP destination правила защиты создаются автоматически. Однако, если выставлена опция "Разрешить перенаправление", то правила созданы не будут. Также не создаются автоматически правила для SIP trunk. Для их защиты требуется настроить статический брандмауэр (раздел 4.1.8.5). На примере настройки доступа с такими ограничениями:

- Разрешить доступ из России;
- Разрешить доступ с подсети 34.192.128.128/28;
- Ограничить доступ с прочих адресов.

Для этого следует создать три правила статического брандмауэра в следующем порядке:

1 Правило для входящего трафика с типом "GeoIP" и страной "Russian Federation (RU)". Действие — Accept;

2 Правило для входящего трафика с типом "Обычное", IP-адресом и маской источника "34.92.128.128/255.255.255.240". Действие — Accept;

3 Правило для входящего трафика с типом "Обычное", источник пакета "Любой". Действие — Drop;

После этого выбрать в списке интерфейсов нужные сетевые интерфейсы и сохранить настройки.

Полное ограничение доступа к SMG с определённого адреса или подсети.

Такое ограничение можно реализовать, активировав динамический брэндмауэр (раздел 4.1.3.2) и внести адрес или подсеть в чёрный список. Обратите внимание — если адресов слишком много, то лучше пойти от обратного и создать правила статического брандмауэра (раздел 4.1.8.5) по принципу "сначала разрешить соединение доверенным узлам, затем отбросить всё" и настройками ограничения доступа через список разрешённых IP-адресов (раздел 4.1.8.6);

Автоматическая блокировка неудачных запросов/авторизаций

Выполняется динамическим брэндмауэром (раздел 4.1.3.2). Следует активировать динамический брандмауэр и настроить условия срабатывания. Также рекомендуется внести в белый список те адреса и подсети, к которым не должны применяться правила автоматической блокировки.

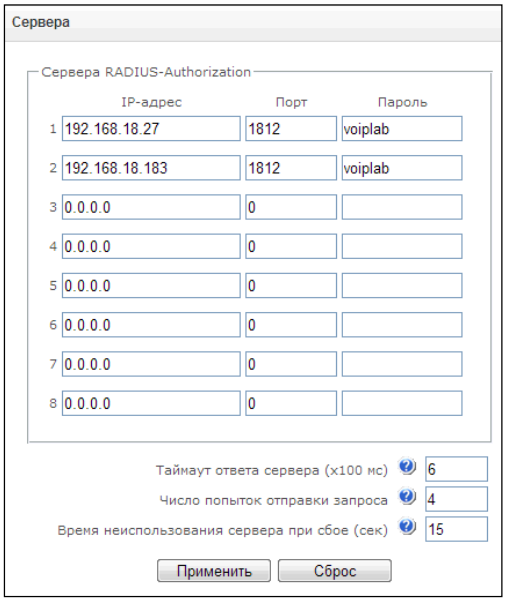
4.1.9 *Настройка RADIUS*

Шлюз поддерживает аутентификацию регистрирующихся через него абонентов и авторизацию вызовов с помощью RADIUS-сервера. При использовании RFC5090 параметры для digest-аутентификации (в сообщении ACCESS-CHALLENGE) шлюз получает от RADIUS сервера и пересылает их абоненту. При использовании RFC5090-no-challenge либо Draft Sterman шлюз самостоятельно отправляет абоненту параметры для digest-аутентификации, далее эти параметры и digest response, полученный от абонента, передает на RADIUS сервер для верификации.

Для использования авторизации с помощью RADIUS-сервера необходимо в настройках направления для SIP-пользователей (раздел SIP Destination) установить нужный профиль RADIUS.

4.1.9.1 Серверы RADIUS

RADIUS –> Серверы

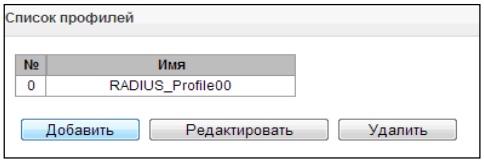


Устройство поддерживает до 8 серверов авторизации (Authorization).

- *Таймаут ответа сервера* — время, в течение которого ожидается ответ сервера;
- *Число попыток отправки запроса* — количество повторов запроса к серверу. При безуспешном использовании всех попыток сервер считается неактивным, и запрос перенаправляется на другой сервер, если он указан, иначе — детектируется ошибка;
- *Время неиспользования сервера при сбое* — время, в течение которого сервер считается неактивным (запросы на него не отправляются).

4.1.9.2 Список профилей

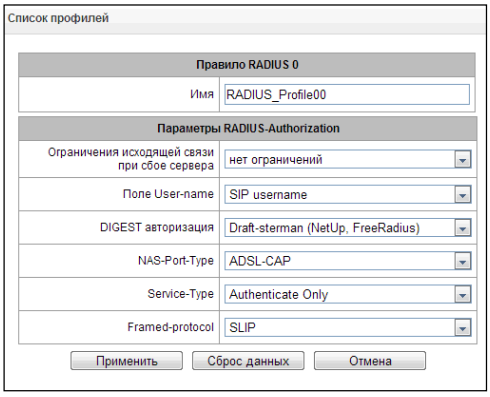
RADIUS –> Список профилей



Может быть создано до 32 профилей. Для создания, редактирования и удаления профилей RADIUS используется меню *«Объекты» - «Добавить объект», «Объекты» - «Редактировать объект»* и *«Объекты» - «Удалить объект»*, а также кнопки:

- *«Добавить»;*
- *«Редактировать»;*
- *«Удалить»*.

RADIUS –> Список профилей –> «Добавить»



Правило RADIUS N

– *Имя* — имя профиля;

Параметры RADIUS- Authorization:

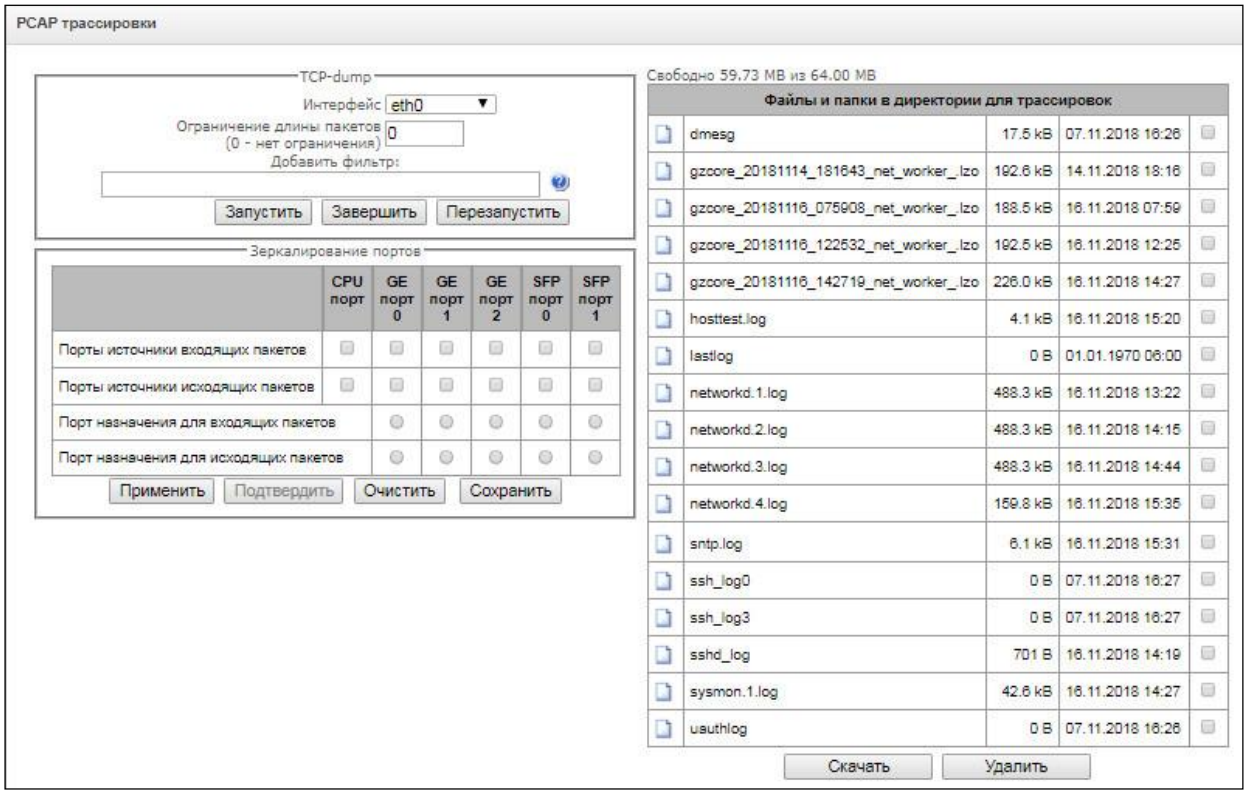
– *Ограничения исходящей связи при сбое сервера* — при сбое сервера (неполучении ответа от сервера) возможно установление ограничений на исходящую связь:
  – *нет ограничений* — разрешать все вызовы;
  – *все запрещено* — запрещать все вызовы.
– *Поле User-name* — выбор значения атрибута User-Name в соответствующем пакете авторизации Access Request (RADIUS-Authorization):
  – *SIP username* — в качестве значения использовать абонентский номер вызывающей стороны (username из поля from);
  – *IP address* — в качестве значения использовать IP-адрес вызывающей стороны;
  – *SIP interface name* — в качестве значения использовать имя SIP-сервера, через который осуществляется входящее занятие.
– *Использовать DIGEST User-name в запросах авторизации* — при включении опции в поле User-Name в RADIUS запросе будет использоваться DIGEST User-name при условии наличия digest записи в sip запросе, в ином случае — согласно настройке 'Поле User-name';
– *DIGEST авторизация* — выбор алгоритма авторизации абонентов через RADIUS-сервер. При дайджест-авторизации пароль передается не в открытом виде, как при использовании базовой аутентификации, а в виде хеш-кода и не может быть перехвачен при сканировании трафика*:*
  – *RFC5090* — полноценная реализация рекомендации RFC5090;
  – *RFC5090-no-challenge* — работа с сервером не передающим Access Challenge;
  – *Draft-sterman (NetUp, FreeRadius)* — работа по драфту, на основании которого была написана рекомендация RFC5090);
– *NAS-Port-Type* — тип физического порта NAS (сервера, где аутентифицируется пользователь), по умолчанию Async;
– *Service-Type* — тип услуги, по умолчанию не используется (Not Used);
– *Framed-protocol* — протокол, указывается при использовании пакетного доступа, по умолчанию не используется (Not Used).

4.1.10 *Трассировки*

4.1.10.1 PCAP трассировки

В меню производится настройка параметров для анализа сетевого трафика и протоколов TDM-сети.

Трассировки –> PCAP трассировки



TCP –dump — настройки для утилиты TCP–dump:

- *Интерфейс* — интерфейса для захвата сетевого трафика;
- *Ограничение длины пакетов (0 — нет ограничений)* — ограничение размера захватываемых пакетов, в байтах;
- *Добавить фильтр* — фильтр пакетов для утилиты tcpdump.

Структура выражений-фильтров

Каждое выражение, задающее фильтр, включает один или несколько примитивов, состоящих из одного или нескольких идентификаторов объекта и предшествующих ему классификаторов. Идентификатором объекта может служить его имя или номер.

Классификаторы объектов

1. **type** — указывает тип объекта, заданного идентификатором. В качестве типа объектов могут указываться значения:
   - **host** (хост),
   - **net** (сеть),
   - **port** (порт).

   Если тип объекта не указан, предполагается значение **host**.

2. **dir** — задает направление по отношению к объекту. Для этого классификатора поддерживаются значения:
   - **src** (объект является отправителем),
   - **dst** (объект является получателем),

– **src or dst** (отправитель или получатель),
– **src and dst** (отправитель и получатель).

Если классификатор **dir** не задан, предполагается значение **src or dst**.

Для режима захвата с фиктивного интерфейса **any** могут использоваться классификаторы **inbound** и **outbound**.

3. **proto** — задает протокол, к которому должны относиться пакеты. Этот классификатор может принимать значения:

   ether, **fddi1**, **tr2**, **wlan3**, **ip**, **ip6**, **arp**, **rarp**, **decnet**, **tcp** и **udp**.

   Если примитив не содержит классификатора протокола, предполагается, что данному фильтру удовлетворяют все протоколы, совместимые с типом объекта.

Кроме объектов и квалификаторов примитивы могут содержать арифметические выражения и ключевые слова:

- **gateway** (шлюз),
- **broadcast** (широковещательный),
- **less** (меньше),
- **greater** (больше).

Сложные фильтры могут содержать множество примитивов, связанных между собой с использованием логических операторов **and**, **or** и **not**. Для сокращения задающих фильтры выражений можно опускать идентичные списки квалификаторов.

Примеры фильтров:

- **dst foo** — отбирает пакеты, в которых поле адреса получателя IPv4/v6 содержит адрес хоста foo;
- **src net 128.3.0.0/16** — отбирает все пакеты Ipv4/v6, отправленные из указанной сети;
- **ether broadcast** — обеспечивает отбор всех широковещательных кадров Ethernet. Ключевое слово ether может быть опущено;
- **ip6 multicast** — отбирает пакеты с групповыми адресами IPv6.

Для получения более детальной информации о фильтрации пакетов обращайтесь к специализированным ресурсам.

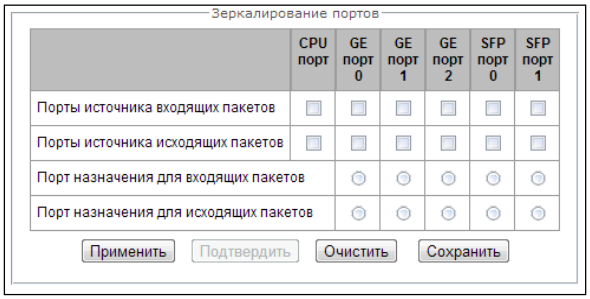
- *Запустить* — начать сбор данных;
- *Завершить* — закончить сбор данных;
- *Перезапустить* — перезапуск сбора данных.

После остановки захвата пакетов справа в списке файлов появится возможность выбрать для скачивания dump с указанного интерфейса на локальный компьютер.

Зеркалирование портов[1] — настройки зеркалирования трафика:

Зеркалирование портов позволяет скопировать с портов коммутатора шлюза принятые и переданные фреймы и направить их на другой порт.

[1] Только для SBC-1000



Для портов устройства возможны следующие действия:

- *Порты источника входящих пакетов* — копировать фреймы, принятые с данного порта (порт-источник);
- *Порты источника исходящих пакетов* — копировать фреймы, переданные данным портом (порт-источник);
- *Порт назначения для входящих пакетов* — порт-приемник для скопированных фреймов, принятых выбранными портами-источниками;
- *Порт назначения для исходящих пакетов* — порт-приемник для скопированных фреймов, переданных выбранными портами-источниками;

Применить — применить параметры настройки зеркалирования;
Подтвердить — подтвердить примененные параметры настройки зеркалирования;
Очистить — сбросить настройки зеркалирования;
Сохранить — сохранить параметры настройки зеркалирования.

Если в течение одной минуты настройки не подтверждены нажатием на кнопку *«Подтвердить»,* то они возвращаются к предыдущим значениям.

В блоке **Файлы и папки в директории** для трассировок доступен список файлов в соответствующей директории. Для сохранения трассировок может использоваться SSD-диск либо оперативная память устройства. В случае использования оперативной памяти запись осуществляется в директорию ***/tmp/log.***

Для скачивания на локальный ПК необходимо установить флаги напротив требуемых имен файлов и нажать кнопку *«Скачать».* Для удаления указанных файлов из директории — кнопку *«Удалить».*

4.1.10.2 SYSLOG

В меню *«SYSLOG»* производится настройка параметров системного журнала.

SYSLOG — протокол, предназначенный для передачи сообщений о происходящих в системе событиях. Программное обеспечение шлюза позволяет формировать журналы данных по работе приложений системы, работе протоколов сигнализации, авариям и передавать их на SYSLOG сервер.

Высокие уровни отладки могут привести к задержкам в работе устройства.
НЕ РЕКОМЕНДУЕТСЯ без необходимости использовать системный журнал.

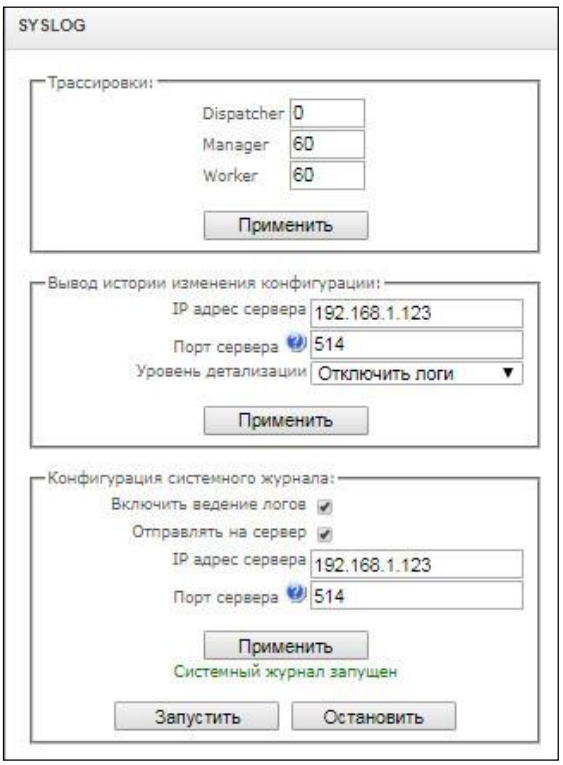
Системный журнал необходимо использовать только в случае возникновения проблем в работе шлюза для выявления их причин. Для того чтобы определиться с необходимыми уровнями отладки, рекомендуем Вам обратиться в сервисный центр ООО «Предприятие «ЭЛТЕКС».

Трассировки — используется для сохранения лога работы и взаимодействия узлов устройства, а также обмена сообщениями по различным протоколам.

В параметрах трассировок настраивается уровень трассировок по событиям и протоколам. Возможные уровни: 0 — выключено, 1-99 — включено. 1 — минимальный, 99 — максимальный уровень отладки.

- *Dispatcher* — логирование работы диспетчера процессов;
- *Manager* — логирование работы менеджера соединений и регистраций, управления RTP трафиком;
- *Worker* — логирование работы SIP-адаптера;

Вывод истории введенных командах — используется для сохранения истории изменений в настройках шлюза.



- *IP адрес сервера* — адрес сервера для сохранения журнала введенных команд;
- *Порт сервера* — порт сервера для сохранения журнала введенных команд;
- *Уровень детализации* — уровень детализации журнала введенных команд:
  - *Отключить логи* — не формировать журнал введенных команд;
  - *Стандартный* — в сообщениях передается название измененного параметра;
  - *Полный* — в сообщениях передается название измененного параметра и значения параметра до и после изменения.

Конфигурация системного журнала — настройки конфигурации системного журнала для передачи событий, касающихся доступа к устройству.

В параметрах syslog настраивается IP-адрес syslog-сервера, UDP порт, на который syslog-сервер принимает сообщения.

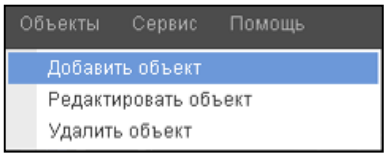
- *Включить ведение логов* — включить ведение журнала событий;
- *Отправлять на сервер* — при установленном флаге запись журнала будет вестись на сервере, IP-адрес которого настраивается ниже, иначе журнал будет сохраняться в оперативную память (размер

журнала ограничен 5 Мб, кроме того, записи в журнале сохраняются только до перезагрузки устройства). Сохранение журнала в оперативную память не рекомендуется к использованию.

– *IP адрес сервера* — адрес сервера для сохранения журнала событий;
– *Порт сервера* — порт сервера для сохранения журнала событий.

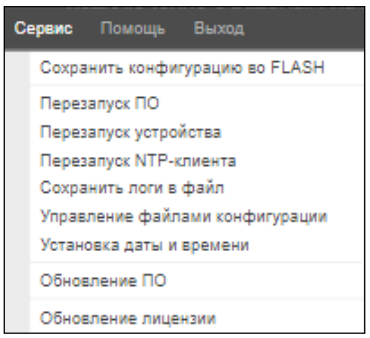
Кнопки *«Запустить»* и *«Остановить»* позволяют соответственно запускать и останавливать передачу журнала на сервер.

4.1.11 *Работа с объектами и меню «Объекты»*



Помимо применения иконок создания, редактирования и удаления объектов в соответствующих вкладках, существует возможность выполнить действия на указанном объекте с помощью соответствующих пунктов меню «Объекты».

4.1.12 *Сохранение конфигурации и меню «Сервис»*



Для отмены всех изменений необходимо выбрать меню *«Сервис» - «Отменить все изменения»*.

Для записи конфигурации в энергонезависимую память устройства необходимо выбрать меню *«Сервис» - «Сохранить конфигурацию во FLASH»*.

Для перезапуска ПО устройства необходимо выбрать меню *«Сервис» - «Перезапуск ПО»*.

Для полного перезапуска устройства необходимо выбрать меню *«Сервис» - «Перезапуск устройства»*.

Для принудительной пересинхронизации времени от сервера необходимо выбрать меню *«Сервис» - «Перезапуск NTP клиента»*.

Для формирования и сохранения логов на устройстве необходимо выбрать меню "Сервис" - "Сохранить логи в файл". Архив с логами можно найти в разделе PCAP трассировки — файлы и папки в директории для трассировок.

Пример названия архива:

sbc_logs_current_calls_20201111_165508.tar.gz

Для принудительного перезапуска SSHD необходимо выбрать меню *«Сервис» - «Перезапуск SSHD*[1]*»*.

Для считывания/записи основного файла конфигурации устройства надо выбрать меню «*Сервис» - «Управление файлами конфигурации»*.

Для сброса конфигурации устройства необходимо выбрать меню «*Сервис» - «Управление файлами конфигурации»* и нажать кнопку *«Сброс»*. При этом будут сброшены все настройки за исключением сетевых параметров, сетевых интерфейсов, сетевых маршрутов, профилей и правил firewall, списка разрешённых IP-адресов и сервера времени (NTP). Для полного сброса к заводским настройкам обратитесь к разделу 2.6 кнопки.

Для ручной настройки локальных даты и времени на устройстве необходимо выбрать меню *«Сервис»*

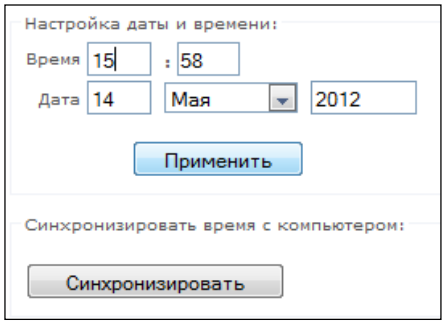
[1] Только для SBC-1000

- *«Установка даты и времени»*, подробнее в пункте 4.1.13 Настройка даты и времени.

Для обновления ПО через Web-интерфейс необходимо выбрать меню «*Сервис*» - *«Обновление ПО»,* подробнее в пункте 4.1.14 Обновление ПО через web-интерфейс.

Для обновления/добавления лицензий необходимо выбрать меню «*Сервис*» - *«Обновление лицензии»,* подробнее в пункте 4.1.15 Лицензии.

4.1.13 *Настройка даты и времени*

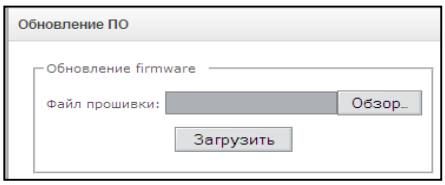


В соответствующих полях возможно задать системное время в формате ЧЧ:ММ и дату в формате ДД.месяц.ГГГГ.

Для сохранения настроек следует воспользоваться кнопкой «*Применить*».

По нажатию на кнопку *«Синхронизировать»* происходит синхронизация системного времени устройства с текущим временем на локальном ПК.

4.1.14 *Обновление ПО через web-интерфейс*



Для обновления ПО устройства необходимо использовать меню *«Сервис» - «Обновление ПО»*.

Откроется форма для загрузки файлов ПО на устройство:

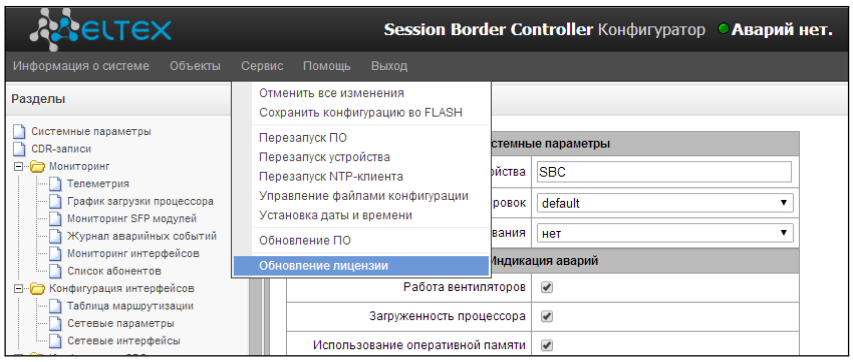
– *Обновление firmware* — обновляет ПО управляющей программы и/или ядро Linux.

Для обновления ПО необходимо в поле «*Файл прошивки*» при помощи кнопки «*Обзор*» указать название файла для обновления и нажать кнопку «*Загрузить*». После завершения операции - перезагрузить устройство через меню *«Сервис» - «Перезапуск устройства»*.

4.1.15 *Лицензии*

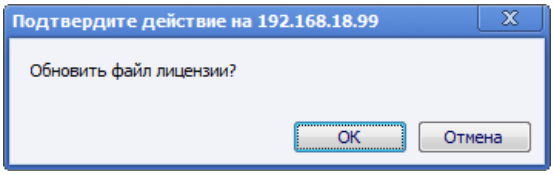
Для обновления/ добавления лицензий необходимо получить файл лицензии, обратившись в коммерческий отдел ООО «Предприятие «ЭЛТЕКС» по адресу eltex@eltex-co.ru или по телефону +7(383) 274-48-48, указав серийный номер и MAC-адрес устройства (подробнее в разделе 4.1.17).

Далее в меню *«Сервис»* выбрать параметр *«Обновление лицензии»*.



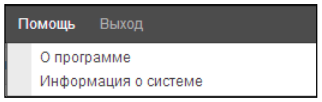
С помощью кнопки *«Выберите файл»* указать путь к файлу лицензии, полученному от производителя, и обновить, нажав *«Обновить».*

Для обновления файла лицензии требуется подтверждение.



После завершения операции будет предложено перезагрузить устройство либо это необходимо сделать через меню *«Сервис» - «Перезапуск устройства»*.

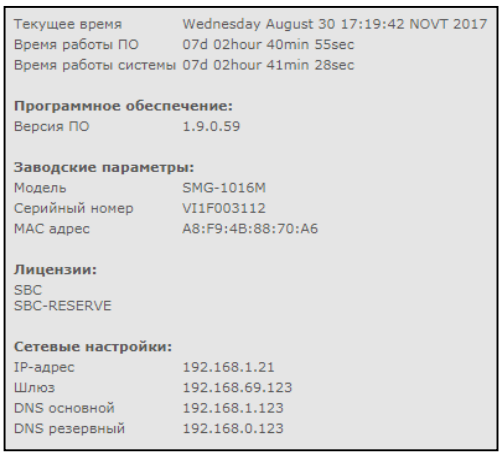
4.1.16 *Меню «Помощь»*



Меню предоставляет сведения о текущей версии программного обеспечения, заводские параметры и другую системную информацию, а также возможность получить самую новую версию документации с сайта http://eltex.org.

4.1.17 *Просмотр заводских параметров и информации о системе*

Для просмотра необходимо использовать меню *«Помощь» - «Информация о системе»*.

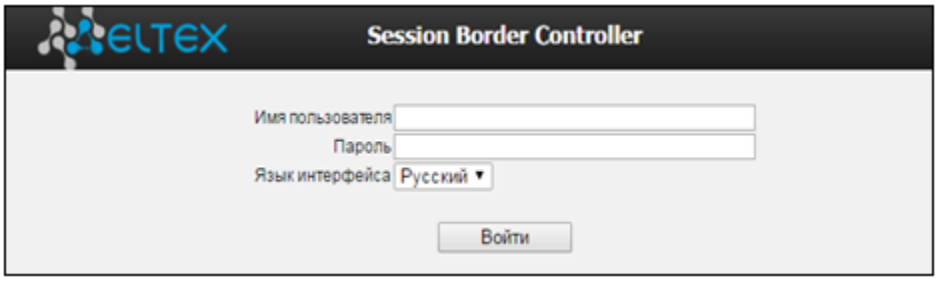


Заводские параметры (Серийный номер и MAC адрес) также указаны в шильде (наклейке) на нижней части корпуса изделия.

Подробная информация о системе (заводские параметры, версия SIP-адаптера, текущая дата и время, время в работе, сетевые настройки, температура внутри корпуса) доступна по нажатию на ссылку *«Информация о системе»* на панели управления.

4.1.18 *Выход из конфигуратора*

При нажатии на ссылку *«Выход»* на панели отобразится следующее окно:



Для возобновления доступа необходимо указать установленные имя пользователя и пароль и нажать кнопку *«Вход»*. По нажатию кнопки *«Отмена»* осуществится выход из программы конфигурирования.

4.2 Настройка SBC через Telnet, SSH или RS-232

Для того чтобы произвести конфигурирование устройства, необходимо подключиться к нему с помощью протокола Telnet, SSH, либо кабелем через разъем RS-232 (при доступе используется консоль). При заводских установках адрес: **192.168.1.2**, маска **255.255.255.0**.

Конфигурация устройства хранится в текстовом виде в файлах, находящихся в каталоге ***/etc/config*** (для выхода в linux наберите команду sh)**,** которые можно редактировать с помощью встроенного текстового редактора joe (такие изменения вступят в силу после перезагрузки устройства).

Для сохранения конфигурации в энергонезависимую память устройства необходимо выполнить команду **save**.

При первом запуске имя пользователя: ***admin***, пароль: ***rootpasswd*.**

4.2.1 *Перечень команд CLI*

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
alarm global			Показать информацию о текущих авариях
alarm list clear			Очистить журнал аварийных событий
alarm list show			Показать журнал аварийных событий с указанием типа и статуса аварии, времени возникновения и параметров локализации.
config			Переход в режим конфигурирования параметров устройства
CPU load statistic			Показать статистику загрузки CPU за последнюю минуту
date	<DAY> <MONTH> <YEAR> <HOURS> <MINS>	1-31 1-12 2011-2037 00-23 00-59	Установить локальные дату и время на устройстве.
firmware update tftp	<FILE> <SERVERIP>	имя файла с ПО IP- адрес в формате AAA.BBB.CCC.DDD	Обновление программного обеспечения без автоматической перезагрузки шлюза FILE — имя файла с ПО SERVERIP — IP-адрес TFTP сервера
firmware update ftp	<FILE> <SERVERIP>	имя файла с ПО IP- адрес в формате AAA.BBB.CCC.DDD	Обновление программного обеспечения без автоматической перезагрузки шлюза FILE — имя файла с ПО SERVERIP — IP-адрес FTP сервера
firmware update usb	<FILE>	имя файла с ПО	Обновление программного обеспечения без автоматической перезагрузки шлюза FILE — имя файла с ПО
firmware update_and_reboot tftp	<FILE> <SERVERIP>	имя файла с ПО IP- адрес в формате AAA.BBB.CCC.DDD	Обновление программного обеспечения с автоматической перезагрузкой шлюза FILE — имя файла с ПО SERVERIP — IP-адрес TFTP сервера
firmware update_and_reboot ftp	<FILE> <SERVERIP>	имя файла с ПО	Обновление программного обеспечения с автоматической перезагрузкой шлюза

		IP- адрес в формате AAA.BBB.CCC.DDD	FILE — имя файла с ПО SERVERIP — IP-адрес FTP сервера
firmware update_and_reboot usb	<FILE>	имя файла с ПО	Обновление программного обеспечения с автоматической перезагрузкой шлюза FILE — имя файла с ПО
get_logs			Формирование и сохранение логов на устройстве
history			Просмотр истории о введенных командах
license download	<FILE> <SERVERIP>	имя файла лицензии IP-адрес сервера в формате AAA.BBB.CCC.DDD	Загрузить файл лицензии с указанного адреса
license update			Обновить лицензию
license reset	no/yes		Удалить все установленные лицензии
password			Смена пароля для доступа через CLI
quit			Завершить данную сессию CLI
reboot	<YES_NO>	yes/no	Перезагрузить устройство
sh			Перейти из CLI в Linux Shell
show environment			Просмотр информации о состоянии аппаратного обеспечения
show system info			Просмотр информации о программном обеспечении
sntp retry			Отправка SNTP запроса к серверу для синхронизации времени
space hint	<SPACE>	yes/no	Включение и отключение подсказки при нажатии клавиши "пробел"
tcpdump	<DEVICE> <FILE> <SNAPLEN>	eth0/eth1/local строка 0-65535	Захватить пакеты с Ethernet-устройства DEVICE — интерфейс для мониторинга; FILE — файл для записи пакетов; SNAPLEN — число байт, захватываемое из каждого пакета. (0 — пакет захватывается полностью).
tftp get	<REMOTE_FILE> <LOCAL_FILE> <SERVERIP>	строка строка IP- адрес в формате AAA.BBB.CCC.DDD	Закачать файл по TFTP на SBC.
tftp put	<LOCAL_FILE> <REMOTE_FILE> <SERVERIP>	строка строка IP- адрес в формате AAA.BBB.CCC.DDD	Залить файл на TFTP. Команда предназначена для скачивания трассировок, снятых командами tcpdump и pcmdump.

