Сетевой коммутатор

BOLID SW-224

Версия 2

Руководство по эксплуатации

АЦДР.203729.004 РЭп

Настоящее руководство по эксплуатации (далее по тексту – РЭ) содержит сведения о назначении, конструкции, принципе работы, технических характеристиках коммутатора сетевого BOLID SW-224 АЦДР.203729.004 (далее по тексту - коммутатор или изделие) и указания, необходимые для правильной и безопасной эксплуатации.

Изделие предназначено только для профессионального использования и рассчитано на непрерывную круглосуточную работу.

ВНИМАНИЕ!

- Руководство по эксплуатации содержит только справочную информацию, необходимую для использования его технических возможностей.
- Дизайн устройства и ПО, упомянутые в данном руководстве, подлежат изменению без обязательного предварительного письменного уведомления.
- Торговые марки и зарегистрированные торговые марки, упомянутые в данном руководстве, являются собственностью правообладателей.
- В случае нахождения неточностей или несоответствий, обращайтесь в службу поддержки.

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ

Сетевой коммутатор предназначен для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети. Поддержка технологии PoE позволяет передавать питание на различные устройства и периферию.

Коммутатор обеспечивает передачу данных от сетевых видеокамер и видеорегистраторов серверу, обеспечивает организацию электропитания сетевых видеокамер по технологии PoE. Организует среду передачи данных между сетевыми устройствами СОТ. Соответствует стандартам IEEE802.3af и IEEE802.3at, порт 1 и порт 2 поддерживают Hi-PoE. Обеспечивает поддержка кольцевого сетевого протокола STP/RSTP.

Уровень радиоизлучения изделия в соответствии с ГОСТ 12.1.006-84 допускает круглосуточное проведение обслуживающим персоналом работ, предусмотренных настоящим РЭ.

По способу защиты от поражения электрическим током изделие относится к классу 3 по ГОСТ 12.2.007.0-75.

2 ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Основные технические характеристики изделия и сервисные особенности представлены ниже (см. Таблица 2.1, Таблица 2.2).

Таблица 2.1 – Основные технические характеристики*

Наименование параметра	Значение параметра
Порты Ethernet	24 порта RJ45 10/100 Base-T (PoE Источник питания) 2 комбо-порта 10/100/1000 BASE-T/1000 Base-X(SFP)
Мощность PoE портов	Порты № 1-2 не более 60 Вт (на порт) Порт № 3-24 не более 30 Вт (на порт) Всего не более 360 Вт
Стандарты PoE	IEEE802.3af, IEEE802.3at, Hi-PoE
Коммутационная матрица	8.8 G
Маршрутизация пакетов	6.55 Mpps
Грозозащита	Основной режим: 4 кВ Дифференциальный: 2 кВ
Напряжение питания	100–240 В переменного тока
Относительная влажность воздуха	От 10 % до 90 %
Диапазон рабочих температур	От -10 °С до +55 °С
Масса	3,51 кг
Габаритные размеры	440×300×44 мм

* Технические характеристики могут отличаться от заявленных.

Таблица 2.2 – Сервисные особенности*

Наименование параметра	Значение параметра
Таблица MAC адресов	4 К
VLAN	802.1Q
Основное дерево	STP, RSTP
Агрегирование (объединение) каналов	LACP, статическое агрегирование
Зеркалирование	"Много к одному"
DHCP	DHCP-клиент
Безопасность	Привязка IP+MAC, IEEE802. 1x
Системное обслуживание	Восстановление, обновление прошивки, системный журнал
QoS	Приоритетный режим, порт/ 802.1p/ DSCP, приоритет протокола
Управление устройством	WEB интерфейс, SNMP V1/V2C/V3
Управление PoE	Настройка PoE (потребление портов в реальном времени), статистика событий PoE, Green PoE
Поддерживает модули следующих типов	1.25G 850nm,500m,LC, Multi-mode 1.25G 1310/1550nm,20km,LC, Single-mode 1.25G 1550/1310nm,20km,LC, Single-mode

* Технические характеристики могут отличаться от заявленных.

3 КОМПЛЕКТНОСТЬ

Состав изделия при поставке (комплект поставки коммутатора) представлен ниже (Таблица 3.1).

Таблица 3.1 – Комплект поставки*

Обозначение	Наименование	Количество
АЦДР.203729.004	Коммутатор «BOLID SW-224»	1 шт.
АЦДР.203729.004 РЭ	Руководство по эксплуатации изделия «BOLID SW-224»	1 экз.
	Кабель питания, 220 В переменного тока	1 шт.
	Крепление в стойку	2 шт.
	Винт М3×5	9 шт.

* Комплект поставки может отличаться от заявленного.

4 МОНТАЖ И ДЕМОНТАЖ

4.1 Меры безопасности

	ВНИМАНИЕ! Монтаж производить только при отключенном напряжении питания.
	ВНИМАНИЕ! Все виды работ с изделием во время грозы запрещаются.

1. К работе с изделием допускается персонал, изучивший настоящее руководство и получивший удостоверение о проверке знаний правил технической эксплуатации и техники безопасности.
2. Все работы по монтажу и наладке производить с соблюдением требований действующих нормативных документов по технике безопасности. Лица, производящие монтаж и наладку, должны иметь удостоверение на право работы с электроустановками напряжением до 1000 В.
3. Подключение устройства должно проводиться только к надежному источнику питания закрытого типа с надлежащими уровнями напряжения и силы тока.

4.2 Конструкция

4.2.1 Передняя панель

На рисунке (Рисунок 4.1) приведен внешний вид передней панели коммутатора, описание портов и индикаторов смотрите в таблице (Таблица 4.1).

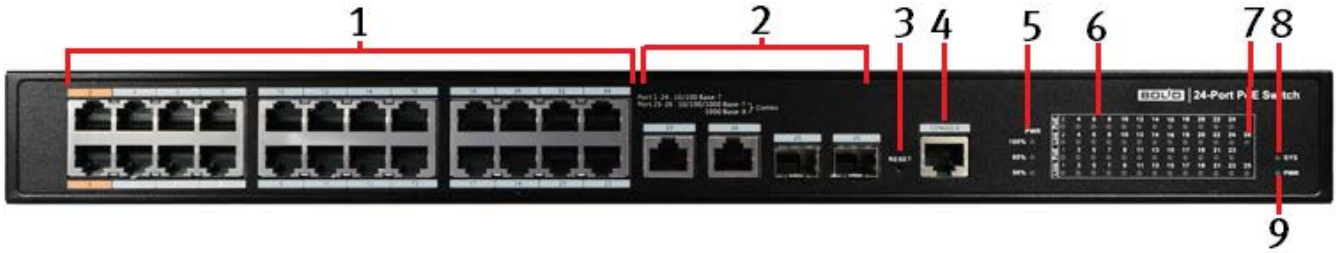

Рисунок 4.1 – Передняя панель конструкции

Таблица 4.1 – Порты и индикаторы передней панели

№	Параметр	Описание
1	RJ45 10/100 Base-T+PoE	Порты подключения PoE устройств и элементов локальной сети.
2	Комбинированные порты	10/100/1000 Base-T: Гигабитные порты с индикаторами состояния. Без PoE. Являются комбинированными (combo) портами. Не работают одновременно с Оптическими SFP портами.
		1000 Base-X: Оптические SFP порты. Являются комбинированными (combo) портами. Не работают одновременно с Гигабитными портами RJ-45.
3	RESET	Кнопка сброса на заводские настройки.
4	Console (RS-232)	Порт для прошивки.
5	PoE PWR	Световой индикатор электропитания PoE.
6	Индикаторы 1-24	Световые индикаторы состояния PoE и Uplink.
7	Индикаторы 25-26	Световые индикаторы соединения комбинированных портов.
8	SYS	Световой индикатор состояния коммутатора. Медленное мигание индикатора означает нормальную работу устройства. При загрузке устройства мигание индикатора ускорено.
9	PWR	Световой индикатор электропитания.

Для подключения к портам Ethernet следует использовать кабель «витая пара» категории 5 или 5e (CAT5 или CAT5e).

Допускается использование как экранированного, так и неэкранированного кабеля. Кабель подсоединяется к разъемам RJ45 коммутатора с помощью стандартного штекера 8P8C.

4.3 Подготовка изделия к монтажу

ВНИМАНИЕ!

При монтаже провода электропитания и выходов следует оставить достаточное пространство для легкого доступа при дальнейшем обслуживании устройства.

Габаритные размеры коммутатора приведены на рисунке ниже (Рисунок 4.2).

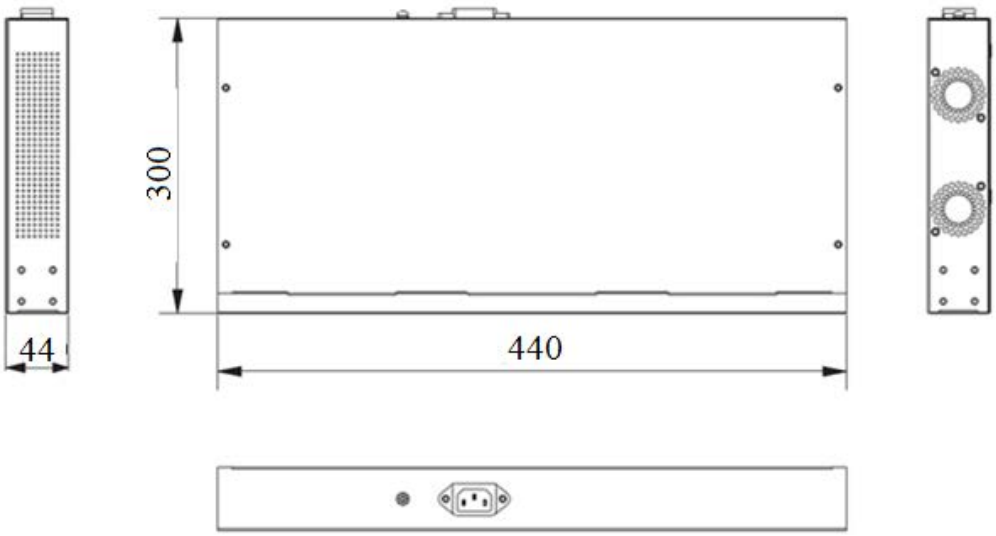

Рисунок 4.2 – Габаритные размеры

Коммутатор предназначен для установки в стойку, стенку, на полку или стол. В комплект поставки коммутатора входит комплект кронштейнов для крепления в стойку или на стену, состоящий из двух скоб и четырех винтов для крепления скоб к корпусу коммутатора.

На задней панели расположен порт для подключения кабеля питания переменного тока 100~240 В и заземления.

4.4 Подготовка изделия к монтажу и стыковке

1. Транспортирование к месту установки должно быть произведено в таре предприятия-изготовителя.
2. При распаковке и осмотре комплекта поставки необходимо проверить:

— целостность упаковки;

— комплектность и соответствие заводских номеров.

3. При вскрытии упаковки исключить попадание пыли, атмосферных осадков и влияние агрессивных сред.

4.5 Монтаж

1. Размещение и монтаж должны проводиться в соответствии с проектом, разработанным для данного объекта. При этом в проекте должны быть учтены:
   — условия эксплуатации изделий;
   — требования к длине и конфигурации линии связи.
2. Технологическая последовательность монтажных операций определяется исходя из удобства их проведения.
3. Запрещается устанавливать ближе 1 м от элементов отопления.
4. Для выбора типа кабеля и сечения проводов необходимо руководствоваться нормативной документацией.
5. Установка изделия должна отвечать следующим требованиям:
   — Индикаторы состояния на передней панели могут быть легко прочитаны;
   — Доступ к портам достаточен для свободной подводки кабелей;
   — Разъем питания находится в пределах досягаемости для подключения к источнику питания;
   — Изделие заземлено;
   — Обеспечена возможность свободной циркуляции воздуха. Следует избегать перегрева, влажных и пыльных мест;
   — Для повышения отказоустойчивости СОТ, при организации сети питания коммутатора рекомендуется использовать источники бесперебойного питания.

6. Распакуйте оборудование и проведите внешний осмотр на предмет наличия повреждений, которые могут возникнуть при транспортировке. При их наличии составьте акт в соответствии с договором о поставке, известите поставщика и направьте один экземпляр акта в адрес поставщика.

4.5.1 Монтаж коммутатора в 19”- стойку с помощью кронштейна BOLID BR-111

ПРИМЕЧАНИЕ!
Кронштейн для крепления в серверную стойку BOLID BR-111, не входит в комплект поставки устройства.

Внешний вид и габаритные размеры кронштейна для крепления (Рисунок 4.3).

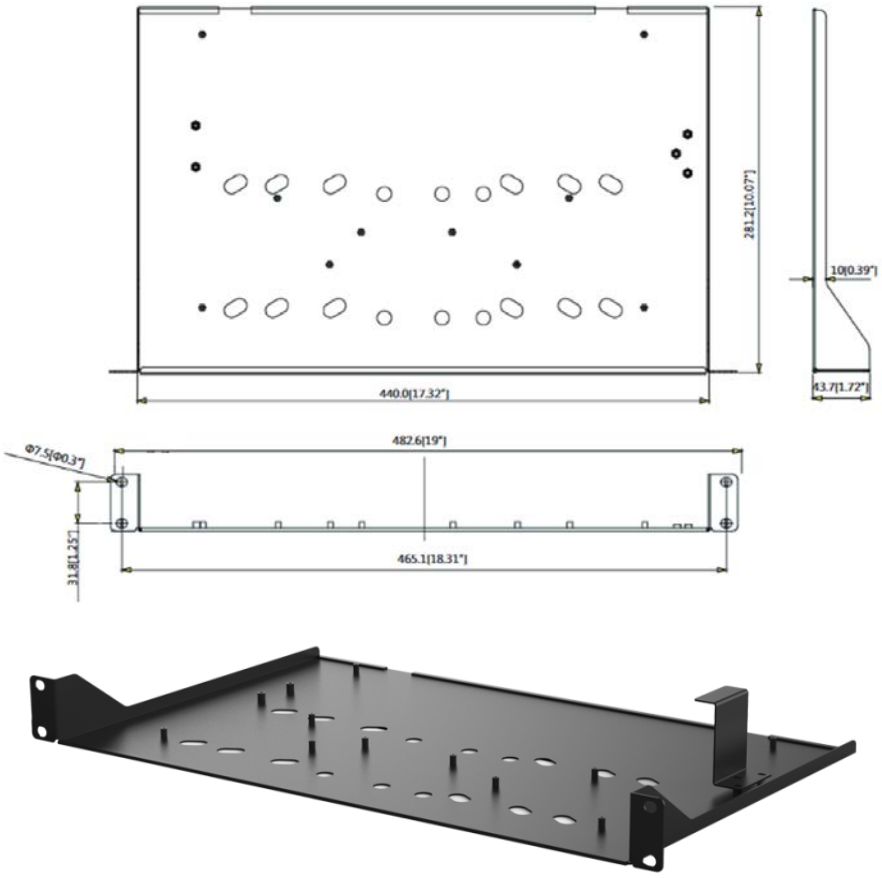

Рисунок 4.3 – Внешний вид и габариты BOLID BR-111

Основные характеристики кронштейна для крепления BOLID BR-111 (Таблица 4.2).

