Управляемый коммутатор
Gigabit Ethernet Switch

Руководство по управлению веб-сетью

Версия 4.1.2

Заявление

Авторское право. Все права закреплены

Настоящее руководство является собственностью нейтральной компании. Выдержки и частичное или полное копирование, а также передача информации, содержащейся в настоящем документе, в любой форме любыми юридическими и физическими лицами без письменного разрешения компании запрещено.

Предисловие

В настоящем руководстве приведено полное описание веб-страниц коммутатора Full Gigabit Ethernet Switch. Пользователи могут управлять коммутатором через веб-страницы коммутатора Full Gigabit Ethernet Switch. Настоящее руководство представляет собой простое введение в работу каждой веб-страницы. Различные функции коммутатора Full Gigabit Ethernet Switch приведены в руководстве пользователя.

Предисловие включает следующее:

- Целевая аудитория
- Общая информация о продукте
- Функции продукта

Целевая аудитория

- Планировщик сетей
- Персонал выездной технической поддержки и обслуживания
- Администратор сети, ответственный за настройку и обслуживание сети

Общая информация о продукте

Управляемый коммутатор Full Gigabit Ethernet Switch разработан и произведен нашей компанией. Коммутатор Ethernet разработан специально для обеспечения высокого уровня безопасности и соответствия требованиям высокопроизводительной сети. Система использует новую программную и аппаратную платформу, предоставляя комплексную систему безопасности, идеальную стратегию обеспечения качества обслуживания и богатую функцию виртуальной локальной сети (VLAN), а также простоту управления и обслуживания. Он идеально подходит для офисных сетей, университетских сетей и может использоваться как коммутатор конвергентного уровня для малых и средних предприятий и их филиалов.

Функции продукта

- Поддержка IEEE 802.3x
- Поддержка IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z
- Поддержка IEEE 802.3ad
- Поддержка IEEE 802.3q, IEEE 802.3q/p
- Поддержка IEEE 802.1w, IEEE 802.1d, EEE 802.1S
- Поддержка таблицы на 16 000 MAC-адресов, автоматическое обновление, двустороннее обучение
- Поддержка VLAN на основе портов, до 4096 VLAN
- Поддержка VLAN стандарта 802.1Q
- Поддержка протокола связующего дерева STP
- Поддержка быстрого протокола связующего дерева RSTP
- Поддержка быстрого протокола связующего дерева MSTP
- Поддержка протокола сети кольцевой топологии EPPS
- Поддержка протокола сети кольцевой топологии EAPS

- Поддержка соглашений для аргументов 802.1x
- Поддержка 8 групп конвергенции, максимум 8 портов в каждой группе
- Зеркала портов, поддерживающие двусторонний прием и передачу данных
- Поддержка функции защиты от образования петель, обнаружение в реальном времени, быстрая сигнализация, точное позиционирование, интеллектуальная блокировка, автоматическое восстановление
- Поддержка нисходящих портов для отделения друг от друга и связи с верхним портом
- Поддержка полудуплексного режима на основе контроля обратного потока
- Поддержка полного дуплекса на основе кадров ПАУЗЫ
- Управление пропускной способностью ввода/вывода на основе портов
- Поддержка IGMPv1/2/3 и MLDv1/2 Snooping
- Поддержка регистрации протокола GMRP
- Поддержка управления адресами многоадресной рассылки, многоадресной рассылки VLAN, порта маршрутизации многоадресной рассылки, статического адреса многоадресной рассылки
- Поддержка технологии DHCP Snooping
- Поддержка подавления зацикливания неизвестных пакетов одноадресной рассылки, многоадресной рассылки, неизвестных пакетов многоадресной рассылки, широковещательной рассылки
- Поддержка подавления зацикливания на основе регулирования полосы пропускания и фильтрации зацикливания
- Поддержка пользовательского порта + IP-адрес + MAC-адрес
- Поддержка списка управления доступом (ACL) на основе IP- и MAC-адресов
- Свойства безопасности, поддерживающие определенное количество MAC-адресов на основе портов
- Поддержка алгоритма приоритизации очереди портов 802.1p
- Поддержка Cos/Tos, разметка QOS

- Поддержка WRR (циклический взвешенный алгоритм), алгоритм приоритизации на основе взвешенной ротации
- Три режима планирования приоритизации, поддерживающих WRR, SP и WFQ
- Поддержка функции Auto-MDIX для автоматической идентификации сквозных сетевых линий и перекрестных сетевых линий
- Поддержка портом функции автоматического согласования (скорость передачи с самосогласованием и дуплексный режим)
- Поддержка загрузки пакета обновлений
- Поддержка просмотра системного журнала
- Поддержка онлайн-восстановления заводской конфигурации
- Поддержка открытия или закрытия порта
- Поддержка стандартного управления расписанием POE
- Поддержка автоматического определения функции онлайн-оборудования (автоматическое определение, автоматическое определение отключено)
- Поддержка управления веб-интерфейсом
- Поддержка управления CLI на основе Telnet и консоли
- Поддержка управления SNMP V1/V2/V3
- Поддержка управления SSHV1/V2
- Поддержка управления RMON

Обновление версии

Версия 4.1.2

Оптимизация пользовательского интерфейса

Проблема устранена, и скорость отклика стала выше.

Поддержка переключения китайского и английского языков одной кнопкой.

Соответствующие функции оптимизированы для упрощения управления.

Содержание

ОБЗОР ВЕБ-СТРАНИЦ 9

1. Характеристики онлайн-доступа 9

2. Системные требования для просмотра веб-страниц 9

3. Вход в сеанс просмотра веб-страниц 10

4. Основная структура веб-страницы 11

5. Структура дерева навигации 13

6. Описание кнопок на странице 13

7. Сообщение об ошибке 14

8. Поле ввода 14

9. Поле состояния 15

ОБЩАЯ ИНФОРМАЦИ О ВЕБ-СТРАНИЦЕ 16

1. Диалоговое окно входа в систему 16

2. Главная страница 17

3. Конфигурация системы 18

4. Конфигурация портов 27

5. Привязка MAC-адресов 37

6. MAC-фильтр 39

7. Конфигурирование VLAN 40

8. Конфигурация SNMP 44

9. Конфигурация ACL 46

10. Конфигурация QOS 52

11. Базовая конфигурация IP 54

12. Конфигурация AAA 56

13. Конфигурация MSTP 62

14. Конфигурация IGMP SNOOPING 63

15. Конфигурация GMRP 65

16. Конфигурация EAPS 67

17. Конфигурация RMON 69

18. Конфигурация кластера 73

19. Конфигурация ERPS 77

20. Управление журналами 80

ОБЗОР ВЕБ-СТРАНИЦ

1. Характеристики онлайн-доступа

Все управляемые коммутаторы Gigabit Ethernet Switch предоставляют пользователям онлайн-доступ. Пользователи могут получать доступ к коммутаторам через веб-браузеры для управления и настройки. Основные преимущества онлайн-доступа:

- Легкий доступ — пользователи могут с легкостью получать доступ к коммутатору из любой точки сети.
- Пользователи могут использовать знакомый Netscape Communicator, Microsoft Internet Explorer и другие браузеры для доступа к веб-странице коммутатора. Веб-страница представляется пользователю в графическом и табличном виде.
- Управляемый коммутатор Gigabit Ethernet Switch предоставляет множество веб-страниц. С помощью этих веб-страниц пользователи могут настраивать большинство функций этих коммутаторов и управлять ими.
- Классификация и интеграция функций веб-страниц, удобная для поиска соответствующей страницы для настройки и управления.

2. Системные требования для просмотра веб-страниц

Системные требования для просмотра веб-страниц приведены в таблице 1.

Таблица 1:

Аппаратное и программное обеспечение	**Системные требования**
ЦП	Pentium 586 и выше
Оперативная память	128 МБ и более
Разрешение	800x600 и выше
Цвет	256 и более цветов
Браузер	IE4.0 и более поздние версии или Netscape4.01 и более

	поздние версии
Операционная система	Microsoft®, Windows95®, Windows98®, WindowsNT®, Windows2000®, WindowsXP®, WindowsME®, WindowsVista®, Windows7®, Windows8®, операционная система MAC, Linux, Unix

Примечание —

Microsoft®, Windows95®, Windows98®, WindowsNT®, Windows2000®, WindowsXP®, Windows ME®, WindowsVista®, Windows7®, Windows8® являются зарегистрированными товарными знаками корпорации Microsoft, все остальные названия продуктов, товарные знаки, зарегистрированные товарные знаки и знаки обслуживания, а также авторские права принадлежат их соответствующим владельцам.

3. Вход в сеанс просмотра веб-страниц

Прежде чем начать сеанс просмотра веб-страниц, вам необходимо убедиться в следующем:

- IP-адрес был настроен на коммутаторе. По умолчанию IP-адрес интерфейса VLAN1 коммутатора — 192.168.0.1.
- Маска подсети — 255.255.255.0.
- Главный компьютер с установленным веб-браузером подключен к сети, и главный компьютер может выполнять пинг через коммутатор.
- После завершения двух вышеуказанных задач пользователь в адресной строке браузера должен ввести адрес коммутатора и нажать кнопку Enter, чтобы перейти на страницу онлайн-входа коммутатора, как показано на рис. 1. При отключенном многопользовательском управлении для входа пользователя в онлайн-систему возникает необходимость в проверке пароля анонимного пользователя (администратора). Вводите только правильный пароль для доступа в Интернет, пароль анонимного пользователя по умолчанию — admin.

Если в системе включено многопользовательское управление и настроены привилегированные пользователи, пароль анонимного пользователя не активируется,

при доступе пользователя к сети не выполняется проверка пароля анонимного пользователя, но выполняется проверка подлинности имени пользователя и пароля для многопользовательского управления.

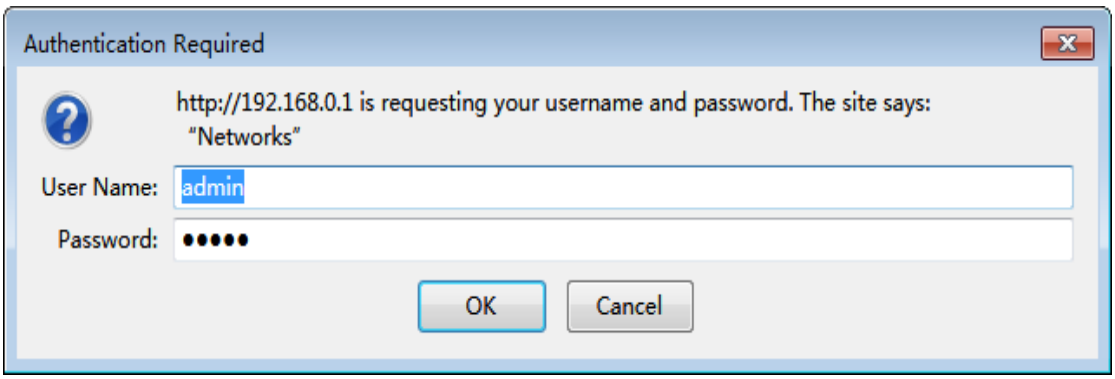


Рисунок 1 — Веб-страница входа в систему для сеанса просмотра

4. Основная структура веб-страницы

На рис. 2. показано, что веб-страница состоит из трех частей: поля заголовка, поля дерева навигации и главной страницы.