4.2.2 *Смена пароля для доступа к устройству*

Поскольку к шлюзу можно удаленно подключиться через Telnet, то во избежание несанкционированного доступа рекомендуется сменить пароль для пользователя ***admin***.

Для этого необходимо:

1) Подключиться к шлюзу, авторизоваться по логину/паролю, ввести команду **`password`** и нажать клавишу **<Enter>**.
2) Ввести новый пароль:
   New password:
3) Повторить введенный пароль:
   Retype password:
   Пароль изменен (Password for admin changed by root)

4) Сохранить конфигурацию во Flash: ввести команду **save** и нажать клавишу **<Enter>**.

4.2.3 *Режим просмотра активных сессий*

В этом режиме имеется возможность просмотреть детальную информацию по установленным через SBC соединениям, включая статистику RTP, информацию из SDP и трассировку сигнализации в вызове.

4.2.3.1 Включение/отключение режима

Команда	Действие
statistics call_sessions enable	Включение мониторинга активных сессий
statistics call_sessions disable	Отключение мониторинга активных сессий

4.2.3.2 Просмотр активных сессий

Для работы с данными командами необходимо включить мониторинг активных сессий (раздел 4.2.3.1).

Команда	Параметр	Значение	Действие
show call list			Просмотр списка активных соединений
show call info	CALL_ID	0-65520.0-5	Просмотр общей информации о выбранном вызове
show call info detailed	CALL_ID	0-65520.0-5	Просмотр детальной информации по выбранному вызову
show call info RTP	CALL_ID	0-65520.0-5	Просмотр статистики по RTP-протоколу в выбранном вызове
show call info SDP	CALL_ID	0-65520.0-5	Просмотр информации SDP в выбранном вызове

4.2.4 *Просмотр активных регистраций*

Команда	Параметр	Значение	Действие
show registration list			Просмотр активных регистраций и блокировок
show registration info	SEARCH_LINE	строка	Поиск по активным регистрациям и блокировками
registration show json			Вывести все активные регистрации в формате json
registration show info	<REG_INDEX>	целое число	Показать подробную информацию о регистрации

4.2.5 *Управление регистрациями*

Команда	Параметр	Значение	Действие
registration del	<REG_INDEX>	0-4095/all	Удалить регистрацию абонента
registration unblock	<REG_INDEX>	0-4095	Разблокировать абонента

4.2.6 *Работа со статистикой SIP*

4.2.6.1 Включение/отключение режима

Команда	Действие
statistics sip_counters enable	Включение счётчиков статистики SIP
statistics sip_counters disable	Отключение счётчиков статистики SIP

4.2.6.2 Просмотр статистики

Команда	Параметр	Значение	Действие
show counters list transport			Показать список сконфигурированных SIP транспортов
show counters list destination			Показать список сконфигурированных SIP destination
show counters list users			Показать список сконфигурированных SIP users
show counters total			Показать счётчики статистики для всей SBC
show counters transport	<TRANSPORT_IDX>	0-255	Показать счётчики статистики для SIP транспорта
show counters destinations	<DESTINATIONS_IDX>	0-255	Показать счётчики статистики для SIP destination
show counters users	<USERS_IDX>	0-255	Показать счётчики статистики для SIP users

4.2.7 Режим конфигурирования

4.2.7.1 Режим конфигурирования общих параметров устройства

Для перехода к конфигурированию/мониторингу параметров устройства необходимо выполнить команду **config**.

SBC> config
Entering configuration mode.
SBC-[CONFIG]>

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
alarm show			Просмотр настроек отображения аварий
alarm set cps	invite/other/subscribe	yes/no	Изменение режима отображения аварии ограничения обработки запросов INVITE/OTHER/SUBSCRIBE
alarm set cpu	<set>	yes/no	Изменение режима отображения аварии высокой загрузки CPU
alarm set fans	<set>	yes/no	Изменение режима отображения аварии вентиляторов
alarm set ram	<set>	yes/no	Изменение режима отображения аварии занятости ОЗУ
alarm set rom	<set>	yes/no	Изменение режима отображения аварии занятости ПЗУ
alarm set reserve	<set>	yes/no	Изменение режима отображения аварий резерва
autoupdate			Переход в режим конфигурирования автоматического обновления ПО и конфигурации
copy running_to_startup			Записать текущую конфигурацию в энергонезависимую память устройства (в стартовую конфигурацию)
copy startup_to_running			Восстановить текущую конфигурацию из стартовой.
dos-protection			Вход в режим конфигурирования защиты от DoS
firewall dynamic			Переход в режим конфигурирования динамического брандмауэра
firewall static			Переход в режим конфигурирования статического брандмауэра
global set	Invite-per-3-sec/other-per-3-sec/subscribe-per-3-sec	60-300	Ограничение обработки запросов INVITE/OTHER/SUBSCRIBE

	<INVITE/OTHER/SUBSCRIBE_RESTRICT>		
global set media-security-timeout	<SECURITY_TIMEOUT>	1-10080	Защитный таймаут для отбоя вызовов без media, мин
global set not-encode-hash		yes/no	Включение опции передавать символ '#' без кодирования
history			Просмотр истории введенных команд
hostping			Переход в режим работы с утилитой ping
log path	<apply> <set> <show>	local /mnt/sd[abc][1-7]*	Применить настройки пути к хранению трассировок. Настройка пути к хранению трассировок: local — локальное хранение в оперативной памяти; /mnt/sd[abc][1-7]* — путь до накопителя для хранения трассировок Просмотр настройки пути к хранению трассировок
network			Переход в режим конфигурирования сетевых параметров
ports start	START_PORT	1024-65535	Установка начального порта для RTP
ports range	RANGE_PORT	1-65535	Установка количества портов для RTP
ports show			Просмотр настройки портов для RTP
quit			Завершить данную сессию CLI
radius			Переход в режим конфигурирования RADIUS
reserve			Переход в режим управления резервом
route			Переход в режим конфигурирования статических маршрутов
rule set			Переход в режим конфигурирования rule set
switch			Переход в режим конфигурирования коммутатора (только для SBC-2000 и SBC-3000)
show running main by_step			Показать текущую основную конфигурацию по шагам
show running main whole			Показать текущую основную конфигурацию полностью
show running network			Показать текущую конфигурацию сети
show running radius_servers			Показать текущую конфигурацию RADIUS-серверов
show running snmp			Показать текущую конфигурацию SNMP
show startup main by_step			Показать начальную основную конфигурацию по шагам
show startup main whole			Показать начальную основную конфигурацию полностью
show startup network			Показать начальную конфигурацию сети
show startup radius_servers			Показать начальную конфигурацию RADIUS-серверов
sip destination			Переход в режим конфигурирования SIP destination
sip transport			Переход в режим конфигурирования SIP transport
sip users			Переход в режим конфигурирования SIP users
snmp			Переход в режим конфигурирования SNMP

switch			Переход в режим конфигурирования внутреннего коммутатора
syslog			Переход в режим конфигурирования параметров системного журнала
top			Возврат на уровень выше
trunk			Переход в режим конфигурирования транков
user agent			Переход в режим редактирования списка запрещённых клиенских приложений

4.2.7.2 Режим конфигурирования автоматического обновления ПО и конфигурации

Для перехода в режим конфигурирования необходимо выполнить команду **autoupdate**.

SBC-[CONFIG]> autoupdate
Entering auto-update mode.
SBC-[CONFIG]-[AUTO-UPDATE]>

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
exit			Переход из данного подменю конфигурирования на уровень выше
quit			Завершить данную сессию CLI
set auth-name	AUTH_NAME	Строка длиной не более 63 символов	Задать имя аутентификации
set auth-pass	AUTH_PASS	Строка длиной не более 63 символов	Задать пароль аутентификации
set authentication	AUTH	on/off	Включение аутентификации на сервере автообновления
set config-name	CFG_NAME	Строка длиной не более 63 символов	Задать имя файла конфигурации. Имя обязательно должно иметь расширение «. cfg"
set enable	EN	on/off	Включить функцию автообновления
set manifest-name	MANIFEST_NAME	Строка длиной не более 63 символов	Задать имя файла версий ПО. Имя обязательно должно иметь расширение «. manifest"
set protocol	PROTO	tftp ftp http https	Указать протокол, который будет использоваться для обновления
set source	NET_IFACE_IDX static	0-39	Задать интерфейс, с которого будет получен адрес сервера (DHCP option 66) и имена файлов конфигурации и версий ПО (DHCP option 57) Если задать static, то информация о сервере и именах файлов будет взята из конфигурации SBC
set static-server	ST_SERVER	Строка длиной не более 63 символов	Задать адрес сервера автообновлений
set update-config	UCONF	on/off	Включить автообновление конфигурации
set update-firmware	UFIRM	on/off	Включить автообновление ПО
set updating-period config	UPD_CONFIG	1-263520	Задать период обновления конфигурации в минутах
set updating-period manifest	UPD_MANIFEST	1-263520	Задать период обновления ПО в минутах
show auto-update-config			Показать конфигурацию автообновления
show net-interfaces			Показать список сетевых интерфейсов, на которых активирован DHCP

4.2.7.3 Режим конфигурирования защиты от DoS

Для перехода в данный режим необходимо в режиме конфигурирования выполнить команду **dos-protection**.

SBC2000-[CONFIG]> dos-protection
Entering dos-protection mode.
SBC2000-[CONFIG]-[DOS-PROTECTION]>

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
exit			Переход из данного подменю конфигурирования на уровень выше
quit			Завершить данную сессию CLI
set enable ICMP_flood	ENABLE	true/false	Активировать защиту от ICMP флуда
set enable PortScan	ENABLE	true/false	Активировать защиту от сканирования портов
set enable protection	ENABLE	true/false	Опция управляет глобальным включением функций защиты от DoS
set enable RTP_flood	ENABLE	true/false	Активировать защиту от RTP флуда
set enable SIP_flood	ENABLE	true/false	Активировать защиту от SIP флуда
set enable User_Agent_filter	ENABLE	true/false	Активировать фильтрацию по User-Agent
set SIP_flood block time	BLOCKTIME	600-3600	Установить время короткой блокировки абонента, секунды
set SIP_flood blocks	BLOCKS	1-10	Установить число попаданий в короткую блокировку перед попаданием в длительную
set SIP_flood forget_time	FORGETTIME	12-48	Установить время длительной блокировки и время прощения абонента, попавшего в короткую блокировку, часы
set SIP_flood	HITS	1-32	Установить число нарушений перед попаданием в короткую блокировку
show			Показать настройки защиты от DoS

4.2.7.4 Режим конфигурирования параметров динамического брандмауэра

Для перехода в данный режим необходимо в режиме конфигурирования выполнить команду **firewall dynami**c.

SBC-[CONFIG]> firewall dynamic
Entering dynamic firewallmode.
SBC-[CONFIG]-[DYN-FIREWALL]>

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
blacklist add	<BLACKIP>	IP- адрес в формате AAA.BBB.CCC.DDD или подсеть в нотации CIDR AAA.BBB.CCC.DDD/FF	Добавить адрес в список блокируемых адресов
blacklist remove by addr	<BLACKIP>	IP- адрес в формате AAA.BBB.CCC.DDD или подсеть в нотации CIDR AAA.BBB.CCC.DDD/FF	Удалить адрес из списка блокируемых адресов
blacklist remove by pos	<POSITION>	0-65635	Удалить адрес из списка блокируемых адресов по его позиции в списке
blacklist show all			Показать список блокируемых адресов
blacklist show count			Показать число записей в списке адресов, блокируемых динамическим брандмауэром
blacklist show address	<BLACKIP>	IP- адрес в формате AAA.BBB.CCC.DDD	Найти указанный адрес в списке блокируемых адресов

		или подсеть в нотации CIDR AAA.BBB.CCC.DDD/FF	
blacklist show first	<COUNT>	0-4095	Показать указанное количество из начала списка блокируемых адресов
blacklist show last	<COUNT>	0-4095	Показать указанное количество с конца списка блокируемых адресов
blacklist show position	<POSITION>	0-65635	Показать запись в указанной позиции списка блокируемых адресов
blacklist subnet	<BLACKIP>	подсеть в нотации CIDR AAA.BBB.CCC.DDD/FF	Добавить подсеть в список блокируемых адресов и удалить адреса и подсети, входящие в добавляемую подсеть
block history show all			Просмотр журнала заблокированных адресов
block show count			Показать число записей в журнале заблокированных адресов
block show address	<BLACKIP>	IP- адрес в формате AAA.BBB.CCC.DDD или подсеть в нотации CIDR AAA.BBB.CCC.DDD/FF	Найти указанный адрес в журнале заблокированных адресов
block show first	<COUNT>	0-4095	Показать указанное количество из начала журнала заблокированных адресов
block show last	<COUNT>	0-4095	Показать указанное количество с конца журнала заблокированных адресов
block show position	<POSITION>	0-65635	Показать запись в указанной позиции журнала заблокированных адресов
blocklist remove by addr	<BLACKIP>	IP- адрес в формате AAA.BBB.CCC.DDD или подсеть в нотации CIDR AAA.BBB.CCC.DDD/FF	Удалить адрес из списка автоматически блокируемых адресов
blocklist remove by pos	<POSITION>	0-65635	Удалить адрес из списка автоматически блокируемых адресов по его позиции в списке
blocklist show all			Показать список автоматически блокируемых адресов
blocklist show count			Показать число записей в списке автоматически блокируемых адресов
blocklist show address	<BLACKIP>	IP- адрес в формате AAA.BBB.CCC.DDD или подсеть в нотации CIDR AAA.BBB.CCC.DDD/FF	Найти указанный адрес в списке автоматически блокируемых адресов
blocklist show first	<COUNT>	0-4095	Показать указанное количество из начала списка автоматически блокируемых адресов
blocklist show last	<COUNT>	0-4095	Показать указанное количество с конца списка автоматически блокируемых адресов
blocklist show position	<POSITION>	0-65635	Показать запись в указанной позиции списка автоматически блокируемых адресов
exit			Переход из данного подменю конфигурирования на уровень выше
history			Просмотр истории введенных команд
quit			Завершить данную сессию CLI
set block_time	<SERVICE> <BLCKTIME>	SIP/WEB/TELNET/SSH /OTHER 60-352800	Установить для сервиса время в секундах, на протяжении которого доступ с подозрительного адреса будет блокирован
set enable	<ENA>	on/off	Включить/отключить динамический брандмауэр
set tries	<SERVICE> <TRIES>	SIP/WEB/TELNET/SSH /OTHER 1-10	Установить максимальное число ошибочных попыток доступа к сервису, прежде чем хост будет заблокирован
set forgive_time	<SERVICE> <FORGIVETIME>	SIP/WEB/TELNET/SSH /OTHER 60-352800	Задать время прощения для сервиса

set increment	<SERVICE> <INCREMENT_FLG>	SIP/WEB/TELNET/SSH /OTHER no/yes	Включить прогрессирующую блокировку для сервиса
set only block	<SERVICE> <ONLY_BLOCK_FLG>	SIP/WEB/TELNET/SSH /OTHER no/yes	Включить опцию «Не отправлять заблокированные адреса в черный список» для сервиса
show			Показать настройки динамического брандмауэра
whitelist add	<WHITEIP>	IP- адрес в формате AAA.BBB.CCC.DDD или подсеть в нотации CIDR AAA.BBB.CCC.DDD/FF	Добавить IP-адрес в список адресов, запрещенных для автоматической блокировки
whitelist remove by addr	<WHITEIP>	IP- адрес в формате AAA.BBB.CCC.DDD или подсеть в нотации CIDR AAA.BBB.CCC.DDD/FF	Удалить IP-адрес из списка адресов, запрещенных для автоматической блокировки
whitelist remove by pos	<POSITION>	0-65635	Удалить IP-адрес из списка адресов, запрещенных для автоматической блокировки по его позиции в списке
whitelist show all			Показать список адресов, запрещенных для автоматической блокировки
whitelist show count			Показать число записей в списке адресов, запрещённых для автоматической блокировки
whitelist show address	<WHITEIP>	IP- адрес в формате AAA.BBB.CCC.DDD или подсеть в нотации CIDR AAA.BBB.CCC.DDD/FF	Найти указанный адрес в списке адресов, запрещенных для автоматической блокировки
whitelist show first	<COUNT>	0-4095	Показать указанное количество из начала списка адресов, запрещенных для автоматической блокировки
whitelist show last	<COUNT>	0-4095	Показать указанное количество с конца списка адресов, запрещенных для автоматической блокировки
whitelist show position	<POSITION>	0-65635	Показать запись в указанной позиции списка адресов, запрещенных для автоматической блокировки
whitelist subnet	<WHITEIP>	подсеть в нотации CIDR AAA.BBB.CCC.DDD/FF	Добавить подсеть в список адресов, запрещенных для автоматической блокировки, и удалить адреса и подсети, входящие в добавляемую подсеть

4.2.7.5 Режим конфигурирования параметров статического брандмауэра

Для перехода в данный режим необходимо в режиме конфигурирования выполнить команду **`firewall static`**.

SBC-[CONFIG]> firewall static
Entering static firewall mode
SBC-[CONFIG]-[FIREWALL]>

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
add profile	<PROF_NAME>	разрешено использовать буквы, цифры, символ '_', максимум 63 символf	Добавить профиль firewall
add rule default	<direction> <ENABLE>	input output enable/disable	Добавить правило firewall Направление работы правила Включение/отключение правила

	<RULE_NAME>	Текст, макс. 63 символа	Имя правила
	<S_IP>	AAA.BBB.CCC.DDD	IP-адрес источника
	<S_MASK>	AAA.BBB.CCC.DDD	Маска подсети источника
	<R_IP>	AAA.BBB.CCC.DDD	IP-адрес получателя
	<R_MASK>	AAA.BBB.CCC.DDD	Маска подсети получателя
	<PROTO>	any tcp udp icmp tcp+udp	Тип протокола
	<S_PORT_START>	1-65535	Начальный порт источника
	<S_PORT_END>	1-65535	Конечный порт источника
	<D_PORT_START>	1-65535	Начальный порт получателя
	<D_PORT_END>	1-65535	Конечный порт получателя
	<ICMP_TYPE>	none any echo-reply destination-unreachable network-unreachable host-unreachable protocol-unreachable port-unreachable fragmentation-needed source-route-failed network-unknown host-unknown network-prohibited host-prohibited TOS-network-unreachable TOS-host-unreachable communication-prohibited host-precedence-violation precedence-cutoff source-quench redirect network-redirect host-redirect TOS-network-redirect TOS-host-redirect echo-request router-advertisement router-solicitation time-exceeded ttl-zero-during-transit ttl-zero-during-reassembly parameter-problem ip-header-bad required-option-missing timestamp-request timestamp-reply address-mask-request address-mask-reply	Тип пакета ICMP

	<ACTION>	accept, drop, reject	Действие — действие, выполняемое данным правилом: — ACCEPT — пакеты, попадающие под данное правило, будут пропущены сетевым экраном firewall; — DROP — пакеты, попадающие под данное правило, будут отброшены сетевым экраном firewall без какого-либо информирования стороны, передавшей пакет; — REJECT — пакеты, попадающие под данное правило, будут отброшены сетевым экраном firewall, стороне, передавшей пакет, будет отправлен либо пакет TCP RST, либо ICMP destination unreachable.
	<P_IDX>	1-65535	Номер профиля firewall
add rule geoip	<direction>	input output	Добавить GeoIP-правило firewall Направление работы правила
	<ENABLE>	enable/disable	Включение/отключение правила
	<RULE_NAME>	Текст, макс. 63 символа	Имя правила
	<COUNTRY>	Название страны	Страна, к которой принадлежит адрес
	<PROTO>	any tcp udp icmp tcp+udp	Тип протокола
	<S_PORT_START>	1-65535	Начальный порт источника
	<S_PORT_END>	1-65535	Конечный порт источника
	<D_PORT_START>	1-65535	Начальный порт получателя
	<D_PORT_END>	1-65535	Конечный порт получателя
	<ICMP_TYPE>	none any echo-reply destination-unreachable network-unreachable host-unreachable protocol-unreachable port-unreachable fragmentation-needed source-route-failed network-unknown host-unknown network-prohibited host-prohibited TOS-network-unreachable TOS-host-unreachable communication-prohibited host-precedence-violation precedence-cutoff source-quench	Тип пакета ICMP

		redirect network-redirect host-redirect TOS-network-redirect TOS-host-redirect echo-request router-advertisement router-solicitation time-exceeded ttl-zero-during-transit ttl-zero-during-reassembly parameter-problem ip-header-bad required-option-missing timestamp-request timestamp-reply address-mask-request address-mask-reply	
	<ACTION>	accept, drop, reject	Действие — действие, выполняемое данным правилом: — ACCEPT — пакеты, попадающие под данное правило, будут пропущены сетевым экраном firewall; — DROP — пакеты, попадающие под данное правило, будут отброшены сетевым экраном firewall без какого-либо информирования стороны, передавшей пакет; — REJECT — пакеты, попадающие под данное правило, будут отброшены сетевым экраном firewall, стороне, передавшей пакет, будет отправлен либо пакет TCP RST, либо ICMP destination unreachable.
	<P_IDX>	1-65535	Номер профиля firewall
add rule string			Добавить правило firewall — проверка строк.
	<direction>	input output	Направление работы правила
	<ENABLE>	enable/disable	Включение/отключение правила
	<RULE_NAME>	Текст, макс. 63 символа	Имя правила
	<CONTENT>	Текст, макс. 127 символов	Текстовая строка, которая должна быть в пакете
	<S_IP>	AAA.BBB.CCC.DDD	IP-адрес источника
	<S_MASK>	AAA.BBB.CCC.DDD	Маска подсети источника
	<R_IP>	AAA.BBB.CCC.DDD	IP-адрес получателя
	<R_MASK>	AAA.BBB.CCC.DDD	Маска подсети получателя
	<PROTO>	any tcp udp icmp tcp+udp	Тип протокола
	<S_PORT_START>	1-65535	Начальный порт источника
	<S_PORT_END>	1-65535	Конечный порт источника

	<D_PORT_START>	1-65535	Начальный порт получателя
	<D_PORT_END>	1-65535	Конечный порт получателя
	<ICMP_TYPE>	none any echo-reply destination-unreachable network-unreachable host-unreachable protocol-unreachable port-unreachable fragmentation-needed source-route-failed network-unknown host-unknown network-prohibited host-prohibited TOS-network-unreachable TOS-host-unreachable communication-prohibited host-precedence-violation precedence-cutoff source-quench redirect network-redirect host-redirect TOS-network-redirect TOS-host-redirect echo-request router-advertisement router-solicitation time-exceeded ttl-zero-during-transit ttl-zero-during-reassembly parameter-problem ip-header-bad required-option-missing timestamp-request timestamp-reply address-mask-request address-mask-reply	Тип пакета ICMP
	<ACTION>	accept, drop, reject	Действие — действие, выполняемое данным правилом: — ACCEPT — пакеты, попадающие под данное правило, будут пропущены сетевым экраном firewall; — DROP — пакеты, попадающие под данное правило, будут отброшены сетевым экраном firewall без какого-либо информирования стороны, передавшей пакет; — REJECT — пакеты, попадающие под данное правило, будут отброшены сетевым экраном firewall, стороне, передавшей пакет, будет отправлен либо пакет TCP RST, либо ICMP destination unreachable.
	<P_IDX>	1-65535	Номер профиля firewall

apply			Применить настройки firewall
config			Возврат в меню Configuration
del profile	<ID>	1-65535	Удалить профиль firewall
del rule	<ID>	1-65535	Удалить правило firewall
exit			Выход из данного подменю конфигурирования на уровень выше
modify profile	<ID> <NAME>	1-65535 разрешено использовать буквы, цифры, символ '_'. Максимум 63 символ	Индекс профиля firewall Ввод нового имени устройства
modify rule	<Type> <ID> <param>	action dport_end dport_start enable icmp-type name prof_id proto r_ip r_mask s_ip s_mask sport_end sport_start traffic-type 1-65535 Новое значение согласно данного типа параметра	Изменить указанное правило firewall (один из параметров)
move down	<ID>	1-65535	Переместить правило вниз на одну позицию
move up	<ID>	1-65535	Переместить правило вверх на одну позицию
quit			Завершить данную сессию CLI
set interface	<IFACE_NAME> <PROFILE ID>	Имя интерфейса	Назначить правило на сетевой интерфейс PROFILE ID = 0 означает, что профиль не используется
show config			Показать конфигурацию
show net-interfaces			Показать параметры интерфейсов
show system			Показать системные параметры

4.2.7.6 Конфигурация и работа с утилитой PING

Для перехода в данный режим необходимо в режиме конфигурирования выполнить команду **hostping**.

SBC1000-[CONFIG]> hostping
Entering hostping mode.
SBC1000-[CONFIG]-[HOSTPING]>

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
exit			Переход из данного подменю конфигурирования на уровень выше
host add	ADDR	AAA.BBB.CCC.DDD	Добавить хост к списку пингуемых
host remove	ADDR	AAA.BBB.CCC.DDD	Удалить хост из списка пингуемых
host show			Показать результаты работы
set onboot	ONBOOT	yes/no	Стартовать проверку при загрузке системы
set period	PINGTIME	1-255	Периодичность пингования, минуты

set tries	TRIES	1-7	Количество запросов к каждому хосту
show			Отобразить настройки утилиты PING
start			Запустить периодический пинг
stop			Остановить периодический пинг
quit			Завершить данную сессию CLI

4.2.7.7 Режим конфигурирования сетевых параметров

Для перехода в данный режим необходимо в режиме конфигурирования выполнить команду **network**.

SBC-[CONFIG]> network
Entering Network mode.
SBC-[CONFIG]-NETWORK>

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
add interface pptpVPNclient	<LABEL> <IPADDR> <USER> <PASS>	разрешено использовать буквы, цифры, символы '_', '.', '-', ':', максимум 255 символов IP-адрес в формате AAA.BBB.CCC.DDD разрешено использовать буквы, цифры, символы '_', '.', '-', максимум 63 символа разрешено использовать буквы, цифры, символы '_', '.', '-', максимум 63 символа	Добавить новый VPN/PPTP-клиент LABEL — имя интерфейса; IPADDR — IP-адрес PPTP сервера; USER — имя пользователя; PASS — пароль
add interface tagged	dynamic/static <LABEL> <VID> <IPADDR> <NETMASK>	 разрешено использовать буквы, цифры, символы '_', '.', '-', ':', максимум 255 символов 1-4095 IP-адрес в формате AAA.BBB.CCC.DDD сетевая маска в формате AAA.BBB.CCC.DDD	Добавить новый сетевой интерфейс LABEL — имя интерфейса; VID — VLAN ID; IPADDR — IP-адрес PPTP сервера; NETMASK — сетевая маска
add interface untagged	dynamic/static <LABEL> <IPADDR> <NETMASK>	 разрешено использовать буквы, цифры, символы '_', '.', '-', ':', максимум 255 символов IP-адрес в формате AAA.BBB.CCC.DDD сетевая маска в формате AAA.BBB.CCC.DDD	Добавить новый сетевой интерфейс LABEL — имя интерфейса; IPADDR — IP-адрес PPTP сервера; NETMASK — сетевая
config			Возврат в меню Configuration.
confirm			Подтвердить измененные сетевые настройки и настройки VLAN без перезагрузки шлюза. Если в течение минуты примененные сетевые настройки не подтверждены, то их значения вернутся к первоначальным

exit			Выход из данного подменю конфигурирования на уровень выше
history			Просмотр истории введенных команд
ntp			Переход в режим конфигурирования NTP
quit			Завершить данную сессию CLI
remove interface	<NET_IFACE_IDX>	0-39	Удалить указанный интерфейс
rollback			Отменить изменения
set interface COS	<NET_IFACE_IDX> <COS>	0-39 0-7	Назначить приоритет 802.1p для указанного интерфейса
set interface dhcp	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Получать сетевые настройки динамически от DHCP-сервера для указанного интерфейса
set interface dhcp_dns	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Получать IP-адрес DNS-сервера динамически от DHCP-сервера для указанного интерфейса
set interface dhcp_no_gw	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Не получать настройки шлюза динамически от DHCP-сервера для указанного интерфейса
set interface gateway	<NET_IFACE_IDX> <IPADDR>	0-39 IP-адрес в формате AAA.BBB.CCC.DDD	Задать шлюз по умолчанию для интерфейса
set interface dhcp_ntp	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Получать настройки NTP динамически от DHCP-сервера для указанного интерфейса
set interface gw_ignore	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Игнорировать настройку шлюза для указанного интерфейса
set interface ipaddr	<NET_IFACE_IDX> <IPADDR> <NETMASK>	0-39 IP-адрес в формате AAA.BBB.CCC.DDD сетевая маска в формате AAA.BBB.CCC.DDD	Задать IP-адрес и сетевую маску для указанного интерфейса
set interface network-label	<NET_IFACE_IDX> <LABEL>	0-39 цифры, символы '_', '.', '-', ':', максимум 255 символов	Задать имя для данного интерфейса
set interface run_at_startup	<NET_IFACE_IDX> <STARTUP>	0-39 on/off	Автоматически запускать интерфейс при старте (только для VPN-интерфейса)
set interface serverip	<NET_IFACE_IDX> <IPADDR>	0-39 IP-адрес в формате AAA.BBB.CCC.DDD	Задать IP-адрес PPTP-сервера
set interface snmp	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Разрешить передачу пакетов SNMP через интерфейс
set interface ssh	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Разрешить ssh сессию через интерфейс
set interface telnet	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Разрешить telnet сессию через интерфейс
set interface use_mppe	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Включит/отключить шифрование (только для VPN-интерфейса)
set interface user_name	<NET_IFACE_IDX> <USER>	0-39 разрешено использовать буквы, цифры, символы '_', '.', '-', максимум 63 символа	Задать имя пользователя (только для VPN-интерфейса)
set interface user_pass	<NET_IFACE_IDX> <PASS>	0-39 разрешено использовать буквы, цифры, символы	Задать пароль (только для VPN-интерфейса)

		'_', '.', '-', максимум 63 символа	
set interface VID	<NET_IFACE_IDX> <VID>	0-39 1-4095	Назначить VID для интерфейса
set interface web	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Разрешить доступ через web-интерфейс
set settings dns primary	<IPADDR>	IP-адрес в формате AAA.BBB.CCC.DDD	Задать IP-адрес основного DNS-сервера
set settings dns secondary	<IPADDR>	IP-адрес в формате AAA.BBB.CCC.DDD	Задать IP-адрес резервного DNS-сервера
set settings gateway_iface	<NET_IFACE_NAME>		Имя интерфейса, шлюз которого будет основным шлюзом по умолчанию
set settings hostname	<HOSTNAME>	разрешено использовать буквы, цифры, символы '_', '.', '-', максимум 63 символа	Задать имя хоста
set settings ssh	<PORT>	1-65535	Задать TCP-порт для доступа к устройству по протоколу SSH, по умолчанию 22
set settings telnet	<PORT>	1-65535	Задать TCP-порт для доступа к устройству по протоколу Telnet, по умолчанию 23
set settings web	<PORT>	1-65535	Задать TCP-порт для web-конфигуратора, по умолчанию 80
show interface by_index	<NET_IFACE_IDX>	0-39	Показать настройки указанного сетевого интерфейса
show interface list			Показать список доступных сетевых интерфейсов
show settings			Показать сетевые параметры
snmp			Переход в режим конфигурирования SNMP
ssh restart			Перезапуск процесса SSH

4.2.7.8 Режим конфигурирования протокола NTP

Для перехода в данный режим необходимо в режиме конфигурирования сетевых параметров выполнить команду **ntp**.

