Сетевой коммутатор

BOLID SW-216

Версия 3

Руководство по эксплуатации

АЦДР.203729.003 РЭп

Настоящее руководство по эксплуатации (далее по тексту – РЭ) содержит сведения о назначении, конструкции, принципе работы, технических характеристиках управляемого сетевого коммутатора BOLID SW-216 АЦДР.203729.003 (далее по тексту – коммутатор, изделие или изделие) и указания, необходимые для правильной и безопасной эксплуатации.

ВНИМАНИЕ!

- Руководство по эксплуатации содержит только справочную информацию, необходимую для использования его технических возможностей.
- Дизайн изделия, технические характеристики 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

1. Сетевой коммутатор предназначен для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети.

2. Поддержка технологии PoE позволяет передавать питание на различные устройства и периферию. Устройство также используется для подключения видеорегистраторов и сетевых видеокамер по технологии PoE, а также передачи данных между сетевыми устройствами СОТ.

3. При совместном использовании с преобразователями интерфейсов «С2000-Ethernet» позволяет коммутировать сигналы охранно-пожарных приборов ИСО «Орион», а также приборов других систем.

4. Область применения коммутатора: системы видеонаблюдения, охранно-пожарная сигнализация, СКУД, системы контроля и диспетчеризации объектов.

5. Коммутатор рассчитан на круглосуточный режим работы.

6. Коммутатор предназначен для работы в жилых, коммерческих и производственных зонах.

7. Конструкция коммутатора не предусматривает его использование в условиях воздействия агрессивных сред, пыли, а также во взрывопожароопасных помещениях.

8. Отличительные особенности версии 3 от версии 2 и версии 1:

– Появилась опция увеличения дальности передачи со 100 м до предельно 250 м для подключенных в порты 1 – 16 PoE устройств, но при её включении снижается скорость передачи до 10 Мбит/с (со 100 Мбит/с). Включение данной опции производится в веб-интерфейсе устройства;

– Реализовано интеллектуальное управление энергопотреблением PoE. Данная функция позволяет отключать устройства, подключенные в PoE порты с наибольшим номером, затем следующий по величине номер, пока потребляемая мощность не снизится ниже общей допустимой мощности PoE;

– Добавлено обнаружение сбоев – «PoE watchdog», которое автоматически определяет сбой сетевого порта и перезапускает сетевую связь на порту. Эта функция позволяет избежать ручного обслуживания и перезапуска сети, экономя время и снижая затраты.

9. Возможное применение:

Рисунок 1.1 – Сетевое соединение

2 ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

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

Таблица 2.1 – Основные технические характеристики*

Наименование параметра	Значение параметра
Сетевые интерфейсы	
Общее количество	18 интерфейсов
RJ-45	Порт № 1 – 16: RJ-45 10/100 Мбит/с (PoE) Порт № 17 – 18: 2 комбо – порта RJ-45 10/100/1000 Мбит/с (uplink)
SFP	Порт № 17 – 18: 2 комбо – порта SFP 1000 Мбит/с (uplink)
SFP+	Нет
Оборудование	
Порты RJ-45	18 портов
Порты SFP	2 порта
Порты SFP+	Нет
Электропитание (переменный ток)	
Напряжение питания устройства	100 − 240 В переменного тока
Потребляемый ток	4 А
Потребляемая мощность	20 Вт в дежурном режиме 400 Вт при полной нагрузке
Производительность	
Уровень	L2
Тип	Управляемый
Время технической готовности прибора к работе	50 с
Коммутационная матрица	8,8 Gbps
Маршрутизация пакетов	5,36 Mpps
Буфер пакетов	2,57 Мбит
Таблица MAC адресов	4 К

Наименование параметра	Значение параметра
Поддерживаемые стандарты	IEEE 802.3, IEEE 802.3u, IEEE 802.3x, IEEE 802.3ab, IEEE 802.3z
PoE	
Стандарты PoE	IEEE802.3af, IEEE802.3at, Hi-PoE, IEEE802.3bt
Мощность PoE портов	Порт №1 – 2: не более 90 Вт (на порт) Порт № 3 – 16: не более 30 Вт (на порт)
Общая мощность PoE	Не более 240 Вт
Распиновка подаваемого питания PoE	1, 2, 4, 5 (V+), 3, 6, 7, 8 (V-)
PoE управление	Настройка PoE (использование порта в реальном времени), статистика событий PoE, Green PoE, поддержка совместимости, PoE watchdog
Расстояние передачи по PoE	До 250 м
Сервисные особенности	
Основное дерево	IEEE 802.1d (STP); 802.1w (RSTP)
VLAN	IEEE802.1q Standard VLAN
Управление потоками	Поддержка управления потоком на основе IEEE802.3X
Агрегирование (объединение) каналов	LACP, статическое агрегирование
Зеркалирование	1:1 (Один к одному), 1:N (Много к одному)
Multicast	IGMP Snooping
DHCP	DHCP-клиент
Безопасность	Привязка IP+MAC, IEEE802. 1x
Системное обслуживание	Восстановление, обновление прошивки, системный журнал
QoS	Приоритетный режим, WRR/802.1p/DSCP, приоритет протокола
Общие сведения	
Предельное напряжение импульсных помех	2 кВ/1 кВ**
Степень защиты оболочки по ГОСТ 14254-2015	IP40

Наименование параметра		Значение параметра
Устойчивость к механическим воздействиям по ГОСТ 25 1099-83		Категория размещения 3
Вибрационные нагрузки	диапазон частот	1 – 35 Гц
	максимальное ускорение	0,5 g
Диапазон рабочих температур		От -10 °С до +55 °С
Относительная влажность воздуха		От 10 % до 90 %
Габаритные размеры		440×300×44 мм
Масса		3,51 кг
Время непрерывной работы коммутатора		Круглосуточно
Средняя наработка прибора на отказ в дежурном режиме работы		80000 ч
Вероятность безотказной работы за 1000 ч		0,98758
Поддерживаемые модули		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.

**В зависимости от синфазного или разностного сигналов.

По устойчивости к электромагнитным помехам коммутатор соответствует требованиям третьей степени жёсткости, с критерием качества функционирования А, соответствующих стандартов, перечисленных в Приложении Б ГОСТ Р 53325-2012.

Коммутатор удовлетворяет нормам индустриальных помех, установленным для оборудования класса Б по ГОСТ Р 30805.22.

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.

Таблица 2.2 – Зависимость максимальной пропускной способности и мощности от длины кабеля*

Кабель (м)	**Максимальная мощность (Вт)**	**Пропускная способность (Мбит/с)**
IEEE802.3bt 90 Вт		
100	71,3	100
150	62	10
200	51	10
250	40	10
Hi-PoE 60 Вт		
100	53	100
150	50	10
200	47	10
250	37	10
IEEE802.3at 30 Вт		
100	25,5	100
150	25,5	10
200	25,5	10
250	25,5	10

*В лабораторных условиях. При напряжении питания PoE 53 В. Для кабелей категории CAT5E/CAT6 и максимальном сопротивлении постоянному току < 10Ω/100 м.

3 КОМПЛЕКТНОСТЬ

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

Таблица 3.1 – Комплект поставки*

Обозначение	Наименование	Количество
АЦДР.203729.003	Коммутатор «BOLID SW-216»	1 шт.
АЦДР.203729.003 РЭ	Руководство по эксплуатации изделия «BOLID SW-216»	1 экз.
	Кабель питания, 220 В переменного тока	1 шт.
	Крепление в стойку	2 шт.
	Винт М3×5	6 шт.
	SFP модуль**	—

*Комплект поставки может отличаться от заявленного.

** – Поставляются по отдельному заказу. Список совместимых комплектных SFP-модулей указан в «Приложение А».

4 КОНСТРУКЦИЯ

4.1 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	RJ-45 10/100 Мбит/с (PoE)	Порты подключения PoE устройств и элементов локальной сети.
2	Комбинированные порты	10/100/1000 Мбит/с: Гигабитные порты Base-T с индикаторами состояния. Без PoE. Являются комбинированными (combo) портами. Не работают одновременно с оптическими SFP портами.
		1000 Мбит/с: Оптические SFP порты. Являются комбинированными (combo) портами. Не работают одновременно с Гигабитными портами Base-T.
3	RESET	Кнопка сброса на заводские настройки.
4	Console (RS-232)	Порт для прошивки.
5	PoE PWR	Световой индикатор электропитания PoE.
6	Индикаторы 1 – 16	Световые индикаторы состояния PoE и Uplink.
7	Индикаторы 17 – 18	Световые индикаторы состояния 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 разъёмам RJ-45 коммутатора с помощью стандартного штекера 8P8C.

4.2 Задняя панель

Конструктивно коммутатор выполнен в металлическом корпусе, подходит для крепления в серверную стойку.

На задней панели устройства расположен винт защитного заземления, клавиша включения/выключения питания, вентиляционное отверстие и разъём питания с поддержкой 100 – 240 В переменного тока.

Рисунок 4.2 – Задняя панель

5 МОНТАЖ И ДЕМОНТАЖ

5.1 Меры безопасности

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

1. Монтаж и техническое обслуживание коммутатора должны производиться лицами, имеющими квалификационную группу по технике безопасности не ниже второй.

2. Конструкция коммутатора удовлетворяет требованиям пожарной и электробезопасности, в том числе в аварийном режиме по ГОСТ 12.2.007.0-75, ГОСТ Р 50571.3.

3. При использовании коммутатора внимательно относитесь к функциям внешнего питания. Для обеспечения защиты системы от внезапных кратковременных скачков электропитания используйте ограничитель напряжения, формирователь линии или источник бесперебойного питания (UPS).

4. Не устанавливайте коммутатор в местах: температура в которых опускается ниже минус 10 °С и/или поднимается выше плюс 55 °С; с влажностью выше 90 %; повышенного испарения и парообразования; усиленной вибрации.

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

6. Предотвращайте механические повреждения коммутатора. Несоответствующие условия хранения и эксплуатации коммутатора могут привести к повреждению оборудования.

7. В случае если от устройства идёт дым или непонятные запахи, немедленно выключите питание и свяжитесь с авторизованным сервисным центром (вашим поставщиком).

8. Если, на ваш взгляд, устройство работает некорректно, ни в коем случае не пытайтесь разобрать его самостоятельно. Свяжитесь с авторизованным сервисным центром (вашим поставщиком).

9. Не допускайте установку устройства под воздействием прямых солнечных лучей и вблизи источников, излучающих тепло.

5.2 Монтаж

1. Размещение и монтаж должен 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;

– У портов достаточно свободного пространства для доступа и подводки кабелей;

– Разъём питания находится в пределах досягаемости для подключения к источнику питания;

– Изделие заземлено согласно ПУЭ-7 п.1.7.126 (сечение медного кабеля: ≥ 2,5 мм^2, сопротивление относительно земли: ≤ 4 Ом);

– 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.

5.2.1 Подготовка изделия к монтажу

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

Коммутатор предназначен для установки в стойку, на полку или стол. В комплект поставки коммутатора входит комплект для крепления в стойку, состоящий из двух скоб и шести винтов.

Габаритные размеры коммутатора приведены на рисунке ниже (Рисунок 5.1).

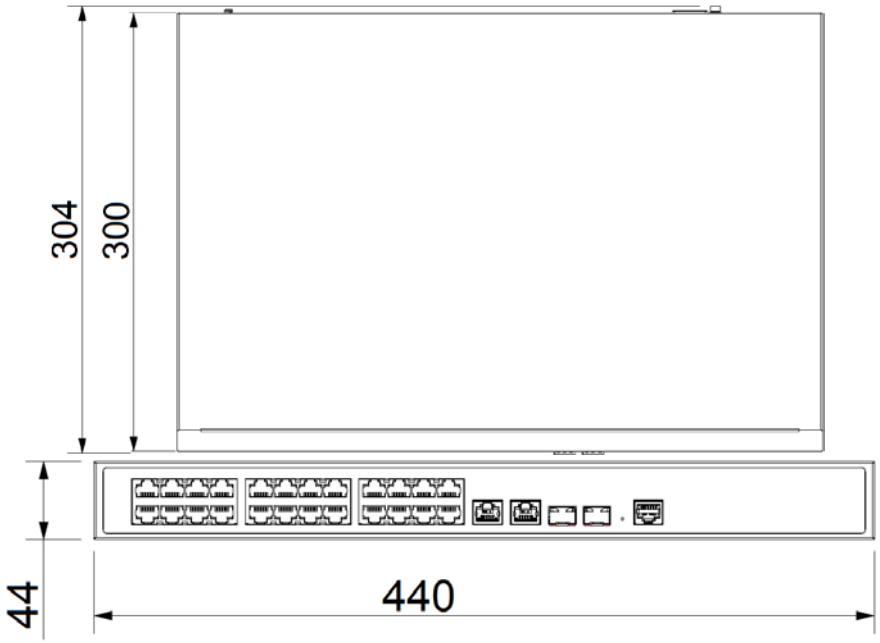

Рисунок 5.1 – Габаритные размеры

5.2.2 Монтаж коммутатора в 19”-стойку

1. Установите и зафиксируйте при помощи винтов из комплекта поставки крепления (скобы) на корпус коммутатора.

2. Установите коммутатор в стойку с учетом достаточного пространства для кабелей на задней панели и с учетом свободной циркуляции воздуха, не перекрывая вентиляционные отверстия.

3. Зафиксируйте винтами, поставляемыми со стойкой, коммутатор к стойке (Рисунок 5.2).

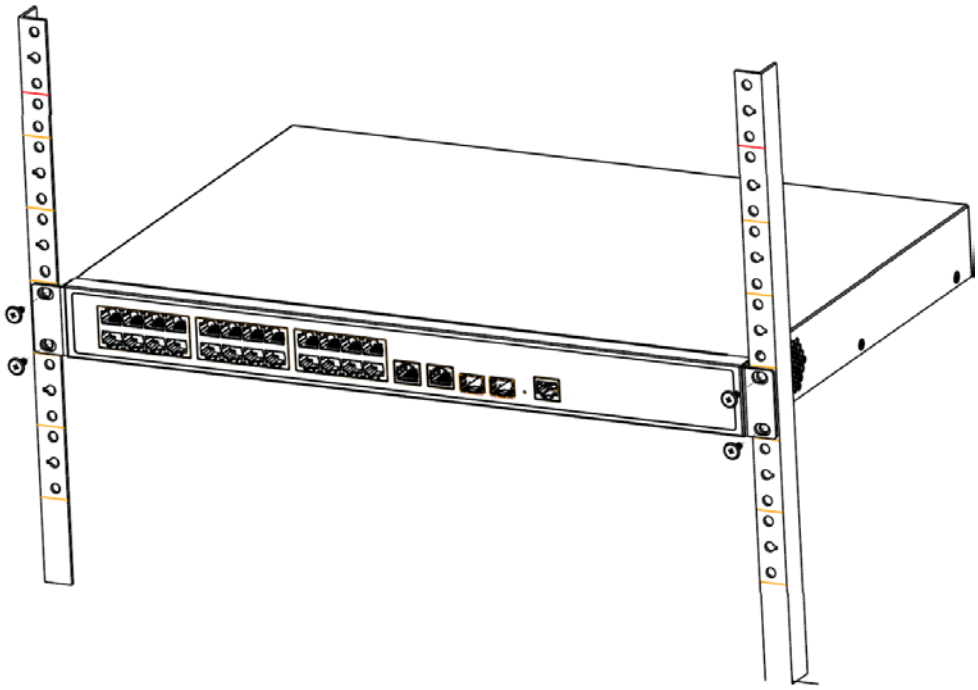

Рисунок 5.2 – Монтаж коммутатора в 19” – стойку

5.2.3 RJ-45

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 разъёмам RJ-45 коммутатора с помощью стандартного штекера 8P8C.

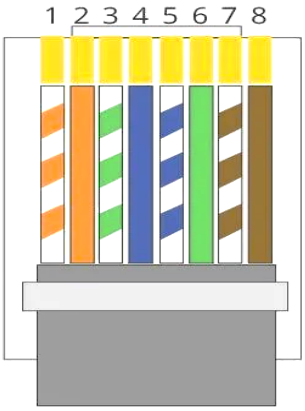

Рисунок 5.3 – Штекер 8P8C

Распиновка кабеля

1, 2, 4, 5 (V+), 3, 6, 7, 8 (V-)

1 – Бело-оранжевый
2 – Оранжевый
3 – Бело-зелёный
4 – Синий
5 – Бело-синий
6 – Зелёный
7 – Бело-коричневый
8 – Коричневый

5.2.4 Установка SFP

ВНИМАНИЕ!

– Не снимайте пылезащитную заглушку с SFP-модуля, также не снимайте защитный колпачок с оптоволоконного кабеля до его подсоединения. Защитная заглушка и колпачок защищают оптические разъёмы и кабель от загрязнений и окружающего света.
– Не устанавливайте SFP-модуль с подключенным оптоволоконным кабелем в слот. Прежде чем установить SFP-модуль извлеките оптоволоконный кабель.
– Многократная установка и извлечение SFP-модуля может сократить его срок эксплуатации.
– При подключении к коммутатору и другим устройствам соблюдайте стандартный порядок работ с платами и электронными компонентами, чтобы предотвратить повреждения из-за электростатических разрядов.

1. Закрепите на руке антистатический браслет и подсоедините его к точке заземления или металлической поверхности.

2. Извлеките модуль из упаковки.

3. Подключите SFP-модуль в разъём коммутатора до появления характерного щелчка фиксации модуля.

