Цифровые шлюзы

SMG-1016M, SMG-2016, SMG-3016 (SIGTRAN)

Руководство по эксплуатации

Версия ПО 1.6.1

Содержание

1 Введение 8

2 Список изменений 9

3 Описание изделий SMG (SIGTRAN) 10

3.1 Назначение 10

3.2 Типовые схемы применения 11

3.2.1 Сопряжение сигнализаций и медиапотоков TDM- и VoIP-сетей 11

3.3 Структура и принцип работы изделия 12

3.3.1 Структура SMG-1016M 12

3.3.2 Структура SMG-2016 14

3.3.3 Структура SMG-3016 14

3.3.4 Принцип работы SMG 15

3.4 Основные технические параметры 16

3.5 Конструктивное исполнение 20

3.5.1 SMG-1016M 20

3.5.2 SMG-2016 21

3.5.3 SMG-3016 23

3.6 Световая индикация 26

3.6.1 Световая индикация устройства в рабочем состоянии 26

3.6.1.1 SMG-1016M 26

3.6.1.2 SMG-2016 27

3.6.1.3 SMG-3016 27

3.6.2 Световая индикация состояния потоков E1 29

3.6.3 Световая индикация интерфейсов Ethernet 1000/100 30

3.6.4 Световая индикация при загрузке и сбросе к заводским настройкам 30

3.6.4.1 SMG-1016M 30

3.6.4.2 SMG-2016, SMG-3016 31

3.6.5 Световая индикация аварий 31

3.7 Использование функциональной кнопки «F» 32

3.8 Сохранение заводской конфигурации 32

3.9 Восстановление пароля 33

3.9.1 Восстановление пароля CLI 33

3.9.2 Восстановление пароля web 33

3.10 Комплект поставки 35

3.10.1 SMG-1016M 35

3.10.2 SMG-2016 35

3.10.3 SMG-3016 35

3.11 Инструкции по технике безопасности 36

3.11.1 Общие указания 36
3.11.2 Требования электробезопасности 36
3.11.3 Меры безопасности при наличии статического электричества 36
3.11.4 Требования к электропитанию 36
3.11.4.1 Требования к виду источника электропитания 36
3.11.4.2 Требования к допустимым изменениям напряжения источника питания постоянного тока 37
3.11.4.3 Требования к допустимым помехам источника электропитания постоянного тока 37
3.11.4.4 Требования к помехам, создаваемым оборудованием в цепи источника электропитания 37
3.11.4.5 Требования к источнику питания переменного тока 38
3.12 Установка SMG 38
3.12.1 Порядок включения 38
3.12.2 Крепление кронштейнов 39
3.12.3 Установка устройства в стойку 39
3.12.4 Установка модулей питания 41
3.12.5 Вскрытие корпуса 41
3.12.6 Установка субмодулей 44
3.12.7 Установка блоков вентиляции 48
3.12.8 Установка SSD-накопителей для SMG-1016M 50
3.12.9 Установка SATA-дисков для SMG-2016, SMG-3016 51
3.12.10 Замена батарейки часов реального времени 52
4 Общие рекомендации при работе со шлюзами SMG (SIGTRAN) 54
5 Конфигурирование устройств SMG (SIGTRAN) 55
5.1 Настройка SMG (SIGTRAN) через web-конфигуратор 55
5.1.1 Системные параметры 59
5.1.2 Мониторинг 64
5.1.2.1 Телеметрия 64
5.1.2.2 Мониторинг потоков E1 66
5.1.2.3 Мониторинг каналов E1 68
5.1.2.4 График загрузки процессора 70
5.1.2.5 Мониторинг SFP-модулей 71
5.1.2.6 Мониторинг front-портов коммутатора 71
5.1.2.7 Мониторинг VoIP-субмодулей 73
5.1.2.8 Сигнализация об авариях. Журнал аварийных событий 75
5.1.2.9 Мониторинг интерфейсов 78
5.1.2.10 Информация о накопителях 78
5.1.2.11 Мониторинг SIGTRAN 79
5.1.2.12 Мониторинг H.248/Megaco 79

5.1.3 Источники синхронизации ... 79
5.1.4 Потоки E1 ... 81
5.1.4.1 Выбор протокола сигнализации ... 81
5.1.4.2 Настройка физических параметров ... 81
5.1.4.3 Настройка протокола M2UA/IUA/Media gateway ... 82
5.1.4.4 Настройка протокола сигнализации COPM ... 86
5.1.5 План нумерации ... 88
5.1.5.1 Работа с префиксами в плане нумерации ... 88
5.1.5.2 Описание маски номера и ее синтаксис ... 89
5.1.6 Настройки SIGTRAN ... 91
5.1.7 Настройки медиа-интерфейсов ... 94
5.1.7.1 Интерфейсы MGCP ... 94
5.1.7.1.1 Конфигурация ... 94
1 Вкладка «Настройка MGCP» ... 95
2 Вкладка «Настройка кодеков RTP» ... 96
3 Вкладка «Настройка факса и передача данных» ... 99
5.1.7.2 Интерфейс H.248/Megaco ... 102
5.1.7.2.1 Вкладка «Настройка интерфейса H.248» ... 102
5.1.7.2.2 Вкладка «Настройка кодеков/RTP» ... 103
5.1.7.2.3 Вкладка «Настройка факса» ... 104
5.1.8 Внутренние ресурсы ... 105
5.1.8.1 Группы линий ОКС-7 ... 105
5.1.8.2 Таблица модификаторов ... 106
5.1.8.2.1 Вкладка «Отбор номера» ... 107
5.1.8.2.2 Вкладка «Модификация номера» ... 107
5.1.8.2.3 Синтаксис правила модификации ... 107
5.1.9 Настройки TCP/IP ... 108
5.1.9.1 Таблица маршрутизации ... 109
5.1.9.2 Сетевые параметры ... 110
5.1.9.3 Сетевые интерфейсы ... 110
5.1.9.4 Диапазон RTP-портов ... 112
5.1.10 Сетевые сервисы ... 114
5.1.10.1 NTP ... 114
5.1.10.2 Настройки SNMP ... 114
5.1.10.3 SNMPv3 ... 116
5.1.10.4 Настройка трапов (SNMP trap) ... 116
5.1.10.5 FTP-сервер ... 117
5.1.11 Коммутатор ... 118
5.1.11.1 Настройки LACP ... 118
5.1.11.2 Настройка портов коммутатора ... 119

5.1.11.3 802.1q ... 122
5.1.11.4 QoS и контроль полосы пропускания ... 123
5.1.11.5 Распределение приоритетов ... 125
5.1.12 Сетевые утилиты ... 125
5.1.12.1 PING ... 125
5.1.12.2 TRACEROUTE ... 128
5.1.13 Безопасность ... 129
5.1.13.1 Настройка SSL/TLS ... 129
5.1.13.2 Динамический брандмауэр ... 130
5.1.13.3 Журнал заблокированных адресов ... 131
5.1.13.4 Статический брандмауэр ... 131
5.1.13.5 Список разрешенных IP-адресов ... 134
5.1.14 Трассировки ... 135
5.1.14.1 PCAP-трассировки ... 135
5.1.14.2 PBX трассировки ... 139
5.1.14.2.1 Вкладка "Основные трассировки" ... 139
5.1.14.2.2 Вкладка "Продвинутые трассировки" ... 140
5.1.14.3 Настройки syslog ... 140
5.1.15 Работа с объектами и меню «Объекты» ... 142
5.1.16 Сохранение конфигурации и меню «Сервис» ... 142
5.1.17 Настройка даты и времени ... 143
5.1.18 Обновление ПО через web-конфигуратор ... 143
5.1.19 Лицензии ... 143
5.1.20 Меню «Помощь» ... 144
5.1.21 Установка пароля для доступа через web-конфигуратор ... 144
5.1.22 Просмотр заводских параметров и информации о системе ... 145
5.1.23 Выход из конфигуратора ... 146
5.2 Настройка SMG (SIGTRAN) с помощью командной строки ... 146
5.2.1 Команды трассировки, доступные через отладочный порт ... 148
5.2.1.1 Глобальное включение отладки ... 148
5.2.1.2 Глобальное выключение отладки ... 148
5.2.1.3 Включение/выключения отладки для определенных аргументов ... 148
5.3 Настройка SMG (SIGTRAN) через Telnet, SSH и RS-232 ... 149
5.3.1 Перечень команд CLI ... 149
5.3.2 Смена пароля для доступа к устройству через CLI ... 151
5.3.3 Режим управления ... 152
5.3.3.1 Режим управления линком M2UA ... 152
5.3.4 Режим конфигурирования общих параметров устройства ... 153
5.3.4.1 Режим конфигурирования параметров SIGTRAN ... 154

5.3.4.2 Режим конфигурирования параметров сервера приложений AS 155
5.3.4.3 Режим конфигурирования параметров процессов сервера приложений ASP 156
5.3.4.4 Режим конфигурирования параметров процессов сигнального шлюза 158
5.3.4.5 Режим конфигурирования параметров плана нумерации 159
5.3.4.5.1 Режим конфигурирования префикса 159
5.3.4.5.2 Режим редактирования масок префикса 160
5.3.4.6 Режим конфигурирования параметров потока E1 161
5.3.4.6.1 Режим конфигурирования параметров сигнализации CORM 163
5.3.4.6.2 Режим конфигурирования параметров сигнализации M2UA 164
5.3.4.6.3 Режим конфигурирования параметров сигнализации IUA 165
5.3.4.7 Режим конфигурирования параметров линксетов ОКС-7 167
5.3.5 Режим конфигурирования таблицы модификаторов 168
5.3.6 Режим конфигурирования параметров firewall 170
5.3.7 Режим конфигурирования сетевых параметров 173
5.3.7.1 Режим конфигурирования параметров DHCP-сервера 179
5.3.7.2 Режим конфигурирования PPTP-клиента 181
5.3.7.3 Режим конфигурирования протокола NTP 183
5.3.7.4 Режим конфигурирования протокола SNMP 184
6 Приложения SMG (SIGTRAN) 186
6.1 Приложение А. Назначение контактов разъёмов кабеля 186
6.1.1 Для SMG-2016, 3016 186
6.1.2 Для SMG-1016M 188
6.1.3 Таблицы соответствия цвета провода и контакта разъема E1 Line 189
6.2 Приложение Б. Резервное обновление встроенного ПО 190
6.2.1 Резервное обновление встроенного ПО устройства через RS-232 190
6.2.2 Резервное обновление встроенного ПО устройства с USB-Flash накопителя 193
6.3 Приложение В. Взаимодействие устройства с системами мониторинга 194
6.4 Приложение Г. Управление и мониторинг по протоколу SNMP 196
6.5 Приложение Д. Обеспечение функций CORM 202
6.5.1 Расчет необходимого числа субмодулей при использовании CORM 202
6.5.2 Логика работы постановки на контроль и перехватов вызовов CORM 203
6.5.3 Методика настройки медиашлюза SMG для сдачи протокола CORM в соответствии с Приказом Минкомсвязи РФ от 19.11.2012 №268 204
6.5.4 Обозначения и коды аварий 205
6.5.5 Причины отказа приёма и невыполнения команд 206
6.6 Приложение Е. Рекомендации по безопасности 208
6.6.1 Смена паролей на web и CLI 208
6.6.2 Создание ограниченных учётных записей 209

6.6.3 Ограничение доступа к интерфейсам сигнализации и управления 209
6.6.4 Настройка статического брандмауэра 210
6.6.5 Настройка динамического брандмауэра 211

1 Введение

В мире интенсивно развиваются средства связи, эксплуатирующие самые современные аппаратные и программные решения. При этом возникает проблема внедрения новых устройств связи, использующих другие принципы передачи информации, в существующие сети связи. Решение состоит в применении специального оборудования, связывающего разнородные участки сети связи в единое целое. Таким оборудованием в настоящий момент являются цифровые шлюзы. Их наличие позволяет проводить постепенный переход от существующей сети связи на сети связи, имеющие более эффективную реализацию, но работающую по другим принципам.

На данный момент наиболее эффективными сетями являются IP-сети, которые слабо зависят от среды передачи данных и от типа данных, вместе с тем являются наиболее гибкими и управляемыми. Для сопряжения традиционных сетей связи, в основе которых лежит принцип коммутации каналов, с сетями связи, использующими для передачи информации IP-сети, предназначен цифровой шлюз SMG, разработанный и производимый предприятием «ЭЛТЕКС».

Данное руководство содержит сведения об основных свойствах SMG-1016M, SMG-2016 и SMG-3016. В документе приведены технические характеристики шлюза и его компонентов. Также представлена вводная информация о порядке эксплуатации и обслуживания с использованием программного обеспечения.

Примечания и предупреждения

Примечания содержат важную информацию, советы или рекомендации по использованию и настройке устройства.

Предупреждения информируют пользователя о ситуациях, которые могут нанести вред устройству или человеку, привести к некорректной работе устройства или потере данных.

2 Список изменений

Версия ПО SMG-1016M: V.1.6.1 **Версия ПО SMG-2016: V.1.6.1** **Версия ПО SMG-3016: V.1.6.1**			
Версия документа	**Версия ПО**	**Дата выпуска**	**Содержание изменений**
Версия 5.0	v.1.6.1	27.10.2023	Изменено: • Добавлена работа по порту OOB для SMG-3016
Версия 4.0	v.1.6.0	31.03.2023	Добавлено: • Полупостоянные соединения каналов потока E1 • Режим кодирования compact text для сообщений протокола H.248/Megaco • Мониторинг каналов для MGCP и H.248/Megaco • Авария при потере связи с контроллером медиашлюзов H.248/Megaco • Мониторинг подключения к контроллеру медиашлюзов H.248/Megaco • SCTP транспорт для протокола H.248/Megaco • Поддержка платформы SMG-3016
Версия 3.0	v.1.3.0	15.10.2018	Добавлено: • Функциональность СОРМ
Версия 2.0	v.1.2.1	16.04.2018	Изменено: • Убраны функции TDM • Исправлены настройки прав доступа для пользователей web-интерфейса Добавлено: • Добавлена поддержка Basic continuity package для протокола H.248/Megaco
Версия 1.0	v.1.1.1	18.10.2017	Первая публикация

3 Описание изделий SMG (SIGTRAN)

3.1 Назначение

Цифровые шлюзы SMG-1016M, SMG-2016 и SMG-3016 предназначены для сопряжения сигнализаций и медиапотоков ТфОП (E1) и VoIP-сетей, а также для работы в качестве медиашлюза (конвертация кодеков, организация конференц-связи, прием и генерация тональных сигналов и DTMF, выдача речевых сообщений).

Количество трактов E1, поддерживаемых SMG, может достигать 16, количество разговорных (медиа) каналов со стороны E1 – до 496, со стороны VoIP – до 496.

Субмодульная конструкция шлюза позволяет гибко изменять емкость, а минимальное количество типов модулей упрощает расширение и модернизацию системы.

SMG является оптимальным надежным решением для задач обновления, построения и миграции телекоммуникационной инфраструктуры из ТфОП в NGN.

Основные характеристики SMG:

- количество интерфейсов E1 от 4 до 16 с шагом 4;
- до 496 каналов VoIP (128 каналов для подключения в TDM на один субмодуль);
- количество Ethernet-портов для SMG-1016M:
  - 3 порта 10/100/1000BASE-T;
  - 2 порта 1000-BASE-X (SFP).
- количество Ethernet-портов для SMG-2016:
  - 2 порта 10/100/1000BASE-T (RJ-45) / 1000BASE-X (SFP)
  - 2 порта 10/100/1000BASE-T (RJ-45)
- количество Ethernet-портов для SMG-3016:
  - 2 порта 10/100/1000BASE-T (RJ-45) / 1000BASE-X (SFP)
  - 2 порта 10/100/1000BASE-T (RJ-45)
- поддержка статического адреса и DHCP;
- DHCP-сервер;
- протоколы IP-телефонии MGCP[1], H.248/MEGACO, SIGTRAN (M2UA, IUA);
- протоколы канального уровня TDM: Q.921 (ISDN PRI), MTP2 (ОКС-7);
- протокол СОРМ [1];
- эхокомпенсация (рекомендация G.168);
- детектор речевой активности (VAD);
- генератор комфортного шума (CNG);
- адаптивный и фиксированный джиттер-буфер;
- передача данных: G.711 pass through;
- передача факса:
  - G.711 pass through;
  - T.38 UDP Real-Time Fax.
- поддержка NTP;
- поддержка DNS;
- поддержка SNMP;
- ограничение полосы и QoS для SMG-1016M;
- ToS и CoS для RTP и сигнализации;
- VLAN для RTP, сигнализации и управления;
- обновление ПО: через web-конфигуратор, CLI (Telnet, SSH, консоль (RS-232));
- конфигурирование и настройка (в том числе удаленно):
  - web-конфигуратор;
  - CLI (Telnet, SSH, консоль (RS-232)).
- удаленный мониторинг:
  - web-конфигуратор;

- SNMP.

---

[1]*При наличии лицензии.*

3.2 Типовые схемы применения

3.2.1 Сопряжение сигнализаций и медиапотоков TDM- и VoIP-сетей

В данной конфигурации устройство обеспечивает следующие возможности сопряжения:

- только сигнализаций (сигнальный шлюз SG);
- только медиапотоков (медиашлюз MG);
- одновременное сопряжение сигнализаций и медиапотоков (сигнальный и медиашлюз на одной платформе).

Сигнальный шлюз обеспечивает подключение до 16 сигнальных линков MTP2, Q.921 в потоках E1 и трансляции передаваемой в них информации в IP-сеть посредством протоколов M2UA, IUA соответственно, а также обратную трансляцию из IP в TDM-сеть. Медиашлюз обеспечивает передачу пользовательских данных (например, речевой информации) между TDM и IP-сетями. К медиашлюзу возможно подключить до 16 потоков E1, что позволяет шлюзу обслуживать до 496 пользовательских каналов без сжатия (кодек G.711) либо до 432 каналов со сжатием (G.729 A). Медиашлюз управляется контроллером медиашлюзов (MGC) посредством протокола сигнализации H.248/Megaco либо MGCP.

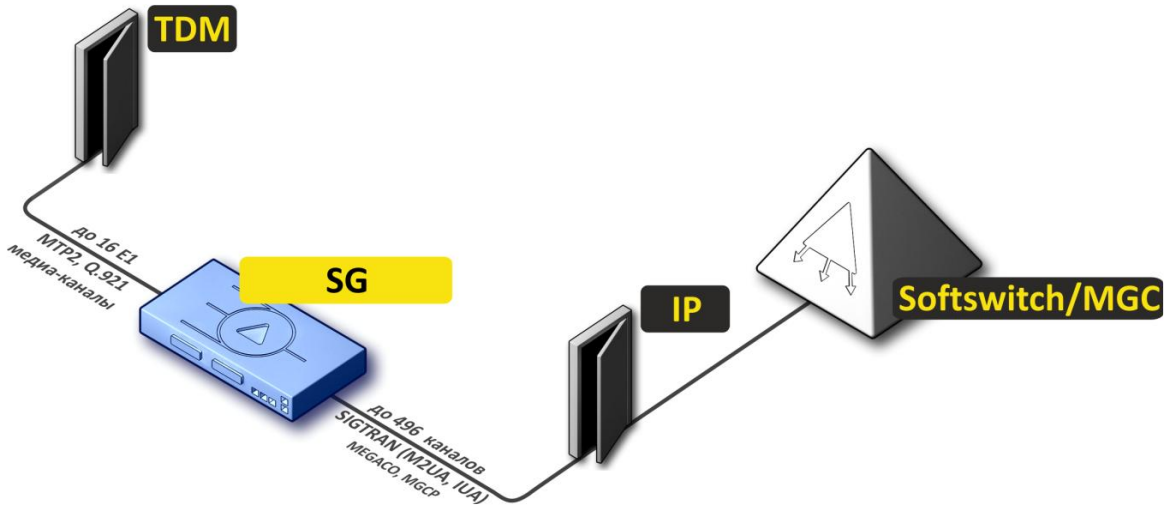


Рисунок 1 – Сопряжение сигнализаций и медиапотоков TDM- и VoIP-сетей

Взаимодействие сигнальных протоколов между TDM- и IP-сетями при использовании сигнального шлюза приведено на рисунке ниже. Сигнальный шлюз SG осуществляет взаимодействие на канальном уровне модели OSI, а сигнализации верхних уровней MTP3/ISUP и Q.931 пропускает прозрачно через себя.

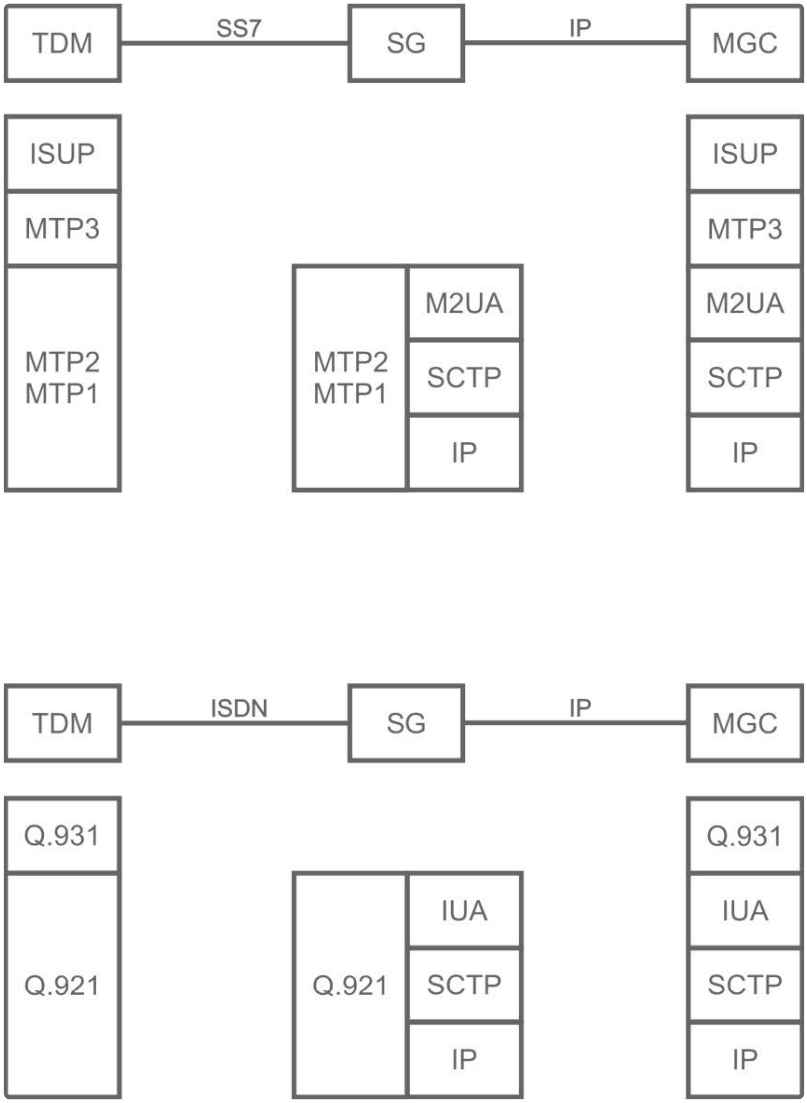


Рисунок 2 – Взаимодействие протоколов TDM- и IP-сетей через сигнальный шлюз SMG

3.3 Структура и принцип работы изделия

3.3.1 Структура SMG-1016M

Устройство SMG-1016M имеет субмодульную архитектуру и содержит следующие элементы:

- Контроллер, в состав которого входит:
  - Управляющий процессор;
  - Flash-память – 64 МБ;
  - ОЗУ – 512 МБ.
- До 4 субмодулей потоков E1 C4E1;
- До 6 субмодулей IP SM-VP-M300;
- Ethernet-коммутатор (L2) на 3 порта 10/100/1000BASE-T, 2 порта MiniGBIC (SFP);
- Матрица коммутации;
- Система ФАПЧ.

Функциональная схема SMG-1016M представлена на рисунке ниже.

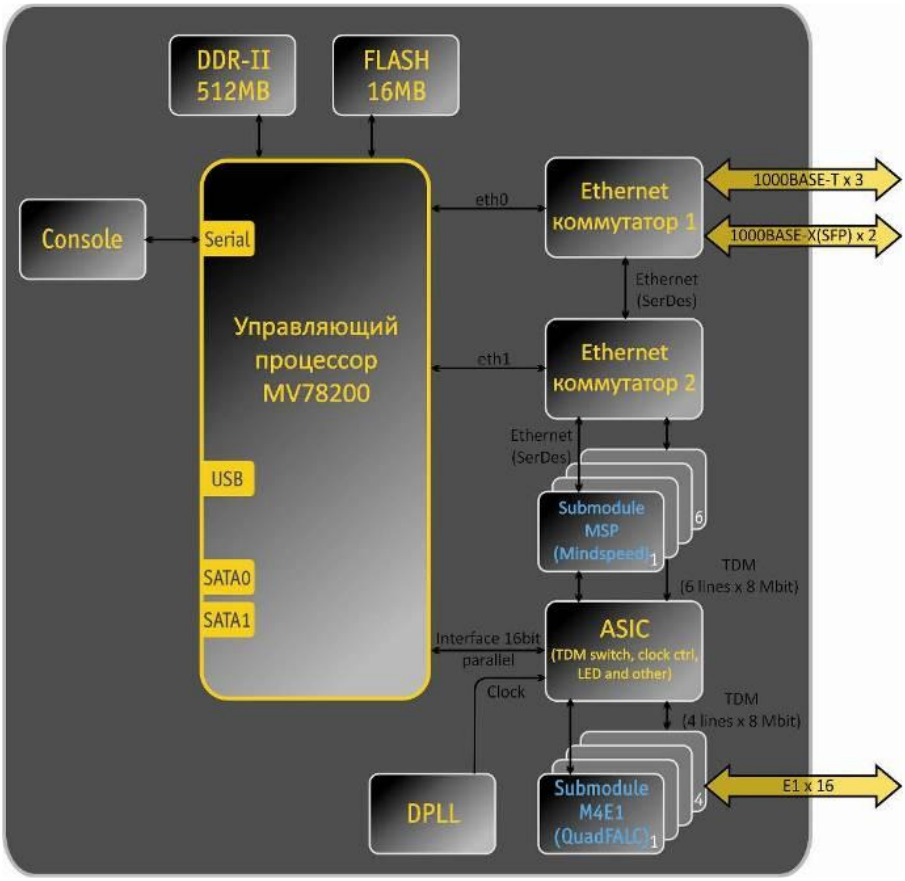


Рисунок 3 – Функциональная схема SMG-1016M

3.3.2 Структура SMG-2016

Устройство SMG-2016 имеет субмодульную архитектуру и содержит следующие элементы:

- Контроллер, в состав которого входит:
  - Управляющий процессор;
  - Flash память – 1024 МБ;
  - ОЗУ – 4096 МБ.
- До 4 субмодулей потоков E1 C4E1;
- До 6 субмодулей IP SM-VP-M300;
- Ethernet-коммутатор (L2) на 4 порта 10/100/1000BASE-T, 2 combo-порта MiniGBIC (SFP);
- Матрица коммутации;
- Система ФАПЧ.

Функциональная схема SMG-2016 представлена на рисунке ниже.

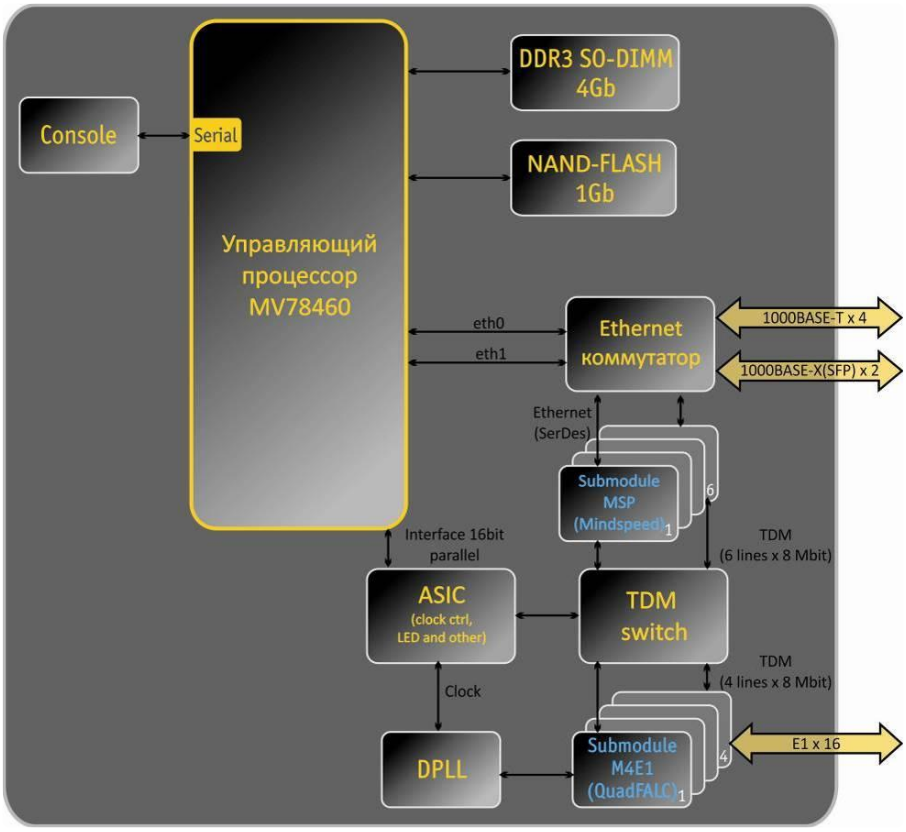


Рисунок 4 – Функциональная схема SMG-2016

3.3.3 Структура SMG-3016

Устройство SMG-3016 имеет субмодульную архитектуру и содержит следующие элементы:

- Контроллер, в состав которого входит:
  - Управляющий процессор;
  - ОЗУ – 8192 МБ.
- До 4 субмодулей потоков E1 C4E1;
- До 6 субмодулей IP SM-VP-M300;
- Ethernet-коммутатор (L2) на 4 порта 10/100/1000BASE-T, 2 combo-порта MiniGBIC (SFP);
- Матрица коммутации;
- Выделенный порт OOB;
- Система ФАПЧ.

Функциональная схема SMG-3016 представлена на рисунке ниже.

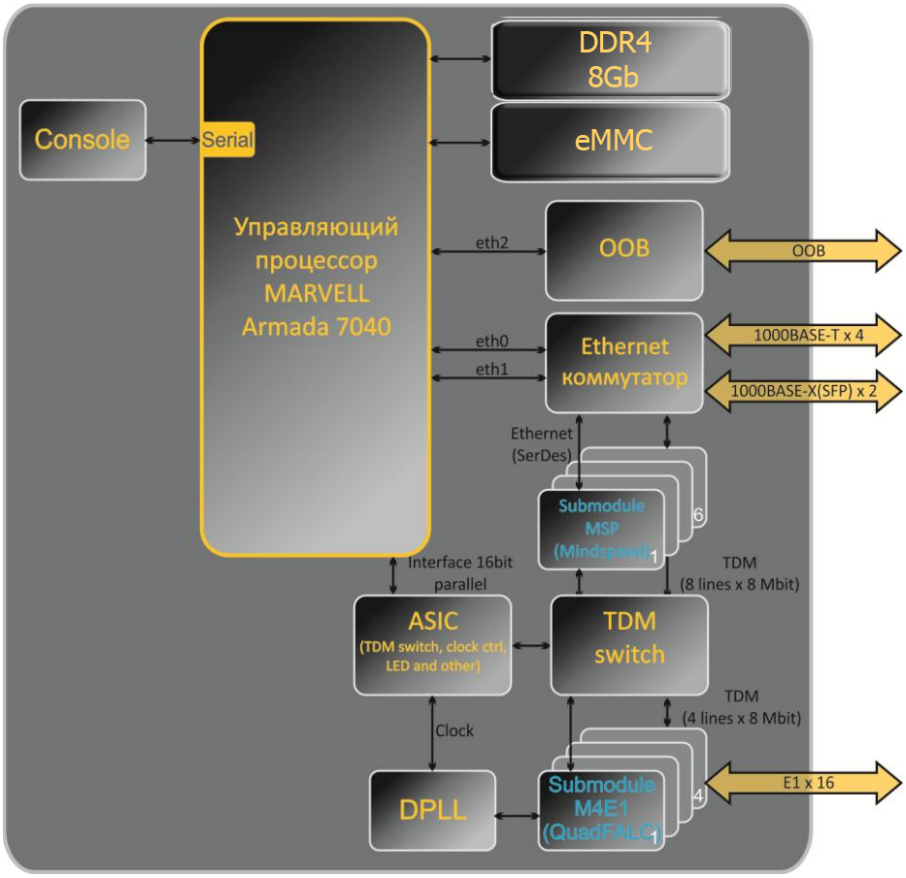


Рисунок 5 – Функциональная схема SMG-3016

3.3.4 Принцип работы SMG

В направлении TDM-IP сигнал, поступающий на потоки E1 через внутрисистемную магистраль, подается на аудиокодеки субмодулей VoIP (6 линий по 128 каналов TDM), кодируется по одному из выбранных стандартов и в виде цифровых пакетов поступает в Ethernet-коммутатор. В направлении IP-TDM цифровые пакеты из Ethernet-коммутатора передаются на субмодули VoIP, декодируются и через внутрисистемную магистраль передаются в потоки E1.

Внешние 2-мегабитные потоки E1 через согласующие трансформаторы поступают на фреймеры, при этом из потока выделяется сигнал синхронизации и выдается на общую линию синхронизации устройства. Управление приоритетностью линий синхронизации происходит на программном уровне, согласно заданному алгоритму.

Матрица коммутации входит в состав внутрисистемной магистрали и осуществляет связь между субмодулями E1 (C4E1) и субмодулями VoIP (SM-VP-M300).

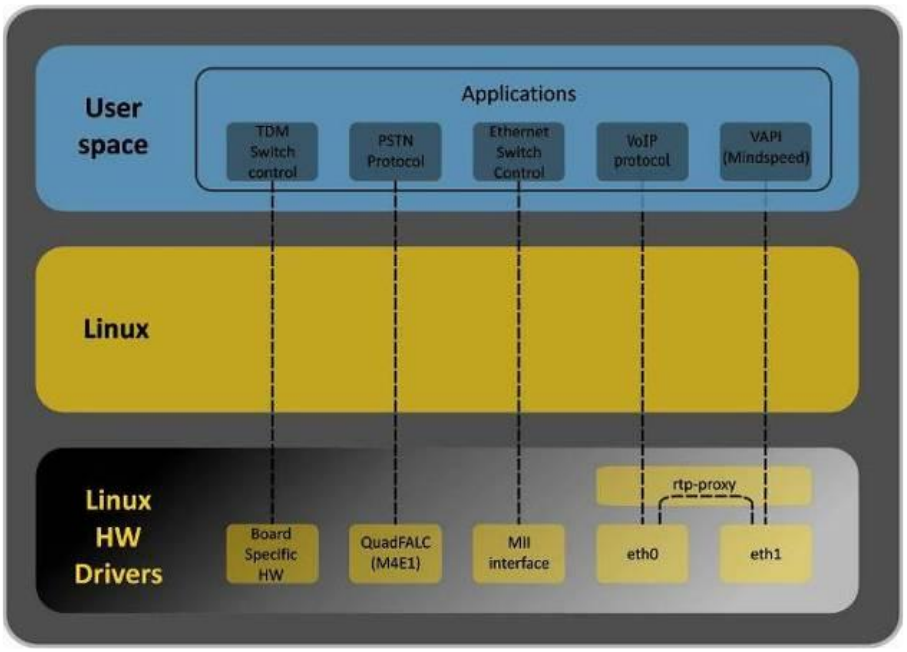


Рисунок 6 − Структура программного обеспечения SMG

Структура программного обеспечения устройства приведена на рисунке ниже.

3.4 Основные технические параметры

Основные технические параметры терминала приведены в таблице ниже.

Таблица 1 − Основные технические параметры

Протоколы VoIP

Поддерживаемые протоколы	MGCP[1] MEGACO SIGTRAN (M2UA, IUA, M3UA[2]) T.38

---

[1] *При наличии лицензии.*
[2] *В данной версии программного обеспечения не поддерживается.*

Аудиокодеки

Кодеки	G.711 (A/U) G.729 AB G.723.1 (6.3 Кбит/с, 5.3 Кбит/с) G.726 (32 Кбит/с) Полупостоянное соединение каналов потоков E1 без использования кодека

Количество VoIPканалов, поддерживаемых субмодулем, в зависимости от типа кодека

Кодек/время пакетизации, мс	Количество каналов
G.711 (A/U)/20-60 G.711 (A/U)/10 G.729 A/20-80 G.729 A/10 G.723.1 (6.3 Кбит/с, 5.3 Кбит/с) G.726/20 G.726/10 T.38	160 112 72 62 58 98 88 54
TDM-каналов на 1 субмодуль	128
Трехсторонних конференций на 1 субмодуль	27

Параметры электрического интерфейса Ethernet

Количество интерфейсов	SMG-1016M	SMG-2016, SMG-3016
	3	4
Электрический разъем	RJ-45	
Скорость передачи	Автоопределение, 10/100/1000 Мбит/с, дуплекс	
Поддержка стандартов	10/100/1000BASE-T	

Параметры оптического интерфейса Ethernet

Количество интерфейсов	SMG-1016M	SMG-2016, SMG-3016
	2	2 combo-порта
Оптический разъем	Mini-Gbic (SFP): 1. Дуплексные, двухволоконные с длиной волны 1310 нм (Single-Mode), 1000BASE-LX (коннектор LC), дальность – до 10 км, напряжение питания – 3,3 В 2. Дуплексные, одноволоконные с длинами волн на прием/передачу 1310/1550 нм, 1000BASE-LX (коннектор SC), дальность – до 10 км, напряжение питания – 3,3 В	
Скорость передачи	1000 Мбит/с, дуплекс	
Поддержка стандартов	1000BASE-X	

Параметры консоли

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

Параметры интерфейса E1

Число каналов	Согласно рекомендациям МСЭ-Т G.703,G.704
Скорость передачи данных в линии	2,048 Мбит/с
Линейный код	HDB3, AMI
Выходной сигнал из линии	3,0 В амплитудное на нагрузке 120 Ом 2,37 В амплитудное на нагрузке 75 Ом (по рекомендации МККТТ G.703)
Входной сигнал в линию	От 0 до -6 дБ по отношению к стандартному выходному импульсу
Эластичный буфер	Ёмкость 2 кадра
Протоколы сигнализации	Q.921, MTP2

Общие параметры

Рабочий диапазон температур		От 0 до +40 °C	
Относительная влажность		до 80 %	
Напряжение питания		Сеть переменного тока: 220 В+-20 %, 50 Гц Сеть постоянного тока: -48 В+30-20 % Варианты питания: • один источник питания постоянного или переменного тока; • два источника питания постоянного или переменного тока, с возможностью горячей замены.	
Источники питания		Сеть переменного тока	Сеть постоянного тока
Обозначение ИП		PM160-220/12	PM100-48/12
Мощность ИП		160 Вт	100 Вт
Потребляемая мощность		не более 50 Вт	
Габариты (Ш × В × Г)		SMG-1016M	SMG-2016, SMG-3016
		430 × 45 × 260 мм	430 × 45 × 340 мм
Конструктив		19" конструктив, типоразмер 1U	
Масса	Устройство в полной комплектации	SMG-1016M	SMG-2016, SMG-3016
		3,2 кг	5,3 кг
	БП	0,5 кг	
	Вентпанель	0,1 кг	
	SATA-накопитель[1]	0,1 кг	

[1] *Только для SMG-2016 и SMG-3016.*

-

3.5 Конструктивное исполнение

3.5.1 SMG-1016M

Цифровой шлюз SMG-1016M выполнен в металлическом корпусе с возможностью установки в 19" каркас типоразмером 1U.

Внешний вид передней панели устройства приведен на рисунке ниже.

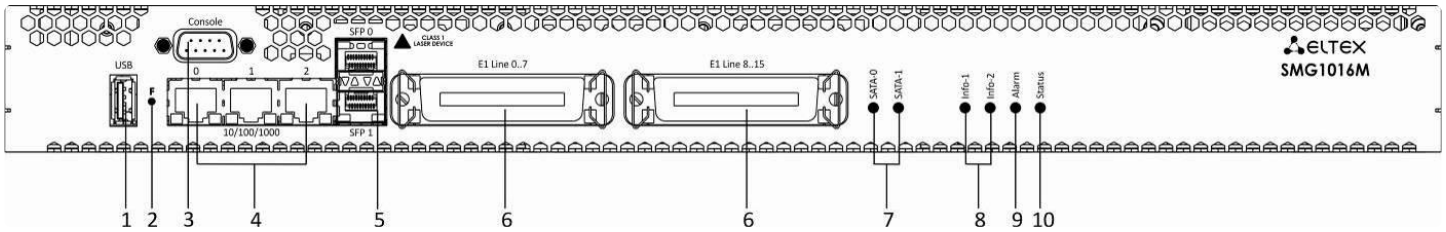


Рисунок 7 – Внешний вид передней панели SMG-1016M

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

Таблица 2 – Описание разъемов, индикаторов и органов управления передней панели SMG-1016M

№	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 (распайка разъемов приведена в Приложении А)
4	10/100/1000 0..2	3 разъема RJ-45 интерфейсов Ethernet 10/100/1000BASE-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 (распайка разъемов приведена в Приложении А)
Индикаторы		
7	SATA-0, SATA-1	Индикаторы работы интерфейсов SATA (в данной версии не используются)
8	Info 1, Info 2	Индикаторы работы оптических интерфейсов SFP
9	Alarm	Индикатор аварии устройства
10	Status	Индикатор работы устройства

Внешний вид задней панели устройства приведен на рисунке ниже.

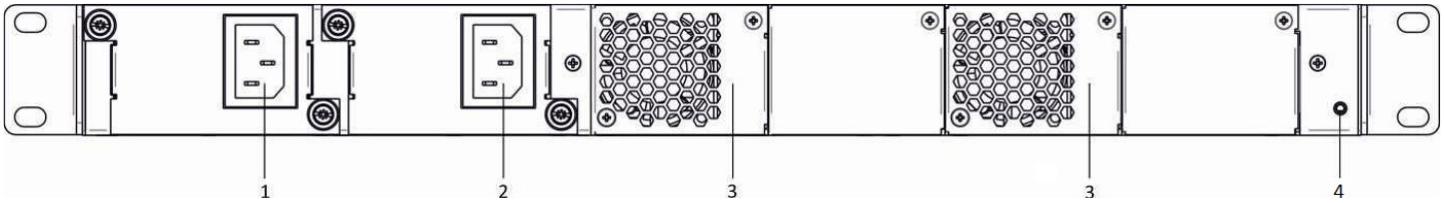


Рисунок 8 – Внешний вид задней панели SMG-1016M

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

Таблица 3 – Описание разъемов задней панели SMG-1016M

№	Элемент задней панели	Описание
1	Разъем питания	Разъем для подключения к источнику электропитания (Блок питания #0)
2	Разъем питания	Разъем для подключения к источнику электропитания (Блок питания #1)
3	Съемные вентиляторы	Съемные вентиляционные модули с возможностью горячей замены
4	Клемма заземления	Клемма для заземления устройства

3.5.2 SMG-2016

Цифровой шлюз SMG-2016 выполнен в металлическом корпусе с возможностью установки в 19" каркас типоразмером 1U.

Внешний вид передней панели устройства приведен на рисунке ниже.

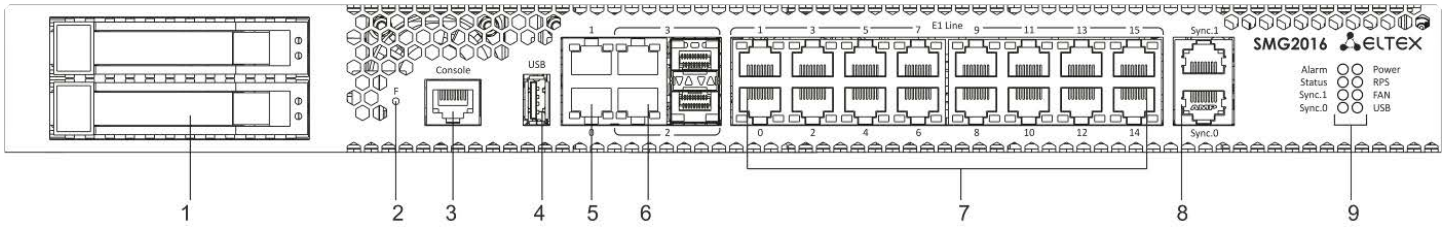


Рисунок 9 – Внешний вид передней панели SMG-2016

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

Таблица 4 – Описание разъемов, индикаторов и органов управления передней панели SMG-2016

№	Элемент передней панели	Описание
1	Разъемы SATA-дисков	Разъемы с салазками для установки SATA-дисков
2	F	Функциональная кнопка
3	Console	Консольный порт для локального управления устройством (распайка разъемов приведена в Приложении А)
4	USB	USB-порт для подключения внешнего накопителя
5	0, 1	2 разъема RJ-45 Ethernet 10/100/1000BASE-T Gigabit uplink для выхода в IP-сеть
6	2, 3	2 шасси для установки SFP-модулей 1000BASE-X uplink-интерфейса для выхода в IP-сеть
		2 разъема RJ-45 10/100/1000BASE-T Gigabit uplink-интерфейса для выхода в IP-сеть
7	E1 Line 0..15	16 разъемов RJ-48 для подключения потоков E1 (распайка разъемов приведена в Приложении А)
8	Sync.0, Sync.1	2 разъема RJ-45 для подключения источников внешней синхронизации
Индикаторы		
9	Alarm	Индикатор аварии устройства
	Status	Индикатор работы устройства
	Sync.1	Индикатор работы интерфейса внешней синхронизации Sync.2
	Sync.0	Индикатор работы интерфейса внешней синхронизации Sync.1

№	Элемент передней панели	Описание
	Power	Индикатор питания устройства
	RPS	Индикатор дополнительного питания устройства
	FAN	Индикатор работы вентиляторов
	USB	Индикатор работы USB

Внешний вид задней панели устройства приведен на рисунке ниже.

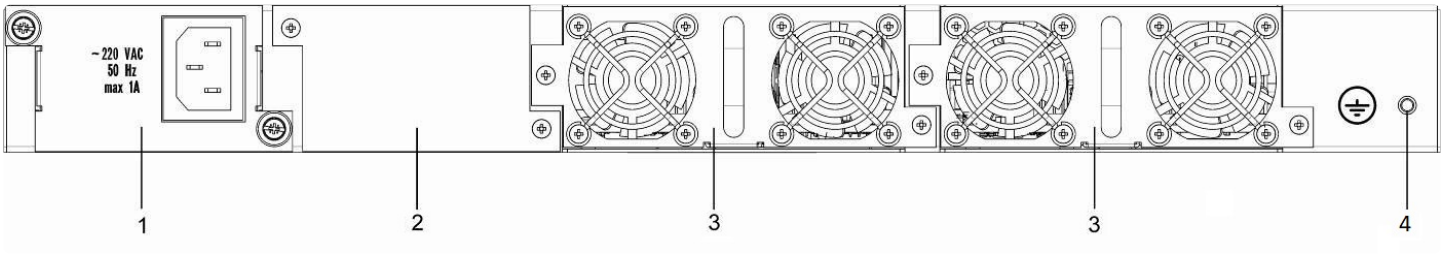


Рисунок 10 – Внешний вид задней панели SMG-2016

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

Таблица 5 – Описание разъемов задней панели SMG-2016

№	Элемент задней панели	Описание
1	Модуль питания	Модуль с разъемом для подключения к источнику электропитания (Блок питания #0)
2	Модуль питания	Модуль с разъемом для подключения к источнику электропитания (Блок питания #1)
3	Панели вентиляторов	Съемные вентиляционные модули с возможностью горячей замены
4	Клемма заземления	Клемма для заземления устройства

3.5.3 SMG-3016

Цифровой шлюз SMG-3016 выполнен в металлическом корпусе с возможностью установки в 19" каркас типоразмером 1U.

Внешний вид передней панели устройства приведен на рисунке ниже.

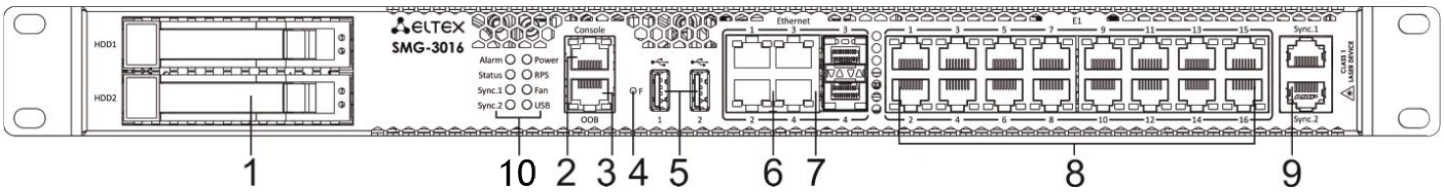


Рисунок 11 – Внешний вид передней панели SMG-3016

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

Таблица 6 – Описание разъемов, индикаторов и органов управления передней панели SMG-3016

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

Внешний вид задней панели устройства приведен на рисунке ниже.

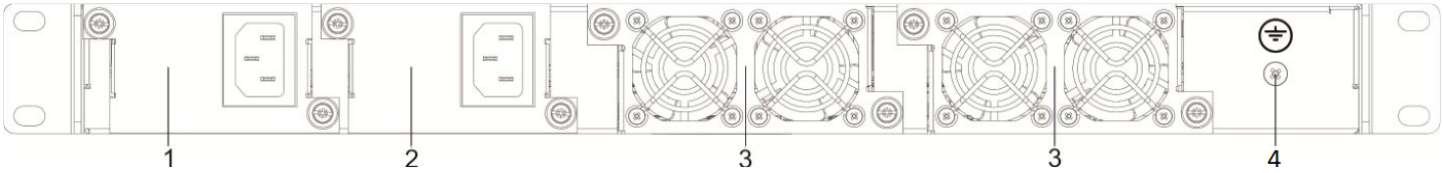


Рисунок 12 – Внешний вид задней панели SMG-3016

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

Таблица 7 – Описание разъемов задней панели SMG-3016

№	Элемент задней панели	Описание
1	Модуль питания	Модуль с разъемом для подключения к источнику электропитания (Блок питания #1)
2	Модуль питания	Модуль с разъемом для подключения к источнику электропитания (Блок питания #2)
3	Панели вентиляторов	Съемные вентиляционные модули с возможностью горячей замены
4	Клемма заземления 	Клемма для заземления устройства

3.6 Световая индикация

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

3.6.1 Световая индикация устройства в рабочем состоянии

3.6.1.1 SMG-1016M

Световая индикация устройства (рисунок 7) в рабочем состоянии приведена в таблице ниже.

Таблица 8 – Световая индикация состояния устройства в рабочем состоянии

№	Индикатор	Состояние индикатора	Состояние устройства
8	Info1 — индикатор работы оптических интерфейсов SFP	Не горит	Отсутствует линк SFP0
		Горит зеленым светом	Линк SFP0 в работе
	Info2 — индикатор работы оптических интерфейсов SFP	Не горит	Отсутствует линк SFP1
		Горит зеленым светом	Линк SFP1 в работе
		Горит красным светом	Загрузка устройства
9	Alarm — индикатор аварии устройства	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
10	Status — индикатор работы устройства	Горит зеленым светом	Нормальная работа
		Не горит	Нет питания устройства

3.6.1.2 SMG-2016

Световая индикация устройства (рисунок 9) в рабочем состоянии приведена в таблице ниже.

Таблица 9 – Световая индикация устройства в рабочем состоянии

№	Индикатор	Состояние индикатора	Состояние устройства
9	Alarm — индикатор аварии устройства	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 — индикатор работы устройства	Горит зеленым светом	Нормальная работа
		Не горит	Нет питания устройства
	Sync.0, Sync.1 — индикаторы работы интерфейса внешней синхронизации	Горит зеленым цветом	Синхронизация от внешнего источника
		Не горит	Внешний источник синхронизации не подключен
	Power — индикатор питания устройства	Горит зеленым цветом	Питание от блока питания #1
		Горит оранжевым цветом	Блок питания #1 установлен, питание на него не подается
	RPS — индикатор дополнительного питания устройства	Горит зеленым цветом	Блок питания #2 установлен, на него подается питание
		Горит красным цветом	Блок питания #2, питание на него не подается
		Не горит	Блок питания #2 не установлен
	FAN — индикатор работы вентиляторов	Горит зеленым цветом	Все модули съемных вентиляторов установлены, все вентиляторы в работе
		Горит оранжевым цветом	Все модули съемных вентиляторов установлены, присутствуют нерабочие вентиляторы
		Горит красным цветом	Один или оба модуля съемных вентиляторов не установлены
	USB — индикатор работы USB	Горит зеленым цветом	USB-flash установлена
		Не горит	USB-flash не установлена

3.6.1.3 SMG-3016

Световая индикация устройства (рисунок 11) в рабочем состоянии приведена в таблице ниже.

Таблица 10 – Световая индикация устройства в рабочем состоянии

№	Индикатор	Состояние индикатора	Состояние устройства
10	Alarm — индикатор аварии устройства	Мигает красным светом	Критическая авария на устройстве
		Горит красным светом	Некритическая авария на устройстве
		Горит желтым светом	Нет аварий, есть некритические замечания
		Горит зеленым светом	Нормальная работа
	Status — индикатор работы устройства	Горит зеленым светом	Нормальная работа
		Не горит	Нет питания устройства
	Sync.1, Sync.2 — индикаторы работы интерфейса внешней синхронизации	Горит зеленым цветом	Синхронизация от внешнего источника активна, идет захват синхронизации от источника
		Горит красным цветом	Синхронизация от внешнего источника активна, внешний источник не подключен (нет частоты в диапазоне)
		Горит оранжевым цветом	Синхронизация от внешнего источника не активна, внешний источник подключен (есть частота в диапазоне)
		Мигает оранжевым цветом	Режим вывода частоты
		Не горит	Внешний источник синхронизации не подключен
	Power — индикатор питания устройства	Горит зеленым цветом	Питание от Блока питания #1
		Горит оранжевым цветом	Блок питания #1 установлен, питание на него не подается
	RPS — индикатор дополнительного питания устройства	Горит зеленым цветом	Блок питания #2 установлен, на него подается питание
		Горит красным цветом	Блок питания #2, питание на него не подается
		Не горит	Блок питания #2 не установлен
	FAN — индикатор работы вентиляторов	Горит зеленым цветом	Все модули съемных вентиляторов установлены, все вентиляторы в работе
		Горит оранжевым цветом	Все модули съемных вентиляторов установлены, присутствуют нерабочие вентиляторы
		Горит красным цветом	Один или оба модуля съемных вентиляторов не установлены
	USB — индикатор работы USB	Горит зеленым цветом	USB-flash установлена
		Не горит	USB-flash не установлена

3.6.2 Световая индикация состояния потоков E1

Световая индикация состояния потоков E1[1] приведена в таблице ниже.

Таблица 8 – Индикация состояния потоков E1

0-15 Разъемы RJ-48	**Индикация (период мерцания)**		
Статус	**Красный**	**Желтый**	**зеленый**
E1 отключен в конфигурации шлюза	Не горит	Не горит	Не горит
Аварийное состояние потока E1	Мигает (200 мс)	Не горит	Не горит
Потеря сигнала (LoS)	Горит	Не горит	Не горит
Авария AIS	Горит	Мигает (200 мс)	Не горит
Авария LOF	Горит	Горит	Не горит
Авария LOMF	Горит	Горит	Не горит
Нормальная работа потока E1	Не горит	Не горит	Горит
Авария на удаленном конце (RAI)	Не горит	Мигает (200 мс)	Мигает (200 мс)
Поток E1 в работе, присутствуют проскальзывания на потоке (SLIP)	Не горит	Мигает (300 мс)	Мигает (1500 мс)
Идет тестирование потока E1	Мигает (200 мс)	Мигает (200 мс)	Мигает (200 мс)

[1] *Только для SMG-2016 и SMG-3016.*

3.6.3 Световая индикация интерфейсов Ethernet 1000/100

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

Таблица 9 – 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

3.6.4 Световая индикация при загрузке и сбросе к заводским настройкам

3.6.4.1 SMG-1016M

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

Таблица 10 – Световая индикация при загрузке и сбросе к заводским настройкам

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

Не рекомендуется удерживать нажатой кнопку «F» во время сброса устройства – это приведет к полной остановке устройства. Возобновление работы будет возможно только после сброса по питанию.
Возможен сброс к заводским настройкам на включаемом устройстве.
В этом случае пункт 1 необходимо пропустить.

3.6.4.2 SMG-2016, SMG-3016

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

Таблица 11 – Световая индикация при загрузке и сбросе к заводским настройкам

№	Индикация				Порядок сброса к настройкам по умолчанию (устройство включено)
	Alarm	Status	Sync.0	Sync.1	
1	Желтый	Желтый	Желтый	Желтый	Нажать и удерживать кнопку «F» в течение 1 секунды до появления данной комбинации. Через 3 секунды начнется перезагрузка устройства
2	Желтый	Красный	Желтый	Желтый	Начало сброса настроек к заводским. Данная комбинация светодиодов загорится в начале загрузки устройства
3	Зелёный	Зелёный	-	-	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 секунд
4	Желтый	Желтый	-	-	При появлении комбинации отпустить кнопку «F». Через некоторое время в консоль будет выведено сообщение: <<<BOOTING IN SAFE-MODE.RESTORING DEFAULT PARAMETERS>>> Сброс к заводским настройкам завершен

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

3.6.5 Световая индикация аварий

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

Таблица 12 – Индикация аварий

Состояние индикатора Alarm	Уровень аварии	Описание аварии
Мигает красным светом	Критическая (critical)	Ошибка конфигурации
		Потеря SIP-модуля
		Авария потока (при установленном флаге *Индикация Alarm* в меню *«Потоки E1/Физические параметры»*)
Горит красным светом	Некритическая (errors)	Потеря VoIP-субмодуля (MSP)
		Авария синхронизации (работа в режиме free-run)

Состояние индикатора Alarm	Уровень аварии	Описание аварии
Горит желтым светом	Предупреждения (warning)	Удаленная авария потока
		Синхронизация от менее приоритетного источника (более приоритетный недоступен)

3.7 Использование функциональной кнопки «F»

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

Порядок сброса к настройкам по умолчанию на включенном устройстве приведен в меню Световая индикация при загрузке и сбросе к заводским настройкам: таблица 10, таблица 11.

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

- через telnet либо console: логин **admin**, пароль **rootpasswd**;
- через web-конфигуратор: логин **admin**, пароль **rootpasswd**.

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

3.8 Сохранение заводской конфигурации

Для сохранения заводской конфигурации:

- произведите сброс устройства к заводским настройкам (меню Световая индикация при загрузке и сбросе к заводским настройкам);
- подключитесь через telnet либо console, используя логин **admin**, пароль **rootpasswd**;
- введите команду **`sh`** (устройство выйдет из режима CLI в режим SHELL);
- введите команду **`save`**;
- перезагрузите устройство командой `reboot`.

Шлюз загрузится с заводской конфигурацией.

```
*******************************************
*        Welcome to SMG-1016M               *
*******************************************
smg login: admin
Password: rootpasswd

*******************************************
*           Welcome to  SMG-1016M           *
*******************************************
Welcome! It is Wed Mar 11 08:45:20 NOVT 2015
SMG> sh
/home/admin # save
tar: removing leading '/' from member names
**********
**********
***Saved successful
New image 1
Restored successful
/home/admin #
# reboot
```

3.9 Восстановление пароля

3.9.1 Восстановление пароля CLI

Для восстановления пароля:

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

Шлюз загрузится с текущей конфигурацией и новым паролем.

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

```
*****************************************
*        Welcome to SMG-1016M             *
*****************************************

smg login: admin
Password: rootpasswd

*****************************************
*           Welcome to  SMG-1016M         *
*****************************************

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

3.9.2 Восстановление пароля web

Для восстановления пароля:

- произведите сброс устройства к заводским настройкам (раздел Световая индикация при загрузке и сбросе к заводским настройкам);

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

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

Шлюз загрузится с текущей конфигурацией и новым паролем.

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

```
*****************************************
*        Welcome to SMG-1016M             *
*****************************************

smg login: admin
Password: rootpasswd

*****************************************
*           Welcome to  SMG-1016M         *
*****************************************

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

На этом этапе производится смена пароля из web.

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

3.10 Комплект поставки

3.10.1 SMG-1016M

В базовый комплект поставки устройства SMG-1016M входят:

- Цифровой шлюз SMG-1016M;
- Разъем CENC-36M – 2 шт. (при отсутствии в заказе кабеля UTP CAT5E 18 пар);
- Защелки на разъемы CENC-36M – 4 шт. (при отсутствии в заказе кабеля UTP CAT5E 18 пар);
- Кабель соединительный RS-232 DB9(F) – DB9(F);
- Комплект крепления в 19" стойку;
- Памятка о документации;
- Паспорт;
- Декларация соответствия;
- Руководство по эксплуатации на CD-диске (опционально).

3.10.2 SMG-2016

В базовый комплект поставки устройства SMG-2016 входят:

- Цифровой шлюз SMG-2016;
- Комплект крепления в 19" стойку;
- Памятка о документации;
- Паспорт;
- Декларация соответствия;
- Руководство по эксплуатации на CD-диске (опционально).

3.10.3 SMG-3016

В базовый комплект поставки устройства SMG-3016 входят:

- Цифровой шлюз SMG-3016;
- Комплект крепления в 19" стойку;
- Памятка о документации;
- Паспорт;
- Декларация соответствия;
- Руководство по эксплуатации на CD-диске (опционально).

3.11 Инструкции по технике безопасности

3.11.1 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.

Подключать к устройству только годное к применению вспомогательное оборудование.

Цифровой шлюз 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 $6{,}0\times10^4$ до $10{,}7\times10^4$ Па (от 450 до 800 мм рт. ст.).

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

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

3.11.2 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 1 В.

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 субмодулей должна осуществляться только при выключенном питании, следуя указаниям раздела Установка модулей питания.

