OSNOVO

cable transmission

# РУКОВОДСТВО ПО НАСТРОЙКЕ

## Управление коммутатором с помощью WEB интерфейса

www.osnovo.ru

# Оглавление

# 1. Введение

В этом руководстве описано использование WEB-интерфейса управления (Web UI) для настройки параметров управляемых коммутаторов данной серии.

### Поддерживаемые браузеры

Веб-интерфейс совместим со следующими браузерами:

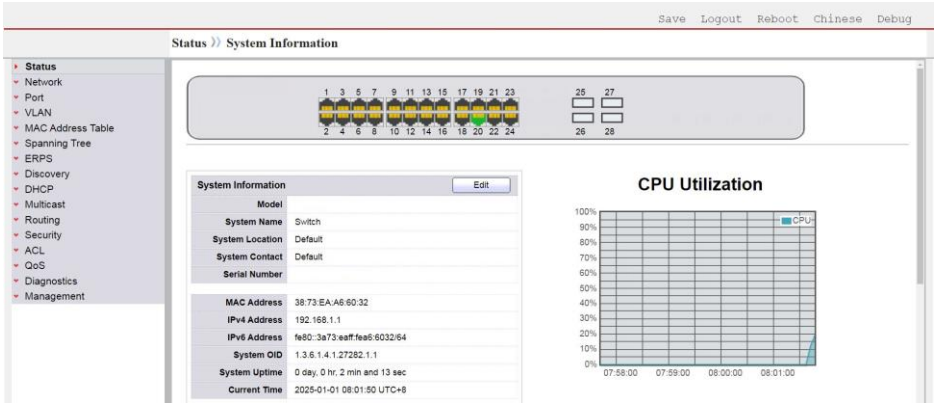
- Internet Explorer 8 и выше
- Firefox 20.0 и выше
- Chrome 23.0 и выше
- Safari 5.1.7 и выше

### Интерфейс пользователя

- **Левая панель** содержит меню настроек.
- **Верхняя строка** отображает текущее состояние портов:
  - Зеленые индикаторы - порт активен (link up)
  - Черные индикаторы - порт неактивен (link down)
- **Панель инструментов** (расположена ниже изображения коммутатора) предоставляет быстрый доступ к часто используемым функциям.
- **Основная рабочая область** отображает параметры конфигурации.

**Внимание!**

Количество основных портов и SFP портов, описываемое в данном руководстве, может отличаться.



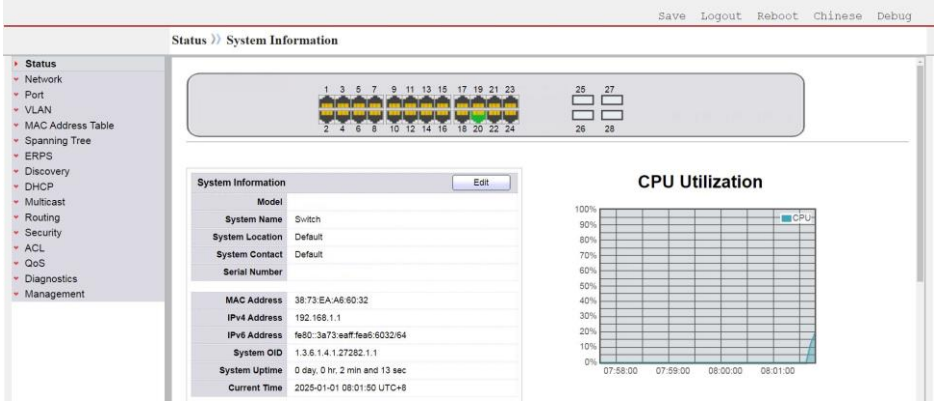

## 2. Состояние системы (Status)

Раздел **«Состояние системы (Status)»** отображает системную информацию и текущий статус работы устройства.

### 2.1. Системная информация (System Information)

**Чтобы открыть страницу с системной информацией (System Information):**

Перейдите в раздел **«Status»** → **«System Information»**.



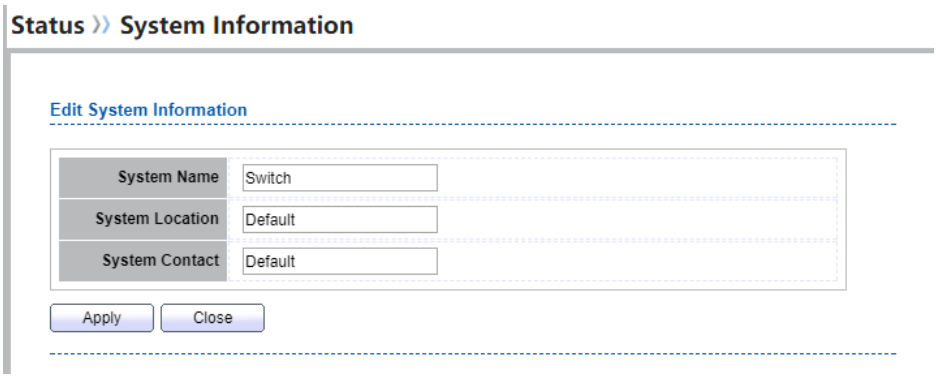
**На этой странице отображается:**

- Графическое представление панели коммутатора (Switch panel)
- Загрузка ЦП (CPU utilization)
- Использование памяти (Memory utilization)
- Другие текущие системные параметры

**Дополнительные возможности:**
Страница позволяет редактировать некоторые системные параметры (system information).

| Параметр | Описание |
|---|---|
| Model | Название модели коммутатора |
| System Name | Системное имя коммутатора. Также используется как префикс в CLI (например, "Switch>" или "Switch#") |
| System Location | Информация о физическом расположении коммутатора |
| System Contact | Контактная информация, связанная с коммутатором |
| MAC Address | Базовый MAC-адрес коммутатора |
| IPv4 Address | Текущий IPv4-адрес системы |
| IPv6 Address | Текущий IPv6-адрес системы |
| System OID | Идентификатор объекта системы для SNMP |
| System Uptime | Общее время работы с момента последней загрузки |
| Current Time | Текущее системное время |
| Loader Version | Версия загрузочного образа |
| Loader Date | Дата сборки загрузочного образа |
| Firmware Version | Версия текущей прошивки |
| Firmware Date | Дата сборки текущей прошивки |
| Telnet | Текущее состояние сервиса Telnet (включен/выключен) |
| SSH | Текущее состояние сервиса SSH (включен/выключен) |
| HTTP | Текущее состояние сервиса HTTP (включен/выключен) |
| HTTPS | Текущее состояние сервиса HTTPS (включен/выключен) |
| SNMP | Текущее состояние сервиса SNMP (включен/выключен) |

Для изменения системных параметров нажмите кнопку **Edit (изменить)** в заголовке таблицы.




| Параметр | Описание |
|---|---|
| System Name | Название системы коммутатора. Используется как префикс в командной строке (CLI) для каждой строки ("Switch>" или "Switch#") |
| System Location | Физическое местоположение коммутатора (здание, этаж, помещение и т.д.) |
| System Contact | Контактная информация ответственного лица или отдела (телефон, email и т.п.) |

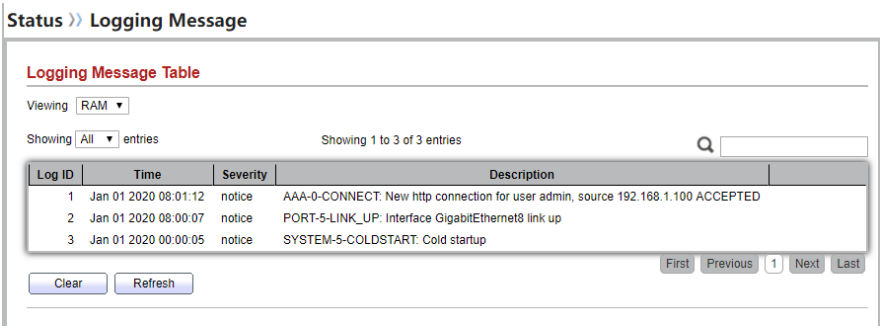
**Примечания:**

1. Для редактирования необходимо иметь соответствующие права доступа администратора
2. Изменения вступают в силу немедленно после сохранения
3. Имя системы (System Name) не должно содержать специальных символов и пробелов
4. Рекомендуется указывать актуальную контактную информацию для оперативного решения проблем

## 2.2. Журнал сообщений (Logging Message)

**Для просмотра журнальных сообщений, хранящихся в RAM и Flash памяти:**

Перейдите в раздел **Status** > **Logging Message**.




***Поля журнала сообщений***

| Параметр | Описание |
|---|---|
| Log ID | Идентификатор записи журнала |
| Time | Временная метка сообщения |
| Severity | Уровень важности сообщения (критическое, предупреждение, информационное и т.д.) |
| Description | Текстовое описание события |

***Управление журналом***

| Параметр | Описание |
|---|---|
| Viewing | Режим просмотра журнала: |
| | **RAM** – отображает сообщения, хранящиеся в оперативной памяти |
| | **Flash** – отображает сообщения, сохранённые в энергонезависимой памяти |

| Параметр | Описание |
|---|---|
| Clear | Очистка всех записей журнала |
| Refresh | Обновление списка |

**Примечания:**

1. Сообщения в RAM памяти теряются при перезагрузке устройства
2. Сообщения в Flash памяти сохраняются после перезагрузки
3. Уровень важности (Severity) помогает фильтровать критически важные события
4. Для сохранения журнала рекомендуется периодически экспортировать данные

## 2.3. Статус портов (Port)

Страница конфигурации портов отображает сводную информацию и статус портов.

### 2.3.1. Статистика информации на портах (Statistics)

**Чтобы открыть страницу счётчиков портов:**

Перейдите в раздел **Status** > **Port** > **Statistics**.

**На этой странице отображаются:**

- Стандартные счётчики сетевого трафика из MIB:
  - **Interfaces** (Интерфейсы)
  - **Ethernet-like** (Ethernet-статистика)
  - **RMON** (Удалённый мониторинг)
- Счётчики **Interfaces** и **Ethernet-like** отображают ошибки в трафике каждого порта.
- Счётчики **RMON** показывают общее количество переданных кадров разных типов и размеров.

Кнопка **Clear (Очистить)** – сбрасывает счётчики выбранного порта.

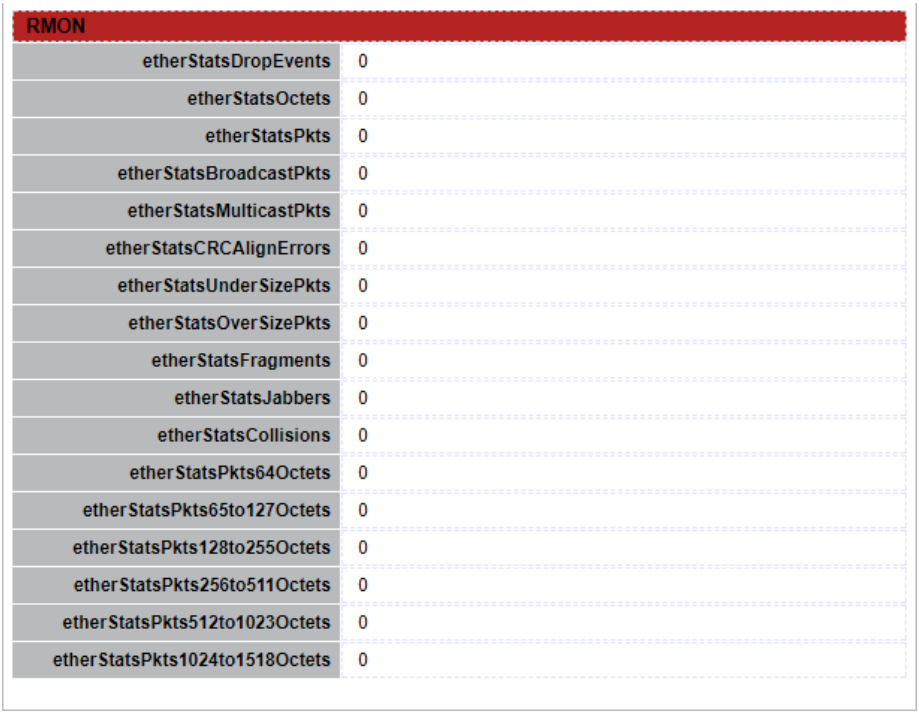
## Status ›› Port ›› Statistics

| | |
|---|---|
| Port | GE1 ▼ |
| MIB Counter | ◉ All<br>○ Interface<br>○ Etherlike<br>○ RMON |
| Refresh Rate | ○ None<br>○ 5 sec<br>◉ 10 sec<br>○ 30 sec |

Clear

| Interface | |
|---|---|
| ifInOctets | 0 |
| ifInUcastPkts | 0 |
| ifInNUcastPkts | 0 |
| ifInDiscards | 0 |
| ifOutOctets | 0 |
| ifOutUcastPkts | 0 |
| ifOutNUcastPkts | 0 |
| ifOutDiscards | 0 |
| ifInMulticastPkts | 0 |
| ifInBroadcastPkts | 0 |
| ifOutMulticastPkts | 0 |
| ifOutBroadcastPkts | 0 |

| Etherlike | |
|---|---|
| dot3StatsAlignmentErrors | 0 |
| dot3StatsFCSErrors | 0 |
| dot3StatsSingleCollisionFrames | 0 |
| dot3StatsMultipleCollisionFrames | 0 |
| dot3StatsDeferredTransmissions | 0 |
| dot3StatsLateCollisions | 0 |
| dot3StatsExcessiveCollisions | 0 |
| dot3StatsFrameTooLongs | 0 |
| dot3StatsSymbolErrors | 0 |
| dot3ControlInUnknownOpcodes | 0 |
| dot3InPauseFrames | 0 |
| dot3OutPauseFrames | 0 |



| RMON | |
|---|---|
| etherStatsDropEvents | 0 |
| etherStatsOctets | 0 |
| etherStatsPkts | 0 |
| etherStatsBroadcastPkts | 0 |
| etherStatsMulticastPkts | 0 |
| etherStatsCRCAlignErrors | 0 |
| etherStatsUnderSizePkts | 0 |
| etherStatsOverSizePkts | 0 |
| etherStatsFragments | 0 |
| etherStatsJabbers | 0 |
| etherStatsCollisions | 0 |
| etherStatsPkts64Octets | 0 |
| etherStatsPkts65to127Octets | 0 |
| etherStatsPkts128to255Octets | 0 |
| etherStatsPkts256to511Octets | 0 |
| etherStatsPkts512to1023Octets | 0 |
| etherStatsPkts1024to1518Octets | 0 |

***Параметры статистики***

| Параметр | Описание |
|---|---|
| **Port** | Выберите порт для отображения статистики. |
| **MIB Counter** | Выберите тип счётчика: |
| | **All** – все счётчики |
| | **Interface** – счётчики интерфейсов (ошибки, сбросы) |
| | **Etherlike** – Ethernet-статистика (коллизии, ошибки CRC) |
| | **RMON** – статистика по типам и размерам кадров |
| **Refresh Rate** | Автообновление страницы (в секундах) для актуальных данных. |

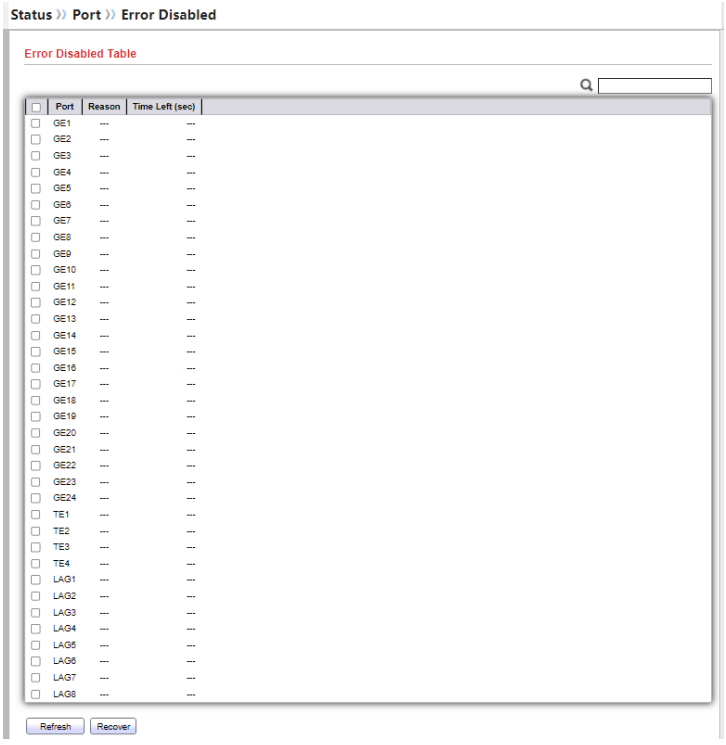
**Примечания:**

1. **MIB (Management Information Base)** – база данных для мониторинга сетевых устройств.
2. **RMON (Remote Monitoring)** – расширенная статистика для анализа трафика.
3. Очистка счётчиков (**Clear**) не влияет на работу портов, только обнуляет статистику.

### 2.3.2. Таблица ошибок на портах (Error Disabled)

**Чтобы просмотреть статус портов, отключённых из-за ошибок:**

Перейдите в раздел **Status** > **Port** > **Error Disabled**



***Информация о портах в состоянии Error Disabled***

| Параметр | Описание |
|---|---|
| **Port (Порт)** | Номер интерфейса/порта. |
| **Reason (Причина отключения)** | Порт может быть отключён по одной из следующих причин: |
| | **BPDU Guard** – Обнаружен BPDU-кадр (защита от петель STP) |
| | **UDLD** – Обрыв двусторонней связи (UniDirectional Link Detection) |
| | **Self Loop** – Обнаружена петля на порту |
| | **Broadcast Flood** – Превышен лимит broadcast-трафика |
| | **Unknown Multicast Flood** – Превышен лимит неизвестного multicast-трафика |
| | **Unicast Flood** – Превышен лимит unicast-трафика |
| | **ACL** – Нарушение правил ACL (Access Control List) |
| | **Port Security Violation** – Нарушение безопасности порта (MAC-фильтрация) |
| | **DHCP rate limit** – Превышена частота DHCP-запросов |
| | **ARP rate limit** – Превышена частота ARP-запросов |
| **Time Left (sec)** | Оставшееся время (в секундах) до автоматического восстановления порта. |

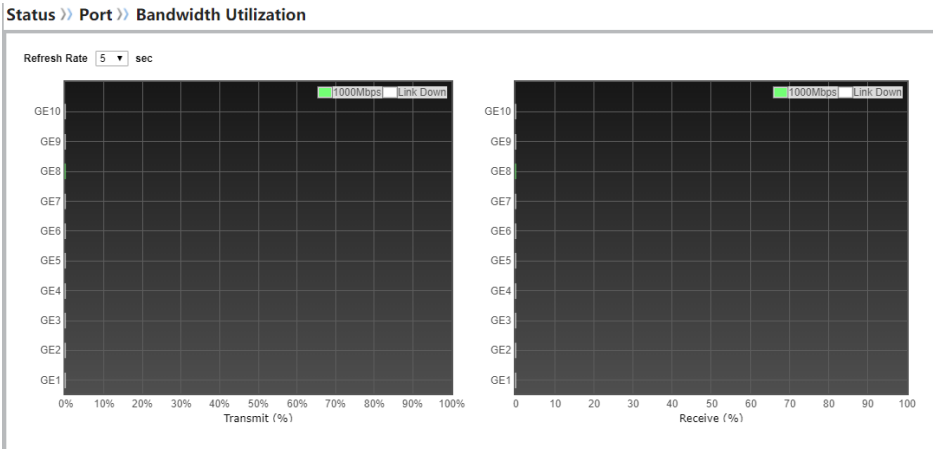
**Примечания:**

1. Состояние **Error Disabled** – защитный механизм, предотвращающий сетевые аномалии.
2. Для восстановления работы порта:
   - Дождаться истечения **Time Left** (автовосстановление),
   - Вручную включить порт через CLI/Web-интерфейс после устранения причины ошибки.
3. **BPDU Guard** и **Port Security** – частые причины отключения в безопасных сетях.

### 2.3.3. Использование полосы пропускания (Bandwidth Utilization)

**Чтобы открыть страницу мониторинга использования полосы пропускания:**

Перейдите в раздел **Status** > **Port** > **Bandwidth Utilization**.




**Функциональные возможности данной страницы WEB интерфейса:**

- Отображение текущей загрузки полосы пропускания для каждого порта в реальном времени
- Автоматическое обновление данных с заданным интервалом

| Параметр | Описание |
|---|---|
| **Refresh Rate** | Интервал автоматического обновления данных (в секундах). Позволяет получать актуальную информацию о загрузке полосы пропускания. |

**Рекомендации по использованию:**

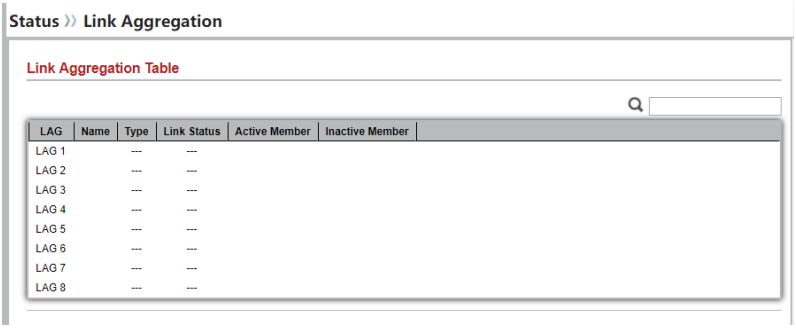
- Для детального анализа установите меньший интервал обновления

- Для долговременного мониторинга рекомендуется использовать большие интервалы
- Данные могут быть полезны для выявления перегруженных портов и оптимизации сети

## 2.4. Статистика агрегации каналов (Link Aggregation)

**Для отображения статуса агрегации каналов:**

Перейдите в раздел **Status** > **Link Aggregation**.




***Параметры агрегированных каналов***

| Параметр | Описание |
|---|---|
| **LAG** | Идентификатор агрегированного канала |
| **Name** | Описание агрегированного порта |
| **Type** | Тип агрегации: |
| | **Static (Статическая)** - порты в группе всегда являются активными участниками |
| | **LACP (Dynamic)** - порты являются кандидатами, активные участники определяются протоколом LACP |
| **Link Status** | Текущее состояние связи агрегированного порта |
| **Active Member** | Список активных портов в составе агрегированного канала |

| Параметр | Описание |
|---|---|
| **Inactive Member** | Список неактивных портов в составе агрегированного канала |

**Примечания:**

1. **Статическая агрегация** не требует дополнительных протоколов, но менее гибкая
2. **LACP (IEEE 802.3ad)** обеспечивает динамическое управление составом агрегированного канала

**Рекомендации:**

- Для критически важных соединений рекомендуется использовать LACP
- Количество портов в агрегированной группе должно соответствовать возможностям оборудования
- Мониторинг статуса помогает выявлять проблемы в работе агрегированных каналов

### 2.5. Информация в таблице MAC-адресов (MAC Address Table)

**Для отображения таблицы MAC-адресов:**

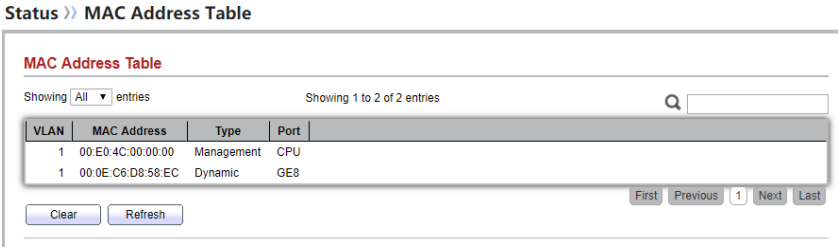
Перейдите в раздел **Status** > **MAC Address Table**.

Данная страница WEB интерфейса отображает все записи MAC-адресов на коммутаторе, включая:

- Статические MAC-адреса, добавленные администратором
- Динамические MAC-адреса, изученные оборудованием автоматически

Для управления предусмотрены кнопки:

- Кнопка **Clear (Очистить)** - удаляет все динамические записи
- Кнопка **Refresh (Обновить)** - получает актуальные записи MAC-адресов




***Параметры таблицы MAC-адресов***

| Параметр | Описание |
|---|---|
| **VLAN** | Идентификатор VLAN, к которой принадлежит MAC-адрес |
| **MAC Address** | Физический адрес устройства |
| **Type** | Тип MAC-адреса: |
| | **Management** - базовый MAC-адрес устройства для управления |
| | **Static** - добавлен администратором вручную |
| | **Dynamic** - изучен коммутатором автоматически |
| **Port** | Тип порта: |
| | **CPU** - порт процессора для управления устройством |
| | **Other** - обычный порт коммутатора |

**Примечания:**

1. Статические записи сохраняются после перезагрузки устройства
2. Динамические записи имеют ограниченное время жизни (aging time)
3. Таблица MAC-адресов используется для коммутации кадров в сети

**Рекомендации:**

- Регулярно проверяйте таблицу MAC-адресов для анализа подключенных устройств
- Используйте статические записи для критически важных устройств в сети
- Очистка динамических записей может быть полезна при диагностике сети

## 3. Настройки сети (Network)

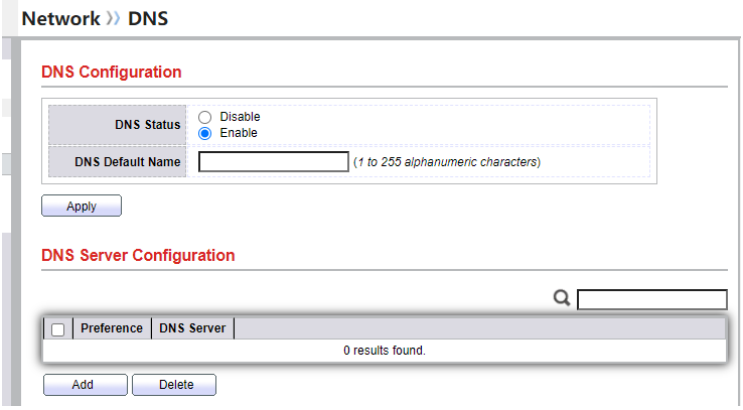
Раздел **Настройки сети (Network)** предназначен для настройки сетевых интерфейсов коммутатора и параметров подключения к удалённым серверам.

### 3.1. Настройка DNS (DNS Configuration)

**DNS (Domain Name System)** – это система доменных имен, используемая для преобразования удобных для пользователя имен (например, example.com) в IP-адреса.

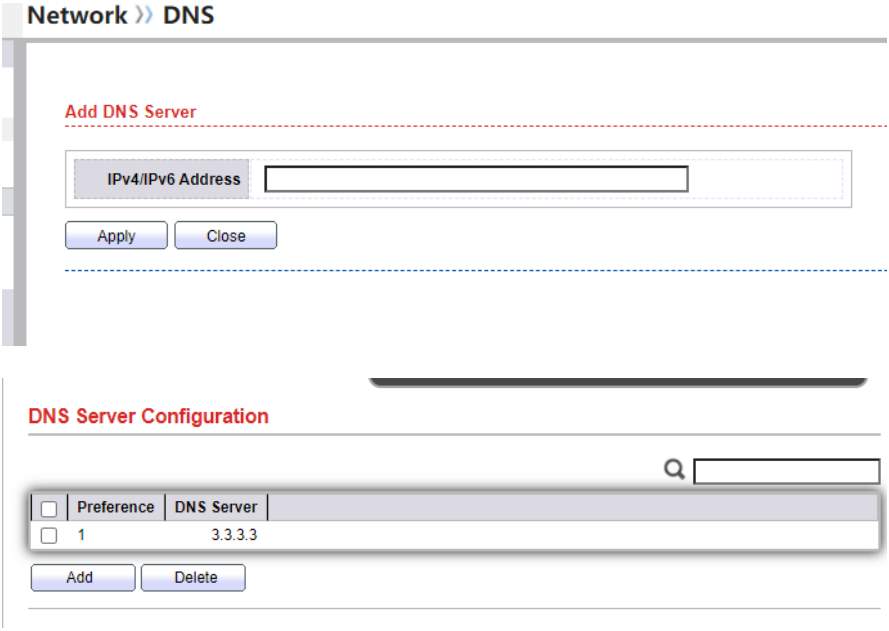
**Как настроить DNS:**

Перейдите в раздел **Network** > **DNS**



***Параметры DNS***

| Параметр | Описание |
|---|---|
| **DNS Status** | Включение/отключение функции DNS. |
| **DNS Default Name** | Введите доменное имя по умолчанию (например, example.com). |




***Добавление DNS-серверов***

1. Нажмите кнопку **Add (Добавить)**, чтобы указать DNS-серверы (например, 8.8.8.8 или 1.1.1.1).
2. Нажмите **Apply (Применить)**, чтобы сохранить настройки.

**Примечания:**

1. DNS используется для:
   - Доступа к сетевым устройствам по именам (вместо IP-адресов).
   - Подключения к интернет-ресурсам.

2. Рекомендуемые DNS-серверы:
    - Google: 8.8.8.8, 8.8.4.4
    - Cloudflare: 1.1.1.1, 1.0.0.1

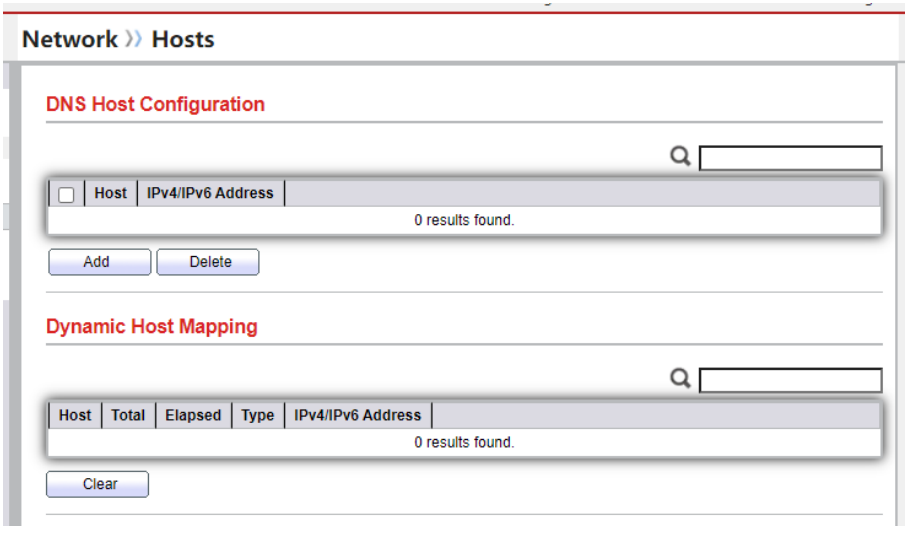
**Пример настройки:**

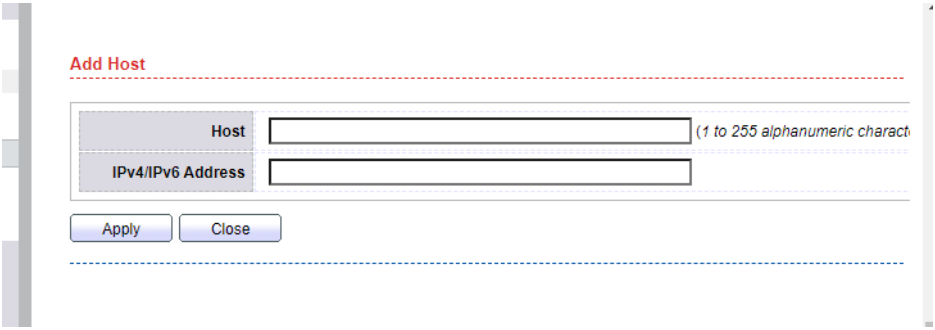
- **DNS Default Name:** switch.local
- **DNS-серверы:** 192.168.1.1 (локальный), 8.8.8.8 (резервный).

## 3.2. Настройка DNS-хостов (DNS Host Configuration)

**Для настройки локальных DNS-записей:**

1. Перейдите в раздел **Network** > **Hosts**.
2. Нажмите кнопку **Add (Добавить)**, чтобы открыть интерфейс настройки.






***Параметры хоста***

| Параметр | Описание |
|---|---|
| **Host** | Имя устройства (например, camera1). |
| **IPv4/IPv6 Address** | Соответствующий IP-адрес (например, 192.168.1.100). |

**Примечания:**

1. Локальные DNS-записи позволяют обращаться к устройствам по именам **без использования внешнего DNS-сервера**.
2. Пример использования:
   - switch1.local → 192.168.1.1
   - nvr.local → 192.168.1.50

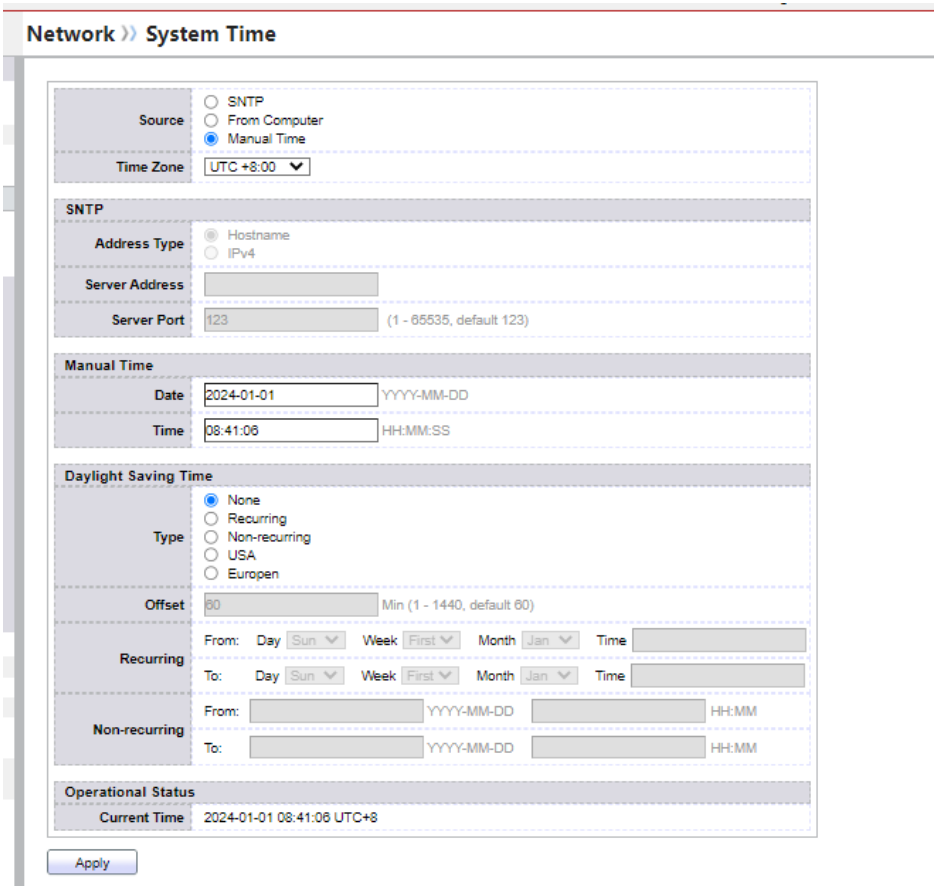
**Рекомендации:**

- Используйте понятные имена для удобства управления сетью.
- Обновляйте записи при изменении IP-адресов устройств.

## 3.3. Настройки системного времени (System Time)

**Для настройки системного времени:**

Перейдите в раздел **Network** > **System Time**.




**Функционал данной страницы WEB интерфейса:**

- Настройка источника времени (NTP, компьютер, ручной ввод)
- Установка часового пояса
- Конфигурация летнего времени (DST)

***Настройки системного времени***

| Параметр | Описание |
|---|---|
| **Source (Источник)** | Выберите источник синхронизации времени: |
| | **SNTP** – синхронизация с NTP-сервером |
| | **From Computer** – использование времени компьютера (браузера) |
| | **Manual Time** – ручная установка времени |
| **Time Zone (Часовой пояс)** | Выберите часовой пояс из списка |

***Настройки SNTP (при выборе источника SNTP)***

| Параметр | Описание |
|---|---|
| **Address Type** | Тип адреса NTP-сервера (IPv4/имя хоста) |
| **Server Address** | Адрес или доменное имя NTP-сервера |
| **Server Port** | Порт NTP-сервера (по умолчанию: 123) |

***Установка времени вручную (Manual Time)***

| Параметр | Описание |
|---|---|
| **Date (Дата)** | Укажите дату вручную |
| **Time (Время)** | Укажите время вручную |

***Настройки летнего времени (Daylight Saving Time)***

| Параметр | Описание |
|---|---|
| **Type (Тип)** | Режим летнего времени: |
| | **Disable** – отключено |
| | **Recurring** – ежегодное (с фиксированными датами) |
| | **Non-Recurring** – разовое (с указанием конкретных дат) |
| | **USA** – по стандарту США (2-е воскресенье марта – |

| Параметр | Описание |
|---|---|
| | 1-е воскресенье ноября) |
| | **European** – по стандарту ЕС (последнее воскресенье марта – октября) |
| **Offset (Смещение)** | Величина коррекции времени (обычно +1 час) |
| **Recurring From/To** | Даты начала/окончания для ежегодного режима |
| **Non-recurring From/To** | Конкретные даты для разового режима |

**Примечания:**

1. **SNTP** требует доступа к NTP-серверу в сети.
2. Часовой пояс влияет на все источники времени.
3. Для **летнего времени** можно выбрать предустановки (США/Европа) или задать вручную.

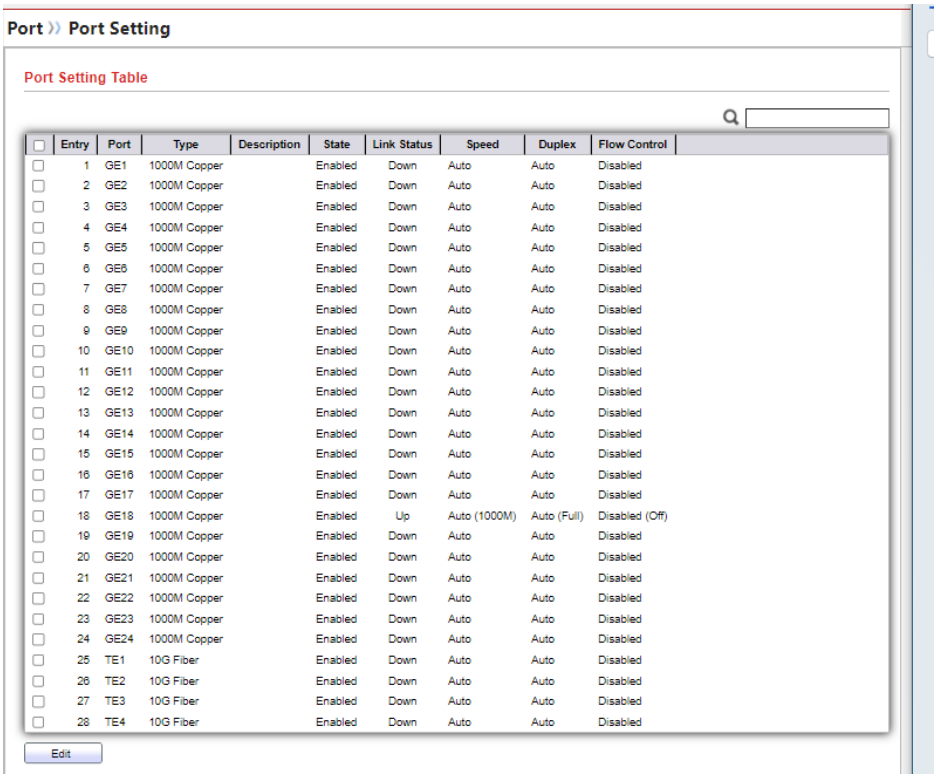
## 4. Порты (Port)

Раздел **Port** предназначен для настройки параметров портов коммутатора.

### 4.1. Настройки портов коммутатора (Port Setting)

**Для настройки параметров портов:**

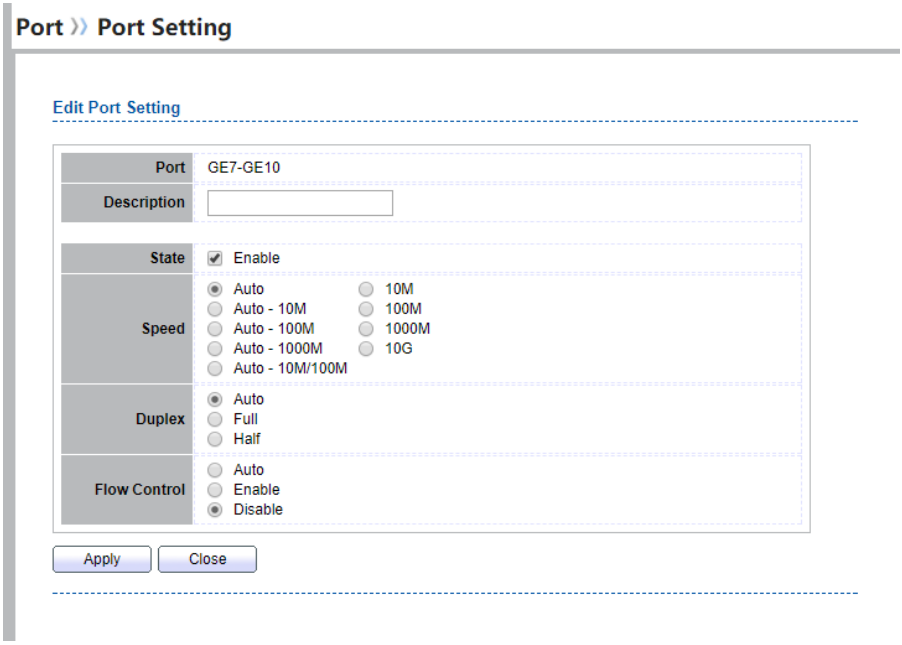
1. Перейдите в раздел **Port** > **Port Setting**.
2. Выберите порт и нажмите кнопку **«Edit» (Изменить)** для редактирования конфигурации.




***Текущее состояние портов***

| Параметр | Описание |
|---|---|
| **Port** | Идентификатор порта |
| **Type** | Тип порта (медиа) |
| **Description** | Описание порта |
| **State** | Состояние порта: |
| | **Enabled (Вкл.)** – порт активирован |
| | **Disabled (Выкл.)** – порт деактивирован |
| **Link Status** | Текущее состояние соединения: |
| | **Up** – соединение установлено |
| | **Down** – соединение отсутствует |

| Параметр | Описание |
|---|---|
| **Speed** | Текущая скорость порта (настройка и фактическое состояние) |
| **Duplex** | Режим дуплекса (настройка и фактическое состояние) |
| **Flow Control** | Управление потоком (настройка и фактическое состояние) |




***Настройки порта (изменение настроек)***

| Параметр | Описание |
|---|---|
| **Port** | Выбранный порт |
| **Description** | Описание порта |
| **State** | Состояние порта: |
| | **Enabled (Вкл.)** |
| | **Disabled (Выкл.)** |
| **Speed** | Настройка скорости: |

| Параметр | Описание |
|---|---|
| | **Auto** – автосогласование (все скорости) |
| | **Auto-10M** – только 10 Мбит/с |
| | **Auto-100M** – только 100 Мбит/с |
| | **Auto-1000M** – только 1000 Мбит/с |
| | **Auto-10M/100M** – 10/100 Мбит/с |
| | **10M** – фиксированная 10 Мбит/с |
| | **100M** – фиксированная 100 Мбит/с |
| | **1000M** – фиксированная 1000 Мбит/с |
| | **10G** – фиксированная 10 Гбит/с (если поддерживается коммутатором) |
| **Duplex** | Режим дуплекса: |
| | **Auto** – автосогласование |
| | **Half** – полудуплекс (только 10/100 Мбит/с) |
| | **Full** – полный дуплекс (1000 Мбит/с и выше) |
| **Flow Control** | Управление потоком: |
| | **Auto** – автосогласование |
| | **Enabled** – включено |
| | **Disabled** – выключено |

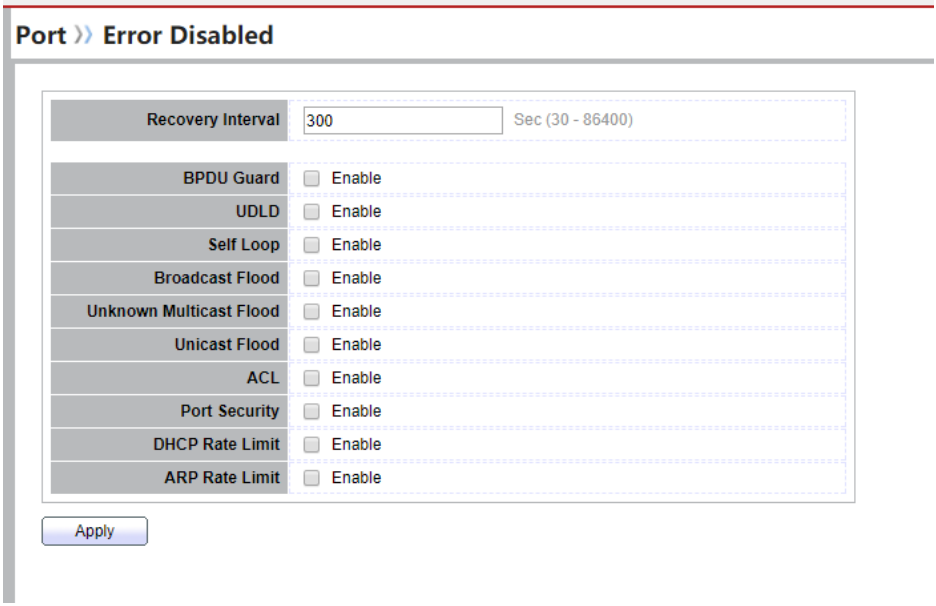
**Примечания:**

1. **Автосогласование (Auto-negotiation)** рекомендуется для большинства сценариев работы.
2. **Flow Control** помогает предотвратить потерю пакетов при перегрузке.
3. Для гигабитных и более скоростных соединений обязателен **полный дуплекс (Full Duplex)**.

## 4.2. Отключение портов по ошибкам (Error Disabled)

**Для настройки параметров автоматического отключения портов:**

Перейдите в раздел **Port** > **Error Disabled**




***Основные параметры***

| Параметр | Описание |
|---|---|
| **Recover Interval** | Интервал автоматического восстановления порта (в секундах) после ошибки. |

***Причины отключения портов***

| Параметр | Описание |
|---|---|
| **BPDU Guard** | Автоматическое отключение порта при получении BPDU-кадров (защита от петель STP). |
| **UDLD** | Автоматическое отключение порта при нарушении двусторонней связи (UniDirectional Link Detection). |

| Параметр | Описание |
|---|---|
| **Self Loop** | Автоматическое отключение порта при обнаружении петли. |
| **Broadcast Flood** | Автоматическое отключение порта при превышении лимита broadcast-трафика. |
| **Unknown Multicast Flood** | Автоматическое отключение порта при превышении лимита неизвестного multicast-трафика. |
| **Unicast Flood** | Автоматическое отключение порта при превышении лимита unicast-трафика. |
| **ACL** | Автоматическое отключение порта при нарушении правил ACL (Access Control List). |
| **Port Security** | Автоматическое отключение порта при нарушении правил безопасности порта (Port Security). |
| **DHCP rate limit** | Автоматическое отключение порта при превышении лимита DHCP-запросов. |
| **ARP rate limit** | Автоматическое отключение порта при превышении лимита ARP-запросов. |

**Примечания:**

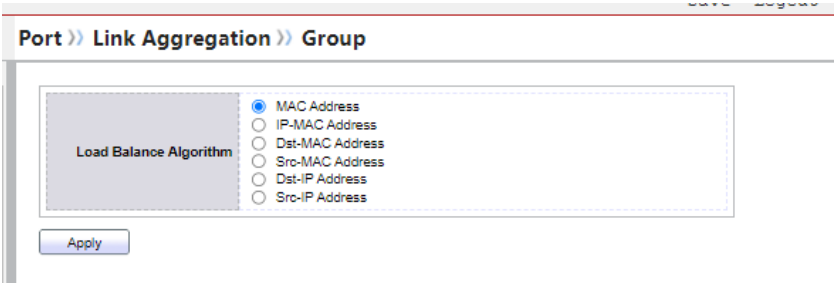
1. **Recover Interval** – порт автоматически восстановится через указанное время (0 = ручное включение).
2. **BPDU Guard** и **Port Security** – наиболее частые причины отключения в защищённых сетях.

## 4.3. Агрегация каналов (Link Aggregation)

### 4.3.1. Настройка групп (Group)

**Для настройки агрегированных групп:**

Перейдите в раздел **Port** > **Link Aggregation** > **Group**




***Алгоритм балансировки нагрузки***

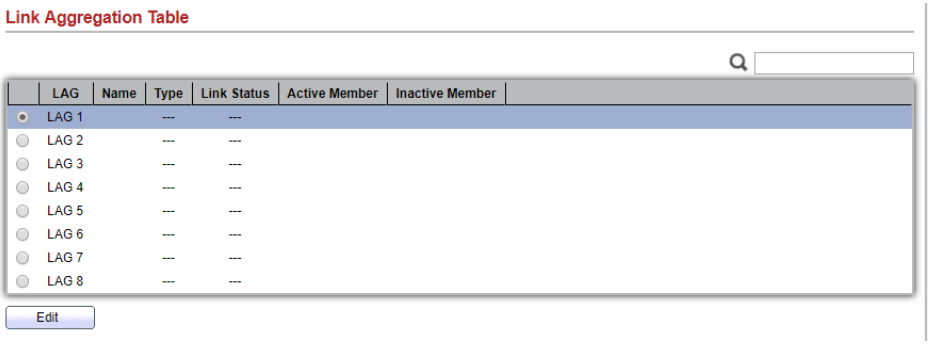
| Параметр | Описание |
|---|---|
| **Load Balance Algorithm** | Алгоритм распределения нагрузки в агрегированной группе: |
| | **MAC Address** – на основе MAC-адресов источника и назначения |
| | **IP-MAC Address** – на основе комбинации IP и MAC-адресов |
| | **Dst-MAC Address** – на основе MAC-адреса назначения |
| | **Src-MAC Address** – на основе MAC-адреса источника |
| | **Dst-IP Address** – на основе IP-адреса назначения |
| | **Src-IP Address** – на основе IP-адреса источника |

**Примечания:**

1. **Алгоритмы балансировки** определяют, как трафик распределяется между портами в агрегированной группе.
2. Рекомендации по выбору алгоритма:
    - **Mac Address/IP-MAC** – для общего использования (универсальный вариант).
    - **Dst-IP/Src-IP** – если в сети преобладает трафик между конкретными IP-адресами (например, серверами).
    - **Dst-MAC/Src-MAC** – для сетей с большим количеством устройств.

**Пример настройки:**

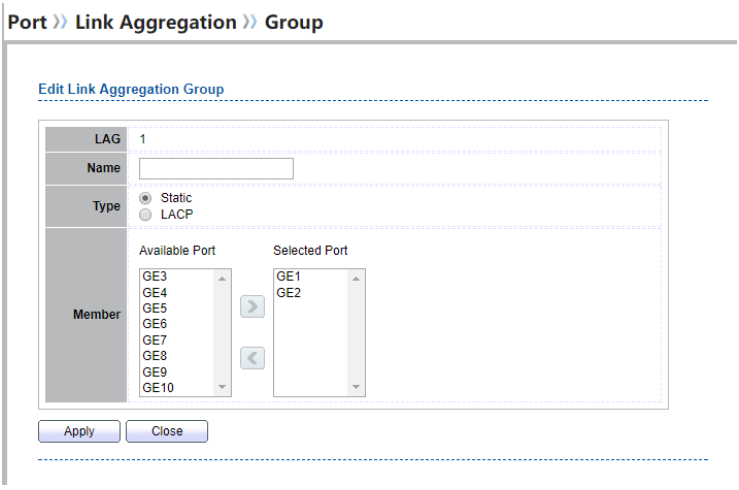
- **Алгоритм: IP-MAC Address** (оптимален для смешанного трафика).




***Список агрегированных групп***

| Параметр | Описание |
|---|---|
| **LAG** | Идентификатор LAG-группы |
| **Name** | Описание группы |
| **Type** | Тип агрегации: |
| | **Static** – порты всегда активны в группе |
| | **LACP** – активные порты определяются протоколом LACP |

| Параметр | Описание |
|---|---|
| **Link Status** | Текущее состояние группы (активна/неактивна) |
| **Active Member** | Список активных портов в группе |
| **Inactive Member** | Список неактивных портов в группе |




***Настройка группы (редактирование)***

| Параметр | Описание |
|---|---|
| **LAG** | Идентификатор выбранной LAG-группы |
| **Name** | Описание группы |
| **Type** | Тип агрегации: |
| | **Static** – статическая агрегация |
| | **LACP** – динамическая агрегация (с использованием протокола LACP) |
| **Member** | Выбор портов для включения в группу |

**Примечания:**

1. **Статическая агрегация (Static)** проще в настройке, но менее гибкая.
2. **LACP (IEEE 802.3ad)** обеспечивает автоматическое управление составом группы.
3. Алгоритм **src-dst-mac-ip (IP-MAC Address)** обеспечивает более равномерное распределение трафика.

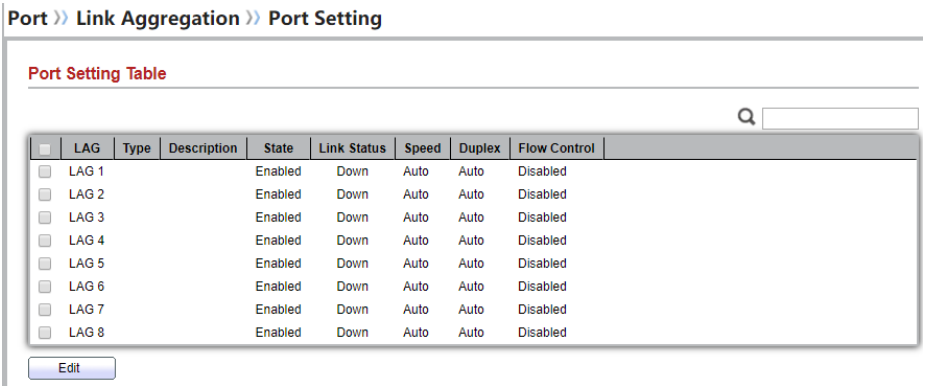
**Рекомендации:**

- Для критически важных соединений используйте **LACP**.

### 4.3.2. Настройки портов агрегации (Port Setting)

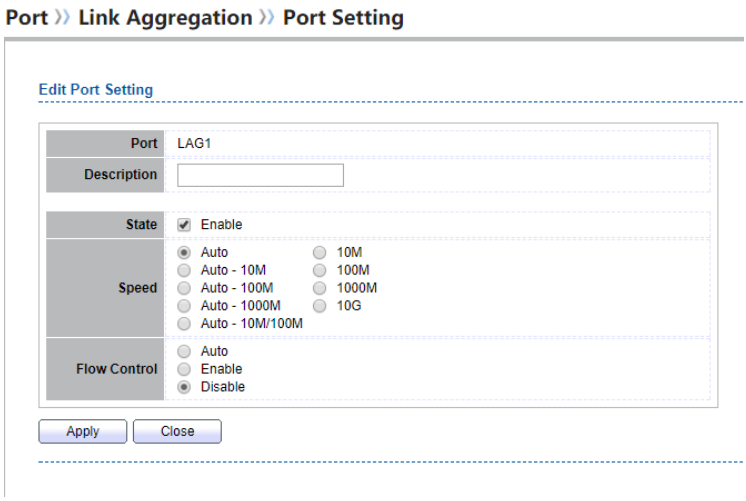
**Для настройки параметров портов в агрегированной группе:**

1. Перейдите в раздел **Port** > **Link Aggregation** > **Port Setting**.
2. Выберите порт LAG и нажмите кнопку **«Edit» (Изменить)** для редактирования конфигурации.




**Текущее состояние портов LAG**

| Параметр | Описание |
|---|---|
| **LAG** | Имя агрегированного порта |
| **Type** | Тип порта (медиа) |
| **Description** | Описание порта |
| **State** | Административное состояние: |
| | **Enabled (Вкл.)** – порт активирован |
| | **Disabled (Выкл.)** – порт деактивирован |
| **Link Status** | Текущее состояние соединения: |
| | **Up** – соединение установлено |
| | **Down** – соединение отсутствует |
| **Speed** | Текущая скорость порта (настройка и фактическое состояние) |
| **Duplex** | Режим дуплекса (настройка и фактическое состояние) |
| **Flow Control** | Управление потоком (настройка и фактическое состояние) |




**Редактирование настроек портов LAG**

| Параметр | Описание |
|---|---|
| **Port** | Выбранные порты |
| **Description** | Описание порта |
| **State** | Состояние порта |
| | **Enable (Вкл.)** |
| | **Disable (Выкл.)** |
| **Speed** | Настройка скорости: |
| | **Auto** – автосогласование (все скорости) |
| | **Auto-10M** – только 10 Мбит/с |
| | **Auto-100M** – только 100 Мбит/с |
| | **Auto-1000M** – только 1000 Мбит/с |
| | **Auto-10M/100M** – 10/100 Мбит/с |
| | **10M** – фиксированная 10 Мбит/с |
| | **100M** – фиксированная 100 Мбит/с |
| | **1000M** – фиксированная 1000 Мбит/с |
| | **10G** – фиксированная 10 Гбит/с (если поддерживается коммутатором) |
| **Flow Control** | Управление потоком: |
| | **Auto** – автосогласование |
| | **Enabled** – включено |
| | **Disabled** – выключено |

**Примечания:**

1. Для портов в агрегированной группе рекомендуется использовать **одинаковые настройки** скорости и дуплекса.
2. **Автосогласование (Auto-negotiation)** – предпочтительный режим для большинства сценариев.

3. **Flow Control** помогает предотвратить перегрузку буферов портов.

**Рекомендации:**

- Для гигабитных соединений используйте **1000M Full Duplex**.
- При использовании LACP убедитесь, что все порты группы имеют **одинаковые настройки**.

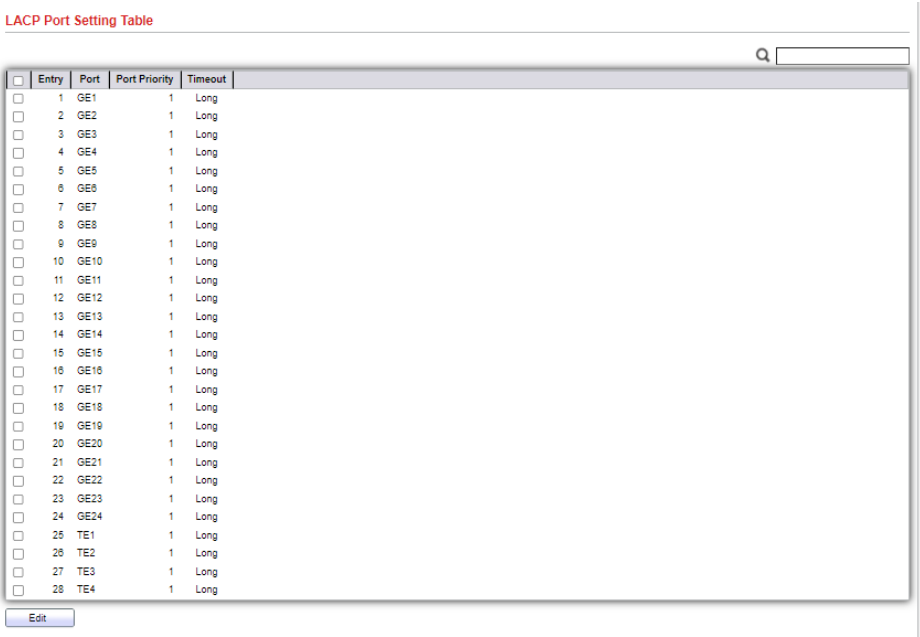
### 4.3.3. Настройки протокола LACP (LACP)

**Для конфигурации параметров протокола LACP:**

1. Перейдите в раздел **Port** > **Link Aggregation** > **LACP**.
2. Выберите порты и нажмите кнопку **«Edit» (Изменить)** для настройки.

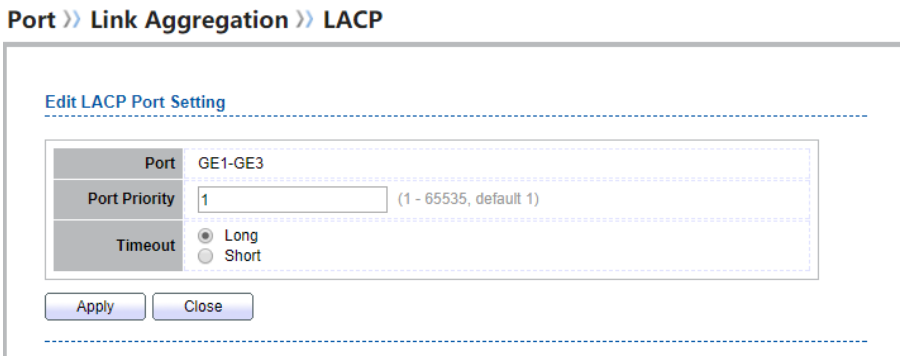

***Глобальные параметры LACP***

| Параметр | Описание |
|---|---|
| **System Priority** | Приоритет системы LACP (влияет на выбор активного устройства при агрегации). |




***Текущие настройки портов LACP***

| Параметр | Описание |
|---|---|
| **Port** | Имя порта |
| **Port Priority** | Приоритет порта в LACP (чем меньше значение, тем выше приоритет). |
| **Timeout** | Интервал отправки LACP-пакетов: |
| | **Long (Длинный)** – 30 секунд (рекомендуется для стабильных сетей) |
| | **Short (Короткий)** – 1 секунда (быстрое обнаружение изменений) |




***Редактирование настроек портов LACP***

| Параметр | Описание |
|---|---|
| **Port** | Выбранные порты |
| **Port Priority** | Укажите приоритет порта (0–65535, чем меньше – тем выше приоритет). |
| **Timeout** | Выберите интервал отправки LACP-пакетов: |
| | • **Long (Длинный)** – 30 секунд |
| | • **Short (Короткий)** – 1 секунда |

**Примечания:**

1. **System Priority** определяет, какое устройство будет "активным" в агрегированной группе.
2. **Port Priority** влияет на выбор активных портов при избыточной конфигурации.
3. **Short Timeout** обеспечивает быструю реакцию на изменения, но увеличивает нагрузку на сеть.

**Рекомендации:**

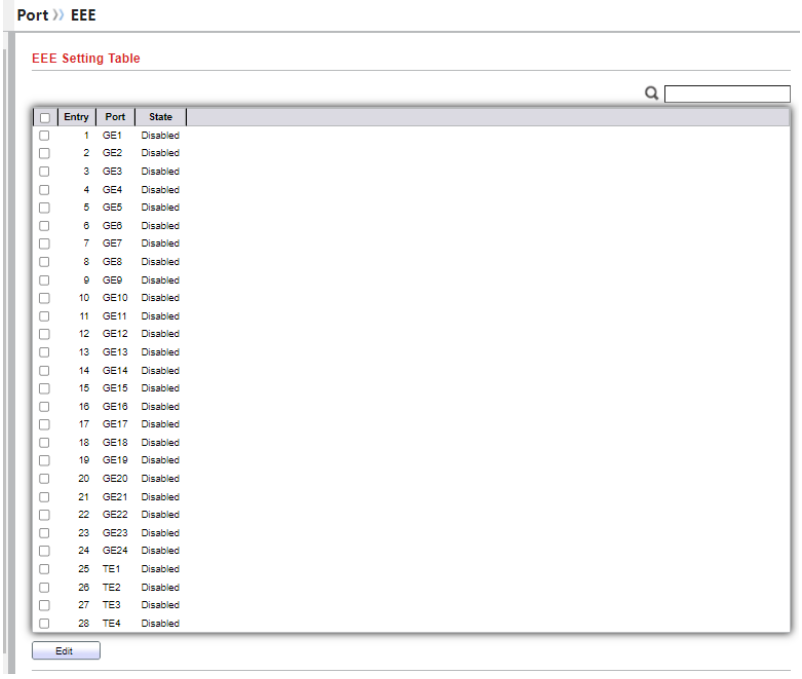
- Для стабильных сетей используйте **Long Timeout (30 сек)**.
- Для критически важных соединений установите **более высокий приоритет (меньшее значение)**.

## 4.4. Настройки Energy Efficient Ethernet, IEEE 802.3az (EEE)

**Для настройки параметров EEE:**

Перейдите в раздел **Port** > **EEE**.

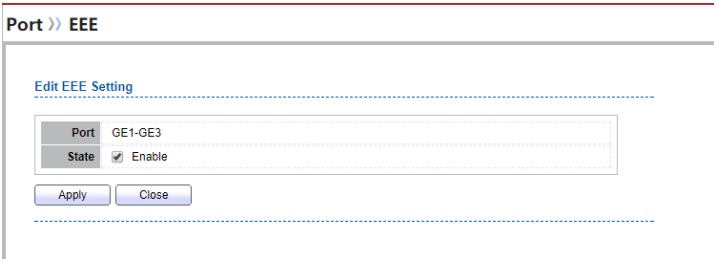
**Функционал страницы:**
Позволяет настроить энергоэффективный режим работы Ethernet-портов (IEEE 802.3az).




***Текущие параметры EEE***

| Параметр | Описание |
|---|---|
| **Port** | Идентификатор порта |
| **State** | Состояние EEE: |
| | **Enabled** - EEE включен |
| | **Disabled** - EEE выключен |

| Параметр | Описание |
|---|---|
| **Operational Status** | Фактический статус работы EEE: |
| | **Enabled** - EEE активен |
| | **Disabled** - EEE неактивен |




***Настройки EEE (редактирование)***

| Параметр | Описание |
|---|---|
| **Port** | Выбранные порты для настройки |
| **State** | Управление режимом EEE: |
| | **Enable** - включить EEE |
| | **Disable** - выключить EEE |

**Примечания:**

1. Energy Efficient Ethernet (IEEE 802.3az) позволяет снизить энергопотребление портов при низкой нагрузке
2. Для работы EEE требуется поддержка на обоих концах соединения
3. Включение EEE может незначительно увеличить задержку передачи данных

**Рекомендации:**

- Включите EEE для портов, где критично энергопотребление
- Для портов с чувствительными к задержкам приложениями (VoIP, видео) рекомендуется отключить EEE

## 4.5. Настройка Jumbo Frame (Jumbo Frame)

**Для настройки параметров Jumbo Frame:**

Перейдите в раздел **Port** > **Jumbo Frame**.

**Функционал страницы:**
Позволяет настроить поддержку кадров увеличенного размера (Jumbo Frame) на коммутаторе.


| Параметр | Описание |
|---|---|
| **Jumbo Frame** | Включение/выключение поддержки Jumbo Frame: |
| | **Enabled** - при активации позволяет настраивать максимальный размер кадра |
| | **Disabled** - используется стандартный максимальный размер кадра (1522 байта) |

**Примечания:**

1. Jumbo Frame поддерживают передачу кадров размером до 9000+ байт (вместо стандартных 1522 байт)
2. Для работы Jumbo Frame требуется поддержка на всех устройствах пути передачи
3. Использование Jumbo Frame может:
    - Увеличить пропускную способность для передачи «тяжелого» трафика
    - Снизить нагрузку на процессор
    - Уменьшить количество прерываний

**Рекомендации:**

- Включайте Jumbo Frame только если вся сеть поддерживает эту функцию
- Оптимально использовать для:
  - Серверных соединений
  - Хранилищ данных (SAN)
  - Видеотрафика
- Стандартное значение (1522 байта) подходит для большинства обычных сетевых задач

## 5. VLAN

Виртуальная локальная сеть (**VLAN**) – это группа устройств с общими требованиями, которые взаимодействуют так, как если бы они находились в одном широковещательном домене, независимо от их физического расположения. VLAN обладает теми же характеристиками, что и физическая локальная сеть (**LAN**), но позволяет объединять устройства, даже если они подключены к разным коммутаторам.

Порты–участники в VLAN настрайваются программно, без необходимости физического перемещения устройств или изменения подключений.

### 5.1. Настройки VLAN (VLAN)

Раздел **VLAN** предназначен для настройки параметров виртуальных локальных сетей.

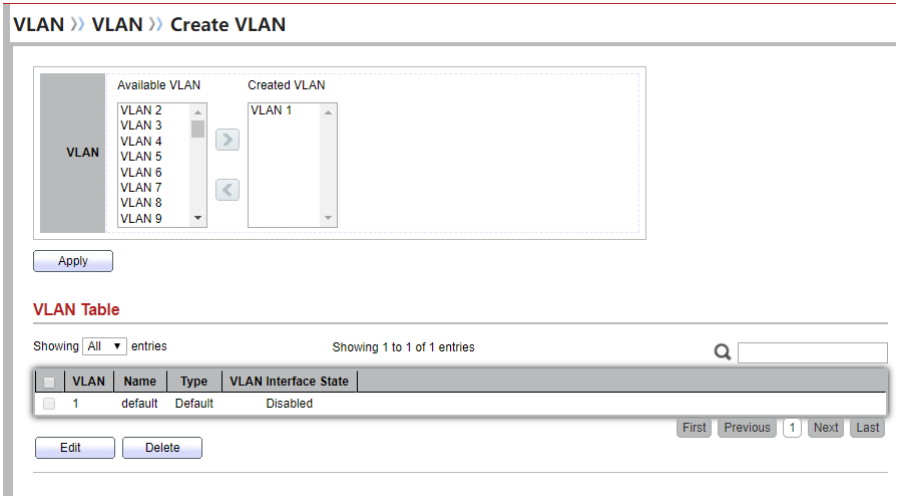
### 5.1.1. Создание VLAN (Create VLAN)

**Чтобы создать VLAN:**

Перейдите в раздел **VLAN** > **VLAN** > **Create VLAN**.

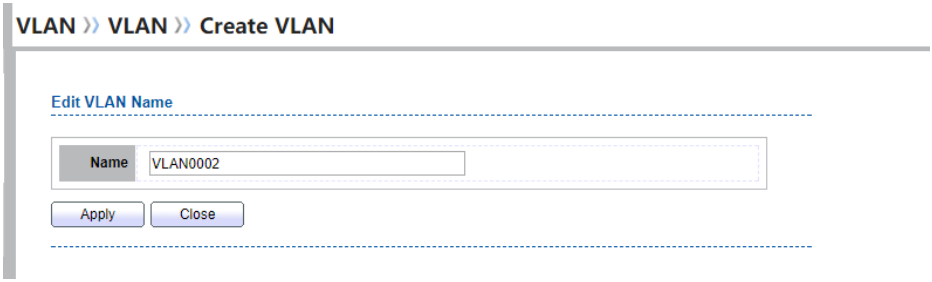
**Функционал страницы:**

- Добавление или удаление идентификаторов VLAN (**VLAN ID**)
- Просмотр всех VLAN, добавленных вручную (**статически**) или автоматически (**через GVRP**)
- Возможность редактирования имени VLAN




***Настройки VLAN***

| Параметр | Описание |
|---|---|
| **Available VLAN** | Список доступных VLAN, которые еще не созданы. |
| | Выберите VLAN из левого окна и перенесите в правое для добавления. |
| **Created VLAN** | Список созданных VLAN. |
| | Выберите VLAN из правого окна и перенесите в левое для удаления. |




| Параметр | Описание |
|---|---|
| **Name** | Введите имя VLAN (уникальное для каждой VLAN). |

**Примечания:**

1. **VLAN ID** – числовой идентификатор (1–4094), где:
   - **1** – используется по умолчанию для управления.
   - **2–1001** – стандартный диапазон для пользовательских VLAN.
   - **1006–4094** – расширенный диапазон (требует поддержки на оборудовании).

2. **GVRP (GARP VLAN Registration Protocol)** – протокол для автоматической регистрации VLAN между коммутаторами.

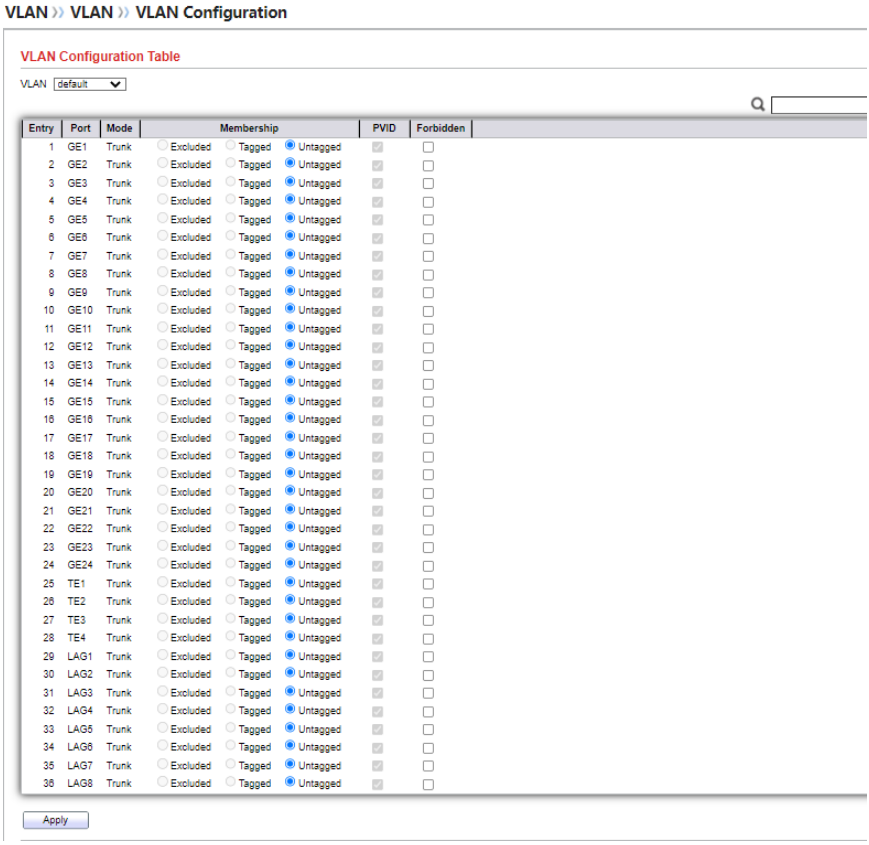
**Рекомендации:**

- Используйте понятные имена (**например, "Office" или "Servers"**) для удобства управления.
- Избегайте удаления VLAN, которые используются активными устройствами.

### 5.1.2. Конфигурация VLAN (VLAN Configuration)

**Для настройки портов – учатстинков в VLAN:**

1. Перейдите в раздел **VLAN** > **VLAN** > **VLAN Configuration**.
2. Выберите VLAN ID для настройки.




***Параметры конфигурации VLAN***

| Параметр | Описание |
|---|---|
| **VLAN** | Выберите VLAN ID для настройки. |
| **Port** | Физический интерфейс порта. |
| **Mode** | Режим VLAN на порту (отображается текущее состояние). |

| Параметр | Описание |
|---|---|
| Membership | Настройка членства порта в VLAN: |
| | **Forbidden** – порт запрещён в VLAN (блокировка) |
| | **Excluded** – порт исключён из VLAN (по умолчанию) |
| | **Tagged** – порт передаёт трафик с тегами VLAN (для межкоммутаторных соединений) |
| | **Untagged** – порт передаёт трафик без тегов (для конечных устройств) |
| PVID | Отображает, является ли VLAN PVID (Port VLAN ID) для порта. |

**Ключевые термины:**

- **Tagged (Тегированный)** – используется для соединений между коммутаторами (802.1Q).
- **Untagged (Не тегированный)** – для подключения конечных устройств (ПК, IP-камеры).
- **PVID (Port VLAN ID)** – VLAN по умолчанию для untagged-трафика на порту.

**Пример настройки:**

- **Порт 1:** Untagged в VLAN 10 (офисные ПК)
- **Порт 24:** Tagged в VLAN 10 и 20 (магистраль к другому коммутатору)

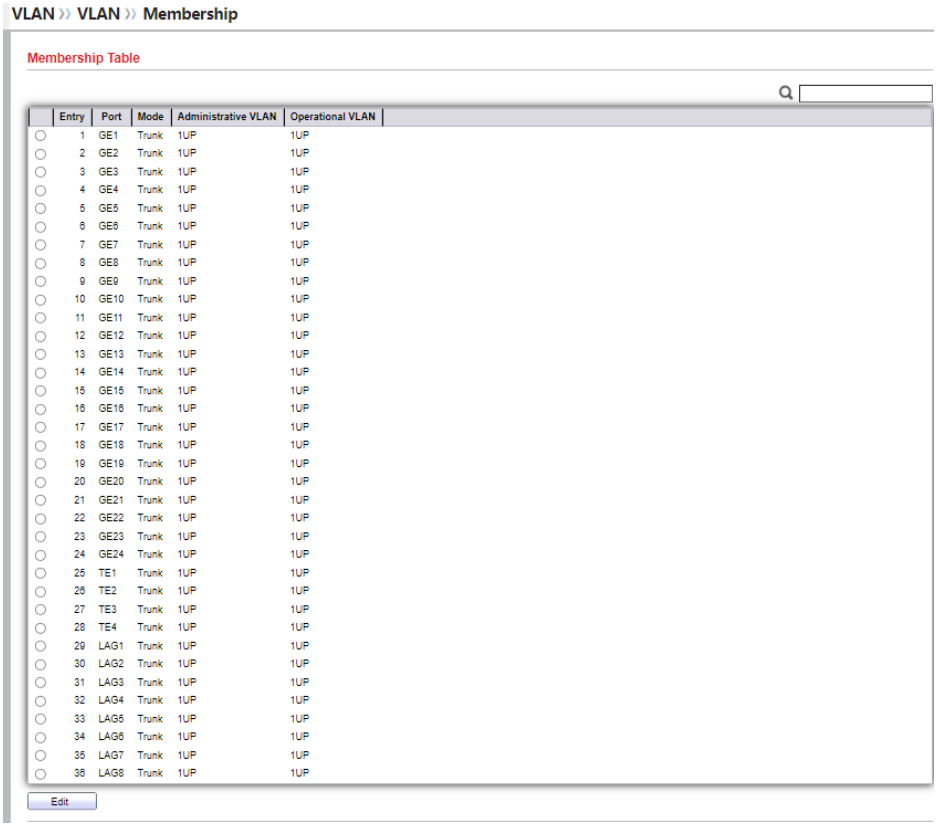
**Примечания:**

1. **Forbidden** – полностью блокирует VLAN на порту.
2. **Excluded** – порт не принадлежит VLAN, но может быть добавлен.

### 5.1.3. Настройка VLAN Membership (Membership)

**Для просмотра и настройки портов участников в VLAN:**

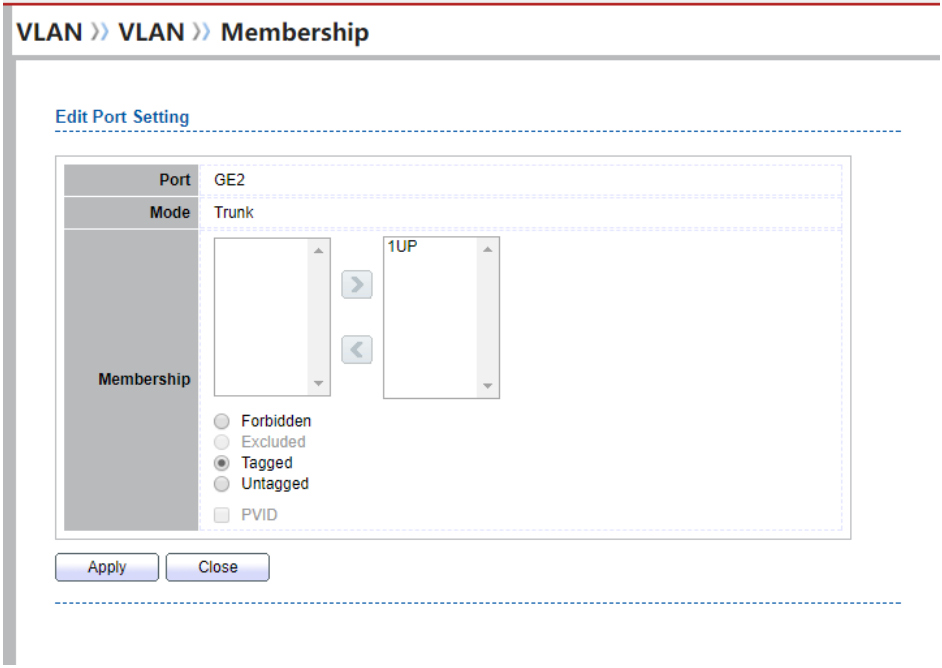
Перейдите в раздел **VLAN** > **VLAN** > **Membership**




***Текущие параметры портов***

| Параметр | Описание |
|---|---|
| **Port** | Физический интерфейс порта. |
| **Mode** | Режим VLAN на порту (например, Access, Trunk, Hybrid). |
| **Administrative** | Список VLAN, назначенных порту администратором |

| Параметр | Описание |
|---|---|
| **VLAN** | (настроенные вручную). |
| **Operational VLAN** | Фактический список VLAN, в которых работает порт. Может отличаться от Administrative VLAN. |




***Настройка портов-участников VLAN***

| Параметр | Описание |
|---|---|
| **Port** | Выбранный порт. |
| **Mode** | Текущий режим VLAN порта. |
| **Membership** | Настройка порта участника VLAN. Выберите VLAN из левого списка. Укажите тип порта – участника: |
| | **Forbidden** – порт запрещён в VLAN. |
| | **Tagged** – порт передаёт трафик с тегами VLAN (для |

| Параметр | Описание |
|---|---|
| | магистральных соединений). |
| | **Untagged** – порт передаёт трафик без тегов (для конечных устройств). |
| | **PVID** – VLAN по умолчанию для untagged-трафика. |

**Ключевые особенности:**

- **Administrative VLAN** и **Operational VLAN**:
  - Administrative – настройки, введённые вручную.
  - Operational – фактические VLAN, которые активны на порту (например, после применения GVRP).
- **PVID (Port VLAN ID)**:
  - Автоматически назначается для untagged-трафика.
  - Нельзя изменить, если порт находится в определённых режимах (например, Forbidden).

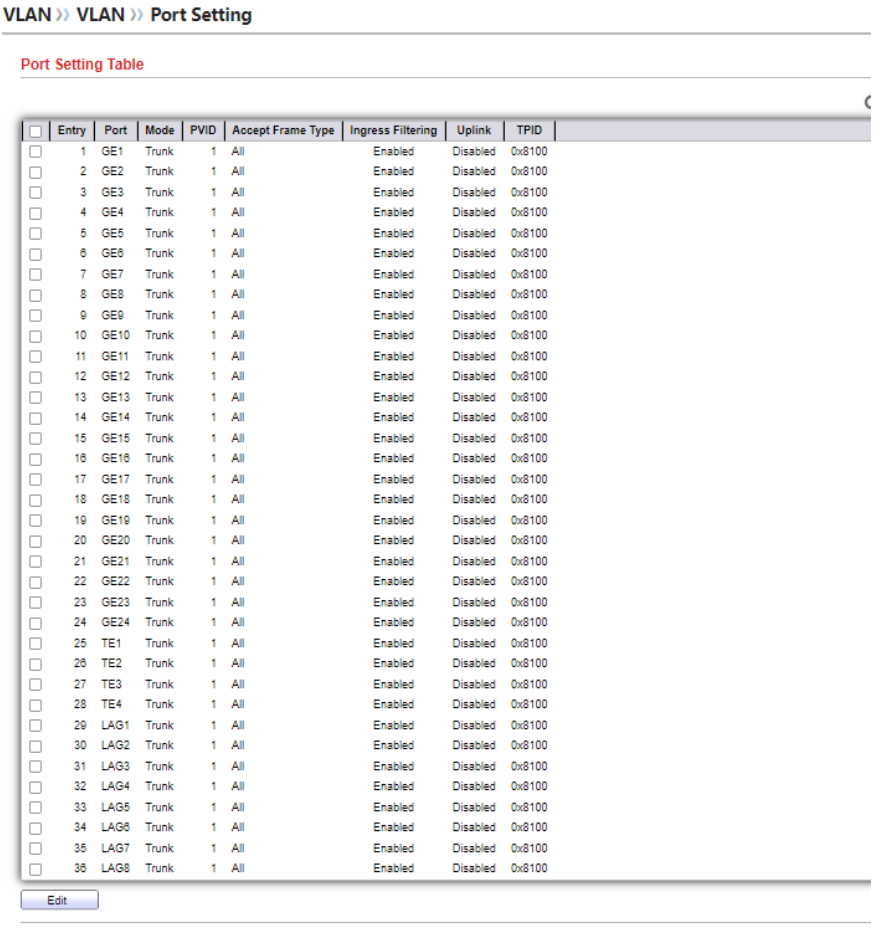
**Пример настройки:**

- **Порт 1:**
  - **Mode:** Access
  - **Untagged VLAN:** 10
  - **PVID:** 10
- **Порт 24:**
  - **Mode:** Trunk
  - **Tagged VLAN:** 10, 20, 30
  - **PVID:** 1 (управление)

### 5.1.4. Настройка портов VLAN (Port Setting)

**Для настройки параметров VLAN на портах:**

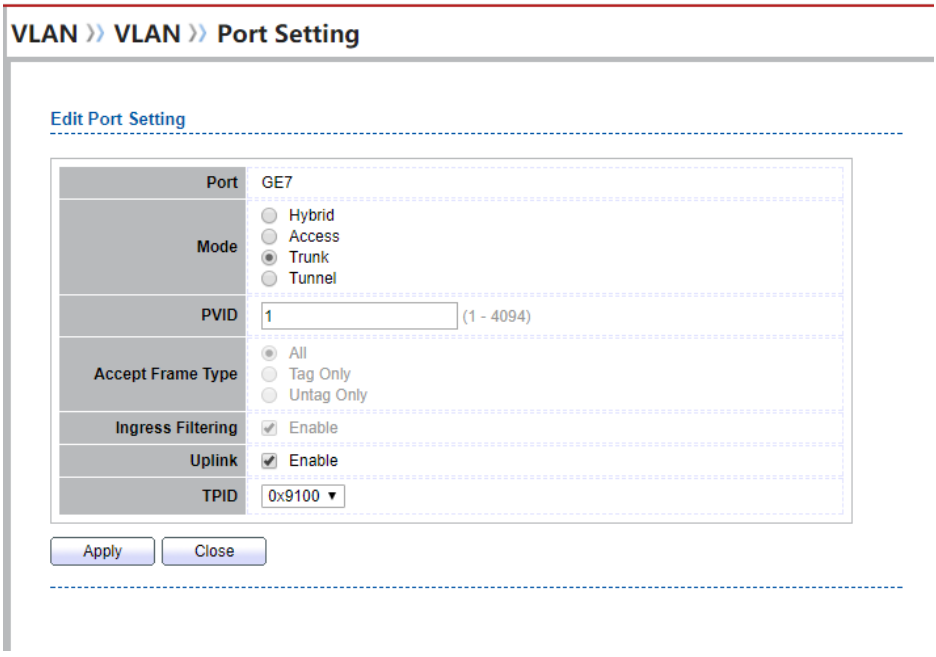
Перейдите в раздел **VLAN** > **VLAN** > **Port Setting**.