4. Извлеките пылезащитную заглушку из модуля. Убедитесь, что фиксатор с цветовой маркировкой находится в защелкнутом состоянии.

5. В соответствии с указателями передатчика ▼ (TX) и приемника ▲ (RX), вставьте оптоволоконный кабель в разъём модуля.

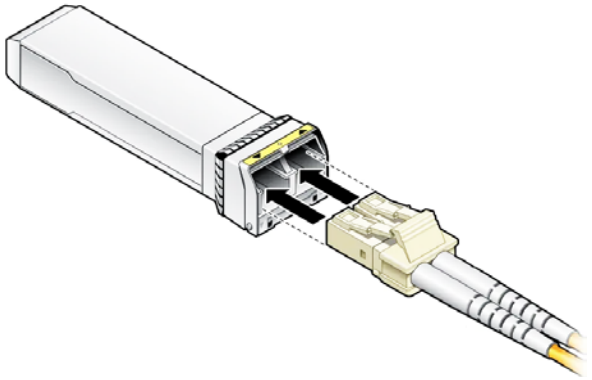

Рисунок 5.4 – Подключения кабеля

5.3 Демонтаж

Демонтаж производится в обратном порядке при отключенном напряжении питания.

6 ПЕРВОЕ ВКЛЮЧЕНИЕ. ИНИЦИАЛИЗАЦИЯ УСТРОЙСТВА

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.

6.1 Инициализация устройства

Шаг 1. Убедитесь, что сетевая карта компьютера находится в той же подсети, что и коммутатор. Запустите веб-браузер и в адресной строке введите IP-адрес коммутатора, по умолчанию (192.168.1.110).

Учётные данные по умолчанию при первом включении коммутатора:	
Имя пользователя	admin
IP-адрес	192.168.1.110
Маска подсети	255.255.255.0

Шаг 2. При заводских настройках пароль по умолчанию отсутствует, поэтому установите пароль учётной записи «admin». В строках «Пароль» и «Подтверждение пароля» введите пароль устройства. Вводимый пароль должен представлять собой комбинацию латинских букв верхнего и нижнего регистра, длиной не менее 8, но не более 32 символов (символы: « ' », « " », « ; », « : », « & » недопустимы для ввода). После ввода пароля нажмите кнопку «Подтвердить».

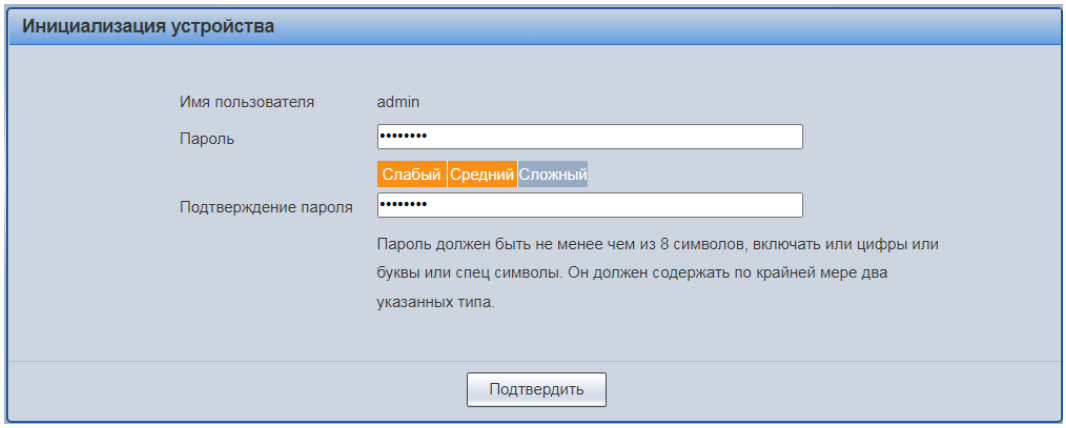

Рисунок 6.1 – Инициализация

Шаг 3. Далее, для входа, повторно введите новый пароль учётной записи admin и нажмите кнопку «Вход».

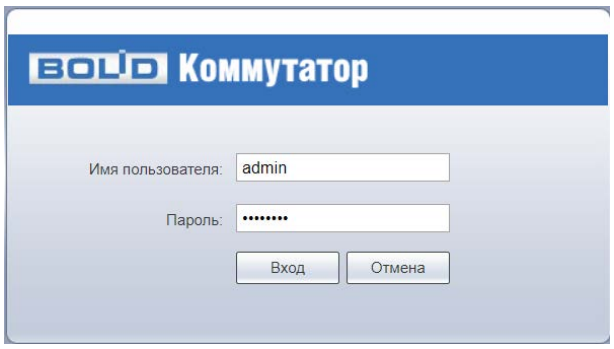

Рисунок 6.2 – Вход

Шаг 4. Измените сетевые настройки коммутатора в соответствии с параметрами вашей сети. Для этого перейдите «Настройки => Конфигурация => Настройки сети» (Рисунок 6.3). Введите новые параметры сети и нажмите «Сохранить».

Устройство перезагрузится автоматически после сохранения сетевых настроек. Если не произошла автоматическая перезагрузка, то перезагрузите устройство самостоятельно, для этого перейдите «Настройки => Перезагрузка системы и нажмите кнопку «Перезагрузить».

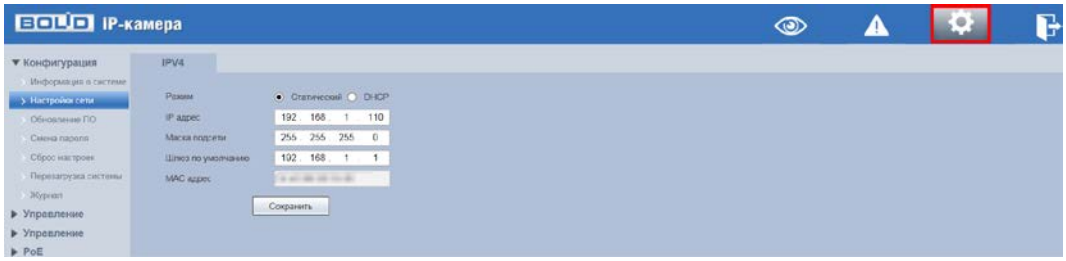

Рисунок 6.3 – Сетевые настройки

Таблица 6.1 – Параметры сетевых настроек 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/маску подсети/шлюз.
IP адрес	Текстовое поле служит для отображения и изменения текущего IP-адреса устройства.
Маска подсети	Текстовое поле служит для отображения и изменения текущей маски подсети, соответствующей сегменту сети, в котором находится коммутатор.
Шлюз по умолчанию	Текстовое поле служит для отображения и изменения текущего IP-адреса шлюза. IP-адрес устройства и шлюз должны находиться в одном сегменте сети.
MAC адрес	Текстовое поле отображает MAC-адреса устройства.

Шаг 5. После изменения настроек веб-интерфейс должен быть доступен по-новому IP-адресу. Корректный вход в систему производится с новыми учётными данными admin.

7 ИНФОРМАЦИОННАЯ ПАНЕЛЬ

Информационная панель включает в себя графическую и текстовую информацию о состоянии портов.

Рисунок 7.1 – Информационная панель

Графическая панель представляет собой изображение передней панели коммутатора. Отображает состояние подключения к каждому порту в реальном времени (Рисунок 7.2).

Рисунок 7.2 – Графическая панель

Активируйте опцию «Информация об устройстве на порте». После активации графическая панель будет отображать не только информацию о состоянии подключений, но и появится разветвление с дополнительной текстовой информацией о подключенном устройстве на выбранном порту. Текстовая информация включает в себя: IP-адрес, MAC-адрес, VLAN, информацию о PoE и модель устройства (Рисунок 7.3).

Рисунок 7.3 – Графическая панель

Дополнительно просмотреть информацию о подключенных устройствах можно при переходе в раздел меню «Список устройств».

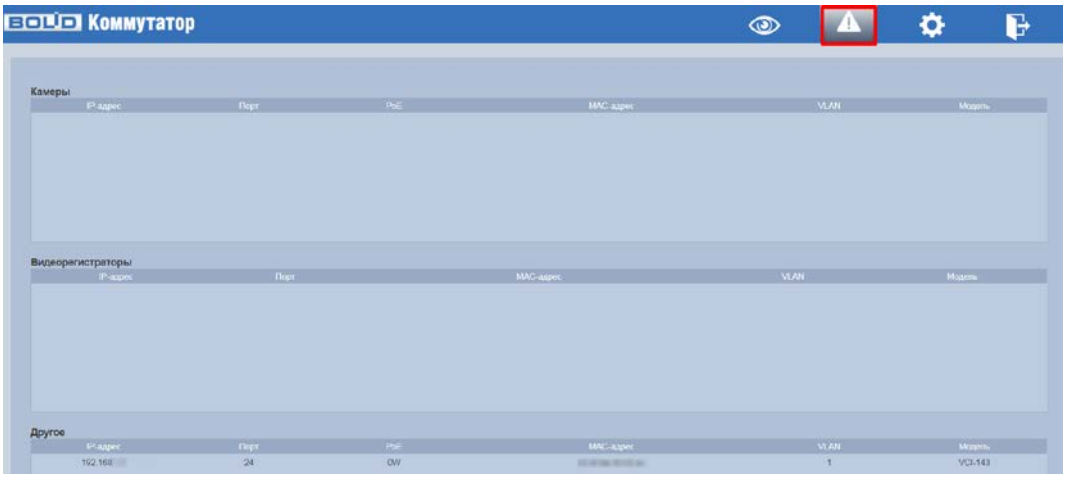

Рисунок 7.4 – Список подключенных устройств

Параметры текстовой панели описаны в таблице ниже (см. Таблица 7.1).

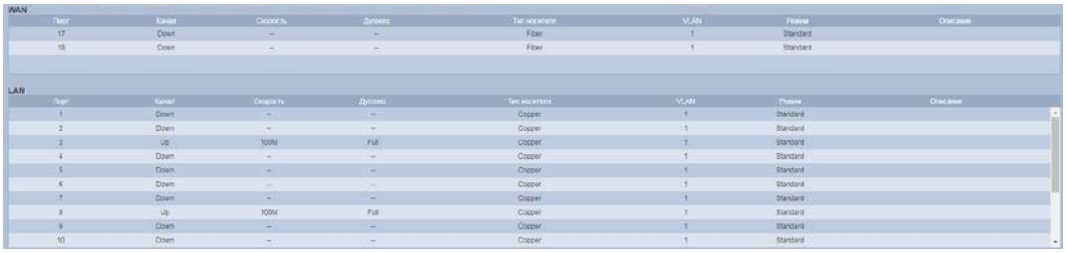

Рисунок 7.5 – Текстовая информационная панель

Таблица 7.1 – Текстовая информация о порте

Параметр	Описание
Порт	Номер порта. Соответствует числу на передней панели.
Канал	– Up – порт подключен; – Down – порт отключен; – Disabled – порт выключен.
Скорость/Дуплекс	Отображает текущую скорость и в каком режиме передачи параллельном (Full) или последовательном находится порт.
Тип носителя	Показывается тип подключенного носителя сигнала. – Copper – медный кабель; – Fiber – волоконно-оптический кабель.
VLAN	Идентификатор VLAN.
Описание	Текстовое поле с описанием порта.

8 НАСТРОЙКА

8.1 Раздел «Конфигурация системы»

8.1.1 Подраздел «Информация о системе»

8.1.1.1 **Пункт «Информация о системе»**

Интерфейс отображает информацию о версии программного обеспечения, системную информацию и время работы устройства.

Рисунок 8.1 – Информация о системе

8.1.1.2 **Пункт «Текущее время»**

Уделите внимание настройкам времени на устройстве. Неправильно выставленное время, может привести к некорректному отображению журналу событий, вызвать проблемы при работе сертификата открытого ключа и т.д. В настройках устройства доступна ручная синхронизация с ПК.

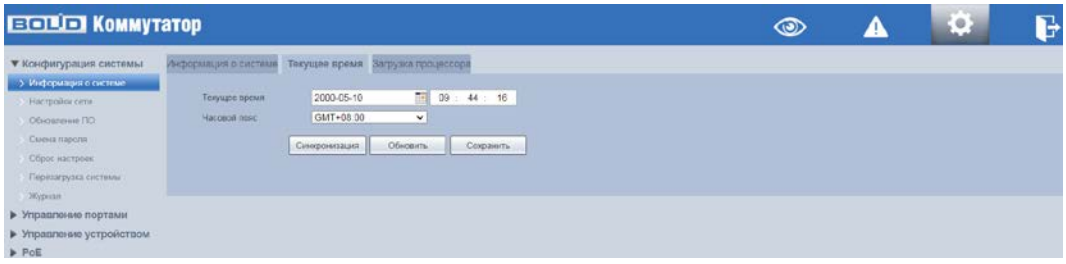

Рисунок 8.2 – Текущее время

Таблица 8.1 – Настройки времени на устройстве

Параметр	Функция
Текущее время	Установка системного времени.
Часовой пояс	Выбор часового пояса из выпадающего списка.

Таблица 8.2 – Кнопки

Кнопка	Функция
Синхронизация	Синхронизировать время с ПК.
Обновить	Обновить информацию.
Сохранить	Сохранить настройки.

8.1.1.3 **Пункт «Загрузка процессора»**

Информация о нагрузке на процессор.

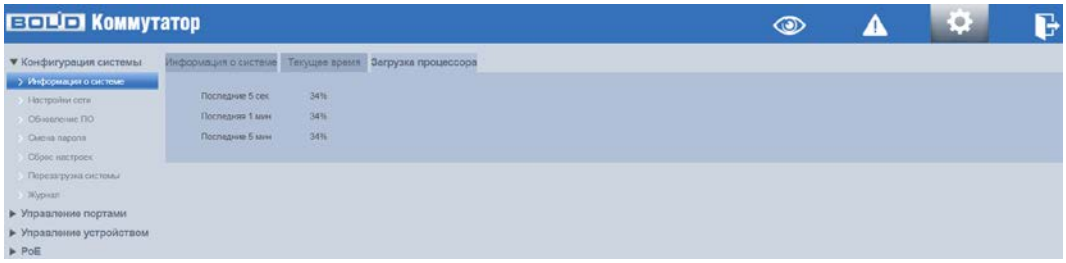

Рисунок 8.3 – Загрузка процессора

8.1.2 Подраздел «Настройки сети»

Измените сетевые настройки коммутатора в соответствии с параметрами вашей сети. После внесения изменений устройство перезагрузится автоматически.

Рисунок 8.4 – Сетевые настройки

Таблица 8.3 – Сетевые настройки устройства

Параметр	Функция
Режим	DHCP: IP-адрес будет получен автоматически от DHCP-сервера. Статический: в этом режиме следует задать вручную IP/маску подсети/шлюз.
IP адрес	Текстовое поле служит для отображения и изменения текущего IP-адреса устройства.
Маска подсети	Текстовое поле служит для отображения и изменения текущей маски подсети, соответствующей сегменту сети, в котором находится коммутатор.
Шлюз по умолчанию	Текстовое поле служит для отображения и изменения текущего IP-адреса шлюза. IP-адрес устройства и шлюз должны находиться в одном сегменте сети.
MAC адрес	Текстовое поле отображает MAC-адреса устройства.

8.1.3 Подраздел «Обновление ПО»

Для обновления ПО необходимо импортировать файл прошивки на устройство, для этого нажмите кнопку «Обзор». В появившемся диалоговом окне выберите файл с прошивкой и нажмите кнопку «Открыть», в строке «Выберите файл прошивки» будет отображен импортированный файл. Нажмите кнопку «Прошивка» для начала обновления.

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

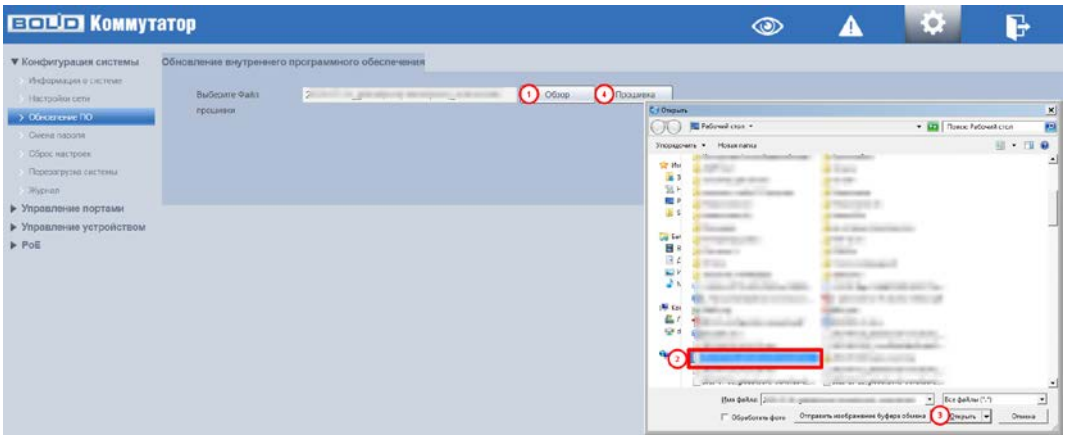

Рисунок 8.5 – Обновление ПО

8.1.4 Подраздел «Смена пароля»

Для изменения пароля учётной записи (Рисунок 8.6):

1. Введите старый пароль устройства в текстовое поле «Старый пароль».

2. Введите новый пароль в текстовое поле «Новый пароль». Вводимый пароль должен представлять собой комбинацию цифр, латинских букв верхнего и нижнего регистра длиной не менее 8, но не более 32 символов (символы: « ' », « " », « ; », « : », « & » недопустимы для ввода).

