Сетевой коммутатор

BOLID SW-324

Версия 1

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.

ВНИМАНИЕ!

- Руководство по эксплуатации содержит только справочную информацию, необходимую для использования его технических возможностей.
- Руководство по эксплуатации описывает интерфейс и функциональные возможности внутреннего ПО – 1.001.100F002.0.R (сборка от 13.05.2020).
- Дизайн изделия, технические характеристики и ПО, упомянутые в данном руководстве, подлежат изменению без обязательного предварительного письменного уведомления.
- В случае нахождения неточностей или несоответствий, обращайтесь в службу поддержки.

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ

1. Управляемый сетевой коммутатор с поддержкой функций L2+ предназначен для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети.

2. Не поддерживает технологию PoE.

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.

2 ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

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

Таблица 2.1 – Основные технические характеристики*

Наименование параметра	Значение параметра
Сетевые интерфейсы	
Общее количество	36 интерфейсов
RJ-45	Порт № 25 – 32: 10/100/1000 Base-T
SFP	Порт № 1 − 24: 100/1000 Base-X (SFP)
SFP+	Порт № 33 – 36: 1000/10 000 10GBase (SFP+)
Оборудование	
Порты RJ-45	8 портов
Порты SFP	24 порта
Порты SFP+	4 порта
Электропитание (переменный ток)	
Напряжение питания устройства	100 − 240 В переменного тока
Потребляемый ток	1 А
Потребляемая мощность	15 Вт в дежурном режиме 100 Вт при полной нагрузке
Производительность	
Уровень	L2+
Тип	Управляемый
Время технической готовности прибора к работе	50 с
Коммутационная матрица	221 Gbps
Скорость перенаправления пакетов	107 Mpps
Буфер пакетов	32 МБ
Таблица MAC адресов	32 К
Статическая таблица MAC- адресов	256
Число VLAN	4 К

Наименование параметра	Значение параметра
Поддерживаемые стандарты	IEEE 802.3, IEEE 802.3u, IEEE 802.3x, IEEE 802.3ab, IEEE 802.3z, IEEE 802.3ad, IEEE 802.3ae
IP интерфейсы	128
Маршруты IPv4	128 статических маршрутов
Функции	
ARP	1 К
Таблица MAC-адресов	Поддержка статического MAC-адреса
Spanning Tree Protocol	STP, RSTP, MSTP и ERPS
VLAN	802.1Q
Управление потоками	Поддержка управления потоком на основе IEEE802.3X
Агрегирование (объединение) каналов	LACP, статическое агрегирование
Зеркалирование портов	1:1 (Один к одному), N:1 (Много к одному)
Multicast	IGMP Snooping
DHCP	DHCP-сервер, DHCP-клиент
Безопасность	IEEE802.1x, поддержка ACL и защиты от петель
QoS	QoS на основе COS, 8 очередей на порт, шейпирование на порту, QoS на основе DSCP
Системное обслуживание	Загрузка и выгрузка файла настроек, обновление прошивки, системный журнал
Управление устройством	Веб-интерфейс, TELNET, CLI, SNMP V1/V2C/V3
Поддерживает модули следующих типов	1.25 G 850 nm, 2 нм, LC, Multi-mode 1.25 G 1310/1550 нм, 20 км, LC, Single-mode 1.25 G 1550/1310 нм, 20 км, LC, Single-mode 10 G 1330/1270 нм, 20 км, LC, Single-mode 10 G 1270/1330 нм, 20 км, LC, Single-mode 10 G 850 нм, 300 м, LC, Multi-mode

Наименование параметра		Значение параметра
Общие сведения		
Порт управления		1 порт (RS-232)
Предельное напряжение импульсных помех		2 кВ/1 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 10 % до 90 %
Диапазон рабочих температур		От -10 °С до +55 °С
Габаритные размеры		360×440×43,6 мм
Масса		Вес нетто: 3,60 кг Вес брутто: 4,75 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 Р 30805.22.

3 КОМПЛЕКТНОСТЬ

Состав изделия при поставке (комплект поставки коммутатора) представлен ниже (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	1 шт.
	Консольный кабель	1 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).

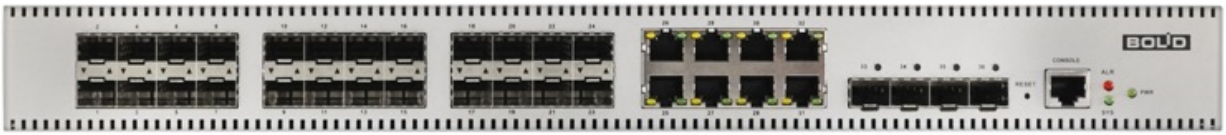


Рисунок 4.1 – Передняя панель

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 «Заводские настройки».
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.

4.2 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 разъём питания с поддержкой 100 – 240 В переменного тока.

Рисунок 4.2 – Задняя панель

5 МОНТАЖ И ДЕМОНТАЖ

5.1 Меры безопасности

ВНИМАНИЕ!
Монтаж производить только при отключенном напряжении питания.

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

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

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

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

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

5. При монтаже провода электропитания и выходов следует оставить достаточное пространство для 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).

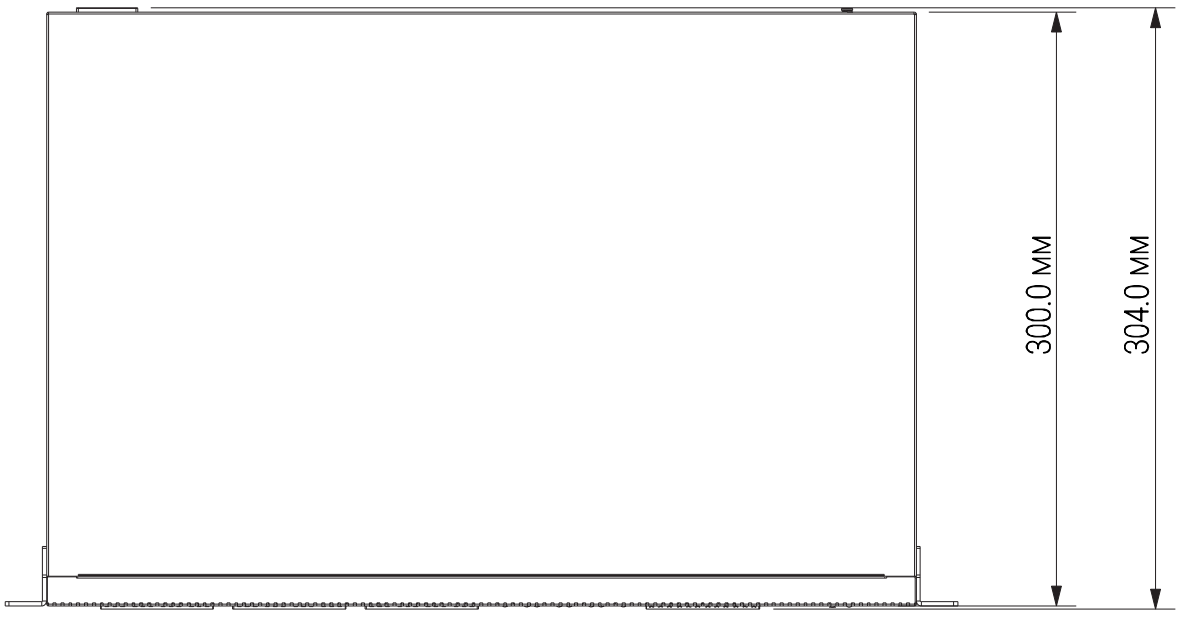


Рисунок 5.1 – Габаритные размеры

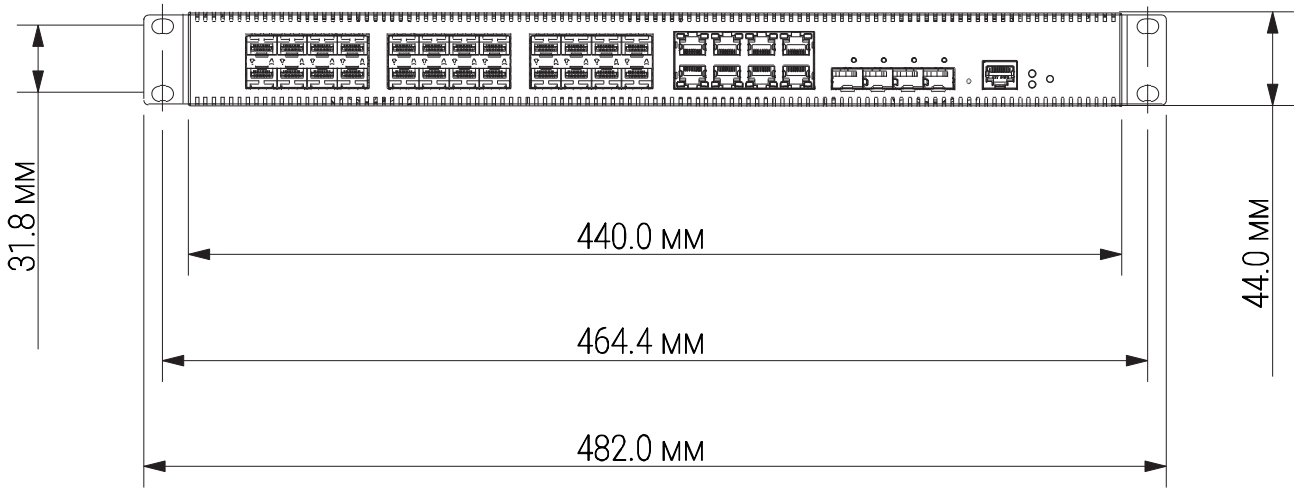


Рисунок 5.2 – Габаритные размеры

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.

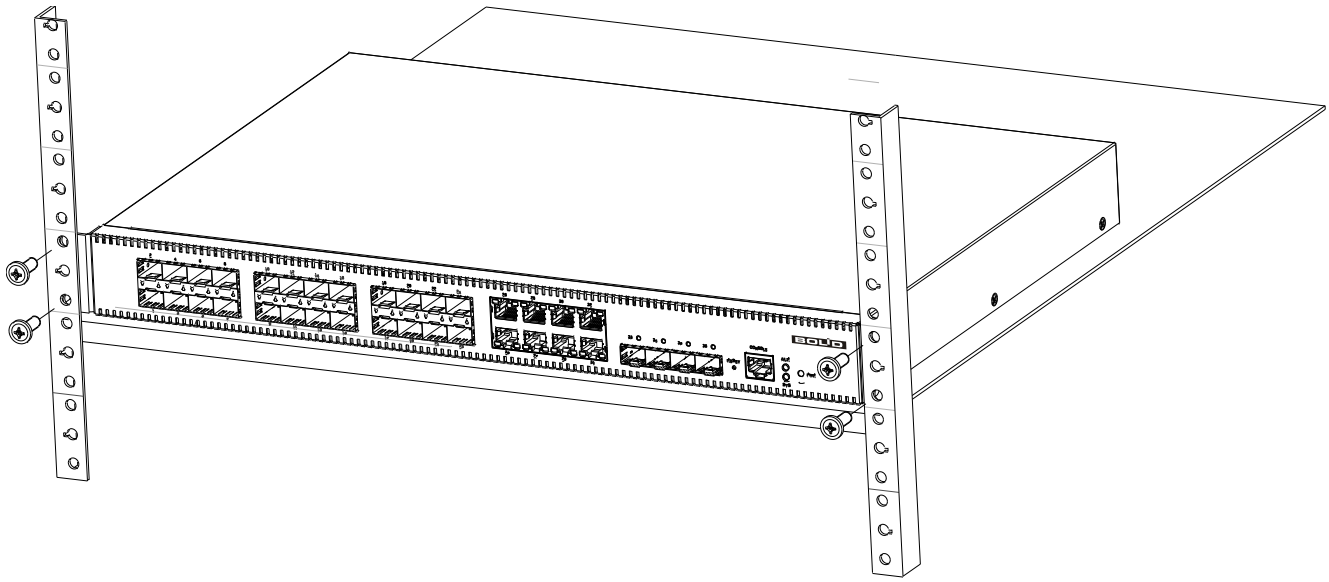


Рисунок 5.3 – Монтаж коммутатора в 19”-стойку

5.2.2 RJ-45

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

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

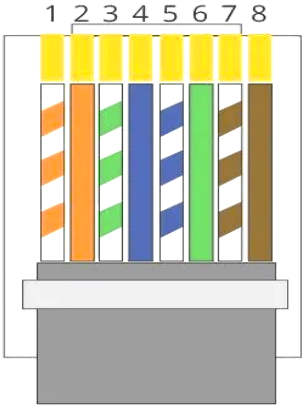


Рисунок 5.4 – Штекер 8P8C

Распиновка кабеля

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

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

5.2.3 Установка SFP и 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.

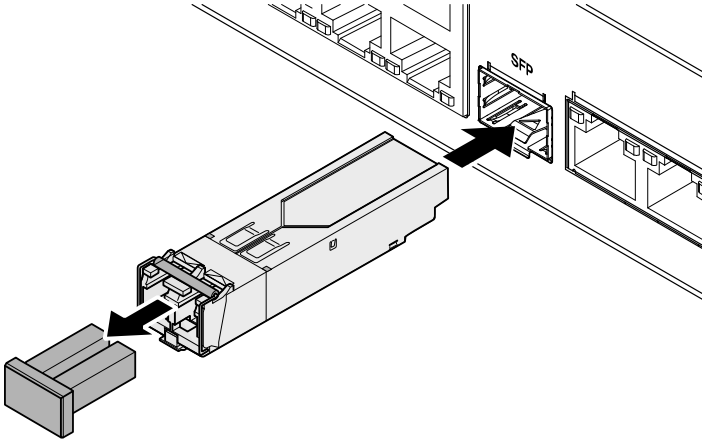


Рисунок 5.5 – Подключения

5.3 Демонтаж

Демонтаж изделия производится в обратном порядке при отключенном напряжении питания.

6 ИНИЦИАЛИЗАЦИЯ УСТРОЙСТВА

6.1 Первое включение

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. В появившемся окне введите имя пользователя (admin) и пароль учётной записи (admin). Интерфейс входа в систему показан на рисунке ниже (Рисунок 6.1).

Учётные данные по умолчанию при первом включении коммутатора:	
Имя пользователя	admin
Пароль (по умолчанию)	admin

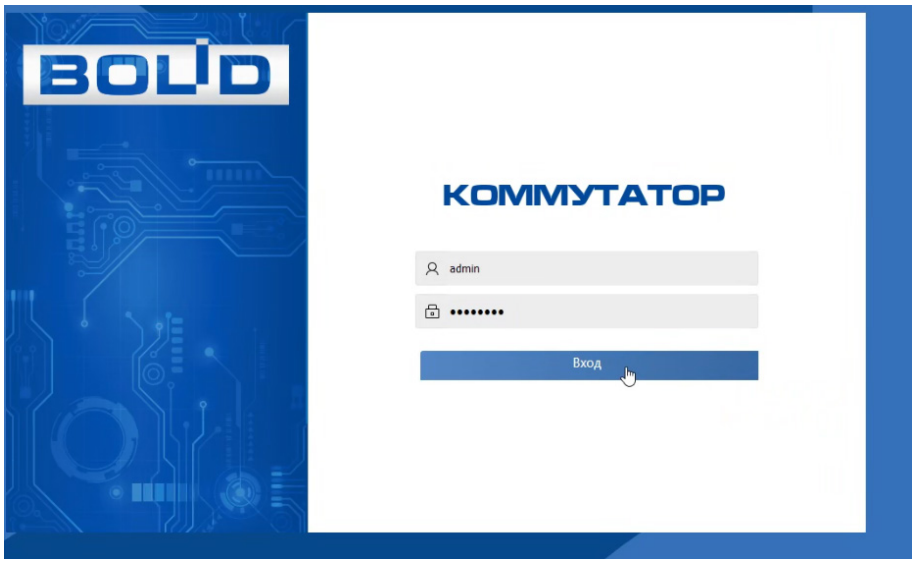


Рисунок 6.1 – Вход

Шаг 3. Далее установите новый пароль учётной записи admin. 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 «Подтвердить» (Рисунок 6.2).

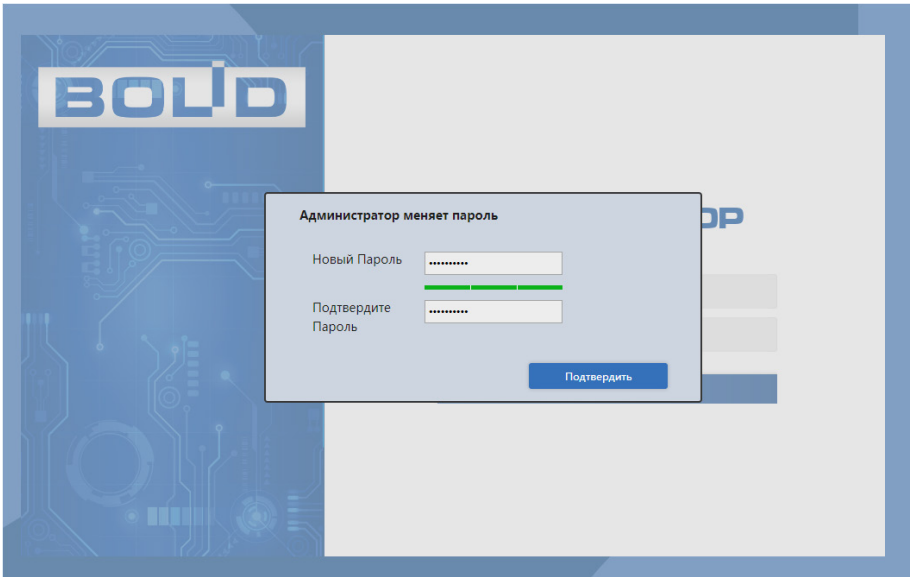


Рисунок 6.2 – Установка пароля

Шаг 4. Для входа, повторно введите новый пароль учётной записи admin и нажмите кнопку «Вход».

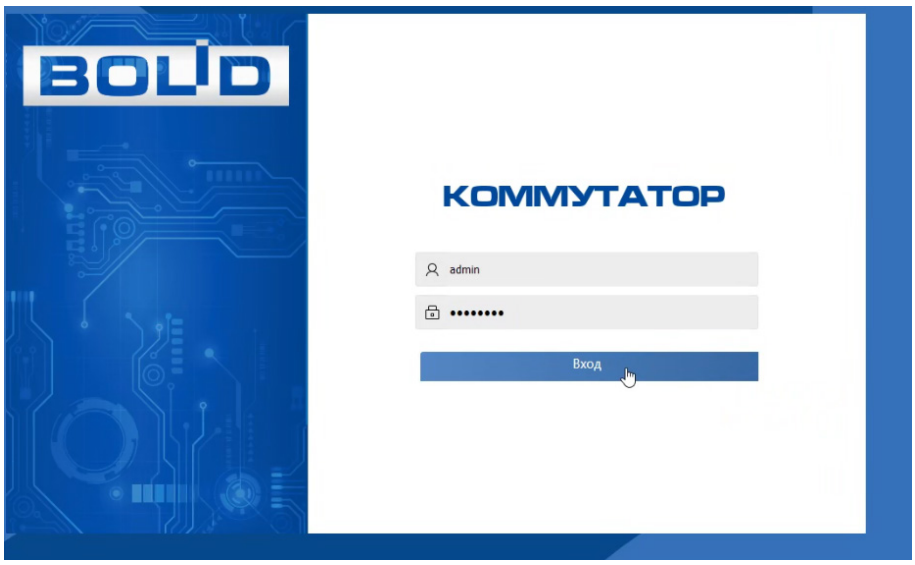


Рисунок 6.3 – Вход

6.2 Локальный адрес

Шаг 5. После первого входа в систему измените сетевые настройки коммутатора в соответствии с параметрами вашей сети.

Для изменения параметров на панели быстрой настройки нажмите кнопку «Локальный адрес» и задайте имя устройства, IP-адрес и префикс подсети. Перезагрузите устройство.

