RUBEZH

ООО «РУБЕЖ»

Руководство по web-управлению коммутатором оптическим сетевым SONAR SNSO-0208

Редакция 1

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

ARP (Address Resolution Protocol) — протокол преобразования IP-адреса в физический адрес.

Auto-Negotiation — автоматическое согласование скорости и режима дуплекса на обоих концах соединения

Broadcast Storm — избыточная широковещательная рассылка, перегружающая сеть и вызывающая тайм-ауты.

Broadcasting — передача данных всем узлам сети.

CoS (Class of Service) — схема приоритезации 802.1p с диапазоном значений 0-7.

DHCP — динамическая выдача IP-адреса, маски, шлюза и других параметров.

DSCP — шестибитное поле в IP-заголовке, позволяющее разделять трафик на 64 класса.

Ethernet — технология локальной сети с общей шиной или звездой; классическая скорость 10 Мбит/с, Fast Ethernet - до 100 Мбит/с.

Flow Control — механизм согласования скоростей между быстрыми и медленными устройствами.

Frame — пакет с заголовком и хвостовой частью, необходимыми для передачи в физической среде.

Full-Duplex — одновременный прием и передача данных в обоих направлениях согласно IEEE802.3x.

Half-Duplex — передача или прием в каждый момент времени только в одном направлении.

IGMP — механизм установления и поддержания связи между хостами и оборудованием multicast 3-го уровня.

QoS — технология, решающая задачи задержек и перегрузки сети.

Trunking — объединение нескольких портов в одну агрегированную группу для увеличения полосы и надежности.

ToS — поле Type of Service в IP-заголовке, задающее характеристики приоритета.

UDP — ненадежный протокол транспортного уровня без установления соединения.

UTP — неэкранированная витая пара.

1 Введение

1.1 Описание продукта

Коммутатор оптический сетевой Sonar SNSO-0208 (далее — коммутатор) применяется для работы в составе системы оповещения и управления эвакуацией в зданиях и сооружениях и является составной частью комплекса технических средств противопожарной защиты.

Коммутатор устанавливается на DIN-рейку 35 мм или на поверхность. Благодаря увеличенной коммутационной способности коммутатор обеспечивает более эффективную передачу данных и подходит для крупномасштабных сетей.

Коммутатор поддерживает двухстековую архитектуру IPv4/IPv6 и широкий набор функций управления, MAC-таблицу, VLAN, изоляцию портов, защиту от петель, IGMP/MLD Snooping, ERPS, DHCP Client, DHCP Snooping, STP/RSTP/MSTP, 802.1X, QoS, зеркалирование портов, LLDP, статическую маршрутизацию, NTP, а также базовый QinQ и до 128 статических маршрутов.

Для удобства администрирования коммутатор поддерживает SNMP v1/v2/v3, CLI, веб-интерфейс и Telnet. Дополнительно реализованы ACL и механизмы защиты от атак, что повышает безопасность управления.

Коммутатор соответствует стандартам FCC и CE, имеет два входа питания постоянного тока. Охлаждение пассивное.

1.2 Основные возможности

Коммутатор обеспечивает следующие возможности и обладает следующими характеристиками:

- поддержка IEEE802.3, IEEE802.3u, IEEE802.3ab, IEEE802.3z, IEEE802.3ae;
- 8 портов 10/100/1000Base-T PoE + 2 порта 100/1000Base-X SFP;
- поддержка кольцевого резервирования ERPS;
- IGMP Snooping, статическая фильтрация multicast, MLD Snooping;
- DHCP Snooping и защита от ARP-атак и несанкционированных DHCP-серверов;
- NTP для синхронизации времени;
- SNMP v1/v2/v3;
- LLDP;
- ACL для повышения гибкости и безопасности управления сетью;
- QoS для повышения стабильности работы сети;
- зеркалирование портов для отладки;
- тестирование кабеля и определение длины линии;
- STP/RSTP/MSTP;
- IEEE802.1Q VLAN и IEEE802.1ad QinQ;
- аутентификация 802.1X по порту и MAC;
- статическая маршрутизация уровня L3;
- два входа питания постоянного тока (резервирование).

1.3 Обзор

Все функции программного обеспечения коммутатора управляются, настраиваются и контролируются с помощью встроенного веб-интерфейса (HTML). С помощью стандартного браузера пользователь может управлять коммутатором на любом удаленном узле сети. Браузер, как универсальный инструмент доступа, использует протокол HTTP для прямой связи с коммутатором.

1.4 Вход в web-интерфейс

Для входа в web-интерфейс открывают браузер на персональном компьютере и вводят IP-адрес коммутатора в формате http://xxx.xxx.xxx.xxx. По умолчанию используется адрес http://192.168.2.1. В окне входа (рисунок 1) вводят имя пользователя admin и пароль system, затем нажимают кнопку OK.

Рисунок 1 — Окно входа в web-интерфейс

1.5 Web-интерфейс

После ввода учетных данных открывается главный экран. На нем отображаются порты коммутатора, их текущее состояние и меню конфигурации.

Веб-агент отображает изображение портов управляемого коммутатора (рисунок 2).

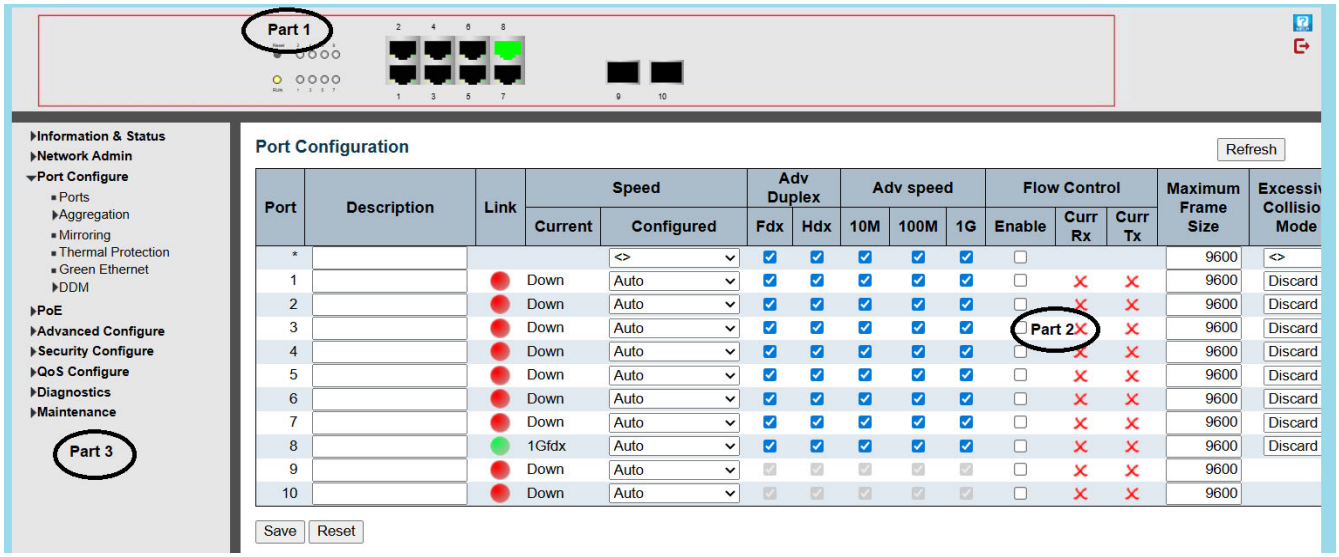

Рисунок 2 — Главная страница web-управления

Разные цвета означают разные состояния, проиллюстрированные следующим образом:

: 100 Мбит/с;

: 1000 Мбит/с;

: Нет линка.

Структура интерфейса главной страницы приведена в таблице 1.

Таблица 1

Область	Описание
Part 1	Логотип компании, панель портов, индикаторы PoE и Link, кнопка выбора языка, ссылка на справку
Part 2	Главное меню, обеспечивающее доступ ко всем командам и статистике
Part 3	Основная рабочая область с параметрами и деталями конфигурации

1.6 Главное меню

Используя встроенный веб-агент, пользователь может определять системные параметры, управлять коммутатором и всеми его портами, а также отслеживать состояние сети. С помощью веб-управления администратор может настроить коммутатор, выбрав функции, перечисленные в главном меню.

Краткое описание функций:

– Information & Status — просмотр общей информации и текущего состояния коммутатора;

– Network Admin — сетевые параметры и базовое администрирование;

– Port Configure — параметры физических портов;

– PoE — настройка Power over Ethernet;

– Advanced Configure — расширенные функции L2;

– Security Configure — механизмы безопасности;

– QoS Configure — параметры качества обслуживания.

2 Управление сетью

2.1 Настройка IP

Экран настройки IP отображается при переходе в раздел «Network Admin > IP» (рисунок 3).

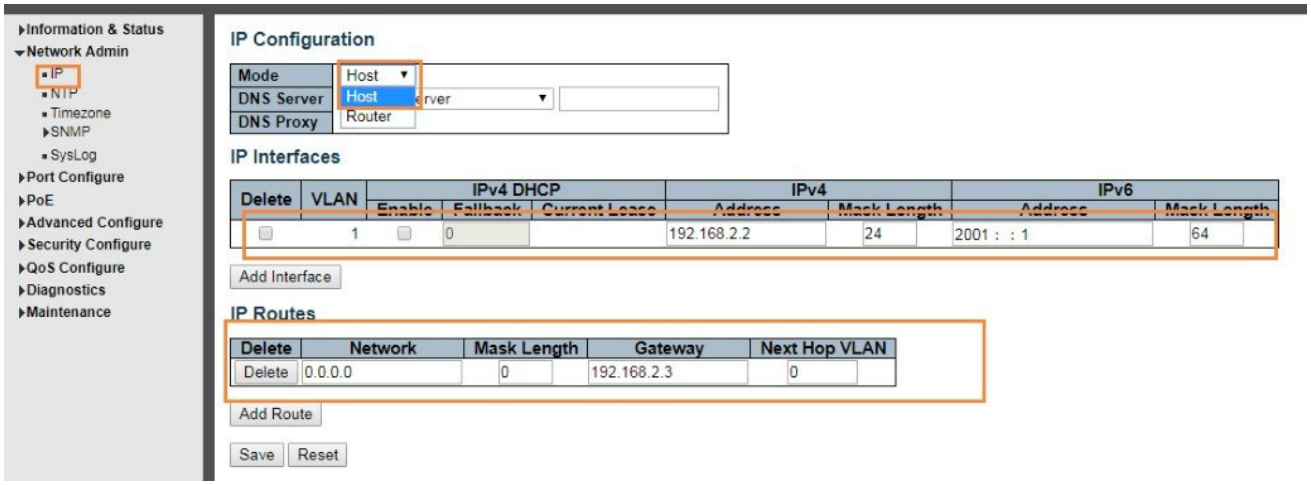

Рисунок 3 — Экран настройки IP

Примечание — По умолчанию коммутатор использует IP-адрес 192.168.2.1 и маску 255.255.255.0 (/24).

Подробное описание конфигурации IP-адреса приведено в таблице 2.

Таблица 2

Параметр	Описание
Port Name	Отображает системное имя порта
VLAN	VLAN, используемый для доступа и управления коммутатором
IPv4 DHCP	Если включено, коммутатор получает IPv4- адрес через DHCP. Иначе используется статический адрес. Fallback (Seconds) — время ожидания адреса, Current Lease — текущий адрес, полученный по DHCP
IPv4	Статический IPv4-адрес и длина маски/префикса
IPv6	Статический IPv6-адрес и длина IPv6-маски
IP Routes	Поля Destination, IP Mask и Next address для настройки статических маршрутов IPv4

Кнопка Add Interface создает новую управленческую связку VLAN + IP.

Для сохранения настроек необходимо нажать кнопку Save.

Примечание — По умолчанию существует только VLAN 1. Если требуется управление через другой VLAN, сначала создают VLAN в модуле VLAN, затем включают в него нужный порт.

2.2 Настройка NTP

NTP (Network Time Protocol) используется для синхронизации времени. В разделе «Network Admin > NTP» можно указать серверы NTP и режим работы (рисунок 4).

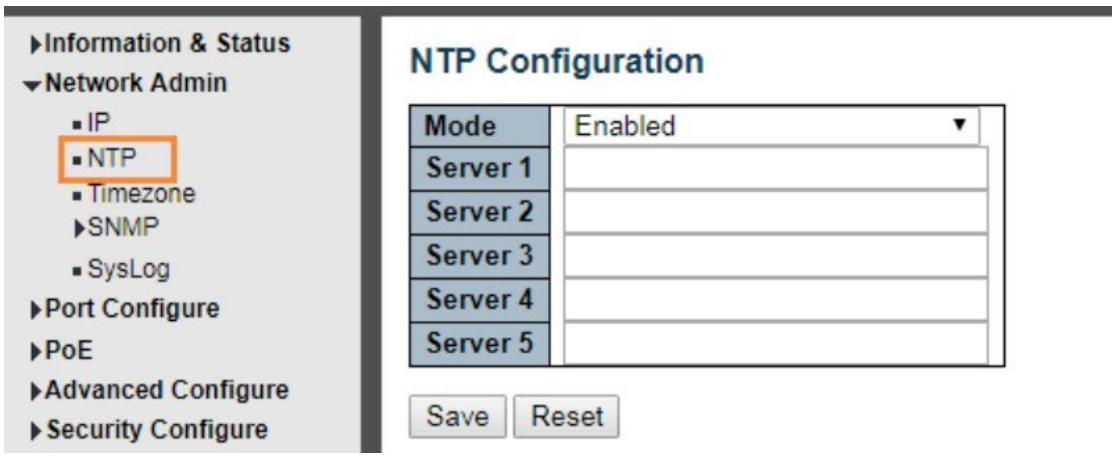

Рисунок 4 — Экран настройки NTP

Объекты конфигурации и их описание приведены в таблице 3.

Таблица 3

Объект	Описание
Mode	Enabled — включить NTP. Агент пересылает NTP-сообщения между клиентами и сервером, даже если они находятся в разных подсетях. Disabled — выключить NTP
NTP Server	IP-адрес одного из NTP-серверов, с которого устройство получает время

Для сохранения настроек необходимо нажать кнопку Save.

2.3 Часовой пояс (Timezone)

Раздел «Network Admin > Timezone» позволяет задать смещение часового пояса для корректного отображения локального времени. Для изменения параметра Timezone setting вводят смещение/время для локального часового пояса и нажимают кнопку Save (рисунок 5).

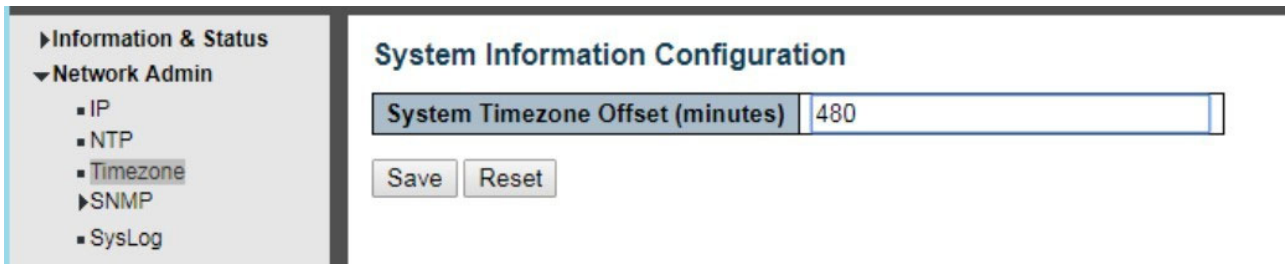

Рисунок 5 — Настройка часового пояса

2.4 Настройка SNMP

Протокол SNMP (Simple Network Management Protocol) — прикладной протокол TCP/IP для обмена управляющей информацией. Он позволяет:

- осуществлять мониторинг производительности сети;
- диагностировать неисправности;
- планировать расширение.

Поддерживаемые версии — SNMP v1, v2c, v3 с разным уровнем безопасности.

MIB (Management Information Base) — виртуальное хранилище управляемых объектов. Коммутатор использует стандартный MIB-II — доступен через SNMP-менеджеры и веб-интерфейс.

Аутентификация (v1/v2c) осуществляется с помощью Community String (аналог пароля):

- public — только чтение MIB;
- private — чтение/запись MIB.

Traps (ловушки) — асинхронные уведомления NMS о событиях:

- перезагрузка устройства;
- смена статуса порта;
- сбои аутентификации.

Преимущества SNMP v3 заключаются в способах аутентификации пользователей и шифрования трафика.

2.4.1 Системная конфигурация SNMP

Пользователь может включить или отключить настройку системы SNMP. Соответствующее окно настройки отображается при открытии раздела «Network Admin > SNMP > System» (рисунок 6).

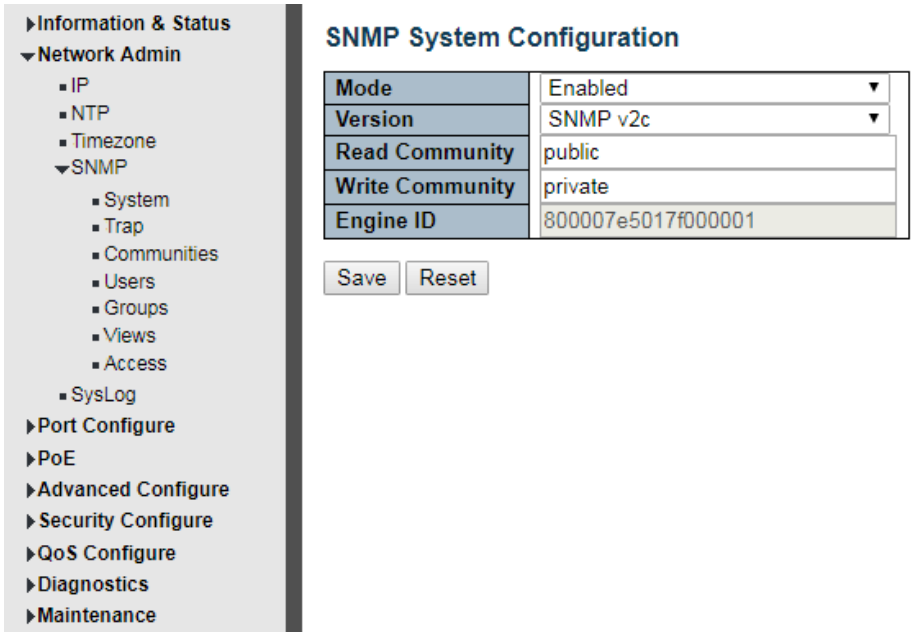

Рисунок 6 — Системные параметры SNMP

Объекты конфигурации и их описание приведены в таблице 4.

Таблица 4

Объект	Описание
Mode	Включение или отключение SNMP
Version	Выбор версии SNMP v1 или SNMP v2c
Read Community	Строка сообщества для чтения объектов MIB
Write Community	Строка сообщества для чтения и записи объектов MIB

Для сохранения настроек необходимо нажать кнопку Save.

2.4.2 SNMP Trap и SNMPv3

Пользователь может включить или отключить функцию SNMP Trap и задать конфигурацию. Соответствующее окно настройки отображается при открытии раздела «Admin > SNMP > Trap» (рисунок 7).

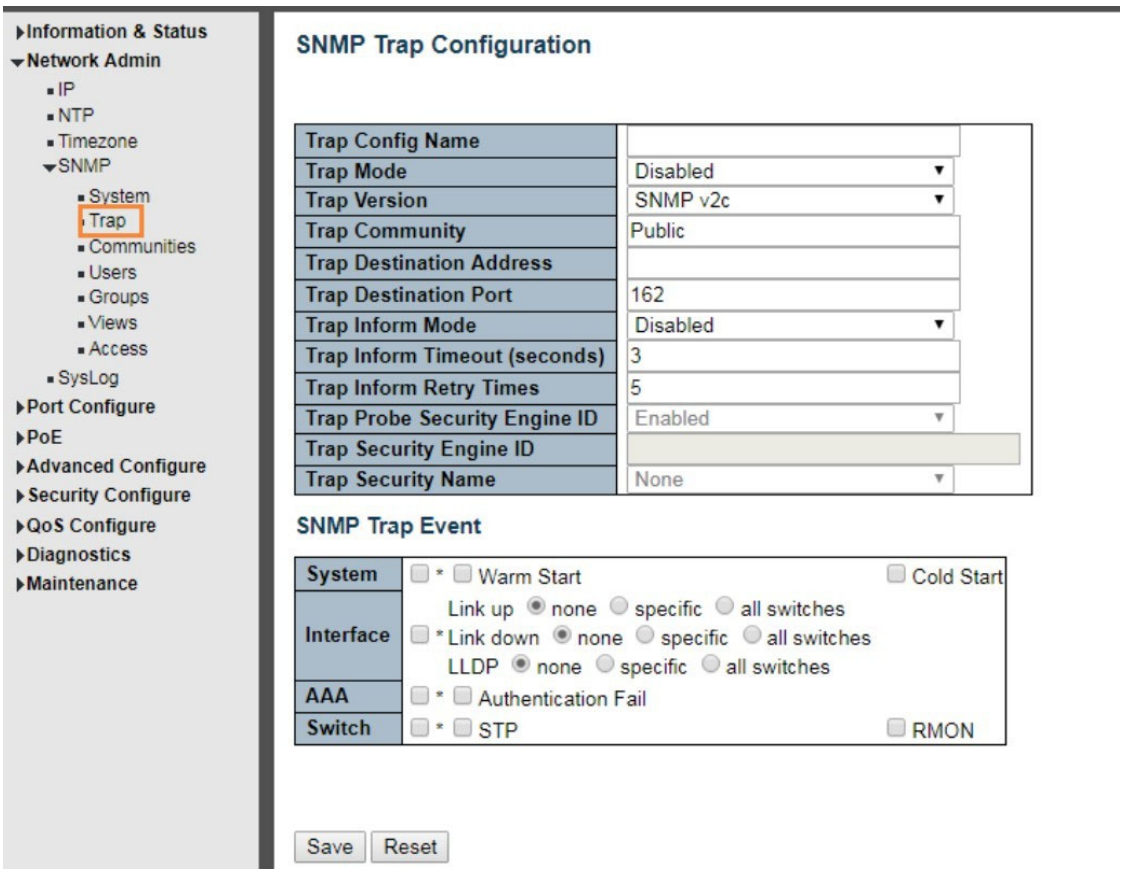

Рисунок 7 — Настройка SNMP Trap

Для сохранения настроек необходимо нажать кнопку Save.

2.4.3 Сообщества (Communities)

Пользователь может задать новое название сообщества. Соответствующее окно настройки отображается при открытии раздела «Network admin > SNMP > Communities» (рисунок 8).

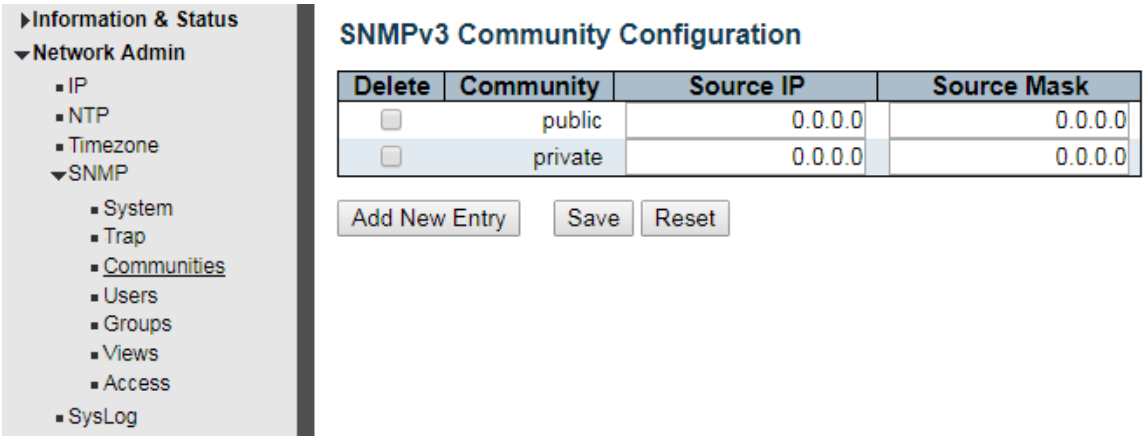

Рисунок 8 — Добавление сообщества

Объекты конфигурации и их описание приведены в таблице 5.

Таблица 5

Объект	Описание
Community	Ввод названия нового сообщества
Source IP	Ввод исходного адреса IPv4
Source Mask	Ввод маски подсети IPv4

Для сохранения настроек необходимо нажать кнопку Save.

2.4.4 Учетные записи (Users)

SNMP v3 использует механизм безопасности USM (User-based Security Model). Администратор может настроить аутентификацию и шифрование. Аутентификация подтверждает подлинность отправителя сообщения и предотвращает несанкционированный доступ. Шифрование защищает сообщения, передаваемые между NMS и агентом, от перехвата. Использование этих двух механизмов обеспечивает более высокий уровень безопасности связи между NMS и агентом.

Пользователь может настроить учетную запись SNMP v3 и режим шифрования. Соответствующее окно настройки отображается при открытии раздела «Network Admin > SNMP > Users» (рисунок 9).

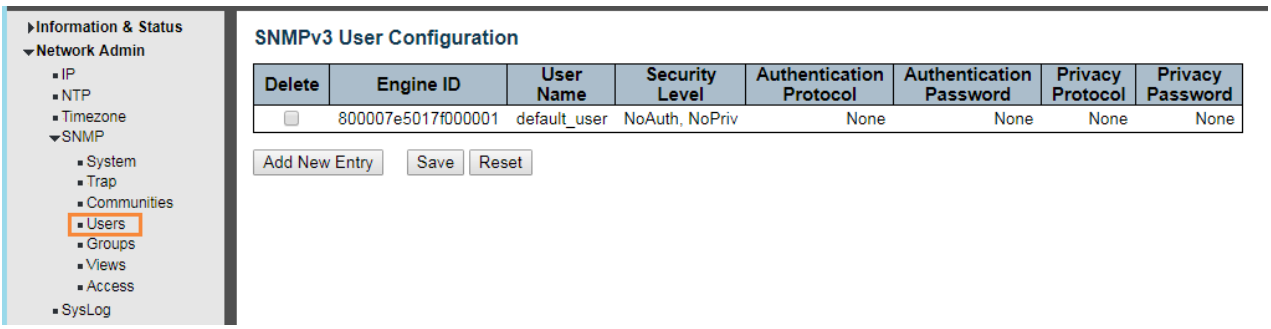

Рисунок 9 — Добавление пользователей

Объекты конфигурации и их описание приведены в таблице 6.

