Коммутаторы Ethernet

MES23xx, MES33xx, MES35xx, MES5324

Руководство по эксплуатации Web-конфигуратора

Версия документа	Дата выпуска	Содержание изменений
Версия 1.0	26.01.2023	Первая публикация
Версия программного обеспечения		

Содержание

1 ВВЕДЕНИЕ 7
2 НАЧАЛО РАБОТЫ 8
2.1 Основные элементы Web-интерфейса 9
2.2 Настройка основных параметров системы. Меню «Система» 14
2.2.1 Системная информация 14
2.2.2 Перезапуск коммутатора 15
2.2.3 Настройка системного времени 15
2.2.3.1 Установка времени и даты 16
2.2.3.2 Настройка синхронизации времени по протоколу SNTP 18
2.2.3.3 Настройка проверки подлинности системы SNTP 20
2.2.4 Настройка IP-адресации и протокола ARP 22
2.2.4.1 Настройка IP-адресации 22
2.2.4.2 Настройка протокола ARP 23
2.2.4.3 Диагностика соединений 25
2.2.5 Настройка параметров DNS 26
2.2.5.1 Настройка сервера DNS 26
2.2.5.2 Установка соответствий между именами хостов и IP-адресами 27
2.2.6 Управление системными журналами 28
2.2.6.1 Общие настройки системного журнала 29
2.2.6.2 Просмотр файла системного журнала 30
2.2.6.3 Просмотр событий журнала, сохраненных в оперативной памяти 31
2.2.6.4 Настройка сервера журнала 32
2.2.7 Управление файлами ПО и конфигурации 33
2.2.7.1 Обновление ПО и конфигурации 33
2.2.7.2 Передача файлов на сервер 35
2.2.7.3 Управление конфигурационными файлами 36
2.2.7.4 Установка исполняемого образа ОС 37
2.3 Настройка протокола SNMP 38
2.3.1 Настройка безопасности 39
2.3.1.1 Настройка глобальных параметров 39
2.3.1.2 Определение объектов OID 40
2.3.1.3 Управление группами SNMP 41
2.3.1.4 Настройка SNMP-пользователей 42
2.3.1.5 Настройка SNMP-сообществ 44
2.3.2 Управление SNMP-сообщениями 45
2.3.2.1 Настройка основных параметров 45
2.3.2.2 Настройка адресатов SNMP-сообщений 45
2.3.2.3 Настройка правил фильтрации trap-сообщений 47
2.4 Диагностика устройства на физическом уровне 49
2.4.1 Настройка зеркалирования сетевого трафика 49
2.4.2 Диагностика медного кабеля 50
2.4.3 Диагностика оптических трансиверов 52
2.4.4 Мониторинг температуры 53
2.4.5 Мониторинг текущей загрузки процессора 53
2.4.6 Мониторинг портов 54
2.5 Управление безопасностью устройства 55
2.5.1 Настройка учетной записи 55
2.5.1.1 Настройка учетной записи пользователя 55
2.5.1.2 Определение паролей для доступа к терминалу 56
2.5.1.3 Определение пароля для смены уровня доступа 57
2.5.2 Настройка механизма аутентитификации 57
2.5.2.1 Настройка профилей аутентификации 57
2.5.2.2 Настройка метода аутентификации при доступе через консоль, Telnet, SSH, HTTP, HTTPS 60
2.5.2.3 Настройка параметров сервера TACACS+ 61
2.5.2.4 Настройка параметров RADIUS-сервера 63
2.5.3 Способы контроля доступа для управления устройством 65

2.5.3.1 Настройка профилей контроля доступа ... 65
2.5.3.2 Управление профилями правил доступа ... 67
2.6 Управление сетевой безопасностью ... 69
2.6.1 Управление трафиком ... 69
2.6.1.1 Контроль широковещательного «шторма» ... 69
2.6.1.2 Обеспечение защиты портов ... 71
2.6.1.3 Обнаружение петель на порту ... 73
2.6.2 Проверка подлинности клиента на основе порта (стандарт 802.1x) ... 74
2.6.2.1 Основные настройки аутентификации (IEEE802.1x) ... 74
2.6.2.2 Базовая проверка подлинности пользователя ... 75
2.6.2.3 Расширенная проверка подлинности пользователя ... 78
2.6.2.4 Просмотр авторизованных пользователей ... 80
2.6.2.5 Статистика протокола EAP (Extensible Authentication Protocol) ... 81
2.6.3 Конфигурирование ACL (списки контроля доступа) ... 82
2.6.3.1 Настройка списков доступа, основанных на MAC-адресации ... 82
2.6.3.2 Настройка списков доступа, основанных на IP-адресации ... 84
2.6.3.3 Назначение списков доступа ACL интерфейсам ... 88
2.7 Настройка функций второго уровня сетевой модели OSI ... 90
2.7.1 Конфигурирование интерфейсов ... 90
2.7.1.1 Определение параметров интерфейсов коммутатора ... 91
2.7.1.2 Управление группами агрегации каналов (LAG) ... 94
2.7.1.3 Управление составом группы LAG ... 96
2.7.1.4 Настройка протокола агрегации каналов LACP ... 98
2.7.2 Управление статической/динамической адресацией ... 99
2.7.2.1 Настройка статической адресации ... 99
2.7.2.2 Настройка динамической адресации ... 100
2.7.3 Настройка протоколов семейства Spanning Tree (STP, RSTP, MSTP) ... 101
2.7.3.1 Общие настройки STP ... 101
2.7.3.2 Настройка STP для определенного интерфейса ... 103
2.7.4 Настройка протокола Rapid STP ... 105
2.7.5 Настройка протокола Multiple STP ... 107
2.7.5.1 Настройка общих параметров для MSTP ... 107
2.7.5.2 Привязка VLAN к экземплярам MSTP ... 108
2.7.5.3 Настройка экземпляров покрывающего дерева ... 109
2.7.5.4 Настройка экземпляров MSTP ... 110
2.7.6 Настройка виртуальных локальных сетей (VLAN) ... 112
2.7.6.1 Общие настройки VLAN ... 112
2.7.6.2 Установка принадлежности интерфейсов к VLAN ... 113
2.7.6.3 Настройки VLAN для интерфейсов коммутатора ... 115
2.7.6.4 Настройка протокола GARP ... 116
2.7.6.5 Настройка протокола GVRP ... 119
2.7.6.6 Просмотр статистики GVRP ... 121
2.7.7 Управление групповой адресацией ... 122
2.7.7.1 Настройка фильтрации групповых адресов ... 122
2.7.7.2 Настройка групп многоадресной передачи, основанных на MAC-адресах ... 123
2.7.7.3 Настройка групп многоадресной передачи, основанных на IP-адресах ... 124
2.7.7.4 Настройка функции IGMP Snooping ... 126
2.7.7.5 Настройка функции MLD Snooping ... 128
2.7.7.6 Просмотр информации о группах, участвующих в групповой рассылке ... 131
2.7.7.7 Настройка интерфейсов к многоадресным маршрутизаторам (mrouter) ... 132
2.7.7.8 Детализация настроек групповой адресации для интерфейсов ... 133
2.7.7.9 Правила для пакетов с незарегистрированными групповыми адресами ... 134
2.7.8 LLDP ... 135
2.8 Управление качеством обслуживания (QoS) ... 136
2.8.1 Общие настройки QoS ... 137
2.8.1.1 Назначение классов сервиса (CoS) для интерфейсов ... 137
2.8.1.2 Настройка очередей ... 139
2.8.1.3 Настройка пропускной способности интерфейсов ... 140
2.8.1.4 Привязка классов обслуживания к очередям ... 142

2.8.1.5 Привязка тега DSCP к очередям ... 143
2.8.2 Базовый режим QoS ... 144
2.8.2.1 Общие настройки для базового режима QoS ... 144
2.8.2.2 Настройка таблицы перемаркировки DSCP ... 145
2.8.3 Расширенный режим QoS ... 146
2.8.3.1 Общие настройки для расширенного режима QoS ... 146
2.8.3.2 Настройка таблицы переопределения кодов DSCP ... 147
2.8.3.3 Настройка критериев классификации трафика ... 148
2.8.3.4 Настройка профиля ограничения скорости ... 149
2.8.3.5 Установка имен политик QoS ... 151
2.8.3.6 Настройка профилей политик QoS ... 151
2.8.3.7 Назначение политики QoS интерфейсу ... 153
2.9 Удаленный мониторинг состояния сети RMON ... 153
2.9.1 Просмотр статистики RMON ... 154
2.9.2 Просмотр и настройка журнала RMON ... 156
2.9.2.1 Настройка журнала RMON ... 156
2.9.2.2 Просмотр журнала RMON ... 157
2.9.3 Просмотр и настройка условий регистрации и генерации событий ... 158
2.9.3.1 Настройка условий регистрации и генерации событий ... 158
2.9.3.2 Просмотр событий, сгенерированных на устройстве ... 159
2.9.4 Настройка аварийной сигнализации ... 160
2.9.5 Просмотр статистики на интерфейсе ... 162
2.9.5.1 Статистика по полученным/переданным пакетам ... 162
2.9.5.2 Статистика уровня Ethernet MAC интерфейса ... 163

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

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.

1 ВВЕДЕНИЕ

Встроенный Web-сервер (WS) позволяет сделать управление коммутатором более наглядным и комфортным. С помощью Web-сервера выполняется конфигурирование, мониторинг, отладка устройства с удаленного рабочего места, используя Web-браузер. Кроме того, Web-интерфейс позволяет получать статистическую информацию об устройстве в графическом виде в реальном времени. Это может быть удобным инструментом для сетевых администраторов при мониторинге производительности сети передачи данных.

В данном руководстве приведена информация о составе Web-интерфейса устройства, об основных навыках навигации по страницам интерфейса. Более подробная информация о конфигурируемых функциях приведена в руководстве по эксплуатации, часть 1, раздел 2.2.

2 НАЧАЛО РАБОТЫ

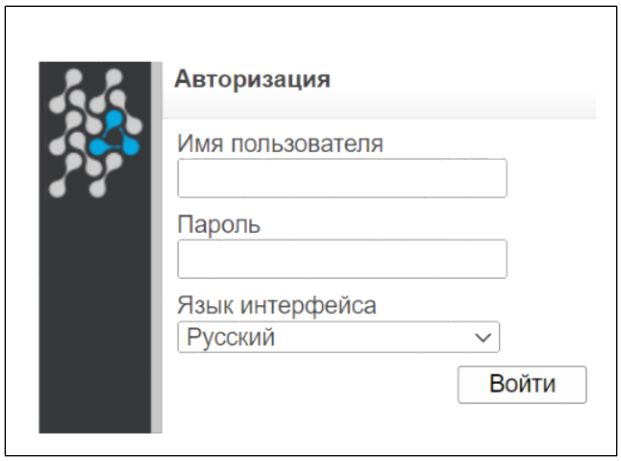
Для начала работы откройте Web-браузер.

Введите в адресной строке браузера IP-адрес устройства, установленный ранее в процедуре начального конфигурирования, и нажмите **Enter**.

Настройка статического IP-адреса, маски подсети и шлюза по умолчанию описана в Руководстве по эксплуатации, часть 1, раздел 4.5.1.2.

При удалении всех IP-адресов коммутатора доступ к нему будет осуществляться по IP-адресу 192.168.1.239/24 во VLAN 1.

При успешном обнаружении устройства в окне браузера отобразится страница с запросом имени пользователя и пароля для доступа к устройству.



Введите имя пользователя и пароль.

По умолчанию определен привилегированный пользователь с именем «admin», с паролем «admin».

Нажмите кнопку «**Войти**». В окне браузера появится страница Web-интерфейса коммутатора: меню *Система* подменю *Информаиця о системе*, см. рисунок 1 на следующей странице.

Во избежание несанкционированного доступа к устройству рекомендуется установить пароль для пользователя «admin», см. раздел 2.5.1 настоящего руководства.

2.1 Основные элементы Web-интерфейса

На рисунке 1 представлены элементы навигации Web-интерфейса коммутатора.

Рисунок 1 — Элементы навигации Web-конфигуратора

Окно Web-интерфейса разделено на четыре области:

1. Поле, в котором отображается системное имя устройства (MES3324), модель устройства (28-port 1G/10G Managed Switch), имя пользователя (admin), а также содержатся управляющие элементы:

   – *Сохранить* — ссылка для записи изменений в энергонезависимую память устройства;
   – *Ru/En* — ссылка для смены языка;
   – *Выйти* — ссылка для выхода или смены пользователя.

2. Меню древовидной структуры, которое содержит папки, гиперссылки для управления полем настроек.
3. Поле настроек устройства, которое базируется на выборе пользователя. Предназначено для просмотра настроек устройства и ввода конфигурационных данных. Управляющие элементы:

   – *Сохранить* — кнопка для применения настроек;
   – — обновление информации в поле настроек устройства;
   – — информация о конфигурируемых параметрах.

4. Информационное поле, в котором отображается версия Web-интерфейса. Описание структуры разделов Web-интерфейса приведено в таблице 1 на следующей странице.

Изменение настроек коммутатора при помощи Web-интерфейса лишь модифицирует текущую конфигурацию и не сохраняет ее при перезагрузке коммутатора. После выполнения настроек для записи изменений в энергонезависимую память устройства нажмите на ссылку «Сохранить».

Таблица 1 — Структура разделов Web-интерфейса

Меню	Описание	№ раздела
Система	Настройка основных параметров системы. Меню «Система»	2.2
Информация о системе	Системная информация	2.2.1
Перезагрузка	Перезапуск коммутатора	2.2.2
Время	Настройка системного времени	2.2.3
Системное время	Установка времени и даты	2.2.3.1
Настройки SNTP	Настройка синхронизации времени по протоколу SNTP	2.2.3.2
Аутенитификация SNTP	Настройка проверки подлинности системы SNTP	2.2.3.3
IP-адресация	Настройка IP-адресации и протокола ARP	2.2.4
IP-интерфейсы	Настройка IP-адресации	2.2.4.1
Настройки ARP	Настройка протокола ARP	2.2.4.2
Утилита Ping	Диагностика соединений	2.2.4.3
Настройка DNS	Настройка параметров DNS	2.2.5
Серверы DNS	Настройка сервера DNS	2.2.5.1
Настройка соответствий имён	Установка соответствий между именами хостов и IP-адресами	2.2.5.2
Журналы	Управление системными журналами	2.2.6
Настройки логирования	Общие настройки системного журнала	2.2.6.1
Журнал на файловой системе	Просмотр файла системного журнала	2.2.6.2
Журнал в оперативной памяти	Просмотр событий журнала, сохраненных в оперативной памяти	2.2.6.3
Syslog-серверы	Настройка сервера журнала	2.2.6.4
Управление файлами	Управление файлами ПО и конфигурации	2.2.7
Загрузка	Обновление ПО и конфигурации	2.2.7.1
Выгрузка	Передача файлов на сервер	2.2.7.2
Копирование	Управление конфигурационными файлами	2.2.7.3
Смена активного образа ПО	Установка исполняемого образа ОС	2.2.7.4
SNMP	Настройка протокола SNMP	2.3
Базопасность	Настройка безопасности	2.3.1
Глобальные параметры	Настройка глобальных параметров	2.3.1.1
Настройки представлений	Определение объектов OID	2.3.1.2
Профили групп	Управление группами SNMP	2.3.1.3
Членство в группах	Настройка SNMP-пользователей	2.3.1.4
Настройки сообществ	Настройка SNMP-сообществ	2.3.1.5
Настройки уведомлений	Управление SNMP-сообщениями	2.3.2
Параметры	Настройка основных параметров	2.3.2.1
Приём уведомлений	Настройка адресатов SNMP-сообщений	2.3.2.2
Фильтрация уведомлений	Настройка правил фильтрации trap-сообщений	2.3.2.3
Аппаратное окружение/ Диагностика	Диагностика устройства на физическом уровне	2.4
Зеркалирование портов	Настройка зеркалирования сетевого трафика	2.4.1
Диагностика кабеля	Диагностика медного кабеля	2.4.2
Оптические трансиверы	Диагностика оптических трансиверов	2.4.3
Термодатчики и охлаждение	Мониторинг температуры	2.4.4
Загрузка процессора	Мониторинг текущей загрузки процессора	2.4.5
Состояние портов	Мониторинг портов	2.4.6
Настройка безопасности	Управление безопасностью устройства	2.5
Пароли	Настройка учетной записи	2.5.1
Локальные пользователи	Настройка учетной записи пользователя	2.5.1.1

Интерфейсы управления	Определение паролей для доступа к терминалу	2.5.1.2
Привилегированный режим	Определение пароля для смены уровня доступа	2.5.1.3
Аутентификация	Настройка механизма аутентитификации	2.5.2
Профили аутентификации	Настройка профилей аутентификации	2.5.2.1
Привязка профилей	Настройка метода аутентификации при доступе через консоль, Telnet, SSH, HTTP, HTTPS	2.5.2.2
TACACS+	Настройка параметров сервера TACACS+	2.5.2.3
RADIUS	Настройка параметров RADIUS-сервера	2.5.2.4
Метод доступа	Способы контроля доступа для управления устройством	2.5.3
Профили доступа	Настройка профилей контроля доступа	2.5.3.1
Настройки правил	Управление профилями правил доступа	2.5.3.2
Сетевая безопасность	Управление сетевой безопасностью	2.6
Управление трафиком	Управление трафиком	2.6.1
Защита от шторма	Контроль широковещательного «шторма»	2.6.1.1
Безопасность портов	Обеспечение защиты портов	2.6.1.2
Обнаружение петель	Обнаружение петель на порту	2.6.1.3
802.1x	Проверка подлинности клиента на основе порта (стандарт 802.1x)	2.6.2
Свойства	Основные настройки аутентификации (IEEE802.1x)	2.6.2.1
Аутентификация портов	Базовая проверка подлинности пользователя	2.6.2.2
Множественный доступ	Расширенная проверка подлинности пользователя	2.6.2.3
Аутентифицированные хосты	Просмотр авторизованных пользователей	2.6.2.4
Статитстика EAP	Статистика протокола EAP (Extensible Authentication Protocol)	2.6.2.5
Списки доступа	Конфигурирование ACL (списки контроля доступа)	2.6.3
По MAC-адресу	Настройка списков доступа, основанных на MAC-адресации	2.6.3.1
По IP-адресу	Настройка списков доступа, основанных на IP-адресации	2.6.3.2
Привязка списков доступа	Назначение списков доступа ACL интерфейсам	2.6.3.3
Настройки L2	Настройка функций второго уровня сетевой модели OSI	2.7
Интерфейсы	Конфигурирование интерфейсов	2.7.1
Конфигурация портов	Определение параметров интерфейсов коммутатора	2.7.1.1
Конфигурация LAG	Управление группами агрегации каналов (LAG)	2.7.1.2
Членство LAG	Управление составом группы LAG	2.7.1.3
Параметры LACP	Настройка протокола агрегации каналов LACP	2.7.1.4
Таблица MAC-адресов	Управление статической/динамической адресацией	2.7.2
Статические адреса	Настройка статической адресации	2.7.2.1
Динамические адреса	Настройка динамической адресации	2.7.2.2
Протокол связующего дерева	Настройка протоколов семейства Spanning Tree (STP, RSTP, MSTP)	2.7.3
Глобальные параметры	Общие настройки STP	2.7.3.1
Параметры интерфейсов	Настройка STP для определенного интерфейса	2.7.3.2
Протокол быстрого связующего дерева (RSTP)	Настройка протокола Rapid STP	2.7.4
Протокол множественных связующих деревьев (MSTP)	Настройка протокола Multiple STP	2.7.5
Глобальные параметры	Настройка общих параметров для MSTP	2.7.5.1
Привязка VLAN к экземплярам связующего дерева	Привязка VLAN к экземплярам MSTP	2.7.5.2
Параметры экземпляров связующего дерева	Настройка экземпляров покрывающего дерева	2.7.5.3
Параметры интерфейсов	Настройка экземпляров MSTP	2.7.5.4
VLAN	Настройка виртуальных локальных сетей (VLAN)	2.7.6
Настройка	Общие настройки VLAN	2.7.6.1

Членство	Установка принадлежности интерфейсов к VLAN	2.7.6.2
Параметры интерфейсов	Настройки VLAN для интерфейсов коммутатора	2.7.6.3
Настройки GARP	Настройка протокола GARP	2.7.6.4
Параметры GVRP	Настройка протокола GVRP	2.7.6.5
Статистика GVRP	Просмотр статистики GVRP	2.7.6.6
Передача группового трафика	Управление групповой адресацией	2.7.7
Глобальные параметры	Настройка фильтрации групповых адресов	2.7.7.1
Статические MAC-группы	Настройка групп многоадресной передачи, основанных на MAC-адресах	2.7.7.2
Статические IP-группы	Настройка групп многоадресной передачи, основанных на IP-адресах	2.7.7.3
IGMP Snooping	Настройка функции IGMP Snooping	2.7.7.4
MLD Snooping	Настройка функции MLD Snooping	2.7.7.5
Просмотр зарегистрированных групп	Просмотр информации о группах, участвующих в групповой рассылке	2.7.7.6
Роли портов в пересылке многоадресного трафика	Настройка интерфейсов к многоадресным маршрутизаторам (mrouter)	2.7.7.7
Контроль передачи многоадресного трафика на порту	Детализация настроек групповой адресации для интерфейсов	2.7.7.8
Управление незарегистрированным многоадресным трафиком	Правила для пакетов с незарегистрированными групповыми адресами	2.7.7.9
Качество обслуживания	Управление качеством обслуживания (QoS)	2.8
Основные настройки	Общие настройки QoS	2.8.1
Класс обслуживания	Назначение классов сервиса (CoS) для интерфейсов	2.8.1.1
Очереди	Настройка очередей	2.8.1.2
Ограничение полосы пропускания	Настройка пропускной способности интерфейсов	2.8.1.3
Соответствие между CoS и очередями	Привязка классов обслуживания к очередям	2.8.1.4
Соответствие между DSCP и очередями	Привязка тега DSCP к очередям	2.8.1.5
Базовый режим	Базовый режим QoS	2.8.2
Основные настройки	Общие настройки для базового режима QoS	2.8.2.1
Изменение DSCP	Настройка таблицы перемаркировки DSCP	2.8.2.2
Расширенный режим	Расширенный режим QoS	2.8.3
Основные настройки	Общие настройки для расширенного режима QoS	2.8.3.1
Настройка соответствия DSCP	Настройка таблицы переопределения кодов DSCP	2.8.3.2
Критерии классификации трафика	Настройка критериев классификации трафика	2.8.3.3
Ограничение полосы пропускания	Настройка профиля ограничения скорости	2.8.3.4
Политики	Установка имен политик QoS	2.8.3.5
Привязка критериев классификации трафика к политике	Настройка профилей политик QoS	2.8.3.6
Привязка политики к интерфейсу	Назначение политики QoS интерфейсу	2.8.3.7
Статистика RMON	Удаленный мониторинг состояния сети RMON	2.9
Просмотр статистики	Просмотр статистики RMON	2.9.1
История	Просмотр и настройка журнала RMON	2.9.2
Управление	Настройка журнала RMON	2.9.2.1
Просмотр	Просмотр журнала RMON	2.9.2.2
События	Просмотр и настройка условий регистрации и генерации событий	2.9.3
Управление	Настройка условий регистрации и генерации событий	2.9.3.1
Журнал	Просмотр событий, сгенерированных на устройстве	2.9.3.2
Аварийные сигналы	Настройка аварийной сигнализации	2.9.4

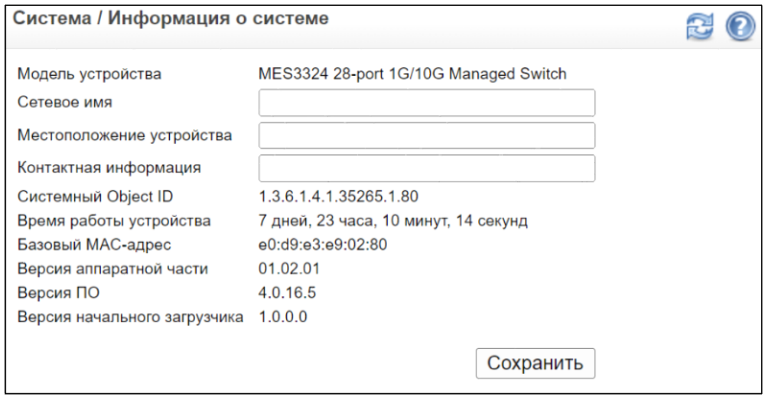
Статистка интерфейсов	Просмотр статистики на интерфейсе	2.9.5
Приём-передача	Статистика по полученным/переданным пакетам	2.9.5.1
Ошибки	Статистика уровня Ethernet MAC интерфейса	2.9.5.2

2.2 Настройка основных параметров системы. Меню «Система»

В данной главе описываются основные настройки коммутаторов серии MES23xx/MES33xx/MES35xx/MES5324.

2.2.1 Системная информация

В меню **Система → Информация о системе** отображается общая системная информация о коммутаторе: модель устройства, версия программного и аппаратного обеспечения, версия загрузчика, время работы устройства, MAC-адрес. Администратор может указать системное имя, место размещения и контактную информацию для устройства.



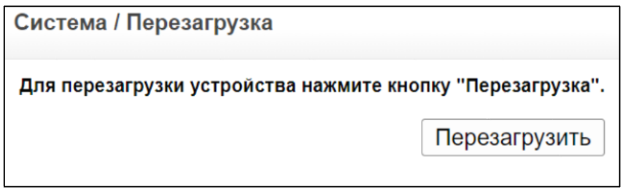
Общая информация о коммутаторе:

- *Модель устройства* — модель коммутатора;
- *Сетевое имя* — сетевое имя устройства, определяемое администратором, ограничивается 160 символами;
- *Местоположение устройства* — местоположение устройства, ограничивается 160 символами;
- *Контактная информация* — контактная информация (пример: имя администратора), ограничивается 160 символами;
- *Системный Object ID* — идентификатор поставщика подсистемы управления сетью;
- *Время работы устройства* — время работы устройства с момента последней перезагрузки, задается в формате: день, часы, минуты, секунды;
- *Базовый MAC-адрес* — MAC-адрес коммутатора;
- *Версия аппаратной части* — номер аппаратной версии;
- *Версия ПО* — номер версии программного обеспечения;
- *Версия начального загрузчика* — текущая версия начального загрузчика.

Для применения настроек нажмите кнопку «Сохранить».

2.2.2 Перезапуск коммутатора

В разделе **Система → Перезагрузка** производится перезапуск коммутатора — осуществляется по нажатию на кнопку «Перезагрузить».



Перед перезагрузкой устройства, для записи изменений в энергонезависимую память устройства нажмите на ссылку «Сохранить».

2.2.3 Настройка системного времени

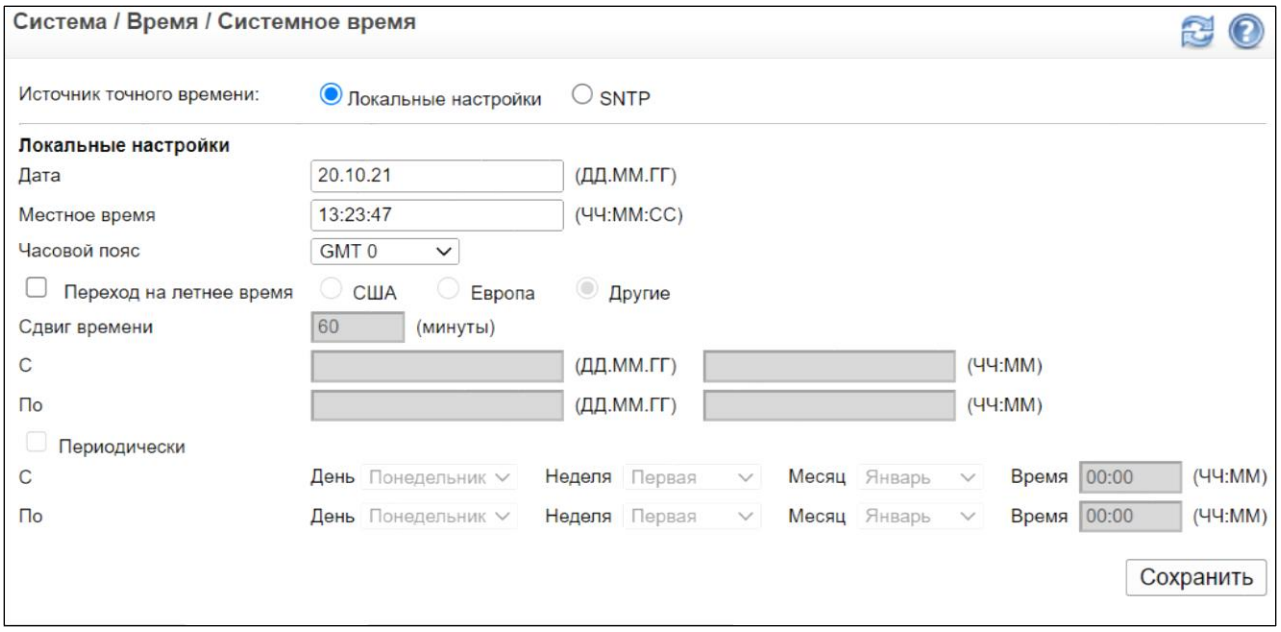
В разделе **Система → Время** производится настройка системного времени коммутатора:

– Установка времени и даты, часового пояса, перехода на летнее время;
– Настройка параметров SNTP;
– Настройка аутентификации SNTP.

2.2.3.1 Установка времени и даты

В разделе **Система → Время → Системное время** устанавливается источник синхронизации времени для устройства, выполняются настройки времени вручную и задается правило перехода на летнее время и обратно.

Настройка системного времени и даты:



– *Источник точного времени* — источник, с которого будут получены настройки времени:

  - *Локальные настройки* — при установленном флаге источник синхронизации времени не используется, системное время и дата будут установлены локально;

  - *SNTP* — при установленном флаге системное время и дата устанавливаются через сервер SNTP, настройки сервера SNTP выполняются в разделе 2.2.3.2.

Настройка системного времени и даты локально:

– *Дата* — текущая дата, задается в формате: день/месяц/год;

– *Местное время* — текущее время, задается в формате: часы: минуты: секунды;

– *Часовой пояс* — часовой пояс относительно среднего времени по Гринвичу;

– *Переход на летнее время* — при установленном флаге включен автоматический переход на летнее время, основанное на местоположении устройства:

  - *США* — при установленном флаге действуют правила перехода на летнее время, используемые в США: переход на летнее время в 2:00 первого воскресенья апреля, и возвращение к стандартному в 2:00 последнего воскресенья октября;

  - *Европа* — при установленном флаге действуют правила перехода на летнее время, используемые Евросоюзом: переход на летнее время в 1:00 последнего воскресенья марта и возвращение к стандартному в 1:00 последнего воскресенья октября;

- *Другие* — при установленном флаге время перехода на летнее время и обратно будет установлено администратором вручную (для определенного года), для этого необходимо заполнить следующие поля:

– *Сдвиг времени* — минуты, добавляемые при переходе на летнее время, (1–1440 минут.) По умолчанию установлено 60 минут;

– *С* — дата и время для автоматического перехода на летнее время: в первом поле указывается дата в формате день/месяц/год, во втором поле время в формате часы:минуты;

– *По* — дата и время для возврата к стандартному времени: в первом поле указывается дата в формате день/месяц/год, во втором поле время в формате часы:минуты;

– *Периодически* — при установленном флаге время перехода на летнее время и обратно будет задано администратором вручную в режиме ежегодно;

– *С* — день и время для автоматического ежегодного перехода на летнее время:

- *День* — день недели (понедельник–воскресенье);
- *Неделя* — неделя месяца (первая, 2, 3, 4, последняя);
- *Месяц* — месяц (январь–декабрь);
- *Время* — время в формате часы: минуты;

– *По* — день и время для возврата к стандартному времени (ежегодно):

- *День* — день недели (понедельник–воскресенье);
- *Неделя* — неделя месяца (первая, 2, 3, 4, последняя);
- *Месяц* — месяц (январь–декабрь);
- *Время* — время в формате часы: минуты.

Для применения настроек нажмите кнопку «Сохранить».

2.2.3.2 Настройка синхронизации времени по протоколу SNTP

В разделе **Система → Время → Настройки SNTP** выполняется настройка синхронизации системного времени устройства с внешним сервером по протоколу SNTP.

SNTP (Simple Network Time Protocol) — упрощенный сетевой протокол синхронизации времени обеспечивает синхронизацию времени сетевого устройства с точностью до миллисекунд. Синхронизация времени осуществляется с сервера SNTP.

Коммутаторы MES23xx/MES33xx/MES35xx/MES5324 работают только в качестве клиента SNTP, и не могут выполнять функции сервера SNTP.

Устройство поддерживает следующие режимы отправки запросов SNTP-серверу:

– *Unicast* — одноадресная передача сообщений. Клиент отправляет запросы выделенному серверу и ожидает от него отклик. Этот режим синхронизации системного времени является наиболее безопасным;

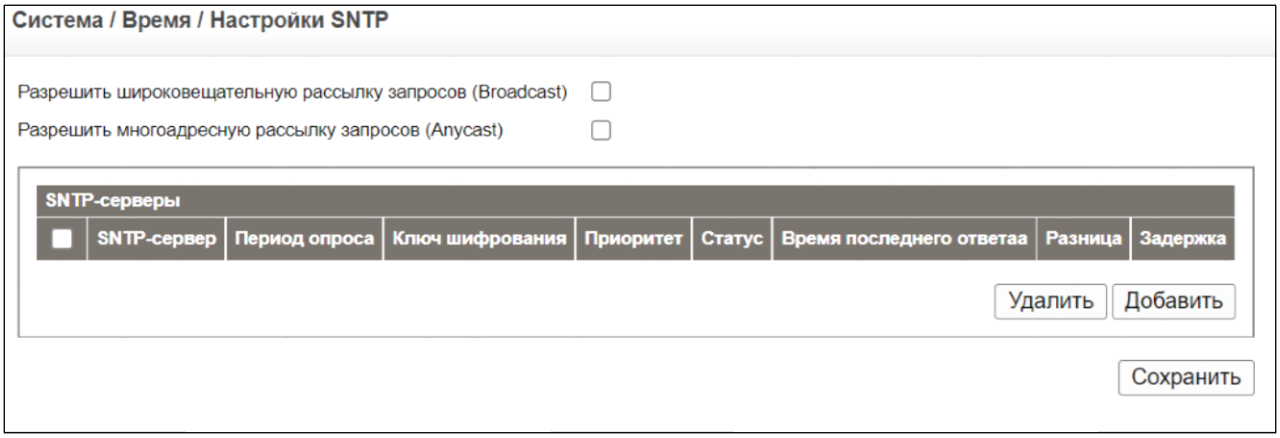
– *Anycast* — передача сообщений ближайшему узлу. Клиент отправляет запросы заданной группе серверов и ожидает отклик от одного серверов. При получении отклика от сервера и установлении с ним соединения последующие ответы от других серверов игнорируются;

– *Broadcast* — широковещательная передача сообщений. В этом режиме клиент ожидает широковещательные сообщения от выделенного сервера. Этот режим рекомендован, когда малое количество серверов обслуживает большое количество клиентов.

Модель синхронизации предполагает иерархическую систему. Уровень определяет точность эталонных часов. Чем выше уровень, где 0 — самый высокий, тем выше точность часов:

– *Уровень 0* — часы реального времени (например, GPS-системы);
– *Уровень 1* — серверы, которые синхронизируются с серверами уровня 0;
– *Уровень 2* — серверы, которые синхронизируются с серверами уровня 1 и тд.

Таким образом, с переходом на каждый уровень возрастает погрешность относительно первичного сервера, но увеличивается общее число серверов и, следовательно, уменьшается их загрузка. Коммутатор получает значение времени с уровня 1 и выше.



Настройка параметров синхронизации по протоколу SNTP:

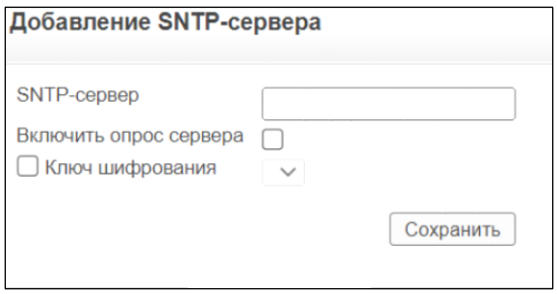
– *Разрешить широковещательную рассылку запросов (Broadcast)* — при установленном флаге информация с сервера SNTP запрашивается широковещательным сообщением. Синхронизация устройства выполняется каждый раз при получении пакета SNTP, даже если запрос на синхронизацию не поступал;

– *Разрешить многоадресную рассылку запросов (Anycast)* — при установленном флаге информация с сервера SNTP запрашивается в режиме «anycast».

В таблице «*SNTP-серверы*» на скриншоте выше приведен пример вывода информации о настроенных SNTP-серверах, которые используются в режиме «Unicast».

– *SNTP-сервер* — IP-адрес SNTP-сервера;
– *Период опроса* — состояние опроса SNTP-сервера:
  - *Включен* — опрос сервера включен;
  - *Выключен* — опрос сервера выключен;
– *Ключ шифрования* — идентификатор ключа шифрования;
– *Приоритет* — описание SNTP-сервера, который предоставляет информацию:
  - *Основной* — информация от первичного SNTP-сервера;
  - *Резервный* — информация от резервного SNTP-сервера;
  - *В работе* — сервер в режиме отправления/получения информации;
  - *Неизвестный* — состояние неизвестно;
– *Статус* — состояние действующего SNTP-сервера:
  - *Настройки получены* — SNTP-сервер работает нормально;
  - *Недоступен* — SNTP-сервер в данный момент не доступен;
  - *Получение настроек* — SNTP-сервер в данный момент в состоянии отправки или получения информации;
  - *Неизвестный* — SNTP-клиент в текущий момент осуществляет поиск SNTP-сервера;
– *Время последнего ответа* — время последнего ответа от SNTP-сервера;
– *Разница* — различие в минутах между DST и временем, установленным на коммутаторе;
– *Задержка* — задержка при подключении к SNTP-серверу.

Для добавления нового SNTP-сервера нужно нажать кнопку «Добавить» и заполнить следующие поля:



Может быть определенно до 8 SNTP-серверов.

– *SNTP-сервер* — IP-адрес SNTP-сервера;

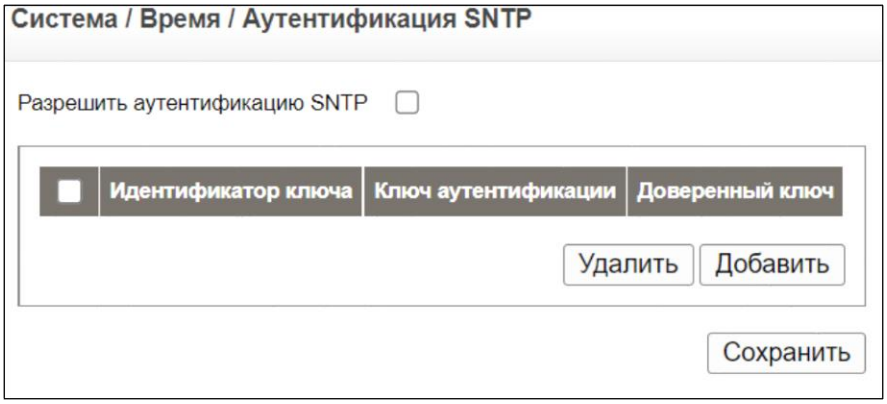
– *Включить опрос сервера* — при установленном флаге коммутатор будет отправлять запросы на SNTP-сервер для получения информации. По умолчанию интервал между опросами составляет 1024 секунды;

– *Ключ шифрования* — при установленном флаге для связи между SNTP-сервером и устройством будет использоваться аутентификация. Из ниспадающего списка требуется выбрать идентификатор ключа (идентификатор ключа шифрования определяется в разделе *Система → Время → Аутентификация SNTP*).

Для применения настроек нажмите кнопку «Сохранить».

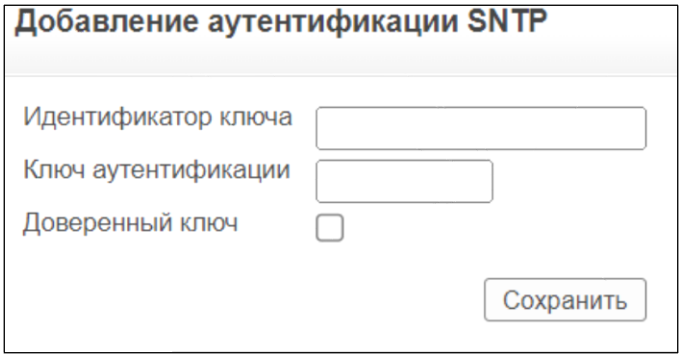
2.2.3.3 Настройка проверки подлинности системы SNTP

В разделе **Система → Время → Аутентификация SNTP** устанавливаются ключи проверки подлинности для протокола SNTP.



– *Разрешить аутентификацию SNTP* — при установленном флаге для получения информации от NTP-серверов требуется проверка подлинности, иначе — не требуется.

При нажатии на кнопку «Добавить» открывается окно настроек:



– *Идентификатор ключа* — идентификатор ключа шифрования;

– *Ключ аутентификации* — идентификатор ключа проверки подлинности, 1–8 символов;

– *Доверенный ключ* — выставленный флаг в данном поле указывает на достоверность вве–денного ключа.

Для применения настроек нажмите кнопку «Сохранить».

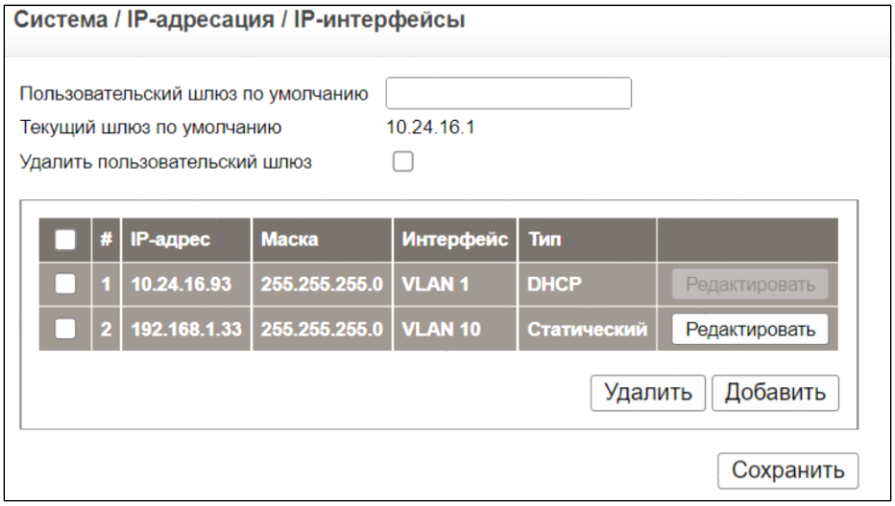
2.2.4 Настройка IP-адресации и протокола ARP

В разделе **Система → IP-адрессация** производятся настройки статических параметров IP-адресации:

– Настройка IP-адресации;
– Настройка протокола ARP;
– Диагностика соединений.

2.2.4.1 Настройка IP-адресации

В разделе **Система → IP-адрессация→ IP-интерфейсы** выполняются настройки статических параметров IP-адресации, таких как IP-адрес, маска подсети, шлюз по умолчанию.

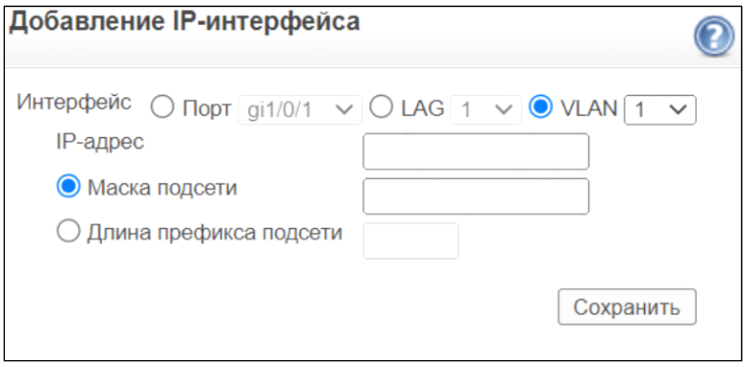


– *Пользовательский шлюз по умолчанию* — IP-адрес шлюза по умолчанию.
Шлюз по умолчанию — это IP-адрес, на который передаются пакеты, имеющие адрес назна–чения вне данной подсети;

– *Текущий шлюз по умолчанию* — используемый IP-адрес шлюза по умолчанию;

– *Удалить пользовательский шлюз* — при установленном флаге шлюз по умолчанию не используется.

Для назначения IP-адреса, маски подсети физическому Ethernet-интерфейсу, интерфейсу VLAN или группе LAG нажмите кнопку «Добавить» и заполните следующие поля:



– *Interface* — укажите интерфейс, которому будет назначен IP-адрес:

  - *Порт* — Ethernet-интерфейс, принимает значения gi0/1..gi0/24, te0/1 .. te0/4;
  - *LAG* — номер агрегированной группы портов LAG;
  - *VLAN* — идентификатор VLAN, принимает значения (1–4094);

– *IP-адрес* — IP-адрес;

– *Маска подсети* — маска подсети;

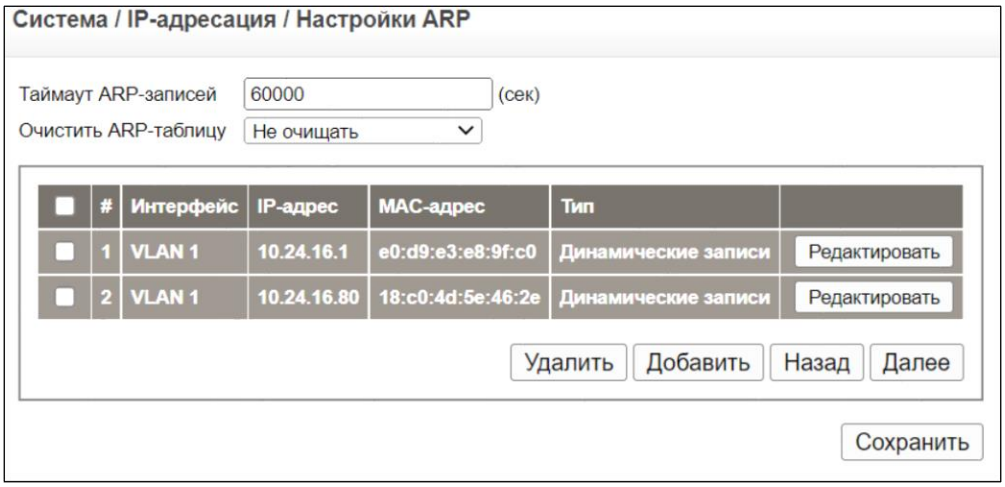
– *Длина префикса подсети* — длина префикса (количество единичных разрядов в маске подсети), принимает значения (8–30). Если установлен флаг «Длина префикса подсети», то поле «*Маска подсети*» не используется.

Для применения настроек нажмите кнопку «Сохранить».

2.2.4.2 Настройка протокола ARP

В разделе **Система → IP-адресация→ Настройки ARP** выполняются настройки для работы устройства по протоколу ARP, осуществляется просмотр и редактирование записей ARP-таблицы.

ARP (Address Resolution Protocol) — протокол определения адресов. Протокол ARP предназначен для установки соответствия IP-адреса с физическим адресом устройства (MAC-адресом) путем поиска соответствующей записи в ARP-таблице. ARP-таблица хранится в памяти и содержит записи (IP-адрес, MAC-адрес) для каждого узла сети и позволяет администратору работать с ARP-записями определенных устройств (добавление, удаление, изменение).



Настройка параметров ARP:

– *Таймаут ARP-записей* — время жизни динамических записей в таблице ARP (1–40000000 секунд), по умолчанию установлено 60000 секунд;

– *Очистить ARP-таблицу* — указывает действие над записями ARP-таблицы по истечении таймаута:

  - *Не очищать* — не удалять записи;
  - *Все записи* — удалить все записи;
  - *Динамические записи* — удалить только динамические ARP-записи;
  - *Статические записи* — удалить только статические ARP-записи.

Работа с ARP-таблицей:

– *Интерфейс* — тип и номер интерфейса, для которого заданы ARP параметры:

  - *Порт* — Ethernet-интерфейс, принимает значения (gi0/1—gi0/48, te0/1 — te0/4);
  - *LAG* — агрегированная группа портов LAG;
  - *VLAN* — идентификатор VLAN, принимает значения (1–4094);

– *IP-адрес* — IP-адрес узла сети;

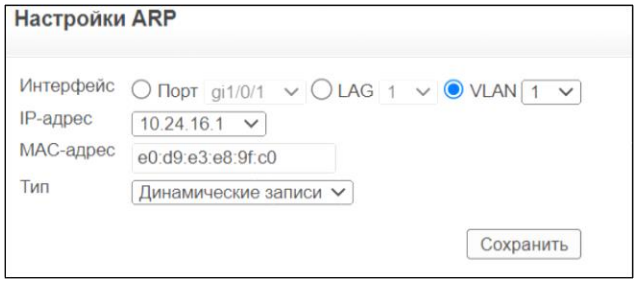
– *MAC-адрес* — MAC-адрес устройства, который соответствует IP-адресу;

– *Тип* — тип ARP-записи:

  - *Динамические записи* — запись внесена динамически — получена коммутатором;
  - *Статические записи* — запись добавлена в таблицу вручную.

Для добавления статической записи в ARP-таблицу нажмите кнопку «Добавить», укажите интерфейс, IP-адрес, MAC-адрес и нажмите кнопку «Сохранить» для сохранения настроек:

Для редактирования параметров нажмите кнопку «Редактировать», заполните соответствующие поля и нажмите кнопку «Сохранить» для сохранения настроек:

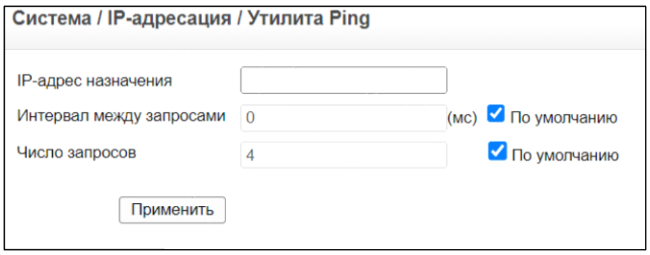


Для удаления записи из ARP-таблицы установите флаг напротив заданной записи и нажмите кнопку «Удалить».

Для применения настроек нажмите кнопку «Сохранить».

2.2.4.3 Диагностика соединений

В разделе **Система→ IP-адресация→ Утилита Ping** можно проверить соединение между коммутатором и другими узлами сети, путем передачи запросов (ICMP Echo—Request) протокола ICMP указанному узлу сети и контроля поступающих ответов (ICMP Echo—Reply).