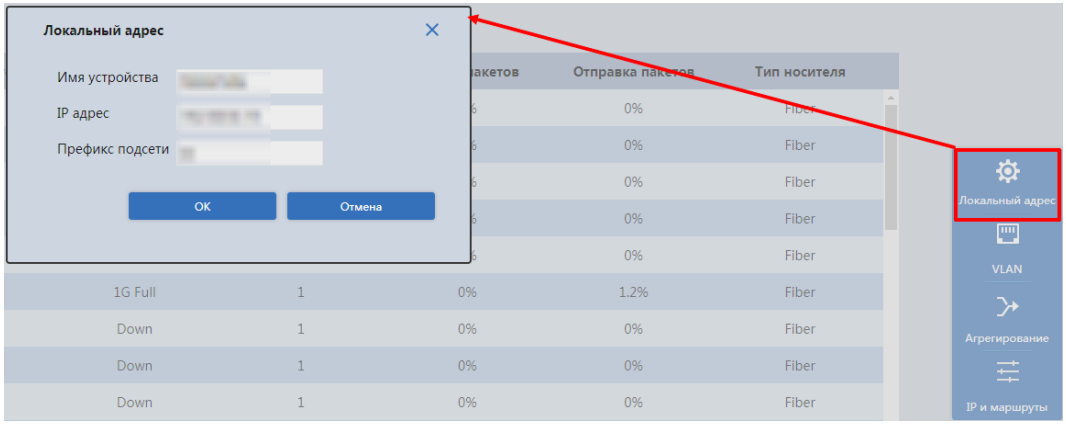


Рисунок 6.4 – Сетевые настройки

Шаг 6. После изменения настроек веб-интерфейс должен быть доступен по-новому IP-адресу. Корректный вход в систему производится с новыми учётными данными admin.

7 БЫСТРАЯ НАСТРОЙКА

Интерфейс быстрой настройки включает в себя графическую и текстовую информацию о состоянии портов, информацию о системе, и панель быстрой настройки.

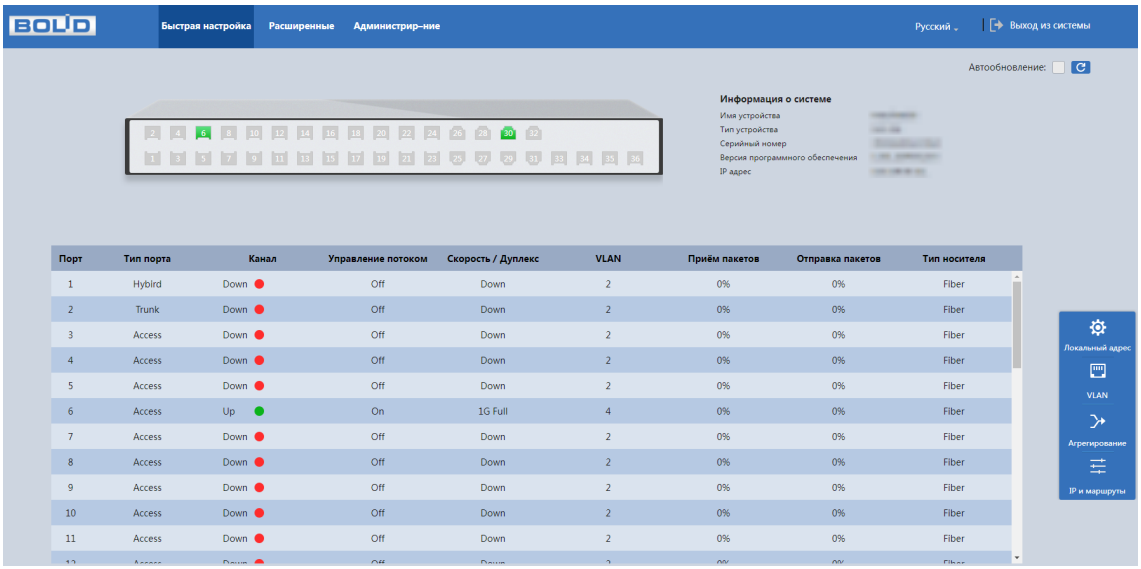


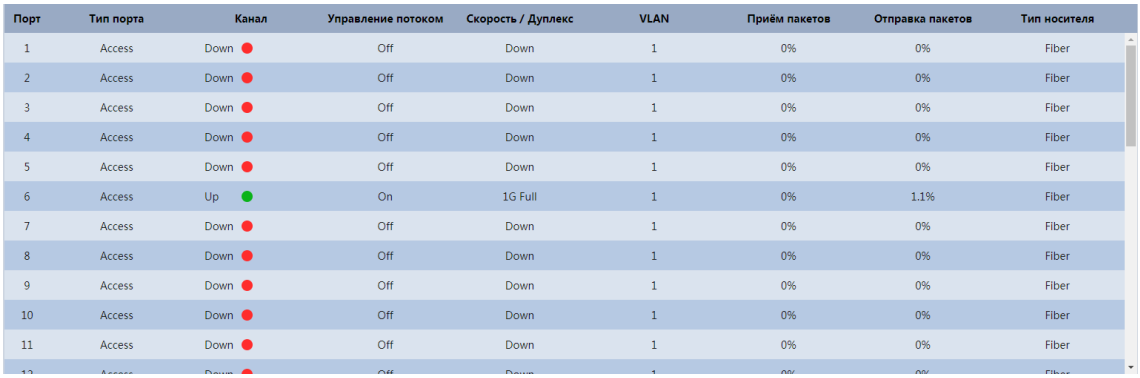
Рисунок 7.1 – Быстрая настройка

7.1 ИНФОРМАЦИЯ О ПОРТАХ

Графическая панель представляет собой изображение передней панели коммутатора. Отображает состояние подключения к портам в режиме реального времени.

Рисунок 7.2 – Графическая панель

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



Порт	Тип порта	Канал	Управление потоком	Скорость / Дуплекс	VLAN	Приём пакетов	Отправка пакетов	Тип носителя
1	Access	Down	Off	Down	1	0%	0%	Fiber
2	Access	Down	Off	Down	1	0%	0%	Fiber
3	Access	Down	Off	Down	1	0%	0%	Fiber
4	Access	Down	Off	Down	1	0%	0%	Fiber
5	Access	Down	Off	Down	1	0%	0%	Fiber
6	Access	Up	On	1G Full	1	0%	1.1%	Fiber
7	Access	Down	Off	Down	1	0%	0%	Fiber
8	Access	Down	Off	Down	1	0%	0%	Fiber
9	Access	Down	Off	Down	1	0%	0%	Fiber
10	Access	Down	Off	Down	1	0%	0%	Fiber
11	Access	Down	Off	Down	1	0%	0%	Fiber

Рисунок 7.3 – Информационная панель

Таблица 7.1– Текстовая информация о порте

Параметр	**Описание**
Порт	Номер порта. Соответствует числу на лицевой панели.
Тип порта	Доступны три вида: Access, Hybrid и Trunk.
Канал	– Up – порт подключен; – Down – порт отключен; – Disabled – порт выключен.
Управление потоком	Состояние управления потоком.
Скорость/Дуплекс	Отображает текущую скорость и в каком режиме передачи параллельном (Full) или последовательном находится порт.
VLAN	Идентификатор VLAN.
Прием пакетов	Нагрузка в процентах от максимальной пропускной способности принимаемых портом пакетов.
Отправка пакетов	Нагрузка в процентах от максимальной пропускной способности передаваемых портом пакетов.
Тип носителя	Показывается тип подключенного носителя сигнала. – Copper – медный кабель; — Fiber – волоконно-оптический кабель.

7.2 Быстрая настройка

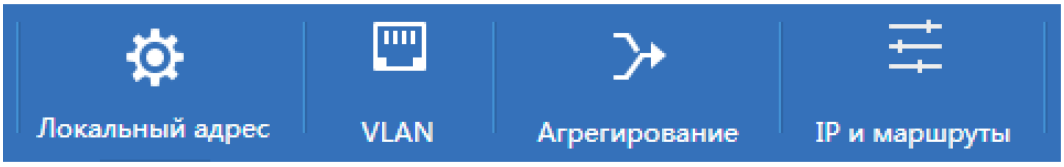


Рисунок 7.4 – Меню

7.2.1 VLAN

Пункт меню быстрой настройки позволяет изменять ранее созданные настройки VLAN на порт. Для получения более подробной информации перейдите в пункт меню «Настройки VLAN».

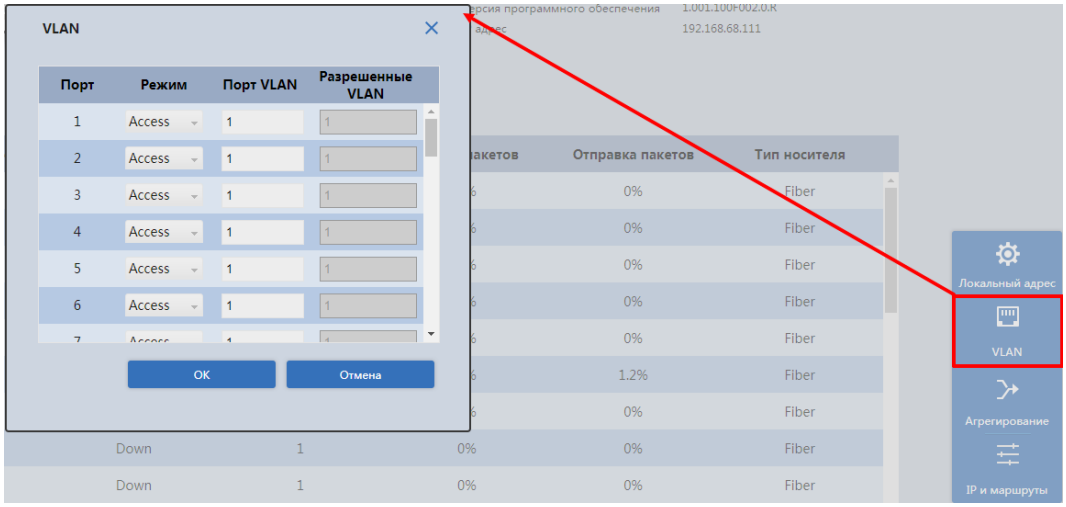


Рисунок 7.5 – VLAN

7.2.2 Агрегирование

Сформируйте из нескольких физических портов коммутатора один логический порт, для увеличения общей пропускной способности. Для получения более подробной информации перейдите в пункт меню «Агрегирование».

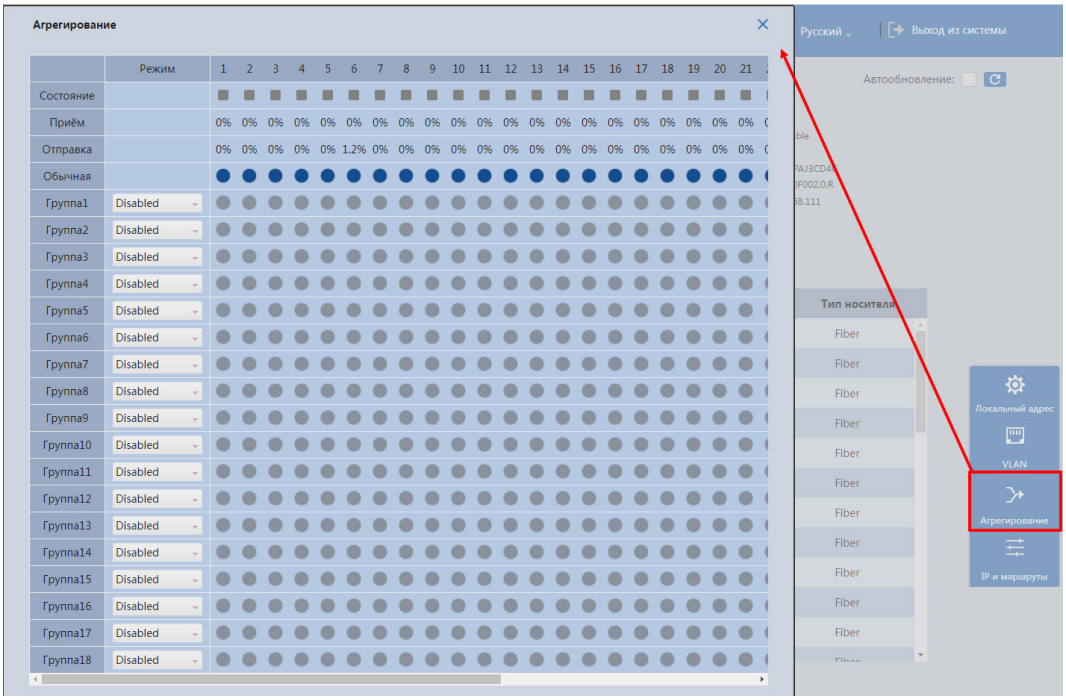


Рисунок 7.6 – Агрегирование

7.2.3 IP и маршруты

Создайте и сохраните IP-адрес виртуального интерфейса VLAN и IP-маршрут для осуществления маршрутизации пакетов, между сетями исходя из ваших подключений к устройству. Для получения более подробной информации перейдите в пункт меню «IP/маршруты».

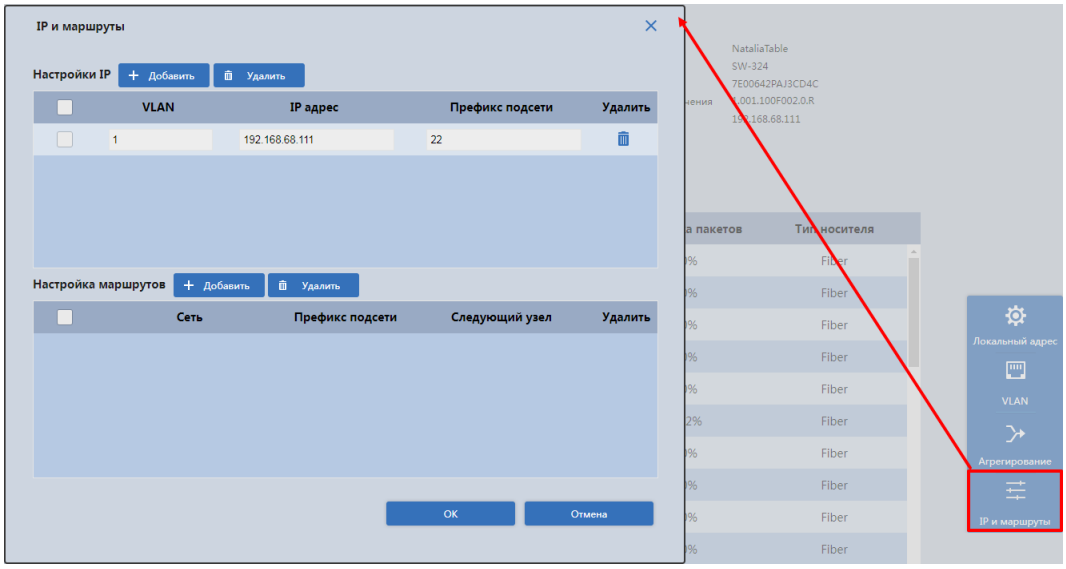


Рисунок 7.7 – IP и маршруты

8 БАЗОВЫЕ НАСТРОЙКИ

8.1 РАСШИРЕННЫЕ/ОБЩИЕ

8.1.1 Конфигурация

8.1.1.1 Информация о системе

Интерфейс ввода, изменения и просмотра системной информации, панели с информацией о программном обеспечении, аппаратной части и версии устройства.

ВНИМАНИЕ!
Будьте осторожны при включении DHCP-клиента. После включения DHCP-клиента IP-маршрутизатор или DHCP сервер, подключающийся к коммутатору, автоматически назначит коммутатору IP-адрес, а существующий IP-адрес будет признан недействительным, после чего вы не сможете получить доступ к веб-интерфейсу по старому IP-адресу.

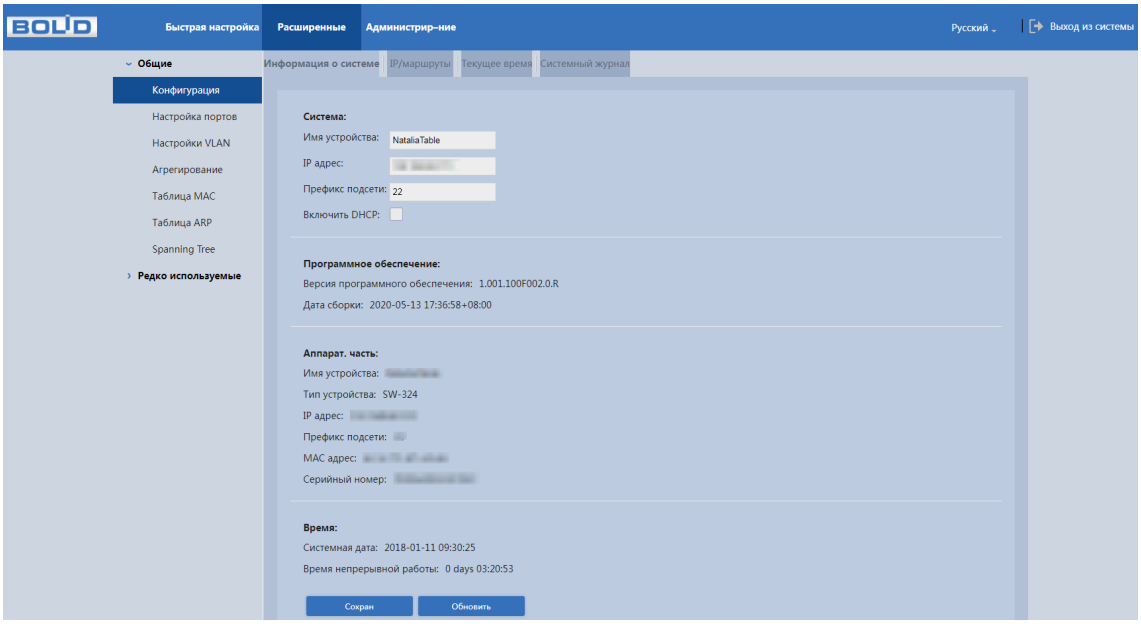


Рисунок 8.1 – Информация о системе и версии ПО

8.1.1.2 Текущее 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.

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

Для синхронизации с NTP-сервером активируйте радиокнопку «Включить NTP» и введите адрес NTP-сервера.

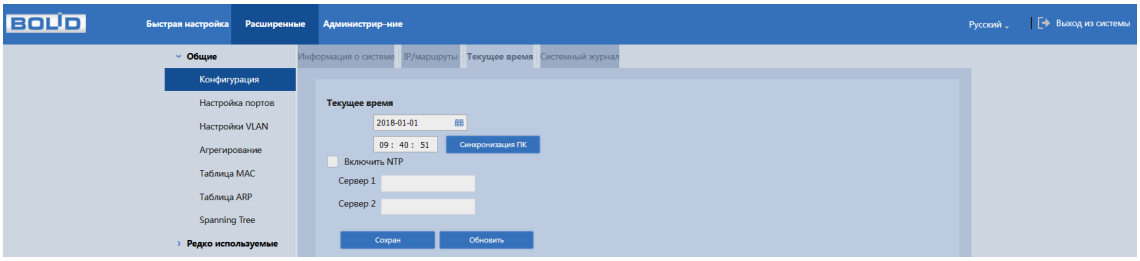


Рисунок 8.2 – Настройка/синхронизация времени

8.2 Расширенные/Редко используемые

8.2.1 Безопасность

8.2.1.1 Управление пользователями

Для изменения пароля учётной записи нажмите кнопку в столбце «Изменить».

