

Сетевой коммутатор

BOLID SW-324

Версия 2

Руководство по эксплуатации

АЦДР.203729.006 РЭп

Настоящее руководство по эксплуатации (далее по тексту – РЭ) содержит сведения о назначении, конструкции, принципе работы, технических характеристиках управляемого сетевого коммутатора L2+ «BOLID SW-324» АЦДР.203729.006 (далее по тексту – коммутатор, устройство 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 отличаются от версии 1.
- Руководство по эксплуатации описывает интерфейс и функциональные возможности внутреннего ПО – 1.001.100F001.0.R (сборка от 13.05.2026).
- 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 7
2 ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ 9
3 КОМПЛЕКТНОСТЬ 12
4 КОНСТРУКЦИЯ 13
4.1 Передняя панель 13
4.1.1 RJ-45 13
4.1.2 Установка SFP 14
4.2 Задняя панель 15
4.2.1 Заземление (GND) 15
5 МОНТАЖ И ДЕМОНТАЖ 17
5.1 Меры безопасности 17
5.2 Монтаж 18
5.2.1 Подготовка изделия к монтажу 19
5.2.1 Монтаж коммутатора в 19”-стойку 20
5.3 Демонтаж 20
6 ПЕРВОЕ ВКЛЮЧЕНИЕ. ИНИЦИАЛИЗАЦИЯ УСТРОЙСТВА 21
6.1 Инициализация устройства 21
6.2 Системное время 22
6.3 Локальный адрес 23
7 ГЛАВНОЕ МЕНЮ 25
8 РАЗДЕЛ ГЛАВНОГО МЕНЮ «БЫСТРАЯ НАСТРОЙКА» 29
8.1 Подраздел «Общие» 29
8.2 Подраздел «Информация о портах» 30
8.3 Подраздел «Список устройств» 32
9 РАЗДЕЛ ГЛАВНОГО МЕНЮ «ОБСЛУЖИВАНИЕ СИСТЕМЫ» 33
9.1 Подраздел «Системное время» 33
9.2 Подраздел «Изменить пароль» 34
9.3 Подраздел «Обслуживание» 35
9.4 Подраздел «Импорт/Экспорт» 36
9.4.1 Экспорт (Конфигурация резервного копирования) 37

9.4.2 Импорт (Восстановление конфигурации)....37
9.5 Подраздел «Системная информация»....38
9.6 Подраздел «Журнал»....39
9.7 Подраздел «Состояние устройства»....39
9.8 Подраздел «Диагностика»....40
9.9 Подраздел «Зеркалирование»....41
10 РАЗДЕЛ ГЛАВНОГО МЕНЮ «СЕТЕВЫЕ НАСТРОЙКИ»....43
10.1 Подраздел «Порт»....43
10.2 Подраздел «Энергоэффективный Ethernet (EEE (Energy Efficient Ethernet))»....46
10.3 Подраздел «VLAN»....46
10.3.1 Пункт «Добавить VLAN»....46
10.3.2 Пункт «VLAN»....48
10.4 Подраздел «Интерфейс VLAN (VLANIF)»....49
10.5 Подраздел «Настройки маршрутизации»....50
10.6 Подраздел «Таблица маршрутизации»....50
10.7 Подраздел «ARP-таблица»....51
10.8 Подраздел «ERPS»....52
10.8.1 Быстрая настройка ERPS....52
10.8.2 Расширенные настройки....55
10.9 Подраздел «IGMP Snooping»....63
10.10 Подраздел «STP»....65
10.10.1 Пункт «STP»....65
10.10.2 Пункт «Экземпляр порта»....66
10.11 Подраздел «Агрегация каналов»....67
10.11.1 Статическая агрегация....68
10.11.2 LACP....69
10.12 Подраздел «SNMP»....71
10.13 Подраздел «MAC-адрес»....75
10.13.1 Пункт «Таблица MAC-адресов»....75
10.13.2 Пункт «Фильтрация MAC-адресов»....75

10.14 Подраздел «LLDP»....76
10.15 Подраздел «Обнаружение петель»....77
10.16 Подраздел «DHCP-сервер»....77
10.16.1 Пункт «DHCP-сервер»....78
10.16.2 Пункт «Статическая привязка»....80
10.16.3 Пункт «Список адресов»....81
10.17 Подраздел «DHCP Snooping»....81
10.17.1 Пункт «Глобальные настройки»....81
10.17.2 Пункт «Конфиг-я порта»....82
10.17.3 Пункт «Конфигурация опции 82»....83
10.18 Подраздел «Тестирование виртуального кабеля»....84
11 РАЗДЕЛ ГЛАВНОГО МЕНЮ «ЦЕНТР БЕЗОПАСНОСТИ»....86
11.1 Подраздел «Доп. сервисы»....86
11.1.1 Пункт «Доп. сервисы»....86
11.1.2 Пункт «HTTPS»....87
11.2 Подраздел «Telnet»....88
11.3 Подраздел «Сертификат CA»....89
11.3.1 Пункт «Сертификат устройства»....89
11.3.2 Пункт «Доверенные сертификаты CA»....91
11.4 Подраздел «Сетевой экран»....91
11.4.1 Пункт «IP фильтр»....91
11.4.2 Пункт «Защита от атак DoS»....93
11.5 Подраздел «Изолирование портов»....94
11.6 Подраздел «Безопасная аутентификация»....94
11.6.1 Пункт «Алгоритм проверки подлинности»....94
12 РАЗДЕЛ ГЛАВНОГО МЕНЮ «НАСТРОЙКИ QOS»....95
12.1 Подраздел «Приоритет портов»....95
Режим доверия «802.1p»....95
Режим доверия «DSCP»....97
12.1.1 Настройка....97
12.2 Подраздел «ACL»....98

12.2.1 Пункт «Конфигурация ACL» 98
12.2.2 Пункт «Период» 108
12.2.3 Пункт «Привязка ACL» 108
12.3 Подраздел «Классификация портов» 109
12.4 Подраздел «Планировщик очереди» 110
12.5 Подраздел «Шейпер трафика» 111
12.6 Подраздел «Контроль шторма» 111
13 РАЗДЕЛ ГЛАВНОГО МЕНЮ «802.1X» 113
13.1 Подраздел «Настройка 802.1X (NSA)» 113
13.2 Подраздел «RADIUS-сервер» 114
14 СБРОС НА ЗАВОДСКИЕ НАСТРОЙКИ 116
14.1 Сброс через веб-интерфейс 116
14.2 Сброс на заводские настройки с помощью кнопки «RESET» 117
15 РАБОТА С УТИЛИТОЙ «BOLID VIDEOSCAN» 118
16 ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ И ПРОВЕРКА РАБОТОСПОСОБНОСТИ 119
17 ВОЗМОЖНЫЕ НЕИСПРАВНОСТИ И СПОСОБЫ ИХ УСТРАНЕНИЯ 120
18 РЕМОНТ 121
19 МАРКИРОВКА 122
20 УПАКОВКА 123
21 ХРАНЕНИЕ 124
22 ТРАНСПОРТИРОВКА 125
23 УТИЛИЗАЦИЯ 126
24 ГАРАНТИИ ИЗГОТОВИТЕЛЯ 127
25 СВЕДЕНИЯ О СЕРТИФИКАЦИИ 128
26 СВЕДЕНИЯ О ПРИЁМКЕЕ 129
ПРИЛОЖЕНИЕ А 130

1 ОБЩИЕ СВЕДЕНИЯ

1. Управляемый сетевой коммутатор BOLID SW-324 с поддержкой функций L2+ предназначен для объединения сетевых устройств и сегментов локальной сети, а также передачи данных между ними. Изделие может использоваться для подключения сетевых видеокамер, видеорегистраторов, других коммутаторов и оборудования систем охранного телевидения (СОТ).

2. Коммутатор оснащён восемью портами RJ-45 10/100/1000 Мбит/с, двадцатью четырьмя портами SFP 100/1000 Мбит/с и четырьмя портами SFP+ 1000/10 000 Мбит/с. Порты SFP и SFP+ предназначены для установки совместимых приёмопередающих модулей и организации соединений между сегментами сети. Технология PoE не поддерживается.

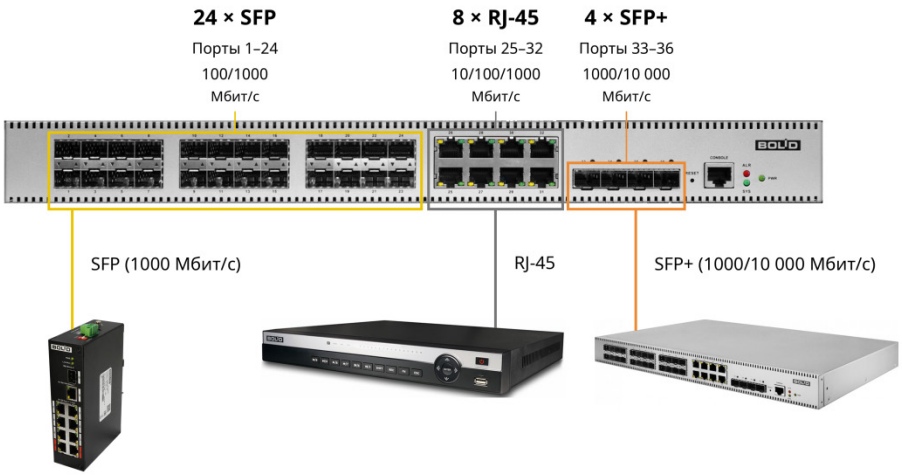


Рисунок 1.1 – Сетевое соединение

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 изделия: системы видеонаблюдения, охранно-пожарная сигнализация, СКУД, системы контроля и диспетчеризации объектов.

5. Коммутатор рассчитан на круглосуточный режим работы.

6. Коммутатор является восстанавливаемым, периодически обслуживаемым изделием.

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

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

9. Основным отличием версии 2 от версии 1 является наличие двух встроенных блоков питания с резервированием, что повышает надёжность работы коммутатора.

10. Возможное применение:

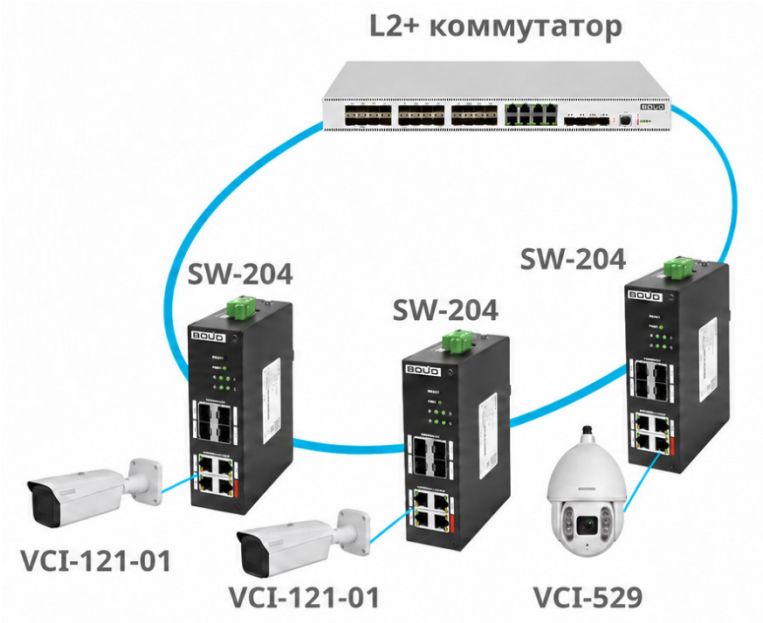


Рисунок 1.2 – Кольцевое соединение

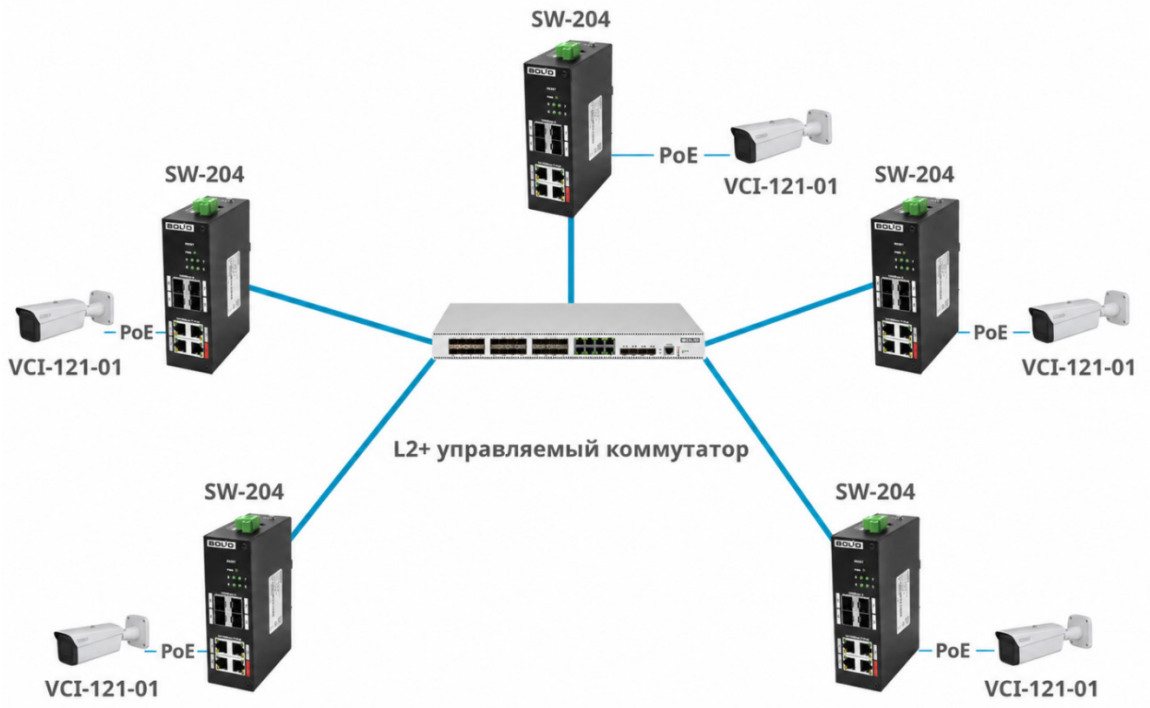


Рисунок 1.3 – Звезда

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	36 интерфейсов
RJ-45	Порт № 25 – 32: 10/100/1000 Мбит/с
SFP	Порт № 1 − 24: 100/1000 Мбит/с
SFP+	Порт № 33 – 36: 1/10 Гбит/с
Оборудование	
Общее количество	37 портов
Порты RJ-45	8 портов
Порты SFP	24 порта
Порты SFP+	4 порта
Порт управления	1 порт (RS-232)
Электропитание (переменный ток)	
Напряжение питания устройства	2 встроенных блока питания 100 − 240 В переменного тока
Потребляемый ток	2,5 А (макс.)
Потребляемая мощность	23,8 Вт в дежурном режиме ≤ 100 Вт при полной нагрузке
Производительность	
Уровень	L2+
Тип	Управляемый
Время технической готовности прибора к работе	50 с
Коммутационная матрица	144 Gbps
Скорость перенаправления пакетов	107.136 Mpps
Буфер пакетов	16 Мбит
Jumbo-кадр	12288 байт
Таблица MAC-адресов	32 К

Наименование параметра	Значение параметра
Общее количество статических MAC-адресов	256
Число VLAN	4094
VLAN интерфейсы	16
Поддерживаемые стандарты	IEEE 802.3; IEEE 802.3u; IEEE 802.3x; IEEE 802.3ab; IEEE 802.3z; IEEE 802.3ad
Функции	
Управление устройством	Веб-интерфейс, TELNET, SNMP V1/V2C/V3, SSH
ARP	1 К
Функции порта	Управление потоком IEEE 802.3x, Unicast Suppression, контроль штормов мультикаст-трафика, Контроль штормов широковещательного трафика
Таблица MAC-адресов	Поддержка статического MAC-адреса
Spanning Tree Protocol	STP, RSTP, ERPS
VLAN	802.1Q
Управление потоками	Поддержка управления потоком на основе IEEE802.3X
Агрегирование (объединение) каналов	LACP, статическое агрегирование, динамическое агрегирование
Зеркалирование портов	1:1 (Один к одному), N:1 (Много к одному)
Multicast	IGMP Snooping
DHCP	DHCP-клиент, DHCP-сервер
Безопасность	IEEE802.1x, изоляция порта, Radius, HTTPS, LLDP
QoS/ACL	Планирование очереди SP/WRR, Сопоставление приоритетов 802.1p DSCP, Ограничение скорости порта
Системное обслуживание	Загрузка и выгрузка файла настроек, обновление прошивки, системный журнал, сброс до заводских настроек, NTP

Наименование параметра		Значение параметра
Общие сведения		
Предельное напряжение импульсных помех		2 кВ/1 кВ**
Защита от статического электричества		Наведенная:8 КВ Контактный разряд: 6 КВ
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
Относительная влажность воздуха		От 5 % до 95 %
Диапазон рабочих температур		От -20 °С до +55 °С
Габаритные размеры		440×308,3×44,0 мм
Масса		Вес нетто: 3,8 кг Вес брутто: 5,3 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

*Технические характеристики могут быть изменены без предварительного уведомления.

**В зависимости от синфазного или разностного сигналов.

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

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

3 КОМПЛЕКТНОСТЬ

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

Таблица 3.1 – Комплект поставки*

Обозначение	Наименование	Количество
АЦДР.203729.006	Коммутатор «BOLID SW-324»	1 шт.
АЦДР.203729.006 РЭ	Руководство по эксплуатации изделия «BOLID SW-324»	1 экз.
	Крепление в стойку	2 шт.
	Винт М3×5	6 шт.
	Кабель питания, 250 В переменного тока	2 шт.
	SFP модуль**	—
	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 Передняя панель

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

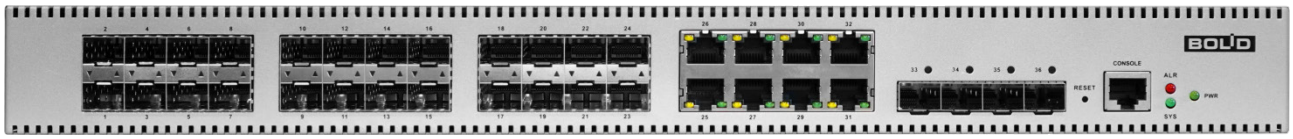


Рисунок 4.1 – Передняя панель

Таблица 4.1 – Порты и индикаторы передней панели

Параметр	Описание
PWR	Световой индикатор электропитания.
SYS	Световой индикатор состояния коммутатора. Мигание индикатора означает нормальную работу устройства. При нарушениях работы коммутатора индикатор будет гореть непрерывно.
ALR	Световой индикатор тревоги.
Reset	Кнопка сброса на заводские настройки. Подробнее о сбросе смотрите – 14.2 Сброс на заводские настройки с помощью кнопки «RESET».
Console (RS-232)	Порт сервисного обслуживания.
24 порта 100/1000 Base-X (SFP)	Порты для подключения модулей стандарта SFP.
8 портов 10/100/1000 Base-T	Порты стандарта RJ-45 (Без поддержки PoE).
4 порта 1000/10000 Base-X (SFP+)	Порты для подключения модулей стандарта SFP+. Фактическая скорость до 10 Гб/с.

4.1.1 RJ-45

Для подключения к портам Ethernet следует использовать кабель «витая пара» UTP/FTP категории 5 либо выше.

Допускается использование как экранированного, так и неэкранированного кабеля. Кабель подсоединяется к разъёмам RJ-45 коммутатора с помощью стандартного штекера 8P8C.

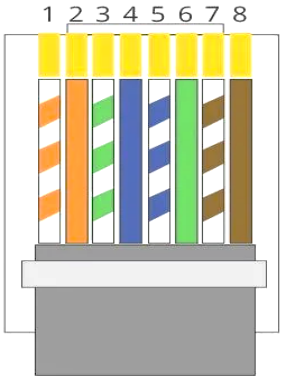


Рисунок 4.2 – Штекер 8P8C

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

4.1.2 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.

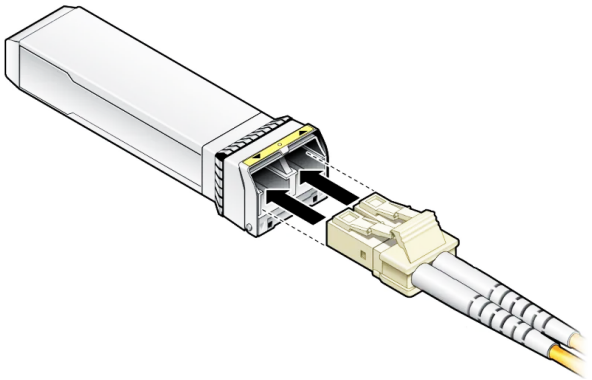


Рисунок 4.3 – Подключения кабеля

4.2 Задняя панель

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

На задней панели устройства расположен винт защитного заземления, вентиляционные отверстия и разъёмы питания с поддержкой 100 – 240 В переменного тока.

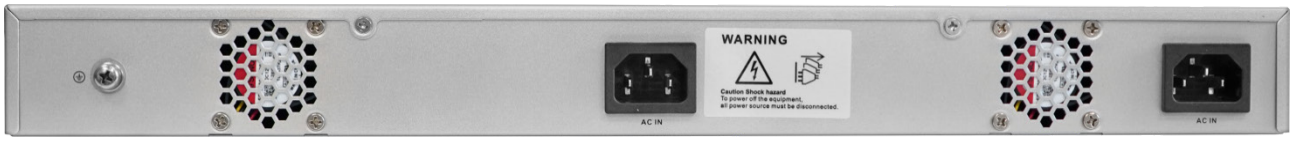


Рисунок 4.4 – Задняя панель

4.2.1 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 задней панели устройства (Рисунок 4.5).



Рисунок 4.5 – Задняя панель

Для подключения:

1. Убедитесь, что коммутатор отключен от питания.

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

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

5 МОНТАЖ И ДЕМОНТАЖ

5.1 Меры безопасности

ВНИМАНИЕ!
Монтаж производить только при отключенном напряжении питания.

ВНИМАНИЕ!
Все виды работ с изделием во время грозы запрещаются.

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

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

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

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

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

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

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

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

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

5.2 Монтаж

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

– Условия эксплуатации изделий;

– Требования к длине и конфигурации линии связи.

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

3. Запрещается устанавливать ближе 1 м от элементов отопления.

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

5. Установка изделия должна отвечать следующим требованиям:

– Индикаторы состояния на передней панели могут быть легко прочитаны;

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

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

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

– Обеспечена возможность свободной циркуляции воздуха. Следует избегать перегрева, влажных и пыльных мест;

– Для повышения отказоустойчивости СОТ, при организации сети питания коммутатора рекомендуется использовать источники бесперебойного питания.

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

5.2.1 Подготовка изделия к монтажу

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

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

Габаритные размеры коммутатора приведены на рисунке ниже (Рисунок 5.1, Рисунок 5.2).

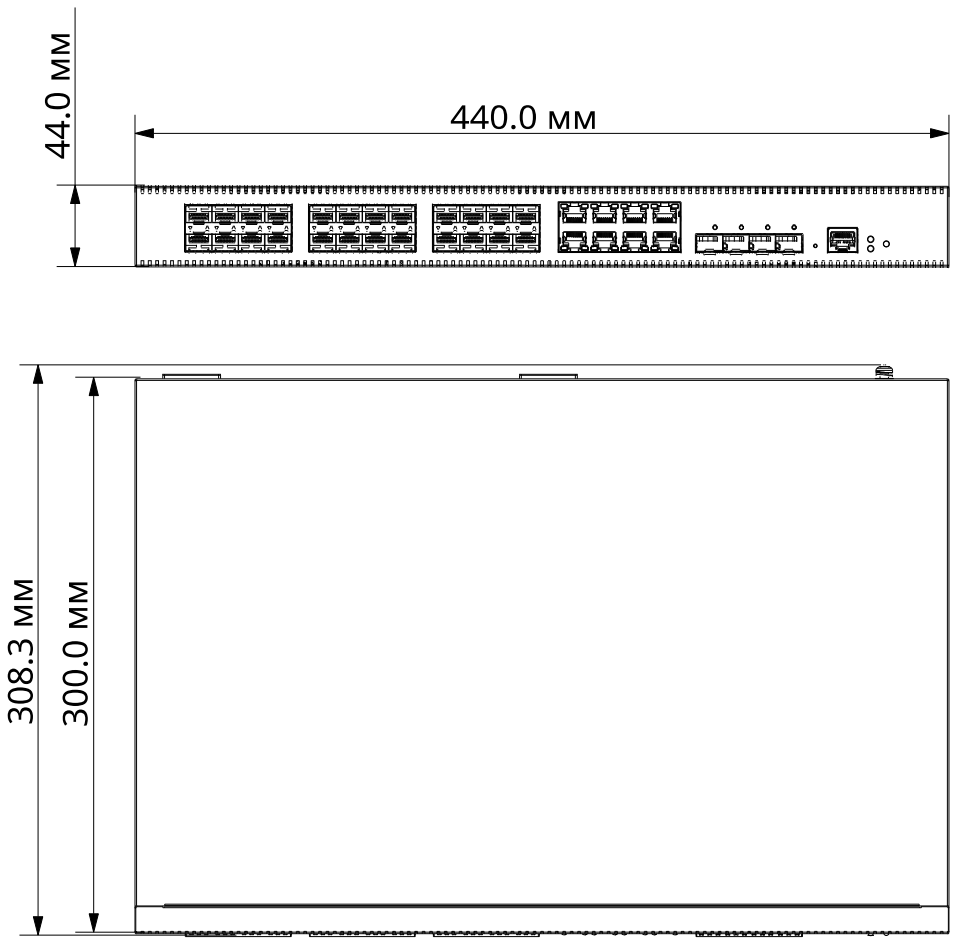


Рисунок 5.1 – Габаритные размеры

5.2.1 Монтаж коммутатора в 19”-стойку

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

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

3. Зафиксируйте винтами, поставляемыми со стойкой, коммутатор к стойке.

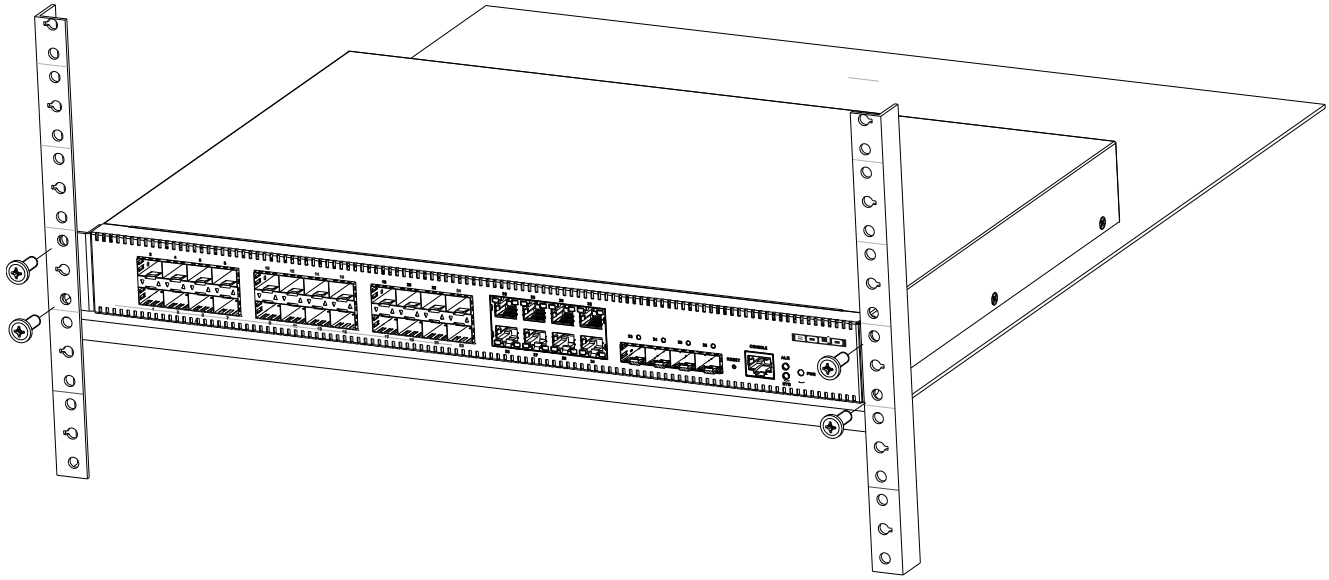


Рисунок 5.2 – Монтаж коммутатора в 19”-стойку

5.3 Демонтаж

Демонтаж изделия 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.

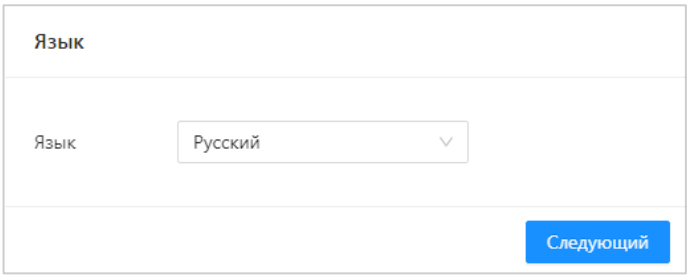


Рисунок 6.1 – Инициализация

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

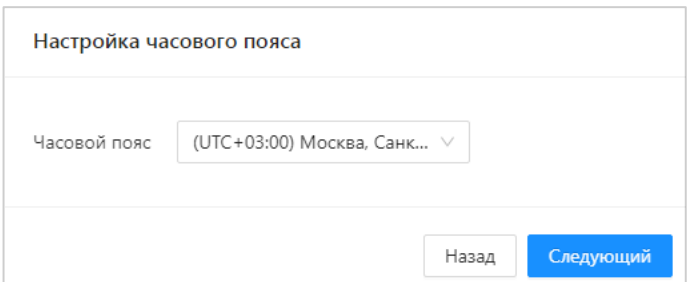


Рисунок 6.2 – Инициализация

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».

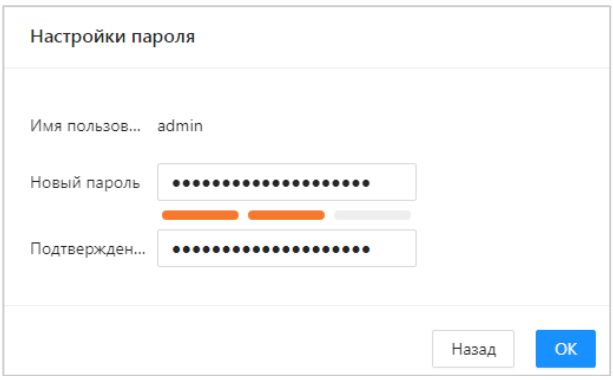


Рисунок 6.3 – Инициализация

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

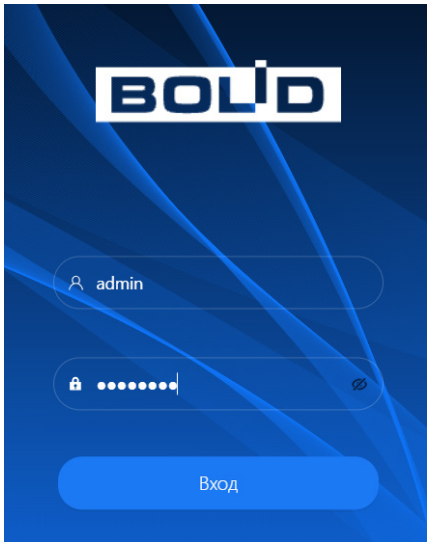


Рисунок 6.4 – Вход

6.2 Системное время

Шаг 6. Настройте время на устройстве по кнопке «Синхронизировать с ПК» или с помощью ввода параметром NTP-сервера. Неправильно выставленное время может привести к некорректному отображению журнала событий, вызвать проблемы при работе сертификата открытого ключа и т.д.

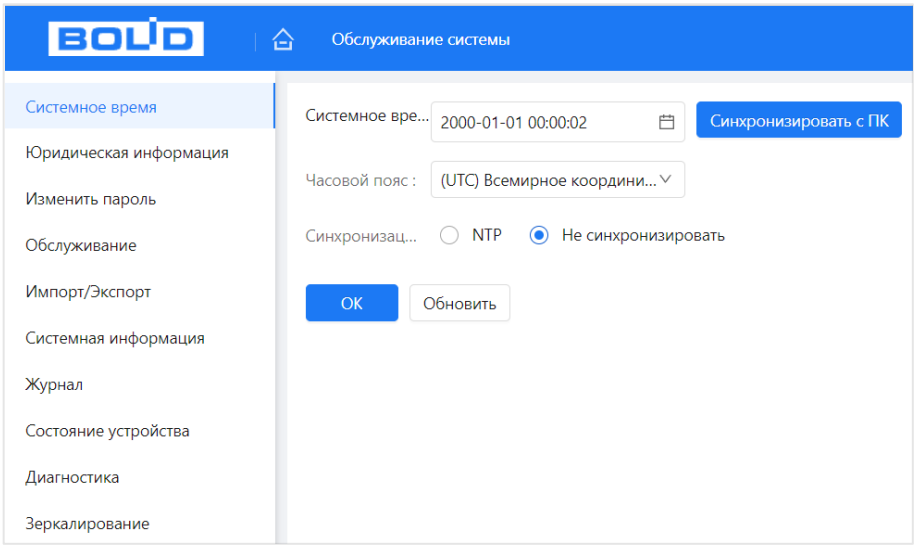


Рисунок 6.5 – Настройка/синхронизация времени

6.3 Локальный адрес

Шаг 7. Измените сетевые настройки коммутатора в соответствии с параметрами вашей сети. Для этого перейдите «Главное меню → Настройки → Быстрая настройка → Общие» (Рисунок 6.6). 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».