SBC-[CONFIG]-NETWORK> ntp
Entering NTP mode.
SBC-[CONFIG]-[NETWORK]-NTP>

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
apply		no/yes	Применить настройки NTP
config			Возврат в меню Configuration
exit			Выход из данного подменю конфигурирования на уровень выше
quit			Завершить данную сессию CLI
restart ntp		no/yes	Перезапустить процесс NTP
set ntp	dhcp period server usage	off/on 10-1440 IP-адрес в формате AAA.BBB.CCC.DDD off/on	Получить настройки NTP по DHCP Задать период синхронизации Задать NTP-сервер Не использовать/использовать NTP
show config			Показать
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-	Задать часовой пояс относительно всемирного координационного времени

		10/GMT+11/GMT-11/GMT+12 Asia Europe	 Выбор города местонахождения в Азии. Выбор города местонахождения в Европе

4.2.7.9 Режим конфигурирования протокола SNMP

Для перехода в данный режим необходимо в режиме конфигурирования выполнить команду **snmp**.

SBC-[CONFIG]-NETWORK> snmp
Entering SNMP mode.
SBC-[CONFIG]-SNMP>

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
add	<TYPE> <IP> <COMM> <PORT>	trapsink/ trap2sink/ informsink IP-адрес в формате AAA.BBB.CCC.DDD строка до 31 символа 1-65535	Добавить правило передачи SNMP трапов: TYPE — тип SNMP сообщения IP — IP-адрес приемника трапов; COMM — пароль, содержащийся в трапах. PORT — UDP-порт приемника трапов
config			Возврат в меню Configuration.
create user	<LOGIN> <PASSWD>	строка до 31 символа пароль от 8 до 31 символа	Создать пользователя (назначить логин и пароль для доступа)
exit			Выход из данного подменю конфигурирования на уровень выше
history			Просмотр истории введенных команд
modify community	<IDX> <COMM>	0-15 строка до 31 символа	Изменить правило передачи SNMP трапов (пароль, содержащийся в трапах)
modify ip	<IDX> <IP>	0-15 IP-адрес в формате AAA.BBB.CCC.DDD	Изменить правило передачи SNMP трапов (адрес приемника трапов)
modify port	<IDX> <PORT>	0-15 1-65535	Изменить правило передачи SNMP трапов (порт приемника трапов)
modify type	<IDX> <TYPE>	0-15 trapsink/ trap2sink/ informsink	Изменить правило передачи SNMP трапов (тип SNMP сообщения)
quit			Завершить данную сессию CLI
remove	<IDX>	0-15	Удалить правило передачи SNMP трапов
restart snmpd	Yes/no		Перезапустить SNMP-клиента
ro	<RO>	строка длиной до 63 символов	Установить пароль на чтение параметров
rw	<RW>	строка длиной до 63 символов	Установить пароль на чтение и запись параметров
show			Показать конфигурацию SNMP
syscontact	<SYSCONTACT>	строка длиной до 63 символов	Указать контактную информацию
syslocation	<SYSLOC>	строка длиной до 63 символов	Указать место расположения устройства
sysname	<SYSNAME>	строка длиной до 63 символов	Указать имя устройства

4.2.7.10 Режим конфигурирования RADIUS

Для перехода в данный режим необходимо в режиме конфигурирования выполнить команду **radius**.

SBC-[CONFIG]> radius
Entering RADIUS mode.
SBC-[CONFIG]-RADIUS>

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
auth ipaddr	<IP_ADDR> <SRV_IDX>	IP-адрес в формате AAA.BBB.CCC.DDD 0-8	Установить IP-адрес сервера авторизации (Authorization). IP_ADDR — IP-адрес; SRV_IDX — номер сервера
auth port	<PORT> <SRV_IDX>	0-65535 0-8	Установить порт сервера авторизации (Authorization) PORT — номер порта; SRV_IDX — номер сервера
auth secret	<SECRET> <SRV_IDX>	строка максимум 31 символ 0-8	Установить пароль для сервера авторизации (Authorization) SECRET — пароль; SRV_IDX — номер сервера
config			Возврат в меню Configuration
deadtime	<DEADTIME>	5-60	Время неиспользования сервера при сбое — время, в течение которого сервер считается неактивным
exit			Выход из данного подменю конфигурирования на уровень выше
history			Просмотр истории введенных команд
profile	<PROFILE_INDEX>	0-31	Переход к конфигурированию параметров профиля RADIUS
quit			Завершить данную сессию CLI
retries	<RETRIES>	2-5	Установить количество попыток отправки запроса
show config			Показать информацию о конфигурации RADIUS-серверов
timeout	<TIMEOUT>	3-10	Установить время, в течение которого ожидается ответ сервера (x100мс)

4.2.7.11 Режим конфигурирования параметров профиля RADIUS

Для перехода в данный режим необходимо в режиме конфигурирования RADIUS выполнить команду **profile <PROFILE_INDEX>**, где **<PROFILE_INDEX>** — номер профиля RADIUS.

SBC-[CONFIG]-RADIUS> profile 0
Entering RADIUS-Profile-mode.
SBC-[CONFIG]-RADIUS-PROFILE[0]>

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
auth digestauth	<DIGESTAUTH>	rfc5090/ rfc5090-no-challenge/ draft-sterman	Выбор алгоритма авторизации абонентов с динамической регистрацией через RADIUS-сервер. При дайджест-аутентификации пароль передается в виде хеш-кода и не может быть перехвачен при сканировании трафика

auth framedprotocol	<FRAMED_PROTOCOL>	none/PPP/ SLIP/ARAP/ Gandalf/Xylogics/ X75_Sync	Назначить протокол при использовании пакетного доступа для запросов аутентификации RADIUS *none* — пакетный доступ не используется
auth nas port type	<PORT_TYPE>	Async/ Sync/ ISDN_Sync/ ISDN_Async_v120/ ISDN_Async_v110/ Virtual/ PIAFS/ HDLC_Channel/ X25/ X75/ G3_Fax/ SDSL/ ADSL_CAP/ ADSL_DMT/ IDSL/ Ethernet/ xDSL/ Cable/ Wireless/ Wireless_IEEE_802.1	Назначить тип физического порта NAS (сервера, где аутентифицируется пользователь), по умолчанию Async
auth restrict	<RESTRICT>	none/ restrict-all	Установить ограничение на исходящую связь при сбое сервера (неполучении ответа от сервера): *none* — разрешать все вызовы; *restrict-all* — запрещать все вызовы
auth service type	<SERVICE_TYPE>	none/ Login/ Framed/ Callback_Login/ Callback_Framed/ Outbound/ Administrative/ NAS_Promt/ Authenticate_Only/ Callback_NAS_Prompt/ Call_Check/ Callback_Administrative	Установить тип услуги, по умолчанию не используется (none)
auth user_name originate	<USERNAME_MODE>	sip_username/ ip/ sip_iface_name	Установить атрибут User-Name в пакетах Access–Request: *cgpn* — в качестве значения использовать телефонный номер вызывающей стороны; *ip_or_stream* — в качестве значения использовать IP-адрес вызывающей стороны или номер потока, по которому осуществляется входящее соединение; *trunk* — в качестве значения использовать имя транка, по которому осуществляется входящее соединение
config			Возврат в меню Configuration
exit			Выход из данного подменю конфигурирования на уровень выше
history			Просмотр истории введенных команд
name	<PRF_NAME>	Строка длиной до 63 символов	Установить наименование профиля
quit			Завершить данную сессию CLI

show			Показать конфигурацию профиля RADIUS

4.2.7.12 Режим работы с резервом

Для перехода в данный режим необходимо в режиме конфигурирования выполнить команду **reserve**.

SBC2000-[CONFIG]> reserve
Entering reserve mode.
SBC2000-[CONFIG]-[RESERVE]>

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
config			Возврат в меню Configuration
exit			Выход из данного подменю конфигурирования на уровень выше
history			Просмотр истории введенных команд
set master	SERIAL_NUMBER	Строка из 10 символов	Сделать мастером устройство с указанным серийным номером
show			Показать информацию о состоянии резерва
quit			Завершить данную сессию CLI
show			Показать конфигурацию профиля RADIUS

4.2.7.13 Режим конфигурирования статических маршрутов

Для перехода в данный режим необходимо в режиме конфигурирования выполнить команду **route**.

SBC-[CONFIG]> route
Entering route mode.
SBC-[CONFIG]-ROUTE>

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
config			Возврат в меню Configuration
exit			Выход из данного подменю конфигурирования на уровень выше
history			Просмотр истории введенных команд
quit			Завершить данную сессию CLI
route default add	<DESTINATION> <MASK> <GATEWAY> <METRIC> <IFACE_NAME> <ENABLE>	IP-адрес в формате AAA.BBB.CCC.DDD маска в формате AAA.BBB.CCC.DDD шлюз в формате AAA.BBB.CCC.DDD целое число без знака строка до 255 символов disable/enable	Добавить статический маршрут: DESTINATION — IP-адрес места назначения; MASK — маска сети для заданного IP-адреса; GATEWAY — IP-адрес шлюза; METRIC — метрика IFACE_NAME — сетевой интерфейс ENABLE — включить/отключить сетевой маршрут
route del	<IDX>	0-4095	Удалить маршрут: IDX — индекс сетевого маршрута

route modify destination	<IDX> <DESTINATION>	0-4095	Изменить адрес назначения
route modify dev	<IDX> <IFACE_NAME>	0-4095 имя сетевого интерфейса	Изменить сетевой интерфейс
route modify enable	<IDX> <EN>	0-4095 enable/disable	Включить или отключить маршрут
route modify gateway	<IDX> <GATEWAY>	0-4095 IP-адрес в формате AAA.BBB.CCC.DDD	Изменить шлюз
route modify metric	<IDX> <METRIC>	0-4095 0-2147483647	Изменить метрику
route modify netmask	<IDX> <NETMASK>	0-4095 маска в формате AAA.BBB.CCC.DDD	Изменить маску сети
route modify vpn-client	<IDX> <VPN_CLIENT>	0-4095 имя VPN-клиента	Изменить VPN-клиента
route VPN add	<DESTINATION> <MASK> <METRIC> <VPN_CLIENT> <ENABLE>	IP-адрес в формате AAA.BBB.CCC.DDD маска в формате AAA.BBB.CCC.DDD целое число без знака строка до 255 символов disable/enable	Добавить маршрут через VPN клиента: DESTINATION — IP-адрес места назначения; MASK — маска сети для заданного IP-адреса; METRIC — метрика VPN_CLIENT — имя VPN клиента ENABLE — включить/отключить сетевой маршрут
show config			Показать информацию о конфигурации маршрута
show net-interfaces			Показать список сетевых интерфейсов
show system			Показать активные маршруты
show vpn-clients			Показать список VPN-клиентов

4.2.7.14 Конфигурирование списка наборов правил rule set

Для перехода в данный режим необходимо в режиме конфигурирования выполнить команду **rule set.**

SBC1000-[CONFIG]> rule set
Entering SBC rule set mode.
SBC1000-[CONFIG]-RULE-SET>

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
add rule set	SBC_RULE_SET_NAME	Строка длиной до 63 символов	Добавить набор правил
edit rule set id	PREFIX_SIGN	1-65535	Редактировать набор правил с указанным ID
edit rule set index	PREFIX_SIGN	0-65534	Редактировать набор правил с указанным индексом
exit			Выход из данного подменю конфигурирования на уровень выше
quit			Завершить данную сессию CLI

remove by id rule set	SBC_RULE_SET_ID	1-65535	Удалить набор правил с указанным ID
show			Отобразить список всех наборов правил rule set

4.2.7.15 Конфигурирование наборов правил rule set

Для перехода в данный режим необходимо в режиме конфигурирования списка наборов правил **rule set** выполнить команду **edit rule set id <ID>** или **edit rule set index <INDEX>**, где **<ID>** и **<INDEX>** — ID или индекс редактируемого правила.

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]>

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
add rule	SBC_RULE_NAME	Строка длиной до 63 символов	Добавить в набор правило с заданным именем
edit rule	SBC_RULE_ID	1-65535	Редактировать правило с указанным ID
exit			Выход из данного подменю конфигурирования на уровень выше
quit			Завершить данную сессию CLI
remove rule	SBC_RULE_ID	1-65535	Удалить правило с указанным ID
show info			Отобразить список всех наборов правил rule set
swap rules	<SBC_RULE_ID_CURRENT> <SBC_RULE_ID_TARGET>	1-65535 1-65535	Обменять местами правила CURRENT и TARGET

4.2.7.16 Конфигурирование правил rule set

Для перехода в данный режим необходимо в режиме конфигурирования наборов правил **rule set** выполнить команду **edit rule <ID>**, где **<ID>** — ID правила для редактирования.

SBC1000-[CONFIG]-RULE-SET-INDEX[13]> edit rule 16
Entering SBC rule edit mode.
SBC1000-[CONFIG]-RULE-SET-INDEX[13]-RULE-ID[16]>

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
exit			Выход из данного подменю конфигурирования на уровень выше
quit			Завершить данную сессию CLI
set action reject	reject		Установить тип правила — запрет вызова
set action send to destination	<DESTINATION_ID>	1-65535	Установить тип правила — отправить вызов на SIP destination с указанным ID
set action send to trunk	<SBC_TRUNK_ID>	1-65535	Установить тип правила — отправить вызов на SBC trunk с указанным ID
set condition all	<CONDITION>	1-5	Установить условие с номером CONDITION — все
set condition none	<CONDITION>	1-5	Очистить условие с номером CONDITION
set condition type	<CONDITION_TYPE>	from-address-user-part/ from-address-host-part/	Установить условие определённого типа from-address-user-part — имя из заголовка From

		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	from-address-host-part — домен из заголовка From from-address-URI — URI из заголовка From to-address-user-part — имя из заголовка To to-address-host-part — домен из заголовка To to-address-URI — URI из заголовка To request-URI-user-part — имя из request-URI request-URI-host-part — домен из request-URI request-URI — URI из request-URI source-IP — IP источника user-agent — значение заголовка User-Agent
	<CONDITION>	1-5	Номер правила
	<CONDITION_MASK>	Строка длиной не более 63 символа	Регулярное выражение, либо IP-адрес
set drop diversion header	<ON_OFF>	on/off	При включении опции заголовок Diversion не будет передаваться на целевое направление
set name	<SBC_RULE_NAME>	Строка длиной не более 63 символа	Имя правила
set work time interval	<WORK_TIME_INTERVAL>	HH:MM-HH:MM где HH = [00-23] MM = [00-59]	Установить интервал времени работы правила
show info			Показать все настройки правила
show sip destination list			Показать доступные SIP destination
show trunk list			Показать доступные SBC trunk

4.2.7.17 Конфигурирование списка SIP destination

Для перехода в данный режим необходимо в режиме конфигурирования выполнить команду **sip destination**.

SBC1000-[CONFIG]> sip destination
Entering SBC SIP destination mode.
SBC1000-[CONFIG]-SIP-DESTINATION>

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
add destination with hostname			Добавить новый SIP destination.
	SIP_DESTINATION_NAME	Строка не более 63 символов	Задать имя.
	SIP_TRANSPORT_ID	1-65535	Задать ID используемого SIP транспорта
	SIP_REMOTE_HOSTNAME	Строка не более 63 символов в формате: hostname/ hostname:port где port = 1-65535	Домен и порт встречной стороны. Если порт не указан, будет использован порт 5060.
add destination with ip address			Добавить новый SIP destination.
	SIP_DESTINATION_NAME	Строка не более 63 символов	Задать имя.

	SIP_TRANSPORT_ID SIP_REMOTE_IP_ADDR	1-65535 AAA.BBB.CCC.DDD/ AAA.BBB.CCC.DDD:port где port = 1-65535	Задать ID используемого SIP транспорта IP-адрес и порт встречной стороны. Если порт не указан, будет использован порт 5060.
edit destination id	PREFIX_SIGN	0-65534	Редактировать destination с выбором по ID
edit destination index	PREFIX_SIGN	1-65535	Редактировать destination с выбором по индексу
exit			Выход из данного подменю конфигурирования на уровень выше
quit			Завершить данную сессию CLI
remove destination	SIP_DESTINATION_INDEX	0-254	Удалить destination по индексу
remove by id destination	SIP_DESTINATION_ID	1-65535	Удалить destination по ID
show info			Показать список всех destination
show sip transport list			Показать список транспортов

4.2.7.18 Конфигурирование SIP destination

Для перехода в данный режим необходимо в режиме конфигурирования списков **SIP destination** выполнить команду **edit destination <ID>** или **edit destination index <INDEX>**, где **<ID>** и **<INDEX>** — ID или индекс редактируемого destination.

SBC1000-[CONFIG]-SIP-DESTINATION> edit destination id 12
Entering SBC SIP destination edit mode.
SBC1000-[CONFIG]-SIP-DESTINATION-ID[12]>

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
exit			Выход из данного подменю конфигурирования на уровень выше
quit			Завершить данную сессию CLI
set adaptation	ADAPTATION	none/ HUAWEI-EchoLife/ Iskratel-SI3000/ HUAWEI-SoftX3000/ ZTE-Softswitch/ Nortel/ MTA-M-200	Установить адаптацию для этого направления
set allow redirection	ON_OFF	on/off	Управление разрешением обработки переадресаций
set auth login	AUTH_LOGIN	Строка не длинней 63 символов	Логин для аутентификации
set auth password	AUTH_LOGIN	Строка не длинней 63 символов	Пароль для аутентификации
set auth remove			Очистить настройки аутентификации
set command line	CMDLINE	Строка	Задать правила расширенных настроек протокола SIP
set const fromto domain	ON_OFF	on/off	Управление опцией «Передавать домен из заголовков FROM и TO»
set convert flash	ON_OFF	on/off	Включить или выключить конвертацию Flash из RFC2833 в SIP INFO
set cps in	<MAX_CPS_IN>	0-100	Входящее максимальное значение CPS; 0 — выключение опции
set cps out	<MAX_CPS_OUT>	0-100	Исходящее максимальное значение CPS; 0 — выключение опции

set ignore source port	ON_OFF	on/off	Включить игнорирование порта источника
set keep-alive server	KEEP_ALIVE_TIMEOUT_0_1000	0-1000	Период проверки рабочего сервера сообщениями OPTIONS
set keep-dead server	KEEP_ALIVE_TIMEOUT_5_1000	5-1000	Период проверки нерабочего сервера сообщениями OPTIONS
set name	SIP_DESTINATION_NAME	Строка не длинней 63 символов	Задать имя SIP destination
set preserve contact header	ON_OFF	on/off	Включить передачу контакта без изменений
set remote address as hotname	SIP_REMOTE_HOSTNAME	Строка не длинней 63 символов в формате: hostname/ hostname:port где port = 1-65535	Задать адрес встречной стороны в виде домена. Если порт не указан, будет использован порт 5060
set remote address as ip	SIP_REMOTE_IP_ADDRESS	AAA.BBB.CCC.DDD/ AAA.BBB.CCC.DDD:port где port = 1-65535	Задать адрес встречной стороны в виде IP-адреса. Если порт не указан, будет использован порт 5060.
set restriction deny-all			Установить ограничение вызовов — всё запрещено
set restriction maximum-sessions	MAXIMUM_SESSIONS	1-65535	Установить ограничение вызовов — максимальное число сессий
set restriction no-restriction			Установить ограничение вызовов — без ограничения
set rtcp timeout	TIMEOUT	10-300/off	Установить таймаут ожидания RTCP от встречной стороны. off — отключить ожидание RTCP.
set rtp-loss timeout	TIMEOUT	10-300/off	Установить таймаут ожидания RTP от встречной стороны. off — отключить ожидание RTP.
set rtp-loss multiplier on hold	TIMEOUT_MULTIPLIER	1-30	Установить множитель ожидания RTP в режиме on hold.
set rtp-loss multiplier silence-suppression	TIMEOUT_MULTIPLIER	1-30	Установить множитель ожидания RTP в режиме подавления тишины
set rule set id	RULE_SET_ID	1-65535	Назначить rule set
set rule set none			Удалить rule set
set session-expires	SESSION_EXPIRES_OR_OFF	90-64800/off	Запрашиваемый период контроля сессии по RFC4028, секунды. off — отключает контроль сессии
set sip header format	SIP_HEADER_FORMAT	full/compact	Установить формат заголовков SIP. full — полный формат; compact — сокращённый формат
set sip transport	SIP_TRANSPORT_ID	1-65535	Назначить SIP transport
set transport protocol	SIP_TRANSPORT	UDP-only/ UDP-prefer/ TCP-prefer/ TCP-only	Назначить транспортный протокол UDP-only — только UDP; UDP-prefer — UDP/TCP с приоритетом UDP; TCP-prefer — UDP/TCP с приоритетом TCP; TCP-only — только TCP
set trunk expires	EXPIRES	0-65535	Время перерегистрации при использовании транковой регистрации
set trunk registration type	REGISTRATION_TYPE	none/ uac/ uas	Выбор типа транковой регистрации none — не использовать транковую регистрацию; uac — регистрироваться на встречном устройстве; uas — принимать регистрацию от встречного устройства

set trunk sip domain	SIP_DOMAIN	Строка не длинней 63 символов	SIP-домен, используемый для транковой регистрации
set trunk username/number	USERNAME_NUMBER	Строка не длинней 63 символов	Имя пользователя, используемое при регистрации
set verify media remote address	ON_OFF	on/off	Включить опцию контроля IP и порта источника RTP
show info			Показать настройки
show rule set list			Показать список настроенных rule set
show sip transport list			Показать список доступных SIP-транспортов

4.2.7.19 Конфигурирование SIP транспортов

Для перехода в данный режим необходимо в режиме конфигурирования списков SIP транспортов выполнить команду **sip transport**.

SBC1000-[CONFIG]> sip transport
Entering SBC SIP transport mode.
SBC1000-[CONFIG]-SIP-TRANSPORT>

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
add transport	SBC_SIP_TRANSPORT_NAME IFACE_ID PORT RTP_IFACE_ID	Строка не длинней 63 символов 1-65535 1-65535 1-65535	Добавить новый SIP транспорт. Задать имя. Задать ID интерфейса, используемого для сигнализации SIP Задать порт сигнализации Задать ID интерфейса, используемого для RTP
exit			Выход из данного подменю конфигурирования на уровень выше
quit			Завершить данную сессию CLI
remove transport	SBC_SIP_TRANSPORT_INDEX	0-254	Удалить destination по индексу
remove by id transport	SBC_SIP_TRANSPORT_ID	1-65535	Удалить destination по ID
set by id name	SBC_SIP_TRANSPORT_ID SBC_SIP_TRANSPORT_NAME	1-65535 Строка не длинней 63 символов	Изменить название транспорта по его ID ID транспорта Новое название транспорта
set by id netiface	SBC_SIP_TRANSPORT_ID IFACE_ID	1-65535 1-65535	Изменить сетевой интерфейс для сигнализации SIP ID транспорта ID сетевого интерфейса
set by id port	SBC_SIP_TRANSPORT_ID PORT	1-65535 1-65535	Изменить порт сигнализации ID транспорта Порт сигнализации
set by id rtp			Изменить сетевой интерфейс для RTP

	SBC_SIP_TRANSPORT_ID RTP_IFACE_ID	1-65535 1-65535	ID транспорта ID сетевого интерфейса
set name	SBC_SIP_TRANSPORT_INDEX SBC_SIP_TRANSPORT_NAME	1-65535 Строка не длинней 63 символов	Изменить название транспорта по его ID Индекс транспорта Новое название транспорта
set netiface	SBC_SIP_TRANSPORT_INDEX IFACE_ID	1-65535 1-65535	Изменить сетевой интерфейс для сигнализации SIP Индекс транспорта ID сетевого интерфейса
set port	SBC_SIP_TRANSPORT_INDEX PORT	1-65535 1-65535	Изменить порт сигнализации Индекс транспорта Порт сигнализации
set rtp	SBC_SIP_TRANSPORT_INDEX RTP_IFACE_ID	1-65535 1-65535	Изменить сетевой интерфейс для RTP Индекс транспорта ID сетевого интерфейса
show info			Показать список всех транспортов
show net-ifaces			Показать список сетевых интерфейсов

4.2.7.20 Конфигурирование списка SIP users

Для перехода в данный режим необходимо в режиме конфигурирования выполнить команду **sip users.**

SBC1000-[CONFIG]> sip users
Entering SBC SIP users mode.
SBC1000-[CONFIG]-SIP-USERS>

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
add user	SIP_USER_NAME SIP_TRANSPORT_ID	Строка не более 63 символов 1-65535	Добавить новый SIP users. Задать имя. Задать ID используемого SIP транспорта
edit user id	PREFIX_SIGN	0-65534	Редактировать user с выбором по ID
edit user index	PREFIX_SIGN	1-65535	Редактировать user с выбором по индексу
exit			Выход из данного подменю конфигурирования на уровень выше
quit			Завершить данную сессию CLI
remove user	SIP_USER_INDEX	0-254	Удалить user по индексу
remove by id user	SIP_USER_ID	1-65535	Удалить user по ID
show info			Показать список всех user
show sip transport list			Показать список транспортов

4.2.7.21 Конфигурирование SIP users

Для перехода в данный режим необходимо в режиме конфигурирования списков **SIP destination** выполнить команду **edit user id <ID>** или **edit user index <INDEX>**, где **<ID>** и **<INDEX>** — ID или индекс редактируемого 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]>

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
exit			Выход из данного подменю конфигурирования на уровень выше
quit			Завершить данную сессию CLI
set allow redirection	ON_OFF	on/off	Управление разрешением обработки переадресаций
set command line	CMDLINE	Строка	Задать правила расширенных настроек протокола SIP
set convert flash	ON_OFF	on/off	Включить или выключить конвертацию Flash из RFC2833 в SIP INFO
set name	SIP_USER_NAME	Строка не длинней 63 символов	Задать имя SIP user
set nat keep-alive	KEEP_ALIVE	0-65535	Время хранения соединения за NAT, сек
set nat subscribers	ON_OFF	on/off	Включает режим "абоненты за NAT"
set preserve contact header	ON_OFF	on/off	Включить передачу контакта без изменений
set radius profile id	RADIUS_PROFILE_ID	1-65535	Привязать RADIUS-профиль
set radius profile none			Отвязать RADIUS-профиль
set registration interval	REG_INTERVAL	60-65535	Задать допустимый интервал перерегистрации для пользователей, сек
set restrictions non-registered deny-all			Установить ограничение вызовов для незарегистрированных пользователей — всё запрещено
set restrictions non-registered maximum-sessions	MAXIMUM_SESSIONS	1-65535	Установить ограничение вызовов для незарегистрированных пользователей — максимальное число сессий
set restrictions non-registered no-restriction			Установить ограничение вызовов для незарегистрированных пользователей — без ограничения
set restrictions registered deny-all			Установить ограничение вызовов для зарегистрированных пользователей — всё запрещено
set restrictions registered maximum-sessions	MAXIMUM_SESSIONS	1-65535	Установить ограничение вызовов для зарегистрированных пользователей — максимальное число сессий
set restrictions registered no-restriction			Установить ограничение вызовов для зарегистрированных пользователей — без ограничения
set rtcp timeout	TIMEOUT	10-300/off	Установить таймаут ожидания RTCP от встречной стороны.

			off — отключить ожидание RTCP.
set rtp-loss timeout	TIMEOUT	10-300/off	Установить таймаут ожидания RTP от встречной стороны. off — отключить ожидание RTP.
set rtp-loss multiplier on hold	TIMEOUT_MULTIPLIER	1-30	Установить множитель ожидания RTP в режиме on hold.
set rtp-loss multiplier silence-suppression	TIMEOUT_MULTIPLIER	1-30	Установить множитель ожидания RTP в режиме подавления тишины
set rule set id	RULE_SET_ID	1-65535	Назначить rule set
set rule set none			Удалить rule set
set session-expires	SESSION_EXPIRES_OR_OFF	90-64800/off	Запрашиваемый период контроля сессии по RFC4028, секунды. off — отключает контроль сессии.
set sip domain	SIP_DOMAIN	Строка не длинней 63 символов	Задать SIP-домен, с которым будет произведена регистрация
set sip header format	SIP_HEADER_FORMAT	full/compact	Установить формат заголовков SIP. full — полный формат; compact — сокращённый формат.
set sip transport	SIP_TRANSPORT_ID	1-65535	Назначить SIP transport
set transport protocol	SIP_TRANSPORT	UDP-only/ UDP-prefer/ TCP-prefer/ TCP-only	Назначить транспортный протокол UDP-only — только UDP; UDP-prefer — UDP/TCP с приоритетом UDP; TCP-prefer — UDP/TCP с приоритетом TCP; TCP-only — только TCP.
set verify media remote address	ON_OFF	on/off	Включить опцию контроля IP и порта источника RTP
show info			Показать настройки
show radius profile list			Показать список настроенных RADIUS-профилей
show rule set list			Показать список настроенных rule set
show sip transport list			Показать список доступных SIP-транспортов

4.2.7.22 Режим конфигурирования протокола SNMP

Для перехода в данный режим необходимо в общем режиме конфигурирования или в режиме конфигурирования сети выполнить команду **snmp**.

SBC-[CONFIG]> snmp
Entering SNMP mode.
SBC-[CONFIG]-[NETWORK]-SNMP>

SBC-[CONFIG]-NETWORK> snmp
Entering SNMP mode.
SBC-[CONFIG]-[NETWORK]-SNMP> exit

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
add	<TYPE> <IP>	trapsink/ trap2sink/ informsink IP-адрес в формате AAA.BBB.CCC.DDD	Добавить правило передачи SNMP трапов: TYPE — тип SNMP сообщения IP — IP-адрес приемника трапов;

	<COMM> <PORT>	строка до 31 символа 1-65535	COMM — пароль, содержащийся в трапах; PORT — UDP-порт приемника трапов
config			Возврат в меню Configuration
create user	<LOGIN> <PASSWD>	строка до 31 символа пароль от 8 до 31 символа	Создать пользователя (назначить логин и пароль для доступа)
exit			Выход из данного подменю конфигурирования на уровень выше
history			Просмотр истории введенных команд
modify community	<IDX> <COMM>	0-15 строка до 31 символа	Изменить правило передачи SNMP трапов (пароль, содержащийся в трапах)
modify ip	<IDX> <IP>	0-15 IP-адрес в формате AAA.BBB.CCC.DDD	Изменить правило передачи SNMP трапов (адрес приемника трапов)
modify port	<IDX> <PORT>	0-15 1-65535	Изменить правило передачи SNMP трапов (порт приемника трапов)
modify type	<IDX> <TYPE>	0-15 trapsink/ trap2sink/ informsink	Изменить правило передачи SNMP трапов (тип SNMP сообщения)
quit			Завершить данную сессию CLI
remove	<IDX>	0-15	Удалить правило передачи SNMP трапов
restart snmpd	Yes/no		Перезапустить SNMP-клиента
ro	<RO>	строка длиной до 63 символов	Установить пароль на чтение параметров
rw	<RW>	строка длиной до 63 символов	Установить пароль на чтение и запись параметров
show			Показать конфигурацию SNMP
syscontact	<SYSCONTACT>	строка длиной до 63 символов	Указать контактную информацию
syslocation	<SYSLOC>	строка длиной до 63 символов	Указать место расположения устройства
sysname	<SYSNAME>	строка длиной до 63 символов	Указать имя устройства

4.2.7.23 Режим конфигурирования параметров switch

Для перехода в данный режим[1] необходимо в режиме конфигурирования выполнить команду **switch**.