3.11.3 Меры безопасности при наличии статического электричества

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

3.11.4 Требования к электропитанию

3.11.4.1 Требования к виду источника электропитания

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

3.11.4.2 Требования к допустимым изменениям напряжения источника питания постоянного тока

Изменения напряжения источника питания с напряжением 48 В допускаются в пределах от 36 до 72 В.

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

3.11.4.3 Требования к допустимым помехам источника электропитания постоянного тока

Оборудование должно нормально функционировать при помехах источника электропитания, не превышающих значения, приведенные в таблице ниже.

Таблица 13 – Требования к допустимым помехам источника электропитания постоянного тока

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

3.11.4.4 Требования к помехам, создаваемым оборудованием в цепи источника электропитания

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

Таблица 14 – Требования к помехам, создаваемым оборудованием в цепи источника электропитания

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

3.11.4.5 Требования к источнику питания переменного тока

Параметры источника питания переменного тока:

- максимально допустимое напряжение – не более 220 В;
- источник питания переменного тока оснащается устройством защитного отключения (УЗО);
- прочность изоляции цепей источника питания переменного тока относительно корпуса выдерживает (в нормальных условиях) не менее 1000 В пик.

3.12 Установка SMG

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

Изделие должно устанавливаться в помещения, имеющие ограниченный доступ – только для обслуживающего персонала.

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 8, рисунок 10, рисунок 12.

3.12.1 Порядок включения

Подключить цифровые потоки, оптический и электрический Ethernet-кабели к соответствующим разъемам шлюза.

Для защиты цифровых потоков от посторонних напряжений линейная сторона кросса должна быть оборудована устройствами комплексной защиты. Рекомендуются штекеры комплексной защиты фирмы KRONE “Com Protect 2/1 CP HGB 180 A1”.

Если предполагается подключение компьютера к консольному порту SMG, соединить консольный порт SMG с COM-портом ПК, при этом ПК должен быть выключен и заземлен в одной точке с цифровым шлюзом. Подключить к устройству кабель питания. Для подключения к сети постоянного тока использовать провод сечением не менее 1 мм^2.

Убедиться в целостности кабелей и их надежном креплении к разъемам.

Включить питание устройства и убедиться в отсутствии аварий по состоянию индикаторов на передней панели.

3.12.2 Крепление кронштейнов

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

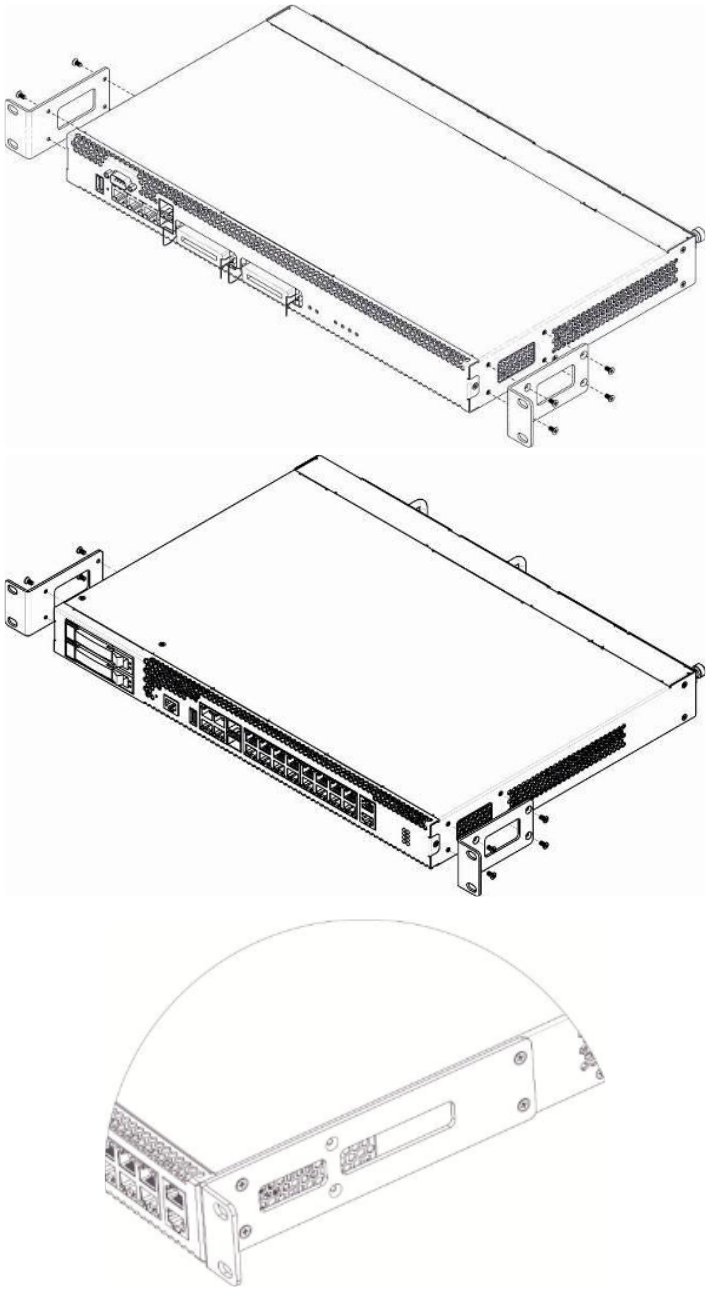


Рисунок 13 – Крепление кронштейнов для SMG-1016M (сверху слева), SMG-2016 (сверху справа) и SMG-3016 (внизу)

Для установки кронштейнов:

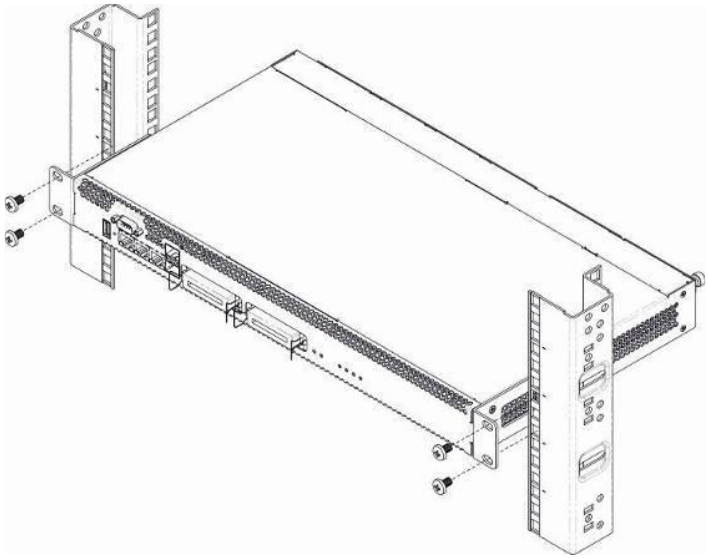
1. Совместите четыре отверстия для винтов на кронштейне с такими же отверстиями на боковой панели устройства, как это показано на рисунке 13.
2. С помощью отвертки прикрепите кронштейн винтами к корпусу.

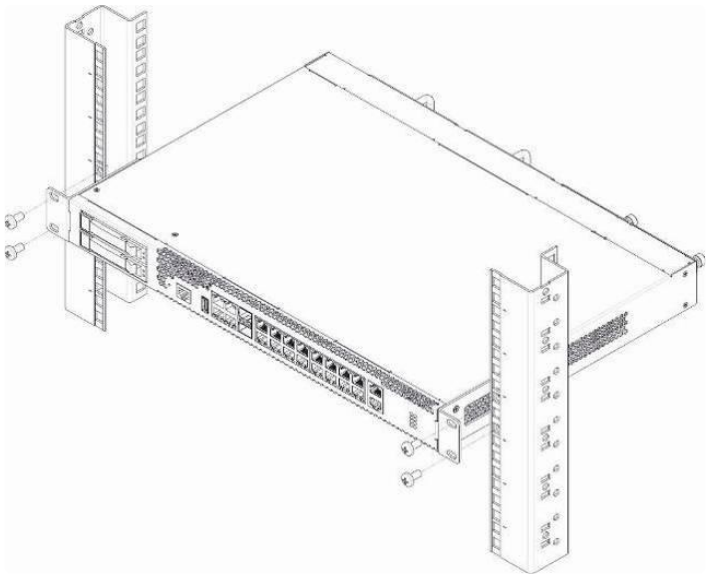
Повторите действия 1, 2 для второго кронштейна.

3.12.3 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. Вытащите устройство из стойки.





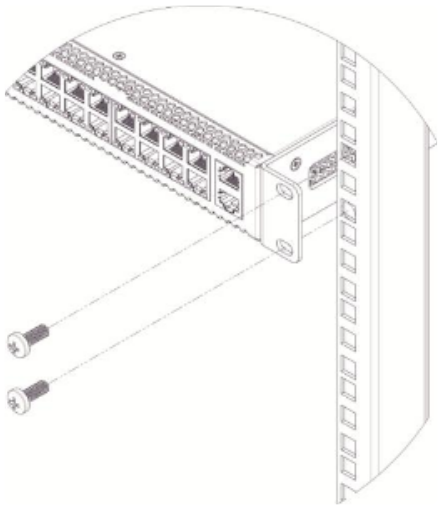


Рисунок 14 – Установка устройства в стойку SMG-1016M (сверху слева), SMG-2016 (сверху справа) и SMG-3016 (внизу)

3.12.4 Установка модулей питания

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

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

В устройстве установлено 2 предохранителя блоков питания номиналом 3,15 А. Самостоятельная замена предохранителей невозможна и осуществляется только квалифицированными специалистами в сервисном центре завода изготовителя.

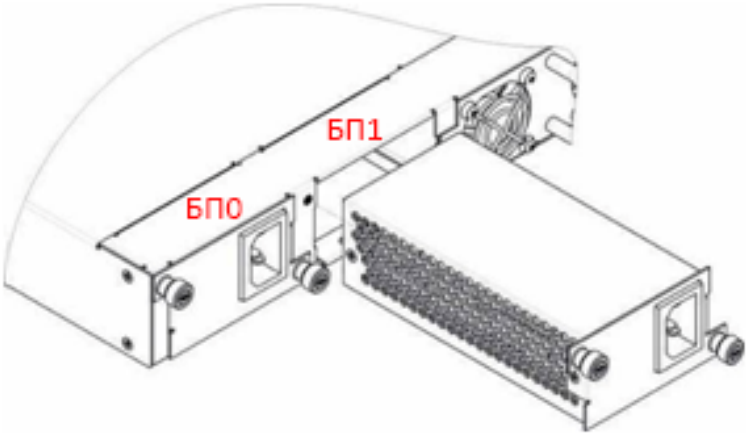


Рисунок 15 – Установка модулей питания

3.12.5 Вскрытие корпуса

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

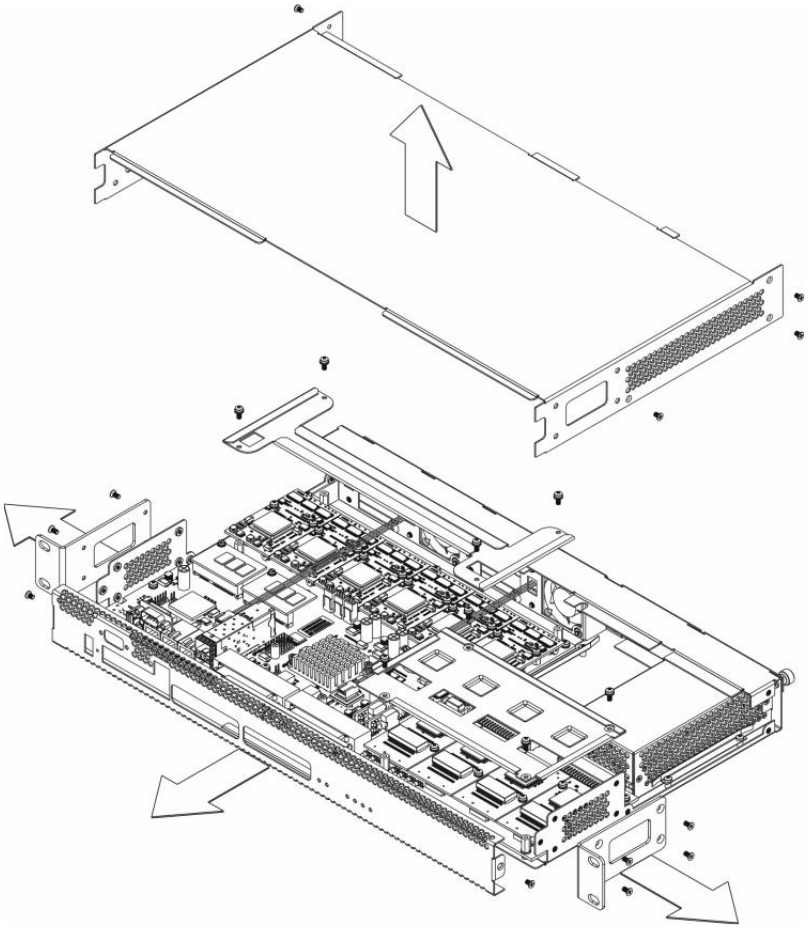


Рисунок 16 – Порядок вскрытия корпуса SMG-1016M

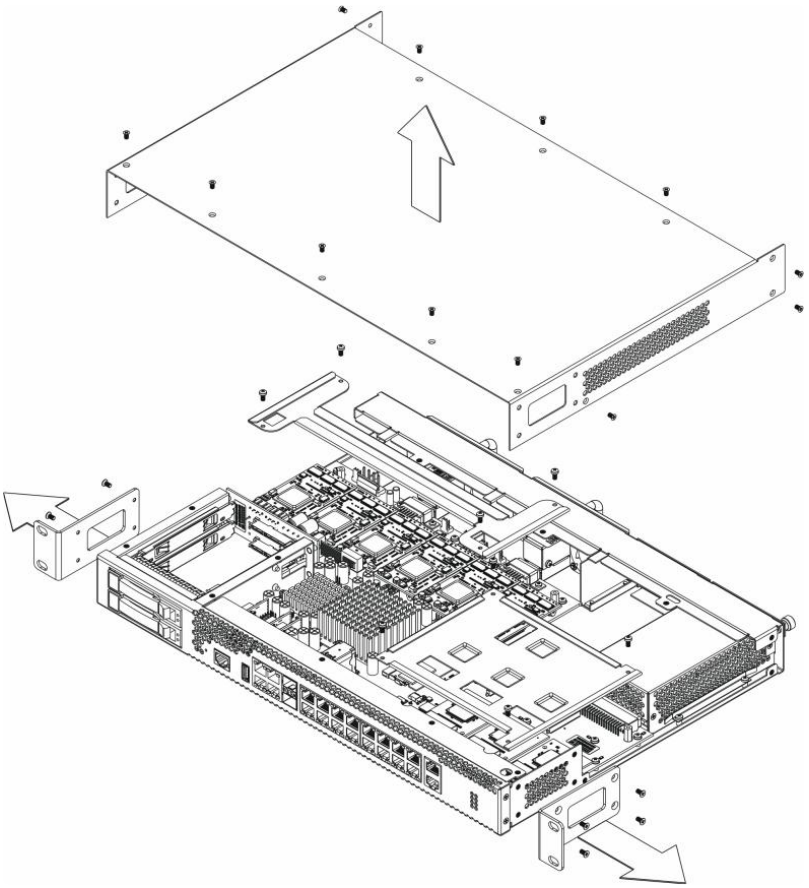


Рисунок 17 – Порядок вскрытия корпуса SMG-2016

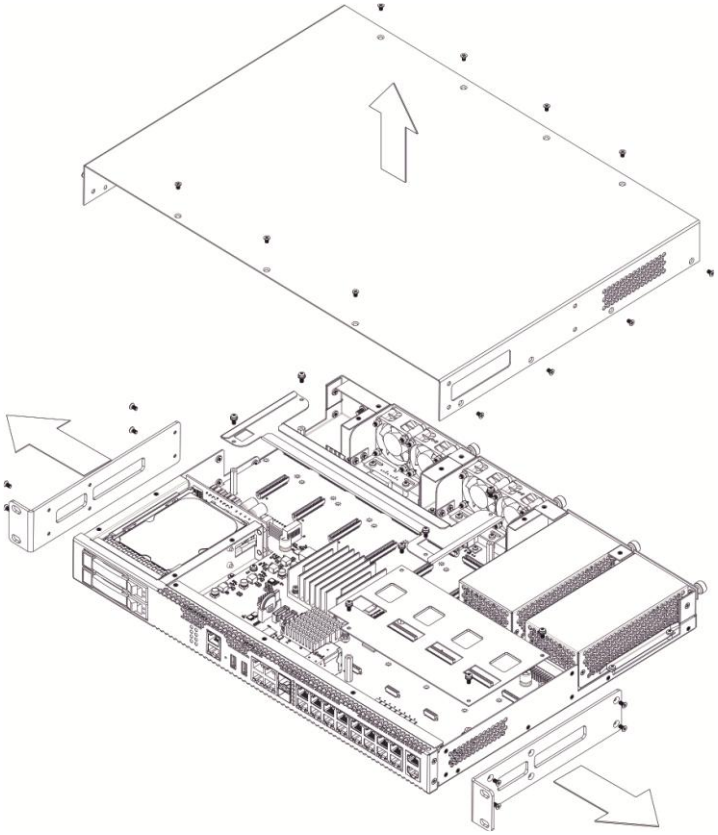


Рисунок 18 – Порядок вскрытия корпуса SMG-3016

1. С помощью отвертки отсоединить кронштейны от корпуса устройства.
2. **Только для SMG-1016M:** необходимо открутить фиксирующие винты передней панели, затем потянуть её на себя до отделения от верхней и боковых панелей (рисунок 16).
3. Открутить винты верхней панели устройства.
4. Снять верхнюю панель (крышку) устройства, потянув ее наверх.

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

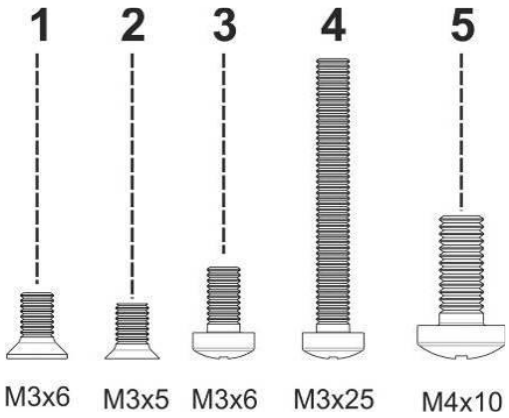


Рисунок 19 – Типы винтов для сборки SMG

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

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

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

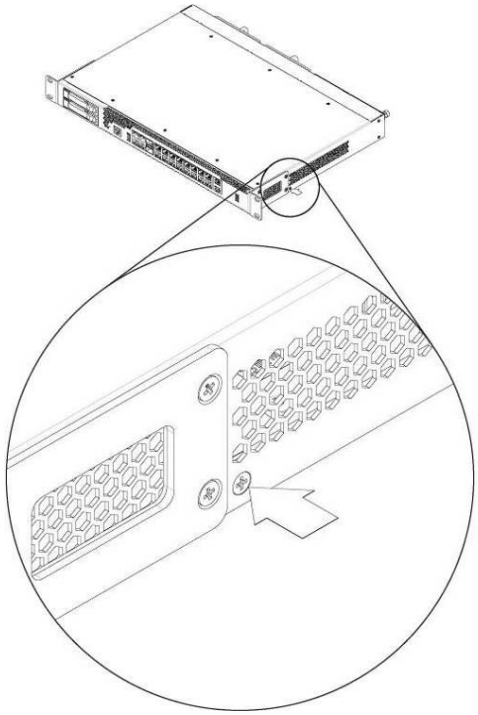


Рисунок 20 – Сборка SMG в корпус

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

3.12.6 Установка субмодулей

Устройство имеет модульную конструкцию с возможностью установки до 6 субмодулей IP SM-VP-M300 *(Submodule MSP)* и до 4 субмодулей потоков E1 C4E1 *(Submodule C4E1)* в позиции, указанные на рисунках ниже.

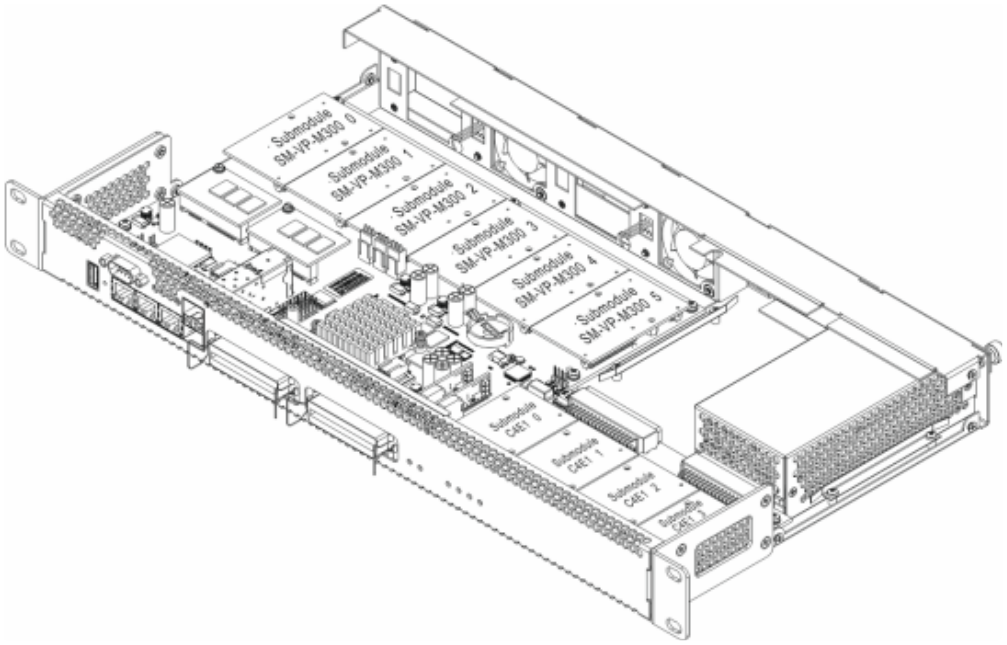


Рисунок 21 – Расположение субмодулей в SMG-1016M

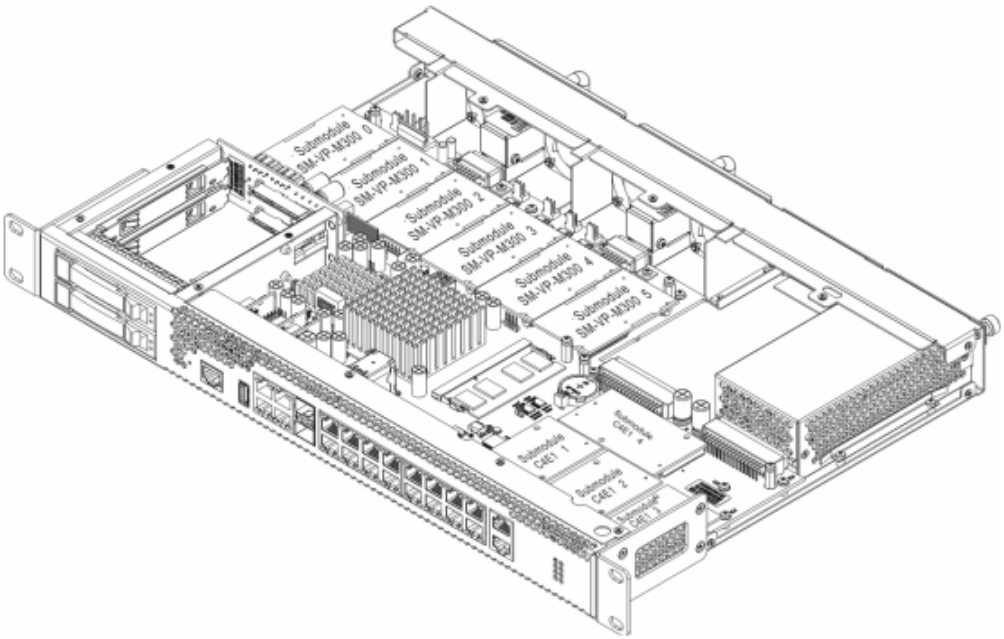


Рисунок 22 – Расположение субмодулей в SMG-2016

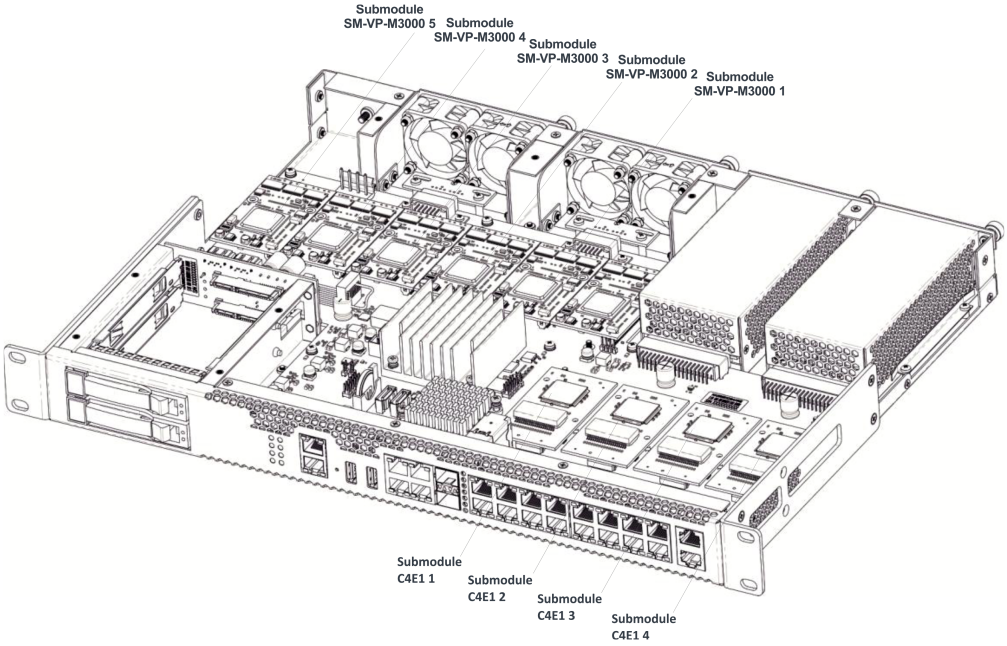


Рисунок 23 – Расположение субмодулей в SMG-3016

Порядок установки субмодулей SMG:

1. Проверить наличие питания сети на устройстве.

2. В случае наличия напряжения – отключить питание.

3. Если требуется, демонтировать устройство из стойки (см. раздел Установка устройства в стойку).

4. Вскрыть корпус устройства (см. раздел Вскрытие корпуса).

5. В некоторых аппаратных ревизиях субмодули закрываются пластинами особой формы, предотвращающими выпадание субмодулей при транспортировке (см. раздел Вскрытие корпуса, рисунки 16, 17, 18). В этом случае следует демонтировать пластину.

6. Установить модуль в свободную позицию (см. рисунки 21, 22, 23).

6.1 На плату установить шайбы, на них установить латунные стойки.

6.2 Установить субмодуль на стойки, убедившись, что разъемы плотно соединены с субмодулем.

6.3 Закрепить субмодуль с помощью винтов.

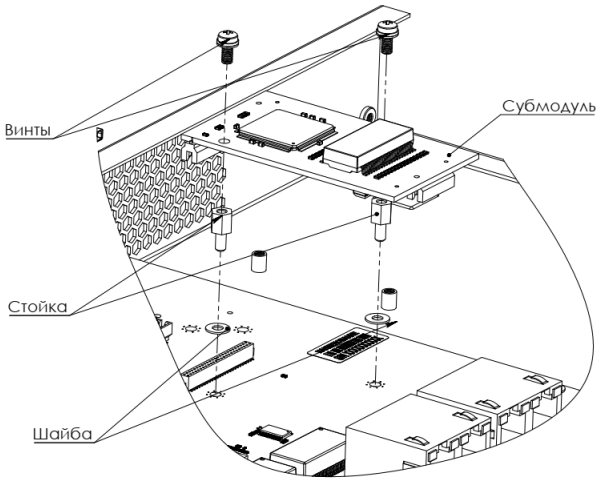


Рисунок 24 – Установка субмодуля на плату

6.4 Установить субмодуль на плату, убедившись, что разъемы плотно соединены с субмодулем.

6.5 Закрепить субмодуль с помощью герметика для фиксации субмодуля на плате.

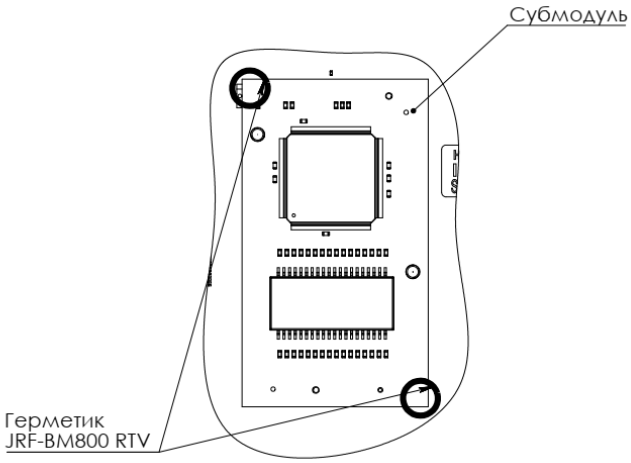


Рисунок 25 – Установка субмодуля на плату

7. Для позиций субмодулей *C4E1* установлено следующее соответствие с номерами потоков E1:

Для SMG-1016M

- Субмодуль C4E1 *0* – Поток E1 *0-3*;
- Субмодуль C4E1 *1* – Поток E1 *4-7*;
- Субмодуль C4E1 *2* – Поток E1 *8-11*;
- Субмодуль C4E1 *3* – Поток E1 *12-15*.

Для SMG-2016

- Субмодуль C4E1 *1*– Поток E1 *0-3*;
- Субмодуль C4E1 *2* – Поток E1 *4-7*;
- Субмодуль C4E1 *3* – Поток E1 *8-11*;
- Субмодуль C4E1 *4* – Поток E1 *12-15*.

Для SMG-3016

- Субмодуль C4E1 1 – Поток E1 *1-4*;
- Субмодуль C4E1 2 – Поток E1 *5-8*;
- Субмодуль C4E1 3 – Поток E1 *9-12*;
- Субмодуль C4E1 4 – Поток E1 *13-16*.

8. Поставить на место ограничительные пластины над субмодулями (если имеются), собрать корпус, установить устройство в стойку (если требуется).

3.12.7 Установка блоков вентиляции

Конструкция устройства предусматривает возможность замены блоков вентиляции без отключения питания.

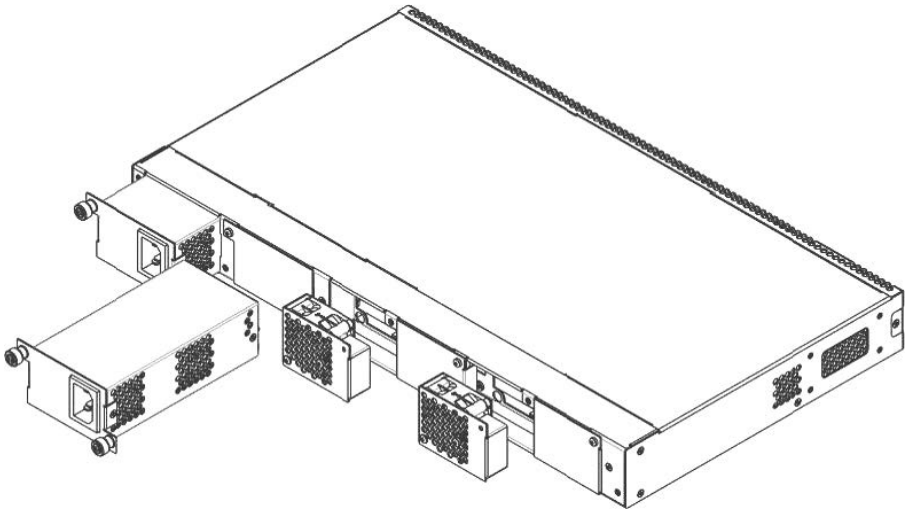


Рисунок 26 – Блок вентиляции SMG-1016M. Крепление в корпус

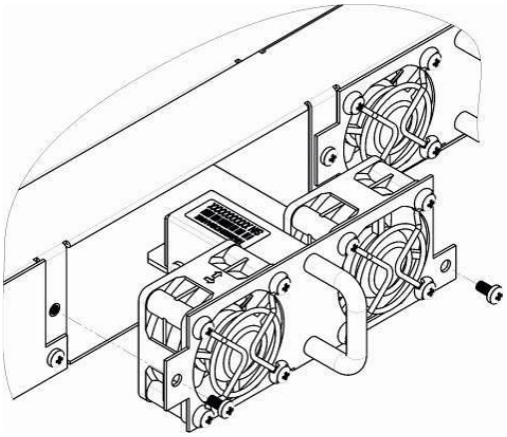


Рисунок 27 – Блок вентиляции SMG-2016. Крепление в корпус

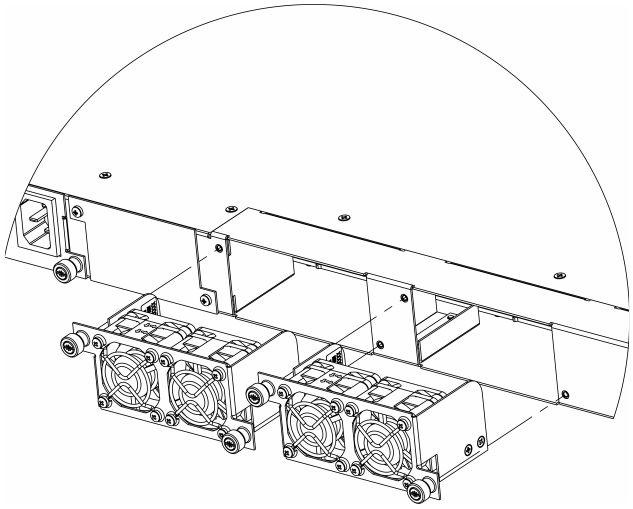


Рисунок 28 – Блок вентиляции SMG-2016 rev.B. Крепление в корпус

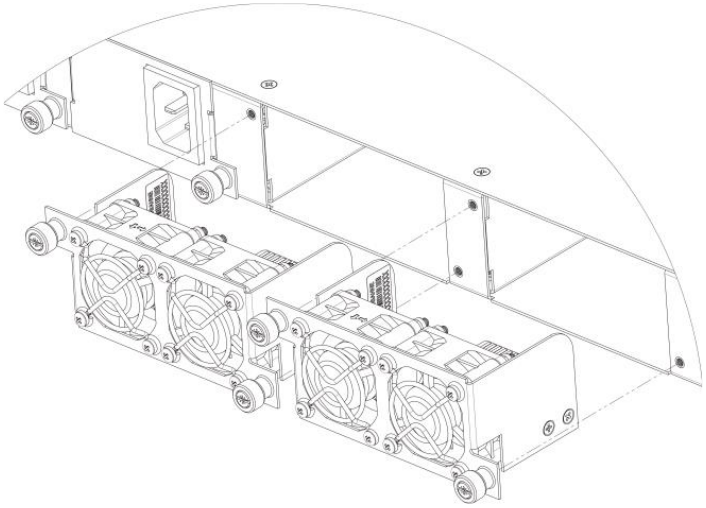


Рисунок 29 – Блок вентиляции SMG-3016. Крепление в корпус

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.

Отсоединить контакты блока от разъема в устройстве, рисунок ниже.

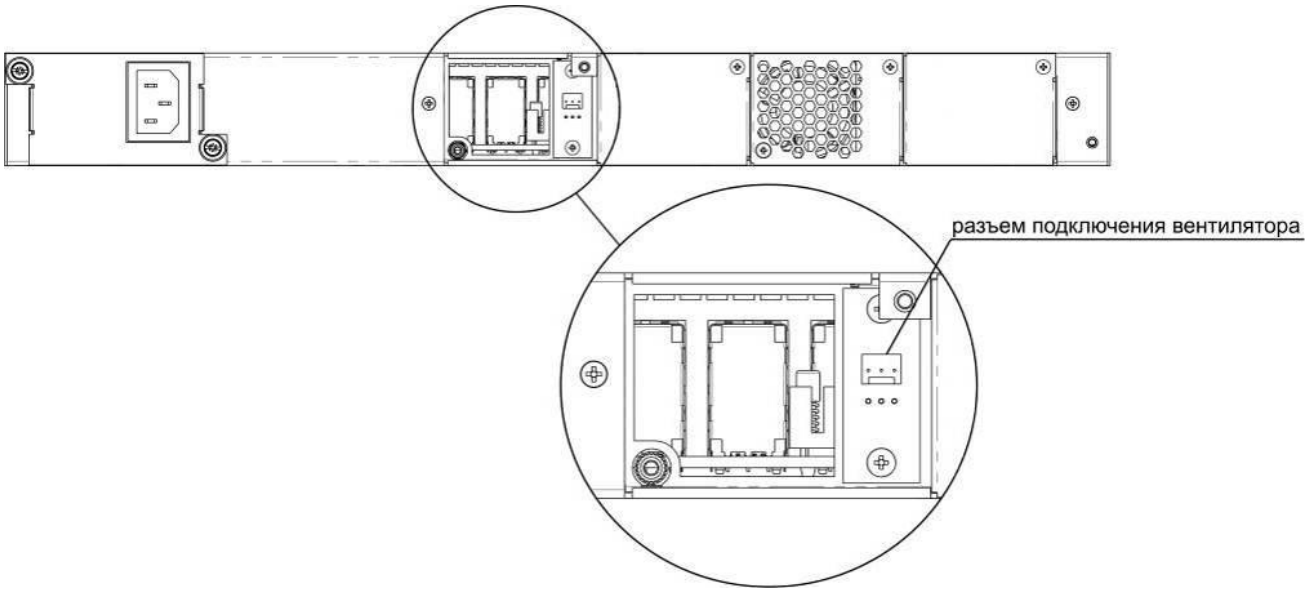


Рисунок 30 – Разъем для подключения вентилятора SMG-1016M

Для установки блока необходимо:

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

3.12.8 Установка SSD-накопителей для SMG-1016M

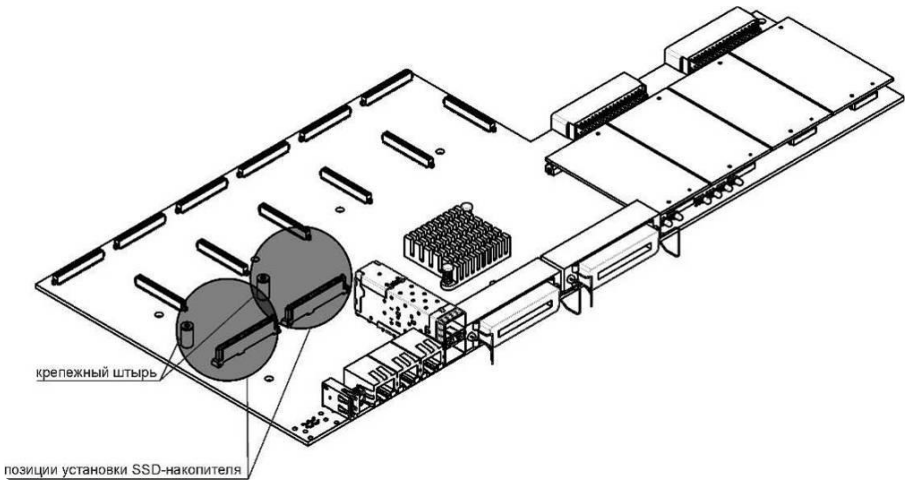


Рисунок 31 – Установка SSD-накопителя

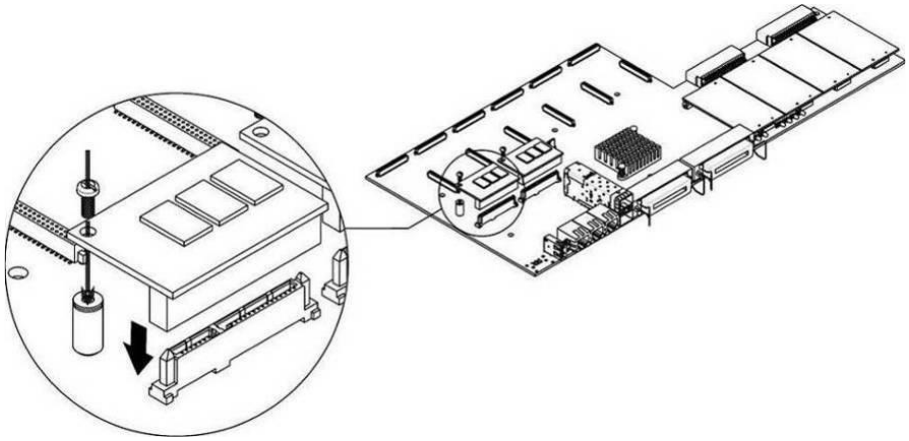


Рисунок 32 – Монтаж SSD-накопителя



1. Проверить наличие питания сети на устройстве.
2. В случае наличия напряжения – отключить питание.
3. Если требуется, демонтировать устройство из стойки (см. раздел Установка устройства в стойку).
4. Вскрыть корпус устройства (см. раздел Вскрытие корпуса).
5. Если на плате устройства отсутствует крепежный штырь (см. рисунок 31), необходимо использовать съемную стойку:
   a. Прикрепить стойку-фиксатор к SSD-накопителю;
   b. Снять верхний защитный слой с клеевой поверхности стойки-фиксатора.
6. Установить накопитель в свободную позицию – всего доступно 2 позиции (см. рисунок 31) и, если на плате присутствует крепежный штырь, закрепить винтом, рисунок 32.

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

3.12.9 Установка SATA-дисков для SMG-2016, SMG-3016

При заказе с устройством могут быть дополнительно поставлены SATA-диски.

При монтаже SATA-дисков необходимо:

1. Извлечь направляющие салазки из корпуса устройства (рисунок 9, рисунок 11, элемент 1), для этого нажать на кнопку справа до отхождения ручки выталкивателя, затем потянуть ручку на себя до извлечения салазок из корпуса.
2. Извлечь комплект крепежа, расположенный под ручкой выталкивателя, рисунок 33.
3. Закрепить диск в лотке направляющих салазок, рисунок 34.
4. Вставить салазки с установленным SATA-диском обратно в разъем и прижать ручку выталкивателя до характерного щелчка.

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

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

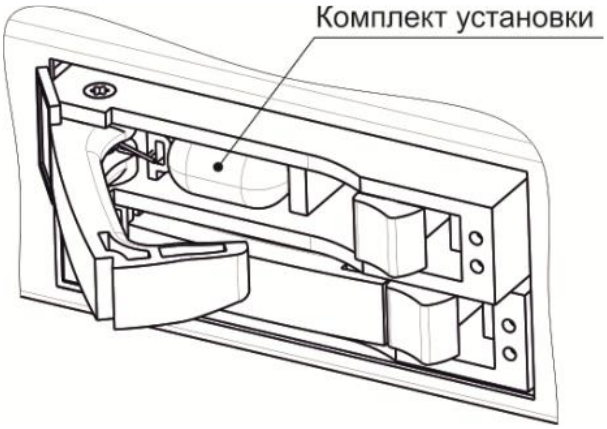


Рисунок 33 – Расположение комплекта крепежных элементов при поставке

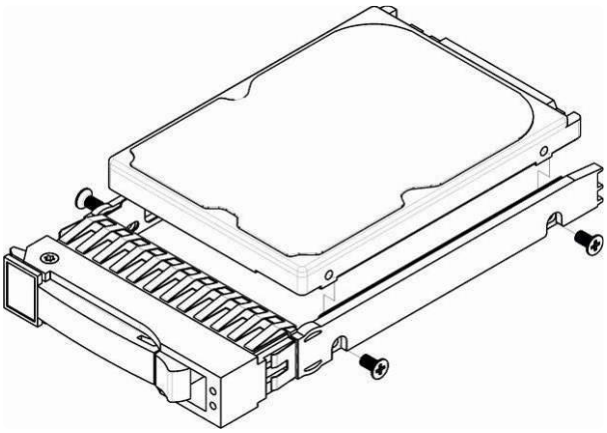


Рисунок 34 – Крепление SATA-диска в лоток направляющих салазок

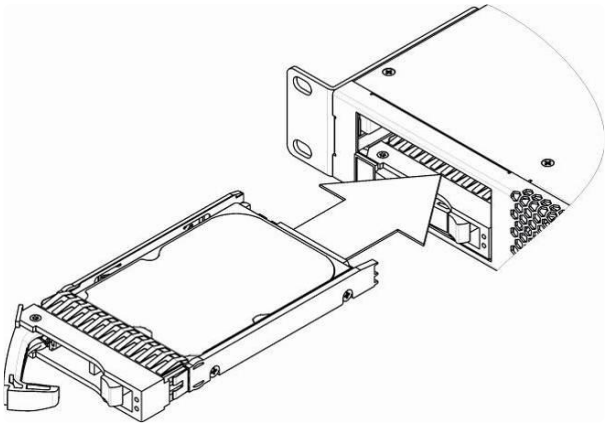


Рисунок 35 – Монтаж SATA-диска в корпус устройства

3.12.10 Замена батарейки часов реального времени

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

Таблица 15 – Характеристики элемента питания для RTC

Параметр	**Значение**
Тип батареи	литиевая
Типоразмер	CR2032 (возможна установка CR2024)
Напряжение	3 В
Емкость	225 мА
Диаметр	20 мм
Толщина	3,2 мм
Срок службы	5 лет
Условия хранения	от -20 до +35 °C

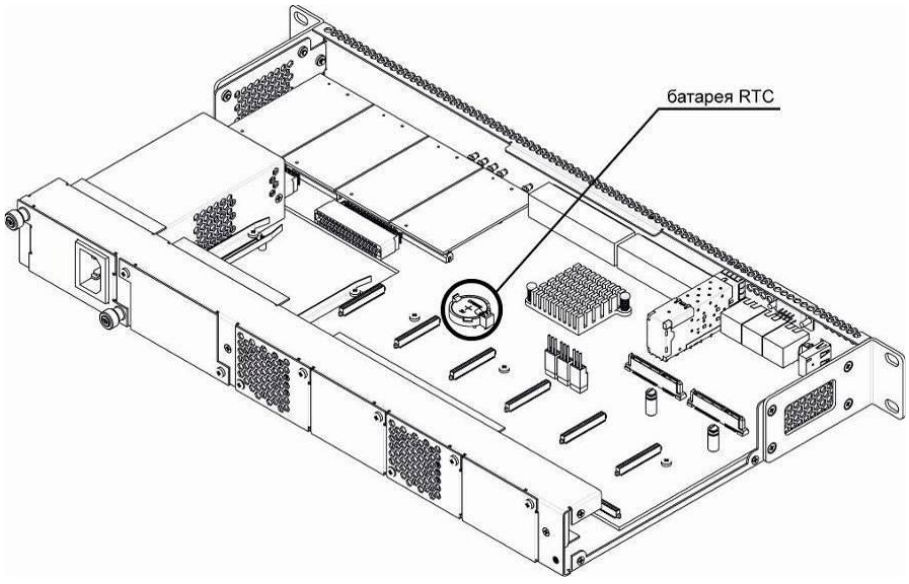


Рисунок 36 – Положение батареи RTC для SMG-1016M

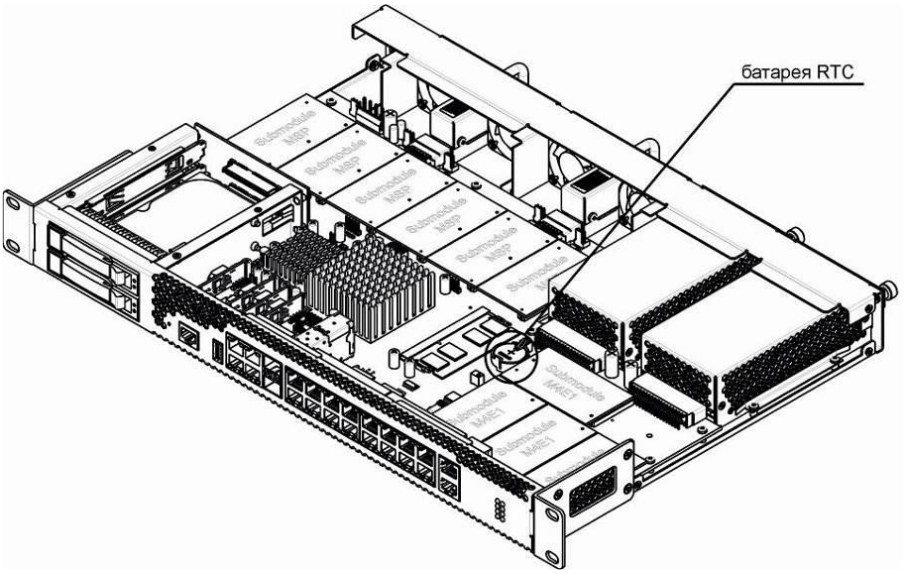


Рисунок 37 – Положение батареи RTC для SMG-2016

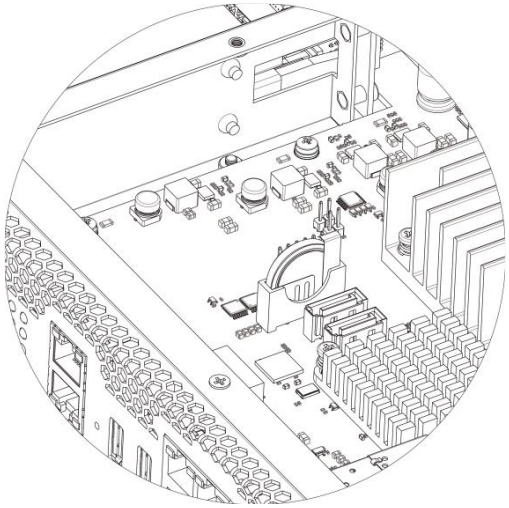


Рисунок 38 – Положение батареи RTC для SMG-3016

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

1. Проверить наличие питания сети на устройстве.
2. В случае наличия напряжения – отключить питание.
3. Если требуется, демонтировать устройство из стойки (см. раздел Установка устройства в стойку).
4. Вскрыть корпус устройства (см. раздел Вскрытие корпуса).
5. Извлечь отработавшую батарейку (рисунок 36, рисунок 37, рисунок 38) и в аналогичной позиции установить новую.

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

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

Использованные батарейки подлежат специальной утилизации.

4 Общие рекомендации при работе со шлюзами SMG (SIGTRAN)

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

Во избежание несанкционированного доступа к устройству рекомендуем сменить пароль на доступ через telnet и консоль (по умолчанию пользователь **admin**, пароль **rootpasswd**), а также сменить пароль для администратора на доступ через web-конфигуратор. Установка пароля для доступа через telnet и консоль описана в разделе Смена пароля для доступа к устройству через CLI. Установка пароля для доступа через web-конфигуратор описана в меню Установка пароля для доступа через web-конфигуратор. Рекомендуется записать и сохранить установленные пароли в надежном месте, недоступном для злоумышленников.

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.

⚠ Для обеспечения безопасности устройства необходимо следовать рекомендациям, описанным в Приложении Е. Рекомендации по безопасности.

5 Конфигурирование устройств SMG (SIGTRAN)

К устройству можно подключиться четырьмя способами: через web-конфигуратор, с помощью протокола Telnet, SSH либо кабелем через разъем RS-232 (при доступе через RS-232, SSH либо Telnet используется CLI). Подробное описание конфигурирования устройств описано в разделах:

- Настройка SMG (SIGTRAN) через web-конфигуратор
- Настройка SMG (SIGTRAN) с помощью командной строки
- Настройка SMG (SIGTRAN) через Telnet, SSH и RS-232

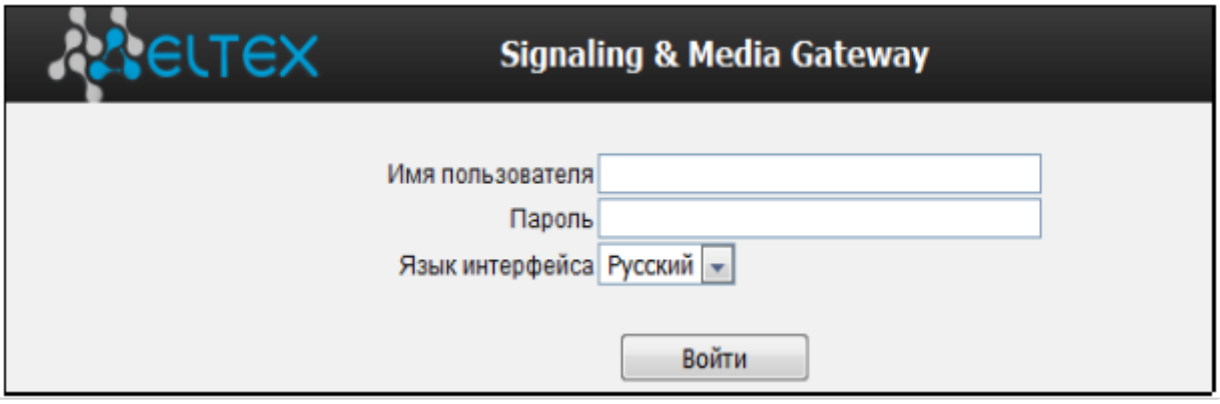
Все настройки применяются без перезагрузки шлюза. Для сохранения измененной конфигурации в энергонезависимую память используйте меню «Сервис/Сохранить конфигурацию во Flash» в web-конфигураторе либо команду `copy running_to_startup` **в CLI.**

5.1 Настройка SMG (SIGTRAN) через web-конфигуратор

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

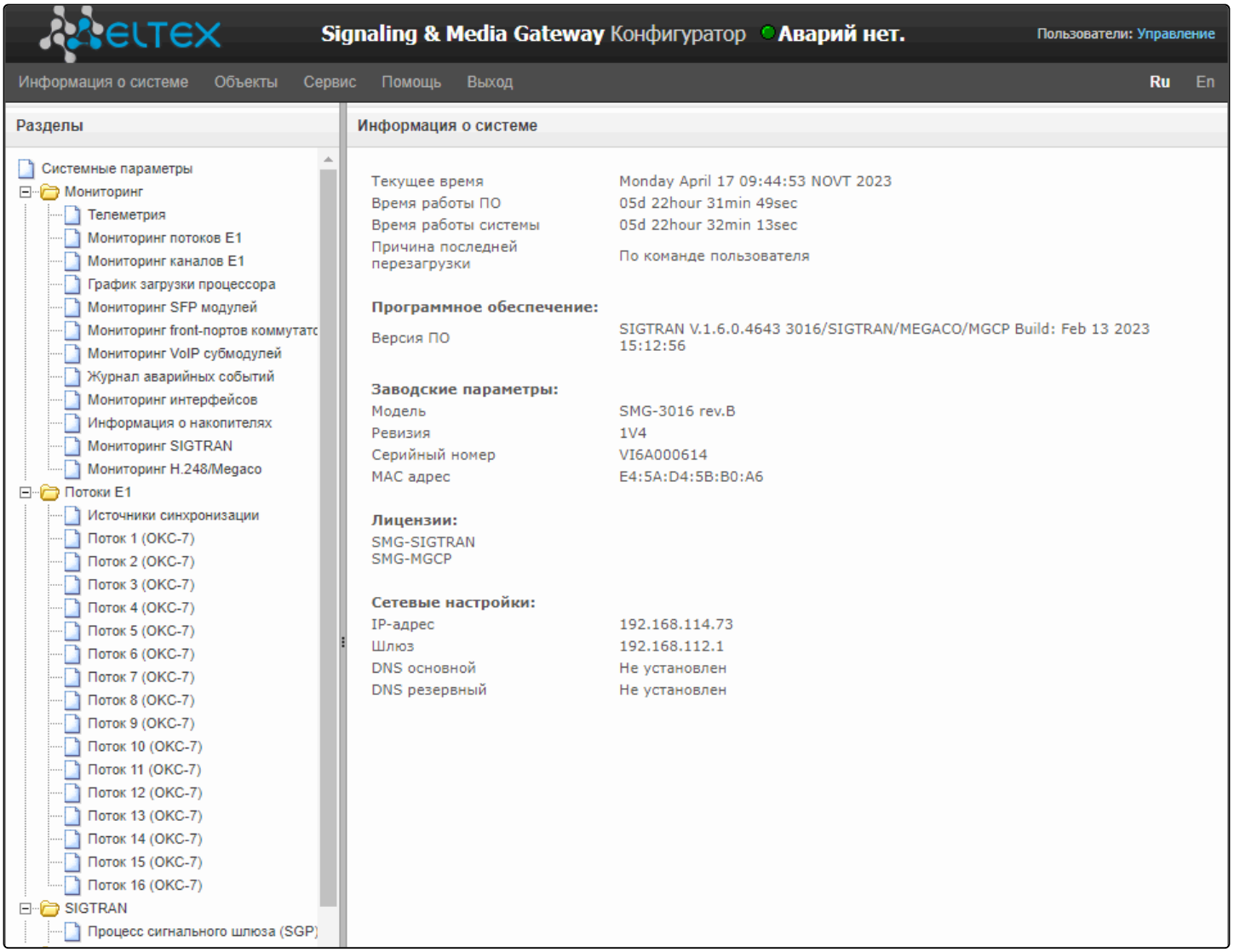
Заводской IP-адрес устройства SMG – 192.168.1.2 маска сети – 255.255.255.0.

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

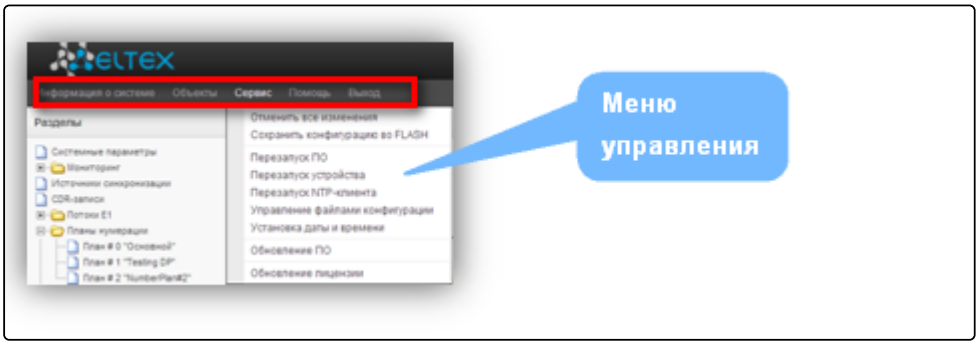


При первом запуске имя пользователя: *admin*, пароль: *rootpasswd*.

После получения доступа к web-конфигуратору откроется страница «*Информация о системе*».



На рисунке ниже представлены элементы навигации web-конфигуратора.



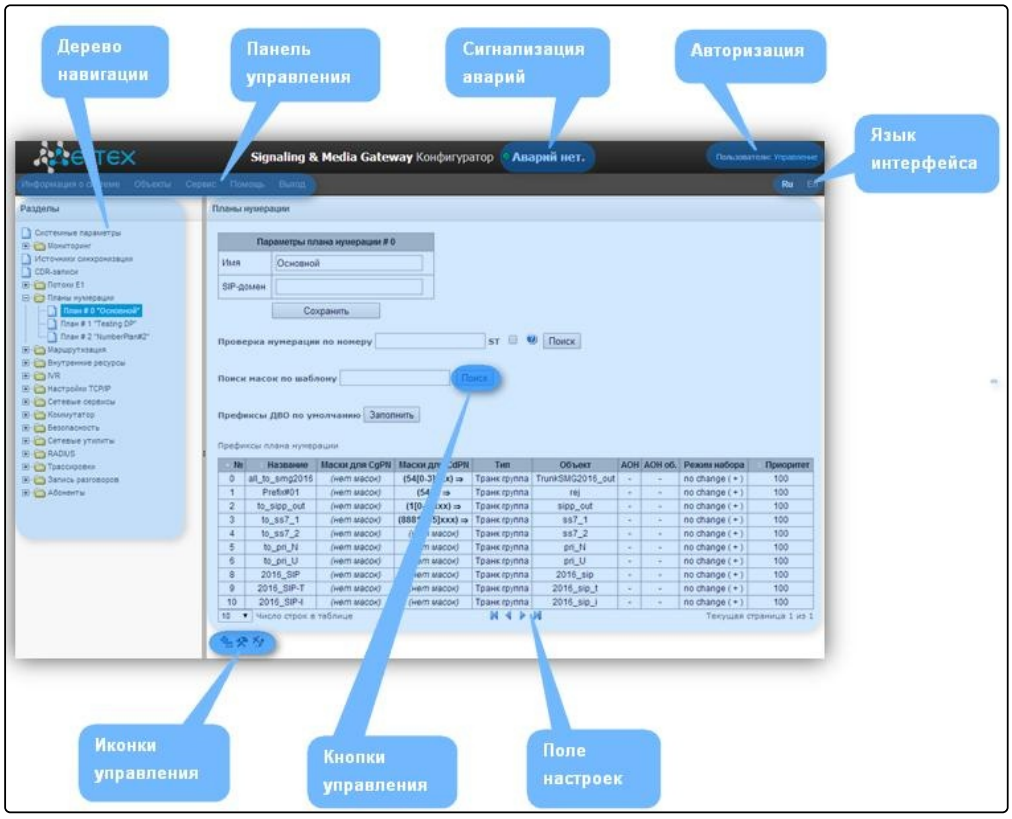


Рисунок 29 − Элементы навигации web-конфигуратора

Окно пользовательского интерфейса разделено на несколько областей:

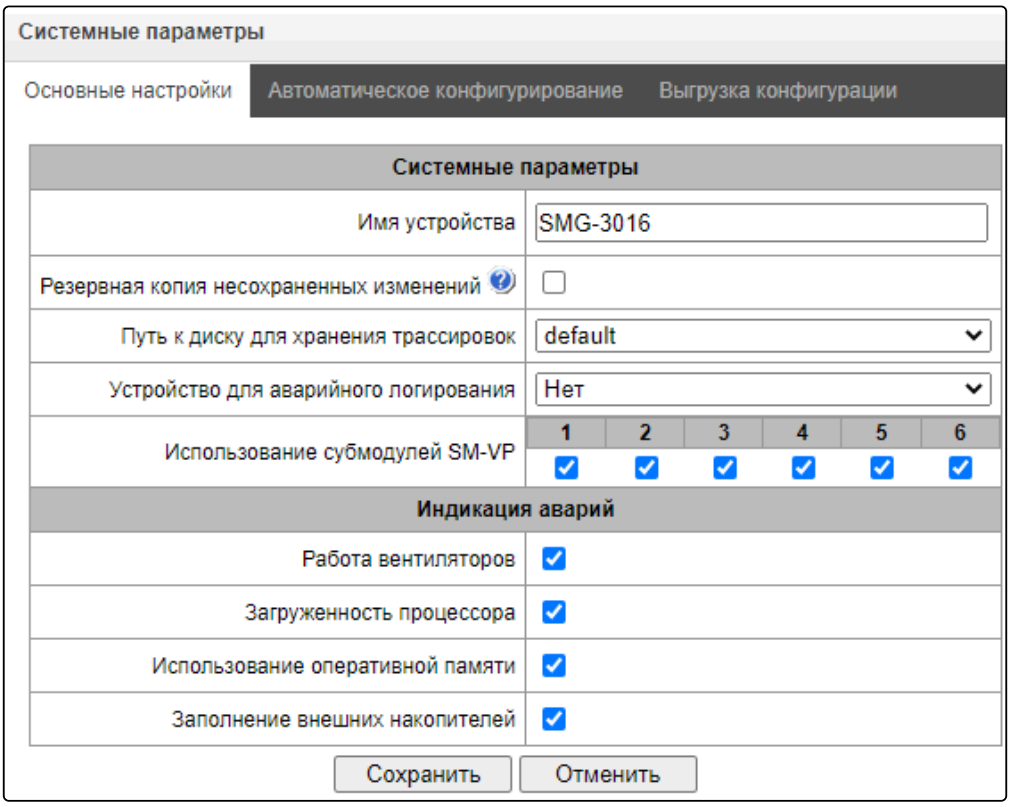
Дерево навигации	служит для управления полем настроек. В дереве навигации иерархически отображены разделы управления и меню, находящиеся в них.
Поле настроек	базируется на выборе пользователя. Предназначено для просмотра настроек устройства и ввода конфигурационных данных.
Панель управления	панель для управления полем настроек и состоянием ПО устройства.
Меню управления	выпадающие меню панели управления полем настроек и состоянием ПО устройства.
Сигнализация аварий	служит для отображения текущей приоритетной аварии, также является ссылкой для работы с журналом аварийных событий.
Авторизация	ссылка для работы с паролями доступа к устройству через web-конфигуратор.
Язык интерфейса	кнопки для переключения языка интерфейса.
Иконки управления	элементы управления для работы с объектами поля настроек, дублируют меню «Объекты» на панели управления:  − *Добавить объект;*  − *Редактировать объект;*  − *Удалить объект;*  − *Посмотреть объект.*
Кнопки управления	элементы управления для работы с полем настроек.