– *IP-адрес назначения* — IP-адрес узла сети, на который будет отправлен ICMP-запрос;

– *Интервал между запросами* — время ожидания ответа на запрос (50–65535 мс), при установленном флаге «По умолчанию» будет использоваться значение по умолчанию равное 2000 мс;

– *Число запросов* — количество пакетов для передачи (0–65535), при установленном флаге «По умолчанию» будет использоваться значение по умолчанию — 4.

Для передачи ICMP-запроса и сохранения настроек нажмите кнопку «Применить».

Ответ системы «Хост доступен» говорит об успешном прохождении ICMP-запросов. Ответ системы «Ошибка: Таймаут.IP-адрес назначения» говорит, что таймаут ожидания ответа от узла истек, ICMP-запрос не прошел.

2.2.5 Настройка параметров DNS

В разделе **Система → Настройка DNS** выполняются настройки для сервера DNS и определяются соответствия между IP-адресом сервера и именем хоста:

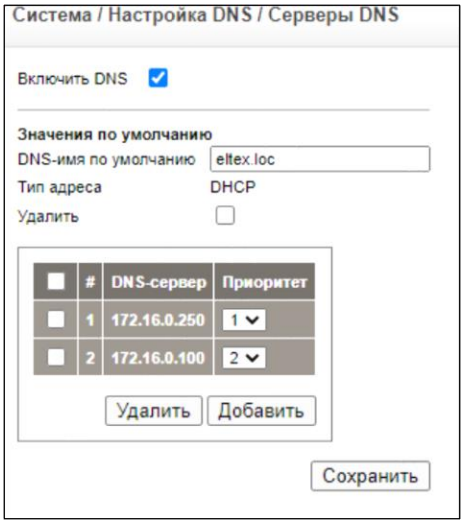
- Настройка параметров сервера DNS;
- Настройка таблицы DNS-имен.

DNS — это протокол, предназначенный для определения IP-адреса узла сети (хоста) по запросу, содержащему его доменное имя. Можно определить IP-адреса для восьми серверов.

Информация о соответствии имени узла IP-адресу хранится в кэш-памяти устройства. В кэш-памяти может содержаться не более 64 записей.

2.2.5.1 Настройка сервера DNS

В разделе **Система → Настройка DNS → Серверы DNS** выполняются настройки для DNS-сервера.



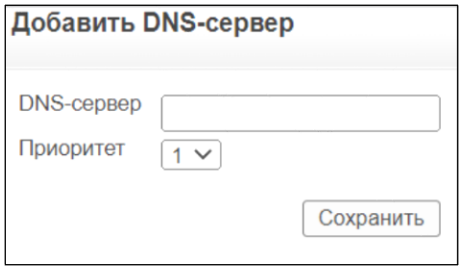
- *Включить DNS* — при установленном флаге разрешена работа по протоколу DNS, иначе — запрещена;

Настройка параметров по умолчанию:

- *DNS-имя по умолчанию* — доменное имя по умолчанию, которое будет использоваться программой для дополнения неправильных доменных имен (доменных имен без точки). Для неправильных имен в конец имени будет добавляться точка и доменное имя, указанное в команде. Имя должно содержать 1 до 158 символов;
- *Тип адреса* — отображается способ получения IP-адреса:
  - *DHCP* — IP-адрес добавлен динамически;
  - *Статический* — IP-адрес добавлен статически;
- *Удалить* — при установленном флаге доменное имя по умолчанию удалится.

Работа с таблицей DNS-серверов:

Для добавления нового DNS-сервера в список доступных серверов нажмите кнопку «Добавить», заполните следующие поля и нажмите кнопку «Сохранить»:



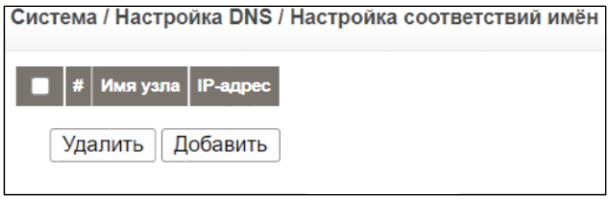
– *DNS-сервер* — IP-адрес DNS-сервера;

– *Приоритет* — Приоритет DNS-сервера от 1 до 8 (чем ниже указанное значение, тем выше приоритет).

Для удаления IP-адреса DNS-сервера из списка доступных установите флаг напротив заданной записи и нажмите кнопку «Удалить». Для изменения приоритета из списка доступных в колонке Приоритет нажать на кнопку выпадающего списка. Для применения настроек нажмите кнопку «Сохранить».

2.2.5.2 Установка соответствий между именами хостов и IP-адресами

В разделе **Система → Настройка DNS → Настройка соответствий** осуществляется просмотр и определение соответствий между именами узлов (хостов) и их IP-адресами. Это позволяет коммутатору получить IP-адрес взаимодействующего устройства по его сетевому имени (хосту).



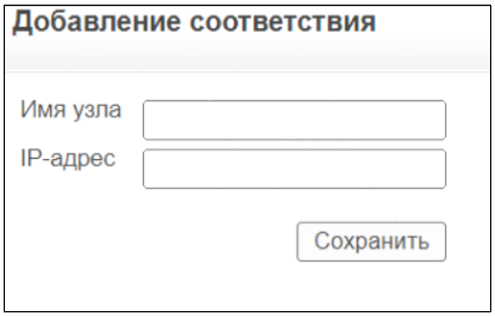
Описание таблицы «Настройка соответствий»:

– # — порядковый номер записи;

– *Имя узла* — имена узлов сети;

– *IP-адрес* — IP-адреса, соответствующие указанным именам узлов сети.

Для добавления записи нажмите кнопку «Добавить», заполните соответствующие поля и нажмите кнопку «Сохранить» для сохранения настроек:



– *Имя узла* — имя узла сети (имя хоста). Каждый хост предоставляет один IP-адрес. Имя узла сети может содержать до 158 символов;

– *IP-адрес* — IP-адрес, назначенный для определенного имени узла сети.

Для удаления записи соответствия имени узла сети IP-адресу установите флаг напротив заданной записи и нажмите кнопку «Удалить».

Для применения настроек нажмите кнопку «Сохранить».

2.2.6 Управление системными журналами

В этом разделе приводится информация об управлении системными журналами.

Системные журналы позволяют просматривать информацию о событиях, произошедших на устройстве, в реальном времени и записывать их для последующего использования. Syslog-журналы используют для записи и контроля произошедших событий, предоставления отчета об ошибках и отправки информационных сообщений.

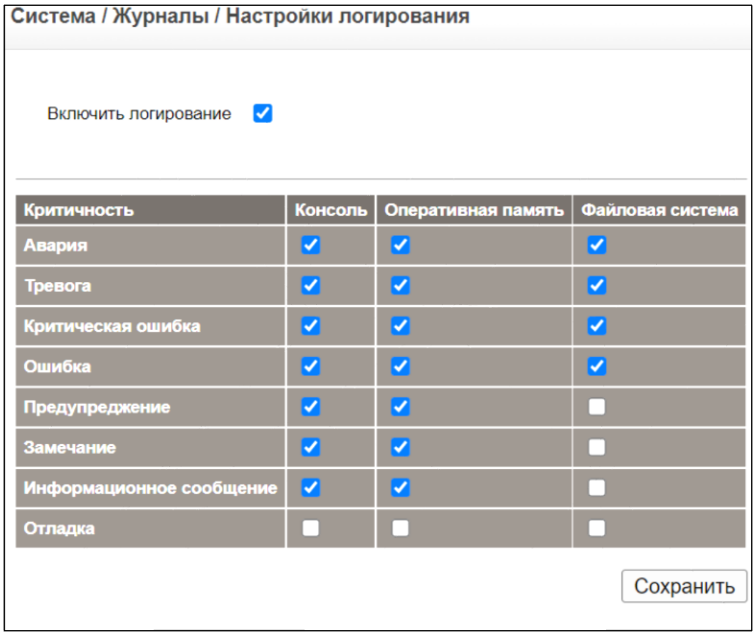
Каждое сообщение имеет свой уровень важности, в таблице 2.1 приведены уровни важности сообщений в порядке их убывания.

Таблица 2.1 — Уровни важности сообщений

Тип важности сообщений	***Уровень***	***Описание***
Авария	0	В системе произошла критическая ошибка, система может работать неправильно.
Тревога	1	Необходимо немедленное вмешательство в систему.
Критическая ошибка	2	В системе произошла критическая ошибка.
Ошибка	3	В системе произошла ошибка.
Предупреждение	4	Предупреждение, неаварийное сообщение.
Замечание	5	Уведомление системы, неаварийное сообщение.
Информационное сообщение	6	Информационные сообщения системы.
Отладка	7	Отладочные сообщения предоставляют пользователю информацию для корректной настройки системы.

2.2.6.1 Общие настройки системного журнала

В разделе **Система → Журналы → Настройки логирования** определяются правила передачи аварийных и отладочных сообщений.



– *Включить логирование* — при установленном флаге включена регистрация отладочных сообщений и сообщений об ошибках.

Настройка свойств Syslog-журнала:

– *Критичность* — уровень важности сообщения, таблица 2.1;

– *Консоль* — при установленном флаге включается передача аварийных и отладочных сообщений заданного уровня на консоль, иначе — сообщения не передаются на консоль;

– *Оперативная память* — при установленном флаге включается передача аварийных и отладочных сообщений заданного уровня во внутренний буфер, иначе — сообщения не передаются во внутренний буфер;

– *Файловая система* — при установленном флаге включается передача аварийных и отладочных сообщений заданного уровня в файл журнала, иначе — сообщения не передаются в файл журнала.

Для применения настроек нажмите кнопку «Сохранить».

2.2.6.2 Просмотр файла системного журнала

В разделе **Система → Журналы → Журнал на файловой системе** приводится информация о событиях устройства, которые сохранены в файле журнала.

Система / Журналы / Журнал на файловой системе

#	Номер сообщения	Время сообщения	Критичность	Описание
1	2147480384	18-Oct-2021 20:41:39	Alert	%RNDMISC-A-RELOAD: Reload requested administratively by user admi
2	2147481446	13-Oct-2021 13:46:42	Alert	%RNDMISC-A-RELOAD: Reload requested administratively by user admi
3	2147481450	13-Oct-2021 13:44:08	Error	%DHCPSNOOP-E-HDRMAC: DHCP packet mac addresses verification pro
4	2147481451	13-Oct-2021 13:43:08	Error	%DHCPSNOOP-E-HDRMAC: DHCP packet mac addresses verification pro
5	2147481452	13-Oct-2021 13:42:09	Error	%DHCPSNOOP-E-HDRMAC: DHCP packet mac addresses verification pro
6	2147481453	13-Oct-2021 13:29:54	Error	%DHCPSNOOP-E-HDRMAC: DHCP packet mac addresses verification pro
7	2147481454	13-Oct-2021 13:28:54	Error	%DHCPSNOOP-E-HDRMAC: DHCP packet mac addresses verification pro
8	2147481455	13-Oct-2021 13:27:55	Error	%DHCPSNOOP-E-HDRMAC: DHCP packet mac addresses verification pro
9	2147481456	13-Oct-2021 13:15:40	Error	%DHCPSNOOP-E-HDRMAC: DHCP packet mac addresses verification pro
10	2147481457	13-Oct-2021 13:14:40	Error	%DHCPSNOOP-E-HDRMAC: DHCP packet mac addresses verification pro
11	2147481458	13-Oct-2021 13:13:40	Error	%DHCPSNOOP-E-HDRMAC: DHCP packet mac addresses verification pro
12	2147481459	13-Oct-2021 13:01:26	Error	%DHCPSNOOP-E-HDRMAC: DHCP packet mac addresses verification pro
13	2147481460	13-Oct-2021 13:00:26	Error	%DHCPSNOOP-E-HDRMAC: DHCP packet mac addresses verification pro
14	2147481461	13-Oct-2021 12:59:26	Error	%DHCPSNOOP-E-HDRMAC: DHCP packet mac addresses verification pro
15	2147481462	13-Oct-2021 12:47:12	Error	%DHCPSNOOP-E-HDRMAC: DHCP packet mac addresses verification pro
16	2147481463	13-Oct-2021 12:46:12	Error	%DHCPSNOOP-E-HDRMAC: DHCP packet mac addresses verification pro
17	2147481464	13-Oct-2021 12:36:06	Error	%DHCPSNOOP-E-HDRMAC: DHCP packet mac addresses verification pro
18	2147481465	13-Oct-2021 12:35:06	Error	%DHCPSNOOP-E-HDRMAC: DHCP packet mac addresses verification pro
19	2147481466	13-Oct-2021 12:33:06	Error	%DHCPSNOOP-E-HDRMAC: DHCP packet mac addresses verification pro

Очистить журнал

Описание полей таблицы:

- *Номер сообщения* — порядковый номер записи события;
- *Время сообщения* — время, когда событие было сгенерировано;
- *Критичность* — уровень важности события, таблица 2.1;
- *Описание* — описание сообщения.

Для удаления записей из журнала нажмите кнопку «Очистить журнал».

2.2.6.3 Просмотр событий журнала, сохраненных в оперативной памяти

В разделе **Система → Журналы → Журнал в оперативной памяти** приводится информация о событиях устройства в хронологическом порядке, которые сохранены во внутреннем буфере.

Система / Журналы / Журнал в оперативной памяти

#	Номер сообщения	Время сообщения	Критичность	Описание
1	2147482083	20-Oct-2021 15:18:42	Информационное сообщение	%BOOTP_DHCP_CL-I-DHCPRENEWED: The devic
2	2147482084	20-Oct-2021 14:39:39	Информационное сообщение	%AAA-I-CONNECT: New http connection for user
3	2147482085	20-Oct-2021 14:14:41	Информационное сообщение	%AAA-I-DISCONNECT: http connection for user a
4	2147482086	20-Oct-2021 12:26:15	Информационное сообщение	%AAA-I-CONNECT: New http connection for user
5	2147482087	20-Oct-2021 12:25:37	Предупреждение	%AAA-W-REJECT: New http connection for user u
6	2147482088	20-Oct-2021 12:18:56	Информационное сообщение	%AAA-I-DISCONNECT: http connection for user a
7	2147482089	20-Oct-2021 11:53:05	Информационное сообщение	%AAA-I-CONNECT: New http connection for user
8	2147482090	20-Oct-2021 11:44:56	Информационное сообщение	%AAA-I-DISCONNECT: http connection for user a
9	2147482091	20-Oct-2021 11:14:54	Информационное сообщение	%AAA-I-CONNECT: New http connection for user
10	2147482092	20-Oct-2021 10:48:41	Информационное сообщение	%AAA-I-DISCONNECT: http connection for user a
11	2147482093	20-Oct-2021 10:34:59	Информационное сообщение	%AAA-I-DISCONNECT: http connection for user a
12	2147482094	20-Oct-2021 10:24:04	Информационное сообщение	%AAA-I-DISCONNECT: User CLI session for user
13	2147482095	20-Oct-2021 10:18:35	Информационное сообщение	%AAA-I-CONNECT: New http connection for user
14	2147482096	20-Oct-2021 10:18:25	Информационное сообщение	%AAA-I-DISCONNECT: http connection for user a
15	2147482097	20-Oct-2021 10:14:35	Информационное сообщение	%AAA-I-CONNECT: New http connection for user
16	2147482098	20-Oct-2021 10:13:58	Информационное сообщение	%AAA-I-CONNECT: User CLI session for user adm
17	2147482099	20-Oct-2021 10:13:56	Предупреждение	%AAA-W-REJECT: New console connection for us
18	2147482100	20-Oct-2021 10:13:18	Информационное сообщение	%AAA-I-DISCONNECT: User CLI session for user
19	2147482101	20-Oct-2021 10:04:57	Информационное сообщение	%AAA-I-CONNECT: New http connection for user
20	2147482102	20-Oct-2021 09:58:46	Информационное сообщение	%AAA-I-CONNECT: User CLI session for user adm

Очистить журнал

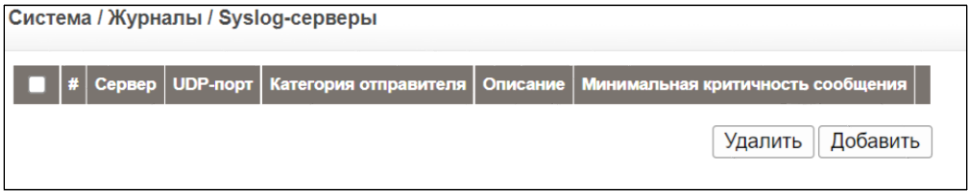
Описание полей таблицы:

- *Номер сообщения* — порядковый номер записи события;
- *Время сообщения* — время, когда событие было сгенерировано;
- *Критичность* — уровень важности события;
- *Описание* — описание сообщения.

Для удаления записей из журнала нажмите кнопку «Очистить журнал».

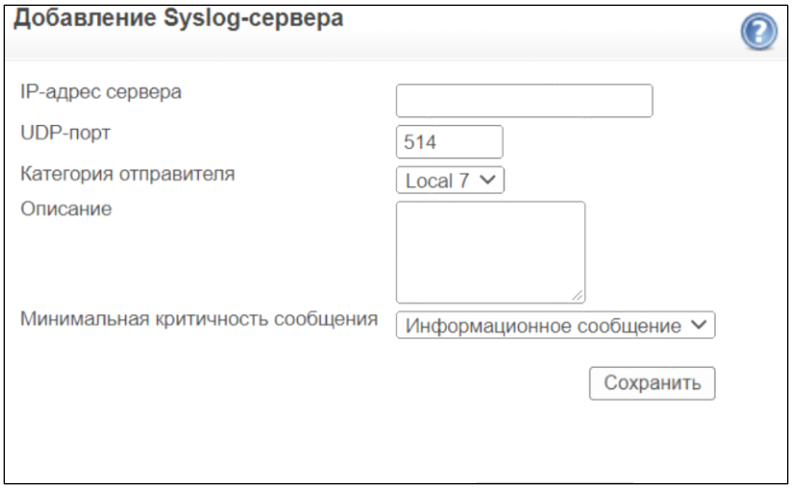
2.2.6.4 Настройка сервера журнала

В разделе **Система → Журналы → Syslog-серверы** выполняется просмотр и настройка удаленных серверов журналов.



Настройка удаленного сервера журналов:

Для добавления нового сервера в список используемых нажмите кнопку «Добавить» и заполните следующие поля:



- *IP-адрес сервера* — IP-адрес удаленного Syslog-сервера;
- *UDP-порт* — порт сервера, используемый для передачи сообщений, (1–65535). По умолчанию установлено значение — 514;
- *Категория отправителя* — идентификатор услуги/канала, передаваемый в сообщениях, (Local0 — Local7). Для каждого сервера можно назначить только один идентификатор. По умолчанию установлено значение — local7;
- *Описание* — описание сервера;
- *Минимальная критичность сообщения* — минимальный уровень важности сообщений (см. таблицу 2.1).

Для применения настроек нажмите кнопку «Сохранить».

2.2.7 Управление файлами ПО и конфигурации

Управление файлами включает в себя управление файлами системного программного обеспечения и конфигурации. Файлы системного ПО необходимы для управления устройством, а файлы конфигурации для настройки устройства.

В коммутаторе существуют следующие типы файлов:

Первоначальная конфигурация хранится в энергонезависимой памяти. При запуске устройства используется для конфигурации устройства. Первоначальная конфигурация может быть создана путем копирования текущей конфигурации (running configuration) или загрузки конфигурации с сервера TFTP либо HTTP. Первоначальная конфигурация может быть удалена, в этом случае после перезагрузки коммутатора будут применены заводские установки (см. раздел **Система → Управление файлами → Копирование)**.

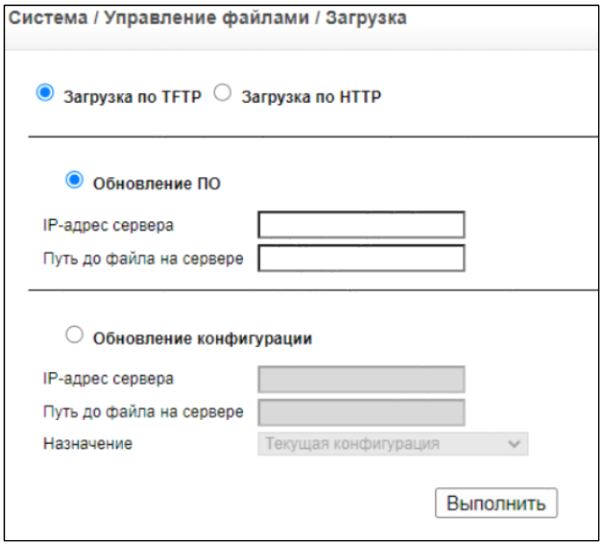
Текущая конфигурация хранится в ОЗУ. При перезагрузке/отключении питания устройства информация, которая сохранена в ОЗУ, удаляется и при включении устройства в текущую конфигурацию копируется информация из первоначальной конфигурации (startup configuration). Таким образом, если необходимо, чтобы текущая конфигурация была восстановлена при включении устройства, необходимо записать ее в файл первоначальной конфигурации (см. раздел **Система → Управление файлами → Копирование)**.

Исполняемые образы ОС — файлы, которые используются при обновлении системного ПО устройства. В коммутаторах серии MES23xx/MES33xx/MES35xx/MES5324 может храниться два файла системного ПО. В разделе **Система → Управление файлами → Смена активного образа** пользователь может указать образ, который будет использоваться после перезагрузки устройства. Загрузить образ ОС в энергонезависимую память устройства можно в разделе **Система → Управление файлами → Загрузка.**

2.2.7.1 Обновление ПО и конфигурации

В разделе **Система → Управление файлами → Загрузка** производится обновление системного ПО устройства и файлов конфигурации.

Загрузка файлов конфигурации и файлов программного обеспечения не может быть выполнена одновременно.



Обновление программного обеспечения:

Для обновления программного обеспечения коммутатора необходимо установить флаг *Обновление ПО* и заполнить следующие поля:

- *Загрузка по TFTP* — при установке данного флага файлы системного ПО будут загружаться с сервера TFTP;
- *Загрузка по HTTP* — при установке данного флага файлы системного ПО будут загружаться с сервера HTTP;
- *IP-адрес сервера* — IP-адрес сервера, с которого будет производиться загрузка;
- *Путь до файла на сервере* — имя файла системного ПО.

Обновление конфигурационных файлов коммутатора:

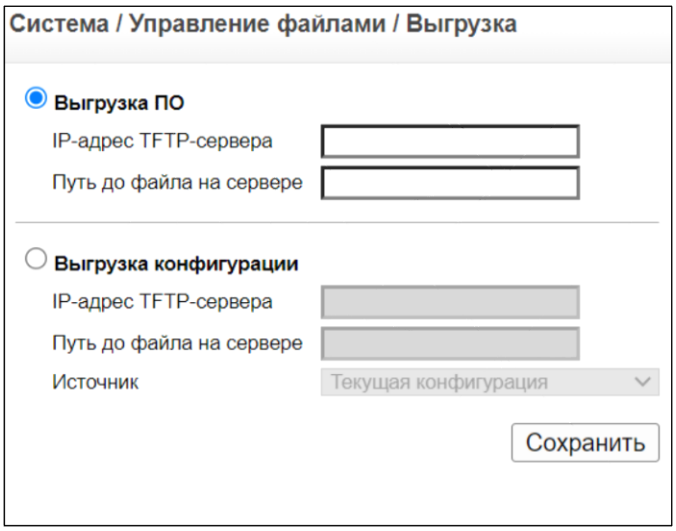
Для обновления файлов конфигурации необходимо установить флаг *Обновление конфигурации* и заполнить следующие поля:

- *Загрузка по TFTP* — при установке данного флага конфигурационные файлы будут загружаться с сервера TFTP;
- *Загрузка по HTTP* — при установке данного флага конфигурационные файлы будут загружаться с сервера HTTP;
- *IP-адрес сервера* — IP-адрес сервера, с которого будет производиться загрузка;
- *Путь до файла на сервере* — имя файла конфигурации;
- *Назначение* — место назначения файла:
  - *Текущая конфигурация* — файл текущей конфигурации;
  - *Первоначальная конфигурация* — файл первоначальной конфигурации.

Нажать кнопку «Выполнить» для загрузки файла.

2.2.7.2 Передача файлов на сервер

В разделе **Система → Управление файлами → Выгрузка** задаются настройки для передачи файлов исполняемого образа ОС и файлов конфигурации на TFTP-сервер.



Передача файлов системного ПО на удаленный TFTP-сервер:

Для передачи файла системного ПО на TFTP-сервер необходимо установить флаг *Выгрузка ПО* и заполнить следующие поля:

– *IP-адрес TFTP-сервера* — IP-адрес TFTP-сервера, на который будет передан файл системного ПО;

– *Путь до файла на сервере* — имя файла системного ПО.

Передача файлов конфигурации на удаленный TFTP-сервер:

Для передачи файлов конфигурации коммутатора на TFTP-сервер необходимо установить флаг *Выгрузка конфигурации* и заполнить следующие поля:

– *IP-адрес TFTP-сервера* — IP-адрес TFTP-сервера;

– *Путь до файла на сервере* — имя файла;

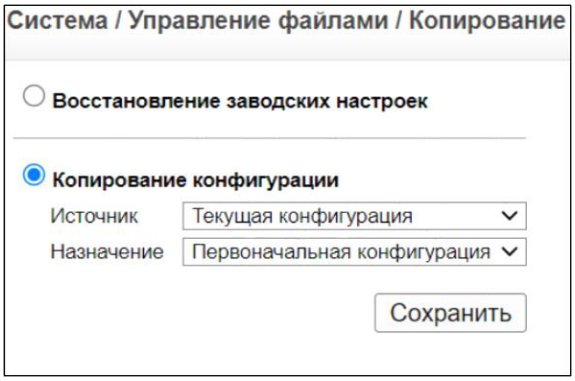
– *Источник* — файл конфигурации, который необходимо передать на удаленный TFTP-сервер:

- *Текущая конфигурация*— файл текущей конфигурации;
- *Первоначальная конфигурация* — файл первоначальной конфигурации.

Для применения настроек нажмите кнопку «Сохранить».

2.2.7.3 Управление конфигурационными файлами

В разделе **Система → Управление файлами → Копирование** производится удаление и копирование конфигурационных файлов.



– *Восстановление заводских настроек* — при установленном флаге осуществляется сброс конфигурации к заводским настройкам. Заводские настройки начинают действовать после сохранения изменений и перезагрузки устройства, иначе устройство поддерживает текущую конфигурацию;

– *Копирование конфигурации* — при установленном флаге производится копирование файлов конфигурации из *текущей* в *первоначальную* или из *первоначальной* в *текущую*. Необходимо указать из какого файла конфигурации будет производиться копирование и файл, в который будет произведено копирование:

  - *Источник* — файл, с которого будет производиться копирование:

    - *Текущая конфигурация* — файл текущей конфигурации;
    - *Первоначальная конфигурация* — файл первоначальной конфигурации;

  - *Назначение* — файл, в который будет производиться копирование:

    - *Текущая конфигурация* — файл текущей конфигурации;
    - *Первоначальная конфигурация* — файл первоначальной конфигурации.

Если необходимо после ряда изменений в конфигурации устройства восстановить начальную конфигурацию, то в поле «*Источник*» нужно указать «*Первоначальная»,* а в поле «*Назначение»* указать «*Текущая конфигурация».*

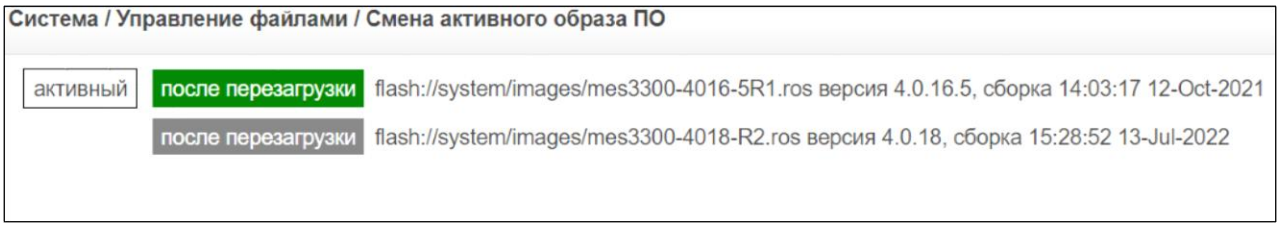
Нажмите кнопку «Сохранить» для копирования начальной конфигурации в текущую.

Если необходимо, чтобы текущая конфигурация была сохранена в энергонезависимой памяти и при включении устройства была восстановлена, то в поле «*Источник*» нужно указать «*Текущая конфигурация»,* а в поле «*Назначение»* указать «*Первоначальная конфигурация».*

Нажмите кнопку «Сохранить» для копирования текущей конфигурации в первоначальную.

2.2.7.4 Установка исполняемого образа ОС

В разделе **Система → Управление файлами → Смена активного образа ПО** можно просмотреть действующий исполняемый образ ОС и задать образ ОС, который будет активен после перезагрузки устройства.



– *Активный* — действующий файл ОС, который устройство загружает при запуске;

– *После перезагрузки* — номер образа ОС, который будет действовать после перезагрузки устройства (подсвечивается зеленым цветом). Выбор осуществляется нажатием левой кнопки мыши на соответствующем поле.

Нажмите кнопку «Сохранить» для применения изменений.

2.3 Настройка протокола SNMP

В данной главе описываются настройки протокола управления сетью SNMP.

Протокол *Simple Network Management Protocol* (SNMP) — простой протокол сетевого администрирования, который предоставляет такие возможности как мониторинг и управление сетевыми устройствами, а также управление конфигурациями устройства, производительностью сети, безопасностью в сети и сбор статистических данных.

Коммутаторы серии MES23xx/MES33xx/MES35xx/MES5324 поддерживают версию 1, v2c и 3 протокола SNMP.

По умолчанию на устройстве включен протокол SNMPv2.

SNMP v1 и v2c

Протокол SNMP используется для получения от сетевых устройств информации об их статусе, производительности и других характеристиках, которые хранятся в базе данных управляющей информации MIB (Management Information Base). База данных MIB содержит переменные, которые контролируются агентом. Агент задает SNMP формат спецификации MIB и формат для доступа к информации через сеть. В SNMP версиях v.1 и v.2 аутентификация пользователей осуществляется при помощи «строки сообщества» («community string»).

SNMP v3

В третьей версии протокола SNMP осуществляется поддержка версий SNMPv1, SNMPv2, используется управление доступом, а также определяется модель, которая ориентирована на пользователя (User-Based Security Model), благодаря которой стало возможным добавление модулей аутентификации и шифрования без смены базовой архитектуры.

Модель USM включает в себя:

– *Аутентификацию* (обеспечивается целостность данных и аутентификация отправителя);

– *Шифрование* (обеспечивается защита передаваемой информации от несанк–ционированного доступа, используется режим шифрования Cipher Block—Chaining);

– *Контроль времени* (обеспечивается защита от задержек);

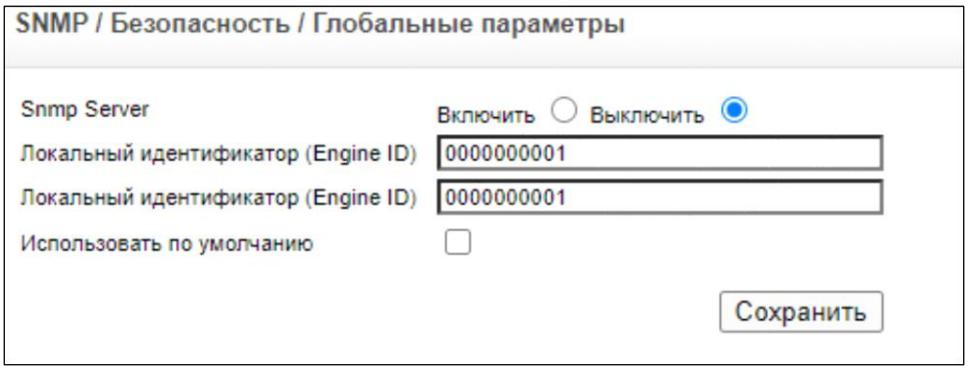
– *Управление ключами* (определяется создание, обновление и использование ключей).

2.3.1 Настройка безопасности

В этом разделе приводится информация о настройках безопасности при работе устройства по протоколу SNMP.

2.3.1.1 Настройка глобальных параметров

В разделе **SNMP → Безопасность → Глобальные параметры** устанавливается идентификатор локального SNMP-устройства.

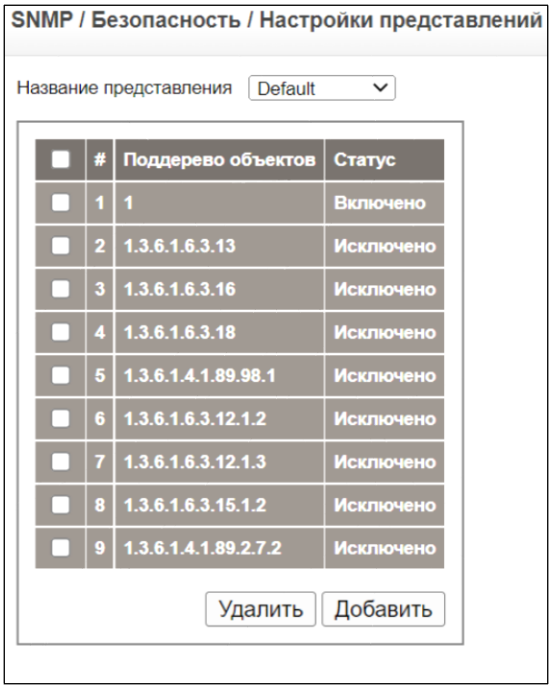


– *SNMP Server* — включить или выключить SNMP-сервер;
– *Локальный идентификатор (Engine ID)* — идентификатор локального SNMP-устройства представляет собой строку из 10–64 шестнадцатеричных символов. Если идентификатор не указан, то устанавливается значение по умолчанию на основе MAC-адреса устройства;
– *Использовать по умолчанию* — при установленном флаге используется значение по умолча–нию, иначе — значение, установленное в поле «Локальный идентификатор (Engine ID)».

Нажмите кнопку «Сохранить» для применений текущей конфигурации.

2.3.1.2 Определение объектов OID

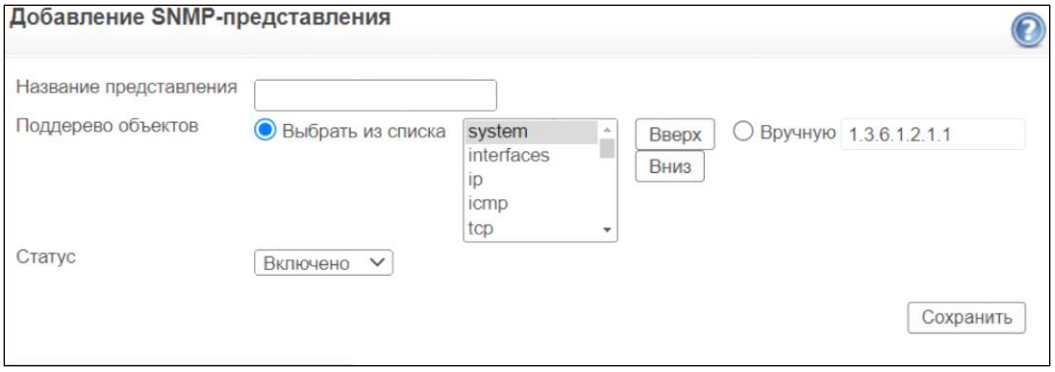
В разделе **SNMP → Безопасность → Настройки представлений** определяются объекты, доступные сообществу.



Описание таблицы:

- *Название представления* — имя для правила обозрения SNMP;
- *Поддерево объектов* — идентификатор объекта MIB, представленный в виде дерева ASN.1;
- *Статус* — указывает, является ли определенная ветвь OID включенной в правило фильтрации.

Для добавления записи нажмите кнопку «Добавить» и заполните следующие поля:



- *Название представления* — имя для правила обозрения SNMP, максимальная длина 30 символов;
- *Поддерево объектов* — идентификатор объекта MIB:

- Если установить флаг *«Выбрать из списка»*, то в ниспадающем списке необходимо указать OID, представленный текстовой строкой. Кнопки «Вверх», «Вниз» служат для перемещения по ветвям дерева ASN.1;

- Если установить флаг «*Вручную*», то необходимо указать идентификатор объекта MIB, представленный в виде дерева ASN.1;

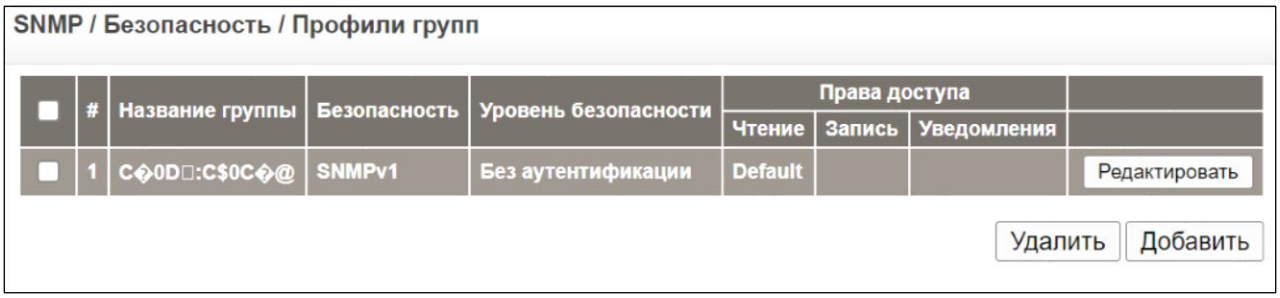
– *Статус* — указывает, является ли определенная ветвь OID включенной в выбранное правило:

- *Включено* — OID включена в правило для обозревания;
- *Исключено* — OID исключена из правила для обозревания.

Нажмите кнопку «Сохранить» для применения изменений. Для удаления записи из таблицы установите флаг напротив заданной записи и нажмите кнопку «Удалить».

2.3.1.3 Управление группами SNMP

В разделе **SNMP → Безопасность → Профили групп** осуществляется просмотр и настройка групп SNMP. Группам SNMP можно назначить версию протокола, уровень безопасности и права доступа.



Описание таблицы:

– *Название группы* — имя группы;

– *Безопасность* — версия протокола SNMP;

– *Уровень безопасности* — уровень безопасности;

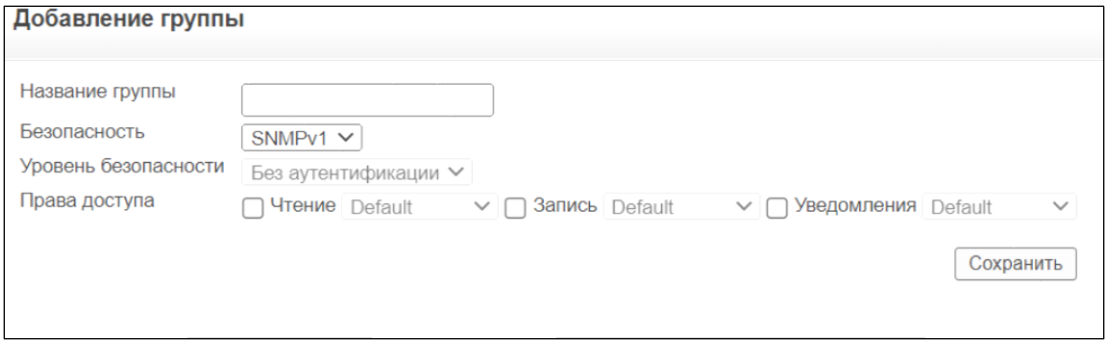
– *Права доступа* — права доступа:

- *Чтение* — только чтение;
- *Запись* — только чтение и запись;
- *Уведомления* — получение рассылки snmp-трапов.

Для редактирования параметров нажмите кнопку «Редактировать», заполните соответствующие поля и нажмите кнопку «Сохранить».

Для удаления записи из таблицы установите флаг напротив заданной записи и нажмите кнопку «Удалить».

Для добавления записи нажмите кнопку «Добавить» и заполните следующие поля:

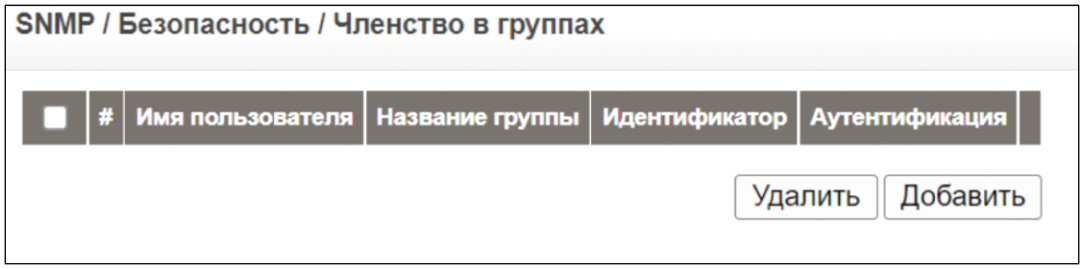


– *Название группы* — имя группы, которое используется при определении правил контроля доступа, максимальная длина — 30 символов;
– *Безопасность* — версия SNMP, используемая данной группой: SNMPv1, SNMPv2c, SNMPv3;
– *Уровень безопасности* — уровень безопасности для заданной группы. Уровень безопасности применяется только для версии протокола SNMPv3:
  - *Без аутентификации* — аутентификация пользователя и шифрование SNMP-сообще–ний отключены;
  - *Аутентификация* — аутентификация пользователя без шифрования;
  - *Шифрование* — аутентификация пользователя с шифрованием SNMP-сообщений;
– *Права доступа* — права доступа:
  - *Чтение* — только чтение;
  - *Запись* — только чтение и запись;
  - *Уведомления* — получение рассылки snmp-трапов.

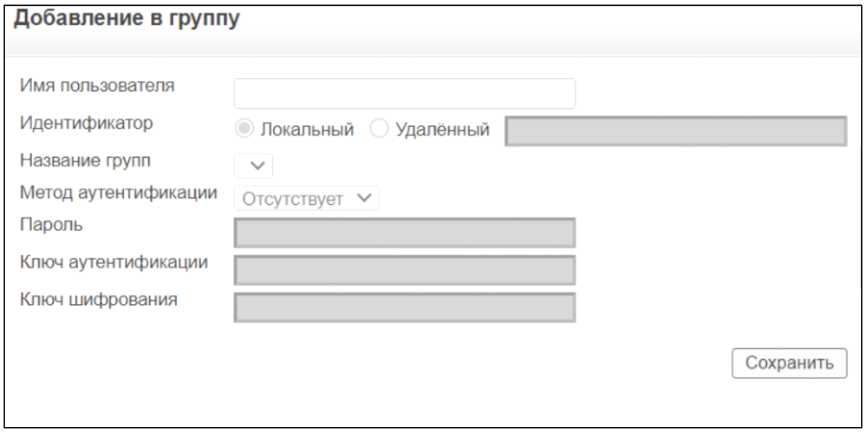
Нажмите кнопку «Сохранить» для применения изменений.

2.3.1.4 Настройка SNMP-пользователей

В разделе **SNMP → Безопасность → Членство в группах** устанавливается принадлежность пользователя к группе, задается метод аутентификации, определяется пароль/ключ аутентификации.



Для редактирования параметров нажмите кнопку «Редактировать». Для добавления записи нажмите кнопку «Добавить»:



– *Имя пользователя* — имя пользователя, максимальная длина — 30 символов;

– *Идентификатор* — идентификатор локального, либо удаленного SNMP-устройства, к которому подключен пользователь. Изменение или удаление локального идентификатора SNMP-устройства приведет к удалению пользователя SNMPv3 из базы данных:

  - *Локальный* — если флаг установлен, то пользователь подключен к локальному SNMP-объекту;
  - *Удаленный* — если флаг установлен, то пользователь подключен к удаленному SNMP-объекту. Если идентификатор SNMP-устройства определен, то удаленные устройства получат сообщение;

– *Название групп* — имя SNMP-группы;

– *Метод аутентификации* — метод, используемый для аутентификации пользователя:

  - *Ключ MD5* — по алгоритму HMAC-MD5;
  - *Ключ SHA* — с использованием уровня проверки подлинности HMAC-SHA-96;
  - *Пароль MD5* — пароль для идентификации HMAC-MD5-96, пользователь должен будет ввести пароль;
  - *Пароль SHA* — пароль для идентификации HMAC-SHA-96, пользователь должен будет ввести пароль;
  - *Отсутствует* — аутентификация не используется;

– *Пароль* — пароль для участников группы;

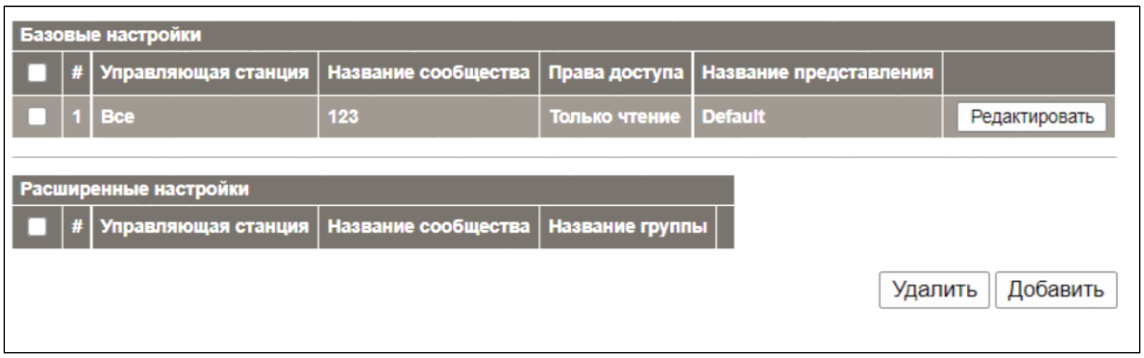
– *Ключ аутентификации* — ключ аутентификации, задается только при проверке подлинности HMAC-MD5-96 или HMAC-SHA-96. Ключи идентификации и конфиденциальности необходимы для определения подлинности ключа. Если необходима только проверка подлинности, то определяется 16 байт. Если необходима аутентификация и шифрование, то определяется 32 байта. Каждый байт в шестнадцатеричной строке состоит из 2 шестнадцатеричных цифр. Каждый байт должен быть отделен точкой или двоеточием;

– *Ключ шифрования* — ключ конфиденциальности (LSB). Если необходима только проверка подлинности, то определяется 20 байт. Если необходима аутентификация и шифрование, то определяется 36 байт. Каждый байт в шестнадцатеричной строке состоит из 2 шестнадцатеричных цифр. Каждый байт должен быть отделен точкой или двоеточием.

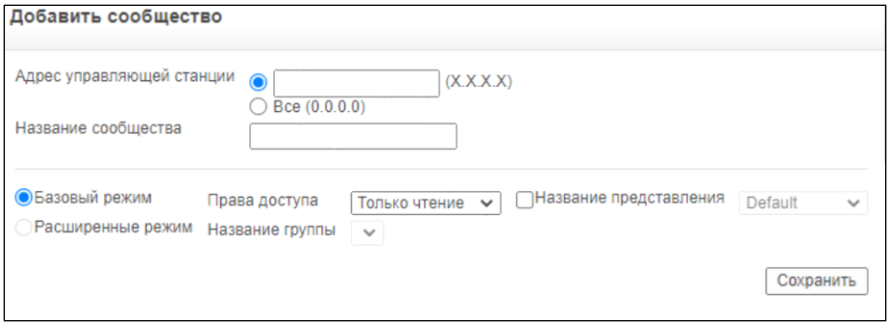
Нажмите кнопку «Сохранить» для применения изменений.

2.3.1.5 Настройка SNMP-сообществ

В разделе **SNMP → Безопасность → Настройки сообществ** выполняется настройка прав доступа на основе сообществ. Если изменить имена сообществ, то изменятся права доступа. Сообщества SNMP определяются только для SNMP v1 и SNMP v2c. Страница настроек разделена на две таблицы: базовые настройки и расширенные настройки.



Для добавления записи нажмите кнопку «Добавить». Для удаления записи установите флаг напротив соответствующей записи и нажмите кнопку «Удалить». Для редактирования записи нажмите кнопку «Редактировать».



– *Адрес управляющей станции* — IP-адрес управляющей станции, для которой определяются настройки сообщества;

– *Название сообщества* — строка сообщества (пароль), которая используется для аутентифи–кации управляющей станции.

Если запись добавляется в основную таблицу, то нужно установить флаг «Базовый режим» и заполнить следующие поля:

– *Права доступа* — права доступа сообщества:

  - *Только чтение* — управление ограниченным доступом, разрешено только чтение;
  - *Чтение/запись* — управление доступом для чтения и записи. Изменения могут быть внесены в конфигурацию устройства, но не в настройки сообщества;
  - *Администратор* — пользователь имеет доступ ко всем настройкам устройства, а также может изменить настройки сообщества;

– *Название представления* — имя для правила обозрения SNMP.

Если запись добавляется в расширенную таблицу, то нужно установить флаг «Расширенный режим» и заполнить следующие поля:

– *Название группы* — имя группы SNMP-сообщества.

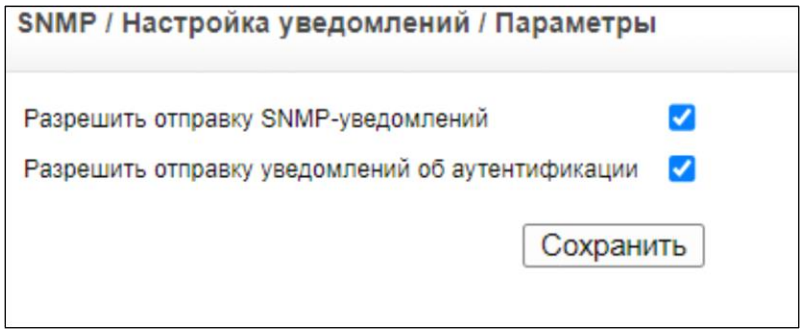
Нажмите кнопку «Сохранить» для применения изменений.

2.3.2 Управление SNMP-сообщениями

В этом разделе приводится информация о настройках уведомлений при работе устройства по протоколу SNMP.

2.3.2.1 Настройка основных параметров

В разделе **SNMP → Настройка уведомлений → Параметры** устанавливаются общие параметры для SNMP-сообщений.



– *Разрешить отправку SNMP-уведомлений* — при установленном флаге устройству разрешена отправка SNMP-сообщений, иначе — запрещена;

– *Разрешить отправку уведомлений об аутентификации* — при установленном флаге разре–шено передавать trap-сообщения серверу, непрошедшему аутентификацию.

Нажмите кнопку «Сохранить» для применения изменений.