Таблица 4.2 – Характеристики BOLID BR-111

Параметр	Значение
Материал корпуса	Сталь
Габаритные размеры	482,6×281,2×43,7 мм
Диапазон рабочих температур	От -50 °С до +60 °С
Относительная влажность воздуха	От 0 % до 90 %
Допустимая нагрузка	Не более 5 кг
Масса	1,4 кг

4.5.1.1 Монтаж коммутатора на кронштейн BOLID BR-111

1. Установите при помощи винтов из комплекта поставки крепления в стойку на корпус коммутатора.

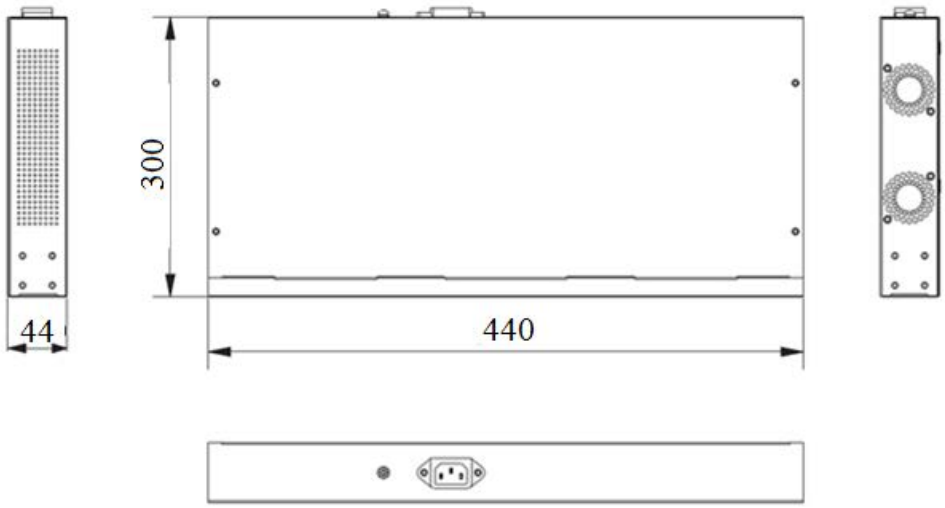

Рисунок 4.4 – Габаритные размеры

2. Установите коммутатор на кронштейн с учетом достаточного пространства для кабелей на задней панели и с учетом свободной циркуляции воздуха, не перекрывая вентиляционные отверстия.
3. Закрепите соединение при помощи винтов.

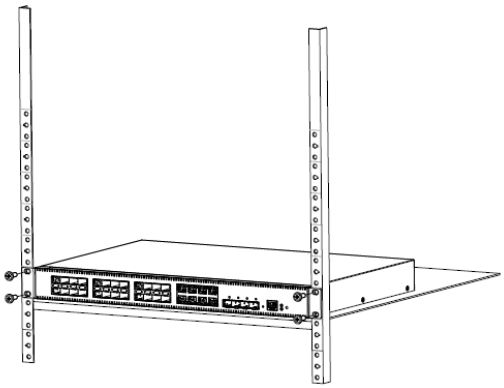

Рисунок 4.5 – Монтаж коммутатора в 19” - стойку с помощью кронштейна

4.6 Демонтаж

Демонтаж изделия производится в обратном порядке при отключенном напряжении питания.

5 ПОДКЛЮЧЕНИЕ

5.1 Первое включение

При наличии напряжения на вводе питания на передней панели коммутатора должен включиться индикатор «PWR». При наличии соединения по портам Ethernet должны включиться соответствующие индикаторы PoE / Link / Uplink. При запуске обмена данными индикаторы PoE / Link / Uplink должны начать мигать, частота мигания зависит от интенсивности обмена.

По умолчанию коммутатор имеет статический сетевой адрес IPv4:
IP адрес: 192.168.1.110
Маска подсети: 255.255.255.0
Учетные данные по умолчанию:
Имя пользователя: admin
Пароль: по умолчанию без пароля

ВНИМАНИЕ!
Из соображений безопасности следует установить пароль после первого входа в систему. Для установки/изменения пароля перейдите «Конфигурация системы => Смена пароля».

1. Убедитесь, что сетевой интерфейс компьютера находится в той же подсети, что и коммутатор.
2. Запустите Web-браузер и в адресной строке введите IP адрес коммутатора.
3. При первом входе введите имя пользователя, установите язык интерфейса и войдите в систему.

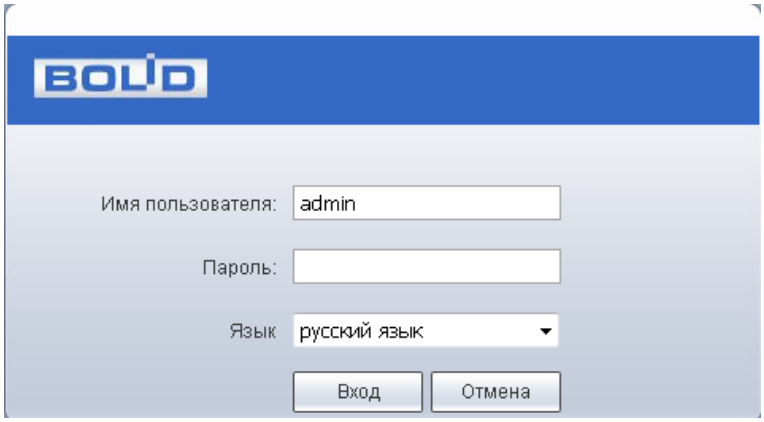

Рисунок 5.1 – Вход

4. Перейдите «Конфигурация системы => Конфигурация сети» для изменения сетевых настроек.
5. Для установки/изменения пароля перейдите «Конфигурация системы => Смена пароля». Перезагрузите устройство.
6. После изменения настроек web-интерфейс должен быть доступен по новому IP-адресу, корректный вход в систему производится с новыми учетными данными.

5.2 Информация

После входа в систему вы автоматически будете перенаправлены на панель информации о портах коммутатора. Панель включает в себя параметры состояния сети, информацию о передаваемых пакетах и состоянии соединений.

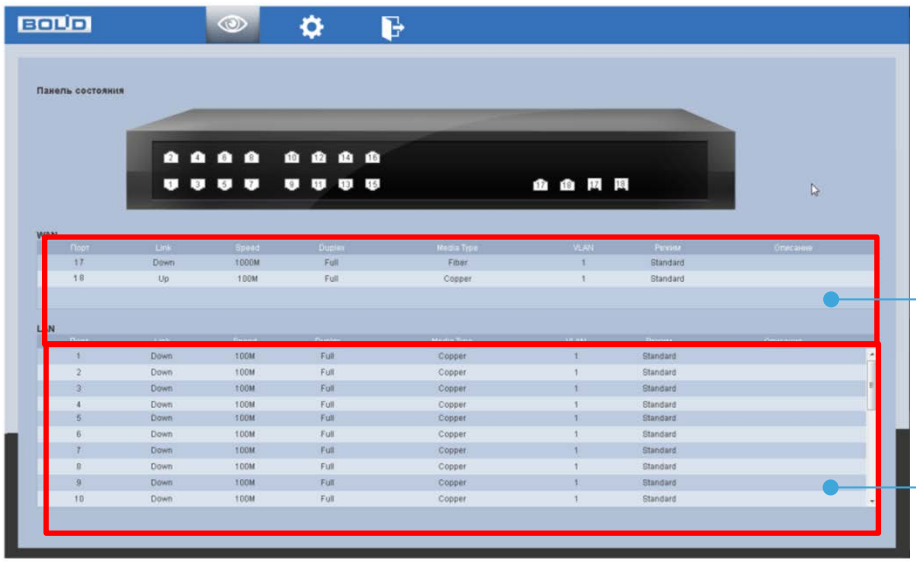

Рисунок 5.2 – Информационная панель

Таблица 5.1 – Информация о порте

Параметр	Описание
Порт	Номер порта соответствует числу на лицевой панели.
Link/Канал	— Up – Порт подключен; — Down – Порт отключен; — Disabled – Порт выключен.
Скорость/ Дуплекс	Отображает текущую скорость и в каком режиме передачи параллельном (Full) или последовательном (Half) находится порт.

Параметр	Описание
Тип носителя	Показывается тип подключенного носителя сигнала: — Copper – медный кабель; — Fiber – волоконно-оптический кабель.

6 НАСТРОЙКА

6.1 Конфигурация системы

6.1.1 Информация о системе

6.1.1.1 Информация о системе

На интерфейсе отображается версия программного обеспечения и информация о модели устройства.

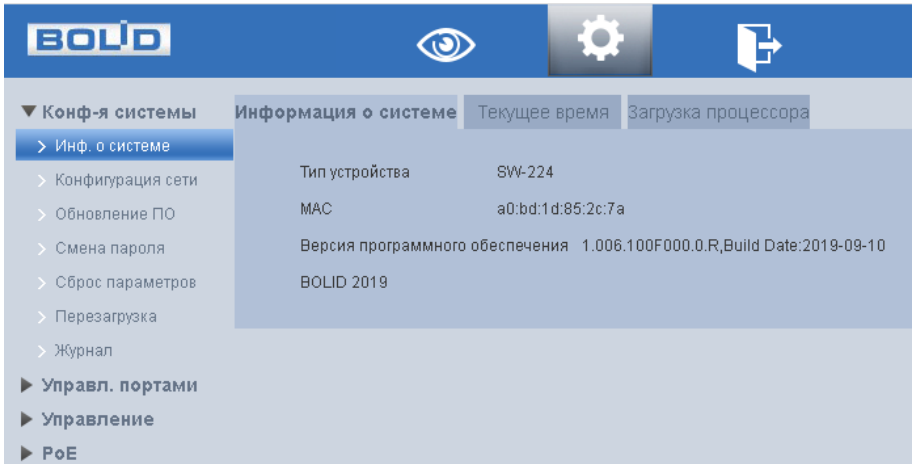

Рисунок 6.1 – Информация о системе и версии ПО

6.1.1.2 Текущее время

Интерфейс настройки/синхронизации времени на устройстве.

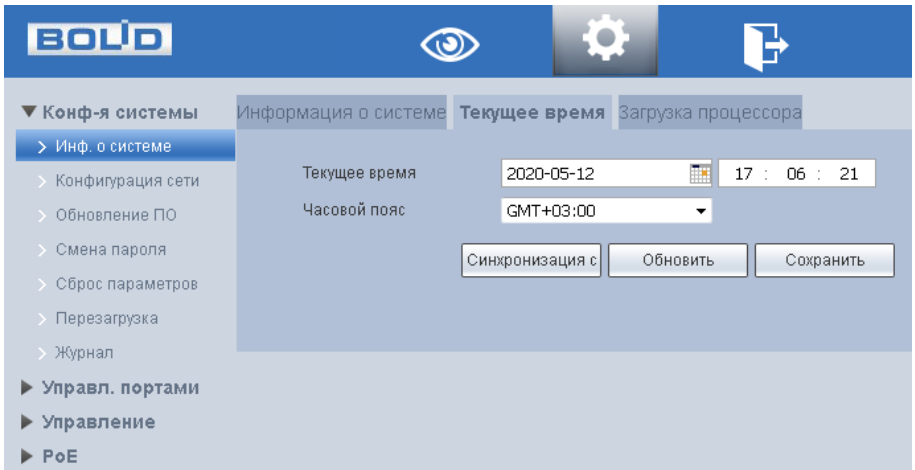

Рисунок 6.2 – Настройка/синхронизация времени

6.1.1.3 Загрузка процессора

Интерфейс мониторинга нагрузки на процессор.

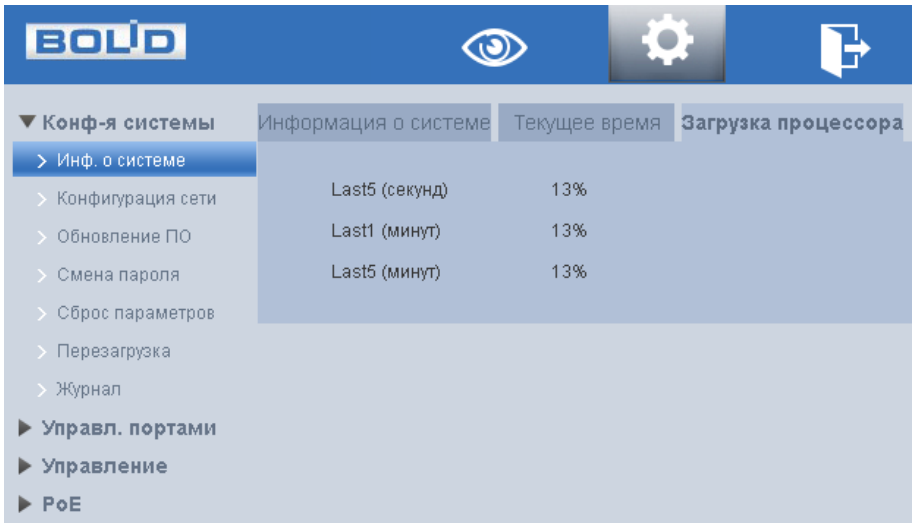

Рисунок 6.3 – Загрузка процессора

6.1.2 Конфигурация сети

Измените сетевые настройки коммутатора в соответствии с параметрами вашей сети. После внесения изменений перезагрузите устройство, перейдя в пункт меню «Перезагрузка».

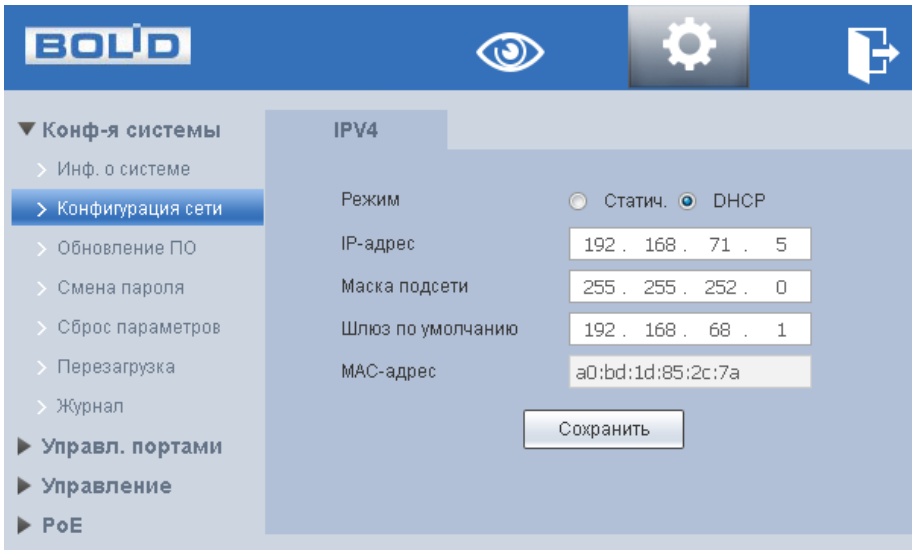

Рисунок 6.4 – Сетевые настройки

Таблица 6.1 – Сетевые настройки коммутатора

Параметр	Функция
Режим	DHCP: IP-адрес будет получен автоматически от DHCP-сервера, пользовательское задание IP/маски подсети/шлюза невозможно. Статический: в этом режиме следует задать вручную IP-адрес, маску подсети, шлюз.