Таблица 6

Объект	Описание
Engine ID	Значение по умолчанию — 800007e5017f000001. Рекомендуется использовать значение по умолчанию
User Name	Вводится новое имя учетной записи SNMPv3
Security Level	Три режима шифрования: – NoAuth, NoPriv; – Auth, NoPriv; – Auth, Priv. Режим выбирается из выпадающего меню
Authentication Protocol	Выбирается для MD5 и SHA
Authentication Password	Вводится зашифрованный пароль
Privacy Protocol	Выбирается для DES и AES
Privacy Password	Вводится зашифрованный пароль

Для сохранения настроек необходимо нажать кнопку Save.

2.4.5 Просмотр посещений (Views)

Пользователь может настроить режим просмотра посещений в SNMPv3. Соответствующее окно настройки отображается при открытии раздела «Network Admin > SNMP > Views» (рисунок 10):

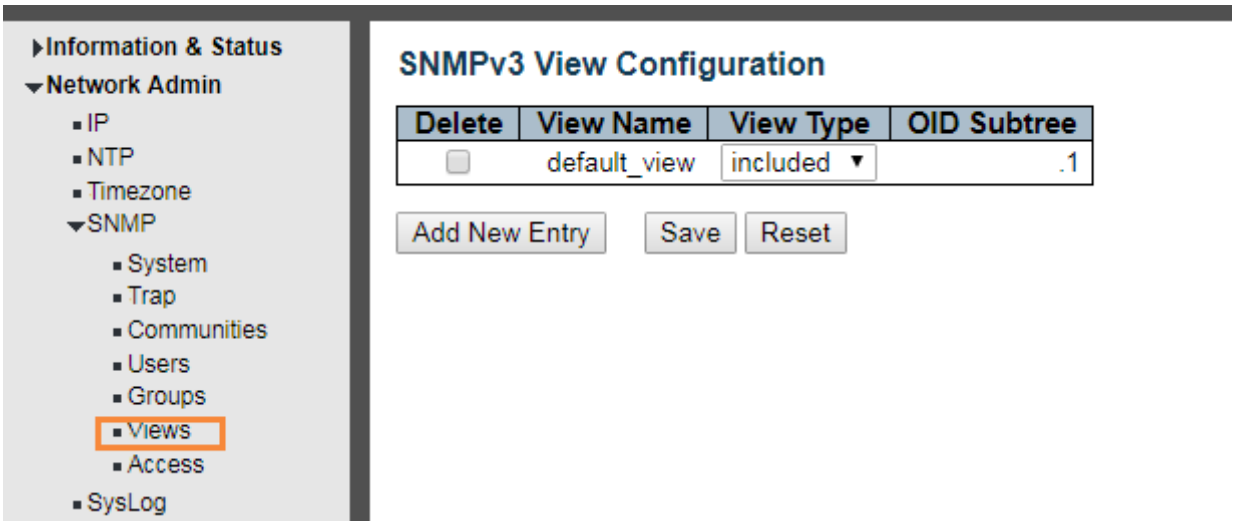

Рисунок 10 — Добавление просмотра SNMPv3

Объекты конфигурации и их описание приведены в таблице 7.

Таблица 7

Объект	Описание
Views Name	Вводится название представлений
Views Type	Выбирается для включенных и исключенных
OID Subtree	Вводится тип OID (например, 1.2)

Для сохранения настроек необходимо нажать кнопку Save.

2.4.6 Настройка доступа (Access)

Пользователь может настроить доступ для загрузки созданных представлений. Соответствующее окно настройки отображается при открытии раздела «Admin > SNMP > Access» (рисунок 11).

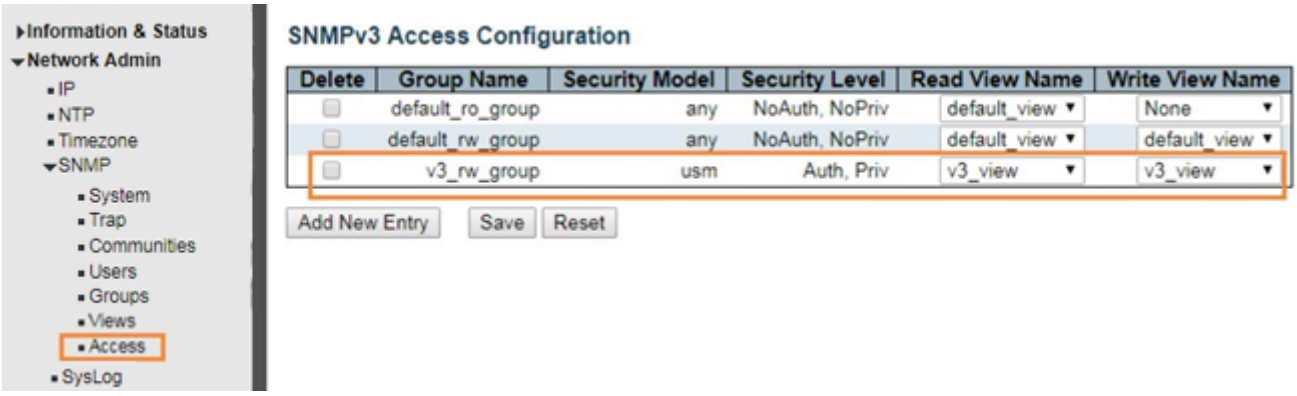

Рисунок 11 — Настройка доступа в SNMPv3

Объекты конфигурации и их описание приведены в таблице 8.

Таблица 8

Объект	Описание
Group Name	Вводится название группы
Security Model	Выбирается для любого usm версии 1 и 2c
Security Level	Три режима шифрования: – NoAuth, NoPriv; – Auth, NoPriv; – Auth, Priv. Режим выбирается из выпадающего меню
Read View Name	Выбираются созданные профили для чтения
Write View Name	Выбираются созданные профили для записи

Для сохранения настроек необходимо нажать кнопку Save.

2.4.7 Группы (Groups)

Пользователь может настроить группы для загрузки созданных пользователей и доступа к ним. Соответствующее окно настройки отображается при открытии раздела «Network Admin > SNMP > Groups» (рисунок 12).

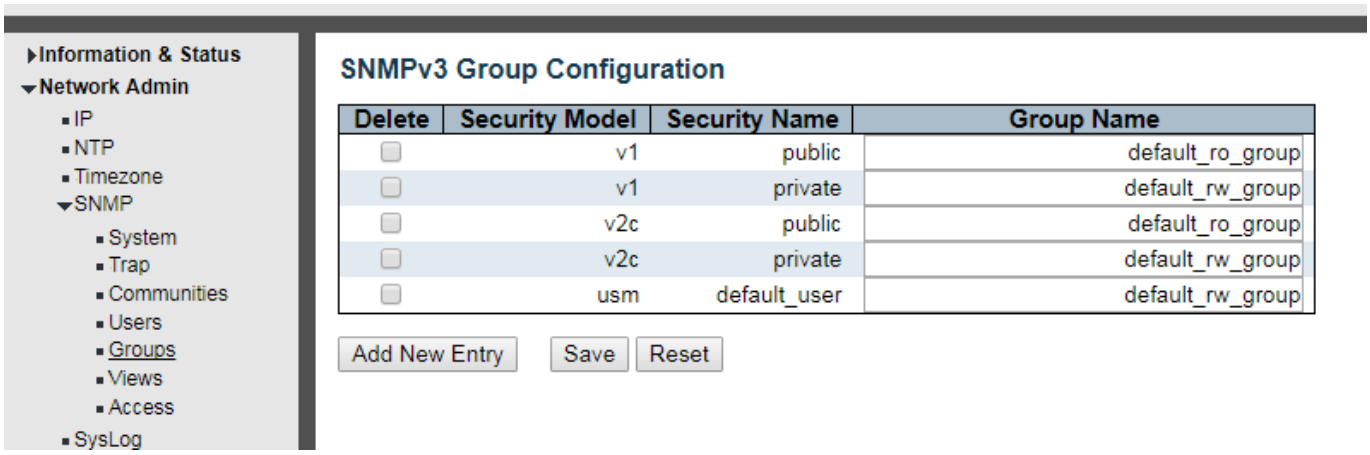

Рисунок 12 — Настройка групп SNMPv3

2.5 Настройка системного журнала (Syslog)

Пользователь может настроить системный журнал коммутатора. Соответствующее окно настройки отображается при открытии раздела «Network Admin > Syslog» (рисунок 13).

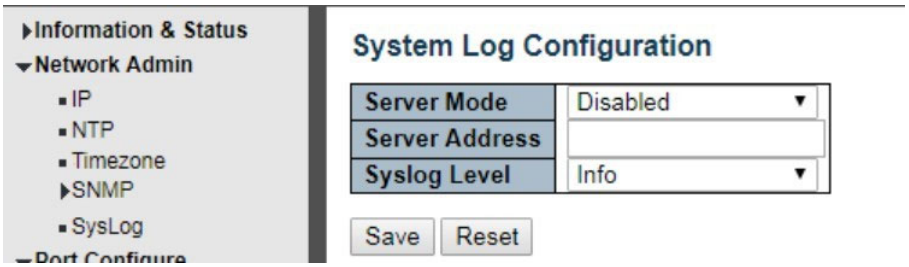

Рисунок 13 — Настройка Syslog

Объекты конфигурации и их описание приведены в таблице 9.

Таблица 9

Объект	Описание
Server Mode	Включение или отключение функции отправки системного журнала
Server Address	IP-адрес syslog-сервера
Syslog Level	Info — информационные сообщения, предупреждения и ошибки. Warning — предупреждения и ошибки. Error – только ошибки

Для сохранения настроек необходимо нажать кнопку Save.

3 Настройка портов

3.1 Параметры порта (Ports)

Данная страница предназначена для настройки параметров портов коммутатора. Соответствующее окно настройки отображается при открытии раздела «Port Configure > Ports» (рисунок 14).

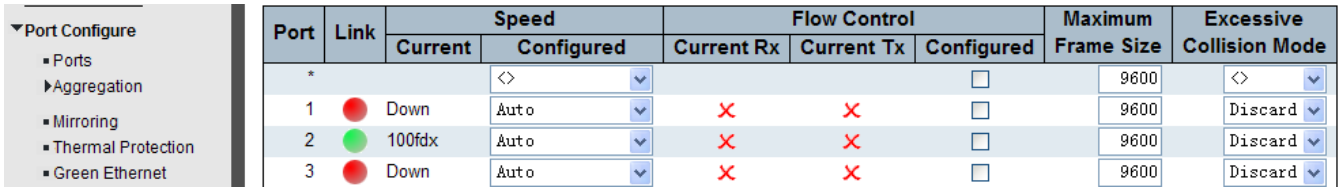

Рисунок 14 – Экран настройки порта

Объекты конфигурации и их описание приведены в таблице 10.

Таблица 10

Объект	Описание
Link	Красный индикатор — Link Down, зеленый — Link Up
Speed	Отключено — порт отключен. Auto — выполняется автоматическое согласование скорости и режима работы между устройствами на скоростях 10, 100 и 1000 Мбит/с; при этом 1000 Мбит/с всегда работает в полнодуплексном режиме. Этот режим позволяет порту автоматически определить наилучшие параметры для подключенного устройства и применить их. 1000-X_AMS — порт является комбинированным Ethernet/оптическим портом, при этом оптический порт имеет приоритет. Другие варианты: 10M HDX, 10M FDX, 100M HDX, 100M FDX, 1000M FDX, 1000-X
Flow Control	Механизм управления потоком для различных конфигураций портов. В полнодуплексных портах используется управление потоком 802.3x, а в полудуплексных портах — управление потоком в режиме backpressure. По умолчанию функция отключена
Maximum Frame Size	Максимальный размер Ethernet-кадра. По умолчанию 9600 байт для поддержки Jumbo Frames

Для сохранения настроек необходимо нажать кнопку Save.

3.2 Агрегирование каналов (Aggregation)

Пользователь может настроить несколько каналов связи между несколькими коммутаторами. Объединение каналов — это метод, при котором несколько физических портов объединяются в один логический порт для увеличения пропускной способности. Этот коммутатор поддерживает до 13 групп объединения каналов, по 2–8 портов в каждой группе.

Примечание — Если какой-либо порт в группе агрегирования каналов отключен, пакет данных, отправленный на отключенный порт, будет разделять нагрузку с другим подключенным портом в этой группе агрегирования.

3.2.1 Статическая агрегация

На этой странице пользователь может настроить статическую агрегацию портов коммутатора. Соответствующее окно настройки отображается при открытии раздела «Port Configure > Aggregation > Static» (рисунок 15).

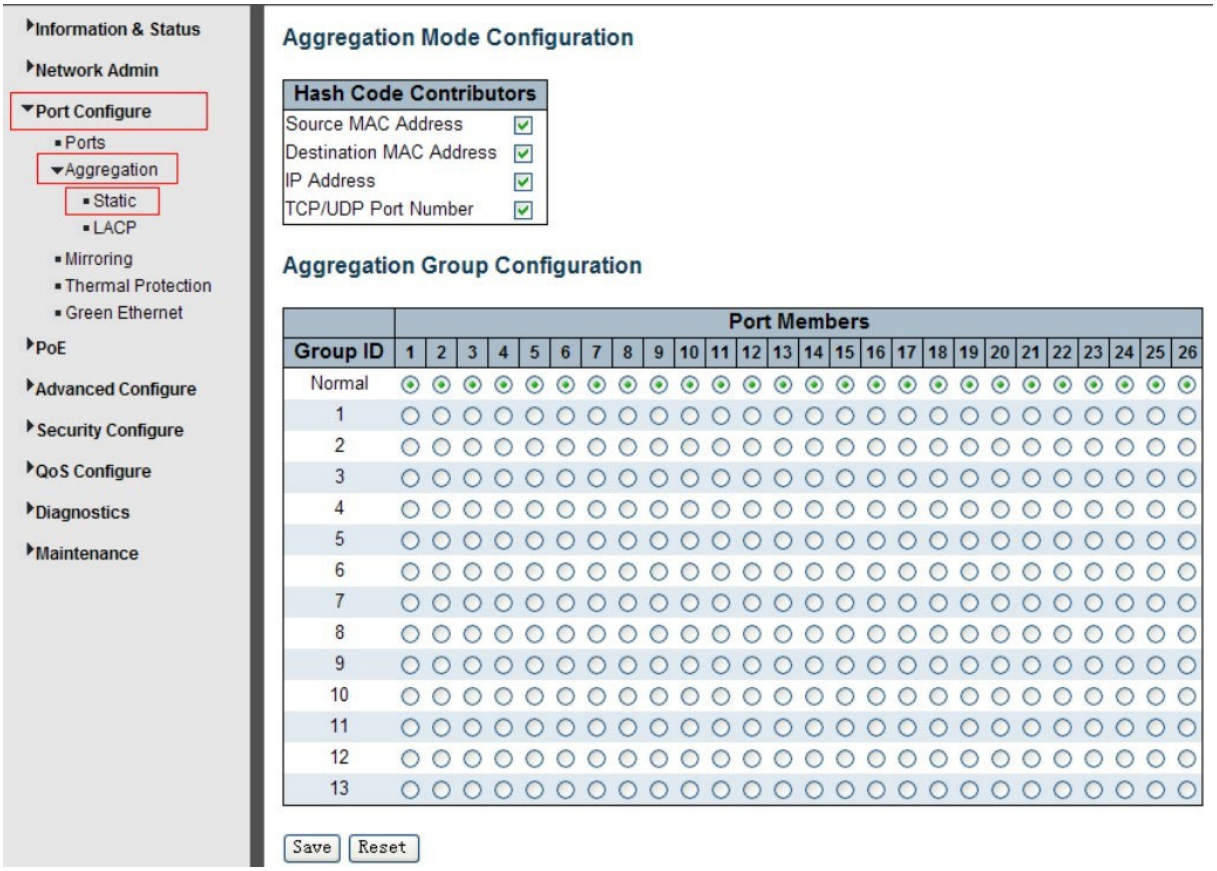

Рисунок 15 — Конфигурация статической агрегации

Объекты конфигурации и их описание представлены в таблице 11.

Таблица 11

Объект	Описание
Aggregation Mode Configuration	Алгоритм hash-распределения трафика между портами LAG
Group ID	Идентификатор группы статической агрегации
Port Members	Состав портов в группе. Одновременно в одной статической trunk-группе может быть не более 8 портов

Для сохранения настроек необходимо нажать кнопку Save.

Примечание — Это позволяет одновременно объединять максимум 8 портов в одну статическую магистральную групп.

3.2.2 LACP-агрегация

Протокол Link Aggregation Control Protocol (LACP) предоставляет стандартизированные средства для обмена информацией между соседними устройствами, которым требуется высокоскоростной резервируемый канал. Агрегация каналов позволяет объединять до восьми портов в один логический канал. Эта функция увеличивает пропускную способность сети. Для работы LACP требуется полнодуплексный режим. Для получения более подробной информации обратитесь к стандарту IEEE 802.3ad.

Пользователь может создавать динамическую группу агрегации для коммутаторов. Соответствующее окно настройки отображается при открытии раздела «Port Configure > Aggregation > LACP» (рисунок 16).

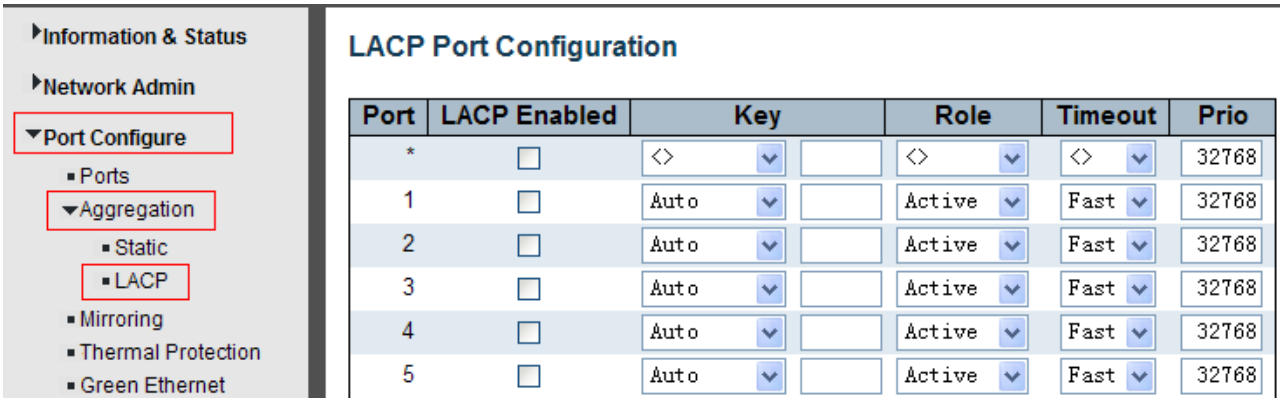

Рисунок 16 — Настройка LACP

Объекты конфигурации и их описание приведены в таблице 12.

Таблица 12

Объект	Описание
LACP	Включение/выключение LACP на порту
Key	Ключ группы. В режиме Auto значение зависит от скорости линка: 10 Мбит/с = 1, 100 Мбит/с = 2, 1 Гбит/с = 3. Порты с одинаковым ключом могут быть в одной группе
Role	Active — порт отправляет LACP-пакеты каждую секунду; Passive — ждет пакеты от партнера
Timeout	Fast — отправка каждую секунду; Slow — раз в 30 секунд
Prio	Приоритет порта: чем меньше значение, тем выше приоритет

Для сохранения настроек необходимо нажать кнопку Save.

3.3 Зеркалирование портов (Mirroring)

На этой странице пользователь может настроить зеркалирование портов. Эта функция позволяет контролировать сетевой трафик, копируя входящие и исходящие пакеты с одного порта коммутатора на другой порт для их анализа. Это дает администратору возможность отслеживать работу коммутатора и при необходимости вносить изменения в его конфигурацию.

Соответствующее окно настройки отображается при открытии раздела «Port Configure > Mirroring» (рисунок 17).

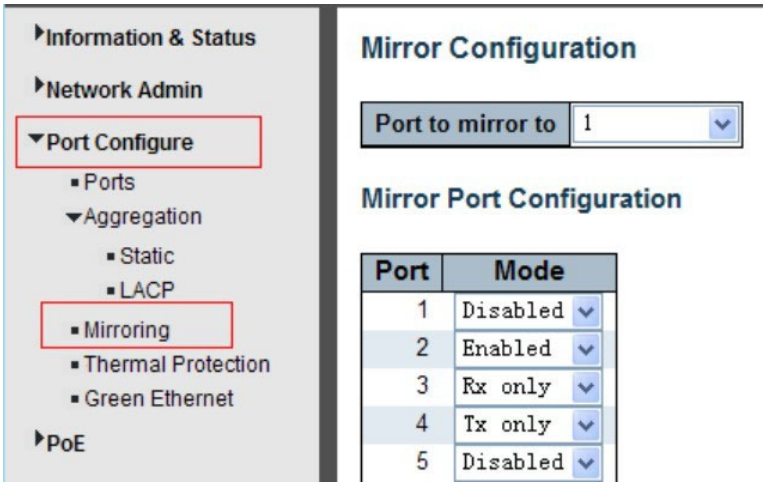

Рисунок 17 — Настройка зеркалирования

Объекты конфигурации и их описание приведены в таблице 13.

Таблица 13

Объект	Описание
Port mirror to	Кадры с портов, для которых включено зеркалирование источника (Rx) или назначения (Tx), передаются на данный порт. Disabled — зеркалирование отключено
Mode	Выбирается режим зеркалирования исходного порта. Rx only — на зеркальный порт передаются только кадры, полученные через этот порт; передаваемые кадры не зеркалируются. Tx only — на зеркальный порт передаются только кадры, отправленные через этот порт; полученные кадры не зеркалируются. Disabled — ни передаваемые, ни принимаемые кадры не зеркалируются. Rx и Tx — на зеркальный порт передаются как входящие, так и исходящие кадры*
* Для данного порта кадр передается только один раз, и зеркалирование Tx-кадров для зеркального порта невозможно. По этой причине для выбранного зеркального порта допустимы только режимы Disabled или Rx only	

Для сохранения настроек необходимо нажать кнопку Save.

Примечание — Пользователь не может настроить зеркальное отображение высокоскоростных портов на низкоскоростные порты. Например, при попытке зеркального отображения портов со скоростью 100 Мбит/с на порт со скоростью 10 Мбит/с возникает проблема. Таким образом, порт назначения должен иметь равную или более высокую скорость по сравнению с портом источника. Кроме того, порт источника и порт назначения не должны совпадать.

3.4 Защита от перегрева (Thermal Protection)

Защита от перегрева предназначена для контроля и защиты работающего коммутатора. Если система обнаруживает, что температура порта превышает заданное значение, она отключает порт, чтобы защитить сам коммутатор.

Соответствующее окно настройки отображается при открытии раздела «Port Configure > Thermal Protection» (рисунок 18).

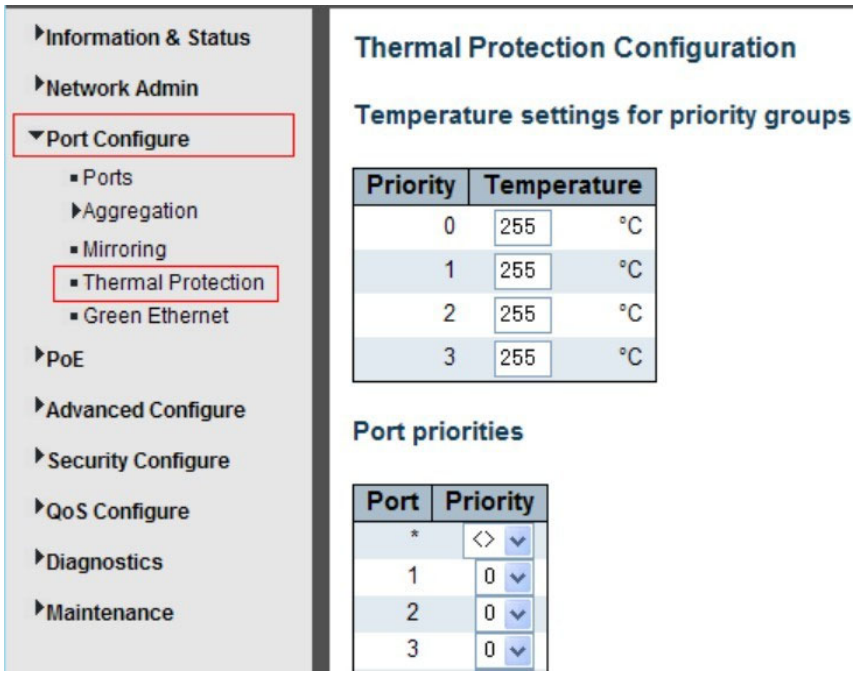

Рисунок 18 — Настройка тепловой защиты

Объекты конфигурации и их описание приведены в таблице 14.

Таблица 14

Объект	Описание
Temperature settings for priority groups	Коммутатор поддерживает 4 группы приоритета тепловой защиты, для каждой из которых задается пороговая температура
Port priorities	Назначение порта в определенную группу приоритета

Для сохранения настроек необходимо нажать кнопку Save.

Примечание — По умолчанию все порты коммутатора относятся к группе приоритета 0, с защищенной температурой 225 °C.

4 PoE

Power over Ethernet (PoE) — это технология подачи питания по Ethernet-кабелю через интерфейсы 100BASE-TX и 1000BASE-T. Максимальная длина линии питания составляет 100 метров. В системе PoE, построенной на кабеле UTP Cat5 или выше, можно подавать питание на IP-камеры, VoIP-телефоны и беспроводные точки доступа, а также передавать данные. Это позволяет не прокладывать отдельные силовые кабели и снижает стоимость построения сети.

Система питания PoE имеет единый стандарт — IEEE 802.3af и IEEE 802.3at. Поэтому устройства разных производителей, как правило, совместимы между собой при условии соответствия этим стандартам.

PD (Powered Device) — это питаемое устройство в системе PoE. К нему относятся IP-камеры, беспроводные точки доступа, VoIP-телефоны и другое IP-оборудование.

