Инструкция по настройке через web-интерфейс

промышленных коммутаторов серии ZIRCON3XXXHP

ИЗДАТЕЛЬ:
ООО «ДИДЖИКОМ»

Адрес: Россия, 117535, г. Москва, Варшавское шоссе, дом 133, строение 2

Тел: +7 (499) 969-81-21
Эл. почта: sales@dgsys.ru
Сайт: www.dgsys.ru

Версия: 1.0 2026 г.

Содержание

1 Введение в продукт

1.1 Общие сведения

Коммутаторы серии **ZIRCON3XXXHP** включают в себя разнообразные типы интерфейсов, а также различное количество интерфейсов. Мощные функции делают сеть более гибкой, безопасной, надёжной, а встроенный веб-сервер управления упрощает управление сетью.

Аппаратные функции:

- Сетевое управление: веб-интерфейс, Telnet, консоль
- Коммутационные атрибуты: VLAN, QoS
- Протоколы резервирования: ERPS, MSTP/RSTP/STP, кольцо
- Мультивещание: IGMP Snooping, статическое мультивещание, MLD Snooping
- Сетевая безопасность: ACL
- Сетевой мониторинг: SNMP v1/v2/v3, RMON
- Управление пропускной способностью: агрегация каналов, ограничение скорости порта
- Диагностика: зеркалирование, LLDP
- Протокол синхронизации: NTP
- Сигнализация: сигнализация порта/питания
- Синхронизация часов: синхронизация часов PTP

Технические стандарты:

- IEEE 802.3u 100Base-TX, 100Base-FX, Fast Ethernet
- IEEE 802.3ab 1000Base-T Gigabit Ethernet по витой паре
- IEEE 802.3z 1000Base-X Gigabit Ethernet по оптоволокну
- IEEE 802.1d STP (Spanning Tree Protocol)
- IEEE 802.1w RSTP (Rapid Spanning Tree Protocol)
- IEEE 802.1s MSTP (Multiple Spanning Tree Protocol)
- ITU-T G.8032/Y.1344 ERPS (Ethernet Ring Protection Switching)
- IEEE 802.1Q Virtual LANs (VLAN)
- IEEE 802.1X Аутентификация и контроль доступа к сети на основе порта и MAC-адреса
- IEEE 802.3ad Агрегация каналов для параллельных линий с использованием LACP (Link Aggregation Control Protocol)
- IEEE 802.3x Управление потоком для полного дуплекса
- IEEE 802.1ad Stacked VLANs, Q-in-Q
- IEEE 802.1p Протокол приоритизации трафика уровня 2 LAN QoS/CoS
- IEEE 802.1ab Протокол обнаружения на канальном уровне (LLDP)
- IEEE 802.3az EEE (Energy Efficient Ethernet)

2 Доступ к коммутатору

- Веб-интерфейс
- Порт консоли
- Telnet

Если IP-адрес управляющей VLAN устройства неизвестен

2.1 Веб-доступ

Введите IP-адрес в адресную строку браузера, отобразится экран входа, затем введите имя пользователя «admin», пароль по умолчанию — 123, как показано на Рисунке 2-1:

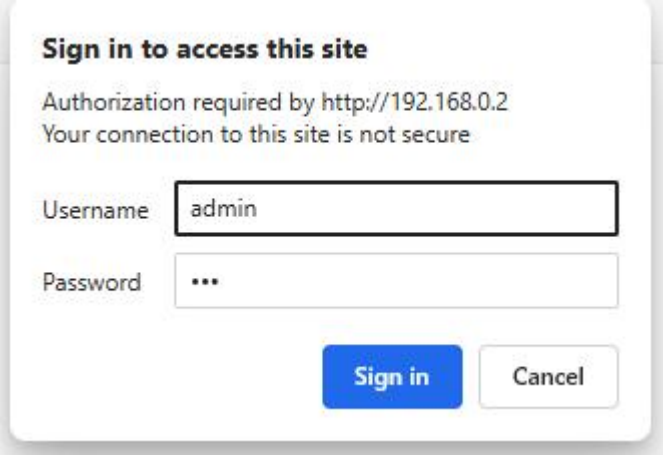


Рисунок 2-1: Интерфейс входа

После входа в веб-интерфейс, как показано на Рисунке 2-2, слева расположено навигационное меню, а справа — подробная информация.

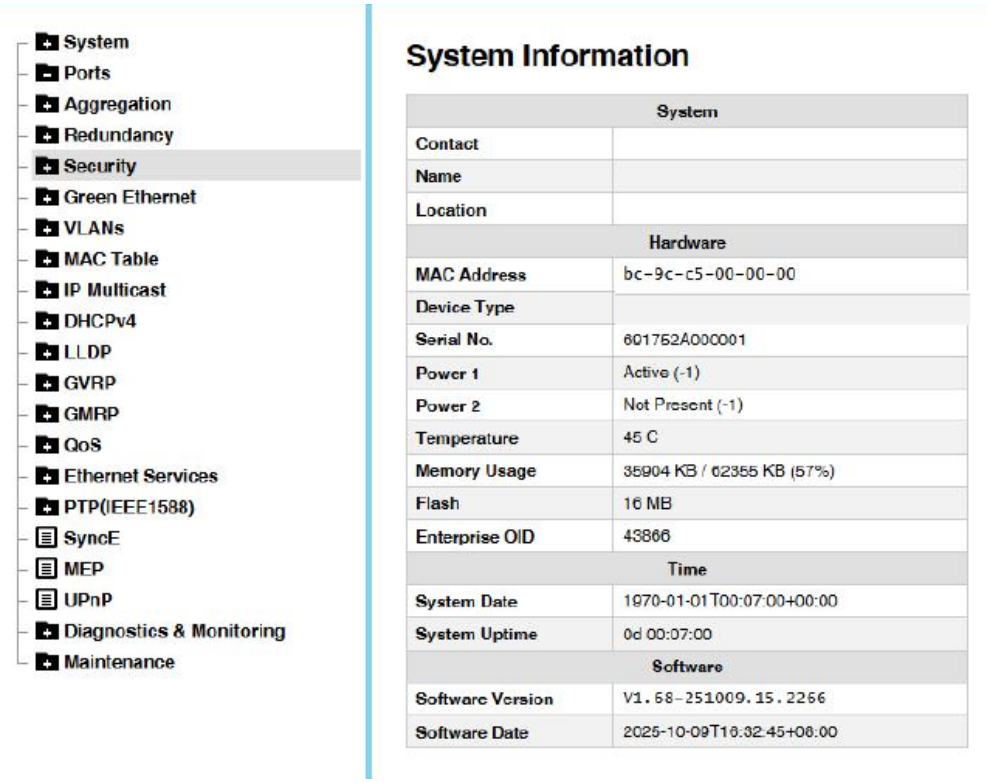


Рисунок 2-2: Веб-интерфейс

2.2 Доступ через порт консоли

Пользователи могут получить доступ к коммутатору через порт консоли с использованием программы «Гипертерминал» Windows или другого программного обеспечения для последовательного подключения, такого как xshell. В следующем примере показано, как получить доступ к коммутатору с помощью «Гипертерминала» через порт консоли:

(1) Подключите последовательный порт ПК к порту консоли с помощью предоставленного кабеля DB9.

(2) Запустите гипертерминал из Windows: Пуск → Все программы → Стандартные → Связь → Гипертерминал.

(3) Создайте новое подключение «Коммутатор», как показано на Рисунке 2-3.

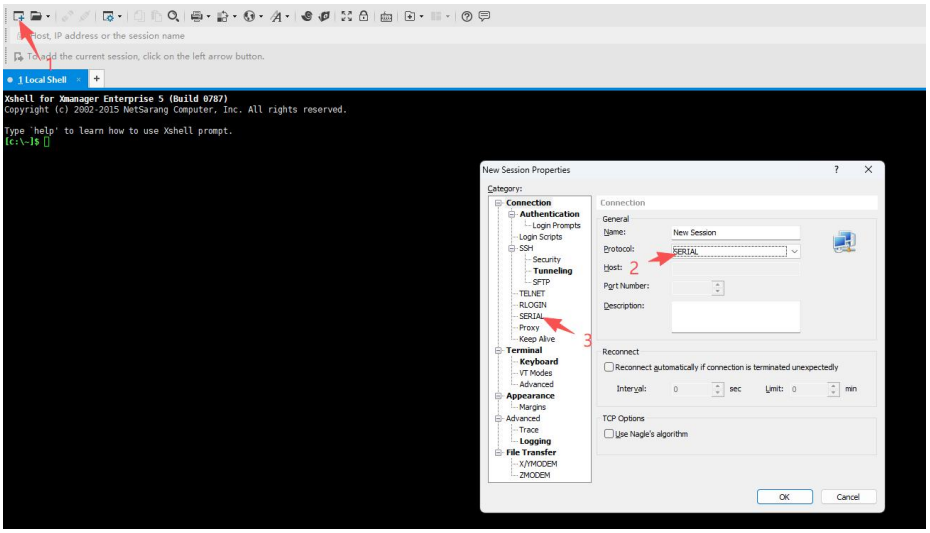


Рисунок 2-3: Новые подключения

(4) Выберите COM1, как показано на Рисунке 2-4.

Примечание: Проверьте диспетчер устройств, чтобы подтвердить соответствующий порт COM.

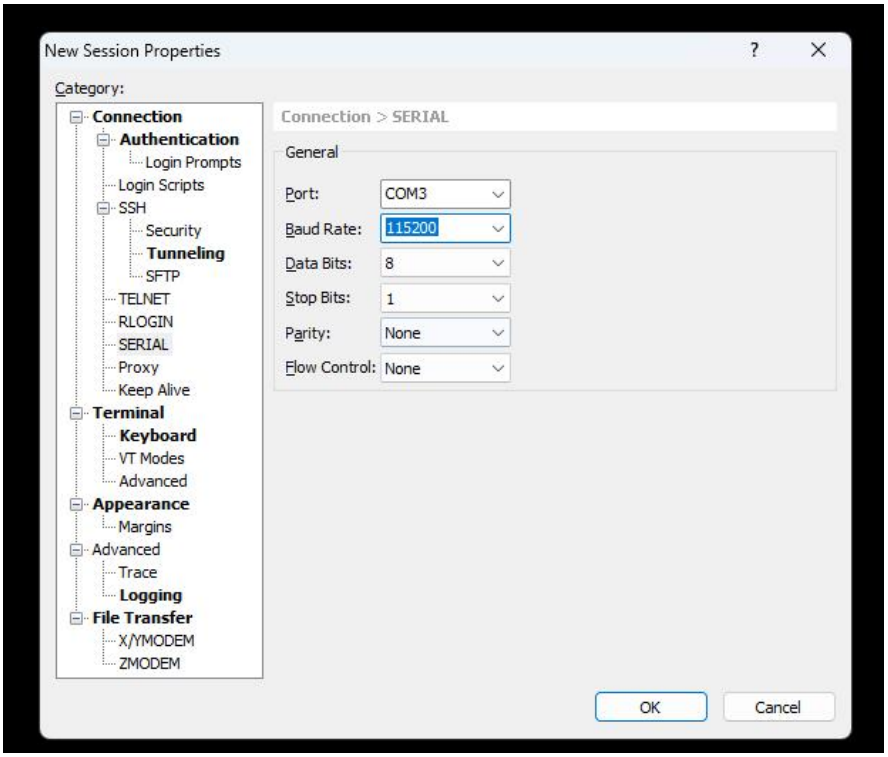


Рисунок 2-4: Выбор порта COM

(5) Настройки COM1 показаны на Рисунке 2-5: скорость передачи (бит/с): 115200; количество бит данных: 8; чётность: отсутствует; стоповые биты: 1; управление потоком: отсутствует.

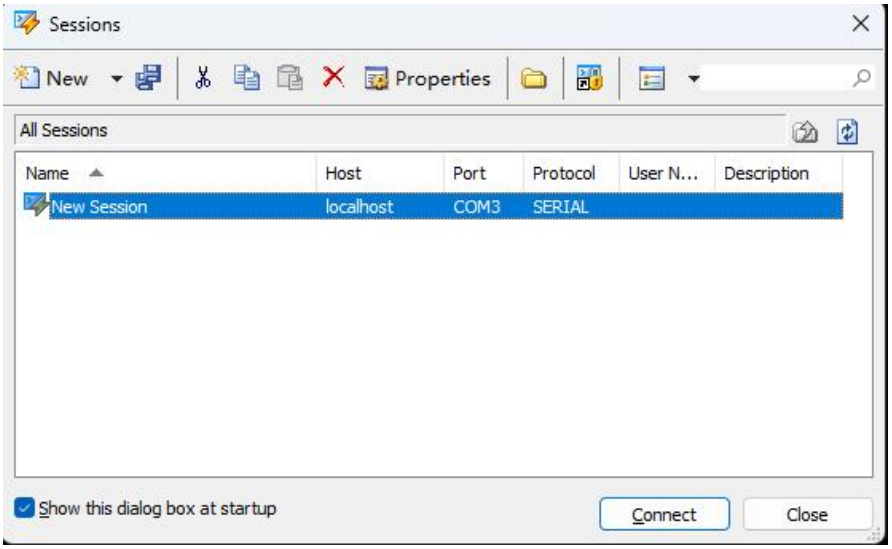


Рисунок 2-5: Настройки последовательного порта

(6) Нажмите «ОК», чтобы войти в CLI. Имя пользователя по умолчанию для управления последовательным портом устройства — «admin», пароль по умолчанию — 123. Как показано на Рисунке 2-6.

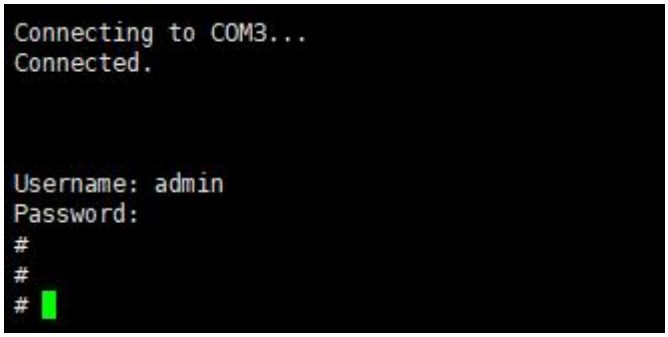


Рисунок 2-6: CLI

2.3 Доступ через Telnet

При использовании Telnet для доступа к устройству IP-адреса ПК и коммутатора должны находиться в одной сети. В диалоговом окне «Выполнить» введите «telnet IP-адрес», как показано на Рисунке 2-7.

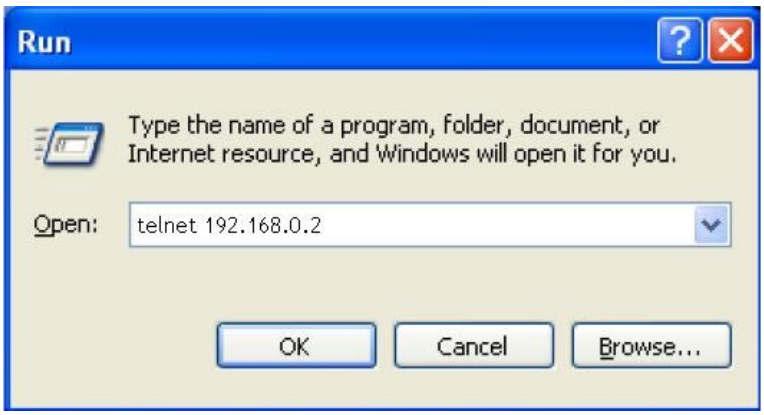


Рисунок 2-7: Доступ через Telnet

Введите имя пользователя «admin» и пароль 123 в интерфейсе Telnet и нажмите клавишу <Enter>, чтобы войти в CLI Telnet, как показано на Рисунке 2-8.

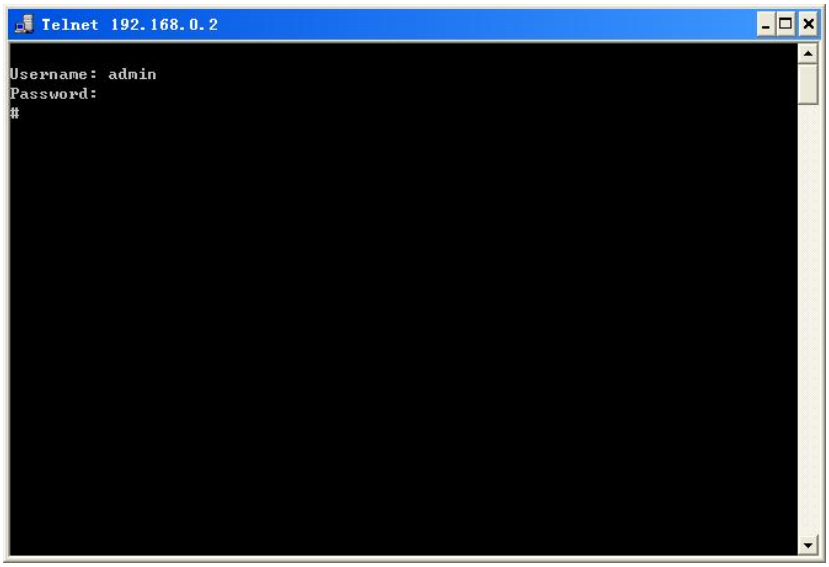


Рисунок 2-8: CLI Telnet

3 Доступ к коммутатору

3.1 Базовая информация

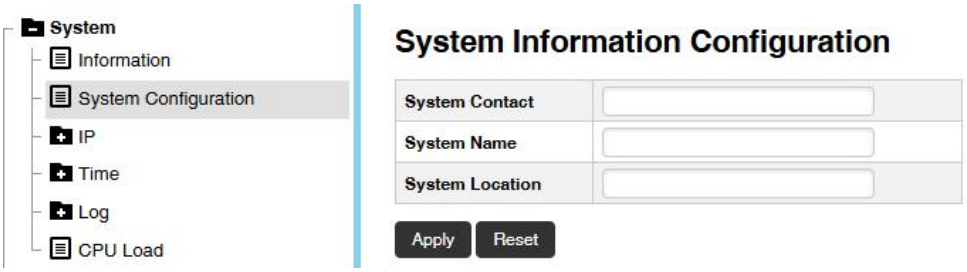


Рисунок 3-1: Базовая информация

Контактная информация системы

Допустимая длина строки — от 0 до 255, допустимое содержимое — символы ASCII от 32 до 126.

Системное имя

Допустимая длина строки — от 0 до 255.

Системный адрес

Допустимая длина строки — от 0 до 255, содержимое — символы ASCII от 32 до 126.

3.2 Изменение IP-адреса

Управляющий IP-адрес можно изменить, как показано на Рисунке 3-2.

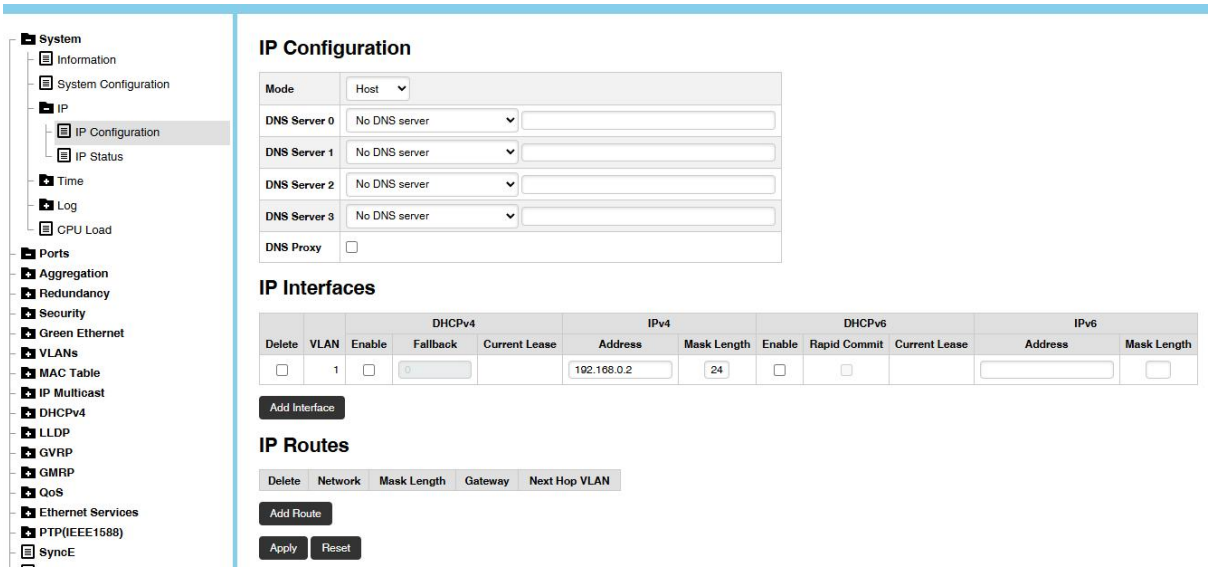


Рисунок 3-2: Изменение IP-адреса

3.3 Обновление прошивки

Обновление программного обеспечения, как показано ниже. Нажмите «Обзор», чтобы найти прошивку в формате '.dat'.

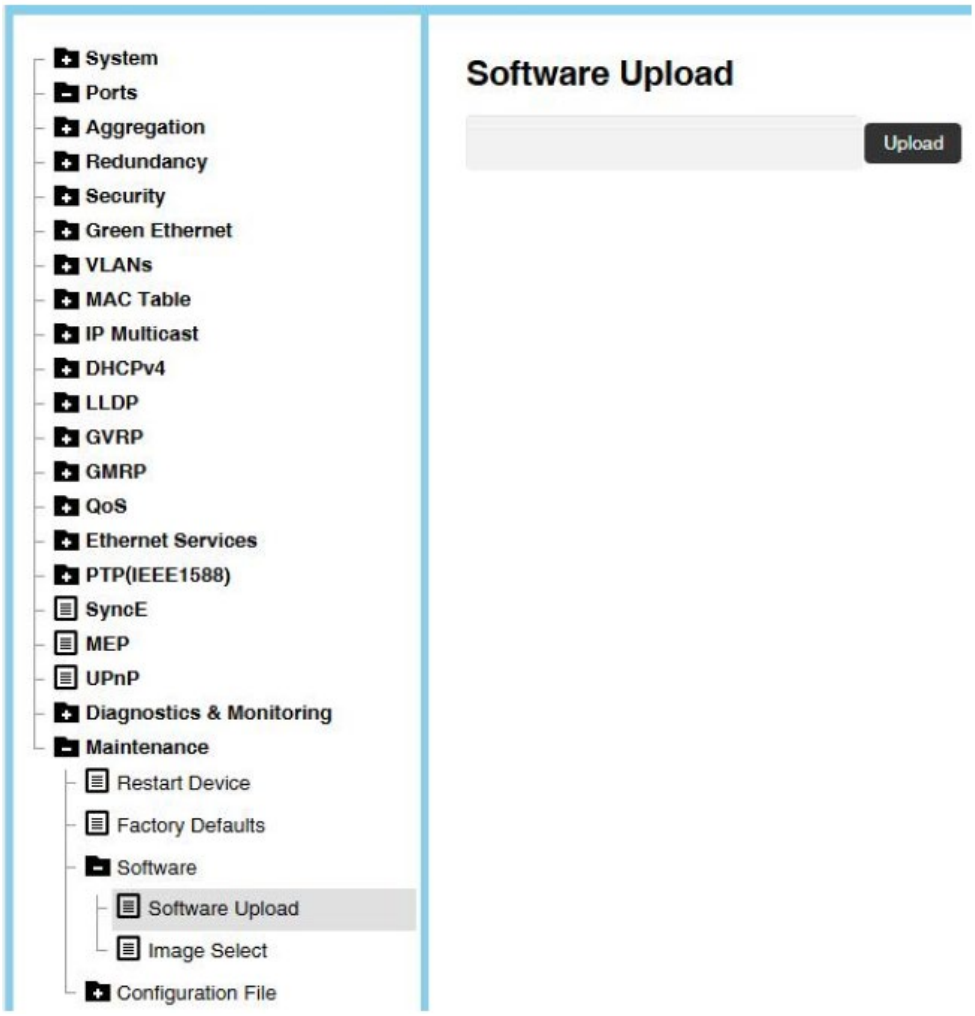


Рисунок 3-3: Обновление программного обеспечения

Выберите программное обеспечение для обновления с помощью кнопки «Обзор», нажмите «Загрузить», как показано на Рисунке 3-4 — выполняется обновление.

Рисунок 3-4: Выполнение обновления прошивки

4 Конфигурация порта

На этой странице можно настроить скорость, управление потоком, максимальный размер кадра и т.д., как показано на Рисунке 4-1:

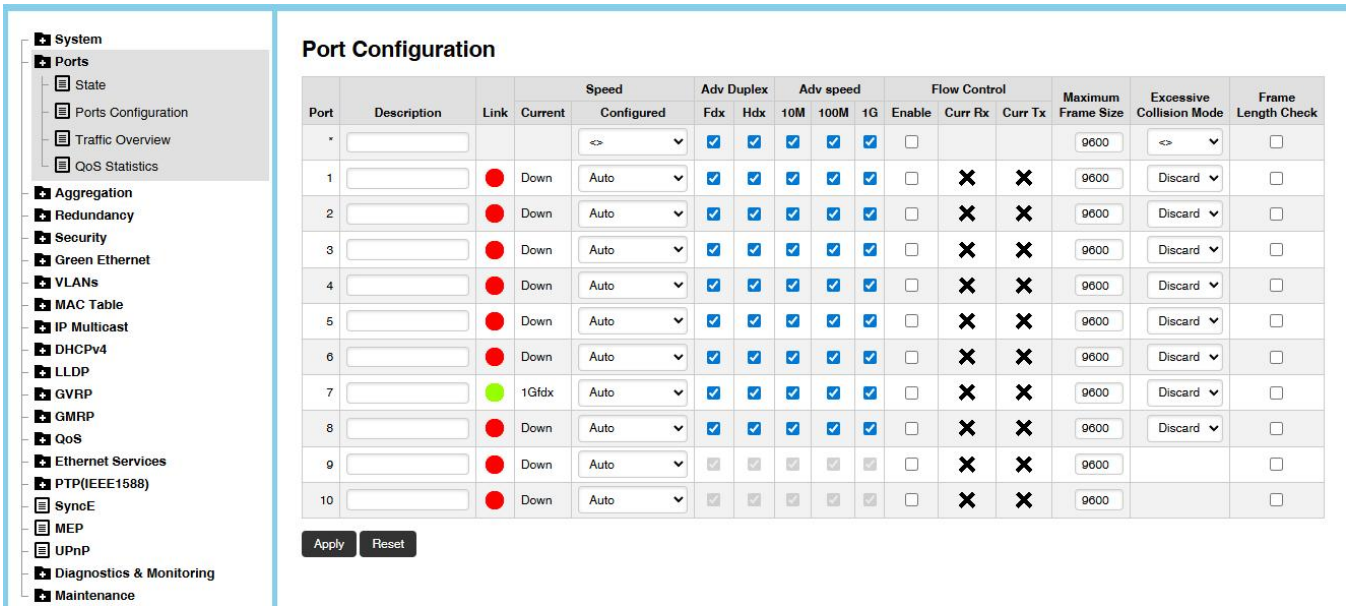


Рисунок 4-1: Конфигурация режима

Если у вас возникнут вопросы, нажмите кнопку справки. Например, справка доступна в правом верхнем углу страницы, как показано на Рисунке 4-2.

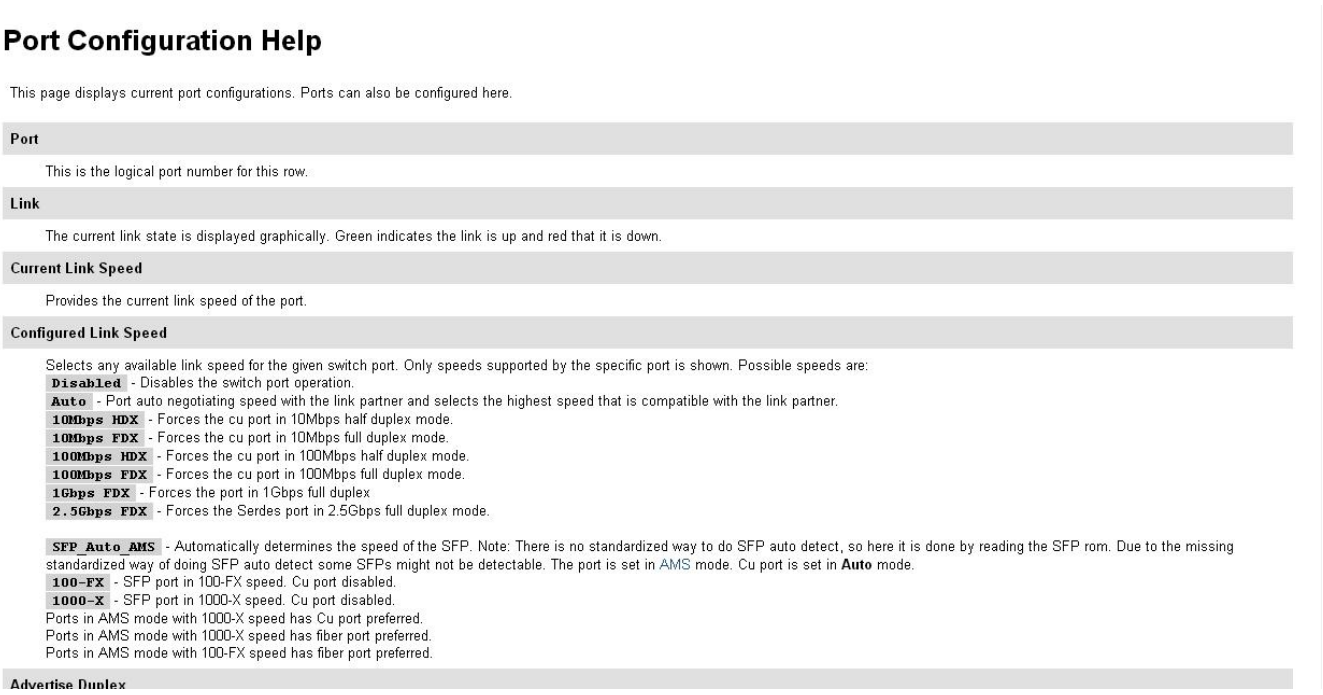


Рисунок 4-2: Справка

5 VLAN

5.1 Глобальная конфигурация VLAN

Добавление VLAN 2 и 3

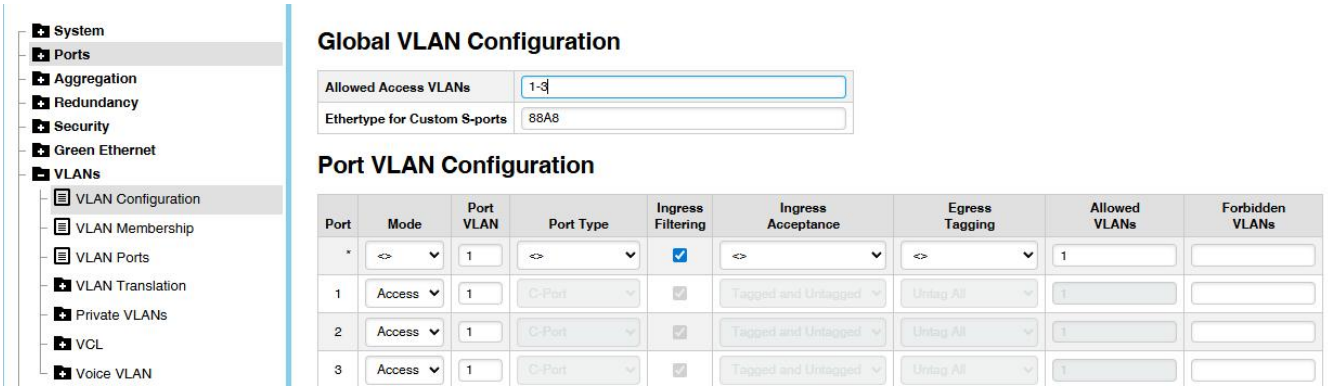


Рисунок 5-1: Добавление VLAN

Удаление VLAN 2

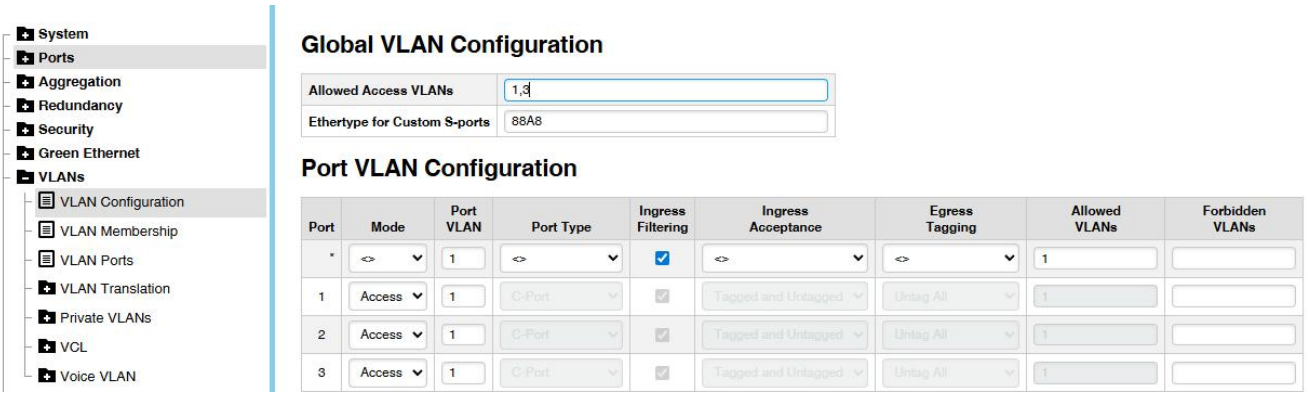


Рисунок 5-2: Удаление VLAN

Отображение существующих VLAN

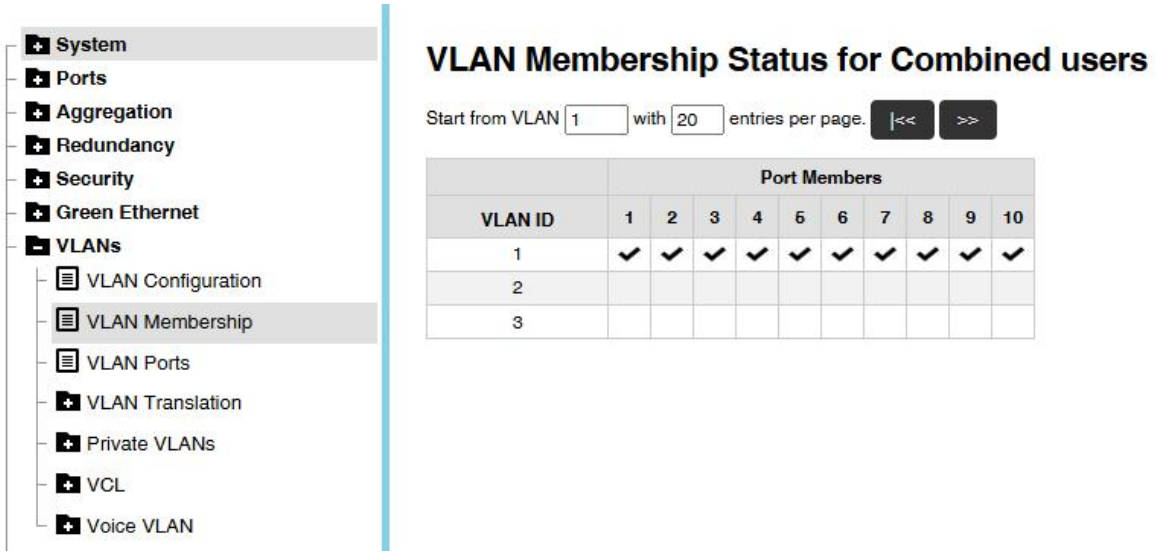


Рисунок 5-3: Отображение существующих VLAN

5.2 Конфигурация VLAN порта

Режим порта (по умолчанию — Access) определяет основное поведение порта в обсуждаемом режиме. Порты могут находиться в одном из трёх режимов.