Параметр	Функция
IP адрес	Служит для отображения и изменения текущего IP адреса устройства.
Маска подсети	Служит для отображения и изменения текущей маски подсети, соответствующей сегменту сети, в котором находится коммутатор.
Шлюз	Служит для отображения и изменения текущего IP-адреса шлюза. IP-адрес устройства и шлюз должны находиться в одном сегменте сети.
MAC адрес	Отображение MAC адреса устройства.

6.1.3 Обновление ПО

Для обновления ПО необходимо импортировать файл прошивки на устройство и нажать кнопку «Обновить».

ВНИМАНИЕ!
В процессе обновления ПО не отключайте питание.
Перезагрузите устройство после завершения обновления

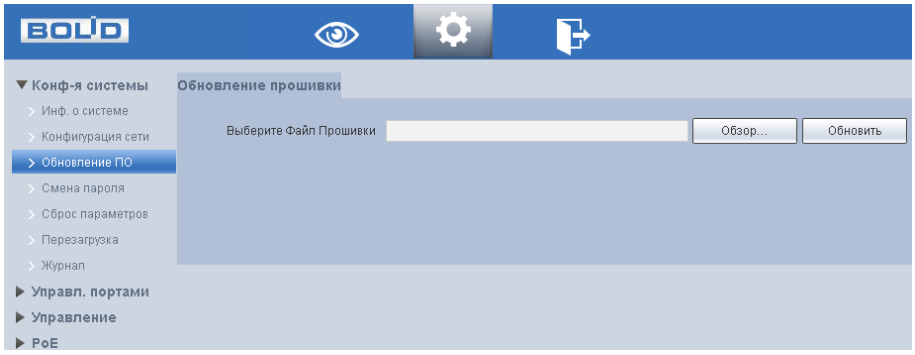

Рисунок 6.5 – Обновление ПО

6.1.4 Смена пароля

При заводских настройках пароль по умолчанию отсутствует, поэтому заполняется только панель с новым паролем. Пароль должен представлять собой комбинацию цифр, латинских букв верхнего и нижнего регистра и длиной не менее 8, но не более 32 символов. После ввода пароля нажмите «Сохранить».

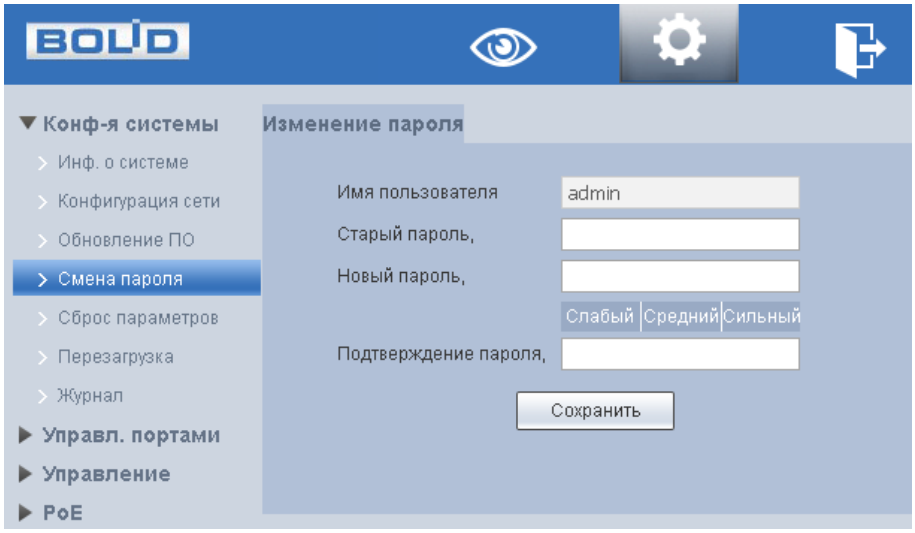

Рисунок 6.6 – Смена пароля

6.1.5 Сброс параметров

При нажатии на кнопку «По умолчанию» все ранее установленные настройки будут сброшены и восстановлены заводские настройки (кроме сетевых настроек и пароля данного коммутатора).

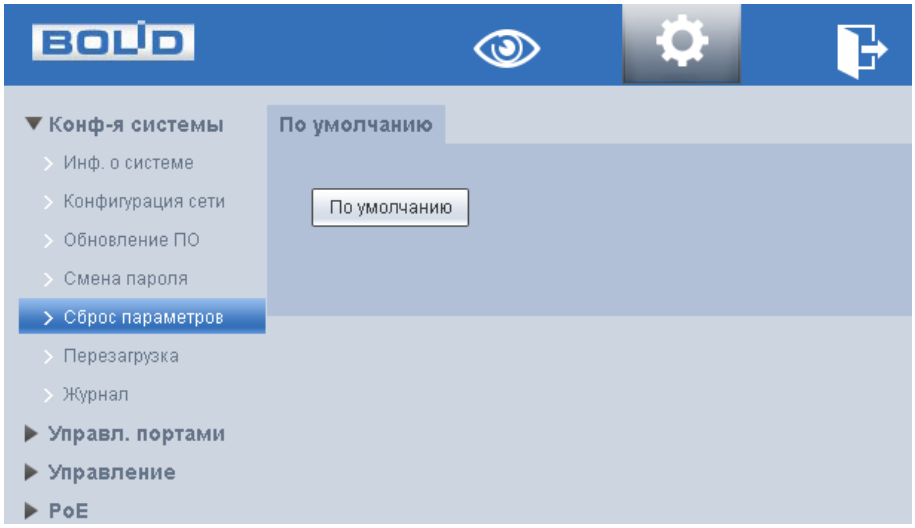

Рисунок 6.7 – Сброс до заводских параметров

6.2 Восстановление пароля

В случае невозможности восстановления пароля администратора:

1 Нажмите на кнопку «RESET» расположенной на передней панели корпуса и удерживайте ее 5 секунд.
2 Коммутатор через 20 секунд перезагрузится и все настройки вернуться к заводским.

6.2.1 Перезагрузка

Интерфейс для программной перезагрузки устройства.

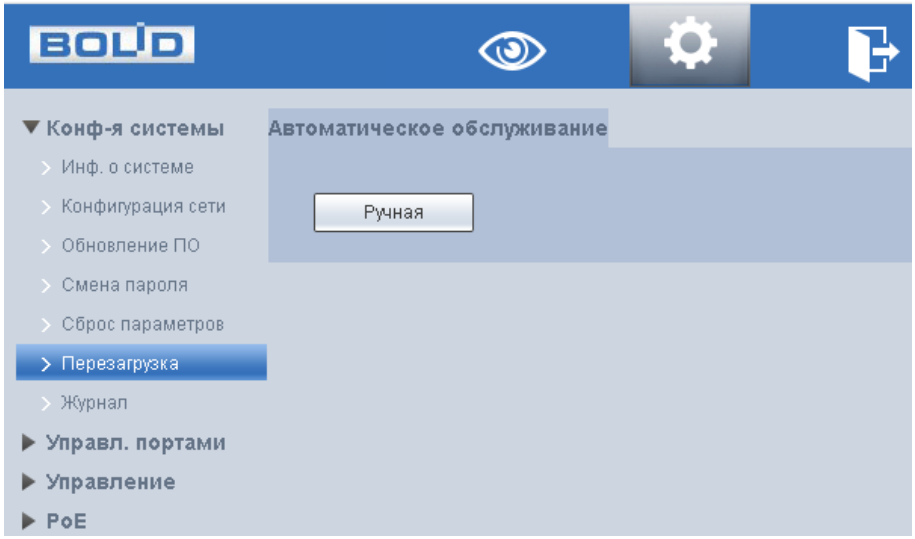

Рисунок 6.8 – Перезагрузка устройства

6.2.2 Журнал

Интерфейс предоставляет возможность просмотра и архивации информации из журнала событий регистрации и системных событий устройства.

Для поиска записи необходимо задать начальное и конечное время, выбрать тип события и нажать на кнопку «Поиск». В таблице ниже будут отображены файлы журнала. В журнале событий хранится максимум 10000 записей. Отображение до 100 записей на каждой из страниц. Для переключения между страницами введите в поле «Страница» номер нужного листа и нажмите на кнопку  .

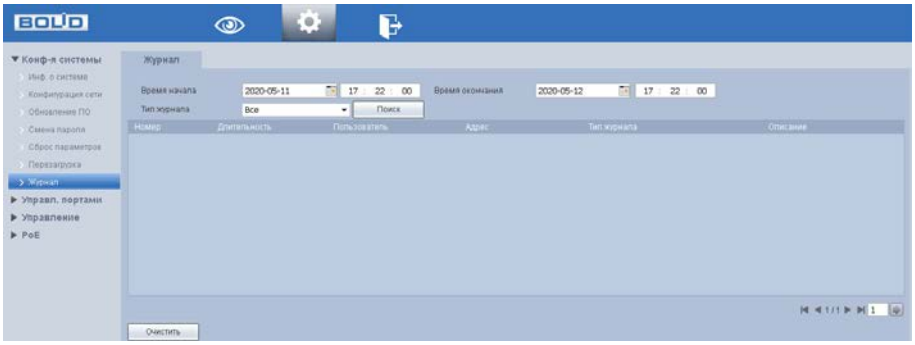

Рисунок 6.9 – Интерфейс просмотра журнала

Функции и значения параметров (Таблица 6.2).

Таблица 6.2 – Параметры просмотра журнала

Параметр	Функция
Время начала	Задание времени начала требуемого журнала.
Время окончания	Задание времени окончания требуемого журнала.
Тип	Тип журнала.
Поиск	Поиск событий журнала.
Удалить все	Удаление всех отображаемых данных журнала.

6.3 Управление портами

6.3.1 Конфигурация портов

На рисунке (Рисунок 6.10) показан интерфейс конфигурации портов коммутатора. Настройка конфигурации порта должна соответствовать практическим требованиям устройства.

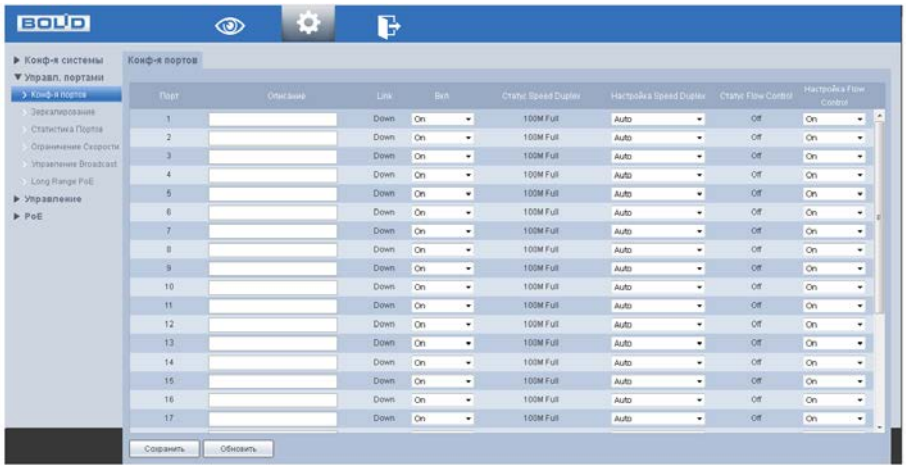

Рисунок 6.10 – Конфигурация портов коммутатора

Таблица 6.3 – Настройка конфигурации портов

Столбец		Описание	
Порт		Номер порта соответствует числу на лицевой панели.	
Описание		Текстовое пользовательское поле для описания порта.	
Вкл.	Служит для включения/выключения порта	On	Переключение порта во включенное состояние.
		Off	Переключение порта в выключенное состояние.

<table>
<tr><th colspan="2">Столбец</th><th colspan="3">Описание</th></tr>
<tr><td rowspan="2">Link</td><td rowspan="2">Отображает статус связи порта</td><td>Up</td><td colspan="2">Порт находится в активном состоянии.</td></tr>
<tr><td>Down</td><td colspan="2">Порт находится в отключенном состоянии.</td></tr>
<tr><td rowspan="9">Настройка Speed Duplex</td><td colspan="4">Отображает текущее состояние скорости порта</td></tr>
<tr><td>Порт</td><td>Скорость</td><td colspan="2">Описание</td></tr>
<tr><td rowspan="6">Ethernet порт</td><td>Авто.</td><td colspan="2">Автоматическая настройка скорости и режима передачи.</td></tr>
<tr><td>10M FULL</td><td colspan="2">Скорость 10Мб/с. Работа в режиме полного дуплекса.</td></tr>
<tr><td>10M HALF</td><td colspan="2">Скорость 10Мб/с. Работа в режиме полудуплекса.</td></tr>
<tr><td>100M HALF</td><td colspan="2">Скорость 100Мб/с. Работа в режиме полудуплекса.</td></tr>
<tr><td>100M FULL</td><td colspan="2">Скорость 100Мб/с. Работа в режиме полного дуплекса.</td></tr>
<tr><td>1000M FULL</td><td colspan="2">Скорость 1000Мб/с. Работа в режиме полного дуплекса.</td></tr>
<tr><td>Оптический порт</td><td>1000-X</td><td colspan="2">Скорость 1000Мб/с. Работа в режиме полного дуплекса.</td></tr>
<tr><td colspan="2">Статус Speed Duplex</td><td colspan="3">Отображает текущее состояние скорости порта.</td></tr>
<tr><td colspan="2">Статус Flow Control</td><td colspan="3">Отображает текущее состояние настройки управления потоком.</td></tr>
</table>

Столбец	Описание	
Настройка Flow Control	Up	Включение функции управления потоком на порте.
	Off	Выключение функции управления потоком на порте.

6.3.2 Зеркалирование

Для мониторинга трафика одного или нескольких портов включите функцию зеркалирования. Принцип работы состоит в дублировании трафика одного из портов на другой порт. Для включения данной функции необходимо:

1. В соответствующем интерфейсе «Зеркалирование» из выпадающего списка «Отслеживание пакетов» выберите: направление пакетов.
   - Отключить. Выбрав данный пункт, функция зеркалирования будет отключена;
   - Egress. Включает функцию отправки копий пакетов передаваемых с порта коммутатора на подключенное в этот порт устройство;
   - Ingress. Включает функцию отправки копий пакетов передаваемых от устройства, подключенного в указанный порт, на порт коммутатора.
2. Выберите из выпадающего списка порт «Порт Dest», куда будут передаваться копии пакетов, и на котором будет осуществляться анализ и мониторинг.
3. Отметьте в таблице порты, с которых хотите получать копии пакетов.