Процесс работы PoE:

1. Обнаружение. PSE на начальном этапе подает очень малое напряжение, чтобы определить, соответствует ли подключенное PD стандарту IEEE 802.3af/802.3at. Если устройство соответствует стандарту, система переходит к следующему этапу.
2. Классификация PD. После обнаружения PSE определяет класс подключенного PD и требуемую мощность.
3. Подача питания. После завершения предыдущих этапов PSE начинает подавать необходимое питание на PD с выходным напряжением 44–57 В DC.
4. Питание. PSE обеспечивает стабильное питание 44–57 В DC и автоматически подает мощность в соответствии с потребностями PD. Максимальная мощность одного PoE-порта для IEEE 802.3af составляет 15,4 Вт, для IEEE 802.3at — 25,5 Вт.
5. Отключение. Если PD отключается или пользователь выключает PoE через программу управления, PSE быстро прекращает подачу питания, обычно за 300–400 мс.

На любом этапе подачи питания PSE прекращает работу и снова начинает процесс с первого шага, если возникает нештатная ситуация, например, короткое замыкание PD, превышение потребляемой мощности или другое аварийное состояние.

4.1 Конфигурация PoE (PoE Setting)

Соответствующее окно настройки отображается при открытии раздела «PoE > PoE Setting» (рисунок 19).

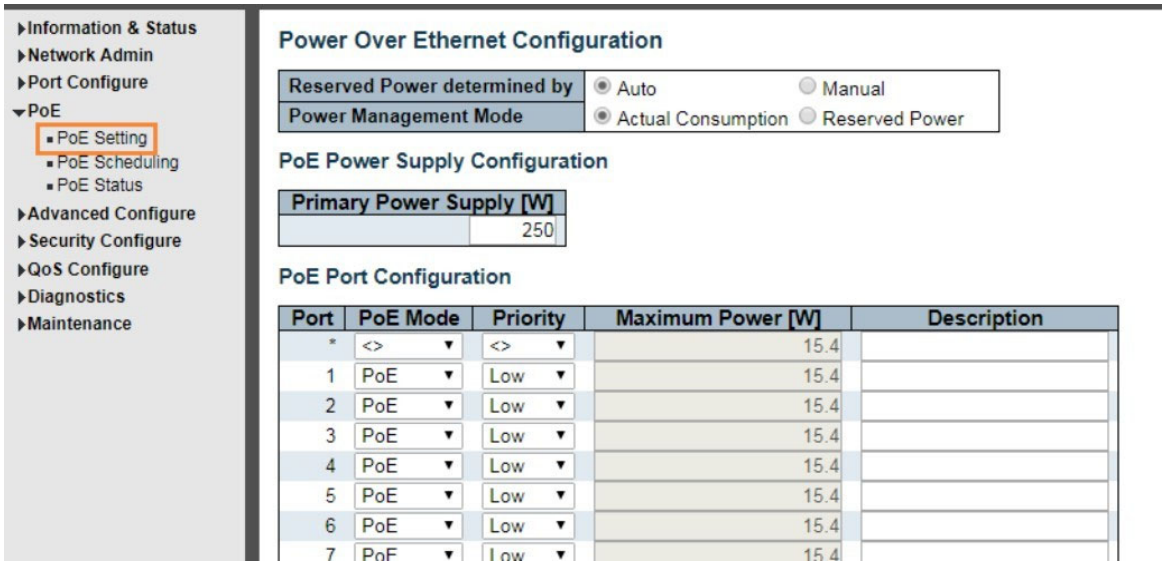

Рисунок 19 — Настройка PoE

Объекты конфигурации и их описание приведены в таблице 15.

Таблица 15

Объект	Описание
Reserved Power determined by	Коммутатор поддерживает 2 режима определения резервируемой мощности. Auto: коммутатор автоматически назначает максимальную мощность порта в соответствии с обнаруженным классом PD. Описание классов PD см. в определениях 802.3af / 802.3at. Manual: максимальная резервируемая мощность порта задается пользователем
Power Management Mode	Коммутатор поддерживает 2 режима управления питанием. Actual Consumption: в этом режиме, если фактическое потребление энергии всеми портами превышает допустимый бюджет питания коммутатора, будет отключен порт с наименьшим приоритетом. Если у всех портов одинаковый приоритет, будет отключен порт с наибольшим номером. Reserved Power: в этом режиме, если суммарная резервируемая мощность всех портов превышает допустимый бюджет питания коммутатора, порт, к которому подключено новое PD-устройство, не будет включен
Primary Power Supply [W]	Пользователь может установить максимальную общую мощность коммутатора. Рекомендуется устанавливать не более 240 Вт

Объект	Описание
PoE Mode	Коммутатор поддерживает режимы 802.3af (PoE) и 802.3at (PoE+). Значение по умолчанию — 802.3at
Priority	Определяет приоритет порта PoE (низкий, высокий, критический)
Maximum Power (W)	Предназначается для определения максимальной мощности порта, когда пользователь устанавливает ручной режим определения зарезервированной мощности.

Для сохранения настроек необходимо нажать кнопку Save.

4.2 Статус PoE (PoE Status)

Пользователь может проверить и просмотреть статус PoE всех портов в окне, отображаемом при открытии раздела «PoE > PoE Status» (рисунок 20).

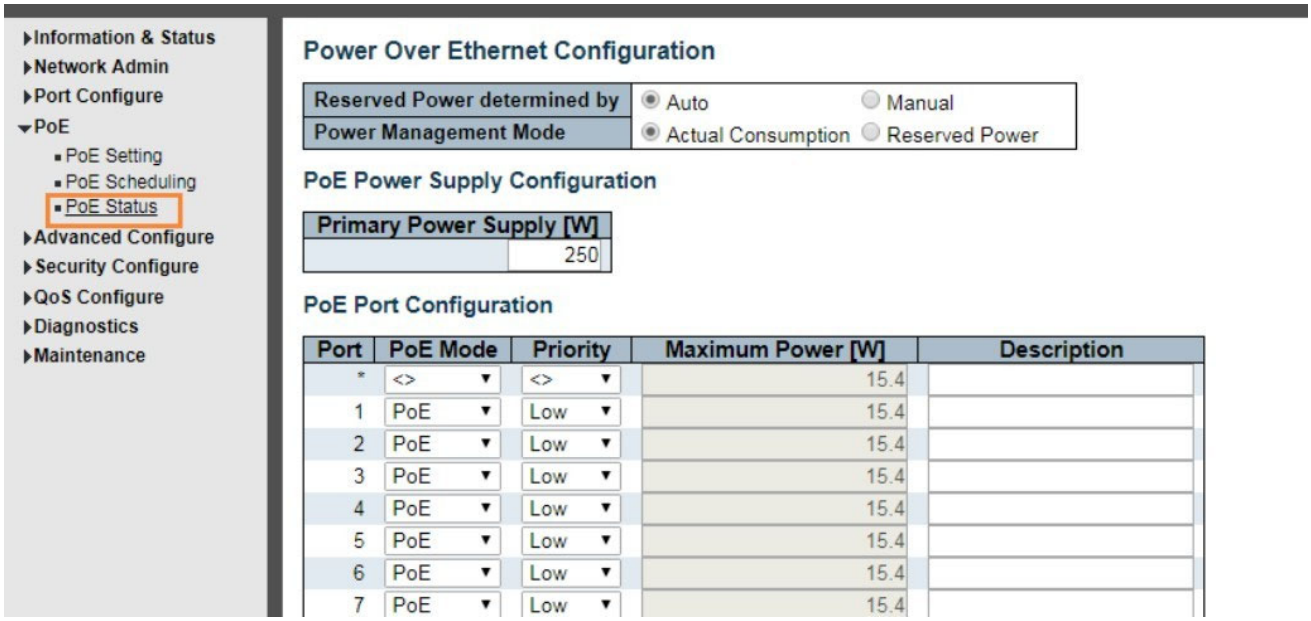

Рисунок 20 — Статус PoE

4.3 Расписание PoE (PoE Scheduling)

Коммутатор поддерживает планирование PoE. Пользователь может устанавливать время перезагрузки PoE и включать/отключать PoE по расписанию. Соответствующее окно настройки отображается при открытии раздела «PoE > PoE Scheduling» (рисунок 21).

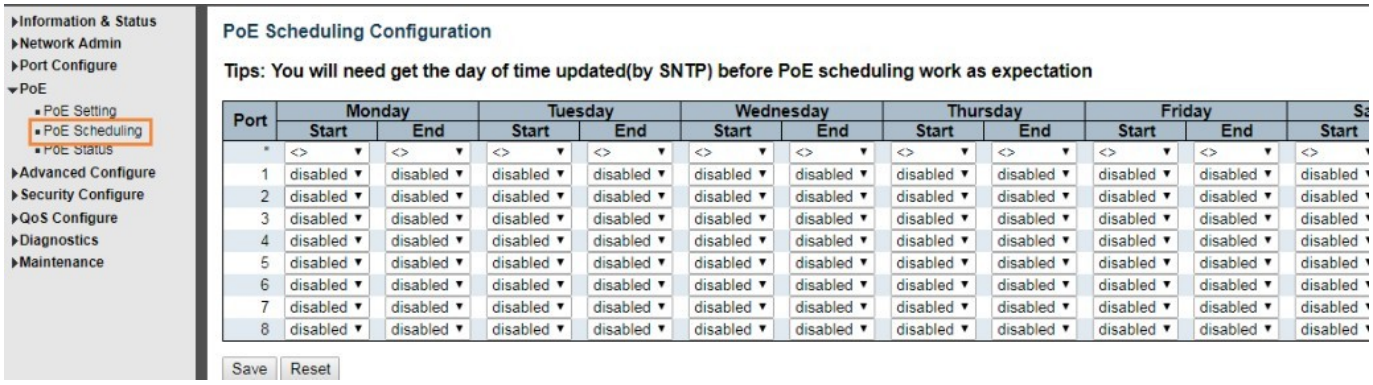

Рисунок 21 — Расписание PoE

Объекты конфигурации и их описание приведены в таблице 16.

Таблица 16

Параметр	Описание
Cycle	Диапазон выбора: с понедельника по воскресенье
Start	Время начала действия расписания. Диапазон 00:00 – 24:00
End	Время завершения действия расписания. Диапазон 00:00 – 24:00

Для сохранения настроек необходимо нажать кнопку Save.

5 Расширенные функции

5.1 VLAN

VLAN (виртуальная локальная сеть) — это технология логического разделения одной физической локальной сети на несколько виртуальных сегментов. Каждая VLAN формирует отдельный широковещательный домен.

Хосты, входящие в одну VLAN, могут взаимодействовать друг с другом напрямую. При этом VLAN не могут обмениваться данными напрямую между собой. Это ограничивает распространение широковещательных пакетов в пределах одной VLAN. Поскольку прямой доступ между VLAN отсутствует, повышается уровень сетевой безопасности. Соответствующее окно настройки отображается при открытии раздела «Advanced Configure > VLANs» (рисунок 22).

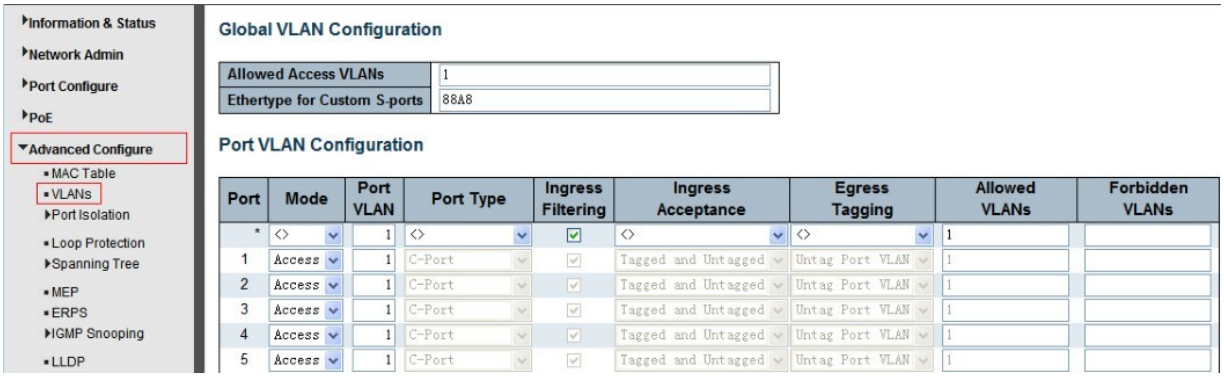

Рисунок 22 — Экран настройки VLAN

Объекты конфигурации и их описание приведены в таблице 17.

Таблица 17

Параметр	Описание
Allowed VLANs	Список созданных VLAN ID. По умолчанию существует VLAN 1. Для создания нового VLAN добавляют его ID в этот список
Ethertype for Custom S-ports	В этом поле указывается значение ethertype/TPID в шестнадцатеричном формате, используемое для пользовательских S-портов. Эта настройка применяется ко всем портам, для которых тип порта установлен как S-Custom-Port
Mode	Режим порта (по умолчанию — Access) определяет основные параметры работы порта. Порт может работать в одном из трех режимов, описанных ниже. При выборе режима остальные параметры строки становятся недоступными либо, наоборот, доступны для настройки в зависимости от режима. Параметры, выделенные серым цветом, показывают значения, которые будут применены к порту после выбора данного режима. **Access** Порты доступа обычно используются для подключения конечных устройств. Для них характерно следующее:

Параметр	Описание
	– порт принадлежит только одной VLAN — VLAN порта (Access VLAN), по умолчанию VLAN 1; – принимаются кадры без меток и с C-тегом; – отбрасываются кадры, не относящиеся к Access VLAN; – на выходе кадры VLAN доступа передаются без меток, а кадры других динамически добавляемых VLAN — с метками. **Trunk** Магистральные порты могут передавать трафик нескольких VLAN одновременно и обычно используются для подключения к другим коммутаторам. Для них характерно следующее: – по умолчанию trunk-порт является членом всех VLAN от 1 до 4094; – список VLAN, к которым принадлежит порт, можно ограничить списком разрешенных VLAN; – кадры VLAN, членом которой порт не является, отбрасываются; – по умолчанию все кадры, кроме кадров собственной VLAN порта, передаются с меткой; кадры собственной VLAN передаются без C-тега; – можно включить режим, при котором все кадры передаются с метками, и тогда на входе будут приниматься только тегированные кадры. **Hybrid** Гибридные порты похожи на trunk-порты, но предоставляют дополнительные возможности настройки. В дополнение к функциям trunk-порта, гибридные порты позволяют: – задавать обработку кадров с VLAN-тегами и без VLAN-тегов, а также C-тегов, S-тегов и пользовательских S-тегов; – управлять фильтрацией входящего трафика; – независимо настраивать прием входящих кадров и правила тегирования выходящих кадров
Port VLAN	Это поле определяет идентификатор VLAN порта (PVID). Допустимый диапазон значений — от 1 до 4094, значение по умолчанию — 1. При приеме входящих кадров их классификация выполняется по VLAN порта. Если порт настроен как не поддерживающий VLAN, либо кадр не имеет тега, либо для порта включена поддержка VLAN, но кадр помечен как приоритетный (VLAN ID = 0), кадр обрабатывается согласно PVID. При передаче кадры, относящиеся к VLAN порта, не помечаются, если для параметра тегирования на выходе выбрано значение «не помечать VLAN порта». VLAN порта называется Access VLAN для портов в режиме доступа и native VLAN для портов в магистральном или гибридном режиме
Port Type	Порты в гибридном режиме позволяют настраивать тип порта, то есть определять, используется ли VLAN-тег кадра для классификации входящего трафика и, если используется, на какой TPID он реагирует. Аналогично, при передаче тип порта определяет TPID тега, если кадр должен быть помечен.

Параметр	Описание
	Unaware: При приеме все кадры, независимо от наличия VLAN-тега, классифицируются по VLAN порта. При передаче теги не удаляются. **C-Port:** При приеме кадры с VLAN-тегом и TPID = 0x8100 классифицируются по VLAN ID, указанному в теге. Если кадр нетегированный или приоритетный, он классифицируется по VLAN порта. При необходимости кадры на выходе помечаются C-тегом. **S-Port:** При приеме кадры с VLAN-тегом и TPID = 0x8100 или 0x88A8 классифицируются по VLAN ID, указанному в теге. Если кадр нетегированный или приоритетный, он классифицируется по VLAN порта. При необходимости кадры на выходе помечаются S-тегом. **S-Custom-Port:** При приеме кадры с VLAN-тегом и TPID = 0x8100 или с TPID, заданным для пользовательских портов, классифицируются по VLAN ID, указанному в теге. Если кадр нетегированный или приоритетный, он классифицируется по VLAN порта. При необходимости кадры на выходе помечаются пользовательским S-тегом
Ingress Filter	Гибридные порты позволяют задавать тип входящих кадров. **Tagged and Untagged** — принимаются как помеченные, так и непомеченные кадры. **Tagged only** — принимаются только помеченные кадры, непомеченные отбрасываются. **Untagged only** — принимаются только непомеченные кадры, помеченные отбрасываются
Ingress Acceptance	Гибридные порты позволяют настраивать входную фильтрацию. На портах доступа и магистральных портах входная фильтрация всегда включена. Если входная фильтрация включена (установлен флажок), кадры, отнесенные к VLAN, членом которой порт не является, отбрасываются. Если входная фильтрация отключена, кадры, отнесенные к VLAN, членом которой порт не является, принимаются и передаются в механизм коммутации. Однако порт никогда не будет передавать кадры, отнесенные к VLAN, членом которой он не является.
Egress Tagging	Порты в магистральном и гибридном режимах могут управлять тегированием исходящих кадров. **Не помечать VLAN порта** Кадры, относящиеся к VLAN порта, передаются без тега. Остальные кадры передаются с соответствующим тегом. **Помечать все** Все кадры, независимо от принадлежности к VLAN порта, передаются с тегом. **Снимать тег со всех кадров** Все кадры, независимо от принадлежности к VLAN порта, передаются без тега. Эта опция доступна только для портов в гибридном режиме

Параметр	Описание
Forbidden VLANs	Порт может быть настроен таким образом, чтобы он никогда не входил в одну или несколько VLAN. Это особенно полезно, когда необходимо запретить динамическое добавление порта в VLAN с помощью динамических протоколов, таких как MVRP и GVRP. Для этого соответствующие VLAN следует отметить, как запрещенные на данном порту. Синтаксис идентичен синтаксису, используемому в поле Enabled VLAN. По умолчанию это поле остается пустым, что означает, что порт может быть членом всех доступных VLAN
Allowed VLANs	Порты в магистральном и гибридном режимах могут управлять тем, к каким VLAN им разрешено принадлежать. Порты доступа могут принадлежать только к одной VLAN — Access VLAN. Синтаксис поля идентичен синтаксису, используемому в поле Enabled VLAN. По умолчанию магистральный или гибридный порт является членом всех VLAN, поэтому для него задан диапазон 1–4094. Поле может быть оставлено пустым, что означает, что порт не будет входить ни в одну VLAN

Для сохранения настроек необходимо нажать кнопку Save.

5.2 Изоляция портов (Port Isolation)

Изоляция портов предназначена для ограничения передачи данных между портами. Она похожа на VLAN, но является более строгой.

5.2.1 Группы портов (Port Group)

Коммутатор поддерживает группы портов. Члены группы портов могут пересылать данные. Окно конфигурации группы портов открывается при открытии раздела «Advanced Configure > Port Isolation > Port Group» (рисунок 23).

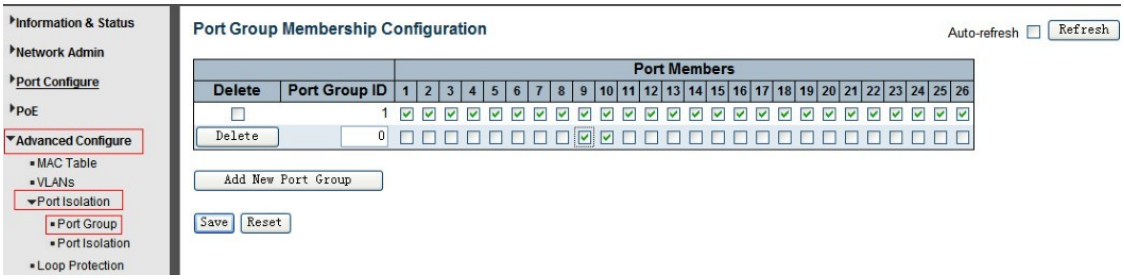

Рисунок 23 — Конфигурация Port Group

Флажками помечаются порты, которые должны входить в одну группу.

Примечание — Порт может принадлежать к нескольким группам портов. Данные могут пересылаться между любыми портами, которые принадлежат к одной группе портов.

Для сохранения настроек необходимо нажать кнопку Save.

5.2.2 Изоляция портов (Port Isolation)

Окно настройки изоляции порта отображается при открытии раздела «Advanced Configure > Port Isolation > Port Isolation» (рисунок 24).

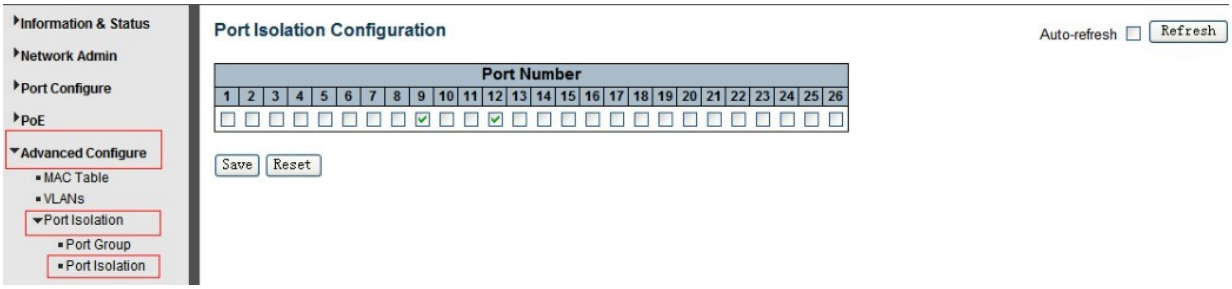

Рисунок 24 — Настройка изоляции портов

Флажками помечаются порты, устанавливаемые в качестве изолированных, чтобы они не могли пересылать поток данных.

Для сохранения настроек необходимо нажать кнопку Save.

5.3 Протокол STP

Протокол связующего дерева (STP) используется для обнаружения и устранения сетевых петель, а также для обеспечения резервных каналов связи между коммутаторами, мостами или маршрутизаторами. Это позволяет коммутатору взаимодействовать с другими сетевыми устройствами так, чтобы между любыми двумя станциями в сети существовал только один активный маршрут, при этом резервные каналы автоматически активируются при отказе основного.

5.3.1 Настройка моста STP (Bridge Settings)

На этой странице пользователь может настроить параметры порта STP. Соответствующее окно настройки отображается при открытии раздела «Advanced Configure > Spanning Tree > Bridge Settings» (рисунок 25).

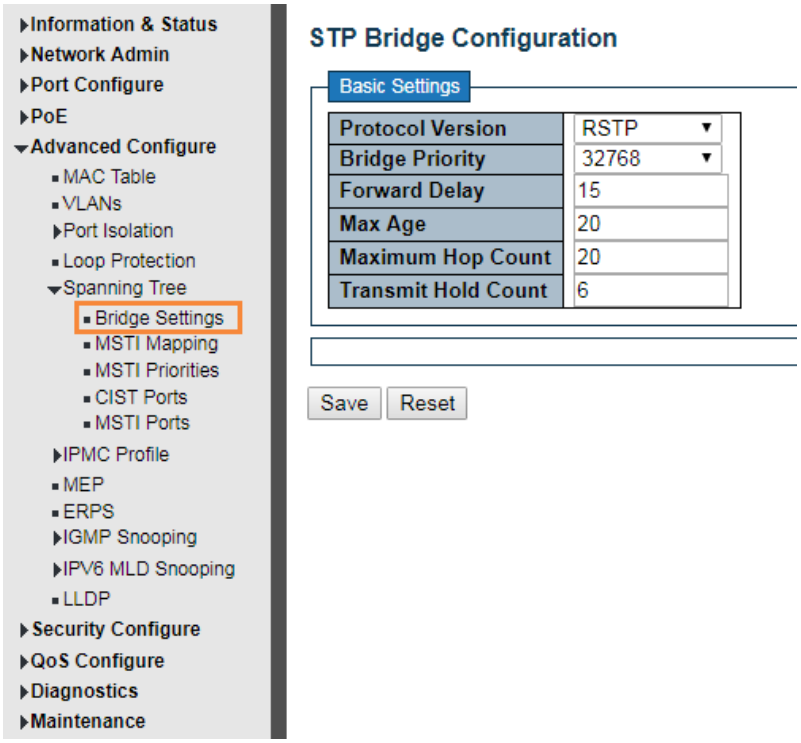

Рисунок 25 — Настройка моста STP

Объекты конфигурации и их описание приведены в таблице 18.

Таблица 18

Параметр	Описание
Protocol Version	Из раскрывающегося меню выбирается версия протокола STP, включая: – STP — протокол основного дерева (IEEE 802.1D); – RSTP — протокол быстрого основного дерева (IEEE 802.1w)
Bridge Priority	Управляет приоритетом моста. Чем меньше числовое значение, тем выше приоритет. Приоритет моста вместе с номером экземпляра MSTI, объединенный с 6-байтовым MAC-адресом коммутатора, формирует Bridge Identifier
Forward Delay (4 – 30)	Диапазон настройки прямой задержки составляет от 4 до 30 секунд. Значение по умолчанию — 15 секунд
Max Age (6 – 40)	Максимальный срок хранения информации, передаваемой мостом, если он является корневым мостом. Допустимые значения находятся в диапазоне от 6 до 40 секунд. Значение по умолчанию – 20
Maximum Hop Count (6 – 40)	Начальное число hops для MSTI, диапазон 6 – 40
Transmit Hold Count (1 – 10)	Максимум BPDU в секунду, диапазон (1 – 10), по умолчанию 6

Для сохранения настроек необходимо нажать кнопку Save.

5.3.2 Отображение MSTI (MSTI Mapping)

Окно настройки отображения MSTI отображается при открытии раздела «Advanced Configure > Spanning Tree > MSTI Mapping» (рисунок 26).