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 «ОК»

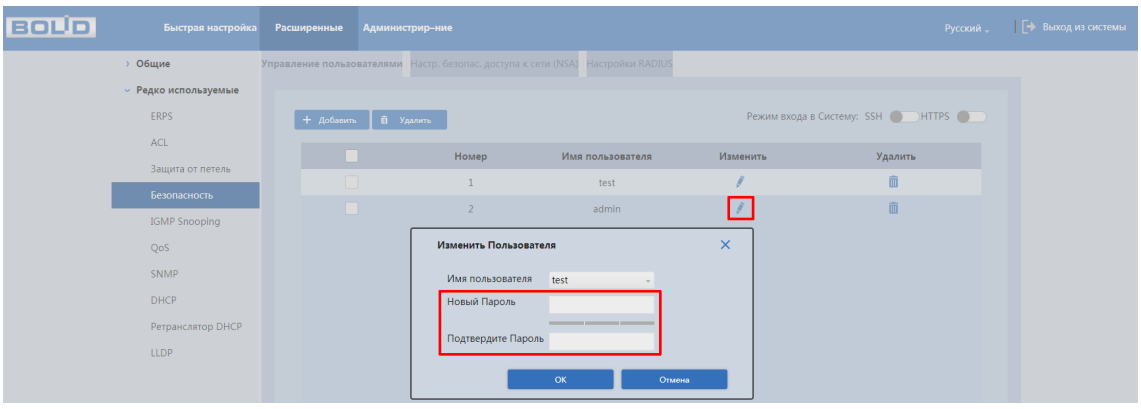


Рисунок 8.3 – Изменение пароля

9 НАСТРОЙКИ ДОСТУПА

9.1 РАСШИРЕННЫЕ/ОБЩИЕ

9.1.1 Настройки 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.

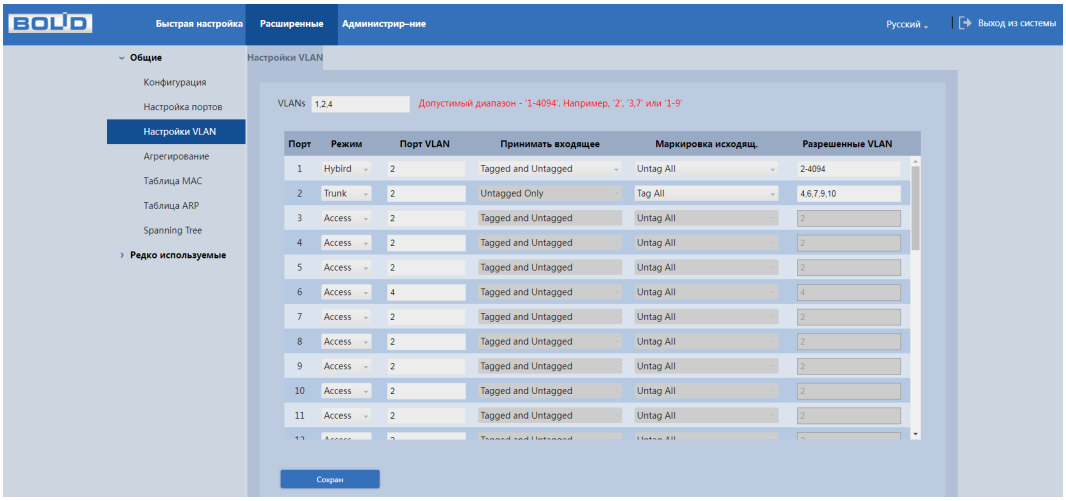


Рисунок 9.1 – Настройка VLAN

Для создания VLAN на устройстве выполните следующие действия:

1. Введите в строке «VLANs» номера создаваемых VLAN, например, введите 1 и 2, чтобы создать VLAN 1 и VLAN 2.

2. Настройте параметры фильтрации, более подробная информация описана в таблице ниже (Таблица 9.1).

Таблица 9.1 – Конфигурирование VLAN-порта

Столбец	Описание
Порт	Выбор логического порта устройства.
Порт VLAN	Задаётся принадлежность порта к конкретному VLAN. Допустимые VLAN находятся в диапазоне от 1 до 4095, по умолчанию 1. В случае работы порта в режиме «Access», поступающий на порт трафик помечается тегом, записанным в данное поле.

Столбец	Описание
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 «Разрешённые VLAN». Становится активным выбор «Egress tagging»; – Hybrid – в отличие от Trunk для исходящего трафика, hybrid режим позволяет снимать все метки VLAN или наоборот обязательно метить тегом «порт VLAN». В остальном принцип работы совпадает.
Принимать входящее	Работа с входящими доступна только в режиме «Hybrid». – Tagged and Untagged – все пакеты с метками VLAN и без будут приниматься; – Tagged Only – только все пакеты с метками VLAN будут приниматься; Untagged Only – Только все пакеты без меток VLAN будут приниматься.
Маркировка исходящ.	При установке режима в «Access» данное поле не доступно. Тег VLAN принудительно снимается. – Untag port VLAN – будет снята метка с пакетов, относящихся к VLAN с тегом, указанным в поле «порт VLAN». Остальные пакеты будут переданы без изменений; – Tag ALL – все пакеты с метками VLAN из списка разрешённых будут передаваться без изменений; – Untag All – все пакеты без меток VLAN из списка разрешённых будут передаваться без изменений.
Разрешённые VLAN	Установите разрешённый VLAN для порта.

9.1.2 Конфигурация

9.1.2.1 IP/маршруты

После создание и настройки на устройстве технологии VLAN, необходимо настроить процесс маршрутизации (IVR).

Создайте и сохраните IP-адрес виртуального интерфейса VLAN и IP-маршрут для осуществления маршрутизации пакетов, между сетями исходя из вашей логической топологии.

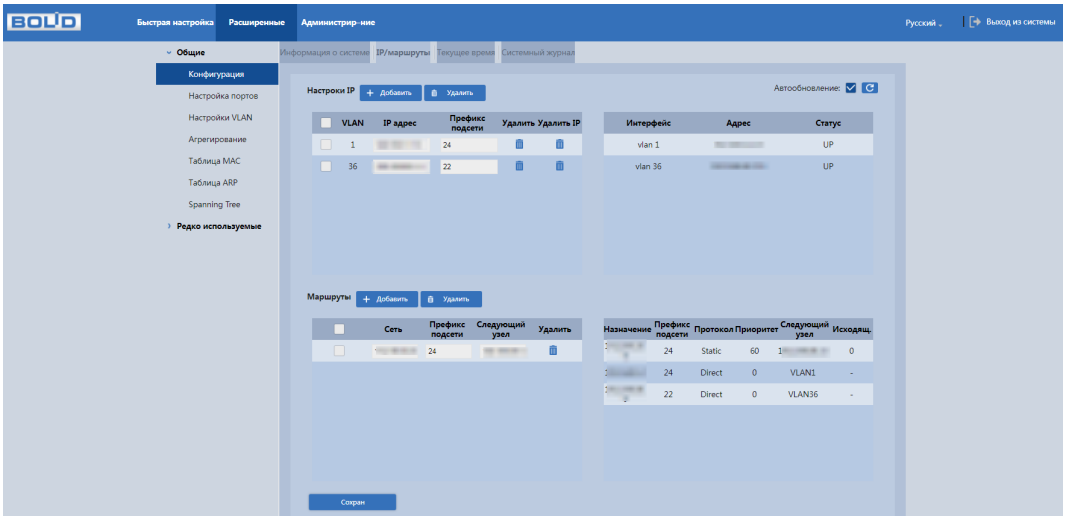


Рисунок 9.2 – Настройка маршрутизации на устройстве

Нажмите кнопку «Добавить» в строке «Настройка IP» для добавления IP-адреса. Далее введите и сохраните данные для добавления.

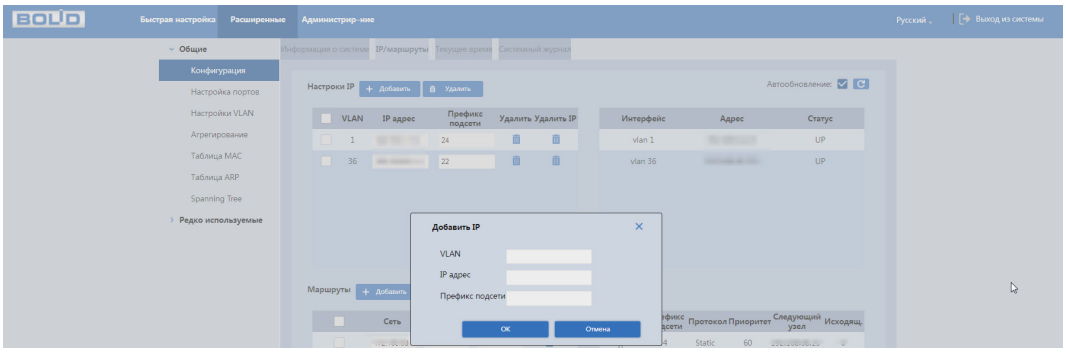


Рисунок 9.3 – Настройка маршрутизации на устройстве. Добавление IP

Таблица 9.2 – Настройка маршрутизации на устройстве. Добавление IP

Параметр	Функция
VLAN	Введите номер VLAN.
IP адрес	Введи IP-адрес добавляемого VLAN.
Префикс подсети	Введите идентификатор подсети.

Нажмите кнопку «Добавить» в строке «Маршруты» для добавления IP-маршрута. Далее введите и сохраните данные для добавления.

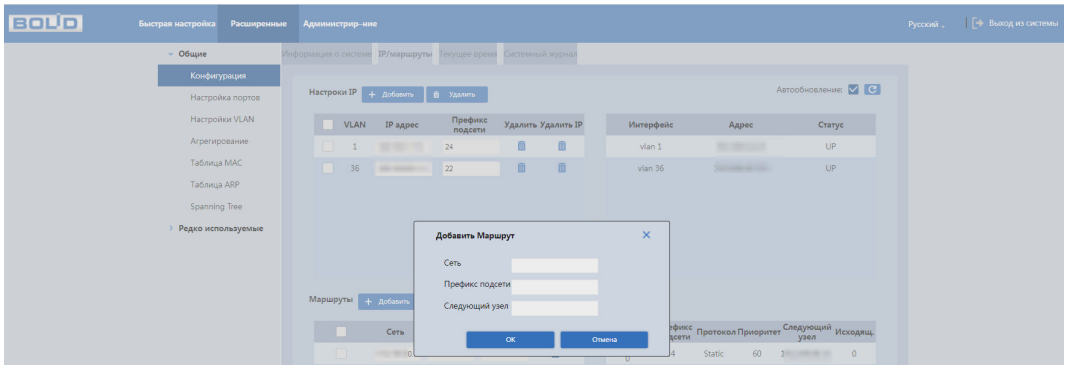


Рисунок 9.4 – Настройка маршрутизации на устройстве. Добавление маршрута

Таблица 9.3 – Настройка маршрутизации на устройстве. Добавление маршрута

Параметр	Функция
Сеть	IP-сеть назначения или адрес хоста этого маршрута.
Префикс подсети	Вписывается префикс подсети.
Следующий узел	IP-адрес следующего перехода маршрута.

9.1.3 Настройка портов

На рисунке (Рисунок 9.5) показан интерфейс конфигурации портов коммутатора. Настройка конфигурации порта должна соответствовать практическим требованиям устройства.

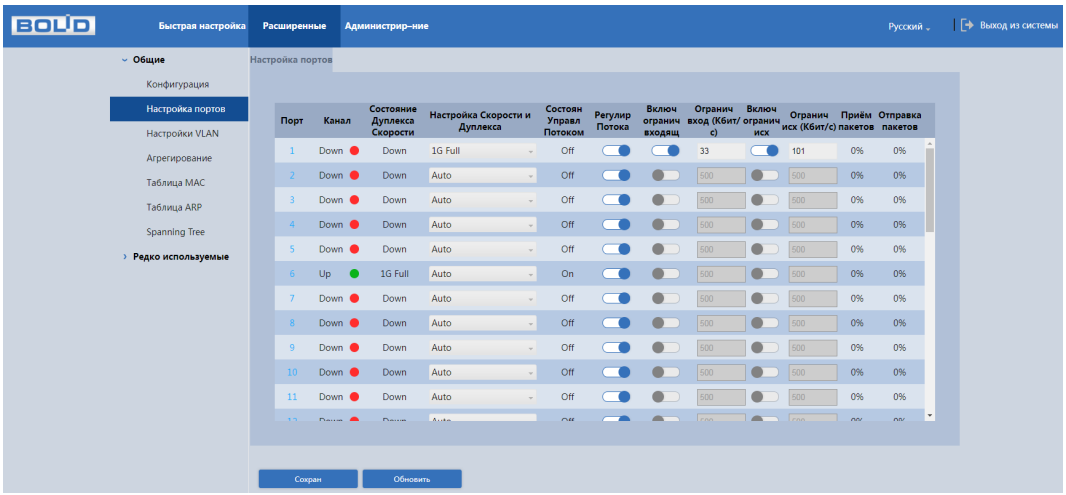


Рисунок 9.5 – Конфигурация портов коммутатора

Таблица 9.4 – Настройка конфигурации портов

<table>
<tr><th colspan="2">Столбец</th><th colspan="3">Описание</th></tr>
<tr><td colspan="2">Порт</td><td colspan="3">Номер порта соответствует числу на лицевой панели. При нажатии на номер порта появиться информационное окно «Информация о порте», более подробная информация о панели содержится в разделе «Настройка портов».</td></tr>
<tr><td rowspan="2">Канал</td><td rowspan="2">Отображает статус связи порта</td><td>Up</td><td colspan="2">Порт находится в активном состоянии.</td></tr>
<tr><td>Down</td><td colspan="2">Порт находится в отключенном состоянии.</td></tr>
<tr><td>Состояние дуплекса скорости</td><td colspan="4">Отображает текущее состояние скорости порта</td></tr>
<tr><td rowspan="9">Настройка скорости и дуплекса</td><td>Порт</td><td>Скорость</td><td colspan="2">Описание</td></tr>
<tr><td rowspan="3">SFP
(1 – 24)</td><td>Авто.</td><td colspan="2">Автоматическая настройка скорости и режима передачи.</td></tr>
<tr><td>100M FULL</td><td colspan="2">Скорость 100 Мб/с. Работа в режиме полного дуплекса.</td></tr>
<tr><td>1G Full</td><td colspan="2">Скорость 1000 Мб/с. Работа в режиме полного дуплекса.</td></tr>
<tr><td rowspan="5">Ethernet порт
(25 – 32)</td><td>Авто.</td><td colspan="2">Автоматическая настройка скорости и режима передачи.</td></tr>
<tr><td>10M FULL</td><td colspan="2">Скорость 10 Мб/с. Работа в режиме полного дуплекса.</td></tr>
<tr><td>10M HALF</td><td colspan="2">Скорость 10 Мб/с. Работа в режиме полудуплекса.</td></tr>
<tr><td>100M HALF</td><td colspan="2">Скорость 100 Мб/с. Работа в режиме полудуплекса.</td></tr>
<tr><td>100M FULL</td><td colspan="2">Скорость 100 Мб/с. Работа в режиме полного дуплекса.</td></tr>
</table>

<table>
<tr><th colspan="2">Столбец</th><th colspan="2">Описание</th></tr>
<tr><td></td><td>Ethernet порт
(25 – 32)</td><td>1G Full</td><td>Скорость 1000 Мб/с. Работа в режиме полного дуплекса.</td></tr>
<tr><td rowspan="3">Настройка скорости и дуплекса</td><td rowspan="3">SFP+
(33 – 36)</td><td>Авто.</td><td>Автоматическая настройка скорости и режима передачи.</td></tr>
<tr><td>1G Full</td><td>Скорость 1000 Мб/с. Работа в режиме полного дуплекса.</td></tr>
<tr><td>10G Full</td><td>Скорость 10 000 Мб/с. Работа в режиме полного дуплекса.</td></tr>
<tr><td colspan="2" rowspan="2">Регулировка потока</td><td>Up</td><td>Включение функции.</td></tr>
<tr><td>Off</td><td>Выключение функции.</td></tr>
<tr><td colspan="2" rowspan="2">Включение ограничений входящих</td><td>Up</td><td>Включить ограничение входящей скорости.</td></tr>
<tr><td>Off</td><td>Выключить ограничение входящей скорости.</td></tr>
<tr><td colspan="2">Ограничение входа (Кбит/с)</td><td colspan="2">Ограничение входящей скорости, доступный диапазон (25 – 13128147)</td></tr>
<tr><td colspan="2" rowspan="2">Включить ограничение исходящих</td><td>Up</td><td>Включить ограничение исходящей скорости.</td></tr>
<tr><td>Off</td><td>Выключить ограничение исходящей скорости.</td></tr>
<tr><td colspan="2">Ограничение исходящих (Кбит/с)</td><td colspan="2">Ограничение исходящей скорости, доступный диапазон (100 – 13107100).</td></tr>
<tr><td colspan="2">Приём пакетов</td><td colspan="2">Отображение текущего состояния приёма пакетов.</td></tr>
<tr><td colspan="2">Отправка пакетов</td><td colspan="2">Отображение текущего состояния отправки пакетов.</td></tr>
</table>

9.1.4 Агрегирование

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

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

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

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

9.1.4.1 Статическая агрегация

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

📖 Режим «Балансировки Нагрузки».

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

Таблица 9.5 – Типы алгоритма балансировки нагрузки

Режим балансировки	Описание
Исходящий MAC-адрес	Балансировка нагрузки, осуществляемая на основе поля MAC-адреса источника.
MAC-адрес назначения	Балансировка нагрузки, осуществляемая на основе поля MAC-адреса назначения.
IP адрес	Балансировка нагрузки, осуществляемая на основе IP-адреса.
TCP/UDP порт	Балансировка нагрузки, осуществляемая на основе номера порта TCP/UDP.

📖 Группа «Агрегирования».

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

📖 Входящие в группу порты.

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

9.1.4.2 LACP

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

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

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

Настройки протокола LACP в основном включают в себя функцию включения режима активности (активный/пассивный режим) и выделение порта LACP.

Порты, которые только включают протокол LACP, могут реализовать согласование LACP, и тогда он может сформировать агрегированный канал.

Режим передачи включает в себя «активный/пассивный» режимы. Устройство будет активно запускать канал агрегации, когда оно находится «активном» состоянии; устройство будет пассивно принимать данные об агрегации, запущенной другими устройствами, когда оно в состоянии «пассивный».

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

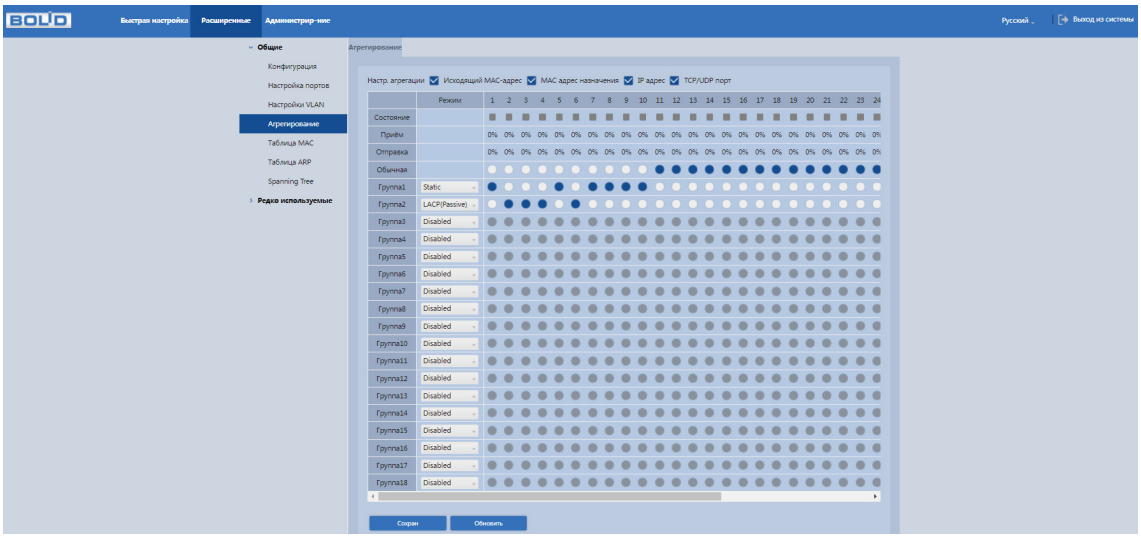


Рисунок 9.6 – Интерфейс настройки агрегации ссылок

9.1.5 Таблица MAC

9.1.5.1 Таблица MAC адресов

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

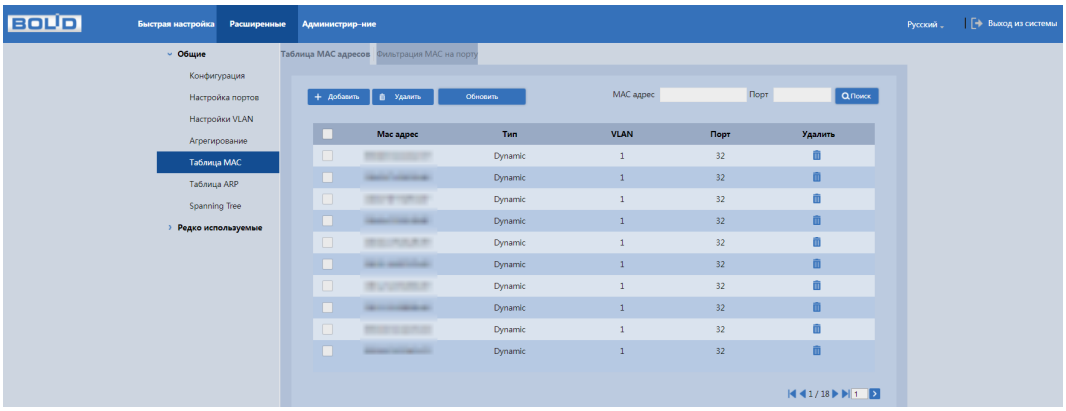


Рисунок 9.7– MAC информация об адресах

9.1.5.2 Фильтрация MAC на порту

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

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

2. Сохраните настройку.