***Текущие параметры портов***

| Параметр | Описание |
|---|---|
| **Port** | Идентификатор порта. |
| **Mode** | Текущий режим VLAN порта (Hybrid, Access, Trunk). |

| Параметр | Описание |
|---|---|
| **PVID** | Port VLAN ID (идентификатор VLAN по умолчанию для untagged-трафика). |
| **Accept Frame Type** | Тип принимаемых кадров (зависит от режима). |
| **Ingress Filtering** | Состояние фильтрации входящего трафика (вкл./выкл.). |
| **Uplink** | Режим uplink (используется для восходящих соединений). |
| **TPID** | Tag Protocol Identifier (идентификатор тега VLAN) |




***Редактирование параметров портов***

| Параметр | Описание |
|---|---|
| **Port** | Выбранный порт для настройки. |

| Параметр | Описание |
|---|---|
| **Mode** | Выберите режим VLAN: |
| | **Hybrid** – поддерживает все функции IEEE 802.1Q (тегированные и untagged-кадры). |
| | **Access** – принимает только untagged-кадры и принадлежит одной VLAN. |
| | **Trunk** – передаёт тегированные кадры для нескольких VLAN. |
| **PVID** | Укажите PVID (1–4094). Доступно только для режимов **Hybrid** и **Trunk**. |
| **Accepted Type** | Тип принимаемых кадров (только для режима **Hybrid**): |
| | **All** – все кадры (тегированные и untagged). |
| | **Tag only**– только тегированные кадры. |
| | **Untag Only** – все кадры (тегированные и untagged). |
| **Ingress Filtering** | Включите/отключите фильтрацию входящего трафика (только для **Hybrid** режима). |
| **Uplink** | Включите/отключите режим uplink (только для **Trunk** режима). |
| **TPID** | Выберите TPID (например, 0x8100 для стандартного VLAN). Доступно только для **Trunk** режима |

**Примечания:**

1. **Режимы портов:**
   - **Access** – для подключения конечных устройств (ПК, камеры).
   - **Trunk** – для соединения между коммутаторами.
   - **Hybrid** – гибкий режим (поддержка тегированных и untagged-кадров).

2. **PVID** – VLAN, в которую попадает untagged-трафик.
3. **Ingress Filtering** – если включено, порт отбрасывает кадры с тегами VLAN, в которых он не состоит.

**Примеры конфигурации:**

- **Access-порт (PVID=10):**
  - Режим: Access
  - Принимает только untagged-трафик и относит его к VLAN 10.
- **Trunk-порт (PVID=1, Tagged VLANs=10,20,30):**
  - Режим: Trunk
  - Передаёт тегированные кадры для VLAN 10, 20, 30.
  - Untagged-трафик попадает в VLAN 1 (управление).

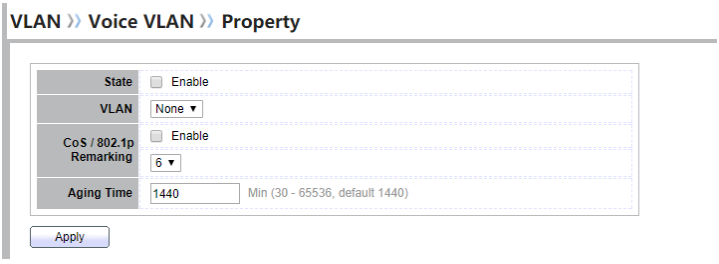
## 5.2. Голосовая VLAN (Voice VLAN)

Раздел **Voice VLAN** предназначен для настройки VLAN, оптимизированной для передачи голосового трафика (VoIP).

### 5.2.1. Свойства Voice VLAN (Property)

**Для настройки глобальных параметров и параметров портов Voice VLAN:**

Перейдите в раздел **VLAN** > **Voice VLAN** > **Property**



***Глобальные настройки Voice VLAN***

| Параметр | Описание |
|---|---|
| **State** | Включение/отключение функции Voice VLAN. |
| **VLAN** | Идентификатор Voice VLAN (не может совпадать с VLAN по умолчанию). |
| **Cos/802.1p** | Приоритет VLAN (VPT) для голосового трафика (0–7). |
| **Remarking** | Включение/отключение перемаркировки приоритета (802.1p). |
| **Aging Time** | Время жизни записей Voice VLAN (по умолчанию: 1440 минут). |

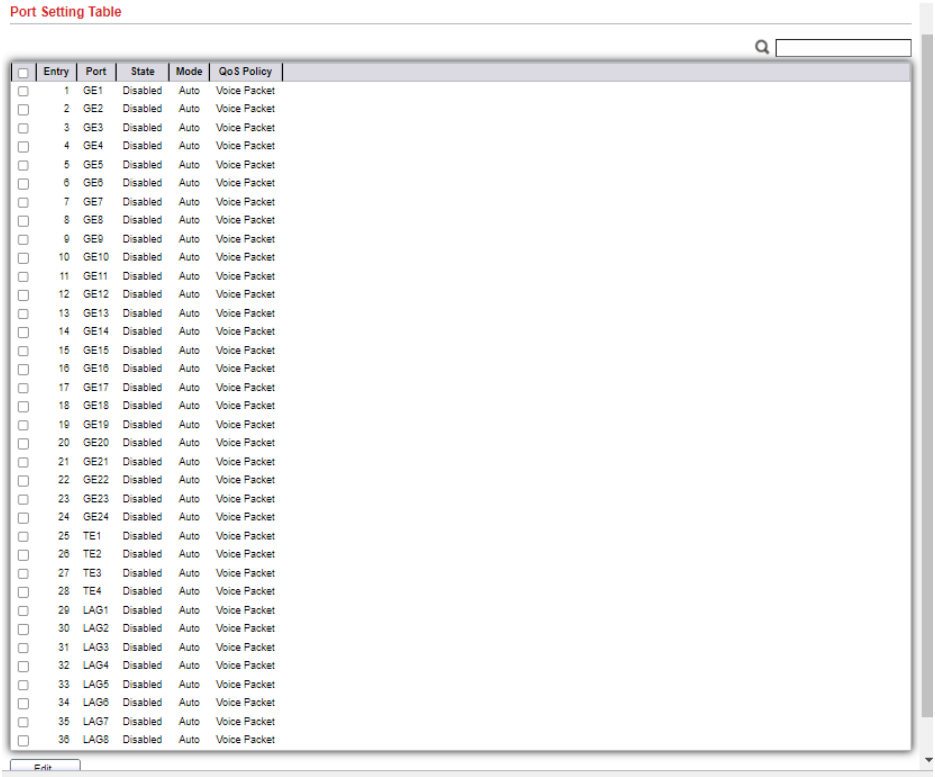
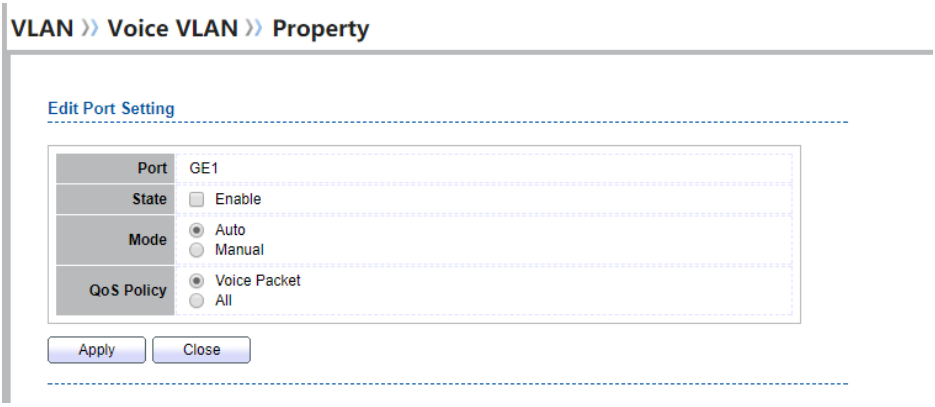


***Таблица текущих параметров портов***

| Параметр | Описание |
|---|---|
| **Port** | Идентификатор порта. |
| **State** | Состояние Voice VLAN на порту (вкл./выкл.). |
| **Mode** | Режим работы Voice VLAN (Auto/Manual). |
| **QoS Policy** | Тип пакетов, к которым применяются QoS-атрибуты. |




***Редактирование параметров портов***

| Параметр | Описание |
|---|---|
| **Port** | Выбранный порт. |
| **State** | Включение/отключение Voice VLAN на порту. |
| **Mode** | Выберите режим работы: |
| | **Auto** – автоматическое добавление порта в Voice VLAN при обнаружении голосового трафика. |
| | **Manual** – ручное добавление порта в Voice VLAN. |
| **QoS Policy** | Политика QoS: |
| | **Voice Packet** – QoS применяется только к пакетам с MAC-адресами из OUI-таблицы. |
| | **All** – QoS применяется ко всем пакетам в Voice VLAN. |

**Примечания:**

1. **OUI (Organizationally Unique Identifier)** – идентификатор производителя VoIP-устройств (например, Cisco, Yealink).
2. **Режим Auto** удобен для IP-телефонов, которые автоматически определяются по MAC-адресу.
3. **Приоритет (802.1p)** обеспечивает качество обслуживания (QoS) для голосового трафика.

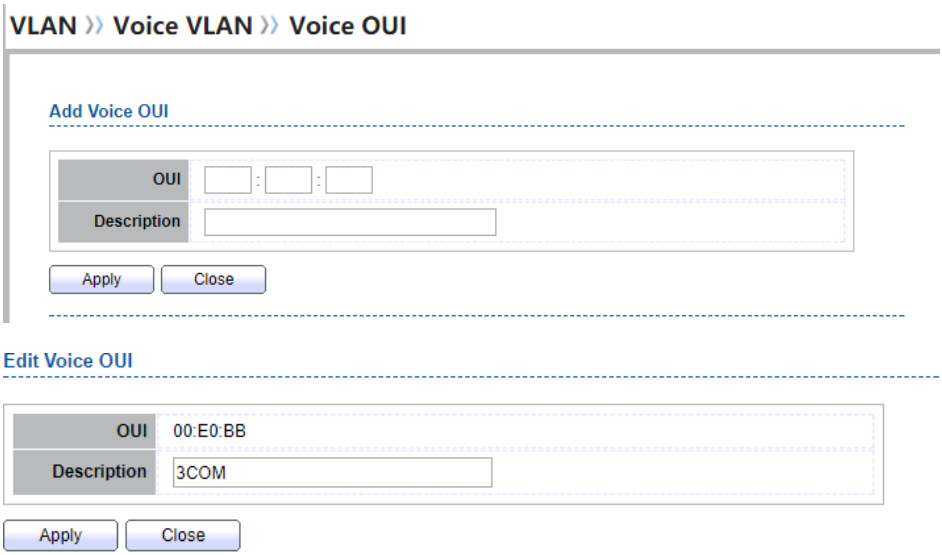
### 5.2.2. Голосовые OUI адреса (Voice OUI)

**Для настройки OUI-адресов VoIP-устройств:**

Перейдите в раздел **VLAN** > **Voice VLAN** > **Voice OUI**.


***Текущие OUI-адреса***

| Параметр | Описание |
|---|---|
| **OUI** | MAC-адрес производителя VoIP-устройства (первые 6 символов, например, 00-01-02). |
| **Description** | Описание производителя (например, "Cisco IP Phone"). |




***Добавление/редактирование OUI***

| Параметр | Описание |
|---|---|
| **OUI** | Введите OUI MAC-адрес (формат: XX-XX-XX или XXXXXX). **Нельзя изменить при редактировании.** |
| **Description** | Укажите описание (например, модель устройства или производитель). |

**Примечания:**

1. **OUI (Organizationally Unique Identifier)** – уникальный идентификатор производителя сетевых устройств.
2. По умолчанию в таблице есть 8 предопределённых OUI (например, для Cisco).
3. Голосовая VLAN автоматически распознаёт трафик от устройств с указанными OUI.

**Пример добавления OUI:**

- **OUI:** A4-B1-C2
- **Description:** "Yealink IP Phone T4 Series"

**Рекомендации:**

- Добавляйте OUI для всех VoIP-устройств в сети.
- Используйте описания для удобства управления (например, "3CX Phones")

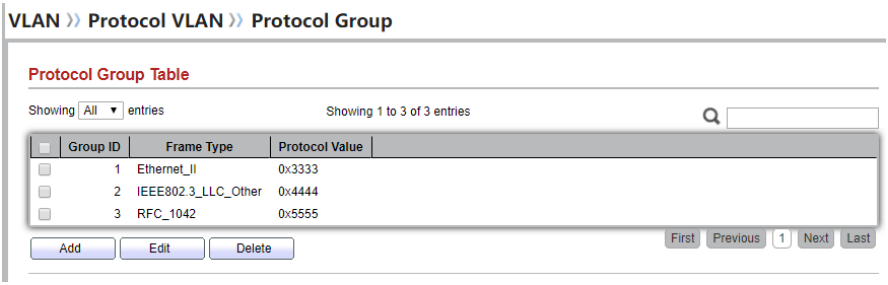
## 5.3. VLAN на основе протоколов (Protocol VLAN)

Раздел **Protocol VLAN** позволяет настраивать VLAN на основе типа протокола в заголовке пакета.

### 5.3.1. Группы протоколов VLAN (Protocol Group)

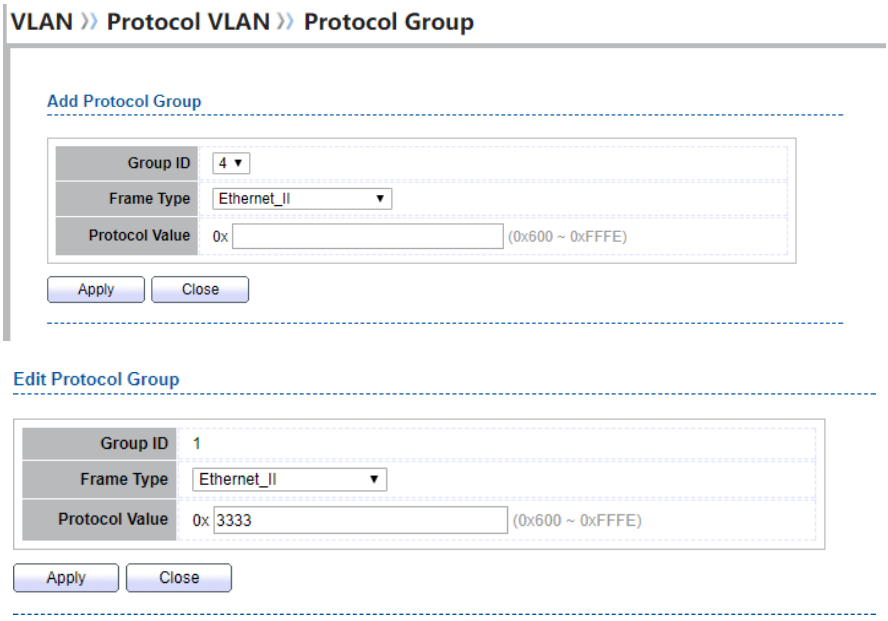
**Для настройки групп протоколов:**

Перейдите в раздел **VLAN** > **Protocol VLAN** > **Protocol Group**.




***Текущие группы протоколов***

| Параметр | Описание |
|---|---|
| **Group ID** | Идентификатор группы |
| **Frame Type** | Тип кадра |
| **Protocol Value** | Значение протокола в HEX формате. Пакеты с этим значением относятся к указанной VLAN. |




***Добавление/редактирование группы***

| Параметр | Описание |
|---|---|
| **Group ID** | Выберите ID группы (1–8). |
| **Frame Type** | Укажите тип кадра из списка. |
| | **Ethernet_II** (например, для IP-трафика). |
| | **IEEE802.3_LLC_Other** (для протоколов с LLC-заголовком). |
| | **RFC_1042** (для инкапсуляции IPX/SPX). |
| **Protocol Value** | Введите значение протокола (например, 0x0800 для IPv4). Пакеты с этим значением относятся к указанной VLAN. |

**Примечания:**

1. **Protocol VLAN** используется для разделения трафика по типу протокола (например, IPv4, IPX, AppleTalk).
2. **Примеры Protocol Value:**
   - 0x0800 – IPv4

- 0x0806 – ARP
- 0x8137 – IPX

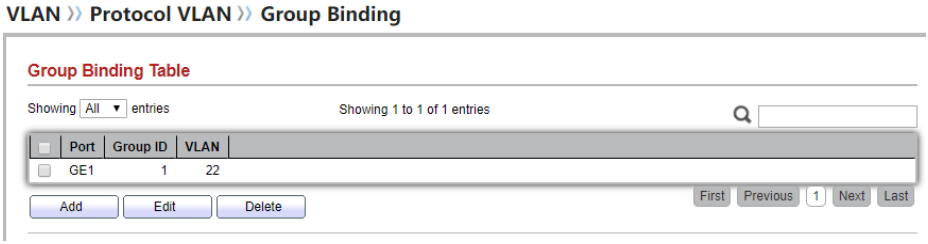
**Рекомендации:**

- Для VoIP-трафика можно создать отдельную группу с типом **Ethernet_II** и значением 0x0800.
- Группы 1–8 позволяют гибко классифицировать трафик без использования тегов VLAN.

### 5.3.2. Привязка групп протоколов (Group Binding)

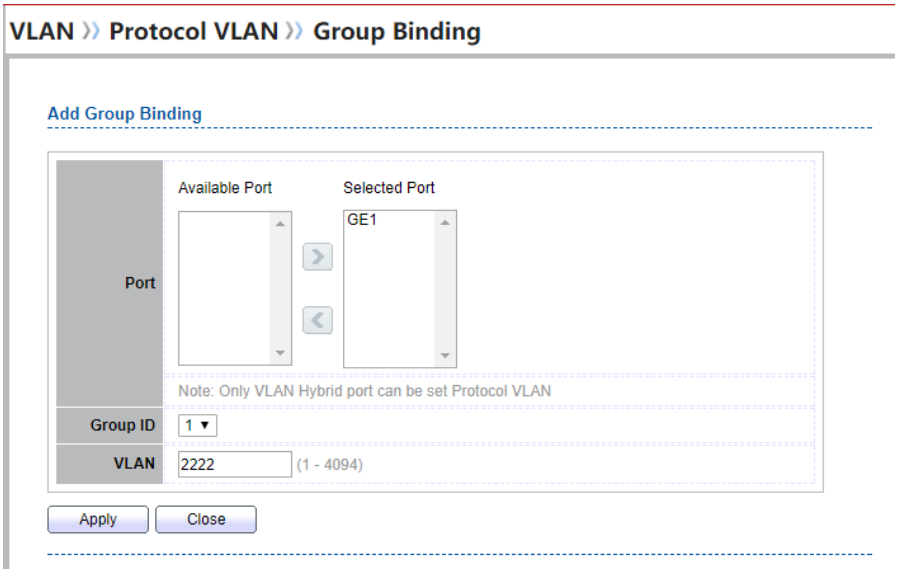
**Для привязки групп протоколов к портам:**

Перейдите в раздел **VLAN** > **Protocol VLAN** > **Group Binding**.




***Текущие привязки***

| Параметр | Описание |
|---|---|
| **Port** | Порт, привязанный к группе протоколов. |
| **Group ID** | Идентификатор группы протоколов (1–8). |
| **VLAN** | VLAN ID, назначаемый пакетам, соответствующим группе. |




***Настройка привязки***

| Параметр | Описание |
|---|---|
| **Port** | Выберите порты для привязки/отвязки от группы. **Только порты в режиме Hybrid.** |
| **Group ID** | Выберите Group ID (1–8) для ассоциации с портом. |
| **VLAN** | Укажите VLAN ID для пакетов, соответствующих группе. |

**Ключевые особенности:**

1. **Только Hybrid-порты** могут быть привязаны к Protocol VLAN.
2. Пакеты, соответствующие группе, автоматически попадают в указанную VLAN.

**Пример настройки:**

- **Порт 1:**
  - **Group ID:** 1 (IPv4, 0x0800)
  - **VLAN:** 10

- **Порт 2:**
  - **Group ID:** 2 (IPX, 0x8137)
  - **VLAN:** 20

**Примечания:**

- Для работы Protocol VLAN убедитесь, что порты находятся в **Hybrid-режиме** (см. раздел 5.1.4).
- Приоритет Protocol VLAN выше, чем у Port-based VLAN.

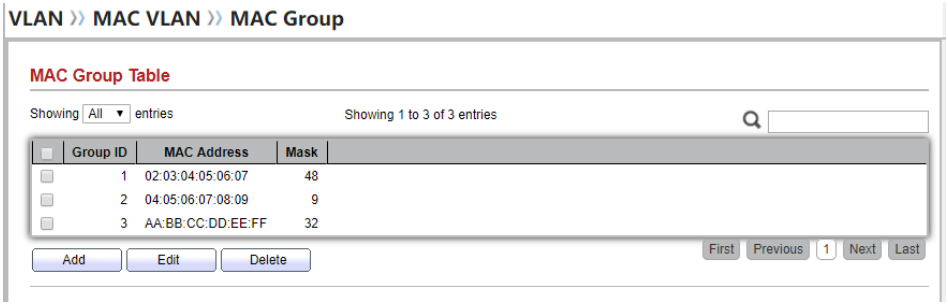
## 5.4. MAC VLAN

Раздел **MAC VLAN** позволяет классифицировать трафик на основе MAC-адресов и назначать его определенным VLAN.

### 5.4.1. Настройка групп MAC-адресов (MAC Group)

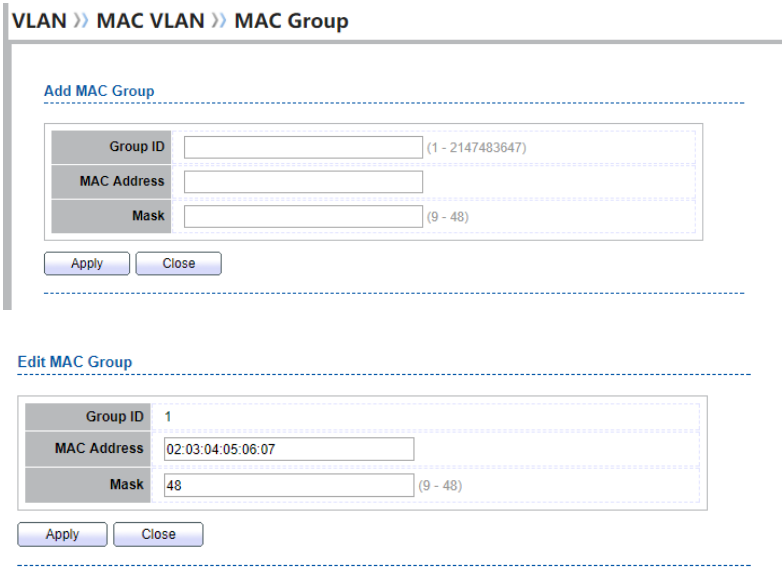
**Для настройки групп MAC-адресов:**

Перейдите в раздел **VLAN** > **MAC VLAN** > **MAC Group**.



***Текущие группы MAC-адресов***

| Параметр | Описание |
|---|---|
| **Group ID** | Уникальный идентификатор группы (1–2147483647). |
| **MAC Address** | MAC-адрес для классификации трафика. |
| **Mask** | Маска MAC-адреса (определяет, какие биты учитываются при классификации). |




***Добавление/редактирование группы***

| Параметр | Описание |
|---|---|
| **Group ID** | Введите уникальный ID группы (1–2147483647). **Только при добавлении.** |
| **MAC Address** | Укажите MAC-адрес (формат: XX-XX-XX-XX-XX-XX или XXXX.XXXX.XXXX). |
| **Mask** | Задайте маску для MAC-адреса (например, FF-FF-FF-00-00-00 для совпадения по первым 3 байтам). |

**Примечания:**

1. **MAC VLAN** назначает VLAN на основе исходного MAC-адреса пакета.
2. **Маска** позволяет группировать устройства по производителю (OUI) или другим критериям.
    - Пример: Маска FF-FF-FF-00-00-00 + MAC 00-1A-2B-XX-XX-XX охватывает все устройства конкретного вендора.

**Пример настройки:**

- **Group ID:** 100
- **MAC Address:** 00-1A-2B-33-44-55
- **Mask:** FF-FF-FF-00-00-00 (совпадение для всех устройств с OUI 00-1A-2B).

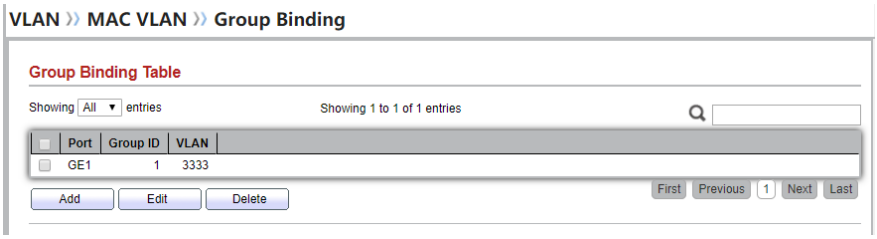
**Рекомендации:**

- Используйте MAC VLAN для:
    - Автоматического распределения IP-телефонов в Voice VLAN.
    - Изоляции устройств IoT в отдельной VLAN.

### 5.4.2. Привязка групп MAC адресов (Group Binding)

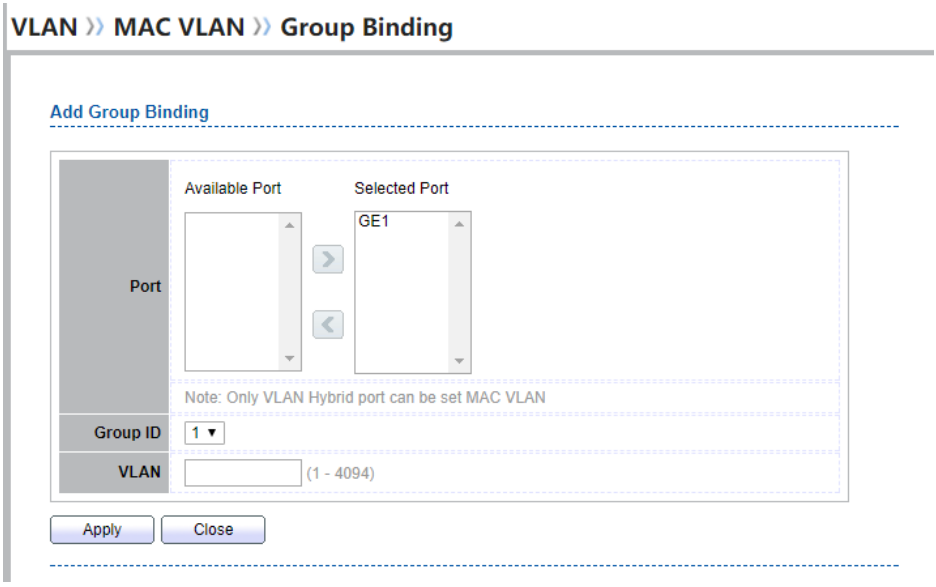
**Для привязки групп MAC-адресов к портам:**

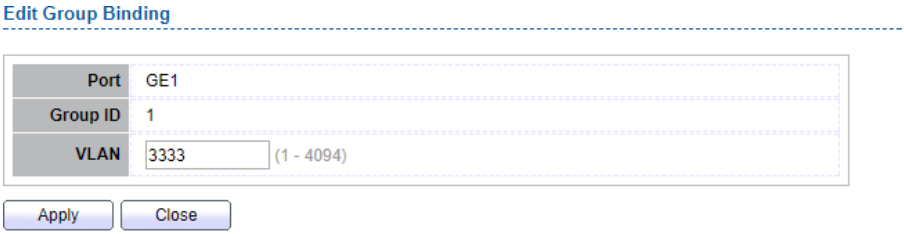
Перейдите в раздел **VLAN** > **MAC VLAN** > **Group Binding**.




***Текущие привязки***

| Параметр | Описание |
|---|---|
| **Port** | Порт, привязанный к группе MAC-адресов. |
| **Group ID** | Идентификатор группы MAC (1–2147483647). |
| **VLAN** | VLAN ID, назначаемый пакетам, соответствующим группе. |






***Настройка привязки***

| Параметр | Описание |
|---|---|
| **Port** | Выберите порты для привязки/отвязки. **Только порты в режиме Hybrid.** |
| **Group ID** | Выберите Group ID для ассоциации с портом. |
| **VLAN** | Укажите VLAN ID для пакетов, соответствующих группе MAC. |

**Ключевые особенности:**

1. **Только Hybrid-порты** поддерживают привязку к MAC VLAN.
2. Пакеты с MAC-адресами, соответствующими группе, автоматически попадают в указанную VLAN.

**Пример настройки:**

- **Порт 1:**
  - **Group ID:** 100 (MAC-адреса 00-1A-2B-XX-XX-XX)
  - **VLAN:** 30 (VLAN для IP-телефонов)

**Примечания:**

- Убедитесь, что порты находятся в **Hybrid-режиме** (см. раздел 5.1.4).
- Приоритет MAC VLAN выше, чем у Port-based VLAN, но ниже, чем у Protocol VLAN.

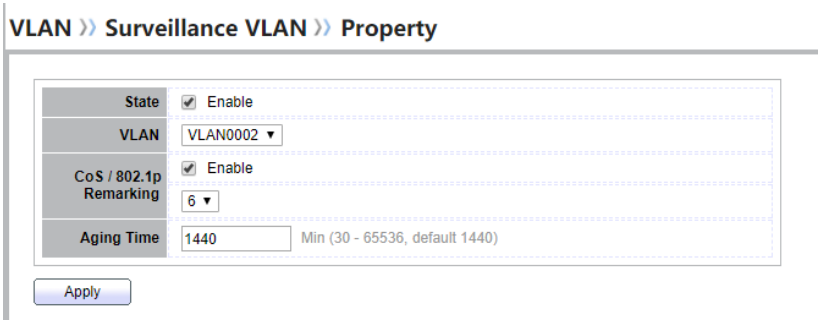
## 5.5. VLAN для видеонаблюдения (Surveillance VLAN)

Раздел **Surveillance VLAN** предназначен для настройки VLAN, оптимизированной для передачи трафика видеокамер и систем безопасности.

### 5.5.1. Свойства (Property)

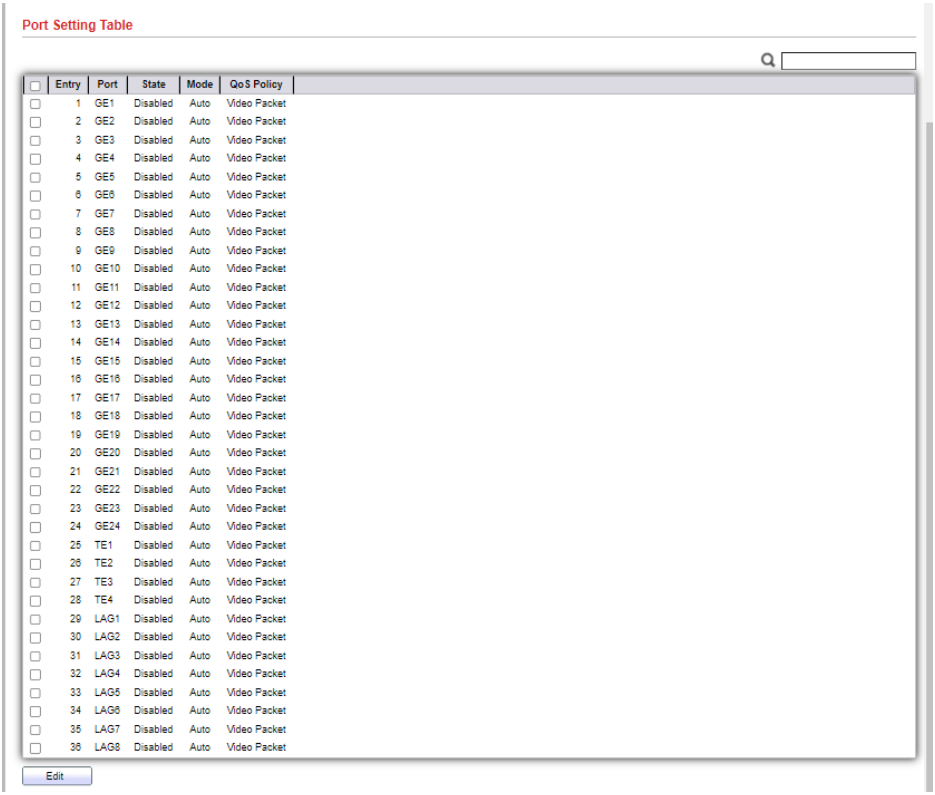
**Для настройки глобальных параметров и параметров портов Surveillance VLAN:**

Перейдите в раздел **VLAN** > **Surveillance VLAN** > **Property**



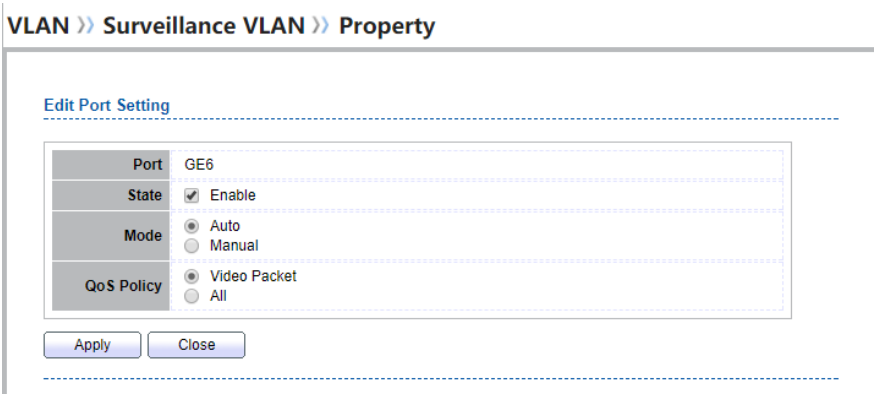

***Глобальные настройки Surveillance VLAN***

| Параметр | Описание |
|---|---|
| **State** | Включение/отключение функции Surveillance VLAN. |
| **VLAN** | Идентификатор Surveillance VLAN (не может совпадать с VLAN по умолчанию). |
| **Cos/802.1p** | Приоритет VLAN (VPT) для видео-трафика (0 –7). |
| **Remarking** | Включение/отключение перемаркировки приоритета (802.1p). |
| **Aging Time** | Время жизни записей Surveillance VLAN (по умолчанию: 1440 минут). |




***Текущие параметры портов***

| Параметр | Описание |
|---|---|
| **Port** | Идентификатор порта. |
| **State** | Состояние Surveillance VLAN на порту (вкл./выкл.). |
| **Mode** | Режим работы Surveillance VLAN (Auto/Manual). |
| **QoS Policy** | Тип пакетов, к которым применяются QoS-атрибуты. |




***Редактирование параметров портов***

| Параметр | Описание |
|---|---|
| **Port** | Выбранный порт. |
| **State** | Включение/отключение Surveillance VLAN на порту. |
| **Mode** | Выберите режим работы: |
| | **Auto** – автоматическое добавление порта в VLAN при обнаружении видео-трафика. |
| | **Manual** – ручное добавление порта в VLAN. |
| **QoS Policy** | Политика QoS: |
| | **Video Packet** – QoS применяется только к пакетам с MAC-адресами из OUI-таблицы. |
| | **All** – QoS применяется ко всем пакетам в Surveillance VLAN. |

**Примечания:**

1. **OUI (Organizationally Unique Identifier)** – идентификатор производителя камер (например, Hikvision, Dahua).
2. **Режим Auto** удобен для IP-камер, которые автоматически определяются по MAC-адресу.
3. **Приоритет (802.1p)** обеспечивает минимальные задержки для видео-трафика.

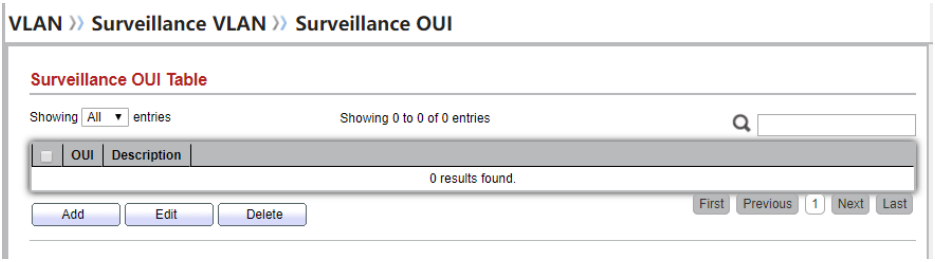
**Рекомендации:**

- Используйте **VLAN ID**, отличный от VLAN по умолчанию (VID 1).
- Для IP-камер с PoE предпочтителен режим **Auto**.
- Настройте **QoS Policy** на **Video Packet** для приоритизации видео-потоков.

### 5.5.2. Настройка OUI адресов для видеонаблюдения (Surveillance OUI)

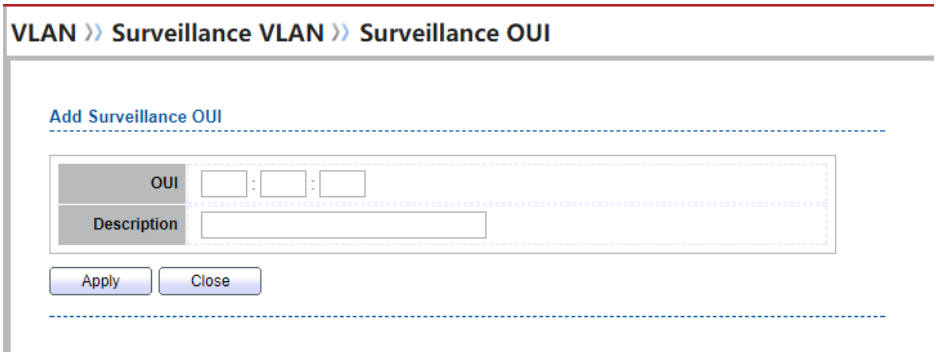
**Для настройки OUI-адресов устройств видеонаблюдения (IP-камер, видеорегистраторов):**

Перейдите в раздел **VLAN** > **Surveillance VLAN** > **Surveillance OUI**.




***Текущие OUI-адреса***

| Параметр | Описание |
|---|---|
| **OUI** | MAC-адрес производителя (первые 6 символов, например, A0-B1-C2). |
| **Description** | Описание устройства (например, "Hikvision IP Camera"). |




***Добавление/редактирование OUI***

| Параметр | Описание |
|---|---|
| **OUI** | Введите OUI MAC-адрес (формат: XX-XX-XX). **Не редактируется при изменении записи.** |
| **Description** | Укажите описание устройства. |

**Примечания:**

1. **OUI** позволяет автоматически классифицировать трафик от камер в Surveillance VLAN.
2. Примеры OUI популярных производителей:
   - Hikvision: 34-CE-00, A4-42-3B
   - Dahua: B8-78-26, D4-EE-07
   - Axis: 00-40-8C, AC-CC-8E

**Рекомендации:**

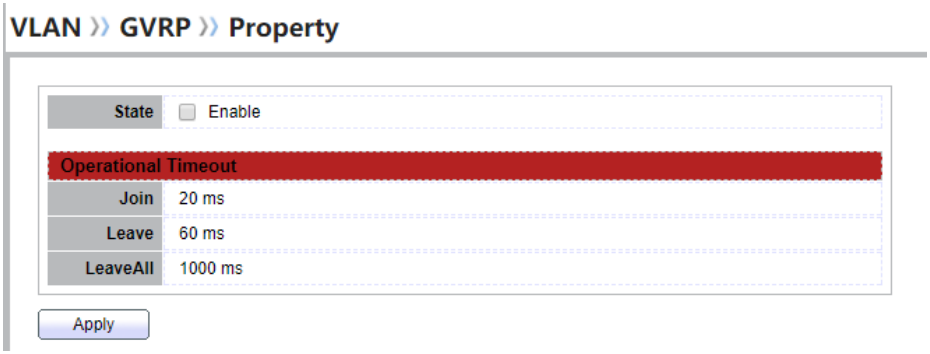
- Добавляйте OUI всех камер в сети для автоматического определения.
- Используйте описания для удобства управления (например, "Камера купольная Hikvision DS-2CD2143G0").

## 5.6. GVRP (GARP VLAN Registration Protocol)

### 5.6.1. Свойства (Property)

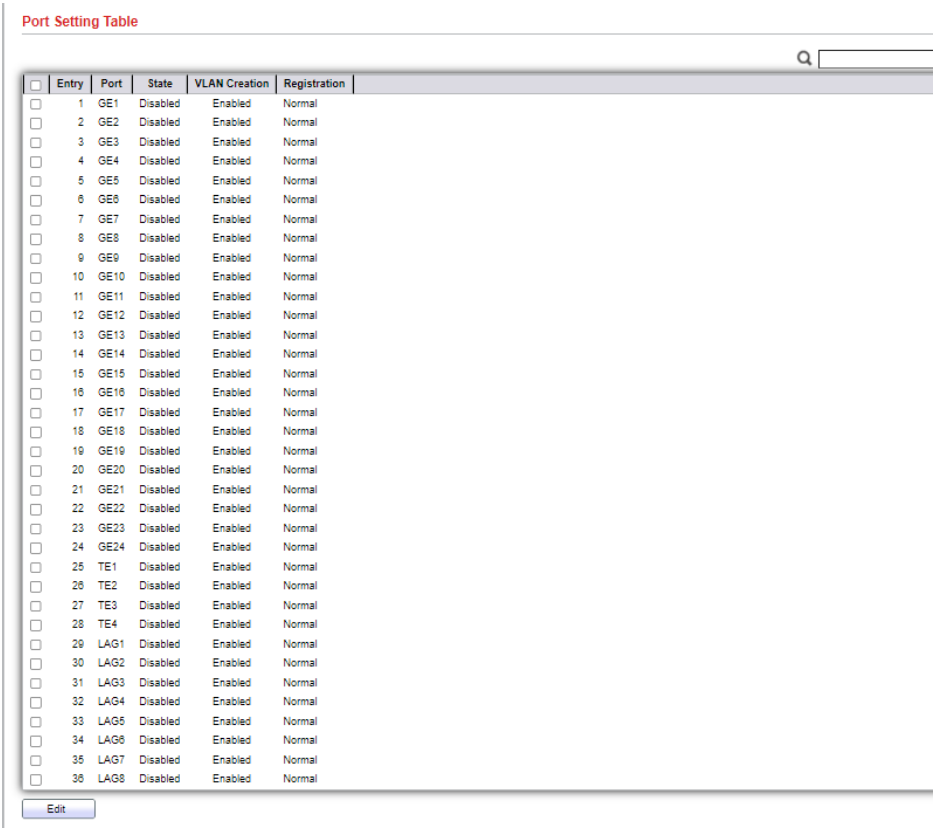
**Для настройки глобальных и портовых параметров GVRP:**

Перейдите в раздел **VLAN** > **GVRP** > **Property**



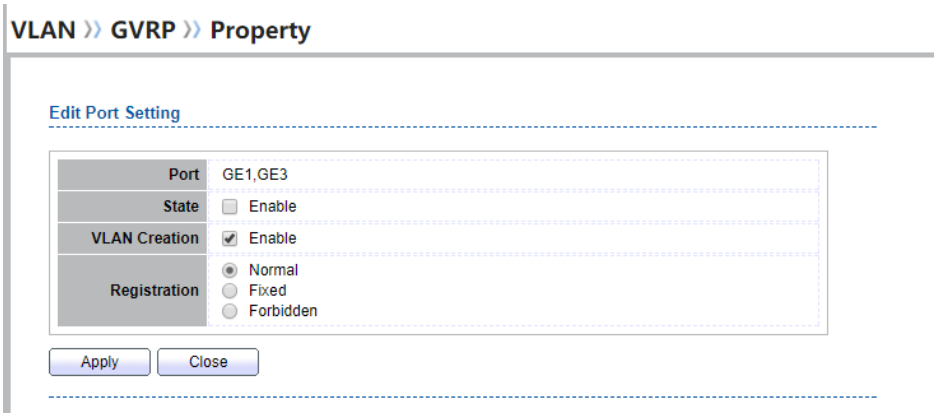

***Глобальные настройки GVRP***

| Параметр | Описание |
|---|---|
| **State** | Включение/отключение функции GVRP: |
| | **Enable** – активирует динамическую регистрацию VLAN между коммутаторами. |
| **Operational Timeout** | Таймауты GVRP: |
| | **Join** – время ожидания присоединения к VLAN. |
| | **Leave** – время ожидания выхода из VLAN. |
| | **Leave All** – время ожидания полного выхода из всех VLAN. |




***Текущие параметры портов***

| Параметр | Описание |
|---|---|
| **Port** | Имя порта. |
| **State** | Состояние GVRP на порту (вкл./выкл.). |
| **VLAN Creation** | Возможность создания динамических VLAN. |
| **Registration** | Режим регистрации: |
| | **Normal** – стандартный режим. |
| | **Fixed** – только статические VLAN. |
| | **Forbidden** – запрет динамических VLAN. |




***Настройка параметров портов***

| Параметр | Описание |
|---|---|
| **Port** | Выбранные порты. |
| **State** | Включение/отключение GVRP на порту. |
| **Vlan Creation** | Разрешение создания динамических VLAN на порту. |
| **Register Mode** | Выберите режим регистрации: |
| | **Normal** – полная поддержка GVRP. |
| | **Fixed** – передача только статических VLAN. |
| | **Forbidden** – разрешён только трафик VLAN по умолчанию. |

**Примечания:**

1. **GVRP** упрощает управление VLAN в крупных сетях, автоматически распространяя информацию о VLAN между коммутаторами.
2. **Режимы портов:**
   - **Normal** – рекомендуется для портов, подключённых к другим коммутаторам.
   - **Fixed/Forbidden** – для портов с конечными устройствами (повышает безопасность).

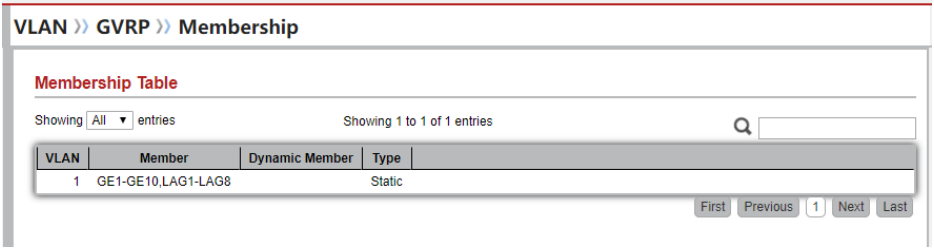
**Рекомендации:**

- Для динамических VLAN используйте **Join Timeout = 20 сек**, **Leave Timeout = 60 сек**.
- На edge-портах (ПК, камеры) активируйте режим **Forbidden**.

### 5.6.2. Настройка VLAN Membership (Membership)

**Для просмотра и управления VLAN, зарегистрированными через GVRP:**

Перейдите в раздел **VLAN** > **GVRP** > **Membership**.




***Информация о VLAN***

| Параметр | Описание |
|---|---|
| **VLAN ID** | Идентификатор VLAN. |
| **Member** | Порты-участники VLAN (включая статические и динамические). |
| **Dynamic Member** | Порты, добавленные автоматически через GVRP. |
| **Type** | Тип VLAN: |
| | **Static** – создана вручную. |
| | **Dynamic** – зарегистрирована через GVRP. |

**Примечания:**

1. **Динамические VLAN** автоматически появляются/исчезают при изменении топологии сети.
2. **Статические VLAN** требуют ручной настройки и не удаляются GVRP.

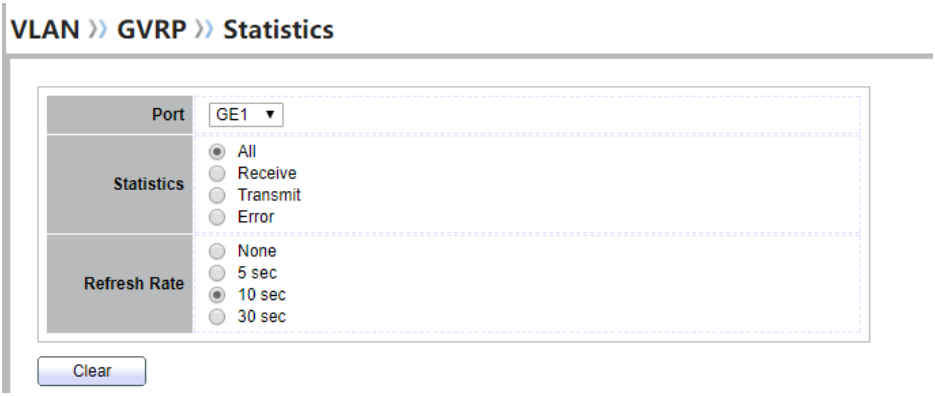
**Пример:**

- **VLAN 10:**
  - **Member:** Port 1 (Static), Port 5 (Dynamic)
  - **Vlan Type:** Static

### 5.6.3. Статистика GVRP (Statistics)

**Для просмотра статистики работы GVRP на портах:**

Перейдите в раздел **VLAN** > **GVRP** > **Statistics**




***Параметры отображения статистики***

| Параметр | Описание |
|---|---|
| **Port** | Идентификатор порта. |

| Параметр | Описание |
|---|---|
| **Statistics** | Тип отображаемой статистики: |
| | **All** – вся статистика (прием, передача, ошибки). |
| | **Receive** – только входящие сообщения GVRP. |
| | **Transmit** – только исходящие сообщения GVRP. |
| | **Error** – только ошибочные сообщения. |
| **Refresh Rate** | Частота обновления данных: |
| | **None** – без автоматического обновления. |
| | **5 sec** – каждые 5 секунд. |
| | **10 sec** – каждые 10 секунд. |
| | **30 sec** – каждые 30 секунд. |

***Детальная статистика GVRP***

| Параметр | Описание |
|---|---|
| **Join Empty** | Количество полученных/переданных сообщений Join Empty. |
| **Empty** | Количество полученных/переданных сообщений Empty. |
| **Leave Empty** | Количество полученных/переданных сообщений Leave Empty. |
| **Join In** | Количество полученных/переданных сообщений Join In. |
| **Leave In** | Количество полученных/переданных сообщений Leave In. |
| **Leave All** | Количество полученных/переданных сообщений Leave All. |
| **Invalid Protocol ID** | Количество ошибок "Неверный ID протокола". |
| **Invalid Attribute Type** | Количество ошибок "Неверный тип атрибута". |
| **Invalid Attribute Value** | Количество ошибок "Неверное значение атрибута". |
| **Invalid Attribute Length** | Количество ошибок "Неверная длина атрибута". |
| **Invalid Event** | Количество ошибок "Неверное событие". |

**Примечания:**

1. **Join/Leave** – сообщения о подключении/отключении VLAN.
2. Высокое количество ошибок может указывать на:
   - Несовместимость оборудования.
   - Проблемы с кабелями или портами.

**Рекомендации:**

- Для диагностики используйте **Refresh Rate = 5 sec**.
- Очищайте статистику (**Clear**) после изменений конфигурации.

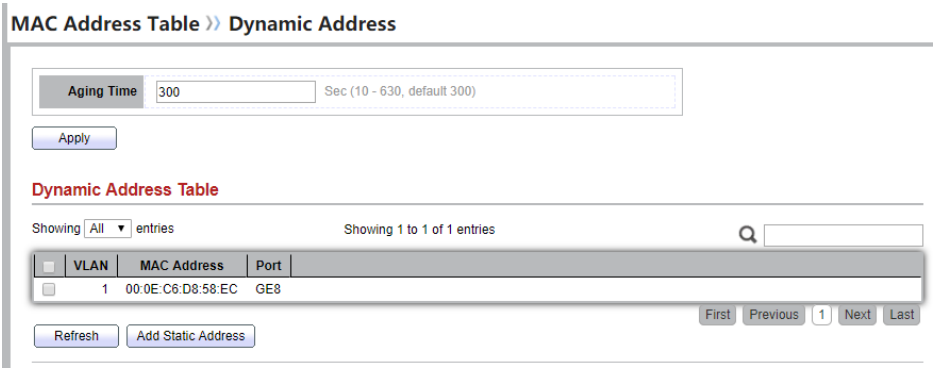
## 6. Таблица MAC-адресов (MAC Address Table)

Раздел **MAC Address Table** отображает динамические MAC-адреса и позволяет настраивать статические записи.

### 6.1. Динамические адреса (Dynamic Address)

**Для настройки времени старения динамических MAC-адресов:**

Перейдите в раздел **MAC Address Table** > **Dynamic Address**.




| Параметр | Описание |
|---|---|
| **Aging Time** | Время (в секундах), в течение которого запись хранится в таблице MAC-адресов. |
| | **Диапазон:** 10–630 секунд. |
| | **По умолчанию:** 300 секунд (5 минут). |

**Примечания:**

1. **Динамические MAC-адреса** автоматически добавляются в таблицу при прохождении трафика через порт.
2. **Слишком короткое** время старения (Aging Time) может привести к:
    - Увеличению широковещательного трафика (частые запросы ARP).
    - Нестабильности коммутации в целом.
3. **Слишком долгое** время старения (Aging Time) занимает память коммутатора.

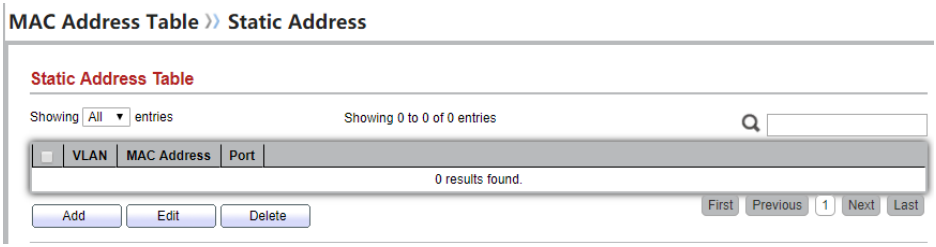
**Рекомендации:**

- Для сетей с мобильными устройствами (Wi-Fi) используйте **300 секунд**.
- Для статичных сетей (серверы) можно увеличить до **600 секунд**.

## 6.2. Статические MAC-адреса (Static Address)

**Для просмотра и настройки статических MAC-адресов:**

Перейдите в раздел **MAC Address Table** > **Static Address**.




***Параметры статических записей***

| Параметр | Описание |
|---|---|

| Параметр | Описание |
|---|---|
| **VLAN** | Укажите VLAN, чтобы отобразить или очистить записи MAC-адресов. |
| **MAC Address** | MAC-адрес устройства, для которого настроена статическая переадресация трафика. |
| **Port** | Порт, к которому привязан MAC-адрес. |

**Примечания:**

1. **Статические MAC-адреса** не удаляются автоматически и имеют приоритет над динамическими.
2. Используйте для:
    - Критически важных устройств (серверы, маршрутизаторы).
    - Защиты от спуфинга MAC-адресов.

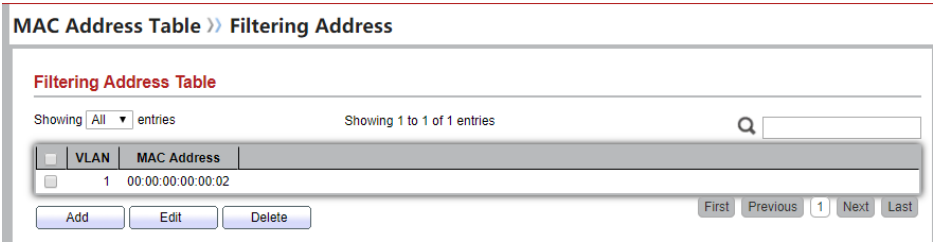
**Пример:**

- **MAC Address:** 00:1A:2B:3C:4D:5E
- **VLAN:** 10
- **Port:** GigabitEthernet 1/0/24

## 6.3. Фильтрация MAC-адресов (Filtering Address)

**Для настройки фильтрации MAC-адресов:**

Перейдите в раздел **MAC Address Table** > **Filtering Address**.




***Параметры фильтрации***

| Параметр | Описание |
|---|---|
| **VLAN** | VLAN ID, к которому применяется фильтр (опционально). |
| **MAC Address** | Укажите MAC-адрес, пакеты с которым будут отбрасываться. |

**Примечания:**

1. Фильтрация блокирует трафик от/к указанному MAC-адресу.
2. Используйте для:
   - Блокировки неавторизованных устройств.
   - Защиты от атак (например, MAC-флудинг).

**Пример:**

- **MAC Address:** 00:1A:2B:3C:4D:5E
- **VLAN:** 10 *(если нужно ограничить фильтр конкретной VLAN)*

## 7. STP (Spanning Tree Protocol)

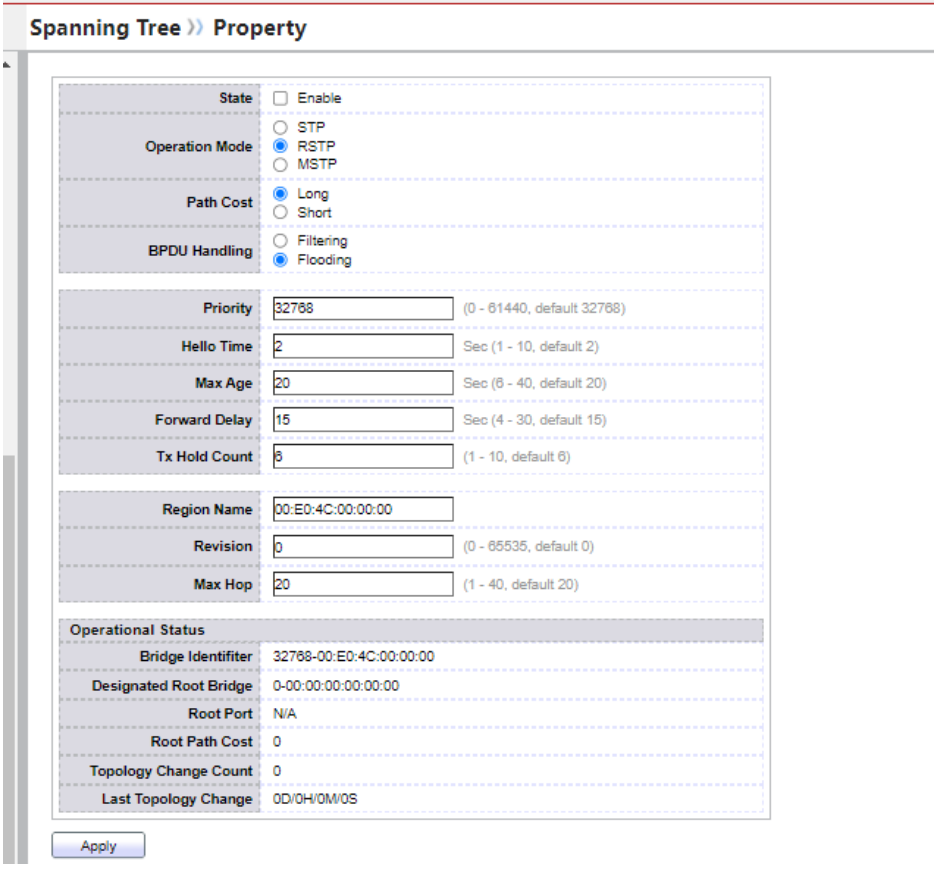
**STP (Spanning Tree Protocol)** – канальный протокол. Основной задачей STP является устранение петель в топологии произвольной сети

Ethernet, в которой есть один или более сетевых мостов, связанных избыточными соединениями. STP решает эту задачу, автоматически блокируя соединения, которые в данный момент для полной связности коммутаторов являются избыточными.

### 7.1. Свойства STP (Property)

**Для настройки глобальных параметров STP:**

Перейдите в раздел **Spanning Tree** > **Property**.




***Основные параметры STP***

| Параметр | Описание |
|---|---|

| Параметр | Описание |
|---|---|
| **State** | Включение/отключение STP на коммутаторе. |
| **Operation Mode** | Режим работы STP: |
| | **STP** – стандартный протокол (IEEE 802.1D). |
| | **RSTP** – Rapid STP (IEEE 802.1w). |
| | **MSTP** – Multiple STP (IEEE 802.1s). |
| **Path Cost** | Метод расчета стоимости пути: |
| | **Long** – диапазон 1–200,000,000. |
| | **Short** – диапазон 1–65,535. |
| **BPDU Handling** | Обработка BPDU при отключенном STP: |
| | **Filtering** – блокировка BPDU. |
| | **Flooding** – широковещательная рассылка BPDU. |
| **Priority** | Приоритет коммутатора (0–61440 с шагом 4096). Чем меньше значение, тем выше вероятность стать корневым мостом. |
| **Hello Time** | Интервал отправки BPDU (1–10 секунд). |
| **Max Age** | Максимальное время ожидания BPDU (6–40 секунд). |
| **Forward Delay** | Время перехода порта в состояние Forwarding (4–30 секунд). |
| **TX Hold Count** | Максимальное количество BPDU в секунду (1–10). |
| **Region Name** | Имя региона MSTP (до 32 символов). По умолчанию – MAC-адрес коммутатора. |
| **Revision** | Номер ревизии MSTP (0–65535). |
| **Max Hops** | Максимальное количество прыжков (хопов) BPDU в регионе MSTP (1–40). |

***Текущее состояние STP***

| Параметр | Описание |
|---|---|
| **Bridge Identifier** | Идентификатор моста (приоритет + MAC). |
| **Designated Root Identifier** | Идентификатор корневого моста. |
| **Root Port** | Порт, ведущий к корневому мосту. |
| **Root Path Cost** | Суммарная стоимость пути к корневому мосту. |
| **Topology Change Count** | Количество изменений топологии. |
| **Last Topology Change** | Время последнего изменения топологии. |

**Примечания:**

1. **RSTP/MSTP** рекомендуется для современных сетей (быстрее реагируют на изменения).
2. **Приоритет:**
   - По умолчанию: 32768.
   - Для назначения корневым мостом установите **0** или **4096**.

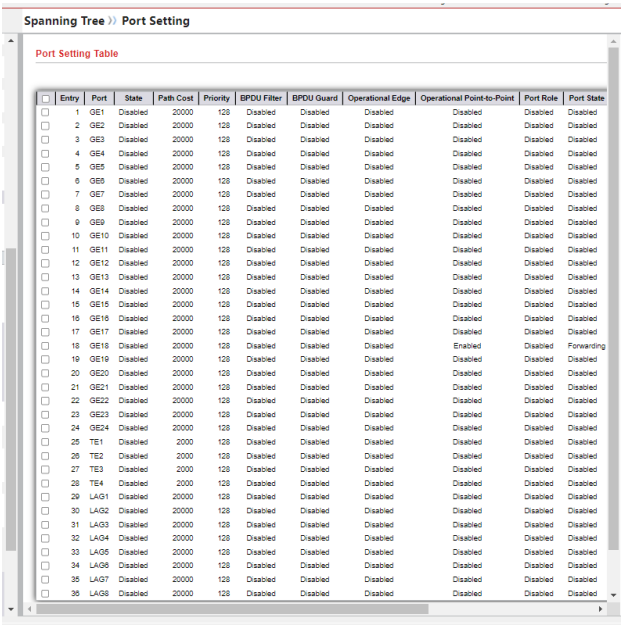
**Пример настройки:**

- **Operation Mode:** RSTP
- **Priority:** 4096
- **Hello Time:** 2 сек
- **Forward Delay:** 15 сек

## 7.2. Настройка портов STP (Port Setting)

### Для настройки параметров STP на портах:

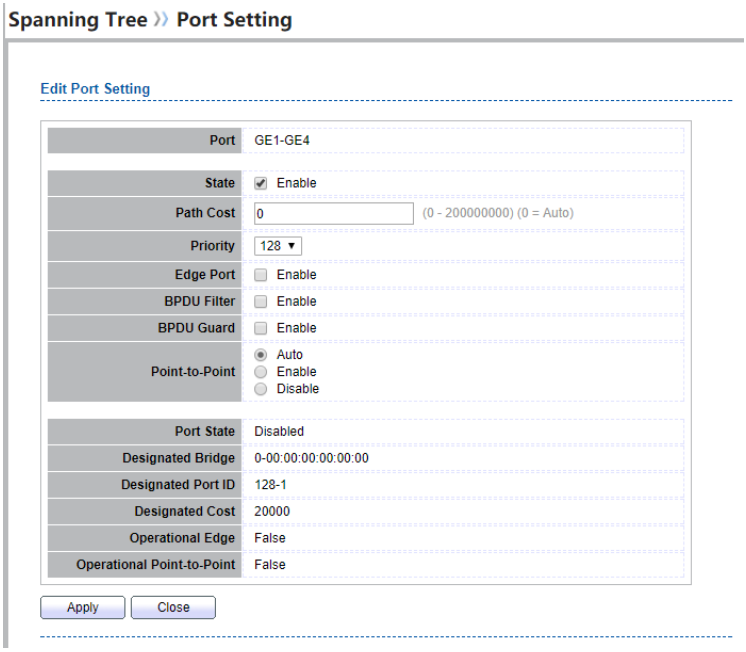
Перейдите в раздел **Spanning Tree** > **Port Setting**.




***Текущие параметры портов***

| Параметр | Описание |
|---|---|
| **Port** | Идентификатор порта. |
| **State** | Текущее состояние STP на порту (вкл./выкл.). |
| **Path Cost** | Стоимость пути STP (влияет на выбор корневого пути). |
| **Priority** | Приоритет порта (0–240 с шагом 16). |
| **BPDU Filter** | Фильтрация BPDU (вкл./выкл.). |
| **BPDU Guard** | Защита от BPDU (вкл./выкл.). |
| **Operational Edge** | Режим Edge Port (автоматический переход в Forwarding). |

| Параметр | Описание |
|---|---|
| **Operational Point-to-Point** | Режим точка-точка (зависит от дуплекса). |
| **Port Role** | Роль порта: Disabled, Master, Root, Designated, Alternative, Backup. |
| **Port State** | Состояние порта: Disabled, Discarding, Learning, Forwarding. |
| **Designated Bridge** | Идентификатор назначенного моста. |
| **Designated Port ID** | Идентификатор назначенного порта. |
| **Designated Cost** | Стоимость пути назначенного порта. |



***Редактирование параметров портов***

| Параметр | Описание |
|---|---|
| **State** | Включение/отключение STP на порту. |
| **Path Cost** | Укажите стоимость пути (1–200,000,000 для **Long**, 1–65,535 для **Short**). |
| **Priority** | Приоритет порта (0–240, шаг 16). |
| **Edge Port** | Режим Edge Port: |
| | **Enable** – для портов, подключенных к конечным устройствам (быстрый переход в состояние Forwarding). |
| | **Disable** – для соединений между коммутаторами. |
| **BPDU Filter** | Блокировка отправки/приема BPDU: |
| | **Enable** – фильтрация активирована. |
| | **Disable** – фильтрация отключена. |
| **BPDU Guard** | Защита от BPDU (отключение порта при получении BPDU): |
| | **Enable** – защита активирована. |
| | **Disable** – защита отключена. |
| **Point-to-Point** | Режим точка-точка: |
| | **Auto** – определяется автоматически (полный дуплекс = точка-точка). |
| | **Enable** – принудительное включение. |
| | **Disable** – принудительное отключение. |

**Примечания:**

1. **Edge Port** следует включать только для портов, подключенных к конечным устройствам (ПК, IP-телефоны).
2. **BPDU Guard** защищает от петель при ошибочном подключении коммутатора к Edge Port.

3. **Path Cost** влияет на выбор корневого пути (меньшее значение = предпочтительный путь).

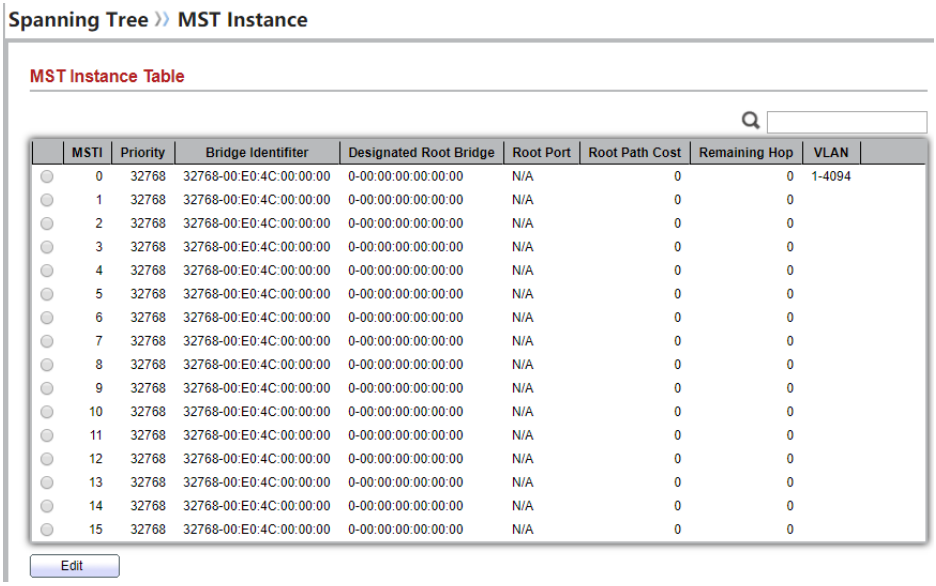
**Пример настройки:**

- **Порт 1 (Edge Port):**
  - **State:** Enabled
  - **Edge Port:** Enable
  - **BPDU Guard:** Enable
- **Порт 24 (Trunk):**
  - **Path Cost:** 2000
  - **Priority:** 32

### 7.3. Настройка MST Instance (MST Instance)

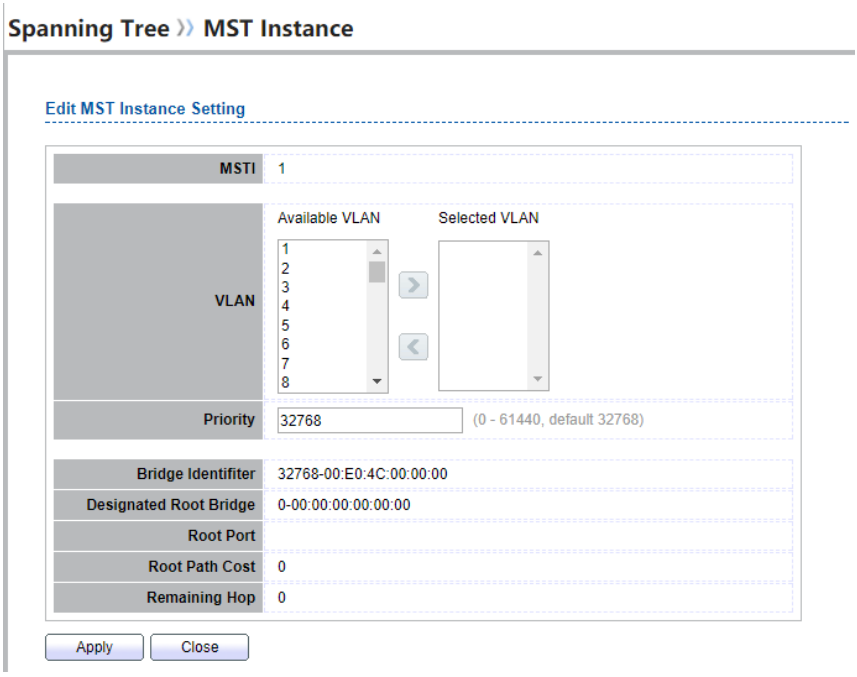
**Для настройки MSTP (Multiple Spanning Tree Protocol):**

Перейдите в раздел **Spanning Tree** > **MST Instance**.



***Текущие параметры MST Instance***

| Параметр | Описание |
|---|---|
| **MSTI** | Идентификатор MST Instance (0–15). |
| **Priority** | Приоритет моста для указанного MST Instance (0–61440, шаг 4096). |
| **Bridge Identifier** | Идентификатор моста (приоритет + MAC) для MST Instance. |
| **Designated Root Bridge** | Идентификатор корневого моста для MST Instance. |
| **Root Port** | Корневой порт для MST Instance. |
| **Root Path Cost** | Стоимость пути к корневому мосту. |
| **Remaining Hop** | Оставшееся количество прыжков (хопов) BPDU. |
| **VLAN** | Список VLAN, сопоставленных с MST Instance. |



***Настройка MST Instance***

| Параметр | Описание |
|---|---|
| **VLAN** | Выберите VLAN для сопоставления с MST Instance. |
| **Priority** | Укажите приоритет моста (0–61440, шаг 4096). Чем меньше значение, тем выше вероятность стать корневым мостом. |

**Примечания:**

1. **MSTI 0** (по умолчанию) включает все VLAN, не назначенные вручную другим MST Instance.
2. **Приоритет:**
   - По умолчанию: 32768.
   - Для назначения корневым мостом установите **0** или **4096**.

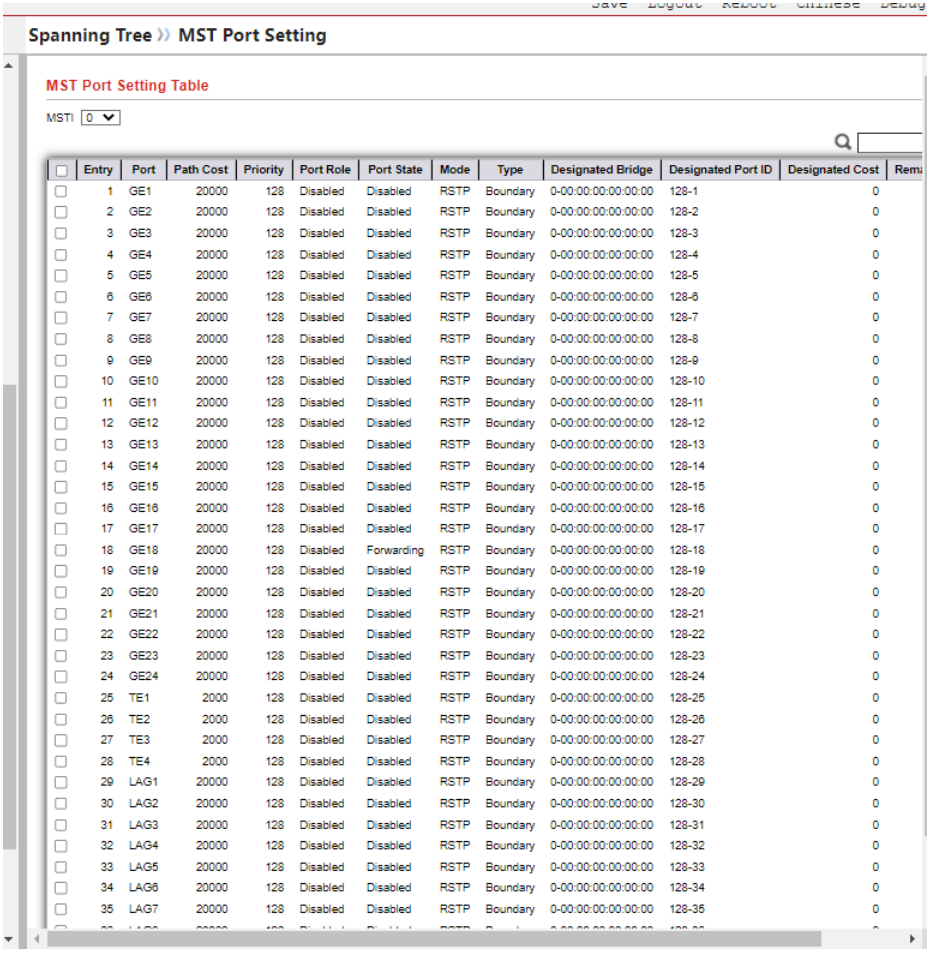
**Пример настройки:**

- **MSTI 1:**
  - **VLAN:** 10, 20, 30
  - **Priority:** 4096
- **MSTI 2:**
  - **VLAN:** 40, 50
  - **Priority:** 8192

## 7.4. Настройка портов MST (MST Port Setting)

### Для настройки параметров портов в MSTP:

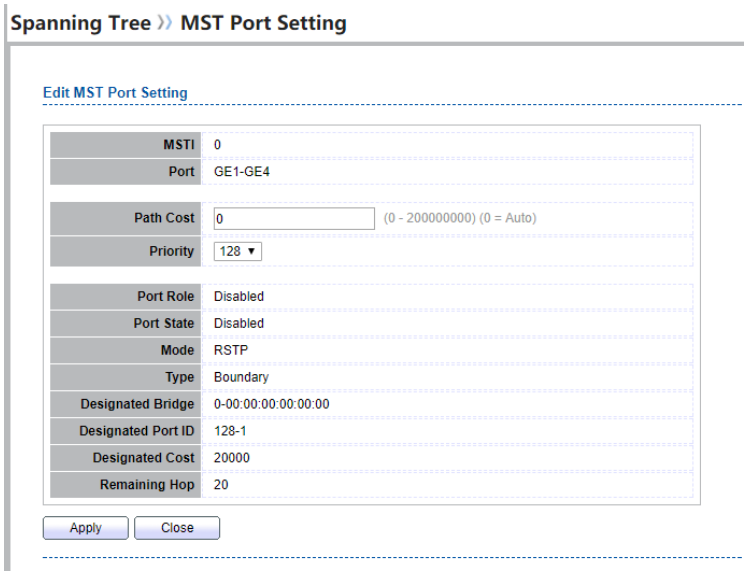
Перейдите в раздел **Spanning Tree** > **MST Port Setting**.




| Entry | Port | Path Cost | Priority | Port Role | Port State | Mode | Type | Designated Bridge | Designated Port ID | Designated Cost | Rema |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | GE1 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-1 | 0 | |
| 2 | GE2 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-2 | 0 | |
| 3 | GE3 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-3 | 0 | |
| 4 | GE4 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-4 | 0 | |
| 5 | GE5 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-5 | 0 | |
| 6 | GE6 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-6 | 0 | |
| 7 | GE7 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-7 | 0 | |
| 8 | GE8 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-8 | 0 | |
| 9 | GE9 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-9 | 0 | |
| 10 | GE10 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-10 | 0 | |
| 11 | GE11 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-11 | 0 | |
| 12 | GE12 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-12 | 0 | |
| 13 | GE13 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-13 | 0 | |
| 14 | GE14 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-14 | 0 | |
| 15 | GE15 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-15 | 0 | |
| 16 | GE16 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-16 | 0 | |
| 17 | GE17 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-17 | 0 | |
| 18 | GE18 | 20000 | 128 | Disabled | Forwarding | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-18 | 0 | |
| 19 | GE19 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-19 | 0 | |
| 20 | GE20 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-20 | 0 | |
| 21 | GE21 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-21 | 0 | |
| 22 | GE22 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-22 | 0 | |
| 23 | GE23 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-23 | 0 | |
| 24 | GE24 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-24 | 0 | |
| 25 | TE1 | 2000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-25 | 0 | |
| 26 | TE2 | 2000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-26 | 0 | |
| 27 | TE3 | 2000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-27 | 0 | |
| 28 | TE4 | 2000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-28 | 0 | |
| 29 | LAG1 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-29 | 0 | |
| 30 | LAG2 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-30 | 0 | |
| 31 | LAG3 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-31 | 0 | |
| 32 | LAG4 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-32 | 0 | |
| 33 | LAG5 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-33 | 0 | |
| 34 | LAG6 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-34 | 0 | |
| 35 | LAG7 | 20000 | 128 | Disabled | Disabled | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-35 | 0 | |

***Текущие параметры портов MST***

| Параметр | Описание |
|---|---|
| **MSTI** | Идентификатор MST Instance (0–15). |
| **Port** | Идентификатор порта. |
| **Path Cost** | Стоимость пути порта для указанного MST Instance. |
| **Priority** | Приоритет порта (0–240, шаг 16). |
| **Port Role** | Роль порта: Disabled, Master, Root, Designated, Alternative, Backup. |
| **Port State** | Состояние порта: Disabled, Discarding, Learning, Forwarding. |
| **Mode** | Режим STP на порту (STP/RSTP/MSTP). |
| **Type** | Тип порта: |
| | **Boundary** – подключен к устройству вне региона MST. |
| | **Internal** – подключен к устройству внутри региона MST. |
| **Designated Bridge** | Идентификатор назначенного моста. |
| **Designated Port ID** | Идентификатор назначенного порта. |
| **Designated Cost** | Стоимость пути назначенного порта. |
| **Remaining Hop** | Оставшееся количество прыжков (хопов) BPDU. |




***Редактирование параметров портов***

| **Параметр** | **Описание** |
|---|---|
| **Path Cost** | Укажите стоимость пути порта для MST Instance. |
| **Priority** | Укажите приоритет порта (0–240, шаг 16). |

**Примечания:**

1. **Path Cost** влияет на выбор корневого пути в рамках MST Instance.
2. **Тип порта:**
   - **Boundary** – требует особого внимания (риск петель между регионами).
   - **Internal** – стандартный порт внутри региона MST.

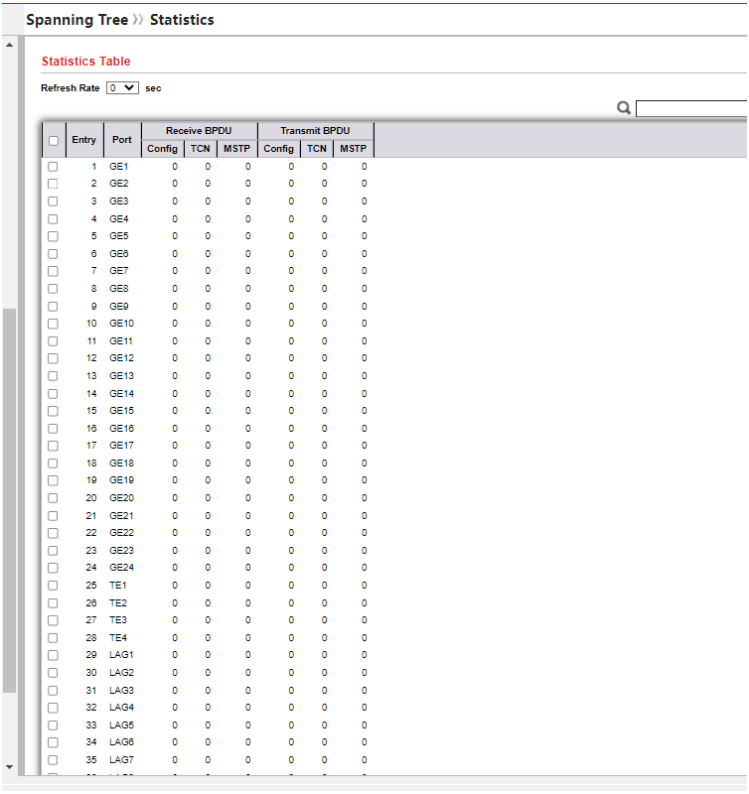
**Пример настройки:**

- **MSTI 1, Порт 24:**
  - **Path Cost:** 2000
  - **Priority:** 32
  - **Type:** Boundary

### 7.5. Статистика STP (Statistics)

**Для просмотра статистики работы STP:**

Перейдите в раздел **Spanning Tree** > **Statistics**.