SBC-[CONFIG]> switch
Entering switch control mode.
SBC-[CONFIG]-[SWITCH]>

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
802.1q			Переход в режим конфигурации 802.1q
apply mirroring settings		no/yes	Применить настройки зеркалирования
apply port settings		no/yes	Применить настройки портов
confirm mirroring settings			Подтвердить настройки зеркалирования. Если в течение одной минуты настройки не

[1] Только для SBC-1000

			подтверждены, то они вернутся к предыдущим значениям
confirm port settings			Подтвердить настройки портов. Если в течение одной минуты настройки не подтверждены, то они вернутся к предыдущим значениям
exit			Выход из данного подменю конфигурирования на уровень выше
history			Просмотр истории введенных команд
LACP[1]			Переход в режим конфигурирования параметров LACP
QoS_control			Переход в режим конфигурирования параметров QoS
quit			Завершить данную сессию CLI
save mirroring			Сохранить настройки зеркалирования без применения
save vlan			Сохранить настройки VLAN без применения
set mirroring	<PORT>

		SFP1(7)	
	<EGRESS>	unmodified/ untagged/ tagged/ double-tag	EGRESS– режим отправки пакетов: – *unmodified* — пакеты передаются данным портом без изменений (т.е. в том же виде, в каком поступили на другой порт коммутатора); – *untagged* — пакеты передаются данным портом всегда без тега VLAN; – *tagged* — пакеты передаются данным портом всегда с тегом VLAN; – *Double tag* — пакеты передаются данным портом с двумя тегами VLAN — если принятый пакет был тегированным и с одним тегом VLAN — если принятый пакет был не тегированным.
set port ieee mode	<PORT>	GE_PORT0(0)/ GE_PORT1(1)/ GE_PORT2(2)/ CPU(4)/ SFP0(6)/ SFP1(7)	Установить режим контроля полученных тегированных пакетов для данного порта.
	<IEEE>	fallback/ check/ secure	IEEE– режим контроля пакетов: – *Fallback*– если через порт принят пакет с тегом VLAN, для которого есть записи в таблице маршрутизации, указанные в записи этой таблицы, иначе для него применяются правила маршрутизации, указанные в «egress» и «output»; – *Check*– если через порт принят пакет с VID, для которого есть запись в таблице маршрутизации «802.1q», то он попадает под правила маршрутизации, указанные в данной записи этой таблицы, даже если этот порт не является членом группы для данного VID. Правила маршрутизации, указанные в «egress» и «output» для данного порта, не применяются; – *Secure*– если через порт принят пакет с VID, для которого есть запись в таблице маршрутизации «802.1q», то он попадает под правила маршрутизации, указанные в данной записи этой таблицы, иначе отбрасывается. Правила маршрутизации, указанные в «egress» и «output», для данного порта не применяются.
set port LACP_trunk[1]	<PORT>	CPU/ GE_PORT0/ GE_PORT1/ GE_PORT2/ SFP0/ SFP1	Назначить транк LACP для указанного порта.

[1] В данной версии ПО не поддерживается

	<LACP>	0-4	
set port MAC GE_PORT0	<MACADDR>	MAC-адрес в формате XX:XX:XX:XX:XX:XX	Задать MAC-адрес для порта
set port output	<PORT> <P_DEST> <ENABLE>	GE_PORT0/ GE_PORT1/ GE_PORT2/ CPU/ SFP0/ SFP1 GE_PORT0/ GE_PORT1/ GE_PORT2/ CPU/ SFP0/ SFP1 on/off	Установка допустимых портов отправки пакетов PORT — настраиваемый порт P_DEST — допустимые порты отправки
set port speed	<SPEED> <PORT>	1000M 100M (full-duplex/ half-duplex) 10M(full-duplex/ half-duplex) auto GE_PORT0/GE_PORT1/ GE_PORT2	Установить режим работы порта
set port vlan enabling	<PORT> <ENABLE>	CPU/ GE_PORT0/ GE_PORT1/ GE_PORT2/ SFP0/ SFP1 on/off	Включить/отключить VLAN на данном порту
set port vlan override	<PORT> <OVER>	CPU/ GE_PORT0/ GE_PORT1/ GE_PORT2/ SFP0/ SFP1 on/off	Установить режим переопределения VLAN ID для данного порта на стандартный
show mirror settings			Показать параметры зеркалирования портов
show port settings			Показать параметры настройки портов

4.2.7.23.1 Режим конфигурирования параметров 802.1q

Для перехода в данный режим необходимо в режиме конфигурирования switch выполнить команду **802.1q**.

SBC-[CONFIG]-[SWITCH]> 802.1q
Entering 802.1q_control mode.
SBC-[CONFIG]-[SWITCH]-[802.1q]>

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
add VTU element	<VID> <PRIO> <OVER> <GE_PORT0>	0-4095 0-7 on/off unmodified/	Добавить новый элемент в VTU таблицу: VID — идентификатор VLAN; PRIO — приоритет 802.1p, назначаемый пакетам в данной VLAN, если параметр *OVER* активен(on);

	<GE_PORT1> <GE_PORT2> <CPU> <SFP0> <SFP1>	untagged/ tagged/ not_member unmodified/ untagged/ tagged/ not_member unmodified/ untagged/ tagged/ not_member unmodified/ untagged/ tagged/ not_member unmodified/ untagged/ tagged/ not_member unmodified/ untagged/ tagged/ not_member	OVER — переписать приоритет 802.1p для данной VLAN (да/нет); PORT — действия, выполняемые данным портом при передаче пакета, имеющего указанный VID: — *Unmodified*– пакеты передаются данным портом без изменений; — *Untagged*– пакеты передаются данным портом всегда без тега VLAN; — *Tagged*– пакеты передаются данным портом всегда с тегом VLAN; — *Not member* — пакеты с указанным VID не передаются данным портом, т.е. порт не является членом этой группы VLAN
apply	<YES_NO>	yes/no	Применить настройки VTU
confirm			Подтвердить настройки VTU. Если в течение одной минуты настройки не подтверждены, то они вернутся к предыдущим значениям
exit			Переход из данного подменю конфигурирования на уровень выше
QoS_control			Переход в режим конфигурации QoS
quit			Завершить данную сессию CLI
remove VTU element	<NUMBER>	0-4095	Удалить данный элемент VTU таблицы
save			Сохранить настройки VTU без применения
set VTU override	<NUMBER> <OVER>	0-4095 on/off	Переписать/не переписывать приоритет 802.1p для данной VLAN (да/нет)
set VTU priority	<NUMBER> <PRIO>	0-4095 0-7	Установить приоритет 802.1p, назначаемый пакетам в данной VLAN, если параметр «set VTU override» активен
set VTU settings_CPU	<NUMBER> <CPU>	0-4095 unmodified/ untagged/ tagged/ not_member	Назначить действия, выполняемые данным портом при передаче пакета, имеющего указанный VID — *Unmodified* — пакеты передаются данным портом без изменений; — *Untagged* — пакеты передаются данным портом всегда без тега VLAN; — *Tagged* — пакеты передаются данным портом всегда с тегом VLAN; — *Not member* — пакеты с указанным VID не передаются данным портом, т.е. порт не является членом этой группы VLAN
settings_GE_PORT0	<NUMBER> <CPU>	0-4095 unmodified/ untagged/ tagged/	Назначить действия, выполняемые данным портом при передаче пакета, имеющего указанный VID

		not_member	– *Unmodified* — пакеты передаются данным портом без изменений; – *Untagged* — пакеты передаются данным портом всегда без тега VLAN; – *Tagged* — пакеты передаются данным портом всегда с тегом VLAN; – *Not member* — пакеты с указанным VID не передаются данным портом, т.е. порт не является членом этой группы VLAN
settings_GE_PORT1	<NUMBER> <CPU>	0-4095 unmodified/ untagged/ tagged/ not_member	Назначить действия, выполняемые данным портом при передаче пакета, имеющего указанный VID: – *Unmodified* — пакеты передаются данным портом без изменений; – *Untagged* — пакеты передаются данным портом всегда без тега VLAN; – *Tagged* — пакеты передаются данным портом всегда с тегом VLAN; – *Not member* — пакеты с указанным VID не передаются данным портом, т.е. порт не является членом этой группы VLAN
settings_GE_PORT2	<NUMBER> <CPU>	0-4095 unmodified/ untagged/ tagged/ not_member	Назначить действия, выполняемые данным портом при передаче пакета, имеющего указанный VID: – *Unmodified* — пакеты передаются данным портом без изменений; – *Untagged* — пакеты передаются данным портом всегда без тега VLAN; – *Tagged* — пакеты передаются данным портом всегда с тегом VLAN; – *Not member* — пакеты с указанным VID не передаются данным портом, т.е. порт не является членом этой группы VLAN
settings_SFP0	<NUMBER> <CPU>	0-4095 unmodified/ untagged/ tagged/ not_member	Назначить действия, выполняемые данным портом при передаче пакета, имеющего указанный VID: – *Unmodified* — пакеты передаются данным портом без изменений; – *Untagged* — пакеты передаются данным портом всегда без тега VLAN; – *Tagged* — пакеты передаются данным портом всегда с тегом VLAN; – *Not member* — пакеты с указанным VID не передаются данным портом, т.е. порт не является членом этой группы VLAN
settings_SFP1	<NUMBER> <CPU>	0-4095 unmodified/	Назначить действия, выполняемые данным портом при передаче пакета, имеющего указанный VID:

		untagged/ tagged/ not_member	– *Unmodified* — пакеты передаются данным портом без изменений; – *Untagged* — пакеты передаются данным портом всегда без тега VLAN; – *Tagged* — пакеты передаются данным портом всегда с тегом VLAN; – *Not member* — пакеты с указанным VID не передаются данным портом, т.е. порт не является членом этой группы VLAN
show list			Показать список элементов в VTU таблице
show one	<NUMBER>	0-4095	Показать информацию о данном элементе VTU таблицы
show table			Показать VTU таблицу

4.2.7.23.2 Режим конфигурирования параметров QoS

Для перехода в данный режим необходимо в режиме конфигурирования switch или 802.1q выполнить команду **QoS_control**.

SBC-[CONFIG]-[SWITCH]> QoS_control
Entering QoS_control mode.
SBC-[CONFIG]-[SWITCH]-[QoS]>

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
802.1q			Вернуться в режим конфигурирования параметров 802.1q
apply	<YES_NO>	yes/no	Применить настройки QoS
confirm			Подтвердить настройки QoS. Если в течение одной минуты настройки не подтверждены, то они вернутся к предыдущим значениям
exit			Переход из данного подменю конфигурирования на уровень выше
quit			Завершить данную сессию CLI
save			Сохранить настройки QoS без применения
set 802.1p_prio_mapping	<PRIO> <QUEUE>	0-7 0-3	Распределить пакеты по очередям в зависимости от приоритета 802.1p PRIO — номер приоритета 802.1p; QUEUE — номер очереди
set default_VLAN_priority	<PORT> <DEFPRIO>	GE_PORT0(0)/ GE_PORT1(1)/ GE_PORT2(2)/ CPU(4)/ SFP0(6)/ SFP1(7) 0-7	Назначить приоритет 802.1p нетегированным пакетам, принятым данным портом. Если пакет уже имеет приоритет 802.1p либо IP diffserv приоритет, то данный параметр не используется (default vlan priority не будет применяться к пакетам, содержащим заголовок IP, в случае использования одного из режимов QoS: DSCP only, DSCP preferred, 802.1p preferred, а также к уже тегированным пакетам)
set diffserv_prio_mapping	<NUMBER> <QUEUE>	*1 0-3	Распределить пакеты по очередям в зависимости от приоритета IP diffserv NUMBER — номер приоритета IP diffserv;

			QUEUE — номер очереди
set egress_limit	<PORT> <EGRLIM>	GE_PORT0(0)/ GE_PORT1(1)/ GE_PORT2(2)/ CPU(4)/ SFP0(6)/ SFP1(7) on/off	Включить/выключить ограничения полосы пропускания для исходящего с данного порта трафика
set egress_rate_limit	<PORT> <EGRRATE>	GE_PORT0(0)/ GE_PORT1(1)/ GE_PORT2(2)/ CPU(4)/ SFP0(6)/ SFP1(7) 0-250000	Установить ограничение полосы пропускания (кбит/с) для исходящего с данного порта трафика
set ingress_limit_mode	<PORT> <INGRMODE>	GE_PORT0(0)/ GE_PORT1(1)/ GE_PORT2(2)/ CPU(4)/ SFP0(6)/ SFP1(7) off/ all/ mult_flood_broad/ mult_broad/ broad	Установить режим ограничения трафика, поступающего на данный порт. INGRMODE — режим ограничения: – *off* — нет ограничения; – *all* — ограничивается весь трафик; – *mult_flood_broad* — ограничивается многоадресный (multicast), широковещательный (broadcast) и лавинный одноадресный (flooded unicast) трафик; – *mult_broad* — ограничивается многоадресный и широковещательный трафик; – *broad* — ограничивается только широковещательный трафик
set ingress_rate_prio_0/1/2/3	<PORT> <INGPRIO>	GE_PORT0(0)/ GE_PORT1(1)/ GE_PORT2(2)/ CPU(4)/ SFP0(6)/ SFP1(7) 0-250000	Установить ограничение полосы пропускания (кбит/с) трафика, поступающего на данный порт для нулевой/первой/второй/третьей очереди.
set QoS_mode	<PORT> <QOSMODE>	GE_PORT0(0)/ GE_PORT1(1)/ GE_PORT2(2)/ CPU(4)/ SFP0(6)/ SFP1(7) DSCP_only/ 802.1p_only/ DSCP_preferred/ 802.1p_preferred	Установить режим использования QoS. QOSMODE — режим использования: – *DSCP only* — распределять пакеты по очередям только на основании приоритета IP diffserv; – *802.1p only* — распределять пакеты по очередям только на основании приоритета 802.1p; – *DSCP preferred* — распределять пакеты по очередям на основании приоритетов IP diffserv и 802.1p, при этом при наличии обоих приоритетов в пакете, распределение по очередям осуществляется на основании IP diffserv;

			— *802.1p preferred* — распределять пакеты по очередям на основании приоритетов IP diffserv и 802.1p, при этом при наличии обоих приоритетов в пакете, распределение по очередям осуществляется на основании 802.1p
set remapping_priority	<PORT> <NUM> <REMAP>	GE_PORT0(0)/ GE_PORT1(1)/ GE_PORT2(2)/ CPU(4)/ SFP0(6)/ SFP1(7) 0-7 0-7	Переназначить приоритеты 802.1p для тегированных пакетов. PORT-настраиваемый порт; NUM — текущее значение приоритета; REMAP- новое значение
show QOS	<PORT>	GE_PORT0(0)/ GE_PORT1(1)/ GE_PORT2(2)/ CPU(4)/SFP0(6)/ SFP1(7)	Показать параметры конфигурации QoS для данного порта
show QOS_diffserv			Показать параметры распределения пакетов по очередям в зависимости от приоритета IP diffserv
show QOS_priomap			Показать параметры распределения пакетов по очередям в зависимости от приоритета 802.1p

4.2.7.24 Режим конфигурирования параметров syslog

Для перехода в данный режим необходимо в режиме конфигурирования выполнить команду **syslog**.

SBC-[CONFIG]> syslog
Entering syslog mode.
SBC-[CONFIG]-SYSLOG>

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
authlog set	IP PORT ONOFF LOCREM	IP-адрес в формате AAA.BBB.CCC.DDD 1-65535 off/on local/remote	Установить адрес сервера для отправки сообщений syslog, а также режим работы. on/off — включить/выключить ведение логов; local/remote — если выставлено в remote, то отправлять логи на сервер syslog.
authlog show			Показать текущие параметры ведения логов
config			Возврат в меню Configuration.
dispatcher	DISPATCHER	0-99	Включить ведение трассировок Dispatcher'a
exit			Переход из данного подменю конфигурирования на уровень выше
manager	MANAGER	0-99	Включить ведение трассировок Manager'a
quit			Завершить данную сессию CLI
show			Показать информацию о конфигурации Syslog
start			Включить отправку данных на syslog-сервер
stop			Выключить отправку данных на syslog-сервер
userlog	<IPADDR> <PORT> <MODE>	IP-адрес в формате AAA.BBB.CCC.DDD 1-65535 off/standart/full	Включить вывод истории введенных команд IPADDR — IP-адрес syslog-сервера PORT — порт Syslog-сервера MODE — уровень детализации журнала введенных команд

			off — не формировать журнал введенных команд; standart — в сообщениях передается название измененного параметра; *full* — в сообщениях передается название измененного параметра и значения параметра до и после изменения
worker	WORKER	0-99	Включить ведение трассировок Worker'a

4.2.7.25 Режим конфигурирования SBC Trunk

Для перехода в данный режим необходимо в режиме конфигурирования выполнить команду **trunk**.

SBC1000-[CONFIG]> trunk
Entering SBC trunk mode.
SBC1000-[CONFIG]-TRUNK>

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
add trunk	SBC_TRUNK_NAME LOAD_BALANCE_MODE LOAD_BALANCE_TIMEOUT	Строка не длинней 63 символов active-active/ active-backup 5-65535	Добавить новый SBC Trunk Имя транка Режим балансировки Таймаут балансировки, сек
exit			Переход из данного подменю конфигурирования на уровень выше
quit			Завершить данную сессию CLI
remove by id destination primary	SBC_TRUNK_ID	1-65535	Удалить основной destination из транка по ID
remove by id destination secondary	SBC_TRUNK_ID	1-65535	Удалить резервный destination из транка по ID
remove by id trunk	SBC_TRUNK_ID	1-65535	Удалить SBC trunk по его ID
remove destination primary	SBC_TRUNK_ID	0-65534	Удалить основной destination из транка по индексу
remove destination secondary	SBC_TRUNK_ID	0-65534	Удалить резервный destination из транка по индексу
remove trunk	SBC_TRUNK_ID	0-65534	Удалить SBC trunk по индексу
set by id destination primary	SBC_TRUNK_ID SBC_SIP_DESTINATION_ID	1-65535 1-65535	Назначить основной destination транку по ID
set by id destination secondary	SBC_TRUNK_ID SBC_SIP_DESTINATION_ID	1-65535 1-65535	Назначить резервный destination транку по ID
set by id load balance mode	SBC_TRUNK_ID LOAD_BALANCE_MODE	1-65535 active-active/ active-backup	Назначить по ID транка режим балансировки
set by id load balance timeout	SBC_TRUNK_ID LOAD_BALANCE_TIMEOUT	1-65535 5-65535	Назначить по ID транка таймаут балансировки, сек
set by id name	SBC_TRUNK_ID SBC_TRUNK_NAME	1-65535 Строка не длинней 63 символов	Назначить имя транку по его ID

set destination primary	SBC_TRUNK_INDEX SBC_SIP_DESTINATION_ID	0-65534 1-65535	Назначить основной destination транку по индексу
set destination secondary	SBC_TRUNK_INDEX SBC_SIP_DESTINATION_ID	0-65534 1-65535	Назначить резервный destination транку по индексу
set load balance mode	SBC_TRUNK_INDEX LOAD_BALANCE_MODE	0-65534 active-active/ active-backup	Назначить по индексу транка режим балансировки
set load balance timeout	SBC_TRUNK_INDEX LOAD_BALANCE_TIMEOUT	0-65534 5-65535	Назначить по индексу транка таймаут балансировки, сек
set name	SBC_TRUNK_INDEX SBC_TRUNK_NAME	0-65534 Строка не длинней 63 символов	Назначить имя транку по его индексу
show info			Показать настройки
show sip destination list			Показать список доступных SIP-destination
swap by id destination	SIP_TRUNK_ID	1-65535	Поменять местами основной и резервный destination'ы в указанном trunk
swap destination	SIP_TRUNK_INDEX	0-65534	Поменять местами основной и резервный destination'ы в указанном trunk

4.2.7.26 Конфигурирование списка запрещённых клиентских приложений

Для перехода в данный режим необходимо в режиме конфигурирования выполнить команду **user agent**.

SBC1000-[CONFIG]> user agent
Entering SBC user agent mode.
SBC1000-[CONFIG]-USER-AGENT>

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
add	USER_AGENT	scan/ crack/ flood/ kill/ sipcli/ sipvicious/ sipsak/ sundayddr/ iWar/ SIVuS/ Gulp/ sipv/ smap/ friendly-request/ VaxIPUserAgent/ VaxSIPUserAgent/ siparmyknife/ Test_Agent/ SIPBomber/ Siprogue	Добавить один из предустановленных User-Agent в список блокируемых
add other	USER_AGENT_NAME	Строка не длиннее 31 символа	Добавить свою маску User-Agent в список
exit			Переход из данного подменю конфигурирования на уровень выше
quit			Завершить данную сессию CLI
remove by id user agent	USER_AGENT_ID	1-65535	Удалить User-Agent из списка по его ID

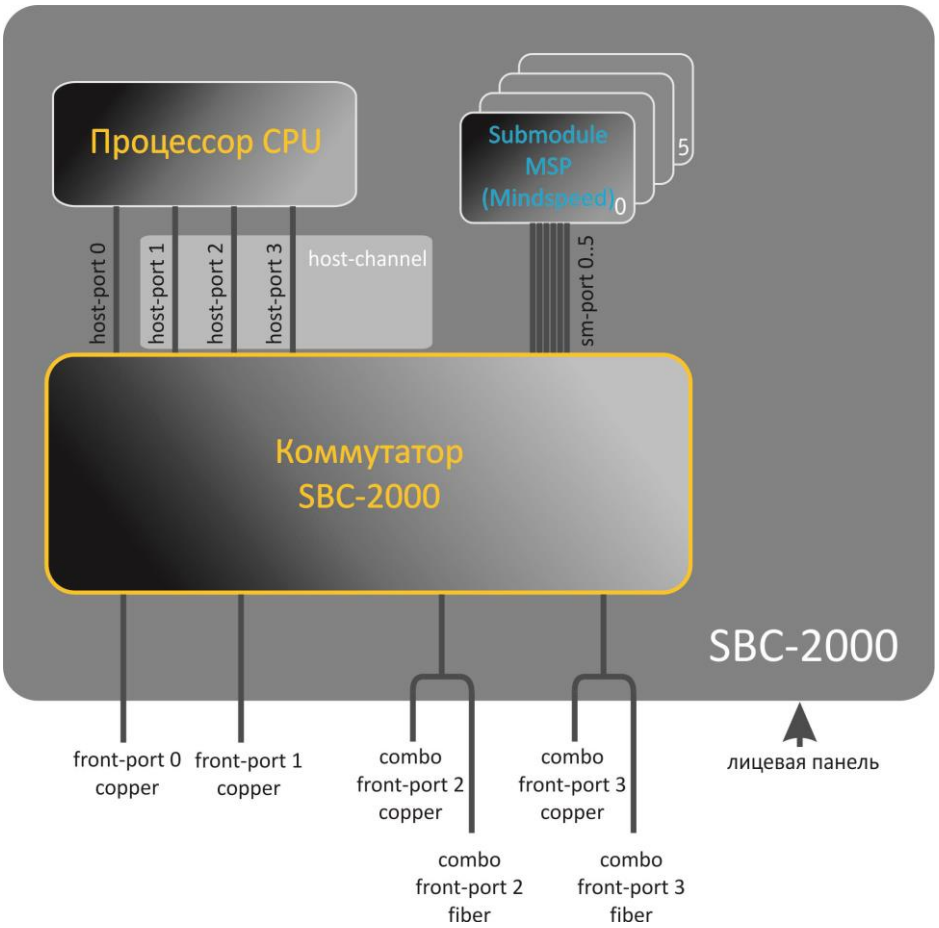
remove user agent	USER_AGENT_INDEX	0-65534	Удалить User-Agent из списка по его индексу
show			Показать сконфигурированный список

4.3 Настройка коммутатора SBC-2000/SBC-3000

Настройка производится из режима конфигурирования коммутатора.

```
SBC2000> config
Entering configuration mode.
SBC2000-[CONFIG]> switch
SBC2000-[CONFIG]-[SWITCH]>
```

4.3.1 *Структура коммутатора*

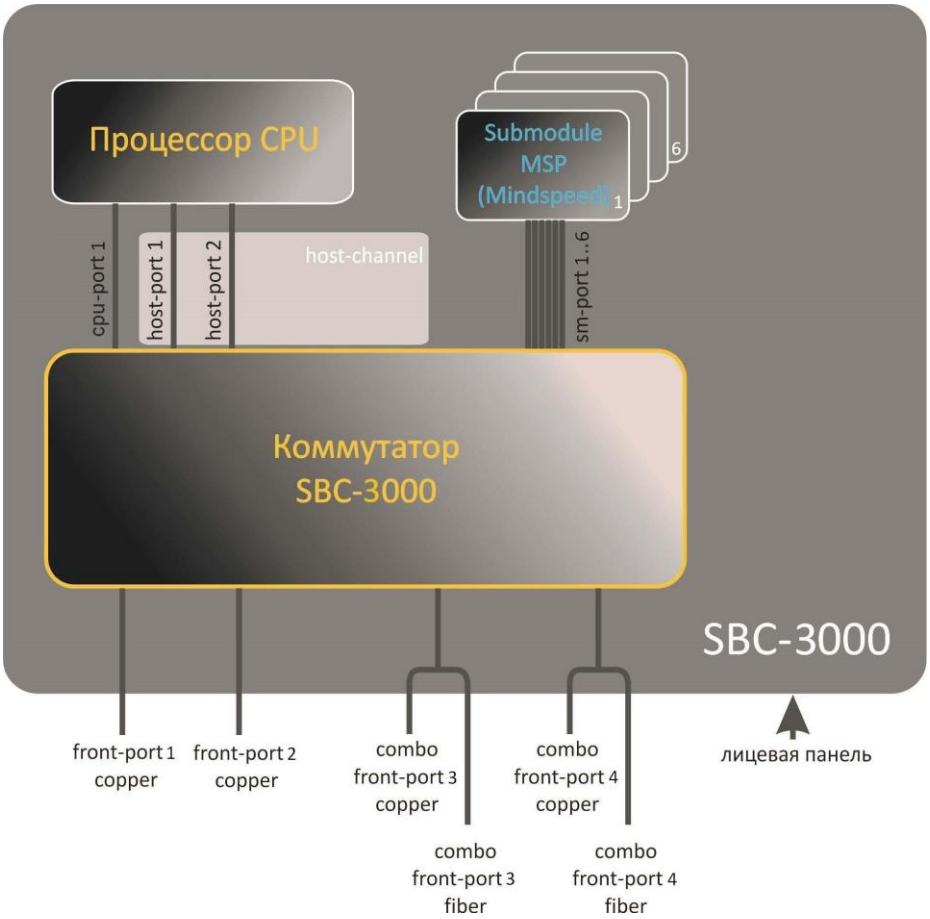


Коммутатор SBC-2000 имеет интерфейсы:

- *front-port* — внешние ethernet-порты коммутатора, которые выведены на лицевую панель.
  Принимаемые значения: 0 - 3.
  - порты 0 .. 1 — медные порты
  - порты 2 .. 3 — оптические и медные комбо-порты.
- *port-channel* — группы агрегации LAG front-port интерфейсов коммутатора, используются в случае объединения нескольких front-port в LACP-группу.
  Принимаемые значения: 1 — 4.
- *host-port* — внутренние порты коммутатора SBC-2000, предназначенные для связи с процессором (CPU) SBC-2000.
  Принимаемые значения: 0 - 2.

– *host-channel* — группа агрегации LAG host-channel интерфейсов коммутатора, данная группа всегда активна.
  Принимаемое значение: 1.

– *sm-port* — внутренние порты коммутатора SBC-2000, предназначенные для связи с субмодулями SM-VP.
  Принимаемые значения: 0 – 5.



Коммутатор SBC-3000 имеет интерфейсы:

– *front-port* – внешние ethernet-порты коммутатора, которые выведены на лицевую панель. Принимаемые значения: 1 – 4.
  – порты 1 .. 2 – медные порты;
  – порты 3 .. 4 – оптические и медные комбо-порты.

– *port-channel* – группы агрегации LAG front-port интерфейсов коммутатора, используются в случае объединения нескольких front-port в LACP-группу. Принимаемые значения: 1 – 4.

– *cpu-port* – внутренний порт коммутатора для управления SBC-3000. Принимаемые значения: 1.

– *host-port* – внутренние порты коммутатора SBC-3000, предназначенные для связи с процессором (CPU) SBC-3000. Принимаемые значения: 1 – 2.

– *host-channel* – группа агрегации LAG host-channel интерфейсов коммутатора, данная группа всегда активна. Принимаемое значение: 1.

– *sm-port* – внутренние порты коммутатора SBC-3000, предназначенные для связи с субмодулями SM-VP. Принимаемые значения: 1 – 6.

При работе с коммутатором используется значение unit number, равное 1.

4.3.2 *Команды управления интерфейсами коммутатора SBC-2000/SBC-3000*

Для SBC-3000 необходимо учитывать, что нумерация портов была изменена, начальный front-port = 1.

interface

Данная команда позволяет перейти в режим конфигурирования интерфейсов коммутатора SBC-2000/SBC-3000.

Синтаксис

interface <interface> <number>

Параметры

<interface> — тип интерфейса:

- front-port — внешние интерфейсы коммутатора;
- host-channel — группы агрегации LAG host-channel интерфейсов коммутатора;
- port-channel — группы агрегации LAG внешних интерфейсов коммутатора;

<number> — номер порта:

- для front-port: <unit/port>, где
  - unit — номер модуля SBC-2000, всегда принимает значения 1;
  - port — номер порта принимает значения [0 .. 3] (или 1 .. 4 для SBC-3000);
- для host-channel: 1;
- для port-channel: [1 .. 4].

Параметр <number> может принимать значение all для настройки сразу всех портов одного типа интерфейсов.

shutdown

Данной командой отключается конфигурируемый интерфейс.

Использование отрицательной формы команды включает конфигурируемый интерфейс.

Синтаксис

[no] shutdown

Параметры

Команда не содержит аргументов.

Пример

```
SBC2000-[CONFIG]-[SWITCH]-[if]> shutdown
```

Конфигурируемый интерфейс отключен.

bridging to

Данной командой устанавливается разрешение на передачу трафика между интерфейсами.

Использование отрицательной формы команды устанавливает запрет на передачу трафика между интерфейсами.

Синтаксис

[no] bridging to <interface> <range>

Параметры

<interface> — тип интерфейса:

- cpu-port;
- front-port — внешние uplink-интерфейсы;
- host-channel;
- host-port;
- port-channel — группы агрегации LAG uplink-интерфейсов;
- sm-port.

<range> — номер порта/портов, с которыми разрешен обмен трафика:

- для cpu-port: <1/0>, где:
- для front-port: <unit/port>, где:
  - unit — номер модуля, принимает значение [1],
  - port — номер порта, принимает значения [0 .. 3];
- для host-channel: [1];
- для host-port:
  - unit — номер модуля, принимает значение [1],
  - port — номер порта, принимает значения [0 .. 2];
- для port-channel: [0 .. 4];
- для sm-port: [0 .. 15].
  - unit — номер модуля, принимает значение [1],
  - port — номер порта, принимает значения [0 .. 5].

Пример

```
SBC2000-[CONFIG]-[SWITCH]-[if]> bridging to front-port all
```

flow-control

Данной командой включается/отключается механизм управления потоком передачи данных (flow control) на конфигурируемом интерфейсе. Механизм flow control позволяет компенсировать различия в скорости передатчика и приемника. Если объем трафика превысит определенный уровень, приемник будет передавать кадры, информирующие передатчик о необходимости уменьшения объема трафика, для снижения числа потерянных пакетов. Для реализации данного механизма необходимо, чтобы на удаленном устройстве также поддерживалась эта функция.

Синтаксис

flow-control <act>

Параметры

<act> — назначаемое действие:

- on — включить;
- off — выключить.