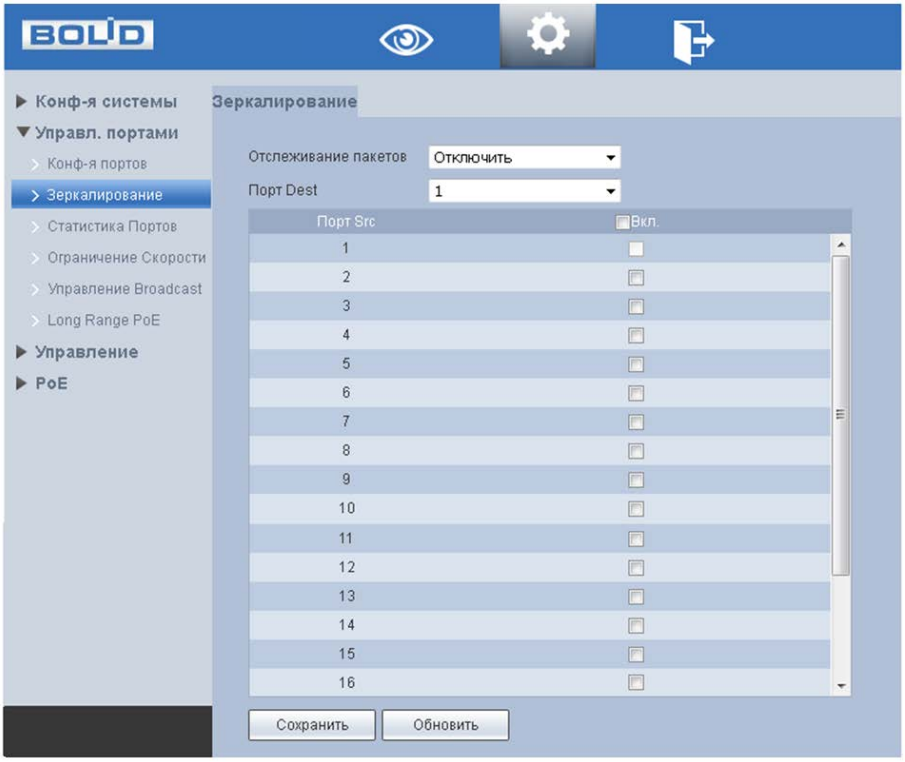

Рисунок 6.11 – Зеркалирование трафика

6.3.3 Статистика портов

Интерфейс статистики портов коммутатора показан на рисунке ниже (Рисунок 6.12).

Для выбора отображаемой статистики выберите в выпадающем меню «Выбор режима счетчика» соответствующий пункт:

- Transmit Packet & Receive Packet: статистика переданных и полученных пакетов;
- Collision Packet & Transmit Packet: статистика пакетов с коллизиями и переданных пакетов;
- Drop Packet & Receive Packet: статистика отброшенных и полученных пакетов;
- CRC Error Packet & Receive Packet: статистика повреждённых пакетов и полученных пакетов.

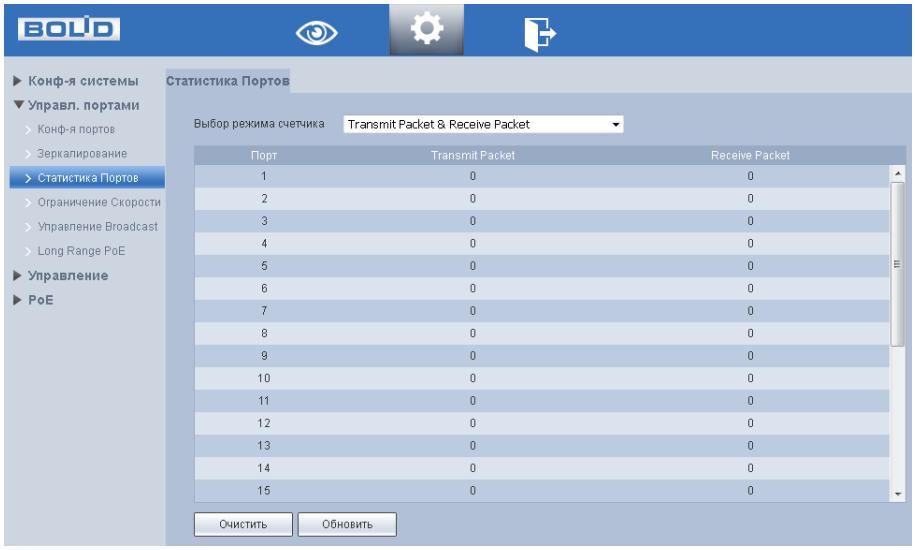

Рисунок 6.12 – Статистика портов

6.3.4 Ограничение скорости

Интерфейс ограничения пропускной способности входящих/исходящих пакетов на порт. Возможно ограничение скорость в пределах от 0 до 63 Мбит/с.

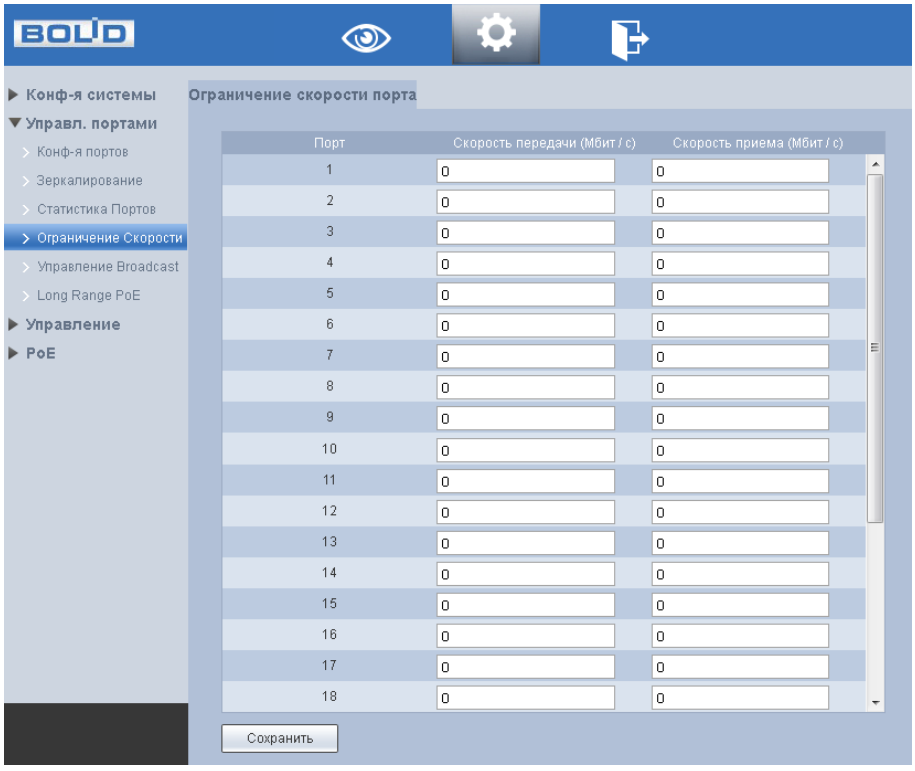

Рисунок 6.13 – Ограничение скорости

6.3.5 Управление broadcast (Широковещательным штормом)

В ПО коммутатора включена функция ограничения широковещательных пакетов. Для настройки отметьте флажком те порты, для которых хотите установить порог числа широковещательных пакетов, разрешенных для входа в каждый порт за определённый промежуток времени. При превышении порога поступающие широковещательные пакеты будут отбрасываться. Указанный промежуток времени зависит от скорости соединения и составляет: при 10 Мбит / с - 5000 мкс, при 100 Мбит / с - 500 мкс, а при 1 Гбит / с - 50 мкс. Для невыделенных портов все широковещательные пакеты будут считаться обычными.

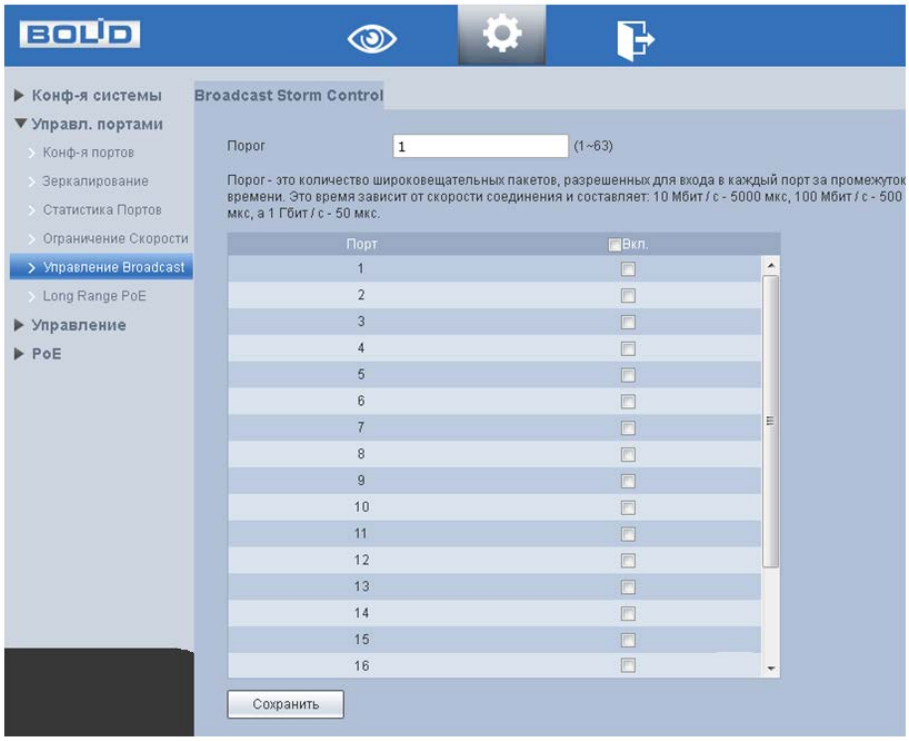

Рисунок 6.14 – Ограничение широковещательных пакетов

6.3.6 Long Distance POE

Функция увеличения максимального расстояния со 100 м до 250 м с PoE питанием. После включения данной функции скорость соединения снижается с 100 Мбит / с до 10 Мбит / с.

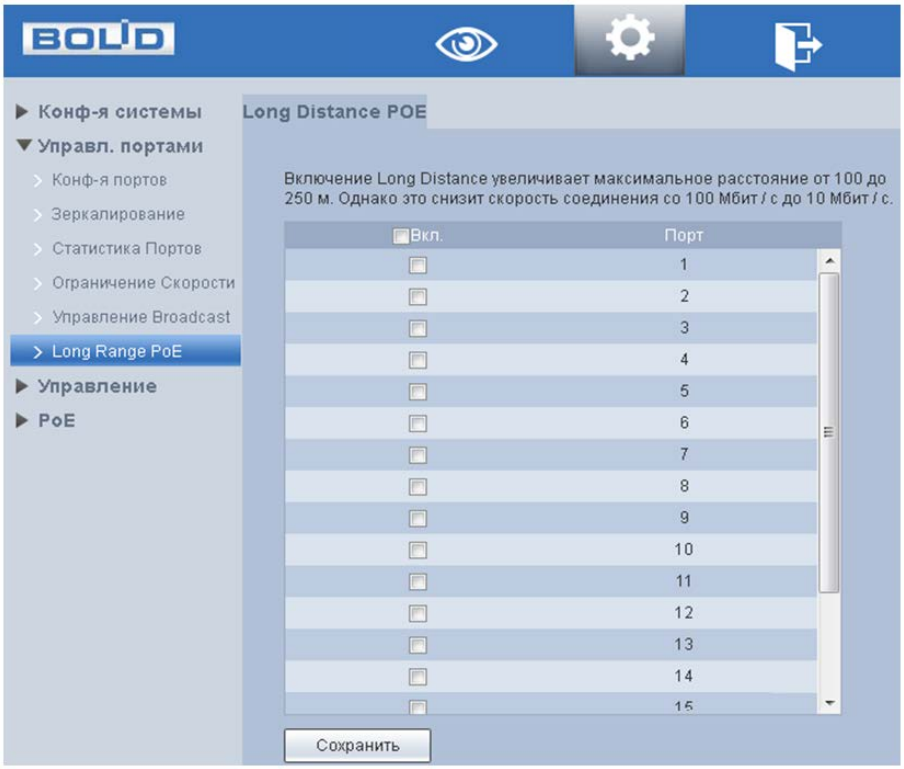

Рисунок 6.15 – Long Distance PoE

6.4 Управление

6.4.1 Spanning Tree

6.4.1.1 Настройки STP Bridge

На рисунке ниже (Рисунок 6.16) изображен интерфейс изменения настроек STP и протокола его работы.

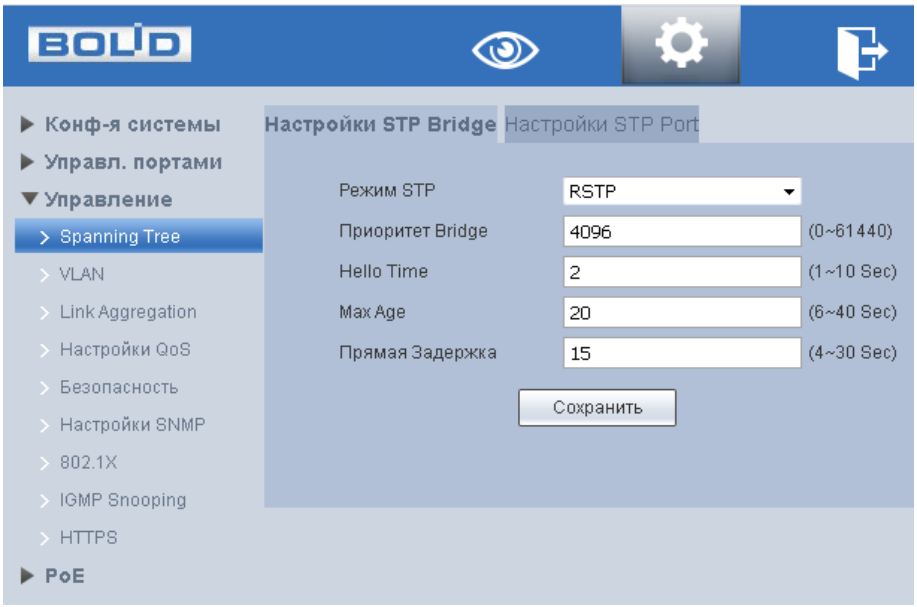

Рисунок 6.16 – Настройка STP

Таблица 6.4 – Параметры настройки STP

Параметр	Функции
Режим STP	Изменение режима работы Spanning Tree. Возможны варианты: —Отключить; —STP; —RSTP.
Приоритет Bridge (Приоритет моста)	Установите приоритет моста STP. Параметр в поле устанавливается в диапазоне от 0 до 61440. Значение должно быть кратно 4096. При наличии двух одинаковых приоритетов, корневым становится устройство с наименьшим MAC - адресом.
Hello Time	Задание интервала между передачей корневым устройством сообщений о конфигурации (BPDU фреймов). Параметр в поле устанавливается в диапазоне от 1 до 10 секунд.
Max Age (Максимальное время)	Установите время, которое устройство может простаивать, не получая конфигурационного сообщения, прежде чем попытается перенастроиться. Параметры времени устанавливаются от 6 до 40 секунд.
Прямая Задержка	Установите максимальное время ожидания перед сменой состояний (от приема до передачи). Состояние меняется от 4 до 30 секунд.

