

OSNOVO

cable transmission

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

Уличный управляемый (L2+) PoE коммутатор на 6 портов с термостабилизацией и резервным питанием

SW-80402/WLU



Прежде чем приступить к эксплуатации изделия,
внимательно прочтите настоящее руководство

www.osnovo.ru

Содержание

| | |
|--|----|
| 1. Назначение | 5 |
| 2. Комплектация | 6 |
| 3. Особенности оборудования | 6 |
| 4. Внешний вид и описание элементов | 7 |
| 4.1 Внешний вид | 7 |
| 4.2 Описание разъемов и индикаторов уличного коммутатора | 8 |
| 5. Установка и подключение | 9 |
| 6. Проверка работоспособности системы | 12 |
| 7. Подготовка перед управлением коммутатором через WEB. | 13 |
| 8. Управление через WEB интерфейс. | 16 |
| 8.1 Основные сведения | 16 |
| 8.2 Главное меню WEB интерфейса | 17 |
| 8.3 Network Admin (Настройка сетевых параметров и администрирование) | 18 |
| 8.3.1 IP Configuration (Настройка IP адреса) | 18 |
| 8.3.2 SNTP Configuration (Настройка протокола времени SNTP) | 19 |
| 8.3.3 SNMP Configuration (Настройка протокола управления SNMP) | 20 |
| 8.3.4 System Log Configuration (Настройка системного журнала) | 22 |
| 8.4 Port Configure (Конфигурирование портов) | 23 |
| 8.4.1 Port Configuration (Настройка портов) | 23 |
| 8.4.2 Link aggregation (Агрегация каналов) | 24 |
| 8.4.3 Port Mirroring (Зеркалирование портов) | 27 |
| 8.4.4. Thermal Protection Configuration (Температурная защита) | 28 |
| 8.5 PoE Configuration (Конфигурация PoE) | 29 |
| 8.5.1 PoE Setting (Настройки PoE) | 30 |
| 8.5.2 PD Alive (Функция антизависания для PoE устройств) | 31 |
| 8.5.3 PoE Status (Состояние PoE на портах) | 32 |

| | |
|---|----|
| 8.6 Advanced Configure (Расширенные настройки)..... | 32 |
| 8.6.1 VLAN (Настройка VLAN)..... | 32 |
| 8.6.2 Port Isolation (Изоляция портов) | 37 |
| 8.6.3 STP (Протокол связующего дерева) | 38 |
| 8.6.4 MAC Address Table (Таблица MAC адресов)..... | 41 |
| 8.6.5 IGMP Snooping | 42 |
| 8.6.6 ERPS (Протокол ERPS)..... | 45 |
| 8.6.7 LLDP (Настройка протокола LLDP) | 48 |
| 8.6.8 Loop Protection (Защита от сетевых петель) | 49 |
| 8.7 QoS (Приоритезация трафика)..... | 50 |
| 8.7.1 QoS Port Classification (Классификация портов с помощью QoS) | 51 |
| 8.7.2 Port Policing (Функция ограничения скорости на портах) | 52 |
| 8.7.3 Storm Control Configuration (Настройка защиты от сетевого шторма)..... | 53 |
| 8.8 Security Configure (Настройки безопасности) | 54 |
| 8.8.1 Password (Пароль)..... | 54 |
| 8.8.2 802.1X..... | 54 |
| 8.8.3 DHCP Snooping (Защита от атак с использованием DHCP) | 56 |
| 8.8.4 IP&MAC Source Guard..... | 57 |
| 8.8.5 ARP Inspection (Проверка ARP пакетов)..... | 60 |
| 8.8.6 ACL (Правила контроля доступа) | 63 |
| 8.9 Diagnostics (Инструменты диагностики и мониторинга) | 66 |
| 8.9.1 Ping Test (Тестирование соединения с помощью PING)..... | 66 |
| 8.9.2 Cable Diagnostics (Проверка кабеля) | 68 |
| 8.9.3 CPU Load (Загрузка CPU коммутатора)..... | 68 |
| 8.10 Maintenance (Обслуживание)..... | 69 |
| 8.10.1 Restart Device (Перезагрузка коммутатора) | 69 |
| 8.10.2 Factory Defaults (Возврат к заводским настройкам)..... | 69 |

| | |
|---|----|
| 8.10.3 Firmware Upgrade (Обновление прошивки) | 70 |
| 8.10.4 Firmware Select (Выбор текущей прошивки коммутатора) | 70 |
| 8.10.5 Configuration (Текущая конфигурация)..... | 71 |
| 9. Технические характеристики* | 74 |
| 10. Гарантия | 76 |
| 11. Приложение А «Габаритные размеры коммутатора» | 77 |
| 12. Приложение Б «Настенные крепления» | 78 |

1. Назначение

Уличный управляемый (L2+) PoE коммутатор на 6 портов SW-80402/WLU с термостабилизацией и резервным питанием предназначен для объединения сетевых устройств, запитывания их по технологии PoE и передачи данных между ними в условиях эксплуатации вне помещений. В основе устройства лежат высоконадежные комплектующие с расширенным диапазоном температур.

Уличный коммутатор оснащен 6 портами Gigabit Ethernet (10/100/1000Base-T) с PoE (соответствуют стандартам IEEE 802.3af/at и автоматически определяют подключаемые PoE-устройства), а также 2-мя Gigabit Ethernet SFP-слотами (1000Base-FX).

К каждому из 4 основных портов уличного коммутатора можно подключать PoE-устройства мощностью до 30 Вт (общая выходная мощность до 120 Вт).

В уличном коммутаторе предусмотрена функция проверки статуса подключенного PoE устройства (PD Alive). Данная функция активируется через WEB интерфейс и позволяет диагностировать в автоматическом режиме «зависание» подключенных PoE устройств и перезагружать их путем переподдачи PoE питания.

Уличный коммутатор гибко настраивается через WEB-интерфейс и имеет множество функций L2+ уровня, таких как VLAN, IGMP snooping, QoS и др.

Кроме того уличный коммутатор поддерживает автоматическое определение MDI/MDIX (Auto Negotiation) на всех портах - распознает тип подключенного сетевого устройства и при необходимости меняет контакты передачи данных, что позволяет использовать кабели, обжатые любым способом (кроссовые и прямые).

Ввод кабелей внутрь уличного коммутатора осуществляется через гермовводы исключая попадание влаги в бокс (класс защиты – IP66). Корпус уличного коммутатора изготовлен из поликарбоната с высокой устойчивостью солнечным лучам.

Система термостабилизации поддерживает нормальную температуру внутри корпуса, а система резервного питания позволяет уличному коммутатору функционировать даже при отключении основного питания.

Уличный коммутатор SW-80402/WLU оснащен оптическим кроссом для удобного подключения оптоволоконного кабеля.

Уличный коммутатор SW-80402/WLU рекомендуется использовать, если есть необходимость объединить несколько сетевых устройств (IP-камеры, IP-телефоны и пр.) в одну сеть и передать к ним питание по кабелю витой пары (PoE) в условиях эксплуатации вне помещений.

2. Комплектация

1. Уличный коммутатор SW-80402/WLU – 1шт;
2. Набор гермовводов – 1шт;
3. Плавкая вставка предохранитель – 2шт;
4. Пигтейл одномодовый SM SC/UPC – 2шт;
5. Кросс оптический – 1шт;
6. Гильза для защиты сварного стыка (КДЗС) – 2 шт
7. Краткое руководство по эксплуатации – 1шт;
8. Паспорт – 1шт.
9. Упаковка – 1шт;

3. Особенности оборудования

- Уличное исполнение – предназначен для организации сети в условиях эксплуатации вне помещений (класс защиты IP66);
- Система термостабилизации и резервного питания (2 Ач);
- Расширенный диапазон рабочих температур: -50... +50 °С;
- Грозозащита медных портов;
- Управление через WEB интерфейс;
- Поддержка функций L2 (VLAN, QOS, LACP, LLDP, IGMP snooping);
- Поддержка кольцевой топологии подключения;
- PD Alive – функция для автоматической диагностики и перезагрузки зависших PoE устройств;
- Оптический кросс для удобства подключения оптоволоконного кабеля.

4. Внешний вид и описание элементов

4.1 Внешний вид



Рис.1 Уличный коммутатор SW-80402/WLU, вид снаружи

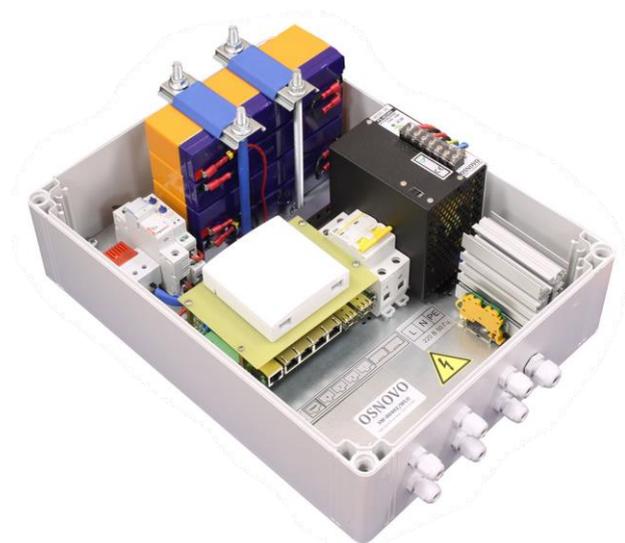


Рис. 2 Уличный коммутатор SW-80402/WLU, вид внутри

4.2 Описание разъемов и индикаторов уличного коммутатора

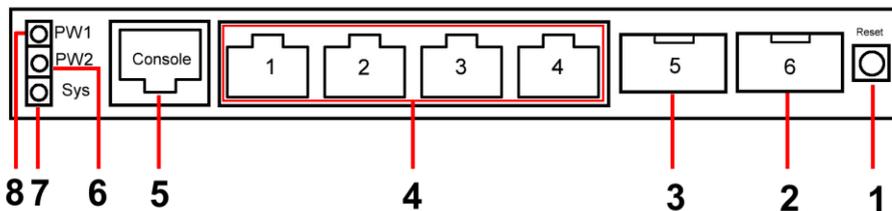


Рис.3 Уличный коммутатор SW-80402/WLU, разъемы, кнопки и индикаторы

Таб. 1 Уличный коммутатор SW-80402/WLU, назначение внутренних элементов

| № п/п | Назначение |
|-------|---|
| 1 | Кнопка для сброса настроек уличного коммутатора к заводским. Необходимо продолжительное нажатие ~3 сек при включенном питании. |
| 2 | SFP-слот (№1) для подключения уличного коммутатора к оптической линии связи на скорости 1000 Мбит/с используя SFP-модули 1,25 Гбит/с (приобретаются отдельно). |
| 3 | SFP-слот (№2) для подключения уличного коммутатора к оптической линии связи на скорости 1000 Мбит/с используя SFP-модули 1,25 Гбит/с (приобретаются отдельно). |
| 4 | Разъемы RJ-45 с 1 по 4й для подключения сетевых устройств на скорости 10/100/1000 Мбит/с и запитывания их по технологии PoE. LED-индикаторы Ethernet и PoE <u>Горит желтым</u> – подключено PoE устройство. <u>Мигает</u> – потребление PoE слишком высоко. <u>Горит/Мигает зеленым</u> – идет передача данных. |
| 5 | Разъем RJ-45 для подключения уличного коммутатора к COM порту. Позволяет загружать в уличный коммутатор прошивку в случае аварийной ситуации |
| 6 | LED-индикатор подключения резервного БП (не используется) |
| 7 | LED индикатор работы коммутатора. <u>Мигает</u> – работа в штатном режиме; <u>Горит</u> – аварийная ситуация (зависание коммутатора); <u>Быстро мигает</u> – идет загрузка прошивки. |

| № | Назначение |
|---|---|
| 8 | LED-индикатор подключения основного БП <u>Горит зеленым</u> – питание подается. <u>Не горит</u> – питание на входе отсутствует. |

5. Установка и подключение

Внимание !

- ✓ Категорически запрещается касаться элементов блока питания, находящихся под высоким напряжением.
- ✓ Качественное заземление является обязательным условием подключения.
- ✓ Хранение и транспортировка уличных коммутаторов с резервной системой питания производится с демонтированной плавкой вставкой – предохранителем для ограничения разряда системы АКБ. Запрещается подключать глубоко разряженные АКБ.
- ✓ Для исключения ложных срабатываний автоматов защиты необходимо выбирать автоматы «С» с током срабатывания >4А.
- ✓ Неиспользуемые гермовводы следует закрыть заглушками. В противном случае, система обогрева может работать в неправильном режиме, также возможно образование конденсата. Это может привести к выходу уличного коммутатора из строя!

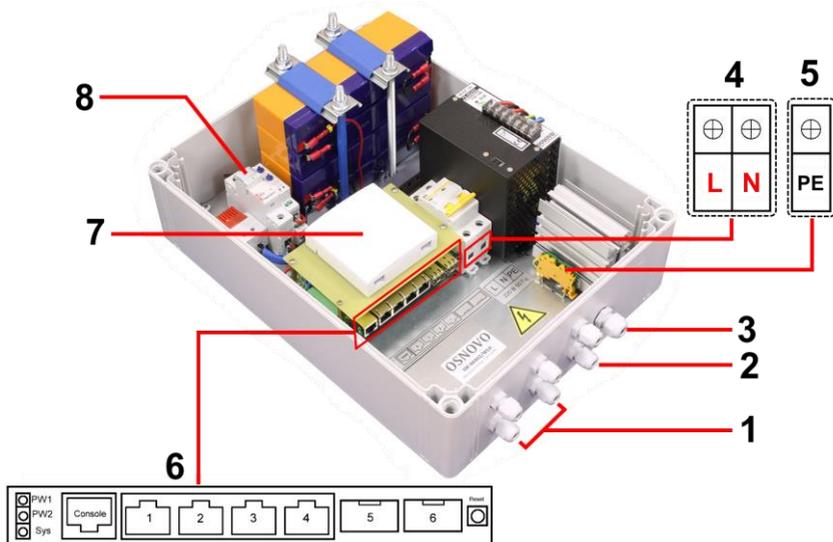


Рис. 4 Подключение уличного коммутатора SW-80402/WLU

Подключение уличного коммутатора SW-80402/WLU осуществляются в следующей последовательности:

1. Проденьте кабели витой пары через соответствующие отверстия гермовводов (1) снаружи внутрь бокса (рис.4).
2. Обожмите концы кабелей с внутренней стороны бокса разъемами RJ45 (рис. 5)

| | RJ45 Pin# |
|---|-------------------|
|  | Бело-оранжевый 1 |
|  | оранжевый 2 |
|  | Бело-зеленый 3 |
|  | синий 4 |
|  | Бело-синий 5 |
|  | зеленый 6 |
|  | Бело-коричневый 7 |
|  | коричневый 8 |

Рис. 5 Обжимка кабеля витой пары разъемами RJ-45

3. Подключите обжатые разъемами RJ-45 кабели к коммутатору (6) и затяните гермовводы (1). Для обеспечения защиты от проникновения влаги внутрь корпуса, кабели должны быть плотно укреплены в гермовводах.
4. Аналогично пункту 1 протяните кабель питания от сети AC 100-240V / 50 Гц внутрь корпуса через соответствующий гермоввод (3) (Ø 4-8мм), подключите кабель питания к контактам **L (фаза)** и **N (ноль)** (4) и **PE** (5). Затяните гермоввод.
5. Зачистите оптоволоконные кабели на длину 25-30 см, пропустите их в отверстия гермовводов (2), затяните резьбу гермовводов так, чтобы кабель жестко фиксировался в зажиме гермовводов.
6. Соблюдая все требования технологии сварки оптоволоконного кабеля, приварите пигтейлы (имеется в комплекте) к оптоволоконным жилам кабеля. Уложите оптоволоконный кабель в пазы оптического кросса (7), следя за тем, чтобы диаметр кольца не был менее 60 мм. Подключите разъемы пигтейлов к SFP модулям (не входят в комплект поставки) установленным предварительно в SFP разъемы коммутатора (6). Закройте крышку оптического кросса (7).