Access:

Порты Access могут принадлежать только одной VLAN.

Принимают немаркированные кадры и кадры с меткой C.

Отбрасывают кадры, которые не принадлежат VLAN.

При передаче все кадры передаются без меток.

Trunk:

Порт Trunk может одновременно принадлежать нескольким VLAN. Обычно он используется для подключения других коммутаторов. Порт Trunk обладает следующими характеристиками:

По умолчанию порт Trunk принадлежит всем VLAN, и пользователи могут настраивать его соответствующим образом.

По умолчанию все сообщения, выходящие из порта Trunk, имеют метку (за исключением случаев, когда VLAN сообщения равна метке по умолчанию PVID).

Hybrid:

Порты типа Hybrid позволяют проходить трафику нескольких VLAN, принимать и отправлять сообщения из нескольких VLAN и могут использоваться как для подключения коммутаторов, так и для подключения пользовательских компьютеров.

Допустимые VLAN

Порты в режиме Trunk и Hybrid могут контролировать, какие VLAN разрешено включать в качестве членов. Порты Access могут быть членами только одной VLAN, то есть Access VLAN.

Пример быстрой конфигурации

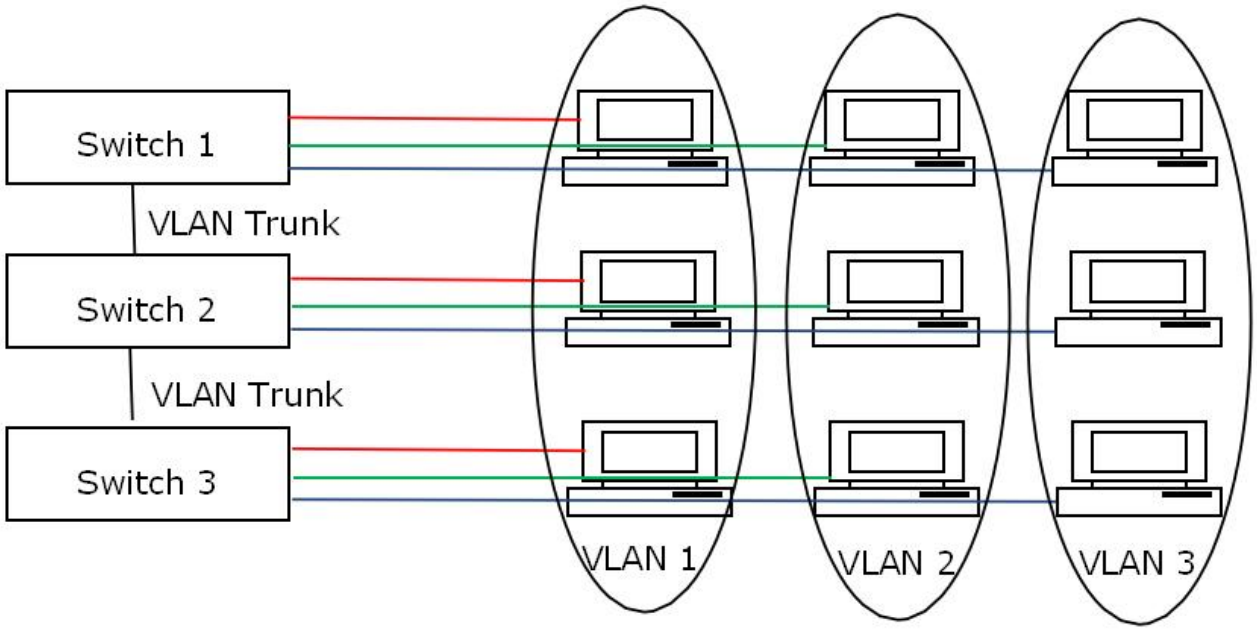


Рисунок 5-4: Пример быстрой конфигурации

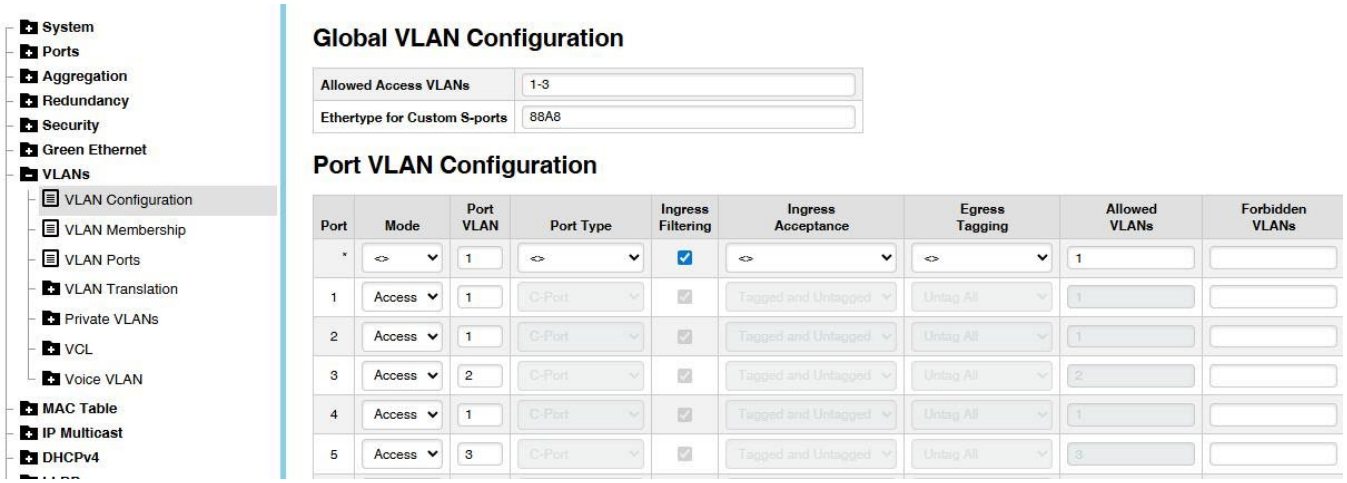


Рисунок 5-5: Конфигурация VLAN порта

6 Настройка QoS

6.1 Реализация QoS

6.1.1 Классификация QoS:

В базовой иерархии и в расширенной иерархии существует два метода классификации по категориям QoS и повторной маркировки информации о приоритете.

Базовая классификация QoS основана на PCP, DEI и SCP:

- Классификация QoS на основе PCP и DEI кадров. Отображение между каждым портом и уровнем QoS от PCP и DEI может быть изменено.
- Классификация QoS на основе значения DSCP.
- Изменение DSCP.
- Маркировка DSCP на основе уровня QoS.
- Конфигурация класса QoS для немаркированных и не-IP сообщений.
- Расширенная классификация QoS использует QCL для обеспечения гибкой классификации:

Расширенная классификация QoS использует QCL для обеспечения гибкой классификации:

- Поля протокола высокого уровня (уровни 2–4) для сопоставления правил.
- Операции включают отображение на классы QoS и преобразование значений PCP, DEI и DSCP.

6.1.2 Политика:

Ограничитель ограничивает пропускную способность принимаемых кадров сверх настраиваемой скорости. Ограничитель может быть настроен либо на уровне очереди, либо на уровне порта.

6.1.3 Алгоритм планирования:

На уровне порта коммутатора может быть два типа планирования.

Строгие приоритеты (Strict priorities):

Все очереди следуют строгим приоритетам.

DWRR (Deficit Weighted Round Robin):

Планирование выполняется на основе весов, настроенных для каждой очереди. Очереди 6 и 7 всегда используют планирование со строгим приоритетом. DWRR может выполняться на очередях в диапазоне от 0 до 5.

6.2 Настройка QoS

6.2.1 Базовая классификация QoS:

Классификация порта:

Порты могут назначать уровни QoS (CoS), PCP, DPL и DEI входящим пакетам.

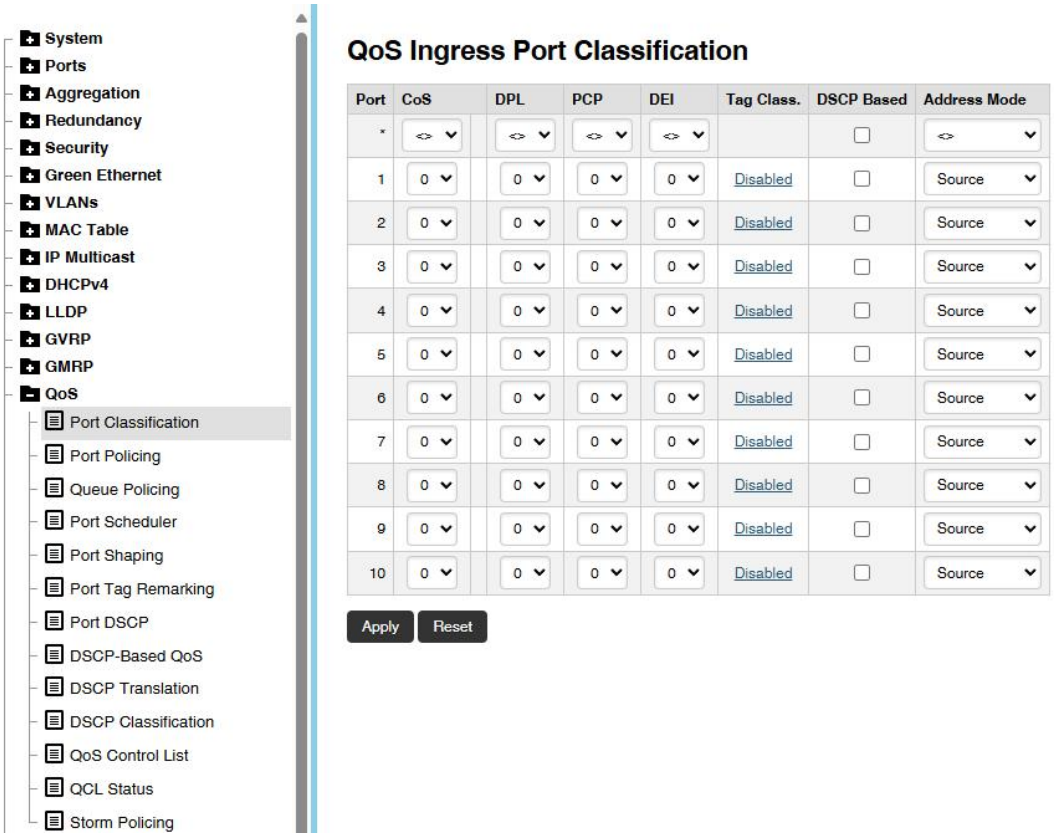


Рисунок 6-1: Классификация порта

6.2.2 Сброс маркировки порта:

Существует три способа маркировки тега сообщения исходящего направления:

Классификация: Значения PCP и DEI отчёта входящего направления могут быть обновлены соответствующими значениями входящего направления.

Значение по умолчанию: Значения PCP и DEI сообщения исходящего направления могут использовать значение по умолчанию, определённое портом.

Отображение: Значения PCP и DEI сообщения исходящего направления обновляются в соответствии с отображением тегов.

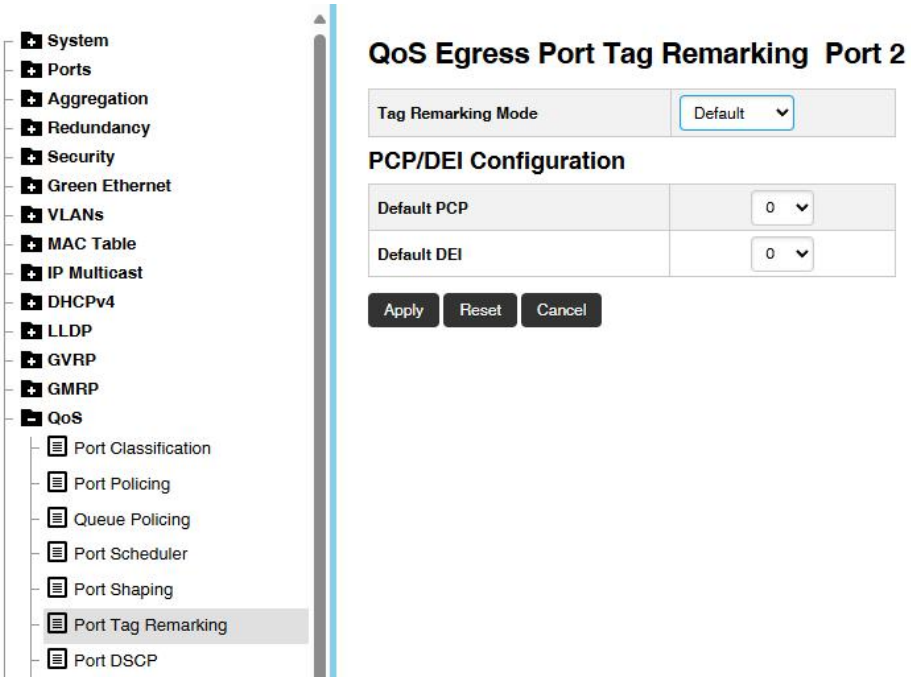


Рисунок 6-2: Маркировка входящего порта QoS

Как показано на Рисунке 6-3, уровень QoS 2 и DPL 0 отображаются на PCP 3 и DEI 0, а уровень QoS 3 и DPL 1 отображаются на PCP 4 и DEI 1.

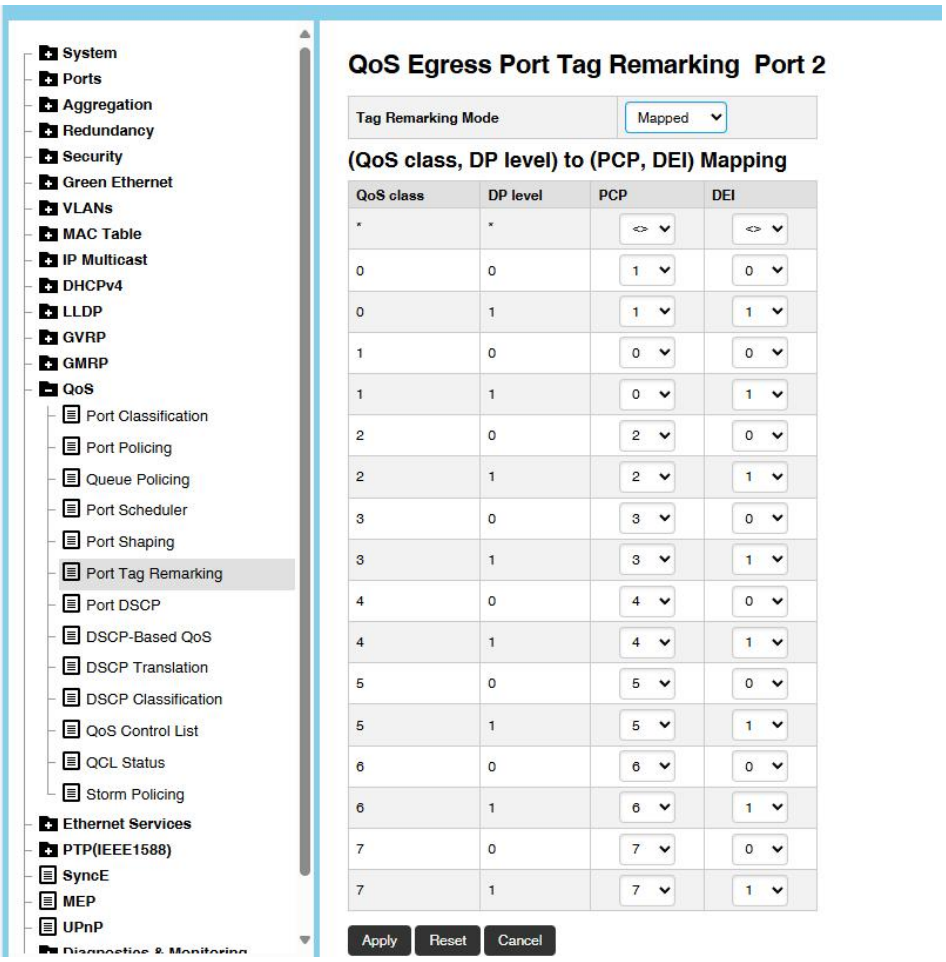


Рисунок 6-3: Маркировка исходящего порта QoS

6.2.3 Настройка DSCP:

DSCP может быть настроен как во входящем, так и в исходящем направлениях.

Как показано на Рисунке 6-4, порт 2 основан на классификации QoS по DSCP во входящем направлении.

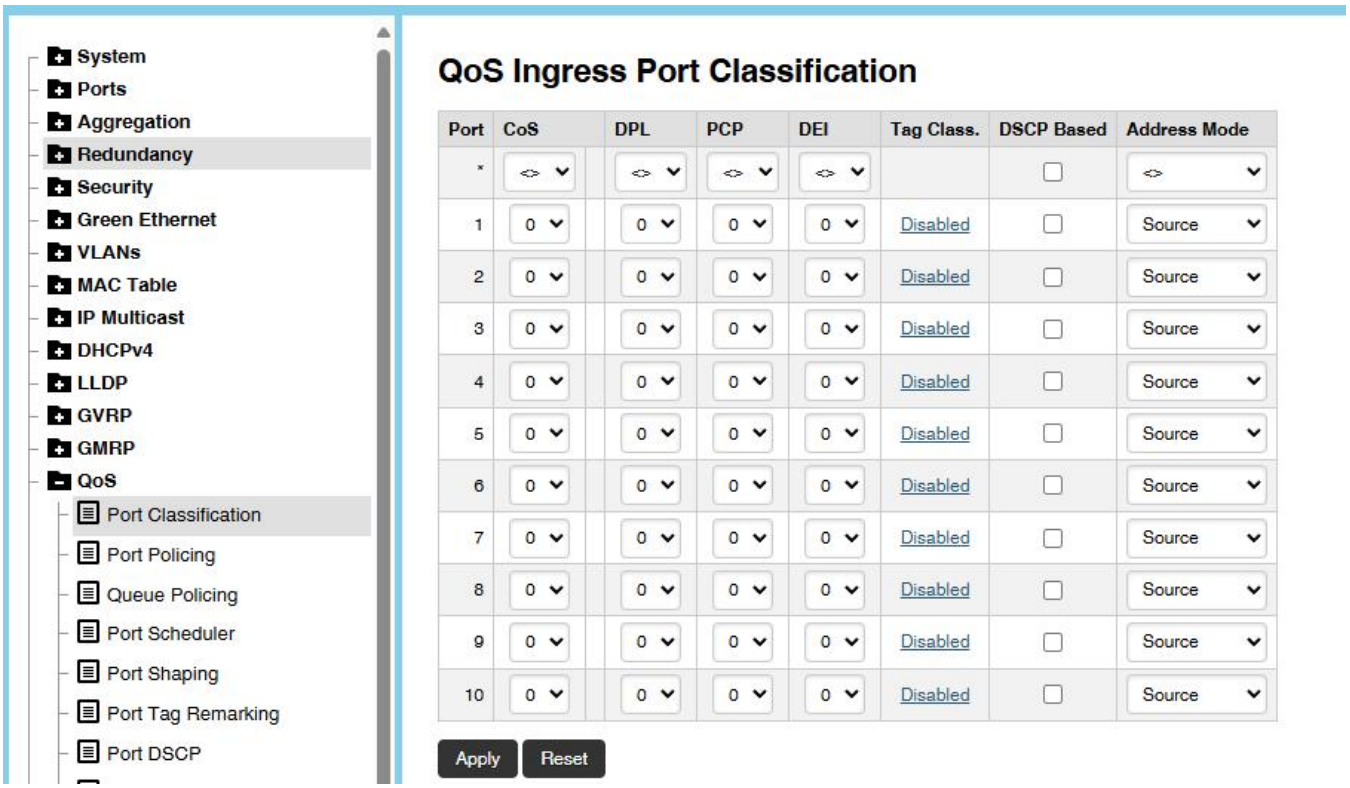


Рисунок 6-4: Классификация QoS на основе DSCP сообщения входящего направления

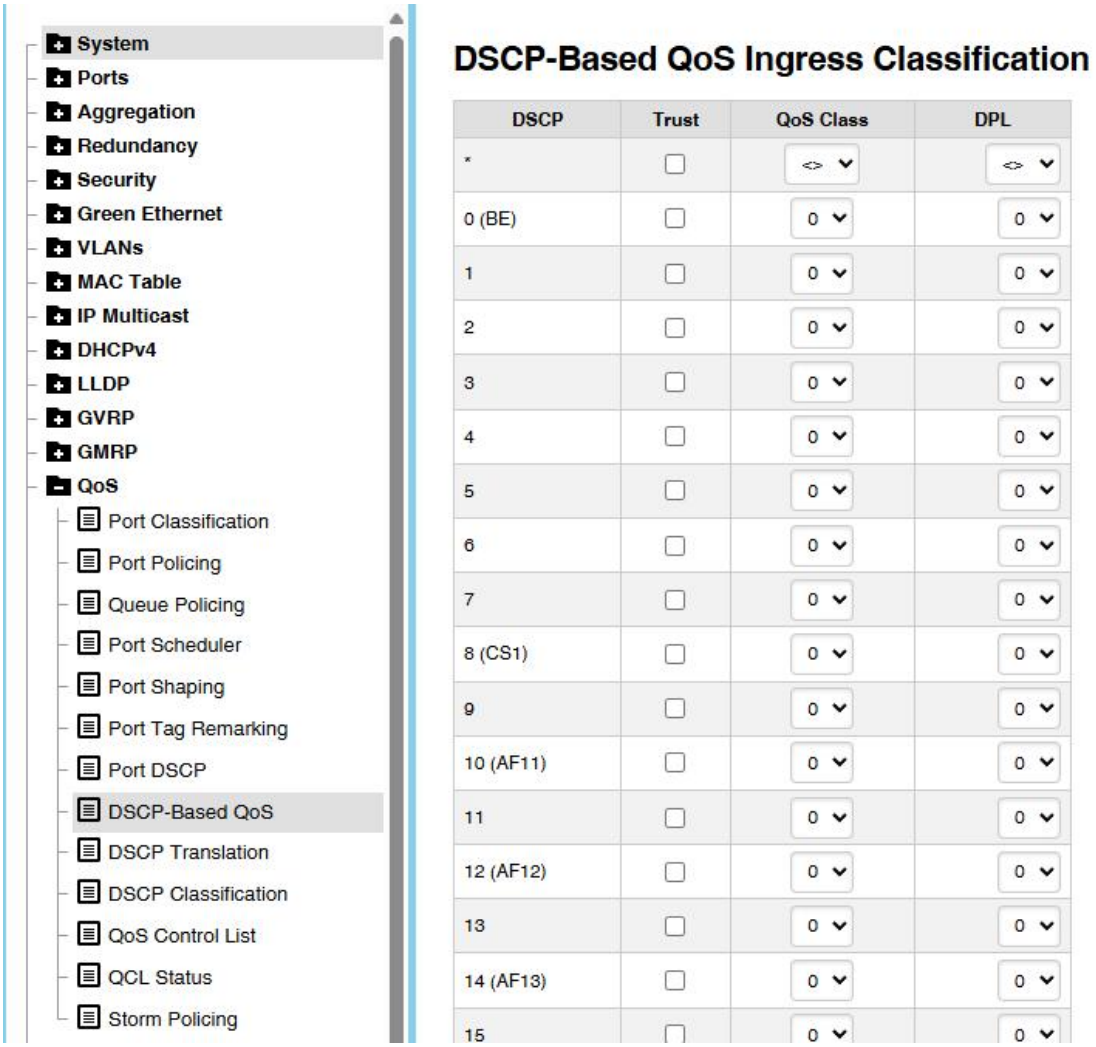


Рисунок 6-5: Классификация входа QoS на основе DSCP

Как показано на Рисунке 6-6, DSCP преобразуется во входящем направлении порта 2 и перезаписывается на порту 3.

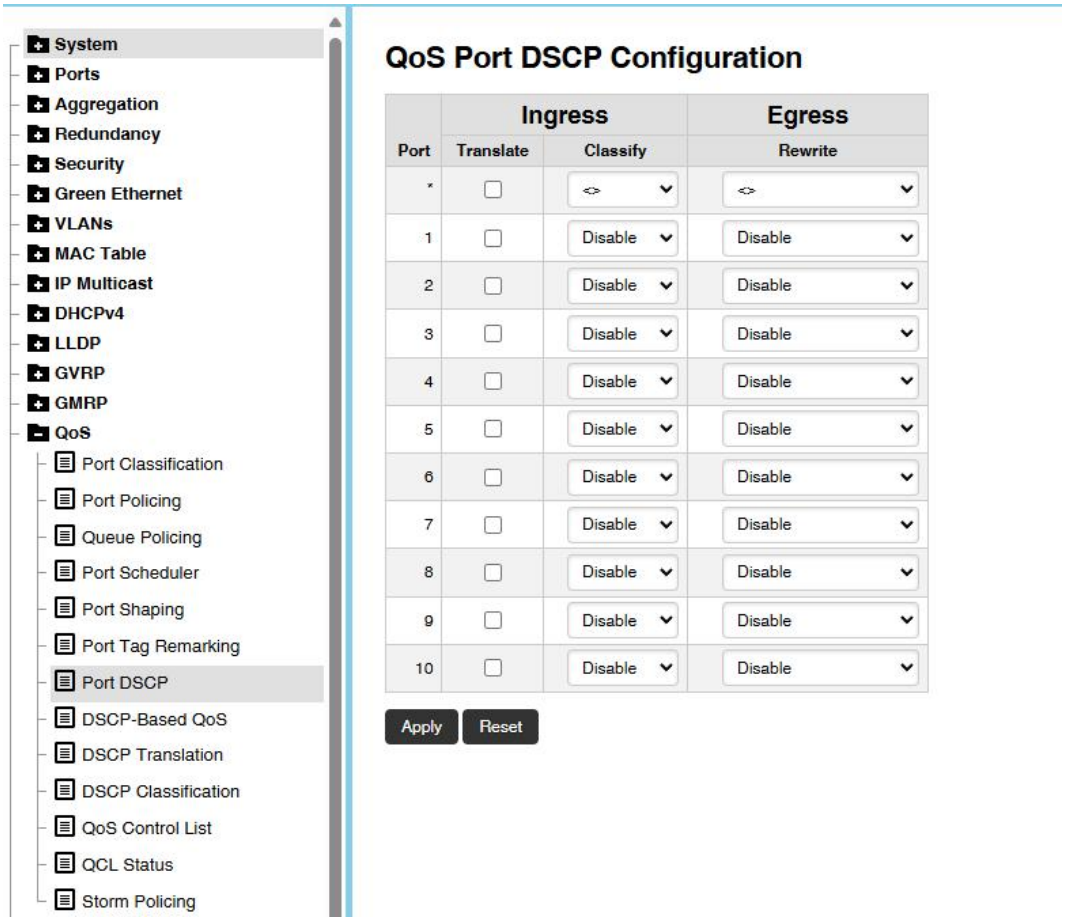


Рисунок 6-6: Преобразует DSCP на входе порта 2 и включает перезапись на порту 3

Как показано на Рисунке 6-7, DSCP = 0 установлен во входящем направлении порта 2, и перезапись включена на порту 3.

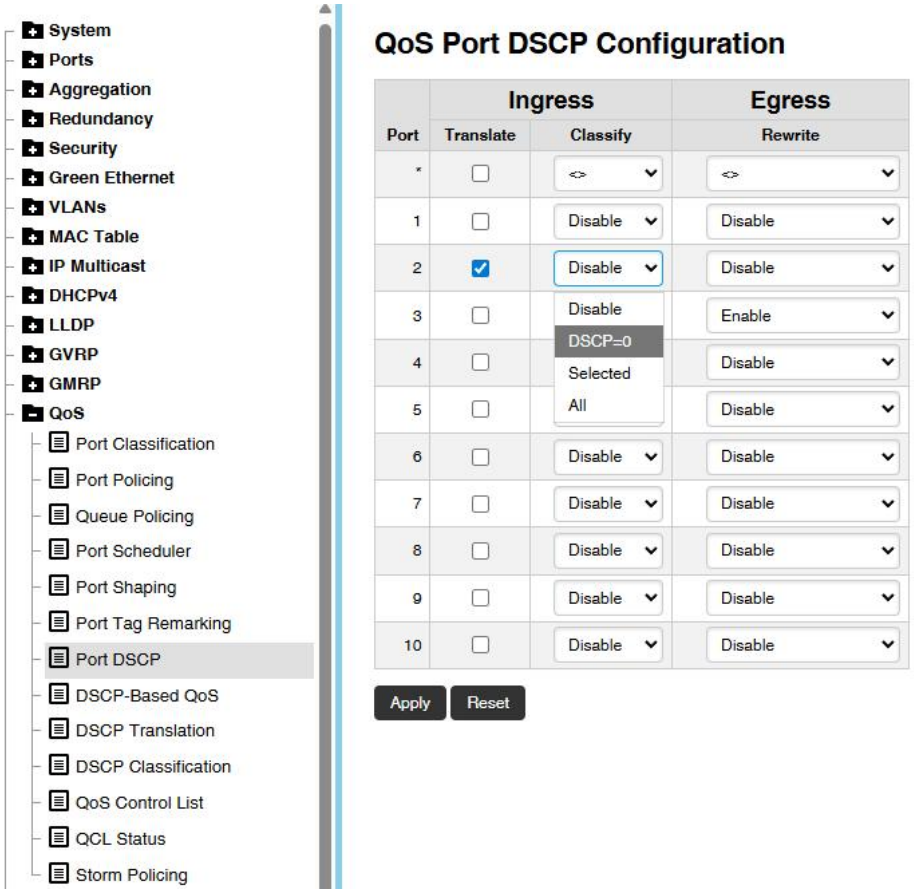


Рисунок 6-7: Устанавливает DSCP = 0 во входящем направлении порта 2 и включает перезапись на порту 3

6.3 Расширенная многоуровневая настройка QoS

6.3.1 QCLs (QoS Classification Lists):

Расширенная классификация QoS может быть выполнена путём проверки полей пакета и отображения их на значения PCP/DEI, классы QoS и значения DSCP.

Как показано на Рисунке 6-8, выполняется сопоставление определённого исходного MAC-адреса на порту 2 и отображение их на уровень QoS 5.

