OSNOVO
cable transmission

# РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

Управляемый (WEB managed) PoE коммутатор
Gigabit Ethernet на 28 портов

## SW-24G2C-M(200W)


Прежде чем приступать к эксплуатации изделия,
внимательно прочтите настоящее руководство

# Оглавление

# 1. Назначение

Управляемый (WEB managed) Gigabit Ethernet PoE коммутатор на 28 портов SW-24G2C-M(200W) предназначен для объединения сетевых устройств и передачи данных между ними по медным и оптическим кабелям.

Коммутатор оснащен 24мя портами Gigabit Ethernet (10/100/1000 Base-T) с поддержкой PoE к каждому из которых можно подключать сетевые устройства. Любой из портов с 1 по 4 способен запитывать PoE устройства с потреблением до 90Вт (IEEE 802.3bt). Остальные 20 портов рассчитаны на максимальную мощность до 30Вт (IEEE 802.3af/at). При этом общая выходная мощность на 24 порта (PoE бюджет) составляет 200Вт, что необходимо учитывать при подключении PoE устройств к каждому порту. Предусмотрено автоматическое определение подключаемых PoE устройств по стандартам IEEE 802.3af/at/bt.

Кроме того, в SW-24G2C-M(200W) предусмотрено 2 отдельных медных Gigabit Ethernet (10/100/1000 Base-T) Uplink порта и 2 Combo Uplink порта (SFP+RJ-45) для подключения коммутатора к локальной сети, сети Ethernet или другому коммутатору с помощью медных кабелей (Cat 5e/6/6a и т.д.) или по оптоволоконному кабелю (SFP модули не входят в комплект поставки).

Коммутатор конфигурируется через WEB-интерфейс (WEB managed) и имеет достаточное количество различных функций и настроек (контроль PoE на портах, VLAN, STP/RSTP/MSTP, работа с таблицей MAC адресов и т.д.)

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

Коммутатор SW-24G2C-M(200W) рекомендуется использовать, если есть необходимость объединить значительное количество сетевых устройств (например, IP-камеры, Wi-Fi точки доступа, IP-телефоны и пр.) в одну сеть и передать к ним питание по кабелю витой пары (PoE).

Коммутатор данной модели с успехом может быть применен на различных объектах, в офисе, в системе видеонаблюдения и т.д.

## 2. Комплектация*

1. Коммутатор – 1шт;
2. Кабель питания для AC 100-240V – 1шт;
3. Руководство по эксплуатации –1шт;
4. Крепление в 19” стойку – 1шт;
5. Упаковка – 1шт.

## 3. Особенности оборудования

- 24 Gigabit Ethernet (10/100/1000Base-T) портов с PoE;
- 1-4 порты поддерживают PoE до 90Вт (IEEE 802.3bt), 5-24 порты – до 30Вт (IEEE 802.3af/at);
- Общий бюджет PoE – 200Вт;
- 2 Gigabit Ethernet (10/100/1000 Base-T) Uplink порта;
- 2 Gigabit Ethernet Combo порта (SFP+RJ-45) для подключения по медному или оптоволоконному кабелю;
- Управление параметрами через WEB интерфейс (WEB Managed);
- Поддержка конфигурирования ряда функций через WEB (VLAN, IGMP, LACP, PoE Settings, SNMP и т.д.);
- Поддержка кольцевой топологии подключения (протоколы STP/RSTP/MSTP);
- Встроенная грозозащита 6 кВ (8/20мс);
- Питание от сети AC 100-240V.

# 4. Внешний вид и описание элементов коммутатора

## 4.1 Внешний вид


Рис.1 Коммутатора SW-24G2C-M(200W), внешний вид

## 4.2 Описание разъемов и индикаторов коммутатора

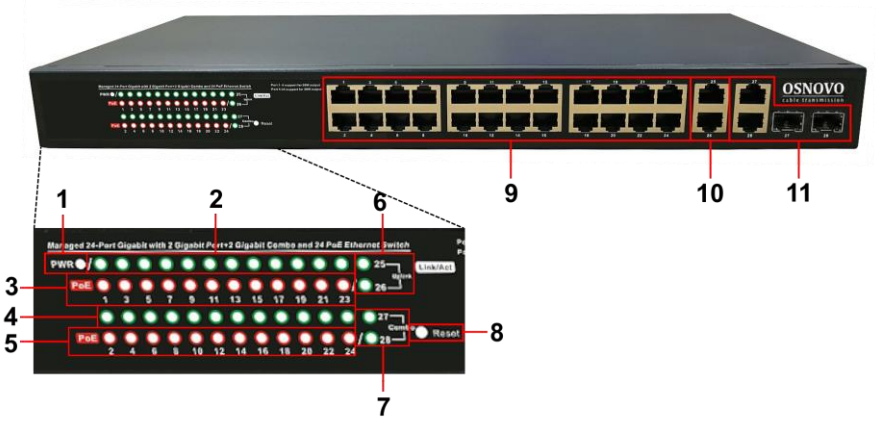



Рис.2 Коммутатор SW-24G2C-M(200W), разъемы, кнопки и индикаторы на передней панели

Таб.1 Коммутатор SW-24G2C-M(200W), назначение разъемов и индикаторов на передней панели

| № п/п | Обозначение | Назначение |
|---|---|---|
| 1 | PWR | *LED индикатор питания*<br><br>Горит зеленым – питание подается, коммутатор включен.<br><br>Не горит – питание отсутствует. Проверьте подключение комплектного кабеля. |

| № п/п | Обозначение | Назначение |
|---|---|---|
| 2 | 1 3 5 7 9 11 13<br>15 17 19 21 23 | *LED индикаторы линка и сетевой активности соответствующих портов*<br>Горит зеленым – подключено устройство<br>Мигает зеленым – идет передача данных.<br>Не горит – порт не используется. Проверьте подключение. |
| 3 | PoE<br>1 3 5 7 9 11 13<br>15 17 19 21 23 | *LED индикаторы PoE соответствующих портов*<br>Горит красным – подключено PoE устройство.<br>Не горит – подключено устройство без PoE или питание PoE не подается (неисправность). |
| 4 | 2 4 6 8 10 12<br>14 16 18 20 22 24 | *LED индикаторы линка и сетевой активности соответствующих портов*<br>Горит зеленым – подключено устройство<br>Мигает зеленым – идет передача данных.<br>Не горит – порт не используется. Проверьте подключение. |
| 5 | PoE<br>2 4 6 8 10 12<br>14 16 18 20 22 24 | *LED индикаторы PoE соответствующих портов*<br>Горит красным – подключено PoE устройство.<br>Не горит – подключено устройство без PoE или питание PoE не подается (неисправность). |

| № п/п | Обозначение | Назначение |
|---|---|---|
| 6 | 25 26<br>Uplink | *LED индикаторы линка и сетевой активности Uplink портов 25, 26*<br>Горит зеленым – подключено устройство<br>Мигает зеленым – идет передача данных.<br>Не горит – порт не используется. Проверьте подключение. |
| 7 | 27 28<br>Combo | *LED индикаторы линка и сетевой активности Combo (SFP+RJ-45) портов 27, 28*<br>Горит зеленым – подключено устройство<br>Мигает зеленым – идет передача данных.<br>Не горит – порт не используется. Проверьте подключение. Если используется SFP – проверьте характеристики SFP модуля. |
| 8 | Reset | *Микрокнопка.*<br>Предназначена для сброса коммутатора к заводским настройкам. |
| 9 | 1-24 | *Разъемы RJ-45 с 1 по 24й*<br>Предназначены для подключения сетевых устройств на скорости 10/100/1000 Мбит/с и запитывания их по технологии PoE.<br>1-4 порт PoE до 90Вт<br>5-24 порты PoE до 30Вт |

| № п/п | Обозначение | Назначение |
|---|---|---|
| 10 | 25, 26 | *Разъемы RJ-45*<br><br>Предназначены для подключения (Uplink порты) коммутатора к сети/другим коммутаторам и устройствам на скорости 10/100/1000 Мбит/с. |
| 11 | 27, 28 | *Разъемы RJ-45 и SFP порты*<br><br>Предназначены для подключения коммутатора к медной (порты RJ-45, кабель Cat 5/5e/6) или оптоволоконной (порты SFP, с помощью SFP модулей) линии связи на скорости 1000 Мбит/с. Одновременно может быть задействован либо RJ-45, либо SFP порты. |


Рис.3 Коммутатор SW-24G2C-M(200W), разъемы, кнопки и индикаторы на передней панели

Таб.2 Назначение разъемов и индикаторов коммутатора SW-24G2C-M(200W)

| № п/п | Обозначение | Назначение |
|---|---|---|
| 1 |  | *Кнопка включения/выключения коммутатора* |
| 2 | | *Разъем для установки/замены предохранителя* |
| 3 | AC/IN<br>100-240V | *Разъем (UAC)*<br>Используется для запитывания коммутатора от сети переменного тока AC 100-240V с помощью комплектного кабеля. |
| 4 |  | *Винтовая клемма*<br>Предназначена для заземления корпуса коммутатора. |

# 5. Подключение

## 5.1 Схема подключения

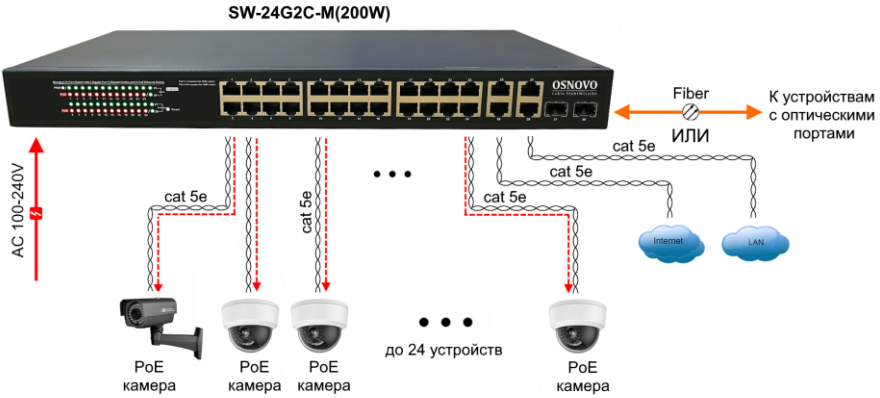



Рис.4 Типовая схема подключения коммутатора SW-24G2C-M(200W)

### 5.2 Подключение питания


Рис.5 Подключение коммутатора к сети переменного тока AC 220V

1) Подключите клемму заземления (1) корпуса коммутатора к контуру заземления.
2) Подключите коммутатор к сети переменного тока AC 230V с помощью комплектного кабеля (2)
3) Включите переключатель (3) в положение «вкл»
4) Коммутатор готов к работе!

**Внимание!**

*Для правильного функционирования системы грозозащиты на портах корпус коммутатора должен быть надежно заземлен.*

## 6. Проверка работоспособности системы

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

Подключите коммутатор к двум ПК с известными IP-адресами, располагающимися в одной подсети, например, 192.168.1.2 и 192.168.1.3

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

**ping 192.168.1.3**

Если все подключено правильно, на экране монитора отобразится ответ от второго компьютера (рис. 6). Это свидетельствует об исправности коммутатора.

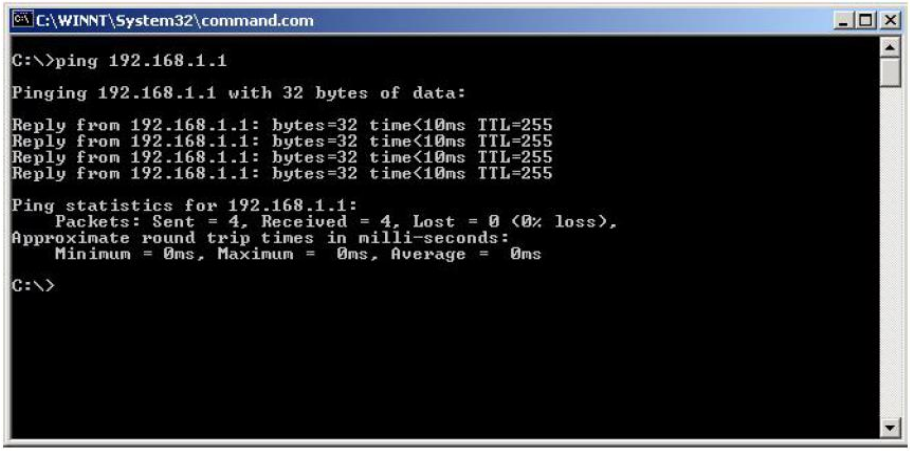



Рис. 6 Данные, отображающиеся на экране монитора, после использования команды Ping.

Если ответ ping не получен («Время запроса истекло»), то следует проверить соединительные кабели и корректность введенных IP-адресов компьютеров.

Если не все пакеты были приняты, это может свидетельствовать:

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

**Примечание**.

Потеря сигнала при передаче по ВОЛС могут быть вызвана:

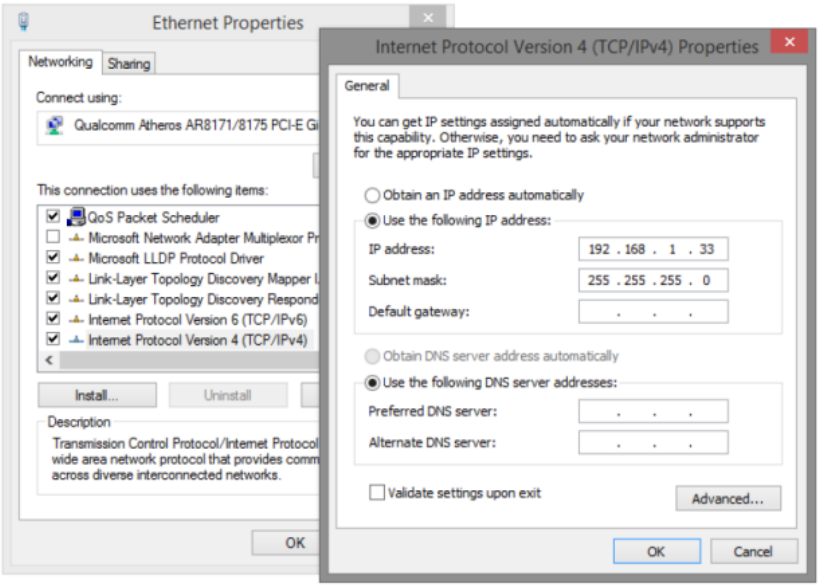
- неисправностью SFP-модулей;
- изгибами кабеля;
- большим количеством узлов сварки;
- неисправностью или неоднородностью оптоволокна.

