OSNOVO
cable transmission

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

Уличный управляемый (L2+) коммутатор
Gigabit Ethernet на 20 портов

SW-71604/WL

Прежде чем приступать к эксплуатации изделия,
внимательно прочтите настоящее руководство

www.osnovo.ru

Оглавление

1. Назначение 6

2. Комплектация* 7

3. Особенности оборудования 7

4. Внешний вид и описание элементов 8

4.1 Внешний вид 8

4.2 Описание элементов уличного коммутатора 8

5. Установка и подключение 11

6. Проверка работоспособности системы 13

7. Подготовка перед управлением коммутатором через WEB-интерфейс 14**

8. Управление через WEB интерфейс, основные элементы 17

8.1 WEB интерфейс, общая информация 17

8.2 System (Системная информация) 21

8.3 IPv4 Settings (Настройки протокола IPv4) 22

8.4 IPv6 Settings (Настройки протокола IPv6) 23

8.4.1 Настройка IPv6 23

8.4.2 IPv6 Neighbor Table (Таблица «соседей» IPv6) 24

8.5 System Time (Системное время) 25

8.5.1 Настройка системного времени 25

8.6 RSTP Configuration (Настройка протокола RSTP) 27

8.6.1 Конфигурирование RSTP. Базовая информация 27

8.6.2 Настройка RSTP для портов 28

8.6.3 RSTP Status 30

8.7 ERPS (Протокол защиты трафика от петель в кольцевой топологии) 33

8.7.1 Настройка ERPS 33

8.8 SNMP (простой протокол сетевого управления).....35
8.8.1 Настройка SNMP сервера.....36
8.8.2 Настройка SNMP Trap 38
8.9 DHCP (Настройка протокола DHCP).....40
8.9.1 Настройка DHCP клиента.....41
8.9.2 Настройка информации DHCP сервера.....42
8.9.3 Настройка привязки информации к DHCP серверу 43
8.9.4 Настройка DHCP relay информации 44
8.11 ModBUS/TCP (Настройка промышленного протокола ModBUS/TCP).....45
8.11.1 Формат данных протокола Modbus/TCP 46
8.11.2 Обработка данных в Modbus/TCP 46
8.11.3 Настройка работы Modbust/TCP протокола.....49
8.12 UPnP (набор протоколов Universal Plug and Play) 50
8.12.1 Настройка UPnP 50
8.13 Port Management (Управление портами) 50
8.13.1 Настройка портов 51
8.13.2 Статус портов 53
8.14 IGMP Snooping (Управление multicast рассылкой) 54
8.14.1 Настройка IGMP Snooping 55
8.14.2 Таблица IGMP Snooping.....56
8.15 IEEE 802.1Q VLAN (Логическая «виртуальная» локальная сеть) ..56
8.15.1 VLAN Q-in-Q 57
8.15.2 Настройка 802.1Q VLAN.....57
8.15.3 Таблица VLAN.....58

8.15.4 Настройка VLAN PVID и Accept Type 59
8.15.5 Настройка VLAN Q-in-Q 60
8.16 QoS (Quality of Service) 63
8.16.1 Настройка QoS 63
8.16.2 Настройка режима Trust для QoS и CoS по умолчанию 64
8.16.3 Настройка CoS 65
8.16.4 Настройка ToS (DSCP) 66
8.17 Port Trunk (агрегация каналов) 67
8.17.1 Настройка функции Port Trunk 68
8.17.2 Статус функции Port Trunk 69
8.18 Storm Control (Защита от широковещательного шторма 70
8.18.1 Настройка функции Storm Control 70
8.19 Port-Based Network Control IEEE 802.1X (контроль доступа и аутентификации) 71
8.19.1 Базовая настройка 802.1X 71
8.19.2 Настройка 802.1X для портов 72
8.19.3 Настройка локальной базы данных 73
8.19.4 Настройка сервера RADIUS 74
8.20 Port Mirroring (Зеркалирование портов) 75
8.20.1 Настройка функции Port Mirroring 75
8.21 Ping (команда PING) 76
8.21.1 Использование команды PING с IPv4/IPv6 76
8.22 LLDP (функция оповещения «соседей») 77
8.22.1 Настройка LLDP 77
8.22.2 LLDP таблица «соседей» 78

8.23 System Warning (Системные оповещения) 79
8.23.1 Настройка системных оповещений 79
8.23.2 Журнал системных событий 80
8.23.3 Настройка SMTP Информации 81
8.23.4 Настройка выбора событий 83
8.24 MAC Table (Таблица MAC адресов) 85
8.24.1 Настройка постоянных (static) MAC адресов 85
8.24.2 Таблица MAC адресов 86
8.25 Authorization (Вход в систему управления коммутатором) 87
8.25.1 Настройка информации для входа в систему 87
8.26 Firmware Upgrade (Обновление прошивки) 88
8.26.1 Загрузка файла с прошивкой 89
8.26.2 Процесс загрузки файла с прошивкой в коммутатор 89
8.26.3 Копирование файла с прошивкой с USB накопителя 91
8.27 Config Backup (Создание резервной копии настроек) 92
8.27.1 Сохранение резервного файла с настройками 92
8.28 Config Restore (Восстановление настроек из файла) 93
8.28.1 Восстановление настроек из файла 93
8.29 USB Auto-Load & Auto – Backup (Функция автоматического сохранения/загрузки настроек) 94
9. Технические характеристики* 95
10. Гарантия 98
11. Приложение А «Габаритные размеры» 99
12. Приложение Б «Крепления на стену / на опору» 100

1. Назначение

Уличный управляемый (L2+) коммутатор Gigabit Ethernet на 20 портов SW-71604/WL предназначен для объединения сетевых устройств и передачи данных между ними в условиях эксплуатации вне помещений.

В основе устройства лежит высоконадежное промышленное оборудование с расширенным диапазоном температур:

1) Промышленный управляемый коммутатор SW-71604/WL;
2) Блок питания на AC100-240V / DC48V в промышленном исполнении.

Кроме того, уличный коммутатор SW-71604/WL оснащен оптическим кроссом для удобного подключения оптоволоконного кабеля.

Уличный коммутатор SW-71604/WL оснащен 16 Gigabit Ethernet (10/100/1000Base-T) портами к каждому из которых можно подключать сетевые устройства на скорости до 1000 Мбит/с.

Помимо этого, в уличном коммутаторе SW-71604/WL предусмотрено 4 SFP порта (1000Base-X) – для обеспечения связи по оптоволоконному кабелю на скорости до 1 Гбит/с. Для связи по оптоволоконному кабелю необходимо использовать промышленные SFP модули со скоростью 1,25 Гбит/с (не входят в комплект поставки).

Уличный коммутатор SW-71604/WL настраивается через WEB-интерфейс и имеет множество функций L2, L2+ уровня, таких как VLAN, QOS, LACP, SNMP, IGMP Snooping и др.

Высокая надежность сети, построенной на базе уличных коммутаторов SW-71604/WL достигается за счет использования RSTP, MSTP (протоколы быстрого развертывания дерева, защита от сетевых петель) и ERPS (топология «кольцо»).

Кроме того, уличный коммутатор SW-71604/WL распознает тип подключенного сетевого устройства и при необходимости меняют контакты передачи данных (Auto Negotiation), что позволяет использовать кабели, обжатые любым способом (кроссовые и прямые).

Конструктивно уличный коммутатор SW-71604/WL представляет собой пластиковый бокс со степень защиты IP65 с установленной в нем монтажной панелью, на которой смонтированы промышленный коммутатор, промышленный блок питания и пластиковый оптический кросс.

В уличном коммутаторе SW-71604/WL предусмотрена функция резервного питания (если необходимо), а также реализована функция оповещения с помощью релейного выхода (1A, DC24V).

Уличный коммутатор SW-71604/WL с успехом может быть использован в самых различных сферах применения (видеонаблюдение, организация сети и тд.), где требуется объединить до 20 сетевых устройств в одну сеть в условиях эксплуатации вне помещений.

2. Комплектация*

SW-71604/WL

1. Уличный коммутатор SW-71604/WL – 1шт;
2. Оптическая розетка – 1шт;
3. Пигтейлы SM SC/UPC – 4шт;
4. КДЗС – 4шт;
5. Краткое руководство по эксплуатации –1шт;
6. Герметизирующая резинка под крышку бокса – 1шт;
7. Упаковка – 1шт.

3. Особенности оборудования

- Уличное исполнение – диапазон рабочих температур - 40…+50°C, степень защиты IP65;
- 16 коммутируемых Gigabit Ethernet (10/100/1000Base-T) портов;
- 4 SFP порта (1000Base-X) – для передачи Ethernet по оптике с помощью SFP-модулей (в комплект не входят);
- Поддержка функций L2, L2+ уровня (VLAN, QOS, SNMP, IGMP Snooping и тд);
- Настройка и управление через WEB-интерфейс/Telnet/SNMP;
- Высокая надежность сети (RSTP, MSTP, ERPS, LACP);
- Автоматическое определение MDI/MDIX;
- Размер таблицы MAC-адресов: 16К;
- Размер буфер пакетов: 12 МБ;
- Пропускная способность коммутационной матрицы: 40 Гбит/с.
- Резервное питание;
- Система оповещения (релейный выход 1A, DC24V).

4. Внешний вид и описание элементов

4.1 Внешний вид

Рис.1 Коммутатор SW-71604/WL, внешний вид

4.2 Описание элементов уличного коммутатора

Рис.2 Уличный коммутатор SW-71604/WL, основные элементы

Таб.1 Уличный коммутатор SW-71604/WL , назначение основных элементов

№ п/п	Назначение
1	Пластиковый оптический кросс, предназначен для удобного подключения оптоволоконного кабеля, укладки и хранения его части внутри себя.
2	Промышленный блок питания AC 100-240V / DC 48V, 1A. Предназначен для питания промышленного коммутатора (3)
3	Промышленный управляемый коммутатор SW-71604/IL на 20 портов. Предназначен для организации сети. Питается от блока питания (2)
4	Металлическая пластина размером. На ней крепятся все основные элементы уличного коммутатора SW-71604/WL внутри пластикового бокса (5)
5	Пластиковый бокс 300x230x111мм (ШхВхГ). В нем смонтированы все элементы уличного коммутатора SW-71604/WL на металлической пластине (4). Обладает степенью защиты IP65.
6	Набор гермовводов внутренним диаметром Ø 4-8мм (1шт), Ø 3-6мм (20шт)

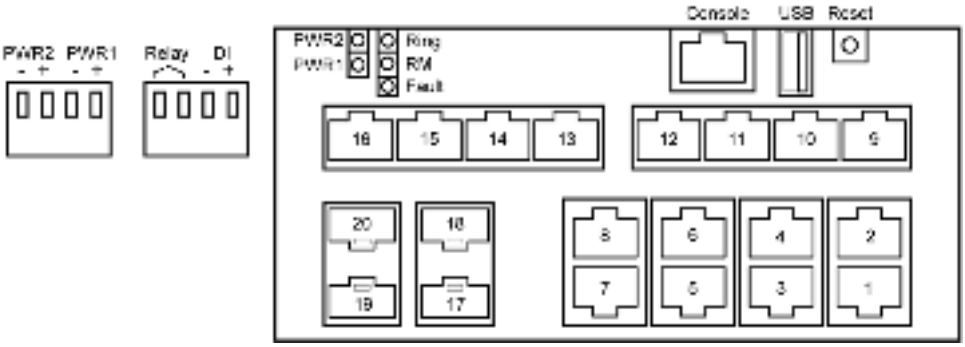


Рис. 3 Уличный коммутатор SW-71604/WL, разъемы кнопки и индикаторы

Таб. 2 Уличный коммутатор SW-71604/WL, назначение разъемов, кнопок и индикаторов

Обозначение	Назначение
PWR2 - +	Часть клеммной колодки для подключения 2го БП DC 12-48V
PWR1 - +	Часть клеммной колодки для подключения 1го БП DC 12-48V. К ней по умолчанию подключен промышленный блок питания AC 100-240V / DC 48V, 1A
Relay	Клеммная колодка релейного выхода 1A DC 24V
DI - +	Клеммная колодка, используется для подключения датчика (фотодатчик, датчик влажности и тд)
PWR1 PWR2	LED индикаторы подключения блоков питания (основного и резервного) Горит – блок питания подключен Не горит – блок питания не подключен/не исправен
RNG	LED индикатор топологии «кольцо» Горит – коммутатор включен в сеть по топологии «кольцо» Мигает – топология «кольцо» используется, но не работает должным образом
RM	LED индикатор работы устройства в режиме Ring Master (используется в топологии «кольцо») Горит зеленым – устройство работает в режиме Ring Master Не горит – устройство не работает в режиме Ring Master
Fault	LED индикатор ошибки Горит зеленым – коммутатор работает в штатном режиме Горит красным – ошибка
Console	Консольный порт RJ-45 используется для управления коммутатором
USB	USB порт используется для оперативной загрузки конфигурации или прошивки

Reset	Короткое нажатие (1сек) – сохраняет текущую конфигурацию на USB носитель с именем «running config» Среднее нажатие (~4сек) – перезагрузка коммутатора Долгое нажатие (>7сек) – возврат к заводским
1-16	Разъемы RJ-45 для подключения сетевых устройств на скорости 10/100/1000 Мбит/с с помощью кабеля витой пары. LED индикаторы скорости подключения. Горит желтым – подключено устройство на скорости 10/100 Мбит/с Горит зеленым – подключено устройство на скорости 1000 Мбит/с
17 18 19 20	SFP порты для подключения сетевых устройств с оптическими портами на скорости 1Гбит/с (SFP модули в комплект поставки не входят) с помощью оптоволоконного кабеля.

5. Установка и подключение

Подключение уличного коммутатора SW-71604/WL осуществляется в следующей последовательности:

1. Проденьте кабели витой пары через соответствующие отверстия гермовводов снаружи внутрь бокса.

2. Обожмите концы кабелей с внутренней стороны бокса разъемами RJ45 (рис. 4)

Рис. 4 Обжимка кабеля витой пары разъемами RJ-45

3. Подключите обжатые разъемами RJ-45 кабели к коммутатору и затяните гермовводы. Для обеспечения защиты от проникновения влаги внутрь корпуса, кабели должны быть плотно укреплены в гермовводах.

5. Аналогично пункту 1 протяните кабель питания от сети AC 100-240V внутрь корпуса через соответствующий гермоввод (Ø 4-8мм), подключите кабель питания к контактам **L (фаза)** и **N (ноль) и «земля»** встроенного промышленного блока питания. Затяните гермоввод.

6. Зачистите оптические кабели на длину 25-30 см, пропустите их в отверстия гермовводов, затяните резьбу гермовводов так, чтобы кабели жестко фиксировались в зажимах гермовводов.

7. Соблюдая все требования технологии сварки оптоволоконного кабеля, приварите пигтейлы (имеются в комплекте) к оптоволоконным жилам кабелей. Уложите оптоволоконный кабель в пазы кросса, следя за тем, чтобы диаметр колец не был менее 60 мм. Подключите разъемы пигтейлов к SFP модулям (не входят в комплект поставки) установленным в SFP разъемы коммутатора. Закройте крышку оптического кросса.

8. Поместите герметизирующую резинку из комплекта поставки в паз по периметру крышки пластикового бокса, избыточную длину отрежьте. Аккуратно закройте крышку, затяните ее 4-мя винтами из комплекта поставки. Уличный коммутатор готов к эксплуатации.