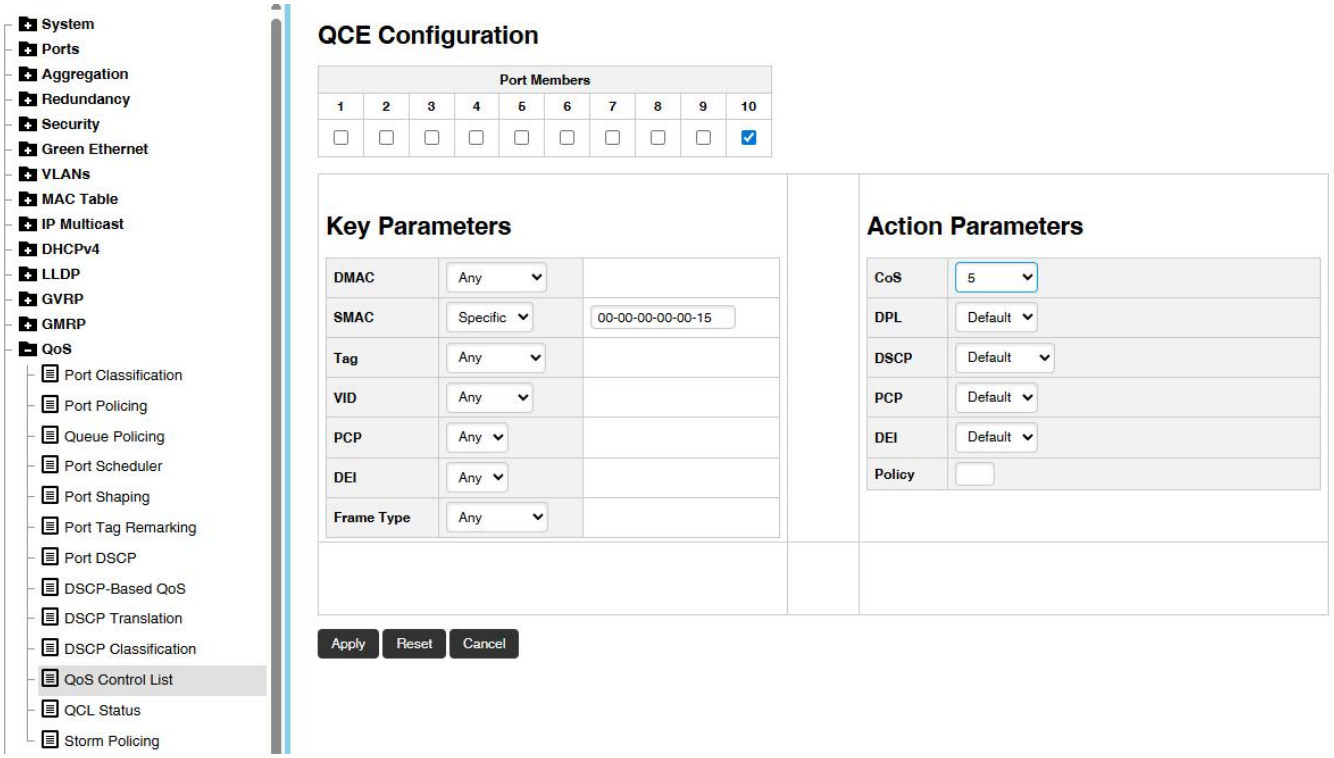


Рисунок 6-8: Сопоставляет определённый исходный MAC-адрес на порту 2 и отображает их на уровень QoS 5

6.3.2 Политика:

6.3.2.1 Политика порта

Включение политик на уровне порта на определённом порту.

Как показано на Рисунке 6-9, политика включена на порту 2 и скорость установлена на 2000 Кбит/с.

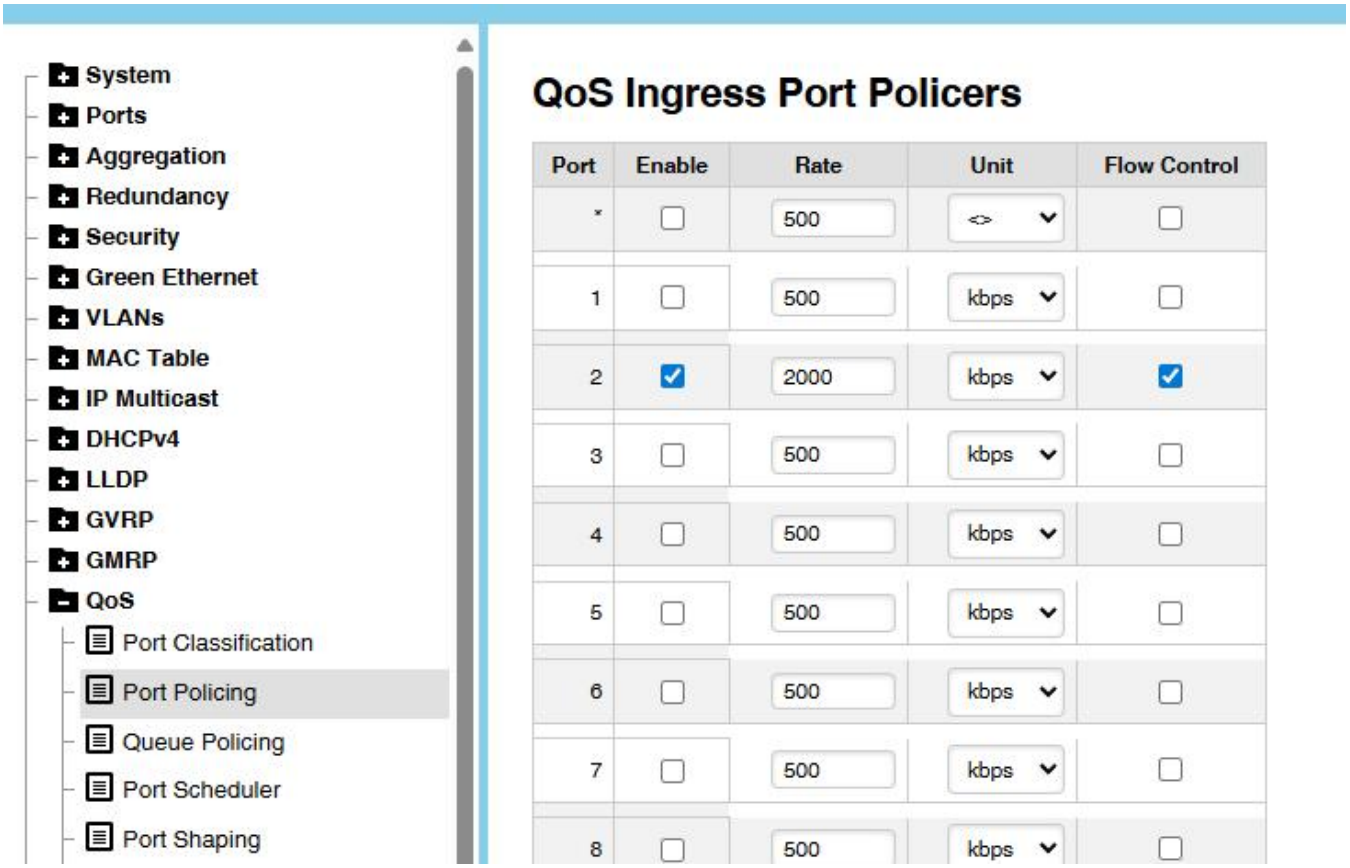


Рисунок 6-9: Устанавливает скорость порта 2 на 2000 Кбит/с

6.3.2.2 Стратегия очередей

Как показано на Рисунке 6-10, политика включена на очереди 2 порта 2. Скорость установлена на 20 Мбит/с.

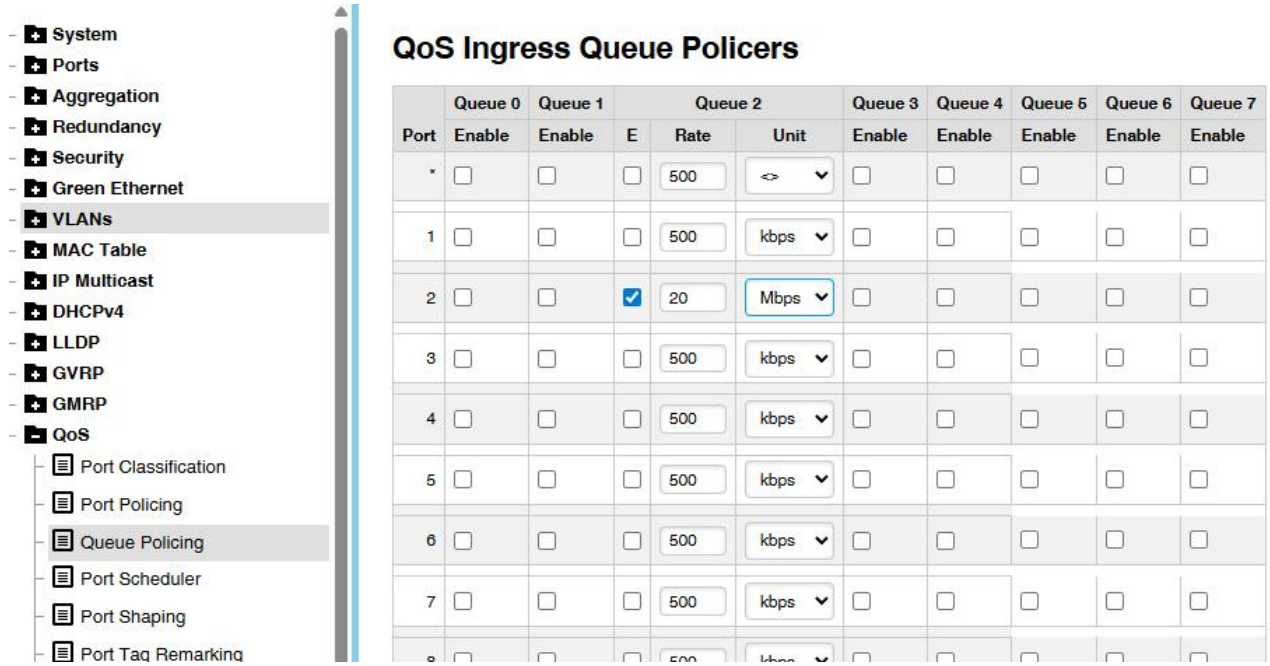


Рисунок 6-10: Включает политику на очереди 2 порта 2

6.4 Формирование трафика (Reshaping)

6.4.1 Формирование порта:

Формирование порта 3 включено со скоростью 4000 Кбит/с, и очереди 2 и 4 порта 3 включены, как показано на Рисунке 6-11.

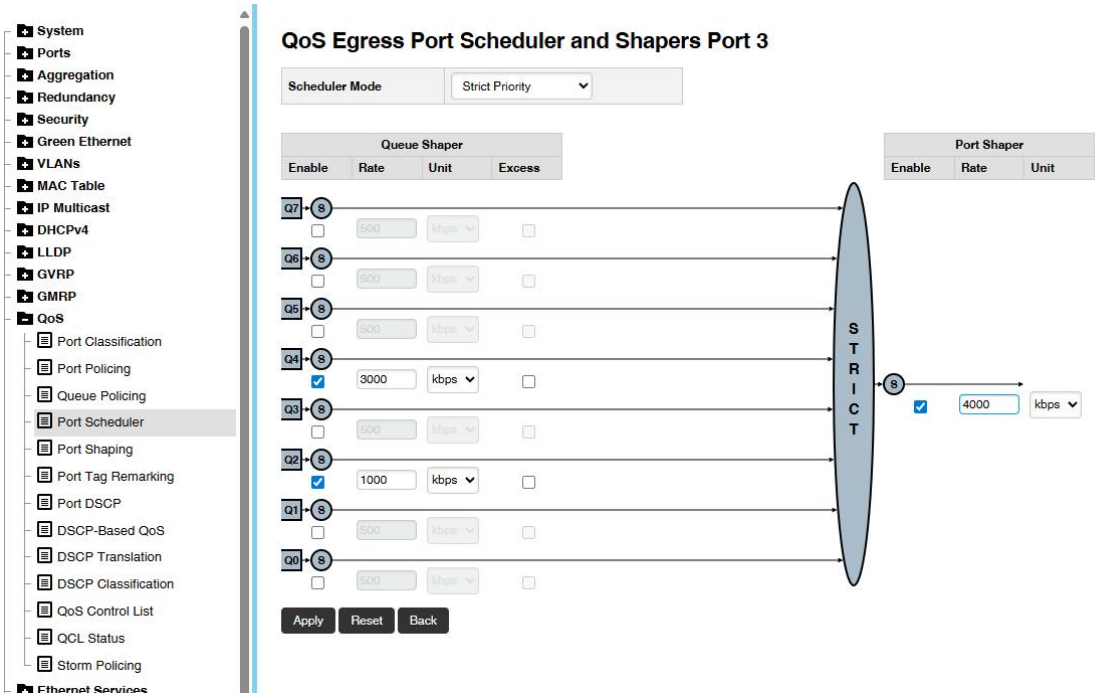


Рисунок 6-11: Формирование порта 3

6.5 Диспетчер (Dispatcher)

6.5.1 DWRR

Как показано на рисунке ниже, режим планирования порта 3 установлен в DWRR, а настройка веса очереди 0 установлена на 40, очереди 1 на 40, очереди 2 на 20, очереди 3 на 20, очереди 4 на 20 и очереди 5 на 20, как показано на Рисунке 6-12.

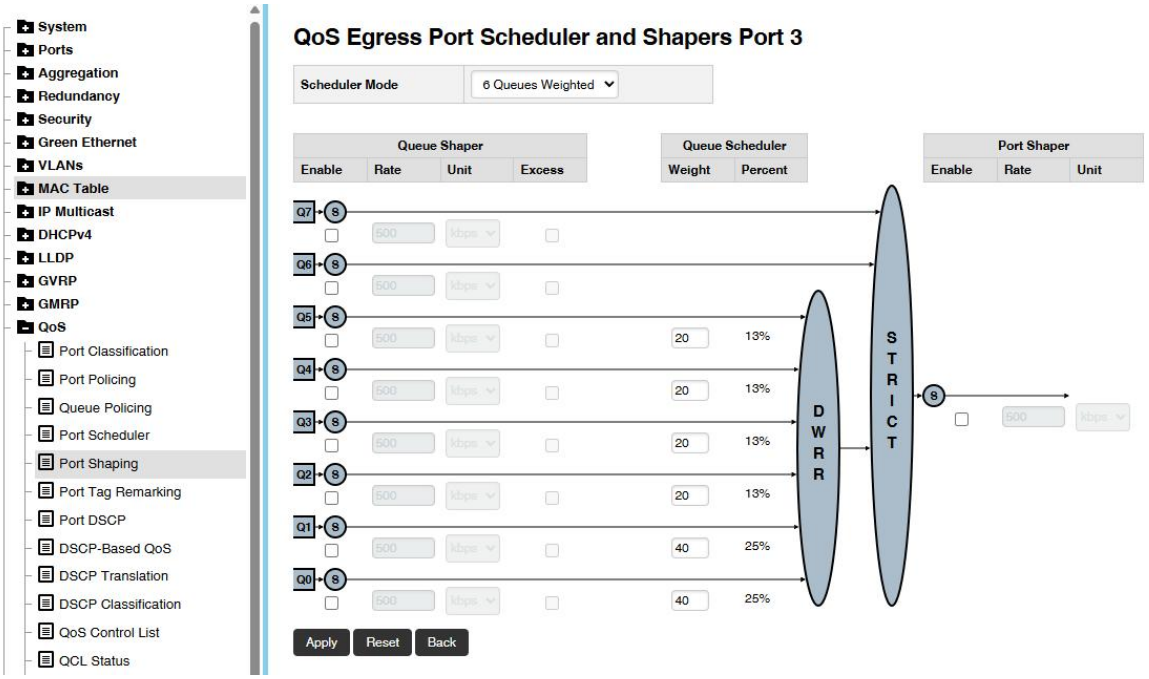


Рисунок 6-12: Конфигурация DWRR порта 3

7 Настройка LACP

7.1 Базовая конфигурация порта

Включение/отключение LACP:

Управляет, включён ли LACP на этом порту коммутатора. LACP сформирует агрегацию, когда два или более портов подключены к одноранговому устройству с включённым LACP. Значение по умолчанию — отключено.

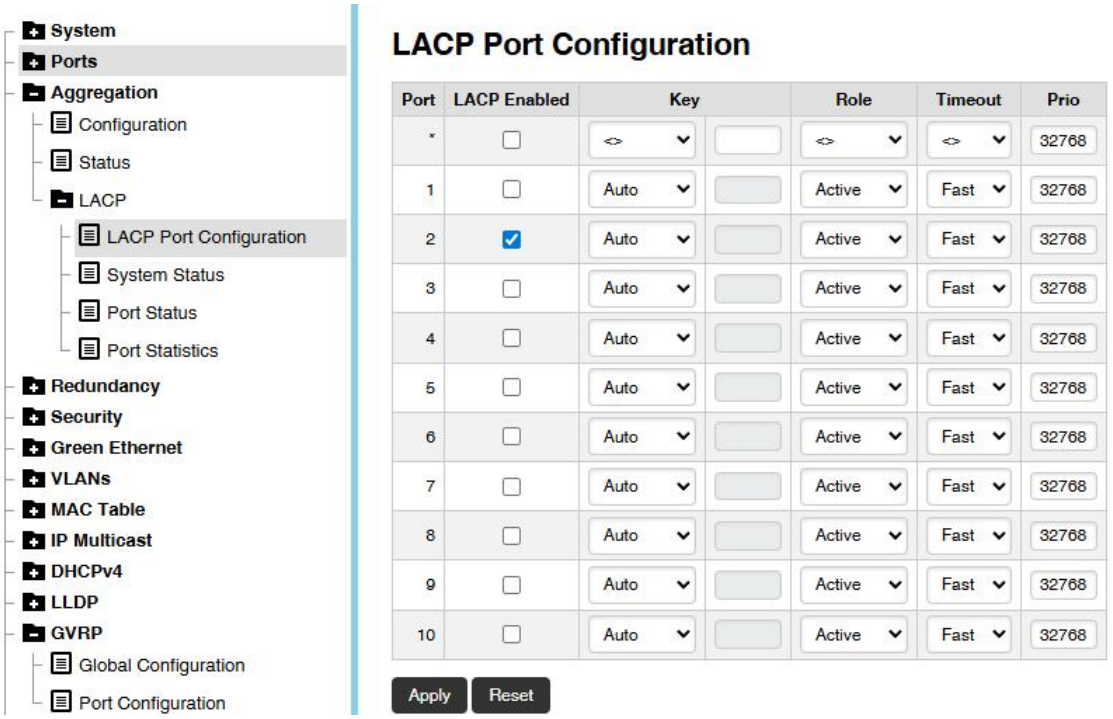


Рисунок 7-1: Включает LACP на порту 2

7.2 Настройка ключа LACP

Порты имеют диапазон ключей от 1 до 65535. Режим автоматической настройки устанавливается в соответствии со скоростью физической связи (10 Мбит = 1, 100 Мбит = 2, 1 Гбит = 3). При определённых конфигурациях могут быть введены пользовательские значения. Порты, имеющие одинаковое значение ключа, могут присоединиться к одной и той же группе агрегации, в то время как порты с разными ключами не могут быть агрегированы. Настройка по умолчанию — автоматическая.

Как показано на Рисунке 7-2, значение ключа установлено на 4 на порту 2.

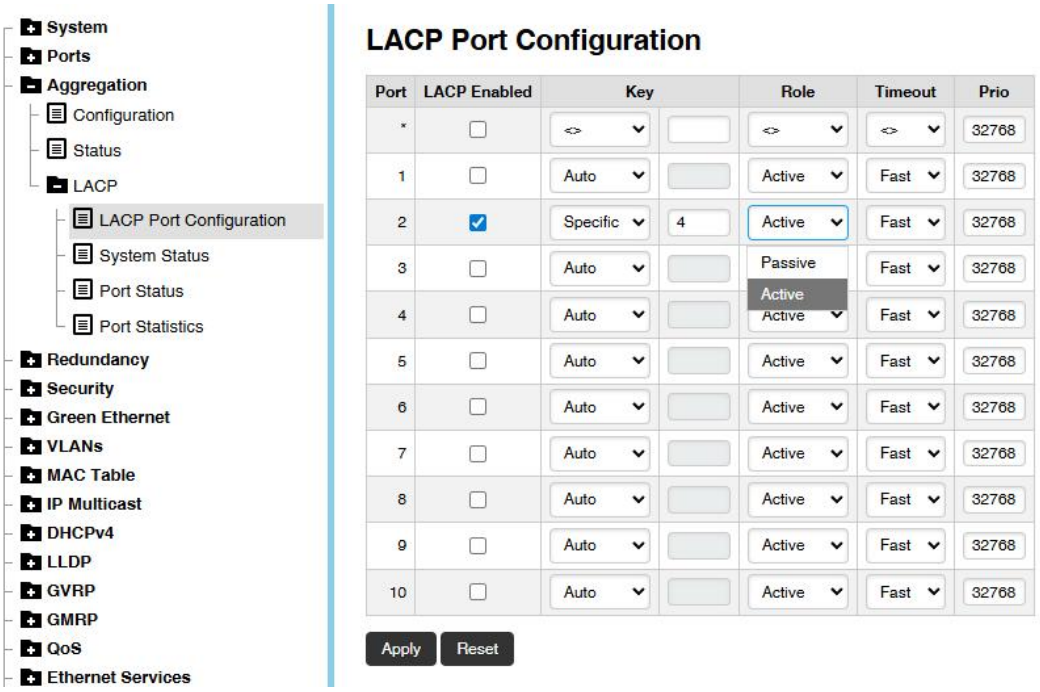


Рисунок 7-2: Устанавливает значение LACP на 4 на порту 2

7.2.1 Настройка роли LACP:

Эта роль показывает состояние активности LACP. Активное состояние будет отправлять пакеты LACP каждую секунду, в то время как пассивное состояние должно ждать пакеты LACP от противоположного конца. Значение по умолчанию — активное, как показано на Рисунке 7-2 выше.

7.2.2 Настройка тайм-аута LACP:

Эта конфигурация управляет временным интервалом между передачами BDU. Быстрый режим передаёт пакеты LACP каждую секунду, в то время как медленный режим отправляет пакеты LACP каждые 30 секунд. Значение по умолчанию — быстрый, как показано на Рисунке 7-2 выше.

8 Таблица MAC-адресов

Коммутация кадров выполняется на основе исходного MAC-адреса в кадре. Коммутатор создаёт таблицу, которая отображает MAC-адреса на порты коммутатора, которая содержит как статические, так и динамические MAC-адреса. Если пользователи хотят отобразить адреса DMAC на порты коммутатора, им необходимо настроить статические MAC-адреса.

Коммутатор автоматически обновляет таблицу динамических MAC-адресов на основе исходного MAC-адреса кадра. Если кадры для этого MAC-адреса не принимаются после времени старения, динамический MAC-адрес удаляется из таблицы MAC-адресов.

8.1 Установка времени старения таблицы MAC-адресов

По умолчанию записи динамической таблицы удаляются из таблицы MAC через 300 секунд. Это удаление называется старением.

Как показано на Рисунке 8-1, время старения изменено на 200 секунд.

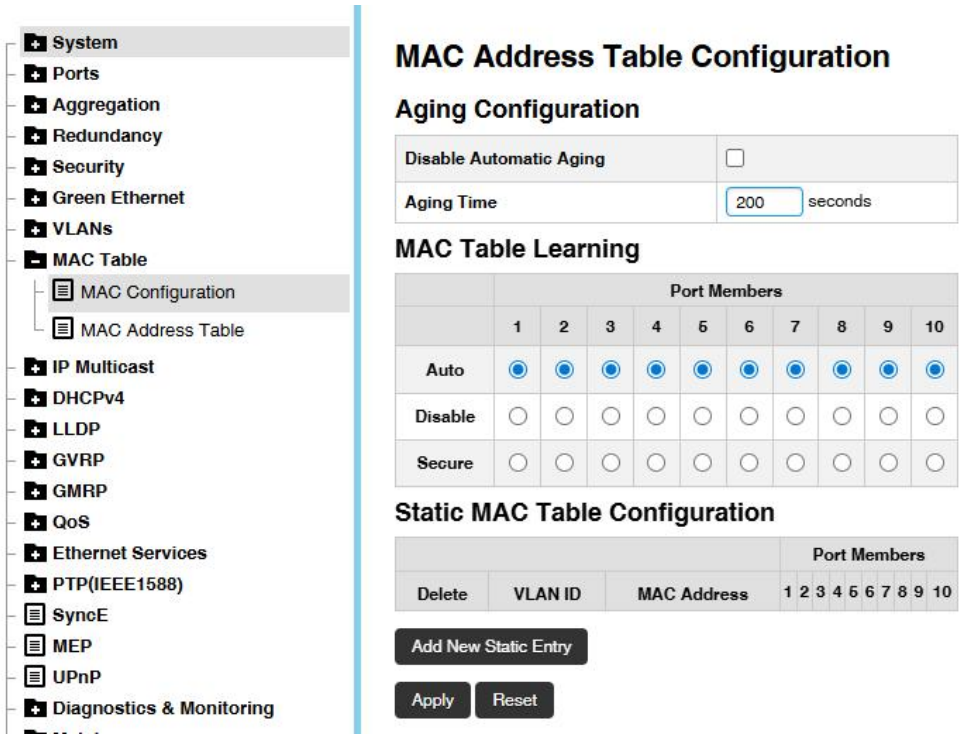


Рисунок 8-1: Изменено время старения на 200 секунд

8.2 Добавление статической таблицы MAC-адресов

Добавление записи статической таблицы MAC-адресов в таблицу MAC-адресов.

Как показано на Рисунке 8-2, добавлен статический MAC-адрес 00:00:00:00:00:0f на порт 3 VLAN1.

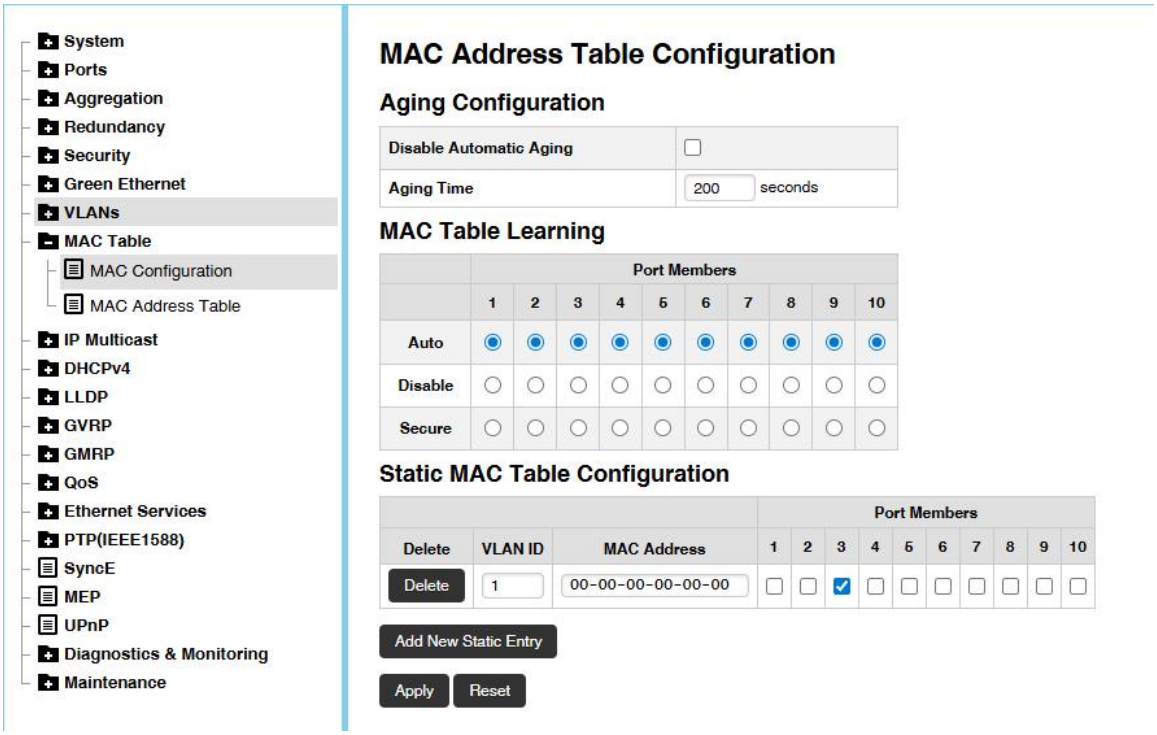


Рисунок 8-2: Добавляет статический MAC-адрес 00:00:00:00:00:0f на порт 3 в VLAN1

8.3 Отображение таблицы MAC-адресов

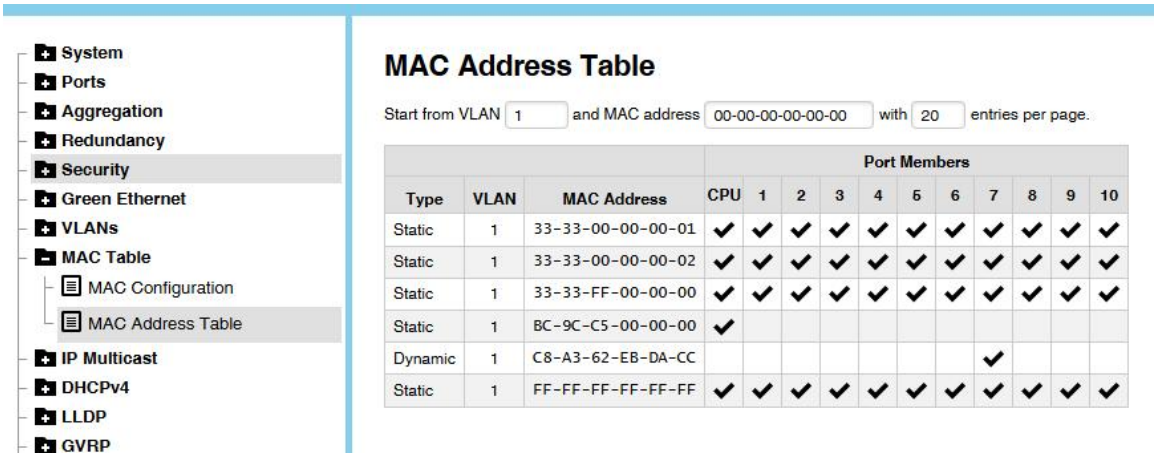


Рисунок 8-3: Показывает таблицу MAC-адресов

9 Зеркалирование и удалённое зеркалирование

9.1 Зеркалирование (локальное)

Для отладки сетевых проблем или мониторинга сетевого трафика система коммутатора может быть настроена для зеркалирования кадров с нескольких портов на порт зеркалирования.

9.1.1 Тип:

Акустический образ (acoustic image):

Настройка коммутатора в режиме локального зеркалирования. Исходный порт и порт назначения находятся на одном коммутаторе.

Источник (source):

Настройка коммутатора в качестве узла-источника зеркалирования. Исходный порт, промежуточный порт и порт отражения расположены на этом коммутаторе.

Промежуточный (intermediary):

Выступает в качестве промежуточной передачи для сообщений зеркалирования.

Назначение (purpose):

Сообщения зеркалирования в конечном итоге обмениваются между коммутаторами для целей зеркалирования.

9.1.2 VLAN ID:

VLAN ID относится к целевому VLAN зеркала. Рекомендуется отделить его от сервисного VLAN.

9.1.3 Конфигурация исходного VLAN:

Коммутаторы могут поддерживать зеркалирование на основе VLAN.

Примечание: Сессии зеркалирования должны иметь возможность использовать порты или VLAN в качестве источников, но не оба одновременно.

9.1.4 Зеркалирование порт-порт:

Как показано на Рисунке 9-1, трафик порта 1 зеркалируется на порт 6.

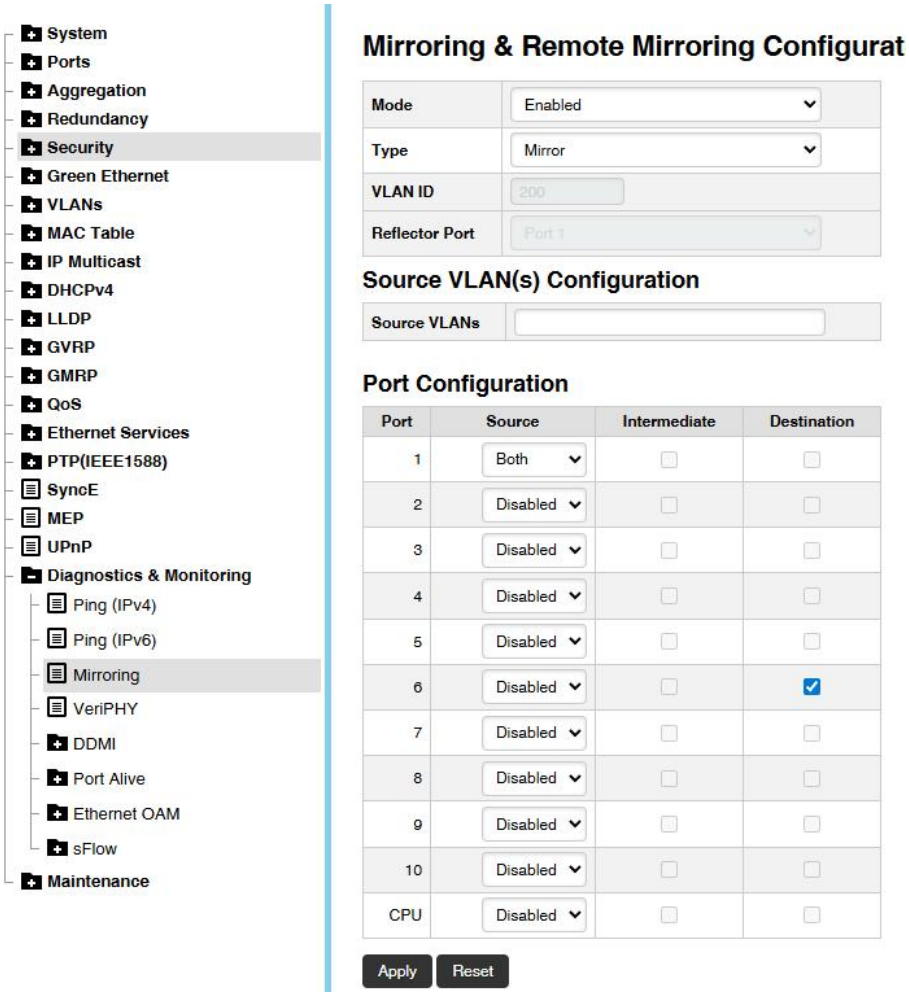


Рисунок 9-1: Порт 1 зеркалируется на порт 6

9.1.5 Зеркалирование VLAN на порты:

Как показано на Рисунке 9-2, трафик VLAN123 зеркалируется на порт 2.

