



Комплексные решения для построения сетей

Eltex SBC-1000

Руководство по эксплуатации, версия 1.1 (17.04.2013)

Пограничный контроллер сессий

Версия ПО: 1.3.120		
Версия документа	Дата выпуска	Содержание изменений
Версия 1.1	17.04.2013	Добавлено: <ul style="list-style-type: none">– настройки RADIUS-Authorization;– настройки RADIUS-профилей;– настройка SIP-транков;– настройка профилей Firewall;– настройки Fail2ban
Версия 1.0	09.01.2013	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	6
2 Описание изделия	6
2.1 Назначение.....	6
2.2 Типовые схемы применения	7
2.2.1 Межоператорское взаимодействие	7
2.2.2 Взаимодействие между оператором и корпоративным клиентом	7
2.2.3 Взаимодействие между оператором и частным пользователем	8
2.3 Основные технические параметры.....	8
2.4 Конструктивное исполнение	10
2.5 Световая индикация	11
2.6 Использование функциональной кнопки F	13
2.7 Сохранение заводской конфигурации	13
2.8 Восстановление пароля	14
2.9 Комплект поставки	14
2.10 Инструкции по технике безопасности	15
2.10.1 Общие указания.....	15
2.10.2 Требования электробезопасности	15
2.11 Установка SBC-1000	16
2.11.1 Порядок включения.....	16
2.11.2 Крепление кронштейнов	16
2.11.3 Установка устройства в стойку.....	17
2.11.4 Установка модулей питания	17
2.11.5 Вскрытие корпуса	18
2.11.6 Установка submodule	19
2.11.7 Установка блоков вентиляции.....	19
3 ОБЩИЕ РЕКОМЕНДАЦИИ ПРИ РАБОТЕ С УСТРОЙСТВОМ	21
4 КОНФИГУРИРОВАНИЕ УСТРОЙСТВА.....	22
4.1 Настройка SBC-1000 через web-интерфейс	22
4.1.1 CDR-записи	24
4.1.1.1 Формат CDR-записи	26
4.1.1.2 Пример CDR файла	26
4.1.2 Мониторинг.....	27
4.1.2.1 Мониторинг загруженности процессора.....	27
4.1.2.2 Мониторинг SFP модулей	27
4.1.2.3 Журнал аварийных событий.....	28
4.1.3 Коммутатор	29
4.1.3.1 Настройки LACP.....	29
4.1.3.2 Настройка портов коммутатора	30
4.1.3.3 802.1q.....	32
4.1.3.4 QoS и контроль полосы пропускания	33
4.1.3.5 Распределение приоритетов	34
4.1.4 Конфигурация интерфейсов	35
4.1.4.1 Таблица маршрутизации	35
4.1.4.2 Простые интерфейсы.....	36
4.1.4.3 VLAN интерфейсы	37
4.1.4.4 VPN/pptr интерфейсы.....	37
4.1.4.5 Общие настройки сети	38
4.1.5 Конфигурация SBC	39
4.1.5.1 Media.....	40
4.1.5.2 SIP	40
4.1.5.3 SIP Trunk.....	42
4.1.5.4 Список абонентов	43
4.1.6 Сетевые сервисы.....	43

4.1.6.1 NTP	43
4.1.6.3 SNMPv3 и SNMP	44
4.1.6.4 VPN/PPTP сервер	45
4.1.7 Безопасность.....	46
4.1.7.1 Управление	46
4.1.7.2 Настройка SSL/TLS.....	46
4.1.7.3 Fail2ban	46
4.1.7.4 Профили firewall	47
4.1.8 Сетевые утилиты.....	50
4.1.8.1 PING.....	50
4.1.8.2 MTR	51
4.1.9 Настройка RADIUS.....	52
4.1.9.1 Сервера RADIUS	52
4.1.9.2 Список профилей.....	53
4.1.10 Настройка трассировки.....	54
4.1.10.1 PCAP трассировки	54
4.1.10.2 Настройки syslog	56
4.1.11 Работа с объектами и меню «Объекты»	57
4.1.12 Сохранение конфигурации и меню «Сервис»	57
4.1.13 Настройка даты и времени.....	58
4.1.14 Обновление ПО через web-интерфейс.....	58
4.1.15 Лицензии.....	58
4.1.16 Меню «Помощь»	59
4.1.17 Установка пароля для доступа через WEB конфигуратор.....	59
4.1.18 Просмотр заводских параметров и информации о системе	59
4.1.19 Выход из конфигуратора.....	60
4.2 Настройка SBC-1000 через Telnet, SSH или RS-232.....	60
4.2.1 Смена пароля для доступа к устройству.....	61
ПРИЛОЖЕНИЕ А. РЕЗЕРВНОЕ ОБНОВЛЕНИЕ ВСТРОЕННОГО ПО УСТРОЙСТВА	62
ПРИЛОЖЕНИЕ Б. НАСТРОЙКА БРАНДМАУЭРА (IPTABLES) НА УСТРОЙСТВЕ.....	64
ПРИЛОЖЕНИЕ В. ПРИМЕРЫ НАСТРОЙКИ SBC-1000.....	65

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-1000 – 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-1000:

- количество одновременных сессий: 350¹;
- количество вызовов/секунду (CPS): 50;
- количество Ethernet-портов:
 - 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 регистрации до 2000 SIP-абонентов;
- поддержка NTP;
- поддержка DNS;
- поддержка SNMP;
- ограничение полосы и QoS;
- ToS и CoS для RTP и сигнализации²;
- VLAN для RTP, сигнализации и управления;
- аварийное логирование;
- запись биллинговой информации;
- внешний вход синхронизации;
- обновление ПО: через WEB-интерфейс, CLI (Telnet, SSH, консоль (RS-232));
- конфигурирование и настройка (в том числе удаленно):
 - WEB - интерфейс;
 - CLI²(Telnet, консоль (RS-232));
- удаленный мониторинг:
 - WEB - интерфейс;
 - SNMP.

¹ Для версий ПО 1.2.x

² В текущей версии ПО не поддерживается

Функционал SIP/SIP-T/SIP-I:

- SIP L5 NAT/Topology hiding;
- SIP dialogue transparency;
- SIP RFC-3326 Reason with Cause;
- 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);
- SIP RFC-2833 relay;
- 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).

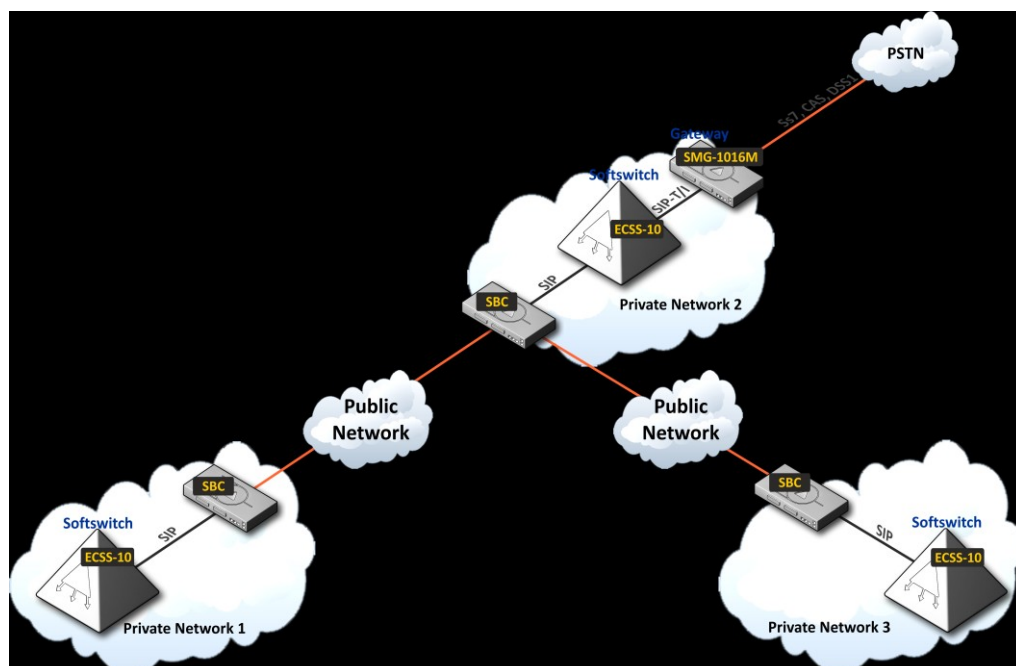
Передача факса

- T.38;
- G.711.

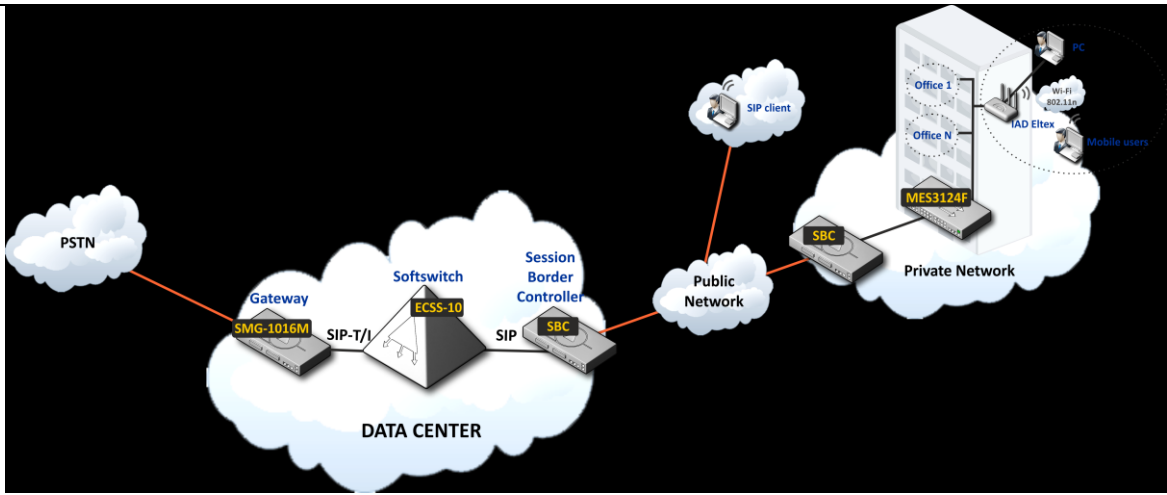
2.2 Типовые схемы применения

В данном руководстве предлагается несколько схем построения сети с использованием SBC-1000.

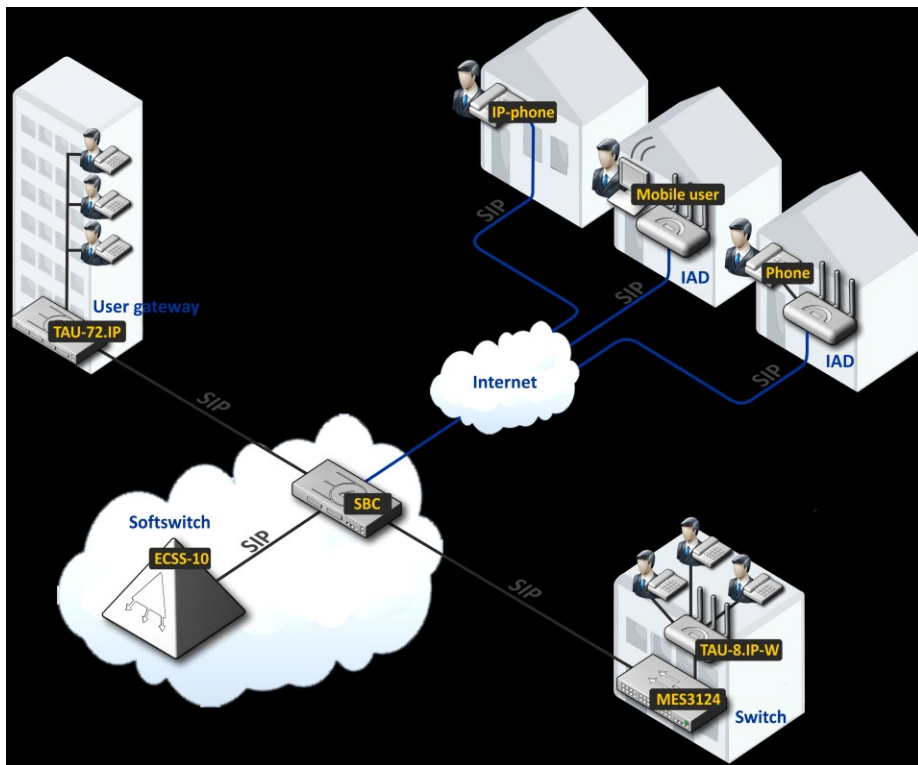
2.2.1 Межоператорское взаимодействие



2.2.2 Взаимодействие между оператором и корпоративным клиентом



2.2.3 Взаимодействие между оператором и частным пользователем



2.3 Основные технические параметры

Основные технические параметры приведены в таблице 1.1.

Таблица 1.1. – Основные технические параметры
Протоколы VoIP

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

Поддерживаемые кодеки

Аудиокодеки	G.711 (A/U) G.729 AB 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	3
Электрический разъем	RJ-45
Скорость передачи, Мбит/с	Автоопределение, 10/100/1000Мбит/с, дуплекс
Поддержка стандартов	10/100/1000BaseT

Параметры оптического интерфейса Ethernet

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

Параметры консоли

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

Прочие интерфейсы

Интерфейс	Количество
USB	1
e-SATA	2

Общие параметры

Напряжение питания	Сеть переменного тока: 220В+-20%, 50 Гц Сеть постоянного тока: -48В+30-20% Варианты питания: - один источник питания постоянного или переменного тока; - два источника питания постоянного или переменного тока, с возможностью горячей замены.
Потребляемая мощность	не более 50Вт
Габариты (ширина, высота, глубина)	420x45x240 мм 19" конструктив, типоразмер 1U
Вес нетто	3,2 кг

2.4 Конструктивное исполнение

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 6.