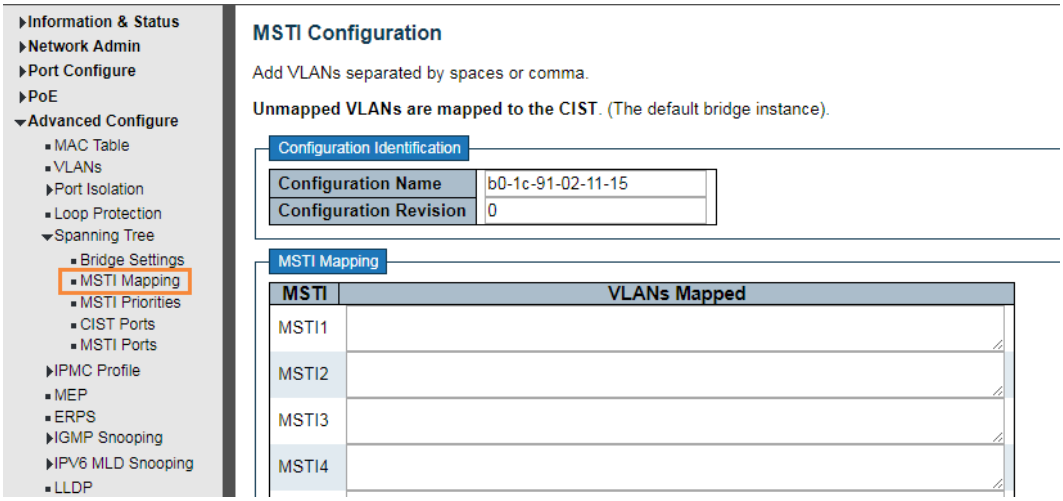

Рисунок 26 — Настройка отображения MSTI

Объекты конфигурации и их описание приведены в таблице 19.

Таблица 19

Параметр	Описание
Configuration Name	Имя домена MSTP.
Configuration Revision	Номер ревизии конфигурации.
MSTI Mapping	Сопоставление VLAN конкретным экземплярам MSTI.

Примечание — Необходимо установить одинаковое значение для имени конфигурации и версии конфигурации всех коммутаторов в замкнутой сети при установке MSTP.

Для сохранения настроек необходимо нажать кнопку Save.

5.3.3 Приоритеты MSTI (MSTI Priorities)

Окно приоритетов MSTI отображается при открытии раздела «Advanced Configure > Spanning Tree > MSTI Priorities» (рисунок 27).

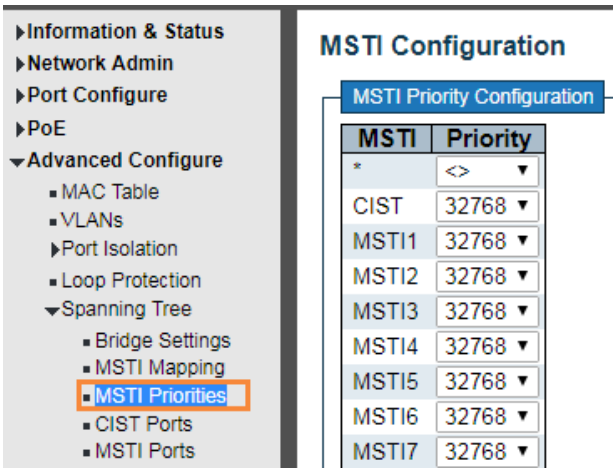

Рисунок 27 —Приоритеты MSTI

Параметр MSTI Priorities устанавливается в диапазоне значений от 0 до 61440.

Примечание — Значение приоритета должно быть кратно 4094 в диапазоне от 0 до 61440.

5.3.4 Порты моста STP (Bridge Ports)

Окно параметров STP на портах отображается при открытии раздела «Advanced Configure > Spanning Tree > Bridge Ports» (рисунок 28).

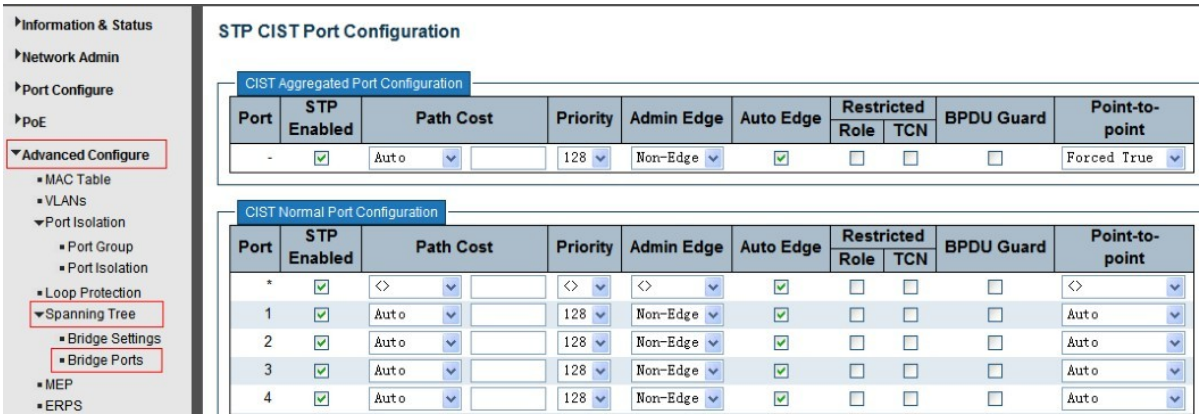

Рисунок 28 — Параметры STP на портах

Объекты конфигурации и их описание приведены в таблице 20.

Таблица 20

Параметр	Описание
STP Enabled	Включение STP на порту.
Path Cost (0=Auto)	Управляет стоимостью пути порта. В режиме автоматической настройки значение стоимости пути выбирается в соответствии со скоростью физического канала с использованием рекомендуемых значений стандарта IEEE 802.1D. При ручной настройке можно задать значение, определяемое пользователем. Стоимость пути используется при построении активной топологии сети. При выборе пути в качестве активных используются порты с меньшей стоимостью пути. Допустимый диапазон значений — от 1 до 200000000
Priority	Управляет приоритетом порта. Используется для выбора между портами с одинаковой стоимостью пути
Auto Edge	Устанавливается флажок, чтобы назначить порту статус Auto Edge
Restricted Role	Устанавливается флажок, чтобы назначить порту статус Restricted Role
Restricted TCN	Устанавливается флажок, чтобы назначить порту статус Restricted TCN
BPDU Guard	Устанавливается флажок, чтобы включить защиту BPDU. В этом случае при получении BPDU порт будет переведен в состояние Shutdown
Point-to-point	Определяет, подключен ли порт к двухточечной сети, а не к среде с общим доступом. Значение может определяться автоматически либо задаваться вручную как true или false. Переход в состояние пересылки для двухточечного соединения выполняется быстрее, чем для среды с общим доступом. Эта настройка относится только к физическим портам. Для агрегированных интерфейсов значение Point-to-Point всегда принудительно включено

Для сохранения настроек необходимо нажать кнопку Save.

5.2.4. Порты MSTI (MSTI Ports)

Окно настройки MSTI на портах отображается при открытии раздела «Advanced Configure > Spanning Tree > MSTI Ports» (рисунок 29).

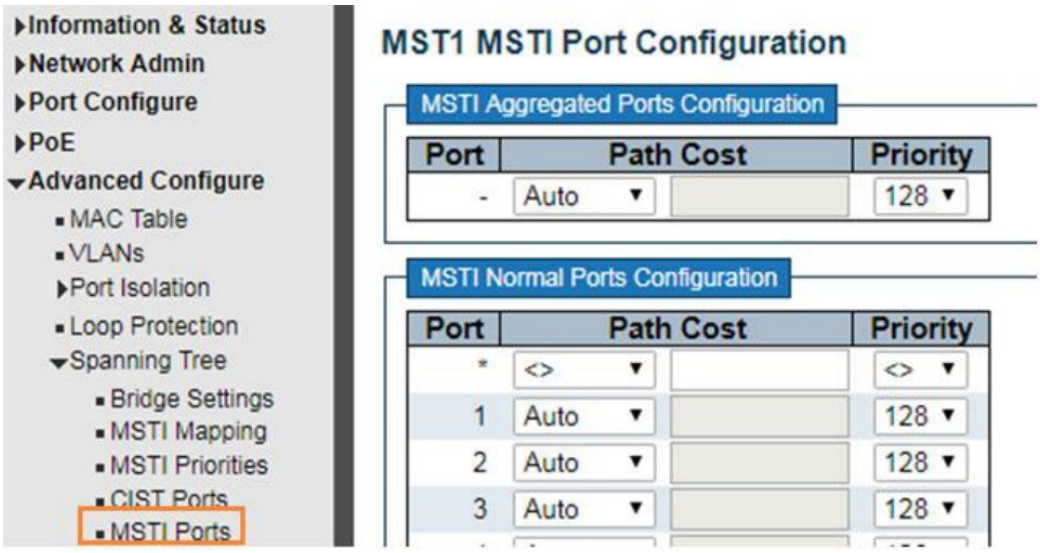

Рисунок 29 — Настройка MSTI на портах

Объекты конфигурации и их описание приведены в таблице 21.

Таблица 21

Параметр	Описание
Path Cost	Этот параметр используется для задания стоимости пути порта при пересылке пакетов по указанному набору портов. Стоимость порта может определяться автоматически либо задаваться вручную. Значение по умолчанию — 0, что соответствует автоматическому режиму. Чем меньше значение, тем выше приоритет порта при выборе для пересылки. Управляет стоимостью пути порта. В автоматическом режиме стоимость пути выбирается в соответствии со скоростью физического канала с использованием рекомендованных значений стандарта IEEE 802.1D. В ручном режиме можно задать пользовательское значение. Стоимость пути используется при построении активной топологии сети: при выборе пути предпочтение отдается портам с меньшей стоимостью пути. Допустимый диапазон значений — от 1 до 200000000
Priority	При одинаковой стоимости пути определяет приоритет порта

Для сохранения настроек необходимо нажать кнопку Save.

5.4 Таблица MAC-адресов (MAC Table)

Окно с таблицей MAC-адресов отображается при открытии раздела «Advanced Configure > MAC Table» (рисунок 30).

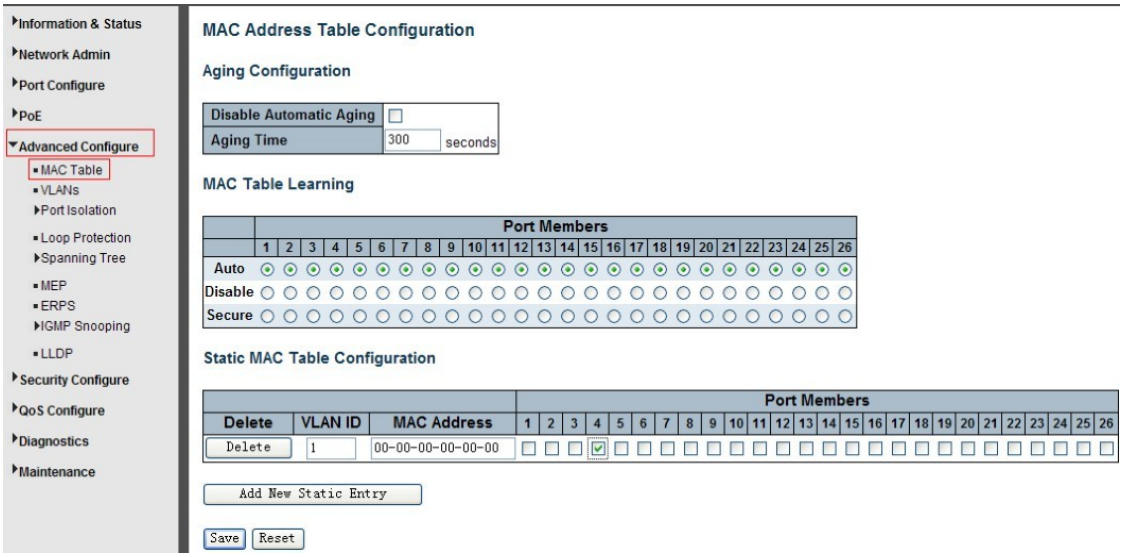

Рисунок 30 — Таблица MAC-адресов

Объекты конфигурации и их описание приведены в таблице 22.

Таблица 22

Параметр	Описание
Disable Automatic Aging	Отключает автоматическое удаление устаревших записей MAC-адресов из таблицы
Aging Time	Время хранения динамической записи; диапазон 10-1000000 секунд, по умолчанию 300 секунд.
MAC Table Learning	Изучение таблицы MAC. Коммутатор поддерживает 3 режима изучения MAC-адресов: – автоматический — порт автоматически изучает MAC-адреса; – отключенный — порт не изучает MAC-адреса; – безопасный — порт передает данные только для заранее настроенного статического MAC-адреса
Static MAC Table Configuration	Таблица статических записей. Создается кнопкой Add New Static Entry

Для сохранения настроек необходимо нажать кнопку Save.

5.5 Отслеживание IGMP (IGMP Snooping)

Протокол управления интернет-группами (IGMP) позволяет хостам и маршрутизаторам обмениваться информацией о членстве в группах многоадресной рассылки. IGMP Snooping — это функция коммутатора, которая отслеживает IGMP-сообщения и передает их в центральный процессор для дальнейшей обработки. Основная цель IGMP Snooping состоит в том, чтобы ограничить пересылку многоадресных кадров только тем портам, которые входят в соответствующую multicast-группу.

5.5.1 Базовая конфигурация

Окно базовой настройки отслеживания IGMP отображается при открытии раздела «Advanced Configure > IGMP Snooping > Basic Configuration» (рисунок 31).

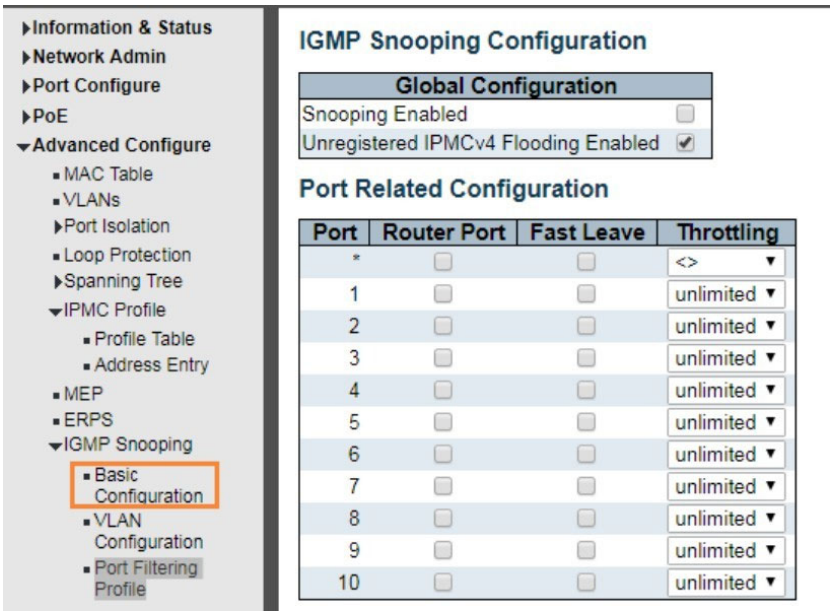

Рисунок 31 — Базовая настройка IGMP Snooping

Объекты конфигурации и их описание приведены в таблице 23.

Таблица 23

Параметр	Описание
Snooping Enabled	Включение или отключение IGMP Snooping
Unregistered IPMCv4 Flooding Enabled	Разрешение или запрет на рассылку незарегистрированного IPv4 multicast-трафика
Router Port	Порты, ведущие к L3 multicast-устройству или IGMP querier
Fast Leave	Немедленно удаляет запись MAC-forwarding при получении сообщения о выходе из группы

Для сохранения настроек необходимо нажать кнопку Save.

5.5.2 Настройка отслеживания IGMP по VLAN

Окно настройки отслеживания IGMP по VLAN отображается при открытии раздела «Advanced Configure > IGMP Snooping > VLAN Configuration» (рисунок 32).

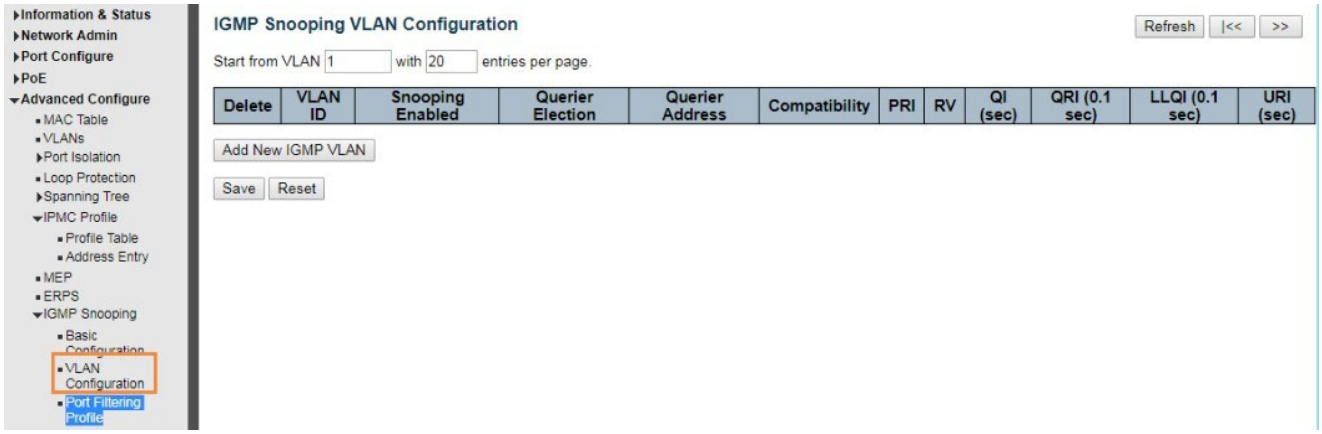

Рисунок 32 — Настройка IGMP Snooping VLAN

Объекты конфигурации и их описание приведены в таблице 24.

Таблица 24

Параметр	Описание
Snooping Enabled	Включается отслеживание IGMP для каждой сети VLAN. Для отслеживания IGMP можно выбрать до 32 сетей VLAN
Querier Election	Включается для присоединения к выбору IGMP-запроса в VLAN. Отключается для обеспечения возможности действовать как IGMP-запрос, не выполняющий функции IGMP-запроса
Querier Address	Задается IPv4-адрес в качестве исходного адреса, используемого в IP-заголовке для запроса IGMP. Если адрес запроса не задан, система использует IPv4-адрес управления IP-интерфейса, связанного с данной VLAN. Если адрес управления IPv4 не задан, система использует первый доступный IPv4-адрес управления. В противном случае используется заранее заданное значение. По умолчанию это значение равно 192.0.2.1

Для сохранения настроек необходимо нажать кнопку Save.

5.5.3 Профиль фильтрации портов

Окно настройки фильтрации портов при отслеживании IGMP отображается при открытии раздела «Advanced Configure > IGMP Snooping > Port Filtering Profile» (рисунок 33).

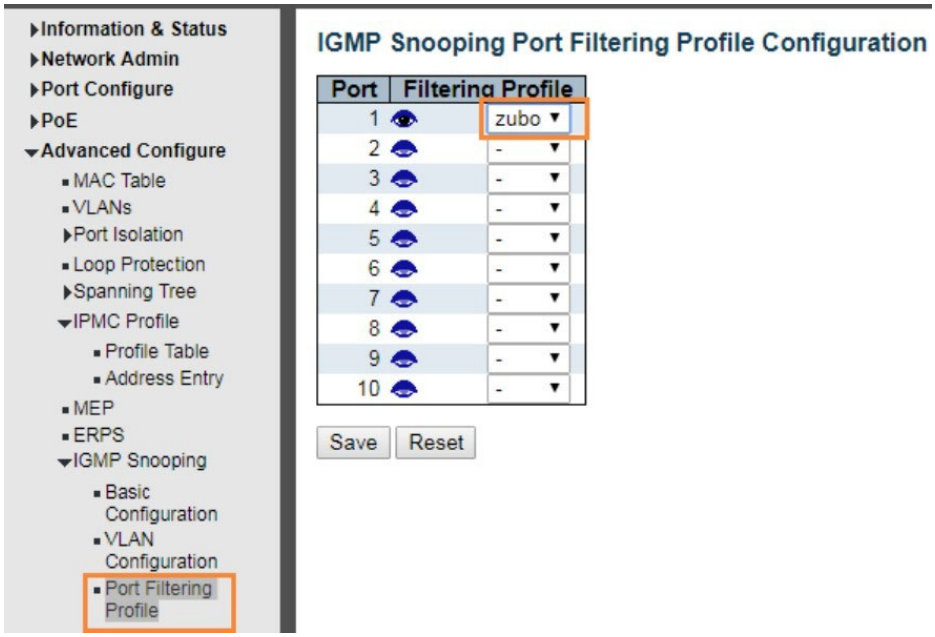

Рисунок 33 — Профиль фильтрации портов

Объекты конфигурации и их описание приведены в таблице 25.

Таблица 25

Параметр	Описание
VLAN ID	Идентификатор VLAN
Enable Snooping	Включается отслеживание IGMP для каждой сети VLAN. Для отслеживания IGMP можно выбрать до 32 сетей VLAN
Querier（Querier Election）	Включается, чтобы коммутатор работал как IGMP Querier в VLAN. Отключается, чтобы коммутатор не выполнял функции IGMP Querier
Querier（Querier Address）	Задается IPv4-адрес в качестве исходного адреса, используемого в IP-заголовке для IGMP-запроса. Если адрес запроса не задан, система использует IPv4-адрес управления IP-интерфейса, связанного с этой VLAN. Если адрес управления IPv4 не задан, система использует первый доступный IPv4-адрес управления. В противном случае система использует заранее заданное значение. По умолчанию это значение равно 192.0.2.1

Для сохранения настроек необходимо нажать кнопку Save.

5.6 Профиль IPMC (IPMC Profile)

Окно добавления диапазона IPMC отображается при открытии раздела «Advanced Configure > IPMC Profile > Address Entry» (рисунок 34).

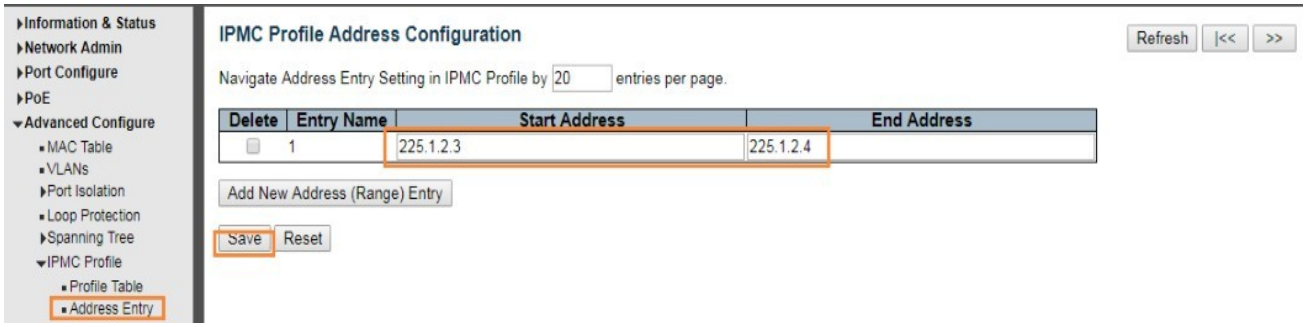

Рисунок 34 — Добавление диапазона IPMC

Объекты конфигурации и их описание приведены в таблице 26.

Таблица 26

Подраздел	Основные поля
Entry Name	Вводится название группы, которую нужно отфильтровать
Start Address	Вводится адрес начальной группы
End Address	Вводится адрес конечной группы

Для сохранения настроек необходимо нажать кнопку Save.

Окно привязки профиля IPMC отображается при открытии раздела «Advanced Configure > IPMC Profile > Profile Table» (рисунок 35).

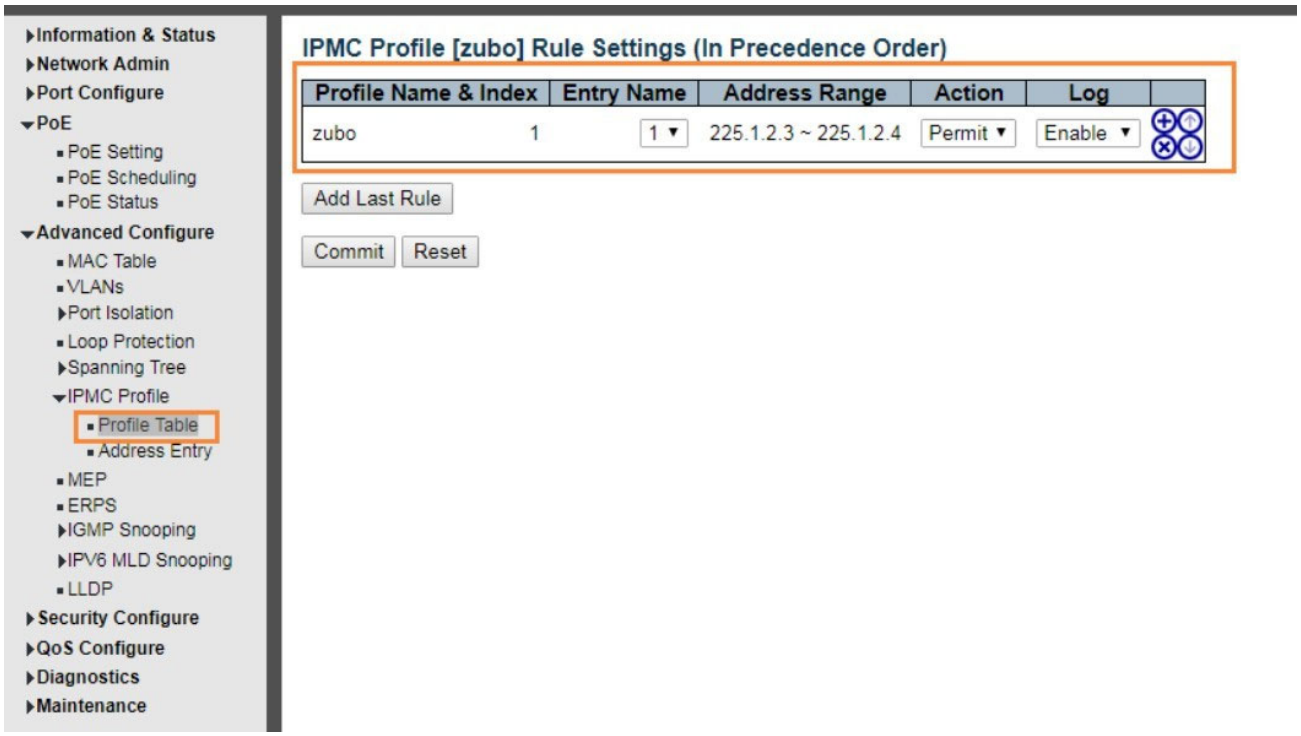

Рисунок 35 — Привязка профиля IPMC

Объекты конфигурации и их описание приведены в таблице 27.