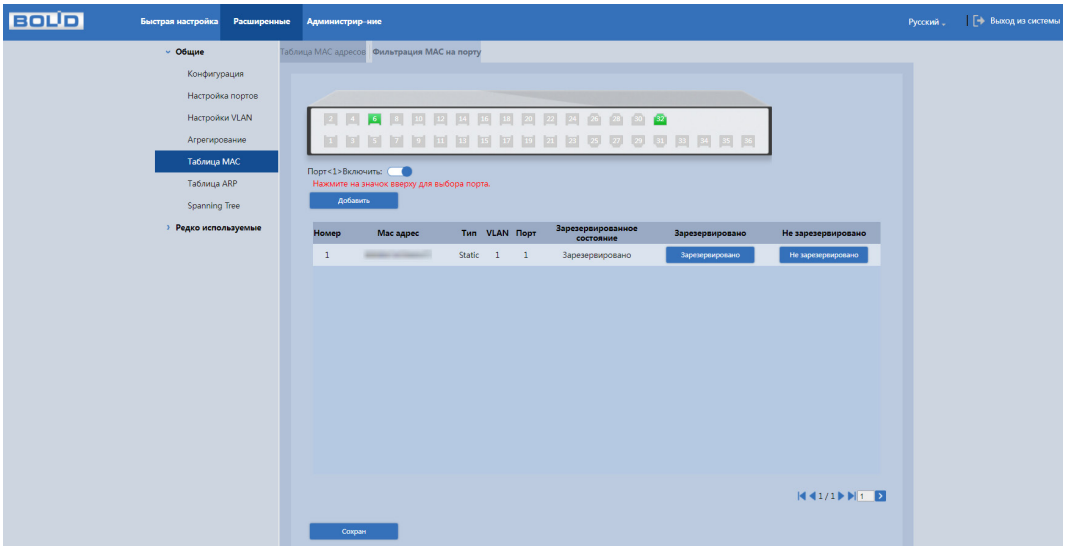


Рисунок 9.8 – Фильтрация портов

9.1.6 Spanning Tree (Связующее дерево)

9.1.6.1 Настройки порта STP

Из выпадающего списка в строке «Режим STP» выберите версию протокола, по которому будет производиться работа с устранением петель.

– Disable – Отключить;

– STP – Spanning Tree Protocol (IEEE 802.1D);

– RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w);

– MSTP – Multiple Spanning Tree Protocol (IEEE 802.1s).

Выделите порт из списка, и сохраните изменения. Система автоматически присваивает приоритеты портов.

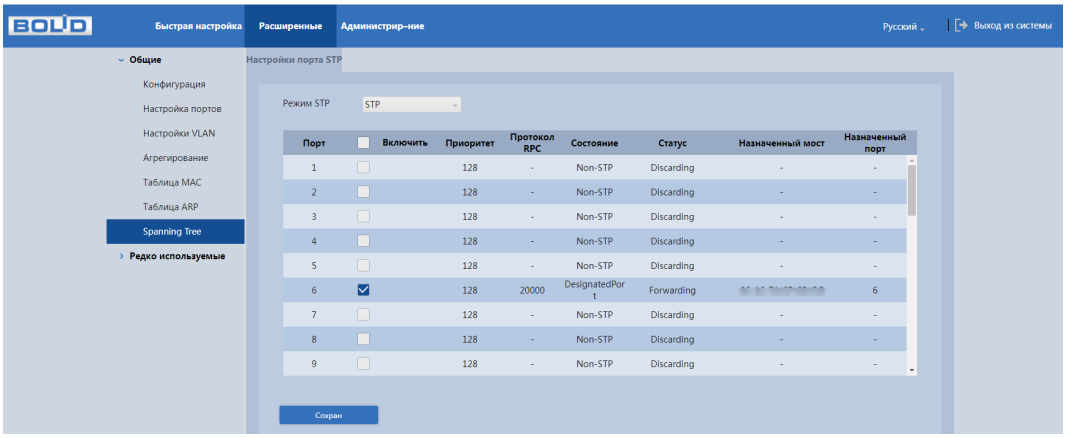


Рисунок 9.9 – Настройка STP

9.2 Редко используемые

9.2.1 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.

9.2.1.1 Настройки ACL

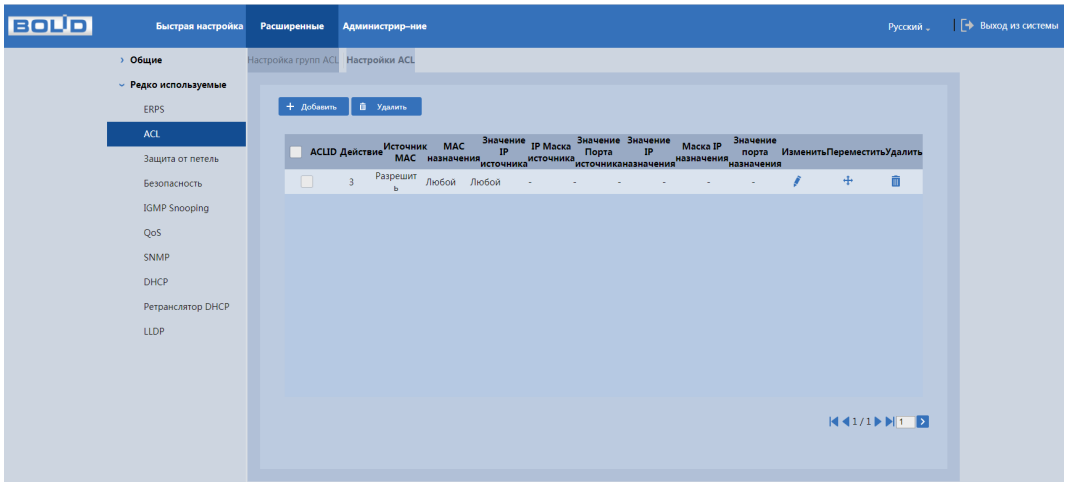


Рисунок 9.10 – Настройки ACL

Настройки фильтрации ACL разделяются на два типа:

– Стандартные (Standard): могут проверять только адреса источников (MAC ACL);

– Расширенные (Extended): могут проверять адреса источников, а также адреса получателей, в случае IP ещё тип протокола и TCP/UDP порты (IP ACL).

Условиями для осуществления приёма или отказа при стандартной фильтрации на уровне 2 будут MAC-адреса содержащиеся в каждом пакете. Параметры для заполнения описаны в таблице ниже (Таблица 9.6).

Таблица 9.6 – Параметры фильтра на основе уровня 2 «MAC ACL»

Параметр	Функция
Режим	При выборе «MAC ACL (уровня 2)» будет проверяться MAC-адрес в заголовке каждого пакета.
ACL ID	Уникальный идентификатор ACL.

Параметр	Функция
Действие	Выбор действия, которое будет происходить с пакетом во время пересылки, permit (разрешить) либо deny (запретить/отказать).
Источник MAC	Выберите из выпадающего списка параметр «Любой» или «Указан».
Исходящий MAC адрес	Введите MAC-адрес источника.
MAC назначение	Выберите из выпадающего списка параметр «Любой» или «Указан».
MAC адрес назначения	Введите MAC-адрес назначения.

Условиями для осуществления приёма или отказа при расширенной фильтрации на уровне 3 будут IP-адреса содержащийся в заголовке пакета, протоколы TCP или UDP и указанные порты. Параметры для заполнения описаны в таблице ниже (Таблица 9.7).

Таблица 9.7 – Параметры фильтра на основе уровня 3 «IP ACL»

Параметр	Функция
Режим	При выборе «IP ACL (уровня 3)» будет проверяться IP-адрес в заголовке каждого пакета.
ACL ID	Уникальный идентификатор ACL.
Действие	Выберите действие, которое будет происходить с пакетом во время пересылки, permit (разрешить) либо deny (запретить/отказать).
Протокол	Выберите протокол который будет проверяться в заголовке каждого пакета.
IP источник	Выберите из выпадающего списка параметр «Любой» или «Указан».
Значение IP источника	Введите IP-адрес источника.
IP маска источника	Введите маску подсети источника.
Порт источника	Выберите из выпадающего списка параметр «Любой» или «Указан».
Значение порта источника	Введите номер порта источника, доступный диапазон для ввода от 0 до 65535. Можно указать только конкретный порт, ввод диапазона недоступен.

Параметр	Функция
IP назначения	Выберите из выпадающего списка параметр «Любой» или «Указан».
Значение IP назначения	Введите IP-адрес назначения.
Маска IP назначения	Введите маску подсети назначения.
Порт назначения 2	Выберите из выпадающего списка параметр «Любой» или «Указан».
Значение порта назначения	Введите номер порта назначения, доступный диапазон для ввода от 0 до 65535. Можно указать только конкретный порт, ввод диапазона недоступен.

9.2.1.2 Настройка групп ACL

Для настройки групп введите в столбец «ACLID» номер ранее созданных настроек фильтрации, сохраните.

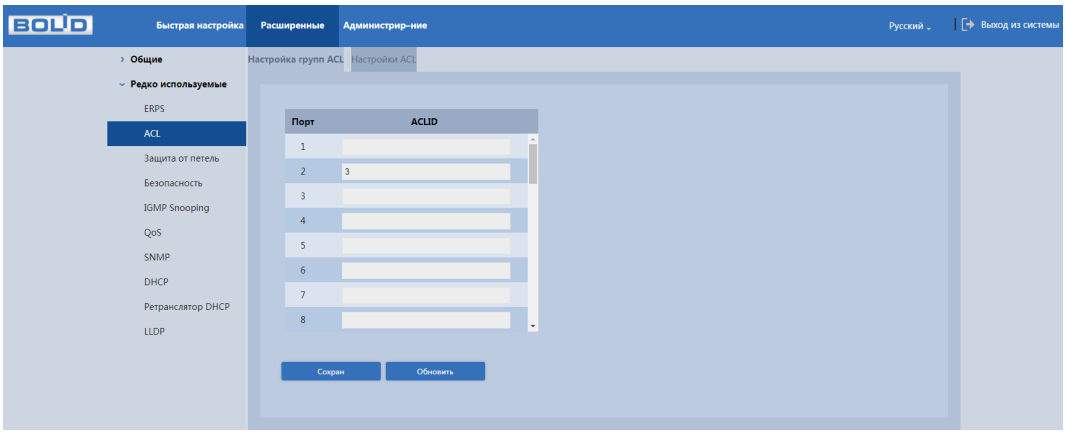


Рисунок 9.11 – Настройка групп ACL

9.2.2 Защита от 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.

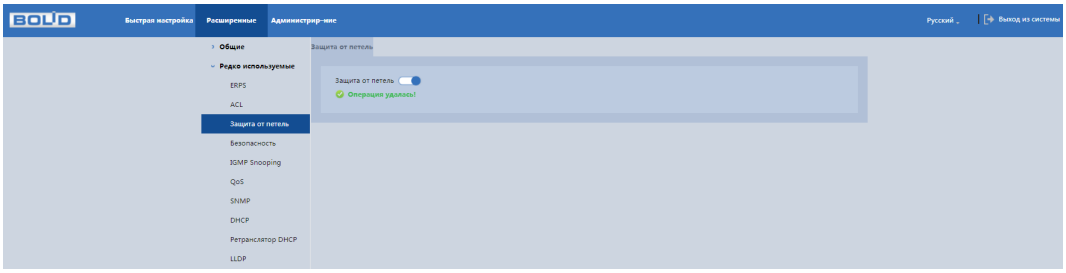


Рисунок 9.12 – Обнаружение петель (Loopback Detection)

9.2.3 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.

На рисунке (Рисунок 9.13) представлен интерфейс настроек в состоянии по умолчанию. При использовании Multicast рассылки, возможно, включить поддержку «Fast leave (Отбрасывание неизвестных многоадресных пакетов)», которая позволяет коммутатору быстрее исключать порт из списка участников соответствующей группы. Для целей видеонаблюдения ее включение не обязательно.

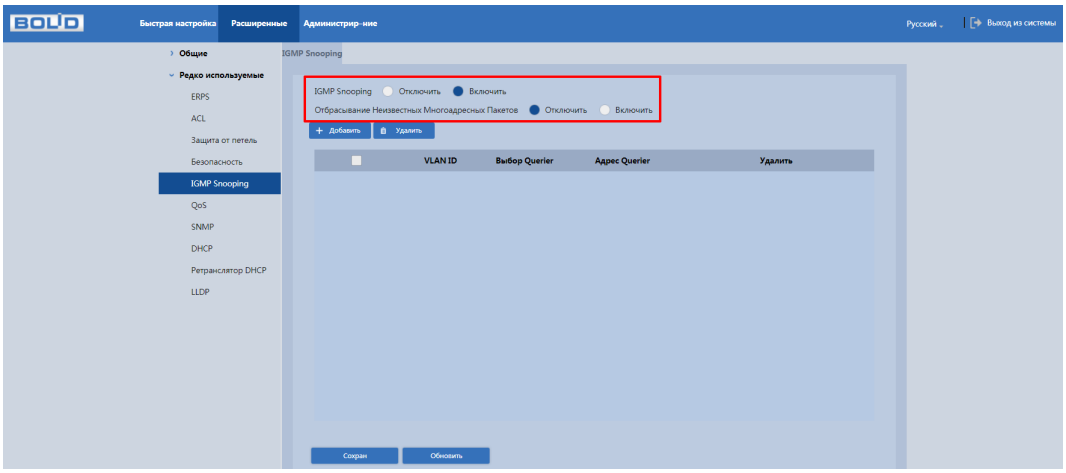


Рисунок 9.13 – Интерфейс IGMP Snooping

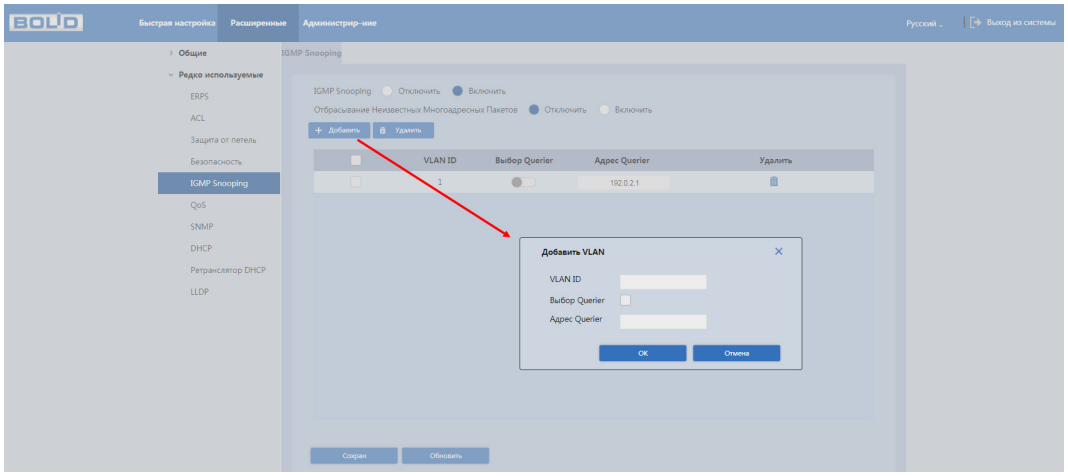


Рисунок 9.14 – Интерфейс настройки IGMP Snooping для VLAN

Таблица 9.8 – Параметры настройки IGMP Snooping для VLAN

Параметр	Описание
VLAN ID	Уникальный идентификатор VLAN соответствует тегу VLAN.
Выбор Querier	Включить маршрутизатор.
Адрес Querier	Поле определяет IPv4 адрес маршрутизатора, выступающего в роли mrouter в локальной сети. Такой маршрутизатор необходим для обработки и формирования заголовков запросов IGMP.

9.2.4 QoS

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

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

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

9.2.4.1 Классификация портов

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

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

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

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

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

Таблица 9.9 – 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.

Класс приоритета	Уровень приоритета 802.1p (десятичная система)	Уровень приоритета 802.1p (двоичная система)	Уровень обслуживания. Тип трафика
Очередь с высоким приоритетом	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.

Настройте класс приоритетности передачи трафика для выходного порта коммутатора при помощи технологии QoS. По умолчанию QoS отключен на всех портах, а приоритет трафика нулевой.

Для настройки:

1. Выберите порт.

2. Из выпадающего списка в столбце «CoS» установите приоритет. Чем выше значение CoS, тем выше приоритет;

3. В зависимости от настроек включите DSCP.

4. Сохраните настройку.

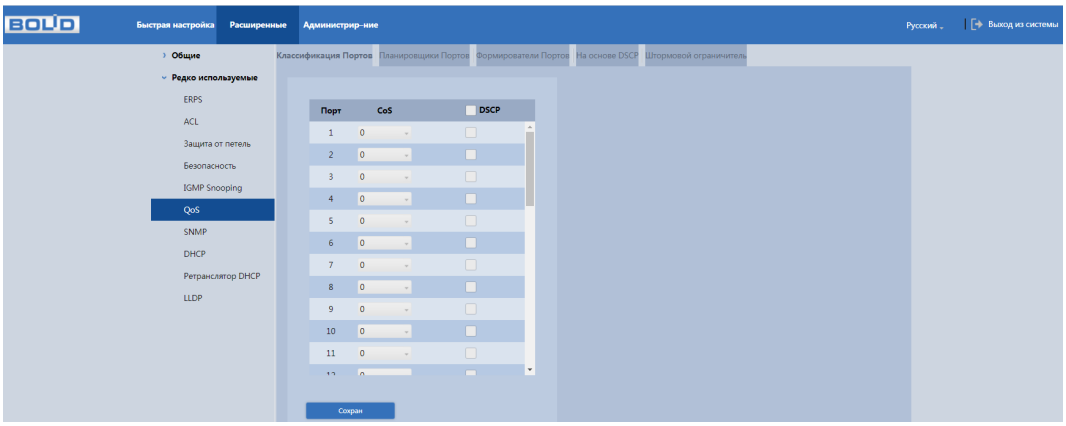


Рисунок 9.15 – Классификация порта

Пример:

Установите для порта 1 значение 1, а для порта 2 значение 2.

Порт 1 и порт 2 являются входными портами, а порт 3 – выходным портом. Значение CoS порта 2 больше, чем у порта 1, поэтому данные порта 2 сначала будут проходить через порт 3.