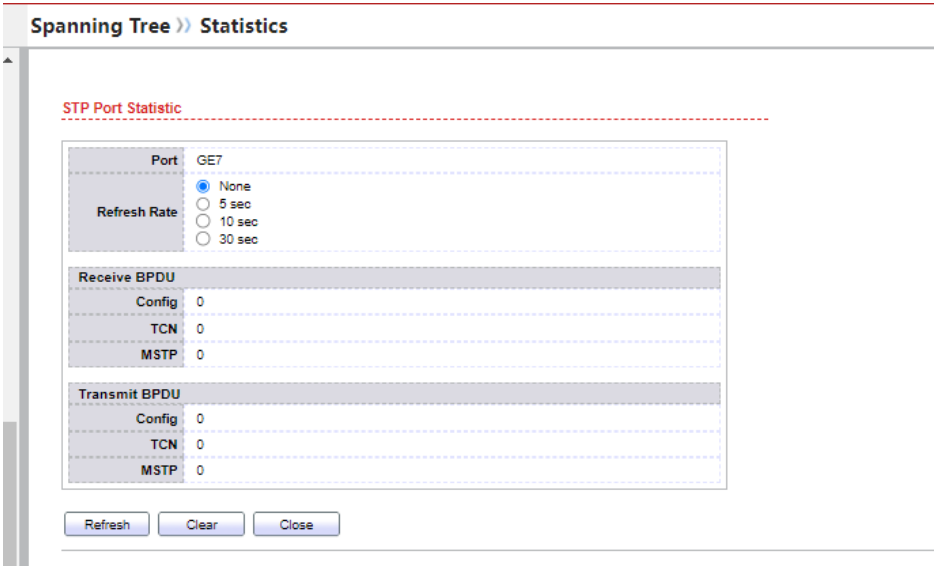



***Параметры статистики***

| Параметр | Описание |
|---|---|
| **Refresh Rate** | Частота автоматического обновления статистики. |
| **Receive BPDU (Config)** | Количество полученных BPDU типа **Configuration**. |
| **Receive BPDU (TCN)** | Количество полученных BPDU типа **Topology Change Notification (TCN)**. |

| Параметр | Описание |
|---|---|
| **Receive BPDU (MSTP)** | Количество полученных BPDU для **MSTP**. |
| **Transmit BPDU (Config)** | Количество отправленных BPDU типа **Configuration**. |
| **Transmit BPDU (TCN)** | Количество отправленных BPDU типа **TCN**. |
| **Transmit BPDU (MSTP)** | Количество отправленных BPDU для **MSTP**. |

| Параметр | Описание |
|---|---|
| **Clear** | Очистка статистики для выбранных интерфейсов. |
| **View** | Просмотр статистики для интерфейса. |



**Примечания:**

1. **BPDU (Bridge Protocol Data Unit)** – служебные кадры STP для обмена информацией между коммутаторами.
    - **Configuration BPDU** – используются для построения дерева.
    - **TCN BPDU** – уведомления об изменении топологии.
2. Высокое количество **TCN BPDU** может указывать на нестабильность сети.

**Рекомендации:**

- Для диагностики используйте **Refresh Rate = 5 sec**.
- Очищайте статистику (**Clear**) после изменений конфигурации.

### 8. ERPS (Ethernet Ring Protection Switching)

**ERPS** – протокол защиты кольцевых сетей Ethernet, разработанный ITU-T. Обеспечивает телекоммуникационную надежность с быстрой сходимостью (<50 мс).

***Ключевые термины ERPS***

1. **ERPS Instance**
    - Аналог домена ERRP.
    - Группа коммутаторов с одинаковым **ID экземпляра** и **Control VLAN**.
2. **Control VLAN**
    - VLAN для передачи служебных кадров ERPS.
3. **RPL (Ring Protection Link)**
    - Заблокированная в штатном режиме связь для предотвращения петель.
4. **Типы узлов:**
    - **RPL Owner** – узел с портом, блокирующим RPL.

- **RPL Neighbour** – узел, подключенный к RPL Owner.
- **Common** – обычные узлы.

5. **Состояния портов:**
   - **Forwarding** – передача трафика и R-APS сообщений.
   - **Discarding** – только прием/отправка R-APS.
   - **Disable** – порт отключен.
6. **Режимы работы:**
   - **Revertive** – автоматическое восстановление RPL после устранения неисправности.
   - **Non-Revertive** – RPL остается разблокированным после восстановления.

## 8.1. Общие настройки ERPS (Property)

**Чтобы включить/отключить ERPS:**

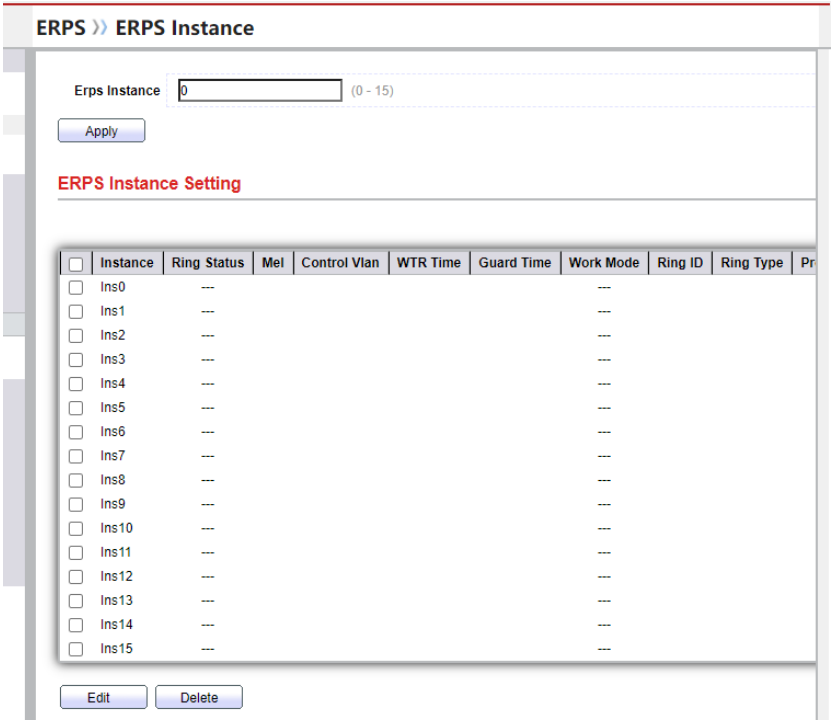
Перейдите в раздел **ERPS** > **Property**.


| Параметр | Описание |
|---|---|
| Disable | Отключить ERPS (по умолчанию) |
| Enable | Включить ERPS |

## 8.2. Настройка ERPS Instance (ERPS Instance)

**Для управления экземплярами ERPS:**

1. Перейдите в раздел **ERPS** > **ERPS Instance**.
2. Возможности:
   - Изменение/удаление (Edit/Delete).
   - Просмотр параметров.




**Примечания:**

- Все узлы кольца должны использовать одинаковые **Control VLAN** и **ID экземпляра**.
- Для RPL Owner/RPL Neighbour требуется ручное назначение портов.

# 9. Обнаружение устройств (Discovery)

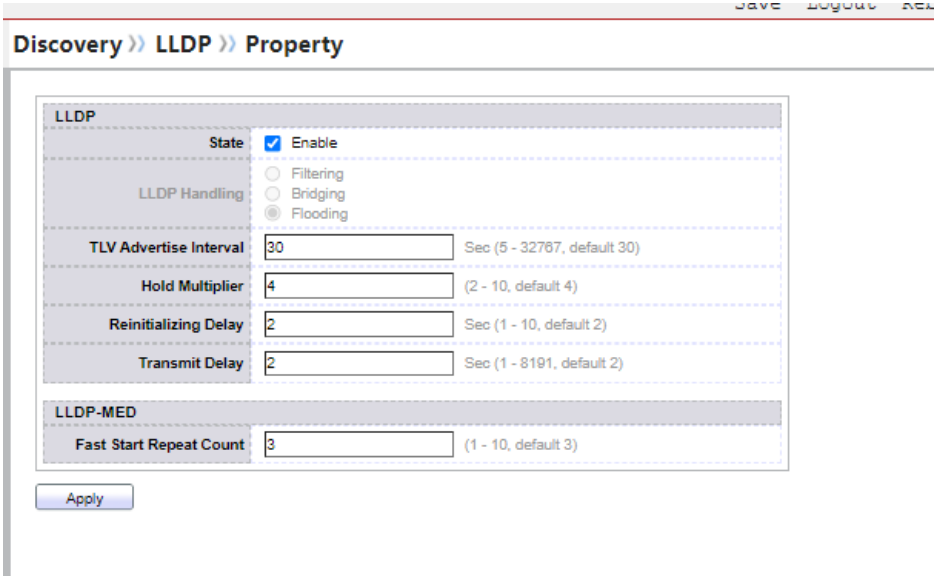
## 9.1. Протокол LLDP (Link Layer Discovery Protocol)

**LLDP** – односторонний протокол для обмена информацией между сетевыми устройствами. Не требует подтверждения получения данных.

### 9.1.1. Свойства LLDP (Property)

**Для настройки глобальных параметров LLDP:**

Перейдите в раздел **Discovery** > **LLDP** > **Property**.




***Параметры LLDP***

| Параметр | Описание |
|---|---|
| **State** | Включение/отключение LLDP на коммутаторе. |
| **LLDP Handling** | Действие при отключенном LLDP: |
| | **Filtering** – удаление LLDP-кадров. |

| Параметр | Описание |
|---|---|
| | **Bridging** – передача только членам VLAN (аналог flooding с учетом VLAN). |
| | **Flooding** – передача на все порты. |
| **TLV Advertise Interval** | Интервал отправки LLDP-кадров (по умолчанию: 30 сек, диапазон: 5–32767 сек). |
| **Holdtime Multiplier** | Множитель для TTL (время жизни данных). Диапазон: 2–10 (по умолчанию: 4). |
| **Reinitialization Delay** | Задержка перед повторной инициализацией порта (1–10 сек, по умолчанию: 2 сек). |
| **Transmit Delay** | Задержка между отправкой LLDP-кадров (1–8191 сек, по умолчанию: 3 сек). |
| **Fast Start Repeat Count** | Количество быстрых повторов при поднятии линка (1–10, по умолчанию: 3). |

**Примечания:**

1. **TLV (Type-Length-Value)** – блоки данных в LLDP-кадрах (информация о портах, VLAN, PoE и т.д.).
2. **Holdtime = Интервал × Множитель** (например, 30 сек × 4 = 120 сек).
3. **Fast Start** ускоряет обнаружение устройств при включении порта.

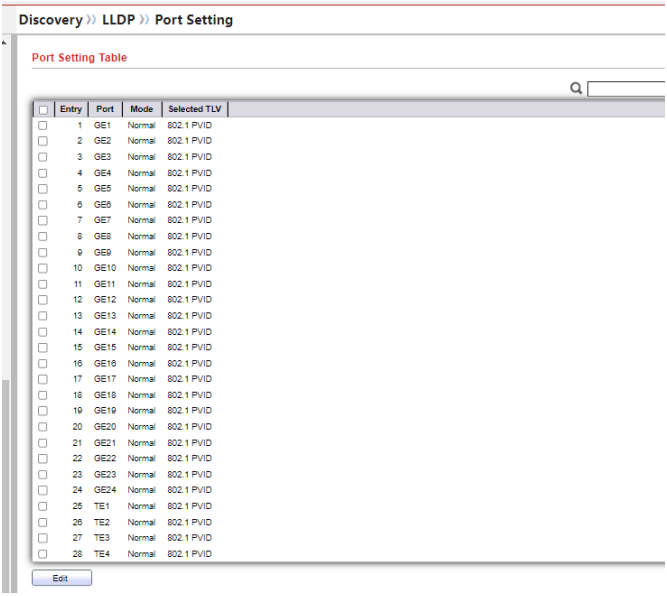
**Рекомендации:**

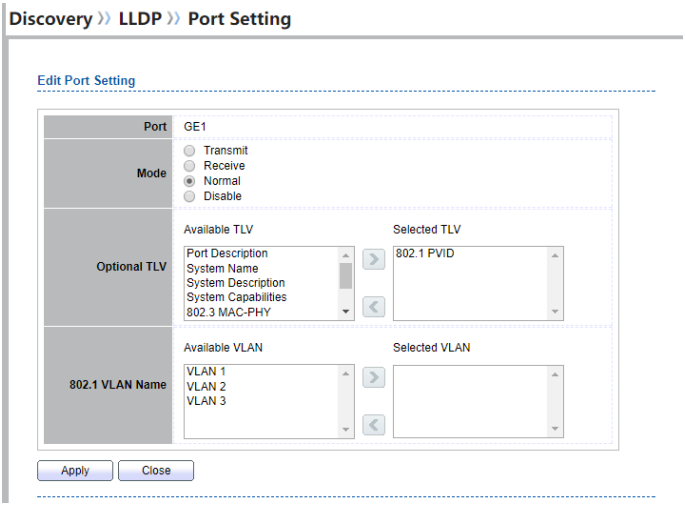
- Для VoIP устройств и IP-камер используйте интервал **30 сек** и **Holdtime Multiplier = 4**.
- На edge-портах активируйте **Filtering** для безопасности.

### 9.1.2. Настройка портов LLDP (Port Setting)

**Для настройки параметров LLDP на портах:**

1. Перейдите в раздел **Discovery** > **LLDP** > **Port Setting**.
2. Выберите порт и нажмите **Edit (Изменить)**.



***Параметры портов LLDP***

| Параметр | Описание |
|---|---|
| **Port** | Выберите порт для настройки (или **All Ports** для всех портов). |
| **Mode** | Режим работы LLDP: |
| | **Disable** – отключение отправки и получения LLDP-кадров. |
| | **RX Only** – только прием LLDP-кадров. |
| | **TX Only** – только отправка LLDP-кадров. |
| | **TX And RX** – отправка и прием LLDP-кадров (рекомендуется). |
| **Optional TLV** | Выберите дополнительные TLV (можно несколько): |
| | **System Name** – имя устройства. |
| | **Port Description** – описание порта. |
| | **System Description** – описание системы. |
| | **System Capability** – возможности устройства (коммутатор, маршрутизатор и т.д.). |
| | **802.3 MAC-PHY** – информация о скорости и дуплексе. |
| | **802.3 Link Aggregation** – поддержка агрегации каналов. |
| | **802.3 Maximum Frame Size** – максимальный размер кадра. |
| | **Management Address** – IP-адрес управления. |
| | **802.1PVID** – PVID порта. |
| **802.1 VLAN Name** | Выберите VLAN Name ID для отправки (можно несколько). |

**Примечания:**

1. **Режимы LLDP:**
   - **TX And RX** используется для взаимодействия с соседними устройствами (например, коммутаторами, IP-телефонами).
   - **RX Only** подходит для мониторинга сети без раскрытия информации о коммутаторе.
2. **TLV (Type-Length-Value):**
   - **System Capability** помогает определить тип устройства (например, Switch, Router).
   - **Management Address** упрощает удаленное управление.

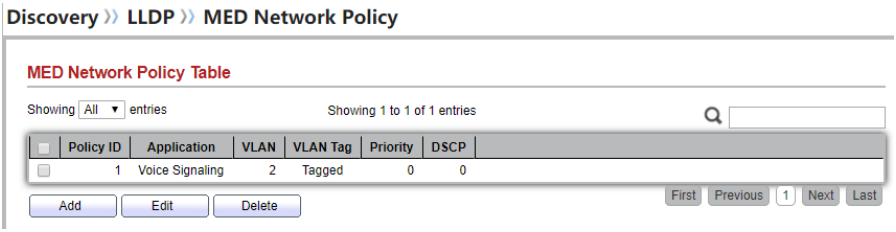
**Пример настройки:**

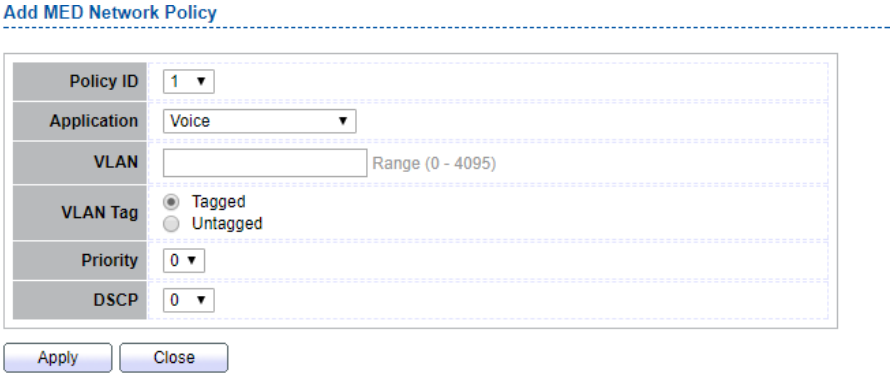
- **Порт 1 (подключен к IP-телефону):**
  - **Mode:** TX And RX
  - **Optional TLV:** System Name, Port Description, Management Address
- **Порт 24 (магистраль):**
  - **Mode:** TX And RX
  - **Optional TLV:** 802.3 Link Aggregation, 802.1PVID

### 9.1.3. Политика сети LLDP-MED (MED Network Policy)

**Для настройки политик QoS для устройств LLDP-MED (например, VoIP):**

1. Перейдите в раздел **Discovery** > **LLDP** > **MED Network Policy**.
2. Нажмите **Add (Добавить)** или **Edit (Изменить)** для создания/редактирования политики.




***Параметры политики***

| Параметр | Описание |
|---|---|
| **Policy ID** | Идентификатор политики (1–65535). |
| **Application** | Тип трафика: |
| | **Voice** – голосовой трафик (VoIP). |
| | **Voice Signaling** – оповещение VoIP (SIP, H.323). |
| | **Guest Voice** – гостевой голосовой трафик. |
| | **Softphone Voice** – голосовой трафик с ПО- |

| Параметр | Описание |
|---|---|
| | телефонов. |
| | **Video Conferencing** – видеоконференции. |
| | **App Streaming Video** – потоковое видео. |
| **VLAN** | VLAN ID для трафика (1–4094). |
| **VLAN Tag** | Тип VLAN: |
| | **Tagged** – тегированные кадры. |
| | **Untagged** – нет тегов. |
| **Priority** | Приоритет L2 (0–7, где 7 – наивысший). |
| **DSCP** | Значение DSCP (0–63) для QoS на L3. |

**Примечания:**

1. **LLDP-MED (Media Endpoint Discovery)** – расширение LLDP для мультимедийных устройств (IP-телефоны, камеры).
2. **Примеры DSCP:**
    - **Voice:** EF (46)
    - **Video Conferencing:** AF41 (34)

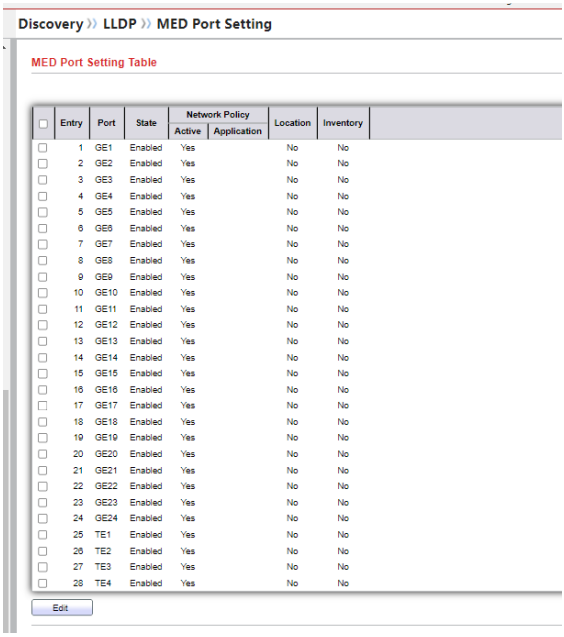
**Рекомендации:**

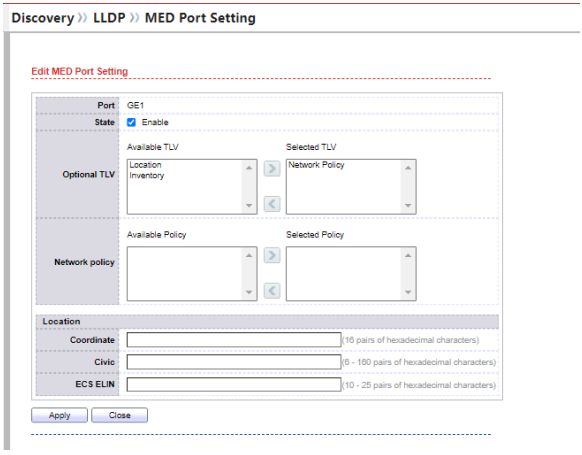
- Для VoIP используйте:
    - **Priority:** 6
    - **DSCP:** 46 (EF)
- Для видеотрафика:
    - **Priority:** 4
    - **DSCP:** 34 (AF41)

### 9.1.4. Настройка портов LLDP-MED (MED Port Setting)

**Для настройки параметров LLDP-MED на портах:**

1. Перейдите в раздел **Discovery** > **LLDP** > **MED Port Setting**.
2. Выберите порт и нажмите **Edit (Изменить)**.



***Основные параметры портов***

| Параметр | Описание |
|---|---|
| **Port** | Выберите порт или **All Ports** для настройки всех портов. |
| **State** | Включение/отключение LLDP-MED на порту. |
| **Optional TLV** | Дополнительные TLV (можно выбрать несколько): |
| | **Network Policy** – передача политик QoS (например, для VoIP). |
| | **Location** – информация о местоположении устройства. |
| | **Inventory** – данные о модели и производителе устройства. |
| **Network Policy** | Привязка политик QoS (должны быть созданы в разделе **MED Network Policy**). |

***Параметры местоположения (Location)***

| Параметр | Описание |
|---|---|
| **Coordinate** | Географические координаты (широта/долгота). |
| **Civic** | Адрес в текстовом формате (например, "ул. Ленина, д. 1"). |
| **ECS ELIN** | Номер экстренного вызова (Emergency Call Service ELIN). |

**Примечания:**

1. **LLDP-MED** используется для:
   - Автоматической настройки VoIP-телефонов (VLAN, QoS).
   - Передачи информации о местоположении для экстренных вызовов.
2. **Inventory TLV** помогает идентифицировать модель устройства (например, "Cisco IP Phone 7960").

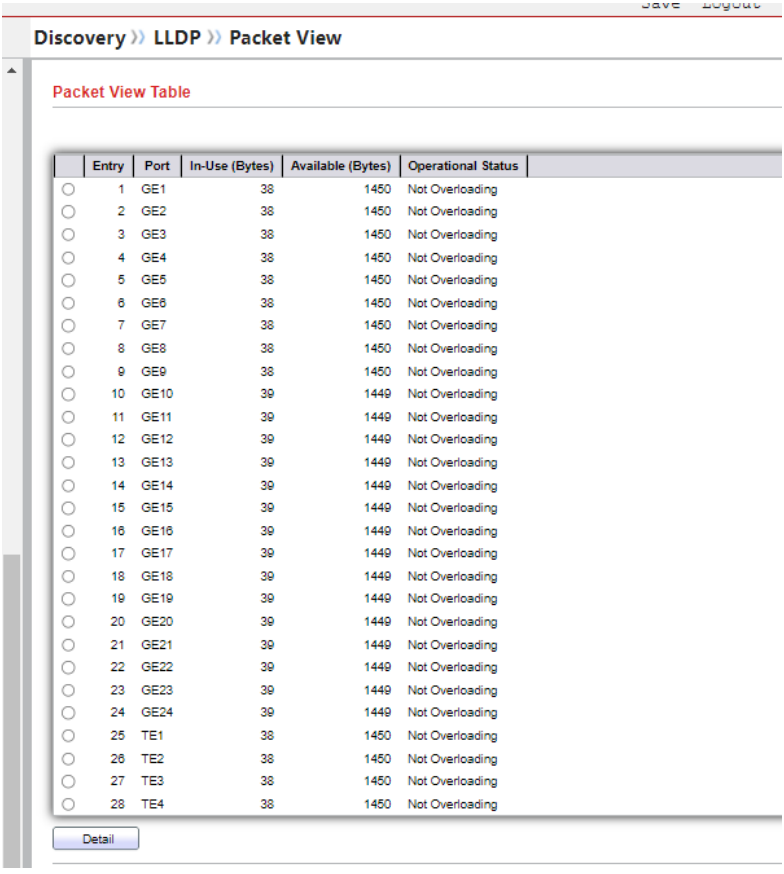
**Пример настройки:**

- **Порт 1 (IP-телефон):**
  - **State:** Enable
  - **Optional TLV:** Network Policy, Inventory
  - **Network Policy:** 1 (Voice), 2 (Voice Signaling)

### 9.1.5. Просмотр пакетов LLDP (Packet View)

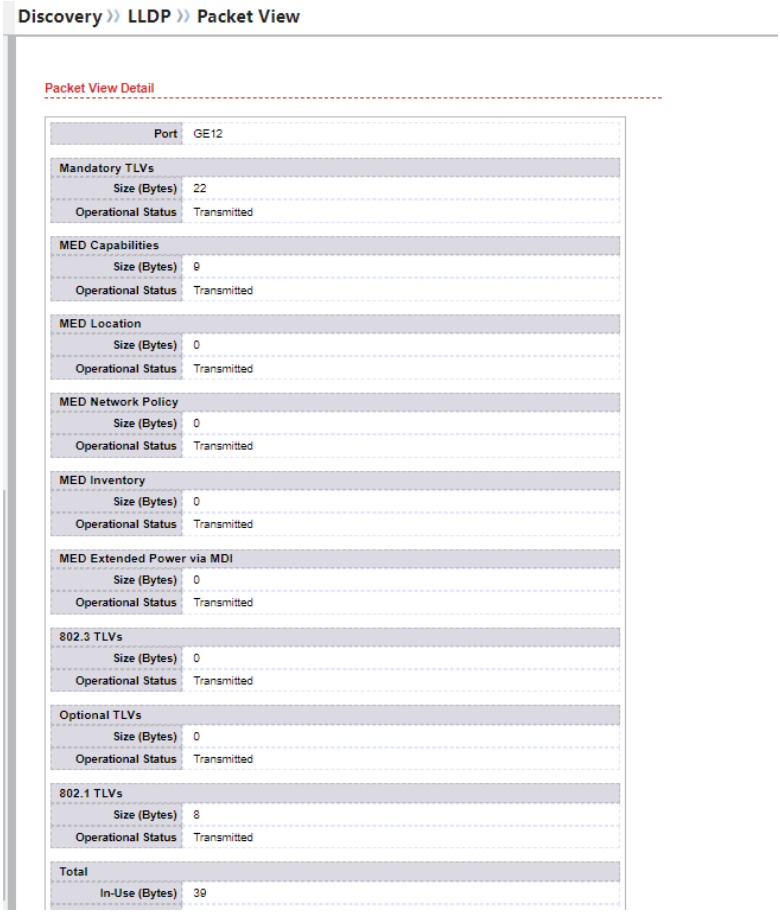
**Для анализа перегрузки LLDP-пакетов:**

Перейдите в раздел **Discovery** > **LLDP** > **Packet View**.



***Сводная информация по портам***

| Параметр | Описание |
|---|---|
| **Port** | Имя порта. |
| **In-Use (Bytes)** | Количество байт, занятых LLDP-информацией в пакете. |
| **Available (Bytes)** | Свободное место для дополнительных TLV (макс. размер пакета: 1500 байт). |
| **Operational Status** | Статус перегрузки: Normal или Overloading. |



***Детальная информация (для выбранного порта)***

| Параметр | Описание |
|---|---|
| **Mandatory TLVs** | Размер обязательных TLV (например, Chassis ID, Port ID). Статус: Sent или Overloading. |
| **MED Capabilities** | Размер TLV возможностей LLDP-MED. |
| **MED Location** | Размер TLV местоположения. |
| **MED Network Policy** | Размер TLV политик QoS. |
| **MED Inventory** | Размер TLV инвентарной информации. |
| **MED Extended Power via MDI** | Размер TLV информации о PoE. |
| **802.3 TLVs** | Размер TLV стандарта 802.3 (MAC/PHY, агрегация). |
| **Optional TLVs** | Размер дополнительных TLV (System Name, Description). |
| **802.1 TLVs** | Размер TLV стандарта 802.1 (VLAN, PVID). |
| **Total** | Общий размер LLDP-пакета. |

**Примечания:**

1. **Перегрузка (Overloading)** возникает, если суммарный размер TLV превышает 1500 байт.
2. Решения:
   - Отключите неиспользуемые TLV (например, **MED Inventory**).
   - Уменьшите количество политик в **MED Network Policy**.

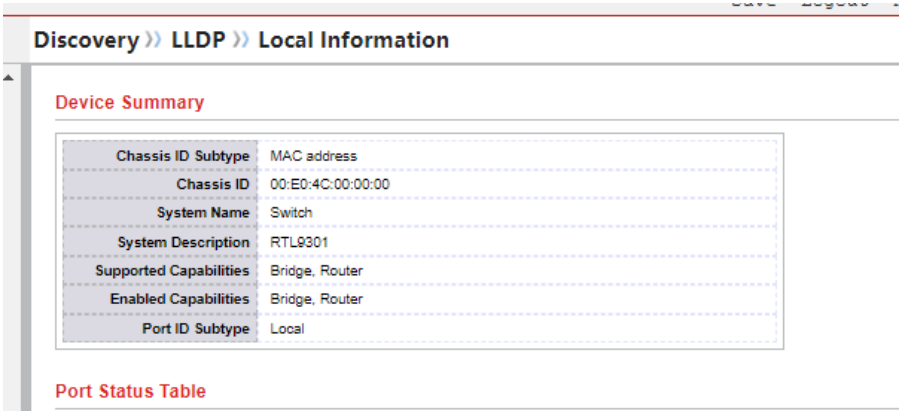
**Пример:**

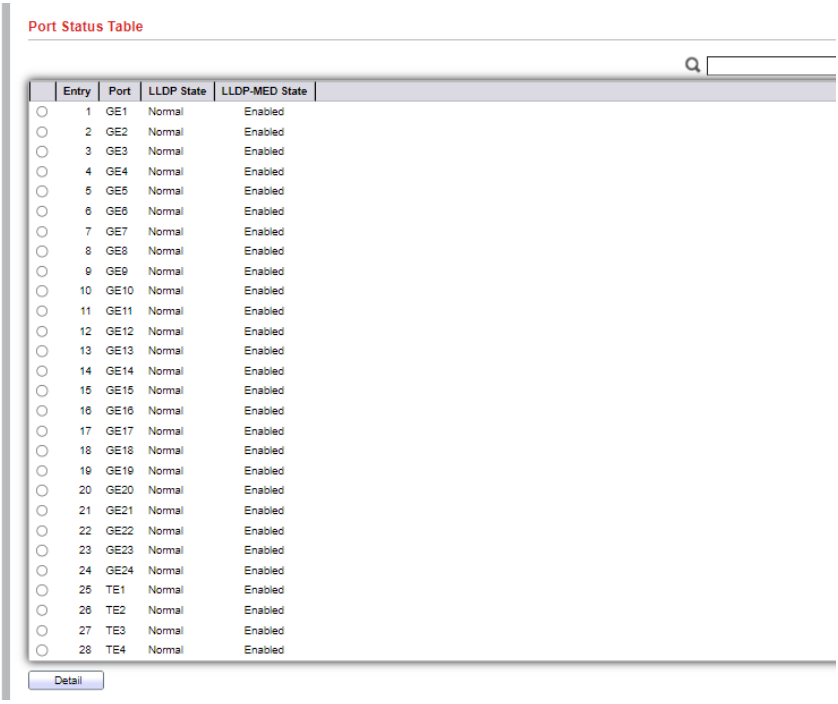
- **Порт 1:**
  - **In-Use:** 1420 байт
  - **Available:** 80 байт
  - **Status:** Normal

### 9.1.6. Локальная информация (Local Information)

**Для просмотра сведений о локальном устройстве в LLDP:**

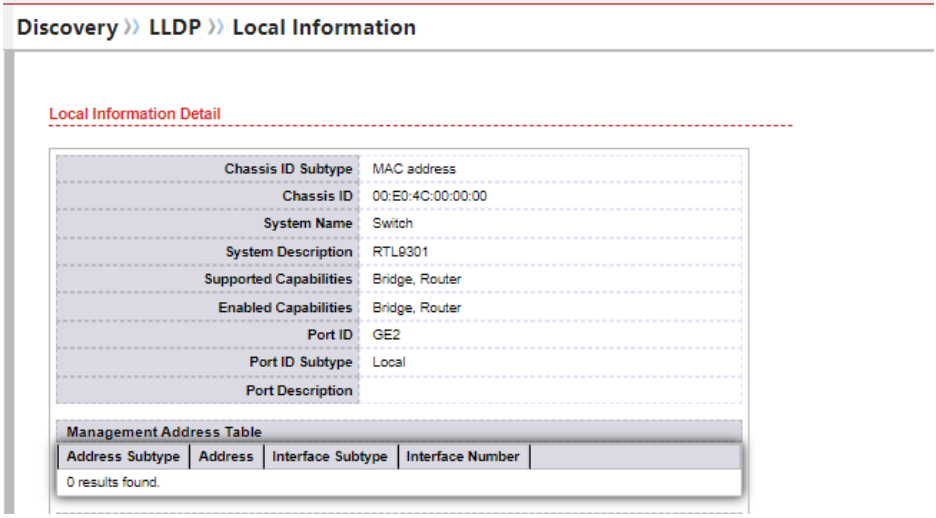
Перейдите в раздел **Discovery** > **LLDP** > **Local Information**.

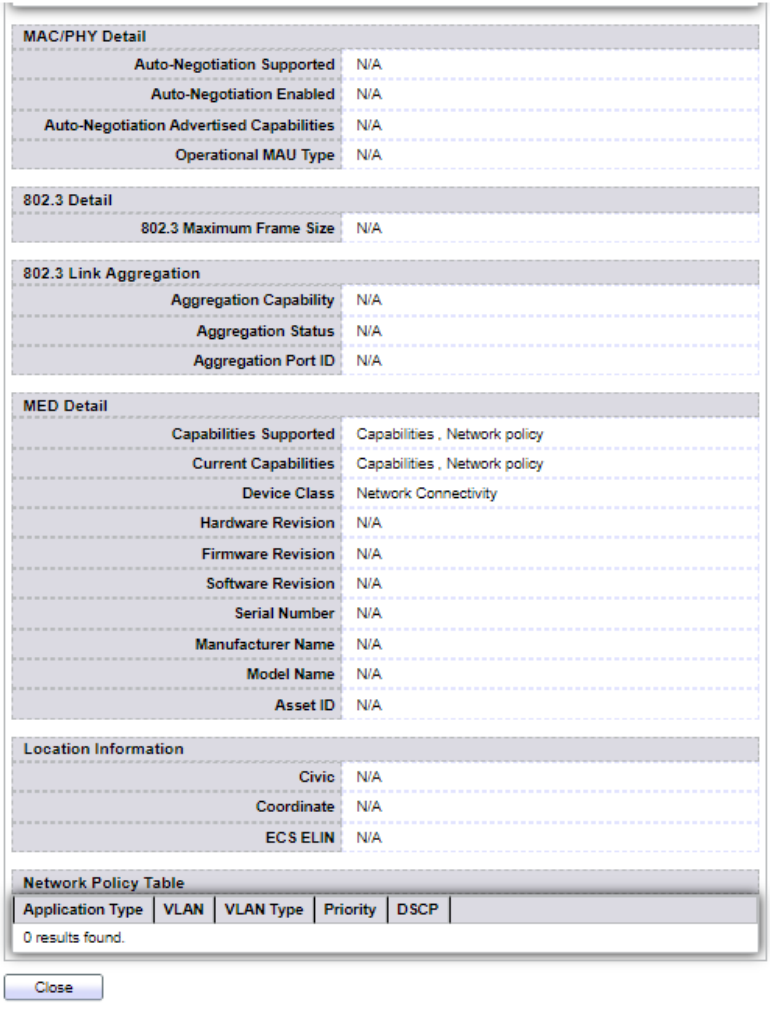


***Основная информация об устройстве***

| Параметр | Описание |
|---|---|
| **Chassis ID Subtype** | Тип идентификатора шасси (например, MAC-адрес). |
| **Chassis ID** | Идентификатор шасси. Если выбран MAC – отображается MAC-адрес коммутатора. |
| **System Name** | Имя коммутатора (например, "Switch-1"). |
| **System Description** | Описание системы (модель, версия ПО). |
| **Capabilities Supported** | Поддерживаемые функции: Bridge, Router, WLAN AP и др. |
| **Capabilities Enabled** | Активные функции устройства. |
| **Port ID Subtype** | Тип идентификатора порта (например, MAC, Interface Name). |
| **LLDP Status** | Режим работы LLDP: Tx/Rx, Tx Only, Rx Only, Disabled. |
| **LLDP Med Status** | Состояние LLDP-MED: Enabled или Disabled. |






### *Детальная информация о порте*

Нажмите кнопку **Detail** для выбранного порта, чтобы просмотреть:

- **Port ID** – идентификатор порта.
- **Port Description** – описание порта.
- **MED Capabilities** – поддержка LLDP-MED.

**Примечания:**

1. **System Name** и **System Description** помогают идентифицировать устройство в сети.
2. **Capabilities** указывают на роль устройства (например, Bridge для L2-коммутатора).

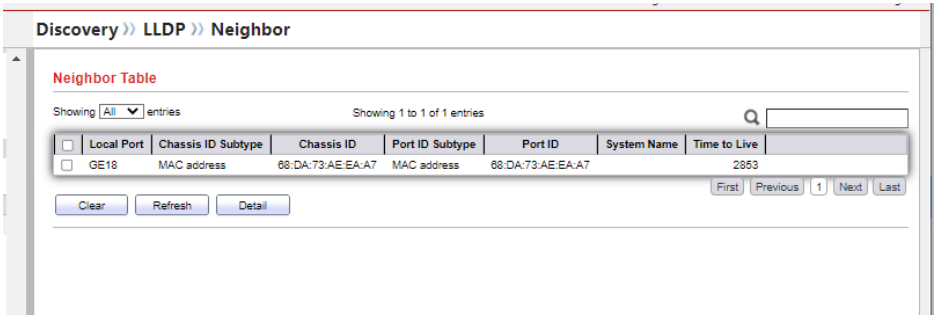
**Пример:**

- **Chassis ID:** 00:1A:2B:3C:4D:5E (MAC)
- **System Name:** "Core-Switch-3"
- **Capabilities Enabled:** Bridge, Router

### 9.1.7. Соседние устройства (Neighbor)

**Для просмотра информации об устройствах, обнаруженных через LLDP:**

Перейдите в раздел **Discovery** > **LLDP** > **Neighbor**.




***Список соседних устройств***

| Параметр | Описание |
|---|---|
| **Local Port** | Локальный порт, к которому подключено устройство. |
| **Chassis ID Subtype** | Тип идентификатора шасси (например, MAC-адрес). |

| Параметр | Описание |
|---|---|
| **Chassis ID** | Идентификатор шасси соседнего устройства. |
| **Port ID Subtype** | Тип идентификатора порта (например, Interface Name). |
| **Port ID** | Идентификатор порта соседнего устройства. |
| **System Name** | Имя соседнего устройства (если опубликовано). |
| **Time to Live (TTL)** | Время жизни записи (в секундах) до удаления из таблицы. |

***Детальная информация***

Нажмите кнопку **Detail** для выбранного устройства, чтобы просмотреть:

- **System Description** – описание системы (модель, версия ПО).
- **Capabilities** – функции устройства (Router, Switch, Phone и т.д.).
- **Management Address** – IP-адрес для управления.

**Примечания:**

1. **TTL** обновляется при получении новых LLDP-кадров.
2. **Port ID** помогает идентифицировать интерфейс на удаленном устройстве.

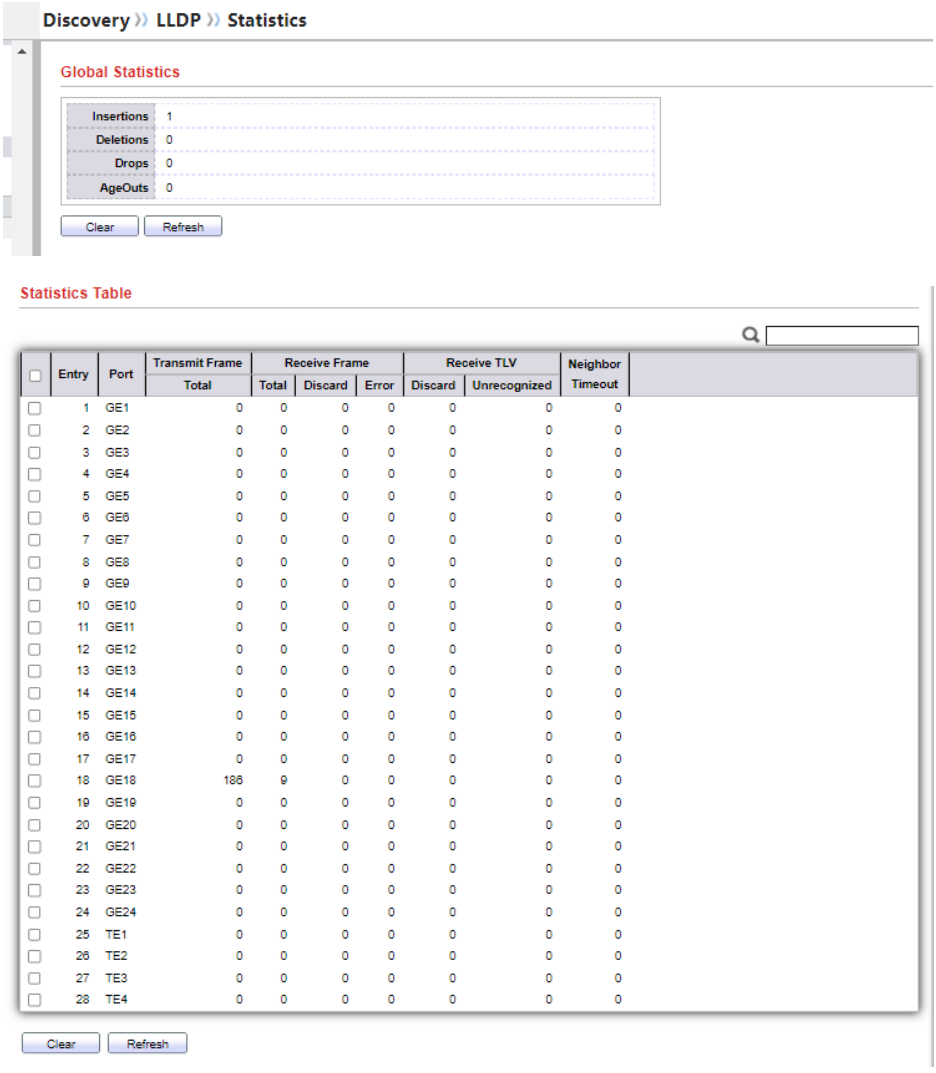
**Пример записи:**

- **Local Port:** GE18
- **Chassis ID:** 00:1B:2C:3D:4E:5F
- **System Name:** "Access-Switch-2"
- **TTL:** 120 сек

### 9.1.8. Статистика LLDP (Statistics)

**Для просмотра статистики работы LLDP:**

Перейдите в раздел **Discovery** > **LLDP** > **Statistics**.



***Глобальная статистика***

| Параметр | Описание |
|---|---|
| **Insertions** | Количество успешно добавленных записей о соседних устройствах. |
| **Deletions** | Количество удаленных записей (вручную или из-за отключения LLDP). |
| **Drops** | Количество отклоненных записей из-за нехватки ресурсов. |
| **Age Outs** | Количество записей, удаленных по истечении времени жизни (TTL). |

***Статистика по портам***

| Параметр | Описание |
|---|---|
| **Port** | Идентификатор порта. |
| **Transmit Frame Total** | Общее количество отправленных LLDP-кадров. |
| **Receive Frame Total** | Общее количество полученных LLDP-кадров. |
| **Receive Frame Discard** | Количество отброшенных LLDP-кадров (например, из-за ошибок). |
| **Receive Frame Error** | Количество невалидных LLDP-кадров. |
| **Receive TLV Discard** | Количество отброшенных TLV (например, неподдерживаемые типы). |
| **Receive TLV Unrecognized** | Количество нераспознанных TLV. |
| **Neighbor Timeout** | Количество записей, удаленных по таймауту. |

**Примечания:**

1. **Высокий уровень ошибок (Receive Frame Error)** может указывать на:
   - Повреждение кадров в сети.
   - Несовместимость оборудования.

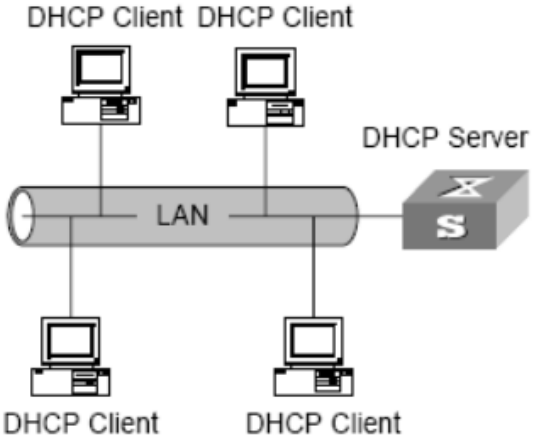
2. **Unrecognized TLV** – нормально для устройств разных производителей.

**Рекомендации:**

- Если **Drops** > 0, попробуйте увеличить размер таблицы LLDP
- Мониторинг **Age Outs** поможет выявить проблемы с подключением.

## 10. DHCP (Dynamic Host Configuration Protocol)

**DHCP** – это протокол динамической настройки хостов, разработанный для автоматического распределения IP-адресов и других сетевых параметров (маска подсети, шлюз, DNS) в компьютерных сетях.




***Принцип работы DHCP***

1. **Режим клиент/сервер**:
    - **DHCP-клиент** (ПК, телефон, IoT-устройство) запрашивает конфигурацию.
    - **DHCP-сервер** (роутер, коммутатор, сервер) назначает параметры на основе политик.

2. **Типичный сценарий**:
    - Один DHCP-сервер обслуживает множество клиентов.
    - Подходит для сетей с мобильными устройствами (Wi-Fi, ноутбуки).

***Решаемые задачи***

- **Динамическое выделение IP**: Автоматизация при изменении местоположения устройств.
- **Ограничение адресов**: Пул адресов для временного использования (например, гостевые сети).
- **Централизованное управление**: Настройка VLAN, QoS через DHCP-опции.

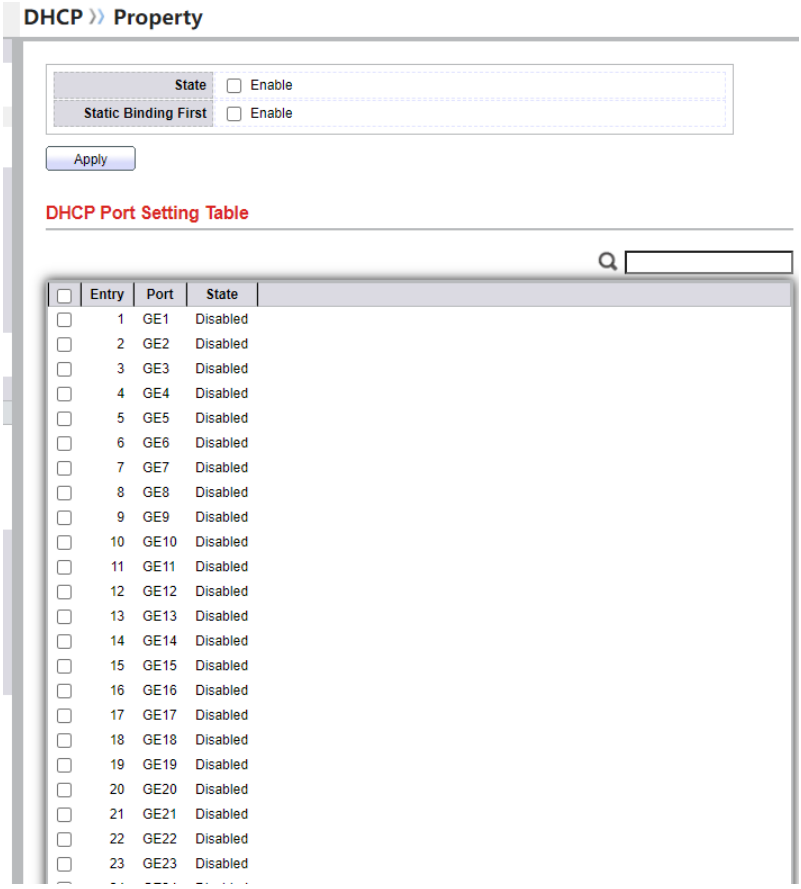
**Пример DHCP-опций**:

- **Option 3**: Шлюз по умолчанию.
- **Option 6**: DNS-серверы.
- **Option 66**: TFTP-сервер (для IP-телефонов).

## 10.1. Настройка протокола DHCP (DHCP Property)

**Для включения/отключения DHCP-сервера и настройки портов:**

Перейдите в раздел **DHCP** > **Property**

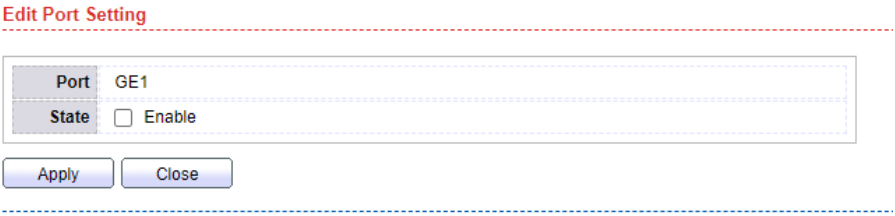



***Глобальные параметры DHCP***

- **Состояние DHCP-сервера**: Включено (Enable) / Отключено (Disable).
- **Список портов**: Отображает текущие настройки DHCP для каждого порта.

***Настройка портов***

1. Нажмите кнопку **Edit (Изменить)** для выбранного порта.
2. Параметры:
    - **State**: Включить/отключить функцию DHCP-сервера на порту.




**Примечания:**

1. Для портов со значением **State = Enable** клиенты смогут получать IP-адреса.
2. Рекомендуется отключать DHCP на портах, подключенных к другим DHCP-серверам (во избежание конфликтов).

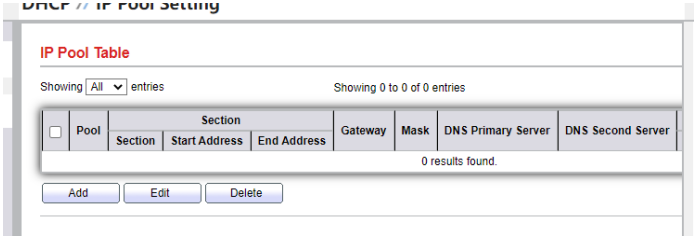
**Пример:**

- Порт 1 (клиентская VLAN):
    - State: **Enable**
- Порт 24 (магистраль):
    - State: **Disable**

## 10.2. Настройка пула IP адресов DHCP (Address Pool Configuration)

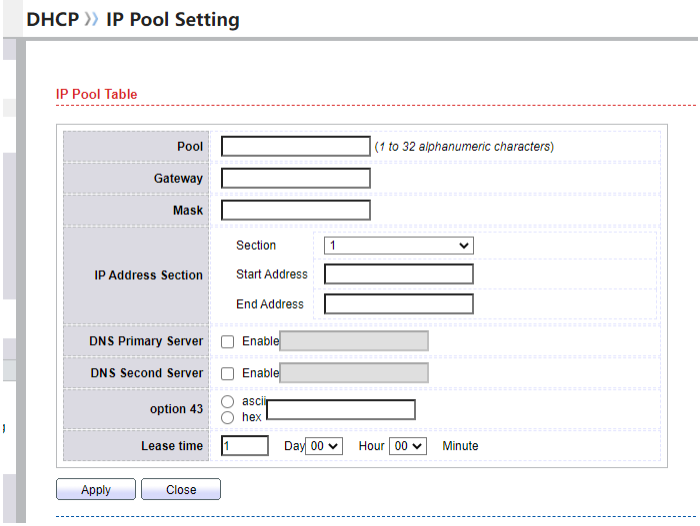
**Для создания и управления пулами DHCP IP адресов:**

Перейдите в раздел **DHCP** > **IP Pool Setting**.




На данной странице отображается список всех настроенных пулов с параметрами

- **Имя пула**
- **Диапазон IP-адресов**
- **Маска подсети**
- **Шлюз**
- **DNS-серверы (основной и резервный)**



***Добавление/редактирование пула***

1. Нажмите **Add (Добавить)** или **Edit (Изменить)**.
2. Укажите параметры:

| Параметр | Описание |
|---|---|
| **Pool** | Уникальное имя пула адресов (например, "Office-VLAN10"). |
| **Gateway** | Основной шлюз (например, 192.168.1.1). |
| **Mask** | Маска подсети (например, 255.255.255.0). |
| **IP Address Section** | Диапазон адресов (например, 192.168.1.100–192.168.1.200). |
| **DNS Primary Server** | Основной DNS-сервер (например, 8.8.8.8, 1.1.1.1). |
| **DNS Second Server** | Резервный DNS-сервер (например, 8.8.8.8, 1.1.1.1). |
| **Lease Time** | Время аренды адреса (например, 24 часа). |

3. Сохраните настройки (**Apply**)

**Примечания:**

- Исключите статические IP-адреса из пула (например, серверы).
- Для гостевых сетей используйте короткое время аренды (2–4 hours).

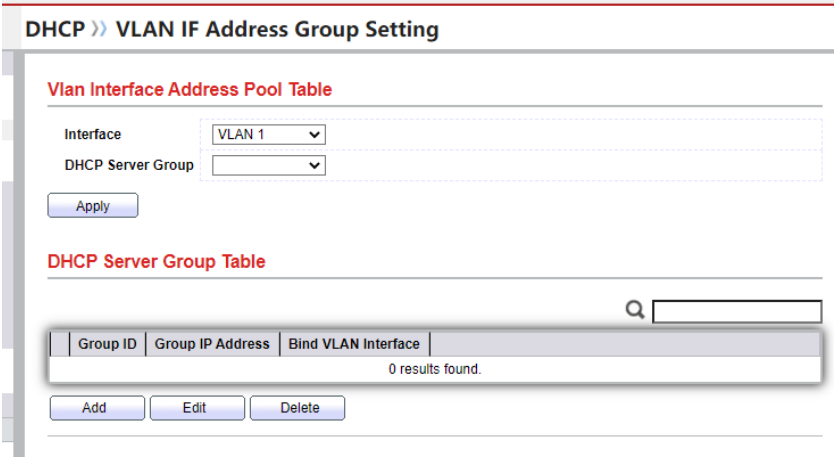
**Пример:**

- **Pool:** Guest-WiFi
- **IP Address Section:** 192.168.10.50–192.168.10.150
- **Lease Time:** 4 hours

## 10.3. Настройка групп адресов VLAN-интерфейсов (VLAN IF Address Group Setting)

**Для привязки DHCP-пулов к VLAN-интерфейсам:**

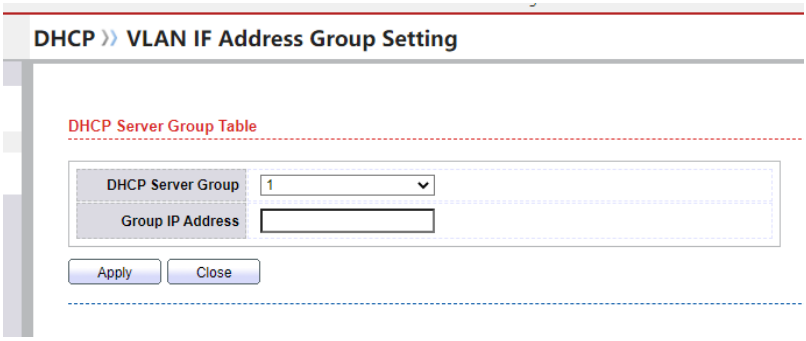
Перейдите в раздел **DHCP** > **VLAN IF Address Group Setting**.




На данной странице отображается таблица с привязками:

- **Interface** – название VLAN интерфейса (должен быть создан заранее).
- **DHCP Server Group** – выбор пула DHCP серверов, к которому будет привязан VLAN выбранный ранее.

- **Group ID** – идентификатор группы VLAN.
- **Group ID address** – адрес группы VLAN-интерфейсов.
- **Bind VLAN Interface** – связанные с группой VLAN интерфейсы.




***Добавление/редактирование группы***

1. Нажмите **Add (Добавить)** или **Edit (Изменить)**.
2. Укажите параметры:

| Параметр | Описание |
|---|---|
| **DHCP Server Group** | Выберите группу из списка (должна быть создана заранее). |
| **Interface IP** | IP-адрес VLAN-интерфейса (например, 192.168.10.1/24). |

3. Сохраните изменения.

**Примечания:**

- Группы серверов позволяют распределять нагрузку между несколькими DHCP-серверами.
- Для резервирования настройте **минимум 2 сервера** в группе.

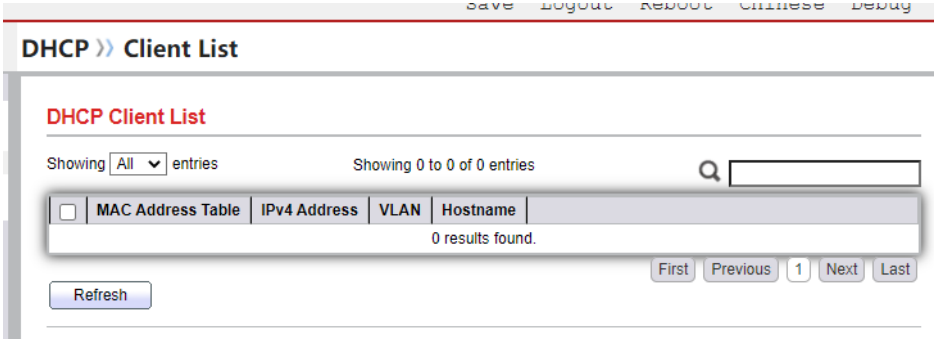
**Пример:**

- **VLAN 10:**
  - **Interface IP:** 192.168.10.1/24
  - **DHCP Server Group:** "Office-Servers"

## 10.4. Список клиентов DHCP (Client List)

**Для просмотра информации о клиентах, получивших IP-адреса через DHCP:**

Перейдите в раздел **DHCP** > **Client List**.




***Информация о клиентах***

| Параметр | Описание |
|---|---|
| **MAC Address Table** | Физический адрес (MAC) клиентского устройства. |
| **IPv4 Address** | Выданный клиенту IPv4 адрес. |
| **VLAN** | Идентификатор VLAN, в которой находится клиент. |
| **Hostname** | Имя устройства (если предоставлено клиентом). |

**Примечания:**

1. Список обновляется автоматически при получении новых DHCP-запросов.
2. Для принудительного обновления нажмите кнопку **Refresh (Обновить)**.

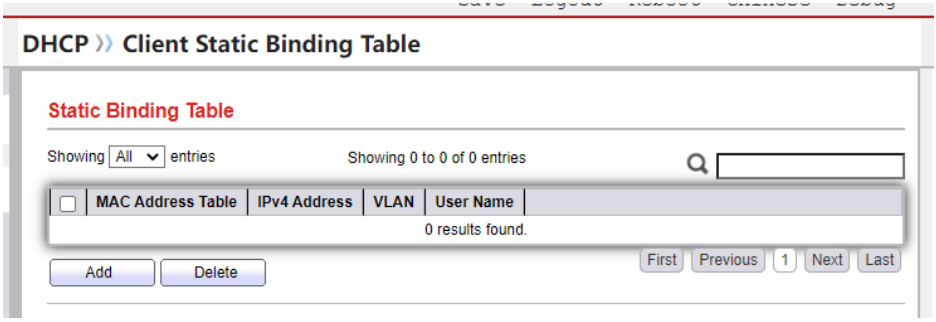
**Пример записи:**

- **IPv4:** 192.168.1.100
- **MAC:** 00:1A:2B:3C:4D:5E
- **VLAN:** 10
- **Port:** GE4

## 10.5. Таблица статической привязки клиентов DHCP (Client Static Binding Table)

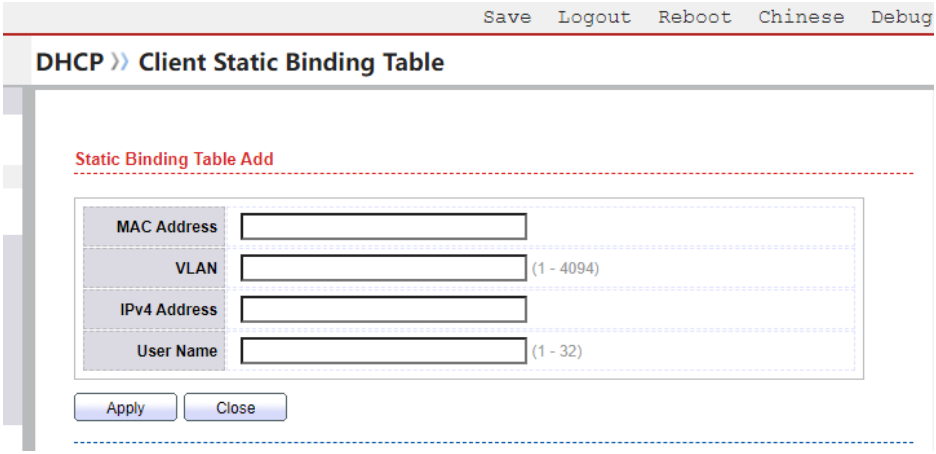
**Для настройки фиксированных (статических) IP-адресов для клиентов:**

Перейдите в раздел **DHCP** > **Client Static Binding Table**.




На данной странице отображается таблица с привязанными IP-адресами:

- **MAC Address Table** – физический (MAC) адрес устройства.
- **IPv4 Address** – закрепленный за клиентом IPv4 адрес.
- **VLAN** – идентификатор VLAN.
- **User Name** – описание




***Добавление новой привязки***

1. Нажмите **Add (Добавить)**.
2. Заполните поля:

| Параметр | Описание |
|---|---|
| **MAC Address** | MAC-адрес устройства (формат: XX-XX-XX-XX-XX-XX или XXXX.XXXX.XXXX). |
| **VLAN** | VLAN, в которой работает устройство. |
| **IPv4 Address** | Фиксированный IP-адрес (например, 192.168.1.50). |
| **User Name** | Комментарий |

3. Сохраните настройки (**Apply**)

**Примечания:**

- Статические привязки имеют приоритет над динамическими.
- Используйте для:
  - Серверов
  - Сетевых принтеров.
  - IP-телефонов.

**Пример:**

- **IPv4:** 192.168.1.100
- **MAC:** 00-1A-2B-33-44-55
- **VLAN:** 10
- **User Name:** "Main Office Phone"

# 11. Настройка Multicast (IGMP, MLD, Static)

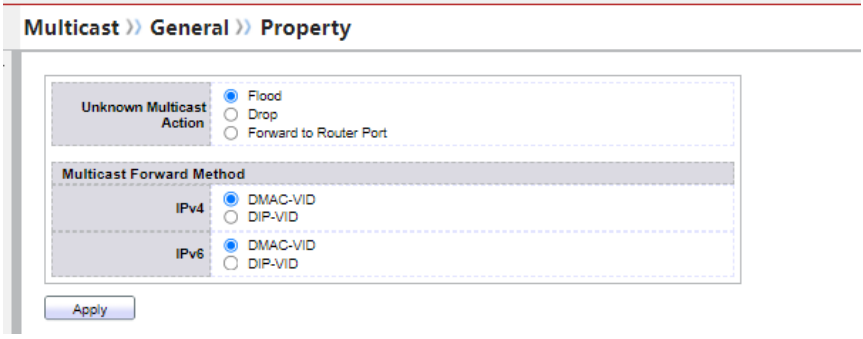
## 11.1. Общие настройки (General)

Раздел **General** предназначен для базовой конфигурации функций IGMP (IPv4) и MLD (IPv6).

### 11.1.1. Свойства Multicast (Property)

**Для настройки методов мультикаст-маршрутизации:**

Перейдите в раздел **Multicast** > **General** > **Property**.




***Параметры обработки мультикаст-трафика***

| Параметр | Описание |
|---|---|
| **Unknown Multicast Action** | Действие для неизвестного мультикаст-трафика: |
| | **Drop** – отбрасывать пакеты. |

| Параметр | Описание |
|---|---|
| | **Flood** – отправлять на все порты (по типу широковещательного трафика). |
| | **Forward to Router port** – отправлять только на порты маршрутизаторов. |
| **IPv4 Forward Method** | Метод маршрутизации для IPv4: |
| | **DMAC-VID** – на основе MAC-адреса назначения + VLAN ID. |
| | **DIP-VID** – на основе IP-адреса назначения + VLAN ID. |
| **IPv6 Forward Method** | Метод маршрутизации для IPv6: |
| | **DMAC-VID** – на основе MAC-адреса назначения + VLAN ID. |
| | **DIP-VID** – на основе младших 32 бит IPv6-адреса + VLAN ID. |

**Примечания:**

1. **Router port** – безопасный вариант, предотвращает flooding для трафика в пользовательских VLAN.
2. **DIP-VID** обеспечивает более точную маршрутизацию для IPv4/IPv6.

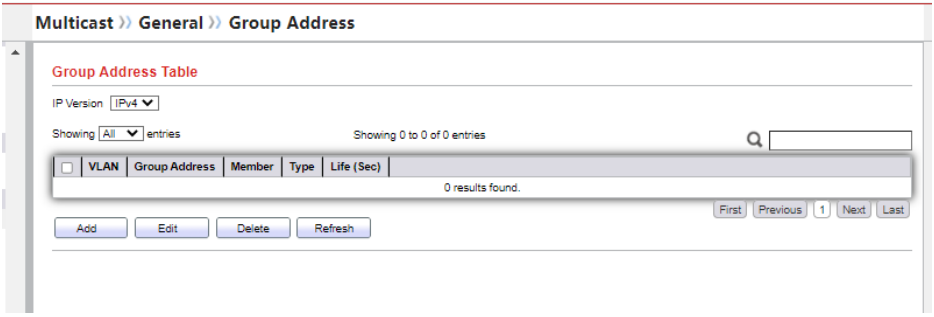
**Рекомендации:**

- Для IP-телевидения используйте **DIP-VID**.
- В средах с VoIP активируйте **Router port** для неизвестного трафика.

### 11.1.2. Группы Multicast (Group Address)

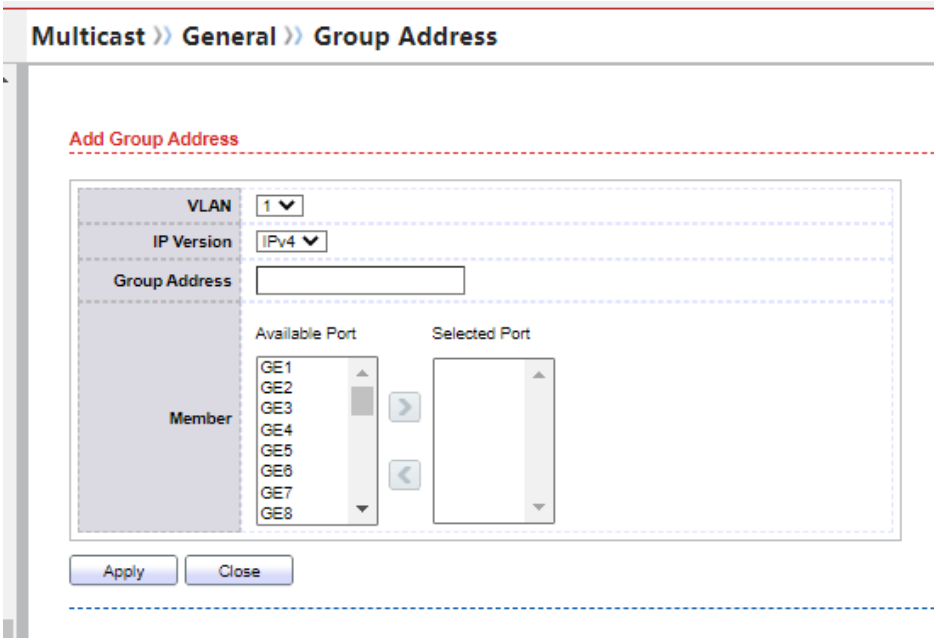
**Для просмотра и управления мультикаст-группами:**

Перейдите в раздел **Multicast** > **General** > **Group Address**.




***Просмотр мультикаст-групп***

| Параметр | Описание |
|---|---|
| **IP Version** | Версия IP: IPv4 или IPv6. |
| **VLAN** | Идентификатор VLAN, к которой относится группа. |
| **Group Address** | IP-адрес мультикаст-группы (например, 239.255.255.250 для IPv4). |
| **Member** | Порта-участники группы. |
| **Type** | Тип группы: Static (ручная настройка)<br>или Dynamic (автоматическое добавление через IGMP/MLD). |
| **Life (Sec)** | Время жизни динамической группы (в секундах). |




***Добавление/редактирование группы***

| Параметр | Описание |
|---|---|
| **VLAN** | Выберите VLAN для группы. |
| **IP Version** | Укажите версию IP (IPv4 или IPv6). |
| **Group Address** | Введите IP-адрес группы |
| **Member** | Выберите порты: |
| | **Available Port** – доступные порты. |
| | **Selected Port** – порты, включенные в группу. |

**Примечания:**

1. **Динамические группы** автоматически добавляются при объединении клиентов через IGMPv3/MLDv2.
2. **Статические группы** используются для:

- Фиксации портов для критического трафика (например, видеонаблюдение).
- Ограничения доступа к мультикаст-потокам.

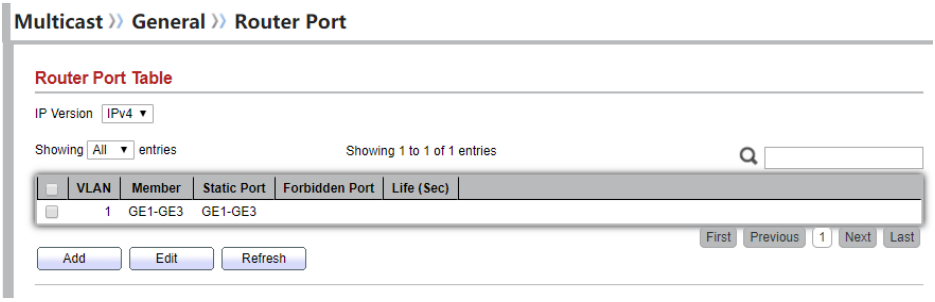
**Пример настройки:**

- **VLAN:** 10
- **IP Version:** IPv4
- **Group Address:** 239.1.1.1
- **Member Ports:** GE4, GE2

### 11.1.3. Настройка Router портов (Router Port)

**Для управления Router портами в мультикаст-трафике:**

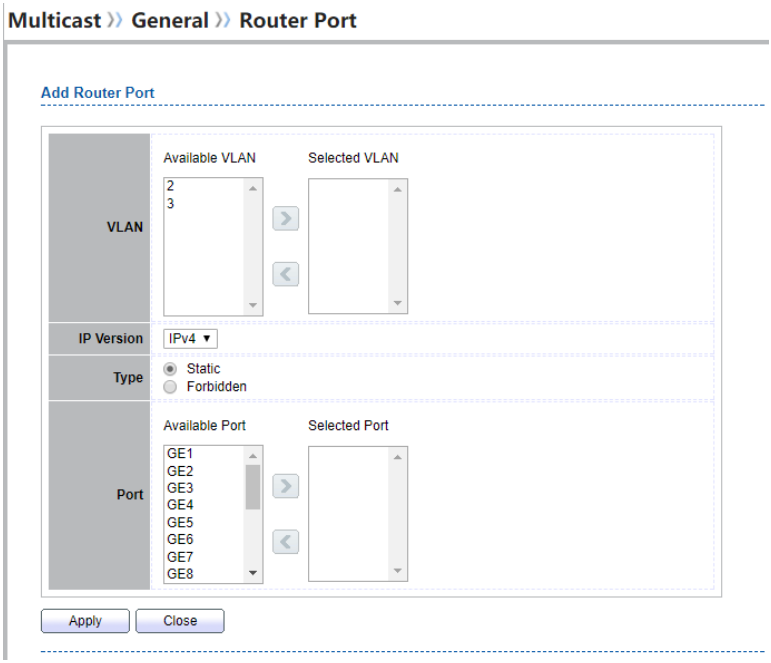
Перейдите в раздел **Multicast** > **General** > **Router Port**.




***Текущие порты маршрутизаторов***

| Параметр | Описание |
|---|---|
| **IP Version** | Версия IP: IPv4 (IGMP) или IPv6 (MLD). |
| **VLAN** | Идентификатор VLAN. |
| **Member** | Router порты (включая статические и динамические). |
| **Static Port** | Порты, назначенные вручную как Router порты |

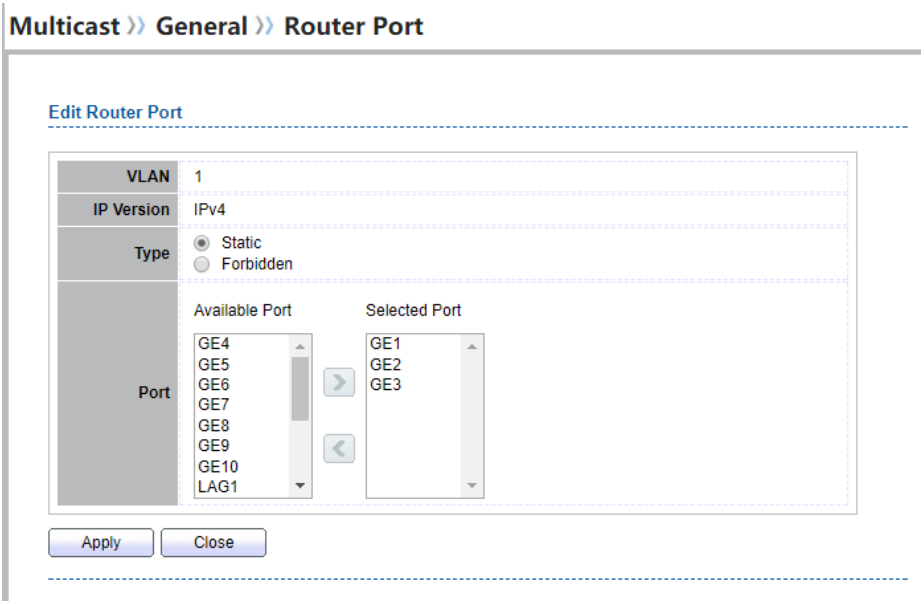
| Параметр | Описание |
|---|---|
| **Forbidden Port** | Порты, запрещенные для работы в качестве Router портов |
| **Life (Sec)** | Время жизни динамически назначенного порта (в секундах). |




***Настройка портов маршрутизаторов***

| Параметр | Описание |
|---|---|
| **VLAN** | Выберите VLAN: |
| | **Available VLAN** – доступные VLAN. |
| | **Selected VLAN** – выбранные VLAN. |
| **IP Version** | Укажите версию IP (IPv4 или IPv6). |
| **Type** | Тип порта: |

| Параметр | Описание |
|---|---|
| | **Static** – статический порт. |
| | **Forbidden** – запрет на работу в качестве Router порта. |
| **Port** | Выберите порты: |
| | **Available Port** – доступные порты. |
| | **Selected Port** – выбранные порты. |




**Примечания:**

1. **Статические порты** используются для:
   - Подключения маршрутизаторов вручную (например, GE16).
   - Гарантированного прохождения мультикаст-трафика.
2. **Forbidden Port** блокирует IGMP/MLD-запросы на указанных портах.

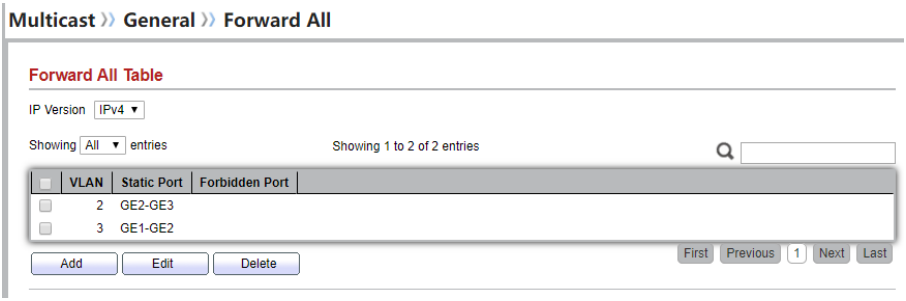
**Пример настройки:**

- **VLAN:** 10
- **IP Version:** IPv4
- **Type:** Static
- **Selected Port:** GE16

### 11.1.4. Принудительная пересылка Multicast трафика (Forward All)

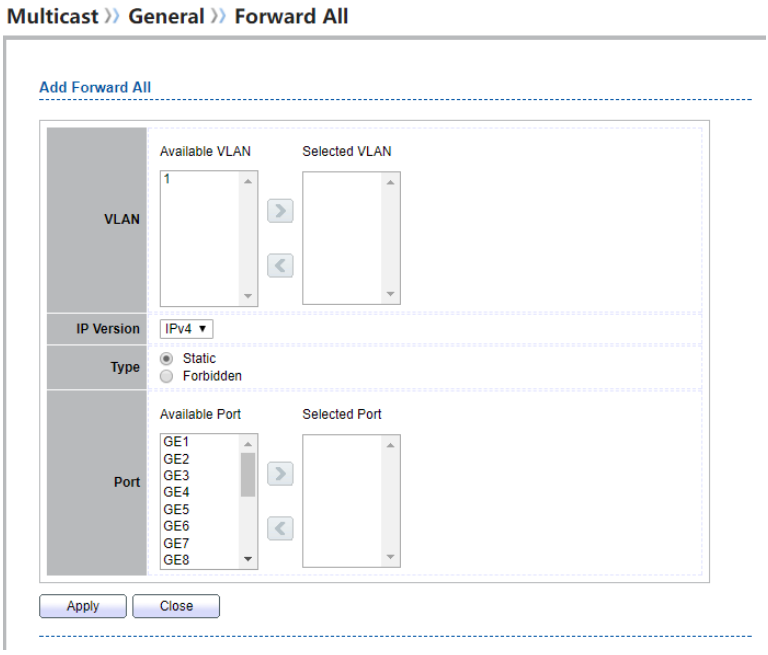
**Для настройки принудительной пересылки мультикаст-трафика:**

Перейдите в раздел **Multicast** > **General** > **Forward All**.



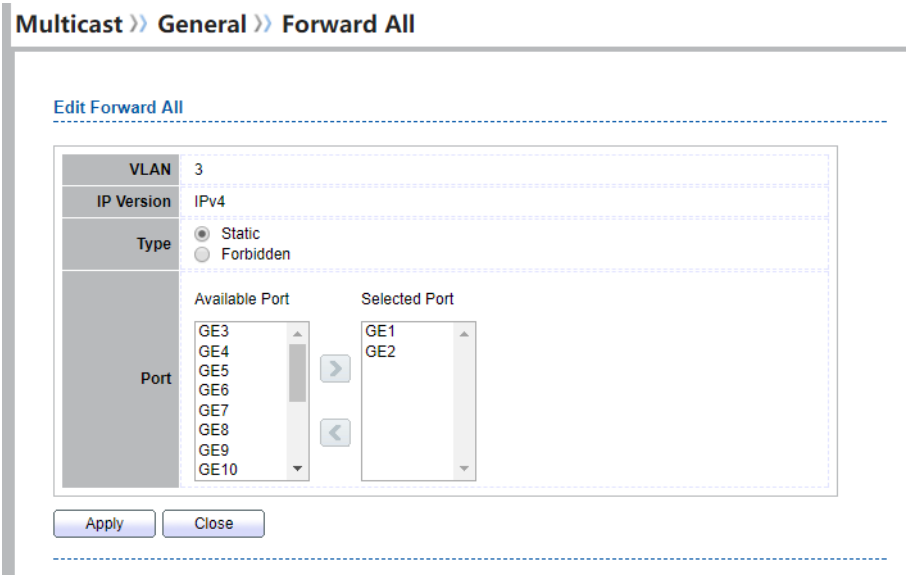

***Текущие настройки Forward All***

| Параметр | Описание |
|---|---|
| **IP Version** | Версия IP: IPv4 или IPv6. |
| **VLAN** | Идентификатор VLAN. |
| **Static Port** | Порты, на которые **всегда** пересылается мультикаст-трафик (даже без подписки IGMP/MLD). |
| **Forbidden Port** | Порты, на которые мультикаст-трафик **никогда** не пересылается. |




***Добавление/редактирование правил***

| Параметр | Описание |
|---|---|
| **VLAN** | Выберите VLAN: |
| | **Available VLAN** – доступные VLAN. |
| | **Selected VLAN** – выбранные VLAN. |
| **IP Version** | Укажите версию IP (IPv4 или IPv6). |
| **Type** | Тип правила: |
| | **Static** – трафик всегда пересылается на выбранные порты. |
| | **Forbidden** – трафик никогда не пересылается на выбранные порты. |
| **Port** | Выберите порты: |
| | **Available Port** – доступные порты. |
| | **Selected Port** – порты, к которым применяется правило. |




**Примечания:**

1. **Static Port** используется для:
   - IP-камер с Multicast передачей.
   - Устройств, не поддерживающих IGMP/MLD.
2. **Forbidden Port** блокирует Multicast трафик для:
   - Пользовательских портов (например, ПК).
   - Экономии полосы пропускания.