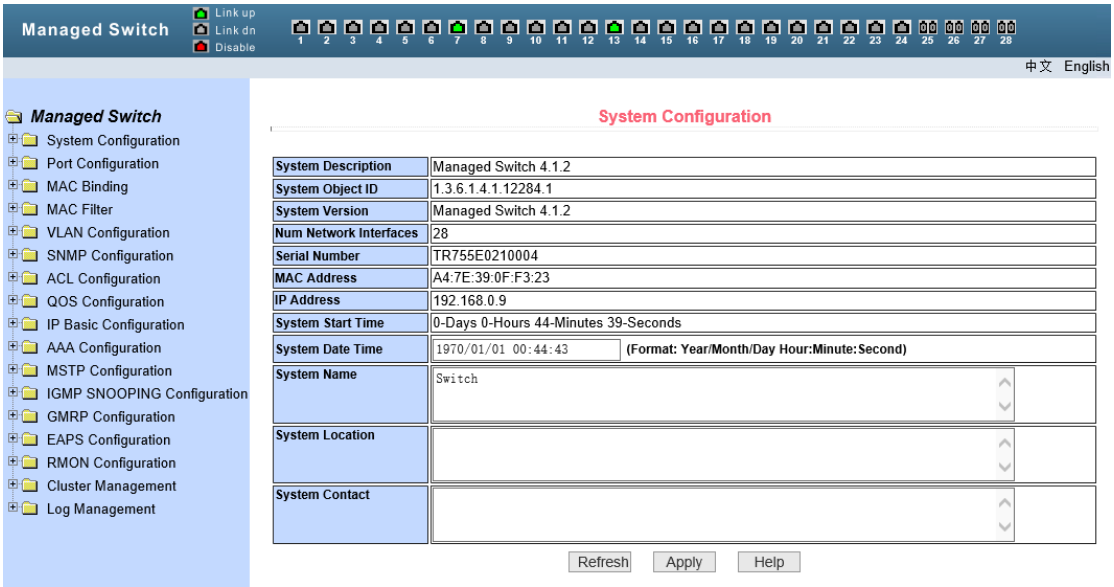


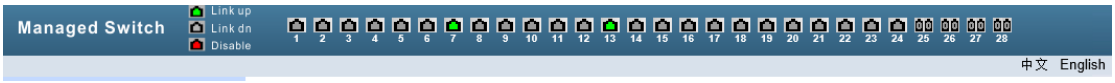
Рисунок 2 — Основная структура веб-страницы коммутатора

Поле заголовка используется для отображения логотипа и состояния портов в реальном времени, как показано ниже

Зеленый индикатор указывает на то, что порт подключен;

Серый индикатор указывает на то, что порт не подключен;

Красный индикатор указывает на то, что порт выключен (конкретная настройка показана на рис. 17).



Главная страница используется для отображения страницы, выбранной пользователем в дереве навигации.

5. Структура дерева навигации

На рис. 3 показана организация дерева навигации.

Дерево навигации расположено в левом нижнем углу каждой страницы и отображает узлы веб-страницы в виде дерева. Пользователь может легко найти веб-страницу для управления. В соответствии с различными функциями страницы будут разделены на разные группы, каждая группа включает в себя одну или несколько страниц. Большинство веб-страниц в дереве навигации представлены сокращенными названиями страниц в верхней части соответствующей страницы.

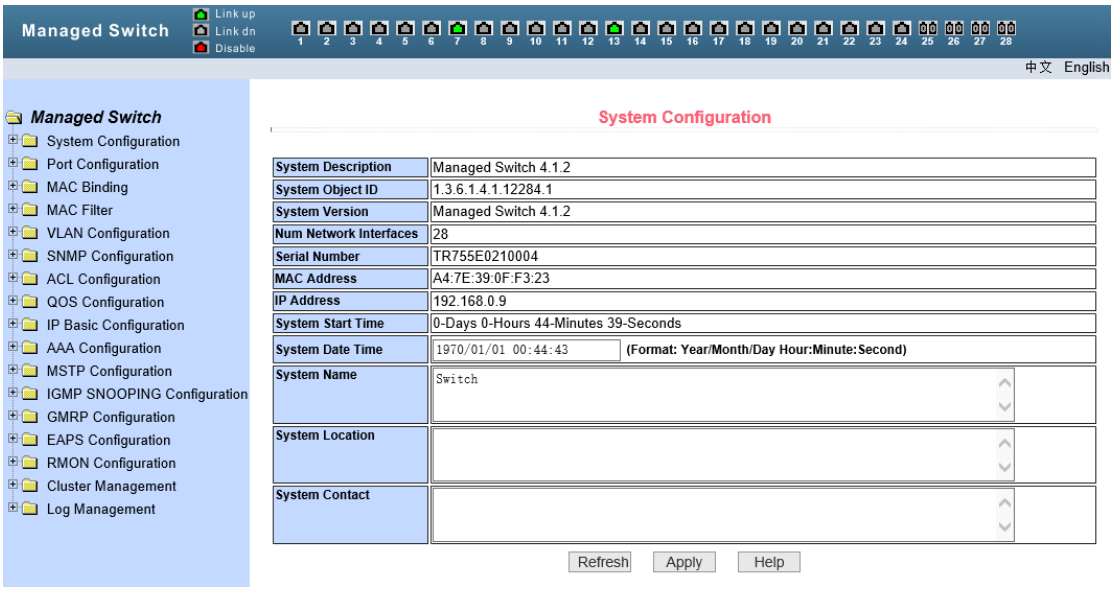


Рисунок 3 — Организация дерева навигации страницы коммутатора

6. Описание кнопок на странице

На странице представлено несколько общих кнопок. Роль этих кнопок в целом одинакова. Для справки роли этих кнопок приведены в таблице 2.

Таблица 2

Кнопка	**Действие**
Обновить (Refresh)	Обновление всех полей на странице

Применить (Apply)	Запись обновленных значений в память. Поскольку проверка ошибок выполняется веб-сервером, проверка ошибок не выполняется до активации этой кнопки пользователем.
Удалить (Delete)	Удаление текущей записи
Справка (Help)	Открытие страницы справки и просмотр инструкций по настройке для каждой страницы

7. Сообщение об ошибке

Если веб-сервер коммутатора выдает ошибку при обработке пользовательских запросов, в диалоговом окне отображается соответствующее сообщение об ошибке. Например, на рис. 4 показано диалоговое окно с сообщением об ошибке.

Рисунок 4 — Страница сообщения об ошибке

8. Поле ввода

В крайнем левом столбце таблицы есть несколько окон, на которых есть поле ввода, как показано на рис. 5, с помощью которого вы можете получить доступ к различным строкам таблицы. При выборе значения в поле ввода соответствующая информация для этой строки отображается в первой строке, и редактировать можно только эту строку, которая также называется активной строкой. Когда загружается первая страница, в поле отображается "Добавить" (New), активная строка не заполнена.

Если вы хотите добавить новую строку, выберите "Добавить" (New) из выпадающего меню поля ввода, введите информацию о новой строке и нажмите кнопку "Применить" (Apply).

Если вы хотите отредактировать существующую строку, выберите соответствующий номер строки из выпадающего меню поля ввода, отредактируйте строку и нажмите кнопку "Применить" (Apply). Соответствующее изменение будет отображено в таблице.

Если вы хотите удалить строку, выберите соответствующий номер строки из выпадающего меню в поле ввода и нажмите кнопку "Удалить" (Delete). Строка исчезнет из таблицы.

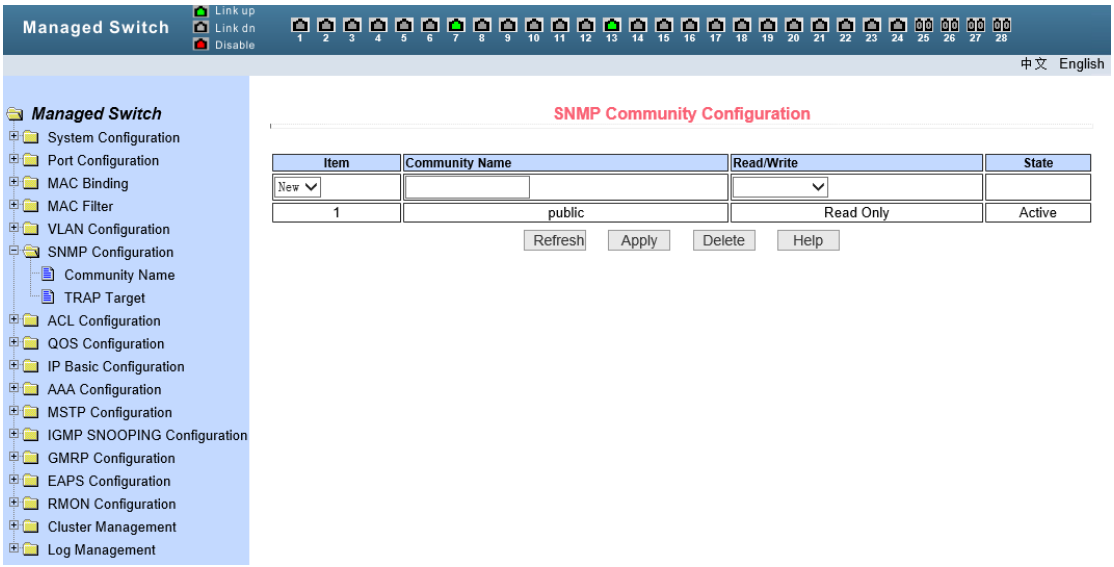


Рисунок 5 – Страница с полем ввода

9. Поле состояния

В крайнем правом столбце таблицы есть несколько окон, на которых представлено поле состояния, как показано на рис. 6. Это поле показывает состояние строки. Поскольку все изменения состояния строки обрабатываются внутри системы, поле состояния доступно только для чтения. Как только вся информация о домене в строке становится действительной, состояние строки автоматически становится активным.