# 7. Подготовка к управлению коммутатором через WEB-интерфейс

WEB-интерфейс позволяет гибко настраивать и отслеживать состояние коммутатора, используя Web браузеры.

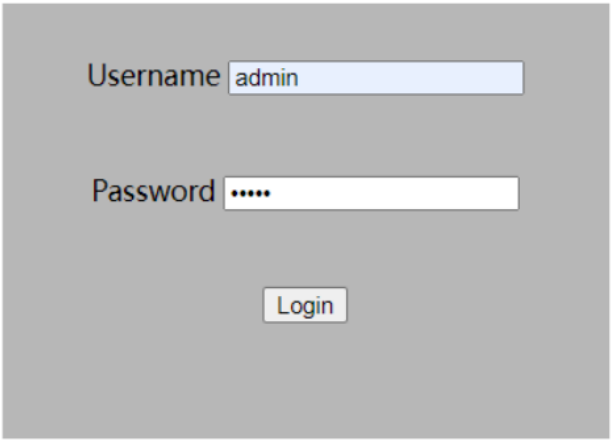
Прежде, чем приступить к настройке коммутатора через Web-интерфейс, необходимо убедиться, что ПК и коммутатор находятся в одной сети. Чтобы правильно сконфигурировать ПК:

1. Убедитесь, что сетевая карта в ПК установлена, работает и поддерживает TCP/IP протокол.
2. Подключите коммутатор к ПК, используя патч-корд с разъемами RJ45
3. По умолчанию IP-адрес коммутатора: **192.168.1.1.** Коммутатор и ПК должны находиться в одной подсети. Измените IP адрес ПК на 192.168.1.X, где X-число от 2 до 254. Пожалуйста, убедитесь, что IP-адрес, который назначаете ПК, не совпадал с IP-адресом коммутатора.




4. Запустите Web-браузер.

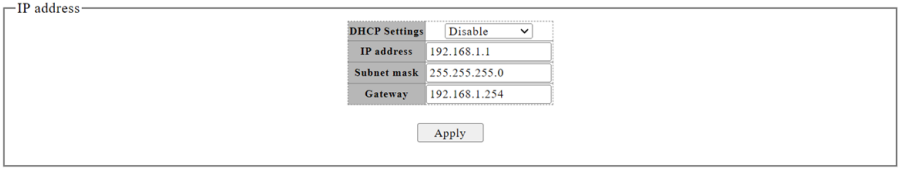
5. Введите в адресную строку **192.168.1.1** (IP-адрес коммутатора) и нажмите Enter на клавиатуре.
6. Появится форма аутентификации.
   По умолчанию логин: ***admin*.** Пароль: ***admin***.




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

*Вся подробная информация о настройках всех функций коммутатора представлена в полном руководстве, которое доступно к скачиванию на сайте www.osnovo.ru*

# 8. Изменение IP адреса коммутатора




Для изменения IP адреса коммутатора:

- Выполните вход в WEB интерфейс коммутатора;
- Перейдите в раздел System> IP Settings (Настройки IP);
- Установите DHCP Setting в положение Disable (откл);
- введите новый адрес в поле *IP address* (адрес должен быть уникальным и не должен повторяться);
- Введите маску подсети в поле Subnet Mask;
- Введите IP адрес шлюза (Gateway), если это необходимо;
- Нажмите кнопку Apply (принять настройки);
- ***Выполните повторный вход в WEB интерфейс, используя новый IP адрес.***

***Внимание!***

Для сохранения нового IP адреса в энергонезависимой памяти коммутатора необходимо перейти в раздел Tool > Save и нажать кнопку Save (сохранить), в противном случае при перезагрузке коммутатора будет установлен предыдущий IP адрес.

# 9. Настройка коммутатора через WEB интерфейс (WEB Managed)

## 9.1 Основные сведения

В руководстве ниже подробно описываются методы настройки функций программного обеспечения коммутатора. Перед началом работы внимательно ознакомьтесь с этим руководством. Руководство предназначено для пользователей, которые понимают и используют возможности данного WEB-интерфейса для управления сетью и возможностями коммутатора (Web managed).

В руководстве отображаются элементы WEB-интерфейса и функции/настройки программного обеспечения коммутатора.

*Обозначение последовательности меню*

- Для указания последовательности выбора пунктов меню используется символ >
- Формат: Главное меню > Меню первого уровня > Меню второго уровня.
- Некоторые функции могут не иметь меню второго уровня.

Названия кнопок и элементов интерфейса в тексте выделяются подчеркнутым жирным шрифтом

Примеры: **Apply** (применить), **Add** (добавить)

*Специальные значки и их описание*

| Значок | Назначение |
|---|---|
| Объяснение | Описание выполняемого действия, дополнительные пояснения и важные замечания. |
| ⚠ Внимание! | Предупреждение о мерах предосторожности. Несоблюдение может привести к потере данных или повреждению оборудования. |

## 9.2 Краткий обзор функций и настроек WEB управления

WEB интерфейс коммутатора позволяет гибко настраивать системные параметры, скорость портов, отслеживать состояние сети, управлять питанием PoE и пр.

Меню облегченного WEB интерфейса состоит из следующих разделов и подразделов:

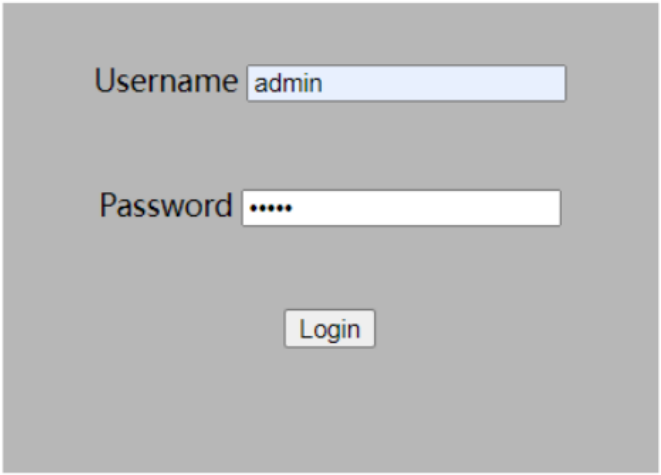
| Раздел меню WEB управления | Описание раздела и функций в нем |
|---|---|
| Главная страница (home page) | ✓ Отображение графической портов коммутатора;<br>✓ Отображение системной информации. |
| Базовые настройки (system) | ✓ Настройка IP адреса;<br>✓ Конфигурация портов;<br>✓ Управление учетными записями пользователей. |
| Конфигурация функции питания PoE (PoE) | ✓ Управление питанием PoE на портах коммутатора. |

| | |
|---|---|
| Настройки основных функций (Configure) | ✓ Настройка VLAN;<br>✓ Настройка QoS;<br>✓ Настройка IGMP Snooping:<br>✓ Настройка агрегации каналов (Link Aggregation);<br>✓ Настройка защиты от петель (Ring Road protection);<br>✓ Настройка протокола STP;<br>✓ Зеркалирование портов (Port mirror);<br>✓ Настройка изоляции портов;<br>✓ Контроль пропускной способности портов (bandwith control);<br>✓ Настройка Jumbo frame;<br>✓ Настройка MAC restrain;<br>✓ Настройка EEE;<br>✓ Настройка протокола SNMP. |
| Настройки безопасности (Security) | ✓ Работа с таблицей MAC адресов;<br>✓ Функция защиты от сетевых штормов (Storm Control). |
| Настройки мониторинга (Monitoring) | ✓ Статистика по портам |
| Различные инструменты обновления, диагностики и пр. (Tool) | ✓ Обновление прошивки;<br>✓ Резервное копирование конфигурации;<br>✓ Сброс к заводским настройкам;<br>✓ Сохранение текущей конфигурации;<br>✓ Перезагрузка коммутатора |

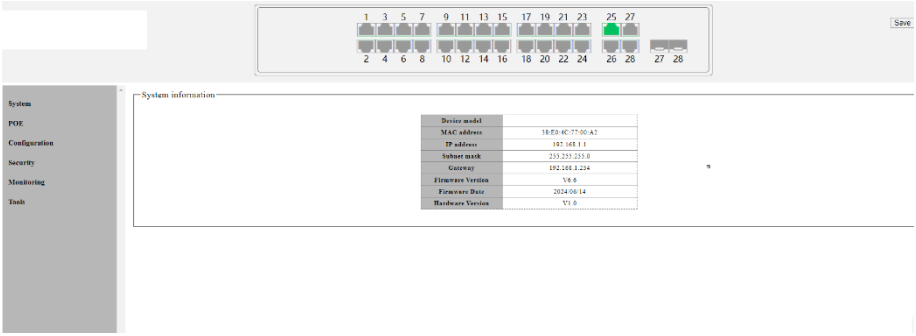
## 9.3 Вход в WEB-интерфейс коммутатора

Для успешного входа в веб-интерфейс управления коммутатором выполните следующие шаги:

1. Убедитесь, что коммутатор включён и работает нормально. Подключите порт коммутатора к сетевой карте компьютера, с которого будет производиться управление.
2. На управляющем ПК должен быть установлен один из следующих браузеров:
    - Internet Explorer версии 8.0 или выше
    - Последняя версия Google Chrome
3. Настройте сетевой интерфейс управляющего ПК *(это обеспечит нахождение ПК в той же подсети, что и порт коммутатора по умолчанию)*:
    - **IP-адрес:** 192.168.1.X (где X – любое целое число от **2** до **254**)
    - **Маска подсети:** 255.255.255.0
4. ⚠ Для оптимального отображения интерфейса рекомендуется установить разрешение экрана 1280x800 пикселей или выше.
5. Запустите браузер и в адресной строке введите IP-адрес коммутатора по умолчанию: http://192.168.1.1
6. Откроется страница входа
7. Введите имя пользователя и пароль учётной записи администратора. По умолчанию логин: **admin**. Пароль: **admin**.




*Структура главной страницы WEB интерфейса*

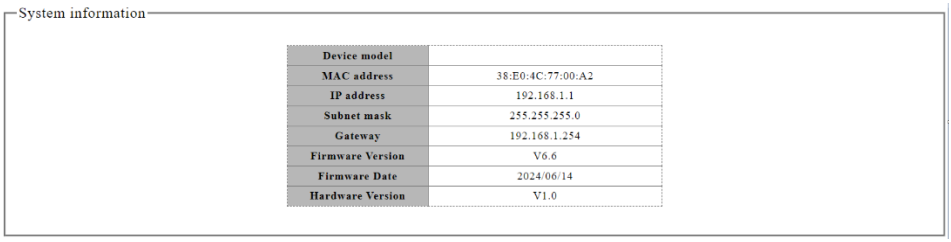



- **Левая навигационная панель** — содержит меню программного обеспечения.
- **Верхняя часть (справа)** – отображает **графическую панель состояния портов** устройства (количество портов зависит от модели коммутатора)
- **Нижняя часть (справа)** – содержит **основную системную информацию** (System Information).

## 9.4 Основная информация о коммутаторе (System Information)

На данной странице WEB интерфейса можно просмотреть информацию об устройстве и узнать его модель.

Для перехода в меню навигации перейдите: **System > System Information**




| Параметр | Описание |
|---|---|
| **Модель устройства (Device Model)** | Отображает модель коммутатора. |
| **MAC-адрес (MAC address)** | Показывает аппаратный (физический) адрес устройства. |
| **IP-адрес (IP address)** | Текущий IP-адрес, используемый для управления устройством. |
| **Маска подсети (Subnet mask)** | Маска подсети, связанная с IP-адресом управления. |
| **Шлюз по умолчанию (Gateway)** | IP-адрес шлюза по умолчанию для устройства. |
| **Версия прошивки (Firmware Version)** | Текущая версия системного программного обеспечения (ПО). |

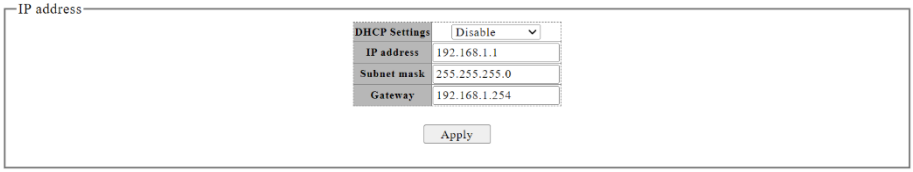
| Параметр | Описание |
| --- | --- |
| **Дата прошивки (Firmware Date)** | Дата сборки текущей версии прошивки. |
| **Аппаратная версия (Hardware Version)** | Ревизия (версия) аппаратной платформы устройства. |

***Примечания***

1. Изменение параметров сети:
    - 💡 Параметры IP-адрес, Маска подсети и Шлюз на данной странице, доступны только для просмотра.
2. Идентификация устройства:
    - 💡 MAC-адрес является уникальным идентификатором и используется при настройке функций безопасности (например, привязка порта к MAC).
    - 💡 Версия прошивки и аппаратная ревизия критически важны при обновлении ПО для выбора корректного файла прошивки.