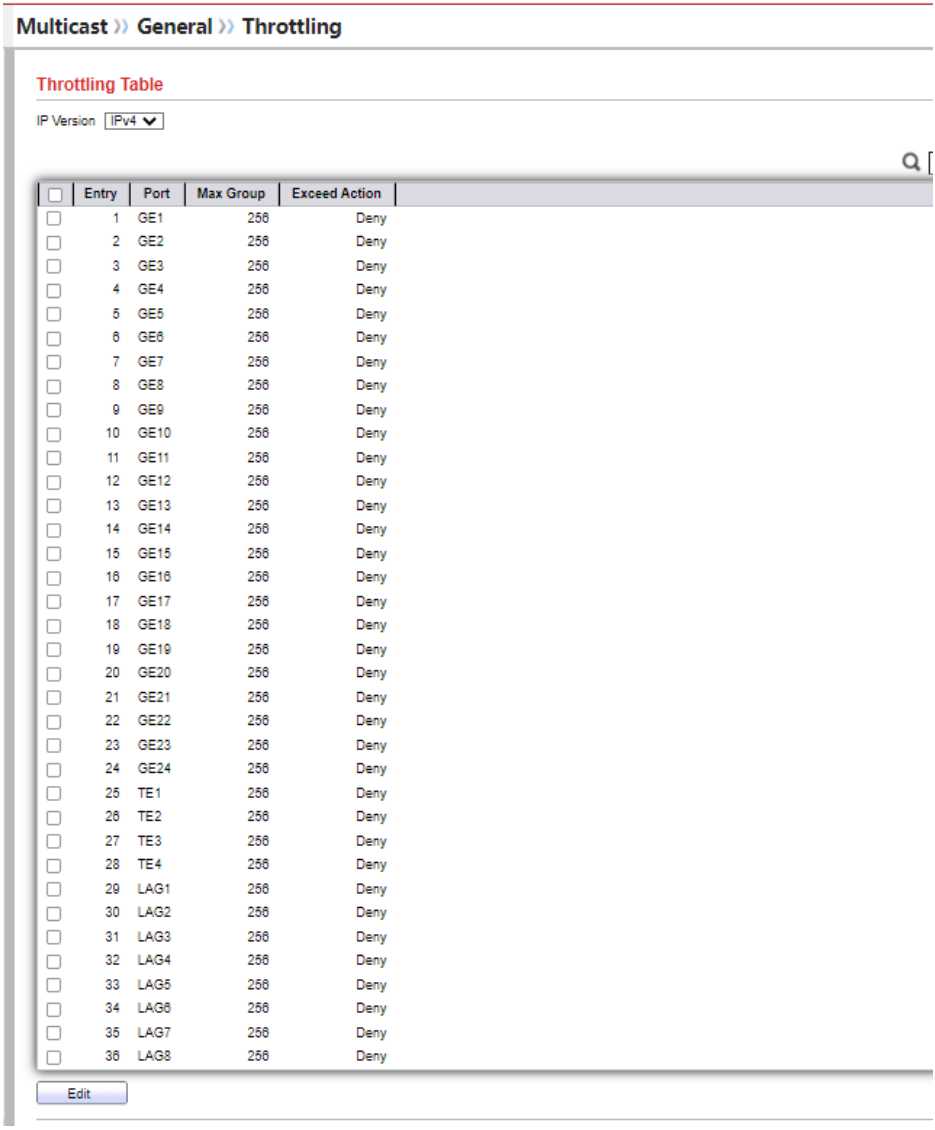
**Пример настройки:**

- **VLAN:** 20
- **IP Version:** IPv4
- **Type:** Static
- **Selected Port:** GE14 (для IP-камеры)

### 11.1.5. Ограничение на кол-во Multicast групп (Throttling)

**Для настройки ограничений на количество мультикаст-групп на порту:**

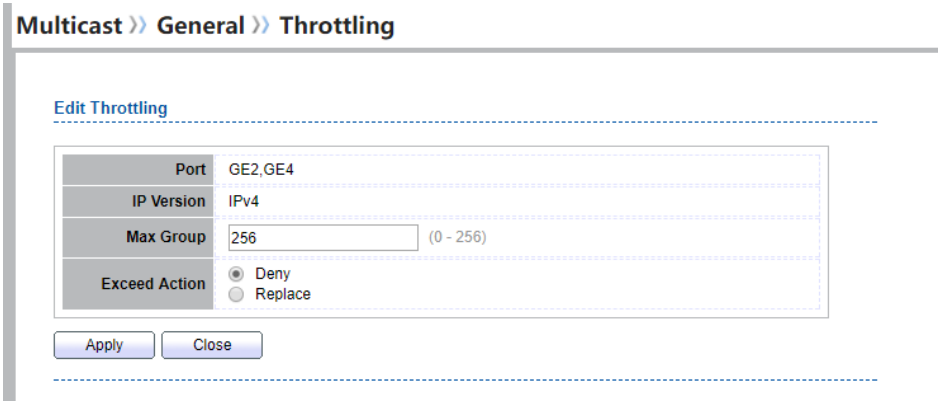
Перейдите в раздел **Multicast** > **General** > **Throttling**.




| Entry | Port | Max Group | Exceed Action |
|---|---|---|---|
| 1 | GE1 | 256 | Deny |
| 2 | GE2 | 256 | Deny |
| 3 | GE3 | 256 | Deny |
| 4 | GE4 | 256 | Deny |
| 5 | GE5 | 256 | Deny |
| 6 | GE6 | 256 | Deny |
| 7 | GE7 | 256 | Deny |
| 8 | GE8 | 256 | Deny |
| 9 | GE9 | 256 | Deny |
| 10 | GE10 | 256 | Deny |
| 11 | GE11 | 256 | Deny |
| 12 | GE12 | 256 | Deny |
| 13 | GE13 | 256 | Deny |
| 14 | GE14 | 256 | Deny |
| 15 | GE15 | 256 | Deny |
| 16 | GE16 | 256 | Deny |
| 17 | GE17 | 256 | Deny |
| 18 | GE18 | 256 | Deny |
| 19 | GE19 | 256 | Deny |
| 20 | GE20 | 256 | Deny |
| 21 | GE21 | 256 | Deny |
| 22 | GE22 | 256 | Deny |
| 23 | GE23 | 256 | Deny |
| 24 | GE24 | 256 | Deny |
| 25 | TE1 | 256 | Deny |
| 26 | TE2 | 256 | Deny |
| 27 | TE3 | 256 | Deny |
| 28 | TE4 | 256 | Deny |
| 29 | LAG1 | 256 | Deny |
| 30 | LAG2 | 256 | Deny |
| 31 | LAG3 | 256 | Deny |
| 32 | LAG4 | 256 | Deny |
| 33 | LAG5 | 256 | Deny |
| 34 | LAG6 | 256 | Deny |
| 35 | LAG7 | 256 | Deny |
| 36 | LAG8 | 256 | Deny |

***Текущие ограничения***

| Параметр | Описание |
|---|---|
| **IP Version** | Версия IP: IPv4 (IGMP) или IPv6 (MLD). |
| **Entry** | Номер записи. |
| **Port** | Имя порта. |
| **Max Group** | Максимальное количество групп, которые порт может изучить (например, 50). |
| **Exceed Action** | Действие при превышении лимита: Deny или Replace. |




***Редактирование ограничений***

| Параметр | Описание |
|---|---|
| **Port** | Выберите порт для настройки. |
| **IP Version** | Укажите версию IP (IPv4 или IPv6). |
| **Max Group** | Установите максимальное количество групп (например, 20 для VoIP). |
| **Exceed Action** | Выберите действие при превышении: |
| | **Deny** – новые группы игнорируются. |
| | **Replace** – случайная замена одной из существующих групп. |

**Примечания:**

1. **Deny** рекомендуется для портов с критически важными группами (например, видеонаблюдение).
2. **Replace** подходит для клиентских портов с динамическими подписками (VoIP, IPTV).

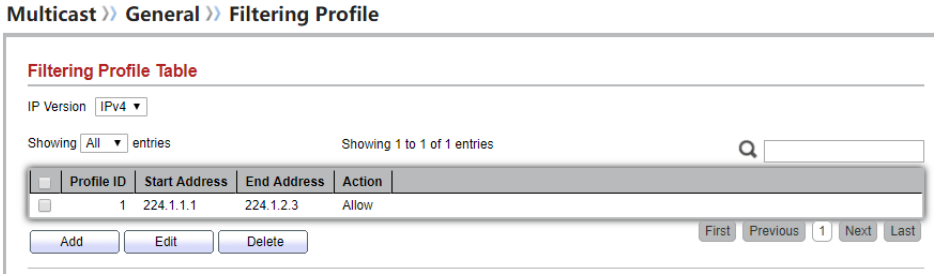
**Пример настройки:**

- **Порт:** GE16
- **IP Version:** IPv4
- **Max Group:** 10
- **Exceed Action:** Replace

### 11.1.6. Фильтрация Multicast групп (Filtering Profile)

**Для настройки фильтрации Multicast групп:**

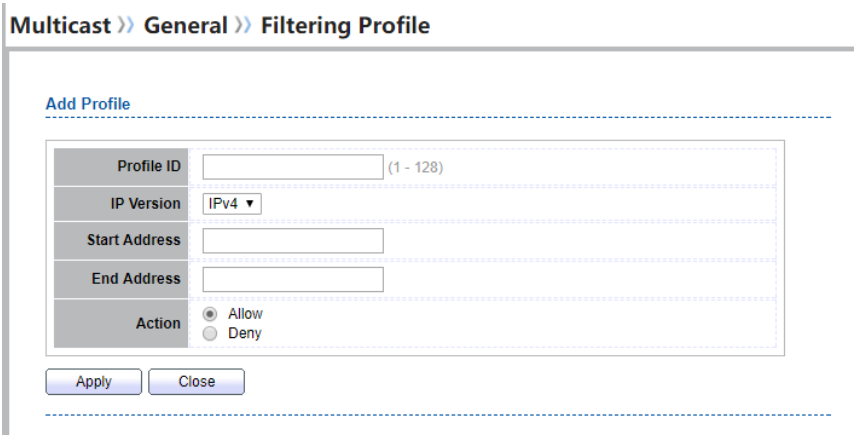
Перейдите в раздел **Multicast** > **General** > **Filtering Profile**.

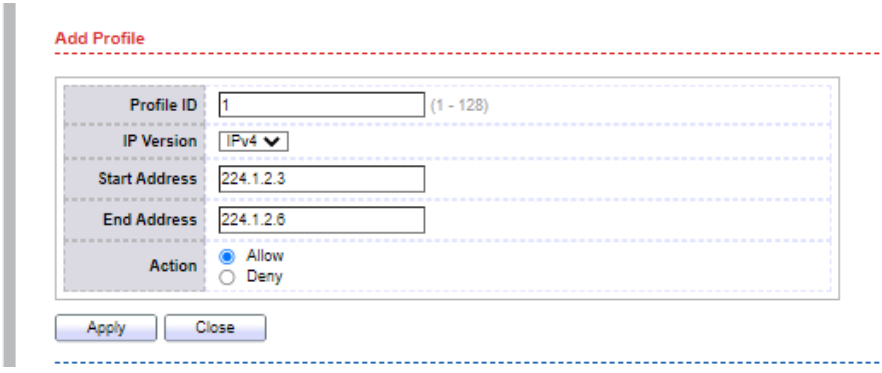



***Текущие профили***

| Параметр | Описание |
|---|---|
| **IP Version** | Версия IP: IPv4 (IGMP) или IPv6 (MLD). |
| **Profile ID** | Идентификатор профиля. |

| Параметр | Описание |
|---|---|
| **Start Address** | Начальный адрес диапазона групп (например, 224.1.1.1). |
| **End Address** | Конечный адрес диапазона (например, 224.1.2.3). |
| **Action** | Действие: Allow (разрешить) или Deny (запретить). |




***Добавление/редактирование профиля***

| Параметр | Описание |
|---|---|
| **Profile ID** | Уникальный ID профиля (1–128). |

| Параметр | Описание |
|---|---|
| **IP Version** | Выберите версию IP (IPv4 или IPv6). |
| **Start Address** | Укажите начальный адрес диапазона. |
| **End Address** | Укажите конечный адрес диапазона. |
| **Action** | Выберите действие: |
| | **Allow** – разрешить группы в диапазоне. |
| | **Deny** – блокировать группы в диапазоне. |

**Примечания:**

1. **Диапазон адресов** можно задать как для одиночной группы (например, 224.1.1.1–224.1.1.1), так и для пула.
2. **Deny** полезен для блокировки нежелательного трафика (например, 224.255.255.250 для SSDP).

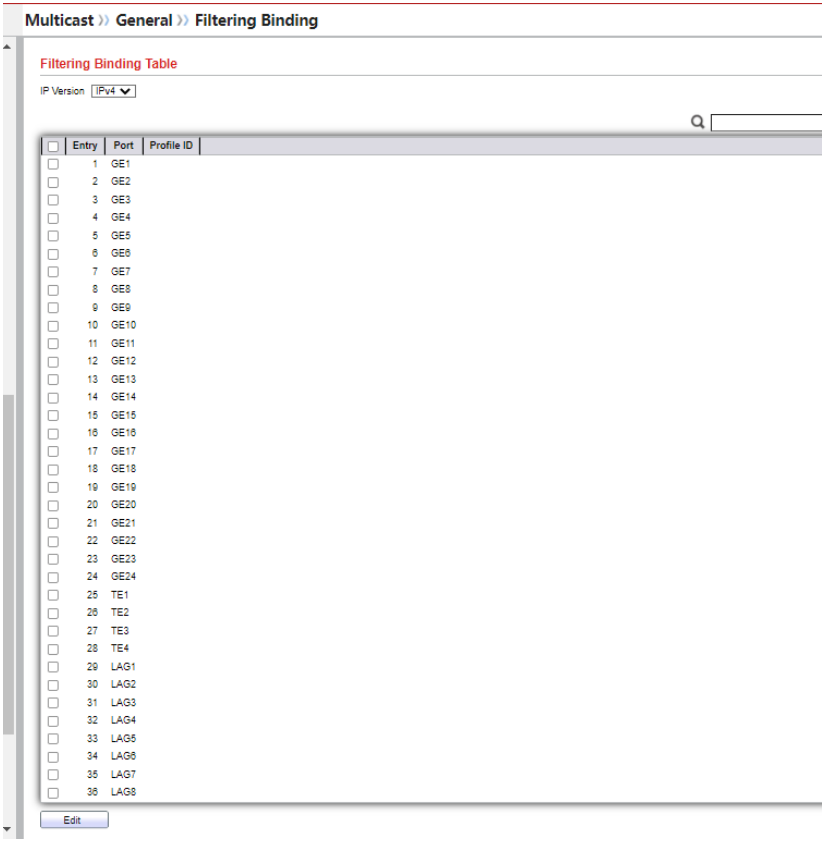
**Пример настройки:**

- **Profile ID:** 10
- **IP Version:** IPv4
- **Start Address:** 224.1.2.3
- **End Address:** 224.1.2.6
- **Action:** Allow

### 11.1.7. Привязка профилей фильтрации к портам (Filtering Binding)

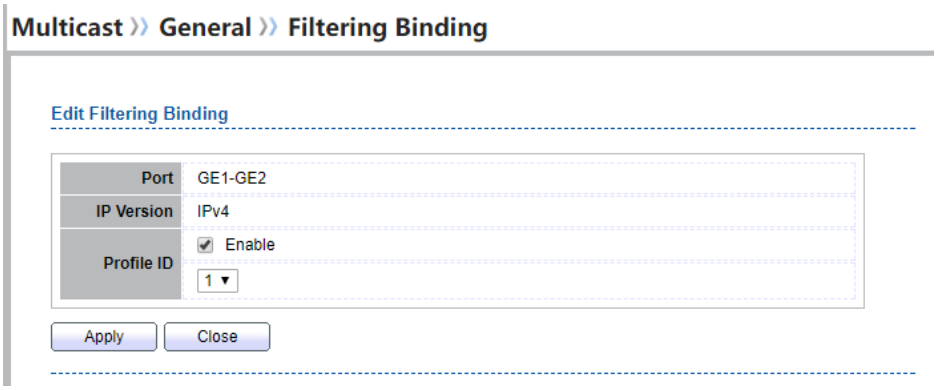
**Для привязки профилей фильтрации к портам:**

Перейдите в раздел **Multicast** > **General** > **Filtering Binding**.




***Текущие привязки***

| Параметр | Описание |
|---|---|
| **Entry** | Номер записи. |
| **Port** | Номер порта. |
| **Profile ID** | Идентификатор привязанного профиля (если есть). |




***Редактирование привязки***

| Параметр | Описание |
|---|---|
| **Port** | Выберите порт для настройки. |
| **IP Version** | Укажите версию IP (IPv4 или IPv6). |
| **Profile ID** | Действие: |
| | **Enable** → выберите ID профиля из списка. |
| | **Disable** → удаляет привязку профиля к порту. |

**Примечания:**

1. Профиль должен быть предварительно создан в разделе **Filtering Profile**.
2. Привязка позволяет:
   - Разрешить/запретить мультикаст-группы на конкретных портах.
   - Ограничить доступ к определенным потокам (например, видео).

**Пример настройки:**

- **Порт:** GE10
- **IP Version:** IPv4
- **Profile ID:** 10 (разрешает группы 239.1.1.1–239.1.1.50)

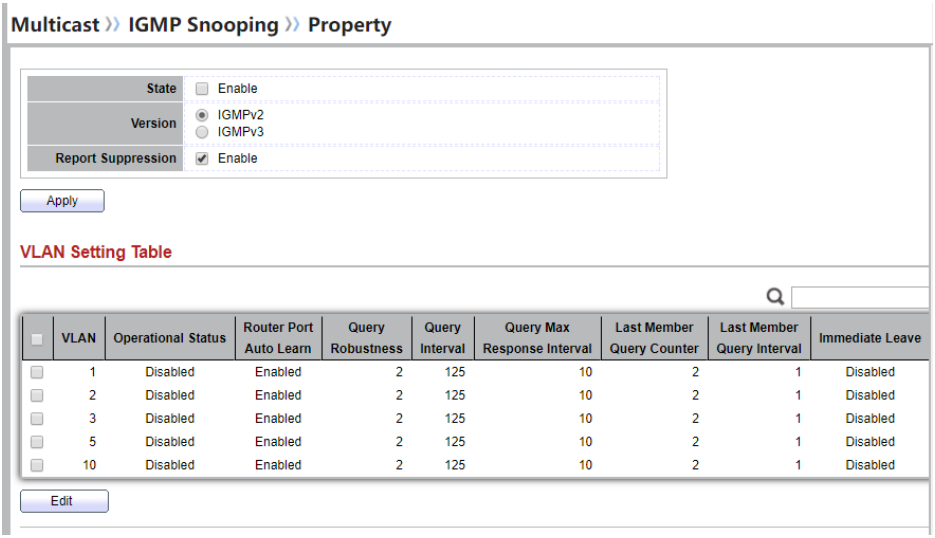
## 11.2. Настройка функции IGMP Snooping (IGMP Snooping)

**IGMP Snooping** – функция коммутатора для управления мультикаст-трафиком на уровне L2.

### 11.2.1. Свойства IGMP Snooping (Property)

**Для настройки глобальных параметров IGMP Snooping:**

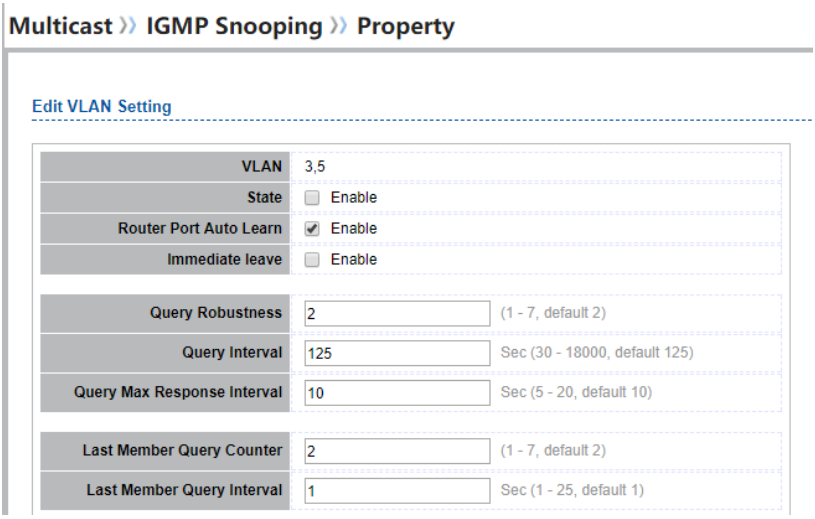
Перейдите в раздел **Multicast** > **IGMP Snooping** > **Property**.




***Глобальные настройки***

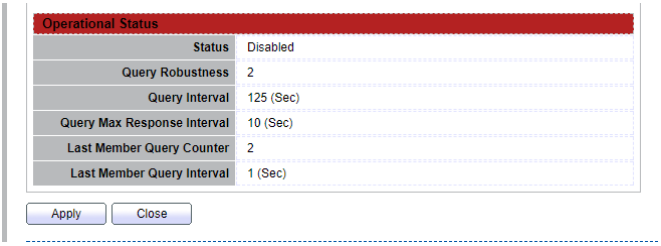
| Параметр | Описание |
|---|---|
| **State** | Включение/отключение IGMP Snooping. |
| **Version** | Версия IGMP: |
| | **IGMPv2** – базовая поддержка. |
| | **IGMPv3** – поддержка v3 + обратная совместимость с v2. |

| Параметр | Описание |
|---|---|
| **Report Suppression** | Подавление лишних IGMPv2 Report-пакетов (оптимизация трафика). |
| **Router Port Auto Learn** | Автоматическое определение портов маршрутизаторов. |
| **Query Robustness** | Коэффициент надежности запросов (учитывает потери пакетов), (по умолчанию: 2). |
| **Query Interval** | Интервал отправки общих запросов (сек). По умолчанию: 125 сек. |
| **Query Max Response Interval** | Максимальное время ответа на запрос (1/10 сек). По умолчанию: 10 (1 сек). |
| **Last Member Query Count** | Количество Group-Specific запросов при получении Leave-сообщения. По умолчанию: 2. |
| **Last Member Query Interval** | Интервал Group-Specific запросов (с). По умолчанию: 1с. |
| **Immediate Leave** | Мгновенное удаление группы при получении Leave (только для портов с одним клиентом). |



***Настройки VLAN***

| Параметр | Описание |
|---|---|
| **VLAN** | Выберите VLAN для настройки. |
| **State** | Включение или отключение IGMP Snooping для VLAN.<br>**Enable** – включить IGMP Snooping для VLAN.<br>**Disable** – отключить. |
| **Router Port Auto Learn** | Автоматическое обучение портов маршрутизатора (Router Port).<br>**Enable** – включить определение через запросы Query, PIM, DVMRP.<br>**Disable** – отключить. |
| **Immediate Leave** | Немедленный выход из группы при получении IGMP Leave.<br>**Enable** – включить.<br>**Disable** – отключить. |
| **Query Robustness** | Коэффициент надежности запросов (учитывает потери пакетов), (по умолчанию: 2). |
| **Query Interval** | Интервал отправки общих запросов (сек). По умолчанию: 125 сек. |
| **Query Max Response Interval** | Максимальное время ответа на запрос (1/10 сек). По умолчанию: 10 (1 сек). |
| **Last Member Query Count** | Количество Group-Specific запросов при получении Leave-сообщения. По умолчанию: 2. |
| **Last Member Query Interval** | Интервал Group-Specific запросов (с). По умолчанию: 1 с. |




| Параметр | Описание |
|---|---|
| **Status** | Состояние IGMP Snooping (вкл/выкл) |
| **Query Robustness** | Коэффициент надежности запросов (учитывает потери пакетов), (по умолчанию: 2). |
| **Query Interval** | Интервал отправки общих запросов (сек). |
| **Query Max Response Interval** | Максимальное время ответа на запрос (1/10 сек). |
| **Last Member Query Count** | Количество Group-Specific запросов при получении Leave-сообщения. |
| **Last Member Query Interval** | Интервал Group-Specific запросов (с). |

**Примечания:**

1. **IGMPv3** рекомендуется для сетей с поддержкой SSM (Source-Specific Multicast).
2. **Immediate Leave** используйте только для портов с одним устройством (например, IP-камеры).

**Пример настройки:**

- **Глобально:**
  - **Version:** IGMPv3
  - **Query Interval:** 60 сек
- **VLAN 10:**
  - **Immediate Leave:** Enable

### 11.2.2. Генерато запросов IGMP (Querier)

Для настройки параметров IGMP Snooping Querier (генератор запросов IGMP) перейдите:

**Multicast > IGMP Snooping > Querier**

На этой странице настраиваются параметры Querier (генератора IGMP-запросов) для конкретных VLAN.

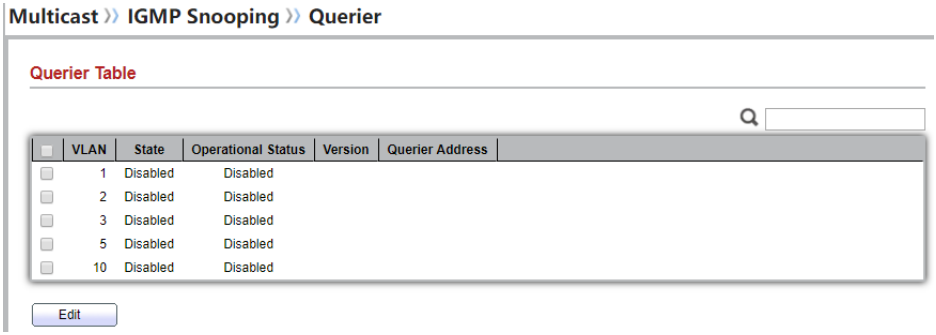
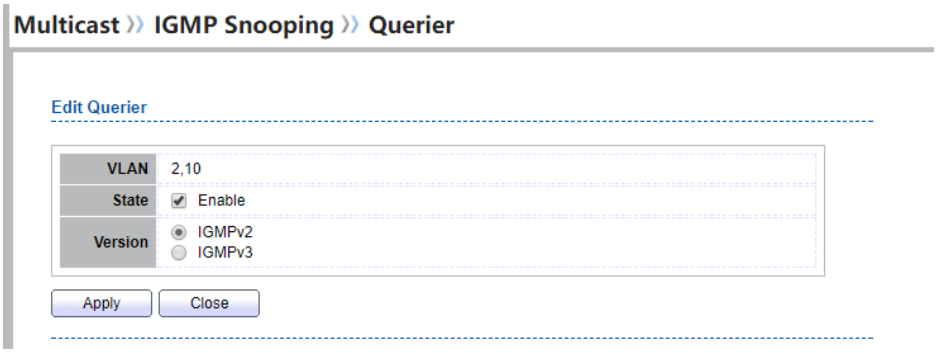



***Таблица работы генератора запросов IGMP***

| Параметр | Описание |
|---|---|
| **VLAN** | ID VLAN, для которой настроен Querier |
| **State** | Состояние Querier (вкл./выкл.) |
| **Operational Status** | Фактический статус работы Querier |
| **Querier Version** | Версия IGMP (v2/v3) |
| **Querier IP** | IP-адрес Querier в VLAN |




***Настройки для VLAN***

| Параметр | Описание |
|---|---|
| **VLAN** | Список VLAN для настройки |
| **State** | Включение/отключение функции Querier для выбранных VLAN:<br>**Enabled** – Querier активен.<br>**Disabled** – Querier отключен. |
| **Version** | Версия IGMP, используемая Querier:<br>• IGMPv2 – Querier работает по IGMP версии 2.<br>• IGMPv3 – Querier работает по IGMP версии 3 (требует, чтобы IGMP Snooping также был в версии v3). |

**Примечания**

1. **Querier** отвечает за отправку IGMP-запросов в сети, чтобы определить активные multicast-группы.

2. Если в VLAN нет маршрутизатора, поддерживающего IGMP, коммутатор может взять на себя роль **Querier** (генератор запросов IGMP), если функция включена.
3. Для работы **IGMPv3 Querier** необходимо, чтобы **IGMP Snooping** также был настроен на версию **v3**.

**Пример настройки**

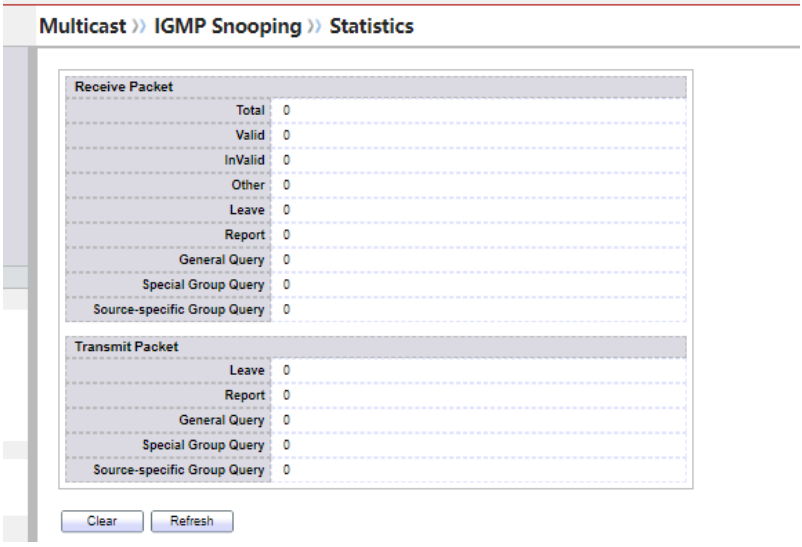
- Выберите VLAN **10** в списке.
- Включите Querier (**State > Enabled**).
- Установите версию **IGMPv3** (если IGMP Snooping работает в v3).
- Сохраните изменения.

### 11.2.3. Статистика IGMP Snooping (Statistics)

Для просмотра статистики **IGMP Snooping** перейдите в раздел:

**Multicast > IGMP Snooping > Statistics**

На этой странице отображается статистика работы IGMP Snooping, а также есть возможность её сбросить.



***Статистика полученных пакетов (Receive Packet)***

| Параметр | Описание |
|---|---|
| **Total** | Общее количество полученных IGMP-пакетов (включая IPv4 multicast-данные, направленные на CPU). |
| **Valid** | Количество корректно обработанных IGMP Snooping-пакетов. |
| **Invalid** | Количество некорректных IGMP Snooping-пакетов. |
| **Other** | Пакеты, не относящиеся к IGMP (ICMP-протокол ≠ 2) и не являющиеся IPv4 multicast-данными. |
| **Leave** | Количество полученных IGMP Leave-пакетов (запросы на выход из группы). |
| **Report** | Количество полученных IGMP Report-пакетов (запросы на присоединение к группе). |
| **General Query** | Количество полученных IGMP General Query-пакетов (общие запросы). |
| **Special Group Query** | Количество полученных IGMP Special Group Query-пакетов (специальные групповые запросы). |
| **Source-specific Group Query** | Количество полученных IGMP Source-Specific Group Query-пакетов (запросы для конкретного источника и группы). |

***Статистика переданных пакетов (Transmit Packet)***

| Параметр | Описание |
|---|---|
| **Leave** | Количество отправленных IGMP Leave-пакетов. |
| **Report** | Количество отправленных IGMP Report-пакетов. |
| **General Query** | Количество отправленных IGMP General Query-пакетов (включая запросы, отправленные через генератор запросов). |
| **Special Group Query** | Количество отправленных IGMP Special Group Query-пакетов (включая запросы, отправленные квайером). |
| **Source-specific Group Query** | Количество отправленных IGMP Source-Specific Group Query-пакетов. |

**Примечания**

1. Статистика помогает анализировать состояние multicast-трафика и выявлять возможные проблемы (например, большое количество **Invalid**-пакетов может указывать на ошибки в настройках).
2. Для сброса статистики предусмотрена кнопка **Clear**

**Пример использования статистики**

- Если **Invalid**-пакетов слишком много:
  - Проверьте настройки **IGMP Snooping** и версию IGMP.

- Убедитесь, что в сети нет некорректных multicast-источников.

- Если **General Query** не приходят:
  - Проверьте, включен ли **Querier** для нужной VLAN.
  - Убедитесь, что маршрутизатор или коммутатор отправляет запросы.

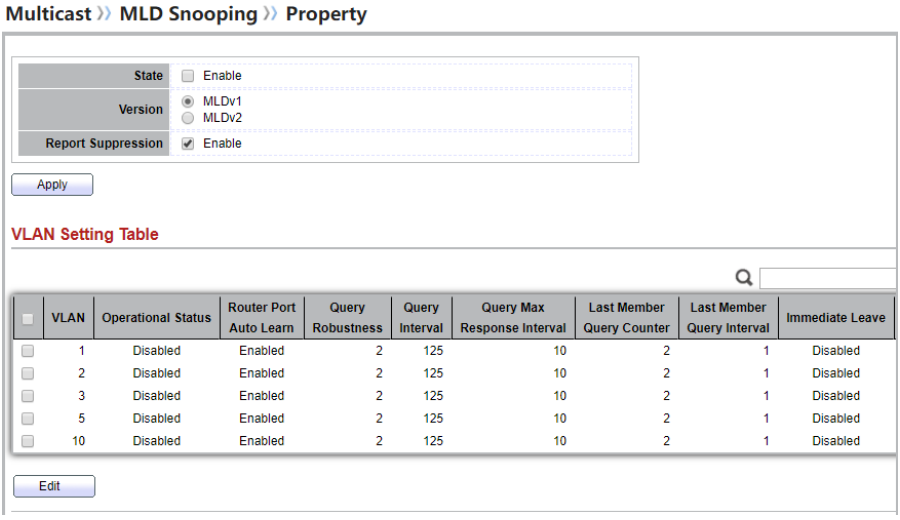
## 11.3. Настройка функции MLD Snooping (MLD Snooping)

**MLD Snooping** – это IPv6-аналог IGMP Snooping, используемый для управления multicast-трафиком в IPv6-сетях.

### 11.3.1. Свойства MLD Snooping (Property)

Чтобы открыть страницу глобальных настроек **MLD Snooping** и параметров VLAN, перейдите в раздел:

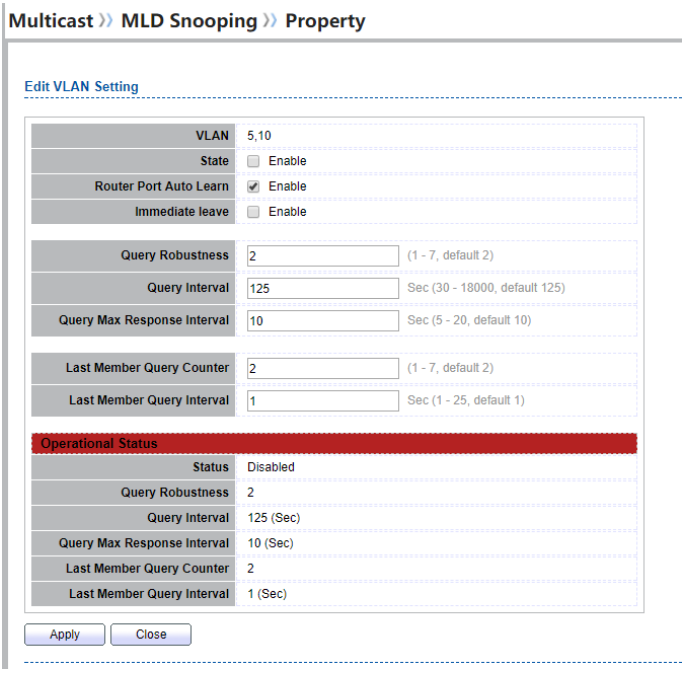
**Multicast > MLD Snooping > Property**



***Глобальные настройки (Global Settings)***

| Параметр | Описание |
|---|---|
| **State** | Включение/отключение функции MLD Snooping:<br>• **Enable** – MLD Snooping активен.<br>• **Disable** – MLD Snooping выключен. |
| **Version** | Версия MLD Snooping:<br>• **MLDv1** – поддерживает только MLD версии 1.<br>• **MLDv2** – поддерживает MLDv2 (включая базовую совместимость с v1). |
| **Report Suppression** | Подавление MLDv1-отчетов:<br>• **Enable** – включено подавление отчетов MLDv1.<br>• **Disable** – функция отключена. |
| **VLAN** | ID VLAN, к которой применяются настройки MLD. |
| **Operation Status** | Статус работы MLD Snooping для VLAN. |
| **Router Port Auto Learn** | Автоматическое определение порта маршрутизатора:<br>• **Enable** – коммутатор автоматически определяет порты маршрутизатора.<br>• **Disable** – функция отключена. |
| **Query Robustness** | Коэффициент надежности запросов (учитывает потери пакетов), (по умолчанию: 2). |
| **Query Interval** | Интервал отправки общих запросов (в секундах). |

| Параметр | Описание |
|---|---|
| **Query Max Response Interval** | Максимальное время (в 1/10 секунды) для отправки ответного отчета после Membership Query. |
| **Last Member Query Count** | Количество Group-Specific Queries, отправляемых при получении Leave Group сообщения. |
| **Last Member Query Interval** | Интервал отправки Group-Specific Queries при получении Leave Group сообщения. |
| **Immediate Leave** | Мгновенный выход из группы при получении сообщения MLD Leave:<br>• **Enable** – включен.<br>• **Disable** – отключен. |



***Настройки VLAN (VLAN Settings)***

| Параметр | Описание |
|---|---|
| **VLAN** | Выбранный список VLAN. |
| **State** | Включение MLD Snooping для VLAN:<br>• **Enable** – MLD Snooping активен для VLAN.<br>• **Disable** – функция отключена. |
| **Router Port Auto Learn** | Автоматическое определение порта маршрутизатора для VLAN:<br>• **Enable** – включено (на основе Query, PIM, DVMRP).<br>• **Disable** – отключено. |
| **Immediate Leave** | Мгновенный выход из группы при получении MLD Leave:<br>• **Enable** – включен.<br>• **Disable** – отключен. |
| **Query Robustness** | Настраиваемая устойчивость к потере пакетов (административная настройка). |
| **Query Interval** | Настраиваемый интервал отправки общих запросов (административная настройка). |
| **Query Max Response Interval** | Настраиваемое максимальное время ответа (в 1/10 секунды). |
| **Last Member Query Counter** | Настраиваемое количество Group-Specific Queries при Leave Group. |
| **Last Member Query Interval** | Настраиваемый интервал Group-Specific Queries при Leave Group. |

| Параметр | Описание |
|---|---|
| **Operational Status** | Текущий статус работы MLD Snooping (активен, только если включен глобально и для VLAN). |
| **Status** | Рабочий статус MLD Snooping. |
| **Query Robustness** | Текущая настройка устойчивости к потере пакетов. |
| **Query Interval** | Текущий интервал запросов. |
| **Query Max Response Interval** | Текущее максимальное время ответа. |
| **Last Member Query Counter** | Текущее количество Group-Specific Queries. |
| **Last Member Query Interval** | Текущий интервал Group-Specific Queries. |

**Примечания**

1. **MLDv2** рекомендуется для современных сетей, так как поддерживает более сложные сценарии multicast-маршрутизации.
2. **Immediate Leave** ускоряет выход из группы, но может привести к преждевременному отключению трафика, если в VLAN остаются участники.

**Пример настройки**

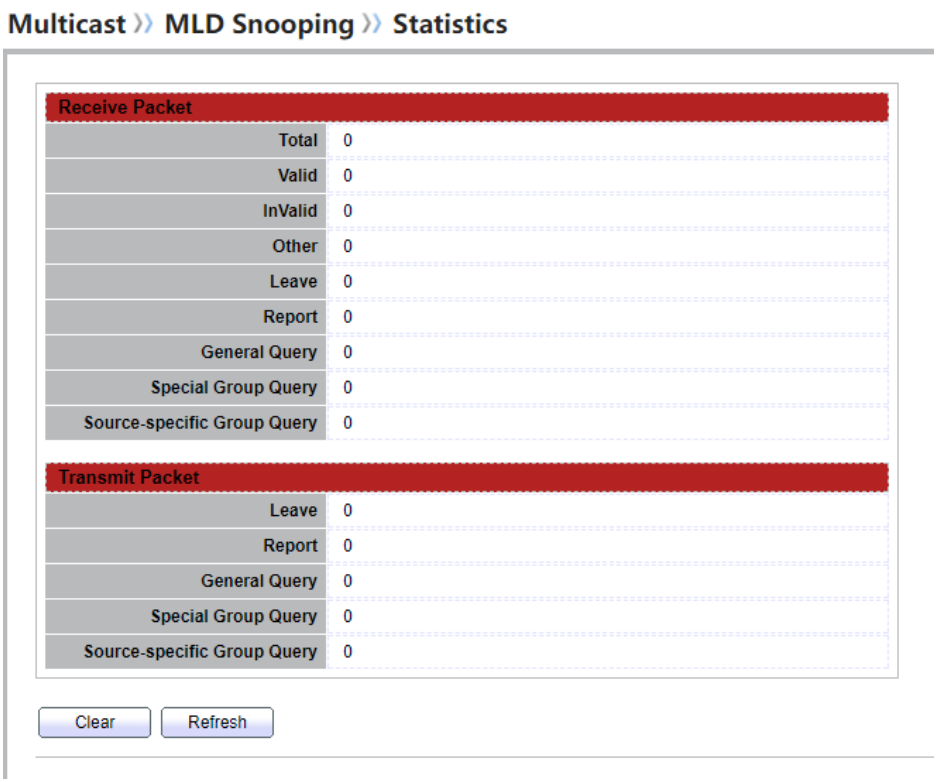
- Включите **MLD Snooping** (State > **Enable**).
- Выберите версию **MLDv2**.
- Для VLAN 20 включите **Router Port Auto Learn** и **Immediate Leave**.
- Установите **Query Interval = 60** секунд.

- Сохраните настройки и перезагрузите коммутатор при необходимости.

### 11.3.2. Статистика MLD Snooping (Statistics)

Для просмотра статистики **MLD Snooping** перейдите в раздел:

**Multicast > MLD Snooping > Statistics**



***Статистика полученных пакетов (Receive Packet)***

| Параметр | Описание |
|---|---|
| **Total** | Общее количество полученных MLD-пакетов (включая IPv6 multicast-данные, направленные на CPU). |
| **Valid** | Количество корректно обработанных MLD Snooping-пакетов. |
| **Invalid** | Количество некорректных MLD Snooping-пакетов. |
| **Other** | Пакеты, не относящиеся к MLD (тип ICMPv6 ≠ MLD), не являющиеся IPv6 multicast-данными и не относящиеся к протоколам маршрутизации IPv6. |
| **Leave** | Количество полученных MLD Leave-пакетов (запросы на выход из группы). |
| **Report** | Количество полученных MLD Report-пакетов (запросы на присоединение к группе). |
| **General Query** | Количество полученных MLD General Query-пакетов (общие запросы). |
| **Special Group Query** | Количество полученных MLD Special Group Query-пакетов (специальные групповые запросы). |
| **Source-specific Group Query** | Количество полученных MLD Source-Specific Group Query-пакетов (запросы для конкретного источника и группы). |

***Статистика переданных пакетов (Transmit Packet)***

| Параметр | Описание |
|---|---|
| **Leave** | Количество отправленных MLD Leave-пакетов. |
| **Report** | Количество отправленных MLD Report-пакетов. |
| **General Query** | Количество отправленных MLD General Query-пакетов. |
| **Special Group Query** | Количество отправленных MLD Special Group Query-пакетов. |
| **Source-specific Group Query** | Количество отправленных MLD Source-Specific Group Query-пакетов. |

**Примечания**

1. Статистика помогает анализировать работу multicast-трафика в IPv6-сетях и выявлять возможные проблемы (например, большое количество **Invalid**-пакетов может указывать на ошибки в настройках).
2. Для сброса статистики обычно предусмотрена кнопка **Clear** или аналогичная.

**Пример использования статистики**

- Если **Invalid**-пакетов слишком много:
  - Проверьте настройки **MLD Snooping** и версию MLD.
  - Убедитесь, что в сети нет некорректных multicast-источников.

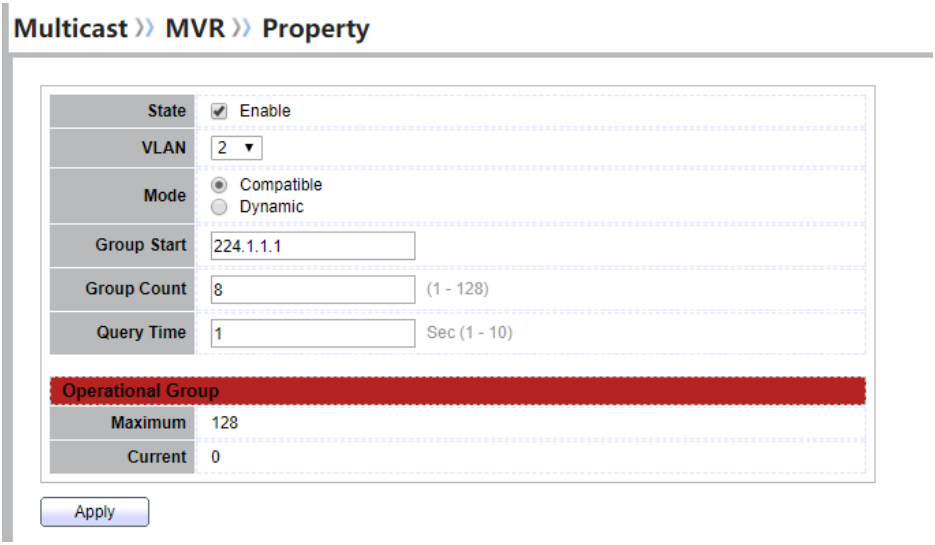
## 11.4. Настройка MVR (Multicast VLAN Registration)

Используйте раздел **MVR** для настройки функции Multicast VLAN Registration, которая позволяет эффективно передавать multicast-трафик между разными VLAN.

### 11.4.1. Свойства MVR (Property)

Чтобы открыть страницу настройки **MVR**, перейдите в раздел:

**Multicast > MVR > Property**




***Параметры MVR***

| Параметр | Описание |
|---|---|
| **State** | Включение/отключение функции MVR:<br>• **Enable** – MVR активен.<br>• **Disable** – MVR выключен. |
| **VLAN** | ID VLAN, используемой для multicast-трафика MVR. |

| Параметр | Описание |
|---|---|
| **Mode** | Режим работы MVR:<br>• **Compatible** – совместимый режим.<br>• **Dynamic** – динамический режим (автоматическое определение участников группы на source-порте). |
| **Group Start** | Начальный адрес диапазона multicast-групп MVR. |
| **Group Count** | Количество multicast-групп в диапазоне. |
| **Query Time** | Время ожидания запроса после получения MVR Leave-пакета. |
| **Maximum** | Максимальное количество записей в базе данных MVR-групп. |
| **Current** | Текущее количество активных MVR-групп. |

**Примечания**

1. **MVR** используется для оптимизации multicast-трафика в сетях с несколькими VLAN, уменьшая дублирование потоков.
2. В **Dynamic** режиме коммутатор автоматически определяет участников multicast-групп, что упрощает настройку, но может потреблять больше ресурсов.

**Пример настройки**

- Включите **MVR** (State > **Enable**).
- Укажите **VLAN 100** в качестве multicast-VLAN.
- Выберите режим **Dynamic**.

- Задайте диапазон групп:
  - **Group Start**: 239.0.0.1
  - **Group Count**: 10
- Установите **Query Time = 2** секунды.
- Сохраните настройки.

### 11.4.2. Настройка портов (Port Setting)

Для настройки ролей портов MVR и параметра Immediate Leave перейдите в раздел:

**Multicast > MVR > Port Setting**

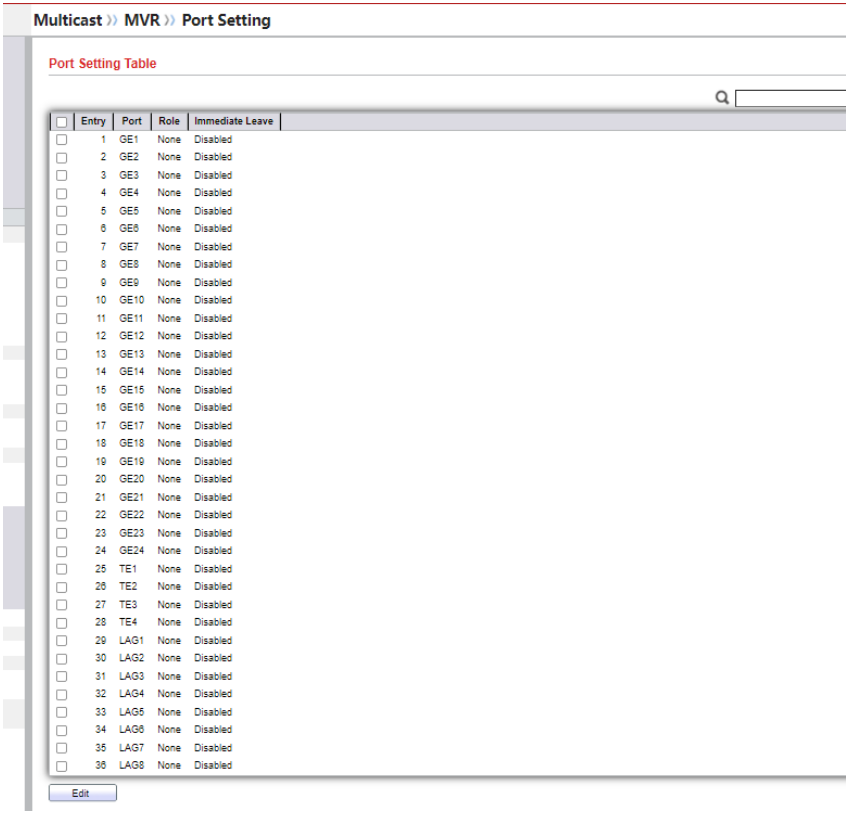
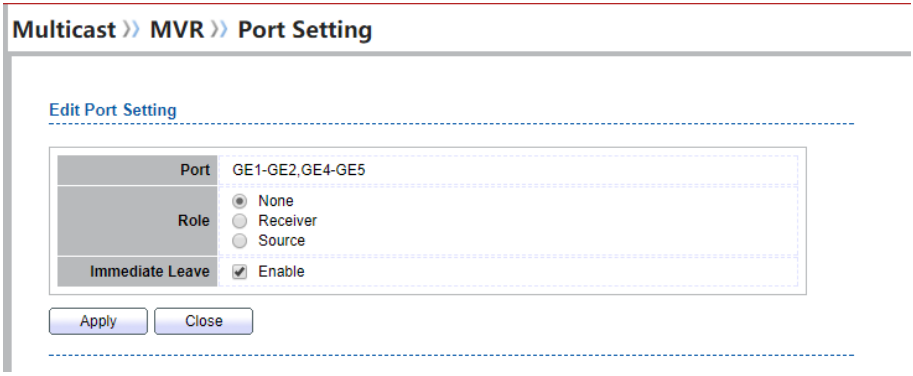


***Таблица настройки портов MVR***

| Параметр | Описание |
|---|---|
| **Entry** | Номер записи в таблице. |
| **Port** | Имя порта. |
| **Role** | Роль порта в MVR:<br>• **None** – порт не участвует в MVR.<br>• **Receiver** – порт получает multicast-трафик.<br>• **Source** – порт передает multicast-трафик. |
| **Immediate Leave** | Статус Immediate Leave:<br>• **Enable** – включен мгновенный выход из группы.<br>• **Disable** – отключен. |



***Параметры настройки портов***

| Параметр | Описание |
|---|---|
| **Port** | Список выбранных портов. |
| **Role** | Назначение роли порта в MVR:<br>• **None** – без роли.<br>• **Receiver** – порт-получатель multicast-трафика.<br>• **Source** – порт-источник multicast-трафика. |
| **Immediate Leave** | Включение/отключение Immediate Leave:<br>• **Enable** – при получении Leave-пакета порт мгновенно выходит из группы.<br>• **Disable** – стандартный режим обработки Leave-пакетов. |

**Примечания**

1. **Source-порты** используются для подключения multicast-источников (например, видео-серверов).
2. **Receiver-порты** подключают конечных пользователей, которые должны получать multicast-трафик.
3. **Immediate Leave** ускоряет освобождение ресурсов при выходе клиента из группы, но может вызвать прерывание трафика, если в группе остаются другие подписчики.

**Пример настройки**

- Выберите порт GE10:
  - Установите роль **Source**.
  - Отключите **Immediate Leave**.

- Выберите порты **GE1-GE5**:
  - Назначьте роль **Receiver**.
  - Включите **Immediate Leave** для быстрого выхода клиентов.
- Сохраните конфигурацию.

### 11.4.3. Групповые адреса (Group Address)

Для просмотра и настройки multicast-групп MVR перейдите в раздел:

**Multicast > MVR > Group Address**

На этой странице отображаются все MVR-группы (динамически изученные или статически добавленные), а также их параметры.

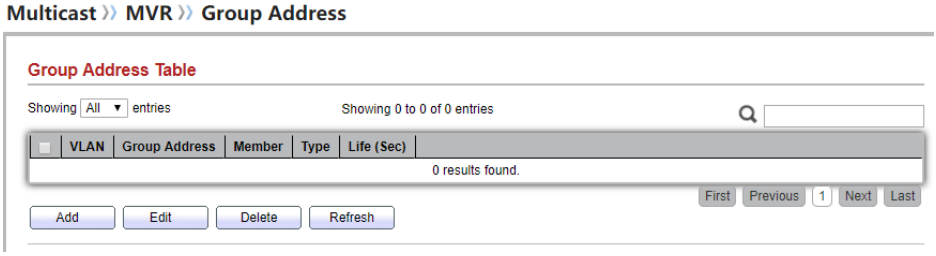
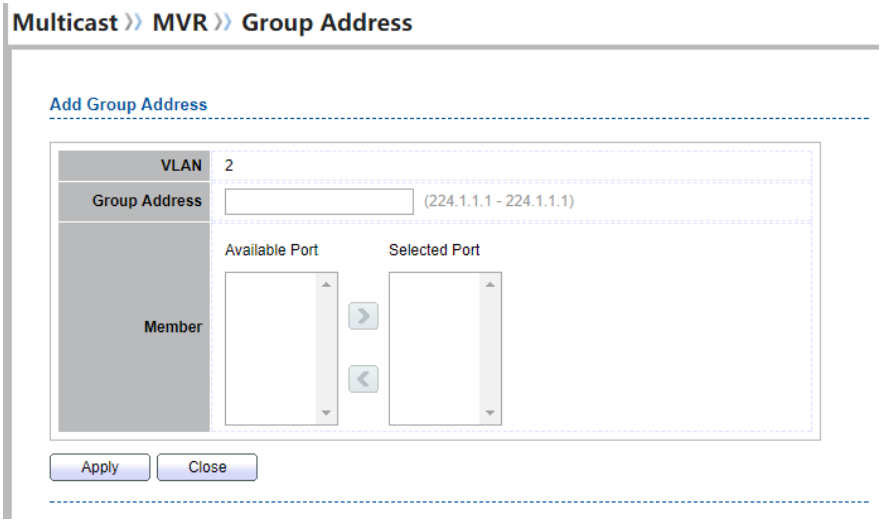



***Таблица MVR-групп***

| Параметр | Описание |
|---|---|
| **VLAN** | ID VLAN, к которой относится MVR-группа. |
| **Group Address** | IP-адрес multicast-группы. |
| **Member** | Порт(ы)-участники группы. |

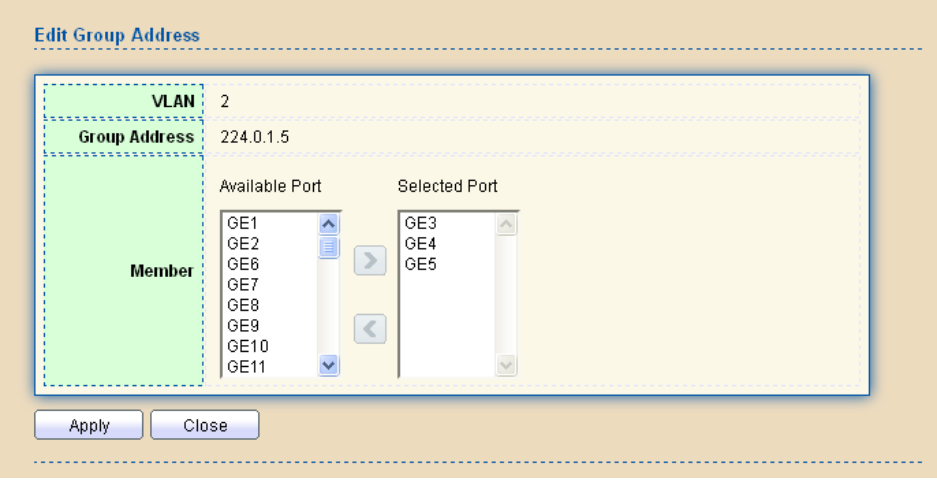
| Параметр | Описание |
|---|---|
| **Type** | Тип группы:<br>• **Static** – статически настроенная группа.<br>• **Dynamic** – динамически добавленная группа. |
| **Life (Sec)** | Время жизни динамической группы (в секундах). |




***Просмотр участников группы***

| Параметр | Описание |
|---|---|
| **VLAN** | ID VLAN MVR-группы. |
| **Group Address** | IP-адрес MVR-группы. |

| Параметр | Описание |
|---|---|
| **Member** | Участники группы:<br>• **Available Port** – доступные порты для добавления (в совместимом режиме – только Receiver-порты, в динамическом – и Source-порты).<br>• **Selected Port** – текущие порты-участники группы. |




***Редактирование группы***

| Параметр | Описание |
|---|---|
| **VLAN** | ID VLAN редактируемой MVR-группы. |
| **Group Address** | IP-адрес редактируемой MVR-группы. |

| Параметр | Описание |
|---|---|
| **Member** | Настройка участников:<br>• **Available Port** – порты, которые можно добавить в группу.<br>• **Selected Port** – текущие участники группы. |

**Примечания**

1. **Статические группы** требуют ручной настройки и не имеют времени жизни.
2. **Динамические группы** создаются автоматически при подключении клиентов и удаляются по истечении **Life (Sec)**.
3. В **динамическом режиме MVR** Source-порты могут автоматически добавляться в группы.

**Пример настройки**

- Для добавления статической группы:
  - Укажите **VLAN 100** и адрес **239.0.0.1**.
  - Выберите **Receiver-порты** (GE2-GE5) в **Selected Port**.
- Для проверки динамических групп:
  - Найдите группу с типом **Dynamic** и проверьте **Life (Sec)**.
- Сохраните изменения.

# 12. Маршрутизация (Routing)

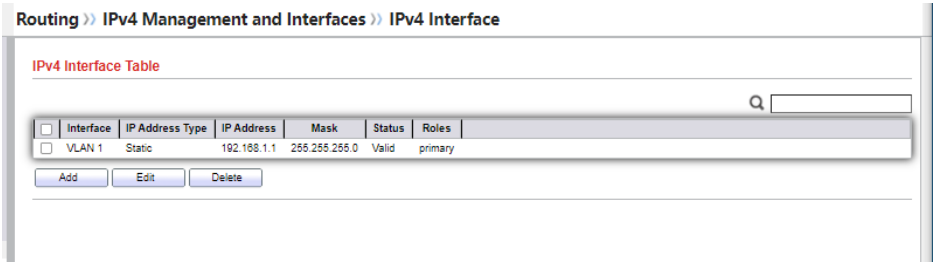
## 12.1. Настройка IPv4 интерфейсов и маршрутизации (IPv4 Management and Interfaces)

### 12.1.1. Настройка IPv4 интерфейсов в коммутаторе (IPv4 Interface)

Для настройки IPv4 интерфейсов (в том числе IP адреса коммутатора) перейдите в раздел:

**Routing > IPv4 Management and Interfaces > IPv4 Interface**

На этой странице отображаются текущие интерфейсы устройства с адресами IPv4.



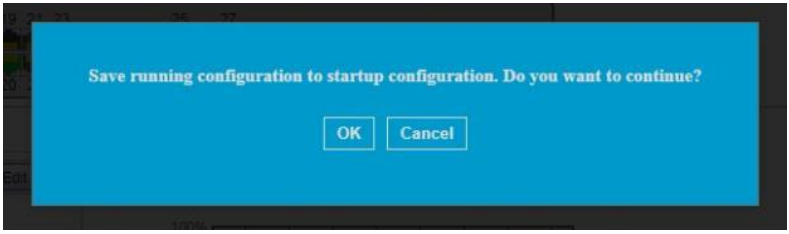

**Для изменения текущего IPv4 адреса коммутатора следует:**

1) Выбрать (отметить галочкой) VLAN 1 (коммутатор) и нажать кнопку **Edit** (изменить);
2) В поле **IP Address** (IP адрес) ввести требуемый IP адрес (по умолчанию 192.168.1.1). В поле **Mask** (маска) требуется ввести значение маски (по умолчанию 255.255.255.0). Если требуется получать IP адрес от маршрутизатора через DHCP – выберите **Dynamic** в поле **Address Type** (тип IP адреса);
3) Нажмите кнопку **Apply** (принять), чтобы сохранить настройки. Старый IP адрес автоматически перестанет действовать;

4) Выполните повторный вход в WEB интерфейс, используя новый IP адрес.


**Внимание!**

Обязательно нажмите кнопку **Save** (сохранить), чтобы сохранить текущую конфигурацию коммутатора, как стартовую. В диалоговом окне (синий фон) нажмите кнопку **OK**. Данная операция позволит коммутатору помнить заданные настройки даже после кратковременного отключения от сети и перезагрузки. В противном случае после перезагрузки IP адрес вернется к предыдущему значению.

**Чтобы добавить IPv4-адрес для другого VLAN**:

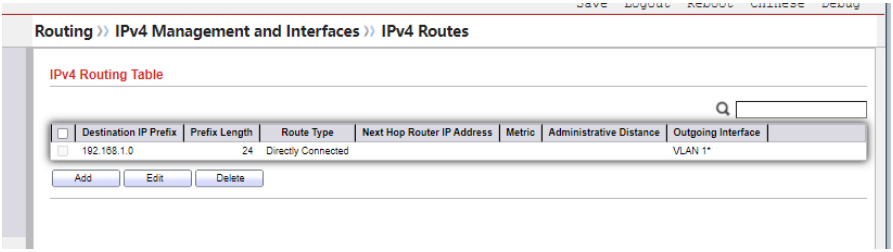
1. Нажмите **Add** (добавить).
2. Укажите:
   - Интерфейс (VLAN 2 и т.д.)
   - IPv4-адрес и маску подсети
3. Сохраните настройки (apply)

### 12.1.2. Маршрутизация IPv4 (IPv4 Routing)

Перейдите в раздел:

**Routing > IPv4 Management and Interfaces > IPv4 Routing**

Здесь отображается таблица IPv4-маршрутов.



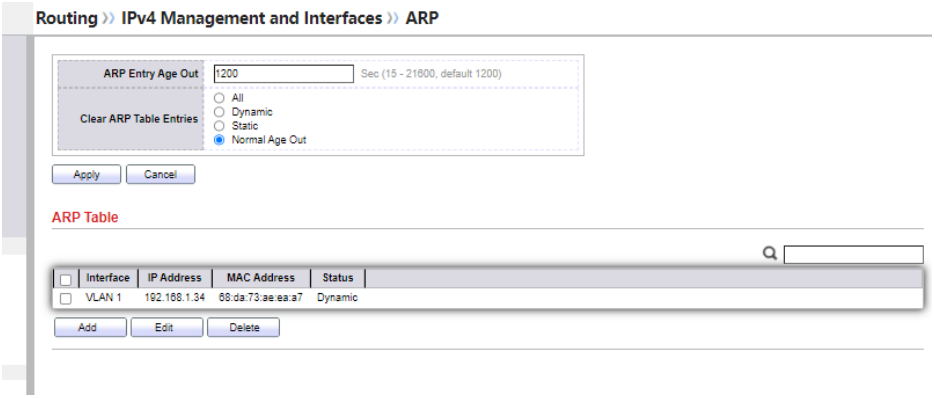

**Добавление постоянного (static) маршрута**:

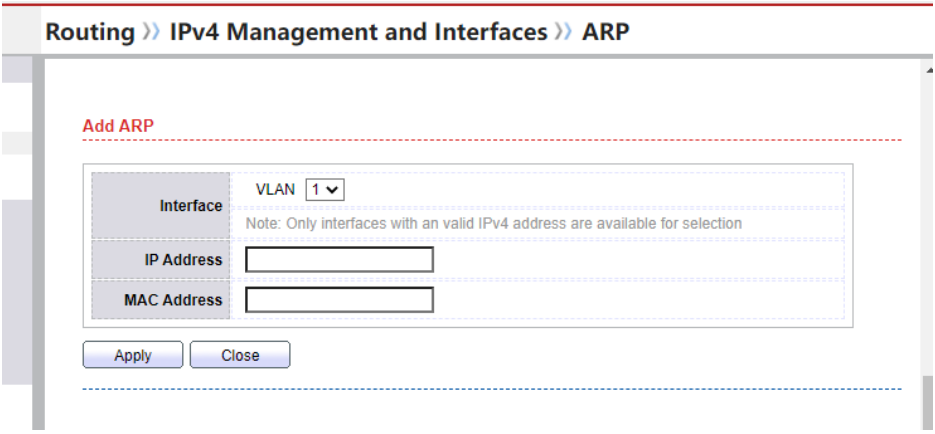
1. Нажмите **Add** (добавить)
2. Заполните поля:
   - Сеть назначения
   - Маска
   - Шлюз (Next Hop)
   - Интерфейс (VLAN 2 и т.д)
3. Примените изменения (**apply**)

### 12.1.3. ARP-таблица (ARP)

Для просмотра ARP таблицы перейдите в раздел:

**Routing > IPv4 Management and Interfaces > ARP**




**Добавление постоянной (static) ARP-записи**:

1. Нажмите **Add** (добавить)
2. Укажите:
   - IP-адрес
   - MAC-адрес
   - Интерфейс

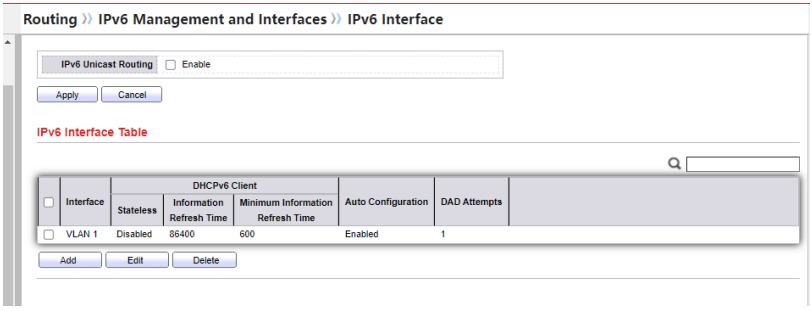
3. Сохраните настройки (**apply**)

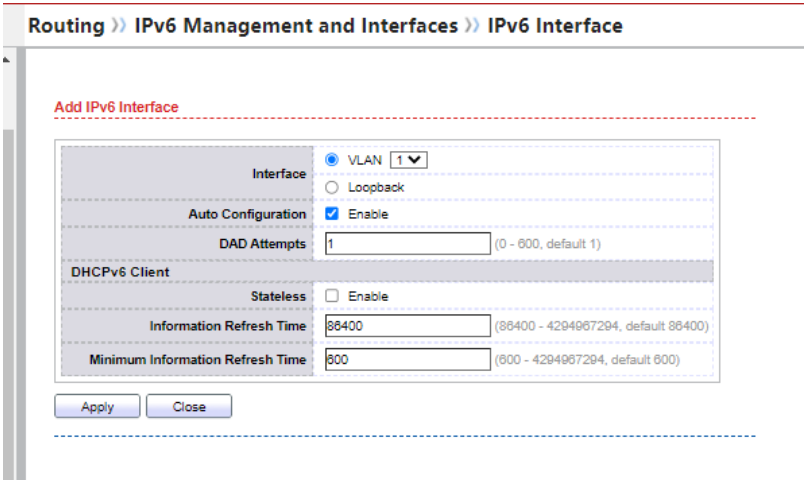
## 12.2. Настройка IPv6 интерфейсов и маршрутизации (IPv6 Management Interface)

### 12.2.1. Настройка IPv6 интерфейсов в коммутаторе (IPv6 Interface)

Для настройки IPv6 адресов перейдите в раздел:

**Routing > IPv6 Management and Interfaces > IPv6 Interface**




**Добавление IPv6-адреса**:

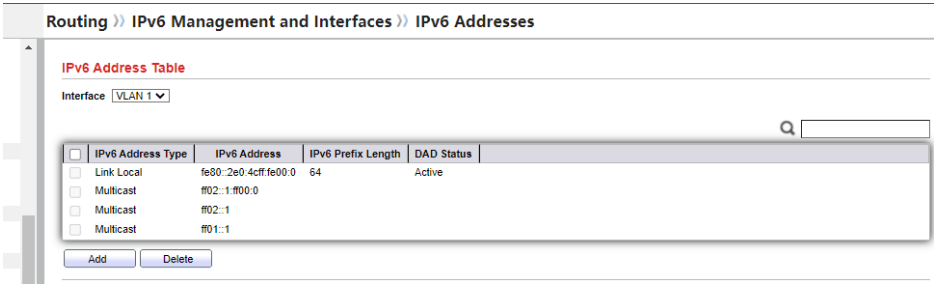
1. Нажмите **Add** (добавить)

2. Выберите:
    - Автоконфигурацию (DHCPv6 Client)
    - Или вручную укажите IPv6-адрес.
3. Сохраните настройки (**apply**)

### 12.2.2. Таблица адресов IPv6 (IPv6 Address)

Для просмотра таблицы IPv6 адресов перейдите в раздел:

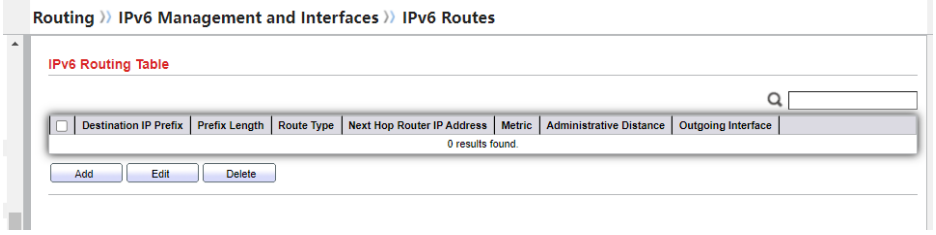
**Routing > IPv6 Management and Interfaces > IPv6 Addresses**

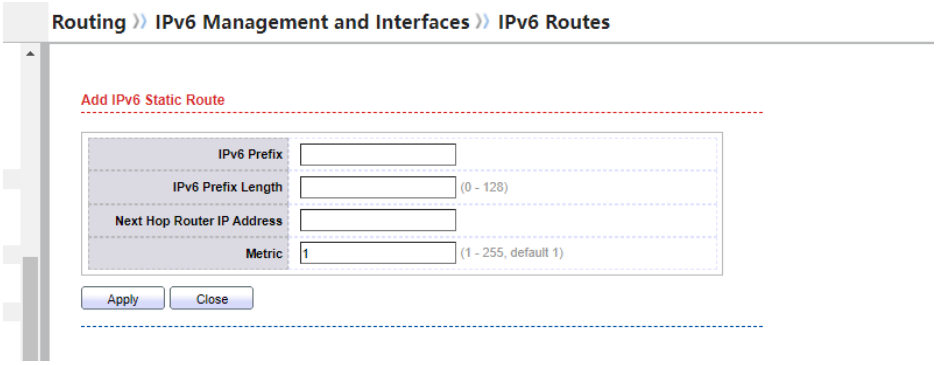



### 12.2.3. Маршрутизация IPv6 (IPv6 Routing)

Для просмотра и настройки IPv6 маршрутизации перейдите в раздел:

**Routing > IPv6 Management and Interfaces > IPv6 Routing**





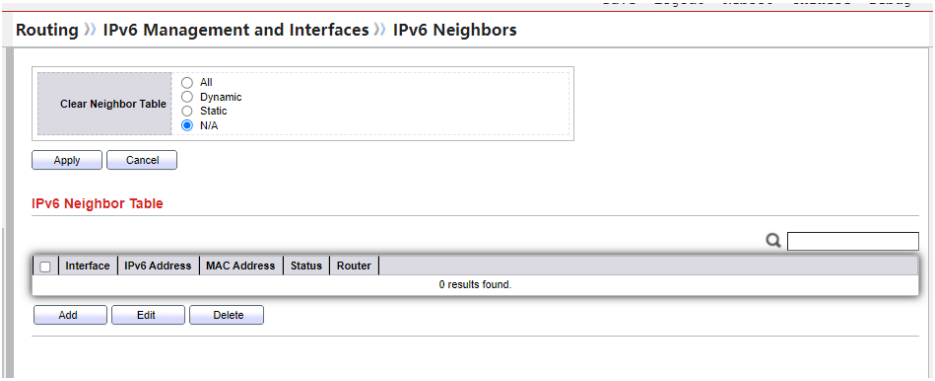

**Добавление статического маршрута IPv6**:

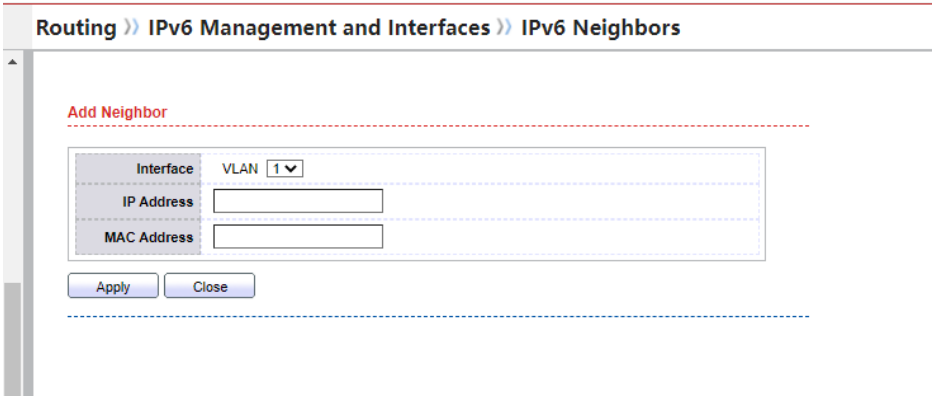
1. Нажмите **Add** (добавить)
2. Укажите:
    - IPv6-сеть назначения
    - Длину префикса
    - Шлюз (Next Hop)
3. Сохраните настройки (**apply**)

### 12.2.4. Настройка IPv6 Neighbors (IPv6 Neighbors)

Для настройки IPv6 Neighbors перейдите в раздел:

**Routing > IPv6 Management and Interfaces > IPv6 Neighbors**



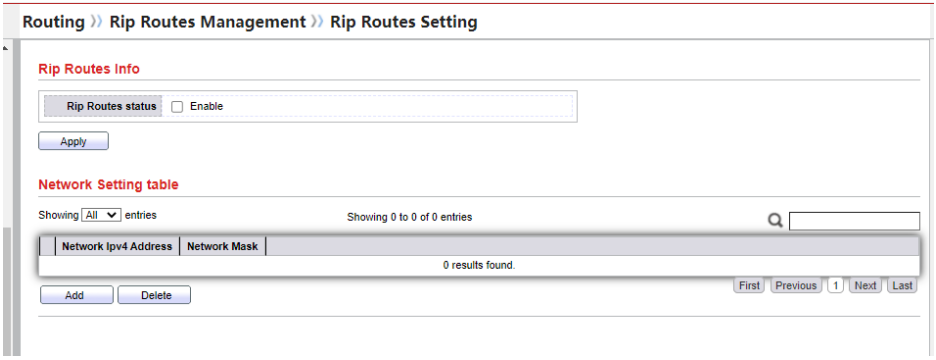

**Добавление постоянной (static) записи**:

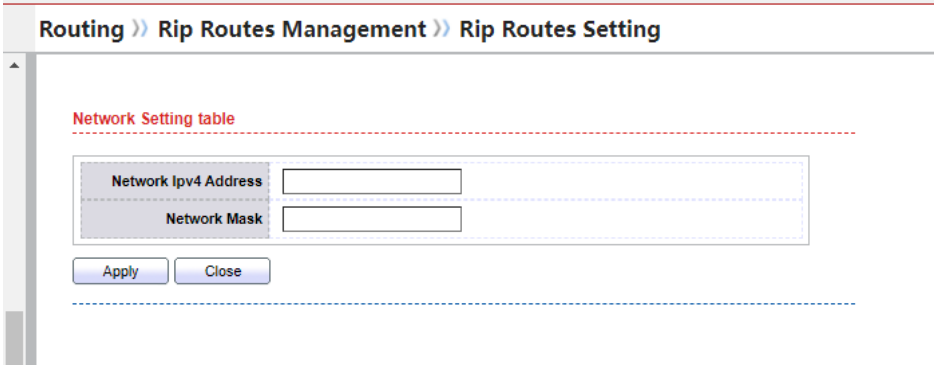
1. Нажмите **Add** (добавить)
2. Укажите:
   - IPv6-адрес
   - MAC-адрес
   - Интерфейс
3. Сохраните настройки (**apply**)

## 12.3. Управление маршрутизацией по протоколу RIP (RIP Routes Management)

Для настройки маршрутизации с помощью протокола RIP перейдите в раздел:

**Routing > RIP Routes Management > RIP Routes Setting**



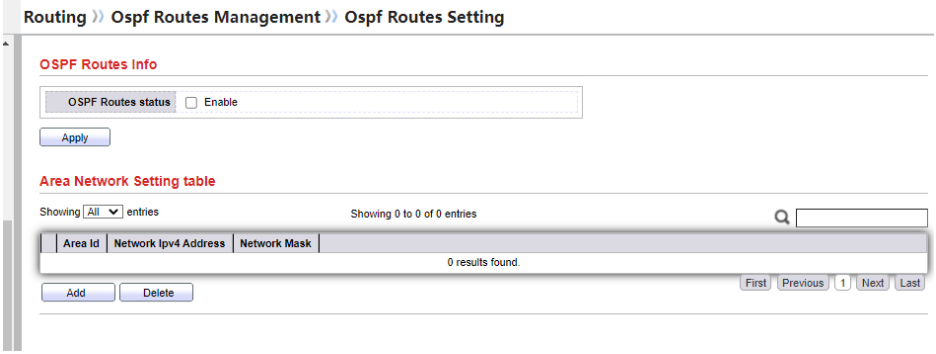

**Чтобы настроить RIP маршрутизацию**:

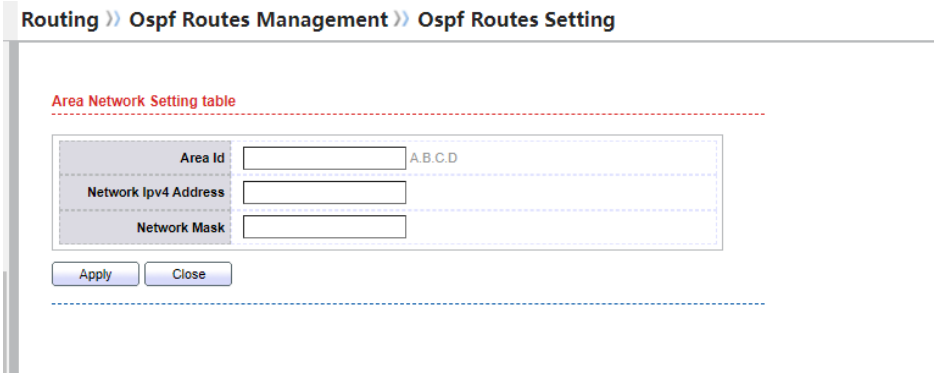
1. Активируйте **RIP Routes Status** (enable)
2. Нажмите **Add** (добавить) для добавления сети в маршрутизацию RIP
3. Сохраните настройки (**apply**)

## 12.4. Управление маршрутизацией по протоколу OSPF (OSPF Routes Management)

Для настройки маршрутизации с помощью протокола OSPF перейдите в раздел:

**Routing > OSPF Routes Management > OSPF Routes Setting**




**Чтобы настроить OSPF маршрутизацию**:

1. Активируйте **OSPF Routes Status** (enable)
2. Нажмите **Add** (добавить) для добавления сети в маршрутизацию OSPF.
3. Сохраните настройки (**apply**)

**Примечания**

1. **Постоянные (static) маршруты** рекомендуются для небольших сетей с фиксированной топологией.
2. **RIP** маршрутизация подходит для простых сетей, **OSPF** маршрутизация – для крупных и сложных.
3. Для IPv6 обязательно настройте протокол **NDP (Neighbor Discovery Protocol)**.

**Пример настройки OSPF**

- Включите **OSPF Routes Status**
- Добавьте сеть **192.168.1.0/24** в зону **0.0.0.0** (Backbone).
- Укажите интерфейс, подключенный к этой сети.
- Сохраните конфигурацию.

## 13. Безопасность (Security)

Используйте раздел **Security** для настройки функций безопасности коммутатора.

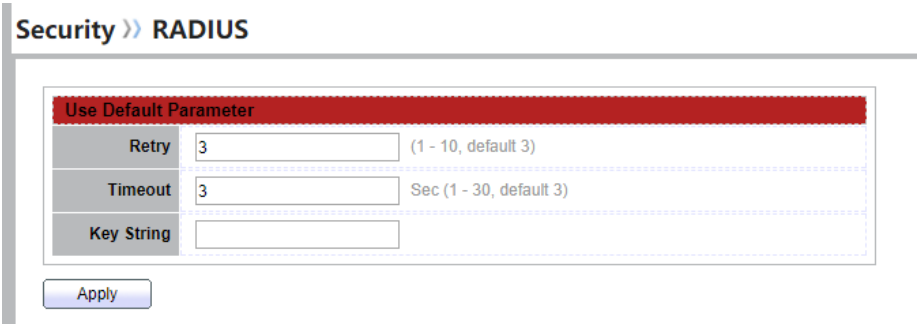
### 13.1. Настройки протокола RADIUS (RADIUS)

RADIUS – расширенный протокол удаленной аутентификации пользователей, представляет собой ключевой элемент в обеспечении безопасности и управлении доступом в сетях.

Для настройки параметров протокола RADIUS перейдите:

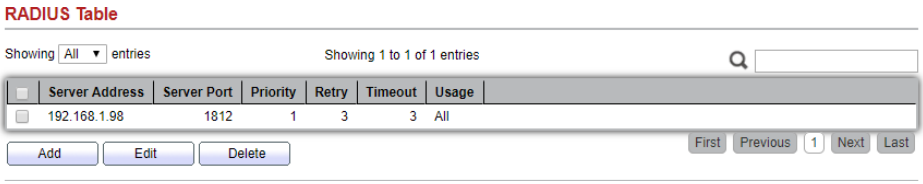
**Security > RADIUS**

На этой странице можно добавлять, редактировать или удалять RADIUS-серверы, а также изменять их параметры по умолчанию.



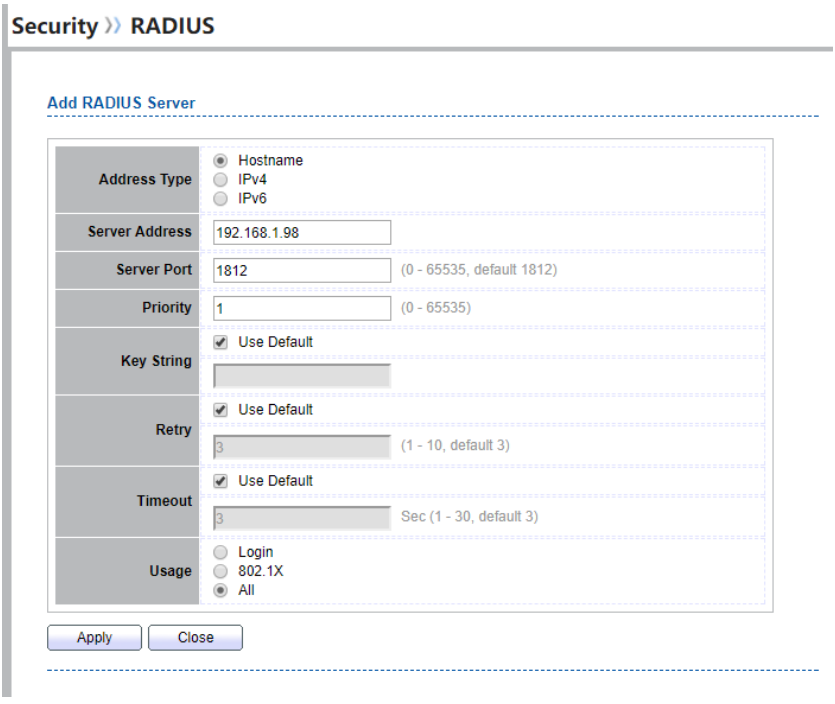

***Глобальные параметры RADIUS***

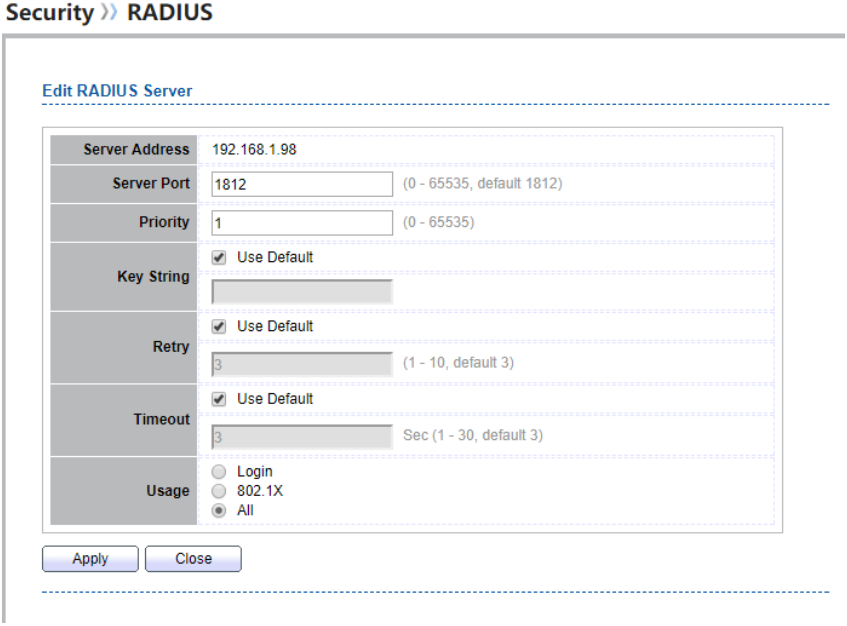
| Параметр | Описание |
|---|---|
| **Retry** | Количество попыток подключения к серверу (по умолчанию 3). |
| **Timeout** | Время ожидания ответа от сервера (в секундах) (по умолчанию 3). |
| **Key String** | Общий ключ (пароль) для аутентификации на RADIUS-сервере. |




***Настройки RADIUS-серверов***

| Параметр | Описание |
|---|---|
| **Server Address** | IP-адрес или доменное имя RADIUS-сервера. |
| **Server Port** | Порт RADIUS-сервера (обычно 1812 для аутентификации). |
| **Priority** | Приоритет сервера (чем меньше число, тем выше приоритет). При аутентификации сначала используется сервер с наивысшим приоритетом. |
| **Retry** | Количество попыток подключения для этого сервера. |
| **Timeout** | Время ожидания ответа (в секундах) для этого сервера. |
| **Usage** | Тип аутентификации:<br>• **Login** – для входа на коммутатор.<br>• **802.1x** – для аутентификации клиентов по стандарту 802.1X.<br>• **All** – для всех типов. |



***Добавление/редактирование RADIUS-сервера***

| Параметр | Описание |
|---|---|
| **Address Type** | Тип адреса сервера:<br>• **Hostname** – доменное имя.<br>• **IPv4** – IPv4-адрес.<br>• **IPv6** – IPv6-адрес. |
| **Server Address** | Адрес сервера (в зависимости от выбранного типа). |
| **Server Port** | Порт сервера. |
| **Priority** | Приоритет сервера (1 – наивысший). |
| **Retry** | Количество попыток подключения. |
| **Timeout** | Время ожидания ответа. |
| **Usage** | Тип аутентификации (Login, 802.1X, All). |

**Примечания**

1. **RADIUS** используется для централизованной аутентификации пользователей и устройств.
2. Для работы **802.1X** необходимо указать сервер с типом **802.1x** или **All**.
3. Рекомендуется настраивать несколько серверов с разными приоритетами для отказоустойчивости.

