Сетевой коммутатор

BOLID SW-204

Руководство по эксплуатации

АЦДР.203729.005 РЭп

Настоящее руководство по эксплуатации (далее по тексту – РЭ) содержит сведения о конструкции, принципе работы, технических характеристиках управляемого сетевого коммутатора «BOLID SW-204» АЦДР.203729.005 (далее по тексту – коммутатор или изделие) и указания, необходимые для правильной и безопасной эксплуатации.

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

ПРИМЕЧАНИЕ!

- Технические характеристики, функционал и интерфейс коммутатора версии 2 отличается от версии 1.
- Руководство по эксплуатации описывает интерфейс и функциональные возможности внутреннего ПО – 1.001.100F002.0.R (сборка от 25.09.2025).
- Руководство по эксплуатации содержит только справочную информацию, необходимую для использования его технических возможностей.
- Дизайн изделия, технические характеристики, а так-же ПО, упомянутые в данном руководстве, подлежат изменению без обязательного предварительного письменного уведомления.
- В случае нахождения неточностей или несоответствий, обращайтесь в службу поддержки.

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ

1. Сетевой коммутатор предназначен для соединения подключенных к коммутатору устройств или нескольких сегментов сети с гибкой настройкой коммутации пакетов данных.

2. Поддержка технологии PoE позволяет передавать питание на различные устройства и периферию. Изделие 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 предназначен для работы в жилых, коммерческих и производственных зонах.

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

7. Отличительными особенностями версии 2 от версии 1 являются:

– Появление двух дополнительных портов SFP 1000 Мбит/с (7 – 8);

– Порты питания PWR1 и PWR2;

– Опция увеличения дальности передачи со 100 м до предельно 250 м для подключенных в порты 1 – 4 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.

8. Возможное применение:

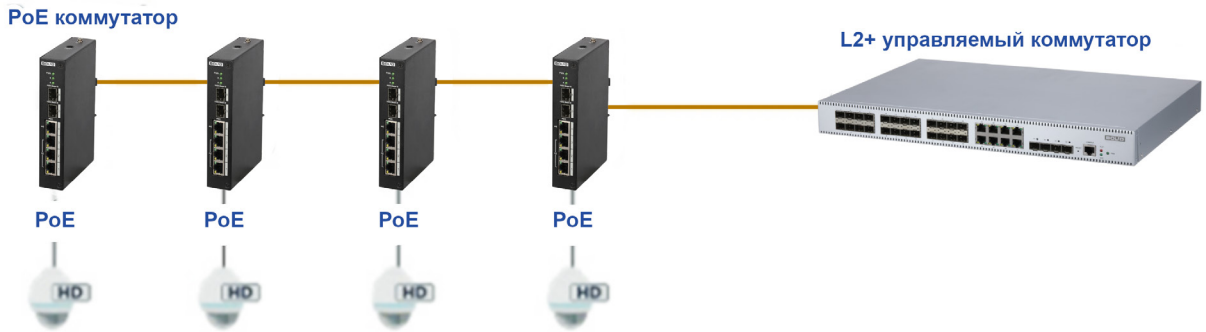


Рисунок 1.1 – Каскадное соединение

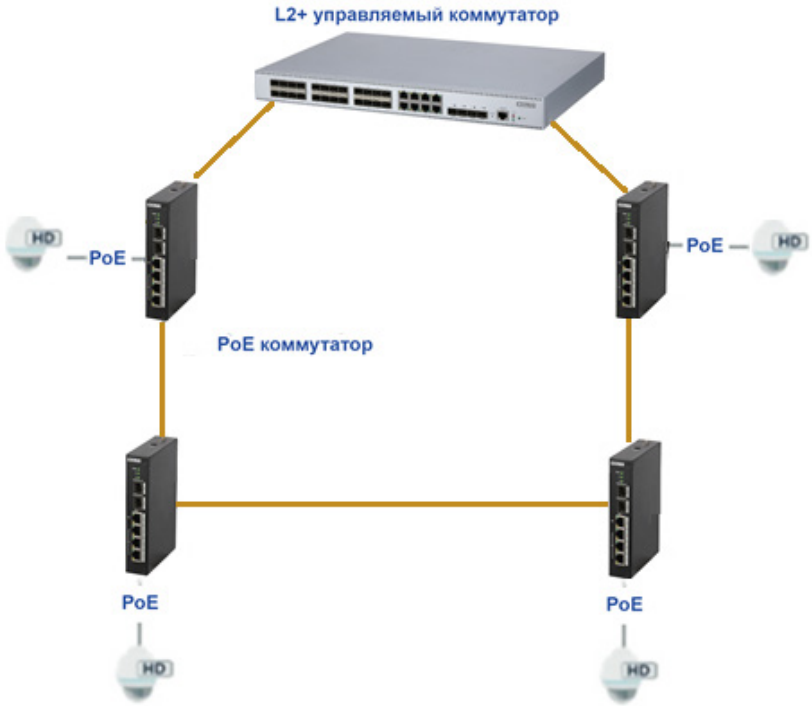


Рисунок 1.2 – Кольцевое соединение

2 ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Основные технические характеристики изделия приведены в таблице ниже (Таблица 2.1).

Таблица 2.1 – Технические характеристики*

Наименование параметра	Значение параметра
Сетевые интерфейсы	
Общее количество	8 интерфейсов
RJ-45	Порт № 1 – 4: RJ-45 10/100 Мбит/с (PoE)
SFP	Порт № 5 – 8: SFP 1000 Мбит/с
SFP+	Нет
Оборудование	
Порты RJ-45	4 порта
Порты SFP	4 порта
Порты SFP+	Нет
Электропитание без БП (постоянный ток)	
Напряжение питания	48 − 57 В постоянного тока
Потребляемый ток	2,5 А (Макс.)
Потребляемая мощность	6 Вт в дежурном режиме 96 Вт при полной нагрузке
Электропитание с комплектным БП (переменный ток)	
Напряжение питания	110 – 220 В переменного тока
Потребляемый ток	0,9 А (Макс.)
Потребляемая мощность	12 Вт в дежурном режиме 150 Вт при полной нагрузке
Производительность	
Уровень	L2
Тип	Управляемый
Время технической готовности прибора к работе	50 с
Коммутационная матрица	8,8 Gbps
Маршрутизация пакетов	6,5472 Mpps
Буфер пакетов	4,1 Мбит
Таблица MAC адресов	8 К
Число VLAN	4094

Наименование параметра	Значение параметра
Интерфейс VLAN	10
Маршруты IPv4	1
Поддерживаемые стандарты	IEEE802.3, IEEE802.3u, IEEE802.3x, IEEE802.3ab, IEEE802.3az
PoE	
Стандарты PoE	Порт 1: IEEE802.3af, IEEE802.3at, Hi-PoE, IEEE802.3bt Порт 2 – 4: IEEE802.3af, IEEE802.3at
Мощность PoE портов	Порт № 1: не более 90 Вт (на порт) Порт № 2 – 4: не более 30 Вт (на порт)
Общая мощность PoE	Не более 96 Вт
Распиновка подаваемого питания PoE	1, 2, 4, 5 (V+) 3, 6, 7, 8 (V-)
Функционал	
Настройки PoE	Long PoE, Green PoE, PoE принудительно, PoE watchdog
Таблица MAC-адресов	Поддержка статического MAC-адреса
Spanning Tree Protocol	STP/RSTP/ERPS
Multicast	IGMP Snooping
DHCP	DHCP-сервер, DHCP-клиент, DHCP Snooping
Безопасность	IEEE802.1x, защита от петель
Агрегирование каналов	LACP, статическое агрегирование
QoS	QoS на основе CoS, QoS на основе DSCP, 8 очередей на порт, шейпирование на порту
Зеркалирование	1:1 (Один к одному), N:1 (Много к одному)
Управление устройством	Веб-интерфейс, SNMP V1/V2C/V3
Системное обслуживание	Загрузка и выгрузка файла настроек, обновление прошивки, системный журнал
Общие сведения	
Диапазон рабочих температур	От -30 °C до +65 °C
Относительная влажность воздуха	От 10 % до 90 %
Защита от статического электричества	Наведенная:8 КВ Контактный разряд: 6 КВ

Наименование параметра		Значение параметра
Грозозащита		В общем случае: 4 КВ Дифференциальная: 2 КВ
Степень защиты оболочки по ГОСТ 14254-2015		IP40
Устойчивость к механическим воздействиям по ГОСТ 25 1099-83		Категория размещения 3
Вибрационные нагрузки	диапазон частот	1 – 35 Гц
	максимальное ускорение	0,5 g
Габаритные размеры		152,9×110,4×42,0 мм
Масса		Вес нетто: 0,622 кг Вес брутто: 1,378 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		155M 20km 1310/1550nm, LC, Single-mode 155M 20km 1550/1310nm, LC, Single-mode 1.25G 20km 1310/1550nm, LC, Single-mode 1.25G 20km 1550/1310nm, LC, Single-mode 155M 2KM 850nm, LC, Multi-mode 1.25G 500m 850nm, LC, Multi-mode

*Технические характеристики могут быть изменены без предварительного уведомления.

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.

Питание коммутатора может осуществляться от резервированного источника питания РИП-48, который передаёт сигналы неисправности линий электропитания на ШС ППКОП (например, «Сигнал-10», «Сигнал-20М», «Сигнал-20П»), либо пульт «С2000М», АРМ «Орион Про», ППКУП «Сириус».

3 КОМПЛЕКТНОСТЬ

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

Таблица 3.1 – Комплект поставки*

Обозначение	Наименование	Количество
АЦДР.203729.005	Коммутатор «BOLID SW-204»	1 шт.
АЦДР.203729.005 РЭ	Руководство по эксплуатации изделия «BOLID SW-204»	1 экз.
	Блок питания, 53 В постоянного тока, 1,81 А	1 шт.
	Кабель питания, 220 В переменного тока	1 шт.
	Винтовой клеммный блок 2Р	1 шт.
	Разъём питания 2Р	1 шт.
	SFP модуль**	—

*Комплект поставки может быть изменён без предварительного уведомления.

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

4 КОНСТРУКЦИЯ

4.1 Верхняя панель

Конструктивно коммутатор выполнен в металлическом корпусе с креплением под DIN-рейку.

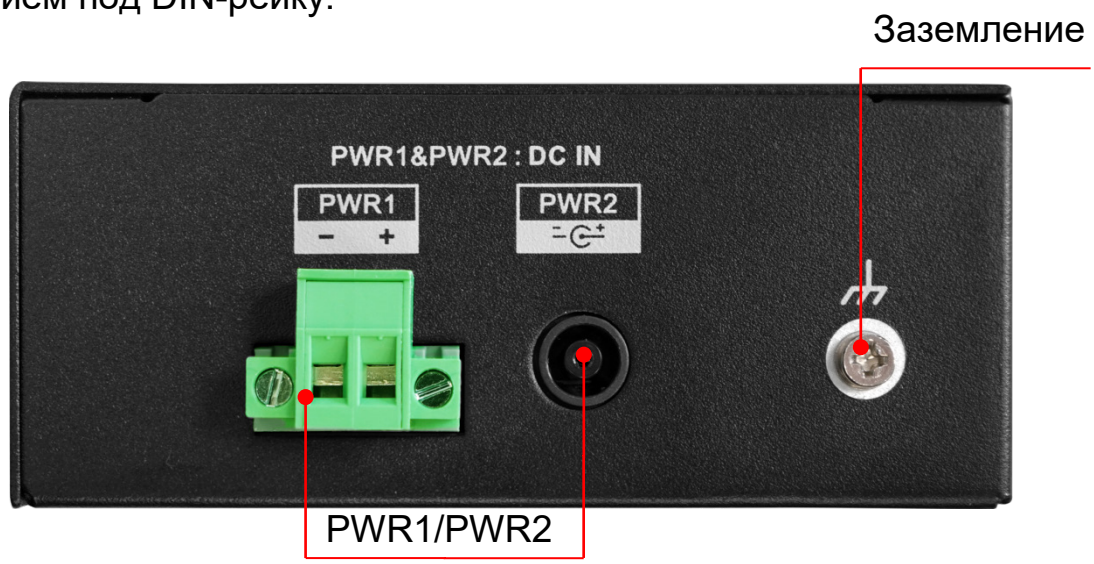


Рисунок 4.1 – Верхняя панель

Таблица 4.1 – Верхняя панель изделия

Параметр	Функции
PWR1/PWR2	– Дублированные разъёмы питания; – Разъём питания с поддержкой 48 − 57 В постоянного тока. Подробнее смотрите в разделе «4.1.2 Порты питания PWR1/PWR2».
Заземление	Винт защитного заземления. Подробнее смотрите в разделе – «4.1.1 Заземление (GND)».

4.1.1 Заземление (GND)

ВНИМАНИЕ!
Правила организации защитного заземления регламентируются документами «Правила устройства электроустановок (ПУЭ). Глава 1.7 «Заземление и защитные меры электробезопасности» ГОСТ 12.2.007.0-75.

Все работы с заземлением производятся при отключенном питании.

Для обеспечения безопасной и надёжной работы сетевого коммутатора следует правильно выполнить его заземление. Заземление помогает защитить устройство от молний, электростатических разрядов и других электрических помех, что способствует стабильной работе всей сети.

Заземляющий винт (GND) расположен на верхней панели устройства (Рисунок 4.2).

Рисунок 4.2 – Верхняя панель

Для подключения:

1. Убедитесь, что коммутатор отключен от питания.

2. С помощью крестовой отвёртки отсоедините заземляющий винт (GND) от верхней панели устройства.

3. Соедините заземляющий винт и клемму заземляющего кабеля и закрепите в резьбовом отверстии (GND) на верхней панели устройства.

📖 Сечение медного кабеля: не менее 0,75 мм^2 и не более 2,5 мм^2, сопротивление относительно земли: не более 4 Ом.

4.1.2 Порты питания PWR1/PWR2

❗	Все работы выполняются только после подключения заземления (GND).
❗	Все работы производятся при отключенном питании.

Порты питания PWR1 и PWR2 используются для подключения к двум источникам питания, поддерживающим постоянное напряжение от 48 В до 57 В. Это позволяет обеспечить автоматическое переключение при сбое основного источника на резервный. Расположены PWR1 и PWR2 на верхней панели устройства.

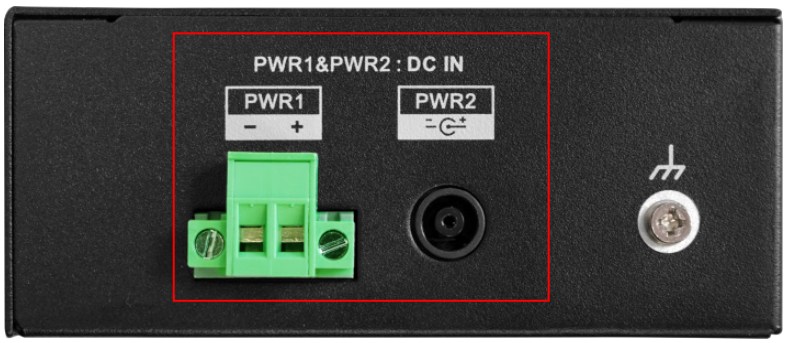


Рисунок 4.3 – Верхняя панель

Таблица 4.2 – Порты питания PWR1/PWR2

Параметр	Функции
PWR1	Винтовой клеммный блок 2P с поддержкой 48 − 57 В постоянного тока.
PWR2	Разъём питания с поддержкой 48 − 57 В постоянного тока.

Подключение к PWR1:

1. Подсоедините заземление к устройству.

2. С помощью шлицевой отвёртки ослабьте верхние винты на клеммном блоке.

3. Подключите «разъём питания 2P» к клеммам «PWR1 минус» и «PWR1 плюс». Подключите блок питания 48 − 57 В постоянного тока.

Подключение к PWR2:

1. Подсоедините заземление к устройству.

2. Подключите к PWR2 блок питания (53 В постоянного тока, 1,81 А) из комплекта поставки.

4.2 Передняя панель

Расшифровка передней панели показана в таблице ниже (см. Таблица 4.3).

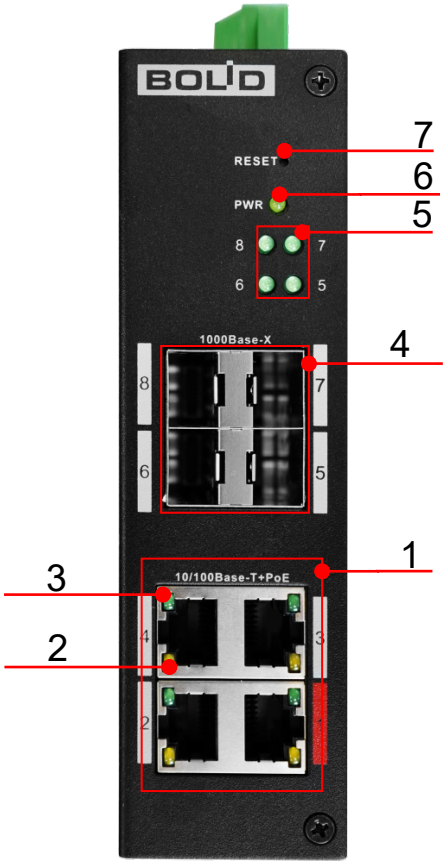


Рисунок 4.2 – Передняя панель

Таблица 4.3 – Порты и индикаторы передней панели

№	Параметр	Функции
1	10/100 Base-T+PoE	4 PoE порта RJ-45. Порт 1 (Красный порт): поддерживает стандарты IEEE802.3af, IEEE802.3at, IEEE802.3bt и Hi-PoE. Мощность PoE порта 90 Вт. Подходит для питания мощных устройств. Порт 2 – 4: поддерживают стандарты IEEE 802.3af и IEEE 802.3at. Мощность PoE портов 30 Вт (на порт).
2	Индикатор PoE	Индикатор состояния источника питания PoE.
3	Индикатор сети	Индикатор состояния порта Ethernet.
4	1000 Base-X	Порты SFP 1000 Мбит/с.
5	Link/Act	Индикаторы состояния SFP портов.
6	PWR	Индикатор питания.

№	Параметр	Функции
7	Reset	Кнопка сброса на заводские настройки. Подробнее смотрите в разделе – 15.2 Сброс на заводские настройки с помощью кнопки «RESET».

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 R-J45 коммутатора с помощью стандартного штекера 8P8C.

4.2.1 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.

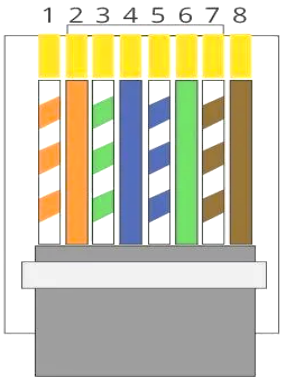


Рисунок 4.4 – Штекер 8P8C

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

4.2.2 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 защёлкнутом состоянии.

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

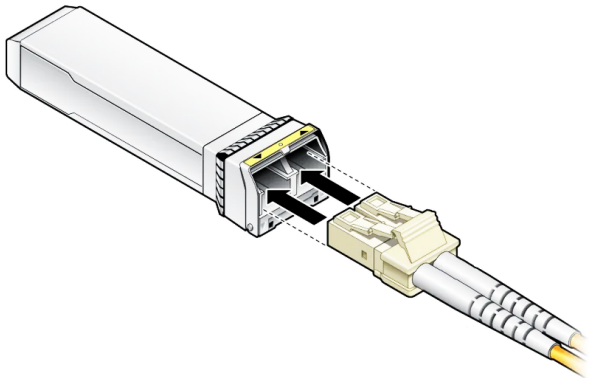


Рисунок 4.5 – Подключения кабеля

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. К работе с изделием допускается квалифицированный персонал, изучивший настоящее руководство.

2. Все работы по монтажу и наладке производить с соблюдением требований действующих нормативных документов по технике безопасности.

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

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

5. Для монтажных работ необходимо использовать исправный, безопасный и удобный монтажный инструмент.

6. Монтаж производить только на чистой, сухой установочной поверхности при отсутствии атмосферных осадков, повышенной влажности и иных неблагоприятных условий.

7. Не устанавливайте коммутатор в местах: температура в которых опускается ниже минус 30 °С и/или поднимается выше плюс 65 °С; с влажностью выше 95 %; повышенного испарения и парообразования; усиленной вибрации.

8. Монтаж производить без повреждения конструкции. Выполненный монтаж должен обеспечивать герметичность внутренней конструкции и электрического подключения.

9. При монтаже провода электропитания и выходов следует оставить достаточное пространство для лёгкого доступа при дальнейшем обслуживании изделия.

10. Необходимо исключить образование, попадание или воздействие конденсата, электроразряда, статического электричества, грязи, жидкости, опасных веществ и мусора на поверхности, на электронных, конструктивных и электрических элементах изделия.

11. Не допускайте установку изделия под воздействием прямых солнечных лучей и вблизи источников, излучающих тепло.

12. В соответствии с правилами устройства электроустановок (ПУЭ) эксплуатация коммутатора без заземления не допускается.

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

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

5.2 Монтаж

1. Размещение и монтаж должны проводиться в соответствии с проектом, разработанным для данного объекта. При этом в проекте должны быть учтены:

– Условия эксплуатации изделий;

– Требования к длине и конфигурации линии связи.

2. Технологическая последовательность монтажных операций определяется исходя из удобства их проведения.

3. Запрещается устанавливать ближе 1 м от элементов отопления.

4. Для выбора типа кабеля и сечения проводов необходимо руководствоваться нормативной документацией.

5. Установка изделия должна отвечать следующим требованиям:

– Индикаторы состояния на передней панели могут быть легко прочитаны;

– Доступ к портам достаточен для свободной подводки кабелей;

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

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

– Обеспечено достаточное пространство для 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 изделие 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

Коммутатор предназначен для установки на DIN-рейку, полку или стол. Габаритные размеры коммутатора приведены на рисунке ниже (Рисунок 5.1).

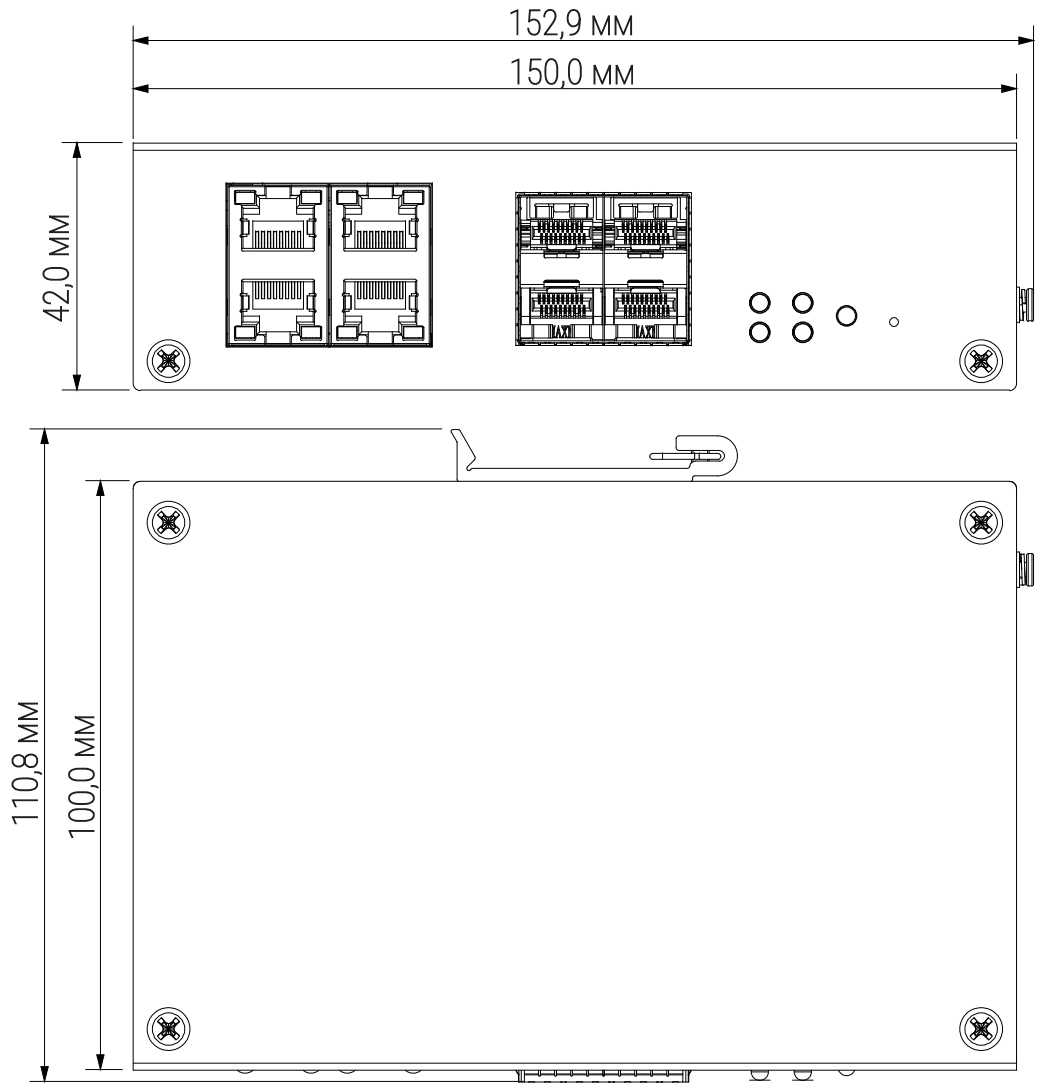


Рисунок 5.1 – Габаритные размеры

5.2.2 Крепление на DIN-рейку

Для данного сетевого коммутатора возможен монтаж на DIN-рейку шириной 35 мм.

Для крепления на DIN-рейку заведите верхний край коммутатора с пружиной за верхнюю часть пластины DIN-рейки, чтобы пружина попала за край пластины. Нажмите на корпус коммутатора до щелчка и фиксации нижнего края рейки в защёлке.

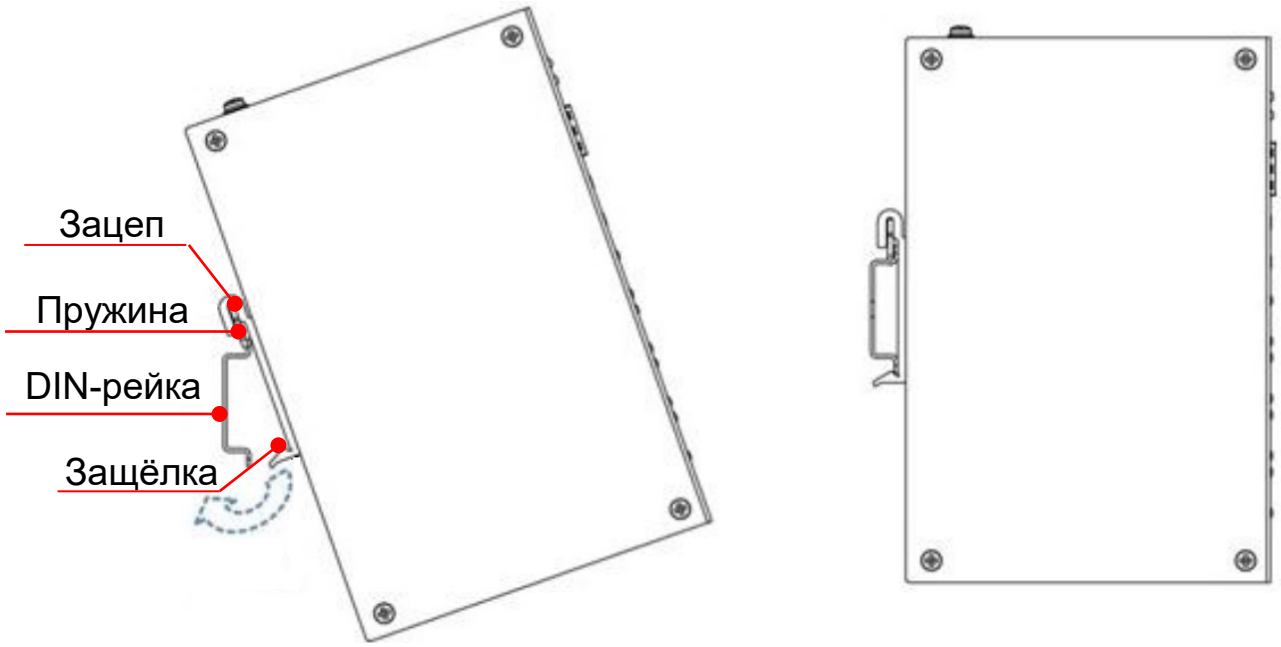


Рисунок 5.2 – Инсталляция

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/Uplink. При запуске обмена данными индикаторы PoE/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).

По умолчанию при первой включении коммутатор имеет статический сетевой адрес IPv4:	
IP-адрес	192.168.1.110
Маска подсети	255.255.255.0

Шаг 2. Из выпадающего списка выберите язык интерфейса. Нажмите кнопку «Следующий» для продолжения.

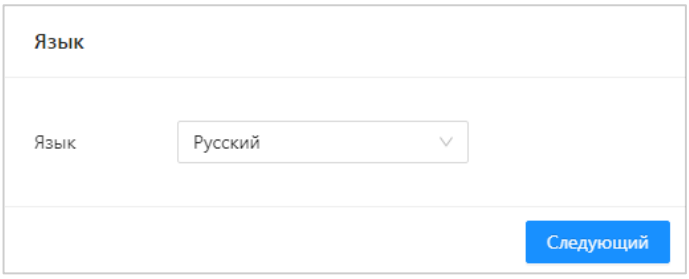


Рисунок 6.1 – Инициализация

Шаг 3. Выберите из выпадающего списка часовой пояс. Нажмите кнопку «Следующий» для продолжения.

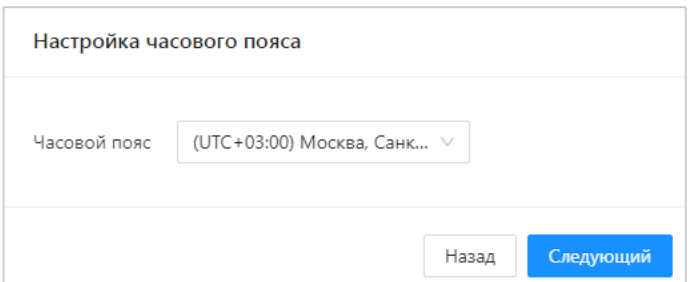


Рисунок 6.2 – Инициализация

Шаг 4. При заводских настройках пароль по умолчанию отсутствует, поэтому установите пароль учётной записи «admin». В строках «Новый 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 «ОК».

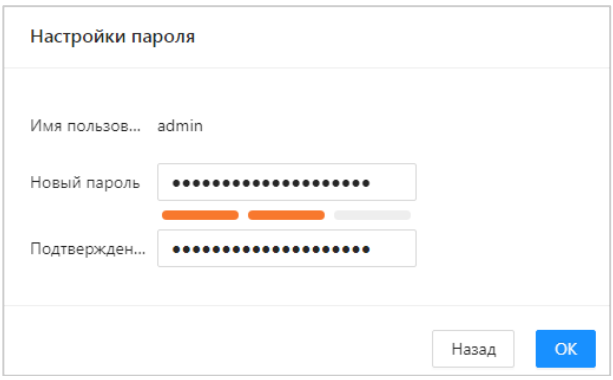


Рисунок 6.3 – Инициализация

Шаг 5. В появившемся окне введите имя пользователя и пароль учётной записи. Нажмите кнопку «Вход».

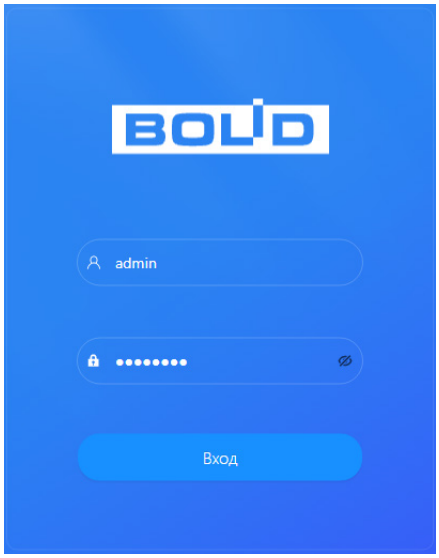


Рисунок 6.4 – Вход

6.2 Локальный адрес

Шаг 6. Измените сетевые настройки коммутатора в соответствии с параметрами вашей сети. Для этого перейдите «Главное меню → Настройки → Быстрая настройка → Общие» (Рисунок 6.5). 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 «Главное меню → Обслуживание системы → Обслуживание» и нажмите кнопку «Перезагрузка».

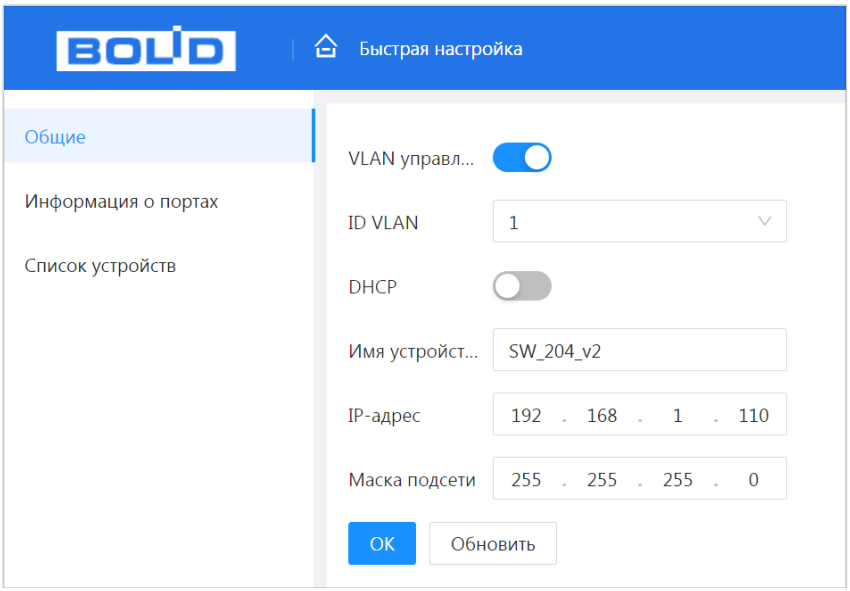


Рисунок 6.5 – Сетевые настройки

Таблица 6.1 – Параметры сетевых настроек коммутатора

Параметр	Функция
DHCP	После активации переключателя «DHCP» IP-адрес будет получен автоматически от DHCP-сервера, пользовательское задание IP/маски – невозможно. Если переключатель «DHCP» деактивирован, то для ручного ввода становятся доступны поля ввода «IP-адрес» и «Маска подсети».
Имя устройства	Поле ввода имени устройства. Вводимый пароль может состоять только из: цифр, латинских букв нижнего и верхнего регистра и нижнего подчёркивания « _ ». Пробелы и ввод иных знаков, кроме « _ » запрещены.
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.

Шаг 7. После изменения настроек веб-интерфейс должен быть доступен по-новому IP-адресу. Корректный вход в систему производится с новыми учётными данными admin.