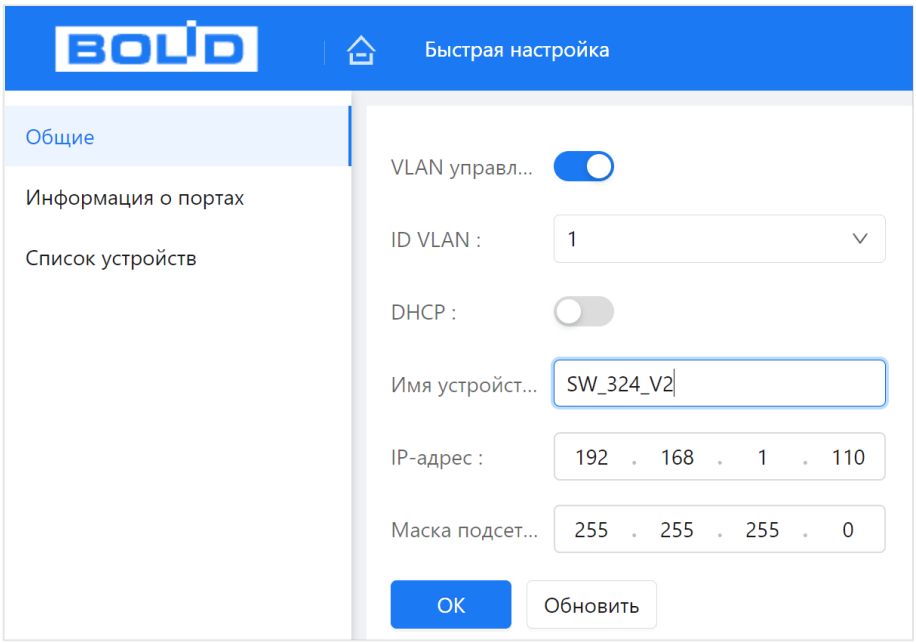


Рисунок 6.6 – Сетевые настройки

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 8. 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

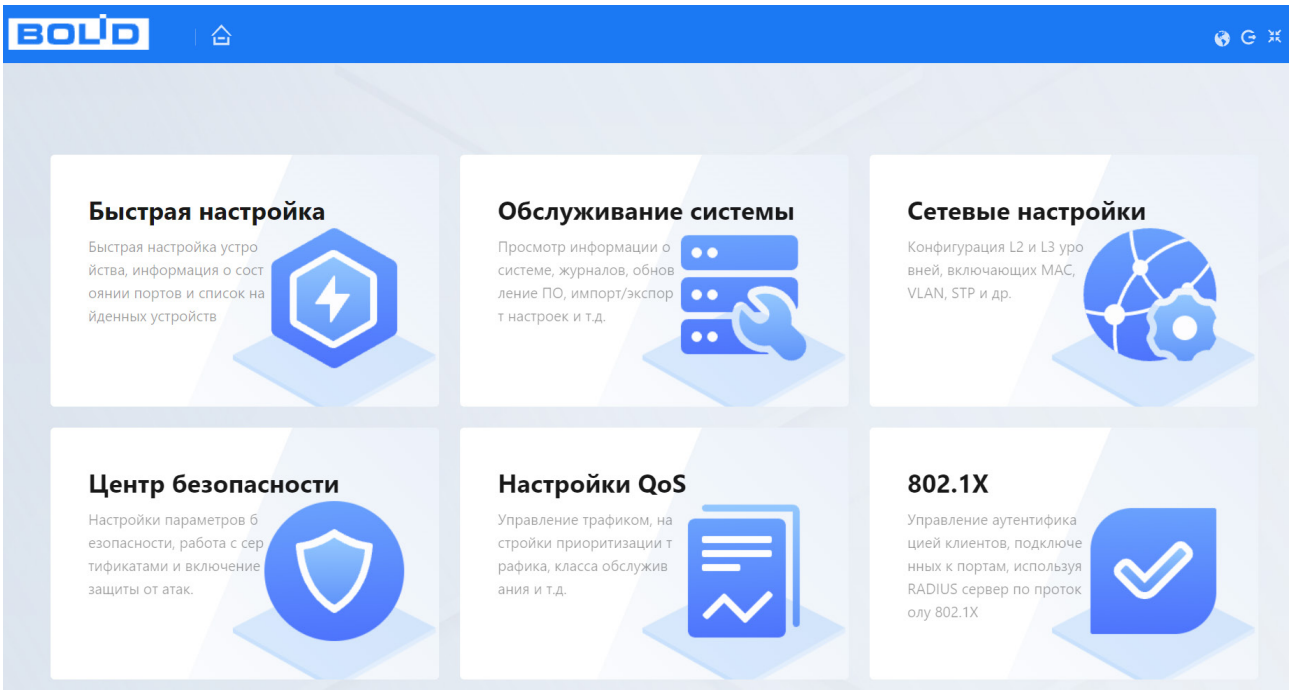


Рисунок 7.1 – Главное меню

Таблица 7.1 – Структура меню

 Быстрая настройка Раздел главного меню «Быстрая настройка»	Подраздел «Общие»
	Подраздел «Информация о портах»
	Подраздел «Список устройств»
 Обслуживание системы Раздел главного меню «Обслуживание системы»	Подраздел «Системное время»
	Подраздел «Изменить пароль»
	Подраздел «Обслуживание»
	Подраздел «Импорт/Экспорт»
	Подраздел «Системная информация»
	Подраздел «Журнал»
	Подраздел «Состояние устройства»
	Подраздел «Диагностика»
	Подраздел «Зеркалирование»

<table>
<tr><td rowspan="20">
Сетевые настройки
Раздел главного меню «Сетевые настройки»</td><td colspan="3">Подраздел «Порт»</td></tr>
<tr><td colspan="3">Подраздел «Энергоэффективный Ethernet (EEE (Energy Efficient Ethernet))»</td></tr>
<tr><td rowspan="2">Подраздел «VLAN»</td><td colspan="2">Пункт «Добавить VLAN»</td></tr>
<tr><td colspan="2">Пункт «VLAN»</td></tr>
<tr><td colspan="3">Подраздел «Интерфейс VLAN (VLANIF)»</td></tr>
<tr><td colspan="3">Подраздел «Настройки маршрутизации»</td></tr>
<tr><td colspan="3">Подраздел «Таблица маршрутизации»</td></tr>
<tr><td colspan="3">Подраздел «ARP-таблица»</td></tr>
<tr><td rowspan="3">Подраздел «ERPS»</td><td colspan="2">Быстрая настройка ERPS</td></tr>
<tr><td rowspan="2">Расширенные настройки</td><td>Пункт «ERPS»</td></tr>
<tr><td>Пункт «MEP»</td></tr>
<tr><td colspan="3">Подраздел «IGMP Snooping»</td></tr>
<tr><td rowspan="2">Подраздел «STP»</td><td colspan="2">Пункт «STP»</td></tr>
<tr><td colspan="2">Пункт «Экземпляр порта»</td></tr>
<tr><td colspan="3">Подраздел «Агрегация каналов»</td></tr>
<tr><td colspan="3">Подраздел «SNMP»</td></tr>
<tr><td rowspan="2">Подраздел «MAC-адрес»</td><td colspan="2">Пункт «Таблица MAC-адресов»</td></tr>
<tr><td colspan="2">Пункт «Фильтрация MAC-адресов»</td></tr>
<tr><td colspan="3">Подраздел «LLDP»</td></tr>
<tr><td colspan="3">Подраздел «Обнаружение петель»</td></tr>
<tr><td rowspan="3">Подраздел «DHCP-сервер»</td><td colspan="2">Пункт «DHCP-сервер»</td></tr>
<tr><td colspan="2">Пункт «Статическая привязка»</td></tr>
<tr><td colspan="2">Пункт «Список адресов»</td></tr>
<tr><td rowspan="3">Подраздел «DHCP Snooping»</td><td colspan="2">Пункт «Глобальные настройки»</td></tr>
<tr><td colspan="2">Пункт «Конфиг-я порта»</td></tr>
<tr><td colspan="2">Пункт «Конфигурация опции 82»</td></tr>
<tr><td colspan="3">Подраздел «Тестирование виртуального кабеля»</td></tr>
</table>

<table>
<tr><td rowspan="9">
Центр безопасности
Раздел главного меню «Центр безопасности»</td><td rowspan="2">Подраздел «Доп. сервисы»</td><td colspan="3">Пункт «Доп. сервисы»</td></tr>
<tr><td colspan="3">Пункт «HTTPS»</td></tr>
<tr><td colspan="4">Подраздел «Telnet»</td></tr>
<tr><td rowspan="2">Подраздел «Сертификат CA»</td><td colspan="3">Пункт «Сертификат устройства»</td></tr>
<tr><td colspan="3">Пункт «Доверенные сертификаты CA»</td></tr>
<tr><td rowspan="2">Подраздел «Сетевой экран»</td><td colspan="3">Пункт «IP фильтр»</td></tr>
<tr><td colspan="3">Пункт «Защита от атак DoS»</td></tr>
<tr><td colspan="4">Подраздел «Изолирование портов»</td></tr>
<tr><td>Подраздел «Безопасная аутентификация»</td><td colspan="3">Пункт «Алгоритм проверки подлинности»</td></tr>
<tr><td rowspan="8">
Настройки QoS
Раздел главного меню «Настройки QoS»</td><td colspan="4">Подраздел «Приоритет портов»</td></tr>
<tr><td rowspan="4">Подраздел «ACL»</td><td rowspan="3">Пункт «Конфигурация ACL»</td><td>Вкладка «MAC ACL»</td></tr>
<tr><td>Вкладка «Базовый IP ACL»</td></tr>
<tr><td>Вкладка «Расширенный IP ACL»</td></tr>
<tr><td colspan="2">Пункт «Период»</td></tr>
<tr><td colspan="2">Пункт «Привязка ACL»</td></tr>
<tr><td colspan="4">Подраздел «Классификация портов»</td></tr>
<tr><td colspan="4">Подраздел «Планировщик очереди»</td></tr>
<tr><td colspan="4">Подраздел «Шейпер трафика»</td></tr>
<tr><td colspan="4">Подраздел «Контроль шторма»</td></tr>
<tr><td rowspan="2">
802.1X
Раздел главного меню «802.1X»</td><td colspan="4">Подраздел «Настройка 802.1X (NSA)»</td></tr>
<tr><td colspan="4">Подраздел «RADIUS-сервер»</td></tr>
</table>

Таблица 7.2 – Функционал главного меню

	Возврат к главному меню.
	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.

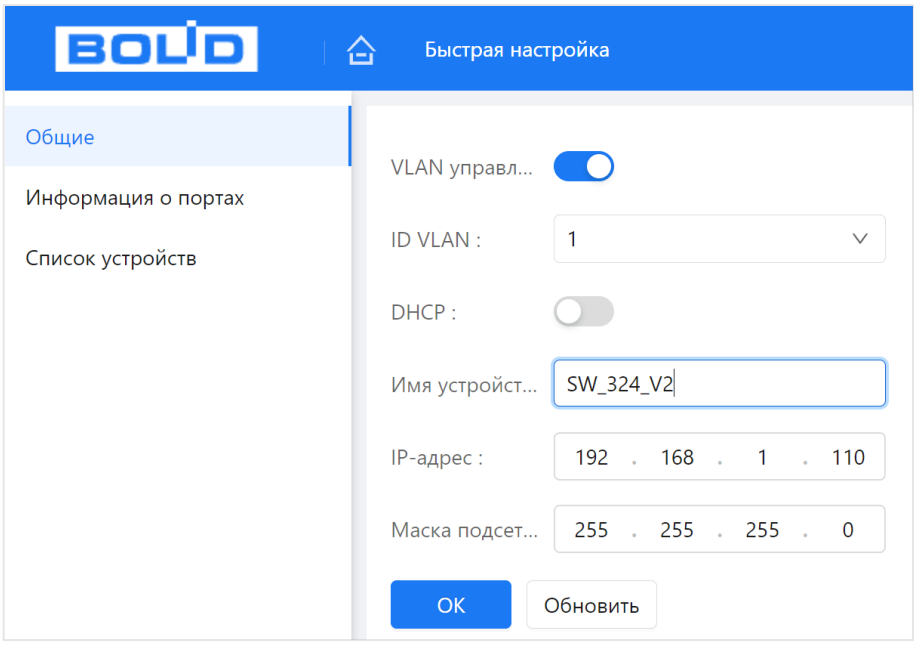


Рисунок 8.1 – Сетевые параметры устройства

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.

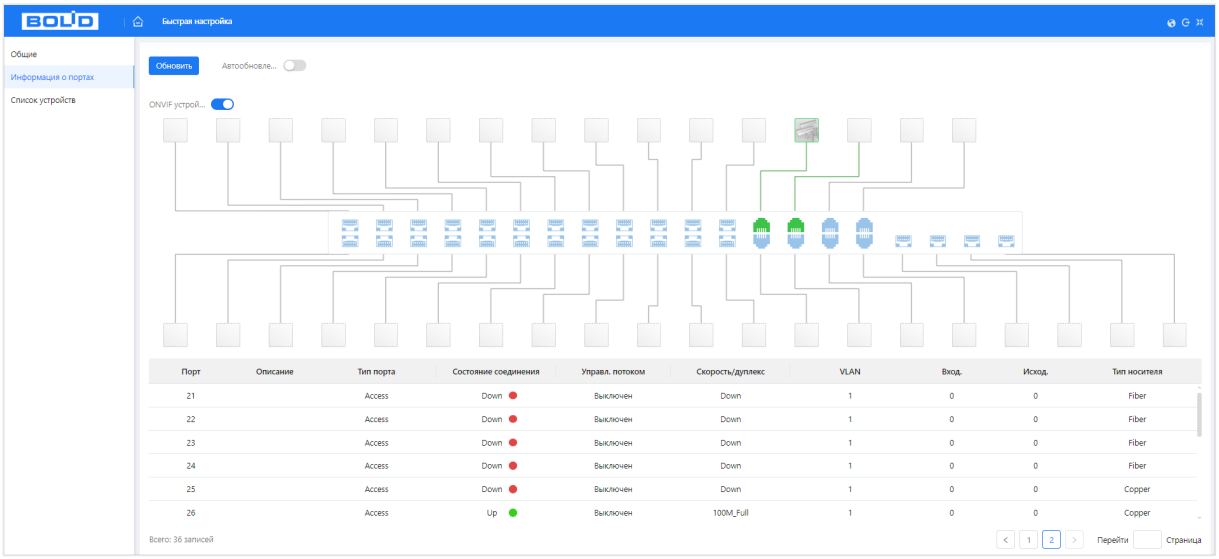


Рисунок 8.2 – Информационная панель

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 подключённом устройстве на выбранном порту. Текстовая информация включает в себя: номер порта, VLAN и информацию о PoE (Рисунок 8.4).

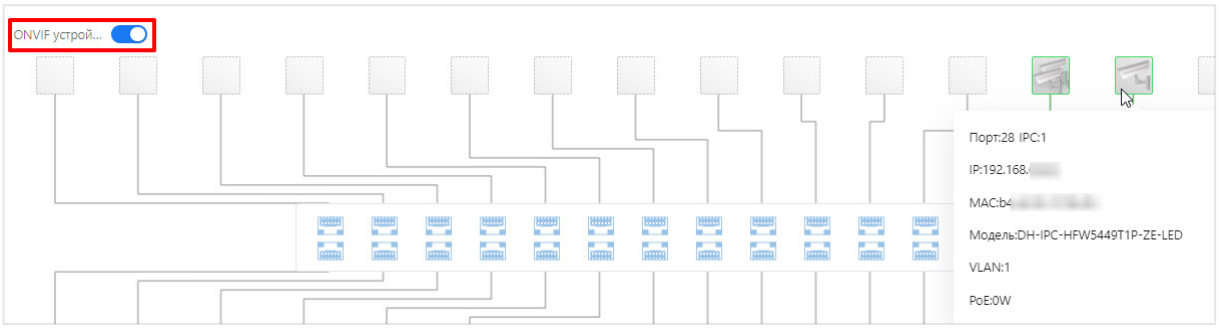


Рисунок 8.4 – Графическая панель

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

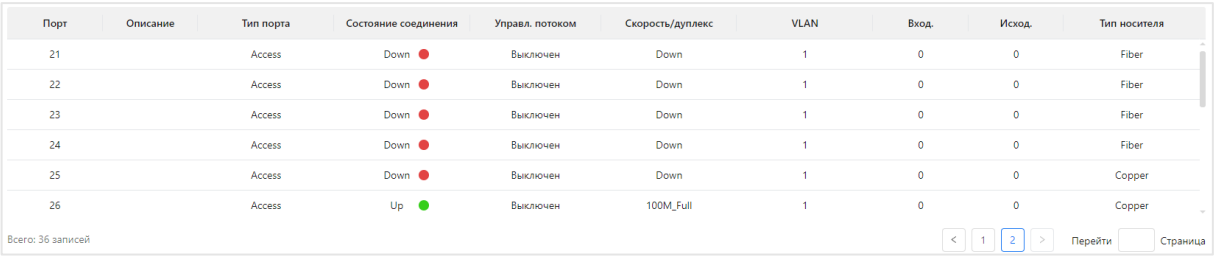


Рисунок 8.5 – Текстовая информационная панель

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».
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».

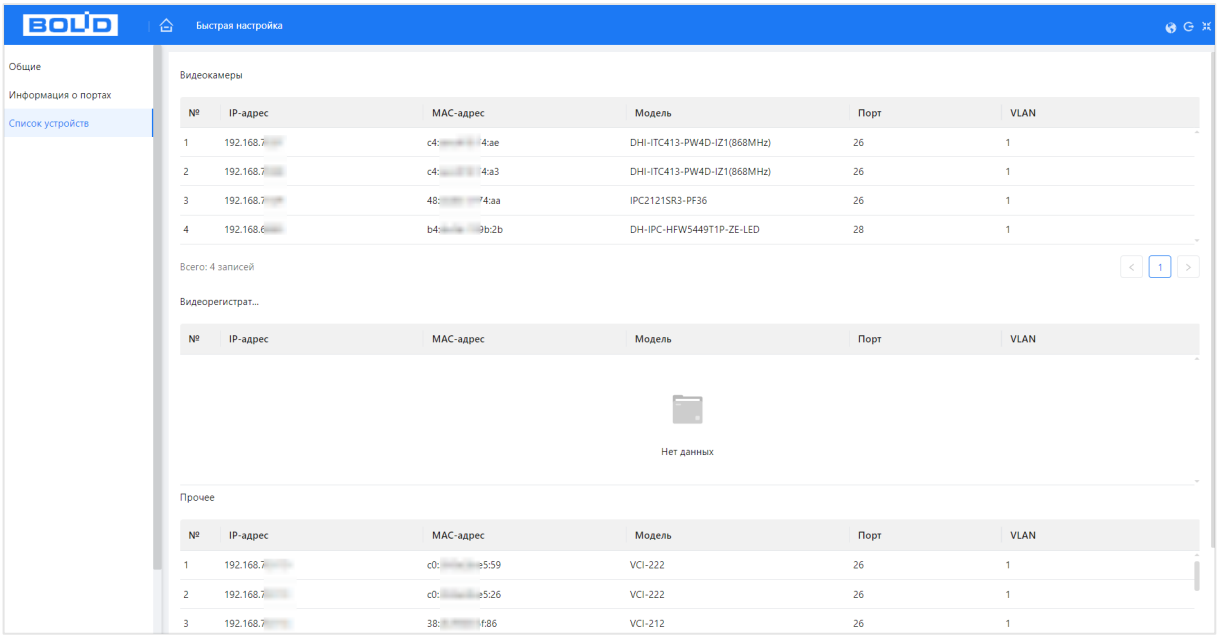


Рисунок 8.6 – Список найденных устройств

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.

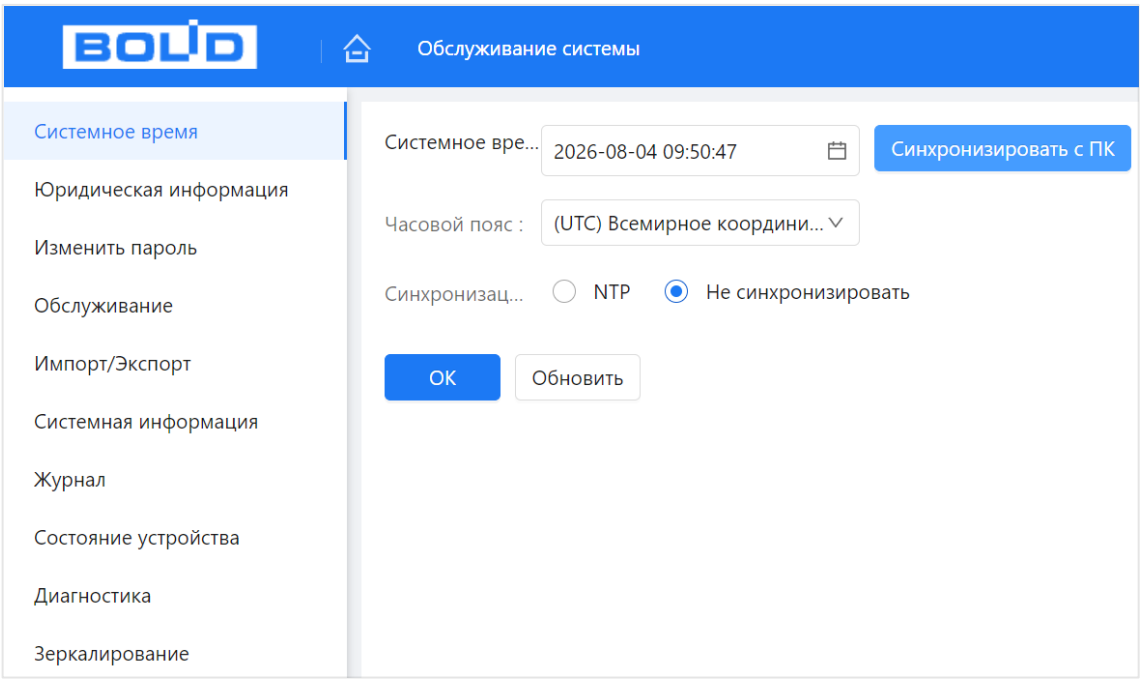


Рисунок 9.1 – Настройка/синхронизация времени

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

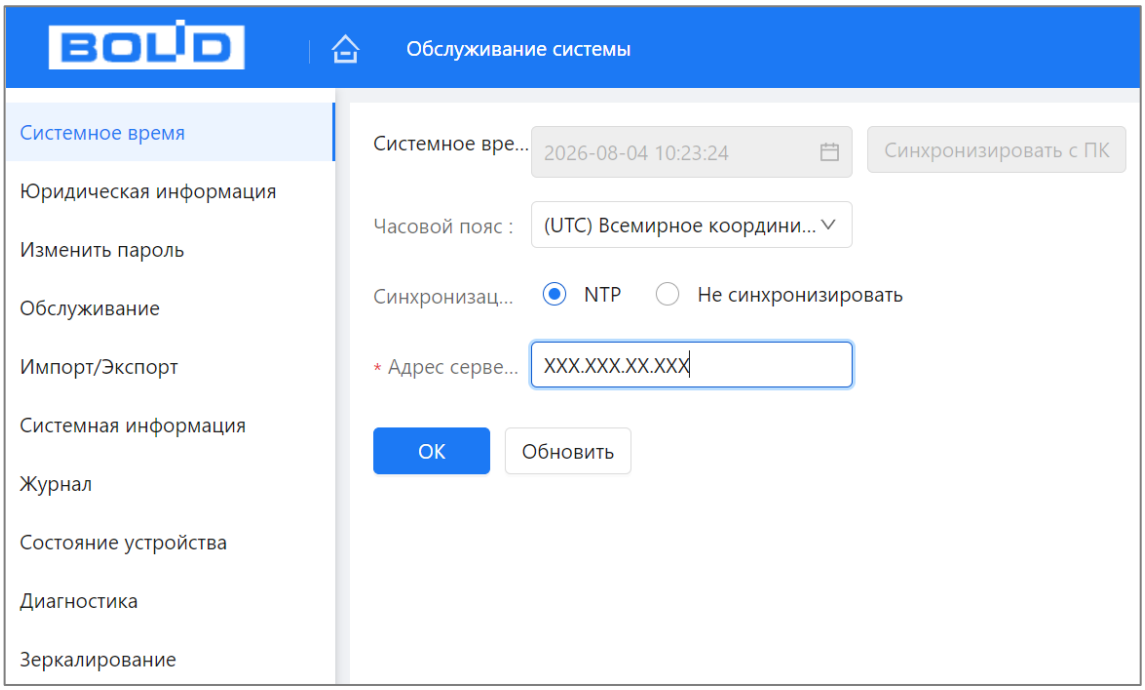


Рисунок 9.2 – Сихронизация с NTP-сервером

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.

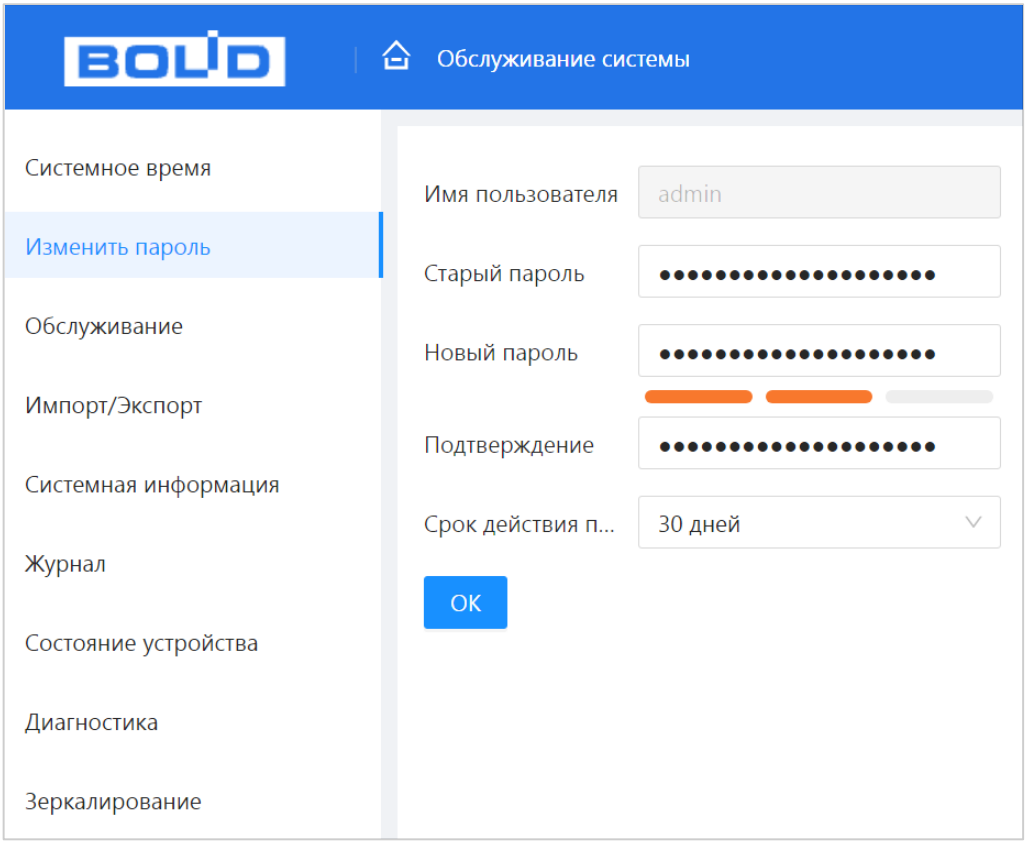


Рисунок 9.3 – Изменение пароля

9.3 Подраздел «Обслуживание»

Подраздел включает в себя несколько системных функций устройства.

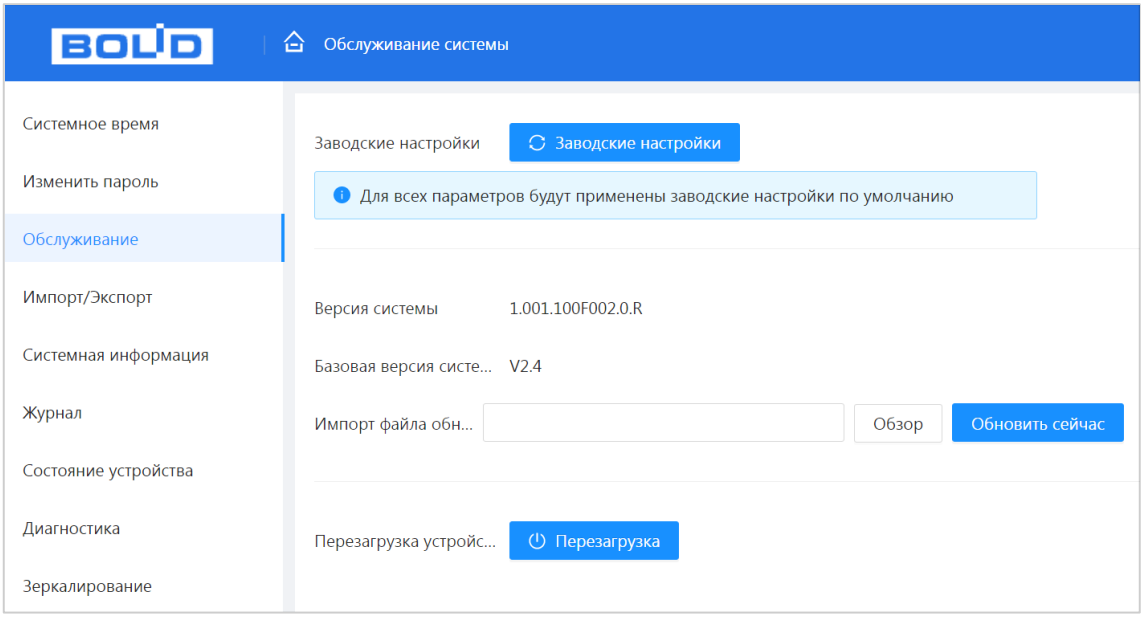


Рисунок 9.4 – Подраздел «Обслуживание»

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 – 14 Сброс на заводские настройки).

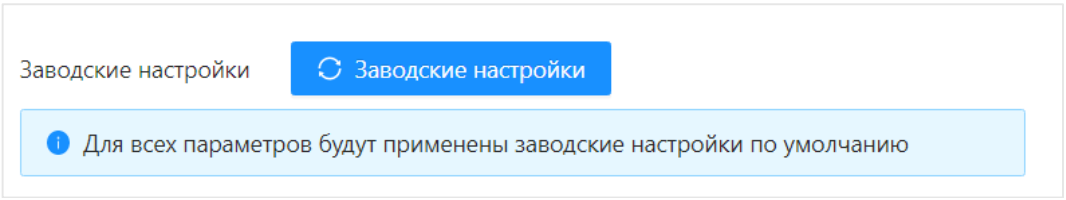


Рисунок 9.5 – Сброс

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.

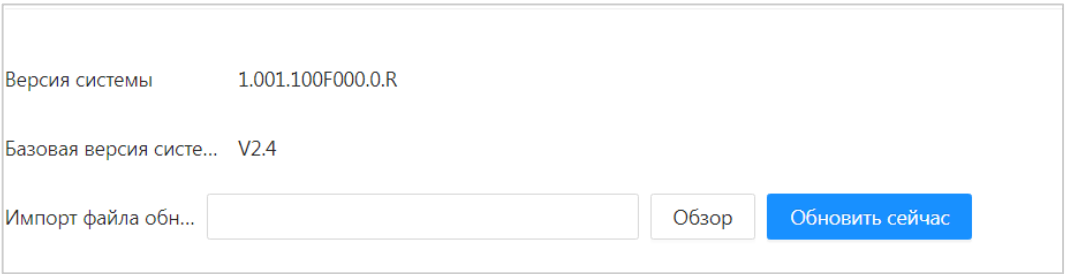


Рисунок 9.6 – Обновление

3. Перезагрузка устройства:

Нажмите кнопку «Перезагрузка» для выполнения программной перезагрузки устройства.

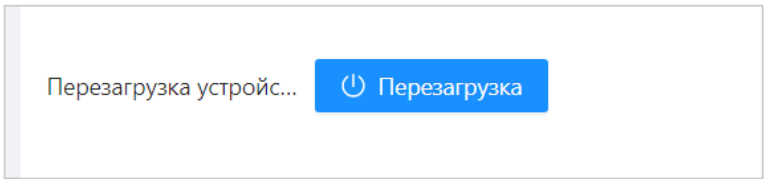


Рисунок 9.7 – Перезагрузка устройства

9.4 Подраздел «Импорт/Экспорт»

Данный подраздел используется для импорта или экспорта файла конфигурации.

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

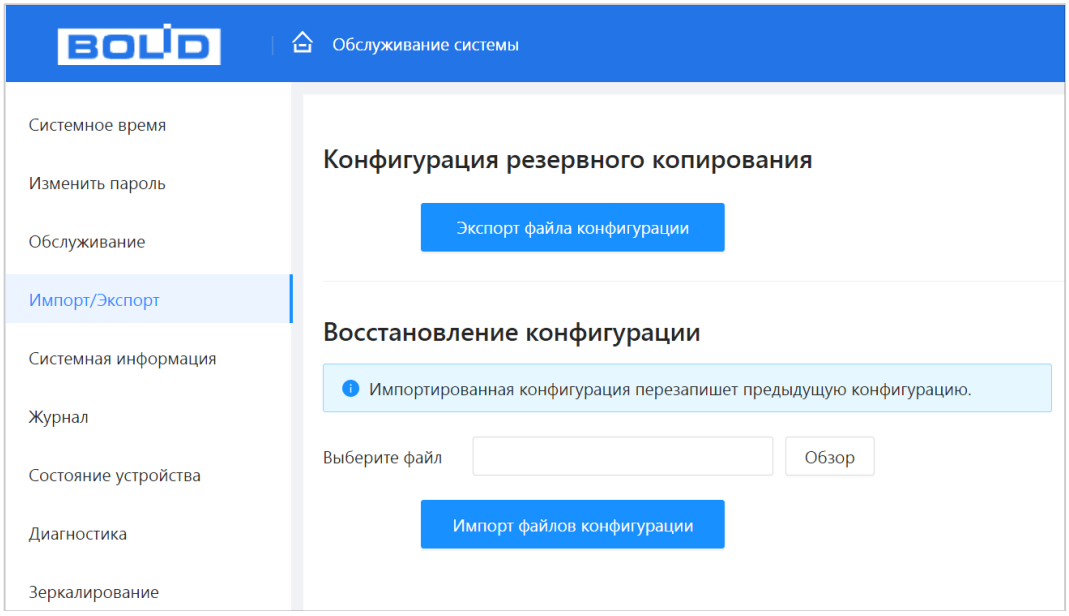


Рисунок 9.8 – Экспорт

9.4.1 Экспорт (Конфигурация резервного копирования)

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

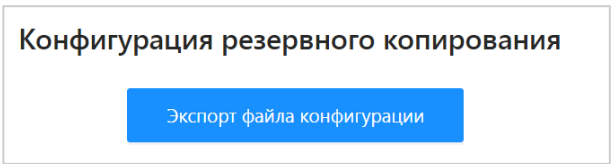


Рисунок 9.9 – Экспорт настроек с устройства

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.

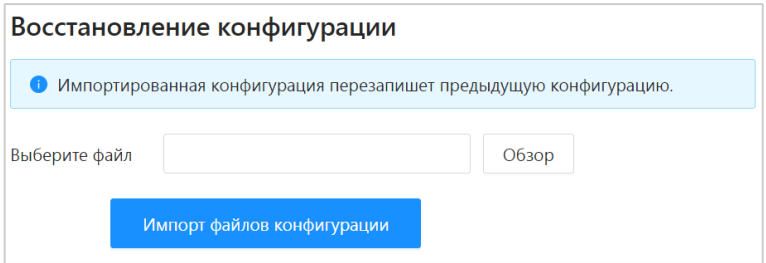


Рисунок 9.10 – Экспорт

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.

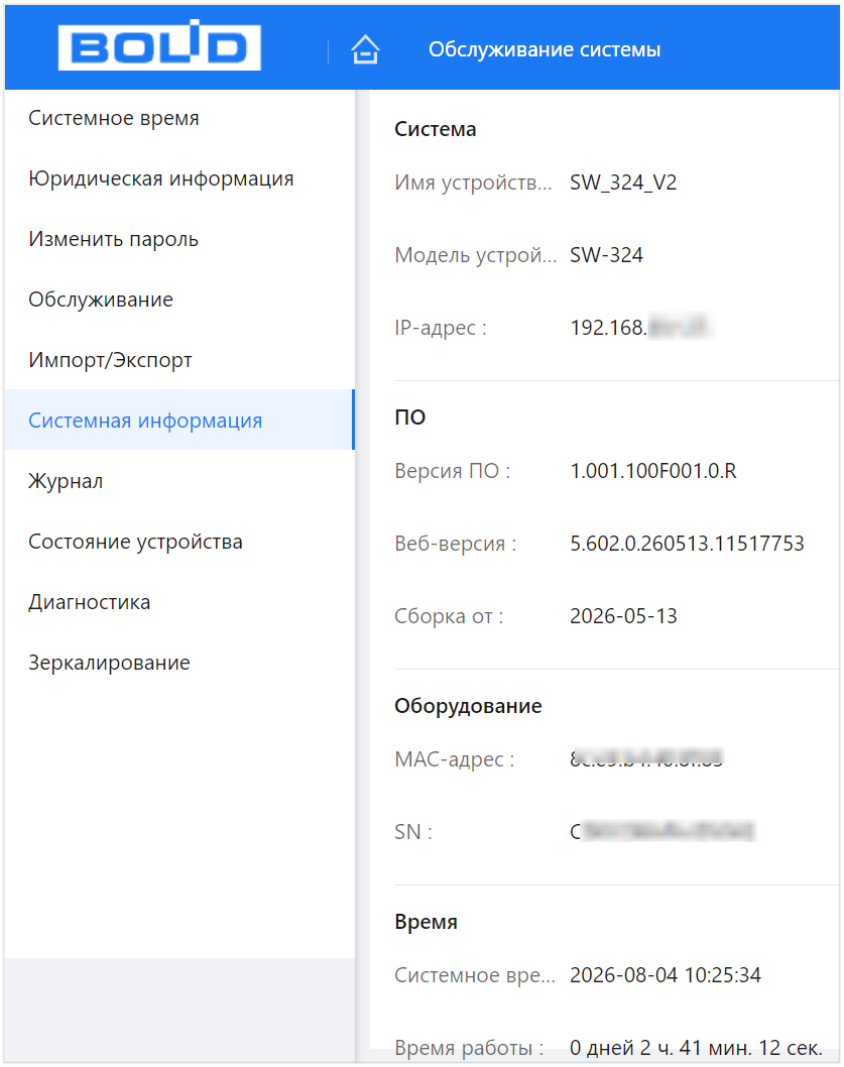


Рисунок 9.11 – Системная информация

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).

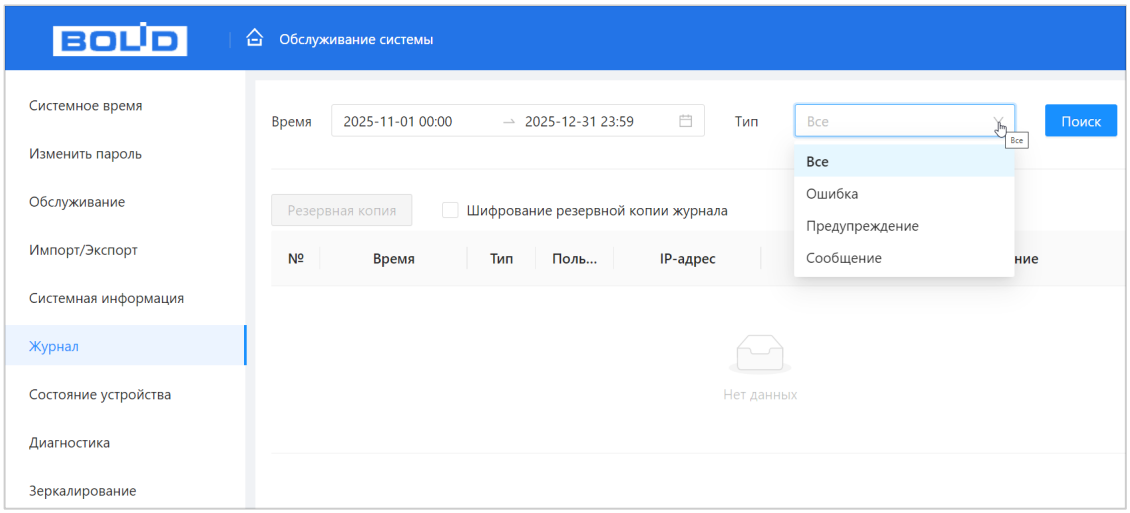


Рисунок 9.12 – Интерфейс просмотра журнала

9.7 Подраздел «Состояние устройства»

Отображение информации о состоянии CPU и памяти.