2.3.2.2 Настройка адресатов SNMP-сообщений

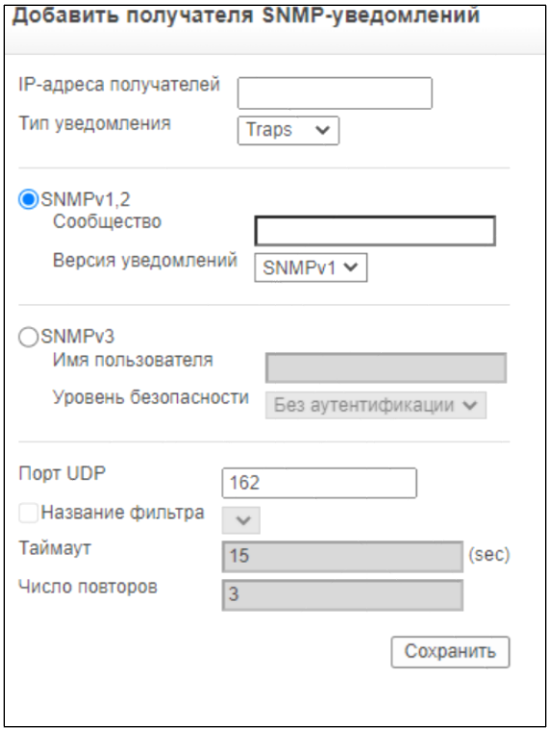
В разделе **SNMP → Настройка уведомлений → Прием уведомлений** устанавливаются правила фильтрации сообщений SNMP при отправке определенным получателям и задается тип сообщений.

Страница настроек разделена на две таблицы: настройка параметров для получателя уведомлений по протоколу SNMPv1,2 (SNMPv1,2 Notification Recipient) и по протоколу SNMPv3 (SNMPv3 Notification Recipient).

Для редактирования параметров нужно нажать кнопку «Редактировать», заполнить соответствующие поля и нажать кнопку «Сохранить».

Для удаления записи из таблицы нужно установить флаг напротив заданной записи и нажать кнопку «Удалить».

Для добавления записи нужно нажать кнопку «Добавить» и заполнить следующие поля:



– *IP-адреса получателей* — IP-адрес, на который отправляются сообщения;
– *Тип уведомления* — тип отправляемых сообщений:
  - *Traps* — trap-сообщения,
  - *Informs* — информационные сообщения.

Если отправка сообщений осуществляется по протоколу SNMPv1 или SNMPv2, установите флаг SNMPv1,2 и заполните следующие поля:

– *Сообщество* — строка сообщества (пароль), отправляемая вместе с trap-сообщениями;
– *Версия уведомлений* — тип протокола SNMP, по которому отправляются сообщения: SNMPv1, SNMPv2c;

Если отправка сообщений осуществляется по протоколу SNMPv3, установите флаг SNMPv3 и заполните следующие поля:

– *Имя пользователя* — имя пользователя, которому отправляются SNMP-сообщения;
– *Уровень безопасности* — уровень безопасности:
  - *Без аутентификации* — пакет не проходит аутентификацию, не защищен шифро–ванием;
  - *Аутентификация* — пакет проходит аутентификацию;
– *Порт UDP* — номер UDP-порта, который используется для отправки сообщений. По умолчанию установлен 162 порт;
– *Название фильтра* — при установке флага указывается имя SNMP-фильтра, который используется при отправке SNMP-сообщений;

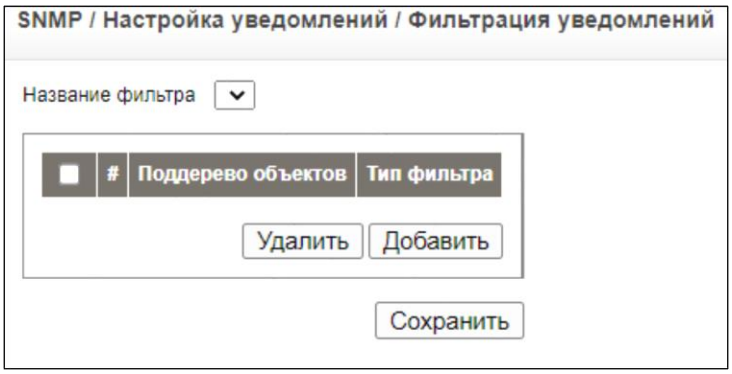
– *Таймаут* — период времени (в секундах), в течение которого устройство ожидает подтверж–дения перед повторной отправкой SNMP-сообщения. По умолчанию установлено 15 секунд;

– *Число повторов* — количество попыток передачи информационных сообщений, при отсутствии их подтверждения. По умолчанию установлено 3 секунды.

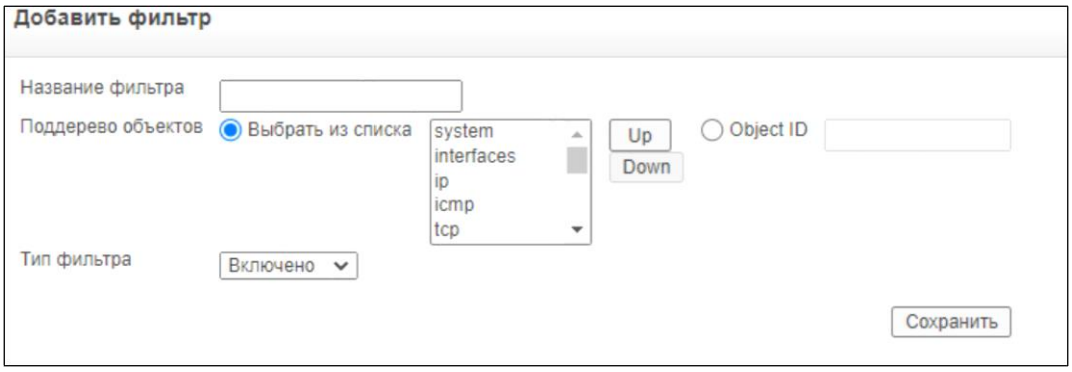
Нажмите кнопку «Сохранить» для применения изменений.

2.3.2.3 Настройка правил фильтрации trap-сообщений

В разделе **SNMP → Настройка уведомлений → Фильтрация уведомлений** устанавливаются правила фильтрации сообщений, основанные на OID. Это позволяет сетевым администраторам фильтровать оповещения. Каждый OID связан с функциями устройства или с частью функции.



Для добавления нового правила фильтрации нажмите кнопку «Добавить» и заполните следующие поля:



– *Название фильтра* — имя фильтра;

– *Поддерево объектов* — OID, который настроен для данного фильтра. Если фильтр прикреплен к OID, trap-сообщения или информационные сообщения формируются и отправляются к получателю трапов:

  - Если установить флаг *«Выбрать из списка»*, то в ниспадающем списке необходимо указать OID, представленный текстовой сорокой. Кнопки «UP», «Down» служат для перемещения по ветвям дерева ASN.1;

  - Если установить флаг «Object ID», то необходимо указать идентификатор объекта MIB, представленный в виде дерева ASN.1;

– *Тип фильтра* — указывает, следует ли отправлять сообщения, связанные с заданным OID:

  - *Включено* — включить отправку сообщений. Устанавливается по умолчанию;
  - *Исключено* — отключить отправку сообщений.

Для удаления правил фильтрации установите флаг напротив заданной записи и нажмите кнопку «Удалить».

Нажмите кнопку «Сохранить» для применения изменений.

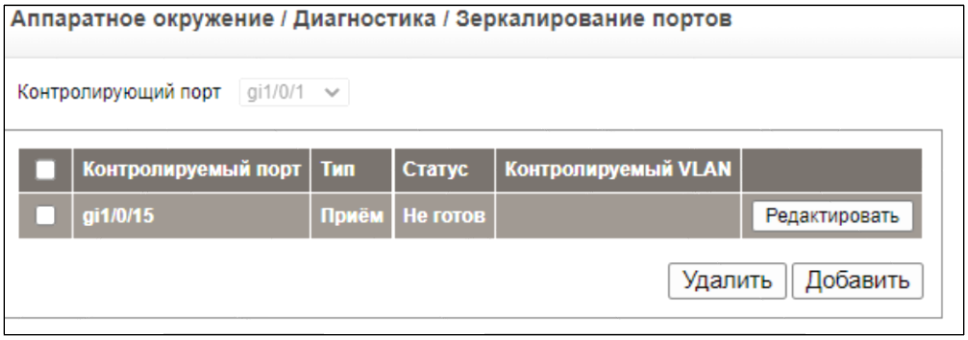
2.4 Диагностика устройства на физическом уровне

В данной главе описывается настройка диагностики устройства на физическом уровне, включая настройку зеркалирования сетевого трафика и тестирования портов.

2.4.1 Настройка зеркалирования сетевого трафика

В разделе **Аппаратное окружение → Диагностика → Зеркалирование портов** выполняется настройка зеркалирования входящего/исходящего трафика.

Зеркалирование трафика — это функция коммутатора, которая позволяет копировать трафик, проходящий через какой-либо из портов устройства, для внешнего анализа.



Описание таблицы зеркалирования трафика:

– *Контролирующий порт* — номер порта, на который копируется трафик;

– *Контролируемый порт* — номер порта, с которого копируется трафик;

– *Тип* — тип копируемого трафика:

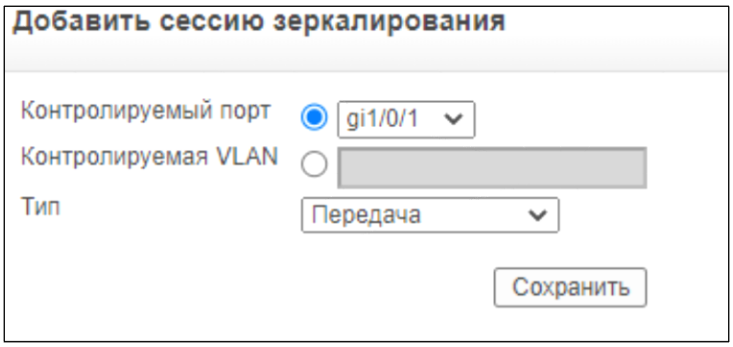
  - *Приём* — входящий трафик;
  - *Передача* — исходящий трафик;
  - *Приём и передача* — весь трафик, установлено по умолчанию;

– *Статус* — текущее состояние мониторинга для заданного порта:

  - *Активный* — мониторинг включен;
  - *Не готов* — мониторинг не активен.

Для настройки зеркалирования трафика нужно в поле «*Контролирующий порт*» указать номер порта, на который будет копироваться трафик. Далее нужно задать список портов, с которых будет копироваться трафик и тип трафика.

Для добавления порта в список нажмите кнопку «Добавить» и заполните следующие поля:



– *Контролируемый порт* — номер порта, с которого зеркалируется трафик;

– *Контролируемая VLAN* — номер влана, с которого зеркалируется трафик;

– *Тип* — тип трафика:

  - *Приём* — входящий трафик;
  - *Передача* — исходящий трафик;
  - *Приём и передача* — весь трафик, установлено по умолчанию.

Для редактирования записи таблицы «Зеркалирование портов» установите флаг напротив заданной записи, нажмите кнопку «Редактировать», заполните соответствующие поля и нажмите кнопку «Сохранить» для сохранения настроек.

Для удаления записи из таблицы установите флаг напротив заданной записи и нажмите кнопку «Удалить».

Нажмите кнопку «Сохранить» для применения изменений.

2.4.2 Диагностика медного кабеля

Раздел **Аппаратное окружение → Диагностика → Диагностика кабеля** предназначен для тестирования медных кабелей. Тестирование кабелей предоставляет информацию о том, в каком состоянии находится кабель и где находится проблемный участок. При тестировании используется рефлектометрический метод (TDR). Максимальная длина тестируемого кабеля составляет 100 метров.

При тестировании кабеля порт переходит в нерабочее состояние.

Аппаратное окружение / Диагностика / Диагностика кабеля

Порт	Результат теста	Расстояние до неисправности	Последний тест		Длина кабеля	
gi1/0/1				Тест		Дополнительно
gi1/0/2				Тест		Дополнительно
gi1/0/3				Тест		Дополнительно
gi1/0/4				Тест		Дополнительно
gi1/0/5				Тест		Дополнительно
gi1/0/6				Тест		Дополнительно
gi1/0/7				Тест		Дополнительно
gi1/0/8				Тест		Дополнительно
gi1/0/9				Тест		Дополнительно
gi1/0/10				Тест		Дополнительно
gi1/0/11				Тест		Дополнительно
gi1/0/12				Тест		Дополнительно
gi1/0/13				Тест		Дополнительно
gi1/0/14				Тест		Дополнительно
gi1/0/15				Тест		Дополнительно
gi1/0/16				Тест		Дополнительно
gi1/0/17				Тест		Дополнительно
gi1/0/18				Тест		Дополнительно
gi1/0/19				Тест		Дополнительно
gi1/0/20				Тест		Дополнительно
gi1/0/21				Тест		Дополнительно
gi1/0/22				Тест		Дополнительно
gi1/0/23				Тест		Дополнительно
gi1/0/24				Тест		Дополнительно

– *Порт* — номер порта, с которым соединен кабель;

– *Результат теста* — результаты тестирования кабеля:

  - *Нет кабеля* — кабель не подключен к порту;
  - *Обрыв* — кабель подключен, но только на одной стороне (обрыв);
  - *Короткое замыкание* — в кабеле произошло короткое замыкание;
  - *Успех* — кабель прошёл тестирование;

– *Расстояние до неисправности* — расстояние от порта до места где была обнаружена проб–лема в кабеле;

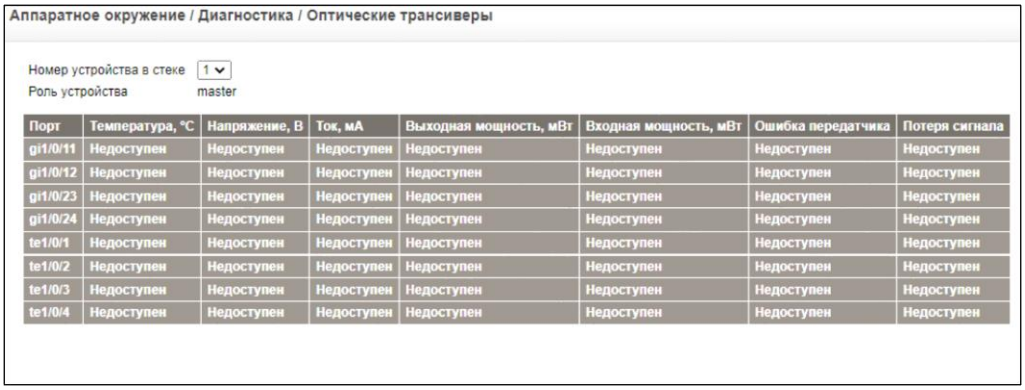
– *Последний тест* — время последнего тестирования кабеля;

– *Длина кабеля* — предположительная длина кабеля. Эта проверка может быть выполнена только, когда порт включен и работает на скорости 1 Гбит/с.

Для начала тестирования кабеля нажмите кнопку «Тест». Для просмотра результатов тестирования нажмите кнопку «Дополнительно».

2.4.3 Диагностика оптических трансиверов

Раздел **Аппаратное окружение → Диагностика → Оптические трансиверы** позволяет администратору сети выполнять тестирование оптических трансиверов. Диагностика оптического трансивера может быть выполнена только при подключенной линии связи и только для трансиверов, поддерживающих функцию диагностики DDM (Digital Diagnostics Monitoring).



Порт	Температура, °C	Напряжение, В	Ток, мА	Выходная мощность, мВт	Входная мощность, мВт	Ошибка передатчика	Потеря сигнала
gi1/0/11	Недоступен	Недоступен	Недоступен	Недоступен	Недоступен	Недоступен	Недоступен
gi1/0/12	Недоступен	Недоступен	Недоступен	Недоступен	Недоступен	Недоступен	Недоступен
gi1/0/23	Недоступен	Недоступен	Недоступен	Недоступен	Недоступен	Недоступен	Недоступен
gi1/0/24	Недоступен	Недоступен	Недоступен	Недоступен	Недоступен	Недоступен	Недоступен
te1/0/1	Недоступен	Недоступен	Недоступен	Недоступен	Недоступен	Недоступен	Недоступен
te1/0/2	Недоступен	Недоступен	Недоступен	Недоступен	Недоступен	Недоступен	Недоступен
te1/0/3	Недоступен	Недоступен	Недоступен	Недоступен	Недоступен	Недоступен	Недоступен
te1/0/4	Недоступен	Недоступен	Недоступен	Недоступен	Недоступен	Недоступен	Недоступен

Описание полей таблицы:

– *Номер устройства в стеке* — выбор номера устройства в стеке;

– *Роль устройства* — роль устройства в стеке:

  - *Master (UID устройства от 1 до 8)* — с него происходит управление всеми устройствами в стеке. Роль можно назначить всем устройствам, но активный master при этом будет один, остальные будут функционировать в роли Backup;
  - Backup (UID устройства от 1 до 8) — устройство, подчиняющееся master. Дублирует все настройки, и, в случае выхода управляющего устройства из строя, берет на себя функции управления стеком. Роль можно назначить максимум семи устройствам;
  - Slave (UID устройства от 1 до 8) — устройство, подчиняющееся master. Не может работать в автономном режиме (если отсутствует master). Роль можно назначить максимум шести устройствам. Допустима корректная работа стека без устройств с данной ролью;

– *Порт* — номер порта, на котором производится тестирование;

– *Температура, ^{0}C* — рабочая температура трансивера, ^{0}C;

– *Напряжение, В* — напряжение питание трансивера;

– *Ток, мА* — ток питания передатчика;

– *Выходная мощность, мВт* — выходная мощность на передаче;

– *Входная мощность, мВт* — входная мощность на приеме;

– *Ошибка передатчика* — индикация аварии передатчика;

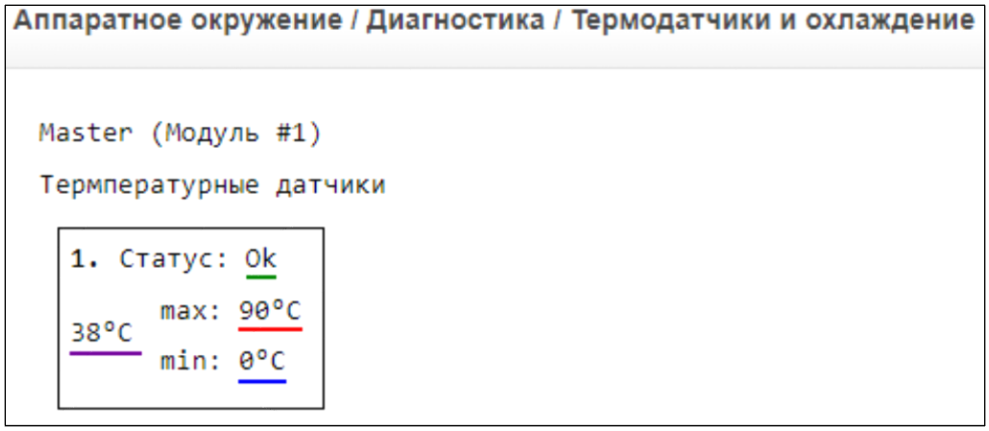
– *Потеря сигнала* — потеря сигнала в кабеле.

Возможные значения полей таблицы:

- *Недоступен* — информация о параметре не доступна;
- *Не поддерживается* — диагностика параметра не поддерживается оборудованием;
- *Предупреждение* — возникло предупреждение;
- *Ошибка* — возникла ошибка.

2.4.4 Мониторинг температуры

В разделе **Аппаратное окружение → Диагностика → Термодатчики и охлаждение** осуществляется мониторинг состояния температуры на коммутаторе.



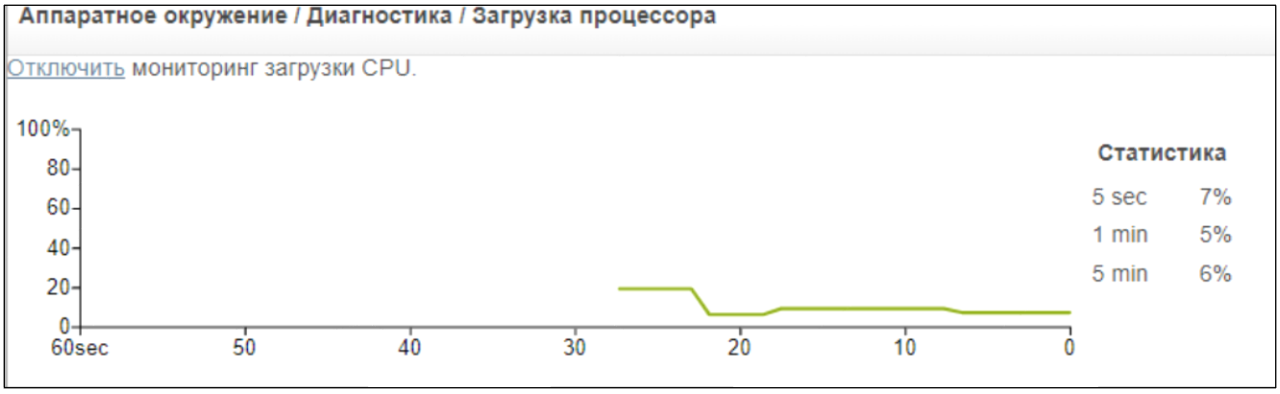
– *Температурные датчики* — состояние и текущие показания датчиков температуры.

– *Статус* — состояние и текущие показания датчиков температуры:

  - *ok* — датчик работает;
  - *not operational* — датчик не в работе.

2.4.5 Мониторинг текущей загрузки процессора

В разделе **Аппаратное окружение → Диагностика → Загрузка процессора** осуществляется просмотр загрузки процессора в процентном отношении за последние 5 секунд /1 минуту/5 минут, а также строится график зависимости загрузки процессора от текущего времени.



2.4.6 Мониторинг портов

В разделе **Аппаратное окружение → Диагностика → Состояние портов** осуществляется просмотр состояния портов.

– *Не подключен* — порт выключен;

– *В стеке* — порт находится в режиме стекирования;

– *Активный* — порт включен;

Служебные статусы портов: Ошибка, Инициализация / Тестирование, Резервный.

2.5 Управление безопасностью устройства

В данной главе описывается настройка параметров безопасности для портов устройства, методы управления устройством, пользователями и сервером аутентификации.

2.5.1 Настройка учетной записи

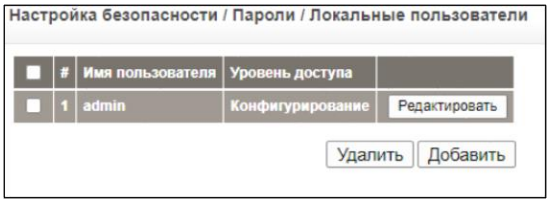
В разделе **Настройка безопасности → Пароли** осуществляется управление учетными записями пользователей:

– Настройка учетной записи пользователя (Локальные пользователи);
– Определение паролей для доступа к терминалу (Интерфейсы управления);
– Установка пароля для контроля изменения привилегий доступа пользователей (Привилегированный режим).

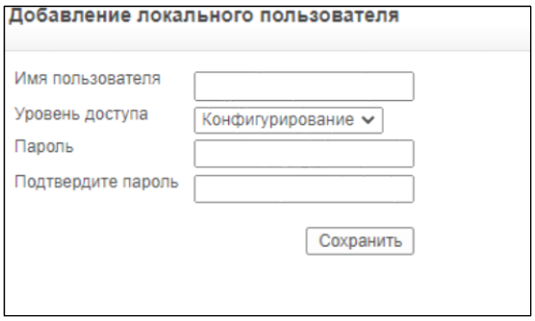
2.5.1.1 Настройка учетной записи пользователя

В разделе **Настройка безопасности → Пароли → Локальные пользователи** выполняется установка параметров для нового пользователя системы или изменение конфигурации уже существующего пользователя: имя пользователя, пароль, уровень привилегий.

Для привилегированного пользователя с именем «admin» можно изменить только пароль.



Для добавления нового пользователя в систему нажмите кнопку «Добавить» и заполните следующие поля:



– *Имя пользователя* — имя пользователя;
– *Уровень доступа* — уровень доступа пользователя:
  - *Конфигурирование* — пользователю разрешены конфигурирование и мониторинг устройства;
  - *Мониторинг* — пользователю разрешен только мониторинг устройства;
– *Пароль* — пароль пользователя, максимальная длина — 159 символов;

– *Подтвердите пароль* — подтверждение пароля.

Нажмите кнопку «Сохранить» для применения настроек.

Для редактирования учетной записи пользователя установите флаг напротив заданной записи, нажмите кнопку «Редактировать» и заполните соответствующие поля. После выполнения настроек нажмите кнопку «Сохранить» для применения настроек.

Для удаления пользователя установите флаг напротив заданной записи, нажмите кнопку «Удалить» и кнопку «Сохранить» для применения настроек.

2.5.1.2 Определение паролей для доступа к терминалу

Раздел **Настройка безопасности → Пароли → Интерфейсы управления** позволяет администратору сети задать пароли для доступа к устройству через консоль (подключение через серийный порт), Telnet, SSH.

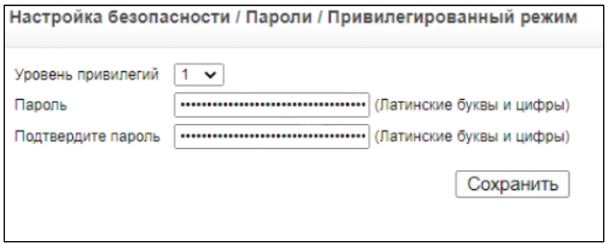
Во избежание несанкционированного доступа к устройству рекомендуется установить пароль для доступа к устройству через консоль, Telnet и SSH. По умолчанию пароль не установлен.

– *Пароль для сеанса консоли* — пароль, при подключении к устройству через сеанс консоли, максимальная длина — 159 символов;
– *Пароль для сеанса Telnet* — пароль, при подключении к устройству через сеанс Telnet, максимальная длина — 159 символов;
– *Пароль для сеанса SSH* — пароль, при подключении к устройству через защищенный сеанс SSH, максимальная длина — 159 символов;
– *Подтвердите пароль* — подтверждение пароля.

Нажмите кнопку «Сохранить» для применения настроек.

2.5.1.3 Определение пароля для смены уровня доступа

В разделе **Настройка безопасности → Пароли → Привилегированный режим** выполняется установка пароля для контроля изменения привилегий доступа пользователей в системе.



– *Уровень привилегий* — уровень доступа, для которого устанавливается пароль, принимает значения (1–15);

– *Пароль* — пароль пользователя;

– *Подтвердите пароль* — подтверждение пароля.

Нажмите кнопку «Сохранить» для применения настроек.

2.5.2 Настройка механизма аутентитификации

В разделе **Настройка безопасности → Аутентификация** выполняется настройка аутентификации, которая включает в себя:

– настройку профилей аутентификации;

– настройку метода аутентификации при доступе через консоль, Telnet, SSH, HTTP, HTTPS;

– настройку параметров сервера TACACS+, RADIUS.

2.5.2.1 Настройка профилей аутентификации

В разделе **Настройка безопасности → Аутентификация → Профили аутентификации** выполняется настройка профилей аутентификации пользователей при входе в систему.

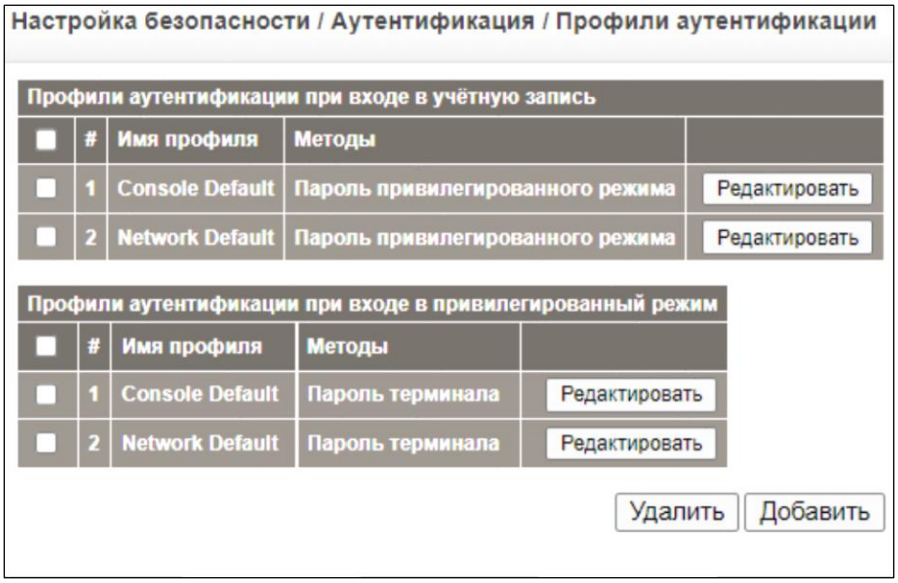
Пройти аутентификацию пользователь может локально или через внешний сервер аутентификации:

– при локальной аутентификации, используются учетные записи, которые настроены на устройстве (см. раздел 2.5.1);

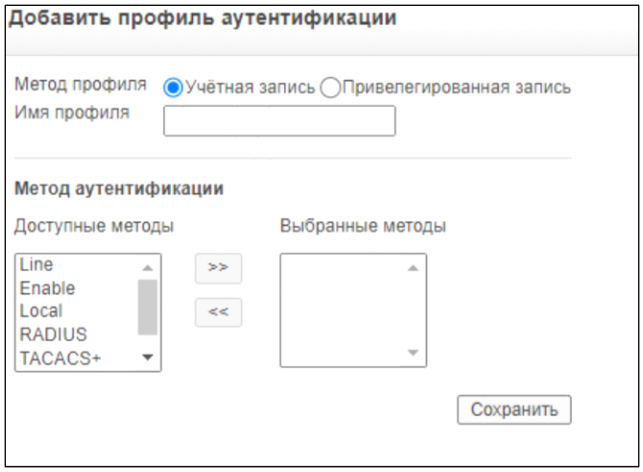
– при внешней аутентификации, используется либо аутентификация на TACACS-сервере, либо на RADIUS-сервере. Это целесообразно, когда аутентификацию необходимо проходить большому количеству пользователей.

Выбор метода аутентификации происходит согласно установленным настройкам в профиле аутентификации. Можно указать несколько методов аутентификации, в этом случае если подлинность пользователя не подтверждена при первом методе проверки, то выбирается следующий метод по списку.

Страница настроек разделена на две таблицы: таблица профилей аутентификации при входе в систему (Профили аутентификации при входе в учетную запись) и таблица профилей аутентификации при повышении уровня привилегий для входа в систему (Профили аутентификации при входе в привилегированный режим).



Для добавления нового профиля аутентификации нажмите кнопку «Добавить» и заполните следующие поля:



– *Метод профиля* — выбор списка для профиля аутентификации:

  - *Учетная запись* — при установленном флаге будет создан профиль аутентификации для входа в систему;

  - *Привилегированная запись* — при установленном флаге будет создан профиль для входа в систему при повышении уровня привилегий;

– *Имя профиля* — имя профиля аутентификации;

– *Метод аутентификации* — метод аутентификации:

  - *None* — не использовать аутентификацию;
  - *Local* — использовать локальную базу учетных записей;
  - *RADIUS* — использовать аутентификацию на RADIUS-сервере (подробная информация о настройках RADIUS-сервера приведена в разделе 2.5.2.4);
  - *TACACS+* — использовать аутентификацию на TACACS-сервере (подробная информация о настройках TACACS-сервера приведена в разделе 2.5.2.3);
  - *Line* — использовать пароль терминала для аутентификации;
  - *Enable* — использовать пароль для аутентификации.

Способ аутентификации выбирается с помощью стрелок

. Метод аутентификации используется в том порядке, в котором был установлен.

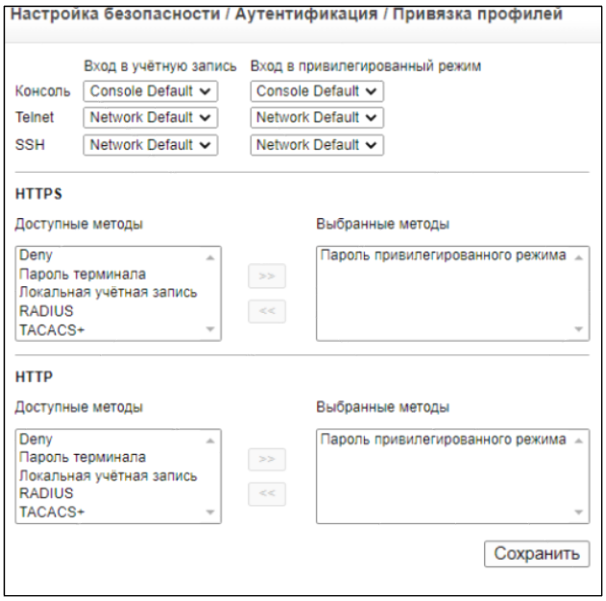
Нажать кнопку «Сохранить» для применения настроек.

Для редактирования профиля аутентификации нужно нажать кнопку «Редактировать» напротив заданной записи, заполнить соответствующие поля и нажать кнопку «Сохранить» для применения настроек.

Для удаления профиля аутентификации нужно установить флаг напротив заданной записи, нажать кнопку «Удалить» и кнопку «Сохранить» для применения настроек.

2.5.2.2 *Настройка метода аутентификации при доступе через консоль, Telnet, SSH, HTTP, HTTPS*

В разделе **Настройка безопасности → Аутентификация → Привязка профилей** выполняется настройка метода аутентификации при доступе к устройству через консоль, Telnet, SSH, HTTP, HTTPS.



– *Консоль* — профиль аутентификации, который будет использоваться при доступе к устройству через консоль;

– *Telnet* — профиль аутентификации, который будет использоваться при доступе к устройству через Telnet;

– *Secure Telnet (SSH)* — профиль аутентификации, который будет использоваться при доступе к устройству через SSH;

– *Secure HTTP* — метод аутентификации при доступе к устройству по протоколу HTTPS;

– *HTTP* — метод аутентификации при доступе к устройству по протоколу HTTP.

Протоколы HTTP и HTTPS могут использовать следующие методы аутентификации:

- *Без аутентификации* — не использовать аутентификацию;
- *Локальная учетная запись* — использовать локальную базу учетных записей;
- *RADIUS* — использовать аутентификацию на RADIUS-сервере (подробная информация о настройках RADIUS-сервера приведена в разделе 2.5.2.4);
- *TACACS+* — использовать аутентификацию на TACACS-сервере (подробная информация о настройках TACACS-сервера приведена в разделе 2.5.2.3).

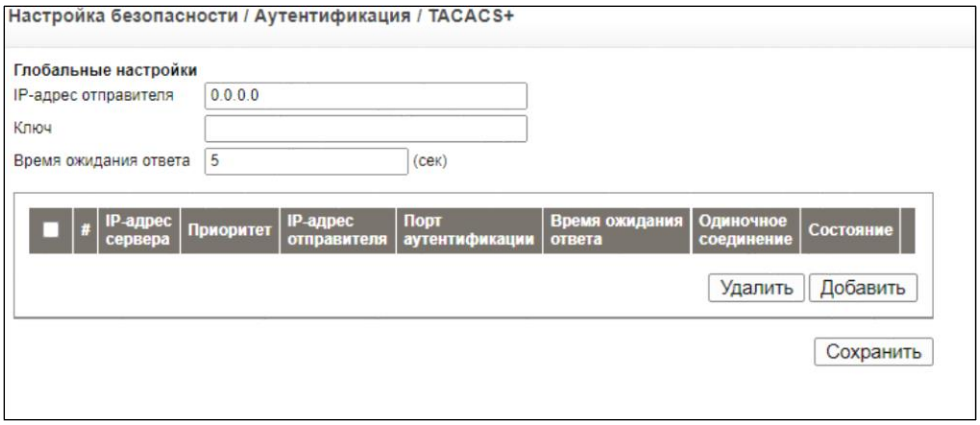
Способ аутентификации выбирается с помощью стрелок . Метод аутентификации используется в том порядке, в котором был установлен.

Нажамите кнопку «Сохранить» для применения настроек.

2.5.2.3 Настройка параметров сервера TACACS+

В разделе **Настройка безопасности → Аутентификация → TACACS+** выполняется настройка параметров TACACS-сервера.

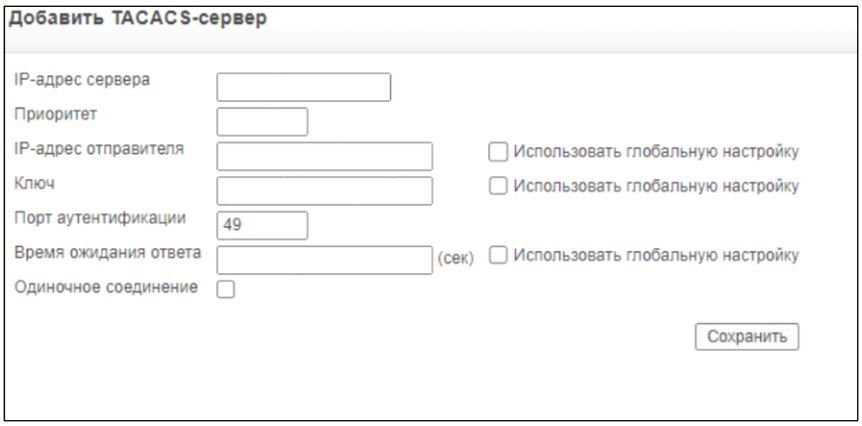
Terminal Access Controller Access Control System (TACACS+) обеспечивает централизованную защиту при проверке пользователя, получающего доступ к устройству, и гарантирует безопасность сети благодаря шифрованию передаваемых данных.



В разделе «*Глобальные настройки*» устанавливаются параметры по умолчанию для сервера TACACS+:

- *IP-адрес отправителя* — IP-адрес, используемый в качестве адреса источника, передаваемого в сообщениях протокола TACACS;
- *Ключ* — ключ для аутентификации и шифрования данных, передаваемых по протоколу TACACS+;
- *Время ожидания ответа* — время ожидания ответа от сервера, по умолчанию — 5 секунд.

Для добавления сервера TACACS+ в список используемых серверов нажмите на кнопку «Добавить» и заполните следующие поля:



- *IP-адрес сервера* — IP-адрес сервера TACACS+;
- *Приоритет* — порядок, в котором будет использоваться данный сервер (0–65535). По умолчанию установлено значение «0». Чем ниже значение, тем выше приоритет сервера;

– *IP-адрес отправителя* — IP-адрес, используемый в качестве адреса источника, передаваемого в сообщениях протокола TACACS. При установке флага «Use Default» будет использоваться значение по умолчанию;

– *Ключ* — ключ для аутентификации и шифрования данных, передаваемых по протоколу TACACS+, (1–128) символов. Этот ключ должен соответствовать шифрованию, которое используется на сервере TACACS+. При установке флага «Use Default» будет использоваться значение по умолчанию;

– *Порт аутентификации* — номер порта для соединения и обмена данными с TACACS+ сервером (0–65535). По умолчанию номер порта 49;

– *Время ожидания ответа* — время ожидания ответа от сервера, (1–1000) секунд. При установке флага «Use Default» будет использоваться значение по умолчанию;

– *Одиночное соединение* — при установленном флаге в каждый момент времени может быть установлено не больше одного соединения для обмена данными с TACACS-сервером.

Нажмите кнопку «Сохранить» для применения настроек.

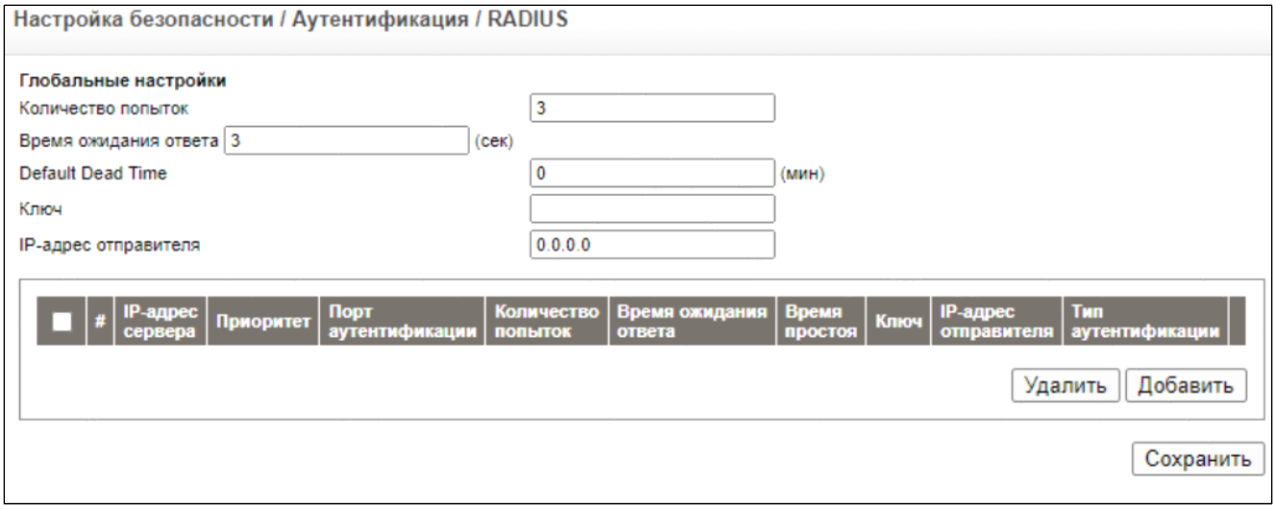
Для изменения настроек сервера TACACS+ нужно установить флаг напротив заданной записи, нажать кнопку «Редактировать» и заполнить соответствующие поля. Для применения настроек нажмите кнопку «Сохранить».

Для удаления сервера TACACS+ установите флаг напротив заданной записи, нажмите кнопку «Удалить» и кнопку «Сохранить» для применения настроек.

2.5.2.4 Настройка параметров RADIUS-сервера

В разделе **Настройка безопасности → Аутентификация → RADIUS** выполняется настройка параметров RADIUS-сервера.

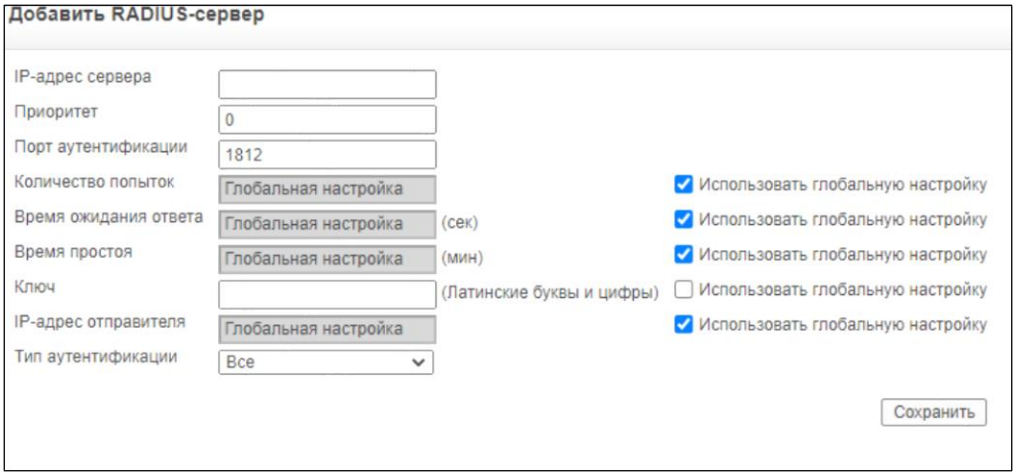
RADIUS (Remote Authorization Dial-In User Service) предоставляет собой протокол безопасности, который предоставляет централизованный метод аутентификации пользователей путем обращения к внешнему серверу.



В разделе «*Глобальные настройки*» для RADIUS-сервера устанавливаются параметры по умолчанию:

- *Количество попыток* — количество запросов, передаваемых на поиск RADIUS-сервера, (1–10). Значение по умолчанию — 3;
- *Время ожидания ответа* — интервал ожидания ответа от сервера (1–30) секунд. Значение по умолчанию — 3;
- *Default Dead Time (Время простоя)* — время, в течение которого недоступные сервера не будут опрашиваться RADIUS-клиентом коммутатора, (0–2000) минут. Значение по умолчанию — 0;
- *Ключ* — ключ для аутентификации и шифрования данных, передаваемых по протоколу RADIUS, 1–128 символов. Этот ключ должен соответствовать шифрованию, которое используется на RADIUS-сервере;
- *IP-адрес отправителя* — IP-адрес по умолчанию для доступа к RADIUS-серверу.

Для добавления новой записи нажмите кнопку «Добавить» и заполните следующие поля:



- *IP-адрес сервера* — IP-адрес RADIUS-сервера;
- *Приоритет* — приоритет использования RADIUS-сервера (1–65535). Чем ниже значение, тем выше приоритет сервера;
- *Порт аутентификации* — номер порта для передачи аутентификационных данных. Значение по умолчанию — 1812;
- *Количество попыток* — количество запросов, передаваемых на поиск RADIUS-сервера, (1–10). Значение по умолчанию — 3;
- *Время ожидания ответа* — интервал ожидания ответа от сервера (1–30) секунд. Значение по умолчанию — 3;
- *Время простоя* — время, в течение которого недоступные сервера не будут опрашиваться RADIUS-клиентом коммутатора, (0–2000) минут. Значение по умолчанию — 0;
- *Ключ* — ключ для аутентификации и шифрования данных, передаваемых по протоколу RADIUS, 1–128 символов. Этот ключ должен соответствовать шифрованию, которое используется на RADIUS-сервере;
- *IP-адрес отправителя* — IP-адрес для доступа к RADIUS-серверу;
- *Тип аутентификации* — модель аутентификации на RADIUS-сервере:
  - *Вход в учетную запись* — соответствие между именем пользователя и паролем;
  - *802.1X* — по стандарту 802.1X;
  - *Все* — соответствие между именем пользователя и паролем, а также по стандарту 802.1X.

Нажмите кнопку «Сохранить» для применения настроек.

Для изменения настроек RADIUS-сервера нужно установить флаг напротив заданной записи, нажать кнопку «Редактировать», заполнить соответствующие поля и нажать кнопку «Сохранить» для применения настроек.

Для удаления записи нужно установить флаг напротив заданной записи, нажать кнопку «Удалить» и кнопку «Сохранить» для применения настроек.

2.5.3 Способы контроля доступа для управления устройством

В данном разделе описываются способы ограничения доступа для управления устройством. Различным группам пользователей может быть назначен свой способ доступа к устройству.

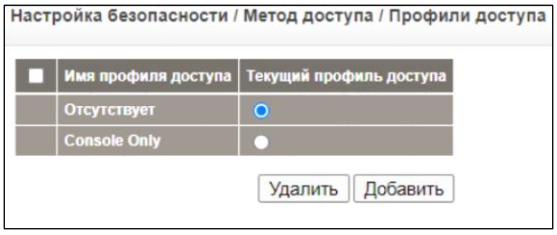
2.5.3.1 Настройка профилей контроля доступа

В разделе **Настройка безопасности → Метод доступа → Профили доступа** устанавливается способ доступа к устройству (Telnet, SSH, HTTP, HTTPS, SNMP), определяются правила фильтрации пакетов, основанные на IP-адресах пользователей/интерфейсов.

В системе по умолчанию установлено два профиля контроля доступа для управления устройством:

– *Отсутствует* — контроль доступа при подключении к устройству для его управления не используется;

– *Console Only* — управление устройством доступно только с консоли.



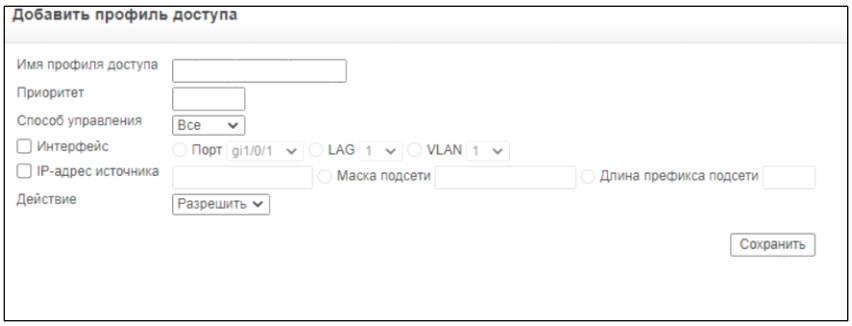
Описание таблицы профилей контроля доступа:

– *Имя профиля доступа* — имя профиля контроля доступа;

– *Текущий профиль доступа* — при установке флага профиль доступа активен, иначе — неактивен.

Профиль доступа применяется сразу после установления флага.

Для добавления новой записи нажмите кнопку «Добавить» и заполните следующие поля:



– *Имя профиля доступа* — имя профиля доступа, максимальная длина — 32 символа;

– *Приоритет* — приоритет правила. Если пакеты соответствуют правилу, то пользователь либо получит разрешение, либо ему будет отказано в доступе к управлению устройством. Правила

проверяются в возрастающем порядке по приоритетам. При совпадении правила, действие выполняется, а правила ниже игнорируются;

– *Способ управления* — способ доступа:

  - *Все* — доступ к устройству любым способом;
  - *Telnet* — доступ к устройству только по Telnet;
  - *Secure Telnet (SSH)* — доступ к устройству только по SSH;
  - *HTTP* — доступ к устройству только по HTTP;
  - *HTTPS* — доступ к устройству только по HTTPS;
  - *SNMP* — доступ к устройству только по SNMP;

– *Интерфейс* — при установленном флаге правило контроля доступа будет основано на интерфейсе:

  - *Порт* — номер порта;
  - *LAG* — номер LAG-группы;
  - *VLAN* — номер VLAN;

– *IP-адрес источника* — при установленном флаге правило доступа будет основано на IP-адресе клиента, передающего трафик. Необходимо указать IP-адрес и маску подсети:

  - *Маска подсети* — маска подсети, задается в формате XXX.XXX.XXX.XXX;
  - *Длина префикса подсети* — длина префикса (количество единичных разрядов в маске подсети), принимает значения (8–30). Если установлен флаг «*Длина префикса подсети*», то поле «*Макска подсети»* не используется. Задается в числовом формате через символ «/»;

– *Действие* — назначаемое действие:

  - *Разрешить* — разрешить доступ к устройству;
  - *Запретить* — запретить доступ к устройству. Установлено по умолчанию.

Нажмите кнопку «Сохранить» для применения настроек.

Для удаления записи нужно установить флаг напротив заданной записи, нажать кнопку «Удалить» и кнопку «Сохранить» для применения настроек.

2.5.3.2 Управление профилями правил доступа

В разделе **Настройка безопасности → Метод доступа → Настройка правил** осуществляется управление профилями правил доступа. В профиле может быть создано до 128 правил, определяющих, каким способом и какие пользователи могут управлять устройством.