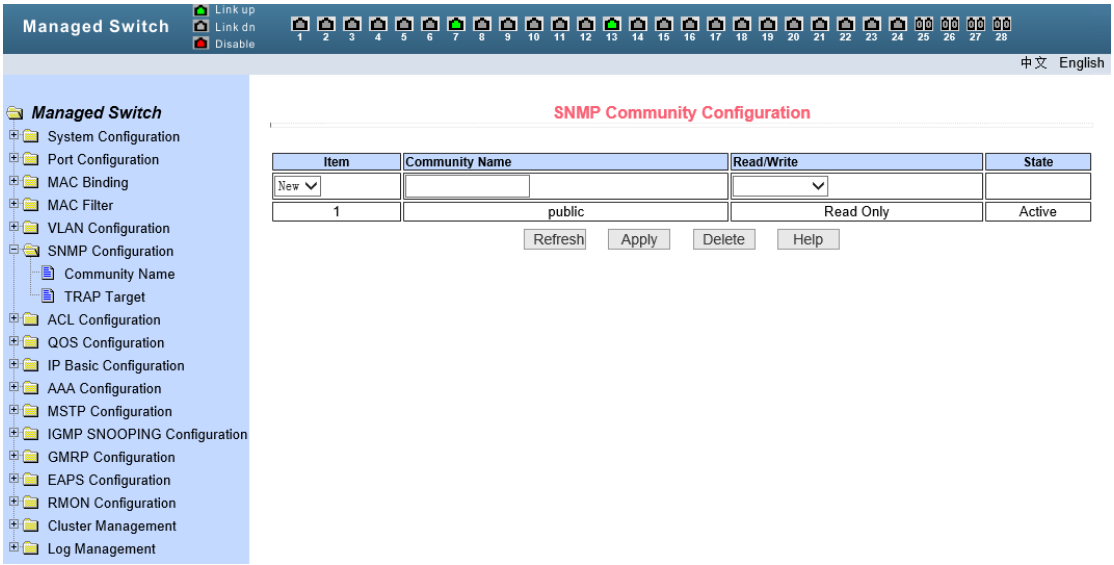


Рисунок 6 – Страница с полем состояния

ОБЩАЯ ИНФОРМАЦИ О ВЕБ-СТРАНИЦЕ

1. Диалоговое окно входа в систему

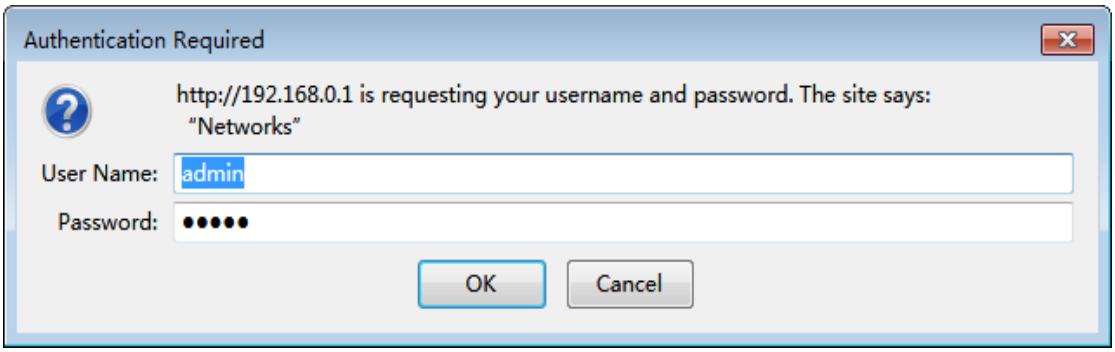


Рисунок 7 – Страница входа в сеанс для онлайн-просмотра

На рис. 7 показано диалоговое окно входа в систему, которое отображается при первом входе пользователя на веб-страницу. Пользователь должен ввести имя пользователя и пароль в соответствующее поле, а затем нажать кнопку OK для входа на веб-сервер коммутатора. Пароль чувствителен к регистру, пароль анонимного пользователя может быть установлен длиной до 16 символов, а имя и пароль для многопользовательского режима могут содержать до 16 символов.

Имя пользователя по умолчанию для коммутатора — имя анонимного пользователя admin. Пароль по умолчанию — пароль анонимного пользователя. Пароль анонимного пользователя по умолчанию пуст.

2. Главная страница

На рис. 8 показана главная страница коммутатора. Страница будет отображаться после входа пользователя в систему.

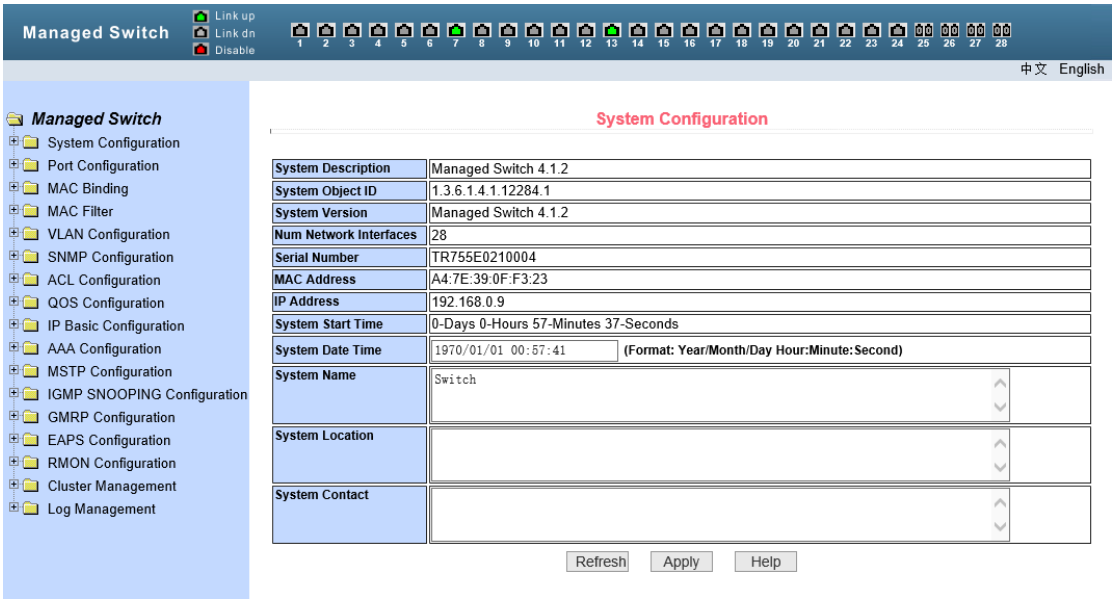
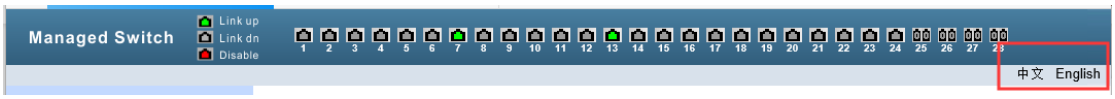


Рисунок 8 – Главная страница коммутатора

3. Конфигурация системы

Переключение языков: кнопки в правом верхнем углу позволяют легко переключаться между системными интерфейсами на китайском и английском языках.



(1) Страница основной информации

На рис. 9 показана страница основной информации о конфигурации, на которой пользователь может настроить основные параметры коммутатора.

Поле "Описание системы" (System Description) отображает описание параметров, связанных с системой.

Идентификационный номер системного дескриптора (System Object ID) указывает на принадлежность системы к сетевому управлению.

Номер версии системы (System Version) показывает номер версии текущего программного обеспечения, используемого коммутатором.

Количество сетевых интерфейсов (Num Network Interfaces) отображает текущее количество сетевых интерфейсов в коммутаторе.

Время работы системы (System Start Time) отображает время с момента запуска коммутатора до настоящего времени.

Системные часы (System Date Time) отображают текущие дату и время системы. Пользователь может изменить текущие дату и время системы, включая параметры года, месяца, дня, часов, минут и секунд.

Системное имя (System Name) отображает системное имя коммутатора в сети. Пользователь может изменить системное имя.

Системное местоположение (System Location) отображает физическое местоположение коммутатора в сети. Пользователь может изменить системное местоположение.

Системные контакты (System Contact) отображает управление текущими контактами узла и контактной информацией. Пользователь может изменить системные контакты.

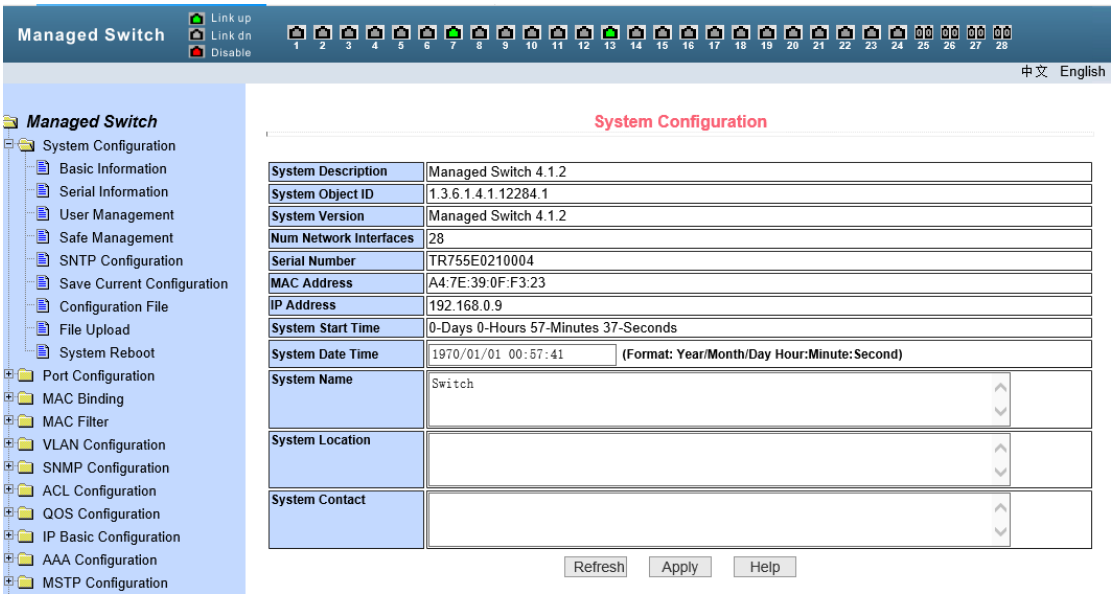


Рисунок 9 – Страница с основной информацией

(2) Страница конфигурации последовательного порта

На рис. 10 показана страница конфигурации последовательного порта, на которой отображается скорость передачи данных последовательного порта и другая информация, относящаяся к нему. Когда хост управляет коммутатором через последовательный терминал (например, Windows HyperTerminal), конфигурация COM-порта терминала последовательного порта должна соответствовать информации на этой странице.