Во избежание несанкционированного доступа при дальнейшей работе с устройством рекомендуется изменить пароль (раздел «Установка пароля для доступа через web-конфигуратор»).

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

5.1.1 Системные параметры

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



- *Имя устройства* – наименование устройства. Данное имя используется в заголовке web-конфигуратора устройства;
- *Резервная копия несохраненных изменений* – при включенной опции устройство каждые 60 секунд создает резервную копию несохраненных изменений конфигурации с возможностью их дальнейшего восстановления. Например, на устройстве были несохраненные изменения и произошел перезапуск по питанию. В случае если опция была включена после старта устройства, в веб-интерфейсе появится окно с предложением восстановить несохраненные изменения;
- *Путь к диску для хранения трассировок* – на устройстве существует возможность сохранения отладочной информации (трассировок) в оперативной памяти (RAM) либо на установленном накопителе:
  - *default* – отладочная информация сохраняется в оперативную память;
  - */mnt/sdX* – путь к локальному накопителю, настройка отображается при установленном накопителе. При выборе накопителя на нем будет создан каталог logs, в котором будут храниться файлы трассировок.

Сохранение трассировок доступно только для SSD-накопителя/ SATA-накопителя, хранение на USB-накопителе невозможно.

- *Количество активных планов нумерации* – количество одновременно активных планов нумерации, всего можно настроить до 16 (до 255 на SMG-2016 при наличии лицензии ДВО) независимых планов нумерации с возможностью добавления абонентов в каждый план и построения своей таблицы маршрутизации вызовов;
- *Отложенное применение плана нумерации* – при выставленном флаге SMG не будет применять изменения в конфигурации до специального подтверждения. Установка этой опции помогает при работе с большими планами нумерации, позволяя избежать их длительной обработки после каждого изменения настроек;

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

Пример файла alarm.txt

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

Описание формата файла:

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

Таблица 16 – Примеры выводимых сообщений об авариях

Аварийное сообщение	**Расшифровка**
Configuration error	Ошибка файла конфигурации
E1-Line alarmed	Авария потока E1
Sync from local source, but sync source table not empty	Потеря источника синхронизации
E1-Line Remote-alarm	Удаленная авария потока E1
Sync from not most priority source	Потеря основного источника синхронизации, текущий источник менее приоритетный
Software started	Запуск ПО устройства

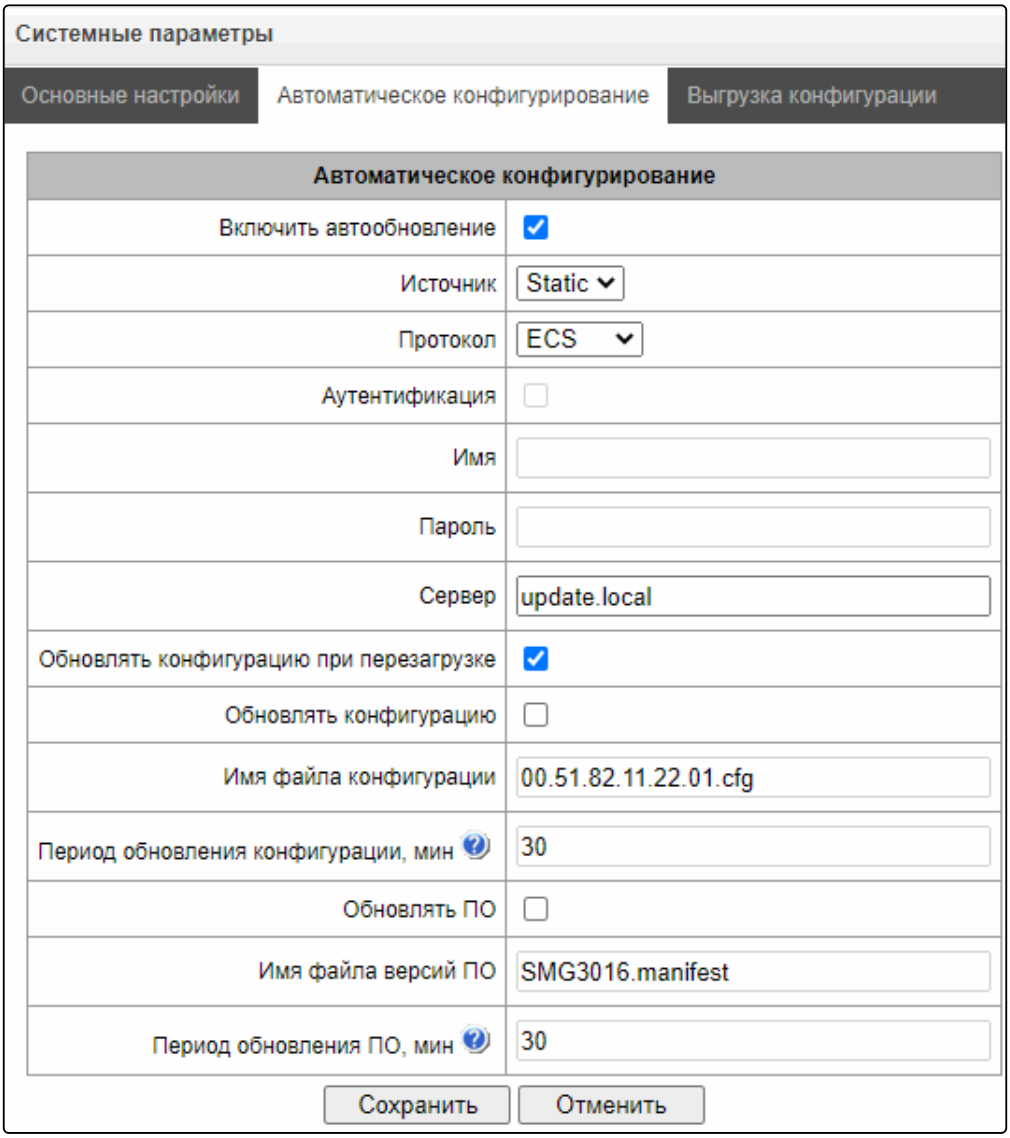
- *Использование субмодулей SM-VP* – выбор субмодулей SM-VP, которые будут находиться в работе.

Индикация аварий

- *Работа вентиляторов* – при установленном флаге в случае выхода из строя охлаждающих вентиляторов будет индикация об аварии (на устройстве загорится индикатор *Alarm*, авария будет занесена в журнал аварий);
- *Загруженность процессора* – при установленном флаге в случае высокой загрузки управляющего процессора будет индикация об аварии (на устройстве загорится индикатор *Alarm*, авария будет занесена в журнал аварий);
- *Использование оперативной памяти* – при установленном флаге в случае занятости более 75 % от общего объема оперативной памяти будет индикация об аварии (на устройстве загорится индикатор *Alarm*, авария будет занесена в журнал аварий);
- *Заполнение внешних накопителей* – при установленном флаге, если один из внешних накопителей заполнен на более чем 80 %, если объем внешнего накопителя не превышает 5 ГБ (или осталось менее 1024 МБ свободного пространства, если объем внешнего накопителя более 5 ГБ), будет индикация об аварии (на устройстве загорится индикатор *Alarm*, авария будет занесена в журнал аварий).

Автоматическое конфигурирование

Системные параметры → Автоматическое конфигурирование



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

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

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

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

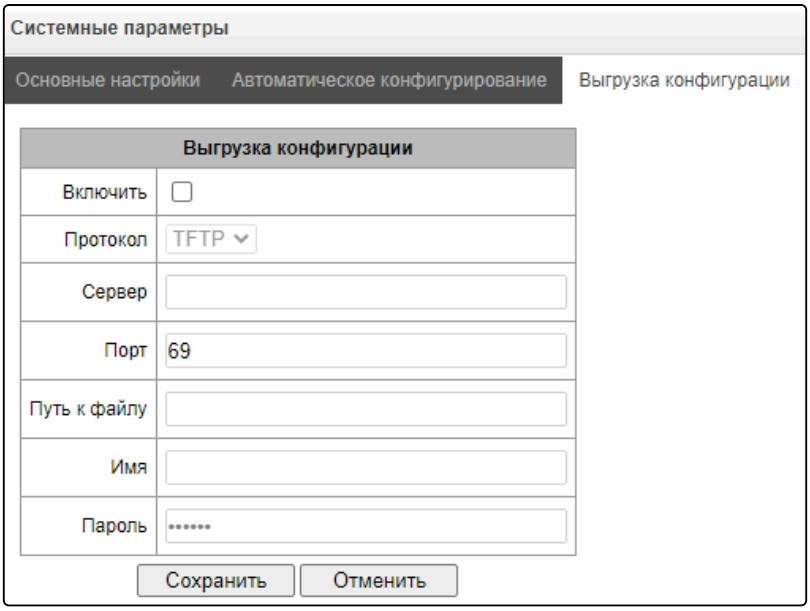
Пример файла описания версий ПО:

3.7.0.1944;smg1016m_firmware_3.7.0.1944.bin
3.8.0.2050;smg1016m_firmware_3.8.0.2050.bin;9-13

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

Выгрузка конфигурации

Системные параметры → Выгрузка конфигурации



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

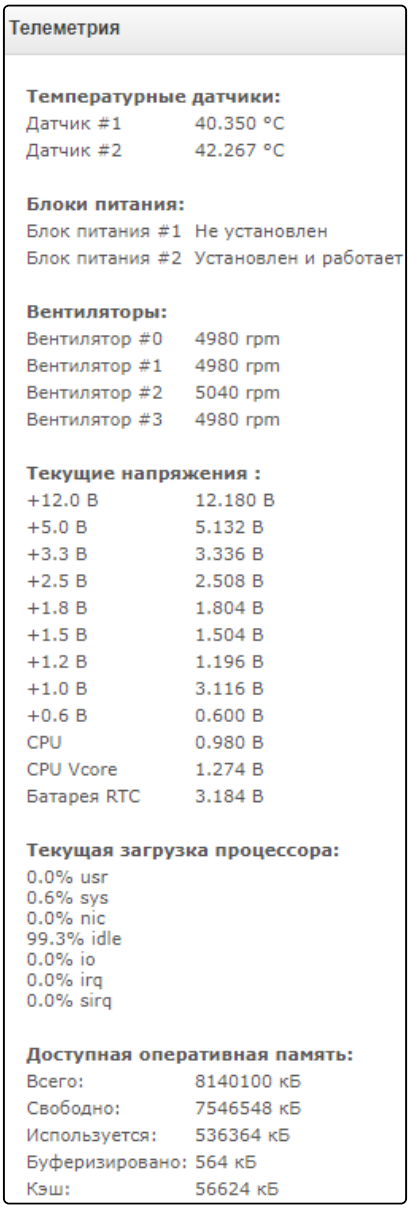
- *Включить* − включает функцию выгрузки конфигурации;
- *Протокол* − выбор протокола, по которому будет производиться выгрузка. Поддерживается FTP или TFTP;
- *Сервер* − IP-адрес сервера, на который будет производиться выгрузка;
- *Порт* − порт сервера, на который будет производиться выгрузка;
- *Путь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

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

5.1.2 Мониторинг

5.1.2.1 Телеметрия

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



Температурные датчики

- *Датчик #0 (Температура CPU)* − показания температурного датчика, находящегося на центральном процессоре;
- *Датчик #1 (Температура RAM)* − показания температурного датчика, находящегося на модуле оперативной памяти.

Блоки питания

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

Возможные состояния блоков питания:

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

Вентиляторы

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

Напряжение[1]

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

Текущее напряжение[2]

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

Текущая загрузка процессора:

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

Доступная оперативная память[2]

- *Всего* – общее количество памяти;
- *Свободно* – количество свободной памяти;
- *Используется* – количество используемой памяти;
- *Буферизировано* – количество забуферизировнной памяти;
- *Кэш* – количество закэшированной памяти.

В устройстве SMG-1016M установлено 2 вентилятора, в SMG-2016, SMG-3016 – 4 вентилятора.

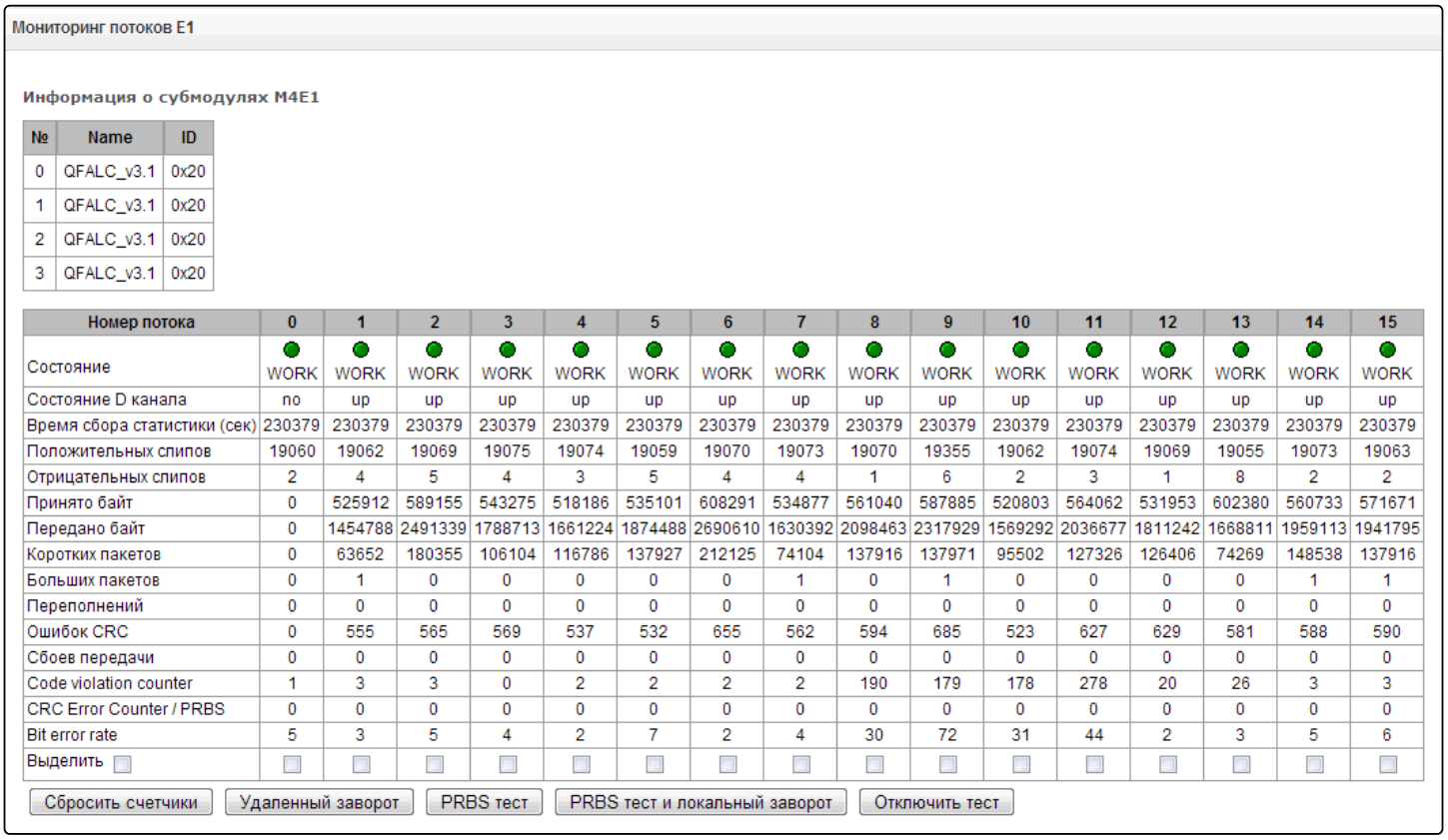
---

[1] *Только для SMG-1016M.*

[2] *Только для SMG-2016, SMG-3016.*

5.1.2.2 Мониторинг потоков E1

В разделе отображается информация об установленных чипах на субмодулях *C4E1*, а также мониторинг и статистика потоков *E1*.



Мониторинг потоков E1

Информация о субмодулях M4E1

№	Name	ID
0	QFALC_v3.1	0x20
1	QFALC_v3.1	0x20
2	QFALC_v3.1	0x20
3	QFALC_v3.1	0x20

Номер потока	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Состояние	WORK	WORK	WORK	WORK	WORK	WORK	WORK	WORK	WORK	WORK	WORK	WORK	WORK	WORK	WORK	WORK
Состояние D канала	no	up	up	up	up	up	up	up	up	up	up	up	up	up	up	up
Время сбора статистики (сек)	230379	230379	230379	230379	230379	230379	230379	230379	230379	230379	230379	230379	230379	230379	230379	230379
Положительных слипов	19060	19062	19069	19075	19074	19059	19070	19073	19070	19355	19062	19074	19069	19055	19073	19063
Отрицательных слипов	2	4	5	4	3	5	4	4	1	6	2	3	1	8	2	2
Принято байт	0	525912	589155	543275	518186	535101	608291	534877	561040	587885	520803	564062	531953	602380	560733	571671
Передано байт	0	1454788	2491339	1788713	1661224	1874488	2690610	1630392	2098463	2317929	1569292	2036677	1811242	1668811	1959113	1941795
Коротких пакетов	0	63652	180355	106104	116786	137927	212125	74104	137916	137971	95502	127326	126406	74269	148538	137916
Больших пакетов	0	1	0	0	0	0	0	1	0	1	0	0	0	0	1	1
Переполнений	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Ошибок CRC	0	555	565	569	537	532	655	562	594	685	523	627	629	581	588	590
Сбоев передачи	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Code violation counter	1	3	3	0	2	2	2	2	190	179	178	278	20	26	3	3
CRC Error Counter / PRBS	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bit error rate	5	3	5	4	2	7	2	4	30	72	31	44	2	3	5	6
Выделить	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Сбросить счетчики | Удаленный заворот | PRBS тест | PRBS тест и локальный заворот | Отключить тест

Для чипов E1 в таблице указывается номер позиции, в которую он установлен (см. раздел Установка субмодулей), имя чипа и идентификатор.

Параметры потоков:

- *Состояние* − статус потока:
  - *WORK* − поток в работе;
  - *LOS* − потеря сигнала;
  - *OFF* − поток выключен в конфигурации;
  - *NONE* − не установлен субмодуль;
  - *AIS* − сигнал индикации аварийного состояния (сигнал, содержащий все единицы);
  - *LOMF* − сигнал индикации аварийного состояния сверхцикла;
  - *RAI* − индикация удаленной аварии;
  - *TEST* − индикация тестирования потока (PRBS test, заворот локальный и удаленный).
- *Состояние D канала* − статус D-канала, служебного канала управления;
  - *up* − *D*-канал в работе;
  - *down* − *D*-канал не в работе;
  - *no* − на потоке отсутствует канал управления;
  - *off* − на потоке выключена сигнализация.
- *Время сбора статистики (сек)* − период времени сбора статистики, в секундах;
- *Положительных слипов* − число положительных проскальзываний на потоке;
- *Отрицательных слипов* − число отрицательных проскальзываний на потоке;
- *Принято байт* − количество принятых байт из потока;
- *Передано байт* − количество переданных байт по потоку;
- *Коротких пакетов* − число принятых пакетов меньше стандартного размера;
- *Больших пакетов* − число принятых пакетов, превышающих стандартный размер;
- *Переполнений* − счетчик ошибок переполнения буфера;

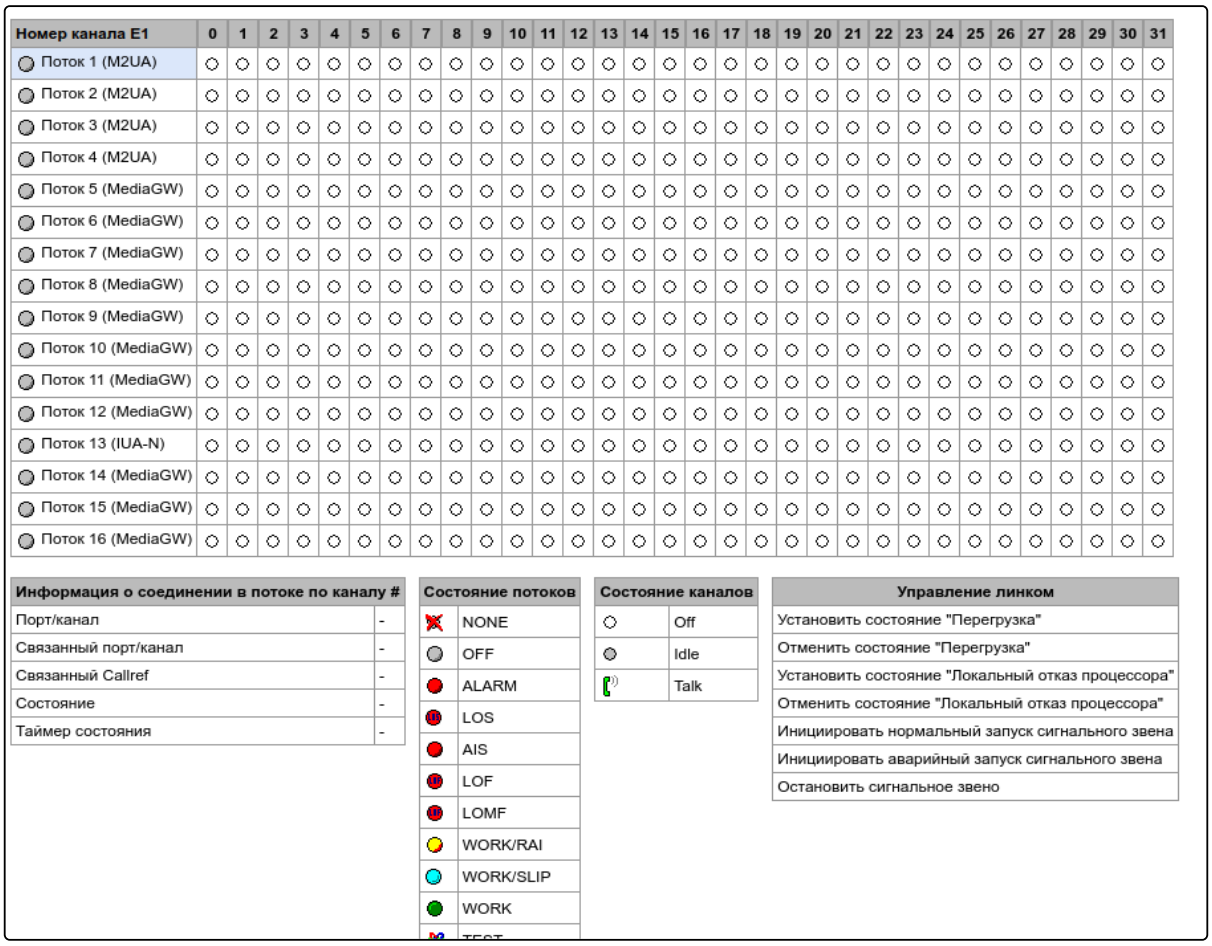
- *Ошибок CRC* – счетчик ошибок CRC;
- *Сбоев передачи* – счетчик сбоев при передаче по потоку;
- *Code violations counter* – счетчик сбоев кодовой последовательности сигнала;
- *CRC Error Counter/PRBS* – количество ошибок CRC (в режиме «PRBS test»);
- *Bit error rate* – количество битовых ошибок по потоку.

Функциональные кнопки:

- *«Сбросить счетчики»* – при установке флага для выбранного потока при нажатии на кнопку *«Сбросить»* накопленная статистика будет обнулена;
- *«Удаленный заворот»* – режим тестирования тракта E1, при котором сигнал, принятый комплектом из подключенного потока E1, будет направлен непосредственно на передачу в этот же поток;
- *«PRBS test»* – включает псевдослучайную последовательность на выходной порт комплекта (передает в подключенный поток E1), при этом на входном порту комплекта (прием потока E1) включается режим детектирования ошибок этой последовательности для оценки качества передачи сигнала. Количество ошибок и счётчик времени анализа можно просмотреть в окне информации о потоке;
- *«PRBS тест и локальный заворот»* – режим тестирования тракта E1, при котором внешняя линия отключается, и передаваемый комплектом сигнал будет направлен непосредственно на прием этого же комплекта. На выходной порт комплекта будет включена псевдослучайная последовательность, входной порт будет работать в режиме детектирования ошибок;
- *«Отключить тест»* – отключение режима тестирования.

5.1.2.3 Мониторинг каналов E1

В разделе отображается информация о состоянии каналов потоков E1. В верхней части поля приведена матрица каналов для потоков E1, где в строке указывается номер канала, а в столбце − номер потока (в скобках приведен протокол сигнализации, установленный для него). В нижней части − информационные таблицы и таблица управления.



Номер канала E1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Поток 1 (M2UA)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Поток 2 (M2UA)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Поток 3 (M2UA)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Поток 4 (M2UA)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Поток 5 (MediaGW)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Поток 6 (MediaGW)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Поток 7 (MediaGW)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Поток 8 (MediaGW)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Поток 9 (MediaGW)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Поток 10 (MediaGW)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Поток 11 (MediaGW)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Поток 12 (MediaGW)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Поток 13 (IUA-N)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Поток 14 (MediaGW)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Поток 15 (MediaGW)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Поток 16 (MediaGW)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Информация о соединении в потоке по каналу #	
Порт/канал	-
Связанный порт/канал	-
Связанный Callref	-
Состояние	-
Таймер состояния	-

Состояние потоков	
	NONE
	OFF
	ALARM
	LOS
	AIS
	LOF
	LOMF
	WORK/RAI
	WORK/SLIP
	WORK
	TEST

Состояние каналов	
	Off
	Idle
	Talk

Управление линком
Установить состояние "Перегрузка"
Отменить состояние "Перегрузка"
Установить состояние "Локальный отказ процессора"
Отменить состояние "Локальный отказ процессора"
Инициировать нормальный запуск сигнального звена
Инициировать аварийный запуск сигнального звена
Остановить сигнальное звено

Информация о соединении в потоке # по каналу #:

- *Порт/канал* − не используется;
- *Связанный порт/канал* − не используется;
- *Связанный Callref* − не используется;
- *Состояние* − состояние канала:
  - *Off* − канал выключен;
  - *Block* − канал заблокирован.
  - *Init* − инициализация канала;
  - *Idle* − канал в исходном состоянии;
  - *In-Dial/Out-Dial* − входящий/исходящий набор номера;
  - *In-Call/Out-Call* − входящее/исходящее занятие;
  - *In-Busy/Out-Busy* − выдача сигнала занято;
  - *Talk* − канал в разговорном состоянии;
  - *Release* − освобождение канала;
  - *Wait-Ack* − ожидание подтверждения;
  - *Wait-CID* − ожидание CgPN (AOH);
  - *Wait-Num* − ожидание набора номера;
  - *Hold* − абонент был поставлен на удержание.
- *Таймер состояния* − длительность нахождения канала в последнем состоянии;
- *Входящая категория SS7* − не используется;
- *Входящий номер CdPN* − не используется;

- *Входящий номер CgPN* − не используется;
- *Исходящая категория SS7* − не используется;
- *Исходящий номер CdPN* − не используется;
- *Исходящий номер CgPN* − не используется.

Состояние потоков − информационная таблица расшифровки графических обозначений в матрице:

- *Состояние* − статус потока:
- *NONE* − субмодуль *C4E1* отсутствует;
- *OFF* − поток выключен в конфигурации;
- *ALARM* − ошибка инициализации субмодуля C4E1;
- *LOS* − потеря сигнала;
- *AIS* − сигнал индикации аварийного состояния (сигнал, содержащий все единицы);
- *LOMF* − сигнал индикации аварийного состояния сверхцикла;
- *WORK/RAI* − индикация удаленной аварии;
- *WORK/SLIP* − индикация проскальзываний (SLIP) на потоке;
- *WORK* − поток в работе;
- *TEST* − индикация тестирования потока (PRBS test, заворот локальный и удаленный).

Состояние каналов − информационная таблица расшифровки графических обозначений в матрице:

- *Off* − канал выключен в конфигурации;
- *Idle* − канал в исходном состоянии;
- *Talk* − канал в разговорном состоянии.

При отсутствии одного из субмодулей *C4E1* выдается сообщение *«Субмодуль C4E1 не установлен, мониторинг каналов недоступен»*.

Обновление состояния канала происходит раз в 5 секунд.

Управление потоками

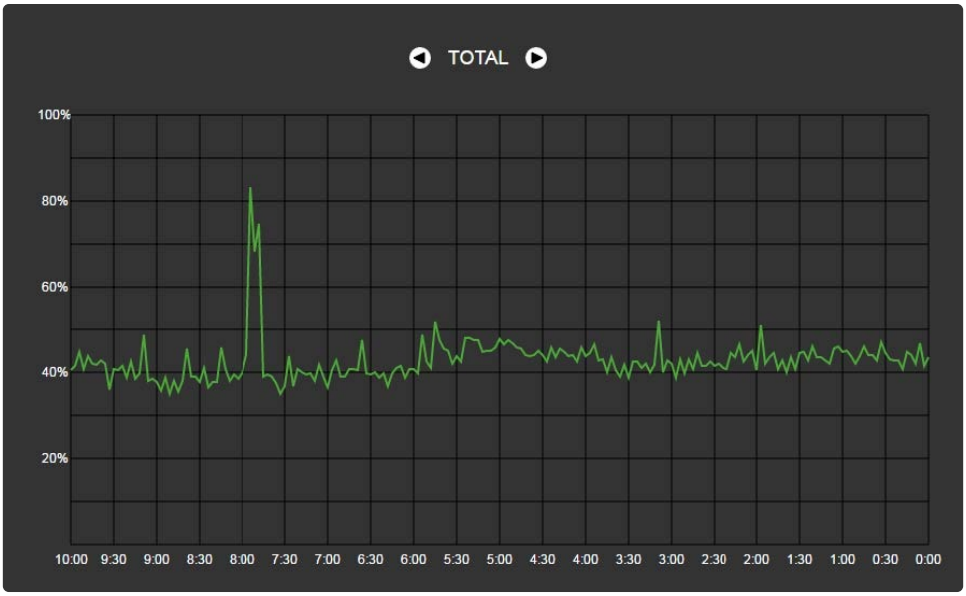
Для возможности управления потоком необходимо щелкнуть левой кнопкой мыши на его названии − поле будет выделено цветом, например, на скриншоте выше представлена информация для потока 0 (M2UA). Далее в таблице *«Управление линком»* выбрать поле с требуемым действием и щелкнуть по нему левой кнопкой мыши. На экран будет выдано всплывающее информационное сообщение о выполнении команды. «Управление линком» доступно на потоках с сигнализацией M2UA.

Управление линком − таблица управления сигнальным звеном:

- *Установить состояние «Перегрузка»* − установить состояние перегрузки сигнального звена;
- *Отменить состояние «Перегрузка»* − отменить состояние перегрузки сигнального звена;
- *Установить состояние «Локальный отказ процессора»;*
- *Отменить состояние «Локальный отказ процессора»;*
- *Инициировать нормальный запуск сигнального звена;*
- *Инициировать аварийный запуск сигнального звена;*
- *Остановить сигнальное звено.*

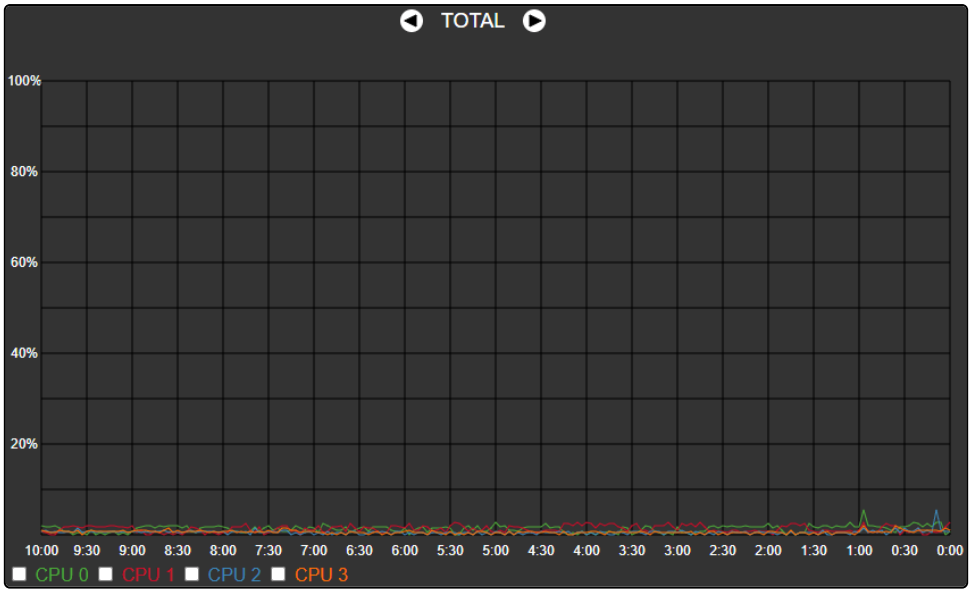
5.1.2.4 График загрузки процессора

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



Навигация между графиками мониторинга по отдельным параметрам осуществляется с помощью кнопок  и . Для облегчения визуальной идентификации на SMG-1016M все графики имеют различную цветовую окраску.

Для SMG-2016 и SMG-3016 графики имеют различную цветовую окраску для разных ядер процессора.



- *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.

5.1.2.5 *Мониторинг SFP-модулей*

В разделе отображаются индикация состояния и параметры оптической линии.

Мониторинг SFP модулей

SFP порт 0 статус	Наличие SFP модуля		Состояние сигнала	
	Модуль установлен		Сигнал установлен	
Температура, °C	Напряжение, В	Ток смещения TX, мА	Исходящая мощность, мВт	Входящая мощность, мВт
33.968	3.2718	20.073	0.2877	0.1556
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 X статус* − состояние оптического модуля:
  - *Наличие 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.

5.1.2.6 *Мониторинг front-портов коммутатора*

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

Мониторинг front-портов коммутатора

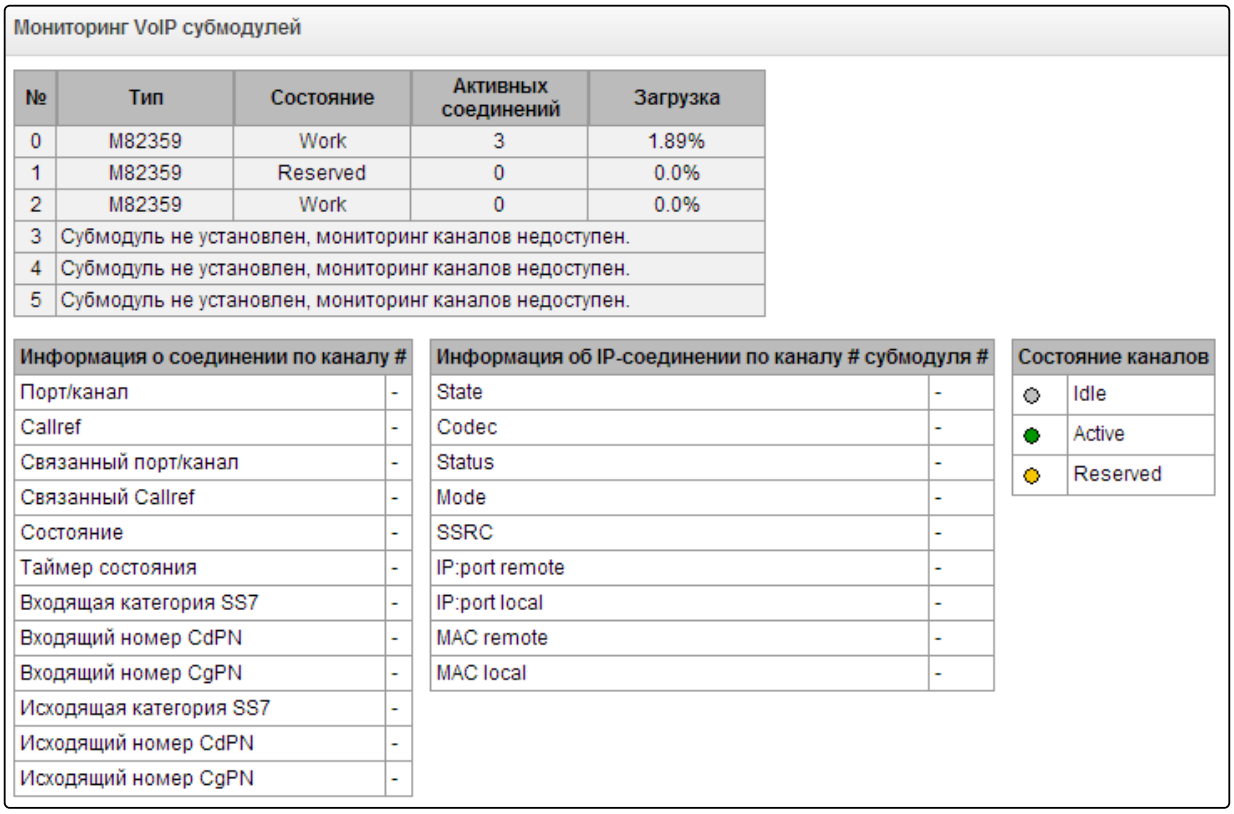
	Port 0	Port 1	Port 2 (SFP)	Port 3
Состояние линка	DOWN	UP	DOWN	UP
Скорость	N/A	100M	N/A	1000M
Режим передачи	N/A	half-duplex	N/A	full-duplex
LACP группа	-	-	-	-
Статус порта LACP	-	-	-	-
Принято байт	0	4230340 (4.0 MiB)	0	4324620 (4.1 MiB)
ошибочных пакетов	0	524	0	0
отброшено пакетов	0	0	0	0
одноадресных пакетов	0	26329	0	8769
широковещательных пакетов	0	84	0	36901
Передано байт	0	635641 (0.6 MiB)	0	3361959 (3.2 MiB)
ошибочных пакетов	0	0	0	0
одноадресных пакетов	0	4808	0	7777
широковещательных пакетов	0	138	0	137

- *Состояние линка* − состояние кабельного подключения на порту (активно/неактивно);
- *Скорость* − согласованная скорость на порту;
- *Режим передачи* − режим, используемый для передачи данных (half-/full-duplex);
- *LACP-группа* − здесь отображается LACP-канал, в который входит порт и его статус (UP/DOWN);
- *Статус порта LACP* − режим, в котором находится порт (active/backup);

- *Принято байт* − накопительный счётчик принятых байт, включая различные виды принятых пакетов;
- *Передано байт* − накопительный счётчик переданных байт, включая различные виды переданных пакетов.

5.1.2.7 Мониторинг VoIP-субмодулей

В разделе отображается информация об установленных субмодулях SM-VP, а также информация о состоянии каналов этих субмодулей.


Мониторинг VoIP субмодулей

№	Тип	Состояние	Активных соединений	Загрузка
0	M82359	Work	3	1.89%
1	M82359	Reserved	0	0.0%
2	M82359	Work	0	0.0%
3	Субмодуль не установлен, мониторинг каналов недоступен.			
4	Субмодуль не установлен, мониторинг каналов недоступен.			
5	Субмодуль не установлен, мониторинг каналов недоступен.			

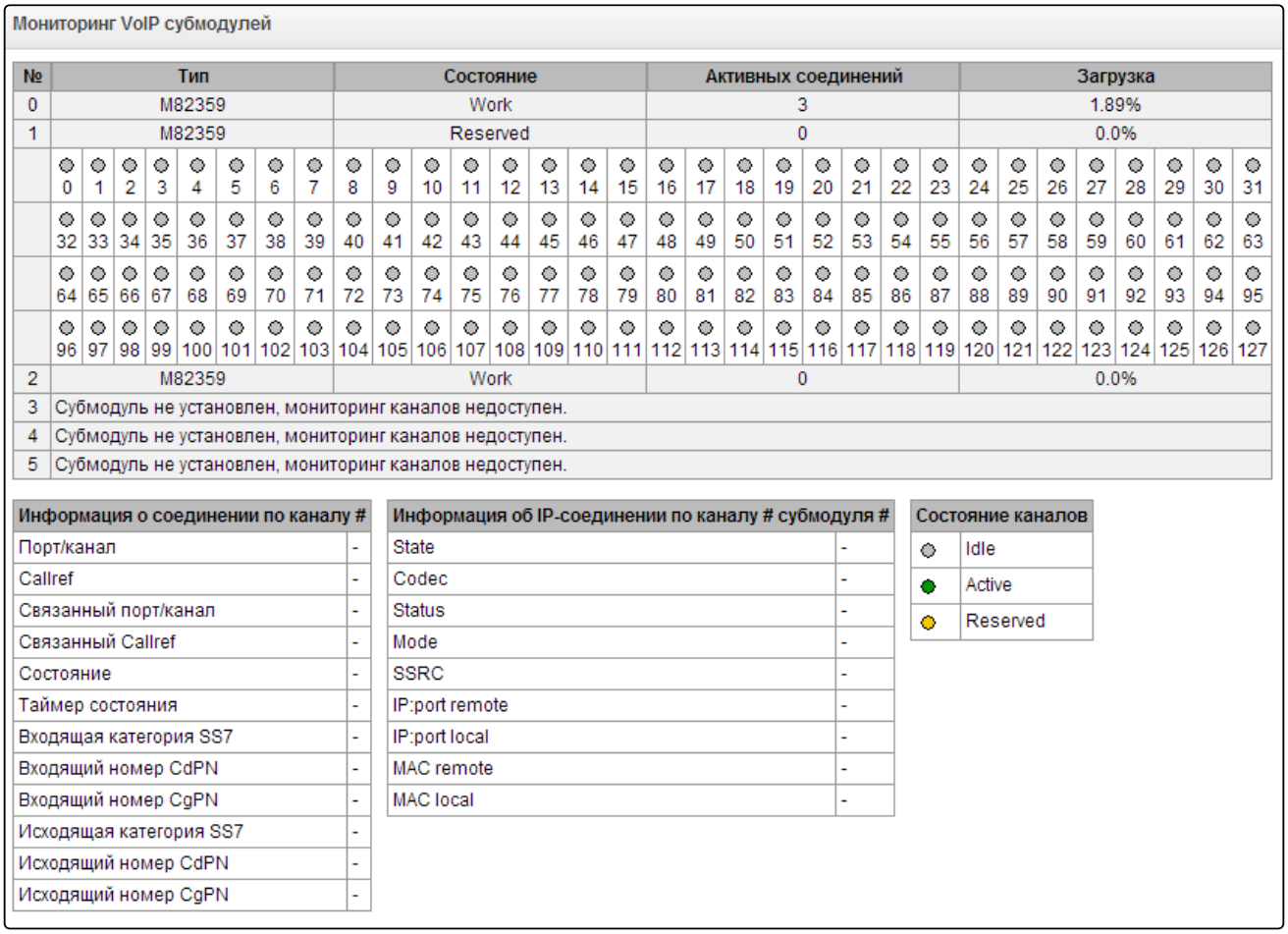
Информация о соединении по каналу #	
Порт/канал	-
Callref	-
Связанный порт/канал	-
Связанный Callref	-
Состояние	-
Таймер состояния	-
Входящая категория SS7	-
Входящий номер CdPN	-
Входящий номер CgPN	-
Исходящая категория SS7	-
Исходящий номер CdPN	-
Исходящий номер CgPN	-

Информация об IP-соединении по каналу # субмодуля #	
State	-
Codec	-
Status	-
Mode	-
SSRC	-
IP:port remote	-
IP:port local	-
MAC remote	-
MAC local	-

Состояние каналов	
	Idle
	Active
	Reserved

- *№* − порядковый номер субмодуля SM-VP*;*
- *Тип* − тип установленного субмодуля*;*
- *Состояние:*
  - *Not Present* − не установлен;
  - *No init* − не инициализирован, не было попыток инициализации*;*
  - *Off* − отключен, начало загрузки субмодуля*;*
  - *Wait Ack* − ожидание подтверждения от ЦП после загрузки субмодуля;
  - *Failed* − субмодуль не отвечает;
  - *Work* − нормальная работа субмодуля*;*
  - *Recovery* − от субмодуля не поступают контрольные пакеты;
  - *Reserved* − субмодуль зарезервирован под нужны СОРМ;
  - *SSW.Sorm* − субмодуль используется СОРМ-посредником;
- *Активных соединений* − количество активных соединений на субмодуле в текущий момент времени;
- *Загрузка* − процент использования ресурсов субмодуля в текущий момент времени.

Для мониторинга состояния каналов необходимо кликнуть на строке с номером требуемого субмодуля левой кнопкой мыши. Чтобы скрыть информацию, необходимо повторно кликнуть на данной строке.



Информация о соединении по каналу #:

- *Порт/канал* − данные о порте/канале:
  - протокол сигнализации (VoIP);
  - координаты порта: № субмодуля VoIP: № канала.
- *Callref* − внутренний идентификатор вызова;
- *Связанный порт/канал* − данные о связанном порте/канале:
  - протокол сигнализации связанного порта (PRI/SS7/VoIP);
  - координаты связанного порта: № потока: № канала для PRI/SS7 либо № субмодуля VoIP: № канала для VoIP.
- *Связанный Callref* − идентификатор вызова по связанному каналу;
- *Состояние* − состояние канала:
  - *Off* − канал выключен;
  - *Block* − канал заблокирован;
  - *Init* − инициализация канала;
  - *Idle* − канал в исходном состоянии;
  - *In-Dial/Out-Dial* − входящий/исходящий набор номера;
  - *In-Call/Out-Call* − входящее/исходящее занятие;
  - *In-Busy/Out-Busy* − выдача сигнала занято;
  - *Talk* − канал в разговорном состоянии;
  - *Release* − освобождение канала;
  - *Wait-Ack* − ожидание подтверждения;
  - *Wait-CID* − ожидание CgPN (АОН);
  - *Wait-Num* − ожидание набора номера;
  - *Hold* − абонент был поставлен на удержание.
- *Таймер состояния* − длительность нахождения канала в последнем состоянии;
- *Входящая категория SS7* − не используется;
- *Входящий номер CdPN* − не используется;

- *Входящий номер CgPN* – не используется;
- *Исходящая категория SS7* – не используется;
- *Исходящий номер CdPN* – не используется;
- *Исходящий номер CgPN* – не используется.

Состояния каналов:

- *Idle (серый)* – исходное состояние, канал готов обслужить вызов;
- *Active (зеленый)* – активное состояние, канал занят активным вызовом;
- *Reserved (желтый)* – канал зарезервирован под служебные нужды (выдача тоновых сигналов «занято», «КПВ», «ответ станции») либо под новый вызов с его участием.

Для просмотра подробной информации по каналу необходимо выделить его в таблице нажатием левой кнопки мыши.

Информация об IP-соединении по каналу # субмодуля #:

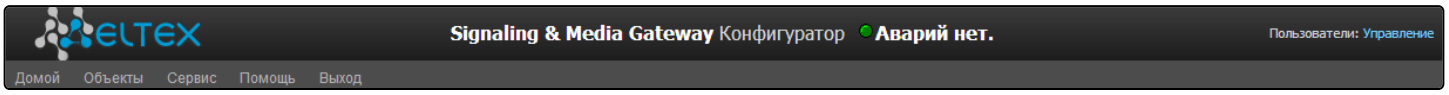
- *State* – состояние канала (описание приведено выше);
- *Codec* – используемый кодек (в квадратных скобках указывается Payload Type);
- *Status* – статус передачи медиаинформации, варианты:
  - *Good* – канал в работе;
  - *Loss of RTP* – потеря встречного RTP потока (при истечении «Таймаут ожидания RTP-пакетов»);
  - *VBD* – по каналу установлена связь в режиме передачи данных;
  - *T38* – по каналу установлена факсимильная связь с использованием протокола T.38.
- *Mode* – режим работы медиаканала:
  - *sendrecv* – канал работает в двустороннем режиме (прием и передача);
  - *sendonly* – канал работает в одностороннем режиме, только на передачу;
  - *recvonly* – канал работает в одностороннем режиме, только на прием;
  - *inactive* – канал не активен, прием и передача неактивны.
- *SSRC* – значение поля SSRC (Synchronizatoin Source) для исходящего от устройства RTP-потока;
- *IP:port remote* – удаленный IP-адрес и порт источника RTP-потока;
- *IP:port local* – локальный IP-адрес и порт источника RTP-потока;
- *MAC remote* – удаленный MAC-адрес источника RTP-потока;
- *MAC local* – локальный MAC-адрес источника RTP-потока.

Ниже таблиц с состоянием канала расположена кнопка *«Разъединить»*, которая позволяет принудительно разорвать соединение (поддержано только для mgcp).

5.1.2.8 Сигнализация об авариях. Журнал аварийных событий

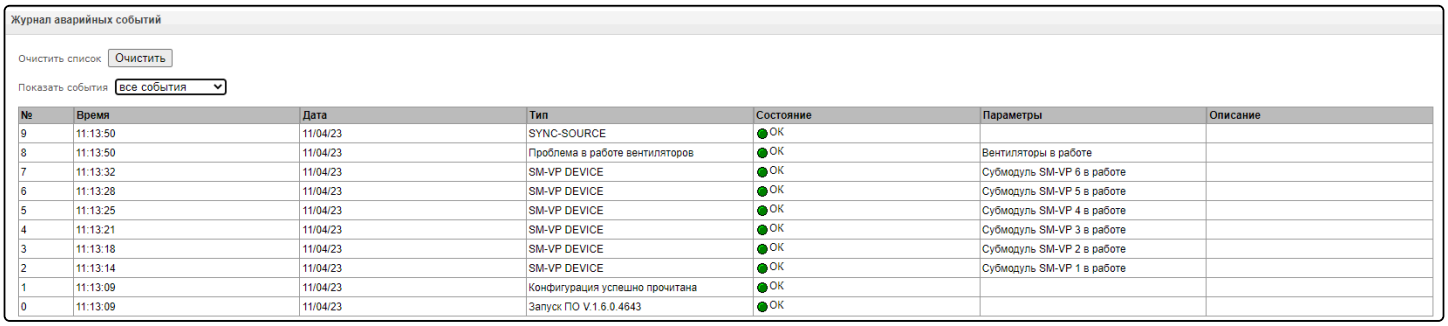
При возникновении аварии информация о ней выводится в заголовке web-конфигуратора с указанием номера аварийного потока неисправного модуля. Если активных аварий несколько, в заголовке web-конфигуратора выводится наиболее критичная в текущий момент авария.

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



Аварийное сообщение	Расшифровка
Конфигурация не прочитана	Ошибка файла конфигурации
Нет связи с MEGACO-модулем	Авария программного модуля, отвечающего за работу протокола H.248/Megaco
Авария потока E1	Авария потока E1
Синхронизация от менее приоритетного источника	Синхронизация от локального источника. Все заданные источники нерабочие
Удаленная авария потока E1	Удаленная авария потока E1
Синхронизация от менее приоритетного источника	Потеря основного источника синхронизации, текущий источник менее приоритетный
Нет связи с VoIP-субмодулем	Нет связи с субмодулем SM-VP
Оперативная память заканчивается	Авария о высоком использовании ресурсов оперативной памяти
Отсутствует питание БП	На одном из БП отсутствует питание первичной сети
Высокая температура процессора	Температура 70 °C – предупреждение; 85 °C – авария; 100 °C – критическая авария
Высокая загрузка процессора	Загрузка выше 90 % – предупреждение; выше 95 % – авария
Проблема в работе вентиляторов	Один или несколько вентиляторов не в работе
Заканчивается свободное место на диске	Заканчивается свободное место на одном из внешних накопителей

Журнал аварийных событий



№	Время	Дата	Тип	Состояние	Параметры	Описание
9	11:13:50	11/04/23	SYNC-SOURCE	OK		
8	11:13:50	11/04/23	Проблема в работе вентиляторов	OK	Вентиляторы в работе	
7	11:13:32	11/04/23	SM-VP DEVICE	OK	Субмодуль SM-VP 6 в работе	
6	11:13:28	11/04/23	SM-VP DEVICE	OK	Субмодуль SM-VP 5 в работе	
5	11:13:25	11/04/23	SM-VP DEVICE	OK	Субмодуль SM-VP 4 в работе	
4	11:13:21	11/04/23	SM-VP DEVICE	OK	Субмодуль SM-VP 3 в работе	
3	11:13:18	11/04/23	SM-VP DEVICE	OK	Субмодуль SM-VP 2 в работе	
2	11:13:14	11/04/23	SM-VP DEVICE	OK	Субмодуль SM-VP 1 в работе	
1	11:13:09	11/04/23	Конфигурация успешно прочитана	OK		
0	11:13:09	11/04/23	Запуск ПО V.1.6.0.4643	OK		

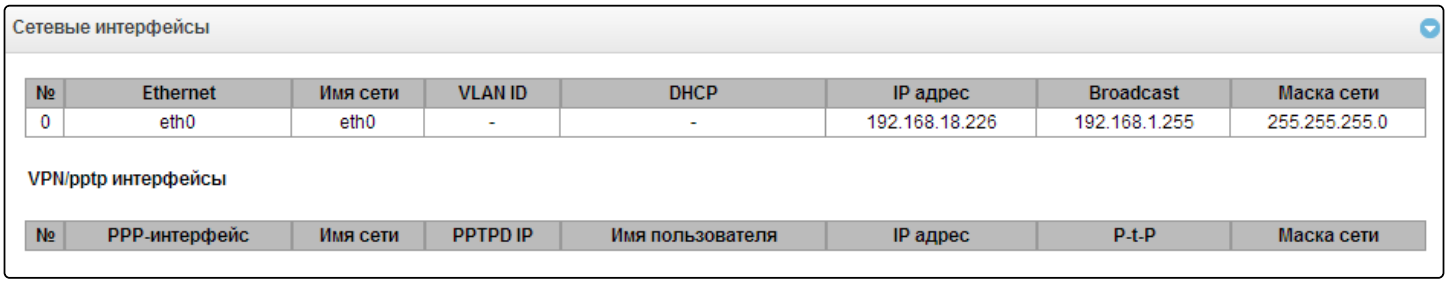
В меню «*Журнал аварийных событий*» выводится список аварийных событий, ранжированных по дате, времени и событиям. В событиях «*Только активные*» показаны актуальные аварии на устройстве в данный момент. В событиях «*все события*» отображается вся доступная информация об авариях. Также присутствует кнопка «*Очистить*», которая удаляет из текущего журнала все информационные сообщения и нормализованные аварии.

Таблица аварий:

- *№* − порядковый номер аварии;
- *Время* − время возникновения аварии в формате ЧЧ:ММ:СС;
- *Дата* − дата возникновения аварии в формате ДД/ММ/ГГ;
- *Тип* − тип аварии:
  - *CONFIG* − критическая авария, авария файла конфигурации;
  - *MEGACO-MODULE* − критическая авария, авария программного модуля, отвечающего за работу протокола Megaco;
  - *STREAM* − критическая авария, поток E1 не в работе;
  - *SM-VP DEVICE* − авария, неисправность модуля SM-VP;
  - *SYNC* − авария синхронизации, пропадание источника синхронизации;
  - *STREAM-REMOTE* − предупреждение, удаленная авария потока E1.
- *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, также требуется вмешательство персонала;
  - *Предупреждение, желтый индикатор* − авария, которая не влияет на оказание услуг связи;
  - *OK, зеленый индикатор* − авария устранена;
- *Параметры* − текстовое описание деталей аварии. В зависимости от типа аварии имеет следующий вид:
  - *CONFIG*;
  - *MEGACO-MODULE* − нет связи с MEGACO-модулем;
  - *STREAM* − авария потока E1 XX, где XX − номер потока;
  - *SM-VP DEVICE* − нет связи с VoIP-субмодулем XX, где XX − номер субмодуля SM-VP.

5.1.2.9 *Мониторинг интерфейсов*

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


Сетевые интерфейсы

№	Ethernet	Имя сети	VLAN ID	DHCP	IP адрес	Broadcast	Маска сети
0	eth0	eth0	-	-	192.168.18.226	192.168.1.255	255.255.255.0

VPN/pptp интерфейсы

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

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

VPN/pptp интерфейсы

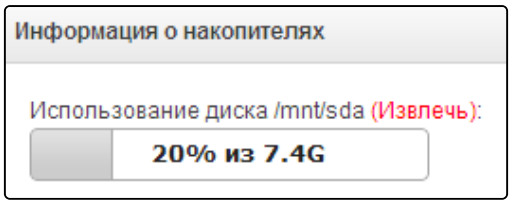
- *PPP-интерфейс* – имя интерфейса;
- *Имя сети* – имя, с которым ассоциированы заданные сетевые настройки;
- *PPTPD IP* – IP-адрес PPTP-сервера для подключения;
- *Имя пользователя* – идентификатор пользователя;
- *IP адрес*, *P-t-P, Маска сети* – сетевые настройки интерфейса.

5.1.2.10 *Информация о накопителях*

В данном разделе отображается информация о подключенных к устройству внешних накопителях.

- *Извлечь* – по нажатию на ссылку будет произведено безопасное извлечение накопителя.

Мониторинг → Информация о накопителях



Имена внешних накопителей привязаны к интерфейсным портам:

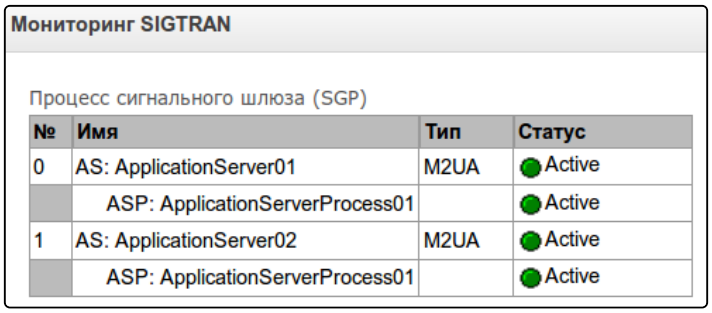
> ⚠ **Именование устройств происходит по принципу /dev/sdX.**

SMG1016M	
SSD № 1	/dev/sda*
SSD № 2	/dev/sdb*
USB	/dev/sdc*
SMG2016	
HDD № 1	/dev/sda*
HDD № 2	/dev/sdb*

USB	/dev/sdc*
SMG3016	
HDD № 1	/dev/sda*
HDD № 2	/dev/sdb*
USB	/dev/sdc*

5.1.2.11 Мониторинг SIGTRAN

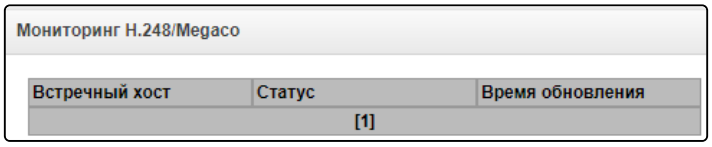
В данном разделе отображается состояние серверов приложений AS- и ASP-процессов (процессов сервера приложений).



- *Красный* − процесс не в работе;
- *Желтый* − процесс в промежуточном состоянии;
- *Зеленый* − процесс в работе.

5.1.2.12 Мониторинг H.248/Megaco

В данном разделе отображается состояние соединения по протоколу H.248/Megaco с контроллером медиашлюзов.



- *Встречный хост* − адрес контроллера медиашлюзов;
- *Статус* − состояние подключения к контроллеру медиашлюзов;
- *Время обновления* − время последнего подключения к контроллеру медиашлюзов.