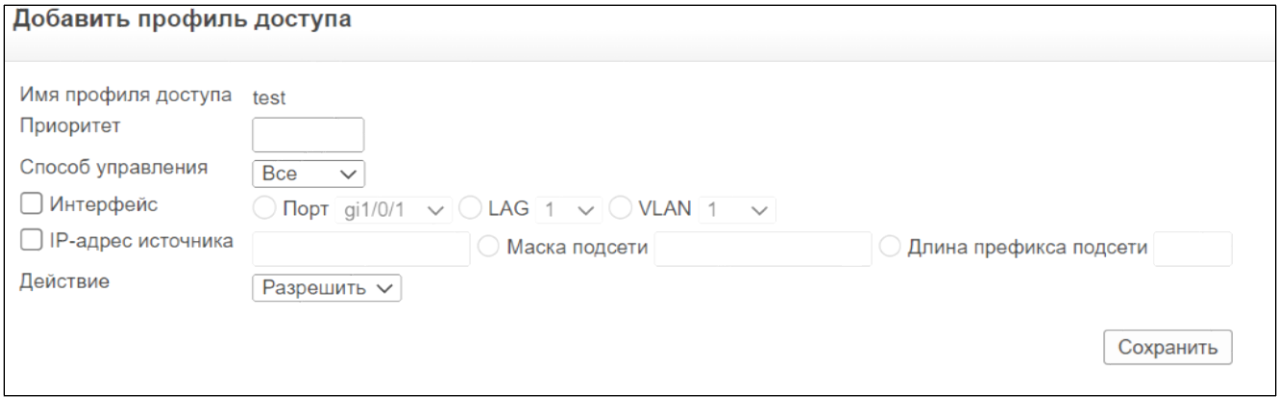
– *Имя профиля доступа* — имя профиля доступа.

Настройки профиля доступа «Console Only» не могут быть изменены, либо удалены.

В таблице будет отображаться список правил, установленных в профиле. Для редактирования правила нужно нажать кнопку «Редактировать» напротив заданной записи, заполнить соответствующие поля и нажать кнопку «Сохранить» для применения настроек.

Для удаления записи установите флаг напротив заданной записи, нажмите кнопку «Удалить» и кнопку «Сохранить» для применения настроек.

Для добавления нового правила в список профиля нажмите кнопку «Добавить» и заполните следующие поля:



– *Приоритет* — приоритет правила;

– *Способ управления* — способ доступа:

- Все — доступ к устройству любым способом;
- *Telnet* — доступ к устройству только по Telnet;
- *SSH* — доступ к устройству только по SSH;
- *HTTP* — доступ к устройству только по HTTP;

- *HTTPS* — доступ к устройству только по HTTPS;
- *SNMP* — доступ к устройству только по SNMP;

– *Интерфейс* — при установленном флаге правило доступа будет основано на интерфейсе:

- *Порт* — номер порта;
- *LAG* — номер группы LAG;
- *VLAN* — номер VLAN;

– *IP-адрес источника* — при установленном флаге правило доступа будет основано на IP-адресе клиента, передающего трафик. Необходимо указать IP-адрес и маску подсети:

- *Маска подсети* — маска подсети, задается в формате XXX.XXX.XXX.XXX;
- *Длина префикса подсети* — длина префикса (количество единичных разрядов в маске подсети), принимает значения (8–30). Если установлен флаг «*Длина префикса подсети*», то поле «*Маска подсети»* не используется. Задается в числовом формате через «/»;

– *Действие* — назначаемое действие:

- *Разрешить* — разрешить доступ к устройству;
- *Запретить* — запретить доступ к устройству. Установлено по умолчанию.

Нажмите кнопку «Сохранить» для применения настроек.

2.6 Управление сетевой безопасностью

В данной главе описываются способы управления сетевой безопасностью устройства. Управление сетевой безопасностью подразумевает контроль трафика, посредством настройки функции контроля штормов и безопасности портов на основе MAC-адресов.

2.6.1 Управление трафиком

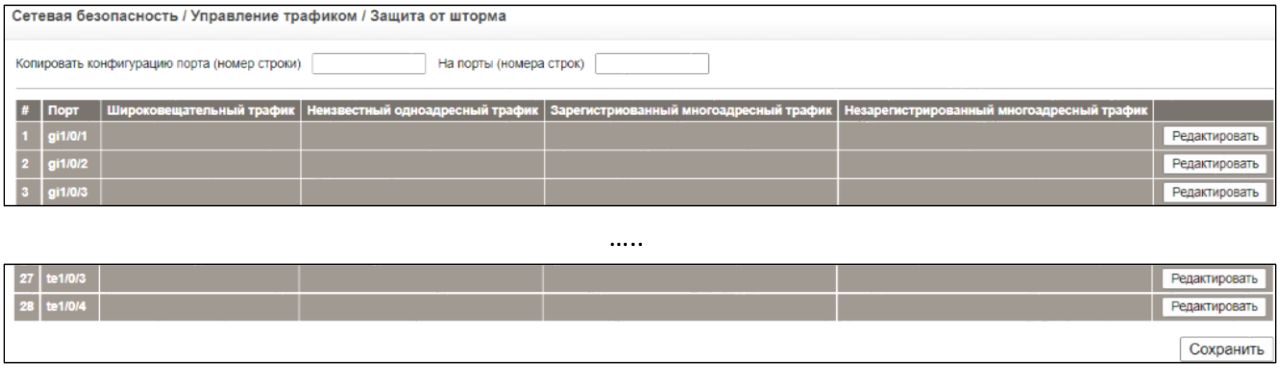
Управление трафиком позволяет повысить безопасность и производительность сети путем ограничения широковещательного служебного трафика и доступа к устройству.

2.6.1.1 Контроль широковещательного «шторма»

В разделе **Сетевая безопасность → Управление трафиком → Защита от шторма** выполняется настройка функции контроля широковещательных «штормов» для портов коммутатора.

Широковещательный «шторм» — это результат единовременной передачи чрезмерного количества широковещательных системных сообщений по сети на один порт, что может повлиять на производительность всей сети. Функция контроля широковещательных «штормов» ограничивать входящий/исходящий широковещательный и многоадресный трафик при достижении максимально допустимого количества пакетов на один порт.

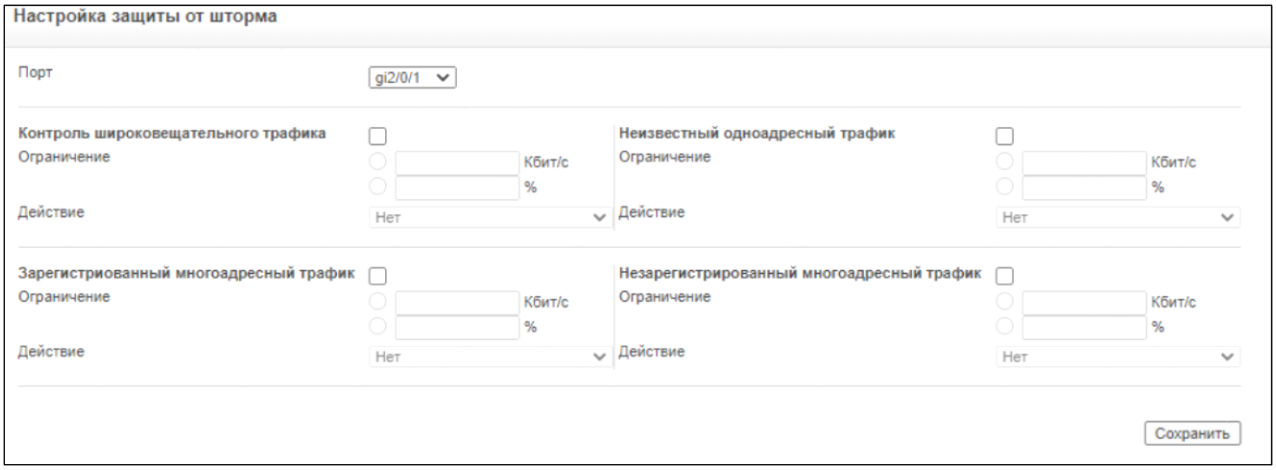
Функция контроля «шторма» включается на всех портах коммутатора путем определения типа и скорости передаваемых пакетов. Система измеряет интенсивность поступления широковещательных и многоадресных пакетов на каждом порту и отбрасывает пакеты, если значение превышает порог, установленный администратором.



Для установки одинаковых значений для диапазона записей необходимо заполнить следующие поля и нажать кнопку «Сохранить»:

- *Копировать конфигурацию порта (номер строки)* — порядковый номер записи, параметры которой будут скопированы;
- *На порты (номера строк)* — порядковый номер/номера записей, для которых будут применены параметры. Можно указать диапазон через «—», либо перечислением через «,».

Для редактирования записи нужно нажать кнопку «Редактировать», заполнить соответствующие поля и нажать кнопку «Сохранить» для применения настроек.



– *Порт* — номер порта коммутатора;

– *Контроль широковещательного трафика, неизвестный одноадресный трафик, зарегистрированный многоадресный трафик, незарегистрированный многоадресный трафик* — при установленном флаге функция контроля шторма включена:

  - *Ограничение* — максимальная скорость для широковещательного, многоадресного и неизвестного одноадресного трафика (для портов gi0/1 — 24 3500–1000000 кбит/с, для портов te0/1— 4 8500–10000000 кбит/с). По умолчанию установлено 100000. Значение округляется до ближайших 64 кбит/с, за исключением 0;

  - *Действие* — действия, которые будут осуществляться при шторме:

    – *Нет* — выполняется действие по умолчанию;
    – *Оповестить* — оповещение о возникновении шторма;
    – *Выключить порт* — выключение порта;
    – *Оповестить и выключить порт* — оповещение о возникновении шторма и выключение порта;

– *Типы трафика*:

• *Широковещательный трафик* — отображает настройки защиты от шторма для широковещательного трафика;

• *Неизвестный одноадресный трафик* — отображает настройки защиты от шторма для неизвестного одноадресного трафика;

• *Зарегистрированный многоадресный трафик* — отображает настройки защиты от шторма для зарегистрированного многоадресного трафика;

• *Незарегистрированный многоадресный трафик* — отображает настройки защиты от шторма для незарегистрированного многоадресного трафика.

2.6.1.2 Обеспечение защиты портов

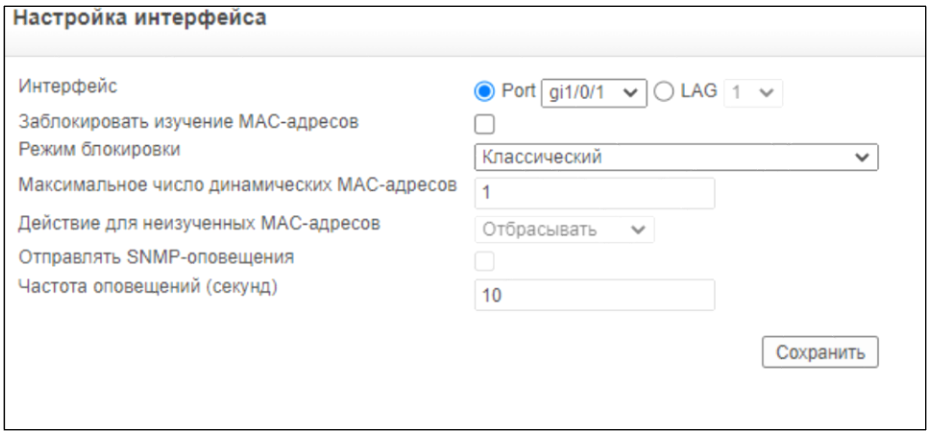
В разделе **Сетевая безопасность → Управление трафиком → Безопасносить портов** выполняется настройка функции безопасности портов коммутатора на основе MAC-адресов.

Сетевая безопасность может быть улучшена, если установить доступ к определенному интерфейсу только по заданным MAC-адресам пользователей. MAC-адрес может быть получен динамически или установлен в системе статически. При получении пакета от пользователя, MAC-адрес которого системе неизвестен, срабатывает механизм защиты (задается в поле «Действие»). Доступ к заблокированным портам разрешен только для пользователей с определенными адресами.

Интерфейс	Состояние	Режим блокировки	Максимальное число динамических MAC-адресов	Действие	Оповещение	Частота оповещений (секунд)	
gi1/0/1	Разблокирован	Классический	1	Отбрасывать	Выключено	10	Редактировать
gi1/0/2	Разблокирован	Классический	1	Отбрасывать	Выключено	10	Редактировать
gi1/0/3	Разблокирован	Классический	1	Отбрасывать	Выключено	10	Редактировать
gi1/0/4	Разблокирован	Классический	1	Отбрасывать	Выключено	10	Редактировать
gi1/0/5	Разблокирован	Классический	1	Отбрасывать	Выключено	10	Редактировать

При установленном флаге «Порты» будет отображена таблица правил для портов коммутатора, при установленном флаге «LAGs» — таблица правил для групп LAG.

Для редактирования записи нужно нажать кнопку «Редактировать» и заполнить соответствующие поля:



- *Интерфейс* — интерфейс, для которого устанавливается правило:
  - *Порт* — номер порта;
  - *LAG* — номер группы LAG;
- *Заблокировать изучение MAC-адресов* — при установленном флаге на интерфейсе включена функция защиты и отключена функция изучения новых адресов. Пакеты с неизученными MAC-адресами источника отбрасываются;
- *Режим блокировки* — режим ограничения изучения MAC-адресов для настраиваемого интерфейса. Поле активно, если не установлен флаг «*Заблокировать изучение MAC-адресов*»:

- *Классический* — сохраняются текущие динамически изученные MAC-адреса, связанные с интерфейсом. Запрещается обучение новым адресам и старение уже изученных адресов;
- *Ограничение динамических MAC-адресов* — удаляются текущие динамически изученные адреса, связанные с интерфейсом. Разрешено изучение ограниченного количества адресов на порту, а также повторное изучение и старение MAC-адресов;

– *Максимальное количество динамических MAC-адресов* — количество MAC-адресов, которое может быть изучено на интерфейсе. Поле активно, если установлен режим ограничения изучения MAC-адресов «*Ограничение динамических MAC-адресов*». По умолчанию установлено 1;

– *Действие для неизученных MAC-адресов* — действие, назначаемое пакетам, приходящим на заблокированный порт. Поле активно, если порт заблокирован (установлен флаг «*Заблокировать изучение MAC-адресов»*):

- *Пропускать* — пакеты, полученные от неизвестного источника, пересылаются без изучения MAC-адреса;
- *Отбрасывать* — пакеты, полученные от неизвестного источника, отбрасываются. Установлено по умолчанию;
- *Выключать порт* — пакеты, полученные от неизвестного источника, отбрасываются и порт блокируется. Порт будет заблокирован, пока его не активируют или не будет перезагружено устройство;

– *Отправлять SNMP-оповещения* — при установленном флаге разрешена отправка trap-сообщений в случае поступления несанкционированных пакетов. Поле активно, если установлен флаг «*Заблокировать изучение MAC-адресов*»;

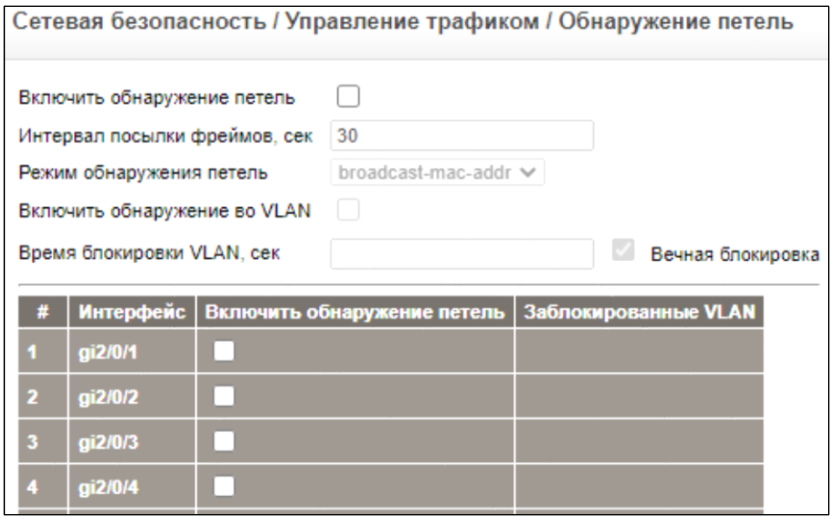
– *Частота оповещений (секунд)* — частота генерируемых сообщений протокола SNMP. По умолчанию установлено 10 секунд.

Нажмите кнопку «Сохранить» для применения настроек.

2.6.1.3 Обнаружение петель на порту

В разделе **Сетевая безопасность → Управление трафиком → Обнаружение петель** выполняется настройка функции обнаружение петель на портах коммутатора.

Данный механизм позволяет устройству отслеживать закольцованные порты. Петля на порту обнаруживается путём отсылки коммутатором кадра с адресом назначения, совпадающим с одним из MAC-адресов устройства.



При установленном флаге *«Включить обнаружение петель»* функция будет включена.

– *Интервал посылки фреймов, сек* — интервал между loopback-кадрами (сек.);

– *Режим обнаружения петель* — определить MAC-адрес назначения, указываемый в Loopback Detection-кадре:

  - *source-mac-addr* — в качестве адреса назначения используется MAC-адрес порта источ–ника;
  - *base-mac-addr* — в качестве адреса назначения используется MAC-адрес коммутатора;
  - *multicast-mac-addr* — в качестве адреса назначения используется групповой адрес;
  - *broadcast-mac-addr* — в качестве адреса назначения используется широковещательный адрес.

  При установленном флаге *«Включить обнаружение во VLAN»* будет включена функция обнаружения петли во VLAN. При наличии петли данный VLAN будет заблокирован на порту, на котором была обнаружена петля.

– *Время блокировки VLAN* — задать время, по истечении которого заблокированный VLAN автоматически разблокируется.

  Флаг *«Вечная блокировка»* — заблокировать VLAN навсегда.

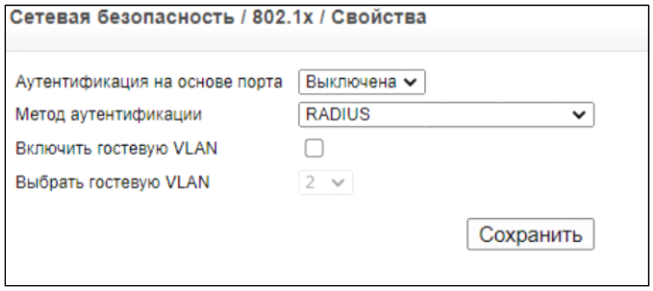
2.6.2 Проверка подлинности клиента на основе порта (стандарт 802.1x)

В данном разделе выполняется просмотр статистики и настройка аутентификации 802.1x на основе портов.

Стандарт IEEE802.1x определяет механизм аутентификации через сервер RADIUS на основе принадлежности к порту.

2.6.2.1 Основные настройки аутентификации (IEEE802.1x)

В разделе **Network Security → 802.1x → Свойства** выполняются основные настройки для аутентификации по стандарту IEEE802.1x.

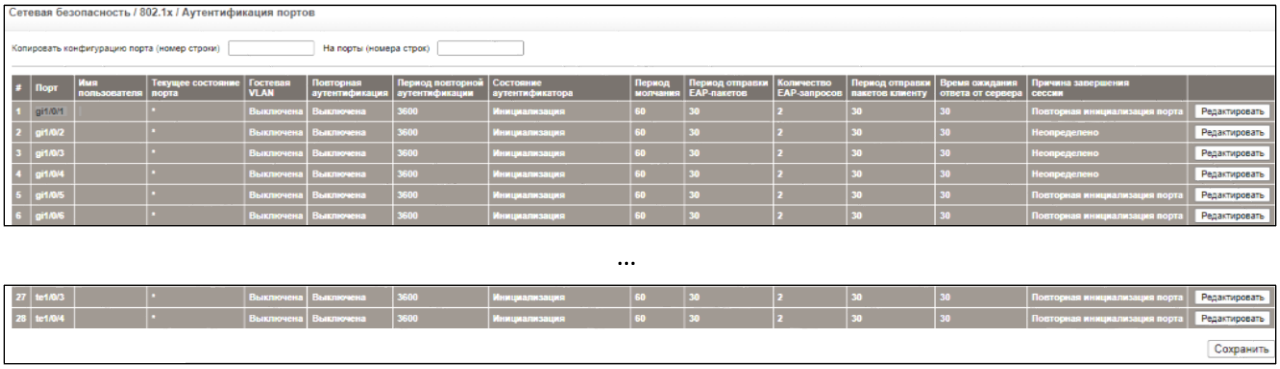


– *Аутентификация на основе порта* — состояние режима аутентификации 802.1x для устройства:
  - *Включена* — аутентификация на основе портов для устройства включена;
  - *Выключена* — аутентификация на основе портов для устройства отключена;
– *Метод аутентификации* — метод проверки подлинности:
  - *Не аутентифицировать* — аутентификация не используется;
  - *RADIUS* — аутентификация происходит на сервере RADIUS;
  - *RADIUS, не аутентифицировать* — аутентификация происходит на сервере RADIUS, если RADIUS-сервер недоступен, то аутентификация не используется;
– *Включить гостевую VLAN* — при установленном флаге если порт не авторизован, то он автоматически присоединяется к гостевой VLAN, номер которой указан в поле «VLAN List». Если флаг не установлен, то гостевая VLAN не используется;
– *Выбрать гостевую VLAN* — номер гостевой VLAN.

Нажать кнопку «Сохранить» для применения настроек.

2.6.2.2 Базовая проверка подлинности пользователя

В разделе **Сетевая безопасность → 802.1x → Аутентификация портов** выполняется настройка глобальных параметров аутентификации 802.1x для каждого порта коммутатора.

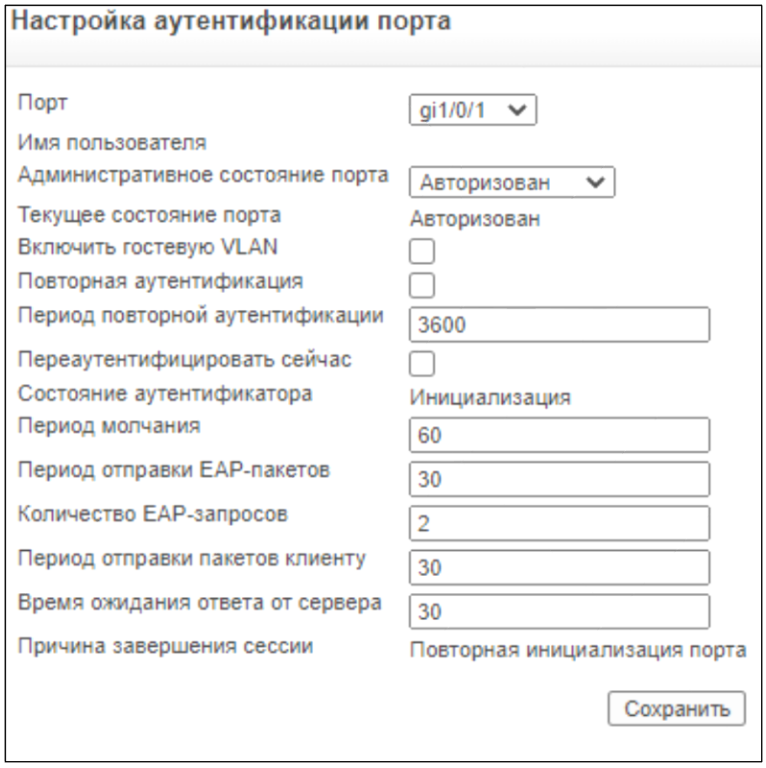


…

Для одновременной настройки нескольких портов можно скопировать значение параметров из одной записи в другую/другие. Для этого заполните следующие поля и нажмите кнопку «Сохранить»:

– *Копировать конфигурацию порта (номер строки)* — порядковый номер записи, параметры которой будут скопированы;

– *На порты (номера строк)* — порядковый номер/номера записей, для которых будут применены параметры. Можно указать диапазон через «—», либо перечислением через «,». Для редактирования настроек аутентификации 802.1x для порта нужно нажать кнопку «Редактировать» напротив заданной записи и заполнить соответствующие поля:



– *Порт* — номер порта;

– *Имя пользователя* — имя пользователя при использовании 802.1X. Если порт авторизован, то отображается имя текущего пользователя. Если порт не авторизован, то отображается имя последнего успешно авторизованного пользователя на порту;

– *Административное состояние порта* — аутентификация 802.1X на интерфейсе. Разрешается ручной контроль за состоянием авторизации порта:

  - *Автоматически* — на интерфейсе включена аутентификация 802.1x. Состояние интерфейса (авторизован/не авторизован) будет изменяться автоматически, в зависимости от результатов аутентификации между устройством и клиентом;

  - *Авторизован* — интерфейс находится в авторизованном состоянии без выполнения аутентификации;

  - *Неавторизован* — интерфейс находится в неавторизованном состоянии. Игнорируются все попытки аутентификации клиента, коммутатор не предоставляет сервис аутентификации для этого интерфейса;

– *Текущее состояние порта* — отображается текущее состояние авторизации порта;

– *Включить гостевую VLAN* — при установленном флаге если интерфейс находится в неавторизованном состоянии, то он автоматически присоединяется к гостевой VLAN, номер которой указан в поле «VLAN List». Включение данной опции позволяет администратору предоставить пользователям, которые не прошли аутентификацию 802.1x, ограниченный доступ к сети. Если флаг не установлен, то гостевая VLAN не используется;

– *Повторная аутентификация* — при установленном флаге на интерфейсе разрешена периодическая повторная аутентификации 802.1x, иначе — повторная аутентификация не используется;

– *Период повторной аутентификации* — период между повторными проверками подлинности клиента, (300–4294967295 секунд). По умолчанию установлено 3600 секунд;

– *Переаутентифицировать сейчас* — немедленная переаутентификация интерфейса при уста–новке флага и сохранении настроек;

– *Состояние аутентификатора* — отображает текущее состояние аутентификации в соответствии со стандартом IEEE802.1X:

  - *Инициализация* — состояние инициализации агента аутентификации;
  - *Disconnected* — состояние возникает при прекращении доступа к сети в результате преднамеренного прекращения сеанса или при разрыве связи;
  - *Connecting* — состояние готовности к началу процедуры аутентификации;
  - *Authenticating* — состояние в процессе процедуры аутентификации;
  - *Authenticated* — доступ к сети получен от RADIUS-сервера;
  - *Aborting* — прерывание процедуры аутентификации;
  - *Held* — состояние временной блокировки порта, при котором игнорируются все сообщения протокола EAP;

- *Принудительно авторизован* — авторизация 802.1X запрещена, порт имеет доступ в сеть без выполнения процедуры аутентификации;
- *Force Unauthorized* — порт не имеет доступа в сеть, попытки аутентификации игнорируются;

– *Период молчания* — период, в течение которого коммутатор остается в состоянии молчания после неудачной проверки подлинности, (0–65535 сек.). По умолчанию установлено 60 секунд;

– *Период отправки EAP-пакетов* — период, в течение которого коммутатор ожидает ответ на запрос либо идентификацию по протоколу EAP от клиента, перед повторной отправкой запроса, (30–65535 сек.). По умолчанию установлено 30 секунд;

– *Количество EAP-запросов* — максимальное число попыток передачи запросов протокола EAP-клиенту перед новым запуском процесса проверки подлинности, (1–10). По умолчанию установлено 2;

– *Период отправки пакетов клиенту* — период между повторными передачами запросов протокола EAP-клиенту, (1–65535 сек.). По умолчанию установлено 30 секунд;

– *Время ожидания ответа от сервера* — период, в течение которого коммутатор ожидает ответа от сервера аутентификации, (1–65535 сек.). По умолчанию установлено 30 секунд;

– *Причина завершения сессии* — указывает причину, по которой была остановлена аутентификация интерфейса.

Нажмите кнопку «Сохранить» для применения настроек.

2.6.2.3 Расширенная проверка подлинности пользователя

В разделе **Сетевая безопасность → 802.1x → Множественный доступ** выполняется расширенная настройка аутентификации 802.1x для проверки подлинности нескольких клиентов, подключенных к одному порту. Если порт в режиме «multiple hosts» не проходит аутентификацию, то всем подключенным хостам будет отказано в доступе к ресурсам сети.

Сетевая безопасность / 802.1x / Множественный доступ

#	Порт	Множественный доступ	Действие при нарушении режима	Оповещения	Частота оповещений	Состояние	Количество нарушений	
1	gi1/0/1	Включен	Отбрасывать	Выключить	0	Авторизация выключена*	0	Редактировать
2	gi1/0/2	Включен	Отбрасывать	Выключить	0	Авторизация выключена*	0	Редактировать
3	gi1/0/3	Включен	Отбрасывать	Выключить	0	Авторизация выключена*	0	Редактировать
4	gi1/0/4	Включен	Отбрасывать	Выключить	0	Авторизация выключена	0	Редактировать
5	gi1/0/5	Включен	Отбрасывать	Выключить	0	Авторизация выключена*	0	Редактировать
6	gi1/0/6	Включен	Отбрасывать	Выключить	0	Авторизация выключена*	0	Редактировать
7	gi1/0/7	Включен	Отбрасывать	Выключить	0	Авторизация выключена*	0	Редактировать
8	gi1/0/8	Включен	Отбрасывать	Выключить	0	Авторизация выключена	0	Редактировать
9	gi1/0/9	Включен	Отбрасывать	Выключить	0	Авторизация выключена*	0	Редактировать
10	gi1/0/10	Включен	Отбрасывать	Выключить	0	Авторизация выключена*	0	Редактировать

Описание полей таблицы:

- *Порт* — отображает номер порта, на котором включена расширенная аутентификация на основе порта;
- *Множественный доступ* — указывает, разрешена ли аутентификация нескольких клиентов на порту. Множественный доступ должен быть разрешён в случае отключения входной фильтрации или блокирования изучения MAC-адресов на выбранном порту. Поле может принимать следующие значения:
    - *Включен* — включен множественный доступ;
    - *Выключен* — включен одиночный доступ;
- *Действие при нарушении режима* — определяет действие, применяемое к пакетам, чей MAC-адрес не соответствует адресу клиента на этом порту в режиме одиночного доступа. Поле может принимать следующие значения:
    - *Пропускать* — переслать пакет;
    - *Отбрасывать* — отбросить пакет. Это значение по умолчанию;
    - *Выключить порт* — отбросить пакет и выключить порт. Порт остаётся выключен, вплоть до ручной активации или перезагрузки устройства;
- *Оповещения* — указывает, включены ли SNMP-оповещения для режима множественного доступа. Поле может принимать следующие значения:
    - *Включить* — SNMP-оповещения включены;
    - *Выключить* — SNMP-оповещения выключены;

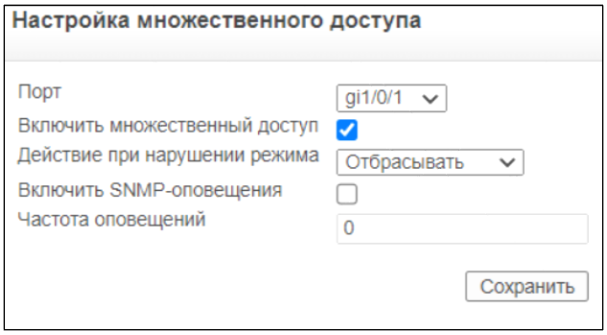
– *Частота оповещений* — определяет частоту, с которой SNMP-оповещения отсылаются клиенту. Поле доступно только при включении режима множественного доступа. Диапазон допустимых значений — от 1 до 1000000. Значение по умолчанию — 10 секунд;

– *Состояние* — отображает состояние клиента. Знак (*) указывает, что соединение отсутствует или не установлено. Поле может принимать следующие значения:

- *Не авторизован* — порт принудительно находится в неавторизованном состоянии или выключен, либо он находится в состоянии "Авто", но клиент не был авторизован;
- *Авторизация выключена* — порт находится в принудительно-авторизованном состоянии, и клиент имеет полный доступ к порту;
- *Подключен единственный клиент* — на порту аутентифицирован единственный разрешённый клиент;
- *Разрешён множественный доступ* — включен режим множественного доступа;

– *Количество нарушений* — количество пакетов, принятых на порту в одиночном режиме, чей MAC-адрес не совпадает с адресом подключенного клиента.

Для редактирования настроек порта нужно нажать кнопку «Редактировать» напротив заданной записи и заполнить соответствующие поля:



– *Порт* — номер порта, для которого включена аутентификация 802.1x;

– *Включить множественный доступ* — при установленном флаге разрешено наличие нескольких клиентов на авторизованном порту 802.1x;

– *Действие при нарушении режима* — действие, которое необходимо выполнить, когда устройство, MAC-адрес которого отличается от MAC-адреса клиента, осуществляет попытку доступа к интерфейсу:

- *Пропускать* — пакеты с MAC-адресом, отличным от MAC-адреса клиента, пересылаются;
- *Отбрасывать* — пакеты с MAC-адресом, отличным от MAC-адреса клиента, отбрасываются. Установлено по умолчанию;
- *Выключать порт* — порт выключается и пакеты с MAC-адресом, отличным от MAC-адреса клиента, отбрасываются;

– *Включить SNMP-оповещения* — при установленном флаге разрешена отправка trap-сообщений в режиме «*Множественный доступ*»;

– *Частота оповещений* — частота генерации trap-сообщений, (1–1000000 сек.). По умолчанию установлено 10 секунд.

Нажмите кнопку «Сохранить» для применения настроек.

2.6.2.4 Просмотр авторизованных пользователей

В разделе **Сетевая безопасность → 802.1x → Аутентифицированные хосты** можно просмотреть список авторизованных пользователей.

Сетевая безопасность / 802.1x / Аутентифицированные хосты

#	Имя пользователя	Порт	Время жизни сессии	Способ аутентификации	MAC-адрес
1		gi1/0/1	0	Аутентификация выключена	000000000000
2		gi1/0/2	0	Аутентификация выключена	000000000000
3		gi1/0/3	0	Аутентификация выключена	000000000000
4		gi1/0/4	0	Аутентификация выключена	000000000000
5		gi1/0/5	0	Аутентификация выключена	000000000000
6		gi1/0/6	0	Аутентификация выключена	000000000000
7		gi1/0/7	0	Аутентификация выключена	000000000000
8		gi1/0/8	0	Аутентификация выключена	000000000000
9		gi1/0/9	0	Аутентификация выключена	000000000000
10		gi1/0/10	0	Аутентификация выключена	000000000000
11		gi1/0/11	0	Аутентификация выключена	000000000000
12		gi1/0/12	0	Аутентификация выключена	000000000000
13		gi1/0/13	0	Аутентификация выключена	000000000000
14		gi1/0/14	0	Аутентификация выключена	000000000000
15		gi1/0/15	0	Аутентификация выключена	000000000000
16		gi1/0/16	0	Аутентификация выключена	000000000000
17		gi1/0/17	0	Аутентификация выключена	000000000000

Описание полей таблицы:

– *Имя пользователя* — имя пользователя, если порт авторизован;

– *Порт* — номер порта;

– *Время жизни сессии* — интервал времени (в секундах) с момента регистрации пользователя;

– *Способ аутентификации* — метод аутентификации:

  ▪ *Аутентификация выключена* — аутентификация 802.1x не используется. Порт переходит в авторизованное состояние без аутентификации;

  ▪ *Не аутентифицирован*— аутентификация не была пройдена;

  ▪ *RADIUS* — аутентификация была пройдена на RADIUS-сервере;

– *MAC-адрес* — MAC-адрес пользователя.

2.6.2.5 Статистика протокола EAP (Extensible Authentication Protocol)

В разделе **Сетевая безопасность → 802.1x → Статистика EAP** можно просмотреть статистику по EAP-пакетам, которые были приняты на определенный порт.

– *Порт* — номер порта, для которого отображается статистика;

– *Частота обновления* — время обновления EAP-статистики:

  ▪ *15 сек* — EAP-статистика обновляется каждые 15 секунд;

  ▪ *30 сек* — EAP-статистика обновляется каждые 30 секунд;

  ▪ *60 сек* — EAP-статистика обновляется каждые 60 секунд;

  ▪ *Не обновлять* — EAP-статистика не обновляется;

– *Принято пакетов* — количество корректных EAPOL-пакетов, принятых на порт;

– *Отправлено пакетов* — количество переданных EAPOL-пакетов с порта;

– *Принято EAPOL Start* — количество пакетов «Start» протокола EAPOL, принятых данным портом;

– *Принято EAPOL Logoff* — количество пакетов «Logoff» протокола EAPOL, принятых данным портом;

– *Принято EAP Resp/Id* — количество пакетов «Resp/Id» протокола EAPOL, принятых портом;

– *Принято EAP Response* — количество EAP-ответов (кроме «Resp/Id»), принятых портом;

– *Отправлено EAP Req/Id* — количество пакетов «Resp/Id» протокола EAPOL, переданных через порт;

– *Отправлено EAP Request* — количество запросов (кроме «Resp/Id») протокола EAPOL, переданных через порт;

– *Принято некорректных пакетов* — количество пакетов протокола EAPOL с нераспознанным типом, принятые данным портом;

– *Принято пакетов неправильной длины* — количество пакетов протокола EAPOL с некорректной длиной, принятые данным портом;

– *Версия последнего принятого пакета* — версия протокола EAPOL, принятая в самом последнем пакете;

– *Отправитель последнего принятого пакета* — MAC-адрес источника, принятый в самом последнем пакете.

2.6.3 Конфигурирование ACL (списки контроля доступа)

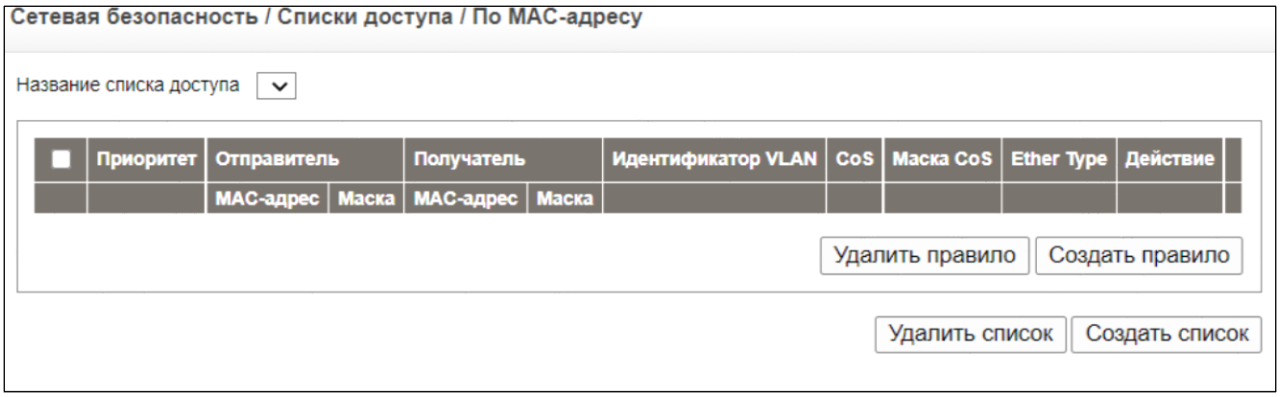
Списки контроля доступа (ACL) позволяют администратору сети установить правила фильтрации входящего трафика на определенных портах коммутатора. Трафик, поступающий на порт коммутатора с включенной функцией ACL, может быть либо пропущен, либо отброшен, согласно установленным правилам ACL. В случае если пакеты были отброшены, можно заблокировать порт, на который они поступили.

Коммутатор позволяет задать до 2048 списков доступа. В данном разделе выполняются настройки списков контроля доступа (ACL) и назначение ACL-списков портам коммутатора. В ACL определяются правила фильтрации входящего и исходящего трафика по различным критериям:

– *По MAC-адресу* — настройка параметров списков доступа, основанных на MAC-адресации;
– *По IP-адресу* — настройка параметров списков доступа, основанных на IP-адресации;
– *Привязка списков доступа* — назначение списков доступа портам коммутатора.

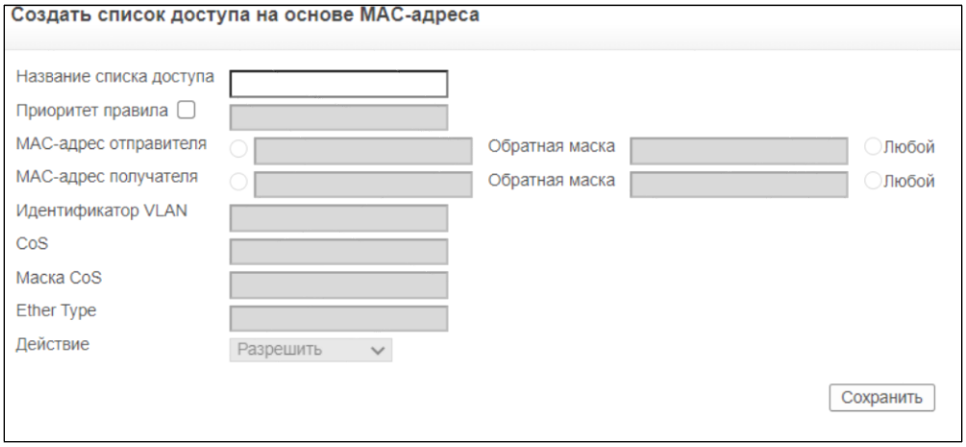
2.6.3.1 Настройка списков доступа, основанных на MAC-адресации

В разделе **Сетевая безопасность → Списки доступа → По MAC-адресу** выполняется настройка основных параметров списков ACL, основанных на MAC-адресации.



Для просмотра конфигурации заданного списка ACL нужно в списке «Название списка доступа» выбрать имя списка доступа.

Для добавления нового списка ACL нужно нажать кнопку «Создать список» и заполнить следующие поля:



– *Название списка доступа* — имя списка ACL, основанного на MAC-адресации;

– *Приоритет правила* — приоритет правила (1–2147483647). При установленном флаге доступны поля для настройки нового правила фильтрации для списка ACL;

– *MAC-адрес отправителя* — при установленном флаге разрешена фильтрация пакетов по MAC-адресу источника. Необходимо указать MAC-адрес источника пакета;

– *MAC-адрес получателя* — при установленном флаге разрешена фильтрация пакетов по MAC-адресу назначения пакета;

– *Обратная маска* — битовая маска, применяемая к MAC-адресу источника пакета. Маска определяет биты MAC-адреса, которые необходимо игнорировать. Пример: чтобы добавить в правило фильтрации все MAC-адреса начинающиеся на 00:00:02:AA.xx.xx необходимо задать значение маски 0.0.0.0.FF.FF, то есть, согласно данной маске, последние 16 бит MAC-адреса будут не важны для анализа;

– *Любой* — при установленном флаге фильтрация по MAC-адресам источника/назначения производиться не будет;

– *Идентификатор VLAN* — идентификатор VLAN фильтруемых пакетов, (1–4094);

– *CoS* — класс обслуживания (CoS) фильтруемых пакетов, (0–7);

– *Маска Cos* — битовая маска, применяемая к классу обслуживания (CoS) фильтруемых пакетов. Маска определяет биты CoS, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы. Пример: чтобы использовать в правиле фильтрации CoS 6 и 7 необходимо в поле CoS указать значение 6, либо 7, а в поле маски значение 1 (7 в двоичном представлении — 111_2, 1 — 001_2, получается, что последний бит будет игнорироваться, то есть CoS может быть либо 110_2 (6), либо 111_2 (7));

– *Ether Type* — значение Ether Type, указывается в десятичном формате;

– *Действие* — назначаемое действие:

  - *Разрешить* — создает разрешающее правило фильтрации в списке ACL;

  - *Запретить* — создает запрещающее правило фильтрации в списке ACL;

- *Выключить порт* — создает запрещающее правило фильтрации и отключает порт, к которому пакет был адресован.

Нажмите кнопку «Сохранить» для применения настроек.

Для удаления списка ACL нужно нажать кнопку «Удалить список».

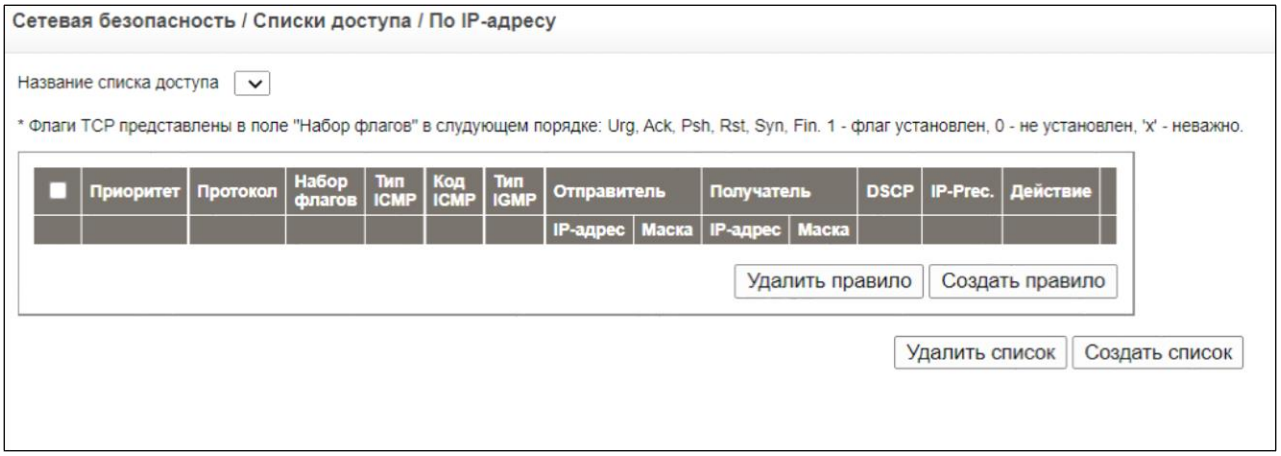
Для добавления нового правила в список ACL нужно в списке «Название списка доступа» выбрать имя списка ACL, нажать кнопку «Добавить правило», заполнить соответствующие поля и нажать кнопку «Сохранить» для применения настроек.

Для редактирования параметров нажмите кнопку «Редактировать», измените необходимые параметры и нажмите кнопку «Сохранить» для применения настроек.

Для удаления правила из списка ACL установите флаг напротив заданной записи и нажмите кнопку «Удалить».

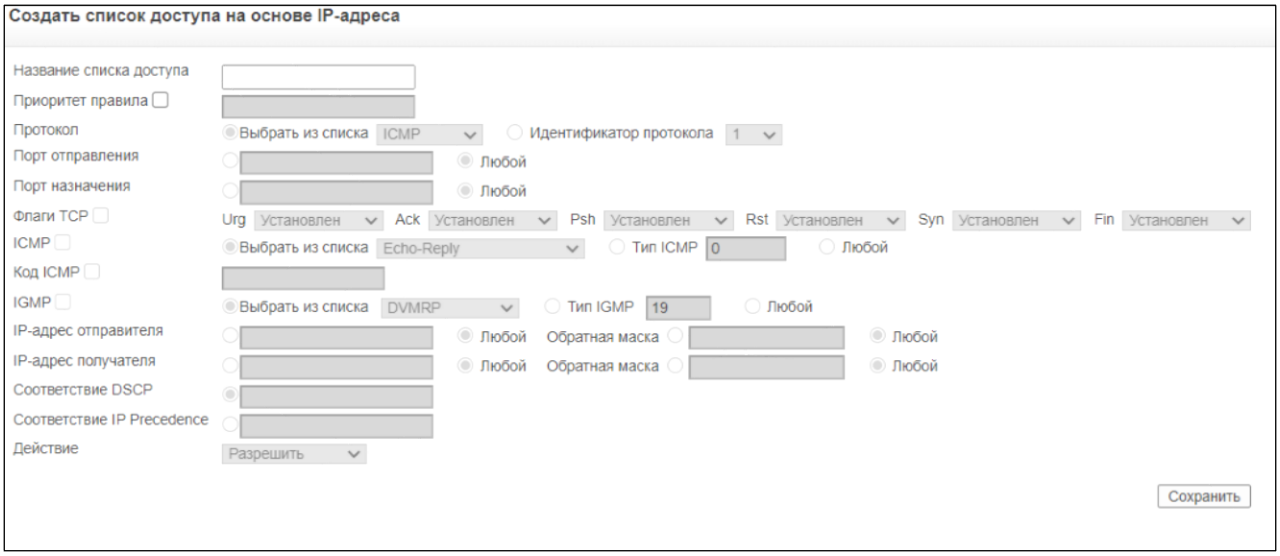
2.6.3.2 Настройка списков доступа, основанных на IP-адресации

В разделе **Сетевая безопасность → Списки доступа → по IP-адресу** выполняется настройка основных параметров списков ACL, основанных на IP-адресации.



Для просмотра конфигурации заданного списка ACL в ниспадающем списке «*Название списка доступа*» нужно выбрать имя списка ACL.

Для добавления нового списка ACL нужно нажать кнопку «Создать список» и заполнить следующие поля:



– *Название списка доступа* — имя списка ACL, основанного на IP-адресации;

– *Приоритет правила* — приоритет правила, (1–2147483647). При установке этого флага становятся доступны поля для настройки нового правила фильтрации для списка ACL;

– *Протокол* — протокол, на основе которого будет осуществляться фильтрация:

  - При установке флага «Выбрать из списка» возможны следующие варианты: icmp, igmp, ip, tcp, egp, igp, udp, hmp, rdp, idpr, ipv6, ipv6:rout, ipv6:frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipip, pim, l2tp, isis. Для соответствия любому протоколу используется значение «любой»**;**

  - Либо при установке флага «Идентификатор протокола» можно задать числовое значение протокола в диапазоне, (0–255);

– *IP-адрес отправителя* — при установленном флаге разрешена фильтрации пакетов по IP-адресу источника. Нужно указать IP-адрес источника пакета. При установленном флаге «Any» фильтрация по IP-адресу источника производится не будет;

– *IP-адрес получателя* — при установленном флаге разрешена фильтрации пакетов по IP-адресу назначения пакета. При установленном флаге «Any» фильтрация по IP-адресу назначения производится не будет;

– *Обратная маска* — битовая маска, применяемая к IP-адресу источника пакета. Маска определяет биты IP-адреса, которые необходимо игнорировать. Пример: используя маску, можно определить для правила фильтрации IP-сеть. Чтобы добавить в правило фильтрации IP-сеть 195.165.0.0, необходимо задать значение маски 0.0.255.255, то есть согласно данной маске последние 16 бит IP-адреса будут игнорироваться. При установленном флаге «Any» битовая маска использоваться не будет;

– *Соответствие DSCP* — значение DSCP-поля diffserv. Возможные коды сообщений поля dscp, (0–63);

– *Соответствие IP Precedence* — приоритет IP-трафика, (0–7);

– *Действие* — назначаемое действие:

- *Разрешить* — создает разрешающее правило фильтрации в списке ACL;
- *Запретить* — создает запрещающее правило фильтрации в списке ACL;
- *Выключить порт* — создает запрещающее правило фильтрации и отключает порт, к которому пакет был адресован.

При выборе протокола ICMP для редактирования станут активны следующие настройки:

– *ICMP* — при установке флага использовать фильтрацию ICMP-пакетов. Тип сообщения протокола ICMP, используемый для фильтрации задается одним из следующих способов:

- *Выбрать из списка* — при установке флага тип сообщения протокола ICMP можно выбрать из ниспадающего списка: echo—reply, destination—unreachable, source—quench, redirect, alternate—host—address, echo—request, router—advertisement, router—solicitation, time—exceeded, parameter—problem, timestamp, timestamp—reply, information—request, information—reply, address—mask—request, address—mask—reply, traceroute, datagram—conversion—error, mobile—host—redirect, mobile—registration—request, mobile—registration—reply, domain—name—request, domain—name—reply, skip, photuris;
- *Тип ICMP* — при установке флага устанавливается числовое значение типа сообщения, (0–255);
- *Любой* — при установке флага фильтрация ICMP-пакетов не используется.