3. Подтвердите введенный пароль, текстовое поле «Подтверждение пароля».

4. Нажмите кнопку «Сохранить».

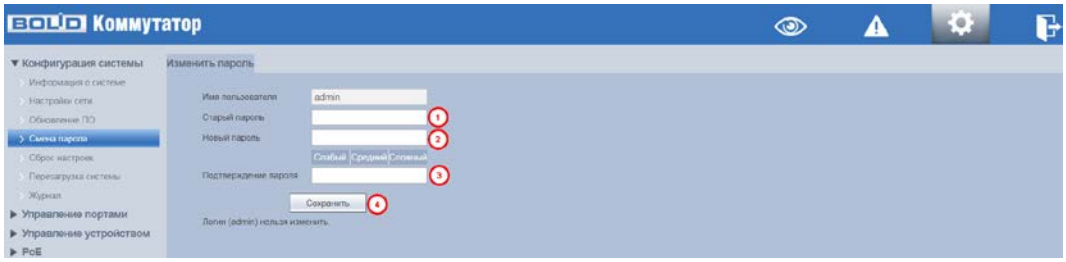

Рисунок 8.6 – Смена пароля

8.1.5 Подраздел «Сброс настроек»

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

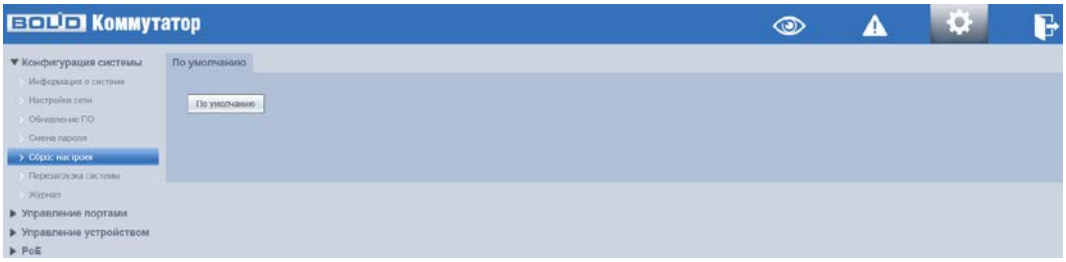

Рисунок 8.7 – Сброс параметров

Для подтверждения сброса, в текстовом поле «Пароль» диалогового окна «По умолчанию» нужно ввести пароль устройства и далее нажать кнопку «Сохранить».

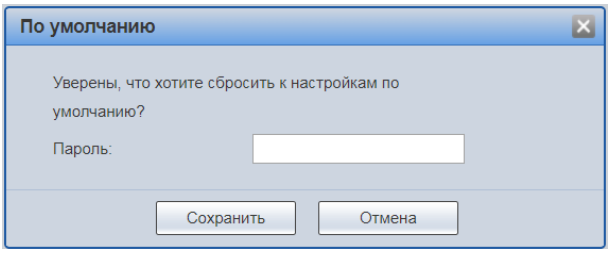

Рисунок 8.8 – Сброс параметров

8.1.6 Заводские настройки

Сброс до заводских настроек возможен при помощи кнопки сброса «RESET» на передней панели.

Рисунок 8.9 – Сброс параметров

В случае невозможности восстановления пароля администратора:

1. Подключите источник питания и дождитесь загрузки устройства.

2. Нажмите кнопку «RESET» и удерживайте ее в течение 5 – 10 секунд до перезагрузки.

3. Отпустите кнопку «RESET».

4. Коммутатор приблизительно через 20 секунд загрузится, и настройки вернутся к заводским (полный сброс всех настроек).

8.1.7 Подраздел «Перезагрузка системы»

Нажмите кнопку «Перезагрузить» для программной перезагрузки устройства.

Рисунок 8.10 – Перезагрузка устройства

8.1.8 Подраздел «Журнал»

Интерфейс (Рисунок 8.11) 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 кнопку «Поиск».

В журнале хранится максимум 10000 записей (до 10 записей на каждой из страниц). Для переключения между страницами используйте стрелки  или введите в поле номер нужной страницы и нажмите кнопку  .

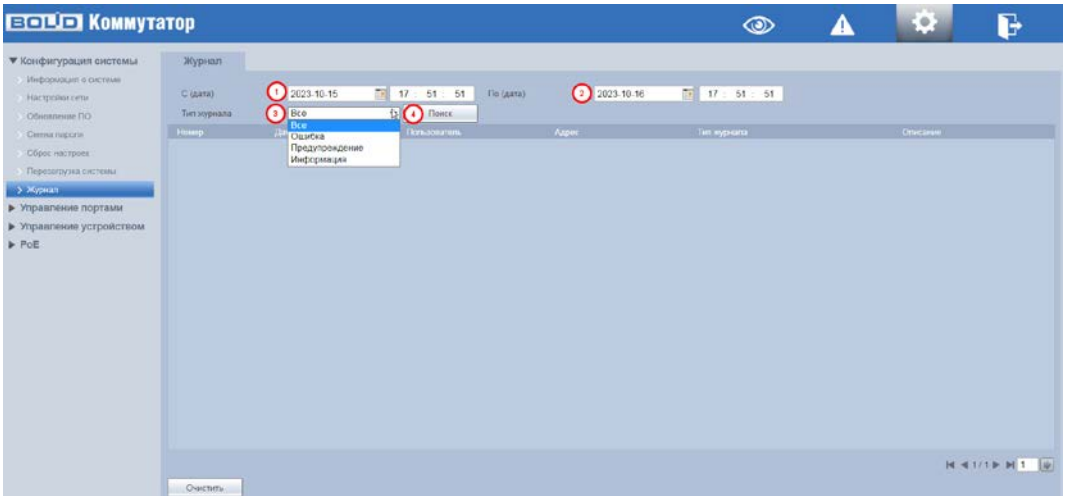

Рисунок 8.11 – Интерфейс просмотра журнала

8.2 Раздел «Управление портами»

8.2.1 Подраздел «Настройка портов»

На рисунке (Рисунок 8.12) показан интерфейс конфигурации портов коммутатора. Настройка конфигурации порта должна соответствовать практическим требованиям устройства (Таблица 8.4).

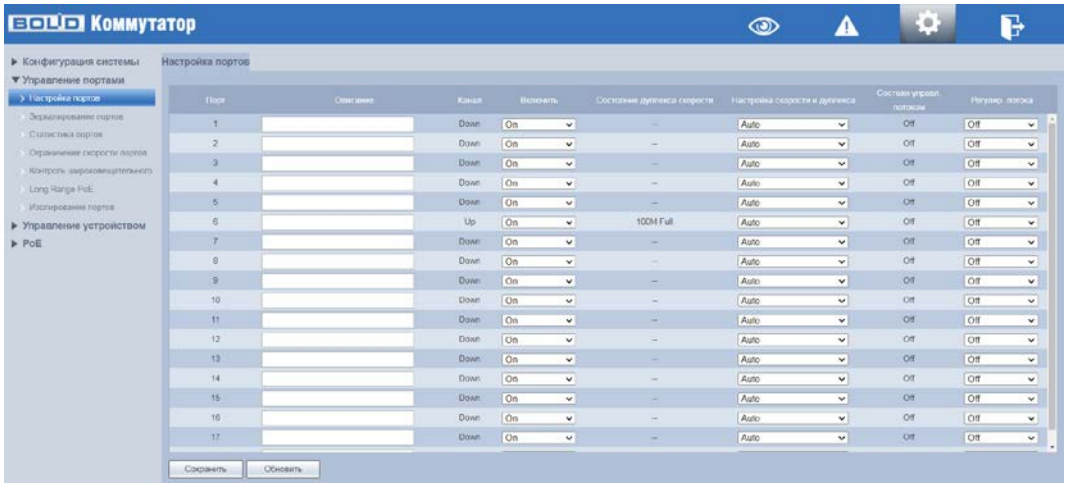

Рисунок 8.12 – Конфигурация портов коммутатора

Таблица 8.4 – Настройка конфигурации портов

<table>
<tr><th colspan="3">Столбец</th><th colspan="3">Описание</th></tr>
<tr><td colspan="3">Порт</td><td colspan="3">Номер порта соответствует числу на лицевой панели.</td></tr>
<tr><td colspan="3">Описание</td><td colspan="3">Текстовое пользовательское поле для описания порта.</td></tr>
<tr><td rowspan="2">Канал</td><td rowspan="2">Отображает статус связи порта</td><td>Up</td><td colspan="3">Порт находится в активном состоянии.</td></tr>
<tr><td>Down</td><td colspan="3">Порт находится в отключенном состоянии.</td></tr>
<tr><td rowspan="2">Включить</td><td rowspan="2">Служит для включения/ выключения порта</td><td>On</td><td colspan="3">Переключение порта во включенное состояние.</td></tr>
<tr><td>Off</td><td colspan="3">Переключение порта в выключенное состояние.</td></tr>
<tr><td colspan="3">Состояние дуплекса скорости</td><td colspan="3">Отображает текущее состояние скорости порта.</td></tr>
<tr><td rowspan="7">Настройка скорости и дуплекса</td><td colspan="5">Отображает текущее состояние скорости порта</td></tr>
<tr><td>Порт</td><td>Скорость</td><td colspan="3">Описание</td></tr>
<tr><td rowspan="4">Ethernet порт</td><td>Авто.</td><td colspan="3">Автоматическая настройка скорости и режима передачи.</td></tr>
<tr><td>10M FULL</td><td colspan="3">Скорость 10 Мб/с. Работа в режиме полного дуплекса.</td></tr>
<tr><td>10M HALF</td><td colspan="3">Скорость 10 Мб/с. Работа в режиме полудуплекса.</td></tr>
<tr><td>100M HALF</td><td colspan="3">Скорость 100 Мб/с. Работа в режиме полудуплекса.</td></tr>
<tr><td>100M FULL</td><td colspan="3">Скорость 100 Мб/с. Работа в режиме полного дуплекса.</td></tr>
<tr><td>Оптический порт</td><td>1000M FULL</td><td colspan="3">Скорость 1000 Мб/с. Работа в режиме полного дуплекса.</td></tr>
</table>

Столбец	Описание	
Состояние управления потоком	Отображает текущее состояние настройки управления потоком.	
Регулировка потока	Up	Включение функции управления потоком на порте.
	Off	Выключение функции управления потоком на порте.

8.2.2 Подраздел «Зеркалирование портов»

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

1. В соответствующем подразделе «Зеркалирование портов» из выпадающего списка «Мониторинг пакетов» выбрать направление пакетов (Рисунок 8.13).

– Отключить – все пакеты (tx и rx) не будут зеркалироваться;

– Исходящий – пакеты, исходящие с этого порта будут отправлены на порт назначения. Получаемые пакеты зеркалироваться не будут.

– Входящий – пакеты, полученные на этот порт, будут отправлены на порт назначения. Исходящие пакеты зеркалироваться не будут.

– Входящий, исходящий – полученные и исходящие пакеты посылаются на порт назначения.

2. Выбрать из выпадающего списка порт назначения. Выбирается только один порт зеркалирования, на который отправляются данные с других портов, но при этом, есть возможность выбрать несколько портов источников.

3. Отметьте в списке порты, с которых хотите получать копии пакетов.

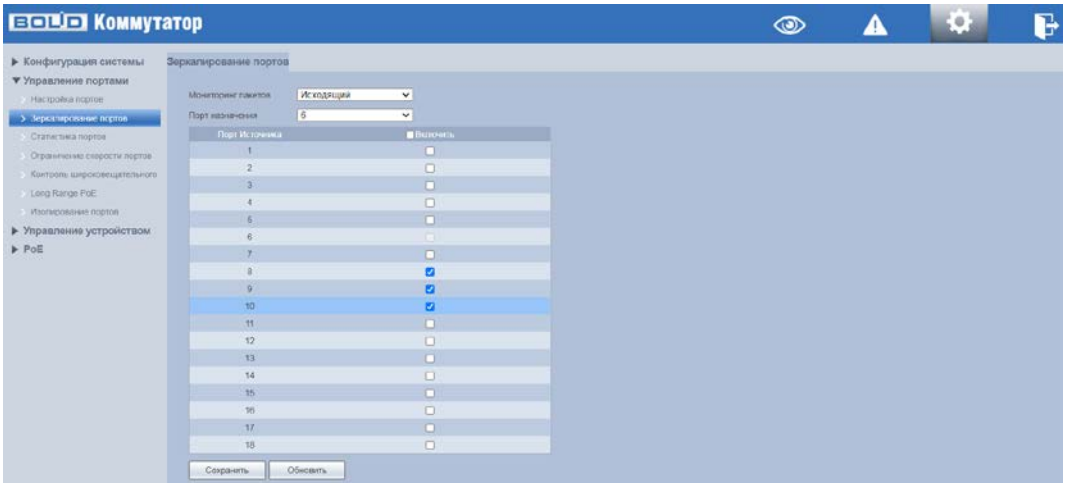

Рисунок 8.13 – Зеркалирование трафика

8.2.3 Подраздел «Статистика портов»

Интерфейс статистики портов коммутатора показан на рисунке ниже (Рисунок 8.14).

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

– Принятые и переданные пакеты – статистика переданных и полученных пакетов;

– Пакеты с коллизиями и пакетов передано – статистика пакетов с коллизиями и переданных пакетов;

– Отброшенные и полученные пакеты – статистика отброшенных и полученных пакетов;

– Пакеты с CRC ошибкой и полученные пакеты – статистика поврежденных пакетов и полученных пакетов.

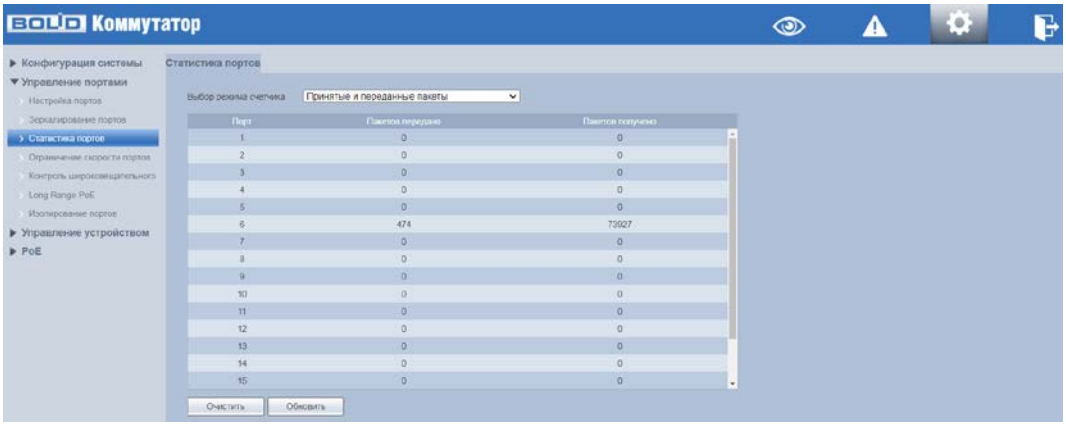

Рисунок 8.14 – Статистика портов

8.2.4 Подраздел «Ограничение скорости портов»

Интерфейс ограничения пропускной способности входящих/ исходящих пакетов на порт. Возможно, ограничить скорость в пределах от 0 до 63 Мбит/с, 0 будет означать отсутствие ограничений скорости.

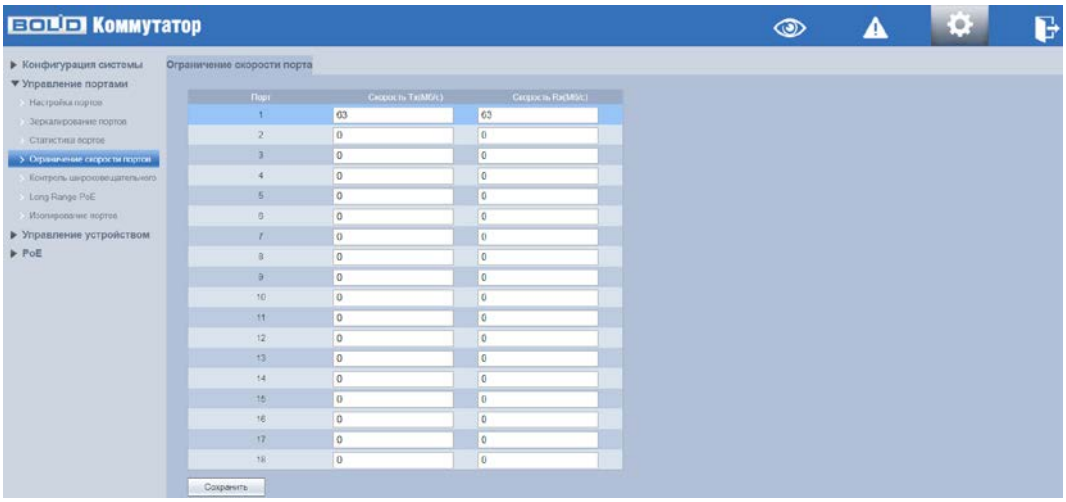

Рисунок 8.15 – Ограничение скорости

8.2.5 Подраздел «Контроль широковещательного шторма»

В ПО коммутатора включена функция ограничения широковещательных пакетов. Для настройки отметьте флажком те порты, для которых хотите установить порог числа широковещательных пакетов, разрешённых для входа в каждый порт за определенный промежуток времени (Рисунок 8.16). 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.