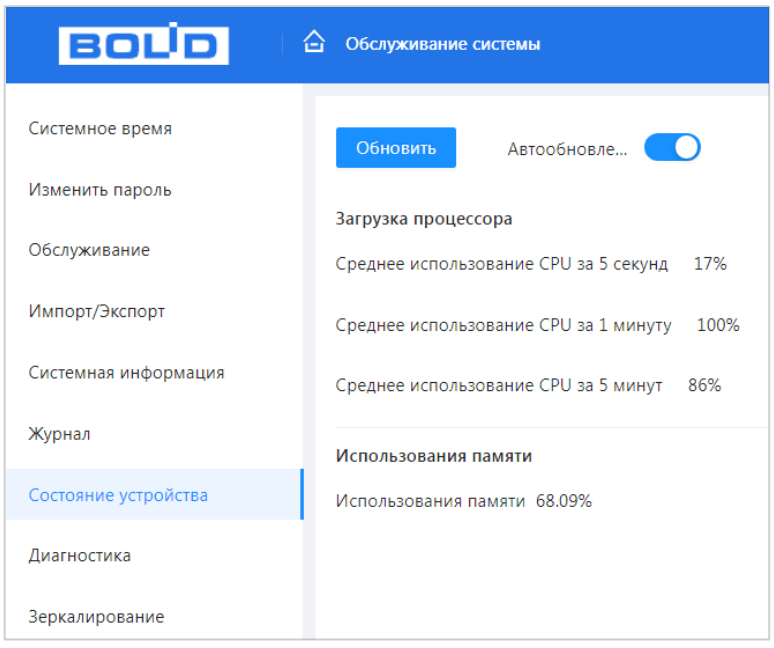


Рисунок 9.13 – Состояние устройства

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».

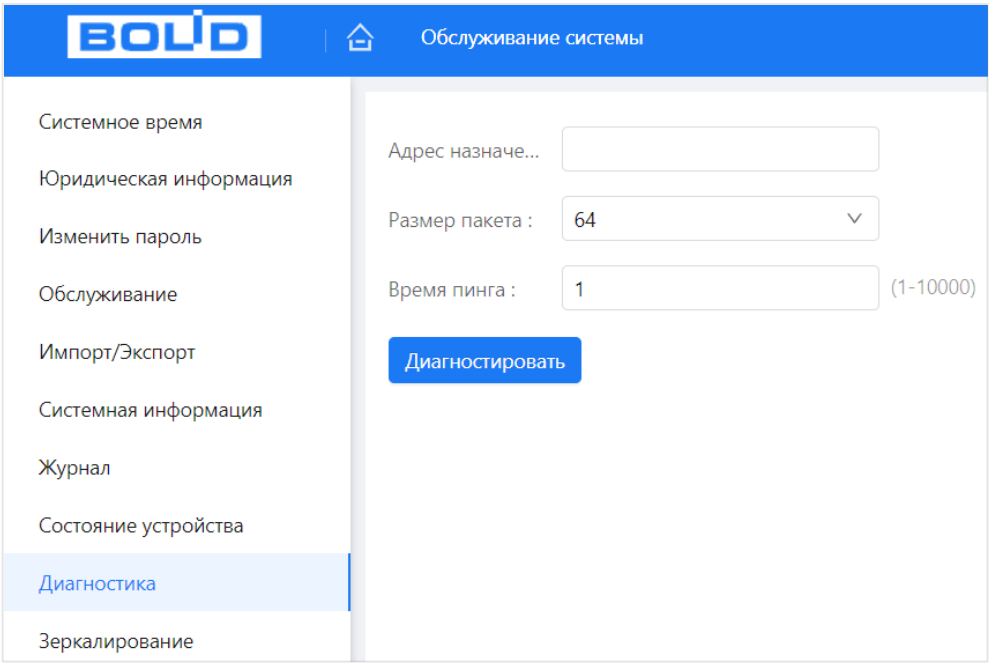


Рисунок 9.14 – Диагностика

Результат диагностики будет отображён в новом окне.

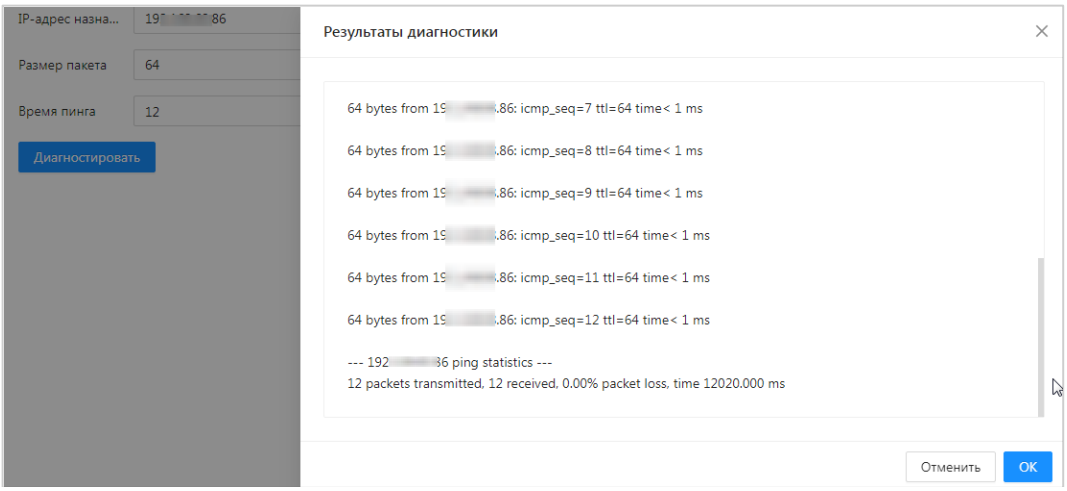


Рисунок 9.15 – Результат

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.

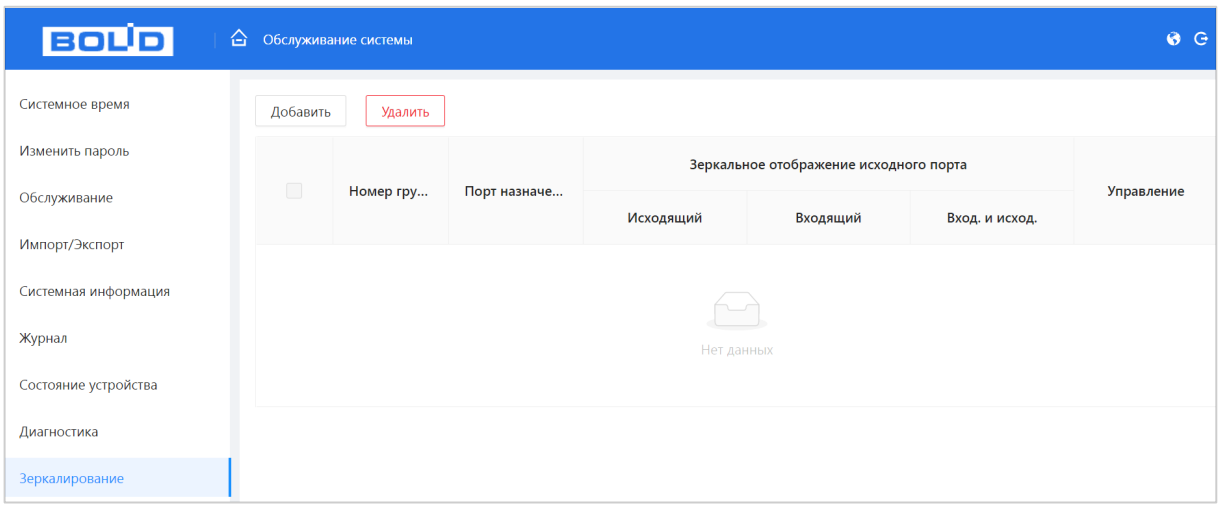


Рисунок 9.16 – Зеркалирование

Для включения данной функции необходимо:

1. Нажать кнопку «Добавить».

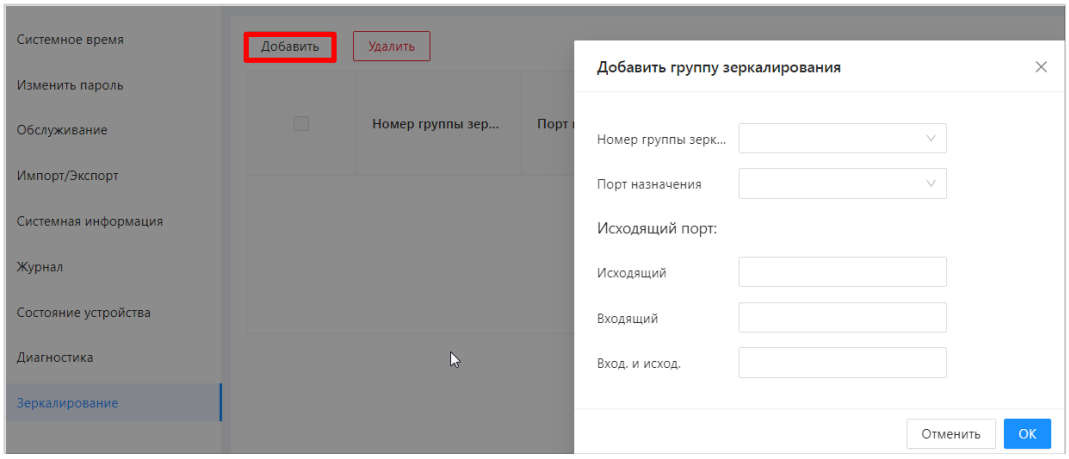


Рисунок 9.17 – Добавление

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.

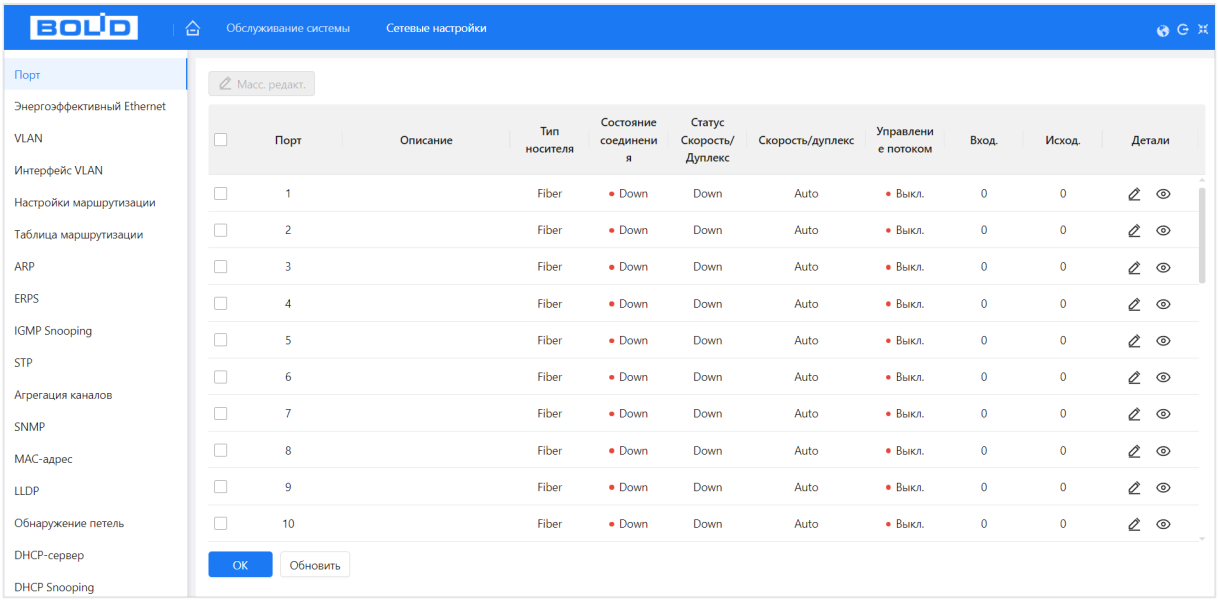


Рисунок 10.1 – Настройка портов

Для внесения изменений в определённый порт нажмите кнопку в столбце «Детали». Если нужно применить одинаковые настройки для нескольких портов, то выделите их с помощью флажков и нажмите кнопку «Масс. редакт.». Откроется окно с параметрами настройки. Подробное описание всех параметров редактирования и отображаемой информации о портах приведено в таблице ниже (Таблица 10.1).

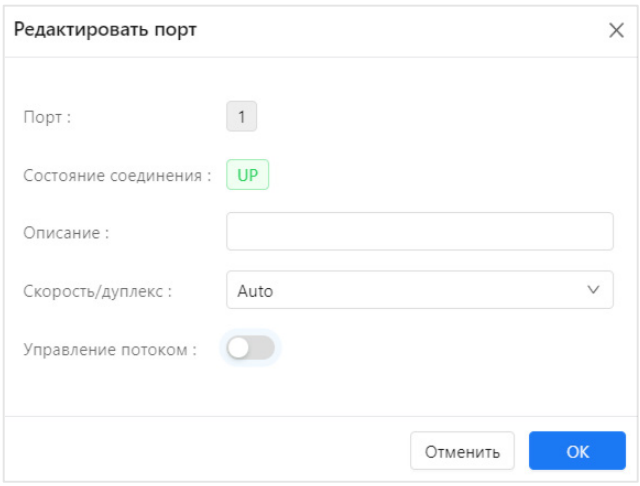


Рисунок 10.2 – Редактирование портов

Таблица 10.1 – Настройка конфигурации портов

<table>
<tr><th colspan="2">Столбец</th><th colspan="2">Описание</th></tr>
<tr><td colspan="2">Порт</td><td colspan="2">Номер порта соответствует числу на лицевой панели.</td></tr>
<tr><td colspan="2">Описание</td><td colspan="2">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.</td></tr>
<tr><td colspan="2">Тип носителя</td><td colspan="2">Показывается тип подключенного носителя сигнала.
– Copper – медный кабель;
– Fiber – волоконно-оптический кабель.</td></tr>
<tr><td colspan="2">Состояние соединения</td><td colspan="2">– Up – порт подключен;
– Down – порт отключен;
– Disabled – порт выключен.</td></tr>
<tr><td colspan="2">Статус скорости/дублирования</td><td colspan="2">Отображает текущее состояние скорости порта.</td></tr>
<tr><td rowspan="5">Скорость/ дуплекс</td><td colspan="3">Отображает текущее состояние скорости порта</td></tr>
<tr><td>Порт</td><td>Скорость</td><td>Описание</td></tr>
<tr><td rowspan="4">Ethernet порт</td><td>Авто.</td><td>Автоматическая настройка скорости и режима передачи.
📖 Рекомендовано для комбинированного порта.</td></tr>
<tr><td>10M FULL</td><td>Скорость 10 Мб/с. Работа в режиме полного дуплекса.</td></tr>
<tr><td>10M HALF</td><td>Скорость 10 Мб/с. Работа в режиме полудуплекса.</td></tr>
<tr><td>100M HALF</td><td>Скорость 100 Мб/с. Работа в режиме полудуплекса.</td></tr>
</table>

Столбец		Описание	
		100M FULL	Скорость 100 Мб/с. Работа в режиме полного дуплекса.
	Оптический порт	1000M FULL	Скорость 1000 Мб/с. Работа в режиме полного дуплекса.
Управление потоком		Вкл.	Включение функции управления потоком на порте.
		Выкл.	Выключение функции управления потоком на порте.
Входящий		Отображение текущего состояния приёма пакетов.	
Исходящий		Отображение текущего состояния отправки пакетов.	

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

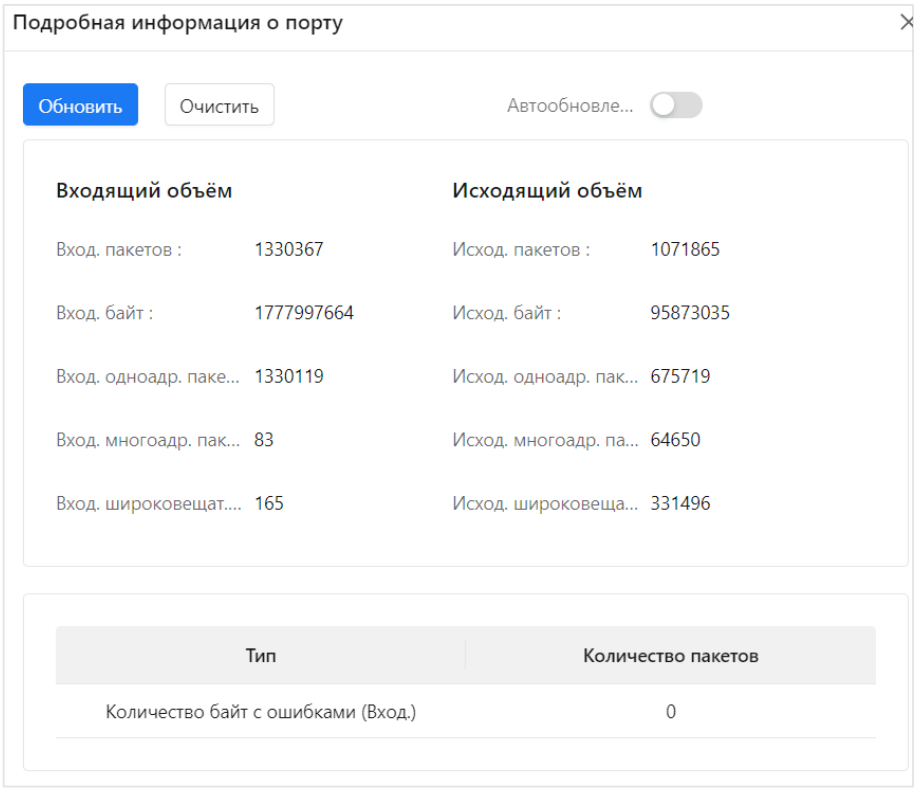


Рисунок 10.3 – Подробная информация о порту

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».

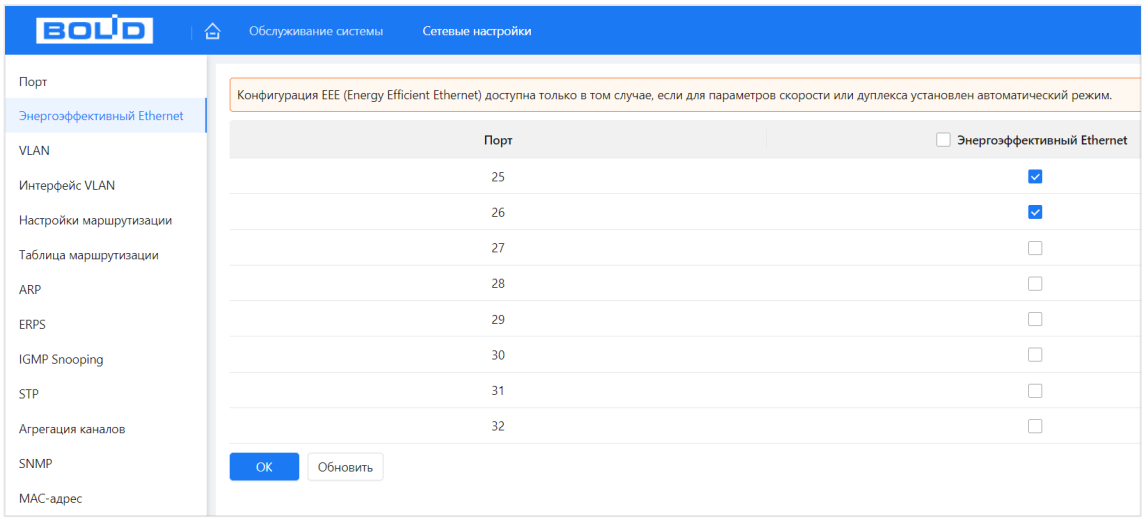


Рисунок 10.4 – Конфигурация EEE

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 10.5).

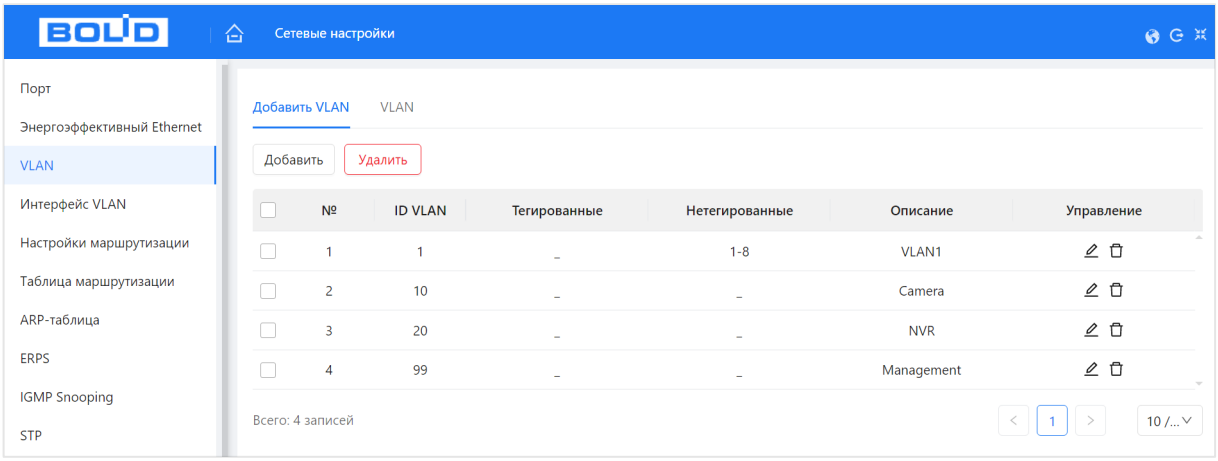


Рисунок 10.5 – Создание VLAN

Для создания VLAN на устройстве нажмите кнопку «Добавить» (Рисунок 10.6). В появившемся диалоговом окне (Рисунок 10.6) 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.

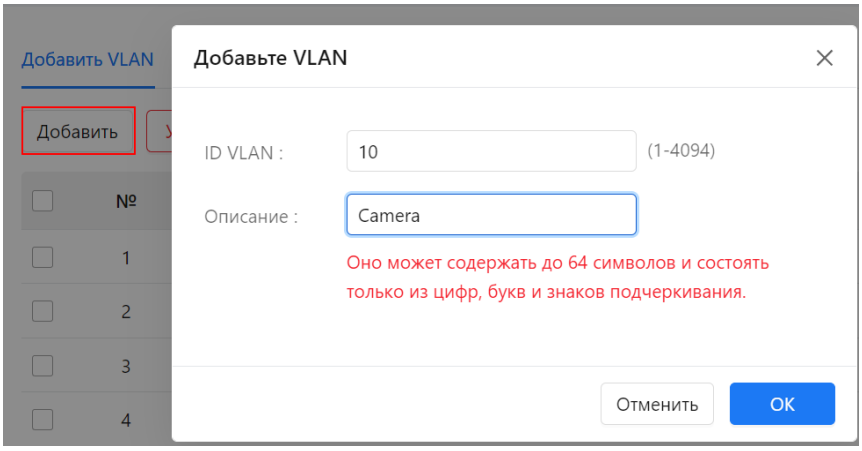


Рисунок 10.6 – Создание VLAN

Таблица 10.2 – Данные списка VLAN

Столбец	Описание
ID VLAN	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.

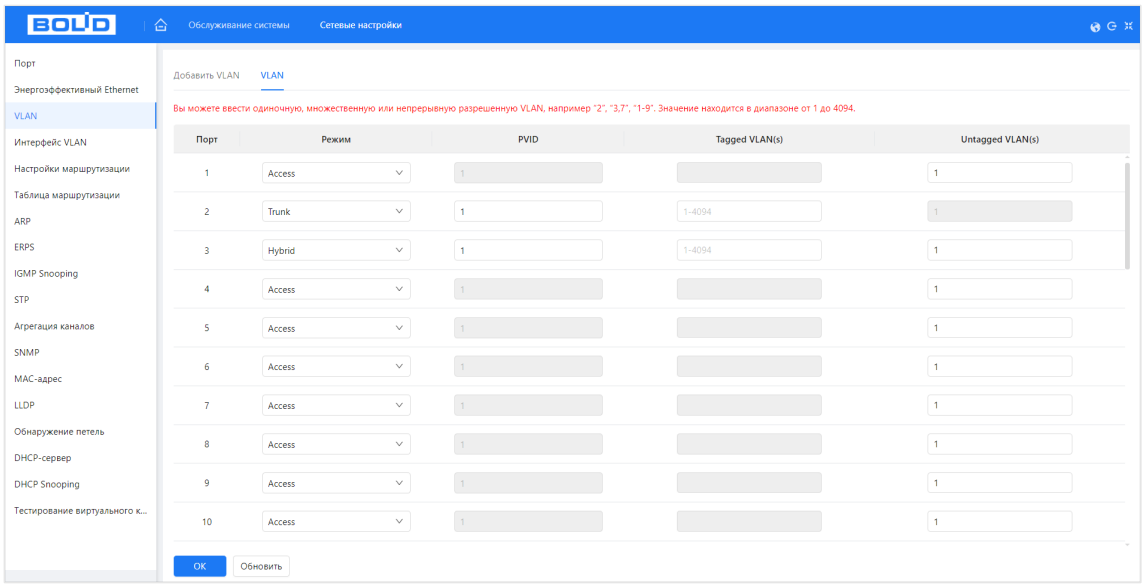


Рисунок 10.7 – Конфигурирование VLAN-порта

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.

Столбец	Описание
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.

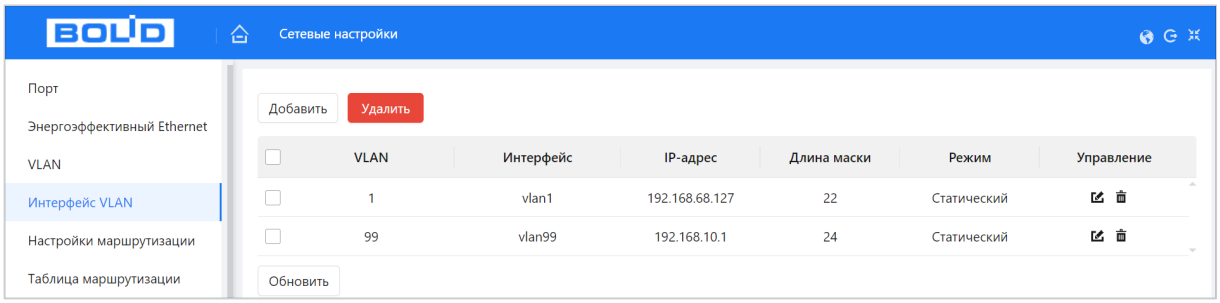


Рисунок 10.8 – VLAN интерфейс

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.

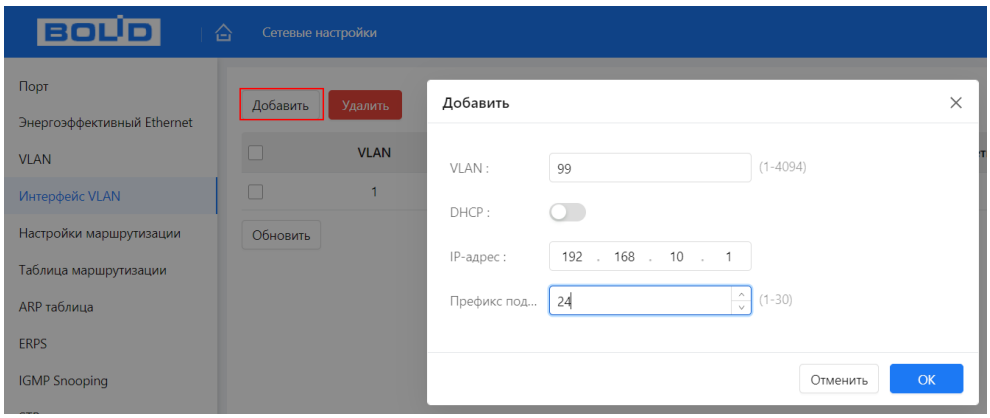


Рисунок 10.9 – Добавление

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	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.

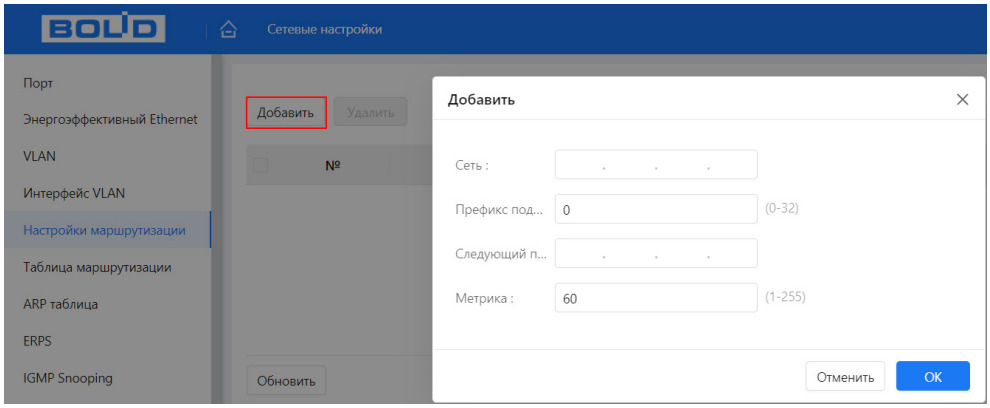


Рисунок 10.10 – Настройки маршрутизации

Таблица 10.5 – Настройка маршрутизации на устройстве. Добавление маршрута

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

10.6 Подраздел «Таблица маршрутизации»

Таблица маршрутизации – это структура данных, используемая сетевыми устройствами для хранения информации о маршрутах. Эта таблица содержит сведения об оптимальных путях к различным сетям или подсетям и служит основной основой для принятия решений о пересылке пакетов.

Перейдите «Сетевые настройки → Таблица маршрутизации», чтобы просмотреть действующую информацию о маршрутизации, включая IP-адрес назначения, длину маски, тип протокола, следующий шлюз и выходной интерфейс.

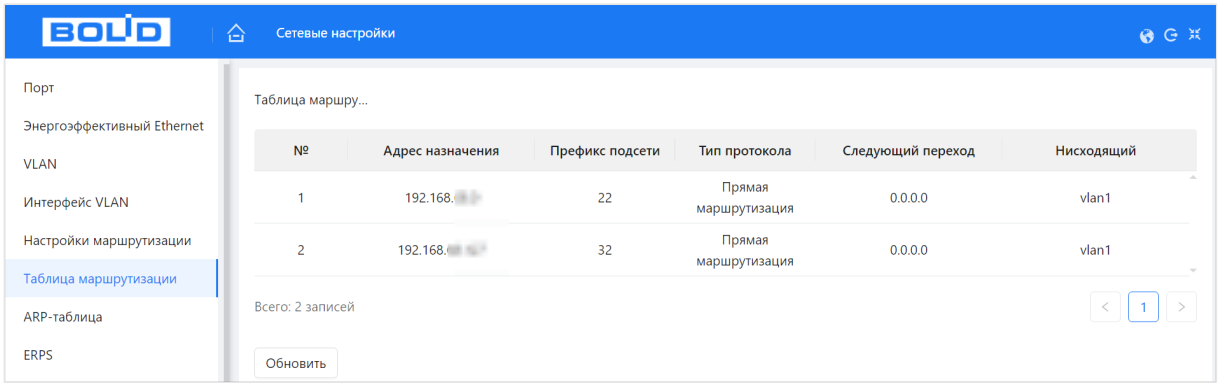


Рисунок 10.11 – Таблица маршрутизации

10.7 Подраздел «ARP-таблица»

ARP (Address Resolution Protocol) – протокол для определения соответствия между логическим адресом сетевого уровня (IP) и физическим адресом устройства (MAC). Сама связь между двумя устройствами в сети проходит на канальном уровне.

Вся информация о сопоставлении между IP-адресами и MAC-адресами заносится ARP-таблицу коммутатора.

В таблице можно просмотреть все существующие записи, удалить записи или добавить.

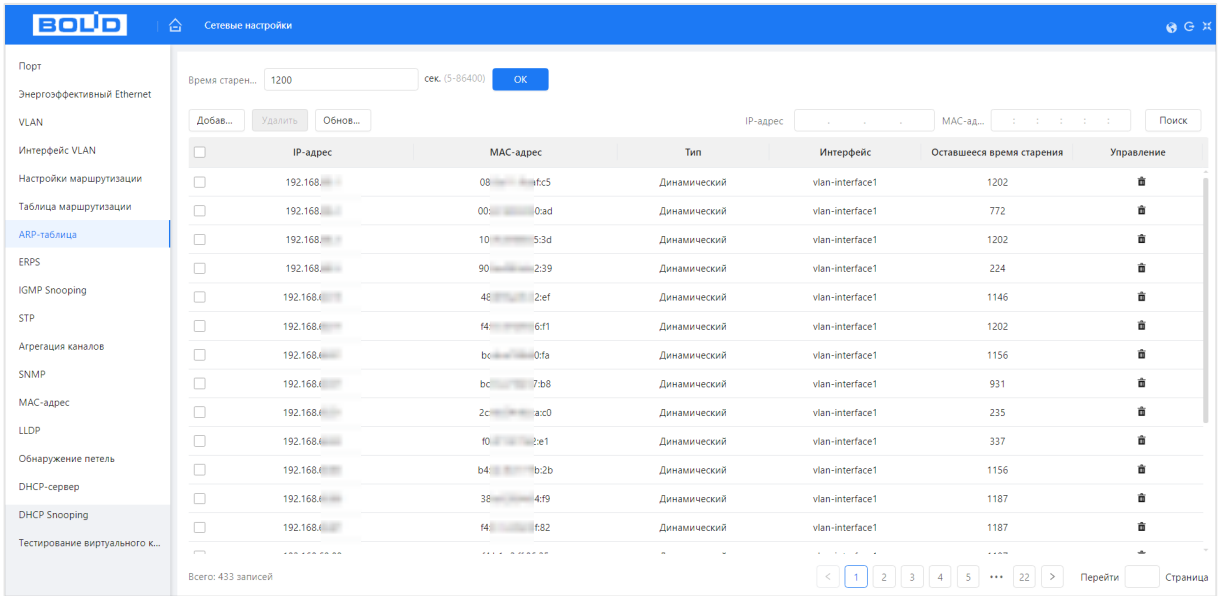


Рисунок 10.12 – ARP-таблица

10.8 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».

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

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

10.8.1 Быстрая настройка ERPS

При выборе и включении режима «Быстрая настройка ERPS» будет создан базовый экземпляр ERPS без необходимости детальной настройки каждого параметра. Для настройки:

1. Выберите режим «Быстрая настройка ERPS».

2. Далее активируйте переключатель «Кольцевая сеть» для создания экземпляра. Деактивация переключателя приведёт к удалению созданного экземпляра.

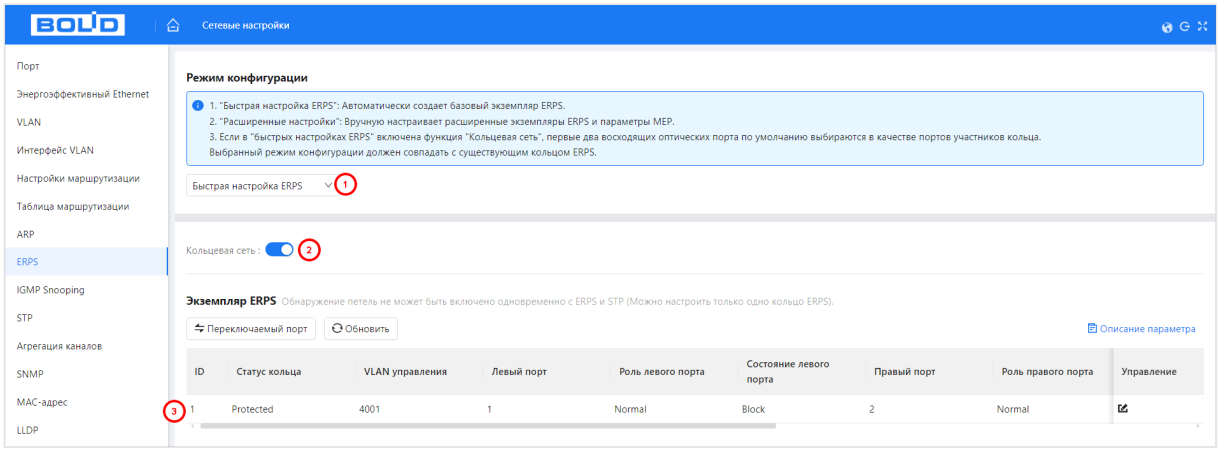


Рисунок 10.13 – Быстрая настройка ERPS

Просмотреть информацию о каждом столбце можно с помощью кнопки «Описание параметра».

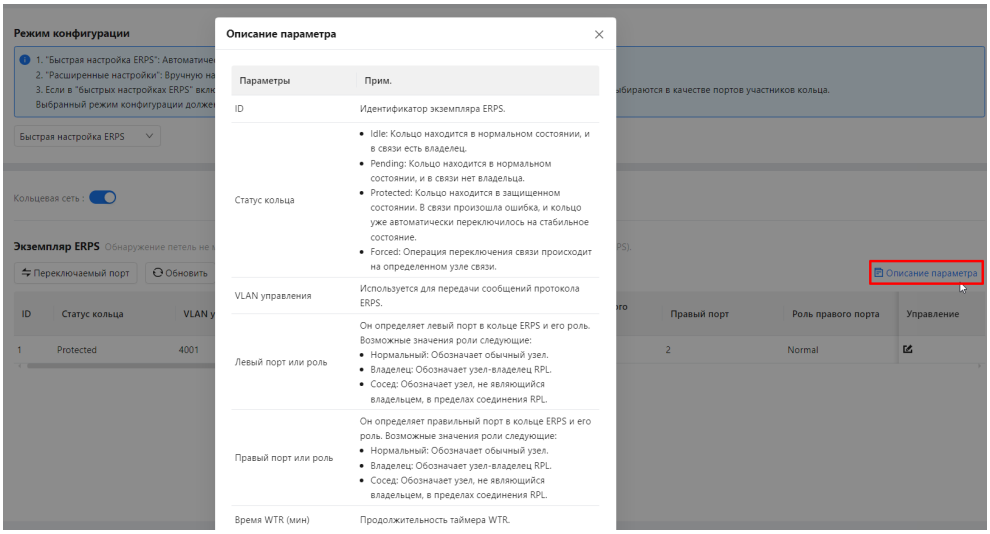


Рисунок 10.14 – Информация

Для внесения изменений в созданный экземпляр нажмите кнопку в столбце «Управление».