При выборе протокола IGMP для редактирования станут активны следующие настройки:

– *IGMP* — при установке флага использовать фильтрацию IGMP-пакетов. Тип сообщения протокола IGMP, используемый для фильтрации задается одним из следующих способов:

- *Выбрать из списка* — при установке флага тип сообщения протокола IGMP можно выбрать из ниспадающего списка: host—query, host—report, dvmrp, pim, trace;
- *Тип IGMP* — при установке флага устанавливается числовое значение типа сообщения, (0–255);
- *Любой* — при установке флага фильтрация IGMP-пакетов не используется.

При выборе протокола TCP для редактирования станут активны следующие настройки:

– *Порт отправления* — при установленном флаге разрешена фильтрации пакетов по номеру TCP-порта источника. Нужно указать TCP-порт источника. Возможные значения поля TCP-порта: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp—data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs—ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). При установленном флаге «Любой» фильтрация по TCP—порту источника производится не будет;

– *Порт назначения* — при установленном флаге разрешена фильтрации пакетов по номеру TCP-порта назначения. Нужно указать TCP-порт назначения. При установленном флаге «Любой» фильтрация по TCP-порту назначения производиться не будет;

– *Флаги TCP* — флаги протокола TCP: urg, ack, psh, rst, syn, fin. Действие, производимое над флагами:

- *Установлен* — включить фильтрацию пакетов по соответствующему флагу;
- *Не установлен* — отключить фильтрацию пакетов по соответствующему флагу;
- *Не важно* — пакет с соответствующим флагом не влияет на процесс фильтрации.

При выборе протокола UDP для редактирования станут активны следующие настройки:

– *Порт отправления* — при установленном флаге разрешена фильтрации пакетов по номеру UDP-порта источника. Нужно указать UDP-порт источника. Возможные значения поля UDP-порта: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile—ip (434), nameserver (42), netbios—dgm (138), netbios—ns (137), on500—isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs—ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). При установленном флаге «Любой» фильтрация по UDP—порту источника производиться не будет;

– *Порт назначения* — при установленном флаге разрешена фильтрации пакетов по номеру UDP-порта назначения. Нужно указать UDP-порт назначения. При установленном флаге «Любой» фильтрация по UDP-порту назначения производиться не будет.

Нажмите кнопку «Сохранить» для применения настроек.

Для удаления списка ACL нужно нажать кнопку «Удалить список».

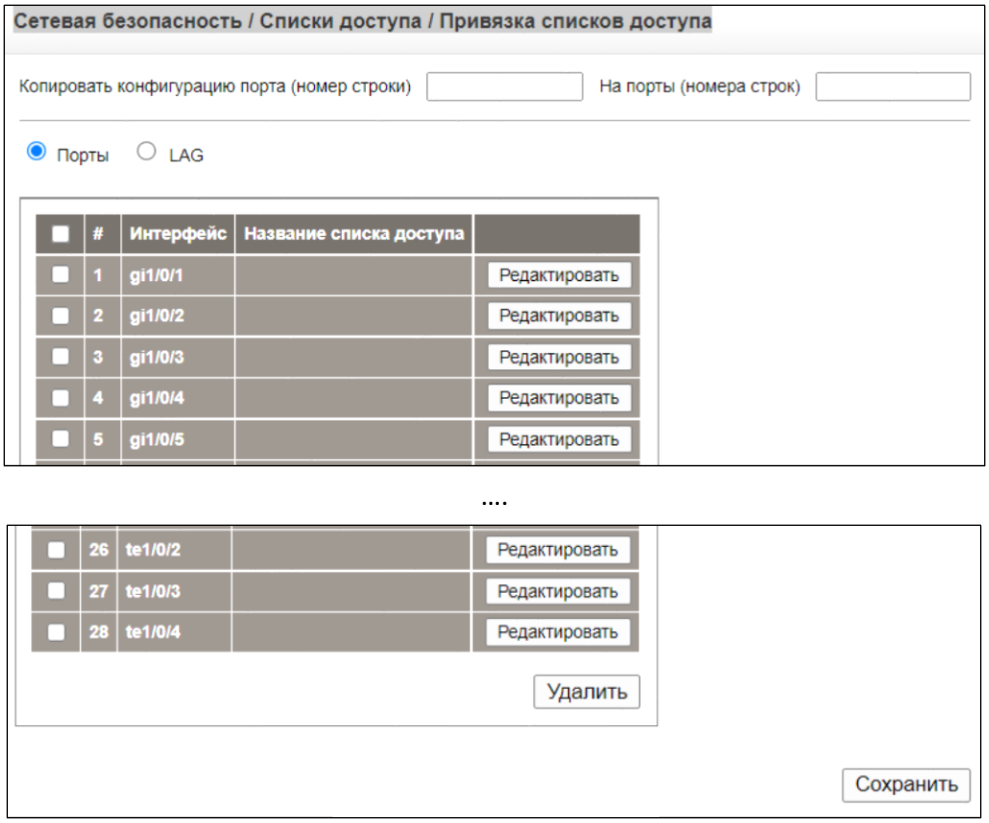
Для добавления нового правила в список ACL нужно в списке «Название списка доступа» выбрать имя списка ACL, нажать кнопку «Создать правило», заполнить соответствующие поля и нажать кнопку «Сохранить» для применения настроек.

Для редактирования параметров нажмите кнопку «Редактировать», измените необходимые параметры и нажмите кнопку «Сохранить» для применения настроек.

Для удаления правила из списка ACL установите флаг напротив заданной записи и нажмите кнопку «Удалить».

2.6.3.3 Назначение списков доступа ACL интерфейсам

В разделе **Сетевая безопасность → Списки доступа → Привязка списка доступа** списки доступа ACL назначаются интерфейсам коммутатора. Списки ACL можно применять к любому физическому интерфейсу или группе LAG.



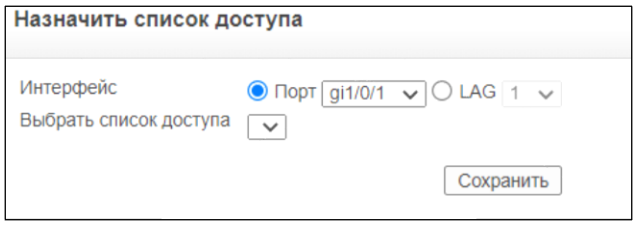
Для одновременной настройки нескольких портов можно скопировать значение параметров из одной записи в другую/другие. Для этого заполните следующие поля и нажмите кнопку «Сохранить»:

– *Копировать конфигурацию порта (номер строки)* — порядковый номер записи, параметры которой будут скопированы;

– *На порты (номера строк)* — порядковый номер/номера записей, для которых будут скопированы параметры. Можно указать диапазон через «—», либо перечислением через «,».

При установленном флаге «Порты» будет отображена таблица для портов коммутатора, при установленном флаге «LAG» — таблица для групп LAG.

Для назначения списка доступа ACL интерфейсу нужно нажать кнопку «Редактировать» напротив заданной записи и заполнить следующие поля:



– *Интерфейс* — интерфейс, которому будет назначен список доступа ACL:

  - *Порт* — Ethernet-интерфейс, принимает значения gi0/1..gi0/48, te0/1 .. te0/4;
  - *LAG* — агрегированная группа портов LAG, принимает значения 1–12;

– *Выбрать список доступа* — имя списка доступа ACL, который будет назначен интерфейсу.

Нажмите кнопку «Сохранить» для применения настроек.

2.7 Настройка функций второго уровня сетевой модели OSI

В данной главе описывается настройка функций второго уровня сетевой модели OSI для коммутатора, которая включает в себя:

– Конфигурирование интерфейсов коммутатора;

– Настройка группы агрегации каналов (LAG);

– Настройка протокола LACP;

– Настройка статической/динамической адресации;

– Настройка работы устройства по протоколам STP, RSTP, MSTP;

– Настройка виртуальной локальной сети (VLAN);

– Управление групповой адресации.

2.7.1 Конфигурирование интерфейсов

В текущем разделе описывается настройка интерфейсов коммутатора:

– Определение параметров интерфейсов коммутатора;

– Управление группами агрегации каналов;

– Объединение интерфейсов в группу LAG;

– Настройка параметров для работы по протоколу LACP.

2.7.1.1 Определение параметров интерфейсов коммутатора

В разделе **Настройки L2 → Интерфейсы → Конфигурация портов** выполняется настройка интерфейсов коммутатора.

Настройки L2 / Интерфейсы / Конфигурация портов

Копировать конфигурацию порта (номер строки) На порты (номера строк)

#	Интерфейс	Описание	Тип	Статус	Скорость	Дуплекс	Автосогласование скорости	Анонсирование	Обратное давление	Управление потоком	Тип кабеля	LAG	
1	gi1/0/1		1000M-copper	Неподключен	0б			Неопределено		Выключено	Авто		Редактировать
2	gi1/0/2		1000M-copper	Неподключен	0б			Неопределено		Выключено	Авто		Редактировать
3	gi1/0/3		1000M-copper	Неподключен	0б			Неопределено		Выключено	Авто		Редактировать
4	gi1/0/4		1000M-copper	Подключен	1Гб	Полный	Включено	Неопределено	Выключено	Выключено	Перекрёстный		Редактировать
5	gi1/0/5		1000M-copper	Неподключен	0б			Неопределено		Выключено	Авто		Редактировать
6	gi1/0/6		1000M-copper	Неподключен	0б			Неопределено		Выключено	Авто		Редактировать
7	gi1/0/7		1000M-copper	Неподключен	0б			Неопределено		Выключено	Авто		Редактировать
8	gi1/0/8		1000M-copper	Подключен	1Гб	Полный	Включено	Неопределено	Выключено	Выключено	Перекрёстный		Редактировать
9	gi1/0/9		1000M-copper	Неподключен	0б			Неопределено		Выключено	Авто		Редактировать
10	gi1/0/10		1000M-copper	Неподключен	0б			Неопределено		Выключено	Авто		Редактировать

.....

26	te1/0/2		10G-FiberOptics	Неподключен	0б			Неопределено		Выключено	Прямой		Редактировать
27	te1/0/3		10G-FiberOptics	Неподключен	0б			Неопределено		Выключено	Прямой		Редактировать
28	te1/0/4		10G-FiberOptics	Неподключен	0б			Неопределено		Выключено	Прямой		Редактировать

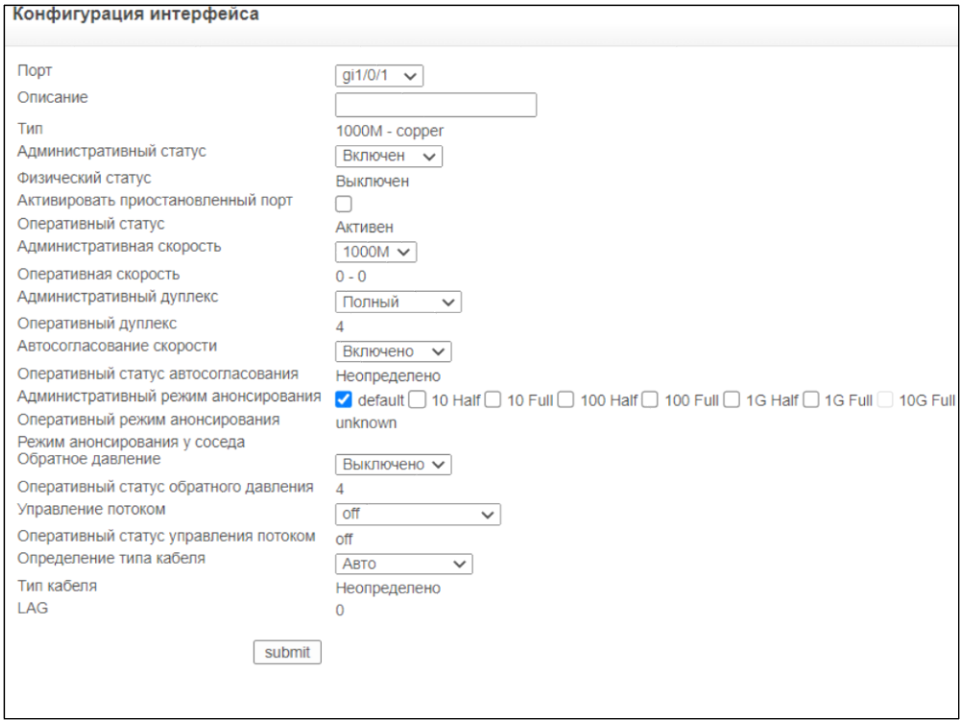
Сохранить

Для одновременной настройки нескольких портов нужно скопировать значения параметров из одной записи в другую/другие. Для этого нужно заполнить следующие поля и нажать кнопку «Сохранить»:

– *Копировать конфигурацию порта (номер строки)* — порядковый номер записи, параметры которой будут скопированы;

– *На порты (номера строк)* — порядковый номер/номера записей, для которых будут применены параметры. Можно указать диапазон через «—», либо перечислением через «,».

Для изменения настроек интерфейса нужно нажать кнопку «Редактировать» напротив заданной записи и заполнить соответствующие поля:



– *Порт* — номер интерфейса коммутатора;

– *Описание* — имя (описание) интерфейса;

– *Тип* — тип интерфейса (определяется автоматически):

  - *1000M-Copper* — подключение по медному Ethernet-кабелю, со скоростью до 1 Гбит/с;
  - *1000M-Combo* — комбинированный порт с двумя интерфейсами — под медный кабель и оптический кабель, скорость до 1Гбит/с;
  - *1000M-FiberOptics* — подключение по оптическому кабелю со скоростью до 1 Гбит/с;
  - *10G-FiberOptics* — подключение по оптическому кабелю со скоростью до 10 Гбит/с;

– *Административный статус* — административный статус интерфейса. Для передачи данных через интерфейс необходимо, чтобы интерфейс был включен:

  - *Включен* — интерфейс включен;
  - *Выключен* — интерфейс отключен;

– *Физический статус* — текущее состояние интерфейса;

– *Активировать приостановленный порт* — при установленном флаге происходит включение порта, который был приостановлен;

– *Оперативный статус* — оперативный статус (текущее состояние интерфейса):

  - *Активен* — интерфейс активен, соединение установлено;
  - *Неактивен* — интерфейс неактивен;

– *Административная скорость* — ручная настройка скорости передачи данных для интерфейса. Значение скорости определяется в зависимости от типа интерфейса. Скорость интерфейса может быть настроена вручную, только если отключено автоматическое согласование скорости;

– *Оперативная скорость* — текущая скорость передачи данных для интерфейса;

– *Административный дуплекс* — режим работы приемопередатчика. Этот параметр может быть настроен, только при отключенном автоматическом согласовании скорости:

- *Полный* — дуплекс;
- *Полудуплекс* — полудуплекс;

– *Оперативный дуплекс* — режим работы приемопередатчика;

– *Автосогласование скорости* — состояние автосогласования для скорости и дуплекса на настраиваемом интерфейсе:

- *Включено* — автосогласование включено;
- *Выключено* — автосогласование выключено;

– *Оперативный статус автосогласования* — текущее состояние автосогласования на интерфейсе;

– *Административный режим анонсирования* — административные параметры автосогласования, объявляемые встречному устройству:

- *default* — поддерживаются все скорости и настройки дуплексного режима;
- *10 Half* — поддерживается скорость 10 Мбит/с и полудуплексный режим;
- *10 Full* — поддерживается скорость 10 Мбит/с и дуплексный режим;
- *100 Half* — поддерживается скорость 100 Мбит/с и полудуплексный режим;
- *100 Full* — поддерживается скорость 100 Мбит/с и дуплексный режим;
- *1000 Full* — поддерживается скорость 1000 Мбит/с и дуплексный режим;
- *1000 Half* — поддерживается скорость 1000 Мбит/с и полудуплексный режим;

– *Обратное давление* — при установленном флаге включена функция «обратного давления» на настраиваемом интерфейсе, иначе — отключена;

– *Оперативный статус обратного давления* — текущее состояние функции «обратного давления» на настраиваемом интерфейсе;

– *Управление потоком* — режим управления потоком. Этот параметр может быть настроен, когда интерфейс находится в режиме полного дуплекса:

- *on* — режим включен;
- *off* — режим выключен;
- *Автосогласование* — включен режим автосогласования;

– *Оперативный статус управления потоком* — текущий режим управления потоком на интерфейсе;

– *Определение типа кабеля* — режим MDI/MDIX на интерфейсе позволяет устройству различать перекрестный кабель или кабель прямого подключения:

- *Авто* — автоматическое определение типа кабеля;
- *Прямой* — стандарт кабелей для подключения оконечных устройств;
- *Перекрестный* (Media-Dependent Interface with Crossover — перекрестный) — стандарт кабелей для подключения концентраторов и коммутаторов;

– *Тип кабеля* — текущий режим MDI/MDIX на интерфейсе;

– *LAG* — указывает, является ли интерфейс частью агрегированной группы LAG.

Нажмите кнопку «Сохранить» для применения настроек.

2.7.1.2 Управление группами агрегации каналов (LAG)

В разделе **Настройки L2 → Интерфейсы → Конфигурация LAG** выполняется настройка агрегированных интерфейсов LAG.

Агрегация каналов (Link Aggregation) — технология объединения нескольких физических каналов в один логический. Использование агрегации каналов способствует не только увеличению пропускной способности каналов между устройствами, но и повышению их надежности.

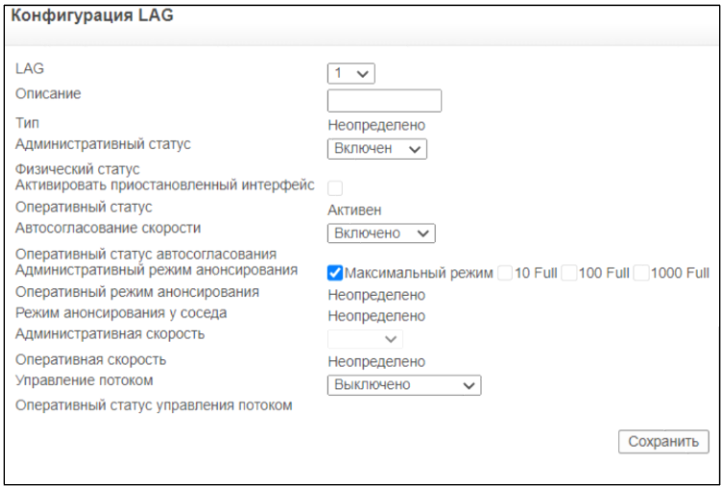
Устройство поддерживает два режима работы группы портов — статическая группа и группа, работающая по протоколу LACP.

Для одновременной настройки нескольких портов нужно скопировать значение параметров из одной записи в другую/другие. Для этого нужно заполнить следующие поля и нажать кнопку «Сохранить»:

– *Копировать конфигурацию порта (номер строки)* — порядковый номер записи, параметры которой будут скопированы;

– *На порты (номера строк)* — порядковый номер/номера записей, для которых будут скопиро–ваны параметры. Можно указать диапазон через «—», либо перечислением через «,».

Для изменения настроек группы LAG нужно нажать кнопку «Редактировать» напротив заданной записи и заполнить соответствующие поля:



– *LAG* — номер группы LAG, (1–48);

– *Описание* — имя (описание) группы LAG;

– *Тип* — тип интерфейса LAG, который определяется по первому добавленному порту в группу LAG;

– *Административный статус* — административный статус интерфейса LAG:

  ▪ *Включен* — интерфейс LAG включен;

  ▪ *Выключен* — интерфейс LAG отключен;

– *Физический статус* — текущий административный статус интерфейса LAG;

– *Активировать приостановленный интерфейс* — при установленном флаге происходит включение порта, который был приостановлен;

– *Оперативный статус* — оперативный статус (текущее состояние интерфейса):

  ▪ *Активен* — интерфейс активен, соединение установлено;

  ▪ Неактивен — интерфейс неактивен;

– *Автосогласование скорости* — состояние автосогласования для скорости и дуплекса на настраиваемом интерфейсе:

  • *Включено* — автосогласование включено;

  • *Выключено* — автосогласование выключено;

– *Оперативный статус автосогласования* — текущее состояние автосогласования на интерфейсе LAG;

– *Административный режим анонсирования* — параметры автосогласования, заданные администратором:

  ▪ *Максимальный режим* — поддерживаются все скорости и настройки дуплексного режима;

  ▪ *10 Full* — поддерживается скорость 10 Мбит/с и дуплексный режим;

  ▪ *100 Full* — поддерживается скорость 100 Мбит/с и дуплексный режим;

  ▪ *1000 Full* — поддерживается скорость 1000 Мбит/с и дуплексный режим;

– *Оперативный режим анонсирования* — параметры автосогласования, объявляемые интер–фейсом локального устройства;

– *Режим анонсирования у соседа* — параметры автосогласования, объявленные интерфейсом соседнего устройства;

– *Административная скорость* — ручная настройка скорости передачи данных интерфейса LAG. Допустимые значения скорости зависят от типа интерфейса. Скорость интерфейса может быть настроена вручную только при отключенном автоматическом согласовании параметров интерфейсов;

– *Оперативная скорость* — текущая скорость передачи данных для интерфейса LAG;

– *Управление потоком* — режим управления потоком:

  - *Включено* — режим включен;
  - *Выключено* — режим выключен;
  - *Автосогласование* — возможность управления потоком определяется в ходе процедуры автосогласования;

– *Оперативный статус управления потоком* — текущий режим управления потоком на интерфейсе.

Нажмите кнопку «Сохранить» для применения настроек.

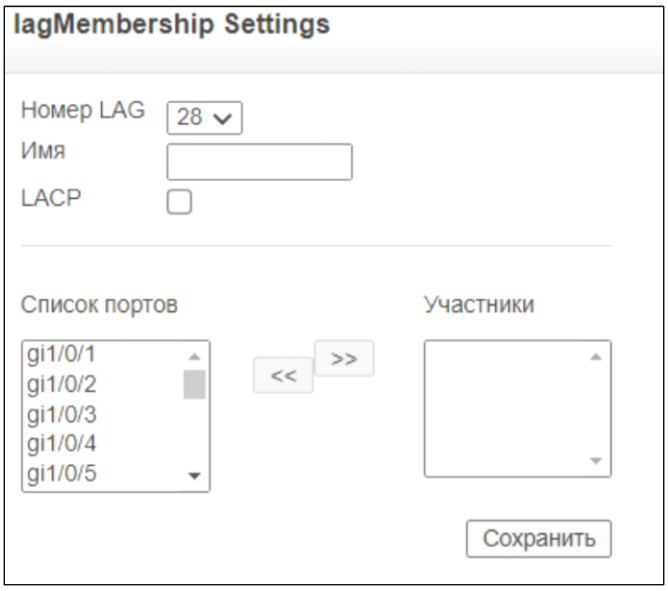
2.7.1.3 Управление составом группы LAG

В разделе **Настройки L2 → Интерфейсы → Членство LAG** формируется список интерфейсов, которые входят в состав группы LAG.

Коммутатор серии MES23xx/MES33xx/MES35xx/MES5324 обеспечивает поддержку до восьми интерфейсов Ethernet в одной группе портов LAG и до восьми групп LAG на устройстве или стеке устройств. Каждая группа портов должна состоять из интерфейсов Ethernet с одинаковой скоростью, работающих в дуплексном режиме с выключенным автосогласованием. Интерфейс не должен принадлежать VLAN и может быть только в одной группе LAG.

Все порты LAG имеют одинаковые правила фильтрации входящего трафика, правила тегирования, режим «обратного давления», режим управления потоком, приоритет интерфейса, тип трансивера. Если интерфейс добавлен в группу LAG, то его индивидуальные настройки не действительны. При удалении интерфейса из группы LAG индивидуальные настройки восстанавливаются.

Для изменения состава группы LAG нужно нажать кнопку «Редактировать» напротив заданной записи и заполнить соответствующие поля:



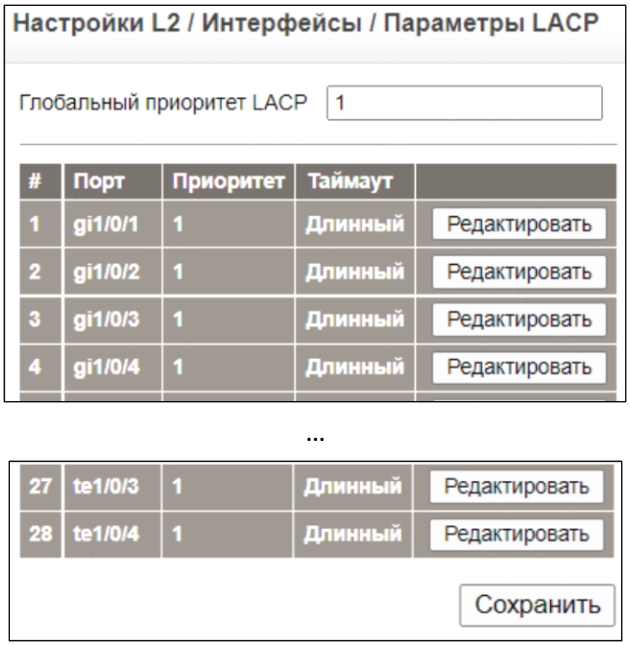
– *Номер LAG* — номер агрегированной группы LAG (1–48);
– *Имя LAG* — имя (описание) группы LAG;
– *LACP* — при установленном флаге включен механизм LACP, иначе — выключен;
– *Список портов* — список доступных интерфейсов;
– *Участники* — список интерфейсов, включенных в данную группу LAG;

Интерфейсы добавляются в список с помощью кнопки >>, удаляются из списка с помощью кнопки << .

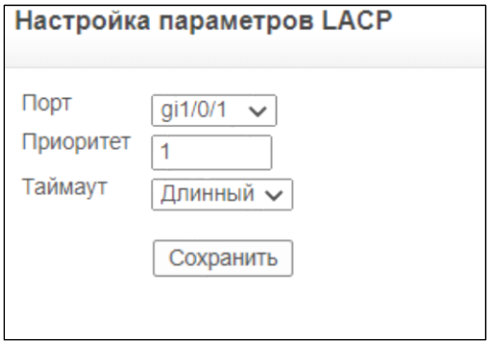
Нажмите кнопку «Сохранить» для применения настроек.

2.7.1.4 Настройка протокола агрегации каналов LACP

В разделе **Настройки L2 → Интерфейсы → Параметры LACP** выполняются настройки устройства для работы по протоколу LACP.



– *Глобальный приоритет LACP* — системный приоритет (1–65535). По умолчанию установлено 1;



– *Порт* — номер конфигурируемого интерфейса;

– *Приоритет* — LACP-приоритет для порта (1–65535);

– *Таймаут* — административный LACP-таймаут:

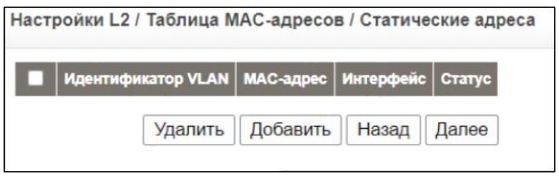
  - *Длинный* — длительное время таймаута;
  - *Короткий* — малое время таймаута.

Нажмите кнопку «Сохранить» для применения настроек.

2.7.2 Управление статической/динамической адресацией

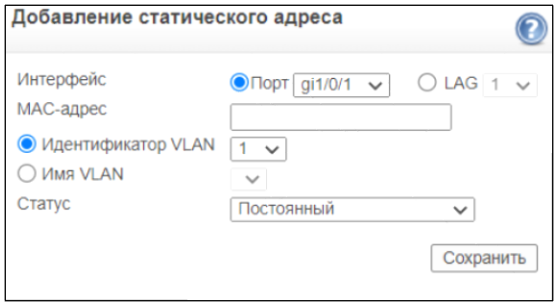
2.7.2.1 Настройка статической адресации

В разделе **Настройки L2 → Таблица MAC-адресов → Статические адреса** выполняется настройка статической адресации MAC—таблицы.



Для удаления статической записи из таблицы MAC-адресов установите флаг напротив заданной записи и нажмите кнопку «Удалить».

Для добавления статической записи в таблицу MAC-адресов нажмите кнопку «Добавить» и заполните соответствующие поля:

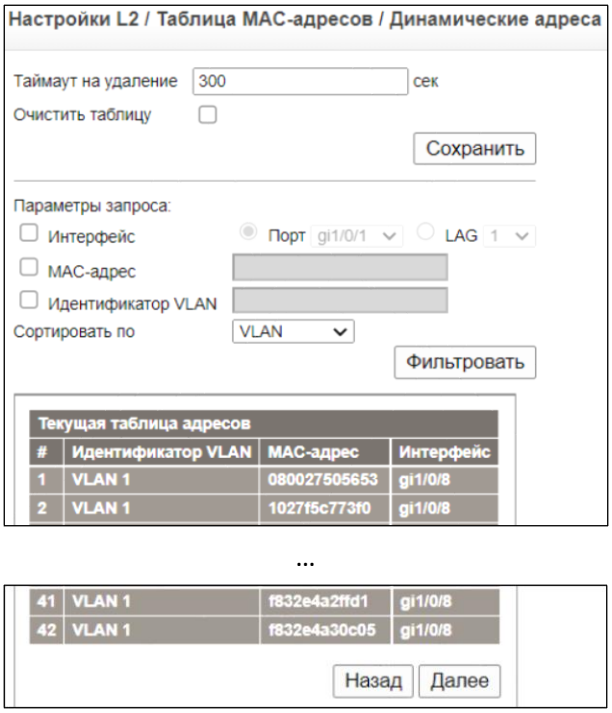


- *Интерфейс* — интерфейс, к которому применяется статический MAC-адрес;
  - *Порт* — номер Ethernet-интерфейса, для которого принимает значения gi0/1..gi0/48, te0/1 .. te0/4;
  - *LAG* — агрегированная группа портов LAG, принимает значение 1–12;
- *MAC-адрес* — MAC-адрес, который включен в текущий список статических адресов;
- *Идентификатор VLAN* — номер VLAN, к которому относится запись;
- *Имя VLAN* — имя VLAN, к которому относится запись;
- *Статус* — тип записи:
  - *Безопасный* — MAC-адрес остается постоянным, пока порт является заблокированным;
  - *Постоянный* — MAC-адрес остается постоянным;
  - *Удаление по перегрузке* — MAC-адрес будет удален после перезагрузки устройства;
  - *Удаление по таймату* — MAC-адрес будет удален по таймауту.

Нажмите кнопку «Сохранить» для применения настроек.

2.7.2.2 Настройка динамической адресации

В разделе **Настройки L2 → Таблица MAC-адресов → Динамические адреса** выполняется настройка динамической адресации MAC-таблицы.



– *Таумаут на удаление* — время хранения записи в таблице MAC-адресов, (1–630 секунд). По умолчанию установлено 300 секунд;

– *Очистить таблицу* — удаление записей из таблицы динамических MAC-адресов. Для удаления записей нужно установить флаг и нажать кнопку «Сохранить»;

Для того чтобы отобразить и отсортировать записи в MAC-таблице по одному из параметров установите один из следующих флагов и нажмите кнопку «Фильтровать»:

– *Интерфейс* — при установленном флаге будет активен фильтр записей по номеру интерфейса:

  ▪ *Порт* — фильтр по номеру Ethernet-интерфейса;

  ▪ *LAG* — фильтр по номеру группы LAG;

– *MAC-адрес* — при установленном флаге будет активен фильтр записей по заданному MAC-адресу;

– *Идентификатор VLAN* — при установленном флаге будет активен фильтр записей по заданному номеру VLAN;

– *Сортировать по* — параметр, по которому будет произведена сортировка: MAC-адрес, интерфейс, VLAN.

Нажмите кнопку «Сохранить» для применения настроек.

2.7.3 Настройка протоколов семейства Spanning Tree (STP, RSTP, MSTP)

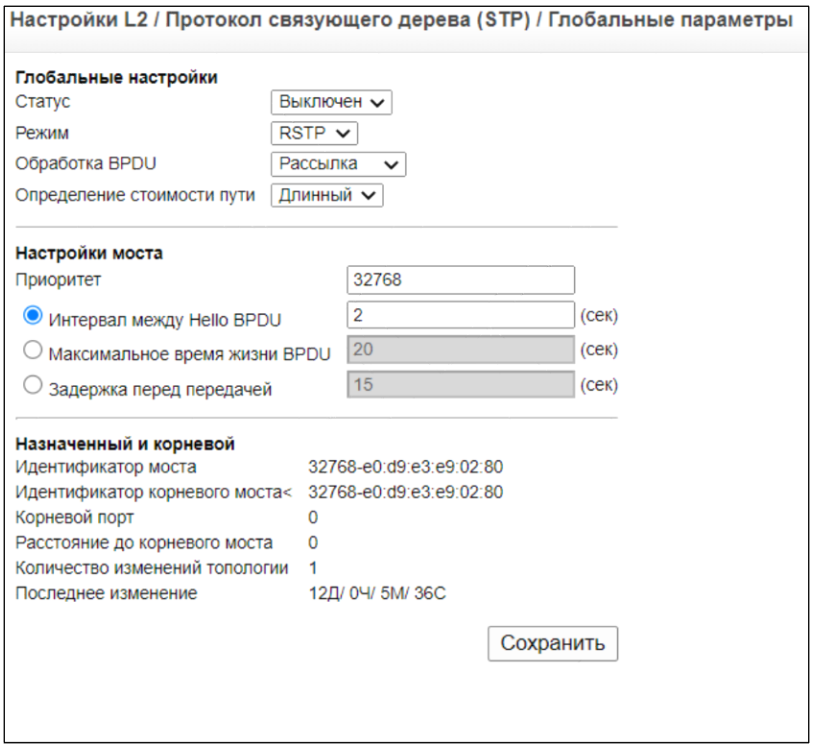
Spanning tree — алгоритм покрывающего дерева, который позволяет установить множество параллельных маршрутов между несколькими локальными сетями или сегментами сетей.

Коммутаторы используют алгоритм «Spanning tree», позволяя автоматически определять древовидную конфигурацию связей в сети без петель при произвольном соединении портов между собой. Конфигурация покрывающего дерева строится автоматически с использованием обмена служебными пакетами.

Коммутаторы серии MES23xx/MES33xx/MES35xx/MES5324 поддерживают протоколы STP (IEEE 802.1d), RSTP (IEEE 802.1w), MSTP (IEEE 802.1s).

2.7.3.1 Общие настройки STP

В разделе **Настройки L2 → Протокол связующего дерева (STP) → Глобальные параметры** выполняются общие настройки для работы устройства по протоколу STP.



Глобальные настройки — общие настройки STP:

– *Статус* — состояние функции STP на устройстве:

  - *Включен* — функция STP включена;
  - *Выключен* — функция STP выключена;

– *Режим* режим работы протокола STP:

  - *STP* — протокол покрывающего дерева (IEEE 802.1d STP). Установлено по умолчанию;
  - *RSTP* — быстрый протокол покрывающего дерева (IEEE 802.1w RSTP);

- *MSTP* — протокол, поддерживающий множество экземпляров покрывающего дерева (IEEE 802.1s MSTP);

– *Обработка BPDU* — режим обработки пакетов BPDU интерфейсом, на котором выключен протокол STP:

- *фильтрация* — на интерфейсе с выключенным протоколом STP BPDU-пакеты фильтруются;
- *рассылка* — на интерфейсе с выключенным протоколом STP нетегированные BPDU-пакеты передаются, тегированные — фильтруются;

– *Определение стоимости пути* — значения стоимости пути, используемые по умолчанию:

- *длинный* — значение ценности в диапазоне (1–200000000);
- *короткий* — значение ценности в диапазоне (1–65535).

Настройки моста:

– *Приоритет* — приоритет связующего дерева STP, (0–65535). Корневым коммутатором назначается коммутатор с меньшим приоритетом. По умолчанию установлено 32768. Значение приоритета должно быть кратно 4096;

– *Интервал между Hello BPDU* — интервал времени между передачами широковещательных сообщений «Hello» к взаимодействующим коммутаторам, (1–10). По умолчанию установлено 2;

– *Максимальное время жизни BPDU* — время жизни связующего дерева STP, (6–40). По умолчанию установлено 20 секунд;

– *Задержка перед передачей* — интервал времени, затрачиваемый на прослушивание и изучение состояний перед переключением в состояние передачи. По умолчанию установлено 10 секунд;

Назначенный и корневой — информация о корневом коммутаторе:

– *Идентификатор моста* — приоритет моста и MAC-адрес;

– *Идентификатор корневого моста* — приоритет корневого моста и MAC-адрес;

– *Корневой порт* — номер порта, который предлагает самую низкую стоимость пути от данного моста до корневого моста;

– *Расстояние до корневого моста* — стоимость пути от данного моста до корневого моста;

– *Количество изменений топологии* — общее количество изменений STP;

– *Последнее изменение* — время с момента последнего изменения топологии сети.

Нажмите кнопку «Сохранить» для применения настроек.

2.7.3.2 Настройка STP для определенного интерфейса

В разделе **Настройки L2 → Протокол связующего дерева (STP) → Параметры интерфейсов** сетевой администратор может выполнить настройку STP для определенного интерфейса.

При установленном флаге «Порты» будет отображена таблица для портов коммутатора, при установленном флаге «LAG» — таблица для групп LAG.

Настройки L2 / Протокол связующего дерева (STP) / Параметры интерфейсов

Порты LAG

#	Порт	STP	Быстрый переход	Включить защиту корневого моста	Включить защиту от несанкционированных BPDU	Состояние порта	Роль порта	Скорость	Стоимость	Приоритет	Идентификатор назначенного моста	Идентификатор назначенного порта	Стоимость назначенного порта	Количество переходов в пересылающее состояние	LAG	
1	gi1/0/1	Выключен	Авто	Выключен	Выключен	Выключен	Выключен	Неопределено	2000000	128	Неопределено	Неопределено	Неопределено	Неопределено		Редактировать
2	gi1/0/2	Включен	Авто	Выключен	Выключен	Выключен	Выключен	Неопределено	2000000	128	Неопределено	Неопределено	Неопределено	Неопределено		Редактировать
3	gi1/0/3	Включен	Авто	Выключен	Выключен	Выключен	Выключен	Неопределено	2000000	128	Неопределено	Неопределено	Неопределено	Неопределено		Редактировать
4	gi1/0/4	Включен	Авто	Выключен	Выключен	Выключен	Выключен	1Гб	20000	128	Неопределено	Неопределено	Неопределено	Неопределено		Редактировать
5	gi1/0/5	Включен	Авто	Выключен	Выключен	Выключен	Выключен	Неопределено	2000000	128	Неопределено	Неопределено	Неопределено	Неопределено		Редактировать
6	gi1/0/6	Включен	Авто	Выключен	Выключен	Выключен	Выключен	Неопределено	2000000	128	Неопределено	Неопределено	Неопределено	Неопределено		Редактировать
7	gi1/0/7	Включен	Авто	Выключен	Выключен	Выключен	Выключен	Неопределено	2000000	128	Неопределено	Неопределено	Неопределено	Неопределено		Редактировать

Для изменения настроек нажмите кнопку «Редактировать» напротив заданной записи и заполните соответствующие поля:

Настройки интерфейса

Порт	gi1/0/1
STP	Выключен
Быстрый переход	Авто
Включить защиту корневого моста	☐
Включить защиту от несанкционированных BPDU	☐
Состояние порта	Выключен
Скорость	Неопределено
Стоимость	2000000
Стоимость по умолчанию	☐
Приоритет	128
Идентификатор назначенного моста	Неопределено
Идентификатор назначенного порта	Неопределено
Стоимость назначенного порта	Неопределено
Количество переходов в пересылающее состояние	Неопределено
LAG	

Сохранить

- *Порт* — номер Ethernet-интерфейса;
- *STP* — режим работы протокола STP на интерфейсе:
  - *Включен* — протокол STP включен;
  - *Выключен* — протокол STP отключен;
- *Быстрый переход* — состояние режима, в котором порт при поднятии на нем линка сразу становится в состояние передачи, не дожидаясь истечения таймера:
  - *Авто — действие по умолчанию;*
  - *Включен* — режим включен;
  - *Выключен* — режим выключен;

– *Включить защиту корневого моста* — при установленном флаге включена защита корневого коммутатора для всех связующих деревьев STP выбранного порта, иначе — защита отключена. Данная защита запрещает интерфейсу быть корневым портом коммутатора и, таким образом, переопределять назначенный ранее корневой порт;

– *Включить защиту от несанкционированных BPDU* — при установленном флаге разрешена защита, выключающая интерфейс при приёме пакетов BPDU;

– *Состояние порта* — текущее состояние работы протокола STP на интерфейсе:

  - *Forwarding* — протокол STP разрешен на порту и порт транслирует пакеты в соответствии с топологией STP;
  - *Disabled* — протокол STP отключен на интерфейсе;
  - *Blocking* — интерфейс заблокирован и не может пересылать трафик или изучать MAC-адреса;
  - *Listening* — порт в режиме прослушивания. В этом состоянии порт не транслирует трафик. Для этого порта не выполняется изучение MAC-адресов;
  - *Learning* — порт в состоянии обучения. Порт не транслирует трафик, но может изучать новые MAC-адреса;

– *Скорость* — текущая скорость передачи данных для интерфейса;

– *Стоимость* — стоимость пути через конфигурируемый интерфейс;

– *Стоимость по умолчанию* — при установленном флаге задается ценность пути по умолчанию, см таблицу 2.2;

– *Приоритет* — приоритет интерфейса в связующем дереве STP, (0–240). Значение приоритета должно быть кратно 16. По умолчанию установлено 128;

– *Идентификатор назначенного моста* — идентификатор назначенного моста;

– *Идентификатор назначенного порта* — идентификатор назначенного порта;

– *Стоимость назначенного порта* — стоимость назначенного порта, участвующего в топологии STP;

– *Количество переходов в пересылающее состояние* — количество переходов интерфейса из состояния Forwarding в состояние Blocking;

– *LAG* — группа LAG, к которой принадлежит порт.

Нажмите кнопку «Сохранить» для применения настроек.

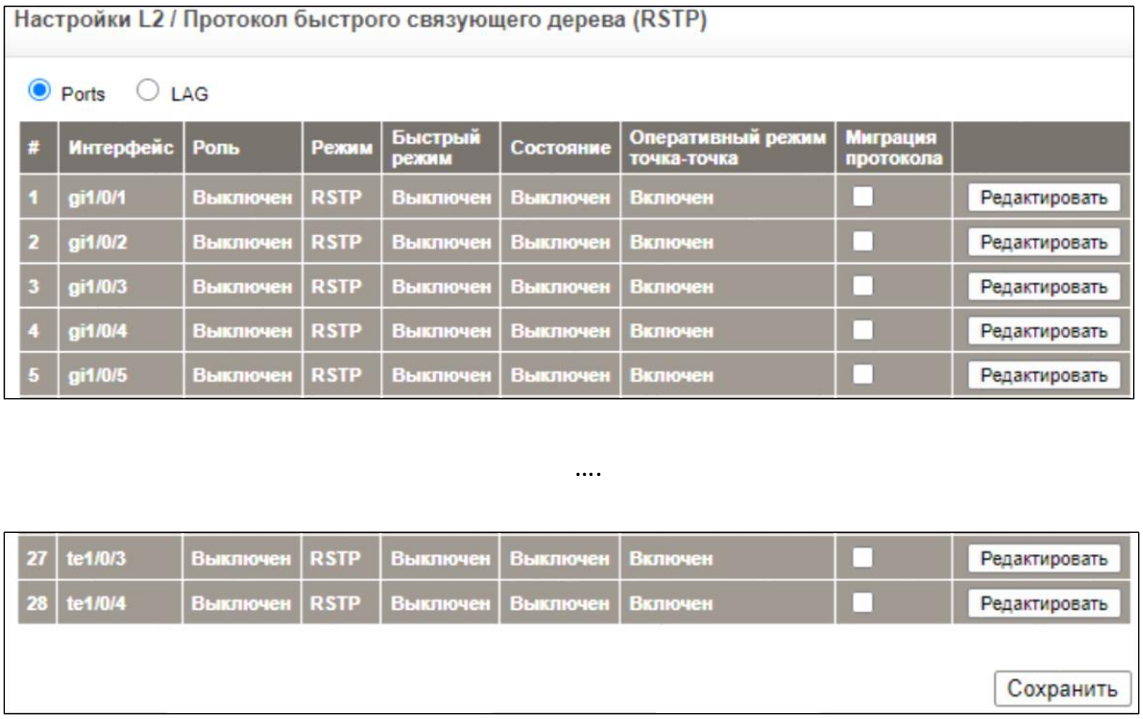
Таблица 2.2 — Ценность пути, установленная по умолчанию (spanning—tree cost)

Интерфейс	***Метод определения ценности пути***	
	Длинный	***Короткий***
Port-channel	20000	4
TenGigabit Ethernet (10000 Mbps)	2000	2
Gigabit Ethernet (1000 Mbps)	20000	4

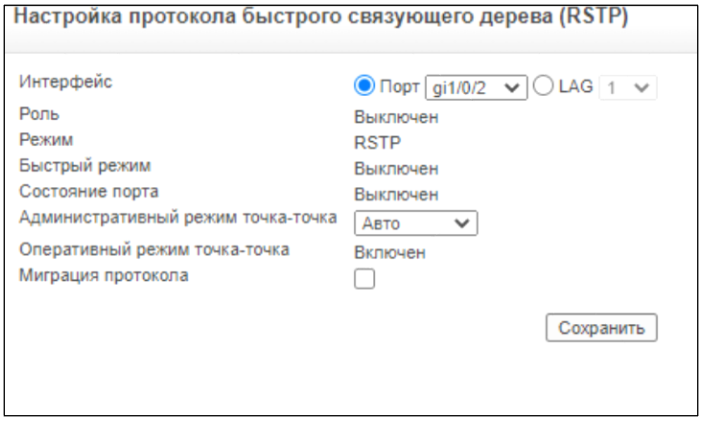
2.7.4 Настройка протокола Rapid STP

В разделе **Настройки L2 → Протокол быстрого связующего дерева (RSTP)** выполняется настройка параметров устройства для работы по быстрому протоколу покрывающего дерева (RSTP).

При установленном флаге «Ports» будет отображена таблица для портов коммутатора, при установленном флаге «LAGs» — таблица для групп LAG.



Для редактирования параметров определенного интерфейса нужно нажать кнопку «Редактировать» напротив записи и заполнить следующие поля:



– *Интерфейс* — интерфейс, для которого выполняются настройки RSTP;

  - *Порт* — номер Ethernet-интерфейса, (gi0/1..gi0/48, te0/1 .. te0/4);
  - *LAG* — агрегированная группа портов LAG, (1–48);

– *Роль* — роль порта в топологии STP в соответсвии с IEEE802.1D:

- *Корневой* — порт с наименьшей стоимостью пути до корневого коммутатора;
- *Назначенный* — интерфейс или группа LAG, через который назначенный коммутатор подключен к LAN;
- *Дополнительный* — альтернативный путь к корневому коммутатору от корневого интерфейса;
- *Резервный* — резервный путь для назначенного порта. В случае перехода designated-порта в нерабочее состояние, backup-порт будет использован для подключения к тому же сегменту сети;
- *Выключен* — порт не участвует в Spanning Tree;

– *Режим* — режим работы протокола STP — RapidSTP;

– *Быстрый режим* — рабочее состояние «Fast Link» (включен/выключен) на интерфейсе или группе LAG. Если на интерфейсе включен режим «Fast Link», то интерфейс автоматически переводится в состояние передачи данных при активации порта (link up);

– *Состояние порта* — состояние порта;

- *Forwarding* — протокол STP разрешен на порту и порт транслирует пакеты в соответствии с топологией STP;
- *Disabled* — протокол STP отключен на интерфейсе;
- *Blocking* — интерфейс заблокирован и не может пересылать трафик или изучать MAC-адреса;
- *Listening* — порт в режиме прослушивания. В этом состоянии порт не транслирует трафик и изучение MAC-адресов для этого порта не выполняется;
- *Learning* — порт в состоянии обучения. Порт не транслирует трафик, но может изучать новые MAC-адреса;

– *Административный режим точка-точка* — состояние соединения точка-точка:

- *Авто* — автоматическое определение типа соединения, определение происходит на основании режима дуплекса. Для дуплексного порта устанавливается тип «точка-точка», для полудуплексного — «разветвленный»;
- *Включен* — на устройстве разрешено устанавливать соединение «точка-точка» и состояние интерфейса определяется по результатам работы протокола LCP (Link Control Protocol) при установлении и закрытии PPP-соединения;
- *Выключен* — на устройстве разрешен тип соединения «разветвленный».

– *Оперативный режим точка-точка* — оперативный статус соединения «точка-точка»;

– *Миграция протокола* — при установленном флаге включена отправка LCP-пакетов для настройки и тестирования канала передачи данных, иначе — отправка LCP-пакетов запрещена.

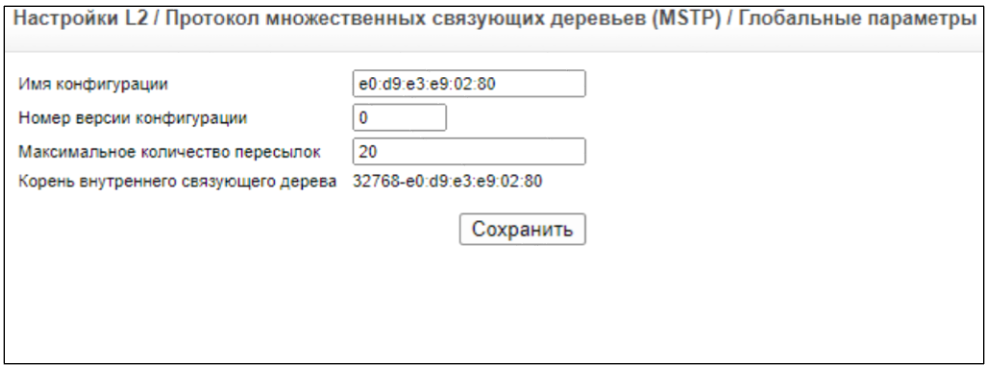
Нажмите кнопку «Сохранить» для применения настроек.

2.7.5 Настройка протокола Multiple STP

В разделе **Настройки L2 → Протокол множественных связующих деревьев (MSTP)** выполняется настройка параметров устройства для работы по протоколу нескольких экземпляров покрывающего дерева (MSTP).

2.7.5.1 Настройка общих параметров для MSTP

В разделе **Настройки L2 → Протокол множественных связующих деревьев (MSTP) → Глобальные параметры** устанавливаются общие параметры для работы по протоколу MSTP.