6.4.1.2 Настройки STP Port

Интерфейс позволяет изменять приоритеты портов и RPC. Параметры меняются после изменения режима STP/RSTP в меню «Настройки STP Bridge», система автоматически присваивает приоритеты портов и RPC.

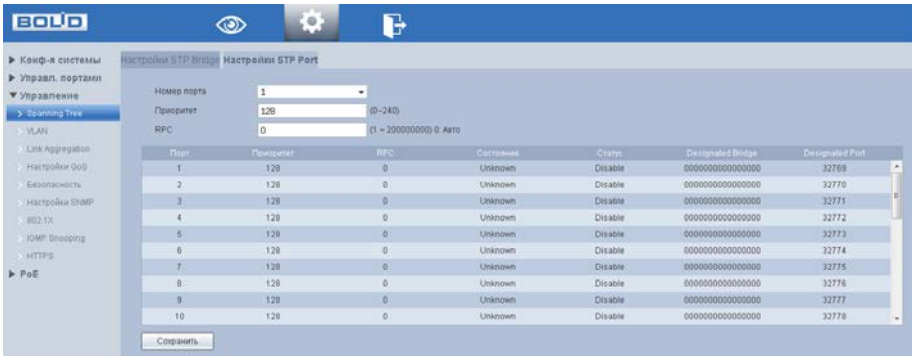

Рисунок 6.17 – Настройка STP

Таблица 6.5 – Параметры настройки STP

Параметр	Функции
Номер порта	Номер порта. Соответствует числу на лицевой панели.
Приоритет	Установите приоритет порта, варьирующийся от 0 до 240 и кратным 16.
RPC	(Root Path Cost) Этот параметр используется STP для определения наилучшего пути между устройствами. Следовательно, более низкие значения должны соответствовать портам, которые взаимодействуют с большим потоком информации, а более высокие значения должны соответствовать меньшим потокам и более удаленным от ядра системы. Параметр устанавливается от 0 до 200000000.

6.4.2 VLAN

6.4.2.1 Список VLAN

Во вкладке «Список VLAN» можно видеть сводную таблицу со всеми созданными в коммутаторе VLAN.

Таблица 6.6 – Данные списка VLAN

Столбец	Описание
VLAN ID	Уникальный идентификатор VLAN соответствует тегу VLAN.
Описание	Текстовая пользовательская метка для удобства настройки.
Член VLAN	Порты, через которые разрешено прохождение трафика с соответствующим тегом VLAN. Настраивается во второй вкладке «Конфигурирование VLAN-порта».

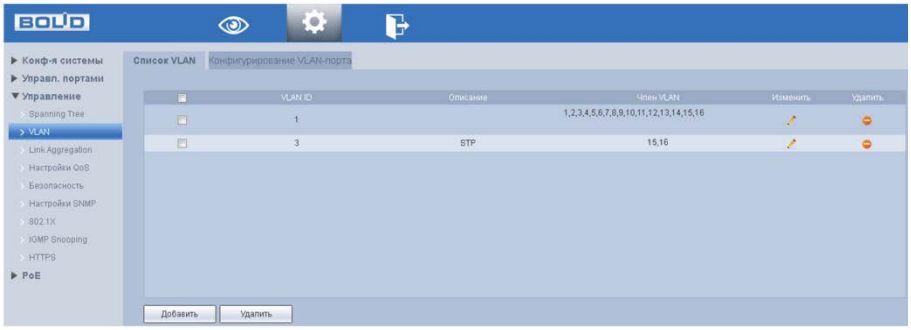

Рисунок 6.18 – Создание VLAN

6.4.2.2 Конфигурирование VLAN-порта

На рисунке ниже (Рисунок 6.20) изображена вкладка «Конфигурирование VLAN-порта».

Таблица 6.7 – Конфигурирование VLAN-порта

Столбец	Описание
Тип порта	Позволяет выбрать режим работы порта. — Access. Данный режим переключает порт в режим со снятием тега VLAN. Наиболее правильно использовать для портов, к которым будут подключаться оконечные устройства; — Trunk. В этом режиме наиболее часто настраиваются порты для подключения к другим коммутаторам. Проходящий через такой порт трафик проверяется на наличие разрешённых в поле «Разрешённые VLAN». Становится активным выбор «Egress tagging»; — Hybrid. В отличие от Trunk для исходящего трафика, hybrid режим позволяет снимать все метки VLAN или наоборот обязательно метить тегом «порт VLAN». В остальном принцип работы совпадает.
Порт VLAN	Задаётся принадлежность порта к конкретному VLAN. В случае работы порта в режиме Access, поступающий на порт трафик помечается тегом, записанным в данное поле.

Столбец	Описание
Egress tagging	При установке «Тип порта» в «Access» данное поле не доступно. Тег VLAN принудительно снимается. — Untag port VLAN: Будет снята метка с пакетов, относящихся к VLAN с тегом, указанным в поле «порт VLAN». Остальные пакеты будут переданы без изменений; — Tag ALL: Все пакеты с метками VLAN из списка разрешённых будут передаваться без изменений; — Tagged only: Все VLAN передаются как есть; — Untagged only: Используется в особых случаях. Все метки со всех VLAN снимаются.
Разрешенные VLAN	Перечисление всех разрешенных к прохождению через этот порт VLAN. Остальные VLAN отбрасываются.

Для конфигурирования нового VLAN необходимо:

- Во вкладке «Список VLAN» нажать «Добавить». Появится окошко создания нового VLAN. Заполнив поля «VLAN ID» и «Описание», нажмите «Сохранить».

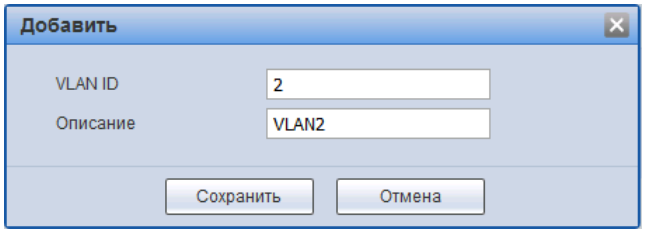

Рисунок 6.19 – Добавить новый VLAN

- Во вкладке «Конфигурирование VLAN-порта» для нужных портов в поле «Разрешенные VLAN» добавьте указанный в шаге 1 «VLAN ID», настройте порт в соответствии с вашими потребностями.

Пример:

Нужно подключить камеру в порт 1. VLAN видеонаблюдения - 2. Порт, куда должны передаваться данные – 18 и этим портом коммутатор подключен к другому коммутатору, поддерживающему 802.1Q,

Для указанной строки с числом 1 в столбце «Порт» изменить:

- Выбрать «Access» в столбце «Тип порта»;
- В поле «Порт VLAN» вписать 2;
- В поле «Разрешенные VLAN» вписать 2.

В строку, соответствующую 18-му порту вписать:

- Выбрать «Trunk» в столбце «Тип порта» (Наиболее вероятно появление и других VLAN на коммутаторе. В этом случае, если все данные будут проходить через 18-й порт, вариант «Trunk» является оптимальным выбором);
- Поле «Порт VLAN» менять не требуется (в поле вписано значение 1);
- В поле «Egress tagging» выбрать «Untag port VLAN» (В этом случае все разрешённые VLAN будут проходить со своими метками, VLAN с ID 1 будет оставаться без метки);
- В поле «Разрешенные VLAN» вписать 2 или дописать через запятую к списку уже имеющихся в поле значений;

Нажать кнопку «Сохранить».

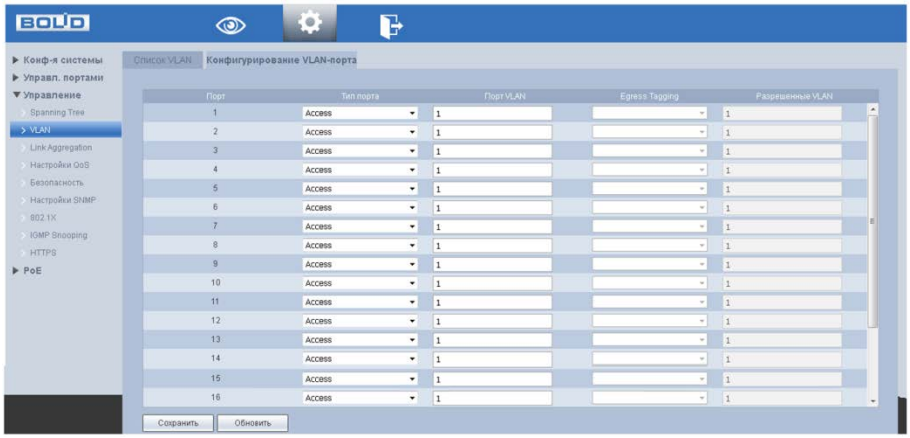

Рисунок 6.20 – Конфигурирование VLAN-порта

6.4.3 Link Aggregation

Суть агрегации каналов заключается в формировании из нескольких физических портов коммутатора одного логического порта, причем несколько каналов, принадлежащих к одной и той же группе агрегации, можно рассматривать как логическое соединение с большей пропускной способностью.

Агрегирование каналов может реализовать разделение ответственности за коммуникационный поток между каждым портом-членом группы агрегирования, что должно увеличить пропускную способность. Между тем, взаимное динамическое резервное копирование может быть реализовано между каждым портом-членом в одной и той же группе агрегации, что должно повысить надежность соединения.

Для этого создаётся определенная конфигурация для портов-членов, которые принадлежат к одной и той же группе агрегации. Эти конфигурации включают настройки STP, QoS, VLAN, свойства портов, изучение MAC-адресов, зеркалирование, фильтрацию 802.1 x и Mac и т. д.

ВНИМАНИЕ!
Не рекомендуется реализовывать конфигурацию портов, которые используются для агрегации каналов, с расширенными функциями.
Агрегация каналов может быть разделена на статическую агрегацию и LACP, как правило, противоположными конечными устройствами агрегации каналов коммутатора являются коммутатор и сетевые карты сервера

6.4.3.1 Статическая агрегация

Статический режим агрегации позволяет ему вручную добавить несколько портов-членов в группу агрегации, все порты находятся в состоянии прямой передачи и совместно используют перегруженный поток. Необходимо создать группу агрегации и добавить порты-члены через ручное конфигурирование без участия протокола LACP (link Aggregation Control Protocol).

Режим «Балансировки Нагрузки».

Существует три типа алгоритма балансировки нагрузки для порта, которые показаны ниже.

Таблица 6.8 – Типы алгоритма балансировки нагрузки

Режим балансировки	Описание
MAC источника	Балансировка нагрузка, осуществляемая на основе поля MAC-адреса источника.
MAC назначения	Балансировка нагрузка, осуществляемая на основе поля MAC-адреса назначения.
MAC Src & Dst	Балансировка нагрузка, осуществляемая на основе поля MAC-адреса источника и назначения.

* Группа Агрегирования

Это сборка группы портов Ethernet. Поддерживаемое число групп агрегации по умолчанию равно трем, которое не может быть изменено. Статус по умолчанию для всех групп агрегации-disable, в группах не активировано ни одного порта.

* Входящие в группу порты

В коммутаторе созданы все группы агрегации по умолчанию, члены порта имеют значение null. Сначала необходимо включить группу агрегирования, если вы хотите настроить порты-члены для группы агрегирования. Затем щелкните группу агрегирования, в которой находится порт, чтобы включить функцию агрегирования.

6.4.3.2 LACP

LACP (Link Aggregation Control Protocol) используется для реализации динамической агрегации основанной на стандарте IEEE 802.3 ad. Обе стороны агрегируемых устройств объединяются вместе по согласованным каналам связи и получают и отправляют данные через пакет LACPDU, взаимодействующий с информацией об агрегировании. Протокол может автоматически добавлять и удалять порты в группе агрегации. Он обладает высокой гибкостью и обеспечивает возможность балансировки нагрузки.

После включения функции LACP порт сообщит противоположной стороне системный приоритет, MAC, номер порта, приоритета и ключ управления (это определяется физическими свойствами, информацией о протоколе верхнего уровня и ключом управления порта).

Сторона с высоким приоритетом устройства будет управлять агрегированием. Приоритет устройства определяется системным приоритетом и MAC-адресом, устройство с меньшим значением системного приоритета имеет более высокий приоритет. Устройство с меньшим значением системного MAC имеет более высокий приоритет, когда значение системного приоритета одинаково. Сторона с более высоким приоритетом устройства выберет порт агрегации в соответствии с приоритетом порта, номером порта и ключом операции. Порты с таким же ключом операции могут быть добавлены в ту же группу агрегации. Порт с меньшим значением приоритета порта будет выбран по приоритету в той же группе конвергенции. Порт с меньшим номером будет выбран, когда приоритет порта будет одинаковым. Выбранные порты будут логически объединены вместе для приема и отправки данных после того, как обе стороны взаимодействуют с информацией об агрегации.

Настройки протокола LACP в основном включают в себя функцию включения порта LACP, значение ключа, активность (активный/пассивный режим) и конфигурацию таймаута.

Порты, которые только включают протокол LACP, могут реализовать согласование LACP, и тогда он может сформировать агрегированный канал. Секретный ключ является основой взаимодействия, и порты с таким же секретным ключом могут вести передачу для формирования канала агрегации. Режим передачи включает в себя «активный/пассивный» режимы.

Устройство будет активно запускать канал агрегации, когда оно находится «активном» состоянии; устройство будет пассивно принимать данные об агрегации, запущенной другими устройствами, когда оно в состоянии «пассивный».

В системе должны быть, по крайней мере, один или две стороны, которые установлены в качестве «активного», чтобы реализовать успешное соединение, когда два устройства объединены между собой.

- Ключ: для членов одной группы агрегации нужно настроить один и тот же ключ операции, он должен быть в диапазоне от 1 до 65535;
- Активность: может выбрать активный и пассивный (по умолчанию). Одно устройство, которое участвует в динамической агрегации, должно быть в активном режиме, а другие должны быть настроены на пассивный режим;
- Тайм-аут: может быть установлено в короткое или долгое (по умолчанию) время ожидания.