## 9.5 Настройка IP адреса в WEB интерфейсе (IP set UP)

Для настройки IP адреса перейдите: **System > IP Settings**




***Параметры и их описание***

| Параметр | Описание |
|---|---|
| **Настройка DHCP (DHCP settings)** | **Включено (Enable)** – устройство автоматически получает сетевые параметры (IP, маску, шлюз) от сервера DHCP<br>**Выключено (Disable)** – позволяет задать параметры сети вручную. |
| **IP-адрес (IP Address)** | Задаёт статический IP-адрес коммутатору для управления. |
| **Маска подсети (Subnet mask)** | Задаёт маску подсети для статического IP-адреса. |
| **Шлюз по умолчанию (Default gateway)** | Задаёт IP-адрес шлюза по умолчанию. |

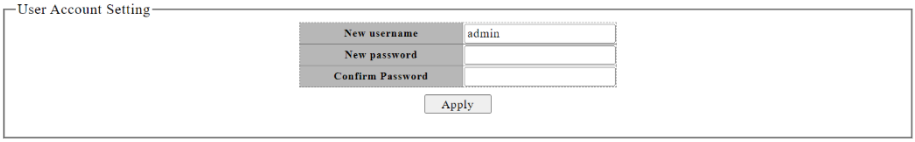
Кнопка **Apply** (Применить) отвечает за сохранение настроек на этой странице.

***Примечания***

1. 💡 **Выбор режима DHCP**:
    - **Ручная настройка (Disable)** рекомендуется для стационарного сетевого оборудования (коммутаторов, маршрутизаторов) для гарантии постоянного доступа по адресу управления.
    - **DHCP (Enable)** удобен при временном подключении или в сетях с централизованным управлением адресами (через маршрутизатор). Запомните или закрепите выданный адрес за устройством на DHCP-сервере.
2. 💡 **Важность шлюза**:
    - Шлюз по умолчанию необходимо указывать, если управляющий ПК находится в другой подсети. Для управления в пределах одной подсети это поле можно оставить пустым.
3. 💡 **Применение настроек**:
    - После сохранения настроек соединение с WEB-интерфейсом коммутатора **может прерваться**, если вы изменили IP-адрес на значение из другой подсети.
    - Для восстановления доступа потребуется настроить IP-адрес управляющего ПК соответствующим образом или переподключиться по новому адресу.

## 9.6 Изменение настроек авторизации пользователей (User Settings)

Для изменения логина и пароля для учетной записи пользователя перейдите в следующий раздел: **System > User Account**




| Параметр | Описание |
|---|---|
| **Имя пользователя (User name)** | Задаёт имя пользователя для входа в коммутатор.<br>• **Ограничения:** не более 16 символов.<br>• **Допустимые символы:** цифры (0-9), английские буквы (a-z, A-Z), символ подчёркивания (_). |
| **Новый пароль (New password)** | Устанавливает новый пароль для входа в коммутатор.<br>• **Ограничения:** не более 16 символов.<br>• **Допустимые символы:** цифры, английские буквы, символ подчёркивания. |
| **Подтвердите пароль (Confirm password)** | Повторный ввод нового пароля для проверки и подтверждения. Пароли должны совпадать. |

Кнопка **Apply** (Применить) отвечает за сохранение настроек на этой странице.

***Примечания***

1. 💡 **Безопасность пароля**:
    - Несмотря на ограничения системы, рекомендуется использовать сложные пароли, комбинируя буквы разных регистров и цифры.
    - Избегайте очевидных паролей по умолчанию (например, `admin`).
2. ⚠️ **Критически важный порядок действий**:
    - **После смены пароля необходимо полностью обновить страницу веб-интерфейса (нажать F5 или Ctrl+F5).**
    - **Не пытайтесь снова изменить пароль до обновления страницы.** Это может привести к конфликту сессии и блокировке.
3. 💡 **Учётные данные по умолчанию**:
    - Заводские значения по умолчанию для большинства моделей: **Имя пользователя:** `admin`, **Пароль:** `admin`.
    - Настоятельно рекомендуется изменить их при первом входе в систему.

После нажатия **Apply** (Применить) выполните обязательный шаг:

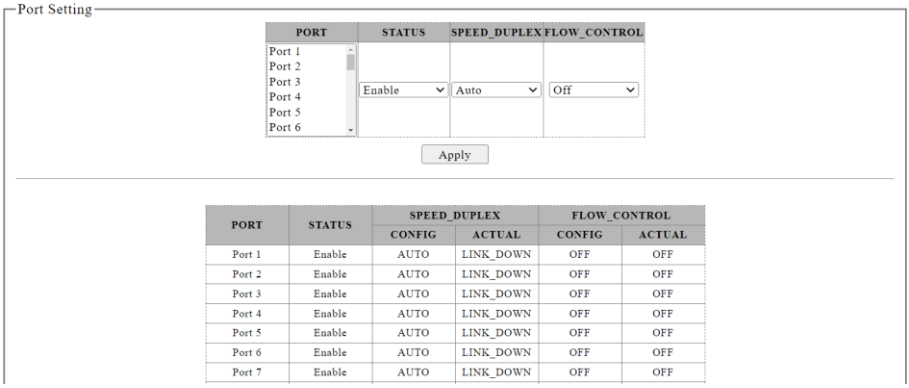
1. **Обновите страницу браузера**.
2. Войдите заново, используя новые учётные данные.

## 9.7 Настройка портов (Port Settings)

В этом разделе можно изменить параметры портов (состояние, скорость/дуплекс и контроль потока)

Для перехода в данный раздел в меню навигации выберите:

**System > Port Settings**




| Параметр | Описание |
|---|---|
| Port | Номер порта |
| **Status (состояние порта)** | **Включить (Enable)** – порт активен и может передавать кадры<br>**Выключить (Disable)** – порт отключён, трафик не обрабатывается |

| Параметр | Описание |
|---|---|
| **Скорость/Дуплекс (Speed / Duplex)** | Режим работы порта:<br>• **10M/Half** – 10 Мбит/с, полудуплекс.<br>• **10M/Full** – 10 Мбит/с, полный дуплекс<br>• **100M/Half** – 100 Мбит/с, полудуплекс.<br>• **100M/Full** – 100 Мбит/с, полный дуплекс.<br>• **Auto** (рекомендуется) – скорость и дуплекс согласуются автоматически (Auto-Negotiation) |
| **Контроль потока (Flow Control)** | **Включить (Enable)** – активирует механизм IEEE 802.3x для предотвращения переполнения буферов<br>**Выключить (Disable)** – отключает контроль потока |

Кнопка **Apply** (Применить) отвечает за сохранение настроек на этой странице.

***Примечания***

1. **Рекомендации по настройке скорости/дуплекса**:
    - **Автосогласование (Auto)** является оптимальным режимом для большинства сценариев. Позволяет портам автоматически выбрать наилучшие общие параметры.
    - **Ручная настройка** требуется только для подключения к устаревшему оборудованию, не поддерживающему автосогласование, или для устранения

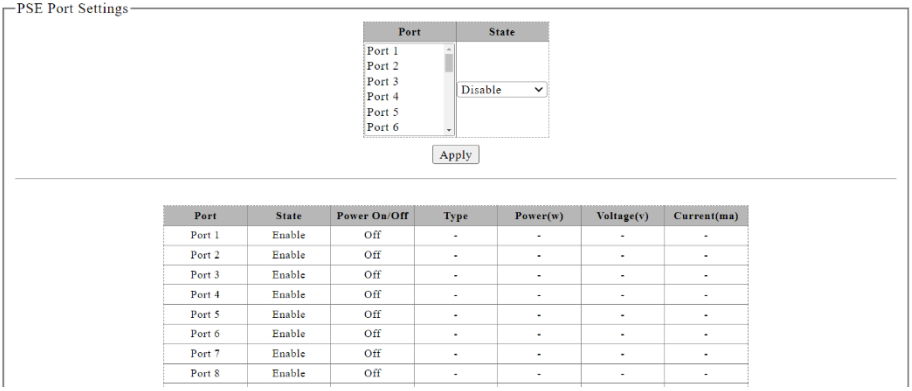
неполадок. **Убедитесь, что настройки совпадают на обоих концах кабеля.**

2. 💡 **Особенности контроля потока (Flow Control)**:
   - Функция **реально работает только в полудуплексном режиме (Half-Duplex)**. В полнодуплексном режиме стандартный контроль потока (802.3x) может не иметь эффекта или должен поддерживаться явно обоими устройствами.
   - Включайте, если наблюдаются потери пакетов из-за временной перегрузки порта, например, при подключении к серверу.
3. 💡 **Административное отключение порта**:
   - Используйте состояние **Disable** для отключения неиспользуемых портов в целях безопасности.

## 9.8 Настройка и управление PoE (PoE)

В этом разделе можно изменить параметры PoE для портов. Для перехода в данный раздел в меню навигации выберите:

**PoE > Port**



| Параметр | Описание |
|---|---|
| **Порты (Port)** | Позволяет выбрать один или несколько портов для настройки. |
| **Состояние (State)** | Управление подачей питания на порт:<br>• **Включить (Enable)** – разрешает подачу PoE на подключённое устройство (PD).<br>• **Выключить (Disable)** – отключает питание PoE на порту. |
| **Мощность (Power)** | Отображает текущую выходную потребляемую мощность на порту (в Ваттах). |
| **Напряжение (Voltage)** | Отображает текущее напряжение питания, подаваемое портом PSE (в Вольтах). |
| **Ток (Current)** | Отображает текущую силу тока, потребляемую устройством (PD) на порту (в миллиамперах). |

Кнопка **Apply** (Применить) отвечает за сохранение настроек на этой странице.

***Примечания***

1. 💡 **Безопасность и управление питанием**:
    - Используйте состояние **Disable** для принудительного отключения питания на порту (например, для перезагрузки подключённого устройства или в целях безопасности).
    - Включение состояния **Enable** разрешит коммутатору автоматически подать питание, если подключено совместимое устройство (PD).
2. 💡 **Мониторинг параметров**:
    - Поля **Мощность, Напряжение, Ток** предназначены только для **отображения** текущих значений и помогают контролировать энергопотребление и исправность подключённых устройств.
    - Резкое увеличение мощности или тока может указывать на неисправность питаемого устройства.
3. 💡 **Ограничения мощности**:
    - Общая потребляемая мощность всех портов не должна превышать максимальную мощность блока питания коммутатора (см. тех. характеристики).
    - При нехватке бюджета мощности коммутатор может отключать питание на приоритетных портах

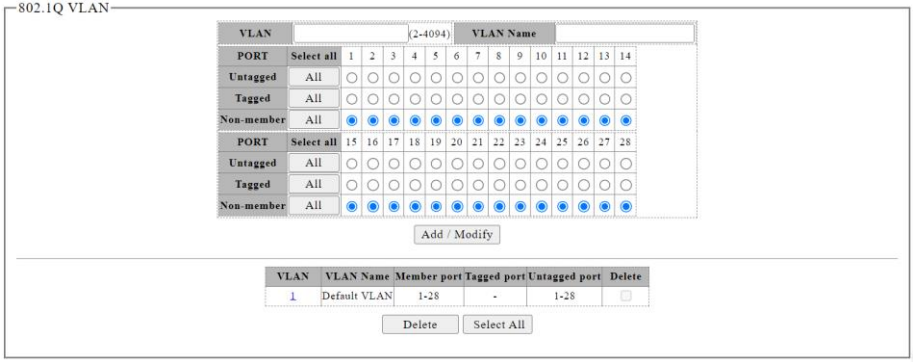
## 9.9 Настройка и управление VLAN (VLAN)

В этом разделе можно создать и настроить виртуальную локальную сеть – VLAN.

VLAN – это технология, которая логически разделяет одну физическую сеть (LAN) на несколько широковещательных доменов. Она добавляет в кадр данных специальный тег (VLAN ID), что позволяет логически сегментировать физическую сеть, ограничивая область распространения кадров.

Для перехода в данный раздел в меню навигации выберите:

**Configure > VLAN > 802.1Q VLAN**




| Параметр | Описание |
|---|---|
| **Идентификатор VLAN (VLAN)** | Выбор идентификатора для создаваемой VLAN от 2 до 4094 (VID 1 занят и не может быть удален/изменен). |
| **Имя VLAN (VLAN Name)** | В этом поле можно задать имя VLAN. |

| Параметр | Описание |
| --- | --- |
| Тип добавляемого в VLAN порта (PORT) | • **Untagged** – добавить порты к создаваемой VLAN и пометить их, как НЕтегированные. Обычно используется для подключения оконечных устройств (ПК, IP-телефоны), которые не понимают теги 802.1Q.<br>• **Tagged** – добавить порты к создаваемой VLAN и пометить их, как тегированные. Используется для соединения коммутаторов между собой (магистральные порты, trunk) или для подключения устройств, работающих с тегами.<br>• **Non-member** – по умолчанию порты находятся в этой категории и не принадлежат VLAN. Такие порты не будут передавать трафик этой VLAN |

Кнопка **Add/Modify** (Добавить/Изменить) отвечает за добавление портов в VLAN, а также изменения существующей VLAN из списка внизу страницы.

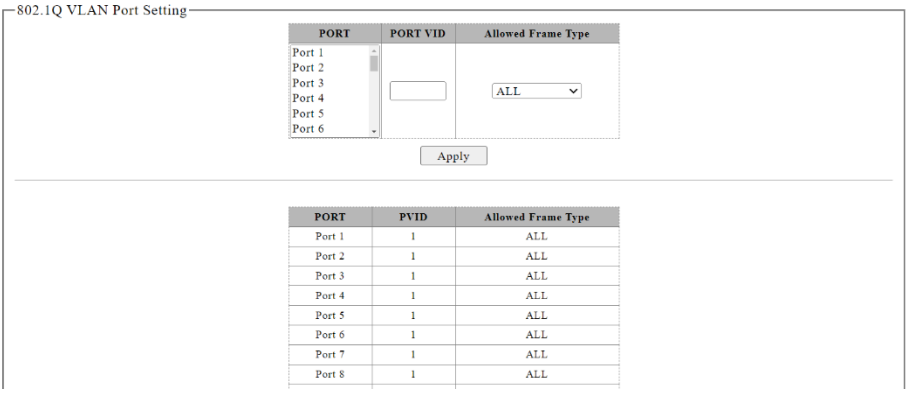
Кнопка **Delete** (Удалить) отвечает за удаление выбранного/выбранных VLAN.

💡 VLAN 1 удалить/изменить нельзя.

Кнопка **Select All** (Выбрать все) позволяет выбрать все доступные для удаления VLAN одним нажатием.