– *Имя конфигурации* — идентификатор области MSTP. Если значение поля не задано, то по умолчанию будет установлено значение MAC-адреса устройства;

– *Номер версии конфигурации* — номер ревизии текущей конфигурации MSTP. Допустимый диапазон значений (0–65535);

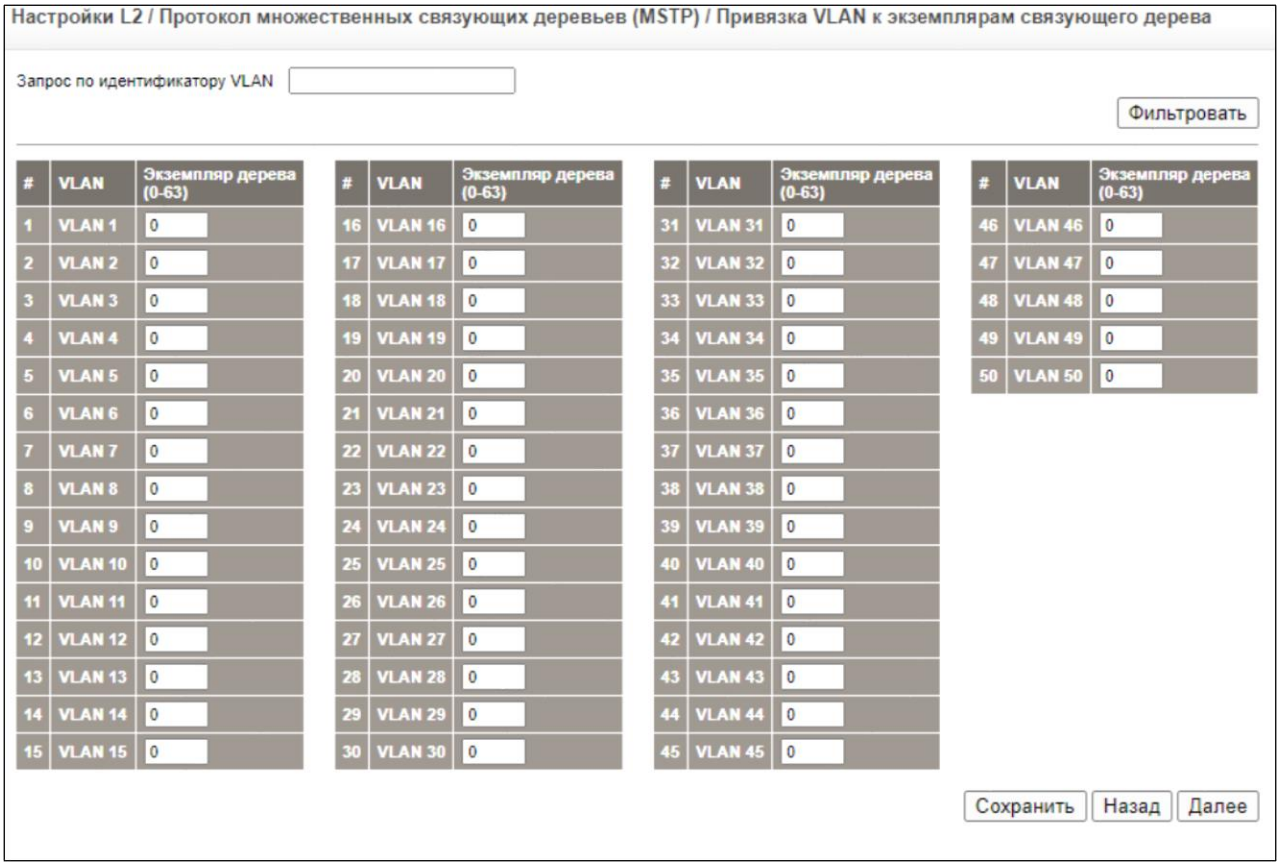
– *Максимальное количество пересылок* — максимальное количество транзитных участков для пакета BPDU, необходимых для формирования дерева и удержания информации о его строении. Если пакет уже прошел максимальное количество транзитных участков, то на следующем участке он отбрасывается. Допустимый диапазон значений от 1 до 40, значение по умолчанию — 20;

– *Корень внутреннего связующего дерева* — идентификатор мастера (root) внутреннего связующего дерева.

Нажмите кнопку «Сохранить» для применения настроек.

2.7.5.2 Привязка VLAN к экземплярам MSTP

В разделе **Настройки L2 → Протокол множественных связующих деревьев (MSTP) → Привязка VLAN к экземплярам связующего дерева** устанавливается соответствие между VLAN и экземплярами протокола MSTP.



Для того чтобы отобразить и отсортировать записи в таблице по номеру VLAN, введите в поле «Запрос по идентификатору VLAN» номер VLAN и нажмите кнопку «Фильтровать».

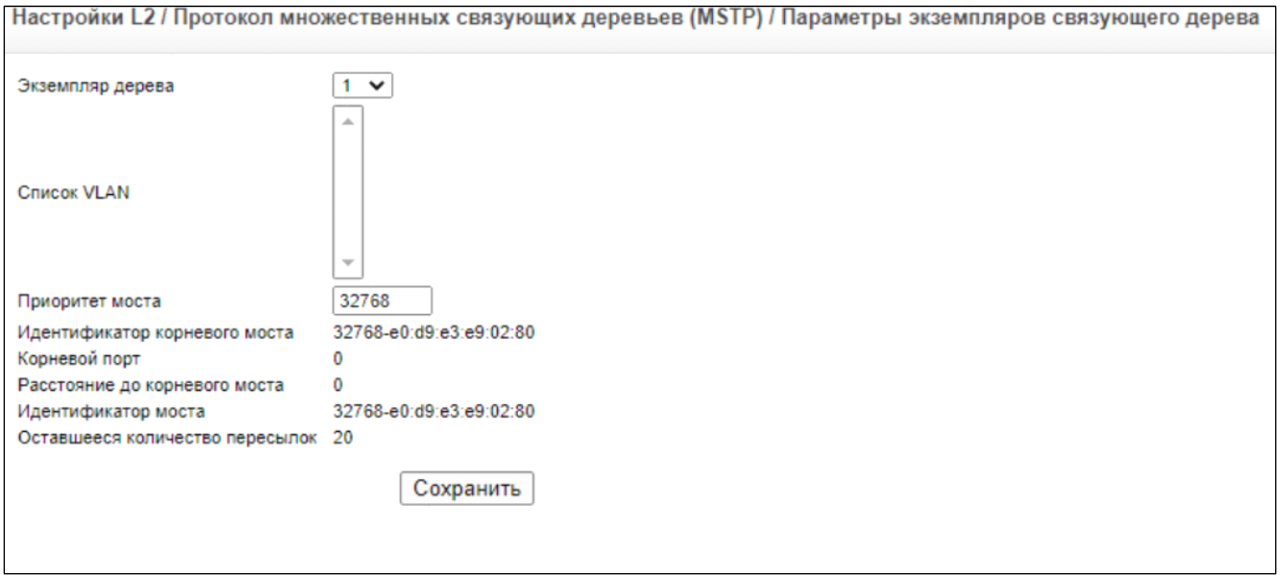
– *VLAN* — идентификатор VLAN;

– *Экземпляр дерева* — идентификационный номер экземпляра протокола MSTP, (0–64).

Нажмите кнопку «Сохранить» для применения настроек.

2.7.5.3 Настройка экземпляров покрывающего дерева

В разделе **Настройки L2 → Протокол множественных связующих деревьев (MSTP) → Параметры экземпляров связующего дерева** выполняется настройка приоритета для данного коммутатора перед остальными, использующими общий экземпляр MSTP.

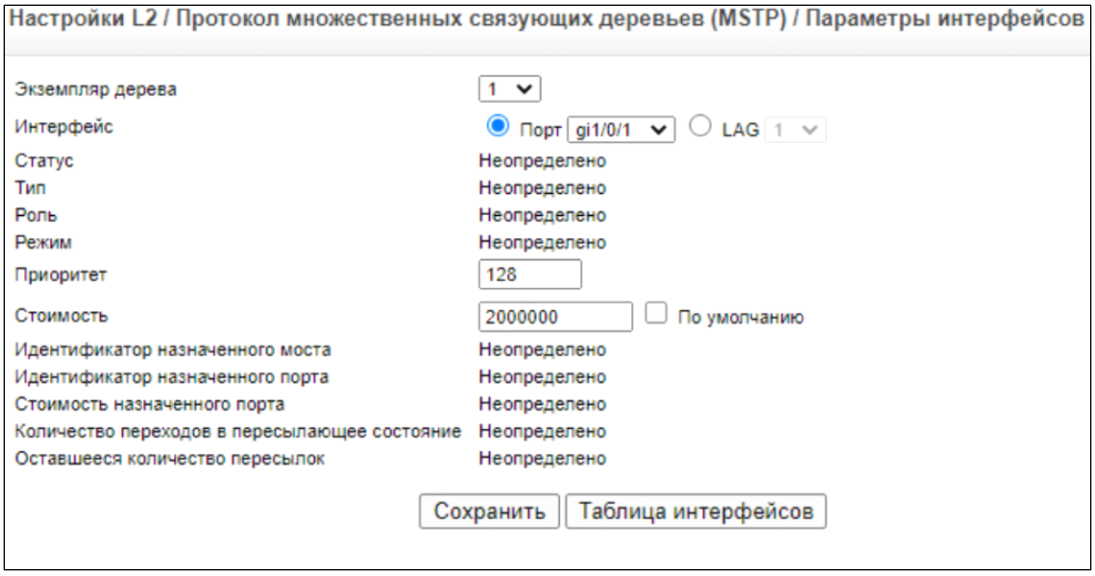


- *Экземпляр дерева* — номер экземпляра MSTP;
- *Список VLAN* — номера VLAN, для которых определен данный номер экземпляра MSTP;
- *Приоритет моста* — приоритет для данного коммутатора перед остальными, использующими общий экземпляр MSTP, (0–61440);
- *Идентификатор корневого моста* — идентификационный номер для корневого моста;
- *Корневой порт* — корневой порт для данного экземпляра;
- *Расстояние до корневого моста* — стоимость пути к корневому мосту для данного экземпляра;
- *Идентификатор моста* — приоритет моста для данного экземпляра;
- *Оставшееся количество пересылок* — количество транзитных участков, оставшихся перед следующем получателем.

Нажмите кнопку «Сохранить» для применения настроек.

2.7.5.4 Настройка экземпляров MSTP

В разделе **Настройки L2 → Протокол множественных связующих деревьев (MSTP) → Параметры интерфейсов** выполняются настройки MSTP для портов. На уровне портов STP блокирует избыточные связи внутри STP-группы.



– *Экземпляр дерева* — номер экземпляра MSTP, настроенный на устройстве, (0–64);

– *Интерфейс* — интерфейс, для которого выполняются настройки MSTP:

  - *Порт* — номер порта;
  - *LAG* — номер группы LAG;

– *Статус* — состояние интерфейса для заданного экземпляра MSTP:

  - *Включен* — интерфейс включен;
  - *Выключен* — интерфейс отключен;

– *Тип* — тип порта:

  - *Граничный* — пограничный порт. Если интерфейс является пограничным, то в этом поле также указывается режим работы устройства (STP, RSTP) на другой стороне;
  - *Мастер* — основной порт;

– *Роль* — роль порта, назначенная алгоритмом STP:

  - *Корневой* — порт с наименьшей стоимостью пути до корневого коммутатора;
  - *Назначенный* — интерфейс или номер группы LAG, через который назначенный коммутатор подключен к LAN;
  - *Дополнительный* — альтернативный относительно root-порта путь к корневому коммутатору;
  - *Резервный* — резервный порт для назначенного (designated) порта;
  - *Выключен* — порт не участвует в Spanning Tree;

- *Режим* — режим работы протокола STP — MSTP;
- *Приоритет* — приоритет интерфейса для определенного экземпляра. По умолчанию установлено 128;
- *Стоимость* — стоимость пути через выбранный интерфейс, для определенного экземпляра протокола MSTP, (1–200 000 000);
- *По умолчанию* — при установленном флаге будет задана стоимость пути по умолчанию, таблица 2.2;
- *Идентификатор назначенного моста* — идентификатор назначенного моста;
- *Идентификатор назначенного порта* — идентификатор назначенного порта;
- *Стоимость назначенного порта* — стоимость назначенного порта;
- *Количество переходов в пересылающее состояние* — количество изменений на интерфейсе при переходе из состояния «Forwarding» в состояние «Blocking»;
- *Оставшееся количество пересылок* — количество транзитных участков, оставшихся до следующего места назначения.

Нажмите кнопку «Сохранить» для применения настроек.

2.7.6 Настройка виртуальных локальных сетей (VLAN)

В данном разделе описывается настройка виртуальной локальной сети:

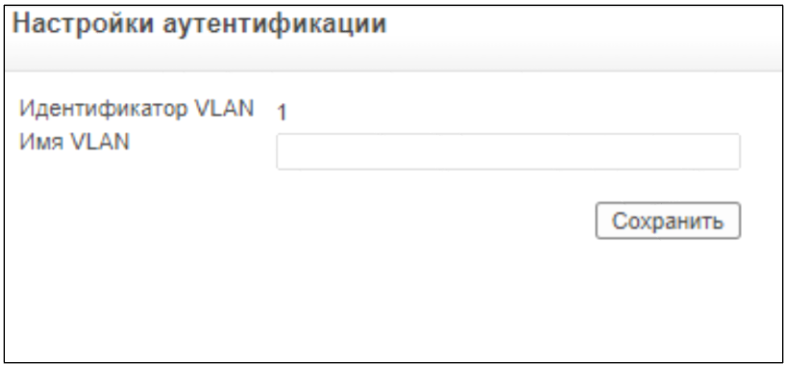
– определяются свойства VLAN;
– принадлежность интерфейсов к VLAN;
– настройка интерфейсов VLAN.

2.7.6.1 Общие настройки VLAN

В разделе **Настройки L2 → VLAN → Настройка** выполняются общие настройки статической VLAN.

Для создания новой VLAN нужно нажать кнопку «Добавить», заполнить соответствующие поля и нажать кнопку «Сохранить» для применения настроек.

Для редактирования параметров нужно нажать кнопку «Редактировать», изменить необходимые параметры и нажать кнопку «Сохранить» для применения настроек.

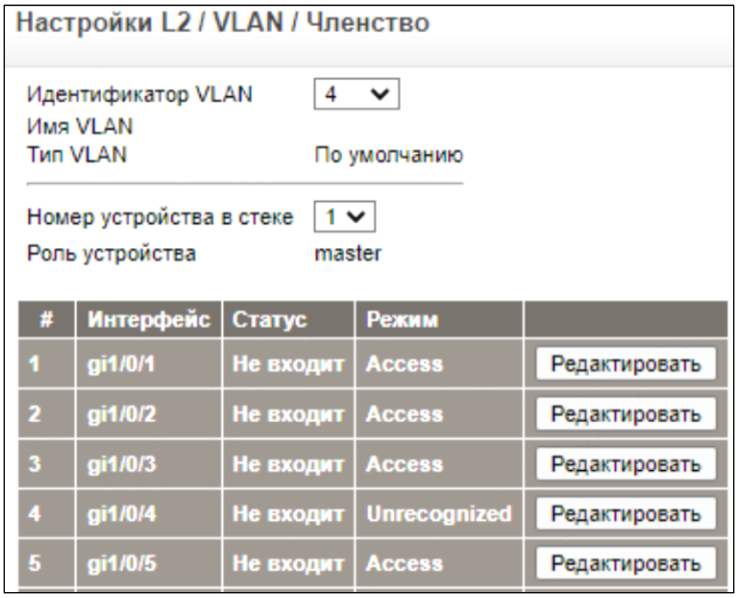


– *Идентификатор VLAN* — идентификационный номер VLAN, (2–4094);

– *Имя VLAN* — имя VLAN.

2.7.6.2 Установка принадлежности интерфейсов к VLAN

В разделе **Настройки L2 → VLAN → Членство** можно просмотреть/изменить таблицу принадлежности интерфейсов к VLAN.



– *Идентификатор VLAN* — в ниспадающем списке необходимо выбрать номер VLAN, для которой будет отображена конфигурация;

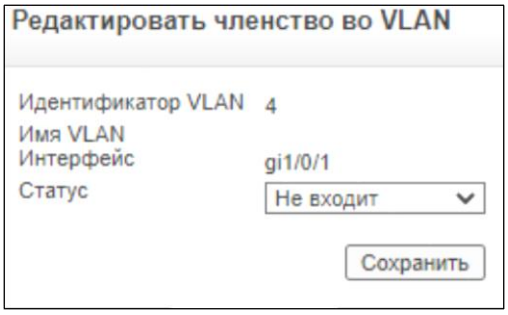
– *Имя VLAN* — имя VLAN;

– *Тип VLAN* — тип VLAN:

  - *Динамическая* — VLAN была задана динамически через GARP;
  - *Статическая* — VLAN была задана пользователем (статически);

- *По умолчанию* — VLAN установлена по умолчанию.

Для изменения настроек интерфейса нажмите кнопку «Редактировать» и заполнить следующие поля:



– *Статус* — состояние интерфейса:

  - *Не входит* — интерфейс не принадлежит текущей VLAN, но может быть добавлен к VLAN через GARP;

  - *Запрещен* — интерфейс не принадлежит текущей VLAN и не может быть добавлен к VLAN через GARP;

  - *Нетегированный* — интерфейс принадлежит данной VLAN. Пакеты, передаваемые через данный интерфейс, не тегируются;

  - *Тегированный* — интерфейс принадлежит данной VLAN. Пакеты, передаваемые через данный интерфейс, тегируются.

Нажмите кнопку «Сохранить» для применения настроек.

2.7.6.3 Настройки VLAN для интерфейсов коммутатора

В разделе **Настройки L2 → VLAN → Параметры интерфейсов** выполняются настройки VLAN для интерфейсов коммутатора.

Настройки L2 / VLAN / Параметры интерфейсов

Порты LAG

#	Интерфейс	Режим	PVID	Типы пакетов	Входная фильтрация	Зарезервированные VLAN	VLAN по умолчанию	
1	gi1/0/1	Access	1	Разрешить все	Включена		Разрешён / Нетегированный	Редактировать
2	gi1/0/2	Access	1	Разрешить все	Включена		Разрешён / Нетегированный	Редактировать
3	gi1/0/3	Access	1	Разрешить все	Включена		Разрешён / Нетегированный	Редактировать
4	gi1/0/4	Trunk	10	Разрешить все	Включена		Разрешён / Нетегированный	Редактировать
5	gi1/0/5	Access	1	Разрешить все	Включена		Разрешён / Нетегированный	Редактировать
6	gi1/0/6	Access	1	Разрешить все	Включена		Разрешён / Нетегированный	Редактировать
7	gi1/0/7	Access	1	Разрешить все	Включена		Разрешён / Нетегированный	Редактировать
8	gi1/0/8	Access	1	Разрешить все	Включена		Разрешён / Нетегированный	Редактировать
9	gi1/0/9	Access	1	Разрешить все	Включена		Разрешён / Нетегированный	Редактировать
10	gi1/0/10	Access	1	Разрешить все	Включена		Разрешён / Нетегированный	Редактировать
11	gi1/0/11	Trunk	1	Разрешить все	Включена		Разрешён / Нетегированный	Редактировать
12	gi1/0/12	Access	1	Разрешить все	Включена		Разрешён / Нетегированный	Редактировать
13	gi1/0/13	Access	1	Разрешить все	Включена		Разрешён / Нетегированный	Редактировать
14	gi1/0/14	Access	1	Разрешить все	Включена		Разрешён / Нетегированный	Редактировать

При установленном флаге «Порты» будет отображена таблица для портов коммутатора, при установленном флаге «LAG» — таблица для групп LAG.

Для изменения настроек интерфейса нужно нажать кнопку «Редактировать» и заполнить следующие поля:

Настройка параметров интерфейса

Интерфейс: gi1/0/1
Режим: Access
PVID: 1
Типы пакетов: Разрешить все
Входная фильтрация: Включена
Текущие зарезервированные VLAN
VLAN по умолчанию запрещён
VLAN по умолчанию тегированный

Сохранить

– *Интерфейс* — номер интерфейса (gi0/1—gi0/48, te0/1—te0/4), либо группы LAG;

– *Режим* — режим работы интерфейса:

  - *General* — интерфейс с полной поддержкой 802.1q, принимает как тегированный, так и нетегированный трафик;

- *Access* — интерфейс доступа — нетегированный интерфейс для одной VLAN;
- *Trunk* — интерфейс, принимающий только тегированный трафик, за исключением одного VLAN*;*
- *Customer* — интерфейс, позволяющий создавать 802.1Q туннели. Интерфейс принад–лежит только к одной VLAN (Native VLAN). Весь принимаемый трафик (тегированный и нетегированный) помещается в Native VLAN. Исходящий трафик передается на интерфейс без тега Native VLAN. При установке режима работы «general» для редактирования станут доступны следующие поля:

– *PVID* — номер VLAN порта, (1–4094). Весь нетегированный трафик, поступающий на данный порт, определяется в данную VLAN;

– *Типы пакетов* — тип пакетов, которые принимаются на основном интерфейсе:

- *Разрешить только тегированные* — принимать только тегированные пакеты;
- *Разрешить все* — принимать все пакеты;

– *Входная фильтрация* — состояние фильтрации входящих пакетов на основе присвоенного им значения VLAN ID:

- *Включена* — включена фильтрация входящих пакетов. В этом случае пакеты, которые не входят в группу VLAN с присвоенным им значением VLAN ID, отбрасываются;
- *Выключена* — фильтрация отключена;

– *Текущие зарезервированные VLAN* — текущая резервная VLAN;

– *VLAN по умолчанию запрещён* — запретить добавление дефолтной VLAN;

– *VLAN по умолчанию тегированный* — сделать тегированным дефолтный VLAN.

Нажмите кнопку «Сохранить» для применения настроек.

2.7.6.4 Настройка протокола GARP

В разделе **Настройки L2 → VLAN → Настройки GARP** выполняется настройка параметров устройства для работы по протоколу GARP.

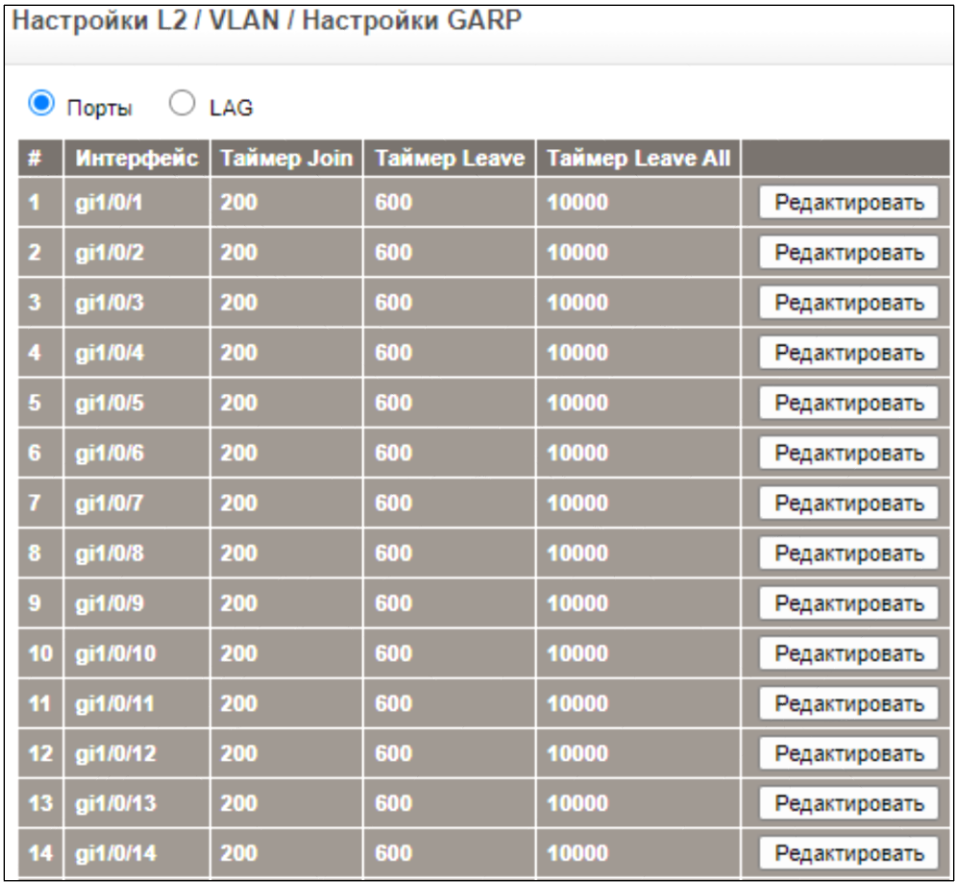
Протокол GARP (Generic Attribute Registration Protocol) — базовый протокол, который используется в коммутаторах серии MES23xx/MES33xx/MES35xx/MES5324 для регистрации (перерегистрации) специальных атрибутов, таких как идентификаторы VLAN и членство в многоадресных группах.

Для настройки протокола GARP необходимо, чтобы выполнялись следующие условия:

– Значение Leave-таймера (отключение) должно быть больше или равно трем значениям Join-таймера (установление соединения);

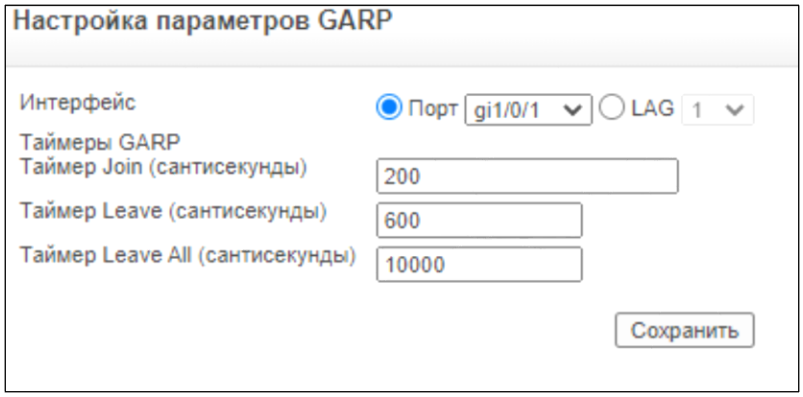
– Значение LeaveAll-таймера должно быть намного больше значения Leave-таймера;

– Значения Join-таймеров должно быть одинаковым для всех взаимодействующих устройств. Если значения таймеров будут отличаться, то коммутатор может некорректно работать по протоколу GVRP.



При установленном флаге «Порты» будет отображена таблица для портов коммутатора, при установленном флаге «LAG» — таблица для групп LAG.

Для изменения настроек интерфейса нужно нажать кнопку «Редактировать» и заполнить следующие поля:



– *Интерфейс* — интерфейс, на котором включен GARP:

- *Порт* — номер интерфейса, (gi0/1—gi0/48, te0/1—te0/4);
- *LAG* — номер группы LAG, (1–48);

– *Таймер Join (сантисекунды)* — интервал передачи запросов на присоединение в группу VLAN. По умолчанию установлено 200 миллисекунд;

– *Таймер Leave (сантисекунды)* — интервал времени, в течение которого интерфейс будет ожидать перед выходом из группы VLAN. Значение Leave-таймера должно быть больше или равно трем значениям Join-таймера. По умолчанию установлено 600 миллисекунд;

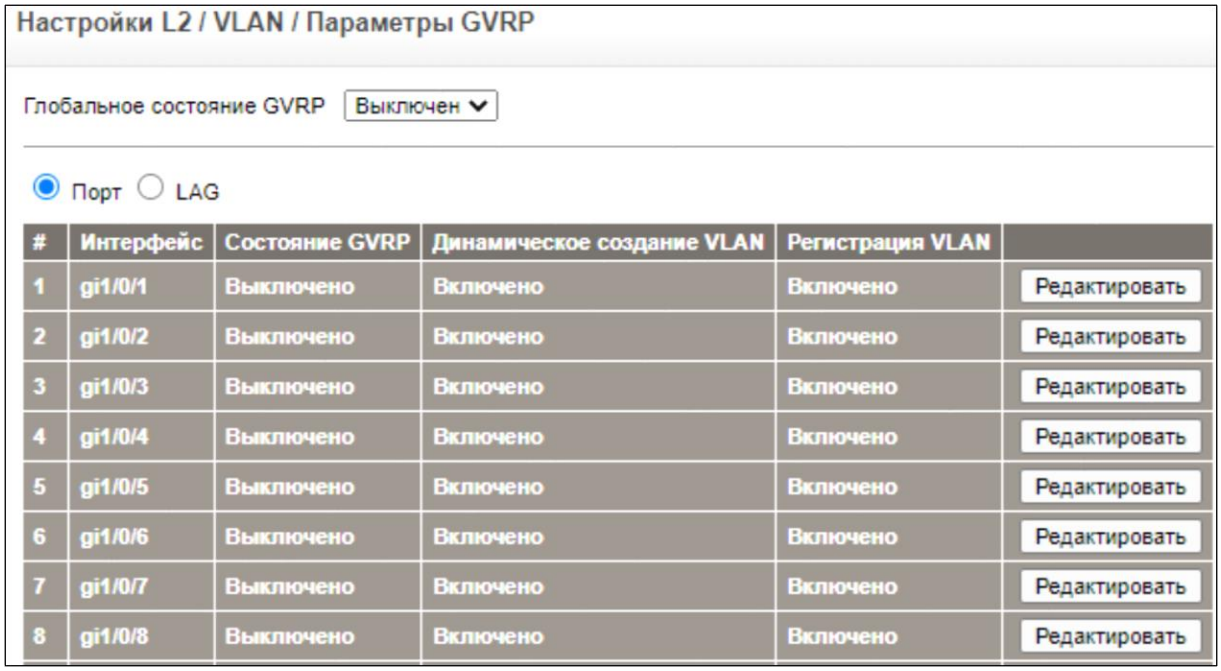
– *Таймер Leave All (сантисекунды)* — интервал времени, в течение которого интерфейс будет ожидать перед отправкой запроса «LeaveAll» на полное отключение от группы VLAN. Значение LeaveAll-таймера должно быть намного больше значения Leave-таймера. По умолчанию установлено 10000 миллисекунд.

Нажмите кнопку «Сохранить» для применения настроек.

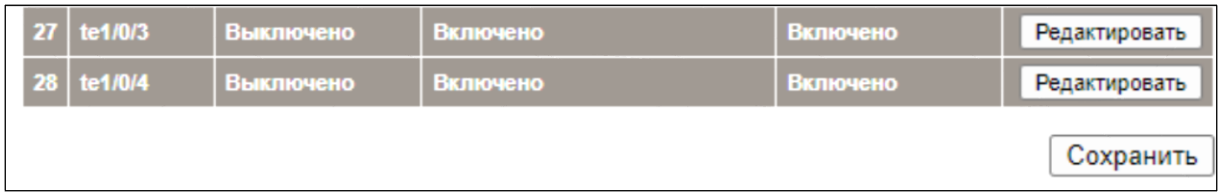
2.7.6.5 Настройка протокола GVRP

В разделе **Настройки L2 → VLAN → Параметры GVRP** выполняется настройка параметров устройства для работы по протоколу GVRP.

Протокол *GVRP (GARP VLAN Registration Protocol)* — протокол регистрации VLAN по GARP. Используется в коммутаторах серии MES23xx/MES33xx/MES35xx/MES5324 для регистрации VLAN, которых нет в текущей базе данных коммутатора.



....

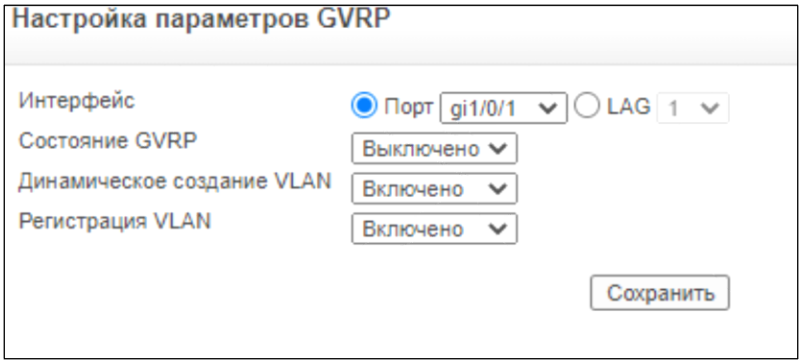


– *Глобальное состояние GVRP*— состояние протокола GVRP на коммутаторе:

  - *Включен* — протокол GVRP включен;
  - *Выключен* — протокол GVRP отключен на коммутаторе.

При установленном флаге «Порт» будет отображена таблица портов коммутатора, при установленном флаге «LAG» — таблица групп LAG.

Для изменения настроек интерфейса нужно нажать кнопку «Редактировать» и заполнить следующие поля:

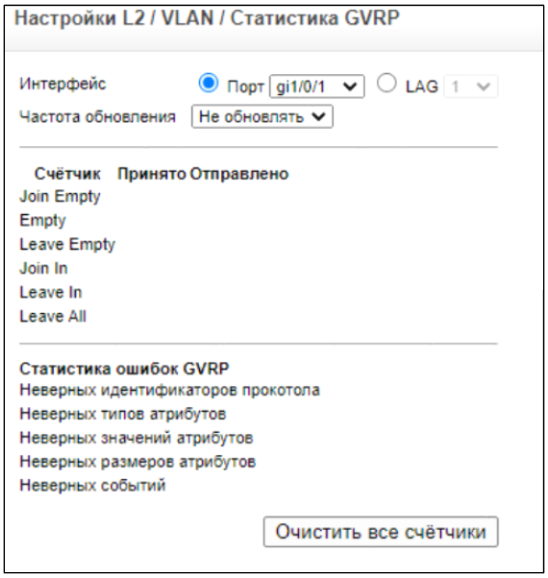


– *Интерфейс* — интерфейс, на котором выполняются настройки GVRP:
  - *Порт* — номер интерфейса, (gi0/1—gi0/48, te0/1—te0/4);
  - *LAG* — номер группы LAG, (1–48);
– *Состояние GVRP* — состояние протокола GVRP на интерфейсе:
  - *Включено* — протокол GVRP включен на интерфейсе;
  - *Выключено* — протокол GVRP отключен на интерфейсе;
– *Динамическое создание VLAN* — динамическое создание VLAN на интерфейсе:
  - *Включено* — на интерфейсе разрешено динамическое создание VLAN;
  - *Выключено* — на интерфейсе запрещено динамическое создание VLAN;
– *Регистрация GVRP* — регистрация VLAN через GVRP на устройстве:
  - *Включено* — на интерфейсе разрешена регистрация VLAN;
  - *Выключено* — на интерфейсе запрещена регистрация VLAN.

Нажмите кнопку «Сохранить» для применения настроек.

2.7.6.6 Просмотр статистики GVRP

В разделе **Настройки L2 → VLAN → Статистика GVRP** осуществляется просмотр статистики по протоколу GVRP, а также статистики по ошибкам при работе протокола GVRP.



– *Интерфейс* — интерфейс, для которого выполняется просмотр статистики GVRP:
  - *Порт* — номер интерфейса, (gi0/1—gi0/48, te0/1—te0/4);
  - *LAG* — номер группы LAG, (1–48);
– *Частота обновления* — время обновления статистики:
  - 15 сек — каждые 15 секунд;
  - 30 сек — каждые 30 секунд;
  - 60 сек — каждые 60 секунд;
  - Не обновлять — статистика не обновляется;
– *Join Empty* — количество принятых сообщений «Join Empty»;
– *Empty* — количество принятых сообщений «Empty»;
– *Leave Empty* — количество принятых сообщений «Leave Empty»;
– *Join In* — количество принятых сообщений «Join In»;
– *Leave In* — количество принятых сообщений «Leave In»;
– *Leave All* — количество принятых сообщений «Leave all».

Статистика ошибок GVRP:

– *Неверных идентификаторов прокотола* — статистика по недопустимым идентификаторам протокола;
– *Неверных типов атрибутов* — статистика по недопустимым типам атрибута протокола;
– *Неверных значений атрибутов* — статистика по недопустимым значениям атрибута протокола;
– *Неверных размеров атрибутов* — статистика по недопустимым значениям длины атрибута;
– *Неверных событий* — статистика по недопустимым событиям протокола GVRP.

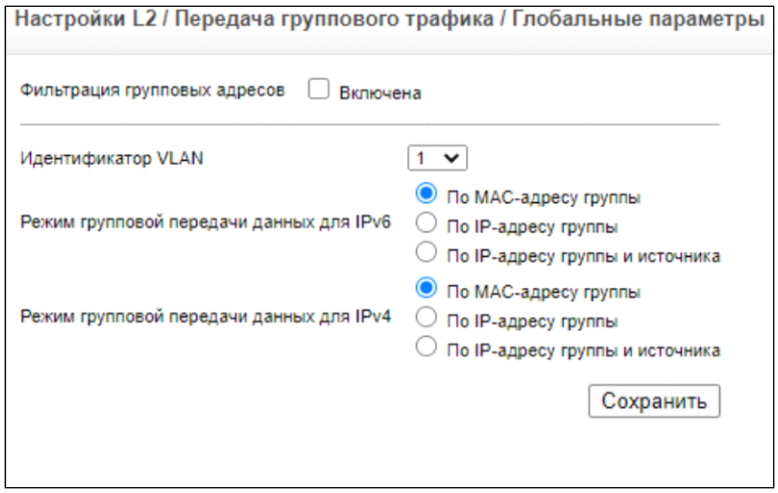
Нажмите кнопку «*Очистить все счетчики*» для удаления статистики.

2.7.7 Управление групповой адресацией

В разделе **Настройки L2 → Передача группового трафика** выполняются настройки для передачи многоадресного трафика.

2.7.7.1 Настройка фильтрации групповых адресов

В разделе **Настройки L2 → Передача группового трафика → Глобальные параметры** настраивается фильтрация групповых адресов на устройстве.



– *Фильтрация групповых адресов* — установите флаг *«Включена»* для включения фильтрации групповых данных на устройстве, иначе — фильтрация отключена;

– *Идентификатор VLAN* — номер VLAN, для которой выполняется настройка режима групповой передачи данных;

– *Режим групповой передачи данных для IPv6* — режим маршрутизации многоадресного трафика для IPv6-адресации:

  - *По MAC-адресу группы* — маршрутизация данных основана на VLAN и MAC-адресе пакета данных;
  - *По IP-адресу группы* — маршрутизация основана на VLAN и адресе приемника в формате IPv6;
  - *По IP-адресу группы и источника* — маршрутизация основана на VLAN, адресе получателя и адресе отправителя в формате IPv6;

– *Режим групповой передачи данных для IPv4* — режим групповой передачи данных для IPv4-адресации:

  - *По MAC-адресу группы* — маршрутизация данных основана на VLAN и MAC-адресе пакета данных;
  - *По IP-адресу группы* — маршрутизация основана на VLAN и адресе приемника в формате IPv4;
  - *По IP-адресу группы и источника* — маршрутизация основана на VLAN, адресе получателя и адресе отправителя в формате IPv4.

Нажмите кнопку «Сохранить» для применения настроек.

2.7.7.2 Настройка групп многоадресной передачи, основанных на MAC-адресах

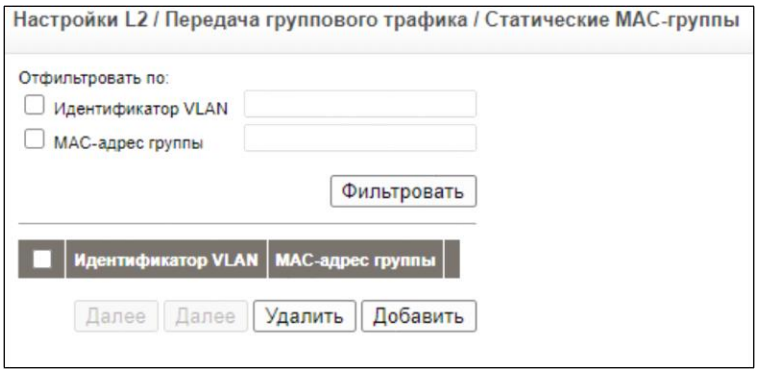
В разделе **Настройки L2 → Передача группового трафика → Статические MAC-группы** выполняется настройка групп многоадресной рассылки с типом фильтрации, основанной на VLAN и групповом MAC-адресе.

Коммутатор поддерживает маршрутизацию многоадресного трафика на основании данных о группах многоадресной рассылки. Эти данные извлекаются из принятых IGMP/MLD пакетов или добавляются путем конфигурирования устройства. Информация о группах хранится в базе данных многоадресной маршрутизации.

В том случае, когда коммутатор принимает пакет данных в VLAN, для которой разрешена маршрутизация многоадресного трафика на основании MAC-адреса, и адрес назначения в пакете является адресом группы многоадресной передачи, этот пакет данных будет предан на все порты, которые являются участниками группы.

Страница управления **Настройки L2 / Передача группового трафика / Статические MAC-группы** предназначена для следующих операций:

- Запрос и просмотр информации из базы данных маршрутизации для выбранной VLAN или выбранной группы;
- Добавление и удаление статических записей в базу данных маршрутизации;
- Просмотр списка портов/групп LAG, являющихся участниками групп многоадресной маршрутизации.

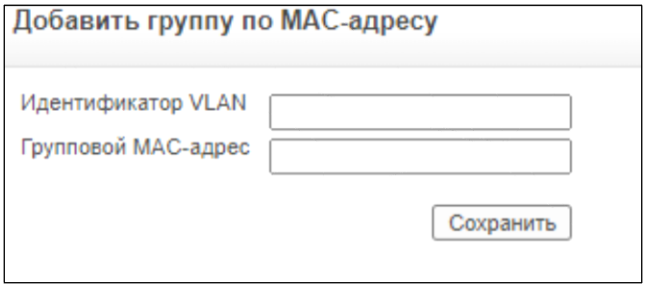


Для того чтобы отобразить и отсортировать записи в таблице по номеру VLAN или по групповому MAC-адресу установите один из следующих флагов, заполните соответствующие поля и нажмите кнопку «Фильтровать»:

- *Идентификатор VLAN* — при установленном флаге будет установлен фильтр записей по заданному номеру VLAN;

- *MAC-адрес группы* — при установленном флаге будет установлен фильтр записей по заданному групповому MAC-адресу.

Для добавления новой записи в таблицу групповой адресации нажмите кнопку «Добавить», укажите номер VLAN, групповой MAC-адрес и нажмите кнопку «Сохранить» для сохранения настроек:



– *Идентификатор VLAN* — номер VLAN для новой группы многоадресной рассылки, (2–4094);

– *Групповой MAC-адрес* — групповой MAC-адрес.

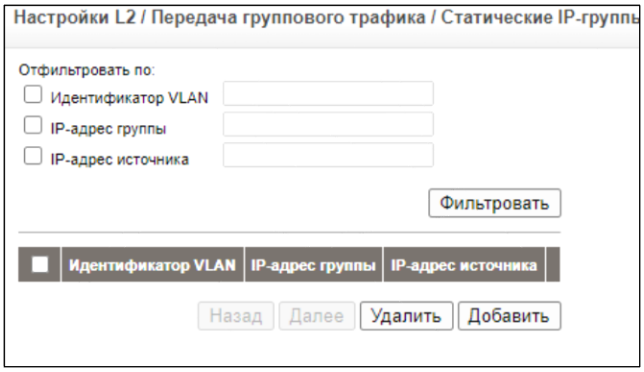
Для удаления записи из таблицы групповой адресации установите флаг напротив заданной записи и нажмите кнопку «Удалить».

2.7.7.3 Настройка групп многоадресной передачи, основанных на IP-адресах

В разделе **Настройки L2 → Передача группового трафика → Статические IP-группы** выполняется настройка групп многоадресной рассылки с типом фильтрации, основанным на VLAN и IP-адресе отправителя.

Страница **Настройки L2 / Передача группового трафика / Статические IP-группы** аналогична странице **Настройки L2 / Передача группового трафика / Статические MAC-группы** за исключением того, что для адресации групп используется IP-адреса. Страница предназначена для запроса информации и для управления группами.

На странице отображаются все групповые IP-адреса, которые были изучены при обработке принятых пакетов (snooping).



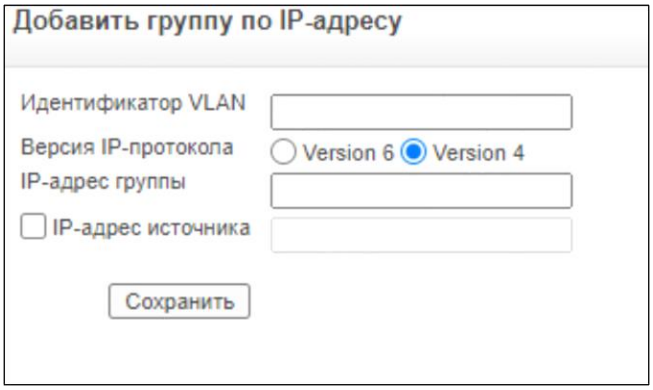
Для того чтобы отобразить и отсортировать записи в таблице по номеру VLAN, IP-адресу или IP-адресу отправителя установите один из следующих флагов, заполните соответствующие поля и нажмите кнопку «Отфильтровать по»:

– *Идентификатор VLAN* — при установленном флаге будет использоваться фильтр записей по заданному номеру VLAN;

– *IP-адрес группы* — групповой IP-адрес;

– *IP-адрес источника* — IP-адрес устройства, посылающего многоадресный трафик. Этот параметр следует указывать в том случае, если адрес источника учитывается в процессе многоадресной рассылки — режим (S,G). Если выбран режим многоадресной маршрутизации (*,G), то это поле не используется.

Для добавления новой записи в таблицу групповой адресации нужно нажать кнопку «Добавить», заполнить следующие поля и нажать кнопку «Сохранить» для сохранения настроек:



– *Идентификатор VLAN* — номер VLAN группы;

– *Версия IP-протокола* — формат IP-адреса:

  - *Version 4* — формат адреса IPv4;
  - *Version 6* — формат адреса IPv6;

– *IP-адрес группы* — IP-адрес для новой многоадресной группы. Следует указывать адрес в выбранном формате — IPv4 или IPv6;

– *IP-адрес источника* — IP-адрес отправителя. Это поле следует заполнять только в том случае, если используется режим групповой маршрутизации (S,G).

Нажмите кнопку «Сохранить» для применения настроек.

2.7.7.4 Настройка функции IGMP Snooping

Раздел **Настройки L2 → Передача группового трафика → IGMP Snooping** предназначен для управления функцией IGMP Snooping, просмотра настроек IGMP Snooping интерфейсов VLAN и вызова диалога конфигурирования VLAN.

Функция IGMP Snooping используется в сетях групповой рассылки. Основной задачей IGMP Snooping является предоставление многоадресного трафика только для тех портов, которые запросили его. Для того, чтобы функция была работоспособна, необходимо активировать фильтрацию многоадресного трафика (см. п.п 2.7.7.1, параметр *Фильтрация групповых адресов*), разрешить IGMP Snooping глобально для устройства и на каждой VLAN, где это необходимо.

По умолчанию коммутатор передает многоадресный трафик на все порты, находящиеся в одной VLAN с источником трафика.

Коммутатор поддерживает IGMP Snooping только на статически сконфигурированных VLAN и не поддерживает на динамических VLAN.

В том случае, когда функция IGMP Snooping разрешена глобально или на VLAN, все IGMP пакеты перенаправляются на управляющий процессор (CPU), который анализирует принятые пакеты и выясняет следующее:

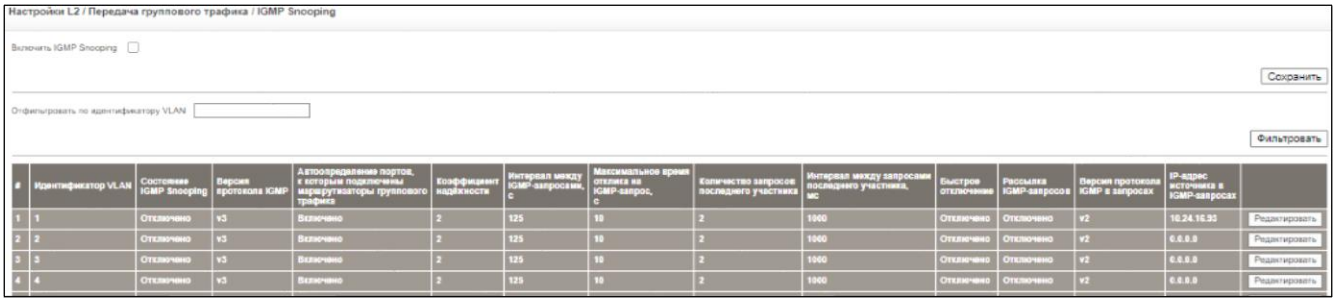
– какие порты запрашивают присоединение к какой группе и в какой VLAN;
– какие порты подключены к маршрутизаторам многоадресного трафика (mrouters), которые формируют IGMP-запросы (IGMP queries);
– какие порты принимают запросы по протоколам PIM и IGMP.

Вся эта информация отображается на странице **Настройки L2 / Передача группового трафика / IGMP Snooping.**

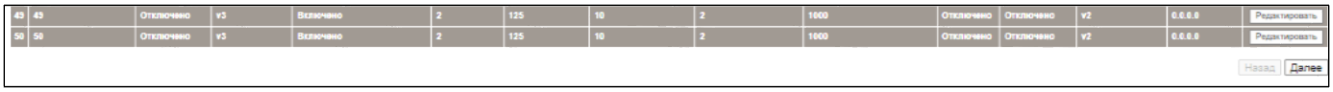
Устройства, запрашивающие присоединение к многоадресным группам, передают IGMP запрос «join», который перечисляет группы, к которым устройство хочет присоединиться. Обработка этих запросов приводит к созданию правил маршрутизации в базе данных маршрутизации многоадресного трафика.

В случае отсутствия в сети маршрутизатора многоадресного трафика (mrouter), для поддержки работоспособности функции многоадресной маршрутизации одно из сетевых устройств должно выполнять функцию IGMP Querier. Только одно устройство в широковещательном домене уровня 2 может выполнять функции Querier. Коммутатор поддерживает стандартную процедуру выборов в том случае, если в сети присутствует более одного устройства с функцией Querier.

Частота отправки многоадресных запросов устройством с функцией Querier должна быть согласована с настройками функции IGMP Snooping на коммутаторах, находящихся в одном широковещательном домене. Запросы (query) должны отправляться с интервалом, не превышающим времена жизни данных, полученных в результате перехвата многоадресных пакетов (snooping). В противном случае подписчик не сможет получать групповые данные.