8. Вставьте плавкую вставку - предохранитель в держатель (8) и его утапливанием подключите источник резервного питания в цепь питания уличного коммутатора. Включите автоматический выключатель. Аккуратно закройте крышку, затяните ее 4-мя винтами из комплекта поставки. Уличный коммутатор готов к эксплуатации.

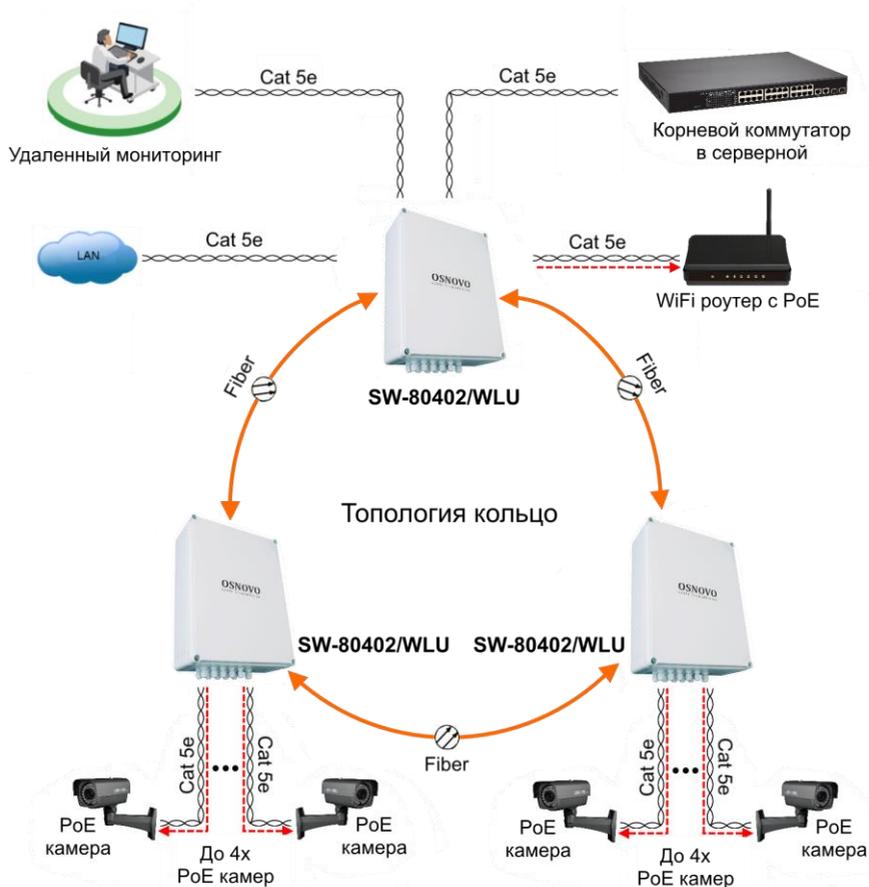


Рис.6 Схема подключения уличного коммутатора SW-80402/WLU в топологии «кольцо»

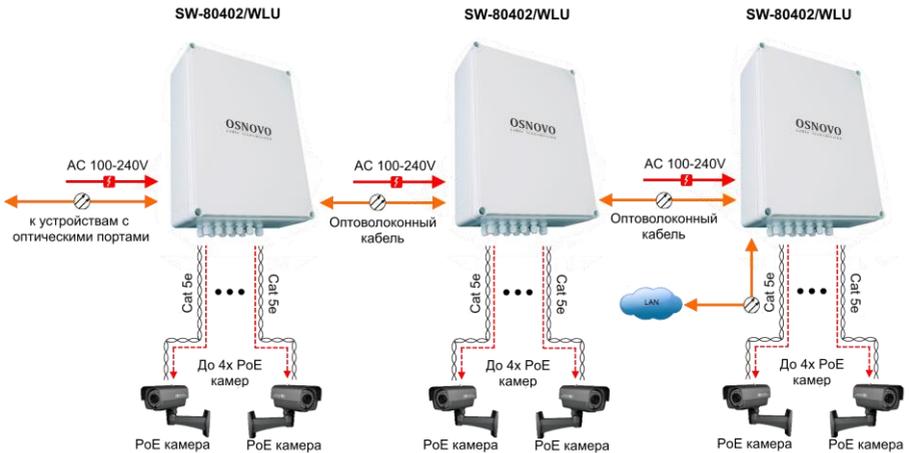


Рис. 7 Типовая схема подключения уличного коммутатора SW-80402/WLU

6. Проверка работоспособности системы

После подключения кабелей к разъёмам и подачи питания можно убедиться в работоспособности уличного коммутатора.

Подключите уличный коммутатор между двумя ПК с известными IP-адресами, располагающимися в одной подсети, например, 192.168.1.1 и 192.168.1.2. (см. также п.8.4 настоящего документа).

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. 8). Это свидетельствует об исправности уличного коммутатора.

```

C:\WINNT\System32\command.com
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<10ms TTL=255
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>

```

Рис. 8 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:

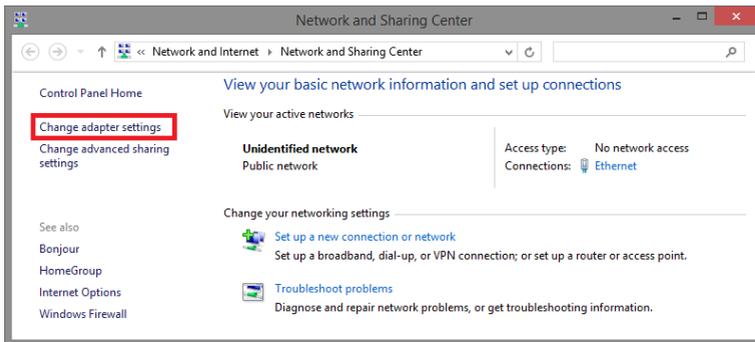
Причины потери в оптической линии могут быть вызваны:

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

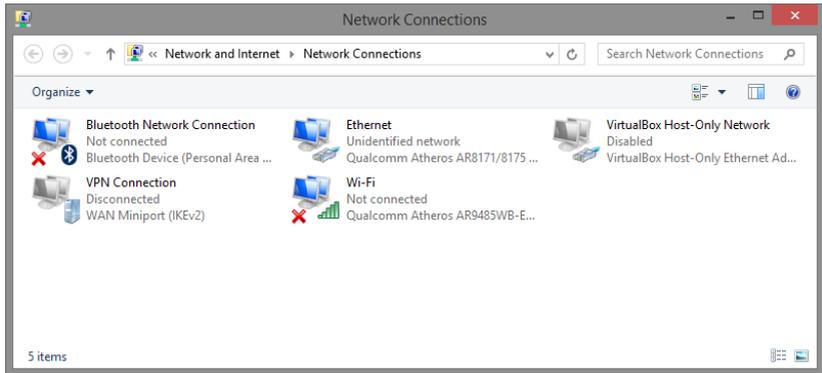
7. Подготовка перед управлением коммутатором через WEB.

Здесь будет показана детальная настройка сети для ПК под управлением Windows 8 (похожий интерфейс у Windows7 и Windows Vista).

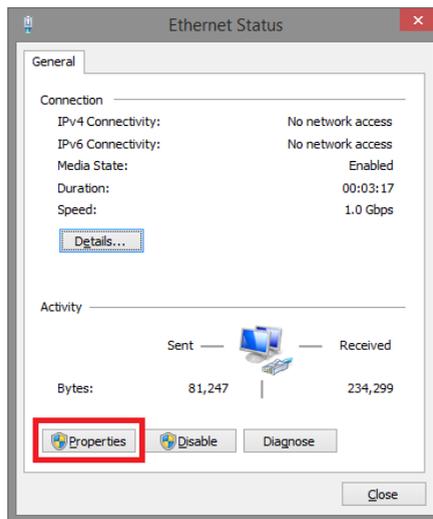
1. Откройте «Центр управления сетями и общим доступом» (Network and Sharing in Control Panel) и нажмите «Изменение параметров адаптера» (Change adapter setting) как на рисунке ниже.



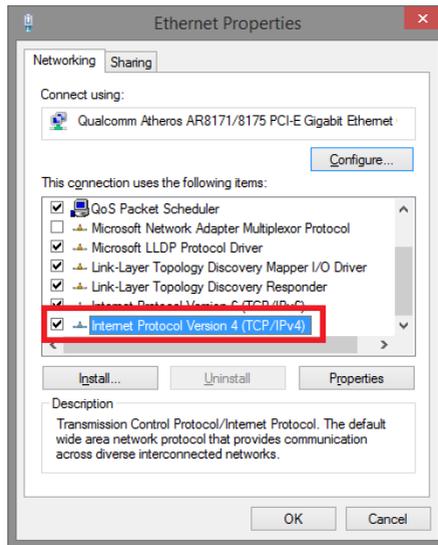
2. В появившемся окне «Сетевые подключения» (Network Connections) отображены все сетевые подключения, доступные вашему ПК. Сделайте двойной клик на подключении, которое вы используете для сети Ethernet



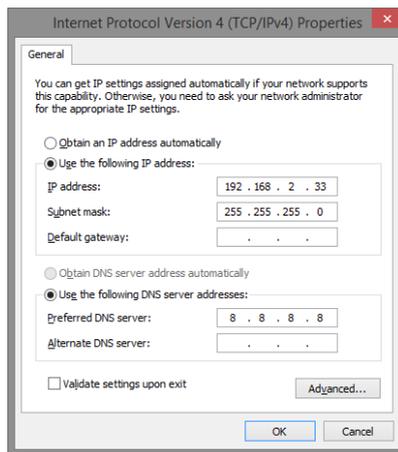
3. В появившемся окне «Состояние - Подключение по локальной сети» (Ethernet Status) нажмите кнопку «Свойства» (Properties) как показано ниже.



4. В появившемся окне «Подключение по локальной сети – Свойства» сделайте двойной клик на «протокол интернета версии IP V4 (TCP/IPv4)» как показано ниже
- 5.



6. В появившемся окне «Протокол интернета версии IP V4 (TCP/IPv4)» сконфигурируйте IP адрес вашего ПК и маску подсети как показано ниже



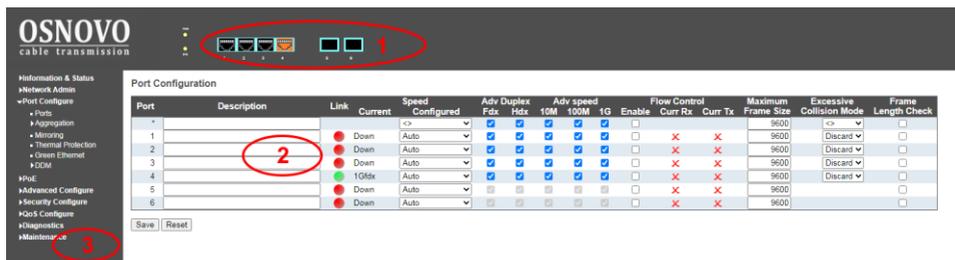
По умолчанию IP адрес коммутатора **192.168.2.1** Вы можете задать любой IP адрес в поле «IP адрес», в той же подсети что и IP адрес коммутатора. Нажмите кнопку ОК, чтобы сохранить и применить настройки.

Теперь вы можете использовать любой браузер для входа в меню настроек коммутатора. Login: **Admin** Password: **System**

8. Управление через WEB интерфейс.

8.1 Основные сведения

WEB интерфейс коммутатора представлен на рисунке ниже:



Визуально WEB интерфейс состоит из 3 частей:

| | |
|----------------------|---|
| Часть 1* (Part 1) | Индикаторы портов, включая PoE статус и статус соединения. Выбор языка. Документ справки. |
| Часть 2 (Part 2) | Основной интерфейс, где доступны настройки и отображается статистика по тем или иным параметрам. |
| Часть 3 (Part 3) | Главное меню WEB интерфейса. Содержит перечень доступных настроек, режимов, инструментов для мониторинга сети, а также инструментов для обслуживания коммутатора. |

* WEB интерфейс отображает схему всех портов коммутатора. Различные цвета на схеме означают, что порт/порты находятся в том или ином состоянии.



Скорость порта 100Мбит/с



Скорость порта 1000 Мбит/с



Нет соединения

8.2 Главное меню WEB интерфейса

С помощью встроенного в коммутатор WEB интерфейса Вы можете гибко настраивать системные параметры, скорость портов, отслеживать состояние сети и многое другое.

Все инструменты и настройки собраны в группы и подгруппы. Основных групп 9:

Information&Status (Общая информация и статус) – пользователи могут проверить общую информацию о коммутаторе, статус, как долго коммутатор находится включенным и тд.

Network Admin (Настройка сетевых параметров и администрирование) – пользователи могут проверить и настроить параметры, относящиеся к сети в данном пункте главного меню WEB интерфейса коммутатора.

Port Configure (Конфигурирование портов коммутатора) – пользователи могут проверить и настроить определенные параметры портов в данном пункте главного меню WEB интерфейса коммутатора.

PoE – пользователи могут проверить и настроить определенные параметры PoE для портов в данном пункте главного меню WEB интерфейса коммутатора.

Advanced Configure (Расширенные настройки) – пользователи могут проверить и настроить L2 и L2+ функции коммутатора в данном пункте главного меню WEB интерфейса.

Security Configure (Настройки безопасности) – пользователи могут проверить и настроить параметры безопасности для коммутатора в данном пункте главного меню WEB интерфейса.

QoS (Управление очередями) – пользователи могут проверить и настроить параметры режима управления очередями QoS в данном пункте главного меню WEB интерфейса.

Diagnostics (Инструменты для диагностики) – пользователи могут воспользоваться инструментами для диагностики сети (Ping), диагностики

кабеля, а также проверить загрузку CPU коммутатора в данном пункте главного меню WEB интерфейса.

Maintenance (Обслуживание) – пользователи могут воспользоваться инструментами обслуживания коммутатора (сброс к заводским настройкам, обновление прошивки, загрузка и сохранение текущей конфигурации, перезагрузка коммутатора) в данном пункте главного меню WEB интерфейса.