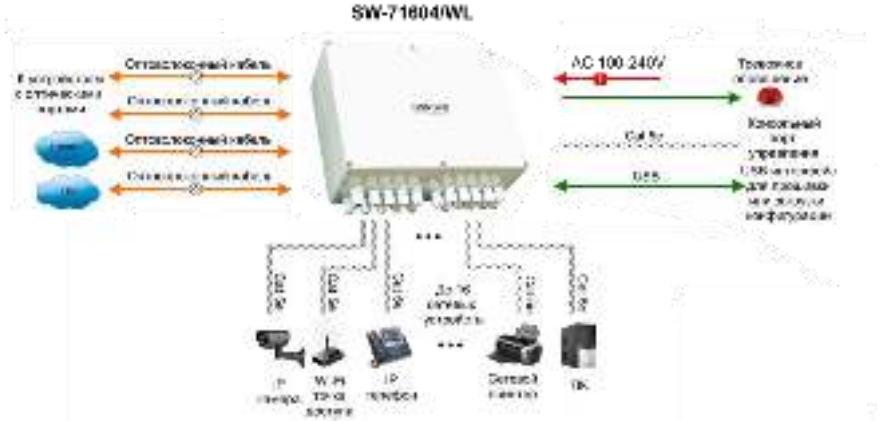


Рис.5 Типовая схема подключения коммутатора SW-71604/WL

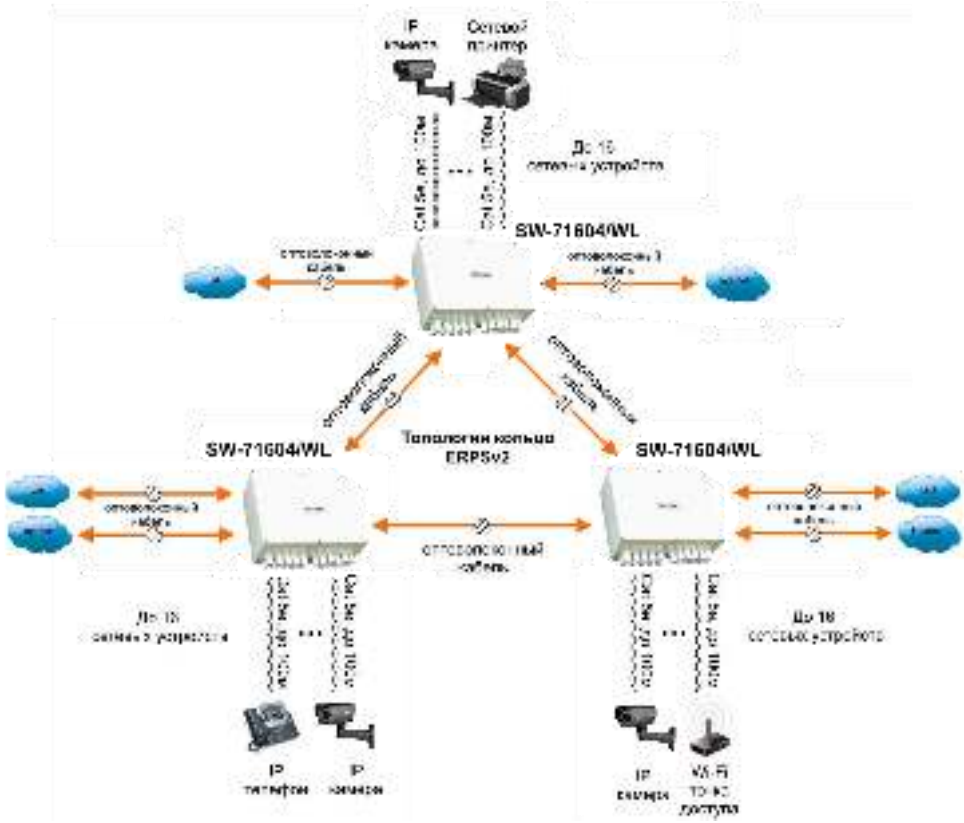


Рис.6 Схема подключения коммутатора SW-71604/WL, топология «кольцо»

6. Проверка работоспособности системы

После подключения кабелей к разъёмам и подачи питания на коммутатор можно убедиться в его работоспособности.

Подключите коммутатор между двумя ПК с известными IP-адресами, располагающимися в одной подсети, например, 192.168.1.1 и 192.168.1.2.

На первом компьютере (192.168.1.2) запустите командную строку (выполните команду cmd) и в появившемся окне введите команду:

ping 192.168.1.1

Если все подключено правильно, на экране монитора отобразится ответ от второго компьютера (Рис.7). Это свидетельствует об исправности коммутатора.

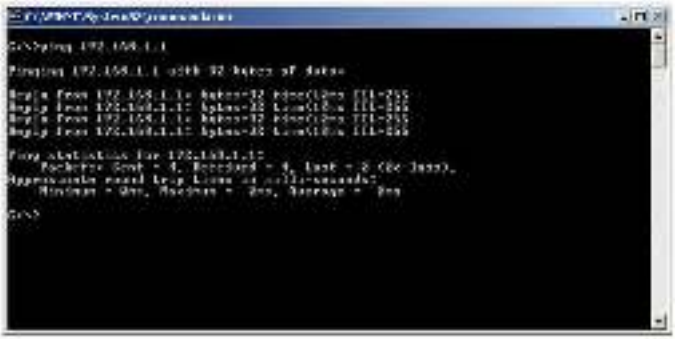


Рис.7 Данные, отображающиеся на экране монитора, после использования команды Ping.

Если ответ ping не получен («Время запроса истекло»), то следует проверить соединительный кабель и IP-адреса компьютеров.

Если не все пакеты были приняты, это может свидетельствовать:

- о низком качестве кабеля;
- о неисправности коммутатора;
- о помехах в линии.

Примечание:

Причины потери в оптической линии могут быть вызваны:

- неисправностью SFP-модулей
- изгибами кабеля
- большим количеством узлов сварки
- неисправностью или неоднородностью оптоволокна.

7. Подготовка перед управлением коммутатором через WEB-интерфейс**

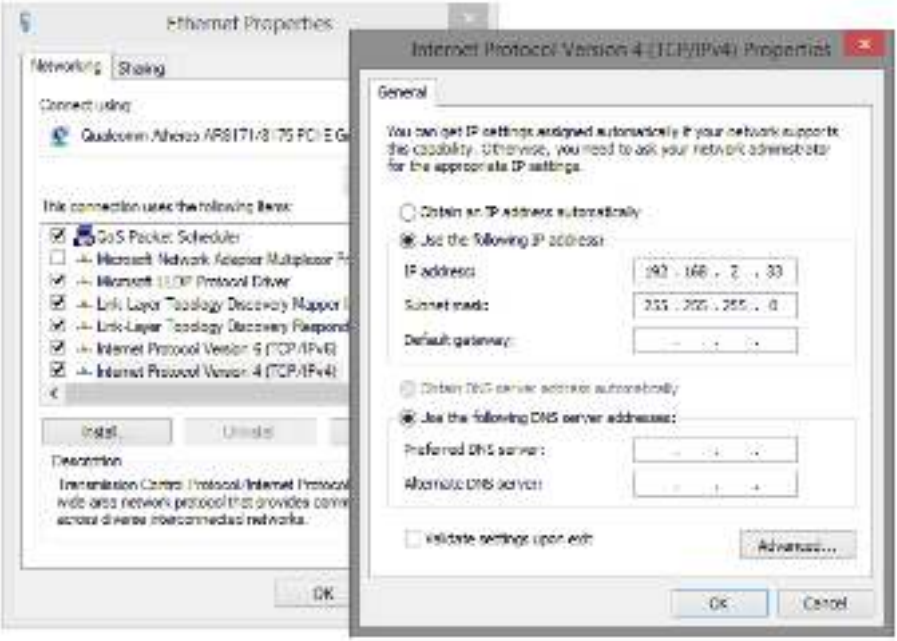
Web-интерфейс позволяет гибко настраивать и отслеживать состояние уличного коммутатора, используя браузер (Google Chrome, Opera, IE и тд) из любой точки в сети.

Прежде, чем приступить к настройке коммутатора через Web-интерфейс, необходимо убедиться, что ваш ПК и коммутатор находятся в одной сети. Чтобы правильно сконфигурировать ваш ПК используйте следующую пошаговую инструкцию:

1. Убедитесь, что сетевая карта в вашем ПК установлена, работает и поддерживает TCP/IP протокол.

2. Подключите между собой коммутатор и ваш ПК, используя патч-корд RJ-45

3. По умолчанию IP-адрес коммутатора: **192.168.2.1.** Коммутатор и ваш ПК должны находиться в одной подсети. Измените IP адрес вашего ПК на 192.168.2.X, где X-число от 2 до 254. Пожалуйста, убедитесь, что IP-адрес, который вы назначаете вашему ПК, не совпадал с IP-адресом коммутатора.



4. Запустите Web-браузер (IE, Firefox, Chrome) на вашем ПК

5. Введите в адресную строку **192.168.2.1** (IP-адрес коммутатора) и нажмите Enter на клавиатуре.

6. Появится форма аутентификации. По умолчанию

Логин: **admin.** Пароль: **admin**

В дальнейшем пароль и логин можно поменять через WEB интерфейс коммутатора.

7. После корректного ввода имени пользователя(логин) и пароля появится главное окно WEB интерфейса коммутатора

**** Подробное описание всех настроек WEB интерфейса уличного коммутатора вы можете найти в полной инструкции к конкретной модели на сайте www.osnovo.ru**

8. Управление через WEB интерфейс, основные элементы

8.1 WEB интерфейс, общая информация

На данной странице WEB интерфейса коммутатора представлена общая информация о системе.

1. Когда для настройки коммутатора через WEB интерфейс используется устройство с низким разрешением видеоизображения поле «Model Information» (Информация о модели) может быть скрыто с помощью нажатия на иконку очков для того, чтобы другие элементы интерфейса были лучше видны.

Страница WEB интерфейса полностью (show model information)

Страница WEB интерфейса частично (hide model information)

2. После завершения конфигурирования нажмите эту иконку для сохранения текущей конфигурации в файле **«startup-config»**. Файл с настройками будет сохранен в системе пока не будет выполнен сброс настроек до заводских.

3. Нажатие на данную иконку удалит файл с текущей конфигурацией из системы. После выполнения сброса до заводских настроек, все настройки будут возвращены к значениям по умолчанию.

4. Нажатие на данную иконку перезагрузит устройство.

5. Нажатие на данную иконку отвечает за выход из WEB интерфейса и возврат к экрану ввода логина и пароля. Кроме того, система автоматически совершает выход по истечении таймера «timeout». Значение таймера настраивается через CLI с использованием команды «exec-timeout». Максимальное значение для таймера – 30 минут.

Удобная таблица с данными

Такой тип таблицы используется для следующих таблиц с данными:

- ✓ «IPv6 Neighbor Table»
- ✓ «IGMP Snooping Table»
- ✓ «VLAN Table»
- ✓ «LLDP Table»
- ✓ «MAC Address Table»

Далее будет описано на примере «MAC Address Table» (Таблица MAC адресов), как использовать функции такого типа страниц с данными, чтобы пользователю было проще получать информацию из них.

Show 10 entries Search:

VID	MAC Address	Type	Source
VLAN 1	EC:08:6B:06:96:53	Learning	2
VLAN 1	1C:49:7B:6A:F3:41	Learning	5
VLAN 1	1C:1B:0D:66:75:E8	Learning	5
VLAN 1	01:00:5E:7F:FF:FA	Static	2
VLAN 1	40:8D:5C:EA:52:02	Learning	5
VLAN 1	9C:EB:E8:3A:54:E7	Learning	5
VLAN 1	40:8D:5C:FA:8D:C3	Learning	5
VLAN 1	1C:1B:0D:66:F7:F8	Learning	5
VLAN 1	FC:3F:DB:53:19:8E	Learning	5
VLAN 1	A4:02:B9:80:7D:66	Learning	5

Showing 1 to 10 of 10 entries First Previous Next Last

Auto Refresh Refresh

Refresh Rate: 5 seconds

- Show 10 entries Пользователь может выбрать количество отображаемых записей на странице. Доступны следующие значения: «10», «25», «50», «100». Значение по умолчанию «10».
- Search: Функция поиска (Search) позволяет пользователю искать ключевое слово в таблице данных. Поиск ведется по всем столбцам таблицы и идентифицирует данные, соответствующие критериям поиска.
- Showing 1 to 10 of 31 entries Отображает общее число записей и текущий номер записи.

- Сортирует поля с данными от меньшего к большему и наоборот – от большего к меньшему.
- First Previous Next Last Возврат к первой (first)/предыдущей (previous)/следующей (next)/последней (last) странице с данными.
- Auto Refresh Выбор этого чекбокса включает функцию Auto Refresh (автообновление). Данные в таблице автоматически обновляются в зависимости от параметра Refresh Rate (время обновления)
- Refresh Rate: 5 seconds Это глобальный настраиваемый параметр, отвечающий за время обновления данных в таблицах при включенной функции Auto Refresh. Значение Refresh Rate может быть в пределах от 5 до 300 сек. По умолчанию значение равно 5 секундам.
- Refresh (Refresh Button) Кнопка принудительного обновления данных в таблице.

8.2 System (Системная информация)

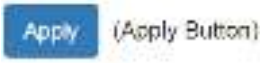
Для получения дополнительной информации о том или ином поле WEB интерфейса наведите мышкой на иконку вопроса, там где этом предусмотрено.

Host Name (Идентификационное имя коммутатора) – используется для более простой идентификации настраиваемого коммутатора в сети серди остальных коммутаторов. Например: CoreSwitch01. Максимальная длина для имени – 32 символа.
Следующие символы: **#** \ **' " ?** нельзя использовать.

Device Description (Описание устройства) – не доступно к изменению, задается системой. Данное поле содержит количество медных портов, оптических портов и поддержу PoE (если предусмотрено).

Switch Location (Местоположение коммутатора) – используется для определения местоположения коммутатора . Например: Area01. Максимальная длина для имени – 32 символа.
Следующие символы: **#** \ **' " ?** нельзя использовать.

Contact Information (Контактная информация) – содержит информацию о лице, ответственном за это устройство, а также его контактные данные. Следующие символы: **# \ ' " ?** нельзя использовать.



Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.3 IPv4 Settings (Настройки протокола IPv4)

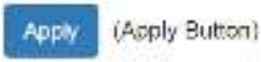
IPv4 это четвертая версия Internet Protocol. Используется в сетях с коммутацией пакетов и без установления соединения. Адрес IPv4 составляет 4 байта (32 бита) и адресное пространство ограничено 4294967296 (2^{32}) уникальными адресами. В локальной сети (LAN) используется частная сеть (Private Network). Она начинается с адреса 192.168.0.0 и содержит 60025 (2^{16}) адресов. Фреймы (пакеты) могут быть отправлены хосту только в одной и той же подсети. Например, по умолчанию IP адрес коммутатора 192.168.10.1. Когда пользователь хочет подключится к коммутатору IP адреса от 192.168.10.2 до 192.168.10.254 должны быть назначены хосту.

IPv4 Mode (режим работы IPv4) – Предусмотрено 2 способа настройки IPv4 адреса.
Static – IP адрес задается вручную.
DHCP Client – IP адрес назначается службой DHCP. В таком случае поля содержащие информацию об IP адресе будут отключены для изменения.

IP Address (IP адрес) – назначает уникальный IP адрес в подсети для доступа к коммутатору. **Адрес по умолчанию 192.168.2.1.**

Subnet Mask (Маска подсети) – определяет тип подсети, к которому подключено это устройство.

Default Gateway (IP Адрес шлюза по умолчанию) – IP адрес маршрутизатора, который используется для подключения LAN к WAN



Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.4 IPv6 Settings (Настройки протокола IPv6)

IPv6 это 6я версия Internet Protocol решающая проблему с ограничением адресного пространства протокола IPv4. IPv6 это протокол 3 уровня OSI (Internet Layer). Количество уникальных адресов для IPv6 составляет 2^{128}. Адрес IPv6 обычно представлен цифрами в шестнадцатеричной системе. 8 групп по 4 цифры. Каждая группа отделена символом **:**

8.4.1 Настройка IPv6

IPv6 Mode (Режим работы IPv6) – Включает (enable) или отключает (disable) IPv6. Когда протокол IPv6 включен, другие устройства могут подключаться к коммутатору. По умолчанию включено.

Default Address (IPv6 адрес по умолчанию) – IPv6 адрес коммутатора по умолчанию. Он автоматически сгенерирован на основе MAC адреса коммутатора и не может быть изменен вручную.

IPv6 Addresses (Доп. IPv6 адреса) – Позволяет пользователям задавать другие IPv6 адреса для коммутатора. Поле IPv6 адреса состоит из 2х секций – сам IPv6 адрес и префикс. По умолчанию префикс равен 64 бит. Нажмите + чтобы добавить IPv6 адрес, нажмите ✖ чтобы удалить IPv6 адрес

(Apply Button) Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.4.2 IPv6 Neighbor Table (Таблица «соседей» IPv6)

IPv6 Address (IPv6 Адрес) – поле содержит IPv6 адрес «соседа»

MAC Address (MAC Адрес) – поле содержит MAC адрес «соседа»

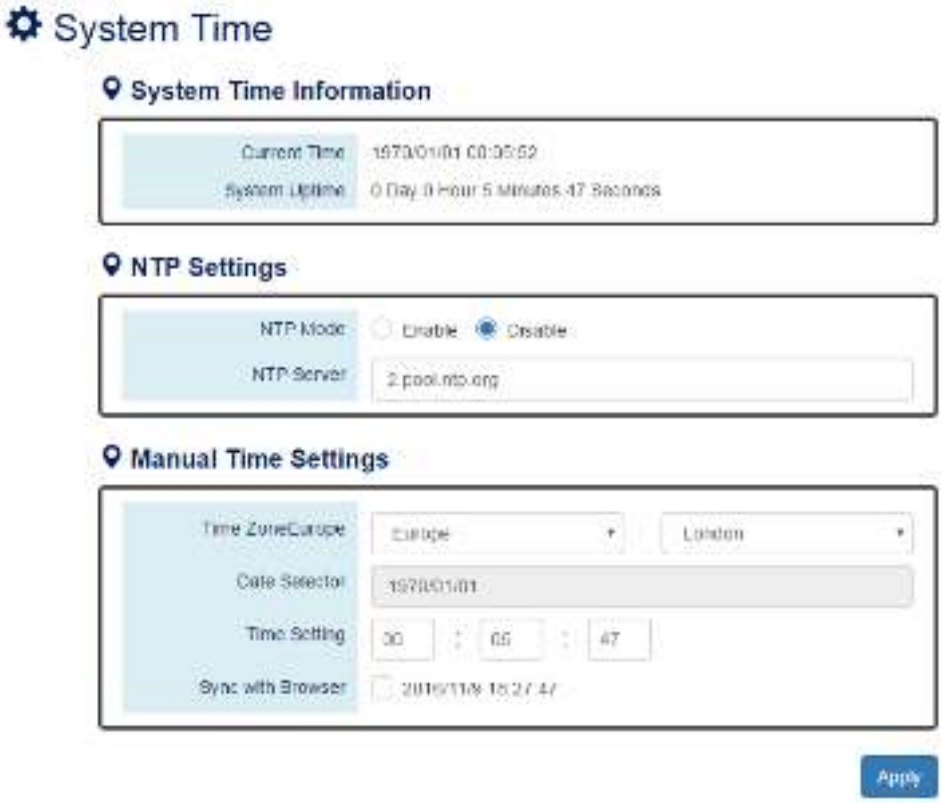
State (Текущее состояние) – состояние подключения. Может быть 5 состояний. «DELAY» «REACHABLE» «STALE» «FAILED» «PROBE»

8.5 System Time (Системное время)

Системное время содержит в себе текущую дату и время. Время безотказной работы определяется временем после последней перезагрузки коммутатора. Коммутатор не оснащен элементом питания для сохранения системного времени в памяти. Пользователи могут настраивать часовой пояс и время вручную, синхронизировать с временем браузера (через который осуществляется настройка коммутатора), или используя службу NTP.