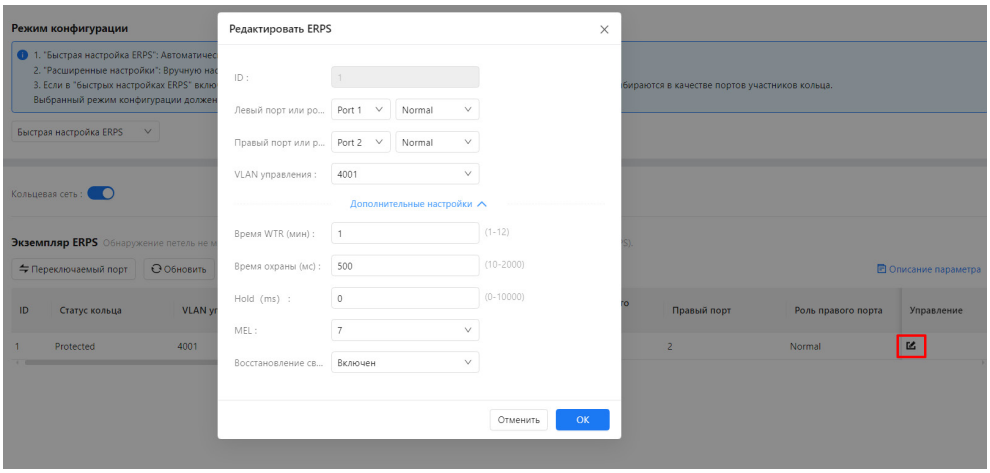


Рисунок 10.15 – Редактирование ERPS экземпляра

Таблица 10.6 – Параметры редактирования ERPS

Параметр	Функция
ERPS ID	Отображён идентификационный номер экземпляра ERPS.
Левый порт или роль	Устанавливается левый порт в кольце ERPS и его роль. Доступен выбор из трёх ролей: – Normal – обычный узел; – Owner – владелец RPL (Ring Protection Link); – Neighbour – узел, не являющийся владельцем, в составе RPL.
Правый порт или роль	Устанавливается правый порт в кольце ERPS и его роль. Доступен выбор из трёх ролей: – Normal – обычный узел; – Owner – владелец RPL; – Neighbour – узел, не являющийся владельцем, в составе RPL.
VLAN управления	Устанавливается идентификатор VLAN для протокола ERPS, чтобы избежать помех служебному трафику.
Дополнительные настройки	
Время WTR (мин)	Устанавливается длительность времени ожидания восстановления (WTR). Большее значение повышает стабильность, меньшее – ускоряет восстановление, но может вызывать колебания.
Время охраны (мс)	Устанавливает длительность защитного времени.
Hold (ms)	Устанавливает длительность времени задержки (hold off).
MEL	Устанавливает уровень обслуживания (Maintenance Entity Level) для пакетов протокола ERPS. Большее значение означает более низкий приоритет.
Восстановление связи	– «On» – автоматическое восстановление заблокированного RPL после сбоя; – «Off» – ручное восстановления.

Кнопка «Переключаемый порт» используется для включения имитации переключения при сбое для ручного тестирования функции ERPS и проверки восстановления сети.

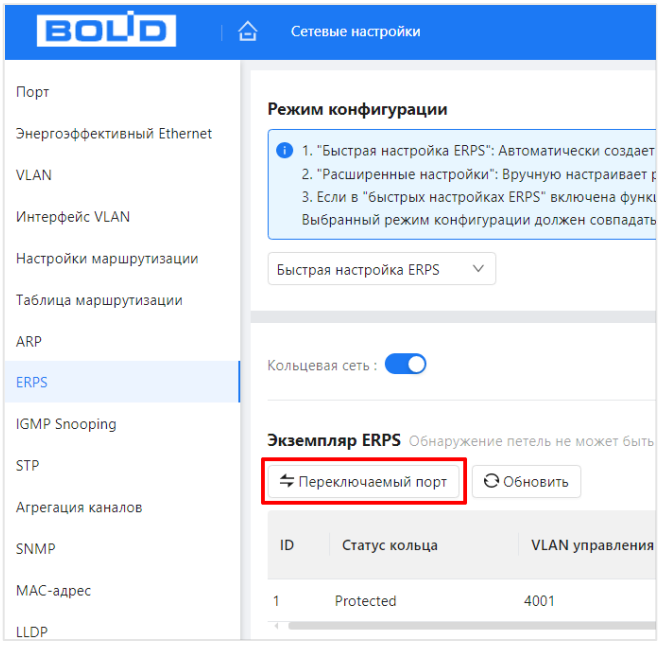


Рисунок 10.16 – Тест

10.8.2 Расширенные настройки

10.8.2.1 **Пункт «ERPS»**

Для пользовательского добавления экземпляра ERPS нажмите кнопку «Добавить». В появившемся окне введите параметры для создаваемого ERPS (Таблица 10.7).

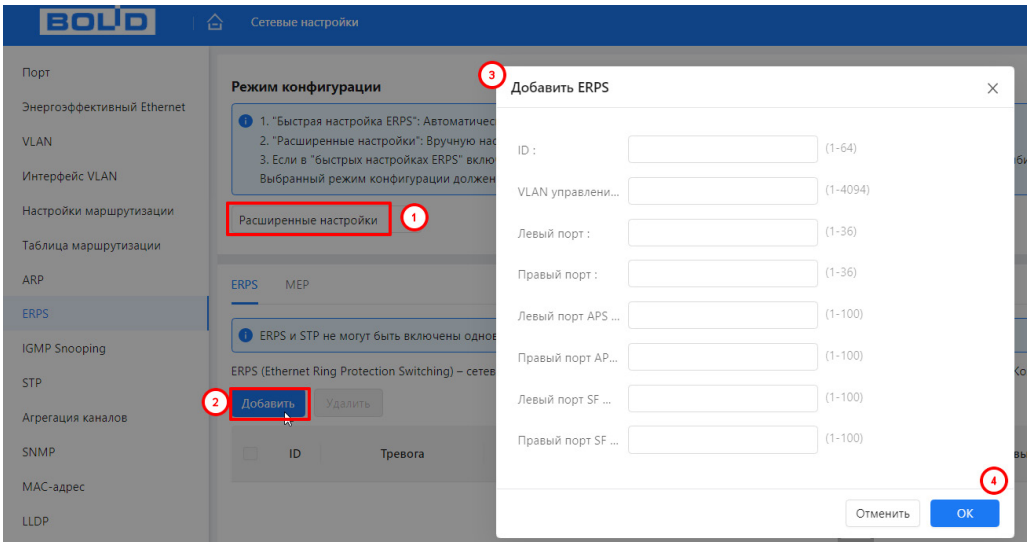


Рисунок 10.17 – Добавление ERPS

Таблица 10.7 – 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 10.18).

Параметр	Функция
VLAN управления	Поле для ввода VLAN ID для протокола ERPS, чтобы избежать помех с рабочим трафиком.
Левый порт	В поля устанавливаются два подключённых порта для кольца ERPS.
Правый порт	
Левый порт APS MEP	Порт APS MEP (точка окончания обслуживания автоматического переключения защиты) – задаёт APS MEP для порта ERPS для обнаружения прерываний пакетов протокола ERPS.
Правый порт APS MEP	Порт SF MEP (точка окончания обслуживания сигнального отказа): задаёт SF MEP для порта ERPS для обнаружения сигнального отказа.
Левый порт SF MEP	Значение «Левый порт APS MEP» должно совпадать со значением «Левый порт SF MEP». Значение «Правый порт APS MEP» должно совпадать со значением «Правый порт SF MEP». Например, установите «Левый порт SF MEP» равно 1, а «Правый порт SF MEP» равен 2.
Правый порт SF MEP	

Нажмите на цифру в столбце «ERPS ID» для перехода к окну настройки экземпляра ERPS (Рисунок 10.18, Таблица 10.8).

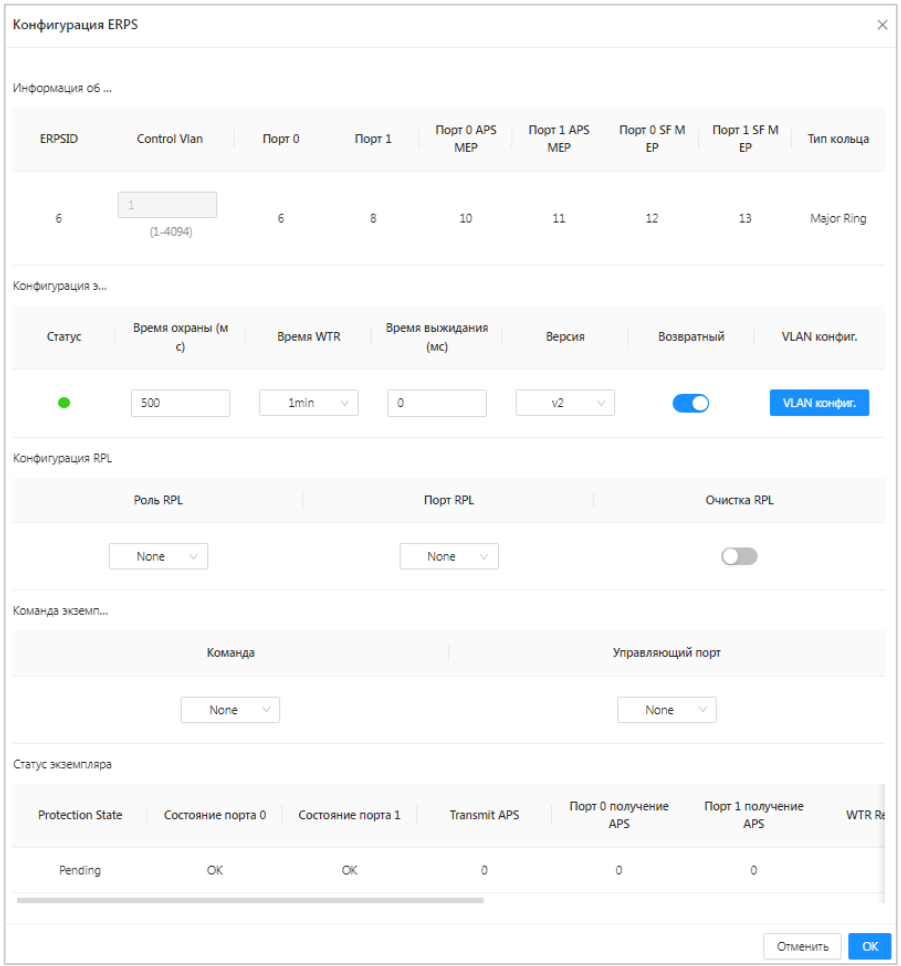
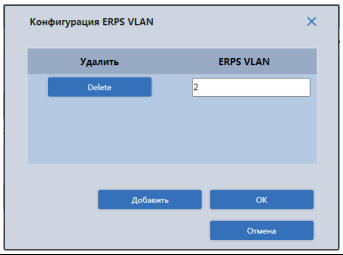


Рисунок 10.18 – Настройка экземпляра ERPS

Таблица 10.8 – Параметры конфигурации ERPS

Параметр	Функция	
Информация об экземпляре	ERPS ID	Панель отображает ранее заданные параметры, более подробно каждый параметр описан в таблице выше (Таблица 10.7).
	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.
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.

Параметр	Функция	
	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.
	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.

<table>
<tr><th>Параметр</th><th colspan="3">Функция</th></tr>
<tr><td rowspan="5"></td><td rowspan="2"></td><td colspan="2">RPL_Owner – коммутатор назначается владельцем RPL. Отвечает за блокировку трафика по RPL в нормальном режиме работы и для разблокирования трафика при разрыве кольца.</td></tr>
<tr><td colspan="2">RPL_Neighbour – коммутатор назначается «соседом (соседний узел кольца)» RPL для кольца. Отвечает за блокировку своего конца RPL в нормальных условиях.</td></tr>
<tr><td rowspan="3">Порт RPL</td><td colspan="2">None – порт не выбран.</td></tr>
<tr><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>
</table>

<table>
<tr><th>Параметр</th><th colspan="3">Функция</th></tr>
<tr><td rowspan="6">Команда экземпляра</td><td rowspan="4">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>
<tr><td colspan="2">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.</td></tr>
<tr><td rowspan="3">Управляющий порт</td><td colspan="2">None – порт не выбран.</td></tr>
<tr><td>Port0</td><td rowspan="2">Порт0 или Порт1 группы защиты, к которому применяется команда.</td></tr>
<tr><td>Port1</td></tr>
<tr><td rowspan="6">Состояние экземпляра</td><td>Состояние защиты</td><td colspan="2">Состояние ERPS в соответствии с таблицами перехода состояний в G.8032.</td></tr>
<tr><td>Состояние порта 0</td><td colspan="2" rowspan="2">– OK – нормальное состояние;
– SF – сбой.</td></tr>
<tr><td>Состояние порта 1</td></tr>
<tr><td>Передано APS</td><td colspan="2">Передаваемые точки доступа в соответствии с таблицами перехода состояний в G.8032.</td></tr>
<tr><td>Порт 0 получение APS</td><td colspan="2" rowspan="2">Принятые точки доступа на порту 0 или 1 в соответствии с таблицами перехода состояний в G.8032.</td></tr>
<tr><td>Порт 1 получение APS</td></tr>
<tr><td>Осталось WTR</td><td colspan="2">Оставшийся таймаут WTR в миллисекундах.</td></tr>
</table>

Параметр	Функция	
	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).

10.8.2.2 **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 10.9).

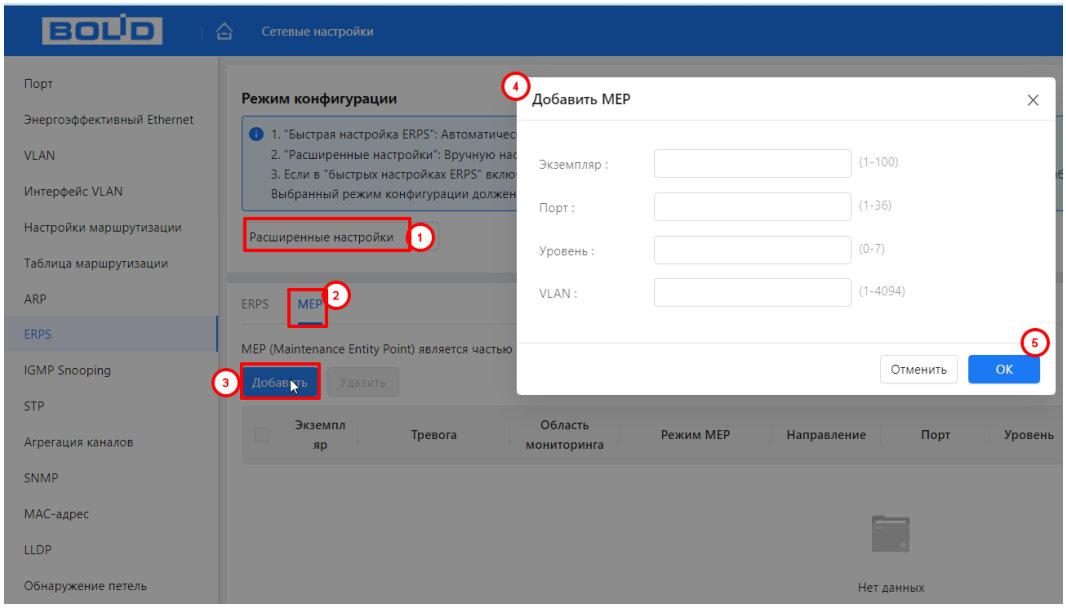


Рисунок 10.19 – Добавление MEP

Таблица 10.9 – 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.

Параметр	Функция
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 10.20, Таблица 10.10).

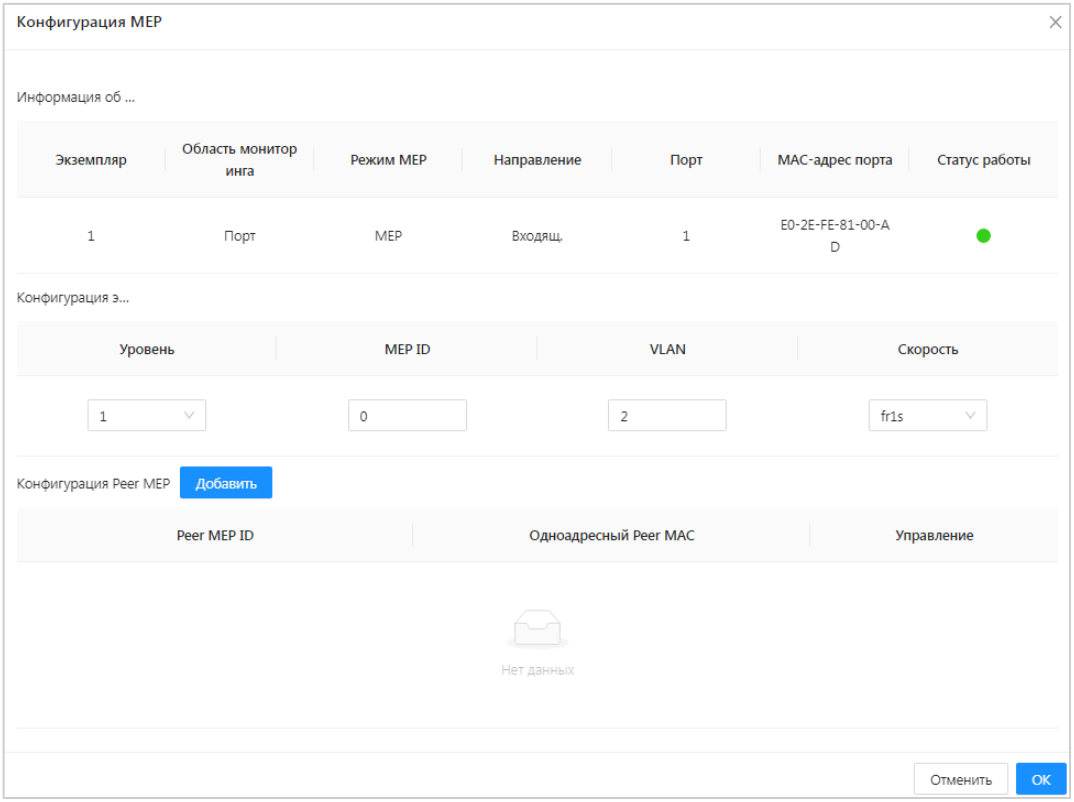


Рисунок 10.20 – Конфигурация MEP

Таблица 10.10 – Параметры настройки MEP

Параметр	Функция	
Информация об экземпляре	Экземпляр	Панель отображает ранее заданные параметры, более подробно каждый параметр описан в таблице выше (Таблица 10.9).
	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.

Параметр	Функция	
	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 одноранговой MEP целевого MEP. Используется только, когда одноадресный MAC-адрес одноранговой устройства состоит из одних нулей.
	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»

10.9 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.

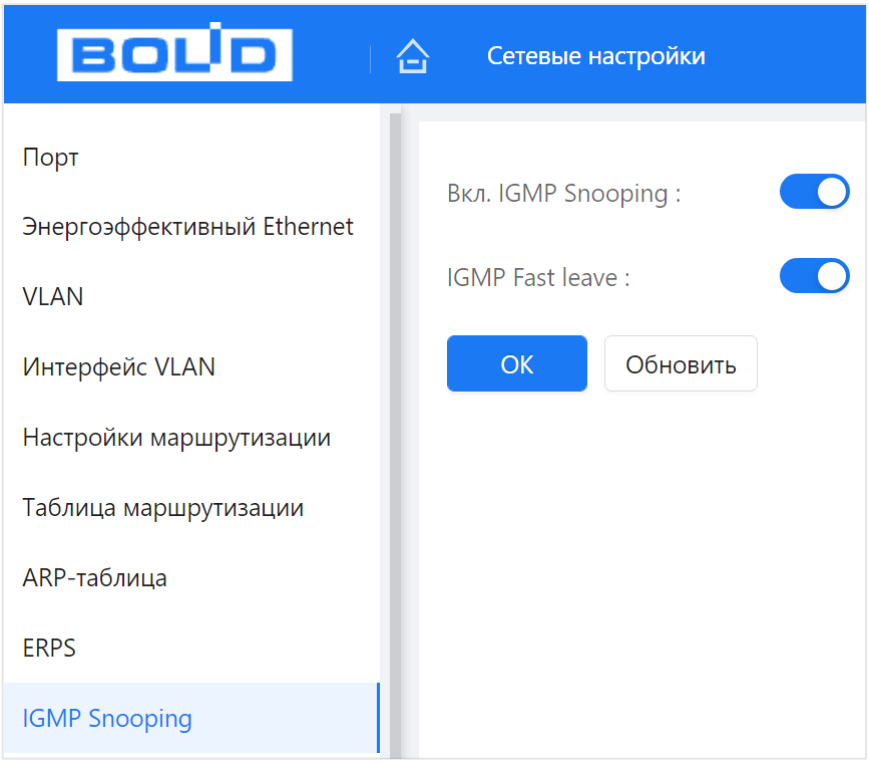


Рисунок 10.21 – Интерфейс IGMP Snooping

10.10 Подраздел «STP»

10.10.1 Пункт «STP»

На рисунке ниже (Рисунок 10.22) изображён интерфейс изменения настроек STP и протокола его работы.

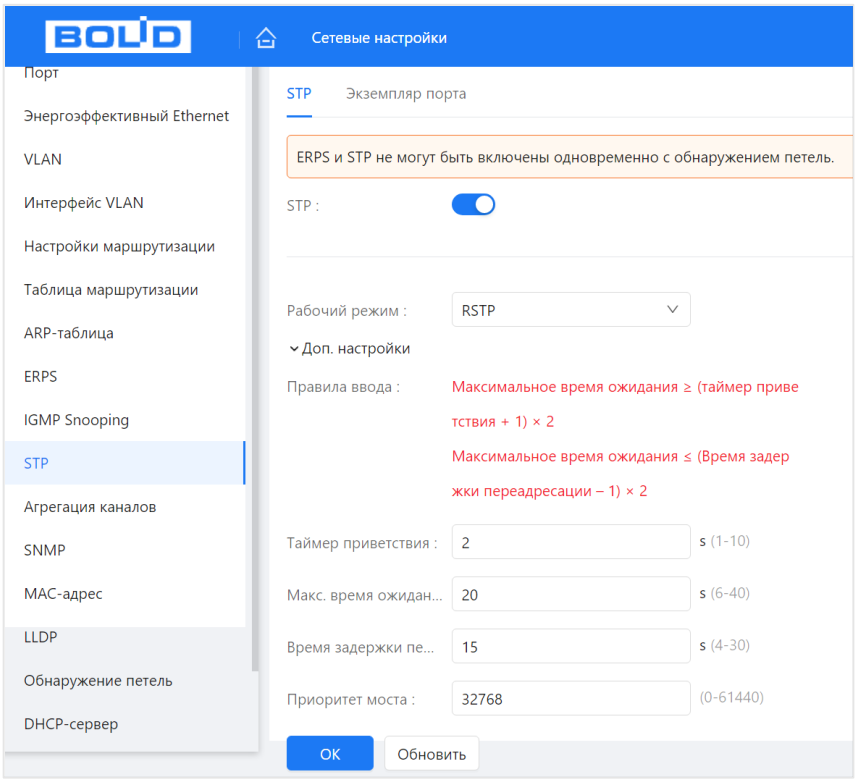


Рисунок 10.22 – Настройка STP

Таблица 10.11 – 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.
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.

10.10.2 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.

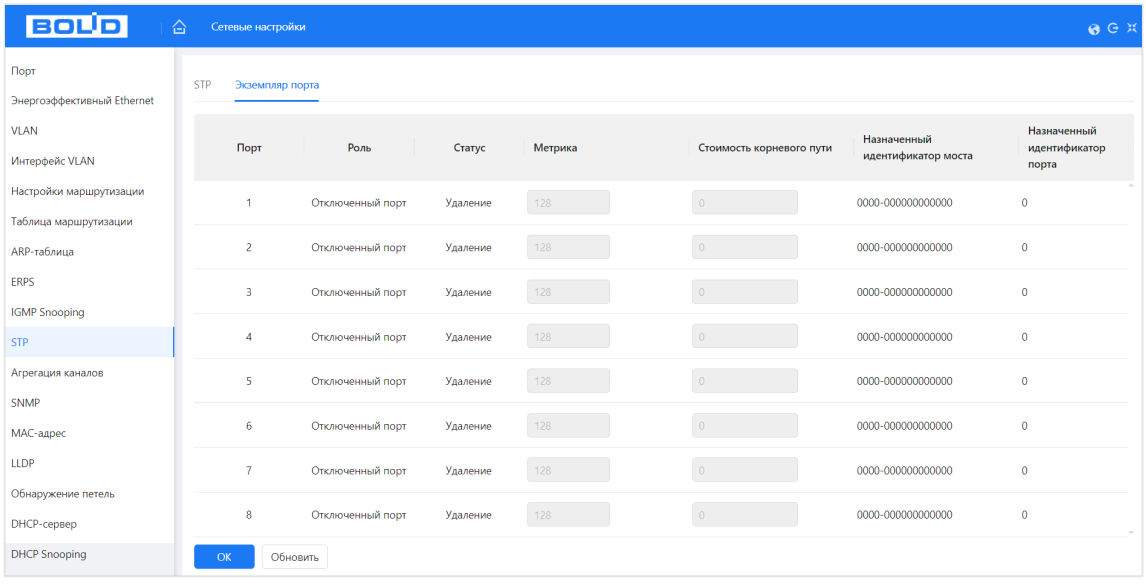


Рисунок 10.23 – Настройка STP

Таблица 10.12 – 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.
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.

10.11 Подраздел «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.

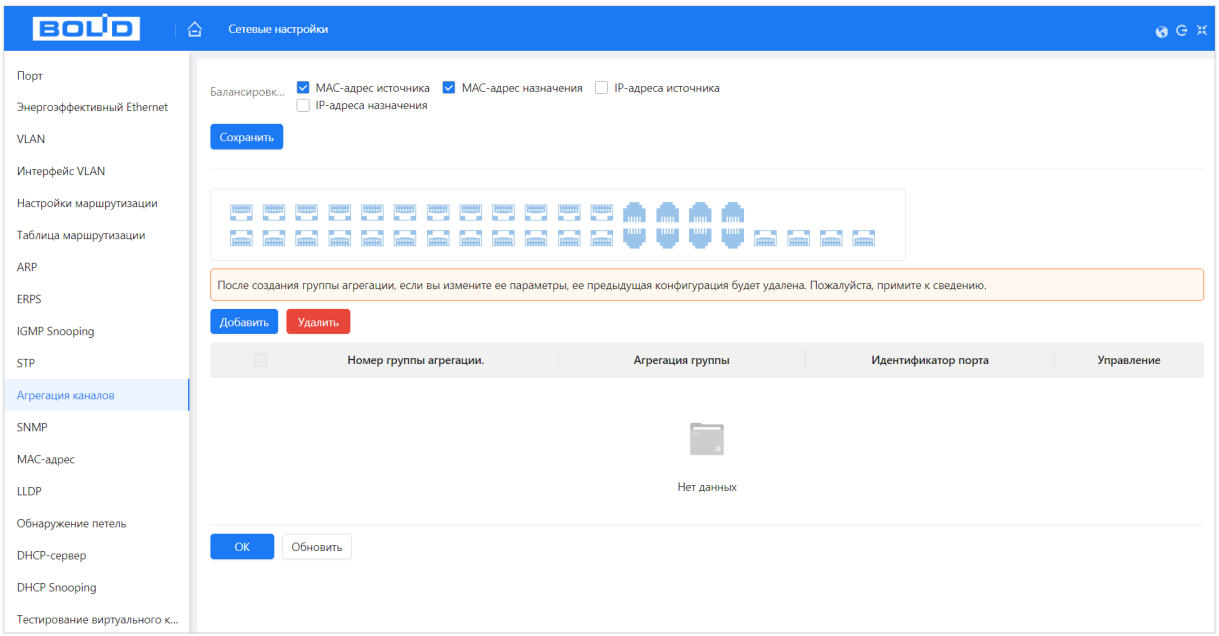


Рисунок 10.24 – Агрегация каналов

10.11.1 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 10.13 – Типы алгоритма балансировки нагрузки

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

10.11.2 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.

10.11.2.1 **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.

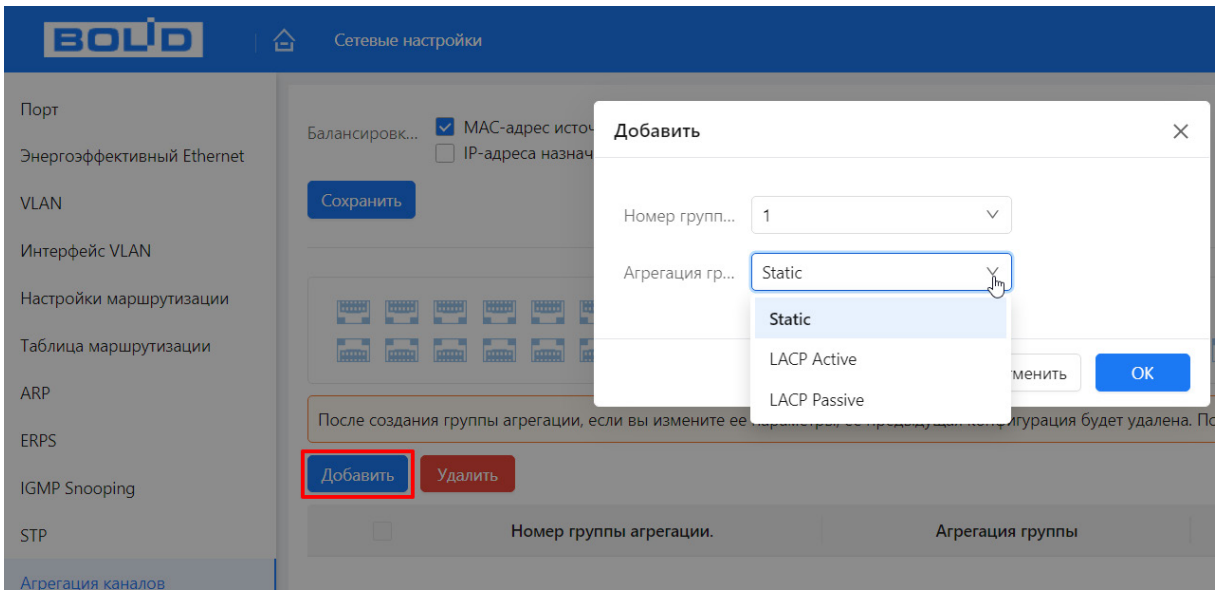


Рисунок 10.25 – Добавление

5. Далее выберите порты для объединения (Рисунок 10.26). Для этого нажмите кнопку  и выделите порты.

6. Нажмите кнопку «ОК» для сохранения.

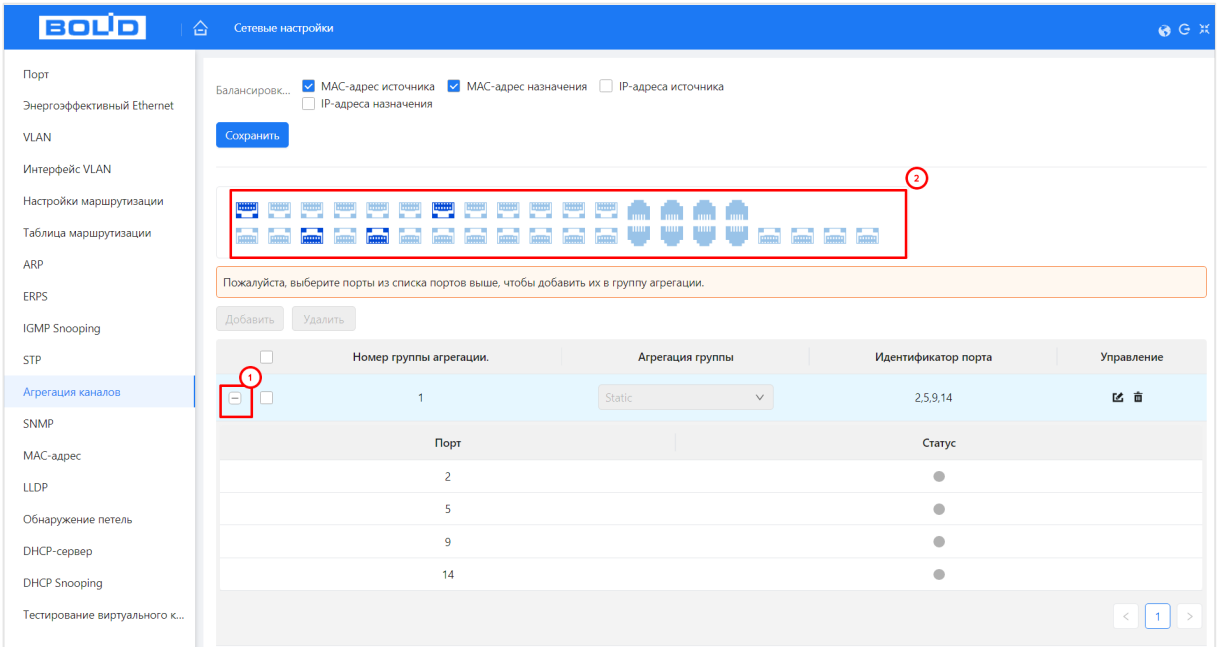


Рисунок 10.26 – Добавление

10.12 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 10.27) 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.

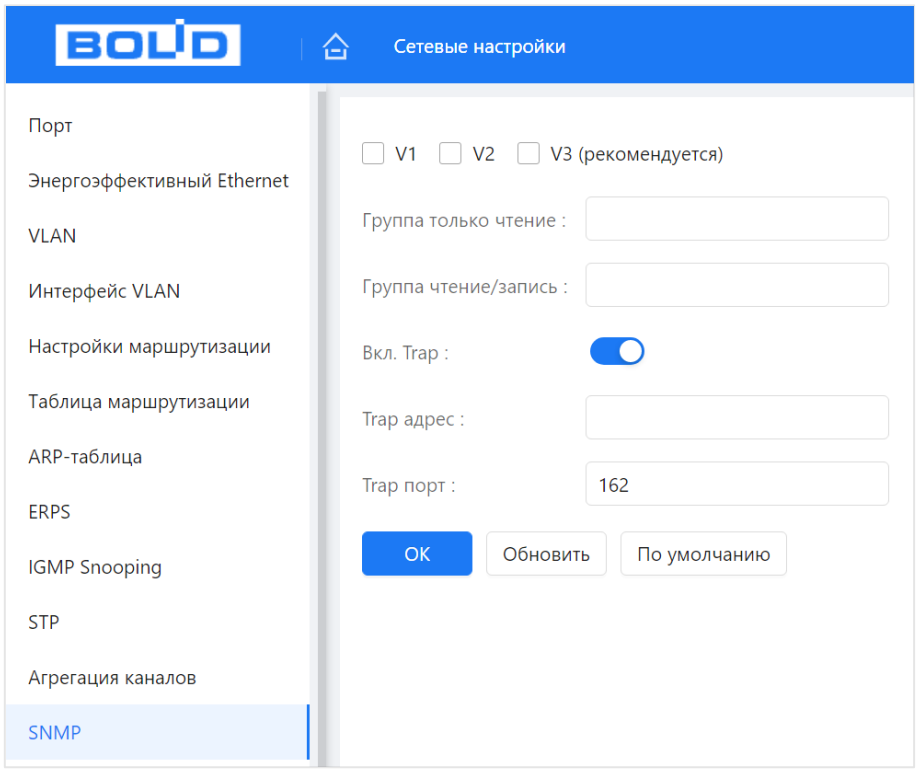


Рисунок 10.27 – Настройки SNMP

На рисунке (Рисунок 10.28) изображён интерфейс настроек SNMP версии 3.