Для настройки PVID для портов перейдите в раздел:

**Configure > VLAN > 802.1Q PVID**




| Параметр | Описание |
|---|---|
| **Номер порта (PORT)** | Выбор физического порта коммутатора из списка. |
| **Идентификатор порта VLAN (PORT VID)** | Идентификатор VLAN по умолчанию для порта.<br>• Все **Untagged** кадры, пришедшие на этот порт, будут ассоциированы с VLAN, указанным здесь.<br>• Значение PVID должно быть предварительно создано в таблице Static VLAN (раздел **802.1Q VLAN)** |
| **Разрешенный тип кадров (Allowed Frame Type)** | ALL – все типы. |

***Примечания***

1. 💡 **Порядок настройки**:
    - **Сначала** создайте нужные VLAN в разделе **802.1Q VLAN**, указав для них **Tagged/Untagged** порты.
    - **Затем** в разделе **802.1Q PVID** для каждого порта укажите его **PVID**, который должен соответствовать **VLAN ID**, созданному на первом шаге.
2. 💡 **Разница между Untagged и Tagged**:
    - **Untagged:** "Нетегированный" режим. Устройство на другом конце кабеля получает "чистый" Ethernet-кадр.
    - **Tagged:** "Тегированный" режим. В кадр добавляется 4-байтовый тег 802.1Q с информацией о VLAN. Требует поддержки на обоих концах соединения.
3. 💡 **Назначение PVID**:
    - PVID – это **VLAN по умолчанию** для порта. Например, если PVID порта = 10, то компьютер, подключённый к этому порту, будет находиться в VLAN 10, даже если он отправляет обычные (untagged) кадры.

***Пример настройки VLAN для офиса:***

**1. Шаг (802.1Q VLAN):**

- Создаем VLAN 10:
    - **VLAN ID:** 10
    - **Untagged порты:** 1, 2, 3 (порты для 1 этажа)
    - **Tagged порты:** 8 (магистральный порт для связи с другим коммутатором)
- Создаем VLAN 20:
    - **VLAN ID:** 20
    - **Untagged порты:** 4, 5, 6 (порты для 2 этажа)
    - **Tagged порты:** 8 (магистральный порт)

**2. Шаг (802.1Q PVID):**

- **Порт GE1-3:** PVID = 10
- **Порт GE4-6:** PVID = 20
- **Порт GE24:** PVID = 1 (обычно для магистрального порта оставляют PVID по умолчанию, например, VLAN 1)

## 9.10 Настройка QoS (QoS)

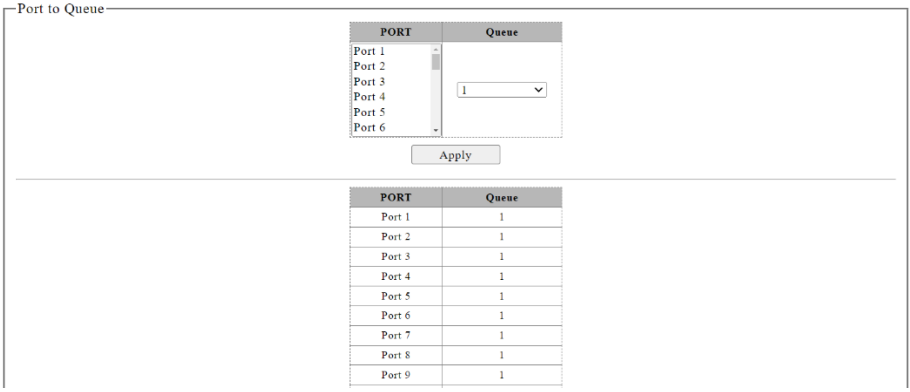
В этом разделе можно создать и настроить функцию QoS коммутатора, предназначенную для оптимизации производительности сети и предоставления более предсказуемого качества сетевых услуг за счёт управления очередями, задержками и потерями пакетов.

### 9.10.1 Привязка порта к очереди (Port to Queue)

Эта функция сопоставляет пакеты, поступившие на определённые физические порты, с одной из восьми внутренних очередей коммутатора. Каждая очередь имеет свой приоритет обработки.

Для перехода в данный раздел в меню навигации выберите:

**Configure > QoS > Port to Queue**



| Параметр | Описание |
| --- | --- |
| **Порт (Port)** | Физический порт коммутатора, для которого настраивается приоритет. |
| **Уровень очереди (Queue Level)** | Номер внутренней очереди (от 0 до 7), в которую будут помещены все пакеты, поступившие на данный порт (если не заданы другие правила).<br>• Чем выше номер очереди (например, 7), тем выше приоритет.<br>• Чем ниже номер очереди (например, 0), тем ниже приоритет. |

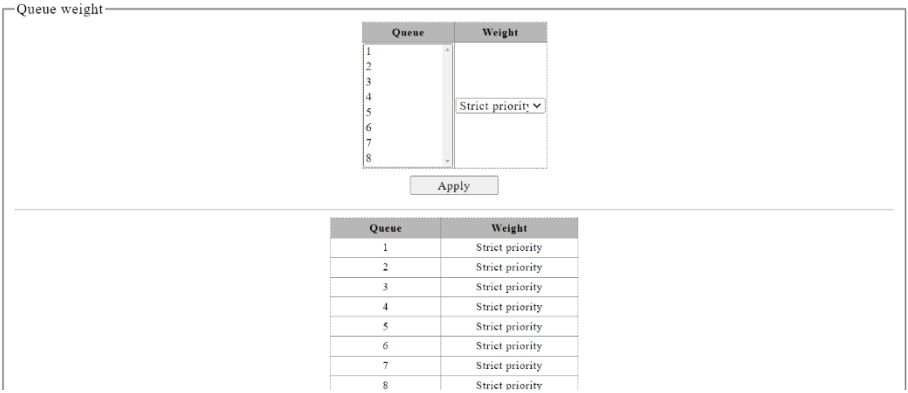
Кнопка **Apply** (Применить) отвечает за сохранение настроек на этой странице.

### 9.10.2 Вес очереди (Queue Weight)

Эта функция настраивает алгоритм взвешенного планирования (например, Weighted Round Robin – WRR) для распределения пропускной способности между восемью очередями. Вес определяет, какую долю доступной полосы пропускания получит каждая очередь при наличии конкурирующего трафика.

Для перехода в данный раздел в меню навигации выберите:

**Configure > QoS > Queue Weight**




| | |
|---|---|
| **Номер очереди (Queue)** | Идентификатор внутренней очереди (от **0** до **7**). |
| **Вес (Weight)** | Значение веса очереди.<br>• **Диапазон:** обычно от 1 до 255.<br>• **Принцип работы:** Пропорция полосы пропускания, выделяемая для очереди, вычисляется как её вес, делённый на сумму весов всех активных очередей.<br>• Чем **выше** вес, тем **больше** полосы пропускания получит трафик из этой очереди.<br>Strict Priority – прямой приоритет, где 8 – максимальный, 0 – минимальный |

Кнопка **Apply** (Применить) отвечает за сохранение настроек на этой странице.

***Примечания***

1. 💡 **Стратегия совместного использования Port-to-Queue и Queue Weight**:
    - **Port to Queue** – это классификация на входе. Она определяет, в какую очередь изначально попадут все пакеты с конкретного порта.
    - **Queue Weight** – это политика выходного планирования. Она определяет, с какой интенсивностью пакеты из каждой очереди будут передаваться в линию.
2. 💡 **Рекомендации по настройке приоритета портов (Port to Queue)**:
    - Назначьте портам, к которым подключены критически важные сервисы (IP-телефония, видеоконференции), высокий номер очереди (например, 6 или 7)**.**
    - Для портов с обычным пользовательским трафиком используйте низкие номера очередей (0-3)**.**
    - Порт для резервного копирования данных можно назначить в очередь 0 с минимальным приоритетом.
3. 💡 **Рекомендации по настройке весов очередей (Queue Weight)**:
    - Настройка имеет смысл только при включённой функции QoS и наличии конкуренции за полосу пропускания.
    - Пример распределения для 4 очередей: очередь 7 (голос) – вес 50, очередь 6 (видео) – вес 30, очередь 1 (данные) – вес 15, очередь 0 (фоновый) – вес 5. Это гарантирует, что голосовой трафик получит наибольшую долю полосы.

***Пример настройки для офиса:***

**1. Port to Queue:**

- **1 (IP-телефон):** Уровень очереди = 7 (Высший приоритет)
- **2 (Видеосервер):** Уровень очереди = 6 (Высокий приоритет)
- **3-7 (Пользовательские ПК):** Уровень очереди = 1 (Низкий приоритет)
- **8 (Резервное копирование):** Уровень очереди = 0 (Самый низкий приоритет)

**2. Queue Weight (Вес очереди):**

- **Очередь 7:** Вес = 60 (для голоса)
- **Очередь 6:** Вес = 30 (для видео)
- **Очередь 1:** Вес = 8 (для данных пользователей)
- **Очередь 0:** Вес = 2 (для фоновых задач)

*При активном трафике из всех очередей голос получит ~60% полосы, видео ~30%, данные ~8%, фоновый ~2%).*

## 9.11 Настройка IGMP Snooping (IGMP Snooping)

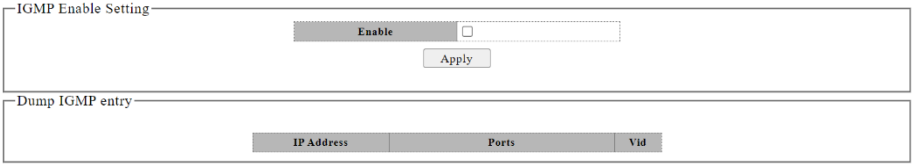
В этом разделе можно настроить работу протокола IGMP. IGMP Snooping – это механизм контроля многоадресного (multicast) трафика, работающий на устройствах второго уровня (коммутаторах). Он управляет и контролирует группы многоадресной рассылки.

Настройка Multicast VLAN позволяет добавить порты коммутатора в специальный VLAN для multicast трафика, так что пользователи из разных обычных VLAN могут совместно получать multicast-данные через этот единый multicast VLAN. При этом сам multicast-трафик передаётся только в пределах этого выделенного VLAN, что экономит

полосу пропускания. Поскольку multicast VLAN полностью изолирован от пользовательских VLAN, обеспечиваются как безопасность, так и гарантия полосы пропускания.

Для перехода в данный раздел в меню навигации выберите:

**Configure > IGMP Snooping**




| Параметр | Описание |
|---|---|
| **IGMP** | Глобальное включение или отключение функции IGMP Snooping на коммутаторе.<br>• **Enable** – активирует механизм IGMP Snooping<br>• **Disable** – отключает. |
| **IP-адрес (IP address)** | Отображает IP-адреса активных multicast-групп, на которые подписаны клиенты в сети. |
| **Порт (Port)** | Отображает список портов коммутатора, на которых находятся получатели для конкретной multicast-группы. |
| **VID** | Отображает идентификатор VLAN (**VLAN ID**), в котором существует и передаётся соответствующая multicast-группа. |

Кнопка **Apply** (Применить) отвечает за сохранение настроек на этой странице.

***Примечания***

1. 💡 **Назначение IGMP Snooping**:
    - Без IGMP Snooping коммутатор будет рассылать multicast-трафик на все порты в пределах широковещательного домена (VLAN), как обычный broadcast трафик, что ведёт к бесполезной нагрузке на сеть.
    - С включённым IGMP Snooping коммутатор "прослушивает" IGMP-сообщения между клиентами и маршрутизатором и направляет multicast-трафик только на те порты, где есть активные получатели
2. 💡 **Таблица отображения (IP, Port, VID)**:
    - Эта таблица является информационной (read-only) и динамически заполняется на основе работы протокола.
    - Она позволяет администратору видеть, какие multicast-потоки **(**IP-адрес**)** активны, в каком VLAN (VID) они находятся, и на какие порты они доставляются.

## 9.12 Агрегация каналов (Link Aggregation)

В этом разделе можно настроить работу механизма агрегации каналов LAG (также известный как Trunk). LAG – то метод объединения нескольких физических интерфейсов (портов) в один логический канал. Это позволяет увеличить:

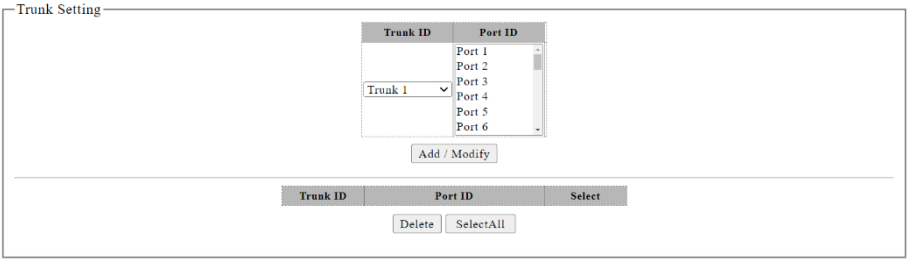
- Пропускную способность (сумма скоростей портов).
- Надёжность (отказоустойчивость – при выходе из строя одного физического линка трафик перенаправляется через оставшиеся).

Данную функцию следует использовать в следующих случаях:

- Когда пропускной способности одного физического соединения между двумя сетевыми устройствами недостаточно.
- Когда надёжность соединения через один канал не удовлетворяет требованиям.

Для перехода в данный раздел в меню навигации выберите:

**Configure > Trunk Settings**




| Параметр | Описание |
|---|---|
| **Идентификатор агрегированной группы (Trunk ID)** | Уникальный номер создаваемой или редактируемой агрегированной группы (trunk).<br>• Обычно доступно ограниченное количество групп (например, от 1 до 8). |
| **Порты (Port ID)** | Список физических портов, включаемых в агрегированную группу.<br>• Выбор осуществляется из списка доступных портов коммутатора. |

Кнопка **Add/Modify** (Добавить/Изменить) отвечает за добавление портов в Trunk, а также изменения существующей Trunk из списка внизу страницы.

Кнопка **Delete** (Удалить) отвечает за удаление выбранного/выбранных Trunk групп.

Кнопка **Select All** (Выбрать все) позволяет выбрать все доступные для удаления Trunk группы одним нажатием.