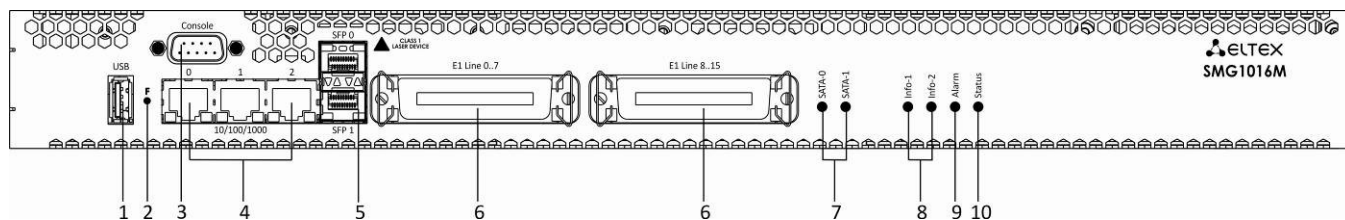


Рисунок 6 – Внешний вид передней панели SBC-1000 (на базе SMG-1016M)

На передней панели устройства расположены следующие разъемы, световые индикаторы и органы управления, таблица 2.1.

Таблица 2.1 – 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

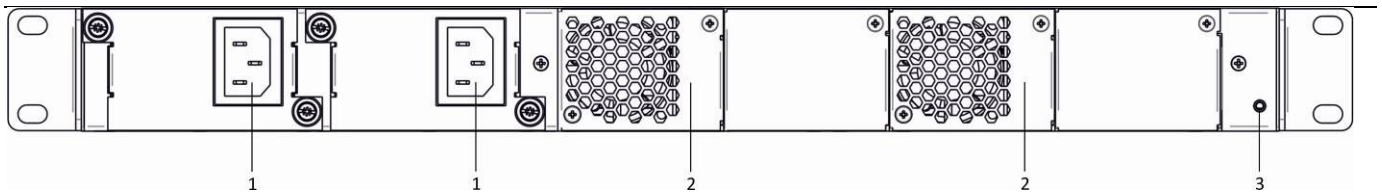



Рисунок 7 – Внешний вид задней панели SBC-1000

В таблице 2.2 приведен перечень разъемов, расположенных на задней панели устройства.

Таблица 2.2 – 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.

2.5 Световая индикация

Текущее состояние устройства отображается при помощи индикаторов *Info1*, *Info2*, *Alarm*, *Status* – расположенных на передней панели.

Перечень состояний индикаторов приведен в таблицах 3.1, 3.2.

Таблица 3.1 – Световая индикация состояния устройства в рабочем состоянии

Индикатор	Состояние индикатора	Состояние устройства
Info1	не горит	отсутствует линк SFPO
	горит зеленым светом	линк SFPO 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

Таблица 3.2 – Световая индикация при загрузке и сбросе к заводским настройкам

№	Индикация				Порядок сброса к заводским настройкам (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	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).
4	желтый	желтый	желтый	желтый	При появлении комбинации отпустить кнопку F. Через некоторое время в консоль будет выведено сообщение: <pre><<<BOOTING IN SAFE-MODE.RESTORING DEFAULT PARAMETERS>>></pre> Сброс к заводским настройкам завершен.



Не рекомендуется удерживать нажатой кнопку F во время сброса настроек устройства (после загорания светодиодов в комбинации 4) - это приведет к полному останову 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.

Состояние интерфейсов Ethernet отображается светодиодными индикаторами, встроенными в разъем 1000/100.

Таблица 3.3 – 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

В таблице 3.4 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 МВ. При заполнении памяти в определенных границах будет индицироваться авария.

Таблица 3.4 –Индикация аварий

Состояние индикатора Alarm	Уровень аварии	Описание аварии
мигает красным светом	критическая(critical)	ошибка конфигурации
		потеря SIP-модуля
		FTP-сервер недоступен, оперативная память для хранения CDR-файлов заполнена свыше 50% (15 - 30 MB)

горит красным светом	не критическая(errors)	потеря VoIP-субмодуля (MSP)
		FTP-сервер недоступен, оперативная память для хранения CDR-файлов заполнена до 50 % (5 - 15 MB)
горит желтым светом	предупреждения (warning)	FTP-сервер недоступен, оперативная память для хранения CDR-файлов заполнена до 5 MB

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 Таблице 3.2.

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: подключитесь через Telnet/SSH либо console, используя логин **admin**, пароль **rootpasswd**, введите команду **save**, перезагрузите устройство командой **reboot**. Шлюз загрузится с заводской конфигурацией.

```
*****
*   SBC v2 Signalling & Media gateway   *
*****

smg login: admin
Password: rootpasswd

*****
*           Welcome to <<SBC>>           *
*****

Welcome! It is Fri Jul  2 12:57:56 UTC 2010
# save
save config
flat0: read block '/dev/mtdblock5'
flat1: read block '/dev/mtdblock5'
flat0: magic [e4e91c09]. flag [1]
flat1: magic [e4e91c09]. flag [0]
magic: FLAT_MAGIC [e4e91c09]
tar: removing leading '/' from member names
recompressed 8916 bytes to device 1
# reboot
```

2.8 Восстановление пароля

Для восстановления пароля: подключитесь через telnet, SSH либо console, 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.

```
*****
* <<SBC>>v2 Signalling & Media gateway *
*****

smg login: admin
Password: rootpasswd

*****
* Welcome to <<SBC>> *
*****

Welcome! It is Fri Jul 2 12:57:56 UTC 2010
# restore
restore saved config
flat0: read block '/dev/mtdblock5'
flat1: read block '/dev/mtdblock5'
flat0: magic [e4e91c09]. flag [1]
flat1: magic [e4e91c09]. flag [0]
magic: FLAT_MAGIC [e4e91c09]
uncompressed 8884 bytes from device 0
restore ret: 0
# passwd admin
Changing password for admin
New password: 1q2w3e4r5t6y
Retype password: 1q2w3e4r5t6y
passwd: password for admin is changed
# save
save config
flat0: read block '/dev/mtdblock5'
flat1: read block '/dev/mtdblock5'
flat0: magic [e4e91c09]. flag [1]
flat1: magic [e4e91c09]. flag [0]
magic: FLAT_MAGIC [e4e91c09]
tar: removing leading '/' from member names
recompressed 8916 bytes to device 1
# reboot
```

2.9 Комплект поставки

В базовый комплект поставки устройства SBC входят:

- Цифровой шлюз SBC;
- Кабель соединительный RS-232 DB9(F) – DB9(F);
- Комплект крепления в 19" стойку;
- Кронштейн – 2шт;
- Руководство по эксплуатации;

При наличии в заказе также могут быть поставлены:

- Mini-Gbic (SFP) – 2 шт.

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.

Цифровой шлюз SBC-1000 предназначен 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 $6,0 \times 10^4$ до $10,7 \times 10^4$ Па (от 450 до 800 мм рт.ст.).

Не подвергать устройство воздействию механических ударов и колебаний, а так же 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.

Установка и удаление submodule должна осуществляться только при выключенном питании, следуя указанием раздела 2.11.4.

2.11 Установка SBC-1000

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, рисунок 7.

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 мм².
3. Если предполагается подключение компьютера к консольному порту SBC, соединить консольный порт SBC с СОМ-портом ПК, при этом ПК должен быть выключен и заземлен в одной точке с цифровым шлюзом.
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.

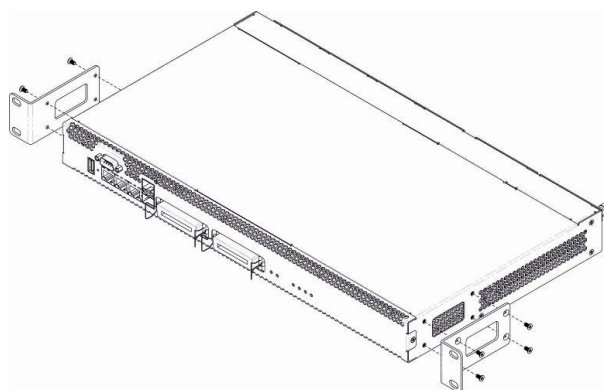


Рисунок 8 – Крепление кронштейнов

Для установки кронштейнов:

1. Совместите четыре отверстия для винтов на кронштейне с такими же отверстиями на боковой панели устройства, рисунок 9.
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

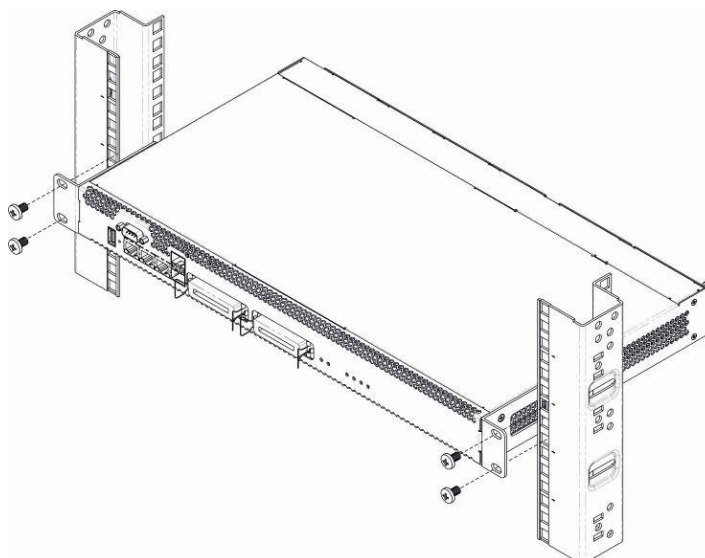


Рисунок 9 – Установка устройства в стойку

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.

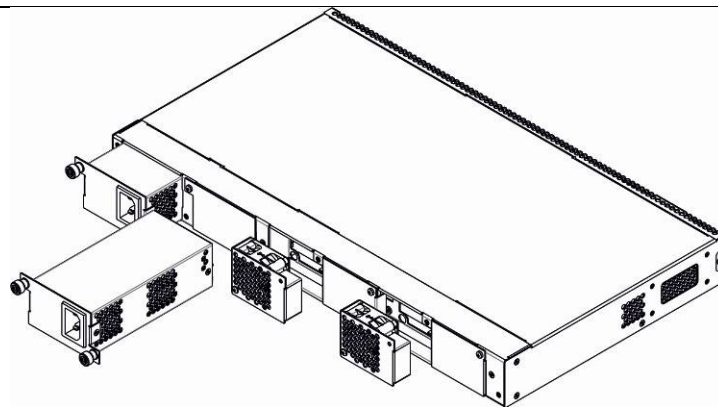


Рисунок 10 – Установка модулей питания

2.11.5 Вскрытие корпуса

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

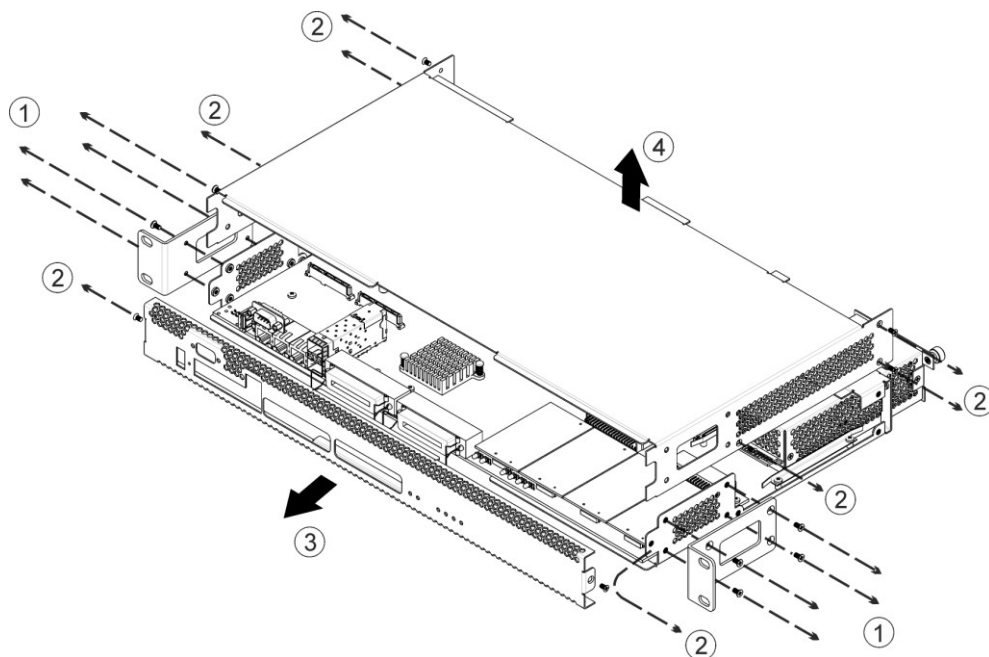


Рисунок 11 – Расположение submodule в SMG-1016M

1. С помощью отвертки отсоединить кронштейны от корпуса устройства.
2. С помощью отвертки отсоединить винты крепления передней и верхней панели устройства, как показано на рисунке.
3. Осторожно потянуть переднюю панель на себя до ее отделения от верхней и боковых панелей.
4. Снять верхнюю панель (крышку) устройства, потянув ее вверх.

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

2.11.6 Установка submodule

Устройство имеет модульную конструкцию с возможностью установки до 6 submodule IP SM-VP-M300 (*Submodule MSP*), позиции указаны на Рисунке 12.

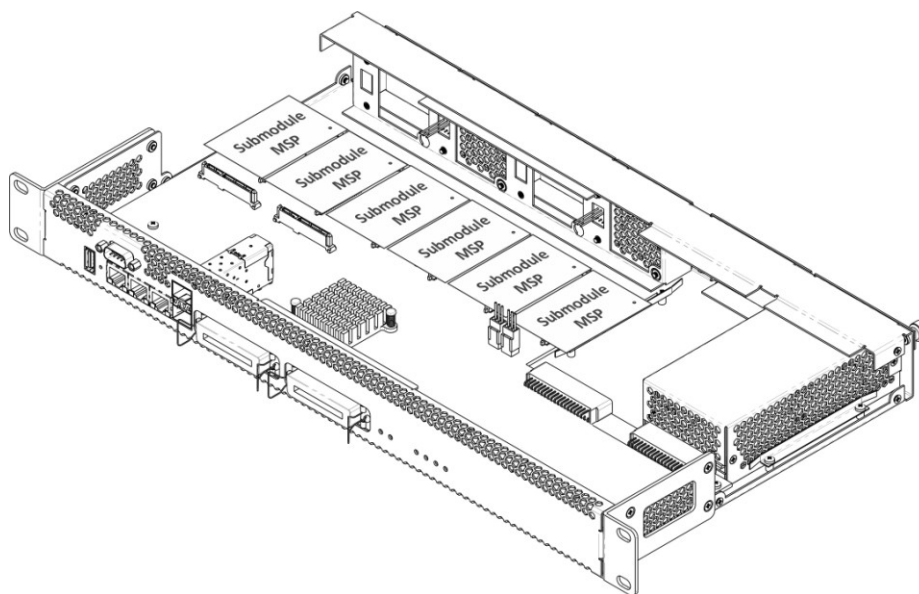


Рисунок 12 – Расположение submodule в SBC-1000

Порядок установки submodule в SBC:

5. Проверьте наличие питания сети на устройстве.
6. В случае наличия напряжения – отключить питание.
7. Установите модуль в свободную позицию (см. Рисунок 11).