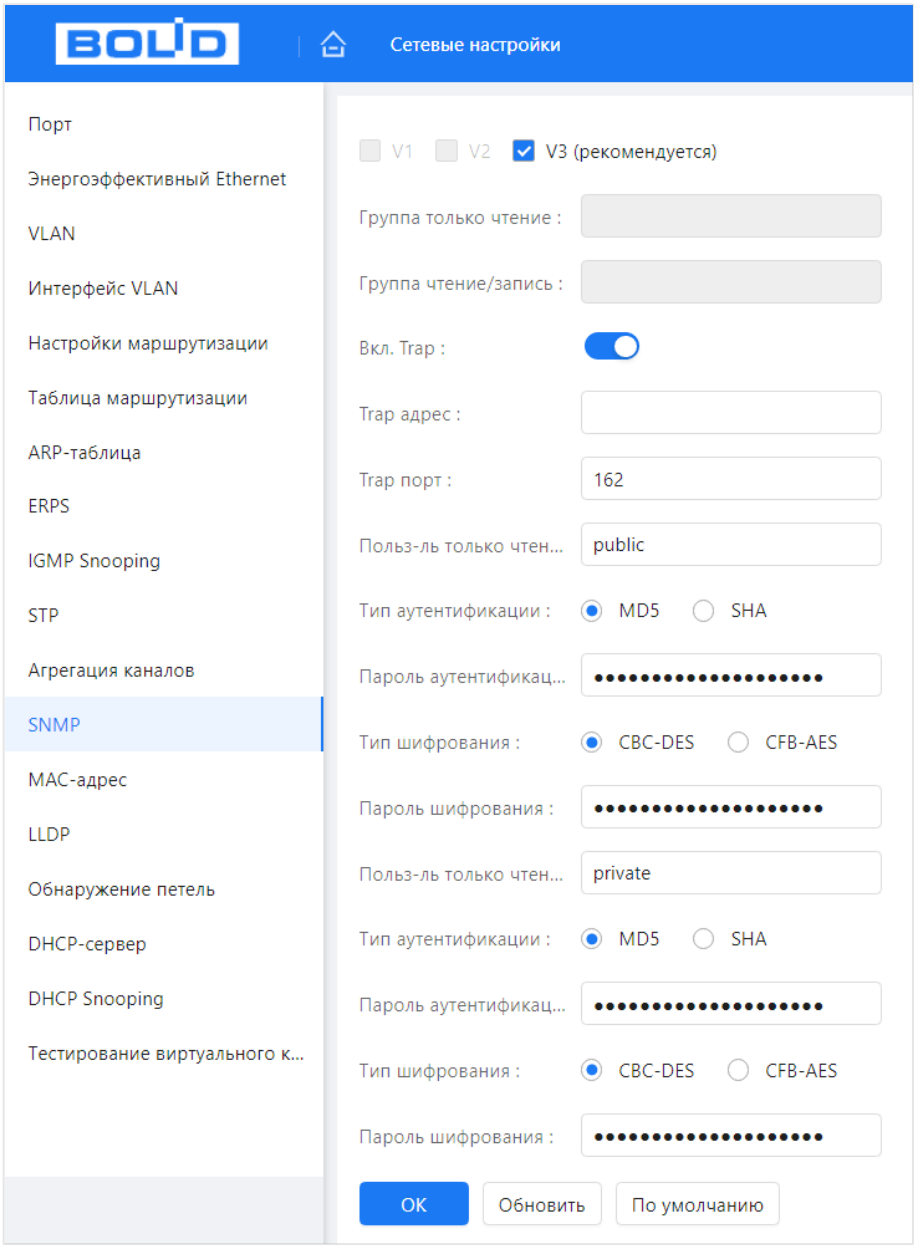


Рисунок 10.28 – Настройки SNMPv3

Таблица 10.14 – 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);

Название	Описание
	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.
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.

10.13 Подраздел «MAC-адрес»

10.13.1 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.

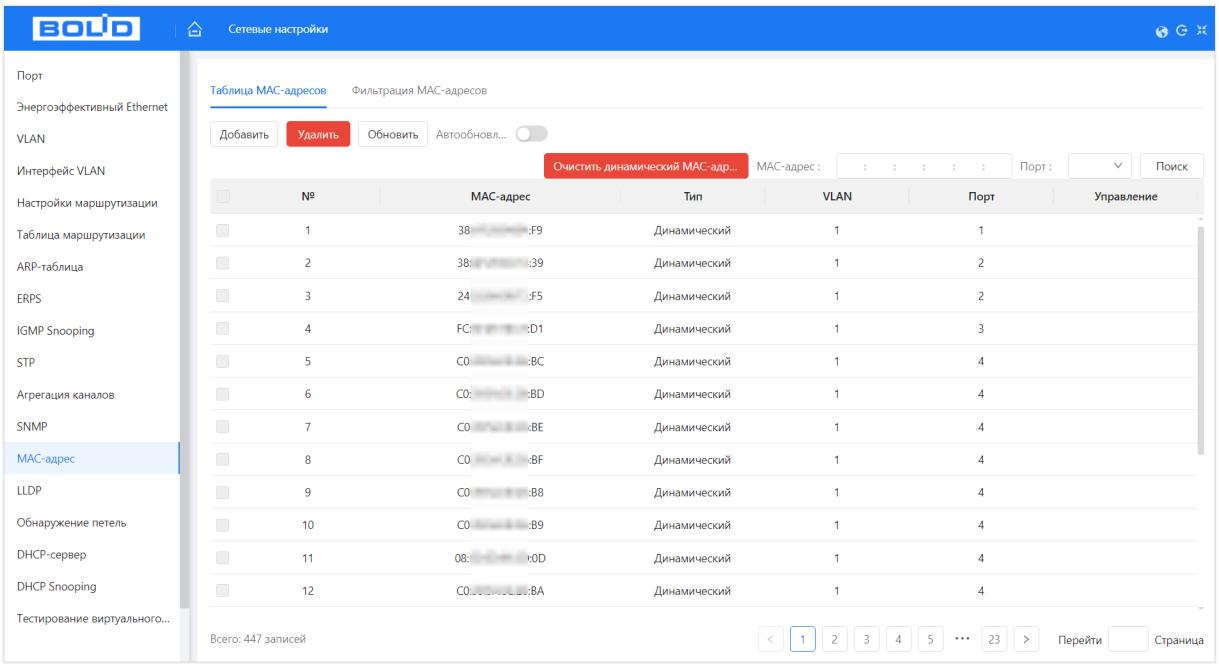


Рисунок 10.29 – MAC информация об адресах

10.13.2 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.

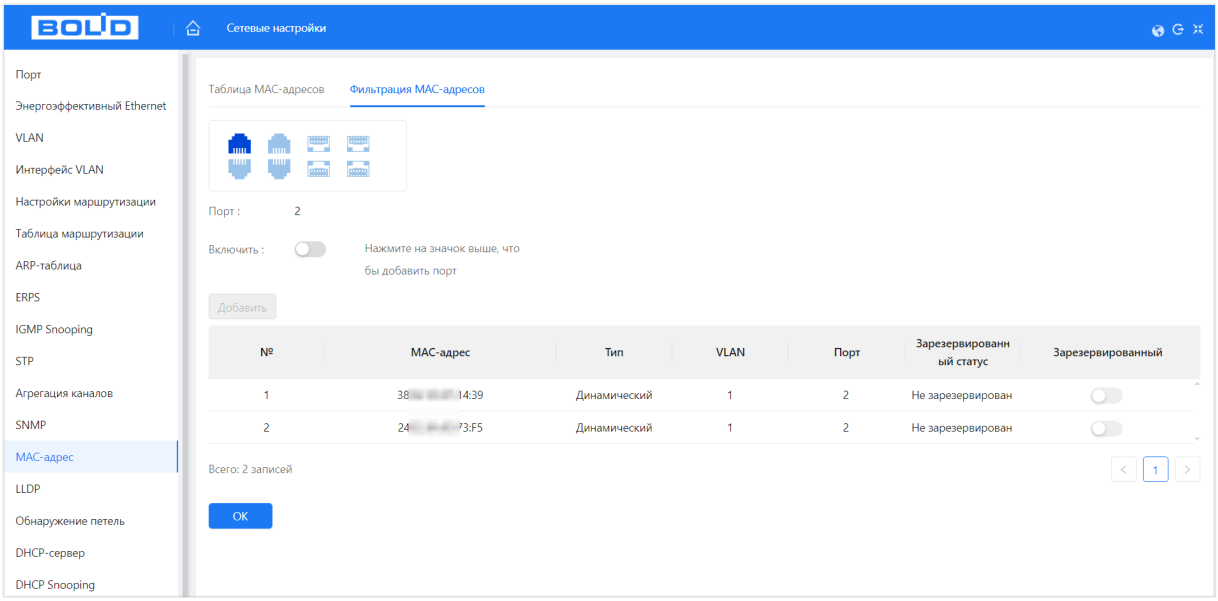


Рисунок 10.30 – Фильтрация портов

10.14 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.

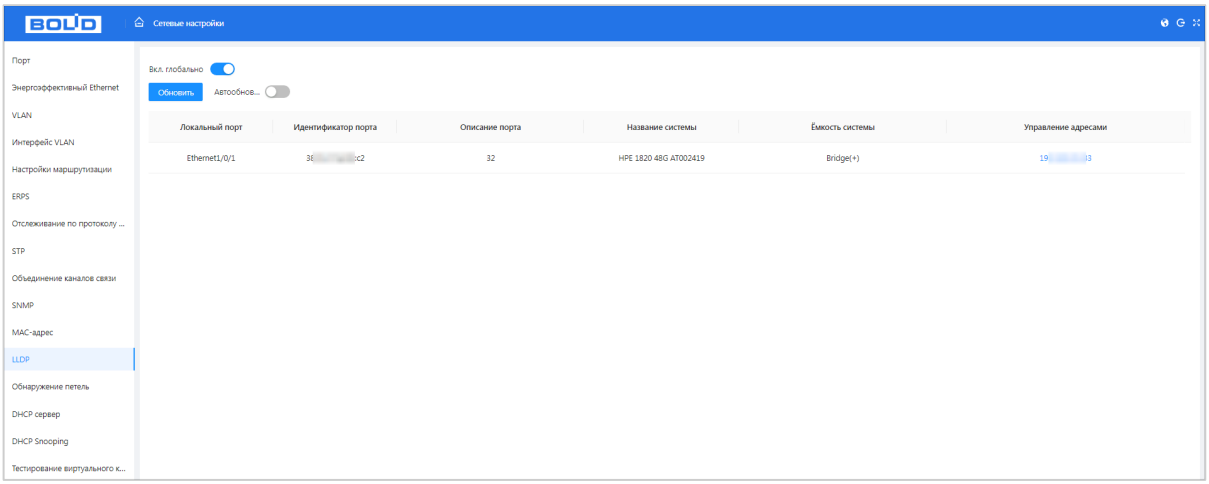


Рисунок 10.31 – Обнаружение по LLDP

10.15 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.

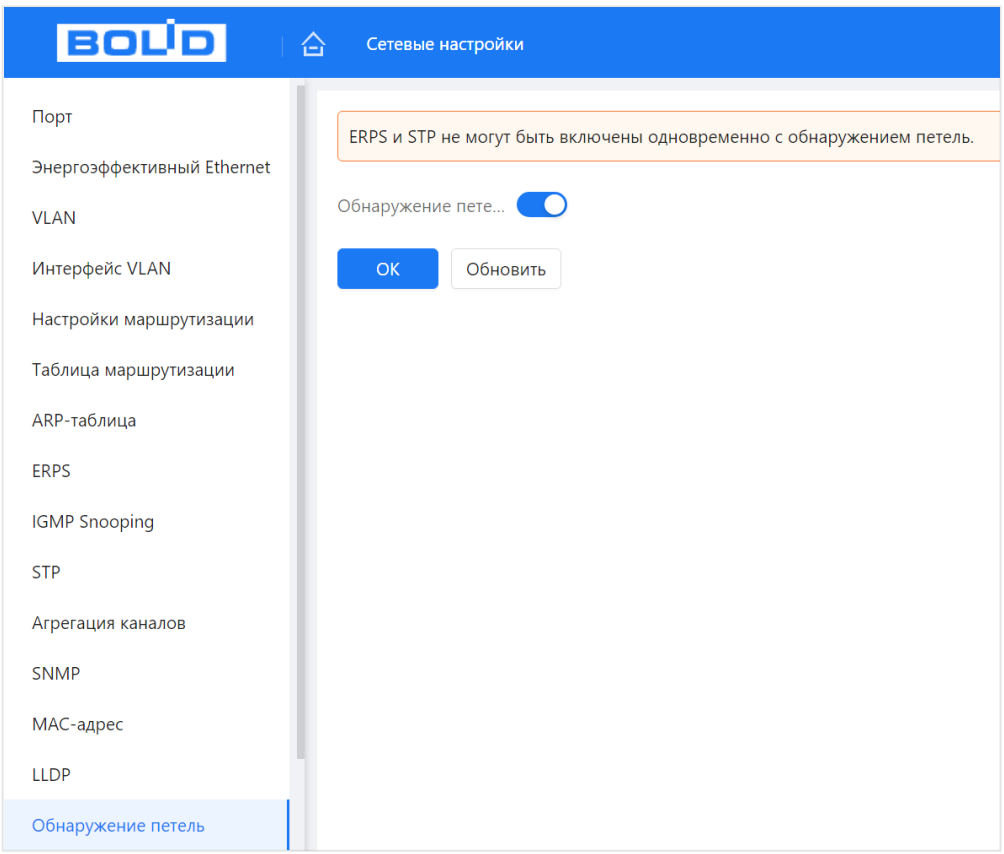


Рисунок 10.32 – Обнаружение петель (Loopback Detection)

10.16 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.

10.16.1 Пункт «DHCP-сервер»

10.16.1.1 **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.

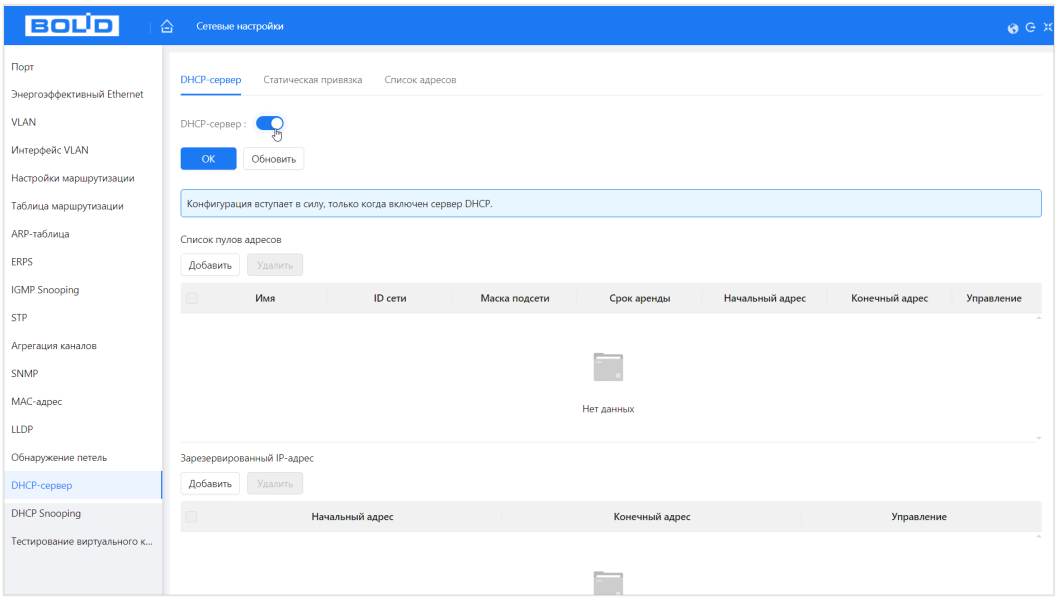


Рисунок 10.33 – Настройка DHCP-сервера

10.16.1.2 **Добавление DHCP POOL**

Для создания пулов IP-адресов, которые будут раздаваться, нажмите «Добавить», далее введите данные для добавления (Рисунок 10.34, Таблица 10.15).

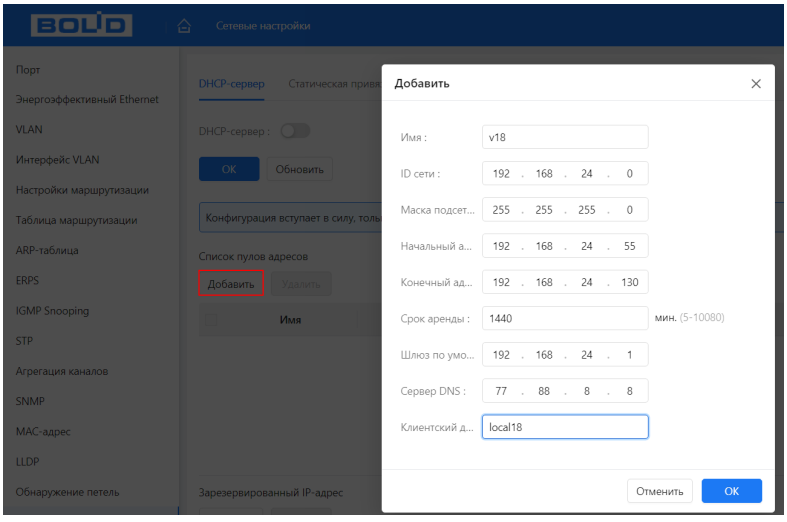


Рисунок 10.34 – Добавить пул

Таблица 10.15 – 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.

10.16.1.3 **Добавление зарезервированного IP-адреса**

После нажатия кнопки «Добавить» в поле «Зарезервированный IP-адрес» откроется окно добавления зарезервированных IP-адресов (Рисунок 10.35). Введите диапазон IP-адресов, которые будут исключены из общего пула назначаемых адресов.

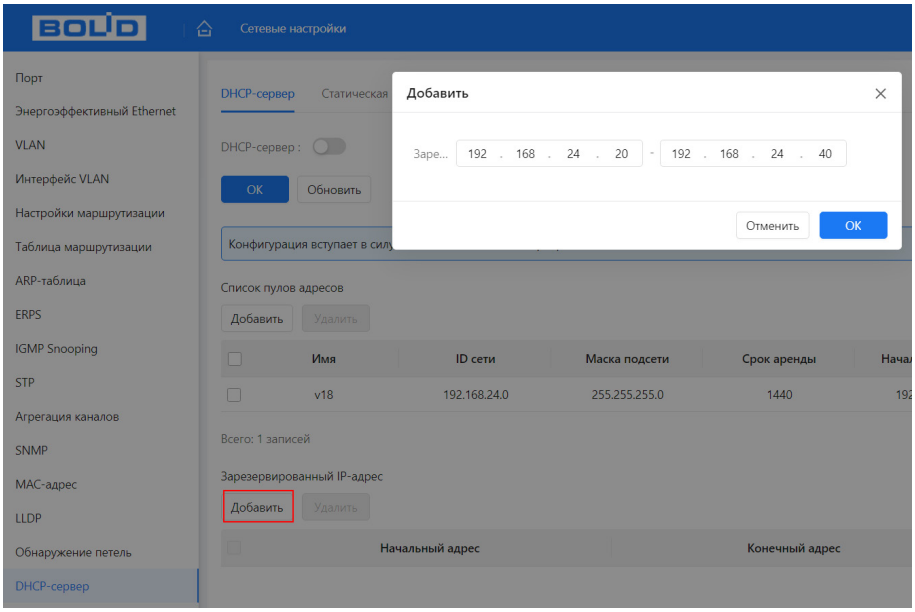


Рисунок 10.35 – Добавление зарезервированных IP-адресов

10.16.2 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.

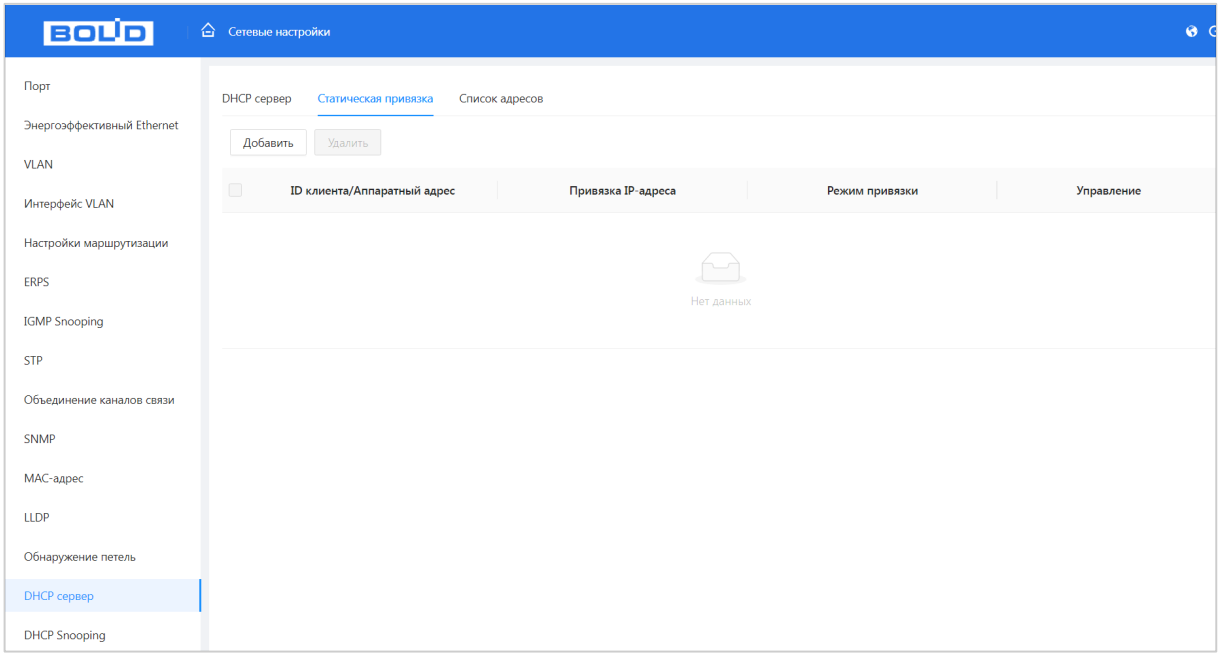


Рисунок 10.36 – Статическая привязка

1. Для добавления нажмите кнопку «Добавить».
2. В появившемся окне заполните поля (Таблица 10.16).

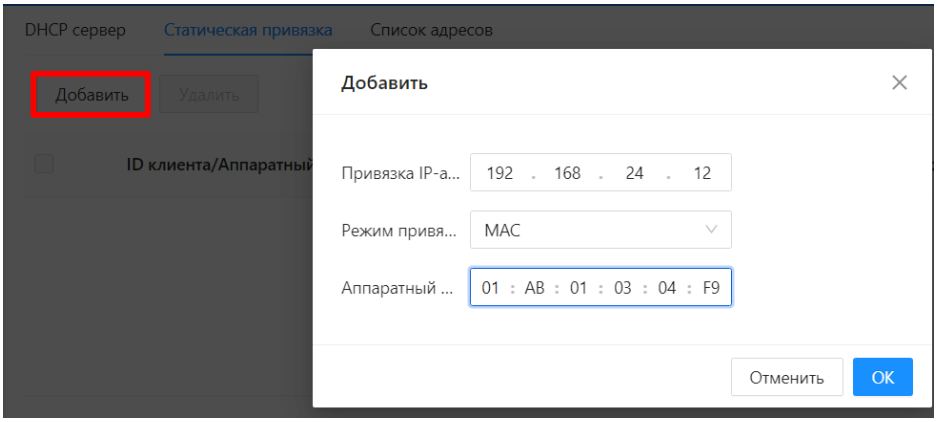


Рисунок 10.37 – Добавление в список

Таблица 10.16 – Статическая привязка

Параметр	Функция
Привязка IP-адреса	Поле ввода зарезервированного IP-адреса.
Режим привязки	Доступен выбор: MAC или Name_ASCII.

Параметр	Функция
Аппаратный адрес/ ID клиента	Поле ввода значения исходя из выбранного режима. – Аппаратный адрес – ввод MAC-адреса; – ID клиента (DHCP Option 61) – ввод идентификатора клиента.

10.16.3 Пункт «Список адресов»

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

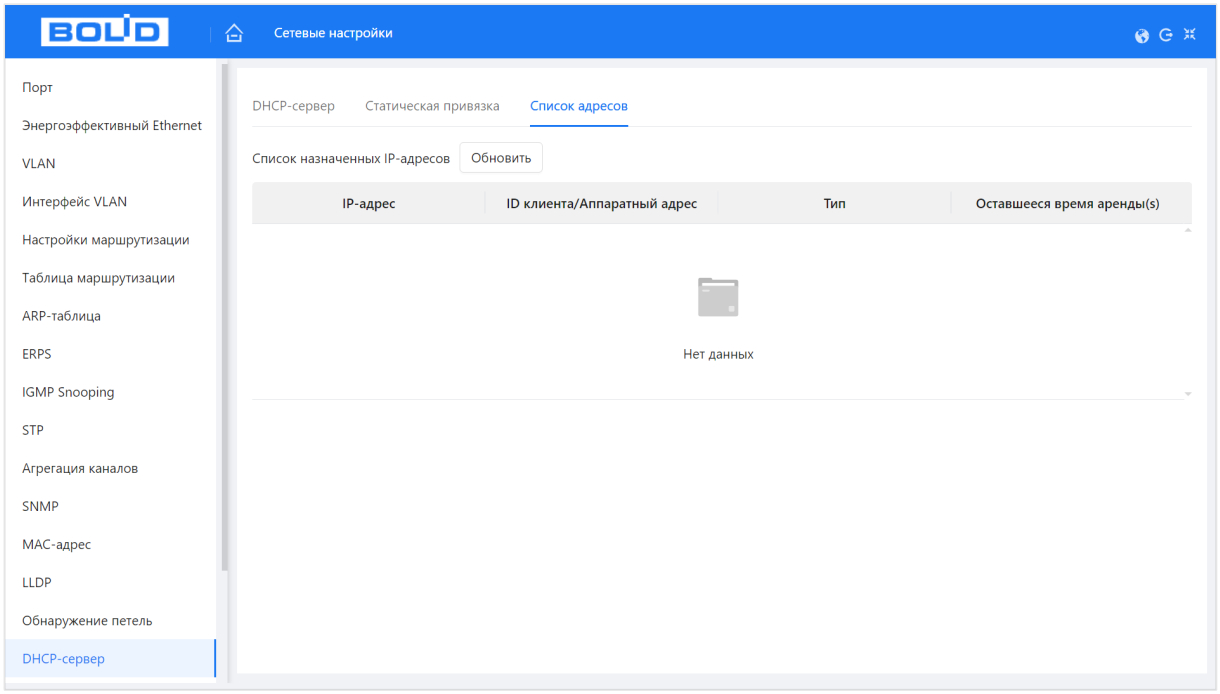


Рисунок 10.38 – Список адресов

10.17 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.

10.17.1 Пункт «Глобальные настройки»

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

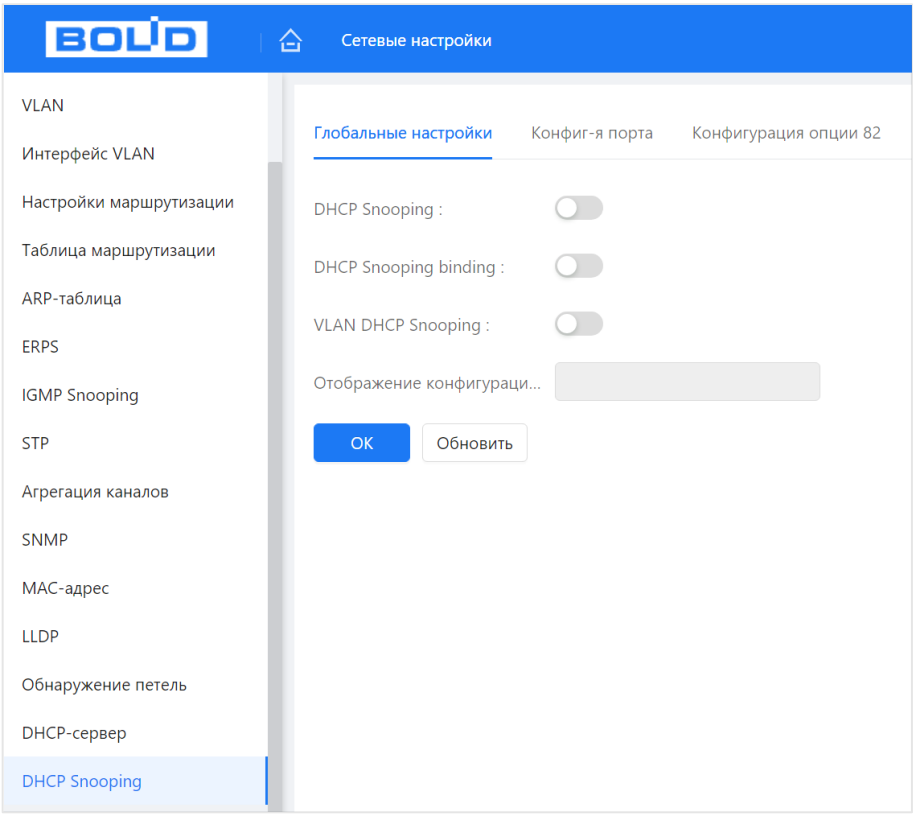


Рисунок 10.39 – Глобальные настройки DHCP Snooping

Переключатель «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.

10.17.2 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.

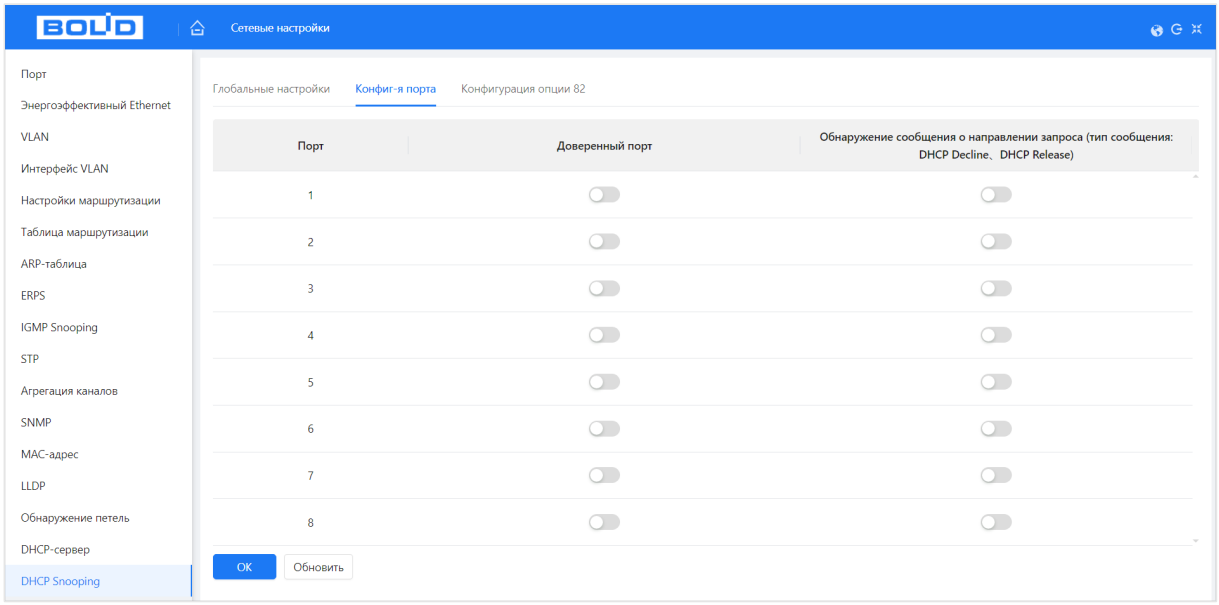


Рисунок 10.40 – Настройка портов

10.17.3 Пункт «Конфигурация опции 82»

Дополнительным шагом настройки является включение на порту «Опции 82» (Рисунок 10.41). Используется эта функция для передачи дополнительной информации о DHCP-клиенте на DHCP-сервер (например, порт, VLAN, название устройства и т.д.).

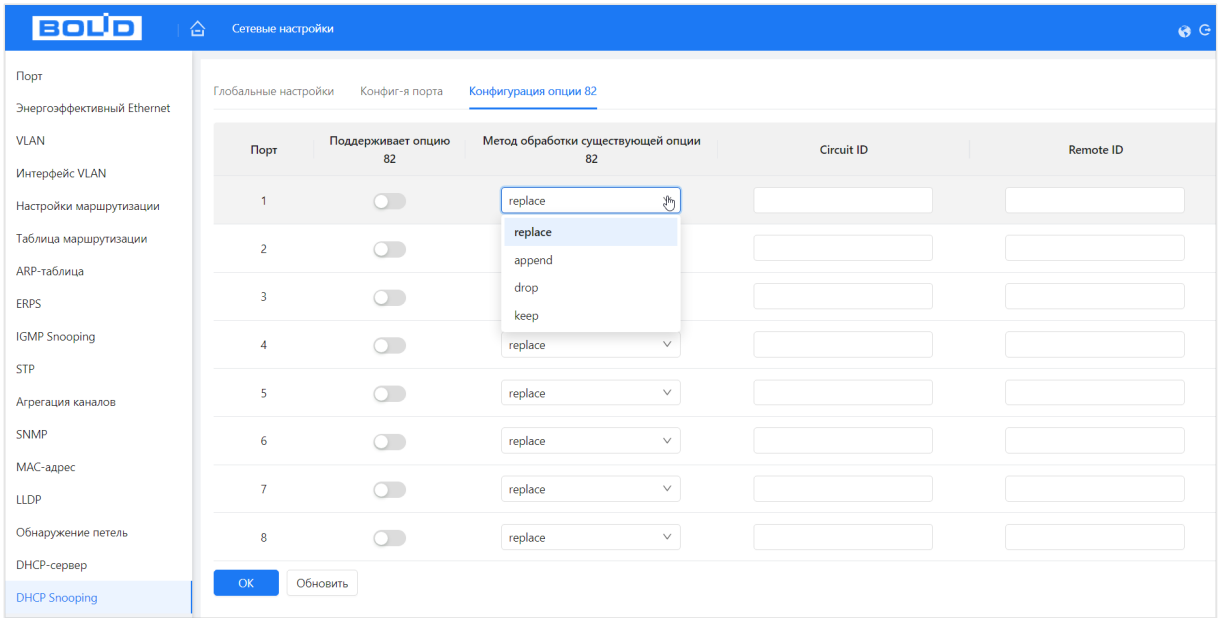


Рисунок 10.41 – Конфигурация опции 82

Таблица 10.17 – Параметры включения «опции 82»

Параметр	Функция
Порт	Номер порта коммутатора.
Поддерживает опцию 82	Включение или выключение функции на порту.

Параметр	Функция
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	Идентификатор подключенного к коммутатору клиентского устройства \ номера клиентского Ethernet порта. Он может быть использован для назначения параметров, уникальных для конкретного пользователя.
Remote ID	Идентификатор коммутатора, который может быть использован для назначения сервером сетевых настроек.

10.18 Подраздел «Тестирование виртуального кабеля»

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

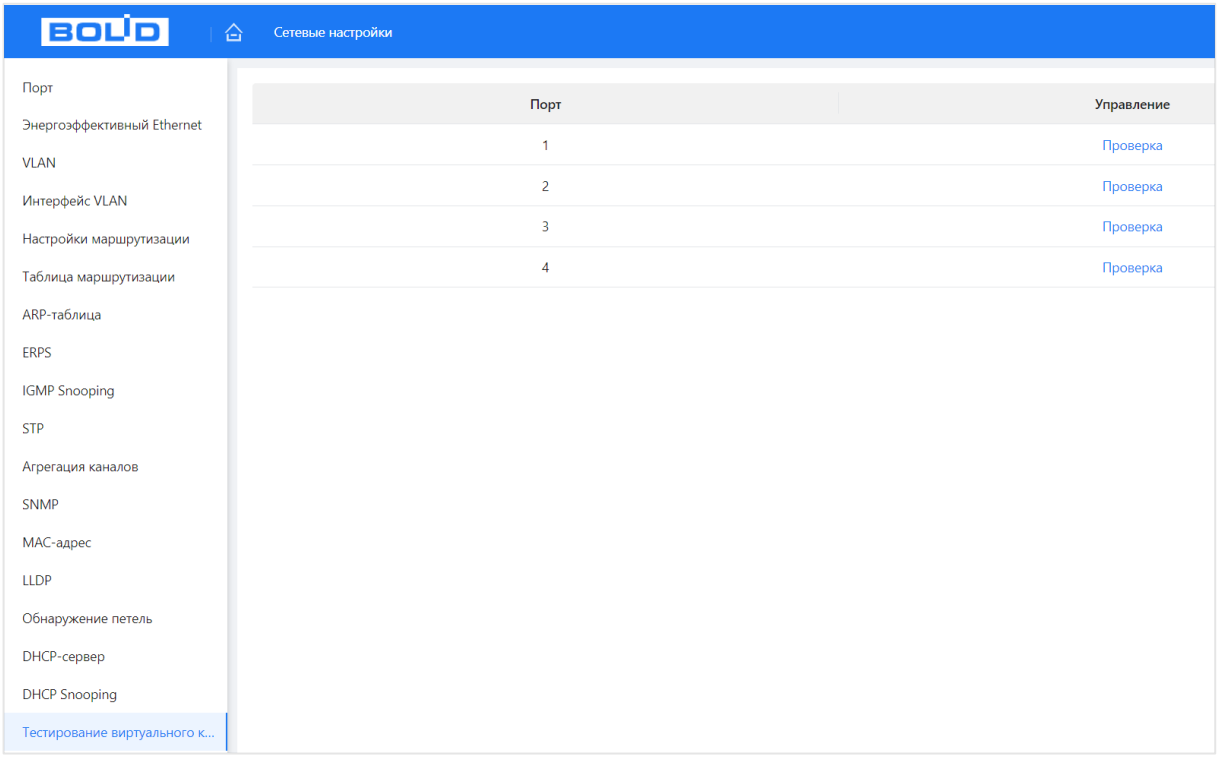


Рисунок 10.42 – Тестирование виртуального канала

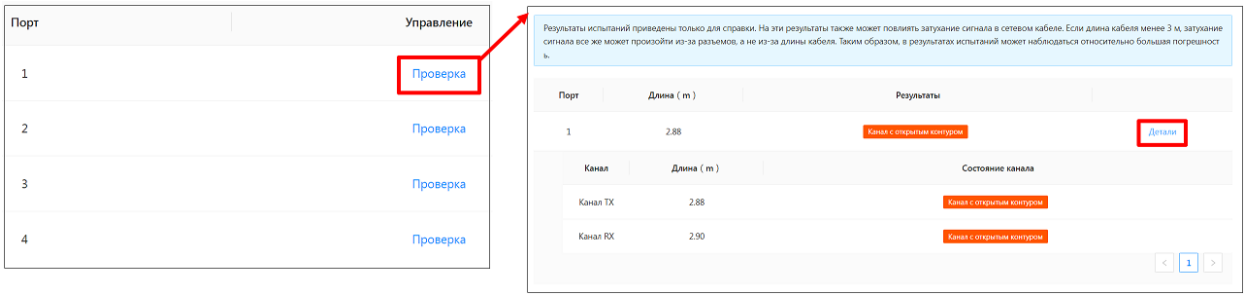


Рисунок 10.43 – Тестирование виртуального канала

11 РАЗДЕЛ ГЛАВНОГО МЕНЮ «ЦЕНТР БЕЗОПАСНОСТИ»

11.1 Подраздел «Доп. сервисы»

11.1.1 Пункт «Доп. сервисы»

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

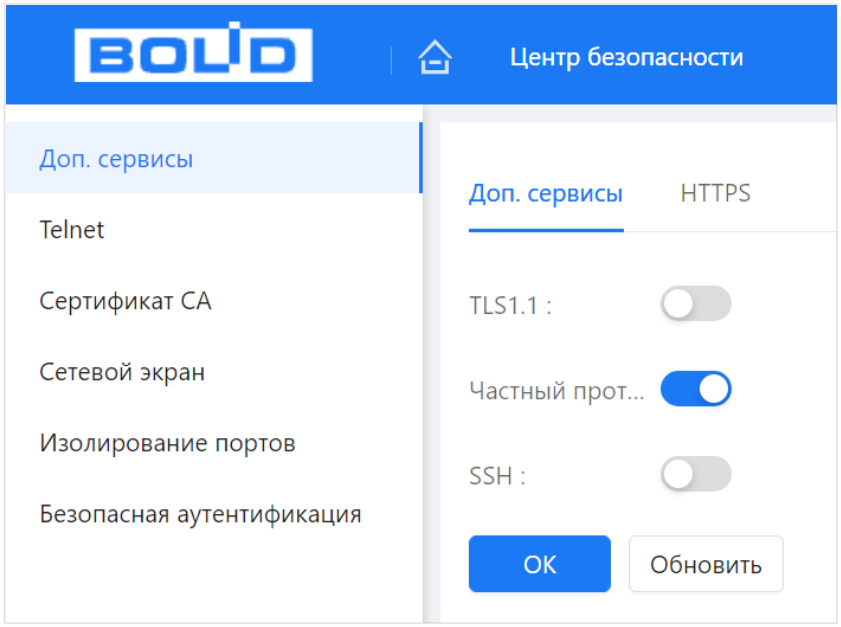


Рисунок 11.1 – Системное обслуживание

Таблица 11.1 – 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.
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.