Значение по умолчанию

off

Пример

```
SBC2000-[CONFIG]-[SWITCH]-[if]> flow-control on
```

frame-types

Команда позволяет назначить определенные правила приема пакетов для интерфейса:

- принимать тегированные и нетегированные пакеты;
- принимать только пакеты с тегом VLAN.

Синтаксис

frame-types <act>

Параметры

<act> — назначаемое действие:

- all — принимать тегированные и нетегированные пакеты;
- tagged — принимать только пакеты с тегом VLAN.

Значение по умолчанию

принимаются все пакеты (тегированные и нетегированные)

Пример

```
SBC2000-[CONFIG]-[SWITCH]-[if]> frame-types all
```

На конфигурируемых портах разрешен прием нетегированного трафика.

speed

Данной командой устанавливается значение скорости для конфигурируемого интерфейса.

Командой устанавливаются следующие режимы: 10 Мбит/с, 100Мбит/с, 1000 Мбит/с. При установке 10 Мбит/с, 100Мбит/с необходимо указать режим работы приемопередатчика: дуплекс, полудуплекс.

Синтаксис

speed <rate> [<mode>]

Параметры

<rate> — значение скорости: 10M; 100M; 1000 Мбит/с;

<mode> — режим работы приемопередатчика:

- full-duplex — дуплекс;
- half-duplex — полудуплекс.

Пример

```
SBC2000-[CONFIG]-[SWITCH]-[if]> speed 10M full-duplex
```

Установлен скоростной режим интерфейса 10Мбит/с, дуплекс.

speed auto

Данной командой устанавливается значение скорости для конфигурируемого интерфейса автоматически.

Синтаксис

speed auto

Параметры

Команда не содержит аргументов.

Пример

```
SBC2000-[CONFIG]-[SWITCH]-[if]> speed auto
```

Скорость для порта будет устанавливаться автоматически.

show interfaces configuration

Данной командой осуществляется просмотр конфигурации интерфейсов коммутатора SBC-2000

Синтаксис

show interfaces configuration <interface> <number>

Параметры

<interface> — тип интерфейса:

- front-port — внешние uplink-интерфейсы;
- host-channel;
- host-port;
- port-channel — группы агрегации LAG внешних uplink-интерфейсов;
- sm-port.

<number> — номер порта:

- all — все порты выбранного интерфейса;
- для front port: <unit/port>, где:
  - unit — номер модуля, принимает значения [1],
  - port — номер порта, принимает значения [0 .. 3];
- для host-channel: [1];
- для host-port:
  - unit — номер модуля, принимает значение [1],
  - port — номер порта, принимает значения [0 .. 2];
- для port-channel: [0 .. 4].
- для sm-port: [0 .. 15].
  - unit — номер модуля, принимает значение [1],
  - port — номер порта, принимает значения [0 .. 5].

Пример

```
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

Данная команда позволяет просмотреть информацию о состоянии интерфейса, группы интерфейсов.

Синтаксис

show interfaces status <interface> <number>

Параметры

<interface> — тип интерфейса:

- front-port — внешние uplink-интерфейсы;
- host-channel
- host-port ;
- port-channel — группы агрегации LAG внешних uplink-интерфейсов;
- sm-port

<number> — номер порта:

- all — все порты выбранного интерфейса;
- для front port: <unit/port>, где:
  - unit — номер модуля, принимает значения [1],
  - port — номер порта, принимает значения [0 .. 3];
- для host-channel: [1];
- для host-port:
  - unit — номер модуля, принимает значение [1],
  - port — номер порта, принимает значения [0 .. 2];
- для port-channel: [0 .. 4].
- для sm-port:
  - unit — номер модуля, принимает значение [1],
  - port — номер порта, принимает значения [0 .. 5].

Пример

```
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

Данная команда позволяет просмотреть счетчики интерфейса или группы интерфейсов.

Синтаксис

show interfaces counters <interface> <number>

Параметры

<interface> — тип интерфейса:

- cpu-port;

- front-port — внешние uplink-интерфейсы;
- host-channel;
- host-port;
- port-channel — группы агрегации LAG uplink-интерфейсов;
- sm-port.

<range> — номер порта/портов, с которыми разрешен обмен трафика:

- для cpu-port: <1/0>, где:
- для front-port: <unit/port>, где:
  - unit — номер модуля, принимает значение [1],
  - port — номер, порта принимает значения [0 .. 3];
- для host-channel: [1];
- для host-port:
  - unit — номер, модуля, принимает значение [1],
  - port — номер порта, принимает значения [0 .. 2];
- для port-channel: [0 .. 4].
- для sm-port:
  - unit — номер модуля, принимает значение [1],
  - port — номер порта, принимает значения [0 .. 5].

Пример

```
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 *Команды настройки групп агрегации*

channel-group

Данной командой добавляется интерфейсы FRONT-PORT в группу агрегации.

Использование отрицательной формы команды (no) удаляет интерфейсы FRONT-PORT из группы агрегации.

Синтаксис

channel-group <id> [force]

no channel-group

Параметры

<id> — порядковый номер группы агрегации, в которую будет добавлен порт, принимает значения [1 .. 4];

- [force] — необязательный параметр, принимает значение;
- force — означает быть совместимым с остальными членами группы.

Пример

```
SBC2000-[CONFIG]-[SWITCH]-[if]> channel-group 1
```

Все порты uplink объединены в группы 1.

lacp mode

Данная команда позволяет выбрать режим агрегации каналов:

- Passive — в этом режиме коммутатор не инициирует создание логического канала, но рассматривает входящие пакеты LACP;
- Active — в этом режиме необходимо сформировать агрегированную линию связи и инициировать согласование.

Объединение линий связи формируется, если другая сторона работает в режимах LACP active или passive.

Использование отрицательной формы команды (no) устанавливает режим агрегации каналов по умолчанию.

Синтаксис

lacp mode <name>

no lacp mode

Параметры

<name> — режим:

- active;
- passive.

Значение по умолчанию

active

Пример

```
SBC2000-[CONFIG]-[SWITCH]-[if]> lacp mode active
```

На настраиваемых портах включен режим агрегации каналов «active».

lacp port-priority

Данной командой устанавливается приоритет для настраиваемого порта. Приоритет устанавливается в диапазоне [1 .. 65535]. Приоритет со значением 1 считается наивысшим.

Использование отрицательной формы команды (no) устанавливает значение приоритета по умолчанию.

Синтаксис

lacp port-priority <priority>

no lacp port-priority

Параметры

<priority> — приоритет для данного порта принимает значения [0 .. 65535].

Значение по умолчанию

для всех портов установлен приоритет 32768

Командный режим

INTERFACE FRONT-PORT

Пример

```
SBC2000-[CONFIG]-[SWITCH]-[if]> lacp port-priority 256
```

На настраиваемых портах установлен приоритет порта 256.

lacp rate

Данной командой задается интервал передачи управляющих пакетов протокола LACPDU.

Использование отрицательной формы команды (no) устанавливает интервал передачи управляющих пакетов протокола LACPDU по умолчанию.

Синтаксис

lacp rate <rate>

no lacp rate

Параметры

<rate> — интервал передачи:

- fast — интервал передачи 1 секунда;
- slow — интервал передачи 30 секунд.

Значение по умолчанию

1 секунда (fast)

Командный режим

INTERFACE FRONT-PORT

Пример

```
SBC2000-[CONFIG]-[SWITCH]-[if]> lacp rate slow
```

Установлен интервал передачи управляющих пакетов LACPDU в 30 секунд.

4.3.4 *Команды управления интерфейсами VLAN*

pvid

Данной командой устанавливается значение VID по умолчанию для пакетов, принимаемых портом.

При поступлении не тегированного пакета или пакета со значением VID в VLAN-теге, равным 0, пакету присваивается значение VID, равное PVID.

Синтаксис

pvid <num>Параметры

<num> — идентификационный номер VLAN порта устанавливается в диапазоне [1 .. 4094].

Значение по умолчанию

PVID = 1

Командный режим

INTERFACE FRONT-PORT

INTERFACE PORT-CHANNEL

Пример

```
SBC-2000-[CONFIG]-[SWITCH]-[if]> pvid 5
```

Конфигурируемому порту назначен PVID 5.

4.3.5 *Команды настройки STP/RSTP*

spanning-tree enable

Данной командой функция STP разрешена на конфигурируемом интерфейсе.

Использование отрицательной формы команды (no) запрещает STP на интерфейсе.

Синтаксис

[no] spanning-tree enable

Параметры

Команда не содержит аргументов.

Командный режим

INTERFACE FRONT-PORT

INTERFACE PORT-CHANNEL

Пример

```
SBC2000-[CONFIG]-[SWITCH]-[if]> spanning-tree enable
```

Функция STP включена для всех front-port.

spanning-tree pathcost

Данной командой для конфигурируемого интерфейса устанавливается ценность пути для работы протокола STP.

Использование отрицательной формы команды (no) устанавливает значение ценности пути по умолчанию.

По умолчанию установлено значение 0.

Синтаксис

spanning-tree pathcost <pathcost>

no spanning-tree pathcost

Параметры

<pathcost> — ценность пути, принимает значения [0..200000000].

Значение по умолчанию

значение ценности пути = 0

Командный режим

INTERFACE FRONT-PORT

INTERFACE PORT-CHANNEL

Пример

```
SBC2000-[CONFIG]-[SWITCH]-[if]> spanning-tree pathcost 1
```

Установлена ценность пути 1.

spanning-tree priority

Данной командой для конфигурируемого порта устанавливается приоритет для работы протокола STP.

Использование отрицательной формы команды (no) устанавливает приоритет для работы протокола STP по умолчанию. По умолчанию установлено значение 128.

Синтаксис

spanning-tree priority <priority>

no spanning-tree priority

Параметры

<priority> — приоритет, принимает значения кратно 16 [0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240].

Значение по умолчанию

128

Командный режим

INTERFACE FRONT-PORT

INTERFACE PORT-CHANNEL

Пример

```
SBC2000-[CONFIG]-[SWITCH]-[if]> spanning-tree priority 144
```

Установлен приоритет 144.

spanning-tree admin-edge

Данной командой устанавливается тип соединения как edge-линк в сторону хоста. В этом случае при поднятии линка на интерфейсе автоматически разрешается передача данных.

Использование отрицательной формы команды (no) восстанавливает значения по умолчанию.

Синтаксис

[no] spanning-tree admin-edge

Параметры

Команда не содержит аргументов.

Значение по умолчанию

off

Командный режим

INTERFACE FRONT-PORT

INTERFACE PORT-CHANNEL

Пример

```
SBC2000-[CONFIG]-[SWITCH]-[if]> spanning-tree admin-edge
```

Для конфигурируемого порта включен тип соединения edge-линк.

spanning-tree admin-p2p

Данной командой устанавливается тип определения соединения p2p.

Использование отрицательной формы команды (no) устанавливает тип определения соединения p2p по умолчанию.

Синтаксис

spanning-tree admin-p2p <type>
no spanning-tree admin-p2p

Параметры

<type> – тип определения соединения:

- auto — определение происходит на основании BPDU;
- force-false — принудительно установить линк как не p2p;
- force-true — принудительно установить линк как p2p.

Значение по умолчанию

определение типа соединения p2p происходит на основании BPDU

Командный режим

INTERFACE FRONT-PORT
INTERFACE PORT-CHANNEL

Пример

```
SBC2000-[CONFIG]-[SWITCH]-[if]> spanning-tree admin-p2p auto
```

Для конфигурируемого порта определение типа соединения p2p происходит на основании BPDU.

spanning-tree auto-edge

Данной командой устанавливается автоматическое определение бриджа на конфигурируемом интерфейсе.

Использование отрицательной формы команды (no) отключает автоматическое определение бриджа на конфигурируемом интерфейсе.

По умолчанию функция автоматическое определение бриджа включена.

Синтаксис

[no] spanning-tree auto-edge

Параметры

Команда не содержит аргументов.

Командный режим

INTERFACE FRONT-PORT
INTERFACE PORT-CHANNEL

Пример

```
SBC2000-[CONFIG]-[SWITCH]-[if]> spanning-tree auto-edge
```

Функция «автоматическое определение бриджа» включена.

4.3.6 *Команды настройки MAC-таблицы*

mac-address-table aging-time

Данной командой устанавливается время жизни MAC-адреса в таблице глобально.

Использование отрицательной формы команды (no) устанавливает время жизни MAC-адреса по умолчанию.

Синтаксис

[no] mac-address-table aging time <aging time>

no mac-address-table aging time

Параметры

<aging time> — время жизни MAC-адреса, принимает значения [10 .. 630] секунд.

Значение по умолчанию

300 секунд

Командный режим

CONFIG-SWITCH

Пример

```
SBC2000-[CONFIG]-[SWITCH]> mac-address-table aging-time 100
```

show mac address-table count

Данная команда позволяет просмотреть количество записей MAC-адресов на всех front-port интерфейсах, port-channel интерфейсах, slot-channel интерфейсах.

Синтаксис

show mac address-table count

Параметры

Команда не содержит аргументов.

Командный режим

CONFIG-SWITCH

Пример

```
SBC2000-[CONFIG]-[SWITCH]> show mac address-table count
17 valid mac entries
```

show mac address-table include/exclude interface

Данная команда позволяет просмотреть таблицу MAC-адресов в соответствии с заданным интерфейсом.

Синтаксис

show mac address-table include/exclude interface <interface> <number>

Параметры

<interface> — тип интерфейса:

- front-port — внешние uplink-интерфейсы;
- host-channel;
- port-channel — группы агрегации LAG внешних uplink-интерфейсов;

<number> — номер порта:

- all — все порты выбранного интерфейса;
- для front port: <unit/port>, где:
  - unit — номер модуля, принимает значения [1],
  - port — номер порта, принимает значения [0 .. 3];
- для host-channel: [1];
- для port-channel: [0 .. 4].

Командный режим

CONFIG-SWITCH

4.3.7 *Команды для настройки зеркалирования портов*

mirror <rx|tx> interface

Данной командой включается операция зеркалирования на портах коммутатора для входящего/исходящего трафика.

Зеркалирование портов позволяет копировать трафик, идущий от одного порта на другой, для внешнего анализа.

Использование отрицательной формы команды (no) выключает операцию зеркалирования.

Синтаксис

[no] mirror <rx|tx> interface <port> <num>

Параметры

<rx|tx> — тип трафика:

- rx — входящий;
- tx — исходящий.

<port> — тип интерфейса:

- front-port — внешние uplink-интерфейсы;
- host-channel — интерфейсы для подключения интерфейсных модулей;
- host-port;
- port-channel — логическое объединение внешних uplink-интерфейсов;
- sm-port.

<num> — порядковый номер порта заданной группы (можно указать несколько портов перечислением через «,» либо диапазон портов через «-»):

- «all» — все порты данной группы;

<interface> — тип интерфейса:

- front-port — внешние uplink-интерфейсы;
- host-channel;
- host-port;
- port-channel — группы агрегации LAG внешних uplink-интерфейсов;
- sm-port.

<number> — номер порта:

- all — все порты выбранного интерфейса;
- для front port: <unit/port>, где:
  - unit — номер модуля, принимает значения [1],
  - port — номер порта, принимает значения [0 .. 3];
- для host-channel: [1];
- для host-port:
  - unit — номер модуля, принимает значение [1],
  - port — номер порта, принимает значения [0 .. 2];
- для port-channel: [0 .. 4].
- для sm-port:
  - unit — номер модуля, принимает значение [1],
  - port — номер порта, принимает значения [0 .. 5].

Командный режим

CONFIG-SWITCH

Пример

```
SBC2000-[CONFIG]-[SWITCH]> mirror rx interface front-port 1/3
```

Для входящего трафика, поступающего на интерфейсы front-port 1/3, включена операция

«зеркалирования портов». Трафик копируется с портов slot-port на порт-анализатор, установленный командной «mirror rx analyzer».

mirror <rx|tx> analyzer

Данная команда позволяет установить порт, на который будут дублироваться пакеты для анализа, входящего/исходящего трафика с портов, установленных командой mirror rx port/ mirror tx port.

Использование отрицательной формы команды (no) отключает анализ передаваемого входящего/исходящего трафика.

Синтаксис

[no] mirror <rx|tx> analyzer <interface> <port>

Параметры

<rx|tx> — тип трафика:

- rx — входящий;
- tx — исходящий.

<interface> — тип интерфейса. В качестве порта-анализатора могут использоваться только интерфейсы front-port, port-channel;

<port> — порядковый номер порта группы front-port в формате <unit/port>, где:

- для front port: <unit/port>, где:
  - unit — номер модуля, принимает значения [1],
  - port — номер порта, принимает значения [0 .. 3];
- для port-channel: [0 .. 4].

Командный режим

CONFIG-SWITCH

Пример

```
SBC2000-[CONFIG]-[SWITCH]> mirror rx analyzer front-port 1/2
```

Данные для внешнего анализа будут дублироваться на front-port 1/2 с порта/портов, на котором/которых установлена опция «зеркалирование входящего трафика».

mirror add-tag

Данная команда добавляет метку 802.1q к анализируемому трафику. Настройка значения метки (тега) выполняется командной **mirror <rx/tx> added-tag-config**.

Использование отрицательной формы команды (no) удаляет тег.

Синтаксис

[no] mirror add-tag

Параметры

Команда не содержит аргументов.

Командный режим

CONFIG-SWITCH

Пример

```
SBC2000-[CONFIG]-[SWITCH]> mirror add-tag
```

mirror <rx|tx> added-tag-config

Данная команда позволяет установить значение метки, которое можно добавить к анализируемому входящему/исходящему трафику.

Синтаксис

mirror <rx|tx> added-tag-config vlan <vid> [user-prio <user-prio>]

Параметры

<vid> — идентификационный номер VLAN, принимает значения от [1 .. 4094];

<user-prio> — приоритет COS, принимает значения от [0 .. 7].

Командный режим

CONFIG-SWITCH

Пример

```
SBC2000-[CONFIG]-[SWITCH]> mirror rx added-tag-config vlan 77 user-prio 5
```

mirror <rx|tx> vlan

Командой задается VLAN ID, который будет использоваться в операции зеркалирования при передаче входящего/исходящего трафика.

Синтаксис

[no] mirror <rx|tx> vlan <vid>

Параметры

<rx|tx> — тип трафика:

- rx — входящий;
- tx — исходящий.

<vid> — идентификационный номер VLAN, принимает значения [1..4094].

Командный режим

CONFIG-SWITCH

Пример

```
SBC2000-[CONFIG]-[SWITCH]> mirror rx vlan 56
```

4.3.8 *Команды для настройки функции SELECTIVE Q-IN-Q*

Для выполнения общих настроек функции Selective Q-in-Q предназначен командный режим **SELECTIVE Q-IN-Q COMMON**. Для установки списка правил Selective Q-in-Q предназначен командный режим **SELECTIVE Q-IN-Q LIST.**

Функция SELECTIVE Q-IN-Q позволяет на основе сконфигурированных правил фильтрации по номерам внутренних VLAN (Customer VLAN) производить добавление внешнего SPVLAN (Service Provider’s VLAN), подменять Customer VLAN, а также запрещать прохождение трафика.

add-tag

Данной командой добавляется внешняя метка на основании внутренней.

Использование отрицательной формы команды (no) удаляет установленное правило.

Синтаксис

[no] add-tag svlan <s-vlan> cvlan <c-vlan>

Параметры

<s-vlan> — номер внешней метки, принимает значения [1..4095];

<c-vlan> — номер/номера внутренней метки, принимает значения 1-4094. Список C-VLAN задается через «,».

Командный режим

SELECTIVE Q-IN-Q

overwrite-tag

Данной командой производится подмена CVLAN в требуемом направлении.

Использование отрицательной формы команды (no) удаляет установленное правило.

Синтаксис

[no] overwrite-tag new-vlan <new-vlan> old-vlan <old-vlan> <rule_direction>

Параметры

<new-vlan> — новый номер VLAN, принимает значения [1 ..4095];

<old-vlan> — номер VLAN, который нужно подменить, принимает значения [1 .. 4094].

<rule_direction> — направление трафика:

- Ingress — входящий;
- Egress — исходящий.

Командный режим

SELECTIVE Q-IN-Q

remove

Данной командой производится удаление правила Selective Q-in-Q по заданному номеру.

Синтаксис

remove <rule_index>

Параметры

<rule_index> — номер правила, принимает значения [0 .. 511].

Командный режим

SELECTIVE Q-IN-Q

clear

Данной командой удаляются все правила Selective Q-in-Q.

Синтаксис

clear

Параметры

Команда не содержит аргументов.

Командный режим

SELECTIVE Q-IN-Q

selective-qinq enable

Данной командой на конфигурируемом интерфейсе коммутатора SMG-2016 включается функция Selective Q-in-Q. Использование отрицательной формы команды (no) отключает функцию Selective Q-in-Q на интерфейсе.

Синтаксис

[no] selective-qinq enable

Параметры

Команда не содержит аргументов.

Командный режим

INTERFACE FRONT-PORT

INTERFACE PORT-CHANNEL

selective-qinq list

Данной командой конфигурируемому интерфейсу коммутатора SMG-2016 назначается список правил Selective Q-in-Q.

Использование отрицательной формы команды (no) удаляет привязку.

Синтаксис

selective-qinq list <name>

no selective-qinq list

Параметры

<name> — имя списка правил Selective Q-in-Q

Командный режим

INTERFACE FRONT-PORT

INTERFACE PORT-CHANNEL

show interfaces selective-qinq lists

Данной командой осуществляется просмотр информации о состоянии функции “Selective Q-in-Q” на интерфейсах коммутатора.

Синтаксис

show interfaces selective-qinq lists

4.3.9 *Настройка протокола DUAL HOMING*

backup interface

Данной командой указывается резервный интерфейс, на который будет происходить переключение при потере связи на основном. Включение резервирования возможно только на тех интерфейсах, на которых отключен протокол SPANNING TREE.

Использование отрицательной формы команды (no) удаляет настройку с интерфейса.

Синтаксис

[no] backup interface <INTERFACE> <INDEX> vlan <VLAN_ID_RANGE>

Параметры

<INTERFACE> — тип интерфейса:

- front-port — внешние интерфейсы;
- port-channel — группы агрегации LAG внешних uplink-интерфейсов.

<INDEX> — номер порта:

- для front port: <unit/port>, где:
  - unit — номер платы SMG-2016, принимает значение [1];
  - port — номер порта, принимает значения [0 .. 3].
- для port-channel: [1 .. 4].

<VLAN_ID_RANGE> — может принимать следующие значения:

- [1..4094] — определенный идентификатор VLAN (диапазона VLAN), для которой необходимо включить резервирование.
- Ignore — включить резервирование независимо от существующих VLAN на порту.

Командный режим

INTERFACE FRONT-PORT

INTERFACE PORT-CHANNEL

Пример

Глобальное резервирование

```
SBC2000-[CONFIG]-[SWITCH]-[if]> no backup interface vlan ignore
SBC2000-[CONFIG]-[SWITCH]-[if]> backup interface front-port 1/1 vlan ignore
```

Резервирование в определенной 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

Данной командой указывается количество копий пакетов с одним и тем же MAC-адресом, которые будут отправлены в активный интерфейс при переключении.

Использование отрицательной формы команды (no) восстанавливает значение по умолчанию (1 пакет).

Синтаксис

[no] backup-interface mac-duplicate <COUNT>

Параметры

<COUNT> — количество копий пакетов, принимает значение [1..4].

Значение по умолчанию

1 пакет

Командный режим

CONFIG SWITCH

Пример

```
SBC2000-[CONFIG]-[SWITCH]> backup-interface mac-duplicate 4
```

backup-interface preemption

Данной командой указывается, что необходимо осуществлять переключение трафика на основной интерфейс при восстановлении связи. Если настроено восстановление основного интерфейса при активном резервном, то тогда при поднятии линка на основном интерфейсе, трафик будет переключен на него. Использование отрицательной формы команды (no) восстанавливает настройку по умолчанию.

Синтаксис

[no] backup-interface preemption

Параметры

Команда не содержит аргументов.

Значение по умолчанию

Переключение отключено.

Командный режим

CONFIG SWITCH

Пример

```
SBC2000-[CONFIG]-[SWITCH]> backup-interface preemption
```

show interfaces backup

Данная команда позволяет просмотреть настройки резервирования интерфейсов.

Синтаксис

show interfaces backup

Параметры

Команда не содержит аргументов.

Командный режим

CONFIG SWITCH

Пример

```
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 *Настройка протокола LLDP*

lldp enable

Данной командой разрешается работа коммутатора по протоколу LLDP.

Использование отрицательной формы команды (no) запрещает коммутатору использование протокола LLDP.

Синтаксис

[no] lldp enable

Параметры

Команда не содержит аргументов.

Командный режим

CONFIG SWITCH

Пример

```
SBC2000-[CONFIG]-[SWITCH]> lldp enable
```

lldp hold-multiplier

Данной командой задается величина времени для принимающего устройства, в течение которого нужно удерживать принимаемые пакеты LLDP перед их сбросом.

Данная величина передается на принимаемую сторону в LLDP update пакетах (пакетах обновления), является кратностью для таймера LLDP (lldp timer). Таким образом, время жизни LLDP пакетов рассчитывается по формуле TTL = min(65535, LLDP-Timer * LLDP-HoldMultiplier).

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

lldp hold-multiplier <hold>

no lldp hold-multiplier

Параметры

<hold> — время, принимает значение [2 .. 10] секунды.

Значение по умолчанию

Значение по умолчанию — 4 секунды.

Командный режим

CONFIG SWITCH

Пример

```
SBC2000-[CONFIG]-[SWITCH]> lldp hold-multiplier 5
```

lldp reinit

Данной командой устанавливается минимальное время, которое LLDP-порт будет ожидать перед повторной инициализацией LLDP.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

lldp reinit <reinit>

no lldp reinit

Параметры

<reinit> — время, принимает значение [1 .. 10] секунд.

Значение по умолчанию

Значение по умолчанию — 2 секунды.

Командный режим

CONFIG SWITCH

Пример

```
SBC2000-[CONFIG]-[SWITCH]> lldp reinit 3
```

lldp timer

Данной командой определяется, как часто устройство будет отправлять обновление информации LLDP.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

lldp timer <timer>

no lldp timer

Параметры

<timer> — время, принимает значение [5..32768] секунд.

Значение по умолчанию

Значение по умолчанию — 30 секунды.

Командный режим

CONFIG SWITCH

Пример

```
SBC2000-[CONFIG]-[SWITCH]> lldp timer 60
```

lldp tx-delay

Данной командой устанавливается задержка между последующими передачами пакетов LLDP, инициированными изменениями значений или статуса в локальных базах данных MIB LLDP.

Рекомендуется, чтобы данная задержка была меньше, чем значение 0.25* LLDP-Timer.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию.

Синтаксис

lldp tx-delay <txdelay>

no lldp tx-delay

Параметры

<txdelay> — время, принимает значение [1..8192] секунд.

Значение по умолчанию

Значение по умолчанию — 2 секунды.

Командный режим

CONFIG SWITCH

Пример

```
SBC2000-[CONFIG]-[SWITCH]> lldp tx-delay 3
```

lldp lldpdu

Данной командой устанавливается режим обработки пакетов LLDP, когда протокол LLDP выключен.

Использование отрицательной формы команды (no) устанавливает значение по умолчанию (filtering).

Синтаксис

lldp lldpdu [mode]

no lldp lldpdu

Параметры

[mode] — режим обработки пакетов LLDP:

- filtering — указывает, что LLDP-пакеты фильтруются, если протокол LLDP выключен на коммутаторе;
- flooding — указывает, что LLDP-пакеты передаются, если протокол LLDP выключен на коммутаторе.

Командный режим

CONFIG SWITCH

Пример

```
SBC2000-[CONFIG]-[SWITCH]> lldp lldpdu flooding
```

show lldp configuration

Данная команда позволяет просмотреть LLDP конфигурацию всех физических интерфейсов устройства либо заданных интерфейсов.

Синтаксис

show lldp configuration [<interface>< number >]

Параметры

Опциональные параметры, если их опустить, то на дисплей будет выведена информация по всем портам.

[interface] — тип интерфейса:

- front-port — внешние uplink-интерфейсы;
- port-channel — группы агрегации LAG внешних uplink-интерфейсов.

[number] — номер порта (можно указать несколько портов перечислением через «,» либо указать диапазон портов через «-»):

- для front port: <unit/port>, где:
  - unit — номер модуля, принимает значения [1],
  - port — номер порта принимает значения [0 .. 3];
- для port-channel: [0 .. 4].

Значение по умолчанию

На дисплей будет выведена информация по всем портам.

Командный режим

CONFIG SWITCH

Пример

```
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

Данная команда позволяет просмотреть информацию о соседних устройствах, на которых работает протокол LLDP.

Синтаксис

show lldp neighbor [<interface>< number >]

Параметры

Опциональные параметры, если их опустить, то на дисплей будет выведена информация по всем портам.

[interface] — тип интерфейса:

- front-port — внешние uplink-интерфейсы;
- port-channel — группы агрегации LAG внешних uplink-интерфейсов.

[number] — номер порта (можно указать несколько портов перечислением через «,» либо указать диапазон портов через «-»):

- для front port: <unit/port>, где:
  - unit — номер модуля, принимает значения [1],
  - port — номер порта, принимает значения [0 .. 3];
- для port-channel: [0 .. 4].

Значение по умолчанию

На дисплей будет выведена информация по всем портам.

Командный режим

CONFIG SWITCH

Пример

```
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

Данная команда позволяет просмотреть LLDP-информацию, которую анонсирует данный порт.

Синтаксис

show lldp local [<interface>< number >]

Параметры

Опциональные параметры, если их опустить, то на дисплей будет выведена информация по всем портам.

[interface] — тип интерфейса:

- front-port — внешние uplink-интерфейсы;
- port-channel — группы агрегации LAG внешних uplink-интерфейсов.

[number] — номер порта (можно указать несколько портов перечислением через «,» либо указать диапазон портов через «-»):

- для front port: <unit/port>, где:
  - unit — номер модуля, принимает значения [1],
  - port — номер порта принимает значения [0 .. 3];

– для port-channel: [0 .. 4].

Значение по умолчанию

На дисплей будет выведена информация по всем портам.

Командный режим

CONFIG SWITCH

Пример

```
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

Данная команда позволяет просмотреть статистику LLDP для интерфейсов front-port, port-channel.

Синтаксис

show lldp statistics [<interface>< number >]

Параметры

Опциональные параметры, если их опустить, то на дисплей будет выведена информация по всем портам.

[interface] — тип интерфейса:

– front-port — внешние uplink-интерфейсы;
– port-channel — группы агрегации LAG внешних uplink-интерфейсов.

[number] — номер порта (можно указать несколько портов перечислением через «,» либо указать диапазон портов через «-»):

– для front port: <unit/port>, где:
  - unit — номер модуля, принимает значения [1],
  - port — номер порта принимает значения [0 .. 3];
– для port-channel: [0 .. 4];
– для slot-channel: [0 .. 15].

Значение по умолчанию

На дисплей будет выведена информация по всем портам.

Командный режим

CONFIG SWITCH

Пример

```
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

Команда служит для просмотра способа обработки LLDPDU-пакетов для интерфейсов, где функция LLDP отключена.

Синтаксис

show lldp lldpdu

Параметры

Команда не содержит аргументов.

Командный режим

CONFIG SWITCH

Пример

```
SBC2000-[CONFIG]-[SWITCH]> show lldp lldpdu
Global: flooding
```

4.3.11 *Настройка QOS*

qos default

Данной командой указывается приоритетная очередь, в которую будут поступать пакеты без предустановленных правил. Очередь со значением 7 считается наиболее приоритетной.

Синтаксис

qos default <queue>

Параметры

< queue > — номер приоритетной очереди, принимает значения [0 .. 7].

Значение по умолчанию

По умолчанию используется очередь 0.

Командный режим

CONFIG SWITCH

Пример

```
qos default 6
```

Пакеты, для которых не установлены другие правила, поступают в очередь с приоритетом 6.

qos type

Данная команда позволяет установить правило, по которому будет осуществляться выбор поля приоритета для пакета.

На основе установленных правил в системе будет приниматься решение, по какому методу будет осуществляться приоритезация трафика (IEEE 802.1p/DSCP).