2.11.7 Установка блоков вентиляции

Конструкция устройства предусматривает возможность замены блоков вентиляции без отключения питания.

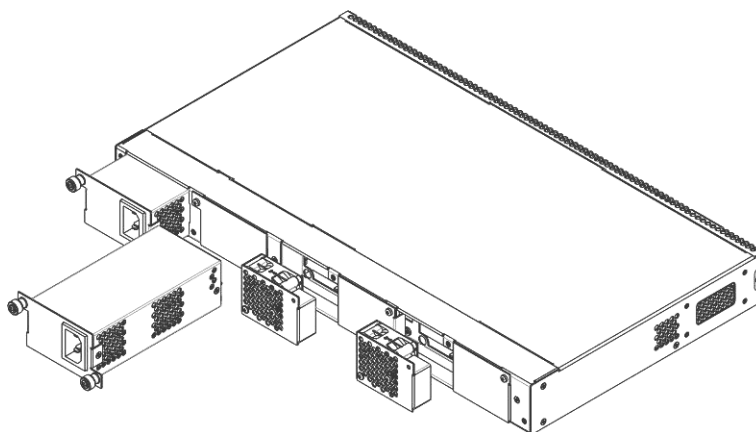


Рисунок 13 – Блок вентиляции. Крепление в корпусе

Для удаления блока необходимо:

1. С помощью отвертки отсоединить правый винт 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 14).

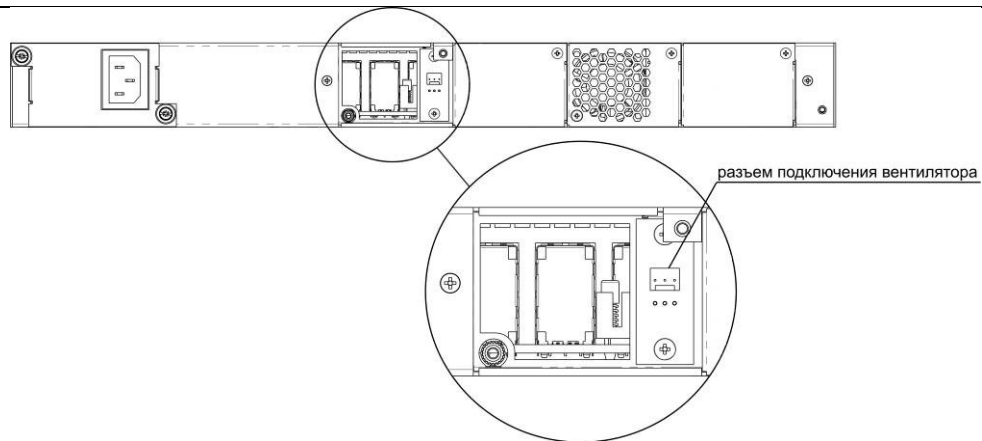


Рисунок 14 – Разъем для подключения вентилятора

Для установки блока необходимо:

1. Соединить контакты блока с разъемом в устройстве (Рисунок 14).
2. Уложить соединительные провода в специальное углубление на внутренней стороне блока.
3. Вставить блок в корпус устройства.
4. Закрепить винтом блок вентиляции на задней панели.

3 ОБЩИЕ РЕКОМЕНДАЦИИ ПРИ РАБОТЕ С УСТРОЙСТВОМ

Самым простым способом конфигурирования и мониторинга устройства является *web*-интерфейс, 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*-интерфейс. Установка пароля для доступа через telnet и консоль описана в разделе **4.2.1 Смена пароля для доступа к устройству**. Рекомендуется записать и сохранить установленные пароли в надежном месте, недоступном для злоумышленников. Также настоятельно рекомендуем не открывать доступ к устройству через Telnet/SSH/WEB из публичной сети.

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.

4 КОНФИГУРИРОВАНИЕ УСТРОЙСТВА

К устройству можно подключиться четырьмя способами: через *web*-интерфейс, с помощью протокола Telnet, SSH либо кабелем через разъем RS-232 (при доступе через RS-232, SSH либо Telnet используется командная консоль¹).



Для сохранения измененной конфигурации в энергонезависимую память используйте меню «Сервис/Сохранить конфигурацию во Flash» в WEB-конфигураторе, либо команду *save* в командной консоли.

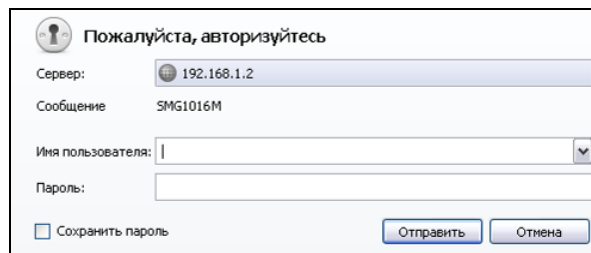
4.1 Настройка SBC-1000 через web-интерфейс

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



Заводской IP-адрес устройства SBC-1000 192.168.1.2, маска сети 255.255.255.0

После ввода IP-адреса устройство запросит имя пользователя и пароль.




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

После получения доступа к web-конфигуратору откроется меню *Системная информация*.

Системная информация	
Текущее время	Friday November 10 07:58:01 GMT+6 2000
Версия ПО	1.2.12
Время в работе	12d 04hour 27min 56sec
Информация о сборке:	
Дата сборки filesystem	2012-12-27 11:11:18
Дата сборки filesystem update	
Заводские параметры:	
Модель	SMG-1016M
Серийный номер	VI1F000301
MAC адрес	A8:F9:4B:81:79:9C
Сетевые настройки:	
Имя хоста	SMG1016M
IP-адрес	192.168.18.120
Маска подсети	255.255.255.0
Шлюз	192.168.18.1
Сервер времени (NTP)	0.0.0.0 GMT+6
Период синхронизации NTP, мин	240
DNS основной	Не установлен
DNS резервный	Не установлен
Использовать DHCP	Нет
Получить DNS автоматически	Нет
Получить NTP автоматически	Нет
Температура:	
Датчик #1	43.500 °C
Датчик #2	40.000 °C

¹ В текущей версии ПО не поддерживается

На рисунке ниже представлены 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.
- Кнопки управления* – элементы управления для работы с полем настроек.

Во избежание несанкционированного доступа при дальнейшей работе с устройством рекомендуется изменить пароль (раздел **Установка пароля для доступа через WEB конфигуратор** **Установка пароля для доступа через WEB конфигуратор**).



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

4.1.1 CDR-записи

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

Параметры сохранения CDR-записей	
Включить сохранение CDR-записей	<input checked="" type="checkbox"/>
Период сохранения: Дни	0
Часы	0
Минуты	1
Добавить заголовок	<input checked="" type="checkbox"/>
Отличительный признак	27
Настройки локального хранения	
Сохранять на локальном диске	<input checked="" type="checkbox"/>
Путь к локальному диску	no path
Время хранения данных: Дни	19
Часы	15
Минуты	18
Настройки FTP сервера	
Сохранять на FTP	<input checked="" type="checkbox"/>
FTP сервер	192.168.16.44
FTP порт	21
Путь к файлу	
Логин для FTP	test
Пароль для FTP
Настройки резервного FTP сервера	
Сохранять на FTP	<input checked="" type="checkbox"/>
FTP сервер	192.168.16.45
FTP порт	23
Путь к файлу	snmpd
Логин для FTP	test
Пароль для FTP
Прочие настройки	
Сохранять неуспешные вызовы	<input checked="" type="checkbox"/>
Сохранять пустые файлы	<input checked="" type="checkbox"/>
Сохранять Redirecting number	<input type="checkbox"/>
Метка переадресации	<input type="checkbox"/>

CDR – детализированные записи о вызовах, позволяют сохранить историю о совершенных через шлюз SBC-1000 вызовах.

Параметры сохранения CDR-записей

- *Включить сохранение CDR записей* – при установленном флаге шлюз будет формировать CDR записи;
- *Период сохранения: Дни, Часы, Минуты* – период формирования CDR записей, в течение данного периода CDR-записи хранятся в оперативной памяти, после - сохраняются на локальный источник хранения;
- *Добавить заголовок* – при установленном флаге в начало CDR файла записывается заголовок вида: SMG1016. 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 SSD диске;
- *Путь к локальному диску* – путь к локальному SSD-диску. 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».

Настройки локального хранения	
Сохранять на локальном диске	<input checked="" type="checkbox"/>
Путь к локальному диску	/mnt/sda1
Время хранения данных: Дни	2
Часы	0
Минуты	0

Папки и файлы на локальном диске	
20111205	<input type="checkbox"/>
20111208	<input type="checkbox"/>
yy.tar.gz	<input type="checkbox"/>

Загрузить Удалить

- *Время хранения данных: Дни, Часы, Минуты* – период хранения CDR записей на локальном SSD диске;



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



Если объем полученных CDR-записей превысит порог 30MB до истечения периода сохранения, 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;
- *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.
- *Сохранять Redirecting number¹* – при установленном флаге в записи CDR будет присутствовать дополнительное поле Redirecting number, иначе в случае переадресованного вызова дополнительного поля Redirecting number не будет, а сам номер, с которого была совершена переадресация будет помещен в параметре Calling party number;
- *Метка переадресации²* – при установленном флаге в записи CDR будет присутствовать дополнительное поле «метка переадресации».

4.1.1.1 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 (DATETIME);
- 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).

4.1.1.2 Пример CDR файла

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

```
<SBC>. CDR. File started at '20120726112449'
SIGNATURE;DATETIME;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;DST_CONTACT;
label;2012-07-26
11:24:39;6502;6501;;;0;16;0;;A;16;zBRyfChAr9mfhIPRI.3xjn4w2X.ui8ap;;192.168.23.170;192.168.23.212;;;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;
```

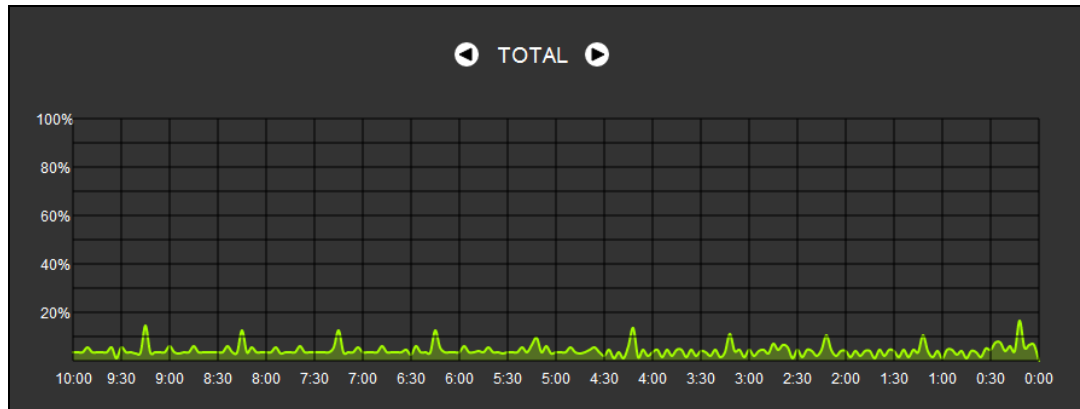
¹ В данной версии ПО функция не поддерживается

² В данной версии ПО функция не поддерживается

4.1.2 Мониторинг

4.1.2.1 Мониторинг 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.



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

4.1.2.2 Мониторинг SFP модулей

В разделе отображаются индикация состояния и параметры оптической линии.

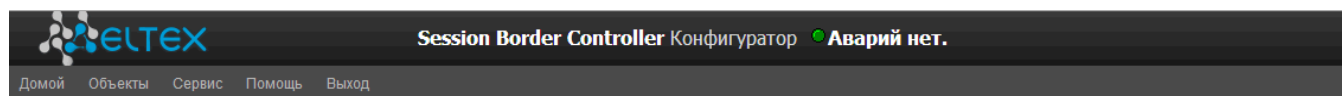
Мониторинг SFP модулей				
SFP порт 0 статус	Наличие SFP модуля		Состояние сигнала	
Laser Fault	Модуль не установлен		Сигнал потерян	
Температура, °C	Напряжение, В	Ток смещения TX, мА	Исходящая мощность, мВт	Входящая мощность, мВт
N/A	N/A	N/A	N/A	N/A
SFP порт 1 статус	Наличие SFP модуля		Состояние сигнала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

4.1.2.3 Журнал аварийных событий

При возникновении аварий информация о самой критичной в текущий момент выводится в заголовке WEB-интерфейса.

При отсутствии аварий выводится сообщение «Аварий нет».



В меню «Журнал аварийных событий» выводится список аварийных событий, ранжированных по дате и времени.

№	Время	Дата	Тип	Состояние	Параметры	Описание
2	15:25:54	01/03/13	CDR-FTP	Предупреждение	[00:00:00]	
1	15:23:39	01/03/13	CDR-FTP	Авария	[00:00:00]	
0	15:22:24	01/03/13	CDR-FTP	Критическая авария	[00:00:00]	

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* – тип аварии:

Тип	Расшифровка
Конфигурация не прочитана	Ошибка чтения файла конфигурации
MSP-module lost	Потеря связи с модулем MSP
FTP error. CDR-send failed	Ошибка передачи CDR файлов на FTP сервер. Возможны 3 уровня аварии – предупреждение, (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 была перезапущена
Звонок запрещен	Поступил вызов, обслуживание которого запрещено
Регистрация абонента запрещена	Поступил запрос регистрации, обслуживание которого запрещено

- *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.

4.1.3 Коммутатор

В данном разделе производится настройка портов коммутатора.

4.1.3.1 Настройки LACP

В данном разделе производится настройка групп LACP.

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

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

Для создания, редактирования и удаления группы LACP используется кнопки:

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

- *Name* – имя группы LACP;
- *Enable LACP* – 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 определенным 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. Требуется 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;
- *Combine interfaces in PortChannel* – список портов, добавленных в группу LACP.