11.1.2 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.

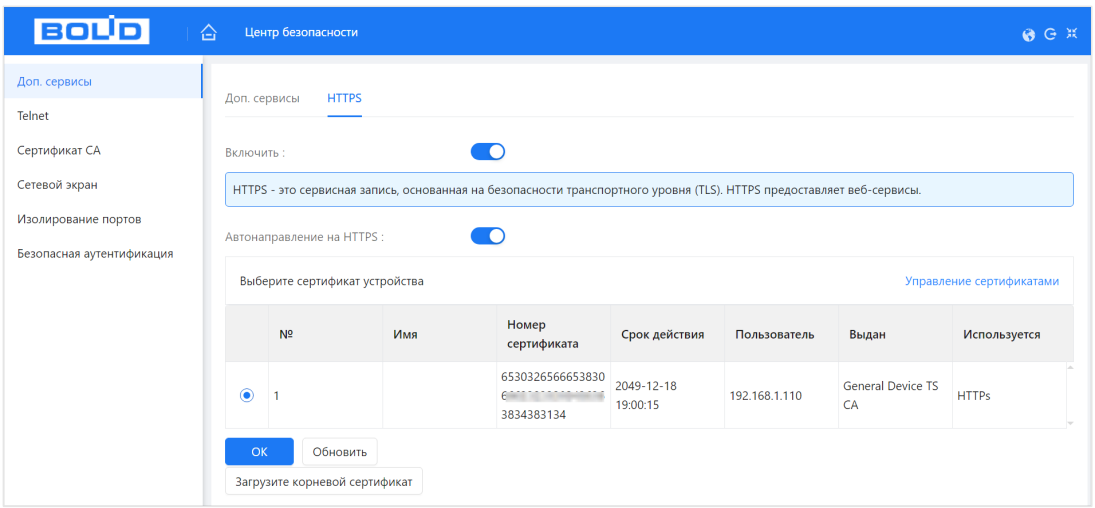


Рисунок 11.2 – HTTPS

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.

11.2 Подраздел «Telnet»

Telnet – это базовый протокол удалённого управления, который обеспечивает доступ к сетевым устройствам через командную строку для выполнения задач по настройке и техническому обслуживанию. Передаваемые данные, включая учётные данные, не шифруется и передаётся в открытом виде. В связи с этим в системах с повышенными требованиями к защите данных рекомендуется использовать более безопасный протокол SSH.

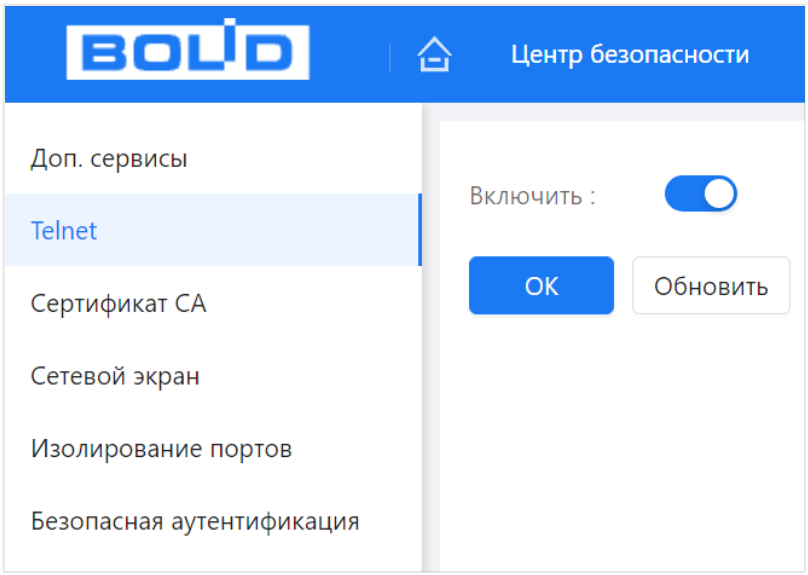


Рисунок 11.3 – Telnet

11.3 Подраздел «Сертификат CA»

11.3.1 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.

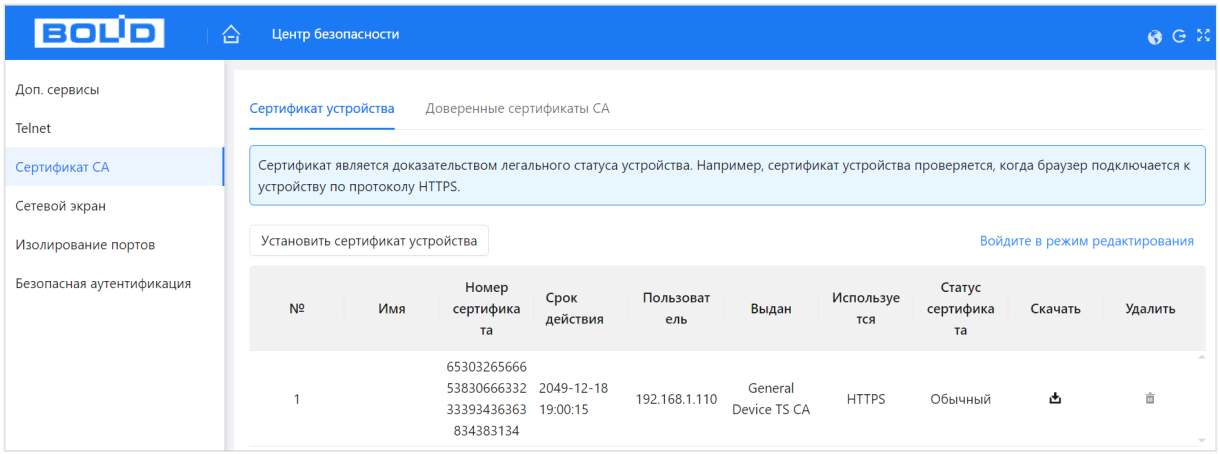


Рисунок 11.4 – Сертификат устройства

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

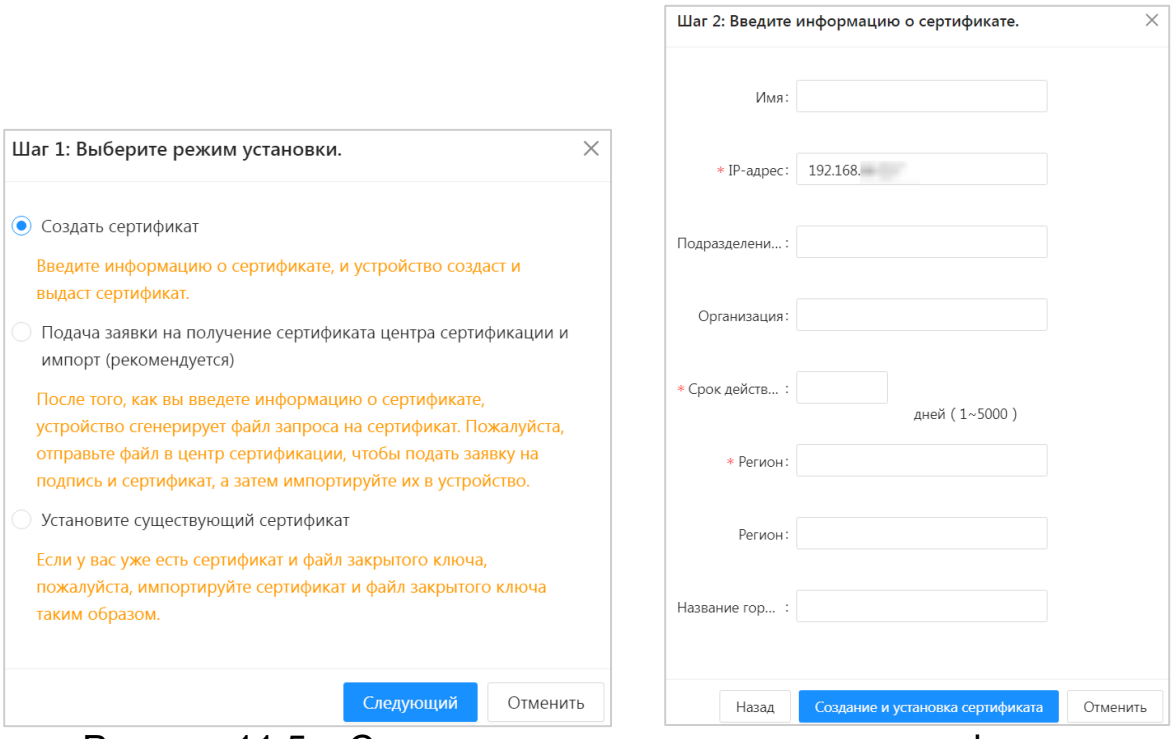


Рисунок 11.5 – Создание самоподписанного сертификата

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.

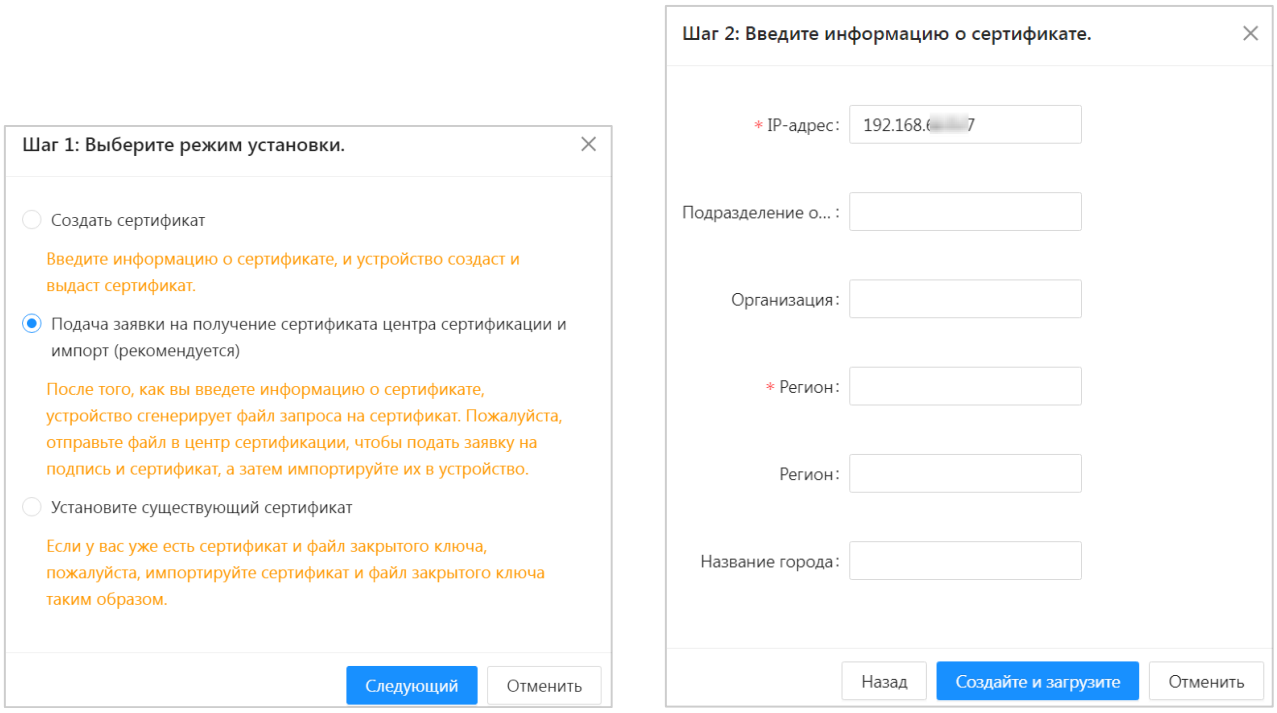


Рисунок 11.6 – Создание и импорт доверенного сертификата

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

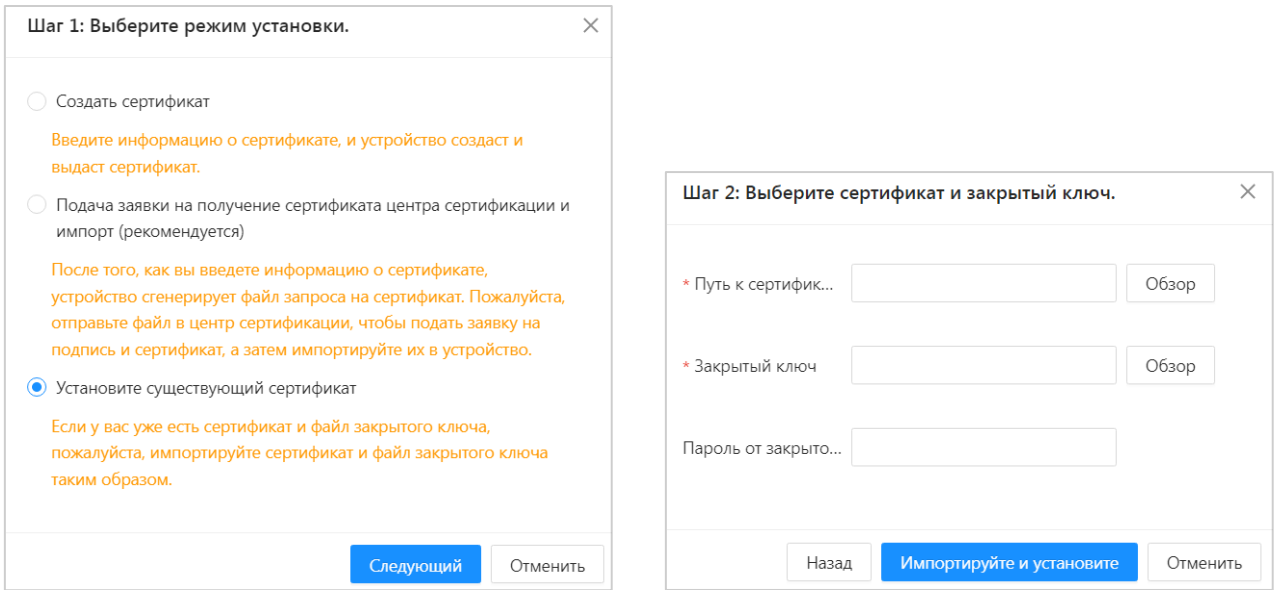


Рисунок 11.7 – Импорт стороннего сертификата

11.3.2 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.

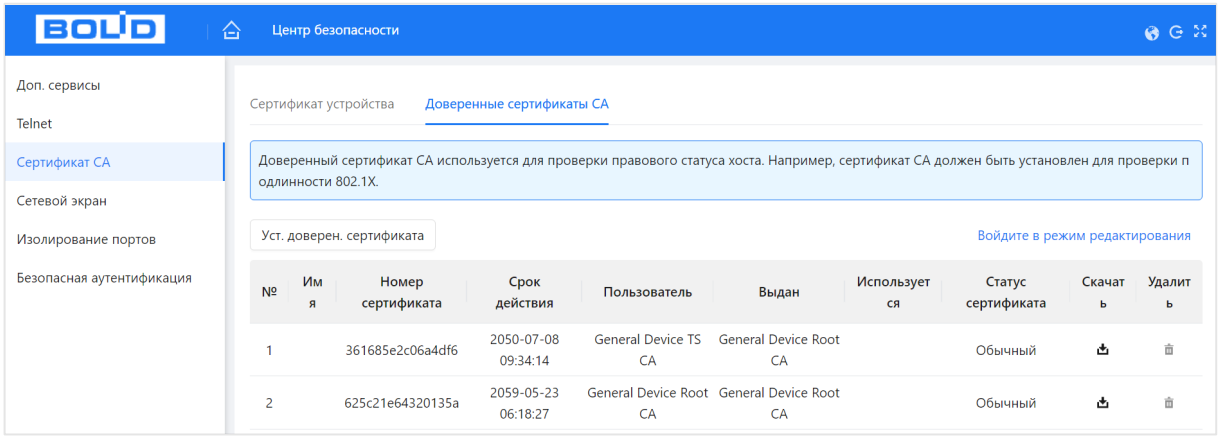


Рисунок 11.8 – Установка доверенного сертификата

11.4 Подраздел «Сетевой экран»

11.4.1 Пункт «IP фильтр»

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

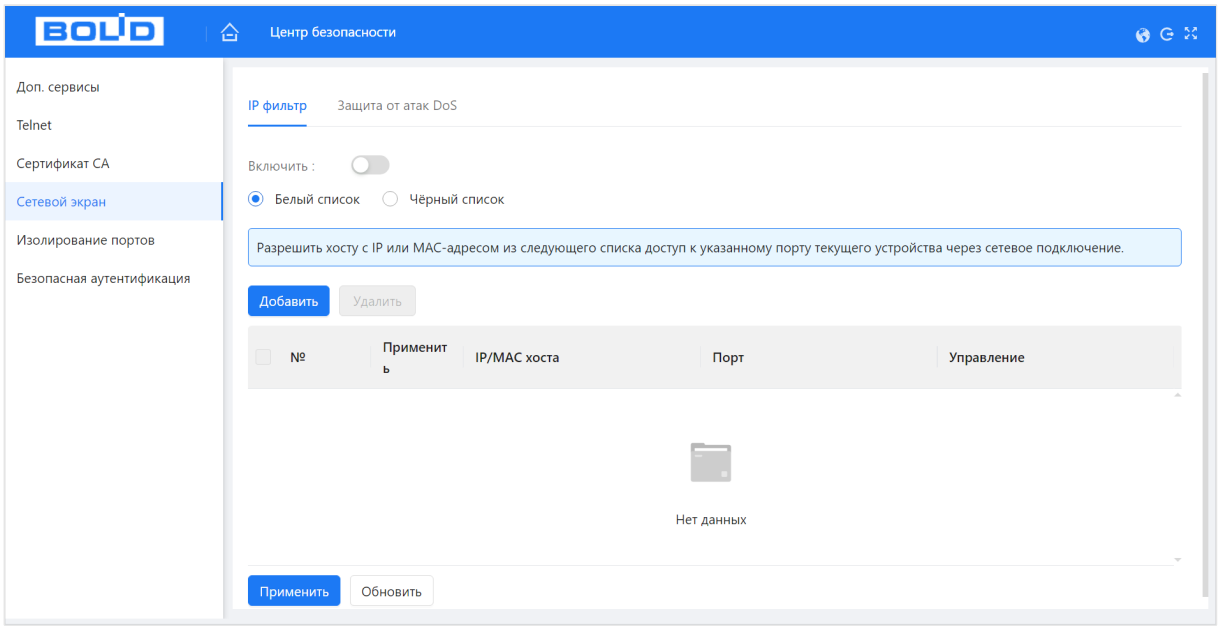


Рисунок 11.9 – Фильтрация по IP

1. Включите функцию и выберите список доступа (Рисунок 11.10). Для данного устройства доступны следующие варианты:

– Белый список – сетевой доступ разрешён;

– Чёрный список – сетевой доступ запрещён.

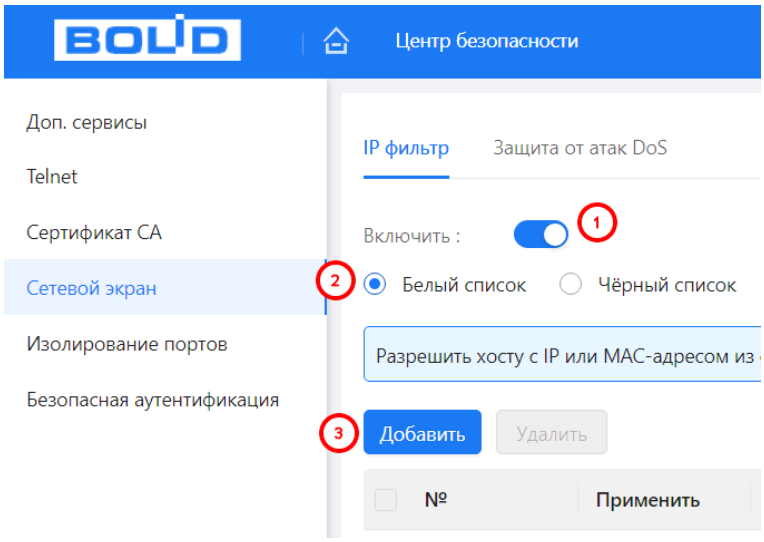


Рисунок 11.10 – Добавить

2. Нажмите кнопку «Добавить», выберите из выпадающего списка способ добавления (Рисунок 11.10). Доступно:

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

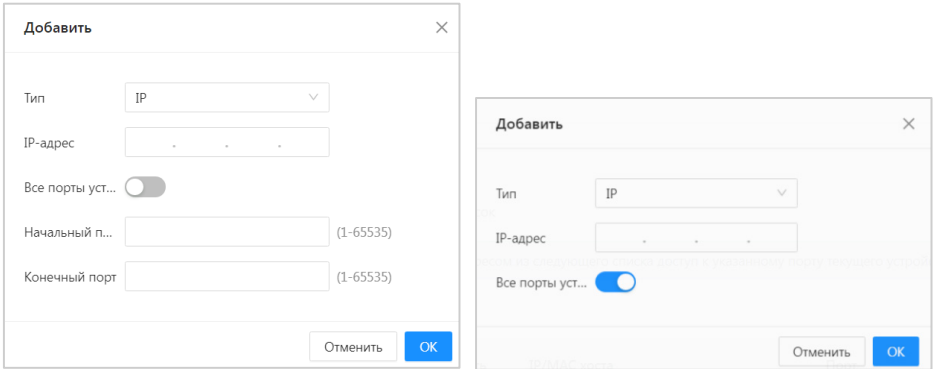


Рисунок 11.11 – Добавить IP-адрес

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

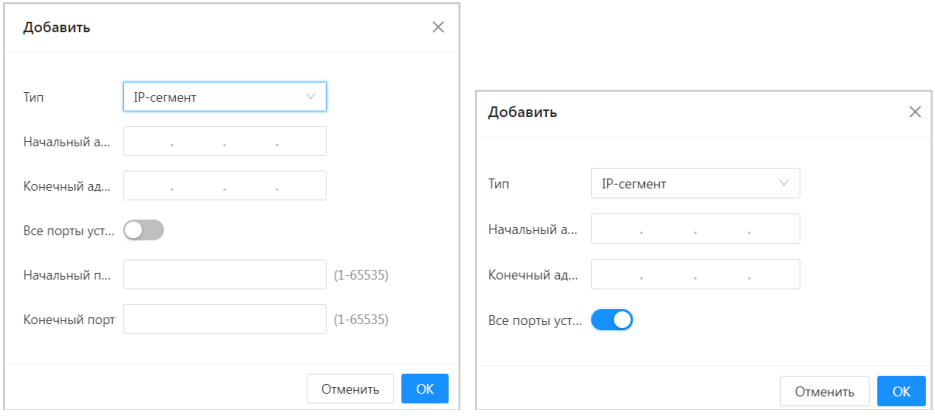


Рисунок 11.12 – Добавить диапазон IP

– Добавление при введении MAC-адреса;

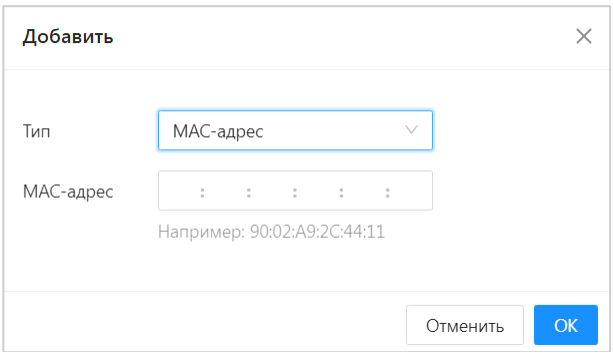


Рисунок 11.13 – Добавить MAC-адрес

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

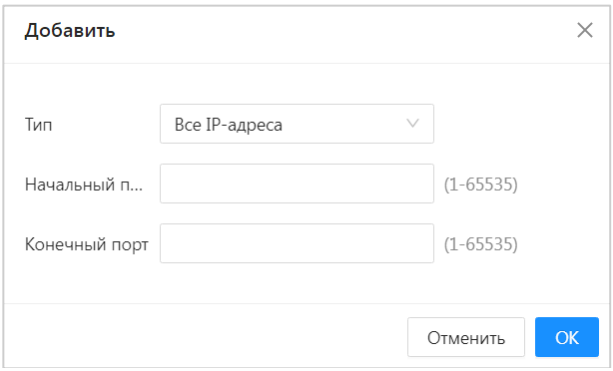


Рисунок 11.14 – Добавить все IP-адреса

11.4.2 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.

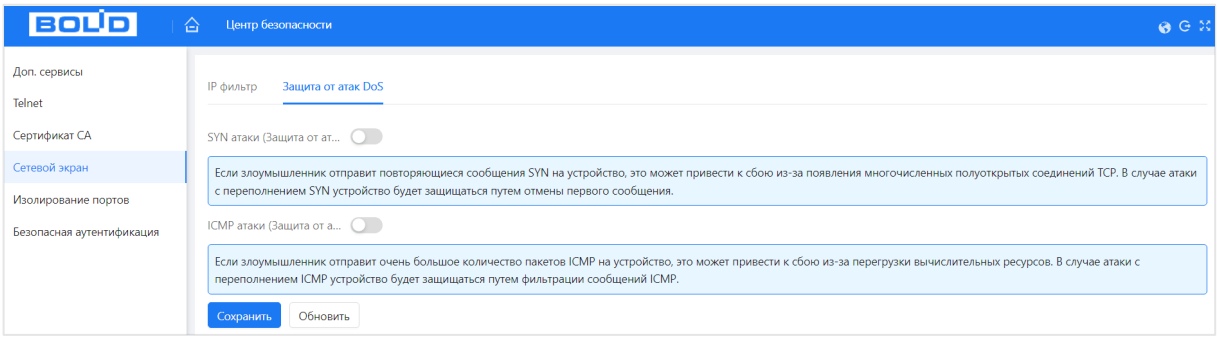


Рисунок 11.15 – Включение защиты от DoS-атак

11.5 Подраздел «Изолирование портов»

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

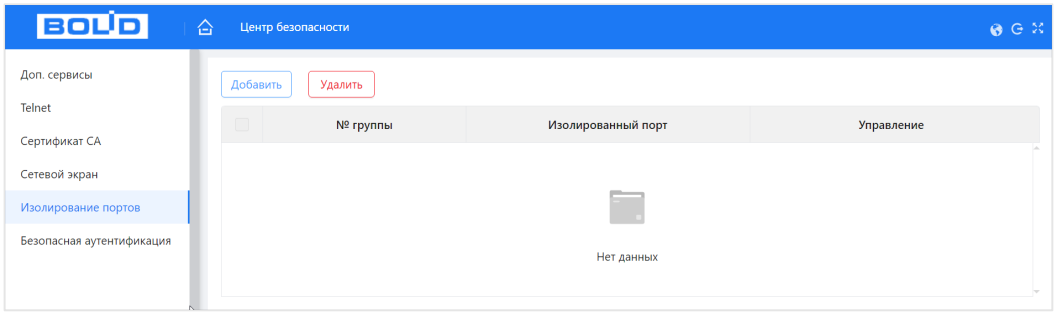


Рисунок 11.16 – Изолирование портов

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.

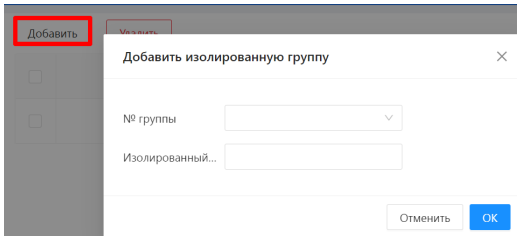


Рисунок 11.17 – Добавление группы

11.6 Подраздел «Безопасная аутентификация»

11.6.1 Пункт «Алгоритм проверки подлинности»

Выбор алгоритма дайджеста для аутентификации.

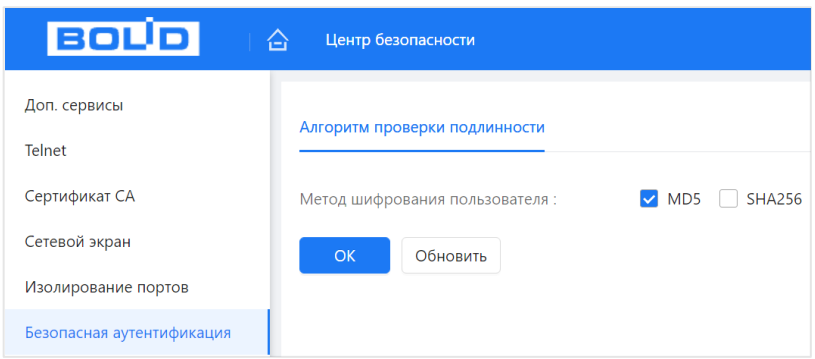


Рисунок 11.18 – Алгоритм проверки подлинности

12 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.

12.1 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 12.1 – 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.

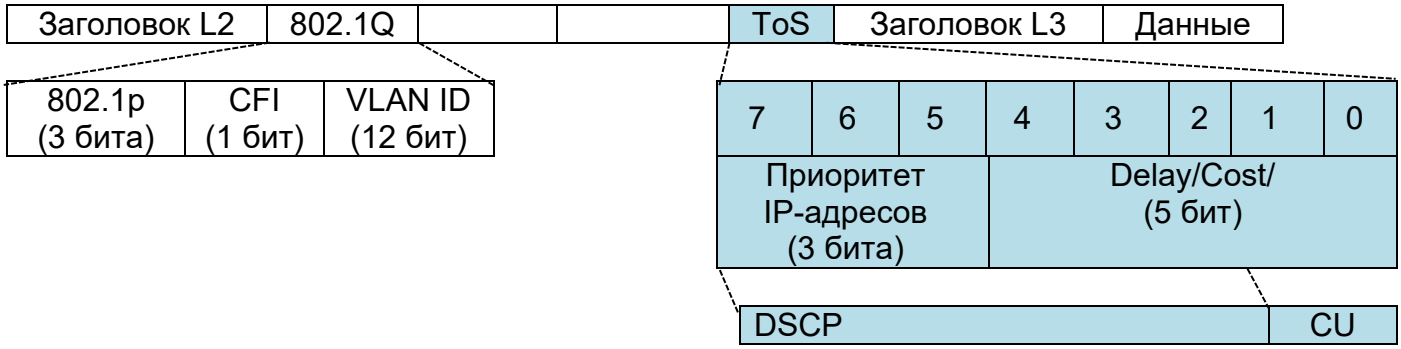


Таблица 12.2 – Привязка по умолчанию DSCP к CoS (приоритетам 802.1p)

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

12.1.1 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.

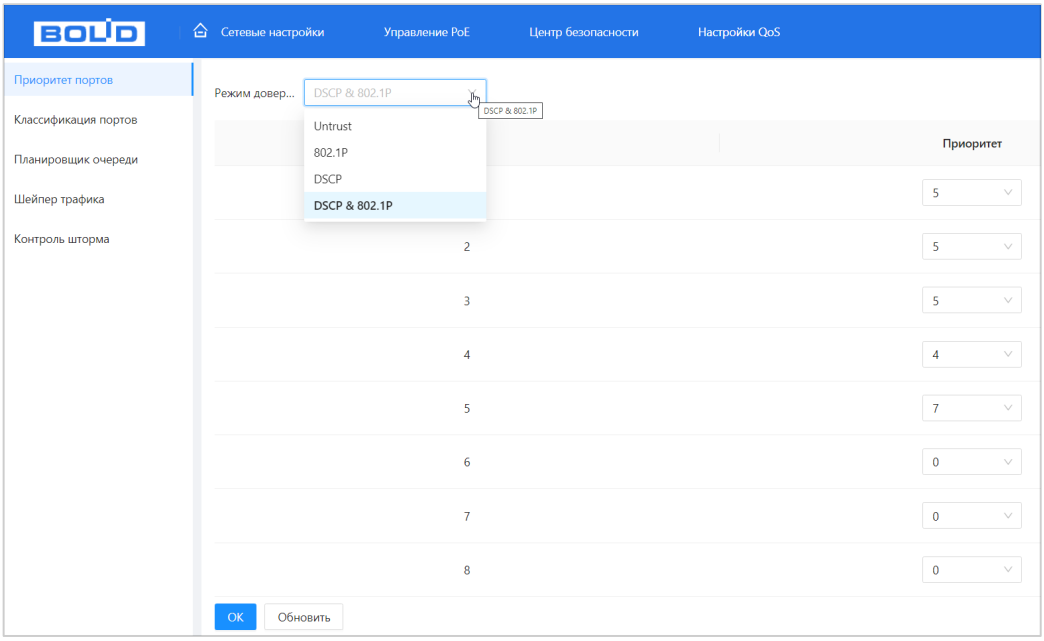


Рисунок 12.1 – Настройка приоритетности

12.2 Подраздел «ACL»

ACL (Access Control List, список контроля доступа) – механизм фильтрации IP-пакетов, позволяющий контролировать сетевой трафик, на аппаратном уровне разрешая или запрещая прохождение пакетов по определённым параметрам.

12.2.1 Пункт «Конфигурация ACL»

12.2.1.1 Вкладка «MAC ACL»

В данной вкладке настраивается фильтрация ACL на основе MAC-адресов.

Первым этапом создаём номер ACL с помощью кнопки «Добавить».

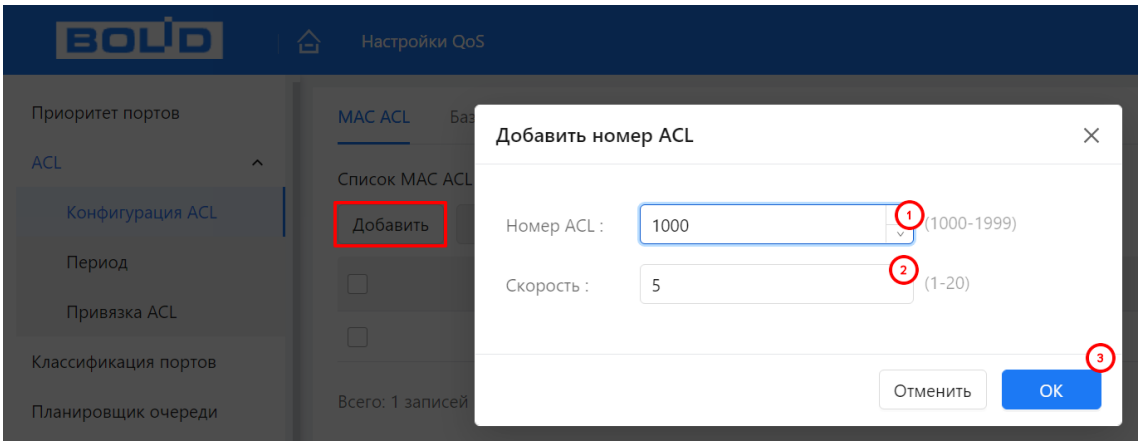


Рисунок 12.2 – Добавление номера ACL

Таблица 12.3 – Добавление номера ACL

Параметр	Функция
Номер ACL	Допустимый зарезервированный диапазон для MAC ACL от 1000 до 1999.
Скорость	Управляет шагом для автоматически назначаемых идентификаторов правил при добавлении новых правил. Это резервирует место для будущей вставки правил и упрощает управление.