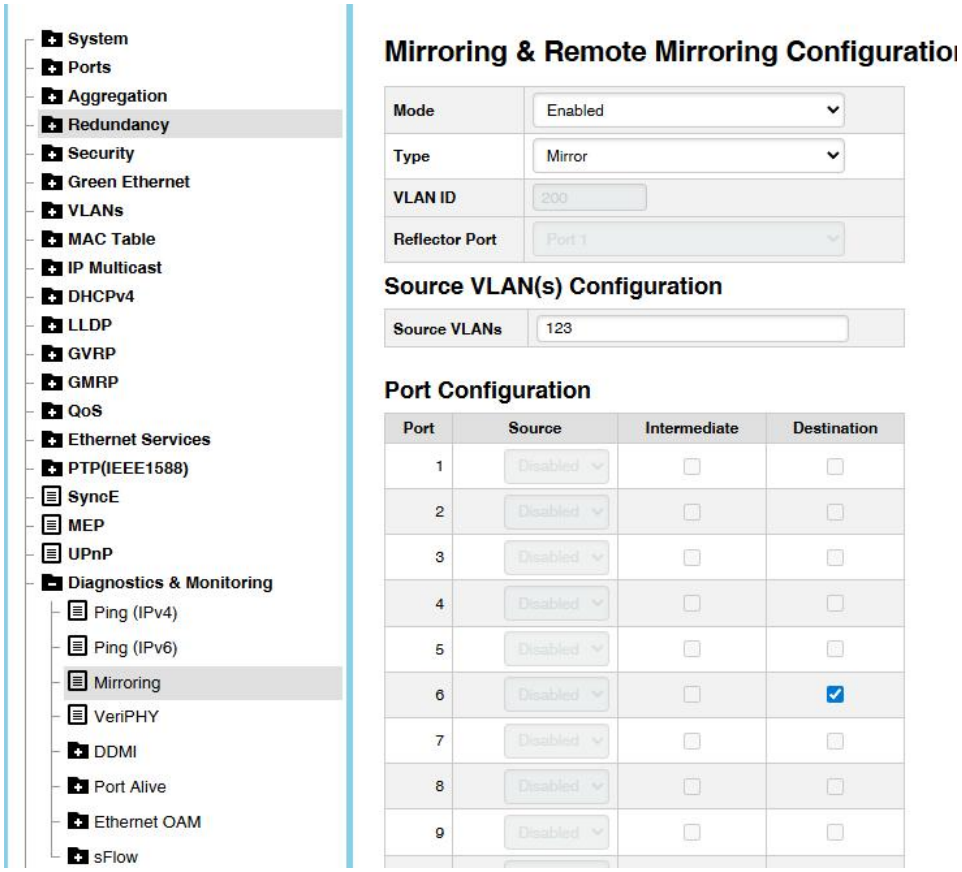


Рисунок 9-2: Зеркалирование пакетов VLAN123 на порт 2

9.2 Удалённое зеркалирование

Удалённое зеркалирование является расширенной функцией зеркалирования. Оно может расширять целевые порты на других коммутаторах, позволяя пользователям анализировать сетевой трафик на других коммутаторах.

Как показано на Рисунке 9-3.

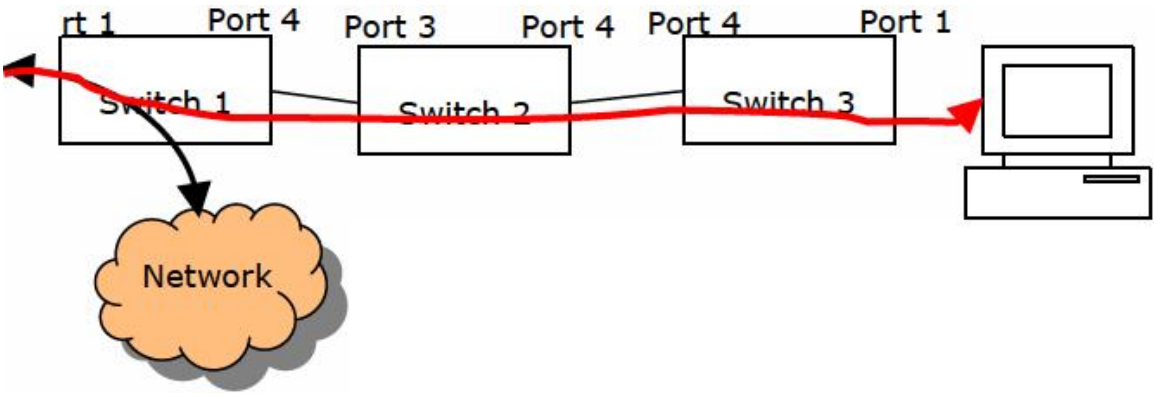


Рисунок 9-3: Топология удалённого зеркалирования

Коммутатор 1:

Используйте следующие параметры для настройки коммутатора 1 в качестве исходного коммутатора:

- Исходный порт: 1
- Режим зеркалирования: Зеркалируются как принимаемые, так и передаваемые кадры.
- Промежуточный порт: 4

Примечание: На промежуточном порту необходимо отключить изучение таблицы MAC.

- Порты отображения: 2

Примечание 1: Порт отображения необходимо выбрать только тип исходного зеркала.

Примечание 2: На порту отображения необходимо отключить изучение таблицы MAC и STP.

Примечание 3: Порт отображения поддерживает только электрические порты.

VLAN зеркалирования: 200

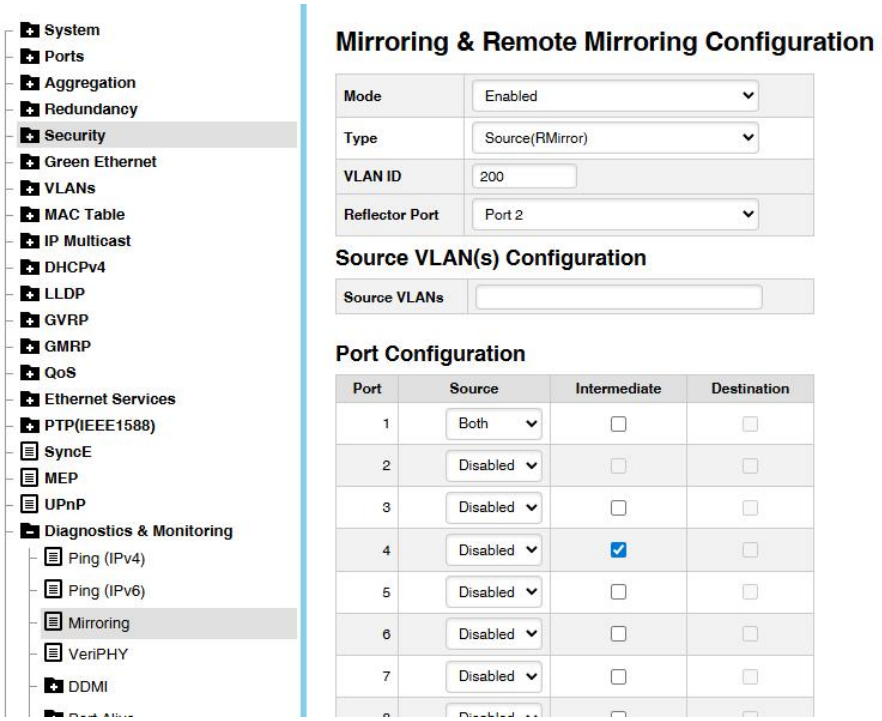


Рисунок 9-4: Удалённое зеркалирование — исходный коммутатор

Коммутатор 2:

Используйте следующие параметры для настройки коммутатора 2 в качестве промежуточного коммутатора:

- Промежуточные порты: 3 и 4

Примечание: На промежуточных портах необходимо отключить изучение таблицы MAC.

- VLAN трафика зеркалирования: 200

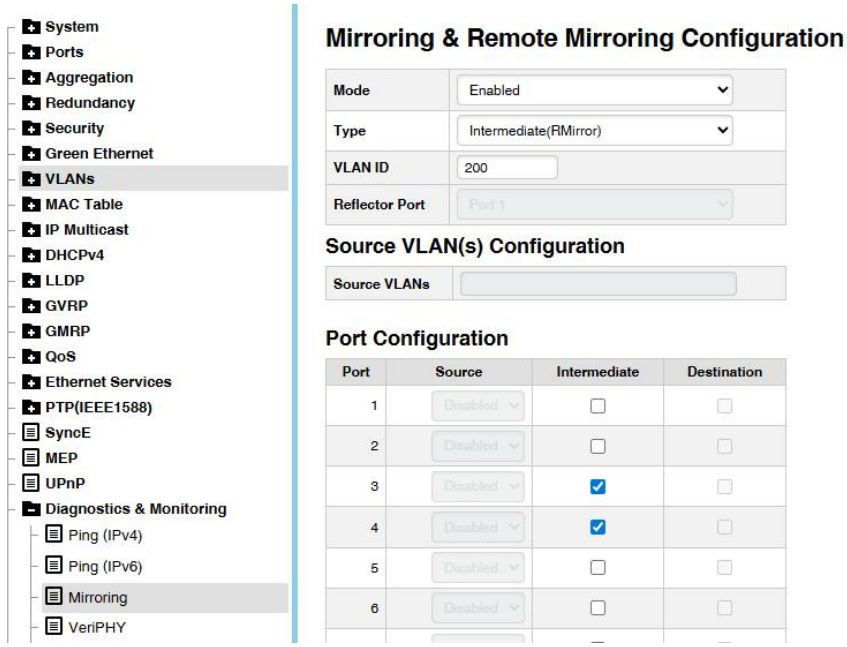


Рисунок 9-5: Конфигурация промежуточного коммутатора удалённого зеркалирования

Коммутатор 3:

Используйте следующие параметры для настройки коммутатора 3 в качестве целевого коммутатора:

- Промежуточный порт: 4

Примечание: На промежуточном порту необходимо отключить изучение таблицы MAC.

- Целевой порт: 1

Примечание 1: Устройство поддерживает только один порт назначения.

Примечание 2: На целевом порту необходимо отключить изучение таблицы MAC.

- VLAN трафика зеркалирования: 200

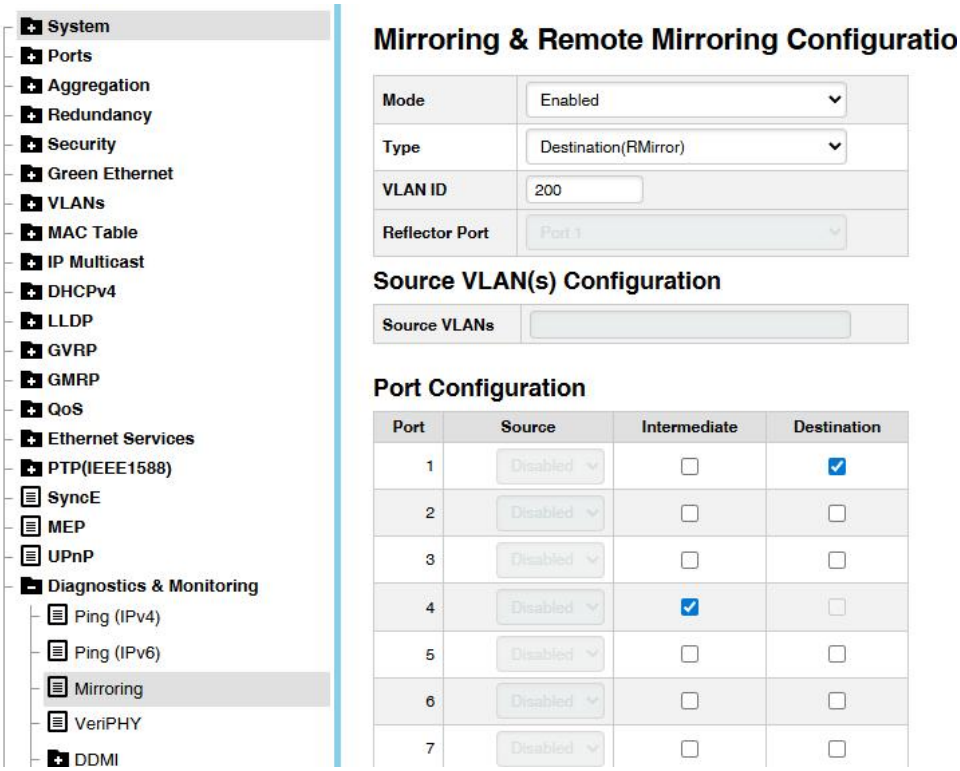


Рисунок 9-6: Коммутатор назначения удалённого зеркалирования

10 GVRP

Общий протокол регистрации VLAN (GVRP, General VLAN Registration Protocol) описан в стандартах IEEE 802.1Q-2005, раздел 11 и IEEE 802.1D-2004, раздел 12.

10.1 Конфигурация порта GVRP

Порт GVRP включается следующим образом:

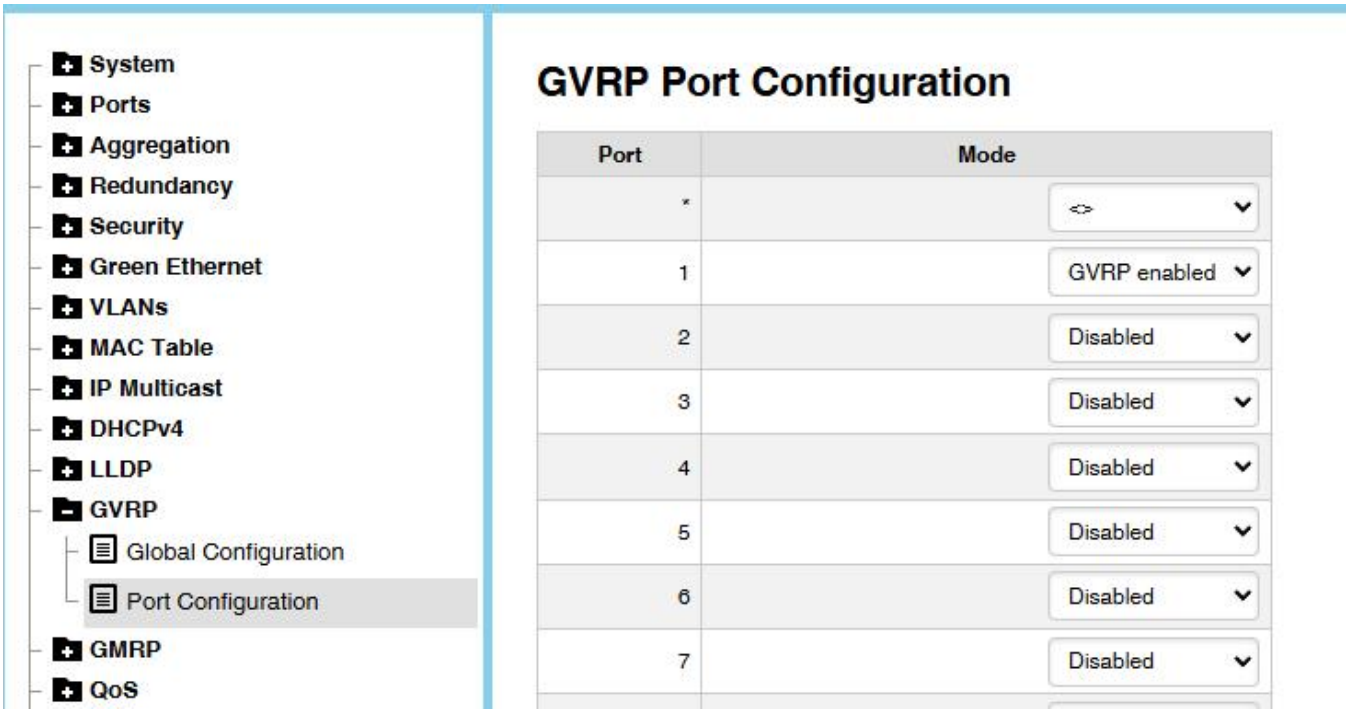


Рисунок 10-1: GVRP включён

10.2 Глобальная конфигурация GVRP

Можно настроить небольшое количество параметров для GVRP. Эти параметры настраиваются в веб-интерфейсе следующим образом:

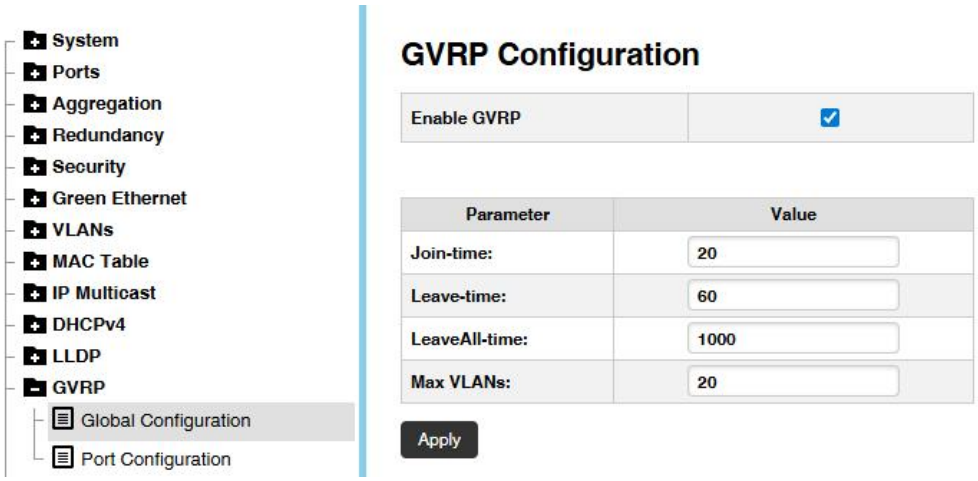


Рисунок 10-2: Конфигурация GVRP

11 Протокол множественного покрывающего дерева (MSTP)

11.1 Конфигурация корневого моста

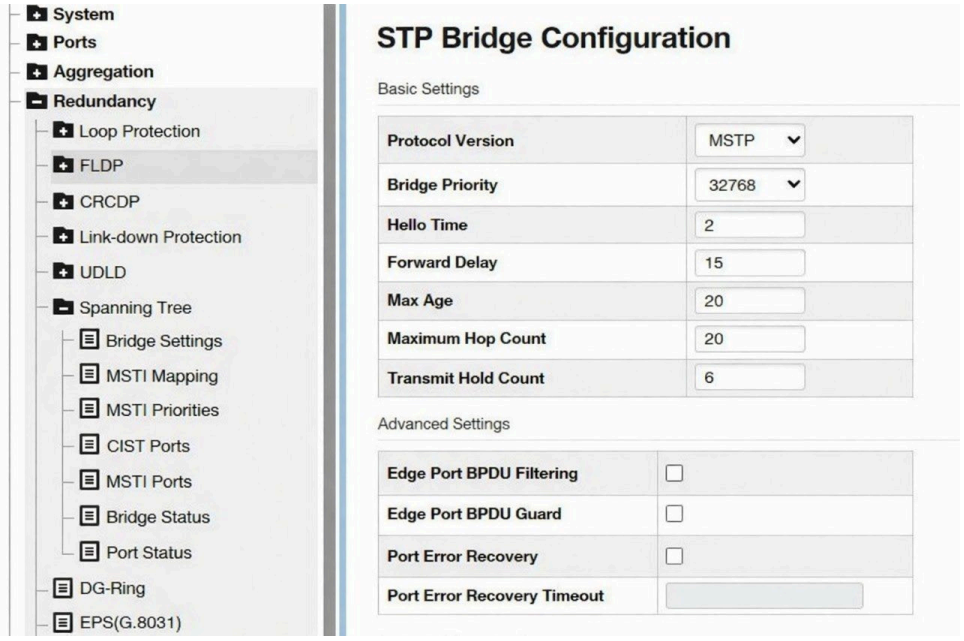


Рисунок 11-1: Конфигурация корневого моста

11.2 Конфигурация MSTI

По умолчанию все идентификаторы VLAN отображаются на CIST (Common and Internal Spanning Tree). Когда тип протокола установлен в MSTP, идентификаторы VLAN могут быть назначены одному из восьми покрывающих деревьев, причём CIST является первым. Оставшиеся семь обозначаются как MSTI1 через MSTI7, как показано на диаграмме. Конфигурации MSTI также имеют имена и версии, как проиллюстрировано. Все эти значения должны быть настроены идентично на всех коммутаторах в сети; в противном случае конфигурация не вступит в силу.

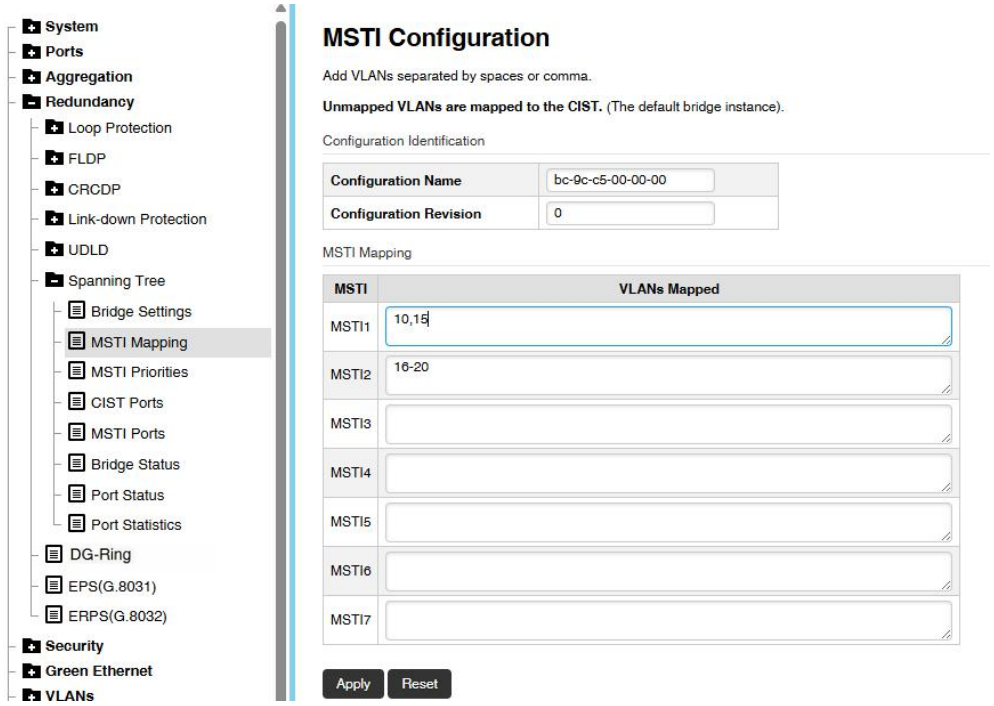


Рисунок 11-2: Конфигурация MSTI

11.3 Приоритет MSTI

Каждый MSTI и CIST имеют приоритет, как показано ниже:

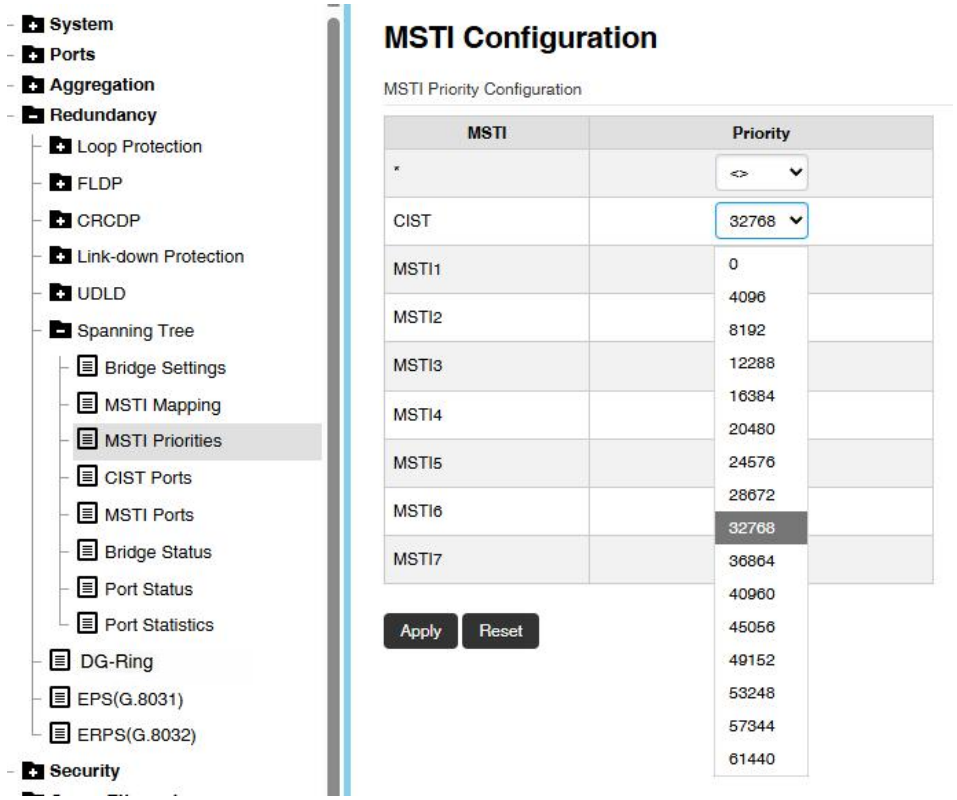


Рисунок 11-3: Атрибуты MSTI

Меньшее число приоритета указывает на более высокий приоритет. Каждый CIST, MSTI1,..., MSTI7 формируют идентификатор моста, который служит приоритетом моста (см. Рисунок 3) и комбинируется с числами на диаграмме выше. Это соответствует MAC-адресу коммутатора. Поэтому идентификатор моста должен быть уникальным.

Меньший идентификатор моста указывает на более высокий приоритет. По сравнению с коммутаторами с более низким приоритетом, данный коммутатор с большей вероятностью станет корнем покрывающего дерева. Поэтому, если два коммутатора имеют идентичные приоритеты моста, выбор приоритета MSTI1 выше, чем у другого коммутатора в MSTI1, и аналогично в MSTI2, один коммутатор имеет тенденцию становиться корнем одного MSTI, в то время как другой становится корнем другого MSTI.

11.4 Конфигурация порта CIST

STP на основе порта настраивается в веб-интерфейсе, как показано на Рисунке 11-4.

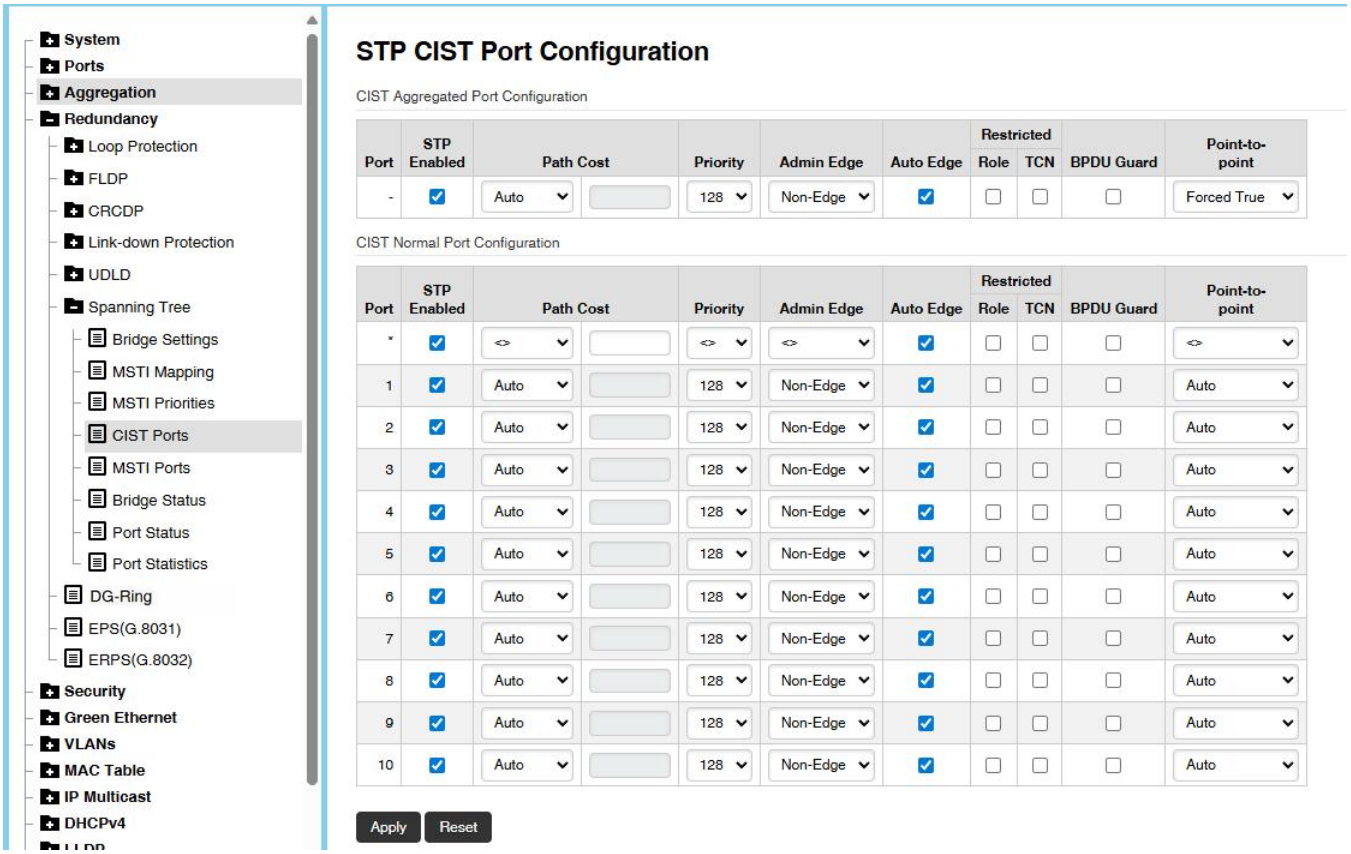


Рисунок 11-4: Конфигурация порта CIST

Следует отметить, что все параметры, упомянутые выше (за исключением стоимости пути и приоритета), применяются к портам, а не к CIST. Существуют две конфигурации для CIST: конфигурация агрегированного порта и обычная конфигурация порта CIST. В последнем случае все завершённые конфигурации выполняются в режиме интерфейса конфигурации.

11.4.1 Пограничные порты (Edge ports):

Пограничный порт — это порт, не подключённый к мосту. Если включено автоматическое определение пограничного порта (auto-edge), порт определяется как пограничный на основе того, принимаются ли BPDU на этом порту. Административный пограничный порт (admin edge) определяет, является ли порт пограничным, до тех пор, пока не будет активировано автоматическое определение и не внесены изменения. Окончательный результат можно просмотреть, выбрав «Мониторинг» → «Покрывающее дерево» → «Состояние моста», затем нажав «CIST». Поле «Edge» отображает результаты.

11.4.2 Ограничение роли и ограничение TCN:

Включение ограничения роли предотвращает выбор портов в качестве корневых портов для CIST или любого MSTI, даже когда они имеют наивысший приоритет покрывающего дерева. Как только корневой порт выбран, такие порты будут назначены как резервные. Если эта конфигурация реализована, это может привести к отсутствию избыточности покрывающего дерева. Сетевые администраторы могут настроить эту функцию для предотвращения влияния мостов за пределами зон основной сети на активную топологию покрывающего дерева, особенно когда эти мосты находятся вне полного административного контроля. Эта функциональность также известна как «Защита корня» (Root Guard). Когда активировано ограничение TCN, порты не будут пересылать полученные уведомления об изменении топологии на другие интерфейсы.

11.4.3 Защита BPDU (BPDU Guard):

Если включено, порт отключает себя, когда принимает корректный BPDU. В отличие от подобных настроек моста, состояние пограничного порта не влияет на эту настройку.

11.4.4 Точка-точка (Point-to-point):

Режим NORMODE эквивалентен установке в автоматический режим (auto).

Установите соединение как точка-точка, что будет отображаться как «Принудительно Истина» (Forced True) в веб-интерфейсе. Установите как общее (shared), что будет отображаться как «Принудительно Ложь» (Force False). Установите как автоматическое (auto), что будет отображаться как «Авто» (Auto).