8.3 Network Admin (Настройка сетевых параметров и администрирование)

8.3.1 IP Configuration (Настройка IP адреса)

Примечание: IP адрес коммутатора по умолчанию 192.168.2.1 Маска подсети по умолчанию 255.255.255.0(24)

Выберите подраздел главного меню WEB интерфейса коммутатора: *Network Admin > IP*

| | |
|-----------|---|
| Port Name | Отображает системное имя порта |
| VLAN | VLAN для доступа к управлению коммутатором |
| IPv4 DHCP | <ul style="list-style-type: none"> - Если включено, это означает, что порт VLAN запускает IPv4 DHCP клиент, чтобы динамически получать IPv4 адреса коммутатора. В противном случае он будет использовать статический IP адрес. - Откат (в секундах) означает время ожидания для коммутатора для получения динамического IP адреса с помощью DHCP. Значение 0 – отменяет время ожидания. - Текущая аренда, поле отображает текущий IP адрес, полученный от DHCP |

| | |
|------|--|
| IPv4 | <ul style="list-style-type: none"> - Адрес: статический IP адрес, введенный пользователем. - Длина маски: статическая IPv4 маска для подсети, введенная пользователем. |
|------|--|

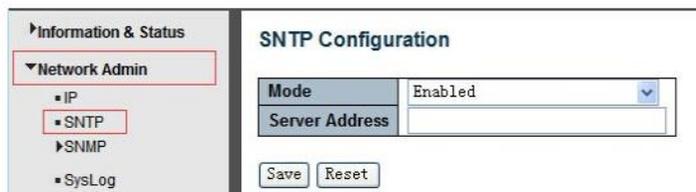
Нажмите Add Interface, чтобы задать новые настройки для VLAN и IP адреса. Нажмите Save, чтобы сохранить настройки.

Примечание: Для управления коммутатором используется VLAN1 по умолчанию. Если пользователю необходима другая VLAN, для управления коммутатором, пожалуйста добавьте VLAN в соответствующем меню WEB интерфейса, а также добавьте порт в эту VLAN.

8.3.2 SNTP Configuration (Настройка протокола времени SNTP)

SNTP это акроним от Simple Network Time Protocol – протокол синхронизации часов с настройками ПК. Вы можете выбрать определенный SNTP сервер и настроить GMT временную зону.

Выберите подраздел главного меню WEB интерфейса коммутатора:
Network Admin > SNTP



| | |
|-------------|--|
| Mode | <p>Нажмите на выпадающее меню, чтобы выбрать Enabled или Disabled</p> <p>Enabled (вкл) – включает режим SNTP. В данном режиме агент отправляет и принимает SNTP сообщения между клиентами и сервером, когда они находятся не в одной подсети.</p> <p>Disabled (выкл) – отключает режим SNTP.</p> |
| SNTP Server | <p>После ввода IP адреса SNTP сервера, SNTP информация будет получена с этого сервера.</p> |

Нажмите Save, чтобы сохранить настройки.

8.3.3 SNMP Configuration (Настройка протокола управления SNMP)

Simple Network Management Protocol (SNMP) это протокол прикладного уровня, который облегчает обмен информацией управления между сетевыми устройствами. SNMP позволяет сетевым администраторам управлять производительностью сети, находить и решать проблемы с сетью, планировать расширение сети.

Коммутатор поддерживает SNMPv1, v2c. Различные версии SNMP обеспечивают разный уровень безопасности для управления станциями и сетевыми устройствами.

В SNMP v1 и v2c для аутентификации пользователей используется «Community String». Функционал этой строки схож с функционалом пароля. Приложение SNMP удаленного пользователя и SNMP коммутатора должны использовать одно и тоже значение Community String. Пакеты SNMP от любых неавторизованных сайтов будут игнорироваться (отбрасываться).

Community String по умолчанию для коммутатора имеет значение:

1. public – позволяет аутентификацию станции управления для чтения MIB объектов.
2. private – позволяет аутентификацию станции управления для чтения, записи и изменения MIB объектов.

Trap

Используется агентом для асинхронного информирования NMS (станция управления) о каком-либо событии. Эти события могут быть очень серьезными, такими, как перезагрузка (кто-то случайно выключил коммутатор), или просто, общая информация, такая как изменение статуса порта. Коммутатор создает информацию о ловушке (Trap), а затем отправляет ее получателю или администратору сети. Типичная ловушка включает в себя информацию о ошибках аутентификации, сетевых изменениях.

MIB

Это коллекция управляемых объектов, находящихся в виртуальном хранилище информации. Коллекции связанных управляемых объектов определены в определенных модулях MIB. Коммутатор использует стандартный модуль управления информацией MIB-II. Таким образом, значение объекта MIB может быть прочитано любым программным обеспечением, управляемым через SNMP протокол.

8.3.3.1 SNMP System Configuration (Настройка SNMP для системы)

Вы можете включить или выключить данную функцию в разделе

Admin>SNMP>System

| SNMP System Configuration | |
|---------------------------|----------|
| Mode | Enabled |
| Version | SNMP v2c |
| Read Community | public |
| Write Community | private |

Save Reset

| | |
|-----------------|---|
| Mode | Включение/выключение SNMP функции |
| Version | Нажмите на выпадающее меню, чтобы выбрать версию протокола SNMP v2c или v1 |
| Read Community | Позволяет аутентификацию станции управления для чтения MIB объектов. |
| Write Community | Позволяет аутентификацию станции управления для чтения, записи и изменения MIB объектов |

8.3.3.2 SNMP Trap Configuration (Настройка SNMP Trap)

Вы можете включить или выключить данную функцию и настроить ее в следующем разделе

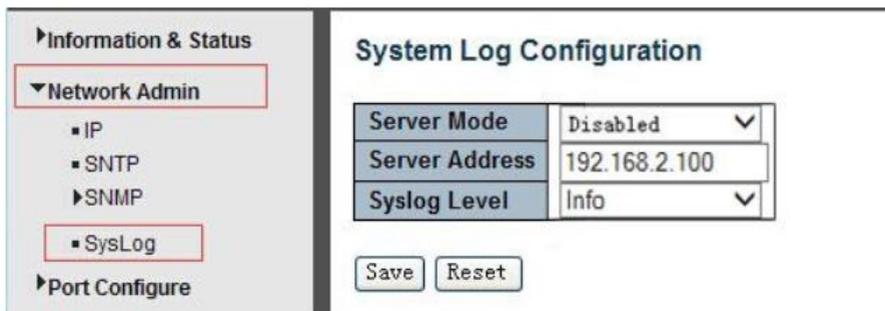
Network Admin>SNMP>Trap



8.3.4 System Log Configuration (Настройка системного журнала)

Вы можете настроить системный журнал коммутатора перейдя в нужный раздел основного меню WEB интерфейса

Network Admin > Syslog



| | |
|----------------|--|
| Server Mode | Вкл/выкл функцию системного журнала для SNMP . Если включено, коммутатор отправляет копию журнала на сторонний сервер |
| Server Address | Сервер, на который отправляется копия системного журнала |
| Syslog Level | Info – информация, предупреждения и ошибки Warning – только предупреждения и ошибки Errors – только ошибки |

8.4 Port Configure (Конфигурирование портов)

8.4.1 Port Configuration (Настройка портов)

Данный раздел WEB интерфейса содержит перечень настроек для портов коммутатора.

Port Configure>Ports

| Port | Link | Speed | | Flow Control | | | Maximum Frame Size | Excessive Collision Mode |
|------|--------|---------|------------|--------------|------------|--------------------------|--------------------|--------------------------|
| | | Current | Configured | Current Rx | Current Tx | Configured | | |
| * | | ◁ | ▼ | | | <input type="checkbox"/> | 9600 | ◁ |
| 1 | Down | Auto | ▼ | × | × | <input type="checkbox"/> | 9600 | Discard ▼ |
| 2 | 100fdx | Auto | ▼ | × | × | <input type="checkbox"/> | 9600 | Discard ▼ |
| 3 | Down | Auto | ▼ | × | × | <input type="checkbox"/> | 9600 | Discard ▼ |

| | |
|--------------------|---|
| Link | Красный цвет означает, что соединения нет. Зеленый – соединение есть. |
| Speed | Выбор скорости и режима работы (дуплекс/полудуплекс) для порта Disabled – порт отключен. Auto – позволяет порту автоматически выбирать наиболее подходящие параметры для подключенного устройства. FDX – дуплекс. По умолчанию для скорости 1000Мбит/с HDX – полудуплекс 1000-X_AMS – означает, что порт является оптическим или комбо-портом и оптический порт – основной. Также есть другие аналогичные параметры: 10M HDX, 10M FDX, 100M HDX, 100M FDX, 1000M FDX, 1000-X |
| Flow Control | Механизм управления потоком. Полнодуплексные порты используют 802.3x протокол для управления потоком, полудуплексные порты используют backpressure управление потоком. По умолчанию данный механизм для портов – отключен. |
| Maximum Frame Size | Поле, где задается максимальный размер передаваемых/принимаемых пакетов. По умолчанию размер – 9600, чтобы обеспечить поддержку Jumbo frames. |

Нажмите Save, чтобы сохранить настройки.

8.4.2 Link aggregation (Агрегация каналов)

Агрегация каналов, это метод, который связывает определенные физические порты вместе, как один логический порт, чтобы увеличить общую пропускную способность.

Коммутатор поддерживает до 13 групп агрегации каналов. От 2 до 8 портов в виде единого логического порта.

Примечание: Если какой-либо порт в группе агрегации каналов отключен, пакет данных, отправленный на отключенный порт будет распределять нагрузку на другой подключенный порт в этой группе агрегации.

8.4.2.1 Static Aggregation (Статическая Агрегация)

В этом разделе WEB интерфейса коммутатора пользователь может настроить статическую агрегацию для портов.

Port Configure > Aggregation > Static

Aggregation Mode Configuration

Hash Code Contributors

| | |
|-------------------------|-------------------------------------|
| Source MAC Address | <input checked="" type="checkbox"/> |
| Destination MAC Address | <input checked="" type="checkbox"/> |
| IP Address | <input checked="" type="checkbox"/> |
| TCP/UDP Port Number | <input checked="" type="checkbox"/> |

Aggregation Group Configuration

| Group ID | Port Members | | | | | | | | | | | | | | | | | | | | | | | | | | |
|----------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | |
| Normal | <input checked="" type="checkbox"/> |
| 1 | <input type="checkbox"/> |
| 2 | <input type="checkbox"/> |
| 3 | <input type="checkbox"/> |
| 4 | <input type="checkbox"/> |
| 5 | <input type="checkbox"/> |
| 6 | <input type="checkbox"/> |
| 7 | <input type="checkbox"/> |
| 8 | <input type="checkbox"/> |
| 9 | <input type="checkbox"/> |
| 10 | <input type="checkbox"/> |
| 11 | <input type="checkbox"/> |
| 12 | <input type="checkbox"/> |
| 13 | <input type="checkbox"/> |

Save Reset

| | |
|--------------------------------|---|
| Aggregation Mode Configuration | Этот режим является алгоритмом хеширования потока между портами LAG (группа агрегированных портов или Link Aggregation Group) |
| Group ID | ID группы статической агрегации |
| Port Members | Коммутатор поддерживает до 13 групп агрегации, от 2 до 8 портов в одной группе. |

Нажмите Save, чтобы сохранить настройки.

Примечание: Статическая агрегация позволяет одновременно объединять не более 8 портов в одну статическую группу.

8.4.2.2 LACP Aggregation (Агрегация на основе LACP)

LACP – Протокол управления агрегацией каналов. Агрегация каналов позволяет объединять до восьми портов в одно выделенное соединение (логический порт).

Эта функция может расширить пропускную способность устройства. Работа LACP требует включения дуплексного режима на портах.

Для получения более подробной информации ознакомьтесь со стандартом IEEE 802.3ad.

Port Configure > Aggregation > LACP

| Port | LACP Enabled | Key | Role | Timeout | Prio |
|------|--------------------------|------|--------|---------|-------|
| * | <input type="checkbox"/> | <> | <> | <> | 32768 |
| 1 | <input type="checkbox"/> | Auto | Active | Fast | 32768 |
| 2 | <input type="checkbox"/> | Auto | Active | Fast | 32768 |
| 3 | <input type="checkbox"/> | Auto | Active | Fast | 32768 |
| 4 | <input type="checkbox"/> | Auto | Active | Fast | 32768 |
| 5 | <input type="checkbox"/> | Auto | Active | Fast | 32768 |

| | |
|---------|--|
| LACP | Включение/выключение поддержки протокола LACP на порте |
| Key | <p>Значение ключа, полученное портом, находится в диапазоне 1-65535.</p> <p>Auto настройка задаст ключ в зависимости от скорости физического канала, 10Mb = 1, 100Mb = 2, 1Gb = 3.</p> <p>Specific настройка позволяет вводить значение ключа вручную. Порты с одинаковым значением ключа могут быть участниками одной группы агрегации, а порты с разными ключами – не могут.</p> |
| Role | <p>Данное поле отвечает за состояние активности LACP.</p> <p>Active – передача пакетов LACP каждую секунду</p> <p>Passive – ожидание пакетов LACP.</p> |
| Timeout | <p>Данное поле отвечает за промежуток времени между передачей BPDU</p> <p>Fast – отправка пакетов LACP каждую секунду</p> <p>Slow – 30 сек ожидания перед отправкой пакета LACP</p> |
| Prio | <p>Данное поле контролирует приоритет порта.</p> <p>Если партнер LACP хочет сформировать большую группу, чем устройство поддерживает, то параметр Prio будет контролировать, какие порты будут в активной роли, а какие в резервной роли.</p> <p>Меньшее значение параметра Prio означает больший приоритет.</p> |

Нажмите Save, чтобы сохранить настройки.

8.4.3 Port Mirroring (Зеркалирование портов)

Функция зеркалирования портов обеспечивает мониторинг сетевого трафика, копия которого (входящие или исходящие пакеты) пересылается с одного порта сетевого коммутатора на другой порт, где трафик может быть исследован.

Это позволяет администратору сети отслеживать производительность коммутатора и при необходимости изменять его настройки.

Port Configure > Mirroring



| | |
|----------------|--|
| Port mirror to | Пакеты с портов, для которых включено зеркалирование rx или tx будут доступны на этом порте. Disabled – отключает зеркалирование |
| Mode | Выбор режима зеркалирования для порта источника. Rx only – пакеты, полученные на этом порте будут отправлены за порт-зеркало (mirror port). Исходящие пакеты зеркалироваться не будут. Tx only – пакеты, исходящие с этого порта будут отправлены за порт-зеркало (mirror port). Получаемые пакеты зеркалироваться не будут. Disabled – все пакеты (tx и rx) не будут зеркалироваться Enabled – все пакеты (tx и rx) будут отправлены на порт-зеркало. |

Нажмите Save, чтобы сохранить настройки.

8.4.4. Thermal Protection Configuration (Температурная защита)

Температурная защита предотвращает перегрев портов. Когда коммутатор определяет порт, на котором температура выше заданной, происходит отключение порта.