***Примечания***

⚠ Ключевое требование – единообразие настроек портов:

- Все физические порты, входящие в одну агрегированную группу, должны иметь идентичные настройки. Это включает:
  - ✓ Скорость и дуплекс (рекомендуется одинаковый ручной режим, например, 1G/Full, или Auto для всех).
  - ✓ VLAN членство (настройки PVID, Tagged/Untagged).
  - ✓ Состояние потока (Flow Control).
- Несоблюдение этого правила может привести к неработоспособности агрегированного канала.

💡 ***Рекомендации по использованию**:*

- Используйте агрегацию для соединения коммутатор-коммутатор (магистральные каналы) или коммутатор-сервер.
- Не включайте в одну группу порты, подключённые к разным устройствам.
- Убедитесь, что соседнее устройство поддерживает и корректно настроено для агрегации тем же методом.

## 9.13 Защита от петель (Loop Protection)

В этом разделе можно настроить работу механизма защиты от сетевых петель. Сетевая петля (Loop) – это топология, при которой соединения между коммутаторами образуют замкнутое кольцо. Появление петли в сети вызывает широковещательный шторм (broadcast storm), который потребляет значительные ресурсы процессора и полосу пропускания коммутаторов, что может привести к отказу оборудования и полному обрушению сети.

Для перехода в данный раздел в меню навигации выберите:

**Configure > Loop > Loop Protection**


| Параметр | Описание |
|---|---|
| **Интервал обнаружения (Detection Interval)** | Периодичность, с которой коммутатор отправляет тестовые кадры для мониторинга сети на наличие петель (в секундах). |
| **Время блокировки (Blocking Time)** | Длительность, на которую порт будет **блокирован (отключён)** после обнаружения на нём петли. По истечении этого времени порт автоматически переводится в нормальное состояние для проверки, устранена ли причина петли. |

Кнопка **Apply** (Применить) отвечает за сохранение настроек на этой странице.

***Примечания***

1. 💡 **Как работает механизм**:
    - Коммутатор периодически **(**Detection Interval**)** отправляет специальные пробные кадры (Loop Detection Frames).
    - Если коммутатор получает обратно свой же кадр, это означает наличие физической или логической петли в сети.
    - При обнаружении петли коммутатор блокирует порт, на котором был получен "возвращённый" кадр, на заданное время (Blocking Time).
2. 💡 **Рекомендации по настройке интервалов**:
    - Интервал обнаружения (Detection Interval): Значение от 5 до 10 секунд является хорошим балансом между скоростью реакции и нагрузкой на сеть. Более частые проверки увеличивают служебный трафик.
    - Время блокировки (Blocking Time): Рекомендуется устанавливать в диапазоне 30-60 секунд. Этого достаточно, чтобы администратор сети успел отреагировать на оповещение, но недостаточно для необратимых последствий. Слишком большое время может привести к длительным простоям порта.
3. 💡 **Отличие от STP**:
    - Эта функция (Loop Protection) является дополнением, а не заменой протоколов STP/RSTP/MSTP.
    - STP предупреждает появление петель, логически блокируя избыточные связи. Loop Protection – это механизм аварийного реагирования, который физически отключает порт при *фактическом* обнаружении шторма (например, если STP был отключен или не сработал).

💡 **Пример настройки:**

- Интервал обнаружения (Detection Interval): 7 (секунд)
- Время блокировки (Blocking Time): 45 (секунд)

Сценарий работы:

1. Коммутатор каждые 7 секунд отправляет тестовый кадр.
2. Если из-за петли кадр возвращается, порт-источник немедленно блокируется**.**
3. Порт остаётся в заблокированном состоянии 45 секунд, после чего автоматически включается**.**
4. Если причина петли не устранена, механизм снова обнаружит её и повторит блокировку.

## 9.14 Настройка протокола STP (Spanning Tree)

В этом разделе можно настроить работу семейства протоколов STP.

В сетях Ethernet для резервирования связей и повышения надёжности часто используются избыточные соединения. Однако это приводит к образованию петель (loops) в сети коммутации, что вызывает такие проблемы, как широковещательный шторм (broadcast storm) и нестабильность таблиц MAC-адресов. В результате ухудшается качество связи пользователей, вплоть до её полного прерывания.

Для решения проблемы петель был разработан протокол STP (Spanning Tree Protocol)**.** Как и многие другие протоколы, он развивался со временем:

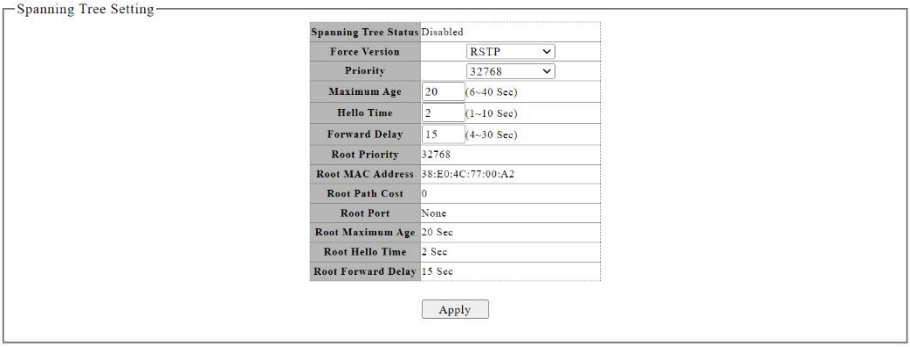
1. **STP** (стандарт IEEE 802.1D) – базовая, медленная версия.

2. **RSTP (Rapid STP)** (стандарт IEEE 802.1w) – быстрый STP с ускоренной сходимостью.
3. **MSTP (Multiple STP)** (стандарт IEEE 802.1s) – позволяет создавать несколько деревьев для разных VLAN, что повышает эффективность использования избыточных линий.

### 9.14.1 Глобальные настройки STP (STP Global)

Для перехода в данный раздел в меню навигации выберите:

**Configure > Loop > STP Global**




| Параметр | Описание |
|---|---|
| **Глобальное состояние STP (Spanning Tree Status)** | Глобальное включение/выключение (enabled/disabled) протокола STP/RSTP/MSTP на коммутаторе. |
| **Версия протокола (Force Version)** | Выбор типа протокола: **STP**, **RSTP** (рекомендуется) или **MSTP**. |

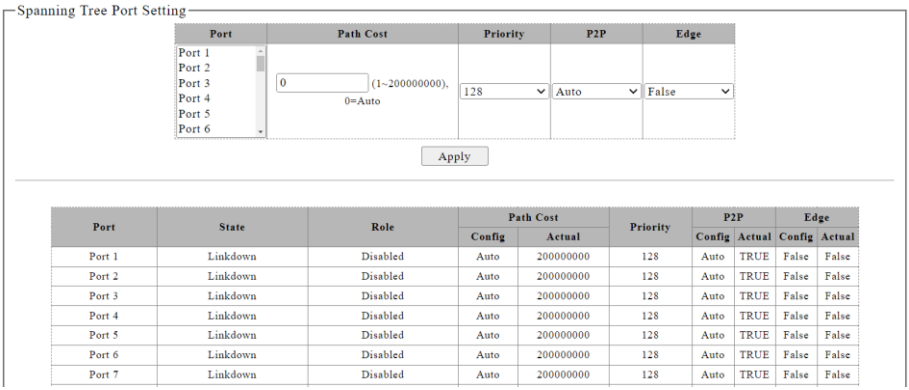
| Параметр | Описание |
|---|---|
| **Приоритет коммутатора (Priority)** | Числовое значение, определяющее приоритет этого коммутатора стать корневым мостом (Root Bridge). Чем меньше число, тем выше приоритет. |
| **Время хранения информации (Maximum Age)** | Максимальное время (в секундах), в течение которого коммутатор хранит информацию о топологии перед её обновлением. Диапазон от 6 – 40 сек. |
| **Hello Time** | Интервал (в секундах) между отправкой конфигурационных BPDU корневым мостом. Диапазон 1-10 сек. |
| **Forward Delay** | Время (в секундах), которое порт проводит в промежуточных состояниях Listening и Learning перед переходом в Forwarding. Диапазон от 4 до 30 сек. |

Кнопка **Apply** (Применить) отвечает за сохранение настроек на этой странице.

### 9.14.2 Настройки STP для портов (STP Port)

Для перехода в данный раздел в меню навигации выберите:

**Configure > Loop > STP Port**




| Параметр | Описание |
|---|---|
| **Порт (Port)** | Физический порт для настройки. |
| **Стоимость пути (Path Cost)** | Стоимость пути до корневого моста через этот порт. Чем меньше стоимость, тем предпочтительнее путь. |
| **Приоритет порта (Priority)** | Значение, влияющее на выбор назначенного порта (Designated Port). Чем меньше число, тем выше приоритет порта. |
| **Порт Point to Point (P2P)** | Подходит для full duplex каналов |

| Параметр | Описание |
| --- | --- |
| **Порт Edge (Edge)** | Порт может быстро переходить в состояние Forwarding |

Кнопка **Apply** (Применить) отвечает за сохранение настроек на этой странице.

***Примечания***

1. 💡 **Выбор версии протокола**:
    - **RSTP** является современным стандартом и настоятельно рекомендуется к использованию, так как он обеспечивает гораздо более быструю сходимость (восстановление связи) после изменений в топологии (1-2 секунды против 30-50 у STP).
    - **MSTP** используйте в сложных сетях с множеством VLAN, чтобы распределить трафик по разным деревьям и задействовать резервные каналы.
2. 💡 **Настройка корневого моста**:
    - ⚠ Всегда назначайте приоритет root bridge вручную (по умолчанию все приоритеты одинаковы).
    - Вручную назначьте наименьший приоритет (например, 4096) на основном, самом производительном коммутаторе в центре сети, чтобы он стал корневым.
3. 💡 **Оптимизация Edge Port**:
    - Для всех портов, к которым подключены **конечные устройства (ПК, серверы, IP-телефоны)**, включайте опцию **Edge Port**. Это позволяет им сразу переходить в состояние **Forwarding**, ускоряя подключение устройств и исключая задержки.

## 9.15 Зеркалирование портов (Port Mirroring)

В этом разделе можно настроить работу функции зеркалирования портов.

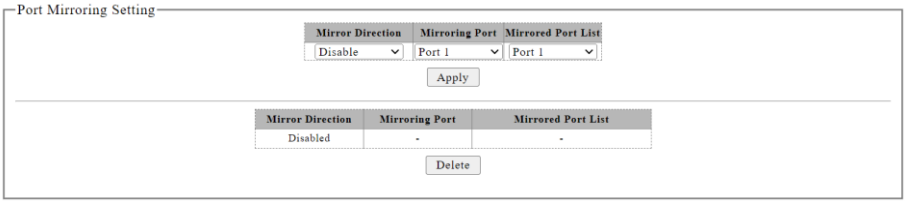
Зеркалирование портов (Port Mirroring) – это функция, при которой коммутатор создаёт копию пакетов с указанного порта (или портов) и направляет её на специальный порт-назначения (Destination Port).

- Порт, с которого копируются пакеты, называется исходным (Source Port).
- Порт, на который отправляются копии, называется портом-назначения (Destination Port) или зеркальным (Mirror Port).

К Mirroring Port подключается устройство для анализа трафика (например, анализатор пакетов, система обнаружения вторжений — IDS). Анализируя полученные копии пакетов, администратор может осуществлять мониторинг сети и устранять неполадки.

Для перехода в данный раздел в меню навигации выберите:

**Configure > Port-Based Mirroring**



| Параметр | Описание |
|---|---|
| **Направление зеркалирования (Mirror Direction)** | Указывает, какие пакеты с исходного порта копировать:<br>• **Disable** – зеркалирование отключено;<br>• **In (Ingress)** – только входящий трафик (поступающий на порт).<br>• **Out (Egress)** – только исходящий трафик (отправляемый с порта).<br>• **Both** – и входящий, и исходящий трафик. |
| **Исходный порт (Mirrored Port)** | Порт (или группа портов), трафик с которого будет копироваться. |
| **Порт-назначения (Mirroring Port)** | Порт, на который будут направляться копии пакетов. На этот порт подключается анализатор. |

Кнопка **Apply** (Применить) отвечает за сохранение настроек на этой странице.

***Примечания***

1. 💡 **Важные ограничения**:
    - Порт-назначения (**Mirroring Port**) не должен использоваться для передачи обычного трафика. Его единственная функция – передача зеркалированных данных для анализа.

- ⚠ **Нагрузка на порт-назначения может быть очень высокой.** Убедитесь, что пропускная способность этого порта (например, 1 Гбит/с) достаточна для обработки копий трафика с одного или нескольких исходных портов. В противном случае пакеты будут теряться.
- Зеркалирование обычно снижает общую производительность коммутатора**,** так как требует дополнительных ресурсов процессора (CPU)

2. 💡 **Выбор направления (Mirror Direction)**:
    - **In (Ingress):** Полезно для анализа трафика, адресованного конкретному серверу или устройству.
    - **Out (Egress):** Полезно для анализа трафика, исходящего от конкретного устройства (например, для выявления вирусов, рассылающих спам).
    - **Both:** Наиболее полный вариант для глубокой диагностики всех проблем, но создаёт максимальную нагрузку.
3. 💡 **Типовые сценарии использования**:
    - **Мониторинг сервера:** Назначьте порт сервера как Исходный порт (Mirrored Port) с направлением Both**,** а порт для анализа на ПК – как Порт-назначения (Mirroring Port)
    - **Безопасность:** Для анализа подозрительной активности зеркалируют порт, к которому подключена проблемная пользовательская VLAN.
    - **Диагностика сети:** Зеркалируют магистральный (uplink) порт**,** чтобы видеть весь трафик, проходящий через коммутатор.