Таблица 27

Подраздел	Основные поля
Entry Name	Выбирается созданная запись адреса через выпадающее меню
Action	Запретить/Разрешить
Log	Включение/выключение

Для сохранения настроек необходимо нажать кнопку Save.

5.7 Отслеживание IPv6 MLD (IPv6 MLD Snooping)

Отслеживание IPv6 MLD — это механизм управления многоадресной рассылкой на коммутаторе Ethernet уровня 2. Когда отслеживание IPv6 MLD включено, коммутатор обрабатывает сообщения MLD, чтобы определить соответствие между интерфейсами и групповыми адресами многоадресной рассылки и на этой основе настроить пересылку многоадресного трафика.

5.7.1 Базовая конфигурация

Окно базовой настройки отслеживания IPv6 MLD отображается при открытии раздела «Advanced Configure > IPV6 MLD Snooping > Basic Configuration» (рисунок 36).

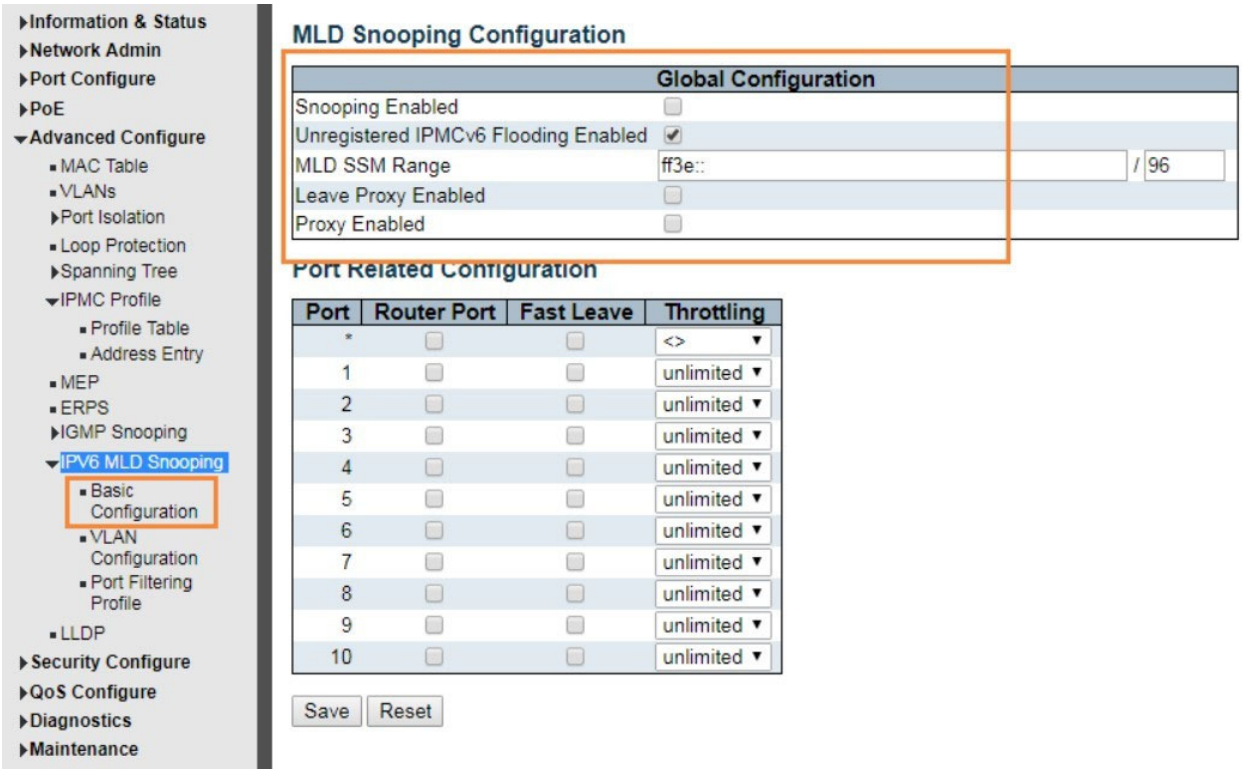

Рисунок 36 — Базовая настройка IPv6 MLD Snooping

Объекты конфигурации и их описание приведены в таблице 28.

Таблица 28

Параметр	Описание
Snooping Enable	Включение или выключение MLD Snooping.
Unregistered IPMCv6 Flooding Enable	Разрешение или запрет на рассылку незарегистрированного IPv4 multicast-трафика
Router Port	Порты, которые используются в качестве портов маршрутизатора. Порт маршрутизатора — это порт коммутатора Ethernet, подключенный к устройству многоадресной рассылки уровня 3 или к источнику запросов MLD. Если в качестве порта маршрутизатора выбран порт участника агрегации, вся группа агрегации будет работать как порт маршрутизатора
Fast Leave	Fast Leave удаляет запись о пересылке MAC-адреса сразу после получения сообщения о выходе из группы

Для сохранения настроек необходимо нажать кнопку Save.

5.7.2 Настройка отслеживания IPv6 MLD по VLAN

Окно настройки отслеживания IPv6 MLD по VLAN отображается при открытии раздела «Advanced Configure > IPV6 MLD Snooping > VLAN Configuration» (рисунок 37).

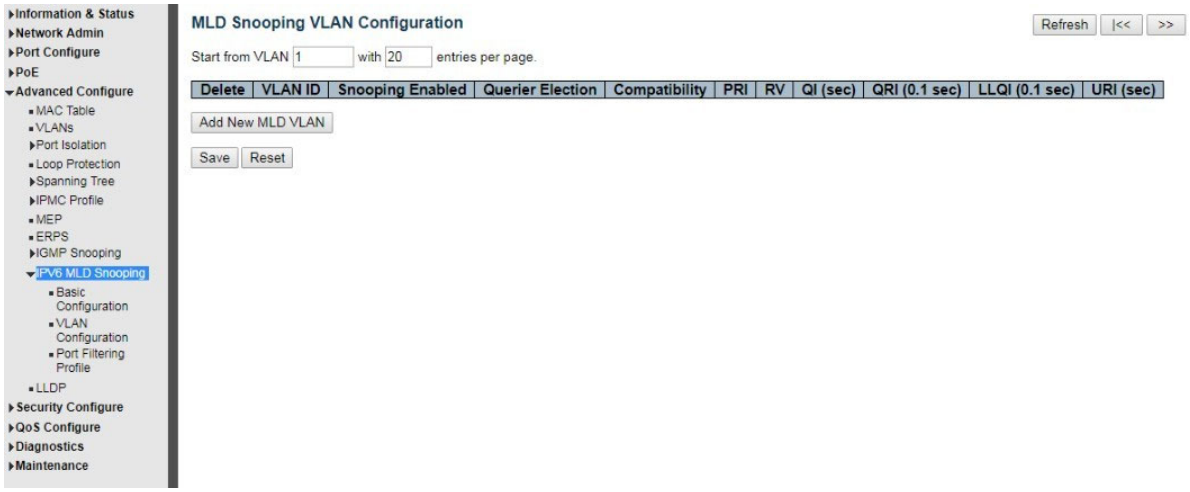

Рисунок 37 — VLAN-параметры IPv6 MLD Snooping

Объекты конфигурации и их описание приведены в таблице 29.

Таблица 29

Параметр	Описание
VLAN ID	Идентификатор VLAN
Snooping Enable	Включение отслеживания IGMP для каждой сети VLAN. Для отслеживания IGMP можно выбрать до 32 сетей VLAN.
Querier（Querier Election）	Разрешение на присоединение к выборам участников запроса MLD в сети VLAN. Параметр отключают, чтобы действовать как участник, не выполняющий запрос MLD

Для сохранения настроек необходимо нажать кнопку Save.

5.8 Протокол ERPS

ERPS (Ethernet Ring Protection Switching) объединяет функции OAM и протокола APS. Если кольцевая сеть неожиданно прерывается, время восстановления после сбоя может составлять менее 50 мс, что позволяет быстро восстановить нормальную работу сети. ITU-T G.8032 — первый отраслевой стандарт для ERPS.

Окно настройки ERPS отображается при открытии раздела «Advanced Configure > ERPS» (рисунок 38).

Примечание — Перед включением ERPS необходимо отключить STP кольцевого порта.

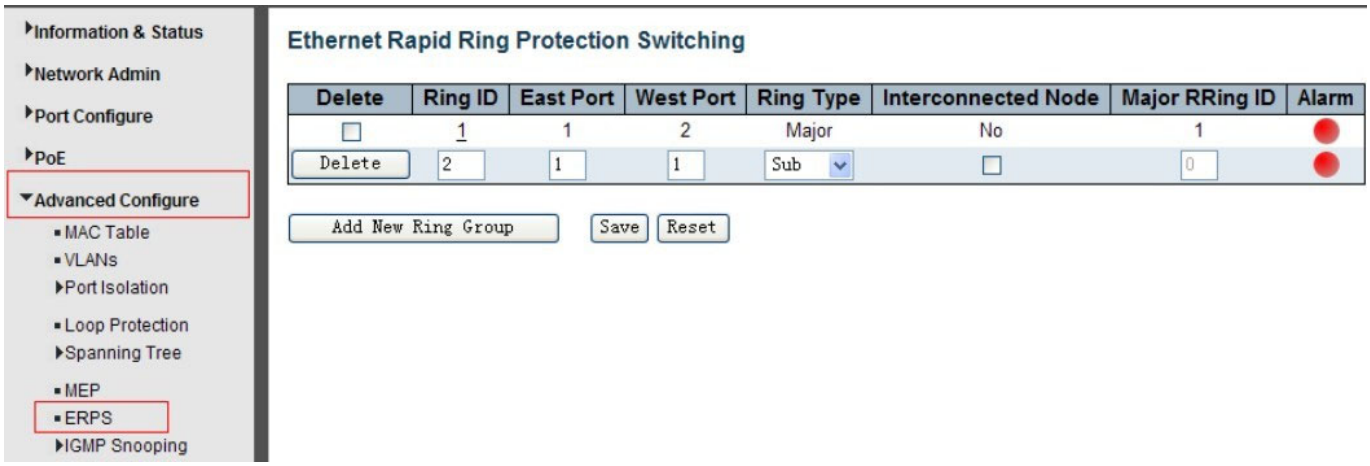

Рисунок 38 — Настройка ERPS

Объекты конфигурации и их описание приведены в таблице 30.

Таблица 30

Параметр	Описание
Ring ID	Идентификатор кольца ERPS
East Port	Номер порта, который участвует в этой кольцевой защите
West Port	Номер другого порта, который участвует в этой кольцевой защите
Ring Type	Доступны варианты: «Основное кольцо» или «Дополнительное кольцо». Настройка «Дополнительного кольца» требуется только в случае приложения с несколькими кольцами. Тип кольца по умолчанию — «Основное кольцо». Устанавливать его нужно только при наличии приложения с несколькими кольцами
Interconnected Node	Узел, который соединяет два и более кольца в режиме Multi Ring.
Major Ring ID	В приложении с одним кольцом идентификатор основного кольца совпадает с идентификатором кольца. В приложении с несколькими кольцами вспомогательное кольцо должно быть введено в качестве идентификатора основного кольца.
R-APS VLAN	VLAN для служебного трафика R-APS.

Чтобы создать новое приложение ERPS ring, необходимо нажать кнопку Add New Ring Group.

Для сохранения настроек необходимо нажать кнопку Save.

После нажатия на номер в разделе Ring ID откроется страница настройки звонка (рисунок 39).

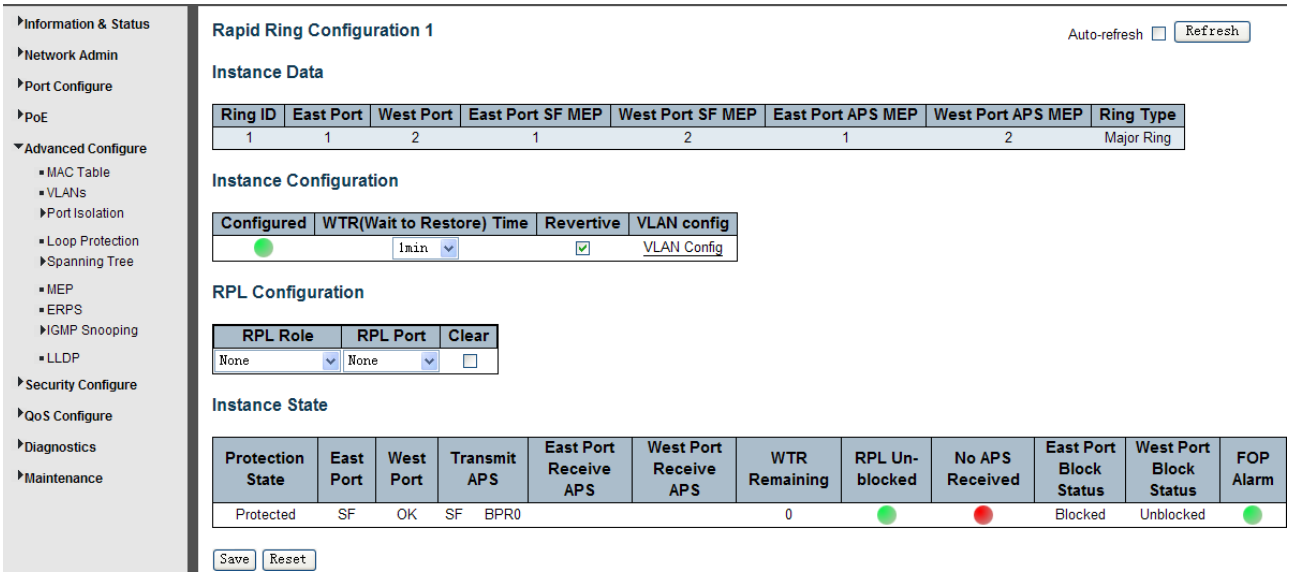

Рисунок 39 — Конфигурация кольца ERPS

Объекты конфигурации и их описание приведены в таблице 31.

Таблица 31

Параметр	Описание
WTR(Wait to Restore) Time	Через раскрывающееся меню выбирается время WTR для R-APS. Доступные значения: 1–12 мин. По умолчанию: 1 мин
Revertive	Выбирается для проверки включения обратного статуса R-APS
VLAN config	Открывает страницу настройки Rapid Ring VLAN
RPLRole	Через раскрывающееся меню выбирается роль «None», «Владелец RPL» или «Сосед RPL»
RPL Port	Через раскрывающееся меню выбирается «None», «East Port» или «West Port»

После нажатия кнопки VLAN config откроется страница настройки кольца VLAN (рисунок 40).

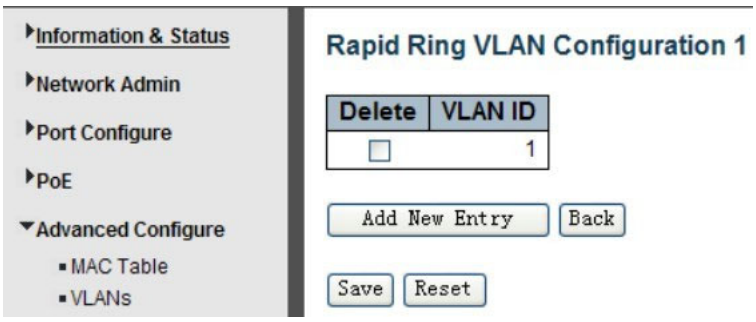

Рисунок 40 — Параметры кольца VLAN

Для создания новой записи необходимо нажать кнопку Add New Entry.

Для сохранения настроек необходимо нажать кнопку Save.

5.9 Протокол LLDP

Протокол обнаружения канального уровня (LLDP) используется для получения базовой информации о соседних устройствах в локальном широковещательном домене. LLDP — это протокол уровня 2, который использует периодические широковещательные объявления для передачи информации об устройстве-отправителе. Рекламируемая информация представляется в формате Type, Length, Value (TLV) в соответствии со стандартом IEEE 802.1AB и может включать сведения об идентификации устройства, его возможностях и параметрах конфигурации. LLDP также определяет, как хранить и обновлять информацию о соседних сетевых узлах, которые он обнаруживает.

Окно настройки LLDP отображается при открытии раздела «Advanced Configure > LLDP» (рисунок 41).

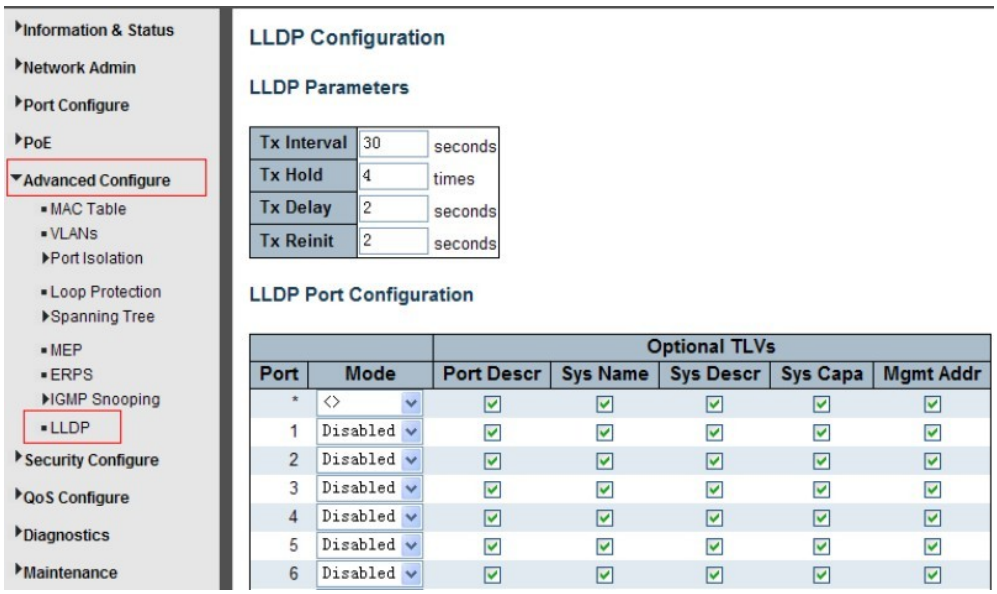

Рисунок 41 — Настройка LLDP

Объекты конфигурации и их описание приведены в таблице 32.

Таблица 32

Параметр	Описание
LLDP Parameters	Здесь пользователь может просматривать и настраивать текущие параметры порта LLDP: Tx Interval (интервал передачи), Tx Hold (множитель времени удержания), Tx Delay (задержка передачи), Tx Remit (время повторной передачи)
Mode	Выбираются режимы передачи и приема сообщений LLDP для блоков данных протокола LLDP. Доступные варианты: только Tx, только Rx, включено и выключено
Optional TLVs	Здесь настраивается информация, включаемая в поле TLV рекламируемых сообщений. Если выбран соответствующий параметр, связанная с ним информация будет включаться в передаваемую LLDP-информацию: Port Descr (описание порта), Sys Name (имя системы), Sys Descr (описание системы), Sys Capa (возможности системы), Mgmt Addr (адрес управления)

Для сохранения настроек необходимо нажать кнопку Save.

5.10 Защита от петель (Loop Protection)

Защита от петель предназначена для предотвращения зацикливания в сети. Окно настройки защиты от петель отображается при открытии раздела «Advanced Configure > Loop Protection» (рисунок 42).

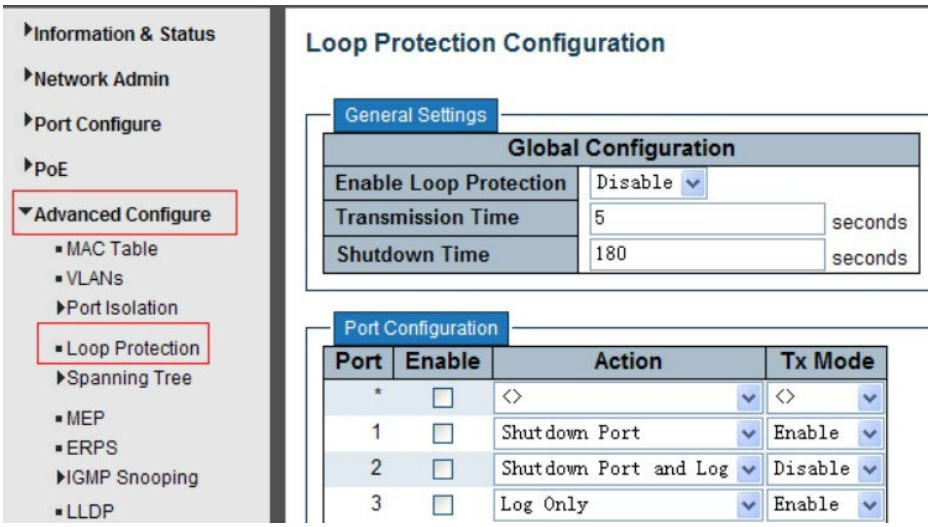

Рисунок 42 — Настройка защиты от петель

Объекты конфигурации и их описание приведены в таблице 33

Таблица 33

Параметр	Описание
Global Configuration	Включение защиты от петель: выбирается в раскрывающемся списке, чтобы включить или отключить защиту от петель. Время передачи: вводится число, чтобы задать интервал защиты от петель. Время отключения: вводится число, чтобы задать время отключения порта.
Enable	Установите флажок, чтобы включить соответствующую защиту порта от петель.
Action	Действие, выполняемое при обнаружении петли на порту. Доступны 3 варианта: – отключить порт; – отключить порт и вести журнал; – только вести журнал
Tx Mode	Включение или отключение передачи данных

Для сохранения настроек необходимо нажать кнопку Save.

6 Настройка QoS

Качество обслуживания (QoS) — это расширенная функция приоритизации трафика, которая позволяет управлять сетевым трафиком. QoS дает возможность назначать разные уровни сетевого обслуживания для различных типов трафика, таких как мультимедийный, видео, протокольный, критичный ко времени и трафик резервного копирования файлов. Эта функция не только позволяет резервировать полосу пропускания, но и ограничивать менее важный трафик.

6.1 Классификация трафика по портам (Port Classification)

Окно настройки классификации трафика по портам отображается при открытии раздела «QoS Configure > Port Classification» (рисунок 43)

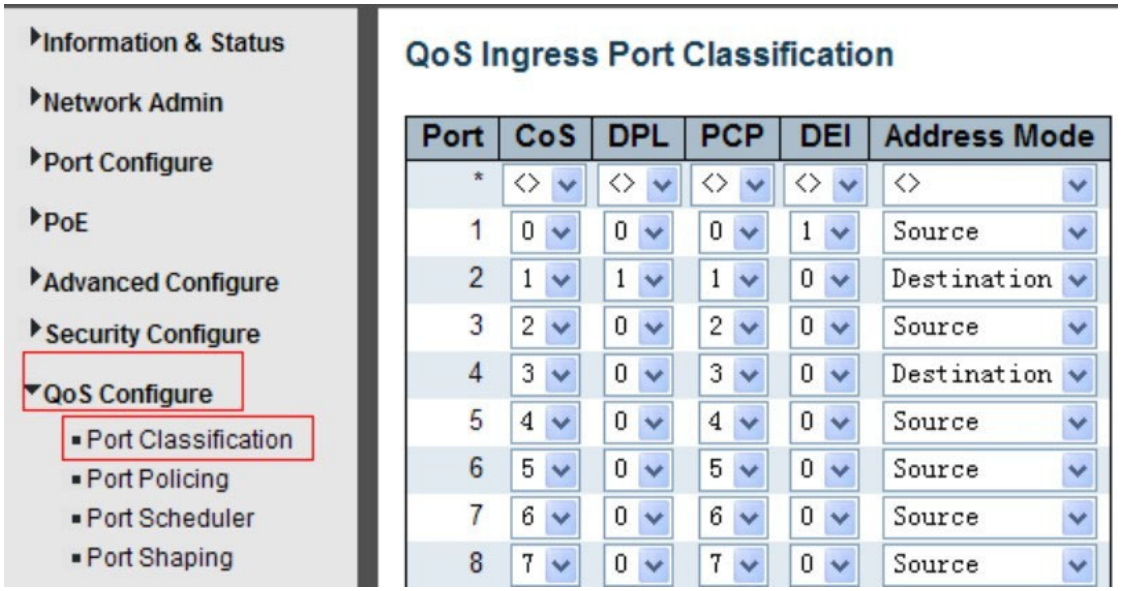

Рисунок 43 — Классификация QoS по портам

Объекты конфигурации и их описание приведены в таблице 34.

Таблица 34

Параметр	Описание
CoS	Определяет значение класса обслуживания по умолчанию в диапазоне от 0 (самый низкий) до 7 (самый высокий). Все кадры классифицируются по CoS. Между CoS, очередью и приоритетом существует соответствие «один к одному». CoS 0 имеет самый низкий приоритет. Назначенный CoS может быть переопределен записью QCL*
DPL	Управляет уровнем приоритета отбрасывания по умолчанию. Все кадры классифицируются по уровню приоритета отбрасывания. Классифицированный DPL может быть отменен с помощью записи QCL

Параметр	Описание
PCP	Управляет значением PCP по умолчанию. Все кадры классифицируются по значению PCP. Если порт поддерживает VLAN и кадр помечен, то он классифицируется по значению PCP в теге. В противном случае кадр классифицируется по значению PCP по умолчанию
DEI	Управляет значением DEI по умолчанию. Все кадры классифицируются по значению DEI. Если порт поддерживает VLAN и кадр помечен, то он классифицируется по значению DEI в теге. В противном случае кадр классифицируется по значению DEI по умолчанию
Address Mode	Режим IP/MAC-адреса, определяющий, должна ли классификация QCL основываться на адресах источника (SMAC/SIP) или назначения (DMAC/DIP) на этом порту. Допустимыми значениями являются: Источник: Включить сопоставление SMAC/SIP. Назначение: Включить сопоставление DMAC/DIP
*Если значение CoS по умолчанию было динамически изменено, фактическое значение CoS по умолчанию отображается в скобках после настроенного значения	

Для сохранения настроек необходимо нажать кнопку Save.

6.2 Контроль портов (Port Policing)

Окно настройки контроля портов отображается при открытии раздела «QoS Configure > Port Policing» (рисунок 44).