11.5 Конфигурация порта MSTI

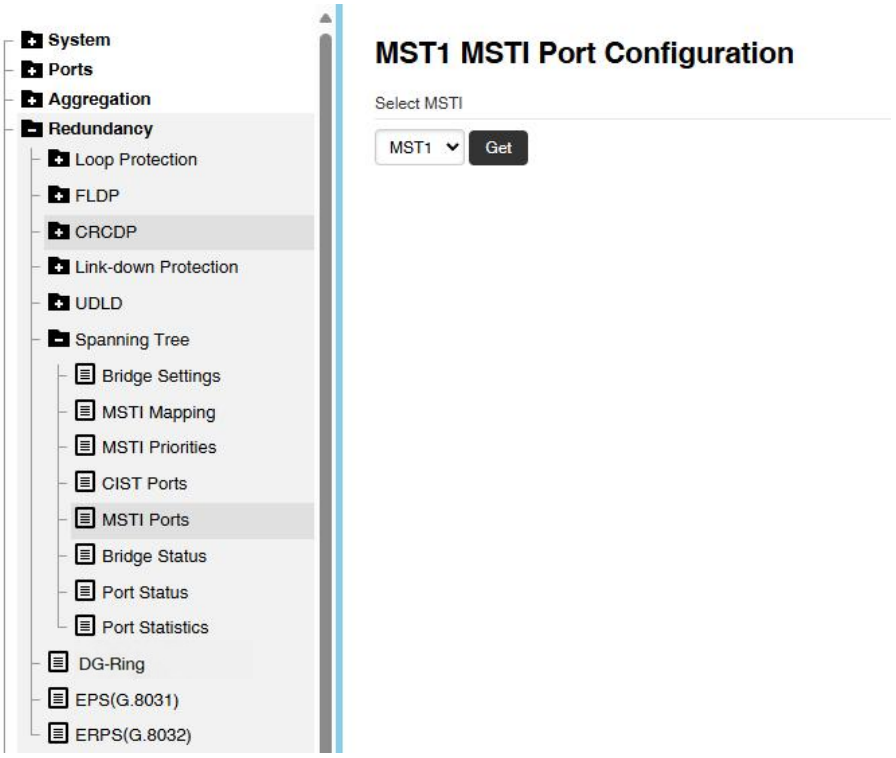


Рисунок 11-5: Конфигурация MSTI

Затем выберите требуемый MSTI и нажмите «Получить» (Get).

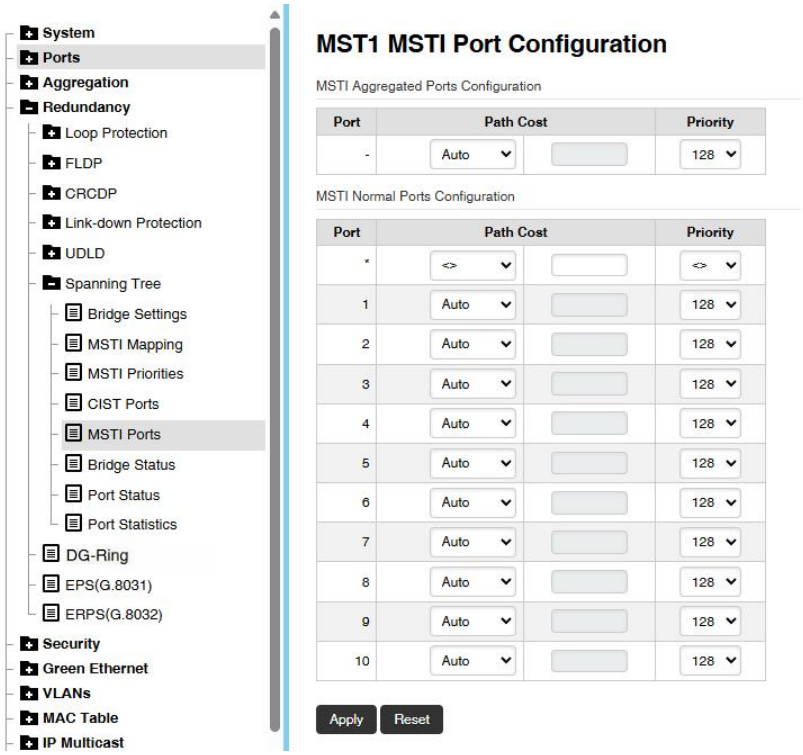


Рисунок 11-6: Конфигурация MSTI и порта

«Стоимость» (<Cost>) — это число в диапазоне от 1 до 200000000 или «авто». Если установлено «авто», стоимость пути будет установлена на значение, подходящее для скорости физического соединения, с использованием рекомендованных значений IEEE 802.1D.

«Приоритет» (<Priority>) — это число, кратное 16, в диапазоне от 0 до 240. Обратите внимание, что если значение не кратно 16, оно будет установлено в 0.

STP использует стоимость пути при выборе портов. Низкая стоимость пути предпочтительнее высокой стоимости пути. Если два порта имеют одинаковую стоимость, приоритет выбирается в качестве основы.

12 Коммутация защиты кольца Ethernet (ERPS)

Идентификатор ERPS

Идентификатор группы защиты должен находиться в диапазоне от 1 до 64. Максимально может быть создано 64 группы защиты ERPS. Нажмите на идентификатор группы защиты, чтобы перейти на страницу конфигурации.

Порт 0

Создать кольцо «порт 0».

Порт 1

Создать кольцо «порт 1».

Тип кольца

Тип защитного кольца. Может быть основным кольцом (main ring) или подкольцом (sub-ring).

Сигнализация

ERPS сообщает об аварийной ситуации.

Пример:

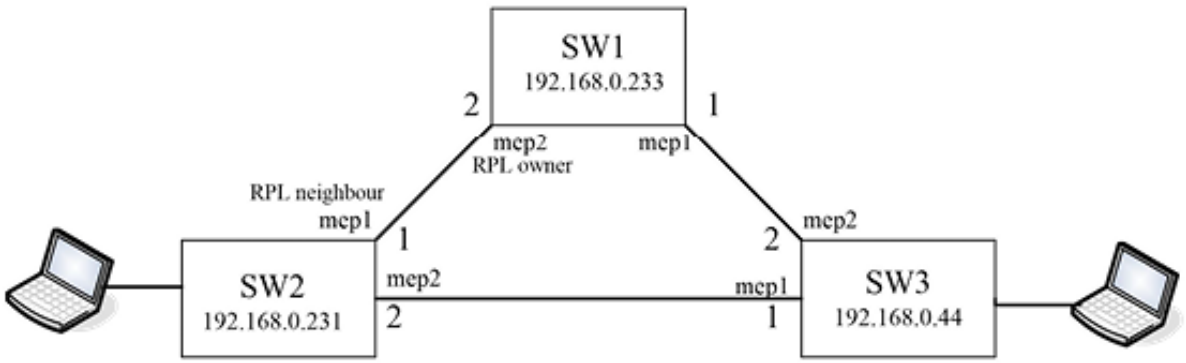


Рисунок 12-1: Топология сетевого подключения

1. Подключите Коммутатор 1 к Коммутатору 2, и Коммутатор 2 к Коммутатору 3. Сначала не подключайте Коммутатор 1 и Коммутатор 3, чтобы избежать петли.
2. Восстановите значения по умолчанию коммутаторов 1/2/3. Отключите DHCP-клиент и установите правильный статический IP-адрес для коммутаторов 1/2/3.

   В данном примере: коммутатор 1 — 192.168.0.233, коммутатор 2 — 192.168.0.231, коммутатор 3 — 192.168.0.44.
3. Отключите покрывающее дерево (которое включено по умолчанию) на коммутаторах 1/2/3, чтобы избежать конфликтов с ERPS.
4. Включите распознавание тегов VLAN на коммутаторах 1/2/3 (установите тип порта как «C-порты» на портах 1 и 2 трёх коммутаторов).
5. Настройка ERPS

5.1 Коммутатор 1, владелец RPL (RPL Owner)

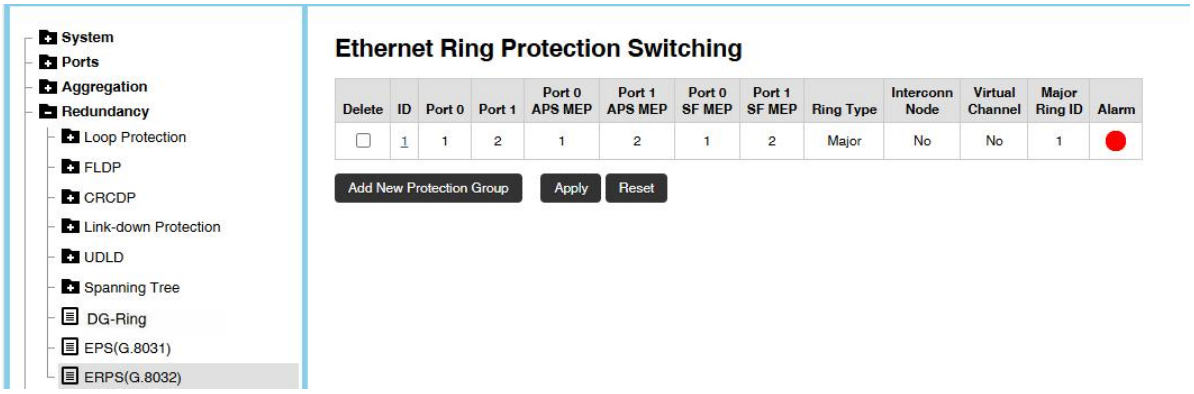


Рисунок 12-2: Добавление ERPS коммутатора 1

Редактирование ERPS (нажав на идентификатор ERPS в таблице ERPS 1):

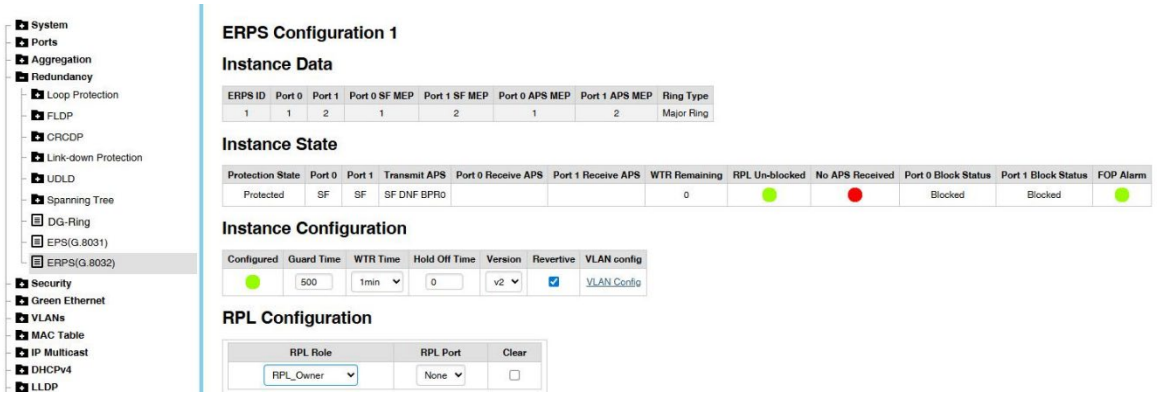


Рисунок 12-3: Редактирование ERPS

Редактирование защищённого VLAN:

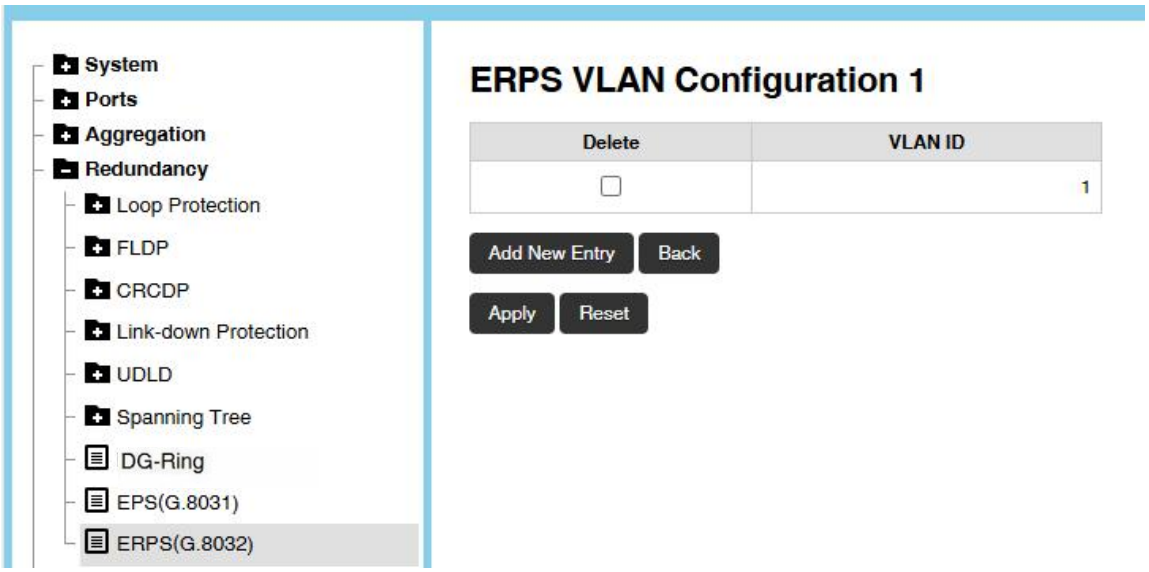


Рисунок 12-4: Защищённый VLAN

5.2 Коммутатор 2, сосед RPL (RPL neighbor)

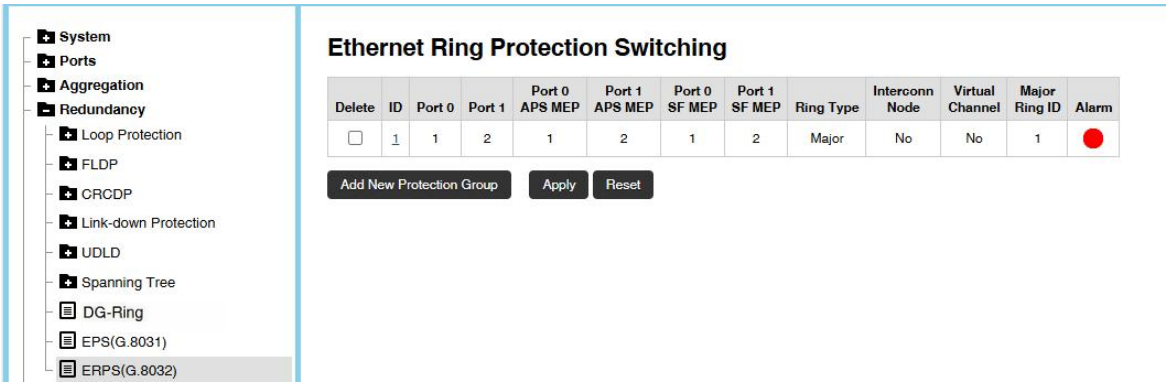


Рисунок 12-5: Добавление ERPS коммутатора 2

Редактирование ERPS1 (нажав на идентификатор ERPS в таблице ERPS 1):

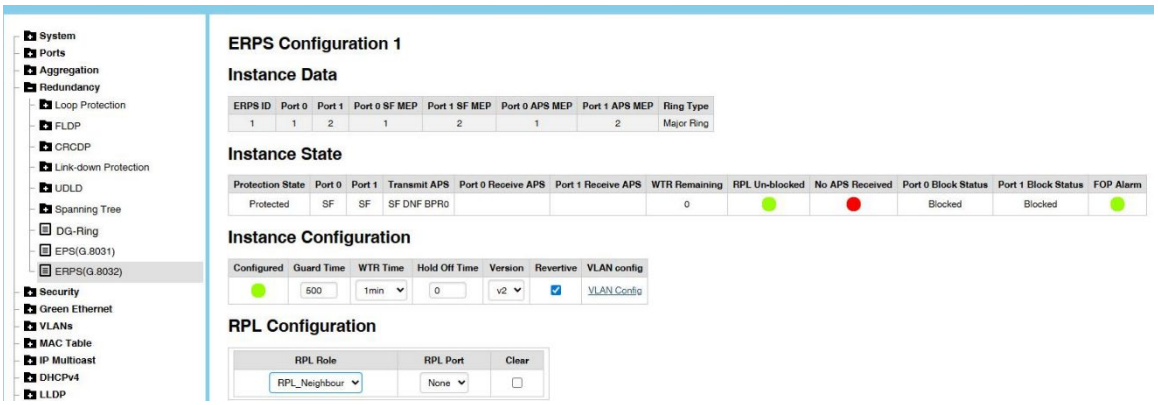


Рисунок 12-6: Редактирование ERPS

Нажмите «Конфигурация VLAN» на изображении выше для редактирования защищённого VLAN:

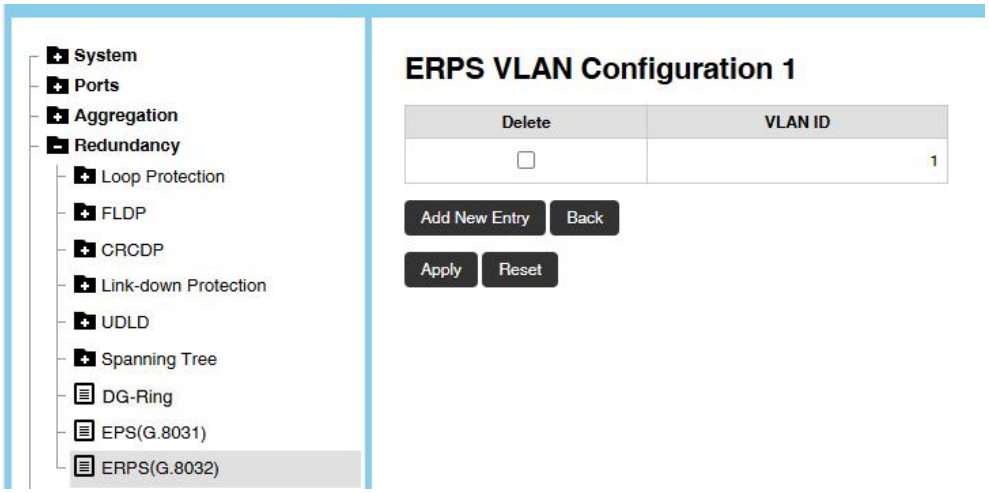


Рисунок 12-7: Защищённый VLAN

5.3 Коммутатор 3

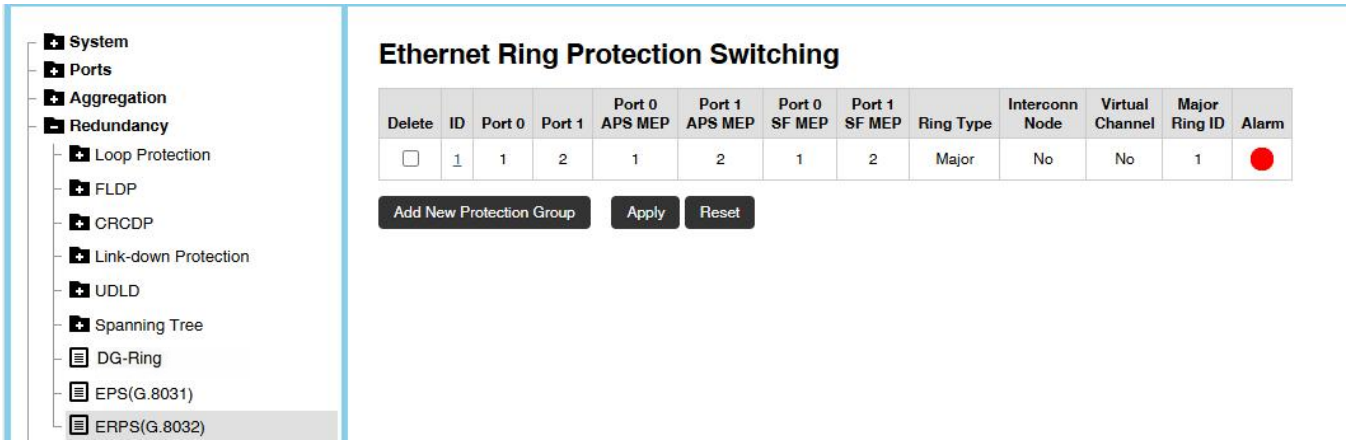


Рисунок 12-8: Добавление ERPS коммутатора 3

Редактирование ERPS1 (нажав на идентификатор ERPS в таблице ERPS 1):

Редактирование защищённого VLAN:

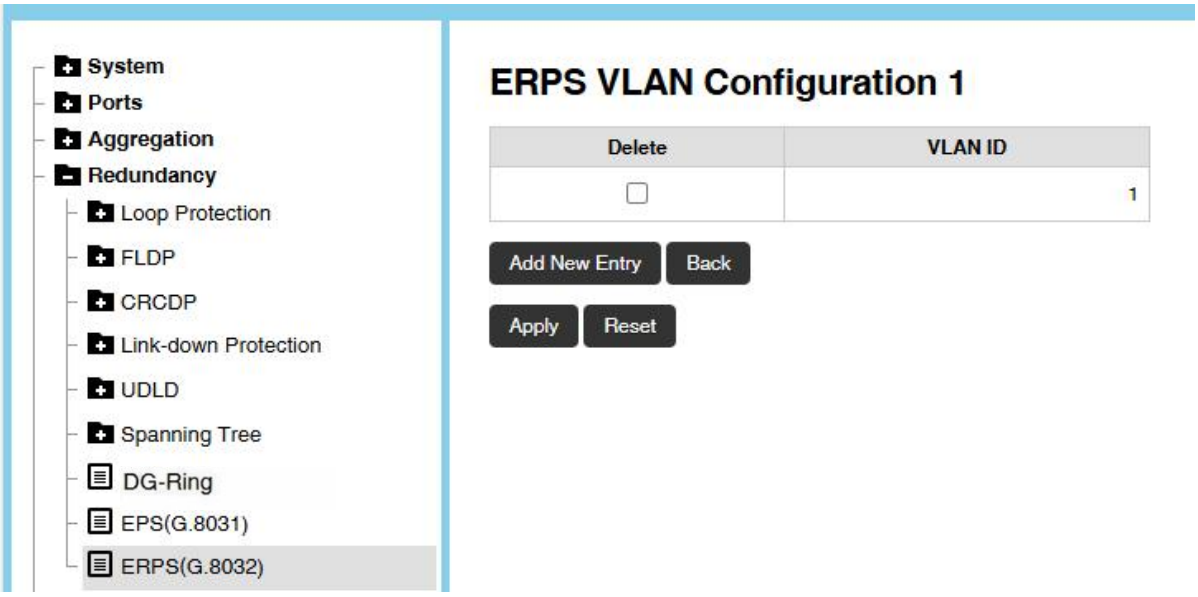


Рисунок 12-9: Защищённый VLAN

Подключите коммутаторы 1 и 3. Проверьте, нормально ли работает MEP трёх устройств.

Коммутатор 1:

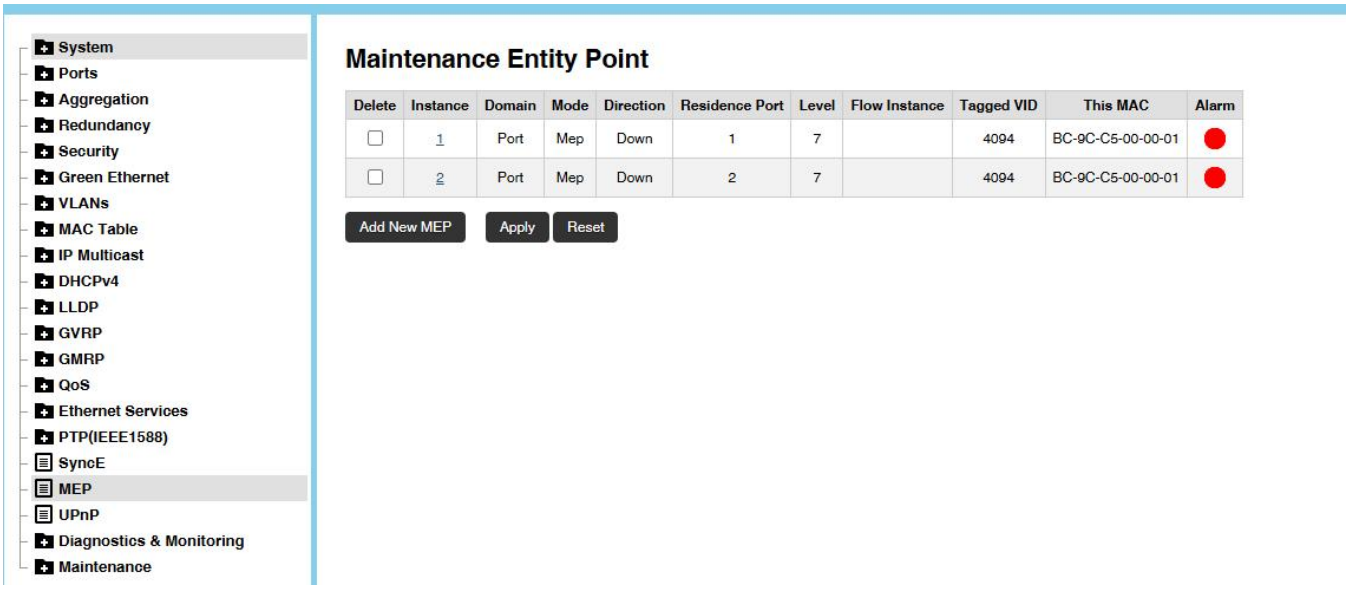


Рисунок 12-10: MEP коммутатора 1

Коммутатор 2:

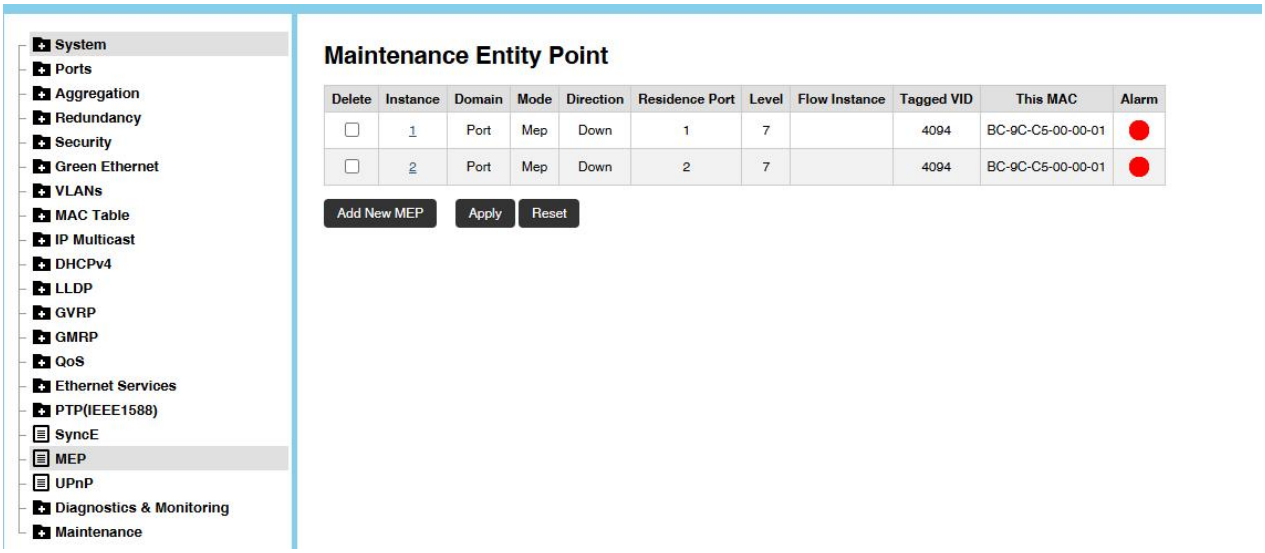


Рисунок 12-11: MEP коммутатора 2

Коммутатор 3:

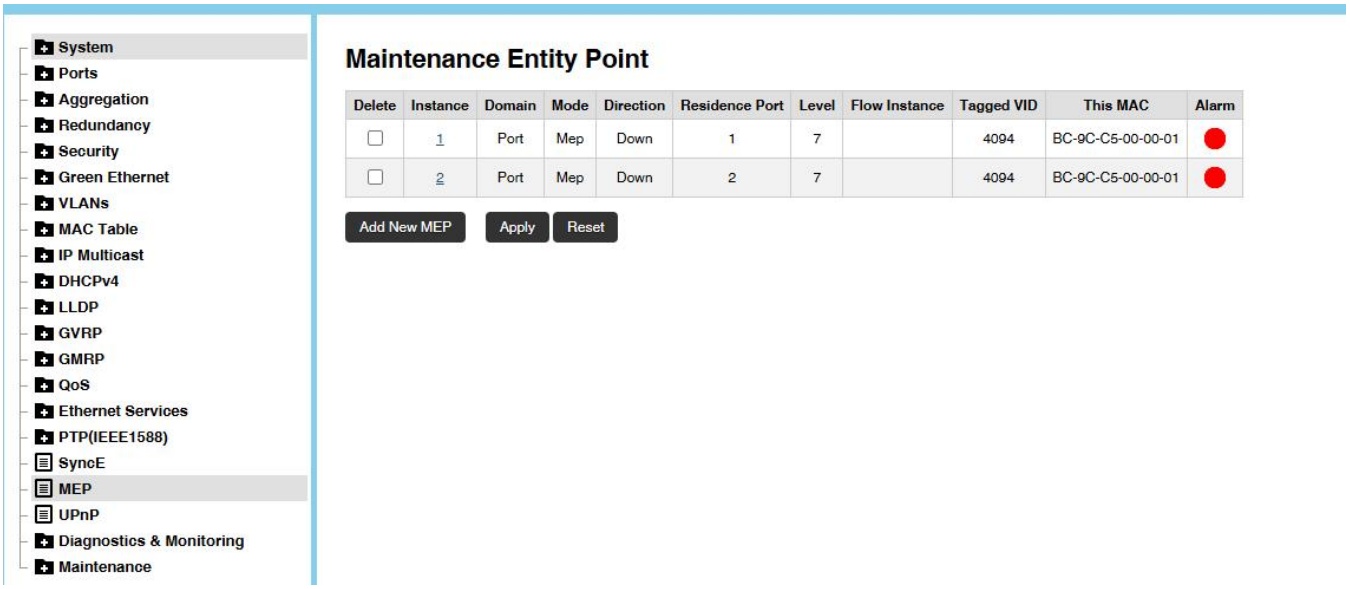


Рисунок 12-12: MEP коммутатора 3

13 PTP (1588) и SyncE

13.1 Режим Ord-Bound

Режим Ord-Bound определяет отношения «ведущий-ведомый» между устройствами через режим самосогласования и в конечном итоге решает, от какого устройства синхронизировать свою информацию о времени.

А) Нажмите «Добавить новый часовой механизм PTP»:

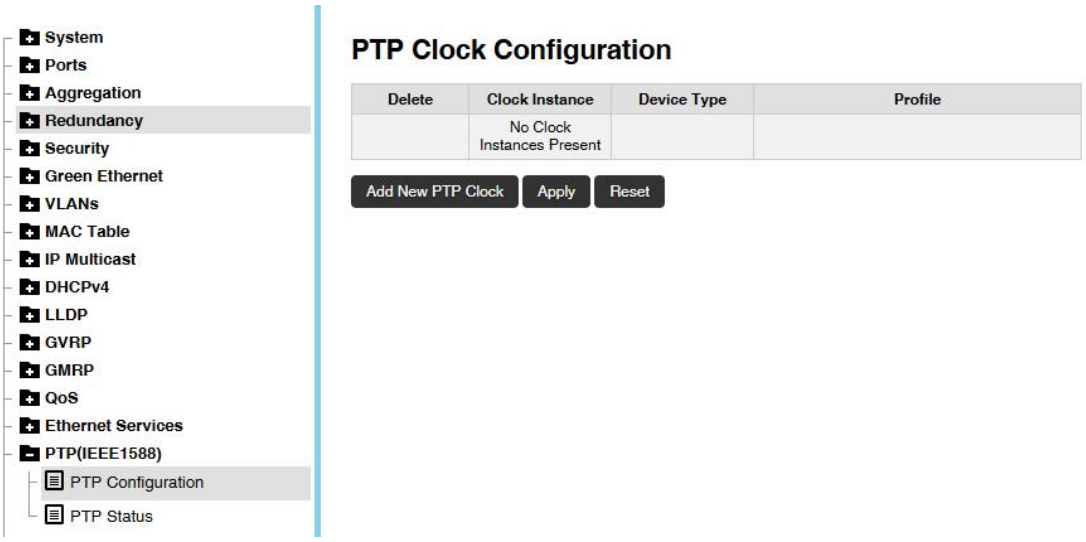


Рисунок 13-1: Создание часов

б) Выберите режим Ord-Bound:

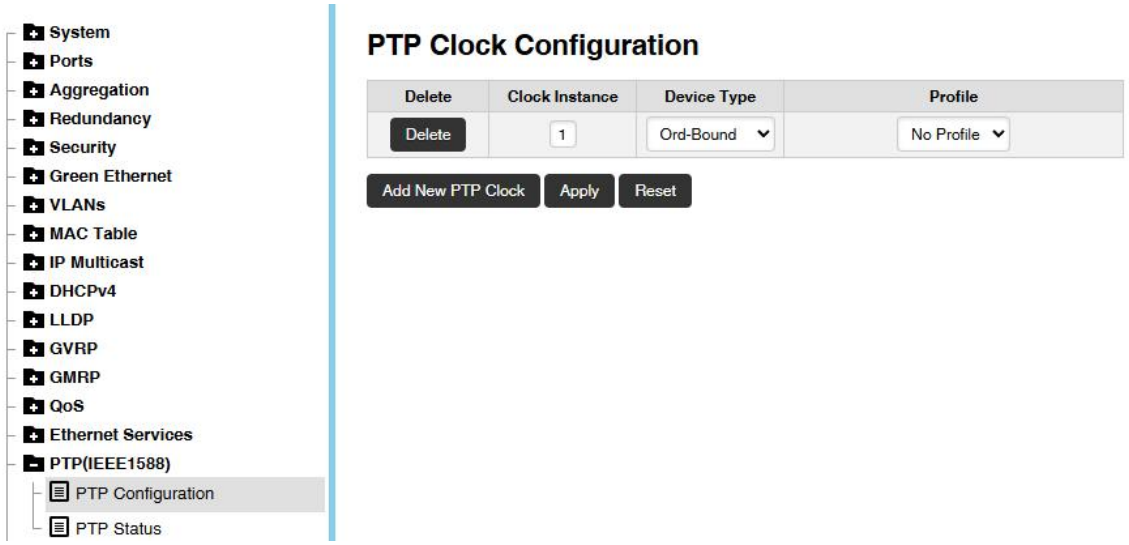


Рисунок 13-2: Выбор режима часов

Экземпляр часов: диапазон ввода от 0 до 3.