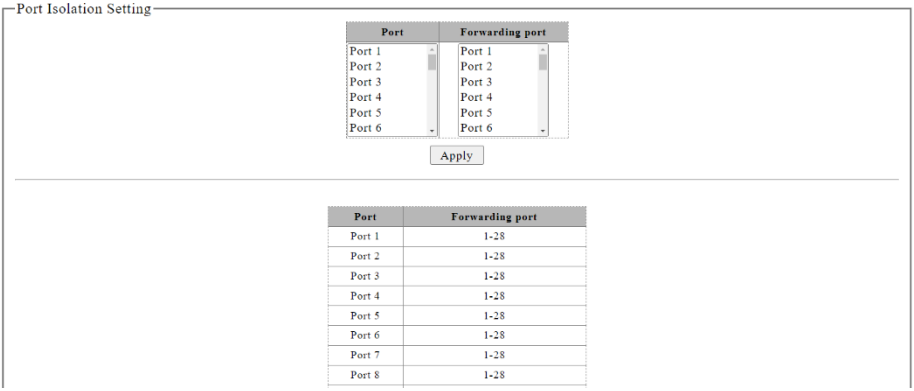
## 9.16 Изоляция портов (Port Isolation)

В этом разделе можно настроить работу функции изоляции портов.

Функция изоляции портов (Port Isolation) ограничивает передачу трафика между портами в пределах одного коммутатора, повышая безопасность и управление широковещательным доменом. Порты, помеченные как изолированные, могут обмениваться данными только с определёнными "общими" портами (обычно это порты восходящей связи), но не между собой.

Для перехода в данный раздел в меню навигации выберите:

**Configure > Port Quarantine**




| Параметр | Описание |
|---|---|
| **Порт (Port)** | Порт, который требуется изолировать. Этот порт будет иметь ограниченную возможность пересылки трафика. |
| **Порты для** | Список портов, на |

| Параметр | Описание |
| --- | --- |
| **пересылки (Forwarding Port)** | которые разрешена пересылка трафика с исходного выбранного порта. Пакеты, полученные на исходном порту, не могут быть отправлены на порты, не указанные в этом списке. |

Кнопка **Apply** (Применить) отвечает за сохранение настроек на этой странице.

***Примечания***

1. **Принцип работы**:
    - Функция Port Isolation создаёт односторонние или ограниченные правила пересылки на уровне коммутатора.
    - Пример: Если для порта 5 в качестве портов для пересылки указаны только 8 и 9, то компьютер, подключённый к порту 5, сможет общаться только с устройствами на портах 8 и 9. Он не сможет связаться с компьютером на порту 6, даже если они находятся в одном VLAN.
2. **Типовые сценарии использования**:
    - **Гостевые сети (Guest Wi-Fi):** Изолируйте порты, к которым подключены точки доступа гостевой сети, разрешив им пересылать трафик только на порт шлюза (Gateway) или порт в Интернет. Это предотвратит попадание гостей во внутреннюю корпоративную сеть.

- **Повышение безопасности внутри VLAN:** Даже внутри одного VLAN можно запретить прямым взаимодействие между пользовательскими портами, заставив весь трафик проходить через порт шлюза (где могут быть применены политики межсетевого экрана).

3. 💡 **Взаимодействие с другими функциями**:
    - Изоляция портов обычно применяется поверх конфигурации VLAN. Сначала трафик сегментируется по VLAN, затем внутри VLAN применяются правила изоляции.
    - ⚠ Убедитесь, что порты для пересылки (например, порт шлюза) находятся в том же VLAN, что и исходный (изолированный) порт, иначе пересылка на уровне L2 будет невозможна.

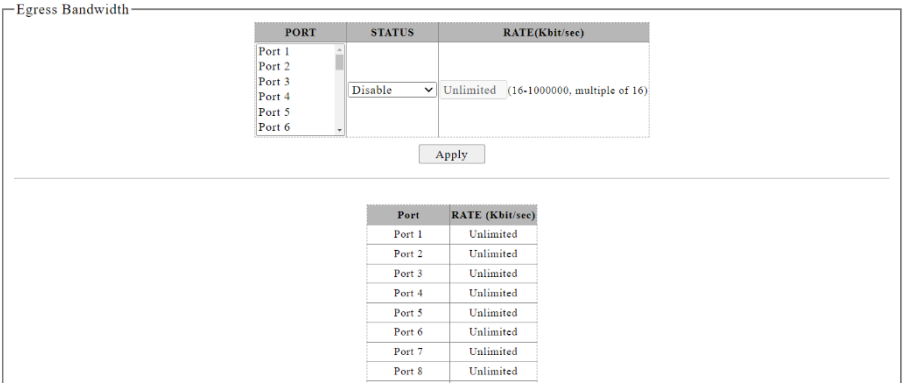
## 9.17 Контроль полосы пропускания (Bandwidth control)

В этом разделе можно настроить работу функции контроля пропускания.

Настройка контроля полосы пропускания (Bandwidth Control), также известная как политика скорости (Rate Limiting), позволяет ограничить скорость передачи данных на физическом интерфейсе

Для перехода в данный раздел в меню навигации выберите:

**Configure > Bandwidth control**




| Параметр | Описание |
|---|---|
| **Порт (Port)** | Физический порт, для которого настраивается ограничение скорости. |
| **Статус (Status)** | Включение или выключение (enable / disable) политики контроля для данного порта. |
| **Скорость (Rate Kbit/sec)** | Числовое значение ограничения скорости.<br>• В **Кбит/с (Kbps)** кратно 16 |

Кнопка **Apply** (Применить) отвечает за сохранение настроек на этой странице.

***Примечания***

1. 💡 **Тактика применения ограничений**:
    - **Ограничение входящего трафика (Ingress)** чаще используется для **защиты сети** от чрезмерного потребления ресурсов одним устройством (например, чтобы клиент не забил весь канал загрузками).

- **Ограничение исходящего трафика (Egress)** чаще используется для **гарантирования качества услуг (QoS)** или **распределения полосы** (например, чтобы поток данных с сервера не превышал заданный лимит и не мешал другим сервисам).

2. 💡 **Выбор значения скорости**:
   - При настройке в **Кбит/с** учитывайте реальную пропускную способность порта (100 Мбит/с, 1 Гбит/с). Нельзя установить значение выше физической возможности порта.

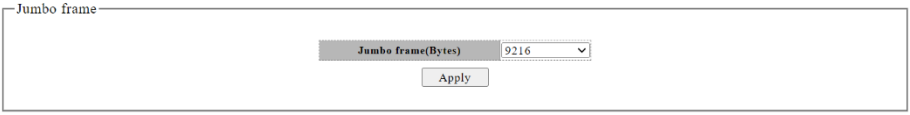
## 9.18 Настройка Jumbo фреймов (Jumbo Frame)

В этом разделе можно включить поддержку кадров большого размера (Jumbo Frame), а также задать их максимальный размер.

Функция Jumbo Frame позволяет настроить максимальную длину кадра (Maximum Transmission Unit – MTU), которую система может обрабатывать и пересылать. Стандартный Ethernet-кадр имеет размер 1518 байт (или 1522 байт с тегом VLAN). Jumbo Frame увеличивает этот лимит, что снижает расход производительности на обработку заголовков и повышает эффективность передачи больших объёмов данных.

Для перехода в данный раздел в меню навигации выберите:

**Configure > Jumbo Frame**



| Параметр | Описание |
|---|---|
| **Jumbo Frame (Bytes)** | Максимальный размер кадра Jumbo в байтах (не более 9216 байт) |

Кнопка **Apply** (Применить) отвечает за сохранение настроек на этой странице.

***Примечания***

1. 💡 **Для чего это нужно?**
    - **Повышение производительности:** Уменьшается соотношение заголовков к полезным данным. Это особенно эффективно для приложений с большими последовательными передачами, таких как резервное копирование (SAN, iSCSI), передача видео, передача multicast трафика, обработка больших данных**.**
    - **Снижение нагрузки на CPU:** Меньше кадров – меньше прерываний для обработки на сетевых картах и коммутаторах.
2. **Ключевое требование — сквозная поддержка:**
    - ⚠ **Jumbo Frame должна быть включена и настроена с одинаковым MTU на всех устройствах на пути трафика:** сетевая карта сервера, все коммутаторы, сетевая карта конечного получателя.
    - Если хотя бы одно устройство в пути не поддерживает Jumbo Frame или имеет меньший MTU, это приведёт к фрагментации пакетов или потере связи**.**

3. 💡 **Недостатки:**
    - Увеличенная задержка (latency) при передаче небольших пакетов из-за большего времени сборки кадра.
    - Риск увеличения потерь: один повреждённый Jumbo Frame означает потерю большего объёма данных, чем стандартный кадр.

## 9.19 Ограничение MAC (MAC Constraint)

В этом разделе можно включить политику ограничения изучения MAC адресов на портах.

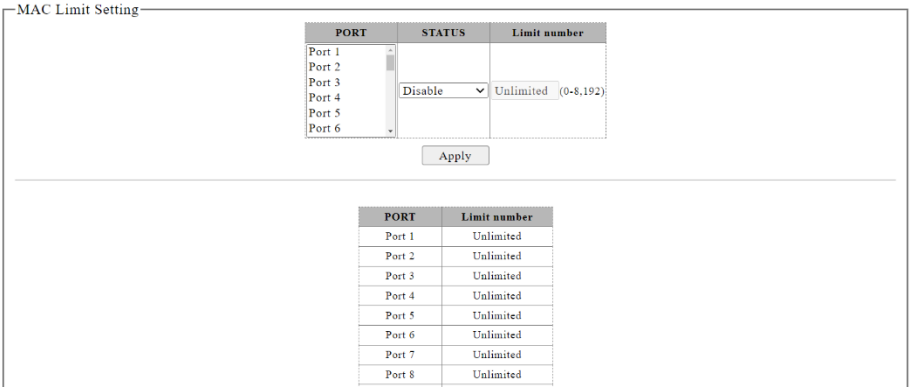
Коммутатор динамически изучает исходные MAC-адреса из поступающих кадров пользователя и сохраняет их в своей таблице MAC-адресов. Когда количество изученных адресов на порту достигает заданного порогового значения, применяется политика ограничения.

Принцип работы:

- Если исходный MAC-адрес из пользовательского кадра уже существует в таблице MAC-адресов коммутатора, кадр обрабатывается и пересылается как обычно.
- Если исходный MAC-адрес из кадра отсутствует в таблице MAC-адресов (т.е. это новый адрес), система обрабатывает кадр в соответствии с настроенной политикой ограничения (Action). Например, если действие – Отбросить (Discard), то кадр будет отброшен на входном порту.

Для перехода в данный раздел в меню навигации выберите:

**Configure > MAC Constrain**




| Параметр | Описание |
|---|---|
| **Порт (Port)** | Физический порт, для которого настраивается ограничение. |
| **Состояние (Status)** | Включение или отключение функции (enable/disable) ограничения MAC для данного порта. |
| **Лимит (Limit)** | Максимальное количество MAC-адресов, которые порт может выучить (запомнить в своей таблице). При достижении этого лимита активируется политика **Действие (Action)**.<br>• Диапазон: от 0 до 8192 |
| **Действие (Action)** | Политика обработки кадров с новыми (неизвестными) MAC-адресами при достижении лимита:<br>• **Отбросить (Discard)** – кадр уничтожается. |

| Параметр | Описание |
| --- | --- |
| | • **Заблокировать порт (Shutdown Port)** – порт полностью отключается.<br>• **Перенаправить (Redirect)** – кадр перенаправляется на указанный порт. |

Кнопка **Apply** (Применить) отвечает за сохранение настроек на этой странице.

***Примечания***

1. **Основная цель – безопасность и контроль:**
    - **Защита от атак MAC Flooding:** Злоумышленник может попытаться переполнить таблицу MAC-адресов коммутатора, отправляя кадры с поддельными MAC-адресами. При переполнении коммутатор может начать работать в режиме хаба (flooding трафика), что позволяет прослушивать трафик. Лимит предотвращает эту атаку.
    - **Ограничение числа устройств:** Позволяет гарантировать, что к одному порту (например, в общедоступной зоне) не будет подключено более N устройств (например, только 1 ПК).
2. **Рекомендации по настройке:**
    - Для **пользовательских портов (ПК, телефон)** установите лимит **1 или 2**. Этого достаточно для ПК с виртуальной машиной или телефона с ПК через гигабитный адаптер.

- Для **портов коммутатора (uplink)** или портов, к которым подключены **точки доступа Wi-Fi**, установите более высокий лимит (например, **32, 64, 128**), чтобы учесть всех клиентов Wi-Fi.
- Для **серверных портов** с виртуализацией (несколько виртуальных машин) установите лимит, равный или превышающий ожидаемое количество виртуальных MAC-адресов.

3. 💡 **Выбор действия (Action):**
    - **Discard** – наиболее безопасный и рекомендуемый вариант. Он просто блокирует трафик от новых устройств, не нарушая работу уже подключённых.
    - **Shutdown Port** – агрессивное действие, полезное для немедленного привлечения внимания администратора через систему оповещений (syslog, SNMP trap) при атаке.

## 9.20 Настройка Energy Efficient Ethernet (EEE)

В этом разделе можно включить поддержку стандарта IEEE 802.3az.

Energy-Efficient Ethernet (EEE) – это стандарт, позволяющий сетевым устройствам переходить в режим пониженного энергопотребления при низкой загрузке канала. Когда активность на линии отсутствует или невелика, обе системы на концах канала могут отключать часть своих функций, что приводит к значительной экономии электроэнергии без нарушения соединения.

Для перехода в данный раздел в меню навигации выберите:

**Configure > EEE**


| Параметр | Описание |
|---|---|
| EEE Function | Включение/выключение поддержки Energy Efficient Ethernet (802.3az) |

Кнопка **Apply** (Применить) отвечает за сохранение настроек на этой странице.

***Примечания***

1. 💡 **Принцип работы**:
    - При отсутствии передаваемых данных в течение короткого периода порт переходит в режим **Low Power Idle (LPI)**.
    - В этом режиме порт практически отключается, отправляя только периодические служебные сигналы для поддержания синхронизации и связи.
    - При появлении данных для передачи порт почти мгновенно (за микросекунды) возвращается в активное состояние.
2. 💡 **Требования для работы**:
    - ⚠ Для корректной работы **EEE должен поддерживаться и быть включён на обоих концах соединения** (например, на коммутаторе и на сетевой карте сервера/другого коммутатора).