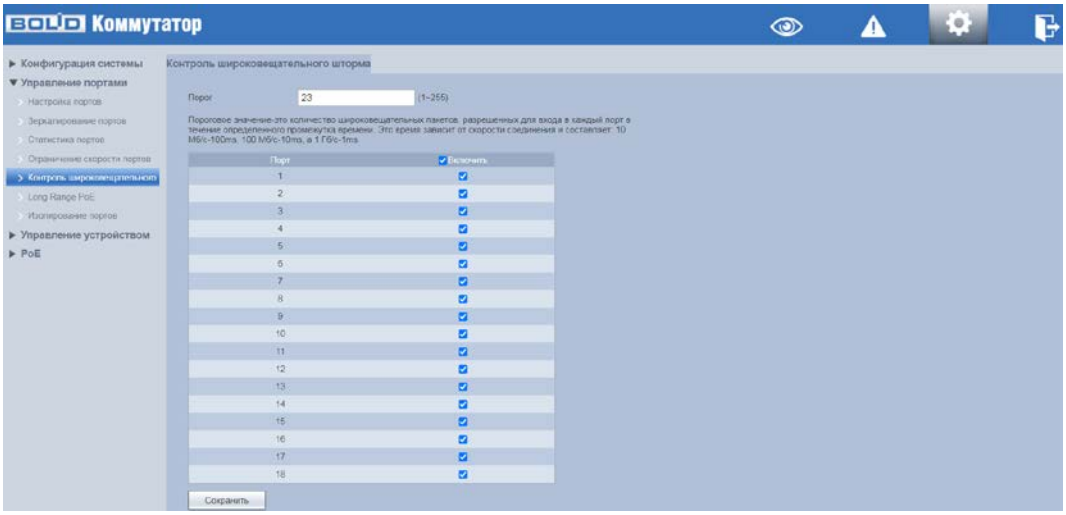

Рисунок 8.16 – Ограничение широковещательных пакетов

8.2.6 Подраздел «Long Range PoE»

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

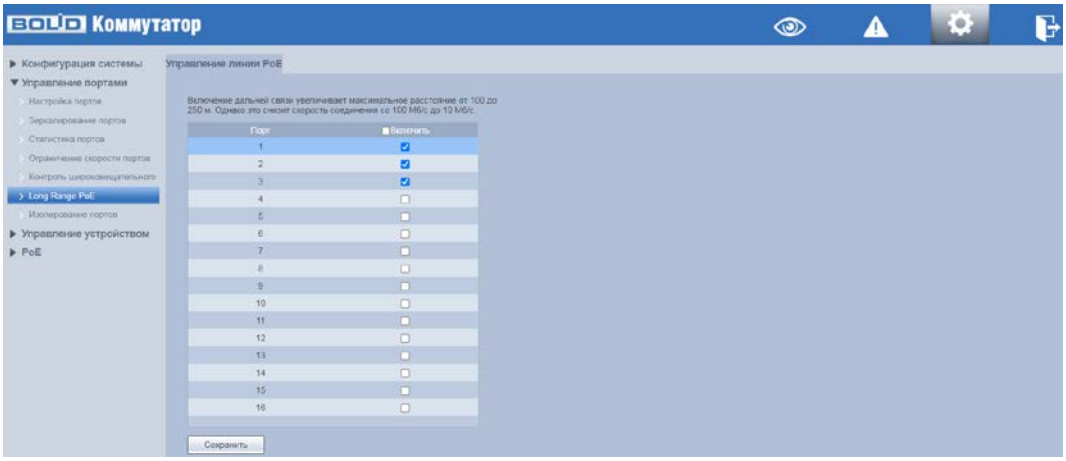

Рисунок 8.17 – Long Distance PoE

8.2.7 Подраздел «Изолирование портов»

ВНИМАНИЕ!
Изоляция портов и VLAN являются взаимоисключающими конфигурациями. При включении изолирования портов, конфигурация VLAN будет автоматически отключена.

Изолирование портов представляет собой функцию, благодаря которой возможно аппаратное изолирование портов коммутатора на втором уровне взаимодействия.

Например, если выделить какое-то количество портов, то трафик с этих устройств будет передаваться через порт, ведущий к серверу, при этом трафик между выбранными изолированными портами передаваться не будет.

Для аппаратной изоляции портов нужно:

1. В строке «Режим» включить и сохранить параметр.

2. Далее выбрать группу портов, которые будут изолированы друг от друга на втором уровне взаимодействия.

3. Сохранить выбранную группу.

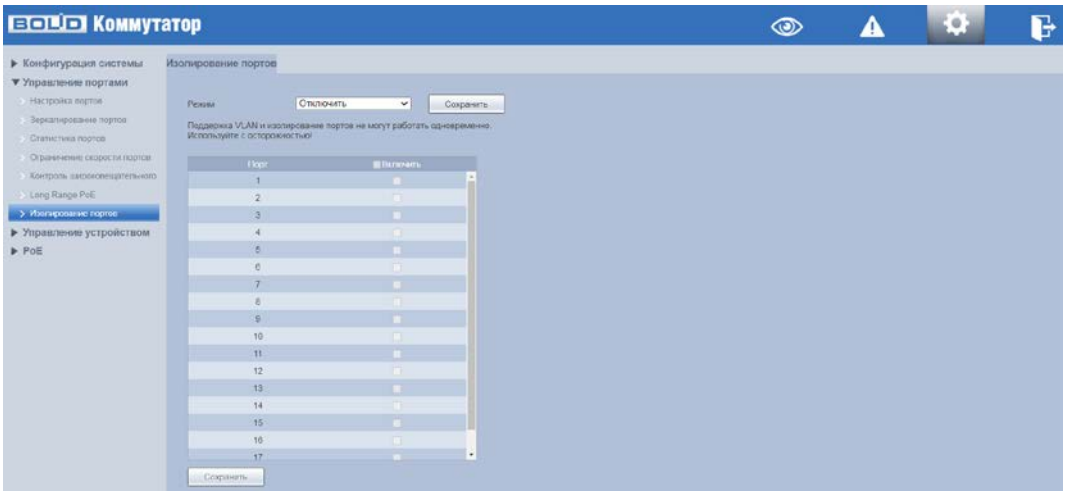

Рисунок 8.18 – Изолирование портов

8.3 Раздел «Управление устройством»

8.3.1 Подраздел «Spanning Tree»

Протокол STP (Spanning Tree Protocol) – это канальный протокол, функционал которого направлен на обеспечение стабильности сети. Например, STP используется для устранения петель в топологии произвольной сети Ethernet или предотвращения широковещательного шторма.

Чтобы предотвратить зацикливания, STP переводит некоторые интерфейсы в состояние пересылки, а другие интерфейсы – в состояние блокировки.

8.3.1.1 **Пункт «Настройки моста STP»**

На рисунке ниже (Рисунок 7.16) изображен интерфейс изменения настроек STP и протокола его работы.

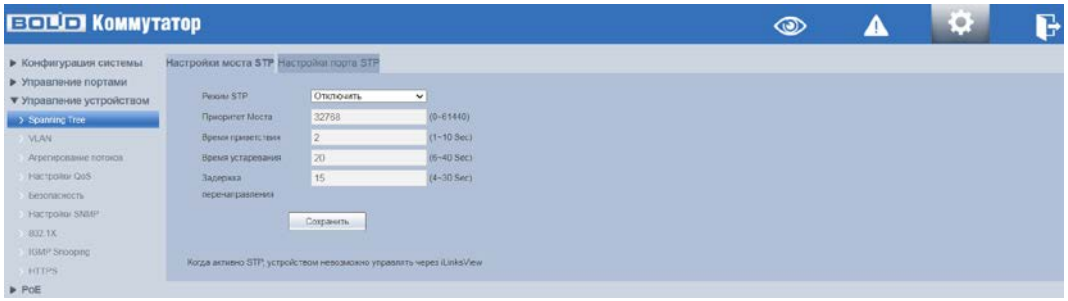

Рисунок 8.19 – Настройка STP

Таблица 8.5 – Параметры настройки STP

Параметр	Функции
Режим STP	Изменение режима работы Spanning Tree. Возможны варианты: отключить, STP, RSTP. Режим STP и функция агрегирования являются взаимоисключающими. После включения агрегации режим STP не может быть включен.
Приоритет моста (ID)	Установите приоритет моста STP, чем меньше значение, тем выше приоритет. 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.
Время приветствия	Задание интервала между передачей корневым устройством сообщений о конфигурации (BPDU фреймов). Параметр в поле устанавливается в диапазоне от 1 до 10 секунд, по умолчанию значение 2.
Время устаревания	Установите время, которое устройство может простаивать, не получая конфигурационного сообщения, прежде чем попытается перенастроиться. Параметры времени устанавливаются от 6 до 40 секунд.
Задержка перенаправления	Установите максимальное время ожидания перед сменой состояний (от приема до передачи). Состояние меняется от 4 до 30 секунд.

8.3.1.2 **Пункт «Настройки порта STP»**

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

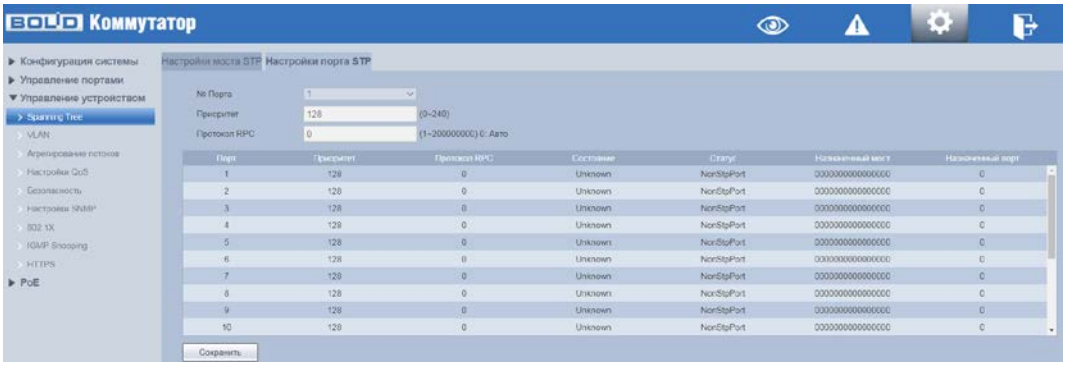

Рисунок 8.20 – Настройка STP

Таблица 8.6 – 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.
Протокол 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.

8.3.2 **Подраздел «VLAN»**

VLAN (Virtual Local Area Network) – логическая виртуальная локальная сеть, используется для создания логической топологии сети, не зависящей от ее физической топологии. Благодаря VLAN группа устройств, имеет возможность взаимодействовать между собой на канальном уровне, хотя физически они будут подключены к разным коммутаторам и наоборот.

8.3.2.1 **Пункт «Список VLAN»**

В данном пункте меню отображена информация о созданных VLAN на коммутаторе. Также именно с этого пункта начинается создание VLAN на устройстве. Добавляется и присваивается VLAN идентификатор, идентификатор состоит из 12 бит и показывает, в каком VLAN находиться кадр (Рисунок 8.21).

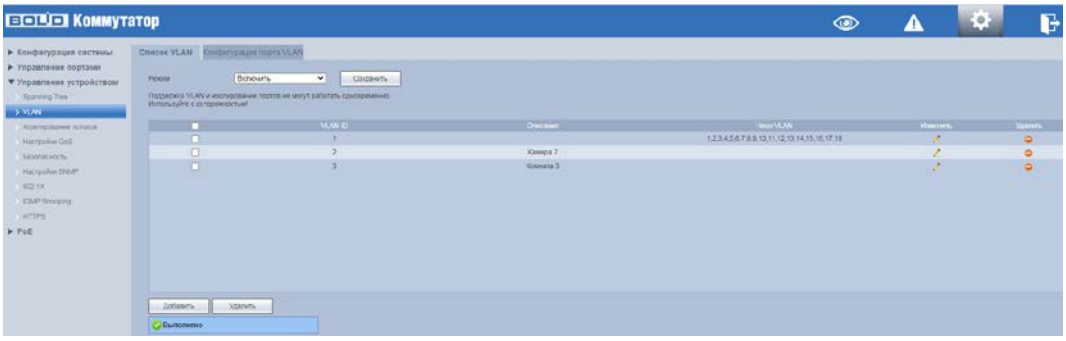

Рисунок 8.21 – Создание VLAN

Для создания VLAN на устройстве нажмите кнопку «Добавить». В появившемся диалоговом окне (Рисунок 8.22) заполните текстовые поля «VLAN ID» и «Описание» (Таблица 8.7), нажмите кнопку «Сохранить». На первом этапе конфигурации VLAN столбец «Член VLAN» будет пуст, для добавления участников VLAN перейдите в пункт «Конфигурация порта VLAN».

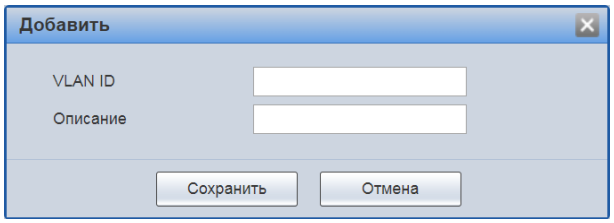

Рисунок 8.22 – Создание VLAN

Таблица 8.7 – Данные списка VLAN

Столбец	Описание
VLAN ID	Уникальный идентификатор VLAN соответствует тегу VLAN, например, введите 1, 2, чтобы создать VLAN 1 и VLAN 2.
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».

8.3.2.2 **Пункт «Конфигурация порта VLAN»**

Данный пункт является вторым шагом конфигурации VLAN. Для нужных портов в текстовом поле столбца «Разрешённые VLAN» добавьте указанный в шаге один «VLAN ID», настройте порт в зависимости от необходимого вам режима работы порта.

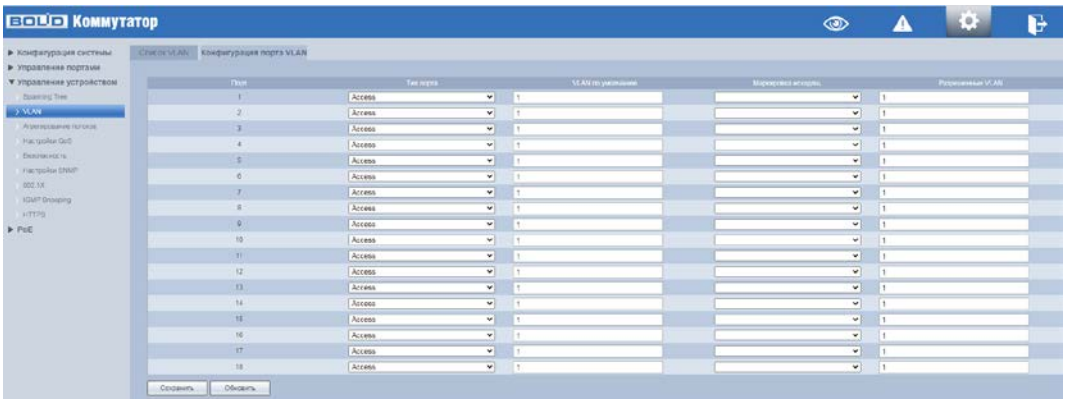

Рисунок 8.23 – Конфигурирование VLAN-порта

Таблица 8.8 – Конфигурирование VLAN-порта

Столбец	Описание
Порт	Столбец отображает физический порт устройства.
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.
VLAN по умолчанию	Задается принадлежность порта к конкретному VLAN. В случае работы порта в режиме Access, поступающий на порт трафик помечается тегом, записанным в данное поле.
Разрешённые VLAN	Перечисление всех разрешённых к прохождению через этот порт VLAN. Остальные VLAN отбрасываются.

Столбец	Описание
Маркировка исходящих	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.

Пример:

Нужно подключить камеру в порт 1. VLAN видеонаблюдения – 4. Порт, куда должны передаваться данные – 16 и этим портом коммутатор подключен к другому коммутатору, поддерживающему 802.1Q.

Для конфигурирования нового VLAN необходимо:

В пункте «Список VLAN» нажать кнопку «Добавить» (Рисунок 8.21). Появится диалоговое окно создания нового VLAN (Рисунок 8.24). Заполните текстовые поля «VLAN ID» и «Описание», нажмите кнопку «Сохранить».

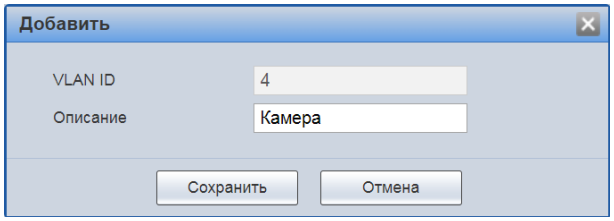

Рисунок 8.24 – Добавить новый VLAN

В пункте «Конфигурирование порта VLAN» (Рисунок 8.25) для нужных портов в поле «Разрешённые VLAN» добавьте указанный в шаге 1 «VLAN ID», настройте порт в зависимости от необходимого вам режима работы порта.

В строке, соответствующую 1 – му порту, нужно:

– Выбрать «Access» в столбце «Тип порта»;

– В текстовом поле «VLAN по умолчанию» вписать – 4;

– В текстовом поле «Разрешённые VLAN» вписать – 4.