Port Configuration > Thermal Protection

Thermal Protection Configuration

Temperature settings for priority groups

| Priority | Temperature |
|----------|-------------|
| 0 | 255 °C |
| 1 | 255 °C |
| 2 | 255 °C |
| 3 | 255 °C |

Port priorities

| Port | Priority |
|------|----------|
| * | ⏵ |
| 1 | 0 |
| 2 | 0 |
| 3 | 0 |

| | |
|--|--|
| Temperature settings for priority groups | Коммутатор поддерживает 4 группы температурной защиты. Каждая может быть настроена на свою максимальную температуру. |
| Port priorities | Поле определяет принадлежность порта к той или иной группе температурной защиты. |

Нажмите Save, чтобы сохранить настройки.

Примечание: по умолчанию все порты коммутатора находят в группе приоритета 0, с максимальной температурой 255 C

8.5 PoE Configuration (Конфигурация PoE)

Power Over Ethernet (PoE) – функция, позволяющая устройствам получать питание и данные по одному кабелю в сети Ethernet.

Таковыми устройствами могут быть PoE IP камеры, точки доступа, телефоны VoIP. Наличие данной функции позволяет снизить затраты на создание сетевой инфраструктуры.

PoE – определяется стандартом IEEE 802.3af/at. Поэтому обычно не возникает сложностей с питанием удаленного устройства, если оно поддерживает/совместимо с данными стандартами.

PD – запрашиваемое устройство, например PoE IP камера.

PSE – устройство обеспечивающее питание удаленного PD

Процесс подачи питания PoE состоит из нескольких шагов:

- 1) Определение. PSE устройство отправляет сигнал с минимальным напряжением, чтобы определить совместимо ли удаленное PD устройство со стандартами IEEE 802.3af/at. Если удаленное устройство совместимо происходит следующий шаг.
- 2) Классификация PD устройства. PSE устройство определяет необходимую мощность для удаленного PD устройства.
- 3) После первых двух шагов PSE устройство начинает подавать в линию полное напряжение и мощность (44-57V, мощность af – 15.4Вт макс, at – 25.5Вт макс.)
- 4) Отключение. Если удаленное PD устройство отключилось, или пользователь отключил его с помощью управления через WEB, PSE устройство в течение 300-400 мс прекращает подачу напряжения PoE в линию.

8.5.1 PoE Setting (Настройки PoE)

Настройки PoE находятся в следующем разделе WEB интерфейса коммутатора.

PoE > PoE Setting

Power Over Ethernet Configuration

Reserved Power determined by Auto Manual

Power Management Mode Actual Consumption Reserved Power

Capacitor Detection Disabled Enabled

PoE Power Supply Configuration

Primary Power Supply [W]

PoE Port Configuration

| Port | PoE Mode | Priority | PD Alive Check | Maximum Power [W] | Description |
|------|----------|----------|----------------|-------------------|-------------|
| * | <> | <> | <> | 15.4 | |
| 1 | PoE+ | Low | ON | 15.4 | |
| 2 | PoE+ | Low | ON | 15.4 | |
| 3 | PoE+ | Low | ON | 15.4 | |
| 4 | PoE+ | Low | ON | 15.4 | |
| 5 | PoE+ | Low | ON | 15.4 | |
| 6 | PoE+ | Low | ON | 15.4 | |
| 7 | PoE+ | Low | ON | 15.4 | |
| 8 | PoE+ | Low | ON | 15.4 | |

Save Reset

| | |
|------------------------------|--|
| Reserved Power determined by | <p>Коммутатор поддерживает 2 режима для определения мощности на порте</p> <p>Auto – коммутатор автоматически определяет мощность на порте в зависимости от класса подключенного PoE устройства.</p> <p>Manual – вручную – максимальная доступная на порте мощность задается пользователем.</p> |
| Power Management Mode | <p>Коммутатор поддерживает 2 режима управления питанием.</p> <p>1. Реальное потребление. В этом режиме общая мощность (PoE бюджет) делится на все порты. Порт с наименьшим приоритетом будет выключен, если мощность превысит бюджет PoE. Если все порты имеют одинаковое значение приоритета – будет отключен порт с крайним номером.</p> <p>2. Зарезервированная мощность. В этом режиме, если мощность превысит PoE бюджет коммутатора, порт к которому будет подключено новое PoE устройство не будет активен.</p> |

| | |
|----------------------|---|
| Primary Power Supply | Пользователи могут настраивать PoE бюджет всего коммутатора (не более значения по умолчанию). Значение по умолчанию 370 W |
| PoE Mode | Режим PoE на портах. По умолчанию – 802.3at (PoE+) |
| Priority | Значение определяющее приоритет порта. Может принимать 3 значения Low – низкий приоритет High – высокий приоритет Critical – критически важный приоритет |
| Maximum Power (W) | В ручном режиме выставляется значение максимальной доступной мощности на порте. |

Нажмите Save, чтобы сохранить настройки.

8.5.2 PD Alive (Функция антизависания для PoE устройств)

Настройки данной функции находятся в следующем разделе WEB интерфейса коммутатора:

PoE > PoE Setting

Power Over Ethernet Configuration

| | | |
|-------------------------------------|---|--------------------------------------|
| Reserved Power determined by | <input checked="" type="radio"/> Auto | <input type="radio"/> Manual |
| Power Management Mode | <input checked="" type="radio"/> Actual Consumption | <input type="radio"/> Reserved Power |
| Capacitor Detection | <input checked="" type="radio"/> Disabled | <input type="radio"/> Enabled |

PoE Power Supply Configuration

Primary Power Supply [W]

250

PoE Port Configuration

| Port | PoE Mode | Priority | PD Alive Check | Maximum Power [W] | Description |
|------|----------|----------|----------------|-------------------|-------------|
| * | <> | <> | <> | 15.4 | |
| 1 | PoE+ | Low | ON | 15.4 | |
| 2 | PoE+ | Low | ON | 15.4 | |
| 3 | PoE+ | Low | ON | 15.4 | |
| 4 | PoE+ | Low | ON | 15.4 | |

Функция работает полностью в автоматическом режиме после ее активации на порте/портах. Срабатывание происходит через 120 сек после того, как коммутатором было зафиксировано состояние «зависания» на порте/портах. Сработка происходит 1 раз.

8.5.3 PoE Status (Состояние PoE на портах)

Позволяет отслеживать состояние PoE на всех портах. Находится в разделе

PoE > PoE Status

| Local Port | Description | PD class | Power Requested | Power Allocated | Power Used | Current Used | Priority | Port Status |
|------------|-------------|----------|-----------------|-----------------|------------|--------------|----------|-------------------------------|
| 1 | - | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | PoE turned OFF - PoE disabled |
| 2 | - | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | PoE turned OFF - PoE disabled |
| 3 | - | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | PoE turned OFF - PoE disabled |
| 4 | - | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | PoE turned OFF - PoE disabled |
| 5 | - | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | PoE turned OFF - PoE disabled |
| 6 | - | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | PoE turned OFF - PoE disabled |
| 7 | - | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | PoE turned OFF - PoE disabled |
| 8 | - | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | PoE turned OFF - PoE disabled |
| 9 | - | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | PoE turned OFF - PoE disabled |
| 10 | - | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | PoE turned OFF - PoE disabled |
| 11 | - | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | PoE turned OFF - PoE disabled |

8.6 Advanced Configure (Расширенные настройки)

8.6.1 VLAN (Настройка VLAN)

VLAN – виртуальная локальная сеть – представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения.

VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным членам группироваться вместе, даже если они не находятся в одной физической сети.

Настройки находятся в разделе

Advanced Configure > VLANs

Information & Status

Network Admin

Port Configure

PoE

Advanced Configure

- MAC Table
- VLANs
- Port Isolation
- Loop Protection
- Spanning Tree
- MEP
- ERPS
- IGMP Snooping
- LLDP

Global VLAN Configuration

Allowed Access VLANs: 1

Ethertype for Custom S-ports: 88A8

Port VLAN Configuration

| Port | Mode | Port VLAN | Port Type | Ingress Filtering | Ingress Acceptance | Egress Tagging | Allowed VLANs | Forbidden VLANs |
|------|--------|-----------|-----------|-------------------------------------|---------------------|-----------------|---------------|-----------------|
| * | <> | 1 | <> | <input checked="" type="checkbox"/> | <> | <> | 1 | |
| 1 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag Port VLAN | 1 | |
| 2 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag Port VLAN | 1 | |
| 3 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag Port VLAN | 1 | |
| 4 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag Port VLAN | 1 | |
| 5 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag Port VLAN | 1 | |

| | |
|------------------------------|--|
| Allowed VLANs | В этом поле отображаются созданные VLAN ID. По умолчанию значение – 1. Если вы хотите создать новую VLAN, измените значение на новое. |
| Ethertype for Custom S-ports | В этом поле указывается значение ethertype / TPID (в шестнадцатеричном формате). Параметр действует для всех портов, тип которых (Port Type) установлен как S-Custom-Port |
| Mode | <p>Режим порта (по умолчанию Access) определяет основное поведение порта.</p> <p>Порт может находиться в одном из трех режимов, как описано ниже. Всякий раз, когда выбран определенный режим, остальные поля в этой строке будут либо недоступны или сделаны изменяемыми в зависимости от рассматриваемого режима. Затененные поля показывают значение, которое порт получит при применении режима.</p> <p><u>Access</u>. Порты с этим режимом обычно используют для подключения к конечным станциям. Имеют следующие характеристики:</p> <ul style="list-style-type: none"> - Порт участник Access VLAN (по умолчанию 1) - Порт принимает пакеты типа untagged и C-tagged - Отбрасывает все пакеты, которые не классифицированы для доступа к Access VLAN - На выходе все пакеты, относящиеся к Access VLAN будут передаваться, как untagged. Другие (динамически добавленные VLANы) будут передаваться, как tagged. |

| | |
|-----------|--|
| | <p><u>Trunk</u>. Trunk (магистральные) порты могут одновременно передавать трафик по нескольким сетям VLAN и обычно используются для подключения к другим коммутаторам. Имеют следующие характеристики:</p> <ul style="list-style-type: none"> - По умолчанию, trunk порт является участником всех VLAN (1-4094) - VLANы, участником которых является trunk порт, могут быть ограничены через поле Allowed VLANs - Пакеты, относящиеся к VLAN, участником которой порт не является – отбрасываются. - По умолчанию все пакеты, кроме пакетов относящихся к Port VLAN (Native VLAN) будут помечены (tagged) на выходе. - Маркирование пакетов на выходе (тегирование) может быть изменено, чтобы пометить все пакеты. В таком случае, только tagged пакеты будут приниматься на входе. <p><u>Hybrid</u>. Такие порты во многом напоминают trunk порты, но имеют дополнительные настройки.</p> <ul style="list-style-type: none"> – Порт может быть настроен так, чтобы VLAN tag не распознавался, C-tag и S-tag поддерживались. - Фильтрация на входе могла контролироваться. - Прием пакетов на входе и настройка исходящего тегирования могут настраиваться независимо. |
| Port VLAN | <p>Поле определяет идентификатор VLAN порта (PVID). Разрешенные VLAN находятся в диапазоне от 1 до 4094, по умолчанию 1</p> |

| | |
|--------------------|---|
| Port Type | <p>Порты в гибридном режиме позволяют изменять тип порта.</p> <p><u>Unaware</u>. На входе все пакеты, независимо от того помечены ли они VLAN tag или нет, будут отнесены к VLAN Port, возможные метки (теги) будут удалены на выходе.</p> <p><u>C-port</u>. На входе пакеты с тегом VLAN с TPID = 0x8100 будут классифицированы по VLAN ID, содержащемуся в метке. Если пакет помечен, как приоритетный, он будет классифицирован Port VLAN. Если пакеты должны быть помечены на выходе, они будут помечаться C-tag меткой.</p> <p><u>S-port</u>. На входе пакеты с тегом VLAN с TPID = 0x8100 или 0x88A8 будут классифицированы по VLAN ID, содержащемуся в метке. Если пакет помечен, как приоритетный, он будет классифицирован Port VLAN. Если пакеты должны быть помечены на выходе, они будут помечаться S-tag меткой.</p> <p><u>S-Custom-Port</u>. На входе пакеты с тегом VLAN с TPID = 0x8100 или Ethertype, настроенный для Custom-S портов будут классифицированы по VLAN ID, содержащемуся в метке. Если пакет не помечен или пакет помечен, как приоритетный, он будет классифицирован Port VLAN. Если пакеты должны быть помечены на выходе, они будут помечаться заданной S-tag меткой.</p> |
| Ingress Filter | <p>Гибридные порты позволяют менять входную фильтрацию. Access и Trunk порты всегда имеют включенную входную фильтрацию.</p> <p>Если входная фильтрация включена (флажок установлен), пакеты относящиеся к VLAN, в которой порт не является участником – будут отброшены.</p> <p>Если входная фильтрация выключена, пакеты относящиеся к VLAN, в которой порт не является участником – будут приняты и обработаны коммутатором.</p> |
| Ingress Acceptance | <p>Гибридные порты позволяют менять тип пакетов, принимаемых на входе.</p> <p><u>Tagged and Untagged</u>. Все типы пакетов с меткой или</p> |

| | |
|-----------------|---|
| | <p>без будут приниматься.</p> <p><u>Tagged only.</u> Только помеченные пакеты будут приниматься на входе. Пакеты без метки будут отброшены.</p> <p><u>Untagged only.</u> Только пакеты без метки будут приниматься на входе. Пакеты с меткой будут отброшены.</p> |
| Egress Tagging | <p>Порты в Trunk и Hybrid режимах могут контролировать присваивание метки на выходе</p> <p><u>Untag Port VLAN.</u> Пакеты относящиеся к Port VLAN будут передаваться без метки. Остальные пакеты получают соответствующую метку.</p> <p><u>Tag All.</u> Все пакеты, относящиеся к Port VLAN или нет будут передаваться с меткой.</p> <p><u>Untag All.</u> Все пакеты, относящиеся к Port VLAN или нет будут передаваться без метки. Только для Hybrid режима.</p> |
| Allowed VLANs | <p>Порты в режимах Trunk и Hybrid могут контролировать в какой VLAN они могут быть участниками. Access порты могут быть участниками только одной VLAN (Access VLAN). По умолчанию Trunk и Hybrid порты могут быть участниками всех VLAN 1-4094. Поле может быть пустым, что означает принадлежность порта ко всем VLAN.</p> |
| Forbidden VLANs | <p>Порт может быть настроен таким образом, чтобы не быть участником ни одной из VLAN. По умолчанию поле пустое, что означает принадлежность порта ко всем VLAN.</p> |

Нажмите Save, чтобы сохранить настройки.

8.6.2 Port Isolation (Изоляция портов)

Изоляция портов ограничивает обмен трафиком между портами. Функция похоже на VLAN, но имеет более строгие правила.

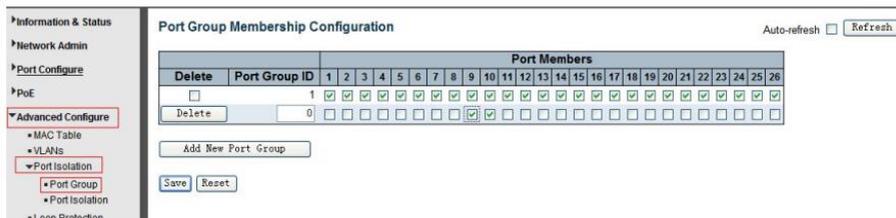
8.6.2.1 Port Group (Группа портов)

Коммутатор поддерживает формирование групп портов. Порты участники группы могут обмениваться данными.