Тип часов: Ord-Bound.

Конфигурационный файл: по умолчанию выбирается «No Profile». После конфигурации нажмите «Сохранить» и применить.

13.2 Включение порта

а) Нажмите «0» в настроенном выше экземпляре часов, чтобы перейти к следующему шагу:

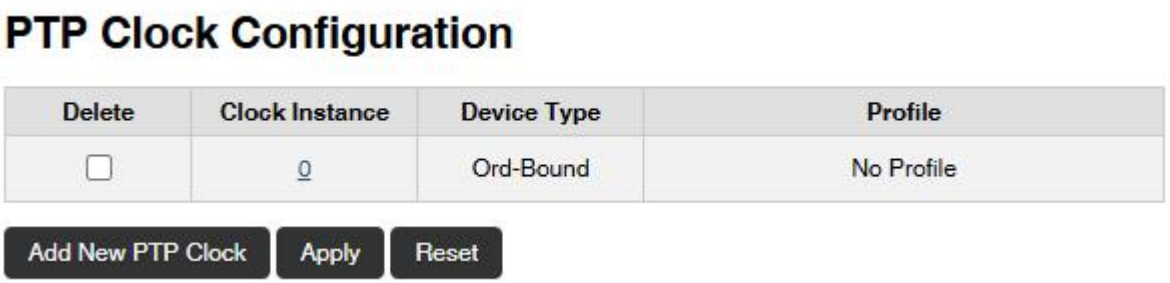


Рисунок 13-3: Включение порта

б) Включите порт (установите флажок напротив порта в поле «Порт включён и настроен», остальные конфигурации оставьте по умолчанию):

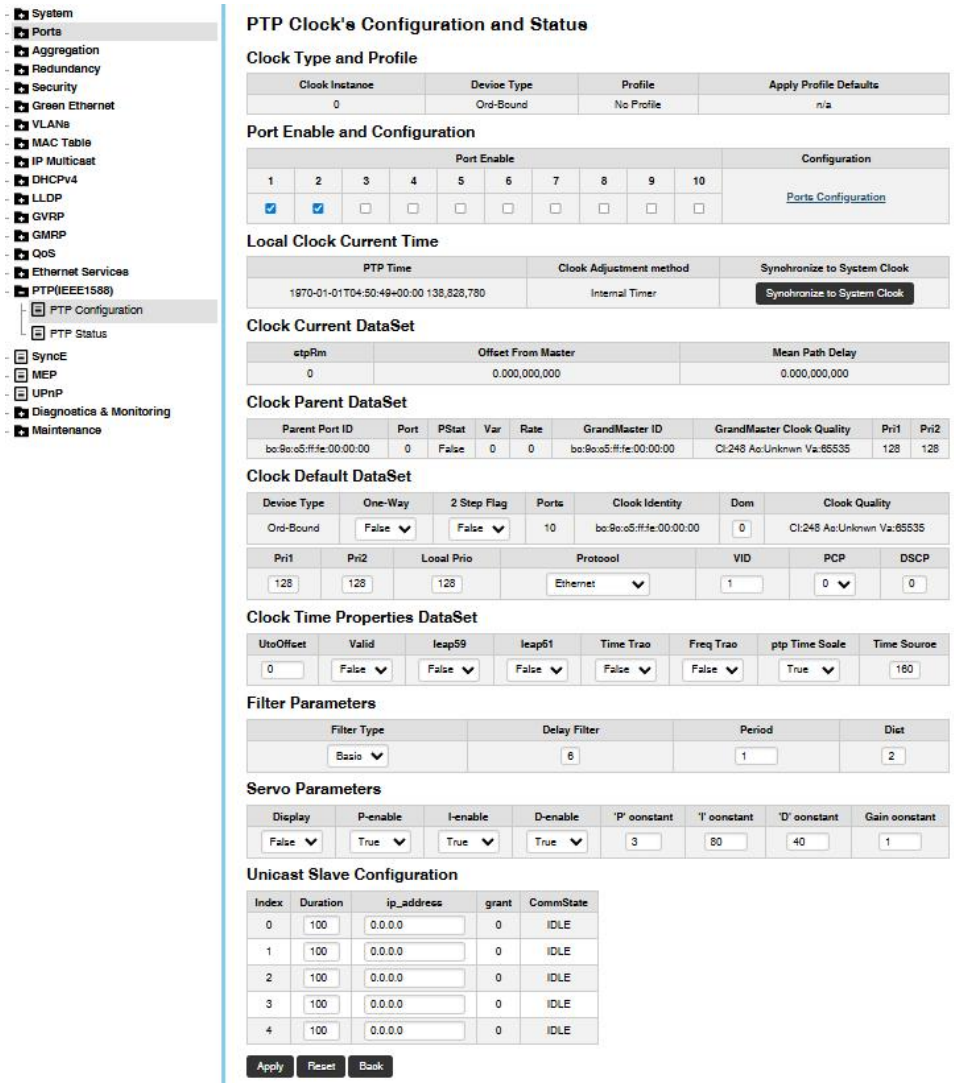


Рисунок 13-4: Включение порта

После конфигурации нажмите «Применить».

Примечание: После конфигурации, показанной на рисунках выше, коммутаторы будут автоматически согласовывать выбор ведущих или ведомых часов. Ведущие часы используются как эталон времени, а ведомые часы синхронизируются с ведущими часами.

в) Войдите в конфигурацию порта:

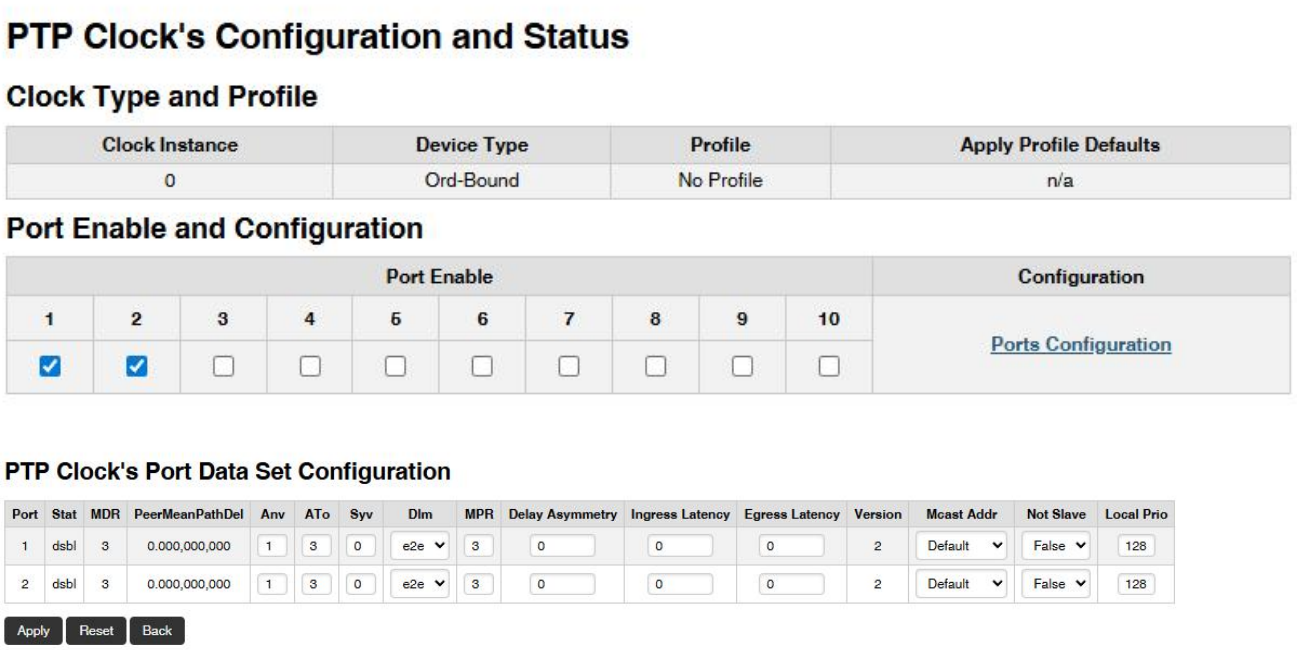


Рисунок 13-5: Конфигурация порта

Пояснение конфигурации:

Интервал отправки уведомлений (Announce sending interval): во ведущем состоянии временной интервал для публикации уведомительных сообщений, диапазон значений от -3 до 4.

Таймаут уведомлений (Announce timeout): время ожидания приёма уведомительного сообщения. Диапазон значений от 1 до 10.

Интервал отправки синхронизации (Sync send interval): временной интервал между синхронизирующими сообщениями, публикуемыми во ведущем состоянии, диапазон значений от -7 до 4.

В этом режиме все конфигурации на странице установлены по умолчанию.

13.3 Режим TC (Transparent Clock)

Режим TC: в этом режиме цель синхронизации часов может быть достигнута без прямого подключения между устройствами.

а) Нажмите «Новый часовой механизм PTP»:

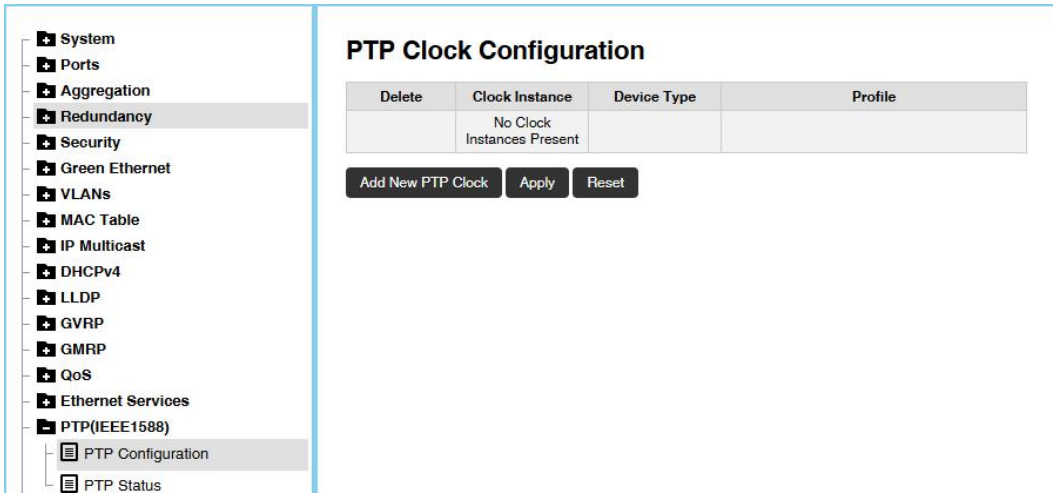


Рисунок 13-6: Создание часов

б) Выберите режим P2PTransp, нажмите «Применить», сохраните конфигурацию:

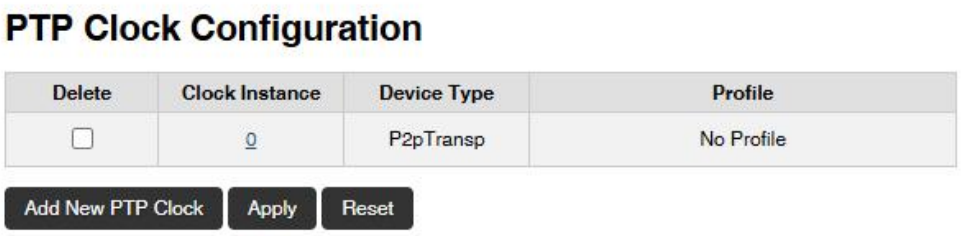


Рисунок 13-7: Выбор режима

в) Нажмите на экземпляр часов «0», установите флажок для включения порта, нажмите «Применить», сохраните конфигурацию:

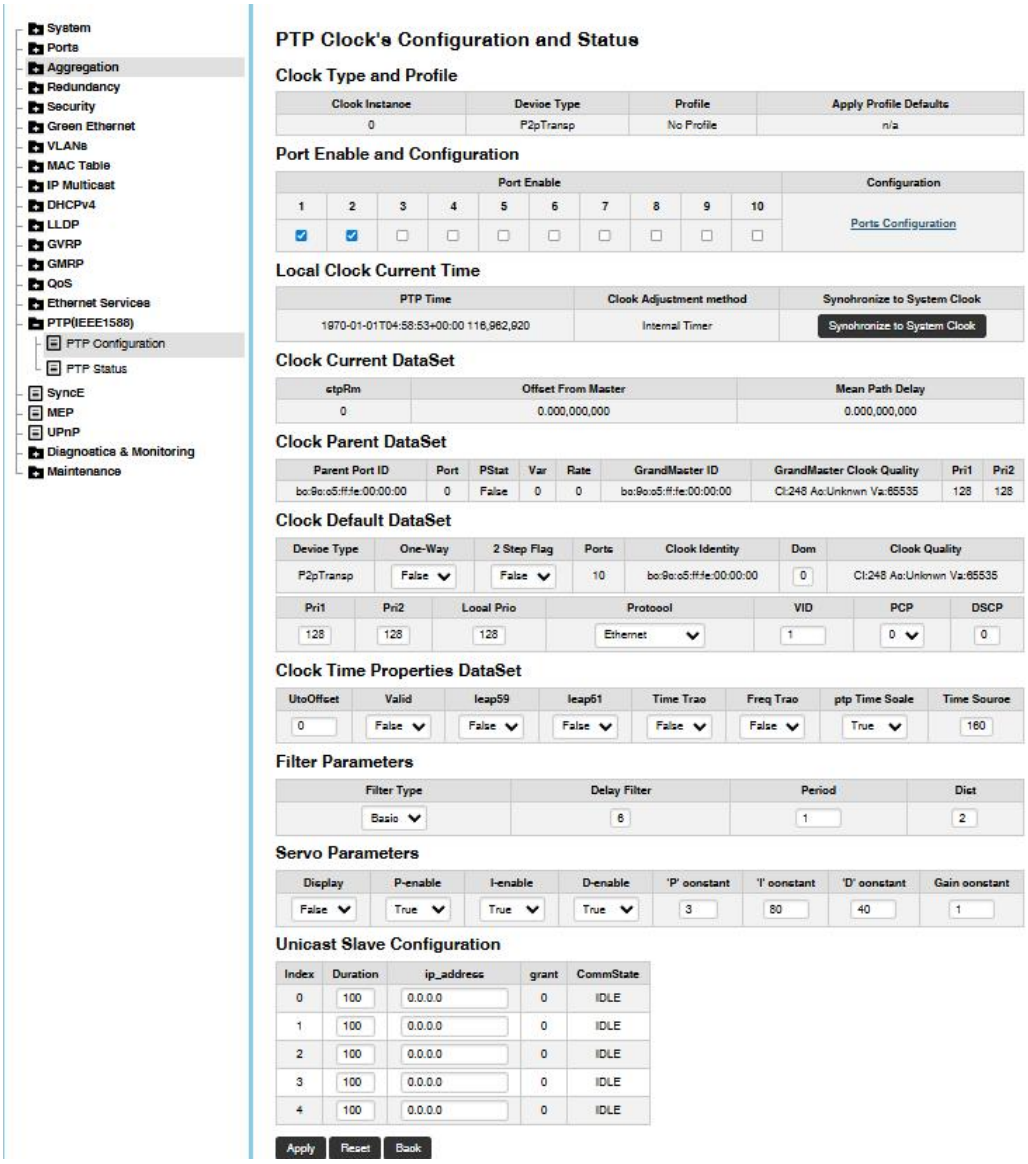


Рисунок 13-8: Включение порта

В этом режиме узел TC пересылает все кадры PTP с одного порта на другой порт и обновляет поле коррекции в кадре PTP для достижения прозрачной передачи.

13.4 Режимы «Ведомый» и «Ведущий»

Пояснение схемы:

Режим ведомого (Slave mode, пассивный режим): процесс синхронизации часов порта является пассивным, и информация о времени зависит от порта в режиме ведущего (Master).

Режим ведущего (Master mode, активный режим): коммутатор, принудительно переведённый в режим ведомого или согласовавший переход в режим ведомого, должен синхронизироваться со временем коммутатора в режиме ведущего.

Процесс конфигурации такой же, как в режиме Ord-Bound, с единственным отличием — выбором типа устройства.

Рисунок 13-9: Режим ведомого

Рисунок 13-10: Режим ведущего

13.5 Режим BC-frontend

Режим BC-frontend: в этом режиме может быть достигнута синхронизация часов между различными VLAN.

A) Нажмите «Новый часовой механизм PTP»:

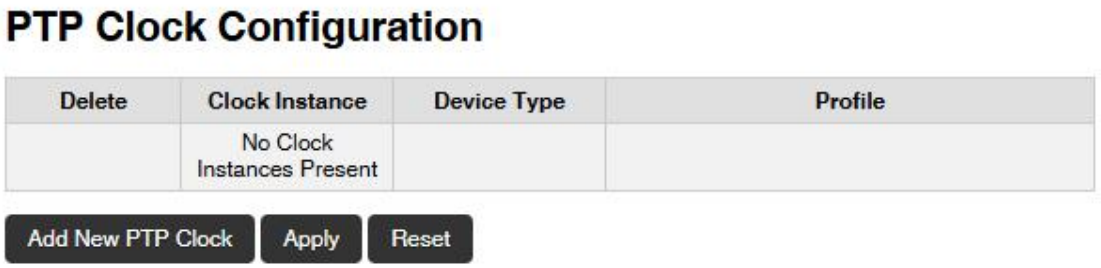


Рисунок 13-11: Создание синхронизирующих часов

б) Выберите режим BC-frontend:

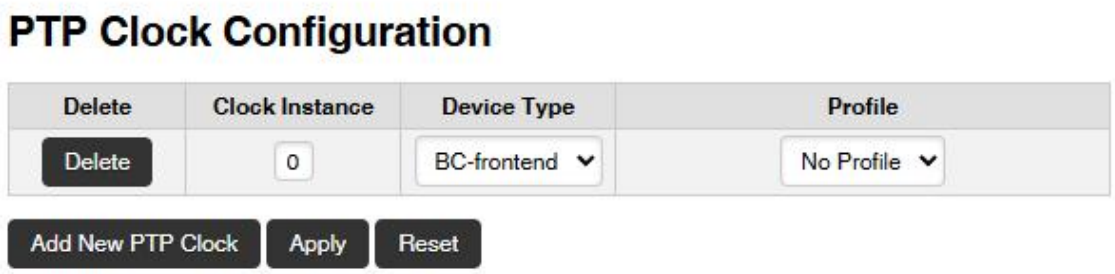


Рисунок 13-12: Выбор режима BC-frontend

в) Выберите порт тем же методом.

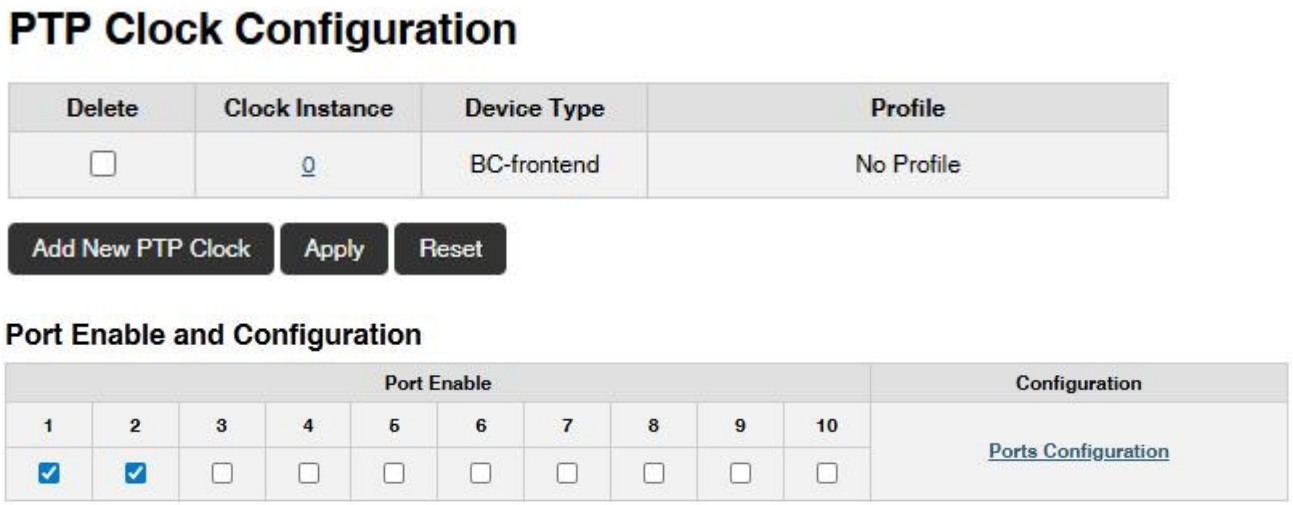
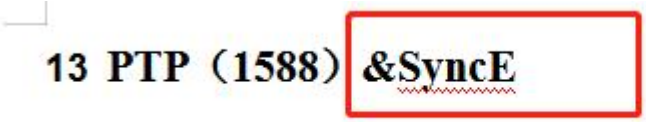


Рисунок 13-13: PTP Clock Configuration

1.SyncE



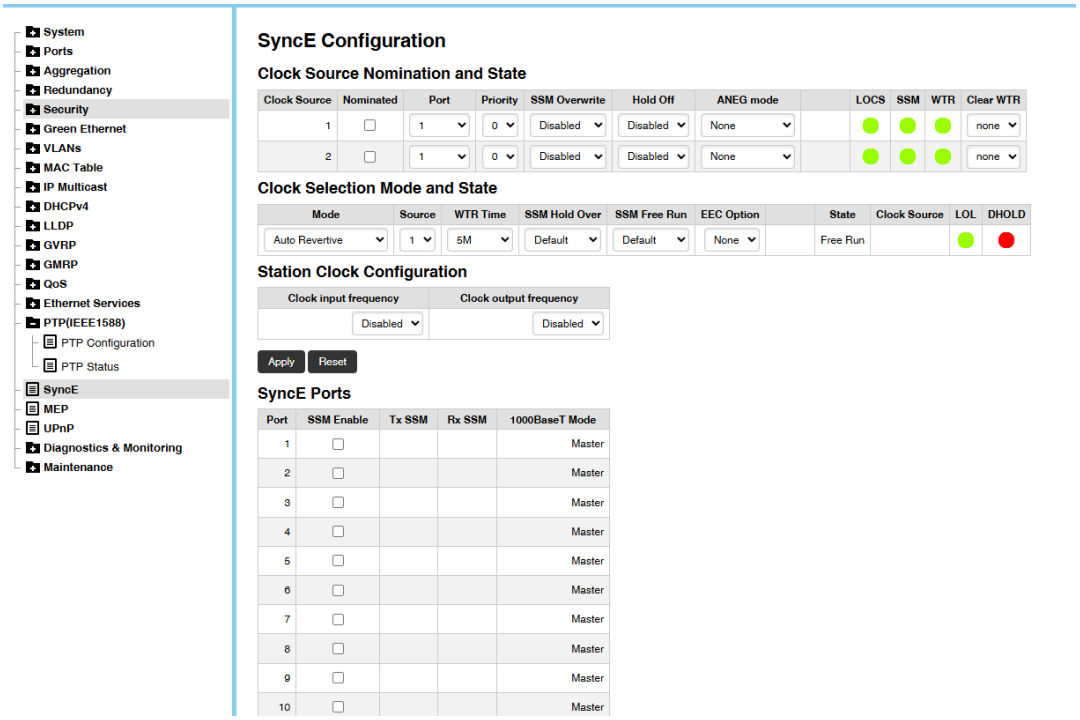


Рисунок 13-14: SyncE конфигурация

14 MRP

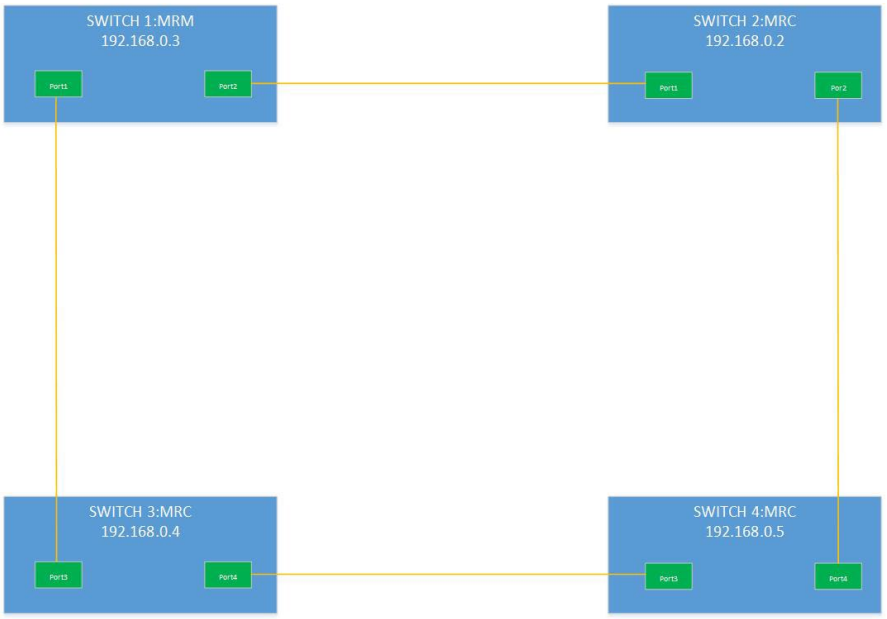


Рисунок 14-1: MRP

Сконфигурируйте устройство с IP-адресом 192.168.0.3 в качестве менеджера медиарезервирования (Media Redundancy Manager, MRM) в режиме менеджера.

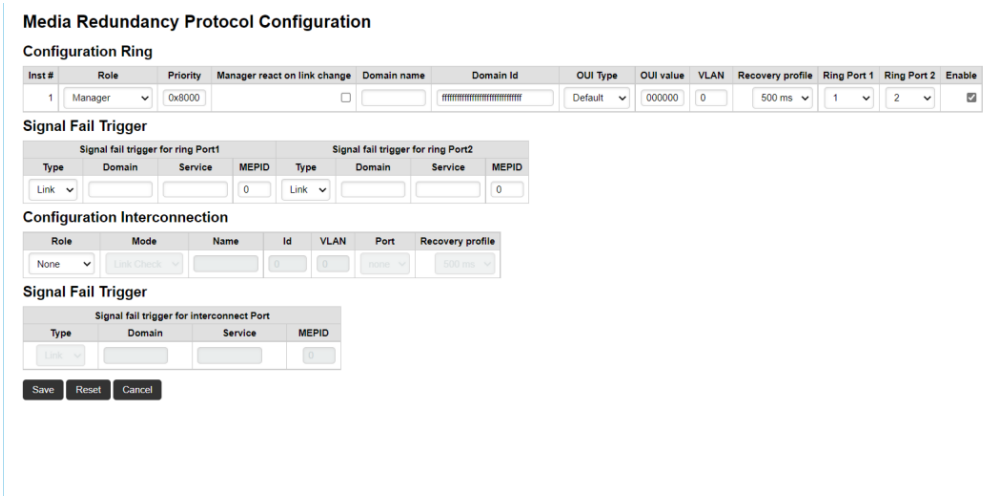


Рисунок 14-2: MRP конфигурация

```
media-redundancy 1
 role mrm
 port1 interface GigabitEthernet 1/1
 port2 interface GigabitEthernet 1/2
 mrm priority 0x8000
 admin-state enable
!
```

Рисунок 14-3: Роль MRM

Сконфигурируйте устройство с IP-адресом 192.168.0.2 в качестве клиента медиарезервирования (Media Redundancy Client, MRC) в режиме клиента.

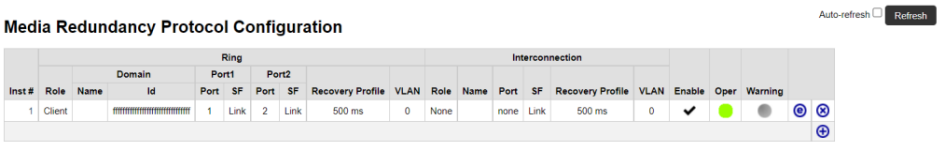


Рисунок 14-4: Конфигурация в качестве клиента

```
media-redundancy 1
 role mrc
 port1 interface GigabitEthernet 1/1
 port2 interface GigabitEthernet 1/2
 admin-state enable
!
```

Рисунок 14-5: Конфигурация в качестве клиента

Сконфигурируйте устройство с IP-адресом 192.168.0.4 в качестве клиента медиарезервирования (Media Redundancy Client, MRC) в режиме клиента.

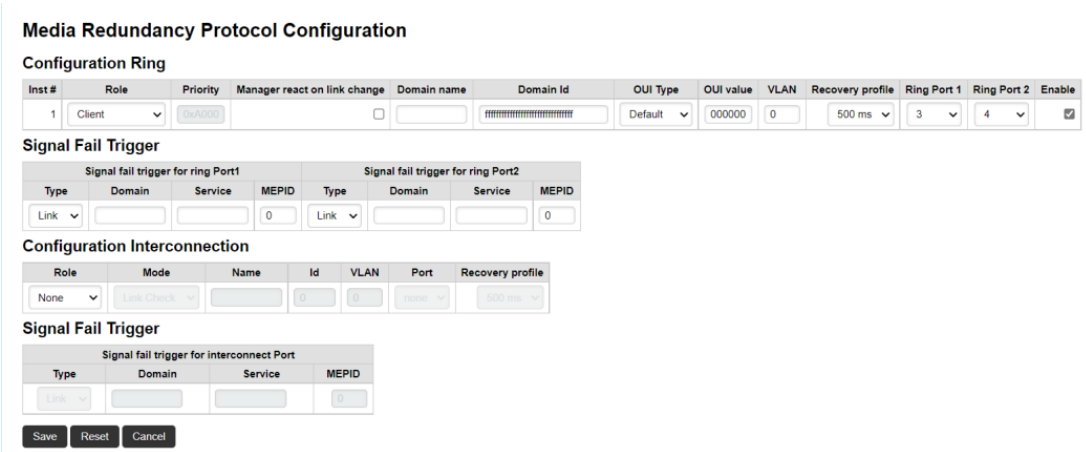


Рисунок 14-6: Конфигурация в качестве клиента

```
media-redundancy 1
 role mrc
 port1 interface GigabitEthernet 1/3
 port2 interface GigabitEthernet 1/4
 admin-state enable
!
```

Рисунок 14-7

Сконфигурируйте устройство с IP-адресом 192.168.0.5 в качестве клиента медиарезервирования (Media Redundancy Client, MRC) в клиентском режиме.

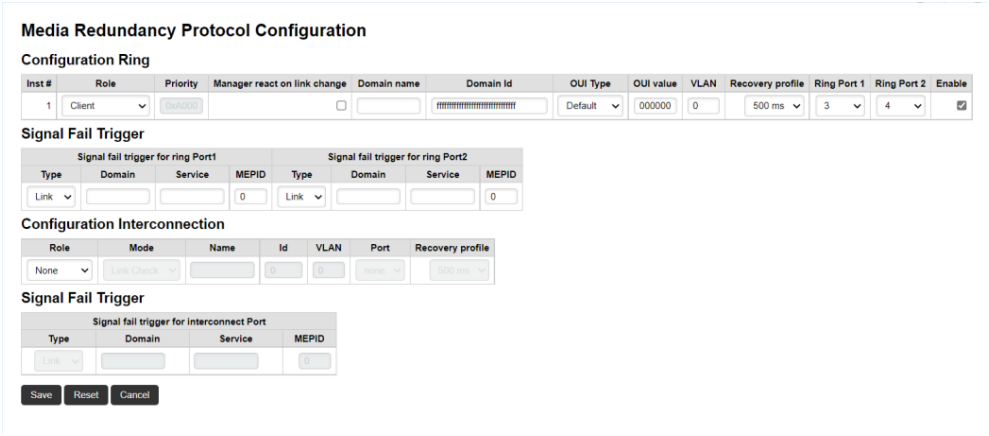


Рисунок 14-8: Конфигурация в качестве клиента медиарезервирования

```
media-redundancy 1
 role mrc
 port1 interface GigabitEthernet 1/3
 port2 interface GigabitEthernet 1/4
 admin-state enable
!
```

Рисунок 14-9: Статус MRP

Конфигурации MIM/MIC

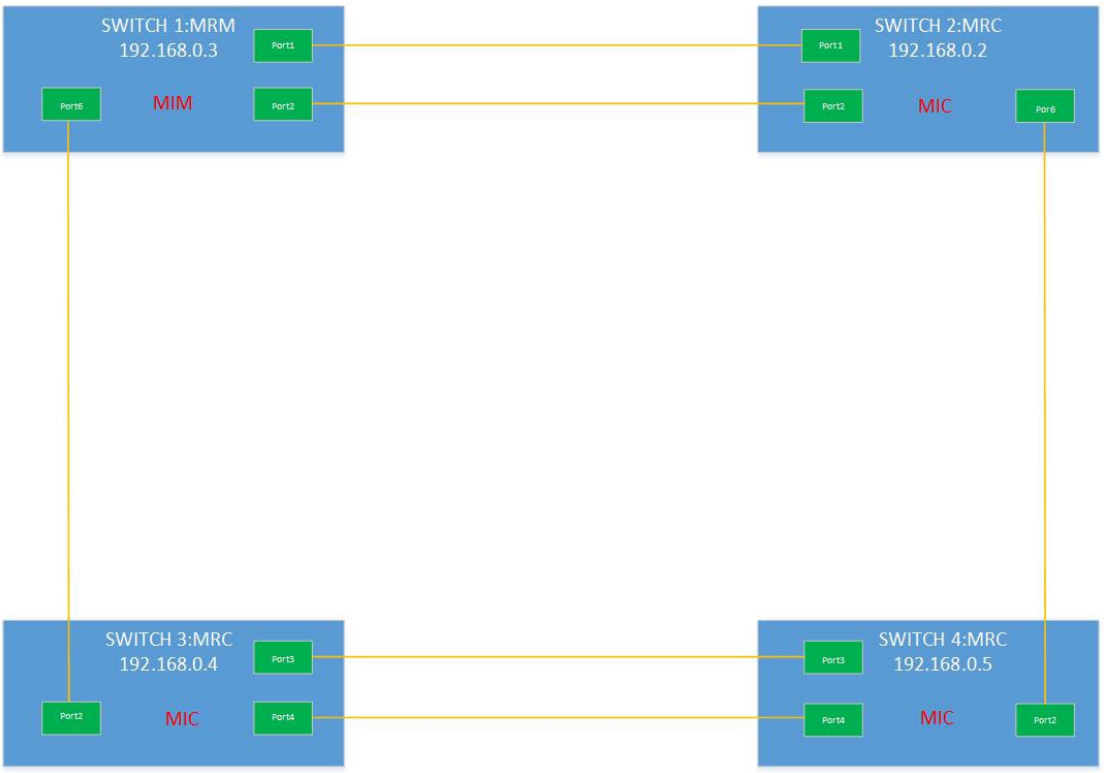


Рисунок 14-10: Конфигурации MIM/MIC

Сконфигурируйте устройство с IP-адресом 192.168.0.3 в качестве менеджера межкольцевого резервирования (Media Redundancy Interconnection Manager, MIM).