После добавления переходим к созданию списка правил. Выделяем в общем списке номер ACL. И нажимаем кнопку «Добавить».

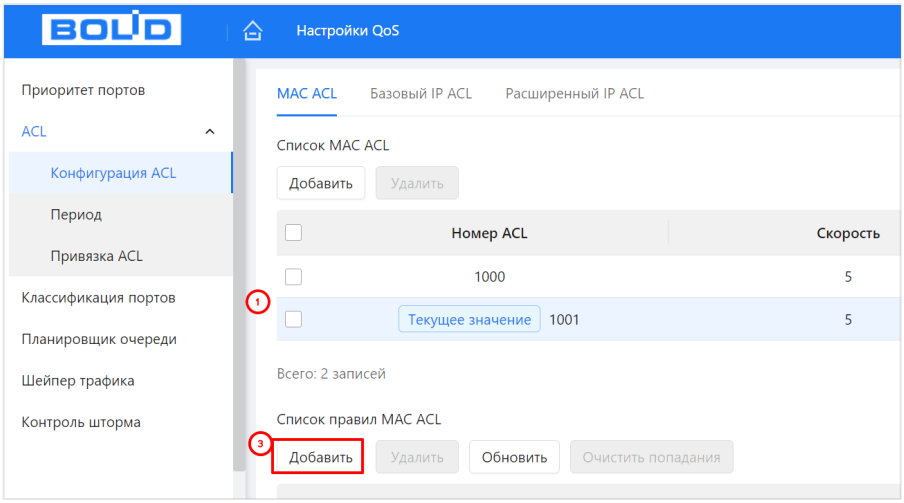


Рисунок 12.3 – Выбор номера MAC ACL

В появившемся окне переходим к заполнению параметров.

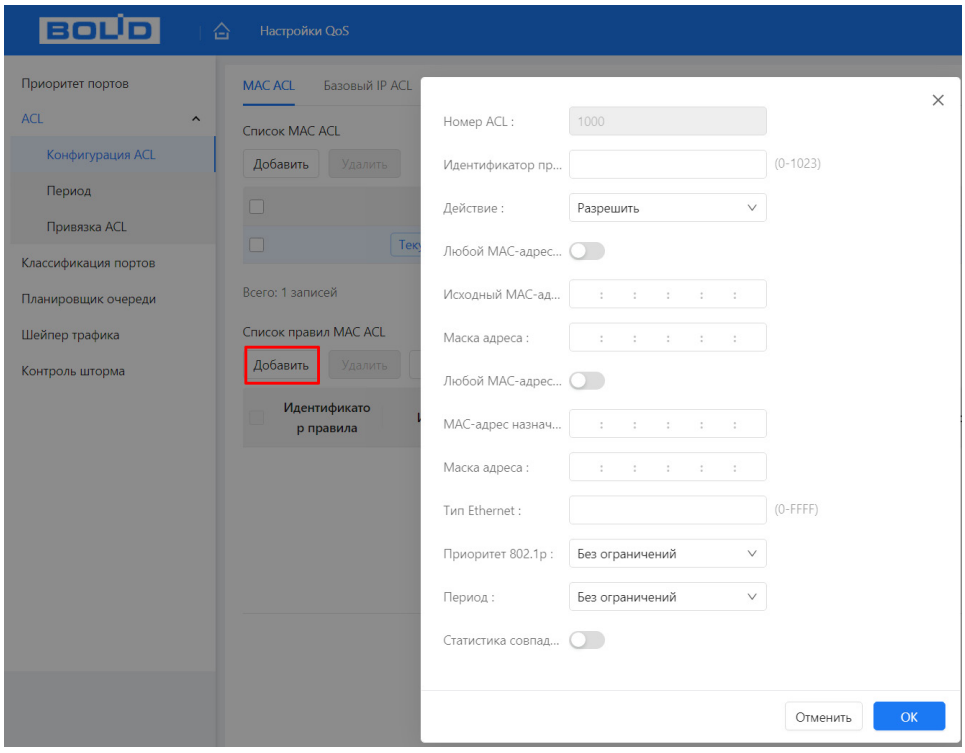


Рисунок 12.4 – Создание правил

Таблица 12.4 – Создание правил ACL

Параметр	Функция
Номер ACL	Фиксированное значение, выставляется при добавлении номера ACL.
Идентификатор правила	Устанавливается порядок следования правила ACL MAC для упрощения управления.
Действие	Выбор действия, которое будет происходить с пакетом во время пересылки: – Разрешить – разрешить доступ от источника к получателю; – Запретить – заблокировать доступ от источника к получателю.
Любой MAC-адрес источника	После активации переключателя, правило применяется к любому MAC-адресу источника. Если нет, то нужно заполнить параметры: «Исходный MAC-адрес» и «Маска адреса».
Исходный MAC-адрес	Введите MAC-адрес источника.
Маска адреса	Ввод маски.
Любой MAC-адрес места назначения	После активации переключателя, правило применяется к любому MAC-адресу назначения. Если нет, то нужно заполнить параметры: «MAC-адрес назначения» и «Маска адреса».
MAC-адрес назначения	Введите MAC-адрес назначения.
Маска адреса	Ввод маски.
Тип Ethernet	Устанавливается тип Ethernet используемый для идентификации протоколов. Диапазон от 0 до FFFF.
Приоритет 802.1p	Уровень приоритета 802.1p (от 0 до 7) для классификации трафика.
Период	Временной интервал, когда правило активно. Можно выбрать из предопределённых периодов или без ограничений.
Статистика совпадений	Если включено, устройство будет подсчитывать количество пакетов, подпадающих под это правило (счётчик совпадений).

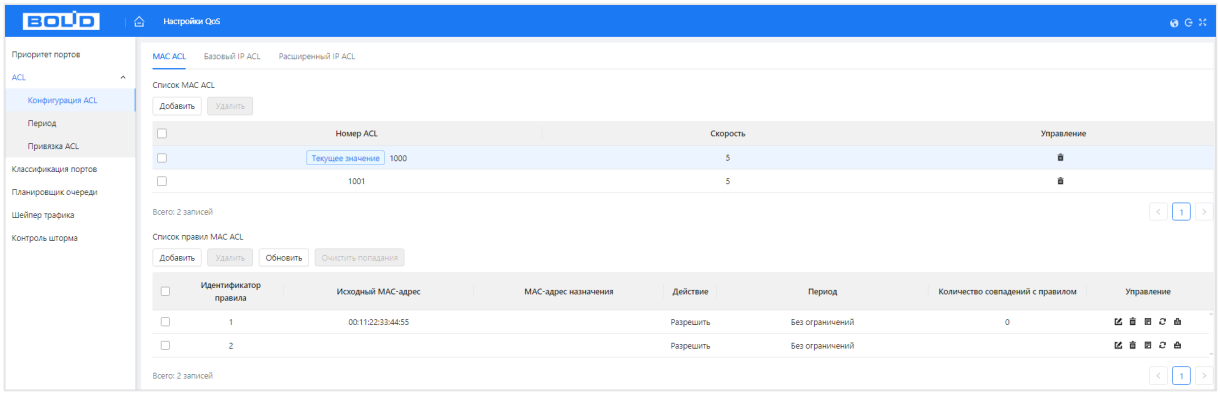


Рисунок 12.5 – Список MAC ACL правил

После создания правил MAC ACL доступны следующие действия:

– – внесение изменений в созданное правило;

– – удаление правила;

– – вызов панели с полной информацией о правиле;

– – обнуление количества пакетов, соответствующих данному правилу.

12.2.1.2 **Вкладка «Базовый IP ACL»**

В данной вкладке настраивается фильтрация ACL на основе IP-адресов.

Первым этапом создаём номер ACL с помощью кнопки «Добавить».

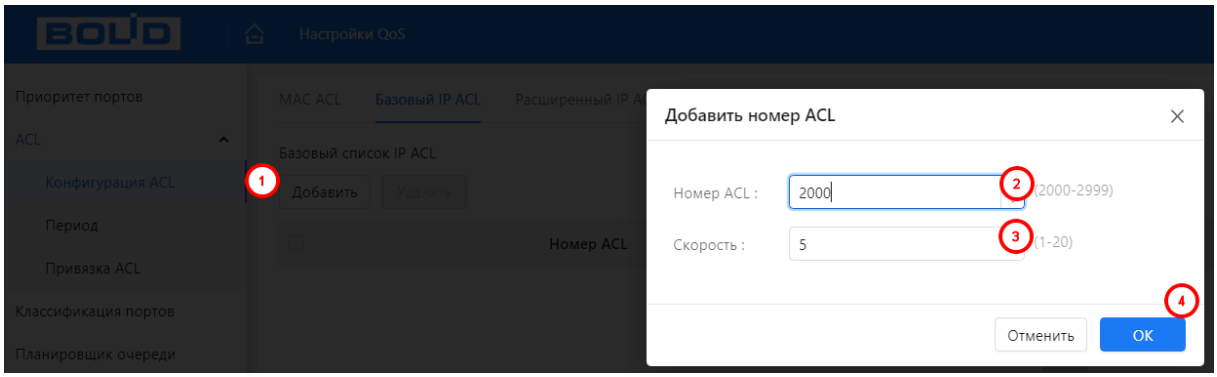


Рисунок 12.6 – Добавление номера IP ACL

Таблица 12.5 – Добавление номера IP ACL

Параметр	Функция
Номер ACL	Допустимый зарезервированный диапазон для IP ACL от 2000 до 2999.

Параметр	Функция
Скорость	Управляет шагом для автоматически назначаемых идентификаторов правил при добавлении новых правил. Это резервирует место для будущей вставки правил и упрощает управление.

После добавления переходим к созданию списка правил. Выделяем в общем списке номер IP ACL. И нажимаем кнопку «Добавить».

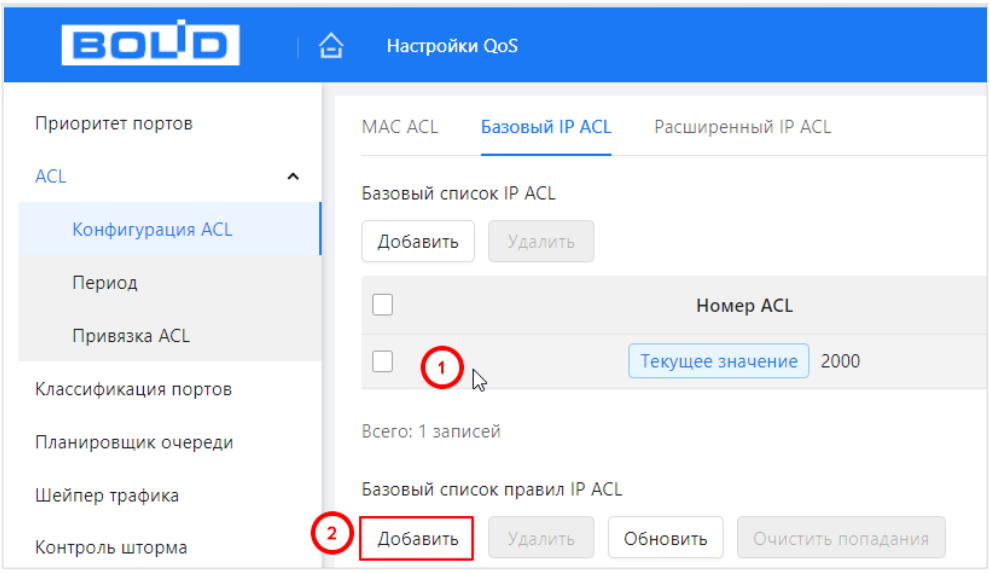


Рисунок 12.7 – Выбор номера MAC ACL

В появившемся окне переходим к заполнению параметров.

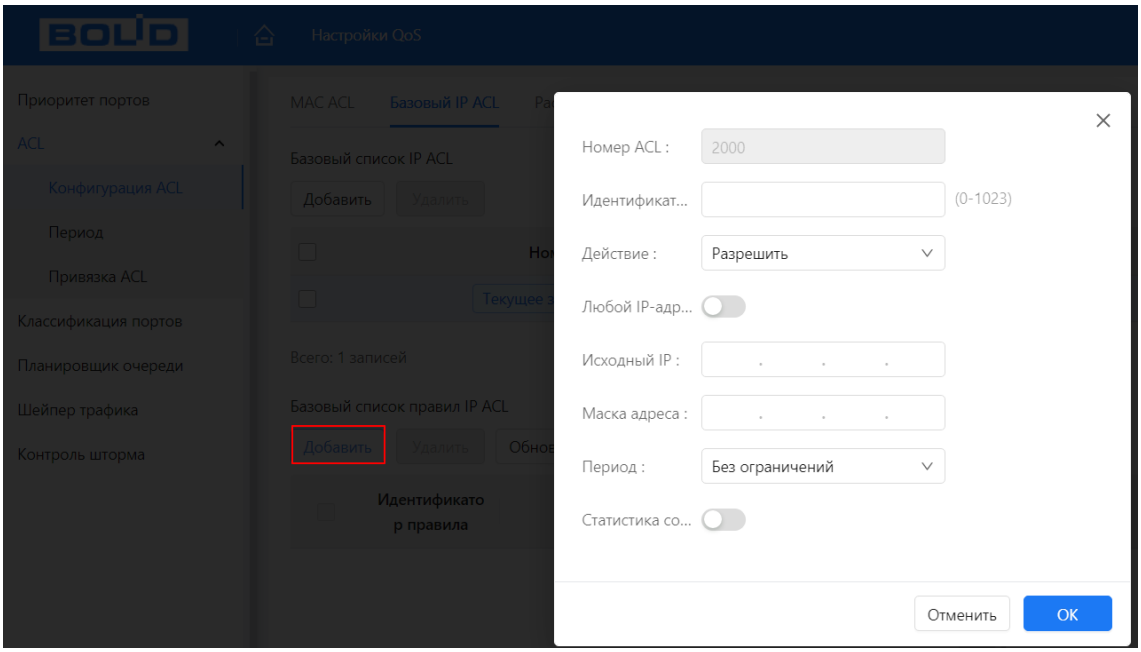


Рисунок 12.8 – Создание правил

Таблица 12.6 – Создание правил IP ACL

Параметр	Функция
Номер ACL	Фиксированное значение, выставляется при добавлении номера IP ACL.

Параметр	Функция
Идентификатор правила	Устанавливается порядок следования правила IP ACL для упрощения управления.
Действие	Выбор действия, которое будет происходить с пакетом во время пересылки: – Разрешить – разрешить доступ от источника к получателю; – Запретить – заблокировать доступ от источника к получателю.
Любой IP-адрес источника	После активации переключателя, правило применяется к любому IP-адресу источника. Если нет, то нужно заполнить параметры: «Исходный IP» и «Маска адреса».
Исходный IP	Введите MAC-адрес источника.
Маска адреса	Ввод маски.
Период	Временной интервал, когда правило активно. Можно выбрать из предопределённых периодов или без ограничений.
Статистика совпадений	Если включено, устройство будет подсчитывать количество пакетов, подпадающих под это правило (счётчик совпадений).

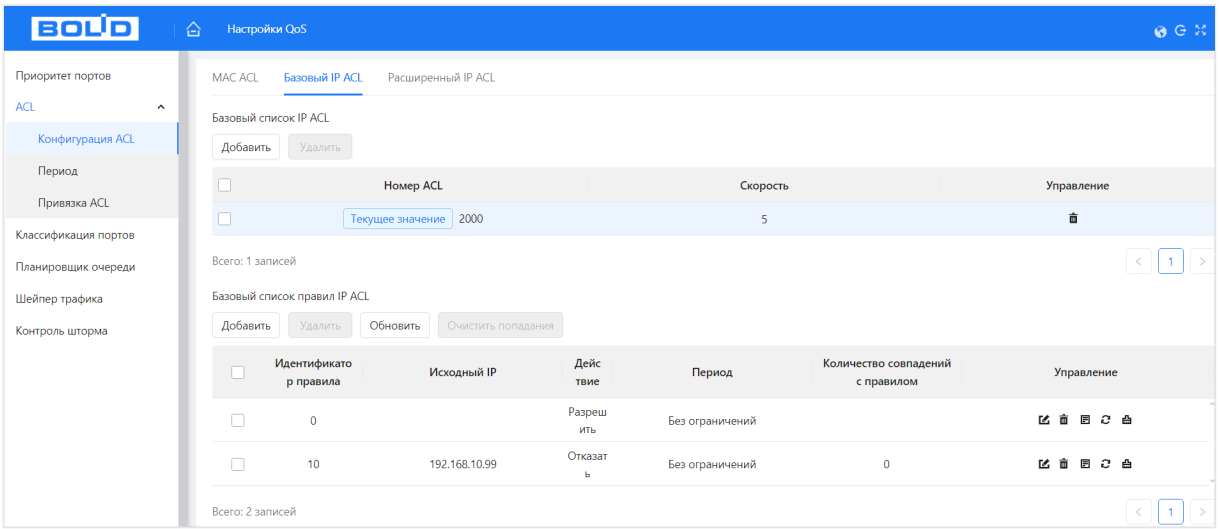


Рисунок 12.9 – Список IP ACL правил

После создания правил IP ACL доступны следующие действия:

– – внесение изменений в созданное правило;

– – удаление правила;

– – вызов панели с полной информацией о правиле;

– – обнуление количества пакетов, соответствующих данному правилу.

12.2.1.3 **Вкладка «Расширенный IP ACL»**

К настройкам фильтрации ACL на основе IP-адресов источника, добавляется расширение, что даёт гораздо более тонкую настройку, позволяя учитывать: IP-адрес источника, получателя, протоколы фильтрации и приоритет трафика.

Первым этапом создаём номер ACL с помощью кнопки «Добавить».

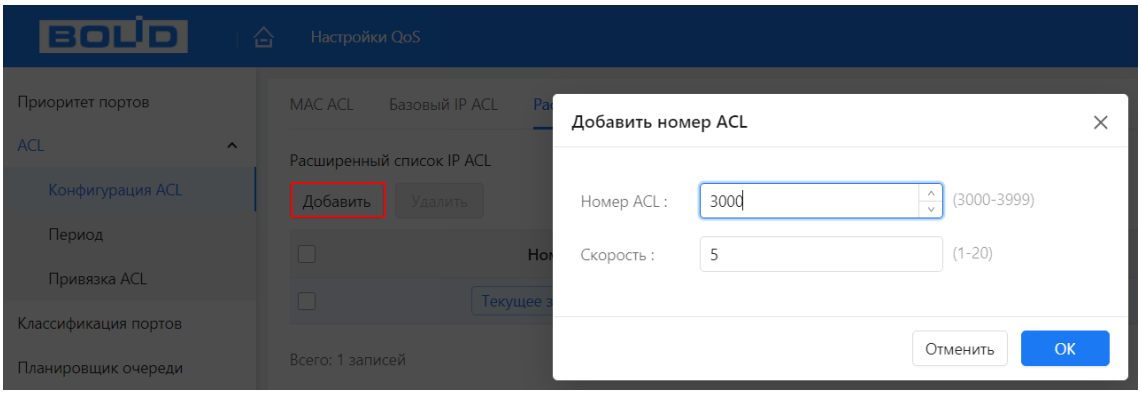


Рисунок 12.10 – Добавление номера IP ACL

Таблица 12.7 – Добавление номера IP ACL

Параметр	Функция
Номер ACL	Допустимый зарезервированный диапазон для IP ACL от 3000 до 3999.
Скорость	Управляет шагом для автоматически назначаемых идентификаторов правил при добавлении новых правил. Это резервирует место для будущей вставки правил и упрощает управление.

После добавления переходим к созданию списка правил. Выделяем в общем списке номер IP ACL. И нажимаем кнопку «Добавить».

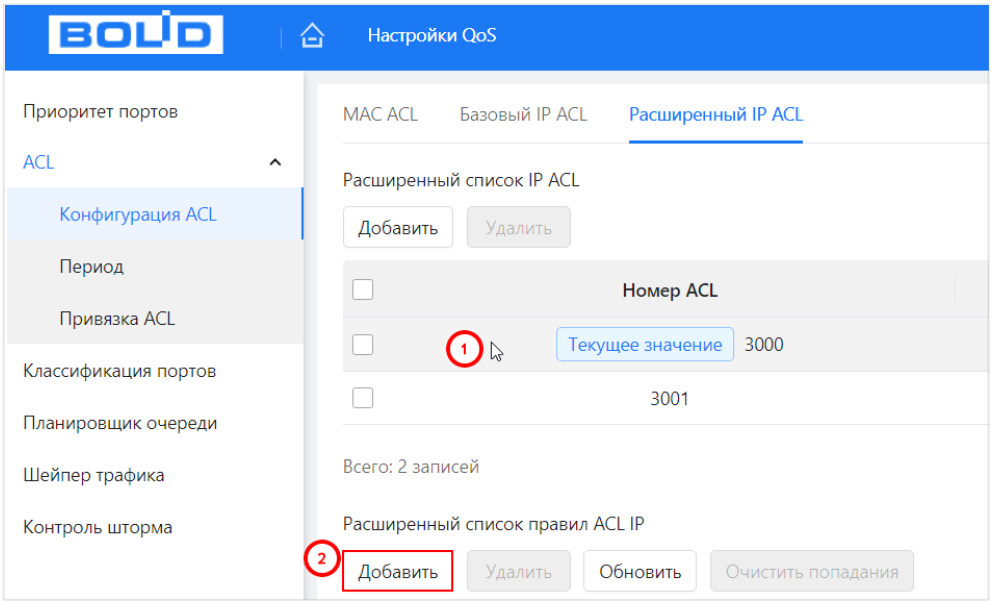


Рисунок 12.11 – Выбор номера MAC ACL

В появившемся окне переходим к заполнению параметров.

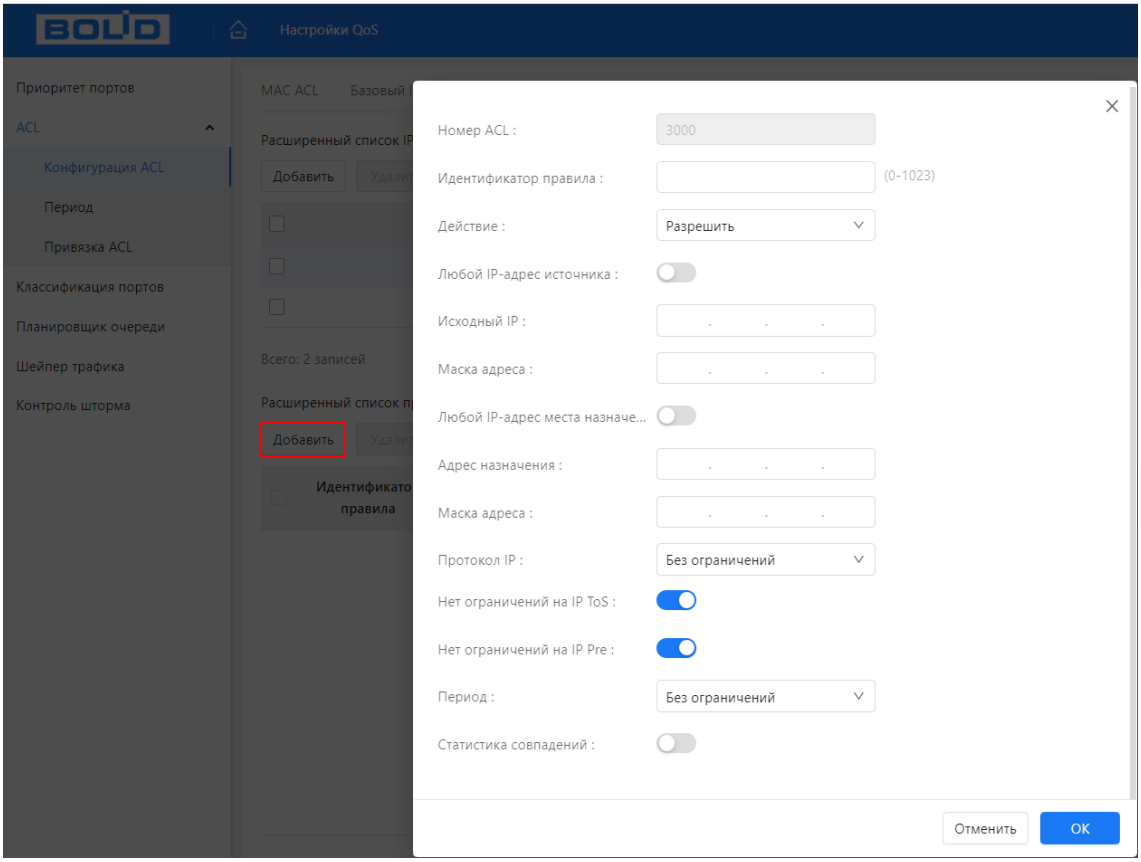


Рисунок 12.12 – Создание правил

Таблица 12.8 – Создание правил IP ACL

Параметр	Функция
Номер ACL	Фиксированное значение, выставляется при добавлении номера IP ACL.
Идентификатор правила	Устанавливается порядок следования правила IP ACL для упрощения управления.

Параметр	Функция
Действие	Выбор действия, которое будет происходить с пакетом во время пересылки: – Разрешить – разрешить доступ от источника к получателю; – Запретить – заблокировать доступ от источника к получателю.
Любой IP-адрес источника	После активации переключателя, правило применяется к любому IP-адресу источника. Если нет, то нужно заполнить параметры: «Исходный IP» и «Маска адреса».
Исходный IP	Введите MAC-адрес источника.
Маска адреса	Ввод маски.
Любой IP-адрес назначения	После активации переключателя, правило применяется к любому IP-адресу источника. Если нет, то нужно заполнить параметры: «Адрес назначения» и «Маска адреса».
Адрес назначения	Введите MAC-адрес назначения.
Маска адреса	Ввод маски.
Протокол IP	Выбор сетевого протокола из выпадающего списка, по умолчанию стоит параметр – «Любой». Доступен, например: TCP, UDP, ICMP, OSPF и т.д.
Нет ограничений на DSCP	Если переключатель активен – DSCP не учитывается. Если снят – нужно задать значение DSCP (0 – 63) для фильтрации. 
Нет ограничений на IP ToS	Если флажок установлен – поле Type of Service не учитывается. Если снят – нужно задать значение ToS (0–15). 

Параметр	Функция
Нет ограничений на IP Pre	Если флажок установлен – поле IP Precedence не учитывается. Если снят – нужно задать значение Pre (0–7). 
Период	Временной интервал, когда правило активно. Можно выбрать из предопределённых периодов или без ограничений.
Статистика совпадений	Если включено, устройство будет подсчитывать количество пакетов, подпадающих под это правило (счётчик совпадений).

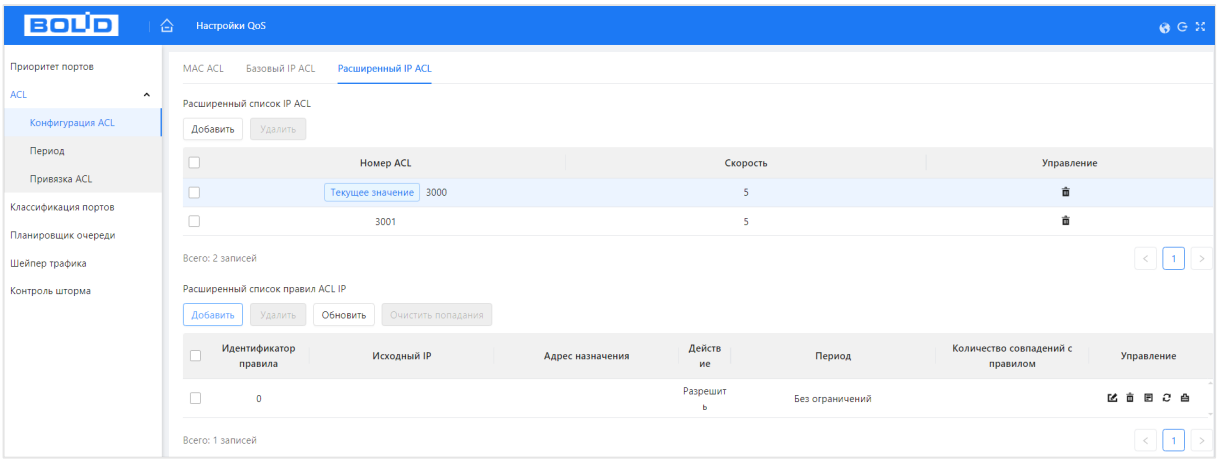


Рисунок 12.13 – Список IP ACL с расширенными правилами

После создания правил IP ACL доступны следующие действия:

– – внесение изменений в созданное правило;

– – удаление правила;

– – вызов панели с полной информацией о правиле;

– – обнуление количества пакетов, соответствующих данному правилу.

12.2.2 Пункт «Период»

Во вкладке производится настройка временного периода.

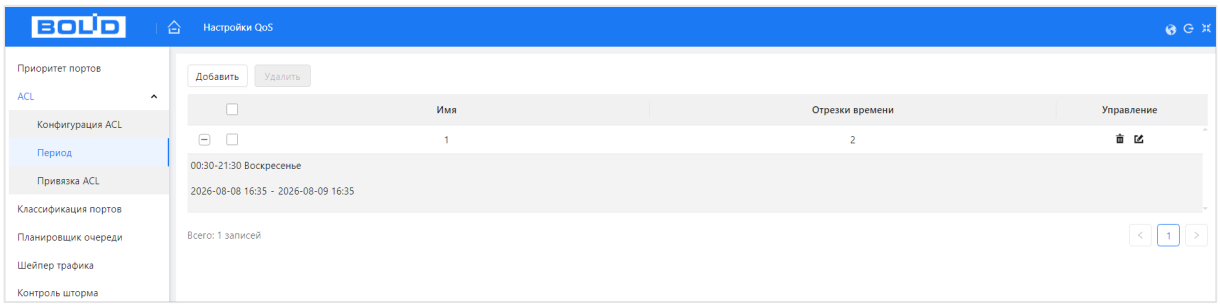


Рисунок 12.14 – Период

Для добавления временного периода нажмите кнопку «Добавить», задайте имя и выставите время.

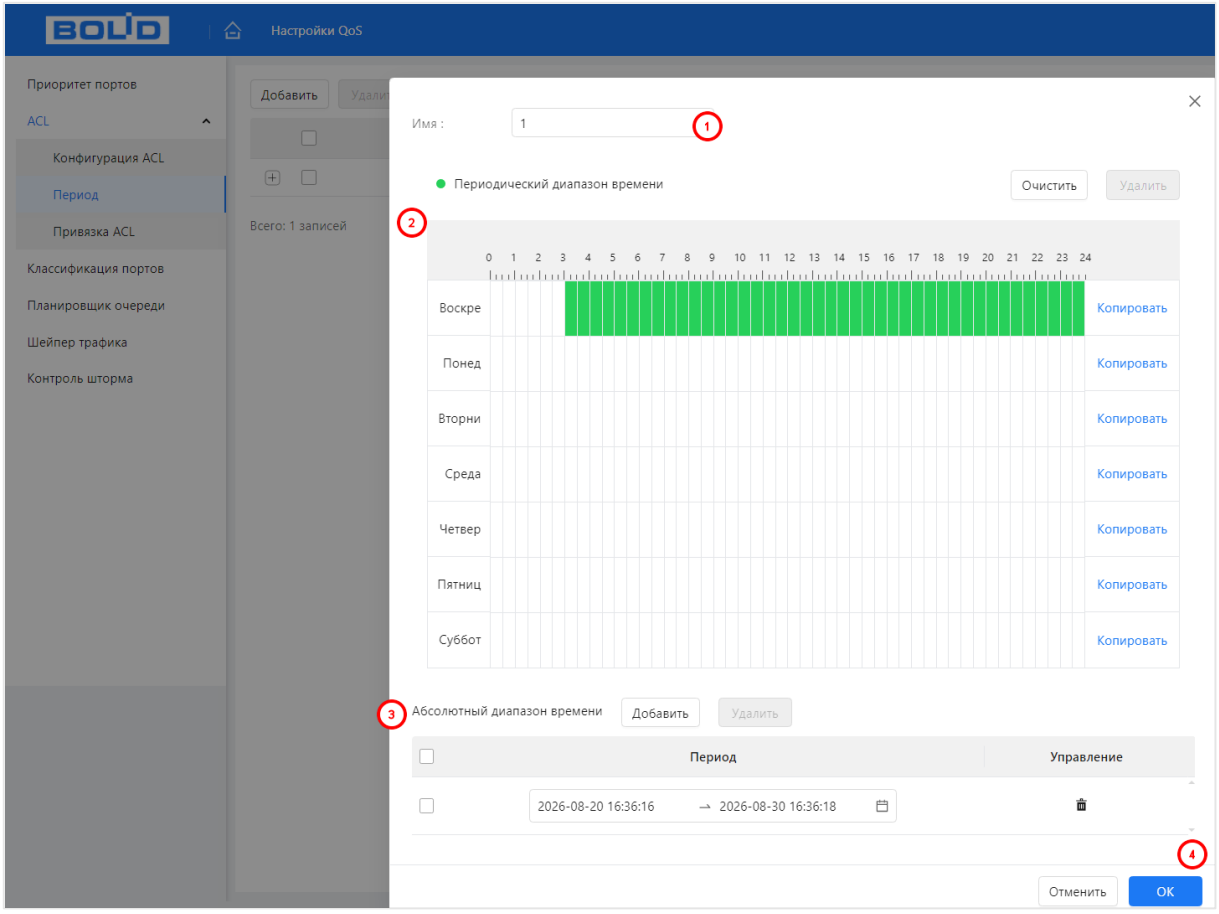


Рисунок 12.15 – Настройка расписания

12.2.3 Пункт «Привязка ACL»

Производится привязка настроенных правил: MAC ACL, стандартный IP ACL или расширенный IP ACL к определённому порту устройства. Для привязки:

1. Нажмите кнопку «Добавить».

2. Из выпадающего списка выберите номер списка.

3. На графической панели выделите порт, на который должен быть применён ACL.

4. Сохраните привязку.

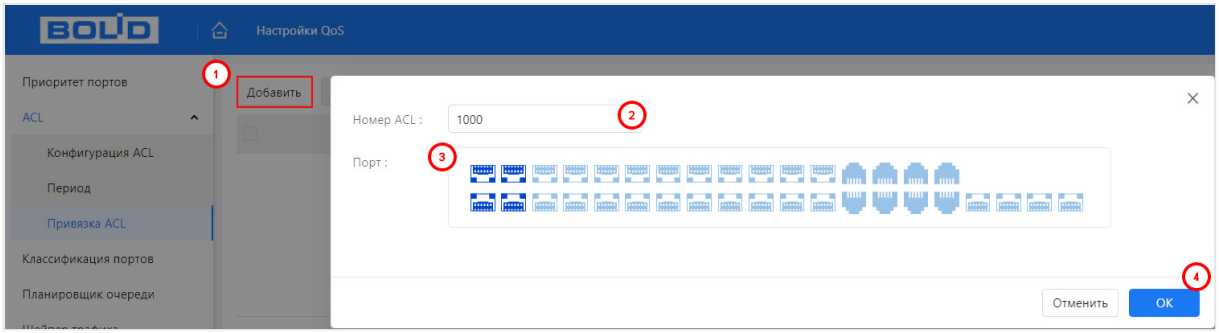


Рисунок 12.16 – Привязка правила к порту

12.3 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.

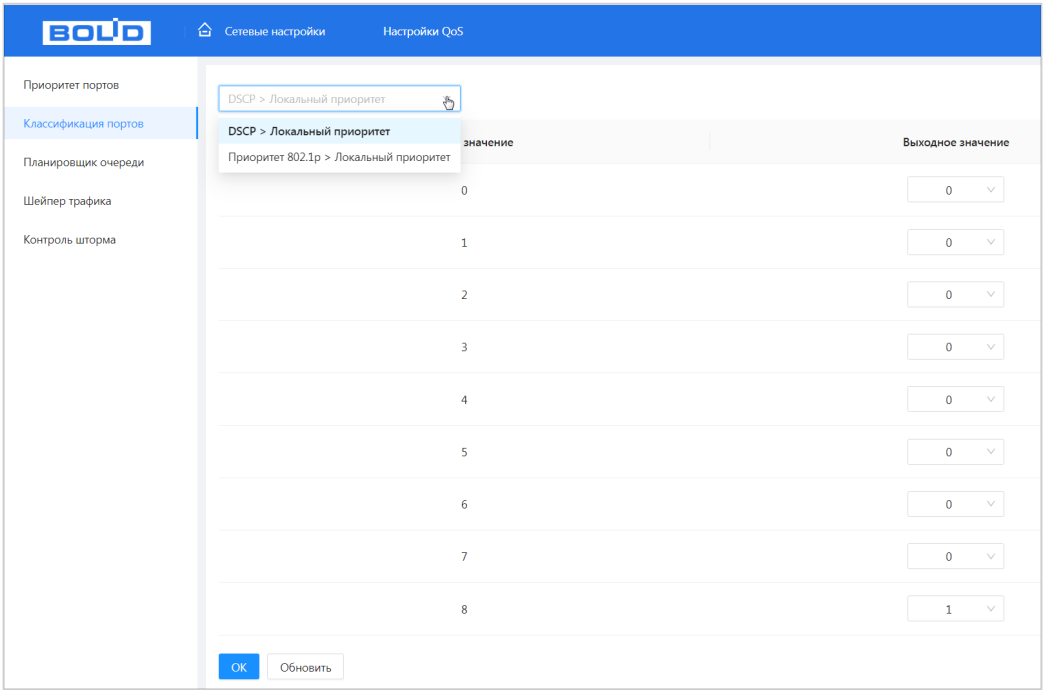


Рисунок 12.17 – Классификация портов

12.4 Подраздел «Планировщик очереди»

Настройки и просмотр информации о весе пакета в очереди.