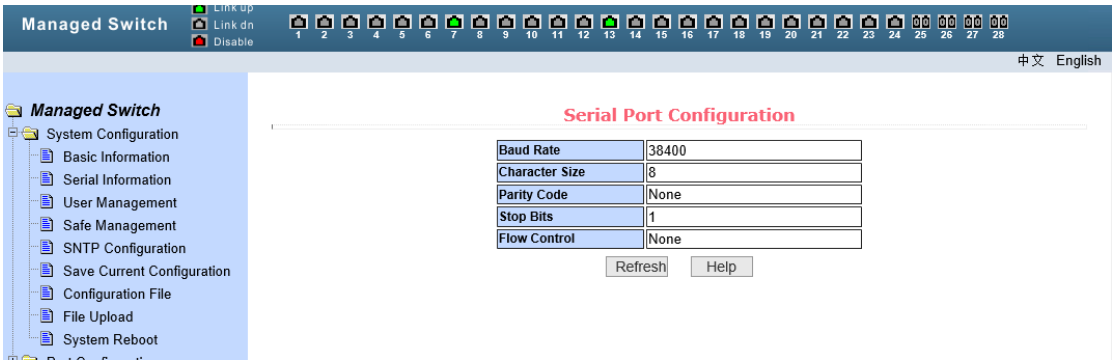


Рисунок 10 – Страница конфигурации последовательного порта

(3) Страница конфигурации многопользовательского управления

На рис. 11 показана страница конфигурации многопользовательского управления, на которой пользователи могут изменять пароль анонимного пользователя (администратора) коммутатора. Если режим многопользовательского управления не включен, протокол Telnet и веб-протокол используют один и тот же пароль анонимного пользователя. Пароли чувствительны к регистру, и могут включать максимум до 16 символов. Для смены пароля пользователю необходимо дважды ввести новый пароль. Как только пользователь нажмет кнопку "Применить" (Apply), активируется новый пароль. Если коммутатор не переходит в многопользовательский режим, отобразится диалоговое окно входа в систему (показано на рис. 7). Для повторного входа в систему пользователь должен ввести новый пароль анонимного пользователя на веб-странице входа в систему.

В то же время через эту страницу пользователи могут активировать многопользовательский режим. По умолчанию многопользовательский режим на коммутаторе отключен, то есть по умолчанию не включает функции многопользовательского управления. В этом режиме для входа в систему не требуется многопользовательская аутентификация по имени пользователя и паролю. Для Telnet при добавлении имени пользователя включается функция многопользовательского управления, а когда все пользователи удаляются, функция многопользовательского управления снова отключается. Для веб-протокола, когда добавляется имя пользователя, если это привилегированный пользователь, включается функция многопользовательского управления, когда все привилегированные пользователи удаляются, функция многопользовательского управления снова отключается. При включенной функции многопользовательского управления пароль анонимного пользователя не действует. Для входа в систему при использовании Telnet и веб-протоколов требуется многопользовательская аутентификация по имени пользователя и паролю. При отключенной функции многопользовательского управления, если настроен пароль анонимного пользователя, для входа в систему при использовании Telnet и веб-протоколов требуется проверка пароля анонимного пользователя.

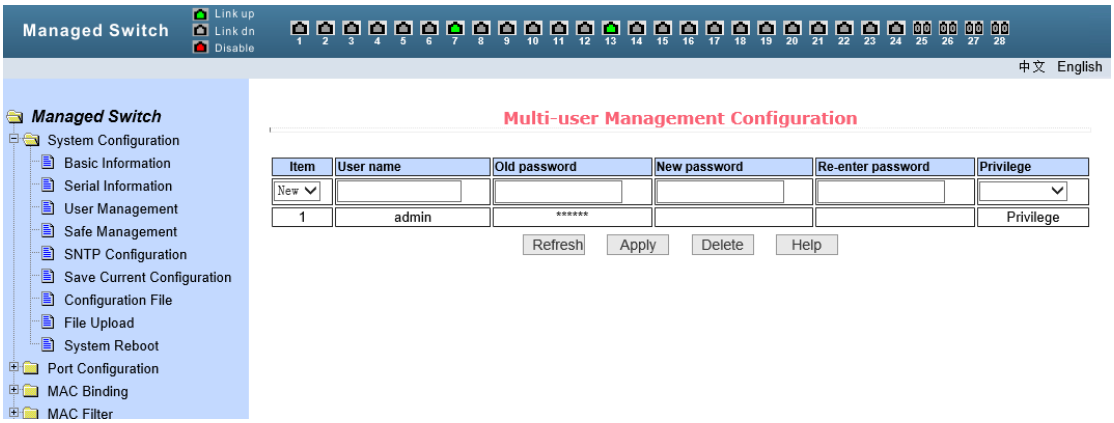


Рисунок 11 – Страница конфигурации многопользовательского управления

(4) Страница конфигурации безопасности пользователя

На рис. 12 показана страница конфигурации безопасности пользователя. Настройки на странице позволяют администратору управлять службами управления сетью TELNET, WEB и SNMP. Вы можете активировать и отключать эти службы. Эти службы могут быть привязаны к группе в списке управления доступом (ACL) стандарта IP для реализации управления по IP-адресу источника, управления доступом хоста к этим службам.

Для коммутатора по умолчанию службы TELNET, WEB и SNMP активированы и не выполняют фильтрацию ACL, то есть все хосты могут получать доступ к этим трем службам коммутатора. Если администратор в целях безопасности не хочет предоставлять другим пользователям одну или несколько из этих служб, он может отключить их. Если администратор хочет предоставить доступ только определенному хосту к одной или нескольким из этих служб, он может выполнить фильтрацию ACL для этих служб. Для выполнения фильтрации ACL необходимо открыть службу и выбрать стандартную группу IP-адресов в ACL (1-99). Группа ACL должна существовать.

Необходимо отметить, что администратор на этой странице управления веб-службами (например, отключив веб-службу) может ограничить использование пользователями веб-страницы. Таким же образом, войдя в систему коммутатора и управляя веб-службами можно открыть пользователям доступ к использованию веб-страницы (например, активировав веб-службу).

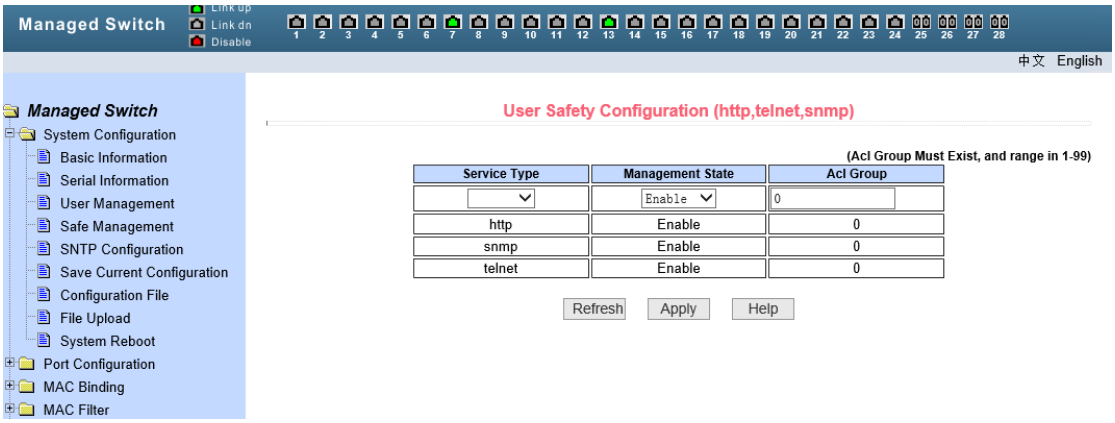


Рисунок 12 – Страница конфигурации безопасности пользователя

(5) Страница конфигурации SNTP

На рис. 13 показана страница конфигурации SNTP, где администратор может настраивать и просматривать системные часы в настройках страницы.

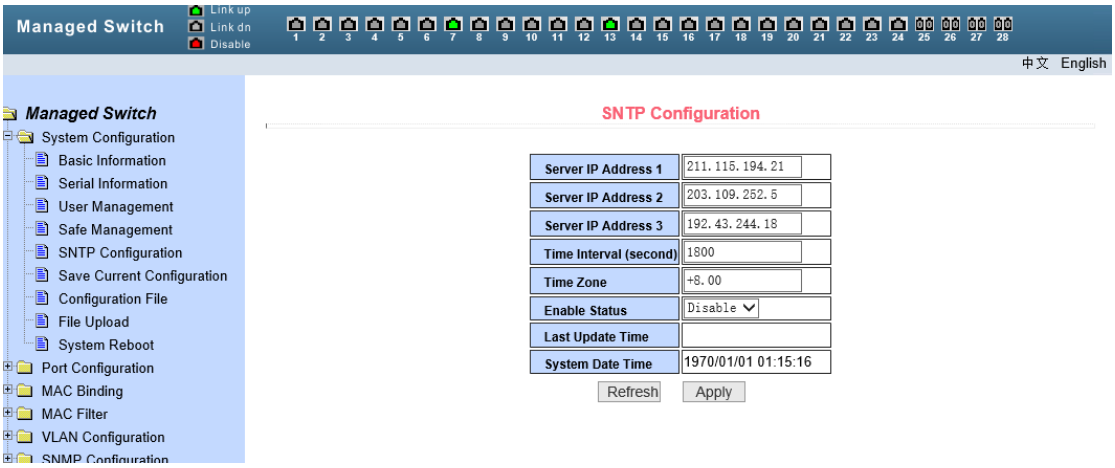


Рисунок 13 – Страница конфигурации SNTP

(6) Страница текущего файла конфигурации

На рис. 14 показана страница текущего файла конфигурации. На этой странице пользователь может просматривать текущую конфигурацию коммутатора. Кнопка "Сохранить" (Save) сохраняет текущую конфигурацию системы в файле конфигурации. Для операции сохранения необходимо стереть информацию во флэш-памяти. Это занимает определенное время. Когда пользователь выполнил настройки на странице и хочет, чтобы конфигурация не потерялась после перезапуска коммутатора, необходимо нажать кнопку "Сохранить" (Save) перед выходом со страницы текущей конфигурации.