7 ГЛАВНОЕ МЕНЮ

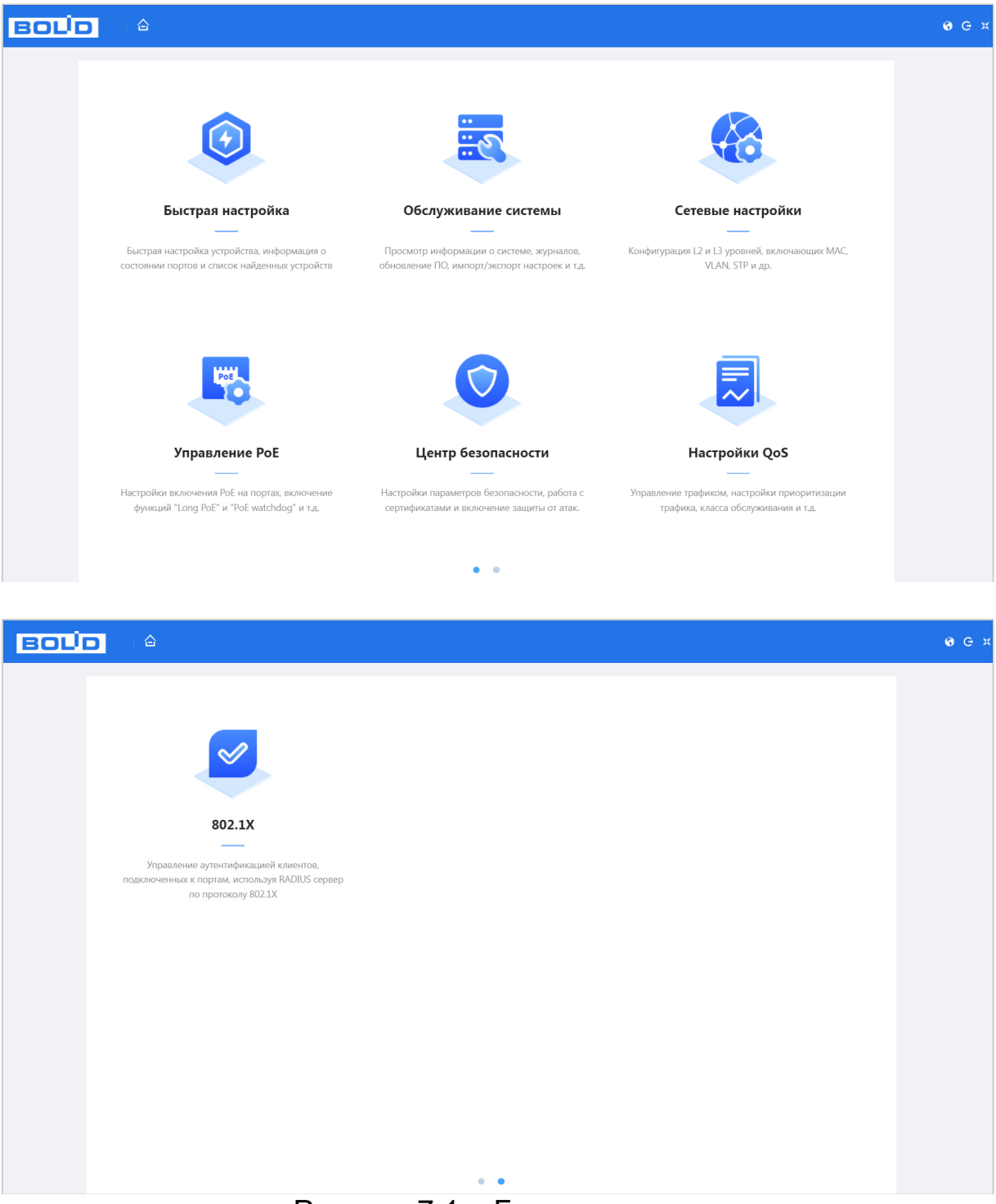


Рисунок 7.1 – Главное меню

Таблица 7.1 – Структура меню

 Быстрая настройка Раздел главного меню «Быстрая настройка»	Подраздел «Общие»
	Подраздел «Информация о портах»
	Подраздел «Список устройств»

<table>
<tr><td rowspan="10"> 
Обслуживание системы
Раздел главного меню «Обслуживание системы»</td><td colspan="2">Подраздел «Системное время»</td></tr>
<tr><td colspan="2">Подраздел «Изменить пароль»</td></tr>
<tr><td colspan="2">Подраздел «Обслуживание»</td></tr>
<tr><td colspan="2">Подраздел «Импорт/Экспорт»</td></tr>
<tr><td colspan="2">Подраздел «Системная информация»</td></tr>
<tr><td colspan="2">Подраздел «Журнал»</td></tr>
<tr><td colspan="2">Подраздел «Состояние устройства»</td></tr>
<tr><td colspan="2">Подраздел «Диагностика»</td></tr>
<tr><td colspan="2">Подраздел «Зеркалирование»</td></tr>
<tr><td rowspan="25"> 
Сетевые настройки
Раздел главного меню «Сетевые настройки»</td><td colspan="2">Подраздел «Порт»</td></tr>
<tr><td colspan="2">Подраздел «Энергоэффективный Ethernet (EEE (Energy Efficient Ethernet))»</td></tr>
<tr><td rowspan="2">Подраздел «VLAN»</td><td>Пункт «Добавить VLAN»</td></tr>
<tr><td>Пункт «VLAN»</td></tr>
<tr><td colspan="2">Подраздел «Интерфейс VLAN (VLANIF)»</td></tr>
<tr><td colspan="2">Подраздел «Настройки маршрутизации»</td></tr>
<tr><td rowspan="2">Подраздел «ERPS»</td><td>Пункт «ERPS»</td></tr>
<tr><td>Пункт «MEP»</td></tr>
<tr><td colspan="2">Подраздел «IGMP Snooping»</td></tr>
<tr><td rowspan="2">Подраздел «STP»</td><td>Пункт «STP»</td></tr>
<tr><td>Пункт «Экземпляр порта»</td></tr>
<tr><td colspan="2">Подраздел «Объединение каналов записи (Агрегация каналов)»</td></tr>
<tr><td colspan="2">Подраздел «SNMP»</td></tr>
<tr><td rowspan="2">Подраздел «MAC-адрес»</td><td>Пункт «Таблица MAC-адресов»</td></tr>
<tr><td>Пункт «Фильтрация MAC-адресов»</td></tr>
<tr><td colspan="2">Подраздел «LLDP»</td></tr>
<tr><td colspan="2">Подраздел «Обнаружение петель»</td></tr>
<tr><td rowspan="3">Подраздел «DHCP сервер»</td><td>Пункт «DHCP сервер»</td></tr>
<tr><td>Пункт «Статическая привязка»</td></tr>
<tr><td>Пункт «Список адресов</td></tr>
<tr><td rowspan="3">Подраздел «DHCP Snooping»</td><td>Пункт «Глобальные настройки</td></tr>
<tr><td>Пункт «Конфиг-я порта</td></tr>
<tr><td>Пункт «Конфигурация опции 82</td></tr>
<tr><td colspan="2">Подраздел «Тестирование виртуального кабеля»</td></tr>
</table>

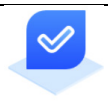
<table>
<tr><td rowspan="7"> 
Управление PoE
Раздел главного меню «Управление PoE»</td><td colspan="2">Подраздел «Настройки PoE»</td></tr>
<tr><td colspan="2">Подраздел «Бессрочный PoE»</td></tr>
<tr><td colspan="2">Подраздел «Long PoE»</td></tr>
<tr><td colspan="2">Подраздел «Статистика событий PoE»</td></tr>
<tr><td colspan="2">Подраздел «Green PoE»</td></tr>
<tr><td colspan="2">Подраздел «PoE принудительно»</td></tr>
<tr><td colspan="2">Подраздел «PoE watchdog»</td></tr>
<tr><td rowspan="8"> 
Центр безопасности
Раздел главного меню «Центр безопасности»</td><td rowspan="2">Подраздел «Доп. сервисы»</td><td>Пункт «Доп. сервисы»</td></tr>
<tr><td>Пункт «HTTPS»</td></tr>
<tr><td rowspan="2">Подраздел «Сертификат CA»</td><td>Пункт «Сертификат устройства»</td></tr>
<tr><td>Пункт «Доверенные сертификаты CA»</td></tr>
<tr><td rowspan="2">Подраздел «Сетевой экран»</td><td>Пункт «IP фильтр»</td></tr>
<tr><td>Пункт «Защита от атак DoS»</td></tr>
<tr><td colspan="2">Подраздел «Изолирование портов»</td></tr>
<tr><td>Подраздел «Безопасная аутентификация»</td><td>Пункт «Алгоритм проверки подлинности»</td></tr>
<tr><td rowspan="5"> 
Настройки QoS
Раздел главного меню «Настройки QoS»</td><td colspan="2">Подраздел «Приоритет портов»</td></tr>
<tr><td colspan="2">Подраздел «Классификация портов»</td></tr>
<tr><td colspan="2">Подраздел «Планировщик очереди»</td></tr>
<tr><td colspan="2">Подраздел «Шейпер трафика»</td></tr>
<tr><td colspan="2">Подраздел «Контроль шторма»</td></tr>
<tr><td rowspan="2"> 
802.1X
Раздел главного меню «802.1X»</td><td colspan="2">Подраздел «Настройка 802.1X (NSA)»</td></tr>
<tr><td colspan="2">Подраздел «RADIUS-сервер»</td></tr>
</table>

Таблица 7.2 – Функционал главного меню

	Возврат к главному меню.
Переключатель	Кнопки переключения страниц.
	Переключение режима просмотра в полноэкранный. Для выхода из полноэкранного режима нажмите клавишу «Esc» на клавиатуре.
	Выбор языка.
	Кнопка выхода из учётной записи.

8 РАЗДЕЛ ГЛАВНОГО МЕНЮ «БЫСТРАЯ НАСТРОЙКА»

8.1 Подраздел «Общие»

В подразделе задаются сетевые параметры устройства.

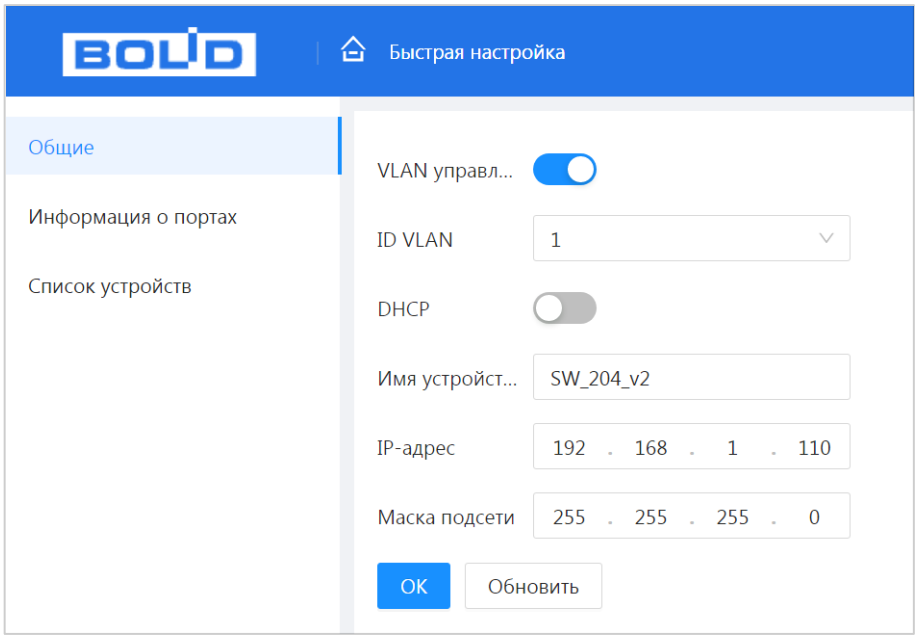


Рисунок 8.1 – Сетевые параметры устройства

Таблица 8.1 – Параметры сетевых настроек коммутатора

Параметр	Функция
VLAN управления	После включения «VLAN управления» доступ к веб-странице возможен только по IP-адресу, заданному для VLAN управления.
ID VLAN	Выбор ID VLAN управления.
DHCP	После активации переключателя «DHCP» IP-адрес будет получен автоматически от DHCP-сервера, пользовательское задание IP/маски – невозможно. Если переключатель «DHCP» деактивирован, то для ручного ввода становятся доступны поля ввода «IP-адрес» и «Маска подсети».
Имя устройства	Поле ввода имени устройства. Вводимое имя может состоять только из: цифр, латинских букв нижнего и верхнего регистра и « _ ». Пробелы и ввод иных знаков, кроме « _ » запрещены.
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.

8.2 Подраздел «Информация о портах»

Подраздел включает в себя графическую и текстовую информацию о состоянии портов.

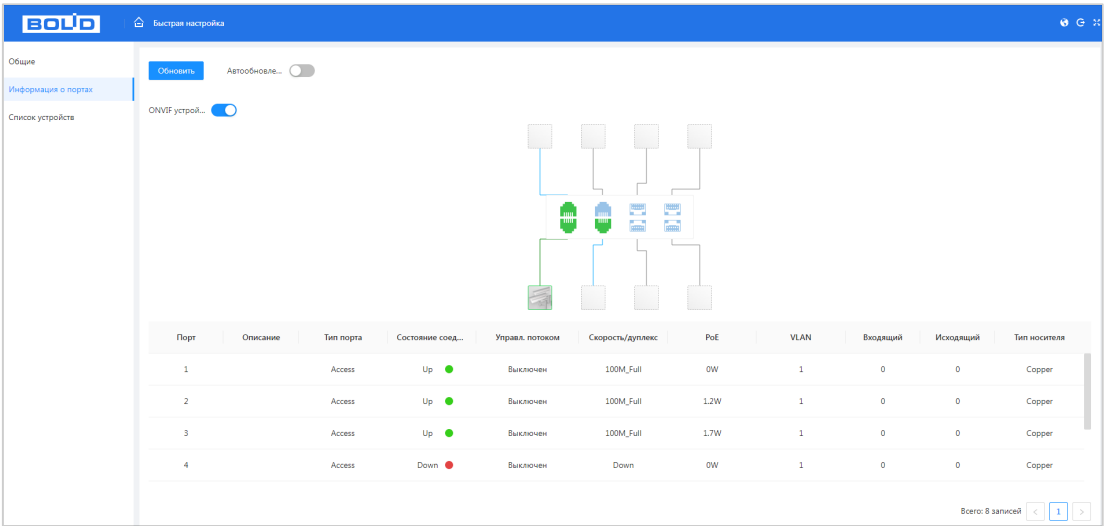


Рисунок 8.2 – Информационная панель

Графическая панель представляет собой изображение передней панели коммутатора. Отображает состояние подключения к каждому порту в реальном времени (Рисунок 8.3).

Рисунок 8.3 – Графическая панель

После активации переключателя «ONVIF устройства» 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: номер порта, VLAN и информацию о PoE (Рисунок 8.4).

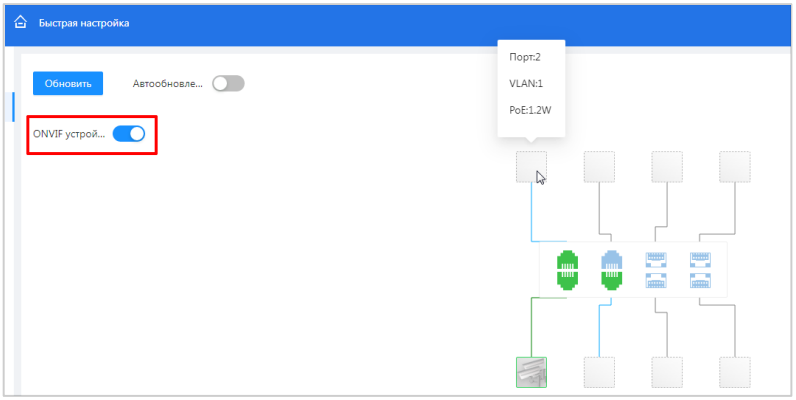
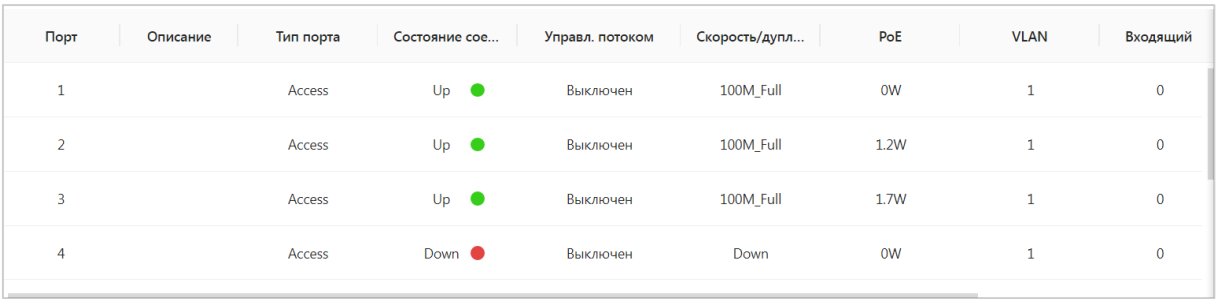


Рисунок 8.4 – Графическая панель

Параметры текстовой панели описаны в таблице ниже (см. Таблица 8.2).



Порт	Описание	Тип порта	Состояние сое...	Управл. потоком	Скорость/дупл...	PoE	VLAN	Входящий
1		Access	Up	Выключен	100M_Full	0W	1	0
2		Access	Up	Выключен	100M_Full	1.2W	1	0
3		Access	Up	Выключен	100M_Full	1.7W	1	0
4		Access	Down	Выключен	Down	0W	1	0

Рисунок 8.5 – Текстовая информационная панель

Таблица 8.2 – Текстовая информация о порте

Параметр	Описание
Порт	Номер порта. Соответствует числу на передней панели.
Описание	Текстовое поле отображает введённую информацию. Отображаемая информация вводится при настройках порта (подробнее смотрите – Подраздел «Порт»).
Тип порта	Столбец отображает тип порта и их функции. Доступны три вида: Access, Hybrid и Trunk. Подробнее о настойках смотрите – Пункт «VLAN».
Состояние соединения	– Up – порт подключен; – Down – порт отключен; – Disabled – порт выключен.
Управл. потоком	Состояние управления потоком. Подробнее о включение потока смотрите – Подраздел «Порт».
Скорость/дуплекс	Отображает текущую скорость и в каком режиме передачи параллельном (Full) или последовательном находится порт. Подробнее о включение потока смотрите – Подраздел «Порт».
PoE	Потребляемая мощность.
VLAN	Идентификатор VLAN.
Входящий	Нагрузка в процентах от максимальной пропускной способности принимаемых портом пакетов.
Исходящий	Нагрузка в процентах от максимальной пропускной способности передаваемых портом пакетов.
Тип носителя	Показывается тип подключенного носителя сигнала. – Copper – медный кабель; – Fiber – волоконно-оптический кабель.

8.3 Подраздел «Список устройств»

Страница раздела «Список устройств» включает в себя три списка обнаруженных коммутатором устройств в сети:

– Список «Видеокамеры»;

– Список «Видеорегистраторы»;

– Список «Прочее».

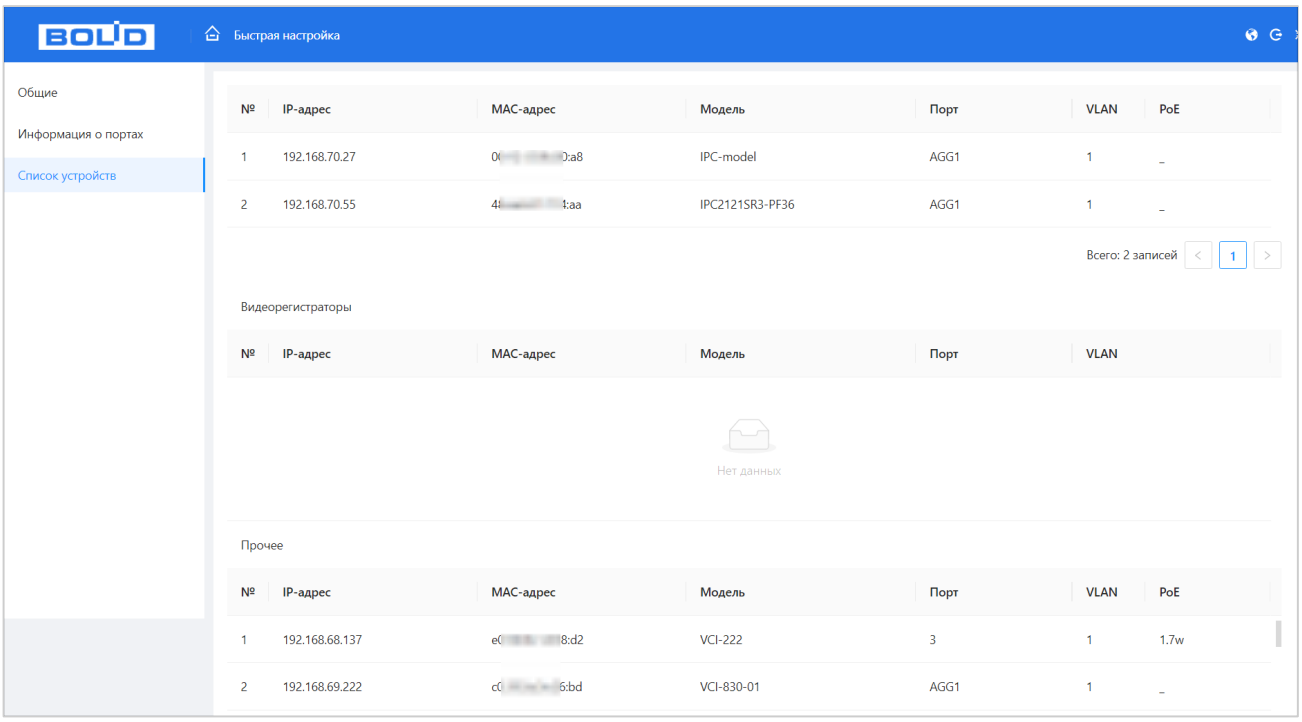


Рисунок 8.6 – Список найденных устройств

9 РАЗДЕЛ ГЛАВНОГО МЕНЮ «ОБСЛУЖИВАНИЕ СИСТЕМЫ»

9.1 Подраздел «Системное время»

ВНИМАНИЕ!
Рекомендуется настроить NTP-сервер для предотвращения сбоев системного времени.

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.

При активации радиокнопки «Не синхронизировать», пользователь самостоятельно устанавливает время на устройстве.

По кнопке «Синхронизировать с ПК» произойдёт синхронизация времени между устройством и ПК.

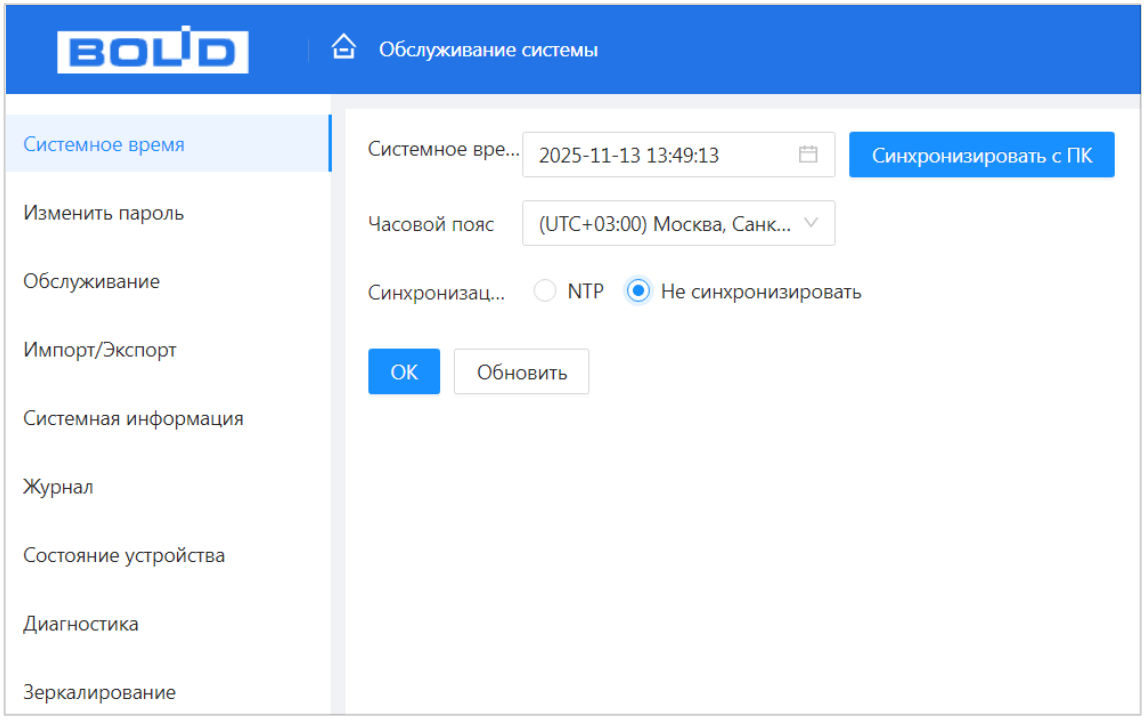


Рисунок 9.1 – Настройка/синхронизация времени

Для синхронизации с NTP-сервером активируйте радиокнопку «NTP» и введите адрес NTP-сервера (Рисунок 9.2).

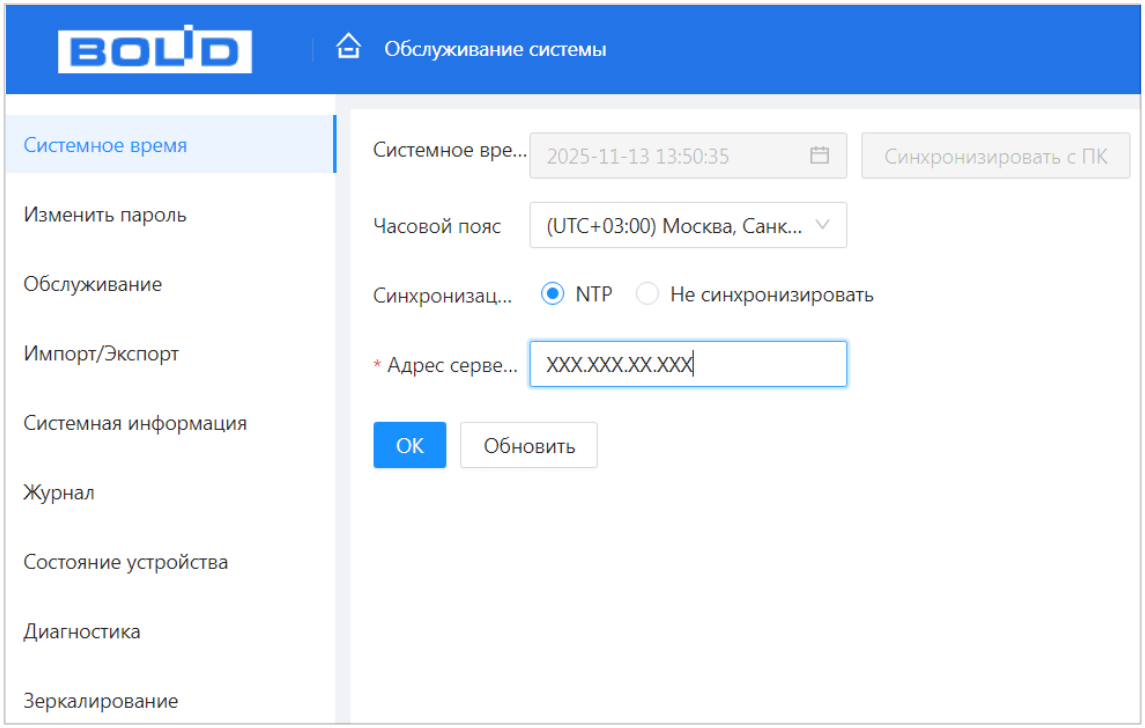


Рисунок 9.2 – Сихронизация с NTP-сервером

9.2 Подраздел «Изменить пароль»

Для изменения пароля учётной записи:

1. Введите старый пароль устройства в текстовое поле «Старый пароль» (Рисунок 9.3).

2. Введите новый пароль в 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 введённый пароль в текстовом поле «Подтверждение пароля».

4. Установите период действия пароля.

5. Нажмите кнопку «ОК» для сохранения.

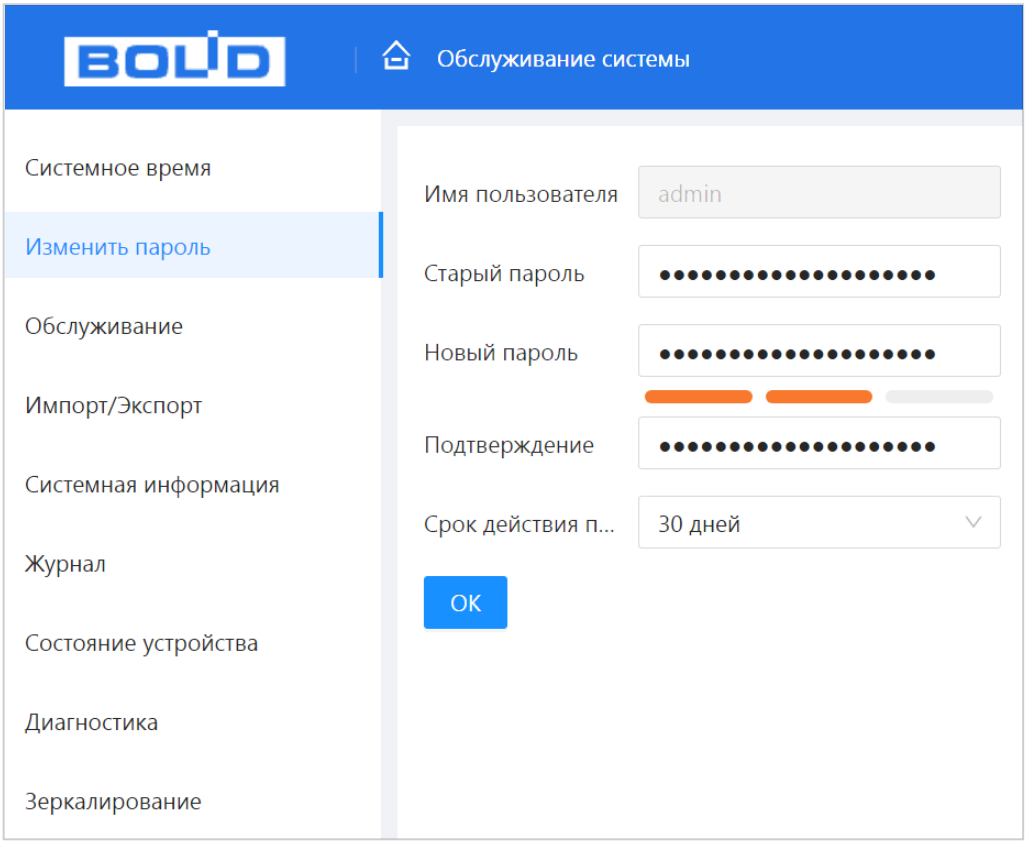


Рисунок 9.3 – Изменение пароля

9.3 Подраздел «Обслуживание»

Подраздел включает в себя несколько системных функций устройства.

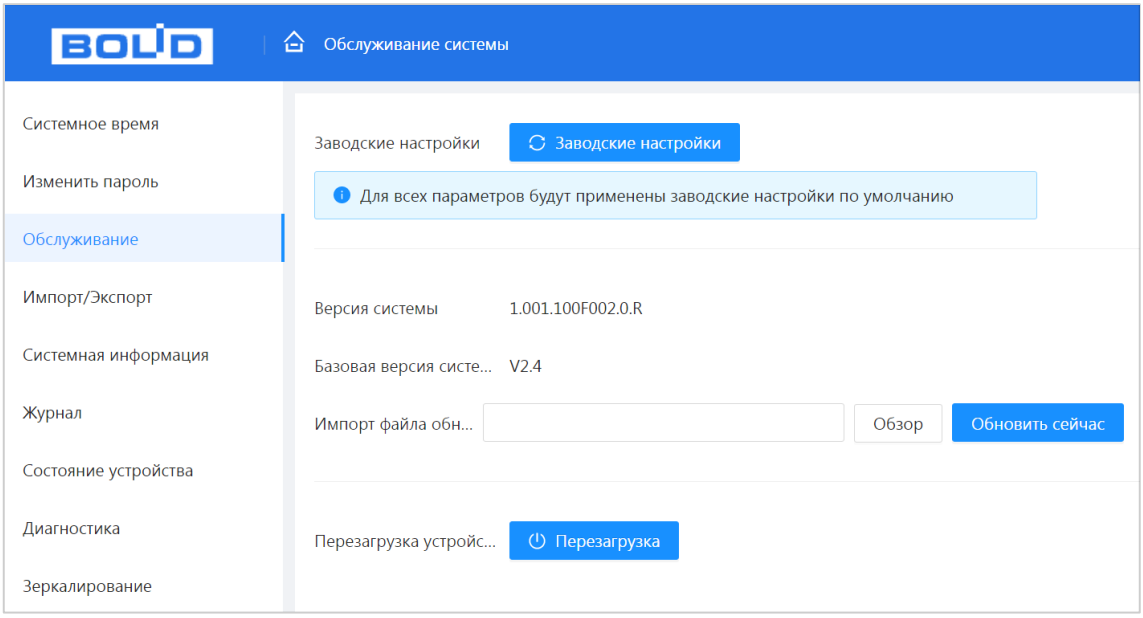


Рисунок 9.4 – Подраздел «Обслуживание»

1. Сброс на заводские настройки:

При нажатии кнопки «Заводские настройки» все ранее установленные настройки будут сброшены и восстановлены заводские настройки (подробнее и сбросе см. раздел – 15 Сброс на заводские настройки).

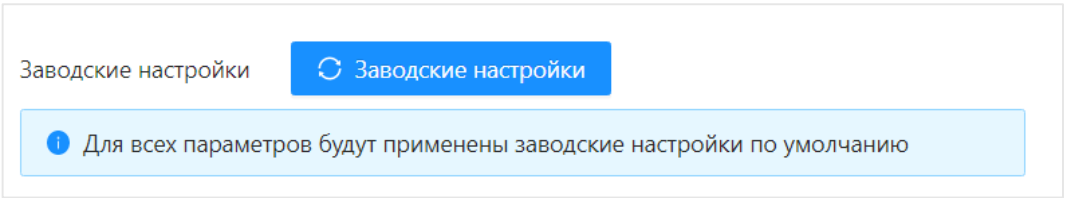


Рисунок 9.5 – Сброс

2. Обновление прошивки:

Для обновления ПО необходимо импортировать файл прошивки на устройство с помощью кнопки «Обзор».

И далее нажать кнопку «Обновить сейчас» для начала обновления.

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

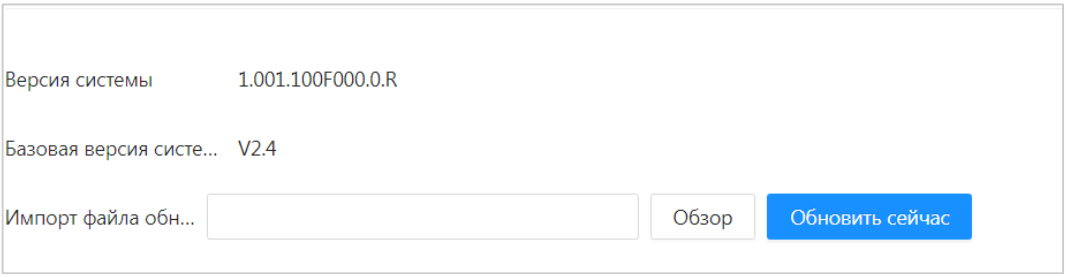


Рисунок 9.6 – Обновление

3. Перезагрузка устройства:

Нажмите кнопку «Перезагрузка» для выполнения программной перезагрузки устройства.

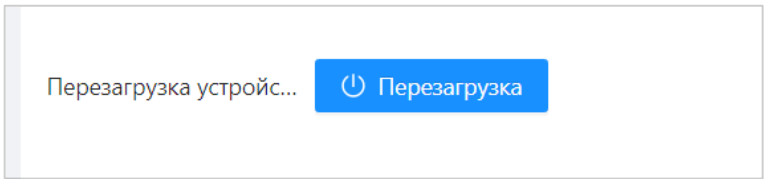


Рисунок 9.7 – Перезагрузка устройства

9.4 Подраздел «Импорт/Экспорт»

Данный подраздел используется для импорта или экспорта файла конфигурации.

СПРАВКА:
Файл конфигурации – совокупность настроек программы, задаваемые пользователем, а также процесс изменения этих настроек в соответствии с нуждами пользователя.