Таблица 17 − Примеры выводимых сообщений об авариях

5.1.3 Источники синхронизации

Для синхронизации устройства от нескольких источников применяется алгоритм приоритетного списка. Суть его заключается в следующем: при пропадании синхросигнала от текущего источника просматривается список на наличие активных сигналов от источников с более низким приоритетом. При восстановлении сигнала от источника с более высоким приоритетом происходит переключение на него. Также возможно иметь несколько источников с одинаковым приоритетом, при этом при восстановлении сигнала с тем же приоритетом переключения не произойдет.

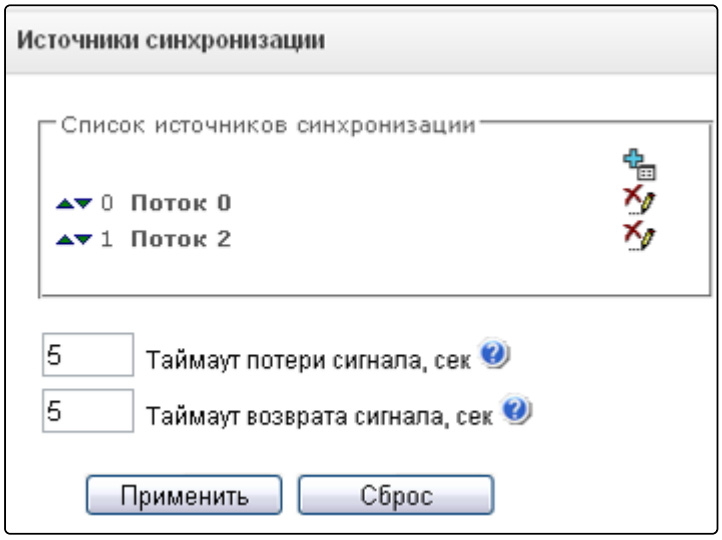
Можно задать до 18 источников синхронизации (от любого из 16 потоков E1 и от двух внешних источников).

Формирование списка происходит при помощи кнопок:

– «*Добавить источник*»;

– «*Удалить*».

Изменение приоритета источника производится кнопками 0 «*Вверх*»/«*Вниз*» напротив каждого источника. Самым приоритетным считается значение «0», самый низкий приоритет имеет значение «14».



- *Таймаут потери сигнала* – временной интервал, в течение которого не происходит переключение на менее приоритетный источник синхронизации при пропадании сигнала. Если сигнал восстановится в течение этого интервала, то переключения не произойдет;
- *Таймаут возврата* – временной интервал, в течение которого должен быть активен вновь появившийся синхросигнал от более приоритетного источника до того, как на него будет осуществлено переключение.

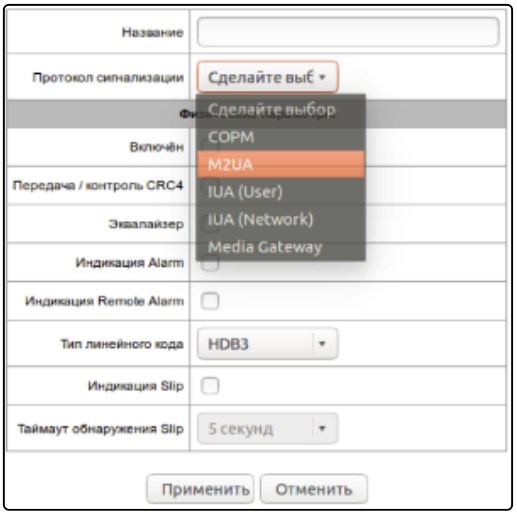
Если на потоке, с которого принимается синхросигнал, настроен D-канал, необходимо убедиться, что D-канал находится в работе, иначе синхросигнал с потока захвачен не будет, что приведет к появлению проскальзываний (slip).

5.1.4 Потоки E1

В этом разделе производится настройка сигнализации и параметров каждого потока E1.

5.1.4.1 Выбор протокола сигнализации

Выбор протокола сигнализации, используемого на потоке, производится в выпадающем списке «*Протокол сигнализации*».



Устройство поддерживает следующие протоколы сигнализации:

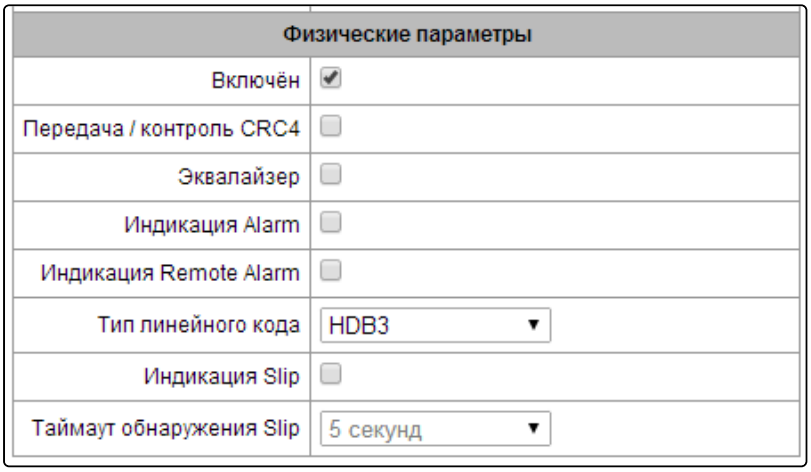
- COPM[1];
- M2UA;
- IUA (User);
- IUA (Network);
- Media Gateway.

---

[1] *При наличии установленной лицензии на данный функционал.*

5.1.4.2 Настройка физических параметров

Физические параметры:



- *Название* – наименование потока E1;
- *Включен* – физическое включение потока;
- *Передача/контроль CRC4* – формирование контрольной суммы CRC4 на передаче и контроль на приеме;
- *Эквалайзер* – при установленном флаге происходит усиление передаваемого сигнала;
- *Индикация Alarm* – при установленном флаге в случае локальной аварии на потоке будет индикация об аварии (на устройстве загорится индикатор *Alarm*, авария будет занесена в журнал аварий);

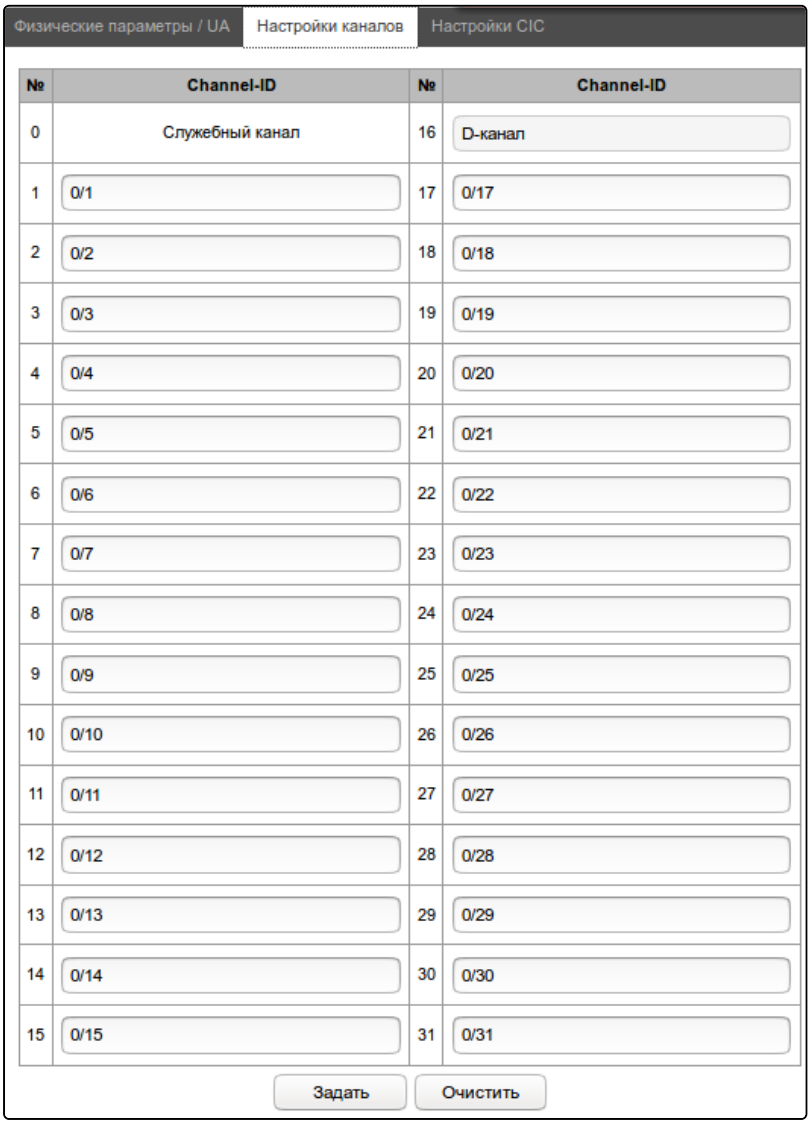
- *Индикация Remote Alarm* – при установленном флаге в случае удаленной аварии на потоке будет индикация об аварии (на устройстве загорится индикатор *Alarm*, авария будет занесена в журнал аварий);
- *Тип линейного кода* – тип кодирования информации в канале(HDB3, AMI);
- *Индикация Slip* – при установленном флаге в случае обнаружения проскальзывания в приемном тракте будет индикация об аварии;
- *Таймаут обнаружения Slip* – периодичность опроса параметров потока у платы, если на данном потоке обнаружилось проскальзывание, то в течение данного таймаута шлюз будет сигнализировать об аварии.

5.1.4.3 Настройка протокола M2UA/IUA/Media gateway

При выборе протокола M2UA либо IUA устройство будет работать в качестве сигнального («*Интерфейс управления B-каналами*» не выбран) либо одновременно сигнального и медиашлюза. При выборе Media gateway устройство будет работать только в качестве медиашлюза.

⚠ **СОРМ-ирование вызовов будет работать только на потоках с установленной сигнализацией M2UA.**

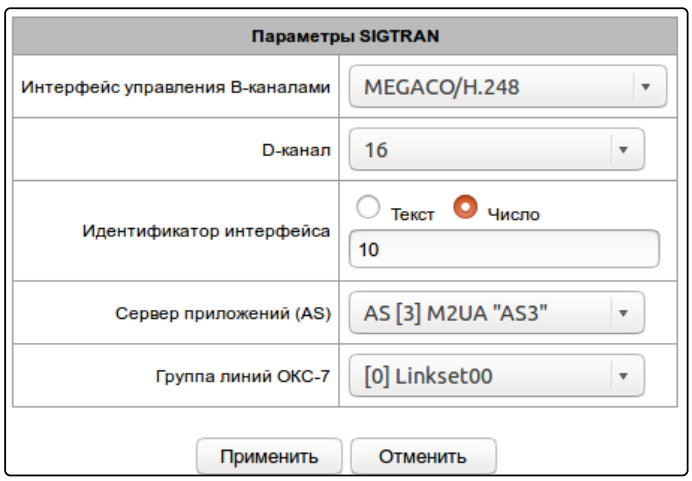
Параметры SIGTRAN:



- *Интерфейс управления B-каналами* – выбор интерфейса и протокола управления медиаканалами (Megaco, MGCP);
- *D-канал* – номер канала, используемого в качестве сигнального в потоке E1 (не используется в режиме Media gateway);
- *Идентификатор интерфейса* – идентификатор интерфейса сигнального линка, связывает сигнальный поток в канале потока E1 с обрабатывающим его сервером приложений AS. Значение может быть текстом либо числом, такое же значение должно быть настроено на сервере приложений AS (не используется в режиме Media gateway);
- *Сервер приложений (AS)* – выбор сервера приложений, с которым будет взаимодействовать процесс сигнального шлюза SGP, обрабатывающий сигнальный линк данного потока E1 (не используется в режиме Media gateway);
- *Группа линий ОКС* – группа разговорных каналов, обеспечивающих взаимодействие между двумя точками PC (point code). Предназначена для изоляции каналов CIC между взаимодействующими точками PC. Если группа линий ОКС-7 не назначена на потоке, то СОРМ-ирование вызовов по данному потоку осуществляться не будет[1].

---

[1]*Опция доступна только при наличии лицензии на функционал СОРМ.*

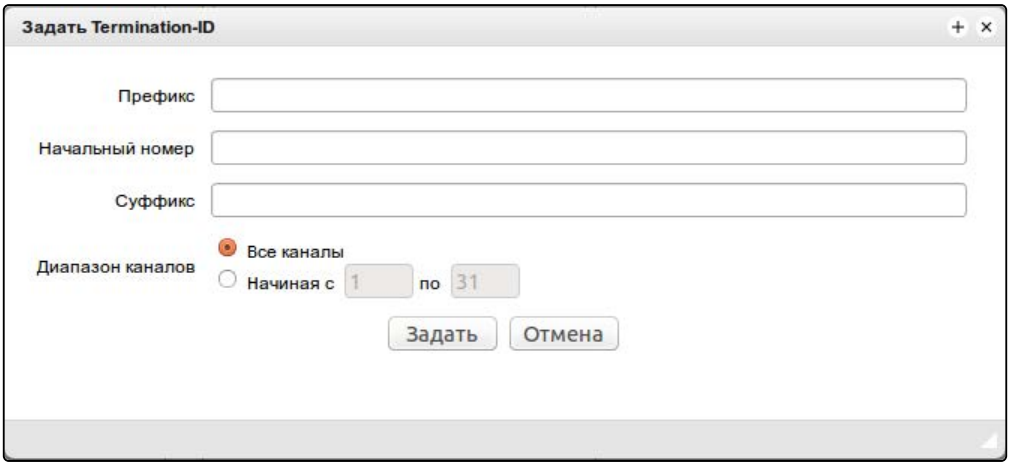


Вкладка «Настройки каналов»

- *№* – номер канала в структуре потока E1;
- *Channel-ID* – логический идентификатор физической терминации, назначается каждому каналу потока E1. Используя данный идентификатор, контроллер медиашлюзов управляет определенным каналом потока E1 на медиашлюзе платформы SMG.

Для автоматической нумерации разговорных каналов необходимо нажать кнопку *«Задать»*.

При этом откроется следующее меню:

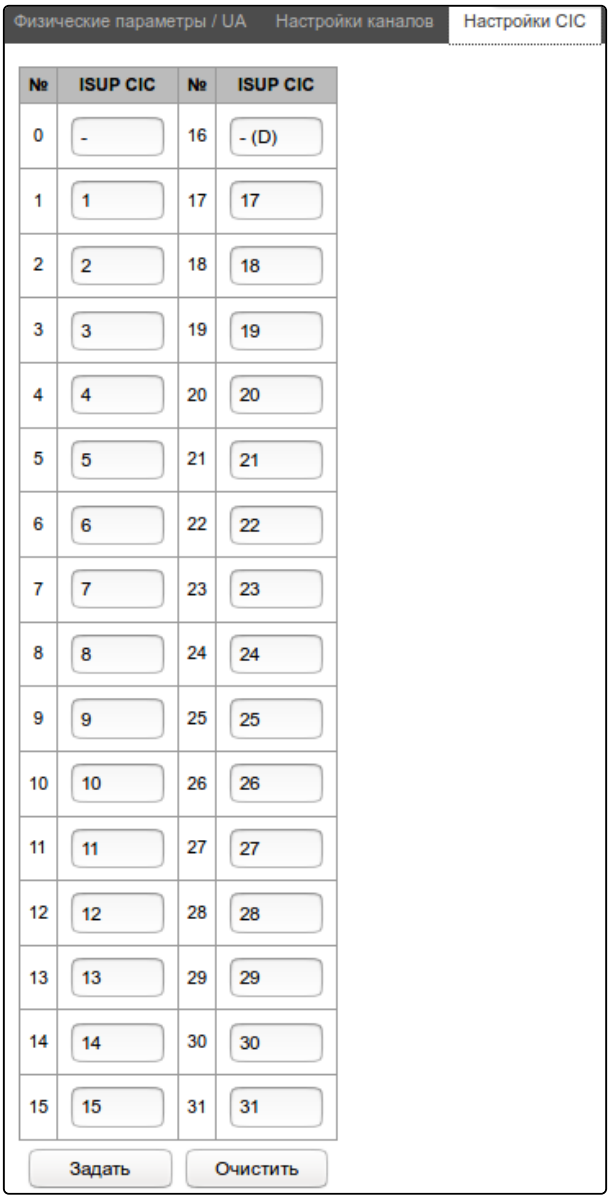


- *Префикс* – префиксная часть идентификатора физической терминации, приписывается в начале идентификатора, одинакова для всех физических терминаций;
- *Начальный номер* – номер первой физической терминации для первого разговорного канала потока E1;
- *Суффикс* – постфиксная часть идентификатора физической терминации, приписывается в конце идентификатора, одинакова для всех физических терминаций;
- *Диапазон каналов* – выбор значений в данном блоке позволяет назначить нумерацию для всех каналов потока E1 либо для указанного диапазона каналов.

Вкладка «Настройки CIC»

> **Данный раздел доступен при наличии лицензии COPM.**

Вкладка доступна только при наличии лицензии с поддержкой протокола COPM и только для уровня адаптации M2UA.



- *№* − номер канала в структуре потока E1;
- *ISUP CIC* − код идентификации канала CIC, настроенный для данного канала на взаимодействующих TDM АТС. Каналы объединяются линксетами, то есть в рамках одного линксета не может быть двух каналов с одинаковыми CIC.

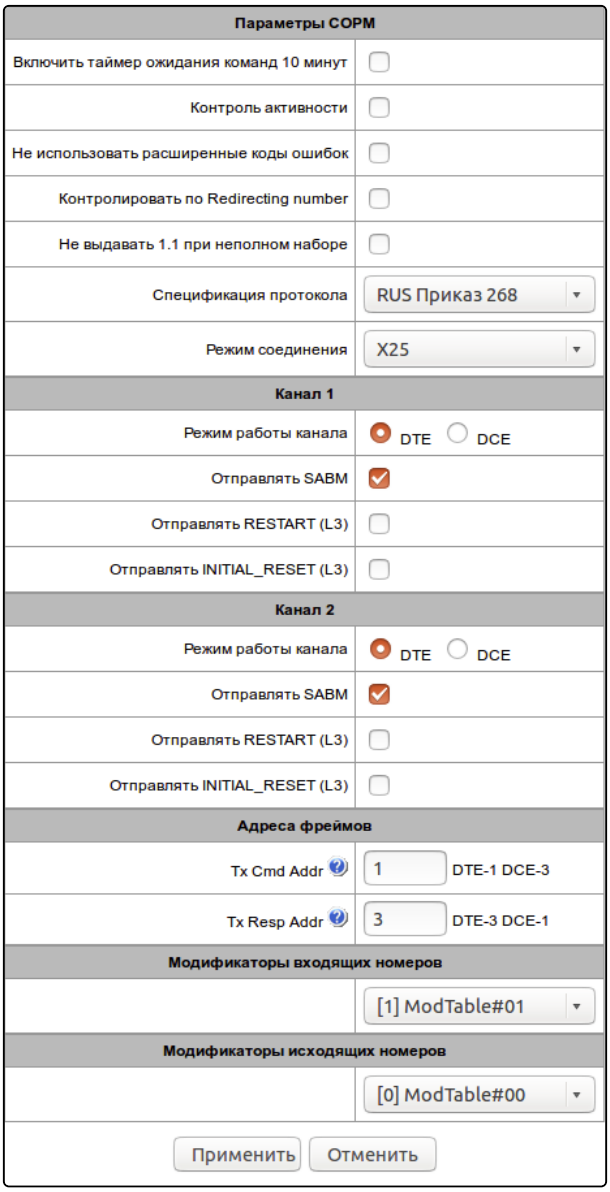
Для автоматической нумерации разговорных каналов необходимо нажать кнопку *«Задать»*.

При этом откроется следующее меню:

- *Начальный номер* − номер первого разговорного канала;
- *Шаг нумерации* − шаг нумерации каналов. Каждому последующему каналу будет присвоен номер на «шаг нумерации» больше относительно предыдущего канала;
- *Последний номер* − отображает номер, который будет присвоен последнему каналу CIC в выбранном диапазоне;
- *Диапазон КИ* − выбор значений в данном блоке позволяет назначить нумерацию для всех каналов потока, либо для указанного диапазона каналов.

5.1.4.4 *Настройка протокола сигнализации СОРМ*

> ⚠ **Данный раздел доступен при наличии лицензии СОРМ.**



- *Включить таймер ожидания команд 10 мин* – включить/выключить таймаут ожидания приема команд от ПУ СОРМ (реализовано согласно пункту 1.5 Приказа №70 Госкомсвязи России от 20.04.1999);
- *Контроль активности* – контроль активности обмена сообщениями на уровне L1, в случае если в течение 15 секунд хотя бы по одному из каналов не было принято пакетов, произойдет сброс и переинициализация фреймера потока E1;
- *Не использовать расширенные коды ошибок* – при установленном флаге в ответ на команду с некорректными параметрами будут отправляться сообщения о невыполнении команды только с признаками, определенными в приказе №268. В противном случае будут использоваться признаки невыполнения команд производителя, позволяющие более точно определить причину отказа команды. Перечень стандартных кодов и кодов производителя приведен в Приложении Д;
- *Контролировать по Redirecting number* – использовать номер из поля Redirecting number (либо diversion в протоколе SIP) для передачи на ПУ. При поступлении звонка с Redirecting number (либо diversion в протоколе SIP) изначально происходит сравнение номера из поля Calling Party Number с номерами, стоящими на контроле, затем, в случае если совпадение не найдено, с номером из поля Redirecting number (либо diversion в протоколе SIP). В случае если опция не стоит сравнения с Redirecting number (либо diversion в протоколе SIP) не происходит.
- *Не выдавать 1.1 при неполном наборе* – не выдавать сообщение 1.1 при неполном наборе;
- *Спецификация протокола* – выбор спецификации СОРМ, по которой будет работать устройство:
  - *RUS Приказ 70* – спецификация СОРМ для приказа Госкомсвязи России от 20.04.1999 №70;
  - *RUS Приказ 268* – спецификация СОРМ для приказа Минкомсвязи России от 19.11.2012 №268;
  - *KZ* – спецификация СОРМ для республики Казахстан.
- *Режим соединения:*
  - *X25* – сигнальные каналы КПД организуются через протокол X25, используя 30-31 канал потока E1;
  - *TCP* – сигнальные каналы КПД организуются через протокол TCP. Настройки активные только при выборе режима соединения *TCP*.
- *Порт 1* – виртуальный TCP-порт для организации сигнального канала КПД-1.
- *Порт 2* – виртуальный TCP-порт для организации сигнального канала КПД-2.
- *Интерфейс* – выбор сетевого интерфейса устройства.

Режим работы каналов

- *Канал 1* – блок настройки параметров канала передачи управляющей информации от ПУ СОРМ;
- *Канал 2* – блок настройки параметров канала передачи информации о контролируемых соединениях от SMG.

Настройки каналов

- *Режим работы канала*:
  - *DTE* – при установленном флаге тип устройства – DTE (передатчик информации);
  - *DCE* – при установленном флаге тип устройства – DCE (принимает данные от DTE-устройств).
- *Отправлять SABM* – при установленном флаге в канал передается сообщение о начале процедуры инициализации соединения;
- *Отправлять RESTART (L3)* – передача сообщения «рестарт уровня 3» при установлении соединения с ПУ СОРМ;
- *Отправлять INITIAL_RESET (L3)* – передача сообщения «сброс уровня 3» при установлении соединения с ПУ СОРМ.

Адреса фреймов

- *TxCmd Addr* – адрес командного фрейма;
- *TxResp Addr* – адрес ответного фрейма.

Модификаторы входящих номеров – выбор таблицы модификаторов, предназначенной для анализа и модификации номера телефона абонента в поступающих от пульта СОРМ-сообщениях.

Модификаторы исходящих номеров – выбор таблицы модификаторов, предназначенной для анализа и модификации номера телефона абонента в отправляемых на пульт СОРМ-сообщениях.

Не допускается установка протокола СОРМ на нескольких потоках. После выбора протокола СОРМ на одном из потоков необходимо произвести перезапуск ПО. Заводской пароль СОРМ "123456".

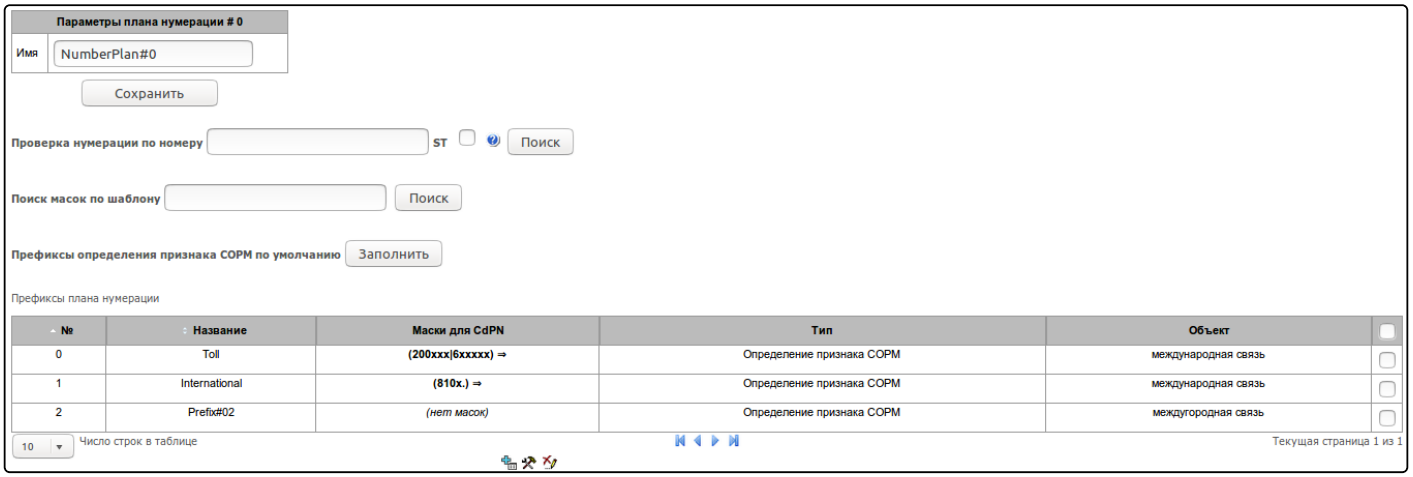
5.1.5 План нумерации

Данный раздел доступен при наличии лицензии СОРМ.

В этом разделе конфигурируется план нумерации устройства для возможности отбора номеров в целях осуществления мероприятий СОРМ. Критерием для отбора номера являются префиксы с масками по номеру вызываемого абонента – CdPN (Called Party Number).

При поступлении команды *«постановка абонента на контроль»* (команда №5) параметры, принятые в команде, анализируются на корректность в соответствии с планом нумерации. Проверяется соответствие запрашиваемого номера с масками префиксов и соответствие признака номера (абонент России, абонент другой страны) с параметром «направление/объект».

- *Междугородная связь* – абонент России;
- *Международная связь* – абонент другой страны;



Параметры плана нумерации:

- *Имя* – название плана нумерации.
- *Проверка нумерации по номеру* – проверка возможности маршрутизации по номеру, введенному в данное поле. Проверка осуществляется по маске вызываемого абонента.
- *Поиск масок по шаблону* – поиск префикса по шаблону номера. В результате проверки выводятся данные о возможности отбора по данному номеру.
- *Префиксы определения признака СОРМ по умолчанию* – позволяет заполнить значения по умолчанию для префиксов «определения признака СОРМ».

5.1.5.1 Работа с префиксами в плане нумерации

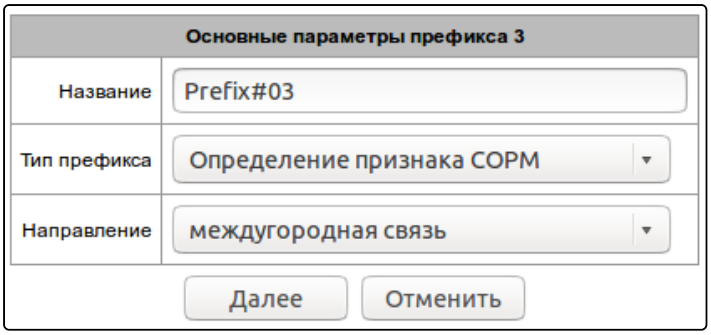
Для создания нового префикса необходимо выбрать меню *«Объекты»* – *«Добавить объект»*, либо нажать на кнопку  под списком и в открывшейся форме заполнить параметры префикса.

Для редактирования префикса необходимо в таблице префиксов дважды щелкнуть левой кнопкой мыши по строке с префиксом или выделить префикс и нажать кнопку  под списком.

Для удаления префикса необходимо выделить префикс и нажать кнопку  под списком либо выбрать меню *«Объекты» − «Удалить объект»*.

Основные параметры префикса:

- *Название* − имя плана нумерации;
- *Тип префикса* − доступно только одно значение «Определения признака СОРМ»;
- *Направление* − направление транзитного вызова, определяется в соответствии с признаком номера, используемого в СОРМ, для абонентов России выбирается междугороднее, для абонентов другой страны − международное.

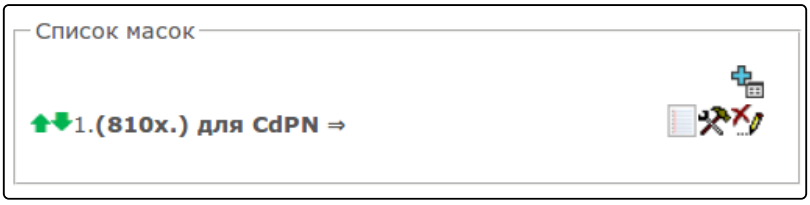


После нажатия на кнопку *«Далее»* становится доступным для редактирования *«Список масок»*.

Список масок:

Для созданных префиксов в разделе «Список масок» конфигурируются маски для отбора номеров, соответствующих выбранному в префиксе признаку.

Формирование списка происходит при помощи кнопок:



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

Зеленые стрелки слева  от созданной маски позволяют перемещать запись в таблице, настраивая их порядок (приоритет).

- *Маска* − шаблон или набор шаблонов, с которым сравнивается номер, принятый в команде №5 для постановки на контроль.

Остальные параметры не используются.

5.1.5.2 Описание маски номера и ее синтаксис

Маска номера представляет собой набор шаблонов *templ*, разделенных спецсимволом ‘|’. Маска должна быть заключена в круглые скобки. (templ) равнозначно (templ1|templ2|...|templN).

Синтаксис:

- **X** или **x** − любая цифра;
- ***** − символ *;
- **#** − символ #;
- **0-9** − цифры от 0 до 9;
- **.** − спецсимвол «точка» обозначает, что символ, стоящий перед ним, может повторяться произвольное количество раз (но не более 30 символов на весь номер), например: **(34 x .)** − всевозможные комбинации номеров, начинающихся на “34”;

- **[ ]** – указание диапазона (через тире), либо перечисление (без пробелов, запятых и прочих символов между цифрами) префиксов, например:
  диапазон **([1-5]XXX)** – все 4-значные номера, начинающиеся на 1,2,3,4 или 5;
  перечисление **([138]xx)** – все 3-значные номера, начинающиеся на 1,3 или 8).
- **{min, max}** – указание количества повторений символа, стоящего перед скобками, например: **(1x{3,5})** – означает, что любых цифр (**x**) может быть от 3 до 5 и равнозначно маске **(1xxx|1xxxx|1xxxxx).**
- **|** – вертикальная черта. Логическое **ИЛИ** – используется для разделения шаблонов в маске.

Если в плане нумерации присутствуют пересекающиеся префиксы, то при обработке номера в плане нумерации приоритетным будет префикс с наиболее точной маской для конкретного номера, например:
Префикс 1: (2xxxx)
Префикс 2: (23xxx)
При поступлении в план нумерации номера 23456 он обработается по префиксу 2.
Также маски, содержащие произвольное количество повторений (x.) либо диапазон количества повторений {min, max}, менее приоритетны, чем маски с указанием точного количества символов, например:
Префикс 1: (2x{4,7})
Префикс 2: (23xxx)
При поступлении в план нумерации номера 23456, он обработается по префиксу 2.
Маски с указанным диапазоном количества повторений {min, max} приоритетней, чем маски с любым количеством повторений (x.), например:
Префикс 1: (2x.)
Префикс 2: (2x{4,7})
При поступлении в план нумерации номера 23456 он обработается по префиксу 2.

5.1.6 Настройки SIGTRAN

В этом разделе конфигурируются настройки взаимодействия процессов сигнального шлюза SGP с серверами приложений AS и их процессами ASP.

Структурная схема процесса SGP приведена на рисунке ниже:

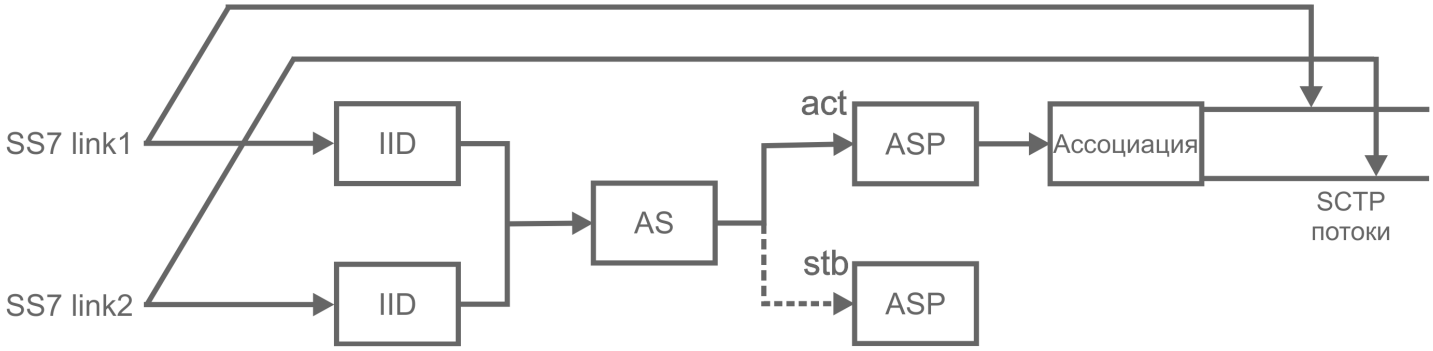
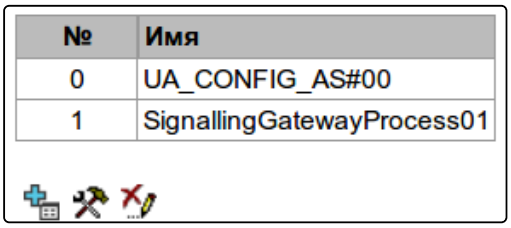


Рисунок 30 – Структурная схема процесса SGP



Протоколы семейства SIGTRAN (M2UA, IUA) ассоциируют идентификаторы интерфейсов (IID) с физическими интерфейсами (канальными интервалами потока E1, использующимися под передачу сигнализации). Процессы сигнального шлюза SGP ассоциируют идентификаторы интерфейсов (IID) с транспортными потоками SCTP в IP-сети. Ассоциация IID-SCTP создается только после получения от ASP сообщения ASP Active для данного идентификатора интерфейса IID. Таким образом, создается сигнальная связка между линком ОКС-7 в TDM-сети и транспортным SCTP потоком в IP-сети.

Для создания нового процесса SGP необходимо выбрать меню *«Объекты» – «Добавить объект»* либо нажать на кнопку  под списком процессов.

Для изменения настроек процесса SGP необходимо выделить процесс и нажать кнопку  под списком.

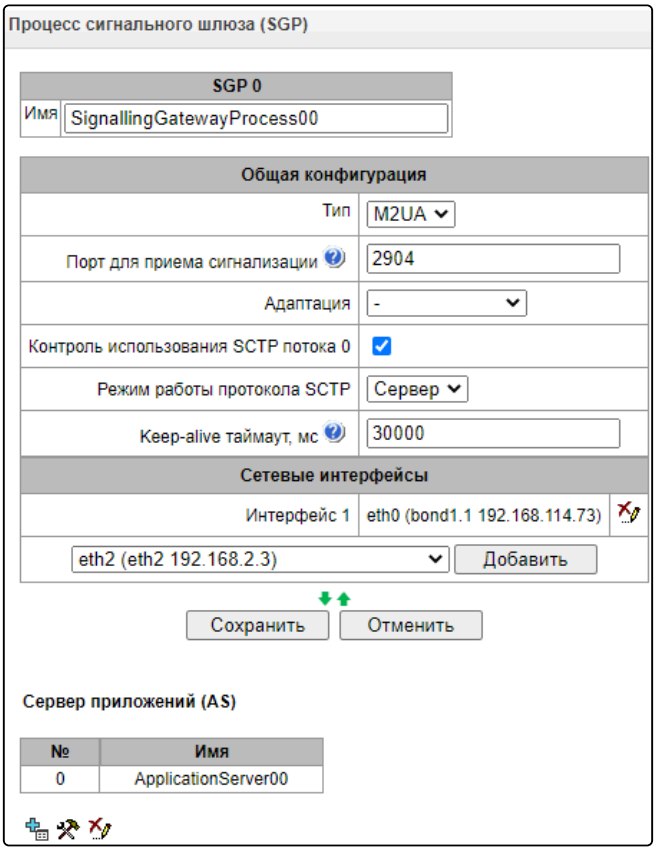
Для удаления процесса SGP необходимо выделить процесс и нажать кнопку  под списком.

Настройки процесса сигнального шлюза SGP

SGP X

- *Имя* − произвольное имя, назначаемое процессу сигнального шлюза.

Общая конфигурация



- *Тип* − протокол уровня адаптации (M2UA, IUA) семейства протоколов SIGTRAN. M2UA предназначен для адаптации со вторым уровнем MTP2 сигнализации ОКС-7, IUA предназначен для адаптации со вторым уровнем Q.921 сигнализации ISDN сети;
- *Порт для приема сигнализации* − транспортный порт SCTP для приема сигнальных сообщений протокола M2UA;
- *Адаптация* − адаптация работы под особенности реализации протокола другими вендорами;
- *Контроль использования SCTP потока 0* − рекомендацией определено, что нулевой SCTP-поток должен использоваться только для передачи управляющих (management) сообщений. При установленном флаге все не управляющие сообщения, принятые не в нулевом потоке будут отклонены, при снятом флаге они будут обработаны;
- *Режим работы протокола SCTP* − определяет в каком режиме будет работать протокол SCTP данного процесса SGP. В режиме клиента шлюз будет сам инициировать процесс установления SCTP-коннекции, в режиме сервера шлюз будет ждать, когда встречная сторона начнет процесс установления SCTP-коннекции;
- *Keep-alive таймаут, мс* − период передачи контрольных сообщений по протоколу SCTP для поддержания коннекции.

Сетевые интерфейсы

В данном разделе выбираются сетевые интерфейсы, через которые процесс сигнального шлюза будет организовывать SCTP-потоки.

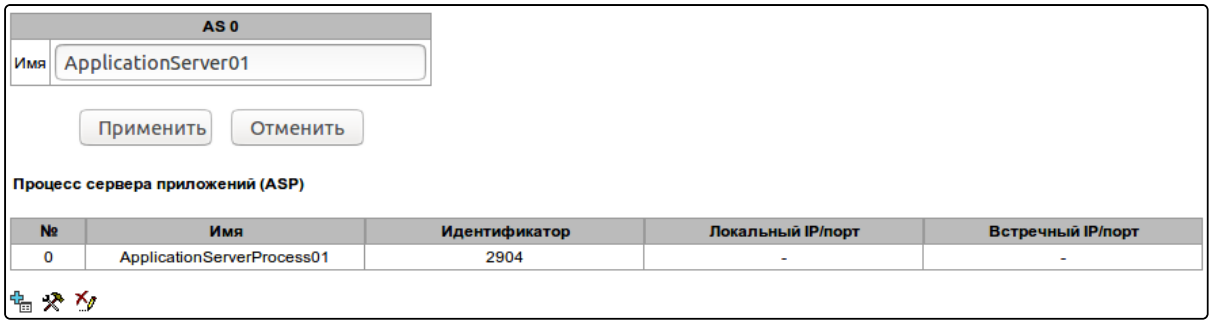
Сервер приложений (AS)

Для создания нового сервера приложений AS необходимо выбрать меню *«Объекты» − «Добавить объект»* либо нажать на кнопку под списком  серверов.

Для изменения настроек сервера приложений AS необходимо выделить сервер и нажать кнопку  под списком.

Для удаления сервера приложений AS необходимо выделить сервер и нажать кнопку  под списком.

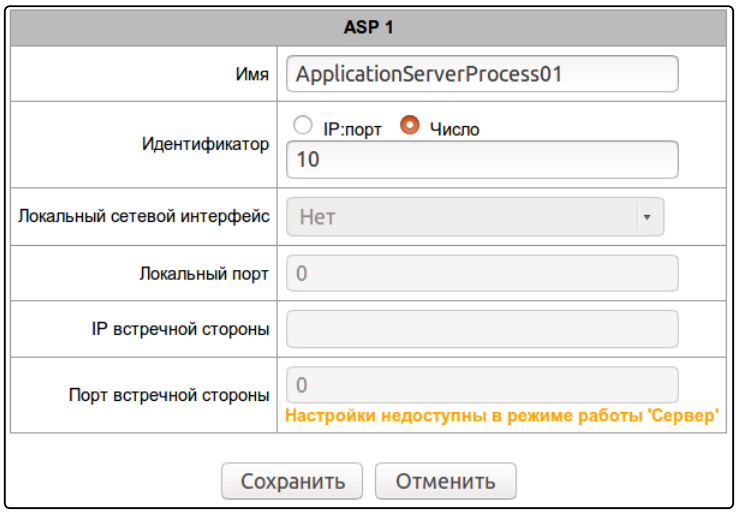
Настройки сервера приложений AS



- *Имя* − произвольное имя, назначаемое серверу приложений.

> **При наличии лицензии COPM сервер приложений ассоциируется с транковой группой, и данное имя будет соответствовать имени транковой группы, по которой может быть осуществлен контроль.**

Процессы сервера приложений (ASP)



Для создания нового процесса сервера приложений ASP необходимо выбрать меню *«Объекты» − «Добавить объект»* либо нажать на кнопку  под списком процессов.
Для изменения настроек процесса сервера приложений ASP необходимо выделить процесс и нажать кнопку  под списком.

Для удаления процесса сервера приложений ASP необходимо выделить процесс и нажать кнопку  под списком.

- *Имя* − произвольное имя, назначаемое процессу сервера приложений;
- *Идентификатор* − идентификатор процесса сервера приложений, связывает процесс с обрабатывающим его сервером приложений AS. Значение может быть текстом либо числом, такое же значение должно быть настроено на взаимодействующей стороне для процесса SGP.

Следующие параметры зависят от режима работы протокола SCTP, настройки будут активны только в режиме работы «Клиент», они позволяют настроить параметры локального сокета – сетевого адреса и транспортного порта на которые шлюз будет принимать сигнальные сообщения для данного процесса сервера приложений и удаленного сокета – сетевого адреса и транспортного порта на которые шлюз будет передавать сигнальные сообщения для данного процесса сервера приложений:

- *Локальный сетевой интерфейс* – сетевой интерфейс, на котором процесс сигнального шлюза будет принимать сигнальные сообщения для данного процесса сервера приложений;
- *Локальный порт* – транспортный порт на котором процесс сигнального шлюза будет принимать сигнальные сообщения для данного процесса сервера приложений;
- *IP встречной стороны* – сетевой адрес, на который процесс сигнального шлюза будет передавать сигнальные сообщения для данного процесса сервера приложений;
- *Порт встречной стороны* – транспортный порт, на который процесс сигнального шлюза будет передавать сигнальные сообщения для данного процесса сервера приложений.

5.1.7 Настройки медиа-интерфейсов

В этом разделе конфигурируются интерфейсы, предназначенные для передачи медиатрафика.

5.1.7.1 Интерфейсы MGCP

Данный раздел доступен при наличии лицензии MGCP.

5.1.7.1.1 Конфигурация

В данном разделе настраиваются общие параметры конфигурации стека MGCP, индивидуальные настройки для каждого направления, работающего по протоколу MGCP.

Протокол MGCP (Media Gateway Control Protocol) – протокол контроля медиашлюзов, является протоколом сигнализации, используемом в распределенных системах IP-телефонии, состоящих из контроллера медиашлюзов (MGC) и медиашлюзов (MG).

Интерфейсы MGCP

№	Название	Префикс для MGCP-окончаний	Идентификатор шлюза	MGCP Call Agent IP-адрес и порт	Кодеки	Способ передачи DTMF	Факс
0	MGCP-interface00	smg	192.168.118.88	192.168.118.10:2727	G.711A	RFC2833	Detect (T.38 only)
1	MGCP-interface01	smg		192.168.118.10:2727	G.711A G.711U	Inband	Detect
2	MGCP-interface02	smg		192.168.118.10:2727	G.711A G.711U	Inband	Detect (T.38 only)
3	MGCP-interface03	smg		192.168.118.10:2727	G.711A G.711U	Inband	Detect (T.38 only)

Максимально возможно создать до 4 интерфейсов. Для создания, редактирования и удаления интерфейсов MGCP используется меню *«Объекты» – «Добавить объект»*, *«Объекты» – «Редактировать объект»* и *«Объекты» – «Удалить объект»*, а также кнопки:

– *«Добавить интерфейс»;*

– *«Редактировать параметры интерфейса»;*

– *«Удалить интерфейс»*.

Сигнальный процессор шлюза выполняет функции кодирования аналогового речевого трафика, данных факса/модема в цифровые сигналы, а также обратного декодирования. Шлюз поддерживает следующие кодеки: G.711A, G.711U, G.729, протокол T.38 и CLEARMODE.

G.711 – представляет собой ИКМ-кодирование без сжатия речевой информации. Данный кодек должен быть обязательно поддержан всеми производителями VoIP-оборудования. Кодеки G.711A и G.711U

отличаются друг от друга законом кодирования (A-закон – линейное кодирование и U-закон – нелинейное). Кодирование по U-закону применяется в Северной Америке, а по A-закону в Европе.

G.726 – является стандартом ITU-T адаптивной импульсно-кодовой модуляции – ADPCM и описывает передачу голоса полосой в 16, 24, 32, и 40 Кбит/с.

G.726-32 – замещает собой G.721, который описывает ADPCM передачу голоса полосой в 32 Кбит/с.

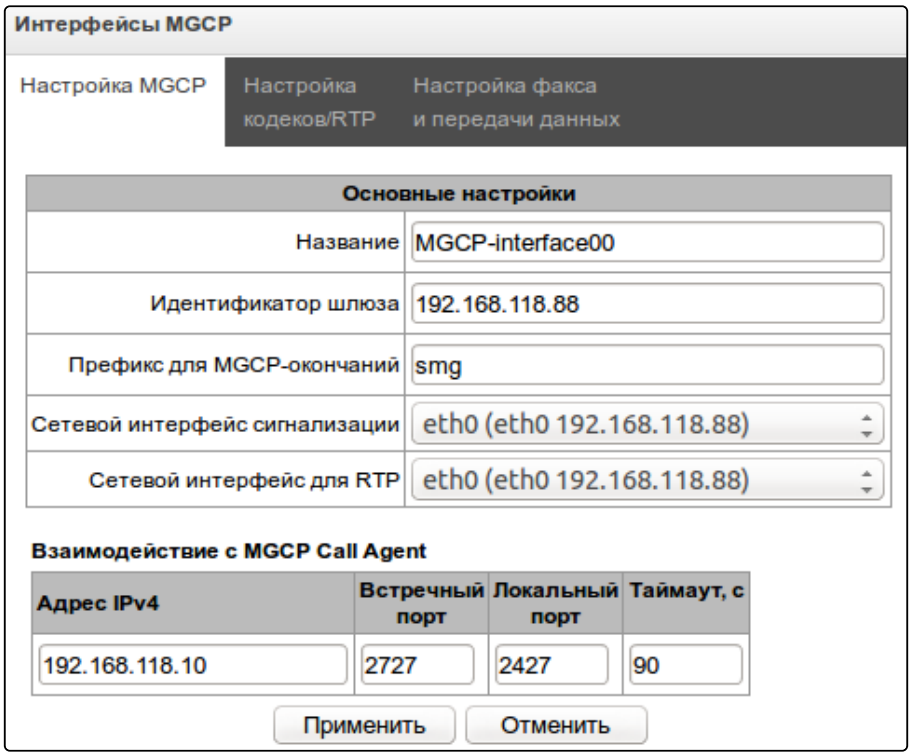
G.723.1 – кодек со сжатием речевой информации, предусматривает два режима работы: 6.3 Кбит/с и 5.3 Кбит/с. Кодек G.723.1 имеет детектор речевой активности и обеспечивает генерацию комфортного шума на удаленном конце в период молчания (Annex A).

G.729 – также является кодеком со сжатием речевой информации и обеспечивает скорость передачи 8 Кбит/с. Аналогично кодеку G.723.1, кодек G.729 поддерживает детектор речевой активности и обеспечивает генерацию комфортного шума (Annex B).

T.38 – стандарт, описывающий передачу факсимильных сообщений в реальном времени через IP-сети. Сигналы и данные, передаваемые факсимильным аппаратом, кодируются в пакеты протокола T.38. В формируемые пакеты может вводиться избыточность – данные из предыдущих пакетов, что позволяет осуществлять надежную передачу факса по нестабильным каналам.

CLEARMODE – режим, в котором не используется кодирование/декодирование сигнала. Организуется для прозрачной передачи цифровой информации 64 Кбит/с (RFC4040).

1 **Вкладка «Настройка MGCP»**



Основные настройки

- *Название* – наименование интерфейса;
- *Идентификатор шлюза* – идентификатор медиашлюза. Может быть доменным именем, либо IP-адресом, протоколом MGCP не рекомендуется использовать IP-адрес в качестве идентификатора шлюза;
- *Префикс для MGCP-окончаний* – префикс, который будет использоваться при нумерации физических терминаций (каналов потока E1) шлюза. Данный префикс будет подставляться в начало идентификатора физической терминации Termination-ID (см. раздел Настройка протокола M2UA/IUA/Media gateway);
- *Сетевой интерфейс сигнализации* – выбор сетевого интерфейса для приема и передачи сигнальных сообщений протокола MGCP;

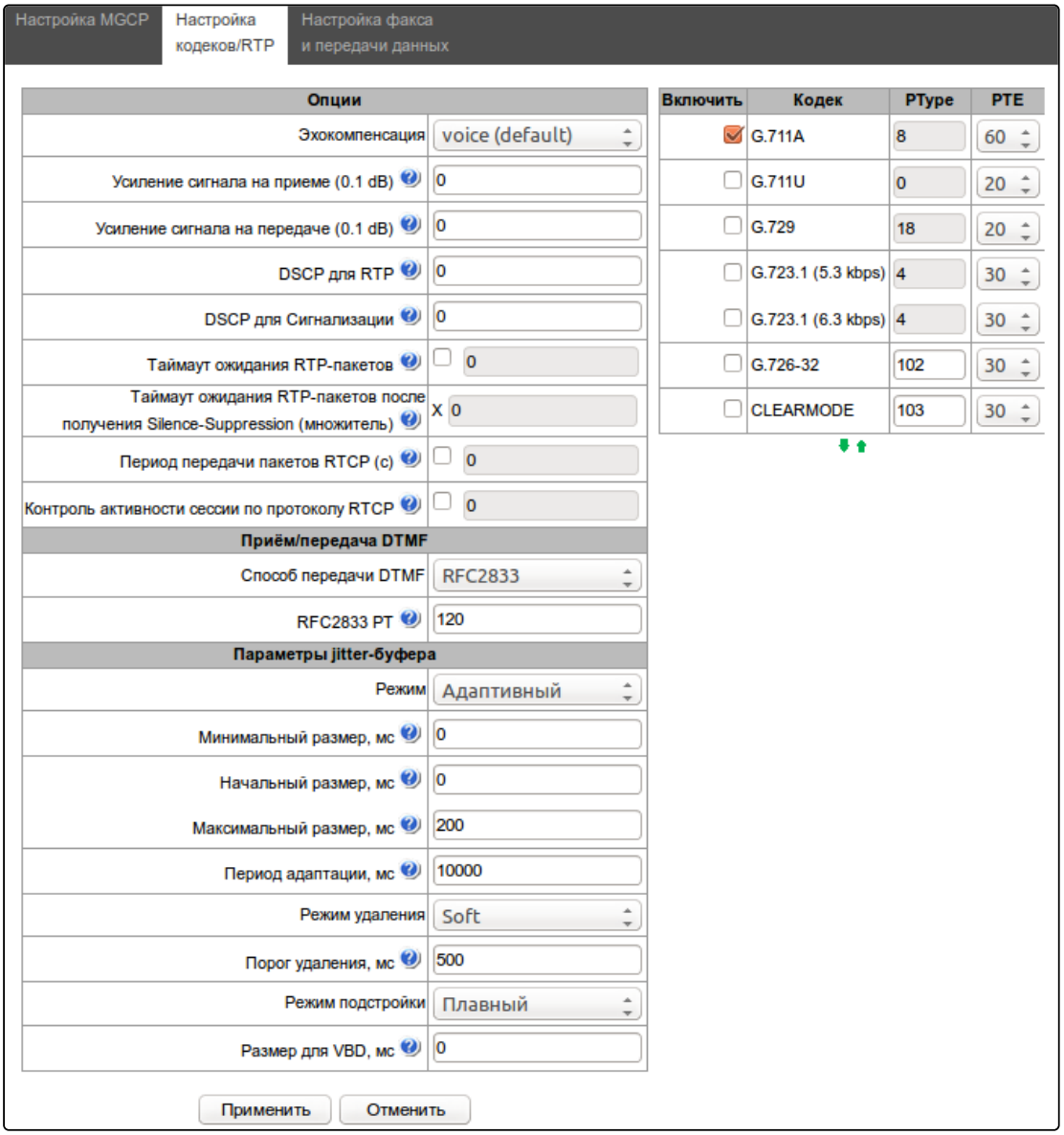
- *Сетевой интерфейс для RTP* − выбор сетевого интерфейса для приема и передачи голосового трафика.

Взаимодействие с MGCP Call Agent

В данной таблице описываются параметры взаимодействия с контроллером медиашлюзов (MGC):

- *Адрес IPv4* − IP-адрес контроллера медиашлюзов;
- *Встречный порт* − сигнальный UDP-порт контроллера медиашлюзов, принимающий сообщения протокола MGCP;
- *Локальный порт* − локальный сигнальный UDP порт шлюза, на котором будут приниматься сообщения протокола MGCP;
- *Таймаут, с* − период контроля доступности контроллера медиашлюзов. С данным интервалом шлюз будет отправлять на контроллер контрольные сообщения NOTIFY, при отсутствии ответа на них принимается решение, что контроллер стал недоступным и инициируется процедура рестарта интерфейса.

2 **Вкладка «Настройка кодеков RTP»**



Опции:

- *Эхокомпенсация* − режим эхокомпенсации:
  - *voice (default)* − эхокомпенсаторы включены в режиме передачи голосовой информации;

    - *voice nlp-off* – эхокомпенсаторы включены в голосовом режиме, нелинейный процессор NLP выключен. В случае когда уровни сигналов на передаче и приеме сильно различаются, слабый сигнал может быть подавлен нелинейным процессором NLP. Для предотвращения подавления используется данный режим работы эхокомпенсаторов;
    - *modem* – эхокомпенсаторы включены в режиме работы модема (фильтрация постоянной составляющей сигнала выключена, контроль процессором NLP выключен, генератор комфортного шума выключен);
    - *off* – не использовать эхокомпенсацию (данный режим установлен по умолчанию).
- *Усиление сигнала на приеме (0.1 dB)* – громкость принимаемого сигнала, усиление/ослабление уровня сигнала, принятого от взаимодействующего шлюза;
- *Усиление сигнала на передаче (0.1 dB)* – громкость передаваемого сигнала, усиление/ослабление уровня сигнала, передаваемого в сторону взаимодействующего шлюза;
- *DSCP для RTP* – тип сервиса (DSCP) для RTP и UDPTL (T.38) пакетов;
- *DSCP для сигнализации* – тип сервиса (DSCP) для MGCP-пакетов;
- *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 отклоняется;
- *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 отклоняется;
- *Период передачи пакетов RTCP (с)* – период времени в секундах (5–65535 с), через который устройство отправляет контрольные пакеты по протоколу RTCP. При отсутствии установленного флага протокол RTCP не используется;
- *Контроль активности сессии по протоколу RTCP* – функция контроля состояния разговорного тракта, принимает значения из диапазона 5–65535. Количество интервалов времени (*RTCP timer*), в течение которого ожидаются пакеты протокола RTCP со встречной стороны. При отсутствии пакетов в заданном периоде времени установленное соединение разрушается. Значение контрольного периода определяется по формуле: ***RTCP timer * RTCP control period*** секунд. При отсутствии установленного флага функция выключена.

Приём/передача DTMF:

- *Способ передачи DTMF* – способ передачи DTMF через IP-сеть;
    - *inband* – в пакетах протокола RTP, внутриполосно;
    - *RFC 2833* – в пакетах протокола RTP, согласно рекомендации rfc2833;
    - *MGCP-NOTIFY* – внеполосно, по протоколу MGCP, используются сообщения NOTIFY.

Для возможности использования донабора во время разговора убедитесь, что аналогичный метод передачи сигналов DTMF настроен на контроллере медиашлюзов.

- *RFC 2833 PT* – тип динамической нагрузки, используемой для передачи пакетов *DTMF* по RFC2833. Разрешенные для использования значения – от 96 до 127. Рекомендация RFC2833 определяет передачу сигналов DTMF посредством RTP-протокола. Данный параметр должен согласовываться с аналогичным параметром взаимодействующего шлюза (наиболее часто используемые значения: 96, 101);

Параметры jitter-буфера:

- *Режим* – режим работы джиттер-буфера: фиксированный либо адаптивный;

- *Минимальный размер, мс* − размер фиксированного джиттер-буфера либо нижняя граница (минимальный размер) адаптивного джиттер-буфера. Диапазон допустимых значений от 0 до 200 мс;
- *Начальный размер, мс* − начальное значение адаптивного джиттер-буфера. Диапазон допустимых значений от 0 до 200 мс;
- *Максимальный размер, мс* − верхняя граница (максимальный размер) адаптивного джиттер-буфера в миллисекундах. Диапазон допустимых значений от «минимального размера» до 200 мс;
- *Период адаптации, мс* − время адаптации буфера к нижней границе при отсутствии нарушений в порядке следования пакетов;
- *Режим удаления* − режим адаптации буфера. Определяет, каким образом будут удаляться пакеты при адаптации буфера к нижней границе:
    - *Soft* − используется интеллектуальная схема выбора пакетов для удаления, превысивших порог;
    - *Hard* − пакеты, задержка которых превысила порог, немедленно удаляются.
- *Порог удаления, мс* − порог немедленного удаления пакетов в миллисекундах. При росте буфера и превышении задержки пакета свыше данной границы пакеты немедленно удаляются. Диапазон допустимых значений от максимального размера до 500 мс;
- *Режим подстройки* − выбор режима подстройки адаптивного джиттер-буфера при его увеличении (плавный/моментальный);
- *Размер для VBD, мс* − размер фиксированного джиттер-буфера, используемого при передаче данных в режиме VBD (модемной связи). Диапазон допустимых значений от 0 до 200 мс.

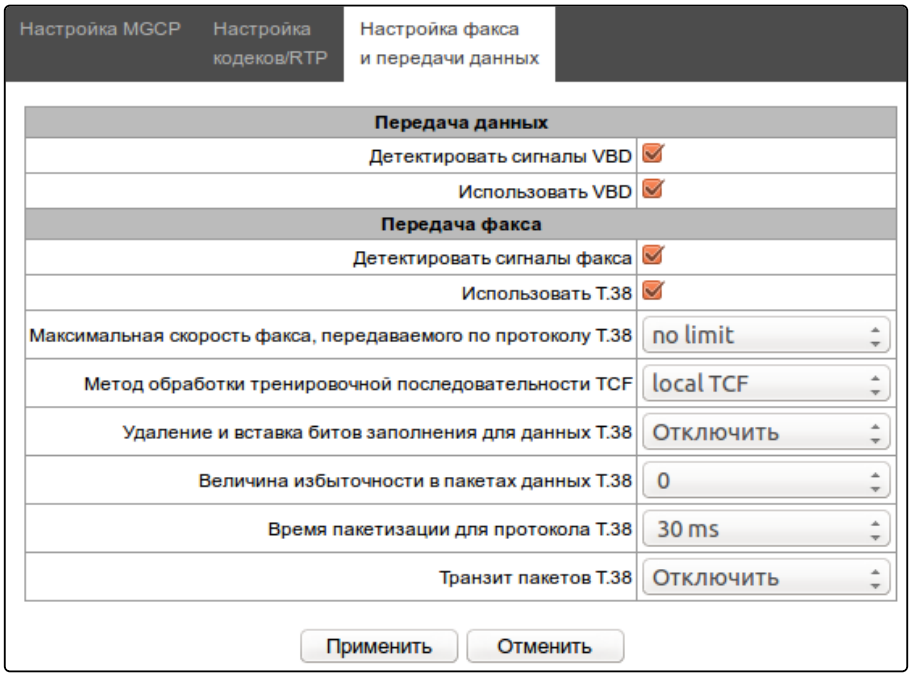
Кодеки:

В данном разделе можно выбрать кодеки для интерфейса и порядок, в котором они будут использоваться при установлении соединения. Кодек с наивысшим приоритетом необходимо установить в верхней позиции.

При нажатии левой кнопкой мыши строка с выбранным кодеком подсвечивается. Для изменения приоритета кодеков используются стрелки  (вниз, вверх).

- *Включить* − при установленном флаге использовать кодек, указанный в поле напротив;
- *Кодек* − кодек, используемый для передачи голосовых данных. Поддерживаемые кодеки G.711A, G.711U, G.729A, G.729B, G.723.1, G.726-32.
- *PType* − тип нагрузки для кодека. Поле доступно для редактирования только при выборе кодека G.726 (разрешенные для использования значения − от 96 до 127, либо 2 для согласования с устройствами, не поддерживающими динамический тип нагрузки для данного кодека). Для остальных кодеков назначается автоматически;
- *PTE* − время пакетизации − количество миллисекунд (мс) речи, передаваемых в одном пакете.

3 Вкладка «Настройка факса и передача данных»



Передача данных:

- *Детектировать сигналы VBD* − при установленном флаге шлюз будет детектировать сигнал модема CED;
- *Использовать VBD* − при установленном флаге при детектировании сигнала CED осуществляется передача события G/MT в сообщении NOTIFY.