**Пример настройки**

- **Глобальные параметры**:
    - **Retry**: 3
    - **Timeout**: 5 сек.
    - **Key String**: secret123
- **Добавление сервера**:
    - **Address Type**: IPv4
    - **Server Address**: 192.168.1.100
    - **Server Port**: 1812
    - **Priority**: 1
    - **Retry**: 2
    - **Timeout**: 3 сек.
    - **Usage**: All
- Сохраните настройки (**Apply**)

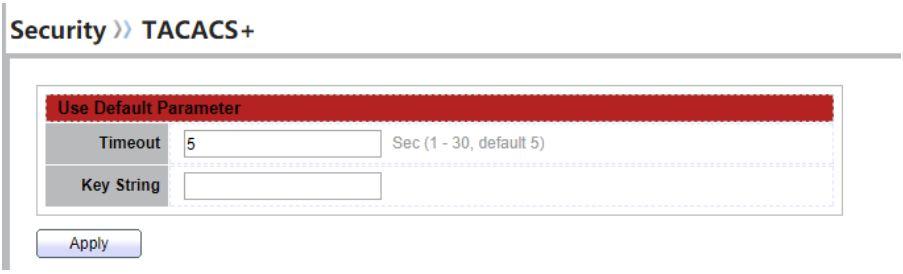
## 13.2. Настройки протокола TACACS+ (TACACS+)

TACACS+ это протокол безопасности, разработанный компанией Cisco.

Для настройки параметров TACACS+ перейдите:

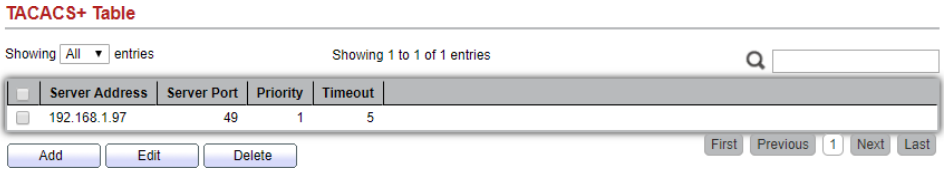
**Security > TACACS+**

На этой странице можно добавлять, редактировать или удалять TACACS+-серверы, а также изменять их параметры по умолчанию.



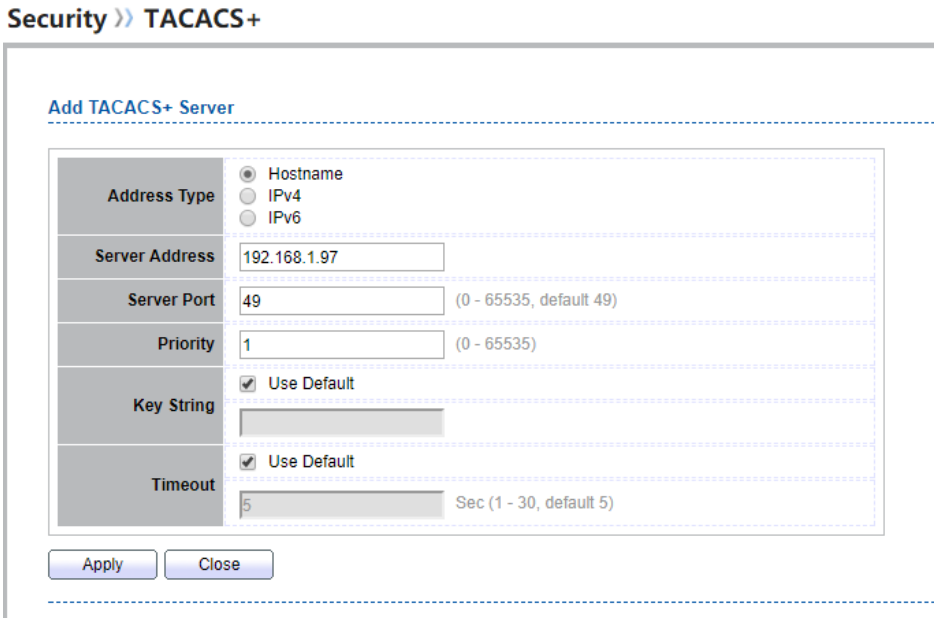

***Глобальные параметры TACACS+***

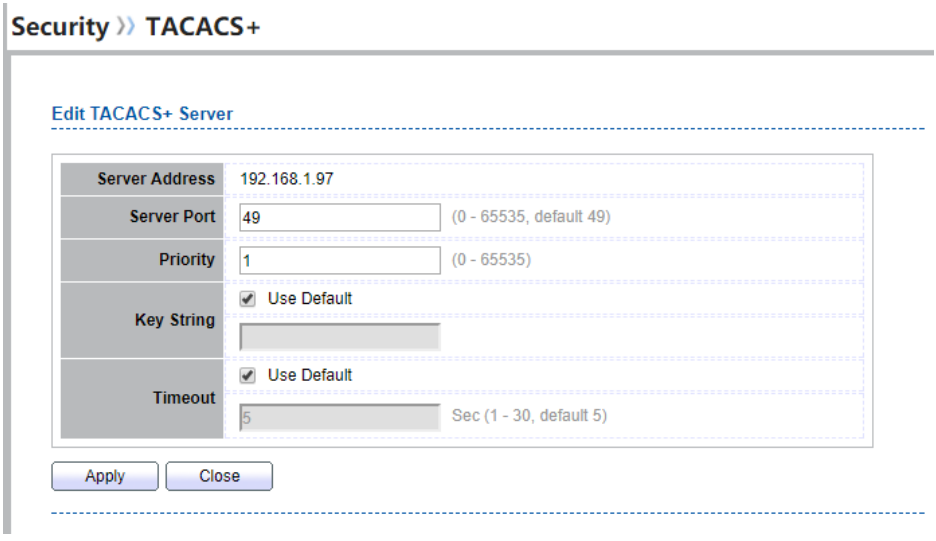
| Параметр | Описание |
|---|---|
| **Timeout** | Время ожидания ответа от сервера (в секундах) по умолчанию. |
| **Key String** | Общий ключ (пароль) для аутентификации на TACACS+-сервере. |




***Настройки TACACS+-серверов***

| Параметр | Описание |
|---|---|
| **Server Address** | IP-адрес или доменное имя TACACS+-сервера. |
| **Server Port** | Порт TACACS+-сервера (как правило – 49). |
| **Priority** | Приоритет сервера (чем меньше число, тем выше приоритет). При аутентификации сначала используется сервер с наивысшим приоритетом. |
| **Timeout** | Время ожидания ответа (в секундах) для этого сервера. |



***Добавление/редактирование TACACS+-сервера***

| Параметр | Описание |
|---|---|
| **Address Type** | Тип адреса сервера:<br>• **Hostname** – доменное имя.<br>• **IPv4** – IPv4-адрес.<br>• **IPv6** – IPv6-адрес. |
| **Server Address** | Адрес сервера (в зависимости от выбранного типа). |
| **Server Port** | Порт сервера. |
| **Priority** | Приоритет сервера (1 – наивысший). |
| **Timeout** | Время ожидания ответа. |

**Примечания**

1. **TACACS+** обеспечивает централизованную аутентификацию, авторизацию и учёт (AAA) для сетевых устройств.
2. В отличие от RADIUS, TACACS+ использует TCP (как правило – 49) и поддерживает более детальный контроль доступа.
3. Рекомендуется настраивать несколько серверов с разными приоритетами для отказоустойчивости.

**Пример настройки**

- **Глобальные параметры**:
  - **Timeout**: 5 сек.
  - **Key String**: tacacs_key_123
- **Добавление сервера**:

- **Address Type**: IPv4
- **Server Address**: 192.168.1.101
- **Server Port**: 49
- **Priority**: 1
- **Timeout**: 3 сек.

- Сохраните настройки (**Apply**)

## 13.3. AAA (Аутентификация, Авторизация и Учет пользователей)

### 13.3.1. Списки методов AAA (Method List)

Для настройки списков методов аутентификации перейдите:

**Security > AAA > Method List**

На этой странице WEB интерфейса можно создавать, редактировать и удалять списки методов аутентификации (список "default" нельзя удалить). Коммутатор будет последовательно пытаться аутентифицировать пользователя с помощью указанных методов - если первый метод не сработает, будет использован следующий и т.д.

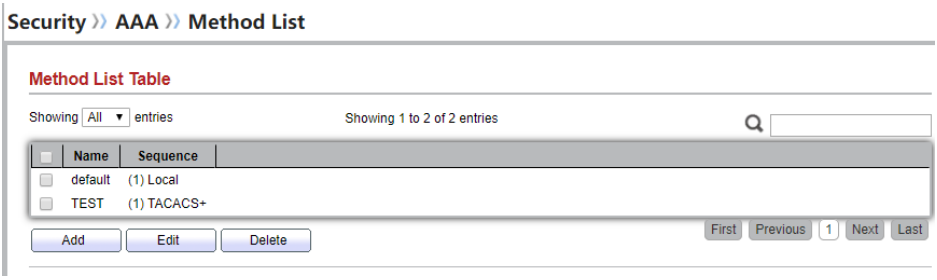
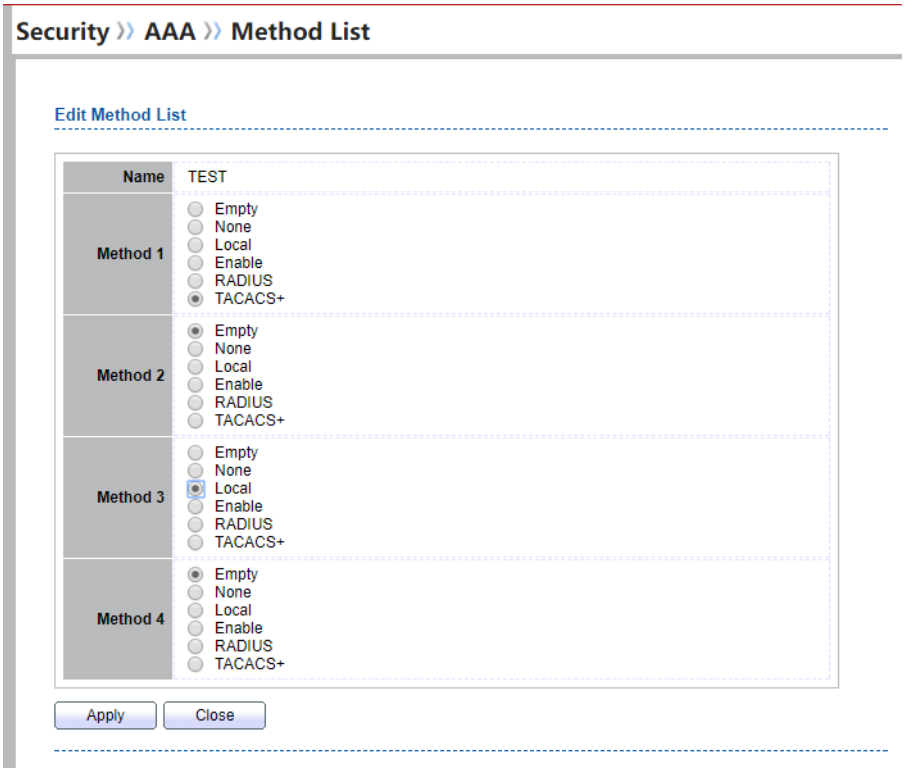


***Таблица списков методов AAA***

| Параметр | Описание |
|---|---|
| **Name** | Уникальное имя списка методов аутентификации. |

***Последовательность методов AAA***

| Параметр | Описание |
|---|---|
| **None** | Разрешает доступ без аутентификации. |
| **Local** | Использует локальную базу учетных записей коммутатора. |
| **TACACS+** | Аутентификация через TACACS+ сервер. |
| **RADIUS** | Аутентификация через RADIUS сервер. |
| **Enable** | Использует пароль коммутатора для аутентификации. |




***Настройка списка методов AAA***

| Параметр | Описание |
|---|---|
| **Name** | Уникальное имя списка методов. |

***Приоритетные методы аутентификации***

| Параметр | Описание |
|---|---|
| **Method 1** | Первичный метод аутентификации (наивысший приоритет). |

| Параметр | Описание |
|---|---|
| | • **None** – Разрешает доступ без аутентификации.<br>• **Local** – Использует локальную базу учетных записей коммутатора.<br>• **TACACS+** – Аутентификация через TACACS+ сервер.<br>• **RADIUS** – Аутентификация через RADIUS сервер.<br>• **Enable** – Использует пароль коммутатора для аутентификации |
| **Method 2** | Вторичный метод аутентификации.<br>• **None** – Разрешает доступ без аутентификации.<br>• **Local** – Использует локальную базу учетных записей коммутатора.<br>• **TACACS+** – Аутентификация через TACACS+ сервер.<br>• **RADIUS** – Аутентификация через RADIUS сервер.<br>• **Enable** – Использует пароль коммутатора для аутентификации |
| **Method 3** | Третий метод аутентификации.<br>• **None** – Разрешает доступ без аутентификации.<br>• **Local** – Использует локальную базу учетных записей коммутатора.<br>• **TACACS+** – Аутентификация через TACACS+ сервер.<br>• **RADIUS** – Аутентификация через RADIUS сервер.<br>• **Enable** – Использует пароль коммутатора для аутентификации |
| **Method 4** | Четвертый метод аутентификации. |

| Параметр | Описание |
|---|---|
| | • **None** – Разрешает доступ без аутентификации.<br>• **Local** – Использует локальную базу учетных записей коммутатора.<br>• **TACACS+** – Аутентификация через TACACS+ сервер.<br>• **RADIUS** – Аутентификация через RADIUS сервер.<br>• **Enable** – Использует пароль коммутатора для аутентификации |

**Примечания**

1. Рекомендуемая последовательность**:**
    - TACACS+/RADIUS (основной метод)
    - Local (резервный метод)
    - Enable (аварийный доступ)
2. При использовании **TACACS+/RADIUS**:
    - **Failed** означает проблемы с подключением к серверу
    - Для локального метода - отсутствие пользователя в базе
3. Список **Default** содержит базовые настройки и не может быть удален.

**Пример настройки**

- Имя списка "Admin_Access":
    - **Method 1**: TACACS+
    - **Method 2**: RADIUS
    - **Method 3**: Local
    - **Method 4**: Enable
- Для общего доступа:

- **Method 1**: RADIUS
- **Method 2**: Local

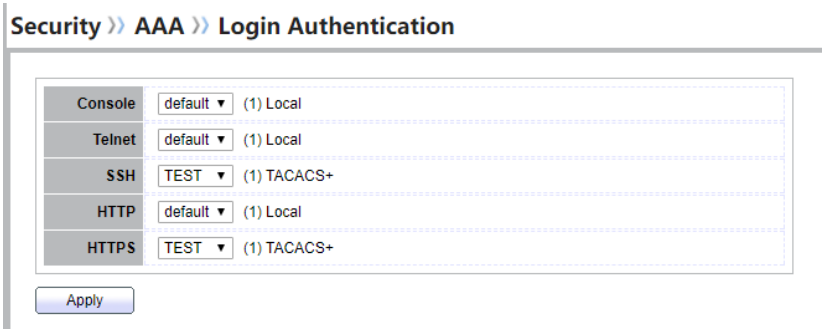
- Для аварийного доступа:
  - **Method 1**: Enable

### 13.3.2. Аутентификация входа (Login Authentication)

Для настройки политик аутентификации для различных способов управления коммутатором перейдите:

**Security > AAA > Login Authentication**

На этой странице можно назначить списки методов аутентификации (из раздела 13.3.1) для всех способов доступа к коммутатору.




***Настройки аутентификации***

| Параметр | Описание |
|---|---|
| **Console** | Список аутентификации для доступа через порт Console на коммутаторе. |

| Параметр | Описание |
|---|---|
| **Telnet** | Список аутентификации для способа управления коммутатором через Telnet. |
| **SSH** | Список аутентификации для способа управления коммутатором через SSH. |
| **HTTP** | Список аутентификации для способа управления коммутатором через WEB-интерфейс по HTTP. |
| **HTTPS** | Список аутентификации для способа управления коммутатором через веб-интерфейса по защищенному протоколу HTTPS. |

**Примечания**

1. Для каждого интерфейса можно выбрать любой созданный ранее список методов (например, **Default** или **Admin_Access**).
2. Рекомендуется:
   - Для **Console** оставить Local/Enable на случай аварийного доступа
   - Для **SSH/HTTPS** использовать строгую аутентификацию (TACACS+/RADIUS + Local)
   - Для **Telnet/HTTP** либо отключить эти сервисы, либо назначить строгую аутентификацию

**Пример настройки**

1. **Console**: default (Local > Enable)
2. **SSH/HTTPS**: Admin_Access (TACACS+ > RADIUS > Local)
3. **Telnet/HTTP**: None (отключить эти сервисы в настройках сервисов)

## 13.4. Управление доступом к коммутатору (Management Access)

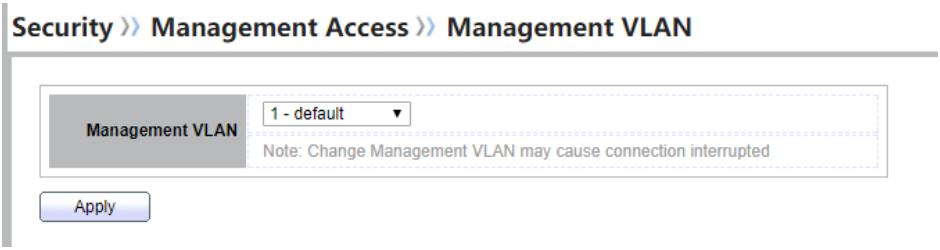
Раздел **Management Access** позволяет настраивать параметры доступа к управлению коммутатором.

### 13.4.1. VLAN управления (Management VLAN)

Для настройки Management VLAN перейдите:

**Security > Management Access > Management VLAN**

На этой странице можно назначить VLAN, через который разрешено управление коммутатором (например, через HTTP, HTTPS, SNMP и другие протоколы).




***Параметры управляющего VLAN***

| Параметр | Описание |
|---|---|
| **Management VLAN** | Выберите VLAN, который будет использоваться для управления коммутатором.<br>• Только подключения из этого VLAN будут разрешены.<br>• Все остальные подключения (из других VLAN) будут блокироваться.<br>**VLAN 1** – VLAN управления по умолчанию. |

**Примечания**

1. **Безопасность**:
   - Назначение отдельного VLAN для управления повышает безопасность, изолируя управляющий трафик от пользовательского.
   - Рекомендуется использовать **нестандартный VLAN ID** (не VLAN 1) в целях безопасности.
2. **Совместимость**:
   - Убедитесь, что выбранный VLAN существует и настроен на коммутаторе.
   - Для доступа к устройству из другого VLAN потребуется маршрутизация между VLAN.
3. **Протоколы**:
   - Настройка применяется ко всем протоколам управления:
     - WEB-интерфейс (HTTP/HTTPS)
     - Telnet/SSH
     - SNMP
     - Другие сервисы (например, RADIUS/TACACS+)

**Пример настройки**

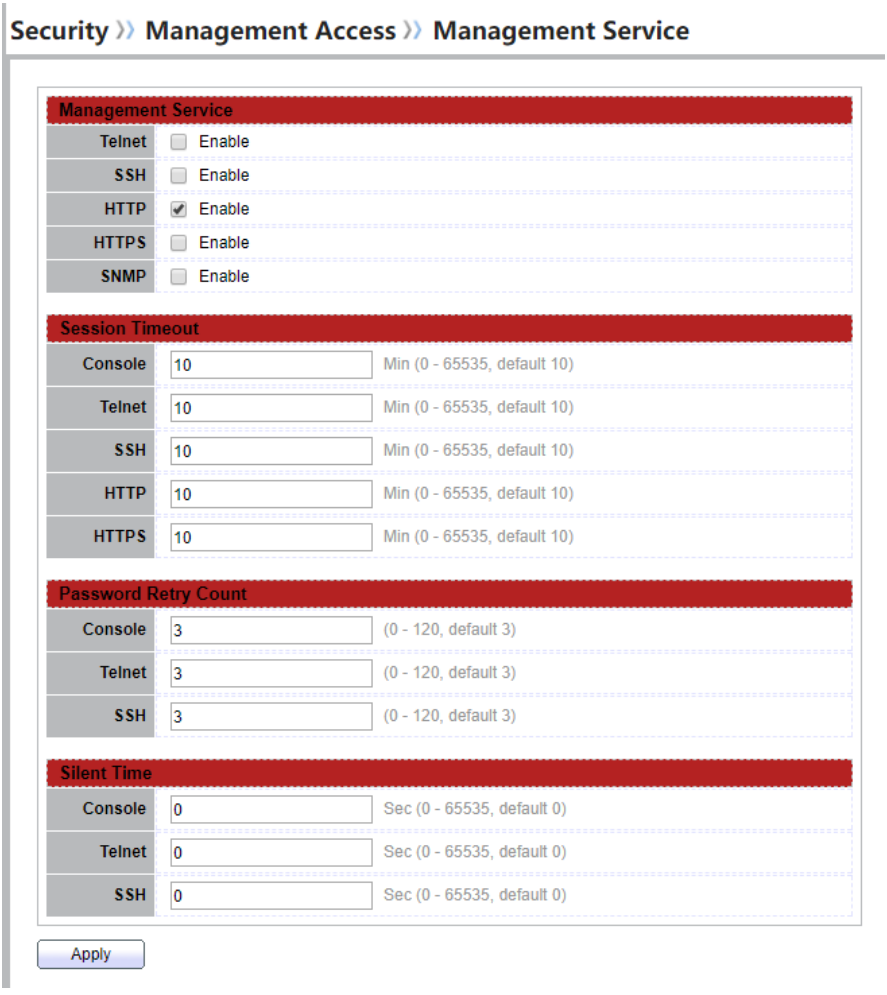
1. Создайте отдельный VLAN для управления (например, **VLAN 100**).
2. Назначьте ему IP-адрес (если требуется доступ из других сетей).
3. На этой странице выберите **Management VLAN = 100**.
4. Сохраните настройки.

### 13.4.2. Настройка способов и сервисов управления коммутатором (Management Service)

Для настройки сервисов управления перейдите:

**Security > Management Access > Management Service**

На этой странице можно включать/отключать сервисы доступа к управлению, а также настраивать параметры безопасности сессий.



***Включение/отключение различных способов управления коммутатором***

| Параметр | Описание |
|---|---|
| **Telnet** | Включение/отключение доступа к CLI через Telnet. (*Не рекомендуется из-за отсутствия шифрования*) |
| **SSH** | Включение/отключение защищенного доступа к CLI через SSH. (*Рекомендуется для безопасного управления коммутатором)* |
| **HTTP** | Включение/отключение доступа к WEB-интерфейсу по HTTP (*Не рекомендуется для производственных сетей)* |
| **HTTPS** | Включение/отключение доступа к WEB-интерфейсу по HTTPS (*Рекомендуется для безопасного доступа)* |
| **SNMP** | Включение/отключение управления коммутатором через протокол SNMP. |

***Параметры безопасности***

| Параметр | Описание |
|---|---|
| **Session Timeout** | Время неактивности (в минутах), после которого сессия управления автоматически завершается. 0 = отсутствие таймаута. (*Рекомендуется: 10-30 минут*) |
| **Password** | Максимальное количество неудачных попыток ввода |

| Параметр | Описание |
|---|---|
| **Retry Count** | пароля перед блокировкой. (*Рекомендуется: 3-5 попыток*) |
| **Silent Time** | Время блокировки (в минутах) после превышения числа попыток ввода пароля. (*Рекомендуется: 5-15 минут*) |

**Рекомендации по настройке**

1. **Безопасные протоколы**:
   - По возможности всегда используйте **SSH** вместо Telnet и **HTTPS** вместо HTTP.
   - Отключите Telnet и HTTP в производственных средах в целях повышения безопасности.
2. **Таймаут сессии**:
   - Установите 30 минут для баланса между безопасностью и удобством.
3. **Защита от перебора паролей**:
   - Password Retry Count = 3
   - Silent Time = 10 минут
4. **SNMP**:
   - Включайте только при необходимости, используйте SNMPv3 с шифрованием.

**Пример конфигурации**

1. Включите:
   - **SSH** и **HTTPS**

2. Отключите:
    - **Telnet** и **HTTP**
3. Установите:
    - Session Timeout = 30
    - Password Retry Count = 3
    - Silent Time = 10

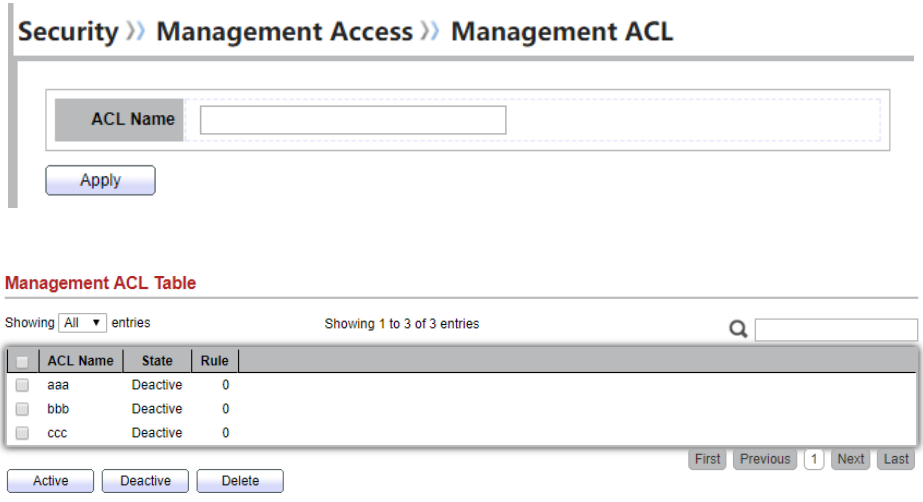
**Внимание!** После отключения Telnet/HTTP убедитесь, что SSH/HTTPS работают корректно.

### 13.4.3. ACL для управления коммутатором (Management ACL)

Для настройки ACL (Access Control List) для управления коммутатором перейдите:

**Security > Management Access > Management ACL**

На этой странице можно создавать и удалять правила ACL, ограничивающие доступ к интерфейсам управления коммутатором.



***Основные параметры***

| Параметр | Описание |
|---|---|
| **ACL Name** | Уникальное имя ACL. |
| **State** | Статус ACL (активен/неактивен). |
| **Rule** | Количество правил в ACL. |

**Добавление/удаление правил Management ACL**

1. **Создание ACL**:
   - Введите имя ACL (например, MGMT_ACCESS).
   - Нажмите **Apply**
2. **Настройка правил**:
   - Укажите:
     - **Тип правила** (разрешить/запретить)
     - **IP-адрес/подсеть** источника
     - **Протокол** (SSH, HTTPS и т.д.)
     - **Порт** (если требуется)
3. **Активация ACL**:
   - Выберите созданный ACL и нажмите **Active**

**Примечания**

1. **Цель создания Managemenet ACL**:
   - Ограничить доступ к управлению коммутатором только с доверенных IP-адресов.
2. **Рекомендации**:
   - Разрешите только подсети администраторов (например, 192.168.1.0/24).
   - Запретите все остальные подключения.

**Внимание!**

Не удаляйте активные ACL – это может привести к потере доступа к коммутатору!

**Пример настройки**

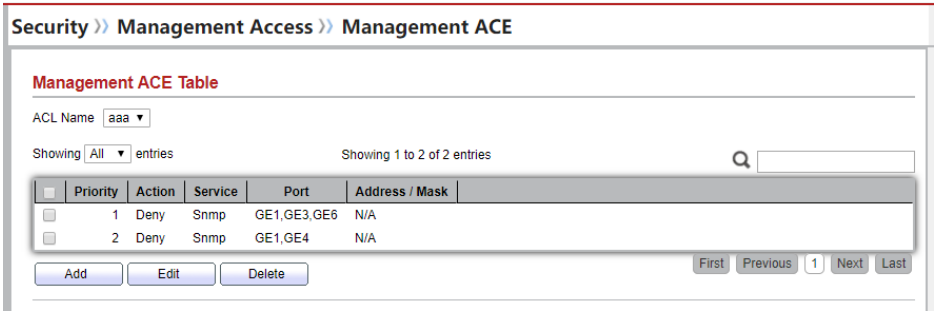
1. Создайте ACL с именем ADMIN_ACCESS.
2. Добавьте правила:
    - Разрешить 192.168.1.0/24 для SSH/HTTPS.
    - Запретить все остальные IP.
3. Активируйте ACL.

### 13.4.4. Правила ACE для управления коммутатором (Management ACE)

Для настройки правил ACE (Access Control Entry) в рамках ACL перейдите:

**Security > Management Access > Management ACE**

На этой странице WEB интерфейса можно добавлять, редактировать и удалять правила ACE, которые определяют, какие IP-адреса и сервисы могут управлять коммутатором.



### *Просмотр существующих правил ACE*

| Параметр | Описание |
|---|---|
| **ACL Name** | Имя ACL, к которому относится правило. |
| **Priority** | Приоритет правила (чем меньше число, тем выше приоритет). |
| **Action** | Действие: **Permit** (разрешить) или **Deny** (запретить). |
| **Service** | Способ/сервис управления, к которому применяется правило (HTTP, SSH и т.д.). |
| **Port** | Порт(ы), к которым применяется правило. |
| **Address / Mask** | Исходный IP-адрес и маска подсети. |


***Добавление/редактирование правил ACE***

| Параметр | Описание |
|---|---|
| **ACL Name** | Выберите ACL, к которому добавляется правило. |
| **Priority** | Приоритет (1 – наивысший). *Доступно только при добавлении.* |
| **Service** | Сервис/способ управления коммутатором:<br>**All** – все сервисы. |

| Параметр | Описание |
|---|---|
| | **HTTP/HTTPS** – WEB-интерфейс.<br>**SSH/Telnet** – CLI.<br>**SNMP** – управление через SNMP протокол. |
| **Action** | Действие:<br>**Permit** – разрешить доступ.<br>**Deny** – запретить доступ. |
| **Port** | Выберите порт(ы) для применения правила. |
| **IP Version** | Версия IP:<br>**All** – все адреса.<br>**IPv4** – только IPv4.<br>**IPv6** – только IPv6. |
| **IPv4** | Укажите IPv4-адрес и маску подсети (например, 192.168.1.0/24). |
| **IPv6** | Укажите IPv6-адрес и префикс (например, 2001:db8::/32). |

**Примечания**

1. **Порядок обработки**:
   - Правила ACE обрабатываются по приоритету (от высшего к низшему).
   - После совпадения с правилом дальнейшая проверка прекращается.
2. **Ограничения**:
   - Нельзя редактировать/удалять правила в активном ACL.

- Нельзя добавлять новые правила ACE в активный ACL (сначала отключите его).

3. **Рекомендации**:
   - Сначала добавляйте разрешающие правила для доверенных IP, затем запрещающие для всех остальных.
   - Для SSH/HTTPS используйте только Permit для административных подсетей.

**Пример настройки**

1. Выберите список, например – ACL ADMIN_ACCESS.
2. Добавьте правило:
   - **Priority**: 1
   - **Service**: SSH
   - **Action**: Permit
   - **IP Version**: IPv4
   - **IPv4**: 192.168.1.0/24
3. Добавьте второе правило:
   - **Priority**: 2
   - **Service**: All
   - **Action**: Deny
   - **IP Version**: All

**Результат**: Разрешен доступ по SSH только из 192.168.1.0/24, все остальные подключения к коммутатору запрещены.

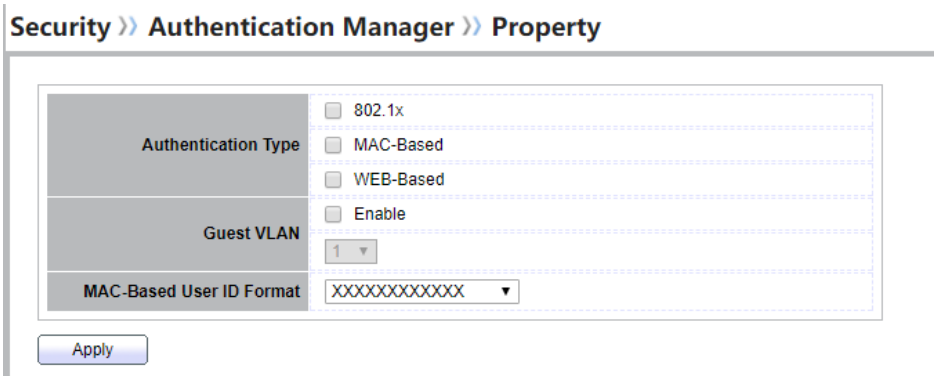
## 13.5. Менеджер аутентификации (Authentication Manager)

### 13.5.1. Свойства Authentication Manager (Property)

Для настройки параметров менеджера аутентификации перейдите:

**Security > Authentication Manager > Property**

На этой странице можно настроить глобальные параметры аутентификации и конфигурации для отдельных портов.




***Глобальные настройки аутентификации***

| Параметр | Описание |
|---|---|
| **Authentication Type** | Включение типов аутентификации:<br>**802.1X** – стандартная аутентификация по IEEE 802.1X<br>**MAC-Based** – аутентификация по MAC-адресу<br>**WEB-Based** – аутентификация через WEB-интерфейс |

| Параметр | Описание |
| --- | --- |
| **Guest VLAN** | Включение гостевого VLAN (требуется указать VLAN ID) |
| **MAC-Based User ID Format** | Формат MAC-адреса для аутентификации (20 вариантов, включая верхний/нижний регистр и разделители :, -, .)<br>• **XXXXXXXXXXXX**<br>• xxxxxxxxxxxx<br>• XX:XX:XX:XX:XX:XX<br>• xx:xx:xx:xx:xx:xx<br>• XX-XX-XX-XX-XX-XX<br>• xx-xx-xx-xx-xx-xx<br>• XX.XX.XX.XX.XX.XX<br>• xx.xx.xx.xx.xx.xx<br>• XXXX:XXXX:XXXX<br>• xxxx:xxxx:xxxx<br>• XXXX-XXXX-XXXX<br>• xxxx-xxxx-xxxx<br>• XXXX.XXXX.XXXX<br>• xxxx.xxxx.xxxx<br>• XXXXXX:XXXXXX<br>• xxxxxx:xxxxxx<br>• XXXXXX-XXXXX<br>• xxxxxx-xxxxxx<br>XXXXXX.XXXXXX<br>xxxxxx.xxxxxx |

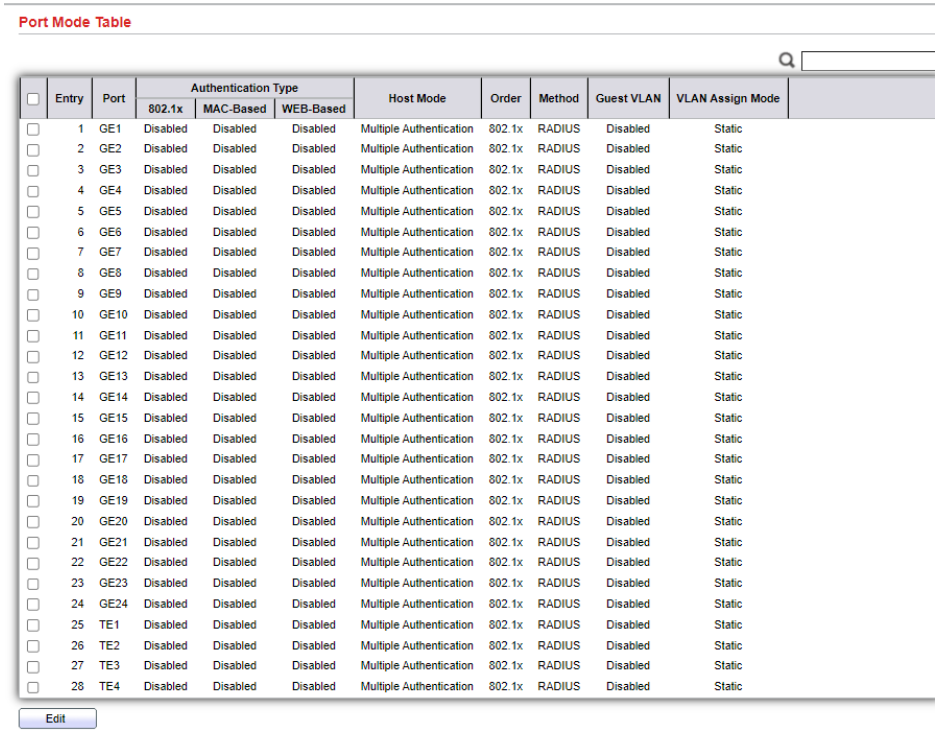



***Таблица аутентификации по портам***

| Параметр | Описание |
|---|---|
| **Port** | Имя порта |
| **Authentication Type** | Состояние типов аутентификации для порта:<br>**802.1X**<br>**MAC-Based**<br>**WEB-Based**<br>С параметрами **Disbale** (откл) **Enable** (вкл) |

| Параметр | Описание |
|---|---|
| **Host Mode** | Режим аутентификации устройств:<br>**Multiple Authentication** – каждое устройство аутентифицируется отдельно<br>**Multiple Hosts** – одно устройство проходит аутентификацию для всех (не поддерживает WEB-Based)<br>**Single Host** – только одно устройство |
| **Order** | Порядок проверки типов аутентификации (WEB-Based всегда последний)<br>• **802.1x**<br>• **MAC-Based**<br>• **WEB-Based**<br>• **802.1x MAC-Based**<br>• **802.1x WEB-Based**<br>• **MAC-Based 802.1x**<br>• **WEB-Based 802.1x**<br>• **802.1x MAC-Based WEB-Based**<br>• **802.1x WEB-Based MAC-Based** |
| **Method** | Методы аутентификации (для MAC/WEB):<br>**Local** – локальная база аутентификации<br>**Radius** – удаленный сервер RADIUS<br>**Local Radius** – сначала локальная, затем RADIUS аутентификация.<br>**RadiusLocal** – сначала RADIUS, затем локальная аутентификация |
| **Guest VLAN** | Включение гостевого VLAN для порта |

| Параметр | Описание |
|---|---|
| | С параметрами **Disbale** (откл) **Enable** (вкл) |
| **VLAN Assign Mode** | Режим назначения VLAN (только для RADIUS аутентификации):<br>**Disable** – игнорировать VLAN из RADIUS<br>**Reject** – требовать VLAN от RADIUS<br>**Static** – использовать VLAN из RADIUS (если настроено) |

***Настройка аутентификации по портам***

| Параметр | Описание |
|---|---|
| **Port** | Имя порта |
| **Authentication Type** | Выбор типа аутентификации для порта:<br>**802.1X**<br>**MAC-Based**<br>**WEB-Based** |
| **Host Mode** | Режим аутентификации устройств:<br>**Multiple Authentication** – каждое устройство аутентифицируется отдельно<br>**Multiple Hosts** – одно устройство проходит аутентификацию для всех (не поддерживает WEB-Based)<br>**Single Host** – только одно устройство |
| **Order** | Порядок проверки типов аутентификации (WEB-Based всегда последний)<br>• **802.1x**<br>• **MAC-Based**<br>• **WEB-Based**<br>• **802.1x MAC-Based**<br>• **802.1x WEB-Based**<br>• **MAC-Based 802.1x**<br>• **WEB-Based 802.1x**<br>• **802.1x MAC-Based WEB-Based**<br>• **802.1x WEB-Based MAC-Based** |
| **Method** | Методы аутентификации (для MAC/WEB): |

| Параметр | Описание |
|---|---|
| | **Local** – локальная база аутентификации<br>**Radius** – удаленный сервер RADIUS<br>**Local Radius** – сначала локальная, затем RADIUS аутентификация.<br>**RadiusLocal** – сначала RADIUS, затем локальная аутентификация |
| **Guest VLAN** | Включение гостевого VLAN для порта |
| **VLAN Assign Mode** | Режим назначения VLAN (только для RADIUS аутентификации):<br>**Disable** – игнорировать VLAN из RADIUS<br>**Reject** – требовать VLAN от RADIUS<br>**Static** – использовать VLAN из RADIUS (если настроено) |

**Примечания**

1. **WEB-Based** аутентификация всегда должна быть последней в порядке проверки.
2. Для **802.1X** поддерживается только метод **Radius**.
3. В режиме **Multiple Hosts** WEB-аутентификация недоступна.

**Пример настройки**

- **Глобальные параметры**:
  - Включите **802.1X** и **MAC-Based**.
  - Выберите формат MAC-адреса: XX-XX-XX-XX-XX-XX.
- **Для порта GE1**:

- **Host Mode**: Multiple Authentication
- **Order**: 802.1X → MAC-Based
- **Method**: Radius
- **VLAN Assign Mode**: Static

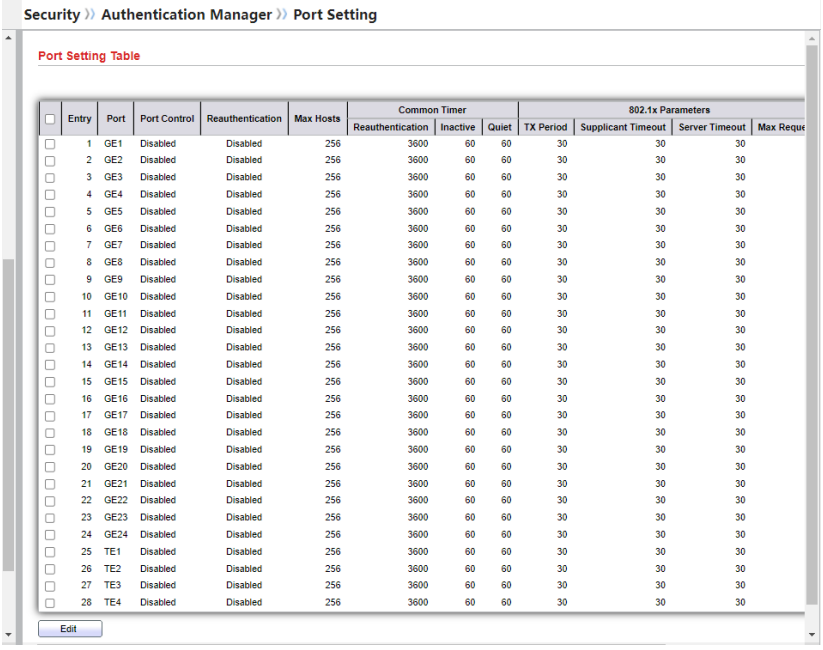
- **Для порта GE2 (гостевой доступ)**:
  - Включите **Guest VLAN** (VLAN 100).
  - **Order**: WEB-Based
  - **Method**: Local Radius

### 13.5.2. Настройки портов для аутентификации (Port Setting)

Для настройки параметров аутентификации на портах перейдите:

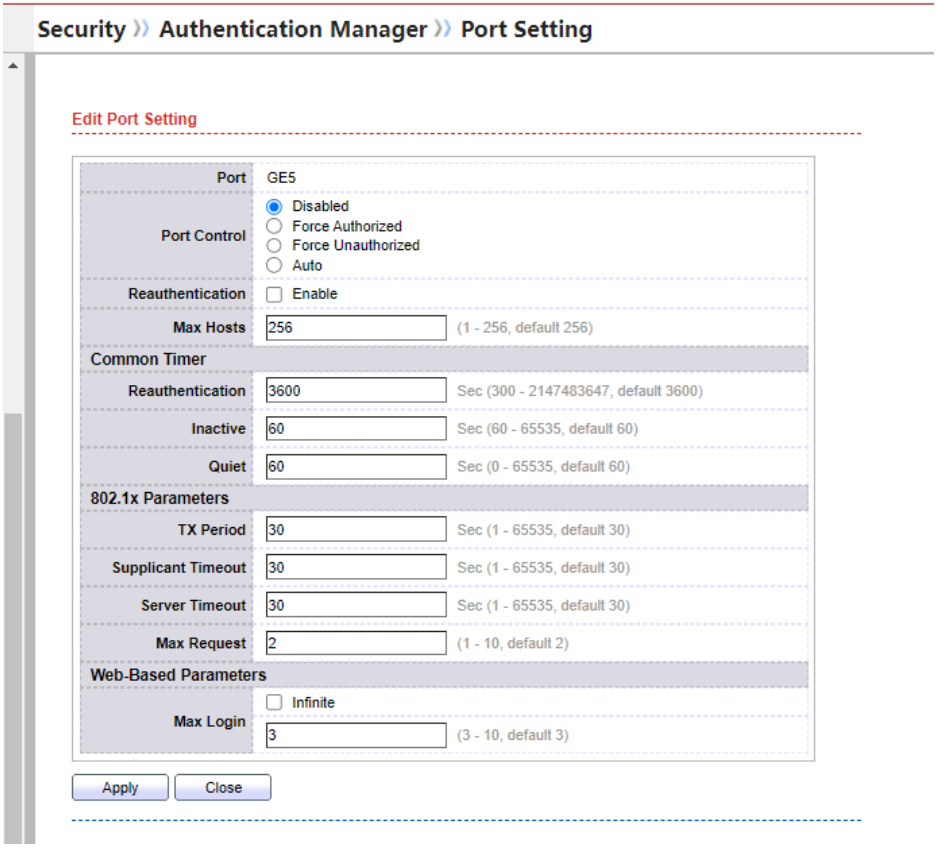
**Security > Authentication Manager > Port Setting**

На этой странице WEB интерфейса можно настроить режимы контроля доступа, таймеры и параметры аутентификации для каждого порта.



| Параметр | Описание |
|---|---|
| **Port** | Имя порта |
| **Port Control** | Режим контроля доступа:<br>**Disable** – аутентификация отключена (все устройства имеют доступ)<br>**Force Authorized** – порт принудительно открыт<br>**Force Unauthorized** – порт принудительно закрыт<br>**Auto** – доступ только после успешной аутентификации |
| **Reauthentication** | Повторная аутентификация:<br>**Enabled** – периодическая проверка<br>**Disabled** – одноразовая аутентификация |
| **Max Hosts** | Максимальное число устройств (для режима Multiple Authentication) |
| Параметры таймера | |
| **Reauthentication** | Интервал повторной аутентификации (сек) |
| **Inactive** | Время неактивности до отключения (сек) |
| **Quiet** | Время блокировки после неудачных попыток (сек) |
| Параметры 802.1X | |
| **TX Period** | Интервал между EAP-запросами (сек) |
| **Supplicant Timeout** | Таймаут ожидания ответа от клиента (сек) |

| Параметр | Описание |
|---|---|
| **Server Timeout** | Таймаут ожидания ответа от сервера (сек) |
| **Max Request** | Максимальное число попыток запроса |



| Параметр | Описание |
|---|---|
| **Port** | Порт |
| **Port Control** | Режим контроля доступа:<br>**Disable** – аутентификация отключена (все устройства имеют доступ)<br>**Force Authorized** – порт принудительно открыт<br>**Force Unauthorized** – порт принудительно закрыт<br>**Auto** – доступ только после успешной аутентификации |
| **Reauthentication** | Повторная аутентификация:<br>**Enabled** – периодическая проверка (повторная аутентификация) включена |
| **Max Hosts** | Максимальное число устройств (для режима Multiple Authentication). От 1 до 256 (значение по умолчанию 256) |
| Параметры таймера | |
| **Reauthentication** | Интервал повторной аутентификации (сек). От 300 до 2147483647сек (значение по умолчанию 3600 сек) |
| **Inactive** | Время неактивности до отключения (сек) От 60 до 65535сек (значение по умолчанию 60сек) |
| **Quiet** | Время блокировки после неудачных попыток (сек) От 60 до 65535сек (значение по умолчанию 60сек) |
| Параметры 802.1X | |

| Параметр | Описание |
|---|---|
| **TX Period** | Интервал между EAP-запросами (сек) От 1 до 65535сек (значение по умолчанию 30сек) |
| **Supplicant Timeout** | Таймаут ожидания ответа от клиента (сек) От 1 до 65535сек (значение по умолчанию 30сек) |
| **Server Timeout** | Таймаут ожидания ответа от сервера (сек) От 1 до 65535сек (значение по умолчанию 30сек) |
| **Max Request** | Максимальное число попыток запроса. От 1 до 10 попыток (значение по умолчанию 2) |
| Параметры WEB аутентификации (WEB based) | |
| **Max Login** | Максимальное число неудачных попыток входа (рекомендуется 3-5, значение по умолчанию – 3)<br>**Infinite** – не ограниченное количество попыток. |

**Рекомендации по настройке**

1. Для **офисных портов**:
   - **Port Control**: Auto
   - **Reauthentication**: Enabled (3600 сек)
   - **Max Hosts**: 1-3
2. Для **гостевых портов**:
   - **Port Control**: Auto
   - **WEB-Based** аутентификация
   - **Max Login**: 3
3. Для **серверных портов**:
   - **Port Control**: Force Authorized

**Пример конфигурации**

1. **Порт GE1** (офисный):
   - **Port Control**: Auto
   - **Reauthentication**: 3600 сек
   - **802.1X Params**: TX Period=30, Max Request=2
2. **Порт GE2** (гостевой):
   - **Port Control**: Auto
   - **WEB-Based Param**: Max Login=3
   - **Quiet Timer**: 300 сек

### 13.5.3. Локальные учетные записи MAC-Based (MAC-Based Local Account)

Для настройки локальных учетных записей MAC-адресов перейдите:

**Security > Authentication Manager > MAC-Based Local Account**

На этой странице можно добавлять, редактировать и удалять локальные записи для MAC-аутентификации.

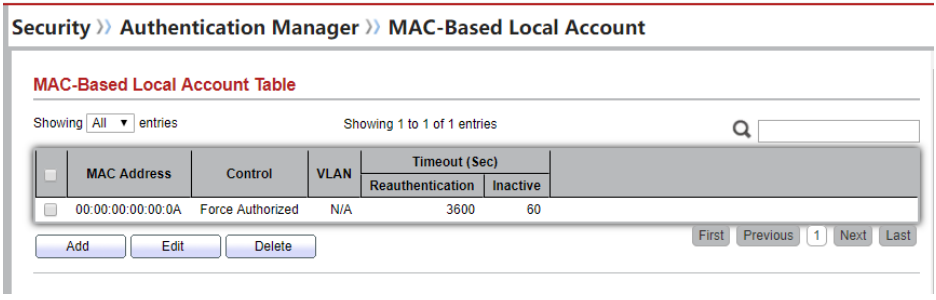
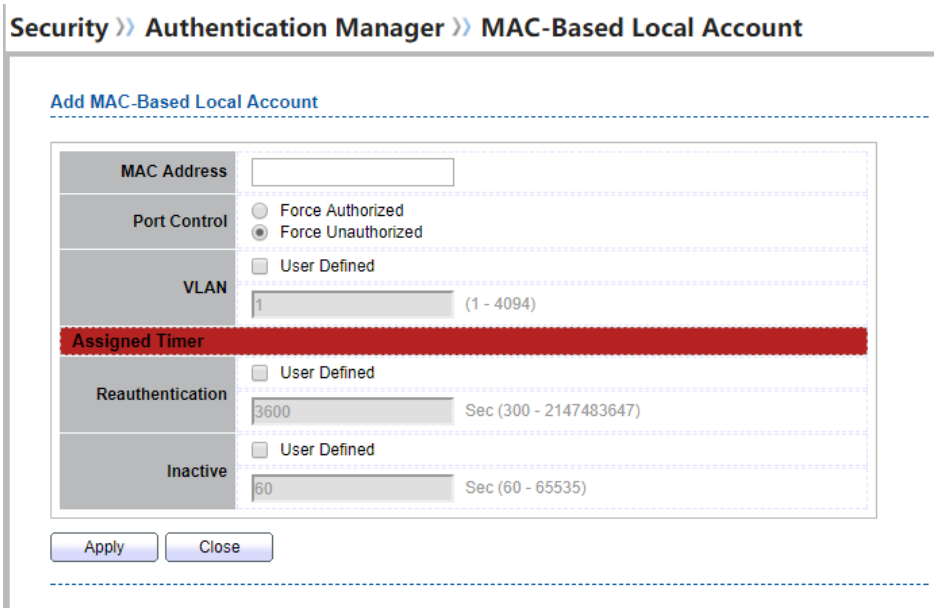
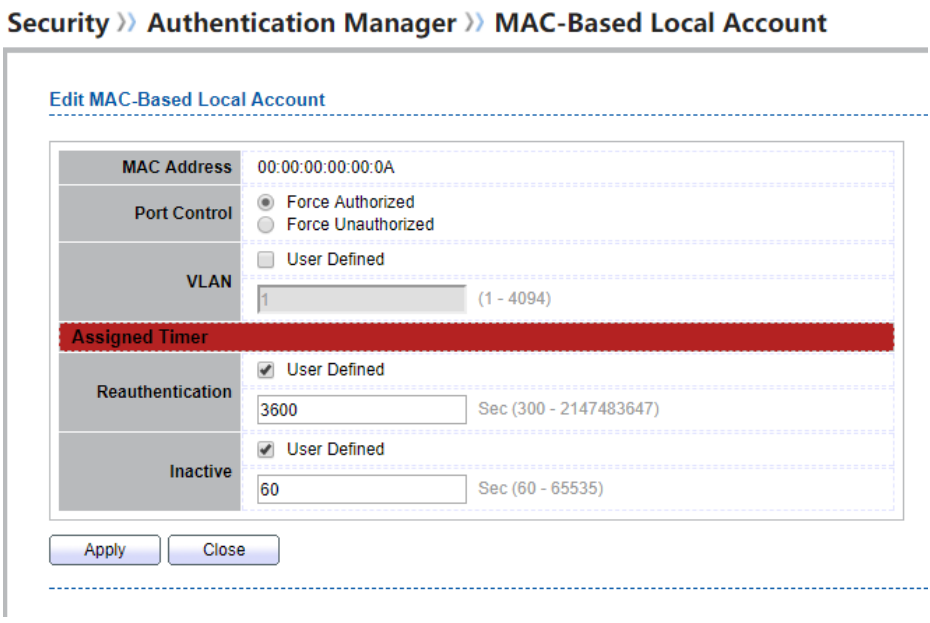


***Таблица локальных учетных записей MAC-Based***

| Параметр | Описание |
|---|---|
| **MAC Address** | MAC-адрес устройства (формат: `XX-XX-XX-XX-XX-XX`). Каждый MAC-адрес может быть добавлен только один раз. |
| **Control** | Тип контроля доступа:<br>**Force Authorized** – устройство всегда получает доступ<br>**Force Unauthorized** – устройство всегда блокируется |
| **VLAN** | VLAN, назначаемый устройству после аутентификации. |
| **Timeout (Reauthentication)** | Интервал повторной аутентификации (в секундах). |
| **Timeout (Inactive)** | Время неактивности до отключения (в секундах). |



***Добавление/редактирование учетной записи MAC-Based***

| Параметр | Описание |
|---|---|
| **MAC Address** | MAC-адрес устройства (формат: XX-XX-XX-XX-XX-XX). Каждый MAC-адрес может быть добавлен только один раз. |
| **Control** | Тип контроля доступа:<br>**Force Authorized** – устройство всегда получает доступ<br>**Force Unauthorized** – устройство всегда блокируется |
| **VLAN** | VLAN, назначаемый устройству после аутентификации. (1-4094) |
| **Timeout (Reauthentication)** | Интервал повторной аутентификации (сек) От 300 до 2147483647сек (Значение по умолчанию 3600сек) |
| **Timeout (Inactive)** | Время неактивности до отключения (сек) От 60 до 65535сек (Значение по умолчанию 60сек) |

Нажмите кнопку **Apply** (применить), чтобы применить настройки.

**Примечания**

1. **Использование**:
   - Для устройств без поддержки 802.1X (принтеры, камеры).

- Для статического назначения VLAN по MAC-адресу.

2. **Приоритет**:
   - Локальные записи имеют приоритет над RADIUS-аутентификацией, если включен метод **Local** или **Local Radius**.
3. **Формат MAC-адреса**:
   - Должен соответствовать выбранному в глобальных настройках (см. раздел **13.5.1**).

**Пример настройки**

1. **Добавление принтера**:
   - **MAC Address**: 00-1A-2B-3C-4D-5E
   - **Control**: Force Authorized
   - **VLAN**: 10
   - **Timeout (Reauthentication)**: 86400 (1 день)
2. **Блокировка устройства**:
   - **MAC Address**: 00-1E-4F-AB-CD-EF
   - **Control**: Force Unauthorized
3. **Гостевой доступ**:
   - **MAC Address**: A0-B1-C2-D3-E4-F5
   - **VLAN**: 100
   - **Timeout (Inactive)**: 1800 (30 минут)

### 13.5.4. Локальные учетные записи WEB-аутентификации (WEB-Based Local Account)

Для настройки локальных учетных записей веб-аутентификации перейдите:

**Security > Authentication Manager > WEB-Based Local Account**

На этой странице можно добавлять, редактировать и удалять учетные записи для аутентификации через WEB-интерфейс.

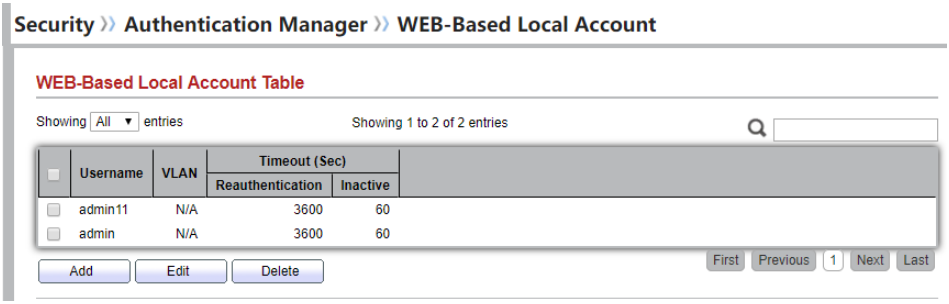
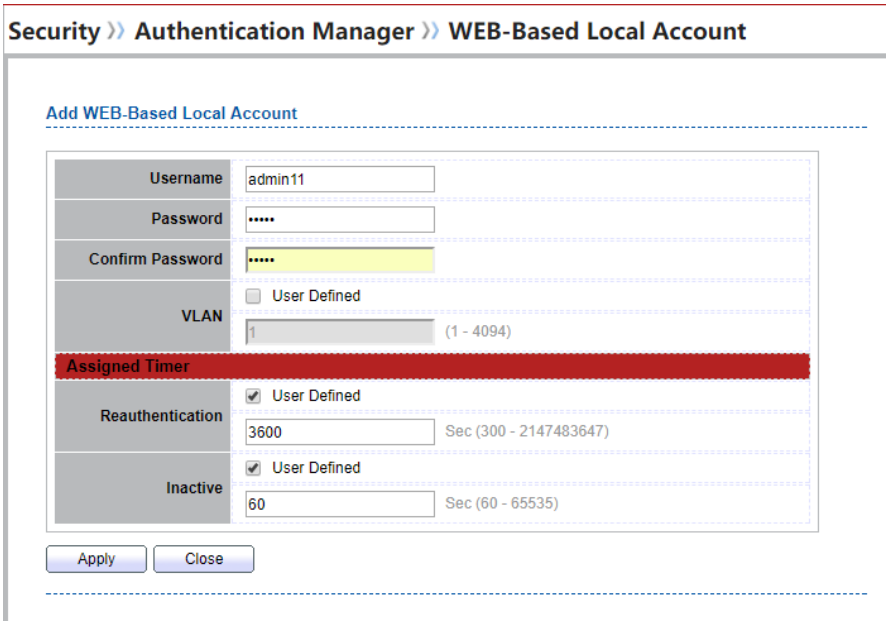
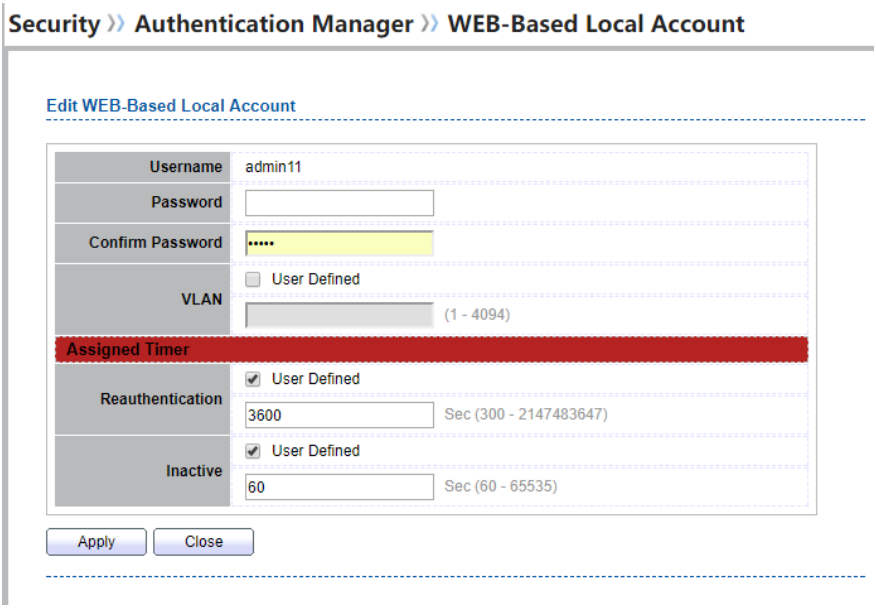



***Таблица учетных записей WEB-Based***

| Параметр | Описание |
|---|---|
| **Username** | Логин пользователя |
| **VLAN** | VLAN, назначаемый после успешной аутентификации |
| **Timeout (Reauthentication)** | Интервал повторной аутентификации (сек) |
| **Timeout (Inactive)** | Таймаут неактивности до отключения (сек) |




***Добавление/редактирование учетной записи***

| Параметр | Описание |
|---|---|
| **Username** | Уникальное имя пользователя (регистрозависимое) |
| **Password** | Пароль (мин. сложность: 8 символов, буквы+цифры) |
| **Confirm Password** | Подтверждение пароля |
| **VLAN** | VLAN ID для пользователя (опционально) 1-4094. |
| **Timeout (Reauthentication)** | Интервал повторного ввода пароля (сек) (0 = никогда) От 300 до 2147483647сек (Значение по умолчанию 3600сек) |
| **Timeout (Inactive)** | Время неактивности пользователя до автоматического выхода (сек) От 60 до 65535сек (Значение по умолчанию 60сек) |

**Примечания**

1. **Использование**:
   - Для гостевого доступа (Wi-Fi, конференц-залы).
   - Когда RADIUS-сервер недоступен.
2. **Безопасность**:
   - Пароли хранятся в зашифрованном виде.
   - Рекомендуется:
     - Минимум 12 символов

- Смена паролей каждые 90 дней

3. **Таймауты**:
   - **Reauthentication**: 14400 сек (4 часа) для офисных пользователей
   - **Inactive**: 900 сек (15 мин) для гостевых зон

**Пример настройки**

1. **Офисный сотрудник**:
   - **Username**: employee1
   - **Password**: N7sK#p92qX!z
   - **VLAN**: 10
   - **Reauthentication**: 28800 (8 часов)
2. **Гостевой доступ**:
   - **Username**: guest
   - **Password**: Welcome123
   - **VLAN**: 100
   - **Inactive Timeout**: 1800 (30 мин)
3. **Администратор**:
   - **Username**: admin
   - **Password**: $Adm1nP@ss
   - **Reauthentication**: 0 (требуется только при входе)

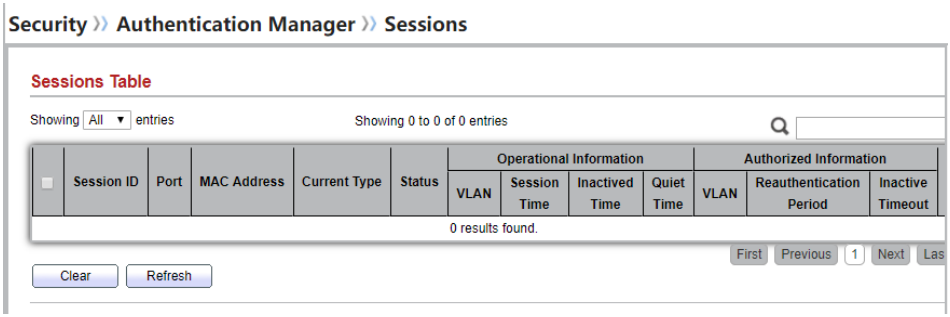
**Внимание!** Для критичных систем используйте только RADIUS-аутентификацию!

### 13.5.5. Просмотр сессий аутентификации (Sessions)

Для просмотра и управления активными сессиями аутентификации перейдите:

**Security > Authentication Manager > Sessions**

На этой странице отображаются все текущие сессии аутентификации с возможностью принудительного завершения.




***Информация о сессиях***

| Поле | Описание |
|---|---|
| **Session ID** | Уникальный идентификатор сессии |
| **Port** | Порт подключения устройства |
| **MAC Address** | MAC-адрес устройства |
| **Current Type** | Тип аутентификации:<br>**802.1X** – стандартная аутентификация<br>**MAC-Based** – по MAC-адресу |

| Поле | Описание |
|---|---|
| | **WEB-Based** – через веб-интерфейс |
| **Status** | Статус сессии:<br>**Disabled** – готова к удалению<br>**Running** – в процессе аутентификации<br>**Authorized** – успешная аутентификация<br>**Unauthorized** – доступ запрещен<br>**Locked** – временная блокировка<br>**Guest** – доступ через гостевой VLAN |
| **Operational (VLAN)** | Текущий VLAN устройства |
| **Operational (Session Time)** | Время с момента авторизации |
| **Operational (Inactived)** | Время неактивности устройства |
| **Operational (Quiet Time)** | Время до разблокировки (для статуса Locked) |
| **Authorized (VLAN)** | VLAN, назначенный при аутентификации |
| **Authorized (Reauthentication Period)** | Интервал повторной аутентификации |
| **Authorized (Inactive Timeouts)** | Таймаут неактивности |

Кнопка **Clear** – принудительное завершение выбранной сессии.
Кнопка **Refresh** – обновить список сессий аутентификации

**Примечания**

1. **Locked** статус возникает после превышения числа неудачных попыток входа (см. **Max Login** в разделе **13.5.2**).
2. Для **гостевых сессий** VLAN может отличаться от назначенного при аутентификации.

**Пример использования**

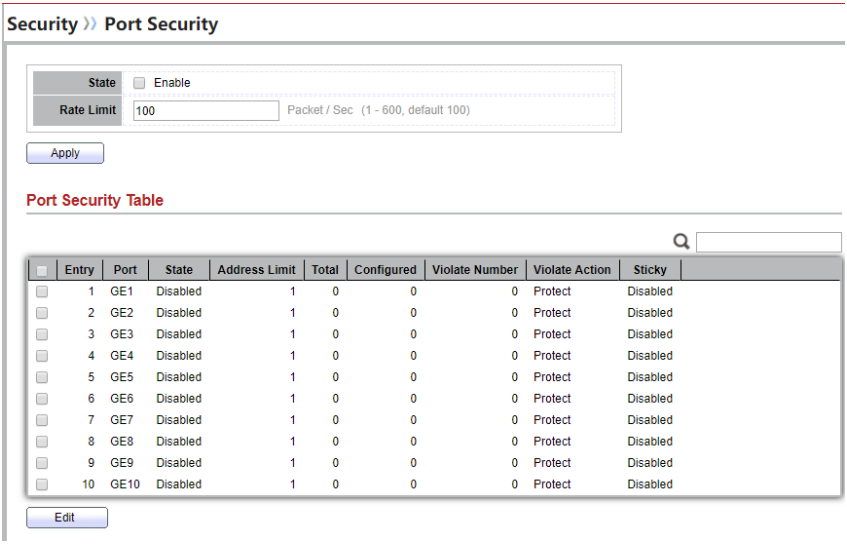
1. **Проблема**: Устройство `00:1A:2B:3C:4D:5E` не может аутентифицироваться.
    - Проверьте **Status**:
        - Если `Locked` – устройство временно заблокировано.
        - Если `Unauthorized` – проверьте настройки RADIUS/MAC-адреса.
2. **Решение**:
    - Для сброса выберите сессию и нажмите **Clear**.

## 13.6. Защита портов (Port Security)

Для настройки защиты портов перейдите:

**Security > Port Security**

На этой странице WEB интерфейса коммутатора есть возможность ограничить количество MAC-адресов на порту и задать действия при превышении лимита.




***Настройки защиты портов***

| Параметр | Описание |
|---|---|
| **Port** | Выберите порт(ы) для настройки. |

| Параметр | Описание |
|---|---|
| **State** | Состояние защиты порта:<br>**Disable** – функция отключена.<br>**Enable** – функция включена. |
| **MAC Address** | Максимальное количество разрешенных MAC-адресов на порту (1-1024). |
| **Action** | Действие при превышении лимита:<br>**Forward** – пропускать новые MAC-адреса (только логирование).<br>**Discard** – блокировать пакеты с новыми MAC-адресами.<br>**Shutdown** – отключать порт при нарушении. |

**Примечания**

1. **Использование**:
   - Защита от MAC-флудинга и несанкционированного доступа.
   - Рекомендуется для портов с фиксированными устройствами (IP-телефоны, принтеры).
2. **Рекомендуемые настройки**:
   - **Офисные порты**: MAC Address = 2-3 (компьютер + телефон).
   - **Серверные порты**: Action = Discard.
   - **Гостевые порты**: Action = Shutdown для полной изоляции.

**Внимание!**

Режим **Shutdown** требует ручного включения порта после срабатывания.

**Пример настройки**

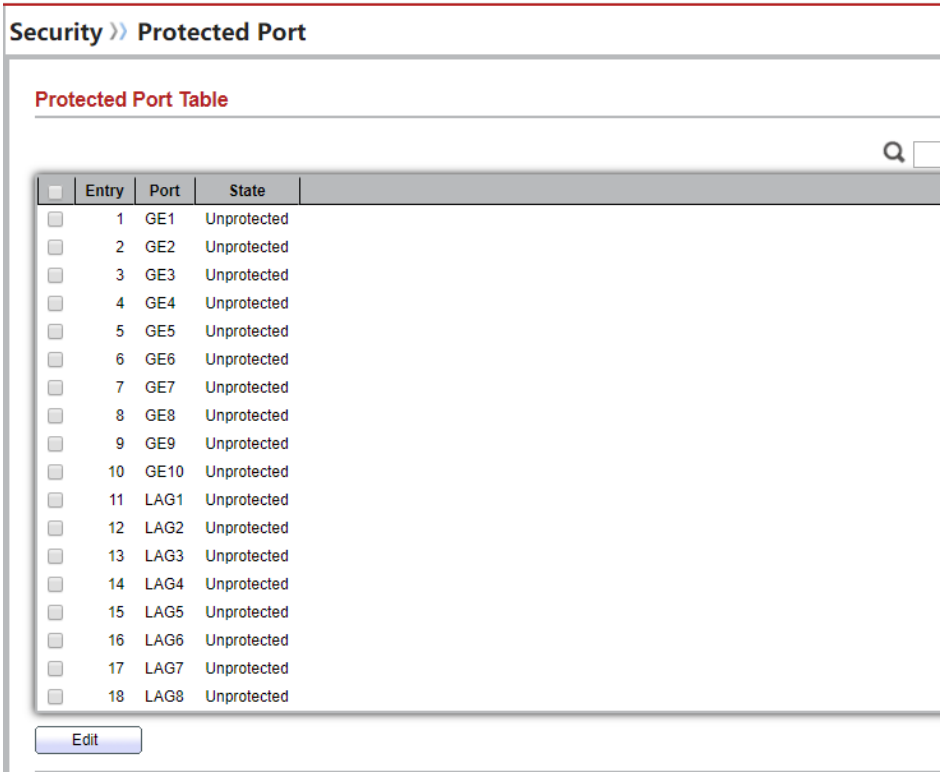
1. **Порт GE1** (рабочее место):
    - **State**: Enable
    - **MAC Address**: 2
    - **Action**: Discard
2. **Порт GE24** (сервер):
    - **State**: Enable
    - **MAC Address**: 1
    - **Action**: Shutdown

## 13.7. Настройка изоляции портов (Protected Port)

Для настройки изолированных портов перейдите в следующий раздел:

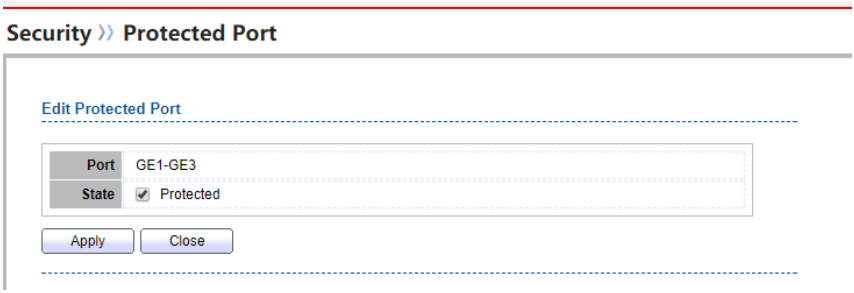
**Security > Protected Port**

На этой странице WEB интерфейса есть возможность включить режим изоляции портов, который запрещает взаимодействие между защищенными (protected) портами, разрешая только обмен с незащищенными портами.




***Список защищенных/незащищенных портов***

| Параметр | Описание |
|---|---|
| **Port** | Номер порта |
| **State** | Режим изоляции:<br>**Protected** – порт изолирован (не может обмениваться данными с другими защищенными портами)<br>**Unprotected** – стандартный режим работы |




***Выбор типа порта для функции изоляции портов***

| Параметр | Описание |
|---|---|
| **Port** | Номер порта |
| **State** | Режим изоляции:<br>**Protected** – порт изолирован (не может обмениваться данными с другими защищенными портами)<br>**Unprotected** – стандартный режим работы |

**Примечания**

1. **Применение**:
   - Изоляция пользователей в общедоступных сетях (гостевые Wi-Fi, интернет-кафе).
   - Защита критичных устройств (серверы, камеры) от несанкционированного доступа с других портов.
2. **Особенности**:
   - Защищенные порты **могут** взаимодействовать с:
     - Незащищенными портами
     - Внешними сетями (через маршрутизатор)

- Запрещено взаимодействие **между защищенными портами** на одном коммутаторе.

3. **Ограничения**:
   - Не влияет на широковещательный трафик (ARP, DHCP).
   - Для полной изоляции требуется сочетать с функцией **Private VLAN**.

**Пример настройки**

1. **Гостевые порты (GE1-GE12)**:
   - **State**: Protected
   - Результат: Гостевые пользователи не могут обмениваться данными между собой, но имеют доступ в интернет.
2. **Серверные порты (GE23-GE24)**:
   - **State**: Unprotected
   - Результат: Серверы доступны со всех портов.
3. **Порт администратора (GE20)**:
   - **State**: Unprotected
   - Результат: Полный доступ ко всем устройствам.

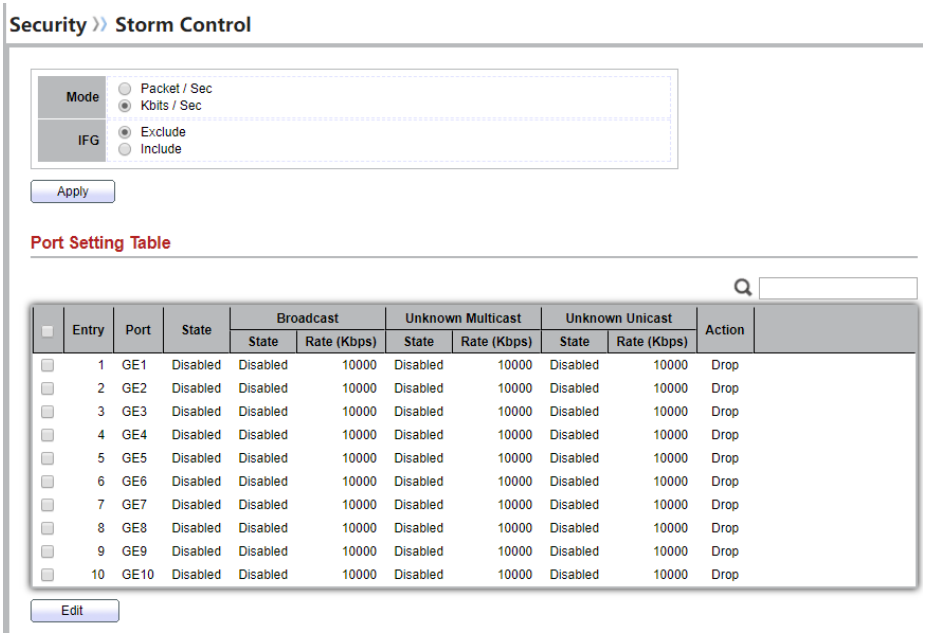
**Важно!**

Для управления защищенными портами используйте незащищенный порт или удаленный доступ (SSH/Web-интерфейс).

## 13.8. Настройка функции Storm Control (Storm Control)

Для настройки защиты от нежелатеьного трафика (broadcast, multicast, unicast) перейдите:

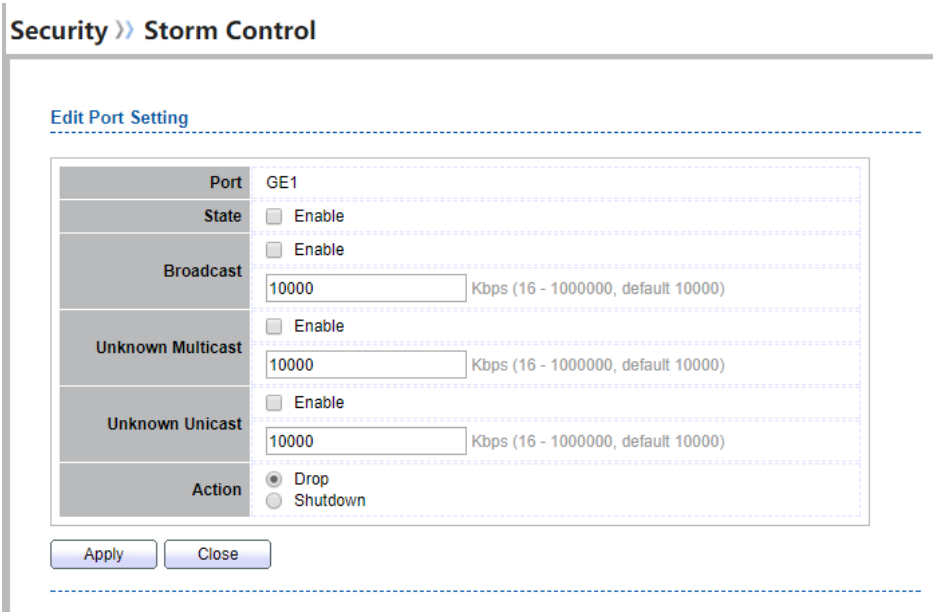
**Security > Storm Control**




***Глобальные настройки***

| Параметр | Описание |
|---|---|
| **Mode** | Единицы измерения:<br>**Packet/Sec** – контроль по количеству пакетов<br>**Kbits/Sec** – контроль по объему трафика |
| **IFG** | Учет межпакетного интервала (20 байт): |

| Параметр | Описание |
|---|---|
| | **Excluded** – не учитывается<br>**Included** – учитывается |




***Настройки портов***

| Параметр | Описание |
|---|---|
| **Port** | Выбранные порты |
| **State** | Включение Storm Control:<br>**Enable** – активировать функцию |

| Параметр | Описание |
|---|---|
| **Broadcast** | Лимит для broadcast-трафика (1-262143 pps или 16-1000000 Kbps) |
| **Unknown Multicast** | Лимит для неизвестного multicast-трафика |
| **Unknown Unicast** | Лимит для неизвестного unicast-трафика |
| **Action** | Действие при превышении объема трафика:<br>**Drop** – отбрасывание пакетов<br>**Shutdown** – отключение порта |

**Рекомендации**

1. **Типовые значения**:
   - **Broadcast**: 100-1000 pps
   - **Multicast**: 500 pps
   - **Unicast**: 1000 pps
2. **Критические порты**:
   - Используйте **Shutdown** для серверных портов.
3. **Мониторинг**:
   - Логируйте события превышения лимитов.

**Пример настройки**

1. **Глобально**:
    - **Unit**: Kbits/Sec
    - **IFG**: Included
2. **Порт GE1**:
    - **Broadcast**: 500 Kbps
    - **Action**: Drop
3. **Порт GE24**:
    - **Unknown Unicast**: 1000 Kbps
    - **Action**: Shutdown

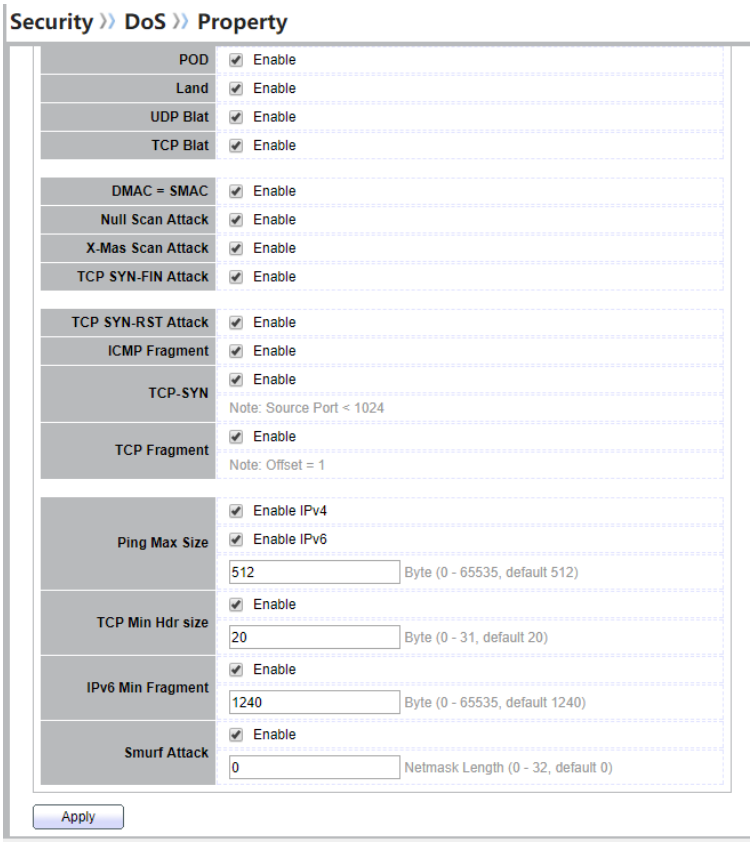
## 13.9. Защита от DoS-атак (Denial of Service)

Функция защиты от DoS-атак предотвращает перегрузку коммутатора за счет блокировки вредоносного трафика.

### 13.9.1. Глобальные настройки функции DOS (Property)

Для настройки перейдите по следующему пути:

**Security > DoS > Property**




| Параметр | Описание | Рекомендации |
|---|---|---|
| **POD** | Защита от атаки Ping of Death | Всегда включать |
| **Land** | Блокировка пакетов, где IP отправителя = IP получателя | Включить |
| **UDP Blat** | Блокировка UDP-пакетов с одинаковыми портами | Для серверов |

| Параметр | Описание | Рекомендации |
|---|---|---|
| **TCP Blat** | Блокировка TCP-пакетов с одинаковыми портами | Для серверов |
| **DMAC = SMAC** | Блокировка пакетов с одинаковыми MAC-адресами | Включить |
| **Null Scan Attack** | Защита от NULL-сканирования | Включить |
| **X-Mas Scan Attack** | Защита от X-Mas сканирования (пакеты с FIN/URG/PSH) | Включить |
| **TCP SYN-FIN Attack** | Блокировка пакетов с SYN+FIN флагами | Включить |
| **TCP SYN-RST Attack** | Блокировка пакетов с SYN+RST флагами | Включить |
| **ICMP Fragment** | Блокировка фрагментированных ICMP-пакетов | Включить |
| **TCP-SYN(SPORT<1024)** | Блокировка SYN-пакетов с портом <1024 | Опционально |
| **TCP Fragment (Offset=1)** | Блокировка TCP-фрагментов со смещением=1 | Включить |
| **Ping Max Size** | Макс. размер ICMP-пакетов (0-65535, по умолч. 512) | 512-1024 байт |
| **IPv4 Ping Max Size** | Проверка размера ICMPv4 пакетов | Включить |

| Параметр | Описание | Рекомендации |
|---|---|---|
| **IPv6 Ping Max Size** | Проверка размера ICMPv6 пакетов | Для IPv6-сетей |
| **TCP Min Hdr Size** | Мин. размер TCP-заголовка (0-31, по умолч. 20) | 20 байт |
| **IPv6 Min Fragment** | Мин. размер IPv6-фрагментов (по умолч. 1240) | 1240 байт |
| **Smurf Attack** | Защита от Smurf-атак (маска 0-32) | Включить |

**Рекомендации**

1. **Базовые настройки**:
   - Включите все защиты, кроме **TCP-SYN(SPORT<1024)** (может блокировать легитимный трафик).
   - Для **Ping Max Size** установите 1024 байта.
2. **Серверные порты**:
   - Активируйте **UDP Blat** и **TCP Blat**.
3. **IPv6-сети**:
   - Включите **IPv6 Ping Max Size** и **IPv6 Min Fragment**.