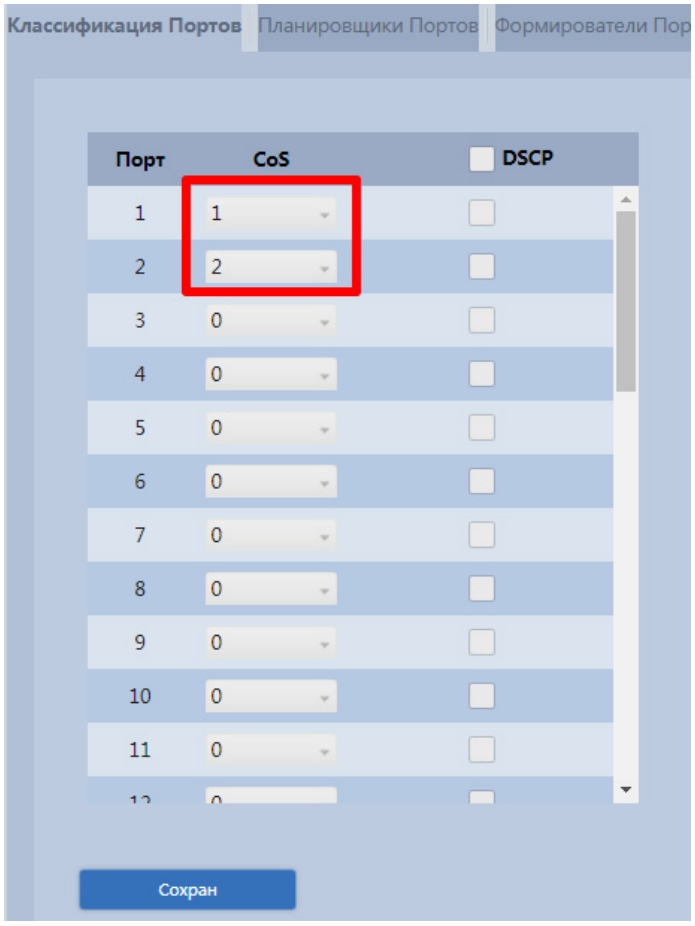


Рисунок 9.16 – Значение CoS порта

9.2.4.2 Разделы «Планировщики портов», «Шейпер трафика (Формирователи портов)»

Настройки в разделах «Планировщики портов» и «Шейпер трафика (Формирователи портов)» идентичны, направлены на настройки класса обслуживания. Разница между интерфейсами заключается в том, что на интерфейсе раздела «Планировщики портов» отображена информация о весе пакета в очереди, а на интерфейсе раздела «Шейпер трафика (Формирователи портов)» отображена информация о скорости передачи трафика.

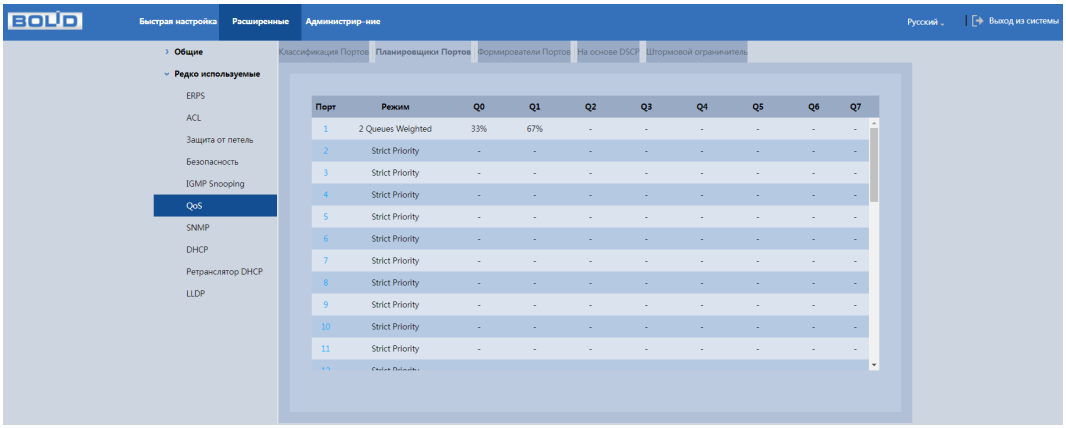


Рисунок 9.17 – Планировщик портов

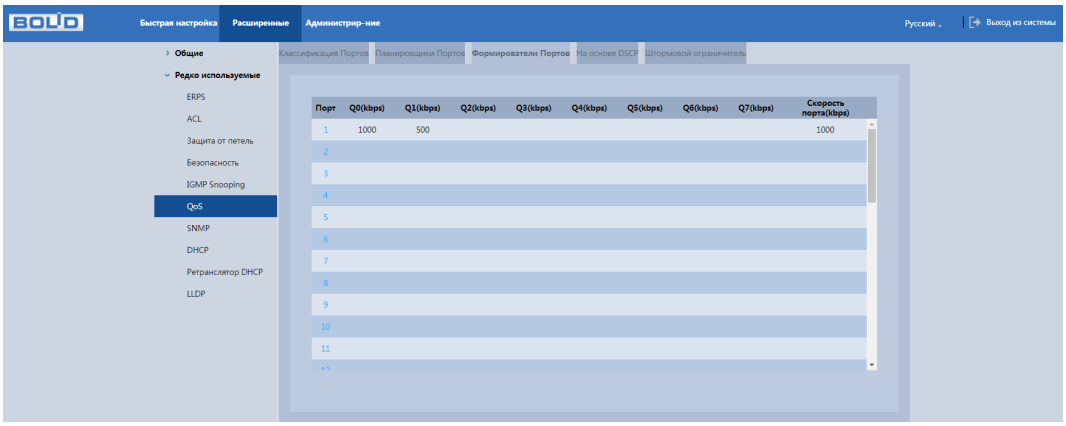


Рисунок 9.18 – Шейпер трафика (Формирователи портов)

Нажмите на цифру в столбце «Порт» для перехода к окну настроек «Планировщик и шейпер QoS исходящего с порта трафика. Порт N» (Рисунок 9.19). Окно настроек позволяет:

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

– Strict Priority (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;

– 2 – 8 Queues Weighted (WFQ – взвешенная справедливая очередь) – данные из каждой очереди обрабатывается последовательно, но в зависимости от приоритета очереди определяется количество передаваемого трафика за один цикл.

2. Настроить скорость и вес входящего трафика для 8 уровней приоритетов (от Q0 до Q7), поле «Шейпер очереди входящего трафика».

3. Настроить скорость исходящего трафика, поле «Шейпер очереди исходящего трафика».

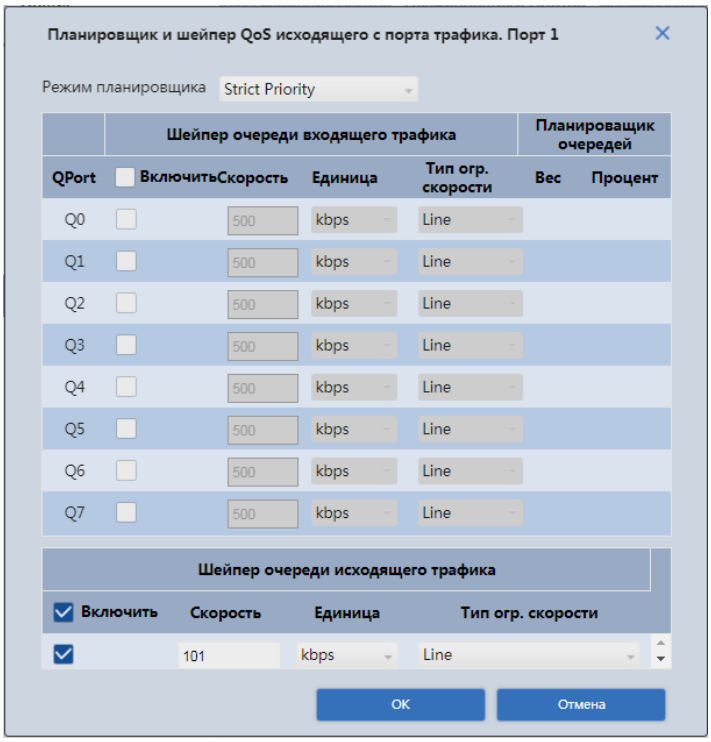


Рисунок 9.19 – Планировщик и шейпер QoS исходящего с порта трафика

Пример настройки:

1. Выберите в строке «Режим планировщика» – «2 Queues Weighted».

2. В поле «Шейпер очереди входящего трафика» установите скорость Q0 и Q1 – 500 кбит/с, а тип скорости – Line.

3. В поле «Шейпер очереди исходящего трафика» установите скорость – 500 кбит/с и тип скорости – Line. Когда возникает перегрузка и скорость двух портов составляет 400 кбит/с, скорость прохождения выходного порта составит 250 кбит/с.

4. Сохраните настройки.

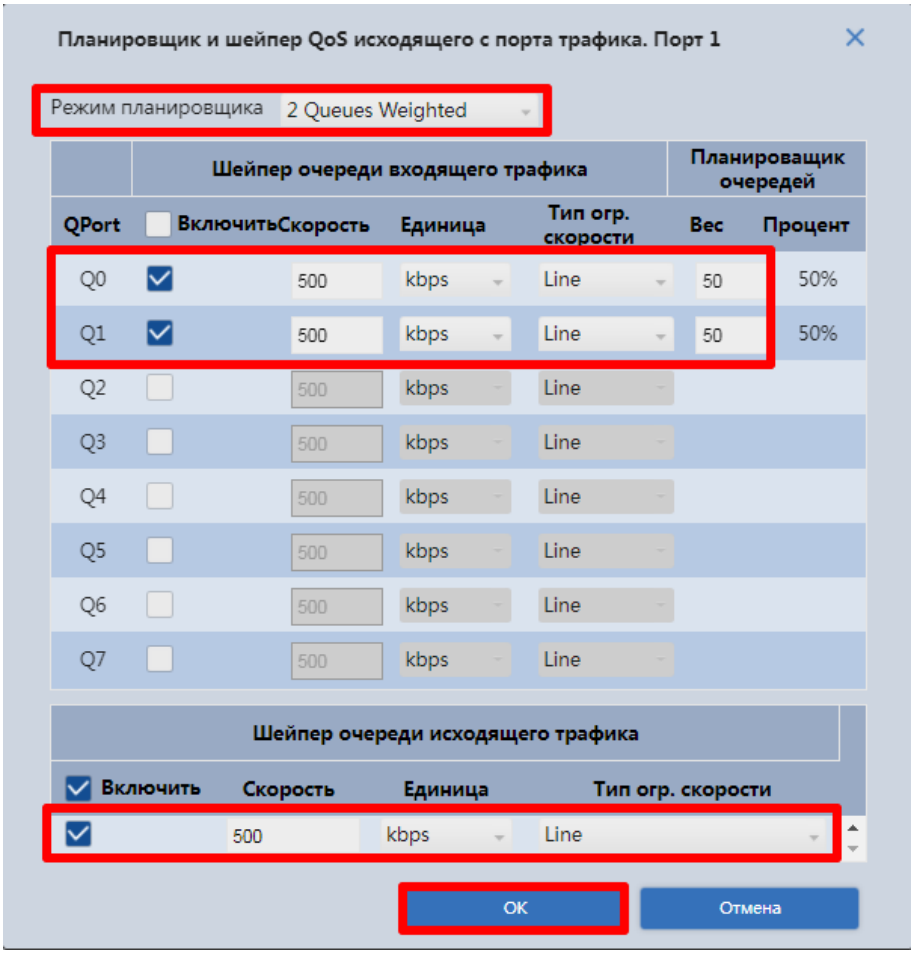


Рисунок 9.20 – Планировщик и шейпер QoS исходящего с порта трафика. Пример

9.2.4.3 На основе DSCP

Если на коммутатор приходят пакеты с DSCP маркировкой, то их можно разбить на 64 различных класса DSCP по 8 очередям приоритета.

Таблица 9.10 – 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

Перед настройкой включите DSCP на порту.

1. Для этого перейдите «Расширенные → Редко используемые → QoS → Классификация портов» (Рисунок 9.21).

2. Выберите порт, например, порт 4 и 8, включите DSCP.

3. Сохраните настройки.

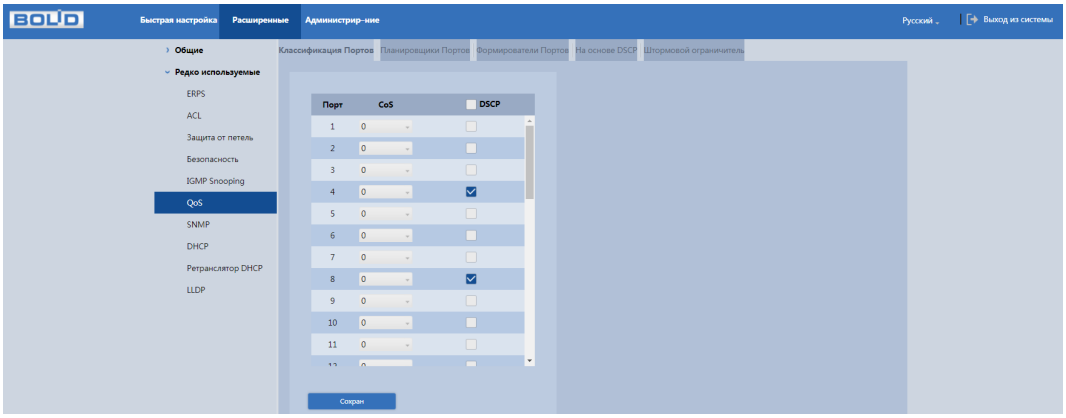


Рисунок 9.21 – Включить DSCP

4. Далее перейдите «Расширенные → Редко используемые → QoS → На основе DSCP».

5. Настройте DSCP. Например, если для DSCP на 4 и 8 заданы значения, CoS – 2, а DPL – 2 и 1, то выполните следующие действия:

– Включите порт 4 и 8, столбец «Доверять»;

– Порт 4: установите CoS равным 2 и DPL равным 2;

– Порт 8: установите CoS равным 2 и DPL равным 1.

– Сохраните настройку.

📖 Чем больше CoS DSCP, тем выше приоритет;

📖 Соответствующий пакет порта сначала пройдёт выходной порт.

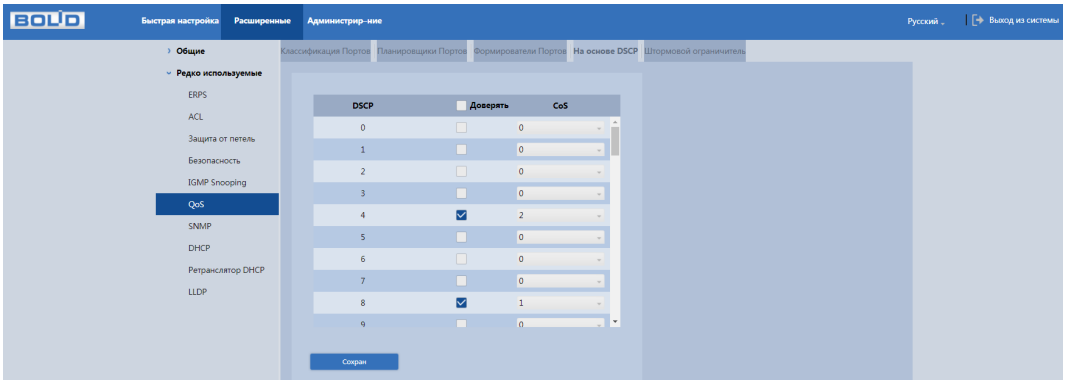


Рисунок 9.22 – На основе DSCP

9.2.4.4 Штормовой ограничитель

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 скорость до 1024 к/с одноадресного пакета.

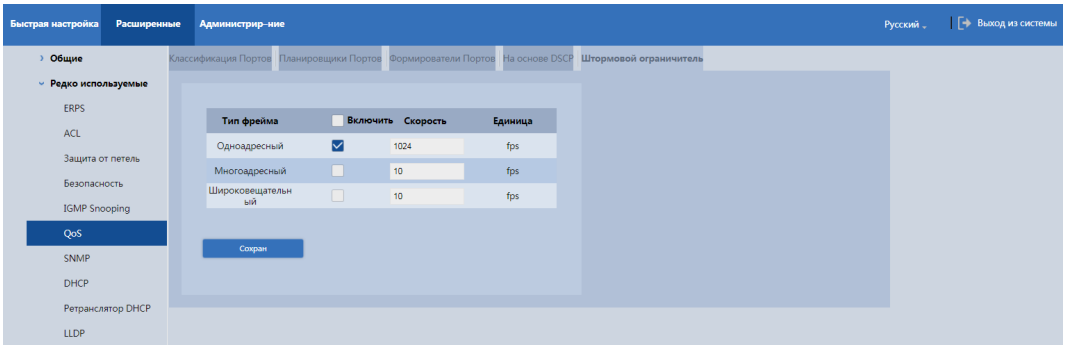


Рисунок 9.23 – Штормовой ограничитель

9.2.5 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 9.24) изображён интерфейс настроек SNMP версий 1 и 2, интерфейс настроек не отличается. По умолчанию значение SNMP порта 161.

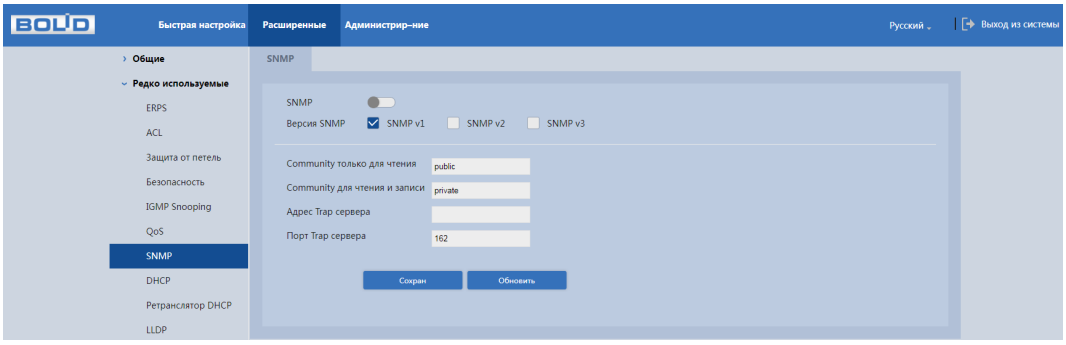


Рисунок 9.24 – Настройки SNMPv1/v2

На рисунке (Рисунок 9.25) изображён интерфейс настроек SNMP версии 3.

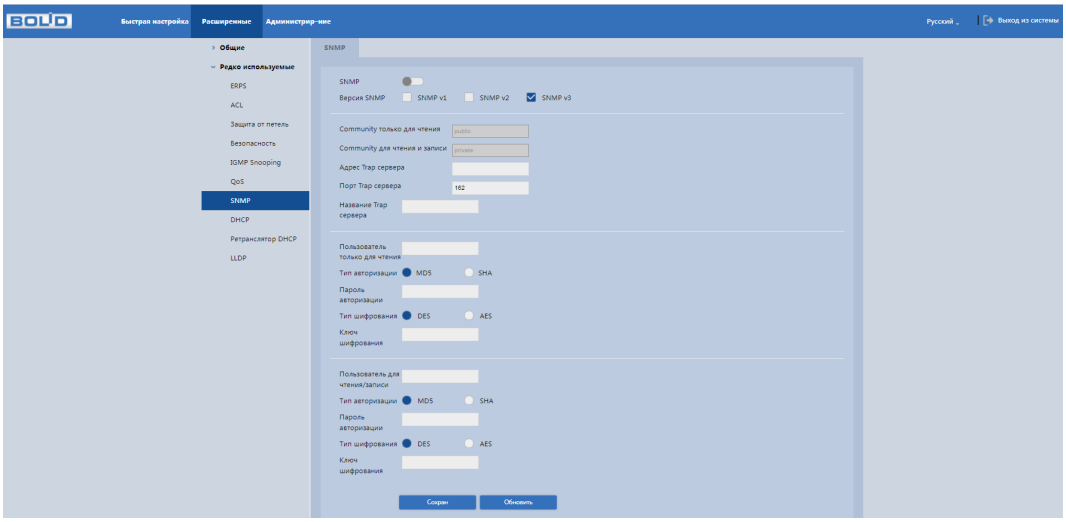


Рисунок 9.25 – Настройки SNMPv3

В следующей таблице описаны поля, относящиеся к этим настройкам.