Передача факса:

- *Детектировать сигналы факса* – при установленном флаге шлюз будет детектировать сигнал факса V.21flag и передавать событие G/FT в сообщении NOTIFY;
- *Использовать T.38* – позволяет использовать протокол T.38 для передачи факса;
- *Максимальная скорость факса, передаваемого по протоколу T.38* – максимальная скорость факса, передаваемого по протоколу T.38. Данная настройка влияет на возможности шлюза работать с высокоскоростными факсимильными аппаратами. Если факсимильные аппараты поддерживают передачу на скорости 14400, а на шлюзе настроено ограничение 9600, то максимальная скорость соединения между факсимильными аппаратами не сможет превысить 9600 бод. Если наоборот, факсимильные аппараты поддерживают передачу на скорости 9600, а на шлюзе настроено ограничение 14400, то данная настройка не окажет влияние на взаимодействие, максимальная скорость будет определяться возможностями факсимильных аппаратов;
- *Метод обработки тренировочной последовательности TCF*:
  - *local TCF* – метод требует, чтобы подстроечный сигнал TCF генерировался приемным шлюзом локально. Обычно используется при передаче T.38 по TCP;
  - *transferred TCF* – метод требует, чтобы подстрочный сигнал TCF передавался с передающего устройства на приемное. Обычно используется при передаче T.38 по UDP.
- *Удаления и вставки битов заполнения для данных T.38* – удаления и вставки битов заполнения для данных, не связанных с ECM (режимом коррекции ошибок);
- *Величина избыточности в пакетах данных T.38* – величина избыточности в пакетах данных T.38 (количество предыдущих пакетов в последующем пакете T.38). Введение избыточности позволяет восстановить переданную последовательность данных на приеме в случае, если были потери среди переданных пакетов;
- *Время пакетизации для протокола T.38* – определяет частоту формирования пакетов T.38 в миллисекундах (мс). Данная настройка позволяет регулировать размер передаваемого пакета. Если взаимодействующий шлюз может принимать дейтаграммы с максимальным размером в 72 байта (maxdatagrammSize: 72), то на SMG время пакетизации необходимо установить минимальным;
- *Транзит пакетов T.38* – в случае, когда вызов осуществляется через два SIP-интерфейса и протокол T.38 для передачи факса используется в обоих интерфейсах, данная настройка позволяет осуществить транзит пакетов T.38 из одного интерфейса в другой с минимальными задержками.

Значения поля «тип сервиса» (IP DSCP) для RTP, T.38 и MGCP:

0 (DSCP 0x00, Diffserv 0x00) – стандартное отправление (Best Effort) – значение по умолчанию;

8 (DSCP 0x08, Diffserv 0x20) – класс 1;

10 (DSCP 0x0A, Diffserv 0x28) – гарантированное отправление, низкая вероятность сброса (Class1, AF11);

12 (DSCP 0x0C, Diffserv 0x30) – гарантированное отправление, средняя вероятность сброса (Class1, AF12);

14 (DSCP 0x0E, Diffserv 0x38) – гарантированное отправление, высокая вероятность сброса (Class1, AF13);

16 (DSCP 0x10, Diffserv 0x40) – класс 2;

18 (DSCP 0x12, Diffserv 0x48) – гарантированное отправление, низкая вероятность сброса (Class2, AF21);

20 (DSCP 0x14, Diffserv 0x50) – гарантированное отправление, средняя вероятность сброса (Class2, AF22);

22 (DSCP 0x16, Diffserv 0x58) – гарантированное отправление, высокая вероятность сброса (Class2, AF23);

24 (DSCP 0x18, Diffserv 0x60) – класс 3;

26 (DSCP 0x1A, Diffserv 0x68) – гарантированное отправление, низкая вероятность сброса (Class3, AF31);

28 (DSCP 0x1C, Diffserv 0x70) – гарантированное отправление, средняя вероятность сброса (Class3, AF32);

30 (DSCP 0x1E, Diffserv 0x78) – гарантированное отправление, высокая вероятность сброса (Class3, AF33);

32 (DSCP 0x20, Diffserv 0x80) – класс 4;

34 (DSCP 0x22, Diffserv 0x88) – гарантированное отправление, низкая вероятность сброса (Class4, AF41);

36 (DSCP 0x24, Diffserv 0x90) – гарантированное отправление, средняя вероятность сброса (Class4, AF42)

38 (DSCP 0x26, Diffserv 0x98) – гарантированное отправление, высокая вероятность сброса (Class4, AF43);

40 (DSCP 0x28, Diffserv 0xA0) – класс 5;

46 (DSCP 0x2E, Diffserv 0xB8) – ускоренное отправление (Class5, Expedited Forwarding).

IP Precedence:

0 – IPP0 (Routine);

8 – IPP1 (Priority);

16 – IPP2 (Immediate);

24 – IPP3 (Flash);

32 – IPP4 (Flash Override);

40 – IPP5 (Critical);

48 – IPP6 (Internetwork Control);

56 – IPP7 (Network Control).

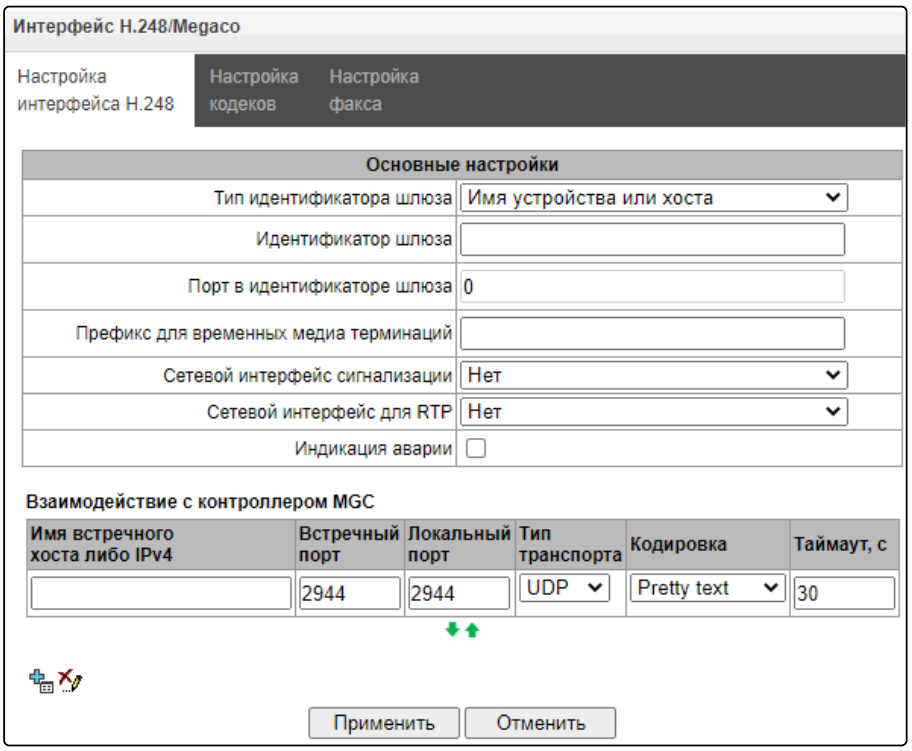
5.1.7.2 Интерфейс H.248/Megaco

В данном разделе настраиваются общие параметры конфигурации стека H.248.

Протокол H.248/Megaco − протокол контроля медиашлюзов является протоколом сигнализации, используемым в распределенных системах IP-телефонии, состоящих из контроллера медиашлюзов (MGC) и медиашлюзов (MG).

На устройстве возможно настроить только один интерфейс H.248/Megaco.

5.1.7.2.1 **Вкладка «Настройка интерфейса H.248»**



Основные настройки:

- *Тип идентификатора шлюза* − определяет вид, в котором будет настроен идентификатор шлюза (строковое имя, доменное имя, IP-адрес, 16 MTP-адрес);
- *Идентификатор шлюза* − идентификатор медиашлюза. Может быть строкой, доменным именем, IP-адресом, либо MTP-адресом, в зависимости от установленного типа;
- *Порт в идентификаторе шлюза* − номер транспортного порта, добавляемый через символ «:» в конец идентификатора шлюза;
- *Префикс для временных медиа терминаций* − префикс который будет использоваться при нумерации временных медиатерминаций (терминаций для голосовых RTP потоков) шлюза;
- *Сетевой интерфейс сигнализации* − выбор сетевого интерфейса для приема и передачи сигнальных H.248 сообщений;
- *Сетевой интерфейс для RTP* − выбор сетевого интерфейса для приема и передачи голосового трафика.

Взаимодействие с контроллером MGC

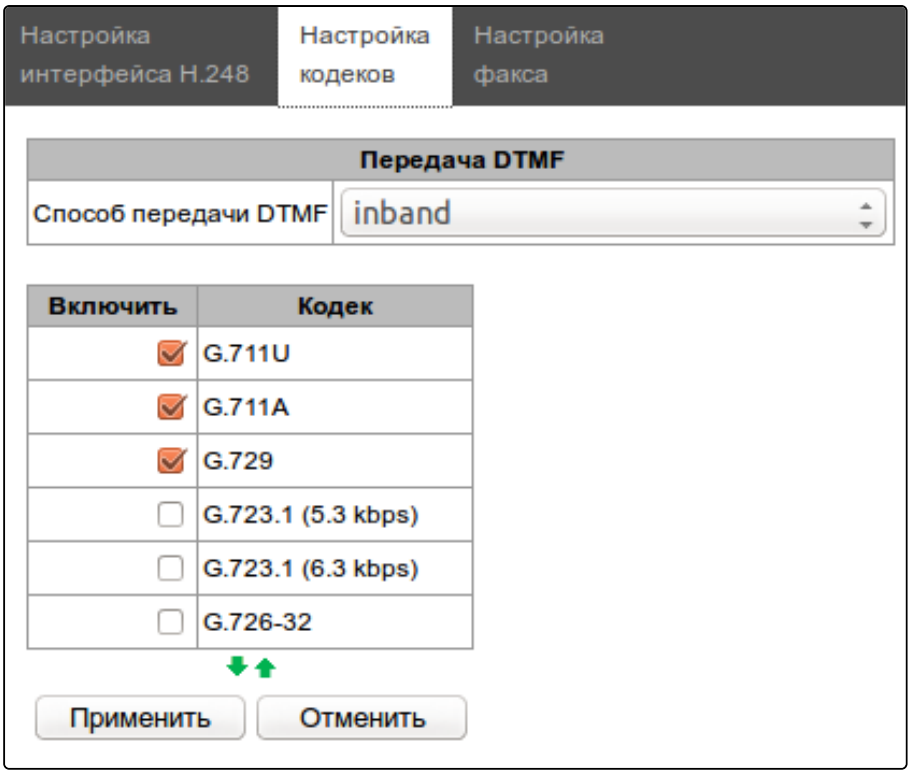
В данной таблице описываются параметры взаимодействия с контроллерами медиашлюзов (MGC).

Кнопка позволяет добавить, а кнопка удалить резервные контроллеры. Стрелками можно менять приоритет между контроллерами медиашлюзов.

- *Имя встречного хоста либо IPv4* − доменное имя, либо IP-адрес контроллера медиашлюзов;

- *Встречный порт* – сигнальный UDP-порт контроллера медиашлюзов, принимающий сообщения протокола H.248;
- *Локальный порт* – локальный сигнальный UDP порт шлюза, на котором будут приниматься сообщения протокола H.248;
- *Тип транспорта* – выбор транспортного протокола для передачи сообщений H.248 (UDP/TCP/SCTP);
- *Кодировка* – выбор типа кодировки, либо "имена параметров и атрибутов целиком" (pretty), либо "сокращенные имена парметров и атрибутов" (compact);
- *Таймаут, с* – период контроля доступности контроллера медиашлюзов. Если в течение данного времени шлюз не получил от контроллера сообщение контроля audit, то принимается решение, что контроллер стал недоступным и инициируется процедура рестарта интерфейса.

5.1.7.2.2 Вкладка «Настройка кодеков/RTP»



Передача DTMF:

- *Способ передачи DTMF* – способ передачи DTMF через IP-сеть:
  - *inband* – внутри полосы, в речевых пакетах RTP;
  - *RFC2833* – согласно рекомендации RFC2833 в качестве выделенной нагрузки в речевых пакетах RTP.

Для возможности использования донабора во время разговора убедитесь, что аналогичный метод передачи сигналов DTMF настроен на встречном шлюзе.

Кодеки:

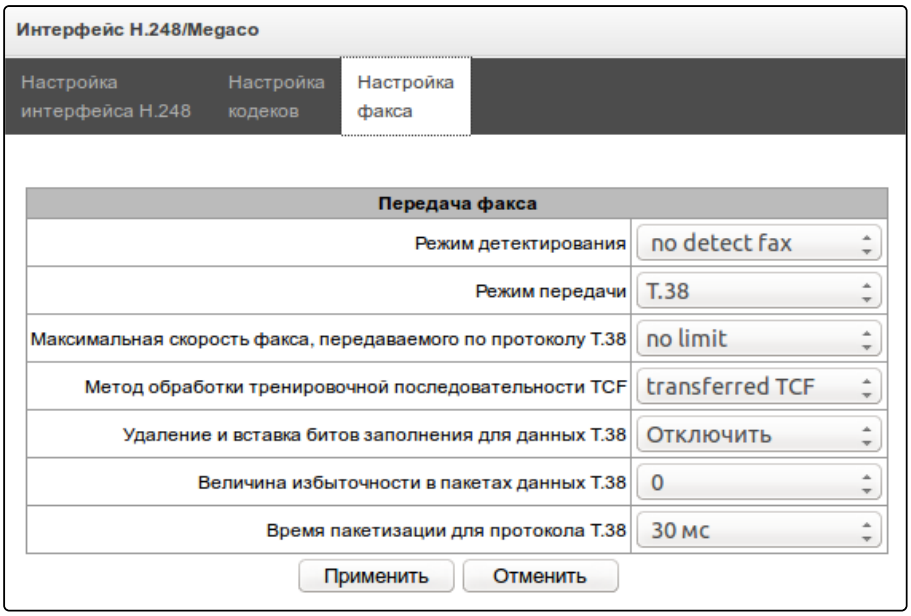
В данном разделе можно выбрать кодеки для интерфейса и порядок, в котором они будут использоваться при установлении соединения. Кодек с наивысшим приоритетом необходимо установить в верхней позиции.

При нажатии левой кнопкой мыши строка с выбранным кодеком подсвечивается. Для изменения приоритета кодеков используются стрелки (вниз, вверх).

- *Включить* – при установленном флаге использовать кодек, указанный в поле напротив;

- *Кодек* – кодек, используемый для передачи голосовых данных. Поддерживаемые кодеки G.711A, G.711U, G.729, G.723.1, G.726-32.

5.1.7.2.3 Вкладка «Настройка факса»



Передача факса:

- *Режим детектирования* – определяет направление передачи, при котором детектируются тоны факса, после чего осуществляется переход на кодек факса:
  - *no detect fax* – отключает детектирование тонов факса, но не запрещает передачу факса (не будет инициироваться переход на кодек факса, но данный переход может быть сделан встречным шлюзом);
  - *Caller and Callee* – детектируются тоны как при передаче факса, так и при приеме. При передаче факса детектируется сигнал CNG FAX с абонентской линии. При приеме факса детектируется сигнал V.21 с абонентской линии;
  - *Caller* – детектируются тоны только при передаче факса. При передаче факса детектируется сигнал CNG FAX с абонентской линии;
  - *Callee* – детектируются тоны только при приеме факса. При приеме факса детектируется сигнал V.21 с абонентской линии.

Сигнал V.21 может быть задетектирован и от передающего факса.

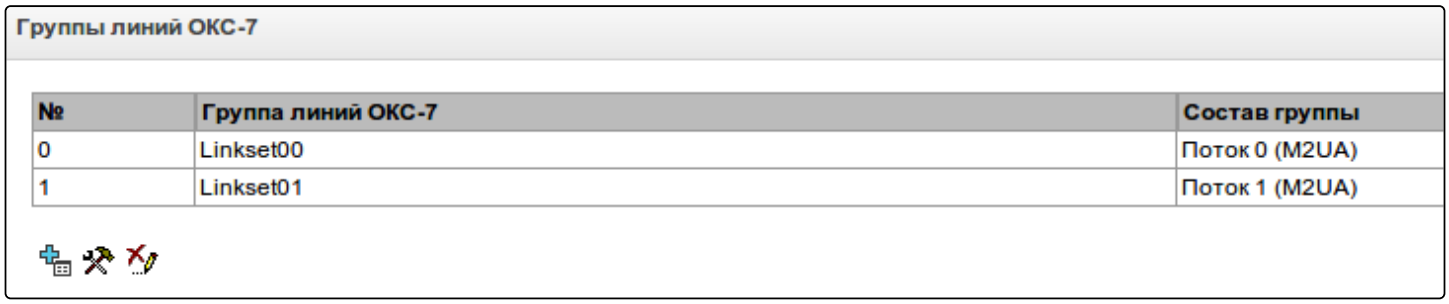
- *Режим передачи* – выбор протокола для передачи факса;
- *Максимальная скорость факса, передаваемого по протоколу T.38* – максимальная скорость факса, передаваемого по протоколу T.38. Данная настройка влияет на возможности шлюза работать с высокоскоростными факсимильными аппаратами. Если факсимильные аппараты поддерживают передачу на скорости 14400, а на шлюзе настроено ограничение 9600, то максимальная скорость соединения между факсимильными аппаратами не сможет превысить 9600 бод. Если наоборот, факсимильные аппараты поддерживают передачу на скорости 9600, а на шлюзе настроено ограничение 14400, то данная настройка не окажет влияние на взаимодействие, максимальная скорость будет определяться возможностями факсимильных аппаратов;
- *Метод обработки тренировочной последовательности TCF*:
  - *local TCF* – метод требует, чтобы подстроечный сигнал TCF генерировался приемным шлюзом локально. Обычно используется при передаче T.38 по TCP;
  - *transferred TCF* – метод требует, чтобы подстроечный сигнал TCF передавался с передающего устройства на приемное. Обычно используется при передаче T.38 по UDP.

- *Удаления и вставки битов заполнения для данных T.38* – удаления и вставки битов заполнения для данных, не связанных с ECM (режимом коррекции ошибок);
- *Величина избыточности в пакетах данных T.38* – величина избыточности в пакетах данных T.38 (количество предыдущих пакетов в последующем пакете T.38). Введение избыточности позволяет восстановить переданную последовательность данных на приеме в случае, если были потери среди переданных пакетов;
- *Время пакетизации для протокола T.38* – определяет частоту формирования пакетов T.38 в миллисекундах (мс). Данная настройка позволяет регулировать размер передаваемого пакета. Если взаимодействующий шлюз может принимать дейтаграммы с максимальным размером в 72 байта (maxdatagrammSize: 72), то на SMG время пакетизации необходимо установить минимальным.

5.1.8 Внутренние ресурсы

5.1.8.1 Группы линий ОКС-7

Настройка доступна только при наличии лицензии СОРМ.



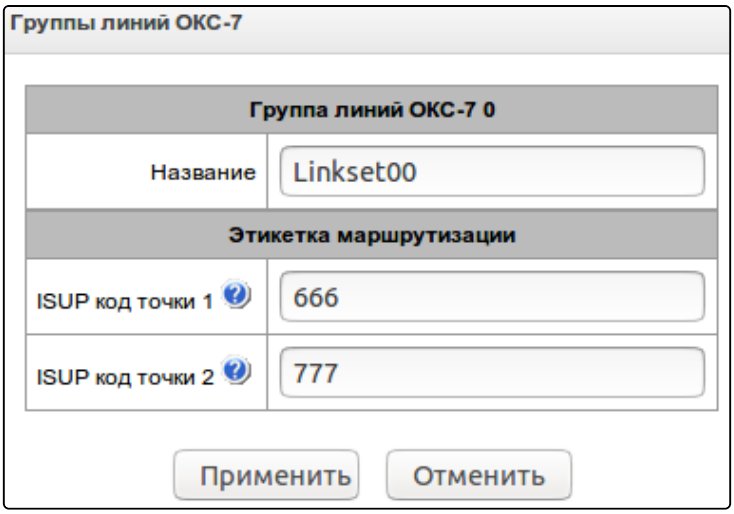
В данной таблице отображаются все созданные группы линий ОКС-7, а также потоки, на которые они назначены.

Для создания, редактирования и удаления группы линий ОКС-7 используется меню «Объекты» – «Добавить объект», «Объекты» – «Редактировать объект» и «Объекты» – «Удалить объект», а также кнопки:

– *«Добавить группу линий ОКС-7»;*

– *«Редактировать параметры группы линий ОКС-7»;*

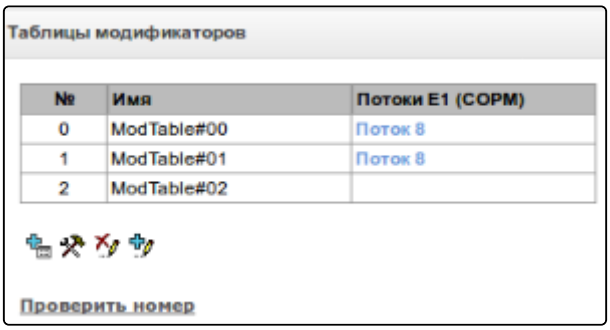
– *«Удалить группу линий ОКС-7».*



Группа линий ОКС – группа разговорных каналов, обеспечивающих взаимодействие между двумя точками PC (point code). Предназначена для изоляции каналов CIC между взаимодействующими точками PC. Если группа линий ОКС-7 не назначена на потоке, то СОРМ-ирование вызовов по данному потоку осуществляться не будет.

- *Название* – имя группы линий ОКС-7;
- *ISUP код точки 1/ISUP код точки 2* – коды OPC и DPC ISUP, настроенные на взаимодействующем шлюзе для взаимодействия по протоколу ОКС-7. SMG будет перехватывать вызовы только между этими двумя точками. Если коды точек 1 и 2 настроить равными нулю, то будут перехватываться все вызовы (независимо от значений OPC/DPC в сигнальных пакетах), проходящие через данную группу линий ОКС-7.

5.1.8.2 Таблица модификаторов



В данной таблице отображаются все созданные модификаторы и видно, каким объектам они присвоены.

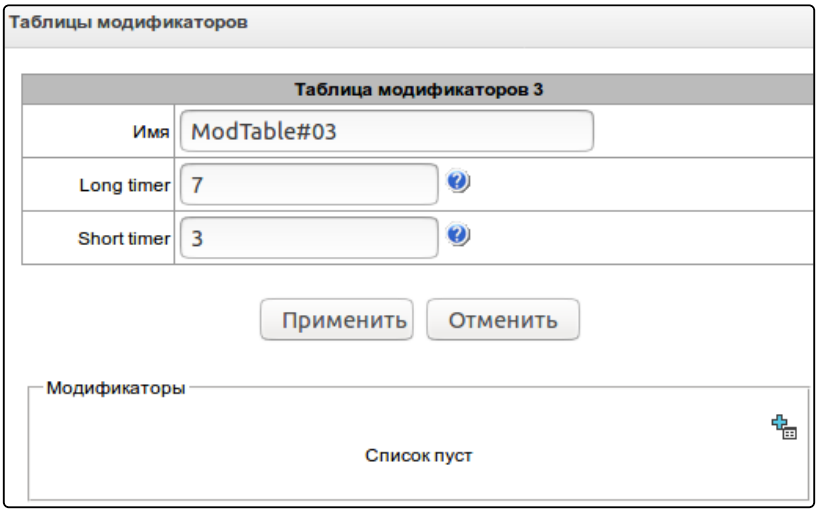
Для создания, редактирования и удаления модификатора используется меню «Объекты» – «Добавить объект», «Объекты» – «Редактировать объект» и «Объекты» – «Удалить объект», а также кнопки:

– *«Добавить модификатор»;*

– *«Редактировать параметры модификатора»;*

– *«Удалить модификатор»;*

– *«Добавить модификатор копированием».*



Общие настройки таблицы модификаторов:

- *Имя* – отображаемое имя таблицы;
- *Long timer* – таймаут ожидания набора номера в режиме overlap;
- *Short timer* – таймаут ожидания набора цифры в режиме overlap;

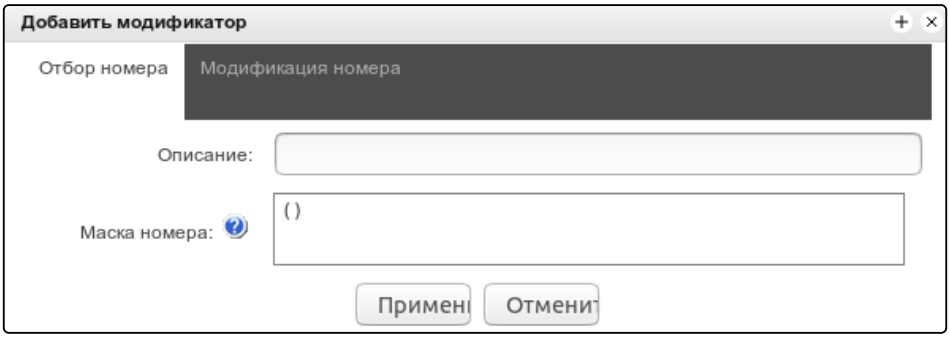
- *Модификаторы* − список модификаторов, используемых в таблице.

Для назначения/редактирования параметров созданного модификатора необходимо выделить соответствующую строку и нажать кнопку .

Для того чтобы подтвердить изменение параметров модификатора, необходимо нажать кнопку «Применить», для выхода без сохранения изменений − кнопку «Отменить».

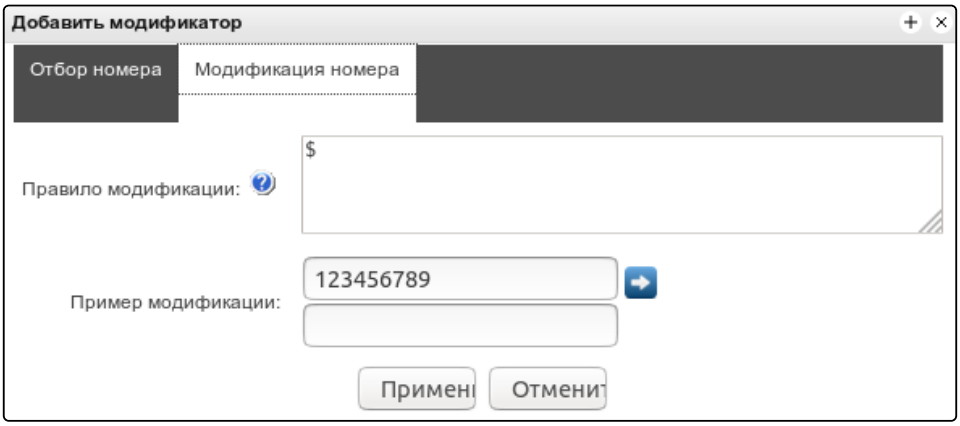
Ссылка «Проверить номер» под таблицей модификаторов не используется в данном программном обеспечении.

5.1.8.2.1 Вкладка «Отбор номера»



- *Описание* − описание модификатора;
- *Маска номера* − шаблон или набор шаблонов, с которым сравнивается номер абонента (синтаксис маски описан в разделе Описание маски номера и ее синтаксис);

5.1.8.2.2 Вкладка «Модификация номера»



- *Правило модификации* − правило преобразования номера. Используемый синтаксис описан в разделе Синтаксис правила модификации.
- *Пример модификации* − по нажатию на кнопку  осуществляется просмотр итоговых результатов модификации после применения заданных правил модификации. Вместо номера 123456789, введенного в примере для проверки правил, рекомендуется задавать номер, над которым планируется осуществить модификацию;

5.1.8.2.3 Синтаксис правила модификации

Правило модификации представляет собой набор спецсимволов, определяющих изменения номера:

- '**.**' и '**-**': спецсимволы, обозначающие, что цифра на данной позиции номера удаляется, и на ее место смещаются цифры 10, следующие далее;
- '**X**', '**x**': спецсимволы, обозначающие, что цифра на данной позиции остается неизменной (обязательное наличие цифры на этой позиции);

- **'?'**: спецсимвол, обозначающий, что цифра на данной позиции остается неизменной (необязательное наличие цифры на этой позиции);
- **'+'**: спецсимвол, означающий, что все знаки, находящиеся между этой позицией и следующим спецсимволом (или концом последовательности), вставляются в номер на заданное место;
- **'!'**: спецсимвол, означающий окончание разбора, все дальнейшие цифры номера отрезаются;
- **'$'**: спецсимвол, означающий окончание разбора, все дальнейшие цифры номера используются неизмененными;
- **0-9, D, #** и ***** (не имеющие перед собою спецсимвола '+'): информационные символы, которые замещают цифру в номере на данной позиции.

Примеры модификаций:

- Добавление кода города 383 к номеру 2220123
- Модификатор: +383
- Результат: 38322201234

- Замена кода страны на 7 в номере 83832220123
- Модификатор: 7
- Результат: 738322201234

- Замена третьей цифры номера 2220123 на 6
- Модификатор: xx6$ или XX6$
- Результат: 22601234

- Удаление префикса 99# у номера 99#2220123
- Модификатор: ---$
- Результат: 2220123

- Удаление последних четырёх цифр номера 22201239876
- Модификатор: $----
- Результат: 2220123

- Отбор первых семи цифр номера 222012349876
- Модификатор: xxxxxxx!
- Результат: 2220123

- Удаление последних двух цифр, замена третьей цифры на 6 и добавление кода города 383 к номеру 222012398
- Модификатор: +383xx6$--
- Результат: 3832260123

5.1.9 Настройки TCP/IP

В данном разделе устанавливаются сетевые настройки устройства, правила 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.
- **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.

- **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.

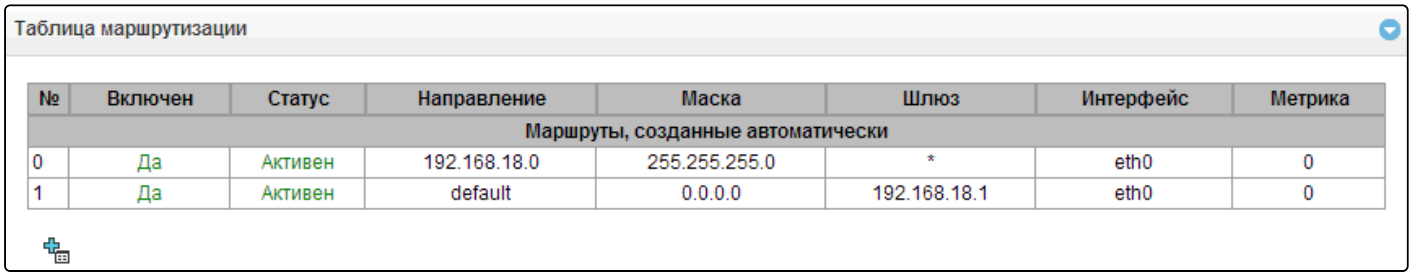
5.1.9.1 Таблица маршрутизации

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

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



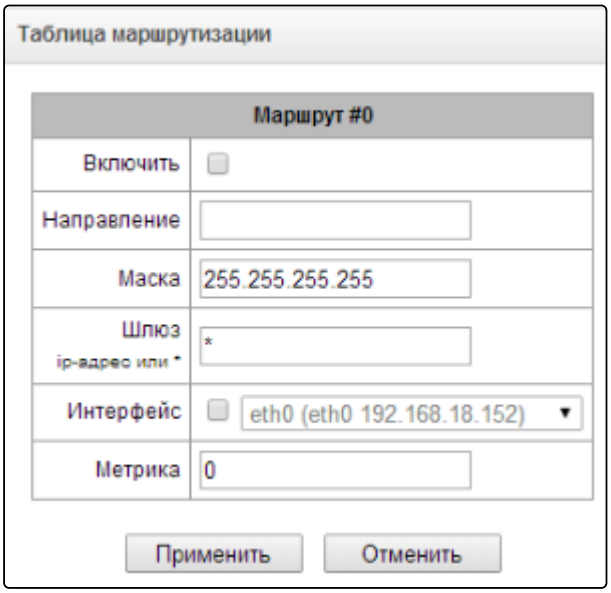
№	Включен	Статус	Направление	Маска	Шлюз	Интерфейс	Метрика
Маршруты, созданные автоматически							
0	Да	Активен	192.168.18.0	255.255.255.0	*	eth0	0
1	Да	Активен	default	0.0.0.0	192.168.18.1	eth0	0

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

– « *Добавить маршрут»;*

– *«Редактировать параметры маршрута»;*

– *«Удалить маршрут»*.



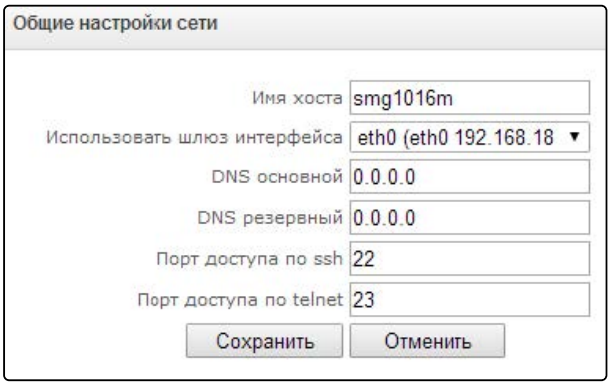
Параметры маршрута:

- *Включить* – при установленном флаге маршрут включен;
- *Направление* – IP-сеть;
- *Маска* – задает маску сети для заданной IP-сети (для IP-адреса используйте маску 255.255.255.255);
- *Интерфейс* – выбор сетевого интерфейса передачи;
- *Шлюз* – задает IP-адрес шлюза для маршрута;
- *Метрика* – метрика маршрута.

5.1.9.2 Сетевые параметры

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

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

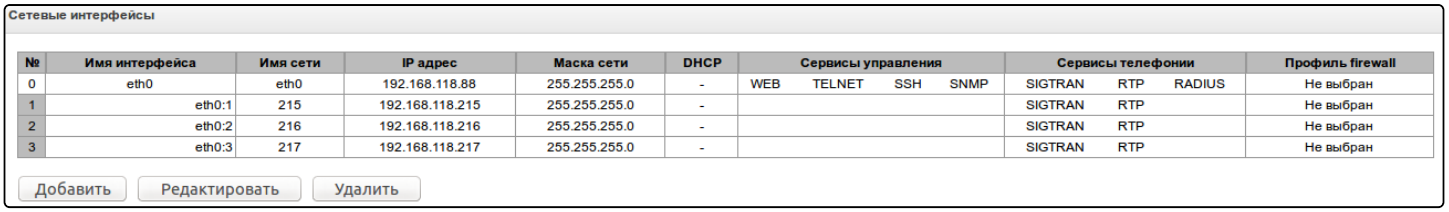


5.1.9.3 Сетевые интерфейсы

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

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

На SMG-3016 есть возможность сконфигурировать 2 основных сетевых интерфейса eth0 и eth2. Интерфейс eth2 имеет тип Management и используется только для управления устройством через порт OOB. Интерфейс поддерживает работу со статическим адресом, с адресом, полученным по DHCP, VLAN. На устройстве может существовать только один интерфейс с типом Management.



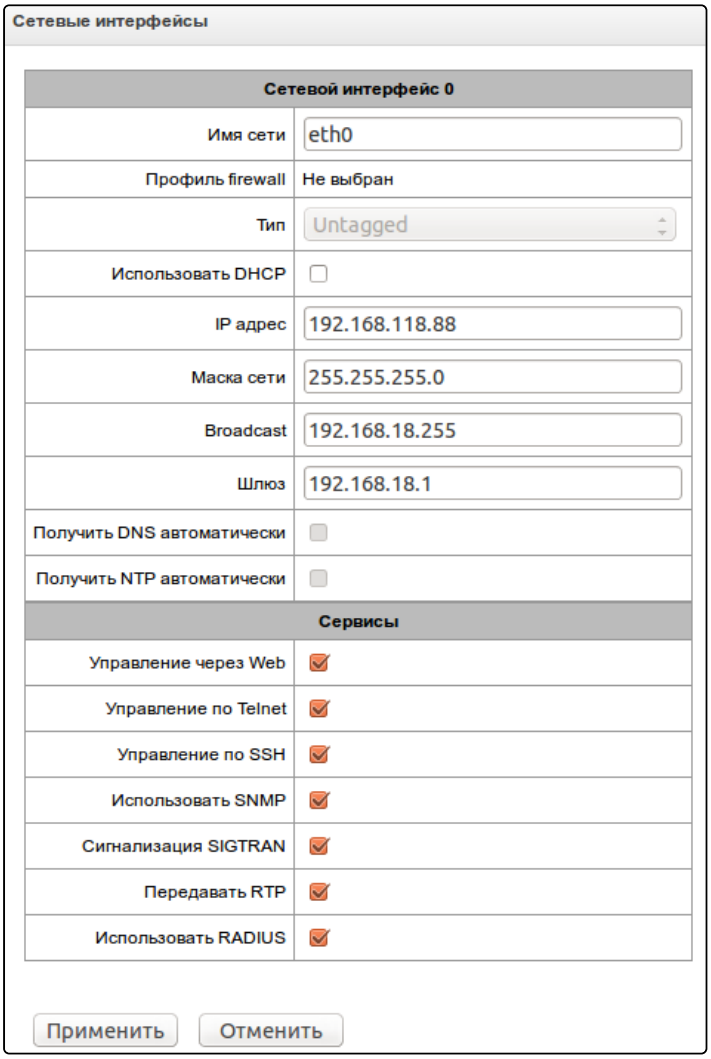
Для создания, редактирования и удаления правил сетевых интерфейсов используются кнопки:

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

Настройки сетевого интерфейса:

- *Имя сети* – наименование сети;
- *Профиль firewall* – отображение выбранного профиля firewall для данного интерфейса;

- *Тип* – тип интерфейса (для интерфейса eth0 всегда untagged);
- *VLAN ID* – идентификатор VLAN (1- 4095) (только для интерфейсов с типом tagged);
- *Использовать DHCP* – получить IP-адрес динамически от DHCP-сервера (для Alias не поддерживается);
- *IP-адрес* – сетевой адрес устройства;
- *Маска подсети* – маска подсети для устройства;
- *Broadcast* – адрес для широковещательных пакетов;
- *Шлюз* – сетевой шлюз для данного интерфейса (для Alias не поддерживается);
- *Получить DNS автоматически* – получить IP-адрес DNS сервера динамически от DHCP сервера (для Alias не поддерживается);
- *Получить NTP автоматически* – IP-адрес NTP сервера динамически от DHCP сервера (для Alias не поддерживается).



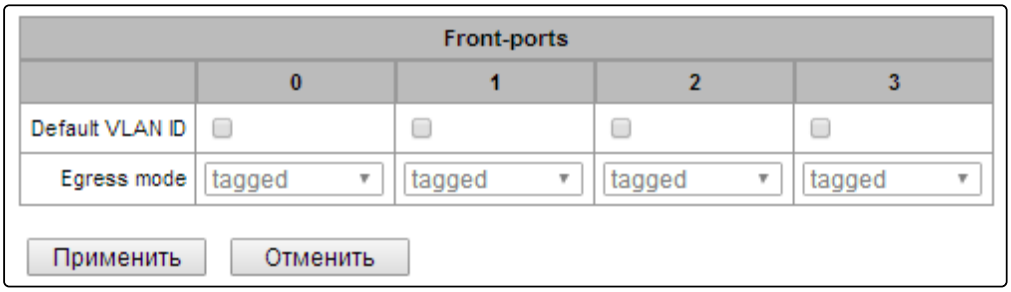
Сервисы – меню управления разрешенных сервисов для данного интерфейса:

- *Управление через web* – разрешает доступ к конфигуратору через интерфейс;
- *Управление по Telnet* – разрешает доступ по протоколу telnet через интерфейс;
- *Управление по SSH* – разрешает доступ по протоколу SSH через интерфейс;
- *Использовать SNMP* – разрешает использования протокола SNMP через интерфейс;
- *Сигнализация SIGTRAN* – разрешает прием и передачу сигнальной информации SIGTRAN (M2UA, IUA) через сетевой интерфейс, настроенный в данном разделе;
- *Передавать RTP* – разрешает прием и передачу голосового трафика через сетевой интерфейс, настроенный в данном разделе;
- *Использовать RADIUS* – разрешает использование протокола RADIUS через интерфейс.

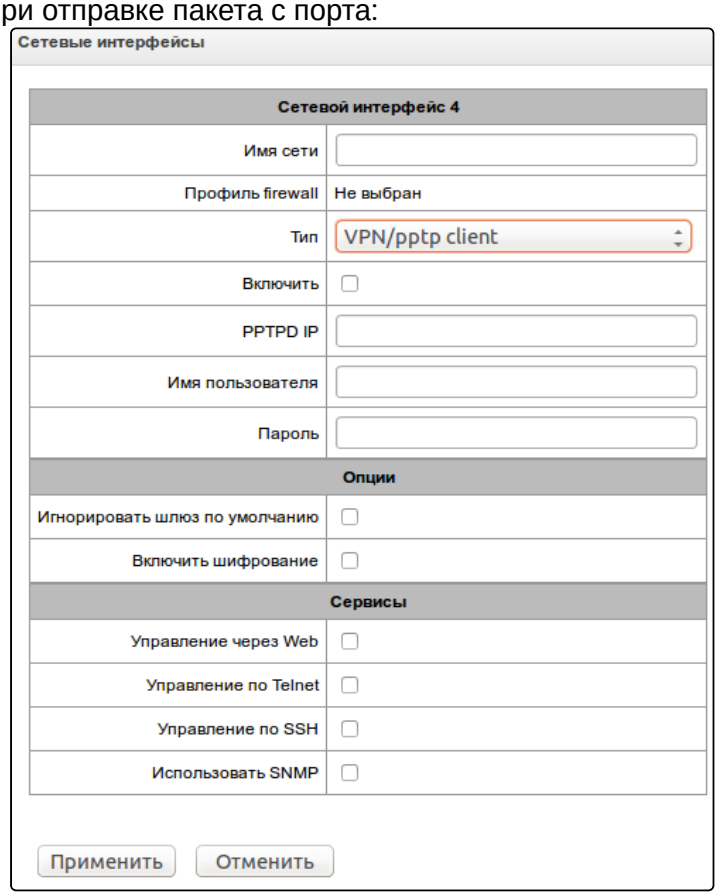
После изменения IP-адреса, маски сети либо при отключении управления через web-конфигуратор на сетевом интерфейсе во избежание потери доступа к устройству необходимо подтвердить данные настройки, подключившись к web-конфигуратору, иначе по истечении двухминутного таймера произойдет откат к предыдущей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

Front-ports [1] *– настройка внешних front-портов*

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



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



Настройки VPN/PPP интерфейса:

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

Опции:

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

Сервисы – меню управления разрешенных сервисов для данного интерфейса:

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

---

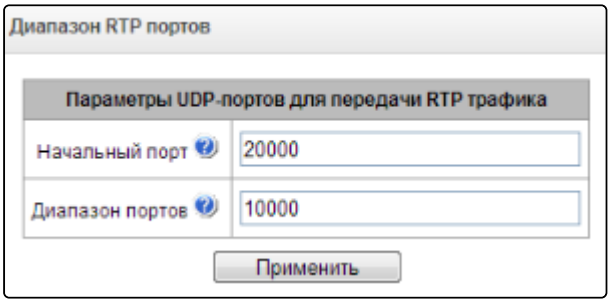
[1] *Только для SMG-2016.*

5.1.9.4 Диапазон RTP-портов

В данном разделе конфигурируется диапазон портов UDP для передачи голосовых RTP-пакетов.

Параметры UDP-портов для передачи RTP-трафика:

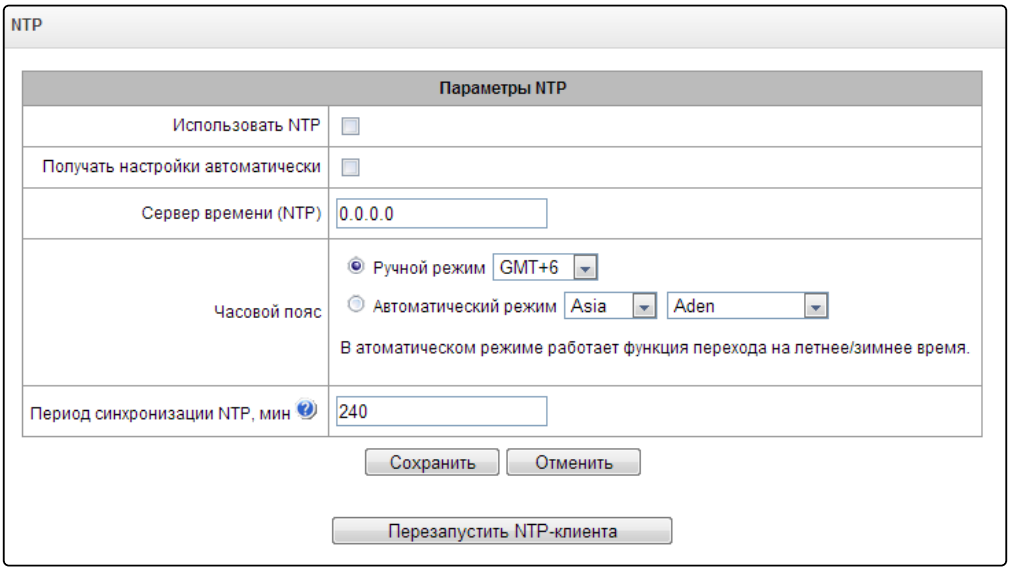
- *Начальный порт* − номер начального UDP-порта, используемого для передачи разговорного трафика (RTP) и данных по протоколу T.38;
- *Диапазон портов* − диапазон (количество) UDP-портов, используемых для передачи разговорного трафика (RTP) и данных по протоколу T.38.



5.1.10 Сетевые сервисы

5.1.10.1 NTP

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



Параметры NTP

- *Использовать NTP* – включение синхронизации времени по протоколу NTP*;*
- *Получать настройки автоматически* – при установленном флаге использовать NTP-сервер, адрес которого получен по протоколу DHCP;
- *Сервер времени (NTP)* – IP-адрес или имя хоста сервера NTP;
- *Часовой пояс* – настройка часового пояса и отклонения текущего времени относительно GMT (Greenwich Mean Time):
  - *Ручной режим* – выбор отклонения времени относительно GMT;
  - *Автоматический режим* – в данном режиме предоставлена возможность выбора местонахождения устройства, отклонение от GMT будет настроено автоматически, также в данном режиме работает автоматический переход на летнее и зимнее время**;**
- *Период синхронизации NTP, мин* – период отправки запросов на синхронизацию времени.

Для сохранения изменений используется кнопка «*Сохранить*» , для отмены «*Отмена*». Для принудительной синхронизации времени от сервера необходимо нажать кнопку «*Перезапустить NTP-клиента*» (происходит перезапуск NTP-клиента).

5.1.10.2 Настройки SNMP

Программное обеспечение SMG позволяет проводить мониторинг устройства, используя протокол SNMP. В подменю «SNMP» выполняются настройки параметров SNMP-агента.

Функции мониторинга по SNMP позволяют запросить у шлюза следующие параметры:

- имя шлюза;
- тип устройства;
- версия программного обеспечения;
- IP-адрес;
- статистика потоков E1;
- статистика субмодулей IP;
- состояние линксетов;
- состояние каналов потоков E1;

- состояние каналов IP (статистика по текущим вызовам через IP).

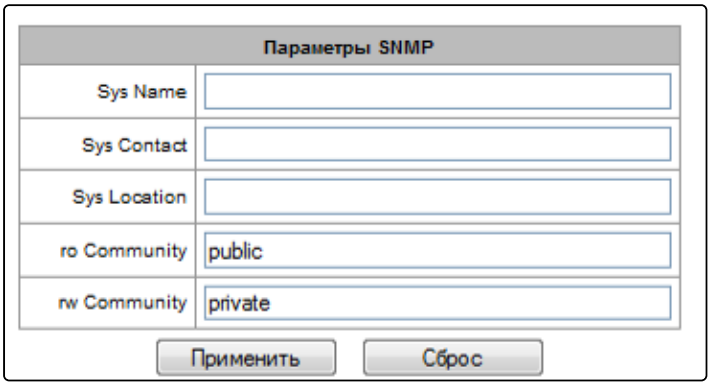
В статистике текущих вызовов по IP-каналам передаются следующие данные:

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

Параметры SNMP

- *Sys Name* − имя устройства;
- *Sys Contact* − контактная информация;
- *Sys Location* − место расположения устройства;
- *ro Community* − пароль/сообщество на чтение параметров;
- *rw Community* − пароль/сообщество на запись параметров;

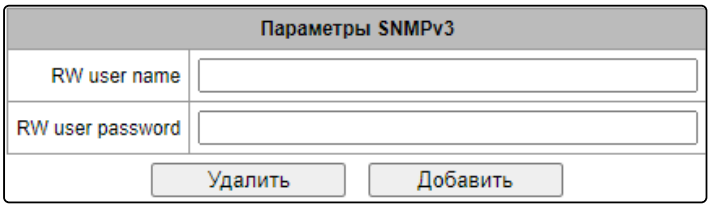
Для применения изменений используется кнопка *«Применить»*, для отмены настроек *«Сброс»*.



5.1.10.3 SNMPv3

В системе используется только один пользователь SNMPv3. Пользователь SNMPv3 используется для передачи команд СОРМ-ирования на шлюз SMG.

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



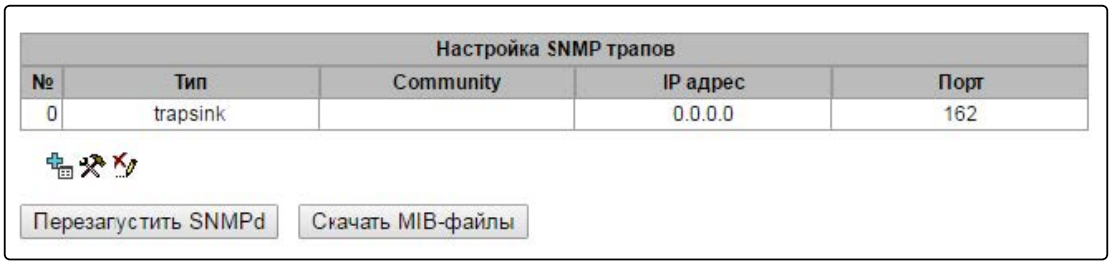
Для применения конфигурации пользователя SNMPv3 используется кнопка *«Добавить»* (настройки применяются сразу после нажатия). Для удаления записи нажать кнопку *«Удалить»*.

5.1.10.4 Настройка трапов (SNMP trap)

Подробное описание параметров мониторинга и сообщений Trap приведено в MIB-файлах, поставляемых на диске вместе со шлюзом.

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

- ошибка конфигурации;
- авария субмодуля IP;
- потеря синхронизации либо синхронизация от менее приоритетного источника;
- авария потока E1;
- удаленная авария потока;
- потеряна связь с контроллером медиашлюзов;
- исправлена ошибка конфигурации;
- восстановлена работоспособность субмодуля IP после аварии;
- восстановлена синхронизация от приоритетного источника;
- нет аварии потока (после наличия аварии либо удаленной аварии потока);
- статус обновления программного обеспечения и загрузки/выгрузки файла конфигурации.



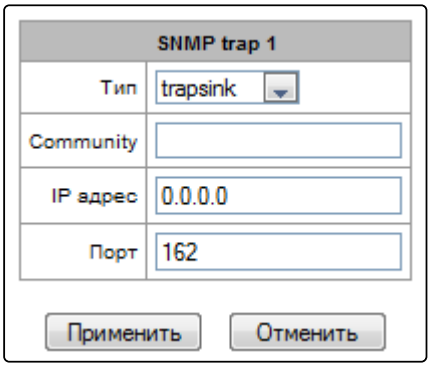
По нажатию на кнопку *«Перезапустить SNMPd»* осуществляется перезапуск SNMP-клиента. Для скачивания актуального MIB-файла используется кнопка *«Скачать MIB-файл»*.

– *«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 (стандартный порт – 162).

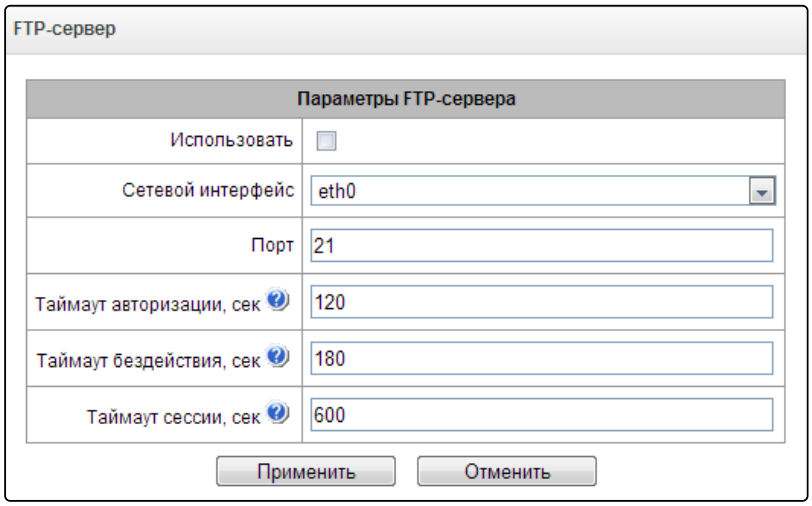


5.1.10.5 FTP-сервер

В данном разделе производится конфигурирование встроенного FTP-сервера, который служит для предоставления доступа по протоколу FTP к каталогам:

- *cdr* – каталог с файлами CDR-записей;
- *log* – каталог с файлами трассировок и другой отладочной информацией;
- *mnt* – каталог с файлами внешних накопителей (SSD-накопителей, SATA-накопителей, USB-flash).

Параметры FTP-сервера:



- *Использовать* – опция включения/отключения использования локального FTP-сервера;
- *Сетевой интерфейс* – выбор сетевого интерфейса, на котором будет запущен FTP-сервер;
- *Порт* – выбор TCP-порта, на котором будет запущен FTP-сервер;
- *Таймаут авторизации, сек* – время ввода данных для авторизации абонента на FTP-сервере, по его истечении сервер принудительно разорвет соединение;
- *Таймаут бездействия, сек* – время бездействия пользователь на FTP-сервере, по его истечении сервер принудительно разорвет соединение;
- *Таймаут сессии, сек* – время продолжительности сессии.

Настройка пользователей:

По умолчанию на устройстве создан абонент с правами на чтение всех каталогов с логином ***ftpuser*** и паролем ***ftppasswd*.**


Настройка пользователей:

Имя	Доступ к директориям		
	log	mnt	CDR
User1	R	R	W

- *Имя* – имя пользователя;
- *Пароль* – пароль пользователя;
- *Доступ к log* – настройка доступа к каталогу log, чтение/запись;
- *Доступ к mnt* – настройка доступа к каталогу mnt, чтение/запись;
- *Доступ к CDR* – настройка доступа к каталогу CDR, чтение/запись.

Для создания, редактирования и удаления параметров трапов используются кнопки:

5.1.11 Коммутатор

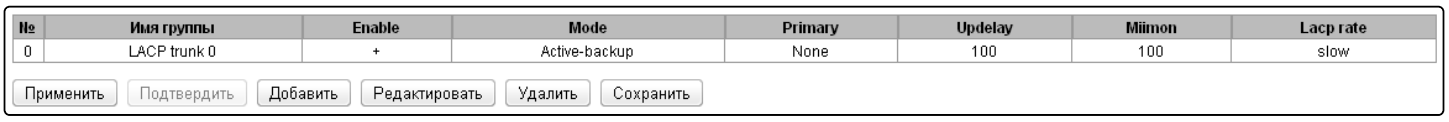
⚠ Меню доступно только для SMG-1016M.

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

5.1.11.1 Настройки LACP

В данном разделе производится настройка групп LACP.

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



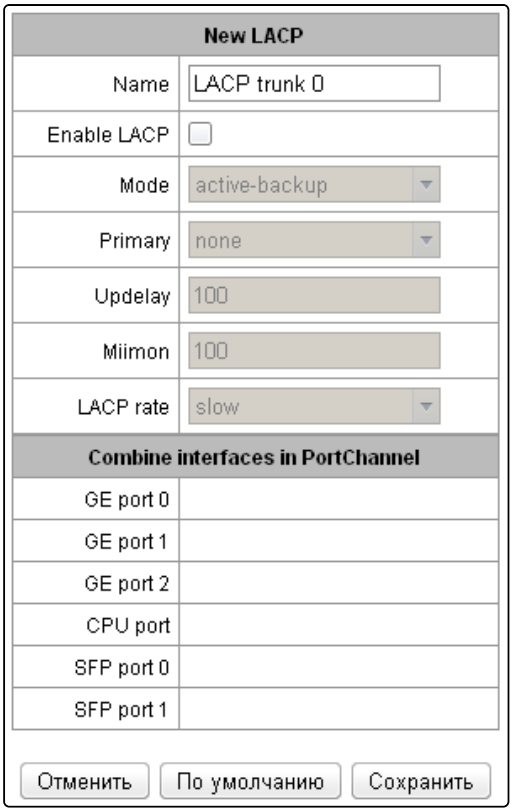
№	Имя группы	Enable	Mode	Primary	Updelay	Miimon	Lacp rate
0	LACP trunk 0	+	Active-backup	None	100	100	slow

Применить | Подтвердить | Добавить | Редактировать | Удалить | Сохранить

Для редактирования, удаления и сохранения группы LACP используется кнопки: *«Редактировать», «Удалить»*, *«Применить»*, *«Сохранить»*.

Для создания новой группы LACP необходимо нажать кнопку *«Добавить»*.

New LACP:



- *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 определённым получателем. Данный режим позволяет сбалансировать нагрузку и повысить отказоустойчивость;
  - *802.3 ad* − динамическое объединение портов. В данном режиме можно получить значительное увеличение пропускной способности как входящего, так и исходящего трафика, используя все объединенные интерфейсы. Требует поддержки данного функционала от коммутатора, а в ряде случаев − дополнительную настройку коммутатора.
- *Primary* − настройка ведущего интерфейса;
- *Updelay* − период смены интерфейса при недоступности ведущего интерфейса;
- *Miimon* − период проверки MII, частота в миллисекундах;
- *LACP rate* − интервал передачи управляющих пакетов протокола LACPDU (*fast* − интервал передачи 1 секунда, *slow* − интервал передачи 30 секунд);
- *Combine interfaces in PortChannel* − список портов, добавленных в группу LACP.

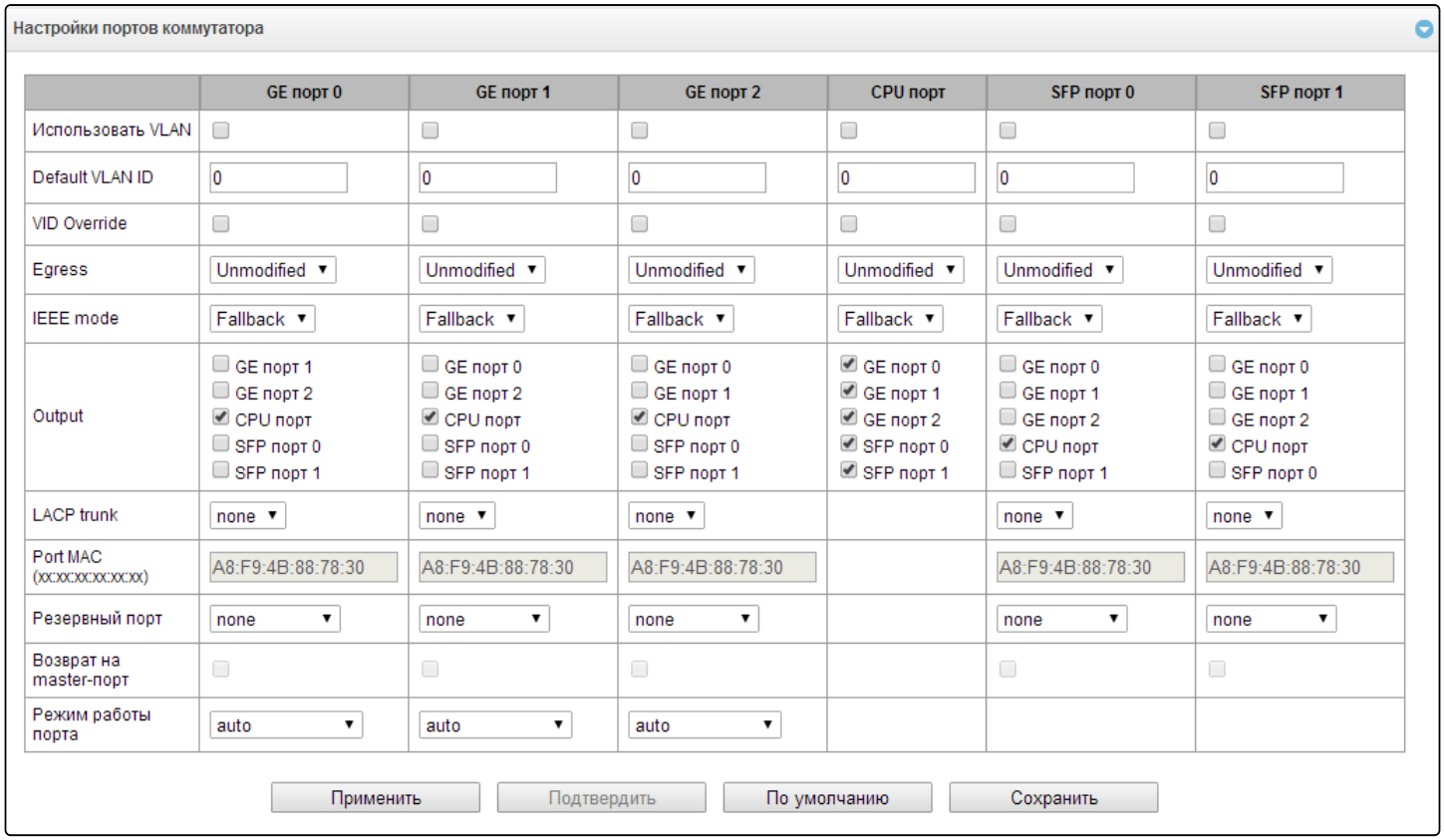
Для сохранения изменений используется кнопка *«Сохранить»,* для отмены *«Отмена».* Для установки параметров по умолчанию, необходимо нажать кнопку *«По умолчанию».*

5.1.11.2 Настройка портов коммутатора

Коммутатор может работать в четырех режимах:

1. ***Без использования настроек VLAN*** − для использования режима на всех портах флаги *«Enable VLAN»* должны быть не установлены, значение *«IEEE Mode»* на всех портах должно быть установлено в «*Fallback*», взаимодоступность портов для передачи данных необходимо определить флагами «*Output*». Таблица маршрутизации *«802.1q»* в закладке «*802.1q*» не должна содержать записей.
2. ***Port based VLAN*** − для использования режима значение *«IEEE Mode»* на всех портах должно быть установлено в «*Fallback*», взаимодоступность портов для передачи данных необходимо определить флагами «*Output*». Для работы с VLAN необходимо использовать настройки *«Enable VLAN», «Default VLAN ID», «Egress» и «Override».* Таблица маршрутизации *«802.1q»* в закладке «*802.1q*» не должна содержать записей.
3. ***802.1q*** − для использования режима значение *«IEEE Mode»* на всех портах должно быть установлено в *«Check»* либо *«Secure».* Для работы с VLAN используются настройки − *«Enable VLAN», «Default VLAN ID», «Override».* А также используются правила маршрутизации, описанные в таблице маршрутизации *«802.1q»* закладки «*802.1q*».
4. ***802.1q + Port based VLAN.*** Режим 802.1q может использоваться совместно с Port based VLAN. В этом случае значение *«IEEE Mode»* на всех портах должно быть установлено в «*Fallback*», взаимодоступность портов для передачи данных необходимо определить флагами «*Output*». Для

работы с VLAN необходимо использовать настройки *«Enable VLAN», «Default VLAN ID», «Egress» и «Override»*. А также используются правила маршрутизации, описанные в таблице маршрутизации *«802.1q»* закладки *«802.1q»*.