NTP – протокол сетевого времени. Работает по принципу клиент-сервер. Клиентом выступает коммутатор, получая от сервера данные текущего времени и даты.

8.5.1 Настройка системного времени



System Time Information (Информация о текущем времени, дате и времени безотказной работы) – содержит следующие поля, доступные для чтения:

Current Time – текущая дата и время;

System Uptime – время безотказной работы с последней перезагрузки.

NTP Settings (Настройки протокола сетевого времени NTP) – состоит из следующих полей:

NTP Mode – включает или отключает использование протокола NTP для получения системного времени. Когда активно – использует NTP Server для синхронизации системного времени;

NTP Server – это поле отображает URL ссылку или IP адрес сервера, к которому будет проводится подключение для синхронизации системного времени.

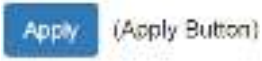
Manual Time Settings (Ручная настройка времени) – перечень настроек, позволяющих вручную задавать дату и время.

Time Zone – выбор часового пояса;

Date Selector – установка даты в ручную в формате год/месяц/день;

Time Setting – установка вручную времени в формате часы:минуты:секунды

Sync with Browser – выбор этого чекбокса позволит синхронизировать время коммутатора с временем браузера, через который осуществляется управление коммутатором

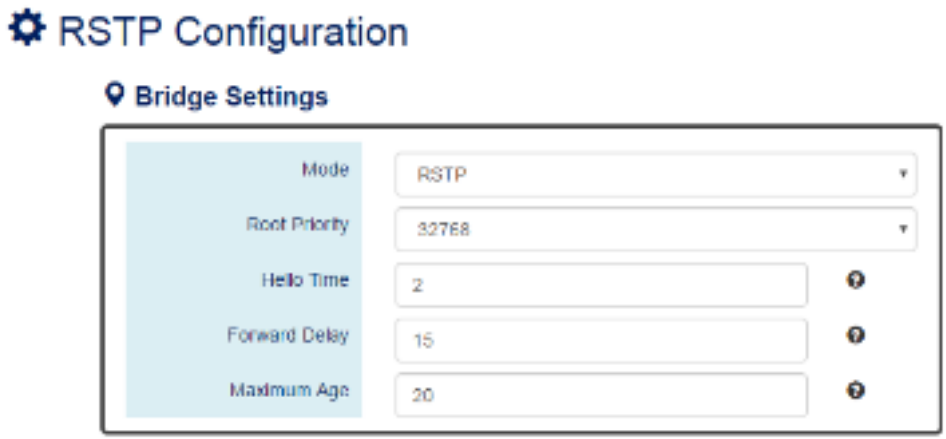


Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.6 RSTP Configuration (Настройка протокола RSTP)

STP – это стандартный протокол (IEEE 802.1D) связующего дерева. Используется для предотвращения появления сетевых петель. Протокол RSTP восстанавливает текущую топологию сети значительно быстрее, чем STP. RSTP (IEEE 802.1.w). Время восстановления топологии при сбое не более 6 секунд (против 30-50 у STP протокола). Это делает использование RSTP протокола основным.

8.6.1 Конфигурирование RSTP. Базовая информация



Mode (режим работы) – предлагает 2 возможных режима

RSTP – протокол STP активен, RSTP используется для резервирования;

Disable – отключает STP. Пользователи используют другой протокол для предотвращения сетевых петель.

Root Priority (значение для определения корневого моста) – используется для определения корневого моста (root bridge). Самый низкий приоритет соответствует корневому мосту. Если все коммутаторы в сети настроены на одно и тоже значение приоритета, то система выберет корневой мост для работы протокола на основе MAC адресов. Диапазон возможных значений 0 – 61440 (с шагом 4096). По умолчанию значение приоритета – 32768

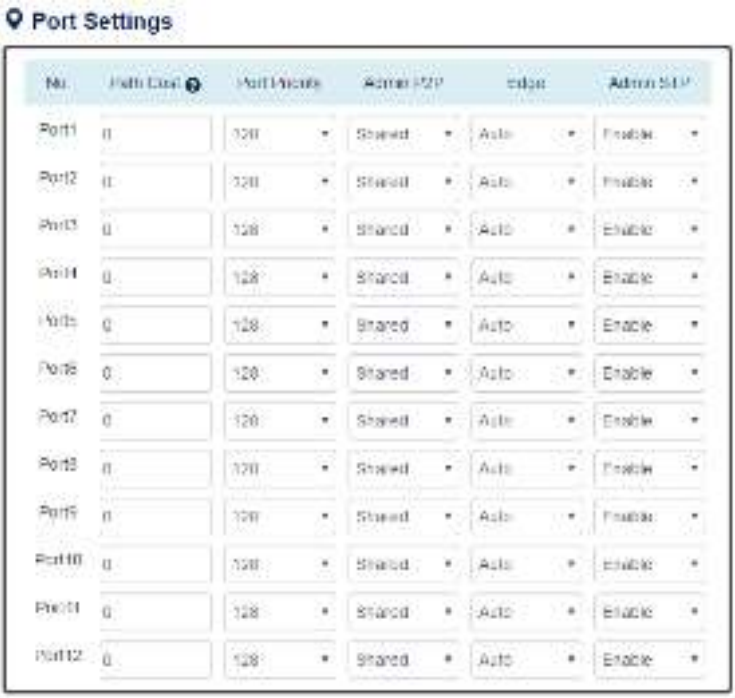
Hello Time (интервал отправки пакетов BPDU) – используется для определения отправки пакетов BPDU для проверки текущей топологии

и состояния RSTP. Диапазон возможных значений 1-10сек. По умолчанию – 2 сек.

Forward Delay (задержка смены состояний) – интервал, через который порт коммутатора меняет состояние с обучения/прослушивания на пересылку. Диапазон возможных значений 4-30сек. Значение по умолчанию – 15 сек.

Maximum Age (время хранения текущей конфигурации) – таймер, определяющий ожидание BPDU пакетов от корневого моста. Если устройство получает пакеты BPDU до истечения времени таймера, значение таймера будет сброшено. Кроме того, устройство отправит топологию с измененным BPDU для уведомления других устройств. Диапазон значений составляет от 6 – 40сек. Значение по умолчанию – 20 сек.

8.6.2 Настройка RSTP для портов



No – номер порта, где N – основан на количестве портов коммутатора.

Path Cost – диапазон «стоимости пути». Диапазон возможных значений от 0 – 200000000. По умолчанию значение – 0. Это означает, что расчет стоимости пути определяется системой автоматически.

Port Priority – используется для определения порта, который должен быть заблокирован при использовании топологии «кольцо». Диапазон возможных значений от 0 – 240 (кратно 16). По умолчанию значение – 128.

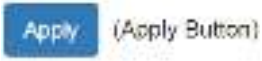
Admin P2P – тип установленного соединения для порта. P2P – полный дуплекс. Shared – полудуплекс

Edge – порт, который может быть подключен к устройству без STP называется EDGE портом.

Пользователь может вручную устанавливать порты коммутатора в состояние EDGE или NON-EDGE.

Значение Auto – система автоматически определяет EDGE и NON EDGE состояние для порта.

Admin STP – позволяет включать/выключать (enable/disable) поддержку STP протокола на выбранном порте.



Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.6.3 RSTP Status

Bridge ID – это поле отображает уникальный идентификатор узла, когда он является частью сети. Идентификатор содержит 8 байт информации. Первые 2 байта занимает Bridge Priority (настраиваемый параметр), остальные 6 байтов занимает MAC адрес.

Root Bridge – корневой мост выбирается из всех коммутаторов, участвующих в топологии STP спустя несколько отправленных BPDU пакетов. Корневым мостом является устройство с наименьшим значением Root Priority. Если все устройства в дереве STP имеют одинаковый показатель Root Priority, корневой мост выбирается на основании MAC адреса.

Root Priority – этот показатель определяет корневой мост (устройство с наименьшим значением Root Priority). Если все устройства в дереве STP имеют одинаковый показатель Root Priority, корневой мост выбирается на основании MAC адреса.

Root Port – порт корневого моста с наименьшим значением Path Cost. Если в поле Root Port отображается NONE, то это устройство является корневым мостом в топологии STP.

Root Path Cost – «стоимость» пути от текущего узла до корневого моста в топологии STP.

Hello Time – используется для определения интервала отправки BPDU пакетов, для проверки состояния и топологии дерева RSTP.

Forward Delay – задержка перед сменой состояний порта с обучения/прослушивания на пересылку.

Max Age – максимальное время ожидания BPDU пакетов от корневого моста.

Port Status

No	Role	Path State	Port Cost	Port Priority	Oper P2P	Oper Edge
Port1	Disabled	Discarding	200000000	128	Shared	Non-Edge
Port2	Disabled	Discarding	200000000	128	Shared	Non-Edge
Port3	Disabled	Discarding	200000000	128	Shared	Non-Edge
Port4	Disabled	Discarding	200000000	128	Shared	Non-Edge
Port5	Disabled	Discarding	200000000	128	Shared	Non-Edge
Port6	Disabled	Discarding	200000000	128	Shared	Non-Edge
Port7	Designated	Forwarding	20000	128	Shared	Edge
Port8	Designated	Forwarding	20000	128	Shared	Edge
Port9	Disabled	Discarding	200000000	128	Shared	Non-Edge
Port10	Disabled	Discarding	200000000	128	Shared	Non-Edge
Port11	Disabled	Discarding	200000000	128	Shared	Non-Edge
Port12	Disabled	Discarding	200000000	128	Shared	Non-Edge

Auto Refresh

Refresh

No – количество портов от Port 1 до Port N, где N – общее количество портов коммутатора.

Role – поле отображающее текущую роль порта в STP.

Root – корневой порт, подключен к корневому мосту, имеет наименьшее значение Root Path Cost.

Designated – назначенный порт, который отправляет самый корректный BPDU другим узлам.

Alternate – альтернативный порт, который заблокирован. Порт все еще способен получать BPDU пакеты от другого моста. При получении BPDU пакета может переслать его в другой сегмент.

Backup – резервный порт, который заблокирован. Соответствует по своему состоянию порту Alternate. Также способен получать BPDU пакеты от того же самого моста. При получении BPDU пакета может переслать его в другой сегмент.

Disabled – порт отключен.

Path State – поле отображающее текущее состояние порта в STP.

Discarding – состояние порта «Отключен» «Блокирован» «Прослушивание». Входящие пакеты будут отброшены, запоминание MAC адресов остановлено.

Learning – порт запоминает MAC адреса, но входящие пакеты будут отброшены.

Forwarding – порт пересылает входящие пакеты на основе ранее запомненных в таблицу MAC адресов.

Port Cost – стоимость пути от порта до корневого моста. STP протокол предполагает, что значение стоимости пути определяется скоростью доступа подключений. Значения стоимости пути RSTP по умолчанию приведены в таблице ниже:

Speed	RSTP Path Cost	Speed	RSTP Path Cost
4 Mbps	5,000,000	1000 Mbps (1Gbps)	20,000
10 Mbps	2,000,000	2000 Mbps (2 Gbps)	10,000
16 Mbps	1,250,000	10000 Mbps (10 Gbps)	2,000
100 Mbps	200,000		

Port Priority – значение, которое определяет, является ли устройство корневым мостом в топологии STP. Порт с наименьшим значением Port Priority имеет больший приоритет среди остальных узлов.

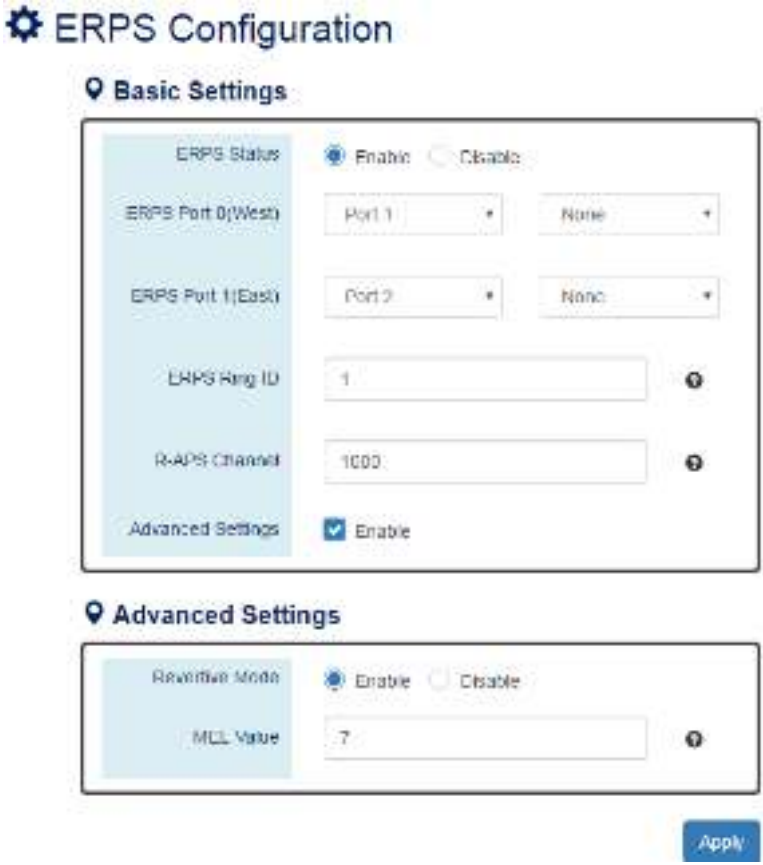
Oper. P2P – это поле отображает тип соединения STP. P2P означает «точка – точка», shared – соединение типа «точка-многоточка»

Oper. Edge – поле отображает состояние типа EDGE для порта в топологии STP.

8.7 ERPS (Протокол защиты трафика от петель в кольцевой топологии)

ERPS является протоколом защиты сетевого трафика от петель в кольцевой топологии. Является альтернативным STP протоколу методом борьбы с сетевыми петлями. Использует специальные пакеты для опроса узлов сети и восстановления топологии. Если в сети возникает ошибка ERPS пересылает трафик по резервному пути. Время восстановления топологии с применением ERPS менее 50мс.

8.7.1 Настройка ERPS



<u>Basic Settings</u> (базовые настройки):

ERPS Status – 2 возможных состояния «включено» (enable) или «отключено» (disable). По умолчанию поддержка протокола ERPS включена;

ERPS Port 0 – также называется «WEST» порт. Выберите один из портов коммутатора для выполнения роли Port 0 в топологии ERPS;

ERPS Port 1 – также называется «EAST» порт. Выберите один из портов коммутатора для выполнения роли Port 1 в топологии ERPS;

Примечание: Только один порт коммутатора может быть выбран для выполнения роли ERPS Port 0 или ERPS Port 1

Role	Description
Owner	There is only one "Owner" in the ERPS ring topology. The Owner is responsible for blocking the traffic in RPL and protects one side of the RPL.
Neighbor	There is only one"Neighbor" in the ERPS ring topology. The Neighbor is the port connected with the Owner port and protects another side of the RPL.
None	The "None" implies that theport is other than an Owner or aNeighbor.

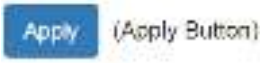
ERPS Ring ID – идентификатор кольца. Участники кольца должны иметь один и тот же ERPS Ring ID. Диапазон ERPS Ring ID от 1 до 239. Значение по умолчанию 1.