В строку, соответствующую 16 – му порту, нужно:

– Выбрать «Trunk» в столбце «Тип порта» (Наиболее вероятно появление и других VLAN на коммутаторе. В этом случае, если все данные будут проходить через 16 – й порт, вариант «Trunk» является оптимальным выбором);

– Текстовое поле «Порт VLAN» менять не требуется (в поле вписано значение 1);

– В столбце «Маркировка исходящ.» выбрать «Untag port VLAN» (В этом случае все разрешённые VLAN будут проходить со своими метками, VLAN с ID 1 будет оставаться без метки);

– В текстовое поле, столбец «Разрешённые VLAN», вписать 4 или дописать через запятую к списку уже имеющихся в поле значений;

– Нажать кнопку «Сохранить».

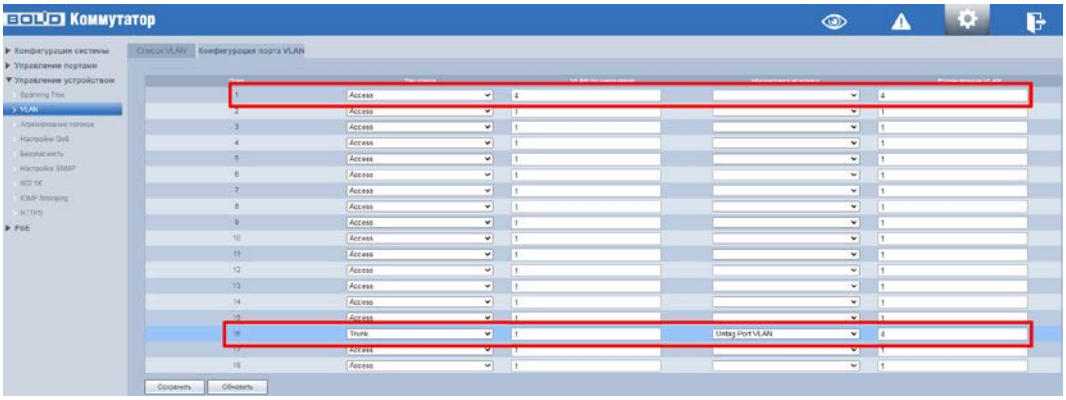

Рисунок 8.25 – Конфигурирование VLAN-порта

8.3.3 Подраздел «Агрегирование потоков»

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 создается 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 802.1x, 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

8.3.3.1 **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 8.9).

Таблица 8.9 – Типы алгоритма балансировки нагрузки

Режим балансировки	Описание
Источник MAC	Балансировка нагрузка, осуществляемая на основе поля MAC-адреса источника.
MAC назначения	Балансировка нагрузка, осуществляемая на основе поля MAC-адреса назначения.
MAC источник и назнач-я	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.

8.3.3.2 **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 операции – 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.

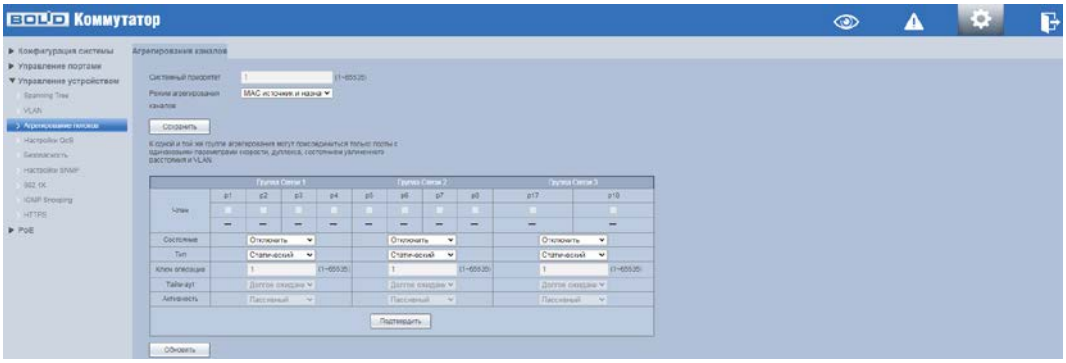

Рисунок 8.26 – Интерфейс настройки агрегации ссылок

8.3.4 Подраздел «Настройки QoS»

QoS (Quality of Service/Качество обслуживания) – это общее название технологий приоритизации трафика для улучшения качества тех или иных услуг в условиях высокой нагруженности сети. При работе данной функции используется алгоритм изменения порядка расположения кадров в очередях (приоритизация).

Приоритизация происходит с помощью разделения трафика на классы и предоставления классам различных приоритетов в обслуживании, с помощью этого обеспечивается своевременная доставка чувствительного к временным задержкам трафика.

Т.е. трафик с большим приоритетом, например, RTSP поток, будет передаваться в первую очередь с минимальными задержками. Трафик с низким приоритетом, например, содержимое веб-интерфейса, будет помещен в очередь с более низким приоритетом, где допускаются временные задержки и могут быть при необходимости отброшены.

8.3.4.1 **Пункт «Режим приоритета»**

В пункте «Режим приоритета» устанавливается класс обслуживания. Под классом обслуживания подразумевается выбор механизма работы коммутатора для управления пропускной способностью сети при возникновении перегрузок.

Благодаря выбранному механизму будет определяться порядок передачи пакетов через выходной интерфейс на основе их приоритетов. Для данной модели доступен выбор из трех механизмов:

– Первый вошел, первый вышел (FIFO (first in – first out)) – механизм FIFO при своей работе не выполняет классификацию, пакеты помещаются в одну очередь и распознаются с одной приоритетностью, т.е пакеты обрабатываются в той очередности в которой и поступили. QoS не работает;

– Всё большое перед малым (приоритет в порядке двух очередей) – поступающие пакеты помещаются в две очереди «Высокоприоритетные» и «Низкоприоритетные». При этом пакеты из низкоприоритетной очереди не начнут передаваться, пока передаются пакеты из высокоприоритетной очереди. При работе такого механизма есть вероятность, что пакеты из низкоприоритетной группы долгое время не будут обрабатываться;

– Round-Robin (приоритет распределяется циклически) – механизм при работе обеспечивает циклическую обработку очередей в соответствии с назначенным им весом и предоставляя полосу пропускания для пакетов низкоприоритетных очередей. Также каждая очередь имеет собственное время обработки, время обработки с наивысшим приоритетом больше, чем у последующих очередей.

Рисунок 8.27 – Приоритетный режим

8.3.4.2 **Пункт «На основе DSCP/порт/802.1p»**

Класс приоритетности выставляется в заголовке пакета. Для классификации трафика используются стандартные поля в заголовках. Устройство анализирует и распределяет пакет в очередь в соответствии с присвоенным цифровым приоритетом.

Для обеспечения QoS на L2 уровне коммутатор поддерживает IEEE 802.1p. Спецификация IEEE 802.1p позволяет задать до 8 уровней приоритетов (от 0 до 7), определяющих способ обработки кадра. Приоритет устанавливается в поле CoS (Class of Service), поле состоит из 3 бит в теге 802.1Q Ethernet-кадра.

Структура Ethernet кадра. Тег 802.1p внутри тега 802.1Q:

Адрес назначения	Адрес источника	802/1Q Тег		Длина/ Тип	Данные	Контрольная последовательность кадра
		TPID	TCI			
6 байт	6 байт	4 байта		2 байта	46 – 1500 байт	4 байта

TPID – идентификатор тега. По умолчанию 0x8100.	Информация об управлении метками (TCI)		
	Priority – уровень приоритета 802.1p (от 0 до 7)	CFI – индикатор канонического формата.	VID – идентификатор VLAN, значения от 0 до 4095
16 бит	3 бита	1 бит	12 бит

Таблица 8.10 – Восемь классов приоритета трафика (стандарт IEEE 802.1p)

Класс приоритета	**Уровень приоритета 802.1p (десятичная система)**	**Уровень приоритета 802.1p (двоичная система)**	**Уровень обслуживания. Тип трафика**
Очередь с низким приоритетом	0	000	Best Effort. Качество передачи не гарантировано, но поддерживается на лучшем уровне из возможного.
	1	001	Background. Фоновый трафик.
	2	010	Standard (spare). Стандартный трафик.
	3	011	Excellent Effort (business critical). Приоритетный трафик. Не критичные к задержке, но критичные к потерям данные. Менее приоритетные, чем контролируемый трафик.
Очередь с высоким приоритетом	4	100	Controlled Load (streaming multimedia). Контролируемый трафик. Критичный к потерям, но не критичный к задержке. Мультимедийные потоки.
	5	101	Video. Видеопотоки. Критичной является задержка свыше 100 мс.
	6	110	Voice. Голосовой трафик. Критичной является задержка свыше 10 мс.
	7	111	Network Control Reserved traffic. Данные управления сетью.

В данном пункте включение параметра означает его приоритетность на порту перед другими (Рисунок 8.28).

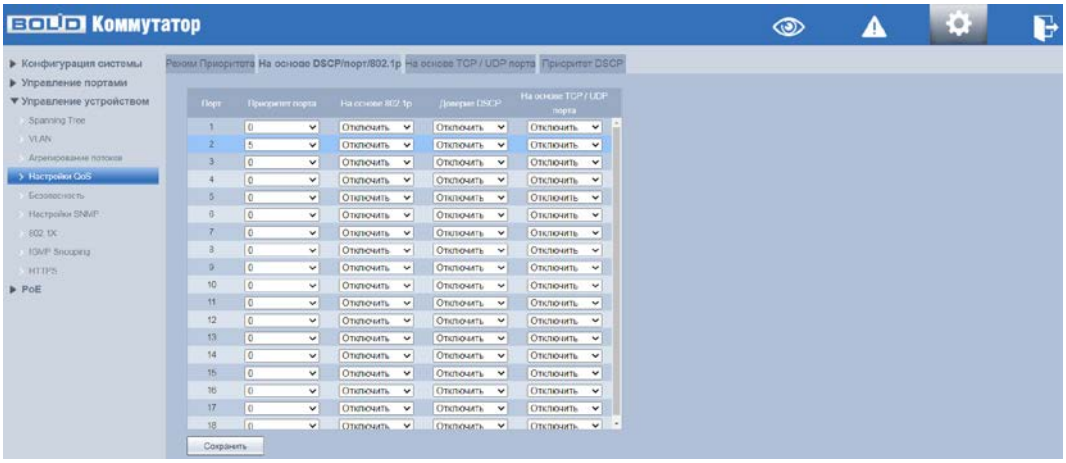

Рисунок 8.28 – Интерфейс настройки Port/802.1p/DSCP Based

8.3.4.3 **Пункт «На основе TCP/UDP порта»**

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 8.29) виден список протоколов, такие как FTP, SSH, TELNET, SMTP и DNS и т.д.. Установите приоритет для порта из списка, в соответствии с требованиями к настраиваемой сети, возможные значения: Q4 ~ Q7 – высокий приоритет, Q0 ~ Q3 – низкий приоритет или discard – отбрасывать.

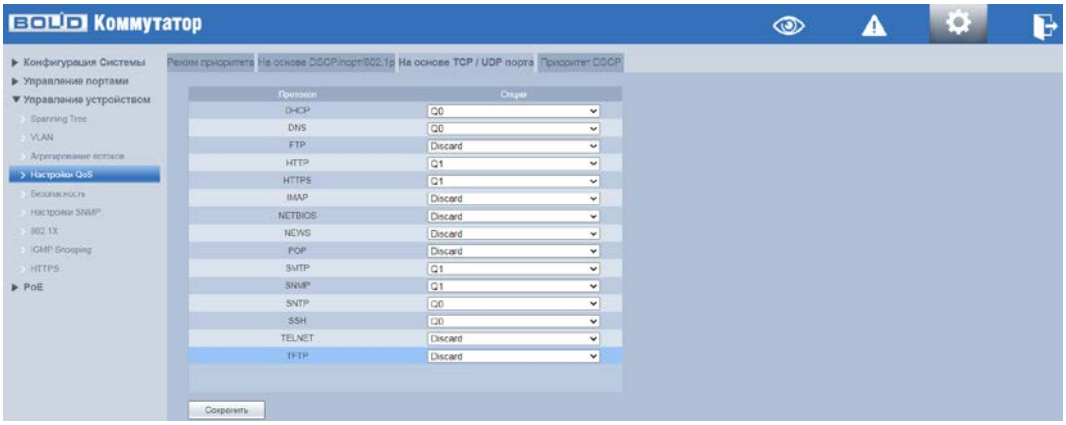

Рисунок 8.29 – Приоритет на основе TCP/UDP порта

8.3.4.4 **Пункт «Приоритет DSCP»**

Для обеспечения QoS на L3 уровне коммутатор поддерживает вид приоритизации, при котором в заголовок IP добавляется специальный байт ToS – Type of Service.

Этот байт может быть заполнен либо значением приоритета IP Precedence, либо значением DSCP (Differentiated Services Code Point) .

Для обеспечения QoS приоритет устанавливается в поле DSCP (Differentiated Services Code Point), поле занимает 6 бит в IP пакете и имеет приоритетность 0 до 63.

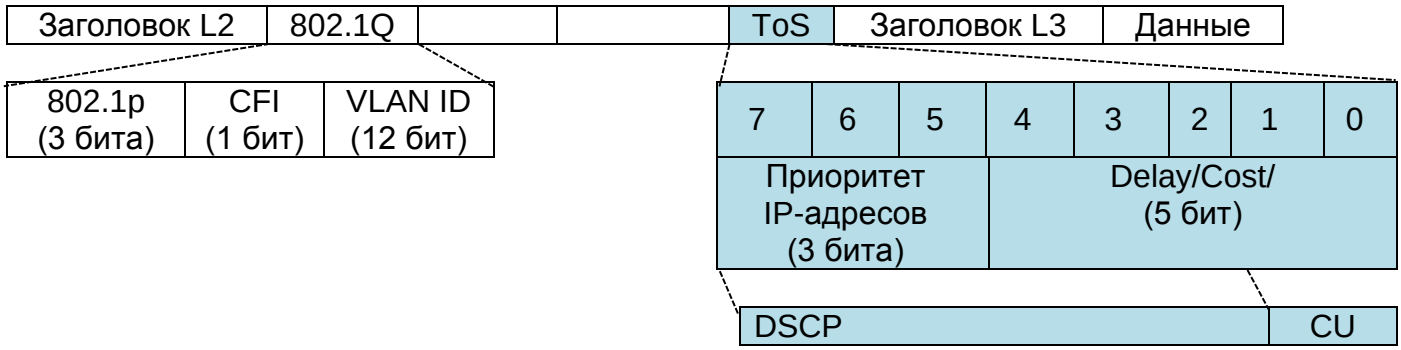

Таблица 8.11 – Привязка по умолчанию DSCP к CoS (приоритетам 802.1p)

Внутренний приоритет	0	1	2	3	4	5	6	7
DSCP	0 – 7	8 – 15	16 – 23	24 – 31	32 – 39	40 – 47	48 – 55	56 – 63
CoS	0	1	2	3	4	5	6	7

В зависимости от задачи переназначьте приоритеты QoS для DSCP (Differentiated Services Code Point).

1. Выберите из выпадающего списка в строке «Не совпадает приоритет» параметр: низкий приоритет (приоритет 0) или приоритизация по тегу/порту.

2. Установите в столбце «Значение» привязки DSCP к CoS (приоритетам 802.1p). Значения должны принадлежать 6-битному диапазону 0…63 (Таблица 8.11).

3. В столбце «Приоритет» выберите класс приоритета (от 0 до 7).

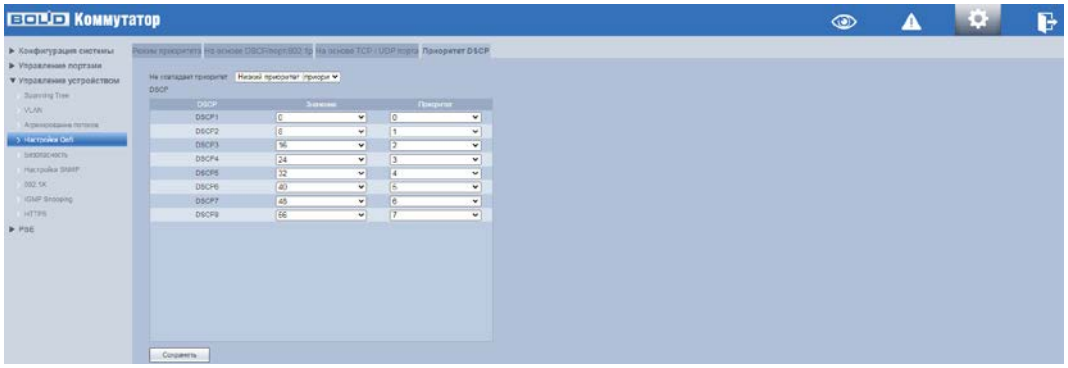

Рисунок 8.30 – Приоритезация по DSCP

8.3.5 Подраздел «Безопасность»

8.3.5.1 Пункт «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 8.31).

Рисунок 8.31 – MAC информация об адресах

8.3.5.2 Пункт «Привязка MAC-порт»

На рисунке ниже (Рисунок 8.32) изображен 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, с камеры.