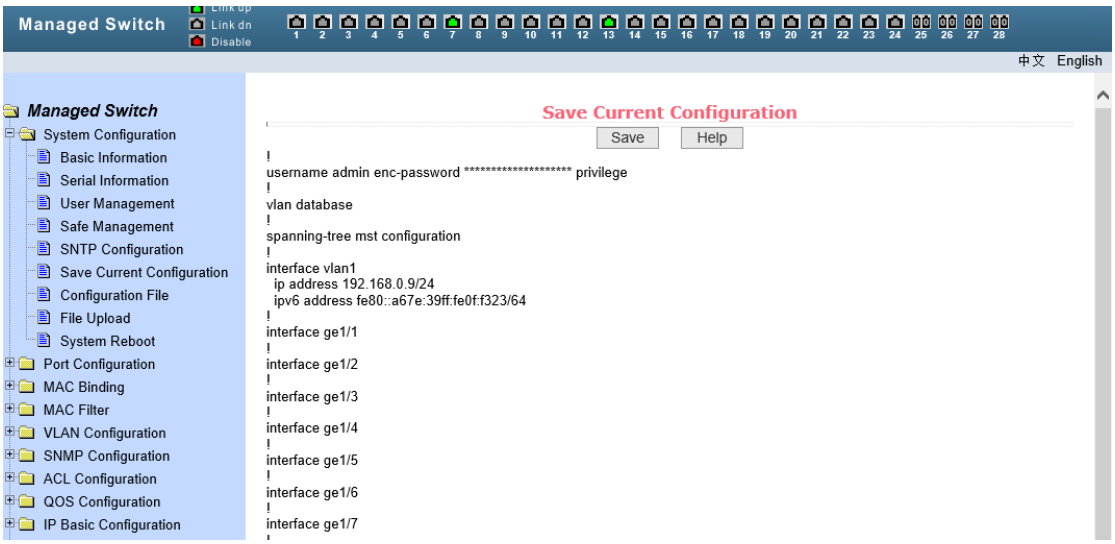


Рисунок 14 – Страница текущего файла конфигурации

(7) Страница файла конфигурации

На рис. 15 показана страница файла конфигурации. Эта страница позволяет пользователю просматривать начальную конфигурацию системы. Начальная конфигурация является текущим файлом конфигурации, сохраненном во флэш-памяти. Если файла конфигурации во флэш-памяти нет, система запускается с конфигурацией по умолчанию. Нажмите кнопку "Удалить" (Delete) для удаления файла конфигурации во флэш-памяти. При нажатии кнопки "Удалить" (Delete), появится диалоговое окно, в котором пользователю будет предложено указать, действительно ли необходимо удалить файл конфигурации. Для удаления нажмите кнопку OK в диалоговом окне, в противном случае нажмите кнопку "Отмена" (Cancel). Для скачивания файла конфигурации на ПК используется кнопка "Скачать" (Download). После нажатия кнопки "Скачать" (Download) появится диалоговое окно, где пользователь может выбрать путь сохранения и сохранить файл конфигурации. Имя загружаемого файла конфигурации — switch.cfg.

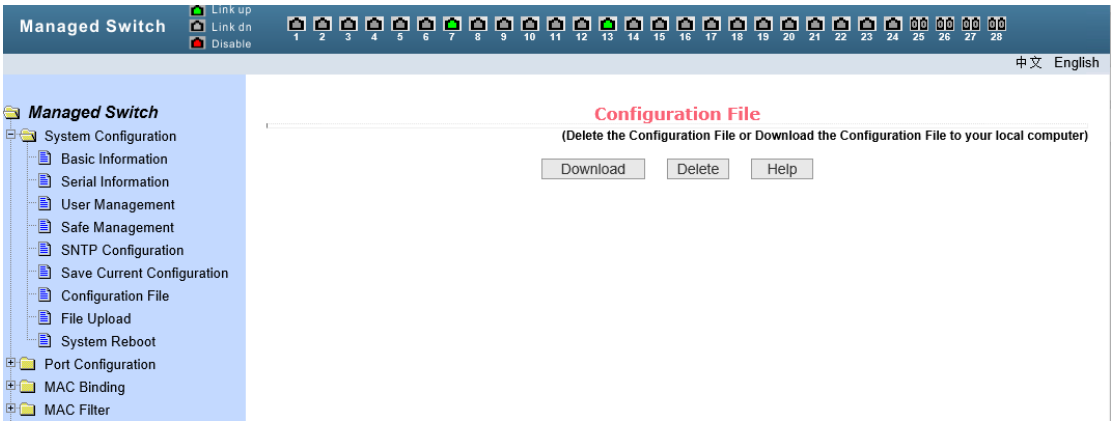


Рисунок 15 – Страница файла конфигурации

(8) Страница загрузки файлов

На рис. 16 показана страница загрузки файлов, через которую пользователи могут загружать файлы конфигурации и файлы изображений на коммутатор. Нажмите кнопку "Обзор" (Browse), чтобы выбрать путь к загружаемому профилю или файлу изображения на ПК. Нажмите кнопку "Загрузить" (Upload), чтобы загрузить файл конфигурации или файл изображения. Суффикс файла конфигурации должен быть *.cfg. Файл изображения должен быть предоставлен производителем, а суффикс имени файла должен быть *.img. Не переходите на другие страницы и не перезагружайте коммутатор до возврата на страницу результатов переноса. В противном случае сбой передачи файлов может привести к сбою системы.

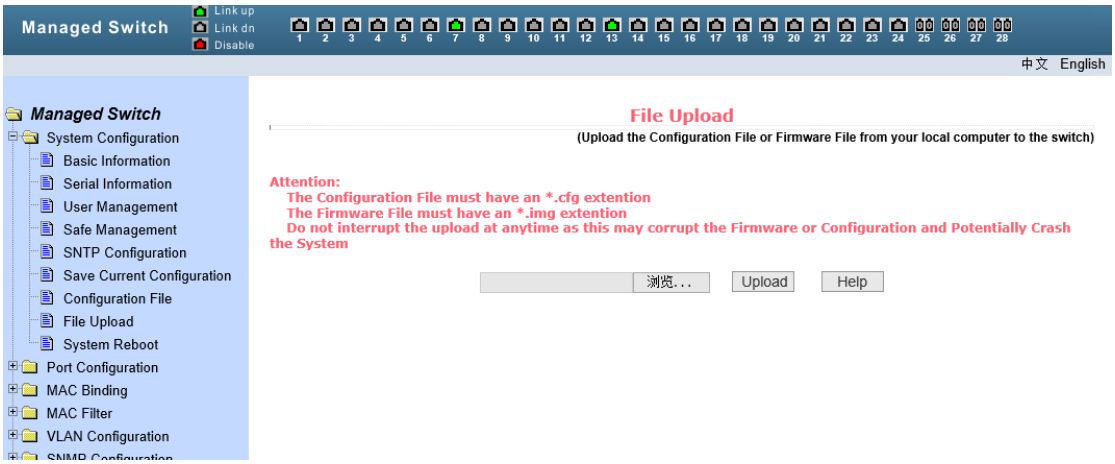


Рисунок 16 — Страница загрузки файлов

(9) Страница перезагрузки системы

На рис. 17 показана страница перезагрузки системы, на которой пользователи могут перезапустить коммутатор. При нажатии кнопки "Перезапуск" (Restart), появится диалоговое окно с запросом, уверен ли пользователь в необходимости перезапуска коммутатора. Если необходимо перезапустить систему, нажмите кнопку OK. В противном случае нажмите кнопку "Отмена" (Cancel). Веб-страница больше не будет открываться при ее перезапуске.

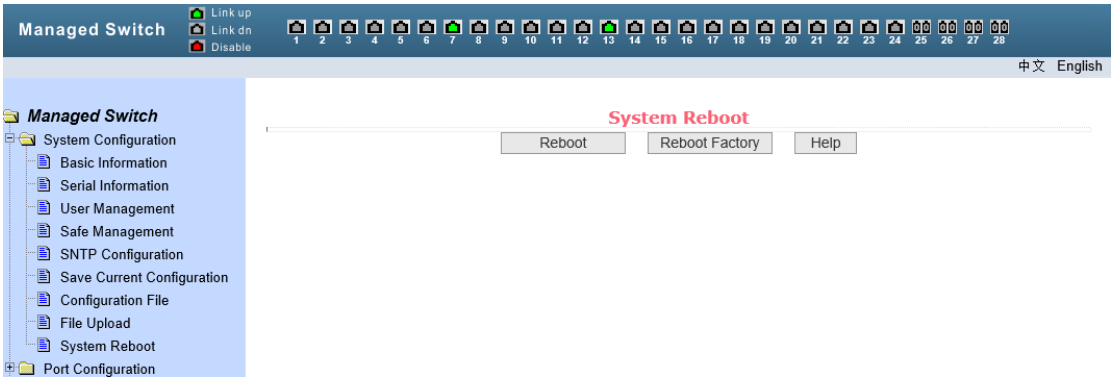


Рисунок 17 – Страница перезапуска системы

4. Конфигурация портов

(1) Страница настройки/отображения состояния портов

На рис. 18 показана страница настройки/отображения состояния портов. На этой странице пользователь может включить или отключить порт, установить скорость передачи данных порта или просмотреть основные сведения обо всех портах.

Для того, чтобы задать определенный порт, выберите соответствующее имя порта в выпадающем меню. Состояние порта (Admin Status) по умолчанию установлено на "вкл." (up), и вы можете выбрать "выкл." (down) в выпадающем меню, чтобы отключить порт. Пользователь также может выбрать настройку в раскрывающемся меню Config speed для настройки скорости порта, например, обязательный полудуплексный режим для 10 мегабитного интерфейса (10 duplex half) и т. д. Пользователи могут просматривать другие основные сведения для всех портов на этой страницы.

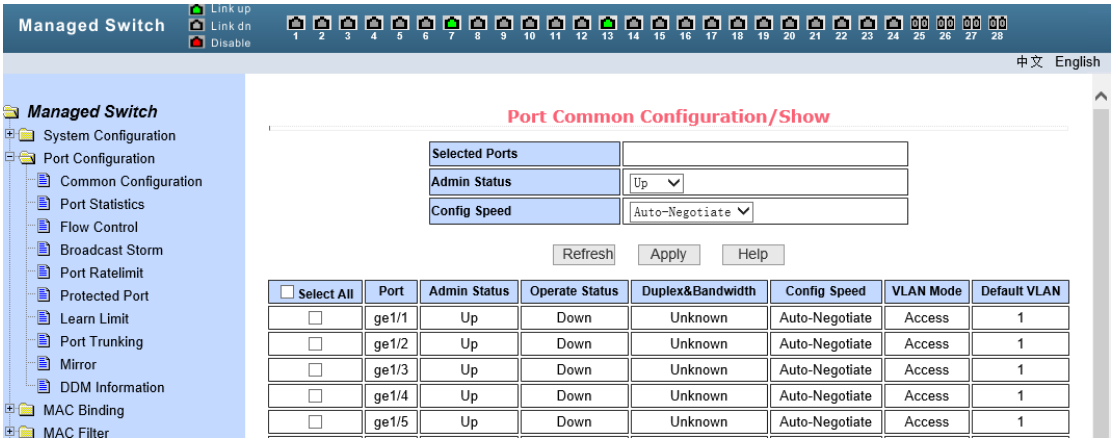


Рисунок 18 Страница настройки/отображения состояния портов

(2) Страница информации о статистике портов

На рис. 19 показана страница информации о статистике порта. Для просмотра данных об определенном порте выберите соответствующее имя порта в выпадающем меню. На этой странице пользователи могут просматривать статистику отправки и получения пакетов данных через порт.