Примечание: Порт может принадлежать к нескольким группам. Данные могут быть переданы между любыми портами, которые принадлежат одной группе портов

Настройки групп находятся в следующем разделе:

Advanced Configure > Port Isolation > Port Group



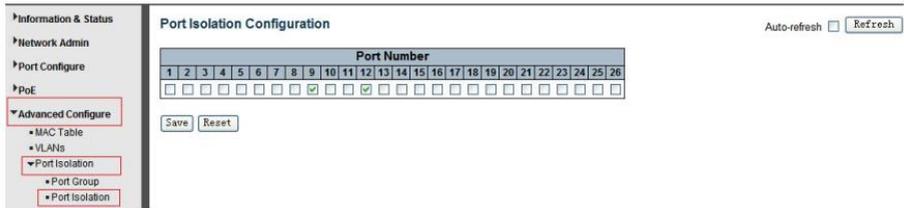
| | |
|--------------|--|
| Port members | Отметьте порты, которые будут принадлежать одной группе. |
|--------------|--|

Нажмите Add new Port Group, чтобы создать новую группу. Delete – чтобы удалить группу. Save – чтобы сохранить текущие настройки.

8.6.2.2 Port Isolation (Изоляция портов)

Настройка изоляции портов находится в следующем разделе WEB интерфейса коммутатора:

Advanced Configure > Port isolation > Port Isolation



| | |
|-------------|--|
| Port number | Отметьте порты, которые будут изолированы. |
|-------------|--|

Нажмите Save, чтобы сохранить настройки.

8.6.3 STP (Протокол связующего дерева)

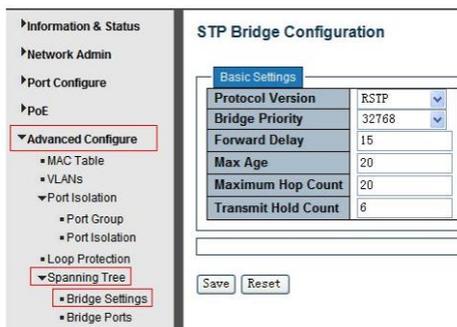
Spaning Tree Protocol (STP) – или протокол связующего дерева используется для обнаружения и исправления сетевых петель. Он обеспечивает запасные соединения между коммутаторами, мостами и маршрутизаторами.

STP позволяет коммутатору взаимодействовать с другими bridge устройствами сети, гарантируя существование только одного маршрута между любыми двумя станциями в сети, и обеспечивая наличие резервных соединений, которые автоматически используются, когда основное соединение по каким-либо причинам перестает существовать.

8.6.3.1 STP Bridge Settings (Настройки протокола STP)

Настройки протокола STP находятся в следующем разделе WEB интерфейса коммутатора:

Advanced Configure > Spanning Tree > Bridge Settings



| | |
|----------------------------|---|
| Protocol Version | Нажмите на выпадающее меню чтобы выбрать версию протокола STP: STP – Spanning Tree Protocol (IEEE 802.1D) RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w) |
| Bridge Priority | Контроль приоритета моста (bridge). Меньшее значение имеет больший приоритет. Приоритет моста + MSTI связан с 6-байтовым MAC адресом коммутатора формирует идентификатор моста (bridge). |
| Forward Delay (4-30) | Задержка перед отправкой. Значение может быть в диапазоне от 4 до 30 сек. По умолчанию – 15 сек. |
| Max age (6-40) | Максимальное время жизни информации отправленной мостом, пока он имеет роль корневого моста (root bridge). Допустимые значения находятся в диапазоне от 6 до 40 сек. Значение по умолчанию – 20 сек. |
| Maximum Hop Count (6-40) | Эта настройка определяет количество необходимых переходов (hop'ов) для MSTI информации, сформированной на границе MSTI. Также это значение определяет как много мостов в роли корневого моста могут передавать BPDU информацию. Допустимые значения находятся в диапазоне от 6 до 40 переходов. |
| Transmit Hold Count (1-10) | Количество BPDU пакетов, которые корневой порт (bridge port) может отправлять за 1 секунду. Если необходимо, может быть организована задержка перед отправкой следующего BPDU пакета. Доступные значения от 1 до 10 BPDU пакетов в секунду. Значение по умолчанию – 6. |

Нажмите Save, чтобы сохранить настройки.

8.6.3.2 STP Bridge Port (Выбор bridge порта)

Настройки STP bridge для портов находятся в следующем разделе WEB интерфейса коммутатора:

Advanced Configure > Spanning Tree > Bridge Ports

| | |
|-----------------|--|
| STP enabled | Отметьте, чтобы включить STP на порте. |
| Path Cost | <p>Поле определяет стоимость пути (path cost) для порта.</p> <p>Auto – стоимость пути высчитывается на основе физической скорости порта, используя значения, рекомендуемые 802.1D.</p> <p>Specific – стоимость пути, задаваемая пользователем.</p> <p>Стоимость пути используется для построения актуальной топологии сети. Порты с меньшим значением используются как forwarding порты.</p> <p>Доступные значения в диапазоне от 1 до 200000000</p> |
| Priority | Поле определяет приоритет порта. |
| Auto Edge | Отметьте, чтобы превратить порт в Auto Edge |
| Restricted Role | Отметьте, чтобы превратить порт в Restricted Role |
| Restricted TCN | Отметьте, чтобы превратить порт в Restricted TCN |

| | |
|----------------|--|
| BPDU Guide | Отметьте, чтобы активировать BPDU Guide. Когда порт получает BPDU пакет, он переходит в состояние «Disable», т.е. отключается. |
| Point-to-point | Поле отвечает за организацию соединения точка-точка. Агрегированные порты всегда находятся в состоянии Point-to-point |

Нажмите Save, чтобы сохранить настройки.

8.6.4 MAC Address Table (Таблица MAC адресов)

Настройки таблицы MAC адресов находятся в следующем разделе WEB интерфейса коммутатора:

Advanced Configure > MAC Table

| | |
|-------------------------|---|
| Disable Automatic Aging | Если этот чекбокс отмечен, функция автоматического устаревания отключена. |
| Aging Time | Время, после которого запись помещенная в таблицу будет исключена из нее. Диапазон 10-1000000 сек. Значение по умолчанию – 300 сек. |

| | |
|---------------------------------------|---|
| <p>MAC Table Learning</p> | <p>Коммутатор поддерживает 3 типа запоминания (learning) MAC адресов в таблицу</p> <p>Auto – порт автоматически запоминает MAC адреса.</p> <p>Disable – порт не запоминает MAC адреса</p> <p>Secure – порт пересылает данные только, если используется статический MAC адрес.</p> |
| <p>Static MAC Table Configuration</p> | <p>Статические записи MAC адресов отображаются в этой таблице. Нажмите «Add New Static Entry» (добавить новую статическую запись), чтобы создать новую запись.</p> |

Нажмите Save, чтобы сохранить настройки.

8.6.5 IGMP Snooping

Internet Group Management Protocol (IGMP) – позволяет хостами маршрутизаторам обмениваться информацией о multicast группах. IGMP Snooping это функция коммутатора, которая отвечает за контроль IGMP сообщениями. Главная цель IGMP Snooping – ограничить пересылку multicast пакетов только для портов, которые являются членами multicast групп.

8.6.5.1 Basic Information

Общая информация о IGMP настройках находится в следующем разделе WEB интерфейса коммутатора:

Advanced Configure > IGMP Snooping > Basic Configuration

- Information & Status
- Network Admin
- Port Configure
- PoE
- ▾ Advanced Configure
 - MAC Table
 - VLANs
 - Port Isolation
 - Loop Protection
 - Spanning Tree
 - MEP
 - ERPS
 - ▾ IGMP Snooping
 - Basic Configuration
 - VLAN Configuration
 - LLDP

IGMP Snooping Configuration

| Global Configuration | |
|--------------------------------------|-------------------------------------|
| Snooping Enabled | <input type="checkbox"/> |
| Unregistered IPMCv4 Flooding Enabled | <input checked="" type="checkbox"/> |

Port Related Configuration

| Port | Router Port | Fast Leave |
|------|--------------------------|--------------------------|
| * | <input type="checkbox"/> | <input type="checkbox"/> |
| 1 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2 | <input type="checkbox"/> | <input type="checkbox"/> |
| 3 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6 | <input type="checkbox"/> | <input type="checkbox"/> |
| 7 | <input type="checkbox"/> | <input type="checkbox"/> |
| 8 | <input type="checkbox"/> | <input type="checkbox"/> |
| 9 | <input type="checkbox"/> | <input type="checkbox"/> |

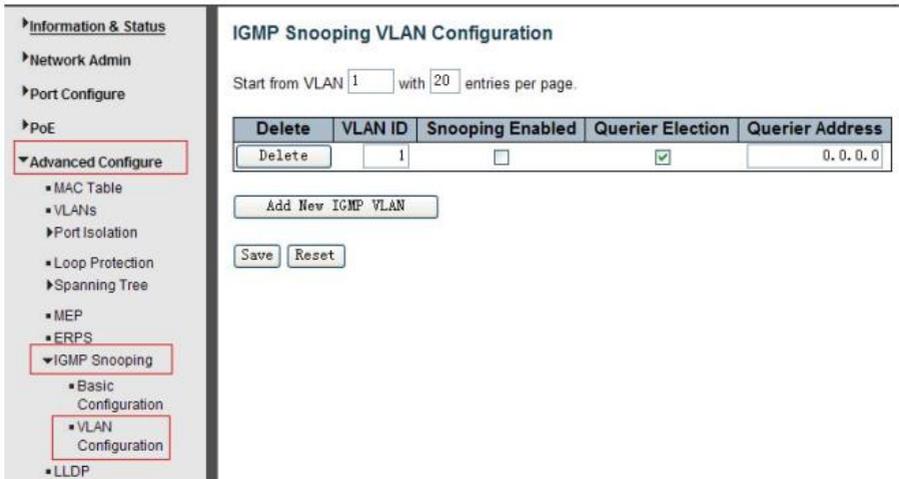
| | |
|-------------------------------------|---|
| Snooping Enabled | Вкл/выкл функции IGMP Snooping. Значение по умолчанию – отключено (disabled) |
| Unregistred IPMCv4 Flooding Enabled | Отметьте чекбокс, чтобы включить функцию Unregistred IPMCv4 Flooding. |
| Router Port | Поле определяет, какие порты будут отмечены, как router порты. Router порт в коммутаторе ведет к multicast устройству или устройству, запрашивающему IGMP. Если в качестве router порта выбран порт агрегированной группы, то вся группа портов будет выполнять роль router портов. |
| Fast Leave | Данная настройка отвечает за удаление MAC адреса немедленно после получения сообщения для группы. |

Нажмите Save, чтобы сохранить настройки.

8.6.5.2 IGMP Snooping VLAN Configuration (Настройка IGMP Snooping для VLAN)

Настройка IGMP Snooping для VLAN находится в следующем разделе WEB интерфейсе коммутатора:

Advanced Configure > IGMP Snooping > VLAN Configuration



| | |
|------------------|--|
| Snooping Enabled | Включение IGMP для VLAN. 32 VLAN могут быть отмечены для IGMP Snooping |
| Querier Election | Включить вступление IGMP Querier в VLAN. |
| Querier Address | Поле определяет IPv4 адрес источника, использующего IP заголовок для IGMP. По умолчанию это поле равно 192.0.2.1 |

Нажмите Save, чтобы сохранить настройки.

8.6.6 ERPS (Протокол ERPS)

ERPS – специальный протокол для защиты коммутатора от сетевых петель при использовании в кольцевой топологии. Время восстановления топологии при использовании этого протокола < 50ms.

Примечание: Перед использованием ERPS необходимо отключить STP на портах, так как они являются взаимоисключающими.

Раздел с настройками ERPS находится по адресу:

Advanced Configure > ERPS

| Delete | Ring ID | East Port | West Port | Ring Type | Interconnected Node | Major RRing ID | Alarm |
|--------------------------|---------|-----------|-----------|-----------|--------------------------|----------------|------------------------------------|
| <input type="checkbox"/> | 1 | 1 | 2 | Major | No | 1 | ● |
| Delete | 2 | 1 | 1 | Sub | <input type="checkbox"/> | 0 | ● |

Buttons: Add New Ring Group, Save, Reset

| | |
|-----------|--|
| Ring ID | Идентификатор ERPS Ring |
| East Port | Номер порта, который участвует в Ring Protection |
| West Port | Номер другого порта, который участвует в Ring Protection |
| Ring Type | Доступен выбор Major Ring – основное кольцо Sub Ring – вспомогательное кольцо По умолчанию тип кольца – Major Ring. |

| | |
|---------------------|---|
| Interconnected Node | В топологии «мультикольцо», Interconnected Node – это узел соединяющий 2 или более колец. |
| Major Ring ID | В топологии «одно кольцо», Major Ring ID имеет тоже самое значение, что и Ring ID. В топологии «мультикольцо», субкольцо имеет тот же тип, что и Major Ring ID |
| R-APS VLAN (1-4094) | Поле определяет VLAN для R-APS VLAN'ов. |

Нажмите Save, чтобы сохранить настройки.

После нажатия на номер под полем «Ring ID» открывается страница WEB интерфейса, как на рисунке ниже:

| | |
|-----------------------------------|---|
| WTR (Wait to restore) Time (1-12) | Нажмите на выпадающее меню, чтобы выбрать время до восстановления R-APS. Доступный диапазон значений 1-12 мин. По умолчанию – 1 мин. |
| Revertive | Отметьте чекбокс, чтобы задать статус Revertive для R-APS |
| VLAN Config | После нажатия на VLAN Config, это приведет на страницу Rapid Ring VLAN Configuration |

| | |
|----------|--|
| RPL Role | Нажмите на выпадающее меню, чтобы выбрать роль: None – без роли RPL Owner – владелец RPL RPL Neighbor – «сосед» RPL |
| RPL Port | Нажмите на выпадающее меню, чтобы выбрать тип порта None – не выбрано East port West port |

Нажмите Save, чтобы сохранить настройки.

После нажатия на VLAN Config открывается страница WEB интерфейса настройки Rapid Ring VLAN, как на рисунке ниже:



Нажмите Add New Entry, чтобы добавить новую запись.
Нажмите Save, чтобы сохранить настройки.

8.6.7 LLDP (Настройка протокола LLDP)

Link Layer Discovery Protocol (LLDP) – протокол канального уровня, позволяющий сетевому оборудованию оповещать оборудование, работающее в локальной сети, о своём существовании и передавать ему свои характеристики, а также получать от него аналогичные сведения. Описание протокола приводится в стандарте IEEE 802.1AB.