**Пример конфигурации**

1. Включите основные защиты:
   - POD, Land, DMAC=SMAC, X-Mas Scan
2. Для корпоративной сети:

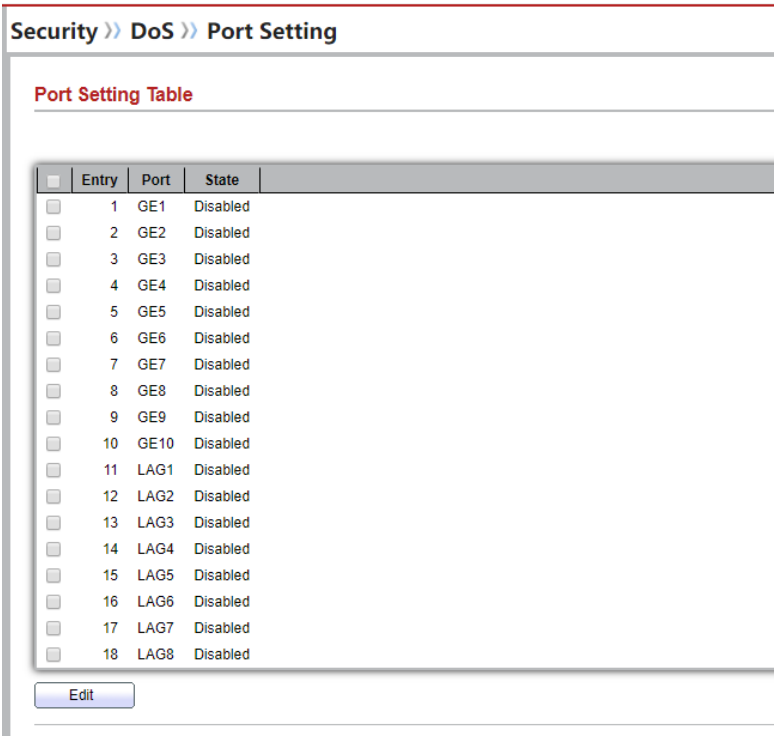
- **Ping Max Size**: 1024
- **TCP Min Hdr Size**: 20

3. Для серверов:
    - **TCP SYN-FIN Attack**: Enable
    - **TCP Blat**: Enable

### 13.9.2. Настройки портов (Port Setting)

Для включения/отключения защиты от DoS на конкретных портах перейдите:

**Security > DoS > Port Setting**



***Параметры настройки***

| Поле | Описание |
|---|---|
| **Port** | Номер порта или интерфейса. |
| **State** | Состояние защиты от DoS: |
| | **Enable** – активация защиты (применяются глобальные правила из раздела **13.9.1**). |
| | **Disable** – отключение защиты для порта. |

**Рекомендации по настройке**

1. **Обязательные порты для защиты**:
   - Порт uplink (подключение к вышестоящему оборудованию)
   - Серверные порты
   - Порт управления (если выделен)
2. **Порты для отключения защиты**:
   - Внутренние доверенные порты (например, между коммутаторами stack)
   - Порты с VoIP-телефонами (если возникают ложные срабатывания)

**Пример конфигурации**

1. **Активация защиты**:
   - Порт GE24 (uplink): **Enable**
   - Порт GE1-GE5 (серверы): **Enable**

2. **Отключение защиты**:
    - Порт GE10 (IP-телефон): **Disable** (если мешает работе)
    - Порт GE23-GE24 (межкоммутаторные соединения): **Disable**

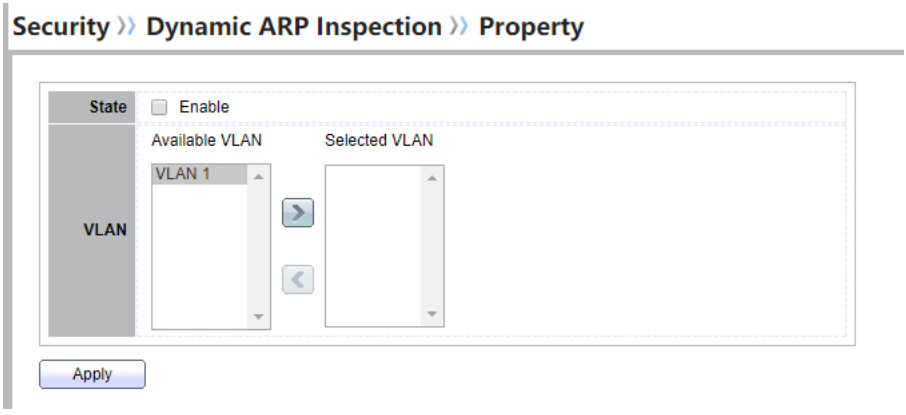
**Внимание!** После изменений проверьте доступность устройств на этих портах.

## 13.10. Dynamic ARP Inspection (DAI)

### 13.10.1. Глобальные настройки DAI (Property)

Для настройки защиты от ARP-спуфинга перейдите:

**Security > Dynamic ARP Inspection > Property**



***Глобальные параметры DAI***

| Параметр | Описание |
|---|---|
| **State** | Включение/отключение DAI на устройстве |
| **VLAN** | Выбор VLAN, в которых будет работать DAI (перемещение между боксами Available VLAN и Selected VLAN) |

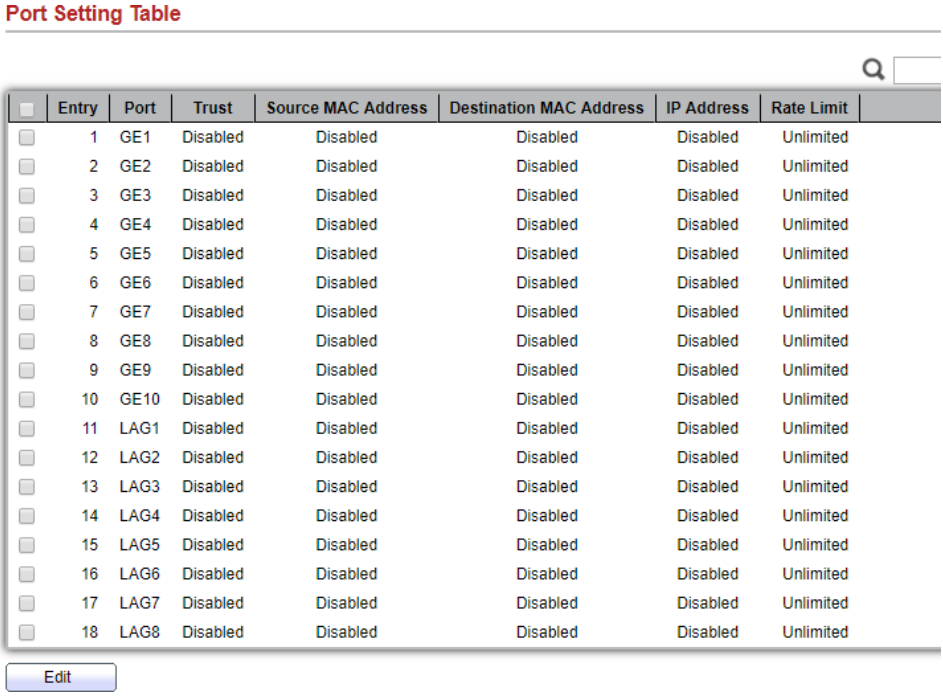
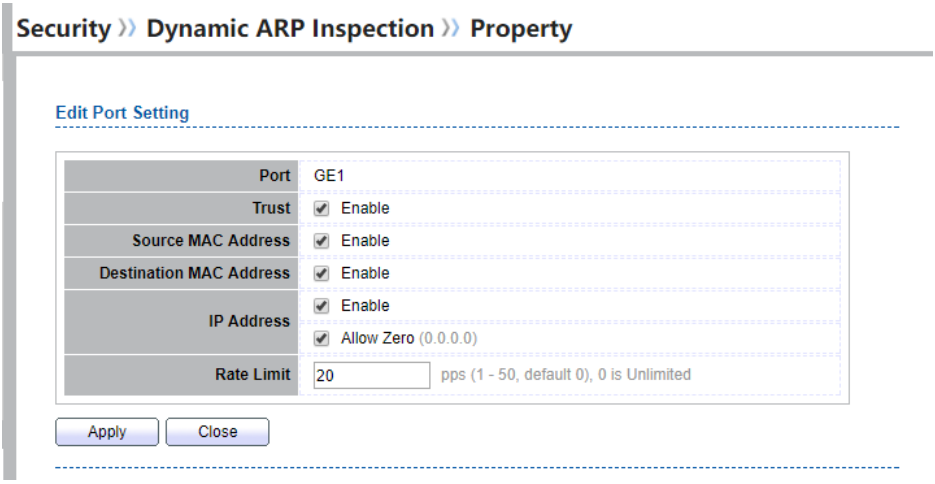


***Таблица DAI для портов***

| Параметр | Описание | Рекомендуемое значение |
|---|---|---|
| **Trust** | Доверенный порт (пропускает все ARP-пакеты без проверки) | Включить для портов маршрутизаторов |
| **Source MAC Validation** | Проверка соответствия MAC отправителя в ARP и Ethernet-заголовке | Включить |
| **Destination MAC Validation** | Проверка MAC получателя в ARP-пакетах | Включить |
| **IP Address Validation** | Проверка IP-адресов (блокировка 0.0.0.0, 255.255.255.255 и multicast) | Включить |
| **Allow Zero** | Разрешение IP 0.0.0.0 (требуется для некоторых VoIP-устройств) | Отключить |
| **Rate Limit** | Лимит ARP-пакетов в секунду (0 = без лимита) | 15-30 pps |




***Настройка портов для DAI***

| Параметр | Описание |
|---|---|
| **Port** | Номер порта |
| **Trust** | Доверенный порт (пропускает все ARP-пакеты без проверки)<br>**Enable** – включить. |
| **Source MAC Validation** | Проверка соответствия MAC отправителя в ARP и Ethernet-заголовке<br>**Enable** – включить. |
| **Destination MAC Validation** | Проверка MAC получателя в ARP-пакетах<br>**Enable** – включить. |

| Параметр | Описание |
|---|---|
| **IP Address** | Проверка IP-адресов (блокировка 0.0.0.0, 255.255.255.255 и multicast)<br>**Enable** – включить. |
| **Allow Zero** | Разрешение IP 0.0.0.0 (требуется для некоторых VoIP-устройств)<br>**Enable** – включить. |
| **Rate Limit** | Лимит ARP-пакетов в секунду (0 = без лимита) От 1 до 50. |

**Рекомендации**

1. **Обязательные настройки**:
   - Включите **IP/MAC Validation** для всех пользовательских портов.
   - Для uplink-портов активируйте **Trust**.
2. **VoIP-оборудование**:
   - Если устройства используют 0.0.0.0, включите **Allow Zero** только для их портов.
3. **Защита от флуда**:
   - Установите **Rate Limit = 30 pps** для пользовательских портов.

**Пример конфигурации**

1. **VLAN**:
    - Активируйте DAI для VLAN 10 (пользователи) и VLAN 20 (серверы).
2. **Порт GE24 (маршрутизатор)**:
    - **Trust**: Enable
    - **Rate Limit**: 0
3. **Порт GE1 (компьютер)**:
    - **Source/Destination MAC Validation**: Enable
    - **Rate Limit**: 30

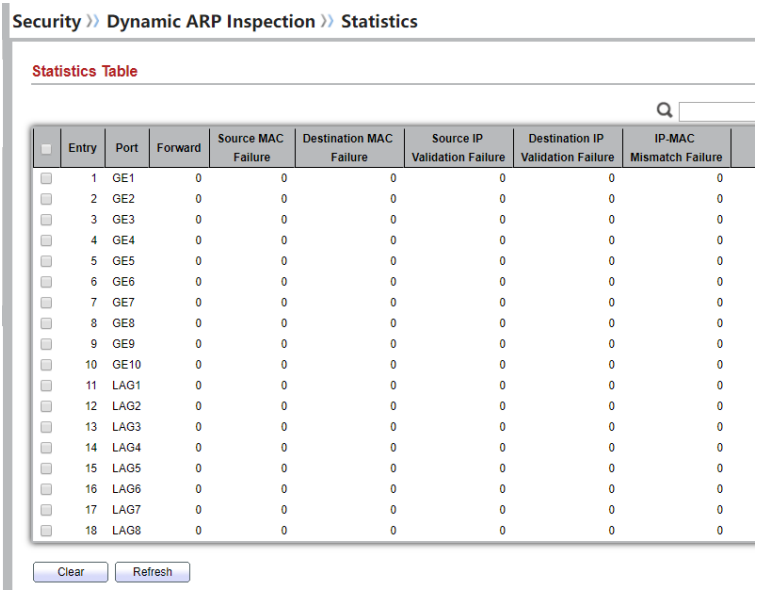
**Внимание!** DAI требует предварительной настройки **DHCP Snooping** для работы с динамическими IP.

### 13.10.2. Статистика работы DAI (Statistics)

Для просмотра статистики работы Dynamic ARP Inspection (DAI) перейдите:

**Security > Dynamic ARP Inspection > Statistics**

На этой странице отображаются данные о работе функции защиты от ARP-спуфинга.




***Параметры статистики***

| Параметр | Описание |
|---|---|
| **Entry** | Номер записи |
| **Port** | Идентификатор порта |
| **Forwarded** | Количество корректных ARP-пакетов, пропущенных системой |
| **Source MAC Failures** | Количество пакетов, заблокированных из-за несоответствия MAC-адреса отправителя (в ARP и Ethernet-заголовке) |
| **Destination MAC** | Количество пакетов, заблокированных из-за |

| Параметр | Описание |
|---|---|
| **Failures** | несоответствия MAC-адреса получателя |
| **Source IP Validation Failures** | Количество пакетов, заблокированных из-за невалидного IP-адреса отправителя (0.0.0.0, multicast и т.д.) |
| **Destination IP Validation Failures** | Количество пакетов, заблокированных из-за невалидного IP-адреса получателя |
| **IP-MAC Mismatch Failures** | Количество пакетов, заблокированных из-за несоответствия IP и MAC в таблице IP Source Guard |

**Анализ статистики**

1. **Нормальная работа**:
   - **Forwarded** > 0, остальные счетчики = 0 или минимальны.
2. **Проблемные ситуации**:
   - Высокие значения **Source MAC Failures** – возможен ARP-спуфинг.
   - **IP-MAC Mismatch** > 0 – несоответствие IP и MAC в сети (проверьте настройки DHCP).
3. **Действия**:
   - При частых блокировках проверьте:
     - Корректность настроек **Trust**-портов
     - Работу легитимных сервисов (например, VoIP)

**Пример использования**

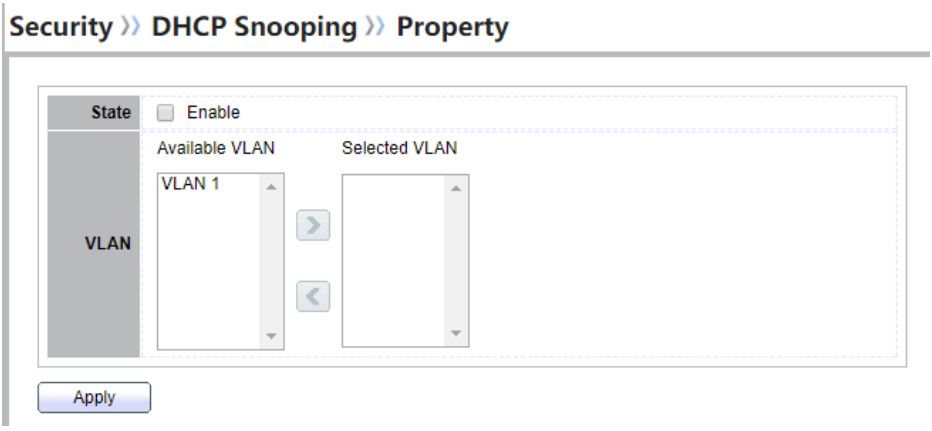
1. **Порт GE1**:
    - **Forwarded**: 1500
    - **Source MAC Failures**: 2 (норма)
2. **Порт GE5**:
    - **IP-MAC Mismatch Failures**: 50 – требуется проверка подключенного устройства.

## 13.11. DHCP Snooping

### 13.11.1. Глобальные настройки (Property)

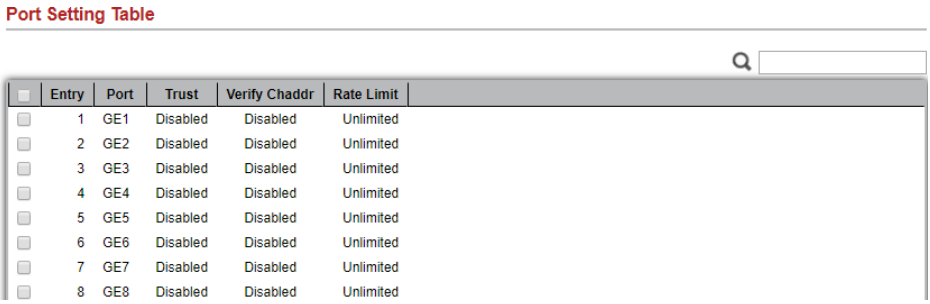
Для защиты от DHCP-атак перейдите:

**Security > DHCP Snooping > Property**



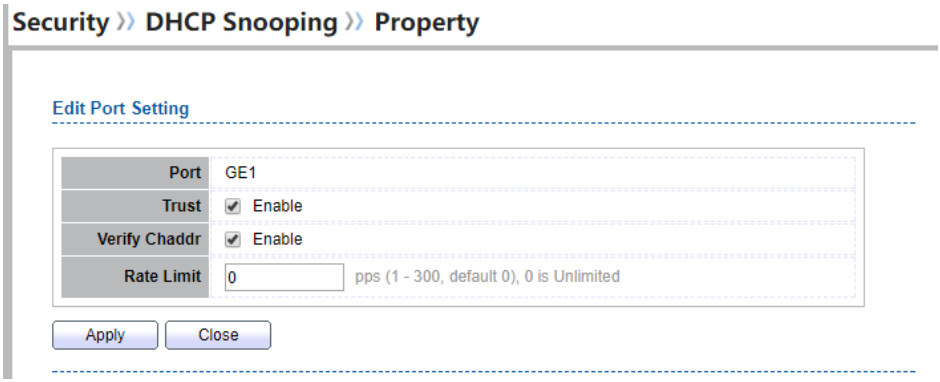
### *Глобальные параметры*

| Параметр | Описание |
|---|---|
| **State** | Включение/отключение DHCP Snooping |
| **VLAN** | Выбор VLAN для мониторинга (перемещение между боксами Available VLAN и Selected VLAN) |




### *Таблица портов с настройкой DHCP Snooping*

| Параметр | Описание |
|---|---|
| **Trust** | Доверенный порт (пропускает DHCP-серверы) |
| **Verify Chaddr** | Проверка соответствия MAC в DHCP и Ethernet-заголовке |
| **Rate Limit** | Лимит DHCP-пакетов (0 = без ограничений) |




***Настройки портов для DHCP Snooping***

| Параметр | Описание | Рекомендации |
|---|---|---|
| **Trust** | Доверенный порт (пропускает DHCP-серверы) | Включить для портов легитимных DHCP-серверов |
| **Verify Chaddr** | Проверка соответствия MAC в DHCP и Ethernet-заголовке | Включить для пользовательских портов |
| **Rate Limit** | Лимит DHCP-пакетов (0 = без ограничений) | 30-100 pps для пользовательских портов |

**Рекомендации**

1. **Обязательная настройка** для работы:
   - Dynamic ARP Inspection (раздел **13.10**)
   - IP Source Guard

2. **Правила применения**:

   - **Trust** включается ТОЛЬКО для портов DHCP-серверов
   - **Verify Chaddr** блокирует подмену MAC в DHCP-запросах

**Пример конфигурации**

- VLAN 10: DHCP Snooping включен
- Порт GE24 (DHCP-сервер): Trust=Enable, Rate Limit=0
- Порт GE1: Verify Chaddr=Enable, Rate Limit=30

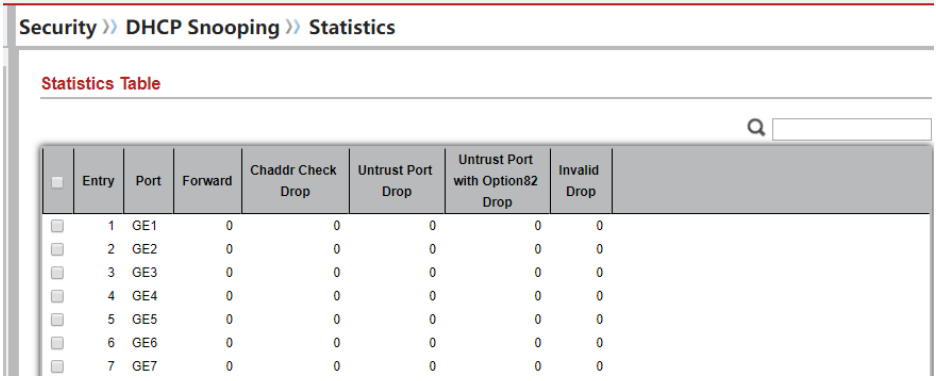
**Внимание!** После включения DHCP Snooping клиенты получают IP только от доверенных серверов.

### 13.11.2. Статистика работы DHCP Snooping (Statistics)

Для просмотра статистики работы **DHCP Snooping** перейдите:

**Security > DHCP Snooping > Statistics**

На этой странице  WEB интерфейса отображаются данные о работе защиты от неавторизованных DHCP-серверов и подмены MAC-адресов.



***Параметры статистики***

| Параметр | Описание |
|---|---|
| **Port** | Идентификатор порта |
| **Forwarded** | Количество корректных DHCP-пакетов, пропущенных коммутатором |
| **Chaddr Check Drop** | Количество пакетов, заблокированных из-за несоответствия MAC в DHCP-запросе (chaddr) и Ethernet-заголовке |
| **Untrusted Port Drop** | Количество DHCP-ответов, заблокированных на **недоверенных** портах (попытка работы неавторизованного DHCP-сервера) |
| **Untrusted Port with Option82 Drop** | Количество пакетов с Option 82, заблокированных на недоверенных портах |
| **Invalid Drop** | Количество пакетов, заблокированных из-за других ошибок (некорректный формат, неверные поля и т.д.) |

**Анализ статистики**

1. **Нормальная работа**:
   - **Forwarded** > 0, остальные счетчики = 0 или минимальны.
2. **Проблемные ситуации**:

- **Untrusted Port Drop** > 0 – попытка подключения неавторизованного DHCP-сервера.
- **Chaddr Check Drop** > 0 – возможна подмена MAC-адресов в сети.

3. **Действия**:
   - При высоких значениях **Untrusted Port Drop** проверьте подключение сетевых устройств к портам.
   - Если **Invalid Drop** растет – возможны проблемы с легитимными DHCP-запросами (например, от VoIP-устройств).

**Пример использования**

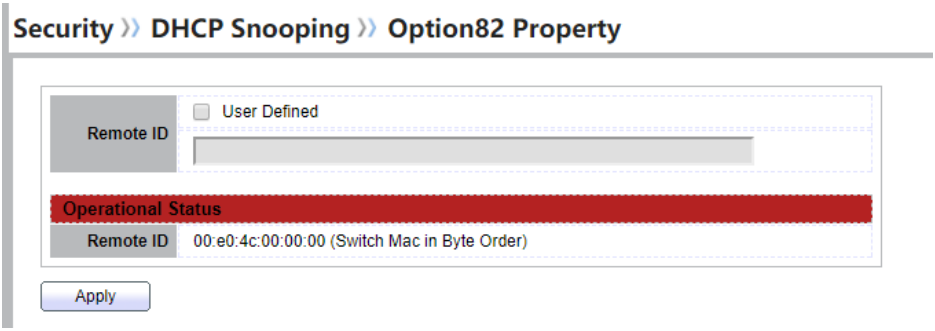
1. **Порт GE1**:
   - **Forwarded**: 500
   - **Untrusted Port Drop**: 0 (норма)
2. **Порт GE5**:
   - **Untrusted Port Drop**: 10 – обнаружен неавторизованный DHCP-сервер.

### 13.11.3. Настройка Option 82 (Option82 Property)

Option 82 помогает идентифицировать источник DHCP-запросов в распределенных сетях.

Для конфигурации DHCP Option 82 перейдите:

**Security > DHCP Snooping > Option82 Property**




***Глобальные настройки Option 82***

| Параметр | Описание |
|---|---|
| **User Defined** | Включение Remote-ID, определяемого администратором (по умолчанию используется MAC коммутатора) |
| **Remote ID** | Пользовательский идентификатор (до 63 символов) |

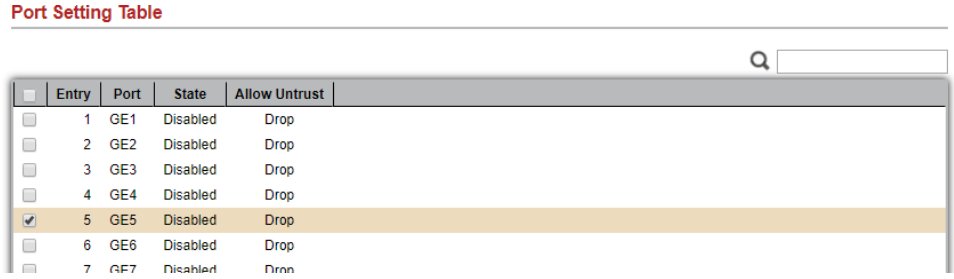
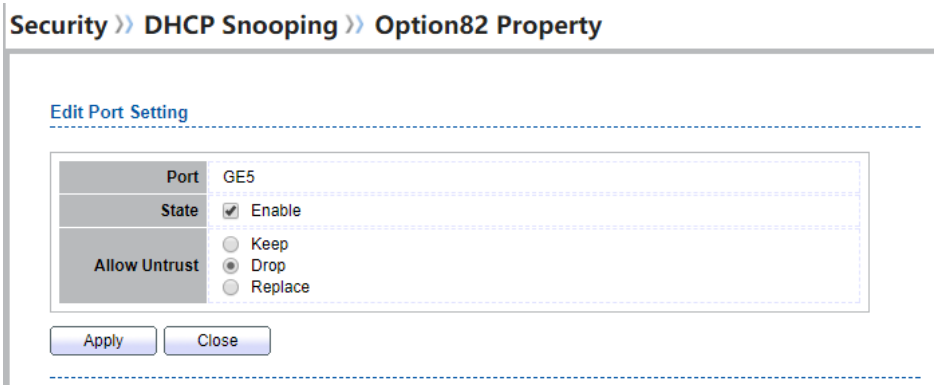


***Таблица с настройками Option 82 на портах***

| Параметр | Описание |
|---|---|
| **State** | Включение Option 82 на порту<br>**Enable** – включить<br>**Disable** – выключить |
| **Allow Untrusted** | Действие для Option 82 на недоверенных портах:<br>**Keep** – оставить оригинальный Option 82<br>**Replace** – заменить на данные коммутатора<br>**Drop** – блокировать пакеты |




***Настройка Option 82 на портах***

| Параметр | Описание |
|---|---|
| **State** | Включение Option 82 на порту |

| Параметр | Описание |
|---|---|
| | **Enable** – включить<br>**Disable** – выключить |
| **Allow Untrusted** | Действие для Option 82 на недоверенных портах:<br>**Keep** – оставить оригинальный Option 82<br>**Replace** – заменить на данные коммутатора<br>**Drop** – блокировать пакеты |

**Рекомендации**

1. **Типовые сценарии**:
   - **Keep**: Для доверенных портов с VoIP-устройствами
   - **Replace**: Для пользовательских портов (унификация данных)
   - **Drop**: Для строгой безопасности
2. **Формат Remote-ID**:
   - Используйте понятные идентификаторы (например, `Floor1-Switch3`)

**Пример настройки**:

- User Defined: Enable
- Remote ID: "BuildingA-Switch1"
- Порт 1/0/1: State=Enable, Allow Untrusted=Replace
- Порт 1/0/24: State=Disable

### 13.11.4. Настройка Circuit ID в Option 82 (Option 82 Circuit ID)

Для настройки **Circuit ID** в DHCP Option 82 перейдите:

**Security > DHCP Snooping > Option82 Circuit ID**

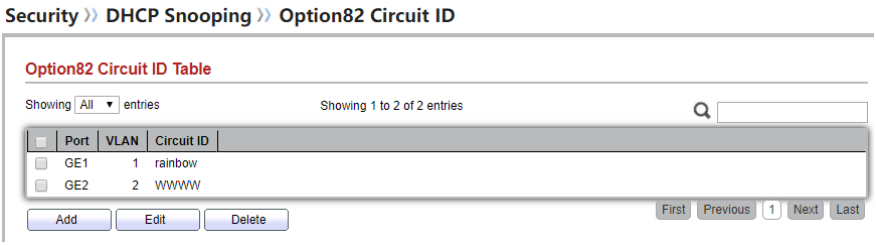
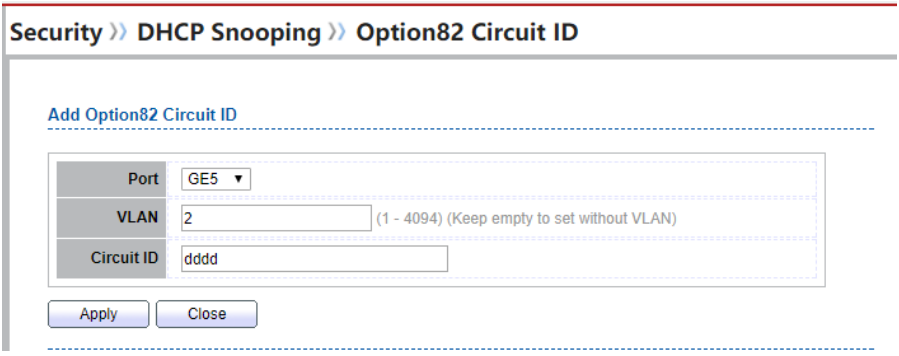
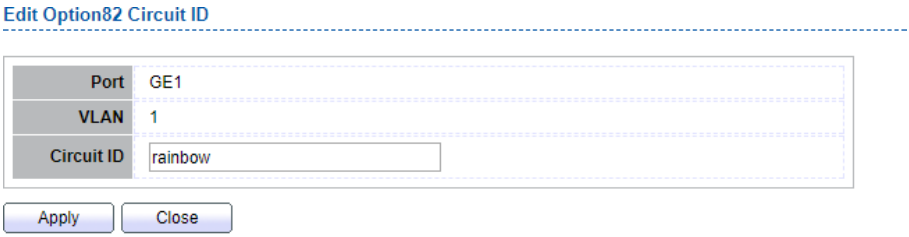



***Таблица настроек Circuit ID***

| Параметр | Описание |
|---|---|
| **Port** | Порт, к которому применено правило |
| **VLAN** | VLAN (опционально) |
| **Circuit ID** | Заданный идентификатор **Circuit ID** |






***Добавление/редактирование Circuit ID***

| Параметр | Описание |
|---|---|
| **Port** | Выбор порта (только при добавлении) |
| **VLAN** | VLAN ID (необязательно) |
| **Circuit ID** | Уникальный идентификатор **Circuit ID** (строка) |

**Рекомендации**

1. **Назначение**:
   - Идентификация физического расположения клиента (например, PortGE3-VLAN10).
   - Совместно с **Remote ID** (из раздела **13.11.3**) формирует полную информацию об агенте.
2. **Формат**:
   - Рекомендуется использовать понятные имена:

- Floor2-Room5-Port8
- SW1-Port24-VLAN20

**Пример настройки**:

- Порт: GE5
- VLAN: 10
- Circuit ID: "BuildingA-Floor1-Port5"

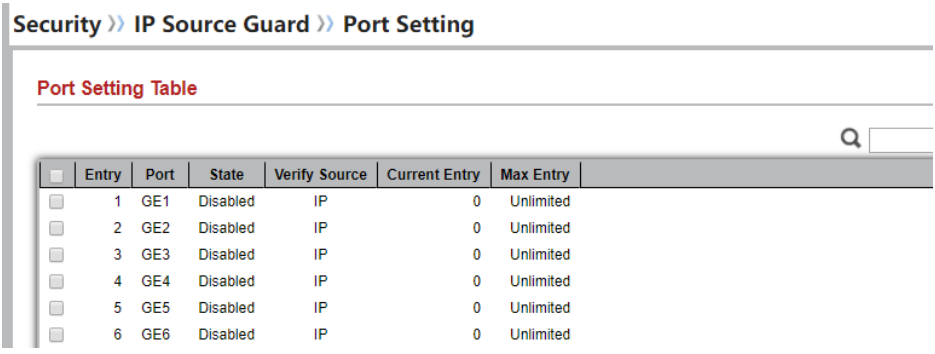
**Примечание:** Если VLAN не указан, Circuit ID применяется ко всем VLAN на порту.

## 13.12. IP Source Guard

### 13.12.1. Настройка портов (Port Setting)

Для защиты от IP-спуфинга перейдите:

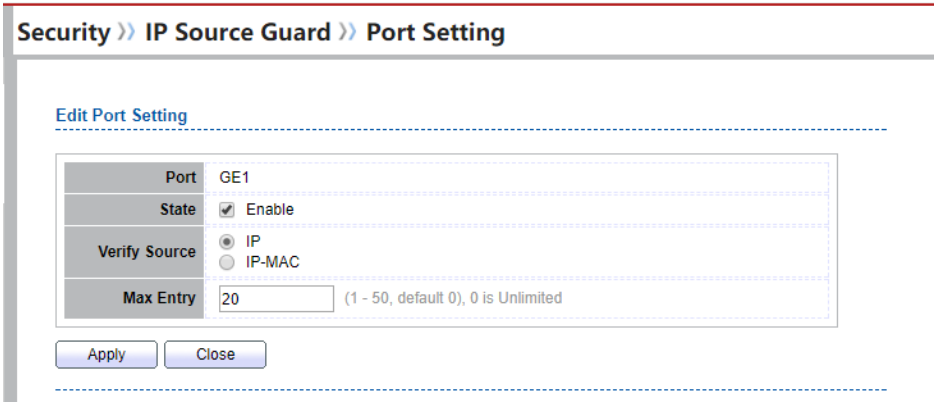
**Security > IP Source Guard > Port Setting**




***Параметры портов***

| Параметр | Описание |
|---|---|
| **Port** | Идентификатор порта |

| Параметр | Описание |
|---|---|
| **State** | Состояние IP Source Guard:<br>**Enable** – защита активна<br>**Disable** – отключена |
| **Verify Source** | Режим проверки:<br>**IP** – только IP-адрес<br>**IP-MAC** – IP и MAC-адрес |
| **Current Binding Entry** | Текущее количество привязок IP/MAC |
| **Max Binding Entry** | Максимальное число привязок (0 = без ограничений) |



***Редактирование настроек***

| Параметр | Описание |
|---|---|
| **Status** | Включение/отключение функции |
| **Verify Source** | Уровень проверки:<br>**IP** – базовая защита<br>**IP-MAC** – строгая проверка |
| **Max Binding Entry** | Лимит привязок |

**Примечания**

Для работы необходимы:

• **DHCP Snooping** (раздел 13.11)

• Статические привязки IP-MAC (если нет DHCP).

**Пример настройки**:

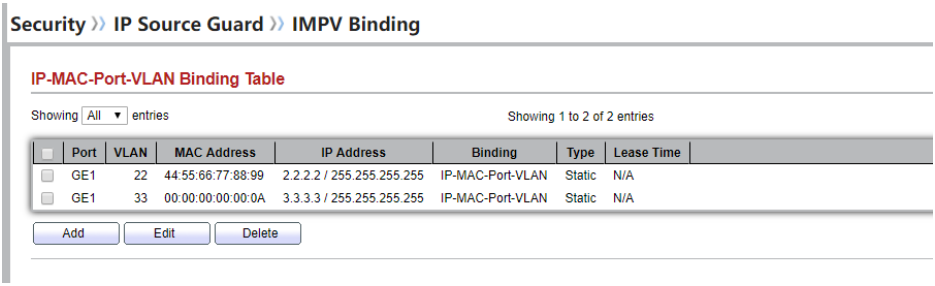
- Порт GE1: Verify Source: IP-MAC, Max Binding Entry: 2
- Порт GE10 (VoIP): Verify Source: IP, Max Binding Entry: 1

**Внимание!** При включенном **IP-MAC** режиме устройства со статическими IP требуют ручной привязки.

### 13.12.2. Таблица привязок IP/MAC адресов (IMPV Binding)

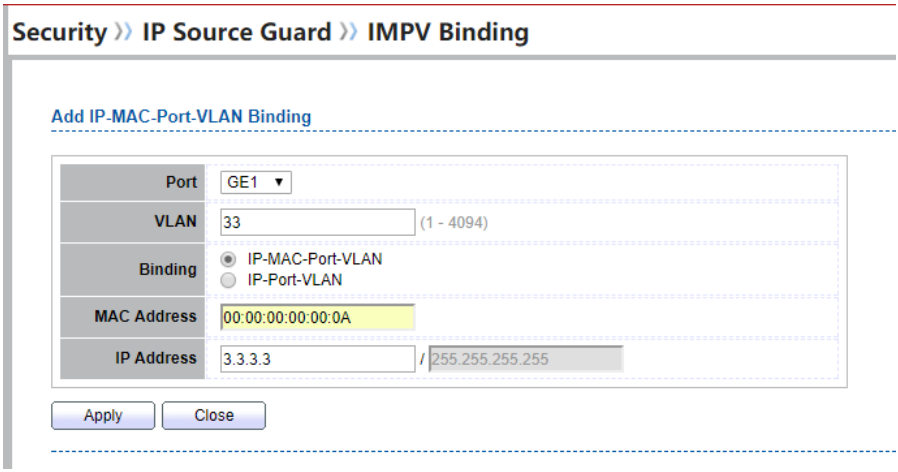
Для просмотра и управления привязками IP/MAC-адресов перейдите:

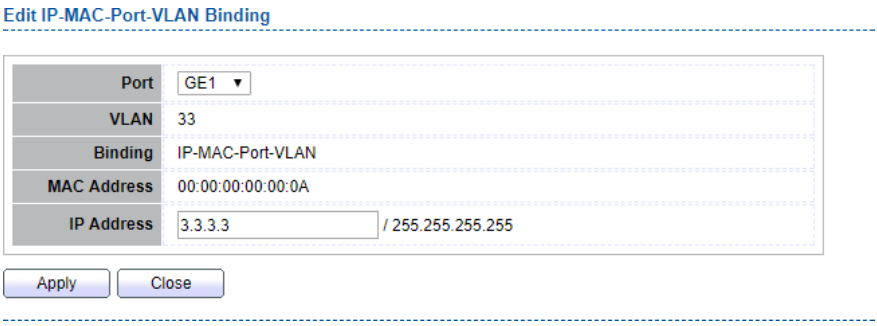
**Security > IP Source Guard > IMPV Binding**




***Просмотр существующих привязок***

| Параметр | Описание |
|---|---|
| **Port** | Порт привязки |
| **VLAN** | VLAN привязки |
| **MAC Address** | MAC-адрес устройства (только для IP-MAC-привязок) |
| **IP Address** | IP-адрес (маска всегда /32 для IP-MAC) |
| **Binding Type** | Тип привязки:<br>**Static** – создана вручную<br>**Dynamic** – получена через DHCP Snooping |
| **Lease Time** | Время жизни динамической записи (только для DHCP) |




***Добавление/редактирование привязок***

| Параметр | Описание |
|---|---|
| **Port** | Выбор порта |
| **VLAN** | Указание VLAN (опционально) |
| **Binding Mode** | Режим привязки:<br>**IP-MAC-Port-VLAN** – строгая привязка по |

| Параметр | Описание |
|---|---|
| | IP+MAC+порту+VLAN<br>**IP-Port-VLAN** – привязка только по IP |
| **MAC Address** | Ввод MAC-адреса (требуется для IP-MAC-Port-VLAN) |
| **IP Address/Mask** | Ввод IP-адреса и маски (маска только для IP-Port-VLAN) |

**Рекомендации**

1. **Для статических устройств** (серверы, принтеры):
   - Используйте **IP-MAC-Port-VLAN** с ручным вводом данных.
   - Пример:
     - Port: GE5, VLAN: 10
     - MAC: 00-1A-2B-3C-4D-5E, IP: 192.168.1.100
2. **Для динамических IP устройств**:
   - Привязки автоматически создаются через **DHCP Snooping** (тип **Dynamic**).
3. **Очистка**:
   - Динамические записи удаляются после прошествия времени, указанного в **Lease Time**.
   - Статические – только вручную.

**Пример использования**

1. **Проблема**: Устройство с статическим IP не работает.
   - Проверьте таблицу привязок:

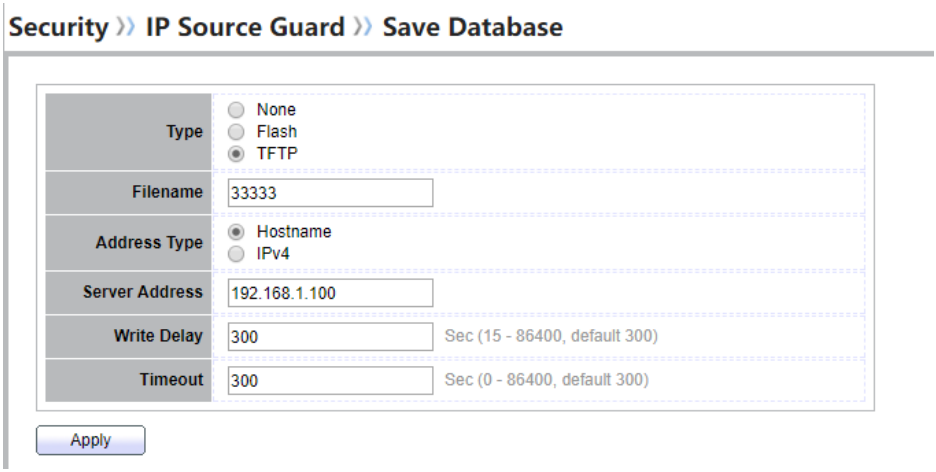
- Если записи нет – добавьте вручную.
- Если есть несоответствие MAC – исправьте.

2. **Для VoIP**:
   - Режим **IP-Port-VLAN** (без жесткой привязки MAC).

### 13.12.3. Сохранение базы данных (Save Database)

Для резервного копирования динамических привязок DHCP Snooping перейдите:

**Security > IP Source Guard > Save Database**



***Настройки сохранения записей в базу***

| Параметр | Описание |
|---|---|
| **Type** | Способ сохранения:<br>**None** – отключено<br>**Flash** – сохранение во внутреннюю память<br>**TFTP** – отправка на TFTP-сервер |
| **Filename** | Имя файла для резервной копии<br>Например: dhcp_bindings_backup.cfg |
| **Address Type** | Тип адреса TFTP-сервера (только для Type=TFTP)<br>**Hostname** – доменное имя<br>**IPv4** – IP-адрес |
| **Server Address** | Адрес TFTP-сервера<br>Например: 192.168.1.100 или tftp.example.com |
| **Write Delay** | Задержка перед сохранением (сек)<br>По умолчанию: 300. Диапазон от 15 до 86400 |
| **Timeout** | Таймаут операции (сек)<br>По умолчанию: 300. Диапазон от 15 до 86400 |

**Рекомендации**

1. **Для надежности**:
   - Используйте **TFTP** с указанием сервера.
   - Пример настроек:

- Type: TFTP
- Filename: dhcp_bindings_$(date).cfg
- Address Type: IPv4
- Server Address: 192.168.1.100

2. **Для локального хранения**:
   - **Type**: Flash
   - **Filename**: backup_dhcp_bindings.cfg
3. **Автоматизация**:
   - При **Write Delay=300** изменения сохраняются каждые 5 минут.

# 14. ACL (Access Control List)

## 14.1. MAC ACL (ACL на основе MAC-адресов)

Для создания и управления ACL на уровне MAC-адресов перейдите:

**ACL > MAC ACL**


***Создание ACL***

| Параметр | Описание |
|---|---|
| **ACL Name** | Уникальное имя ACL (до 32 символов).<br>Пример: BLOCK_UNAUTHORIZED_MAC |

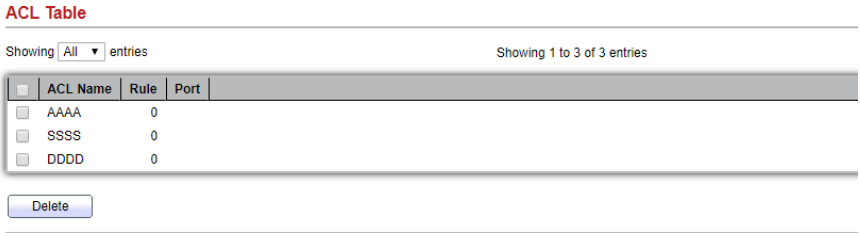



***Таблица существующих ACL***

| Параметр | Описание |
|---|---|
| **ACL Name** | Имя созданного ACL |
| **Rule** | Количество правил (ACE) в ACL |
| **Port** | Список портов, к которым применен ACL |

**Применение**:

- Блокировка устройств по MAC-адресу.
- Ограничение доступа к портам.

**Пример**:

1. Введите имя ACL (например, GUEST_RESTRICTION).
2. Нажмите **Apply** (принять)
3. Перейдите в раздел **MAC ACE** (**14.2**) для добавления правил.

**Внимание!** Удаление ACL возможно только если он не привязан к портам.

## 14.2. MAC ACE (Правила ACL для MAC-адресов)

Для настройки правил фильтрации трафика на уровне MAC-адресов перейдите:

**ACL > MAC ACE**

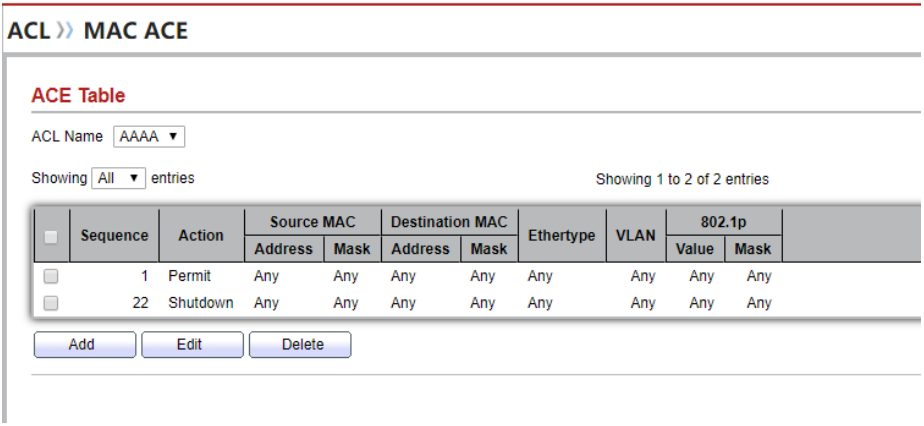
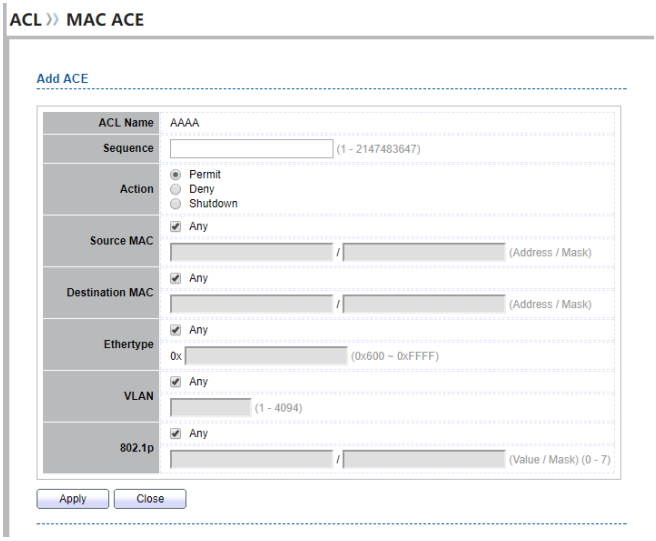


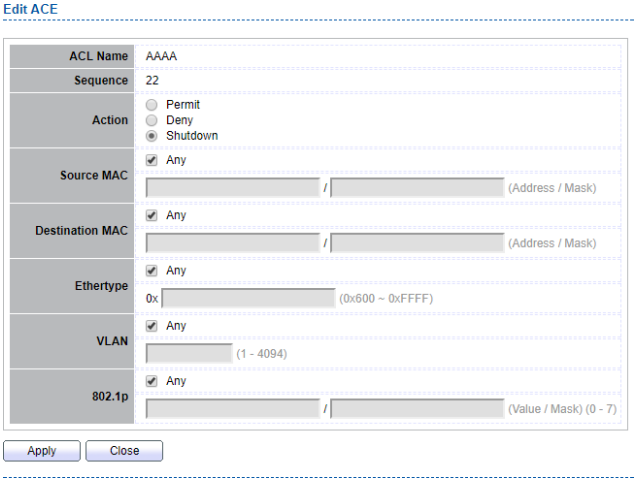

***Таблица правил MAC ACE***

| Параметр | Описание |
|---|---|
| **ACL Name** | Выбор ACL, к которому добавляется правило |
| **Showing** | Показывать все записи в таблице или часть записей. |
| **Sequence** | Приоритет правила (1 – наивысший). Правила обрабатываются по возрастанию. |
| **Action** | Действие: |

| Параметр | Описание |
|---|---|
| | **Permit** – разрешить трафик |
| | **Deny** – заблокировать трафик |
| | **Shutdown** – заблокировать трафик и отключить порт |
| **Source MAC** | Фильтр по MAC-адресу отправителя: |
| | **Any** – любые адреса |
| | **User Defined** – конкретный MAC или диапазон |
| **Destination MAC** | Фильтр по MAC-адресу получателя (аналогично Source MAC)<br>**Any** – любые адреса<br>**User Defined** – конкретный MAC или диапазон |
| **Ethertype** | Тип Ethernet-фрейма (например, `0x0800` для IPv4, `0x86DD` для IPv6)<br>**Any** – любой тип<br>Или 0x0800 для IPv4, 0x86DD для IPv6 |
| **VLAN ID** | Фильтр по VLAN ID<br>**Any** – любой VLAN<br>или **VLAN ID** |
| **802.1p Value** | Приоритет QoS (0-7) |

| Параметр | Описание |
|---|---|
| | **0-7** – приоритет от 0 до 7<br>**Any** – любой приоритет |



***Настройка правил MAC ACE***

| Параметр | Описание |
|---|---|
| **ACL Name** | Выбор ACL, к которому добавляется правило |
| **Sequence** | Приоритет правила (1 – наивысший). Правила обрабатываются по возрастанию. |
| **Action** | Действие: |
| | **Permit** – разрешить трафик |
| | **Deny** – заблокировать трафик |
| | **Shutdown** – заблокировать трафик и отключить порт |
| **Source MAC** | Фильтр по MAC-адресу отправителя: |
| | **Any** – любые адреса |
| | **User Defined** – конкретный MAC или диапазон (с маской, например 00:1A:2B:00:00:00/FF:FF:FF:00:00:00) |
| **Destination MAC** | Фильтр по MAC-адресу получателя (аналогично Source MAC) |
| **Ethertype** | Тип Ethernet-фрейма (например, 0x0800 для IPv4, 0x86DD для IPv6) |
| **VLAN ID** | Фильтр по VLAN ID (номер 1-4094 или **Any**) |

| Параметр | Описание |
|---|---|
| **802.1p Value** | Приоритет QoS (0-7). Маска указывает биты для проверки (например, маска 0x7 проверяет все 3 бита). |

**Примеры настройки**

1. **Блокировка устройства по MAC**:
   - **Action**: Deny
   - **Source MAC**: User Defined (00:1A:2B:3C:4D:5E/FF:FF:FF:FF:FF:FF)
   - **Destination MAC**: Any
2. **Разрешение только VoIP-трафика (VLAN 100, 802.1p=5)**:
   - **Action**: Permit
   - **Ethertype**: User Defined (0x0800)
   - **VLAN ID**: User Defined (100)
   - **802.1p Value**: User Defined (5, маска 0x7)
3. **Защита от спама (широковещательный трафик)**:
   - **Action**: Deny
   - **Destination MAC**: User Defined (FF:FF:FF:FF:FF:FF/FF:FF:FF:FF:FF:FF)

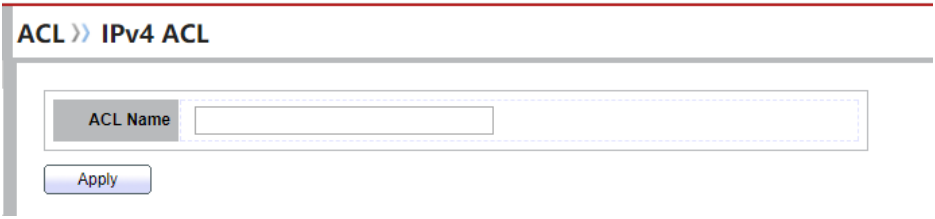
**Внимание!**

- Правила нельзя изменить/удалить, если ACL привязан к порту.

## 14.3. IPv4 ACL (Access Control List для IPv4)

Для создания и управления ACL на уровне IPv4-адресов перейдите:

**ACL > IPv4 ACL**




***Создание IPv4 ACL***

| Параметр | Описание |
|---|---|
| **ACL Name** | Уникальное имя ACL (до 32 символов).<br>Пример: BLOCK_UNAUTHORIZED_IP |

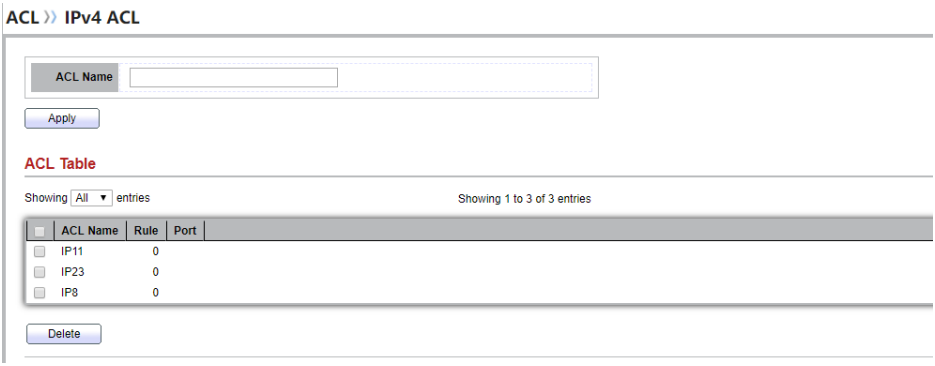


***Таблица существующих IPv4 ACL***

| Параметр | Описание |
|---|---|
| **ACL Name** | Имя созданного ACL |
| **Rule** | Количество правил (ACE) в ACL |
| **Port** | Список портов, к которым применен ACL |

**Применение**:

- Фильтрация трафика по IP-адресам/подсетям.
- Ограничение доступа к сервисам (например, веб-интерфейсу).

**Пример создания**:

1. Введите имя ACL (например, RESTRICT_WEB_ACCESS).
2. Нажмите **Apply** (принять)**.**
3. Перейдите в раздел **IPv4 ACE** (**14.4**) для добавления правил.

**Внимание!**

- Удаление ACL возможно только если он не привязан к портам.
- Для правил с масками используйте CIDR-формат (192.168.1.0/24).

## 14.4. IPv4 ACE (Правила ACL для IPv4)

Для настройки правил фильтрации IPv4-трафика перейдите:

**ACL → IPv4 ACE**

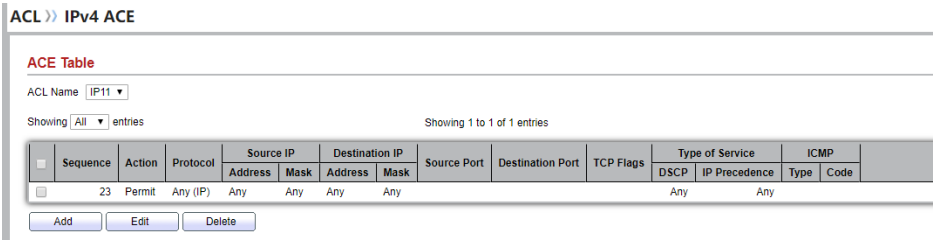
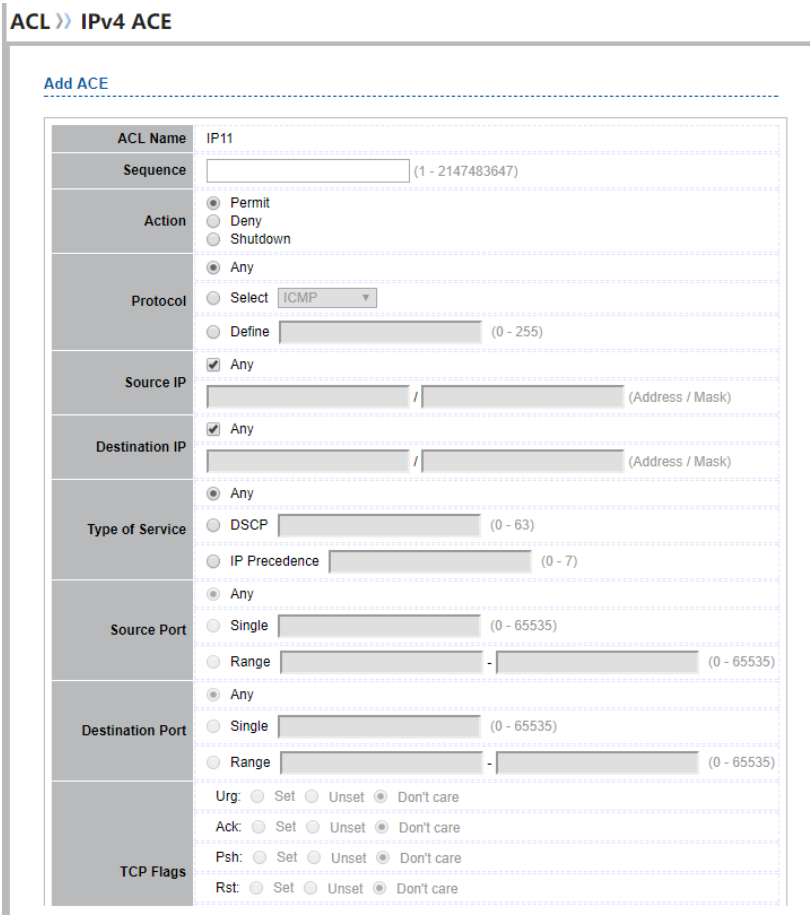


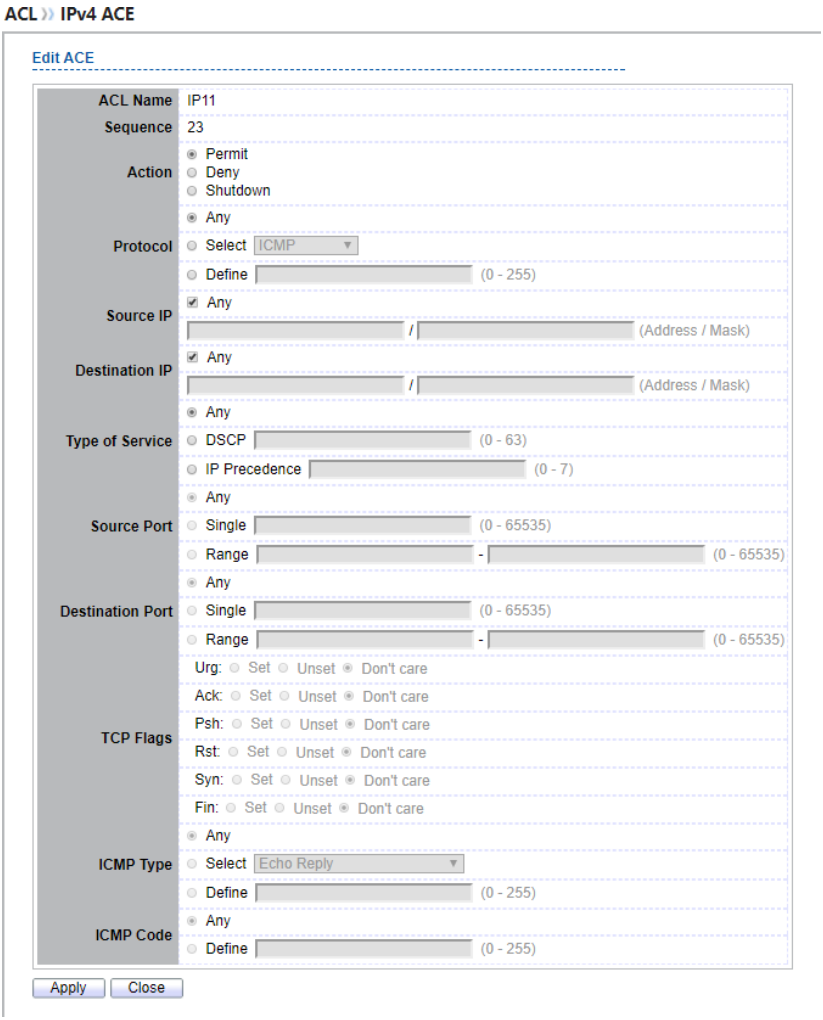

***Таблица правил IPv4 ACE***

| Параметр | Описание |
|---|---|
| **ACL Name** | Выбор ACL, к которому добавляется правило |
| **Sequence** | Приоритет (1 – наивысший). Правила обрабатываются по возрастанию. |
| **Action** | Действие: |
| | **Permit** – разрешить трафик |
| | **Deny** – заблокировать трафик |
| | **Shutdown** – заблокировать трафик и отключить порт |
| **Protocol** | Протокол: |
| | **Any** – все протоколы |

| Параметр | Описание |
|---|---|
| | **TCP/UDP/ICMP** и др. – конкретный протокол |
| | **Protocol ID** – номер протокола (например, 47 для GRE) |
| **Source IP** | IP-адрес отправителя: |
| | **Any** – любые адреса |
| | **User Defined** – конкретный IP/подсеть (например, 192.168.1.0/24) |
| **Destination IP** | IP-адрес получателя.<br>**Any** – любые адреса<br>**User Defined** – конкретный MAC или диапазон |
| **Source Port** | Порт отправителя (только для TCP/UDP): |
| | **Any** – все порты |
| | **Single** – один порт |
| | **Range** – диапазон портов |
| **Destination Port** | Порт получателя (аналогично Source Port)<br>**Any** – все порты<br>**Single** – один порт<br>**Range** – диапазон портов |
| **TCP Flags** | Флаги TCP (только для протокола TCP): SYN, ACK, FIN и др. |
| **Type of Service** | Приоритет трафика: |
| | **DSCP** (0-63) |

| Параметр | Описание |
|---|---|
| | **IP Precedence** (0-7) |
| **ICMP Type/Code** | Тип и код ICMP (только для ICMP): |
| | **Echo Request** (8/0) |
| | **Destination Unreachable** (3/1) |






***Настройка правил IPv4 ACE***

| Параметр | Описание |
|---|---|
| **ACL Name** | Выбор ACL, к которому добавляется правило |
| **Sequence** | Приоритет (1 – наивысший). Правила обрабатываются по возрастанию. |

| Параметр | Описание |
|---|---|
| **Action** | Действие: |
| | **Permit** – разрешить трафик |
| | **Deny** – заблокировать трафик |
| | **Shutdown** – заблокировать трафик и отключить порт |
| **Protocol** | Протокол: |
| | **Any** – все протоколы |
| | **SELECT** (выбор)**. TCP/UDP/ICMP** и др. – конкретный протокол |
| | **DEFINE** (определенный протокол) **Protocol ID** – номер протокола (например, 47 для GRE) 0- 255 |
| **Source IP** | IP-адрес отправителя: |
| | **Any** – любые адреса |
| | **User Defined** – конкретный IP/подсеть (например, 192.168.1.0/24) |
| **Destination IP** | IP-адрес получателя (аналогично Source IP) |
| **Type of Service** | Приоритет трафика:<br>**DSCP** (0-63)<br>**IP Precedence** (0-7) |
| **Source Port** | Порт отправителя (только для TCP/UDP): |
| | **Any** – все порты |

| Параметр | Описание |
|---|---|
| | **Single** – один порт (например, 80 для HTTP) |
| | **Range** – диапазон портов (например, 5000-6000) |
| **Destination Port** | Порт получателя (аналогично Source Port) |
| **TCP Flags** | Флаги TCP (только для TCP): SYN, ACK, FIN и др. |
| **ICMP Type** | Тип ICMP (только для ICMP): |
| | **Echo Request** (8/0) |
| | **Destination Unreachable** (3/1) |
| | **Define** – определенный (0-255) |
| **ICMP Code** | Код ICMP<br>**Any** – любой<br>**Define** – определенный (0-255) |

**Примеры настройки**

1. **Блокировка доступа к WEB-интерфейсу**:
    - **Action**: Deny
    - **Protocol**: TCP
    - **Destination Port**: 80 (HTTP), 443 (HTTPS)
    - **Source IP**: Any
2. **Разрешение только ICMP Ping**:
    - **Action**: Permit
    - **Protocol**: ICMP

- **ICMP Type**: Echo Request (8)
- **ICMP Code**: 0

3. **Защита от SYN-флуда**:
    - **Action**: Deny
    - **Protocol**: TCP
    - **TCP Flags**: SYN
    - **Destination Port**: Any

**Внимание!**

- Для правил с **Shutdown** порт включается вручную в **Port Settings**.
- Порядок правил критичен: первое совпадение определяет действие.

## 14.5. IPv6 ACL (Access Control List для IPv6)

Для создания и управления ACL на уровне IPv6-адресов перейдите:

**ACL > IPv6 ACL**

***Создание IPv6 ACL***

| Параметр | Описание |
|---|---|
| **ACL Name** | Уникальное имя ACL (до 32 символов) |

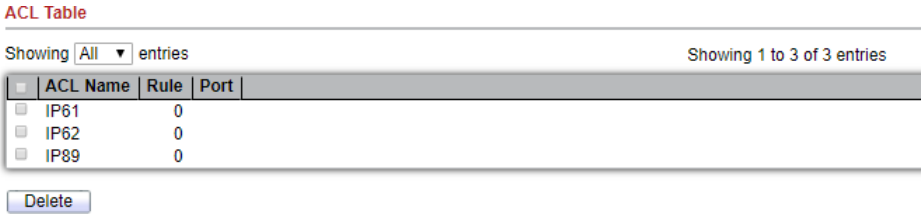



***Таблица существующих IPv6 ACL***

| Параметр | Описание |
|---|---|
| **ACL Name** | Имя созданного ACL |
| **Rule** | Количество правил (ACE) в ACL |
| **Port** | Список портов, к которым применен ACL |

**Ключевые особенности**

**Применение**:

- Фильтрация IPv6-трафика (например, блокировка служебных диапазонов fe80::/10 или ff00::/8).
- Ограничение доступа к сервисам.

**Пример создания**:

- Введите имя ACL (например, ALLOW_IPV6_HTTP).
- Нажмите **Apply** (принять).
- Перейдите в раздел **IPv6 ACE** (**14.6**) для добавления правил.

**Внимание!**

- Удаление ACL возможно только если он не привязан к портам.
- Для IPv6-префиксов используйте формат CIDR (например, 2001:db8::/32).

## 14.6. IPv6 ACE (Правила ACL для IPv6)

Для настройки правил фильтрации IPv6-трафика перейдите:

**ACL > IPv6 ACE**

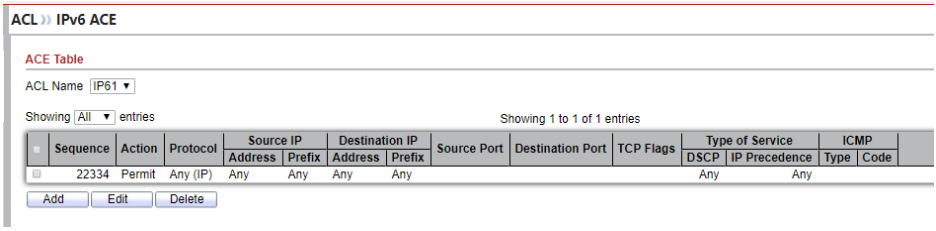
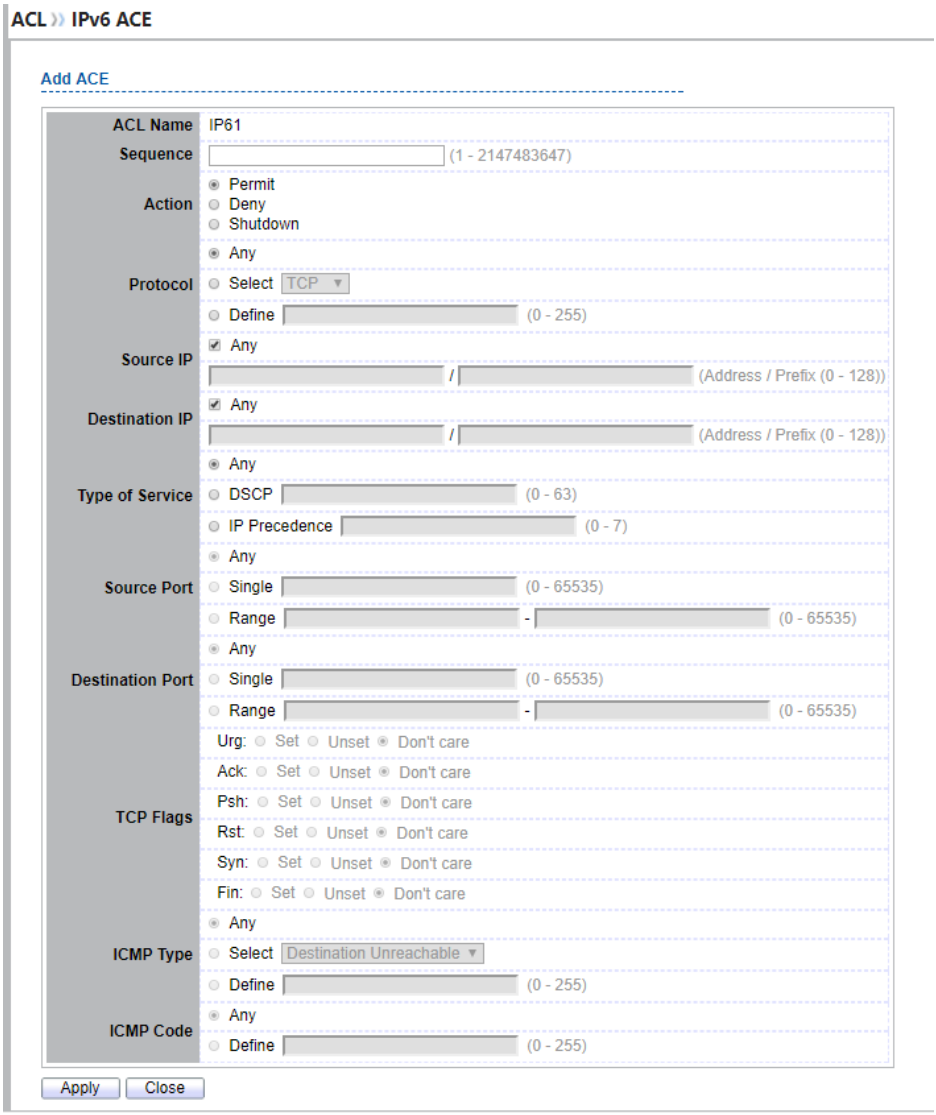


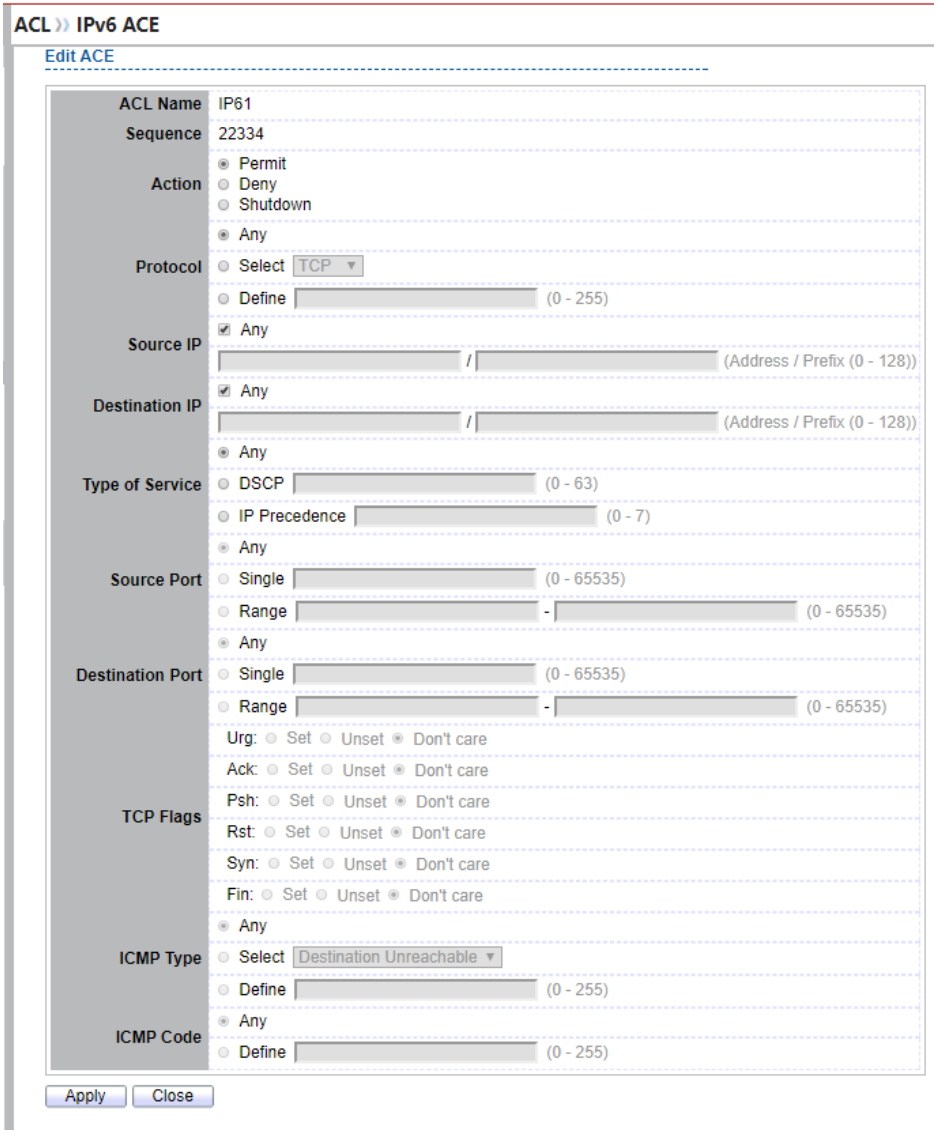

***Таблица правил IPv6 ACE***

| Параметр | Описание |
|---|---|
| **ACL Name** | Выбор ACL, к которому добавляется правило |
| **Sequence** | Приоритет (1 — наивысший). Правила |

| Параметр | Описание |
|---|---|
| | обрабатываются по возрастанию. |
| **Action** | Действие: |
| | **Permit** — разрешить трафик |
| | **Deny** — заблокировать трафик |
| | **Shutdown** — заблокировать трафик и отключить порт |
| **Protocol** | Протокол: |
| | **Any** — все протоколы |
| | **TCP/UDP/ICMPv6** — конкретный протокол |
| | **Protocol ID** — номер протокола (например, 58 для ICMPv6) |
| **Source IP** | IPv6-адрес отправителя: |
| | **Any** — любые адреса |
| | **User Defined** — конкретный IPv6/префикс (например, 2001:db8::/32) |
| **Destination IP** | IPv6-адрес получателя (аналогично Source IP)<br>**Any** – любые адреса<br>**User Defined** – конкретный IPv6/префикс |
| **Source Port** | Порт отправителя (только для TCP/UDP): |
| | **Any** — все порты |

| Параметр | Описание |
|---|---|
| | **Single** — один порт (например, 80 для HTTP) |
| | **Range** — диапазон портов (например, 5000-6000) |
| **Destination Port** | Порт получателя (аналогично Source Port)<br>**Any** – все порты<br>**Single** – один порт<br>**Range** – диапазон портов |
| **TCP Flags** | Флаги TCP (только для TCP): SYN, ACK, FIN и др. |
| **Type of Service** | Приоритет трафика: |
| | **DSCP** (0-63) |
| | **IP Precedence** (0-7) |
| **ICMPv6 Type/Code** | Тип и код ICMPv6 (только для ICMPv6): |
| | **Echo Request** |
| | **Neighbor Solicitation** |





***Настройка правил IPv6 ACE***

| Параметр | Описание |
|---|---|
| **ACL Name** | Выбор ACL, к которому добавляется правило |
| **Sequence** | Приоритет (1 — наивысший). Правила обрабатываются по возрастанию. |
| **Action** | Действие: |
| | **Permit** — разрешить трафик |
| | **Deny** — заблокировать трафик |
| | **Shutdown** — заблокировать трафик и отключить порт |
| **Protocol** | Протокол: |
| | **Any** — все протоколы |
| | **Select (выбор)** – **TCP/UDP/ICMPv6** (конкретный протокол) |
| | **Protocol ID** — номер протокола (например, 58 для ICMPv6) От 0 до 255 |
| **Source IP** | IPv6-адрес отправителя: |
| | **Any** — любые адреса |
| | **User Defined** — конкретный IPv6/префикс (например, 2001:db8::/32) |
| **Destination IP** | IPv6-адрес получателя (аналогично Source IP)<br>**Any** – любые адреса<br>**User Defined** – конкретный IPv6/префикс |

| Параметр | Описание |
|---|---|
| **Type of Service** | Приоритет трафика: |
| | **DSCP** (0-63) |
| | **IP Precedence** (0-7) |
| **Source Port** | Порт отправителя (только для TCP/UDP): |
| | **Any** — все порты |
| | **Single** — один порт (например, 80 для HTTP) |
| | **Range** — диапазон портов (например, 5000-6000) |
| **Destination Port** | Порт получателя (аналогично Source Port)<br>**Any** – все порты<br>**Single** – один порт<br>**Range** – диапазон портов |
| **TCP Flags** | Флаги TCP (только для TCP): SYN, ACK, FIN и др. |
| **ICMPv6 Type** | Тип ICMPv6:<br>**Echo Request**<br>**Destination Unreachable**<br>**Neighbor Solicitation**<br>**Define** – определенный (0-255) |
| **ICMPv6 Code** | Тип и код ICMPv6 (только для ICMPv6): |
| | **Any** – любой |
| | **Define** – определенный (0-255) |

**Примеры настройки**

1. **Блокировка служебного IPv6-трафика**:
    - **Action**: Deny
    - **Source IP**: fe80::/10 (link-local)
    - **Destination IP**: ff00::/8 (multicast)
2. **Разрешение ICMPv6 для NDP**:
    - **Action**: Permit
    - **Protocol**: ICMPv6
    - **ICMP Type**: 135 (Neighbor Solicitation), 136 (Neighbor Advertisement)
3. **Ограничение доступа к WEB-серверу**:
    - **Action**: Permit
    - **Protocol**: TCP
    - **Destination Port**: 80, 443
    - **Destination IP**: 2001:db8:100::1/128

**Внимание!**

- Для **Shutdown** порт включается вручную в **Port Settings**.
- Используйте **DSCP** для QoS в IPv6-сетях.

## 14.7. Привязка ACL (ACL Binding)

Для применения ACL к портам перейдите:

**ACL > ACL Binding**

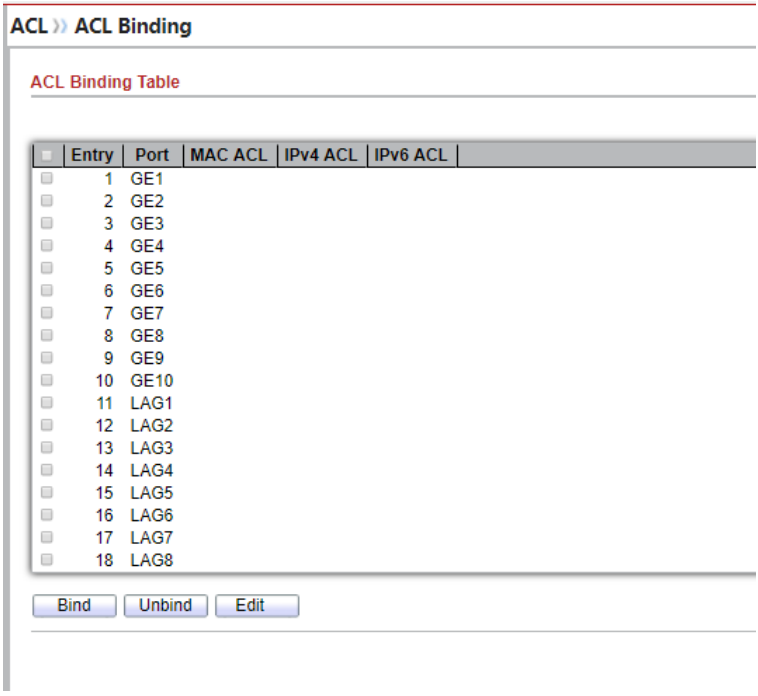
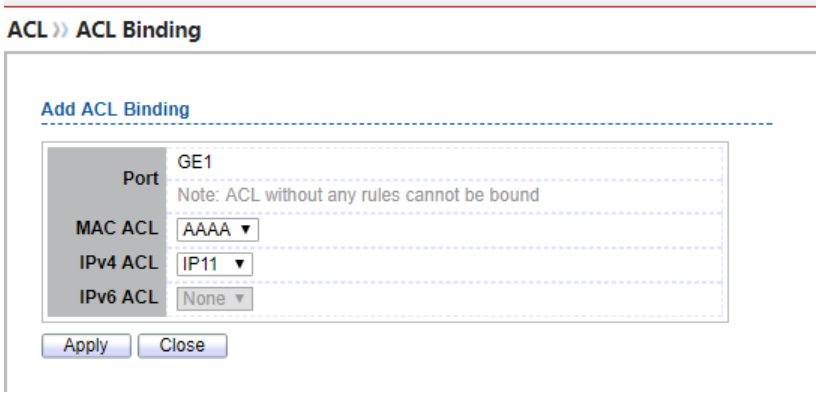



***Таблица привязок ACL***

| Параметр | Описание |
|---|---|
| **Entry** | Номер записи в таблице |
| **Port** | Порт коммутатора |

| Параметр | Описание |
|---|---|
| **MAC ACL** | Имя привязанного MAC ACL (если есть) |
| **IPv4 ACL** | Имя привязанного IPv4 ACL (если есть) |
| **IPv6 ACL** | Имя привязанного IPv6 ACL (если есть) |




***Настройка привязки ACL***

| Параметр | Описание |
|---|---|
| **Port** | Выбор порта |
| **MAC ACL** | Выбор MAC ACL из списка |
| **IPv4 ACL** | Выбор IPv4 ACL из списка |
| **IPv6 ACL** | Выбор IPv6 ACL из списка |

**Ограничения**:

- К одному порту можно привязать только **один тип ACL** (MAC, IPv4 или IPv6).
- Привязка нового ACL автоматически заменяет старый ACL.

**Рекомендации**:

- **Для пользовательских портов**:
  - MAC ACL – фильтрация по MAC-адресам
  - IPv4/IPv6 ACL – контроль доступа к сервисам
- **Для серверных портов**:
  - IPv4/IPv6 ACL с разрешением только нужных протоколов

**Пример настройки**:

- **Порт GE1**:
  - **MAC ACL**: BLOCK_UNKNOWN_MAC

- **Порт GE24 (сервер):**
  - **IPv4 ACL**: ALLOW_WEB_ACCESS

**Внимание!**

Изменения вступают в силу сразу после сохранения настроек.