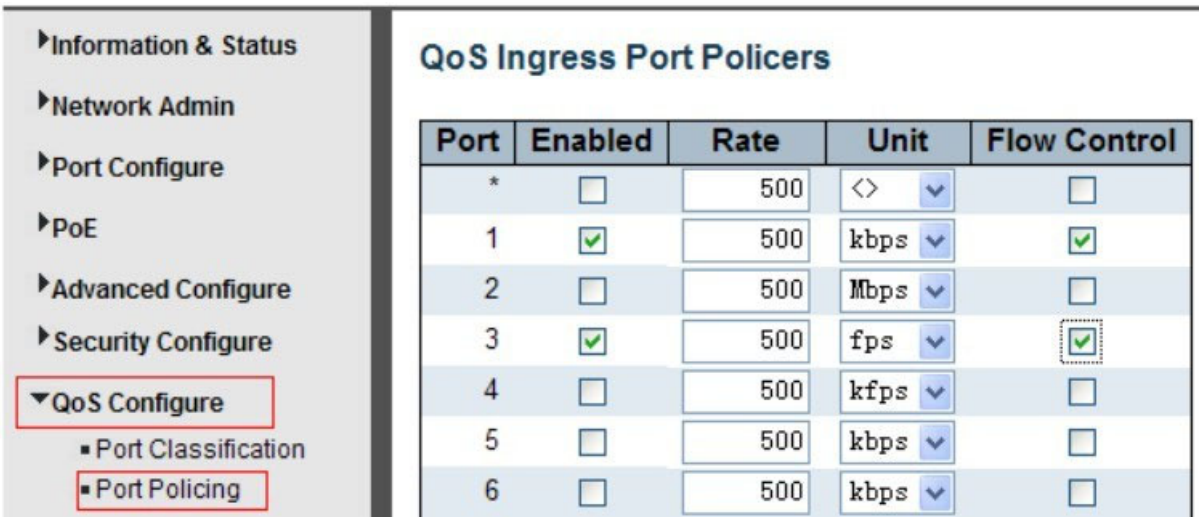

Рисунок 44 — Настройка контроля портов

Объекты конфигурации и их описание приведены в таблице 35.

Таблица 35

Параметр	Описание
Enabled	Флажок устанавливается, чтобы включить контроль портов
Rate	Управляет скоростью политики. Значение по умолчанию — 500. Это значение ограничено от 100 до1000000, если «Единицей измерения» является «кбит/с» или «кадр/с», и от 1 до 3300, если «Единицей измерения» является «Мбит/с» или «кф/с»
Unit	Определяет единицу измерения скорости работы политики устройства в кбит/с, Мбит/с, кадрах в секунду или фпс. Значение по умолчанию — «кбит/с»
Flow Control	Если управление потоком включено и порт находится в режиме управления потоком, то кадры паузы отправляются вместо отбрасывания кадров

Для сохранения настроек необходимо нажать кнопку Save.

6.3 Настройка Storm Control

Окно настройки Storm Control отображается при открытии раздела «QoS Configure > Storm Control» (рисунок 45).

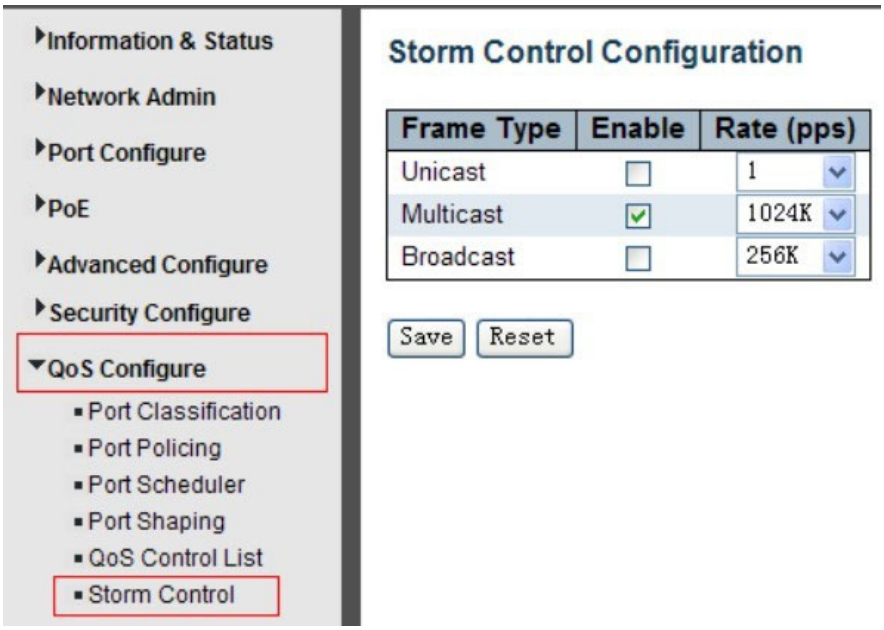

Рисунок 45 —Настройка Storm Control

Объекты конфигурации и их описание приведены в таблице 36.

Таблица 36

Параметр	Описание
Frame Type	Коммутатор поддерживает 3 типа кадров: Unicast, Unknown Multicast или Broadcast
Enable	Флажок устанавливается, чтобы включить управление шторм-контролем
Rate (pps)	Количество данных в секунду (pps). Допустимые значения:1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1 КБ, 2 КБ, 4 КБ, 8 КБ, 16 КБ, 32 КБ, 64 КБ, 128 КБ, 256 КБ, 512 КБ или 1024 КБ

Для сохранения настроек необходимо нажать кнопку Save.

7 Настройка безопасности

7.1 Пароль (Password)

В разделе «Security Configure > Password» пользователь может изменить пароль входа в систему (рисунок 46). После изменения необходимо нажать Save.

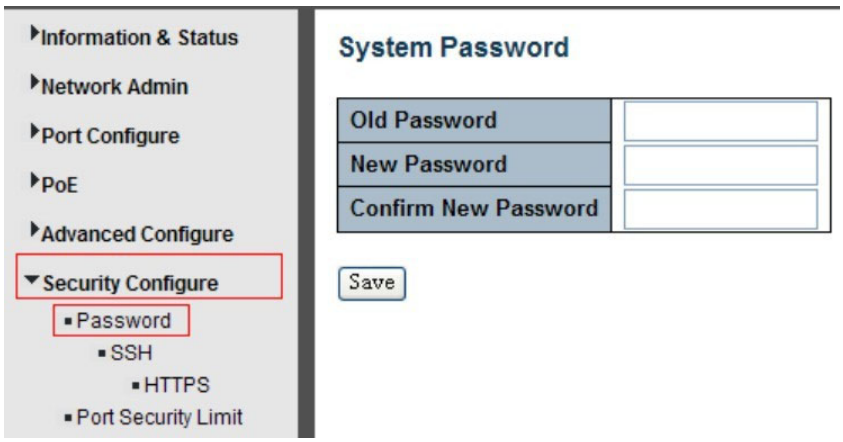

Рисунок 46 — Смена системного пароля

7.2 Стандарт 802.1X

В архитектуре 802.1X пользователь называется supplicant, коммутатор — authenticator, а сервер RADIUS — сервером аутентификации. Коммутатор выступает посредником и пересылает запросы и ответы между supplicant и сервером аутентификации. Кадры, передаваемые между supplicant и коммутатором, являются специальными кадрами 802.1X и называются EAPOL (EAP over LANs). Кадры EAPOL инкапсулируют EAP PDU (RFC 3748). Кадры, передаваемые между коммутатором и сервером RADIUS, являются пакетами RADIUS.

Пакеты RADIUS также инкапсулируют EAP PDU и содержат дополнительные атрибуты, например, IP-адрес коммутатора, его имя и номер порта supplicant на коммутаторе. EAP является гибким протоколом, поскольку поддерживает различные методы аутентификации, такие как MD5-Challenge, PEAP и TLS. При этом аутентификатору, то есть коммутатору, не нужно знать, какой метод аутентификации используется и сколько кадров обмена требуется для его выполнения. Коммутатор просто инкапсулирует часть EAP в соответствующий тип кадра — EAPOL или RADIUS — и пересылает ее.

После завершения аутентификации сервер RADIUS отправляет специальный пакет с результатом проверки — успешным или неуспешным. Коммутатор не только передает это решение supplicant, но и использует его, чтобы разрешить или заблокировать трафик на порту, к которому подключен supplicant.

Стандарт IEEE 802.1X определяет протокол управления доступом и аутентификации на основе модели клиент-сервер, который ограничивает подключение неавторизованных клиентов к LAN через общедоступные порты. Сервер аутентификации проверяет каждого клиента, подключенного к порту коммутатора, прежде чем предоставить ему доступ к службам коммутатора или локальной сети.

Пока клиент не аутентифицирован, управление доступом 802.1X разрешает через порт только трафик EAPOL. После успешной аутентификации через порт может передаваться обычный трафик.

Коммутатор поддерживает аутентификацию 802.1X на основе портов. На этой странице пользователь может настроить параметры 802.1X. После перехода в раздел «Security Configure > 802.1X» откроется соответствующая страница (рисунок 47).

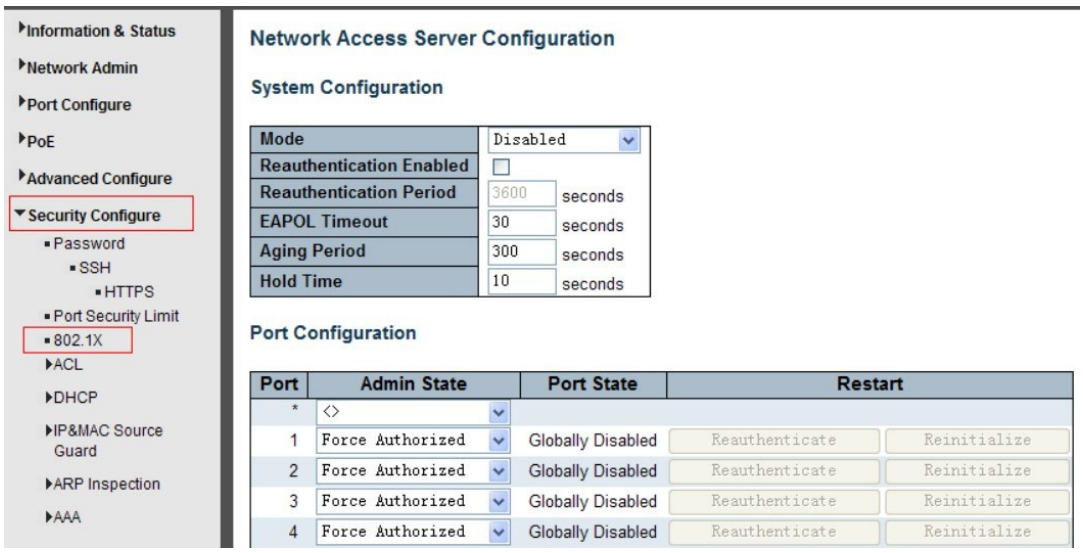

Рисунок 47 — Параметры 802.1X

Объекты конфигурации и их описание приведены в таблице 37.

Таблица 37

Параметр	Описание
System Configuration	Включение/отключение 802.1X и Re- authentication; настройка Re-authentication Period, EAPOL Timeout, Aging Period и Hold Time
Port Configuration	Из выпадающего меню выбирается режим администратора. Доступные опции: Принудительная авторизация, принудительная авторизация без разрешения, 802.1X, авторизация на базе Mac

Для сохранения настроек необходимо нажать кнопку Save.

7.3 Настройка AAA

7.3.1 Протокол RADIUS

Окно настройки RADIUS отображается при открытии раздела «Security Configure > AAA > RADIUS» (рисунок 48).

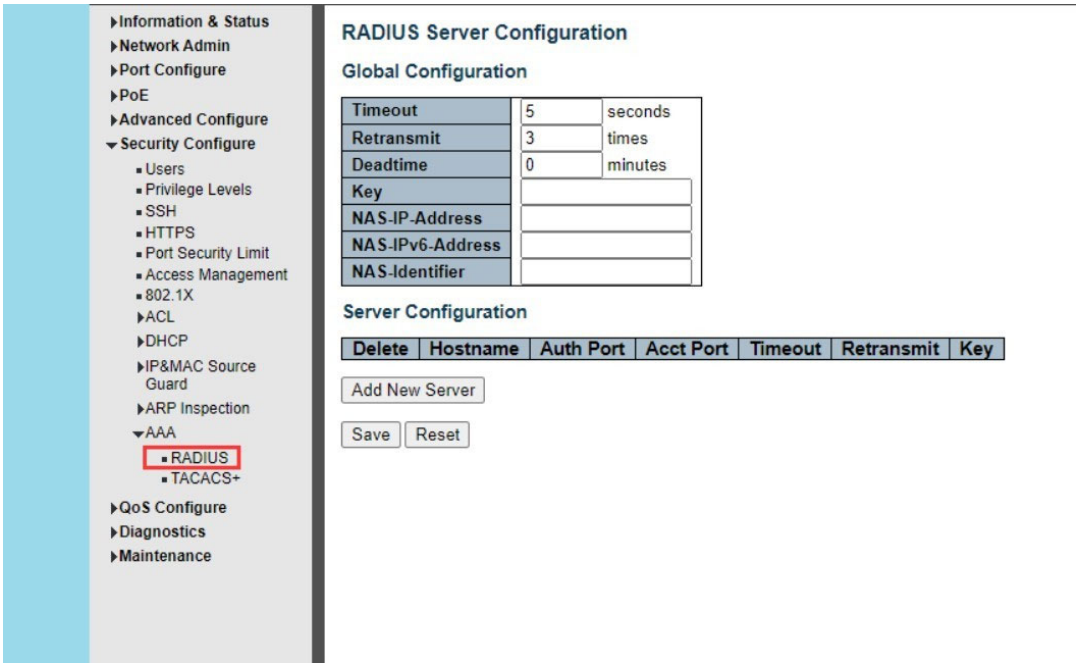

Рисунок 48 — Настройка RADIUS

Объекты конфигурации (Global Configuration) и их описание приведены в таблице 38.

Таблица 38

Параметр	Описание
Timeout	Количество секунд в диапазоне от 1 до 1000, в течение которых ожидается ответ от сервера RADIUS перед повторной отправкой запроса
Retransmit	Количество попыток в диапазоне от 1 до 1000, в течение которых запрос RADIUS повторно отправляется на неотвечающий сервер. Если сервер не ответил после последней попытки повторной передачи, он считается недоступным
Deadtime	Период, который можно задать в диапазоне от 0 до 1440 минут, в течение которого коммутатор не будет отправлять новые запросы серверу, не ответившему на предыдущий запрос. Это предотвращает постоянные попытки связаться с сервером, который уже определен как недоступный. Установка значения Deadtime больше 0 включает эту функцию, но только если настроено более одного сервера
Key	Секретный ключ длиной до 63 символов, использующийся совместно сервером RADIUS и коммутатором

Параметр	Описание
NAS-IP-Address (Attribute 4)	IPv4-адрес, используемый как атрибут 4 в пакетах RADIUS Access-Request. Если это поле оставить пустым, будет использован IP-адрес исходящего интерфейса
NAS-IPv6-Address (Attribute 95)	IPv6-адрес, используемый как атрибут 95 в пакетах RADIUS Access-Request. Если это поле оставить пустым, будет использован IP-адрес исходящего интерфейса
NAS-Identifier (Attribute 32)	Идентификатор длиной до 253 символов, используемый как атрибут 32 в пакетах RADIUS Access-Request. Если это поле оставить пустым, NAS-Identifier не будет включен в пакет

Объекты конфигурации (Server Configuration) и их описание приведены в таблице 39.

Таблица 39

Параметр	Описание
Delete	Флажок устанавливается, чтобы удалить запись сервера RADIUS. Запись будет удалена при следующем сохранении
Hostname	IP-адрес или имя хоста сервера RADIUS
Auth Port	[UDP]-порт, используемый на сервере RADIUS для аутентификации. Чтобы отключить аутентификацию, необходимо установить значение 0
Acct Port	[UDP]-порт, используемый на сервере RADIUS для учета. Чтобы отключить учет, необходимо установить значение 0
Timeout	Эта необязательная настройка переопределяет глобальное значение тайм-аута. Если оставить поле пустым, будет использовано глобальное значение тайм-аута
Retransmit	Эта необязательная настройка переопределяет глобальное значение повторной передачи. Если оставить поле пустым, будет использовано глобальное значение повторной передачи
Key	Эта необязательная настройка переопределяет глобальный ключ. Если оставить поле пустым, будет использован глобальный ключ

Для добавления нового сервера RADIUS необходимо нажать кнопку Add New Server. В таблицу будет добавлена пустая строка, после чего сервер RADIUS можно настроить по необходимости. Поддерживается до 5 серверов. Кнопка Cancel позволяет отменить добавление нового сервера.

Для сохранения настроек необходимо нажать кнопку Save.

Для отмены всех локальных изменений и восстановления ранее сохраненных значений необходимо нажать кнопку Reset.

7.3.2 Протокол TACACS+

Окно настройки TACACS+ отображается при открытии раздела «Security Configure > AAA > TACACS+» (рисунок 49).

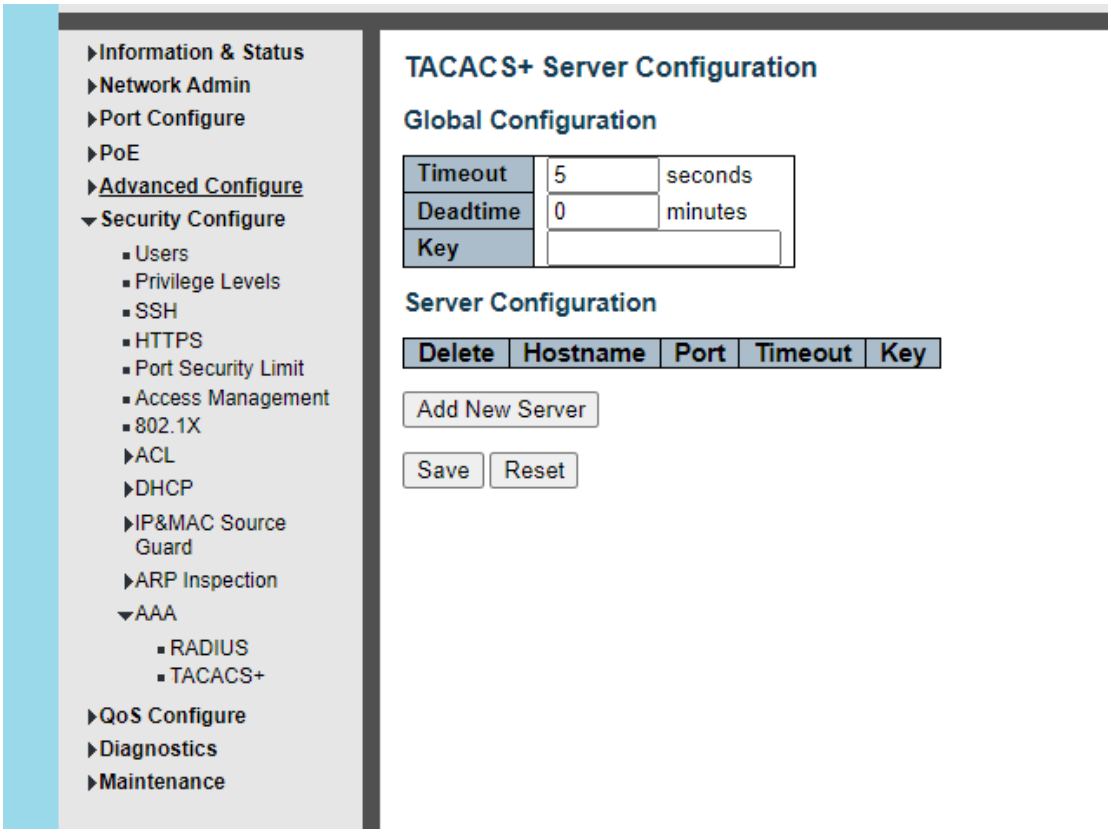

Рисунок 49

Объекты конфигурации и их описание приведены в таблице 40.

Таблица 40

Параметр	Описание
Timeout	Количество секунд в диапазоне от 1 до 1000, в течение которых ожидается ответ от сервера TACACS+ перед повторной отправкой запроса
Deadtime	Период, который можно задать в диапазоне от 0 до 1440 минут, в течение которого коммутатор не будет отправлять новые запросы серверу, не ответившему на предыдущий запрос. Это предотвращает постоянные попытки связаться с сервером, который уже определен как недоступный. Установка значения Deadtime больше 0 включает эту функцию, но только если настроено более одного сервера
Key	Секретный ключ длиной до 63 символов, использующийся совместно сервером TACACS+ и коммутатором

Объекты конфигурации (Server Configuration) и их описание приведены в таблице 41.

Таблица 41

Параметр	Описание
Delete	Флажок устанавливается, чтобы удалить запись сервера TACACS+. Запись будет удалена при следующем сохранении
Hostname	IP-адрес или имя хоста сервера TACACS+
Port	TCP-порт, используемый на сервере TACACS+ для аутентификации
Timeout	Эта необязательная настройка переопределяет глобальное значение тайм-аута. Если оставить поле пустым, будет использовано глобальное значение тайм-аута
Key	Эта необязательная настройка переопределяет глобальный ключ. Если оставить поле пустым, будет использован глобальный ключ

Для добавления нового сервера TACACS+ необходимо нажать кнопку Add New Server. В таблицу будет добавлена пустая строка, после чего сервер TACACS+ можно настроить по необходимости. Поддерживается до 5 серверов. Кнопка Cancel позволяет отменить добавление нового сервера.

Для сохранения настроек необходимо нажать кнопку Save.

Для отмены всех локальных изменений и восстановления ранее сохраненных значений необходимо нажать кнопку Reset.

7.4 Отслеживание DHCP (DHCP Snooping)

7.4.1 Обзор DHCP

Протокол DHCP широко используется для динамического выделения повторно используемых сетевых ресурсов, таких как IP-адрес. Типичный процесс получения IP-адреса по DHCP представлен на рисунке 50.

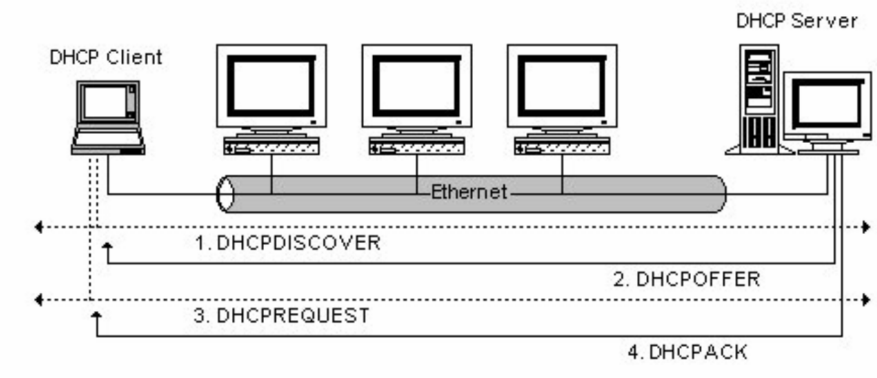

Рисунок 50

DHCP-клиент отправил сообщение DHCP DISCOVER на DHCP-сервер, если клиент не получил ответа от сервера в течение определенного периода времени, он повторно отправит сообщение DHCP DISCOVER.

После получения сообщения DHCP DISCOVER DHCP-сервер назначит источники (например, IP-адрес) клиенту, а затем отправит DHCP-клиенту сообщение с предложением DHCP.

После получения сообщения о предложении DHCP клиент DHCP отправляет DHCP-запрос на предоставление сервера в аренду и уведомляет другие серверы о том, что он принял этот сервер для назначения адресов.

После получения запроса DHCP сервер проверит, может ли ресурс быть выделен. Если все в порядке, он отправит сообщение DHCP ACK, если нет, он отправит сообщение DHCP NAK. После получения сообщения DHCP ACK начните использовать источник, который назначил сервер. Если получен DHCP NAK, DHCP-клиент повторно отправит сообщение об обнаружении DHCP.

7.4.2 Назначение DHCP Snooping

Адреса, назначаемые DHCP-клиентам на небезопасных портах, можно тщательно контролировать с помощью динамических привязок, регистрируемых функцией DHCP Snooping. DHCP Snooping позволяет коммутатору защищать сеть от неавторизованных DHCP-серверов и других устройств, которые отправляют в DHCP-сервер сведения о портах. Эта информация может быть полезна для определения физического порта, к которому привязан IP-адрес.

Использование команды:

– сетевой трафик может быть нарушен при получении вредоносных DHCP-сообщений из внешнего источника. DHCP Snooping используется для фильтрации DHCP-сообщений, поступающих на небезопасный интерфейс из-за пределов сети или межсетевого экрана. Если DHCP Snooping включен глобально и включен на интерфейсе VLAN, DHCP-сообщения, полученные на ненадежном интерфейсе от устройства, не указанного в таблице DHCP Snooping, будут отброшены;

– записи таблицы создаются только для доверенных интерфейсов. Запись добавляется в таблицу DHCP Snooping или удаляется из нее динамически, когда клиент получает или освобождает IP-адрес от DHCP-сервера. Каждая запись включает MAC-адрес, IP-адрес, время аренды, идентификатор VLAN и идентификатор порта;

– когда DHCP Snooping включен, DHCP-сообщения, поступающие на ненадежный интерфейс, фильтруются на основе динамических записей, полученных с помощью DHCP Snooping;

– если DHCP-пакет от клиента проходит критерии фильтрации, он будет передан только на доверенные порты в той же VLAN;

– если DHCP-пакет от сервера получен на доверенном порту, он будет передан как на доверенные, так и на ненадежные порты в той же VLAN;

– если DHCP Snooping глобально отключен, все динамические привязки удаляются из таблицы привязок.

7.4.3 Настройка отслеживания DHCP

Окно настройки отслеживания DHCP отображается при открытии раздела «Security Configure > DHCP > Snooping Setting» (рисунок 51).

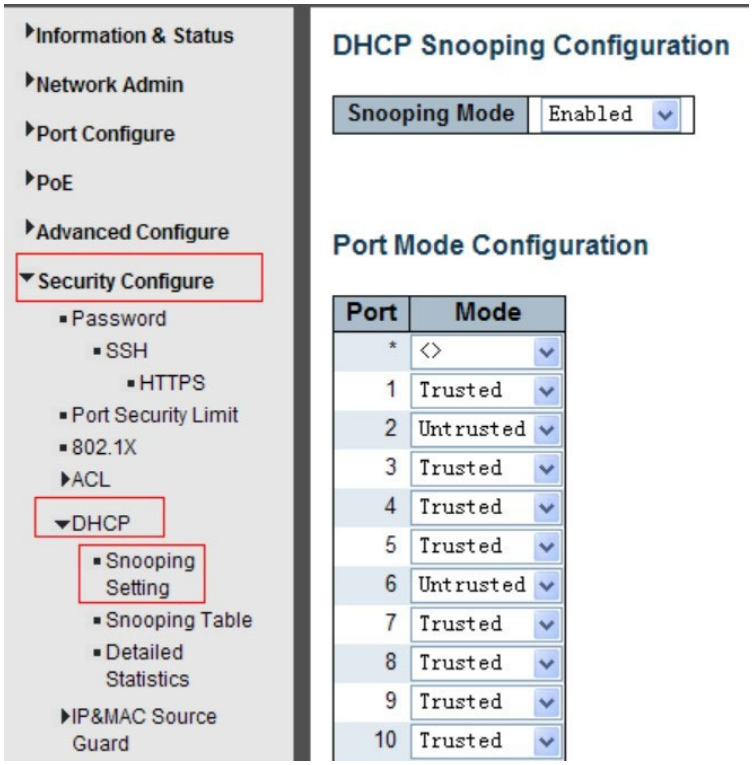

Рисунок 51 — DHCP Snooping

Объекты конфигурации и их описание приведены в таблице 42.