Таблица 9.11 – 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).
Community только для чтения	Доступ SNMP только для чтения: поддерживается для всех целей SNMP.
Community для чтения и записи	Доступ SNMP для чтения и записи: поддерживается для всех целей SNMP.
Адрес trap сервера	Адрес системы мониторинга сети или ПК с предустановленным специализированным программным средством мониторинга. Служит для самостоятельной отправки видеорегистратором информации о событиях по протоколу SNMP.
Порт Trap сервера	Порт системы мониторинга сети или ПК с предустановленным специализированным программным средством мониторинга для захвата пакетов по SNMP протоколу. Значения параметра в диапазоне от 1 до 65535, с шагом 1. Значение по умолчанию: 162.
Название Trap сервера	Задание имени сервера
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	Устройством используется режим SNMPv3 «авторизация с шифрованием». Здесь можно задать метод шифрования ключа авторизации. Можно выбрать между MD5 или SHA.
Пароль авторизации	Введите пароль для аутентификации. Пароль должен содержать не менее восьми символов.
Тип шифрования	Поле выбора метода шифрования передаваемых данных. Можно выбрать между DES или AES.
Ключ шифрования	Поле для задания ключа шифрования передаваемых данных.

9.3 DHCP

9.3.1 Ретранслятор DHCP

DHCP (Dynamic Host Configuration Protocol) – протокол динамического конфигурирование хоста. 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, сервер предоставляет сетевой адрес и параметры конфигурации клиентам.

9.3.1.1 Включение

Для выбора устройства в качестве сервера DHCP включите функцию в строке «Глобальный режим». Настройка DHCP-сервера состоит из трёх частей: «VLAN», «Исключенный IP» и «Пул».

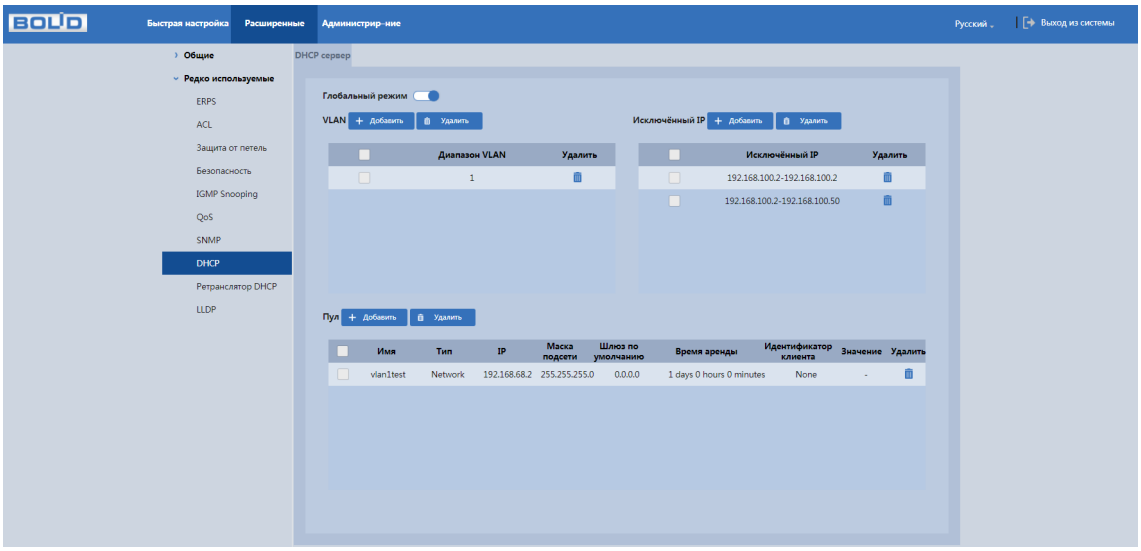


Рисунок 9.26 – Настройка DHCP серверов

9.3.1.2 Добавление VLAN

Укажите диапазон VLAN'ов, в котором DHCP будет включен или отключен.

Нажмите «Добавить» в поле «VLAN», далее введите диапазон VLAN, которые нужно добавить в список.

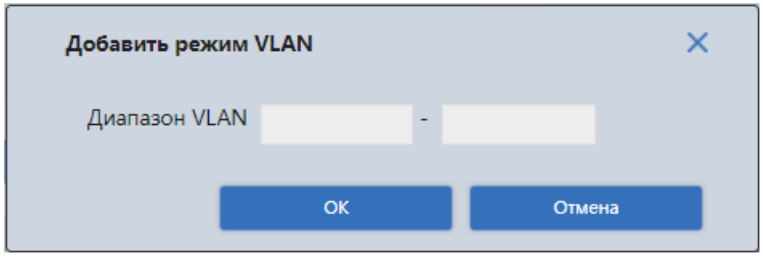


Рисунок 9.27 – Добавить режим VLAN

9.3.1.3 Добавление исключенного IP-адреса

Сохраненные IP-адреса из списка исключенных не будут назначаться DHCP-клиенту.

Нажмите «Добавить» в поле «Исключенный IP», далее введите IP-адрес или диапазон IP, которые нужно добавить в список.

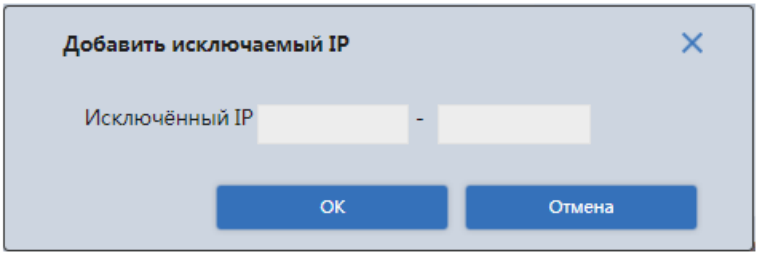


Рисунок 9.28 – Добавить исключаемый IP

9.3.1.4 Добавление DHCP POOL

Настройка DHCP сервера включает в себя определение пула адресов, которые будут раздаваться.

Нажмите «Добавить» в поле «Пул», далее введите данные для добавления (Таблица 9.12).

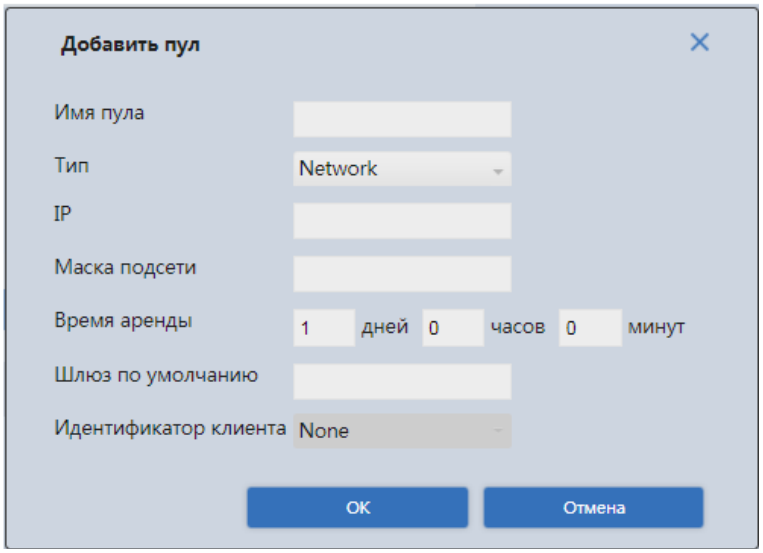


Рисунок 9.29 – Добавить пул

Таблица 9.12 – Добавляемые параметры при добавление пула

Параметр	Функция
Имя пула	Поле для ввода имени пула адресов (при вводе исключите пробелы, например, vlan2_test).
Тип	Из выпадающего списка выберите тип пула адресов: – None – тип не выбран; – Network – данные вводятся для сегмента IP адресов; – Host – данные вводятся для конкретного DHCP клиента, определяемого по аппаратному адресу или идентификатору клиента. Индивидуальные параметры клиента вводятся в строке «Идентификатор клиента».
IP	Поле для ввода IP-адреса хоста или сети.
Маска подсети	Поле для ввода маски подсети хоста или сети.
Время аренды	Поля для ввода времени аренды для выбранного пула адресов.
Шлюз по умолчанию	Поле для ввода шлюза по умолчанию для пула адресов.
Идентификатор клиента	Поле активно при установке «Тип – Host». Из выпадающего списка выберите и введите индивидуальные данные клиента.

10 НАСТРОЙКИ БЕЗОПАСНОСТИ

10.1.1 Безопасность

10.1.1.1 Управление пользователями

На рисунке ниже (Рисунок 10.1) показан интерфейс управления системными параметрами учётной записи пользователя.

Для изменения пароля учётной записи нажмите кнопку в столбце «Изменить».

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 «ОК»

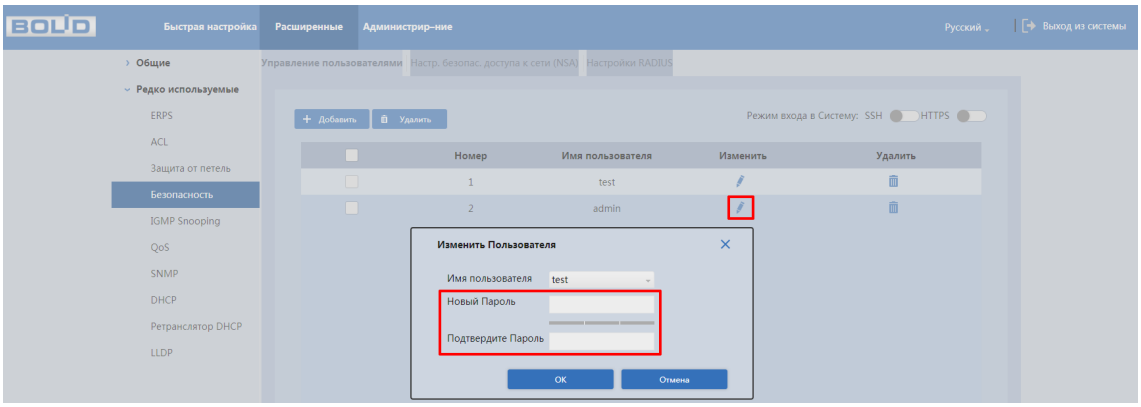


Рисунок 10.1 – Изменение пароля

Для добавления нового пользователя:

1. Нажмите кнопку «Добавить».

2. В появившемся окне введите имя нового пользователя и пароль.

3. Сохраните пользователя.

📖 Добавленный пользователь имеет аналогичные права, что и пользователь admin;

📖 Невозможно удалить пользователя admin.

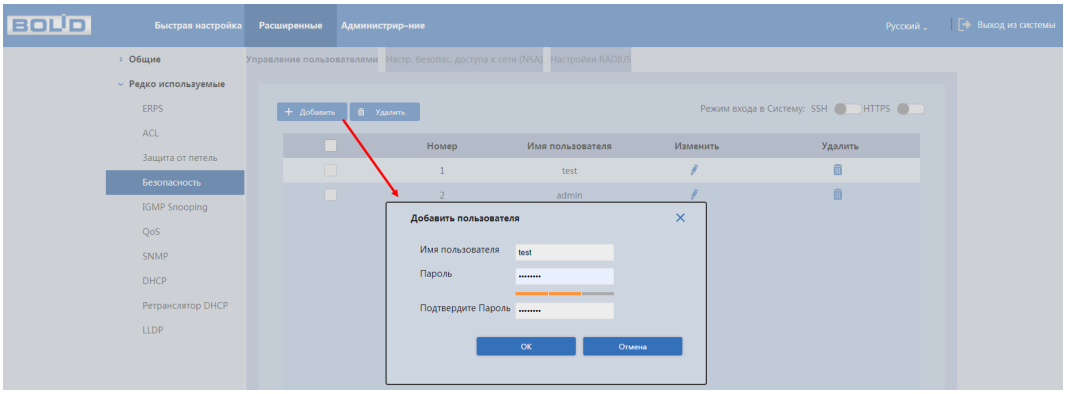


Рисунок 10.2 – Добавление пользователя

10.1.2 802.1X

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.

10.1.2.1 Структура сети 802.1x

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

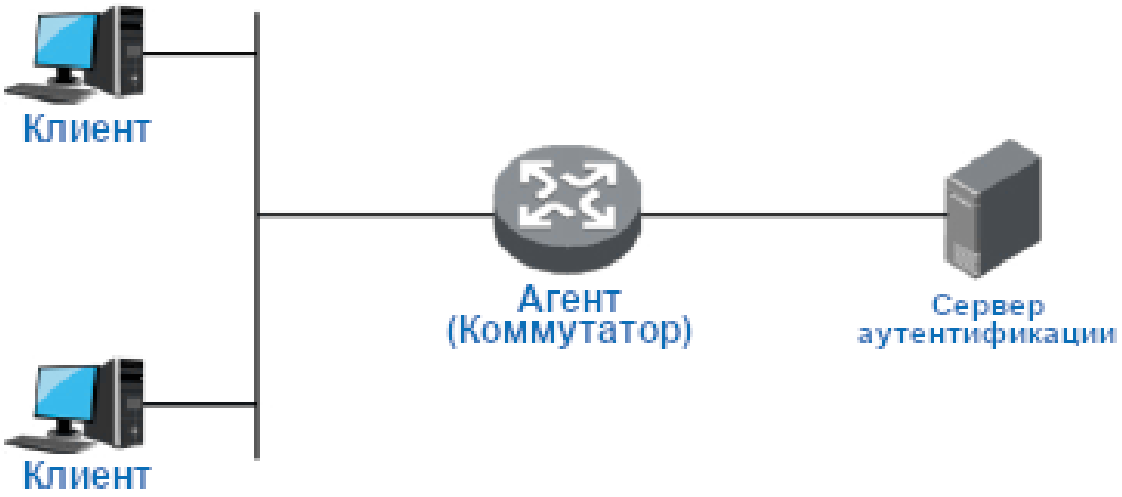


Рисунок 10.3 – Схема

– Клиент (суппликант) – это пользовательское терминальное устройство, требующее доступа к локальной сети, которое аутентифицируется в локальной сети. Клиент должен будет установить программное обеспечение, поддерживающее 802.1x идентификацию;

– Агент (аутентификатор) – это сетевое устройство, которое управляет клиентским доступом в сеть LAN. Оно расположено между клиентами и сервером аутентификации, который предоставляет пользователям порт доступа к локальной сети (физический порт или логический порт) и реализует аутентификацию на подключённом клиенте посредством взаимодействия с сервером;

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

10.1.2.2 802.1x Аутентификация портов

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

– Неконтролируемый порт всегда находится в состоянии двунаправленного соединения, которое используется в основном для передачи пакетов аутентификации. Это необходимо, чтобы клиент всегда мог обмениваться пакетами идентификации;

– Контролируемый порт находится:

– в состоянии двунаправленного соединения после успешной авторизации;

– запрета принимать любые пакеты от клиента в состоянии несанкционированного доступа.

10.1.2.3 Режим запуска аутентификации 802.1x

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

1. Режим активации триггера клиентом:

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

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

2. Режим активации триггера устройством:

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

– Триггер многоадресной рассылки – устройство активно отправляет пакет запроса аутентификации клиенту с регулярным интервалом (по умолчанию – 30 секунд);

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

10.1.2.4 Управление авторизацией порта (NSA)

Это меню позволяет управлять состоянием аутентификации порта. Поддерживается четыре следующих авторизованных состояния:

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

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

– 802.1x на основе порта – 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;

– Авторизация по MAC – означает, что авторизация происходит на базе MAC-адреса. Это не позволяет получить доступ в сеть. Порт будет переключен в авторизованное состояние, если клиент пройдёт проверку подлинности. После этого сможет обмениваться данными в сети.

Пример конфигурации:

– Схема сети:

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

Требуется аутентификация сервером аутентификации при обращении ко всем портам устройства.

Настройка:

1. Переключите все порты в состояние аутентификации «802.1x на основе порта» как показано на рисунке ниже (Рисунок 10.4).

2. Настройте адрес сервера аутентификации, как показано на рисунке ниже (Рисунок 10.5).

10.1.2.5 Настр. безопас. доступа к сети (NSA)

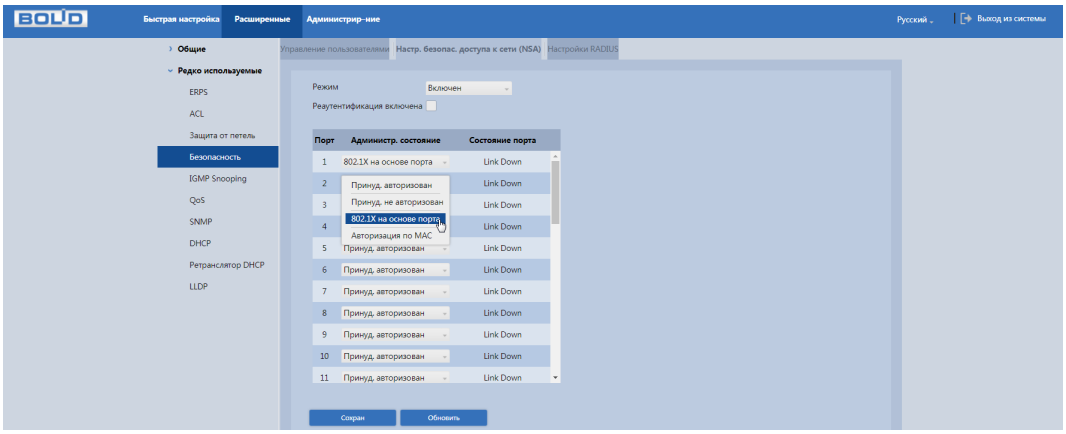


Рисунок 10.4 – Настройка безопасности доступа к сети (NAS)

10.1.2.6 Настройки RADIUS

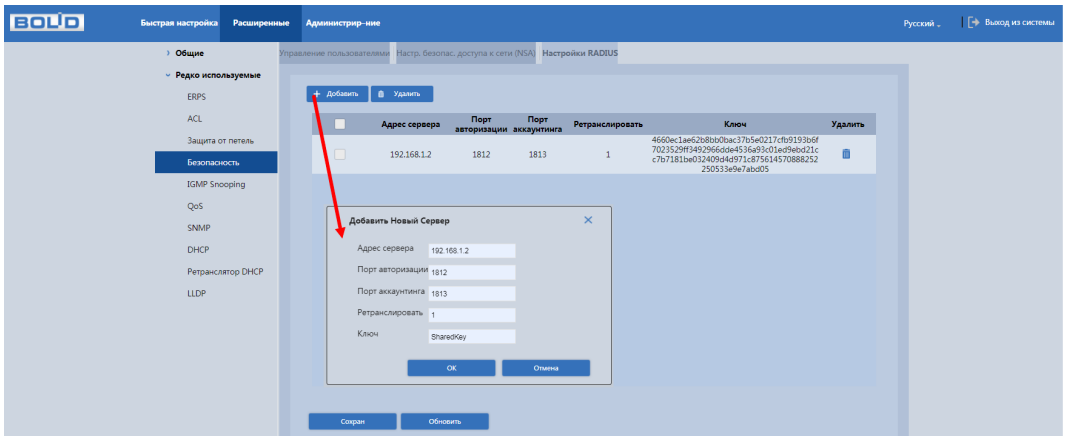


Рисунок 10.5 – Настройки RADIUS

11 ДИАГНОСТИКА И ОБСЛУЖИВАНИЕ

11.1 Расширенные/Общие

11.1.1 Конфигурация

11.1.1.1 Системный журнал

Интерфейс (Рисунок 11.1) предоставляет возможность просмотра и архивации информации из журнала событий регистрации и системных событий устройства.

Для поиска записи необходимо задать начальное и конечное время, выбрать тип события и нажать кнопку «Поиск».

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

Для сохранения журнала событий, необходимо нажать кнопку «Экспорт».