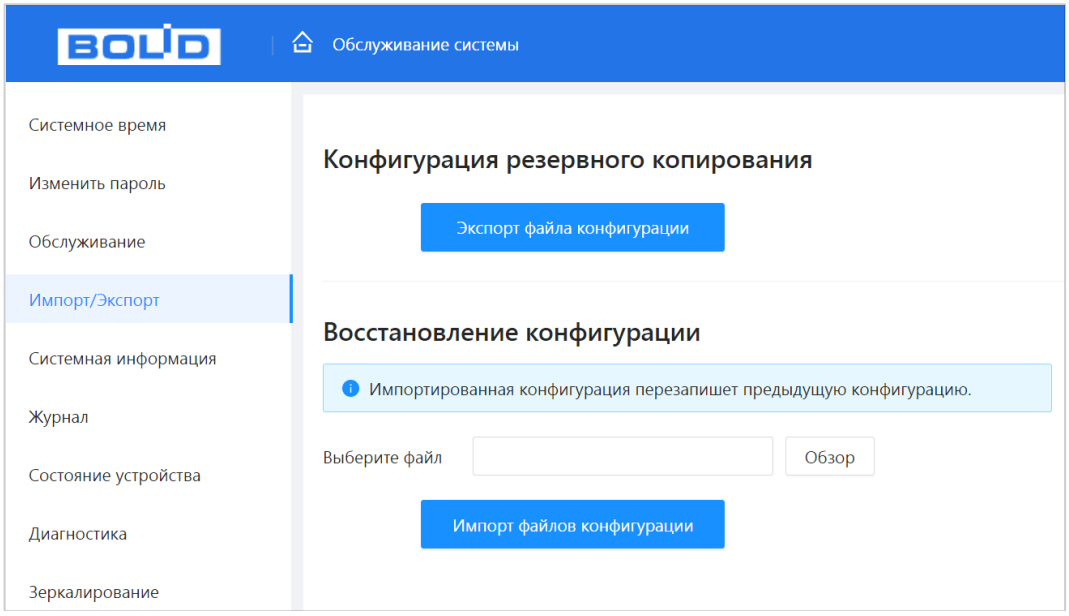


Рисунок 9.8 – Экспорт

9.4.1 Экспорт (Конфигурация резервного копирования)

Нажмите кнопку «Экспорт файла конфигурации» для сохранения файла конфигурации (настроек) коммутатора на ПК.

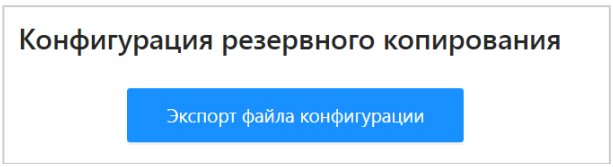


Рисунок 9.9 – Экспорт настроек с устройства

9.4.2 Импорт (Восстановление конфигурации)

1. Нажмите кнопку «Обзор» и выберите файл для загрузки совокупности ранее сохранённых настроек (Рисунок 9.10).

2. Нажмите кнопку «Импорт файлов конфигурации» и перезагрузите устройство.

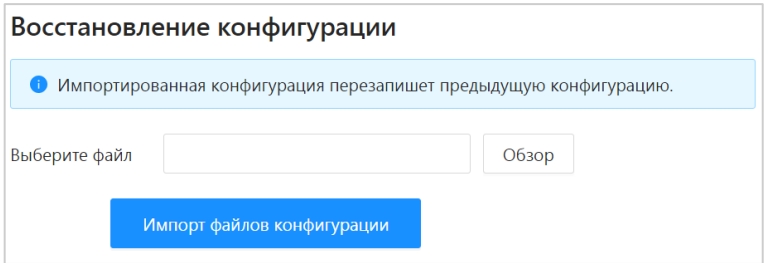


Рисунок 9.10 – Экспорт

9.5 Подраздел «Системная информация»

Раздел включает в себя ключевые системные данные об устройстве и установленном ПО.

Общая информация об устройстве включает в себя такие параметры как: Имя устройства, модель, серийный номер устройства и временные параметры работы.

Также отображаются сетевые параметры устройства, а именно: IP-адрес и MAC-адрес устройства.

Информация о ПО включает в себя информацию о версии и сборке установленного ПО.

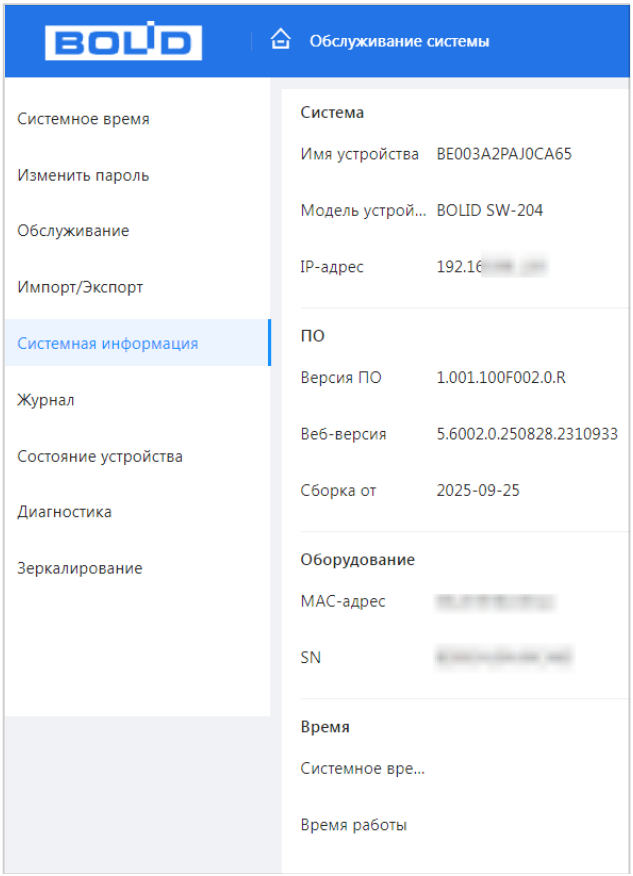


Рисунок 9.11 – Системная информация

9.6 Подраздел «Журнал»

Интерфейс предоставляет возможность просмотра и архивации информации из журнала устройства.

Для поиска записи необходимо задать начальное и конечное время, выбрать тип события (все, ошибка, предупреждение, сообщение) и нажать кнопку «Поиск».

В журнале хранится максимум 10000 записей (до 10 записей на каждой из страниц).

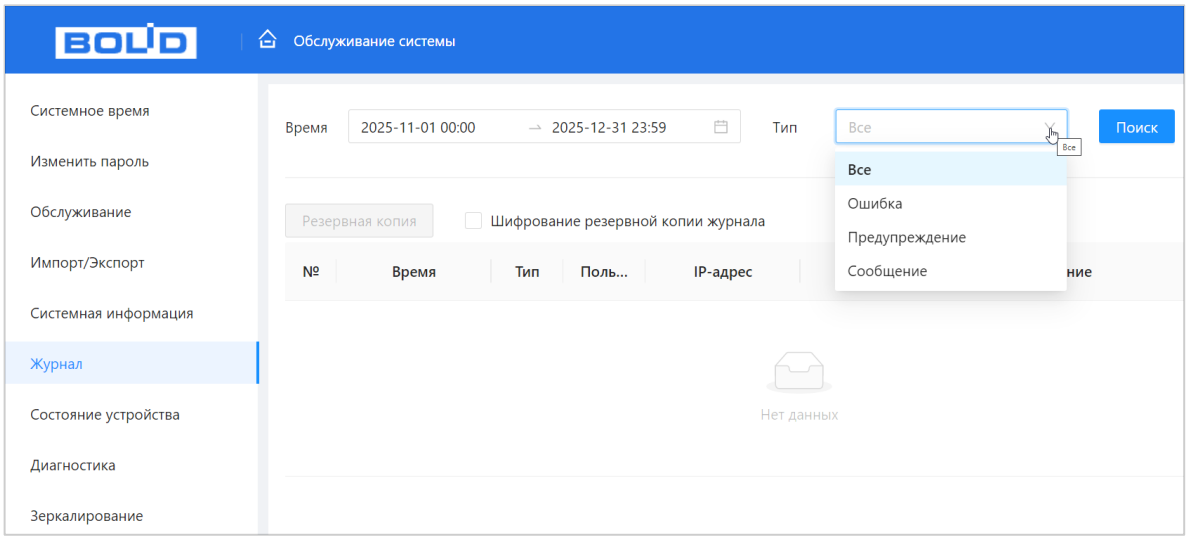


Рисунок 9.12 – Интерфейс просмотра журнала

9.7 Подраздел «Состояние устройства»

Отображение информации о состоянии CPU и памяти.

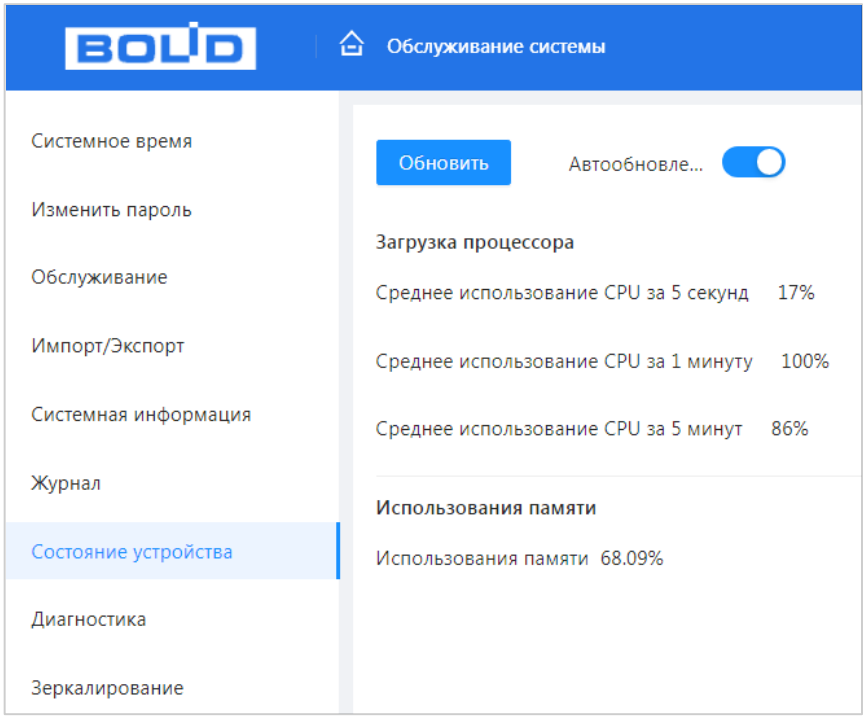


Рисунок 9.13 – Состояние устройства

9.8 Подраздел «Диагностика»

В подразделе выполняется диагностика состояния сетевого соединения до узла назначения. Для выполнения диагностики:

1. Введите IP-адреса назначения.
2. Из выпадающего списка установите размер отправляемого пакета.
3. Введите количество запросов (число повторов).
4. Нажмите кнопку «Диагностировать».

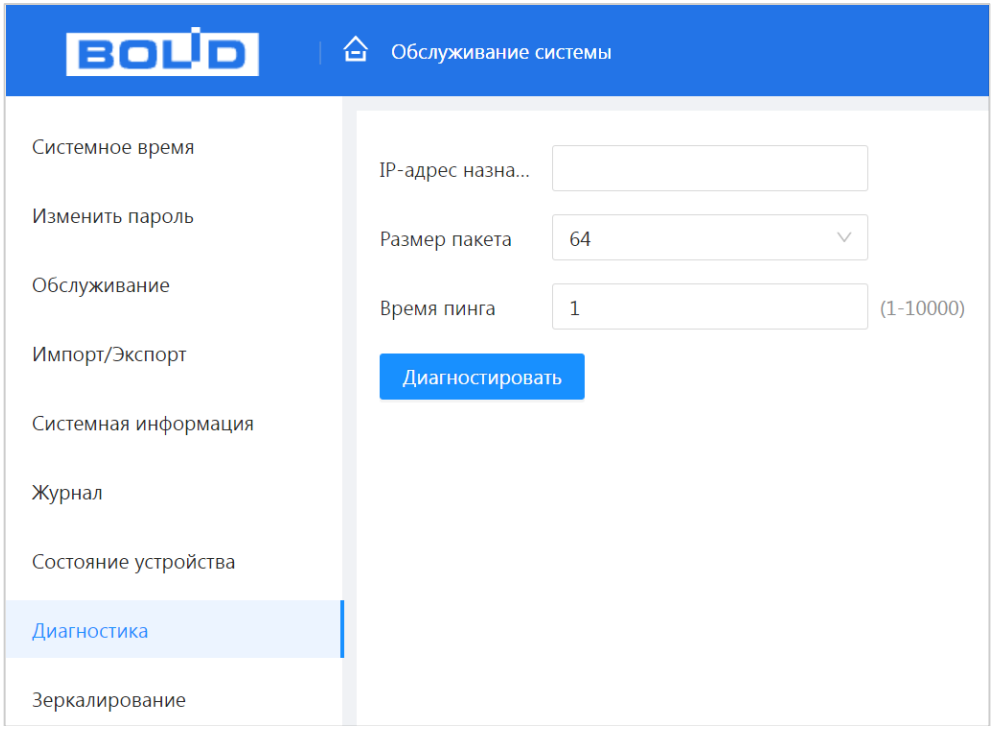


Рисунок 9.14 – Диагностика

Результат диагностики будет отображён в новом окне.

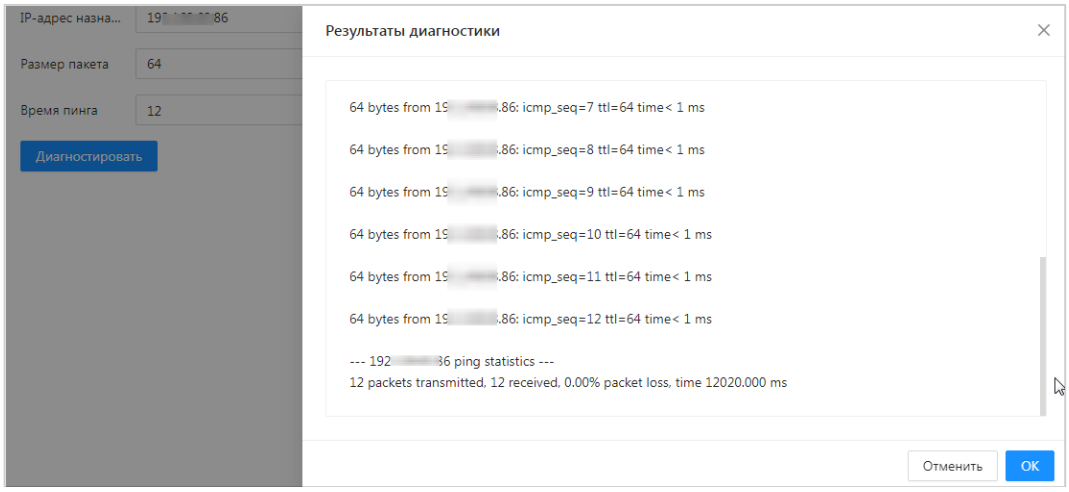


Рисунок 9.15 – Результат

9.9 Подраздел «Зеркалирование»

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

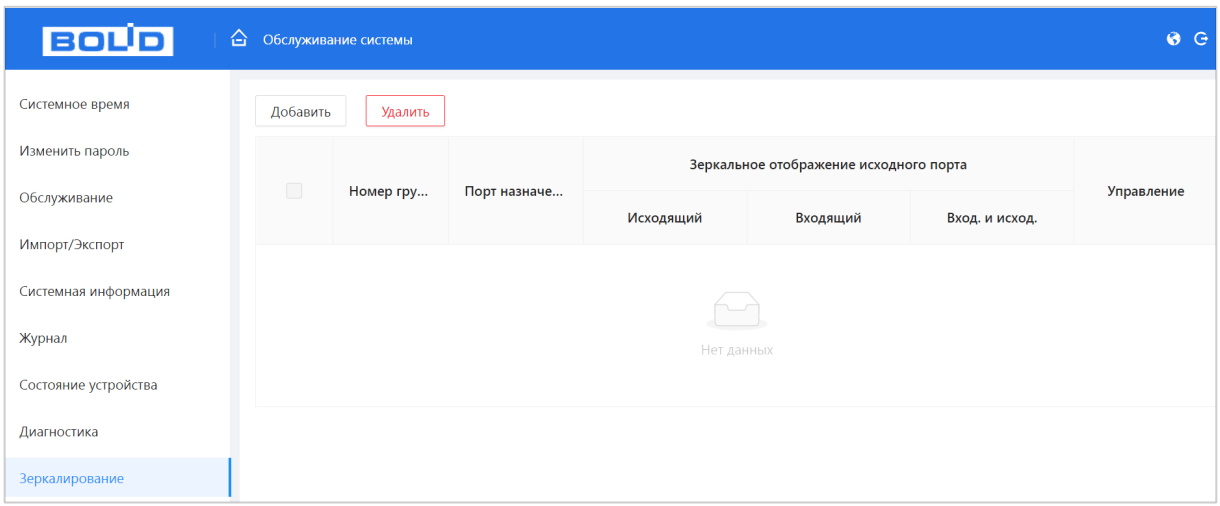


Рисунок 9.16 – Зеркалирование

Для включения данной функции необходимо:

1. Нажать кнопку «Добавить».

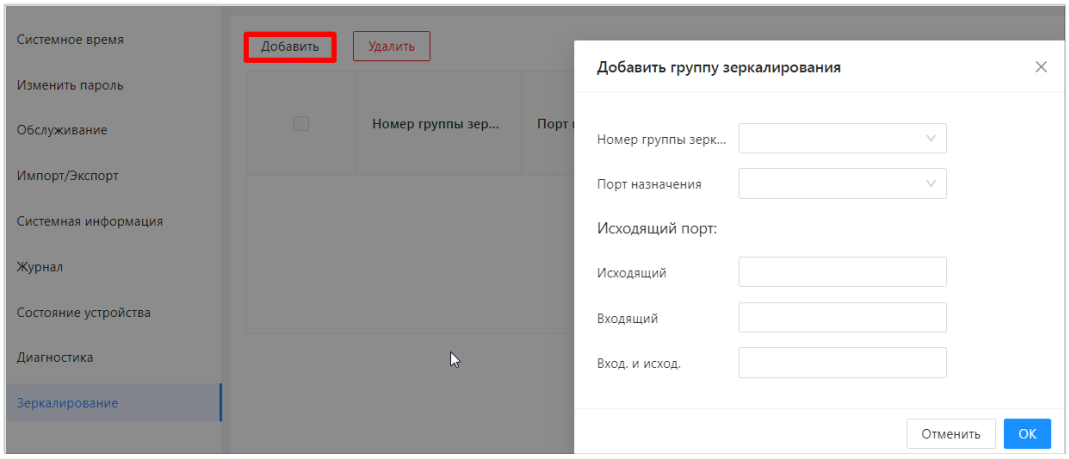


Рисунок 9.17 – Добавление

2. Выберите номер группы зеркалирования и порт назначения.

📖 Возможно зеркалировать только на 1 порт.

3. Далее установите режим передачи копий пакетов.

– Исходящий (TX Only) – пакеты, исходящие с этого порта будут отправлены на назначенный порт (порт-зеркало). Получаемые пакеты зеркалироваться не будут;

– Входящий (RX Only) – пакеты, полученные на этот порт, будут отправлены на назначенный порт (порт-зеркало). Исходящие пакеты зеркалироваться не будут;

– Вход. и исход. (Both) – и полученные и исходящие пакеты посылаются на назначенный порт (порт-зеркало).

10 РАЗДЕЛ ГЛАВНОГО МЕНЮ «СЕТЕВЫЕ НАСТРОЙКИ»

10.1 Подраздел «Порт»

На рисунке (Рисунок 10.1) показан интерфейс конфигурации портов коммутатора. Настройка конфигурации порта должна соответствовать практическим требованиям устройства.

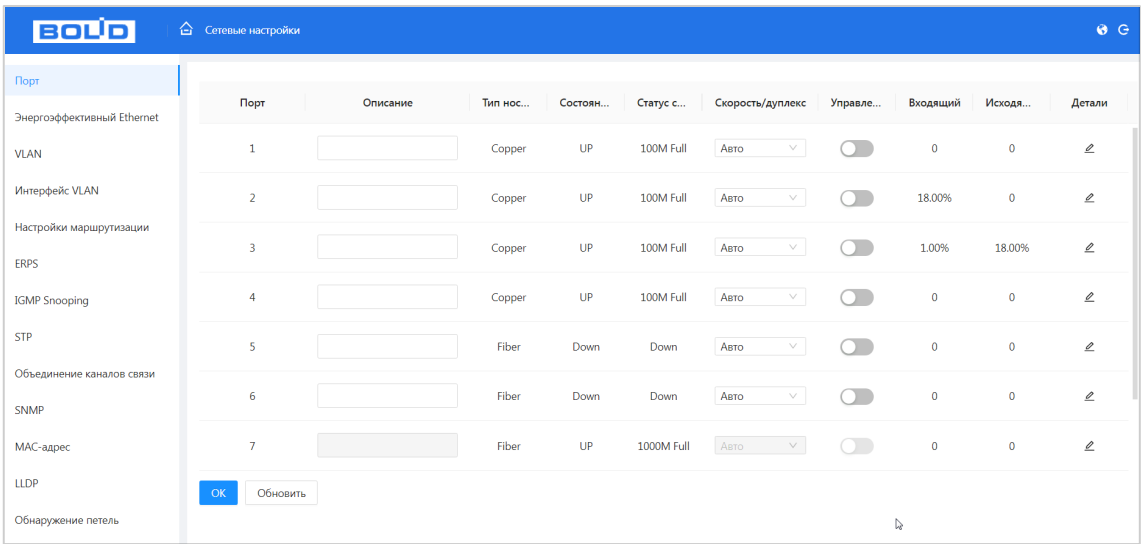


Рисунок 10.1 – Настройка портов

Таблица 10.1 – Настройка конфигурации портов

Столбец	Описание
Порт	Номер порта соответствует числу на лицевой панели.
Описание	Текстовое поле для ввода информации. Вводимая информация может состоять только из: цифр, латинских букв нижнего и верхнего регистра, символов: « _ », « – ». Пробелы и ввод иных знаков, кроме « _ » и « – » – запрещены. Допустимое количество символов ввода равно 16.
Тип носителя	Показывается тип подключенного носителя сигнала. – Copper – медный кабель; – Fiber – волоконно-оптический кабель.
Состояние соединения	– Up – порт подключен; – Down – порт отключен; – Disabled – порт выключен.

<table>
<tr><th colspan="2">Столбец</th><th colspan="3">Описание</th></tr>
<tr><td colspan="2">Статус скорости/дублирования</td><td colspan="3">Отображает текущее состояние скорости порта.</td></tr>
<tr><td rowspan="7">Скорость/ дуплекс</td><td colspan="4">Отображает текущее состояние скорости порта</td></tr>
<tr><td>Порт</td><td>Скорость</td><td colspan="2">Описание</td></tr>
<tr><td rowspan="5">Ethernet порт</td><td>Авто.</td><td colspan="2">Автоматическая настройка скорости и режима передачи.
📖 Рекомендовано для комбинированного порта.</td></tr>
<tr><td>10M FULL</td><td colspan="2">Скорость 10 Мб/с. Работа в режиме полного дуплекса.</td></tr>
<tr><td>10M HALF</td><td colspan="2">Скорость 10 Мб/с. Работа в режиме полудуплекса.</td></tr>
<tr><td>100M HALF</td><td colspan="2">Скорость 100 Мб/с. Работа в режиме полудуплекса.</td></tr>
<tr><td>100M FULL</td><td colspan="2">Скорость 100 Мб/с. Работа в режиме полного дуплекса.</td></tr>
<tr><td>Оптический порт</td><td>1000M FULL</td><td colspan="2">Скорость 1000 Мб/с. Работа в режиме полного дуплекса.</td></tr>
<tr><td colspan="2" rowspan="2">Управление потоком</td><td>Вкл.</td><td colspan="2">Включение функции управления потоком на порте.</td></tr>
<tr><td>Выкл.</td><td colspan="2">Выключение функции управления потоком на порте.</td></tr>
<tr><td colspan="2">Входящий</td><td colspan="3">Отображение текущего состояния приема пакетов.</td></tr>
<tr><td colspan="2">Исходящий</td><td colspan="3">Отображение текущего состояния отправки пакетов.</td></tr>
</table>

Для отображения более подробной информации нажмите кнопку в столбце «Детали».

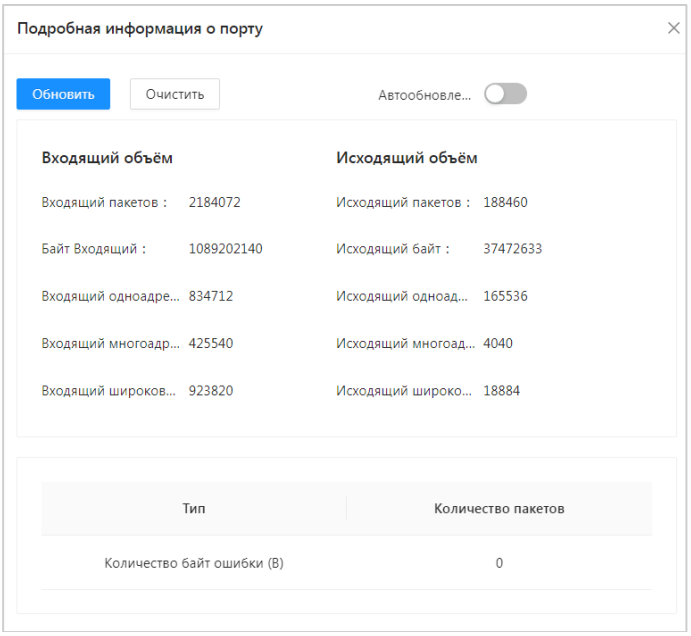


Рисунок 10.2 – Подробная информация о порту

10.2 Подраздел «Энергоэффективный Ethernet (EEE (Energy Efficient Ethernet))»

Energy Efficient Ethernet (EEE) – это стандарт, разработанный для снижения потребления энергии сетевыми устройствами путём автоматического переключения портов в режим низкого энергопотребления, когда они не используются. Правильная настройка EEE позволяет снизить затраты на электроэнергию и увеличить срок службы оборудования.

Для включения функции установите флажок и нажмите кнопку «ОК».

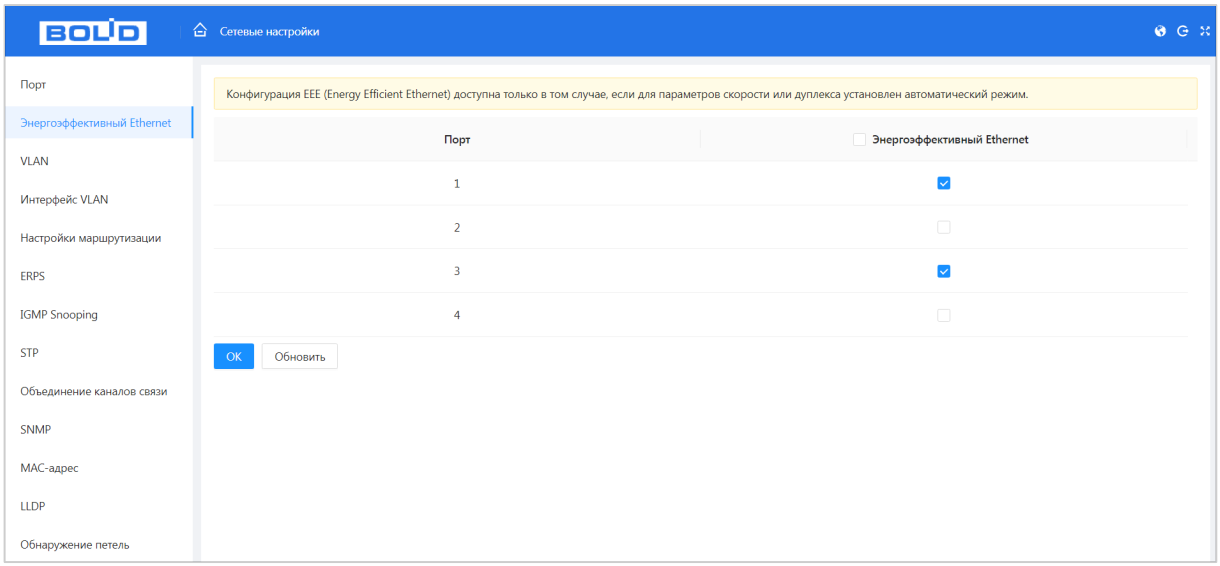


Рисунок 10.3 – Конфигурация EEE

10.3 Подраздел «VLAN»

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

10.3.1 Пункт «Добавить 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 10.4).

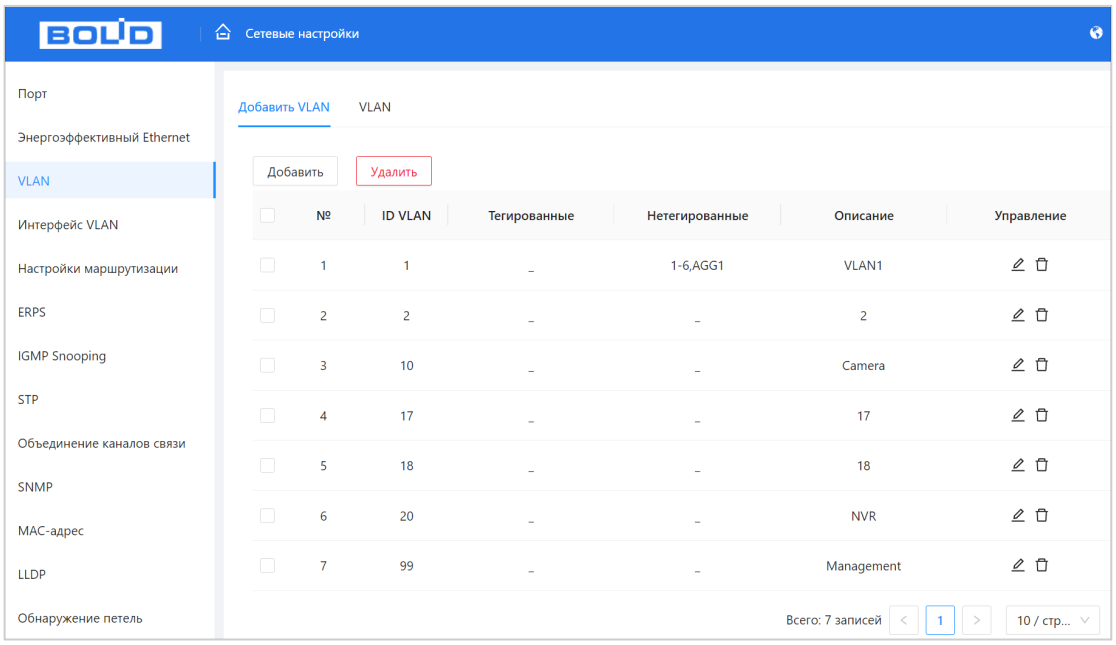


Рисунок 10.4 – Создание VLAN

Для создания VLAN на устройстве нажмите кнопку «Добавить» (Рисунок 10.5). В появившемся диалоговом окне (Рисунок 10.5) заполните текстовые поля «VLAN ID» и «Описание» (Таблица 10.2), нажмите кнопку «Сохранить». На первом этапе конфигурации VLAN столбец «Нетегированные» будет пуст, для добавления участников VLAN перейдите в пункт «VLAN».

📖 VLAN 1 не может быть удалён.

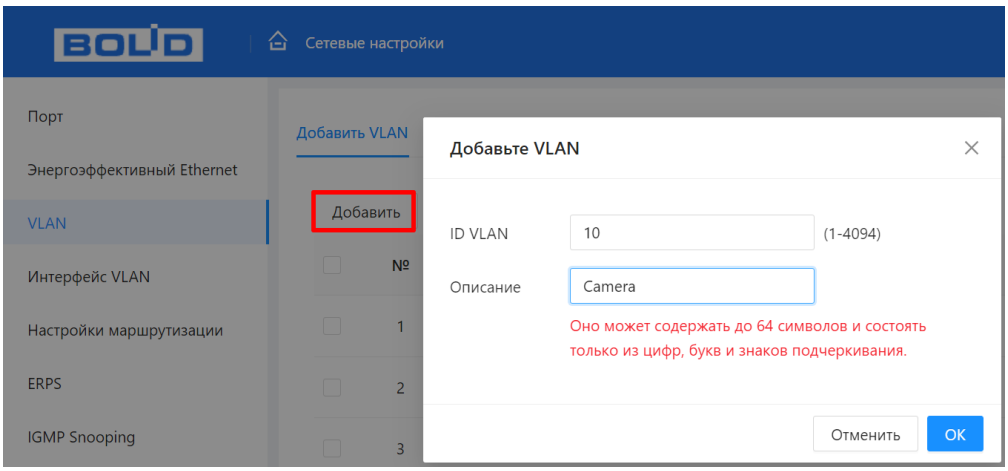


Рисунок 10.5 – Создание VLAN

Таблица 10.2 – 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.

10.3.2 Пункт «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.

ПРИМЕЧАНИЕ!
Одновременное включение функций «Изолирование портов» и «VLAN» невозможно.

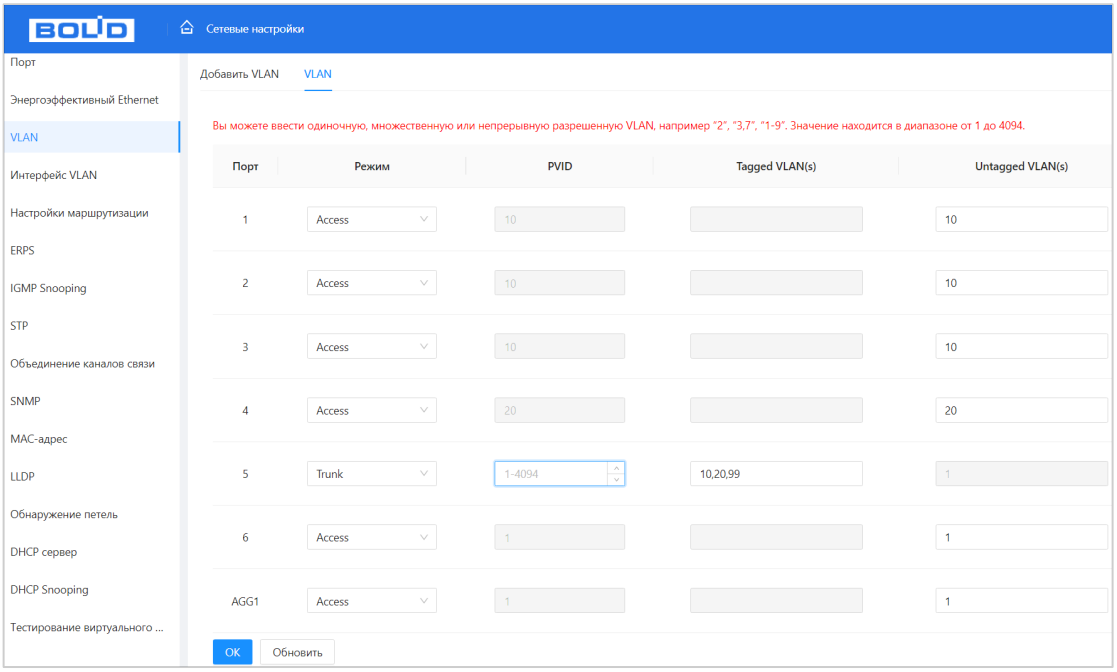


Рисунок 10.6 – Конфигурирование VLAN-порта

Таблица 10.3 – Конфигурирование VLAN-порта

Столбец	Описание
Порт	Столбец отображает физический порт устройства.
Режим	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 «Tagged VLAN(s)»; – «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.
PVID	Идентификатор порта VLAN.
Tagged VLAN(s)	Установите идентификатор VLAN для порта, которому разрешено тегировать пакеты при их отправке.
Untagged VLAN(s)	Установите идентификатор VLAN для порта, которому разрешено не тегировать пакеты при их отправке.