## 15. Настройка QoS (QoS)

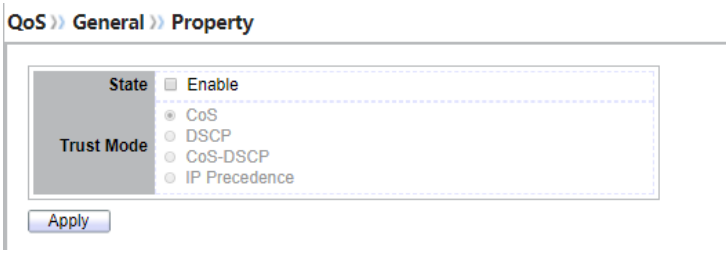
QoS (Quality of Service) – это набор технологий, которые позволяют оптимизировать передачу данных в сети, обеспечивая приоритет разным типам трафика. Это значит, что важные данные, такие как голос или видео, передаются с минимальными задержками и потерями, даже при перегрузке сети.

### 15.1. Общие настройки QoS (General)

#### 15.1.1. Основные параметры QoS (Property)

Для настройки глобальных параметров QoS перейдите:

**QoS > General > Property**



### *Глобальные настройки QoS*

| Параметр | Описание |
|---|---|
| **State** | Включение/отключение QoS (enable/disable) |
| **Trust Mode** | Режим приоритезации трафика: |
| | **CoS** – приоритет определяется по полю 802.1p в теге VLAN. Если тег отсутствует, используется значение CoS по умолчанию для порта. |
| | **DSCP** – приоритет определяется по полю DSCP (6 бит) в IP-заголовке. Не-IP трафик направляется в очередь Best Effort (0). |
| | **CoS-DSCP** – гибридный режим: для IP-трафика используется DSCP, для остального – CoS. |
| | **IP Precedence** – устаревший аналог DSCP (3 бита) |

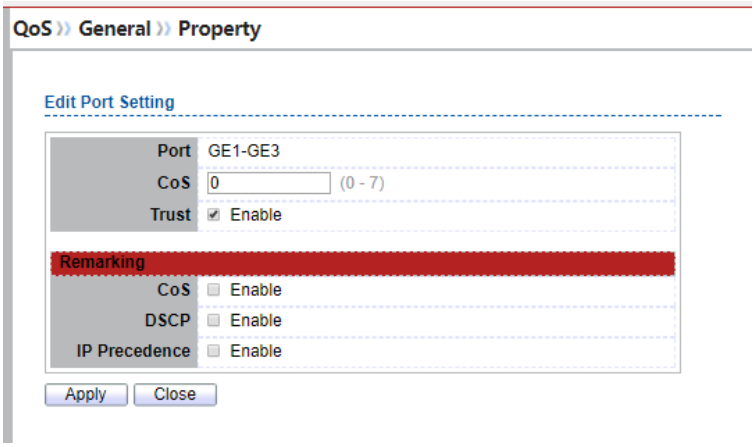
Port Setting Table

| Entry | Port | CoS | Trust | Remarking | | |
|---|---|---|---|---|---|---|
| | | | | CoS | DSCP | IP Precedence |
| 1 | GE1 | 0 | Enabled | Disabled | Disabled | Disabled |
| 2 | GE2 | 0 | Enabled | Disabled | Disabled | Disabled |
| 3 | GE3 | 0 | Enabled | Disabled | Disabled | Disabled |
| 4 | GE4 | 0 | Enabled | Disabled | Disabled | Disabled |
| 5 | GE5 | 0 | Enabled | Disabled | Disabled | Disabled |
| 6 | GE6 | 0 | Enabled | Disabled | Disabled | Disabled |
| 7 | GE7 | 0 | Enabled | Disabled | Disabled | Disabled |
| 8 | GE8 | 0 | Enabled | Disabled | Disabled | Disabled |
| 9 | GE9 | 0 | Enabled | Disabled | Disabled | Disabled |
| 10 | GE10 | 0 | Enabled | Disabled | Disabled | Disabled |
| 11 | LAG1 | 0 | Enabled | Disabled | Disabled | Disabled |
| 12 | LAG2 | 0 | Enabled | Disabled | Disabled | Disabled |
| 13 | LAG3 | 0 | Enabled | Disabled | Disabled | Disabled |
| 14 | LAG4 | 0 | Enabled | Disabled | Disabled | Disabled |
| 15 | LAG5 | 0 | Enabled | Disabled | Disabled | Disabled |
| 16 | LAG6 | 0 | Enabled | Disabled | Disabled | Disabled |
| 17 | LAG7 | 0 | Enabled | Disabled | Disabled | Disabled |
| 18 | LAG8 | 0 | Enabled | Disabled | Disabled | Disabled |

Edit

***Настройки QoS для портов***

| Параметр | Описание |
|---|---|
| **Port** | Имя порта |
| **CoS** | Приоритет по умолчанию (0-7), если тег 802.1p отсутствует |
| **Trust** | Определяет, учитывается ли глобальный Trust Mode для порта:<br>**Enabled** – порт доверяет приоритету, указанному в трафике.<br>**Disabled** – весь трафик получает приоритет Best Effort (0). |
| **Remarking (CoS)** | Перезапись поля 802.1p в теге VLAN:<br>**Enabled** – коммутатор может изменять значение CoS.<br>**Disabled** – оригинальное значение сохраняется. |
| **Remarking (DSCP)** | Перезапись значения DSCP в IP-заголовке |
| **Remarking (IP Precedence)** | Перезапись значения IP Precedence |




| Параметр | Описание |
|---|---|
| **Port** | Имя порта |
| **CoS** | Приоритет по умолчанию (0-7), если тег 802.1p отсутствует |
| **Trust** | Определяет, учитывается ли глобальный Trust Mode для порта:<br>**Enabled** – порт доверяет приоритету, указанному в трафике.<br>**Disabled** – весь трафик получает приоритет Best Effort (0). |
| **Remarking (CoS)** | Перезапись поля 802.1p в теге VLAN:<br>**Enabled** – коммутатор может изменять значение CoS.<br>**Disabled** – оригинальное значение сохраняется. |
| **Remarking (DSCP)** | Перезапись значения DSCP в IP-заголовке |

| Параметр | Описание |
|---|---|
| **Remarking (IP Precedence)** | Перезапись значения IP Precedence |

**Рекомендации**

1. **Глобальные параметры**:
    - Для VoIP: **Trust Mode = CoS** (приоритезация по тегу VLAN).
    - Для IP-трафика: **Trust Mode = DSCP**.
2. **Настройки портов**:
    - **Trust=Enabled** для портов с доверенным оборудованием (маршрутизаторы, IP-телефоны).
    - **CoS=6** для VoIP-портов (если не используется тегирование).
    - **Remarking** включется для граничных портов.

**Пример настройки**:

- Trust Mode: CoS-DSCP
- Порт GE1 (VoIP):
- CoS: 6
- Trust: Enabled
- Remarking (CoS): Enabled

**Внимание!**

- При **Trust=Disabled** весь трафик на порту получает приоритет **Best Effort (0)**
- Режим **Remarking** изменяет приоритеты трафика «на лету» – рекомендуется осторожное использование этого режима.

### 15.1.2. Планирование очередей (Queue Scheduling)

Для настройки алгоритмов обработки трафика в очередях перейдите:

**QoS > General > Queue Scheduling**

Коммутатор поддерживает **8 очередей** на каждый интерфейс, где:

- **Очередь 8** – наивысший приоритет.
- **Очередь 1** – низший приоритет.

***Алгоритмы планирования***

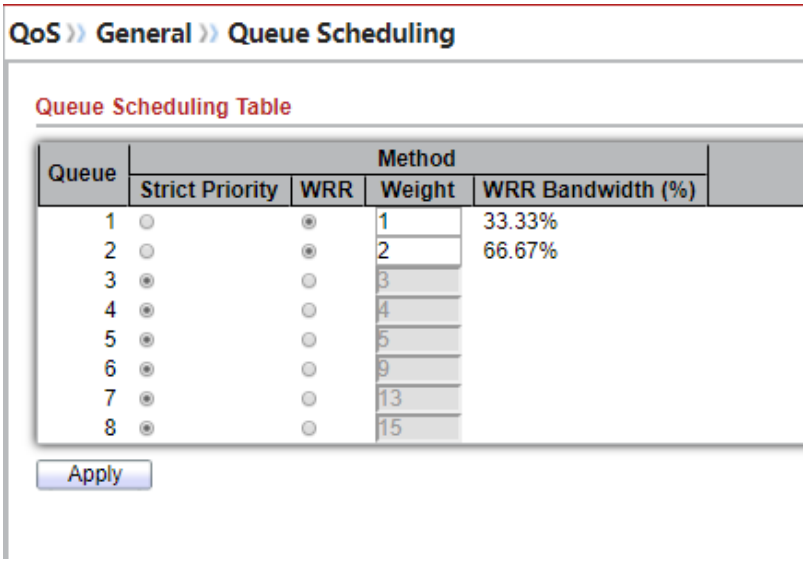
| Алгоритм | Описание |
|---|---|
| **Strict Priority (SP)** | Трафик из очереди с наивысшим приоритетом (8) передается **первым**. Остальные очереди обрабатываются только после ее опустошения. |
| **Weighted Round Robin (WRR)** | Трафик передается пропорционально **весу** (weight) очереди (чем больше вес, тем больше пакетов обрабатывается). |

**Гибридный режим**:

В коммутаторе предусмотрена возможность комбинировать SP и WRR.

Например:

- Очереди 6–8: **Strict Priority** (критичный трафик).
- Очереди 1–5: **WRR** (фоновый трафик).




***Параметры настройки очередей***

| Параметр | Описание |
|---|---|
| **Queue** | Номер очереди (1–8). |
| **Strict Priority** | Включение алгоритма SP для очереди. |
| **WRR** | Включение алгоритма WRR для очереди. |
| **Weight** | Вес очереди (1–255) – актуально только для WRR. |
| **WRR Bandwidth** | Процент полосы пропускания для WRR-очередей. |

**Примеры настройки**

**1. Приоритезация VoIP (Strict Priority, SP)**

- Очередь 8: Strict Priority = Enable (VoIP, CoS=6)
- Очередь 7: Strict Priority = Enable (Видео, CoS=5)
- Очереди 1–6: WRR = Enable, Weight = 10 (фоновый трафик)

**2. Пропорциональное распределение (WRR)**

- Очередь 8: WRR, Weight = 50 (важный трафик)
- Очередь 7: WRR, Weight = 30
- Очереди 1–6: WRR, Weight = 5 (низкоприоритетный трафик)

**3. Гибридный режим**

- Очереди 7–8: Strict Priority = Enable (VoIP и видео)
- Очереди 1–6: WRR = Enable, Weight = 20 (WEB серфинг, почта)

**Рекомендации**

1. **Для VoIP и реального времени**:
    - Используйте **Strict Priority** для очередей 6–8.
    - Назначьте CoS 5–7 этим очередям (в разделе **15.1.3 CoS Mapping**).
2. **Для балансировки нагрузки**:
    - Настройте **WRR** с весами, например:
        - Очередь 4 (CoS=3): Weight = 30
        - Очередь 3 (CoS=2): Weight = 20
3. **Мониторинг**:
    - Проверяйте статистику очередей, чтобы избежать перегрузки.

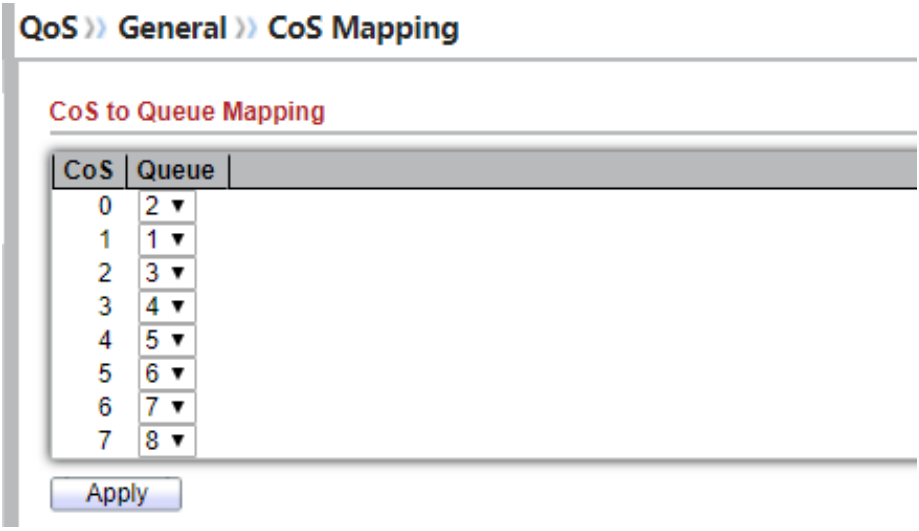
**Внимание!**

- Приоритет SP всегда превосходит WRR.
- Вес WRR влияет только на **относительную** пропускную способность.

### 15.1.3. Сопоставление CoS (CoS Mapping)

Для настройки привязки приоритетов CoS (802.1p) к очередям перейдите:

**QoS > General > CoS Mapping**




***CoS → Queue (Назначение очередей)***

Определяет, в какую очередь попадет трафик на основе тега 802.1p. Для нетэгированных кадров используется CoS по умолчанию.

| Параметр | Описание |
|---|---|
| **CoS** | Значение приоритета (0 – 7), где:<br>• **0** – (низший)<br>• **7** – (высший) |
| **Queue** | Номер очереди (1–8), куда направляется трафик. |


***Queue → CoS (Перемаркировка приоритетов)***

Задает новое значение 802.1p для трафика, выходящего из указанной очереди.

| **Параметр** | **Описание** |
|---|---|
| Queue | Номер очереди (1 – 8). |
| CoS | Новое значение 802.1p (0 – 7) для перемаркировки. |

**Рекомендации по настройке**

1. **Для VoIP и видео в реальном времени**:
    - Назначьте высокие приоритеты CoS (5–7) на высокоуровневые очереди (6–8).
2. **Для перемаркировки (Mapping)**:
    - Если трафик из очереди 3 должен выходить с низким приоритетом: *Queue 3 → CoS 1*

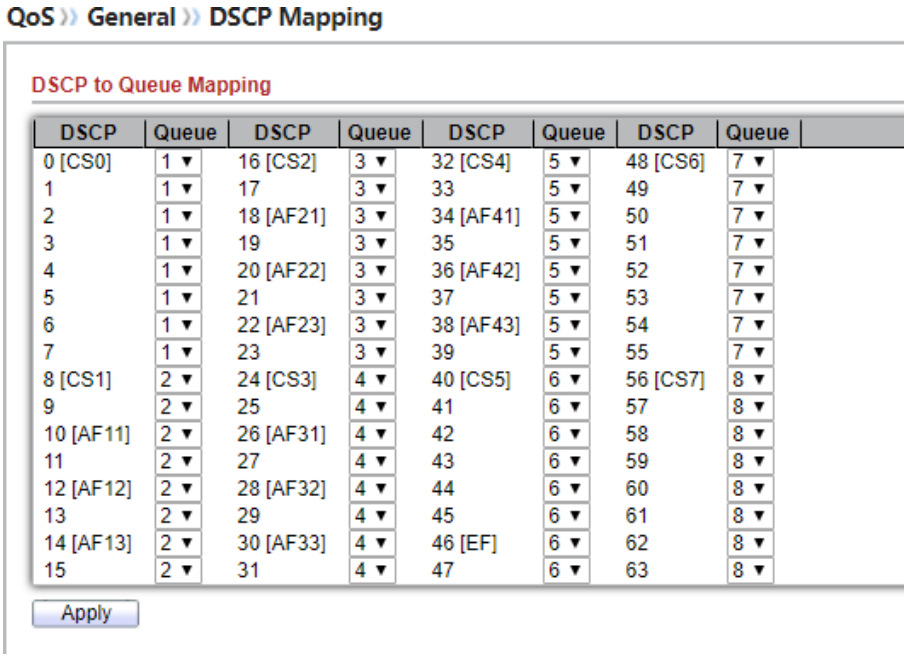
**Внимание!**

- Настройки **CoS > Queue** и **Queue > CoS** работают **независимо**.
- Перемаркировка полезна для граничных портов, где нужно изменить приоритет перед отправкой в другую сеть.

### 15.1.4. Сопоставление DSCP (DSCP Mapping)

Для настройки привязки значений DSCP к очередям и обратной перемаркировки перейдите в следующий раздел:

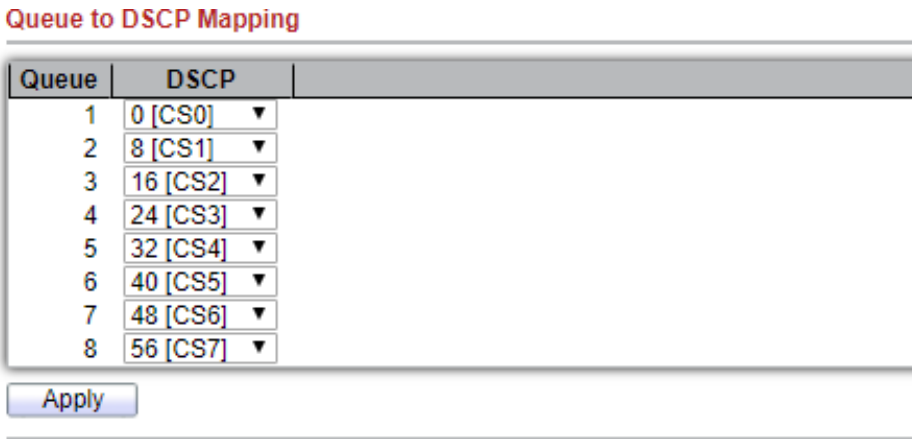
**QoS > General > DSCP Mapping**



***DSCP → Queue (Назначение очередей)***

Определяет, в какую очередь попадет **IP-трафик** на основе значения DSCP (6 бит в IP-заголовке).

| Параметр | Описание |
|---|---|
| **DSCP** | Значение Differentiated Services Code Point (или DSCP (0–63)):<br>• **0** – Best Effort<br>• **46 (EF)** – Expedited Forwarding (VoIP)<br>• **34 (AF41)** – Video |
| **Queue** | Номер очереди (1–8). |



***Queue → DSCP (Перемаркировка DSCP)***

Задает **новое значение DSCP** для трафика, выходящего из указанной очереди.

| Параметр | Описание |
|---|---|
| **Queue** | Номер очереди (1–8). |
| **DSCP** | Новое значение DSCP (0–63). |

**Рекомендации**

1. **Критичный трафик (VoIP, видео)**:
    - Назначьте DSCP EF (46) и AF41 (34) на высокоприоритетные очереди (7–8).

*DSCP 46 → Queue 8*

*DSCP 34 → Queue 7*

2. **Перемаркировка**:
    - Если трафик из очереди 3 должен выходить с низким приоритетом:

*Queue 3 → DSCP 10*

3. **Совместимость с CoS**:
    - При **Trust Mode = CoS-DSCP** настройки DSCP применяются только к IP-трафику.

**Пример настройки**

1. **Назначение очередей**:

   *DSCP 46 → Queue 8*

   *DSCP 34 → Queue 7*

   *DSCP 0–32 → Queue 1–6*

2. **Перемаркировка на выходе**:

   *Queue 8 → DSCP 46*

   *Queue 1 → DSCP 0*

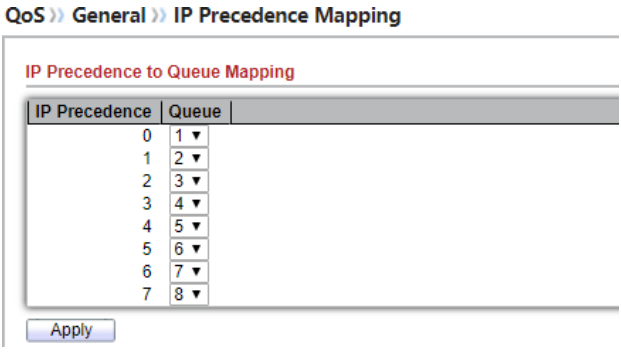
**Внимание!**

- DSCP-перемаркировка не влияет на тег 802.1p (если не включен **CoS-DSCP Trust Mode**).
- Для VoIP используйте **EF (46)** и **Strict Priority** для очереди 8.

### 15.1.5. Сопоставление IP Precedence (IP Precedence Mapping)

Для настройки привязки значений IP Precedence к очередям и обратной перемаркировки перейдите в следующий раздел WEB интерфейса:

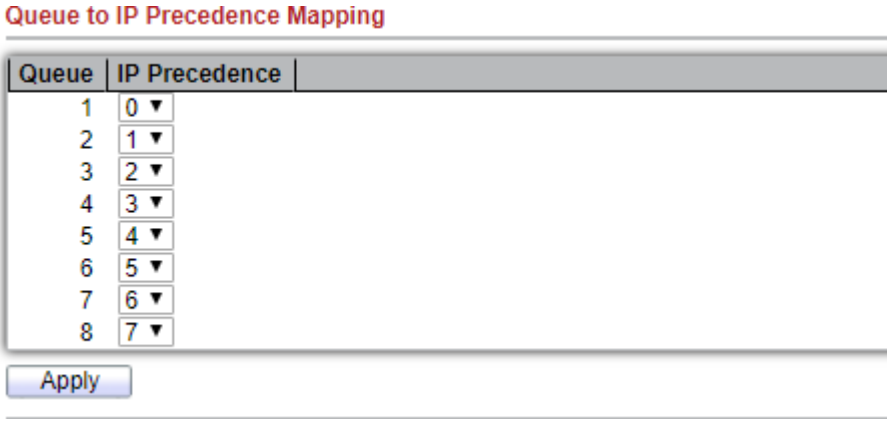
**QoS > General > IP Precedence Mapping**



***IP Precedence → Queue (Назначение очередей)***

Определяет, в какую очередь попадет трафик на основе значения IP Precedence (3 бита в IP-заголовке).

| Параметр | Описание |
|---|---|
| **IP Precedence** | Приоритет (0–7), где:<br>• **0** – Routine (Best Effort)<br>• **7** – Network Control (Highest) |
| **Queue** | Номер очереди (1–8). |




***Queue → IP Precedence (Перемаркировка)***

Задает **новое значение IP Precedence** для трафика, выходящего из очереди.

| Параметр | Описание |
|---|---|
| **Queue** | Номер очереди (1–8). |
| **IP Precedence** | Новое значение (0–7). |

**Рекомендации**

1. **Устаревший стандарт**:
    - IP Precedence (3 бита) заменен на DSCP (6 бит). Используйте только для совместимости со старым оборудованием.
2. **Сопоставление с DSCP**:
    - IP Precedence 5 ≈ DSCP 40 (CS5) – для VoIP.

**Внимание!**

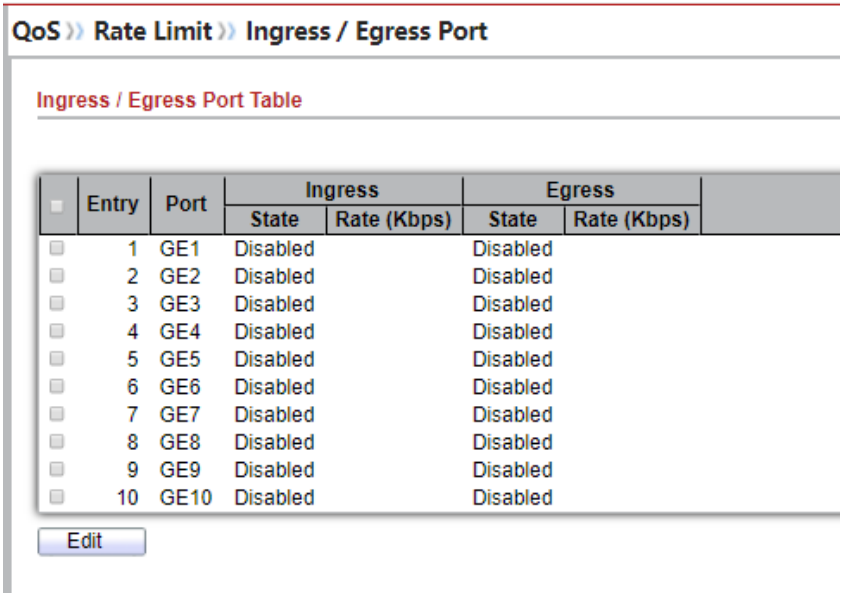
- Настройки **не влияют** на DSCP/CoS, если не включена соответствующая перемаркировка.
- Для современных сетей предпочтительнее функция **DSCP Mapping**.

## 15.2. Ограничение скорости (Rate Limit)

### 15.2.1. Входящий/Исходящий порт (Ingress/Egress Port)

Для настройки ограничения скорости на портах перейдите в следующий раздел WEB интерфейса:

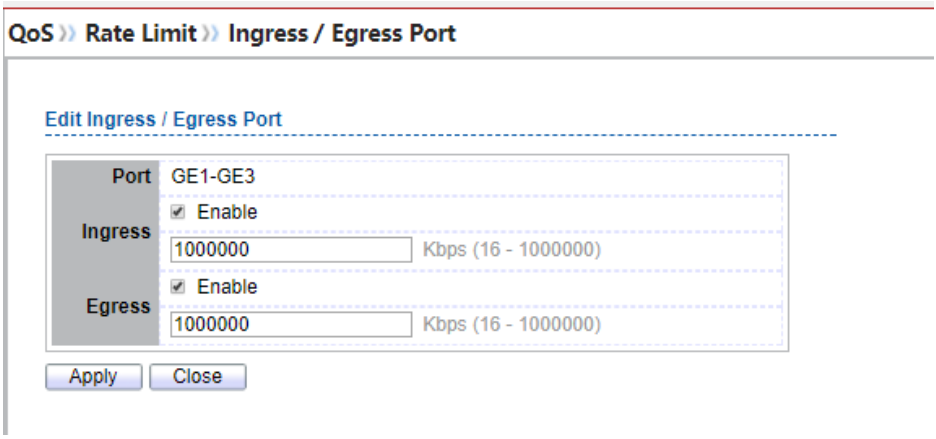
**QoS > Rate Limit > Ingress/Egress Port**




***Текущие настройки***

| Параметр | Описание |
|---|---|
| **Port** | Имя порта |

| Параметр | Описание |
|---|---|
| **Ingress (State)** | Состояние ограничения входящей скорости:<br>• **Enabled** – включено<br>• **Disabled** – выключено |
| **Ingress (Rate)** | Макс. входящая скорость (Кбит/с) |
| **Egress (State)** | Состояние ограничения исходящей скорости |
| **Egress (Rate)** | Макс. исходящая скорость (Кбит/с) |




***Редактирование настроек***

| Параметр | Описание |
|---|---|
| **Port** | Выбор порта |

| Параметр | Описание |
|---|---|
| **Ingress** | Включение/выключение ограничения входящего трафика. При включении требуется указать **Rate** в Кбит/с |
| **Egress** | Включение/выключение ограничения исходящего трафика. При включении требуется указать **Rate** в Кбит/с |

**Рекомендации**

1. **Для аплинк-портов**:
   - Установите **Egress Rate** = 90% от физической скорости (например, 900 Мбит/с для 1 Гбит/с).
2. **Для пользовательских портов**:
   - **Ingress Rate = 10 Мбит/с** – защита от флуда.
3. **Формат значения**:
   - Указывается в **битах в секунду** (например, 10000000 = 10 Мбит/с).

**Пример настройки**

1. **Порт GE1 (гостевой Wi-Fi)**:

   *Ingress: Enabled, Rate = 5000000 (5 Мбит/с)*

   *Egress: Enabled, Rate = 10000000 (10 Мбит/с)*

2. **Порт GE24 (аплинк)**:

   *Egress: Enabled, Rate = 900000000 (900 Мбит/с)*

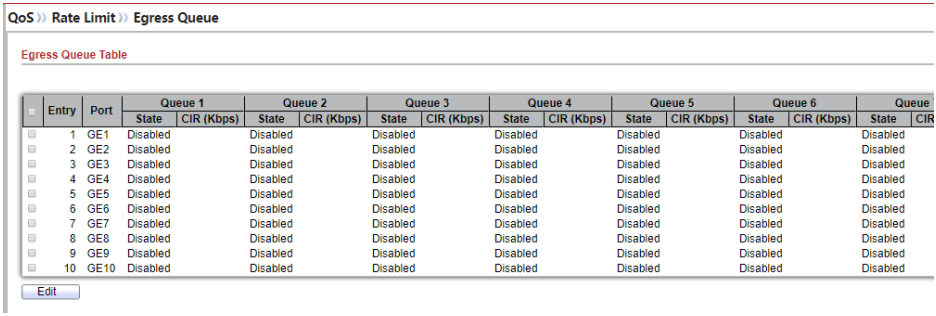
**Внимание!**

- Ограничение **Ingress** работает на аппаратном уровне и отбрасывает избыточные пакеты.
- **Egress** ограничение формирует очередь (без потерь, если включен QoS).

### 15.2.2. Ограничение скорости для исходящих очередей (Egress Queue)

Для настройки ограничения скорости передачи данных для отдельных очередей на портах перейдите в следующий раздел:

**QoS > Rate Limit > Egress Queue**

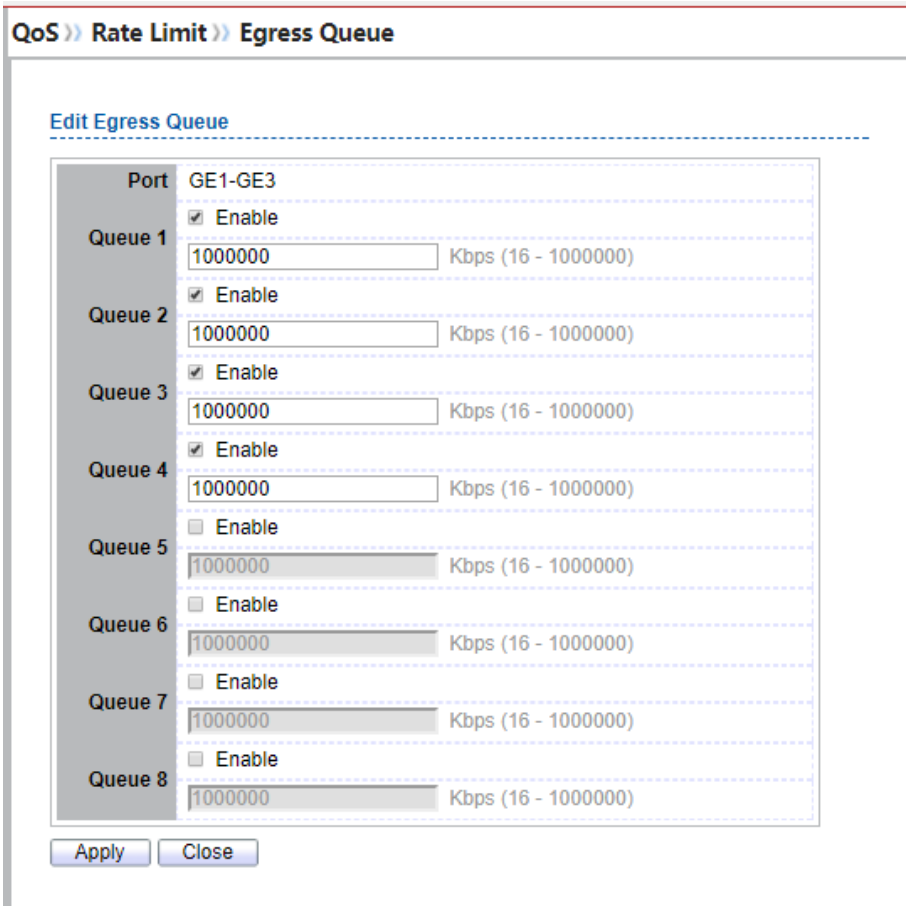



***Текущие настройки ограничения скорости очередей***

| Параметр | Описание |
|---|---|
| **Port** | Идентификатор порта |

| Параметр | Описание |
|---|---|
| **Queue 1 (State)** | Состояние ограничения скорости для очереди 1:<br>• **Enabled** – ограничение включено<br>• **Disabled** – ограничение выключено |
| **Queue 1 (CIR)** | Гарантированная скорость передачи (Committed Information Rate) для очереди 1 в битах в секунду |
| **Queue 2 (State)** | Состояние ограничения скорости для очереди 2:<br>• **Enabled** – ограничение включено<br>• **Disabled** – ограничение выключено |
| **Queue 2 (CIR)** | Гарантированная скорость передачи (Committed Information Rate) для очереди 2 в битах в секунду |
| **Queue 3 (State)** | Состояние ограничения скорости для очереди 3:<br>• **Enabled** – ограничение включено<br>• **Disabled** – ограничение выключено |
| **Queue 3 (CIR)** | Гарантированная скорость передачи (Committed Information Rate) для очереди 3 в битах в секунду |
| **Queue 4 (State)** | Состояние ограничения скорости для очереди 4:<br>• **Enabled** – ограничение включено<br>• **Disabled** – ограничение выключено |
| **Queue 4 (CIR)** | Гарантированная скорость передачи (Committed Information Rate) для очереди 4 в битах в секунду |

| Параметр | Описание |
|---|---|
| **Queue 5 (State)** | Состояние ограничения скорости для очереди 5:<br>• **Enabled** – ограничение включено<br>• **Disabled** – ограничение выключено |
| **Queue 5 (CIR)** | Гарантированная скорость передачи (Committed Information Rate) для очереди 5 в битах в секунду |
| **Queue 6 (State)** | Состояние ограничения скорости для очереди 6:<br>• **Enabled** – ограничение включено<br>• **Disabled** – ограничение выключено |
| **Queue 6 (CIR)** | Гарантированная скорость передачи (Committed Information Rate) для очереди 6 в битах в секунду |
| **Queue 7 (State)** | Состояние ограничения скорости для очереди 7:<br>• **Enabled** – ограничение включено<br>• **Disabled** – ограничение выключено |
| **Queue 7 (CIR)** | Гарантированная скорость передачи (Committed Information Rate) для очереди 7 в битах в секунду |
| **Queue 8 (State)** | Состояние ограничения скорости для очереди 8:<br>• **Enabled** – ограничение включено<br>• **Disabled** – ограничение выключено |
| **Queue 8 (CIR)** | Гарантированная скорость передачи (Committed Information Rate) для очереди 8 в битах в секунду |




***Настройка ограничений скорости***

| Параметр | Описание |
|---|---|
| **Port** | Выбор порта для настройки |
| **Queue 1** | Включение/выключение ограничения скорости и задание значения CIR для очереди 1 |

| Параметр | Описание |
|---|---|
| **Queue 2** | Включение/выключение ограничения скорости и задание значения CIR для очереди 2 |
| **Queue 3** | Включение/выключение ограничения скорости и задание значения CIR для очереди 3 |
| **Queue 4** | Включение/выключение ограничения скорости и задание значения CIR для очереди 4 |
| **Queue 5** | Включение/выключение ограничения скорости и задание значения CIR для очереди 5 |
| **Queue 6** | Включение/выключение ограничения скорости и задание значения CIR для очереди 6 |
| **Queue 7** | Включение/выключение ограничения скорости и задание значения CIR для очереди 7 |
| **Queue 8** | Включение/выключение ограничения скорости и задание значения CIR для очереди 8 |

**Рекомендации**

1. **Для критически важного трафика (VoIP, видео):**
    - Очереди 7-8 (высший приоритет):
        - Включите ограничение скорости

        - Установите CIR = 20-30% от общей пропускной способности порта
2. **Для стандартного трафика:**
    - Очереди 3-6:
        - CIR = 40-50% от общей пропускной способности
3. **Для фонового трафика:**
    - Очереди 1-2:
        - CIR = 10-20% от общей пропускной способности

**Внимание!**

1. **Совместимость:**
    - Настройки применяются только при включенном QoS
    - Для очередей в режиме Strict Priority ограничение скорости может быть менее эффективным

2. Для достижения оптимальной производительности сумма всех CIR на порту не должна превышать 90% от его физической пропускной способности.

# 16. Инструменты диагностики (Diagnostics)

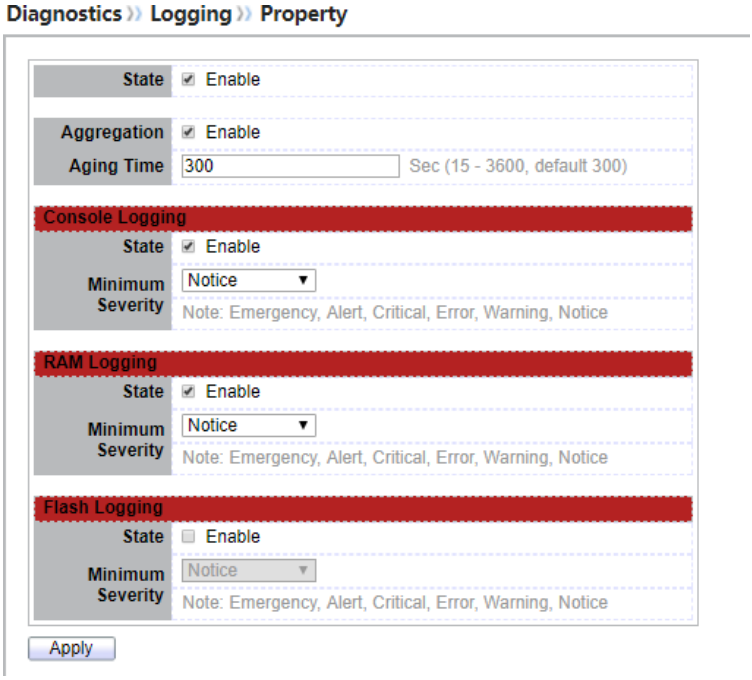
В данном разделе WEB интерфейса содержутся инструменты и механизмы диагностики работы коммутатора.

## 16.1. Ведение журналов событий (Logging)

### 16.1.1. Основные параметры (Property)

Для управления системой журналирования перейдите в следующий раздел WEB интерфейса:

**Diagnostics > Logging > Property**



***Глобальные настройки функции ведения журналов***

| Параметр | Описание |
|---|---|
| **State** | Включение/отключение системы ведения журналов:<br>• **Enable** – активация функции ведения журналов<br>• **Disable** – полное отключение (логи не сохраняются нигде) |

***1. Вывод сообщений в консоль (Console)***

| Параметр | Описание |
|---|---|
| **State** | Вывод логов (сообщений о событиях) в консоль:<br>• **Enable** – вывод сообщений в консоль<br>• **Disable** – отключение вывода сообщений |
| **Minimum Severity** | Минимальный уровень важности сообщений:<br>• **Emergency** (0) – аварийные<br>• **Alert** (1) – тревожные<br>• **Critical** (2) – критически важные<br>• **Error** (3) – об ошибках<br>• **Warning** (4) – предупреждающие<br>• **Notice** (5) – уведомления<br>• **Informational** (6) – информационные<br>• **Debug** (7) – отладочные |

***Вывод сообщений в оперативную память (RAM)***

| Параметр | Описание |
|---|---|
| **State** | Вывод сообщений в буфер оперативной памяти<br>• **Enable** – включено<br>• **Disable** – отключено |
| **Minimum Severity** | Минимальный уровень важности сообщений:<br>• **Emergency** (0) – аварийные<br>• **Alert** (1) – тревожные<br>• **Critical** (2) – критически важные<br>• **Error** (3) – об ошибках<br>• **Warning** (4) – предупреждающие<br>• **Notice** (5) – уведомления<br>• **Informational** (6) – информационные<br>• **Debug** (7) – отладочные |

***3. Вывод сообщений в встроенную постоянная память (Flash)***

| Параметр | Описание |
|---|---|
| **State** | Сохранение логов во внутреннюю память устройства (Flash)<br>• **Enable** – включено<br>• **Disable** – отключено |
| **Minimum Severity** | Минимальный уровень важности сообщений:<br>• **Emergency** (0) – аварийные |

| Параметр | Описание |
|---|---|
| | • **Alert** (1) – тревожные<br>• **Critical** (2) – критически важные<br>• **Error** (3) – об ошибках<br>• **Warning** (4) – предупреждающие<br>• **Notice** (5) – уведомления<br>• **Informational** (6) – информационные<br>• **Debug** (7) – отладочные |

**Рекомендации**

1. **Для мониторинга в реальном времени**:
    - Включите **Console Logging** с уровнем **Warning** (4).
2. **Для сбора истории событий**:
    - Активируйте **Flash Logging** с уровнем **Informational** (6).

**Пример настройки**:

*Global State: Enable*

*Console:*

*- State: Enable*

*- Minimum Severity: Warning*

*RAM:*

*- State: Enable*

*- Minimum Severity: Error*

*Flash:*

*- State: Enable*

*- Minimum Severity: Informational*

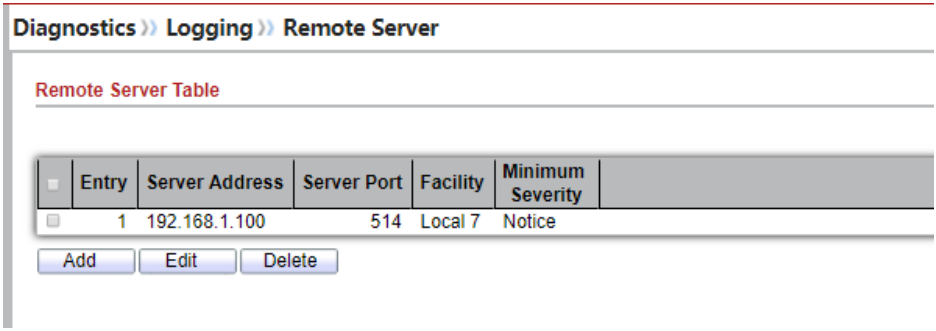
**Внимание!**

- Логи в **RAM** очищаются после перезагрузки.
- Логи в **Flash** сохраняются, но могут перезаписываться при заполнении памяти.

### 16.1.2. Удаленный сервер для отправки логов (Remote Server)

Для настройки отправки логов на внешний сервер (например, syslog) перейдите в следующий раздел WEB интерфейса:

**Diagnostics > Logging > Remote Server**




***Параметры сервера для отправки логов***

| Параметр | Описание |
|---|---|
| **Server Address** | IP-адрес или доменное имя сервера для отправки логов |
| **Server Port** | Порт сервера (обычно 514 для syslog) |

| Параметр | Описание |
|---|---|
| **Facility** | Категория сообщений:<br>• **local0–local7** – пользовательские категории |
| **Severity** | Минимальный уровень важности сообщений:<br>• **Emergency** (0) – аварийные<br>• **Alert** (1) – тревожные<br>• **Critical** (2) – критически важные<br>• **Error** (3) – об ошибках<br>• **Warning** (4) – предупреждающие<br>• **Notice** (5) – уведомления<br>• **Informational** (6) – информационные<br>• **Debug** (7) – отладочные |

**Рекомендации**

1. **Типовая конфигурация для мониторинга**:

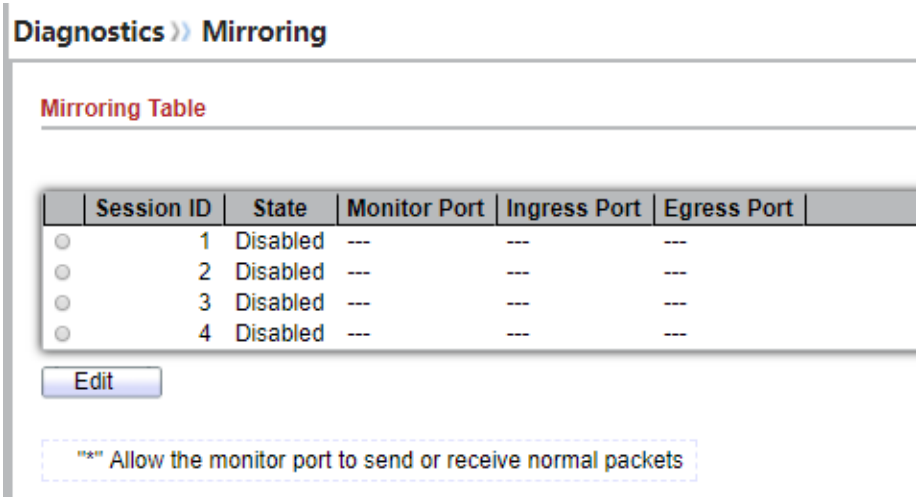
   *Server Address: 192.168.1.100*
   *Server Port: 514*
   *Facility: local4*
   *Severity: Warning*

2. **Для отладки**:
   - Установите **Severity = Debug** (учтите, что это увеличит объем логов).
3. **Безопасность**:
   - Используйте **VPN** или **TLS** протоколы для защиты логов, если сервер находится в другой сети.

## 16.2. Зеркалирование портов (Mirroring)

Для доступа к настройкам зеркалирования (функция для контроля трафика на порту путем копирования его на другой порт) перейдите в следующий раздел WEB интерфейса:

**Diagnostics > Mirroring**




**Параметры таблицы настройки зеркалирования**

| Параметр | Описание |
|---|---|
| **Session ID** | Выберите идентификатор сессии зеркалирования |
| **State** | Выберите состояние сессии зеркалирования:<br>• **Enabled**: активировать зеркалирование на основе порта<br>• **Disabled**: отключить зеркалирование |

| Параметр | Описание |
|---|---|
| **Monitor Port** | Выберите порт мониторинга для сессии зеркалирования и укажите, могут ли обычные пакеты передаваться или приниматься через этот порт |
| **Ingress port** | Выберите исходные RX-порты (прием трафика) для зеркалирования |
| **Egress ports** | Выберите исходные TX-порты (передача трафика) для зеркалирования |

**Рекомендации:**

- Зеркалирование портов полезно для анализа сетевого трафика и диагностики проблем
- Порт мониторинга не должен использоваться для передачи критического трафика, так как его производительность может снизиться

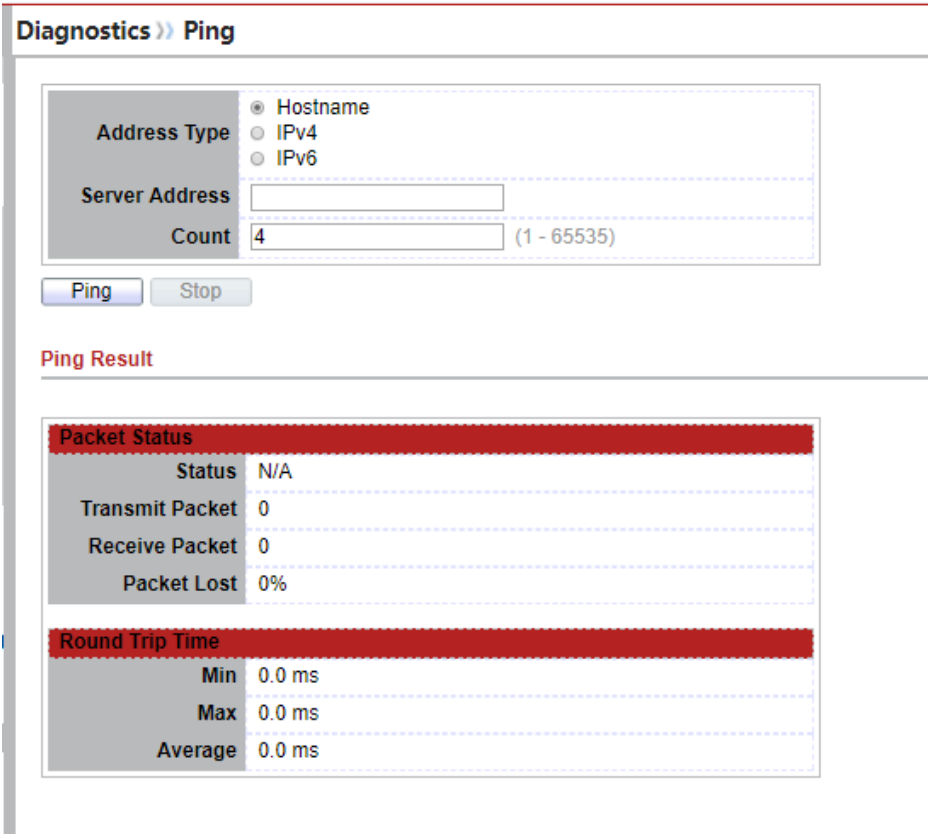
**Пример настройки:**

- Перейдите в раздел Diagnostics > Mirroring;
- Выберите Session ID (например, 1);
- Установите State в значение Enabled;
- Укажите Monitor Port (например, Port 24);
- Выберите Ingress port (например, Port 1-5) для копирования входящего трафика;
- Выберите Egress ports (например, Port 6-10) для копирования исходящего трафика;
- Сохраните настройки.

## 16.3. Инструмент проверки связи (Ping)

Для использования функции PING в коммутаторе перейдите в следующий раздел WEB интерфейса:

**Diagnostic > Ping**




| Параметр | Описание |
|---|---|
| **Address Type** | Укажите тип адреса:<br>• **Hostname** - доменное имя |

| Параметр | Описание |
|---|---|
| | • **IPv6** - адрес IPv6<br>• **IPv4** - адрес IPv4 |
| **Server Address** | Укажите IP адрес удаленного сервера, связь с которым надо проверить посредством PING |
| **Count** | Задайте количество отправляемых ICMP запросов PING |

**Рекомендации:**

- Функция PING используется для проверки доступности сетевых устройств
- Для диагностики соединения рекомендуется отправлять 3-5 запросов
- При использовании доменного имени убедитесь в правильности настроек DNS

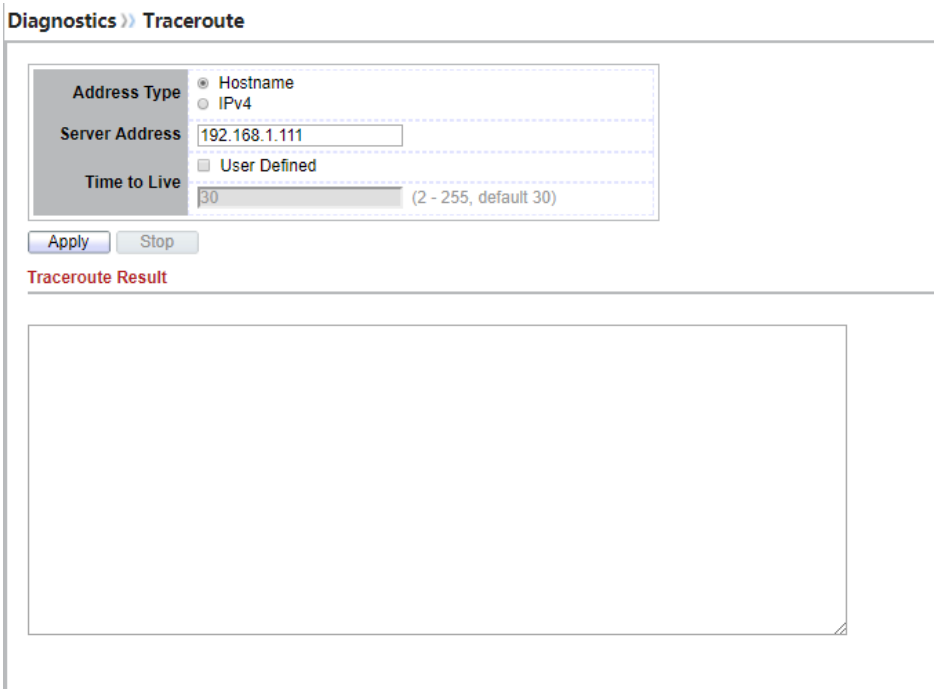
**Пример использования:**

1. Перейдите в раздел Diagnostic > Ping;
2. Установите Address Type = IPv4;
3. Введите Server Address = 192.168.1.1;
4. Установите Count = 5;
5. Нажмите PING для выполнения проверки;
6. Анализируйте результаты (время ответа, процент потерь)

## 16.4. Трассировка маршрута (Traceroute)

Для выполнения трассировки маршрута перейдите в следующий раздел WEB интерфейса:

**Diagnostic > Traceroute**




| Параметр | Описание |
|---|---|
| **Address Type** | Выберите тип адреса:<br>• **Hostname** - доменное имя<br>• **IPv4** - IPv4 адрес |
| **Server** | Укажите адрес целевого устройства, проверку |

| Параметр | Описание |
| --- | --- |
| **Address** | маршрута к которому требуется выполнить. |
| **Time to Live** | Укажите максимальное количество переходов (hops) для трассировки |

**Рекомендации:**

- Трассировка маршрута помогает определить путь прохождения пакетов и выявить проблемные участки сети
- Для локальных сетей обычно достаточно значения TTL 15-20
- При использовании доменного имени убедитесь в работоспособности DNS-резолвинга

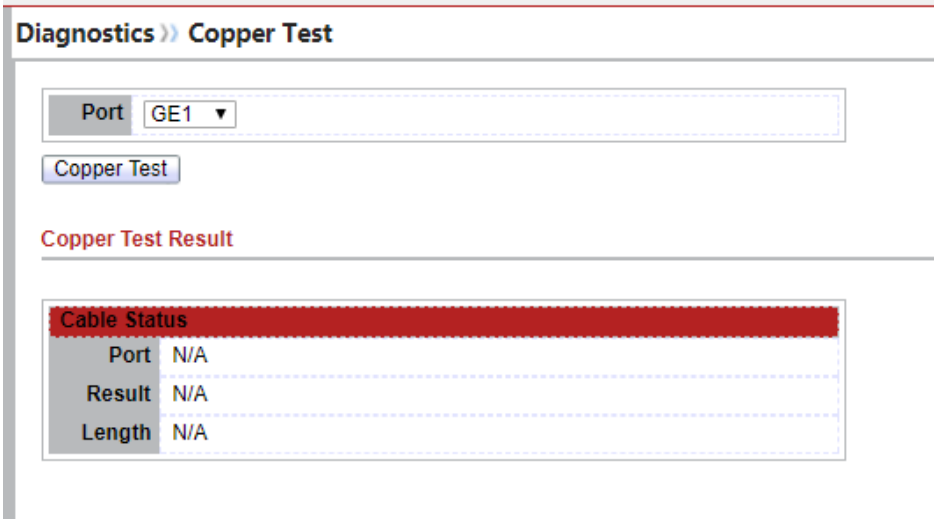
**Пример использования:**

1. Перейдите в раздел Diagnostic > Traceroute;
2. Установите Address Type = IPv4;
3. Введите Server Address = 8.8.8.8;
4. Установите Time to Live = 30;
5. Нажмите Apply для выполнения трассировки;
6. Анализируйте результаты (узлы на пути, время отклика)

## 16.5. Тестирование медных кабелей (Copper Test)

Для диагностики медных кабелей перейдите в следующий раздел WEB интерфейса:

**Diagnostic > Copper Test**




***Параметры тестирования***

| Параметр | Описание |
|---|---|
| **Port** | Выберите интерфейс для проведения теста |

***Результаты тестирования***

| Параметр | Описание |
|---|---|
| **Port** | Тестируемый интерфейс |

| Параметр | Описание |
|---|---|
| **Result** | Результат теста:<br>**OK** - исправная линия<br>**Short Cable** - короткое замыкание<br>**Open Cable** - обрыв линии<br>**Impedance Mismatch** - несоответствие импеданса<br>**Line Drive** - проблема с драйвером линии |
| **Length** | Расстояние до места неисправности (в метрах) |

**Рекомендации:**

1. Тестирование рекомендуется проводить при:
    - Первоначальном монтаже сети
    - Возникновении проблем с подключением
    - Плановом техническом обслуживании
2. Для получения точных результатов:
    - Отключите кабель от активного оборудования
    - Убедитесь в чистоте контактов разъемов
    - Проверяйте каждый порт отдельно

**Пример использования:**

1. Перейдите в раздел Diagnostic > Copper Test;
2. Выберите Port = GE1;
3. Нажмите Copper Test;
4. Дождитесь завершения теста (10-30 секунд);
5. Проанализируйте результаты:
    - При Result: OK - кабель исправен

- При других результатах - проверьте указанный участок кабеля

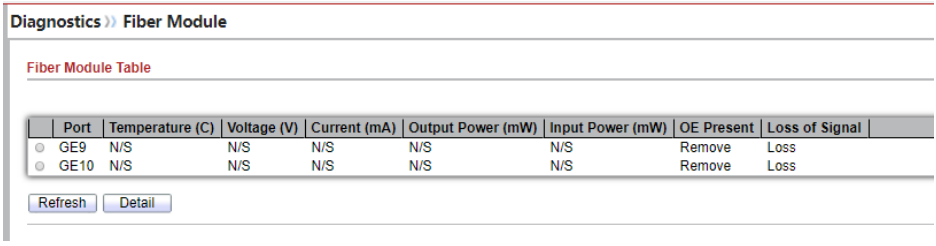
**Внимание!**

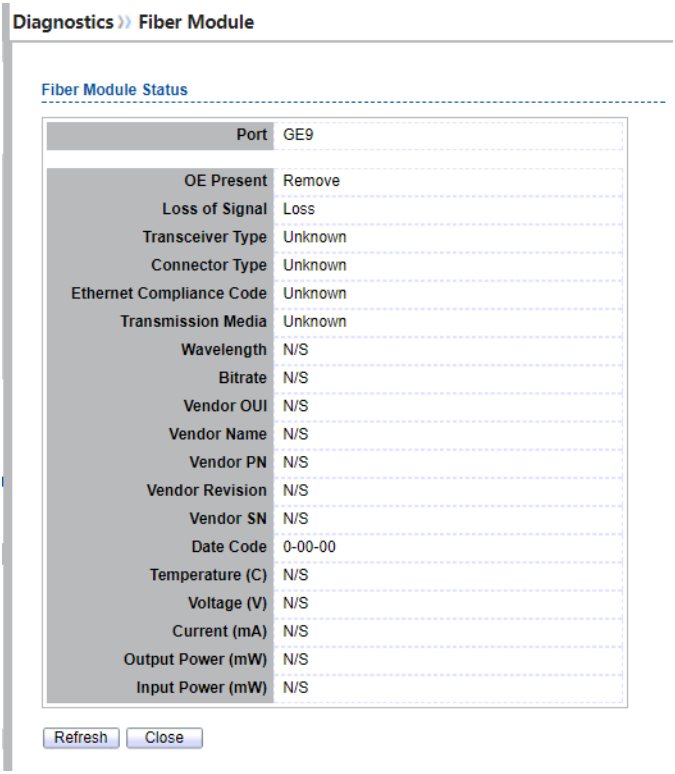
Для точного определения места неисправности используйте специализированные кабельные тестеры. Результаты работы инструмента Copper Test в коммутаторе могут быть использованы только для ознакомления.

## 16.6. Инструмент диагностики SFP модулей (Fiber Module)

Данная страница WEB интерфейса отображает статус SFP модулей, т рабочую информацию, передаваемую трансиверами SFP. Некоторые данные могут быть недоступны для модулей, не поддерживающих стандарт цифрового мониторинга SFF-8472.

**Diagnostic > Fiber Module**






***Параметры оптических модулей***

| Параметр | Описание |
|---|---|
| **Port** | Номер интерфейса/порта |
| **Temperature** | Температура трансивера (°C) |
| **Voltage** | Напряжение питания (В) |
| **Current** | Ток смещения передатчика (мА) |
| **Output Power** | Выходная мощность передатчика (мВт) |

| Параметр | Описание |
|---|---|
| **Input Power** | Уровень принимаемого сигнала (мВт) |
| **Transmitter Fault** | Состояние неисправности передатчика |
| **OE Present** | Индикатор готовности модуля (питание подано, данные доступны) |
| **Loss of Signal** | Индикатор потери сигнала |

Кнопка Refresh (обновить) нужна для обновления информации об используемых SFP модулях.

**Рекомендации:**

1. Регулярно проверяйте ключевые параметры:
    - Температура (норма: 0...+70°C)
    - Мощность передатчика и принимаемого сигнала
    - Напряжение питания (стандартное значение: 3.3В)
2. Критические состояния:
    - **Transmitter Fault** = Yes - неисправность передатчика
    - **Loss of Signal** = Yes - отсутствие сигнала
    - Выход параметров за допустимые пределы

**Пример мониторинга:**

1. Перейдите в раздел Diagnostic > Fiber Module
2. Выберите интересующий SFP порт (например, GE10);
3. Проверьте основные параметры:

- Output Power > -7 dBm (оптимально)
- Input Power в допустимом диапазоне
- Отсутствие аварийных индикаторов

4. Для проблемных портов нажмите **Detail** для получения детальной информации
5. Используйте **Refresh** для обновления данных об SFP модуле

**Внимание!**

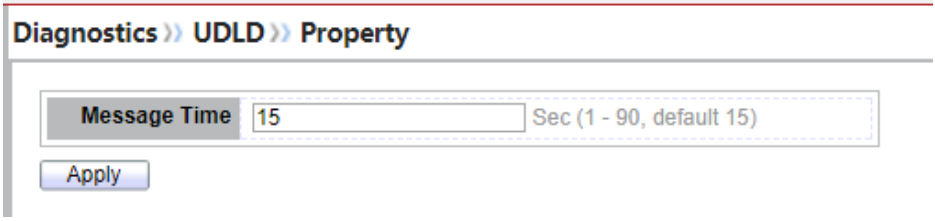
Допустимые значения параметров зависят от конкретной модели SFP-модуля. Для точной диагностики сверяйтесь с технической документацией производителя модуля.

## 16.7. Обнаружение однонаправленных соединений UDLD (UniDirectional Link Detection)

### 16.7.1. Свойства (Property)

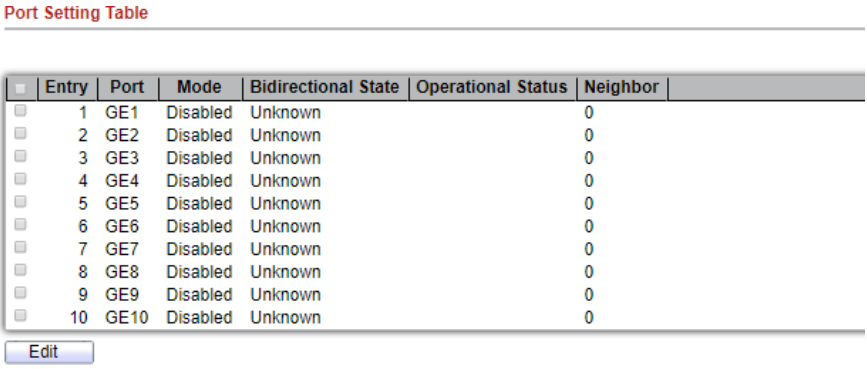
Для настройки параметров UDLD перейдите в следующий раздел WEB интерфейса:

**Diagnostics > UDLD > Property**



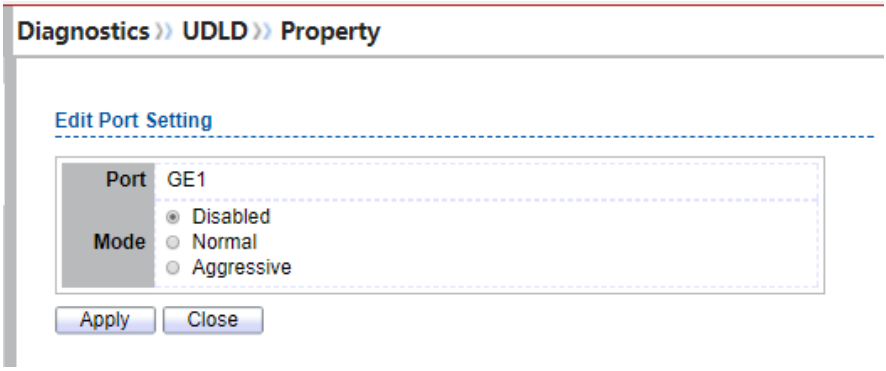
### *Глобальные настройки UDLD*

| Параметр | Описание |
|---|---|
| **Message Time** | Интервал отправки UDLD-сообщений (1-90 секунд) |




### Статус портов

| Параметр | Описание |
|---|---|
| **Mode** | Текущий режим работы UDLD на интерфейсе |
| **Bidirectional State** | Состояние двунаправленной связи |
| **Operational Status** | Текущий операционный статус |
| **Neighbor** | Количество обнаруженных устройств – соседей |




**Настройки порта:**

| Параметр | Описание |
|---|---|
| **Port** | Выбранный порт для настройки |
| **Mode** | Режим работы UDLD:<br>• **Disabled** - функция отключена<br>• **Normal** - обычный режим (переход в состояние Link Up One)<br>• **Aggressive** - агрессивный режим (переход в состояние Re-Establish) |

**Рекомендации:**

1. Для критически важных соединений используйте агрессивный режим
2. Оптимальный интервал сообщений - 15-30 секунд
3. Регулярно проверяйте статус bidirectional state на ключевых портах

**Пример настройки:**

1. Перейдите в раздел Diagnostics > UDLD > Property;
2. Установите Message Time = 20;
3. Выберите порт для настройки;
4. Установите Mode = Aggressive (для важных соединений);
5. Нажмите Apply (принять) для сохранения

**Внимание!**

Режим Aggressive обеспечивает более быстрое обнаружение проблем, но может создавать дополнительную нагрузку на оборудование.

### 16.7.2. Соседние устройства (Neighbor)

Для просмотра информации о соседних устройствах перейдите в раздел WEB интерфейса:

**Diagnostics > UDLD > Neighbor**

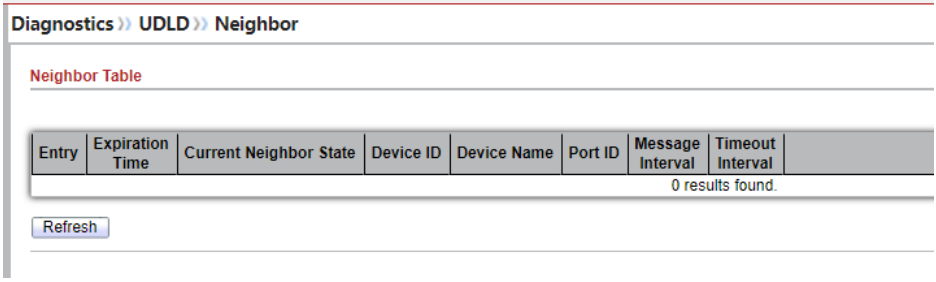


***Таблица устройств-соседей:***

| Параметр | Описание |
|---|---|
| **Entry** | Индекс записи |
| **Expiration Time** | Время до удаления записи (age out) |
| **Current Neighbor State** | Текущее состояние соседнего устройства |
| **Device ID** | Идентификатор соседнего устройства |
| **Device Name** | Имя соседнего устройства |
| **Port ID** | Идентификатор порта подключения |
| **Message Interval** | Интервал отправки сообщений соседним устройством |
| **Timeout Interval** | Таймаут соседнего устройства |

**Рекомендации:**

1. Регулярно проверяйте состояние соседей (Current Neighbor State) на критически важных соединениях
2. Обращайте внимание на:
    - Неожиданные изменения Device ID/Name - могут указывать на несанкционированное подключение
    - Увеличение Expiration Time - может свидетельствовать о проблемах связи

3. Для важных соединений сравнивайте Message Interval с локальными настройками

**Пример использования:**

1. Перейдите в раздел Diagnostics > UDLD > Neighbor;
2. Проверьте:
    - Соответствие Device Name ожидаемым соседним устройствам
    - Стабильность Current Neighbor State (должно быть "Bidirectional")
    - Соответствие Port ID ожидаемым точкам подключения
3. Для проблемных соединений:
    - Сравните Message Interval с настройками на обоих концах
    - Проверьте Expiration Time (резкие изменения могут указывать на нестабильность связи)

**Внимание!**

Информация обновляется динамически. Для актуальных данных может потребоваться обновление страницы (кнопка Refresh).

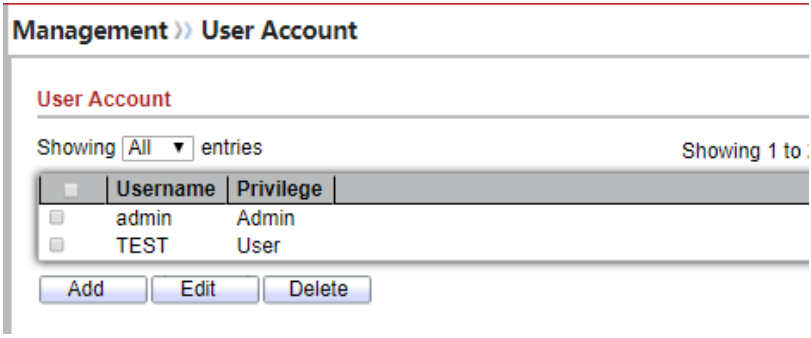
# 17. Параметры управления коммутатором (Management)

Раздел управления позволяет настраивать параметры управления коммутатором.

## 17.1. Учетные записи пользователей (User Account)

Для управления учетными записями перейдите в следующий раздел:

**Management > User Account**

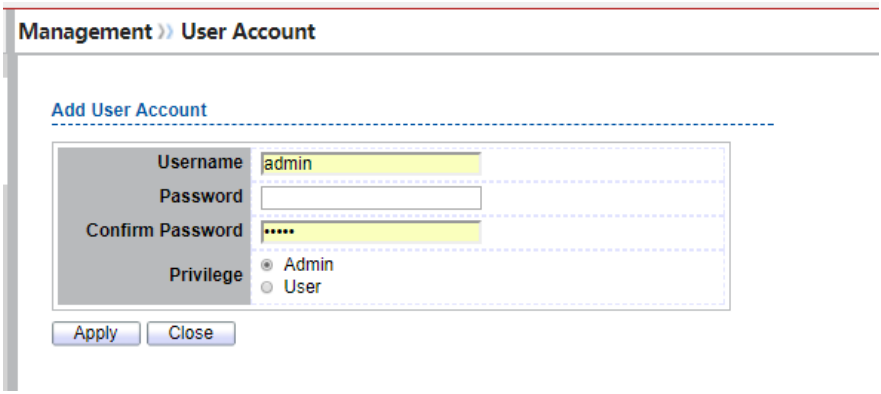


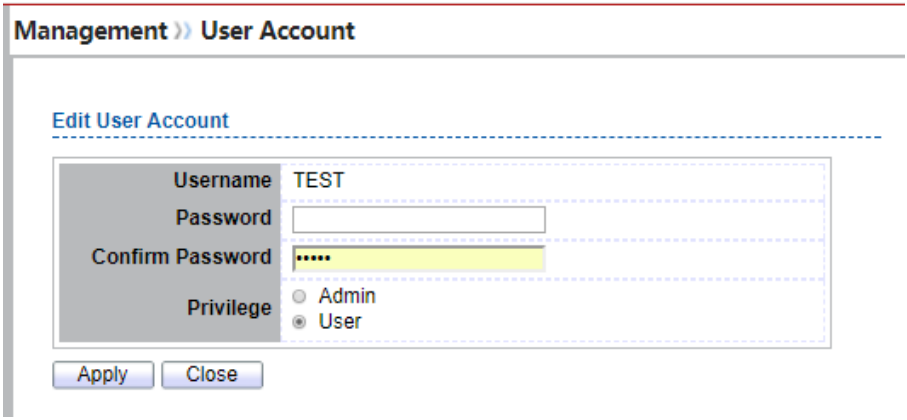

*Примечание:* Учетная запись по умолчанию (admin/admin) не может быть удалена.

***Таблица учетных записей***

| Параметр | Описание |
|---|---|
| **Username** | Имя пользователя |
| **Privilege** | Уровень привилегий: |

| Параметр | Описание |
|---|---|
| | • **Admin** (15) - полный доступ к настройкам<br>• **User** (1) - только просмотр настроек |




***Диалог добавления/редактирования пользователя***

| Параметр | Описание |
|---|---|
| **Username** | Имя пользователя (латинские буквы/цифры) |

| Параметр | Описание |
|---|---|
| **Password** | Пароль пользователя |
| **Confirm Password** | Подтверждение пароля |
| **Privilege** | Уровень доступа:<br>• **Admin** - полные права (редактирование/чтение/запись)<br>• **User** - только чтение |

**Рекомендации по безопасности:**

1. Сразу после первого входа измените пароль администратора
2. Создавайте индивидуальные учетные записи для каждого администратора
3. Для обычных сотрудников используйте учетные записи с уровнем User
4. Пароль должен содержать:
    - Не менее 8 символов
    - Заглавные и строчные буквы
    - Цифры и специальные символы

**Пример настройки:**

1. Перейдите в настройки Management > User Account;
2. Нажмите "Add" для создания новой записи;
3. Заполните поля:
    - Username: network_admin
    - Password: Str0ngP@ss2023

- Confirm Password: Str0ngP@ss2023
- Privilege: Admin

4. Нажмите "Apply" для сохранения настроек

**Внимание!**

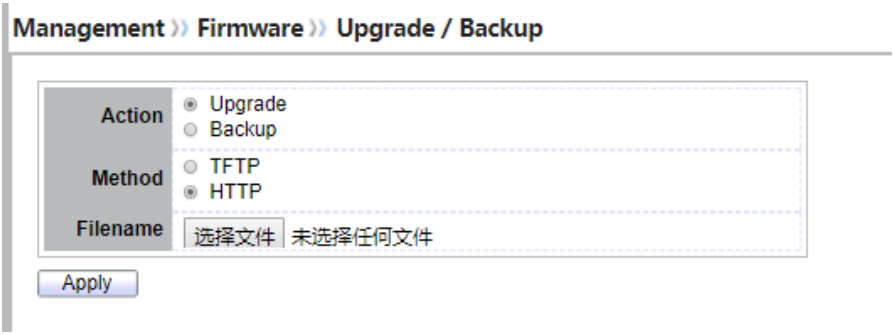
Регулярно обновляйте пароли (рекомендуется каждые 3-6 месяцев) и удаляйте неиспользуемые учетные записи.

## 17.2. Управление прошивкой коммутатора (Firmware)

### 17.2.1. Обновление/Резервное копирование (Upgrade/Backup)

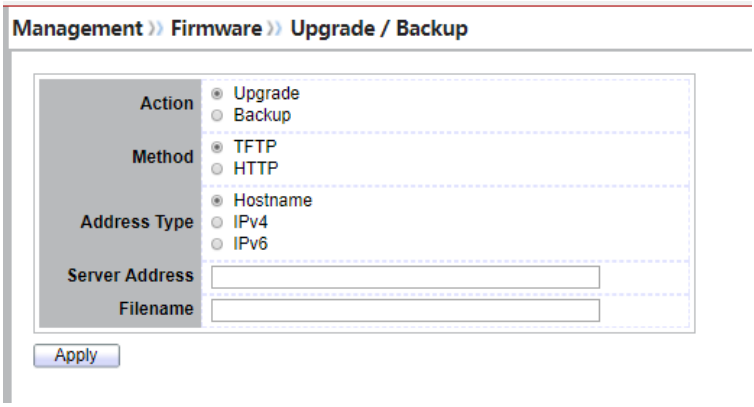
Для управления прошивкой коммутатора перейдите в следующий раздел:

**Management > Firmware > Upgrade/Backup**



***Обновление через HTTP***

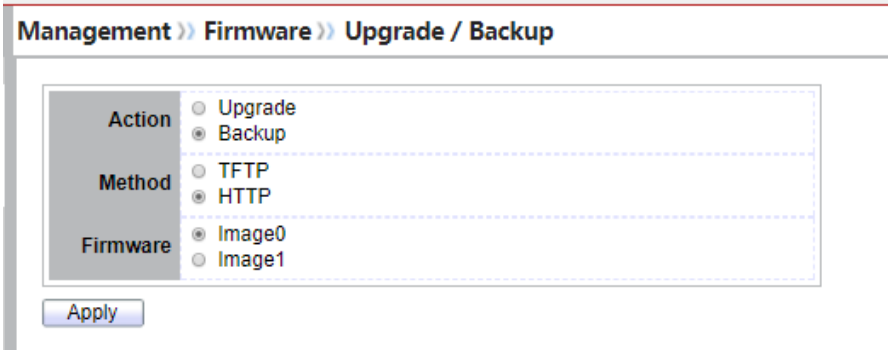
| Параметр | Описание |
|---|---|
| **Action** | Выберите операцию с прошивкой:<br>• **Upgrade** - обновление прошивки<br>• **Backup** - резервное копирование |
| **Method** | Способ передачи прошивки:<br>• **HTTP** - через веб-интерфейс<br>• **TFTP** - через TFTP-сервер |
| **Filename** | Выберите файл прошивки с локального компьютера через браузер |




***Обновление через TFTP***

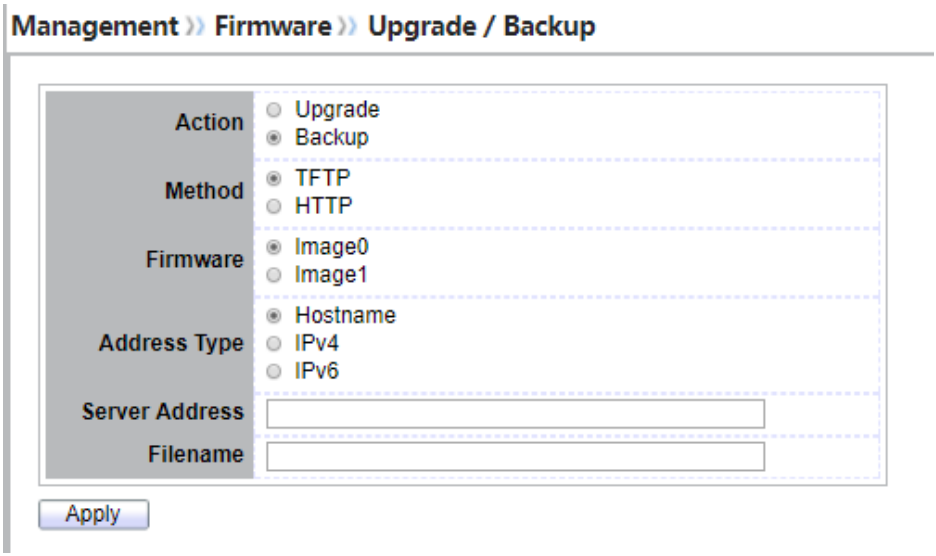
| Параметр | Описание |
|---|---|
| **Address Type** | Тип адреса сервера: |

| Параметр | Описание |
|---|---|
| | • **Hostname** - доменное имя<br>• **IPv4** – адрес IPv4<br>• **IPv6** – адрес IPv6 |
| **Server Address** | Адрес TFTP-сервера |
| **Filename** | Имя файла прошивки на сервере |




***Резервное копирование через HTTP***

| Параметр | Описание |
|---|---|
| **Firmware** | Выбор раздела прошивки:<br>• **Image0** - раздел 0<br>• **Image1** - раздел 1 |




***Резервное копирование через TFTP***

Дополнительные параметры:

| Параметр | Описание |
|---|---|
| **Action** | Выберите операцию с прошивкой:<br>• **Upgrade** - обновление прошивки<br>• **Backup** - резервное копирование |
| **Method** | Способ передачи прошивки:<br>• **HTTP** - через веб-интерфейс<br>• **TFTP** - через TFTP-сервер |
| **Firmware** | Выбор раздела прошивки:<br>• **Image0** - раздел 0<br>• **Image1** - раздел 1 |

| Параметр | Описание |
|---|---|
| **Address Type** | Тип адреса сервера:<br>• **Hostname** - доменное имя<br>• **IPv4** – адрес IPv4<br>• **IPv6** – адрес IPv6 |
| **Server Address** | Адрес TFTP-сервера |
| **Filename** | Имя для сохранения резервной копии |

**Рекомендации:**

1. Перед обновлением:
    - Сделайте резервную копию текущей прошивки
    - Сохраните конфигурацию устройства
    - Убедитесь в стабильности питания
2. Процесс обновления:
    - Не прерывайте питание устройства
    - Не перезагружайте коммутатор
    - Дождитесь полного завершения процесса

**Пример обновления через HTTP:**

1. Перейдите в раздел Management > Firmware > Upgrade/Backup;
2. Установите:
    - Action: Upgrade
    - Method: HTTP
3. Выберите файл прошивки

4. Нажмите "Apply" для начала обновления
5. Дождитесь автоматической перезагрузки

**Примечание:** Время обновления может занимать 5-15 минут. После успешного обновления рекомендуется выполнить сброс к заводским настройкам и восстановить конфигурацию вручную.