R-APS Channel – канал R-APS Channel используется для пересылки ERPS информации и сопоставляется с идентификаторами VLAN. Эти VLAN ID не могут быть настроены как VLAN ID для обычного сетевого трафика. Участники кольца должны иметь одинаковое значение R-APS Channel. Диапазон возможных значений от 1 до 4094. Значение R-APS Channel по умолчанию 1000.

Advanced Settings (расширенный настройки). Данное поле отображается, когда отмечен галкой чекбокс «Advanced Settings» в основных настройках ERPS (Basic Settings)

Revertive Mode – реверсивный режим работы ERPS. Включить / выключить (enable/disable). Если реверсивный режим ERPS включен, заблокированная ссылка вернется к RPL после того, как неудачная ссылка будет восстановлена. По умолчанию реверсивный режим ERPS включен.

MEL Value – значение подразумевает MEG уровень. Значение MEL содержится в R-APS PDU пакетах. Диапазон возможных значений от 0 до 7. Значение по умолчанию 7.



Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

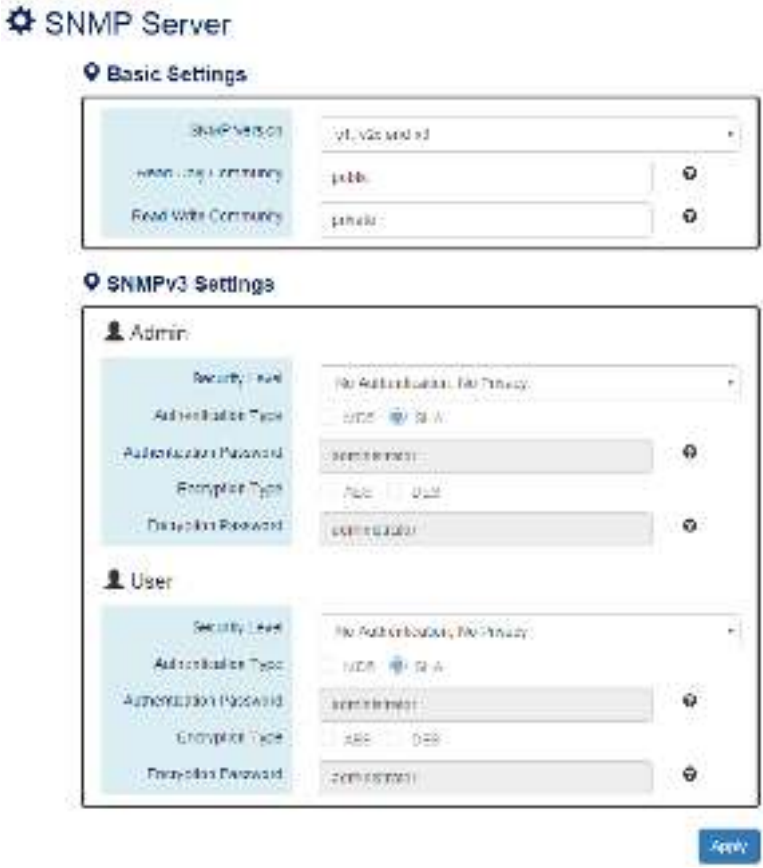
8.8 SNMP (простой протокол сетевого управления)

SNMP – простой протокол сетевого управления, является стандартом для получения и структурирования информации с управляемого коммутатора. С помощью SNMP можно частично изменять информацию для изменения поведения устройств. Обычно SNMP используется для мониторинга сети. Пользователи могут удаленно запрашивать информацию от устройств через SNMP.

Управляемые коммутаторы поддерживают протоколы SNMP v1, v2c, v3. Протоколы SNMP v1, v2c используют для аутентификации командную строку «только для чтения» и «чтение/запись». Протокол SNMP v3 требует аутентификацию на основе хеширования (md5 или SHA). Это делает использование SNMP v3 более безопасным. Подробная информация о разнице в версиях протокола SNMP дана в таблице ниже

Version	Web Setting	Authentication	Encryption	Method
v1 & v2c	Read Only Community	Community String	No	String match for authentication
	Read-Write Community	Community String	No	String match for authentication
v3	Security Level – No Authentication, No Privacy	No	No	Access by an account (admin or user)
	Security Level – Authentication, No Privacy	MD5 / SHA	No	Access by an account (admin or user) and password with more than 8 characters, which is based on MD5 or SHA
	Security Level – Authentication, Privacy	MD5 / SHA	Yes AES / DES	Access by an account (admin or user) and password more than 8 characters, which is based on MD5 or SHA. The data encryption is based on AES or DES and the key requires 8 to 32 characters

8.8.1 Настройка SNMP сервера



<u>Basic Settings</u> (базовые настройки)

<u>SNMP Version</u> – По умолчанию включена поддержка SNMP v1, v2c, v3. Пользователи могут выбрать поддержку SNMP v1 и v2c или SNMP v3. None – означает, что сервер SNMP будет отключен.

<u>Read Only Community</u> – группа пользователей к серверу SNMP с правами «только для чтения». Максимальная длина для группы 32 символа. Нельзя использовать символы **# \ ' " ?**

Read-Write Community – группа пользователей к серверу SNMP с правами «чтение/запись». Максимальная длина для группы 32 символа. Нельзя использовать символы **# \ ' " ?**

SNMPv3 Settings (Настройки SNMPv3) Эта секция отображается только когда в основных настройках выставлены SNMP Version v1, v2c, v3 или SNMP v3. Предоставляются 2 учетные записи Admin и User для доступа в роли SNMP агента. Пользователи могут настраивать различные уровни безопасности для 2 учетных записей.

Security Level – 3 уровня безопасности:

No Authentication, No Privacy – без аутентификации и конфиденциальности. Доступ с помощью учетной записи Admin или User;

Authentication, No Privacy – аутентификация, без конфиденциальности. Доступ с помощью учетной записи Admin или User с паролем;

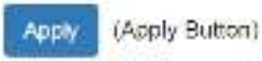
Authentication, Privacy – аутентификация, конфиденциальность. Доступ с помощью учетной записи Admin или User с паролем и шифрованием.

Authentication Type – тип аутентификации MD5 или SHA.

Authentication Password – строка или ключ для прохождения процесса аутентификации на сервере SNMP. Пароль будет хеширован MD5 или SHA методом перед аутентификацией. Минимальная длина пароля 8 символов. Максимальная – 32 символа. Нельзя использовать символы **# \ ' " ?**

Encryption Type – 2 алгоритма шифрования AES и DES на выбор.

Encryption Password – строка/ключ используется для шифрования данных, отправляемых на SNMP сервер. Минимальная длина пароля 8 символов. Максимальная – 32 символа. Нельзя использовать символы **# \ ' " ?**



Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.8.2 Настройка SNMP Trap

<u>Basic Settings</u> (базовые настройки)

<u>Trap Mode</u> – По умолчанию включена поддержка SNMP v1, v2c, v3. Пользователи могут выбрать поддержку SNMP v1 и v2c или SNMP v3. None – означает, что сервер SNMP будет отключен.

<u>Inform Retry</u> – SNMP Trap отправит значение Повторить (Retry), когда Trap настроен на «V2 Inform» или «V3 Inform» режим. Диапазон возможных значений от 1 до 100. Значение по умолчанию 5.

<u>Inform Timeout</u> – временной интервал, использующийся для отправки Trap, когда Trap настроен на «V2 Inform» или «V3 Inform» режим. Диапазон возможных значений от 1 до 300 сек. Значение по умолчанию 1сек.

<u>Trap Receiver IP</u> – IP адрес Trap сервера для получения Trap информации.

Community – строка в SNMP Trap идентифицирующая устройство. Максимальная длина – 32 символа. Нельзя использовать символы **# \ ' " ?**

SNMPv3 Trap/Inform Settings (Настройки Trap/Inform для SNMPv3). Эта секция с настройками активна, только если выставлен режим в Trap Mode «v3 Trap» или «v3 Inform»

Username – особое имя пользователя для аутентификации на SNMP Trap сервере.

Engine ID – идентификатор приложения SNMP.

Security Level – уровни безопасности:

No Authentication, No Privacy – без аутентификации и конфиденциальности. Доступ с использованием только имени пользователя (Username)

Authentication, No Privacy – аутентификация, без конфиденциальности. Доступ с использованием только имени пользователя (Username) с паролем;

Authentication, Privacy – аутентификация, конфиденциальность. Доступ с использованием только имени пользователя (Username) с паролем и шифрованием.

Authentication Type – 2 алгоритма хеширования MD5 или SHA на выбор.

Authentication Password – строка/ключ для прохождения процесса аутентификации к SNMP Trap серверу. Пароль будет хеширован MD5 или SHA методом перед аутентификацией. Минимальная длина пароля 8 символов. Максимальная – 32 символа. Нельзя использовать символы **# \ ' " ?**

Encryption Type – 2 алгоритма шифрования AES и DES на выбор.

Encryption Password – строка/ключ используется для шифрования данных, отправляемых на SNMP Trap сервер.

Минимальная длина пароля 8 символов. Максимальная – 32 символа. Нельзя использовать символы **# \ ' " ?**

Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.9 DHCP (Настройка протокола DHCP)

DHCP Сервер/Клиент

DHCP это протокол динамической настройки узла, является стандартизированным протоколом, используемым в IP сетях. DHCP сервер содержит пул IP адресов и когда DHCP клиент запрашивает IP адрес, DHCP сервер выбирает его из пула адресов и назначает этому DHCP клиенту. DHCP также управляет IP информацией, такой как Шлюз по умолчанию (Default Gateway) и DNS сервер. DHCP очень удобен для настройки параметров нескольких устройств сразу. Только администратор может включить DHCP клиент для каждого устройства и настроить DHCP клиент. Далее клиенты получат уникальные IP адреса и другие настройки IP для подключения к сети.

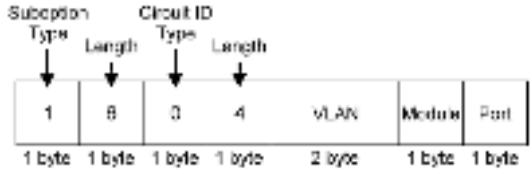
DHCP Server Binding

Помимо динамического распределения IP адресов между клиентами DHCP сервер также позволяет вручную задавать статичный IP адрес для устройства с определенным MAC адресом. Такая функция называется DHCP Server Binding.

DHCP Relay/Option82

В крупной сети может существовать несколько подсетей и DHCP клиент не может быть обслужен DHCP серверами напрямую. В этом случае необходим агент для ретрансляции (relay agent), который может помочь передать фреймы на сервера DHCP.

Опция 82 (Option82) это информационный вариант идентификации клиентов на основе Circuit ID и Remote ID. Circuit ID это идентификатор, содержащий имя и VLAN информацию. Remote ID это идентификатор удаленного узла (агента ретрансляции, relay agent). DHCP сервер может назначать IP адреса клиентам в соответствии с Option 82 сделав процесс назначения IP адресов более контролируемым. Формат фрейма **Circuit ID** представлен ниже:

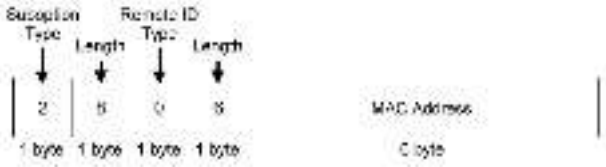


VLAN – это поле в фрейме предназначено для идентификации VLAN ID, по умолчанию установлено на 1

Module – часть номеров для устройства, отправляющего DHCP запрос. Для промышленных коммутаторов этот байт всегда равен 0.

Port – номер порта, который идентифицирует входящий DHCP запрос от DHCP клиента.

Формат фрейма **Remote ID** представлен ниже:



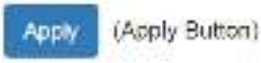
MAC Address – по умолчанию содержит MAC адрес DHCP relay agent

8.9.1 Настройка DHCP клиента

<u>IPv4 Mode</u>

Выберите «DHCP Client» чтобы включить режим DHCP клиента. Система отправляет «discovery» фрейм в сеть и пытается получить IP адрес от сервера DHCP.

После включения «DHCP Client» режима, пользователям необходимо подключиться к консольному порту (Console Port) и для получения IP адреса ввести команду в CLI «show ip address».



Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.9.2 Настройка информации DHCP сервера

Server Status – поле отображает статус DHCP сервера: Down (Не работает) UP (Работает). Информация только для чтения.

Server Mode – вкл/выкл функции DHCP сервера.

Start IP Address – начальный IP адрес пула IP адресов для DHCP сервера.

End IP Address – конечный IP адрес пула IP адресов для DHCP сервера. Должен быть в одной подсети с Start IP Address

Default Gateway – IP адрес шлюза по умолчанию, DHCP клиенты используют его, чтобы выйти в WAN. Должен находится в одной подсети с IP адресом самого коммутатора

DNS Server – DNS сервер присваивает URL DHCP клиентам вместо IP адресов.

Lease Time – DHCP сервер арендует IP адрес для устройства на некоторое время. По истечении времени аренды DHCP сервер может назначить устройству другой свободный адрес из указанного пула IP адресов.

Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.9.3 Настройка привязки информации к DHCP серверу

Binding ID – идентификатор привязки. Диапазон возможных значений от 1 до 32.

MAC Address – устройство с указанным в этом поле MAC адресом будет соответствовать статическому IP адресу привязки.

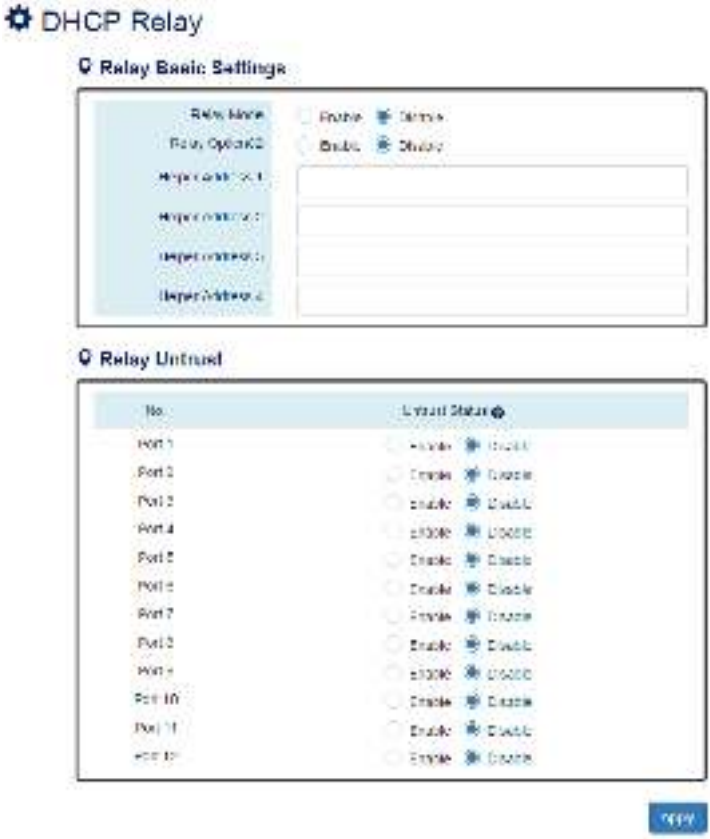
Binding IP Address – статический IP адрес, связан с MAC адресом из поля (Mac Address)

Добавить DHCP привязку

Удалить DHCP привязку

Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.9.4 Настройка DHCP relay информации



<u>Relay Basic Settings</u> (базовые настройки ретрансляции DHCP Relay)

<u>Relay Mode</u> – вкл/выкл функцию ретрансляции DHCP запросов

<u>Relay Option82</u> – вкл/выкл ретрансляцию DHCP запросов с включенной опцией 82 (описано в начале раздела)

<u>Helper Address 1 – 4</u> – 4 IP адреса, предоставленные DHCP сервером DHCP клиентам, сохраненные в резервную копию.

<u>Relay Untrust</u> (Выбор «ненадежного» порта)

<u>No</u> – номер порта от 1 до N, где N – общее число портов коммутатора.

Untrust Status – вкл/выкл статус «ненадежного» порта. Система будет отбрасывать фреймы DHCP управления на выбранном порте.

Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.11 ModBUS/TCP (Настройка промышленного протокола ModBUS/TCP)

Modbus – это открытый коммуникационный протокол, основанный на архитектуре master-slave и работающий с программируемыми логическими контроллерами (PLC). Широко применяется в промышленном сегменте для организации связи между электронными устройствами.

Modbus/TCP использует локальную сеть для работы и позволяет устройствам с поддержкой Modbus протокола обмениваться Modbus сообщениями. Для расшифровки сообщений Modbus необходимо использовать утилиты, например, Modscan. В коммутаторах Modbus сообщения содержат системную информацию, информацию о прошивке, информацию о портах, о пакетах и тд.