Таблица 42

Параметр	Описание
DHCP Snooping Mode	Включение или выключение отслеживания DHCP через выпадающее меню
Port Mode	Указывает режим порта DHCP Snooping. Возможные режимы порта: Trusted: настраивает порт как доверенный источник DHCP-сообщений. Untrusted: настраивает порт как недоверенный источник DHCP-сообщений.

Для сохранения настроек необходимо нажать кнопку Save.

7.5 Функция IP & MAC Source Guard

IP & MAC Source Guard — это функция безопасности, которая ограничивает IP-трафик на недоверенных портах DHCP Snooping, фильтруя трафик на основе таблицы DHCP Snooping или вручную настроенных привязок IP Source Binding. Она помогает предотвращать атаки подмены IP-адреса, когда хост пытается использовать IP-адрес другого устройства.

7.5.1 Конфигурация порта

Окно настройки Source Guard отображается при открытии раздела «Security Configure > IP&MAC Source Guard > Configuration» (рисунок 52).

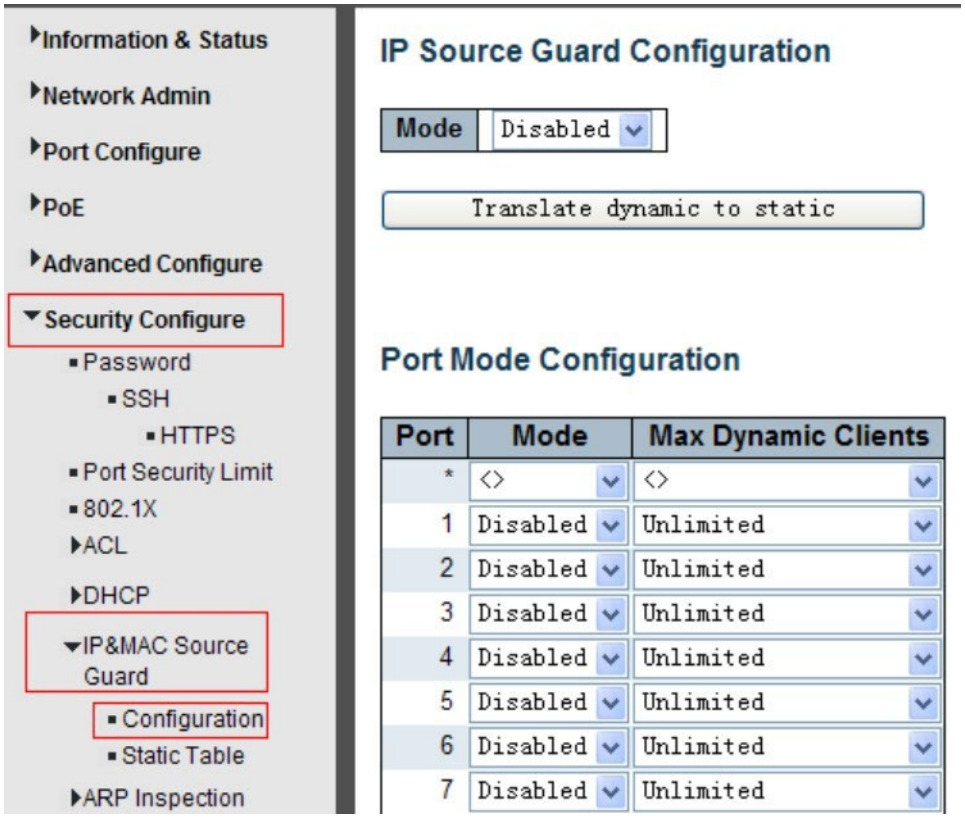

Рисунок 52 — Source Guard на портах

Объекты конфигурации и их описание приведены в таблице 43.

Таблица 43

Параметр	Описание
Global Mode	Включение/выключение глобальной функции защиты IP-адресов и MAC-адресов от несанкционированного доступа через выпадающее меню
Port Mode	Включение/отключение защиты для конкретного порта
Max Dynamic Clients	Максимум динамических клиентов: Unlimited, 0, 1 или 2

Для сохранения настроек необходимо нажать кнопку Save.

7.5.2 Статическая таблица

Статическая таблица Source Guard отображается при открытии раздела «Security Configure > IP&MAC Source Guard > Static Table» (рисунок 53).

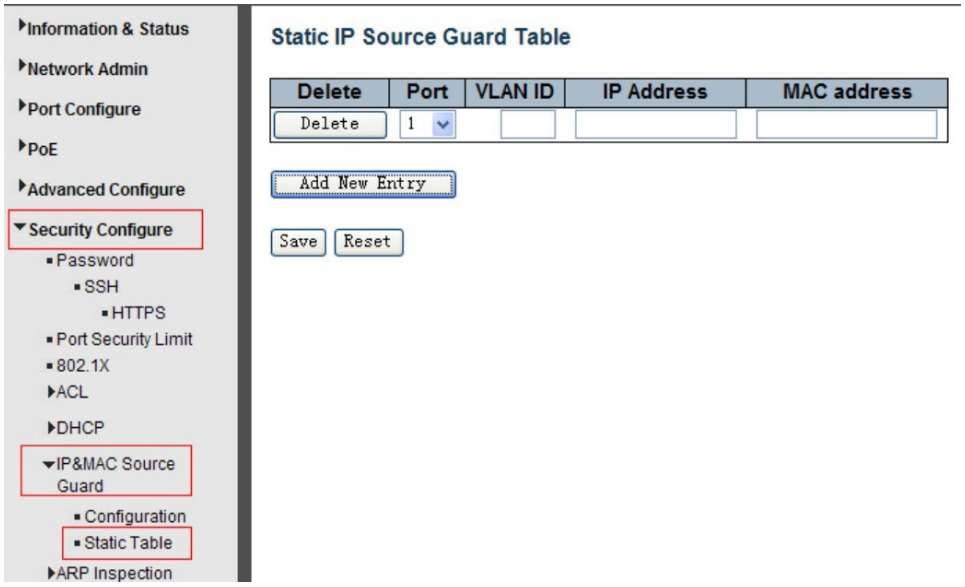

Рисунок 53 — Статическая таблица Source Guard

Объекты конфигурации и их описание приведены в таблице 44.

Таблица 44

Параметр	Описание
Port	Через выпадающее меню выбирается, какой порт следует зафиксировать
VLAN	Вводится VLAN ID, который должен быть зафиксирован
IP Address	Вводится IP-адрес, который должен быть зафиксирован
MAC Address	Вводится MAC-адрес, который должен быть зафиксирован

Для создания новой записи необходимо нажать кнопку Add New Entry.

Для сохранения настроек необходимо нажать кнопку Save.

7.6 Функция ARP Inspection

Dynamic ARP Inspection (DAI) — это функция безопасности. На устройства и хосты, подключенные к сетям уровня 2, могут быть совершены различные атаки путем «отравления» кэша ARP. Эта функция используется для блокировки таких атак. Через DUT могут проходить только действительные ARP-запросы и ARP-ответы. Dynamic ARP Inspection предотвращает прохождение недоверенных ARP-пакетов на основе базы данных DHCP Snooping. На этой странице настраиваются параметры, связанные с ARP Inspection.

7.6.1 Конфигурация портов

Окно настройки ARP Inspection отображается при открытии раздела «Security Configure > IP&MAC Source Guard > Port Configuration» (рисунок 54).

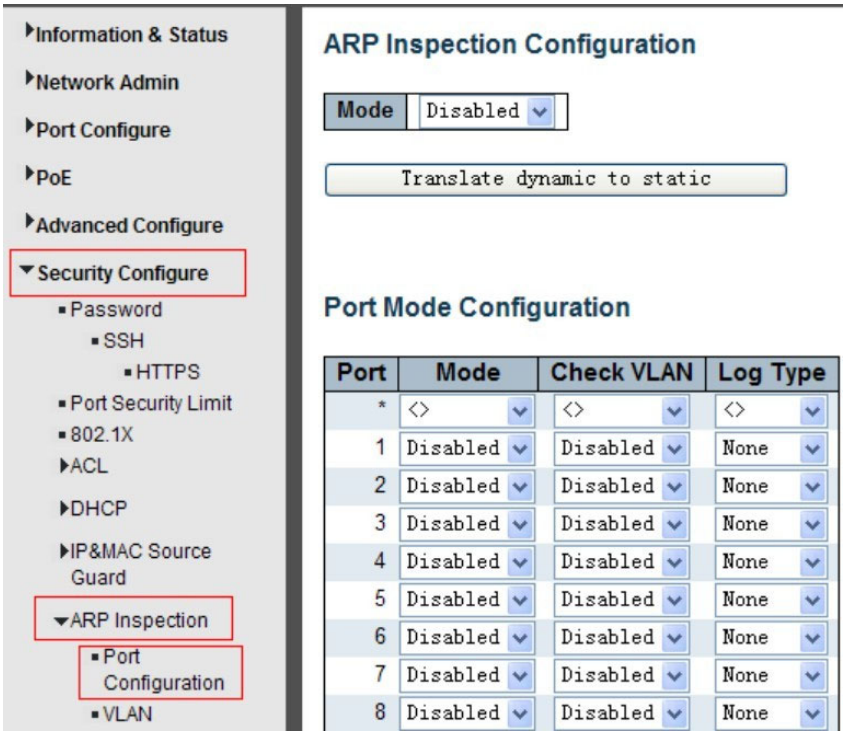

Рисунок 54 — Параметры ARP Inspection на портах

Объекты конфигурации и их описание приведены в таблице 45.

Таблица 45

Параметр	Описание
Global Mode	Включение/выключение глобальной проверки ARP через выпадающее меню
Port Mode	Включение/выключение проверки ARP на основе портов через выпадающее меню
Check VLAN	Чтобы проверить конфигурацию VLAN, необходимо включить параметр «Check VLAN». По умолчанию этот параметр отключен. Когда «Check VLAN» отключен, тип журнала для ARP Inspection будет определяться настройкой порта. Когда «Check VLAN» включен, тип журнала для ARP Inspection будет определяться настройкой VLAN. Значение «Check VLAN» журнала проверки ARP будет зависеть от настройки VLAN. Возможны следующие настройки «Check VLAN»: – Enabled — включить проверку работы VLAN; – Disabled — отключить проверку работы VLAN
Log Type	Только Global Mode и Port Mode на данном порту включены, а параметр «Check VLAN» отключен, тогда тип журнала для ARP Inspection будет определяться настройкой порта. Доступны четыре типа журнала: – None: не вести журнал; – Deny: регистрировать отклонённые записи; – Permit: регистрировать разрешённые записи; – ALL: регистрировать все записи

Для сохранения настроек необходимо нажать кнопку Save.

7.6.2 Конфигурация по VLAN

Окно настройки ARP Inspection по VLAN отображается при открытии раздела «Security Configure > ARP Inspection > VLAN Configuration» (рисунок 55).

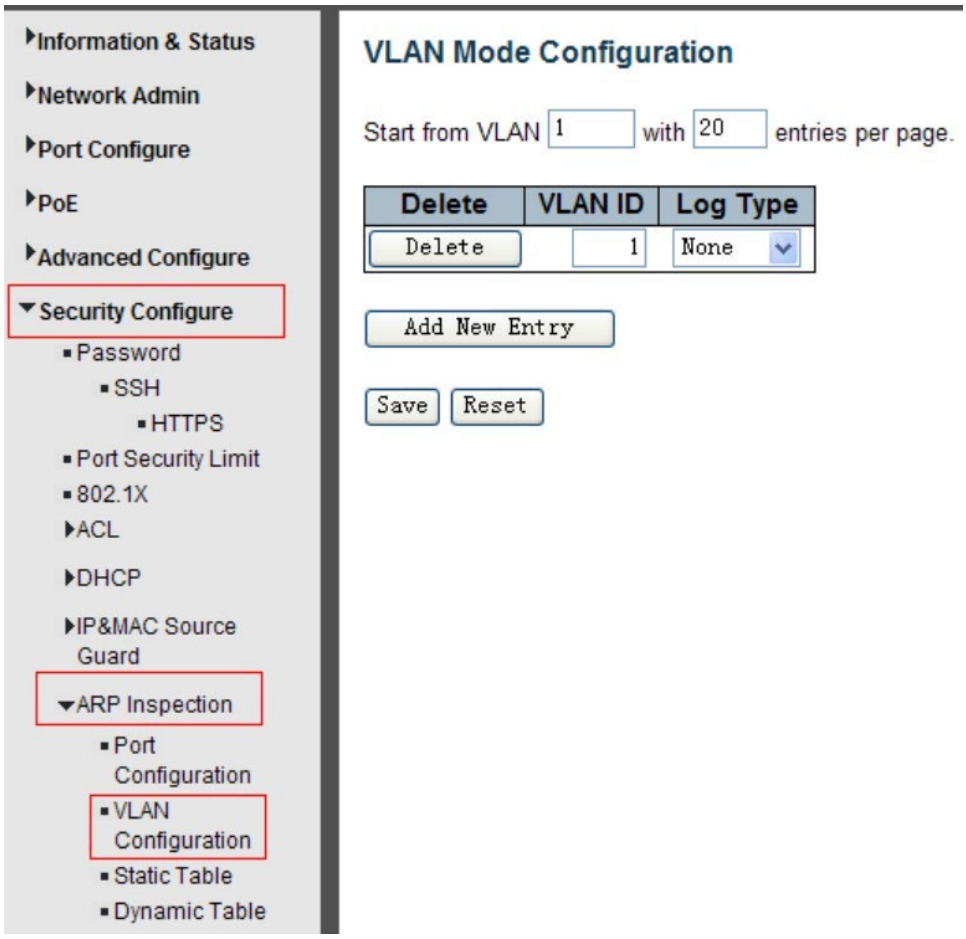

Рисунок 55 — Настройка ARP Inspection по VLAN

Объекты конфигурации и их описание приведены в таблице 46.

Таблица 46

Параметр	Описание
VLAN ID	Идентификатор VLAN
Log Type	Включение/выключение ARP Inspection на уровне порта через выпадающее меню. Необходимо указать, для каких VLAN будет включена ARP Inspection. Сначала нужно включить параметр порта на странице настройки Port mode. ARP Inspection будет активна на порту, только когда на нем включены и Global Mode, и Port Mode. Затем на странице настройки VLAN mode можно указать, для каких VLAN будет выполняться проверка. Для каждого VLAN также можно настроить тип журнала. Возможные типы: – None: ничего не записывать; – Deny: записывать отклонённые записи; – Permit: записывать разрешённые записи; – ALL: записывать все записи

Для сохранения настроек необходимо нажать кнопку Save.

7.6.3 Статическая таблица ARP Inspection

Статическая таблица ARP Inspection отображается при открытии раздела «Security Configure > ARP Inspection > Static Table» (рисунок 56).

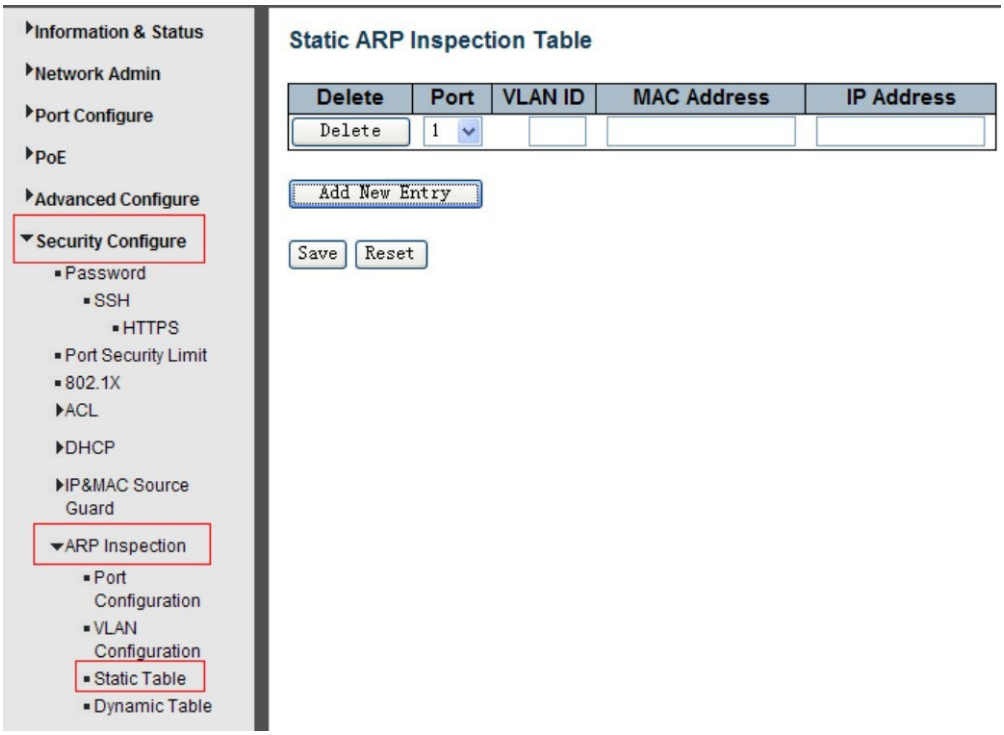

Рисунок 56 — Статическая таблица ARP Inspection

Объекты конфигурации и их описание приведены в таблице 47.

Таблица 47

Параметр	Описание
Port	Через выпадающее меню выбирается, какой порт следует зафиксировать
VLAN	Вводится идентификатор VLAN, который должен быть зафиксирован
IP Address	Вводится IP-адрес, который должен быть зафиксирован
MAC Address	Вводится MAC-адрес, который должен быть зафиксирован

Для сохранения настроек необходимо нажать кнопку Save.

7.7 Настройка ACL

ACL — это аббревиатура от Access Control List («список контроля доступа»). Это таблица записей ACE (Access Control Entries), содержащая элементы контроля доступа, которые указывают, каким отдельным пользователям или группам разрешён или запрещён доступ к определённым объектам трафика, например, к процессу или программе. Каждый доступный объект трафика содержит идентификатор своей ACL. Привилегии определяют, есть ли у конкретного объекта трафика права доступа.

Реализация ACL может быть довольно сложной, например, когда записи ACE имеют приоритет в различных ситуациях. В сетевых технологиях ACL означает список сервисных портов или сетевых служб, доступных на хосте или сервере, вместе со списком хостов или

серверов, которым разрешено или запрещено использовать эти службы. ACL обычно можно настраивать для управления входящим трафиком, и в этом смысле они похожи на межсетевые экраны.

7.7.1 Параметры ACL на портах

Статическая таблица ARP Inspection отображается при открытии раздела «Security Configure > ACL > Ports» (рисунок 57)..

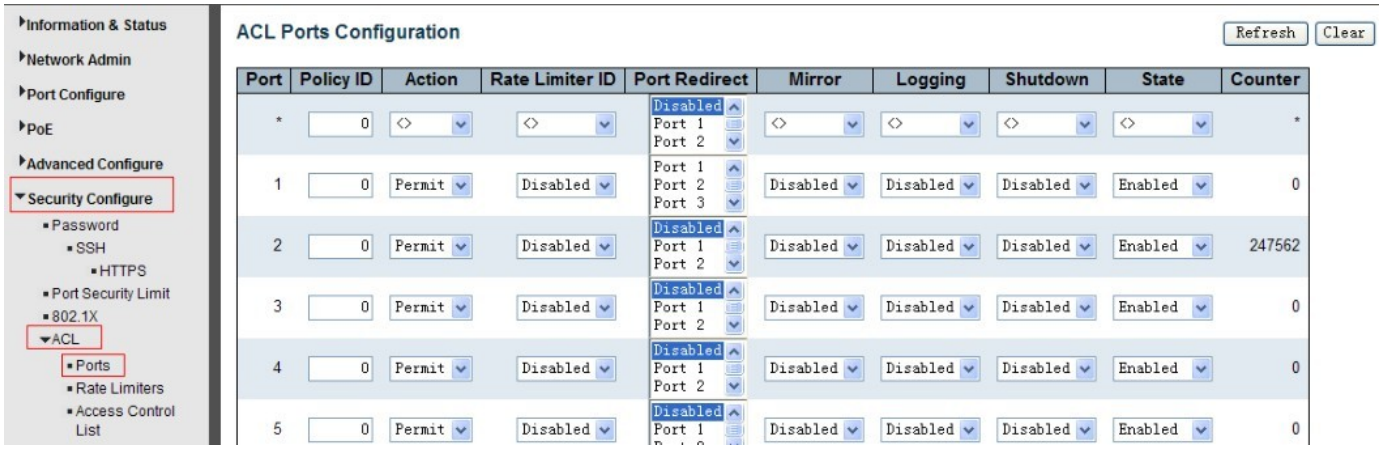

Рисунок 57 — ACL на портах

Объекты конфигурации и их описание приведены в таблице 48.

Таблица 48

Параметр	Описание
Action	Доступны 2 варианта: Permit (этот конкретный порт разрешает прохождение данных) и Deny (этот конкретный порт запрещает прохождение данных)
Rate Limiter ID	Фиксированный идентификатор Rate Limiter для порта (подробности — в 7.7.2)
Port Redirect	Выбирается порт, на который будут перенаправляться кадры. Допустимые значения: Disabled или номер конкретного порта. Этот параметр нельзя задать, если действие разрешено (Permit). Значение по умолчанию — Disabled
Mirror	Указывается режим зеркалирования для этого порта. Допустимые значения: Enabled (кадры, полученные на порту, зеркалируются) и Disabled (кадры, полученные на порту, не зеркалируются). Значение по умолчанию — Disabled
Logging	Включение/отключение логирования
Shut Down	Указывается режим отключения порта для этого порта. Допустимые значения: Enabled (если на порт поступает кадр, порт будет отключён) и Disabled (отключение порта не выполняется). Значение по умолчанию — Disabled*
State	Указывается состояние этого порта. Допустимые значения: Enabled (повторно открыть порты, изменив временную конфигурацию порта в модуле ACL пользователя) и Disabled (закрыть порты, изменив временную конфигурацию порта в модуле ACL пользователя). Значение по умолчанию — Enabled
Counter	Счетчик кадров, попавших под правило
*Функция отключения работает только тогда, когда длина пакета меньше 1518 байт (без VLAN-тегов)	

Для сохранения настроек необходимо нажать кнопку Save.

7.7.2 Настройка Rate Limiter

Пользователь может создать профили ограничения скорости для дальнейшей привязки к правилам ACL. Соответствующее окно настройки отображается при открытии раздела «Security Configure > ACL > Rate Limiters» (рисунок 58).

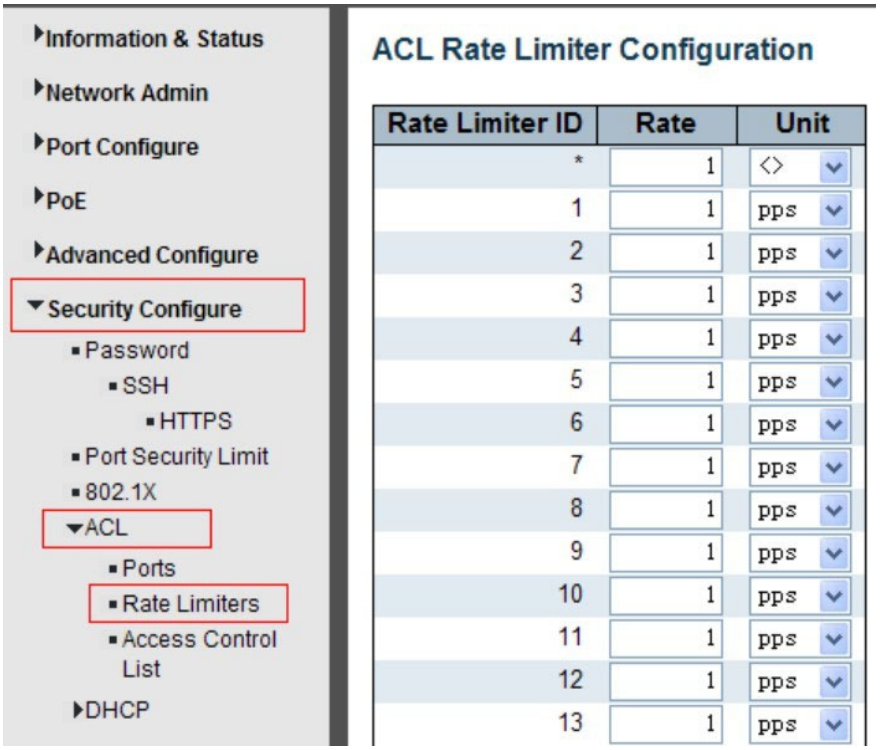

Рисунок 58 — Конфигурация Rate Limiter

7.7.3 Список правил ACL

В разделе Access Control List создаются и редактируются сами правила доступа. Список правил отображается при открытии раздела «Security Configure > ACL > Access Control List» (рисунок 59).