- В системе различают следующие методы приоритезации трафика:
- Все приоритеты равноправны;
- Выбор пакетов по стандарту IEEE 802.1p;
- Выбор пакетов только по IP ToS (тип обслуживания) на 3 уровне — поддержка Differentiated Services Codepoint (DSCP);
- Взаимодействие либо по 802.1p, либо по DSCP/TOS;

Синтаксис

qos type <type>

Параметры

<type> — метод приоритезации трафика:

- 0 — все приоритеты равноправны;
- 1 — выбор пакетов только по 802.1p (поле Priority в 802.1Q Tere);
- 2 — выбор пакетов только по DSCP/TOS (поле Differentiated Services заголовка IP-пакета, старшие 6 бит);
- 3 — взаимодействие либо по 802.1p, либо по DSCP/TOS.

Значение по умолчанию

По умолчанию все приоритеты равноправны.

Командный режим

CONFIG SWITCH

Пример

```
qos type 2
```

Приоритезация трафика будет осуществляться только по DSCP/TOS.

qos map

Данной командой задаются параметры для приоритетной очереди:

- указывается значение поля Differentiated Services заголовка IP пакета, старшие 6 бит,
- значение поля Priority в 802.1Q Tere.

На основе правил, установленных командой qos type, и заданных значений приоритета осуществляется отбор пакетов в данную приоритетную очередь.

Использование отрицательной формы команды (no) позволяет удалить запись из таблицы настроек очередей.

Синтаксис

[no] qos map <type> <field values> to <queue>

Параметры

<type> — метод приоритезации трафика:

- 0 — по стандарту 802.1p (используется на 2 уровне);

- 1 — по стандарту DSCP/TOS (используется на 3 уровне).

<field values> — значение поля, по которому осуществляется отбор пакетов устанавливается в зависимости от <параметра 1> (значения полей вводятся через запятую, либо как диапазон через «-»):

- если <type> = 0, то устанавливается значение поля Priority в 802.1Q Tege: [0 .. 7];
- если <type> = 1, то устанавливаются значения полей *Differentiated Services* заголовка IP-пакета, старшие 6 бит. Значение вводится в 10-чном формате: [0 .. 63].

<queue> — номер приоритетной очереди, принимает значения [0 .. 7].

Командный режим

CONFIG SWITCH

Пример

```
qos map 0 7 7
```

Для 7-ой приоритетной очереди указано значение поля priority = 7 в 802.1Q Tege.

cntrset

Данной командой осуществляется привязка сборщика статистики очередей к очередям с заданными критериями.

Синтаксис

cntrset <PORT> <UNIT> <SET> <VLAN> <QUEUE> <DROP PRECEDENCE>

Параметры

< PORT > — тип порта для подсчета принимает значения:

- all — все порты;
- cpu — CPU-порт;
- front-port — counting front-port;
- host-port;
- sm-port.

< UNIT > — порядковый номер порта:

- для cpu: принимает значения [1];
- для front port: <unit/port>, где:
  - unit — номер модуля, принимает значения [1];
  - port — номер порта, принимает значения [0 .. 3].
- для host-port: <unit/port>, где:
  - unit — номер модуля, принимает значения [1];
  - port — номер порта, принимает значения [0 .. 2].
- для sm-port: <unit/port>, где:
  - unit — номер модуля, принимает значения [1];
  - port — номер порта, принимает значения [0 .. 5].
- < SET > — номер сборщика статистики, принимает значения [0 .. 1];
- < VLAN > — идентификационный номер VLAN, принимает значения [1 .. 4094] или all;
- < QUEUE > — номер очереди, принимает значения [0 .. 7] или all;
- < DROP PRECEDENCE > — значение drop precedence [0 .. 1] или all.

-

Командный режим

CONFIG – SWITCH

Пример

```
cntrset sm-port 1/2 1 22 2 1
```

show cntrset

Команда для просмотра информации сборщика очередей.

Синтаксис

show cntrset <SET>

Параметры

<SET> — номер счетчика [0 .. 1].

Командный режим

CONFIG – SWITCH

show qos

Данная команда предназначена для просмотра назначенных очередям приоритетов. По умолчанию приоритет очереди равен 0. Значение приоритета для очереди устанавливается в диапазоне [0 .. 7], очередь со значением приоритета 7 считается наиболее приоритетной.

Синтаксис

show qos

Параметры

Команда не содержит аргументов.

Командный режим

CONFIG – SWITCH

4.3.12 *Команды работы с конфигурацией*

У коммутатора SBC-2000 есть 2 типа конфигурации:

- running-config — конфигурация, которая в данный момент активна на устройстве;
- candidate-config — конфигурация, в которую внесены какие-либо изменения, running-config она станет после ее применения командой apply.

Просмотр конфигурации

show running-config

Синтаксис

show running-config

Параметры

Команда не содержит аргументов.

Командный режим

CONFIG – SWITCH

show candidate-config

Синтаксис

show candidate-config

Параметры

Команда не содержит аргументов.

Командный режим

CONFIG – SWITCH

4.3.13 *Команды применения и подтверждения конфигурации*

После выполнения действий по конфигурированию коммутатора SBC-2000 необходимо применить конфигурацию (apply), чтобы она стала активной на устройстве, и подтвердить применение (confirm) для защиты от того, что внесенные изменения стали причиной потери доступа до устройства. Если в течение 60 сек. не было выполнено подтверждение, то конфигурация откатывается до предыдущей running-config.

Команда применения конфигурации.

Синтаксис

apply

Параметры

Команда не содержит аргументов.

Командный режим

CONFIG – SWITCH

Команда подтверждения.

Синтаксис

confirm

Параметры

Команда не содержит аргументов.

Командный режим

CONFIG – SWITCH

4.3.14 *Прочие команды*

config

Команда для возврата в меню Configuration.

Синтаксис

config

Параметры

Команда не содержит аргументов.

Командный режим

CONFIG – SWITCH

exit

Команда выхода из данного подменю конфигурирования на уровень выше

Синтаксис

exit

Параметры

Команда не содержит аргументов.

Командный режим

CONFIG – SWITCH

history

Команда просмотра истории введенных команд.

Синтаксис

history

Параметры

Команда не содержит аргументов.

Командный режим

CONFIG – SWITCH

ПРИЛОЖЕНИЕ А. РЕЗЕРВНОЕ ОБНОВЛЕНИЕ ВСТРОЕННОГО ПО УСТРОЙСТВА

В случае, когда не удается обновить ПО через Web-конфигуратор или консоль (telnet, RS-232), существует возможность резервного обновления ПО через RS-232.

Для того чтобы обновить встроенное ПО устройства, необходимы следующие программы:

- программа терминалов (например, TERATERM);
- программа TFTP-сервера.

Последовательность действий при обновлении устройства:

1. Подключиться к порту Ethernet устройства;

2. Подключить скрещенным кабелем Console-порт компьютера к Console-порту устройства;

3. Запустить терминальную программу;

4. Настроить скорость передачи 115200, формат данных 8 бит, без паритета, 1 бит стоповый, без управления потоком;

5. Запустить на компьютере программу *tftp* сервера и указать путь к папке *smg_files*, в ней создать папку *smg2016*, в которую поместить файлы *smg2016_kernel, smg2016_initrd для SBC-2000* (*smg1016M_kernel, smg1016M_initrd для SBC-1000*) (компьютер, на котором запущен TFTP-server, и устройство должны находиться в одной сети);

6. Включить устройство и в окне терминальной программы остановить загрузку путем введения команды “**stop**”:

Для 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>>
```

Для 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. Ввести **set ipaddr** <IP-адрес устройства> <ENTER>;

   Пример: `set ipaddr 192.168.2.2`

8. Ввести **set netmask** <сетевая маска устройства> <ENTER>;

   Пример: `set netmask 255.255.255.0`

9. Ввести **set serverip** <IP-адрес компьютера, на котором запущен tftp сервер> <ENTER>;

   Пример: `set serverip 192.168.2.5`

10. Для SBC-1000 dвести **mii si** <ENTER> для активации сетевого интерфейса:

```
=> mii si
Init switch 0: ..Ok!
Init switch 1: ..Ok!
Init phy 1: ..Ok!
Init phy 2: ..Ok!
=>
```

11. Обновить ядро Linux командой **run flash_kern**:

    Для 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>>
```

    Для 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. Обновить файловую систему командой **`run flash_initrd`**:

Для 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>>
```

Для SBC-1000:

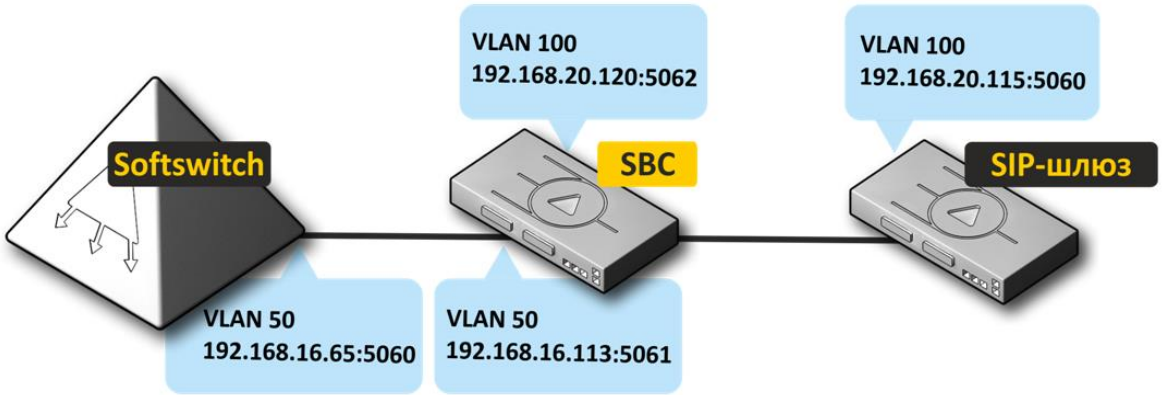
```
=> run flash_initrd
Using ppc_4xx_eth0 device
TFTP from server 192.168.2.5; our IP address is 192.168.2.2
Filename ' smg/smg1016M_initrd'.
Load address: 0x400000
Loading: ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ####################
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. Запустить устройство командой **`run bootcmd`**.

ПРИЛОЖЕНИЕ Б. ПРИМЕРЫ НАСТРОЙКИ SBC

1. Настройка SBC для SIP абонентов

Схема применения



Алгоритм работы

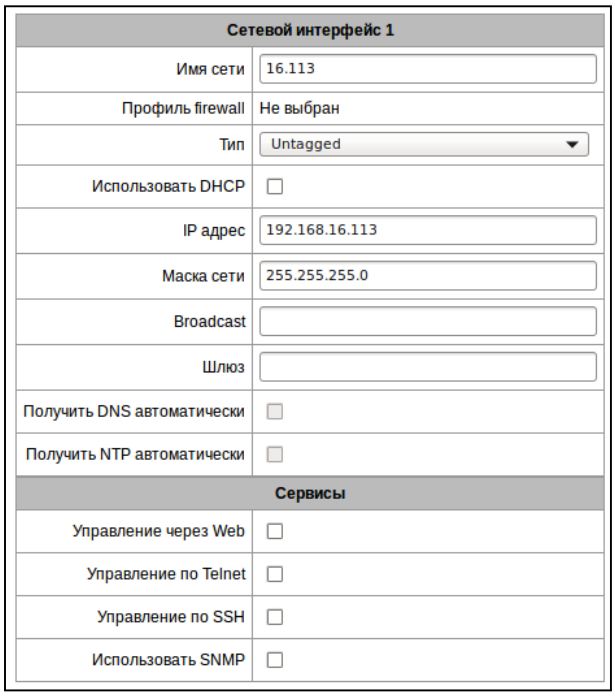
Абонентский шлюз отправляет сообщение на IP-адрес 192.168.20.120 порт 5062, SBC-2000 пересылает данный трафик с IP-адреса 192.168.16.113 порт 5061 на адрес Softswitch 192.168.16.65 порт 5060.

Порядок конфигурирования SBC

1. Конфигурирование интерфейсов (меню **Конфигурация интерфейсов/Сетевые интерфейсы, раздел 4.1.4.3**).

   a. Создать интерфейс в направлении Softswitch.

Параметры интерфейса: *192.168.16.113.*



Сетевой интерфейс 1	
Имя сети	16.113
Профиль firewall	Не выбран
Тип	Untagged
Использовать DHCP	☐
IP адрес	192.168.16.113
Маска сети	255.255.255.0
Broadcast	
Шлюз	
Получить DNS автоматически	☐
Получить NTP автоматически	☐
Сервисы	
Управление через Web	☐
Управление по Telnet	☐
Управление по SSH	☐
Использовать SNMP	☐

b. Создать интерфейс в направлении абонентского шлюза.

Параметры интерфейса: *192.168.20.120.*

Сетевой интерфейс 2	
Имя сети	20.120
Профиль firewall	Не выбран
Тип	Untagged
Использовать DHCP	☐
IP адрес	192.168.20.120
Маска сети	255.255.255.0
Broadcast	
Шлюз	
Получить DNS автоматически	☐
Получить NTP автоматически	☐
Сервисы	
Управление через Web	☐
Управление по Telnet	☐
Управление по SSH	☐
Использовать SNMP	☐

2. Конфигурирование медиа для SIP (меню **Конфигурация SBC/Диапазон RTP портов, раздел 4.1.3.6**).

Необходимо задать диапазоны используемых для RTP портов.

Параметры UDP-портов для передачи RTP трафика	
Начальный порт	24000
Количество портов	1000

Применить

3. Конфигурирование SIP-транспорта (меню **Конфигурация интерфейсов/SIP транспорт, раздел 4.1.3.1**).

a. Добавить SIP-транспорт в направлении абонентского шлюза.

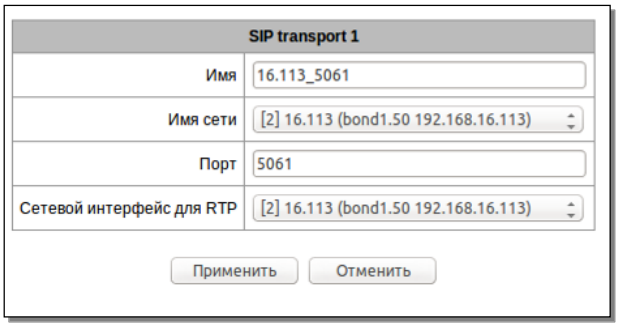
Параметры интерфейса:
сетевой интерфейс 20.120;
порт для сигнализации — 5062;
медиа — 20.120.

SIP transport 0	
Имя	20.120_5062
Имя сети	[1] 20.120 (bond1.100 192.168.20.120)
Порт	5062
Сетевой интерфейс для RTP	[1] 20.120 (bond1.100 192.168.20.120)

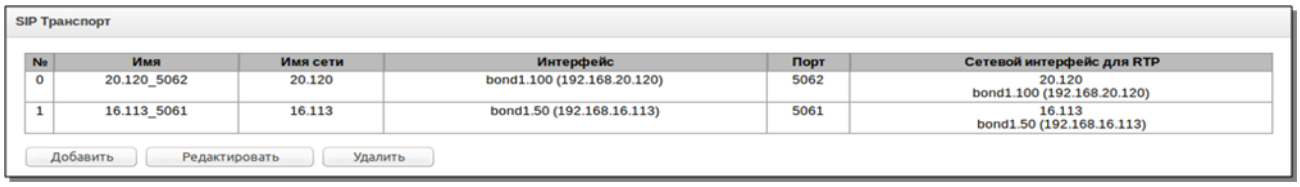
Применить Отменить

b. Добавить SIP-транспорт в направлении Softswitch.

Параметры интерфейса:
сетевой интерфейс 16.113;
порт для сигнализации — 5061;
медиа — 16.113.



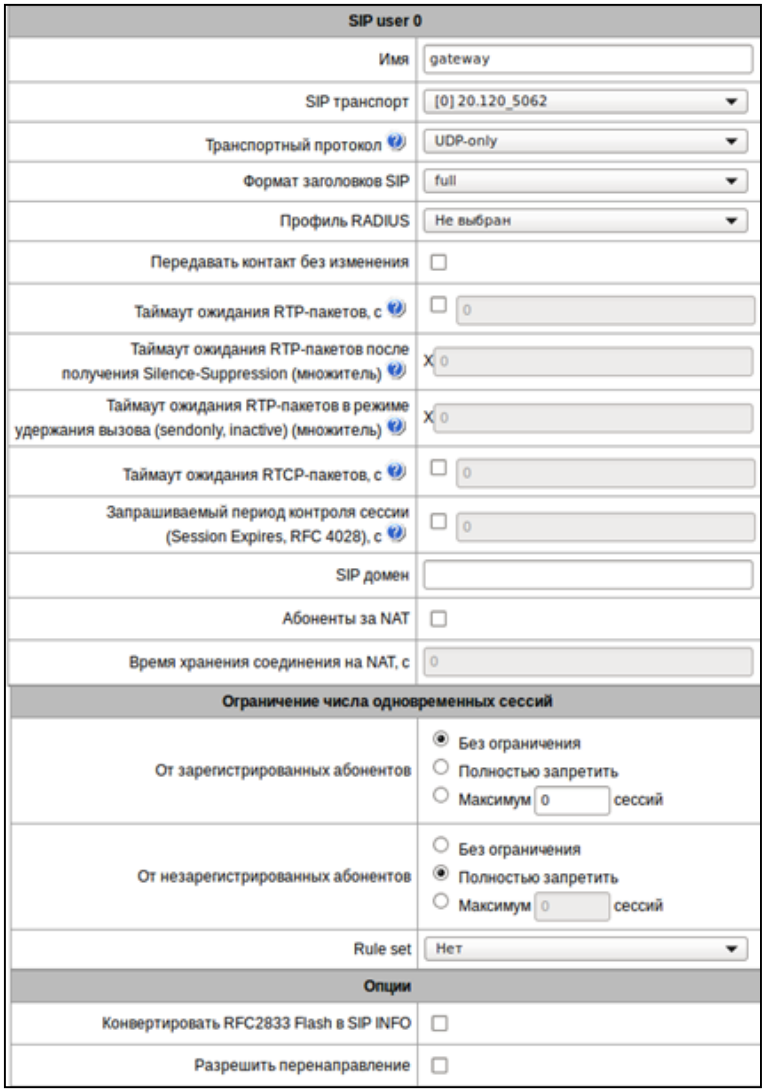
c. Таблица SIP-транспорта будет иметь следующий вид:



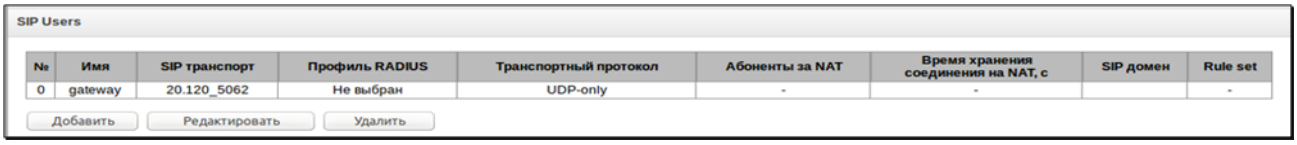
4. Конфигурирование SIP-пользователей (меню **Конфигурация SBC/SIP Users, раздел 4.1.3.3**).

a. Добавить SIP Users.

В поле *«SIP транспорт»* выбрать транспорт в направлении абонента (*20.120_50 62*), если абоненты находятся за NAT, установить флаг *«Абоненты за NAT»* и указать время хранения соединения на NAT.



b. Таблица SIP-пользователей будет иметь следующий вид:



5. Конфигурирование SIP направлений (меню **Конфигурация SBC/SIP Destination, раздел 4.1.3.2**).

   a. Добавить SIP Destination.

В поле *«SIP транспорт»* выбрать транспорт в направлении Softswitch (*16.113_5061*), в поле *«Remote address»* указать IP-адрес Softswitch.

SIP destination 0	
Имя	softswitch
SIP транспорт	[1] 16.113_5061
Remote address	192.168.16.65
Транспортный протокол	UDP-only
Формат заголовков SIP	full
Адаптация	-
Передавать контакт без изменения	☐
Таймаут ожидания RTP-пакетов, с	☐ 0
Таймаут ожидания RTP-пакетов после получения Silence-Suppression (множитель)	X 0
Таймаут ожидания RTP-пакетов в режиме удержания вызова (sendonly, inactive) (множитель)	X 0
Таймаут ожидания RTCP-пакетов, с	☐ 0
Запрашиваемый период контроля сессии (Session Expires, RFC 4028), с	☐ 0
Период проверки рабочего сервера, с (после завершения предыдущей транзакции OPTIONS)	60
Период проверки нерабочего сервера, с (после завершения предыдущей транзакции OPTIONS)	20
Аутентификация SBC	
Логин	
Пароль	
Регистрация SIP trunk	
Тип регистрации	Нет
Период регистрации, с	0
Имя пользователя/Номер	
SIP-домен	
Ограничение числа одновременных сессий	◉ Без ограничения ○ Полностью запретить ○ Максимум 0 сессий
Rule set	Нет
Опции	
Конвертировать RFC2833 Flash в SIP INFO	☐
Разрешить перенаправление	☐

b. Таблица SIP-направлений будет иметь следующий вид:

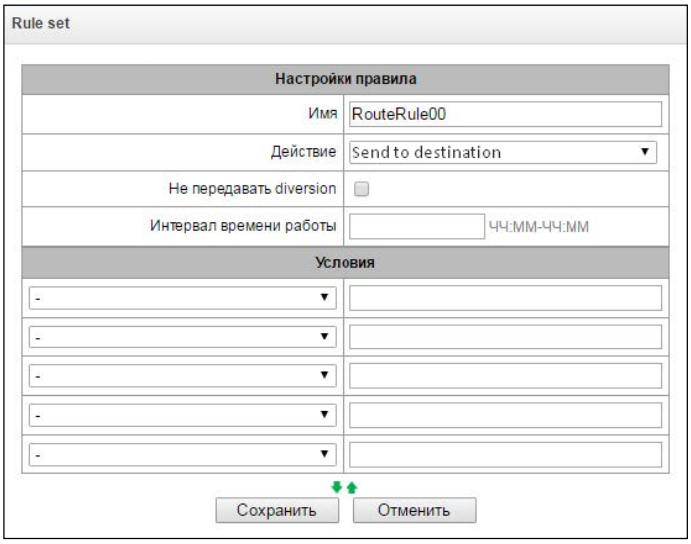
SIP Destination

№	Имя	SIP транспорт	Remote address	Адаптация	Транспортный протокол	Rule set
0	softswitch	16.113_5061	192.168.16.65	-	UDP-only	-

Добавить | Редактировать | Удалить

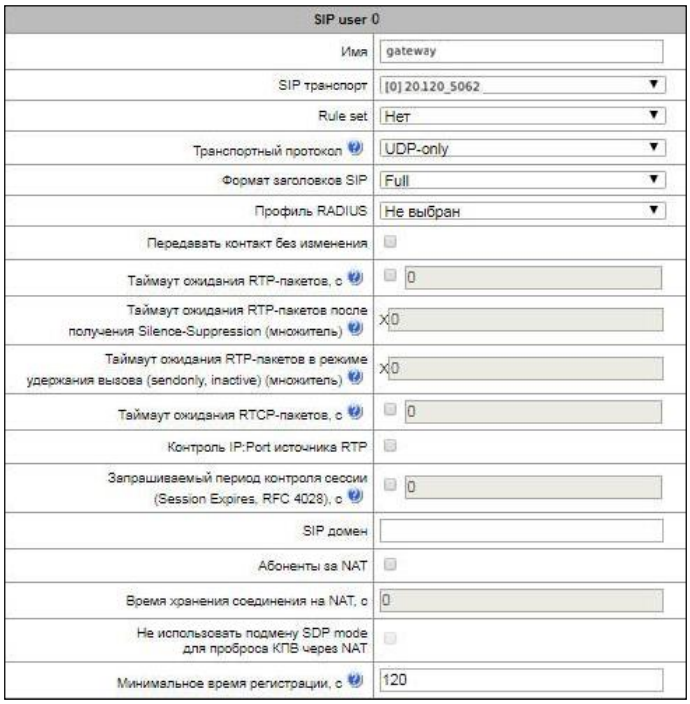
6. Конфигурирование наборов правил (меню **Конфигурация SBC/Rule set, раздел 4.1.3.5**).

Создать набор правил, указать его имя, добавить правило в набор. В поле *«Действие»* выбрать *«Send to destination»,* в поле *«SIP Destination»* указать направление, которое конфигурировалось для Softswitch. Выставить условие *«Все»,* сохранить правило и набор правил.



7. Привязка правила к направлению для абонентов.

a. Зайти в раздел *«SIP Users»,* выбрать ранее созданное направление и в поле *«Rule set»* выбрать созданный набор правил.



b. Таблица SIP пользователей будет иметь следующий вид:

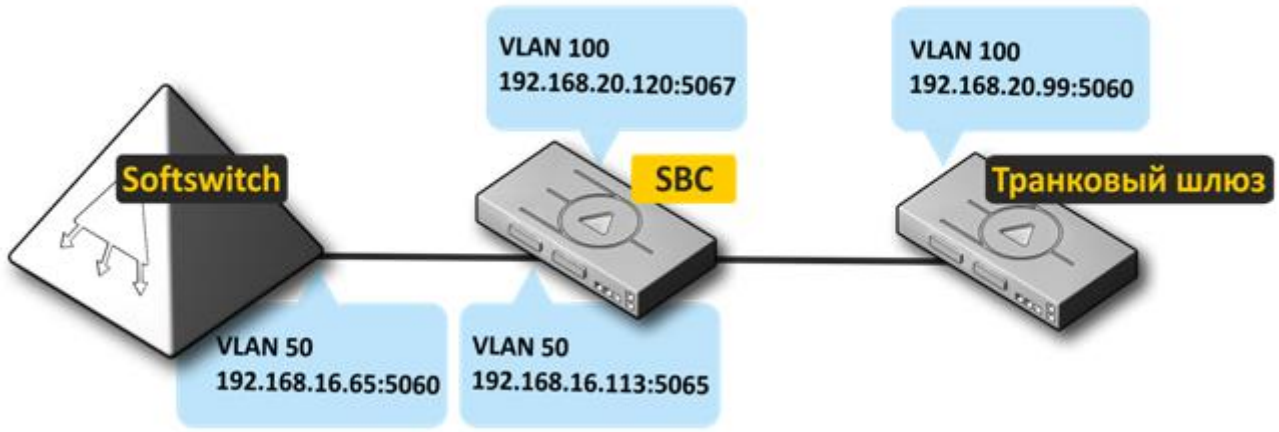
№	Имя	SIP транспорт	Профиль RADIUS	Транспортный протокол	Абоненты за NAT	Время хранения соединения на NAT, с	SIP домен	Rule set
0	gateway	20.120_5062	Не выбран	UDP-only	-	-		to_softswitch

Добавить Редактировать Удалить

8. Для применения настроек сохранить конфигурацию во Flash (меню **Сервис/Сохранить конфигурацию во FLASH, раздел 4.1.12**).

2. Настройки SBC для SIP-транков

Схема применения



SBC не анализирует типы трафика (абонентский или sip trunk), для разного трафика необходимо использовать разные порты.

Порядок конфигурирования SBC

1. Конфигурирование интерфейсов.

Подробнее в разделе 1 **Настройка SBC для SIP абонентов** данного Приложения.

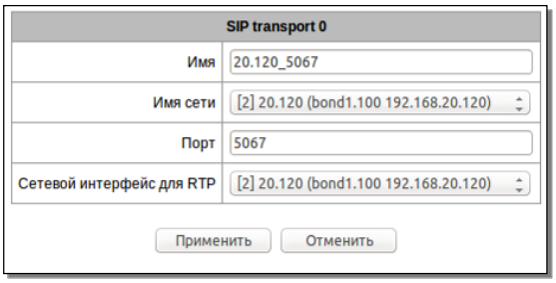
2. Конфигурирование медиа для SIP.

Подробнее в разделе 1 **Настройка SBC для SIP абонентов** данного Приложения.

3. Конфигурирование SIP-транспорта (меню **Конфигурация SBC/SIP транспорт, раздел 4.1.3.1**).

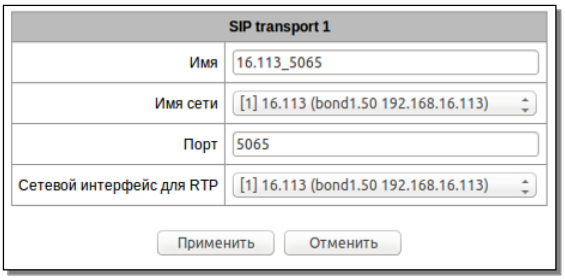
   a. Добавить SIP-транспорт в направлении транкового шлюза.

Параметры интерфейса:
сетевой интерфейс 20.120;
порт для сигнализации — 5067;
медиа — 20.120.



   b. Добавить SIP-транспорт в направлении Softswitch.

Параметры интерфейса:
сетевой интерфейс 16.113;
порт для сигнализации — 5065;
медиа — 16.113.



c. Таблица SIP-транспорта будет иметь следующий вид:

SIP Транспорт

№	Имя	Имя сети	Интерфейс	Порт	Сетевой интерфейс для RTP
0	20.120_5067	20.120	bond1.100 (192.168.20.120)	5067	20.120 bond1.100 (192.168.20.120)
1	16.113_5065	16.113	bond1.50 (192.168.16.113)	5065	16.113 bond1.50 (192.168.16.113)

Добавить | Редактировать | Удалить

4. Конфигурирование SIP-направлений (меню **Конфигурация SBC/SIP Destination, раздел 4.1.3.2**).

a. Добавить SIP destination в направлении транкового шлюза (поле *«Rule set»* на данном этапе заполнять не требуется).

SIP destination 0	
Имя	trunk_gateway
SIP транспорт	[0] 20.120_5067
Remote address	192.168.20.99
Транспортный протокол	UDP-only
Формат заголовков SIP	full
Адаптация	-
Передавать контакт без изменения	☐
Таймаут ожидания RTP-пакетов, с	☐ 0
Таймаут ожидания RTP-пакетов после получения Silence-Suppression (множитель)	X 0
Таймаут ожидания RTP-пакетов в режиме удержания вызова (sendonly, inactive) (множитель)	X 0
Таймаут ожидания RTCP-пакетов, с	☐ 0
Запрашиваемый период контроля сессии (Session Expires, RFC 4028), с	☐ 0
Период проверки рабочего сервера, с (после завершения предыдущей транзакции OPTIONS)	60
Период проверки нерабочего сервера, с (после завершения предыдущей транзакции OPTIONS)	20
Аутентификация SBC	
Логин	
Пароль	
Регистрация SIP trunk	
Тип регистрации	Нет
Период регистрации, с	0
Имя пользователя/Номер	
SIP-домен	
Ограничение числа одновременных сессий	◉ Без ограничения ○ Полностью запретить ○ Максимум 0 сессий
Rule set	Нет
Опции	
Конвертировать RFC2833 Flash в SIP INFO	☐
Разрешить перенаправление	☐

b. Добавить SIP destination в направлении Softswitch (поле *«Rule set»* на данном этапе заполнять не требуется).