Настройки данного протокола находятся в следующем разделе WEB интерфейса коммутатора:

Advanced Configure > LLDP

LLDP Configuration

LLDP Parameters

| | | |
|-------------|----|---------|
| Tx Interval | 30 | seconds |
| Tx Hold | 4 | times |
| Tx Delay | 2 | seconds |
| Tx Reinit | 2 | seconds |

LLDP Port Configuration

| Port | Mode | Optional TLVs | | | | |
|------|----------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| | | Port Descr | Sys Name | Sys Descr | Sys Capa | Mgmt Addr |
| * | <> | <input checked="" type="checkbox"/> |
| 1 | Disabled | <input checked="" type="checkbox"/> |
| 2 | Disabled | <input checked="" type="checkbox"/> |
| 3 | Disabled | <input checked="" type="checkbox"/> |
| 4 | Disabled | <input checked="" type="checkbox"/> |
| 5 | Disabled | <input checked="" type="checkbox"/> |
| 6 | Disabled | <input checked="" type="checkbox"/> |

LLDP Parameters

В данном поле есть возможность настроить текущие LLDP настройки для порта:

TX interval

Tx Hold

Tx Delay

Tx Reinit

| | |
|---------------|---|
| Mode | Выбор LLDP сообщений для режима отправки и приема. Tx Only Rx Only Enabled Disabled |
| Optional TLVs | Поле отвечающее за настройку информации, которая включена в TLV поле публикуемых сообщений. Port Descr Sys Name Sys Descr Sys Capa Mgmt Addr |

Нажмите Save, чтобы сохранить настройки.

8.6.8 Loop Protection (Защита от сетевых петель)

Данный раздел WEB интерфейса коммутатора предоставляет доступ к настройкам защиты от сетевых петель во время broadcast или multicast шторма.

Advanced Configure > Loop Protection

Loop Protection Configuration

General Settings

Global Configuration

| | | |
|------------------------|---------|---------|
| Enable Loop Protection | Disable | |
| Transmission Time | 5 | seconds |
| Shutdown Time | 180 | seconds |

Port Configuration

| Port | Enable | Action | Tx Mode |
|------|--------------------------|-----------------------|---------|
| * | <input type="checkbox"/> | <> | <> |
| 1 | <input type="checkbox"/> | Shutdown Port | Enable |
| 2 | <input type="checkbox"/> | Shutdown Port and Log | Disable |
| 3 | <input type="checkbox"/> | Log Only | Enable |

| | |
|----------------------|--|
| Global Configuration | <p>Вкл/выкл защиты от сетевых петель.</p> <p>Transmission time – значение в сек, отвечающее за показатель Loop Protection Interval Time</p> <p>Shutdown Time – значение в сек для настройки порта Shutdown Time</p> |
| Enable | Отметьте чекбокс, чтобы активировать Loop Protection на порте. |
| Action | <p>Действие, применяющееся к порту, на котором замечена сетевая петля.</p> <p>Shutdown port – отключение порта</p> <p>Shutdown port and log – отключение порта и запись в журнал</p> <p>Log only – только запись в журнал.</p> |
| Tx Mode | Вкл/выкл Режимы передачи Tx |

Нажмите Save, чтобы сохранить настройки.

8.7 QoS (Приоритезация трафика)

Quality of Service (QoS) – технология предоставления различным классам трафика различных приоритетов в обслуживании.

QoS позволяет задавать различные уровни сетевого обслуживания для разных типов трафика, таких как мультимедийный, видео, и прочие типы. С помощью QoS можно понижать приоритет обработки трафика, который не является важным.

8.7.1 QoS Port Classification (Классификация портов с помощью QoS)

Настроить разные классы для портов можно в следующем разделе WEB интерфейса коммутатора:

QoS Configure > Port Classification

QoS Ingress Port Classification

| Port | CoS | DPL | PCP | DEI | Address Mode |
|------|-----|-----|-----|-----|--------------|
| * | <> | <> | <> | <> | <> |
| 1 | 0 | 0 | 0 | 1 | Source |
| 2 | 1 | 1 | 1 | 0 | Destination |
| 3 | 2 | 0 | 2 | 0 | Source |
| 4 | 3 | 0 | 3 | 0 | Destination |
| 5 | 4 | 0 | 4 | 0 | Source |
| 6 | 5 | 0 | 5 | 0 | Source |
| 7 | 6 | 0 | 6 | 0 | Source |
| 8 | 7 | 0 | 7 | 0 | Source |

| | |
|--------------|--|
| CoS | Поле отвечает класс обслуживания. Диапазон от 0 до 7, где 0 (самый низкий приоритет), а 7 (самый высокий приоритет). <i>Примечание: По умолчанию значение CoS изменяется динамически.</i> |
| DPL | Поле отвечает за Drop Precedence Level |
| PCP | Поле отвечает за значение PCP. Все пакеты классифицируются на основе PCP. |
| DEI | Поле отвечает за значение DEI по умолчанию. Все пакеты классифицируются на основе DEI. |
| Address Mode | IP/MAC режим |

Нажмите Save, чтобы сохранить настройки.

8.7.2 Port Policing (Функция ограничения скорости на портах)

Данная функция находится в следующем разделе WEB интерфейса коммутатора:

QoS Configure > Port Policing

| Port | Enabled | Rate | Unit | Flow Control |
|------|-------------------------------------|------|------|-------------------------------------|
| * | <input type="checkbox"/> | 500 | <> | <input type="checkbox"/> |
| 1 | <input checked="" type="checkbox"/> | 500 | kbps | <input checked="" type="checkbox"/> |
| 2 | <input type="checkbox"/> | 500 | Mbps | <input type="checkbox"/> |
| 3 | <input checked="" type="checkbox"/> | 500 | fps | <input checked="" type="checkbox"/> |
| 4 | <input type="checkbox"/> | 500 | kfps | <input type="checkbox"/> |
| 5 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> |
| 6 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> |

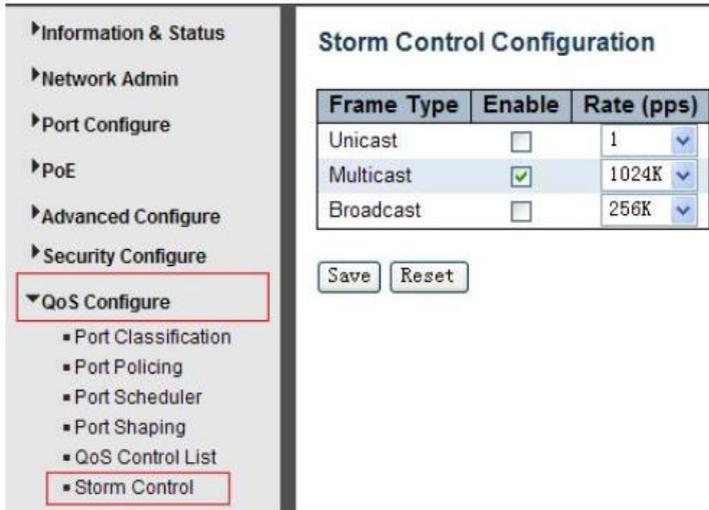
| | |
|--------------|--|
| Enabled | Отметьте чекбокс, чтобы активировать функцию Port Policing для порта |
| Rate | Значение по умолчанию 500. Диапазон возможных значений 100-1000000, если в поле Unit выбрано kbps (Кбит/с) или fps (пакетов в сек) и 1-3300, если в поле Unit выбрано mbps (Мбит/с) или kfps (тысяч пакетов/сек) |
| Unit | Значение по умолчанию – kbps (Кбит/с) |
| Flow Control | Если управление потоком включено и порт находится в таком режиме, то отправляются пакеты «паузы», вместо отбрасывания пакетов. |

Нажмите Save, чтобы сохранить настройки.

8.7.3 Storm Control Configuration (Настройка защиты от сетевого шторма)

Данная функция находится в следующем разделе WEB интерфейса коммутатора:

QoS Configure > Storm Control



| | |
|------------|---|
| Frame Type | Коммутатор поддерживает до 3 типов пакетов, которые могут нести угрозу в виде сетевого шторма: Unicast Unknown Multicast Broadcast |
| Enable | Отметьте чекбокс, чтобы включить защиту от сетевого шторма |
| Rate (pps) | Скорость пропускания пакетов в сек (pps). Доступные значения: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, 1024K. |

Нажмите Save, чтобы сохранить настройки.

8.8 Security Configure (Настройки безопасности)

8.8.1 Password (Пароль)

Пароль системы можно поменять в данном разделе WEB интерфейса коммутатора:

Security Configure > Password



| | |
|----------------------|----------------------|
| Old Password | <input type="text"/> |
| New Password | <input type="text"/> |
| Confirm New Password | <input type="text"/> |

Нажмите Save, чтобы сохранить настройки.

8.8.2 802.1X

Стандарт IEEE 802.1X определяет протокол контроля доступа и аутентификации, который ограничивает права неавторизованных компьютеров, подключенных к коммутатору.

Сервер аутентификации проверяет каждый компьютер перед тем, как тот сможет воспользоваться сервисами, которые предоставляет ему коммутатор. До тех пор, пока компьютер не аутентифицировался, он может использовать только протокол EAPOL (англ. extensible authentication protocol over LAN) и только после успешной аутентификации весь остальной трафик сможет проходить через тот порт коммутатора, к которому подключен данный компьютер.

Коммутатор поддерживает протокол контроля доступа на основе IEEE 802.1X. Настройки находятся в следующем разделе WEB интерфейса коммутатора:

Security Configure > 802.1X

Network Access Server Configuration

System Configuration

| | |
|--------------------------|--------------------------|
| Mode | Disabled |
| Reauthentication Enabled | <input type="checkbox"/> |
| Reauthentication Period | 3600 seconds |
| EAPOL Timeout | 30 seconds |
| Aging Period | 300 seconds |
| Hold Time | 10 seconds |

Port Configuration

| Port | Admin State | Port State | Restart |
|------|------------------|-------------------|-----------------------------|
| * | <> | | |
| 1 | Force Authorized | Globally Disabled | Reauthenticate Reinitialize |
| 2 | Force Authorized | Globally Disabled | Reauthenticate Reinitialize |
| 3 | Force Authorized | Globally Disabled | Reauthenticate Reinitialize |
| 4 | Force Authorized | Globally Disabled | Reauthenticate Reinitialize |

| | |
|----------------------|--|
| System Configuration | В этом поле пользователь может вкл/выкл 802.1X или повторную аутентификацию, а также настроить период повторной аутентификации, таймаут для EAPOL, период устаревания и время удержания. |
| Port Configuration | В выпадающем меню можно выбрать настройки для состояния портов: Force Authorized – ускоренная авторизация Force Unauthorized 802.1X – авторизация на базе протокола 802.1X Mac Based Auth – авторизация на базе MAC адреса |

Нажмите Save, чтобы сохранить настройки.

8.8.3 DHCP Snooping (Защита от атак с использованием DHCP)

8.8.3.1 About DHCP Snooping (Описание функции DHCP Snooping)

DHCP snooping — функция коммутатора, предназначенная для защиты от атак с использованием протокола DHCP. Например, атаки с подменой DHCP-сервера в сети или атаки DHCP starvation, которая заставляет DHCP-сервер выдать все существующие на сервере адреса злоумышленнику.

DHCP snooping регулирует только сообщения DHCP и не может повлиять напрямую на трафик пользователей или другие протоколы. Некоторые функции коммутаторов, не имеющие непосредственного отношения к DHCP, могут выполнять проверки на основании таблицы привязок DHCP snooping (DHCP snooping binding database). В их числе:

- ✓ Dynamic ARP Protection (Inspection) — проверка ARP-пакетов, направленная на борьбу с ARP-spoofing,
- ✓ IP Source Guard — выполняет проверку IP-адреса отправителя в IP-пакетах, предназначенная для борьбы с IP-spoofingом.

DHCP snooping позволяет:

- ✓ защитить клиентов в сети от получения адреса от неавторизованного DHCP-сервера,
- ✓ регулировать какие сообщения протокола DHCP отбрасывать, какие перенаправлять и на какие порты.

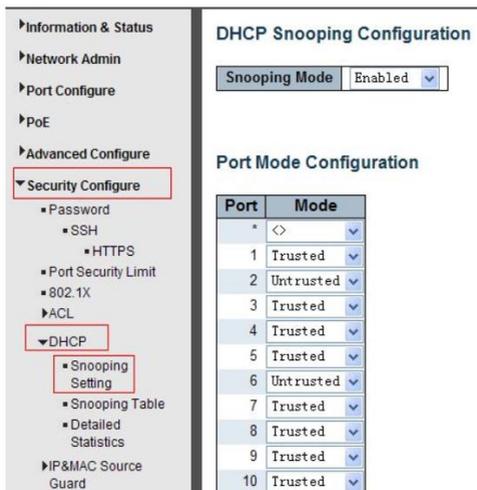
Для правильной работы DHCP snooping, необходимо указать какие порты коммутатора будут доверенными (trusted), а какие — нет (untrusted, в дальнейшем — ненадёжными):

- ✓ Ненадёжные (Untrusted) — порты, к которым подключены клиенты. DHCP-ответы, приходящие с этих портов отбрасываются коммутатором. Для ненадёжных портов выполняется ряд проверок сообщений DHCP и создаётся база данных привязки DHCP (DHCP snooping binding database).
- ✓ Доверенные (Trusted) — порты коммутатора, к которым подключен другой коммутатор или DHCP-сервер. DHCP-пакеты, полученные с доверенных портов не отбрасываются.

8.8.3.2 DHCP Snooping Configure (Настройка DHCP Snooping)

Настройки функции DHCP Snooping находятся в следующем разделе WEB интерфейса коммутатора:

Security Configure > DHCP > Snooping Settings



| | |
|--------------------|---|
| DHCP Snooping Mode | Нажмите на выпадающее меню, чтобы вкл/выкл DHCP Snooping |
| Port Mode | Поле отображает режим DHCP Snooping для портов: Trusted – доверенные порты Untrusted – недоверенные порты Подробнее в пункте 8.8.3.1 About DHCP Snooping |

Нажмите Save, чтобы сохранить настройки.

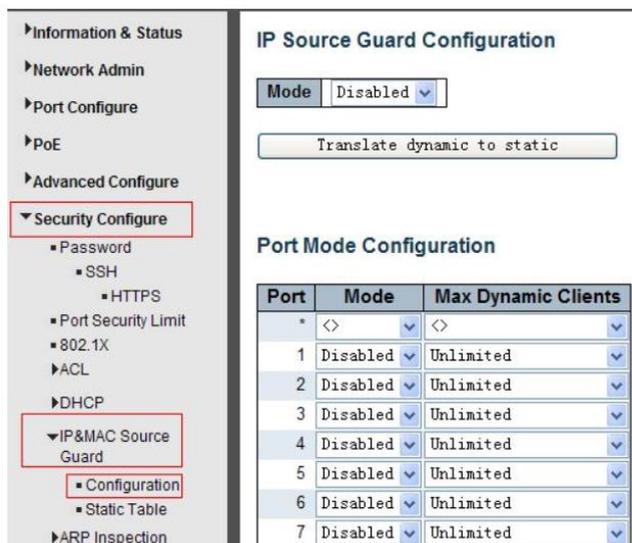
8.8.4 IP&MAC Source Guard

Функция коммутатора, которая ограничивает IP-трафик на интерфейсах 2го уровня, фильтруя трафик на основании таблицы привязок DHCP snooping и статических соответствий. Функция используется для борьбы с IP-spoofingом.