10.4 Подраздел «Интерфейс VLAN (VLANIF)»

Производится настройка логического интерфейса VLAN, который используется для связи между различными VLAN в сетевых устройствах.

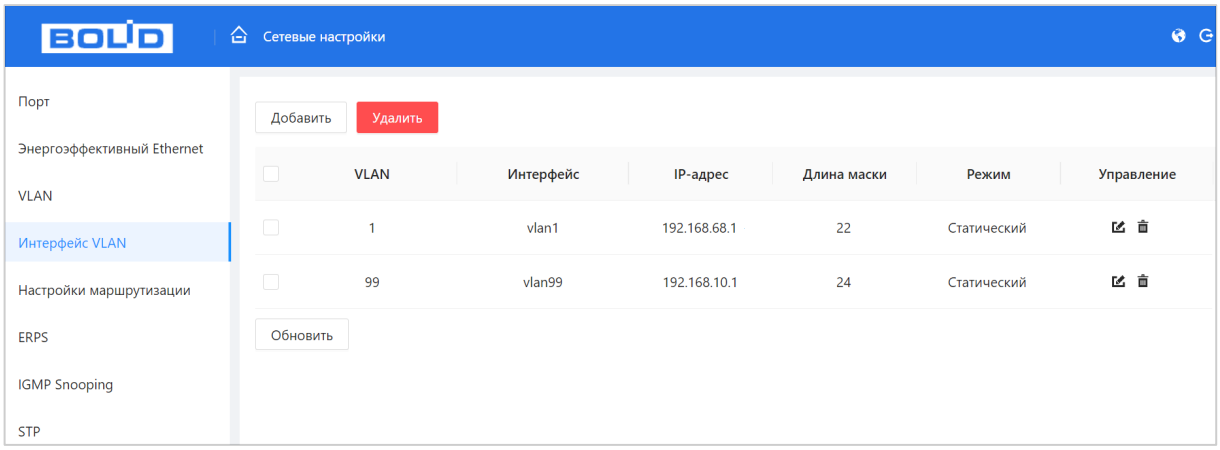


Рисунок 10.7 – VLAN интерфейс

Для добавления нажмите кнопку «Добавить». В появившемся окне введите номер VLAN, затем либо активируйте DHCP для интерфейса с режимом «Динамический IP». Если DHCP-сервер в VLAN отсутствует, можно задать IP-адрес и маску подсети вручную.

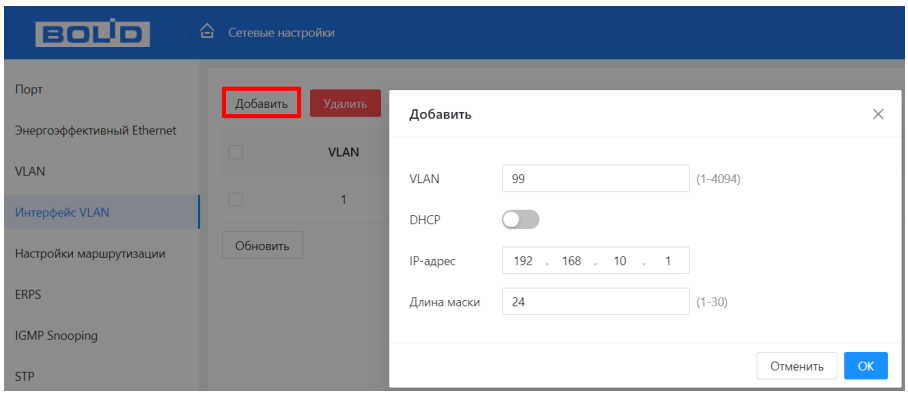


Рисунок 10.8 – Добавление

Таблица 10.4 – Настройка маршрутизации на устройстве. Добавление IP

Параметр	Функция
VLAN	Поле ввода номера VLAN.
DHCP	Активация DHCP-сервера.
IP-адрес	Поле ввода IP-адреса добавляемого VLAN.
Префикс подсети (Длина маски)	Поле ввода маски подсети.

10.5 Подраздел «Настройки маршрутизации»

В этом разделе представлены настройки маршрутизации коммутатора.

Для настройки нажмите кнопку «Добавить» и заполните поля.

📖 Данная модель поддерживает только маршрут по умолчанию.

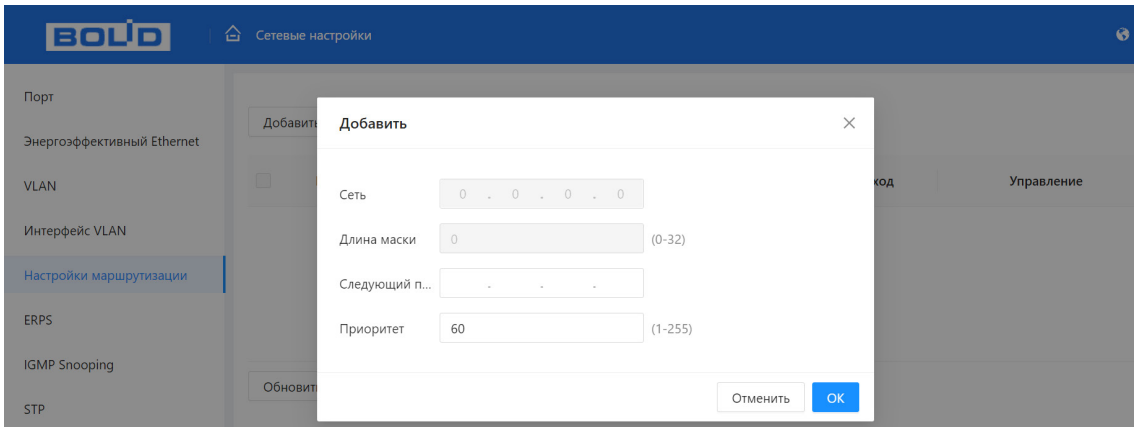


Рисунок 10.9 – Настройки маршрутизации

Таблица 10.5 – Настройка маршрутизации на устройстве. Добавление маршрута

Параметр	Функция
Сеть	IP-сеть назначения или адрес хоста этого маршрута.
Префикс подсети (Длина маски)	Поле ввода маски подсети.
Следующий узел	IP-адрес следующего перехода маршрута.
Метрика (Приоритет)	Используется для выбора маршрута с наименьшим значением метрики

10.6 Подраздел «ERPS»

ERPS (Ethernet Ring Protection Switching) – сетевой протокол, использующийся для предотвращения образования петель в топологии типа «Кольцо» методом отключения порта. Протокол используется только в кольцевой топологии и обладает лучшей сходимостью (порядка 50 – 200 мс), чем протоколы семейства STP у которых время сходимости достигает 30 – 50 с для STP и 4 с для RSTP. Данный протокол не способен определять топологию, отличную от настроенной, что позволяет так быстро реагировать, но при этом требует включения (где это необходимо) дополнительных мер, таких как, например, «Борьба с петлями».

10.6.1 Пункт «ERPS»

Для добавления экземпляра ERPS нажмите кнопку «Добавить». В появившемся окне введите параметры для создаваемого ERPS (Таблица 10.6).

ПРИМЕЧАНИЕ!
Перед использованием ERPS необходимо отключить STP на портах, так как они являются взаимоисключающими.

ПРИМЕЧАНИЕ!
ERPS и IGMP Snooping не могут быть включены одновременно.

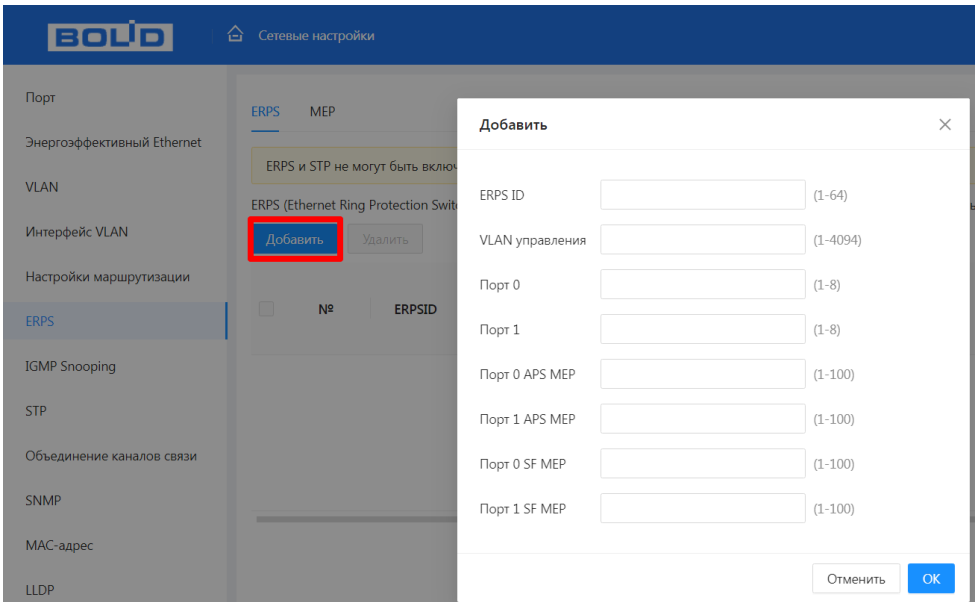


Рисунок 10.10 – Добавление ERPS

Таблица 10.6 – Параметры добавления ERPS

Параметр	Функция
ERPS ID	Поле ввода идентификатора для создания группы защиты, допустимые значения ввода от 1 до 64. Нажмите на идентификатор группы защиты, чтобы перейти на страницу конфигурации, более подробную информацию смотрите ниже (Рисунок 10.11).
Упр. VLAN	Управляющая VLAN
Порт 0 (Запад/ WEST порт)	Поле ввода выбранного порта коммутатора для выполнения роли «Port 0» в топологии ERPS. Только один порт коммутатора может быть выбран для выполнения роли ERPS Port 0.
Порт 1 (Восток/ EAST порт)	Поле ввода выбранного порта коммутатора для выполнения роли «Port 1» в топологии ERPS. Только один порт коммутатора может быть выбран для выполнения роли ERPS Port 1.
Порт 0 APS MEP	PDU порта 0 APS MEP.
Порт 1 APS MEP	PDU порта 1 APS MEP. Поскольку только один APS MEP связан со взаимосвязанным вспомогательным кольцом без виртуального канала, он настроен как «0» для таких экземпляров кольца. «0» в этом поле указывает, что с этим экземпляром не связан порт 1 APS MEP.
Порт 0 SF MEP	Порт 0 SF MEP сообщает об обнаружение сбоя.
Порт 1 SF MEP	Порт 1 SF MEP сообщает об обнаружение сбоя. Поскольку только один SF MEP связан с взаимосвязанным субкольцом без виртуального канала, он настроен как «0» для таких случаев вызова.

Нажмите на цифру в столбце «ERPS ID» для перехода к окну настройки экземпляра ERPS (Рисунок 10.11, Таблица 10.7).

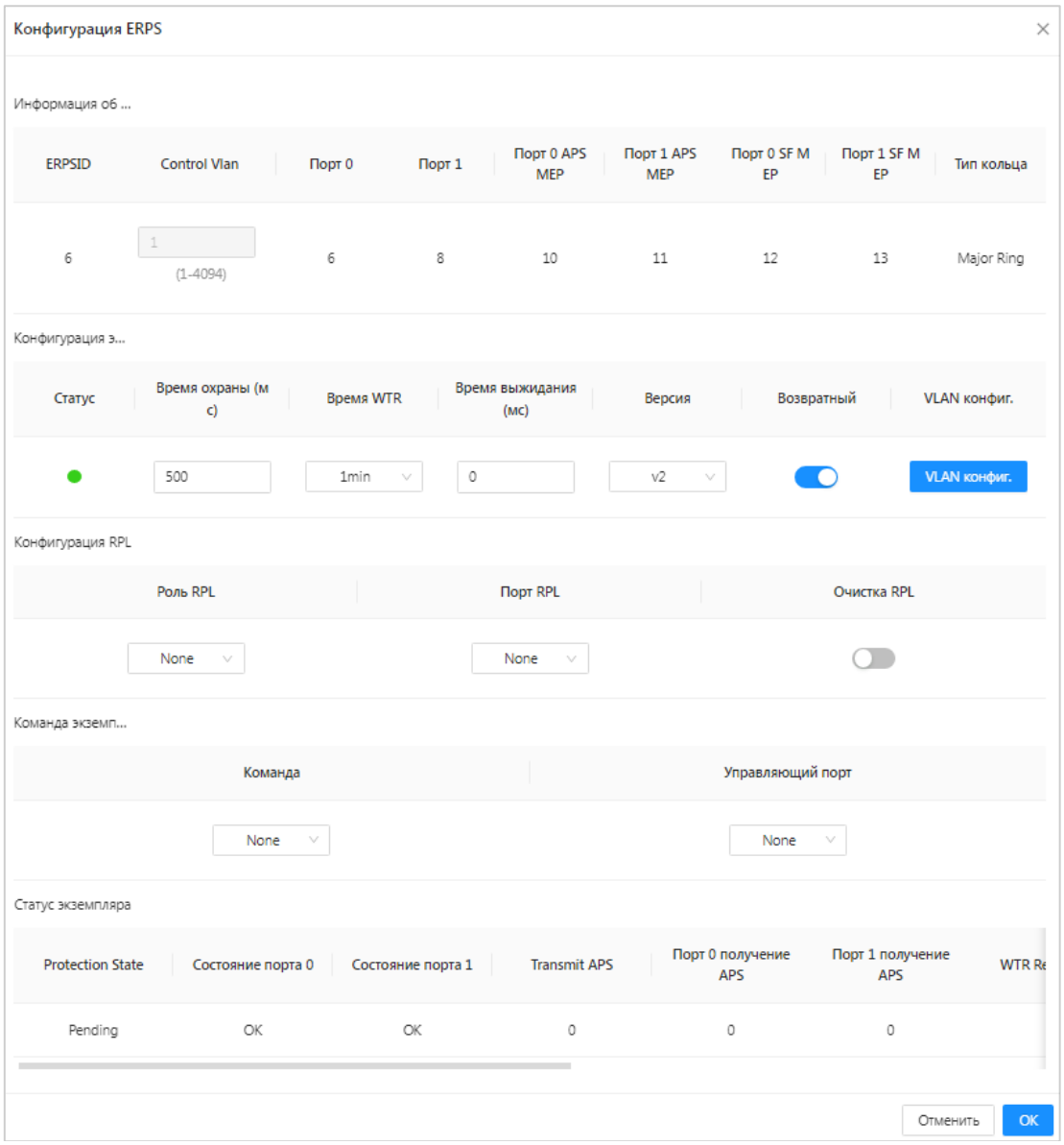
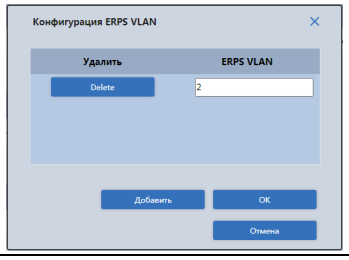


Рисунок 10.11 – Настройка экземпляра ERPS

Таблица 10.7 – Параметры конфигурации ERPS

Параметр	Функция	
Информация об экземпляре	ERPS ID	Панель отображает ранее заданные параметры, более подробно каждый параметр описан в таблице выше (Таблица 10.6).
	Control Vlan	
	Порт 0	
	Порт 1	
	Порт 0 APS MEP	
	Порт 1 APS MEP	
	Порт 0 SF MEP	
	Порт 1 SF MEP	
	Тип кольца	Тип работы защитного кольца: Major ring – основное кольцо; Sub-ring – субкольцо.

Параметр	Функция	
Конфигурация экземпляра	Статус	Статус состояния.
	Время охраны (мс) (Guard Time)	Поле ввода времени игнорирования узлом R-APS сообщений после восстановления аварийного соединения. Используется для предотвращения получений кольцевыми узлами устаревших сообщений R-APS. Когда узел обнаруживает, что аварийное соединение восстановилось, он отсылает сообщение R-APS PDU с NR флагом и запускает время охраны (Guard Timer). Установленное время должно быть больше, чем максимальная возможная задержка передачи, в течение которой одно R-APS сообщение обойдёт все кольцо. По умолчанию значение – 500 мс.
	Время WTR (Wait to restore)	Из выпадающего списка выберите время до восстановления R-APS. Параметр нужен для того, чтобы предотвратить частое переключение RPL порта, если соединение на каком-то участке кольца очень часто меняет состояние. Таймер используется только узлом RPL_Owner. Доступный диапазон значений 1 – 12 мин, по умолчанию значение – 1 мин.
	Время выжидания (мс) (Hold-Off Time)	Поле ввода времени между тем как узел обнаружил аварию на одном из своих соединений до отправки им сообщения Signal Fail (SF). Диапазон значений от 0 до 10 секунд с шагом в 100 мс. По умолчанию значение – 0.
	Версия	Из выпадающего списка выберите версию протокола ERPS: v1 – поддерживает топологию с одним кольцом; v2 – поддерживает топологию с несколькими кольцами/многозвенной схемой.

Параметр	Функция	
	Возвратный (реверсивный)	Поставьте переключатель в зависимости от настроек в состояние Вкл./Выкл. – реверсивный режим ERPS отключен;  – реверсивный режим ERPS включен.
	VLAN конфиг.	Нажмите кнопку «VLAN конфиг.» для создания R-APS VLAN. Создаётся VLAN для передачи пакетов ERPS, для контроля кольца и поддержки его рабочих функций. В появившемся окне нажмите кнопку «Добавить». В поле ввода введите номер VLAN. 
Конфигурация RPL (Ring Protection Link/Канал защиты кольца)	Роль RPL	None – роль RPL для коммутатора не выбрана. Участвующие в кольце коммутаторы, которые находятся рядом с владельцем или соседом RPL в кольце, называются участниками кольца. Основная функция этих коммутаторов – пересылать полученный трафик.
		RPL_Owner – коммутатор назначается владельцем RPL. Отвечает за блокировку трафика по RPL в нормальном режиме работы и для разблокирования трафика при разрыве кольца.
		RPL_Neighbour – коммутатор назначается «соседом (соседний узел кольца)» RPL для кольца. Отвечает за блокировку своего конца RPL в нормальных условиях.
	Порт RPL	None – порт не выбран.

<table>
<tr><th>Параметр</th><th colspan="3">Функция</th></tr>
<tr><td rowspan="2"></td><td rowspan="2"></td><td>Port0 (Запад/ WEST порт)</td><td rowspan="2">Один из кольцевых портов коммутатора назначается как RPL-порт (канал защиты кольца (Ring Protection Link, RPL)). Трафик на порте блокируется при нормальной работе. Если произойдёт разрыв связи на кольце, то через работающий порт будет получено служебное сообщение об обрыве и тем самым RPL_Owner будет извещён, далее будет включен заблокированный порт.
При восстановлении сигнала на порту в состоянии «Down» коммутатор блокирует его на время, указанное в параметре WTR, чтобы при нестабильном сигнале с этого порта не приходилось постоянно перестраивать топологию.</td></tr>
<tr><td>Port1 (Восток/ EAST порт)</td></tr>
<tr><td>Очистка RPL</td><td colspan="2">Включение/выключение очистки RPL. Используется для пометки ERPS для удаления при следующей операции сохранения.</td></tr>
<tr><td rowspan="3">Команда экземпляра</td><td rowspan="3">Команда</td><td colspan="2">None – команда не выбрана.</td></tr>
<tr><td colspan="2">Manual Switch (MS) – команда принудительной блокировки порта экземпляра вручную. Используется при сбое соединения и при отсутствии настроек «Forced Switch».</td></tr>
<tr><td colspan="2">Forced Switch (FS) – команда принудительной блокировки порта экземпляра. Порт блокируется вне зависимости от того, произошёл ли разрыв соединения, или нет.</td></tr>
</table>

Параметр	Функция		
		Clear – команда удаления последствий после применения команда FS и MS. запускает реверсивное переключение до момента истечения WTR timer/WTB timer в реверсивном режиме работы; запускает реверсивное переключение в нереверсивном режиме работы.	
	Управляющий порт	None – порт не выбран.	
		Port0	Порт0 или Порт1 группы защиты, к которому применяется команда.
		Port1	
Состояние экземпляра	Состояние защиты	Состояние ERPS в соответствии с таблицами перехода состояний в G.8032.	
	Состояние порта 0	OK – нормальное состояние; SF – сбой.	
	Состояние порта 1		
	Передано APS	Передаваемые точки доступа в соответствии с таблицами перехода состояний в G.8032.	
	Порт 0 получение APS	Принятые точки доступа на порту о или 1 в соответствии с таблицами перехода состояний в G.8032.	
	Порт 1 получение APS		
	Осталось WTR	Оставшийся таймаут WTR в миллисекундах.	
	RPL разблокирован	Точки доступа принимаются в рабочем потоке.	
	Ни одного APS не получено	Состояние блокировки порта 0 или 1 (состояние блокировки как трафика, так и R-APS). Канал R-APS никогда не блокируется на вспомогательных кольцах без виртуального канала.	
	Порт 0 статус блокировки		
	Порт 1 статус блокировки		
	FOP тревога	Сбой состояния протокола (FOP).	

10.6.2 Пункт «MEP»

MEP (Maintenance Entity Point) является частью ERPS. Устройство уровня 2, добавленное в ERPS, называется узлом. Добавляйте не более двух портов в ERPS для каждого узла.

Для добавления MEP нажмите кнопку «Добавить». В появившемся окне введите параметры для создаваемого MEP (Таблица 10.8).

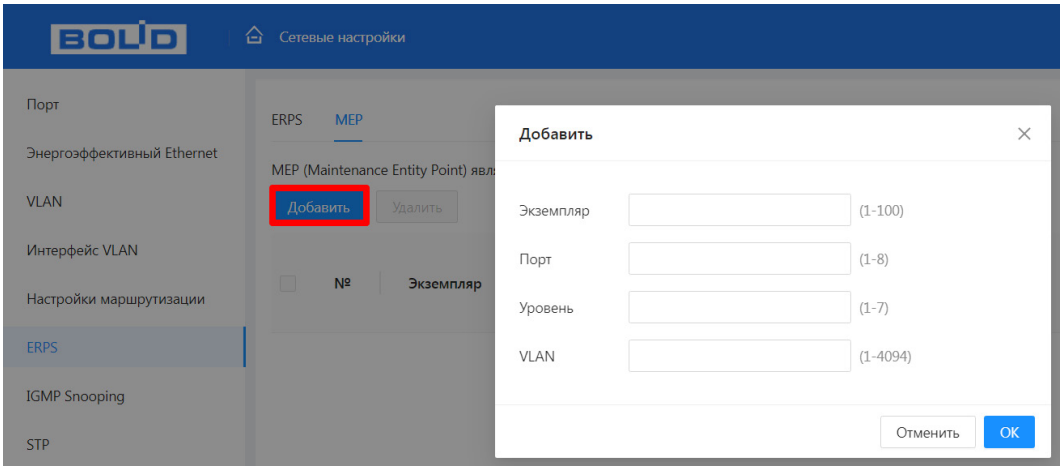


Рисунок 10.12 – Добавление MEP

Таблица 10.8 – Параметры добавление MEP

Параметр	Функция
Экземпляр	Поле ввода номера экземпляра MEP. Доступный диапазон от 1 до 1077.
Порт	Поле ввода номера порта, которому будет принадлежать MEP. Доступный диапазон от 1 до 36.
Уровень	Поле ввода уровня обслуживания. Доступный диапазон от 0 до 7.
VLAN	Поле ввода ранее настроенного протокола VLAN, например, VLAN 3. Доступный диапазон от 1 до 4094.

Нажмите кнопку в столбце «Управление» для перехода в окно конфигурации MEP (Рисунок 10.13, Таблица 10.9).

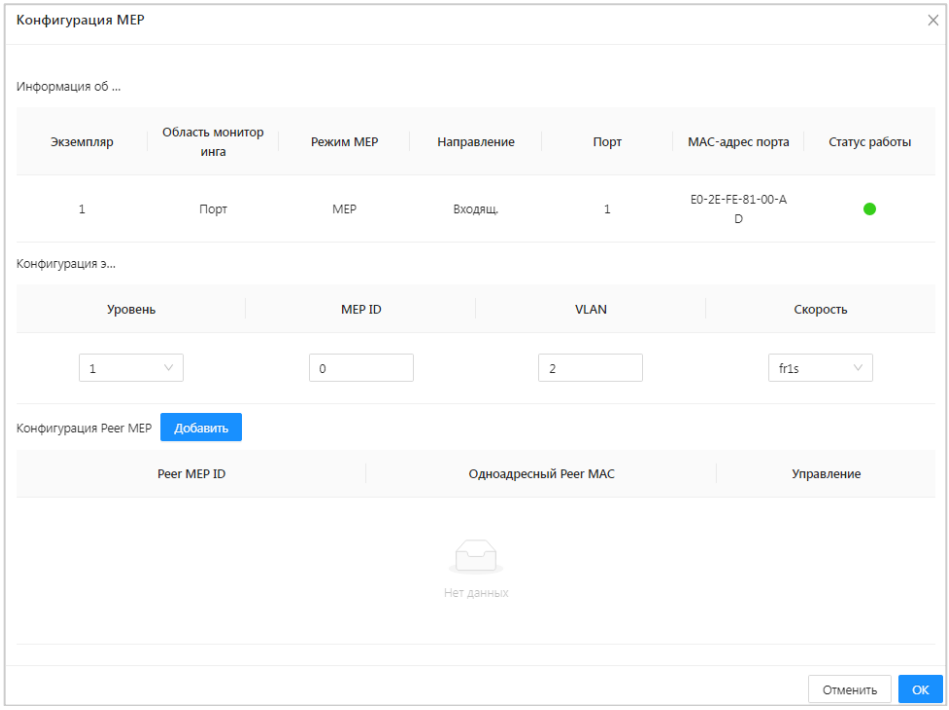


Рисунок 10.13 – Конфигурация MEP

Таблица 10.9 – Параметры настройки MEP

Параметр	Функция	
Информация об экземпляре	Экземпляр	Панель отображает ранее заданные параметры, более подробно каждый параметр описан в таблице выше (Таблица 10.8).
	Область мониторинга	
	Режим MEP	
	Направление	
	Порт	
	MAC-адрес порта	
	Статус работы	
Конфигурация экземпляра	Уровень	Выберите из выпадающего списка уровень MGP настраиваемого MEP.
	MEP ID	Идентификатор MEP.
	VLAN	Номер тегированной VLAN. Для VLAN с этим VID будет добавлен C-tag или Stag (в зависимости от типа порта VLAN). Если добавление тега не требуется, введите 0.
Конфигурация Peer MEP	Peer MEP ID	Идентификатор однорангового MEP целевого MEP. Используется только, когда одноадресный MAC-адрес однорангового устройства состоит из одних нулей.

Параметр	Функция	
	Одноадресный Peer MAC	Отображается одноадресный MAC-адрес одноранговой устройства состоит из одних нулей. (MAC-адрес одноадресного одноранговой устройства): Одноадресный MAC-адрес целевого коммутатора или устройства. Вы можете ввести одноадресный MAC-адрес в формате «xx:xx:xx:xx:xx:xx», где x – шестнадцатеричная цифра. ПРИМЕЧАНИЕ: Когда задано содержимое поля «Peer MEP ID(Идентификатор одноранговой MEP)», устройство может осуществлять автосогласование параметров с соседним устройством (по MAC-адресу). Поэтому, пользователь при начальном конфигурировании может задать в поле «Одноадресный Peer MAC (Одноадресный MAC-адрес одноранговой устройства)» одни нули, то есть «00:00:00:00:00:00».
	Удалить	Нажмите кнопку «Delete» для удаления созданного «Peer MEP»

10.7 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 её членов (для ретрансляции группового трафика). И наоборот: услышав запрос «IGMP Leave» (покинуть), удаляет соответствующий порт из списка группы.

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

При использовании Multicast рассылки, возможно, включить поддержку «IGMP Fast leave(Отбрасывание неизвестных многоадресных пакетов)», которая позволяет коммутатору быстрее исключать порт из списка участников соответствующей группы. Для целей видеонаблюдения её включение не обязательно.

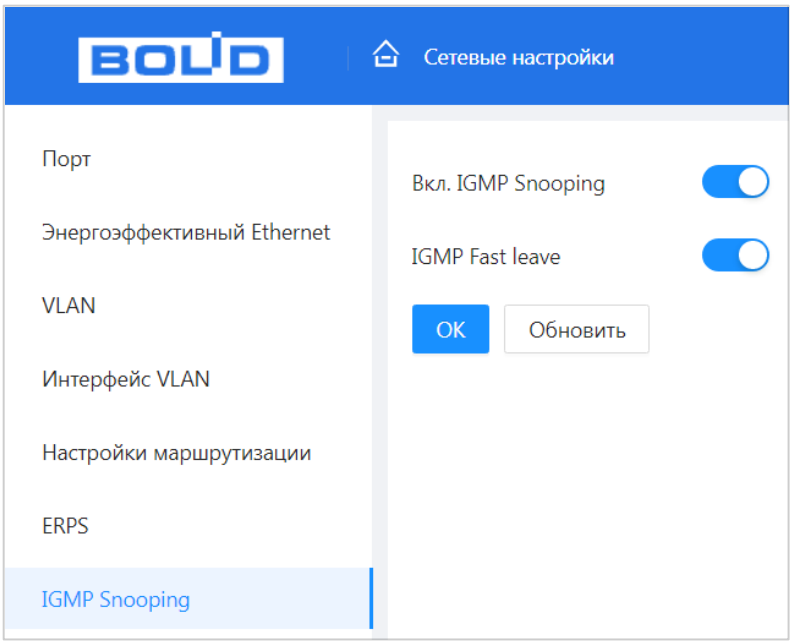


Рисунок 10.14 – Интерфейс IGMP Snooping

10.8 Подраздел «STP»

10.8.1 Пункт «STP»

На рисунке ниже (Рисунок 10.15) изображён интерфейс изменения настроек STP и протокола его работы.

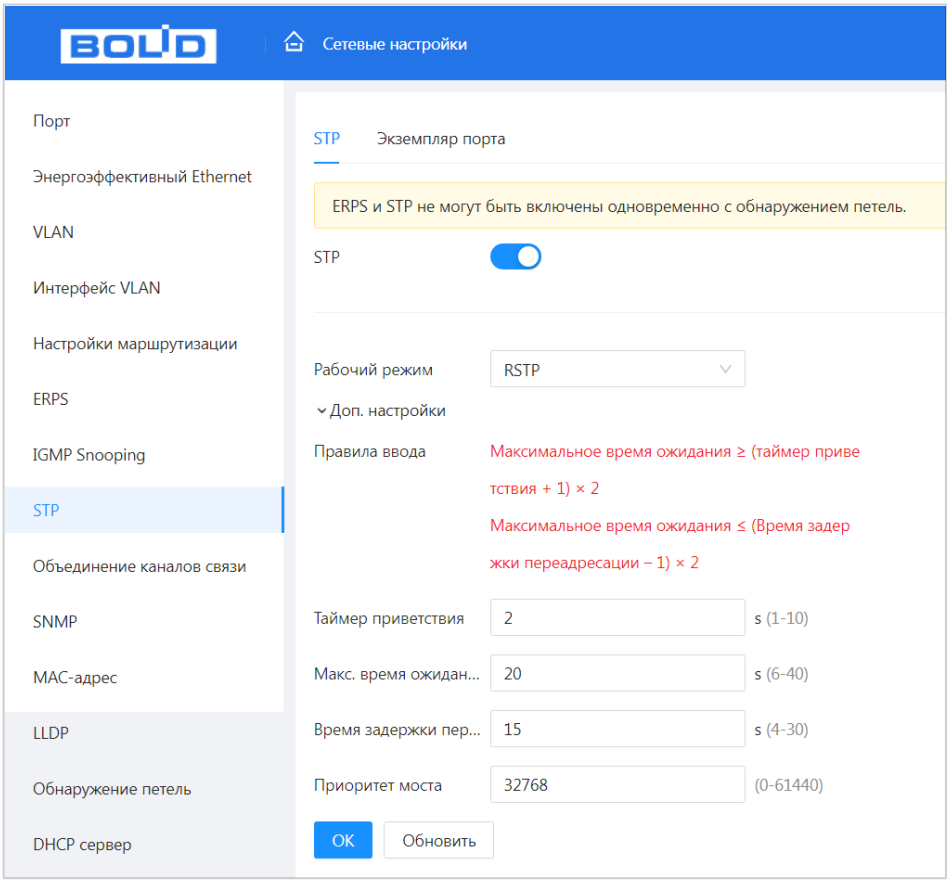


Рисунок 10.15 – Настройка STP

Таблица 10.10 – Параметры настройки STP

Параметр	Функции
Рабочий режим	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.
Таймер 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.
Маск. время ожидания	Установите время, которое устройство может простаивать, не получая конфигурационного сообщения, прежде чем попытается перенастроиться. Параметры времени устанавливаются от 6 до 40 секунд.

Параметр	Функции
Время задержки переадресации	Установите максимальное время ожидания перед сменой состояний (от приёма до передачи). Состояние меняется от 4 до 30 секунд.
Приоритет моста	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.

10.8.2 Пункт «Экземпляр порта»

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.

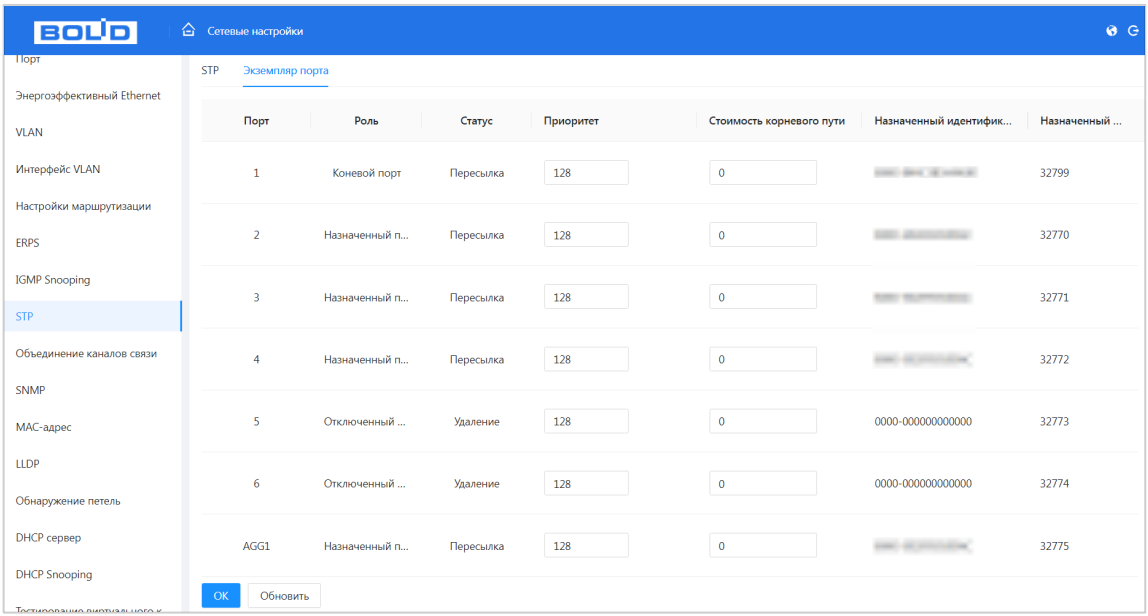


Рисунок 10.16 – Настройка STP

Таблица 10.11 – Параметры настройки STP

Параметр	Функции
Номер порта	Номер порта. Соответствует числу на лицевой панели.
Приоритет	Установите «приоритет порта». Значение параметра варьируется от 0 до 240 и кратно 16. Приоритет используется для определения «корневого порта», который будет выбран для передачи данных, как самый короткий путь до корневого моста в сети. Чем ниже значение параметра, тем выше приоритет. При одинаковом «приоритете порта» для передачи выбирается порт с большей скоростью.

Параметр	Функции
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 удалённым от ядра системы. Параметр устанавливается от 0 до 200000000.

10.9 Подраздел «Объединение каналов записи (Агрегация каналов)»

Суть агрегации каналов заключается в формировании из нескольких физических портов коммутатора одного логического порта, причём 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 надёжность соединения.