В заводской конфигурации порты коммутатора недоступны между собой.

Коммутатор устройства имеет 3 (для SMG-1016M) либо 4 (для SMG-2016 и SMG-3016) электрических порта Ethernet, 2 оптических и один порт для взаимодействия с процессором:

- *GE порт* – электрические Ethernet-порты устройства;
- *SFP порт* – оптические Ethernet-порты устройства;
- *CPU* – внутренний порт, подключенный к центральному процессору устройства.

Настройки коммутатора

- *Использовать VLAN* – при установленном флаге использовать настройки Default VLAN ID, Override и Egress на данном порту;
- *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 нетегированным.
- *IEEE mode* – устанавливает режимы безопасности при обработке принятых тегированных фреймов*:*
  - *fallback* – фрейм принимается на входящем порту независимо от наличия его 802.1q-тега в таблице маршрутизации «802.1q».
    Если 802.1q-тег не содержится в таблице маршрутизации «802.1q», то фрейм передаётся на исходящий порт при условии, что он разрешён в секции «output» в настройках входящего порта.
    Если 802.1q-тег содержится в таблице маршрутизации «802.1q», то фрейм передаётся на исходящий порт при условии, что исходящий порт является членом VLAN в таблице «802.1q» и разрешён в секции «output» в настройках входящего порта;
  - *check* – фрейм принимается на входящем порту если его 802.1q-тег содержится в таблице маршрутизации «802.1q» (входящий порт не обязан быть членом VLAN в таблице «802.1q»). Фрейм передаётся на исходящий порт если исходящий порт является членом VLAN в таблице «802.1q» и разрешён в секции «output» в настройках входящего порт;
  - *secure* – фрейм принимается на входящем порту если его 802.1q-тег содержится в таблице маршрутизации «802.1q» и входящий порт является членом VLAN в таблице «802.1q». Фрейм передаётся на исходящий порт если исходящий порт является членом VLAN в таблице «802.1q» и разрешён в секции «output» в настройках входящего порта.
- *Output* – взаимодоступность портов для передачи данных. Устанавливаются разрешения отправки пакетов, принятых данным портом, в порты, отмеченные флагом;
- *Резервный порт* – выбор порта, на который будет переключен трафик в случае возникновения нештатной ситуации (например, разрыв линии). Данная настройка необходима для обеспечения резервирования Dual Homing;
- *Возврат на master-порт* – при установленном флаге будет осуществлен переход на основной порт после его восстановления;

В текущей версии ПО поддерживается только global dual homing.

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

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

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

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

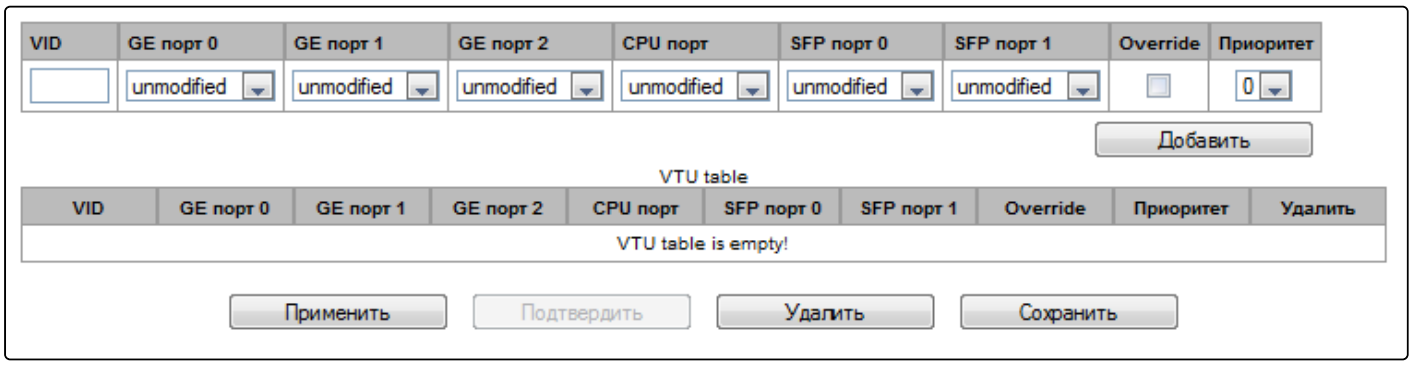
Для сохранения настроек в файл конфигурации без применения необходимо нажать кнопку «*Сохранить*».

5.1.11.3 802.1q

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

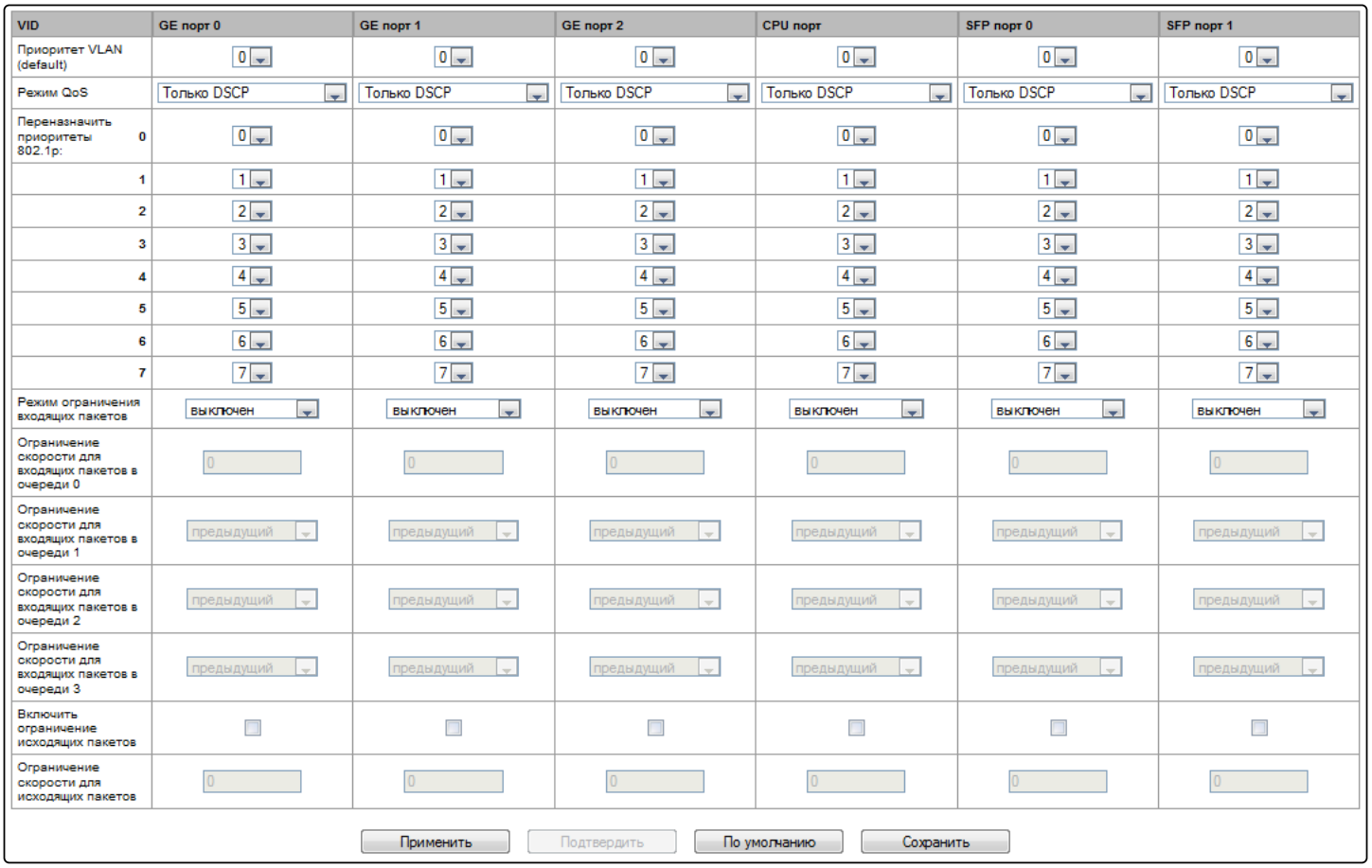
- *Сохранить* – сохранить настройки во Flash-память устройства без применения.

Удаление записи из таблицы маршрутизации пакетов

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

5.1.11.4 QoS и контроль полосы пропускания

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



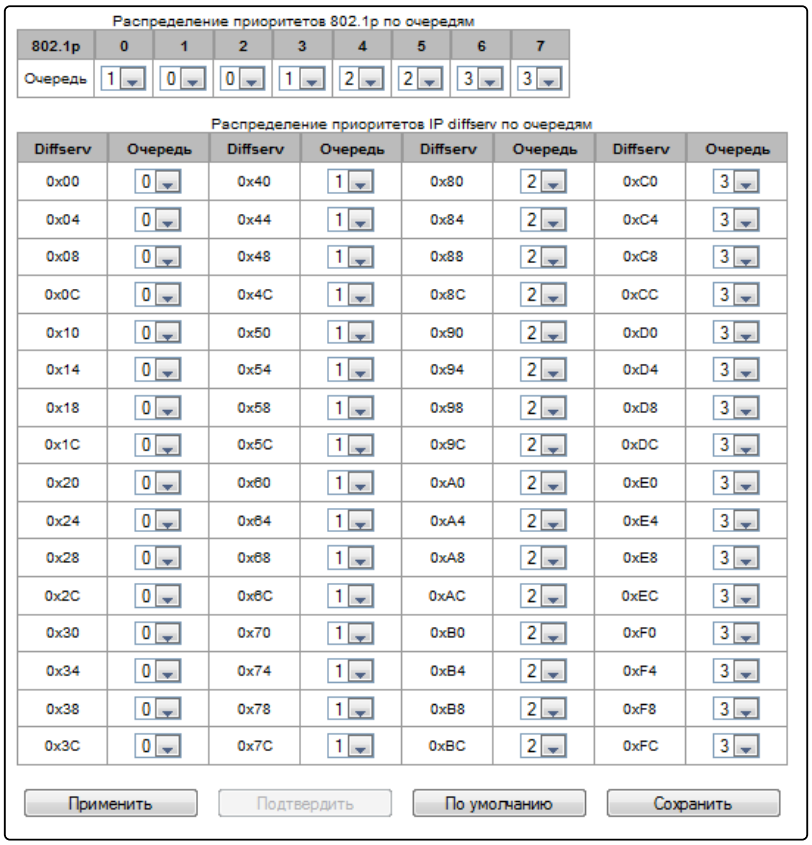
- *Приоритет VLAN (default)* – приоритет 802.1p, назначаемый нетегированным пакетам, принятым данным портом. Если пакет уже имеет приоритет *802.1p* либо *IP diffserv*, то данный параметр не используется (default vlan priority не будет применяться к пакетам, содержащим заголовок IP, в случае использования одного из режимов QoS: *DSCP only* , *DSCP preferred* , *802.1 p preferred*);
- *Режим QoS* – режим использования QoS:
  - *Только DSCP* – распределять пакеты по очередям только на основании приоритета IP diffserv;
  - *Только 802.1 p* – 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 802.1 p* – 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.

5.1.11.5 Распределение приоритетов



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

Имеются следующие кнопки:

- «*Применить*» − применить установленные настройки;
- «*Подтвердить*» − подтвердить измененные настройки;
- «*По умолчанию*» − установить настройки по умолчанию;
- «*Сохранить*» − сохранить настройки во Flash-память устройства без применения.

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

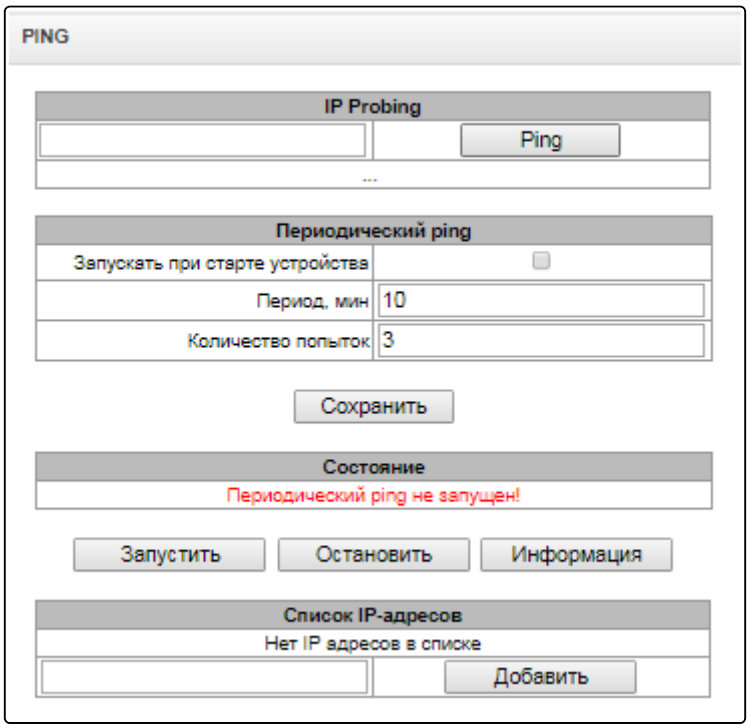
Очередь 3 является наиболее приоритетной, очередь 0 − наименее приоритетной. Взвешенное распределение пакетов по исходящим очередям 3/2/1/0 следующее: 8/4/2/1.

5.1.12 Сетевые утилиты

5.1.12.1 PING

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

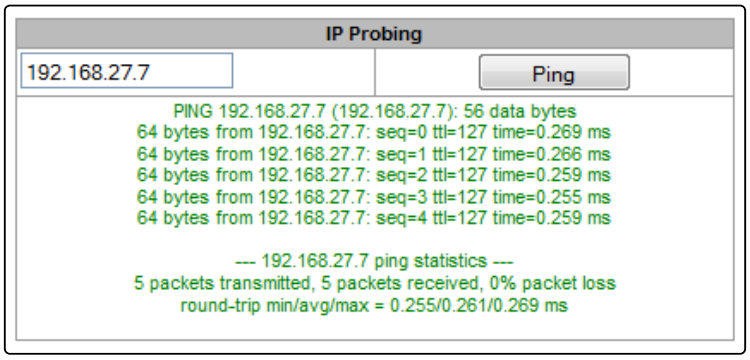
Сетевые утилиты → PING



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

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

Сетевые утилиты → PING

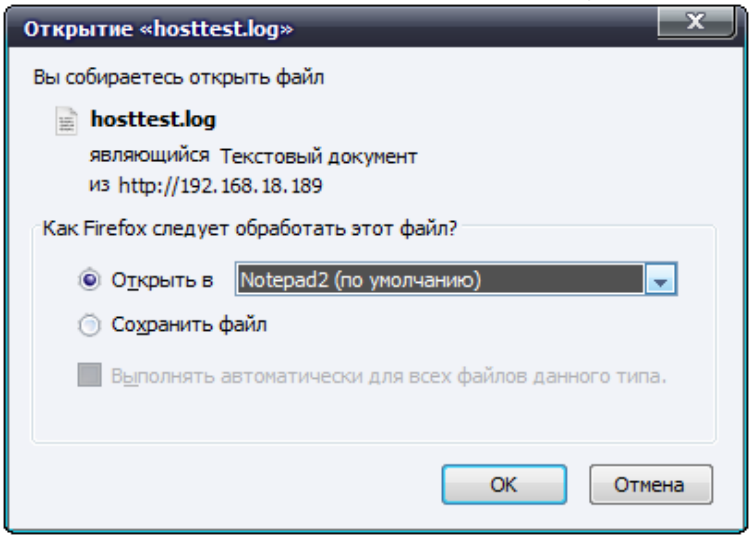


Периодический ping − используется для периодического контроля соединений до устройств в сети.

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

Состояние

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



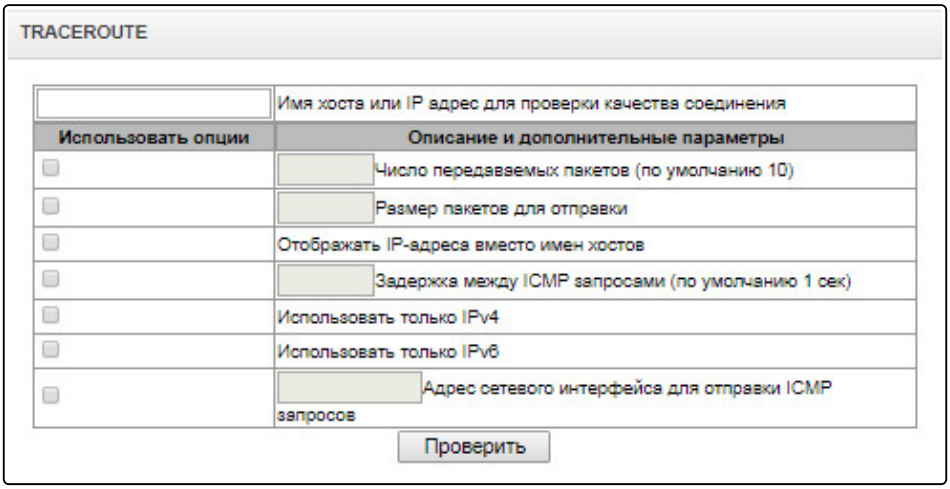
Список IP-адресов − список IP-адресов, на которые будут отправляться периодические ping-запросы.

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

5.1.12.2 TRACEROUTE

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

Сетевые утилиты → TRACEROUTE



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 1 сек)* − 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:

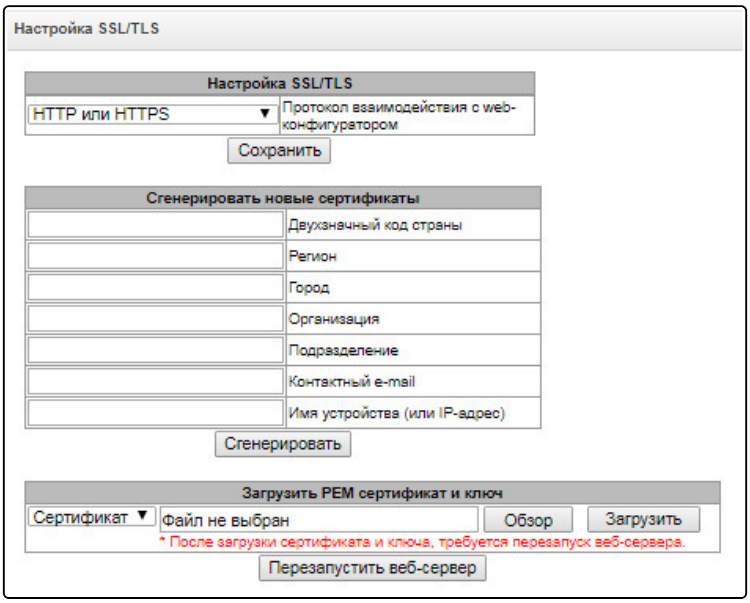
- номер узла и его IP-адрес (либо сетевое имя);
- процент потерянных пакетов (Loss%);
- количество отправленных пакетов (Snt);
- время кругового обращения последнего пакета (Last);
- среднее время кругового обращения пакета (Avg);
- лучшее время кругового обращения пакета (Best);
- худшее время кругового обращения пакета (Wrst);
- среднеквадратичное отклонение задержек для каждого узла (StDev).

Сетевые утилиты → TRACEROUTE → Ввод IP-адреса сетевого устройства

HOST:	smg2016	Loss%	Snt	Last	Avg	Best	Wrst	StDev
1.|--	192.168.18.56	0.0%	10	0.1	0.1	0.1	0.2	0.0

5.1.13 Безопасность

5.1.13.1 Настройка SSL/TLS



Данный раздел предназначен для получения самоподписанного сертификата, который позволяет использовать шифрованное подключение к шлюзу по протоколу HTTP и загрузку/выгрузку файлов конфигурации по протоколу FTPS.

- *Протокол взаимодействия с web-конфигуратором* – режим подключения к web-конфигуратору:
  - *HTTP или HTTPS* – разрешено как нешифрованное подключение – по HTTP, так и шифрованное – по HTTPS. При этом подключение по HTTPS возможно только при наличии сгенерированного сертификата;
  - *только HTTPS* – разрешено только шифрованное подключение по HTTPS. Подключение по HTTPS возможно только при наличии сгенерированного сертификата.

Сгенерировать новые сертификаты

> ⚠ **Данные параметры необходимо вводить латинскими буквами.**

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

Загрузить PEM сертификат и ключ

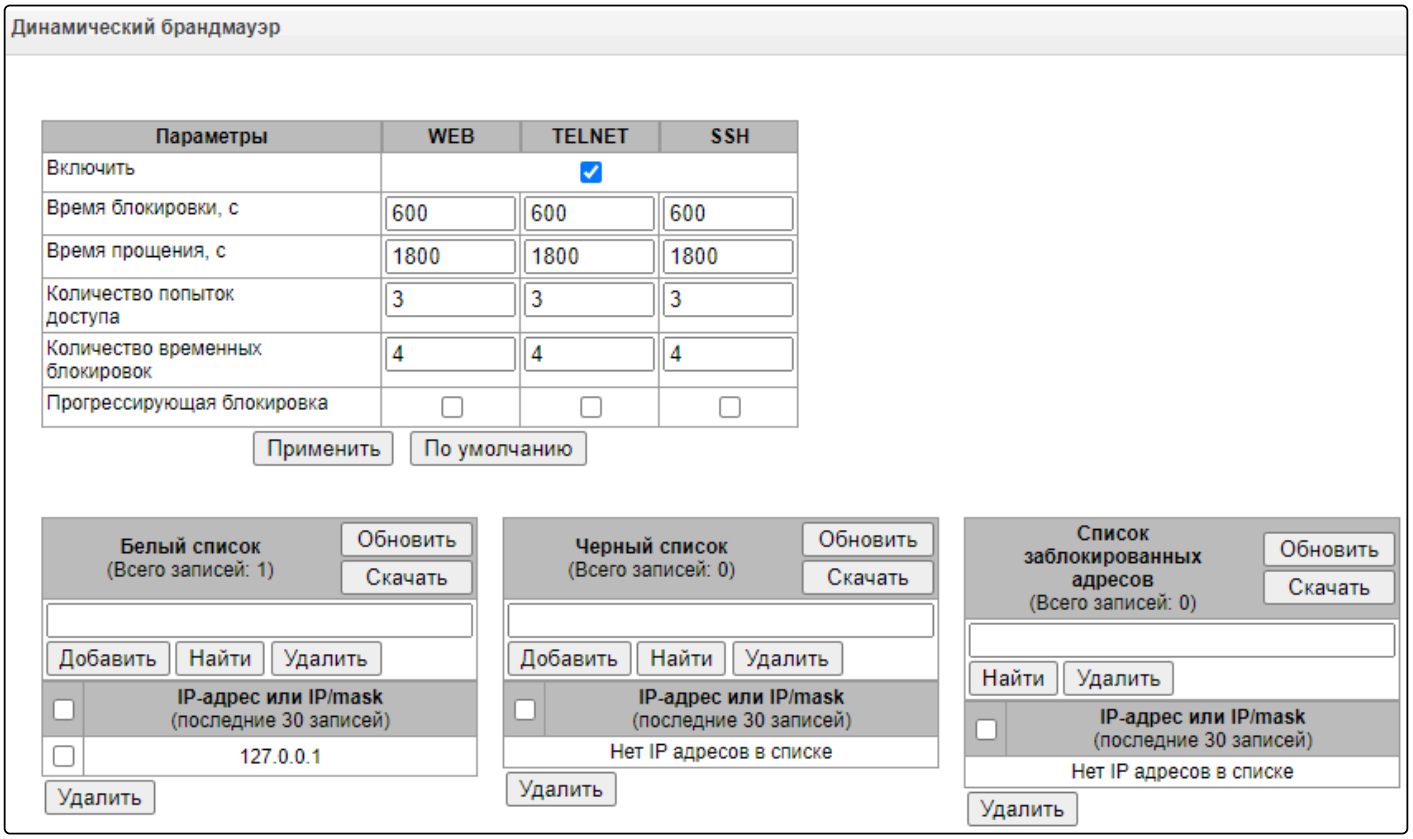
Раздел позволяет загрузить заранее сгенерированный и подписанный PEM-сертификат и ключ. Для загрузки следует выбрать в выпадающем меню тип загружаемого файла. Нажать кнопку *«Обзор»* и выбрать требуемый файл. После чего нажать кнопку *«Загрузить»*.

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

5.1.13.2 Динамический брандмауэр

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

В качестве неудачной попытки может быть идентифицирован подбор аутентификационных данных для web-конфигуратора или по протоколу SSH, т.е. попытки зайти в интерфейс управления с неверным логином или паролем.



Параметры:

- *Включить* – запустить утилиту динамический брандмауэр;
- *Время блокировки, с* – время в секундах, на протяжении которого доступ с подозрительного адреса будет блокирован;
- *Время прощения, с* – время, через которое адрес, с которого пришел проблемный запрос, будет забыт, если ни разу не был заблокирован;
- *Количество попыток доступа* – максимальное число неудачных попыток доступа к сервису, прежде чем хост будет заблокирован с помощью динамического брандмауэра;
- *Количество временных блокировок* – количество блокировок, после которых проблемный адрес будет принудительно занесен в черный список;
- *Прогрессирующая блокировка* – при установленном флаге каждая очередная блокировка адреса будет вдвое больше предыдущей, и для блокировки адреса будет использоваться вдвое меньше попыток доступа. Например, в первый раз адрес был заблокирован на 30 секунд после 16 попыток, во второй раз – на 60 секунд после 8 попыток, в третий раз – на 120 секунд после 4 попыток и так далее.

Белый список (последние 30 записей) – список IP-адресов или подсетей, которые не могут быть блокированы динамическим брандмауэром.

Черный список (последние 30 записей) – список запрещенных адресов или подсетей, доступ с которых будет всегда заблокирован. Всего может быть создано до 131072 записей на SMG-1016M и 1048576 записей на SMG-2016.

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

Возможно ввести как IP-адрес, так и подсеть.

Для ввода подсети необходимо ввести данные в следующем формате:

AAA.BBB.CCC.DDD/mask

Пример:

192.168.0.0/24 – запись соответствует адресу сети 192.168.0.0 с маской 255.255.255.0.

- Скачать белый/черный список IP-адресов целиком – в web-конфигураторе 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 динамического брандмауэра.

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

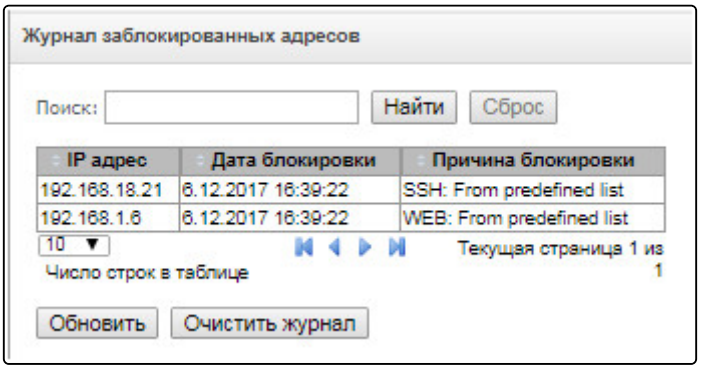
Обновление списков происходит по нажатию кнопки *«Обновить»* напротив заголовка.

Log-файл работы динамического брандмауэра находится в файле **pbx _ sip _ bun . log**.

5.1.13.3 Журнал заблокированных адресов

В данном разделе отображается журнал заблокированных динамическим брандмауэром адресов, который позволяет проанализировать, когда и какие адреса попадали в блокировку за все время с момента включения шлюза.

Безопасность → Журнал заблокированных адресов

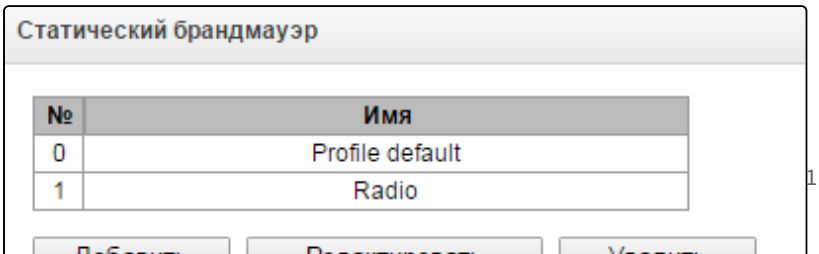


- *Поиск* – ввод адреса для поиска в таблице заблокированный адресов;
- *IP-адрес* – IP-адрес, который попадал в блокировку;
- *Дата блокировки* – дата и время попадания IP-адреса в блокировку;
- *Причина блокировки* – пояснение, каким сервисом и за что произведена блокировка;
- *Обновить* – обновить журнал заблокированных адресов;
- *Очистить журнал* – удалить все записи из журнала заблокированных адресов.

5.1.13.4 Статический брандмауэр

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.

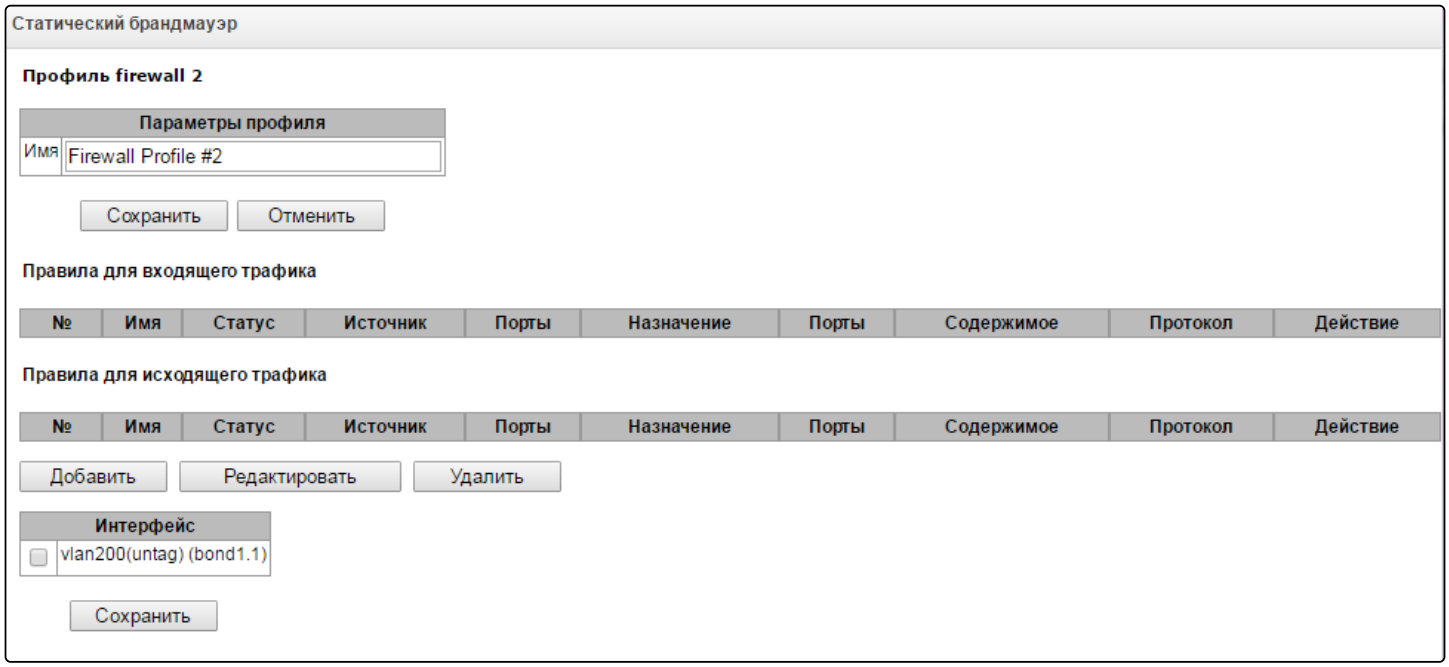
Профили firewall

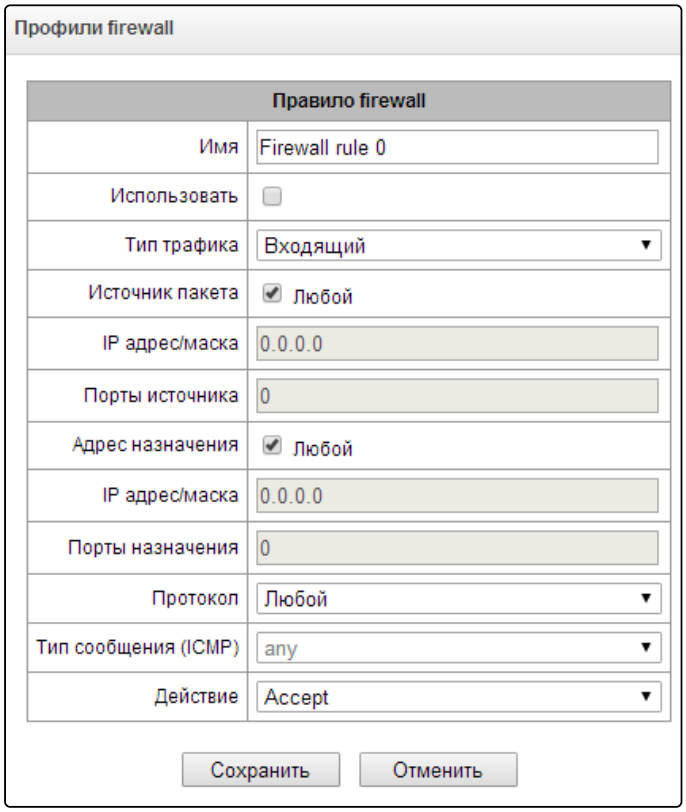


Для создания, редактирования и удаления профилей firewall используются кнопки:

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

Программное обеспечение позволяет настроить правила firewall для входящего, исходящего и транзитного трафика, а также для определенных сетевых интерфейсов.





- *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 SMG;
  - *исходящий* – отправляемый SMG;
- *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.

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

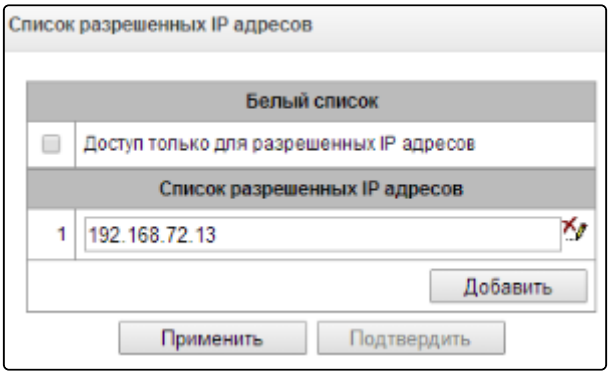
Также в *профиле firewall* возможно указать сетевые интерфейсы, для которых будут использоваться правила данного профиля.

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

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

5.1.13.5 Список разрешенных IP-адресов

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

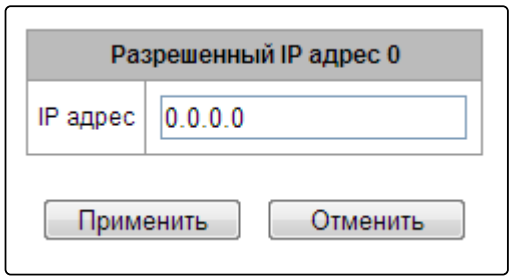


- *Доступ только для разрешенных IP адресов* − при установке флага применяется список разрешенных IP-адресов, иначе доступ разрешен с любого адреса.

Существует возможность разрешать доступ для подсетей, для этого необходимо задать адрес в формате IP/mask, например: 192.168.0.0/24.

- «*Применить*» − применить изменения;
- «*Подтвердить*» − подтвердить изменения;
- «*Сохранить*» − сохранить настройки доступа в файл конфигурации без применения.

Для создания, редактирования и удаления списка разрешенных адресов используются кнопки:



 − «*Добавить*»;

 − «*Редактировать*»;

 − «*Удалить*».

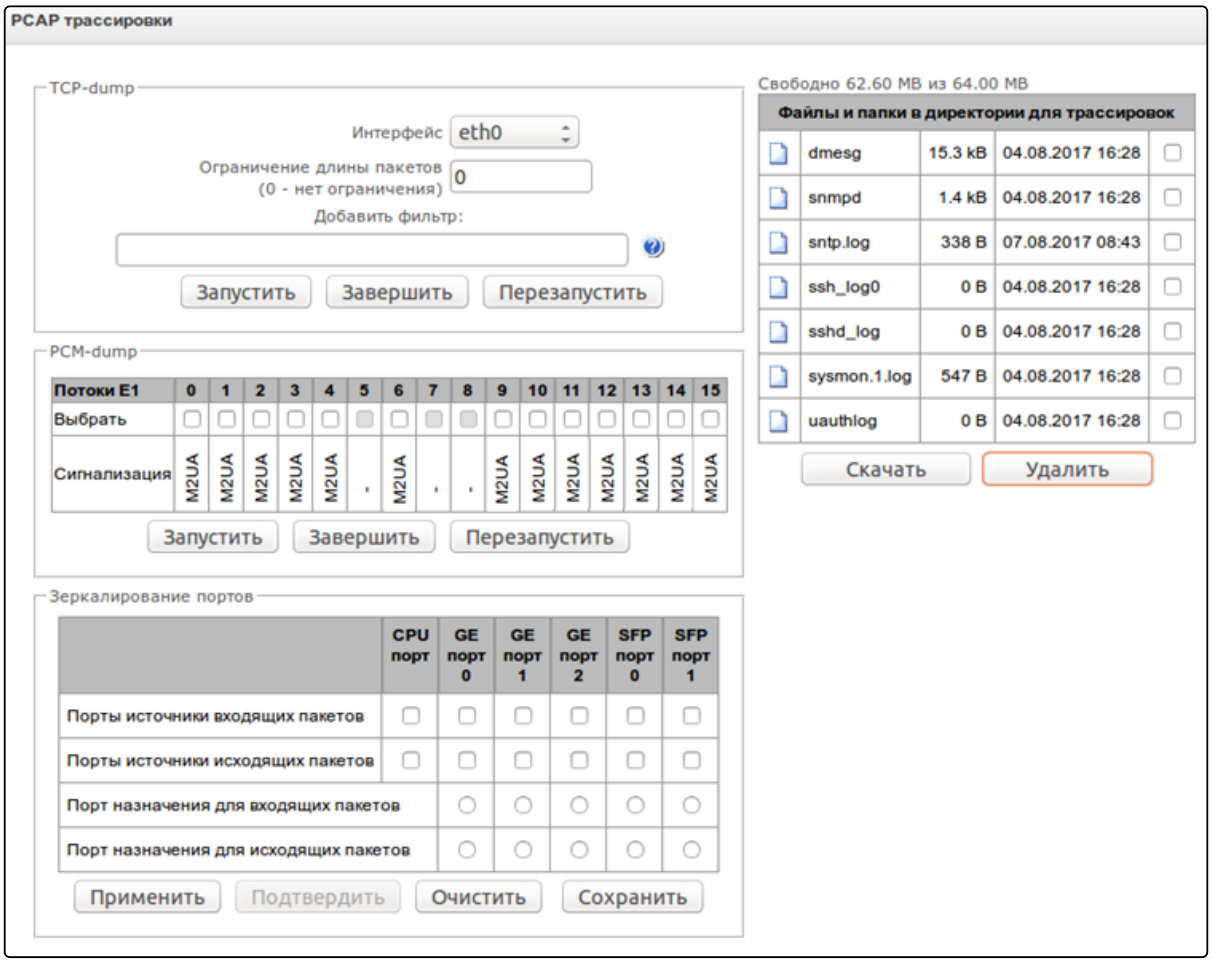
После формирования списка адресов необходимо нажать кнопку *«Применить»* и *«Подтвердить»*, если в течение 60 секунд не подтвердить изменения, настройки возвращаются к предустановленным значениям − это позволяет защитить пользователя от потери доступа к устройству.

При создании правила настраиваются следующие параметры:

5.1.14 Трассировки

5.1.14.1 PCAP-трассировки

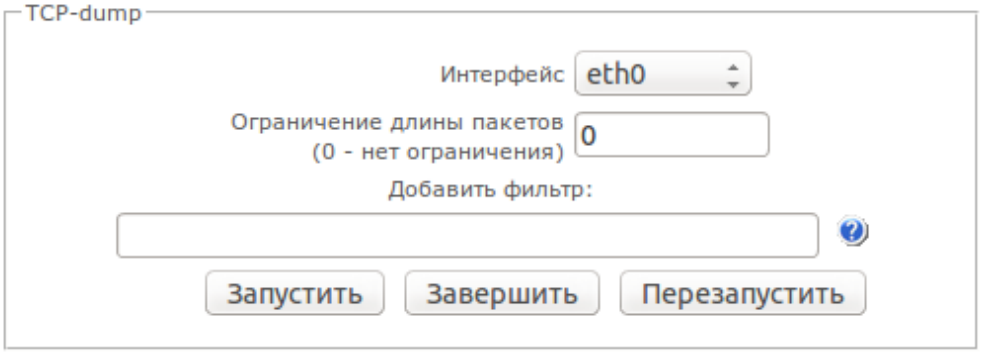
В меню производится настройка параметров для анализа сетевого трафика и протоколов TDM-сети.



TCP-dump – настройки для утилиты TCP-dump:

TCP-dump – утилита, позволяющая перехватывать и анализировать сетевой трафик.

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



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**.

1. **proto** – задает протокол, к которому должны относиться пакеты. Данный 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 классификаторов 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 классификаторов.

Примеры фильтров:

dst foo – отбирает пакеты, в которых поле адреса получателя IPv4/IPv6 содержит адрес хоста foo;

src net 128.3.0.0/16 – отбирает все пакеты IPv4/IPv6, 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 утилиты, начать заново сбор данных.

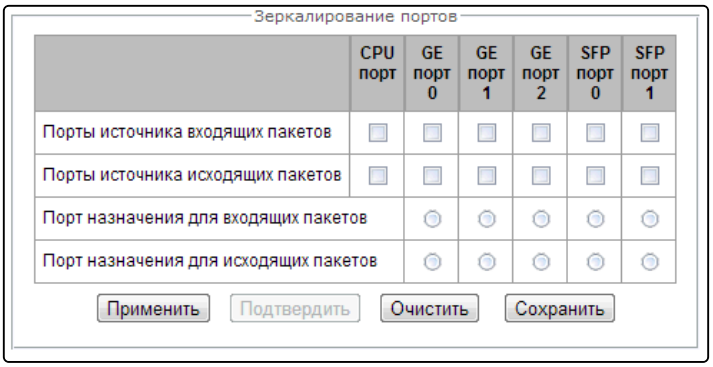
В блоке ***Файлы и папки в директории для трассировок*** доступен список файлов трассировок.

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

PCM-dump – настройки для утилиты PCM-dump.

PCM-dump – утилита, позволяющая перехватывать и анализировать сигнальный трафик по потокам E1. На устройстве реализована возможность снятия PCM-dump как с одного потока, так и с нескольких, при снятии PCM-dump с нескольких потоков одновременно трассировка записывается в один файл, в

который заносятся сигнальные сообщения с нескольких потоков, при этом одновременное снятие PCM-dump с потоков с разными протоколами сигнализациями невозможна.



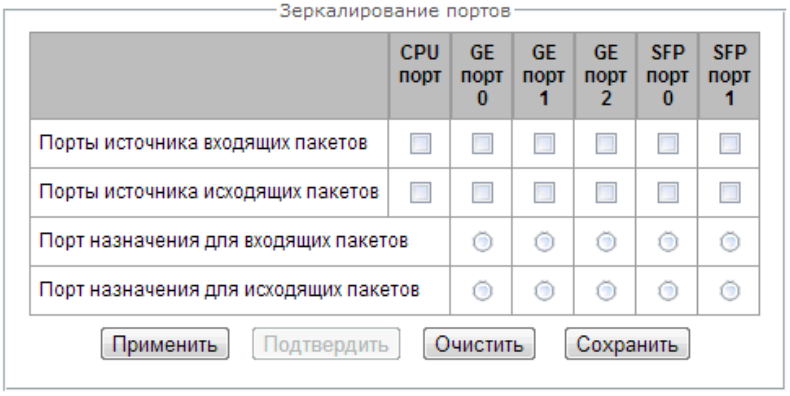
- *Выбрать* − выбор потоков E1;
- *Сигнализация* − протокол сигнализации, выбранный на потоке.

Описание кнопок:

- *Запустить* − начать сбор данных;
- *Завершить* − закончить сбор данных;
- *Перезапустить* − перезапустить утилиту и начать сбор данных заново.

Зеркалирование портов[1] **– настройки зеркалирования трафика:**

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



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.

---

[1] *Только для SMG-1016M.*

Описание кнопок:

- *«Применить»* − применить параметры настройки зеркалирования;
- *«Подтвердить»* − подтвердить примененные параметры настройки зеркалирования;
- *«Очистить»* − сбросить настройки зеркалирования;

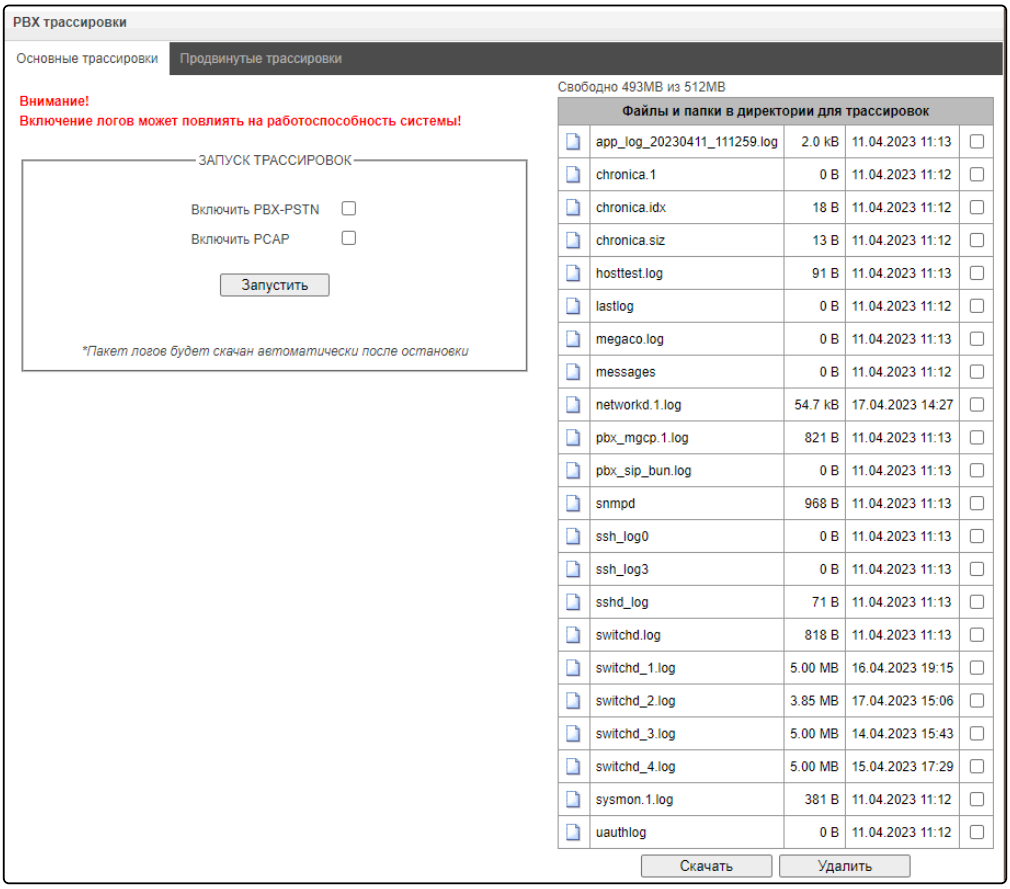
- *«Сохранить»* − сохранить параметры настройки зеркалирования.

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

5.1.14.2 PBX трассировки

5.1.14.2.1 Вкладка "Основные трассировки"

Использование трассировки IP PBX приводит к задержкам в работе устройства. Данный вид отладки рекомендуется использовать только в случае возникновения проблем в работе шлюза для выявления их причин.



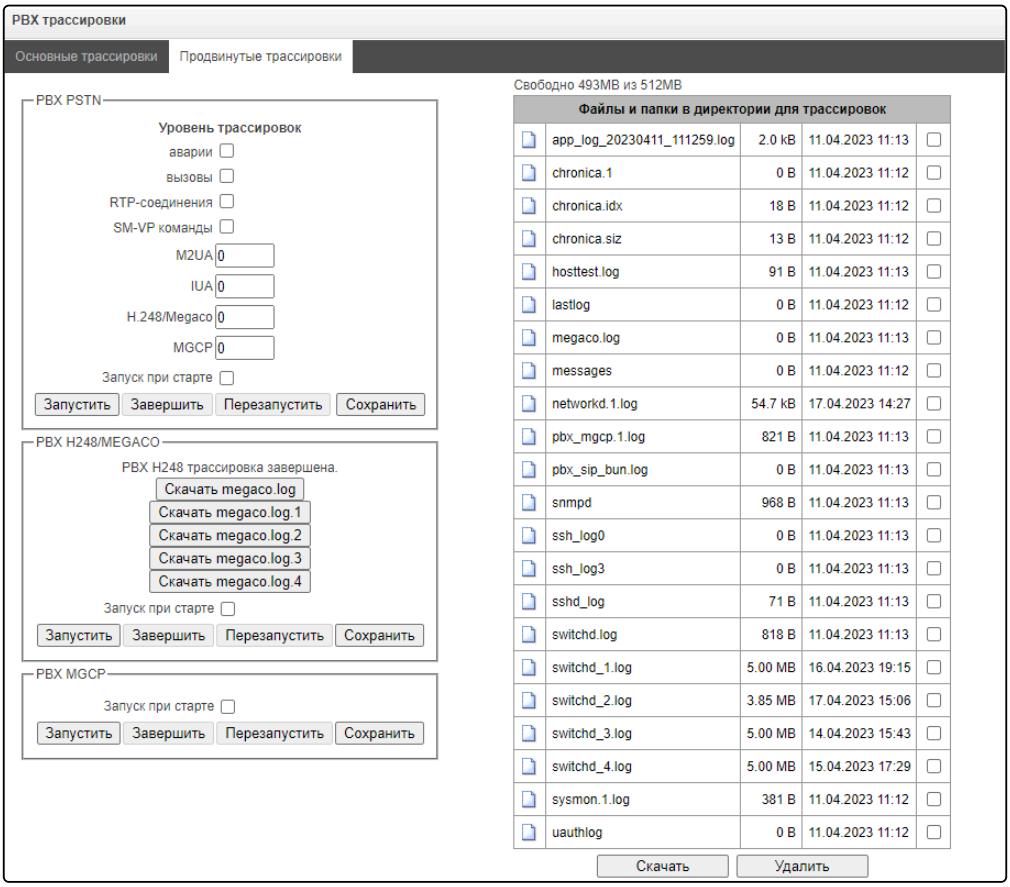
Следующие опции позволяют наиболее быстро выявить причины при некорректной работе шлюза.

Включить PBX-PSTN – позволяет запустить лог работы и взаимодействия узлов устройства, а также обмен сообщениями по различным протоколам.

Включить PCAP – позволяет запустить TCP-dump для основного сетевого интерфейса.

Для запуска сбора данных необходимо включить необходимые опции и нажать кнопку «*Запустить*». Остановка сбора данных производится кнопкой «*Завершить*». После остановки сбора данных автоматически сформируется и будет скачан архив со всеми снятыми трассировками.

5.1.14.2.2 Вкладка "Продвинутые трассировки"



В блоке **PBX PSTN** снимается лог работы и взаимодействия узлов устройства, а также обмен сообщениями по различным протоколам. В параметрах PBX PSTN настраивается уровень трассировок по событиям и протоколам.

В блоке **PBX H.248/MEGACO** снимается трассировка сообщений и ошибок протокола H.248:

- *Запустить* – начать сбор данных;
- *Завершить* – закончить сбор данных;
- *Перезапустить* – перезапуск, начать заново сбор данных.

В блоке **PBX MGCP** снимается трассировка сообщений и ошибок протокола MGCP:

- *Запустить* – начать сбор данных;
- *Завершить* – закончить сбор данных;
- *Перезапустить* – перезапуск, начать заново сбор данных.

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»*.

5.1.14.3 Настройки syslog

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

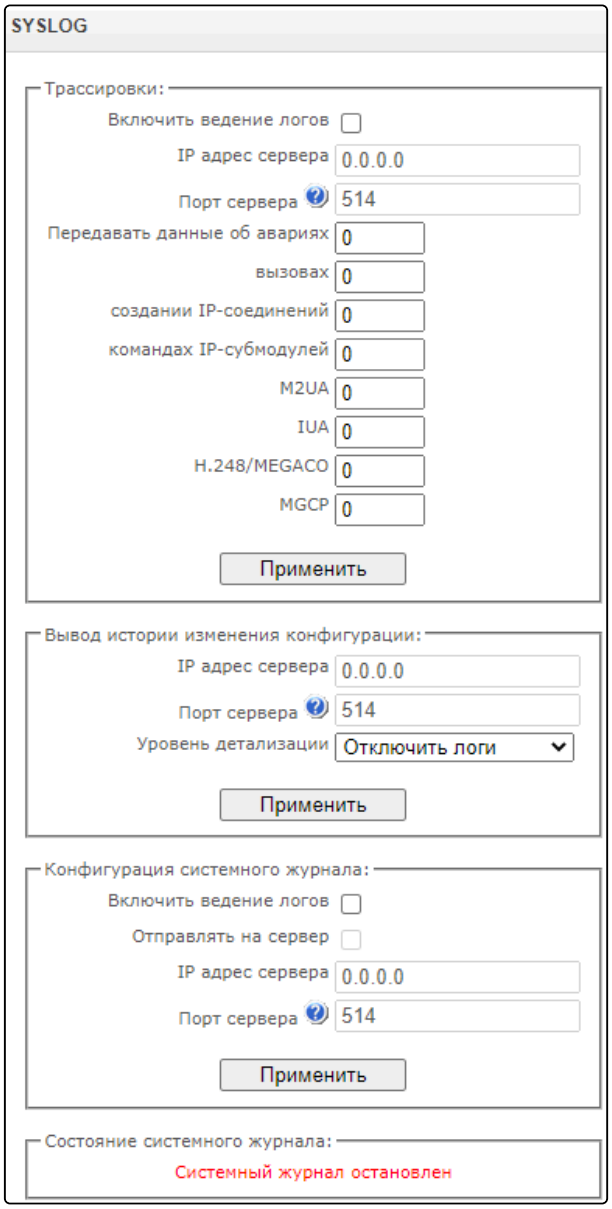
SYSLOG – протокол, предназначенный для передачи сообщений о происходящих в системе событиях. Программное обеспечение шлюза позволяет формировать журналы данных по работе приложений системы, работе протоколов сигнализации, авариям и передавать их на SYSLOG-сервер.

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

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

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

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



- *IP адрес сервера* – адрес сервера, на который будет передаваться трассировка;
- *Порт сервера* – порт сервера, на который будет передаваться трассировка.

Вывод истории введенных команд – используется для сохранения истории изменений в настройках шлюза.

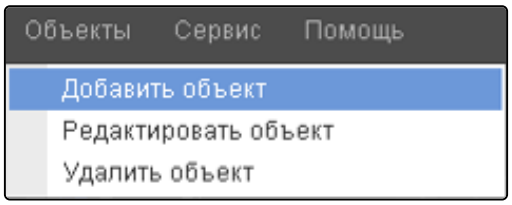
- *IP адрес сервера* − адрес сервера, на который будет передаваться журнал введенных команд;
- *Порт сервера* − порт сервера, на который будет передаваться журнал введенных команд;
- *Уровень детализации* − уровень детализации журнала введенных команд:
- *Отключить логи* − не формировать журнал введенных команд;
- *Стандартный* − в сообщениях передается название измененного параметра;
- *Полный* − в сообщениях передается название измененного параметра и значения параметра до и после изменения.

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

- *Включить ведение логов* − при установленном флаге история событий, касающихся доступа к устройству будет сохраняться, при отсутствии флага ведение журнала остановлено;
- *Отправлять на сервер* − при установленном флаге системный журнал будет сохраняться на сервере по указанному адресу;
- *IP адрес сервера* − адрес сервера для хранения системного журнала;
- *Порт сервера* − порт сервера, на который будет передаваться системный журнал.

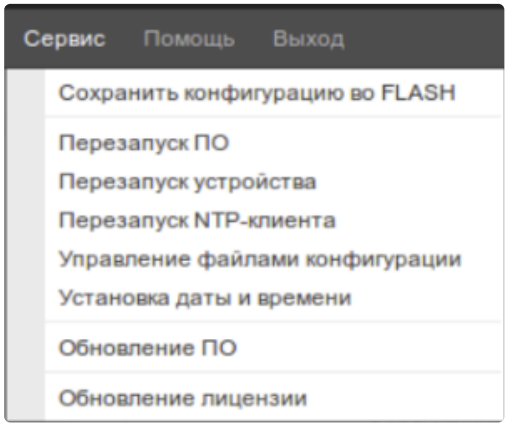
5.1.15 Работа с объектами и меню «Объекты»

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



5.1.16 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 NTP-сервера необходимо выбрать меню *«Сервис» − «Перезапуск NTP клиента»*.

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

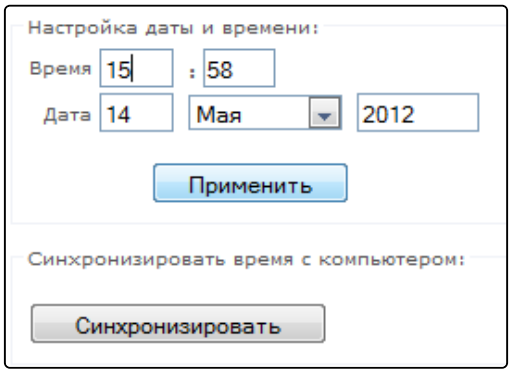
Для ручной настройки локальных даты и времени на устройстве необходимо выбрать меню *«Сервис» − «Установка даты и времени»*, см. раздел Настройка даты и времени.

Для обновления ПО через web-конфигуратор необходимо выбрать меню «*Сервис*» − *«Обновление ПО»,* см. раздел Обновление ПО через web-конфигуратор.

Для обновления/ добавления лицензий необходимо выбрать меню «*Сервис*» − *«Обновление лицензии»,* см. раздел Лицензии.

5.1.17 Настройка даты и времени

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



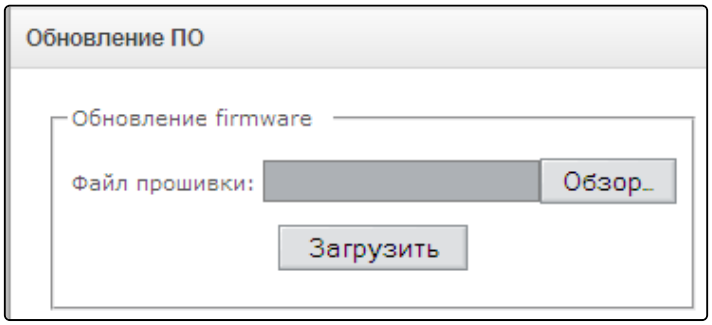
Для сохранения настроек следует воспользоваться кнопкой «*Применить*».

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

5.1.18 Обновление ПО через web-конфигуратор

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

Откроется форма для загрузки файлов ПО на устройство:



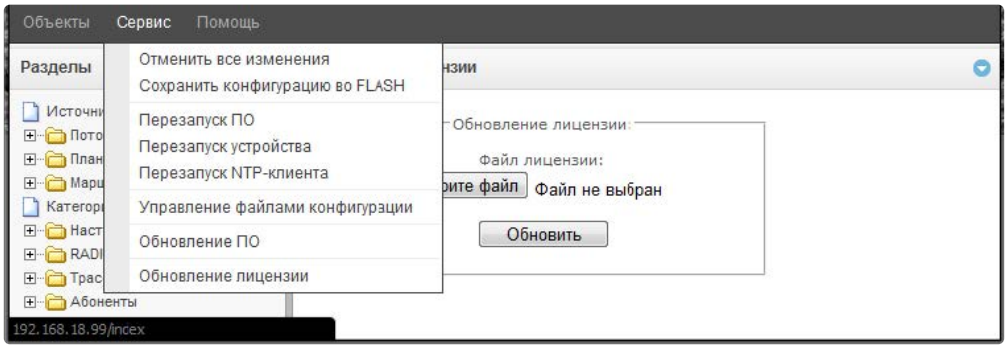
- *Обновление firmware* – обновляет ПО управляющей программы и/или ядро Linux.