8.8.4.1 Port Configuration (Настройка IP&MAC Source Guard для портов)

Настроить функцию IP&MAC Source Guard для портов можно в следующем разделе WEB интерфейса коммутатора:

Security Configure > IP & MAC Source Guard > Configuration



| | |
|---------------------|--|
| Global Mode | Нажмите на выпадающее меню, чтобы вкл/выкл функцию IP&MAC Source Guard глобально. |
| Port Mode | Нажмите на выпадающее меню, чтобы вкл/выкл функцию IP&MAC Source Guard для выбранного порта. |
| Max Dynamic Clients | Нажмите на выпадающее меню, чтобы выбрать максимальное количество динамических клиентов. Доступные значения: Unlimited, 0, 1, 2. |

Нажмите Save, чтобы сохранить настройки.

8.8.4.2 Static Table (Таблица статических соответствий)

На данной странице WEB интерфейса коммутатора есть возможность вручную настроить Таблицу статических соответствий для функции IP&MAC Source Guard. Все настройки доступны здесь:

Security Configure > IP&MAC Source Guard > Static Table

Static IP Source Guard Table

| Delete | Port | VLAN ID | IP Address | MAC address |
|--------|------|---------|------------|-------------|
| Delete | 1 | | | |

Add New Entry

Save Reset

| | |
|-------------|---|
| Port | Нажмите на выпадающее меню, чтобы выбрать порт |
| VLAN | Нажмите на выпадающее меню, чтобы выбрать VLAN ID |
| IP Address | Поле с IP адресом |
| MAC Address | Поле с MAC адресом |

Нажмите Save, чтобы сохранить настройки.

8.8.5 ARP Inspection (Проверка ARP пакетов)

Функция коммутатора, предназначенная для защиты от атак с использованием протокола ARP. Например, атаки ARP-spoofing, позволяющей перехватывать трафик между узлами, которые расположены в пределах одного широковещательного домена.

Dynamic ARP Inspection (Protection) регулирует только сообщения протокола ARP и не может повлиять напрямую на трафик пользователей или другие протоколы.

8.8.5.1 Port Configuration (Настройка ARP Inspection для портов)

Пользователь может настроить ARP Inspection для конкретного порта на этой странице WEB интерфейса коммутатора:

Security Configure > ARP Inspection > Port Configuration

ARP Inspection Configuration

Mode: Disabled

Translate dynamic to static

Port Mode Configuration

| Port | Mode | Check VLAN | Log Type |
|------|----------|------------|----------|
| * | <> | <> | <> |
| 1 | Disabled | Disabled | None |
| 2 | Disabled | Disabled | None |
| 3 | Disabled | Disabled | None |
| 4 | Disabled | Disabled | None |
| 5 | Disabled | Disabled | None |
| 6 | Disabled | Disabled | None |
| 7 | Disabled | Disabled | None |
| 8 | Disabled | Disabled | None |

| | |
|-------------|--|
| Global Mode | Нажмите на выпадающее меню, чтобы вкл/выкл ARP Inspection глобально. |
| Port Mode | Нажмите на выпадающее меню, чтобы вкл/выкл ARP Inspection для портов. |
| Check VLAN | Если необходимо включить ARP Inspection для VLAN, активируйте (enable) функцию в выпадающем меню «Check VLAN». Значение по умолчанию – отключено (disable). |
| Log Type | None – журнал ARP Inspection не ведется. Deny – журнал ведется для заблокированных записей. Permit – журнал ведется для разрешенных записей. ALL – журнал ведется для всех типов записей. |

Нажмите Save, чтобы сохранить настройки.

8.8.5.2 VLAN Configuration (Настройка ARP Inspection для VLAN)

Настройки ARP Inspection для VLAN находятся в следующем разделе WEB интерфейса коммутатора:

Security Configure > ARP Inspection > VLAN Configuration

The screenshot displays the 'VLAN Mode Configuration' page. On the left, the navigation menu is expanded to 'Security Configure' > 'ARP Inspection' > 'VLAN Configuration'. The main panel shows a table for deleting entries:

| Delete | VLAN ID | Log Type |
|---------------------------------------|---------|----------|
| <input type="button" value="Delete"/> | 1 | None |

Below the table, there is an 'Add New Entry' button, and at the bottom, 'Save' and 'Reset' buttons. The text 'Start from VLAN 1 with 20 entries per page.' is visible at the top of the configuration area.

| | |
|----------|--|
| VLAN ID | Отображает VLAN ID для текущей VLAN |
| Log Type | None – журнал ARP Inspection не ведется. Deny – журнал ведется для заблокированных записей. Permit – журнал ведется для разрешенных записей. ALL – журнал ведется для всех типов записей. |

Нажмите Save, чтобы сохранить настройки.

8.8.5.3 Static Table (Таблица соответствий для ARP Inspection)

Пользователь может самостоятельно настроить таблицу соответствий для ARP Inspection. Соответствующие настройки находятся в следующем разделе WEB интерфейса коммутатора:

Security Configure > ARP Inspection > Static Table

The screenshot displays the configuration page for the Static ARP Inspection Table. On the left, a navigation menu is visible with the following structure:

- Information & Status
- Network Admin
- Port Configure
- PoE
- Advanced Configure
 - Security Configure (highlighted with a red box)
 - Password
 - SSH
 - HTTPS
 - Port Security Limit
 - 802.1X
 - ACL
 - DHCP
 - IP&MAC Source Guard
 - ARP Inspection (highlighted with a red box)
 - Port Configuration
 - VLAN Configuration
 - Static Table (highlighted with a red box)
 - Dynamic Table

The main content area is titled "Static ARP Inspection Table" and contains the following elements:

| Delete | Port | VLAN ID | MAC Address | IP Address |
|---------------------------------------|------------------------------------|----------------------|----------------------|----------------------|
| <input type="button" value="Delete"/> | 1 <input type="button" value="v"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |

Below the table, there is an "Add New Entry" button and "Save" and "Reset" buttons.

| | |
|-------------|--|
| Port | Нажмите на выпадающее меню, чтобы выбрать порт |
| VLAN | Выберите VLAN ID для настраиваемой VLAN |
| IP Address | Укажите IP адрес |
| MAC Address | Укажите MAC адрес |

Нажмите Save, чтобы сохранить настройки.

8.8.6 ACL (Правила контроля доступа)

Access Control List или ACL — список управления доступом, который определяет, кто или что может получать доступ к объекту (программе, процессу или файлу), и какие именно операции разрешено или запрещено выполнять субъекту (пользователю, группе пользователей).

8.8.6.1 ACL Port Configure (Настройка ACL для портов)

Настройки правил контроля доступа (ACL) находятся в соответствующем разделе:

Security Configure > ACL > Ports

| Port | Policy ID | Action | Rate Limiter ID | Port Redirect | Mirror | Logging | Shutdown | State | Counter |
|------|-----------|--------|-----------------|------------------------------|----------|----------|----------|---------|---------|
| * | 0 | <> | <> | Disabled Port 1 Port 2 | <> | <> | <> | <> | * |
| 1 | 0 | Permit | Disabled | Port 1 Port 2 Port 3 | Disabled | Disabled | Disabled | Enabled | 0 |
| 2 | 0 | Permit | Disabled | Disabled Port 1 Port 2 | Disabled | Disabled | Disabled | Enabled | 247562 |
| 3 | 0 | Permit | Disabled | Disabled Port 1 Port 2 | Disabled | Disabled | Disabled | Enabled | 0 |
| 4 | 0 | Permit | Disabled | Disabled Port 1 Port 2 | Disabled | Disabled | Disabled | Enabled | 0 |
| 5 | 0 | Permit | Disabled | Disabled Port 1 | Disabled | Disabled | Disabled | Enabled | 0 |

| | |
|-----------------|--|
| Action | <p>Permit – разрешает выбранному порту пропускать данные</p> <p>Deny – запрещает выбранному порту пропускать данные</p> |
| Rate Limiter ID | <p>Ограничитель пропускной способности портов. Настройки находятся в соответствующем разделе.</p> |
| Port Redirect | <p>Выбор порта, пакеты с которого будут перенаправлены. Значение по умолчанию – Disabled (отключено)</p> |
| Mirror | <p>Поле определяет параметры зеркалирования на настраиваемом порте. Доступные значения</p> <p>Enabled – включено</p> <p>Disabled – отключено</p> <p>Значение по умолчанию – Disabled</p> |
| Logging | <p>Включение/выключение ведения журнала записей</p> |
| Shut Down | <p>Enabled – если пакеты будут получены на этом порте, порт будет выключен.</p> <p>Disabled – порт не будет выключен при получении пакетов.</p> <p>Значение по умолчанию – Disabled.</p> <p><i>Примечание: данная функция работает, только если размер пакета меньше 1518 (без VLAN тэгов)</i></p> |
| State | <p>Enabled – для открытия порта используются правила ACL заданные пользователем</p> <p>Disabled – для закрытия порта используются правила ACL заданные пользователем</p> <p>Значение по умолчанию – Enabled</p> |
| Counter | <p>Количество пакетов удовлетворяющих заданным правилам</p> |

Нажмите Save, чтобы сохранить настройки.

8.8.6.2 Rate Limiter Configuration (Настройка ограничителя пропускной способности портов)

Пользователь может настроить правила ACL для ограничителя пропускной способности для портов в соответствующем разделе WEB интерфейса коммутатора:

Security Configure > ACL > Rate Limiter

ACL Rate Limiter Configuration

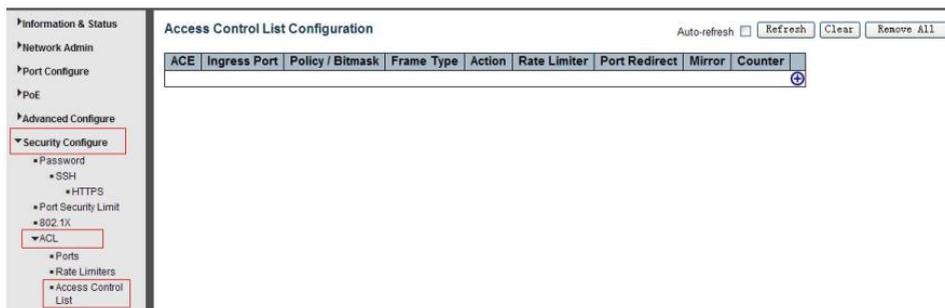
| Rate Limiter ID | Rate | Unit |
|-----------------|------|-------|
| * | 1 | <> ▾ |
| 1 | 1 | pps ▾ |
| 2 | 1 | pps ▾ |
| 3 | 1 | pps ▾ |
| 4 | 1 | pps ▾ |
| 5 | 1 | pps ▾ |
| 6 | 1 | pps ▾ |
| 7 | 1 | pps ▾ |
| 8 | 1 | pps ▾ |
| 9 | 1 | pps ▾ |
| 10 | 1 | pps ▾ |
| 11 | 1 | pps ▾ |
| 12 | 1 | pps ▾ |
| 13 | 1 | pps ▾ |

Нажмите Save, чтобы сохранить настройки.

8.8.6.3 Access Control List Configuration (Настройка ACL)

Пользователь может гибко настроить ACL в соответствующем разделе WEB интерфейса коммутатора:

Security Configure > ACL > Access Control List



Чтобы добавить и изменить запись нажмите кнопку «+»

8.9 Diagnostics (Инструменты диагностики и мониторинга)

8.9.1 Ping Test (Тестирование соединения с помощью PING)

PING это небольшой модуль, который взаимодействует с ECHO пакетами от IP адреса, который принадлежит удаленному устройству.

Данный инструмент находится в соответствующем разделе WEB интерфейса коммутатора:

Diagnostics > Ping

The screenshot shows a network configuration interface. On the left is a sidebar menu with the following items: Information & Status, Network Admin, Port Configure, PoE, Advanced Configure, Security Configure, QoS Configure, Diagnostics (highlighted with a red box), Ping (highlighted with a red box), Cable Diagnostics, and CPU Load. The main area is titled 'ICMP Ping' and contains four input fields: IP Address (0.0.0.0), Ping Length (56), Ping Count (5), and Ping Interval (1). Below these fields is a 'Start' button.

| | |
|---------------|--|
| IP Address | IP адрес удаленного адресата, который необходимо проверить |
| Ping Length | Число от 1 до 1452. Значение по умолчанию – 56 |
| Ping Count | Количество отправляемых PING запросов. От 1 до 60. |
| Ping Interval | Интервал между отправкой PING запросов. |

Нажмите кнопку «Start», чтобы приступить к тестированию с помощью Ping

8.9.2 Cable Diagnostics (Проверка кабеля)

Диагностика кабеля доступна только для медных кабелей, совместимых с 10/100/1000BaseT. Инструмент позволяет определить длину кабеля и его состояние.

Diagnostics > Cable Diagnostics

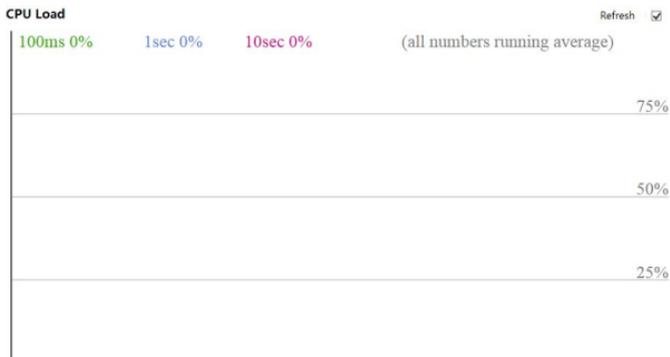
| Cable Status | | | | | | | | |
|--------------|--------|----------|--------|----------|--------|----------|--------|----------|
| Port | Pair A | Length A | Pair B | Length B | Pair C | Length C | Pair D | Length D |
| 1 | Open | 0 | Open | 0 | Open | 0 | Open | 0 |
| 2 | OK | 6 | OK | 6 | -- | 0 | -- | 0 |
| 3 | Open | 0 | Open | 0 | Open | 0 | Open | 0 |
| 4 | Open | 0 | Open | 0 | Open | 0 | Open | 0 |

Нажмите кнопку «Start», чтобы приступить к диагностике.

8.9.3 CPU Load (Загрузка CPU коммутатора)

На данной странице WEB интерфейса находится график загрузки CPU коммутатора в реальный момент времени.

Diagnostics > CPU Load

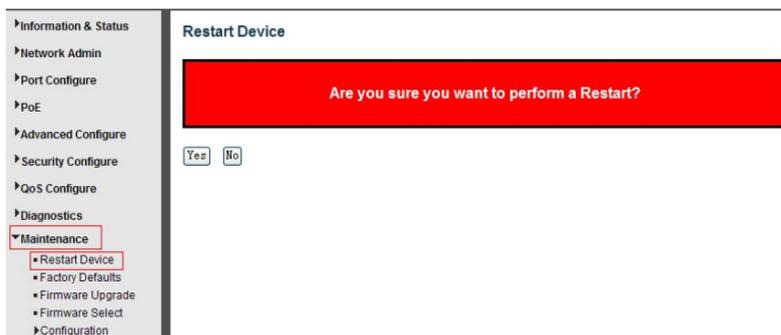


8.10 Maintenance (Обслуживание)

8.10.1 Restart Device (Перезагрузка коммутатора)

На данной странице WEB интерфейса находится инструмент для удаленной перезагрузки коммутатора.