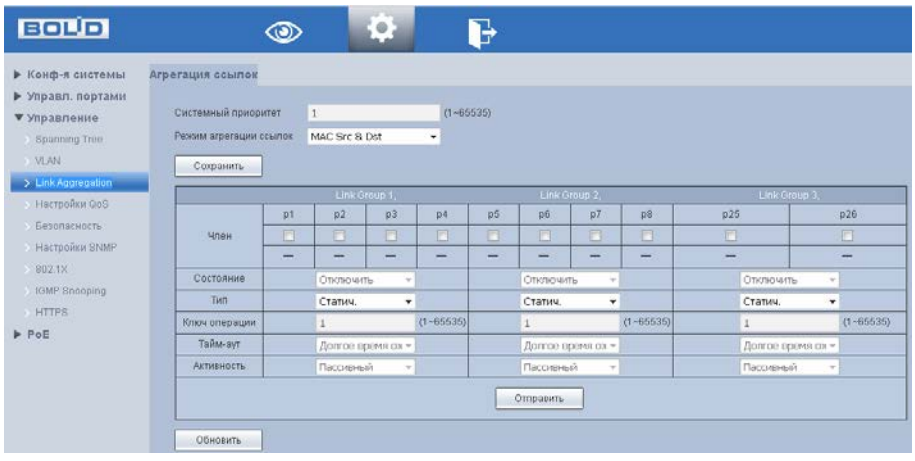

Рисунок 6.21 – Интерфейс настройки агрегации ссылок

6.4.4 Настройки QoS

6.4.4.1 Приоритетный режим

Доступны три режима приоритетности:

— First-In-First-Out (приоритет в порядке очередности): пакеты в очереди обслуживаются в порядке их поступления;

— All-High-Before-Low (приоритет в порядке двух очередей): поступающие пакеты помещаются в две очереди «Высокоприоритетные» и «Низкоприоритетные». При этом пакеты из второй очереди не начнут передаваться, пока передаются пакеты из первой очереди;

— Weight-Round-Robin (приоритет распределяется циклически): пакеты разбиваются на четыре очереди. Трафик передается в соответствии с номером пакета в каждой очереди.

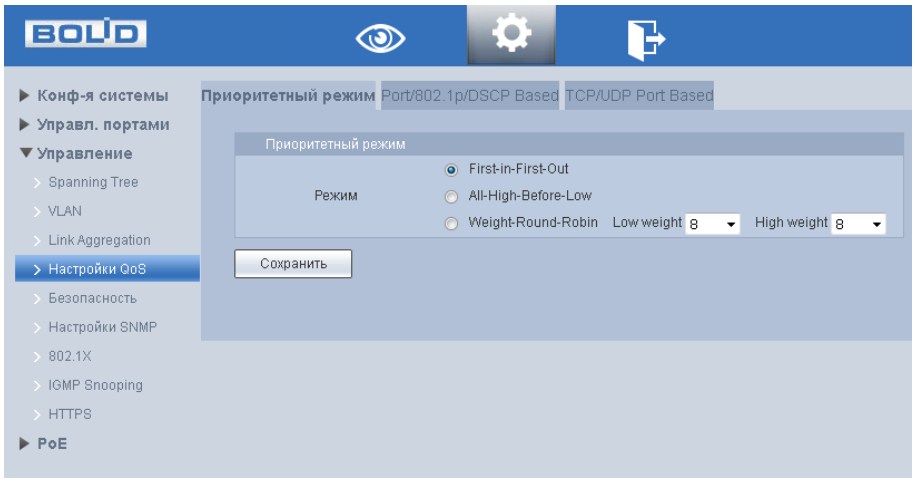

Рисунок 6.22 – Приоритетный режим

6.4.4.2 Port/802.1p/DSCP Based

В данном окне можно включить приоритет по порту, по флагу VLAN или по маркеру пакета IP/DS Enable High Priority (обозначение наибольшего приоритета): галочка в соответствующем окне означает, что данный параметр наиболее приоритетен.

— Port Base (приоритетность по порту): Выбранный порт становится высокоприоритетным. Пакеты, полученные на высокоприоритетном порту, попадают в приоритетную очередь;

— При включении QoS на основе 802.1p, приоритизация трафика начинается на основании значения приоритета, указанного в заголовке L2 поля TCI, полученного извне. Коммутатор, исходя из флага приоритета, разделяет входящие пакеты. Значения флага 4~7 – высокий приоритет, 0~3 – низкий приоритет;

— DSCP. Коммутатор, исходя из маркера IP TOS (Differentiated Services) пакетов входящего трафика Ipv4 DS и Ipv6 TC задает приоритет:

  — высокий – для значений 10,18,26,34,46,48,56;

  — низкий – для всех остальных.

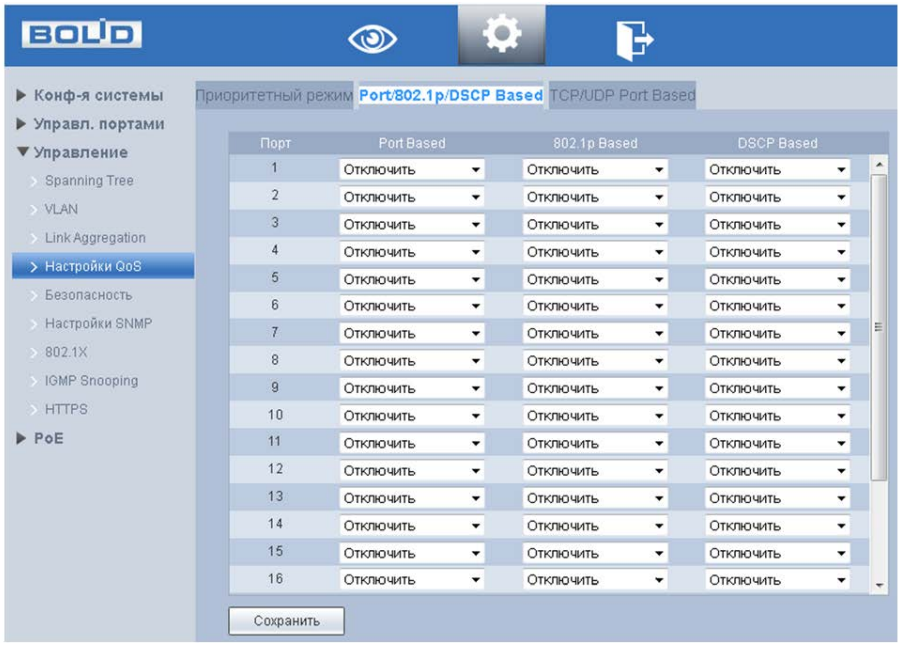

Рисунок 6.23 – Интерфейс настройки Port/802.1p/DSCP Based

6.4.4.3 TCP/UDP Port Based

TCP и UDP используют 16-разрядный порт для распознавания приложений. Серверы обычно используют стандартные порты. Например, TCP-порт FTP-сервера – 21. TCP порт Telnet – 23. UDP. порт TFTP-сервера – 69. Зарезервированный диапазон TCP/IP 1-1023 порт.

На рисунке (Рисунок 6.26) виден список стандартных портов, которые может обрабатывать устройство, такие как FTP, SSH, TELNET, SMTP и DNS. Возможные значения: высокий приоритет, низкий приоритет, FIFO или отбрасывать. Значение по умолчанию - FIFO.

Пример конфигурации.

1 Сетевое подключение

— К коммутатору подключены некие устройства в порт 1, 2 и FTP сервер через 16 порт;

— Настроена функция QoS, Порт 2 имеет высокий приоритет, порт 1 нет, и устройству в порте 2 заблокирован для доступа к FTP серверу.

2 Настройки:

a. Установите режим работы приоритета в состояние «All-High-Before-Low»;

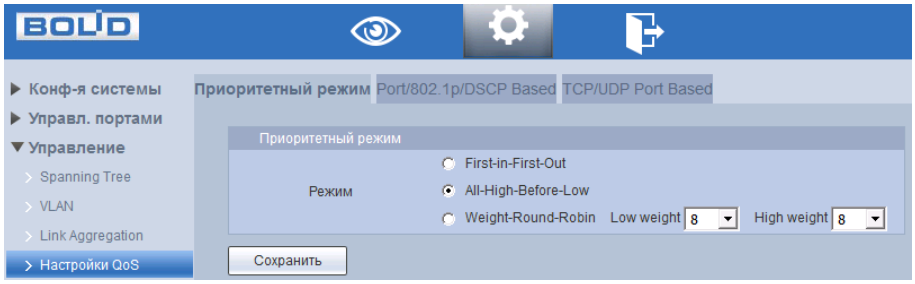

Рисунок 6.24 – Приоритетный режим

b. Для порта 2 установите высокий приоритет;

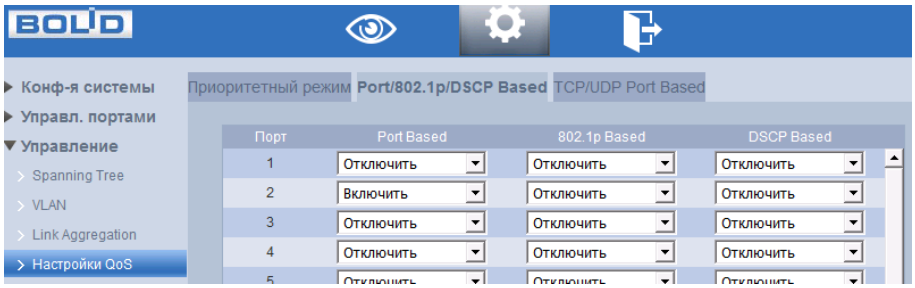

Рисунок 6.25 – Приоритетный режим

c. Задайте «Discard» для пакетов, относящихся к FTP серверу.

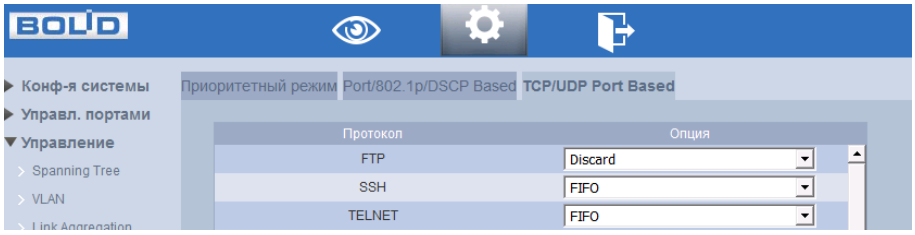

Рисунок 6.26 – Задайте «Discard»

6.4.5 Безопасность

6.4.5.1 Таблица MAC адресов

Коммутатор, для передачи пакета, выполняет поиск в листе MAC-адресов в соответствии с MAC-адресом назначения. Если адрес найден в таблице, используется соответствующий порт для пересылки пакета. Если нет, устройство использует широковещательный режим для пересылки через соответствующий VLAN (за исключением порта, с которого этот пакет поступил). На следующем рисунке представлена такая таблица адресов.

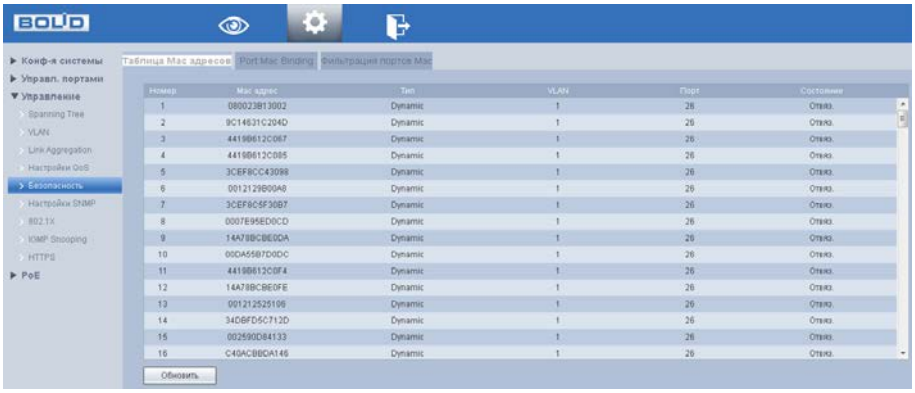

Рисунок 6.27 – MAC информация об адресах

6.4.5.2 Port Mac Binding/ Привязка MAC-адреса к порту

На рисунке ниже (Рисунок 6.28) изображён интерфейс привязки MAC-адресов. Нажмите на выбранный действующий порт для настройки привязки к нему MAC-адресов. В результате только трафик с этим MAC-адресом будет допущен к передаче на этом порте.

Данной функцией можно пользоваться, чтобы через данный порт могла осуществляться передача данных только конкретного устройства, например, камеры.

Рисунок 6.28 – Привязка MAC-адреса

6.4.5.3 Фильтрация MAC-адресов

Функция используется для ограничения поступающих пакетов при помощи настройки белого списка MAC адресов. Для настройки функции:

1 Нажмите «Добавить» и введите в появившемся поле белый MAC адрес;
2 Сохраните настройку;
3 Для просмотра информации, нажмите на порт устройства и в «Mac Filtering Port» просмотри входящие пакеты.

Рисунок 6.29 – Фильтрация портов

6.4.6 SNMP

Коммутатором поддерживаются SNMPv1, SNMPv2 и SNMPv3.

- SNMPv1 для авторизации использует community имя аналогично паролю. Если community отличаются, устройства игнорируют такие пакеты;
- SNMPv2 Отличий в методе авторизации нет. Расширен список возможных операций, типов данных и кодов ошибок;
- SNMPv3 авторизация на основе пользовательской модели. Возможна настройка различных параметров авторизации, в том числе шифрования. Этот протокол SNMP является наиболее безопасным и рекомендуется для использования в условиях, требующих повышенной безопасности.

ВНИМАНИЕ!
Протоколы различных версий не совместимы между собой. Отличие протоколов, как и неверные настройки авторизации, приведут к игнорированию обмена с обеих сторон.

6.4.6.1 Настройки SNMP

На рисунке (Рисунок 6.30) изображен интерфейс настроек SNMP и пример такой настройки, являющийся в большинстве устройств устанавливаемым по умолчанию. Для SNMP протоколов версий 1 и 2 интерфейс настроек не отличается.

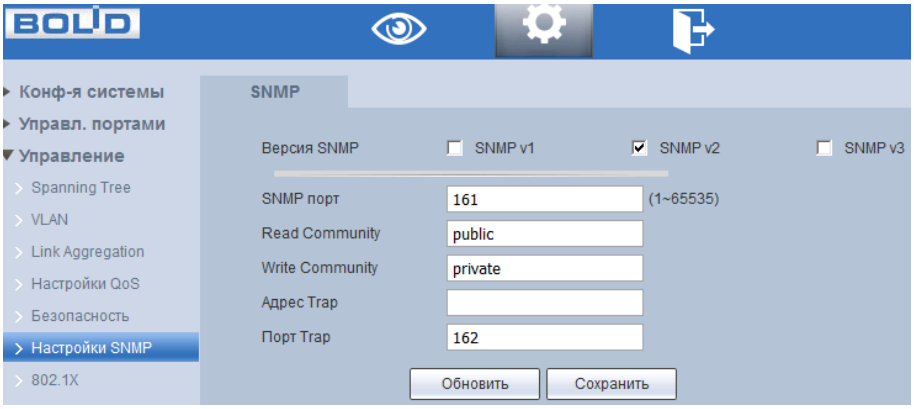

Рисунок 6.30 – Настройки SNMP

На рисунке (Рисунок 6.31) изображен интерфейс настроек SNMP версии 3. Для безопасности пример таких настроек не приведён.

В следующей таблице подробно описаны поля, относящиеся к этим настройкам:

Таблица 6.9 – Поля настроек

Название	Описание
Пользователь (чтение)	Поле, используемое для получения параметров с устройства.
Пользователь (запись)	Поле, используемое для изменения параметров устройства.
Адрес trap сервера	В этом поле указывается адрес, на который самим устройством будут посылаться trap пакеты.