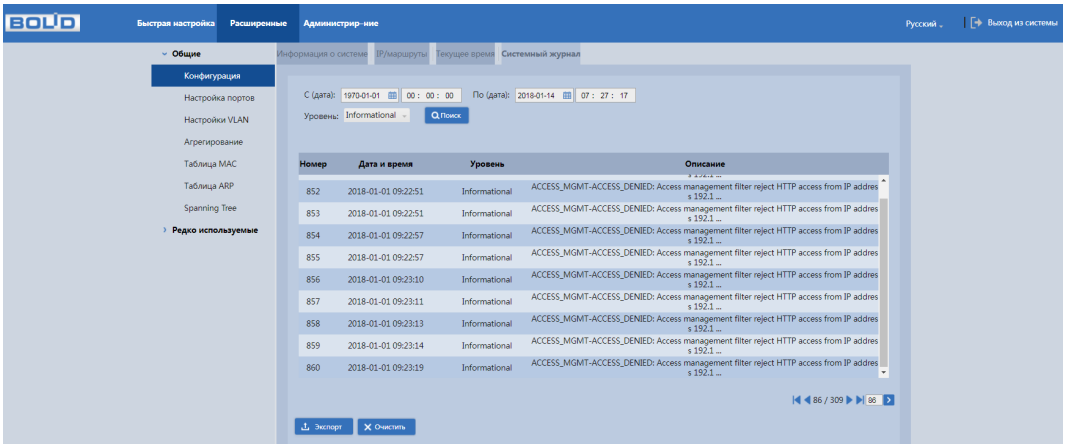


Рисунок 11.1 – Интерфейс просмотра журнала

11.1.2 Настройка портов

Для перехода к информационному окну «Информация о порте» нажмите на номер выбранного порта в столбце «Порт».

Выберите из выпадающего списка параметр «Подробная статистика». В окне будет отображена детальная статистика и информацию для каждого порта коммутатора.

Логическую детальную статистику о переданных/полученных пакетах (Пакеты Tx/Пакеты Rx), количестве принятых/отправленных байтов (Rx/Tx) и о ошибках приёма/передачи (Tx счётчик ошибок/Rx счётчик ошибок).

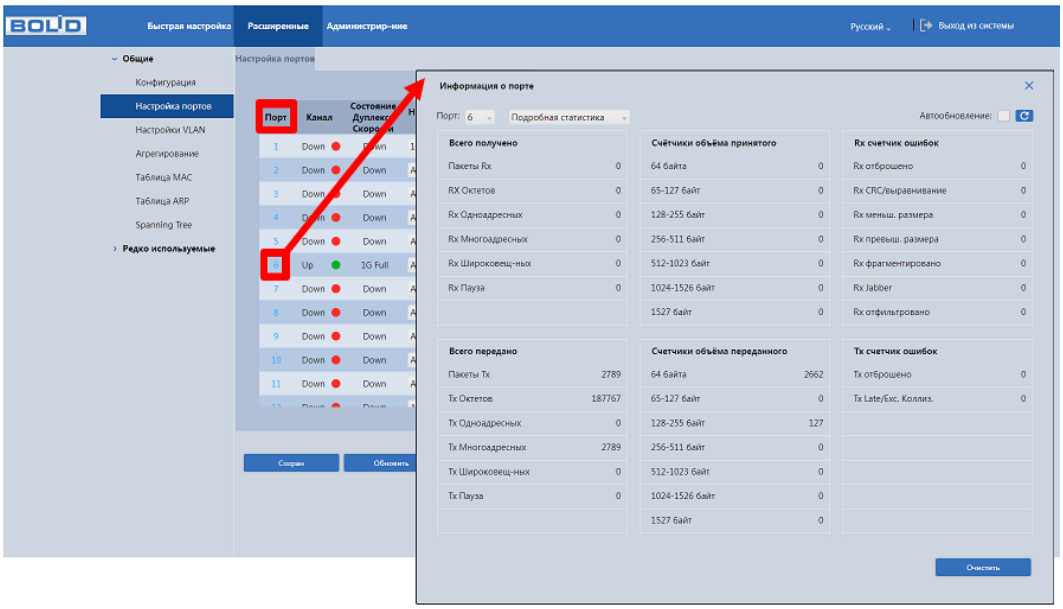


Рисунок 11.2 – Подробная статистика

Выберите из выпадающего списка параметр «Информация о трансивере». В окне будет отображена основная информация о подключенном оптическом модуле (производитель, part номер, серийный номер и т.д); состояние оптической линии, за счёт мониторинга уровней сигналов и прочих параметров оптических передатчиков (DDMI) (напряжение, температура, ток смещения, мощность).

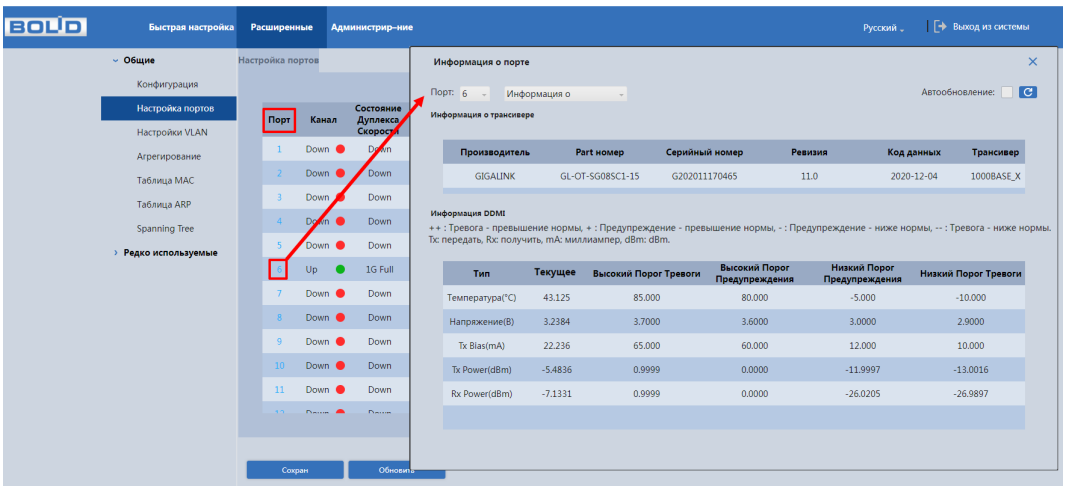


Рисунок 11.3 – Информация о трансивере

11.1.3 Таблица ARP

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.

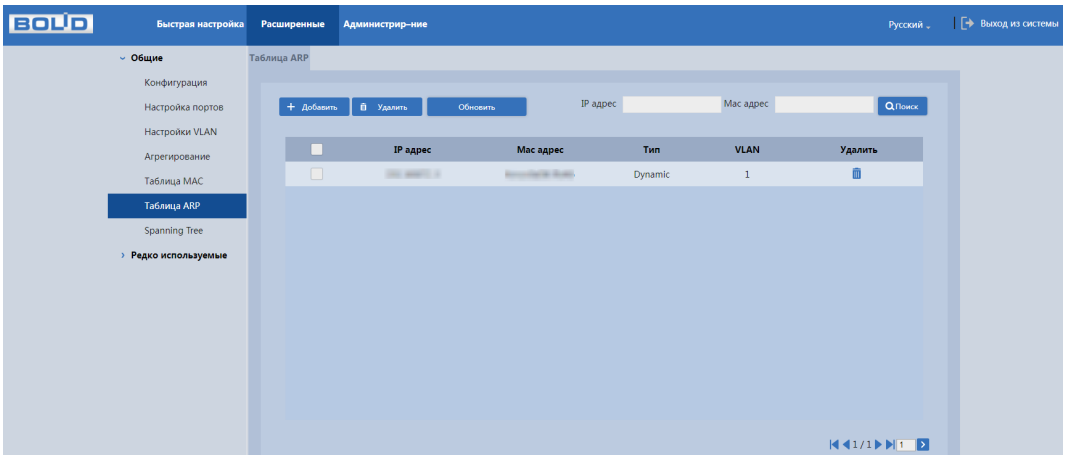


Рисунок 11.4 – ARP-таблица

11.2 Расширенные/Редко используемые

11.2.1 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».

11.2.1.1 Настройки MEP (Maintenance End Points)

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 11.1).

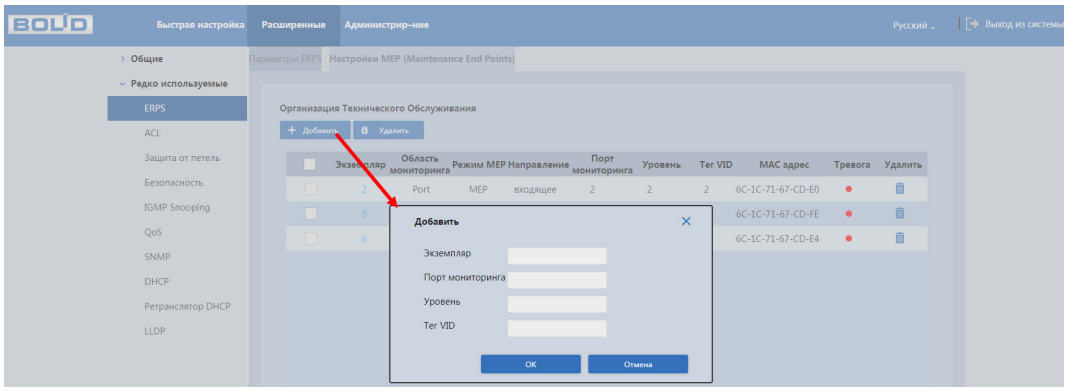


Рисунок 11.5 – Добавление MEP

Таблица 11.1 – Параметры добавление MEP

Параметр	Функция
Экземпляр	Поле ввода номера экземпляра MEP. Доступный диапазон от 1 до 1077.
Порт мониторинга	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.
Тег VIN	Поле ввода ранее настроенного протокола VLAN, например, VLAN 3. Доступный диапазон от 1 до 4094.

Нажмите на цифру в столбце «Экземпляр» для перехода в окно конфигурации MEP (Таблица 11.2).

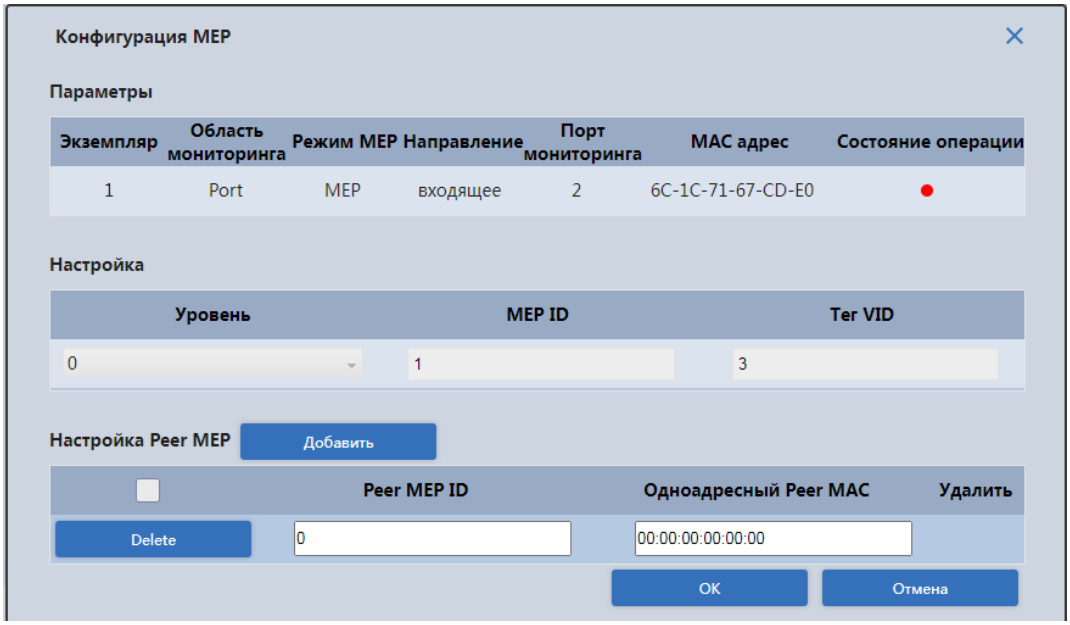


Рисунок 11.6 – Конфигурация MEP

Таблица 11.2 – Параметры настройки MEP

Параметр	Функция	
Параметры	Экземпляр	Панель отображает ранее заданные параметры, более подробно каждый параметр описан в таблице выше (Таблица 11.1).
	Область мониторинга	
	Режим MEP	
	Направление	
	Порт мониторинга	
	MAC адрес	
	Состояние операции	
Настройка	Уровень	Выберите из выпадающего списка уровень MGP настраиваемого MEP.
	MEP ID	Идентификатор MEP.
	Тег VID	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.
Настройка Peer MEP	Peer MEP ID	Идентификатор одноранговой MEP целевого MEP. Используется только, когда одноадресный MAC-адрес одноранговой устройства состоит из одних нулей.

Параметр	Функция	
	Одноадресный Peer MAC	Отображается одноадресный MAC-адрес одноранговое устройства состоит из одних нулей. (MAC-адрес одноадресного одноранговое 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 одноранговое 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 одноранговое устройства)» одни нули, то есть «00:00:00:00:00:00».
	Удалить	Нажмите кнопку «Delete» для удаления созданного «Peer MEP»

11.2.1.2 Параметры ERPS

Для добавления экземпляра ERPS нажмите кнопку «+Добавить». В появившемся окне введите параметры для создаваемого ERPS (Таблица 11.3).

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

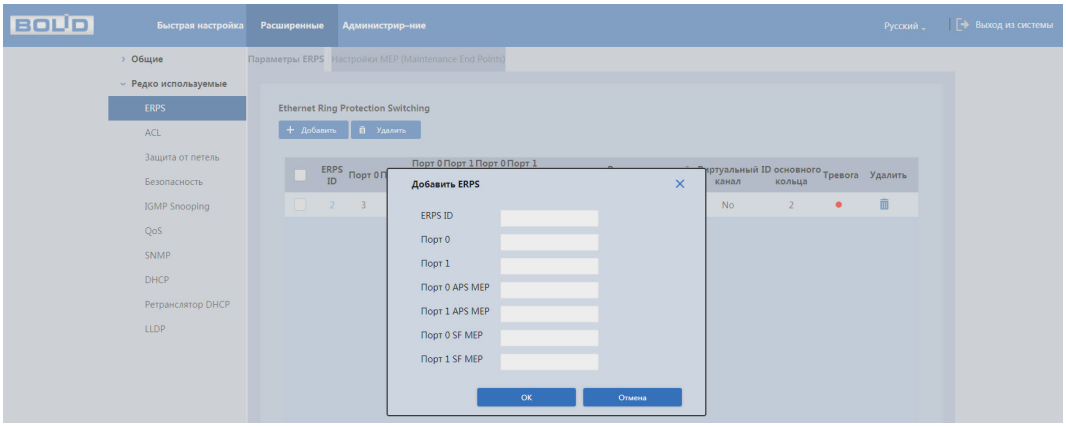


Рисунок 11.7 – Добавление ERPS

Таблица 11.3 – 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 11.8).
Порт 0 (Запад/ WEST порт)	Поле ввода выбранного порта коммутатора для выполнения роли «Port 0» в топологии ERPS. Только один порт коммутатора может быть выбран для выполнения роли ERPS Port 0.
Порт 1 (Восток/ EAST порт)	Поле ввода выбранного порта коммутатора для выполнения роли «Port 1» в топологии ERPS. Только один порт коммутатора может быть выбран для выполнения роли ERPS Port 1.
Порт 0 APS MEP	PDU порта 0 APS MEP.
Порт 1 APS MEP	PDU порта 1 APS MEP. Поскольку только один APS MEP связан со взаимосвязанным вспомогательным кольцом без виртуального канала, он настроен как «0» для таких экземпляров кольца. «0» в этом поле указывает, что с этим экземпляром не связан порт 1 APS MEP.
Порт 0 SF MEP	Порт 0 SF MEP сообщает об обнаружение сбоя.
Порт 1 SF MEP	Порт 1 SF MEP сообщает об обнаружение сбоя. Поскольку только один SF MEP связан с взаимосвязанным субкольцом без виртуального канала, он настроен как «0» для таких случаев вызова.

Нажмите на цифру в столбце «ERPS ID» для перехода к окну настройки экземпляра ERPS (Таблица 11.4).

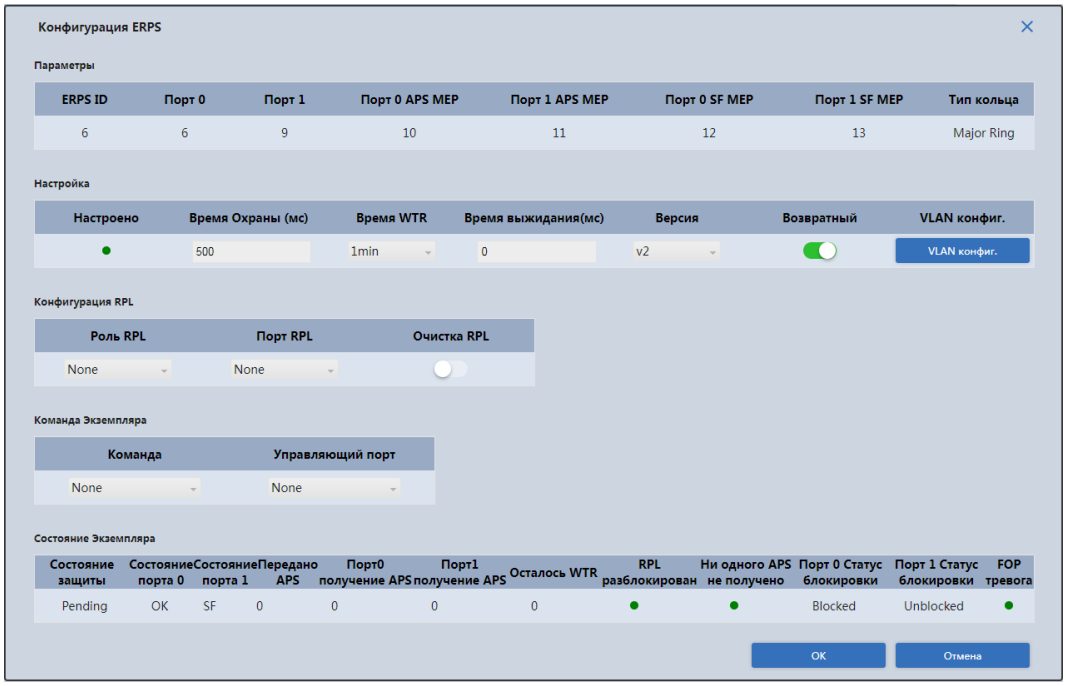
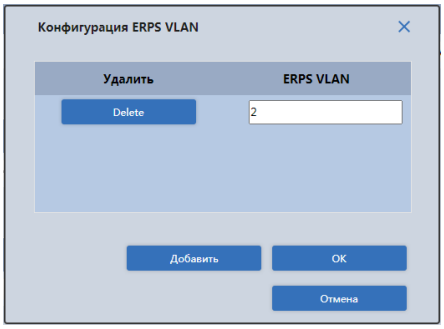


Рисунок 11.8 – Настройка экземпляра ERPS

Таблица 11.4 – Параметры конфигурации ERPS

Параметр	Функция	
Параметры	ERPS ID	Панель отображает ранее заданные параметры, более подробно каждый параметр описан в таблице выше (Таблица 11.3).
	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.
	Настроено	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

Параметр	Функция	
Настройка (Настройка экземпляра)		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 обойдет все кольцо. По умолчанию значение – 500 мс.
	Время WTR (Wait to restore)	Из выпадающего списка выберите время до восстановления R-APS. Параметр нужен для того, чтобы предотвратить частое переключение RPL порта, если соединение на каком-то участке кольца очень часто меняет состояние. Таймер используется только узлом RPL_Owner. Доступный диапазон значений 1 – 12 мин, по умолчанию значение – 1 мин.
	Время выжидания (мс) (Hold-Off Time)	Поле ввода времени между тем как узел обнаружил аварию на одном из своих соединений до отправки им сообщения Signal Fail (SF). Диапазон значений от 0 до 10 секунд с шагом в 100 мс. По умолчанию значение – 0.
	Версия	Из выпадающего списка выберите версию протокола ERPS: v1 – поддерживает топологию с одним кольцом; v2 – поддерживает топологию с несколькими кольцами/многозвенной схемой.
	Возвратный (реверсивный)	Поставьте переключатель в зависимости от настроек в состояние Вкл./Выкл. – реверсивный режим ERPS отключен;  – реверсивный режим ERPS включен.