8.11.1 Формат данных протокола Modbus/TCP

Основные 4 типа данных, используемые Modbus/TCP это:

Data Access Type		Function Code	Function Name
Bit Access	Physical Discrete Inputs	2	Read Discrete Inputs
	Internal Bits or Physical Coils	1	Read Coils
Word Access (16-bit Access)	Physical Input Registers	4	Read Input Registers
	Physical Output Registers	3	Read Holding Registers

8.11.2 Обработка данных в Modbus/TCP

Следующие примеры предполагают, что общее количество портов равно 8. Таблица ниже для кода функции №3 (чтение значений из нескольких регистров хранения (Read Holding Registers)) и для кода функции №6 (запись значения в один регистр хранения (Preset Single Register)).

Address Offset	Data Type	Interpretation	Description
System Information			
0x0000 to 0x0008	1 word	HEX	**Port 1 to Port 8 Status** 0x0000: Disable 0x0001: Enable **Port 1 to Port 8 Status Configuration** 0x0000: Disable 0x0001: Enable

Таблица ниже предназначена для кода функции №4 (Input Registers). Значение начинается с адреса Modbus 30001. Например, смещение адреса 0x0000H равно адресу Modbus 30001, а смещение адреса 0x0030H равно адресу Modbus 30049. Вся информация, считываемая с коммутаторов хранится в режиме HEX и пользователи могут ссылаться на таблицу ASCII для сопоставления полученных данных (например, 0x4B= “K”, 0x74= “t”).

Address Offset	Data Type	Interpretation	Description
System Information			
0x0030	20 words	ASCII	**Product Name = "MT-0804G"** Word 0 Hi byte = 'M' Word 0 Lo byte = 'T' Word 1 Hi byte = '-' Word 1 Lo byte = '0' Word 2 Hi byte = '8' Word 2 Lo byte = '0' Word 3 Hi byte = '4' Word 3 Lo byte = 'G'
0x0050	1 word		Product Serial Number
0x0051	2 words	HEX	**Firmware Version** For example: Word 0 = 0x0103 Word 1 = 0x0202 Firmware version is 1.3.2

Address Offset	Data Type	Interpretation	Description
System Information			
0x0053	2 words	HEX	**Firmware Release Date** For example: Word 0 = 0x1719 Word 1 = 0x1506 Firmware was released on 2015-06-17 19 o'clock
0x0055	3 words	HEX	**Ethernet MAC Address** Ex: MAC = 01:02:03:0A:0B:0C Word 0 Hi byte = 0x01 Word 0 Lo byte = 0x02 Word 1 Hi byte = 0x03 Word 1 Lo byte = 0x0A Word 2 Hi byte = 0x0B Word 2 Lo byte = 0x0C
0x0058	1 word	HEX	**Power 1** 0x0000: Off 0x0001: On

Address Offset	Data Type	Interpretation	Description
0x0059	1 word	HEX	**Power 2** 0x0000: Off 0x0001: On
0x005A	1 word	HEX	**Fault LED Status** 0x0000: Boot error 0x0001: Normal 0x0002: Fault
0x0062	1 word	HEX	**DO1** 0x0000: Off 0x0001: On

Address Offset	Data Type	Interpretation	Description
Port Information			
0x1000 to 0x1008	1 word	HEX	**Port 1 to Port 8 Status** 0x0000: Link down 0x0001: Link up 0x0002: Disable 0xFFFF: No port
0x1100 to 0x1108	1 word	HEX	**Port 1 to Port 8 Speed** 0x0000: 10M-Half 0x0001: 10M-Full 0x0002: 100M-Half 0x0003: 100M-Full 0xFFFF: No port
0x1200 to 0x1208	1 word	HEX	**Port 1 to Port 8 Flow Ctrl** 0x0000: Off 0x0001: On 0xFFFF: No port
0x1300 to 0x1313 (Port 1) 0x1314 to 0x1327 (Port 2) ... 0x138C to 0x139F (Port 8)	20 words	ASCII	**Port 1 to Port 8 Description** Port Description = "100Tx,RJ45." Word 0 Hi byte = '1' Word 0 Lo byte = '0' Word 1 Hi byte = '0' Word 1 Lo byte = 'T' ... Word 4 Hi byte = '4' Word 4 Lo byte = '5' Word 5 Hi byte = '.' Word 5 Lo byte = '0'

Packet Information

Address Offset	Data Type	Interpretation	Description
0x2000 to 0x200F	2 words	HEX	Port 1 to Port 8 Tx Packets Ex: port 1 Tx Packet Amount = 13248635 Received Modbus response: 0x13248635 Word 0 = 1324 Word 1 = 8635

Address Offset	Data Type	Interpretation	Description
0x2080 to 0x208F	2 words	HEX	Port 1 to Port 8 Tx Bytes Ex: port 1 Tx Bytes Amount = 13248635 Received Modbus response: 0x13248635 Word 0 = 1324 Word 1 = 8635
0x2100 to 0x21(YY*2-1)	2 words	HEX	Port 1 to YY Rx Packets Ex: port 1 Rx Packet Amount = 13248635 Received Modbus response: 0x13248635 Word 0 = 1324 Word 1 = 8635
0x2180 to 0x218F	2 words	HEX	Port 1 to Port 8 Rx Bytes Ex: port 1 Rx Bytes Amount = 13248635 Received Modbus response: 0x13248635 Word 0 = 1324 Word 1 = 8635

8.11.3 Настройка работы Modbust/TCP протокола

Modbus Mode – вкл/выкл (enable/disable) протокол Modbus/TCP

Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.12 UPnP (набор протоколов Universal Plug and Play)

UPnP (Universal Plug and Play) это набор сетевых протоколов, позволяющий сетевым устройствам легко обнаруживать друг друга в сети. Набор протоколов UPnP расширяет технологию «plug&play» для подключений к сетевым устройствам без возможности конфигурирования (неуправляемые устройства). Когда UPnP устройство, такое как сетевой принтер, Wi-Fi точка доступа или мобильное устройство подключается к сети, оно автоматически создаст текущую рабочую конфигурацию с другим устройством.

8.12.1 Настройка UPnP

UPnP Mode – вкл/выкл (enable/disable) UPnP набор протоколов.

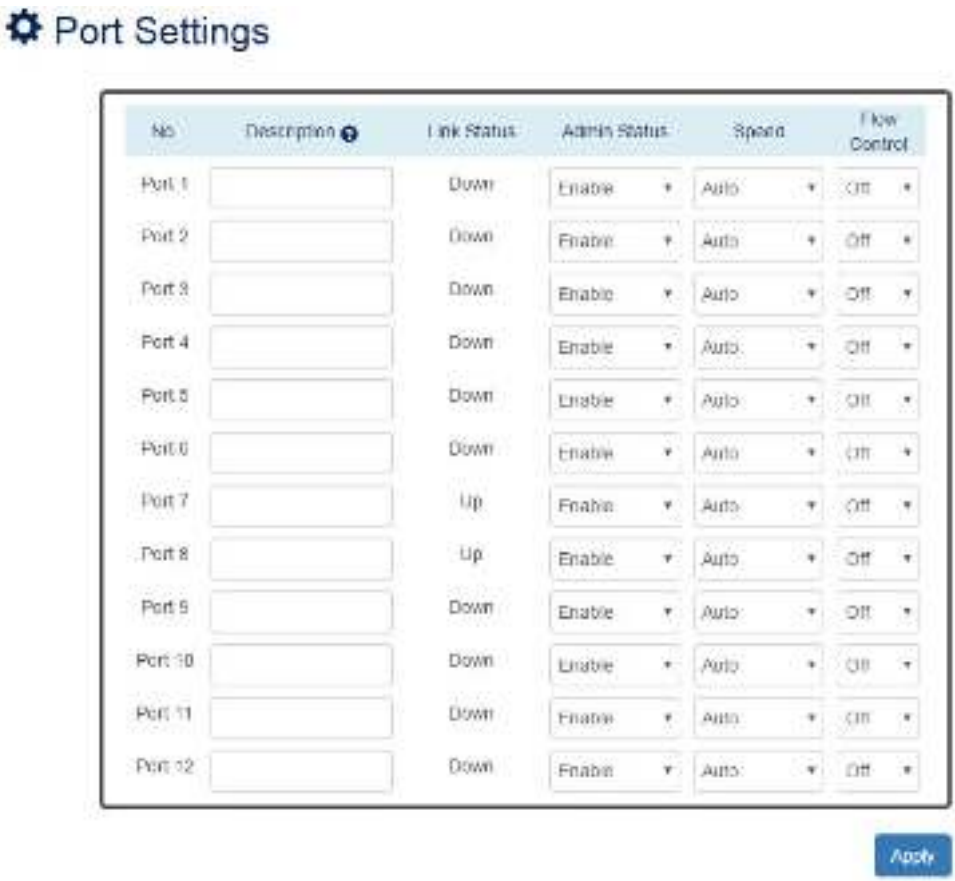
Advertisement Interval – промежуток времени используемый для отправки advertisement фрейма. Значение может быть в пределах от 300 до 86400 сек. Значение по умолчанию 1800сек.

Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.13 Port Management (Управление портами)

Раздел WEB интерфейса «Управление портами» содержит поле «Description» (описание), возможность вкл/выкл определенные порты, настраивать скорость передачи (дуплекс/полудуплес), вкл/выкл Flow Control (управление потоком передачи данных). Пользователи могут получать такую информацию, как состояние подключения, скорость, количество переданных и полученных байт данных, PoE статус. Все это является очень полезным для администратора при управлении коммутатором.

8.13.1 Настройка портов



No – номер порта от 1 до N, где N – общее количество портов коммутатора.

Description – поле «Описание» может оказаться полезным для администратора. При заполнении в дальнейшем поможет понять разницу между портами. Максимальная длина – 32 символа. Нельзя использовать символы **#** \ **' " ?**

Link Status – поле отображает текущее состояние порта, UP (соединение установлено), Down (соединение не установлено), Disable (отключен).

Admin Status – вкл/выкл (enable/disable) статус Admin на выбранном порте. Данный режим ограничивает передачу на данный порт.

Примечание. Администратор системы может отключить неиспользуемый порт, чтобы предотвратить подключение непредвиденных устройств к нему

Speed – пользователи могут вручную выставлять на выбранном порте скорость и дуплекс или выставить режим auto.

Auto – Порт работает согласно стандарту IEEE 802.3uб автоматически согласуя скорость с подключенным устройством;

1000M-Full – порт передает данные со скоростью 1000Мбит/с в режиме полного дуплекса;

1000M-Half – порт передает данные со скоростью 1000Мбит/с в режиме полудуплекса;

100M-Full – порт передает данные со скоростью 100Мбит/с в режиме полного дуплекса;

100M-Half – порт передает данные со скоростью 100Мбит/с в режиме полудуплекса;

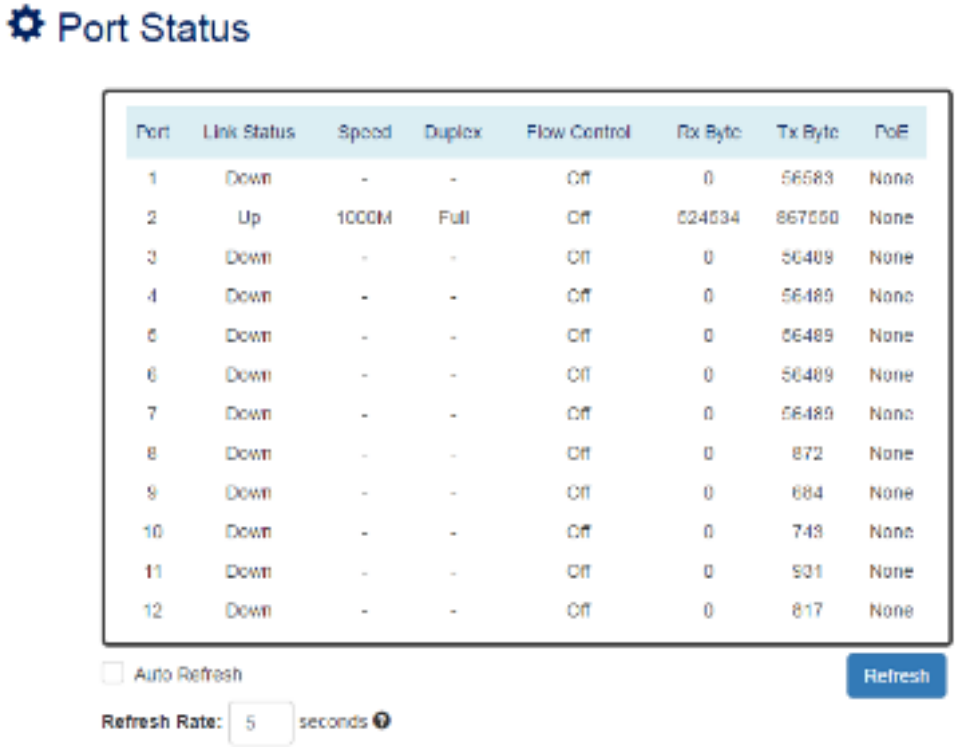
10M-Full – порт передает данные со скоростью 10Мбит/с в режиме полного дуплекса;

10M-Half – порт передает данные со скоростью 10Мбит/с в режиме полудуплекса.

Flow Control – вкл/выкл (enable/disable) управление потоком данных, если в поле Speed выставлено Auto. Flow Control предотвращает потерю сетевого трафика при перегрузке сети.

Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.13.2 Статус портов



Port	Link Status	Speed	Duplex	Flow Control	Rx Byte	Tx Byte	PoE
1	Down	-	-	Off	0	56583	None
2	Up	1000M	Full	Off	524534	867050	None
3	Down	-	-	Off	0	56489	None
4	Down	-	-	Off	0	56489	None
5	Down	-	-	Off	0	56489	None
6	Down	-	-	Off	0	56489	None
7	Down	-	-	Off	0	56489	None
8	Down	-	-	Off	0	872	None
9	Down	-	-	Off	0	684	None
10	Down	-	-	Off	0	743	None
11	Down	-	-	Off	0	931	None
12	Down	-	-	Off	0	817	None

Port – отображает номер порта от 1 до N, где N – общее количество портов коммутатора.

Link Status – поле отображает текущее состояние порта, UP (соединение установлено), Down (соединение не установлено), Disable (отключен).

Speed – отображает текущую скорость порта в бит/с. Если порт не подключен, отображается «-».

Duplex – отображает режим передачи данных. Full (полный дуплекс) Half – полудуплекс.

Flow Control – отображает состояние функции Flow Control. On (вкл) Off (выкл.)

Rx Byte – количество принятых байтов.

Tx Byte – количество переданных байтов.

PoE – Отображает состояние функции PoE на порте.

Delivery – подключено PoE устройство, PoE передается;

No PD – подключено устройство без PoE;

Disabled – функция PoE отключена на порте;

None – порт не поддерживает PoE.

Примечание: Это информация отображается только на модели коммутатора с поддержкой PoE.

Нажатие вручную кнопки REFRESH принудительно обновит данные в таблице на актуальные.

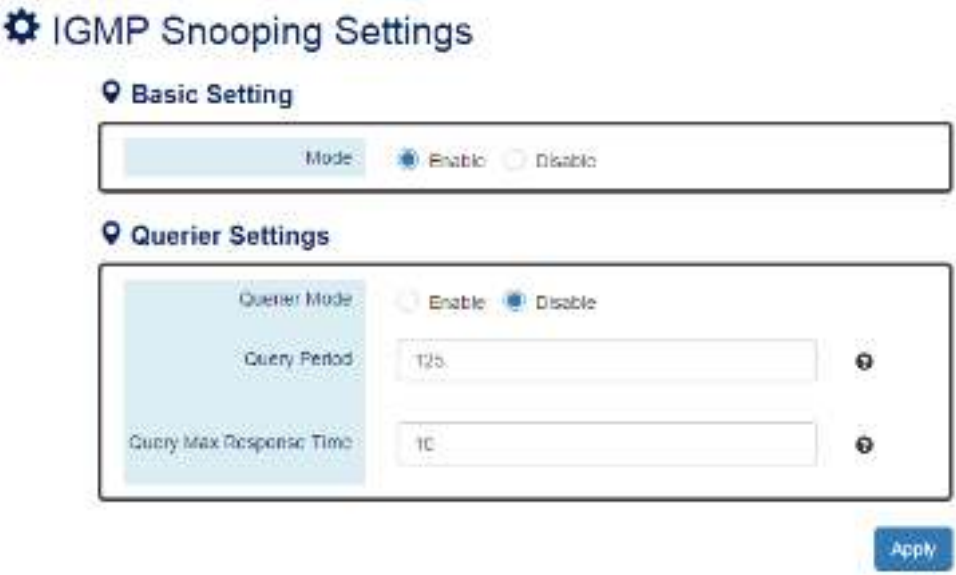
8.14 IGMP Snooping (Управление multicast рассылкой)

IGMP – протокол управления групповой (multicast) передачей данных в IP сетях. Использование IGMP позволяет снизить негативно влияние multicast трафика на сеть. Коммутаторы, работающие на 2 уровне не могут обработать IGMP информацию.

Функция IGMP Snooping дает возможность «прослушивать» коммутатору IGMP связи между хостами и маршрутизаторами и поддерживать таблицу с IP адресами multicast рассылки и участниками группы.