Maintenance > Restart Device



Yes – перезагрузка коммутатора

8.10.2 Factory Defaults (Возврат к заводским настройкам)

На данной странице WEB интерфейса находится инструмент для возврата коммутатора к заводским настройкам.

Maintenance > Factory Defaults

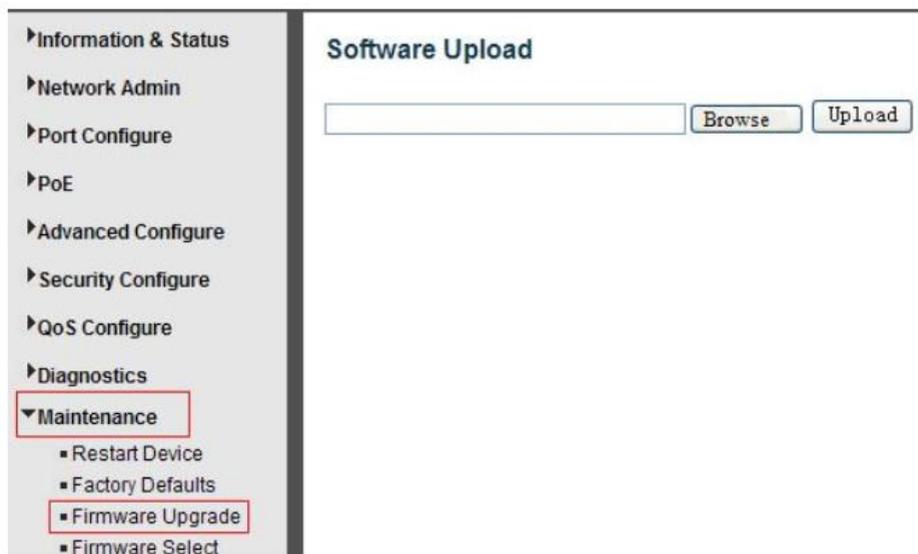


Yes – сброс настроек коммутатора к заводским.

8.10.3 Firmware Upgrade (Обновление прошивки)

На данной странице WEB интерфейса находится инструмент для обновления прошивки коммутатора.

Maintenance > Firmware Upgrade



Нажмите Browse, выберите файл с прошивкой. Нажмите Upload, чтобы загрузить прошивку в коммутатор.

8.10.4 Firmware Select (Выбор текущей прошивки коммутатора)

Коммутатор позволяет выбрать один из 2х образов текущей прошивки коммутатора

Maintenance > Firmware Select

Для выбора альтернативной прошивки нажмите кнопку «Activate Alternate Image»

Software Image Selection

| Active Image | |
|--------------|--|
| Image | managed |
| Version | 24GF-4G (standalone) V1.1-ONV-20150401 |
| Date | 2015-07-15T14:55:28+08:00 |

| Alternate Image | |
|-----------------|--|
| Image | managed.bk |
| Version | 24GF-4G (standalone) V1.1-ONV-20150401 |
| Date | 2015-06-11T21:44:05+08:00 |

Activate Alternate Image Cancel

8.10.5 Configuration (Текущая конфигурация)

В данном разделе содержатся инструменты для сохранения и загрузки файла с текущей конфигурацией коммутатора

8.10.5.1 Download (Сохранение файла с текущей конфигурацией коммутатора)

Maintenance > Configuration > Download

Download Configuration

Select configuration file to save.

Please note: running-config may take a while to prepare for download.

File Name

running-config

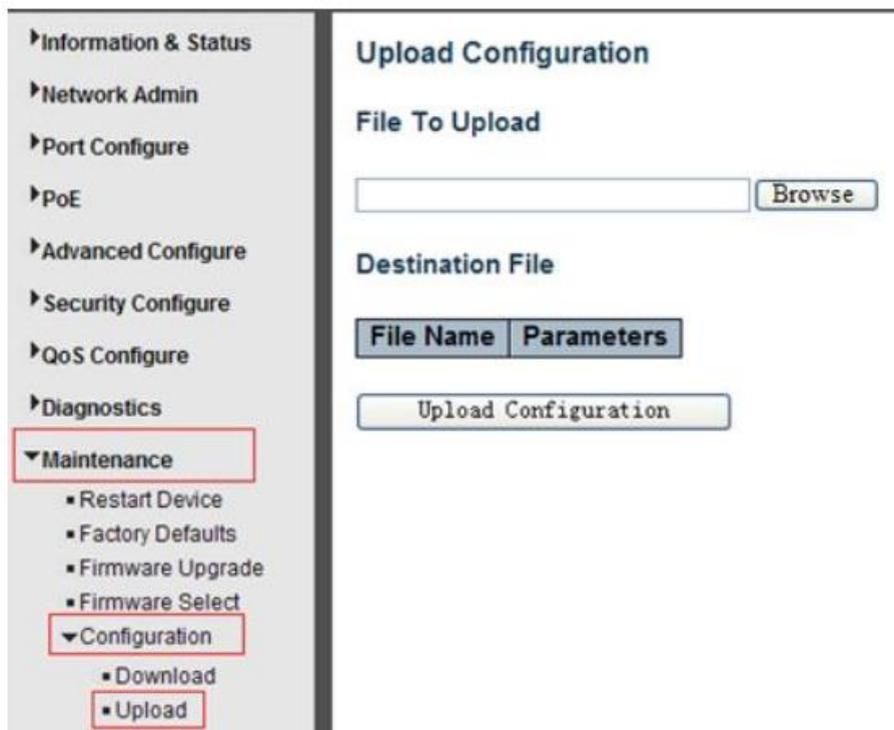
default-config

Download Configuration

Выберите файл с текущей конфигурацией (running config) или конфигурацией по умолчанию (default config), а затем нажмите кнопку «Download Configuration»

8.10.5.2 Upload Configuration (Загрузка файла с конфигурацией)

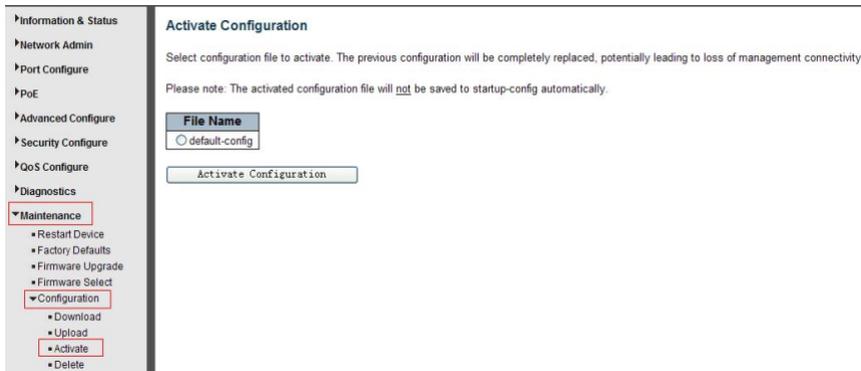
Maintenance > Configuration > Upload



Нажмите кнопку «Browse», чтобы выбрать файл с конфигурацией для коммутатора. Нажмите кнопку «Upload Configuration», чтобы загрузить файл с конфигурацией в коммутатор.

8.10.5.3 Activate Configuration (Активация файла с конфигурацией)

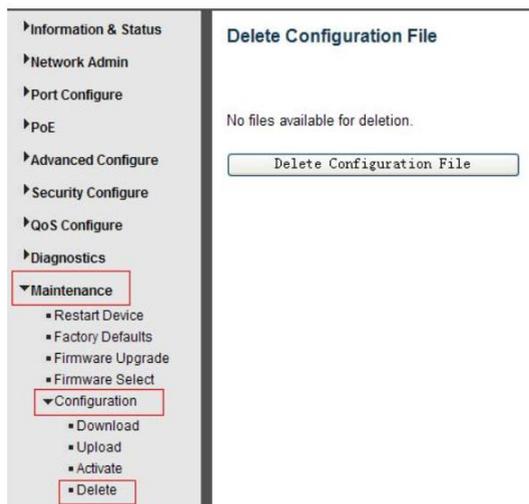
Maintenance > Configuration > Activate



Для активации нажмите кнопку «Activate Configuration»

8.10.5.4 Delete Configuration File (Удаление файла с конфигурацией)

Maintenance > Configuration > Delete



Для удаления файла с конфигурацией из коммутатора нажмите кнопку «Delete Configuration File»

9. Технические характеристики*

| Модель | SW-80402/WLU |
|--|---|
| Общее кол-во портов | 6 |
| Кол-во портов FE+PoE | - |
| Кол-во портов FE | - |
| Кол-во портов GE+PoE | 4 |
| Кол-во портов GE (не Combo порты) | - |
| Кол-во портов Combo GE (RJ45+SFP) | - |
| Кол-во портов SFP (не Combo порты) | 2 GE (1000Мбит/с) |
| Мощность PoE на один порт (макс.) | 30 Вт |
| Суммарная мощность PoE всех портов (макс.) | 120 Вт |
| Стандарты PoE | IEEE 802.3af IEEE 802.3at |
| Метод подачи PoE | Метод А 1/2(+), 3/6(-) |
| Встроенные оптические порты | - |
| Топологии подключения | звезда каскад кольцо |
| Буфер пакетов | 4 МБ |
| Таблицы MAC-адресов | 8 К |
| Пропускная способность коммутационной матрицы (Switching fabric) | 12 Гбит/с |
| Скорость обслуживания пакетов (Forwarding rate) | 1000 Мбит/с – 1488,000 пакетов/с 100 Мбит/с - 148,800 пакетов/с 10 Мбит/с- 14,880 пакетов/с |
| Поддержка jumbo frame | 9 КБ |
| Размер flash памяти | 128 МБ |

| Модель | SW-80402/WLU |
|-----------------------------|--|
| Стандарты и протоколы | <ul style="list-style-type: none"> • 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 |
| Функции уровня 2 | <ul style="list-style-type: none"> • 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 v1/v2/v3 • IGMP Static Multicast Addresses • Storm Control |
| Качество обслуживания (QoS) | <ul style="list-style-type: none"> • 8 очередей / порт |
| Безопасность | <ul style="list-style-type: none"> • Management System User Name/Password Protection • IEEE 802.1x Port-based Access Control • HTTP & SSL (Secure Web) • SSH v2.0 (Secured Telnet Session) |

| Модель | SW-80402/WLU |
|--------------------------------|---|
| Управление | <ul style="list-style-type: none"> • Управление через Web-интерфейс • CLI • Telnet • SNMP |
| Индикаторы | <ul style="list-style-type: none"> ✓ PWR1, ✓ PWR2, ✓ SYS, ✓ Link ✓ PoE |
| Грозозащита | 6 kV |
| Питание | AC 195-265V / 50 Гц |
| Резервное питание | набор свинцово-кислотных АКБ общей емкостью 2 Ач |
| Энергопотребление | <200 Вт (с учетом системы обогрева) |
| Термостабилизация / Охлаждение | Конвекционная (без вентилятора), с нагревательным элементом, мощностью 75 Вт |
| Класс защиты | IP66 |
| Размеры (ШхВхГ) (мм) | 300x400x187 |
| Способ монтажа | на стену, на опору |
| Рабочая температура | -50...+50 °С |
| Относительная влажность | 0-95% без конденсата |

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

10. Гарантия

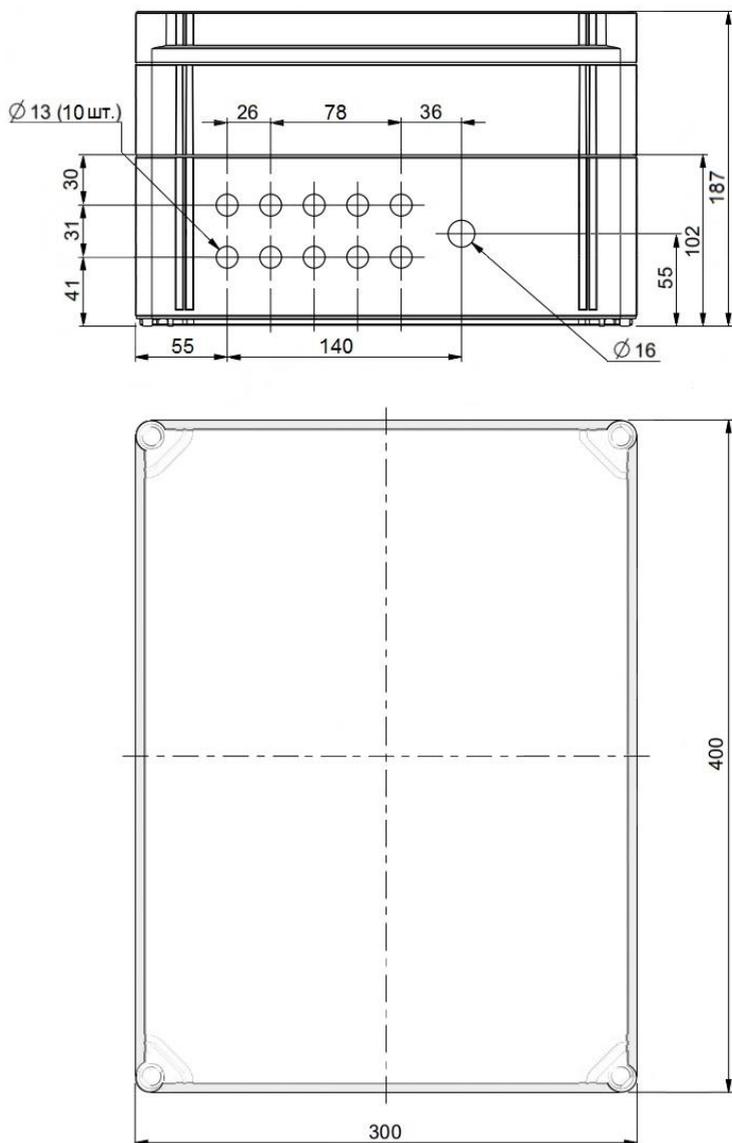
Гарантия на все оборудование OSNOVO – 60 месяцев с даты продажи, за исключением аккумуляторных батарей, гарантийный срок - 12 месяцев.

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 коммутатора»



* Все размеры даны в мм

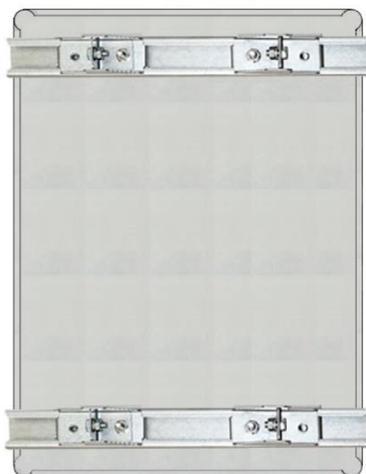
12. Приложение Б «Настенные крепления»

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.