<table>
<tr><th>Параметр</th><th colspan="2">Функция</th></tr>
<tr><td>Настройка (Настройка экземпляра)</td><td>VLAN конфиг.</td><td>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.
 
</td></tr>
<tr><td rowspan="3">Конфигурация RPL (Ring Protection Link/Канал защиты кольца)</td><td rowspan="2">Роль RPL</td><td>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.</td></tr>
<tr><td>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>RPL_Neighbour – коммутатор назначается «соседом (соседний узел кольца)» RPL для кольца. Отвечает за блокировку своего конца RPL в нормальных условиях.</td></tr>
<tr><td>Порт RPL</td><td>None – порт не выбран.</td></tr>
</table>

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

<table>
<tr><th>Параметр</th><th colspan="3">Функция</th></tr>
<tr><td rowspan="3"></td><td></td><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="10">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>
<tr><td>RPL разблокирован</td><td colspan="2">Точки доступа принимаются в рабочем потоке.</td></tr>
<tr><td>Ни одного APS не получено</td><td colspan="2" rowspan="3">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.</td></tr>
<tr><td>Порт 0 статус блокировки</td></tr>
<tr><td>Порт 1 статус блокировки</td></tr>
<tr><td>FOP тревога</td><td colspan="2">Сбой состояния протокола (FOP).</td></tr>
</table>

11.3 Расширенные

11.3.1 Редко используемые

11.3.1.1 LLDP

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.

На представленном интерфейсе (Рисунок 11.9) установите из выпадающего списка режим отправки и приёма на канал.

– Enable – включить передачу;

– Disable – отключить передачу;

– Tx only – пакеты, исходящие с этого порта будут отправлены на оборудование, работающее в локальной сети;

– Rx only – пакеты, полученные на этом порте, будут отправлены на оборудование, работающее в локальной сети.

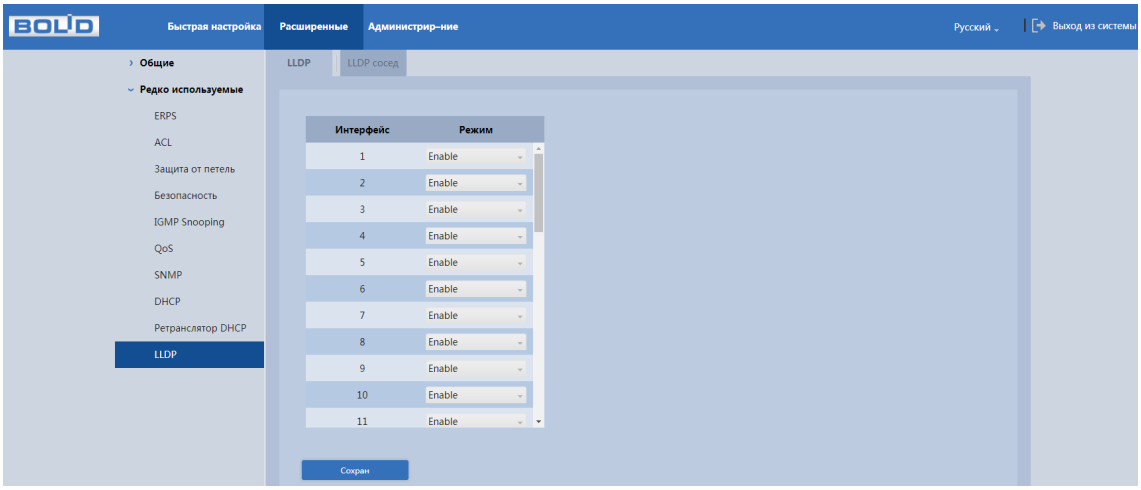


Рисунок 11.9 – Включение LLDP

LLDP сосед

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

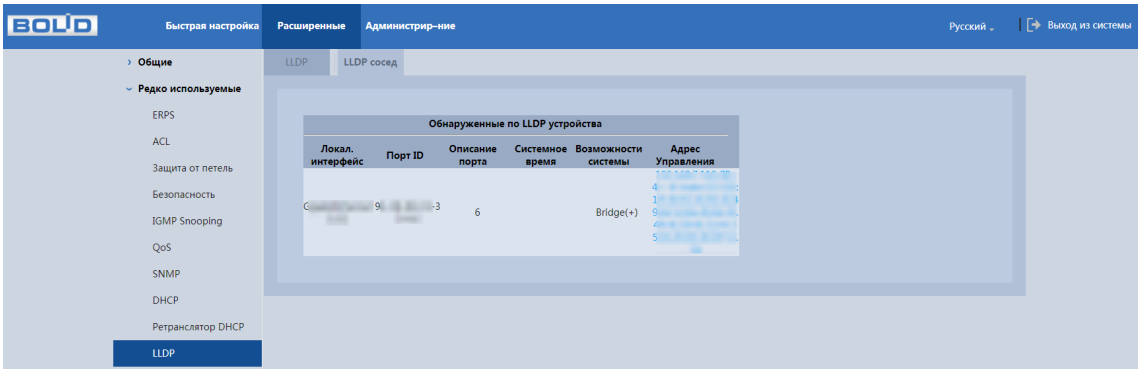


Рисунок 11.10 – Обнаружение по LLDP

11.3.2 Таблица ARP

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.

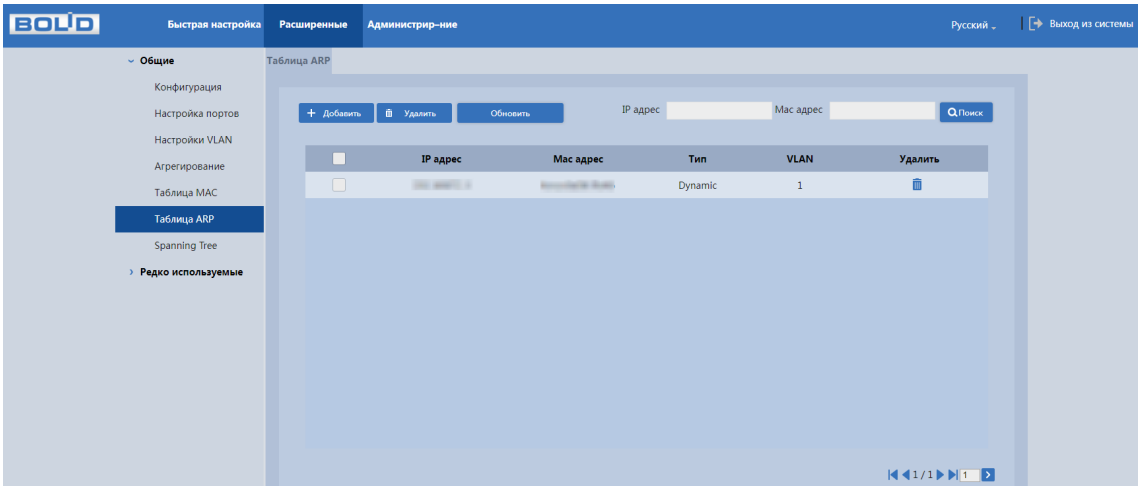


Рисунок 11.11 – ARP-таблица

11.4 Администрир-ние

11.4.1 Перезагрузка системы

Нажмите кнопку «Перезагрузить» для программной перезагрузки устройства.

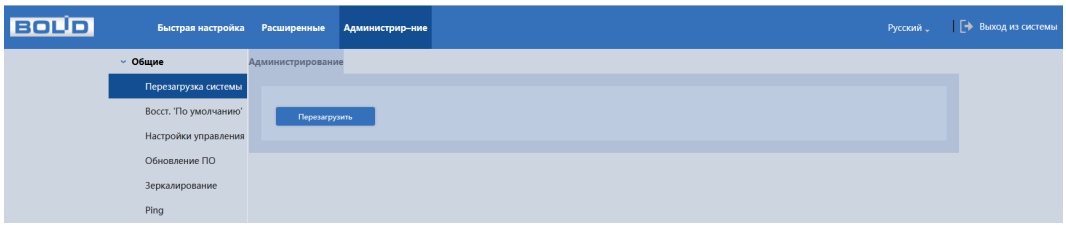


Рисунок 11.12 – Интерфейс программной перезагрузки устройства

11.4.2 Восст. «По умолчанию»

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

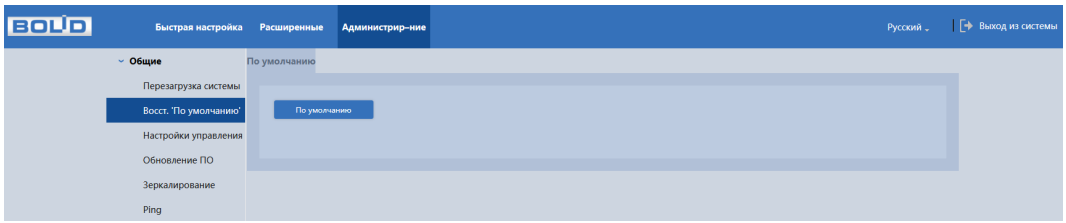


Рисунок 11.13 – Сброс параметров

11.4.3 Заводские настройки

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

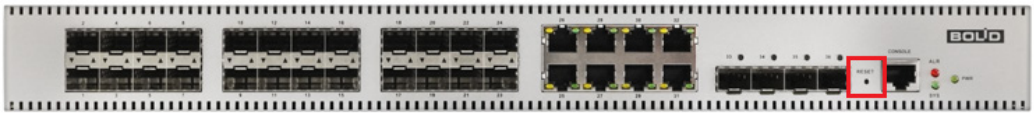


Рисунок 11.14 – Сброс параметров

Для сброса:

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». Процедура сброса до заводских настроек завершена.

11.4.4 Настройки управления

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

11.4.4.1 Импорт настроек

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

2. Нажмите кнопку «Импорт настроек» и перезагрузите устройство.

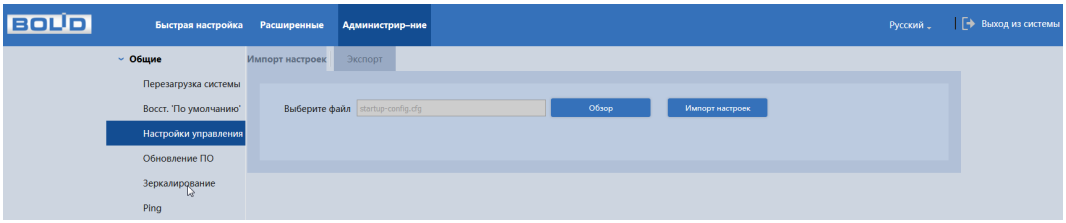


Рисунок 11.15 – Импорт

11.4.4.2 Экспорт

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

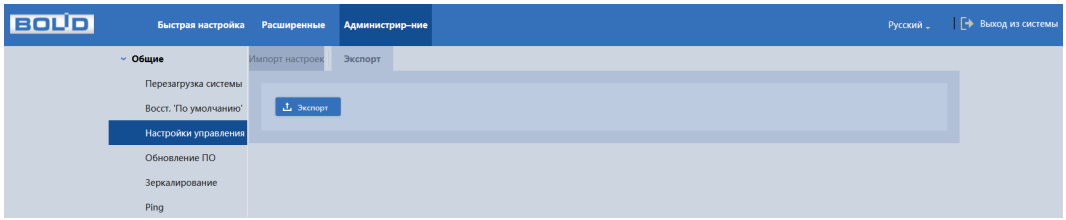


Рисунок 11.16 – Экспорт

11.4.5 Обновление ПО

Для обновления ПО необходимо импортировать файл прошивки на устройство и нажать кнопку «Прошивка» для сохранения.

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

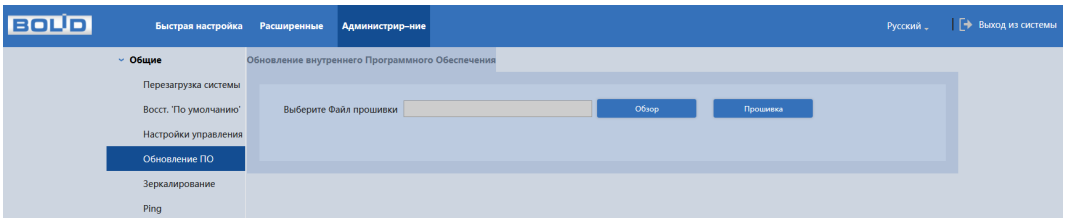


Рисунок 11.17 – Обновление ПО

11.4.6 Зеркалирование

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

1. Из выпадающего списка в строке «Режим» выбрать:

– Отключен – функция зеркалирования отключена;

– Включен – функция зеркалирования включена.

2. Выберите порт назначения для зеркалирования.

3. Из выпадающего списка выберите «Disabled» и установите галочку в столбце «Назначение».

📖 Возможно зеркалировать только на 1 порт.

4. Далее выберите порты, с которых будет зеркалироваться пакеты, и установите режим передачи копий пакетов.

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

– Both – и полученные и исходящие пакеты посылаются на назначенный порт (порт-зеркало);

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

– Rx only – пакеты, полученные на этот порт, будут отправлены на назначенный порт (порт-зеркало). Исходящие пакеты зеркалироваться не будут.

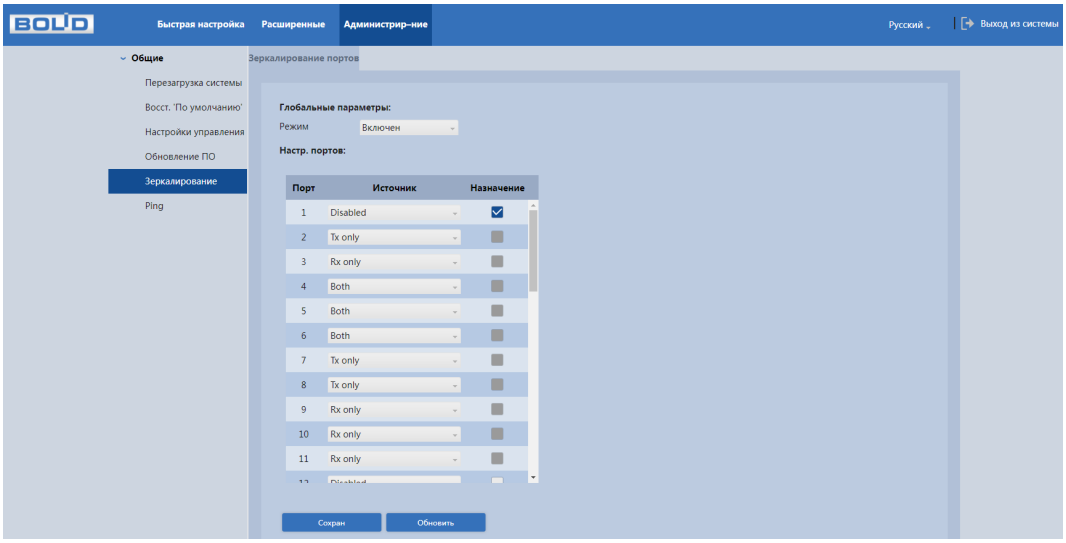


Рисунок 11.18 – Зеркалирование трафика

11.4.7 Ping

Введите IP-адрес целевого устройства для проверки времени отклика и доступности.

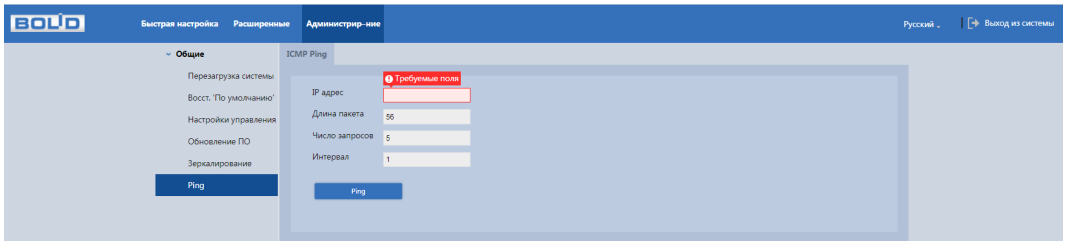


Рисунок 11.19 – ICMP Ping

12 РАБОТА С УТИЛИТОЙ «BOLID VIDEOSCAN»

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

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

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

Выполнив запуск утилиты BOLID VideoScan, в открывшемся окне визуального интерфейса пункта меню «Сеть» измените IP-адрес изделия и нажмите кнопку «Сохранить». На рисунке (Рисунок 12.1) представлены базовые параметры для изменения.

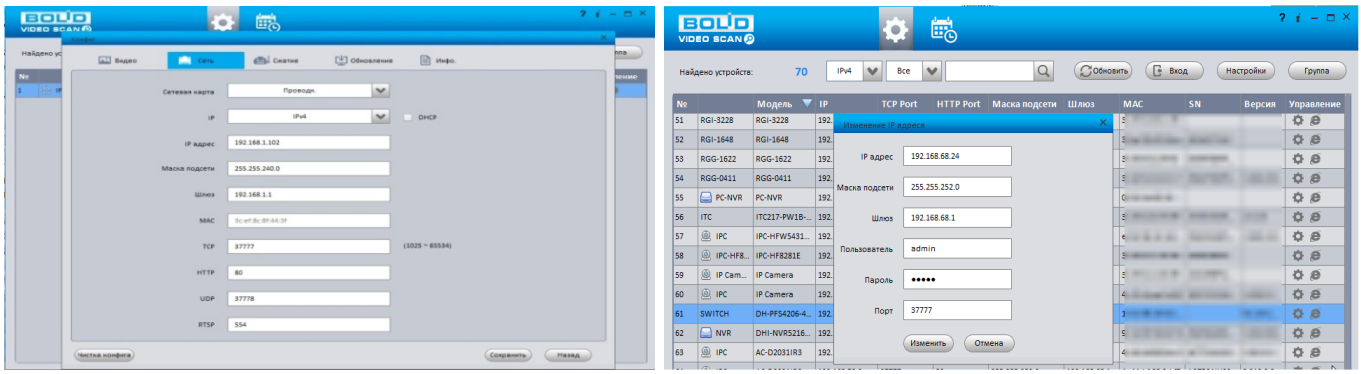


Рисунок 12.1 – Работа с BOLID VideoScan

13 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.

14 ВОЗМОЖНЫЕ НЕИСПРАВНОСТИ И СПОСОБЫ ИХ УСТРАНЕНИЯ

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

Перечень неисправностей и способы их устранения представлены в таблице ниже (Таблица 14.1).

Таблица 14.1 – Перечень возможных неисправностей

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

15 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.

16 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.

17 УПАКОВКА

Изделие и эксплуатационная документация упакованы в картонную коробку.

18 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.

19 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.

20 УТИЛИЗАЦИЯ

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

Содержание драгоценных материалов: не требует учёта при хранении, списании и утилизации (п. 1.2 ГОСТ 2.608-78).

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

21 ГАРАНТИИ ИЗГОТОВИТЕЛЯ

Гарантийный срок эксплуатации – 36 месяцев с даты приобретения.

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

22 СВЕДЕНИЯ О СЕРТИФИКАЦИИ

Изделие соответствует требованиям технического регламента Таможенного союза ТР ТС 004/2011 «О безопасности низковольтного оборудования и имеет декларацию о соответствии N RU Д-RU.PA02.B.95113/21.

Изделие соответствует требованиям технического регламента Таможенного союза ТР ТС 020/2011 «Электромагнитная совместимость технических средств» и имеет декларацию о соответствии N RU Д-RU.PA12.B.21417/25.

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.

23 СВЕДЕНИЯ О ПРИЁМКЕ

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 рисунков

Перечень таблиц

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

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

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