📖 Агрегация ссылок несовместима с режимом STP, IGMP Snooping и режимом 802.1x. Когда включен режим STP, настройка агрегации каналов невозможна; необходимо сначала отключить режим STP;

📖 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;

📖 Только порты с одинаковой скоростью, дуплексом, расстоянием и конфигурацией VLAN могут находиться в одной группе агрегации.

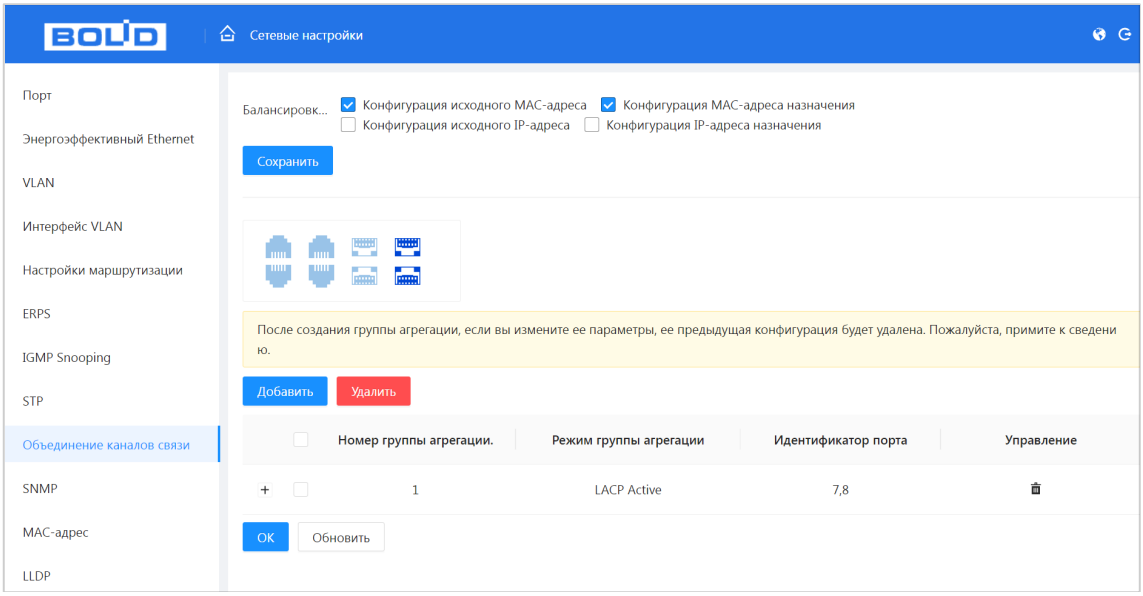


Рисунок 10.17 – Агрегация каналов

10.9.1 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 «Балансировка нагрузки».

Доступны четыре типа алгоритма балансировки нагрузки для порта, которые показаны ниже.

Таблица 10.12 – Типы алгоритма балансировки нагрузки

Режим балансировки	Описание
Конфигурация исходного MAC-адреса	Балансировка нагрузки, осуществляемая на основе поля MAC-адреса источника.
Конфигурация MAC-адреса назначения	Балансировка нагрузки, осуществляемая на основе поля MAC-адреса назначения.
Конфигурация исходного IP-адреса	Балансировка нагрузки, осуществляемая на основе IP-адреса источника.
Конфигурация IP-адреса назначения	Балансировка нагрузки, осуществляемая на основе IP-адреса назначения.

10.9.2 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, приоритет 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 приёма и отправки данных после того, как обе стороны взаимодействуют с информацией об агрегации.

10.9.2.1 **Настройка**

1. Перейдите «Сетевые настройки → Объединение каналов связи».

2. Нажмите кнопку «Добавить».

3. В появившемся окне выберите номер группы и режим группы агрегации. Режимы агрегации группы включают: статический, LACP активный и LACP пассивный.

– «Статический (Static)» – также известен как ручной режим. Интерфейс Eth-Trunk создаётся и заполняется вручную, LACP не требуется;

– «LACP активный (LACP Active)» – интерфейс Eth-Trunk нужно вручную создать и интерфейсы-участники добавить вручную. В отличие от статического, выбор интерфейса настраивается с помощью протокола LACP. Этот режим устанавливает интерфейс в активное состояние переговоров, инициируя переговоры с другими интерфейсами путём отправки LACPDUs;

– «LACP пассивный (LACP Passive)» – интерфейсы Eth-Trunk создаются, и интерфейсы-участники добавляются с помощью протокола LACP. Этот режим устанавливает интерфейс в пассивное состояние переговоров, где интерфейс отвечает на LACPDUs, которые он получает, но не инициирует переговоры по LACPDU.

4. Нажмите кнопку «ОК» для сохранения.

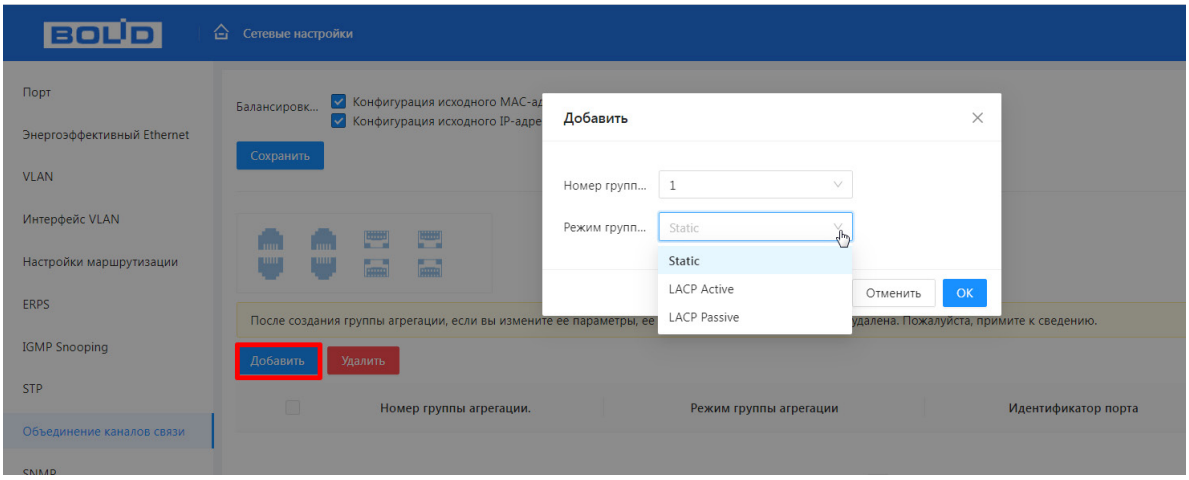


Рисунок 10.18 – Добавление

5. Далее выберите порты для объединения (Рисунок 10.19). Для этого нажмите кнопку  и выделите порты.

6. Нажмите кнопку «ОК» для сохранения.

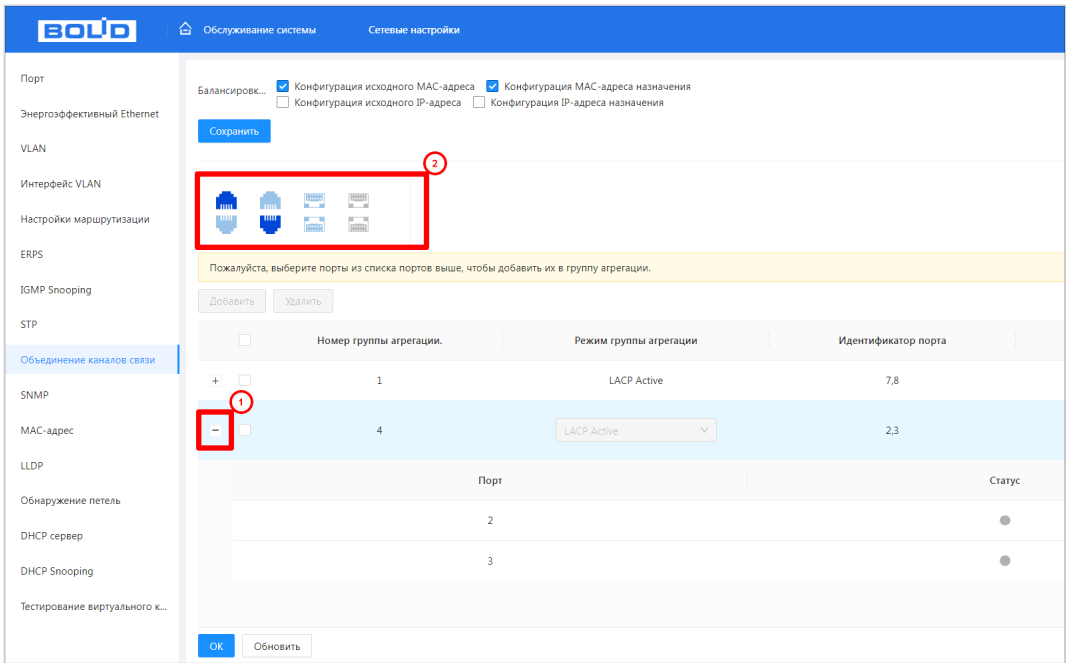


Рисунок 10.19 – Добавление

10.10 Подраздел «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 10.20) изображён 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.

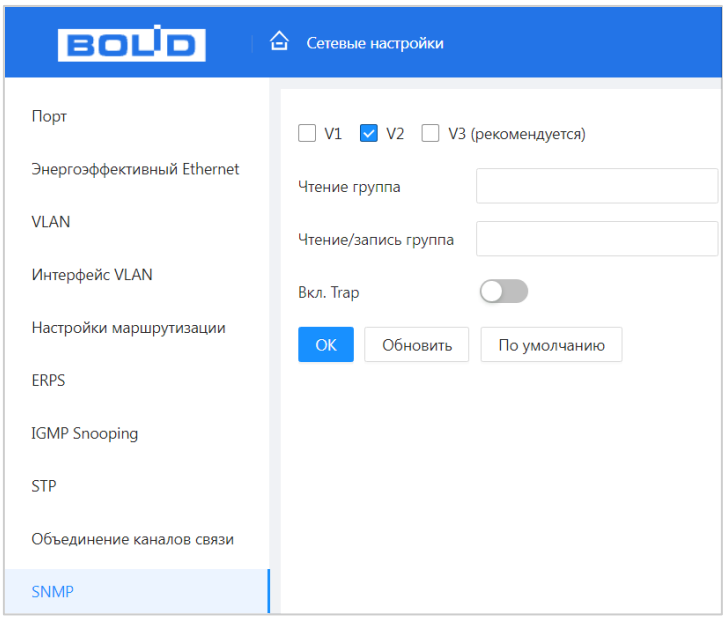


Рисунок 10.20 – Настройки SNMP

На рисунке (Рисунок 10.21) изображён интерфейс настроек SNMP версии 3.

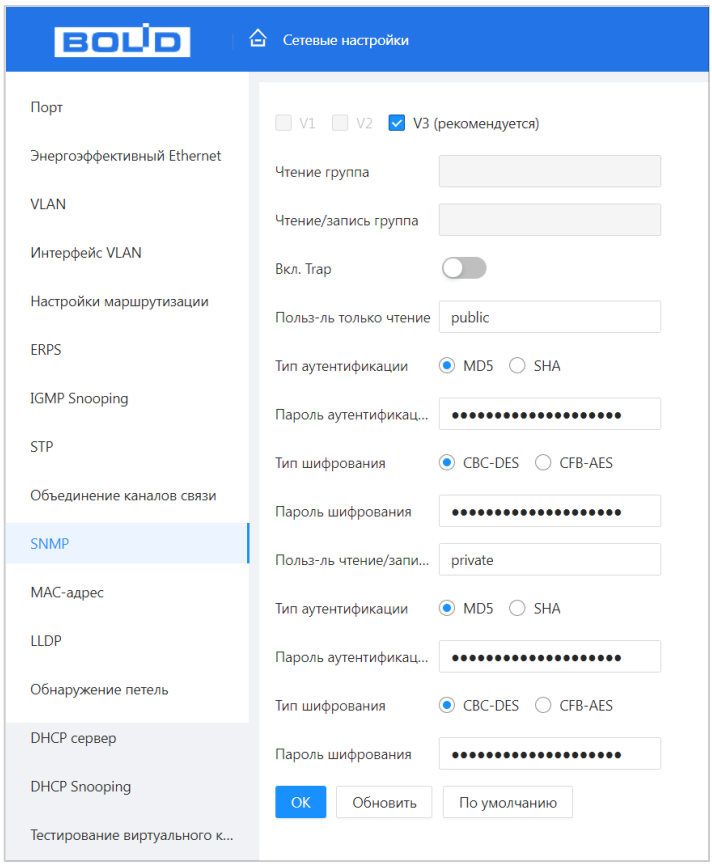


Рисунок 10.21 – Настройки SNMPv3

Таблица 10.13 – 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 счёт 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.
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.

Название	Описание
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.

10.11 Подраздел «MAC-адрес»

10.11.1 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.

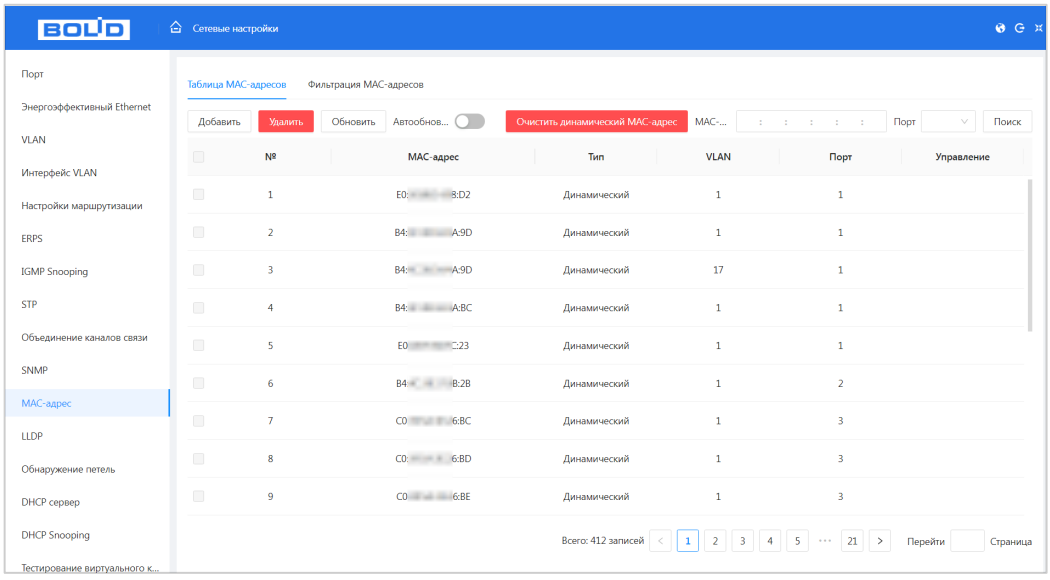


Рисунок 10.22 – MAC информация об адресах

10.11.2 Пункт «Фильтрация MAC-адресов»

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

1. Нажмите «Добавить» и введите в появившемся поле «белый» MAC-адрес.

3. Сохраните настройку.

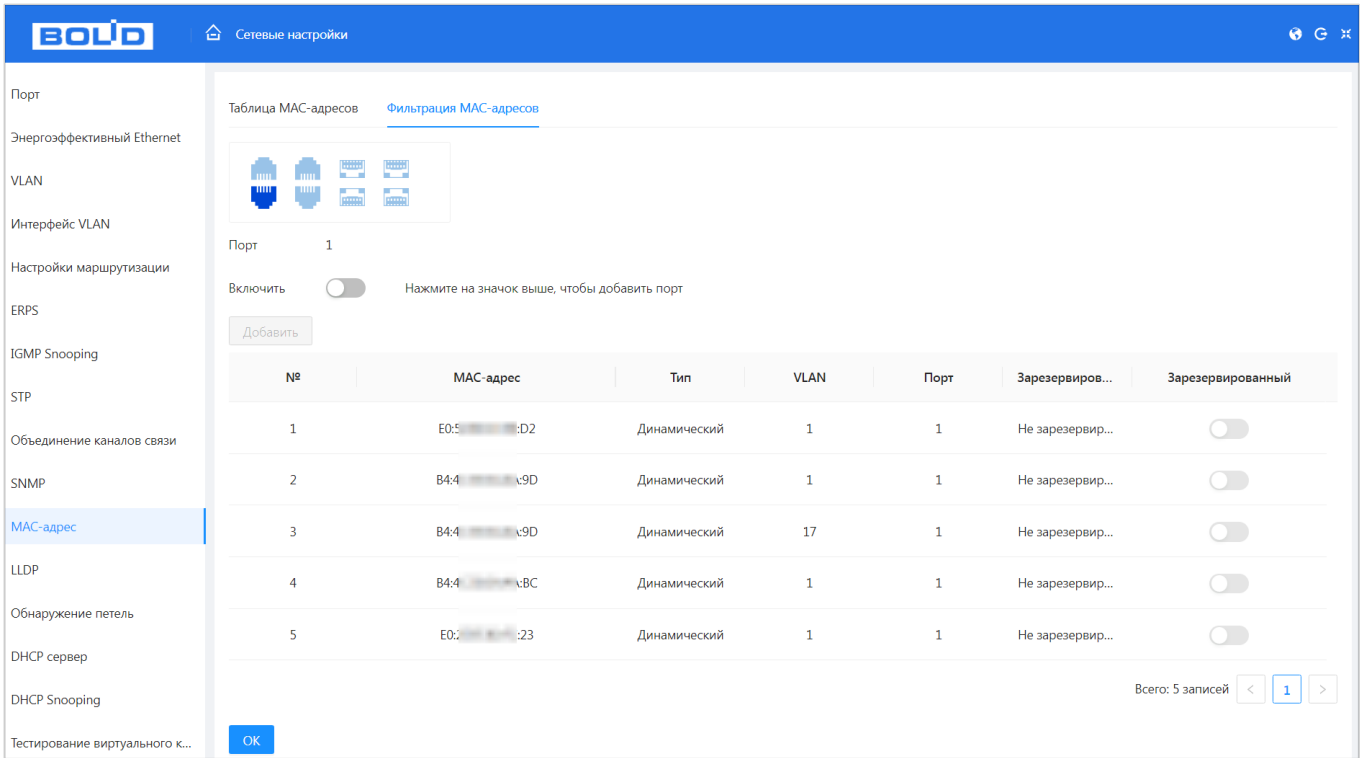


Рисунок 10.23 – Фильтрация портов

10.12 Подраздел «LLDP»

Link Layer Discovery Protocol (LLDP) – протокол канального уровня, позволяющий сетевому оборудованию оповещать оборудование, работающее в локальной сети, о своём существовании и передавать ему свои характеристики, а также получать от него аналогичные сведения.

Интерфейс показывает список обнаруженных по LLDP устройств работающих вместе с коммутатором в локальной сети.

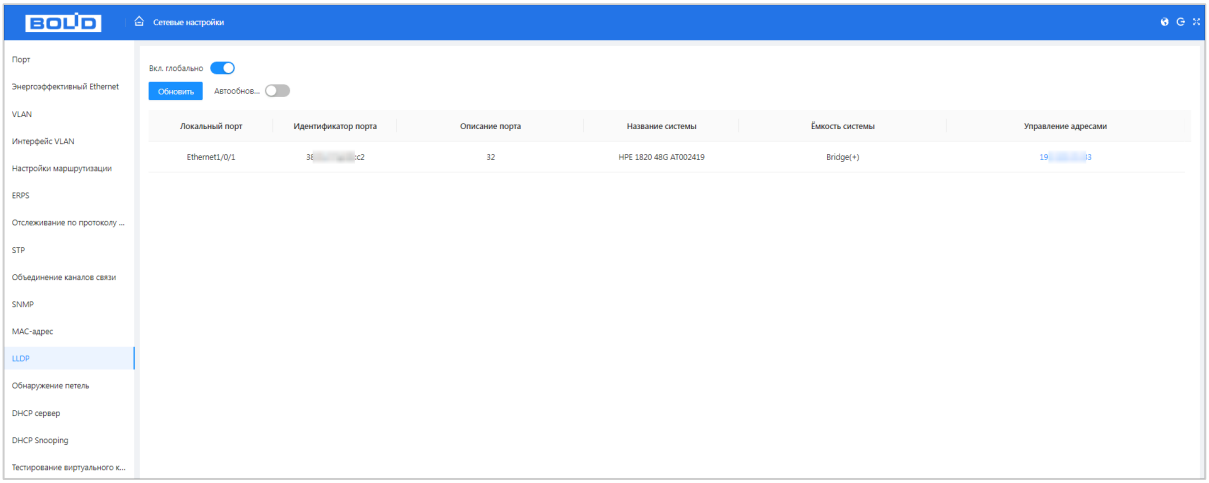


Рисунок 10.24 – Обнаружение по LLDP

10.13 Подраздел «Обнаружение петель»

Функция кольцевого дублирования используется для предотвращения сбоев, которые могут возникнуть при работе оборудования, что приведёт к созданию петли в сети. Защита от петель позволяет принудительно отключить линию, на которой было обнаружено петлевое соединение.

1. Настройте адресацию всем коммутаторам, находящимся в одной подсети.

2. Включите защиту.

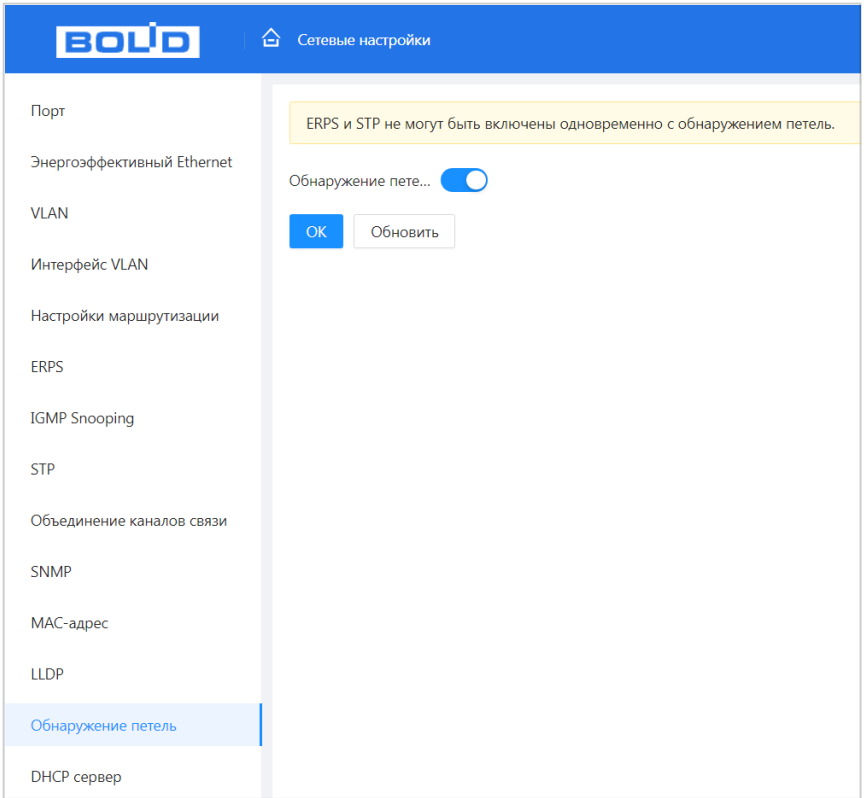


Рисунок 10.25 – Обнаружение петель (Loopback Detection)

10.14 Подраздел «DHCP сервер»

DHCP (Dynamic Host Configuration Protocol) – протокол динамического конфигурирования хоста. Он обеспечивает получение сетевыми устройствами IP-адресов от сервера в локальной сети. DHCP – имеет архитектуру «Клиент – Сервер». DHCP-клиент запрашивает сетевой адрес и другие параметры у DHCP-сервера, а сервер предоставляет сетевой адрес и параметры конфигурации клиентам.

10.14.1 Пункт «DHCP сервер»

10.14.1.1 **Включение**

Для включения работы коммутатора в роли DHCP-сервера:

1. Активируйте переключатель в строке «DHCP-сервер».
2. Нажмите кнопку «ОК» для сохранения.

После включения IP-адреса DHCP-клиентам будут выдаваться из введённого списка пулов.

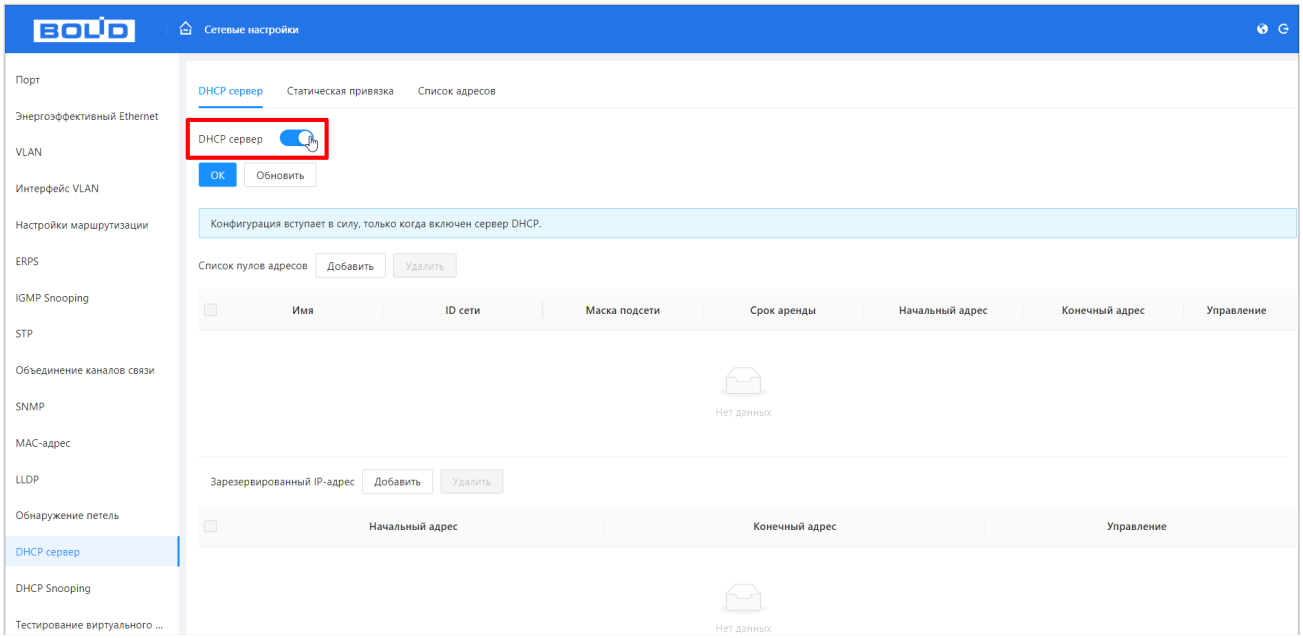


Рисунок 10.26 – Настройка DHCP-сервера

10.14.1.2 **Добавление DHCP POOL**

Для создания пулов IP-адресов, которые будут раздаваться, нажмите «Добавить», далее введите данные для добавления (Рисунок 10.27, Таблица 10.14).

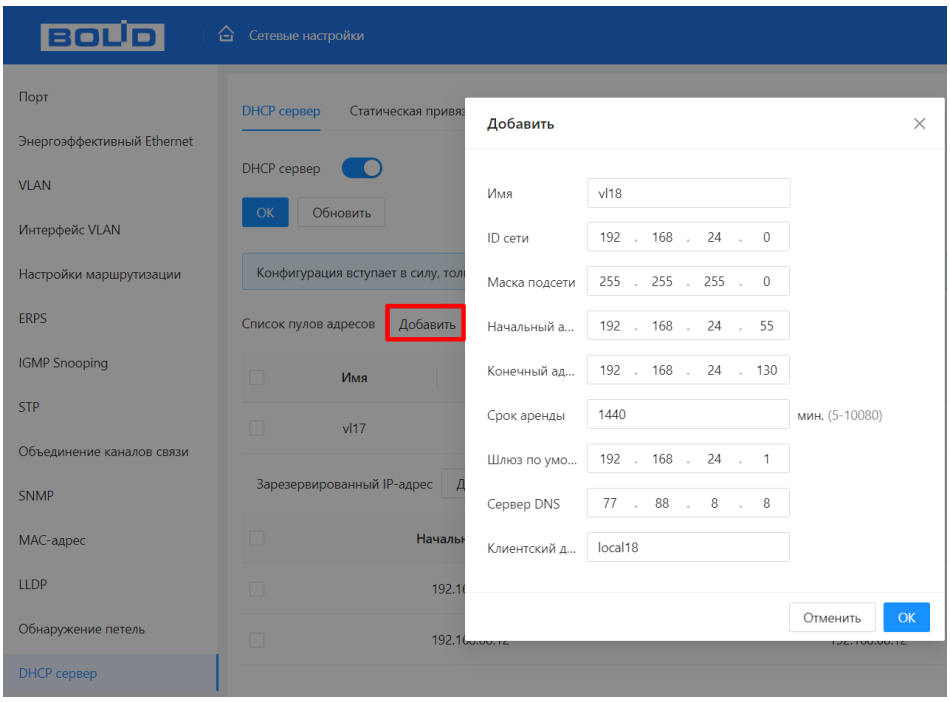


Рисунок 10.27 – Добавить пул

Таблица 10.14 – Добавляемые параметры при добавлении пула

Параметр	Функция
Имя	Поле для ввода имени пула адресов (при вводе исключите пробелы, например, vlan2_test).
ID сети	Поле для ввода адреса подсети.
Маска подсети	Поле для ввода маски подсети.
Начальный адрес	Начальный адрес в диапазоне, который DHCP-сервер может выдать клиентам.
Конечный адрес	Конечный адрес в диапазоне, который DHCP-сервер может выдать клиентам.
Срок аренды	Поля для ввода времени аренды для выбранного пула адресов.
Шлюз по умолчанию	Поле для ввода шлюза по умолчанию для пула адресов.
Сервер DNS	Адрес(а) DNS-серверов.
Клиентский домен	Поле ввода доменного имени, передаваемое клиентам.

10.14.1.1 **Добавление зарезервированного IP-адреса**

После нажатия кнопки «Добавить» в поле «Зарезервированный IP-адрес» откроется окно добавления зарезервированных IP-адресов (Рисунок 10.28). Введите диапазон IP-адресов, которые будут исключены из общего пула назначаемых адресов.

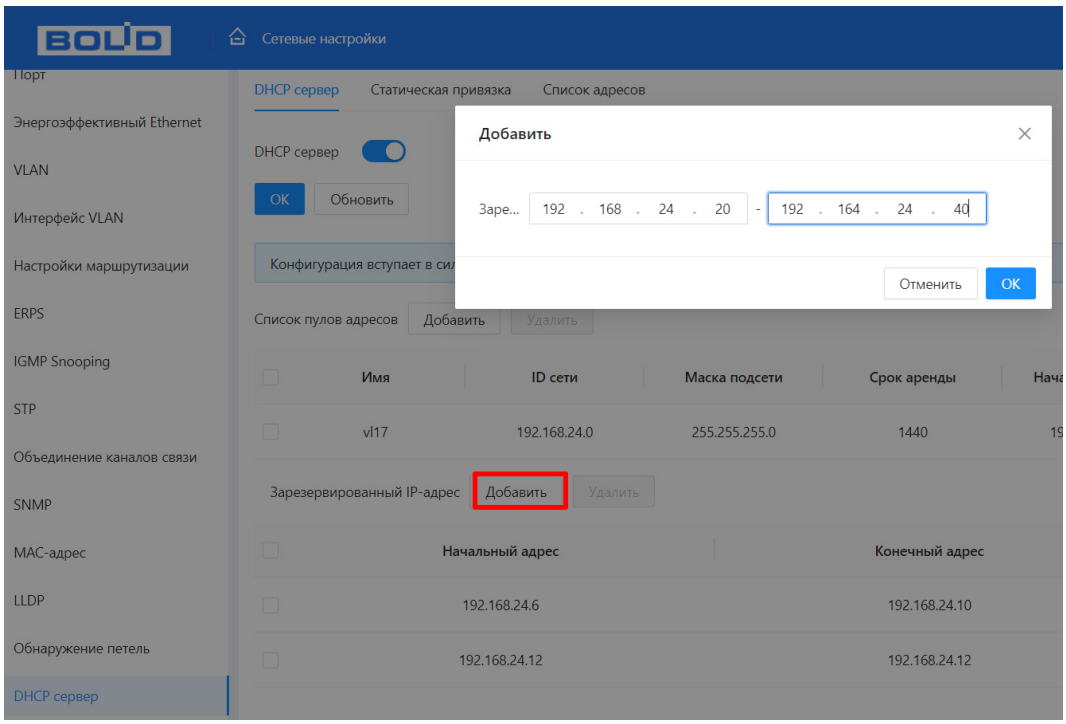


Рисунок 10.28 – Добавление зарезервированных IP-адресов

10.14.2 Пункт «Статическая привязка»

Статическая привязка фиксирует соответствие конкретного DHCP-клиента определённому IP-адресу. Когда клиент запрашивает адрес, сервер сопоставляет его идентификатор (MAC или Client ID) с записью в списке и выдаёт заранее назначенный IP. Используется данная функция, например, для видеокамер, видеорегистраторов и серверов.

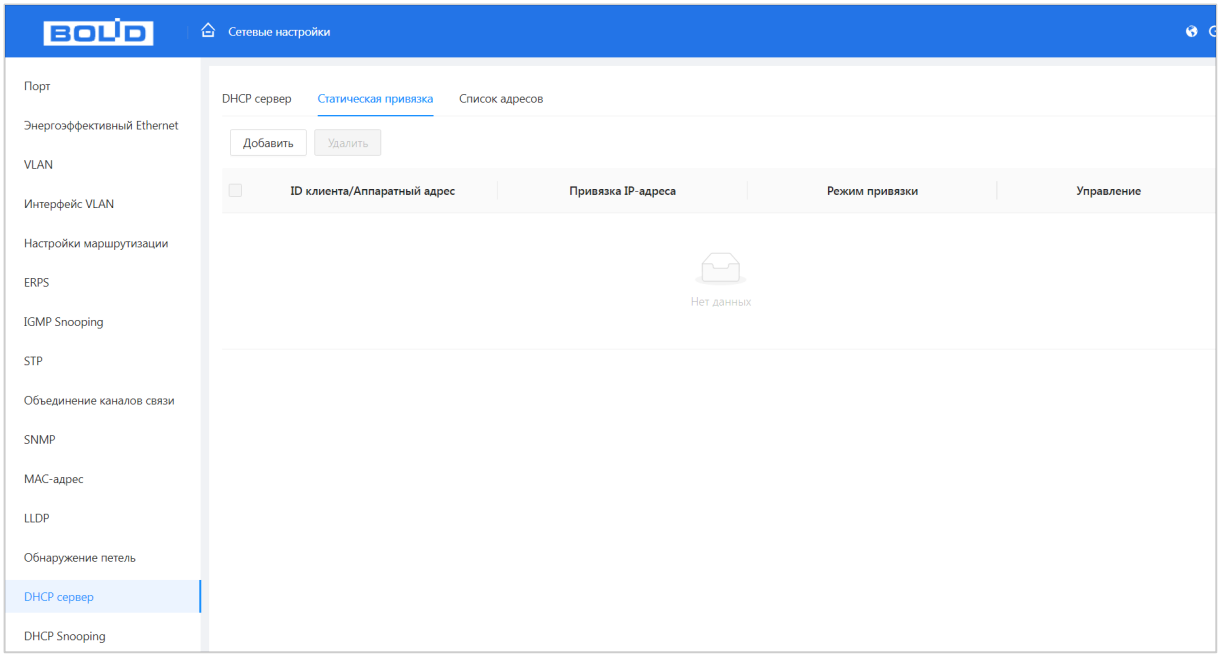


Рисунок 10.29 – Статическая привязка

1. Для добавления нажмите кнопку «Добавить».
2. В появившемся окне заполните поля (Таблица 10.15).