New LACP	
Name	<input type="text" value="LACP trunk 0"/>
Enable LACP	<input type="checkbox"/>
Mode	<input type="text" value="active-backup"/>
Primary	<input type="text" value="none"/>
Updelay	<input type="text" value="100"/>
Miimon	<input type="text" value="100"/>
LACP rate	<input type="text" value="slow"/>
Combine interfaces in PortChannel	
GE port 0	
GE port 1	
GE port 2	
CPU port	
SFP port 0	
SFP port 1	

4.1.3.2 Настройка портов коммутатора

Коммутатор может работать в четырех режимах:

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.

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.

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*.

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*.

Настройки портов коммутатора						
	GE порт 0	GE порт 1	GE порт 2	CPU порт	SFP порт 0	SFP порт 1
Использовать VLAN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Default VLAN ID	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
VID Override	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Egress	<input type="text" value="Unmodified"/>	<input type="text" value="Unmodified"/>	<input type="text" value="Unmodified"/>	<input type="text" value="Unmodified"/>	<input type="text" value="Unmodified"/>	<input type="text" value="Unmodified"/>
IEEE mode	<input type="text" value="Fallback"/>	<input type="text" value="Fallback"/>	<input type="text" value="Fallback"/>	<input type="text" value="Fallback"/>	<input type="text" value="Fallback"/>	<input type="text" value="Fallback"/>
Output	<input checked="" type="checkbox"/> GE порт 1 <input checked="" type="checkbox"/> GE порт 2 <input checked="" type="checkbox"/> CPU порт <input checked="" type="checkbox"/> SFP порт 0 <input checked="" type="checkbox"/> SFP порт 1	<input checked="" type="checkbox"/> GE порт 0 <input checked="" type="checkbox"/> GE порт 2 <input checked="" type="checkbox"/> CPU порт <input checked="" type="checkbox"/> SFP порт 0 <input checked="" type="checkbox"/> SFP порт 1	<input checked="" type="checkbox"/> GE порт 0 <input checked="" type="checkbox"/> GE порт 1 <input checked="" type="checkbox"/> CPU порт <input checked="" type="checkbox"/> SFP порт 0 <input checked="" type="checkbox"/> SFP порт 1	<input checked="" type="checkbox"/> GE порт 0 <input checked="" type="checkbox"/> GE порт 1 <input checked="" type="checkbox"/> GE порт 2 <input checked="" type="checkbox"/> SFP порт 0 <input checked="" type="checkbox"/> SFP порт 1	<input checked="" type="checkbox"/> GE порт 0 <input checked="" type="checkbox"/> GE порт 1 <input checked="" type="checkbox"/> GE порт 2 <input checked="" type="checkbox"/> CPU порт <input checked="" type="checkbox"/> SFP порт 1	<input checked="" type="checkbox"/> GE порт 0 <input checked="" type="checkbox"/> GE порт 1 <input checked="" type="checkbox"/> GE порт 2 <input checked="" type="checkbox"/> CPU порт <input checked="" type="checkbox"/> SFP порт 0
LACP trunk	<input type="text" value="none"/>	<input type="text" value="none"/>	<input type="text" value="none"/>	<input type="text" value="none"/>	<input type="text" value="none"/>	<input type="text" value="none"/>

Коммутатор устройства имеет 3 электрических порта Ethernet, 2 оптических и один порт для взаимодействия с процессором:

- *GE порт 0, GE порт 1, GE порт 2* – электрические Ethernet-порты устройства;
- *SFP порт 0, SFP порт 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

- *Включить* – 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:
 - *disabled* – для пакета, принятого данным портом, применяются правила маршрутизации, указанные в разделе таблицы - «*output*».
 - *fallback* – если через порт принят пакет с тегом VLAN, для которого есть запись в таблице маршрутизации «802.1q», то этот пакет попадает под правила 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.
- *Output* – взаимодоступность портов для передачи данных. Устанавливаются разрешения отправки пакетов, принятых данным портом, в порты, отмеченные флагом;
- *LACP trunk* – группе LACP, к которой принадлежит указанный порт коммутатора.



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*».

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

4.1.3.3 802.1q

В подменю «802.1q» устанавливаются правила маршрутизации пакетов при работе коммутатора в режиме 802.1q.

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

- GE порт0, порт 1, порт 2 – электрические Ethernet-порты устройства;
- CPU – внутренний порт, подключенный к центральному процессору устройства;
- SFP порт 0, SFP порт 1 – оптические Ethernet-порты устройства.

Добавление записи в таблицу маршрутизации пакетов

В поле “VID” 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.
- *override* – при установленном флаге переписать приоритет 802.1p для данной VLAN, иначе – оставить приоритет неизменным;
- *priority* – приоритет 802.1p, назначаемый пакетам в данной VLAN, если установлен флаг *override*;

Затем необходимо нажать кнопку «Добавить».

- *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.

Удаление записи из таблицы маршрутизации пакетов

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

4.1.3.4 QoS и контроль полосы пропускания

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

VID	GE порт 0	GE порт 1	GE порт 2	CPU порт	SFP порт 0	SFP порт 1
Приоритет VLAN (default)	0	0	0	0	0	0
Режим QoS	Только DSCP	Только DSCP	Только DSCP	Только DSCP	Только DSCP	Только DSCP
Переназначить приоритеты 802.1p:	0	0	0	0	0	0
1	1	1	1	1	1	1
2	2	2	2	2	2	2
3	3	3	3	3	3	3
4	4	4	4	4	4	4
5	5	5	5	5	5	5
6	6	6	6	6	6	6
7	7	7	7	7	7	7
Режим ограничения входящих пакетов	выключен	выключен	выключен	выключен	выключен	выключен
Ограничение скорости для входящих пакетов в очереди 0	0	0	0	0	0	0
Ограничение скорости для входящих пакетов в очереди 1	предыдущий	предыдущий	предыдущий	предыдущий	предыдущий	предыдущий
Ограничение скорости для входящих пакетов в очереди 2	предыдущий	предыдущий	предыдущий	предыдущий	предыдущий	предыдущий
Ограничение скорости для входящих пакетов в очереди 3	предыдущий	предыдущий	предыдущий	предыдущий	предыдущий	предыдущий
Включить ограничение исходящих пакетов	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ограничение скорости для исходящих пакетов	0	0	0	0	0	0

- *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 preferred, 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;
- *Предпочтительно 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 IP diffserv;
- *Предпочтительно 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 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;
 - *mult_flood_broad* – ограничивается многоадресный (multicast), широковещательный (broadcast) и лавинный одноадресный (flooded unicast) трафик;
 - *mult_broad* – 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.

4.1.3.5 Распределение приоритетов

- *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 (основные значения diffserv приведены в таблице 7).
- *diffserv* – значение приоритета IP diffserv;
- *Очередь* – номер исходящей очереди.
- *Применить* – применить установленные настройки;
- *Подтвердить* – подтвердить измененные настройки;

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



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.



Очередь 3 является наиболее приоритетной, очередь 0 – наименее приоритетной. Взвешенное распределение пакетов по исходящим очередям 3/2/1/0 следующее: 8/4/2/1.

4.1.4 Конфигурация интерфейсов

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 (англ. Virtual Private Network — виртуальная частная сеть) — технология, позволяющая обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет).

PPTP (англ. Point-to-Point Tunneling Protocol) — 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

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 предназначена для задания маршрутов в IP-сети.

№	Статус	Режим	Направление	Маска	Шлюз	Интерфейс	Метрика
0	Активен	Создан автоматически	192.168.20.125	255.255.255.255	192.168.23.1	eth0	0
1	Активен	Создан автоматически	192.169.10.1	255.255.255.255	*	ppp0	0
2	Активен	Создан автоматически	11.10.10.110	255.255.255.255	*	ppp100	0
3	Активен	Создан автоматически	192.168.23.0	255.255.255.0	*	eth0	0
4	Активен	Задан вручную	192.168.26.0	255.255.255.0	192.168.23.1	eth0	0
5	Активен	Создан автоматически	11.10.10.0	255.255.255.0	*	eth0	0
6	Активен	Создан автоматически	default	0.0.0.0	192.168.23.1	eth0	0

Добавить Редактировать Удалить

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.

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

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

Направление:

ИР-сеть или default:

Маска:

Шлюз:

ИР-адрес или *:

Интерфейс:

Метрика:

Параметры маршрута:

- **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);
- **Интерфейс** – интерфейс передачи (если флажок не установлен, то будет выбран наиболее подходящий интерфейс на основе адреса шлюза);

- **Шлюз** – задает IP-адрес шлюза для маршрута;
- **Метрика** – метрика маршрута.

4.1.4.2 Простые интерфейсы

В данном подменю представлены порождения основного физического интерфейса. Добавление нового интерфейса позволяет создать интерфейсы в различные сети без использования VLAN, так же возможно использовать в целях периодического тестирования или изучения функционала SBC, не нарушая работу основной части: на интерфейсе можно настроить тестовую конфигурацию, которая выключится при удалении интерфейса (при этом настройки конфигурации будут сохранены и восстановлены при повторном создании интерфейса).

№	Ethernet	Имя сети	IP адрес	Маска сети	DHCP	Управление
0	eth0:0	n200	192.168.23.215	255.255.255.0	-	Web/Telnet/SSH
1	eth0:1	vpn_sbc_in	11.10.10.3	255.255.255.0	-	-

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

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

Сетевой интерфейс 3

Ethernet ID:

Имя сети:

IP адрес:

Маска сети:

Broadcast:

Использовать DHCP:

Управление через Web:

Управление по Telnet:

Управление по SSH:

Кнопка «Применить» служит для испытания созданной конфигурации: в случае неправильной настройки после перезагрузки устройства конфигурация вернется в состояние до редактирования (если не было выполнено сохранение конфигурации в энергонезависимую память устройства).

Параметры интерфейса:

- **Ethernet ID** – идентификатор клонируемого интерфейса (в текущей версии доступно клонирование только общесистемного интерфейса);
- **Имя сети** – произвольное имя (для удобства оператора), с которым будут ассоциированы заданные сетевые настройки;
- **IP адрес, Маска сети, Broadcast** – сетевые настройки

интерфейса (если не используется DHCP);

- **Использовать DHCP** – флажок для получения сетевых настроек автоматически посредством

- протокола DHCP (требуется наличие DHCP сервера в сети оператора);
- *Управление через Web, Управление по Telnet, Управление по SSH* — доступность соответствующего сервиса управления по заданному адресу интерфейса.

4.1.4.3 VLAN интерфейсы

В данном подменю можно редактировать состав VLAN интерфейсов (см. IEEE 802.1Q).

VLAN интерфейсы							
№	Ethernet	Имя сети	VLAN ID	IP адрес	Маска сети	DHCP	Управление
0	eth0.11:0	test	11	-	-	+	SSH

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

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

Кнопка «Применить» служит для испытания созданной конфигурации: в случае неправильной настройки после перезагрузки устройства конфигурация вернется в состояние до редактирования (если не было выполнено сохранение конфигурации).

VLAN интерфейс 1	
Ethernet ID	0
Имя сети	
VLAN ID	1
IP адрес	
Маска сети	255.255.255.0
Broadcast	
Использовать DHCP	<input type="checkbox"/>
Управление через Web	<input type="checkbox"/>
Управление по Telnet	<input type="checkbox"/>
Управление по SSH	<input type="checkbox"/>

Параметры интерфейса:

- *Ethernet ID* — идентификатор клонируемого интерфейса (в текущей версии доступно клонирование только общесистемного интерфейса);
 - *Имя сети* — произвольное имя (для удобства оператора), с которым будут ассоциированы заданные сетевые настройки;
 - *VLAN ID* — идентификатор виртуальной сети;
 - *IP адрес, Маска сети, Broadcast* — сетевые настройки интерфейса (если не используется DHCP);
 - *Использовать DHCP* — флажок для получения сетевых настроек автоматически посредством протокола DHCP (требуется наличие DHCP сервера в сети оператора в указанной виртуальной сети)
- *Управление через Web, Управление по Telnet, Управление по SSH* — доступность соответствующего сервиса управления по заданному адресу интерфейса.

4.1.4.4 VPN/pptp интерфейсы

В данном подменю можно создавать, редактировать интерфейсы для подключений к VPN сетям.

VPN/pptp интерфейсы						
№	Имя сети	PPTP IP	Имя пользователя	Статус интерфейса	Запустить	Остановить
0	ttt	192.168.20.125	test1	Запущен	Старт	Стоп

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

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

Для управления подключением используются кнопки «Старт» и «Стоп».

Параметры интерфейса:

- *Имя сети* — произвольное имя (для удобства оператора), с которым будут ассоциированы заданные сетевые настройки;
- *PPTPD IP* — IP адрес PPTP сервера для подключения;
- *Имя пользователя, Пароль* — идентификаторы пользователя;
- *Запуск при старте устройства* — флаг для автоматической попытки подключения при запуске/перезагрузке устройства;
- *Игнорировать шлюз по умолчанию* — при установленном флаге установить запрет модификации адреса шлюза по умолчанию при установке соединения;
- *Включить шифрование* — при установленном флаге осуществлять шифрование передаваемых данных.

VPN/pptp интерфейс 1	
Имя сети	<input type="text"/>
PPTPD IP	<input type="text" value="0.0.0.0"/>
Имя пользователя	<input type="text"/>
Пароль	<input type="text"/>
Опции:	
Запуск при старте устройства	<input type="checkbox"/>
Игнорировать шлюз по умолчанию	<input type="checkbox"/>
Включить шифрование	<input type="checkbox"/>

4.1.4.5 Общие настройки сети

В этом подменю редактируются настройки основного интерфейса (eth0).

Общие настройки сети

Имя хоста

Имя сети

IP-адрес

Маска подсети

Шлюз

DNS-Primary

DNS-Secondary

Использовать DHCP

Получить DNS автоматически

Использовать SNMP

Настройки управления через сетевой интерфейс eth0

Управление через Web

Управление по Telnet

Управление по SSH

Параметры:

- *Имя хоста* — сетевое имя устройства;
- *Имя сети* — произвольное имя (для удобства оператора), с которым будут ассоциированы заданные сетевые настройки;
- *IP адрес, Маска подсети* — сетевые настройки интерфейса (если не используется DHCP);
- *Шлюз* — IP адрес шлюза по умолчанию;
- *DNS-Primary, DNS-Secondary* — адреса основного и резервного DNS серверов;
- *Использовать DHCP* — флаг для получения сетевых настроек автоматически посредством протокола DHCP (требуется наличие DHCP сервера в сети оператора);
- *Получить DNS автоматически* — получить IP адрес DNS сервера через службу DHCP;
- *Использовать SNMP* — флаг для включения SNMP клиента;

- Управление через Web, Управление по Telnet, Управление по SSH — доступность соответствующего сервиса управления по заданному адресу интерфейса.