SIP destination 1	
Имя	softswitch
SIP транспорт	[1] 16.113_5065
Remote address	192.168.16.65
Транспортный протокол	UDP-only
Формат заголовков SIP	full
Адаптация	-
Передавать контакт без изменения	☐
Таймаут ожидания RTP-пакетов, с	☐ 0
Таймаут ожидания RTP-пакетов после получения Silence-Suppression (множитель)	X 0
Таймаут ожидания RTP-пакетов в режиме удержания вызова (sendonly, inactive) (множитель)	X 0
Таймаут ожидания RTCP-пакетов, с	☐ 0
Запрашиваемый период контроля сессии (Session Expires, RFC 4028), с	☐ 0
Период проверки рабочего сервера, с (после завершения предыдущей транзакции OPTIONS)	60
Период проверки нерабочего сервера, с (после завершения предыдущей транзакции OPTIONS)	20
Аутентификация SBC	
Логин	
Пароль	
Регистрация SIP trunk	
Тип регистрации	Нет
Период регистрации, с	0
Имя пользователя/Номер	
SIP-домен	
Ограничение числа одновременных сессий	◉ Без ограничения ○ Полностью запретить ○ Максимум 0 сессий
Rule set	Нет
Опции	
Конвертировать RFC2833 Flash в SIP INFO	☐
Разрешить перенаправление	☐

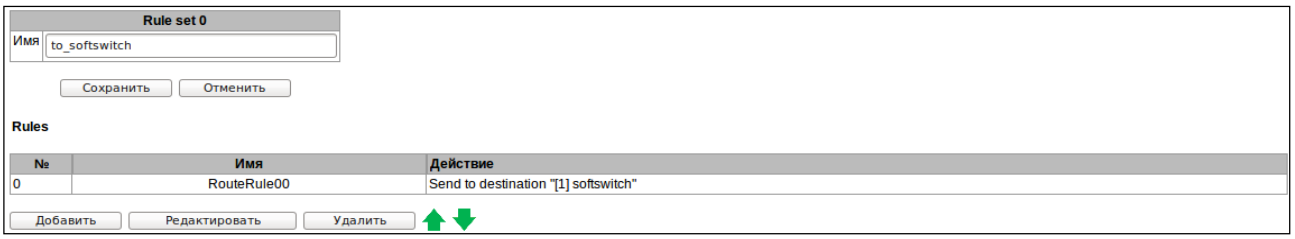
c. Таблица SIP-направлений будет иметь следующий вид:

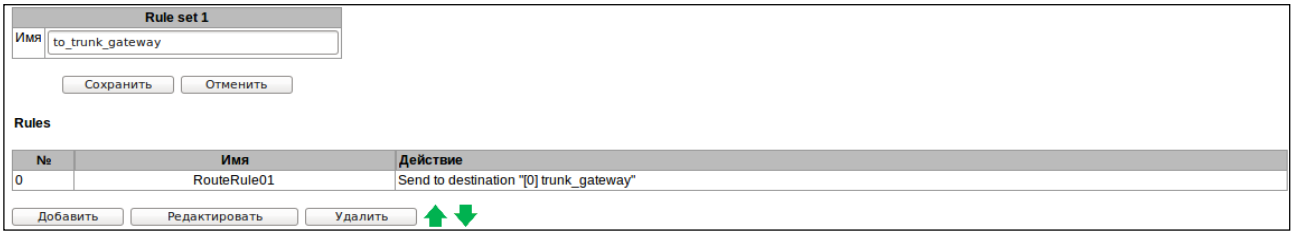
№	Имя	SIP транспорт	Remote address	Адаптация	Транспортный протокол	Rule set
0	trunk_gateway	20.120_5067	192.168.20.99	-	UDP-only	-
1	softswitch	16.113_5065	192.168.16.65	-	UDP-only	-

Добавить | Редактировать | Удалить

5. Конфигурирование наборов правил (меню **Конфигурация SBC/Rule set, раздел 4.1.3.5**).

Создать два набора правил. В первом в поле *«SIP Destination»* указать направление, которое конфигурировалось для Softswitch. Во втором указать направление на транковый шлюз.





6. Привязать правило к направлениям.

Для привязки в настройках направления для Softswitch в разделе *«SIP Users»* выбрать набор правил, у которого в правиле, в поле *«SIP destination»* указано направление на транковый шлюз. Соответственно в настройках направления для транкового шлюза выбрать другой набор правил, направляющий всё на Softswitch.

Таблица SIP-направлений будет иметь следующий вид:

№	Имя	SIP транспорт	Remote address	Адаптация	Транспортный протокол	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

Добавить Редактировать Удалить

7. Для применения настроек сохранить конфигурацию во Flash (меню **Сервис/Сохранить конфигурация во FLASH, раздел 4.1.12**).

ПРИЛОЖЕНИЕ В. ОБЕСПЕЧЕНИЕ ФУНКЦИИ РЕЗЕРВИРОВАНИЯ SBC

Начиная с версии 1.7.0, на SBC реализована функция резервирования. Данная функция активируется автоматически установкой дополнительной лицензии SBC-RESERVE. Принцип работы заключается в том, что резервирующее устройство находится в спящем режиме (SLAVE), не неся никаких функций и не имея своего IP-адреса в сети, постоянно наблюдает за основным устройством (MASTER) и, как только MASTER выходит из строя SLAVE, принимает все функции на себя, полностью заменяя вышедшего из строя MASTER. Для полного дублирования функции резервирующее устройство постоянно получает от основного актуальную конфигурацию, базу данных абонентов и другие, необходимые для работы файлы.

Для обеспечений функций резервирования используются только однотипные устройства SBC-2000 либо SBC-3000.

Рассмотрим схемы подключения:

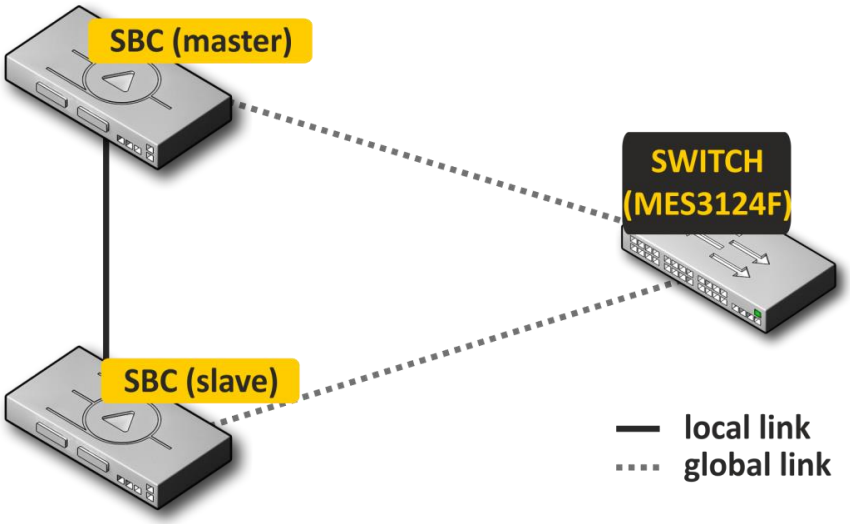


Рисунок 33 — Схема резервирования с одним коммутатором

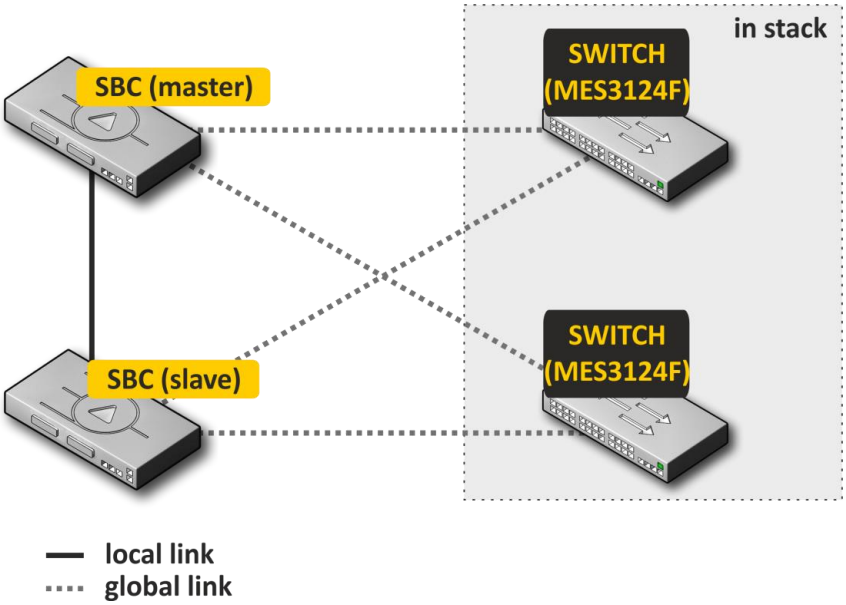


Рисунок 34 — Схема резервирования двумя коммутаторами в стеке

При резервировании на устройстве выделяется 2 типа front-порта, это локальный и глобальный. На SBC-2000 локальные порты — это 0 и 1, глобальные — 2 и 3. На SBC-3000 локальные порты — это 1 и 2, глобальные — 3 и 4. При соединении устройств необходима связь одновременно по локальному и глобальному линку. Схема резервирования работает по протоколу IPv6, в процессе работы устройства обмениваются конфигурационными и другими, необходимыми для поддержания актуальной информации файлами. Для связи по локальному линку используется 4091 VLAN, по глобальному 4092 VLAN. В случае разрыва по локальному линку устройства обмениваются рабочими файлами по глобальному линку.

При разрыве связи по одному из линков устройство инициирует аварию.

Порядок подключения и настройки резерва

Будет рассмотрен случай подключения к двум коммутаторам MES в стеке (Рисунок 35). Исходное состояние: две однотипные SBC с лицензией резерва, два коммутатора MES в стеке. Настройка стека на коммутаторах производится согласно документации на коммутаторы.

Для начала следует настроить прохождение служебных VLAN на коммутаторах. На портах, куда будут подключены global линки SBC, следует разрешить прохождение VLAN 4092. При этом порты должен пропускать и прочие VLAN, настроенные на SBC. Также порты, к которым будут подключаться SBC, следует объединить в port-channel. Итоговая схема на этом этапе будет выглядеть так:

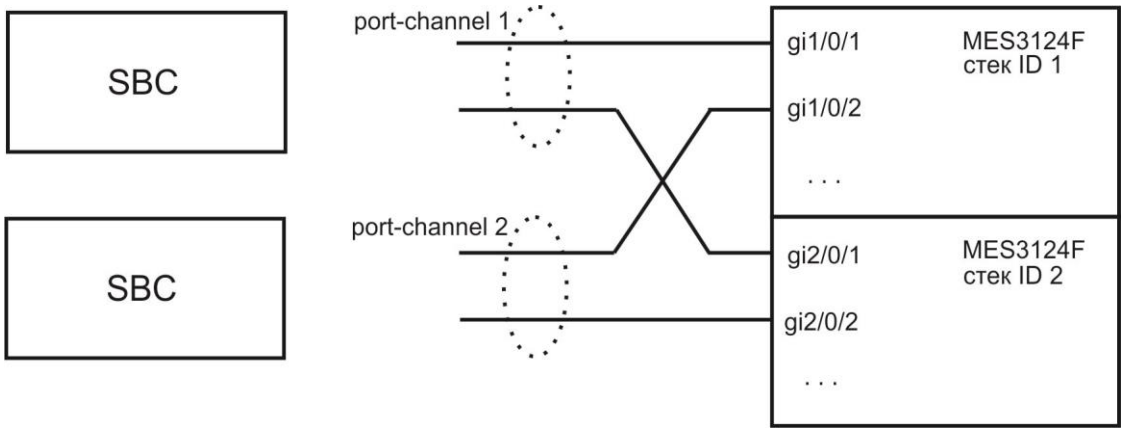


Рисунок 35 — Схема объединения портов в port-chanel

Далее производится подключение ведущей (master) SBC. На этом этапе подключаются только global линки. После этого SBC запускается в работу и становится ведущей (master). Схема на этом этапе будет выглядеть так:

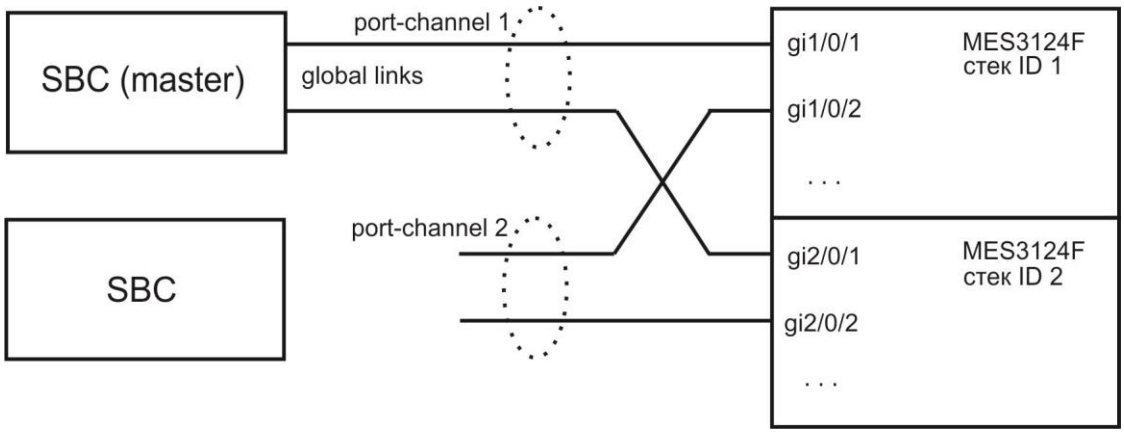


Рисунок 36 — Схема подключения ведущей SBC (master)

После этого к ведущей (master) SBC local линком подключается ведомый (slave) SBC. На этом этапе следует дождаться, пока устройства не обнаружат друг друга и не включатся в работу как пара ведомый-ведущий (см. раздел Мониторинг - Резерв). Схема на этом этапе будет выглядеть так:

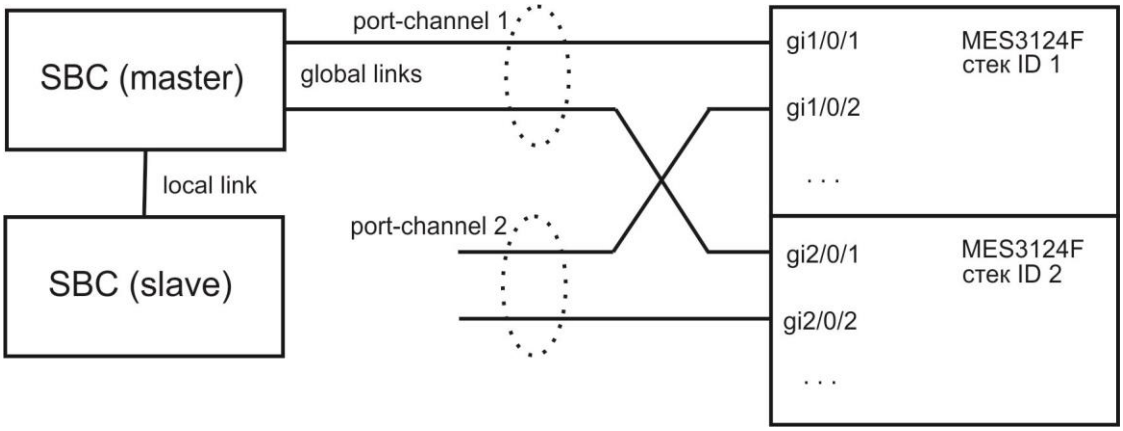


Рисунок 37 — Схема подключения ведомого SBC (slave)

После того, как пара ведомы-ведущий была образована, можно подключить global линки на ведомое устройство:

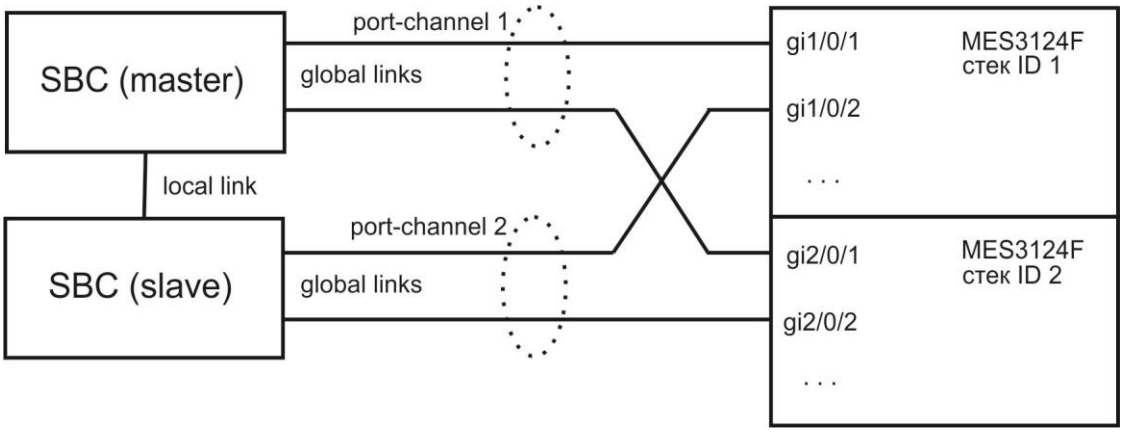


Рисунок 38 — Схема подключения global links

Сборка резерва на этом завершается. В мониторинге следует убедиться, что обе SBC видят друг друга как на локальном, так и на глобальном линке.

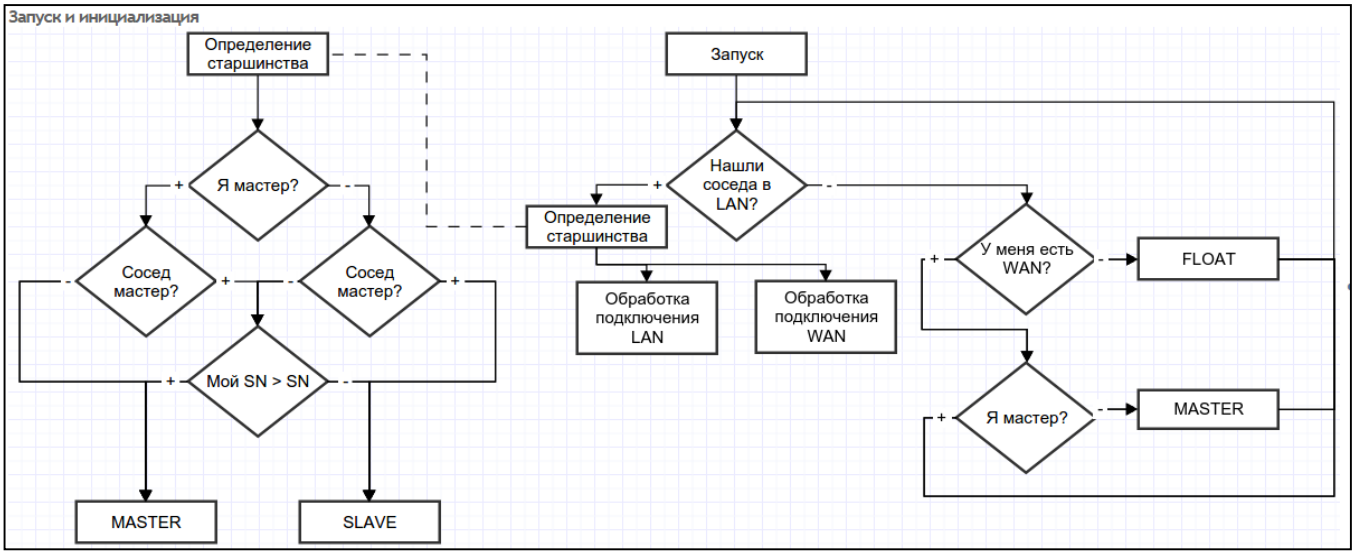
В случае возникновения проблем с установлением отношений ведущий-ведомый или отсутствия видимости по локальному и глобальному линкам следует проверить правильность выполнения всех этапов настройки.

Определение старшинства

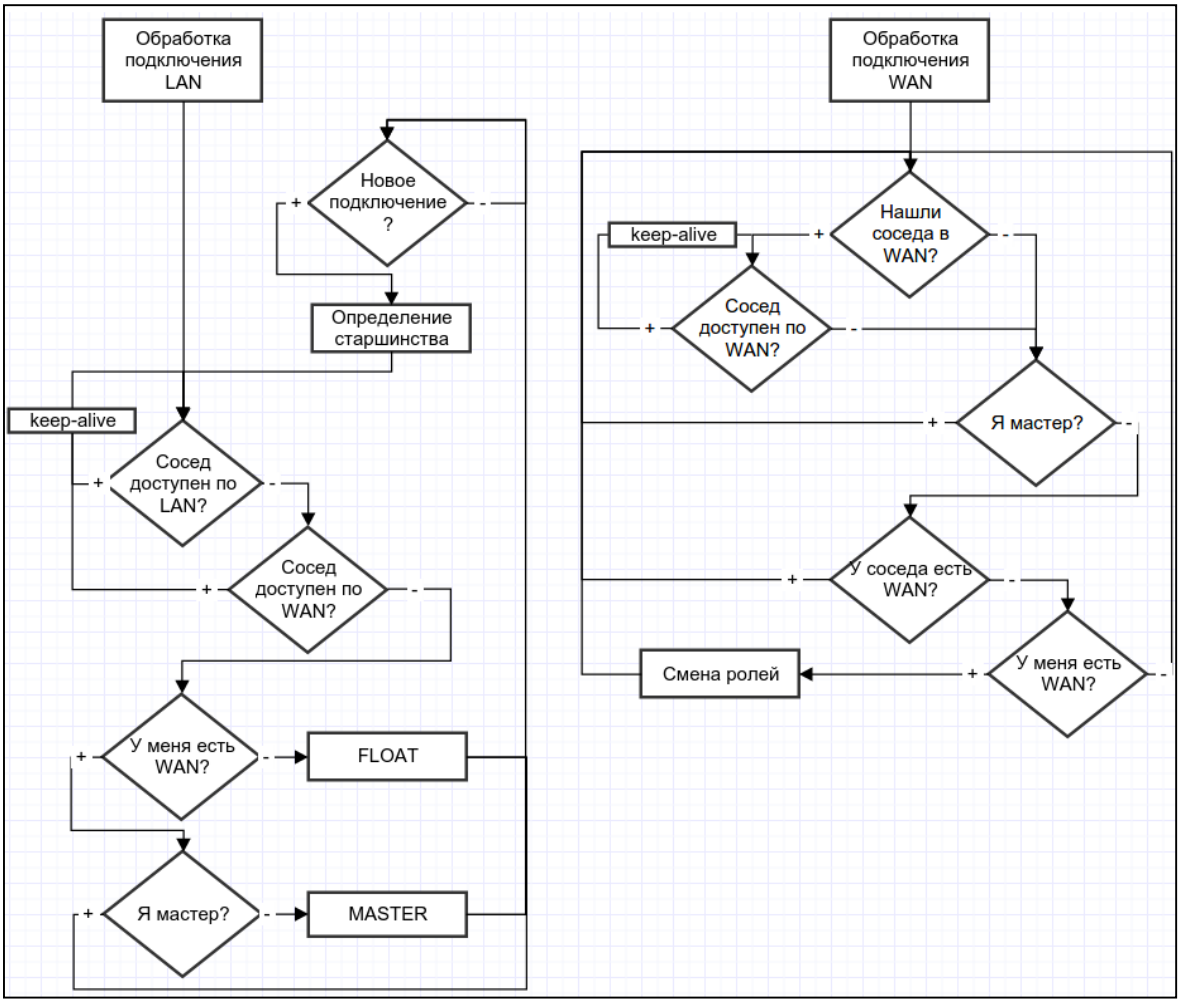
При определении кто из устройств будет MASTER или SLAVE используется следующий алгоритм:

- Если при включении устройства локальные линки не активны, то устройства становится MASTER.
- Если при включении устройства глобальные линки не активены, то устройство становится SLAVE.
- Если в процессе работы к устройству, которое является MASTER, подключить SLAVE, то старшинство не изменится.
- Если в процессе работы к устройству, которое является MASTER, подключить MASTER, то старшинство определится на основе серийного номера, у кого серийный номер больше, тот станет MASTER.

Блок схемы определения старшинства:



Обработка подключении по глобальному или локальному линку.



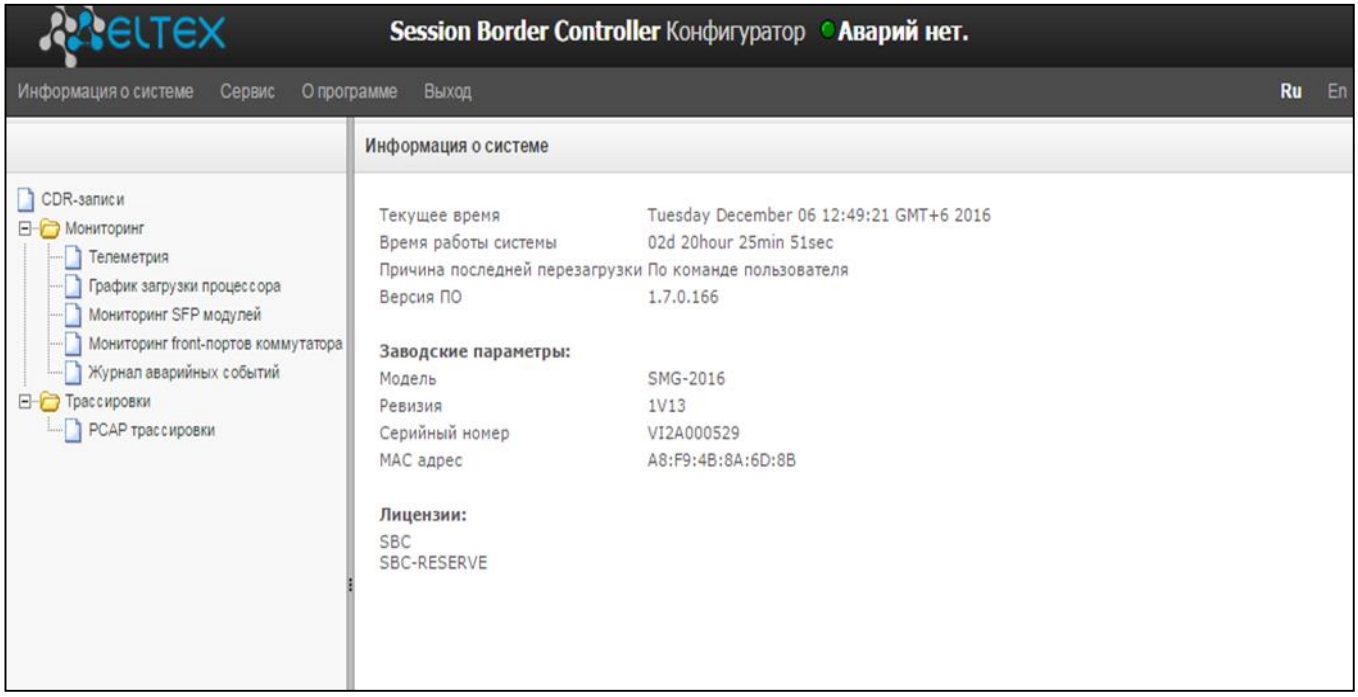
При подключении устройства к уже работающему, необходимо отключить все WAN линки на подключаемом устройстве, подключить LAN линк к работающему (MASTER) SBC, дождаться согласования, подключить WAN линки к SLAVE, иначе вновь подключаемое устройство может определится как MASTER и передать свои неактуальные рабочие файлы.

Рабочие файлы передаются сразу после подключении к MASTER, каждый раз после записи конфигурации на flash, спустя 10 секунд после каждого изменения конфигурации и периодически раз в 180 секунд.

Список передаваемых файлов:

- файл конфигурации записаной во flash;
- файл текущей запущенной конфигурации;
- ключи для создания ssh-туннелей;
- база даных зарегистрированных абонентов;
- файлы пользователей linux;
- файлы паролей пользователей Web-интерфейса и CLI;
- все списки адресов динамического брандмауэра;
- ключи и сертификаты для протокола https.

В процессе работы пользователь может зайти на Web-интерфейс SLAVE, для этого необходимо зайти в закладку "Мониторинг" - "Резервирование" - "открыть Веб", либо по ссылке: http://192.168.0.100:8080/login, где вместо 192.168.0.100 ввести IP-адрес MASTER.



ПРИЛОЖЕНИЕ Г. УПРАВЛЕНИЕ И МОНИТОРИНГ ПО ПРОТОКОЛУ SNMP

SBC поддерживает мониторинг и конфигурирование при помощи протокола SNMP (Simple Network Management Protocol).

Реализованы следующий функции мониторинга:
- сбор общей информации об устройстве, показаниях датчиков, установленном ПО;
- состояние SIP-интерфейсов;
- сбор статистики SIP

Реализованы следующие функции управления:
- обновление программного обеспечения устройства;
- сохранение текущей конфигурации;
- перезагрузка устройства;
- управление SIP-абонентами.

В таблицах с описанием OID в колонке “запросы” будет принят следующий формат описания:
- Get — значение объекта или дерева можно прочитать, отправив GetRequest.
- Set — значение объекта можно установить, отправив SetRequest (обратите внимание, при установке значения через SET к OID следует привести к виду “OID.0”);
- {} — имя объекта или OID;
- N — в команде используется числовой параметр типа integer;
- U — в команде используется числовой параметр типа unsigned integer;
- S — в команде используется строковый параметр;
- A — в команде используется IP-адрес (обратите внимание, некоторые команды, принимающие как аргумент IP-адрес, используют строковый тип данных “s”).