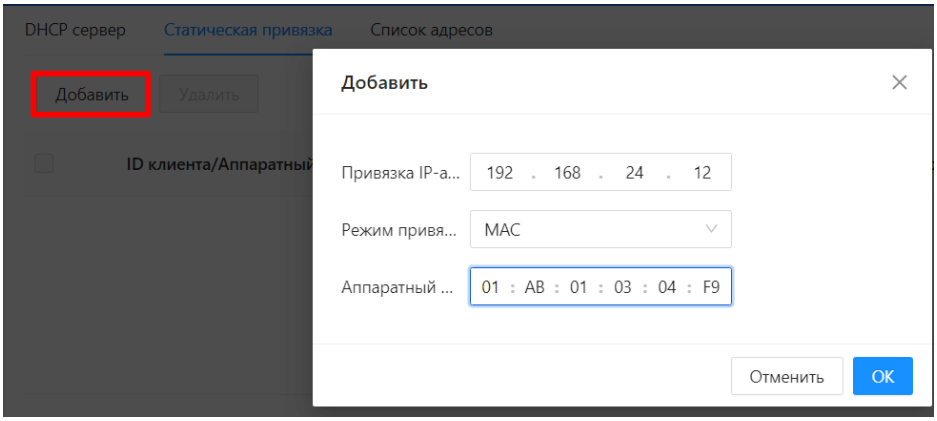


Рисунок 10.30 – Добавление в список

Таблица 10.15 – Статическая привязка

Параметр	Функция
Привязка IP-адреса	Поле ввода зарезервированного IP-адреса.
Режим привязки	Доступен выбор: MAC или Name_ASCII
Аппаратный адрес/ ID клиента	Поле ввода значения исходя из выбранного режима. Аппаратный адрес – ввод MAC-адреса; ID клиента (DHCP Option 61) – ввод идентификатора клиента.

10.14.3 Пункт «Список адресов»

Список текущих DHCP-аренд: показывает, какие IP уже выданы клиентам, с каким MAC и сколько осталось времени до окончания аренды.

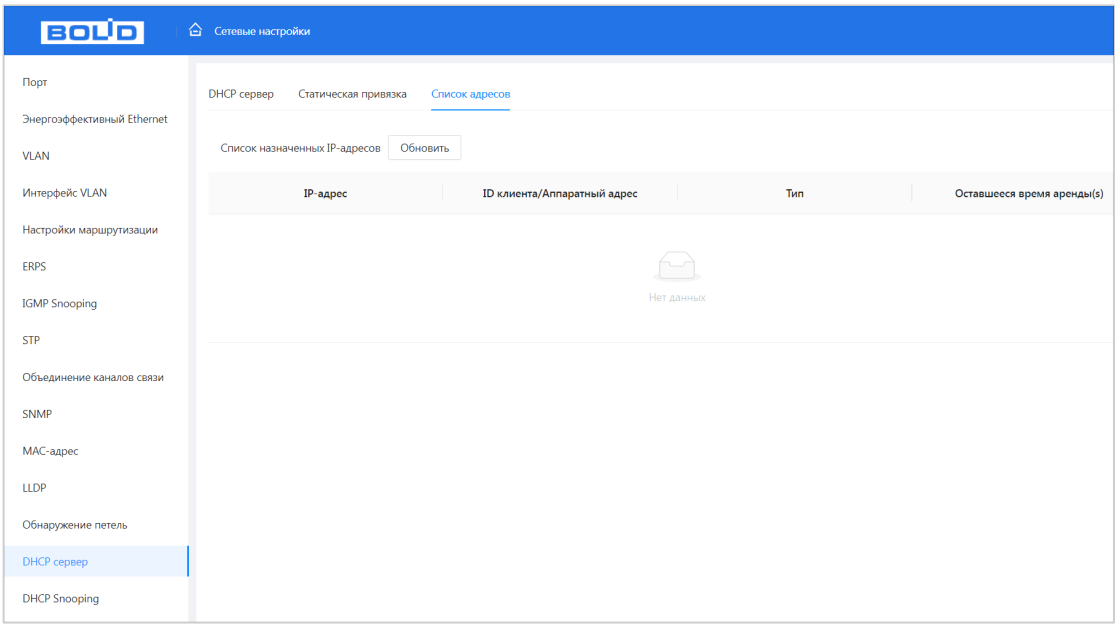


Рисунок 10.31 – Список адресов

10.15 Подраздел «DHCP Snooping»

DHCP Snooping – функция безопасности на управляемых коммутаторах, которая отслеживает и фильтрует DHCP-запросы и ответы на портах устройства, блокируя ответы от недоверенных DHCP-серверов и защищая сеть от атак.

10.16 Пункт «Глобальные настройки»

Первым этапом настройки функции является включение функции с помощью переключателя «DHCP Snooping».

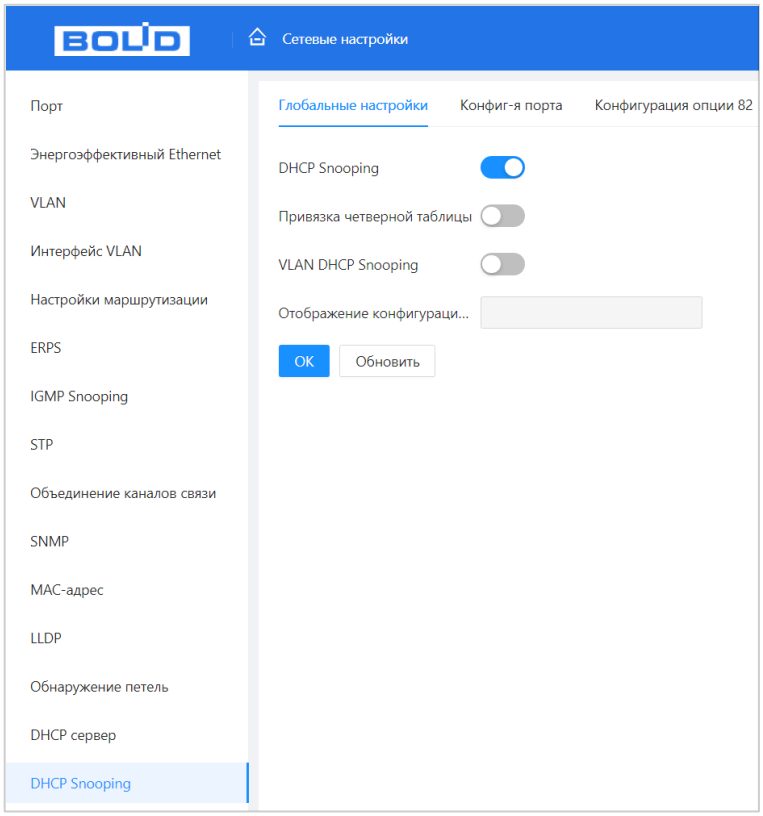


Рисунок 10.32 – Глобальные настройки DHCP Snooping

Переключатель «Привязка четверной таблицы (DHCP Snooping binding)» – включение таблицы с динамическими записями, которые используются для механизмов безопасности.

Переключатель «VLAN DHCP Snooping» – используется, если нужно включить функцию для конкретных VLAN(ов). То есть эта функция отслеживания и фильтрации DHCP-трафика выполняется в пределах указанных VLAN, а не глобально по всему коммутатору.

10.16.1 Пункт «Конфиг-я порта»

Вторым этапом настройки производится включение функции DHCP Snooping на порту, с которого разрешены DHCP-ответы. Отмеченные порты будут определяться как доверенные (trusted), остальные будут определяться как недоверенные (untrusted).

Дополнительно включается отслеживание направлений DHCP-сообщений: DHCPDECLINE и DHCPRELEASE.

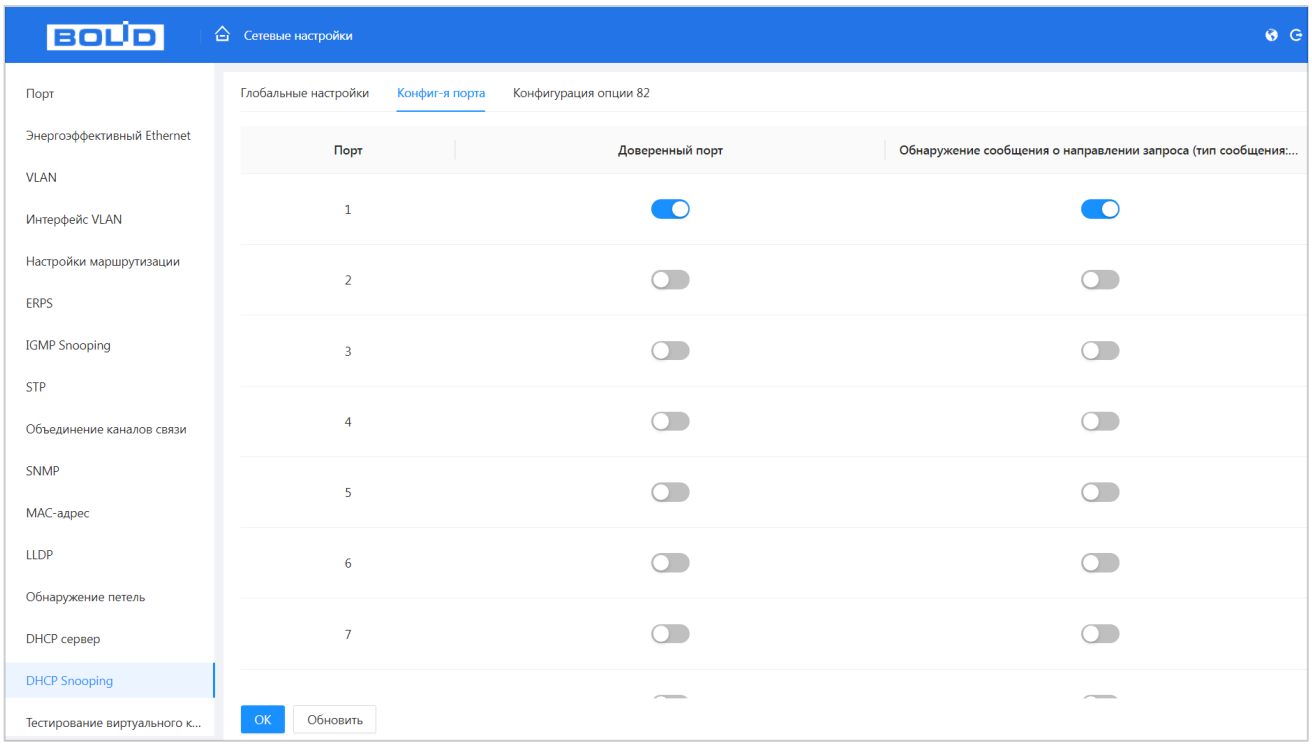


Рисунок 10.33 – Настройка портов

10.16.2 Пункт «Конфигурация опции 82»

Дополнительным шагом настройки является включение на порту «Опции 82» (Рисунок 10.34). Используется эта функция для передачи дополнительной информации о DHCP-клиенте на DHCP-сервер (например, порт, VLAN, название устройства и т.д.).

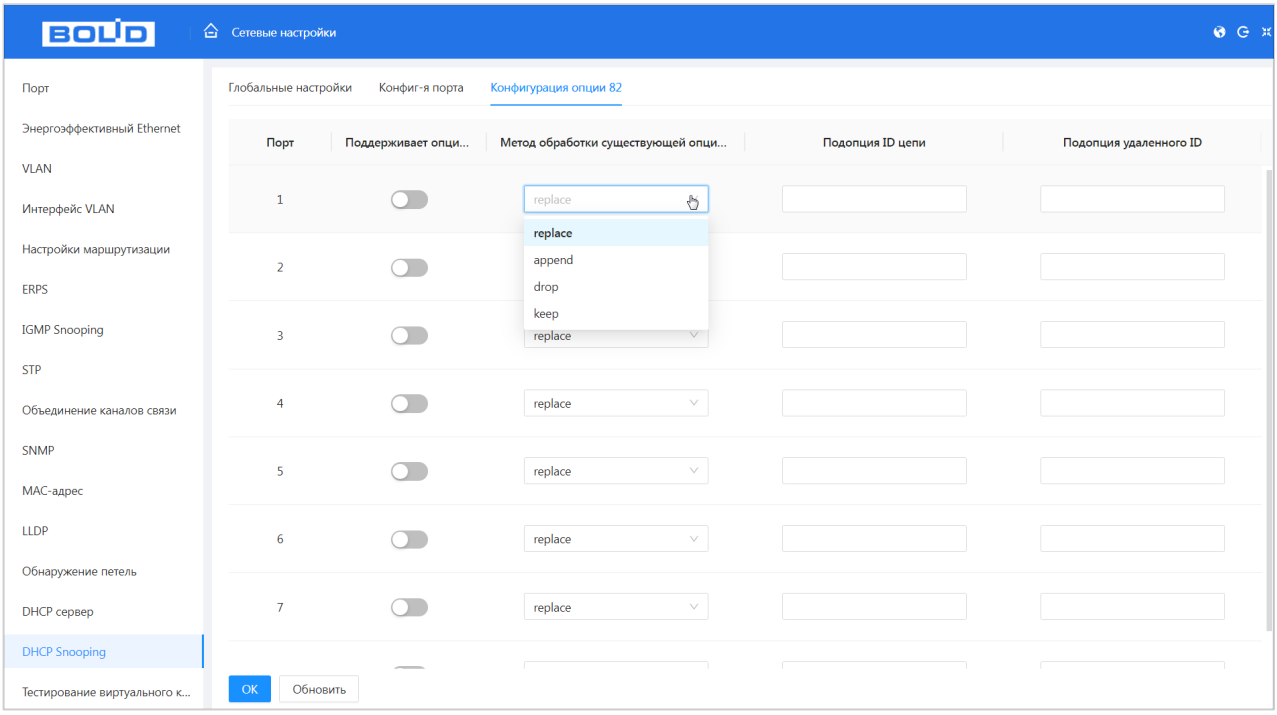


Рисунок 10.34 – Конфигурация опции 82

Таблица 16 – Параметры включения «опции 82»

Параметр	Функция
Порт	Номер порта коммутатора.
Поддерживает опцию 82	Включение или выключение функции на порту.
Метод обработки существующей опции 82	Метод обработки «опции 82»: – Replace – заменить существующую «опцию 82» на собственную; – Append – добавить «опцию 82», при отсутствии; – Drop – отбросить опцию при пересылке; – Keep/Forward – не изменять поле опции.
Circuit ID (Подопция ID цепи)	идентификатор подключенного к коммутатору клиентского устройства \ номера клиентского Ethernet порта. Он может быть использован для назначения параметров, уникальных для конкретного пользователя.
Remote ID (Подопция удаленного ID	идентификатор коммутатора, который может быть использован для назначения сервером сетевых настроек.

10.17 Подраздел «Тестирование виртуального кабеля»

Функция тестирования виртуального канала предназначена для быстрой диагностики состояния кабеля и отображения приблизительной длины до неисправности.

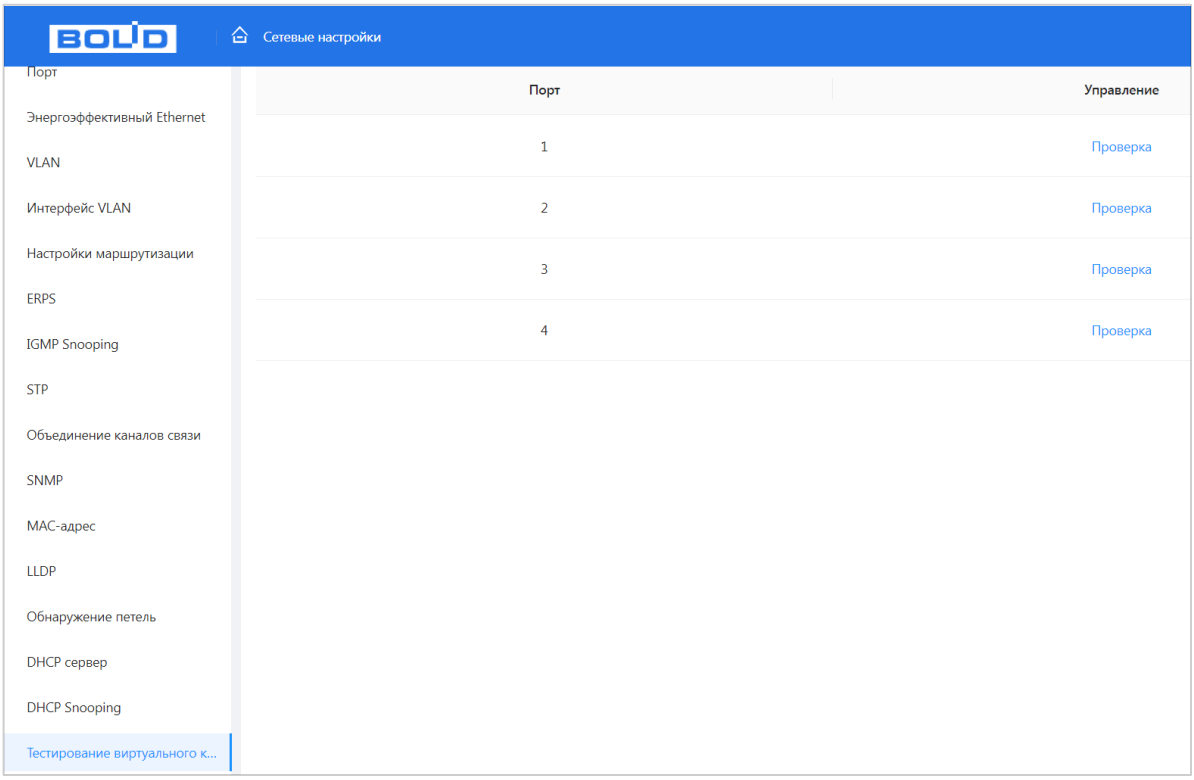


Рисунок 10.35 – Тестирование виртуального канала

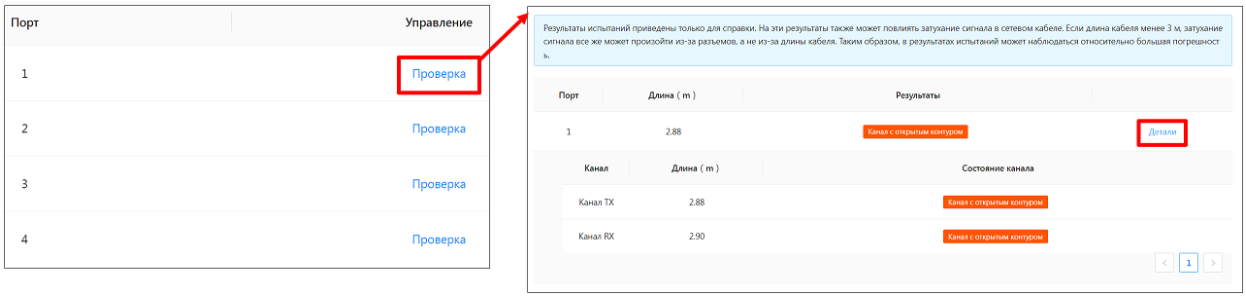


Рисунок 10.36 – Тестирование виртуального канала

11 РАЗДЕЛ ГЛАВНОГО МЕНЮ «УПРАВЛЕНИЕ POE»

11.1 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.

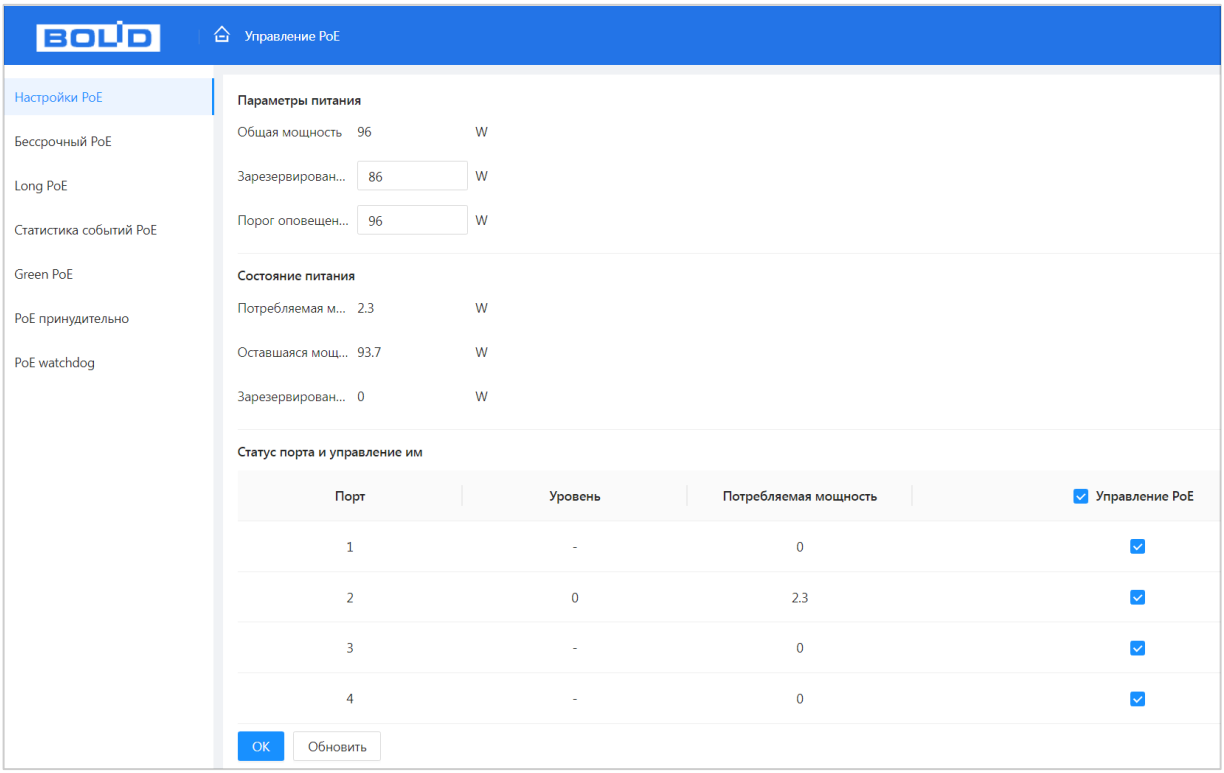


Рисунок 11.1 – Питания порта по PoE

Таблица 11.1 – Параметры настройки

Параметр		Функция
Параметры питания	Общая мощность	Предельная мощность устройства.
	Зарезервированная мощность	Настраиваемая доступная мощность PoE.
	Мощность оповещения (Порог оповещения)	Пороговые значения для оповещений в случае, если потребление мощности приближается к лимиту.
Состояние питания	Потребляемая мощность	Отображает текущую потребляемую мощность.
	Оставшаяся мощность	Отображает текущую остаточную мощность.

Параметр		Функция
	Зарезервированная мощность	Непригодное для использования питание по PoE. Зарезервированная мощность = общая мощность при перегрузке.
Статус порта и управление им	Уровень	Подача питания на устройство, подключенное к порту. Уровень подачи питания колеблется от 0 до 8, при Hi-PoE отображается как 5+.
	Потребляемая мощность	Отображает текущую мощность PoE, потребляемую соответствующим отдельным портом.
	Управление PoE	Включение или выключение PoE на выбранном порту.

11.2 Подраздел «Бессрочный PoE»

Включение этой функции обеспечивает постоянную подачу питания по PoE на портах коммутатора независимо от перезагрузок, обновлений ПО или временной потери управления.

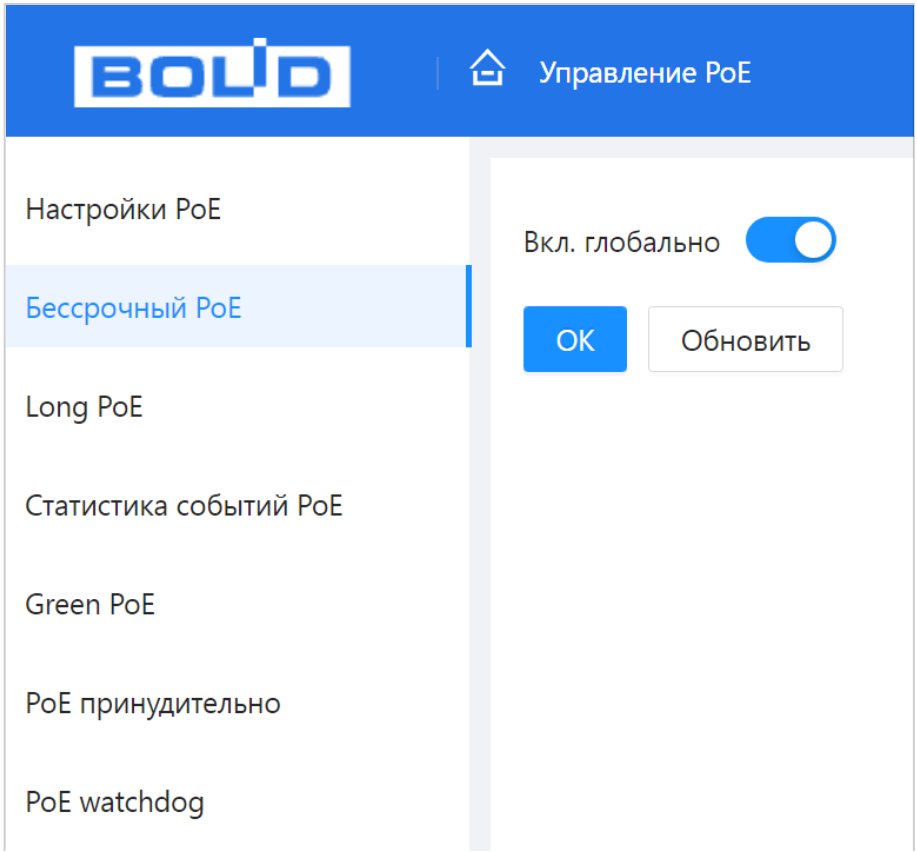


Рисунок 11.2 – Бессрочный PoE

11.3 Подраздел «Long PoE»

Включение технологии увеличения дальности передачи со 100 м до 250 м для подключенных в порты PoE устройств. При включении снижается скорость передачи до 10 Мбит/с (со 100 Мбит/с).

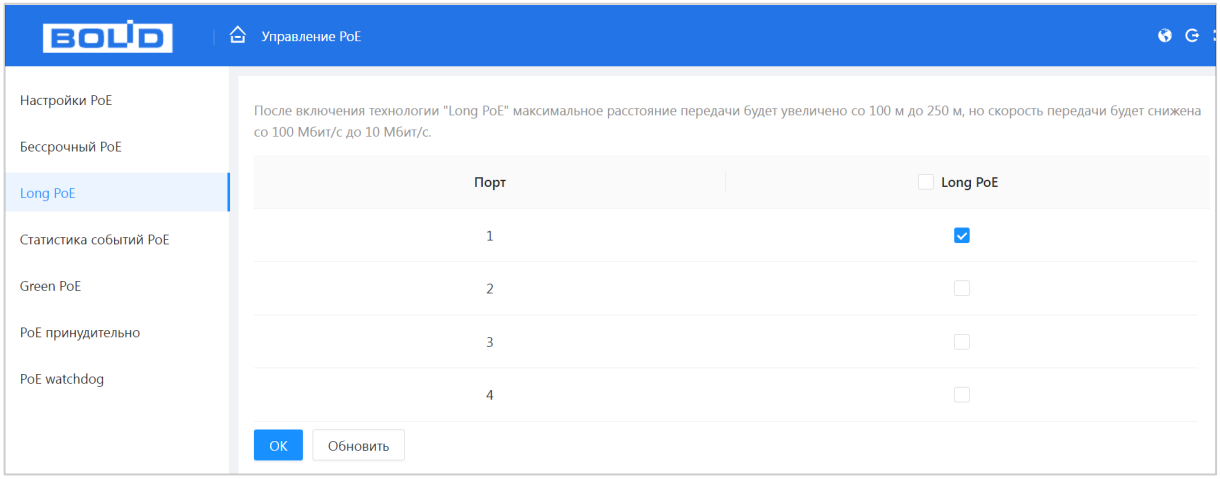


Рисунок 11.3 – Long PoE

11.4 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.

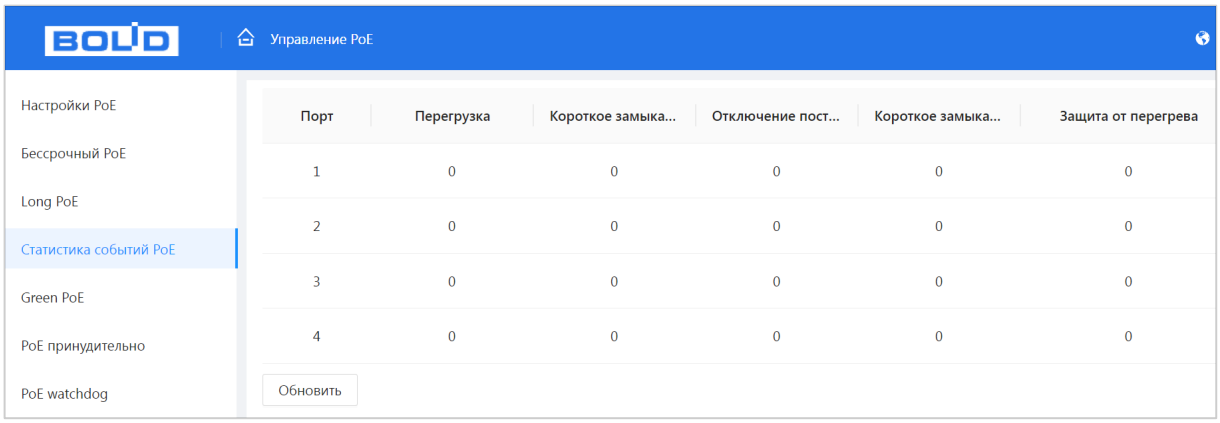


Рисунок 11.4 – Статистика событий PoE

11.5 Подраздел «Green PoE»

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

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

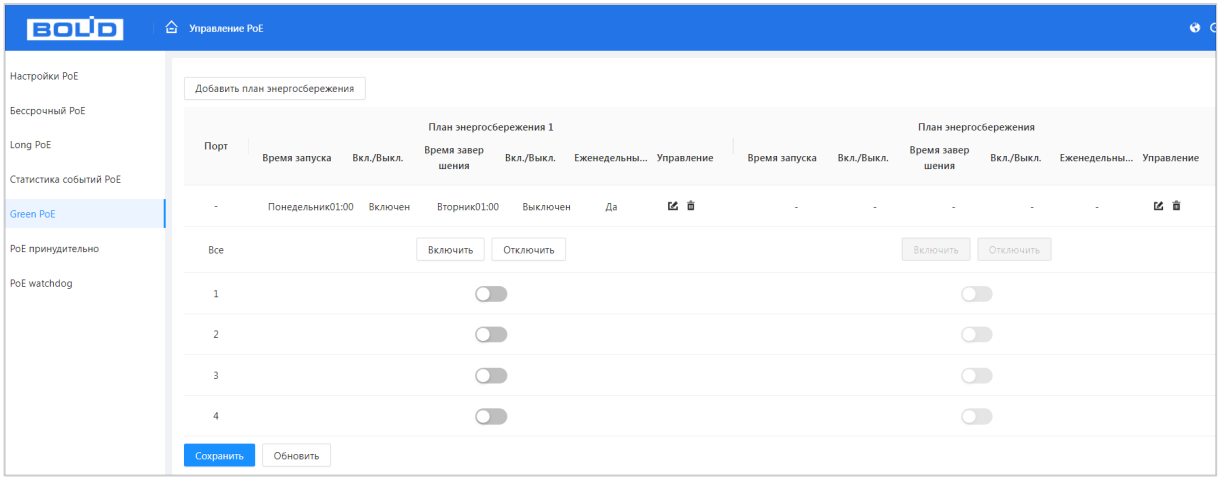


Рисунок 11.5 – Параметры энергосбережения PoE

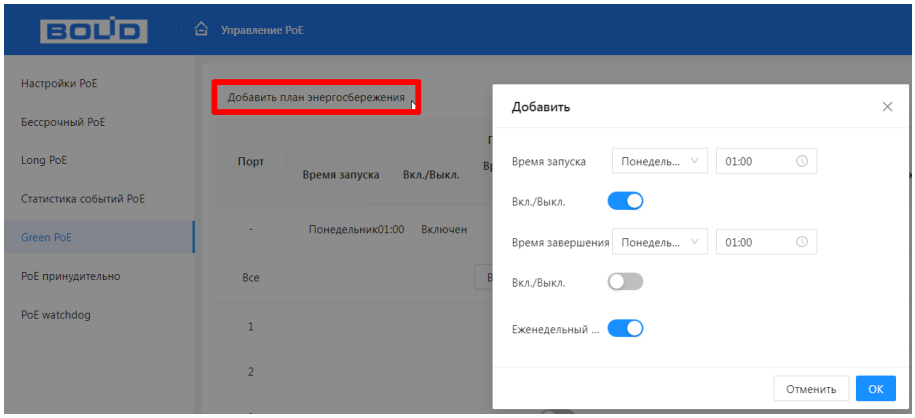


Рисунок 11.6 – Параметры энергосбережения PoE

11.6 Подраздел «PoE принудительно»

После включения функции, отмеченные порты принудительно подают питание (PoE), независимо от того, соответствует ли подключённое устройство стандарту передачи питания или нет (Рисунок 11.7).

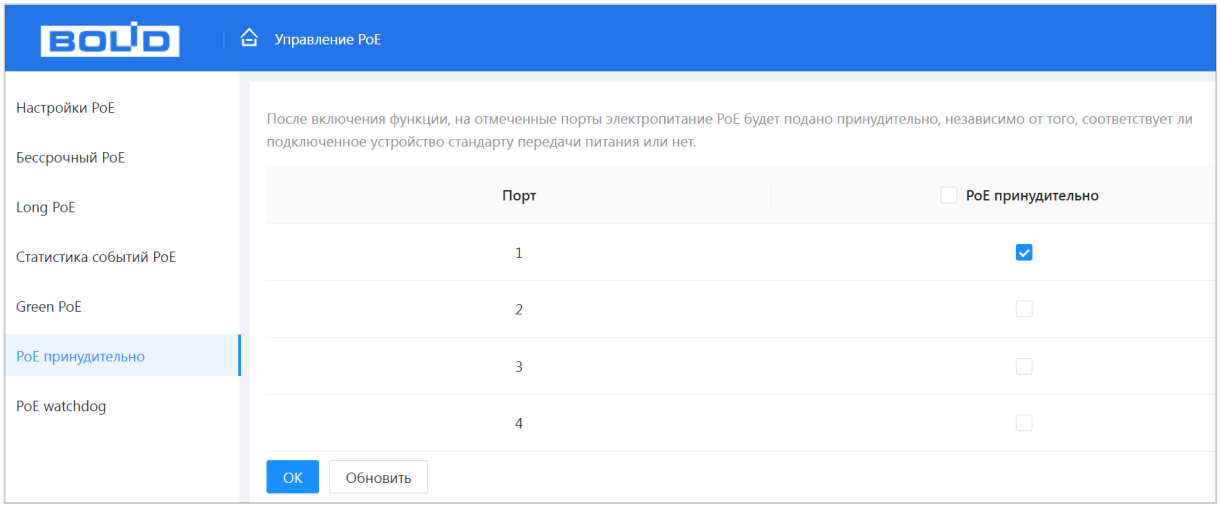


Рисунок 11.7 – Поддержка устаревших устройств

11.7 Подраздел «PoE watchdog»

ВНИМАНИЕ!
Возможно, одновременно включить либо «PoE watchdog», либо непрерывную подачу электропитания (см. 11.6 Подраздел «PoE принудительно»).

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.