После смены IP-адреса в окне WEB-конфигуратора появится информационное сообщение о том, что через 5 секунд конфигуратор подключится по новому адресу. Нажатие на ссылку «Продолжить» также приведет к перенаправлению на новый адрес.

Изменился IP-адрес устройства, необходимо подключиться по новому адресу,
подтвердить изменения и сохранить конфигурацию во FLASH.
Подключение будет сделано автоматически через 5 секунд.
[Продолжить](#)

После подключения конфигуратором по новому адресу необходимо подтвердить изменение адреса. Для этого нажать ссылку «Подтвердить». Нажатие на ссылку «Отмена» приведет к переподключению по старому адресу.

Изменился IP-адрес устройства, Вы подключены по новому адресу!
[Подтвердить](#) [Отмена](#)



В случае если вы не можете подключиться по новому адресу, через минуту шлюз будет снова доступен по старому адресу.

4.1.5 Конфигурация SBC

Функционально SBC-1000 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. То есть можно сказать, что SBC-1000 осуществляет коммутацию сообщений между SBC SIP серверами. В общем случае в одной подсети может быть создано несколько SBC-1000 SIP серверов (например, туннели из одной в разные подсети). 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 речевой информации выделяется диапазон портов в каждой подсети, где планируется ее передавать.

Общий алгоритм настройки SBC-1000:

- выделить диапазон медиа портов в каждой подсети, где планируется передавать речь;
- создать SBC-1000 SIP серверы в тех подсетях, между которыми будет осуществляться коммутация;
- настроить коммутацию между SBC-1000 SIP серверами (создать SIP Trunk).

4.1.5.1 Media

В данном подменю указываются диапазоны выделенных портов для речевой информации абонентов (для передачи RTP пакетов, пакетов данных протокола T.38).

№	Имя сети	Интерфейс	Диапазон портов
0	n200	eth0 (192.168.23.215)	24000 - 25000

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

«Добавить»;
«Редактировать»;
«Удалить».

Media 1	
Имя сети	[0] n200 (eth0 192.168.23.215)
Начальный порт	24000
Конечный порт	30000

Параметры:

- *Имя сети* — имя сети (присвоенное оператором при редактировании сетевых интерфейсов), в которой создается диапазон, для удобства также показан IP-адрес;
- *Начальный порт*, *Конечный порт* — нижняя и верхняя границы диапазона UDP-портов.



После внесения всех изменений в конфигурацию, для вступления изменений в силу нужно перезапустить программу (меню «Сервис» - «Перезапуск ПО»).

4.1.5.2 SIP

В этом подменю редактируется список SBC SIP серверов (точки входа в туннели).

№	Имя сервера	Имя сети	Интерфейс	Порт	Media	Профиль RADIUS	Адаптация
0	ssw	ssw	eth0 (192.168.18.90)	5060	ssw (порты 34001-40000)	Не выбран	-
1	local	localnet	eth0.20 (192.168.16.199)	5060	localnet (порты 24000-50000)	Не выбран	-
2	model	ModelSSW	- (-)	5060	ModelSSW (порты 24000-50000)	Не выбран	-
3	ppp	345uu	ppp1 (адрес не получен)	5060	345uu (порты 24000-30000)	Не выбран	-

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

«Добавить»;
«Редактировать»;
«Удалить».

Параметры SBC SIP сервера:

- *Имя сервера* — произвольное имя для идентификации (удобное для оператора);
- *Имя сети* — имя сети (присвоенное оператором при редактировании сетевых интерфейсов), в которой создается сервер, для удобства также показан IP-адрес;
- *Порт* — порт для приема сигнализации SIP (по умолчанию протоколом SIP используется порт 5060);

- *Media* — диапазон портов для передачи речевой информации, для удобства также показаны границы диапазона;
- *Профиль RADIUS* — профиль RADIUS, используемый данным SIP сервером;
- *Адаптация* — настройка предназначена для адаптации взаимодействия через SBC шлюзов различных производителей с программным коммутатором ESCC-10.

SIP 0	
Имя сервера	ssw
Имя сети	[0] ssw (eth0 192.168.18.90)
Порт	5060
Media	[0] ssw (порты 48960-49999)
Профиль RADIUS	Не выбран
Адаптация	-
Таймаут ожидания RTP-пакетов, с	<input type="checkbox"/> 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	<input type="checkbox"/> 0
Запрашиваемый период контроля сессии (Session Expires, RFC 4028), с	<input checked="" type="checkbox"/> 198

- *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.

- *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 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.
- *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 во время обновлена (от 90 до 64800 с, рекомендуемое значение - 1800 с);



Контроль ожидания RTP, RTCP пакетов, а также использование RFC4028 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.

4.1.5.3 SIP Trunk

В данном подменю настраивается коммутация сообщений между SBC SIP-серверами.

В общем случае SBC-1000 транслирует SIP запросы на основании двух правил:

- на основании правила коммутации (для которого прописывается SIP-сервер приема, SIP-сервер отправки и адрес следующего SIP-сервера) (*статическая маршрутизация*);
- на основании зарегистрированного номера абонента (*динамическая маршрутизация*), правила коммутации для успешно зарегистрированного абонента создаются автоматически и имеют срок действия равный величине expires в ответном сообщении.

№	Сервер приема	Сервер передачи	Адрес назначения	Порт назначения	Тип	Абоненты за NAT	Время хранения соединения на NAT, с	SIP домен
0	model	model	192.168.2.101	5060	Абоненты	-	-	
1	local	ssw	192.168.18.27	5060	Абоненты	+	0	
2	ppp	ssw	192.168.18.27	5061	SIP trunk	-	-	-
3	ssw	local	192.168.16.150	0	Абоненты	-	-	

Добавить Редактировать Удалить

Параметры:

- *Сервер приема* — имя SIP сервера, где ожидаются входящие вызовы;
- *Сервер передачи* — имя SIP сервера, через который будет отправлен запрос;
- *IP адрес назначения, Порт назначения* — адрес следующего SIP-сервера, на который будет отправлен запрос;
- *Тип* – режим работы направления (*абонентский* – для обслуживания вызовов и регистраций от sip абонентов; *sip-trunk* – для обслуживания транзитных вызовов по протоколам SIP, SIP-T, SIP-I);
- *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 иницирующем 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;
- *SIP домен* – определяет принадлежность абонента к определенному домену. Передается шлюзом абонента в параметре «host» схемы SIP URI полей from и to (см. раздел 3.1.6.3 Интерфейсы SIP/SIP-T/SIP-I, SIP профили);

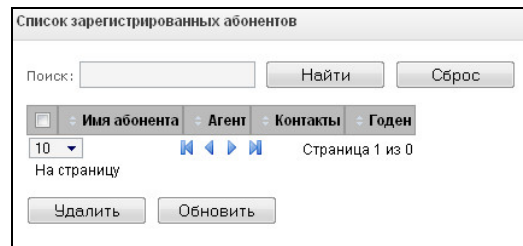
SIP Trunk 0

Сервер приема	[2] model
Сервер передачи	[2] model
Адрес назначения	192.168.2.101
Порт назначения	5060
Тип	Абоненты
Абоненты за NAT	<input type="checkbox"/>
Время хранения соединения на NAT, с	0
SIP домен	
Аутентификация SBC	
Логин	
Пароль	

Следует учитывать, что маршрут является *однаправленным*, вызовы могут осуществляться только со стороны сервера приема. Для того чтобы вызовы могли проходить в обе стороны, необходимо дополнительно создать маршрут в обратном направлении. Исключением является случай с зарегистрированным абонентом. В этом случае созданное правило используется для осуществления регистрации на регистраторе и для исходящих вызовов от абонента, а динамическое правило будет использоваться для входящих вызовов к абоненту, то есть в данном случае встречное правило создавать нет необходимости. Для получения дополнительной информации рекомендуется **ПРИЛОЖЕНИЕ В. ПРИМЕРЫ НАСТРОЙКИ SBC-1000.**

4.1.5.4 Список абонентов

В данном подменю отображаются зарегистрированные через SBC абоненты.



Поиск – проверка наличия номера абонента в списке зарегистрированных SIP-абонентов;

- *Имя абонента* – публичный номер зарегистрированного абонента, значение, переданное в заголовке To запроса REGISTER;
- *Агент* – SIP-клиент абонента, значение, переданное в заголовке User-Agent запроса REGISTER;
- *Контакты* – частные адреса зарегистрированного абонента, значения, переданные в заголовках Contact запроса REGISTER;
- *Годеи* – время, оставшееся до окончания действия регистрации;
- *Удалить* – позволяет удалить абонента или группу абонентов из базы зарегистрированных абонентов. Для удаления абонентов необходимо установить флаг напротив нужной строки и нажать кнопку «Удалить».
- *Обновить* – позволяет обновить список зарегистрированных абонентов.

4.1.6 Сетевые сервисы

4.1.6.1 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.

Параметры NTP	
Использовать NTP	<input type="checkbox"/>
Получать настройки автоматически	<input type="checkbox"/>
Сервер времени (NTP)	192.168.16.44
Часовой пояс	GMT+7
Период синхронизации NTP, мин	240

- *Использовать NTP* – включить NTP-клиента;
- *Получать настройки автоматически* – получить IP адрес SNTP сервера автоматически (при использовании протокола DHCP);
- *Сервер времени (NTP)* – сервер времени, с которого устройство будет синхронизировать дату и время;
- *Часовой пояс* - в выпадающем меню производится выбор часового пояса;
- *Период синхронизации NTP, мин* – период пересинхронизации времени, в минутах.

Для принудительной синхронизации времени от сервера необходимо нажать кнопку «Перезапустить NTP клиента» (или в пункте меню «Сервис/Перезапуск NTP-клиента»).

4.1.6.2 Настройки SNMP

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

4.1.6.3 SNMPv3 и COPM

Реализация функции COPM основана на рекомендации RFC 3924 Cisco Architecture for Lawful Intercept in IP Networks. Для осуществления перехвата используются MIB: CISCO-IP-TAP-MIB.my и CISCO-TAP2-MIB.my.

Конфигурация SNMPv3:

В системе используется только один пользователь SNMPv3. Пользователь SNMPv3 используется для выполнения команд COPMирования.

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

Параметры SNMPv3	
RW user name	<input type="text"/>
RW user password	<input type="password"/>
<input type="button" value="Удалить"/> <input type="button" value="Добавить"/>	

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

4.1.6.3.1 Настройка трапов (SNMP trap)



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

Настройка SNMP трапов				
№	Тип	Community	IP адрес	Порт
0	trap2sink		0.0.0.0	0

- *Перезапустить SNMPd* – по нажатию на кнопку осуществляется перезапуск SNMP клиента.

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.

SNMP trap 1	
Тип	trapsink
Community	<input type="text"/>
IP адрес	0.0.0.0
Порт	162
<input type="button" value="Применить"/> <input type="button" value="Отменить"/>	

4.1.6.4 VPN/PPTP сервер

Параметры VPN/PPTP сервера

– *Запускать при старте устройства* — запускать службу при старте/перезагрузке;

– *Адрес сервера* — IP-адрес, который будет сообщен в качестве рег всем подключающимся PPTP клиентам;

– *Начальный адрес клиента, Конечный адрес клиента* — границы диапазона IP адресов, назначаемых PPTP клиентам;

– *Адрес прослушивания соединения* — IP-адрес, к которому должны подключаться клиенты;

– *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).

VPN/pptp сервер

Параметры VPN/PPTP сервера	
Запускать при старте устройства	<input checked="" type="checkbox"/>
Адрес сервера	11.10.10.3
Начальный адрес клиента	11.10.10.100
Конечный адрес клиента	11.10.10.200
Адрес прослушивания соединения	192.168.23.215
DNS сервер	0.0.0.0
Количество возможных клиентов	100
Включить шифрование данных	<input checked="" type="checkbox"/>

Применить Сброс Отмена

Управление сервером

Запустить Остановить

VPN/pptp сервер запущен.

Параметры VPN/PPTP клиентов			
№	Имя	Пароль	Адрес
0	test1	q1w2e3r4	11.10.10.110
1	test2	q1w2e3r4	0.0.0.0

Добавить Редактировать Удалить

Для управления PPTP сервером используются кнопки «Запустить» и «Остановить». При остановке новые соединения клиентов не будут создаваться, однако уже созданные будут продолжать работать.

Параметры VPN/PPTP клиентов

В таблице показывается список идентификаторов клиентов, которым разрешено подключаться к данному серверу.

VPN/pptp сервер

VPN/pptp клиент 2	
Имя пользователя	VPN client 2
Пароль	
Адрес клиента	0.0.0.0

Сохранить Отменить

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.

4.1.7 Безопасность

4.1.7.1 Управление

В этом подменю изменяются пароли доступа к средствам конфигурирования SBC-1000.

В окне «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.

Управление

Установить пароль администратора веб-интерфейса:

Введите пароль:

Подтвердите пароль:

Пользователи веб-интерфейса:

№	Имя	Группа
0	admin	administrators

Установить пароль администратора для telnet и ssh:

Введите пароль:

Подтвердите пароль:

4.1.7.2 Настройка SSL/TLS

Данное меню позволяет настроить шифрование данных при доступе к web-интерфейсу: выбрать протокол доступа (HTTP и/или шифрованный HTTPS), а также сгенерировать сертификаты, используемые для доступа по HTTPS.

Настройка SSL/TLS

HTTP или HTTPS Протокол взаимодействия с web-конфигуратором

Сгенерировать новые сертификаты

<input type="text"/>	Двузначный код страны
<input type="text"/>	Регион
<input type="text"/>	Город
<input type="text"/>	Организация
<input type="text"/>	Подразделение
<input type="text"/>	Контактный e-mail
<input type="text"/>	Имя устройства (или IP-адрес)

4.1.7.3 Fail2ban

Fail2ban - это утилита, которая отслеживает в log-файлах попытки обращения к различным сервисам. При обнаружении постоянно повторяющихся неудачных попыток обращения с одного и того же IP-адреса или хоста, fail2ban блокирует дальнейшие попытки с этого IP-адреса/хоста.