Таблица Г.1 — Примеры команд

Описание запроса	Команда
`Get {}`	snmpwalk -v2c -c public -m +ELTEX-SBC $ip_sbc activeCallCount
`Get {}.x`	snmpwalk -v2c -c public -m +ELTEX-SBC $ip_sbc pmExist.1 snmpwalk -v2c -c public -m +ELTEX-SBC $ip_sbc pmExist.2 и т.д.
`Set {} N`	snmpset -v2c -c public -m +ELTEX-SBC $ip_sbc \ 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 \ getGroupUserByID.0 u 2
`Set {} S`	snmpset -v2c -c private -m +ELTEX-SBC $ip_sbc \ sbcUpdateFw.0 s \ "smg1016m_firmware_sbc_1.9.0.51.bin 192.0.2.2"
`Set {} "NULL"111`	snmpset -v2c -c private -m +ELTEX-SBC $ip_sbc \ getUserByNumber.0 s "NULL"
`Set {} A111`	snmpset -v2c -c private -m +ELTEX-SBC $ip_sbc \ sbcSyslogTracesAddress.0 a 192.0.2.44

Примеры выполнения запросов:

Ниже приведённые запросы эквивалентны. Пример запроса объекта sbcActiveCallsCount, который отображает число текущих вызовов на 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
```

Описание OID из MIB ELTEX-SMG

Таблица Г.2 — Общая информация и датчики

Имя	OID	Запросы	Описание
sbc	1.3.6.1.4.1.35265.1.49	`Get {}`	Корневой объект для дерева OID
sbcDevName	1.3.6.1.4.1.35265.1.49.1	`Get {}`	Имя устройства
sbcDevType	1.3.6.1.4.1.35265.1.49.2	`Get {}`	Тип устройства (всегда 49)
sbcFwVersion	1.3.6.1.4.1.35265.1.49.3	`Get {}`	Версия ПО
sbcUptime	1.3.6.1.4.1.35265.1.49.5	`Get {}`	Время работы ПО
sbcUpdateFw	1.3.6.1.4.1.35265.1.49.25	`Set {} S`	Обновление ПО. Для этого следует сделать запрос Set с параметрами (разделить пробелом): - имя файла ПО без пробелов; - адрес TFTP-сервера
sbcReboot	1.3.6.1.4.1.35265.1.49.27	`Set {} 1`	Перезагрузка оборудования
sbcSave	1.3.6.1.4.1.35265.1.49.29	`Set {} 1`	Сохранение конфигурации
sbcFreeSpace	1.3.6.1.4.1.35265.1.49.32	`Get {}`	Свободное место на встроенной флэш-памяти
sbcFreeRam	1.3.6.1.4.1.35265.1.49.33	`Get {}`	Количество свободной оперативной памяти
sbcMonitoring	1.3.6.1.4.1.35265.1.49.35	`Get {}`	Отображение датчиков температуры и скорости вращения вентиляторов, корневой объект
sbcTemperature1	1.3.6.1.4.1.35265.1.49.35.1	`Get {}`	Температурный датчик 1
sbcTemperature2	1.3.6.1.4.1.35265.1.49.35.2	`Get {}`	Температурный датчик 2
sbcFan0	1.3.6.1.4.1.35265.1.49.35.3	`Get {}`	Датчик оборотов вентилятора 1
sbcFan1	1.3.6.1.4.1.35265.1.49.35.4	`Get {}`	Датчик оборотов вентилятора 2
sbcFan2	1.3.6.1.4.1.35265.1.49.35.5	`Get {}`	Датчик оборотов вентилятора 3
sbcFan3	1.3.6.1.4.1.35265.1.49.35.6	`Get {}`	Датчик оборотов вентилятора 4

Имя	OID	Запросы	Описание
sbcPowerModuleTable	1.3.6.1.4.1.35265.1.49.36	Get {}	Информация о состоянии блоков питания, корневой объект. Для дочерних объектов указывается номер БП: 1 или 2
sbcPowerModuleEntry	1.3.6.1.4.1.35265.1.49.36.1	Get {}	см. sbcPowerModuleTable
pmExist	1.3.6.1.4.1.35265.1.49.36.1.2.x	Get {}.x	Установлен ли БП 1 — установлен 2 — не установлен
pmPower	1.3.6.1.4.1.35265.1.49.36.1.3.x	Get {}.x	Подаётся ли питание на БП 1 — подаётся 2 — не подаётся
pmType	1.3.6.1.4.1.35265.1.49.36.1.4.x	Get {}.x	Тип установленного БП 1 — PM48/12 2 — PM220/12 3 — PM220/12V 4 — PM150-220/12
sbcCpuLoadTable	1.3.6.1.4.1.35265.1.49.37	Get {}	Загрузка CPU, корневой объект. Показывает процент загрузки процессора по типам задач. Для дочерних объектов указывается номер процессора: sbc1016M — 1 sbc2016 — 1..4
sbcCpuLoadEntry	1.3.6.1.4.1.35265.1.49.37.1	Get {}	см. sbcCpuLoadTable
cpuUsr	1.3.6.1.4.1.35265.1.49.37.1.2.x	Get {}.x	% CPU, приложения пользователя
cpuSys	1.3.6.1.4.1.35265.1.49.37.1.3.x	Get {}.x	% CPU, приложения ядра
cpuNic	1.3.6.1.4.1.35265.1.49.37.1.4.x	Get {}.x	% CPU, приложения с изменённым приоритетом
cpuIdle	1.3.6.1.4.1.35265.1.49.37.1.5.x	Get {}.x	% CPU, нахождение в простое
cpuIo	1.3.6.1.4.1.35265.1.49.37.1.6.x	Get {}.x	% CPU, операции ввода-вывода
cpuIrq	1.3.6.1.4.1.35265.1.49.37.1.7.x	Get {}.x	% CPU, обработка аппаратных прерываний
cpuSirq	1.3.6.1.4.1.35265.1.49.37.1.8.x	Get {}.x	% CPU, обработка программных прерываний
cpuUsage	1.3.6.1.4.1.35265.1.49.37.1.9.x	Get {}.x	% CPU, общее использование
activeCallCount	1.3.6.1.4.1.35265.1.49.42.1	Get {}	Текущее число активных вызовов
registrationCount	1.3.6.1.4.1.35265.1.49.42.2	Get {}	Текущее число регистраций

Таблица Г.3 — Настройки syslog

Имя	OID	Запросы	Описание
sbcSyslog	1.3.6.1.4.1.35265.1.49.34	Get {}	Настройки syslog, корневой объект
sbcSyslogHistory	1.3.6.1.4.1.35265.1.49.34.2	Get {}	Настройки логирования истории команд в syslog, корневой объект
sbcSyslogHistoryAddress	1.3.6.1.4.1.35265.1.49.34.2.1	Get {} Set {} S	IP адрес сервера syslog для приёма истории команд

Имя	OID	Запросы	Описание
sbcSyslogHistoryPort	1.3.6.1.4.1.35265.1.49.34.2.2	Get {} Set {} N	Порт сервера syslog для приёма истории команд
sbcSyslogHistoryLVL	1.3.6.1.4.1.35265.1.49.34.2.3	Get {} Set {} N	Уровень детализации логов 0 — отключить логирование; 1 — стандартный; 2 — полный
sbcSyslogHistoryRowStatus	1.3.6.1.4.1.35265.1.49.34.2.4	Get {} Set {} 1	Применить изменения в логировании истории команд
sbcSyslogConfig	1.3.6.1.4.1.35265.1.49.34.3	Get {}	Настройки системного журнала
sbcSyslogConfigLogsEnabled	1.3.6.1.4.1.35265.1.49.34.3.1	Get {} Set {} N	Включить ведение логов 1 — включить; 2 — отключить
sbcSyslogConfigSendToServer	1.3.6.1.4.1.35265.1.49.34.3.2	Get {} Set {} N	Отправлять сообщения на сервер syslog 1 — включить; 2 — выключить
sbcSyslogConfigAddress	1.3.6.1.4.1.35265.1.49.34.3.3	Get {} Set {} S	IP адрес сервера syslog
sbcSyslogConfigPort	1.3.6.1.4.1.35265.1.49.34.3.4	Get {} Set {} N	Порт сервера syslog
sbcSyslogConfigRowStatus	1.3.6.1.4.1.35265.1.49.34.3.5	Get {} Set {} 1	Применить изменения в настройках системного журнала

Просмотр информации о зарегистрированных пользователях

В описании команды вызова утилит SNMP будут представлены следующими скриптами для краткости и наглядности изложения:

Скрипт **swalk**, реализующий чтение значений:

```
#!/bin/bash
/usr/bin/snmpwalk -v2c -c public -m +ELTEX-SBC 192.0.2.1 "$@"
```

Скрипт **sset**, реализующий установку значений:

```
#!/bin/bash
/usr/bin/snmpset -v2c -c private -m +ELTEX-SBC 192.0.2.1 "$@"
```

Для просмотра требуется сделать следующие шаги:

1) Сбросить статус поиска;
2) Задать критерии поиска (опционально);
3) Отобразить информацию.

Пример поиска абонента по номеру

```
sset sbcSubResetSearch.0 i 1                # сбросить поиск
sset getSbcSubBySubstring.0 s 40012         # задать критерий
swalk tableOfSbcSubscribers                 # отобразить результаты
```

Результат:

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

Таблица Г.4 — Просмотр информации о зарегистрированных пользователях

Имя	OID	Запросы	Описание
sbcSubSearchStatus	1.3.6.1.4.1.35265.1.49.44.1	`Get {}`	Статус поиска по критерию. Without search — поиск не производится; Search by substring — режим поиска по подстроке
sbcSubResetSearch	1.3.6.1.4.1.35265.1.49.44.2	`Set {} N`	Сброс поиска по в состояние without search. Для сброса установить любое числовое значение.
sbcSubCount	1.3.6.1.4.1.35265.1.49.44.3	`Get {}`	Общее число зарегистрированных через SBC абонентов
getSbcSubBySubstring	1.3.6.1.4.1.35265.1.49.44.4	`Get {}` `Set {} S`	Задаёт подстроку для поиска в списке регистраций и переводит поиск в режим "search by substring"
tableOfSbcSubscribers	1.3.6.1.4.1.35265.1.49.44.5	`Get {}`	Спискок зарегистрированных абонентов. В режиме "without search" выводит всех абонентов. В режиме "search by substring" выводит всех абонентов, в описании которых встречается заданная подстрока.
subName	1.3.6.1.4.1.35265.1.49.44.5.1.2	`Get {}`	Имя (SIP URI) абонента
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 адрес и порт, откуда регистрировался абонент
subContacts	1.3.6.1.4.1.35265.1.49.44.5.1.5	`Get {}`	Контактный IP адрес и порт абонента (из заголовка Contact)
subRegAddr	1.3.6.1.4.1.35265.1.49.44.5.1.6	`Get {}`	Адрес регистратора, одобрившего регистрацию
subSipUser	1.3.6.1.4.1.35265.1.49.44.5.1.7	`Get {}`	Наименование SIP Users, с которого зарегистрировался абонент
subSipDest	1.3.6.1.4.1.35265.1.49.44.5.1.8	`Get {}`	Наименование SIP Destination, со стороны которого была одобрена регистрация

Имя	OID	Запросы	Описание
subBloked	1.3.6.1.4.1.35265.1.49.44.5.1.9	`Get {}`	Статус блокировки абонента
subRetries	1.3.6.1.4.1.35265.1.49.44.5.1.10	`Get {}`	Количество неудачных попыток доступа
subExpires	1.3.6.1.4.1.35265.1.49.44.5.1.11	`Get {}`	Время, через которое истечёт регистрация

Просмотр статистики SIP

В описании команды вызова утилит SNMP будут представлены следующими скриптами для краткости и наглядности изложения:

Скрипт **swalk**, реализующий чтение значений:

```
#!/bin/bash
/usr/bin/snmpwalk -v2c -c public -m +ELTEX-SBC 192.0.2.1 "$@"
```

Скрипт **sset**, реализующий установку значений:

```
#!/bin/bash
/usr/bin/snmpset -v2c -c private -m +ELTEX-SBC 192.0.2.1 "$@"
```

Статистика сгруппирована в шесть групп по типам:

1. Накопительные счётчики по SIP Users
2. Мгновенные счётчики по SIP Users
3. Накопительные счётчики по SIP Transport
4. Мгновенные счётчики по SIP Transport
5. Накопительные счётчики по SIP Destination
6. Мгновенные счётчики по SIP Destination

OID счётчика формируется следующим образом:

1.3.6.1.4.1.35265.1.49.43.<TYPE>.1.<COUNTER>.<ID>, где

TYPE — один из шести типов счётчика;

COUNTER — идентификатор счётчика;

ID — идентификатор объекта, на который указывает счётчик.

Узнать идентификатор объекта можно из колонки ID в CLI. Для этого, находясь в режиме редактирования SIP destination, SIP users или SIP transport надо дать команду show info. Второй способ — запросить по SNMP счётчик с COUNTER = 3 без указания ID.

Примеры:

Запрос имён всех SIP Transport, обратите внимание на то, что в ответе следующая цифра после имени, запрошенного OID — идентификатор транспорта, который можно далее использовать в запросах:

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

Запросы по счётчикам:

1.3.6.1.4.1.35265.1.49.43.3.1.9.20

TYPE = 3 — накопительный счётчик по SIP Transport;

COUNTER = 9 — неудачные вызовы, завершённые SIP кодами 4xx;

ID = 20 — счётчик по SIP Transport с идентификатором 20.

ELTEX-SBC::countStatTransportAnswSuccessCalls.20 = Gauge32: 21946

1.3.6.1.4.1.35265.1.49.43.5.1.408.14

TYPE = 3 — накопительный счётчик по SIP Destination;

COUNTER = 408 — неудачные вызовы, завершённые SIP кодом 408;

ID = 14 — счётчик по SIP Destination с идентификатором 14.

ELTEX-SBC::countStatDestUnansw408.14 = Gauge32: 33

Таблица Г.5 — Просмотр статистики SIP

Имя	OID	Запросы	Описание
sbcCallStatistics	1.3.6.1.4.1.35265.1.49.43	Get {}	Таблица со всеми счётчиками SIP
tableOfCallCountStatUsers	1.3.6.1.4.1.35265.1.49.43.1	Get {}	Таблица со всеми накопительными счётчиками SIP Users
countStatUserIndex	1.3.6.1.4.1.35265.1.49.43.1.1.2	Get {}	Индексы SIP Users
countStatUserName	1.3.6.1.4.1.35265.1.49.43.1.1.3	Get {}	Названия SIP Users
countStatUserElapsedTime	1.3.6.1.4.1.35265.1.49.43.1.1.4	Get {}	Общее время активных разговоров
countStatUserIncCalls	1.3.6.1.4.1.35265.1.49.43.1.1.5	Get {}	Число входящих вызовов
countStatUserOutCallLegs	1.3.6.1.4.1.35265.1.49.43.1.1.6	Get {}	Число исходящих вызовов
countStatUserMsgRcv	1.3.6.1.4.1.35265.1.49.43.1.1.7	Get {}	Число входящих SIP-сообщений
countStatUserMsgSend	1.3.6.1.4.1.35265.1.49.43.1.1.8	Get {}	Число исходящих SIP-сообщений
countStatUserAnswSuccess Calls	1.3.6.1.4.1.35265.1.49.43.1.1.9	Get {}	Число успешно принятых вызовов
countStatUserAnswFinalErr Calls	1.3.6.1.4.1.35265.1.49.43.1.1.10	Get {}	Число отклюнённых вызовов

Имя	OID	Запросы	Описание
countStatUserUnanswOther4xx	1.3.6.1.4.1.35265.1.49.43.1.1.11	Get {}	Число неотвеченных вызовов с SIP кодами 4xx
countStatUserUnanswOther5xx	1.3.6.1.4.1.35265.1.49.43.1.1.12	Get {}	Число неотвеченных вызовов с SIP кодами 5xx
countStatUserUnanswOther6xx	1.3.6.1.4.1.35265.1.49.43.1.1.13	Get {}	Число неотвеченных вызовов с SIP кодами 6xx
countStatUserUnanswOtherUndef	1.3.6.1.4.1.35265.1.49.43.1.1.14	Get {}	Число неотвеченных вызовов с SIP кодами, не попавшими в другие счётчики.
countStatUserRedirectCalls<CODE> где CODE — одно из значений: 300, 301, 302, 305, 308	1.3.6.1.4.1.35265.1.49.43.1.1.300 ... 1.3.6.1.4.1.35265.1.49.43.1.1.308	Get {}	Индивидуальные счётчики по кодам — число переадресованных вызовов (завершены SIP кодами 3xx)
countStatUserUnansw<CODE> где CODE — одно из значений: 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 ... 1.3.6.1.4.1.35265.1.49.43.1.1.606	Get {}	Индивидуальные счётчики по кодам — число переадресованных вызовов (завершены SIP кодами 4xx-6xx)
tableOfCallPerSecStatUsers	1.3.6.1.4.1.35265.1.49.43.2	Get {}	Таблица со всеми мгновенными счётчиками SIP Users
perSecStatUserIndex	1.3.6.1.4.1.35265.1.49.43.2.1.2	Get {}	Индексы SIP Users
perSecStatUserName	1.3.6.1.4.1.35265.1.49.43.2.1.3	Get {}	Названия SIP Users
perSecStatUserElapsedTime	1.3.6.1.4.1.35265.1.49.43.2.1.4	Get {}	Общее время активных разговоров
perSecStatUserIncCalls	1.3.6.1.4.1.35265.1.49.43.2.1.5	Get {}	Число входящих вызовов
perSecStatUserOutCallLegs	1.3.6.1.4.1.35265.1.49.43.2.1.6	Get {}	Число исходящих вызовов
perSecStatUserMsgRcv	1.3.6.1.4.1.35265.1.49.43.2.1.7	Get {}	Число входящих SIP-сообщений
perSecStatUserMsgSend	1.3.6.1.4.1.35265.1.49.43.2.1.8	Get {}	Число исходящих SIP-сообщений
perSecStatUserAnswSuccessCalls	1.3.6.1.4.1.35265.1.49.43.2.1.9	Get {}	Число успешно принятых вызовов
perSecStatUserAnswFinalErrCalls	1.3.6.1.4.1.35265.1.49.43.2.1.10	Get {}	Число отклюнённых вызовов
perSecStatUserUnanswOther4xx	1.3.6.1.4.1.35265.1.49.43.2.1.11	Get {}	Число неотвеченных вызовов с SIP кодами 4xx
perSecStatUserUnanswOther5xx	1.3.6.1.4.1.35265.1.49.43.2.1.12	Get {}	Число неотвеченных вызовов с SIP кодами 5xx
perSecStatUserUnanswOther6xx	1.3.6.1.4.1.35265.1.49.43.2.1.13	Get {}	Число неотвеченных вызовов с SIP кодами 6xx

Имя	OID	Запросы	Описание
perSecStatUserUnanswOtherUndef	1.3.6.1.4.1.35265.1.49.43.2.1.14	Get {}	Число неотвеченных вызовов с SIP кодами, не попавшими в другие счётчики.
perSecStatUserRedirectCalls<CODE> где CODE — одно из значений: 300, 301, 302, 305, 308	1.3.6.1.4.1.35265.1.49.43.2.1.300 ... 1.3.6.1.4.1.35265.1.49.43.2.1.308	Get {}	Индивидуальные счётчики по кодам — число переадресованных вызовов (завершены SIP кодами 3xx)
perSecStatUserUnansw<CODE> где CODE — одно из значений: 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	1.3.6.1.4.1.35265.1.49.43.2.1.400 ... 1.3.6.1.4.1.35265.1.49.43.2.1.606	Get {}	Индивидуальные счётчики по кодам — число переадресованных вызовов (завершены SIP кодами 4xx-6xx)
tableOfCallCountStatTransport	1.3.6.1.4.1.35265.1.49.43.3	Get {}	Таблица со всеми накопительными счётчиками SIP Transport
countStatTransportIndex	1.3.6.1.4.1.35265.1.49.43.3.1.2	Get {}	Индексы SIP Transport
countStatTransportName	1.3.6.1.4.1.35265.1.49.43.3.1.3	Get {}	Названия SIP Transport
countStatTransportElapsedTime	1.3.6.1.4.1.35265.1.49.43.3.1.4	Get {}	Общее время активных разговоров
countStatTransportIncCalls	1.3.6.1.4.1.35265.1.49.43.3.1.5	Get {}	Число входящих вызовов
countStatTransportOutCallLegs	1.3.6.1.4.1.35265.1.49.43.3.1.6	Get {}	Число исходящих вызовов
countStatTransportMsgRcv	1.3.6.1.4.1.35265.1.49.43.3.1.7	Get {}	Число входящих SIP-сообщений
countStatTransportMsgSend	1.3.6.1.4.1.35265.1.49.43.3.1.8	Get {}	Число исходящих SIP-сообщений
countStatTransportAnswSuccessCalls	1.3.6.1.4.1.35265.1.49.43.3.1.9	Get {}	Число успешно принятых вызовов
countStatTransportAnswFinalErrCalls	1.3.6.1.4.1.35265.1.49.43.3.1.10	Get {}	Число отклюнённых вызовов
countStatTransportUnanswOther4xx	1.3.6.1.4.1.35265.1.49.43.3.1.11	Get {}	Число неотвеченных вызовов с SIP кодами 4xx
countStatTransportUnanswOther5xx	1.3.6.1.4.1.35265.1.49.43.3.1.12	Get {}	Число неотвеченных вызовов с SIP кодами 5xx
countStatTransportUnanswOther6xx	1.3.6.1.4.1.35265.1.49.43.3.1.13	Get {}	Число неотвеченных вызовов с SIP кодами 6xx
countStatTransportUnanswOtherUndef	1.3.6.1.4.1.35265.1.49.43.3.1.14	Get {}	Число неотвеченных вызовов с SIP кодами, не попавшими в другие счётчики.
countStatTransportRedirectCalls<CODE>	1.3.6.1.4.1.35265.1.49.43.3.1.300 ... 1.3.6.1.4.1.35265.1.49.43.3.1.308	Get {}	Индивидуальные счётчики по кодам — число переадресованных

Имя	OID	Запросы	Описание
где CODE — одно из значений: 300, 301, 302, 305, 308			вызовов (завершены SIP кодами 3xx)
countStatTransportUnansw<CODE> где CODE — одно из значений: 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	1.3.6.1.4.1.35265.1.49.43.3.1.400 ... 1.3.6.1.4.1.35265.1.49.43.3.1.606	Get {}	Индивидуальные счётчики по кодам — число переадресованных вызовов (завершены SIP кодами 4xx-6xx)
tableOfCallPerSecStatTransport	1.3.6.1.4.1.35265.1.49.43.4	Get {}	Таблица со всеми мгновенными счётчиками SIP Transport
perSecStatTransportIndex	1.3.6.1.4.1.35265.1.49.43.4.1.2	Get {}	Индексы SIP Transport
perSecStatTransportName	1.3.6.1.4.1.35265.1.49.43.4.1.3	Get {}	Названия SIP Transport
perSecStatTransportElapsedTime	1.3.6.1.4.1.35265.1.49.43.4.1.4	Get {}	Общее время активных разговоров
perSecStatTransportIncCalls	1.3.6.1.4.1.35265.1.49.43.4.1.5	Get {}	Число входящих вызовов
perSecStatTransportOutCallLegs	1.3.6.1.4.1.35265.1.49.43.4.1.6	Get {}	Число исходящих вызовов
perSecStatTransportMsgRcv	1.3.6.1.4.1.35265.1.49.43.4.1.7	Get {}	Число входящих SIP-сообщений
perSecStatTransportMsgSend	1.3.6.1.4.1.35265.1.49.43.4.1.8	Get {}	Число исходящих SIP-сообщений
perSecStatTransportAnswSuccessCalls	1.3.6.1.4.1.35265.1.49.43.4.1.9	Get {}	Число успешно принятых вызовов
perSecStatTransportAnswFinalErrCalls	1.3.6.1.4.1.35265.1.49.43.4.1.10	Get {}	Число отклюнённых вызовов
perSecStatTransportUnanswOther4xx	1.3.6.1.4.1.35265.1.49.43.4.1.11	Get {}	Число неотвеченных вызовов с SIP кодами 4xx
perSecStatTransportUnanswOther5xx	1.3.6.1.4.1.35265.1.49.43.4.1.12	Get {}	Число неотвеченных вызовов с SIP кодами 5xx
perSecStatTransportUnanswOther6xx	1.3.6.1.4.1.35265.1.49.43.4.1.13	Get {}	Число неотвеченных вызовов с SIP кодами 6xx
perSecStatTransportUnanswOtherUndef	1.3.6.1.4.1.35265.1.49.43.4.1.14	Get {}	Число неотвеченных вызовов с SIP кодами, не попавшими в другие счётчики.
perSecStatTransportRedirectCalls<CODE> где CODE — одно из значений: 300, 301, 302, 305, 308	1.3.6.1.4.1.35265.1.49.43.4.1.300 ... 1.3.6.1.4.1.35265.1.49.43.4.1.308	Get {}	Индивидуальные счётчики по кодам — число переадресованных вызовов (завершены SIP кодами 3xx)

Имя	OID	Запросы	Описание
perSecStatTransportUnansw<CODE> где CODE — одно из значений: 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 ... 1.3.6.1.4.1.35265.1.49.43.4.1.606	Get {}	Индивидуальные счётчики по кодам — число переадресованных вызовов (завершены SIP кодами 4xx-6xx)
tableOfCallCountStatDest	1.3.6.1.4.1.35265.1.49.43.5	Get {}	Таблица со всеми накопительными счётчиками SIP Destination
countStatDestIndex	1.3.6.1.4.1.35265.1.49.43.5.1.2	Get {}	Индексы SIP Destination
countStatDestName	1.3.6.1.4.1.35265.1.49.43.5.1.3	Get {}	Названия SIP Destination
countStatDestElapsedTime	1.3.6.1.4.1.35265.1.49.43.5.1.4	Get {}	Общее время активных разговоров
countStatDestIncCalls	1.3.6.1.4.1.35265.1.49.43.5.1.5	Get {}	Число входящих вызовов
countStatDestOutCallLegs	1.3.6.1.4.1.35265.1.49.43.5.1.6	Get {}	Число исходящих вызовов
countStatDestMsgRcv	1.3.6.1.4.1.35265.1.49.43.5.1.7	Get {}	Число входящих SIP-сообщений
countStatDestMsgSend	1.3.6.1.4.1.35265.1.49.43.5.1.8	Get {}	Число исходящих SIP-сообщений
countStatDestAnswSuccessCalls	1.3.6.1.4.1.35265.1.49.43.5.1.9	Get {}	Число успешно принятых вызовов
countStatDestAnswFinalErrCalls	1.3.6.1.4.1.35265.1.49.43.5.1.10	Get {}	Число отклюнённых вызовов
countStatDestUnanswOther4xx	1.3.6.1.4.1.35265.1.49.43.5.1.11	Get {}	Число неотвеченных вызовов с SIP кодами 4xx
countStatDestUnanswOther5xx	1.3.6.1.4.1.35265.1.49.43.5.1.12	Get {}	Число неотвеченных вызовов с SIP кодами 5xx
countStatDestUnanswOther6xx	1.3.6.1.4.1.35265.1.49.43.5.1.13	Get {}	Число неотвеченных вызовов с SIP кодами 6xx
countStatDestUnanswOtherUndef	1.3.6.1.4.1.35265.1.49.43.5.1.14	Get {}	Число неотвеченных вызовов с SIP кодами, не попавшими в другие счётчики.
countStatDestRedirectCalls<CODE> где CODE — одно из значений: 300, 301, 302, 305, 308	1.3.6.1.4.1.35265.1.49.43.5.1.300 ... 1.3.6.1.4.1.35265.1.49.43.5.1.308	Get {}	Индивидуальные счётчики по кодам — число переадресованных вызовов (завершены SIP кодами 3xx)
countStatDestUnansw<CODE> где CODE — одно из значений: 400, 401, 402, 403, 404, 405, 406, 407, 408, 410, 413, 414, 415, 416, 420, 421, 422, 423, 480, 481,	1.3.6.1.4.1.35265.1.49.43.5.1.400 ... 1.3.6.1.4.1.35265.1.49.43.5.1.606	Get {}	Индивидуальные счётчики по кодам — число переадресованных вызовов (завершены SIP кодами 4xx-6xx)

Имя	OID	Запросы	Описание
482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 493, 500, 501, 502, 503, 504, 505, 513, 580, 600, 603, 604, 606			
tableOfCallPerSecStatDest	1.3.6.1.4.1.35265.1.49.43.6	Get {}	Таблица со всеми мгновенными счётчиками SIP Destination
perSecStatDestIndex	1.3.6.1.4.1.35265.1.49.43.6.1.2	Get {}	Индексы SIP Destination
perSecStatDestName	1.3.6.1.4.1.35265.1.49.43.6.1.3	Get {}	Названия SIP Destination
perSecStatDestElapsedTime	1.3.6.1.4.1.35265.1.49.43.6.1.4	Get {}	Общее время активных разговоров
perSecStatDestIncCalls	1.3.6.1.4.1.35265.1.49.43.6.1.5	Get {}	Число входящих вызовов
perSecStatDestOutCallLegs	1.3.6.1.4.1.35265.1.49.43.6.1.6	Get {}	Число исходящих вызовов
perSecStatDestMsgRcv	1.3.6.1.4.1.35265.1.49.43.6.1.7	Get {}	Число входящих SIP-сообщений
perSecStatDestMsgSend	1.3.6.1.4.1.35265.1.49.43.6.1.8	Get {}	Число исходящих SIP-сообщений
perSecStatDestAnswSuccessCalls	1.3.6.1.4.1.35265.1.49.43.6.1.9	Get {}	Число успешно принятых вызовов
perSecStatDestAnswFinalErrCalls	1.3.6.1.4.1.35265.1.49.43.6.1.10	Get {}	Число отклюнённых вызовов
perSecStatDestUnanswOther4xx	1.3.6.1.4.1.35265.1.49.43.6.1.11	Get {}	Число неотвеченных вызовов с SIP кодами 4xx
perSecStatDestUnanswOther5xx	1.3.6.1.4.1.35265.1.49.43.6.1.12	Get {}	Число неотвеченных вызовов с SIP кодами 5xx
perSecStatDestUnanswOther6xx	1.3.6.1.4.1.35265.1.49.43.6.1.13	Get {}	Число неотвеченных вызовов с SIP кодами 6xx
perSecStatDestUnanswOtherUndef	1.3.6.1.4.1.35265.1.49.43.6.1.14	Get {}	Число неотвеченных вызовов с SIP кодами, не попавшими в другие счётчики.
perSecStatDestRedirectCalls<CODE> где CODE — одно из значений: 300, 301, 302, 305, 308	1.3.6.1.4.1.35265.1.49.43.6.1.300 ... 1.3.6.1.4.1.35265.1.49.43.6.1.308	Get {}	Индивидуальные счётчики по кодам — число переадресованных вызовов (завершены SIP кодами 3xx)
perSecStatDestUnansw<CODE> где CODE — одно из значений: 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 ... 1.3.6.1.4.1.35265.1.49.43.6.1.606	Get {}	Индивидуальные счётчики по кодам — число переадресованных вызовов (завершены SIP кодами 4xx-6xx)

Устаревшие OID

Некоторые OID были изменены и в последующих релизах старые ветки могут быть удалены или заменены новыми назначениям. Рекомендуется перенастроить системы мониторинга и скрипты на использование новых OID.

Таблица Г.6 — Устаревшие OID

Имя	OID	Запросы	Описание
sbcCpuLoad	1.3.6.1.4.1.35265.1.49.17	`Get {}`	Заменён на 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`	Заменён на 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`	Заменён на 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`	Заменён на 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`	Заменён на 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`	Заменён на 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`	Заменён на 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`	Заменён на 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`	Заменён на cpuUsage (1.3.6.1.4.1.35265.1.49.37.1.9.x)

Поддержка OID MIB-2 (1.3.6.1.2.1)

SMG поддерживает следующие ветки MIB-2:

- system (1.3.6.1.2.1.1) — общая информация о системе;
- interfaces (1.3.6.1.2.1.2) — информация о сетевых интерфейсах;
- snmp (1.3.6.1.2.1.11) — информация о работе SNMP.

ПРИЛОЖЕНИЕ Д. ОГРАНИЧЕНИЕ РЕСУРСОВ SBC

Параметр	SBC-3000	SBC-2000	SBC-1000	Примечание
Групп LACP	4	4	5	
Записей в таблице 802.1q	NA	NA	1024	
Статических маршрутов в таблице маршрутизации (свитч)	255	255	255	
Сетевых интерфейсов	40	40	40	Для SBC2000 и SBC3000 возможно расширение до 500 при наличии лицензии 500VNI
SIP-транспортов	256	256	256	Для SBC2000 и SBC3000 возможно расширение до 500 при наличии лицензии 500VNI
SIP Destination	256	256	256	Для SBC2000 и SBC3000 возможно расширение до 500 наличии лицензии 500VNI
SIP Users	256	256	256	Для SBC2000 и SBC3000 возможно расширение до 500 наличии лицензии 500VNI
SBC Trunk	256	256	256	Для SBC2000 и SBC3000 возможно расширение до 500 наличии лицензии 500VNI
Rule set	1000	1000	512	
Правил для каждого Rule set в отдельности	1500	1500	1000	нет ограничения на каждый профиль, есть только общее ограничение

Правил Rule set для устройства	1500	1500	1000	
Портов для RTP	диапазон для начального порта: 10000-65535 кол-во портов: 1-32000	диапазон для начального порта: 10000-65535 кол-во портов: 1-32000	диапазон для начального порта: 10000-65535 кол-во портов: 1-32000	
SNMP trap	16	16	16	
Адресов клиентов для VPN/PPTP сервера	5	5	5	SBC выступает в роли клиента - VPN/pptp client
Адресов клиентов для L2TP сервера	-	-	-	SBC не может выступать как L2TP-client, только как сервер
Пользователей VPN/PPTP/L2TP	255	255	255	
Пользователей WEB-интефейса (вкладка Безопасность/Управление)	10	10	10	
Записей в белом списке Fail2ban	ND	ND	ND	
Записей в черном списке Fail2ban	16384	16384	8192	
Записей в списке заблокированных Fail2ban	16384	16384	8192	
Записей в Журнале заблокированных адресов	10000	10000	10000	
Профилей Firewall	32	32	32	
Правил для веток входящего/исходящего/транзитного трафика, в профиле и всего для устройства	1000	1000	1000	

Записей в списке разрешенных IP-адресов (доступ к управлению с определенных адресов)	255	255	255	
Профилей RADIUS	32	32	32	

NA — not applicable;

ND — not defined.

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Для получения технической консультации по вопросам эксплуатации оборудования ООО «Предприятие «ЭЛТЕКС» Вы можете обратиться в Сервисный центр компании:

Форма обратной связи на сайте: **http://eltex-co.ru/support/**
Servicedesk: **https://servicedesk.eltex-co.ru**

На официальном сайте компании Вы можете найти техническую документацию и программное обеспечение для продукции ООО «Предприятие «ЭЛТЕКС», обратиться к базе знаний, оставить интерактивную заявку или проконсультироваться у инженеров Сервисного центра на техническом форуме.

Официальный сайт компании: **http://eltex-co.ru/**
Технический форум: **http://eltex-co.ru/forum**
База знаний: **https://docs.eltex-co.ru/display/EKB/Eltex+Knowledge+Base**
Центр загрузок: **http://eltex-co.ru/support/downloads**