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

5.1.19 Лицензии

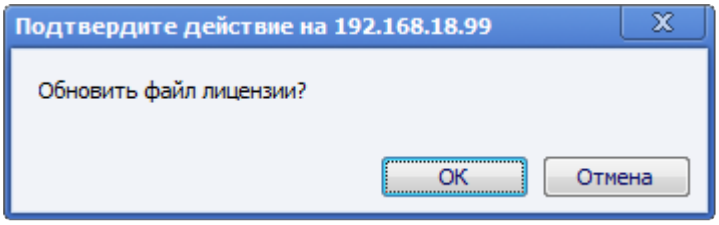
Для обновления/добавления лицензий необходимо получить файл лицензии, обратившись в коммерческий отдел ООО «Предприятие «ЭЛТЕКС» по адресу eltex@eltex-co.ru или по телефону +7(383) 274-48-48, указав серийный номер и MAC-адрес устройства (см. раздел Просмотр заводских параметров и информации о системе).

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»*.

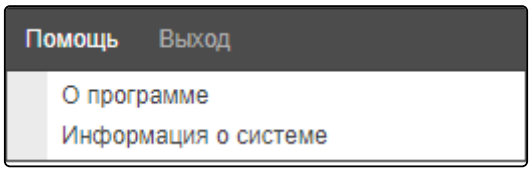
Для обновления файла лицензии требуется подтверждение.



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

5.1.20 Меню «Помощь»

Меню предоставляет сведения о текущей версии программного обеспечения, заводские параметры и другую системную информацию.



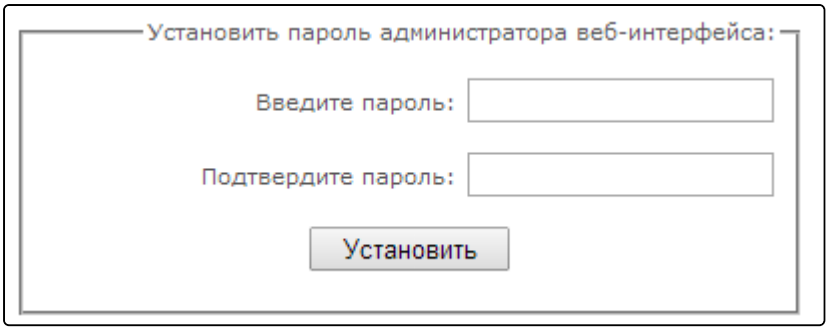
5.1.21 Установка пароля для доступа через web-конфигуратор

Ссылка 

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

Установить пароль администратора web-интерфейса:

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

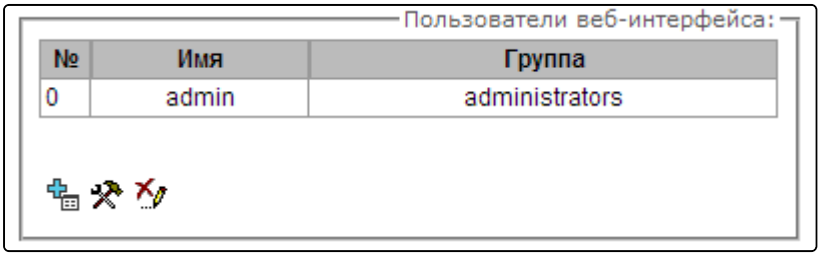


Для сохранения конфигурации необходимо использовать меню *«Сервис» − «Сохранить конфигурацию»*.

Пользователи web-интерфейса:

Данный блок предназначен для настройки ограничения доступа к web-конфигуратору на уровне пользователей. В системе всегда есть администратор, который может добавлять и удалять пользователей, а также назначать уровень доступа.

Для создания, редактирования и удаления пользователя используются кнопки:



− *«Добавить пользователя»;*

− *«Редактировать параметры пользователя»;*

− *«Удалить пользователя»*.

Изменять права доступа администратора и удалять его из списка пользователей программа не позволяет, что обеспечивает гарантированный вход в программу администратора системы.

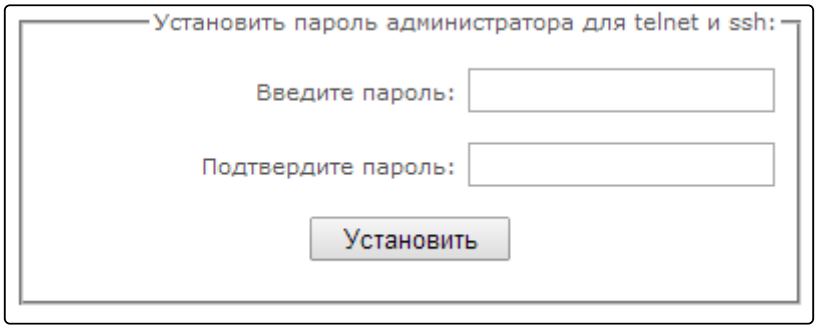
- *[имя пользователя]* − имя пользователя для входа в web-конфигуратор;
- *[группа]* − тип группы пользователей. Данный параметр должен иметь значение Webs;
- *[введите пароль]* − пароль для доступа в web-конфигуратор;
- *[подтвердите пароль]* − подтвердить пароль для доступа в web-конфигуратор.

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

Установить пароль администратора для Telnet и SSH:

Данный блок предназначен для изменения пароля доступа через Telnet, SSH и консоль.

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



5.1.22 Просмотр заводских параметров и информации о системе

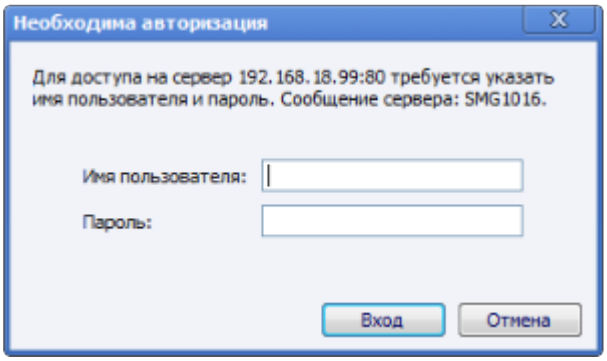
Для просмотра необходимо использовать меню *«Помощь» − «Информация о системе»*.

Заводские параметры также указаны в шильде (наклейке) на нижней части корпуса изделия.

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

5.1.23 Выход из конфигуратора

При нажатии на ссылку *«Выход»* осуществляется выход из конфигуратора, после чего в браузере 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.

5.2 Настройка SMG (SIGTRAN) с помощью командной строки

В SMG предусмотрено несколько отладочных терминалов, каждый из них выполняет определенную функцию:

- *Терминал (com-порт)* – предназначен для конфигурирования устройства посредством интерфейса командной строки CLI и смены программного обеспечения;
- *Telnet порт 23* – дубликат терминала (com-порт);
- *SSH порт 22* – дубликат терминала (com-порт).

Система команд для работы со шлюзом SMG в режиме отладки

Для перехода в отладочный режим необходимо подключиться к интерфейсу командной строки CLI и ввести команду `tracemode`.

Таблица 18 – Команды режима отладки

Команда	Описание
`help`	просмотр списка доступных команд
`quit`	выход из отладочного режима
`logout`	выход из отладочного режима
`exit`	выход из отладочного режима
`history`	вывод списка ранее введенных команд
`radact [on/off]`	включение/выключение RADIUS
`radshow`	просмотр списка запросов к RADIUS-серверу
`resolve`	проверка разрешения доменных имен. Параметр: доменное имя
`rstat`	просмотр статистики работы по протоколу RADIUS
`q931timers`	просмотр значений таймеров Q.931

`mspping [on/off] <idx>`	включение/выключение опроса сигнального процессора, idx – номер сигнального процессора – 0..5
`stream [stream]`	просмотр состояния потоков E1, либо состояния конкретного потока, stream – номер потока 0..15
`e1stat <stream>`	просмотр счетчиков потока E1
`alarm`	просмотр информации о журнале аварий
`sync`	просмотр информации об источниках синхронизации
`syncfreq`	просмотр информации о частотах синхронизации
`setsync`	принудительная смена источника синхронизации. Параметр – <номер потока>
`checkmod`	проверка срабатывания модификатора номеров по определенному номеру. Параметры: <таблица модификатора> <проверяемый телефонный номер>
`frmtrace`	включение трассировки низкого уровня на сигнальных потоках E1. Параметры: <уровень> <номер потока> <использование> • уровень: l1, l2, l3 • использование: 1 – вкл., 0 – выкл.
`cic <linkset>`	просмотр состояния каналов в группе линий, <linkset> – номер группы линий ОКС-7
`checknum`	проверка номера по плану нумерации
`cfg_read`	применение текущей конфигурации, данная команда приводит к сбросу и повторной инициализации потоков E1
`callref`	вывод информации об активных SIP-вызовах
`rtpdebug <level>`	включение отладки RTP свитча, <level> – уровень отладки **Использование данной команды может привести к зависанию шлюза при работе под нагрузкой.**
`mspcports`	просмотр состояния RTP-портов
`mspcshow <device>`	просмотр статистики соединений на сигнальных процессорах
`route`	просмотр информации о сетевых маршрутах, обрабатываемых телефонией
`showcall`	просмотр информации о текущих активных вызовах
`license`	просмотр информации о текущих активных лицензиях
`mspreglog`	включение трассировки команд сигнальных процессоров
`mspunreglog`	выключение трассировки команд сигнальных процессоров
`talk`	просмотр статистики по вызовам
`sys`	просмотр системной информации, версии программного обеспечения

`trace`	функции трассировки
`regcon`	команда необходима для возврата в нормальный режим после использования команды **`unregcon`** (если приложение не завершилось аварийно)
`unregcon`	команда используется в крайних случаях для определения точного места аварийного завершения приложения
`stop`	перезапуск программного обеспечения
`sigtran_state`	просмотр состояния SIGTRAN-объектов
`megaco_iface`	просмотр состояния H.248/Megaco-интерфейса
`megaco_chans`	просмотр состояния H.248/Megaco E1-каналов
`megaco_term`	просмотр состояния H.248/Megaco-терминаций
`megaco_ctxt`	просмотр состояния H.248/Megaco-контекстов

5.2.1 Команды трассировки, доступные через отладочный порт

5.2.1.1 Глобальное включение отладки

Синтаксис команды: `trace start`

5.2.1.2 Глобальное выключение отладки

Синтаксис команды: `trace stop`

5.2.1.3 Включение/выключения отладки для определенных аргументов

Синтаксис команды: `trace <POINT> on/off <IDX> <LEVEL>`

Параметры:

<POINT> − аргумент;
<IDX> − числовой параметр;
<LEVEL> − уровень отладки.

Таблица 19 − Допустимые аргументы (*<POINT>*)

Значение <POINT>	**Расшифровка команды**	**Значение <IDX>**
hwpkt	трассировка содержимого пакета первого уровня обмена основного приложения с драйвером потока E1	0..15
stream	трассировка потока E1	0..15
port	трассировка работы приложения	не используется
isup	трассировка работы подсистемы ISUP протокола ОКС-7	не используется
mtp3	трассировка работы уровня MTP3 протокола ОКС-7 по потоку E1	0..15
pril3	трассировка работы третьего уровня протокола DSS1 по потоку E1	0..15

Значение <POINT>	Расшифровка команды	Значение <IDX>
sw	трассировка работы коммутационного поля	не используется
mspc	трассировка IP-проключений	не используется
mspd	трассировка работы сигнального процессора	0..7
net	трассировка работы сети передачи данных 2 уровня	не используется
sync	трассировка работы источников синхронизации	не используется
snmp	трассировка работы SNMP-протокола	не используется
np	трассировка работы плана нумерации (маршрутизации)	не используется
mod	трассировка работы модификаторов	не используется
alarm	трассировка аварийных состояний шлюза	не используется
radius	трассировка работы RADIUS-протокола	не используется

5.3 Настройка SMG (SIGTRAN) через Telnet, SSH и 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 CLI). 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).

Изменения конфигурации, выполненные через CLI (Command Line Interface) или web-конфигуратор, применяются непосредственно после совершения.

Для сохранения конфигурации в энергонезависимую память устройства необходимо выполнить команду `copy running_to_startup`.

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

Ниже представлен полный перечень команд в алфавитном порядке.

5.3.1 Перечень команд CLI

Команда	Параметр	Значение	Действие
`?`			Показать перечень доступных команд
`alarm global`			Показать информацию о текущих авариях
`alarm list clear`			Очистить журнал аварийных событий
`alarm list show`			Показать журнал аварийных событий с указанием типа и статуса аварии, времени возникновения и параметров локализации.
`config`			Переход в режим конфигурирования параметров устройства

Команда	Параметр	Значение	Действие
`CPU load statistic`			Показать статистику загрузки CPU за последнюю минуту
`firmware update tftp`	**<FILE> <SERVERIP>**	имя файла с ПО IP-адрес в формате AAA.BBB.CCC.DDD	Обновление программного обеспечения без автоматической перезагрузки шлюза FILE – имя файла с ПО SERVERIP – IP-адрес TFTP сервера
`firmware update ftp`	`<FILE>` `<SERVERIP>`	имя файла с ПО IP-адрес в формате AAA.BBB.CCC.DDD	Обновление программного обеспечения без автоматической перезагрузки шлюза FILE – имя файла с ПО SERVERIP – IP-адрес FTP-сервера
`firmware update usb`	`<FILE>`	имя файла с ПО	Обновление программного обеспечения без автоматической перезагрузки шлюза FILE – имя файла с ПО
`firmware update_and_reboot tftp`	`<FILE>` `<SERVERIP>`	имя файла с ПО IP-адрес в формате AAA.BBB.CCC.DDD	Обновление программного обеспечения с автоматической перезагрузкой шлюза FILE – имя файла с ПО SERVERIP – IP-адрес TFTP-сервера
`firmware update_and_reboot ftp`	`<FILE>` `<SERVERIP>`	имя файла с ПО IP-адрес в формате AAA.BBB.CCC.DDD	Обновление программного обеспечения с автоматической перезагрузкой шлюза FILE – имя файла с ПО SERVERIP – IP-адрес FTP-сервера
`firmware update_and_reboot usb`	`<FILE>`	имя файла с ПО	Обновление программного обеспечения с автоматической перезагрузкой шлюза FILE – имя файла с ПО
`history`			Просмотр истории о введенных командах
`license key`			Посмотреть содержимое файла лицензии
`license download`	`<FILE>` `<SERVERIP>`	имя файла лицензии IP-адрес сервера в формате AAA.BBB.CCC.DDD	Загрузить файл лицензии с указанного адреса
`license update`			Обновить лицензию
`license reset`	`no/yes`		Удалить все установленные лицензии
`management`			Переход в режим управления потоками ОКС-7
`md5sum`	`<FILE>`		Посмотреть md5-сумму файла на диске, расположенного в директории /tmp/log
`password`			Смена пароля для доступа через CLI

Команда	Параметр	Значение	Действие
`pcmdump single_stream`	`<STREAM>` `<FILE>`	0-15 строка	Собрать пакеты с указанного потока E1. STREAM – номер потока для захвата; FILE – файл для записи
`pcmdump multi_streams`	`<STREAMS>` `<FILE>`	0-15 строка	Собрать пакеты с указанных потоков E1. STREAMS – номера потоков для захвата; FILE – файл для записи
`quit`			Завершить данную сессию CLI
`reboot`	`<YES_NO>`	yes/no	Перезагрузить устройство
`sh`			Перейти из CLI в Linux Shell
`show system info`			Показать системную информацию
`show enviroment`			Показать состояние аппаратной платформы
`sntp retry`			Отправка SNTP-запроса к серверу для синхронизации времени
`space hint`	`<YES_NO>`	yes/no	Дополнять команду нажатием на кнопку «Пробел»
`tcpdump`	`<DEVICE>` `<FILE>` `<SNAPLEN>`	eth0/eth1/local строка 0-65535	Захватить пакеты с Ethernet-устройства DEVICE – интерфейс для мониторинга; FILE – файл для записи пакетов; SNAPLEN – число байт, захватываемое из каждого пакета. (0 – пакет захватывается полностью).
`tracemode`			Переход в режим снятия трассировки

5.3.2 Смена пароля для доступа к устройству через CLI

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 через CLI, авторизоваться по логину/паролю, ввести команду `password` и нажать клавишу <Enter>.
2. Ввести новый пароль:

```
New password:
```

3. Повторить введенный пароль:

```
Retype password:
Пароль изменен (Password for admin changed by root)
```

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

5.3.3 Режим управления

Для перехода в режим управления сигнальными линками необходимо выполнить команду `management`.

```
SMG> management
Entering management mode.
SMG-[MGMT]>
```

Команда	Параметр	Значение	Действие
`?`			Показать перечень доступных команд
`exit`			Переход на один уровень меню выше
`history`			Просмотр истории введенных команд
`m2ua7link`	`<M2UA_LINK>`	0-15	Переход к управлению параметрами указанного линка M2UA
`nslookup`	`<HOST>`	строка	Запросить IP-адрес для хоста с указанным именем. *HOST* – адрес для запроса
`ping host`	`<HOST>`		Отправить PING-запрос на указанный хост
`ping ip`	`<IP>`	IP- адрес в формате AAA.BBB.CCC.DDD	Отправить PING-запрос на указанный IP-адрес
`quit`			Завершить данную сессию CLI
`top`			Возврат на верхний уровень меню

5.3.3.1 Режим управления линком M2UA

Для перехода в данный режим необходимо в режиме управления выполнить команду `m2ualink <Link>`, где `<Link>` – номер потока с линком M2UA, принимает значения из диапазона от 0 до 15.

```
SMG-[MGMT]> m2ualink 0
E1[0]. Signaling is M2UA
SMG-[MGMT]-[M2UALINK][0]>
```

Команда	Параметр	Значение	Действие
`?`			Показать перечень доступных команд
`exit`			Переход из данного подменю конфигурирования на уровень выше
`link clr outage`			Снять состояние «Локальный отказ процессора» на линке
`link clr congestion`			Снять состояние «Перегрузка» на линке

`link set congestion`			Установить на линке состояние «Перегрузка»
`link set outage`			Установить на линке состояние «Локальный отказ процессора»
`link start emergency`			Инициировать аварийный запуск сигнального линка
`link start normal`			Инициировать нормальный запуск сигнального линка
`link stop`			Выключить сигнальный линк из работы
`quit`			Завершить данную сессию CLI
`top`			Возврат на верхний уровень меню

5.3.4 Режим конфигурирования общих параметров устройства

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

В каждом меню конфигурирования доступна команда `do`, которая позволяет выполнить команду из корневого меню CLI при нахождении в любом подменю конфигурации и команда `top` для перехода в корневое меню CLI.

```
SMG> config
Entering configuration mode.
SMG-[CONFIG]>
```

Команда	Параметр	Значение	Действие
`?`			Показать перечень доступных команд
`alarm set cpu|fans|ram|rom`	**`<VALUE>`**	off|on	Генерация аварий по событиям: загрузки процессора, состоянии вентиляторов, превышении показателей постоянной и оперативной памяти. Off – отключена; On – включена.
`alarm show`			Показать настройки по генерации аварий
`copy running_to_startup`			Записать текущую конфигурацию в энергонезависимую память устройства (в стартовую конфигурацию)
`copy startup_to_running`			Восстановить текущую конфигурацию из стартовой
`count pcm-dump`			Показать количество объектов для снятия PCM-трассировки
`delete pcm-dump`	**`<OBJECT>`**	0-15	Удалить объект для снятия PCM-трассировки
`do`	**`<COMMAND>`**	..	Выполнить команду верхнего уровня
`new pcm-dump`			Создать новый объект для снятия PCM-трассировки

`pcmdump`	**`<OBJECT>`**	0-15	Перейти в режим конфигурирования объекта для снятия PCM-трассировок
`e1`	**`<OBJECT>`**	0-15	Перейти в режим конфигурирования потока E1
`exit`			Переход на один уровень меню выше
`firewall`			Переход в режим конфигурирования firewall
`history`			Просмотр истории введенных команд
`linkset count`			Выводит количество созданных линксетов
`linkset delete`	**`<OBJECT>`**	0-15	Удаление линксета
`linkset edit`	**`<OBJECT>`**	0-15	Перейти в режим редактирования линксета
`linkset list`			Выводит список линксетов
`linkset new`			Создать новый линксет
`modifiers` **`new`**			Добавление модификатора COPM
`modifiers delete`	**`<OBJECT>`**	0-255	Удаление модификатора COPM
`modifiers count`			Выводит количество созданных модификаторов COPM
`modifiers table`	**`<OBJECT>`**	0-255	Перейти в режим редактирования таблицы модификаторов
`network`			Перейти в режим редактирования сетевых параметров
`numplan`			Перейти в режим конфигурирования плана нумерации
`quit`			Завершить данную сессию CLI
`top`			Возврат на верхний уровень меню
`ua`			Переход в режим конфигурирования параметров SIGTRAN

5.3.4.1 Режим конфигурирования параметров SIGTRAN

Режим доступен только для сигнализации SIGTRAN. Для перехода в данный режим необходимо в режиме конфигурирования выполнить команду `ua`.

```
SMG-[CONFIG]> ua
Entering UA mode
SMG-[CONFIG]-[UA]>
```

Команда	Параметр	Значение	Действие
`?`			Показать перечень доступных команд
`as`	**`<as_index>`**	0-15	Перейти в режим конфигурирования сервера приложений as

Команда	Параметр	Значение	Действие
`asp`	`<asp_index>`	0-15	Перейти в режим конфигурирования процесса сервера приложений asp
`config`			Возврат в меню Configuration
`do`	`<command>`	..	Выполнить команду верхнего уровня
`exit`			Переход из данного подменю конфигурирования на уровень выше
`history`			Просмотр истории введенных команд
`link`	`<link_index>`	0-15	Перейти в режим конфигурирования линка
`new as`	`<index>`	0-15	Создать новый объект as для sgp
`new asp`	`<index>`	0-15	Создать новый объект asp для as
`new sgp`			Создать новый объект sgp
`quit`			Завершить данную сессию CLI
`remove as`	`<index>`	0-15	Удалить объект as
`remove asp`	`<index>`	0-15	Удалить объект asp
`remove sgp`	`<index>`	0-15	Удалить объект sgp
`sgp`	`<as_index>`	0-15	Перейти в режим конфигурирования процесса сигнального шлюза sgp
`show list`	`<type>`	as|asp|sgp	Показать список объектов as, asp либо sgp
`top`			Возврат на верхний уровень меню

5.3.4.2 Режим конфигурирования параметров сервера приложений AS

Режим доступен только для сигнализации SIGTRAN. Для перехода в данный режим необходимо в режиме конфигурирования SIGTRAN выполнить команду `as <index>`.

```
SMG-[CONFIG]-[UA]> as 0
SMG-[CONFIG]-[UA]-AS[0]>
```

Команда	Параметр	Значение	Действие
`?`			Показать перечень доступных команд
`do`	`<command>`	..	Выполнить команду верхнего уровня
`exit`			Переход из данного подменю конфигурирования на уровень выше
`history`			Просмотр истории введенных команд

quit			Завершить данную сессию CLI
set sgp	**<value>**	0-15	Привязать к серверу приложений процесс сигнального шлюза
set name	**<name>**	строка	Настроить имя для сервера приложений
show asps			Показать список процессов данного сервера приложений
show config			Показать настройки сервера приложений
top			Возврат на верхний уровень меню

5.3.4.3 Режим конфигурирования параметров процессов сервера приложений ASP

Режим доступен только для сигнализации SIGTRAN. Для перехода в данный режим необходимо в режиме конфигурирования SIGTRAN выполнить команду **asp <index>**.

```
SMG-[CONFIG]-[UA]> asp 0
SMG-[CONFIG]-[UA]-ASP[0]>
```

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
do	**<command>**	..	Выполнить команду верхнего уровня
exit			Переход из данного подменю конфигурирования на уровень выше
history			Просмотр истории введенных команд
set name	**<name>**	строка	Настроить имя для процесса сервера приложений
quit			Завершить данную сессию CLI
set as	**<value>**	0-15	Привязать к процессу сервер приложений
set address	**<IP>** **<port>**	IP-адрес в формате AAA.BBB.CCC.DDD 0-65535	Настроить aspid в формате ip:port
set id	**<value>**	число	Настроить aspid в численном формате
set client local iface	**<iface_name>**	сетевой интерфейс	Настроить локальный сетевой интерфейс при работе процесса в режиме клиента
set client local port	**<value>**	0-65535	Настроить локальный транспортный порт при работе процесса в режиме клиента
set client remote address	**<IP>**	IP-адрес в формате AAA.BBB.CCC.DDD	Настроить удаленный адрес при работе процесса в режиме клиента

Команда	Параметр	Значение	Действие
`set client remote port`	`<value>`	0-65535	Настроить удаленный транспортный порт при работе процесса в режиме клиента
`show ases`			Показать список серверов приложений
`show config`			Показать настройки процесса сервера приложений
`show net-interfaces`			Показать список сетевых интерфейсов
`top`			Возврат на верхний уровень меню

5.3.4.4 Режим конфигурирования параметров процессов сигнального шлюза

Режим доступен только для сигнализации SIGTRAN. Для перехода в данный режим необходимо в режиме конфигурирования SIGTRAN выполнить команду **`sgp <index>`**.

```
SMG-[CONFIG]-[UA]> sgp 0
SMG-[CONFIG]-[UA]-SGP[0]>
```

Команда	Параметр	Значение	Действие
`?`			Показать перечень доступных команд
`do`	**`<command>`**	..	Выполнить команду верхнего уровня
`exit`			Переход из данного подменю конфигурирования на уровень выше
`history`			Просмотр истории введенных команд
`name`	**`<name>`**	строка	Настроить имя для процесса сигнального шлюза
`quit`			Завершить данную сессию CLI
`set adaptation`	**`<value>`**	none|nortell	Настроить режим адаптации протокола
`set keep-alive`	**`<value>`**	0-3600000	Настроить период опроса по протоколу SCTP
`set net-interface add`	**`<iface_name>`**	сетевой интерфейс	Добавить сетевой интерфейс для работы через него процесса сигнального шлюза
`set net-interface remove`	**`<iface_name>`**	сетевой интерфейс	Удалить сетевой интерфейс из списка интерфейсов процесса сигнального шлюза
`set port`	**`<value>`**	0-65535	Настроить локальный транспортный порт для приема сигнализации
`set sctp mode`	**`<value>`**	server|client	Настроить режим работы протокола SCTP
`set strict stream zero`	**`<value>`**	on/off	Настроить режим строгого использования SCTP потока 0
`set type`	**`<value>`**	m2ua|iua	Выбрать сигнальный протокол
`show ases`			Показать список серверов приложений
`show config`			Показать настройки процесса сигнального шлюза
`show net-interfaces`			Показать список сетевых интерфейсов
`top`			Возврат на верхний уровень меню

5.3.4.5 Режим конфигурирования параметров плана нумерации

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

```
SMG-[CONFIG]> numplan
Entering Numbering-plan mode.
SMG-[CONFIG]-[NUMPLAN]>
```

Команда	Параметр	Значение	Действие
`?`			Показать перечень доступных команд
`config`			Возврат в меню Configuration
`create prefix`			Создать префикс
`delete prefix`	`<IDX Prefix>`		Удалить заданный префикс
`do`	`<command>`	..	Выполнить команду верхнего уровня
`exit`			Переход из данного подменю конфигурирования на уровень выше
`history`			Просмотр истории введенных команд
`prefix id`			Переход в режим конфигурирования префиксов по идентификатору
`prefix index`			Переход в режим конфигурирования префиксов по индексу
`quit`			Завершить данную сессию CLI
`set default prefixes`			Задать значения префиксов по умолчанию
`show prefixes`	`<YES_NO>`	yes/no	Показать настройки префиксов
`top`			Возврат на верхний уровень меню

5.3.4.5.1 Режим конфигурирования префикса

Для перехода в данный режим необходимо в режиме конфигурирования планов нумерации выполнить команду **`prefix index <INDEX>`** или `prefix id <ID>`.

```
SMG-[CONFIG]-[NUMPLAN]> prefix index 0
Entering Prefix-mode.
SMG-[CONFIG]-[NUMPLAN]-PREFIX-INDEX[0]>
```

Команда	Параметр	Значение	Действие
`?`			Показать перечень доступных команд

`config`			Возврат в меню Configuration
`direction`	`<PFX_DIRECTION>`	toll/international	Установить признак номера: toll – междугородняя связь (абонент России); international – международная связь (абонент другой страны)
`do`	`<command>`	..	Выполнить команду верхнего уровня
`exit`			Переход из данного подменю конфигурирования на уровень выше
`history`			Просмотр истории введенных команд
`mask edit`			Перейти в режим редактирования масок префикса
`mask show`			Показать маски префикса
`name`	`<s_name>`	строка не более 31 символа (разрешено использовать буквы, цифры и '_')	Задать имя/обозначение для префикса
`quit`			Завершить данную сессию CLI
`show`			Показать настройки префикса
`top`			Возврат на верхний уровень меню
`type sorm`			Определяет тип префикса "Определение параметров СОРМ"

5.3.4.5.2 Режим редактирования масок префикса

Для перехода в данный режим необходимо в режиме конфигурирования префиксов выполнить команду `mask edit`.

```
SMG-[CONFIG]-[NUMPLAN]-PREFIX-INDEX[0]> mask edit
Entering Prefix-Mask mode.
SMG-[CONFIG]-[NUMPLAN]-PREFIX-INDEX[0]-MASK>
```

Команда	Параметр	Значение	Действие
`?`			Показать перечень доступных команд
`add`	`<PREFIX_MASK>` `[called]`	маска-префикс. Максимум 255 символов, необходимо заключать в круглые скобки «(» и «)»	Добавить новую маску в префикс. Тип маски всегда – called
`config`			Возврат в меню Configuration
`do`	`<command>`	..	Выполнить команду верхнего уровня

exit			Переход из данного подменю конфигурирования на уровень выше
history			Просмотр истории введенных команд
modify mask index	**<PREFIX_MASK_INDEX>** **<PREFIX_MASK>**	0-65535 маска-префикс. Максимум 255 символов, необходимо заключать в круглые скобки «(» и «)»	Корректировать маску по индексу PREFIX_MASK_INDEX − индекс маски; PREFIX_MASK − маска
modify mask id	**<PREFIX_MASK_ID>** **<PREFIX_MASK>**	0-65535 маска-префикс. Максимум 255 символов, необходимо заключать в круглые скобки «(» и «)»	Корректировать маску по идентификатору PREFIX_MASK_ID − идентификатор маски; PREFIX_MASK − маска
modify prefix index	**<PREFIX_MASK_INDEX>** **<PFX_INDEX>**	0-65535 0-255	Перенести маску в другой префикс PREFIX_MASK_INDEX − индекс маски, которая переносится; PFX_INDEX − префикс, в который переносится маска
modify prefix id	**<PREFIX_MASK_ID>** **<PFX_INDEX>**	0-65535 0-255	Перенести маску в другой префикс PREFIX_MASK_ID − идентификатор маски, которая переносится; PFX_INDEX − префикс, в который переносится маска
name	**<s_name>**	строка не более 31 символа (разрешено использовать буквы, цифры и '_')	Задать имя/обозначение для префикса
quit			Завершить данную сессию CLI
remove id	**<PREFIX_MASK_ID>**	0-65535	Удалить маску по идентификатору
remove index	**<PREFIX_MASK_INDEX>**	0-65535	Удалить маску по индексу
show			Показать настройки маски
top			Возврат на верхний уровень меню

5.3.4.6 Режим конфигурирования параметров потока E1

Для перехода в данный режим необходимо в режиме конфигурирования выполнить команду **e1 <index>**.

```
SMG-[CONFIG]> e1 0
Entering E1-stream mode.
SMG-[CONFIG]-E1[0]>
```

Команда	Параметр	Значение	Действие

`?`			Показать перечень доступных команд
`alarm`	`<ON_OFF>`	on/off	Включить/выключить индикацию аварий данного потока E1
`config`			Возврат в меню Configuration
`crc4`	`<ON_OFF>`	on/off	Включить/выключить контроль CRC4 данного потока E1
`disabled`			Выключить поток из работы
`do`	`<command>`	..	Выполнить команду верхнего уровня
`enabled`			Включить поток в работу
`equalizer`	`<ON_OFF>`	on/off	Включить/выключить усиление сигнала потока E1
`exit`			Переход из данного подменю конфигурирования на уровень выше
`history`			Просмотр истории введенных команд
`iua`			Перейти в режим настройки параметров протокола IUA для текущего потока E1
`linecode AMI`			Установить на данном потоке тип линейного кодирования AMI
`linecode HDB3`			Установить на данном потоке тип линейного кодирования HDB3
`m2ua`			Перейти в режим настройки параметров протокола M2UA для текущего потока E1
`name`		буква, цифра, или символ '_', '.', '-'. Максимально 63 символа	Наименование потока E1
`quit`			Завершить данную сессию CLI
`remalarm`	`<ON_OFF>`	on/off	Включить/выключить индикацию при удаленной аварии на данном потоке
`show`			Показать конфигурацию данного потока
`signaling`	`<Signaling type>`		Задать тип сигнализации для потока. Возможные типы сигнализации: M2UA, IUA_USR, IUA_NET, MEDIA, SORM, NONE
`slipIND`	`<ON_OFF>`	on/off	Выводить индикацию об аварии в случае возникновения проскальзывания в приемном тракте
`slipTO`	`<TIMEOUT>`	5sec/10sec/20sec/ 30sec/45sec/1min/ 2min/3min/ 5min/ 10min/15min/30min/ 1hour/2hour/6hour	Установить периодичность опроса параметров потока у платы, если на данном потоке обнаружилось проскальзывание, то в течение данного таймаута станция будет сигнализировать об аварии
`sorm`			Переход в режим конфигурирования SORM для текущего потока E1
`top`			Возврат на верхний уровень меню

5.3.4.6.1 Режим конфигурирования параметров сигнализации СОРМ

Для перехода в данный режим необходимо в режиме конфигурирования потока E1 выполнить команду `sorm`.

```
SMG-[CONFIG]-E1[8]> sorm
E1[8]. Signaling is SORM
SMG-[CONFIG]-E1[8]-SORM>
```

Команда	Параметр	Значение	Действие
`?`			Показать перечень доступных команд
`activity`	`<ON_OFF>`	on/off	Включить/выключить контроль активности обмена сообщениями на уровне L1
`chan1(2) mode`	`<SORM_MODE>`	DCE/DTE	Установить режим для КПД1 (КПД2). Допустимые режимы: DCE, DTE
`chan1(2) send L3 Reset`	`<ON_OFF>`	on/off	Разрешить/запретить посылать каналу КПД1 (КПД2) команду перезапуска L3
`chan1(2) send L3 Restart`	`<ON_OFF>`	on/off	Разрешить/запретить посылать каналу КПД1 (КПД2) команду сброса установок L3
`chan1(2) send SABME`	`<ON_OFF>`	on/off	Установить/отключить сбалансированный асинхронный расширенный режим (SABME) на канале КПД1 (КПД2)
`cmd`	`<CMD_ADDR>`	1/3	Задать адрес командного фрейма
`config`			Возврат в меню Configuration
`control by redirecting`	`<YES_NO>`	yes/no	Разрешить контроль по переадресующему номеру (Redirecting number)
`do`	`<command>`	..	Выполнить команду верхнего уровня
`exit`			Переход из данного подменю конфигурирования на уровень выше
`history`			Просмотр истории введенных команд
`mode`		tcp/x25	Выбор режима работы сигнальных каналов КПД
`protocol specification`	`<SPECIFICATION>`	order_70/ KZ_specification/ order_268	Выбор спецификации СОРМ
`quit`			Завершить данную сессию CLI
`resp`	`<RESP_ADDR>`	1/3	Задать адрес ответного фрейма
`show`			Показать конфигурацию протокола СОРМ
`skip incomplete`	`<YES_NO>`	yes/no	Не выдавать сообщение 1.1 при неполном наборе

station type tranzit			Установить тип узла связи "Транзитный" (значение по умолчанию, изменить нельзя)
tcp interface	**<IFACE_NAME>**	строка	Выбор сетевого интерфейса для организации TCP-соединения
tcp port1		10000-65535	Выбор виртуального tcp-порта для организации КПД-1
tcp port2		10000-65535	Выбор виртуального tcp-порта для организации КПД-2
timer 10min	**<ON_OFF>**	on/off	Включить/выключить таймаут ожидания приема команд от ПУ СОРМ
top			Возврат на верхний уровень меню
vendor specific error codes	**<YES_NO>**	yes/no	Включить/выключить выдачу расширенных кодов ошибок

5.3.4.6.2 Режим конфигурирования параметров сигнализации M2UA

Для перехода в данный режим необходимо в режиме конфигурирования потока E1 выполнить команду **m2ua**.

```
SMG-[CONFIG]-E1[0]> m2ua
E1[0]. Signaling is M2UA.
SMG-[CONFIG]-E1[0]-M2UA>
```

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
cic fill	**<CIC>** **<step>**	CIC: 0-4095, step: 0-255	Заполнить коды идентификации каналов CIC: CIC – начальное значение CIC; step – шаг нумерации
cic set	**<timeslot>** **<CIC>**	timeslot: 1-31, CIC: 0-4095	Установить значение кода идентификации канала CIC для канала потока E1: timeslot: канал потока E1; CIC – код идентификации канала
config			Возврат в меню Configuration
do	**<command>**	..	Выполнить команду верхнего уровня
linkset	**<value>**	0-15, none	Назначить линксет на поток
set as	**<value>**	0-15	Привязать к сигнальному линку сервер приложений
set Dchan	**<value>**	1-31, none	Назначить канал для сигнального линка
set IID integer	**<id>**	число	Настроить идентификатор интерфейса

set IID text	**<id>**	строка	Настроить идентификатор интерфейса
exit			Переход из данного подменю конфигурирования на уровень выше
history			Просмотр истории введенных команд
tid fill	**<prefix> <TID> <postfix>**	строка, число, строка	Заполнить идентификаторы физических терминаций для каналов потока E1
tid set	**<timeslot>** **<TID>**	timeslot: 1-31, TID: строка 64 символа	Установить значение идентификатора физической терминации для канала потока E1: timeslot: канал потока E1; TID – идентификатор физической терминации
quit			Завершить данную сессию CLI
show			Показать настройки M2UA
top			Возврат на верхний уровень меню

5.3.4.6.3 Режим конфигурирования параметров сигнализации IUA

Для перехода в данный режим необходимо в режиме конфигурирования потока E1 выполнить команду **iua**.

```
SMG-[CONFIG]-E1[5]> iua
E1[5]. Signaling is IUA.
SMG-[CONFIG]-E1[5]-IUA>
```

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
config			Возврат в меню Configuration
do	**<command>**	..	Выполнить команду верхнего уровня
set as	**<value>**	0-15	Привязать к сигнальному линку сервер приложений
set IID integer	**<id>**	число	Настроить идентификатор интерфейса
set IID text	**<id>**	строка	Настроить идентификатор интерфейса
exit			Переход из данного подменю конфигурирования на уровень выше
history			Просмотр истории введенных команд

tid fill	**<prefix> <TID> <postfix>**	строка, число, строка	Заполнить идентификаторы физических терминаций для каналов потока E1
tid set	**<timeslot>** **<TID>**	timeslot: 1-31, TID: строка 64 символа	Установить значение идентификатора физической терминации для канала потока E1: timeslot: канал потока E1; TID – идентификатор физической терминации
quit			Завершить данную сессию CLI
show			Показать настройки IUA
top			Возврат на верхний уровень меню

5.3.4.7 Режим конфигурирования параметров линксетов ОКС-7

Для перехода в данный режим необходимо в режиме конфигурирования выполнить команду **`linkset edit <index>`**.

```
SMG-[CONFIG]> linkset edit 0
Entering Linkset-mode.
SMG1016M-SIGTRAN-[CONFIG]-LINKSET[0]>
```

Команда	Параметр	Значение	Действие
`?`			Показать перечень доступных команд
`config`			Возврат в меню Configuration
`do`	`<command>`	..	Выполнить команду верхнего уровня
`exit`			Переход из данного подменю конфигурирования на уровень выше
`history`			Просмотр истории введенных команд
`name`		буква, цифра, или символ '_', '.', '-'. Максимально 63 символа	Наименование линксета
`point code`	**`<value 1>`** **`<value 2>`**	0-16383 0-16383	Настройка PC (point code) взаимодействующих точек сигнализации
`quit`			Завершить данную сессию CLI
`show`			Показать конфигурацию данного потока
`top`			Возврат на верхний уровень меню

5.3.5 Режим конфигурирования таблицы модификаторов

Для перехода в данный режим необходимо в режиме конфигурирования выполнить команду **`modifiers table <MODTBL_INDEX>`**, где `<MODTBL_INDEX>` – номер таблицы.

```
SMG-[CONFIG]-TRUNK[0]> modifiers table
Entring TRUNK-Modifiers mode.
SMG-[CONFIG]-TRUNK[0]-MODIFIER>
```

Команда	Параметр	Значение	Действие
`?`			Показать перечень доступных команд
`add`			Добавить модификатор:
	`<MODIFIER_MASK>`	маска-модификатор, максимум 255 символов, необходимо заключать в круглые скобки «(» и «)»	MODIFIER_MASK – маска модификатора
	`[CLD_RULE]`	правило-модификатор, максимум 30 символов, необходимо заключать в кавычки	CLD_RULE – правило преобразования номера вызываемого
`change called rule`			Редактировать правило преобразования номера вызываемого для модификатора
	`<MODIFIER_INDEX>`	0-8191	MODIFIER_INDEX – номер модификатора
	`<CLD_RULE>`	правило-модификатор, максимум 30 символов, необходимо заключать в кавычки	CLD_RULE – правило преобразования номера вызываемого
`change mask`			Редактировать маску модификатора
	`<MODIFIER_INDEX>`	0-8191	MODIFIER_INDEX – номер модификатора
	`<MODIFIER_MASK>`	маска-модификатор, максимум 255 символов, необходимо заключать в круглые скобки «(» и «)»	MODIFIER_MASK – маска модификатора

Команда	Параметр	Значение	Действие
`change modtable`			Перенести модификатор в таблицу с указанным номером
	`<MODIFIER_INDEX>`	0-8191	MODIFIER_INDEX – номер модификатора
	`<NEW_MODTBL_INDEX>`	0-255	
`change name`			Редактировать имя модификатора
	`<MODIFIER_INDEX>`	0-8191	MODIFIER_INDEX – номер модификатора
	`<MODIFIER_NAME>`	разрешено использовать буквы, цифры, символы '-', '.', '_', максимум 31 символ	MODIFIER_NAME – имя модификатора
`remove`	`<MODIFIER_INDEX>`	0-8191	Удалить указанный модификатор
`show`	`<MODIFIER_INDEX>`	0-8191	Показать конфигурацию модификатора
`set Ltimer`	`<L_TIMER>`	0-255	Задать L-таймер
`set Stimer`	`<S_TIMER>`	0-255	Задать S-таймер
`set name`	`<MODIFIER_NAME>`	разрешено использовать буквы, цифры, символы '-', '.', '_', максимум 31 символ	Установить имя модификатора
`quit`			Завершить данную сессию CLI
`config`			Возврат в меню Configuration
`do`	`<command>`	..	Выполнить команду верхнего уровня
`exit`			Выход из данного подменю конфигурирования на уровень выше
`top`			Возврат на верхний уровень меню
`history`			Просмотр истории введенных команд

5.3.6 Режим конфигурирования параметров firewall

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

```
SMG-[CONFIG]> firewall
Entering firewall mode
SMG-[CONFIG]-[firewall]>
```

Команда	Параметр	Значение	Действие
`?`			Показать перечень доступных команд
`add profile`	**`<PROF_NAME>`**	разрешено использовать буквы, цифры, символ '_', максимум 63 символа	Добавить профиль firewall

Команда	Параметр	Значение	Действие
`add rule`	`<direction>`	forward input output	Добавить правило firewall Направление работы правила
	`<ENABLE>`	enable/disable	Включение/отключение правила
	`<RULE_NAME>`	Текст, максимум 63 символа	Имя правила
	`<S_IP>`	AAA.BBB.CCC.DDD	IP-адрес источника
	`<S_MASK>`	AAA.BBB.CCC.DDD	Маска подсети источника
	`<R_IP>`	AAA.BBB.CCC.DDD	IP-адрес получателя
	`<R_MASK>`	AAA.BBB.CCC.DDD	Маска подсети получателя
	`<PROTO>`	any tcp udp icmp tcp+udp	Тип протокола
	`<S_PORT_START>`	1-65535	Начальный порт источника
	`<S_PORT_END>`	1-65535	Конечный порт источника
	`<D_PORT_START>`	1-65535	Начальный порт получателя
	`<D_PORT_END>`	1-65535	Конечный порт получателя
	`<ICMP_TYPE>`	none any echo-reply destination-unreachable network-unreachable host-unreachable protocol-unreachable port-unreachable fragmentation-needed source-route-failed network-unknown host-unknown network-prohibited host-prohibited TOS-network-unreachable TOS-host-unreachable communication-prohibited host-precedence-violation	Тип пакета ICMP

Команда	Параметр	Значение	Действие
	<ACTION>	precedence-cutoff source-quench redirect network-redirect host-redirect TOS-network-redirect TOS-host-redirect echo-request router-advertisement router-solicitation time-exceeded ttl-zero-during-transit ttl-zero-during-reassembly parameter-problem ip-header-bad required-option-missing timestamp-request timestamp-reply address-mask-request address-mask-reply accept, drop, reject	Действие – действие выполняемое данным правилом: ACCEPT – пакеты, попадающие под данное правило, будут пропущены сетевым экраном firewall; DROP – пакеты, попадающие под данное правило, будут отброшены сетевым экраном firewall без какого-либо информирования стороны, передавшей пакет; REJECT – пакеты, попадающие под данное правило, будут отброшены сетевым экраном firewall, стороне, передавшей пакет, будет отправлен либо пакет TCP RST, либо ICMP destination unreachable
	<P_IDX>	1-65535	Номер профиля firewall
apply			Применить настройки firewall
config			Возврат в меню Configuration
do	**<command>**	..	Выполнить команду верхнего уровня
del profile	**<ID>**	1-65535	Удалить профиль firewall
del rule	**<ID>**	1-65535	Удалить правило firewall
exit			Выход из данного подменю конфигурирования на уровень выше
modify profile	**<ID>** **<NAME>**	1-65535 разрешено использовать буквы, цифры, символ '_'. Максимум 63 символ	Индекс профиля firewall Ввод нового имени устройства

Команда	Параметр	Значение	Действие
modify rule	**<Type>** <ID> **<param>**	action dport_end dport_start enable icmp-type name prof_id proto r_ip r_mask s_ip s_mask sport_end sport_start traffic-type 1-65535 Новое значение согласно данного типа параметра	Изменить указанное правило firewall (один из параметров)
movedown	**<ID>**	1-65535	Переместить правило вниз на одну позицию
move up	**<ID>**	1-65535	Переместить правило вверх на одну позицию
quit			Завершить данную сессию CLI
set eth	**<PROFILE ID>**	0-65535	Назначить правило на сетевой интерфейс PROFILE ID = 0 означает, что профиль не используется
set pptp	**<PPP_IDX>** **<PROFILE ID>**	0-5 0-65535	Назначить правило на интерфейс PROFILE ID = 0 означает, что профиль не используется
set vlan	**<VLAN_IDX>** **<PROFILE ID>**	VLAN1…VLAN8 0-65535	Назначить правило на VLAN PROFILE ID = 0 означает, что профиль не используется
show config			Показать конфигурацию
show interfaces			Показать параметры интерфейсов
show system			Показать системные параметры
top			Возврат на верхний уровень меню

5.3.7 Режим конфигурирования сетевых параметров

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

```
SMG-[CONFIG]> network
Entering Network mode.
SMG-[CONFIG]-NETWORK>
```

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд

Команда	Параметр	Значение	Действие
`add interface pptpVPNclient`			Добавить новый VPN/PPTP-клиент
	`<LABEL>`	разрешено использовать буквы, цифры, символы '_', '.', '-', ':', максимум 255 символов	LABEL – имя интерфейса
	`<IPADDR>`	IP-адрес в формате AAA.BBB.CCC.DDD разрешено использовать буквы, цифры, символы '_', '.', '-', максимум 63 символа	IPADDR – IP-адрес PPTP-сервера
	`<USER>`	разрешено использовать буквы, цифры, символы '_', '.', '-', максимум 63 символа	USER – имя пользователя
	`<PASS>`		PASS – пароль
`add interface tagged`			Добавить новый сетевой интерфейс
	`dynamic/static`		
	`<LABEL>`	разрешено использовать буквы, цифры, символы '_', '.', '-', ':', максимум 255 символов	LABEL – имя интерфейса
	`<VID>`	1-4095	VID – VLAN ID
	`<IPADDR>`	IP-адрес в формате AAA.BBB.CCC.DDD	IPADDR – IP-адрес PPTP-сервера
	`<NETMASK>`	сетевая маска в формате AAA.BBB.CCC.DDD	NETMASK – сетевая маска
`add interface untagged`			Добавить новый сетевой интерфейс
	`dynamic/static`		
	`<LABEL>`	разрешено использовать буквы, цифры, символы '_', '.', '-', ':', максимум 255 символов	LABEL – имя интерфейса
	`<IPADDR>`	IP-адрес в формате AAA.BBB.CCC.DDD	IPADDR – IP-адрес PPTP-сервера
	`<NETMASK>`	сетевая маска в формате AAA.BBB.CCC.DDD	NETMASK – сетевая маска
`config`			Возврат в меню Configuration
`confirm`			Подтвердить измененные сетевые настройки и настройки VLAN без перезагрузки шлюза. Если в течение минуты примененные сетевые настройки не подтверждены, то их значения вернутся к первоначальным
`dhcp server`			Переход в режим конфигурирования параметров DHCP-сервера
`exit`			Выход из данного подменю конфигурирования на уровень выше
`history`			Просмотр истории введенных команд

Команда	Параметр	Значение	Действие
`ntp`			Переход в режим конфигурирования NTP
`quit`			Завершить данную сессию CLI
`remove interface`	`<NET_IFACE_IDX>`	0-39	Удалить указанный интерфейс
`rollback`			Отменить изменения
`set interface broadcast`			Задать адрес для широковещательных пакетов для указанного интерфейса
	`<NET_IFACE_IDX>`	0-39	
	`<BROADCAST>`	IP-адрес в формате AAA.BBB.CCC.DDD	
`set interface COS`			Назначить приоритет 802.1p для указанного интерфейса
	`<NET_IFACE_IDX>`	0-39	
	`<COS>`	0-7	
`set interface dhcp`			Получать сетевые настройки динамически от DHCP-сервера для указанного интерфейса
	`<NET_IFACE_IDX>`	0-39	
	`<ON_OFF>`	on/off	
`set interface dhcp_dns`			Получать IP-адрес DNS-сервера динамически от DHCP-сервера для указанного интерфейса
	`<NET_IFACE_IDX>`	0-39	
	`<ON_OFF>`	on/off	
`set interface dhcp_no_gw`			Не получать настройки шлюза динамически от DHCP-сервера для указанного интерфейса
	`<NET_IFACE_IDX>`	0-39	
	`<ON_OFF>`	on/off	
`set interface gateway`			Задать шлюз по умолчанию для интерфейса
	`<NET_IFACE_IDX>`	0-39	
	`<IPADDR>`	IP-адрес в формате AAA.BBB.CCC.DDD	
`set interface dhcp_ntp`			Получать настройки NTP динамически от DHCP-сервера для указанного интерфейса

Команда	Параметр	Значение	Действие
	<NET_IFACE_IDX>	0-39	
	<ON_OFF>	on/off	
set interface gw_ignore			Игнорировать настройку шлюза для указанного интерфейса
	<NET_IFACE_IDX>	0-39	
	<ON_OFF>	on/off	
set interface h323			Разрешить обмен сигнализацией H.323 для указанного интерфейса
	<NET_IFACE_IDX>	0-39	
	<ON_OFF>	on/off	
set interface ipaddr			Задать IP-адрес и сетевую маску для указанного интерфейса
	<NET_IFACE_IDX>	0-39	
	<IPADDR>	IP-адрес в формате AAA.BBB.CCC.DDD	
	<NETMASK>	сетевая маска в формате AAA.BBB.CCC.DDD	
set interface network-label			Задать имя для данного интерфейса
	<NET_IFACE_IDX>	0-39	
	<LABEL>	цифры, символы '_', '.', '-', ':', максимум 255 символов	
set interface radius			Разрешить передачу сообщений RADIUS через интерфейс
	<NET_IFACE_IDX>	0-39	
	<ON_OFF>	on/off	
set interface rtp			Разрешить передачу RTP-пакетов через интерфейс
	<NET_IFACE_IDX>	0-39	
	<ON_OFF>	on/off	
set interface run_at_startup			Автоматически запускать интерфейс при старте (только для VPN-интерфейса)
	<NET_IFACE_IDX>	0-39	
	<STARTUP>	on/off	

Команда	Параметр	Значение	Действие
`set interface serverip`			Задать IP-адрес PPTP-сервера
	`<NET_IFACE_IDX>`	0-39	
	`<IPADDR>`	IP-адрес в формате AAA.BBB.CCC.DDD	
`set interface signaling`			Разрешить передачу сообщений SIP через интерфейс
	`<NET_IFACE_IDX>`	0-39	
	`<ON_OFF>`	on/off	
`set interface snmp`	`<NET_IFACE_IDX>`	0-39	Разрешить передачу пакетов SNMP через интерфейс
	`<ON_OFF>`	on/off	
`set interface ssh`			Разрешить ssh-сессию через интерфейс
	`<NET_IFACE_IDX>`	0-39	
	`<ON_OFF>`	on/off	
`set interface telnet`			Разрешить telnet-сессию через интерфейс
	`<NET_IFACE_IDX>`	0-39	
	`<ON_OFF>`	on/off	
`set interface use_mppe`			Включить/отключить шифрование (только для VPN-интерфейса)
	`<NET_IFACE_IDX>`	0-39	
	`<ON_OFF>`	on/off	
`set interface user_name`			Задать имя пользователя (только для VPN-интерфейса)
	`<NET_IFACE_IDX>`	0-39	
	`<USER>`	разрешено использовать буквы, цифры, символы '_', '.', '-', максимум 63 символа	
`set interface user_pass`			Задать пароль (только для VPN-интерфейса)
	`<NET_IFACE_IDX>`	0-39	
	`<PASS>`	разрешено использовать буквы, цифры, символы '_', '.', '-', максимум 63 символа	
`set interface VID`			Назначить VID для интерфейса
	`<NET_IFACE_IDX>`	0-39	

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

После изменения IP-адреса, маски сети либо при отключении управления через web-конфигуратор на сетевом интерфейсе необходимо подтвердить данные настройки командой **confirm**, иначе по истечении двухминутного таймера произойдет откат конфигурации на предыдущую.

5.3.7.1 Режим конфигурирования параметров DHCP-сервера

Для перехода в данный режим необходимо в режиме конфигурирования сетевых параметров выполнить команду **`dhcp server`**.

```
SMG-[CONFIG]-NETWORK> dhcp server
Entering Network mode.
SMG-[CONFIG]-[NETWORK]-[DHCPD]>
```

Команда	Параметр	Значение	Действие
`?`			Показать перечень доступных команд
`conflicttime`	`<CONFLICT>`	10-10000000	Установить период времени, на который IP-адрес будет зарезервирован в случае обнаружения конфликта MAC-адресов, не менее 10 секунд
`declinetime`	`<DECLINE>`	10-10000000	Период времени, на который IP-адрес будет зарезервирован в случае получения сообщения отказа (DHCP decline), не менее 10 секунд
`dhcpd start`			Запустить DHCP-сервер
`dhcpd stop`			Остановить DHCP-сервер
`dns 0/1/2/3`	`<DNS>`	IP-адрес в формате AAA.BBB.CCC.DDD	Установить адреса DNS-серверов из сети оператора
`domain`	`<DOMAIN>`	строка длиной не более 31 символа	Установить имя домена, используемое по умолчанию для DHCP-клиентов
`enabled`	`<ENABLE>`	no/yes	Запускать/не запускать DHCP-сервер при старте шлюза
`exit`			Выход из данного подменю конфигурирования на уровень выше
`gateway`	`<GW>`	IP-адрес в формате AAA.BBB.CCC.DDD	Установить адрес маршрутизатора или шлюза по умолчанию, назначаемый клиентам DHCP-сервера
`interface`	`<IFACE_NAME>`	строка до 255 символов	Выбор сетевого интерфейса для DHCP-сервера
`ipaddr end`	`<IPADDR>`	IP-адрес в формате AAA.BBB.CCC.DDD	Установить конечный адрес диапазона назначаемых IP-адресов
`ipaddr start`	`<IPADDR>`	IP-адрес в формате AAA.BBB.CCC.DDD	Установить начальный адрес диапазона назначаемых IP-адресов
`max_lease`	`<MAX_LEASE>`	10-10000000 sec	Установить максимальное время использования устройством IP-адреса, назначенного сервером DHCP, не менее 10 секунд
`maxleases`	`<MAXLEASES>`	1-65535	Установить ограничения количества арендуемых адресов

Команда	Параметр	Значение	Действие
`min_lease`	`<MIN_LEASE>`	10-10000000 sec	Установить минимальное время использования устройством IP-адреса, назначенного сервером DHCP, не менее 10 секунд
`netmask`	`<NETMASK>`	IP-адрес в формате AAA.BBB.CCC.DDD	Установить маску сети
`ntp announce external server address`	`<NTP_SERVER>`	IP-адрес в формате AAA.BBB.CCC.DDD	Задать адрес внешнего сервера NTP для анонсирования в опции 42
`ntp announce external server enable`	`<ANNOUNCE_EXT>`	no/yes	Разрешить анонсирование внешнего сервера NTP в опции 42
`ntp announce local`	`<ANNOUNCE_LOCAL>`	no/yes	Разрешить анонсирование локального сервера NTP в опции 42
`offertime`	`<OFFER>`	10-10000000	Установить период времени, на который запрошенный IP-адрес будет зарезервирован, не менее 10 секунд
`quit`			Завершить данную сессию CLI
`savetime`	`<SAVE>`	7200-10000000 /off	Установить период времени, через который устройство будет сохранять информацию об арендованных адресах в файл dhcpd.leases *off* – не сохранять БД
`show config`			Показать конфигурацию DHCP: статус использования, диапазон адресов, маска сети, шлюз по умолчанию, адреса доменов, Wins-сервера, количество арендуемых адресов, таймауты запросов
`static_lease add`			Назначить статические соответствия IP- и MAC-адресов:
	`<NAME>`	строка длиной не более 63 символов	NAME – имя соответствия
	`<IPADDR>`	IP-адрес в формате AAA.BBB.CCC.DDD	IPADDR – IP-адрес
	`<MAC>`	MAC-адрес в формате XX:XX:XX:XX:XX:XX	MAC – MAC-адрес
`static_lease remove`	`<INDEX>`	0-4095	Удалить указанное правило в таблице статических соответствий IP- и MAC-адресов

Команда	Параметр	Значение	Действие
`static_lease show`			Показать таблицу статических соответствий IP- и MAC-адресов
`wins`	`<WINS>`	IP-адрес в формате AAA.BBB.CCC.DDD	Установить IP-адрес основного WINS-сервера для использования DHCP-клиентом

5.3.7.2 Режим конфигурирования PPTP-клиента

```
SMG-[CONFIG]-NETWORK> pptp
Entering PPTP mode.
SMG-[CONFIG]-[NETWORK]-PPTP>
```

Команда	Параметр	Значение	Действие
`?`			Показать перечень доступных команд
`add interface`	`<USER>`	строка до 31 символа	Задать имя пользователя
	`<PASS>`	строка до 31 символа	Задать пароль
	`<IP_SRV>`	IP-адрес в формате AAA.BBB.CCC.DDD	Задать IP-адрес PPTP-сервера
	`<LABEL>`	строка до 31 символа	Задать метку
	`< MPPE>`	on/off	Включить/отключить шифрование
	`<STARTUP>`	on/off	Запускать при старте
`config`			Возврат в меню Configuration
`exit`			Выход из данного подменю конфигурирования на уровень выше
`history`			Просмотр истории введенных команд
`modify interface`			Изменить параметры PPTP
	`label`	строка до 31 символа	Изменить метку
	`mppe pssword`	on/off строка до 31 символа	Изменить включение шифрования Изменить пароль
	`server_ip`	IP-адрес в формате AAA.BBB.CCC.DDD on/off	Изменить IP-адрес сервера PPTP Изменить автоматически запуск PPTP
	`startup username`	строка до 31 символа	Изменить имя пользователя
`show`			Показать настройки PPTP

Команда	Параметр	Значение	Действие
`start interface`	`<IDX_INERFACE>`	0-16	Запустить PPTP-интерфейс в текущий момент времени
`status interface`	`<IDX_INERFACE>`	0-16	Просмотр состояния заданного интерфейса
`stop interface`	`<IDX_INERFACE>`	0-16	Остановить PPTP-интерфейс в текущий момент времени

5.3.7.3 Режим конфигурирования протокола NTP

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

```
SMG-[CONFIG]-NETWORK> ntp
Entering NTP mode.
SMG-[CONFIG]-[NETWORK]-NTP>
```

Команда	Параметр	Значение	Действие
?			Показать перечень доступных команд
apply		no/yes	Применить/отклонить настройки NTP
config			Возврат в меню Configuration
exit			Выход из данного подменю конфигурирования на уровень выше
quit			Завершить данную сессию CLI
restart ntp		no/yes	Перезапустить процесс NTP
set ntp dhcp			Получить настройки NTP по DHCP с заданного интерфейса
	NET_IFACE_IDX	индекс сетевого интерфейса	
	ON_OFF	off/on	
set ntp local server enable	ON_OFF	off/on	Активировать локальный NTP-сервер для получения времени от SMG
set ntp local server interface	NET_IFACE_IDX	индекс сетевого интерфейса	Установить сетевой интерфейс, на котором будет работать локальный сервер NTP
set ntp period	NTP_PERIOD	10-1440	Задать период синхронизации времени
set ntp server	NTP	строка 63 символа	Задать адрес NTP-сервера, с которым будет синхронизироваться SMG
set ntp usage	ON_OFF	off/on	Активация NTP-клиента
show config			Показать конфигурацию
timezone set		GMT/GMT+1/GMT-1/GMT+2/ GMT-2/GMT+3/GMT-3/ GMT+4/GMT-4/GMT+5/ GMT-5/GMT+6/GMT-6/ GMT+7/GMT-7/GMT+8/ GMT-8/GMT+9/GMT-9/ GMT+10/GMT-10/GMT+11/ GMT-11/GMT+12	Задать часовой пояс относительно всемирного координационного времени
		Asia	Выбор города местонахождения в Азии

Команда	Параметр	Значение	Действие
		Europe	Выбор города местонахождения в Европе

5.3.7.4 Режим конфигурирования протокола SNMP

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

```
SMG-[CONFIG]-NETWORK> snmp
Entering SNMP mode.
SMG-[CONFIG]-SNMP>
```

Команда	Параметр	Значение	Действие
`?`			Показать перечень доступных команд
`add`			Добавить правило передачи SNMP-трапов:
	`<TYPE>`	trapsink/ trap2sink/ informsink	TYPE – тип SNMP-сообщения
	`<IP>`	IP-адрес в формате AAA.BBB.CCC.DDD	IP – IP-адрес приемника трапов
	`<COMM>`	строка до 31 символа	COMM – пароль, содержащийся в трапах
	`<PORT>`	1-65535	PORT – UDP-порт приемника трапов
`config`			Возврат в меню Configuration
`create user`			Создать пользователя (назначить логин и пароль для доступа)
	`<LOGIN>`	строка до 31 символа	
	`<PASSWD>`	пароль от 8 до 31 символа	
`exit`			Выход из данного подменю конфигурирования на уровень выше
`history`			Просмотр истории введенных команд
`modify community`			Изменить правило передачи SNMP-трапов (пароль, содержащийся в трапах)
	`<IDX>`	0-15	
	`<COMM>`	строка до 31 символа	
`modify ip`			Изменить правило передачи SNMP-трапов (адрес приемника трапов)
	`<IDX>`	0-15	
	`<IP>`	IP-адрес в формате AAA.BBB.CCC.DD	

Команда	Параметр	Значение	Действие
`modify port`			Изменить правило передачи SNMP-трапов (порт приемника трапов)
	`<IDX>`	0-15	
	`<PORT>`	1-65535	
`modify type`			Изменить правило передачи SNMP-трапов (тип SNMP-сообщения)
	`<IDX>`	0-15	
	`<TYPE>`	trapsink/ trap2sink/ informsink	
`quit`			Завершить данную сессию CLI
`remove`	`<IDX>`	0-15	Удалить правило передачи SNMP-трапов
`restart snmpd`	`Yes/no`		Перезапустить SNMP-клиента
`ro`	`<RO>`	строка длиной до 63 символов	Установить пароль на чтение параметров
`rw`	`<RW>`	строка длиной до 63 символов	Установить пароль на чтение и запись параметров
`show`			Показать конфигурацию SNMP
`syscontact`	`<SYSCONTACT>`	строка длиной до 63 символов	Указать контактную информацию
`syslocation`	`<SYSLOC>`	строка длиной до 63 символов	Указать место расположения устройства
`sysname`	`<SYSNAME>`	строка длиной до 63 символов	Указать имя устройства

6 Приложения SMG (SIGTRAN)

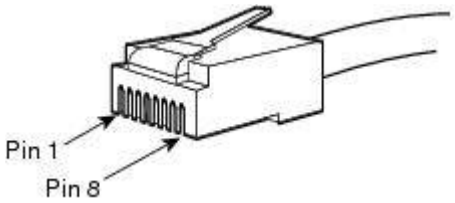
- Приложение А. Назначение контактов разъёмов кабеля
- Приложение Б. Резервное обновление встроенного ПО
- Приложение В. Взаимодействие устройства с системами мониторинга
- Приложение Г. Управление и мониторинг по протоколу SNMP
- Приложение Д. Обеспечение функций СОРМ
- Приложение Е. Рекомендации по безопасности

6.1 Приложение А. Назначение контактов разъёмов кабеля

6.1.1 Для SMG-2016, 3016

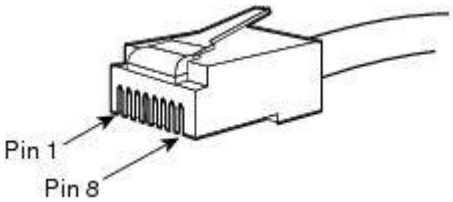
Назначение контактов разъемов **RJ-48** для подключения потоков E1 ***E1 Line 0..15*** соответствует спецификации ISO/IEC 10173 и приведено в таблице ниже.