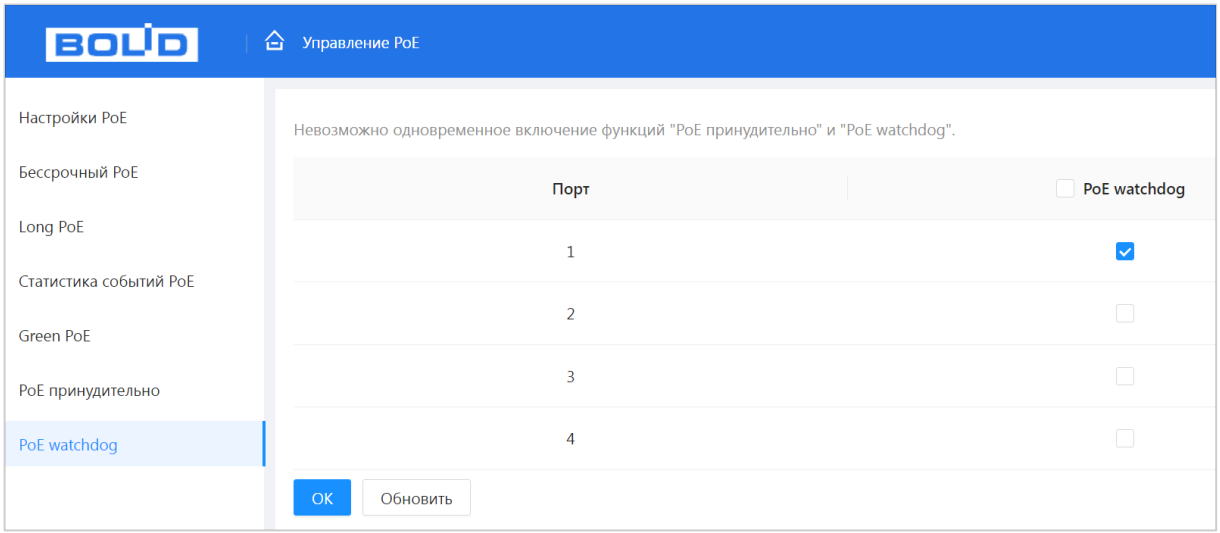


Рисунок 11.8 – PoE watchdog

12 РАЗДЕЛ ГЛАВНОГО МЕНЮ «ЦЕНТР БЕЗОПАСНОСТИ»

12.1 Подраздел «Доп. сервисы»

12.1.1 Пункт «Доп. сервисы»

Перейдите в раздел для включения/отключения функций уведомления и доступа по протоколам.

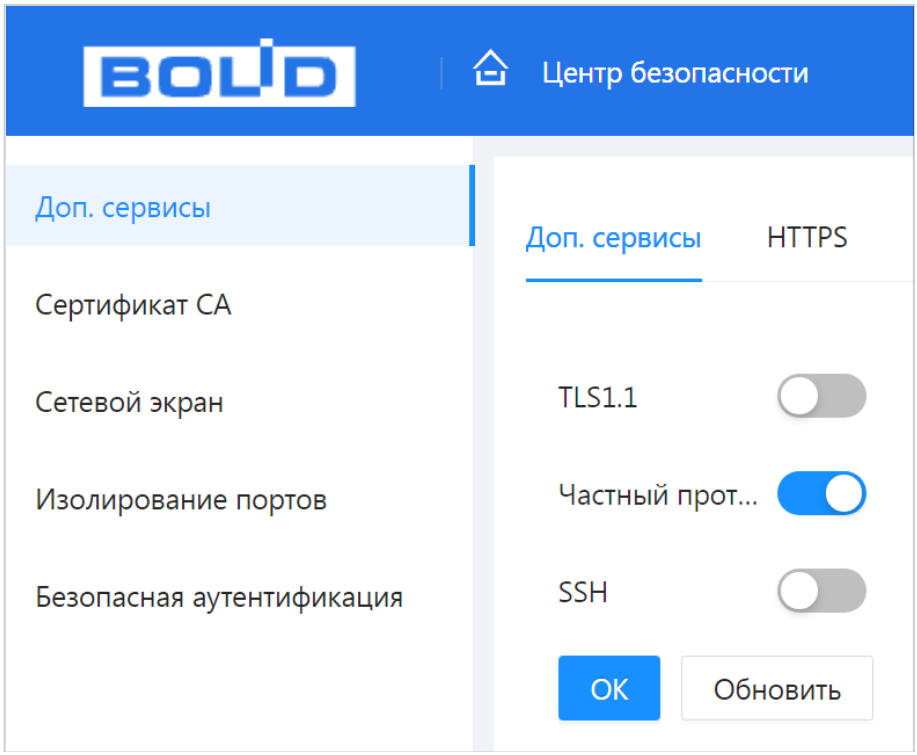


Рисунок 12.1 – Системное обслуживание

Таблица 12.1 – Параметры системного обслуживания

Параметр	Функции
TLSv1.1	Протокол защищённого транспортного уровня (TLS) обеспечивает конфиденциальность и целостность данных между двумя прикладными приложениями. TLS включает два уровня: TLS Record (уровень записей) и TLS Handshake (процедура установления соединения). 📖 TLS 1.1 использует устаревшие и слабые алгоритмы шифрования; рекомендуется отключить поддержку TLS 1.1.
Частный протокол	Приватный протокол. 📖 При использовании функции могут возникнуть риски для безопасности. Рекомендуется отключить эту функцию, если она не используется.

Параметр	Функции
SSH	Включение доступа через протокол SSH. Функция отключена по умолчанию. 📖 При использовании функции могут возникнуть риски для безопасности. Рекомендуется отключить эту функцию, если она не используется.

12.1.2 Пункт «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 «Сертификат CA → Сертификат устройства». 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.

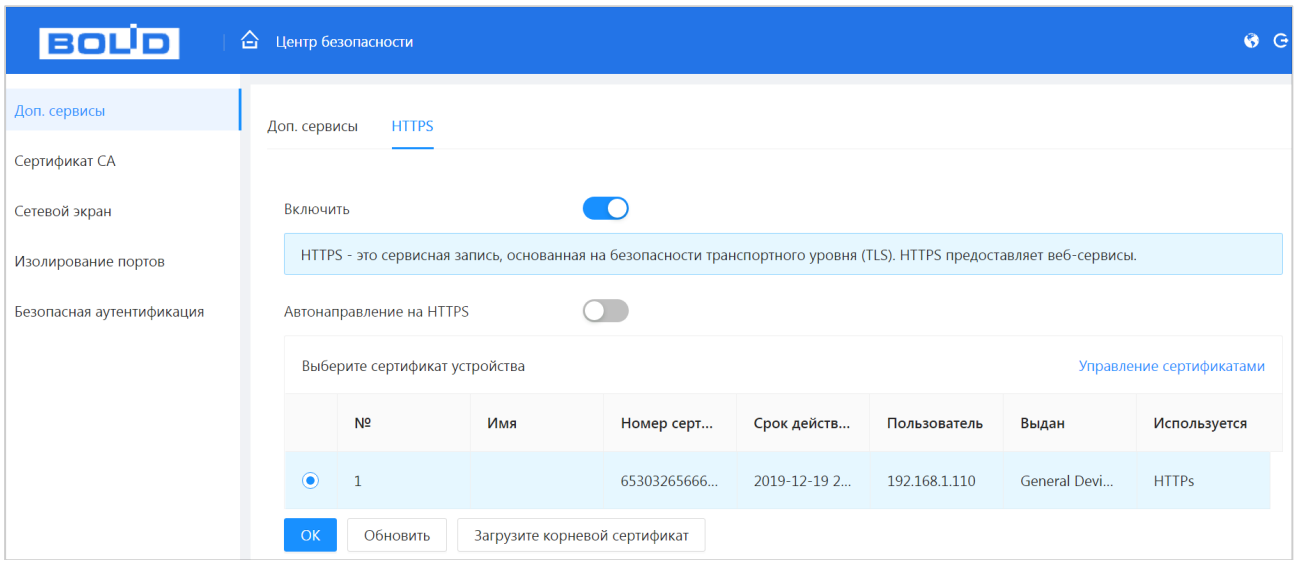


Рисунок 12.2 – HTTPS

1. Убедитесь в актуальности текущей даты.

2. Включите HTTPS для повышения безопасности системы.

3. Далее включите совместимость TLSv1.1, чтобы обеспечить совместимость протоколов (Пункт «Доп. сервисы»).

4. Выберите пакет сертификатов устройства.

5. Для создания, импорта или экспорта сертификата нажмите кнопку «Управление сертификатами».

6. Сохраните настройку.

12.2 Подраздел «Сертификат CA»

12.2.1 Пункт «Сертификат устройства»

Перейдите «Главное меню → Центр безопасности → Сертификат CA → Сертификат устройства» для создания сертификата или для импорта стороннего сертификата на устройство.

Следуйте инструкциям на экране для создания или импорта стороннего сертификата.

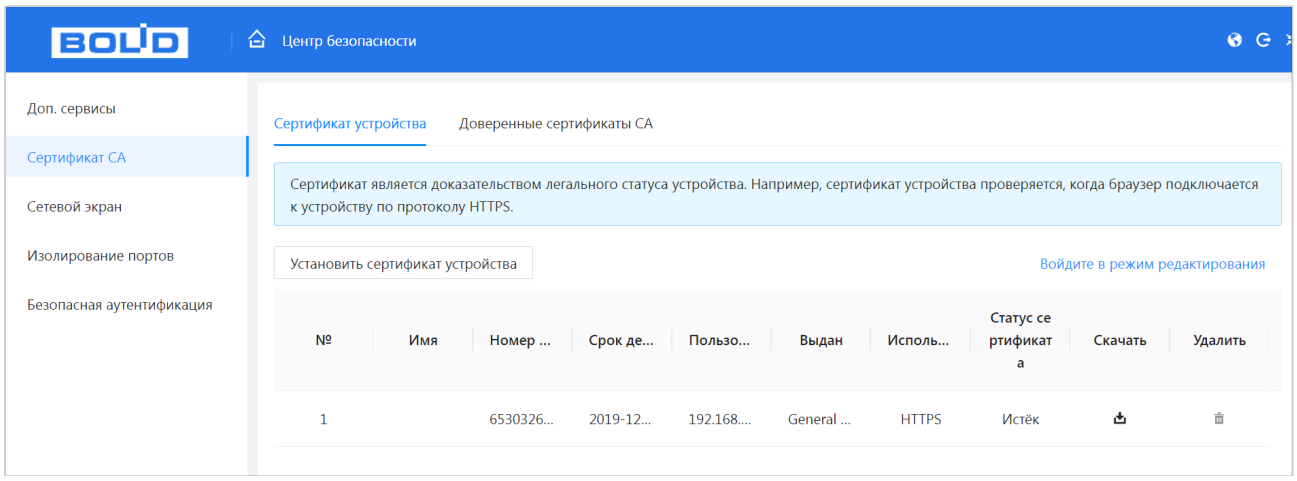


Рисунок 12.3 – Сертификат устройства

Создать сертификат – служит для создания самоподписанного сертификата. Сертификат может быть использован, например, при подключении по HTTPS.

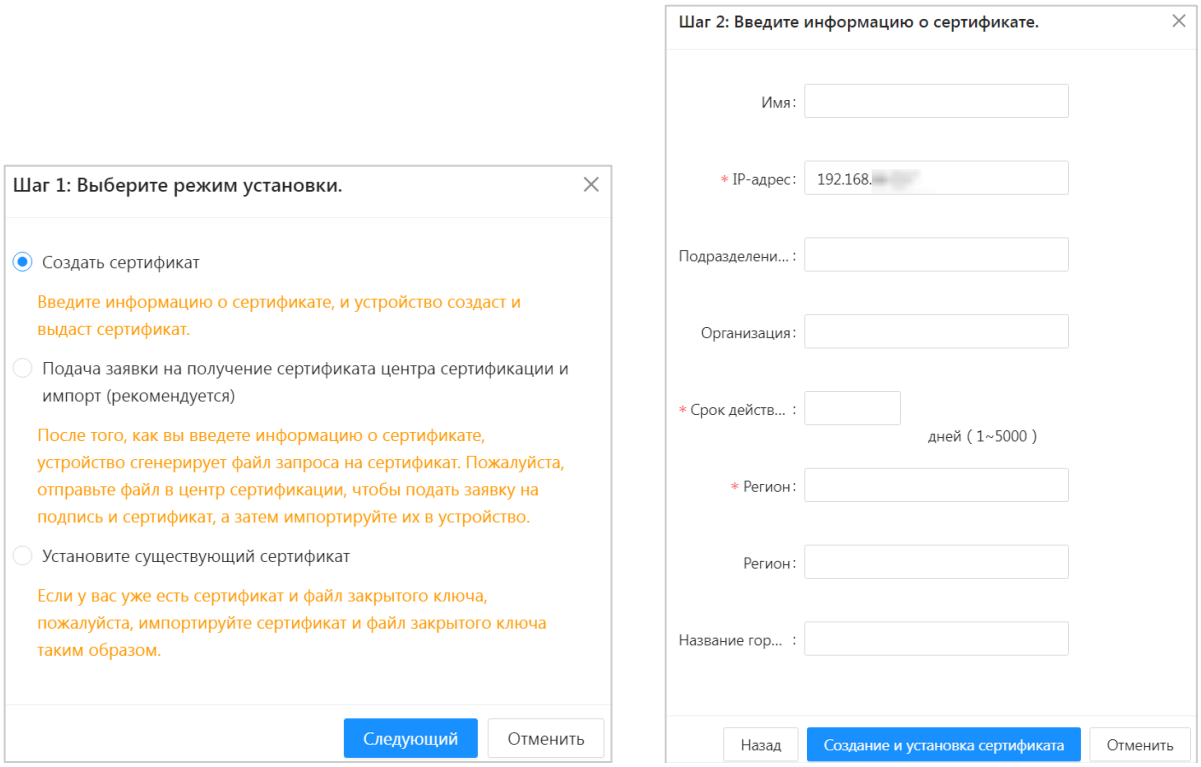


Рисунок 12.4 – Создание самоподписанного сертификата

Подача заявки на получение сертификата центра сертификации и импорт (рекомендуется) – служит для создания и импорта доверенного сертификата путём создания запроса для отправки в центр сертификации и импорта возвращённого из центра сертификации сертификата.

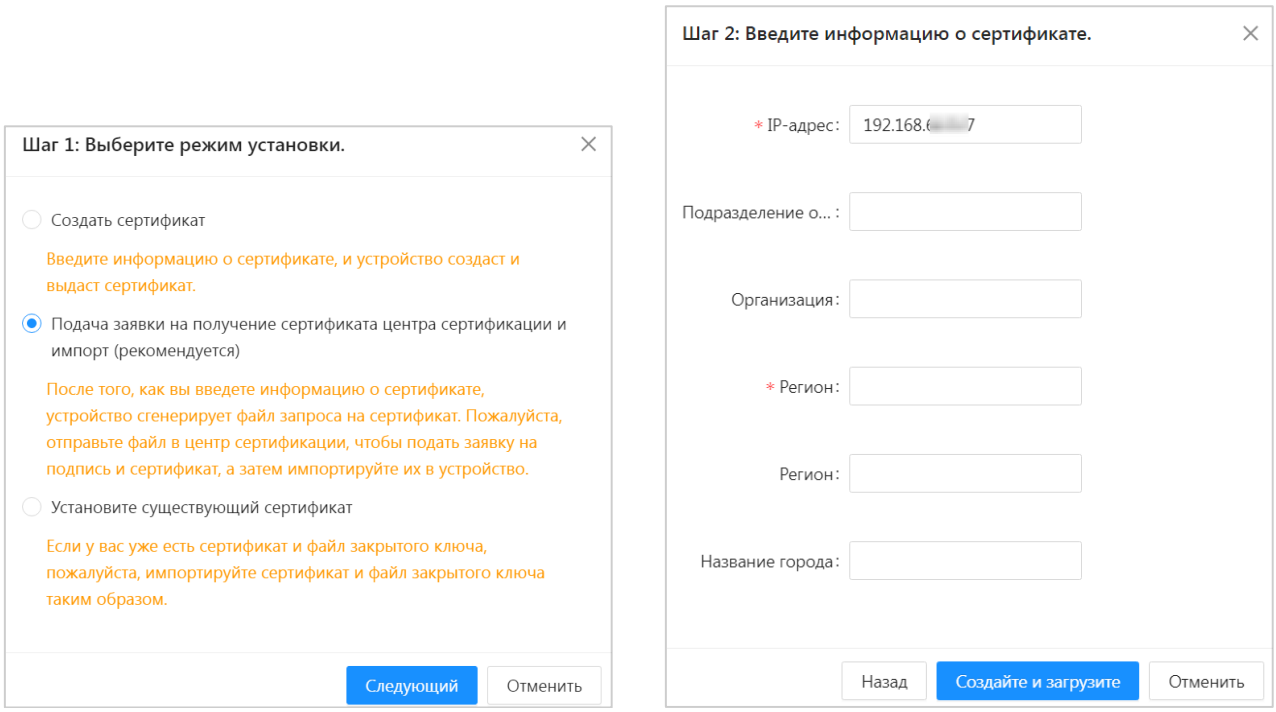


Рисунок 12.5 – Создание и импорт доверенного сертификата

Установить существующий сертификат – служит для импорта готового сертификата выпущенного любым способом без помощи видеорегистратора.

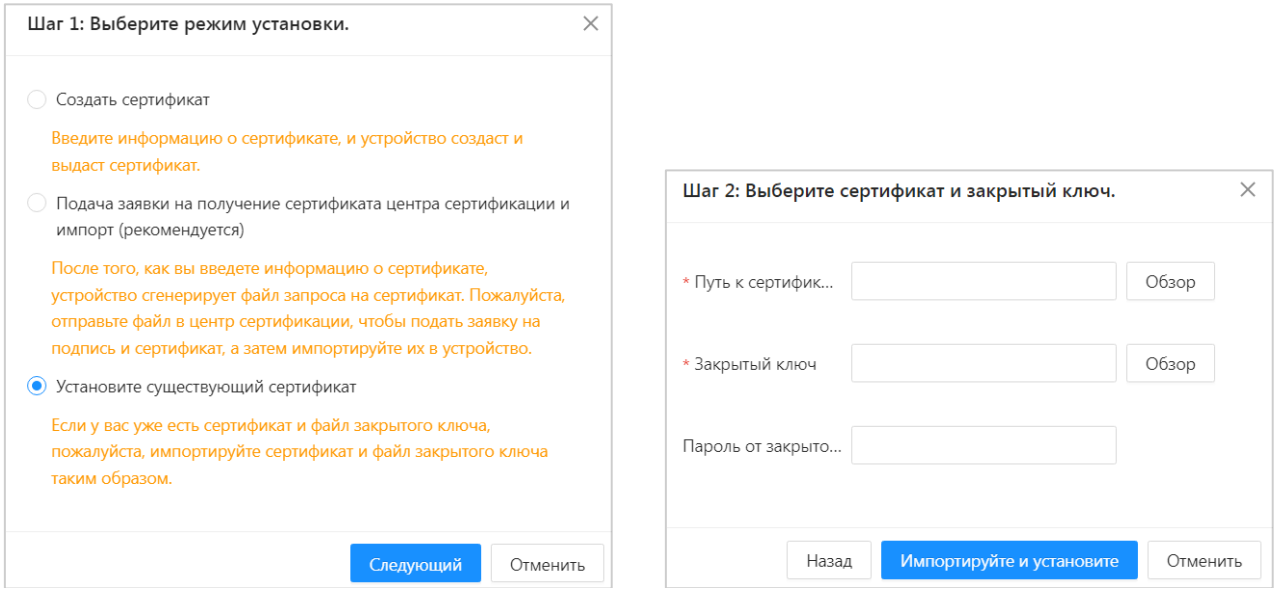


Рисунок 12.6 – Импорт стороннего сертификата

12.2.2 Пункт «Доверенные сертификаты CA»

Перейдите «Главное меню → Центр безопасности → Сертификат CA → Доверенные сертификаты CA» для импорта доверенного сертификата на устройство. Далее сертификат будет использован при настройке 802.1x.

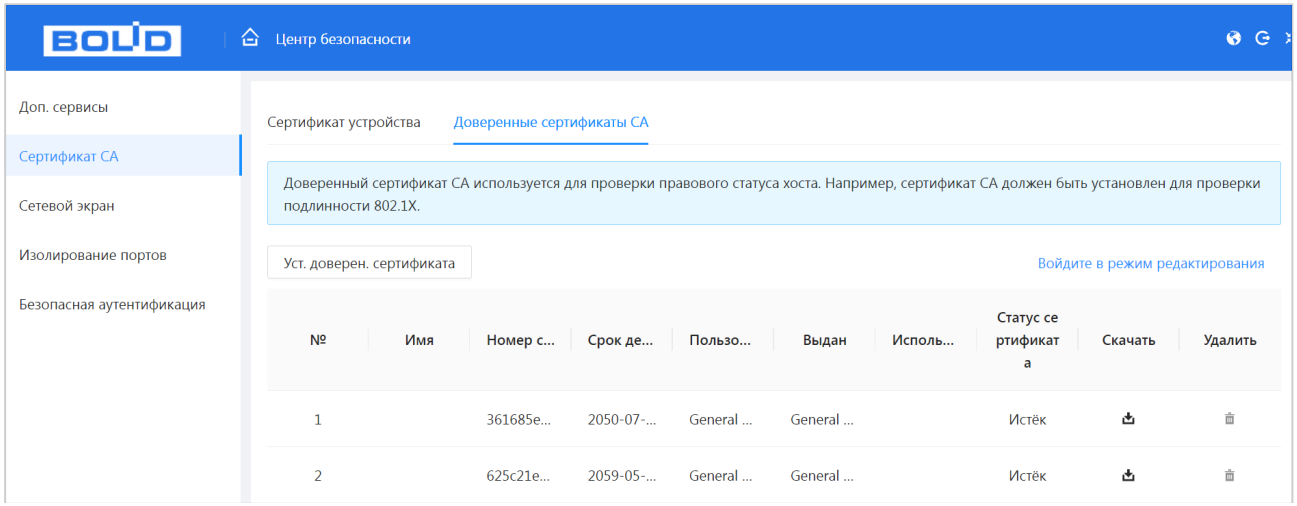


Рисунок 12.7 – Установка доверенного сертификата

12.3 Подраздел «Сетевой экран»

12.3.1 Пункт «IP фильтр»

Добавьте IP-адрес, MAC-адрес или диапазон IP в выбранный список для блокировки или для разрешения доступа к устройству по сети.

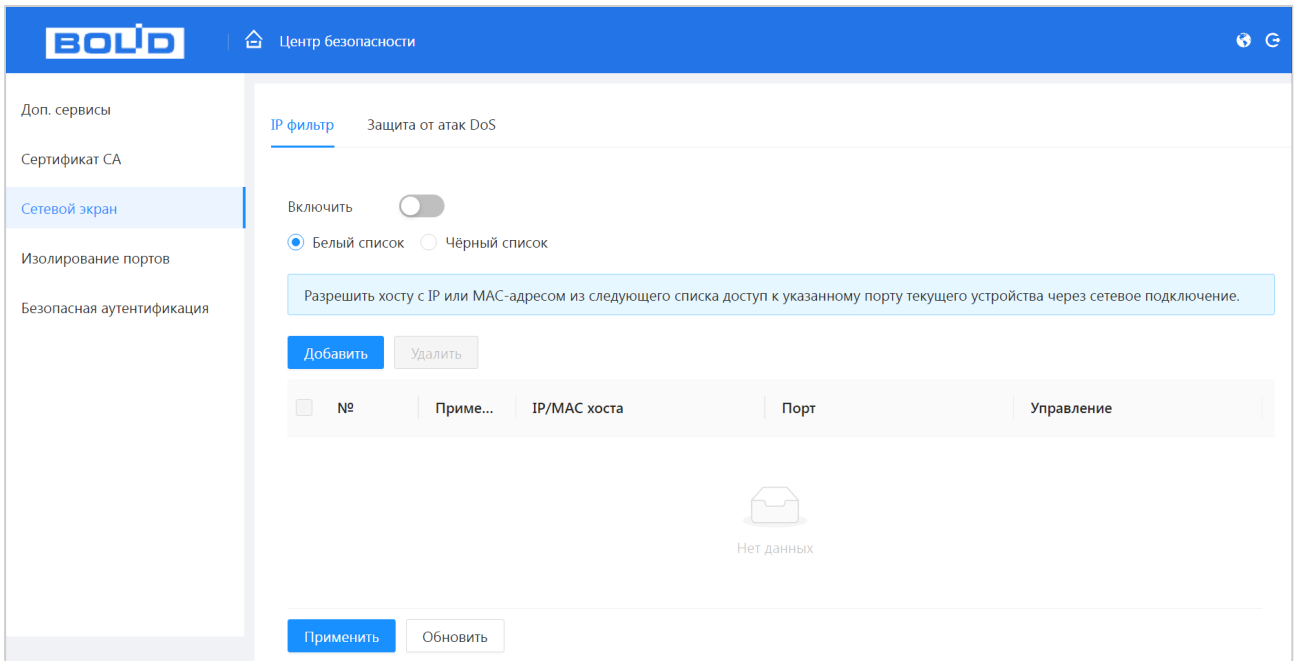


Рисунок 12.8 – Сетевой экран

1. Включите функцию и выберите список доступа (Рисунок 12.9). Для данного устройства доступны следующие варианты:

– Белый список – сетевой доступ разрешён;

– Чёрный список – сетевой доступ запрещён.

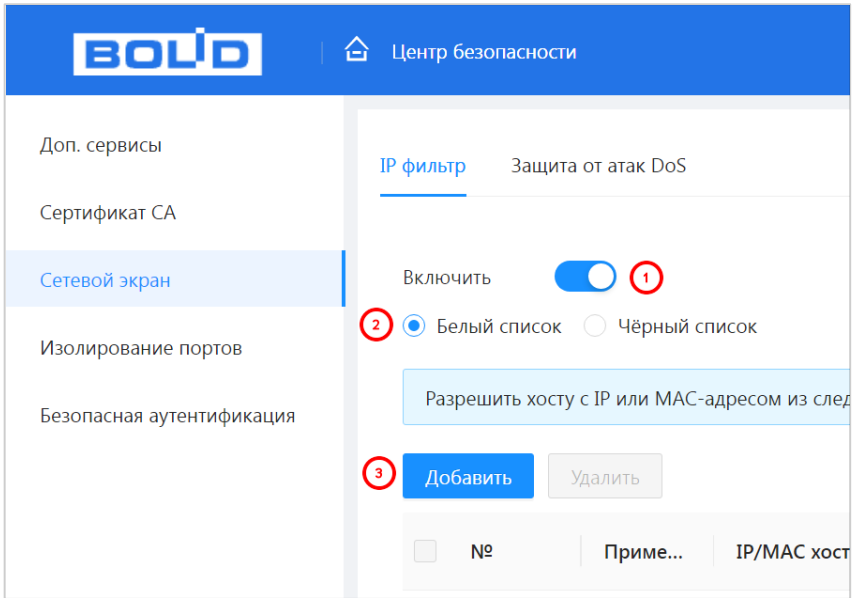


Рисунок 12.9 – Добавить

2. Нажмите кнопку «Добавить», выберите из выпадающего списка способ добавления (Рисунок 12.9). Доступно:

– Добавление при введении IP-адреса устройства. Дополнительно вводится диапазон доступных сетевых портов для введённого IP-адреса;

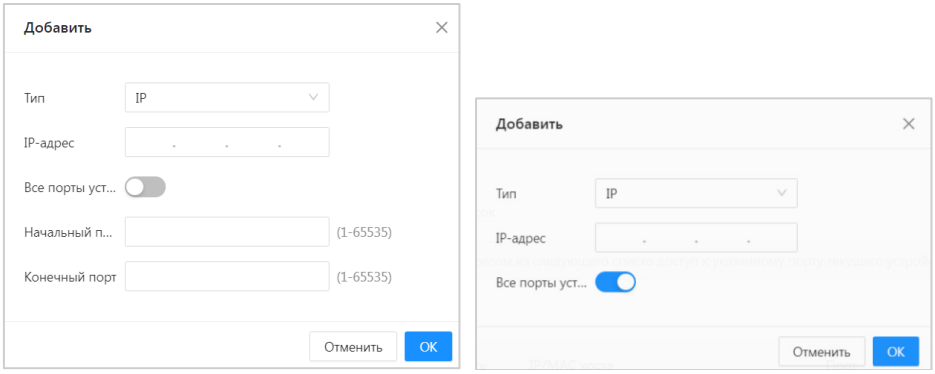


Рисунок 12.10 – Добавить IP-адрес

– Добавление диапазона IP-адресов в список. Дополнительно вводится диапазон доступных сетевых портов для введённого диапазона IP-адресов;

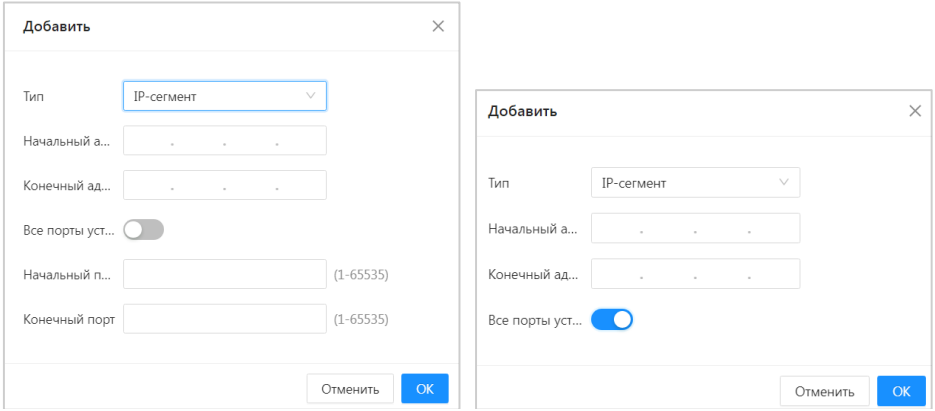


Рисунок 12.11 – Добавить диапазон IP

– Добавление при введении MAC-адреса;

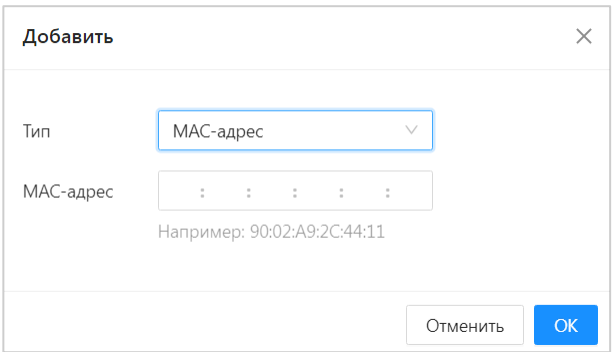


Рисунок 12.12 – Добавить MAC-адрес

– Добавление для всех IP-адресов диапазона портов с начального порта до конечного.

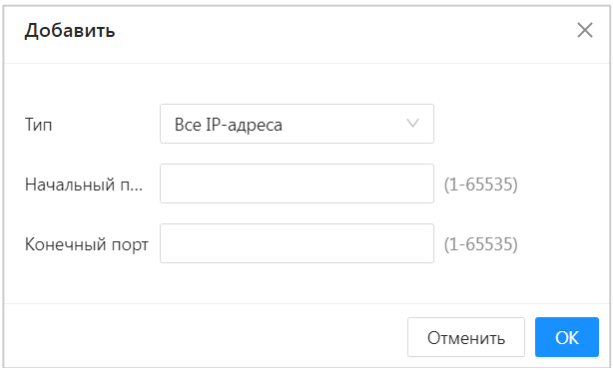


Рисунок 12.13 – Добавить все IP-адреса

12.3.2 Пункт «Защита от атак DoS»

Выберите «SYN атаки (Защита от атак с переполнением SYN)» или «ICMP атаки (Защита от атак с переполнением ICMP)» для защиты устройства от DoS-атак.

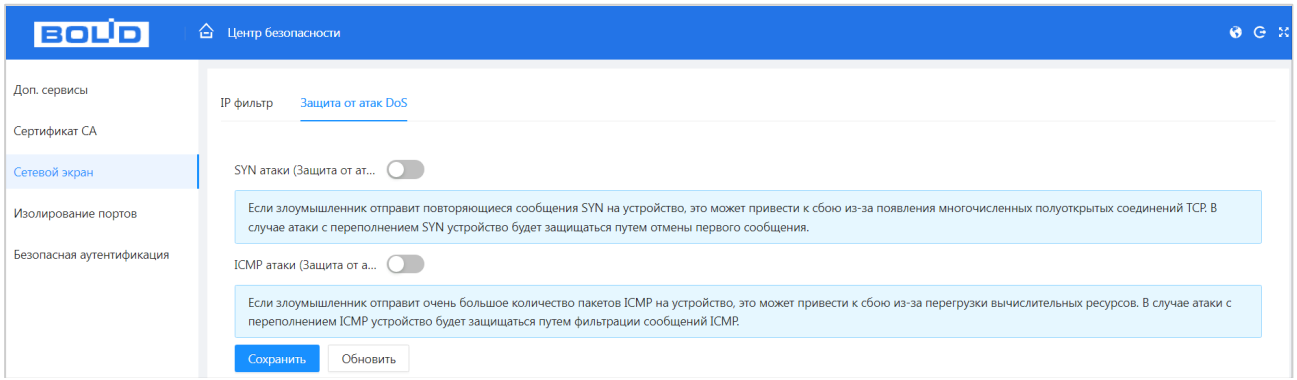


Рисунок 12.14 – Включение защиты от DoS-атак

12.4 Подраздел «Изолирование портов»

Изоляция портов обеспечивает разделение трафика на канальном уровне (уровне 2).

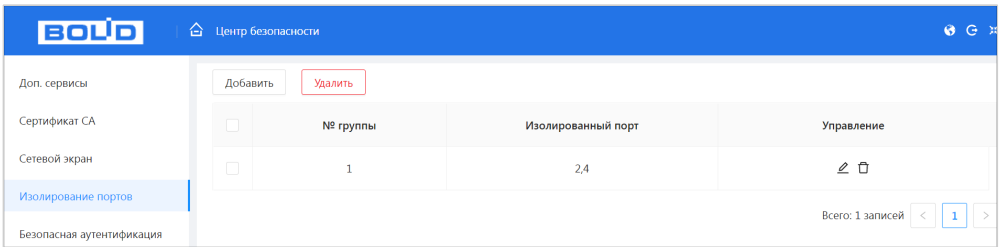


Рисунок 12.15 – Изолирование портов

Чтобы изолировать L2-данные между портами, нужно добавить порты в группу изоляции. Для этого:

1. Нажмите кнопку «Добавить».

2. Далее в появившемся окне установите группу (доступно 4 группы) и установите порты, которые будут входить в эту группу.

3. После сохранения кадры канального уровня не будут передаваться между портами этой группы.

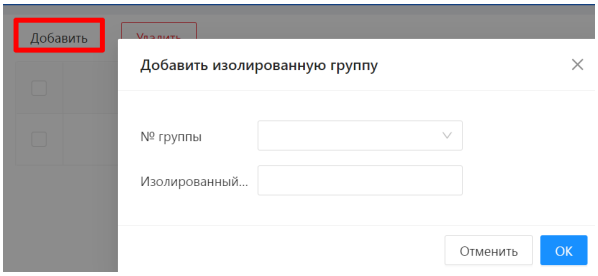


Рисунок 12.16 – Добавление группы

12.5 Подраздел «Безопасная аутентификация»

12.5.1 Пункт «Алгоритм проверки подлинности»

Выбор алгоритма дайджеста для аутентификации.

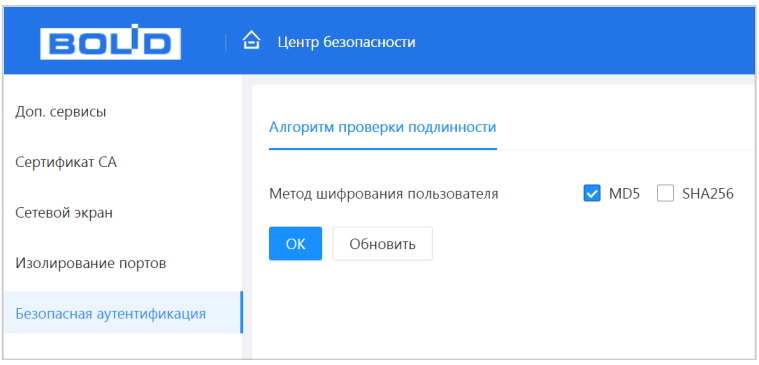


Рисунок 12.17 – Алгоритм проверки подлинности

13 РАЗДЕЛ ГЛАВНОГО МЕНЮ «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 помещён в очередь с более низким приоритетом, где допускаются временные задержки и могут быть при необходимости отброшены.