Использование IGMP Snooping поможет хостам в сети не получать лишний multicast трафик от группы, которая не входит в состав первоначальной определенной группы.

8.14.1 Настройка IGMP Snooping



Basic Setting

Mode – вкл/выкл (enable/disable) функцию IGMP Snooping

Querier Settings

Querier Mode – вкл/выкл (enable/disable) функцию опрашивания IGMP Snooping. Если включено – система отправляет в сеть запросы IGMP Snooping v1 и V2;

Querier Period – интервал отправки запросов IGMP Snooping. Диапазон значений от 1 до 3600сек. Значение по умолчанию – 125 сек;

Query Max Response Time – время ожидания ответа участника IGMP группы. Используется для удаления IGMP информации из группы, если ни один из участников не ответил на запрос.

Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.14.2 Таблица IGMP Snooping

Multicast IP – IP адрес multicast группы.

Group – отображает номера портов – участников группы.

8.15 IEEE 802.1Q VLAN (Логическая «виртуальная» локальная сеть)

VLAN или логическая «виртуальная» локальная сеть это функция, упрощающая планирование сети. Устройства участники VLAN могут быть расположены где угодно и объедены разными способами (по меди, по оптоволоконному кабелю и тд.), но работают как если бы они находились в одной и той же локальной сети.

IEEE 802.1Q предполагает тегирование VLAN трафика, путем добавления в пакет особого заголовка. Несколько VLAN групп могут передаваться по общему соединению – VLAN trunk'у.

Максимальное количество VLAN в сети Ethernet 4096. VLAN 0 и VLAN 4095 зарезервированы системой и не могут быть использованы для конфигурирования.

8.15.1 VLAN Q-in-Q

VLAN Q-in-Q также называемая Stacked VLAN это расширение стандартной IEEE 802.1Q VLAN. VLAN Q-in-Q поддерживает 4096*4096 VLAN групп. VLAN Q-in-Q может использовать порт в роли провайдера, пользователя или туннеля для различных приложений.

Заголовок Stacked VLAN содержит 2 заголовка формата 802.1Q с различным TPID. TPID “0x88A8” это внешний тег по умолчанию, а TPID “0x8100” является внутренним тегом для 802.1Q VLAN.

8.15.2 Настройка 802.1Q VLAN

Management VLAN

VLAN ID – используется для удобного и простого управления VLAN. Только через порты такой VLAN можно получить доступ к управлению коммутатором через Ethernet.

VLAN Member Settings

VLAN ID – уникальный идентификатор присвоенный настраиваемой VLAN группе. Диапазон возможных значений от 1 до 4094;

NAME – имя для идентификации VLAN группы среди остальных. Максимальная длина – 32 символа.
Нельзя использовать символы **# \ ' " ?**

Untagged Ports – выберите нетегированные (untagged) порты VLAN группы. Система удаляет VLAN тег перед передачей трафика с порта,

который настроен как нетегированный. Чаще всего такой порт подключен к конечному устройству, принадлежащему этой VLAN.

Tagged Ports – выберите порты, которые будут отмечены как тегированные (tagged). Система сохраняет VLAN тег перед отправкой трафика с порта, который настроен как тегированный. Обычно такой порт подключен к порту другого коммутатора и использует VLAN тег для передачи VLAN информации.

Нажмите, чтобы добавить новую VLAN

Нажмите, чтобы удалить существующую VLAN

8.15.3 Таблица VLAN

VLAN ID – уникальный идентификатор VLAN.

VLAN Name – имя, присвоенное VLAN.

Untag Member – список нетегированных портов.

Tag Member – список тегированных портов.

8.15.4 Настройка VLAN PVID и Accept Type

VLAN PVID

No – номер порта от 1 до N, где N – общее количество портов коммутатора.

PVID – назначьте VLAN ID для пакетов без VLAN тега, которые поступают на конкретный порт.

Accept Type

No – номер порта от 1 до N, где N – общее количество портов коммутатора.

Filter – три типа фильтра.

All – принимать все пакеты на выбранный порт, как тегированные, так и нетегированные;

Tagged Only – принимать только тегированные пакеты;

Untagged Only – принимать только нетегированные пакеты.

Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.15.5 Настройка VLAN Q-in-Q

Specific Provider Ethertype

Глобальное значение конфигурации. Ethertype назначается для всех портов, которые настроены, как «Specific Provider». Это поле заблокировано до тех пор, пока хотя бы 1 порт не будет настроен, как «Specific Provider» в секции настроек Q-in-Q Port Settings.

Диапазон возможных значений от 0x0000 до 0xFFFF. Значение 0x8100 нельзя использовать. По умолчанию Ethertype равно 0x88A8.

Q-in-Q Port Settings

No – Номер порта от 1 до N, где N – общее количество портов коммутатора.

Mode – настроить порт в один из режимов Q-in-Q.

Режим Q-in-Q Tunnel	Нетегированные пакеты: TPID 0x88A8 помечать и отправлять фреймы Тегированные пакеты: 1. TPID 0x8100 помечать и отправлять фреймы 2. TPID 0x88A8 отправлять фреймы
Режим Customer	Порт настроенный как Customer используется обычно в 802.1Q VLAN

	Нетегированные пакеты: TPID 0x8100 Тегированные пакеты: 1. TPID 0x8100 a. Одинаковые VLAN ID отправлять фреймы b. Разные VLAN ID отбрасывать все фреймы 2. TPID 0x88A8 – отбрасывать все фреймы
Режим Provider	Нетегированные пакеты: TPID 0x88A8 помечать и отправлять пакеты Тегированные пакеты: 1. TPID 0x8100 Отбрасывать все фреймы 2. TPID 0x88A8 a. Одинаковые VLAN ID отправлять фреймы b. Разные VLAN ID отбрасывать все фреймы.
Режим Specific Provider	Пользователь может поменять Ethertype для Provider Нетегированные пакеты: Определенные пользователем TPID фреймы помечать и отправлять Тегированные пакеты 1. TPID 0x8100 Отбрасывать все фреймы 2. TPID 0x88A8 Отбрасывать все фреймы 3. TPID (задано пользователем) a. Одинаковые VLAN ID отправлять фреймы b. Разные VLAN ID отбрасывать все фреймы.

Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.16 QoS (Quality of Service)

Quality of Service (QoS) технология предоставления различным классам сетевого трафика различных приоритетов обслуживания. Применение QoS обеспечивает стабильную и предсказуемую передачу данных в сети. Кроме того, использование QoS может оптимизировать пропускную способность сети, где она используется.

8.16.1 Настройка QoS

Queue Scheduling

Scheduling Mode Выберите метод разбивания трафика на очереди для QoS:

WRR – Weighted Round Robin. Метод при котором учитывается «вес» (low weight, high weight), а трафик разбивается на очереди;

Strict – Strict Priority Queue. Метод на основе приоритетности трафика от самого высокого до самого низкого.

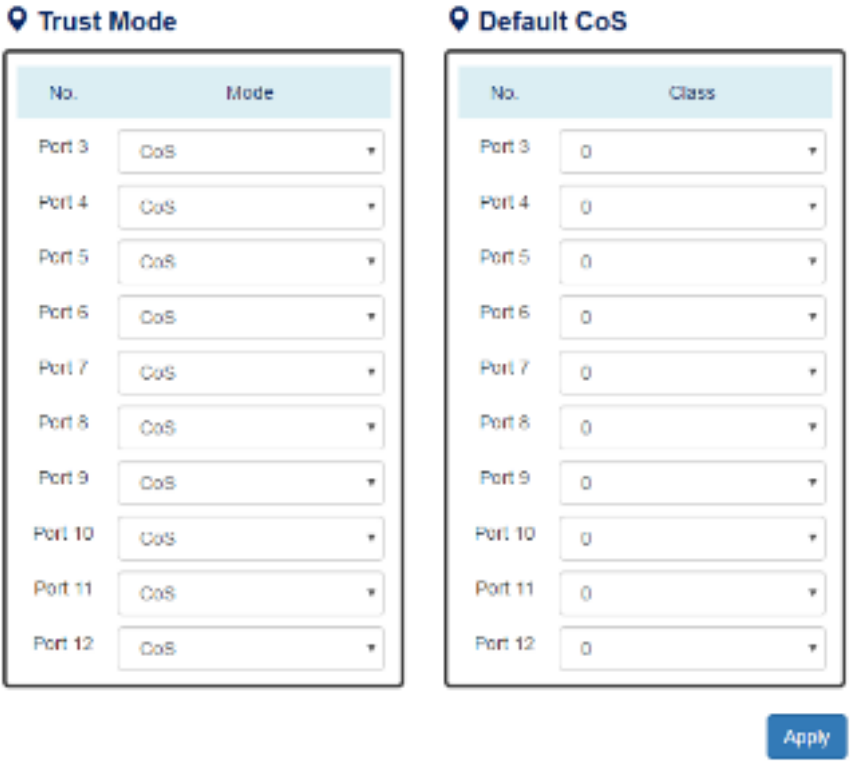
Queue Weight

Queue – поддерживается 8 очередей для передачи трафика от 0 до 7.

Weight – задает определенный «вес» для порта. Диапазон возможных значений от 1 до 100. Вес для каждого номера очереди представлен в таблице ниже:

Queue Weight	0	1	2	3	4	5	6	7
	1	2	3	4	5	6	7	8

8.16.2 Настройка режима Trust для QoS и CoS по умолчанию



Trust Mode

No – номер порта от 1 до N, где N – общее количество портов коммутатора.

Mode – выбор режима «доверия»

CoS – Class of Service. Использует 3 бита «PRI» в поле VLAN тега. Это позволяет классифицировать весь трафик на 8 различных классов от 0 до 7;

DSCP – использует 6 битов «DSCP» в поле ToS тега. Позволяет разделить весь сетевой трафик на 64 различных типа от 0 до 63.

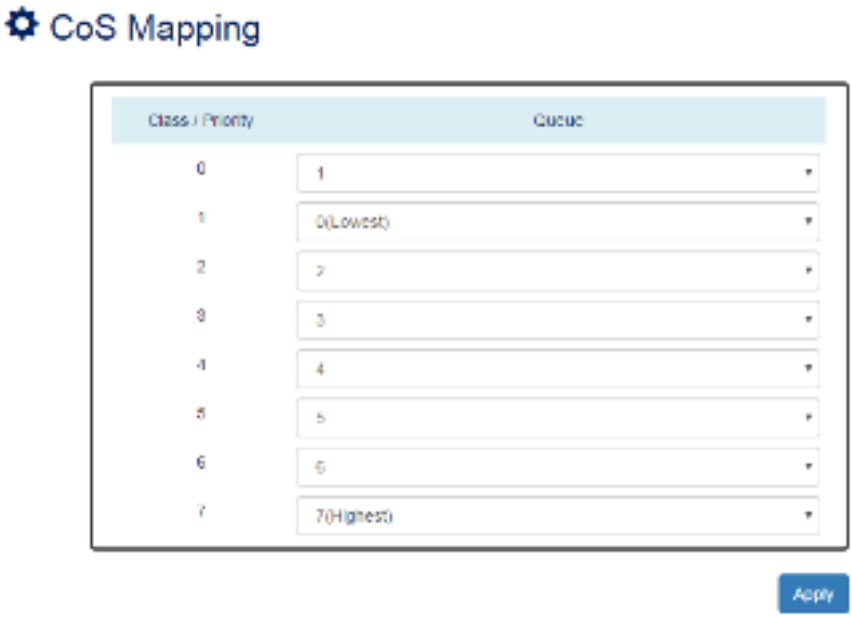
Default CoS

No – номер порта от 1 до N, где N – общее количество портов коммутатора.

Class – пользователь может определить класс трафика для порта. Система будет автоматически ставить класс трафика в передаваемые фреймы в заголовок. По умолчанию класс каждого порта равен 0.

Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.16.3 Настройка CoS



Class / Priority

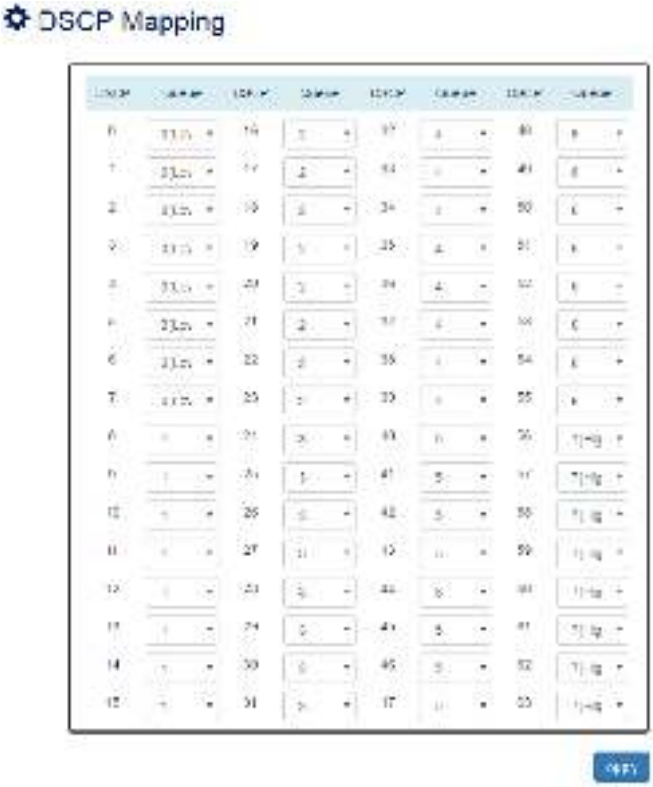
В поле CoS называемом «PRI» в теге VLAN содержится 3 бита с информацией о классе трафика от 0 до 7

Queue

Коммутатор поддерживает до 8 очередей сетевого трафика от 0 до 8. Трафик в очереди 8 имеет наименьший приоритет, а в очереди 7 наибольший. Настройка очередей по умолчанию дана в таблице ниже:

Class	0	1	2	3	4	5	6	7
Queue	1	0	2	3	4	5	6	7

8.16.4 Настройка ToS (DSCP)



DSCP

В поле ToS называемом «DSCP» в теге ToS содержится 6 битов с информацией о типе трафика от 0 до 63.

Queue

Коммутатор поддерживает до 8 очередей сетевого трафика от 0 до 8. Трафик в очереди 8 имеет наименьший приоритет, а в очереди 7 наибольший. Настройка очередей по умолчанию дана в таблице ниже:

Type: Queue	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
	0	1	2	3	4	5	6	7

Apply (Apply Button) Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.17 Port Trunk (агрегация каналов)

Функция Port Trunk (создание транков портов), также известная как Link Aggregation (агрегация каналов) позволяет объединять группы линков в trunk'и.

Всего обеспечивается 8 групп Trunk ов. Это хороший способ распределить нагрузку в сети и создать запасные линки.

Например, когда порты с 1 по 4 объединены в trunk 1 и все порты поддерживают скорость 100Tx в полном дуплексе общая пропускная способность такого trunk'а будет равна 800Мбит/с.

Трафик, передающийся в trunk, распределяется по одному из каналов на основе MAC адреса источника для достижения баланса нагрузки.

Если режим создания trunk'а выставлен, как «LACP», и один из каналов внутри trunk'а вышел из строя, то весь трафик будет передан по другому каналу в таком trunk'е.

8.17.1 Настройка функции Port Trunk

Group – 8 групп trunk’ов.

Trunking Mode – 2 метода организации trunk’ов:

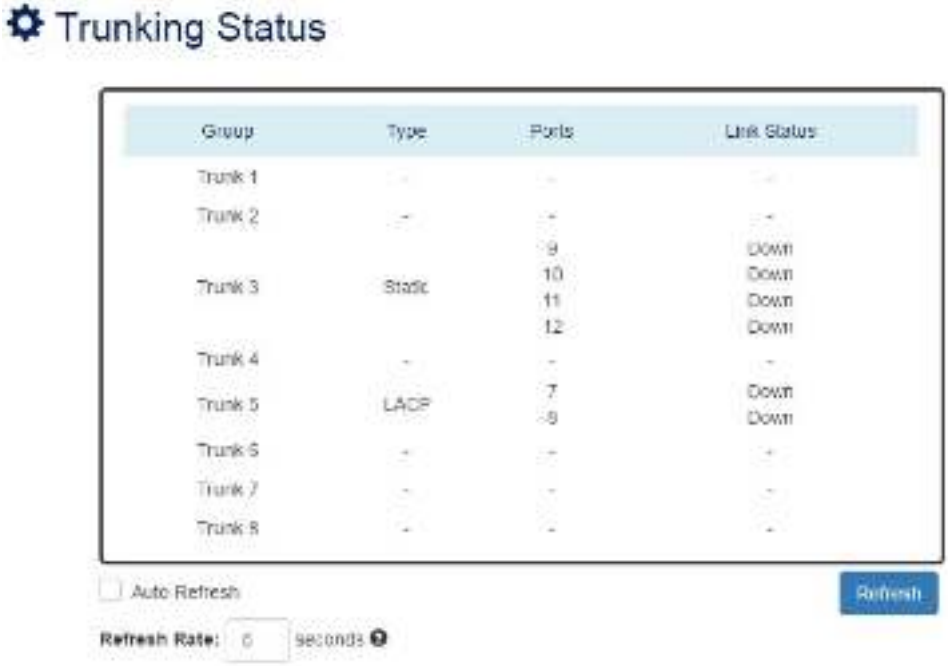
Static – трафик передается по одному из каналов в группе. Канал определяется MAC адресом в заголовке пакета. Если канал не исправен трафик не может быть передан остальными каналами в группе;

LACP – динамическая организация trunk’ов. Если текущий канал передачи данных не исправен трафик может быть передан по другому каналу в группе.