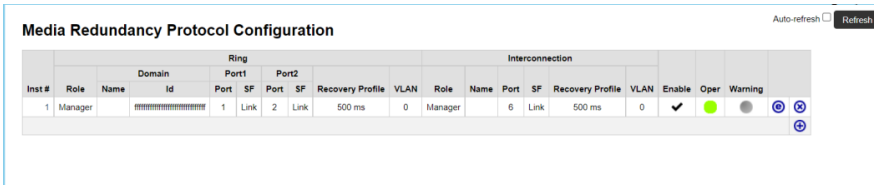


Рисунок 14-11: Страница MIM

Рисунок 14-12: Статус MRP

```
interface vlan 1
 ip address 192.168.0.3 255.255.255.0
!
media-redundancy 1
 role mrm
 port1 interface GigabitEthernet 1/1
 port2 interface GigabitEthernet 1/2
 mrm priority 0x8000
 interconnection role mim
 interconnection id 2
 interconnection interface FastEthernet 1/2
 admin-state enable
!
spanning-tree aggregation
 spanning-tree link-type point-to-point
```

Рисунок 14-13: Статус MRP

Сконфигурируйте устройство с IP-адресом 192.168.0.2 в качестве клиента межкольцевого резервирования (Media Redundancy Interconnection Client, MIC).

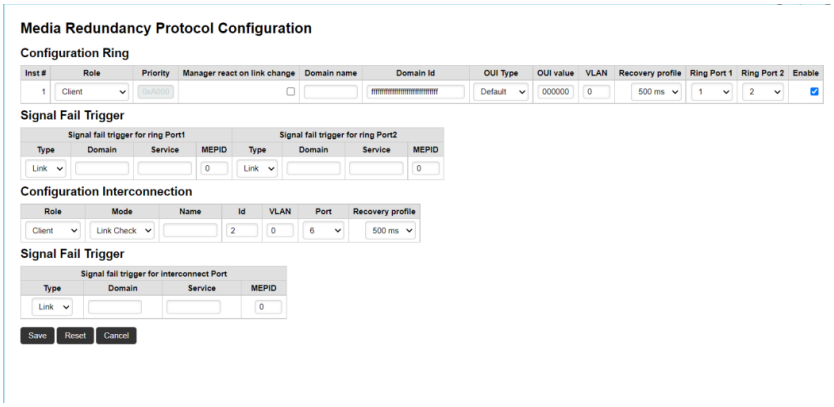


Рисунок 14-14: Страница конфигурации MRP

Рисунок 14-15: Статус MRP

```
interface vlan 1
 ip address 192.168.0.2 255.255.255.0
!
media-redundancy 1
 role mrc
 port1 interface GigabitEthernet 1/1
 port2 interface GigabitEthernet 1/2
 interconnection role mic
 interconnection id 2
 interconnection interface FastEthernet 1/2
 admin-state enable
!
```

Рисунок 14-16: Статус MRP

Сконфигурируйте устройство с IP-адресом 192.168.0.4 в качестве клиента межкольцевого резервирования (Media Redundancy Interconnection Client, MIC).

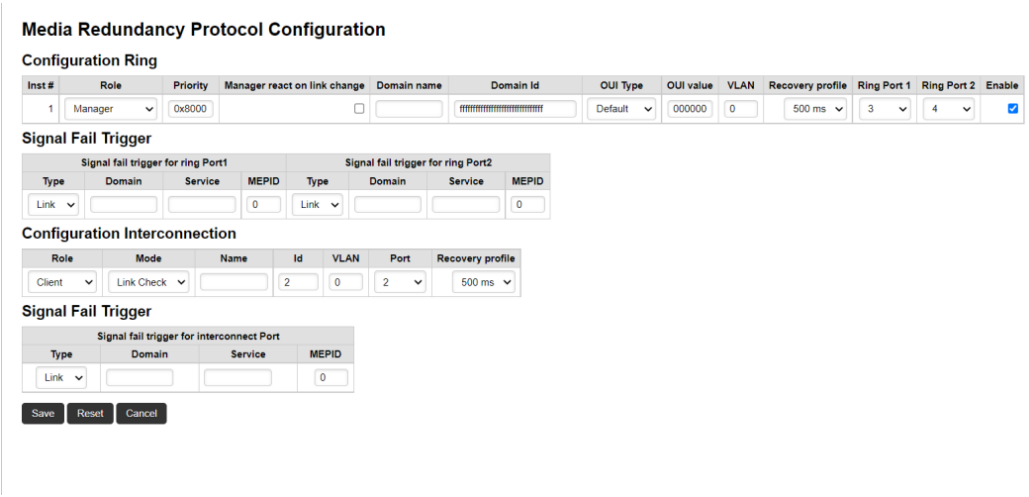


Рисунок 14-17: Страница конфигурации MRP

Рисунок 14-18: Статус MRP

```
interface vlan 1
 ip address 192.168.0.4 255.255.255.0
!
media-redundancy 1
 role mrm
 port1 interface GigabitEthernet 1/3
 port2 interface GigabitEthernet 1/4
 mrm priority 0x8000
 interconnection role mic
 interconnection id 2
 interconnection interface GigabitEthernet 1/2
 admin-state enable
```

Рисунок 14-19: Статус MRP

Сконфигурируйте устройство с IP-адресом 192.168.0.5 в качестве клиента межкольцевого резервирования (Media Redundancy Interconnection Client, MIC).

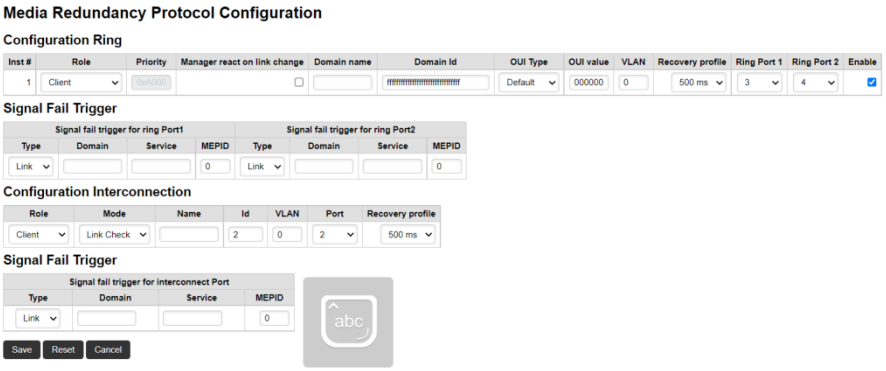


Рисунок 14-20: Страница конфигурации MRP

Рисунок 14-21: Статус MRP

```
interface vlan 1
 ip address 192.168.0.5 255.255.255.0
!
media-redundancy 1
 role mrc
 port1 interface GigabitEthernet 1/3
 port2 interface GigabitEthernet 1/4
 interconnection role mic
 interconnection id 2
 interconnection interface GigabitEthernet 1/2
 admin-state enable
```

Рисунок 14-22: Статус MRP

15 DG-ring

15.1 Концептуальная архитектура

Протокол DG-Ring — это протокол канального уровня, специально разработанный для кольцевых топологий Ethernet. При целостном кольце он предотвращает возникновение широковещательных штормов, вызванных петлями передачи данных. При обрыве линка связи в кольце протокол обеспечивает высокоскоростное восстановление соединения между узлами за счёт минимального времени сходимости.

Для организации защиты используется решение на базе протокола распределённой избыточности (Distributed Redundancy Protocol, DRP) с поддержкой автоматической выборы мастер-узла, запретом обратного переключения (non-rollback) и быстрой локализацией отказов.

Сеть на базе DG-Ring организует коммутаторы в узлы с фиксированными ролями. Узлы обмениваются служебными пакетами для постоянного мониторинга состояния кольца и распространения обновлений топологии, протокол DG-Ring развернут в сети. Ниже приведены базовые концепции протокола с опорой на данную схему.

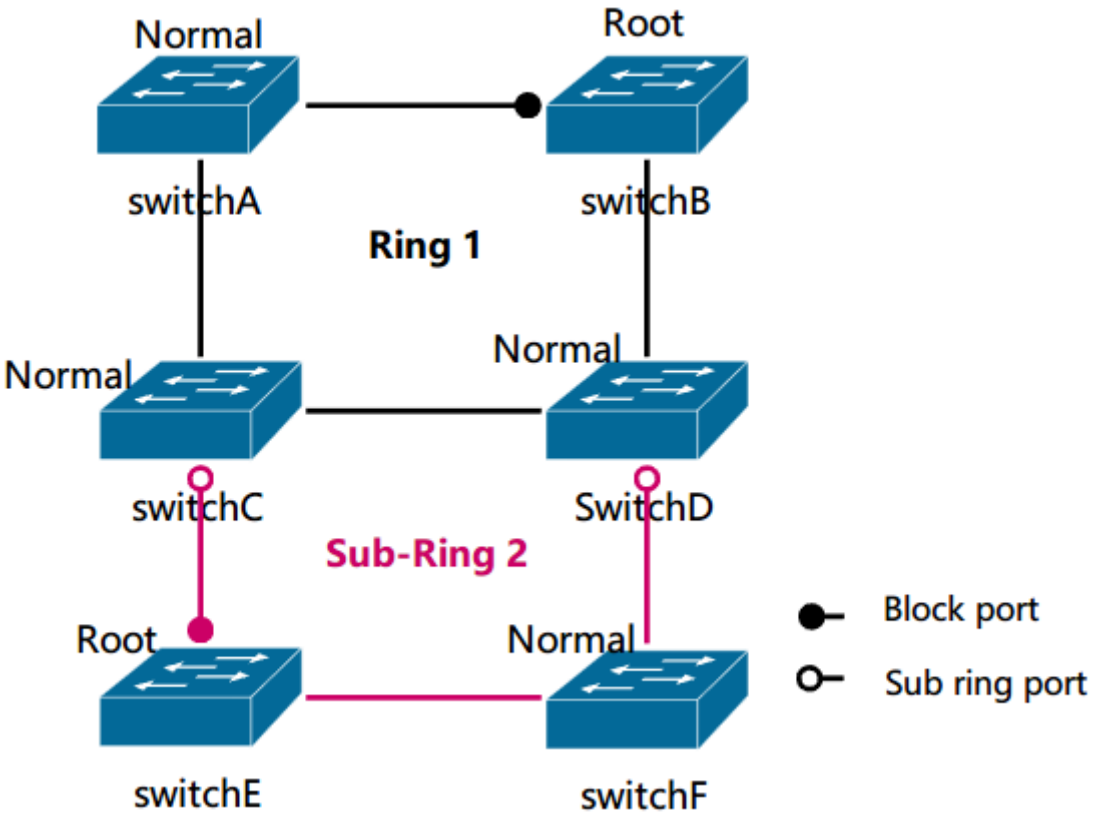


Рисунок 15-1: Схема принципа работы DG-Ring.

Кольцо DG-Ring является базовой функциональной единицей протокола DG-Ring и состоит из сетевых устройств, соединённых через сконфигурированные кольцевые порты. Кольцо включает основное (primary) и вторичное (secondary) кольца: основное кольцо образует замкнутый контур, вторичное — разомкнутый.

Принадлежность портов к основному или вторичному кольцу задаётся администратором. На рис. 15-1 основное кольцо образовано коммутаторами A, B, C и D, вторичное — коммутаторами C, E, F и D.

Функция вложенного кольца (Sub-Ring) поддерживается только в версии DG-Ring v2; в DG-Ring v1 недоступна.

Узел (Node)

Сетевые устройства, входящие в кольцо DG-Ring, называются узлами. Каждый узел может использовать до двух портов (исключая резервные) в рамках одного кольца. На рис. 15-1 коммутаторы A–D являются узлами основного кольца.

Идентификатор кольца (Ring ID)

Все узлы одного кольца должны иметь одинаковый идентификатор кольца (Ring ID).

Тип кольца (Ring Type)

Протокол DG-Ring поддерживает следующие типы:

- Ring — стандартное кольцо с возможностью настройки резервного порта.

- Sub-Ring — вложенное кольцо. Для соединения основного и вложенного колец допускается использовать только один порт, называемый портом вложенного кольца (sub-ring port).

- Dual-Homing — механизм двойного подключения с двумя портами на одном устройстве, работающими в режиме взаимного резервирования. При отказе одного линка трафик автоматически переключается на резервный.

- Hybrid-Ring — гибридное кольцо. Используется для интеграции устройств с разными кольцевыми протоколами в единую кольцевую топологию.

Роль узла (Node Role)

Узел в кольце может находиться в одной из четырёх ролей:

- INIT — начальное состояние коммутатора после включения или перезагрузки.

- ROOT — корневой узел. В кольце присутствует единственный корневой узел, избираемый автоматически всеми узлами. При изменении топологии состав узлов может меняться. Только один порт корневого узла находится в состоянии пересылки (forwarding).

- ROOT-B — резервный корневой узел. При обрыве линка узлы на обоих концах повреждённого участка избираются в роли ROOT и ROOT-B для ускоренного восстановления.

- NORMAL — обычный узел. Оба порта находятся в состоянии пересылки трафика.

Состояние кольца (Ring State)

Отражает топологическое состояние кольца:

- Ring-Close — кольцо замкнуто (петля заблокирована для предотвращения штормов).

- Ring-Open — кольцо разомкнуто (например, при отказе линка или в процессе восстановления).

Состояние порта (Port Status)

Кольцевой порт может находиться в трёх состояниях:

- Blocked — порт принимает и передаёт служебные пакеты протокола DG-Ring, но блокирует пользовательский трафик.

- Unblocked — порт принимает и пересылает все типы пакетов.

- Down — порт находится в состоянии физического отказа (Link Down).

15.2 Базовый принцип работы DG-Ring

Протокол DG-Ring — стандартный кольцевой протокол канального уровня Ethernet, базовой функциональной единицей которого является кольцо DG-Ring. В данной главе на примерах рассматриваются принципы реализации протокола, включая вложенные кольца (Sub-Ring), резервные порты (Backup), двойное подключение (Dual-Homing) и гибридные кольца (Hybrid-Ring).

15.2.1 Механизм восстановления при отказе канала

Для предотвращения образования петель в кольцевой сети активируется протокол DG-Ring (конфигурация см. рис. 15-2). Протокол блокирует один из портов корневого узла (Root) и периодически передаёт служебные пакеты для мониторинга состояния сети. Как показано на рис. 15-2, корневой узел блокирует один порт, в то время как остальные порты продолжают пересылку трафика в штатном режиме.
Все узлы в кольце (контуре) должны иметь одинаковый ID. Допускается только один Главный узел, остальные — обычные.

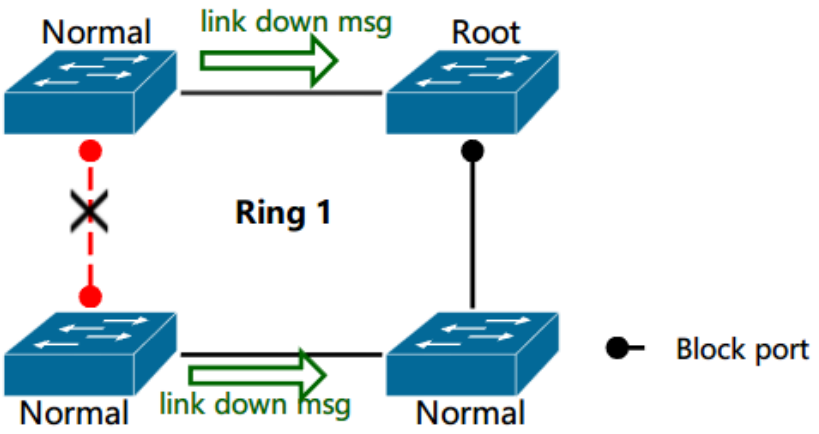


Рисунок 15-2: Схема восстановления связи при повреждении линии в кольцевой топологии DG-Ring.

При обрыве линка слева в топологии (см. схему) протокол DG-Ring блокирует порты на обоих концах повреждённого участка и мгновенно активирует заблокированный порт корневого узла, восстанавливая сквозную пересылку трафика без прерывания сервиса. Процедура восстановления:

- Два узла, обнаружившие обрыв линка, блокируют соответствующий порт, обновляют записи таблицы адресов (FDB) и рассылают уведомление об обрыве линка.
- Остальные узлы, получившие уведомление, ретранслируют его по кольцу и обновляют собственные записи FDB.
- Корневой узел, получив уведомление, разблокирует ранее заблокированный порт и обновляет таблицу адресов.

15.2.2 Резервный порт (Backup)

Резервный порт обеспечивает взаимосвязь между двумя кольцами (или с кольцами сторонних производителей, а также с одиночными устройствами), как показано на рис. 15-3 и 15-4. В штатном режиме два резервных порта в пределах одного кольца работают в асимметричном режиме: один находится в состоянии пересылки (forwarding), второй — в состоянии блокировки (blocking). При отказе линка порт, находившийся в состоянии блокировки, мгновенно активируется, обеспечивая бесперебойную передачу трафика.

В пределах одного кольца узел может иметь только один резервный порт, а общее число резервных портов в кольце не должно превышать двух. При объединении двух колец достаточно сконфигурировать резервные порты только на одном из колец.

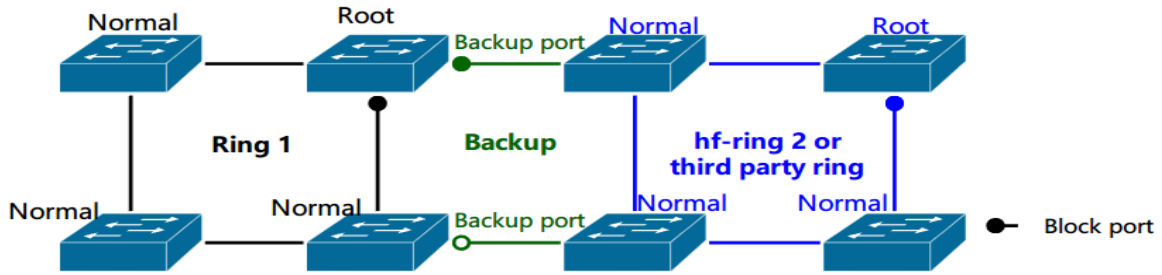


Рисунок 15-3 Схема топологии резервного межкольцевого соединения

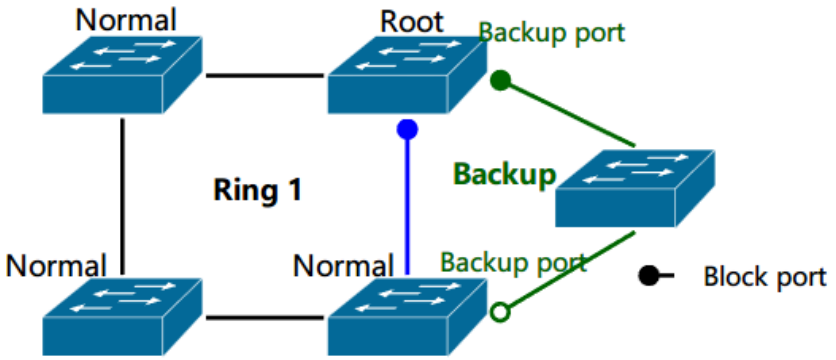


Рисунок 15-4: Схема топологии взаимного резервирования между кольцевой сетью и устройством.

15.2.3 Функция вложенного кольца (Sub-Ring)

Вложенные кольца позволяют формировать сложные топологии, включая пересекающиеся кольца, что обеспечивает гибкость при построении крупных сетей. На рис. 15-5 показан пример: кольцо 2 является вложенным относительно кольца 1.

Вложенное кольцо представляет собой цепочку устройств с двумя концевыми портами (порты вложенного кольца). Промежуточные узлы функционируют как обычные узлы кольца. Все узлы в пределах одного вложенного кольца должны иметь одинаковый идентификатор (Ring ID).

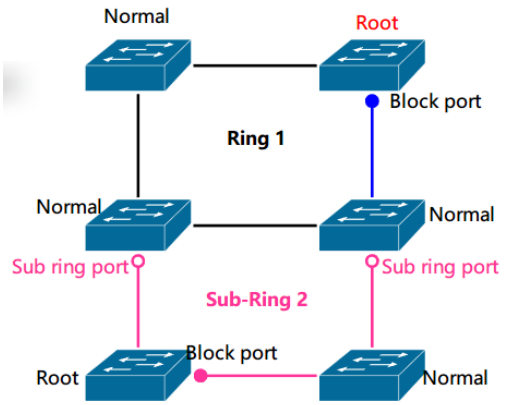


Рисунок 15-5: Схема топологии subring в сети DG-Ring

15.2.4 Двойное подключение (Dual-Homing)

Топология Dual-Homing позволяет одиночному устройству подключаться к сети через два независимых линка, повышая отказоустойчивость. Два порта на одном устройстве работают в режиме взаимного резервирования: при отказе основного линка трафик мгновенно переключается на резервный. В промышленных сетях кольцевая топология является основным решением для избыточности, однако конечные устройства часто подключаются по одному линку. Dual-Homing устраняет это ограничение, обеспечивая двойную избыточность на уровне отдельного устройства.

Конфигурация Dual-Homing возможна только на одном коммутаторе. Сетевая сторона подключения может представлять собой кольцо, цепочку, произвольную топологию, два независимых устройства или даже один и тот же коммутатор.

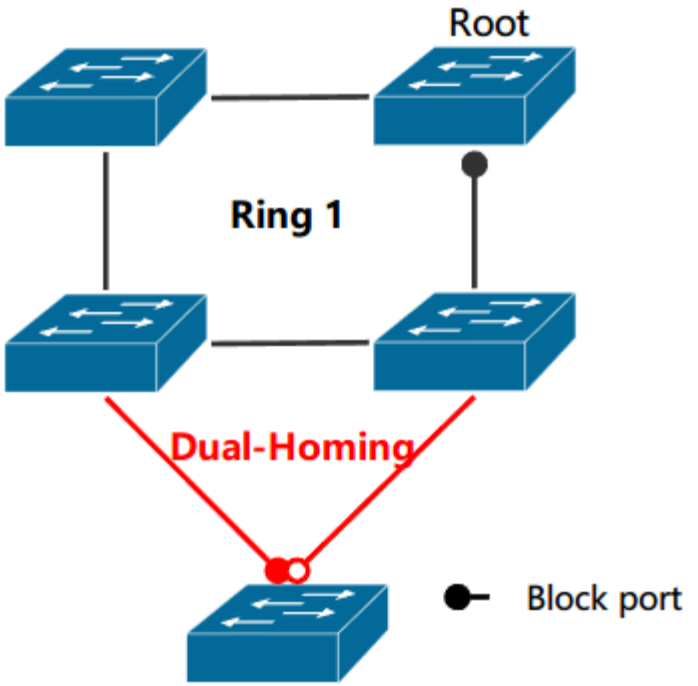


Рисунок 15-6: Схема топологии DG-Ring с двумя ведущими устройствами и резервированием линий связи.

15.2.5 Гибридное кольцо (Hybrid-Ring)

Архитектура гибридного кольца обеспечивает прозрачную интеграцию с сетями сторонних производителей для формирования единой кольцевой топологии. Режим Hybrid-Ring специально оптимизирован для гетерогенных сред и обеспечивает сверхбыстрое восстановление. На рис. 15-7 показано: четыре устройства нижнего уровня образуют кольцо совместно с сетью стороннего производителя. При обрыве линка в сторонней сети корневой узел мгновенно обнаруживает отказ, активирует заблокированный порт и обновляет записи FDB на всех узлах Hybrid-Ring, обеспечивая восстановление менее чем за 20 мс.

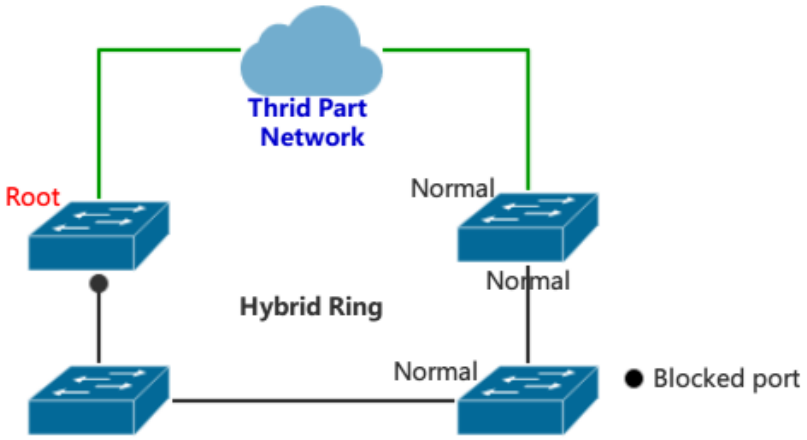


Рисунок 15-7: Схема подключения и настройки Hybrid-Ring.

Стандартный режим Ring также поддерживает интеграцию со сторонними сетями, однако время восстановления при отказе линка составляет секунды. Режим Hybrid-Ring обеспечивает восстановление менее 20 мс.

Конфигурирование

Пользователь может сначала разделить сеть на несколько колец DG-Ring в соответствии с требованиями топологии, а затем определить тип каждого кольца.

15.3 Версии DG-Ring

По умолчанию устанавливайте версию протокола DG-Ring v2. При построении кольца с устройствами, не поддерживающими v2, выбирайте версию v1 (выпадающий список выбора версии → «Сохранить»).

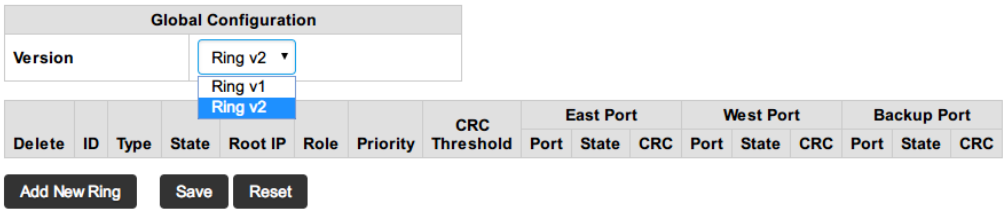


Рисунок 15-8: Страница выбора версии DG-Ring.

Версии DG-Ring v1 и v2 несовместимы. Все узлы одного кольца обязаны использовать одинаковую версию. При изменении версии убедитесь, что экземпляр кольца не содержит сконфигурированных портов.

15.4 Обнаружение кольца

Выберите тип кольца Ring, назначьте восточный (East) и западный (West) порты, при необходимости настройте резервный порт (Backup) и нажмите «Сохранить».

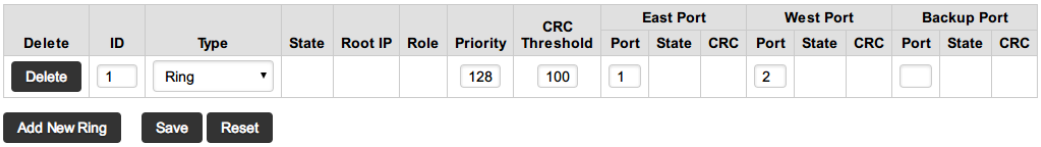


Рисунок 15-9: Создание кольца DG-Ring

Перед созданием кольца убедитесь, что выбранные порты не участвуют в других протоколах избыточности (STP, RSTP и др.) и не входят в состав агрегированных групп (LAG).

Один физический порт может принадлежать только одному кольцу.

15.5 Создание вложенного кольца

Выберите тип Sub-Ring, сконфигурируйте порт (порт подкольца) и нажмите «Сохранить».

Delete	ID	Type	State	Root IP	Role	Priority	CRC Threshold	East Port			West Port			Backup Port		
								Port	State	CRC	Port	State	CRC	Port	State	CRC
Delete	1	Sub-Ring				128	100	1								

Add New Ring Save Reset

Рисунок 15-10: Создание кольца DG-Ring

Вложенное кольцо имеет только один кольцевой порт для подключения к основному кольцу.

15.6 Настройка двойного подключения

Выберите режим Dual-Homing, назначьте порты и сохраните конфигурацию (см. рис. 15-11).

Delete	ID	Type	State	Root IP	Role	Priority	CRC Threshold	East Port			West Port			Backup Port		
								Port	State	CRC	Port	State	CRC	Port	State	CRC
Delete	1	Dual-Homing				128	100	1			2					

Add New Ring Save Reset

Рисунок 15-11: Топология двойного подключения использует ровно два порта на одном устройстве; резервные порты (Backup) в данном режиме не применяются.

15.7 Настройка гибридного кольца

Выберите тип Hybrid-Ring, назначьте восточный и западный порты, при необходимости настройте резервные порты и сохраните конфигурацию (см. рис. 15-12).

Delete	ID	Type	State	Root IP	Role	Priority	CRC Threshold	East Port			West Port			Backup Port		
								Port	State	CRC	Port	State	CRC	Port	State	CRC
Delete	1	Hybrid-Ring				128	100	1			2					

Add New Ring Save Reset

Рисунок 15-12: Конфигурирование гибридного и стандартного колец выполняется одинаково.

15.8 Проверка состояния DG-Ring

На странице статуса (см. рис. 15-6) отображаются: текущее состояние кольца (открыто/закрыто), IP-адрес корневого узла (Root), статус кольцевых портов (Blocked/Unblocked/Down), идентификатор кольца (Ring ID), версия протокола.

Global Configuration	
Version	Ring v2

Delete	ID	Type	State	Root IP	Role	Priority	CRC Threshold	East Port			West Port			Backup Port		
								Port	State	CRC	Port	State	CRC	Port	State	CRC
	1	Ring	-	192.168.0.233	NORMAL	128	100	3	Unblocked	0	4	Unblocked	0			
	2	Sub-Ring	Ring-Open	0.0.0.0	ROOT	128	100	1	Unblocked	0						
	3	Dual-Homing	-	-	-	128	100	5	Down	0	6	Down	0			
	4	Hybrid-Ring	-	0.0.0.0	INIT	128	100	7	Down	0	8	Down	0			

Add New Ring Save Reset

Рисунок 15-13: Страница состояния кольца DG

15.9 Типовые сетевые применения

Типовые сценарии применения протокола DG-Ring охватывают следующие сетевые топологии: одиночное кольцо, многокольцевые структуры (пересекающиеся кольца, касательные соединения и др.).

15.9.1 Одиночное кольцо

Как показано на Рисунке 15-14, сетевая топология представляет собой одиночное кольцо

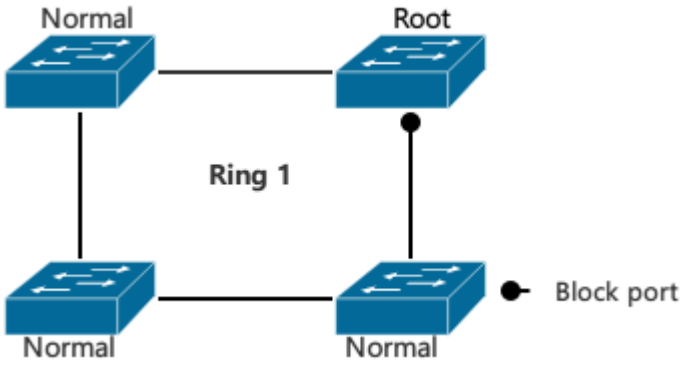


Рисунок 15-14: Схема сети с одиночным кольцом DG-Ring

Одиночное кольцо поддерживается как в версии DG-Ring v1, так и в версии DG-Ring v2.

15.9.2 Сеть с касающимися кольцами

Как показано на Рисунке 15-2, если сетевая топология содержит два или более колец, соединённых ровно одним общим узлом, для каждого кольца необходимо определить отдельный экземпляр протокола DG-Ring.