В качестве неудачных попыток могут быть идентифицированы:

- подбор аутентификационных данных – прием запросов REGISTER с известного IP-адреса, но с неверными аутентификационными данными;
- прием запросов (REGISTER, INVITE, SUBSCRIBE, и других) с неизвестного IP-адреса;
- прием неизвестных запросов по SIP-порту.

Параметры fail2ban																																																								
Включить	<input type="checkbox"/>																																																							
Время блокировки, с	<input type="text" value="600"/>																																																							
Количество попыток доступа	<input type="text" value="3"/>																																																							
<input type="button" value="Применить"/>																																																								
Управление fail2ban																																																								
fail2ban не запущен!																																																								
<input type="button" value="Перезапустить"/> <input type="button" value="Остановить"/>																																																								
<table border="1"> <thead> <tr> <th colspan="2">Белый список: (последние 30 записей)</th> <th><input type="button" value="Обновить"/></th> </tr> <tr> <th>№</th> <th>IP адрес</th> <td></td> </tr> </thead> <tbody> <tr> <td colspan="2" style="text-align: center;">Нет IP адресов в списке</td> <td></td> </tr> <tr> <td><input type="text"/></td> <td></td> <td><input type="button" value="Добавить"/></td> </tr> <tr> <td></td> <td></td> <td><input type="button" value="Удалить"/></td> </tr> <tr> <td></td> <td></td> <td><input type="button" value="Найти"/></td> </tr> <tr> <td colspan="2">Скачать белый список IP адресов целиком</td> <td><input type="button" value="Скачать"/></td> </tr> </tbody> </table>	Белый список: (последние 30 записей)		<input type="button" value="Обновить"/>	№	IP адрес		Нет IP адресов в списке			<input type="text"/>		<input type="button" value="Добавить"/>			<input type="button" value="Удалить"/>			<input type="button" value="Найти"/>	Скачать белый список IP адресов целиком		<input type="button" value="Скачать"/>	<table border="1"> <thead> <tr> <th colspan="2">Черный список: (последние 30 записей)</th> <th><input type="button" value="Обновить"/></th> </tr> <tr> <th>№</th> <th>IP адрес</th> <td></td> </tr> </thead> <tbody> <tr> <td colspan="2" style="text-align: center;">Нет IP адресов в списке</td> <td></td> </tr> <tr> <td><input type="text"/></td> <td></td> <td><input type="button" value="Добавить"/></td> </tr> <tr> <td></td> <td></td> <td><input type="button" value="Удалить"/></td> </tr> <tr> <td></td> <td></td> <td><input type="button" value="Найти"/></td> </tr> <tr> <td colspan="2">Скачать черный список IP адресов целиком</td> <td><input type="button" value="Скачать"/></td> </tr> </tbody> </table>	Черный список: (последние 30 записей)		<input type="button" value="Обновить"/>	№	IP адрес		Нет IP адресов в списке			<input type="text"/>		<input type="button" value="Добавить"/>			<input type="button" value="Удалить"/>			<input type="button" value="Найти"/>	Скачать черный список IP адресов целиком		<input type="button" value="Скачать"/>	<table border="1"> <thead> <tr> <th colspan="2">Список заблокированных адресов</th> <th><input type="button" value="Обновить"/></th> </tr> <tr> <th>№</th> <th>IP адрес</th> <td></td> </tr> </thead> <tbody> <tr> <td colspan="2" style="text-align: center;">Нет IP адресов в списке</td> <td></td> </tr> <tr> <td colspan="2">Скачать список заблокированных IP адресов целиком</td> <td><input type="button" value="Скачать"/></td> </tr> </tbody> </table>	Список заблокированных адресов		<input type="button" value="Обновить"/>	№	IP адрес		Нет IP адресов в списке			Скачать список заблокированных IP адресов целиком		<input type="button" value="Скачать"/>
Белый список: (последние 30 записей)		<input type="button" value="Обновить"/>																																																						
№	IP адрес																																																							
Нет IP адресов в списке																																																								
<input type="text"/>		<input type="button" value="Добавить"/>																																																						
		<input type="button" value="Удалить"/>																																																						
		<input type="button" value="Найти"/>																																																						
Скачать белый список IP адресов целиком		<input type="button" value="Скачать"/>																																																						
Черный список: (последние 30 записей)		<input type="button" value="Обновить"/>																																																						
№	IP адрес																																																							
Нет IP адресов в списке																																																								
<input type="text"/>		<input type="button" value="Добавить"/>																																																						
		<input type="button" value="Удалить"/>																																																						
		<input type="button" value="Найти"/>																																																						
Скачать черный список IP адресов целиком		<input type="button" value="Скачать"/>																																																						
Список заблокированных адресов		<input type="button" value="Обновить"/>																																																						
№	IP адрес																																																							
Нет IP адресов в списке																																																								
Скачать список заблокированных IP адресов целиком		<input type="button" value="Скачать"/>																																																						

Параметры Fail2ban:

Включить – запустить утилиту Fail2ban;

Время блокировки, с – время в секундах, на протяжении которого доступ с подозрительного адреса будет блокирован;

Количество попыток доступа – максимальное число неудачных попыток доступа к сервису, прежде чем хост будет заблокирован с помощью fail2ban.

Управление Fail2ban:

Управление fail2ban	
fail2ban запущен!	
<input type="button" value="Перезапустить"/> <input type="button" value="Остановить"/>	

Перезапустить – начать/возобновить работу Fail2ban;

Остановить – остановить работу Fail2ban.

Белый список (последние 30 записей) - список IP-адресов, которые не могут быть заблокированы fail2ban. 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 4096 записей.

Для добавления/поиска адреса в списке необходимо указать его в поле ввода и нажать кнопку «Добавить»/ «Найти», для удаления – нажать «Удалить» напротив требуемого адреса.

Скачать белый/черный список IP адресов целиком – в Web-интерфейсе отображается только 30 последних записей в файле, нажатие на данную кнопку позволяет скачать весь белый или черный список на компьютер.

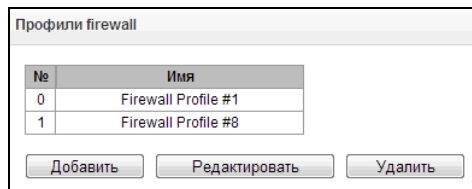
Список заблокированных адресов – перечень адресов, заблокированных в ходе работы fail2ban.

Скачать список заблокированных IP адресов целиком – позволяет скачать весь список заблокированных адресов на компьютер.

Обновление списков происходит по нажатию кнопки «Обновить» напротив заголовка.

4.1.7.4 Профили firewall

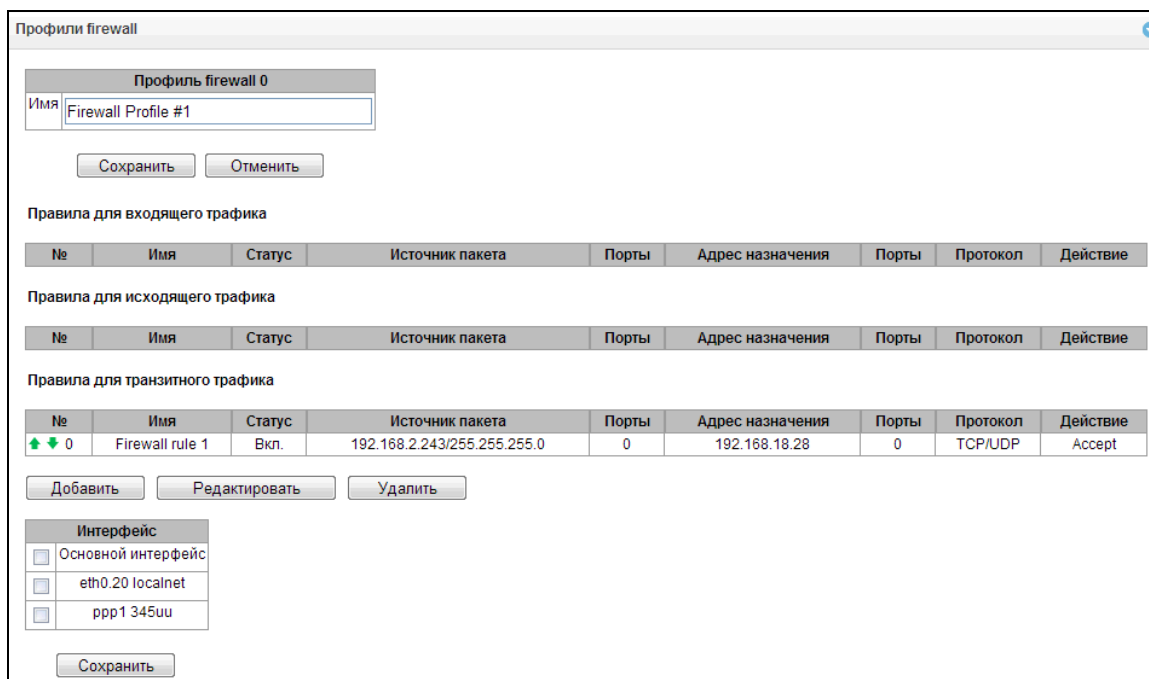
Firewall или **сетевой экран** — комплекс программных средств, осуществляющий контроль и фильтрацию передаваемых через него сетевых пакетов в соответствии с заданными правилами, что необходимо для защиты устройства от несанкционированного доступа.



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.



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, транзитный – проходящий через SBC);
- *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.

Правило firewall	
Имя	Firewall rule 5
Использовать	<input type="checkbox"/>
Тип трафика	Транзитный
Источник пакета	<input checked="" type="checkbox"/> Любой
IP адрес/маска	0.0.0.0
Порты источника	0
Адрес назначения	<input checked="" type="checkbox"/> Любой
IP адрес/маска	0.0.0.0
Порты назначения	0
Протокол	Любой
Тип сообщения (ICMP)	any
Действие	Accept

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.

Интерфейс	
<input type="checkbox"/>	Основной интерфейс
<input type="checkbox"/>	eth0.20 localnet
<input type="checkbox"/>	ppp1 345uu

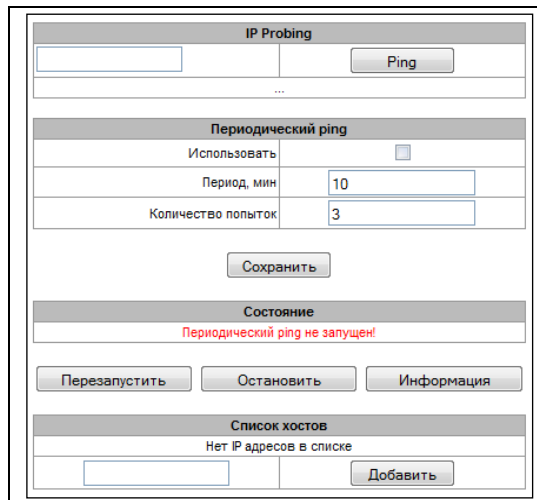


Каждый сетевой интерфейс может одновременно использоваться только в одном профиле firewall. При попытке назначения сетевого интерфейса в новый профиль из старого он будет удален.

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

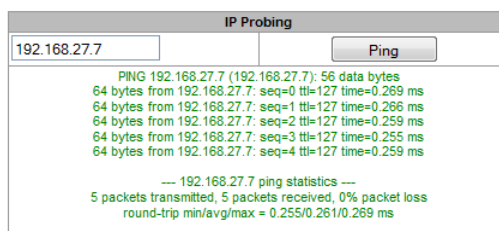
4.1.8 Сетевые утилиты

4.1.8.1 PING



IP Probing

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.

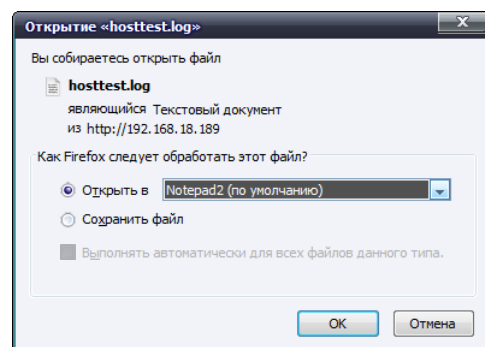


Периодический ping

- *Использовать* – при установленном флаге посылать ping-запросы на адреса, указанные в списке хостов;
- *Период, мин* – интервал между запросами в минутах;
- *Количество попыток* – число попыток отправить ping-запрос.

Состояние

- *Перезапустить* – запуск периодического ping;
- *Остановить* – принудительный останов периодического ping;
- *Информация* – по нажатию данной кнопки для просмотра станет доступен лог-файл '/tmp/log/hoststest.log' с данными о последней попытке периодического ping-запроса.

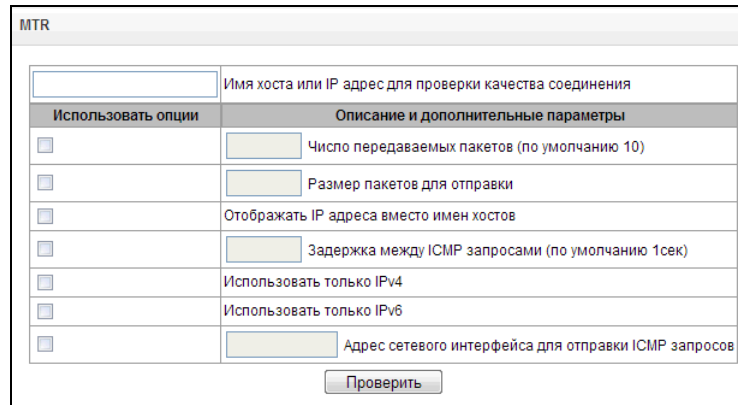


Список хостов – список IP-адресов, на которые будут отправляться периодические ping-запросы.

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

4.1.8.2 MTR

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



Использовать опции	Описание и дополнительные параметры
<input type="checkbox"/>	Число передаваемых пакетов (по умолчанию 10)
<input type="checkbox"/>	Размер пакетов для отправки
<input type="checkbox"/>	Отображать IP адреса вместо имен хостов
<input type="checkbox"/>	Задержка между ICMP запросами (по умолчанию 1сек)
<input type="checkbox"/>	Использовать только IPv4
<input type="checkbox"/>	Использовать только IPv6
<input type="checkbox"/>	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).