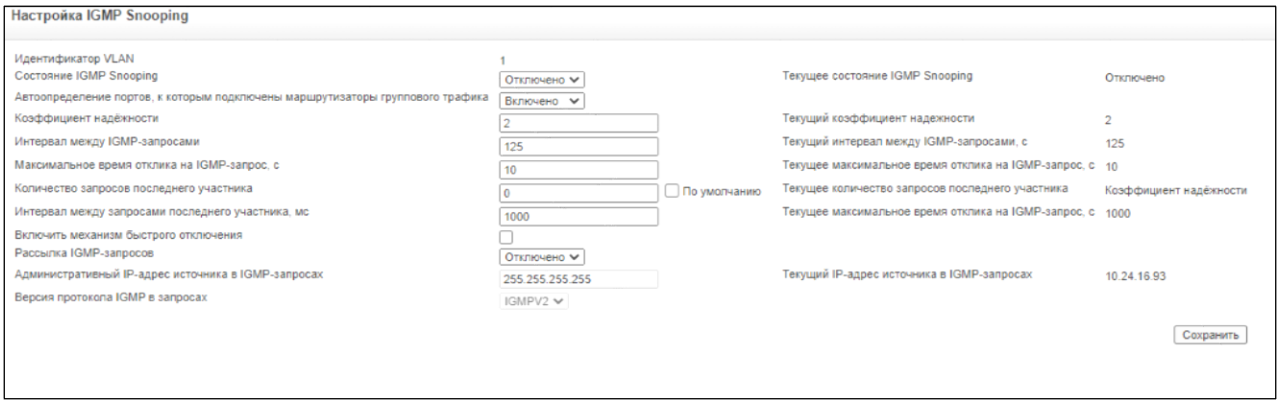
…



– *Включить IGMP Snooping* — для включения функции IGMP Snooping на коммутаторе глобально нужно установить флаг и нажать кнопку «Сохранить», иначе — функция отключена;

– *Отфильтровать по идентификатору VLAN* — для того чтобы отобразить и отсортировать записи в таблице по номеру VLAN заполните данное поля и нажмите кнопку «Фильтровать».

Для открытия окна настроек функции IGMP Snooping определенной VLAN нажмите кнопку «Редактировать»:



– *Идентификатор VLAN* — идентификационный номер VLAN, на которой включена функция IGMP Snooping;

– *Состояние IGMP Snooping* — состояние функции IGMP snooping на определенном интерфейсе VLAN:

  - *Включено* — функция включена;
  - *Отключено* — функция отключена;

– *Автоопределение портов, к которым подключены маршрутизаторы группового трафика* — состояние автоматического распознавания портов, к которым подключен многоадресный маршрутизатор:

  - *Включено* — включено;
  - *Отключено* — отключено;

– *Коэффициент надёжности* — значение устойчивости IGMP, (1–7). Если подсеть нестабильна и подвержена потере пакетов, то необходимо повысить значение устойчивости. По умолчанию установлено 2;

– *Интервал между IGMP-запросами* — таймаут, по которому система отправляет основные запросы всем участникам группы многоадресной передачи для проверки их активности, (30–18000) секунд. По умолчанию установлено 125 секунд;

– *Максимальное время отклика на IGMP-запрос, с* — максимальное время ответа на запрос, (5–20) секунд. По умолчанию установлено 10 секунд;

– *Количество запросов последнего участника* — количество запросов, после рассылки которых коммутатор определяет, что на данном порту нет желающих участвовать в многоадресной рассылке, (1–7). По умолчанию присваивается значение, установленное в поле «Query Robustness»;

– *Интервал между запросами последнего участника, мс* — устанавливает интервал запроса для последнего участника, (100–25500) миллисекунд. По умолчанию установлено 1000 миллисекунд;

– *Включить механизм быстрого отключения* — при установленном флаге включена процедура, при которой порт после получения сообщения IGMP leave должен быть немедленно удален из группы IGMP;

– *Рассылка IGMP-запросов* — включает/выключает поддержку коммутатором выдачи запросов IGMP query в данной VLAN:

  - *Включено* — включено;
  - *Отключено* — отключено;

– *Административный IP-адрес источника в IGMP-запросах* — IP-адрес, который будет использоваться в качестве адреса источника запросов IGMP query;

– *Версия протокола IGMP в запросах* — версия IGMP-протокола, на основании которой будут формироваться IGMP query-запросы. По умолчанию установлена версия 3.

В правой колонке указана текущая конфигурация IGMP Snooping выбранной VLAN.

Для сохранения настроек нужно нажать кнопку «Сохранить».

2.7.7.5 Настройка функции MLD Snooping

В разделе **Настройки L2 → Передача группового трафика → MLD Snooping** включается функция MLD Snooping на коммутаторе, осуществляется просмотр настроек MLD Snooping для интерфейсов VLAN коммутатора и вызов диалога настроек функции.

MLD snooping — механизм многоадресной рассылки сообщений, позволяющий минимизировать многоадресный трафик в IPv6-сетях.

Коммутатор поддерживает MLD Snooping только на статически сконфигурированных VLAN и не поддерживает на динамических VLAN.

Коммутатор не поддерживает функцию MLD Querier.

Коммутатор поддерживает две версии MLD Snooping:

– MLDv1 Snooping обнаруживает управляющие пакеты MLD версии 1 и настраивает маршрутизацию на основании IPv6 групповых адресов назначения.

– MLDv2 Snopping использует управляющие пакеты MLD версии 2 и управляет передачей многоадресного трафика на основании IPv6 адреса источника и группового адреса назначения.

Какая из версий протокола будет использована зависит от маршрутизатора (multicast router). Обработка MLD данных сходна с обработкой пакетов протокола IGMP при работе функции IGMP Snooping.

Настройки L2 / Передача группового трафика / MLD Snooping

Включить MLD Snooping ☐

Сохранить

Отфильтровать по идентификатору VLAN

Фильтровать

Идентификатор VLAN	Состояние MLD Snooping	Версия протокола MLD	Автоопределение портов, к которым подключены маршрутизаторы группового трафика	Коэффициент надёжности	Интервал между MLD-запросами, с	Максимальное время отклика на MLD-запрос, с	Количество запросов последнего участника	Интервал между запросами последнего участника, мс	Быстрое отключение	
1	Выключен	v2	Включен	2	125	10	2	1000	Выключен	Редактировать
2	Выключен	v2	Включен	2	125	10	2	1000	Выключен	Редактировать
3	Выключен	v2	Включен	2	125	10	2	1000	Выключен	Редактировать
4	Выключен	v2	Включен	2	125	10	2	1000	Выключен	Редактировать
5	Выключен	v2	Включен	2	125	10	2	1000	Выключен	Редактировать

...

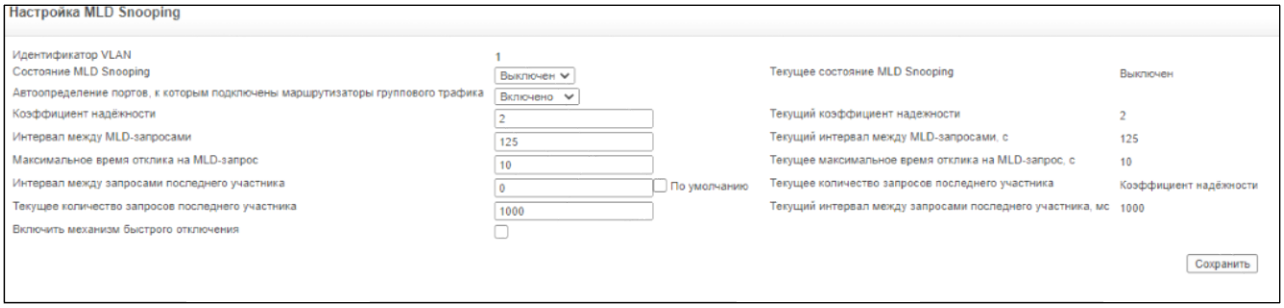
49	Выключен	v2	Включен	2	125	10	2	1000	Выключен	Редактировать
50	Выключен	v2	Включен	2	125	10	2	1000	Выключен	Редактировать

Назад Далее

– *Включить MLD Snooping* — для включения функции MLD Snooping на коммутаторе глобально нужно установить флаг и нажать кнопку «Сохранить», иначе — функция отключена. Чтобы функция MLD Snooping была активна, функция фильтрации групповых адресов должна быть включена;

– *Отфильтровать по идентификатору VLAN* — для того чтобы отобразить и отсортировать записи в таблице по номеру VLAN заполните данное поля и нажмите кнопку «Фильтровать».

Для открытия окна настроек функции MLD Snooping определенной VLAN нужно нажать кнопку «Редактировать»:



– *Идентификатор VLAN* — идентификационный номер VLAN, на которой включена функция MLD Snooping;

– *Состояние MLD Snooping* — состояние функции *MLD Snooping* на определенном интерфейсе VLAN. Чтобы функция *MLD Snooping* была активна, функция фильтрации групповых адресов должна быть включена:

  - *Включен* — функция включена;
  - *Выключен* — функция отключена;

– *Автоопределение портов, к которым подключены маршрутизаторы группового трафика* — состояние автоматического распознавания портов, к которым подключен многоадресный маршрутизатор:

  - Включено — включено;
  - Выключено — отключено;

– *Коэффициент надёжности* — значение устойчивости протокола MLD, (1–7). Если подсеть нестабильна и подвержена потере пакетов, то необходимо повысить значение устойчивости. По умолчанию установлено 2;

– *Интервал между MLD-запросами* — таймаут, по которому система отправляет основные запросы всем участникам группы многоадресной передачи для проверки их активности, (30–18000) секунд. По умолчанию установлено 125 секунд;

– *Максимальное время отклика на MLD-запрос* — максимальное время ответа на запрос, (5–20) секунд. По умолчанию установлено 10 секунд;

– *Текущее количество запросов последнего участника* — количество запросов, после рассылки которых, коммутатор определяет, что на данном порту нет желающих участвовать в многоадресной IPv6-рассылке, (1–7);

– *Интервал между запросами последнего участника* — устанавливает интервал запроса для последнего участника, (100–25500) миллисекунд. По умолчанию установлено 1000 миллисекунд;

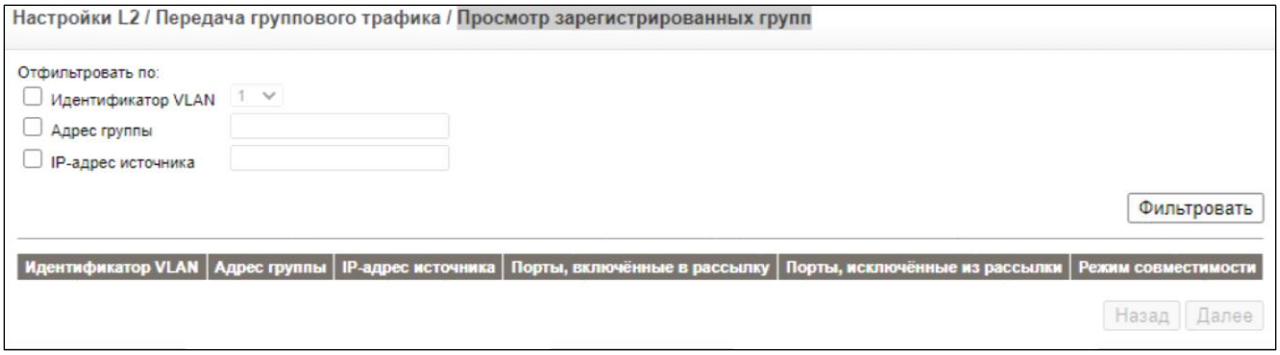
– *Включить механизм быстрого отключения* — при установленном флаге включена процедура, при которой порт после получения сообщения «leave» должен быть немедленно удален из группы MLD.

В правой колонке указаны действующие (текущие) параметры MLD Snooping выбранной VLAN.

Для сохранения настроек нужно нажать кнопку «Сохранить».

2.7.7.6 Просмотр информации о группах, участвующих в групповой рассылке

В разделе **Настройки L2 → Передача группового трафика → Просмотр зарегистрированных групп** осуществляется просмотр информации о многоадресных IPv4 и IPv6 группах, участвующих в групповой рассылке.



Для того чтобы отсортировать записи в таблице по номеру VLAN, групповому адресу или IP-адресу отправителя установите один из следующих флагов, заполните соответствующие поля и нажмите кнопку «Фильтровать»:

- *Идентификатор VLAN* — при установленном флаге будет установлен фильтр записей по заданному номеру VLAN;
- *Адрес группы* — групповой IP- или MAC-адрес;
- *IP-адрес источника* — адрес источника.

Описание полей таблицы:

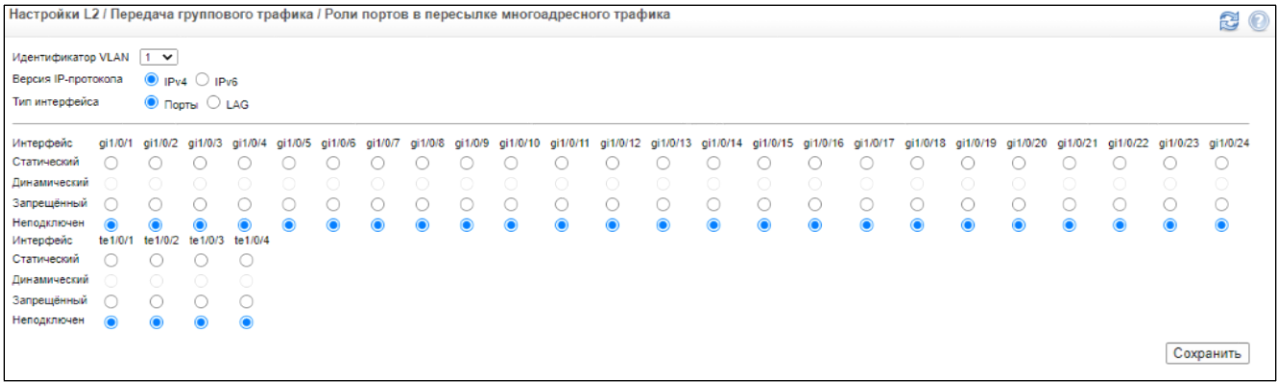
- *Идентификатор VLAN* — идентификатор VLAN;
- *Адрес группы* — MAC- или IP-адрес группы многоадресной рассылки;
- *IP-адрес источника* — адрес отправителя для всех указанных портов группы;
- *Порты, включённые в рассылку* — список интерфейсов, на которые направляется соответствующий поток многоадресной рассылки;
- *Порты, исключённые из рассылки* — список портов, которые не входят в состав группы;
- *Режим совместимости* — версия IGMP/MLD.

2.7.7.7 Настройка интерфейсов к многоадресным маршрутизаторам (mrouter)

В разделе **Настройки L2 → Передача группового трафика → Роли портов в пересылке многоадресного трафика** приведена конфигурация, в которой определено, какие интерфейсы коммутатора подключены к многоадресному маршрутизатору.

Mrouter — это порты, к которым подключен(ы) многоадресные маршрутизаторы (mrouter). Информация о mrouter—портах возникает в результате обработки коммутатором потоков групповых данных или в результате конфигурирования статически определенных портов.

Страница **Настройки L2 / Передача группового трафика / Роли портов в пересылке многоадресного трафика** предоставляет возможность конфигурирования статических портов и просмотра перечня динамически изученных портов.



– *Идентификатор VLAN* — номер VLAN для отображения таблицы настроек интерфейсов коммутатора;

При установленном флаге «Порты» будет отображена таблица правил для портов коммутатора, при установленном флаге «LAG» — таблица правил для групп LAG.

Для каждого интерфейса можно установить способ определения его состояния:

– *Статический* — для выбранной VLAN порт статически определен как mrouter-порт;

– *Динамический* — порт динамически конфигурируется как mrouter-порт за счет обработки запросов IGMP/MLD (IGMP/MLD query). Для включения динамического изучения портов, необходимо перейти в раздел Передача группового трафика > IGMP Snooping или Передача группового трафика > MLD Snooping;

– *Запрещенный* — устанавливает запрет на определение порта как порта, к которому подключен маршрутизатор многоадресной рассылки даже в том случае, если на этом порту обнаружены запросы IGMP/MLD;

– *Неподключен* — порт не является mrouter-портом.

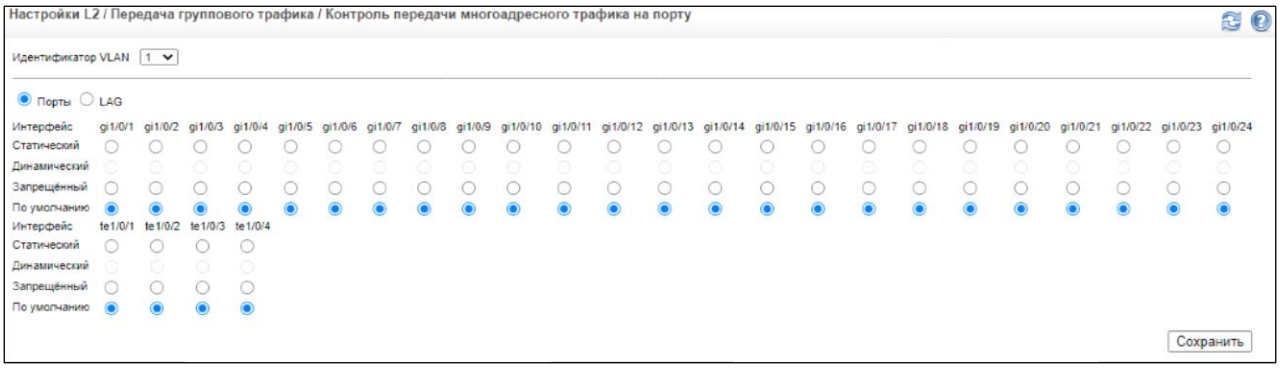
Нажмите кнопку «Сохранить» для применения настроек.

2.7.7.8 Детализация настроек групповой адресации для интерфейсов

В разделе **Настройки L2 → Передача группового трафика → Контроль передачи многоадресного трафика на порту** выполняется конфигурация интерфейсов, которые получают групповую рассылку в определенной VLAN. Чтобы функция была активна, функция групповой фильтрации должна быть включена.

IGMP- или MLD-сообщения не пересылаются к интерфейсам, определенным как “forward all”.

Конфигурация применяется только для интерфейсов, которые являются членами заданной VLAN.



– *Идентификатор VLAN* — номер VLAN для отображения таблицы настроек интерфейсов коммутатора;

При установленном флаге «Порты» будет отображена таблица правил для портов коммутатора, при установленном флаге «LAG» — таблица правил для групп LAG.

Для каждого интерфейса можно установить способ определения его состояния:

– *Статический* — разрешена передача всех многоадресных пакетов на порту;

– *Динамический* — не применяется;

– *Запрещенный* — порту запрещается динамически добавляться к многоадресной группе;

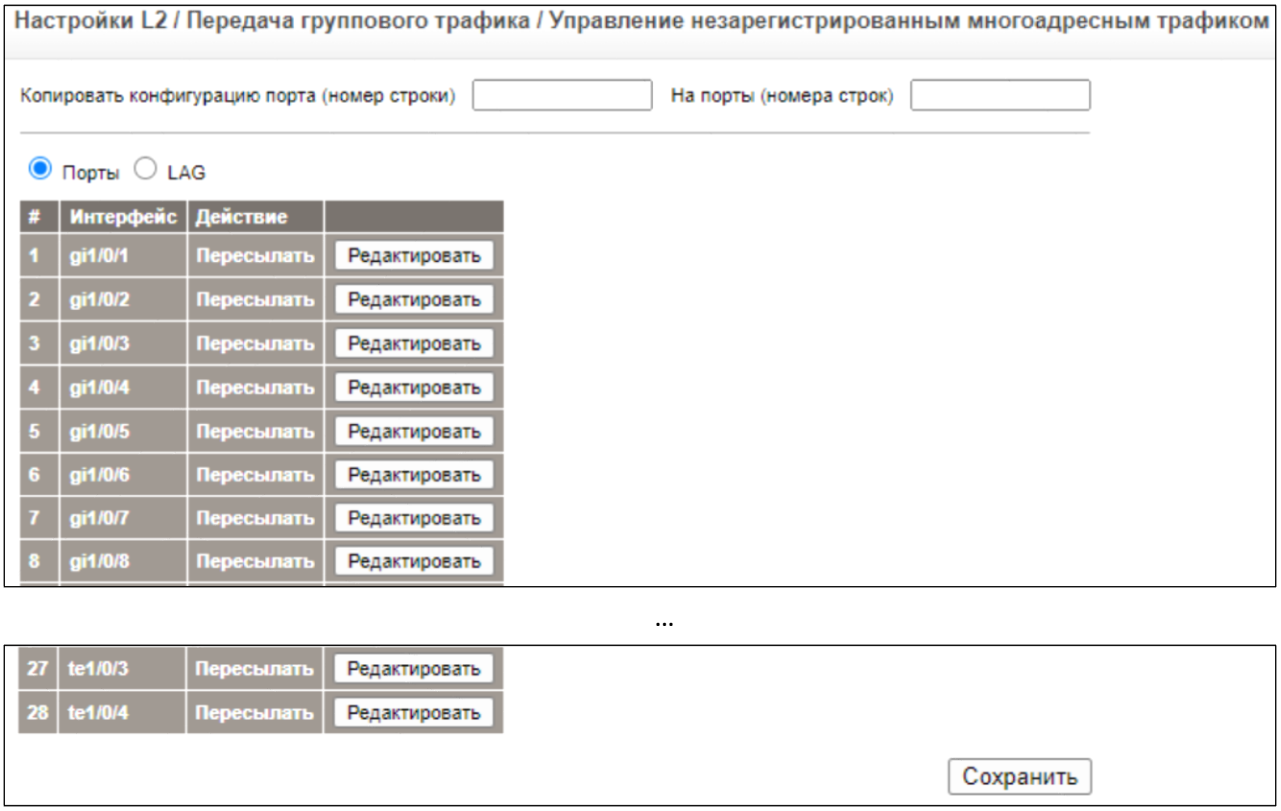
– *По умолчанию* — интерфейсу в настоящее время передача всех многоадресных пакетов запрещена, динамически присоединяться к многоадресной группе не запрещено.

Нажмите кнопку «Сохранить» для применения настроек.

2.7.7.9 Правила для пакетов с незарегистрированными групповыми адресами

В разделе **Настройки L2 → Передача группового трафика → Управление незарегистрированным многоадресным трафиком** устанавливаются правила передачи пакетов с незарегистрированных групповых адресов.

Страница **Управление незарегистрированным многоадресным трафиком** предназначена для управления обработкой многоадресных пакетов, принадлежащих к незарегистрированным в коммутаторе группам рассылки. Как правило, такие пакеты передаются на все порты в пределах VLAN. Настройки порта позволяют изменять его поведение при обработке многоадресного трафика для неизвестных групп — может быть разрешена передача или фильтрация этих данных. Настройка действует для любой VLAN, членом которой порт является или будет являться в будущем.



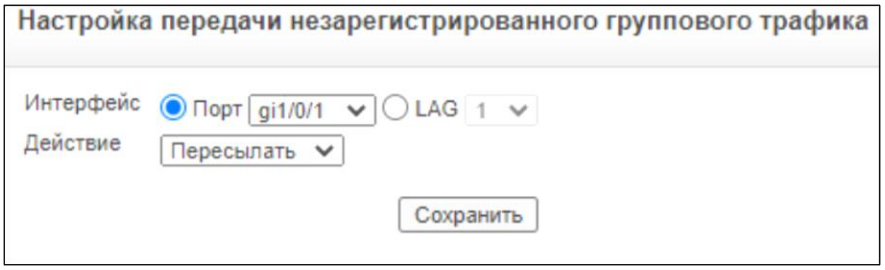
Для одновременной настройки нескольких портов нужно скопировать значение параметров из одной записи в другую/другие. Для этого нужно заполнить следующие поля и нажать кнопку «Сохранить»:

– *Копировать конфигурацию порта (номер строки)* — порядковый номер записи, параметры которой будут скопированы;

– *На порты (номера строк)* — порядковый номер/номера записей, для которых будут применены параметры. Можно указать диапазон через «—», либо перечислением через «,».

При установленном флаге «Порты» будет отображена таблица правил для портов коммутатора, при установленном флаге «LAG» — таблица правил для групп LAG.

Для изменения настроек интерфейса нужно нажать кнопку «Редактировать» напротив заданной записи и заполнить соответствующие поля:



– *Интерфейс* — интерфейс, для которого выполняется настройка:
  - *Порт* — номер интерфейса, (gi0/1—gi0/48, te0/1—te0/4);
  - *LAG* — номер группы LAG, (1–48);
– *Действие* — назначаемое действие:
  - *Пересылать* — передавать незарегистрированные многоадресные пакеты;
  - *Отбрасывать* — фильтровать незарегистрированные многоадресные пакеты.

Нажмите кнопку «Сохранить» для применения настроек.

2.7.8 LLDP

В данном разделе осуществляется просмотр информации о соседних устройствах посредством протокола LLDP.

Link Layer Discovery Protocol (LLDP) — протокол канального уровня, позволяющий сетевому оборудованию оповещать оборудование, работающее в локальной сети, о своём существовании и передавать ему свои характеристики, а также получать от него аналогичные сведения.

– *Port* — номер порта, к которому подключено встречное устройство;
– *Device ID* — MAC-адрес встречного устройства;
– *Port ID* — номер порта, которым встречное устройство подключено к коммутатору;
– *System Name* — имя встречного устройства (по умолчанию пустое);
– *Capabilities* — индентификаторы TVL-поля;
– *TTL* — предельный период времени или число итераций, или переходов, за которые набор данных может существовать до своего исчезновения.

2.8 Управление качеством обслуживания (QoS)

В данной главе описывается управление качеством обслуживания (QoS) на коммутаторах MES23xx/MES33xx/MES35xx/MES5324:

– определение основных настроек QoS;
– настройка базового режима QoS;
– настройка расширенного режима QoS.

Под качеством обслуживания (QoS) понимается способность сети обеспечить необходимый приоритет заданному трафику. Использование QoS позволяет улучшить показатели передачи трафика чувствительного к задержкам (потоковое видео, голос), и тем самым повысить производительность сети в целом. Механизм QoS, реализованный в коммутаторах MES23xx/MES33xx/MES35xx/MES5324 позволяет организовать восемь очередей приоритета пакетов в зависимости от типа передаваемых данных.

Настройка QoS включает в себя два этапа:

– *Настройка классификации (Classification)* — определяется совпадение отдельных полей пакета со значениями, заданными пользователем и производится разделение трафика на потоки с разными приоритетами;

– *Настройка правил политики (Action)* — определяются действия над классифицирован–ными потоками трафика.

Приоритет данных, используемый для управления качеством обслуживания, определяется на основании таких полей пакетов данных, как User Priority (приоритет в соответствии с IEEE802.1p) и кода DSCP (DiffServ Code Piont).

Назначенный приоритет данных используется для выбора одной из восьми очередей на исходящем интерфейсе. В коммутаторе предусмотрены параметры конфигурации для сопоставления User Priority и кодов DSCP с выходными очередями коммутатора.

После того, как сделано сопоставление кодов приоритетов с выходными очередями, необходимо настроить режим работы диспетчера очередей. Может быть выбран один из следующих режимов:

– *Strict Priority* — строгое соблюдение приоритетов обеспечивает передачу пакетов без потерь для приложений с высоким приоритетом и чувствительных к задержкам трафика;

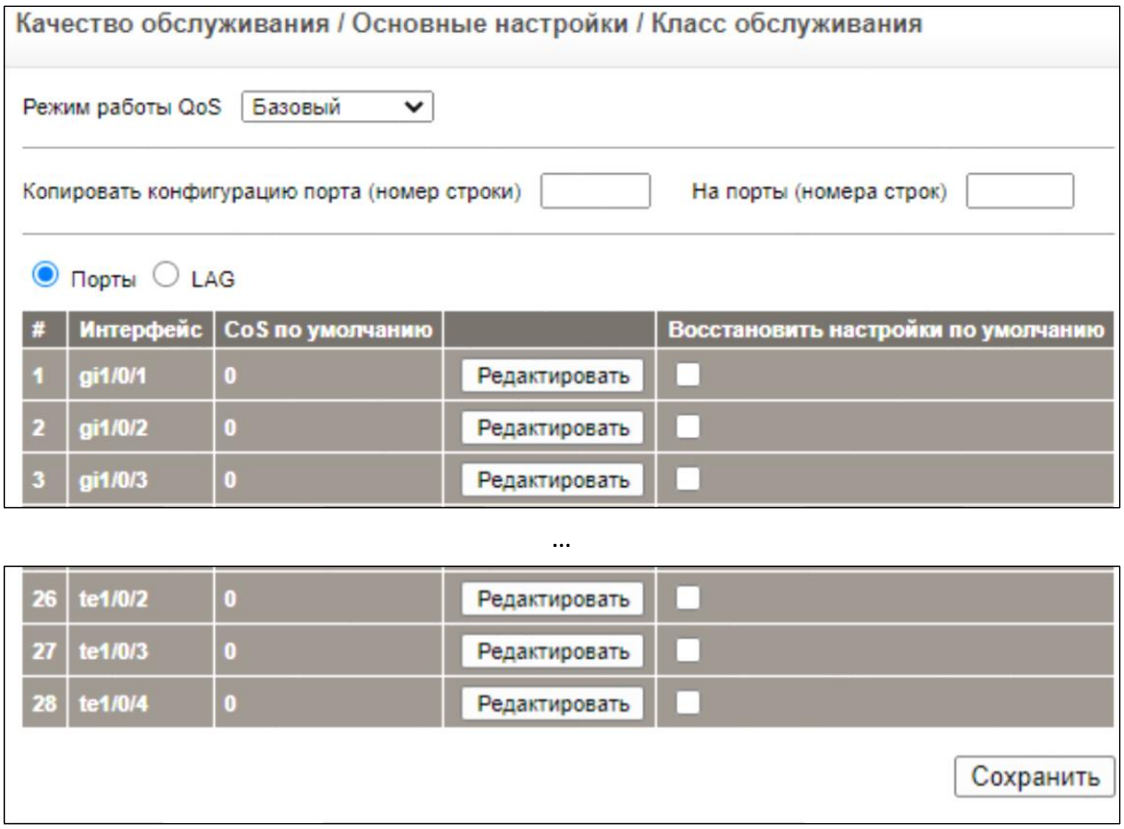
– *Weighted Round Robin* — взвешенное равномерное распределение приоритетов предотвращает доминирование высокоприоритетных приложений, вызывающее блокирование передачи менее приоритетного трафика. Режим WRR обеспечивает взвешенное распределение полосы пропускания канала между очередями, очередям назначаются веса в следующей последовательности: 1,2,4,8.

2.8.1 Общие настройки QoS

В разделе **Качество обслуживания → Основные настройки** выполняются общие настройки QoS.

2.8.1.1 Назначение классов сервиса (CoS) для интерфейсов

В разделе **Качество обслуживания → Основные настройки → Класс обслуживания** устанавливается режим работы QoS для всего устройства и класс сервиса по умолчанию для определенного интерфейса.



– *Режим работы QoS*— режим работы QoS:

  - *Выключен* — управление QoS выключено. Механизм передачи данных — FIFO;
  - *Базовый* — включен базовый режим QoS;
  - *Расширенный* — включен расширенный режим QoS.

Для одновременной настройки нескольких портов можно скопировать значение параметров из одной записи в другую/другие. Для этого заполните следующие поля и нажмите кнопку «Сохранить»:

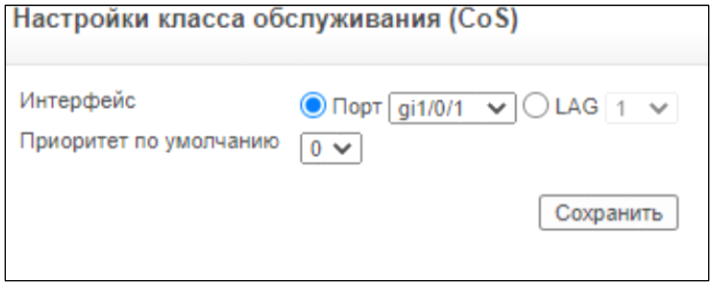
– *Копировать конфигурацию порта (номер строки)* — порядковый номер записи, параметры которой будут скопированы;

– *На порты (номера строк)* — порядковый номер/номера записей, для которых будут скопированы параметры. Можно указать диапазон через «—», либо перечислением через «,».

При установленном флаге «Порты» будет отображена таблица правил для портов коммутатора, при установленном флаге «LAG» — таблица правил для групп LAG.

– *Восстановить настройки по умолчанию* — при установленном флаге для заданного порта используются настройки QoS, установленные по умолчанию.

Для редактирования записи нужно нажать кнопку «Редактировать», заполнить соответствующие поля:



– *Интерфейс* — интерфейс, для которого выполняются настройки:

  - *Порт* — номер интерфейса, (gi0/1—gi0/48, te0/1—te0/4);
  - *LAG* — номер группы LAG, (1–48);

– *Приоритет по умолчанию* — значение CoS, установленное по умолчанию, для входящих пакетов без тега VLAN. Принимает значения (0–7). По умолчанию установлено значение 0.

Нажмите кнопку «Сохранить» для применения настроек.

2.8.1.2 Настройка очередей

В разделе **Качество обслуживания → Основные настройки → Очереди** осуществляется просмотр состояния очередей на коммутаторе и определение способа обработки очередей.

Коммутатор поддерживает следующие способы обработки очередей: взвешенный циклический алгоритм (Weighted Round Robin — WRR), строгое соблюдение приоритетов (Strict Priority Queuing).

- *Строгая приоритизация* — при установленном флаге включено управление трафиком строго на основе приоритетов очередей;
- *Циклическое планирование на основе весов (WRR)* — при установленном флаге для очереди назначается режим «Weighted Round Robin» и для этой очереди необходимо задать ее WRR-вес. Поле «WRR Weight» активно только для очередей в режиме взвешенной циклической обработки (WRR). Если очередь имеет вес 0, то она неактивна;
- *Номер очереди* — номер очереди, для которой определяется режим обработки (SP или WRR);
- *Весовой коэффициент* — вес WRR;
- *Использование полосы пропускания, %* — вычисленное значение полосы пропускания заданной очереди в %.

2.8.1.3 Настройка пропускной способности интерфейсов

В разделе **Качество обслуживания → Основные настройки → Ограничение полосы пропускания** осуществляется управление сетевым трафиком посредством ограничения пропускной способности.

Для управления полосой пропускания интерфейсам назначаются следующие параметры:

- *Commited Burst Size (CBS)* — задает максимальное количество бит данных, отправляемых в единицу времени, размер «вспышки» трафика;
- *Согласованная скорость передачи* — задает значение скорости, на которой должна передаваться информация.

Измерения скорости усредняются в переделах единицы времени.

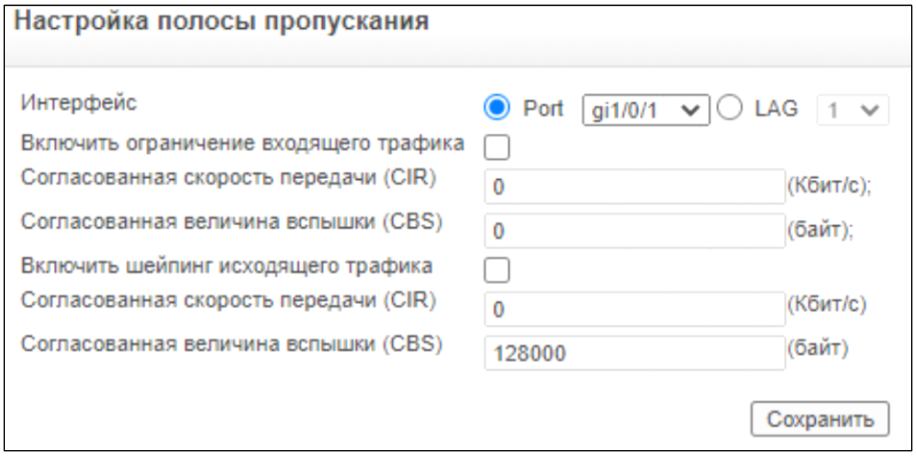
Качество обслуживания / Основные настройки / Ограничение полосы пропускания

Порты LAG

#	Порт	Ограничение входящего трафика			Шейпинг исходящего трафика			
		Состояние	CIR	CBS	Состояние	CIR	CBS	
1	gi1/0/1	Выключен	0	0	Выключен	0	128000	Редактировать
2	gi1/0/2	Выключен	0	0	Выключен	0	128000	Редактировать
3	gi1/0/3	Выключен	0	0	Выключен	0	128000	Редактировать
4	gi1/0/4	Выключен	0	0	Выключен	0	128000	Редактировать
5	gi1/0/5	Выключен	0	0	Выключен	0	128000	Редактировать
6	gi1/0/6	Выключен	0	0	Выключен	0	128000	Редактировать

При установленном флаге «Порты» будет отображена таблица правил для портов коммутатора, при установленном флаге «LAG» — таблица правил для групп LAG.

Для редактирования записи нужно нажать кнопку «Редактировать», заполнить соответствующие поля:



– *Интерфейс* — интерфейс, для которого выполняются настройки:

  - *Порт* — номер интерфейса, (gi0/1—gi0/48, te0/1—te0/4);
  - *LAG* — номер группы LAG, (1–48);

– *Включить ограничение входящего трафика* — при установленном флаге разрешено ограничение скорости для входящего трафика заданного интерфейса;

  - *Согласованная скорость передачи (CIR)* — назначенная скорость передачи данных (64–1000000) Кбит/с;
  - *Согласованная величина вспышки (CBS)* — максимальный размер «вспышки» трафика (4096–16762902) байт;

– *Включить шейпинг исходящего трафика*— при установленном флаге включен шейпер для исходящего трафика заданного интерфейса:

  - *Согласованная скорость передачи (CIR)* — назначенная скорость передачи данных (64–1000000) Кбит/с;
  - *Согласованная величина вспышки (CBS)* — максимальный размер «вспышки» трафика (4096–16762902) байт.

Нажмите кнопку «Сохранить» для применения настроек.

2.8.1.4 Привязка классов обслуживания к очередям

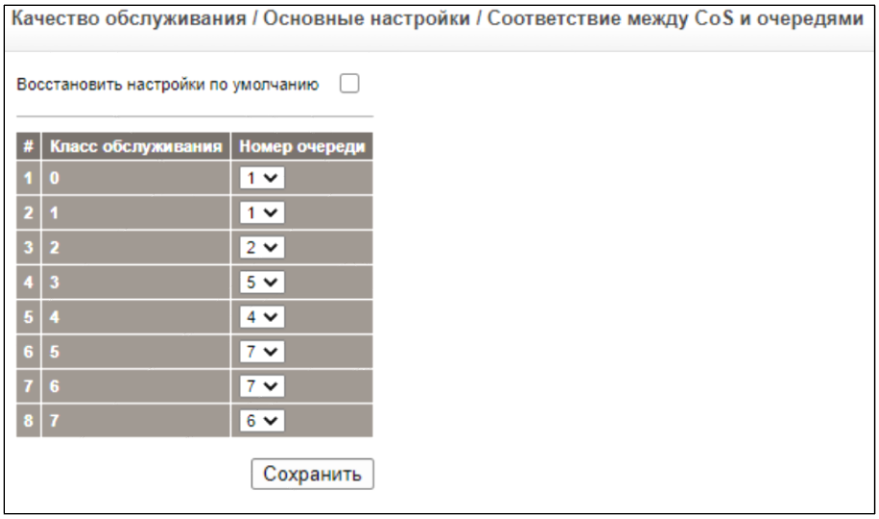
В разделе **Качество обслуживания → Основные настройки → Соответствие между CoS и очередями** выполняется привязка классов обслуживания к очередям. Класс обслуживания CoS соответствует приоритету пакета, который содержится в структуре метки VLAN — IEEE802.1p.

По умолчанию устанавливается следующее соответствие между очередями и приоритетами CoS:

Cos 0	Очередь 3
Cos 1	Очередь 1
Cos 2	Очередь 2
Cos 3	Очередь 4
Cos 4	Очередь 5
Cos 5	Очередь 6
Cos 6	Очередь 7
Cos 7	Очередь 8

Очередь 1 имеет наименьший приоритет, очередь 8 — наивысший.

Страница **Качество обслуживания / Основные настройки / Соответствие между CoS и очередями** позволяет изменить соответствие кодов CoS очередям.



– *Восстановить настройки по умолчанию* — при установленном флаге используется конфигу–рация очередей по умолчанию;

– *Класс обслуживания* — значение 802.1p тега приоритета, где 0 — наименьший приоритет, 7 — наивысший приоритет;

– *Номер очереди* — номер очереди для заданного класса обслуживания (CoS). Поддерживается до 8-ми очередей приоритета трафика.

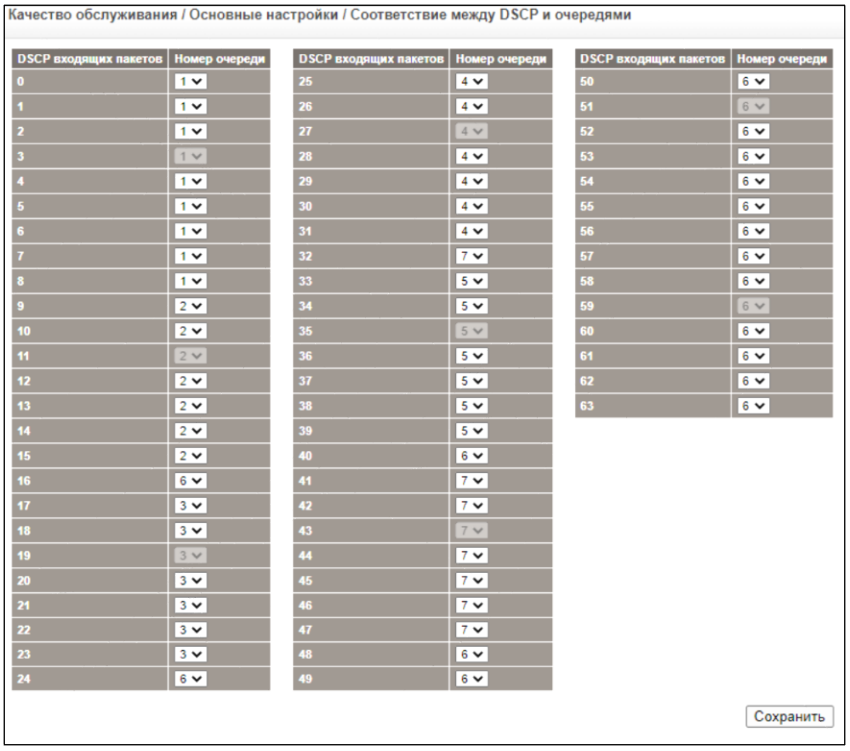
Нажмите кнопку «Сохранить» для применения настроек.

2.8.1.5 Привязка тега DSCP к очередям

В разделе **Качество обслуживания → Основные настройки → Соответствие между DSCP и очередями** выполняется настройка таблицы привязки кода DSCP IP-пакетов к очередям.

По умолчанию используется следующая схема соответствия кодов DSCP очередям:

DSCP 0—7	Очередь 1
DSCP 8—15	Очередь 2
DSCP 16—23	Очередь 3
DSCP 24—31	Очередь 4
DSCP 32—39	Очередь 5
DSCP 40—47	Очередь 6
DSCP 48—55	Очередь 7
DSCP 56—63	Очередь 8



– *DSCP входящих пакетов* — тег DSCP у входящего пакета;

– *Номер очереди* — из ниспадающего списка нужно выбрать номер очереди для заданного DSCP-тега. Поддерживается до 8-ми очередей приоритета трафика.

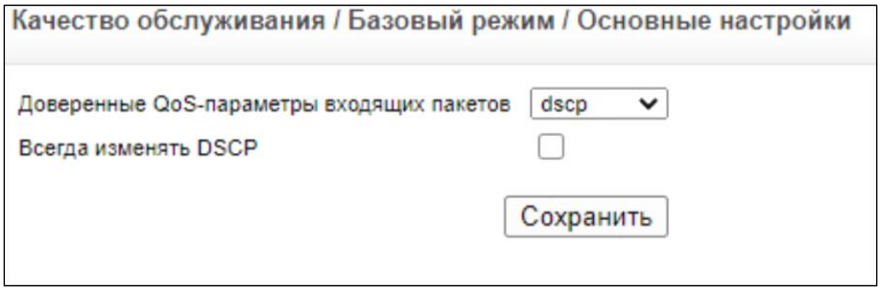
Нажмите кнопку «Сохранить» для применения настроек.

2.8.2 Базовый режим QoS

В базовом режиме выполняются настройки режима доверия QoS и переопределения тега DSCP. Перед выполнением настроек базового режима в разделе **QoS → General → CoS** необходимо установить режим QoS как базовый (QoS Mode— Basic).

2.8.2.1 Общие настройки для базового режима QoS

В разделе **QoS → Basic Mode→ General** устанавливается глобальный режим доверия QoS в базовом режиме, который действует на интерфейсах коммутатора. Пакеты, входящие в область действия QoS классифицируются на границе области. В том случае, когда пакеты классифицируются на границе области, на пограничных портах может быть настроен доверительный режим QoS и правила переопределения кодов DSCP для согласования параметров QoS соседних областей. Режим доверия настраивается для определения поля (CoS или DSCP), на основании которого будет устанавливаться приоритет данных. Это необходимо, когда в IP-пакете присутствуют 802.1p-тег и код DSCP, и при этом номера очередей, назначенные этим тегам, различны.



– *Доверенные QoS-параметры входящих пакетов* — режим доверия коммутатора:

  - *CoS* — приоритет очереди определяется по таблице CoS (раздел QoS → General → CoS to Queue Mapping). Для нетегированных пакетов используется значение CoS по умолчанию (Default User Priority), назначенное для порта, принявшего пакет (страница QoS → General → CoS);

  - *DSCP* — приоритет очереди определяется по таблице DSCP (раздел QoS → General → DSCP to Queue). К пакетам с данными, относящимися к протоколам отличным от IP, применяется правило best effort — коммутатор предпринимает попытку передачи этих пакетов, но помещает их в очередь с минимальным приоритетом (очередь 1). Определение приоритета данных по коду DSCP не может работать для дважды тегированных пакетов (QinQ);

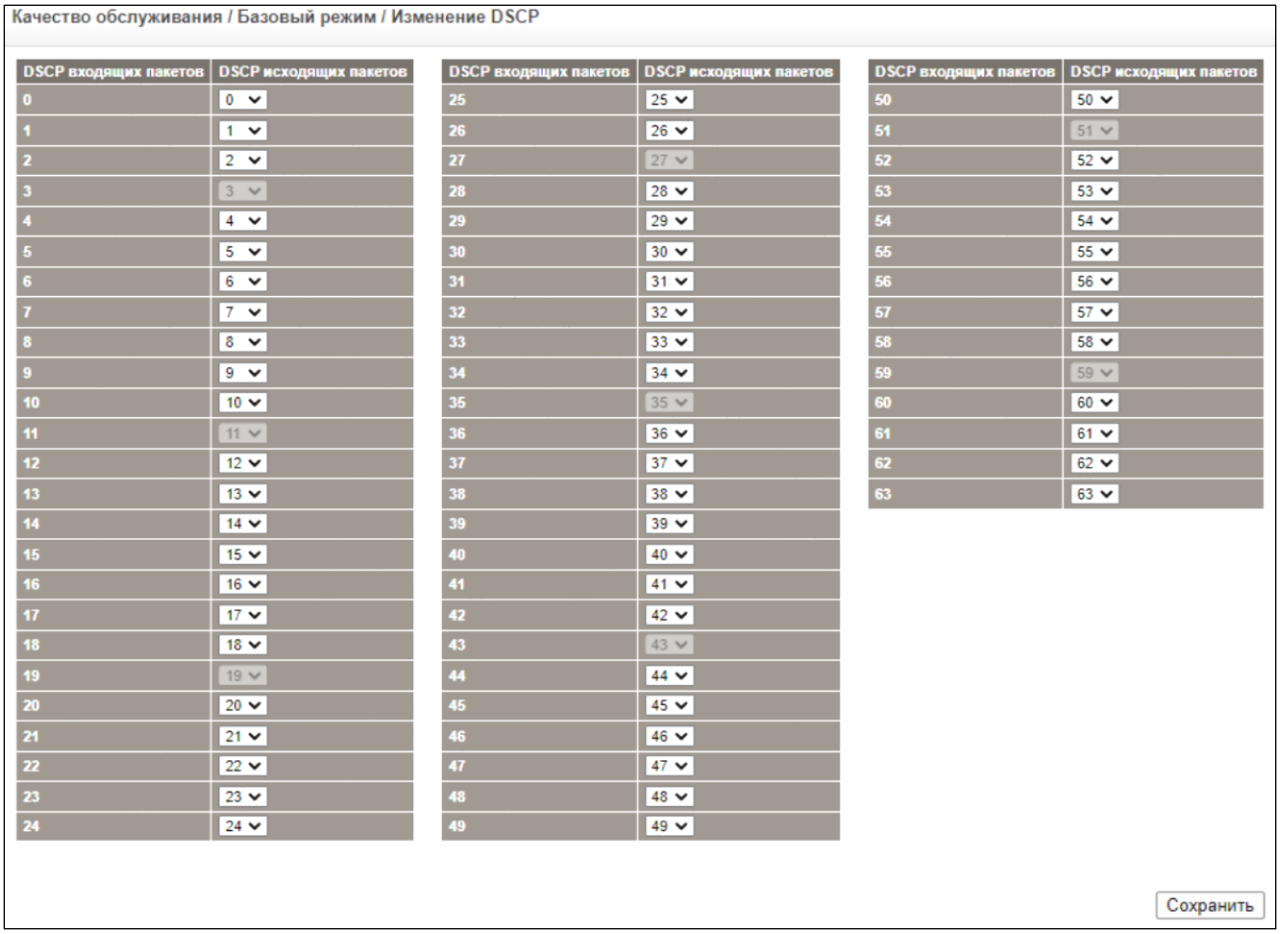
  - *cos-dscp* — приоритет очереди определяется по таблице DSCP, если это IP-пакеты, иначе по таблице CoS;

– *Всегда изменять DSCP* — при установленном флаге код DSCP будет переписан согласно таблице изменений, DSCP базового режима (QoS → Basic Mode→ DSCP Rewrite). Данная функция может быть активна только, если установлен доверительный режим по DSCP. Этот режим может быть полезен для обеспечения взаимодействия сетей с различными политиками QoS.

Нажмите кнопку «Сохранить» для применения настроек.

2.8.2.2 Настройка таблицы перемаркировки DSCP

В разделе **Качество обслуживания → Базовый режим → Изменение DSCP** выполняется настройка таблицы перемаркировки DSCP.



– *DSCP входящих пакетов* — DSCP-тег входящего пакета в базовом режиме;

– *DSCP исходящих пакетов* — DSCP-тег исходящего пакета в базовом режиме.

Нажмите кнопку «Сохранить» для применения настроек.