Название	Описание
Имя пользователя только для чтения	Задание имени пользователя.
Тип аутентификации	Устройством используется режим SNMPv3 «авторизация с шифрованием». Здесь можно задать метод шифрования ключа авторизации. Можно выбрать между MD5 или SHA.
Пароль для аутентификации	Поле для задания пароля авторизации.
Тип шифрования	Поле выбора метода шифрования передаваемых данных. Устройством поддерживается только режим «CBC-DES».
Пароль шифрования	Поле для задания ключа шифрования передаваемых данных.

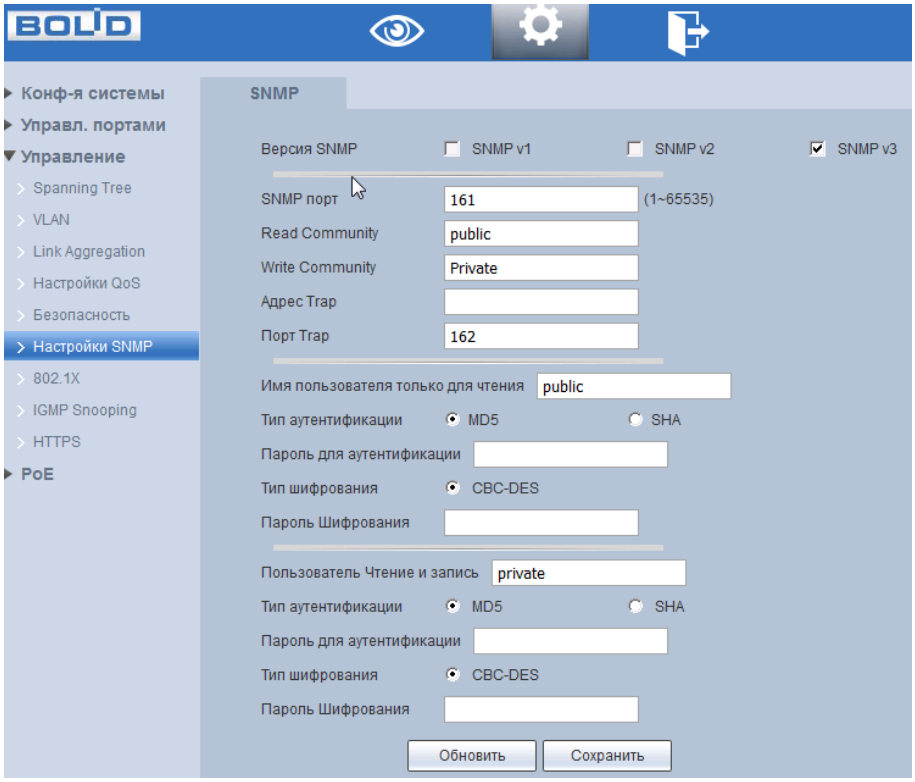

Рисунок 6.31 – Настройки SNMPv3

6.4.7 802.1X

IEEE 802.1x – это стандарт аутентификации устройств, подключенных к коммутатору. Это тип протокола управления доступом к сети на основе порта, поэтому для работы этого протокола на порту коммутатора должна быть сконфигурирована функция аутентификации. Что касается пользовательского устройства, которое подключается к настроенному на авторизацию по 802.1X порту, оно должно поддерживать данный протокол аутентификации.

6.4.7.1 Структура сети 802.1x

Простейшая схема 802.1x включает в себя три части: клиент, агент (коммутатор), настроенный на работу с конкретным сервером аутентификации и сервер аутентификации.

Рисунок 6.32 – Схема

— Клиент (Суппликант) – это пользовательское терминальное устройство, требующее доступа к локальной сети, которое аутентифицируется в локальной сети. Клиент должен будет установить программное обеспечение, поддерживающее 802.1x идентификацию;
— Агент (Аутентификатор) – это сетевое устройство, которое управляет клиентским доступом в сеть LAN. Оно расположено между клиентами и сервером аутентификации, который предоставляет пользователям порт доступа к локальной сети (физический порт или логический порт) и реализует аутентификацию на подключенном клиенте посредством взаимодействия с сервером;

— Сервер аутентификации используется для реализации аутентификации, авторизации и биллинга. Для 802.1X это сервер RADIUS. Сервер проверки подлинности проверяет законность клиента в соответствии с аутентификационной информацией клиента, отправленной со стороны устройства, и информирует устройство о результатах проверки. По параметрам агента принимается решение, позволить ли клиенту доступ или нет. Роль сервера аутентификации в небольших сетевых средах может выполнять устройство, которое реализует локальную аутентификацию, авторизацию и биллинг клиентов.

6.4.7.2 802.1x Аутентификация портов

Порты доступа LAN, предоставляемые устройством клиентам, можно разделить на два типа «Контролируемые» и «Неконтролируемые» порты. Любой кадр, поступивший в порт, может быть отправлен как на контролируемый порт, так и неконтролируемый порт.

— Неконтролируемый порт всегда находится в состоянии двунаправленного соединения, которое используется в основном для передачи пакетов аутентификации. Это необходимо, чтобы клиент всегда мог обмениваться пакетами идентификации;
— Контролируемый порт находится:
  — В состоянии двунаправленного соединения после успешной авторизации;
  — Запрета принимать любые пакеты от клиента в состоянии несанкционированного доступа.

6.4.7.3 Режим запуска аутентификации 802.1x

Процесс аутентификации 802.1x инициализируется клиентом, но также может запускаться и коммутатором.

1. Режим активации триггера клиентом:
   — Триггер многоадресной рассылки: клиент отправляет на устройство пакет запроса аутентификации, для инициации процесса аутентификации. Адрес назначения пакета является MAC-адресом многоадресной рассылки 01:80:C2:00:00:03;

— Триггер широковещательной рассылки: клиент отправляет на устройство пакет запроса аутентификации для инициации процесса аутентификации, адрес назначения пакета - широковещательный MAC-адрес адрес. Этот режим позволяет решить проблему, связанную с тем, что устройство не может получить запрос от клиента на аутентификацию, поскольку некоторые устройства не поддерживают многоадресные пакеты в сети.

2. Режим активации триггера устройством:

Режим активации триггера устройством используется для совместимости с клиентами, которые не могут самостоятельно отправлять пакет запроса аутентификации. Существует два типа активации триггера аутентификации устройством:

— Триггер многоадресной рассылки: Устройство активно отправляет пакет запроса аутентификации клиенту с регулярным интервалом (по умолчанию - 30 секунд);

— Одноадресный триггер: когда коммутатор получает неизвестный пакет от MAC-адреса источника, устройство будет отправлять пакет запроса аутентификации на MAC-адрес источника передачи для запуска процесса идентификации. Процесс повторится, если за указанное время от клиента не будет получен ответ.

6.4.7.4 Управление авторизацией порта (NSA)

Это меню позволяет управлять состоянием аутентификации порта.

Поддерживается три следующих авторизованных состояния:

— Принудительно авторизован: это означает, что порт всегда находится в авторизованном состоянии, что позволяет клиенту, подключенному в соответствующий порт, получить доступ к сети без прохождения процесса аутентификации;

— Принудительно не авторизован: означает, что порт всегда находится в неавторизованном состоянии. Устройство не будет предоставлять службу проверки подлинности для клиента и, соответственно, доступ к сети;

— Авторизация порта на основе 802.1x: означает, что начальное состояние порта является неавторизованным. Это не позволяет получить доступ в сеть; Порт будет переключен в авторизованное состояние, если клиент пройдёт проверку подлинности. После этого сможет обмениваться данными в сети.

Пример конфигурации:

— Схема сети:

Подсеть клиента - 192.168.1.1/24, IP-адрес сервера аутентификации в этой сети - 192.168.1.100.

Требуется аутентификация сервером аутентификации при обращении ко всем портам устройства.

— Настройка:

1 Переключите все порты в состояние аутентификации на основе 802.1x как показано на рисунке ниже (Рисунок 6.35).
2 Настройте адрес сервера аутентификации, как показано на рисунке (см. Рисунок 6.34).

6.4.7.5 Настройки NSA

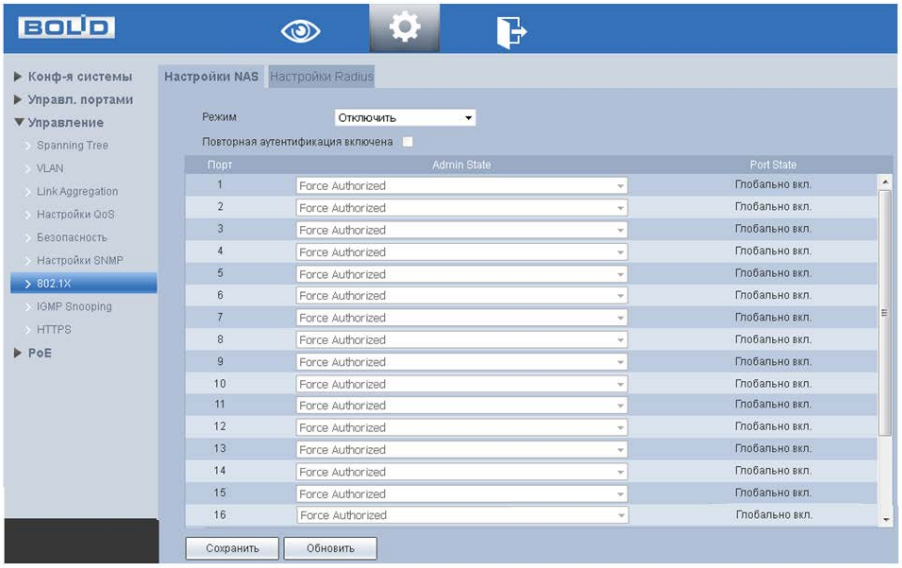

Рисунок 6.33 – Настройки NSA

6.4.7.6 Настройки Radius

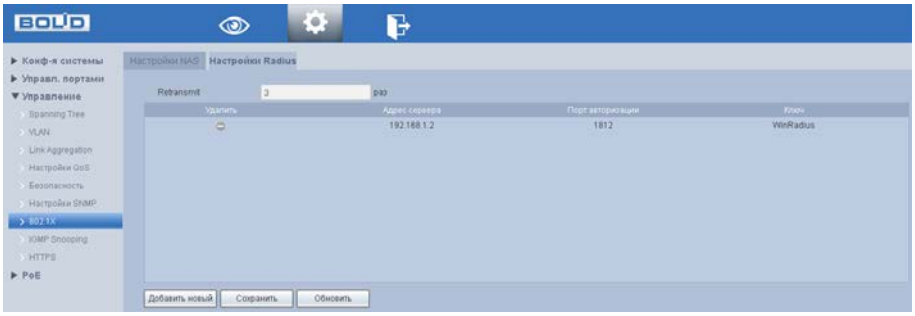

Рисунок 6.34 – Настройки Radius

6.4.8 IGMP Snooping

Данный протокол рекомендуется использовать в случае, если требуется одновременный доступ к видеопотоку из нескольких точек. Как то:

- Использование нескольких несвязанных дублирующих серверов видеонаблюдения;
- Организация видеонаблюдения без использования центрального сервера с одновременным доступом к камерам из множества мест.

Т.е. любой сценарий, требующий множественного повторения одного (нескольких) видеопотока для нескольких устройств в рамках одной локальной сети.

Настройка процесса отслеживания сетевого трафика IGMP, позволяющий сетевым устройствам второго уровня (коммутаторам) отслеживать обмен IGMP пакетами между потребителями и поставщиками (маршрутизаторами) многоадресного (multicast) IP-трафика, формально происходящий на более высоком (сетевом) уровне.

После включения IGMP snooping, коммутатор начинает анализировать все IGMP-пакеты между подключенными к нему компьютерами - потребителями и маршрутизаторами - поставщиками multicast трафика. Обнаружив IGMP-запрос потребителя на подключение к multicast группе, коммутатор включает порт, к которому тот подключён, в список её членов (для ретрансляции группового трафика). И наоборот: услышав запрос «IGMP Leave» (покинуть), удаляет соответствующий порт из списка группы.

Multicast, являясь протоколом 3-го уровня, становится полностью неуправляемым при отключенной функции IGMP snooping. Её включение обязательно при наличии каких-либо многоадресных рассылок любого типа.

На рисунке (Рисунок 6.35) представлен интерфейс настроек в состоянии по умолчанию. При использовании Multicast рассылки, возможно, включить поддержку «Fast leave», которая позволяет коммутатору быстрее исключать порт из списка участников соответствующей группы. Для целей видеонаблюдения её включение не обязательно.

Рисунок 6.35 – Интерфейс IGMP Snooping

6.4.9 HTTPS

Меню «HTTPS» поддерживает просмотр и управление параметрами повышения безопасности сетевой работы с использованием сетевых сертификатов.

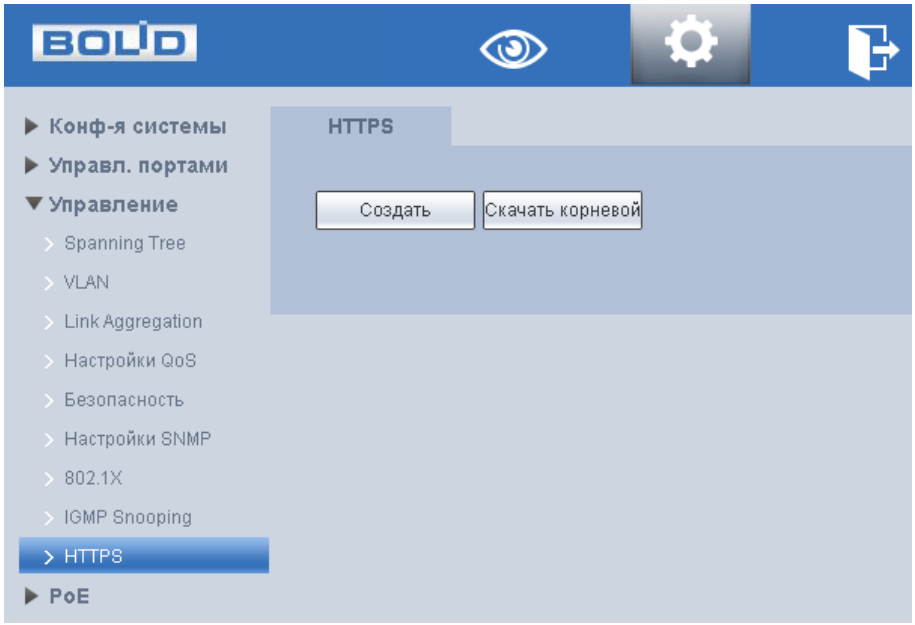

Рисунок 6.36 – Подпункт меню «HTTPS»

Чтобы перейти на работу по https протоколу, администратор должен получить и установить в систему сертификат открытого ключа для этого веб-сервера. Сертификат открытого ключа подтверждает принадлежность данного открытого ключа владельцу. Сертификат открытого ключа и сам открытый ключ посылаются клиенту при установлении соединения; закрытый ключ используется для расшифровки сообщений от клиента.