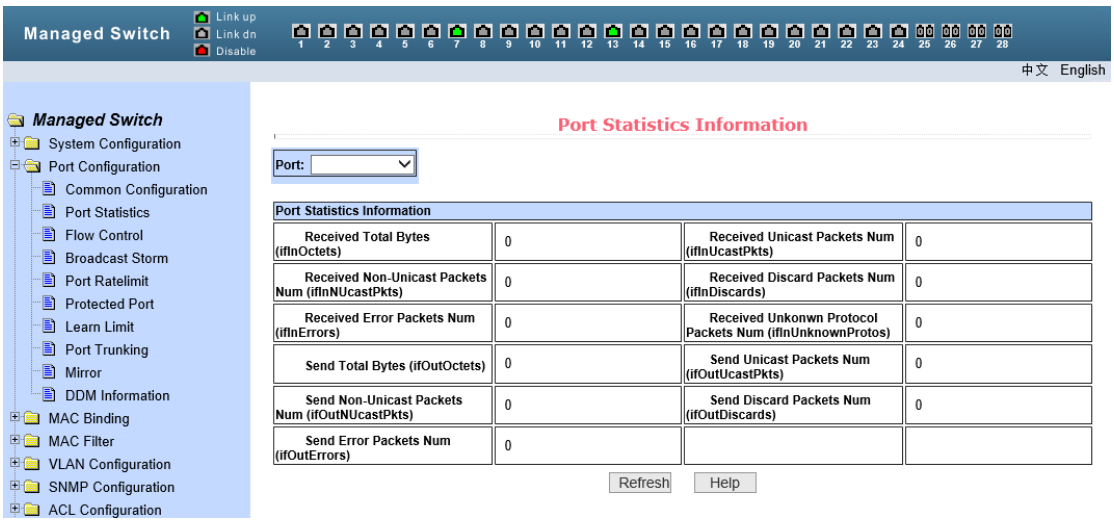


Рисунок 19 – Страница информации о статистике портов

(3) Страница управления потоком данных

На рис. 20 показана страница управления потоком данных. Пользователь может использовать эту страницу, чтобы активировать или отключать управление потоком данных для каждого порта.

Выберите "Включить" (On) или "Отключить" (Off) в раскрывающемся списке, чтобы активировать или отключить управление потоком данных порта. Кроме того, на этой странице вы можете просматривать состояние функции управления потоком данных всех портов.

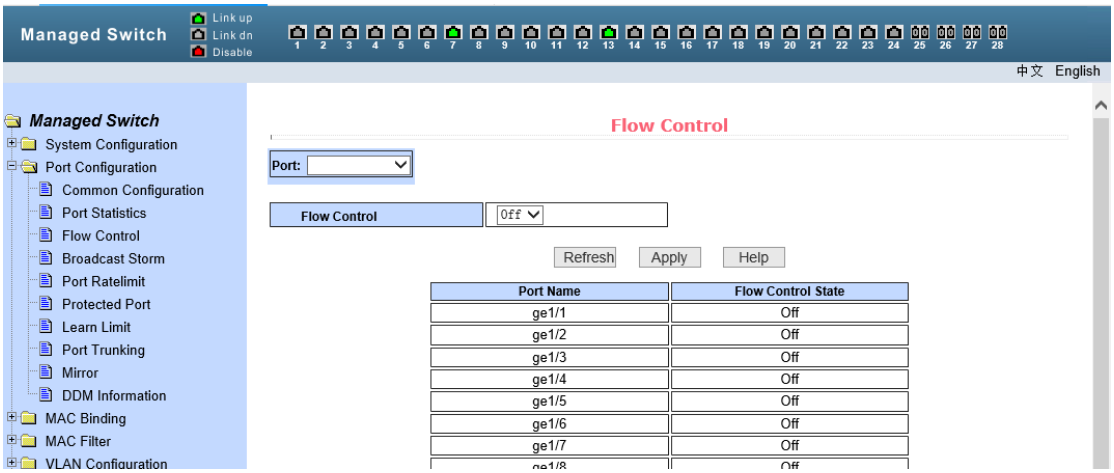


Рисунок 20 – Страница управления потоком данных

(4) Страница управления зацикливанием широковещательных передач

На рис. 21 показана страница управления зацикливанием широковещательных передач. Эта страница используется для настройки подавления пакетов широковещательной рассылки, пакетов многоадресной рассылки и пакетов DLF на порту.

Выберите порт, который необходимо настроить, из выпадающего списка портов. Выберите "Включить" (On) или "Отключить" (Off), чтобы активировать или отключить подавление пакетов широковещательной рассылки, пакетов многоадресной рассылки и пакетов DLF на порту. Термин "скорость подавления" используется для настройки скорости подавления порта в диапазоне 1–1024000 кбит. Скорости подавления пакетов широковещательной рассылки, пакетов многоадресной рассылки и пакетов DLF на одном и том же порту равны. Кроме того, на этой странице вы можете просматривать информацию о конфигурации управления зацикливанием широковещательных передач для всех портов.

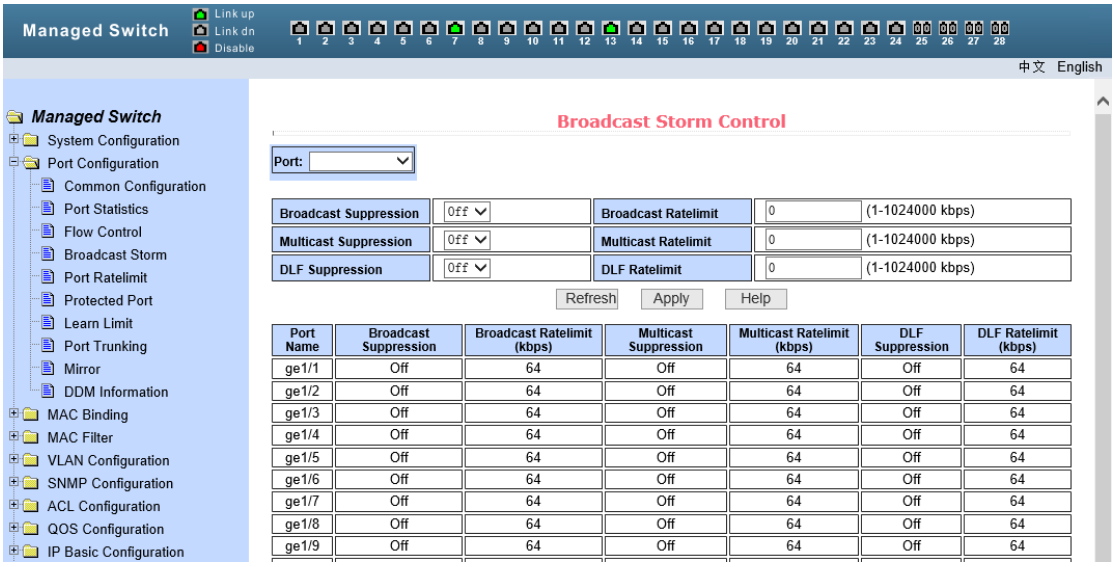


Рисунок 21 – Страница управления зацикливанием широковещательных передач

(5) Страница ограничения скорости передачи данных порта

На рис. 22 показана страница ограничения скорости передачи данных порта. Эта страница используется для настройки скорости отправки и приема данных портов.

Выберите порт, который необходимо настроить, из выпадающего списка. Управление пропускной способностью при передаче пакетов используется для настройки и отображения значений управления пропускной способностью при отправке пакетов данных в диапазоне 1–1024000 кбит. После ввода нажмите кнопку "Применить" (Apply), чтобы изменения вступили в силу.

Если в настройках порта не активирован контроль пропускной способности, он отображается как выключенный (Off). Соответствующая кнопка "Отмена" (Cancel) используется для отмены управления пропускной способностью при отправке пакетов данных (Send Packets Rate Control). Управление пропускной способностью для приема пакетов данных (Receive Packets Rate Control) используется для настройки и отображения управления пропускной способностью при приеме пакетов данных в диапазоне 1—1024000 кбит. После ввода нажмите кнопку "Применить" (Apply), чтобы изменения вступили в силу. Если в настройках порта не активировано управление пропускной способностью, он отображается как выключенный (Off). Соответствующая кнопка "Отмена" (Cancel) используется для отмены управления пропускной способностью при приеме пакетов данных (Send Packets Rate Control).

Если для порта активировано контролем пропускной способностью, он будет отображаться в списке.

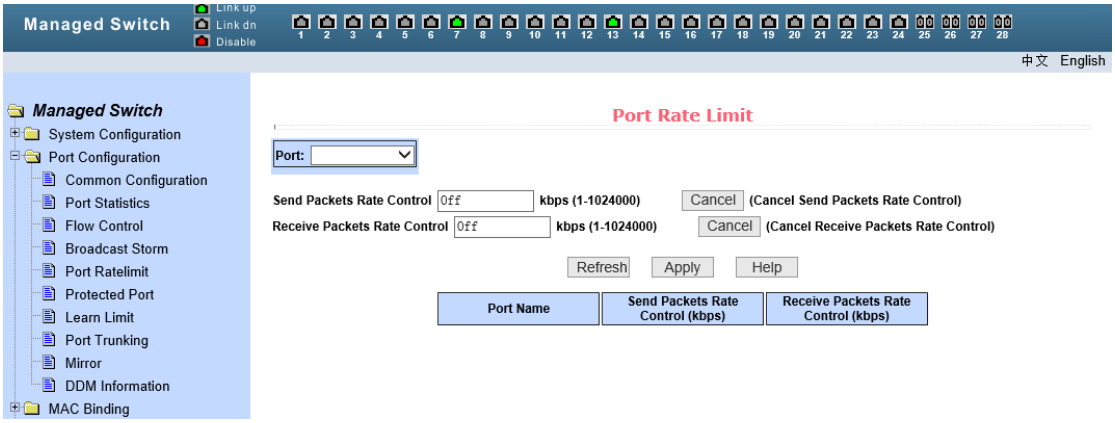


Рисунок 22 – Страница ограничения скорости передачи данных порта

(6) Страница защищенных портов

На рис. 23 показана страница защищенных портов. Эта страница используется для настройки защиты портов.