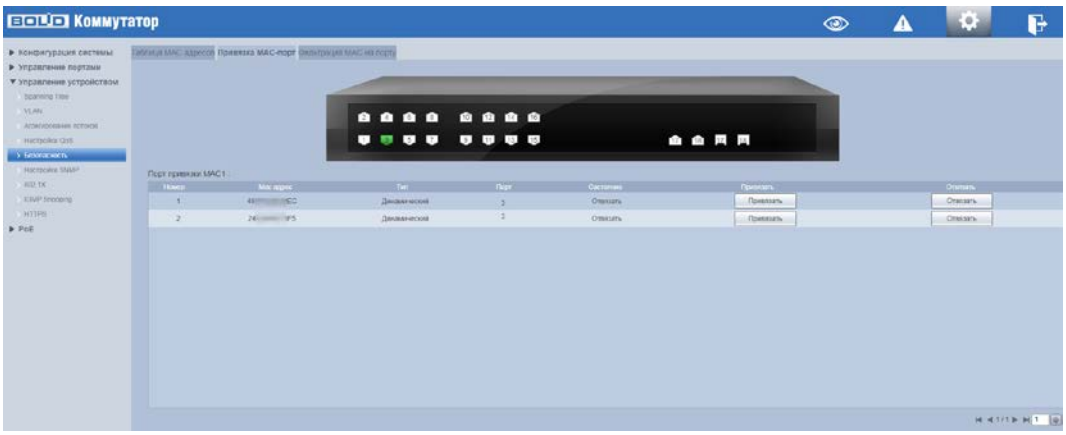

Рисунок 8.32 – Привязка MAC-адреса

8.3.5.3 **Пункт «Фильтрация MAC на порту»**

Функция используется для ограничения поступающих пакетов при помощи настройки белого списка MAC-адресов (Рисунок 8.34). Для настройки функции:

1. Нажмите кнопку «Добавить» и введите в текстовое поле диалогового окна «белый» MAC-адрес.

2. Сохраните настройку.

3. Для просмотра информации, нажмите на порт устройства и в списке «Порт MAC фильтрации: номер пота» будут отображены входящие пакеты.

Рисунок 8.33 – Фильтрация портов

8.3.6 Подраздел «Настройки 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.

На рисунке (Рисунок 8.34) 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.

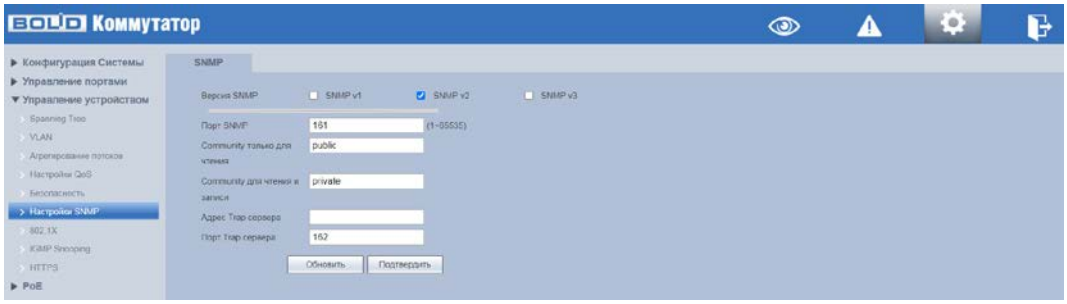

Рисунок 8.34 – Настройки SNMP

На рисунке (Рисунок 8.35) изображен интерфейс настроек SNMP версии 3.

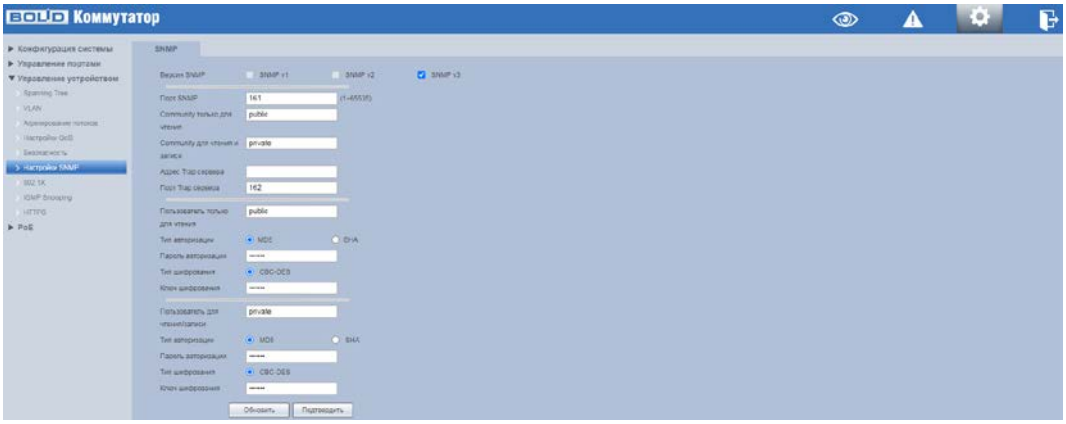

Рисунок 8.35 – Настройки SNMPv3

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

Таблица 8.12 – Поля настроек

Название	Описание
Версия SNMP	SNMP v1 – устройство выполняет только процессы версии v1 SNMP. (SNMPv1 – изначальная реализация протокола SNMP, работает с такими протоколами, как UDP, IP, CLNS, DDP и IPX); SNMP v2 – устройство выполняет только процессы версии v2 SNMP. (SNMPv2 пересматривает версию 1 и включает в себя улучшения в области производительности, безопасности, конфиденциальности и связях между сетевыми менеджерами, служит для получения большого количества управляющих данных через один запрос. Версии SNMP v1 и v2 совместимы для одновременного применения); SNMP v3 – устройство выполняет только процессы версии v3 SNMP, необходимы логин и пароль для работы. (Версии SNMP v1 и v2 одновременно с SNMP v3 не применяются. SNMP v3 приносит изменения в протокол добавлением криптографической защиты, является улучшением за счет новых текстовых соглашений, концепций и терминологии SNMP).
Порт SNMP	Порт прослушивания прокси – программы устройства. Это UDP – порт не является портом TCP. Значение варьируется от 1 до 65535. Значение по умолчанию – 161.
Community только для чтения	Доступ SNMP только для чтения: поддерживается для всех целей SNMP.

Название	Описание
Community для чтения и записи	Доступ SNMP для чтения и записи: поддерживается для всех целей SNMP.
Адрес Trap сервера	Адрес системы мониторинга сети или ПК с предустановленным специализированным программным средством мониторинга. Служит для самостоятельной отправки видеорегистратором информации о событиях по протоколу SNMP.
Порт Trap сервера	Порт системы мониторинга сети или ПК с предустановленным специализированным программным средством мониторинга для захвата пакетов по SNMP протоколу. Значения параметра в диапазоне от 1 до 65535, с шагом 1. Значение по умолчанию: 162.
Пользователь только для чтения	Вводится имя пользователя с правами только на чтение.
Пользователь для чтения/записи	Вводится имя пользователя с правами на чтение и запись.
Тип авторизации	Выберите метод хэширования MD5 или SHA. Система автоматически распознает метод.
Пароль авторизации	Введите пароль для аутентификации. Пароль должен содержать не менее восьми символов
Тип шифрования	Выберите алгоритм симметричного шифрования CBC или DES.
Ключ шифрования	Введите пароль шифрования.

8.3.7 Подраздел «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.

8.3.7.1 **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 8.36 – 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.

8.3.7.2 **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.

8.3.7.3 **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.

8.3.7.4 **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 пройдет 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 8.37).

2. Настройте адрес сервера аутентификации, как показано на рисунке (см. Рисунок 8.38).

8.3.7.5 **Пункт «Настройки безопасного доступа к сети (NSA)»**

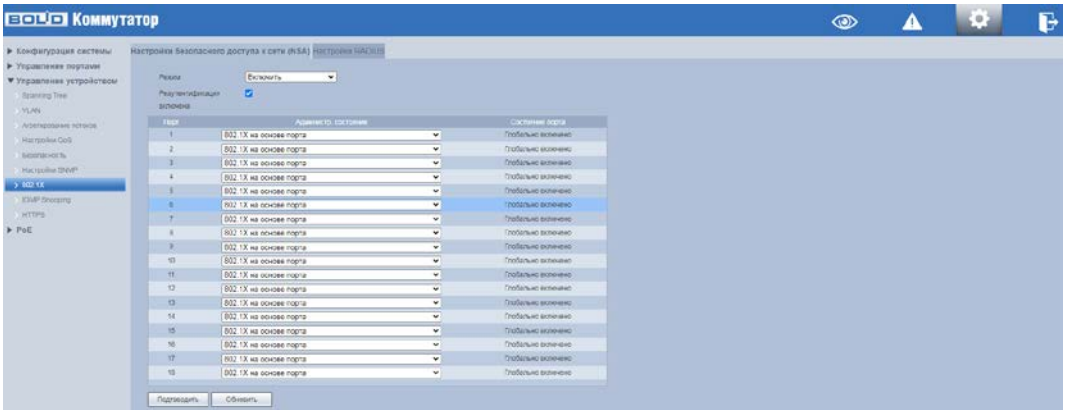

Рисунок 8.37 – Настройки NSA

8.3.7.6 **Пункт «Настройки RADIUS»**

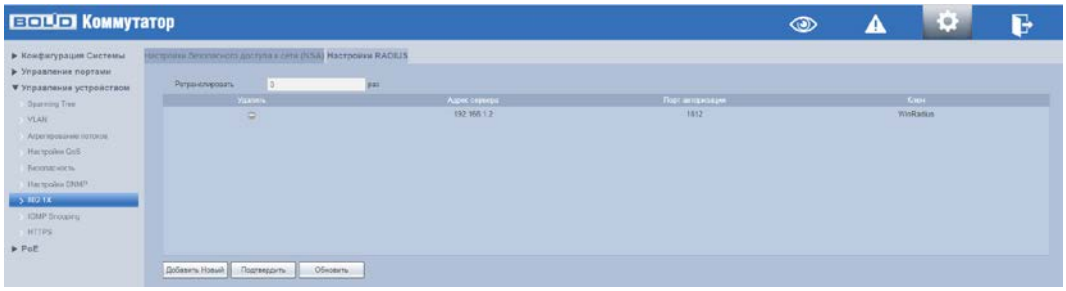

Рисунок 8.38 – Настройки Radius

8.3.8 **Подраздел «IGMP Snooping»**

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

– 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 подключен, в список ее 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. Ее включение обязательно при наличии каких-либо многоадресных рассылок любого типа.

На рисунке (Рисунок 8.39) представлен интерфейс настроек в состоянии по умолчанию. При использовании Multicast рассылки, возможно, включить поддержку «Отображение неизвестных многоадресных пакетов (Fast leave)», которая позволяет коммутатору быстрее исключать порт из списка участников соответствующей группы. Для целей видеонаблюдения ее включение не обязательно.

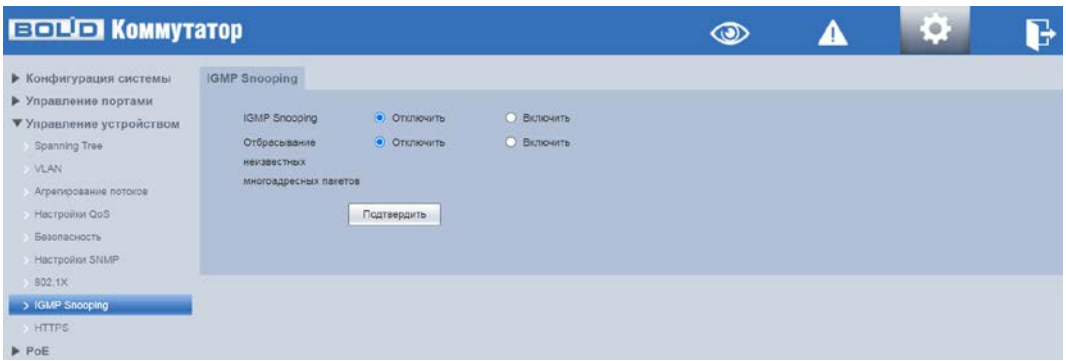

Рисунок 8.39 – Интерфейс IGMP Snooping

8.3.9 Подраздел «HTTPS»

ВНИМАНИЕ!
Перед включением HTTPS и созданием сертификата убедитесь, что текущее время и часовой пояс установлены правильно.

Подраздел HTTPS поддерживает просмотр и управление параметрами повышения безопасности сетевой работы с использованием сетевых сертификатов.

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.

Для создания сертификата в данном подразделе сначала нужно включить HTTPS. Для этого перейдите в пункт «HTTPS». Далее перейдите в пункт «Управление сертификатами». В данном пункте можно создать новый сертификат и после заполнения соответствующих полей скачать сгенерированный сертификат.

📖 При первой настройке HTTPS или изменении IP-адреса коммутатора необходимо заново создать сертификат сервера;

📖 Если вы впервые используете HTTPS после замены компьютера, необходимо загрузить корневой сертификат заново.

8.3.9.1 Пункт «HTTPS»

Для создания сертификата, который используется для шифрования данных и идентификации сайта при установлении защищенного соединения, включите HTTPS. Подтвердите включения и дождитесь перезагрузки. Далее перейдите в пункт «Управление сертификатами».

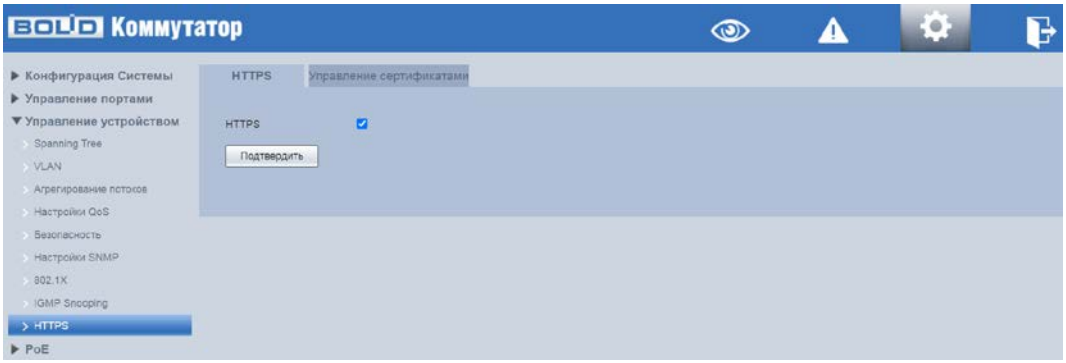

Рисунок 8.40 – Включение протокола HTTPS

8.3.9.2 **Пункт «Управление сертификатами»**

Для создания сертификата открытого ключа нажмите кнопку «Создать». В появившемся окне заполните соответствующие поля и нажмите кнопку «Создать» (Рисунок 8.42).

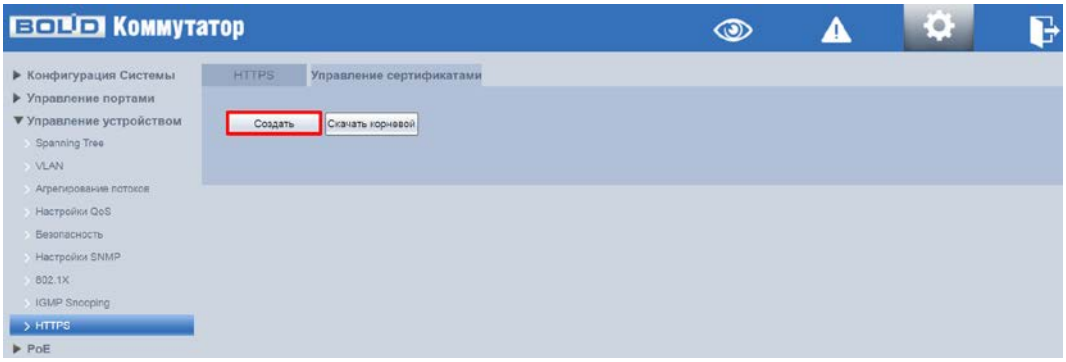

Рисунок 8.41 – Пункт меню «Управление сертификатами»

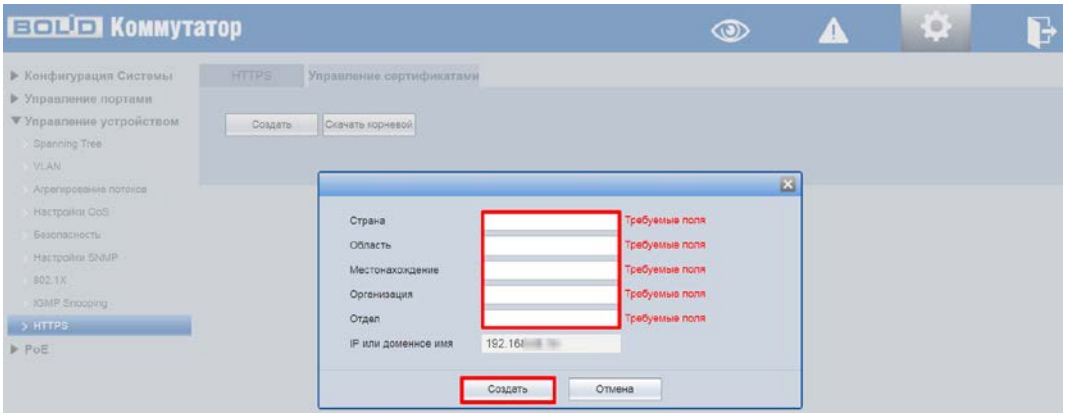

Рисунок 8.42 – Создание сертификата

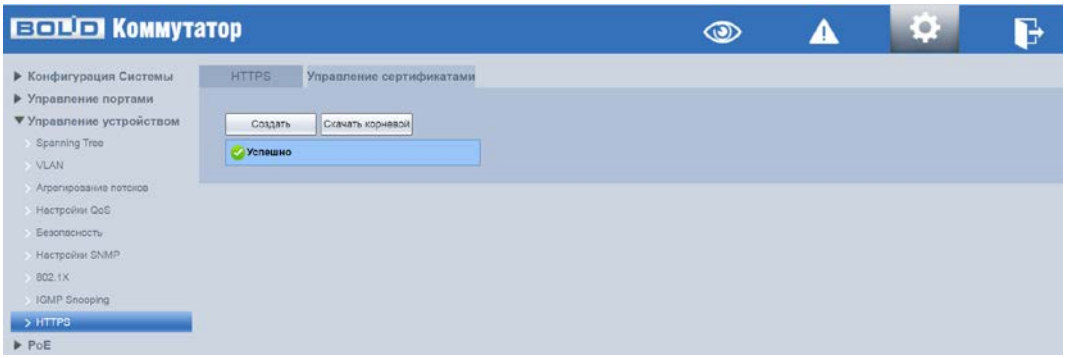

Рисунок 8.43 – Создание сертификата

На данный момент времени, созданный сертификат с открытым ключом не является доверенным (Рисунок 8.44), инициализируйте HTTPS-соединение вручную. Для этого нажмите кнопку «Скачать корневой сертификат».