Таблица А1 – Назначение контактов разъемов **RJ-48** для подключения потоков E1

№ контакта (Pin)	Назначение	Нумерация контактов
1	RCV from network (tip)	
2	RCV from network (ring)	
3	RCV shield	
4	XMT tip	
5	XMT ring	
6	XMT shield	
7	Не используется	
8	Не используется	

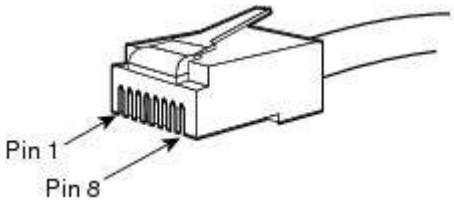
Назначение контактов разъема **RJ-45** консольного порта ***Console*** приведено в таблице ниже.

Таблица А2 – Назначение контактов разъемов **RJ-45** консольного порта

№ контакта (Pin)	Назначение	Нумерация контактов
1	Не используется	
2	Не используется	
3	TX	
4	Не используется	
5	GND	
6	RX	
7	Не используется	
8	Не используется	

Назначение контактов разъемов **RJ-45** для подключения внешнего источника синхронизации ***Sync.0/ Sync.1*** приведено в таблице ниже.

Таблица А3 – Назначение контактов разъемов **RJ-45** для подключения внешнего источника синхронизации

№ контакта (Pin)	Назначение	Нумерация контактов
1	Sync A[1]	
2	Sync B[2]	
3	Не используется	
4	Sync A	
5	Sync B	
6	Не используется	
7	Не используется	
8	Не используется	

---

[1] Контакты 1 и 4 электрически соединены между собой внутри устройства
[2] Контакты 2 и 5 электрически соединены между собой внутри устройства

6.1.2 Для SMG-1016M

E1 Line 0..7 E1

Синхр + 0	1	19	Синхр - 0
	2	20	
ПРД ”б” 7	3	21	ПРД ”а” 7
ПРМ ”б” 7	4	22	ПРМ ”а” 7
ПРД ”б” 6	5	23	ПРД ”а” 6
ПРМ ”б” 6	6	24	ПРМ ”а” 6
ПРД ”б” 5	7	25	ПРД ”а” 5
ПРМ ”б” 5	8	26	ПРМ ”а” 5
ПРД ”б” 4	9	27	ПРД ”а” 4
ПРМ ”б” 4	10	28	ПРМ ”а” 4
ПРД ”б” 3	11	29	ПРД ”а” 3
ПРМ ”б” 3	12	30	ПРМ ”а” 3
ПРД ”б” 2	13	31	ПРД ”а” 2
ПРМ ”б” 2	14	32	ПРМ ”а” 2
ПРД ”б” 1	15	33	ПРД ”а” 1
ПРМ ”б” 1	16	34	ПРМ ”а” 1
ПРД ”б” 0	17	35	ПРД ”а” 0
ПРМ ”б” 0	18	36	ПРМ ”а” 0

E1 Line 8..15

Синхр + 1	1	19	Синхр - 1
	2	20	
ПРД ”б” 15	3	21	ПРД ”а” 15
ПРМ ”б” 15	4	22	ПРМ”а” 15
ПРД ”б” 14	5	23	ПРД ”а” 14
ПРМ ”б” 14	6	24	ПРМ ”а” 14
ПРД ”б” 13	7	25	ПРД ”а” 13
ПРМ ”б” 13	8	26	ПРМ ”а” 13
ПРД ”б” 12	9	27	ПРД ”а” 12
ПРМ ”б” 12	10	28	ПРМ ”а” 12
ПРД ”б” 11	11	29	ПРД ”а” 11
ПРМ ”б” 11	12	30	ПРМ ”а” 11
ПРД ”б” 10	13	31	ПРД ”а” 10
ПРМ ”б” 10	14	32	ПРМ ”а” 10
ПРД ”б” 9	15	33	ПРД ”а” 9
ПРМ ”б” 9	16	34	ПРМ ”а” 9
ПРД ”б” 8	17	35	ПРД ”а” 8
ПРМ ”б” 8	18	36	ПРМ ”а” 8

Рисунок 31 – Назначение контактов разъемов *E1 Line*

Контакты *ПРМ* предназначены для приема сигнала из канала в устройство;

Контакты *ПРД* предназначены для передачи сигнала из устройства в канал;

Контакты *Синхр* предназначены для синхронизации устройства от внешних источников (входное сопротивление 120 Ом).

Console

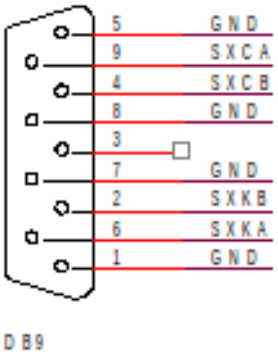


Рисунок 32 – Назначение контактов разъема *Console*

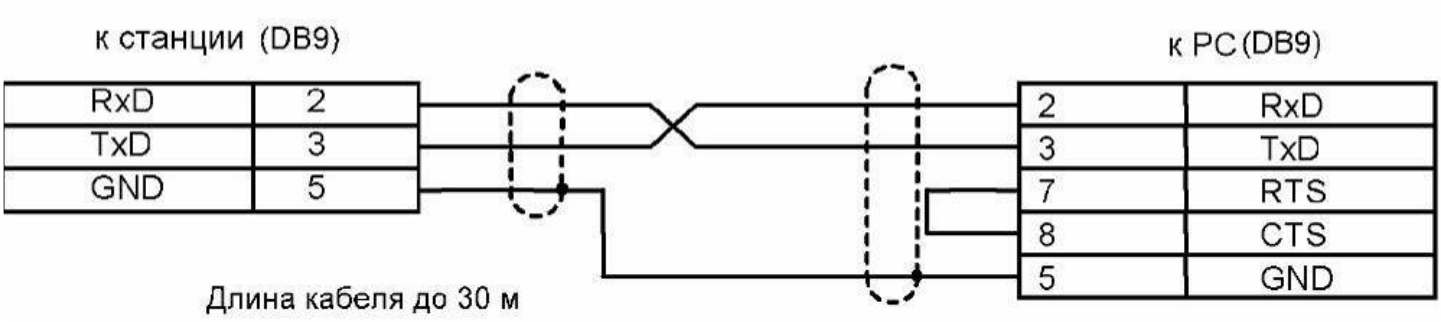


Рисунок 33 – Схема кабеля для подключения к ПОРТ1, ПОРТ2

6.1.3 Таблицы соответствия цвета провода и контакта разъема E1 Line

Таблица А4 – Соответствие цвета провода и контакта разъема E1 Line (кабель NENSHI NSPC-7019-18)

Цвет провода	**Контакт разъема**	**Цвет провода**	**Контакт разъема**
Бело-голубой	1	**Черно-голубой**	10
Голубой	19	Голубой	28
Бело-оранжевый	2	**Черно-оранжевый**	11
Оранжевый	20	Оранжевый	29
Бело-зеленый	3	**Черно-зеленый**	12
Зеленый	21	Зеленый	30
Бело-коричневый	4	**Черно-коричневый**	13
Коричневый	22	Коричневый	31
Фиолетовый	5	**Желто-голубой**	14
Серый	23	Голубой	32
Красно-голубой	6	**Желто-оранжевый**	15
Голубой	24	Оранжевый	33
Красно-оранжевый	7	**Желто-зеленый**	16
Оранжевый	25	Зеленый	34
Красно-зеленый	8	**Желто-коричневый**	17
Зеленый	26	Коричневый	35
Красно-коричневый	9	**Желто-серый**	18
Коричневый	27	Серый	36

Таблица А5 – Соответствие цвета провода и контакта разъема E1 Line (кабель HANDIAN UTP 18PR)

Цвет провода	**Контакт разъема**	**Цвет провода**	**Контакт разъема**
Бело-голубой	1	**Красно-серый**	10
Голубой	19	Серый	28
Бело-оранжевый	2	**Черно-голубой**	11
Оранжевый	20	Голубой	29

Бело-зеленый	3	**Черно-оранжевый**	12
Зеленый	21	Оранжевый	30
Бело-коричневый	4	**Черно-зеленый**	13
Коричневый	22	Зеленый	31
Фиолетово-серый	5	**Черно-коричневый**	14
Серый	23	Коричневый	32
Красно-голубой	6	**Черно-серый**	15
Голубой	24	Серый	33
Красно-оранжевый	7	**Желто-голубой**	16
Оранжевый	25	Голубой	34
Красно-зеленый	8	**Желто-оранжевый**	17
Зеленый	26	Оранжевый	35
Красно-коричневый	9	**Желто-зеленый**	18
Коричневый	27	Зеленый	36

6.2 Приложение Б. Резервное обновление встроенного ПО

6.2.1 Резервное обновление встроенного ПО устройства через RS-232

В случае, когда не удается обновить ПО через Web-конфигуратор или консоль (Telnet, SSH), 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 Com-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 *SMG_kernel, SMG_initrd* (компьютер, на котором запущен TFTP сервер 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: SMG-1016Mv2 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>:

```
set ipaddr 192.168.2.2
```

8. Ввести **`set netmask <сетевая маска устройства>`** <ENTER>:

```
set netmask 255.255.255.0
```

9. Ввести **`set serverip <IP-адрес компьютера, на котором запущен tftp сервер>`** <ENTER>:

```
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 preceeding transfer (eth0):
- Sent packet number 0
- Received packet number 0
- Handled packet number 0
ENET Speed is 1000 Mbps - FULL duplex connection (EMAC0)
Using ppc_4xx_eth0 device
TFTP from server 192.168.2.5; our IP address is 192.168.2.2
Filename ' smg/SMG_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/SMG_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`**.

6.2.2 Резервное обновление встроенного ПО устройства с USB-Flash накопителя

В случае, когда остальные способы обновления ПО недоступны, существует возможность обновления ПО при помощи USB-flash накопителя.

Для того чтобы обновить встроенное ПО устройства при помощи USB-flash, необходимо следующие:

- USB-flash накопитель;
- Программа терминалов (например, TERATERM).

Последовательность действий при обновлении устройства:

1. Скопировать файл ПО в корневую директорию USB-flash накопителя;
2. Подключить скрещенным кабелем Com-порт компьютера к Console-порту устройства, либо установить соединение с устройством по протоколу Telnet/SSH;
3. Запустить терминальную программу;
4. Настроить скорость передачи 115200, формат данных 8 бит, без паритета, 1 бит стоповый, без управления потоком (в случае соединения по RS-232);
5. Включить устройство и дождаться его загрузки;
6. После загрузки подключится в терминальном режиме по протоколу Telnet/SSH либо по RS-323;
7. В режиме CLI ввести команду: **`firmware update <file-name> usb;`**
   В случае если режим CLI недоступен, обновление возможно в режиме shell, для этого нужно ввести в режиме shell: **`/usr/local/scripts/get_firmware <file-name> usb.`** Где **`<file-name>`** – наименование файла ПО;
8. Дождаться завершения обновления ПО и перезапустить устройство.

6.3 Приложение В. Взаимодействие устройства с системами мониторинга

Для возможности отслеживания в реальном времени аварийных ситуаций, возникающих на устройстве необходимо настроить работу с системой мониторинга.

Отсутствие каких-либо аварий считается нормальной работой, при возникновении аварийного события состояние устройства меняется на аварийное, при нормализации всех текущих аварий восстанавливается нормальное рабочее состояние.

Возможные индикации состояния устройства:

- световая индикация на лицевой панели − светодиод *Alarm* (индикация светодиода *Alarm* описана в меню Описание изделий SMG (SIGTRAN) раздел «Световая индикация»),
- индикация самой критичной аварии в шапке web-конфигуратора (более подробная информация приведена в журнале работы),
- передача событий об авариях в систему мониторинга по протоколу SNMP (trap, inform).

События, по которым генерируются аварийные состояния, делятся на безусловные и опциональные:

- *Безусловные* − аварии, выдача индикации о которых не конфигурируется, к ним относятся:
  - *CONFIG* − критическая авария, авария файла конфигурации;
  - *MEGACO-MODULE* − критическая авария, авария программного модуля H.248/Megaco, отвечающего за работу IP-телефонии;
  - *MGCP-MODULE* − критическая авария, авария программного модуля MGCP, отвечающего за работу IP-телефонии;
  - *SM-VP DEVICE* − авария, неисправность IP-субмодуля SM-VP;
  - *SYNC* − авария при пропадании источника синхронизации либо предупреждение при работе от низкоприоритетного источника синхронизации;
  - *PM-POWER-STATE* − предупреждение об отсутствии напряжения на выходе одного из установленных блоков питания.
- *Опциональные* − аварии, выдача индикации о которых конфигурируется соответствующими настройками, к ним относятся:
  - *STREAM* − критическая авария, поток E1 не в работе;
  - *STREAM-REMOTE* − предупреждение, удаленная авария потока E1;
  - *STREAM-SLIP* − предупреждение, на потоке проскальзывания.

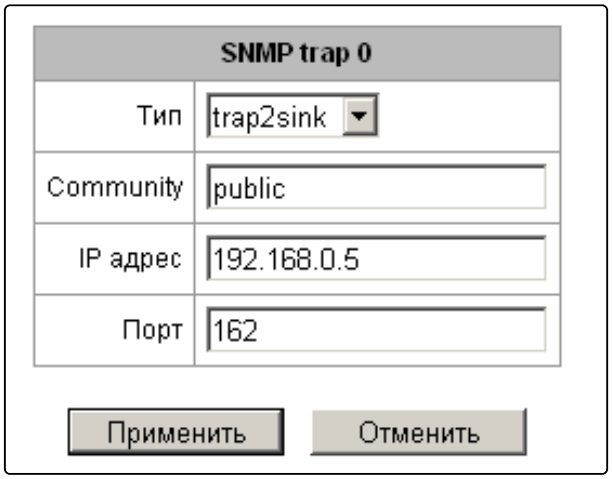
Данные аварии конфигурируются в настройке физических параметров потоков E1 (меню Конфигурирование устройств SMG (SIGTRAN) → подменю Настройка SMG (SIGTRAN) через web-конфигуратор → раздел «Мониторинг потоков E1»).

По умолчанию индикация об опциональных авариях отключена, то есть при взаимодействии с системами мониторинга необходимо сконфигурировать индикацию аварий по всем включенным в работу потокам E1.

Для взаимодействия с системой мониторинга по протоколу SNMP на устройстве необходимо включить протокол SNMP и настроить выдачу сообщений SNMP TRAP или INFORM на IP-адрес сервера мониторинга.

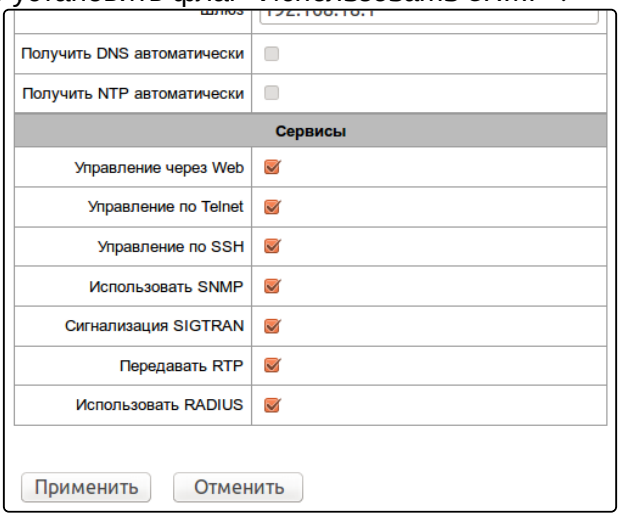
Настройка параметров через web-конфигуратор

1. Настройка индикации опциональных аварий при конфигурировании потока E1 (меню *«Потоки E1/ Физические параметры»*, см. меню Конфигурирование устройств SMG (SIGTRAN) → подменю Настройка SMG (SIGTRAN) через web-конфигуратор → раздел «Настройка физических параметров»).

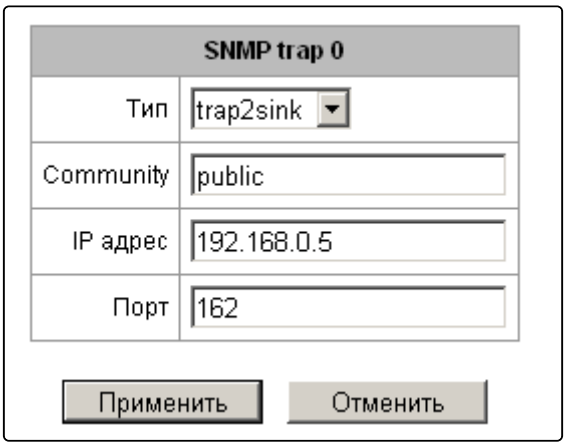


Для индикации аварий LOS, AIS на потоке E1 необходимо установить флаг *«Индикация Alarm»*.Для индикации аварии RAI необходимо установить флаг *«Индикация Remote Alarm»*.Для индикации о проскальзываниях (SLIP) на потоке необходимо поставить флаг *«Индикация SLIP»* и настроить таймер обнаружения SLIP.

2. Включение протокола SNMP производится в меню *«Настройки TCP/IP/Сетевые интерфейсы»* (меню Конфигурирование устройств SMG (SIGTRAN) → подменю Настройка SMG (SIGTRAN) через web-конфигуратор → раздел «Сетевые параметры»*)*.
   Для настройки необходимо установить флаг *«Использовать SNMP»*.



3. Настройка выдачи SNMP трапов производится в меню *«Сетевые сервисы/ SNMP»* (меню Конфигурирование устройств SMG (SIGTRAN) → подменю Настройка SMG (SIGTRAN) через web-конфигуратор → раздел «Настройки SNMP»).



Для настройки необходимо указать тип SNMP сообщения (TRAPv1, TRAPv2, INFORM), пароль (Community), IP-адрес и порт приемника трапов SNMP.

После настройки и применения конфигурации необходимо перезапустить SNMP-агента, нажав на кнопку *«Перезапустить SNMPd»*.

6.4 Приложение Г. Управление и мониторинг по протоколу SNMP

Шлюз поддерживает мониторинг и конфигурирование при помощи протокола SNMP (Simple Network Management Protocol).

Реализованы следующий функции мониторинга:

- сбор общей информации об устройстве, показаниях датчиков, установленном ПО;
- состояние потоков E1 и их каналов;
- состояние VoIP субмодулей и их каналов.

Реализованы следующие функции управления:

- обновление программного обеспечения устройства;
- сохранение текущей конфигурации;
- перезагрузка устройства.

В таблицах с описанием OID в колонке “запросы” будет принят следующий формат описания:

- Get – значение объекта или дерева можно прочитать, отправив GetRequest;
- Set – значение объекта можно установить, отправив SetRequest (обратите внимание, при установке значения через SET к OID следует привести к виду “OID.0”);
- {} – имя объекта или OID;
- N – в команде используется числовой параметр типа integer;
- U – в команде используется числовой параметр типа unsigned integer;
- S – в команде используется строковый параметр;
- A – в команде используется IP-адрес (обратите внимание, некоторые команды, принимающие как аргумент IP-адрес, используют строковый тип данных “s”).

Таблица Г1 – Примеры команд

Описание запроса	**Команда**
Get {}	snmpwalk -v2c -c public -m +ELTEX-SMG $ip_smg activeCallCount
Get {}.x	snmpwalk -v2c -c public -m +ELTEX-SMG $ip_smg pmExist.1 snmpwalk -v2c -c public -m +ELTEX-SMG $ip_smg pmExist.2 и т.д.
Set {} N	snmpset -v2c -c public -m +ELTEX-SMG $ip_smg \ smgSyslogTracesCalls.0 i 60
Set {} 1	snmpset -v2c -c private -m +ELTEX-SMG $ip_smg smgReboot.0 i 1
Set {} U	snmpset -v2c -c public -m +ELTEX-SMG $ip_smg \ getGroupUserByID.0 u 2
Set {} S	snmpset -v2c -c private -m +ELTEX-SMG $ip_smg \ smgUpdateFw.0 s "smg1016m_firmware_3.8.0.1966.bin 192.0.2.2"
Set {} "NULL"	snmpset -v2c -c private -m +ELTEX-SMG $ip_smg \ getUserByNumber.0 s "NULL"
Set {} A	snmpset -v2c -c private -m +ELTEX-SMG $ip_smg \ smgSyslogTracesAddress.0 a 192.0.2.44

Примеры выполнения запросов

Нижеприведённые запросы эквивалентны. На примере запроса объекта `activeCallsCount`, который отображает число текущих вызовов на SMG.

```
$ snmpwalk -v2c -c public -m +ELTEX-SMG 192.0.2.1 activeCallCount
ELTEX-SMG::activeCallCount.0 = INTEGER: 22

$ snmpwalk -v2c -c public -m +ELTEX-SMG 192.0.2.1 smg.42.1
ELTEX-SMG::activeCallCount.0 = INTEGER: 22

$ snmpwalk -v2c -c public -m +ELTEX-SMG 192.0.2.1 1.3.6.1.4.1.35265.1.29.42.1
ELTEX-SMG::activeCallCount.0 = INTEGER: 22

$ snmpwalk -v2c -c public 192.0.2.1 1.3.6.1.4.1.35265.1.29.42.1
SNMPv2-SMI::enterprises.35265.1.29.42.1.0 = INTEGER: 22
```

Описание OID из MIB ELTEX-SMG

Таблица Г2 – Общая информация и датчики

Имя	OID	Запросы	Описание
smg	1.3.6.1.4.1.35265.1.29	Get {}	Корневой объект для дерева OID
smgDevName	1.3.6.1.4.1.35265.1.29.1	Get {}	Имя устройства
smgDevType	1.3.6.1.4.1.35265.1.29.2	Get {}	Тип устройства (всегда 29)
smgFwVersion	1.3.6.1.4.1.35265.1.29.3	Get {}	Версия ПО
smgEth0	1.3.6.1.4.1.35265.1.29.4	Get {}	IP-адрес основного интерфейса
smgUptime	1.3.6.1.4.1.35265.1.29.5	Get {}	Время работы ПО
smgUpdateFw	1.3.6.1.4.1.35265.1.29.25	Set {} S	Обновление ПО. Для этого следует сделать запрос Set с параметрами (разделить пробелом): • имя файла ПО без пробелов; • адрес TFTP-сервера
smgReboot	1.3.6.1.4.1.35265.1.29.27	Set {} 1	Перезагрузка оборудования
smgSave	1.3.6.1.4.1.35265.1.29.29	Set {} 1	Сохранение конфигурации
smgFreeSpace	1.3.6.1.4.1.35265.1.29.32	Get {}	Свободное место на встроенной флэш-памяти
smgFreeRam	1.3.6.1.4.1.35265.1.29.33	Get {}	Количество свободной оперативной памяти
smgMonitoring	1.3.6.1.4.1.35265.1.29.35	Get {}	Отображение датчиков температуры и скорости вращения вентиляторов, корневой объект
smgTemperature1	1.3.6.1.4.1.35265.1.29.35.1	Get {}	Температурный датчик 1
smgTemperature2	1.3.6.1.4.1.35265.1.29.35.2	Get {}	Температурный датчик 2

Имя	OID	Запросы	Описание
smgFan0	1.3.6.1.4.1.35265.1.29.35.3	Get {}	Датчик оборотов вентилятора 1
smgFan1	1.3.6.1.4.1.35265.1.29.35.4	Get {}	Датчик оборотов вентилятора 2
smgFan2	1.3.6.1.4.1.35265.1.29.35.5	Get {}	Датчик оборотов вентилятора 3
smgFan3	1.3.6.1.4.1.35265.1.29.35.6	Get {}	Датчик оборотов вентилятора 4
smgPowerModuleTable	1.3.6.1.4.1.35265.1.29.36	Get {}	Информация о состоянии блоков питания, корневой объект. Для дочерних объектов указывается номер БП: 1 или 2
smgPowerModuleEntry	1.3.6.1.4.1.35265.1.29.36.1	Get {}	см. smgPowerModuleTable
pmExist	1.3.6.1.4.1.35265.1.29.36.1.2.x	Get {}.x	Установлен ли БП 1 - установлен 2 - не установлен
pmPower	1.3.6.1.4.1.35265.1.29.36.1.3.x	Get {}.x	Подаётся ли питание на БП 1 - подаётся 2 - не подаётся
pmType	1.3.6.1.4.1.35265.1.29.36.1.4.x	Get {}.x	Тип установленного БП 1 - PM100-48/12 2 - PM220/12 3 - PM220/12V 4 - PM160-220/12
smgCpuLoadTable	1.3.6.1.4.1.35265.1.29.37	Get {}	Загрузка CPU, корневой объект. Показывает процент загрузки процессора по типам задач. Для дочерних объектов указывается номер процессора: SMG1016M - 1 SMG2016 - 1..4
smgCpuLoadEntry	1.3.6.1.4.1.35265.1.29.37.1	Get {}	см. smgCpuLoadTable
cpuUsr	1.3.6.1.4.1.35265.1.29.37.1.2.x	Get {}.x	% CPU, приложения пользователя
cpuSys	1.3.6.1.4.1.35265.1.29.37.1.3.x	Get {}.x	% CPU, приложения ядра
cpuNic	1.3.6.1.4.1.35265.1.29.37.1.4.x	Get {}.x	% CPU, приложения с изменённым приоритетом
cpuIdle	1.3.6.1.4.1.35265.1.29.37.1.5.x	Get {}.x	% CPU, нахождение в простое
cpuIo	1.3.6.1.4.1.35265.1.29.37.1.6.x	Get {}.x	% CPU, операции ввода-вывода
cpuIrq	1.3.6.1.4.1.35265.1.29.37.1.7.x	Get {}.x	% CPU, обработка аппаратных прерываний
cpuSirq	1.3.6.1.4.1.35265.1.29.37.1.8.x	Get {}.x	% CPU, обработка программных прерываний
cpuUsage	1.3.6.1.4.1.35265.1.29.37.1.9.x	Get {}.x	% CPU, общее использование

Таблица Г3 – Настройки syslog

Имя	OID	Запросы	Описание
smgSyslog	1.3.6.1.4.1.35265.1.29.34	Get {}	Настройки syslog, корневой объект
smgSyslogTraces	1.3.6.1.4.1.35265.1.29.34.1	Get {}	Настройки трассировок в syslog, корневой объект
smgSyslogTracesAddress	1.3.6.1.4.1.35265.1.29.34.1.1	Get {} Set {} S	IP-адрес сервера syslog для приёма трассировок
smgSyslogTracesPort	1.3.6.1.4.1.35265.1.29.34.1.2	Get {} Set {} N	Порт сервера syslog для приёма трассировок
smgSyslogTracesAlarms	1.3.6.1.4.1.35265.1.29.34.1.3	Get {} Set {} N	Уровень трассировки аварий 1-99 - включить трассировку; 0 - отключить трассировку
smgSyslogTracesCalls	1.3.6.1.4.1.35265.1.29.34.1.4	Get {} Set {} N	Уровень трассировки вызовов 1-99 - включить трассировку; 0 - отключить трассировку
smgSyslogTracesRTP	1.3.6.1.4.1.35265.1.29.34.1.8	Get {} Set {} N	Уровень трассировки RTP 1-99 - включить трассировку; 0 - отключить трассировку
smgSyslogTracesMSP	1.3.6.1.4.1.35265.1.29.34.1.9	Get {} Set {} N	Уровень трассировки команд голосовых субмодулей 1-99 - включить трассировку; 0 - отключить трассировку
smgSyslogTracesRowStatus	1.3.6.1.4.1.35265.1.29.34.1.11	Get {} Set {} i 1	Применить изменения в конфигурации трассировок
smgSyslogHistory	1.3.6.1.4.1.35265.1.29.34.2	Get {}	Настройки логирования истории команд в syslog, корневой объект
smgSyslogHistoryAddress	1.3.6.1.4.1.35265.1.29.34.2.1	Get {} Set {} S	IP-адрес сервера syslog для приёма истории команд
smgSyslogHistoryPort	1.3.6.1.4.1.35265.1.29.34.2.2	Get {} Set {} N	Порт сервера syslog для приёма истории команд
smgSyslogHistoryLVL	1.3.6.1.4.1.35265.1.29.34.2.3	Get {} Set {} N	Уровень детализации логов 0 - отключить логирование; 1 - стандартный; 2 - полный
smgSyslogHistoryRowStatus	1.3.6.1.4.1.35265.1.29.34.2.4	Get {} Set {} i 1	Применить изменения в логировании истории команд
smgSyslogConfig	1.3.6.1.4.1.35265.1.29.34.3	Get {}	Настройки системного журнала
smgSyslogConfigLogsEnabled	1.3.6.1.4.1.35265.1.29.34.3.1	Get {} Set {} N	Включить ведение логов 1 - включить; 2 - отключить
smgSyslogConfigSendToServer	1.3.6.1.4.1.35265.1.29.34.3.2	Get {} Set {} N	Отправлять сообщения на сервер syslog 1 - включить; 2 - выключить

Имя	OID	Запросы	Описание
smgSyslogConfigAddress	1.3.6.1.4.1.35265.1.29.34.3.3	Get {} Set {} S	IP-адрес сервера syslog
smgSyslogConfigPort	1.3.6.1.4.1.35265.1.29.34.3.4	Get {} Set {} N	Порт сервера syslog
smgSyslogConfigRowStatus	1.3.6.1.4.1.35265.1.29.34.3.5	Get {} Set {} i 1	Применить изменения в настройках системного журнала

Таблица Г4 – Мониторинг потоков E1

Имя	OID	Запросы	Описание
eOneLineInfoPhyState	1.3.6.1.4.1.35265.1.29.7.1.2 1.3.6.1.4.1.35265.1.29.7.1.2.x	Get {} Get {}.x	Физическое состояние потока E1. Для получения состояния конкретного потока надо дополнить OID его номером (0..15) Состояния потока: 0 — поток отключен; 1 — ALARM; 2 — LOS; 3 — AIS; 4 — LOM; 5 — LOMF; 6 — поток в работе; 7 — на потоке включен PRBS тест
eOneLineInfoRemAlarm	1.3.6.1.4.1.35265.1.29.7.1.3 1.3.6.1.4.1.35265.1.29.7.1.3.x	Get {} Get {}.x	Наличие на потоке сигнала RAI - ошибка на удалённой стороне. Для получения состояния конкретного потока надо дополнить OID его номером (0..15) 0 — нормальное состояние; 1 — получен сигнал RAI
eOneLineInfoRemAlarmTS16	1.3.6.1.4.1.35265.1.29.7.1.4 1.3.6.1.4.1.35265.1.29.7.1.4.x	Get {} Get {}.x	Наличие на потоке сигнала RAI16 - ошибка на удалённой стороне по 16 канальному интервалу. Для получения состояния конкретного потока надо дополнить OID его номером (0..15) 0 — нормальное состояние; 1 — получен сигнал RAI16
eOneLineStateAlarm	1.3.6.1.4.1.35265.1.29.7.1.5 1.3.6.1.4.1.35265.1.29.7.1.5.x	Get {} Get {}.x	Состояние аварий на потоке. Для получения состояния конкретного потока надо дополнить OID его номером (0..15) 0 — аварий нет или поток выключен; 1 — критическая авария, поток не в работе; 2 — авария, есть ошибки; 3 — код не используется; 4 — авария, ошибка RAI
eOneLineStatePhyWork	1.3.6.1.4.1.35265.1.29.7.1.6 1.3.6.1.4.1.35265.1.29.7.1.6.x	Get {} Get {}.x	Состояние физического линка на потоке (приём сигнала). Для получения состояния конкретного потока надо дополнить OID его номером (0..15) 0 — нет сигнала; 1 — сигнал есть
eOneLinkState	1.3.6.1.4.1.35265.1.29.7.1.7 1.3.6.1.4.1.35265.1.29.7.1.7.x	Get {} Get {}.x	Общее состояние линка. Для получения состояния конкретного потока надо дополнить OID его номером (0..15) 0 — поток не работает; 1 — поток работает;

Имя	OID	Запросы	Описание
eOneStatistTimer	1.3.6.1.4.1.35265.1.29.7.1.9 1.3.6.1.4.1.35265.1.29.7.1.9.x	Get {} Get {}.x	Время сбора статистики, секунды. Для получения состояния конкретного потока надо дополнить OID его номером (0..15)
eOneSlipUp	1.3.6.1.4.1.35265.1.29.7.1.10 1.3.6.1.4.1.35265.1.29.7.1.10.x	Get {} Get {}.x	Проскальзывания (повтор фрейма). Для получения состояния конкретного потока надо дополнить OID его номером (0..15)
eOneSlipDown	1.3.6.1.4.1.35265.1.29.7.1.11 1.3.6.1.4.1.35265.1.29.7.1.11.x	Get {} Get {}.x	Проскальзывания (потеря фрейма). Для получения состояния конкретного потока надо дополнить OID его номером (0..15)
eOneBERCount	1.3.6.1.4.1.35265.1.29.7.1.12 1.3.6.1.4.1.35265.1.29.7.1.12.x	Get {} Get {}.x	Битовые ошибки. Для получения состояния конкретного потока надо дополнить OID его номером (0..15)
eOneCVC	1.3.6.1.4.1.35265.1.29.7.1.13 1.3.6.1.4.1.35265.1.29.7.1.13.x	Get {} Get {}.x	Ошибки сбоя сигнала. Для получения состояния конкретного потока надо дополнить OID его номером (0..15)
eOneCEC	1.3.6.1.4.1.35265.1.29.7.1.14 1.3.6.1.4.1.35265.1.29.7.1.14.x	Get {} Get {}.x	Счётчик ошибок CRC/PRBS. Для получения состояния конкретного потока надо дополнить OID его номером (0..15)
eOneRxCount	1.3.6.1.4.1.35265.1.29.7.1.16 1.3.6.1.4.1.35265.1.29.7.1.16.x	Get {} Get {}.x	Принято байт. Для получения состояния конкретного потока надо дополнить OID его номером (0..15)
eOneTxCount	1.3.6.1.4.1.35265.1.29.7.1.17 1.3.6.1.4.1.35265.1.29.7.1.17.x	Get {} Get {}.x	Передано байт. Для получения состояния конкретного потока надо дополнить OID его номером (0..15)
eOneRxLow	1.3.6.1.4.1.35265.1.29.7.1.18 1.3.6.1.4.1.35265.1.29.7.1.18.x	Get {} Get {}.x	Принято коротких пакетов. Для получения состояния конкретного потока надо дополнить OID его номером (0..15)
eOneRxBig	1.3.6.1.4.1.35265.1.29.7.1.19 1.3.6.1.4.1.35265.1.29.7.1.19.x	Get {} Get {}.x	Принято длинных пакетов. Для получения состояния конкретного потока надо дополнить OID его номером (0..15)
eOneRxOvfl	1.3.6.1.4.1.35265.1.29.7.1.20 1.3.6.1.4.1.35265.1.29.7.1.20.x	Get {} Get {}.x	Переполнение приёмника. Для получения состояния конкретного потока надо дополнить OID его номером (0..15)
eOneRxCRC	1.3.6.1.4.1.35265.1.29.7.1.21	Get {} Get {}.x	Ошибки CRC. Для получения состояния конкретного потока надо дополнить OID его номером (0..15)
eOneTxUrun	1.3.6.1.4.1.35265.1.29.7.1.22	Get {} Get {}.x	Сбои передачи. Для получения состояния конкретного потока надо дополнить OID его номером (0..15)

Поддержка OID MIB-2 (1.3.6.1.2.1)

SMG поддерживает следующие ветки MIB-2:

- system (1.3.6.1.2.1.1) – общая информация о системе;
- interfaces (1.3.6.1.2.1.2) – информация о сетевых интерфейсов;
- snmp (1.3.6.1.2.1.11) – информация о работе SNMP.

6.5 Приложение Д. Обеспечение функций СОРМ

Программно-аппаратные средства устройства позволяют выполнить технические требования к системе технических средств по обеспечению функций оперативно-розыскных мероприятий на электронных АТС, утвержденные приказом Госкомсвязи России от 20.04.1999 №70 и приказом Минкомсвязи России №268 от 19.11.2012. Организация каналов передачи данных (КПД) между SMG и ПУ СОРМ для передачи управляющей информации и информации о контролируемых соединениях предусматривает вариант, представленный на рисунке ниже.

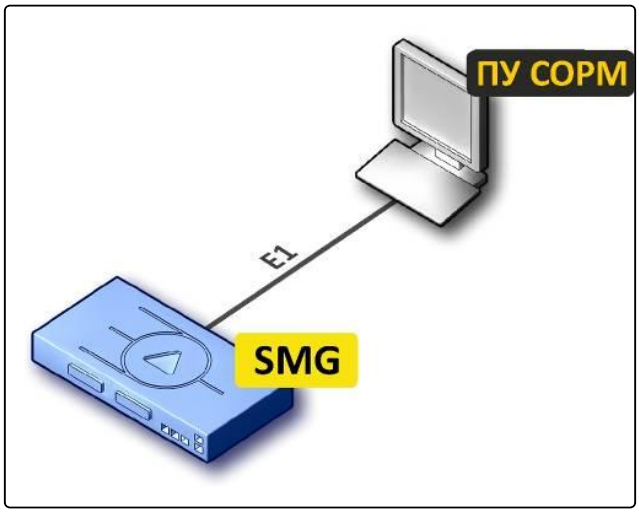


Рисунок 34 – Схема подключения SMG к ПУ СОРМ

Медиашлюз SMG позволяет организовать один поток E1 до пульта СОРМ спецслужб. Один поток E1 СОРМ содержит 28 разговорных каналов (КСЛ – контрольно соединительных линий) для прослушивания контролируемых абонентов.

При совмещенном контроле в разговорный канал потока СОРМ замешивается звуковой трафик от абонентов А и Б. Смешивание звуковых потоков происходит при помощи трехсторонней конференции на VoIP-субмодуле. Один субмодуль VoIP поддерживает 27 трехсторонних конференций. Таким образом, для обеспечения возможности перехвата одновременно по всем каналам потока E1 необходимо, чтобы на шлюзе было установлено не менее 2 субмодулей VoIP (SM-VP-M300).

Для обеспечения работы СОРМ полностью резервируется один субмодуль SM-VP-M300. Прочие вызовы через него ходить не будут.

6.5.1 Расчет необходимого числа субмодулей при использовании СОРМ

При использовании шлюза для коммутации сетей TDM и VoIP, количество субмодулей определяется необходимым количеством каналов для обслуживания вызовов. Вызов между двумя VoIP-интерфейсами или SIP-абонентами задействует два канала субмодуля VoIP.

Данные о количестве VoIP-каналов, поддерживаемых субмодулем в зависимости от типа кодека, приведены в меню Конфигурирование устройств SMG (SIGTRAN) → подменю Настройка SMG (SIGTRAN) через web-конфигуратор → раздел «Основные технические параметры».

При расчете необходимо учитывать, что количество свободных каналов при 28 одновременных перехватах будет ограничено, данное ограничение приведено в таблице ниже. Например, при использовании кодека G.711 для передачи голоса на три субмодуля VoIP останутся свободны всего 108 каналов.

Таблица Д1 – Количество свободных каналов при использовании СОРМ для различных кодеков

Кодек/время пакетизации	Количество свободных каналов при использовании 3х субмодулей VoIP и занятии всех 28 каналов в потоке СОРМ
G.711 (A/U) / 20-60	108
G.711 (A/U) / 10	76
G.729 A / 20-80	48
G.729 A / 10	42
G.723.1 (6.3 Kbps, 5.3 Kbps)	42
G.726 / 20	66
G.726 / 10	60
T.38	38

6.5.2 Логика работы постановки на контроль и перехватов вызовов СОРМ

Шлюз работает только в качестве транзитного узла связи.

ПУ СОРМ подключается по потоку E1 и, при необходимости, по TCP/IP.

Первоначально с ПУ СОРМ подается команда старта технических средств СОРМ. Затем происходит закрепление групп КСЛ (канальных интервалов потока E1 для прослушки вызовов) для совмещенного (в одном КИ слышны оба абонента) или раздельного (один абонент в одном КИ, второй в другом) контроля. Одна группа КСЛ используется либо только для совмещенного, либо только для раздельного контроля.

Далее идет *«постановка абонента на контроль»* (команда №5). Закрепление на контроль идет в формате E.164:

- междугородные российские номера <7>+<код города>+<номер телефона>;
- международные номера <код страны>+<код города>+<номер телефона>;

Параметры принятые в команде анализируются на корректность: соответствие типа объекта (абонент сети по полному/неполному номеру или пучок каналов) и признака номера (абонент России, абонент другой страны), номера группы КСЛ с типом контроля (совмещенный/раздельный), указанной длины номера с количеством цифр в номере.

Имени пучка каналов соответствует имя сервера приложений (AS).

Соответствие типа контроля и признака номера следующее:

- тип объекта «абонент сети по полному/неполному номеру» может иметь признак «абонент России», «абонент другой страны»;
- тип объекта «пучок каналов» ставится на контроль без признака номера телефона.

После этого идет сравнение полученного номера, типа и признака с префиксами CdPN нулевого плана нумерации. Признак префикса определяется по параметру «направление/объект»:

- междугородная связь – абонент России;
- международная связь – абонент другой страны.

Если подходящий абонент/префикс найден, то даем подтверждение команды и заносим номер и его параметры в БД СОРМ. Иначе отклоняем выполнение команды с указанием кода ошибки, по причине которой не произошла постановка на контроль.

На этом постановка на контроль закончена. Начиная со следующего вызова будет осуществляться «перехват вызовов» контролируемого абонента.

При поступлении вызова производится сверка номеров CgPN, CdPN и Redirecting PN (при соответствующей настройке) с БД СОРМ. Если номер стоит на контроле — выделяем для него КСЛ в соответствии с типом контроля и выдаем на ПУ информацию об этапах установления соединения (41-43).

6.5.3 Методика настройки медиашлюза SMG для сдачи протокола СОРМ в соответствии с Приказом Минкомсвязи РФ от 19.11.2012 №268

Постановка на контроль – получение от ПУ СОРМ команды №5 с номером абонента, который необходимо контролировать, а также его параметров контроля. При наличии номера в конфигурации его номер и параметры контроля заносятся во внутреннюю базу данных устройства, при этом на ПУ СОРМ будет отправлено подтверждение успешного выполнения команды. Если номер отсутствует в конфигурации или какие-либо параметры в команде №5 были заданы неверно, на ПУ СОРМ будет отправлено сообщение о невыполнении данной команды.

Перехват вызова – передача ПУ СОРМ сообщений обо всех этапах установления соединения абонента, поставленного на контроль (занесенного во внутреннюю базу данных устройства).

Для успешной сдачи функции оперативно-розыскных мероприятий необходимо произвести следующие действия:

1. Убедиться, что в шлюзе установлено не менее двух субмодулей SM-VP-M300. Количество установленных субмодулей можно посмотреть в web-конфигураторе в меню Конфигурирование устройств SMG (SIGTRAN) → подменю Настройка SMG (SIGTRAN) через web-конфигуратор → раздел Мониторинг VoIP субмодулей;
2. Обновить ПО на версию не менее V.1.3.0.xxx;
3. Установить лицензию СОРМ;
4. Организовать поток E1 между медиашлюзом SMG и ПУ СОРМ Спецслужб:
    - расшить поток E1;
    - в конфигурации шлюза включить поток;
    - в конфигурации шлюза на потоке выбрать протокол СОРМ;
    - в конфигурации шлюза на потоке СОРМ выбрать спецификацию RUS Приказ №268;
    - при необходимости настроить модификаторы и установить их в настройках данного потока;
    - убедиться, что на каналах 1 и 2 установлен режим работы канала «DTE», сообщить сотрудникам спецслужб, что они должны установить на своем оборудовании режим «DCE»;
    - убедиться, что на потоке нет увеличения счетчиков положительных и отрицательных слипов (настроена синхронизация между SMG и пультом СОРМ)

    После выбора протокола СОРМ на одном из потоков необходимо произвести перезапуск ПО.
5. В плане нумерации настроить отбор вызовов в соответствии с требованиями Приказа Минкомсвязи РФ от 19.11.2012 №268.
   В Приказе Минкомсвязи РФ от 19.11.2012 №268 описан формат номеров, в котором абоненты должны закрепляться на контроль, и требования к выдаче номеров А и Б в сообщениях о перехвате вызовов абонентов.

Междугородные абоненты закрепляются на контроль и передаются в сообщениях перехвата в формате 11 цифр с префиксом 7 в начале номера.
Международные абоненты закрепляются на контроль и передаются в сообщениях перехвата без префикса выхода на международную сеть (без префикса 810).

6. В настройках групп линий ОКС-7 добавьте необходимо количество групп линий ОКС-7 по количеству взаимодействующих пар точек доступа подсистем ISUP и задайте значения их кодов. Речевая информация передаваемая по каналам между этими точками впоследствии будет отправляться на пульт СОРМ.
7. При необходимости модифицировать номера, принимаемые в сообщениях от пульта СОРМ либо передаваемые в сторону пульта СОРМ, необходимо настроить "Модификаторы". Данные "Модификаторы" нужно установить на поток Е1, сконфигурированный для работы по протоколу СОРМ.
8. В настройках потока Е1 с настроенной сигнализацией M2UA установите группы линий ОКС-7 и задайте нумерацию каналов CIC.

> ⚠ СОРМ-ирование осуществляется только на для потоков с сигнализацией M2UA.

6.5.4 Обозначения и коды аварий

При возникновении аварий потока Е1 (потеря сигнала (LOS), удаленная авария (RAI)) и аварии на пульт СОРМ будет отправлено сообщение №1 с соответствующим кодом аварии.

Таблица Д2 – Обозначения и коды аварий

Код (Dec)	Код (Hex)	Описание
01	01	авария потока Е1 потеря сигнала (LOS)
02	02	удаленная авария потока Е1 (RAI)

6.5.5 Причины отказа приёма и невыполнения команд

Таблица Д3 – Причины отказа приёма команд, отправляемые в сообщении 7, определенные в Приказе Минкомсвязи РФ от 19.11.2012 №268

Код (Dec)	Код (Hex)	Описание
0	00H	Команда принята к исполнению
1	01H	Команда отвергнута в связи с некорректно заданным форматом команды или некорректно заданными с пункта управления СОРМ параметрами команды
2	02H	Команда отвергнута в связи с заданием команды до запуска технических средств СОРМ

Таблица Д4 – Причины невыполнения команд, отправляемые в сообщении 8, определенные в Приказе Минкомсвязи РФ от 19.11.2012 №268

Код (Dec)	Код (Hex)	Описание
0	00H	Команда выполнена успешно
1	01H	Команда не выполнена
3	03H	Команда не выполнена в связи с неправильным паролем
5	05H	Команда не выполнена в связи с неправильным «номером технических средств СОРМ»
7	07H	Команда не выполнена, так как технические средства СОРМ запущены

Код (Dec)	Код (Hex)	Описание
16	10H	Команда не принята: неверная длина (или неверное количество знаков в номере)
17	11H	Ошибка параметра/параметров
18	12H	Неверный типа объекта
19	13H	Неверный тип номера
20	14H	Неверная категория
21	15H	Ошибка приоритета
22	16H	Команда не принята: СОРМ уже стартовал
23	17H	Команда не принята: СОРМ не запущен
24	18H	Команда не принята: неверный номер СОРМ
25	19H	Неверная длина номера
32	20H	Не задан ни номер ни транк при постановке на контроль
33	21H	Прервано по команде ПУ
37	25H	Транк-группа не задана
48	30H	Группа определена другим типом
49	31H	Таблица объектов переполнена, мониторинг не начат
50	32H	В указанной группе нет такой КСЛ
51	33H	Объект уже задан
52	34H	Неверный номер объекта
53	35H	Номер вызова не найден (в ответах на команды 7 и 8)
54	36H	Номер уже задан
55	37H	Номер объекта не подходит для команды
56	38H	Неверный типа объекта или неверный тип номера
57	39H	Вывод уже завершен (ответ на команду остановить вывод)
58	3AH	КСЛ-а уже закреплена
59	3BH	Совпадает номер
61	3DH	Неверный номер объекта (при подключении к соединению, при отсоединении)
62	3EH	Неверный номер группы КСЛ (нет такой группы, группа занята)
63	3FH	Неверный номер КСЛ-а
64	40H	КСЛ не совпадает (неверная КСЛ)
65	41H	Ошибка команды
68	44H	Количество цифр не совпадает

Код (Dec)	Код (Hex)	Описание
71	47H	Не задан номер транка для объекта типа «транк»
72	48H	Задан и номер объекта, и номер транка
73	49H	Не найден транк с таким номером
74	4AH	Такой транк уже контролируется
75	4BH	Общее количество контролируемых транков достигло 10
76	4CH	Номер транка не совпадает с ранее заданным
78	4EH	Задан номер транка не для того типа объекта
83	53H	Не найден ни номер, ни направление
84	54H	Порт не локальный
85	55H	Признак номера неверен
86	56H	Неверный тип объекта для локального порта
87	57H	Передан неподходящий признак номера для данного номера
95	5FH	Ни одна КСЛ не была выбрана (нет КСЛ, соответствующих запросу)
97	61H	ДВО не заданы
115	73H	Ошибка выделения КСЛ

Таблица Д5 – Нестандартные причины отказа приёма и невыполнения команд, отправляемые в сообщениях 7 и 8, определенные в SMG

6.6 Приложение Е. Рекомендации по безопасности

При установке и настройке SMG следует уделить внимание настройкам безопасности – организации доступа к управлению и мониторингу АТС, а также безопасности обработки вызовов. Также следует уделить внимание резервному копированию конфигурации.

Организация доступа подразумевает:

- смену стандартных паролей на web и CLI;
- создание ограниченных учётных записей для отдельных видов настроек и мониторинга;
- настройку ограничений IP-адресов и/или подсетей, с которых может производиться конфигурирование и мониторинг;
- настройку статического брандмауэра, ограничивающих доступ к интерфейсам сигнализации и управления только доверенными узлами;
- настройку динамического брандмауэра, что позволит в автоматическом режиме отсечь нежелательные попытки доступа для общедоступных интерфейсов.

⚠ Применение SMG в публичной сети нежелательно без использования дополнительных средств защиты, таких как пограничный контроллер сессий (SBC), межсетевой экран (firewall) и т.п.

6.6.1 Смена паролей на web и CLI

⚠ Смена паролей для учетных записей admin/root является обязательной для обеспечения безопасности устройства.

Смена паролей производится через меню «*Пользователи: Управление*».

Смена пароля web для учётной записи admin производится в блоке «Установить пароль администратора веб-интерфейса».

Смена пароля CLI для учётной записи admin производится в блоке «Установить пароль администратора для telnet и ssh». Более подробную информацию по настройке можно найти в разделе меню «Управление».

Смена пароля для учетной записи root производится через shell. Для того чтобы изменить пароль нужно подключиться к SMG через ssh/console и выполнить следующие команды:

```
SMG2016>
SMG2016> sh (выход из режима cli в режим shell)
/home/admin #
/home/admin #
/home/admin # passwd root (команда для смены пароля root)
Changing password for root
New password: (ввести новый пароль)
Retype password: (повторить новый пароль)
Password for root changed by root
/home/admin #
/home/admin #
/home/admin # save
tar: removing leading '/' from member names
***Saved successful
New image 0
Restored successful
/home/admin #
```

6.6.2 Создание ограниченных учётных записей

Создание ограниченных учётных записей для web производится через меню «*Пользователи: Управление*».

- В блоке «Пользователи веб-интерфейса» нажать «*Добавить»;*
- Задать имя и пароль пользователя;
- Выбрать разрешения доступа.

Для CLI создание ограниченных учётных записей не поддерживается. Более подробную информацию по настройке можно найти в разделе «Управление».

6.6.3 Ограничение доступа к интерфейсам сигнализации и управления

Настройка ограничений производится в меню «*Настройки TCP/IP -> «Сетевые интерфейсы»*.

- Зайти в настройки сетевого интерфейса.
- В блоке «Сервисы» отключить все неиспользуемые на интерфейсе протоколы управления и сигнализации.
- Для интерфейса управления рекомендуется разрешать доступ только к web-интерфейсу и ssh

Более подробную информацию по настройке можно найти в разделе Сетевые интерфейсы.

Доступ к устройству по протоколу telnet должен быть запрещен через публичный IP-адрес.

Управление должно быть разрешено НЕ через публичные адреса. Если все-таки используется управление через публичный IP, то необходимо обязательно использовать список разрешенных IP-адресов — нужно внести в белый список адрес, с которого будет разрешено подключение. Для всех остальных доступ должен быть запрещен.

СМЕНА СТАНДАРТНЫХ ПОРТОВ ДЛЯ ДОСТУПА К УСТРОЙСТВУ

Настройка производится в меню *«Настройки TCP/IP» -> «Сетевые параметры»*

- Сменить стандартные (22 для ssh и 23 для telnet) порты доступа к устройству по протоколам ssh/telnet
- Стандартный порт для доступа к устройству через web (по протоколу http) можно изменить через CLI. Для этого необходимо подключиться к SMG через ssh/console и выполнить следующие команды:

  SMG2016>

  SMG2016> config

  Entering configuration mode.

  SMG2016-[CONFIG]> network

  Entering Network mode.

  SMG2016-[CONFIG]-NETWORK>

  PORT Number in the range 1-65535

  SMG2016-[CONFIG]-NETWORK> set settings web (указать необходимый порт в диапазоне 1-65535)

Для доступа к web-интефейсу рекомендуется использовать протокол HTTPS. Настроить его работу можно в разделе *«Безопасность» → «Настройка SSL/TLS»*. В настройках SSL/TLS «Протокол взаимодействия с web-конфигуратором» должен быть выбран режим «только HTTPS». Также возможно использование авторизации через PAM/RADIUS. Более подробную информацию по настройке можно найти в разделе Настройка SSL/TLS.

НАСТРОЙКА СПИСКА РАЗРЕШЕННЫХ IP-АДРЕСОВ

Настройка производится в меню *«Безопасность» -> «Список разрешенных IP адресов»*.

- Внести в белый список адреса, с которых разрешен доступ к устройству через web-конфигуратор и по протоколам telnet/ssh;
- Включить опцию «Доступ только для разрешенных IP адресов»;
- Нажать кнопки *«Применить»* и *«Подтвердить»*.

Более подробную информацию по настройке можно найти в разделе Список разрешенных IP-адресов.

6.6.4 Настройка статического брандмауэра

Статический брандмауэр служит для ограничения доступа к сетевым интерфейсам по списку заранее заданных правил.

Настройка производится в меню «*Безопасность» -> «Статический брандмауэр»*.

- Зайти в настройки брандмауэра;
- Создать профиль брандмауэра, нажав кнопку *«Добавить»;*
- Задать имя профиля, нажать *«Далее»;*

- Задать правила фильтрации для входящего и исходящего трафика. При этом надо помнить, что если входящий или исходящий пакет не попал ни под одно правило фильтрации, то для него применяется действие *«Accept»* (разрешить прохождение пакета). Поэтому, если требуется разрешить доступ лишь некоторым узлам и запретить всем прочим, то необходимо конфигурировать профиль брандмауэра так, чтобы последним правилом было правило с типом источника и назначение «Любое» и действием *«Reject»* или *«Drop»* (отбросить пакет с уведомлением по ICMP или отбросить без уведомления);
- В блоке «Интерфейс» выбрать сетевые интерфейсы, для которых будет применяться фильтрация;
- Нажать кнопку *«Сохранить»,* расположенную под списком интерфейсов;
- Нажать кнопку *«Применить»,* расположенную вверху страницы;
- Нажать кнопку *«Сохранить»*, расположенную над таблицами фильтров.

Более подробную информацию по настройке можно найти в разделе Статический брандмауэр.

6.6.5 Настройка динамического брандмауэра

Динамический брандмауэр служит для ограничения доступа к сетевым интерфейсам на основе анализа запросов к различным сервисам. При обнаружении повторяющихся неудачных попыток обращения к сервису с одного и того же IP адреса динамический брандмауэр производит его временную блокировку. Если адрес попадает во временную блокировку несколько раз, он блокируется постоянно в чёрном списке адресов.

Настройка производится в меню «*Безопасность» -> «Динамический брандмауэр»*.

- Зайти в настройки брандмауэра;
- Внести в белый список адреса доверенных узлов и подсетей;
- Поставить флажок «Включить»;
- Нажать кнопку *«Применить»*.

Более подробную информацию по настройке можно найти в разделе Динамический брандмауэр.

Не рекомендуется для сигнализации SIP использовать стандартный порт 5060.

Необходимо периодически проверять информацию в разделе *«Безопасность» → «Журнал заблокированных адресов»*. В нем отображается список заблокированных динамическим брандмауэром адресов, с которых была произведена неудачная попытка получения доступа к устройству.

Рекомендуется периодически менять пароли для доступа к устройству через web/ssh. Политика смены паролей должна определяться вашей службой безопасности.

⚠ Рекомендуется использовать актуальную версию ПО: https://eltex-co.ru/support/downloads/.

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

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

Форма обратной связи на сайте: https://eltex.ru/support/

Servicedesk: https://servicedesk.eltex-co.ru

На официальном сайте компании вы можете найти техническую документацию и программное обеспечение для продукции ООО «Предприятие «ЭЛТЕКС», обратиться к базе знаний или оставить интерактивную заявку:

Официальный сайт компании: https://eltex.ru/

База знаний: https://docs.eltex-co.ru/display/EKB/Eltex+Knowledge+Base

Центр загрузок: https://eltex.ru/download