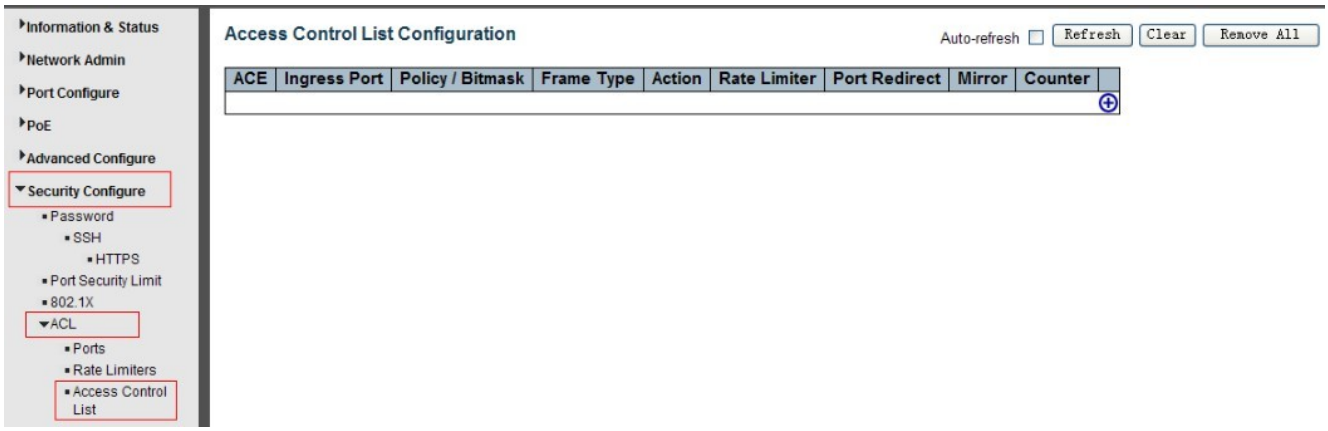

Рисунок 59 — Экран списка правил ACL

Для перехода к списку контроля доступа и для его редактирования необходимо нажать кнопку ⊕.

8 Диагностика

8.1 Тест Ping

Ping — это программа, которая может отправлять пакеты ICMP Echo на указанный пользователем IP-адрес. Узел назначения отвечает на эти пакеты, отправленные со свитча. Тест Ping используется для диагностики проблем с IP-соединением. Соответствующее окно отображается при открытии раздела «Diagnostics > Ping» (рисунок 60).

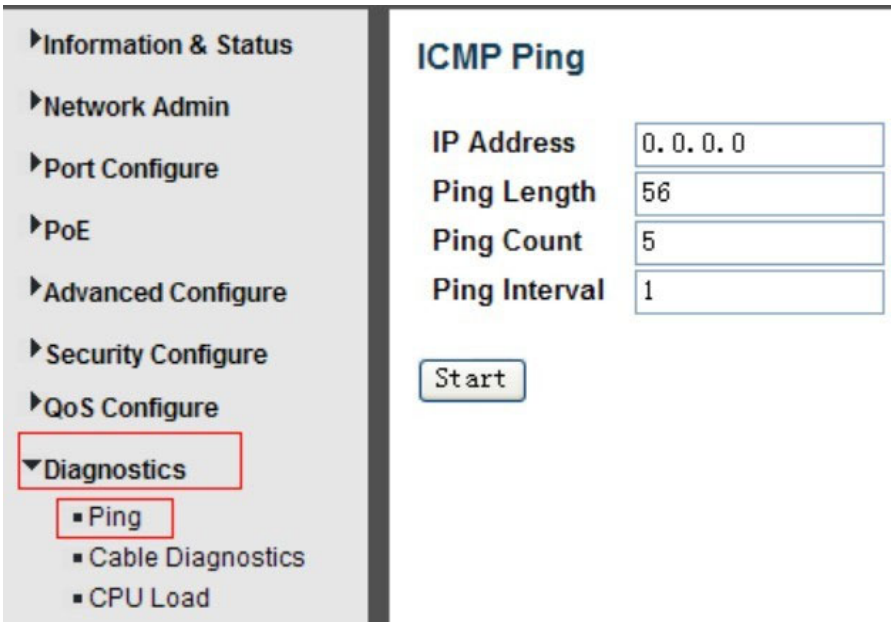

Рисунок 60 — Ping Test

Объекты конфигурации и их описание приведены в таблице 49.

Таблица 49

Параметр	Описание
IP Address	IP-адрес назначения, необходимый для проверки связи
Ping Length	Размер пакета от 1 до 1452 байт; по умолчанию 56
Ping Count	Количество запросов: от 1 до 60
Ping Interval	Интервал между отправкой ICMP-пакетов

Для запуска теста необходимо нажать кнопку Start.

8.2 Диагностика кабеля (Cable Diagnostics)

Cable Diagnostics выполняет тестирование медных кабелей 10/100/1000BASE-T. Эти функции позволяют определить длину кабеля и условия его работы, а также выявить и локализовать различные распространённые неисправности, которые могут возникать в кабельной линии Cat5 на витой паре. Соответствующее окно отображается при открытии раздела «Diagnostics > Cable Diagnostics» (рисунок 61).

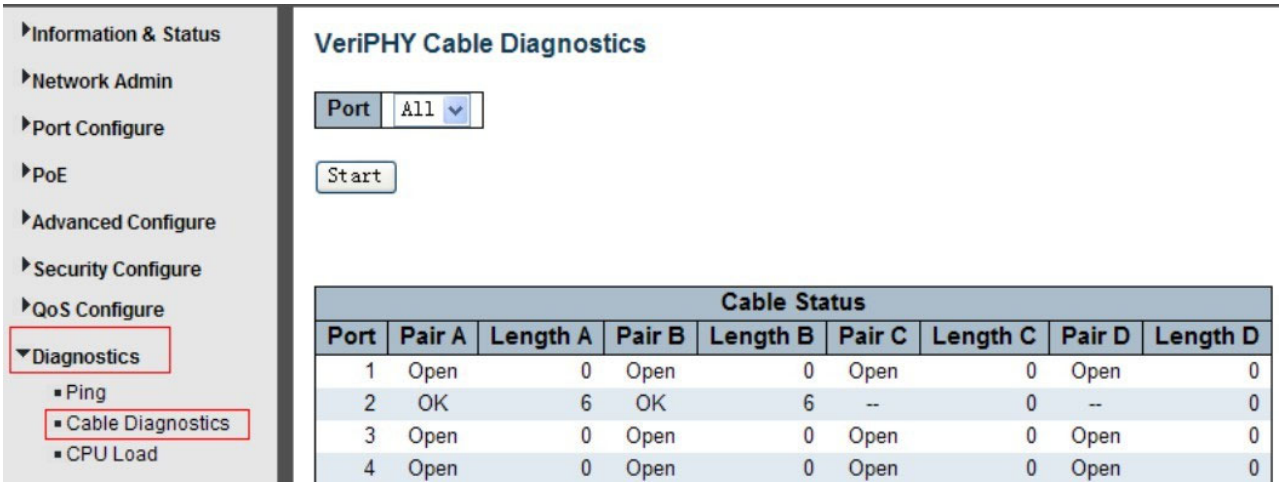

Рисунок 61 — Cable Diagnostics

Чтобы начать тестирование Cable Diagnostics, необходимо нажать кнопку Start.

8.1 Загрузка CPU (CPU Load)

Раздел «Diagnostics > CPU Load» показывает загрузку процессора в процентах (рисунок 62).

Рисунок 62 — Загрузка процессора

9 Техническое обслуживание

9.1 Перезапуск устройства (Restart Device)

В разделе «Maintenance > Restart Device» пользователь может перезагрузить коммутатор (рисунок 63). Для подтверждения необходимо нажать кнопку Yes.

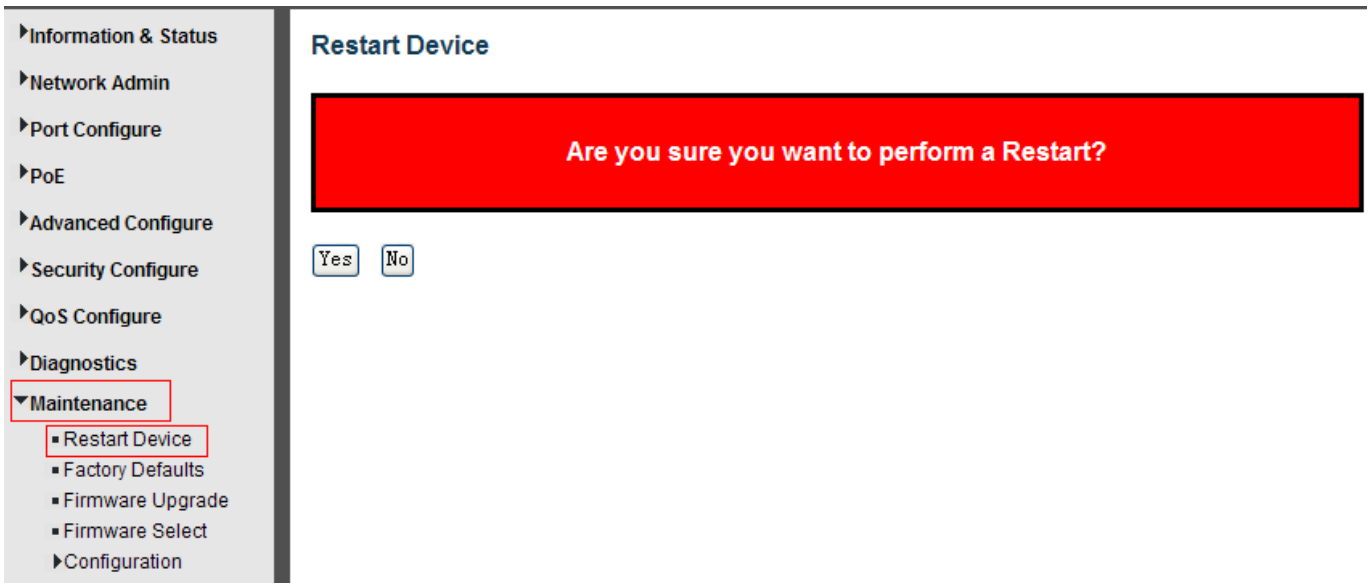

Рисунок 63 — Перезапуск устройства

9.2 Сброс к заводским настройкам (Factory Defaults)

В разделе «Maintenance > Factory Defaults» пользователь может сбросить конфигурацию к заводскому состоянию и восстановить настройки конфигурации по умолчанию (рисунок 64). Для подтверждения необходимо нажать кнопку Yes.

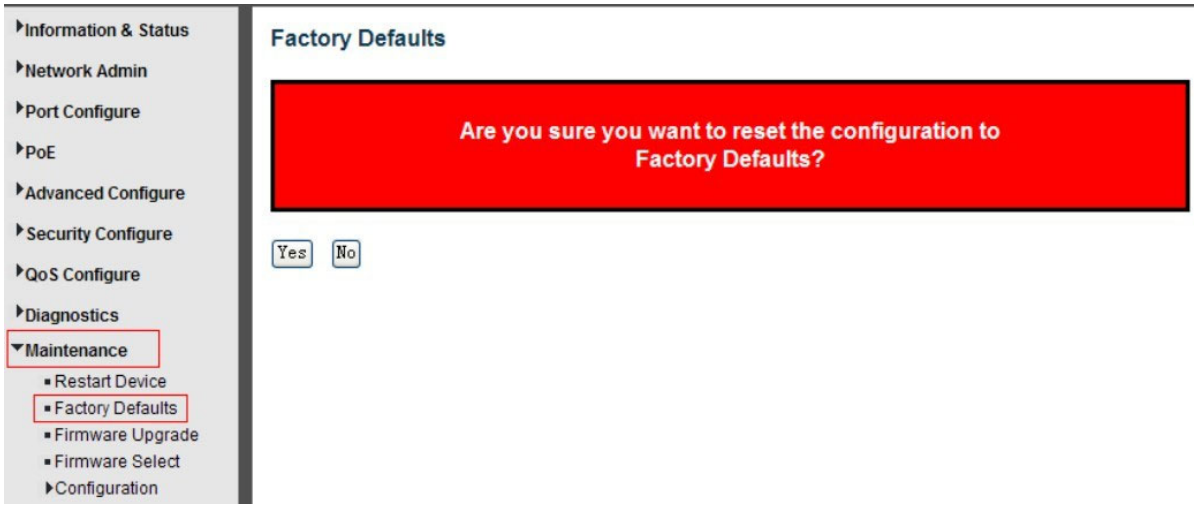

Рисунок 64 — Сброс к заводским настройкам

9.3 Обновление прошивки (Firmware Upgrade)

В разделе «Maintenance > Firmware Upgrade» пользователь может обновить прошивку (рисунок 65). Для этого необходимо нажать кнопку Browse, выбрать файл прошивки и нажать кнопку Upload.

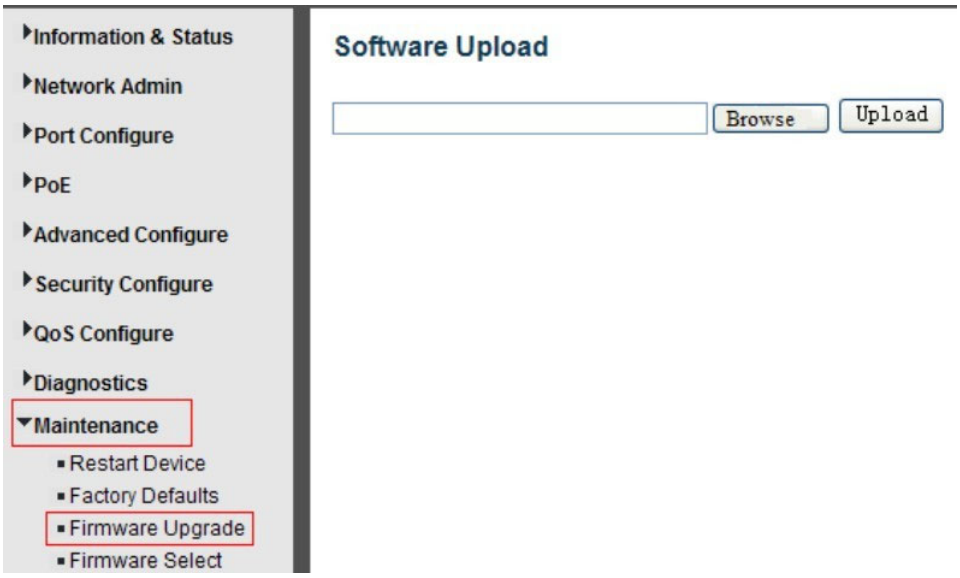

Рисунок 65 — Обновление прошивки

9.4 Выбор прошивки (Firmware Select)

В разделе «Maintenance > Firmware Select» пользователь может активировать альтернативный образ прошивки (рисунок 66). Чтобы выбрать встроенное программное обеспечение, необходимо нажать кнопку Activate Alternate Image.

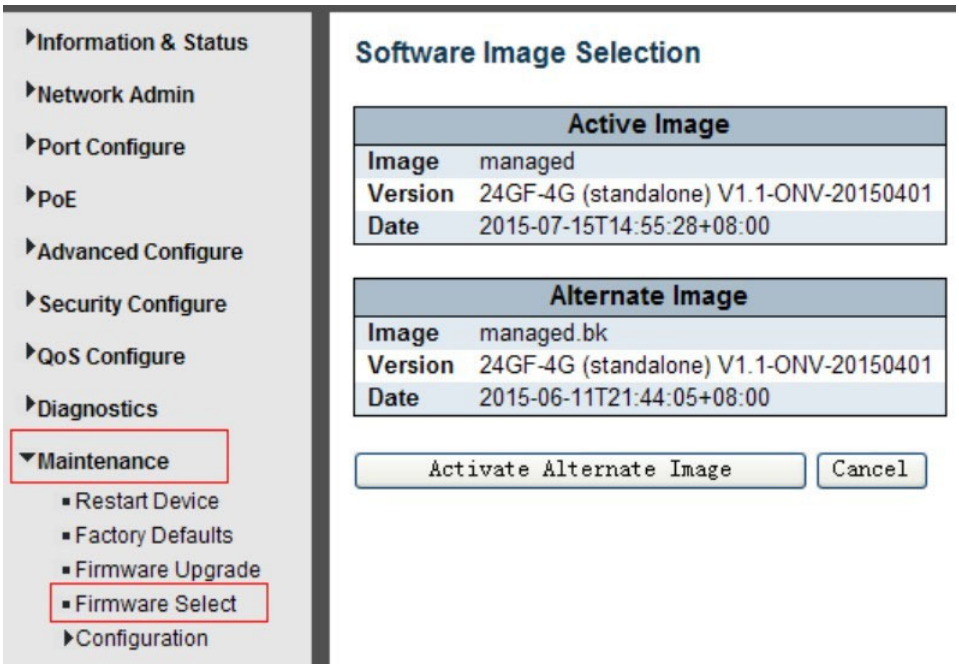

Рисунок 66 — Выбор образа прошивки

9.5 Выбор файлов конфигурации

В разделе «Maintenance > Configuration» пользователь может скачивать, выгружать, активировать или удалять файлы конфигурации.

9.5.1 Загрузка конфигурационного файла

Для загрузки файла конфигурации необходимо открыть раздел «Maintenance > Configuration > Download» и нажать кнопку Download Configuration (рисунок 67).

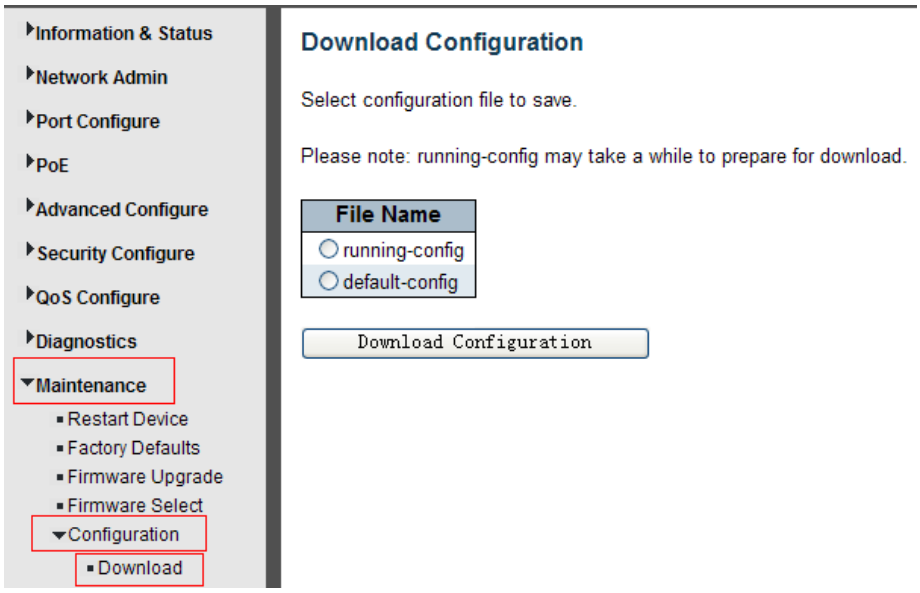

Рисунок 67 — Загрузка конфигурации

9.5.2 Выгрузка конфигурационного файла

Для выгрузки файла конфигурации необходимо открыть раздел «Maintenance > Configuration > Upload», нажать кнопку Browse, выбрать файл конфигурации и нажать кнопку Upload Configuration (рисунок 68).

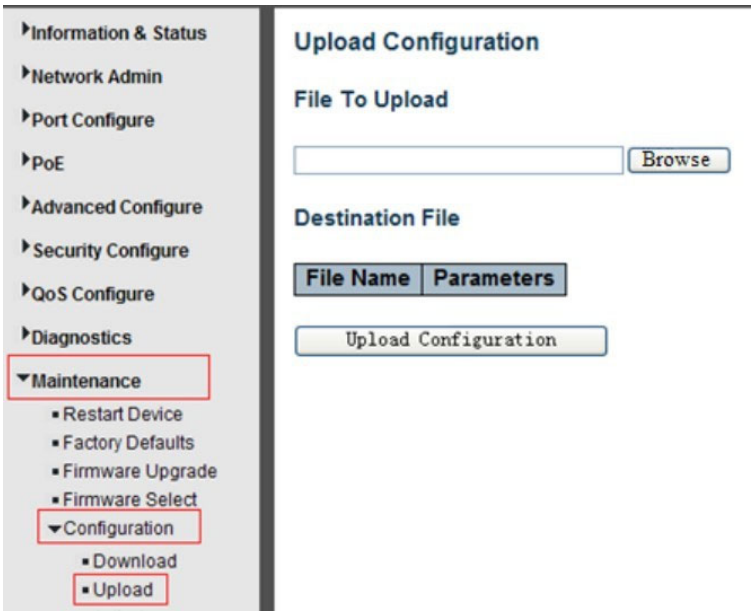

Рисунок 68 — Выгрузка конфигурации

9.5.3 Активация конфигурации

Пользователь может активировать конфигурацию в разделе «Maintenance > Configuration > Activate» (рисунок 69). Для этого необходимо выбрать файл и нажать кнопку Activate Configuration.

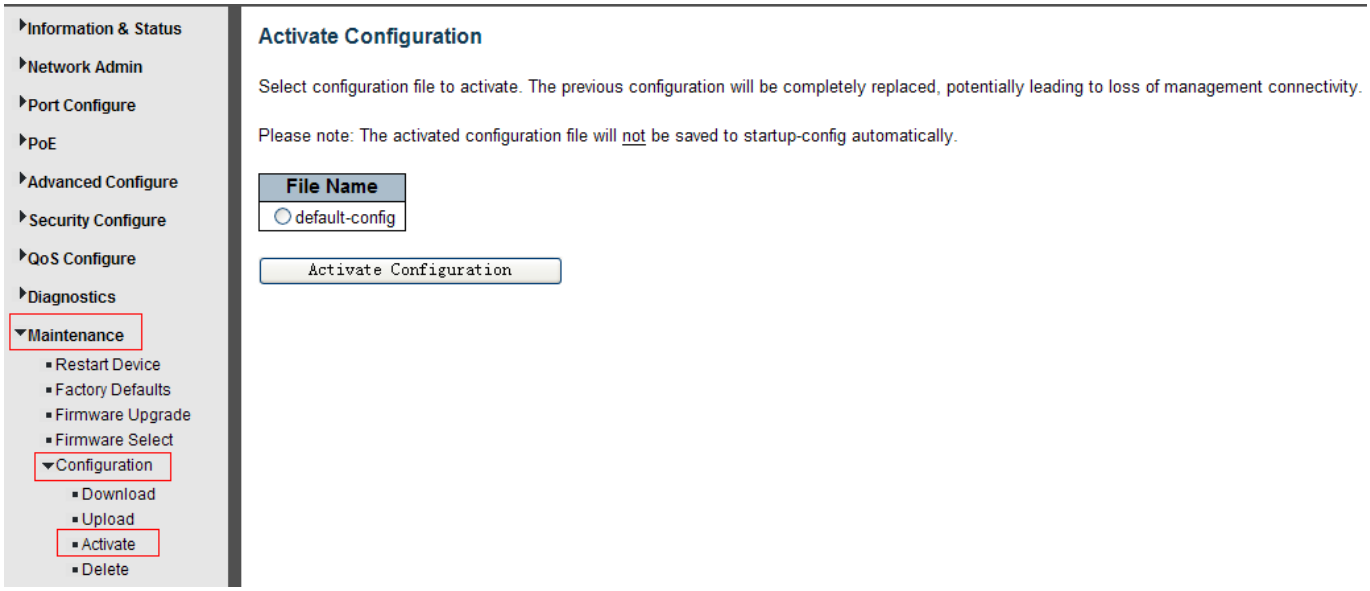

Рисунок 69 — Активация конфигурации

9.5.4 Удаление конфигурационного файла

Пользователь может удалить конфигурационный файл в разделе «Maintenance > Configuration > Delete» (рисунок 70). Для этого необходимо выбрать файл и нажать кнопку Delete Configuration File.

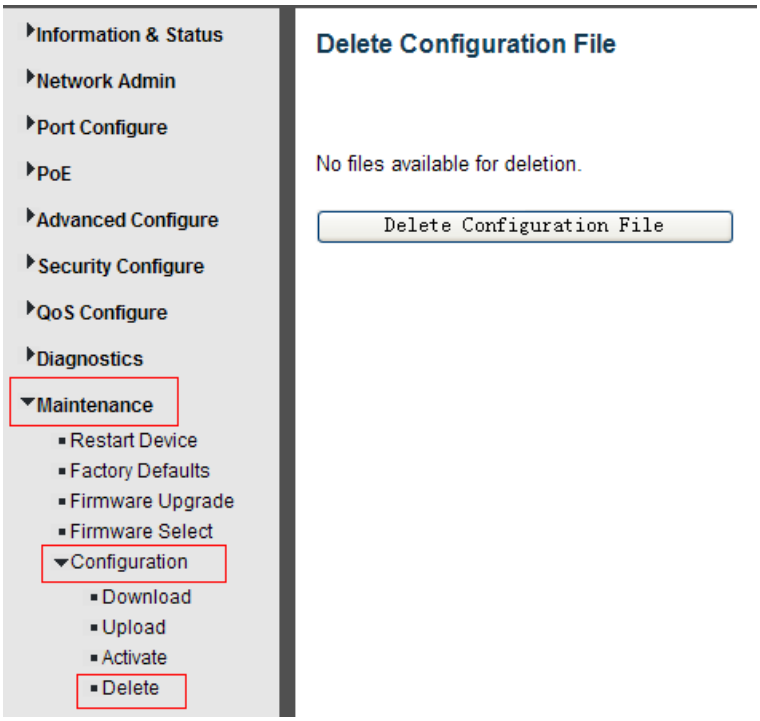

Рисунок 70 — Удаление конфигурации

Приложение А

Часто задаваемые вопросы

1. Почему web-страница управления отображается некорректно?

Ответ: Перед доступом к WEB-интерфейсу очистите кэш и cookies браузера Internet Explorer/браузера. Иначе возможно некорректное отображение.

2. Что делать, если забыт пароль?

Ответ: Сбросьте пароль возвратом к заводским настройкам. Удерживайте кнопку около 10 секунд. После сброса используйте имя пользователя admin и пароль system

3. Можно ли настраивать устройство и через web, и через CLI?

Ответ: Да. Оба способа управления поддерживаются.

4. Почему после настройки trunking пропускная способность не увеличилась?

Ответ: Проверьте, совпадают ли параметры портов trunk: скорость, режим дуплекса, VLAN и другие связанные настройки.

5. Что делать, если часть портов работает некорректно?

Ответ: Проверьте по шагам: 1) не меняя порт, замените сетевой кабель; 2) не меняя кабель и порт, замените компьютер/сетевую карту; 3) не меняя кабель и компьютер, переключитесь на другой порт коммутатора; 4) если проблема подтверждается именно на порту коммутатора, обратитесь к поставщику для ремонта.

6. В каком порядке порт выполняет автоопределение скорости и дуплекса?

Ответ: Проверка выполняется в следующем порядке: 1000 Мбит/с full-duplex, 100 Мбит/с full-duplex, 100 Мбит/с half-duplex, 10 Мбит/с full-duplex, 10 Мбит/с half-duplex. Затем выбирается максимальная доступная скорость.