Member Ports – отметьте порты-участники trunk группы. Порт может принадлежать только одной из trunk групп.

Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.17.2 Статус функции Port Trunk



Group – поддерживаемые trunk группы от Trunk 1 до Trunk 8

Type – метод организации trunk'ов. «-» отображается если не выбраны порты для организации trunk'ов.

Ports – порты- участники trunk группы

Link Status – поле отображает текущее состояние для конкретного порта. UP или Down.

8.18 Storm Control (Защита от широковещательного шторма)

Широковещательный шторм (Net Storm или Broadcast Storm) происходит, если в сети передается/принимается слишком много пакетов.

Функция Storm Control используется для предотвращения обрушивания сети multicast broadcast или другим видом трафика.

Когда функция Storm Control включена для определенного вида трафика, система будет осуществлять проверку входящего трафика. Если трафик отличается от настроенного, система будет отбрасывать пакеты для предотвращения возникновения шторма.

8.18.1 Настройка функции Storm Control

Traffic Type – выбор типа отслеживаемого трафика:

Broadcast, Multicast и Unknown Unicast.

Mode – вкл/выкл функцию Strom Control для конкретного типа трафика.

Level – три уровня скорости приема пакетов. Если принимается слишком много пакетов в сек выбранного типа трафика система начнет автоматически дропать их во избежание возникновения широковещательного шторма.

High (Высокий) – более чем 2500 пакетов / сек;

Middle (Средний) – более чем 1000 пакетов / сек;

Low (Низкий) – более чем 500 пакетов / сек.

Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.19 Port-Based Network Control IEEE 802.1X (контроль доступа и аутентификации)

IEEE 802.1X это протокол контроля доступа и аутентификации, который ограничивает права неавторизованных компьютеров, подключенных к коммутатору. Протокол контроля Port-based является удобным средством обеспечения безопасности, так как аутентификация проходит только один раз для каждого порта, и нет необходимости в дальнейшем проходить ее снова, при смене подключенного устройства, например.

Управление доступом основанное на MAC адресе (MAC - based) это более безопасный, но менее удобный способ аутентификации. В сеть может получить доступ лишь то устройство, которое прошло проверку MAC адреса.

Оба метода являются необязательными к использованию и могут быть отключены совсем.

8.19.1 Базовая настройка 802.1X

Basic Settings (базовые настройки)

802.1X Mode – вкл/выкл (enable/disable) функцию контроля доступа.

Server Type – выбор сервера для аутентификации согласно 802.1X. «Local Database» или «RADIUS Server»

Local Database – база данных хранящаяся на коммутаторе. Клиент при авторизации отправляет имя и пароль, которые сравниваются с теми, что хранятся в базе данных коммутатора.

RADIUS Server – база данных, которая поддерживается на всех устройствах с протоколом RADIUS. Аутентификация выполняется по протоколу RADIUS и включает в себя шифрование.

8.19.2 Настройка 802.1X для портов

<u>Port Settings</u> (Настройка портов)

<u>No</u> – номер порта от 1 до N, где N – общее количество портов коммутатора.

<u>Enable</u> – состояние функции контроля доступа 802.1X на выбранном порте. YES значит, что функция 802.1X активна и порт заблокирован, пока не будет выполнена аутентификация.

Mode – выбор метода аутентификации:

MAC-based – аутентификация на основе MAC адреса. Только устройство с известным MAC может быть подключено к сети;

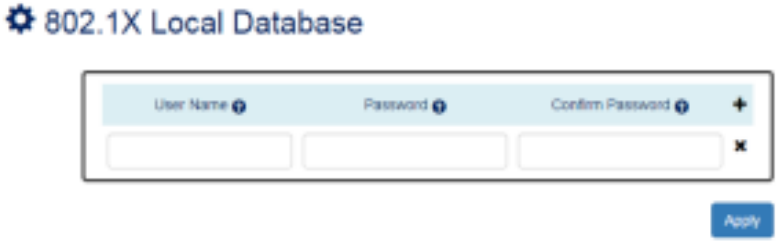
Port-based – аутентификация на основе порта, любое устройство подключенное к порту может получить доступ к сети.

Re-Auth – вкл/выкл повторную аутентификацию на порте. Порт будет запрашивать повторную аутентификацию через время указанное в Re-Auth Period.

Re-Auth Period – Интервал времени, через который порт будет запрашивать повторную аутентификацию.

Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.19.3 Настройка локальной базы данных



User Name

Имя пользователя, который будет проходить аутентификацию

Максимальная длина 32 символа. Нельзя использовать символы **# \ ' " ?**

Password

Пароль, используется для аутентификации пользователя.
Максимальная длина 32 символа. Нельзя использовать символы **# \ ' " ?**

Confirm Password

Введите пароль еще раз в качестве подтверждения.

Нажмите, чтобы добавить нового пользователя и пароль

Нажмите, чтобы удалить запись о пользователе из таблицы

Apply (Apply Button) Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.19.4 Настройка сервера RADIUS

Server IP – IP адрес сервера RADIUS

Service Port – сервисный порт, который будет прослушиваться на сервере RADIUS

Shared Key – ключ, используемый для подтверждения подключения между сервером и устройством, запрашивающим аутентификацию до процесса самой аутентификации.

Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.20 Port Mirroring (Зеркалирование портов)

Зеркалирование портов (Port Mirroring) позволяет копировать входящие и исходящие пакеты с одного или нескольких портов на порт назначения. Это очень полезный инструмент мониторинга сетевого трафика, который поможет внимательно следить за сетью и отслеживать возникновение проблем.

8.20.1 Настройка функции Port Mirroring

Mirroring Mode – вкл/выкл (enable/disable) функции Port Mirroring. Если пользователь включил зеркалирование, система будет копировать сетевой трафик с порта-источника (Source port) на порт назначения (Destination Port) с использованием режима Sniffer Mode.

Source Port – порт или порты с которого/которых трафик будет копироваться на порт назначения (Destination port)

Sniffer Mode

Both Tx and Rx – режим копирования на порт назначения (Destination port) как принимаемых так и отправляемых пакетов;

Tx Only – режим копирования на порт назначения (Destination port) только принимаемых пакетов;

Rx Only – режим копирования на порт назначения (Destination port) только отправляемых пакетов.

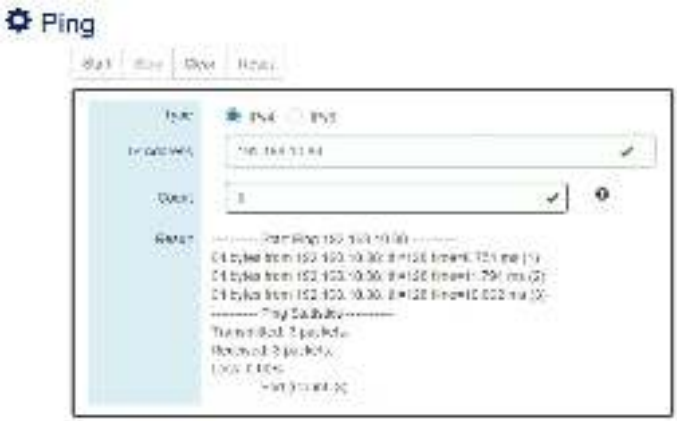
Destination Port – порт назначения, на который копируется трафик с порта/портов источника (Source port) для дальнейшего анализа.

Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.21 Ping (команда PING)

Ping это простой инструмент для проверки состояния подключения в IP сети. PING подразумевает отправку запроса согласно протоколу ICMP конечному устройству и ожидания ответного сообщения с целью проверки подключения.

8.21.1 Использование команды PING с IPv4/IPv6



Type – выбор протокола IPv4 или Pv6

IP Address – IP адрес подключенного сетевого устройства. Формат адреса основан на выборе протокола в поле Type.

Count – количество отправленных сообщений ICMP на заданный IP адрес. Диапазон возможных значений от 3 до 50. Значение по умолчанию 3.

Result – поле с результатами работы PING отображает ответы от удаленного IP устройства. Если удаленное устройство не отвечает на запросы будет отображено No Response (нет ответа).

«Start» Button – Нажмите кнопку, чтобы начать пинговать удаленный IP адрес.

«Stop» Button – Нажмите кнопку, чтобы закончить пинговать удаленный IP адрес.

«Clear» Button – Нажмите кнопку, чтобы очистить поле Result от информации.

«Reset» Button – Нажмите кнопку, чтобы сбросить ранее заданную информацию (IP Address, Count) и результаты в поле Result.

8.22 LLDP (функция оповещения «соседей»)

LLDP (IEEE 802.1AB) протокол канального уровня, позволяющий сетевому оборудованию оповещать оборудование, работающие в локальной сети о своем существовании и передавать ему свои характеристики, а также получать от него аналогичные сведения.

8.22.1 Настройка LLDP

LLDP Mode

Вкл/выкл функцию LLDP в коммутаторе.

LLDP Timer

Интервал отправки LLDP сообщений. Диапазон возможных значений от 5 до 32767 сек. Значение по умолчанию 30 сек.

Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.22.2 LLDP таблица «соседей»

Local Port

Порт, подключенный к LLDP «соседу» в коммутаторе

Remote System Name

Имя LLDP «соседа». Это имя настраивается на удаленном устройстве.

Chassis ID

Этот идентификатор определяет MAC адрес LLDP «соседа».

Remote Port

Поле отображает информацию о порте, полученную от LLDP «соседа»

Port ID

Port ID отображает идентификатор порта, подключенного LLDP «соседа».

Address

Поле отображает IP адрес LLDP «соседа».

8.23 System Warning (Системные оповещения)

Системные оповещения содержат следующие типы оповещений:

«System Event Log» (Журнал системных событий);

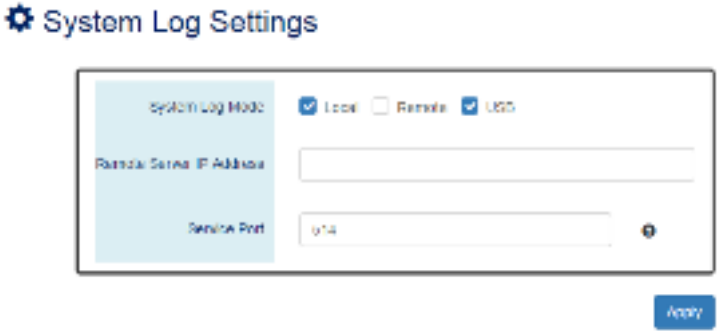
«SMTP Settings» (Настройки SMTP);

«Event Selection» (Выбор события).

Эти журналы со сведениями очень полезны для системного администратора, как средство отладки сети. Когда система была отключена, кто пытался выполнить вход в систему, когда система была перезапущена в нештатном режиме и тд. – все эти события попадают в журналы.

Пользователь может дополнительно настроить звуковое оповещение, используя выходы реле на коммутаторе.

8.23.1 Настройка системных оповещений



System Log Mode

Выбор способа сохранения логов (записанных событий).

Local – в памяти коммутатора;

Remote – на удаленном сервере;

USB – на USB flash накопитель.

Remote Server IP Address

Поле содержит IP адрес удаленного сервера. Если выбран режим сохранения логов «Remote», пользователи могут использовать указанный IP адрес для получения системных логов.

Service Port

Порт, использующийся для прослушивания пакетов с логами от удаленного сервера.

Диапазон возможных значений выбора порта от 1 до 65535.

Значение порта по умолчанию – 514.

Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.23.2 Журнал системных событий

Log Text Area

В это поле отображаются системные события, если в System Log Mode выбрано значение Local.

Нажмите эту кнопку, чтобы очистить журнал системных событий.

Refresh Нажмите эту кнопку чтобы обновить информацию в журнале системных событий.

8.23.3 Настройка SMTP Информации

Server Settings (Настройки сервера SMTP)

SMTP Status – вкл/выкл функцию SMTP.

Server Address – поле с IP адресом или URL ссылкой SMTP почтового сервера. Например, адрес SMTP сервера, предоставляемого Google – smtp.gmail.com

Server Port – поле содержащее номер порта, прослушивающего запросы от SMTP сервера. Для безопасности, рекомендуется использовать порты 465 для SSL и 587 для TLS.

Диапазон возможных значений от 1 до 65535. Значение по умолчанию – 25. Порт 25 – порт по умолчанию для e-mail сервера.

Sender E-mail – e-mail адрес отправителя.

Mail Subject – тема e-mail сообщения.

Нельзя использовать символы **#** \ **' " ?**

SMTP Authentication – вкл/выкл выполнение аутентификации на SMTP сервере с использованием имени пользователя и пароля.

User Name – имя пользователя, используется для аутентификации на SMTP сервере. Максимальная длина 32 символа. Нельзя использовать символы **#** \ **' " ?**

Password – пароль, используется для аутентификации на SMTP сервере вместе с именем пользователя (User Name). Максимальная длина 32 символа. Нельзя использовать символы **#** \ **' " ?**

Recipient Settings (Настройки получателей)

E-mail Address 1-4 – e-mail адреса получателей уведомлений. Поля доступны к заполнению, если SMTP отправка включена.

Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.23.4 Настройка выбора событий

Event

Предусмотрено реагирование на 5 типов системных событий:

Authentication Failure – Ошибка логина при входе с WEB или через командную строку. Может быть вызвано вводом неправильного имени пользователя или пароля.

ERPS Change – защита от петель ERPS работает и топология изменилась.

Power 1 or 2 – Один из источников питания отключился / вышел из строя.

Cold Start – система была перезагружена из за отключения питания.

Warm Start – система была перезагружена с помощью команды reboot через командную строку или с помощью кнопки reboot в WEB интерфейсе

Digital Input – уровень сигнала на пинах DI изменился с высокого на низкий или наоборот.

Interface Events

Event	Fault Alarm	System Log	SMTP	SNMP Trap
All Ports Link	Down	Up Down	Up Down	Up Down
Port 1 Link	Down	Up Down	Up Down	Up Down
Port 2 Link	Down	Up Down	Up Down	Up Down
Port 3 Link	Down	Up Down	Up Down	Up Down
Port 4 Link	Down	Up Down	Up Down	Up Down
Port 5 Link	Down	Up Down	Up Down	Up Down
Port 6 Link	Down	Up Down	Up Down	Up Down
Port 7 Link	Down	Up Down	Up Down	Up Down
Port 8 Link	Down	Up Down	Up Down	Up Down
Port 9 Link	Down	Up Down	Up Down	Up Down
Port 10 Link	Down	Up Down	Up Down	Up Down
Port 11 Link	Down	Up Down	Up Down	Up Down
Port 12 Link	Down	Up Down	Up Down	Up Down

Apply

Event – отображают статус линка для каждого порта. Аварийный сигнал срабатывает только если линк пропал и в системных событиях поддерживается как установление соединения, так и ошибка установления соединения.

Fault Alarm – LED индикатор ошибки на коммутаторе загорится красным, и сработает реле, если настроенные события произошли. По умолчанию индикатор ошибки горит зеленым, а реле не срабатывает.

System Log – когда настроенные события произошли, они попадают в журнал системных событий на удаленном сервере, на USB накопителе и тд.

SMTP – если отправка логов по электронной почте (SMTP) активна, то когда настроенные события произошли, система отправит запись о них на указанные e-mail адреса (SMTP Settings).

SNMP Trap – если функция SNMP Trap включена, то, когда настроенные события произошли, система отправит информацию о них на IP адрес получателя сообщений SNMP Trap.

Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

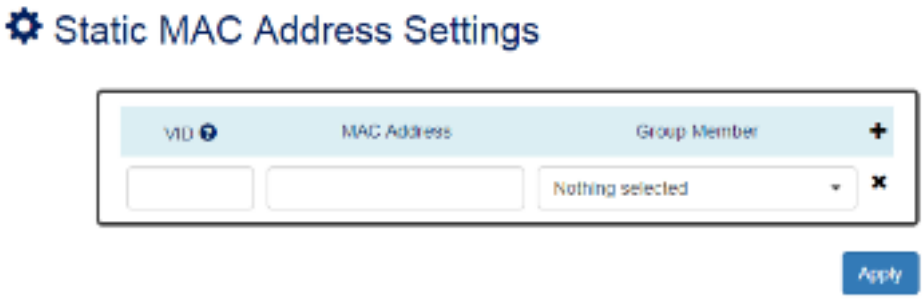
8.24 MAC Table (Таблица MAC адресов)

MAC адрес (Media Control Access address) – уникальный идентификатор, присваиваемый каждой единице активного сетевого оборудования в компьютерных сетях Ethernet.