Перейдите в загрузки и откройте скачанный корневой сертификат (Рисунок 8.45)

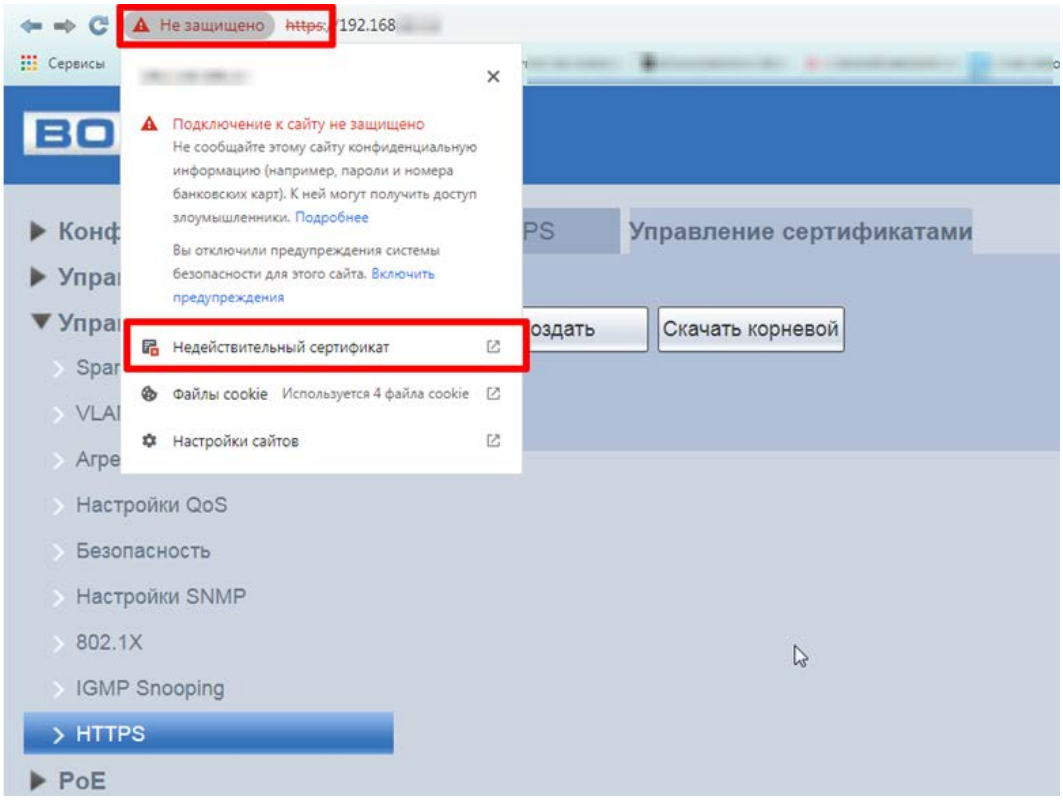

Рисунок 8.44 – Активация

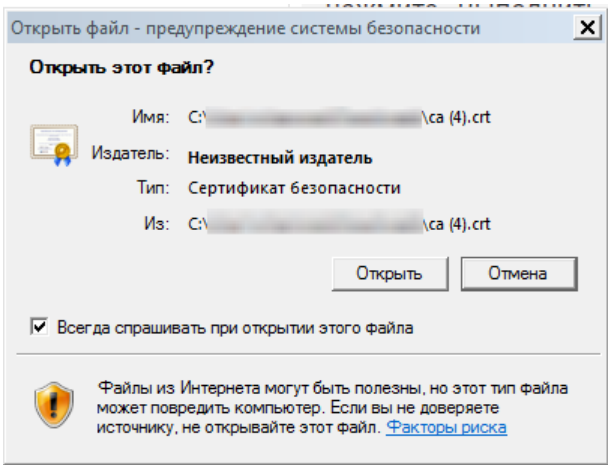

Рисунок 8.45 – Установка

Нажмите кнопку «Установить сертификат…» (Рисунок 8.46).

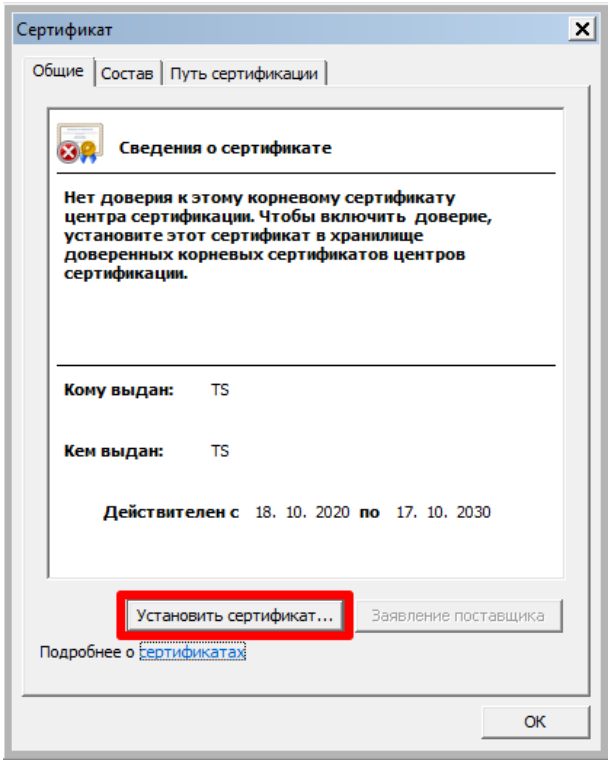

Рисунок 8.46 – Установка

Нажмите кнопку «Далее» (Рисунок 8.47).

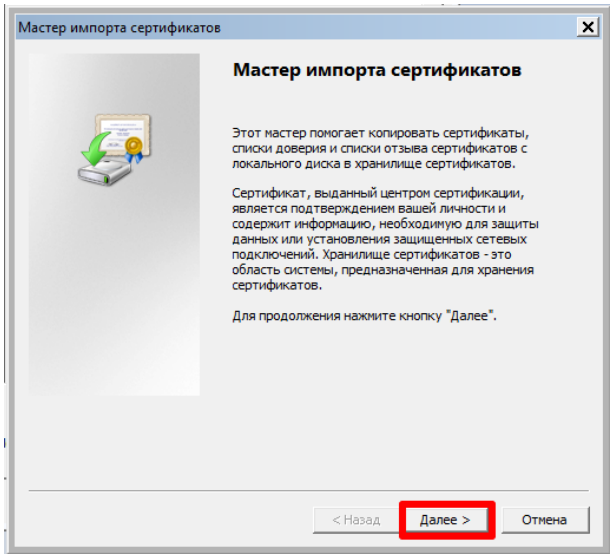

Рисунок 8.47 – Установка

Поставьте флажок «Поместить все сертификаты в следующее хранилище».

Нажмите кнопку «Обзор» и выберите хранилище сертификата «Доверенные корневые центры сертификации». Нажмите «ОК» и «Далее» (Рисунок 8.48).

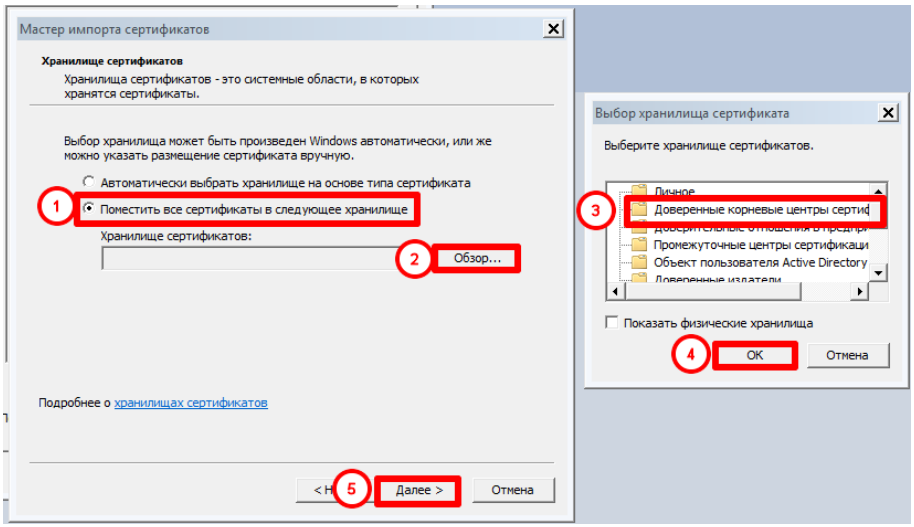

Рисунок 8.48 – Установка

Нажмите кнопку «Готово» (Рисунок 8.49).

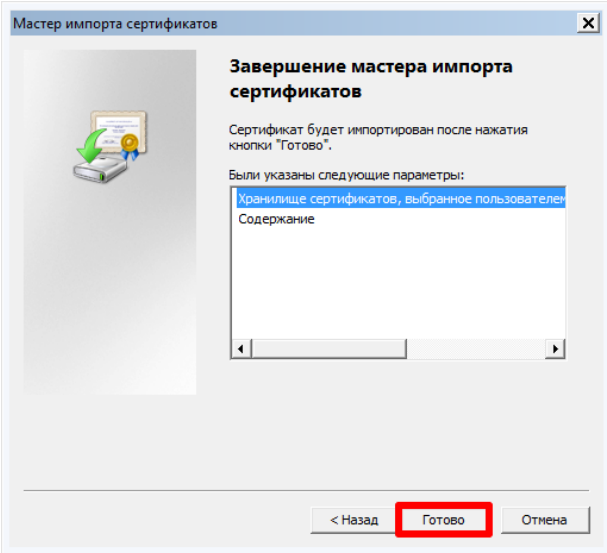

Рисунок 8.49 – Установка

Подтвердите (Рисунок 8.50).

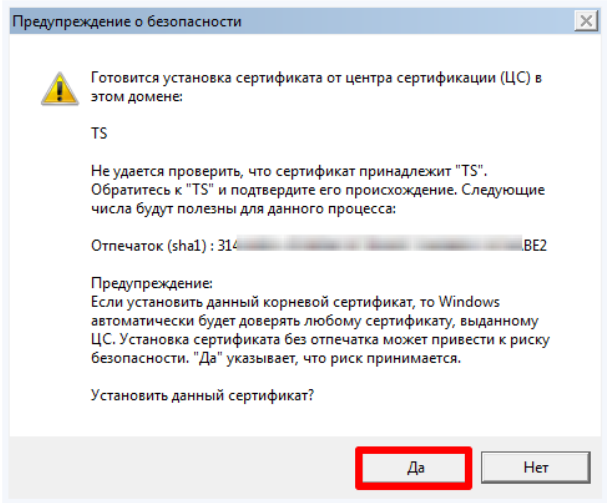

Рисунок 8.50 – Установка

Нажмите кнопку «ОК» (Рисунок 8.51).

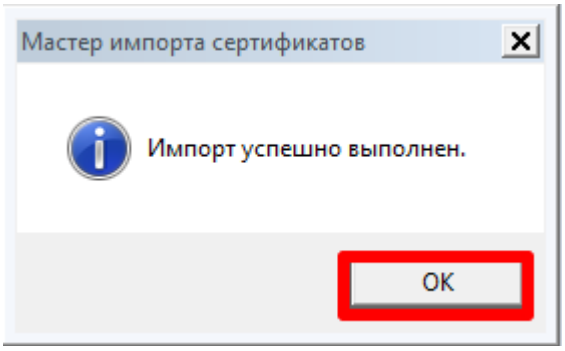

Рисунок 8.51 – Установка

Перезагрузите устройство. На рисунке ниже (Рисунок 8.52) видим, что статус сертификата изменился на доверенный и HTTPS-соединение прекратило нести угрозу. На этом работа с сертификатом на устройстве окончена.

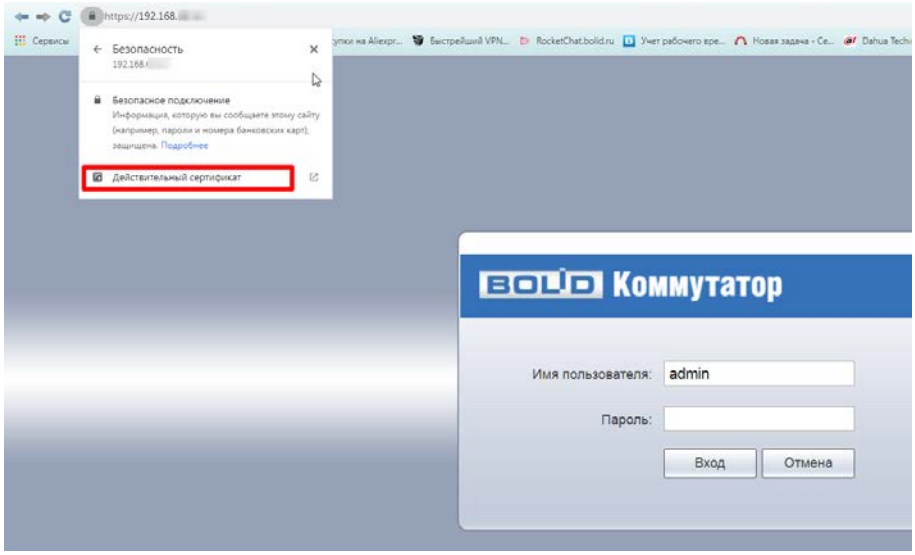

Рисунок 8.52 – Установка

8.4 Раздел «PoE»

8.4.1 Подраздел «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.

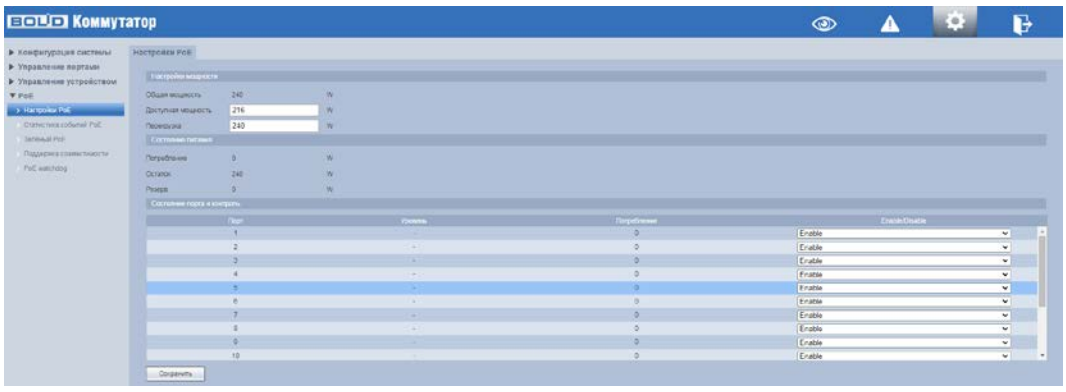

Рисунок 8.53 – Питания порта по PoE

Таблица 8.13 – Параметры настройки

Параметр		Функция
Настройки мощности	Общая мощность	Предельная мощность устройства.
	Доступная мощность	Настраиваемая доступная мощность PoE.
	Перезагрузка	Настраиваемая мощность PoE при перегрузке.
Состояние питания	Потребление	Отображает текущую потребляемую мощность.
	Остаток	Отображает текущую остаточную мощность.
	Резерв	Непригодное для использования питание по PoE. Зарезервированная мощность = общая мощность при перегрузке.
Состояние порта и контроль	Уровень	Подача питания на устройство, подключенное к порту. Уровень подачи питания колеблется от 0 до 8, при Hi-PoE отображается как 5+.
	Потребление	Отображает текущую мощность PoE, потребляемую соответствующим отдельным портом.
	Enable/Disable	Включение или выключение PoE на выбранном порту.

8.4.2 Подраздел «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.

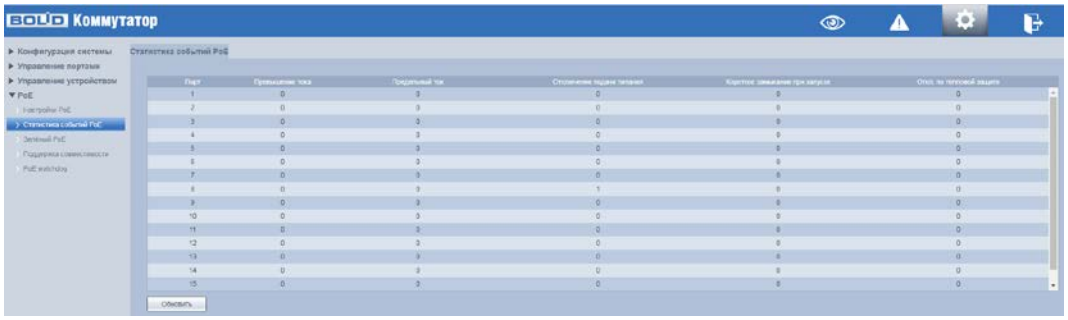

Рисунок 8.54 – Статистика событий PoE

8.4.3 Подраздел «Зеленый 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.