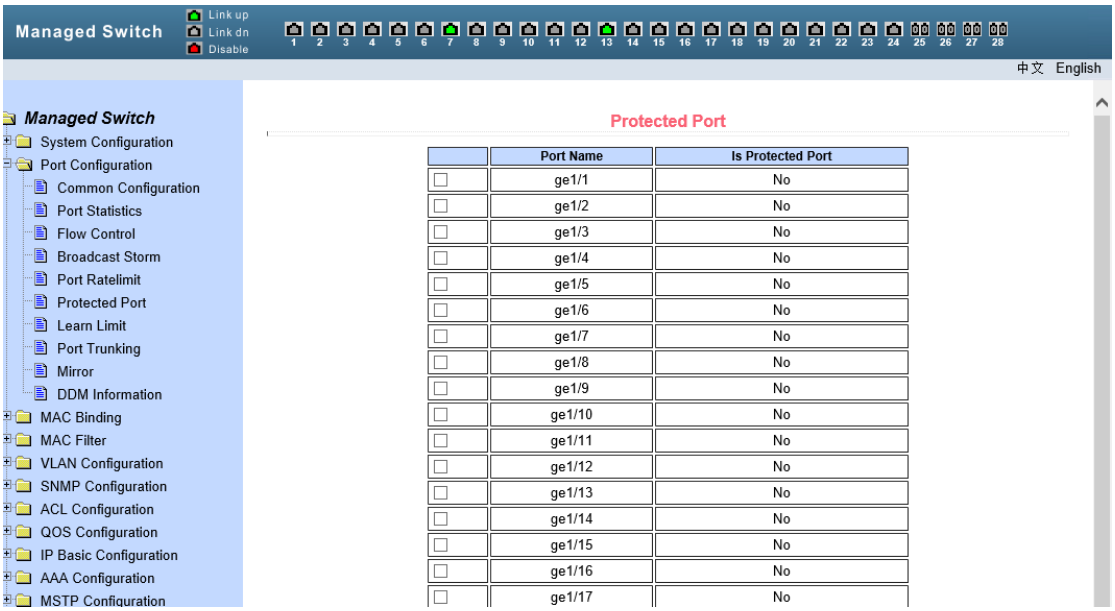


Рисунок 23 – Страница защищенных портов

(7) Страница ограничения памяти адресов портов

На рис. 24 показана страница ограничения памяти адресов портов. Эта страница используется для ограничения количества MAC-адресов, которые может запомнить порт. Диапазон значений: 0—8191. Значение по умолчанию равно 8191, что также является максимальным значением, указывающим на отсутствие установленного ограничения памяти порта. В списке отображаются ограничения памяти для всех портов.

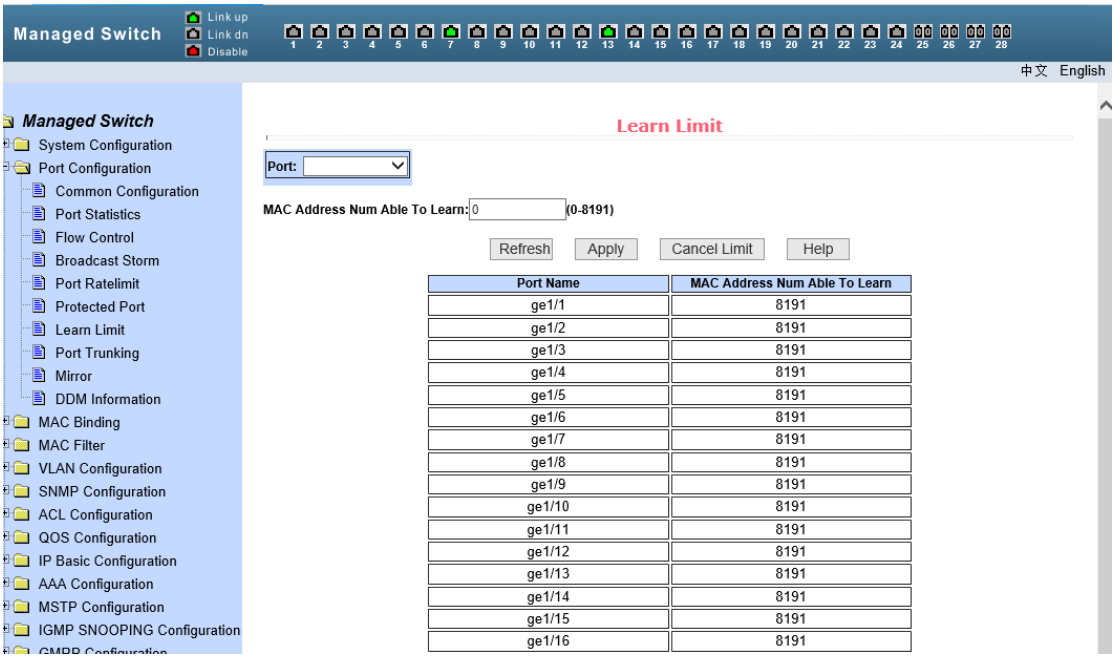


Рисунок 24 – Страница ограничения памяти адресов портов

(8) Страница настройки объединения портов

На рис. 25 показана страница настройки объединения портов. На этой странице пользователь может настроить группирование портов. Страница состоит из четырех частей: выбор идентификатора группы портов (Trunk Group ID), настройка метода группирования (Trunk Method), настраиваемый порт (Able Config Port) и порт в группе (Member Port).

Для создания или изменения группы портов пользователю необходимо выбрать идентификатор группы (1–8). Пользователь должен нажать на соответствующий идентификатор группы портов в поле списка. Информация о группе портов отображается в поле "Порт в группе" (Member Port). Для создания группы портов, выберите соответствующий идентификатор в перечне идентификаторов групп портов, нажмите кнопку "Создать группу портов" (Create Trunk Group). В случае успешного создания группы на панели отображения идентификатора в скобках рядом с соответствующим идентификатором указывается "Создан" (Created). Если группа портов не создана, в скобках рядом с соответствующим идентификатором указывается "Не создан" (Uncreated). Для того, чтобы задать метод группирования портов, выберите метод группирования в раскрывающемся списке и нажмите кнопку "Настроить метод

группирования" (Set Trunk Method). Для выбора порта для группирования выберите соответствующий порт в поле "Настраиваемый порт" (Able Config Port) и нажмите кнопку "Добавить порт в группу =>" (Member Port =>). Для удаления порта из существующей группы, выберите порт в поле "Порт в группе" (Member Port) и нажмите кнопку "Удалить порт из группы <=" (Unmember Port <=). Для удаления целой группы портов нажмите кнопку "Удалить группу портов" (Delete Trunk Group).

В процессе настройки страницы метод группирования настраивается таким образом, чтобы соответствовать выбранному идентификатору группы портов. Для существующей группы портов можно настроить метод группирования. Вы можете добавлять порты в существующую группу или удалять их из нее. Если в группе не остается хотя бы одного порта, группа удаляется.

Коммутатор обеспечивает шесть типов группирования портов: на основе MAC-адреса источника, на основе MAC-адреса назначения, на основе MAC-адресов источника и назначения, на основе IP-адреса источника, на основе IP-адреса назначения, на основе IP-адресов источника и назначения.

Коммутатор поддерживает до восьми групп группирования портов. Каждая группа группирования поддерживает до восьми портов. Для каждой группы портов можно настроить собственный метод группирования портов.

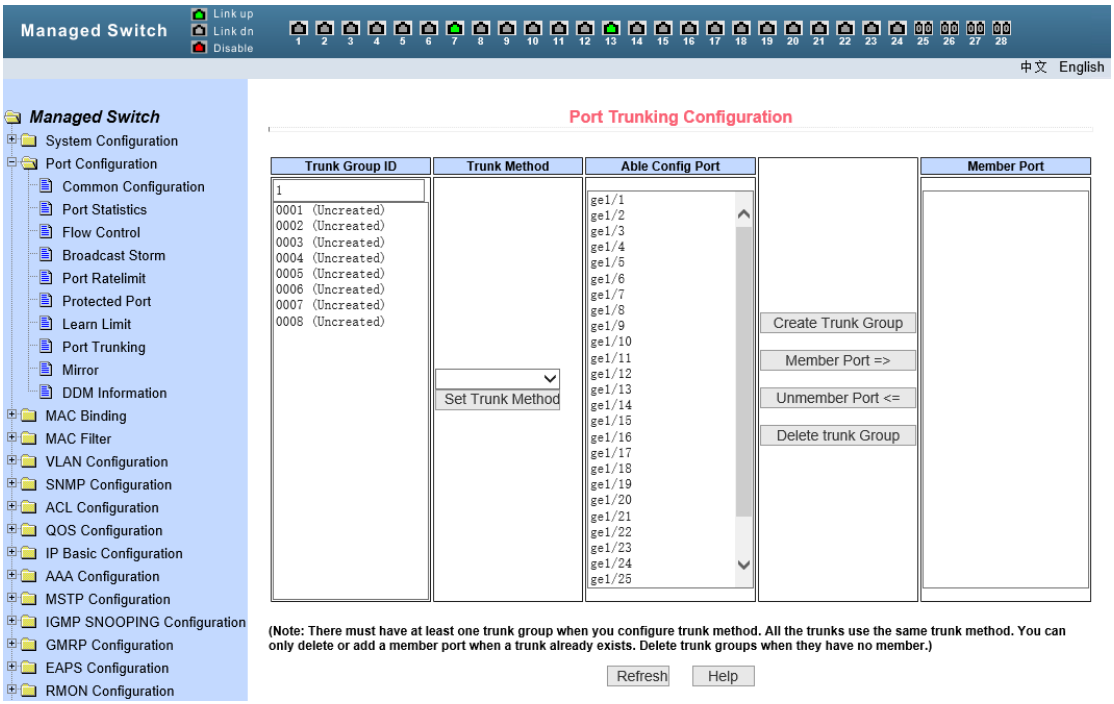


Рисунок 25 – Страница настройки объединения портов

(9) Страница конфигурирования зеркального отражения портов

На рис. 26 показана страница конфигурирования зеркального отражения портов. Эта страница позволяет пользователю настраивать зеркальное отражение портов. Зеркальное отражение портов осуществляется через порт зеркалирования для мониторинга выходных данных зеркального выходного порта и входных пакетов зеркального входного порта. В качестве порта зеркалирования можно выбрать только один порт, а зеркальных выходных портов и зеркальных входных портов может быть выбрано несколько. Страница состоит из четырех частей: порт прослушивания, настраиваемый порт, направление прослушивания и информация о конфигурировании зеркального отображения. Выберите порт для зеркалирования в поле Mirror Port для создания зеркального порта с порта прослушивания. В качестве порта прослушивания можно выбрать только один порт. Выберите зеркальный порт из списка настраиваемых портов (Able Config Mirrored Ports), выберите направление прослушивания в поле "Направление прослушивания" (Mirror Direction) и нажмите кнопку "Применить" (Apply). В результате будет отображена информация о конфигурировании зеркального отображения в поле Mirror Config Info.

Когда в качестве направления прослушивания выбран ПРИЕМ (RECIEVE), это указывает на то, что пакет принят, ПЕРЕДАЧА (TRANSMIT) указывает на отправку пакета, ПРИЕМ И ПЕРЕДАЧА (BOTH) указывает на все пакеты, которые отправляются и принимаются, НЕ_ПОЛУЧЕН (NOT_RECEIVE) указывает на то, что прием пакета отменен, НЕ_ПЕРЕДАН (NOT_TRANSMIT) указывает на то, что отправка пакета отменена, НИЧЕГО (NEITHER) отменяет мониторинг получаемых и отправляемых пакетов, то есть отменяет прослушивание.