- Функция поддерживается для стандартов скорости 100BASE-TX, 1000BASE-T, 10GBASE-T**.**

3. 💡 **Преимущества и недостатки**:
    - **Преимущество:** Существенная экономия энергии (до 50% и более на порт) в сетях с переменной или низкой нагрузкой (офисы ночью, резервные каналы).
    - **Недостаток/Особенность:** Может **незначительно увеличивать задержку (latency)** при переходе из спящего в активный режим. Это критично только для приложений, сверхчувствительных к задержкам (высокочастотный трейдинг, некоторые виды профессионального аудио).
4. 💡 **Рекомендации по настройке**:
    - **Включите (Enable)** EEE для всех пользовательских портов (ПК, телефоны, принтеры), где трафик носит импульсный характер.
    - **Включите (Enable)** EEE для магистральных портов (uplink) между коммутаторами, если они не постоянно загружены на 100%.
    - **Отключите (Disable)** EEE на портах, подключённых к:
        - Критически важным серверам с постоянным трафиком (экономия будет минимальна).
        - Оборудованию для задач в реальном времени, где важна минимальная и стабильная задержка.

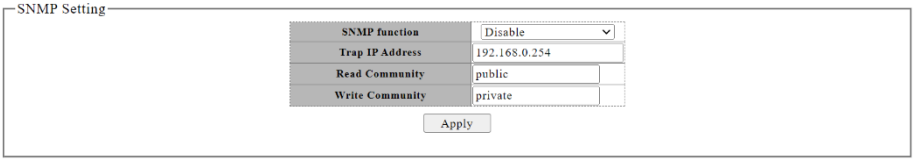
## 9.21 Настройка протокола SNMP (SNMP)

В этом разделе можно включить поддержку протокола SNMP

SNMP (Simple Network Management Protocol) – это стандартный протокол для управления устройствами в сетях TCP/IP. Он позволяет системе сетевого управления (NMS, Osnovo Monitoring System, Zabbix и т.д.) осуществлять мониторинг и управление любыми подключёнными к сети устройствами, которые его поддерживают.

Для перехода в данный раздел в меню навигации выберите:

**Configure > SNMP**




| Параметр | Описание |
|---|---|
| **SNMP Function (Протокол SNMP)** | Включение/выключение протокола SNMP и выбор версии.<br>• **v1** – устаревшая, минимальная безопасность.<br>• **v2c** – наиболее распространённая; использует community string для аутентификации.<br>• **v3** – современная; поддерживает шифрование и аутентификацию пользователей (может отсутствовать в данной модели) |
| **Trap IP Address** | IP адрес системы мониторинга NMS. |

| Параметр | Описание |
| --- | --- |
| **Read Community (Пароль для чтения)** | Строка сообщества для **чтения** (пароль). Используется системой управления NMS (Osnovo Monitoring System, Zabbix и т.д.) для запроса данных (GET) с устройства. По умолчанию public. |
| **Write Community (Пароль для записи)** | Строка сообщества для **записи** (пароль). Используется NMS (Osnovo Monitoring System, Zabbix и т.д.) для изменения настроек (SET) на устройстве. По умолчанию private. |

Кнопка **Apply** (Применить) отвечает за сохранение настроек на этой странице.

***Примечания***

1. 💡 **Безопасность**:
    - ⚠ **Никогда не оставляйте значения по умолчанию (**public**/**private**)** для строк сообщества в производственной сети. Используйте сложные строки, как пароли.
    - **SNMP v2c** не поддерживает шифрование, community string передаётся в открытом виде. Для безопасного управления используйте **SNMP v3** (если поддерживается).
2. 💡 **Для чего используется SNMP**:
    - **Мониторинг:** Сбор статистики по портам (загрузка, ошибки), состояния устройств (температура, напряжение), доступности (ping через SNMP).

- **Управление:** Дистанционное изменение некоторых настроек, сброс порта.
- **Оповещения:** Настройка **SNMP Trap** – устройство само отправляет сообщение на NMS (Osnovo Monitoring System, Zabbix и т.д.) о критических событиях (отключение порта, перегрев и т.д.).

3. 💡 **Настройка на стороне NMS**:
    - Для добавления коммутатора в систему мониторинга вам потребуются:
        1. IP-адрес устройства.
        2. Read Community и Write Community (для v2c).
        3. Загруженный MIB-файл (для корректного отображения названий параметров и OID).

## 9.22 Работа с MAC адресами (MAC address)

В этом разделе можно добавить статические MAC адреса, посмотреть таблицу MAC адресов и т.д.

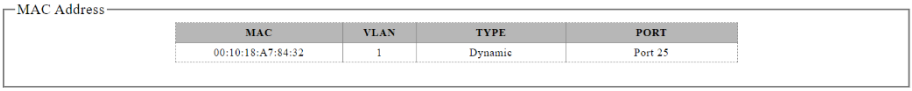
MAC-адрес (Media Access Control Address) – это уникальный идентификатор сетевого интерфейса, используемый для определения местоположения устройства в сети на канальном уровне (L2).

### 9.22.1 Таблица MAC адресов (MAC Table)

Таблица MAC-адресов – это база данных коммутатора, в которой хранятся изученные MAC-адреса устройств и соответствующие им порты. Это основа для коммутации кадров на уровне L2.

Для перехода в данный раздел в меню навигации выберите:

**Security > MAC Address > MAC Address Table**




| Параметр | Описание |
|---|---|
| **MAC-адрес (MAC)** | Физический (аппаратный) адрес сетевого устройства. |
| **VLAN ID (VLAN)** | Идентификатор VLAN, в котором был обнаружен MAC-адрес. |
| **Тип (Type)** | Способ, которым запись попала в таблицу:<br>• **Динамический (Dynamic)** – выучен коммутатором автоматически из входящих кадров. Имеет время жизни (aging time).<br>• **Статический (Static)** – добавлен администратором вручную. Хранится постоянно до удаления. |
| **Порт (Port)** | Номер физического порта коммутатора, с которого был получен кадр с данным MAC-адресом. |

***Примечания***

1. 💡 **Как работает таблица MAC-адресов**:
    - Когда коммутатор получает кадр на порт, он смотрит на исходный MAC-адрес (Source MAC) и связывает его с этим портом, обновляя таблицу.

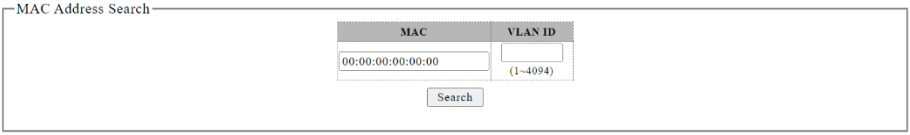
- При отправке кадра коммутатор ищет MAC-адрес назначения (Destination MAC) в своей таблице. Если запись найдена, кадр отправляется только на соответствующий порт. Если нет – рассылается на все порты данного VLAN (flooding).

2. 💡 **Типы записей и их использование**:
    - **Динамические записи:** Основа работы. Имеют время жизни (Aging Time, обычно 300 сек)**.** Если в течение этого времени не поступит кадр с данным MAC, запись удаляется.
    - **Статические записи:** Добавляются вручную. Не удаляются автоматически. Используются для закрепления устройства за портом (повышение безопасности) или для оптимизации трафика.
3. 💡 **Диагностика с помощью таблицы**:
    - Таблица помогает находить петли (loops)**:** если один и тот же MAC-адрес появляется на нескольких портах – это признак появления сетевых петель.
    - Позволяет идентифицировать, к какому порту подключено конкретное устройство (по его MAC).
    - Помогает в поиске неисправностей: если MAC-адрес не появляется в таблице, возможно, устройство неактивно или есть проблема с кабелем/портом.

### 9.22.2 Поиск в таблице MAC адресов (MAC Search)

Для перехода в данный раздел в меню навигации выберите:

**Security > MAC Address > MAC Search**




| Параметр | Описание |
|---|---|
| **MAC-адрес (MAC)** | Физический (аппаратный) адрес сетевого устройства. |
| **VLAN ID (VLAN)** | Идентификатор VLAN для поиска MAC адреса |

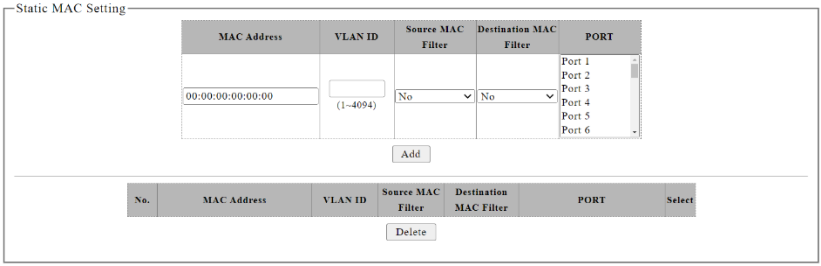
Кнопка **Search** (Искать) отвечает за поиск MAC адреса с помощью инструментов на этой странице.

### 9.22.3 Статические MAC адреса (Static MAC)

Эта страница WEB используется для настройки и добавления статических записей в таблицу MAC-адресов.

Для перехода в данный раздел в меню навигации выберите:

**Security > MAC Address > Static MAC**



| Параметр | Описание |
| --- | --- |
| **MAC-адрес (MAC Address)** | Физический адрес устройства, который требуется статически привязать к порту. Формат: `XX:XX:XX:XX:XX:XX`. |
| **VLAN ID** | Идентификатор VLAN, для которого добавляется статическая запись. Диапазон от 1 до 4094. |
| **Фильтр по источнику (Source MAC Filter)** | Вкл/выкл фильтр MAC по источнику трафика |
| **Фильтр по получателю (Destination MAC Filter)** | Вкл/выкл фильтр MAC по получателю трафика |
| **Порт (Port)** | Физический порт коммутатора, к которому будет жёстко привязан указанный MAC-адрес. |

Кнопка **Add** (Добавить) отвечает за добавление привязки MAC адреса с помощью инструментов на этой странице.

Кнопка **Delete** (Удалить) отвечает за удаление привязки MAC адреса.

***Примечания***

1. 💡 **Назначение статических MAC-записей**:
    - **Повышение безопасности:** Предотвращает атаки, связанные с подменой MAC-адресов (MAC spoofing) на

критически важных портах. Трафик с указанным MAC будет приниматься только с назначенного порта.

- **Привязка устройств:** Гарантирует, что важное устройство (сервер, шлюз, контроллер) всегда будет ассоциироваться с определённым портом, даже если его трафик временно прекратится (в отличие от динамической записи, которая со временем удалится).
- **Оптимизация производительности:** Незначительно снижает нагрузку на процессор коммутатора, исключая необходимость повторного изучения адреса.

2. 💡 **Ограничения и важные моменты**:
    - ⚠ **Статическая запись имеет приоритет над любой динамической.** Если устройство с привязанным MAC-адресом будет подключено к другому порту, его трафик не будет корректно обрабатываться.
    - Максимальное количество статических записей ограничено размером таблицы MAC-адресов коммутатора (см. таблицу технических характеристик)
    - Убедитесь, что устройство действительно находится в указанном VLAN (VLAN ID)**,** иначе связь не будет работать.
3. 💡 **Типичные сценарии использования**:
    - **Серверы:** Для серверов с фиксированным местоположением.
    - **Сетевая инфраструктура:** Для портов, подключённых к маршрутизаторам, межсетевым экранам, контроллерам беспроводной сети.
    - **Критичные рабочие ПК и устройства:** Для ПК или устройств, работа с которыми требует повышенного уровня безопасности.

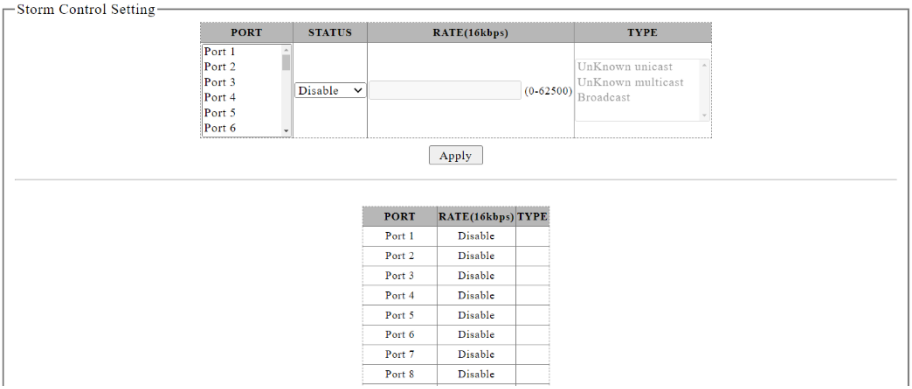
## 9.23 Настройка Storm Control (Storm Control)

В этом разделе можно включить и настроить защиту от NET шторма.

Сетевой шторм (Net Storm), возникает, когда из-за непрерывной циклической пересылки количество broadcast, multicast трафика или неизвестных кадров в сети превышает допустимые пределы. Это нарушает нормальную сетевую связь, серьёзно снижая производительность. Шторм занимает значительную полосу пропускания, блокирует передачу обычных пакетов и может привести к отказу сетевых служб, вызывая отказ части или всей сети.

Для перехода в данный раздел в меню навигации выберите:

**Security > Storm Control**



| Параметр | Описание |
|---|---|
| **Порт (Port)** | Выбор одного или нескольких портов для применения Storm Control |
| **Состояние (Status)** | Включение или отключение (enable/disable) функции Storm Control для выбранных портов и типа трафика. |
| **Тип пакетов (Type)** | Выбор типа трафика для Storm Control:<br>• **Broadcast** – широковещательные кадры (FF:FF:FF:FF:FF:FF).<br>• **Unknown Unicast** – кадры с неизвестным индивидуальным MAC-адресом назначения (отсутствующим в таблице MAC).<br>• **Unknown Multicast** – кадры с неизвестным групповым MAC-адресом. |
| **Ограничение скорости (Rate)** | Пороговое значение скорости для выбранного типа трафика. При превышении этого порога дальнейшие кадры данного типа будут отбрасываться.<br>• **Задаётся в:** килобитах в секунду (Kbps)<br>Диапазон от 0 до 62500 Кбит/с |

Кнопка **Apply** (Применить) отвечает за сохранение настроек на этой странице.