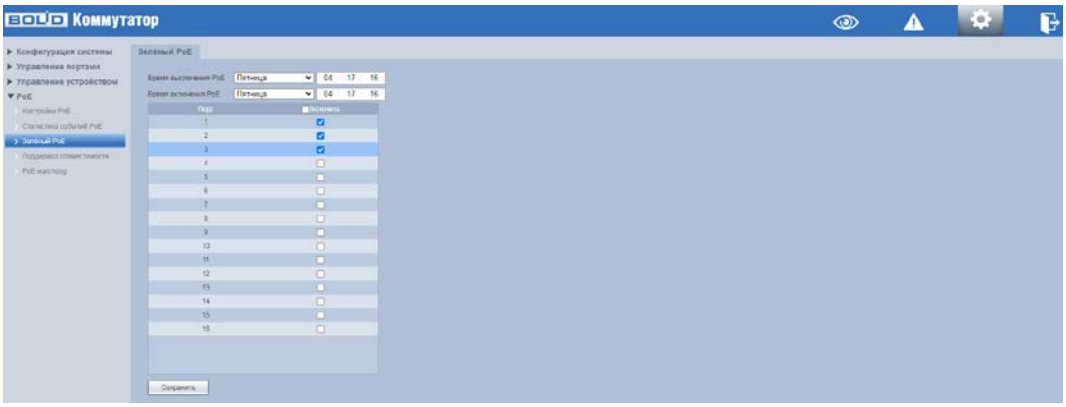

Рисунок 8.55 – Параметры энергосбережения PoE

8.4.4 Подраздел «Поддержка совместимости»

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

Рисунок 8.56 – Поддержка устаревших устройств

8.4.5 Подраздел «PoE watchdog»

ВНИМАНИЕ!
Возможно, одновременно включить либо «PoE watchdog», либо непрерывную подачу электропитания (см. Подраздел «Поддержка совместимости»).

В данном подразделе выполняется настройка автоматического контроля сбоев на устройствах подключенных к PoE портам коммутатора. При обнаружении сбоя устройство перезапускает сетевую связь на порту.

Технология «PoE watchdog» облегчает обслуживание подключенных устройств и позволяет совершать перезапуск без вмешательства обслуживающего персонала.

Для настройки выберите порт из списка, выделите его флажком и сохраните настройку.

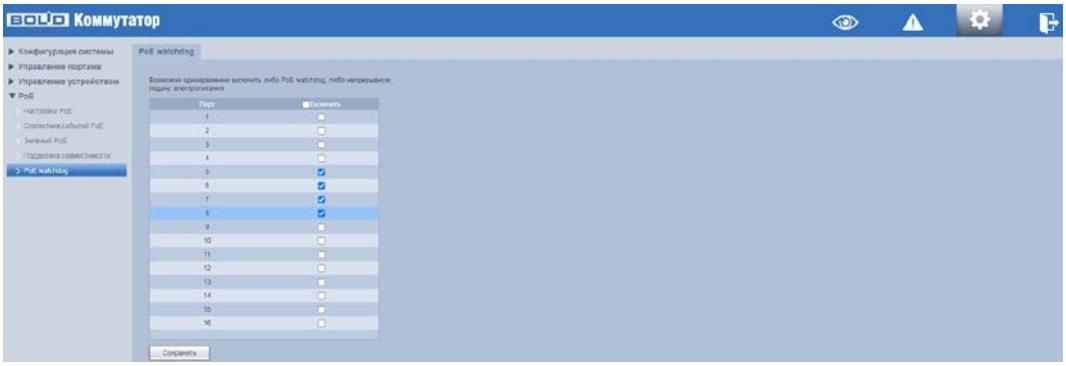

Рисунок 8.57 – PoE watchdog

9 РАБОТА С УТИЛИТОЙ «BOLID VIDEOSCAN»

В случае отсутствия возможности доступа к изделию через веб-интерфейс, а также, если текущий IP-адрес устройства неизвестен, 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 нажмите кнопку «Сохранить». На рисунке (Рисунок 8.1) представлены базовые параметры для изменения.

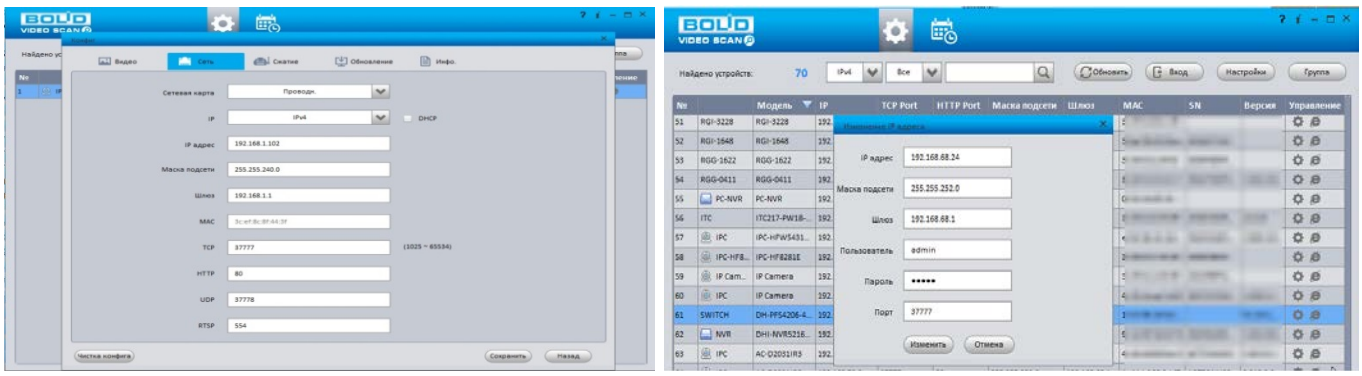

Рисунок 9.1 – Работа с BOLID VideoScan

10 ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ И ПРОВЕРКА РАБОТОСПОСОБНОСТИ

Техническое обслуживание коммутатора должно производиться лицами, имеющими квалификационную группу по электробезопасности не ниже второй. Ежегодные и ежемесячные работы по техническому обслуживанию проводятся согласно принятых и действующих в организации пользователя регламентов и норм (при отсутствии в организации пользователя действующих регламентов и норм для работ технического обслуживания, необходимо привлечь необходимые для этого организацию и специалистов, имеющих право, квалификацию и условия для этого), и в том числе могут включать:

– Проверку работоспособности изделия, согласно руководству по эксплуатации;

– Проверку целостности корпуса, целостность изоляции кабеля, надежности 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.

11 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;
E-mail: support@bolid.ru.

Перечень неисправностей и способы их устранения представлены в таблице ниже (Таблица 10.1).

Таблица 11.1 – Перечень возможных неисправностей

Внешнее проявление неисправности	**Возможные причины неисправности**	**Способы и последовательность определения неисправности**
Отсутствует свечение всех индикаторов	Нет питания.	Проверьте кабель питания на частичный обрыв.
Отсутствует свечение индикатора питания	Кабель питания неправильно подключен к коммутатору.	
	Источник питания не отвечает требованиям входного напряжения устройства.	
Порт не устанавливает соединение, свечение индикатора не присутствует	Частичный обрыв кабеля	Проверьте кабель соединения на частичный обрыв.
	Неисправность камеры	Убедитесь в исправности камеры.
	Превышение длины кабеля	Длина кабеля не должна превышать 100 метров для медных линий.

12 РЕМОНТ

При выявлении неисправного изделия его нужно направить в ремонт по адресу предприятия-изготовителя. Отправка изделия для проведения текущего ремонта оформляется в соответствии с СТО СМК 8.5.3-2015, размещенном на нашем сайте https://bolid.ru/support/remont/.

При направлении изделия в ремонт к нему обязательно должен быть приложен акт с описанием возможной неисправности, с описанием: возможной неисправности, сетевой настройки устройства (IP-адрес, маска подсети, шлюз), примененные логин и пароль.

Рекламации направлять по адресу:

ЗАО НВП «Болид», 141070, Московская область, г. Королёв, ул. Пионерская, д. 4.

При затруднениях, возникших при эксплуатации изделия, рекомендуется обращаться в техническую поддержку по телефону +7 (495) 775-71-55 или по электронной почте support@bolid.ru.

13 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.

14 УПАКОВКА

Изделие и эксплуатационная документация упакованы в картонную коробку.

15 ХРАНЕНИЕ

Хранение изделия в потребительской таре допускается только в отапливаемых помещениях при температуре от плюс 5 °С до плюс 40 °С и относительной влажности до 80 % при температуре плюс 20 °С.

Хранение изделия в упаковке предприятия-изготовителя допускается при температуре окружающего воздуха от минус 50 °С до плюс 50 °С и относительной влажности до 95 % при температуре плюс 35 °С.

В помещениях для хранения не должно быть паров кислот, щелочей, агрессивных газов и других вредных примесей, вызывающих коррозию.

16 ТРАНСПОРТИРОВКА

Изделие необходимо транспортировать только в упакованном виде: в неповреждённой заводской упаковке или в специально приобретённой потребителем транспортной упаковке, обеспечивающей сохранность изделия при перевозке. Транспортирование упакованных изделий производится при температуре окружающего воздуха от минус 50 °С до плюс 50 °С и относительной влажности до 95 % при температуре плюс 35 °С любым видом крытых транспортных средств, не допуская разрушения изделия и изменения его внешнего вида. При транспортировании изделие должно оберегаться от ударов, толчков, воздействия влаги и агрессивных паров и газов, вызывающих коррозию.

17 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 (п. 1.2 ГОСТ 2.608-78).

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

18 ГАРАНТИИ ИЗГОТОВИТЕЛЯ

Гарантийный срок эксплуатации – 36 месяцев с даты приобретения.

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

19 СВЕДЕНИЯ О СЕРТИФИКАЦИИ

Изделие соответствует требованиям технического регламента ТР ТС 020/2011, ТР ТС 004/2011. Имеет декларацию о соответствии N RU Д-RU.PA02.B.95113/21.

Изделие соответствует требованиям технического регламента ТР ЕАЭС 043/2017 «О требованиях к средствам обеспечения пожарной безопасности и пожаротушения» и имеет сертификат соответствия № ЕАЭС RU C-RU.ПБ68.B.01662/23.

Изделие сертифицировано на соответствие требованиям к техническим средствам обеспечения транспортной безопасности в составе системы видеонаблюдения, № МВД РФ.03.000973.

20 СВЕДЕНИЯ О ПРИЁМКЕ

Изделие, коммутатор сетевой «BOLID SW-216» АЦДР.203729.003, 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.

ПРИЛОЖЕНИЕ А

Таблица А.1 – Список совместимых комплектных SFP-модулей

Модель	BOLID SFP-GMM-1D	BOLID SFP-GSM-3D	BOLID SFP-GSM-3SA	BOLID SFP-GSM-3SB	BOLID SFP-XMM-1D
Форм-фактор	SFP	SFP	SFP	SFP	SFP+
Пропускная способность	1 Гбит/с	1 Гбит/с	1 Гбит/с	1 Гбит/с	10 Гбит/с
Длина кабеля	550 м	20 км	20 км	20 км	300 м
Кол-во используемых волокон	2	2	1	1	2
Тип разъёма	LC/UPC	LC/UPC	LC/UPC	LC/UPC	LC/UPC
Тип оптоволоконного кабеля	MM	SM	SM	SM	MM
Парность	Tx850/ Rx850	Tx1310/ Rx1310	Tx1310/ Rx1550	Tx1550/ Rx1310	Tx850/ Rx850
Напряжение питания	3,3 В	3,3 В	3,3 В	3,3 В	3,3 В
Диапазон рабочих температур	От -40 °C до +85 °C	От -40 °C до +85 °C	От -40 °C до +85 °C	От -40 °C до +85 °C	От -40 °C до +85 °C
Относительная влажность воздуха	От 5 % до 95 %	От 5 % до 95 %	От 5 % до 95 %	От 5 % до 95 %	От 5 % до 95 %
Габаритные размеры	55,5×13,4× 8,5 мм	55,5×13,4× 8,5 мм	55,5×13,4× 8,5 мм	55,5×13,4× 8,5 мм	55,5×13,4× 8,5 мм

Перечень терминов и сокращений

АРМ	Автоматизированное рабочее место – это рабочее место специалиста, оснащенное персональным компьютером, программным обеспечением и совокупностью информационных ресурсов индивидуального или коллективного пользования
Веб	Web (паутина) – сокращенное альтернативное название Всемирной Сети Интернет, являющей собой систему взаимосвязанных за счет ссылок отдельных веб-страниц и других документов
ИМ	Инструкция по монтажу
ОС	Операционная система
ПО	Программное обеспечение
ПК	Персональный компьютер
РЭ	Руководство по эксплуатации
СКУД	Система контроля и управления доступом – это комплекс оборудования, главная функция которого – ограничение доступа на охраняемый объект. Элементы СКУД объединены в сеть, которая управляется с помощью специализированного программного оборудования
AC	Alternating Current – переменный ток
DC	Direct Current – Постоянный ток
DHCP	Dynamic Host Configuration Protocol – Протокол динамического конфигурирование хоста. Обеспечивает получение сетевыми устройствами IP-адресов от сервера в локальной сети
Ethernet	Локальная сеть, используемая для подключения между собой компьютеров, принтеров, рабочих станций, терминалов и т.п. в настоящее время реализуется на базе кабелей типа «витая пара». Скорость передачи сигнала составляет от десятков до тысяч мегабит в секунду
HTTP	HyperText Transfer Protocol – протокол передачи гипертекстовых документов

HTTPS	HyperText Transfer Protocol Secure – Расширение протокол передачи гипертекстовых документов для поддержки шифрования в целях повышения безопасности
ID	Identifier – идентификатор
IGMP	Internet Group Management Protocol (Протокол управления группами Интернета) – протокол управления групповой (multicast) передачей данных в сетях, основанных на протоколе IP. IGMP используется маршрутизаторами и IP-узлами для организации сетевых устройств в группы
IP	Internet Protocol – межсетевой протокол
IPv4	Internet Protocol version 4 – четвертая версия интернет протокола. Широко используемый тип IP-адреса, состоящий из 4 байт (32 бит)
IPV6	Internet Protocol version 6 – шестая версия интернет протокола. Новая система адресации, в которой адрес состоит из 16 Б (128 бит)
LACP	Link Aggregation Control Protocol – протокол, предназначенный для объединения нескольких физических каналов в один логический в сетях Ethernet
MAC	Media Access Control – уникальный идентификатор, присваиваемый сетевым адаптерам. Играет роль физического адреса сетевого адаптера
MicroSD	Secure Digital Memory Card – защищенная цифровая карта памяти. Электронное энергонезависимое запоминающее устройство для хранения цифровой информации размером 11x15x1 мм
PoE	Power over Ethernet – стандарты IEEE 802.3af, IEEE 802.3at, позволяющие передавать по сети Ethernet не только данные, но и электрический ток
QoS	Quality of Service – качество обслуживания. Набор технологий, обеспечивающих приоритетное использование канала связи

RJ-45	Registered Jack 45 – стандартизированный физический сетевой интерфейс, включающий описание конструкции обеих частей разъёма («вилки» и «розетки») и схемы их коммутации. Используется для соединения телекоммуникационного оборудования
RSTP	Rapid Spanning Tree Protocol – версия протокола STP с ускоренной реконфигурацией дерева, использующегося для исключения петель (исключения дублирующих маршрутов) в соединениях коммутаторов Ethernet с дублирующими линиями
SFP	Small Form-factor Pluggable – промышленный стандарт модульных компактных приемопередатчиков (трансиверов), используемых для передачи и приема данных в телекоммуникациях
SFP+	Enhanced Small Form-factor Pluggable, SFF-8431, SFF-8083 – промышленный стандарт модульных компактных приемопередатчиков (трансиверов), используемых для передачи данных в телекоммуникациях. Расширенная версия приемопередатчика SFP, способного поддерживать скорости передачи данных от от 2,5 Гб/с до 10 Гб/с
SNMP	Simple Network Management Protocol (простой протокол сетевого управления) – стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP
SSH	Secure Shell – безопасная оболочка. Сетевой протокол прикладного уровня, позволяющий производить удаленное управление операционной системой и туннелирование TCP-соединений. Позволяет безопасно передавать в незащищенной среде практически любой другой сетевой протокол
STP	Spanning Tree Protocol – сетевой протокол (или семейство сетевых протоколов) предназначенный для автоматического удаления циклов (петель коммутации) из топологии сети на канальном уровне в Ethernet-сетях
VLAN	Virtual Local Area Network – виртуальная локальная компьютерная сеть
8P8C	8 Position 8 Contact – унифицированный разъём, используемый в телекоммуникации. Имеет 8 контактов и фиксатор

Перечень рисунков

Перечень таблиц

Лист регистрации изменений

№ Изме-нения	Номера листов (страниц)				Всего листов (страниц) в доку-менте	№ доку-мента	Входящий № сопроводи-тельного документа и дата	Под-пись	Дата
	Изме-нённых	Заме-нённых	Новых	Аннули-рован-ных					

ЗАО НВП «Болид»

Центральный офис:

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

Тел.: +7 (495) 775-71-55

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