2.8.3 Расширенный режим QoS

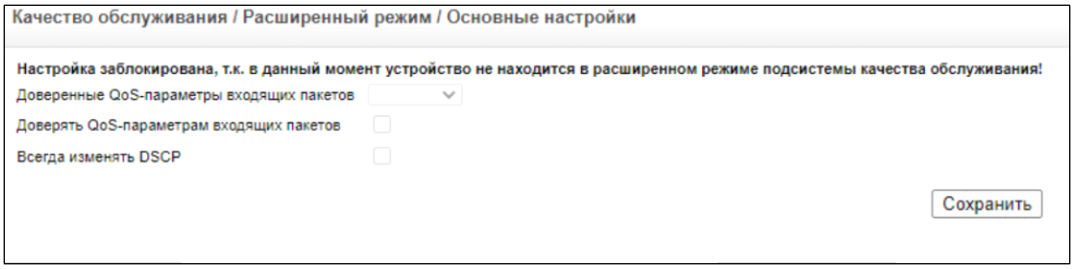
В расширенном режиме выполняются следующие настройки QoS:

– Настройка доверительного режима;
– Настройка таблицы переопределения DSCP;
– Настройка критериев классификации трафика;
– Определение ограничения скорости для входящего/исходящего трафика;
– Определение политики;
– Установка политики для интерфейсов.

Перед выполнением настроек расширенного режима необходимо в разделе **Качество обслуживания → Основные настройки → Класс обслуживания** установить режим работы QoS как расширенный.

2.8.3.1 Общие настройки для расширенного режима QoS

В разделе **Качество обслуживания → Расширенный режим → Основные настройки** выполняются настройки доверительного режима (указывается значение (ToS, DSCP), которое QoS будет использовать в качестве внутреннего DSCP).



– *Доверенные QoS-параметры входящих пакетов* — используемый доверительный режим:

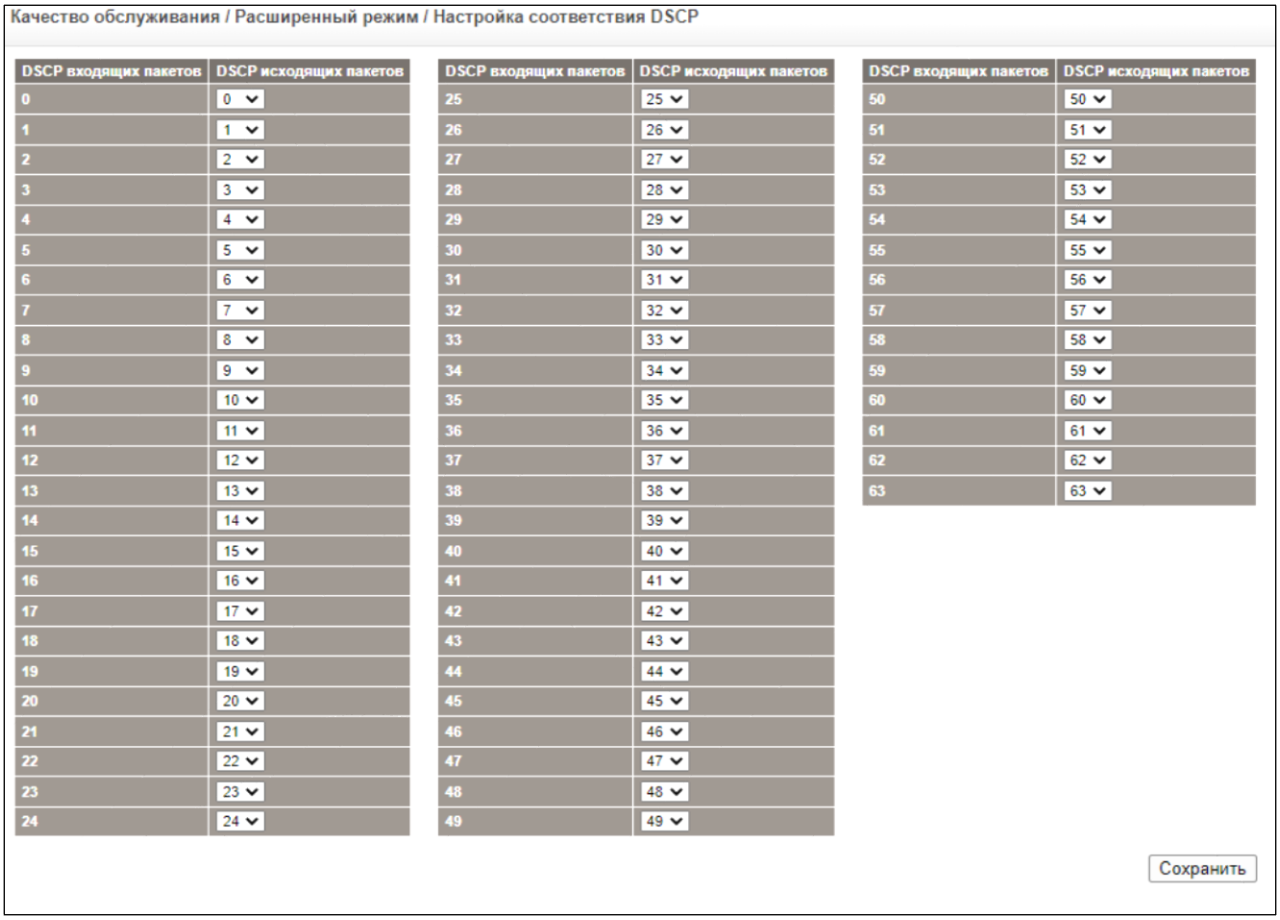
  - *cos* — приоритет очереди определяется по таблице CoS (раздел QoS → General → CoS to Queue Mapping). Для нетегированных пакетов используется значение CoS по умолчанию (Default User Priority), назначенное для порта, принявшего пакет (страница QoS → General → CoS);
  - *dscp* — приоритет очереди определяется по таблице DSCP (раздел QoS → General → DSCP to Queue). К пакетам с данными, относящимися к протоколам отличным от IP, применяется правило best effort — коммутатор предпринимает попытку передачи этих пакетов, но помещает их в очередь с минимальным приоритетом (очередь 1). Определение приоритета данных по коду DSCP не может работать для дважды тегированных пакетов (QinQ);
  - *cos-dscp* — приоритет очереди определяется по таблице DSCP, если это IP-пакеты, иначе по таблице CoS;

– *Доверять QoS-параметрам входящих пакетов* — при установленном флаге включен режим по умолчанию;

– *Всегда изменять DSCP* — при установленном флаге тег DSCP будет переписан согласно таблице изменений, DSCP расширенного режима (Качество обслуживания → Расширенный режим→ Изменение DSCP). Данная функция может быть активна только, если установлен доверительный режим по DSCP.

2.8.3.2 Настройка таблицы переопределения кодов DSCP

В разделе **Качество обслуживания → Расширенный режим→ Настройка соответствия DSCP** выполняется настройка таблицы перемаркировки DSCP. Когда объем трафика превышает установленный допустимый предел, используется таблица «Настройка соответствия DSCP» для определения DSCP-тега, который будет использоваться вместо DSCP-тега входящего пакета.



– *DSCP входящих пакетов* — DSCP-тег входящего пакета в расширенном режиме;

– *DSCP исходящих пакетов* — DSCP-тег исходящего пакета в расширенном режиме.

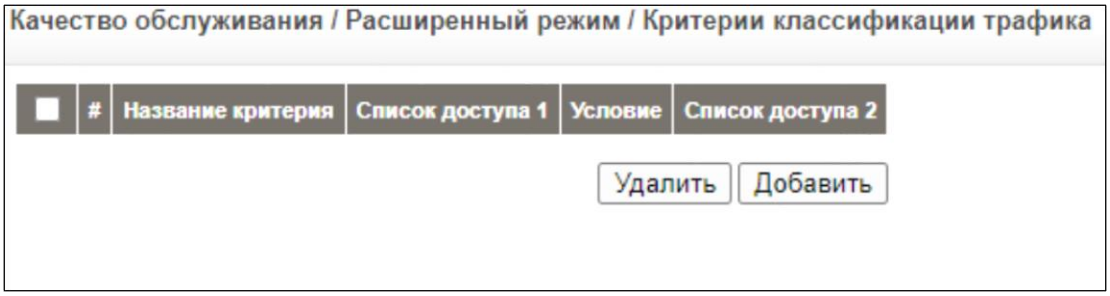
Нажмите кнопку «Сохранить» для применения настроек.

2.8.3.3 Настройка критериев классификации трафика

В разделе **Качество обслуживания → Расширенный режим → Критерии классификации трафика** выполняется настройка класса для классификации трафика: добавляются критерии отбора трафика и настраивается взаимосвязь критериев, образующих класс.

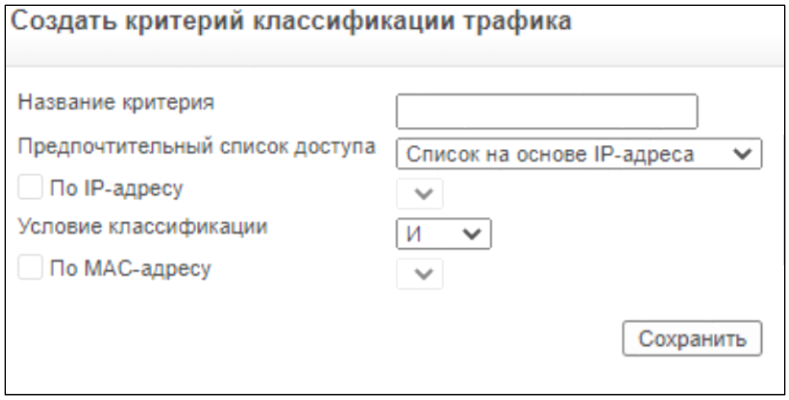
Класс образуется одним или двумя списками контроля доступа (ACL), один из которых может быть IP ACL, а второй — MAC ACL. Два списка ACL одного типа не могут быть использованы в одном классе.

Для удаления записи из таблицы классов установите флаг напротив заданной записи и нажмите кнопку «Удалить».



- *Название критерия* — имя класса;
- *Список доступа 1* — имя списка контроля доступа, основанного на IP (настройки ACL IP выпол–няются в разделе *Сетевая безопасность / Списки доступа / По IP-адресу*);
- *Условие* — правило сочетания критериев ACL1 и ACL2:
  - *И* — пакет должен соответствовать всем условиям, присутствующим в списках IP ACL и MAC ACL;
  - *ИЛИ* — пакет должен соответствовать всем условиям одного из списков IP ACL или MAC ACL;
- *Список доступа 2* — имя списка контроля доступа, основанного на MAC (настройки ACL MAC выполняются в разделе *Сетевая безопасность / Списки доступа / По MAC-адресу*).

Для добавления новой записи в таблицу классов нажмите кнопку «Добавить» и заполните соответствующие поля:



– *Название критерия* — имя класса;

– *Предпочтительный список доступа* — предпочтение списка ACL:

  ▪ *Список на основе IP-адреса* — первым применяются список контроля доступа, основан–ный на IP;

  ▪ *Список на основе MAC-адреса* — первым применяются список контроля доступа, осно–ванный на MAC;

– *По IP-адресу* — список контроля доступа уровня IP (IP ACL);

– *Условие классификации* — правило сочетания критериев:

  ▪ *И* — пакет должен соответствовать всем условиям списков IP ACL и MAC ACL;

  ▪ *ИЛИ* — пакет должен соответствовать всем условиям одного из списков — IP ACL или MAC ACL;

– *По MAC-адресу* — список контроля доступа уровня MAC (MAC ACL).

Нажмите кнопку «Сохранить» для применения настроек.

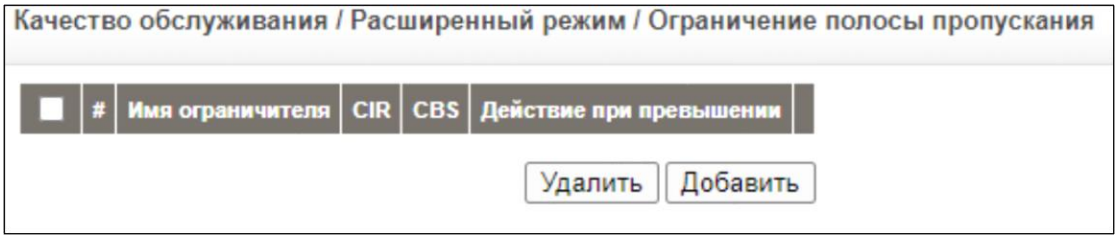
2.8.3.4 Настройка профиля ограничения скорости

В разделе **Качество обслуживания → Расширенный режим → Ограничение полосы пропускания** выполняется настройка профиля ограничения скорости. Назначение данного профиля в разделе **Качество обслуживания → Расширенный режим → Привязка критериев классификации тарифа к политике** позволяет ограничить полосу пропускания канала и в то же время гарантировать определенную скорость передачи данных.

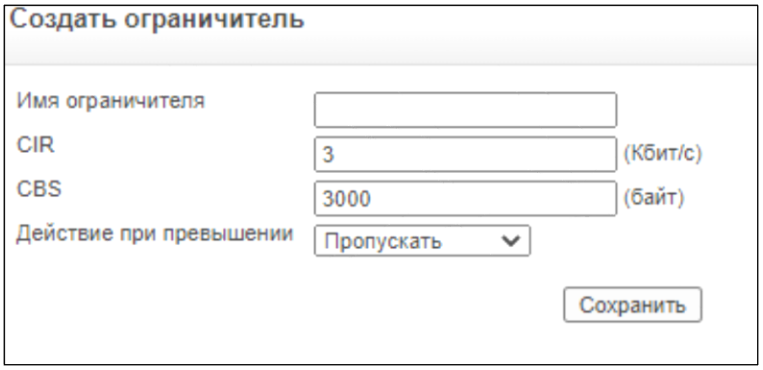
После завершения классификации пакета запускается процедура контроля параметров. Анализатор проверяет соответствие интенсивности входящего потока данных установленным ограничениям по скорости и применяет заданное действие к трафику, нарушающему пределы. В качестве таких действий могут быть: трансляция (forwarding), отбрасывание (dropping) или переназначение кода DSCP пакета данных.

Профиль ограничения скорости устанавливает ограничения на группу потоков данных и объединяет несколько политик контроля трафика (policy map).

Профиль не может быть удален, если он используется хотя бы одной политикой контроля. Для управления полосой пропускания используется алгоритм «корзины маркеров». Задачей алгоритма является принятие решения: передать пакет или отбросить. Параметрами алгоритма являются — скорость поступления маркеров в «корзину» (CIR) и объём «корзины» (CBS).



Для добавления новой записи в таблицу нужно нажать кнопку «Добавить» и заполнить соответствующие поля:



– *Имя ограничителя* — имя профиля ограничения скорости;

– *CIR* — фиксированная скорость входящего потока данных (3–57982058) Кбит/с;

– *CBS* — фиксированный размер «вспышки» трафика (3000–19173960) байт;

– *Действие при превышении* — действие, назначаемое пакетам, которые превысят установленные ограничения:

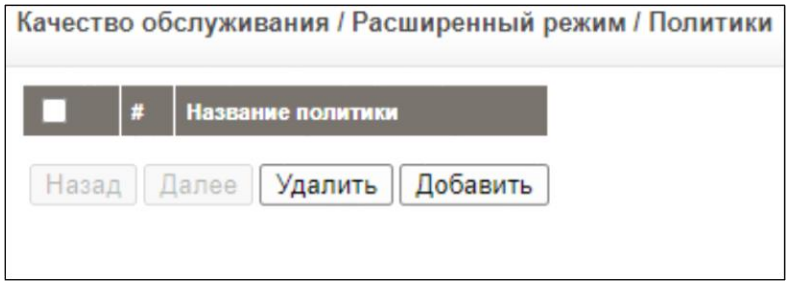
  - *Отбрасывать* — пакет будет отброшен, когда «корзина» будет опустошена;
  - *Изменять DSCP* — при опустошении «корзины», значение DSCP будет переопределено;
  - *Пропускать* — пересылать пакеты.

Нажмите кнопку «Сохранить» для применения настроек.

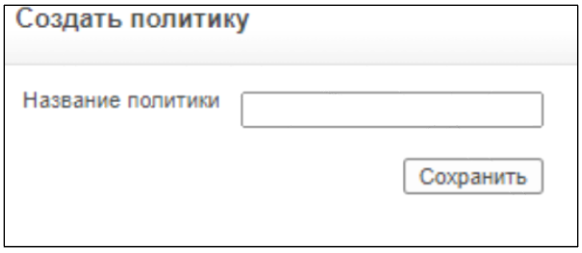
Для удаления записи из таблицы нужно установить флаг напротив заданной записи и нажать кнопку «Сохранить».

2.8.3.5 Установка имен политик QoS

В разделе **Качество обслуживания → Расширенный режим → Политики** задается имя политики QoS. Настройка политики QoS выполняется в разделе **Качество обслуживания → Расширенный режим → Привязка критериев классификации тарифа к политике.**



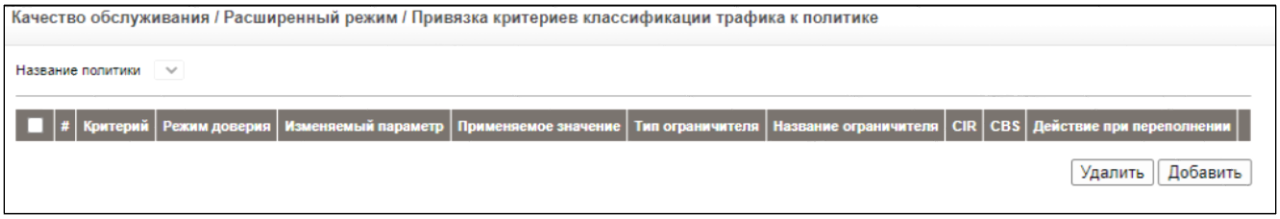
Для добавления новой записи в таблицу нужно нажать кнопку «Добавить», указать имя политики QoS и нажать кнопку «Сохранить».



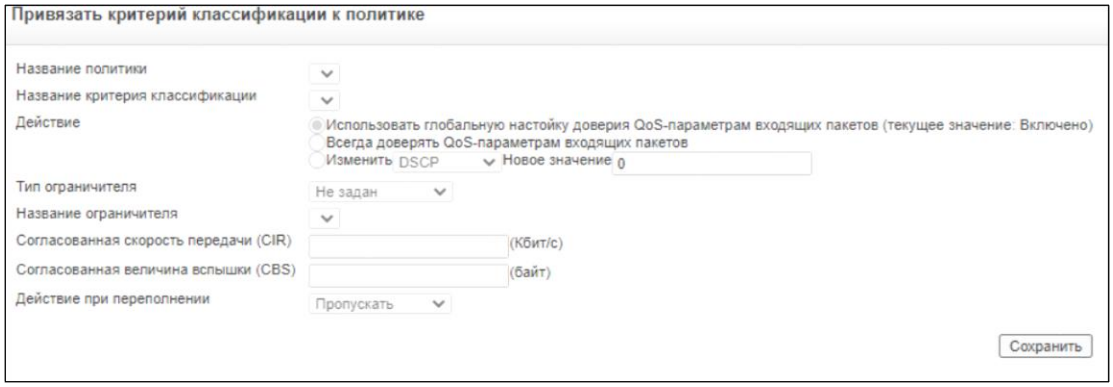
Для удаления записи из таблицы нужно установить флаг напротив заданной записи и нажать кнопку «Удалить».

2.8.3.6 Настройка профилей политик QoS

В разделе **Качество обслуживания → Расширенный режим → Привязка критериев классификации тарифа к политике** выполняется настройка профилей политик QoS. После выполнения настроек профиль можно назначить определенному интерфейсу в разделе **Качество обслуживания → Расширенный режим → Привязка политики к интерфейсу**.



Для добавления новой записи в таблицу нужно нажать кнопку «Добавить» и заполнить соответствующие поля:



– *Название политики* — имя политики;

– *Название критерия классификации* — имя записи критериев классификации трафика, которая будет применена в текущем профиле;

– *Действие* — дополнительные действия для классификации:

  - *Использовать глобальную настройку доверия QoS-параметрам входящих пакетов* (текущее значение: Включено) — использовать доверительный режим по умолчанию;
  - *Всегда доверять QoS-параметрам входящих пакетов* — включить доверительный режим для классификации;
  - *Изменить* — установить новые значения для DSCP, Queue, Cos/802.1p;
  - *Новое значение* — новое значение атрибута «Set»;

– *Тип ограничителя* — тип ограничителя скорости:

  - *Агрегированный* — при выборе данного параметра устанавливается профиль ограничения скорости (Название ограничителя);
  - *Одиночный* — при выборе данного параметра можно задать ограничения скорости вручную, заполнив поля *Ingress Согласованная скорость передачи (CIR), Согласованная величина вспышки (CBS);*

– *Название ограничителя* — из ниспадающего списка выбрать созданный ранее профиль ограничения скорости;

– *Согласованная скорость передачи (CIR)* — гарантированная полоса пропускания (3–10485760) Кбит/с;

– *Согласованная величина вспышки (CBS)* — размер сдерживающего порога (3000–19173960) байт;

– *Действие при переполнении* — действие, назначаемое пакетам, которые превысят установленные ограничения скорости:

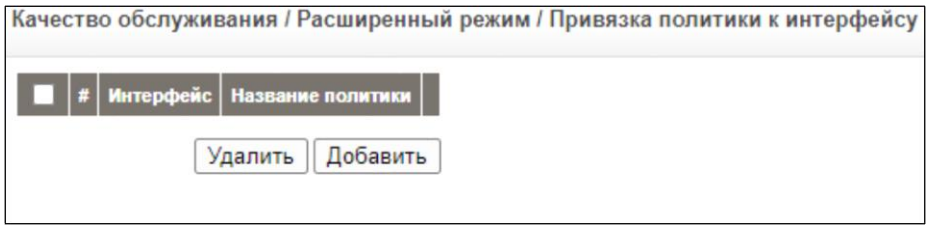
  - *Отбрасывать* — отбрасывать пакеты;
  - *Изменять DCSP* — изменить код DSCP в соответствии с таблицей QoS → Advances Mode→ DSCP Mapping;
  - *Пропускать* — пересылать пакеты.

Нажмите кнопку «Сохранить» для применения настроек.

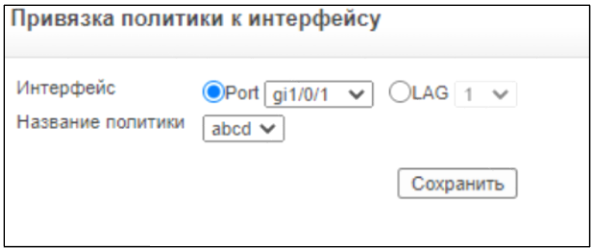
Для удаления записи из таблицы установите флаг напротив заданной записи и нажмите кнопку «Удалить». Для редактирования записи нажмите кнопку «Редактировать».

2.8.3.7 Назначение политики QoS интерфейсу

В разделе **Качество обслуживания → Расширенный режим → Привязка политики к интерфейсу** выполняется назначение политики QoS определенному интерфейсу.



Для добавления новой записи в таблицу нужно нажать кнопку «Добавить» и заполнить соответствующие поля:



– *Интерфейс* — интерфейс, для которого выполняются настройки:

  - *Порт* — номер интерфейса, (gi0/1—gi0/48, te0/1—te0/4);
  - *LAG* — номер группы LAG, (1–48);

– *Название политики* — имя политики, которая назначается данному интерфейсу.

Нажмите кнопку «Сохранить» для применения настроек.

Для удаления записи из таблицы нужно установить флаг напротив заданной записи и нажать кнопку «Удалить». Для редактирования записи нажмите кнопку «Редактировать».

2.9 Удаленный мониторинг состояния сети RMON

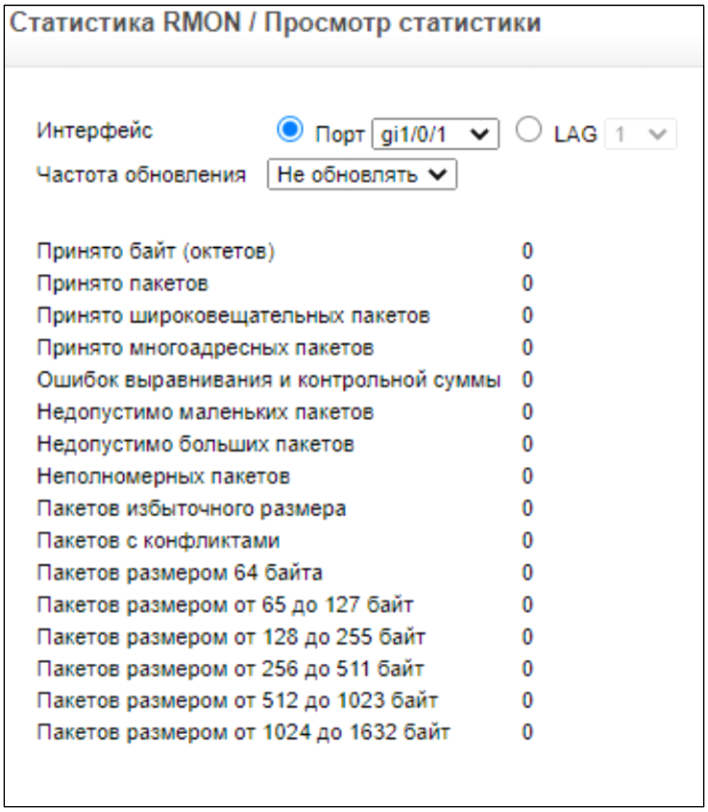
В разделе **Статистика RMON** для администратора сети предоставляется удаленный мониторинг (RMON) состояния сети.

Протокол мониторинга сети (RMON) является расширением протокола SNMP, позволяя предоставить более широкие возможности контроля сетевого трафика. Отличие RMON от SNMP состоит в характере собираемой информации — данные собираемые RMON в первую очередь характеризуют трафик между узлами сети. Информация, собранная агентом, передается в приложение управления сетью.

Стандарт RMON предусматривает четыре группы мониторинга: статистика, журнал, сигналы тревоги и события.

2.9.1 Просмотр статистики RMON

В разделе **Статистика RMON → Просмотр статистики** отображаются текущие накопленные статистические данные о характеристиках пакетов, количестве коллизий.



– *Интерфейс* — интерфейс, для которого отображается статистика:

  - *Порт* — номер интерфейса, (gi0/1—gi0/48, te0/1—te0/4);
  - *LAG* — номер группы LAG, (1–48);

– *Частота обновления* — период обновления статистики:

  - *15 сек* — каждые 15 секунд;
  - *30 сек* — каждые 30 секунд;
  - *60 сек* — каждые 60 секунд;
  - *Не обновлять* — не обновляется;

– *Принято байт (октетов)* — количество байт данных (включая байты плохих пакетов), принятых из сети (исключая фреймовые биты, но включая биты контрольной суммы);

– *Принято пакетов* — общее число полученных пакетов (включая ошибочные);

– *Принято широковещательных пакетов* — количество принятых широковещательных пакетов (только корректные пакеты);

– *Принято многоадресных пакетов* — количество принятых многоадресных пакетов (только корректные пакеты);

- *Ошибок выравнивания и контрольной суммы* — количество принятых пакетов длиной от 64 до 1518 байт включительно, имеющих неверную контрольную сумму либо с целым числом байт (ошибки проверки контрольной суммы — FCS), либо с нецелым числом байт (ошибки выравнивания — Alignment);

- *Недопустимо маленьких пакетов* — количество принятых пакетов длиной меньше 64 байт (исключая фреймовые биты, но включая биты контрольной суммы), но в остальном правильно сформированных;

- *Недопустимо больших пакетов* — количество принятых пакетов длиной больше 1518 байт (исключая фреймовые биты, но включая биты контрольной суммы), но в остальном правильно сформированных;

- *Неполномерных пакетов* — количество принятых пакетов длиной меньше 64 байт (исключая фреймовые биты, но включая биты контрольной суммы), имеющих неверную контрольную сумму либо с целым числом байт (ошибки проверки контрольной суммы — FCS), либо с нецелым числом байт (ошибки выравнивания — Alignment);

- *Пакетов избыточного размера* — количество принятых пакетов длиной больше 1518 байт (исключая фреймовые биты, но включая биты контрольной суммы), имеющих неверную контрольную сумму либо с целым числом байт (ошибки проверки контрольной суммы — FCS), либо с нецелым числом байт (ошибки выравнивания — Alignment);

- *Пакетов с конфликтами* — оценка количества коллизий на данном Ethernet сегменте;

- *Пакетов размером 64 байта* — количество принятых пакетов (включая плохие пакеты) длиной 64 байта (исключая фреймовые биты, но включая биты контрольной суммы);

- *Пакетов размером от 65 до 127 байт* — количество принятых пакетов (включая плохие пакеты) длиной от 65 до 127 байт включительно (исключая фреймовые биты, но включая биты контрольной суммы);

- *Пакетов размером от 128 до 255 байт* — количество принятых пакетов (включая плохие пакеты) длиной от 128 до 255 байт включительно (исключая фреймовые биты, но включая биты контрольной суммы);

- *Пакетов размером от 256 до 511 байт* — количество принятых пакетов (включая плохие пакеты) длиной от 256 до 511 байт включительно (исключая фреймовые биты, но включая биты контрольной суммы);

- *Пакетов размером от 512 до 1023 байт* — количество принятых пакетов (включая плохие пакеты) длиной от 512 до 1023 байт включительно (исключая фреймовые биты, но включая биты контрольной суммы);

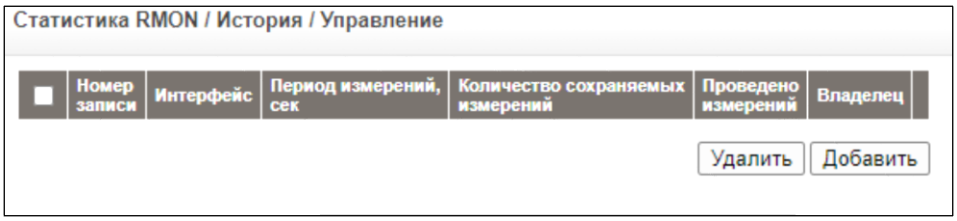
- *Пакетов размером от 1024 до 1632 байт* — количество принятых пакетов (включая плохие пакеты) длиной от 1024 до 1632 байт включительно (исключая фреймовые биты, но включая биты контрольной суммы).

2.9.2 Просмотр и настройка журнала RMON

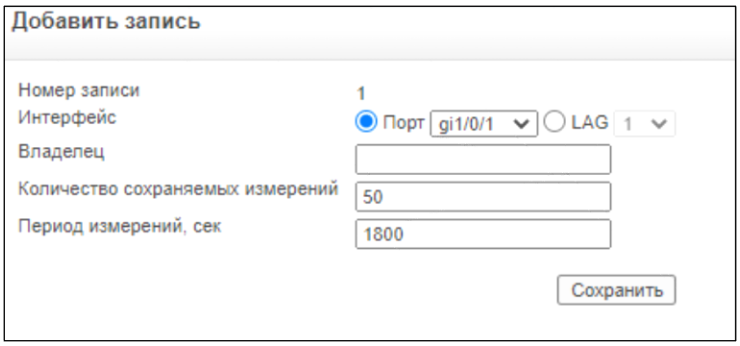
В разделе **Статистика RMON → История** можно настроить и посмотреть журнал RMON.

2.9.2.1 Настройка журнала RMON

В разделе **Статистика RMON → История → Управление** выполняется настройка журнала RMON: задается количество выборок, которое может храниться в журнале, и интервал между последовательными выборками.



Для добавления новой записи в таблицу нужно нажать кнопку «Добавить» и заполнить соответствующие поля:



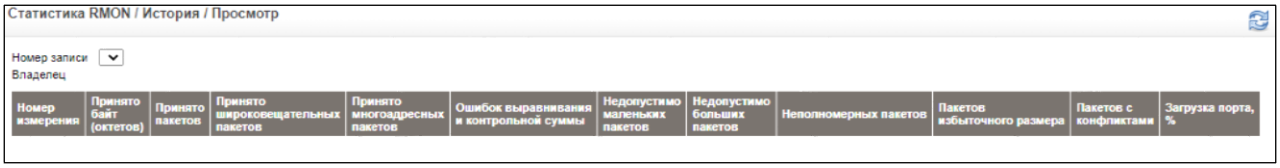
- *Номер записи* — номер записи;
- *Интерфейс* — интерфейс, из которого были получены выборки:
  - *Порт* — номер интерфейса, (gi0/1—gi0/48, te0/1—te0/4);
  - *LAG* — номер группы LAG, (1–48);
- *Владелец* — устройство или пользователь, который запрашивает RMON-информацию. Размер поля (0–20) символов;
- *Количество сохраняемых измерений* — максимальное количество выборок для хранения, (1–65535). Значение по умолчанию 50;
- *Период измерений, сек* — интервал между последовательными выборками, (1–3600) секунд. По умолчанию установлено 1800 секунд.

Нажмите кнопку «Сохранить» для применения настроек.

Для удаления записи из таблицы нужно установить флаг напротив заданной записи и нажать кнопку «Удалить». Для редактирования записи нажать кнопку «Редактировать».

2.9.2.2 Просмотр журнала RMON

В разделе **Статистика RMON → История → Просмотр** осуществляется просмотр журнала RMON. Статистические данные сохраняются в журнале через определенные промежутки времени для последующего анализа тенденций.



– *Номер записи* — номер записи журнала;

– *Владелец* — устройство или пользователь, который запрашивает RMON-информацию;

– *Номер измерения* — номер выборки, из которого были взяты статистические данные;

– *Принято байт (октетов)* — количество принятых байт на интерфейсе с последней перезагрузки устройства. В данное число включены пакеты с дефектами и байты FCS, исключая фреймовые биты;

– *Принято пакетов* — количество принятых пакетов на заданном интерфейсе с последней перезагрузки устройства. В данное число включены пакеты с дефектами, пакеты широковещательной и многоадресной рассылки;

– *Принято широковещательных пакетов* — количество хороших широковещательных пакетов, принятых на заданном интерфейсе с последней перезагрузки устройства. В данное число не включены пакеты многоадресной рассылки;

– *Принято многоадресных пакетов* — количество хороших многоадресных пакетов, принятых на заданном интерфейсе с последней перезагрузки устройства;

– *Ошибок выравнивания и контрольной суммы* — количество ошибок CRC (не верная контрольная сумма) и Align (не целое число байт) в принятых пакетах на заданном интерфейсе с последней перезагрузки устройства;

– *Недопустимо маленьких пакетов* — количество принятых пакетов длиной менее 64 байта (исключая фреймовые биты, но включая биты контрольной суммы), но в остальном правильно сформированных;

– *Недопустимо больших пакетов* — количество принятых пакетов длиной более 1518 байтов (исключая фреймовые биты, но включая биты контрольной суммы), но в остальном правильно сформированных;

– *Неполномерных пакетов* — количество принятых пакетов длиной менее 64 байта (исключая фреймовые биты, но включая биты контрольной суммы), имеющих неверную контрольную сумму либо с целым числом байт (ошибки проверки контрольной суммы — FCS), либо с нецелым числом байт (ошибки выравнивания — Alignment);

– *Пакетов избыточного размера* — количество принятых пакетов длиной более 1518 байтов (исключая фреймовые биты, но включая биты контрольной суммы), имеющих неверную

контрольную сумму либо с целым числом байт (ошибки проверки контрольной суммы — FCS), либо с нецелым числом байт (ошибки выравнивания — Alignment);

– *Пакетов с конфликтами* — оценка количества коллизий на заданном интерфейсе с последней перезагрузки устройства;

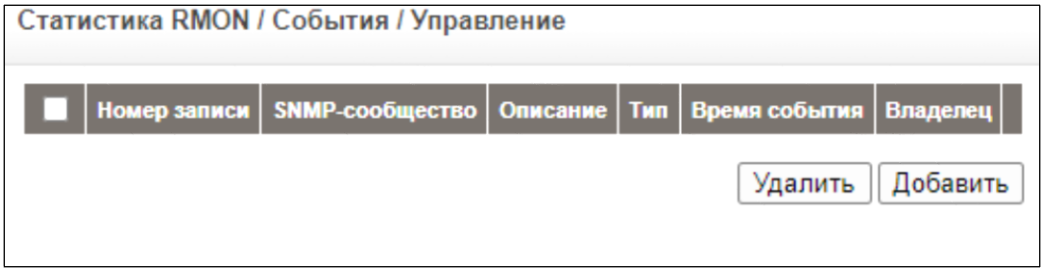
– *Загрузка порта, %* — оценка средней пропускной способности физического уровня на заданном интерфейсе с последней перезагрузки устройства. Пропускная способность оценивается величиной до тысячной процента.

2.9.3 Просмотр и настройка условий регистрации и генерации событий

В разделе **Статистика RMON → События** можно настроить и посмотреть условия регистрации и генерации событий.

2.9.3.1 Настройка условий регистрации и генерации событий

В разделе **Статистика RMON → События → Управление** выполняется настройка условий регистрации и генерации событий.

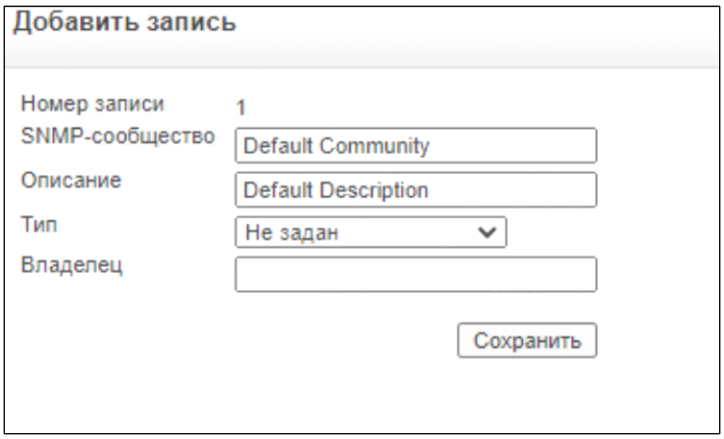


– *Номер записи* — идентификатор события;
– *SNMP-сообщество* — строка сообщества SNMP для пересылки trap-сообщений;
– *Описание* — описание события;
– *Тип* — тип уведомления, генерируемого устройством по этому событию:
  - *Не задан* — не генерировать уведомления;
  - *Запись в журнале* — генерировать запись в таблице;
  - *Оповещение* — отсылать SNMP trap;
  - *Запись и оповещение* — генерировать запись в таблице и отсылать SNMP trap;
– *Время события* — время и дата последнего сгенерированного события;
– *Владелец* — пользователь, создавший событие.

Для удаления записи из таблицы установите флаг напротив заданной записи и нажмите кнопку «Удалить».

Для редактирования параметров нажмите кнопку «Редактировать», заполните соответствующие поля и нажмите кнопку «Сохранить» для сохранения настроек.

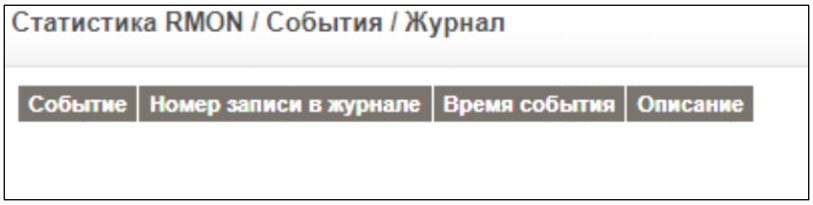
Для добавления записи в таблицу нажмите кнопку «Добавить» заполните поля: SNMP-сообщество, Описание, Тип, Владелец:



Нажмите кнопку «Сохранить» для применения настроек.

2.9.3.2 Просмотр событий, сгенерированных на устройстве

В разделе **Статистика RMON → События → Журнал** осуществляется просмотр событий, сгенерированных на устройстве.



– *Событие* — идентификатор события RMON;

– *Номер записи в журнале* — номер записи;

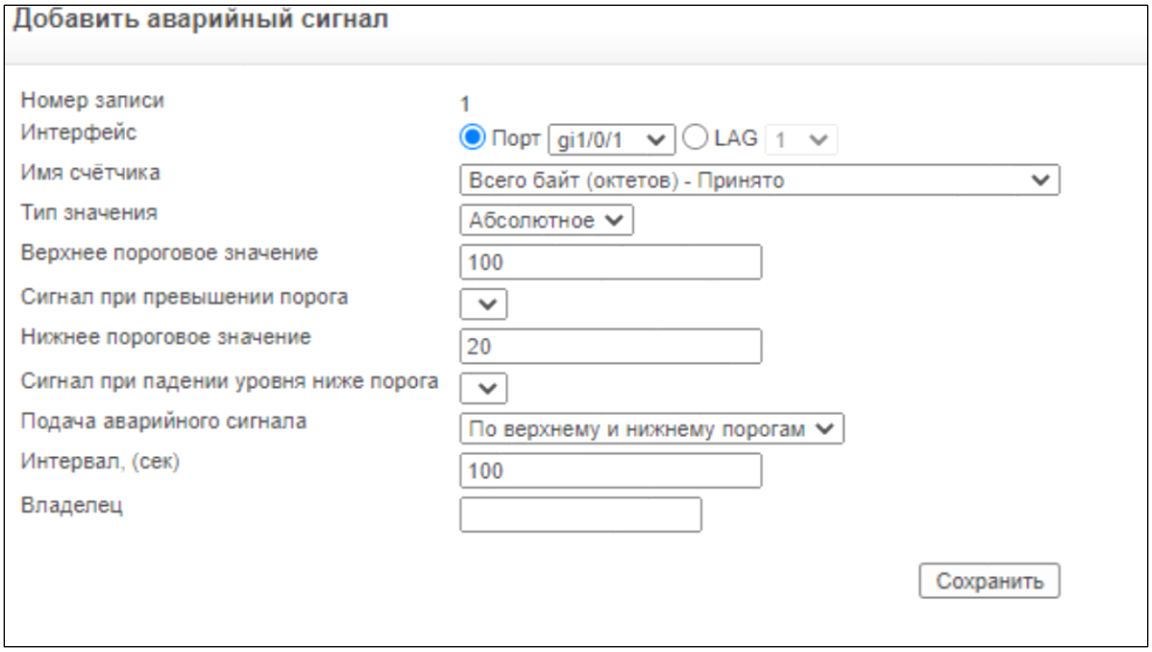
– *Время события* — время, когда была создана запись;

– *Описание* — описание события.

2.9.4 Настройка аварийной сигнализации

В разделе **Статистика RMON → Аварийные сигналы** осуществляется настройка пороговых значений статистических показателей, при превышении которых агент RMON посылает сообщение об аварии менеджеру.

Для добавления новой записи в таблицу нужно нажать кнопку «Добавить» и заполнить соответствующие поля:



– *Номер записи* — номер записи Alarm;

– *Интерфейс* — интерфейс, для которого отображается статистика:

  ▪ *Порт* — номер интерфейса, (gi0/1—gi0/48, te0/1—te0/4);

  ▪ *LAG* — номер группы LAG, (1–48);

– *Имя счетчика* — имя переменной MIB;

– *Тип значения* — метод отбора указанных переменных и подсчета значения для сравнения с границами:

  ▪ *Дельта* — значение выбранной переменной при последнем отборе будет вычтено из текущего значения и разница будет сравнена с границами (разница между значениями переменной в конце и в начале контрольного интервала);

- *Абсолютное* — абсолютное значение выбранной переменной будет сравнено с границей на конце исследуемого интервала;

– *Верхнее пороговое значение* — восходящая граница;

– *Сигнал при превышении порога* — способ уведомления, генерируемого устройством в случае превышения верхней границы:

- *LOG* — генерировать запись в таблице;
- *TRAP* — отсылать SNMP trap-сообщения;
- *Both* — генерировать запись в таблице и отсылать SNMP trap-сообщения;

– *Нижнее пороговое значение* — нисходящая граница;

– *Сигнал при падении уровня ниже порога* — способ уведомления, генерируемого устройством в случае нарушения нижней границы;

– *Подача аварийного сигнала* — правило генерации аварийных событий для первого контрольного интервала путем сравнения отобранной переменной с одной, либо обеими границами:

- *По верхнему порогу* — генерировать единичное аварийное событие по восходящей границе, если значение отобранной переменной на первом контрольном интервале больше либо равно этой границе;

- *По нижнему порогу* — генерировать единичное аварийное событие по нисходящей границе, если значение отобранной переменной на первом контрольном интервале меньше либо равно этой границе;

- *По верхнему и нижнему порогам* —генерировать единичное аварийное событие по восходящей и/или нисходящей границе, если значение отобранной переменной на первом контрольном интервале больше либо равно восходящей границе, и/или меньше либо равно нисходящей границе;

– *Интервал, (сек)* — интервал, в течение которого данные отбираются и сравниваются с верхней и нижней границами, в секундах;

– *Владелец* — устройство или пользователь, который определяет аварийную ситуацию.

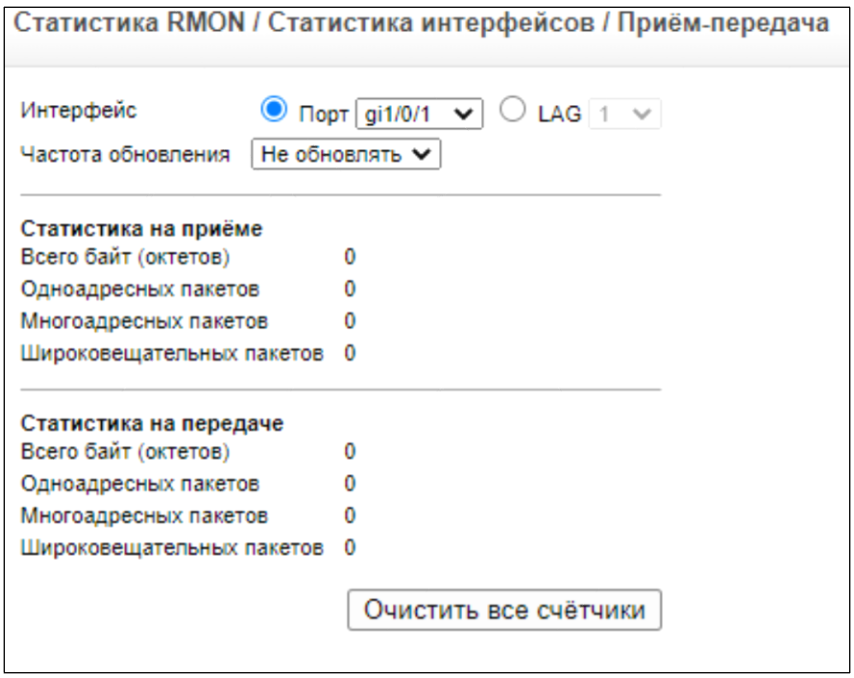
Нажмите кнопку «Сохранить» для применения настроек.

Для удаления записи из таблицы нужно установить флаг напротив заданной записи и нажать кнопку «Удалить». Для редактирования записи нажать кнопку «Редактировать».

2.9.5 Просмотр статистики на интерфейсе

2.9.5.1 Статистика по полученным/переданным пакетам

В разделе **Статистика RMON → Статистика интерфейсов → Приём-передача** можно просмотреть статистику по полученным и переданным пакетам на заданном интерфейсе.



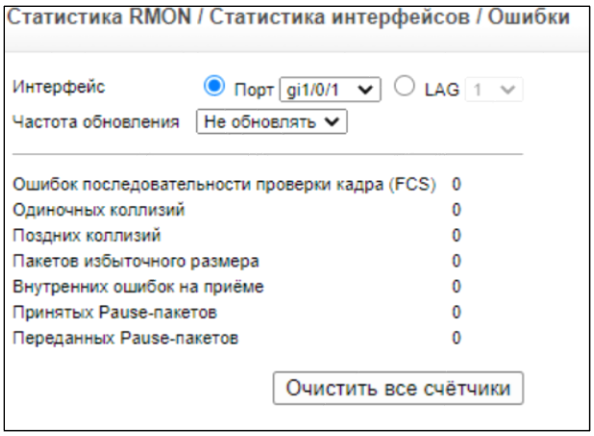
– *Интерфейс* — интерфейс, для которого отображается статистика:
  - *Порт* — номер интерфейса, (gi0/1—gi0/48, te0/1—te0/4);
  - *LAG* — номер группы LAG, (1–48);
– *Частота обновления* — время обновления статистики на интерфейсе:
  - *15 сек* — каждые 15 секунд;
  - *30 сек* — каждые 30 секунд;
  - *60 сек* — каждые 60 секунд;
  - *Не обновлять* — не обновляется;
– *Статистика на приёме* — статистика по полученным пакетам;
– *Статистика на передаче* — статистика по переданным пакетам;
– *Всего байт (октетов)* — общее количество байтов, полученных/принятых на заданном интерфейсе;
– *Одноадресных пакетов* — количество unicast-пакетов, полученных/принятых на заданном интерфейсе;
– *Многоадресных пакетов* — количество multicast-пакетов, полученных/принятых на заданном интерфейсе;
– *Широковещательных пакетов* — количество broadcast-пакетов, полученных/принятых на заданном интерфейсе;

Для обнуления всей статистики нажмите кнопку «Очистить все счётчики».

2.9.5.2 Статистика уровня Ethernet MAC интерфейса

В разделе **Статистика RMON → Статистика интерфейсов → Ошибки** выполняется просмотр статистики Ошибок для заданного интерфейса.

– *Интерфейс* — интерфейс, для которого отображается статистика:
  - *Порт* — номер интерфейса, (gi0/1—gi0/48, te0/1—te0/4);
  - *LAG* — номер группы LAG, (1—48);
– *Частота обновлений* — время обновления статистики на интерфейсе:
  - *15 сек* — каждые 15 секунд;
  - *30 сек* — каждые 30 секунд;
  - *60 сек* — каждые 60 секунд;
  - *Не обновлять* — не обновляется;



– *Ошибок последовательности проверки кадра (FCS)* — количество принятых фреймов с количеством байт, соответствующим длине, но не прошедших проверку контрольной суммы (FCS);
– *Одиночных коллизий* — количество фреймов, вовлеченных в единичную коллизию, но впоследствии переданных успешно;
– *Поздних коллизий* — количество случаев, когда коллизия зафиксирована после того, как в канал связи уже были переданы первые 64 байт (slotTime) пакета;
– *Пакетов избыточного размера* — количество принятых пакетов, размер которых превышает максимальный разрешенный размер фрейма;
– *Внутренних ошибок на приёме* — количество фреймов, которые не были приняты успешно из-за внутренней ошибки приема на уровне MAC;
– *Принятых Pause-пакетов* — количество принятых управляющих MAC-фреймов с кодом опера–ции PAUSE;
– *Переданных Pause-пакетов* — количество переданных управляющих MAC-фреймов с кодом операции PAUSE.

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-co.ru/support/**
Servicedesk: **https://servicedesk.eltex-co.ru/**

На официальном сайте компании вы можете найти техническую документацию и программное обеспечение для продукции ООО «Предприятие «ЭЛТЕКС», обратиться к базе знаний, оставить интерактивную заявку или проконсультироваться у инженеров Сервисного центра на техническом форуме:

Официальный сайт компании: **https://eltex-co.ru/**
Технический форум: **https://eltex-co.ru/forum**
База знаний: **https://docs.eltex-co.ru/display/EKB/Eltex+Knowledge+Base**
Центр загрузок: **https://eltex-co.ru/support/downloads**