***Примечания***

1. 💡 **Назначение и принцип работы**:
    - Функция непрерывно отслеживает интенсивность указанных типов трафика на порту.
    - Когда скорость поступления кадров выбранного типа **(**Broadcast, Multicast и т.д.) превышает заданный порог (Rate), коммутатор начинает отбрасывать (discard) излишки кадров, предотвращая перегрузку порта и всей сети.
    - Как только интенсивность падает ниже порога, нормальная пересылка возобновляется.
2. 💡 **Рекомендации по настройке порогов**:
    - **Широковещательный трафик (Broadcast):** Рекомендуемый порог – 1-5% от скорости порта. Для гигабитного порта (1000 Мбит/с) это 10-50 Мбит/с. Широковещательный трафик выше этого уровня почти всегда аномален.
    - **Многоадресный трафик (Multicast):** Порог зависит от приложений (видеотрансляции, IPTV). Может быть установлен выше – 10-20%**.**
    - **Неизвестный одноадресный (Unknown Unicast):** Рекомендуется установить низкий порог (0.1-1%), так как этот тип трафика указывает на неэффективное заполнение (flooding) и часто связан с атаками или проблемами в сети.
3. 💡 **Основные сценарии использования**:
    - **Защита от сетевых петель (Loops):** Основное применение. Петля вызывает лавинообразный рост

широковещательного трафика. Storm Control ограничит ущерб, сдерживая шторм на входных портах.

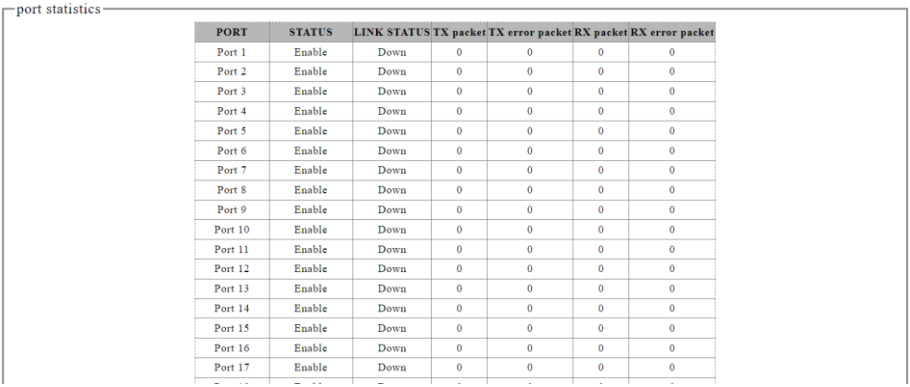
- **Ограничение широковещательного трафика:** Некоторые протоколы (например, старые реализации NetBIOS) могут генерировать чрезмерный широковещательный трафик. Функция ограничивает их влияние.
- **Предотвращение атак:** Защищает от атак типа "отказ в обслуживании" (DoS), связанных с flooding сети подменными кадрами.

## 9.24 Статистика портов (Port Statistics)

В этом разделе содержится информация о количестве переданных/принятых пакетов по портам, состоянии портов, а также статистика пакетов принятых или отправленных с ошибками.

Для перехода в данный раздел в меню навигации выберите:

**Monitoring > Port Statistics**


port statistics

| PORT | STATUS | LINK STATUS | TX packet | TX error packet | RX packet | RX error packet |
|---|---|---|---|---|---|---|
| Port 1 | Enable | Down | 0 | 0 | 0 | 0 |
| Port 2 | Enable | Down | 0 | 0 | 0 | 0 |
| Port 3 | Enable | Down | 0 | 0 | 0 | 0 |
| Port 4 | Enable | Down | 0 | 0 | 0 | 0 |
| Port 5 | Enable | Down | 0 | 0 | 0 | 0 |
| Port 6 | Enable | Down | 0 | 0 | 0 | 0 |
| Port 7 | Enable | Down | 0 | 0 | 0 | 0 |
| Port 8 | Enable | Down | 0 | 0 | 0 | 0 |
| Port 9 | Enable | Down | 0 | 0 | 0 | 0 |
| Port 10 | Enable | Down | 0 | 0 | 0 | 0 |
| Port 11 | Enable | Down | 0 | 0 | 0 | 0 |
| Port 12 | Enable | Down | 0 | 0 | 0 | 0 |
| Port 13 | Enable | Down | 0 | 0 | 0 | 0 |
| Port 14 | Enable | Down | 0 | 0 | 0 | 0 |
| Port 15 | Enable | Down | 0 | 0 | 0 | 0 |
| Port 16 | Enable | Down | 0 | 0 | 0 | 0 |
| Port 17 | Enable | Down | 0 | 0 | 0 | 0 |

| Параметр | Описание |
|---|---|
| **Порт (Port)** | Номер физического порта коммутатора. |
| **Состояние (Status)** | Административное состояние порта (Включен/Выключен). В состоянии **Включен (Enable)** порт может нормально пересылать пакеты. |
| **Состояние соединения (Link Status)** | Текущий физический статус канала (LINK):<br>• **Up** – кабель подключён, связь установлена.<br>• **Down** – кабель не подключён или связь неактивна. |
| **Число отправленных корректных пакетов (TX packet)** | Общее количество **успешно переданных** (отправленных с порта) пакетов с момента последнего сброса статистики или включения порта. |
| **Число отправленных пакетов с ошибкой (TX Error packet)** | Общее количество пакетов с **ошибками при отправке** (например, коллизии в полудуплексном режиме). |
| **Число принятых корректных пакетов (RX packet)** | Общее количество **успешно принятых** (полученных на порт) корректных пакетов. |

| Параметр | Описание |
| --- | --- |
| **Число принятых пакетов с ошибками (RX Error packet)** | Общее количество **принятых с ошибками** пакетов (например, с CRC-ошибкой, кадры неверной длины). |

***Примечания***

1. 💡 **Диагностика проблем с помощью статистики**:
    - **Резкий рост общего трафика (TX/RX packet):** Может указывать на сетевую атаку, активность вредоносного ПО или некорректную работу сетевого приложения.
    - **Высокое значение TX/RX error packet:** Признак серьёзных проблем:
        - **Ошибки при отправке (TX error packet):** Часто указывают на **коллизии (collisions)**, что характерно для устаревшего оборудования, работающего в полудуплексном (Half-Duplex) режиме, или на неисправный кабель.
        - **Ошибки при приёме (RX Error packet):** Обычно вызваны кабелем плохого качества**,** неисправными коннекторами, электромагнитными помехами или несоответствием настроек дуплекса/скорости на двух концах канала.
2. 💡 **Как использовать данные**:
    - Сравнивайте значения **RX packet** и **RX error packet**. Если количество ошибок составляет более 0,1-1% от

общего числа принятых пакетов — это повод для детального изучения.

- Статистика полезна для долгосрочной эксплуатации сети: порт, постоянно работающий на 80-90% от своей пропускной способности, может стать узким местом.

## 9.25 Обновление прошивки коммутатора (Firmware Upgrade)

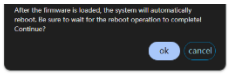
В этом разделе содержится инструменты для обновления прошивки коммутатора.

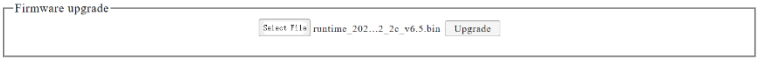
Для перехода в данный раздел в меню навигации выберите:

**Tools > Firmware Upgrade**


💡 Порядок действий для обновления прошивки следующий:

1) Подключите коммутатор к ПК
2) Нажмите кнопку **Select File** (Выбор файла) для выбора и загрузки файла прошивки с ПК
3) Нажмите кнопку **Upgrade** (Обновить)
4) Дождитесь загрузки прошивки в память коммутатора и нажмите кнопку **OK** в всплывающем сообщении




5) В конце процесса обновления прошивки появится сообщение вида

⚠ **Внимание!**

В процессе обновления прошивки коммутатора не отключайте питание, убедитесь, что питание стабильно. Также не обновляйте страницу WEB интерфейса *Tools > Firmware Upgrade* пока процесс прошивки не завершится. Перед обновлением прошивки сохраните текущую конфигурацию настроек коммутатора на ПК (см. пункт 9.26)

## 9.26 Инструмент для экспорта/импорта настроек (Configure Backup)

В этом разделе содержится инструмент для экспорта/импорта текущих настроек коммутатора в файл/из файла на ПК.

Для перехода в данный раздел в меню навигации выберите:

**Tools > Configure Backup**


💡 Порядок действий для экспорта (сохранения) настроек коммутатора на ПК:

1) Нажмите кнопку **Backup** (Экспорт)
2) Задайте имя файла и выберите место на ПК через файловый менеджер для экспорта настроек коммутатора

Порядок действий для импорта настроек коммутатора из файла:

1) Нажмите кнопку **Select File** (Выбор файла) и выберите файл с настройками, сохраненными ранее
2) Нажмите кнопку **Restore** (Восстановить) настройки коммутатора из выбранного файла. Далее перезагрузите устройство.

## 9.27 Сброс коммутатора к заводским настройкам (Reset)

В этом разделе содержится инструмент для сброса всех настроек коммутатора к заводским установкам.

Для перехода в данный раздел в меню навигации выберите:

**Tools > Reset**


Кнопка **Restore** отвечает за сброс коммутатора к заводским настройкам.

**⚠Внимание!**

В процессе сброса настроек текущая конфигурация будет потеряна. Перед процессом сброса рекомендуется выполнить экспорт настроек в файл (см. раздел 9.26) Кроме того, после сброса настроек к заводским **IP адрес коммутатора, а также логин и пароль будут изменены на значения по умолчанию**

## 9.28 Сохранить текущую конфигурацию (Save)

В этом разделе содержится инструмент для сохранения текущей конфигурации.

Для перехода в данный раздел в меню навигации выберите:

**Tools > Save**


Кнопка **Save** отвечает за сохранение текущей конфигурации коммутатора во Flash память.

💡 обязательно сохраняйте текущую конфигурацию коммутатора, чтобы не потерять ее после отключения питания или перезагрузки коммутатора.

## 9.29 Перезагрузка (Reboot)

В этом разделе содержится инструмент для удаленной перезагрузки коммутатора.

Для перехода в данный раздел в меню навигации выберите:

**Tools > Reboot**


Кнопка **Reboot** отвечает за перезагрузку коммутатора.

⚠**Внимание!**

В процессе перезагрузки коммутатора не отключайте питание физически от устройства.

## 10. Технические характеристики*

| **Модель** | **SW-24G2C-M(200W)** |
|---|---|
| Общее кол-во портов | 28 |
| Кол-во портов FE+PoE | - |
| Кол-во портов FE | - |
| Кол-во портов GE+PoE | 24 |
| Кол-во портов GE<br>(не Combo порты) | 2 |
| Кол-во портов Combo GE<br>(RJ45+SFP) | 2 |
| Кол-во портов SFP (не Combo порты) | - |
| Мощность PoE на один порт (макс.) | 90 Вт (1-4 порты)<br>30 Вт (5-24 порты) |
| Суммарная мощность PoE всех портов (макс.) | 200 Вт |
| Стандарты PoE | IEEE 802.3bt (1-4 порты)<br>IEEE 802.3af<br>IEEE 802.3at |
| Метод подачи PoE | 1-4 порты: метод A+B 1/2,4/5 (+) 3/6, 7/8 (-)<br>5-24 порты: метод A 1/2(+), 3/6(-) |
| Топологии подключения | звезда<br>каскад<br>кольцо |
| Буфер пакетов | 4.1 Мб |
| Таблицы MAC-адресов | 8 К |
| Пропускная способность коммутационной матрицы (Switching fabric) | 56 Гбит/с |
| Скорость обслуживания пакетов (Forwarding rate) | 41,664Mbps |

| **Модель** | **SW-24G2C-M(200W)** |
|---|---|
| Поддержка jumbo frame | 10 К |
| Размер flash памяти | 2 МБ |
| Управление | Управление через WEB-интерфейс (WEB managed) |
| Качество обслуживания (QoS) | IEEE 802.1p, 8 очередей |
| Стандарты и протоколы | • IEEE 802.3 – 10BaseT<br>• IEEE 802.3u – 100BaseTX<br>• IEEE 802.3ab – 1000BaseT<br>• IEEE 802.3z – 1000 BaseSX/LX<br>• IEEE 802.3x – Flow Control<br>• IEEE 802.1Q – VLAN<br>• IEEE 802.1D – Spanning Tree<br>• IEEE 802.1w – Rapid Spanning Tree<br>• IEEE 802.3ad – Link Aggregation Control Protocol (LACP)<br>• IGMP Snooping |
| Функции уровня 2 | • IEEE 802.1D (STP)<br>• IEEE 802.1w (RSTP)<br>• VLAN / VLAN Group 4K<br>• Tagged Based<br>• Port-based<br>• Link Aggregation IEEE 802.3ad with LACP<br>• Storm Control |
| Интерфейс управления | WEB/SNMP |
| Индикаторы | PWR – наличие питания;<br>Link – передача данных;<br>PoE – индикатор подачи PoE;<br>25,26 – линк/активность Uplink порты;<br>27,28 – линк/активность Combo порты. |
| Питание | AC100-240V(240Вт) |
| Встроенная грозозащита | 6 кВ (8/20 мкс) |
| Охлаждение | Конвекционное (без вентилятора) |
| Тип монтажа | на плоскую поверхность;<br>в 19” стойку |
| Рабочая температура | 0...+40° С |

| **Модель** | **SW-24G2C-M(200W)** |
|---|---|
| Относительная влажность | до 90% без конденсата |
| Вес (без упаковки), кг | 3.6 |
| Размеры (ШхВхГ), мм | 440x44x200 |
| Дополнительно | Кнопка для сброса коммутатора к заводским настройкам |

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

## 11. Гарантия

Гарантия на все оборудование OSNOVO – 7 лет (84 месяца) 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