13.1 Подраздел «Приоритет портов»

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

Режим доверия «802.1p»

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 13.1 – 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.

Режим доверия «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.

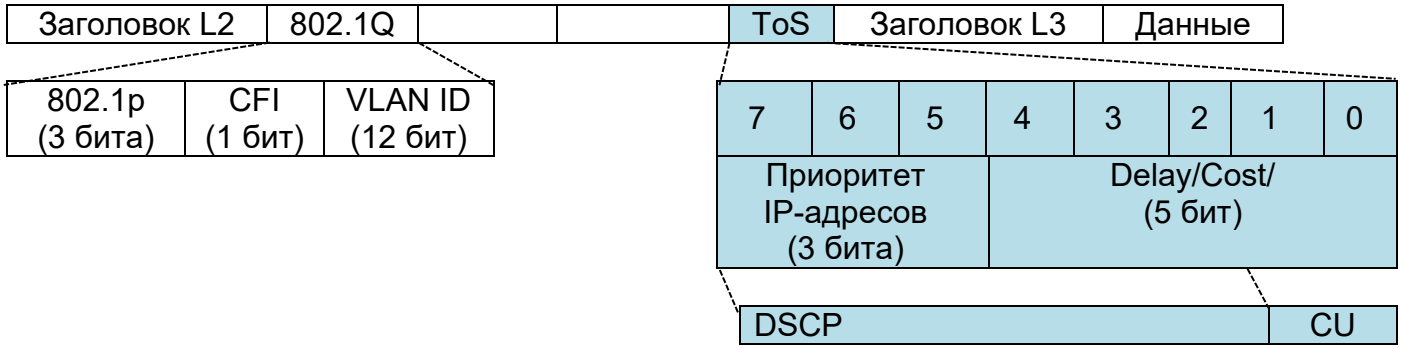


Таблица 13.2 – Привязка по умолчанию DSCP к CoS (приоритетам 802.1p)

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

13.1.1 Настройка

В зависимости от задачи установите из выпадающего списка «Режим доверия» и приоритет на порту:

Режим доверие включает четыре варианта: Untrust (не доверять), 802.1P, DSCP и DSCP & 802.1P.

Выбор режима определяет, какие метки приоритета будут учитываться входящими портами (только 802.1p, только DSCP, оба или ни одного).

📖 По умолчанию приоритет 802.1p и приоритет DSCP для голосовой VLAN равны 6 и 46 соответственно.

Нажмите OK для сохранения настроек.

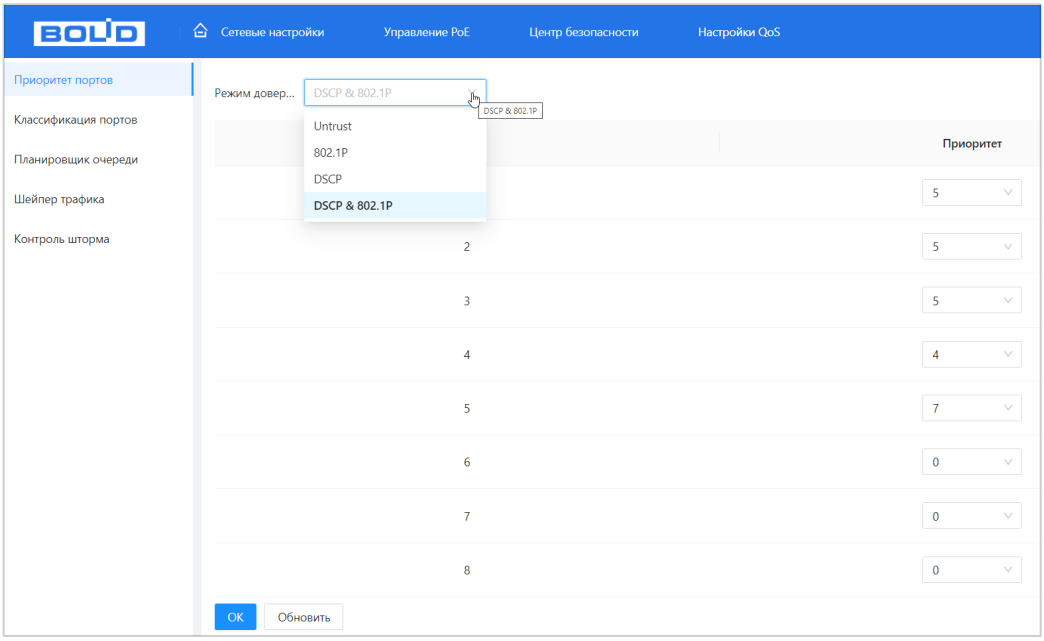


Рисунок 13.1 – Настройка приоритетности

13.2 Подраздел «Классификация портов»

Для корректного распределения трафика по очередям и обеспечения качества обслуживания (QoS) настраивается сопоставление меток приоритета, содержащихся в пакетах (DSCP в заголовке IPv4 или 802.1p в 802.1Q VLAN-кадре), с локальными приоритетами коммутатора или шлюза. Это позволяет устройству правильно размещать пакеты в очередях и применять соответствующие политики обработки.

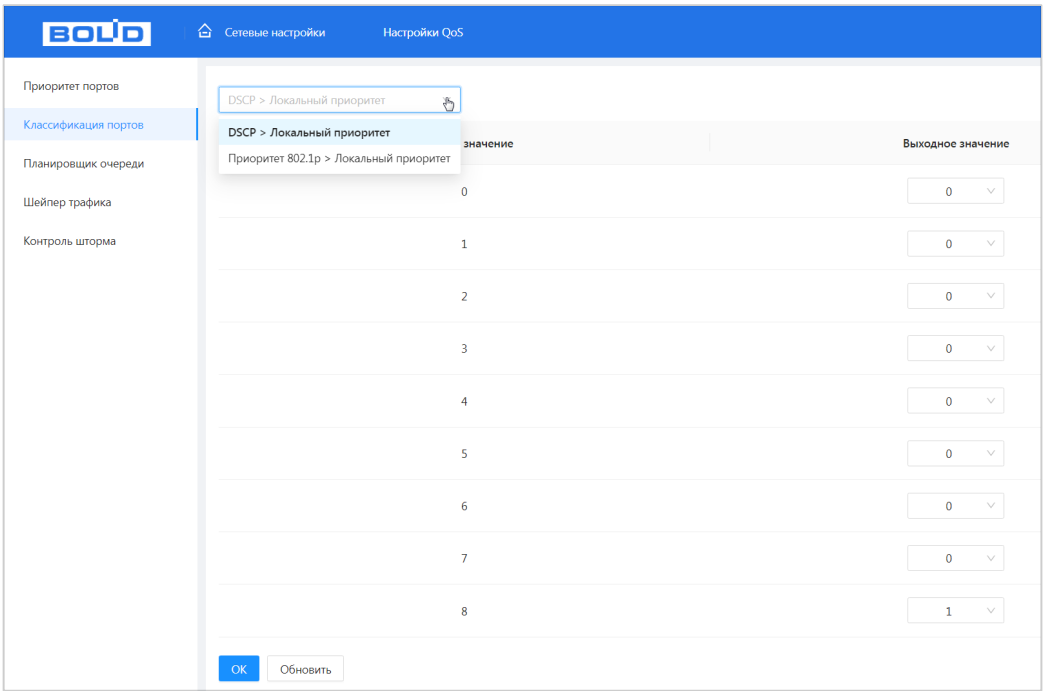


Рисунок 13.2 – Классификация портов

13.3 Подраздел «Планировщик очереди»

Настройки и просмотр информации о весе пакета в очереди.

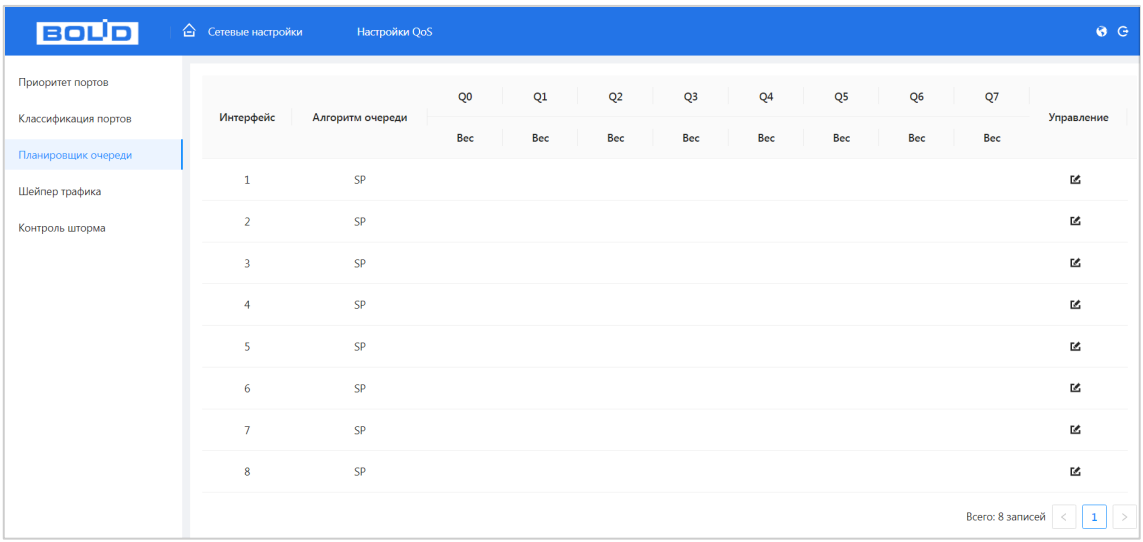


Рисунок 13.3 – Планировщик очереди

Выберите порт и нажмите кнопку в столбце «Управление». Появившейся окно настроек позволяет:

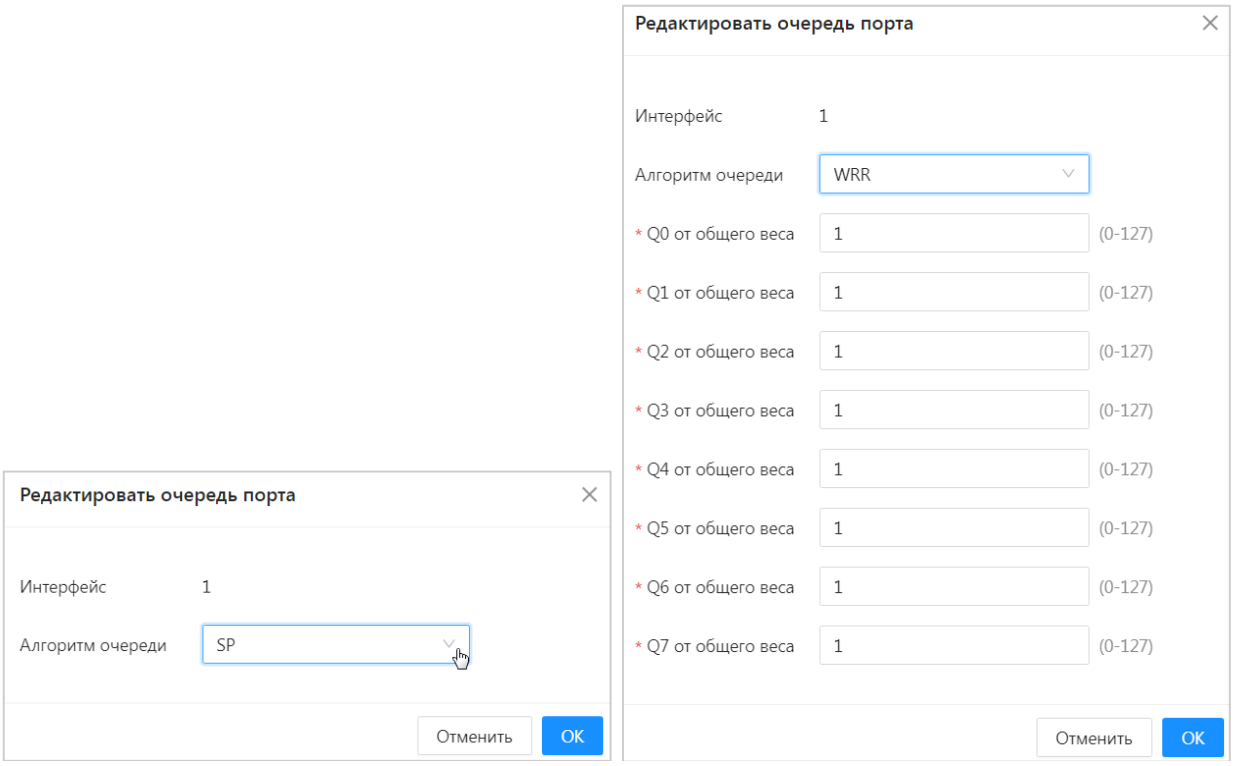


Рисунок 13.4 – Настройка очереди порта

1. Выбирать алгоритм работы.

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

– Priority queuing (PQ – строгий приоритет очереди) – пакеты распределяются в соответствии с установленным приоритетом. Сначала отправляются пакеты с наивысшим приоритетом в очереди, затем со следующей очереди и так до очереди с наименьшим приоритетом;

– Weighted Round Robin (WRR – взвешенная справедливая очередь) – При планировании по WRR устройство обслуживает очереди в опросном порядке на основе веса каждой очереди. После одного раунда планирования веса всех очередей уменьшаются на 1. Очередь, чей вес уменьшился до 0, не может быть запланирована.

📖 В режиме WRR весовое соотношение приоритетной очереди равно Queue0:Queue1:Queue2:Queue3=1:2:4:8.

2. Настроить скорость и вес входящего трафика для 8 уровней приоритетов (от Q0 до Q7).

13.4 Подраздел «Шейпер трафика»

Настройки и просмотр информации о скорости передачи трафика.

Нажмите кнопку «Добавить» и в появившемся окне заполните поля.

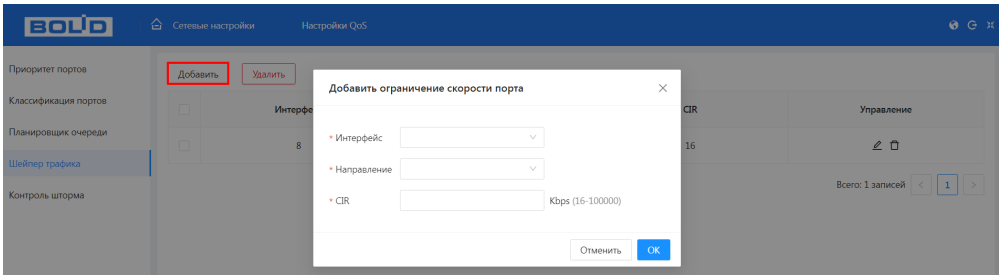


Рисунок 13.5 – Шейпер трафика

13.5 Подраздел «Контроль шторма»

Настройте защиту от сетевого шторма. Устройство поддерживает три пакета, которые могут нести угрозу: одноадресный, многоадресный и широковещательный.

Выберите пакет и включите защиту от сетевого шторма. В поле ввода, столбец «Скорость», введите пропускную скорость пакетов. Например, выберите «Одноадресный» установите флажок «Включить» и введите 1024 с в поле «Скорость». Это означает, что порт может принимать одноадресные пакеты на скорости до 1024 Кб/с.

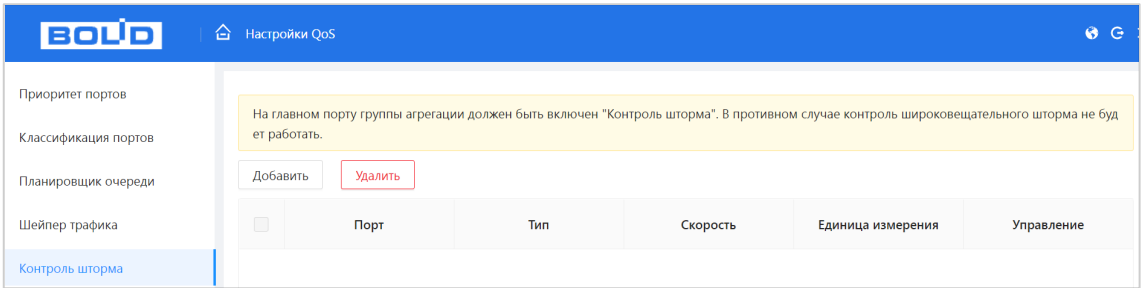


Рисунок 13.6 – Штормовой ограничитель

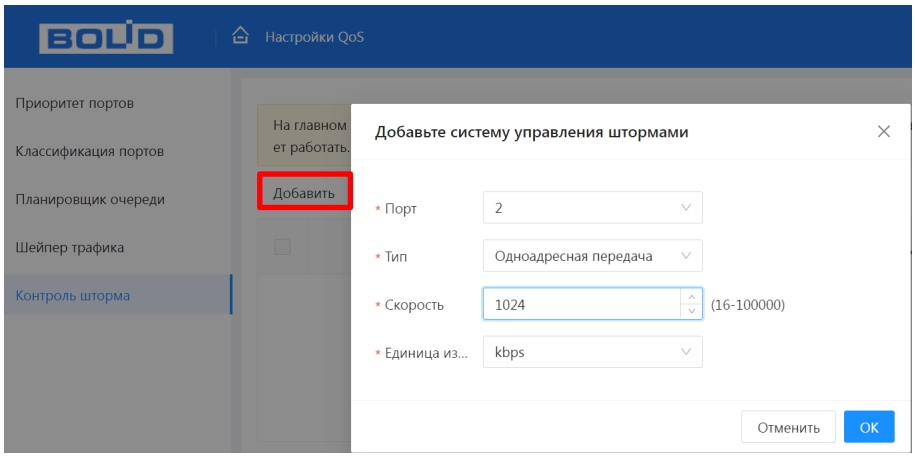


Рисунок 13.7 – Добавление и настройка

14 РАЗДЕЛ ГЛАВНОГО МЕНЮ «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.

14.1 Подраздел «Настройка 802.1X (NSA)»

Это меню позволяет управлять состоянием аутентификации порта.

Поддерживается три следующих авторизованных состояния:

– Авто – означает, что начальное состояние порта является неавторизованным. Это не позволяет получить доступ в сеть; Порт будет переключен в авторизованное состояние, если клиент пройдёт проверку подлинности. После этого сможет обмениваться данными в сети;

– 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.

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:

3. Переключите все порты в состояние аутентификации на основе 802.1x как показано на рисунке ниже (Рисунок 14.1).

4. Настройте адрес сервера аутентификации, как показано на рисунке (см. Рисунок 14.2).

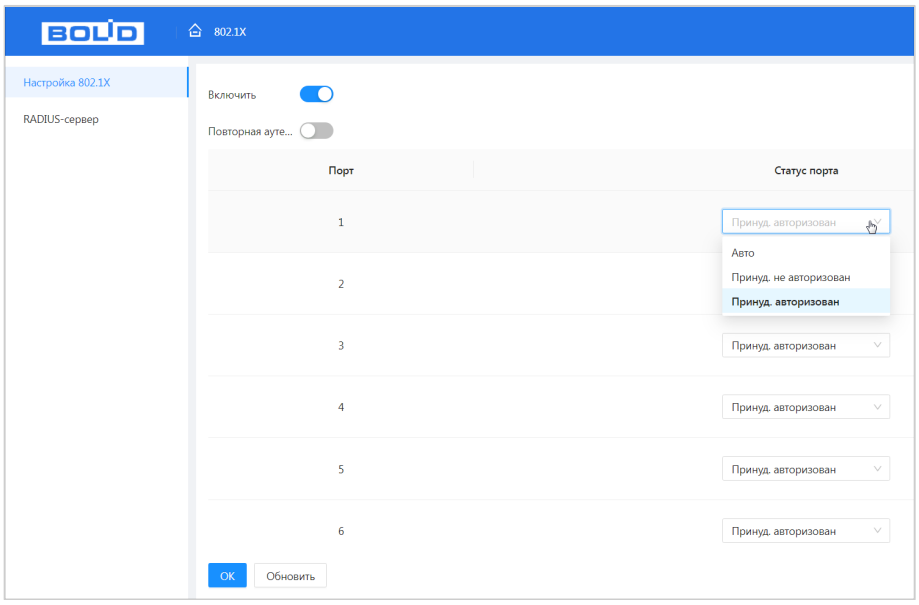


Рисунок 14.1 – Настройки NSA

14.2 Подраздел «RADIUS-сервер»

RADIUS (Remote Authentication Dial-In User Service) – распространённый протокол для реализации AAA: аутентификации, авторизации и учёта (Authentication, Authorization and Accounting).

Это протокол взаимодействия с распределённой клиент-серверной архитектурой, предназначенный для защиты сети от неавторизованного доступа и применения в средах с удалённым доступом и повышенными требованиями к безопасности.

Протокол определяет формат RADIUS-пакетов и механизм передачи сообщений; в качестве транспортного протокола используется UDP. Первоначально RADIUS создавался для разрешения доступа dial-up пользователей, но по мере развития технологий стал применяться и для других типов доступа, например, Ethernet и ADSL. RADIUS обеспечивает процедуру аутентификации и авторизации при подключении к серверу и ведёт учёт использования сетевых ресурсов (accounting).

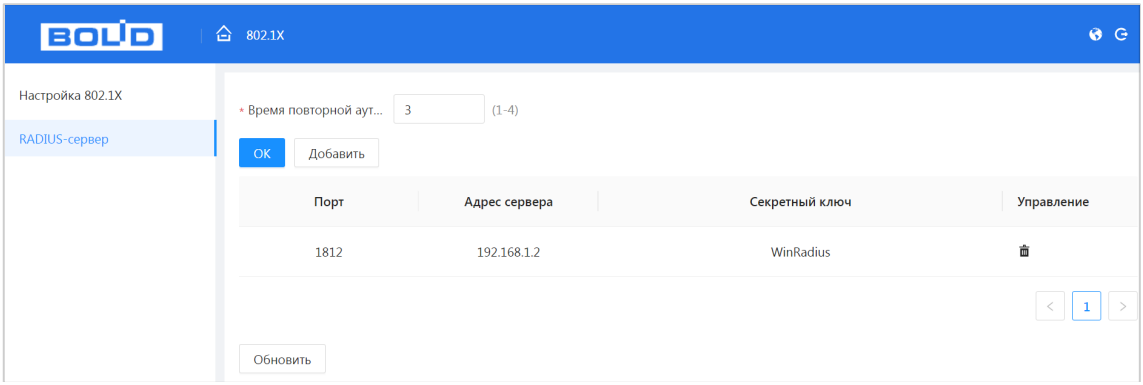


Рисунок 14.2 – Настройки Radius

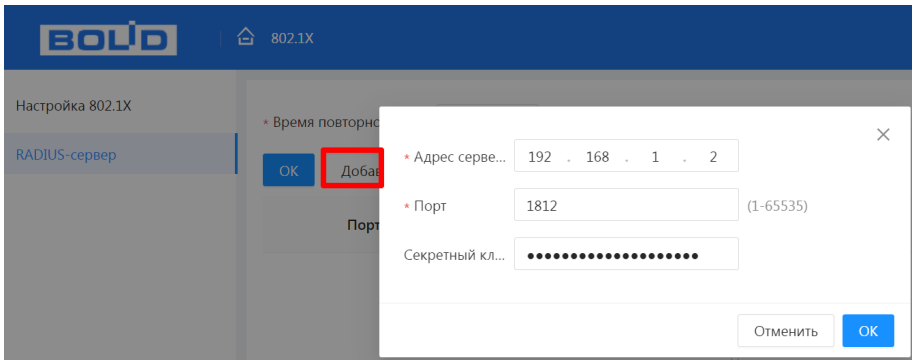


Рисунок 14.3 – Добавление

15 СБРОС НА ЗАВОДСКИЕ НАСТРОЙКИ

15.1 Сброс через веб-интерфейс

1. Перейдите «Главное меню → Обслуживание системы → Обслуживание».

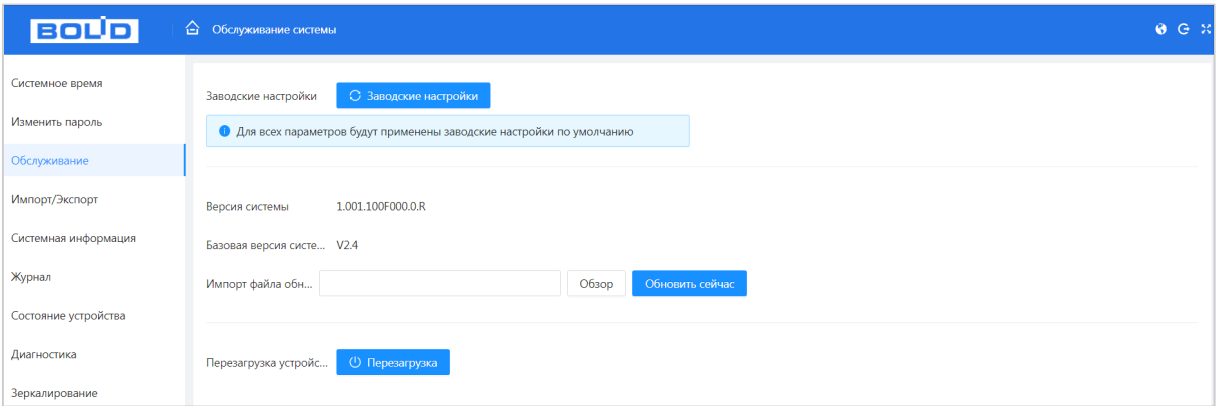


Рисунок 15.1 – Сброс на заводские настройки

2. Нажмите кнопку «Заводские настройки».

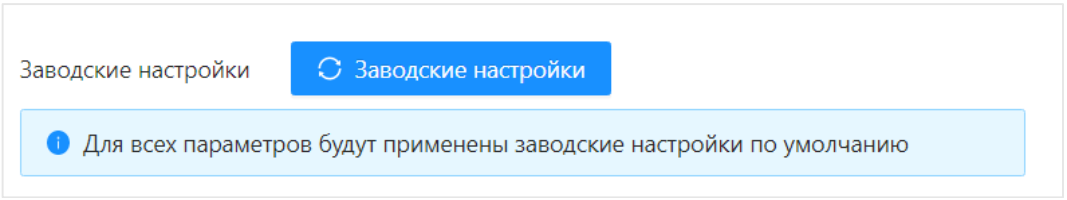


Рисунок 15.2 – Сброс на заводские настройки

3. Далее в появившемся окне введите пароль устройства.

4. Нажмите «ОК».

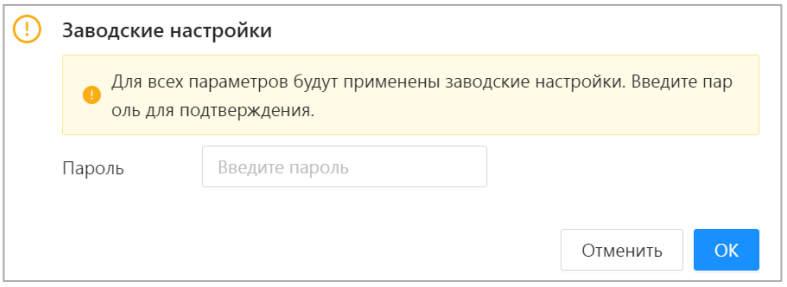


Рисунок 15.3 – Ввод пароля

Произойдёт перезагрузка устройства. Все ранее установленные настройки будут сброшены и восстановлены заводские настройки.

После перезагрузки устройство будет доступно со следующими сетевыми параметрами:

IP-адрес	192.168.1.110
Маска подсети	255.255.255.0

15.2 Сброс на заводские настройки с помощью кнопки «RESET»

Сброс до заводских настроек возможен при помощи кнопки сброса «RESET» на передней панели. Данный способ используется при невозможности сброса через веб-интерфейс устройства.

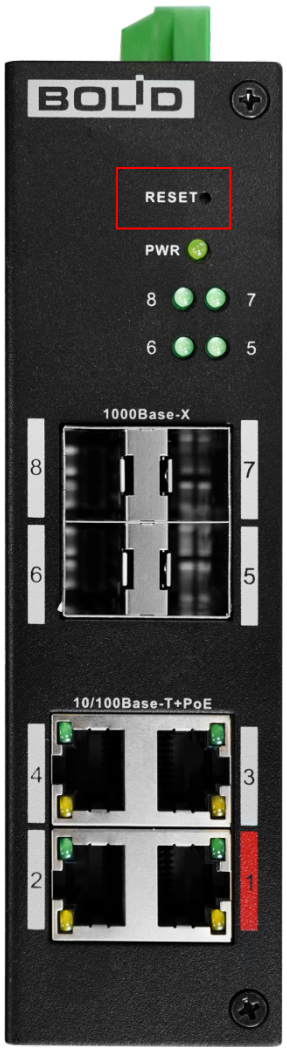


Рисунок 15.2 – Сброс на заводские настройки

В случае невозможности восстановления пароля администратора:

1. Подключите источник питания и дождитесь загрузки устройства.

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

3. Отпустите кнопку «RESET».

4. Коммутатор приблизительно через 180 секунд загрузится, и настройки вернутся к заводским (полный сброс всех настроек).

16 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. Актуальную версию программы можно скачать на сайте bolid.ru в разделе: «Продукция → Видеонаблюдение → Программное обеспечение → ПО «BOLID VideoScan»».

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

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

Выполнив запуск утилиты BOLID VideoScan, в открывшемся окне визуального интерфейса пункта меню «Сеть» измените IP-адрес изделия и чтобы завершить изменение нажмите кнопку «Сохранить». На рисунке (Рисунок 16.1) представлены базовые параметры для изменения.

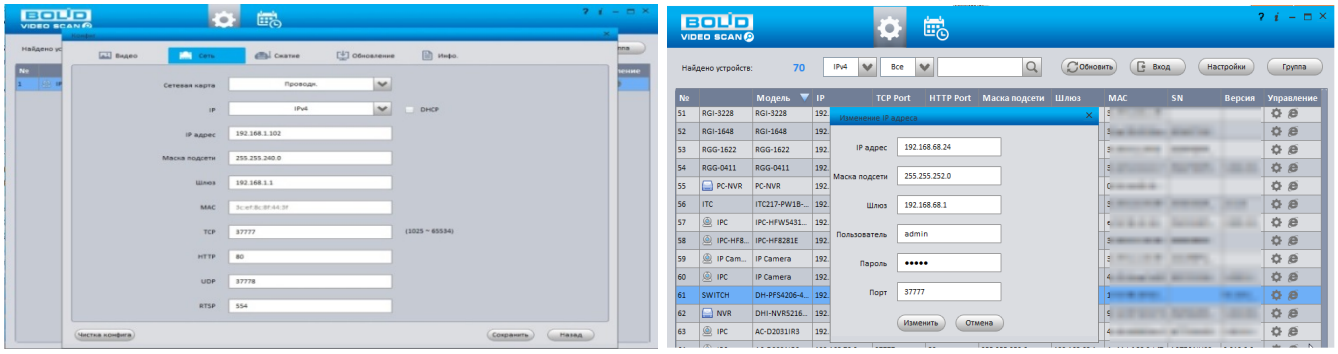


Рисунок 16.1 – Работа с BOLID VideoScan

17 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, надёжности креплений, контактных соединений;

– Очистку корпуса от пыли и грязи;

– Тестирование кабельных линий связи и электропитания;

– Очистку и антикоррозийную обработку электроконтактов кабельного подключения.

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

18 ВОЗМОЖНЫЕ НЕИСПРАВНОСТИ И СПОСОБЫ ИХ УСТРАНЕНИЯ

СПРАВКА:
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 18.1).

Таблица 18.1 – 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.
	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.

19 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, размещённом 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), применённые логин и пароль.

Рекламации направлять по адресу:

АО 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.

20 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.

21 УПАКОВКА

Изделие и эксплуатационная документация упакованы в картонную коробку.

22 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.

23 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

24 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 изделия приобретатель изделия 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.

25 ГАРАНТИИ ИЗГОТОВИТЕЛЯ

Гарантийный срок эксплуатации – 36 месяцев с даты приобретения.

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

26 СВЕДЕНИЯ О СЕРТИФИКАЦИИ

Изделие соответствует требованиям технических регламентов Таможенного союза ТР ТС 004/2011 «О безопасности низковольтного оборудования», ТР ТС 020/2011 «Электромагнитная совместимость технических средств» и 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.03.001732.

27 СВЕДЕНИЯ О ПРИЁМКЕ

Изделие, коммутатор сетевой «BOLID SW-204» АЦДР.203729.005, принято в соответствии с обязательными требованиями государственных стандартов и действующей технической документации, признано годным к эксплуатации АО 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
Форм-фактор	SFP	SFP	SFP	SFP
Пропускная способность	1 Гбит/с	1 Гбит/с	1 Гбит/с	1 Гбит/с
Длина кабеля	550 м	20 км	20 км	20 км
Кол-во используемых волокон	2	2	1	1
Тип разъёма	LC/UPC	LC/UPC	LC/UPC	LC/UPC
Тип оптоволоконного кабеля	MM	SM	SM	SM
Парность	Tx850/ Rx850	Tx1310/ Rx1310	Tx1310/ Rx1550	Tx1550/ Rx1310
Напряжение питания	3,3 В	3,3 В	3,3 В	3,3 В
Диапазон рабочих температур	От -40 °С до +85 °С	От -40 °С до +85 °С	От -40 °С до +85 °С	От -40 °С до +85 °С
Относительная влажность воздуха	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

Перечень терминов и сокращений

БП	Блок питания
Веб	Web (паутина) – сокращенное альтернативное название Всемирной Сети Интернет, являющей собой систему взаимосвязанных за счет ссылок отдельных веб-страниц и других документов
ЗИП	Запасные части, инструменты и принадлежности
ПО	Программное обеспечение
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
DNS	Domain Name System – Система доменных имён. Таблица перевода интернет имён в IP-адреса
ID	Identifier – идентификатор
IP	Internet Protocol – межсетевой протокол
IPv4	Internet Protocol version 4 – четвёртая 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)
MAC	Media Access Control – уникальный идентификатор, присваиваемый сетевым адаптерам. Играет роль физического адреса сетевого адаптера
PoE	Power over Ethernet – стандарты IEEE 802.3af, IEEE 802.3at, позволяющие передавать по сети Ethernet не только данные, но и электрический ток
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 приёмопередатчиков (трансиверов), используемых для передачи и приема данных в телекоммуникациях
SFP+	Enhanced Small Form-factor Pluggable, SFF-8431, SFF-8083 – промышленный стандарт модульных компактных приёмопередатчиков (трансиверов), используемых для передачи данных в телекоммуникациях. Расширенная версия приемопередатчика SFP, способного поддерживать скорости передачи данных 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
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
VLC	Свободный медиапроигрыватель, поддерживающий различные форматы воспроизведения
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					
0	–	–	–	–	32	269039			27.09. 2019
1	1 – 35	1 – 35	32 – 36	–	36	290513			25.12. 2020
2	1 – 37	1 – 37	36 – 37	–	37	309363			06.12. 2021
3	3 – 38	3 – 38	37 – 38	–	38	326252			02.03. 2023
4	3 – 45	3 – 45	38 – 45	–	45	352275			18.08. 2023
5	3, 9, 13 – 45	3, 9, 13 – 45	45 – 46	–	46	360891			02.11. 2023
6	3, 6 – 8, 41 – 46	3, 6 – 8, 41 – 46	46 – 47	–	47	423143			05.07. 2024
7	2, 18, 29, 32, 39, 40, 41, 46, 47	2, 18, 29, 32, 39, 40, 41, 46, 47	–	–	47	581044			03.07. 2025
8	1 – 129	1 – 129	47 – 129	–	129	596719			12.12. 2025

АО НВП «Болид»

Центральный офис:

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