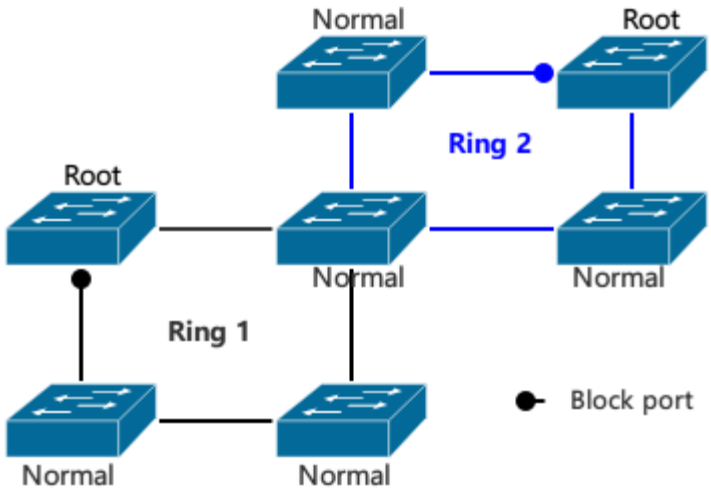


Рисунок 15-15: Схема сети с касательными кольцами DG-Ring

Касательные кольца поддерживаются как в версии DG-Ring v1, так и в версии DG-Ring v2.

15.9.3 Сеть с пересекающимися кольцами

Если топология содержит два или более колец с двумя общими узлами между каждой парой колец, необходимо определить одно основное кольцо DG-Ring и одно или несколько субколец (Sub-Ring). Как показано на Рисунке 15-16, одно основное кольцо напрямую соединено с двумя субкольцами.

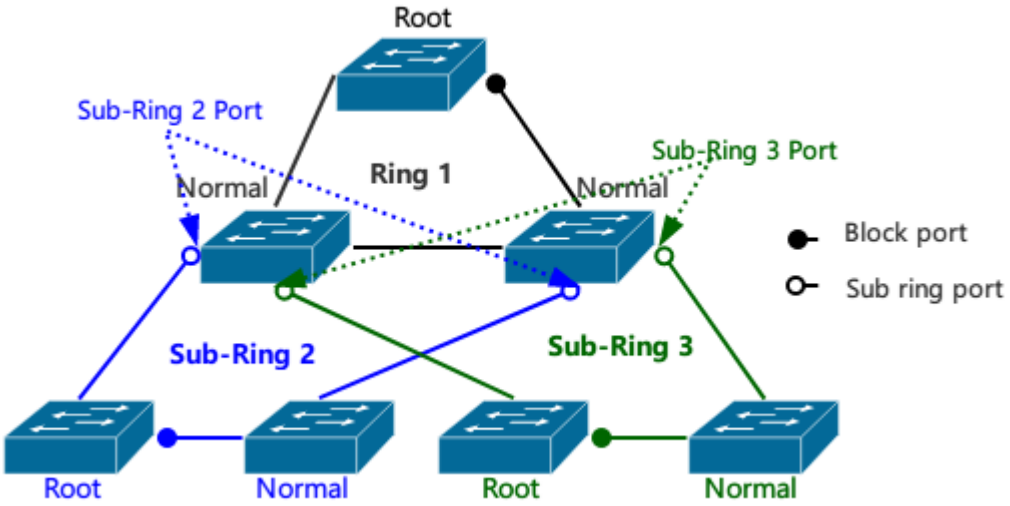


Рисунок 15-16: Схема сети с пересекающимися кольцами DG-Ring (вариант 1)

Субкольца также могут образовывать иерархическую структуру. Как показано на Рисунке 15-16, субкольцо 3 является вложенным относительно субкольца 2.

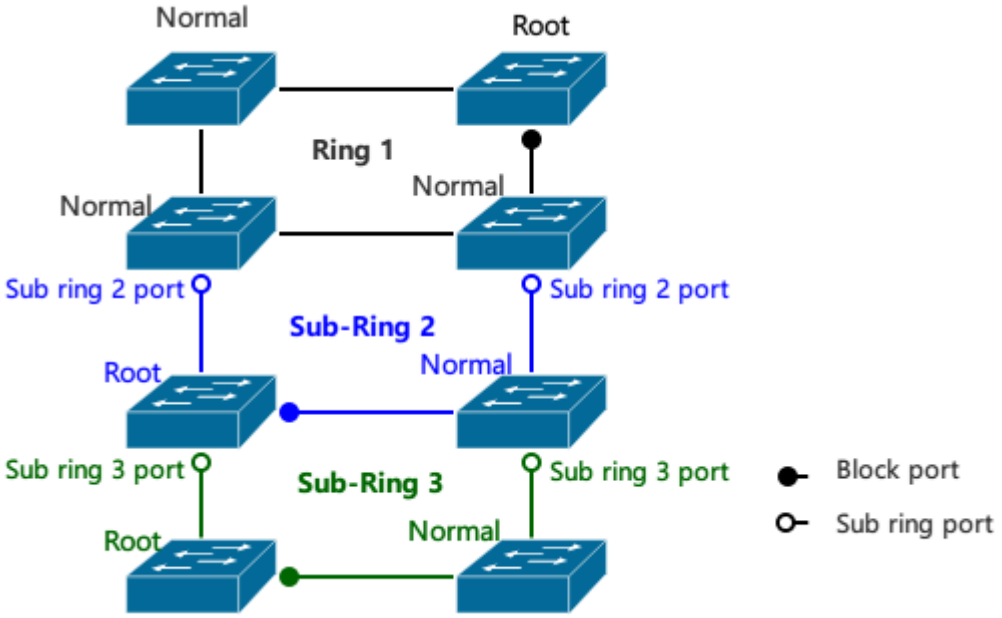


Рисунок 15-17: Схема сети с пересекающимися кольцами DG-Ring (вариант 2)

Межкольцевое взаимодействие (cross-ring networking) поддерживается только в версии DG-Ring v2.

15.9.4 Применение двойного подключения

Технология дуал-хоминг (dual-homing) обеспечивает резервирование подключения отдельного устройства к основной сети. Поддерживаются следующие варианты подключения:

- два канала к одному и тому же узлу;
- два канала к разным узлам в пределах одной сети;
- два канала к разным сетям.

Как показано на Рисунках 15-17 – 15-20, дуал-хоминг допускает гибкое развёртывание в различных топологиях с двухканальным резервированием.

Рисунок 15-17: Схема подключения дуал-хоминг к одному устройству

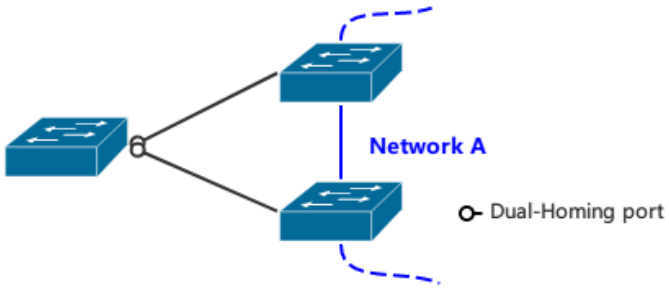


Рисунок 15-18: Подключение дуал-хоминг к разным устройствам в пределах одной сети

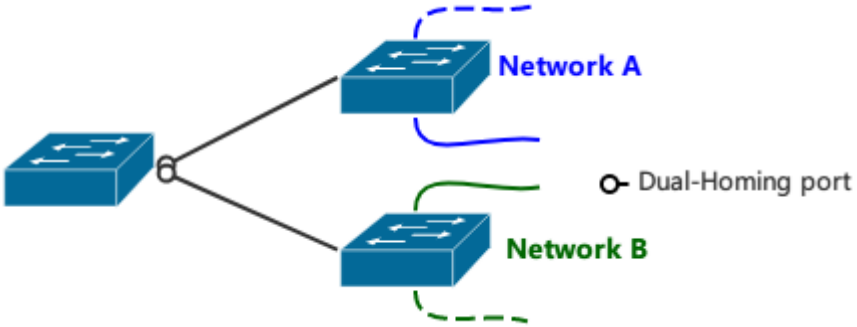


Рисунок 15-19: Подключение дуал-хоминг к сегментам A и B

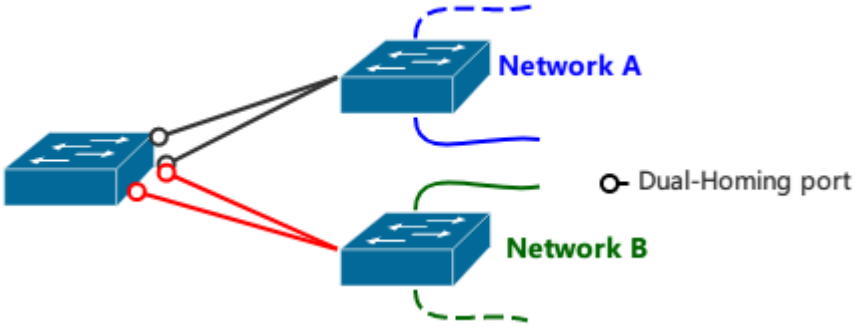


Рисунок 15-20: Подключение дуал-хоминг к сегментам A и B

15.9.5 Гибридная кольцевая сеть

Как показано на Рисунке 15-9, гибридное кольцо (Hybrid-Ring) может быть интегрировано с кольцевой сетью стороннего производителя для формирования единой расширенной сети на базе DG-Ring.

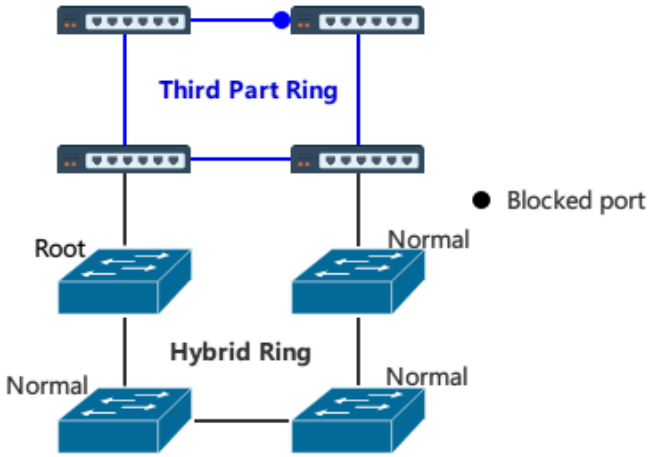


Рисунок 15-21: Комбинированная работа гибридного кольца и кольца стороннего производителя

По сравнению с кольцевыми протоколами STP, RSTP и ERPS протокол DG-Ring обеспечивает более высокую скорость сходимости и упрощённую процедуру конфигурирования.

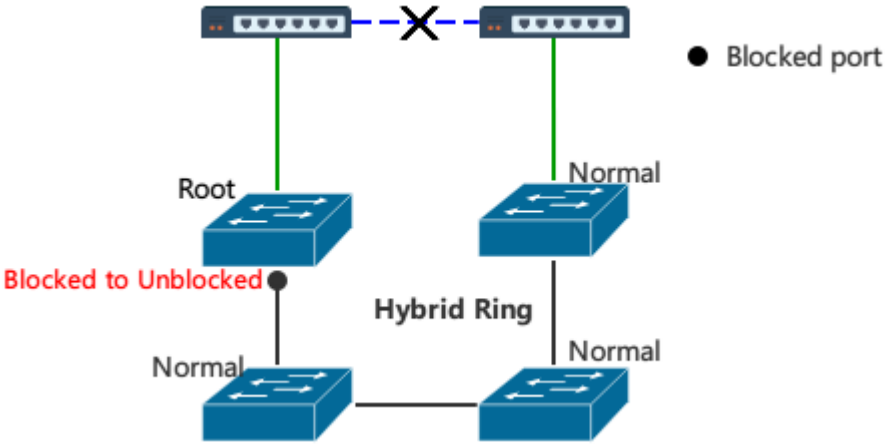


Рисунок 15-22: Отказ линка сторонней сети

15.10 Сравнение с другими кольцевыми протоколами

По сравнению с кольцевыми протоколами STP, RSTP и ERPS протокол DG-Ring обеспечивает более высокую скорость сходимости и упрощённую процедуру конфигурирования.

Таблица 15.1 - Сравнение DG-Ring с другими протоколами.

Протокол	Совместимость с оборудованием других производителей	Максимальное количество узлов	Поддерживаемые топологии	Резервное переключение	Сложность настройки	Время сходимости
STP	Да	40	Произвольная топология	Да	Как у аналогов	>30 с
RSTP (802.1D-2004)	Да	40	Произвольная топология	Да	Как у аналогов	<100 мс
ERPS (G.8032)	Да	Теоретически неограниченно	Кольцо, подкольцо, множественные экземпляры	Настраивается	Сложная	<20 мс
DG-Ring V1	Нет	Теоретически неограниченно	Циклическая, полициклическая	Нет	Простая	<20 мс
DG-Ring V2	Оптимизированная совместимость	Теоретически неограниченно	Кольцо, полициклическая, подкольцо, двойная спираль	Нет	Простая	<15 мс

16 Протокол маршрутизации

В сети Интернет для доступа к другому хосту на удаленном конце один хост должен выбрать подходящий путь через серию маршрутизаторов или коммутатор уровня 3.

Маршрутизаторы или коммутаторы уровня 3 оба вычисляют пути через ЦП, за исключением того, что коммутаторы уровня 3 добавляют вычисленные пути в коммутационный чип, и чип пересылает данные на линейной скорости; в то время как маршрутизаторы сначала сохраняют вычисленные пути в таблице маршрутизации и кэше маршрутизации, и ЦП отвечает за пересылку данных. Видно, что и маршрутизаторы, и коммутаторы уровня 3 могут выбирать пути, и коммутаторы уровня 3 имеют относительно сильные преимущества в пересылке данных. Далее кратко описываются основные принципы и методы выбора пути для коммутатора третьего уровня.

16.1 Статическая маршрутизация

Статическая маршрутизация относится к пути, указанному человеком к сети или определенному хосту, который не может быть изменен произвольно. Преимущества статической маршрутизации заключаются в том, что она проста и удобна в настройке, стабильна и ограничивает незаконные изменения маршрутов, что способствует балансировке нагрузки и резервированию маршрутов. Однако, поскольку она настраивается искусственно, маршруты, которые необходимо настроить для больших сетей, слишком велики и сложны, поэтому они не подходят для средних и крупных сетей.

Конфигурация статической маршрутизации:

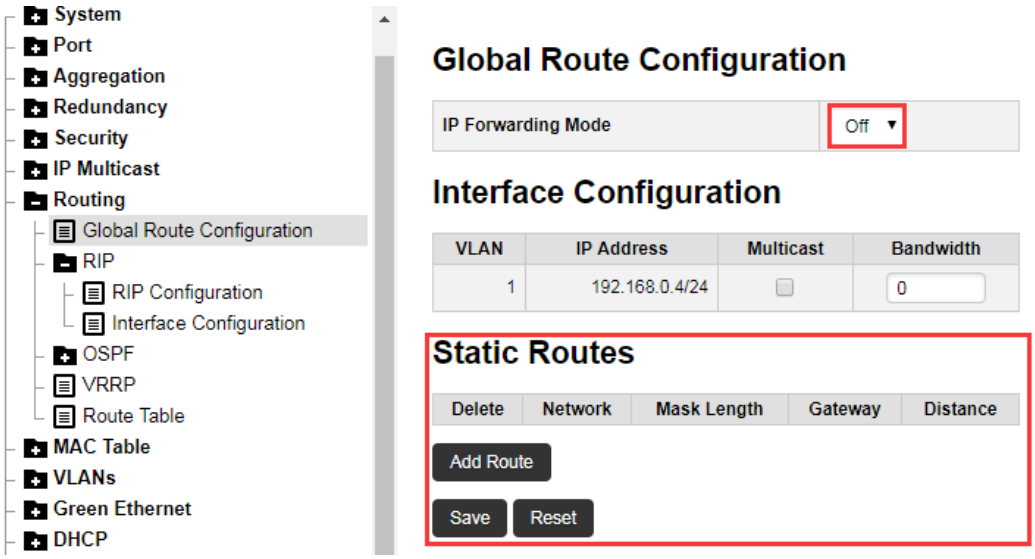


Рисунок 16-1: Конфигурация статической маршрутизации

1. Включение/выключение

Описание функции: Включение/выключение функции маршрутизации

2. Сеть

Описание функции: настройка адреса назначения.

3. Длина маски

Описание функции: настройка маски подсети для адреса назначения.

4. Шлюз

Описание функции: настройка адреса следующего перехода, который является IP-адресом однорангового устройства, для указания пути маршрутизации.

5. Расстояние

Описание функции: настройка значения взвешивания маршрута, значение по умолчанию для статического маршрута равно 1.

16.2 Динамическая маршрутизация

Динамическая маршрутизация относится к пути, который коммутатор уровня 3 динамически вычисляет к сети или определенному хосту на основе инициированного протокола маршрутизации. Если следующий переход коммутатора уровня 3 на пути недоступен, коммутатор уровня 3 может автоматически отбросить путь через коммутатор уровня 3 и выбрать путь через другие коммутаторы уровня 3.

Протоколы динамической маршрутизации обычно делятся на две категории: протоколы маршрутизации внутреннего шлюза (IGP) и протоколы маршрутизации внешнего шлюза (EGP). Протокол маршрутизации внутреннего шлюза (IGP) — это протокол, используемый для вычисления маршрутов назначения внутри автономной системы. Протоколы динамической маршрутизации внутреннего шлюза, поддерживаемые коммутатором уровня 3, — это протоколы маршрутизации RIP и OSPF, и протоколы маршрутизации RIP и OSPF могут быть настроены по мере необходимости. Коммутаторы уровня 3 поддерживают одновременный запуск нескольких протоколов динамической маршрутизации внутреннего шлюза, и другие протоколы динамической маршрутизации и статическая маршрутизация также могут быть повторно введены в один протокол динамической маршрутизации для соединения нескольких протоколов маршрутизации.

16.2.1 Конфигурация маршрута RIP

Конфигурация маршрута RIP:

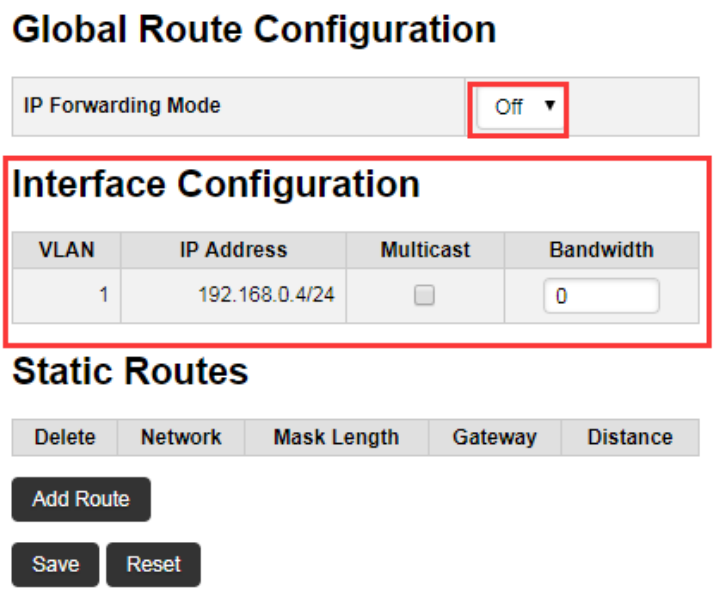


Рисунок 16-2: Конфигурация маршрутизации RIP

1. Включение/выключение

   Описание функции: Включение/выключение функции маршрутизации

2. Multicast

   Описание функции: включение функции многоадресной рассылки версии RIPv2. После установки флажка сообщения будут отправляться через многоадресную рассылку версии RIPv2.

Глобальная конфигурация маршрутизации RIP:

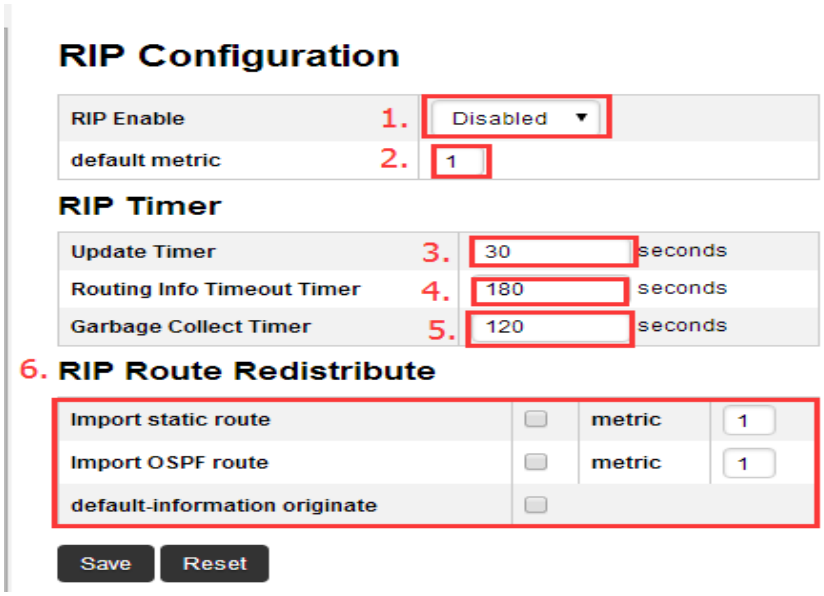


Рисунок 16-3: Глобальная конфигурация маршрутизации RIP

1. Включение/выключение

   Описание функции: Включение/выключение протокола RIP

2. Default metric

   Описание функции: настройка взвешенного значения маршрута RIP, диапазон значений от 1 до 16, значение по умолчанию равно 1.

3. Update Timer

   Описание функции: настройка временного интервала для отправки пакета RIP, диапазон значений от 1 до 2147483647, конфигурация по умолчанию 30.

4. Тайм-аут информации о маршрутизации

   Описание функции: настройка времени сбоя маршрута RIP. Если в течение этого периода времени не получена информация об обновлении таблицы маршрутизации от определенного соседа, все маршруты от этого устройства станут недействительными и перейдут в подавленное состояние. Время конфигурации недействительности маршрута должно быть больше времени обновления маршрута. Диапазон значений от 1 до 2147483647, конфигурация по умолчанию 30.

5. Таймер сбора мусора

   Описание функции: настройка времени, в течение которого маршрут RIP находится в подавленном состоянии. Если в течение этого периода времени не получена информация об обновлении устройства, удалите эти маршруты из таблицы, если информация об обновлении устройства не была получена в течение этого периода времени. Время подавления маршрута должно быть больше времени обновления маршрута, диапазон значений от 1 до 2147483647, конфигурация по умолчанию 120.

6. Перераспределение маршрута RIP

   Описание функции: введение маршрута по умолчанию/статического маршрута/маршрута OSPF, но только активного маршрута с состоянием

Конфигурация интерфейса маршрутизации RIP:

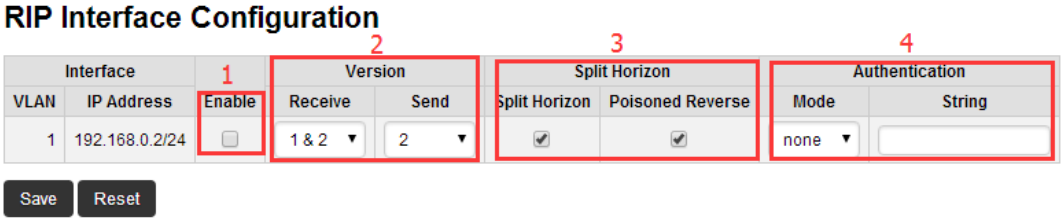


Рисунок 16-4: Конфигурация интерфейса маршрутизации RIP

1. Enable

   Описание функции: включение протокола RIP на интерфейсе третьего уровня

2. Version Receive/Send

   Описание функции: настройка интерфейса для приема версии информации пакета RIP. По умолчанию принимаются версии RIP 1 и 2, настройка версии пакета RIP, отправляемого интерфейсом.

3. Split Horizon/poisoned Reverse

   Описание функции: настройка разрешения горизонтального разделения. Используется для предотвращения петель маршрутизации, то есть коммутатор уровня 3 отправляет маршруты, изученные с интерфейса, с этого интерфейса.

Обратное отравление: в сети на основе протокола информации о маршрутизации после того, как сообщение о пути становится недействительным, маршрутизатор не удаляет его немедленно из таблицы маршрутизации, а транслирует его с метрикой 16, недостижимой. Для более быстрой конвергенции.

4. Аутентификация Описание функции: настройка метода проверки, text представляет текстовую проверку; MD5 представляет обычную проверку MD5, и может быть добавлен в собственную таблицу маршрутизации только при совпадении ключей.

16.2.2 Конфигурация маршрутизации OSPF

Протокол OSPF (Open Shortest Path First), т.е. "Протокол открытого кратчайшего пути первого". Это динамический протокол маршрутизации внутри автономной системы на основе состояния канала, который составляет базу данных состояния канала путем обмена информацией о состоянии канала между коммутаторами третьего уровня, а затем генерирует таблицу маршрутизации на основе этой базы данных с использованием алгоритма кратчайшего пути первого.

Автономные системы (AS) — это самоуправляемая взаимосвязанная сеть. В больших сетях, таких как Интернет, чрезвычайно взаимосвязанные сети разбиваются на автономные системы. Крупные корпоративные сети, подключенные к Интернету, являются независимыми автономными системами, потому что другие хосты в Интернете не управляются ею, и она и коммутаторы уровня 3 Интернета не обмениваются внутренней информацией о маршрутизации.

Глобальная конфигурация маршрутизации OSPF:

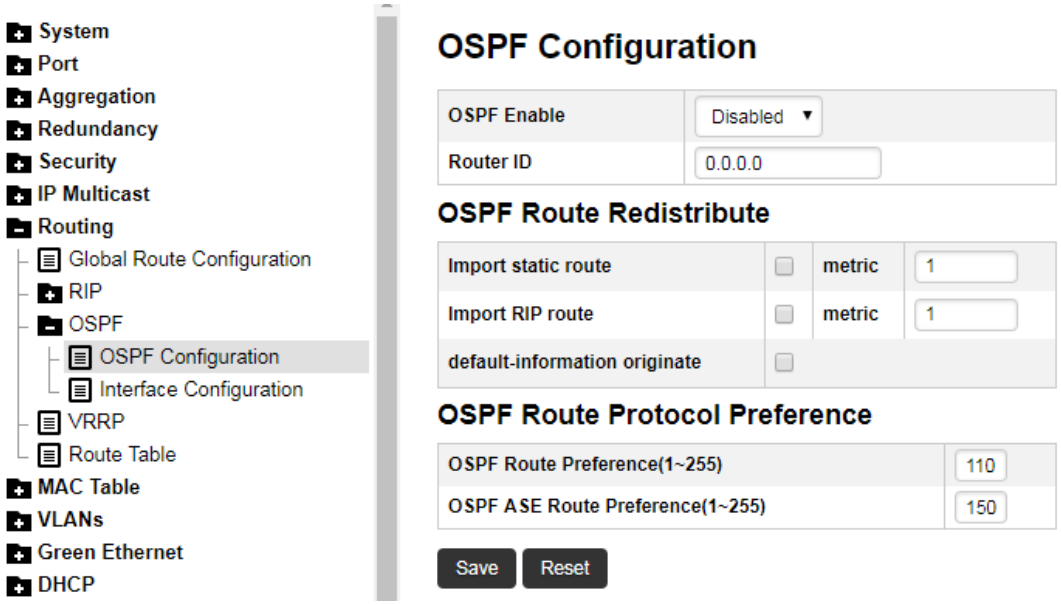


Рисунок 16-5: Глобальная конфигурация маршрутизации OSPF

1. Disable/enable

   Описание функции: Выключение/включение функции OSPF.

2. Router ID

   Описание функции: идентифицирует один маршрутизатор и имеет уникальность.

3. Перераспределение маршрута OSPF

   Описание функции: введение маршрута по умолчанию/статического маршрута/маршрута OSPF, но только активный маршрут с состоянием может быть введен

4. Ссылка на протокол маршрута OSPF

   Описание функции: настройка приоритета маршрута OSPF и настройка приоритета внешнего маршрута, введенного OSPF.

Конфигурация интерфейса маршрутизации OSPF:

Рисунок 16-6: Конфигурация интерфейса маршрутизации OSPF

1. Enable

   Описание функции: установите флажок этой функциональной опции, чтобы включить функцию маршрутизации интерфейса OSPF.

2. Passive

   Описание функции: установите флажок этой функциональной опции, этот интерфейс уровня 3 не будет активно отправлять OSPF, больше не будет устанавливать отношения с соседями, а также отправлять и получать информацию о маршрутизации.

3. Cost

   Описание функции: настройка значения стоимости пути маршрутизации OSPF для вычисления более быстрых путей маршрутизации.

4. Area

   Описание функции: настройка интерфейса для разделения на определенную область, принадлежат маршрутизаторы одной и той же области и соответствуют одному и тому же значению Area.

5. Timer Hello

Описание функции: настройка временного интервала для отправки сообщений Hello, это значение должно быть одинаковым для всех маршрутизаторов, подключенных к общей сети.

6. Timer Dead

   Описание функции: настройка времени сбоя маршрута. Если в течение этого времени не получено сообщение Hello от соседнего маршрутизатора, это означает, что маршрут не работает.

7. Timer Retransmit

   Описание функции: настройка временного интервала для повторной передачи описания базы данных и информации уровня канала, OSPF должен подтвердить каждое вновь поступившее объявление состояния канала (LSA), зная, что подтверждение получено, значение по умолчанию составляет 5 секунд.

8. Timer Transmit

   Описание функции: эта переменная используется для добавления указанного времени в поле возраста обновления, этот параметр важен для каналов с очень низкой скоростью передачи.

9. Аутентификация

   Описание функции: настройка способа проверки, Text для текстовой проверки; MD5 указывает на "обычную" проверку MD5, и необходимо настроить значение Key ID, когда ключи совпадают, он может быть добавлен в собственную таблицу маршрутизации.

16.2.3 Конфигурация маршрутизации VRRP

Протокол виртуальной избыточности маршрутизатора устраняет риск отказа единой точки обслуживания в среде статической маршрутизации по умолчанию. VRRP избегает недостатков статически указанных шлюзов. Через VRRP группа коммутаторов маршрутизации может работать вместе, чтобы сформировать виртуальный коммутатор маршрутизации. Виртуальный коммутатор маршрутизации внешне оснащен виртуальным IP-адресом и виртуальным MAC-адресом. VRRP выбирает один из блоков коммутации маршрутизации в качестве главного, ответственного за пересылку пакетов. Когда главный коммутатор маршрутизации выходит из строя, резервный коммутатор маршрутизации быстро берет на себя функции главного коммутатора маршрутизации, хосту не нужно изменять адрес шлюза по умолчанию, и этот процесс прозрачен для терминальной системы. Это обеспечивает более быстрое и эффективное решение в случае сбоя.

Конфигурация маршрутизации VRRP:

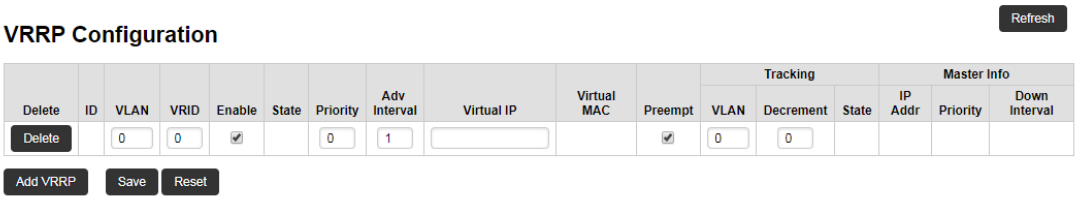


Рисунок 16-7: Конфигурация маршрутизации VRRP

1. Добавить VRRP

   Описание функции: добавить сессионный интерфейс VRRP и заполнить интерфейс маршрутизации, на котором необходимо включить VRRP в VLAN.

2. VRID

   Описание функции: настройка того, что интерфейс разделен на определенную резервную группу, которая может иметь несколько участников, формируя избыточную структуру.

3. Enable

   Описание функции: включение функции маршрутизации VRRP на этом интерфейсе.

4. Priority

   Описание функции: настройка приоритета этого маршрутизатора, чем больше значение приоритета, тем выше приоритет, маршрутизатор с наивысшим приоритетом станет маршрутизатором Master.

5. Adv Internal

   Описание функции: настройка временного интервала объявления VRRP, это значение в основном используется для локализации и устранения неисправностей при неправильной настройке маршрутизатора.

6. Virtual IP

   Описание функции: настройка виртуального IP-адреса VRRP.

7. Preempt

   Описание функции: установка флажка функционального модуля настроит маршрутизатор в режим вытеснения. При проведении выборов главного маршрутизатора маршрутизатор будет активно отправлять сообщение со своим приоритетом для проведения выборов главного маршрутизатора.

8. Отслеживание VLAN

   Описание функции: настройка мониторинга интерфейса маршрутизации для изменения приоритета маршрутизатора в соответствии с состоянием восходящего порта. При сбое восходящего канала и невозможности доступа хоста в локальной сети к внешней сети через маршрутизатор, отслеживаемый элемент Track становится отрицательным и снизит приоритет маршрутизатора на определенную величину, тем

самым сделав приоритет других маршрутизаторов в резервной группе выше приоритета этого маршрутизатора и став маршрутизатором Master, чтобы обеспечить непрерывность связи.

9. Информация Master

   Описание функции: отобразить базовую информацию маршрутизатора Master здесь.

Техническая поддержка

Если вы столкнулись с проблемой при первичной настройке или при эксплуатации, свяжитесь с нашим сервисным центром.

Головной офис, Москва

Телефоны: +7 (495) 723-81-21, +7 (499) 969-81-21

E-mail: sales@dgsys.ru

Техническая поддержка 24/7

E-Mail: support@dgsys.ru

Телефон: +7 (495) 723-33-33

Адрес офиса обслуживания и склада:

117535, г. Москва, Варшавское шоссе, дом 133, строение 2, помещение 301А

Для получения дополнительной информации, посетите наш сайт DGSYS.RU