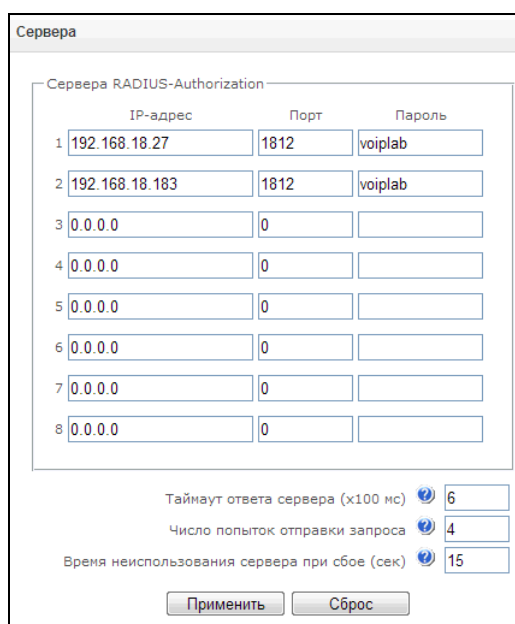
HOST:	src	Loss%	Snt	Last	Avg	Best	Wrst	StDev
1.	192.168.16.44	0.0%	10	0.3	0.3	0.2	0.3	0.0

4.1.9 Настройка RADIUS

Шлюз поддерживает аутентификацию регистрирующихся через него абонентов и авторизацию вызовов с помощью RADIUS-сервера. При использовании RFC4590 параметры для digest-аутентификации (в сообщении ACCESS-CHALLENGE) шлюз получает от RADIUS сервера и пересылает их абоненту. При использовании RFC4590-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 соответствующего SIP-сервера (раздел 4.1.5.2 SIP) установить нужный *Профиль RADIUS*.

4.1.9.1 Сервера RADIUS



	IP-адрес	Порт	Пароль
1	192.168.18.27	1812	voiplab
2	192.168.18.183	1812	voiplab
3	0.0.0.0	0	
4	0.0.0.0	0	
5	0.0.0.0	0	
6	0.0.0.0	0	
7	0.0.0.0	0	
8	0.0.0.0	0	

Таймаут ответа сервера (x100 мс)

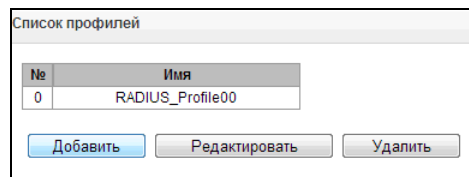
Число попыток отправки запроса

Время неиспользования сервера при сбое (сек)

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



№	Имя
0	RADIUS_Profile00

Добавить Редактировать Удалить

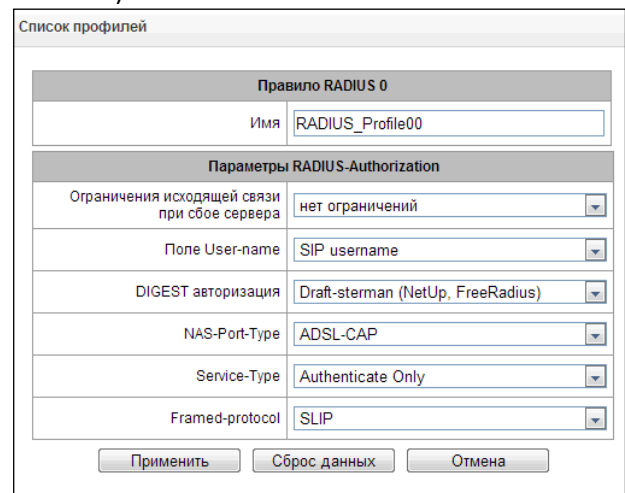
Для создания, редактирования и удаления профилей RADIUS используется меню «Объекты» - «Добавить объект», «Объекты» - «Редактировать объект» и «Объекты» - «Удалить объект», а также кнопки:

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

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.



Правило RADIUS 0	
Имя	RADIUS_Profile00
Параметры RADIUS-Authorization	
Ограничения исходящей связи при сбое сервера	нет ограничений
Поле User-name	SIP username
DIGEST авторизация	Draft-sterman (NetUp, FreeRadius)
NAS-Port-Type	ADSL-CAP
Service-Type	Authenticate Only
Framed-protocol	SLIP

Применить Сброс данных Отмена

- *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:
 - *RFC4590* – полноценная реализация рекомендации RFC4590;
 - *RFC4590-no-challenge* – работа с сервером не передающим Access Challenge;
 - *Draft-sterman (NetUp, FreeRadius)* – работа по драфту, на основании которого была написана рекомендация RFC4590);
- *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 Настройка трассировки

4.1.10.1 PCAP трассировки

В меню производится настройка параметров для анализа сетевого трафика.

PCAP трассировки

TCP-dump

Интерфейс: eth0

Ограничение длины пакетов: 3000

Добавить фильтр:

Запустить Завершить Перезапустить

Зеркалирование портов

	CPU порт	GE порт 0	GE порт 1	GE порт 2	SFP порт 0	SFP порт 1
Порты источника входящих пакетов	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Порты источника исходящих пакетов	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Порт назначения для входящих пакетов	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Порт назначения для исходящих пакетов	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Применить Подтвердить Очистить Сохранить

Файлы и папки в директории /tmp/log

dmesg	<input type="checkbox"/>
ecss	<input type="checkbox"/>
hosttest.log	<input type="checkbox"/>
lastlog	<input type="checkbox"/>
snmpd	<input type="checkbox"/>
wtmp	<input type="checkbox"/>

Загрузить Удалить

TCP-dump – настройки для утилиты TCP-dump:

- *Интерфейс* – интерфейса для захвата сетевого трафика;
- *Ограничение длины пакетов* – ограничение размера захватываемых пакетов, в байтах;
- *Добавить фильтр* – фильтр пакетов для утилиты tcpdump.

TCP-dump

TCP-dump для интерфейса eth0 завершен.

Загрузить eth0.pcap

Интерфейс: eth0

Ограничение длины пакетов: 3000

Запустить Завершить Перезапустить

TCP-dump завершен!

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 появится кнопка, позволяющая скачать **dump** с указанного интерфейса на локальный компьютер.



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 /tmp/log** доступен список файлов в соответствующей директории **/tmp/log**.

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

Port mirroring – настройки зеркалирования трафика:

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

Зеркалирование портов

	CPU порт	GE порт 0	GE порт 1	GE порт 2	SFP порт 0	SFP порт 1
Порты источника входящих пакетов	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Порты источника исходящих пакетов	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Порт назначения для входящих пакетов	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Порт назначения для исходящих пакетов	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

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* – сохранить параметры настройки зеркалирования;
- *Очистить* – сбросить настройки зеркалирования.



Настройки зеркалирования сохраняются только до перезагрузки шлюза.



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

4.1.10.2 Настройки 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.



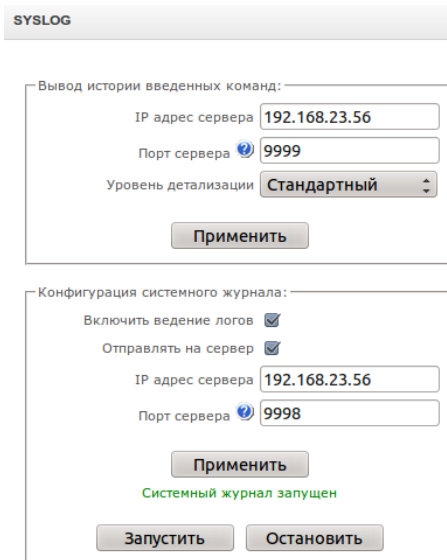
Системный журнал необходимо использовать только в случае возникновения проблем в работе шлюза для выявления их причин. Для того чтобы определиться с необходимыми уровнями отладки рекомендуется обратиться в сервисный центр ООО «Предприятие «Элтекс».

Вывод истории введенных команд

- *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;*
 - *Стандартный;*
 - *Полный.*

Конфигурация системного журнала

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

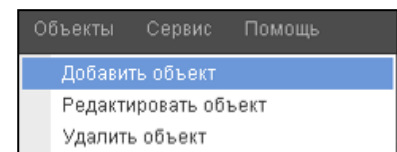


- *Включить ведение логов* – включить ведение журнала событий;
- *Отправлять на сервер* – при установленном флаге запись журнала будет вестись на сервере, IP-адрес которого настраивается ниже, иначе журнал будет сохраняться в оперативную память (размер журнала ограничен 5 Мб, кроме того, записи в журнале 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».

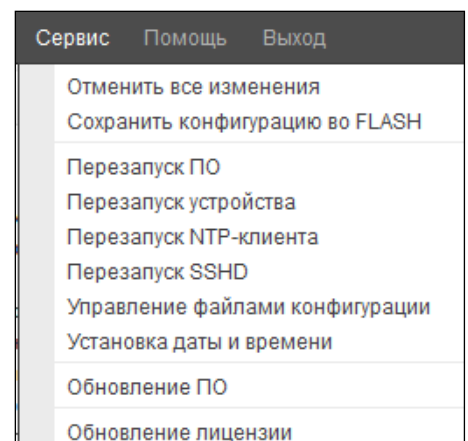
Для принудительного перезапуска SSHD необходимо выбрать меню «Сервис» - «Перезапуск SSHD».

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

Для ручной настройки локальных даты и времени на устройстве необходимо выбрать меню «Сервис» - «Установка даты и времени», см. пункт 4.1.13 **Настройка даты и времени.**

Для обновления ПО через Web-интерфейс необходимо выбрать меню «Сервис» - «Обновление ПО», см. пункт 4.1.14 **Обновление ПО через web-интерфейс.**

Для обновления/ добавления лицензий необходимо выбрать меню «Сервис» - «Обновление



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».

Открывается 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

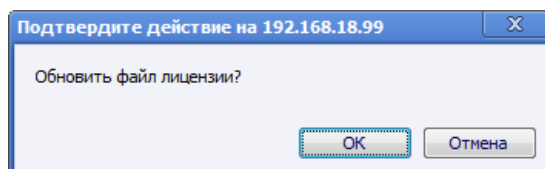
Для обновления/ добавления лицензий необходимо получить файл лицензии, обратившись в коммерческий отдел ООО «Предприятие «Элтекс» по адресу eltex@eltex.nsk.ru или по телефону +7(383) 274-48-48, указав серийный номер и MAC-адрес устройства (см. раздел 4.1.18 Просмотр заводских параметров и информации о системе).

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».

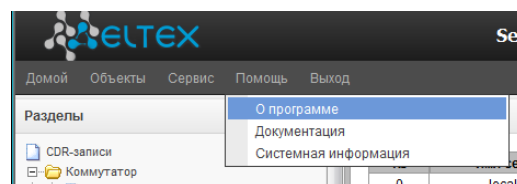
Для обновления файла лицензии требуется подтверждение.



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>.

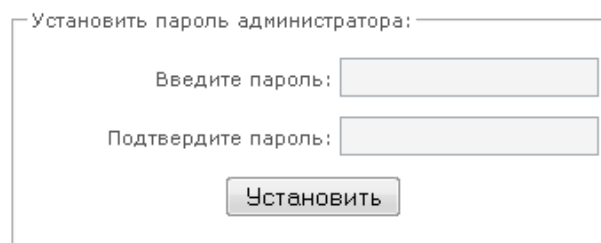


4.1.17 Установка пароля для доступа через WEB configurator

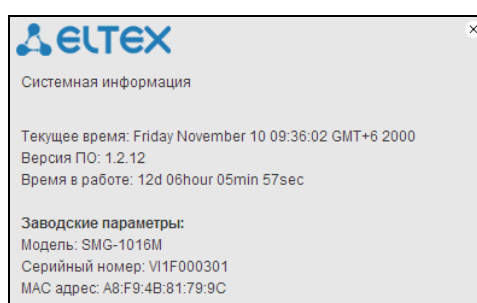
Ссылка предназначена для работы с паролями доступа к устройству через web-интерфейс.

Для смены пароля для администратора необходимо ввести новый пароль в поле «Введите пароль», в поле «Подтвердите новый пароль» повторить новый пароль. Нажать кнопку «Установить» для применения пароля.

Для сохранения конфигурации необходимо использовать меню «Сервис» - «Сохранить конфигурацию».



4.1.18 Просмотр заводских параметров и информации о системе



Для просмотра необходимо использовать меню «Помощь» - «Системная информация».

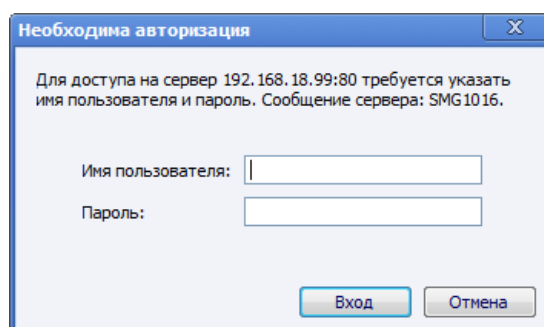
Заводские параметры (Серийный номер и MAC адрес) также указаны в шильдике (наклейке) на нижней части корпуса изделия.

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 «Домой» на панели управления.