В данном меню можно создать новый сертификат и после заполнения соответствующих полей скачать сгенерированный сертификат.

6.5 PoE

6.5.1 Настройки PoE

Настройка предоставляет параметры включения/выключения питания PoE для каждого отдельного порта. А также общую доступную для использования мощность и пороговое значение перегрузки для всех портов. После настройки и сохранения конфигурации на панели будет отображаться состояние порта.

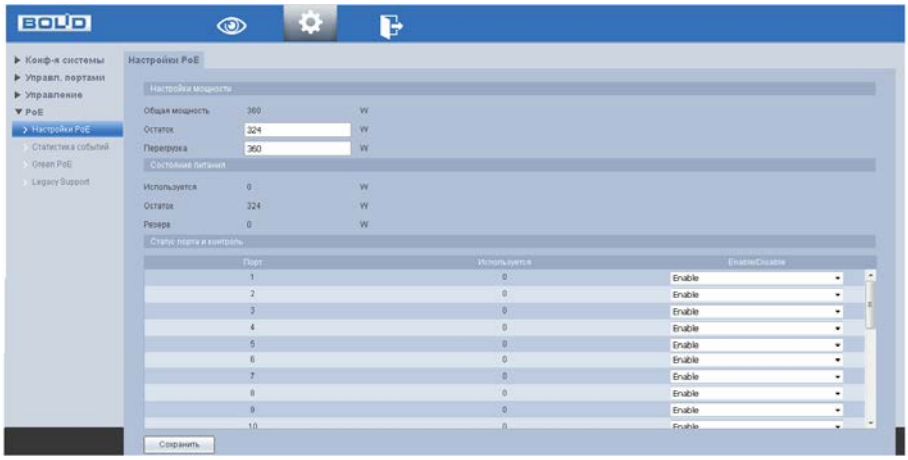

Рисунок 6.37 – Питания порта по PoE

6.5.2 Статистика событий PoE

Интерфейс статистики событий для каждого порта PoE. Включает в себя информацию о:

— Превышении порогового значения перегрузки конкретного порта;

— Коротких замыканиях;

— Отключениях подачи питания на устройство во время его работы;

— Коротких замыканиях при запуске подачи питания на устройство;

— Срабатываниях датчика тепловой защиты.

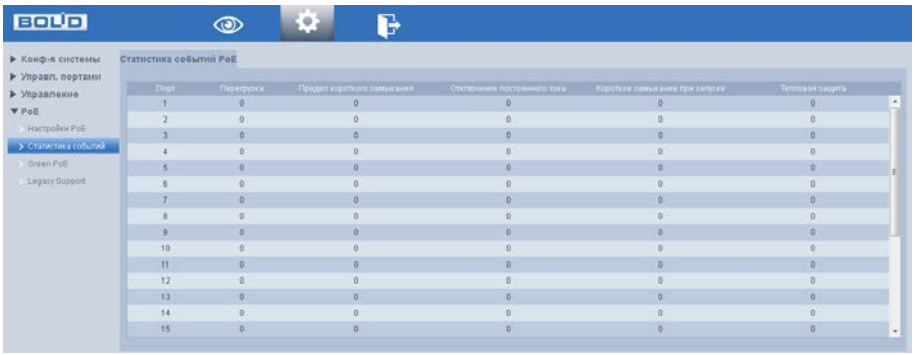

Рисунок 6.38 – Статистика событий PoE

6.5.3 Green PoE

В данном интерфейсе можно настроить период времени, в которое на устройства будет подаваться питание PoE. При выходе за рамки этого периода, устройство отключит подачу питания с отмеченных в этом меню портов в целях экономии энергии.

Данный функционал можно также использовать в целях перезагрузки с задержкой включения.

Рисунок 6.39 – Параметры энергосбережения PoE

6.5.4 Legacy support (Поддержка устаревших устройств)

После включения функции, отмеченные порты будут обеспечивать электропитание принудительно, независимо от того, соответствует ли подключенное устройство стандарту передачи питания или нет.

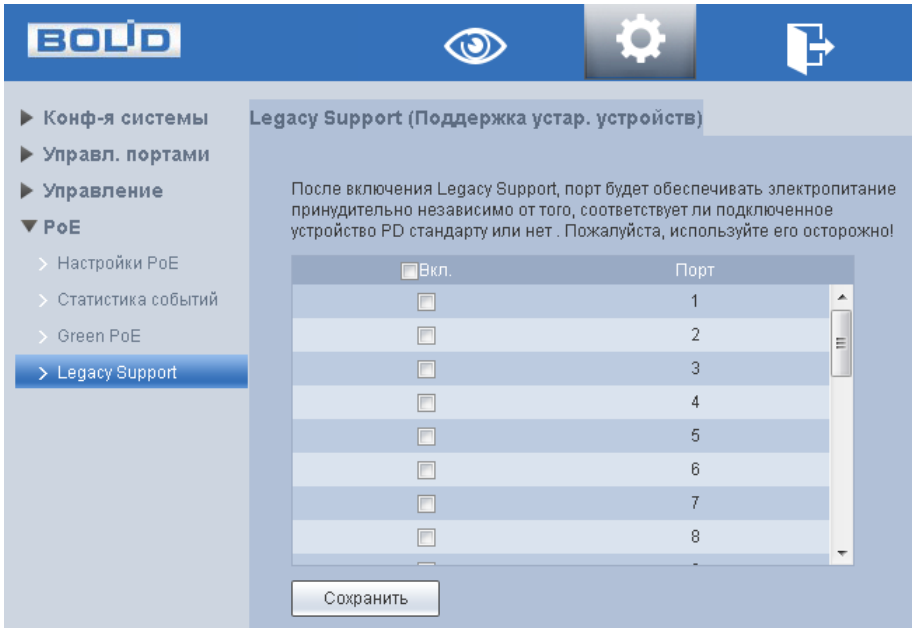

Рисунок 6.40 – Поддержка устаревших устройств

7 РАБОТА С УТИЛИТОЙ «BOLID VIDEOSCAN»

В случае отсутствия возможности доступа к продукту через Web-интерфейс, а также, если неизвестен текущий IP-адрес изделия, можно воспользоваться утилитой BOLID VideoScan. Скачать утилиту для работы возможно по ссылке: **https://bolid.ru/video/.**

Программа утилиты «BOLID VideoScan» используется для обнаружения текущего IP-адреса устройства в сети, для изменения IP-адреса, управления базовыми настройками, а также для обновления программного обеспечения.

ВНИМАНИЕ!

При работе с утилитой BOLID VideoScan используется по умолчанию имя пользователя admin, пароль – admin, порт 37777.

Выполнив запуск утилиты «BOLID VideoScan», в открывшемся окне визуального интерфейса пункта меню «Сеть» измените IP-адрес изделия и чтобы завершить изменение нажмите кнопку «Сохранить». На рисунке (Рисунок 7.1) представлены базовые параметры для изменения.

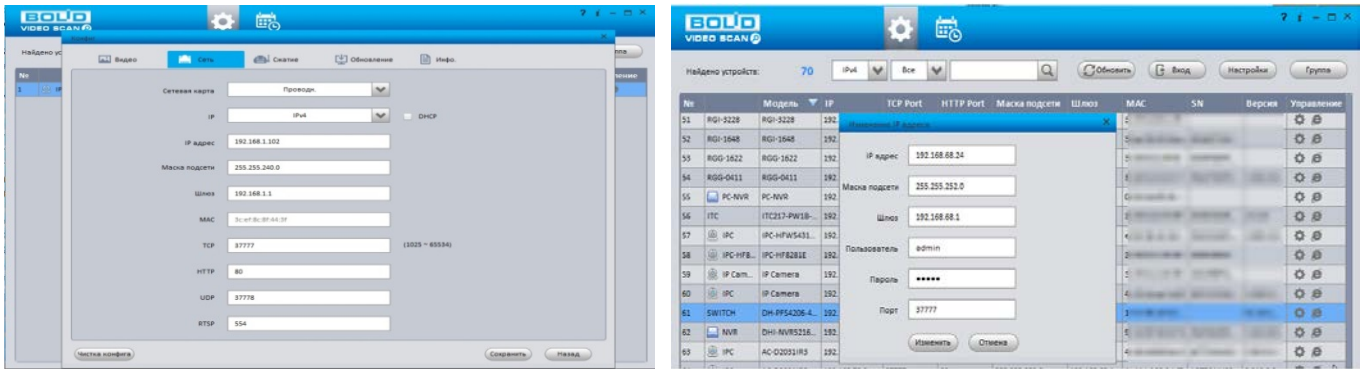

Рисунок 7.1 – Работа с BOLID VideoScan

8 ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ И ПРОВЕРКА РАБОТОСПОСОБНОСТИ

Техническое ежемесячное и ежегодное обслуживание изделия должно проводиться электромонтерами, имеющими группу по электробезопасности не ниже 3. Ежегодные и ежемесячные работы по техническому обслуживанию проводятся согласно принятых и действующих в организации пользователя регламентов и норм и в том числе могут включать:

- проверку работоспособности изделия, согласно инструкции по монтажу;
- проверку целостности корпуса, целостность изоляции кабеля, надёжности креплений, контактных соединений;
- очистку корпуса от пыли и грязи;
- тестирование кабельных линий связи и электропитания;
- очистку и антикоррозийную обработку электроконтактов кабельного подключения.

Техническое обслуживание должно исключать возможность образования конденсата на контактах по завершению и в ходе работ технического обслуживания.

9 ВОЗМОЖНЫЕ НЕИСПРАВНОСТИ И СПОСОБЫ ИХ УСТРАНЕНИЯ

ВНИМАНИЕ!
При затруднениях, возникающих во время настройки и эксплуатации изделия, обратитесь в службу технической поддержки BOLID:
Тел.: (495) 775-71-55 (многоканальный);
E-mail: support@bolid.ru.

Перечень неисправностей и способы их устранения (Таблица 8.1).

Таблица 8.1 – Перечень возможных неисправностей

Внешнее проявление неисправности	Возможные причины неисправности	Способы и последовательность определения неисправности
Отсутствует свечение индикаторов	Нет питания	
Порт не устанавливает соединение, свечение индикатора присутствует	Частичный обрыв кабеля	Проверьте кабель соединения на частичные обрывы.
	Неправильная настройка портов	Проверьте настройки портов на соответствие скорости и режима работы.
	Неисправность камеры	Замените камеру.

10 РЕМОНТ

При выявлении неисправного изделия его нужно направить в ремонт по адресу предприятия – изготовителя. При направлении изделия в ремонт к нему обязательно должен быть приложен акт с описанием возможной неисправности.

Рекламации направлять по адресу: ЗАО НВП «Болид», 141070, Московская область, г. Королёв, ул. Пионерская, д. 4.

Тел./факс: (495) 775-71-55 (многоканальный);

https://bolid.ru;

E-mail: info@bolid.ru;

Техническая поддержка: support@bolid.ru.

11 МАРКИРОВКА

На изделиях нанесена маркировка с указанием наименования, заводского номера, месяца и года их изготовления в соответствии с требованиями, предусмотренными ГОСТ Р 51558-2014. Маркировка нанесена на лицевой (доступной для осмотра без перемещения составной части изделия) стороне.

Маркировка составных частей изделия после хранения, транспортирования и во время эксплуатации не осыпается, не расплывается, не выцветает.

12 УПАКОВКА

Упаковка прочная и обеспечивает защиту от повреждений при перевозке, переноске, а также от воздействия окружающей среды и позволяет осуществлять хранение изделия в закрытых помещениях, в том числе и неотапливаемых, а также снабжена эксплуатационной документацией.

13 ХРАНЕНИЕ

Хранение изделия в потребительской таре должно соответствовать условиям хранения 1 по ГОСТ 15150-69. Средний срок сохраняемости изделия в отапливаемых помещениях не менее 5 лет, в неотапливаемых помещениях не менее 2 лет.

В помещениях для хранения не должно быть паров кислот, щелочей, агрессивных газов и других вредных примесей, вызывающих коррозию. Хранение изделия должно осуществляться в упаковке предприятия-изготовителя при температуре окружающего воздуха от -10 до +55°С и относительной влажности до 90%.

14 ТРАНСПОРТИРОВКА

Транспортирование выполнять только в упакованном виде – в исправной заводской упаковке комплекта поставки или в специально приобретенной потребителем упаковке для транспортирования, обеспечивающей сохранность видеорегистратора при ее транспортировании. Транспортирование упакованных изделий должно производиться любым видом транспорта в крытых транспортных средствах, без разрушения изделия и без изменения внешнего вида изделия. При транспортировании изделие должно оберегаться от ударов, толчков, воздействия влаги и агрессивных паров и газов, вызывающих коррозию. Транспортирование изделия должно осуществляться в упаковке предприятия-изготовителя при температуре окружающего воздуха от 223 до 323 К (от -60 до +65°С).

15 УТИЛИЗАЦИЯ

Изделие не представляет опасности для жизни, здоровья людей и окружающей среды в течение срока службы и после его окончания. Специальные меры безопасности при утилизации не требуются. Утилизацию устройства приобретатель устройства выполняет самостоятельно согласно государственных правил (регламента, норм) сдачи в мусоросбор на утилизацию, выполнение утилизации бытовой электронной техники, видео и фото - электронной техники.

Содержание драгоценных материалов: не требует учёта при хранении, списании и утилизации.

Содержание цветных металлов: не требует учёта при списании и дальнейшей утилизации изделия.

16 ГАРАНТИИ ИЗГОТОВИТЕЛЯ

Гарантийный срок эксплуатации – 36 месяцев с момента приобретения.

При отсутствии документа, подтверждающего факт приобретения, гарантийный срок исчисляется от даты производства.

17 СВЕДЕНИЯ О СЕРТИФИКАЦИИ

Изделие соответствует требованиям технического регламента ТР ТС 020/2011, ТР ТС 004/2011. Имеет сертификат соответствия № RU C-RU.ME61.B.01431, декларацию о соответствии № RU Д-RU.PA02.B.95113/21 и сертификат соответствия технических средств обеспечения транспортной безопасности № МВД РФ.03.000973.

18 СВЕДЕНИЯ О ПРИЕМКЕ

Изделие, коммутатор сетевой «BOLID SW-224» АЦДР.203729.004, принято в соответствии с обязательными требованиями государственных стандартов и действующей технической документации, признано годным к эксплуатации ЗАО НВП «Болид». Заводской номер, месяц и год выпуска указаны на корпусе изделия, товарный знак BOLID обозначен на корпусе и упаковке.

Перечень рисунков

Перечень таблиц

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ докум.	Входящий № сопроводительного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					

ЗАО НВП «Болид»

Центральный офис:

Адрес: 141070, Московская обл., г. Королев, ул. Пионерская, 4

Тел./факс: +7 (495) 775-71-55 (многоканальный)

Режим работы: пн – пт, 9:00 - 18:00

Электронная почта: info@bolid.ru

Техническая поддержка: support@bolid.ru

Сайт: https://bolid.ru

Все предложения и замечания Вы можете отправлять по адресу support@bolid.ru