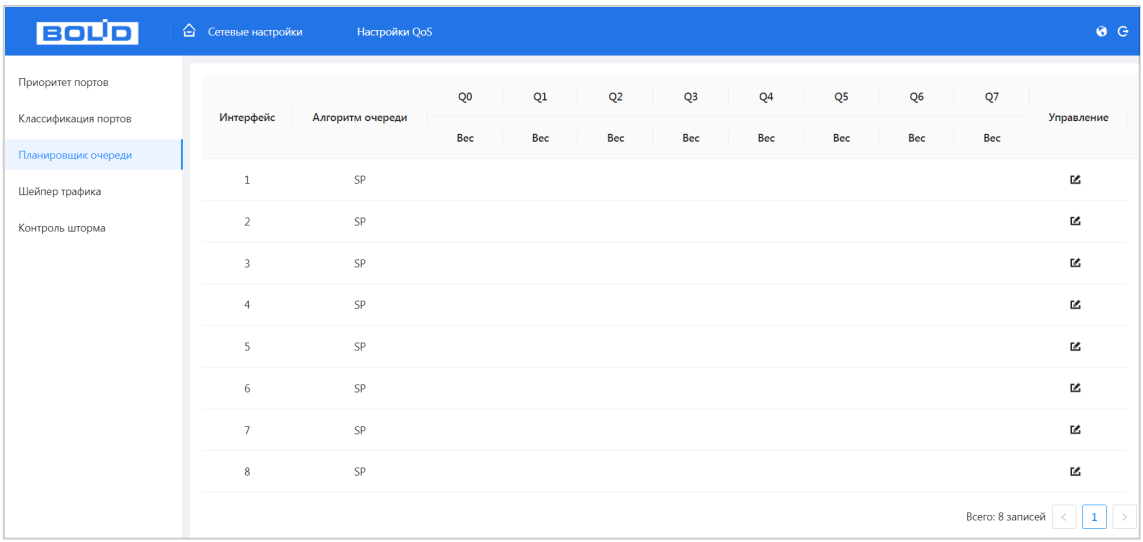


Рисунок 12.18 – Планировщик очереди

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

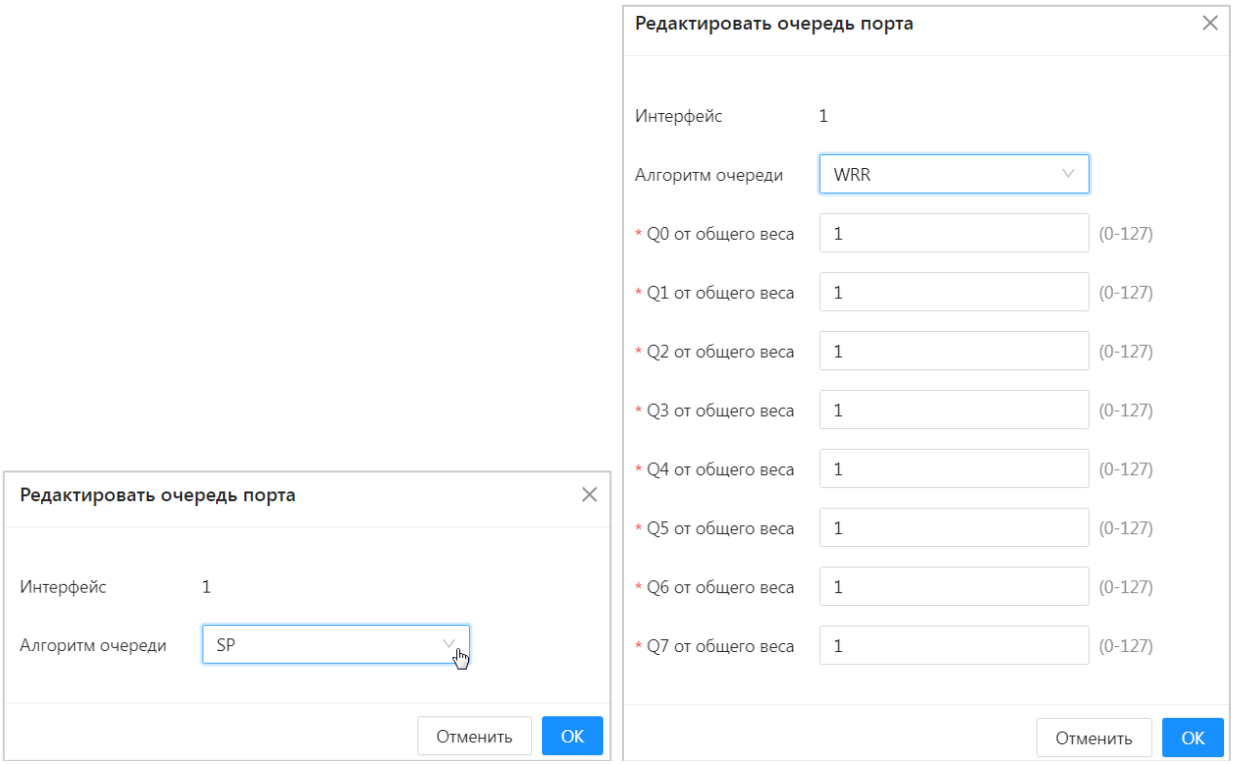


Рисунок 12.19 – Настройка очереди порта

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).

12.5 Подраздел «Шейпер трафика»

Настройки и просмотр информации о скорости передачи трафика.

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

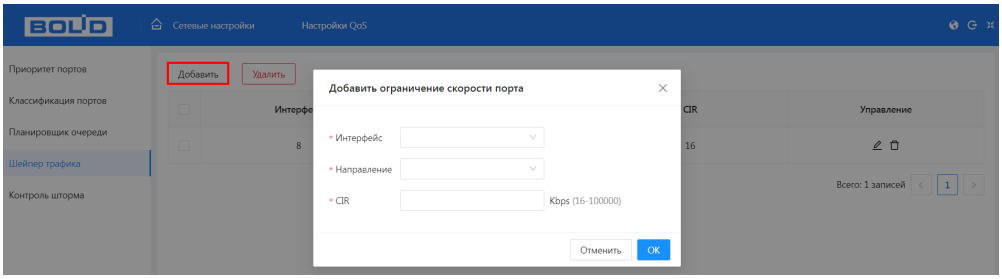


Рисунок 12.20 – Шейпер трафика

12.6 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.

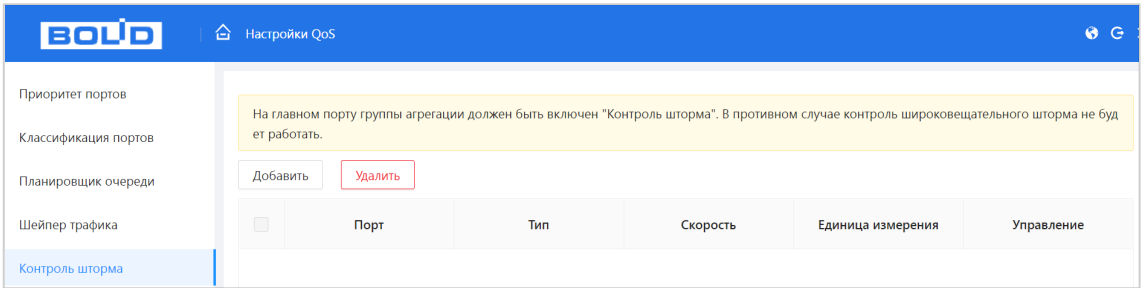


Рисунок 12.21 – Штормовой ограничитель

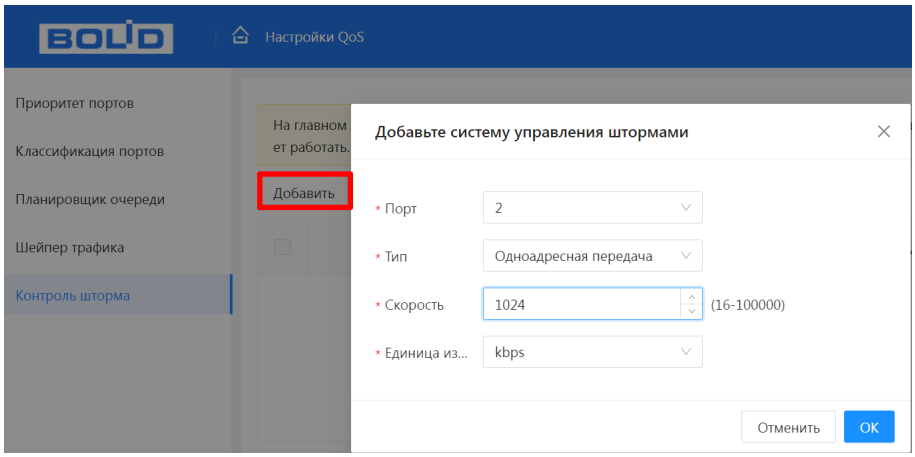


Рисунок 12.22 – Добавление и настройка

13 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.

13.1 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 13.1).

4. Настройте адрес сервера аутентификации, как показано на рисунке (см. Рисунок 13.2).

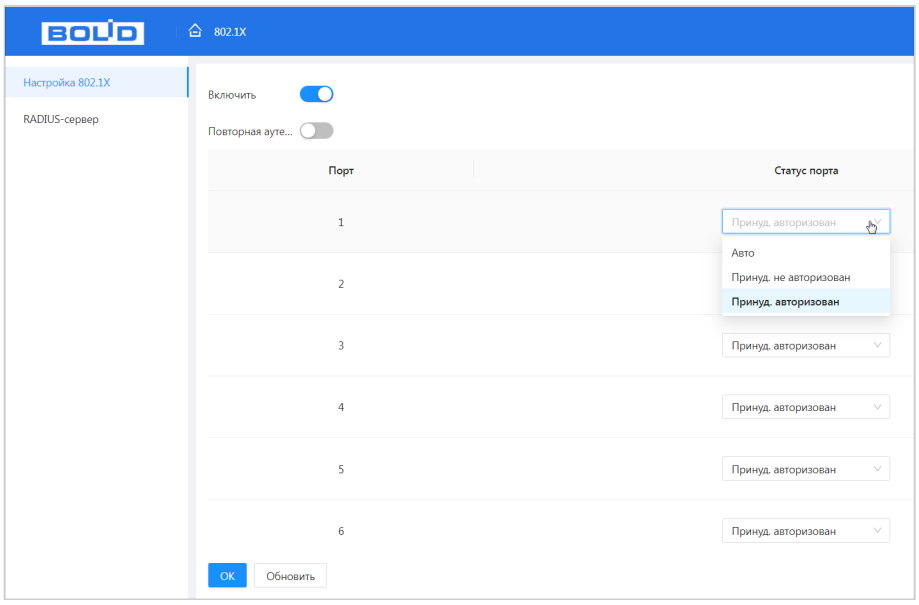


Рисунок 13.1 – Настройки NSA

13.2 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).

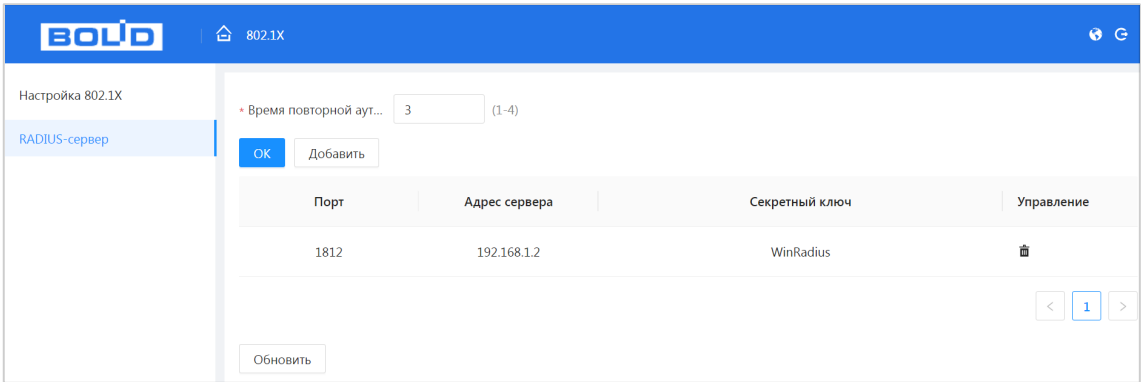


Рисунок 13.2 – Настройки Radius

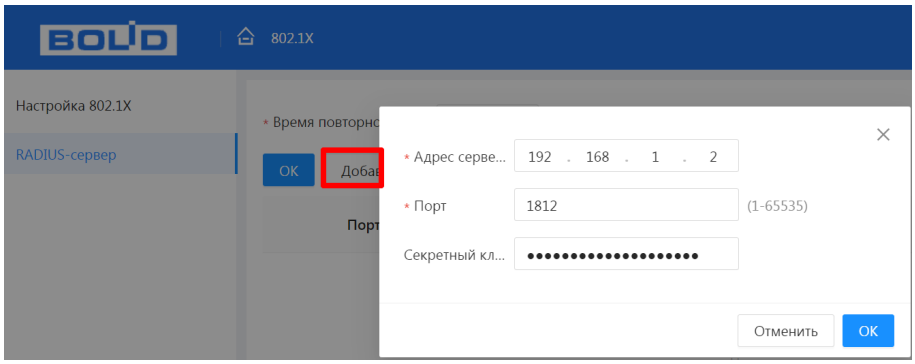


Рисунок 13.3 – Добавление

14 СБРОС НА ЗАВОДСКИЕ НАСТРОЙКИ

14.1 Сброс через веб-интерфейс

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

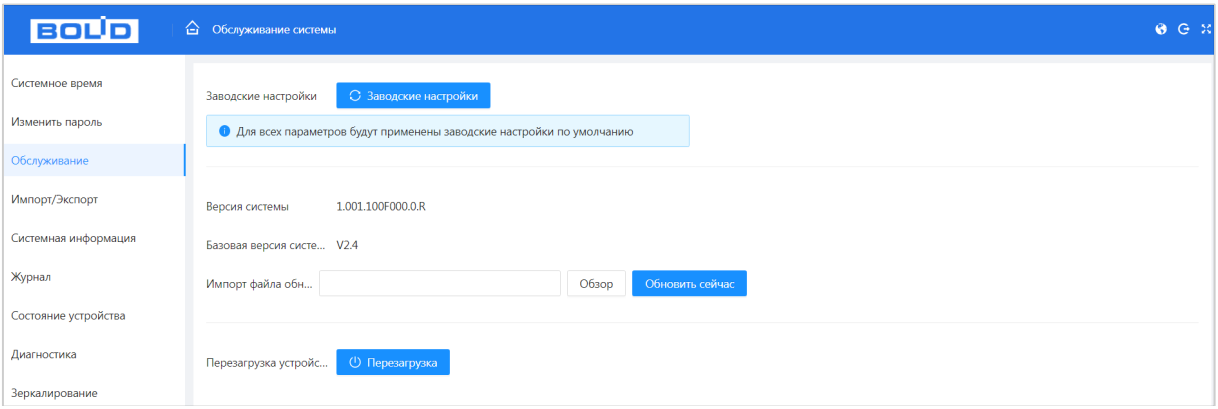


Рисунок 14.1 – Сброс на заводские настройки

2. Нажмите кнопку «Заводские настройки».

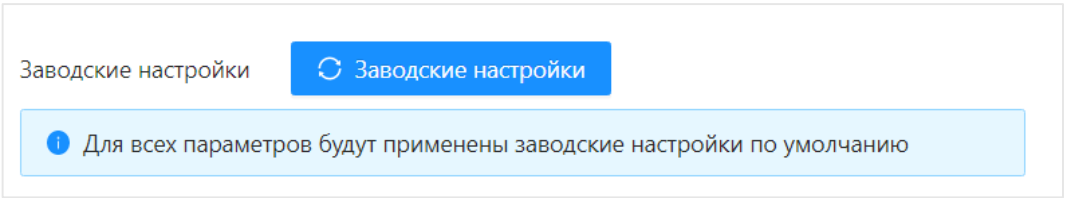


Рисунок 14.2 – Сброс на заводские настройки

3. Далее в появившемся окне введите пароль устройства.

4. Нажмите «ОК».

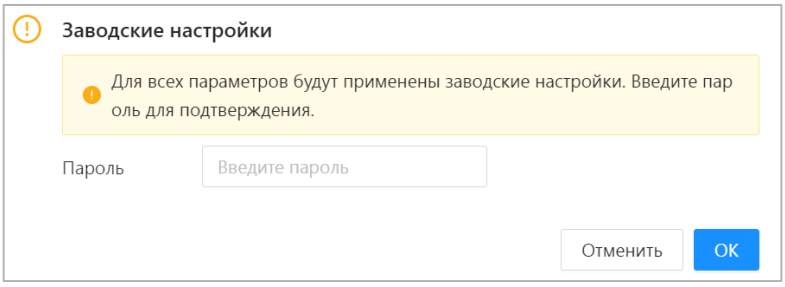


Рисунок 14.3 – Ввод пароля

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

14.2 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.

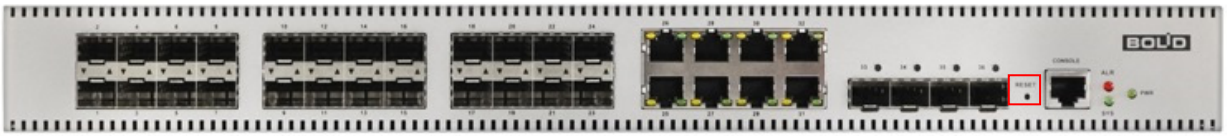


Рисунок 14.2 – Сброс на заводские настройки

В случае невозможности восстановления пароля администратора:

1. Подключите источник питания и дождитесь загрузки устройства.

2. Нажмите кнопку «RESET» и удерживайте её в течение 5 – 15 секунд до перезагрузки.

3. Отпустите кнопку «RESET».

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

15 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 для видеонаблюдения → 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.

СПРАВОЧНАЯ ИНФОРМАЦИЯ.
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 15.1) представлены базовые параметры для изменения.

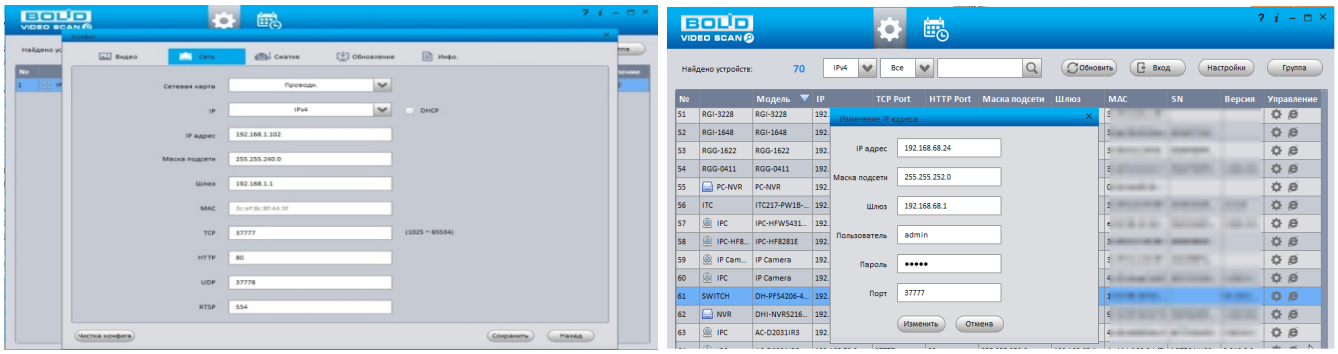


Рисунок 15.1 – Работа с BOLID VideoScan

16 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.

17 ВОЗМОЖНЫЕ НЕИСПРАВНОСТИ И СПОСОБЫ ИХ УСТРАНЕНИЯ

СПРАВОЧНАЯ ИНФОРМАЦИЯ.
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 17.1).

Таблица 17.1 – 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.

18 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.

19 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.

20 УПАКОВКА

Изделие и эксплуатационная документация упакованы в картонную коробку.

21 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.

22 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

23 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.

24 ГАРАНТИИ ИЗГОТОВИТЕЛЯ

Гарантийный срок эксплуатации – 36 месяцев с даты приобретения.

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

25 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.PA10.B.56907/26.

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.

26 СВЕДЕНИЯ О ПРИЁМКЕЕ

Изделие, коммутатор сетевой «BOLID SW-324» АЦДР.203729.006, 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 S FP-GSM-3SA	BOLID FP-GSM-3SB	BOLID SFP-XMM-1D
Форм-фактор	SFP	SFP	SFP	SFP	SFP+
Пропускная способность	1 Гбит/с	1 Гбит/с	1 Гбит/с	1 Гбит/с	10 Гбит/с
Длина кабеля	550 м	20 км	20 км	20 км	300 м
Кол-во используемых волокон	2	2	1	1	2
Тип разъёма	LC/UPC	LC/UPC	LC/UPC	LC/UPC	LC/UPC
Тип оптоволоконного кабеля	MM	SM	SM	SM	MM
Парность	Tx850/ Rx850	Tx1310/ Rx1310	Tx1310/ Rx1550	Tx1550/ Rx1310	Tx850/ Rx850
Напряжение питания	3,3 В	3,3 В	3,3 В	3,3 В	3,3 В
Диапазон рабочих температур	От -40 °C до +85 °C	От -40 °C до +85 °C	От -40 °C до +85 °C	От -40 °C до +85 °C	От -40 °C до +85 °C
Относительная влажность воздуха	От 5 % до 95 %	От 5 % до 95 %	От 5 % до 95 %	От 5 % до 95 %	От 5 % до 95 %
Габаритные размеры	55,5×13,4× 8,5 мм	55,5×13,4× 8,5 мм	55,5×13,4× 8,5 мм	55,5×13,4× 8,5 мм	55,5×13,4× 8,5 мм

Перечень терминов и сокращений

АРМ	Автоматизированное рабочее место – это рабочее место специалиста, оснащённое персональным компьютером, программным обеспечением и совокупностью информационных ресурсов индивидуального или коллективного пользования
Веб	Web (паутина) – сокращённое альтернативное название Всемирной Сети Интернет, являющей собой систему взаимосвязанных за счёт ссылок отдельных веб-страниц и других документов
ИМ	Инструкция по монтажу
ОС	Операционная система
ПО	Программное обеспечение
ПК	Персональный компьютер
Пул	Object pool – набор готовых к использованию объектов
РЭ	Руководство по эксплуатации
СКУД	Система контроля и управления доступом – это комплекс оборудования, главная функция которого – ограничение доступа на охраняемый объект. Элементы СКУД объединены в сеть, которая управляется с помощью специализированного программного оборудования
AC	Alternating Current – переменный ток
ARP	Address Resolution Protocol – Протокол определения адреса
ACL	Access Control List, список контроля доступа
CLI	Command Line Interface (интерфейс командной строки) – инструмент для работы пользователя с программой с помощью команд
DC	Direct Current – Постоянный ток
DHCP	Dynamic Host Configuration Protocol – Протокол динамического конфигурирование хоста. Обеспечивает получение сетевыми устройствами IP-адресов от сервера в локальной сети
DSCP	Differentiated Services Code Point (Точка кода дифференцированных услуг) – элемент архитектуры компьютерных сетей, описывающий простой масштабируемый механизм классификации, управления трафиком и обеспечения качества обслуживания

DNS	Domain Name System – Система доменных имён. Таблица перевода интернет имён в IP-адреса
Ethernet	Локальная сеть, используемая для подключения между собой компьютеров, принтеров, рабочих станций, терминалов и т.п. в настоящее время реализуется на базе кабелей типа «витая пара». Скорость передачи сигнала составляет от десятков до тысяч мегабит в секунду
ERPS	Ethernet Ring Protection Switching– сетевой протокол, использующийся для предотвращения образования петель в топологии типа «Кольцо» методом отключения порта
HTTP	HyperText Transfer Protocol – протокол передачи гипертекстовых документов
HTTPS	HyperText Transfer Protocol Secure – Расширение протокол передачи гипертекстовых документов для поддержки шифрования в целях повышения безопасности
ID	Identifier – идентификатор
IGMP	Internet Group Management Protocol (Протокол управления группами Интернета) – протокол управления групповой (multicast) передачей данных в сетях, основанных на протоколе IP. IGMP используется маршрутизаторами и IP-узлами для организации сетевых устройств в группы
IP	Internet Protocol – межсетевой протокол
IPv4	Internet Protocol version 4 – четвертая версия интернет протокола. Широко используемый тип IP-адреса, состоящий из 4 байт (32 бит)
IPV6	Internet Protocol version 6 – шестая версия интернет протокола. Новая система адресации, в которой адрес состоит из 16 Б (128 бит)
LAN	Local Area Network/Локальная вычислительная сеть
LACP	Link Aggregation Control Protocol – протокол, предназначенный для объединения нескольких физических каналов в один логический в сетях Ethernet
LLDP	Link Layer Discovery Protocol – протокол канального уровня, позволяющий сетевому оборудованию оповещать оборудование, работающее в локальной сети, о своем существовании и передавать ему свои характеристики, а также получать от него аналогичные сведения
MAC	Media Access Control – уникальный идентификатор, присваиваемый сетевым адаптерам. Играет роль физического адреса сетевого адаптера

MSTP	Multiple Spanning Tree Protocol (IEEE 802.1s)
Multicast	Передача пакетов с одного узла сети на специфическую группу IP-адресов, принадлежащих разным получателям данных
MEP	Maintenance Entity Point – является частью ERPS
PoE	Power over Ethernet – стандарты IEEE 802.3af, IEEE 802.3at, позволяющие передавать по сети Ethernet не только данные, но и электрический ток
PQ	Priority queuing – схема управления программными очередями в компьютерных сетях, при которой планировщик обслуживает очереди с более высоким приоритетом в ущерб низко-приоритетным очередям
QoS	Quality of Service – качество обслуживания. Набор технологий, обеспечивающих приоритетное использование канала связи
RADIUS	Remote Authentication in Dial-In User Service – протокол для реализации аутентификации, авторизации и сбора сведений об использованных ресурсах, разработанный для передачи сведений между центральной платформой и оборудованием
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
RS-232	Recommended Standard 232/Electronic Industries Alliance-232 (EIA232) – Рекомендуемый стандарт 232. Интерфейс (набор разъёмов, кабелей) для последовательной передачи данных
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
RPL	Ring Protection Link — это канал защиты кольца, который блокируется в состоянии простоя. Используется, чтобы предотвратить образование петли в мостовом кольце ERPS
SFP	Small Form-factor Pluggable – промышленный стандарт модульных компактных приёмопередатчиков (трансиверов), используемых для передачи и приёма 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 приёмопередатчика 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
SSH	Secure Shell – безопасная оболочка. Сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений. Позволяет безопасно передавать в незащищённой среде практически любой другой сетевой протокол
STP	Spanning Tree Protocol – сетевой протокол (или семейство сетевых протоколов) предназначенный для автоматического удаления циклов (петель коммутации) из топологии сети на канальном уровне в Ethernet-сетях
TELNET	Teletype Network – сетевой протокол для реализации текстового терминального интерфейса по сети (в современной форме — при помощи транспорта TCP). Название «telnet» имеют также некоторые утилиты, реализующие клиентскую часть протокола
TCP	Transmission Control Protocol – Протокол управления передачей
UDP	User Datagram Protocol – Пользовательский протокол передачи. Протокол передачи данных, не требующий подтверждения приёма пакетов
VLAN	Virtual Local Area Network – виртуальная локальная компьютерная сеть
WFQ	Weighted fair queuing (Взвешенная справедливая очередь) – механизм планирования пакетных потоков данных с различными приоритетами
8P8C	8 Position 8 Contact – унифицированный разъём, используемый в телекоммуникации. Имеет 8 контактов и фиксатор

Перечень рисунков

Рисунок 1.1 – Сетевое соединение 7
Рисунок 1.2 – Кольцевое соединение 8
Рисунок 1.3 – Звезда 8
Рисунок 4.1 – Передняя панель 13
Рисунок 4.2 – Штекер 14
Рисунок 4.3 – Подключения кабеля 15
Рисунок 4.4 – Задняя панель 15
Рисунок 4.5 – Задняя панель 16
Рисунок 5.1 – Габаритные размеры 19
Рисунок 5.2 – Монтаж коммутатора в 19”-стойку 20
Рисунок 6.1 – Инициализация 21
Рисунок 6.2 – Инициализация 21
Рисунок 6.3 – Инициализация 22
Рисунок 6.4 – Вход 22
Рисунок 6.5 – Настройка/синхронизация времени 23
Рисунок 6.6 – Сетевые настройки 23
Рисунок 7.1 – Главное меню 25
Рисунок 8.1 – Сетевые параметры устройства 29
Рисунок 8.2 – Информационная панель 30
Рисунок 8.3 – Графическая панель 30
Рисунок 8.4 – Графическая панель 30
Рисунок 8.5 – Текстовая информационная панель 31
Рисунок 8.6 – Список найденных устройств 32
Рисунок 9.1 – Настройка/синхронизация времени 33
Рисунок 9.2 – Сихронизация с NTP-сервером 34
Рисунок 9.3 – Изменение пароля 35
Рисунок 9.4 – Подраздел «Обслуживание» 35
Рисунок 9.5 – Сброс 36
Рисунок 9.6 – Обновление 36
Рисунок 9.7 – Перезагрузка устройства 36
Рисунок 9.8 – Экспорт 37
Рисунок 9.9 – Экспорт настроек с устройства 37
Рисунок 9.10 – Экспорт 37
Рисунок 9.11 – Системная информация 38
Рисунок 9.12 – Интерфейс просмотра журнала 39
Рисунок 9.13 – Состояние устройства 39
Рисунок 9.14 – Диагностика 40
Рисунок 9.15 – Результат 40
Рисунок 9.16 – Зеркалирование 41
Рисунок 9.17 – Добавление 41
Рисунок 10.1 – Настройка портов 43
Рисунок 10.2 – Редактирование портов 43
Рисунок 10.3 – Подробная информация о порту 45

Рисунок 10.4 – Конфигурация EEE 46
Рисунок 10.5 – Создание VLAN 47
Рисунок 10.6 – Создание VLAN 47
Рисунок 10.7 – Конфигурирование VLAN-порта 48
Рисунок 10.8 – VLAN интерфейс 49
Рисунок 10.9 – Добавление 49
Рисунок 10.10 – Настройки маршрутизации 50
Рисунок 10.11 – Таблица маршрутизации 51
Рисунок 10.12 – ARP-таблица 51
Рисунок 10.13 – Быстрая настройка ERPS 53
Рисунок 10.14 – Информация 53
Рисунок 10.15 – Редактирование ERPS экземпляра 53
Рисунок 10.16 – Тест 55
Рисунок 10.17 – Добавление ERPS 55
Рисунок 10.18 – Настройка экземпляра ERPS 56
Рисунок 10.19 – Добавление MEP 61
Рисунок 10.20 – Конфигурация MEP 62
Рисунок 10.21 – Интерфейс IGMP Snooping 65
Рисунок 10.22 – Настройка STP 65
Рисунок 10.23 – Настройка STP 66
Рисунок 10.24 – Агрегация каналов 68
Рисунок 10.25 – Добавление 71
Рисунок 10.26 – Добавление 71
Рисунок 10.27 – Настройки SNMP 72
Рисунок 10.28 – Настройки SNMPv3 73
Рисунок 10.29 – MAC информация об адресах 75
Рисунок 10.30 – Фильтрация портов 76
Рисунок 10.31 – Обнаружение по LLDP 76
Рисунок 10.32 – Обнаружение петель (Loopback Detection) 77
Рисунок 10.33 – Настройка DHCP-сервера 78
Рисунок 10.34 – Добавить пул 78
Рисунок 10.35 – Добавление зарезервированных IP-адресов 79
Рисунок 10.36 – Статическая привязка 80
Рисунок 10.37 – Добавление в список 80
Рисунок 10.38 – Список адресов 81
Рисунок 10.39 – Глобальные настройки DHCP Snooping 82
Рисунок 10.40 – Настройка портов 83
Рисунок 10.41 – Конфигурация опции 82 83
Рисунок 10.42 – Тестирование виртуального канала 84
Рисунок 10.43 – Тестирование виртуального канала 85
Рисунок 11.1 – Системное обслуживание 86
Рисунок 11.2 – HTTPS 87
Рисунок 11.3 – Telnet 88
Рисунок 11.4 – Сертификат устройства 89
Рисунок 11.5 – Создание самоподписанного сертификата 89
Рисунок 11.6 – Создание и импорт доверенного сертификата 90

Рисунок 11.7 – Импорт стороннего сертификата 90
Рисунок 11.8 – Установка доверенного сертификата 91
Рисунок 11.9 – Фильтрация по IP.....91
Рисунок 11.10 – Добавить.....92
Рисунок 11.11 – Добавить IP-адрес.....92
Рисунок 11.12 – Добавить диапазон IP 92
Рисунок 11.13 – Добавить MAC-адрес.....93
Рисунок 11.14 – Добавить все IP-адреса.....93
Рисунок 11.15 – Включение защиты от DoS-атак.....93
Рисунок 11.16 – Изолирование портов 94
Рисунок 11.17 – Добавление группы 94
Рисунок 11.18 – Алгоритм проверки подлинности 94
Рисунок 12.1 – Настройка приоритетности 98
Рисунок 12.2 – Добавление номера ACL.....98
Рисунок 12.3 – Выбор номера MAC ACL 99
Рисунок 12.4 – Создание правил.....99
Рисунок 12.5 – Список MAC ACL правил.....101
Рисунок 12.6 – Добавление номера IP ACL 101
Рисунок 12.7 – Выбор номера MAC ACL 102
Рисунок 12.8 – Создание правил.....102
Рисунок 12.9 – Список IP ACL правил.....103
Рисунок 12.10 – Добавление номера IP ACL 104
Рисунок 12.11 – Выбор номера MAC ACL 105
Рисунок 12.12 – Создание правил.....105
Рисунок 12.13 – Список IP ACL с расширенными правилами 107
Рисунок 12.14 – Период 108
Рисунок 12.15 – Настройка расписания.....108
Рисунок 12.16 – Привязка правила к порту 109
Рисунок 12.17 – Классификация портов.....109
Рисунок 12.18 – Планировщик очереди.....110
Рисунок 12.19 – Настройка очереди порта.....110
Рисунок 12.20 – Шейпер трафика.....111
Рисунок 12.21 – Штормовой ограничитель 112
Рисунок 12.22 – Добавление и настройка 112
Рисунок 13.1 – Настройки NSA 114
Рисунок 13.2 – Настройки Radius 115
Рисунок 13.3 – Добавление 115
Рисунок 14.1 – Сброс на заводские настройки 116
Рисунок 14.2 – Сброс на заводские настройки 116
Рисунок 14.3 – Ввод пароля 116
Рисунок 15.1 – Работа с BOLID VideoScan.....118

Перечень таблиц

Таблица 2.1 – Технические характеристики* 9
Таблица 3.1 – Комплект поставки* 12
Таблица 4.1 – Порты и индикаторы передней панели 13
Таблица 6.1 – Параметры сетевых настроек коммутатора 24
Таблица 7.1 – Структура меню 25
Таблица 7.2 – Функционал главного меню 28
Таблица 8.1 – Параметры сетевых настроек коммутатора 29
Таблица 8.2 – Текстовая информация о порте 31
Таблица 10.1 – Настройка конфигурации портов 44
Таблица 10.2 – Данные списка VLAN 47
Таблица 10.3 – Конфигурирование VLAN-порта 48
Таблица 10.4 – Настройка маршрутизации на устройстве. Добавление IP 49
Таблица 10.5 – Настройка маршрутизации на устройстве. Добавление маршрута 50
Таблица 10.6 – Параметры редактирования ERPS 54
Таблица 10.7 – Параметры добавления ERPS 55
Таблица 10.8 – Параметры конфигурации ERPS 57
Таблица 10.9 – Параметры добавление MEP 61
Таблица 10.10 – Параметры настройки MEP 62
Таблица 10.11 – Параметры настройки STP 66
Таблица 10.12 – Параметры настройки STP 67
Таблица 10.13 – Типы алгоритма балансировки нагрузки 69
Таблица 10.14 – Поля настроек 73
Таблица 10.15 – Добавляемые параметры при добавлении пула 79
Таблица 10.16 – Статическая привязка 80
Таблица 10.17 – Параметры включения «опции 82» 83
Таблица 11.1 – Параметры системного обслуживания 86
Таблица 12.1 – Восемь классов приоритета трафика (стандарт IEEE 802.1p) 96
Таблица 12.2 – Привязка по умолчанию DSCP к CoS (приоритетам 802.1p) 97
Таблица 12.3 – Добавление номера ACL 99
Таблица 12.4 – Создание правил ACL 100
Таблица 12.5 – Добавление номера IP ACL 101
Таблица 12.6 – Создание правил IP ACL 102
Таблица 12.7 – Добавление номера IP ACL 104
Таблица 12.8 – Создание правил IP ACL 105
Таблица 17.1 – Перечень возможных неисправностей 120

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	–	–	–	–	104	328390			08.08. 2024
1	2, 8, 85, 92, 93, 103, 104	2, 8, 85, 92, 93 103, 104	–	–	104	580790			01.07. 2025
2	92	92	–	–	104	599434			20.01. 2026
3	1 – 138	1 – 138	104 – 139	–	139	615051			18.08. 2026
4	7,8, 11,13, 128, 139	7,8, 11,13, 128, 139	139 – 140	–	140	623401			17.11. 2026



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