Системная информация	
Текущее время	Friday November 10 07:58:01 GMT+6 2000
Версия ПО	1.2.12
Время в работе	12d 04hour 27min 56sec
Информация о сборке:	
Дата сборки filesystem	2012-12-27 11:11:18
Дата сборки filesystem update	
Заводские параметры:	
Модель	SMG-1016M
Серийный номер	VI1F000301
MAC адрес	A8:F9:4B:81:79:9C
Сетевые настройки:	
Имя хоста	SMG1016M
IP-адрес	192.168.18.120
Маска подсети	255.255.255.0
Шлюз	192.168.18.1
Сервер времени (NTP)	0.0.0.0 GMT+6
Период синхронизации NTP, мин	240
DNS основной	Не установлен
DNS резервный	Не установлен
Использовать DHCP	Нет
Получить DNS автоматически	Нет
Получить NTP автоматически	Нет
Температура:	
Датчик #1	43.500 °C
Датчик #2	40.000 °C

4.1.19 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-1000 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**, 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 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 `passwd` 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>`

ПРИЛОЖЕНИЕ А. РЕЗЕРВНОЕ ОБНОВЛЕНИЕ ВСТРОЕННОГО ПО УСТРОЙСТВА

В случае, когда не удастся обновить ПО через web-интерфейс 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 *smg*, в которую поместить файлы *smg1016M_kernel*, *smg1016M_initrd* (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":

```
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. Ввести *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*:

```
=> run flash_kern
About preceding 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*:

```
=> 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. НАСТРОЙКА БРАНДМАУЭРА (IPTABLES) НА УСТРОЙСТВЕ

Команда	Описание
<code>iptables</code>	настройка правил брандмауэра (firewall)
<code>save-iptables</code>	сохранение созданных правил брандмауэра (firewall)
<code>restore-iptables</code>	восстановление первоначальных правил брандмауэра (firewall) в случае если текущие правила не сохранены

Для настройки firewall необходимо подключиться к шлюзу через COM-порт, SSH либо через Telnet (при заводских установках адрес **192.168.1.2**, маска **255.255.255.0**) терминальной программой, например TERATERM.

Последовательность действий при настройке брандмауэра:

1. *Для настройки через COM-порт*
Подключить нуль-модемным кабелем COM-порт компьютера к порту «Console» устройства либо
Для настройки через SSH, Telnet
Подключить компьютер Ethernet-кабелем к Ethernet-порту устройства.
2. Запустить терминальную программу;
3. Настроить подключение через COM-порт: скорость передачи 115200, формат данных 8 бит, без паритета, 1 бит стоповый, без управления потоком либо через Telnet, SSH: IP-адрес при заводских установках 192.168.1.2, порт 23 (Telnet), порт 22 (SSH);
4. Ввести логин `admin`, при заводских установках пароль `rootpasswd`;
5. Создать необходимые правила в соответствии с руководством на утилиту `iptables`, руководство доступно по команде `iptables -h`;

Примеры использования утилиты `iptables` :

а) принимать пакеты протокола TCP по 25 -му порту от хоста 212.164.54.162:

```
iptables -A INPUT -s 212.164.54.162 -p tcp -m tcp --dport 25 -j ACCEPT
```

б) отбрасывать все пакеты от хоста 216.223.9.208:

```
iptables -A INPUT -s 216.223.9.208 -j DROP
```

в) отбрасывать все пакеты от сети 216.223.0.0/255.255.0.0:

```
iptables -A INPUT -s 216.223.0.0/255.255.0.0 -j DROP
```

г) посмотреть все таблицы:

```
iptables -L
```

6. Сохранить созданные правила командой `save-iptables`.

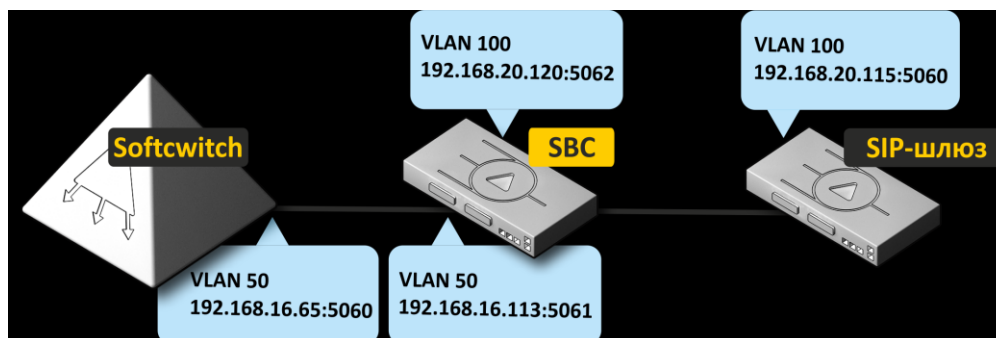


Восстановление первоначальных правил, если текущие изменения не сохранены, осуществляется командой `restore-iptables`.

ПРИЛОЖЕНИЕ В. ПРИМЕРЫ НАСТРОЙКИ SBC-1000

1. Настройка SBC-1000 для SIP абонентов

Схема применения



Алгоритм работы

Абонентский шлюз отправляет сообщение на IP-адрес 192.168.20.120 порт 5062, SBC-1000 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/Простые интерфейсы**).

a. Создать интерфейс в направлении Softswitch.

Параметры интерфейса: *vlan 100 192.168.16.113*

Сетевой интерфейс 1	
Ethernet ID	0
Имя сети	16.113
IP адрес	192.168.16.113
Маска сети	255.255.255.0
Broadcast	
Использовать DHCP	<input type="checkbox"/>
Управление через Web	<input type="checkbox"/>
Управление по Telnet	<input type="checkbox"/>
Управление по SSH	<input type="checkbox"/>
<input type="button" value="Сохранить"/> <input type="button" value="Отменить"/>	

b. Создать интерфейс в направлении абонентского шлюза.

Параметры интерфейса: *192.168.20.120*

Сетевой интерфейс 2	
Ethernet ID	0
Имя сети	20.120
IP адрес	192.168.20.120
Маска сети	255.255.255.0
Broadcast	
Использовать DHCP	<input type="checkbox"/>
Управление через Web	<input type="checkbox"/>
Управление по Telnet	<input type="checkbox"/>
Управление по SSH	<input type="checkbox"/>
<input type="button" value="Сохранить"/> <input type="button" value="Отменить"/>	

2. Конфигурирование медиа для SIP-интерфейсов (меню **Конфигурация SBC/Media**)

a. создать диапазон RTP портов для интерфейса 20.120

Media 0	
Имя сети	[1] 20.120 (eth0:1)
Начальный порт	24000
Конечный порт	30000
<input type="button" value="Применить"/> <input type="button" value="Отменить"/>	

b. создать диапазон RTP портов для интерфейса 16.113

Media 1	
Имя сети	[2] 16.113 (eth0.100)
Начальный порт	24000
Конечный порт	30000

c. Таблица Media будет иметь следующий вид:

№	Имя сети	Интерфейс	Диапазон портов
0	20.120	eth0.1 (адрес не получен)	24000 - 30000
1	16.113	eth0.100 (адрес не получен)	24000 - 30000

3. Конфигурирование SIP-интерфейсов (меню **Конфигурация SBC/SIP**)

a. Добавить SIP-интерфейс в направлении абонентского шлюза.

Параметры интерфейса:

*сетевой интерфейс 20.120;
порт для сигнализации – 5062;
медиа – 20.120.*

SIP 0	
Имя сервера	20.120_5062
Имя сети	[1] 20.120 (eth0:1)
Порт	5062
Media	[0] 20.120 (порты 24000-30000)

b. Добавить SIP-интерфейс в направлении Softswitch.

Параметры интерфейса:

*сетевой интерфейс 16.113;
порт для сигнализации – 5061;
медиа – 16.113.*

SIP 1	
Имя сервера	16.113_5061
Имя сети	[2] 16.113 (eth0.100)
Порт	5061
Media	[1] 16.113 (порты 24000-30000)

c. Таблица SIP -интерфейсов будет иметь следующий вид:

№	Имя сервера	Имя сети	Интерфейс	Порт	Media
0	16.113_5061	16.113	eth0.1 (192.168.16.113)	5061	16.113 (порты 24000-30000)
1	20.120_5062	20.120	eth0.2 (192.168.20.120)	5062	20.120 (порты 24000-30000)

4. Конфигурирование SIP Trunk (меню **Конфигурация SBC/SIP Trunk**)

a. Добавить SIP Trunk.

В поле «Сервер приема» выбрать SIP-интерфейс в направлении абонента (20.120_5060), для сервера передачи выбрать SIP-интерфейс в направлении Softswitch (16.120_5060), в полях «IP- адрес назначения» и «Порт назначения» указать адрес и порт, используемые для сигнализации на softswitch (ip адрес 192.168.20.113 порт 5060), тип выбираем абонентский, если абоненты находятся за NAT включаем флаг абоненты за NAT, выставляем время хранения соединения на NAT.

SIP Trunk 0	
Сервер приема	[1] 20.120_5062
Сервер передачи	[0] 16.113_5061
IP адрес назначения	192.168.16.65
Порт назначения	5060
Тип	Абоненты
Абоненты за NAT	<input checked="" type="checkbox"/>
Время хранения соединения на NAT, с	100



Необходимо учитывать, что маршрут является *однаправленным*, вызовы могут осуществляться только со стороны *Сервера приема*. Для того чтобы вызовы могли проходить в обе стороны, необходимо дополнительно создать маршрут в обратном направлении. Исключением является случай с зарегистрированным абонентом. В этом случае созданное правило используется для осуществления регистрации на регистраторе и для исходящих вызовов от абонента, а динамическое правило будет использоваться для входящих вызовов к абоненту, то есть в данном случае встречное правило создавать нет необходимости.

b. Таблица SIP –транков будет иметь следующий вид:

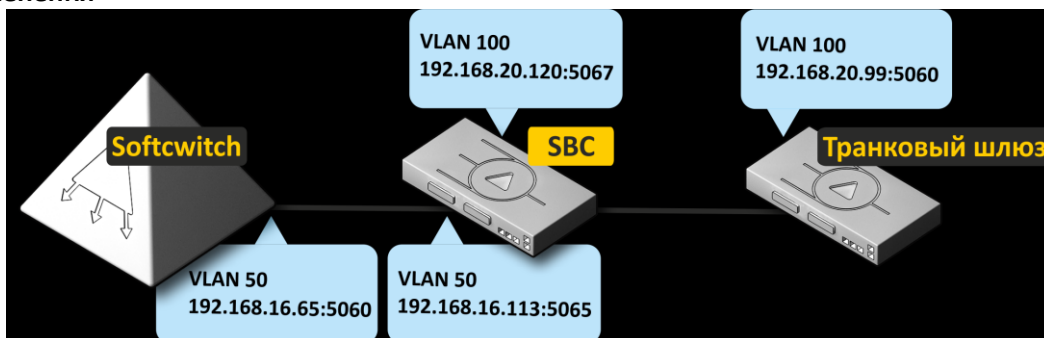
№	Сервер приема	Сервер передачи	IP адрес назначения	Порт назначения	Тип	Абоненты за NAT	Время хранения соединения на NAT, с
0	20.120_5062	18.113_5081	192.168.16.65	5060	Абоненты	*	100

Добавить Редактировать Удалить

5. Для применения настроек сохранить конфигурацию во flash (**Сервис/сохранить конфигурация во FLASH**) и перезапустить устройство.

2. Настройки SBC-1000 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

См. раздел **1 Настройка SBC-1000 для SIP абонентов** данного Приложения.

2. Конфигурирование медиа для SIP-интерфейсов

См. раздел **1 Настройка SBC-1000 для SIP абонентов** данного Приложения.

3. Конфигурирование SIP-интерфейсов (меню **Конфигурация SBC/SIP**)

a. Добавить SIP-интерфейс в направлении транкового шлюза.

Параметры интерфейса:

*сетевой интерфейс 20.120;
порт для сигнализации – 5067;
медиа – 20.120.*

SIP 2	
Имя сервера	20.120_5067
Имя сети	[1] 20.120 (eth0:1)
Порт	5067
Media	[0] 20.120 (порты 24000-30000)

Применить Отменить

b. Добавить SIP-интерфейс в направлении Softswitch.

Параметры интерфейса:

*сетевой интерфейс 16.113;
порт для сигнализации – 5065;
медиа – 16.113.*

SIP 3	
Имя сервера	16.113_5065
Имя сети	[2] 16.113 (eth0.100)
Порт	5065
Media	[1] 16.113 (порты 24000-30000)

c. Таблица SIP -интерфейсов будет иметь следующий вид:

№	Имя сервера	Имя сети	Интерфейс	Порт	Media
0	16.113_5061	16.113	eth0:1 (192.168.16.113)	5061	16.113 (порты 24000-30000)
1	20.120_5062	20.120	eth0:2 (192.168.20.120)	5062	20.120 (порты 24000-30000)
2	20.120_5067	20.120	eth0:2 (192.168.20.120)	5067	20.120 (порты 24000-30000)
3	16.113_5065	16.113	eth0:1 (192.168.16.113)	5065	16.113 (порты 24000-30000)

4. Конфигурирование SIP транков (меню **Конфигурация SBC/SIP Trunk**)

a. Добавить SIP Trunk в направлении транкового шлюза.

SIP Trunk 1	
Сервер приема	[3] 16.113_5065
Сервер передачи	[2] 20.120_5067
IP адрес назначения	192.168.20.99
Порт назначения	5060
Тип	SIP trunk
Абоненты за NAT	<input type="checkbox"/>
Время хранения соединения на NAT, с	0

b. Добавить SIP Trunk в направлении Softswitch.

SIP Trunk 2	
Сервер приема	[2] 20.120_5067
Сервер передачи	[3] 16.113_5065
IP адрес назначения	192.168.16.65
Порт назначения	5060
Тип	SIP trunk
Абоненты за NAT	<input type="checkbox"/>
Время хранения соединения на NAT, с	0



Необходимо учитывать, что маршрут является **однаправленным**, вызовы могут осуществляться только со стороны **Сервера приема**. Для того чтобы вызовы могли проходить в обе стороны, необходимо дополнительно создать маршрут в обратном направлении. Исключением является случай с зарегистрированным абонентом. В этом случае созданное правило используется для осуществления регистрации на регистраторе и для исходящих вызовов от абонента, а динамическое правило будет использоваться для входящих вызовов к абоненту, то есть в данном случае встречное правило создавать нет необходимости.

с. Таблица SIP–транков будет иметь следующий вид:

№	Сервер приема	Сервер передачи	IP адрес назначения	Порт назначения	Тип	Абоненты за NAT	Время хранения соединения на NAT, с
0	20.120_5062	16.113_5061	192.168.16.65	5060	Абоненты	+	100
1	16.113_5065	20.120_5067	192.168.20.99	5060	SIP trunk	-	-
2	20.120_5067	16.113_5065	192.168.16.65	5060	SIP trunk	-	-

- Для применения настроек сохранить конфигурацию во flash (**Сервис/сохранить конфигурация во FLASH**)и перезапустить устройство.

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Для получения технической консультации по вопросам эксплуатации оборудования ООО «Предприятие «Элтекс» Вы можете обратиться в Сервисный центр компании:

Российская Федерация, 630020, г. Новосибирск, ул. Окружная, дом 29 в.

Телефон:

+7(383)274-47-88

+7(383) 274-47-87

+7(383) 272-83-31

E-mail: techsupp@eltex.nsk.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:

<http://eltex.nsk.ru>

<http://eltex.nsk.ru/support/documentations>

<http://eltex.nsk.ru/forum>

<http://eltex.nsk.ru/database>

<http://eltex.nsk.ru/interaktivnyi-zapros>