### 17.2.2. Активный образ прошивки (Active Image)

Для управления активным образом прошивки перейдите в следующий раздел WEB интерфейса:

**Management > Firmware > Active Image**

***Информация о прошивке***

| Параметр | Описание |
|---|---|
| **Active Image** | Выбор активного образа прошивки для следующей загрузки коммутатора |
| **Firmware** | Наименование прошивки |
| **Version** | Версия прошивки |
| **Name** | Название прошивки |
| **Size** | Размер образа прошивки |
| **Created** | Дата создания прошивки |
| **Backup Image** | Информация о резервном образе прошивки |
| **Firmware** | Наименование резервной прошивки |
| **Version** | Версия резервной прошивки |
| **Name** | Название резервной прошивки |
| **Size** | Размер образа резервной прошивки |
| **Created** | Дата создания резервной прошивки |

**Рекомендации:**

1. При выборе активного образа:
    - Убедитесь, что выбранная версия прошивки стабильна
    - Проверьте совместимость с текущей конфигурацией
    - Для тестирования новых версий используйте неактивный раздел
2. Перед переключением:
    - Сохраните текущую конфигурацию
    - Запланируйте перезагрузку в период минимальной нагрузки на сеть
    - Имейте возможность быстро вернуть предыдущую версию прошивки

**Пример настройки:**

1. Перейдите в раздел Management > Firmware > Active Image;
2. Выберите нужный образ в поле **Active Image**:
    - Image0 (основной раздел)
    - Image1 (резервный раздел)
3. Проверьте информацию о версии:
    - Сравните версии в обоих разделах
    - Убедитесь в достаточном размере образа
4. Нажмите **Apply** для сохранения изменений
5. Выполните перезагрузку коммутатора для применения новой прошивки

**Внимание!**

После переключения активного образа рекомендуется:

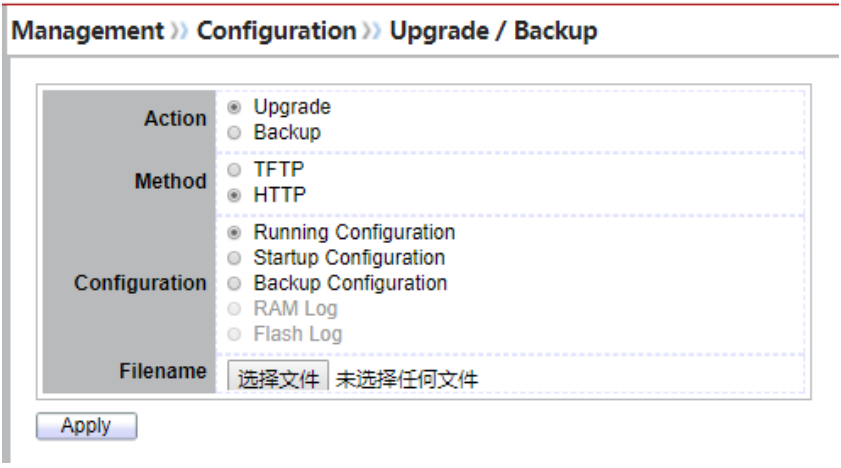
- Проверить журналы системы на наличие ошибок
- Убедиться в работоспособности всех критических функций
- Протестировать работу сетевых интерфейсов

## 17.3. Конфигурация (Configuration)

### 17.3.1. Обновление/Резервное копирование конфигурации (Upgrade/Backup)

Для управления конфигурацией перейдите в следующей раздел WEB интерфейса:

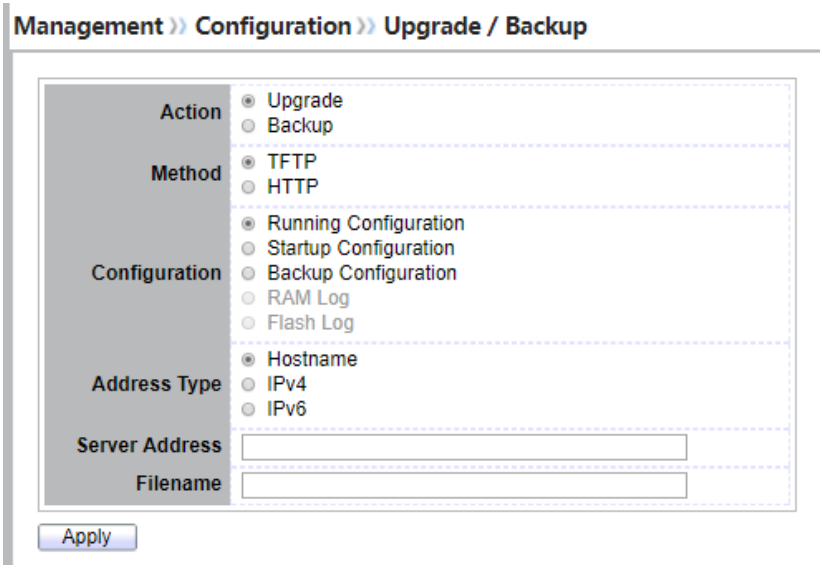
**Management > Configuration > Upgrade/Backup**




***Обновление конфигурации через HTTP***

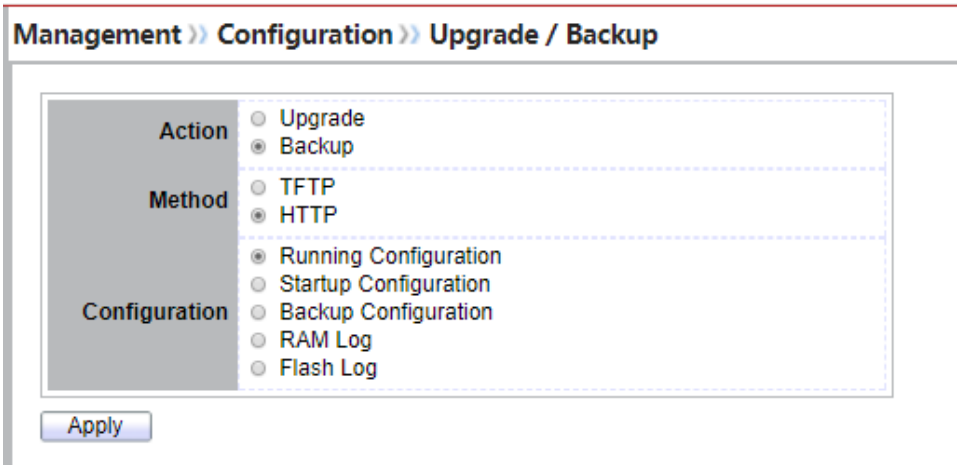
| Параметр | Описание |
|---|---|
| **Action** | Выбор операции:<br>• **Upgrade** - загрузка конфигурации<br>• **Backup** - сохранение конфигурации |

| Параметр | Описание |
|---|---|
| **Method** | Метод передачи:<br>• **TFTP**<br>• **HTTP** |
| **Configuration** | Тип конфигурации:<br>• **Running Configuration** - объединение полученной конфигурации с текущей<br>• **Startup Configuration** - замена конфигурации в качестве стартовой<br>• **Backup Configuration** - замена резервной конфигурации на новую |
| **Filename** | Выбор файла конфигурации |



***Обновление конфигурации через TFTP***

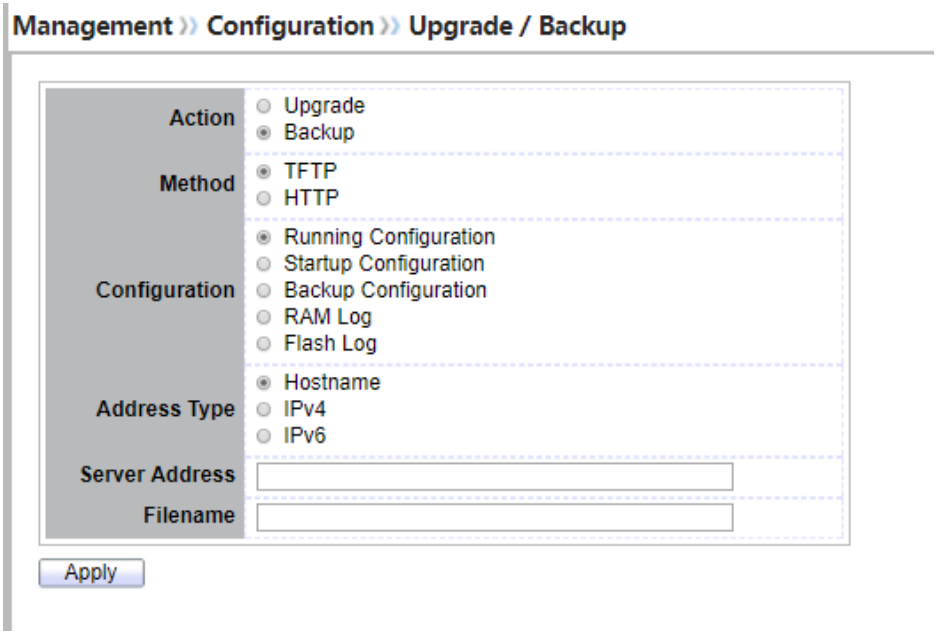
| Параметр | Описание |
|---|---|
| **Action** | Выбор операции:<br>• **Upgrade** - загрузка конфигурации<br>• **Backup** - сохранение конфигурации |
| **Method** | Метод передачи:<br>• **TFTP**<br>• **HTTP** |
| **Configuration** | Тип конфигурации:<br>• **Running Configuration** - объединение полученной конфигурации с текущей<br>• **Startup Configuration** - замена конфигурации в качестве стартовой<br>• **Backup Configuration** - замена резервной конфигурации на новую |
| **Address Type** | Тип адреса:<br>• **Hostname**<br>• **IPv4**<br>• **IPv6** |
| **Server Address** | Адрес TFTP-сервера |
| **Filename** | Имя файла на сервере |




***Резервное копирование через HTTP***

| Параметр | Описание |
|---|---|
| **Action** | Выбор операции:<br>• **Upgrade** - загрузка конфигурации<br>• **Backup** - сохранение конфигурации |
| **Method** | Метод передачи:<br>• **TFTP**<br>• **HTTP** |
| **Configuration** | Тип конфигурации:<br>• **Running Configuration** – текущая конфигурация<br>• **Startup Configuration** – стартовая конфигурация<br>• **Backup Configuration** – резервная конфигурация<br>• **RAM Log** – логи в оперативной памяти |

| Параметр | Описание |
|---|---|
| | коммутатора<br>• **Flash Log** – логи в постоянной памяти коммутатора |




***Резервное копирование через TFTP***

| Параметр | Описание |
|---|---|
| **Action** | Выбор операции:<br>• **Upgrade** - загрузка конфигурации<br>• **Backup** - сохранение конфигурации |

| Параметр | Описание |
|---|---|
| **Method** | Метод передачи:<br>• **TFTP**<br>• **HTTP** |
| **Configuration** | Тип конфигурации:<br>• **Running Configuration** – текущая конфигурация<br>• **Startup Configuration** – стартовая конфигурация<br>• **Backup Configuration** – резервная конфигурация<br>• **RAM Log** – логи в оперативной памяти коммутатора<br>• **Flash Log** – логи в постоянной памяти коммутатора |
| **Address Type** | Тип адреса:<br>• **Hostname**<br>• **IPv4**<br>• **IPv6** |
| **Server Address** | Адрес TFTP-сервера |
| **Filename** | Имя для сохранения файла |

**Рекомендации:**

1. Регулярно сохраняйте конфигурацию:
    - Перед внесением изменений
    - После успешной настройки
    - По расписанию (еженедельно/ежемесячно)
2. Используйте разные имена для версий. Например:

- config_20240101_startup.cfg
- config_20240101_after_update.cfg

**Пример резервного копирования стартовой прошивки:**

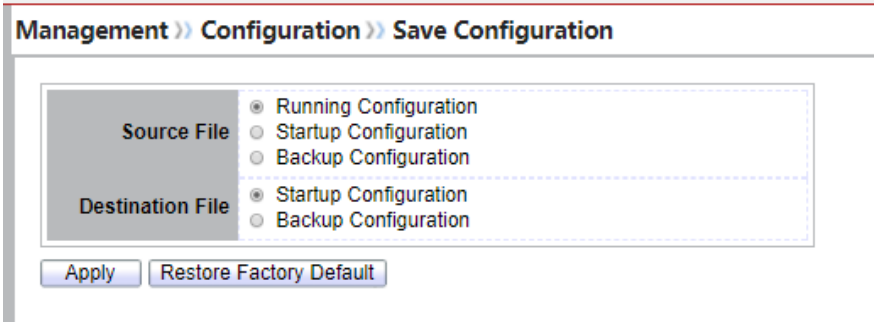
1. Перейдите в раздел Management > Configuration > Upgrade/Backup
2. Установите:
   - Action: Backup
   - Method: HTTP
   - Configuration: Startup Configuration
3. Нажмите "Backup"
4. Сохраните файл на локальный компьютер

**Внимание!** При объединении конфигураций (Running) могут возникать конфликты настроек. Проверяйте изменения перед сохранением.

### 17.3.2. Сохранение конфигурации (Save Configuration)

Для управления конфигурационными файлами перейдите в следующий раздел WEB интерфейса:

**Management > Configuration > Save Configuration**



***Параметры сохранения конфигурации***

| Параметр | Описание |
|---|---|
| **Source File** | Исходный файл конфигурации:<br>• **Running Configuration** - текущая рабочая конфигурация<br>• **Startup Configuration** - стартовая конфигурация<br>• **Backup Configuration** - резервная копия конфигурации |
| **Destination File** | Целевой файл конфигурации:<br>• **Startup Configuration** - сохранить как стартовую конфигурацию<br>• **Backup Configuration** - сохранить как резервную копию конфигурации |

**Дополнительные функции:**

- Кнопка **Restore Factory Default** - сброс настроек к заводским

**Рекомендации:**

1. Регулярно сохраняйте текущую конфигурацию (Running) в Startup:
    - После внесения изменений
    - Перед обновлением ПО
    - При стабильной работе оборудования
2. Сохраняйте резервные копии перед:
    - Крупными изменениями настроек
    - Обновлением прошивки
    - Изменением топологии сети

**Пример использования:**

1. Перейдите в раздел Management > Configuration > Save Configuration;
2. Выберите:
    - Source File: Running Configuration
    - Destination File: Startup Configuration
3. Нажмите "Apply" для сохранения
4. Для создания резервной копии:
    - Source File: Running Configuration
    - Destination File: Backup Configuration
5. Нажмите "Apply"

**Внимание!**

- Сброс к заводским настройкам (**Restore Factory Default**) требует перезагрузки устройства
- После сброса все текущие настройки будут потеряны
- Рекомендуется предварительно сохранить текущую конфигурацию

## 17.4. Настройка SNMP (SNMP)

### 17.4.1. SNMP View (View)

Для настройки и просмотра таблицы SNMP view перейдите в следующий раздел WEB интерфейса:

**Management > SNMP > View**


| Параметр | Описание |
|---|---|
| **View** | Имя SNMP (максимальная длина - 30 символов) |
| **OID Subtree** | ASN.1 OID поддерева, включаемого/исключаемого из SNMP view |
| **Type** | Тип представления:<br>• **Include** - включить указанные MIB<br>• **Exclude** - исключить указанные MIB |

**Рекомендации:**

1. Используйте осмысленные имена SNMP view, отражающие их назначение
2. Для безопасности рекомендуется:
    - Создавать минимально необходимые представления
    - Исключать чувствительные OID из публичных представлений
3. Проверяйте корректность указанных OID

**Пример создания SNMP view:**

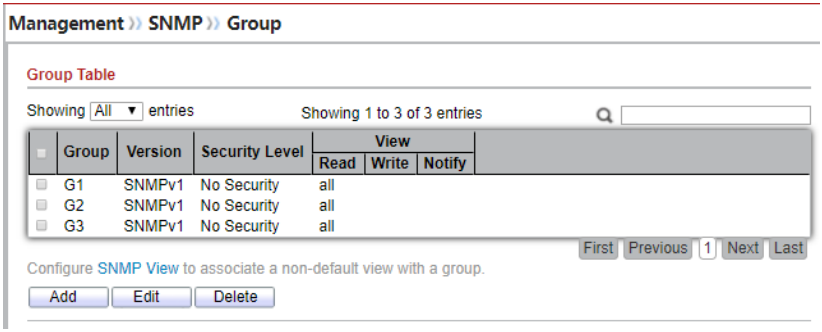
1. Перейдите в раздел Management > SNMP > View;
2. Нажмите "Add";
3. Заполните параметры:
    - View: limited_access
    - Subtree OID: 1.3.6.1.2.1.2 (интерфейсы)
    - View Type: Include
4. Нажмите "Apply"

**Примечание:** OID должны указываться в числовом формате (например, 1.3.6.1.2.1.1 для системной группы MIB-II).

### 17.4.2. Группы SNMP (Group)

Для настройки параметров SNMP-групп перейдите в следующий раздел WEB интерфейса:

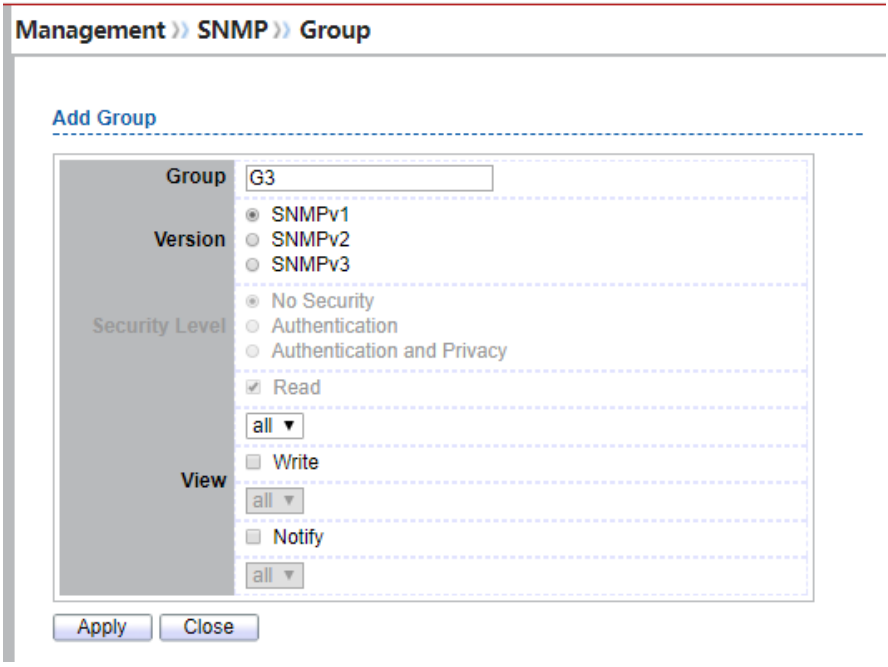
**Management > SNMP > Group**




***Основные параметры группы SNMP***

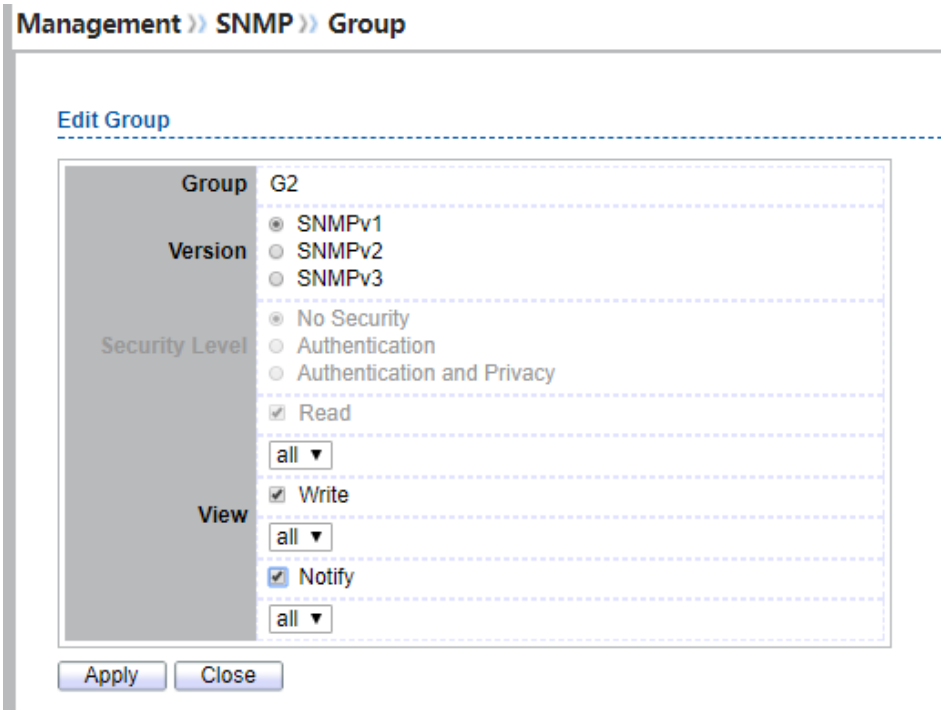
| Параметр | Описание |
|---|---|
| **Group** | Название SNMP-группы (до 30 символов) |
| **Version** | Версия SNMP:<br>• **SNMPv1**<br>• **SNMPv2c (community-based)**<br>• **SNMPv3 (user security model)** |
| **Security Level** | Уровень безопасности (для SNMPv3):<br>• **No Security** - без аутентификации<br>• **Authentication** - только аутентификация<br>• **Authentication and Privacy** - аутентификация и шифрование |

| Параметр | Описание |
|---|---|
| ***Права доступа группы SNMP*** | |
| **Read View** | Представление для чтения |
| **Write View** | Представление для записи |
| **Notify View** | Представление для уведомлений (traps) |



***Диалог добавления SNMP группы***

| Параметр | Описание |
|---|---|
| **Group** | Название SNMP-группы (до 30 символов) |
| **Version** | Версия SNMP:<br>• **SNMPv1**<br>• **SNMPv2c (community-based)**<br>• **SNMPv3 (user security model)** |
| **Security Level** | Уровень безопасности (только для SNMPv3):<br>• **No Security** - без аутентификации<br>• **Authentication** - только аутентификация<br>• **Authentication and Privacy** - аутентификация и шифрование |
| ***Права доступа группы SNMP*** | |
| **Read View** | Представление для чтения |
| **Write View** | Представление для записи |
| **Notify View** | Представление для уведомлений (traps) |




***Диалог редактирования SNMP группы***

| Параметр | Описание |
|---|---|
| **Group** | Название SNMP-группы (до 30 символов) |
| **Version** | Версия SNMP:<br>• **SNMPv1**<br>• **SNMPv2c (community-based)**<br>• **SNMPv3 (user security model)** |
| **Security Level** | Уровень безопасности (только для SNMPv3):<br>• **No Security** - без аутентификации<br>• **Authentication** - только аутентификация |

| Параметр | Описание |
|---|---|
| | • **Authentication and Privacy** - аутентификация и шифрование |

**Рекомендации по безопасности:**

1. Для разных уровней доступа создавайте отдельные группы
2. Для SNMPv3 всегда используйте Authentication and Privacy
3. Ограничивайте Write-права минимально необходимыми OID
4. Регулярно пересматривайте назначенные права

**Пример создания группы:**

1. Перейдите в раздел Management > SNMP > Group;
2. Нажмите "Add";
3. Заполните параметры:
    - Group: network_admins
    - Version: SNMPv3
    - Security Level: Authentication and Privacy
    - Read View: full_access
    - Write View: config_access
    - Notify View: trap_events
4. Нажмите "Apply"

**Внимание!** Для SNMPv1/v2c community-строка выступает в роли аутентификатора. Используйте сложные community-строки вместо стандартных "public"/"private".

### 17.4.3. Настройка SNMP community (Community)

Для настройки параметров SNMP community перейдите:

**Management > SNMP > Community**

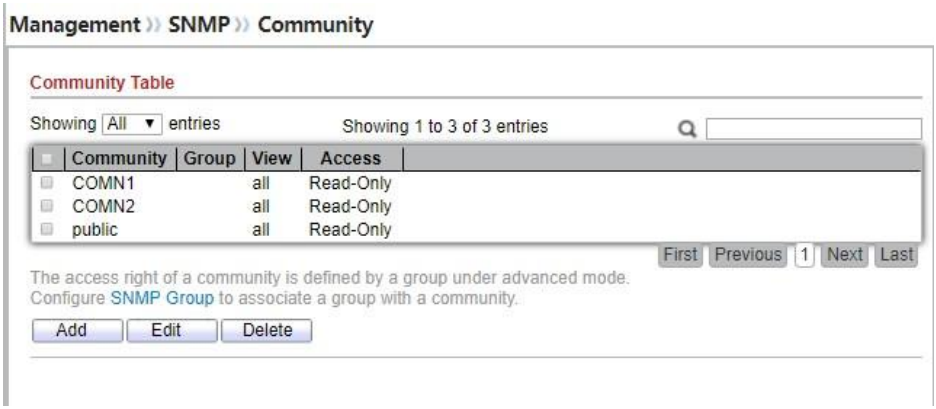
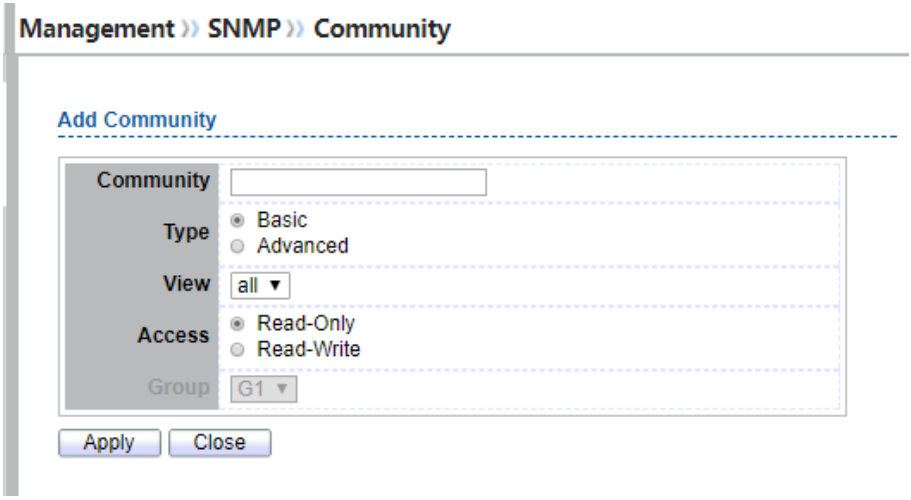


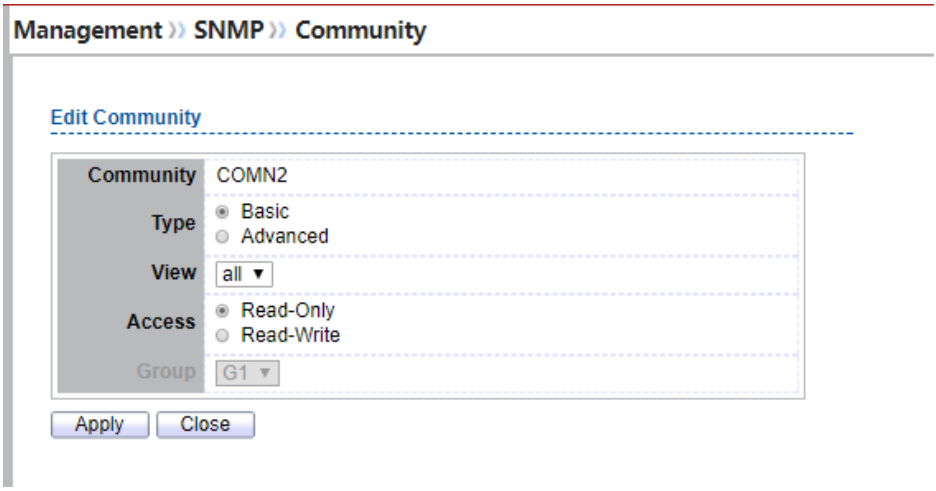

***Таблица SNMP community***

| Параметр | Описание |
|---|---|
| **Community** | Имя SNMP community (до 20 символов) |
| **Group** | Связанная SNMP-группа (в Advanced-режиме) |
| **View** | SNMP view для доступа (в Basic-режиме) |
| **Access** | Уровень доступа:<br>• **Read-Only** (только чтение)<br>• **Read-Write** (чтение и запись) |




***Диалог добавления SNMP community***

| Параметр | Описание |
|---|---|
| **Community** | Имя SNMP community (до 20 символов) |
| **Type** | Режим работы SNMP community:<br>• **Basic** - прямое назначение прав<br>• **Advanced** - привязка к группе |
| **View** | SNMP view |
| **Access** | Уровень доступа:<br>• **Read-Only** (только чтение)<br>• **Read-Write** (чтение и запись) |




***Диалог редактирования SNMP community***

| Параметр | Описание |
|---|---|
| **Community** | Имя SNMP community (до 20 символов) |
| **Type** | Режим работы SNMP community:<br>• **Basic** - прямое назначение прав<br>• **Advanced** - привязка к группе |
| **View** | SNMP view |
| **Access** | Уровень доступа:<br>• **Read-Only** (только чтение)<br>• **Read-Write** (чтение и запись) |

**Рекомендации по безопасности:**

1. Никогда не используйте стандартные имена (public/private)
2. Для разных устройств используйте разные community-строки
3. Регулярно обновляйте community-строки (каждые 3-6 месяцев)
4. Для записи используйте сложные строки длиной не менее 12 символов

**Пример настройки (Basic-режим):**

1. Перейдите в раздел Management > SNMP > Community;
2. Нажмите "Add";
3. Заполните параметры:
    - Community: N3tW0rk_M0n1t0r
    - Type: Basic
    - View: read_only_view
    - Access: Read-Only
4. Нажмите "Apply"

**Пример настройки (Advanced-режим):**

1. Перейдите в раздел Management > SNMP > Community;
2. Нажмите "Add";
3. Заполните параметры:
    - Community: C0nF1g_Adm1n
    - Type: Advanced
    - Group: config_admins
4. Нажмите "Apply"

**Внимание!** В Advanced-режиме права доступа наследуются от связанной SNMP-группы. Этот режим рекомендуется для сложных конфигураций.

### 17.4.4. Пользователи SNMP (User)

Для настройки параметров SNMP-пользователей перейдите в раздел:

**Management > SNMP > User**

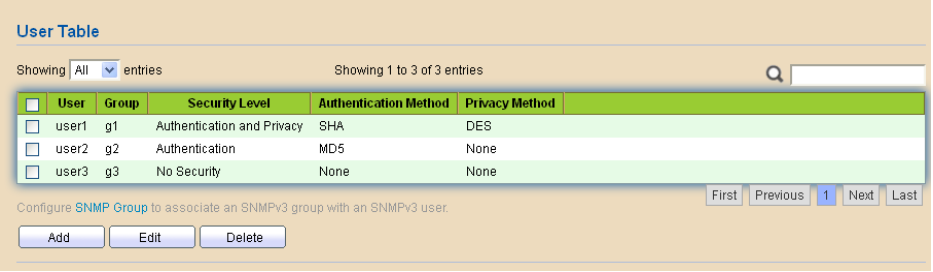
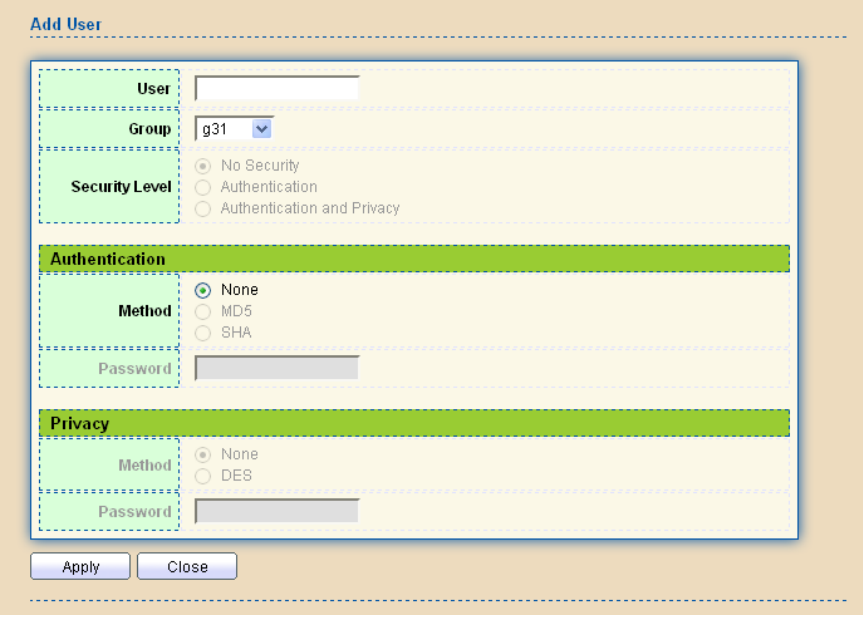



***Таблица SNMP пользователей***

| Параметр | Описание |
|---|---|
| **User** | Имя пользователя (до 30 символов). Для SNMPv1/v2c должно совпадать с community-строкой |
| **Group** | Группа SNMP, к которой принадлежит пользователь |
| **Security Level** | Уровень безопасности:<br>• **No Security** - без защиты<br>• **Authentication** - только аутентификация<br>• **Authentication and Privacy** - аутентификация и шифрование |
| **Authentication Method** | Метод аутентификации:<br>• **None** (отсутствует)<br>• **MD5** (HMAC-MD5-96) |

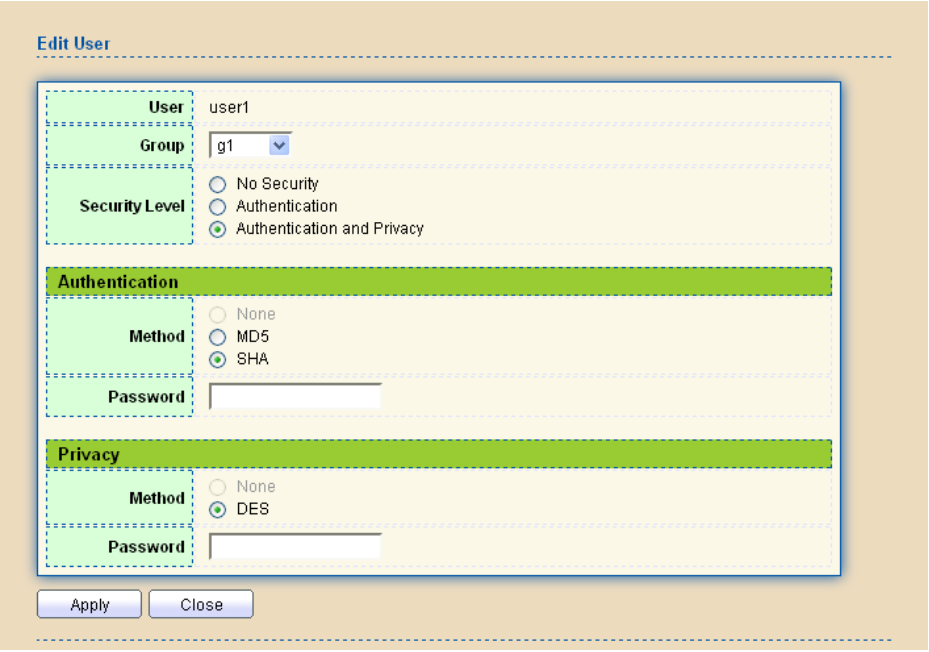
| Параметр | Описание |
|---|---|
| | • **SHA** (HMAC-SHA-96) |
| **Privacy Method** | Метод шифрования:<br>• **None** (отсутствует)<br>• **DES** |




***Диалог добавления нового пользователя SNMP***

| Параметр | Описание |
|---|---|
| **User** | Имя пользователя (до 30 символов). Для SNMPv1/v2c должно совпадать с community-строкой |

| Параметр | Описание |
|---|---|
| **Group** | Группа SNMP, к которой принадлежит пользователь |
| **Security Level** | Уровень безопасности:<br>• **No Security** - без защиты<br>• **Authentication** - только аутентификация<br>• **Authentication and Privacy** - аутентификация и шифрование |
| **Authentication** | |
| **Method** | Метод аутентификации:<br>• **None** (отсутствует)<br>• **MD5** (HMAC-MD5-96)<br>• **SHA** (HMAC-SHA-96) |
| **Password** | Пароль аутентификации (8-32 символа) |
| **Privacy** | |
| **Method** | Метод шифрования:<br>• **None** (отсутствует)<br>• **DES** |
| **Password** | Пароль шифрования (8-64 символа) |




***Диалог редактирования пользователя SNMP***

| Параметр | Описание |
|---|---|
| **User** | Имя пользователя (до 30 символов). Для SNMPv1/v2c должно совпадать с community-строкой |
| **Group** | Группа SNMP, к которой принадлежит пользователь |
| **Security Level** | Уровень безопасности:<br>• **No Security** - без защиты<br>• **Authentication** - только аутентификация<br>• **Authentication and Privacy** - аутентификация и шифрование |

| Параметр | Описание |
|---|---|
| **Authentication** | |
| **Method** | Метод аутентификации:<br>• **None** (отсутствует)<br>• **MD5** (HMAC-MD5-96)<br>• **SHA** (HMAC-SHA-96) |
| **Password** | Пароль аутентификации (8-32 символа) |
| **Privacy** | |
| **Method** | Метод шифрования:<br>• **None** (отсутствует)<br>• **DES** |
| **Password** | Пароль шифрования (8-64 символа) |

**Рекомендации по безопасности:**

1. Для SNMPv3 всегда используйте:
    - Security Level: Authentication and Privacy
    - Authentication Method: SHA
    - Privacy Method: DES
2. Пароли должны:
    - Быть не менее 12 символов
    - Содержать буквы, цифры и спецсимволы
    - Не совпадать с другими учетными данными

**Пример создания пользователя:**

1. Перейдите в раздел Management > SNMP > User;
2. Нажмите "Add";
3. Заполните параметры:
    - User: netadmin_snmp
    - Group: network_admins
    - Security Level: Authentication and Privacy
    - Authentication Method: SHA
    - Password: Str0ngAuthP@ss!
    - Privacy Method: DES
    - Privacy Password: EvenStr0ngerPriv@cy
4. Нажмите "Apply"

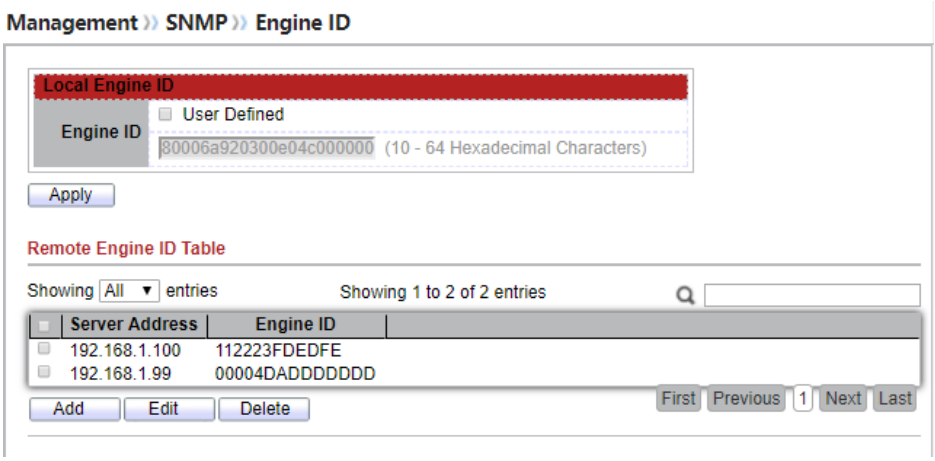
**Внимание!**

- Для SNMPv1/v2c настройки аутентификации и шифрования недоступны
- Пароли хранятся в зашифрованном виде в конфигурации
- Регулярно обновляйте пароли (рекомендуется каждые 3-6 месяцев)

### 17.4.5. Идентификатор Engine (Engine ID)

Для настройки локального и удаленного Engine ID перейдите:

**Management > SNMP > Engine ID**

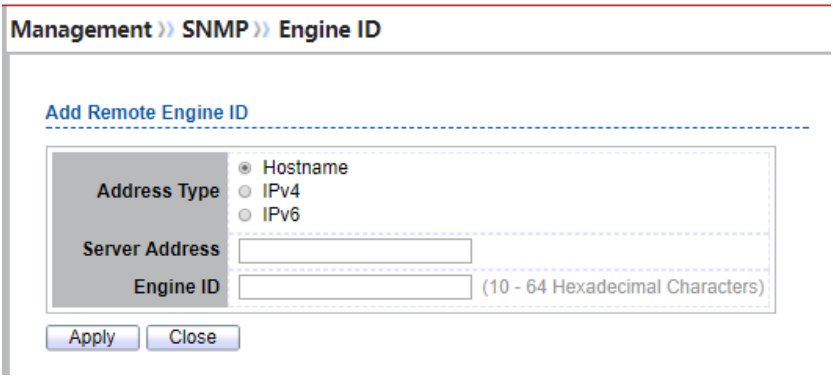



***Локальный Engine ID***

| Параметр | Описание |
|---|---|
| **Engine ID** | Режим определения:<br>• **User Defined** - ручной ввод (10-64 hex-символов, четное количество)<br>• **По умолчанию** - автоматическая генерация на основе MAC-адреса и Enterprise ID |

*Таблица удаленных Engine ID*

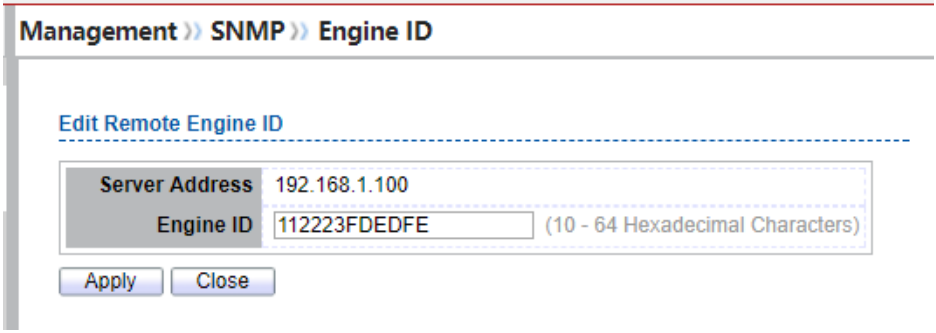
| Параметр | Описание |
|---|---|
| **Server Address** | Адрес удаленного хоста |
| **Engine ID** | Идентификатор Engine удаленного SNMP-устройства (10-64 hex-символов) |




*Диалог добавления Engine ID*

| Параметр | Описание |
|---|---|
| **Address Type** | Тип адреса<br>• Hostname<br>• IPv4<br>• IPv6 |
| **Server Address** | Адрес удаленного хоста |

| Параметр | Описание |
|---|---|
| **Engine ID** | Идентификатор Engine удаленного SNMP-устройства (10-64 hex-символов) |




**Диалог изменения существующего Engine ID**

| Параметр | Описание |
|---|---|
| **Server Address** | Адрес удаленного хоста |
| **Engine ID** | Идентификатор Engine удаленного SNMP-устройства (10-64 hex-символов) |

**Рекомендации:**

1. Для совместимости между устройствами:
    - Используйте одинаковый формат Engine ID в пределах одной сети
    - Регистрируйте назначенные ID в документации
2. При ручной настройке:

- Используйте осмысленные hex-значения
- Включайте идентификатор организации
- Сохраняйте записи о назначенных ID

**Пример настройки:**

1. Перейдите в раздел Management > SNMP > Engine ID;
2. Для локального Engine ID:
    - Выберите "User Defined"
    - Введите: 800007C00008ABCDEF12 (пример)
3. Для удаленного Engine ID:
    - Нажмите "Add"
    - Укажите:
        - Address Type: IPv4
        - Server Address: 192.168.1.100
        - Engine ID: 800007C00009FEDCBA98
    - Нажмите "Apply"

**Примечание:**

- Engine ID используется для безопасного обмена SNMPv3-сообщениями
- Изменение Engine ID сбрасывает все SNMPv3-ключи
- Для генерации ID можно использовать MAC-адрес устройства с префиксом предприятия

### 17.4.6. Настройка SNMP Trap Event (Trap Event)

Для настройки SNMP-трапов событий перейдите в следующий раздел:

**Management > SNMP > Trap Event**


***Настройки трапов SNMP***

| Параметр | Описание |
|---|---|
| **Authentication Failure** | Генерация трапа при ошибке аутентификации (неверный community или пароль) |
| **Link Up/Down** | Трапы изменения состояния линка порта (up/down) |
| **Cold Start** | Трап при перезагрузке устройства по команде пользователя |
| **Warm Start** | Трап при перезагрузке устройства из-за сбоя питания |

**Рекомендации по настройке:**

1. Обязательные SNMP трапы для мониторинга:
    - Link Up/Down - для отслеживания состояния портов
    - Authentication Failure - для выявления попыток несанкционированного доступа
2. Дополнительные настройки:
    - Для Cold/Warm Start укажите корректные community-строки
    - Настройте корректные адреса NMS-серверов

**Пример включения SNMP трапов:**

1. Перейдите в раздел Management > SNMP > Trap Event;
2. Активируйте нужные события:
    - ☑ Authentication Failure
    - ☑ Link Up/Down
    - ☑ Cold Start
3. Нажмите "Apply"

**Внимание!** Для работы трапов необходимо предварительно настроить:

- SNMP-community (для v1/v2c) или пользователей (для v3)
- Корректные Engine ID для SNMPv3

### 17.4.7. Уведомления SNMP (Notification)

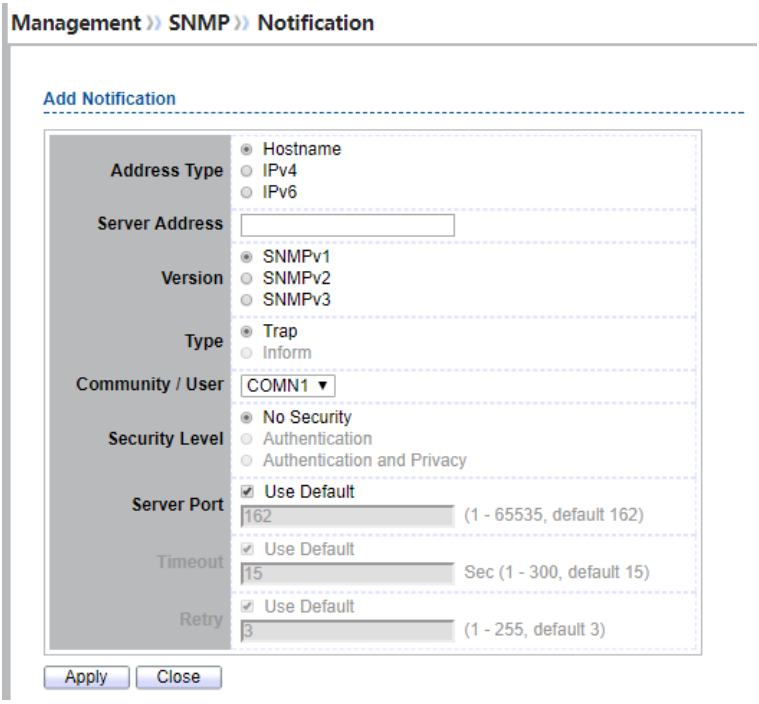
Для настройки получателей SNMP-уведомлений перейдите:

**Management > SNMP > Notification**


***Таблица уведомлений SNMP***

| Параметр | Описание |
|---|---|
| **Server Address** | IP-адрес или имя хоста получателя |
| **Server Port** | UDP-порт получателя (по умолчанию 162) |
| **Timeout** | Таймаут между SNMP уведомлениями (по умолчанию 15 сек) |
| **Retry** | Счетчик попыток SNMP уведомлений (по умолчанию 3) |
| **Version** | Версия SNMP:<br>• **SNMPv1**<br>• **SNMPv2**<br>• **SNMPv3** |

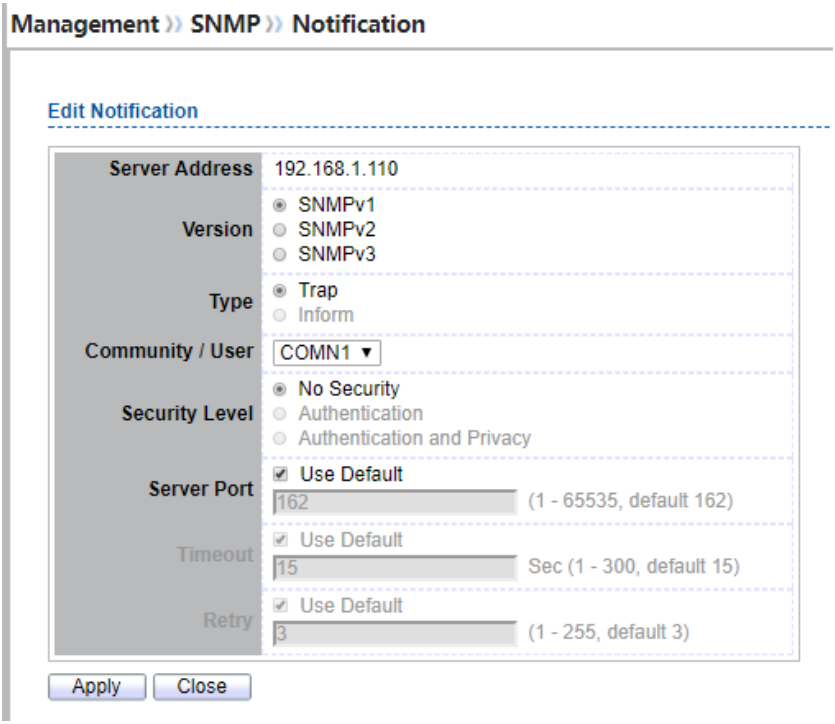
| Параметр | Описание |
|---|---|
| **Type** | Тип уведомления:<br>• **Trap** (однонаправленные)<br>• **Inform** (с подтверждением) |
| **Community/User** | Community-строка (SNMP v1/v2) или имя пользователя (SNMP v3) |
| **Security Level** | Уровень безопасности (SNMP v3):<br>• **No Security** – без аутентификации<br>• **Authentication** – аутентификация<br>• **Authentication and Privacy** – аутентификация и шифрование. |



***Диалог добавления SNMP уведомлений***

| Параметр | Описание |
|---|---|
| **Address Type** | Тип адреса<br>• Hostname<br>• IPv4<br>• IPv6 |
| **Server Address** | IP-адрес или имя хоста получателя |
| **Version** | Версия SNMP:<br>• **SNMPv1**<br>• **SNMPv2**<br>• **SNMPv3** |
| **Type** | Тип уведомления:<br>• **Trap** (однонаправленные)<br>• **Inform** (с подтверждением) |
| **Community/User** | Community-строка (SNMP v1/v2) или имя пользователя (SNMP v3) |
| **Security Level** | Уровень безопасности (SNMP v3):<br>• **No Security** – без аутентификации<br>• **Authentication** – аутентификация<br>• **Authentication and Privacy** – аутентификация и шифрование. |
| **Server Port** | UDP-порт получателя (по умолчанию 162) |
| **Timeout** | Таймаут между SNMP уведомлениями (по умолчанию 15 сек) |

| Параметр | Описание |
| --- | --- |
| **Retry** | Счетчик попыток SNMP уведомлений (по умолчанию 3) |




***Диалог изменения SNMP уведомлений***

| Параметр | Описание |
| --- | --- |
| **Address Type** | Тип адреса<br>• Hostname<br>• IPv4<br>• IPv6 |

| Параметр | Описание |
| --- | --- |
| **Server Address** | IP-адрес или имя хоста получателя |
| **Version** | Версия SNMP:<br>• **SNMPv1**<br>• **SNMPv2**<br>• **SNMPv3** |
| **Type** | Тип уведомления:<br>• **Trap** (однонаправленные)<br>• **Inform** (с подтверждением) |
| **Community/User** | Community-строка (SNMP v1/v2) или имя пользователя (SNMP v3) |
| **Security Level** | Уровень безопасности (SNMP v3):<br>• **No Security** – без аутентификации<br>• **Authentication** – аутентификация<br>• **Authentication and Privacy** – аутентификация и шифрование. |
| **Server Port** | UDP-порт получателя (по умолчанию 162) |
| **Timeout** | Таймаут между SNMP уведомлениями (по умолчанию 15 сек) |
| **Retry** | Счетчик попыток SNMP уведомлений (по умолчанию 3) |

**Рекомендации:**

1. Для критически важных уведомлений используйте Inform (с подтверждением)
2. Разделяйте трапы по версиям и получателям:
    - SNMPv1/v2c - для legacy-систем (устаревших)
    - SNMPv3 - для безопасной передачи
3. Для SNMPv3 всегда используйте максимальный уровень безопасности

**Пример настройки:**

1. Перейдите в раздел Management > SNMP > Notification;
2. Нажмите "Add";
3. Заполните параметры:
    - Address Type: IPv4
    - Server Address: 192.168.1.200
    - Version: SNMPv3
    - Type: Inform
    - User: snmp_admin
    - Security Level: Authentication and Privacy
    - Server Port: 162 (default)
    - Timeout: 20 (сек)
    - Retry: 5
4. Нажмите "Apply"

**Внимание!**

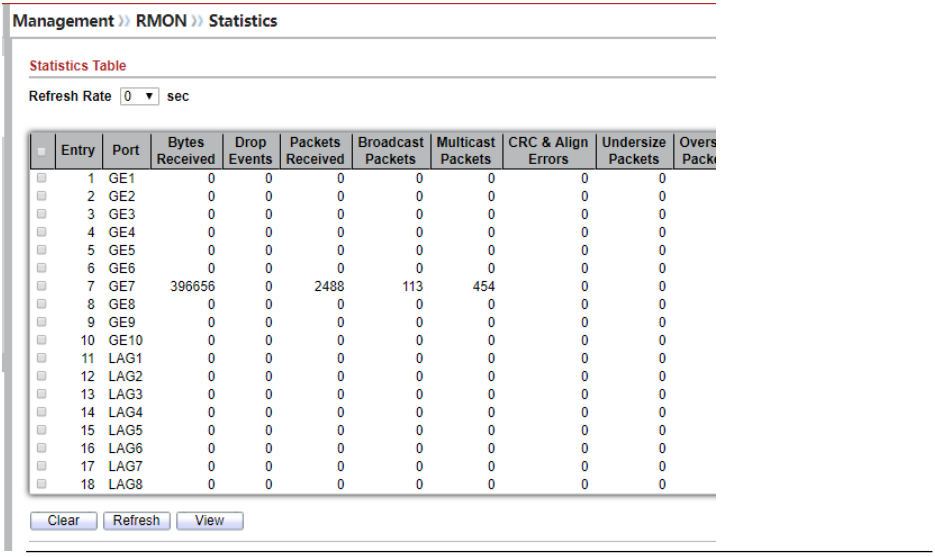
- SNMPv1 не поддерживает Inform-сообщения
- Для Inform-сообщений требуется больше ресурсов коммутатора
- Убедитесь, что брандмауэр разрешает трафик на указанный порт

## 17.5. Настройка RMON (Remote Monitoring)

### 17.5.1. Статистика RMON (Statistics)

Для просмотра RMON-статистики перейдите в следующий раздел WEB интерфейса:

**Management > RMON > Statistics**




| Entry | Port | Bytes Received | Drop Events | Packets Received | Broadcast Packets | Multicast Packets | CRC & Align Errors | Undersize Packets | Overs Packe |
|---|---|---|---|---|---|---|---|---|---|
| 1 | GE1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 2 | GE2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 3 | GE3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 4 | GE4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 5 | GE5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 6 | GE6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 7 | GE7 | 396656 | 0 | 2488 | 113 | 454 | 0 | 0 | |
| 8 | GE8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 9 | GE9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 10 | GE10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 11 | LAG1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 12 | LAG2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 13 | LAG3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 14 | LAG4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 15 | LAG5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 16 | LAG6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 17 | LAG7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 18 | LAG8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |

***Таблица статистики RMON***

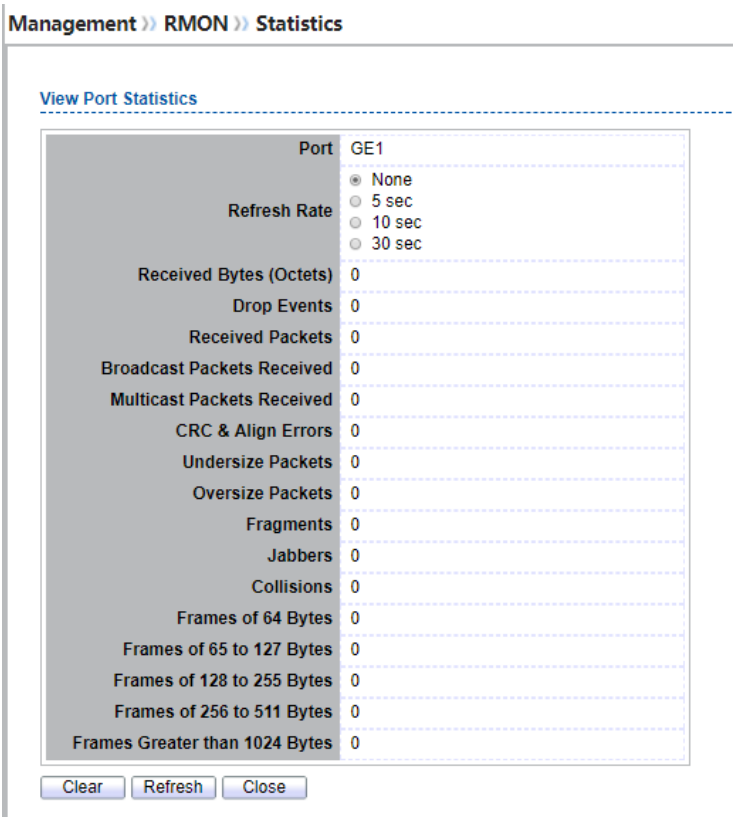
| Параметр | Описание |
|---|---|
| **Entry** | Номер записи в таблице |
| **Port** | Номер порта |

| Параметр | Описание |
|---|---|
| **Bytes Received** | Общее количество полученных байт (включая ошибки) |
| **Drop Events** | Количество отброшенных пакетов |
| **Packets Received** | Общее количество полученных пакетов |
| **Broadcast Packets** | Количество широковещательных пакетов |
| **Multicast Packets** | Количество multicast-пакетов |
| **CRC & Align Errors** | Ошибки CRC (контрольной суммы) и выравнивания |
| **Undersize Packages** | Пакеты менее 64 байт |
| **Oversize Packages** | Пакеты более 1518 байт |
| **Fragments** | Фрагментированные пакеты (<64 байт без ошибок) |
| **Jabbers** | Ошибочные пакеты (>1632 байт) |
| **Collision** | Количество коллизий |
| **Frames of 64 Bytes** | Количество полученных пакетов размером до 64 байт |

| Параметр | Описание |
|---|---|
| **Frames of 65 to 127 Bytes** | Количество полученных пакетов размером от 65 до 127 байт |
| **Frames of 128 to 255 Bytes** | Количество полученных пакетов размером от 128 до 256 байт |
| **Frames of 256 to 511 Bytes** | Количество полученных пакетов размером от 256 до 511 байт |
| **Frames of 512 to 1024 Bytes** | Количество полученных пакетов размером от 512 до 1024 байт |
| **Frames Greater than 1024 Bytes** | Количество полученных пакетов размером более 1024 байт |

***Управление***

| Кнопка | Описание |
|---|---|
| **Clear** | Сброс статистики для выбранных портов |
| **View** | Просмотр детальной статистики на выбранном порту |




**Рекомендации по анализу данных:**

1. Мониторинг ошибок:
    - **CRC & Align Errors** > 1% от общего трафика - проверить кабель/порт
    - **Collision** > 5% - возможны проблемы в сети
2. Анализ распределения:
    - Преобладание **64 Bytes** - может указывать на атаки на сеть
    - Высокий % **Broadcast** пакетов (>20%) - возможен broadcast storm

**Пример использования:**

1. Перейдите в раздел Management > RMON > Statistics;
2. Выберите интересующий порт;
3. Нажмите **View** для детальной статистики;
4. Проанализируйте:
    - Общий объем трафика (Bytes Received)
    - Процент ошибок (CRC & Align Errors)
    - Распределение по размерам пакетов
5. Для сброса статистики нажмите **Clear**

**Внимание!** Статистика собирается с момента последнего сброса или включения порта. Для долгосрочного мониторинга используйте SNMP-мониторинг с внешней системой (Zabbix и т.д.)

### 17.5.2. История RMON (History)

Для настройки и просмотра RMON-истории перейдите:

**Management > RMON > History**

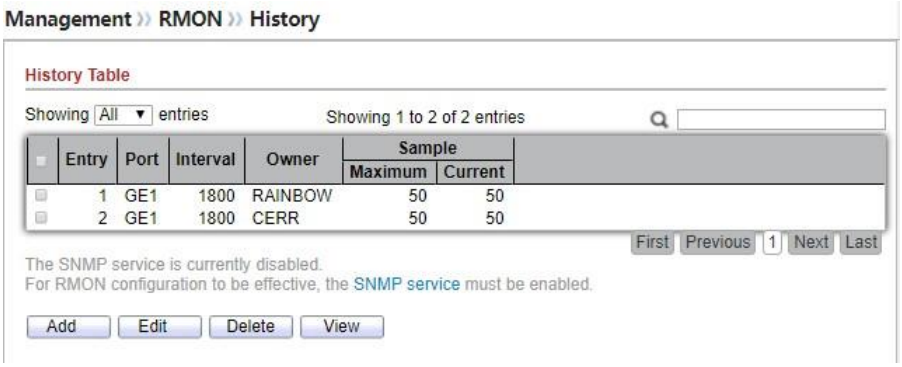
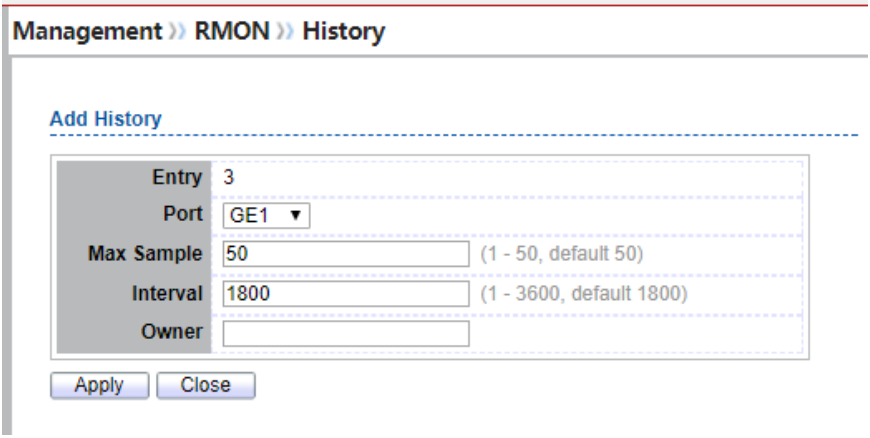


***Таблица RMON***

| Параметр | Описание |
|---|---|
| **Entry** | Номер записи |
| **Port** | Номер порта для мониторинга |
| **Interval** | Интервал сбора данных (в секундах) |
| **Owner** | Владелец записи (0-31 символ) |
| **Max Sample** | Максимальное количество хранимых образцов |
| **Current Sample** | Текущее количество собранных образцов |

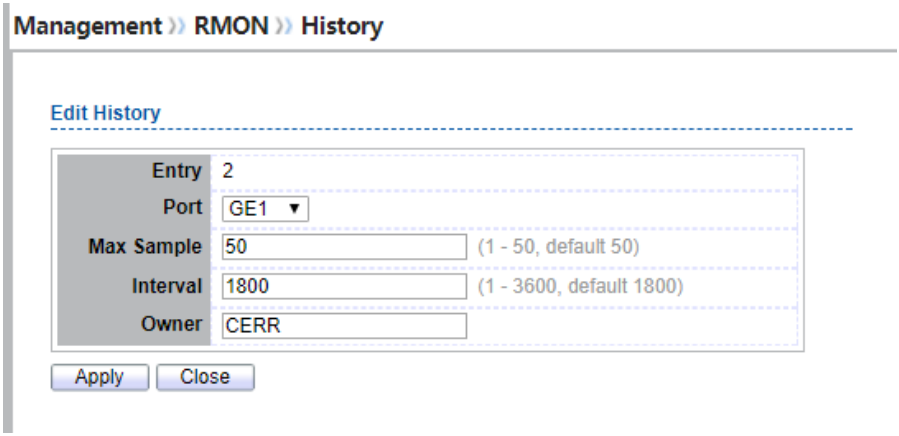
***Управление записями***

| Кнопка | Описание |
|---|---|
| **Add** | Добавить новую запись мониторинга |
| **Edit** | Изменить параметры сбора |
| **Delete** | Удалить запись мониторинга |
| **View** | Просмотр собранных данных |



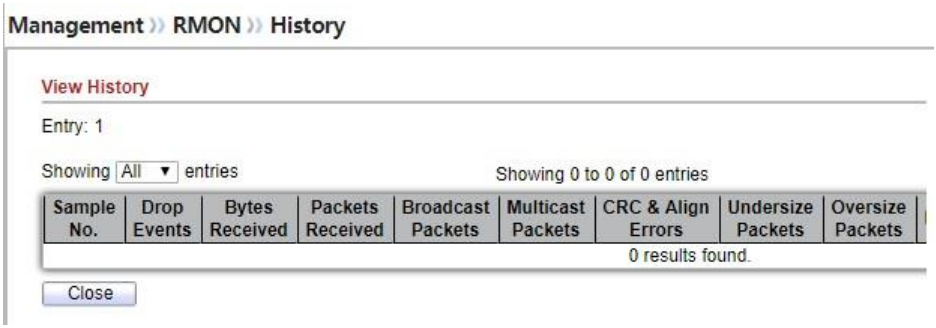

***Диалог добавления записи RMON***

| Параметр | Описание |
|---|---|
| **Entry** | Номер записи |
| **Port** | Номер порта для мониторинга |
| **Max Sample** | Максимальное количество хранимых образцов (1-50) |
| **Interval** | Интервал сбора данных (в секундах, 1 – 3600сек) |
| **Owner** | Владелец записи (0-31 символ) |




***Диалог редактирования записи RMON***

| Параметр | Описание |
|---|---|
| **Entry** | Номер записи |
| **Port** | Номер порта для мониторинга |
| **Max Sample** | Максимальное количество хранимых образцов (1-50) |
| **Interval** | Интервал сбора данных (в секундах, 1 – 3600сек) |
| **Owner** | Владелец записи (0-31 символ) |




***Параметры журнала RMON History***

| Параметр | Описание |
|---|---|
| **Sample No.** | Номер образца |
| **Drop Events** | Количество отброшенных пакетов |
| **Bytes Received** | Общее количество полученных байт |
| **Packets Received** | Общее количество полученных пакетов (включая ошибочные, multicast и broadcast) |
| **Broadcast Packets** | Количество корректных broadcast-пакетов (без учета multicast) |
| **Multicast packets** | Количество корректных multicast-пакетов |
| **CRC & Align** | Ошибки передачи данных |

| Параметр | Описание |
|---|---|
| **Errors** | |
| **Undersize Packages** | Количество пакетов размером менее 64 октетов |
| **Oversize Packages** | Количество пакетов размером более 1518 октетов |
| **Fragments** | Количество фрагментированных пакетов (<64 октетов, исключая служебные биты, но включая FCS) |
| **Jabbers** | Количество ошибочных пакетов (>1632 октетов), соответствующих критериям:<br>• Длина пакета превышает MRU<br>• Неверная CRC (контрольная сумма пакета)<br>• Не обнаружены RX-ошибки |
| **Utilization** | Процент использования пропускной способности порта |

**Рекомендации по настройке:**

1. Оптимальные параметры сбора данных:
    - **Interval**: 30-300 сек для долгосрочного анализа
    - **Max Sample**: 50-100 записей для недельного мониторинга
2. Для критичных портов:
    - Уменьшите интервал сбора (10-30 сек)
    - Увеличьте количество образцов (150-200)

**Пример настройки:**

1. Перейдите в раздел Management > RMON > History;
2. Нажмите "Add"
3. Заполните параметры:
    - Port: GE24
    - Interval: 60
    - Max Sample: 1440 (сутки с минутным интервалом)
    - Owner: Network_Admin
4. Нажмите "Apply"

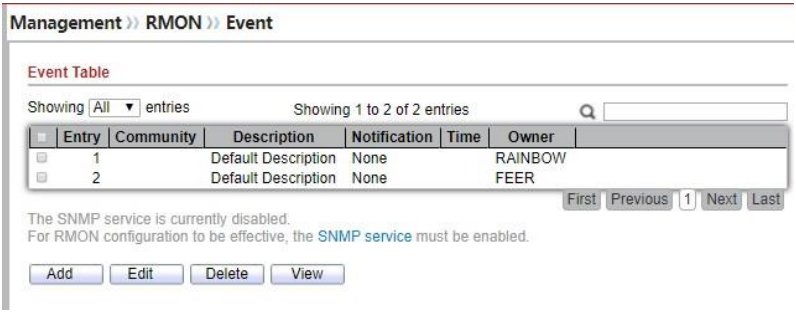
**Внимание!**

- Данные сохраняются до перезагрузки коммутатора
- Для долговременного хранения используйте внешние системы мониторинга
- Высокий % Utilization (>70%) требует анализа и оптимизации трафика

### 17.5.3. События RMON (Event)

Для настройки RMON-событий перейдите в следующий раздел WEB интерфейса коммутатора:

**Management > RMON > Event**



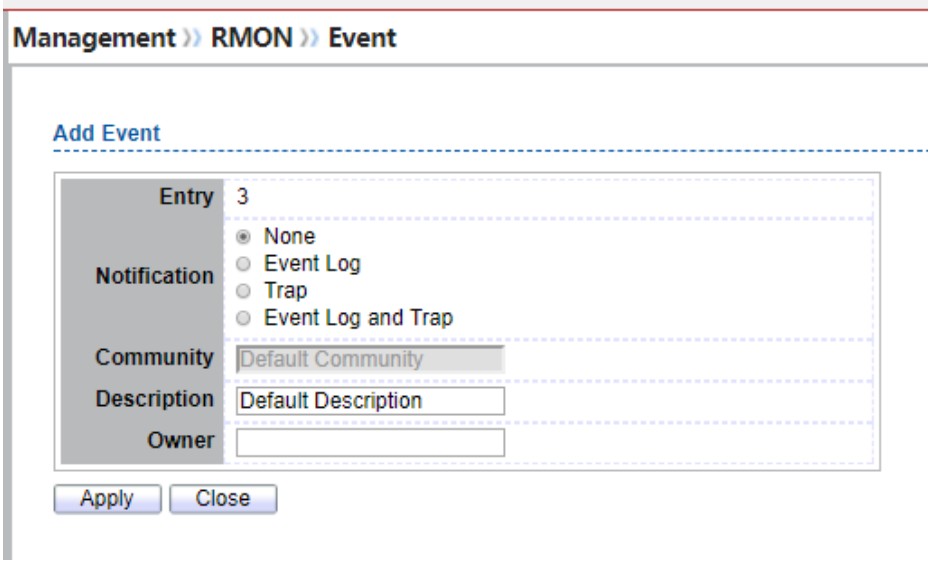

***Основные параметры событий***

| Параметр | Описание |
|---|---|
| **Entry** | Номер записи в журнале |
| **Community** | SNMP-community для отправки trap-сообщений |
| **Description** | Описание события (до 255 символов) |
| **Notification** | Тип уведомления:<br>• None - без уведомления<br>• Event Log - запись в лог<br>• Trap - отправка SNMP-trap<br>• Event Log and Trap - запись + trap |

| Параметр | Описание |
|---|---|
| **Time** | Время срабатывания события |
| **Owner** | Владелец события (до 31 символа) |

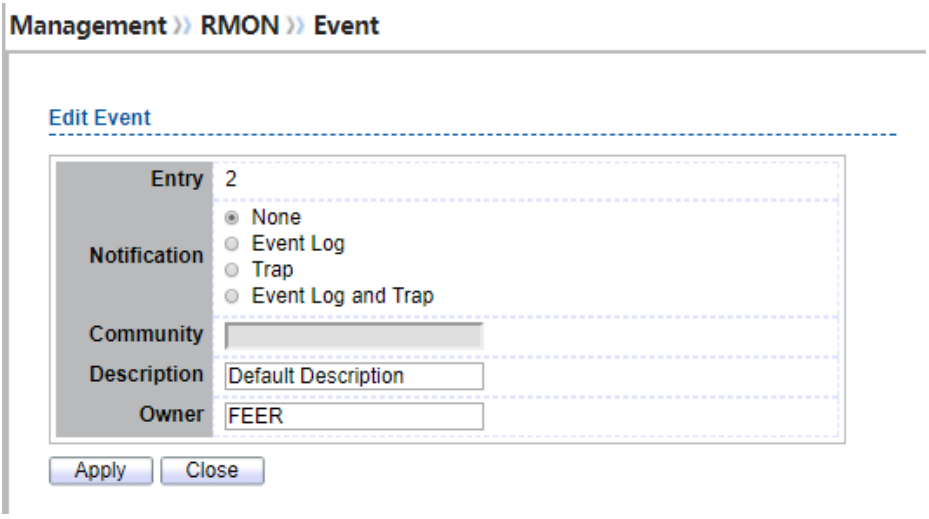
***Управление событиями (описание кнопок)***

| Действие (кнопка) | Описание |
|---|---|
| **Add** | Добавить новое событие |
| **Edit** | Изменить параметры события |
| **Delete** | Удалить событие |



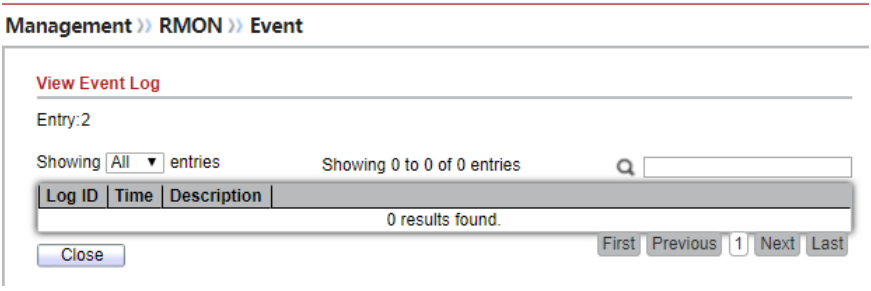
*Диалог добавления события RMON*

| Параметр | Описание |
|---|---|
| **Notification** | Тип уведомления:<br>• None - без уведомления<br>• Event Log - запись в лог<br>• Trap - отправка SNMP-trap<br>• Event Log and Trap - запись + trap |
| **Community** | SNMP-community для отправки trap-сообщений |
| **Description** | Описание события (до 255 символов) |
| **Owner** | Владелец события (до 31 символа) |



***Диалог изменения события RMON***

| Параметр | Описание |
|---|---|
| **Notification** | Тип уведомления:<br>• None - без уведомления<br>• Event Log - запись в лог<br>• Trap - отправка SNMP-trap<br>• Event Log and Trap - запись + trap |
| **Community** | SNMP-community для отправки trap-сообщений |
| **Description** | Описание события (до 255 символов) |
| **Owner** | Владелец события (до 31 символа) |




***Параметры журнала событий***

| Параметр | Описание |
|---|---|
| **Log ID** | Уникальный идентификатор записи |
| **Time** | Время возникновения события |

| Параметр | Описание |
|---|---|
| **Description** | Описание зарегистрированного события |

**Рекомендации по настройке:**

1. Для критических событий используйте "Event Log and Trap"
2. Настройте разные сообщества для:
    - Информационных событий (read-only)
    - Критических событий (read-write)
3. Используйте описательные имена владельцев:
    - "Network_Monitoring"
    - "Security_Alerts"

**Пример настройки:**

1. Перейдите в раздел Management > RMON > Event
2. Нажмите "Add" (добавить)
3. Заполните параметры:
    - Description: "High Port Utilization >80%"
    - Notification: Event Log and Trap
    - Community: critical_traps
    - Owner: Network_Operations
4. Нажмите "Apply" (принять)

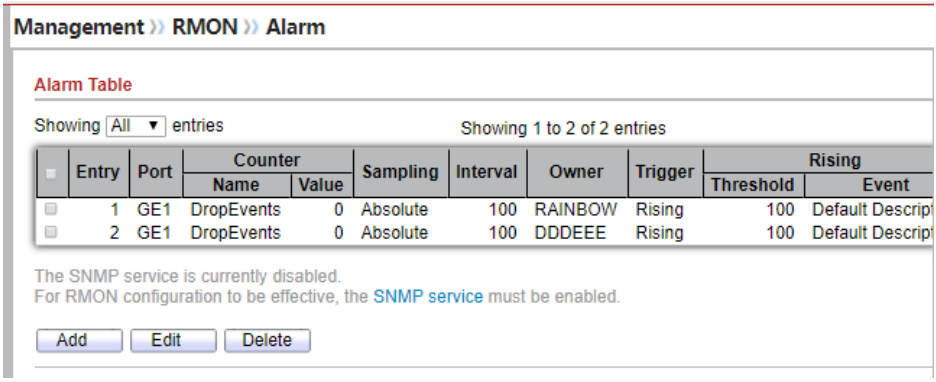
**Внимание!**

- Для работы trap-уведомлений должна быть настроена SNMP-инфраструктура
- Логи событий сохраняются до перезагрузки устройства
- Регулярно экспортируйте логи для долговременного хранения

### 17.5.4. Тревожные сообщения RMON (Alarm)

Для настройки RMON-тревожный сообщений перейдите в следующий раздел WEB интерфейса:

**Management > RMON > Alarm**

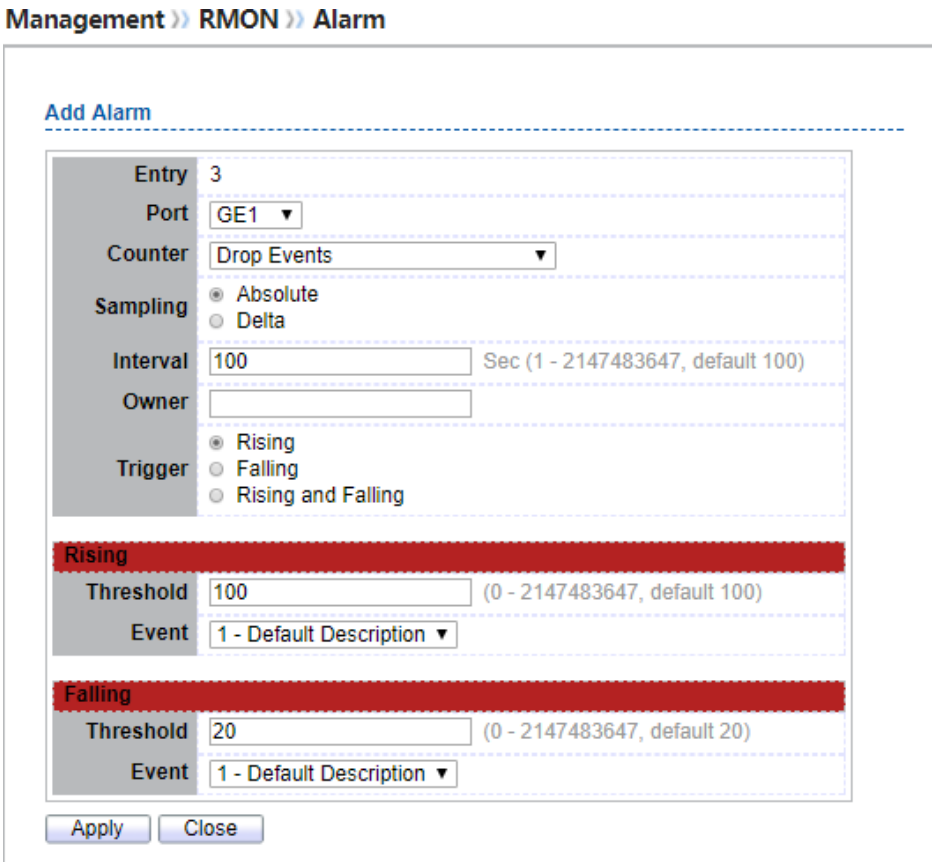



***Основные параметры тревожных собщений RMON***

| Параметр | Описание |
|---|---|
| **Entry** | Номер записи |
| **Port** | Порт для мониторинга |
| **Counter** | Счетчик отслеживаемых событий:<br>• Drop Events – отброшенные пакеты<br>• Received Bytes – принятые байты<br>• Received Packets – принятые пакеты<br>• Broadcast Packets – пакеты broadcast-трафика |

| Параметр | Описание |
|---|---|
| | • Multicast Packets – пакеты multicast-трафик<br>• CRC and Align Error – ошибки CRC суммы<br>• Undersize Packets – пакеты размером <64 байт<br>• Oversize Packets – пакеты размером >1518 байт<br>• Fragments – общее кол-во фрагментированных пакетов<br>• Jabbers – общее вол-во ошибочных пакетов<br>• Collisions – коллизии<br>• Pkts64Octetes – кол-во пакетов размером 64 байта<br>• Pkts65to127Octetes – кол-во пакетов размером от 65 до 127 байт<br>• Pkts128to255Octetes – кол-во пакетов размером от 128 до 255 байт<br>• Pkts256to511Octetes – кол-во пакетов размером от 256 до 511 байт<br>• Pkts512to1023Octetes – кол-во пакетов размером от 512 до 1023 байт<br>• Pkts1024to1518Octetes – кол-во пакетов размером от 1024 до 1518 байт |
| **Sampling** | Тип сэмплирования:<br>• Absolute - абсолютное значение<br>• Delta - разница с предыдущим замером |
| **Interval** | Интервал проверки (в секундах) |
| **Owner** | Владелец алерта (до 31 символа) |

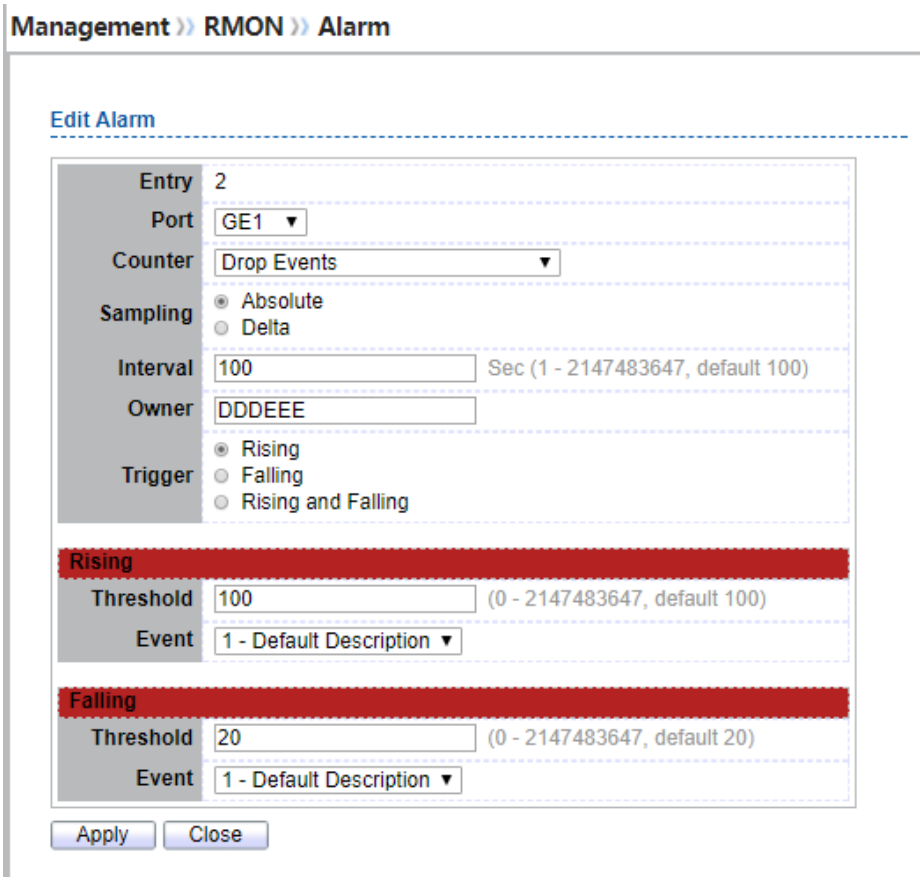
| Параметр | Описание |
|---|---|
| **Trigger** | Параметр срабатывания тревоги RMON |
| **Rising** | • Rising Threshold – Порог срабатывания "тревоги"<br>• Rising Event – Событие при превышении порога |
| **Falling** | • Falling Threshold – Порог срабатывания "нормы"<br>• Falling Event – Событие при возврате к норме |



***Диалог добавления тревожных собщений RMON***

| Параметр | Описание |
|---|---|
| **Port** | Порт для мониторинга |
| **Counter** | Счетчик отслеживаемых событий:<br>• Drop Events – отброшенные пакеты<br>• Received Bytes – принятые байты<br>• Received Packets – принятые пакеты<br>• Broadcast Packets – пакеты broadcast-трафика<br>• Multicast Packets – пакеты multicast-трафик<br>• CRC and Align Error – ошибки CRC суммы<br>• Undersize Packets – пакеты размером <64 байт<br>• Oversize Packets – пакеты размером >1518 байт<br>• Fragments – общее кол-во фрагментированных пакетов<br>• Jabbers – общее вол-во ошибочных пакетов<br>• Collisions – коллизии<br>• Pkts64Octetes – кол-во пакетов размером 64 байта<br>• Pkts65to127Octetes – кол-во пакетов размером от 65 до 127 байт<br>• Pkts128to255Octetes – кол-во пакетов размером от 128 до 255 байт<br>• Pkts256to511Octetes – кол-во пакетов размером от 256 до 511 байт<br>• Pkts512to1023Octetes – кол-во пакетов размером от 512 до 1023 байт<br>• Pkts1024to1518Octetes – кол-во пакетов размером от 1024 до 1518 байт |

| Параметр | Описание |
|---|---|
| **Sampling** | Тип сэмплирования:<br>• Absolute - абсолютное значение<br>• Delta - разница с предыдущим замером |
| **Interval** | Интервал проверки (в секундах). Значение по умолчанию 100сек. Допустимый интервал значений 1 – 2147483647 сек |
| **Owner** | Владелец алерта (до 31 символа) |
| **Trigger** | Параметр срабатывания тревоги RMON<br>• Rising – превышение<br>• Falling – возврат к норме<br>• Rising and falling – Превышение и возврат к норме |
| **Rising** | • Rising Threshold – Порог срабатывания "тревоги". По умолчанию 100. Допустимый интервал значений 0 – 2147483647.<br>• Rising Event – Событие при превышении порога |
| **Falling** | • Falling Threshold – Порог срабатывания "нормы". По умолчанию 20. Допустимый интервал значений 0 – 2147483647.<br>• Falling Event – Событие при возврате к норме |




***Диалог изменения тревожных собщений RMON***

| Параметр | Описание |
|---|---|
| **Port** | Порт для мониторинга |
| **Counter** | Счетчик отслеживаемых событий:<br>• Drop Events – отброшенные пакеты<br>• Received Bytes – принятые байты<br>• Received Packets – принятые пакеты |

| Параметр | Описание |
| --- | --- |
| | • Broadcast Packets – пакеты broadcast-трафика<br>• Multicast Packets – пакеты multicast-трафик<br>• CRC and Align Error – ошибки CRC суммы<br>• Undersize Packets – пакеты размером <64 байт<br>• Oversize Packets – пакеты размером >1518 байт<br>• Fragments – общее кол-во фрагментированных пакетов<br>• Jabbers – общее вол-во ошибочных пакетов<br>• Collisions – коллизии<br>• Pkts64Octetes – кол-во пакетов размером 64 байта<br>• Pkts65to127Octetes – кол-во пакетов размером от 65 до 127 байт<br>• Pkts128to255Octetes – кол-во пакетов размером от 128 до 255 байт<br>• Pkts256to511Octetes – кол-во пакетов размером от 256 до 511 байт<br>• Pkts512to1023Octetes – кол-во пакетов размером от 512 до 1023 байт<br>• Pkts1024to1518Octetes – кол-во пакетов размером от 1024 до 1518 байт |
| **Sampling** | Тип сэмплирования:<br>• Absolute - абсолютное значение<br>• Delta - разница с предыдущим замером |
| **Interval** | Интервал проверки (в секундах). Значение по умолчанию 100сек. Допустимый интервал значений 1 – 2147483647 сек |

| Параметр | Описание |
|---|---|
| **Owner** | Владелец алерта (до 31 символа) |
| **Trigger** | Параметр срабатывания тревоги RMON<br>• Rising – превышение<br>• Falling – возврат к норме<br>• Rising and falling – Превышение и возврат к норме |
| **Rising** | • Rising Threshold – Порог срабатывания "тревоги". По умолчанию 100. Допустимый интервал значений 0 – 2147483647.<br>• Rising Event – Событие при превышении порога |
| **Falling** | • Falling Threshold – Порог срабатывания "нормы". По умолчанию 20. Допустимый интервал значений 0 – 2147483647.<br>• Falling Event – Событие при возврате к норме |

**Рекомендации по настройке:**

1. Для критичных портов:
   - Интервал: 30-60 сек
   - Rising Threshold: 80% от критического значения
   - Falling Threshold: 50% от критического значения
2. Примеры порогов:
   - Broadcast: >100 пакетов/сек
   - CRC Errors: >5 ошибок/интервал
   - Utilization: >70%

**Пример настройки:**

1. Перейдите в раздел Management > RMON > Alarm
2. Нажмите "Add" (добавить)
3. Заполните параметры:
    - Port: GE24
    - Counter: CRC and Align Error
    - Sampling: Delta
    - Interval: 60
    - Rising Threshold: 10
    - Rising Event: High_CRC_Error
    - Falling Threshold: 2
    - Owner: Network_Security
4. Нажмите "Apply" (принять)

**Внимание!**

Для работы событий (Events) они должны быть предварительно созданы в разделе Management >RMON > Event.

2 (250804)