Заполнение таблицы MAC адресов в коммутаторе необходимо для более эффективной передачи пакетов внутри сети. Когда коммутатор получает пакет, система проверяет таблицу MAC адресов и направляет пакет в соответствующий порт.

Таблица MAC адресов динамически наполняется MAC адресами. Когда система получает MAC адрес которого нет в таблице, она пересылает пакет на все порты LAN в той же VLAN. Когда устройство, которому предназначен пакет отвечает, система добавляет его MAC адрес в таблицу.

8.24.1 Настройка постоянных (static) MAC адресов



VID

VID это ID группы VLAN, которая содержит заданный MAC адрес. Диапазон возможных значений от 1 до 4094.

MAC Address

Это поле содержит постоянный MAC адрес портов-участников VLAN группы.

Group Member

Участник группы – это порт принадлежащий VLAN группе, которому принадлежит настроенный постоянный MAC адрес.

Нажмите, чтобы добавить дополнительный постоянный MAC адрес

Нажмите, чтобы удалить привязку постоянного MAC адреса.

Apply (Apply Button) Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.24.2 Таблица MAC адресов

VID

VID это ID VLAN содержащей настроенный MAC адрес.

MAC Address

Этот столбец содержит список заданных MAC адресов.

Type

Отображает тип MAC адреса:

Learning – MAC адрес был получен от передаваемых пакетов;

Static – MAC адрес был вручную задан пользователем.

Source

Отображает порт, которому принадлежит MAC адрес.

8.25 Authorization (Вход в систему управления коммутатором)

Имя пользователя (username) и пароль (password) играют ключевую роль при управлении коммутатором через WEB интерфейс или командную строку. Пользователи обязаны выполнить вход в систему, прежде чем вносить какие-либо изменения в конфигурацию коммутатора. Настоятельно рекомендуется изменить хотя бы пароль для доступа к коммутатору в рамках безопасности.

8.25.1 Настройка информации для входа в систему

Username (имя пользователя)

Необходимо для входа в систему.

Максимальная длина 20 символов. Можно использовать только латинские символы обоих регистров(A-Z, a-z) и числа от 0 – 9. Имя пользователя по умолчанию **admin**

Password (пароль)

Пароль необходим для входа в систему.

Максимальная длина 20 символов. Можно использовать только латинские символы обоих регистров(A-Z, a-z) и числа от 0 – 9. Пароль пользователя по умолчанию **admin**

Confirm Password (пароль подтверждение)

Необходимо ввести Password еще раз в этом поле для подтверждения.

Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

8.26 Firmware Upgrade (Обновление прошивки)

Для стабильной работы и наилучшей совместимости с промышленными приложениями рекомендуется обновлять систему до новейшей прошивки, представленной на нашем сайте.

Предусмотрено 2 способа выполнения процедуры обновления прошивки из WEB интерфейса:

1) С помощью USB накопителя, сохранив на нем файл с прошивкой;
2) С помощью ПК, сохранив на жестком диске ПК файл с прошивкой.

8.26.1 Загрузка файла с прошивкой

Firmware Image

Нажмите «+Selected File» чтобы выбрать образ с прошивкой.

Версия прошивки отображается в системе и основана на имени файла с прошивкой. Пользователь может добавить номер прошивки к имени файла с прошивкой. Например, XXX-v1.2.3, где XXX – оригинальное имя файла с прошивкой.

Selected File

После выбора файла с прошивкой его имя отобразится в этом поле.

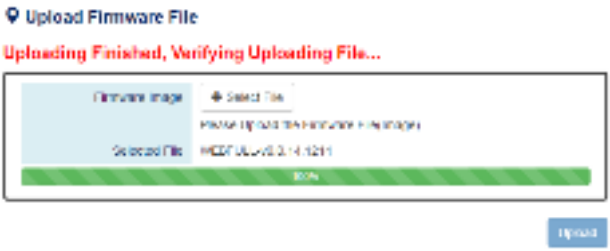
После выбора прошивки на ПК, нажмите эту кнопку, чтобы загрузить прошивку в коммутатор.

8.26.2 Процесс загрузки файла с прошивкой в коммутатор

Следующие шаги выполняются, когда система приступила к обновлению прошивки:

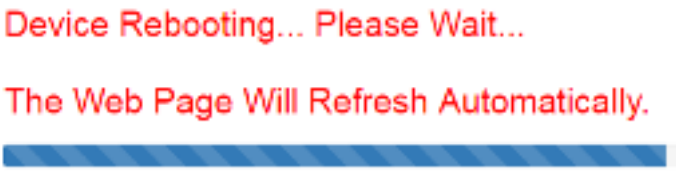
1. Процесс загрузки образа с прошивкой. Прогресс будет отображен шкалой заполнения (в %);

2. Проверка загруженного файла. Когда процесс загрузки образа с прошивкой завершен на 100%, система приступит к проверке загруженного файла, чтобы убедится, что он подходит. По умолчанию образ прошивки зашифрован.



3. Установка загруженного файла с прошивкой. Новая прошивка будет установлена на коммутатор после окончания процесса проверки.

4. Перезагрузка системы. Система будет перезагружена автоматически, если процесс обновления прошивки прошел без ошибок.



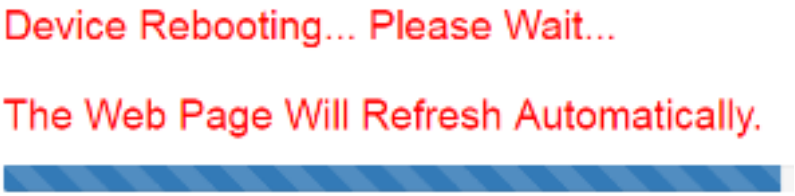
8.26.3 Копирование файла с прошивкой с USB накопителя

1. Копирование файла с прошивкой с USB накопителя в коммутатор. Система проверяет, вставлен ли USB накопитель, а также наличие файла на нем.

2. Процесс проверки загруженного файла. После копирования файла прошивки на коммутатор, система выполняет его проверку на совместимость. По умолчанию файл прошивки шифруется.

3. Процесс установки загруженного файла с прошивкой. Новая прошивка будет установлена на коммутатор после окончания процесса проверки.

4. Перезагрузка системы. Система будет перезагружена автоматически, если процесс обновления прошивки прошел без ошибок.



8.27 Config Backup (Создание резервной копии настроек)

Зачастую, в сети работает несколько одинаковых коммутаторов и чтобы настроить их на одни и те же функции, пользователю достаточно настроить только один из коммутаторов, и, сохранив настройки в файл, перенести их на остальные.

Файл с текущими настройками может быть сохранен, как на ПК так и на USB накопитель.

8.27.1 Сохранение резервного файла с настройками

<u>Backup to Localhost</u> (Создание резервной копии настроек на ПК)

<u>File Name</u> – укажите имя файла для сохраняемой резервной копии с настройками, который будет загружен на ПК.

Backup to USB (Создание резервной копии настроек на Flash накопителе)

Backup Running Config File – укажите имя файла для сохраняемой резервной копии с текущими настройками, который будет загружен на USB Flash накопитель

Backup Start Config File – укажите имя файла для сохраняемой резервной копии со стартовыми настройками, который будет загружен на USB Flash накопитель.

Нажмите эту кнопку, чтобы выполнить процесс загрузки файла с настройками на ПК или USB накопитель

Примечание!

Если поле имени файла оставить пустым система создаст файл с именем по умолчанию config-[datatime].cfg

8.28 Config Restore (Восстановление настроек из файла)

Пользователю рекомендуется сохранять файл с конфигурацией после серии настроек коммутатора. Если на другом коммутаторе потребуются аналогичные настройки, пользователь может восстановить их из файла.

8.28.1 Восстановление настроек из файла

Restore from Localhost (Восстановление настроек из файла с ПК)

File Name – Выберите ранее сохраненный файл с настройками на ПК.

Restore from USB (Восстановление настроек из файла с USB Flash накопителя)

File Name in USB – укажите имя файла с настройками, сохраненного на USB Flash накопителе. Если файл находится в папке, укажите полный путь.

Нажмите эту кнопку, чтобы восстановить настройки коммутатора из файла с ПК или USB Flash накопителя.

8.29 USB Auto-Load & Auto – Backup (Функция автоматического сохранения/загрузки настроек)

USB Auto-Load – вкл/выкл (enable/disable) функции автоматической загрузки настроек. Если функция включена, то система будет искать файл со стартовой конфигурацией (startuo-config) на USB Flash накопителе и загружать его при перезагрузке.

USB Auto-Backup – вкл/выкл (enable/disable) функции автоматического сохранения настроек. Если данная функция включена, то система будет сохранять файл с текущими настройками (running config) на USB Flash накопителе при каждом изменении конфигурации коммутатора.

Кнопка подтверждения сохранения внесенных данных. После ее нажатия внесенные изменения будут применены.

Внимание
Для защиты оборудования от грозовых разрядов необходимо устанавливать устройства грозозащиты!

9. Технические характеристики*

Модель	**SW-71604/WL**
Общее кол-во портов	20
Кол-во портов FE+PoE	-
Кол-во портов FE	-
Кол-во портов GE+PoE	-
Кол-во портов GE (не Combo порты)	16
Кол-во портов Combo GE (RJ45+SFP)	-
Кол-во портов SFP (не Combo порты)	4
Встроенные оптические порты	-
Мощность PoE на один порт (макс.) Вт	-
Суммарная мощность всех портов (макс.) (Вт)	-
Стандарты PoE	-
Метод подачи PoE	-
Топологии подключения	звезда каскад кольцо
Буфер пакетов	12 МБ
Таблицы MAC-адресов	16 К
Пропускная способность коммутационной матрицы (Switching fabric)	40 Гбит/с

Скорость обслуживания пакетов (Forwarding rate)	1000Mbps port – 1,488,000 пакетов/с 100Mbps port - 148,800 пакетов/с 10Mbps port - 14,880 пакетов/с
Поддержка jumbo frame	9,6 КБ
Стандарты и протоколы	• IEEE 802.3 – 10BaseT • IEEE 802.3u – 100BaseTX • IEEE 802.3ab – 1000BaseT • IEEE 802.3z 1000 BaseSX/LX • IEEE 802.3af Power over Ethernet (PoE) • IEEE 802.3at Power over Ethernet (PoE+) • IEEE 802.3x – Flow Control • IEEE 802.1Q – VLAN • IEEE 802.1p – Class of Service • IEEE 802.1D – Spanning Tree • IEEE 802.1w – Rapid Spanning Tree • IEEE 802.1s – Multiple Spanning Tree • IEEE 802.3ad – Link Aggregation Control Protocol (LACP) • IEEE 802.1AB – LLDP (Link Layer Discovery Protocol) • IEEE 802.1X – Access Control • ITU-T G.8032/Y.1344-Ethernet Ring ProtectionSwitching (ERPS)
Функции уровня 2	• IEEE 802.1D (STP) • IEEE 802.1w (RSTP) • IEEE 802.1s (MSTP) • VLAN • VLAN Group 4K • Tagged Based • Port-based • Voice VLAN • Link Aggregation IEEE 802.3ad with LACP • IGMP Snooping • IGMP Snooping v1/v2/v3 Supports 1023 IGMP groups • IGMP Static Multicast Addresses • Querier, Immediate Leave • Storm Control • G.8032-Ethernet Ring Protection Switching (ERPS)

QoS	• CoS • DSCP • WRR/SPQ Queuing
Безопасность	• Management System User Name/Password Protection • IEEE 802.1x Port-based Access Control • RADIUS (Authentication, Authorization, Accounting) • HTTP & SSL (Secure Web) • SSH v2.0 (Secured Telnet Session)
Управление	• Web management – управление через Web-интерфейс • CLI • Telnet • SNMP
Индикаторы	PWR1, PWR2, Fault, Ring Master, Ring State; Link/наивысшая скорость(зел.), низкая скорость (жёлт.) PoE: индикация подключения PoE устройств
Реле аварийной сигнализации	DC24V,1A(НО, НЗ)
Питание	Блок питания AC 100-240V / DC 48V, 1A
Энергопотребление	<23Вт
Встроенная грозозащита	-
Охлаждение	Конвекционное (без вентилятора)
Класс защиты	IP65
Размеры (ШхВхГ) (мм)	300x230x111
Способ монтажа	Монтаж на стену, на столб (крепление приобретается отдельно)
Рабочая температура	-40…+50°C
Относительная влажность	0-95% без конденсата
Дополнительно	-

* Производитель имеет право изменять технические характеристики изделия и комплектацию без предварительного уведомления.

10. Гарантия

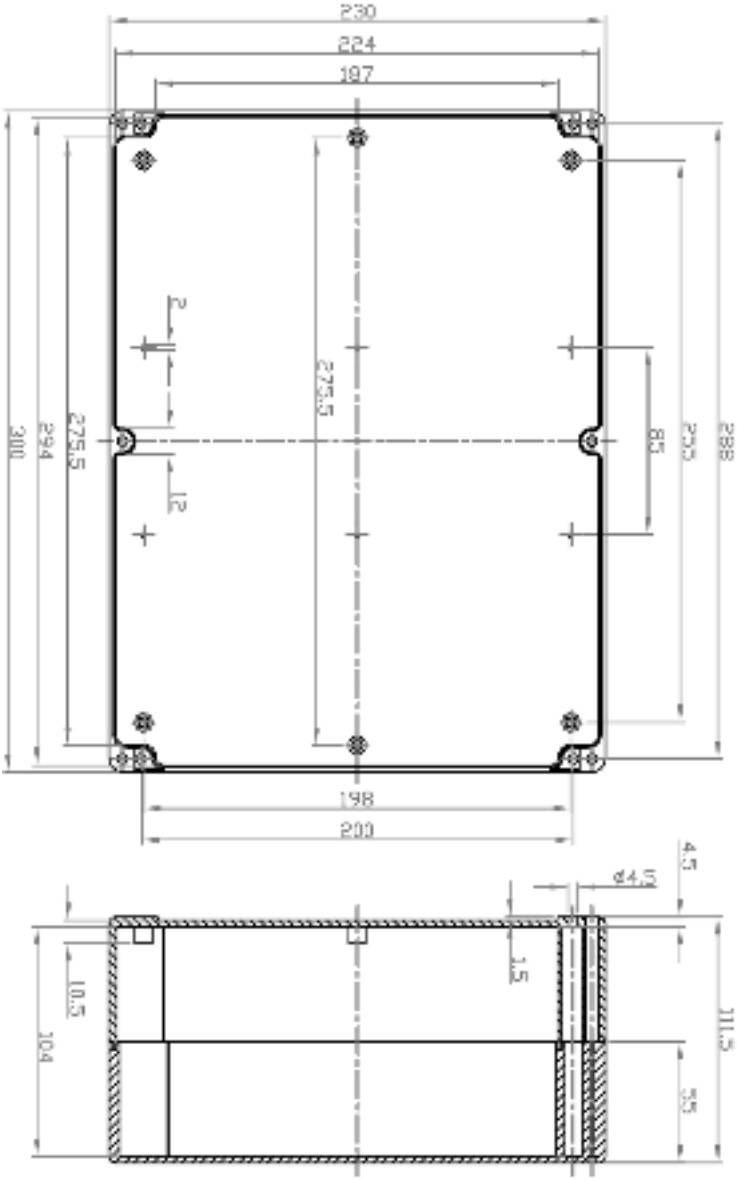
Гарантия на все оборудование OSNOVO – 60 месяцев с даты продажи, за исключением аккумуляторных батарей, гарантийный срок - 12 месяцев.

В течение гарантийного срока выполняется бесплатный ремонт, включая запчасти, или замена изделий при невозможности их ремонта.

Подробная информация об условиях гарантийного обслуживания находится на сайте www.osnovo.ru

Составил: Елагин С.А.

11. Приложение А «Габаритные размеры»



* Все размеры даны в мм

12. Приложение Б «Крепления на стену / на опору»

Для монтажа уличных коммутаторов на стенах, опорах, подвесах и т.д применяются настенные крепления (приобретаются отдельно).

Для монтажа уличного коммутатора на стену или опору:

1. Распаковать крепления.

2. Расположить корпус на твердой ровной поверхности, приложить планки креплений к задней стенке корпуса так, чтобы сквозные крепежные отверстия корпуса совпадали с отверстиями, просверленными для этой цели в планках

3. Прикрепить планки к корпусу болтами М4, используя шайбы и гайки (имеются в комплекте) прикрепить планки к корпусу коммутатора.

4. Планки обеспечивают возможность крепления коммутатора на стену и другие плоские поверхности. Для крепления на столб присоединить к планкам крепежные зубчатые элементы треугольной формы (крепежные элементы вдвигаются внутрь планок).

5. Отрезав кусок перфорированной металлической ленты (имеется в комплекте), используя ленту, укрепить корпус коммутатора на столбе или опоре, затянуть винтами.