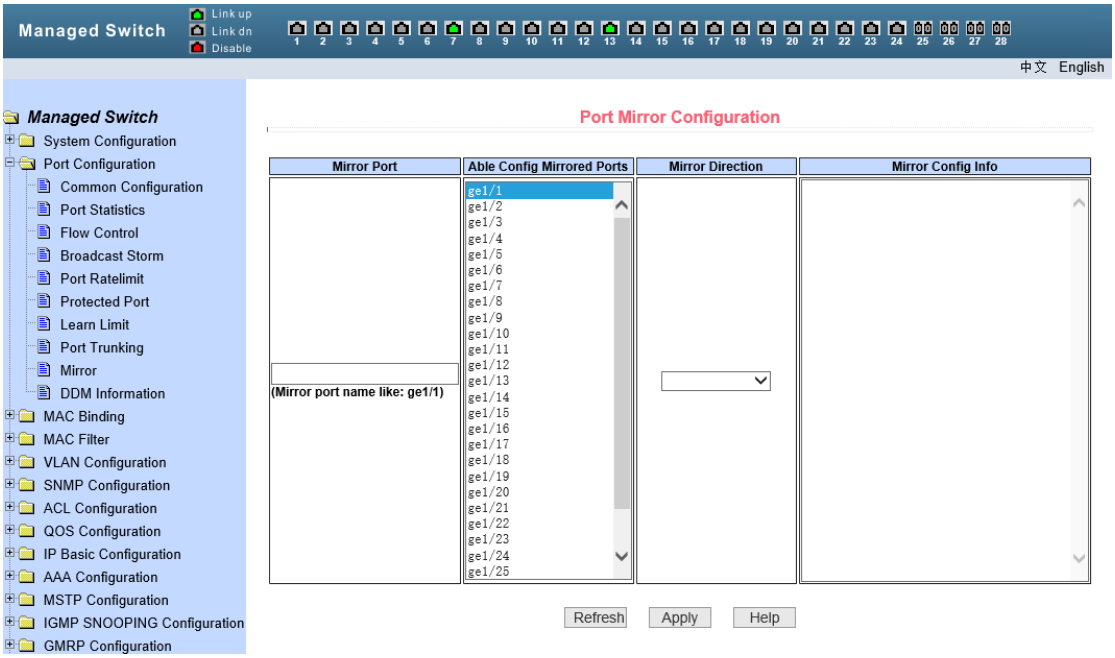


Рисунок 26 – Страница конфигурирования зеркального отражения портов

(10) Информация о DDM

Используя интеллектуальный оптический модуль, блок управления сетью может контролировать температуру, напряжение питания, ток смещения лазера, а также передающую и принимающую оптическую мощность модуля приемопередатчика в режиме реального времени. Измерение этих параметров может помочь блоку управления определить место возникновения неисправности в оптоволоконной линии связи, упростить работы по техническому обслуживанию и повысить надежность системы.

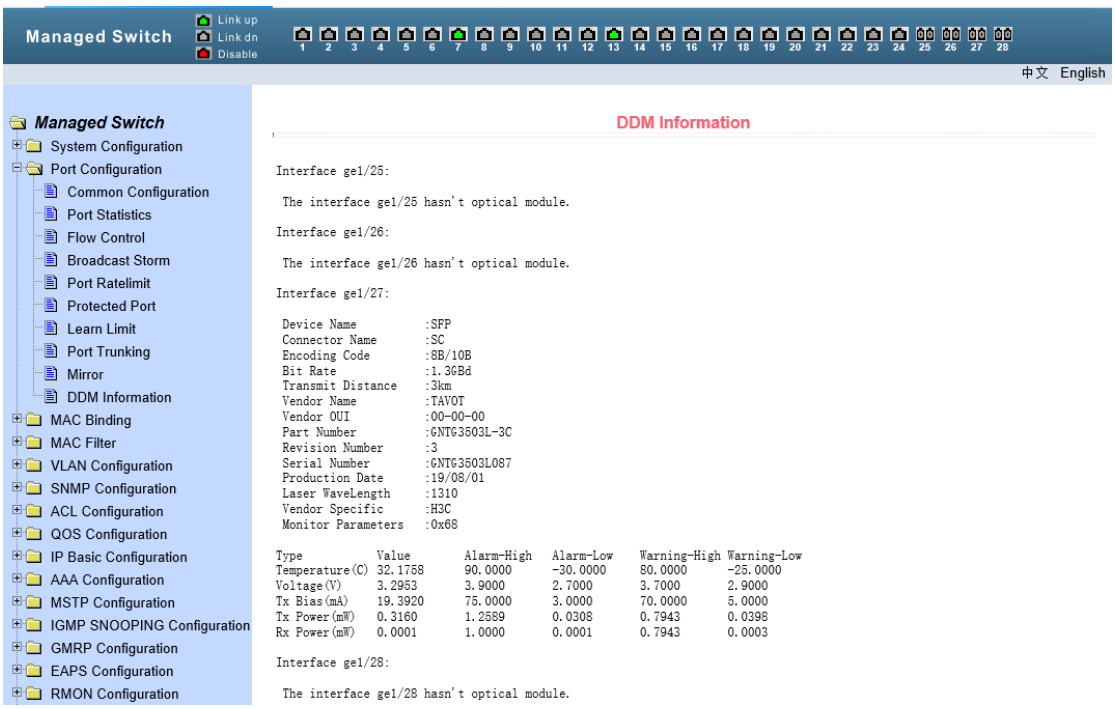


Рисунок 27 – Сведения о DDM

5. Привязка MAC-адресов

(1) Страница конфигурирования привязки MAC-адресов

На рис. 28 показана страница конфигурирования привязки MAC-адресов. Эта страница используется для привязки порта к MAC-адресу.

Поле "MAC-адрес" (MAC Address) на странице используется для ввода привязанного MAC-адреса. Поле "Идентификатор VLAN" (VLAN ID) используется для ввода VLAN, к которой принадлежит MAC-адрес.

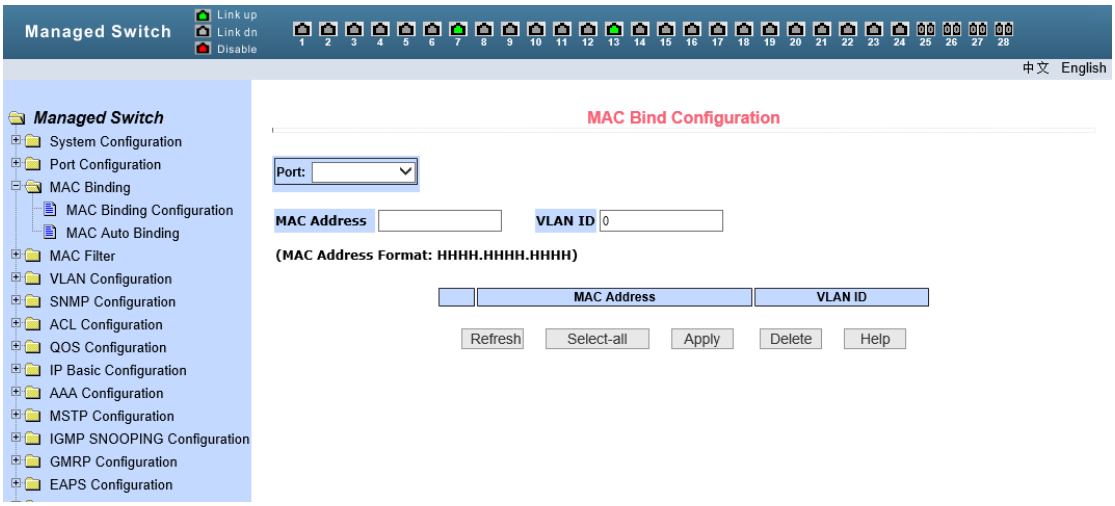


Рисунок 28 – Страница конфигурирования привязки MAC-адресов

(2) Страница автоматической привязки MAC-адресов

На рис. 29 показана страница автоматического преобразования привязки MAC-адресов. Эта страница используется для реализации автоматической привязки MAC-адреса к порту.

Отображает динамический MAC-адрес и VLAN порта в таблице двухуровневой аппаратной переадресации. Вы можете выбирать в них элементы и преобразовывать их в статические привязки.

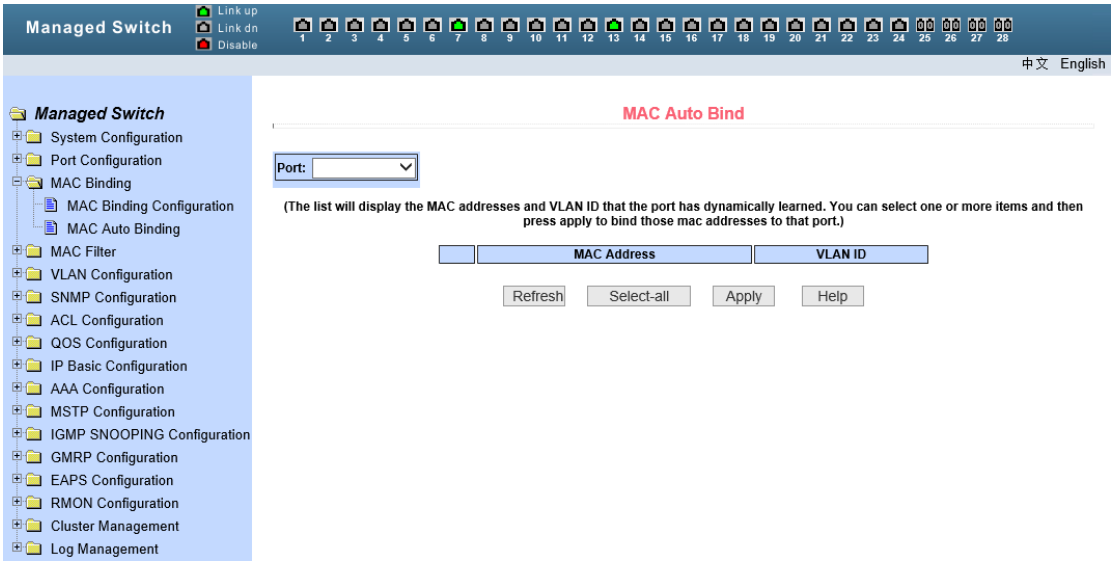


Рисунок 29 – Страница автоматической привязки MAC-адресов

6. MAC-фильтр

(1) Страница конфигурирования MAC-фильтра

На рис. 30 показана страница конфигурирования MAC-фильтра. Эта страница используется для настройки порта для фильтрации по MAC-адресам.

Поле "MAC-адрес" (MAC Address) на странице используется для ввода MAC-адреса, подлежащего фильтрации. Поле "Идентификатор VLAN" (VLAN ID) используется для ввода VLAN, к которой принадлежит MAC-адрес.

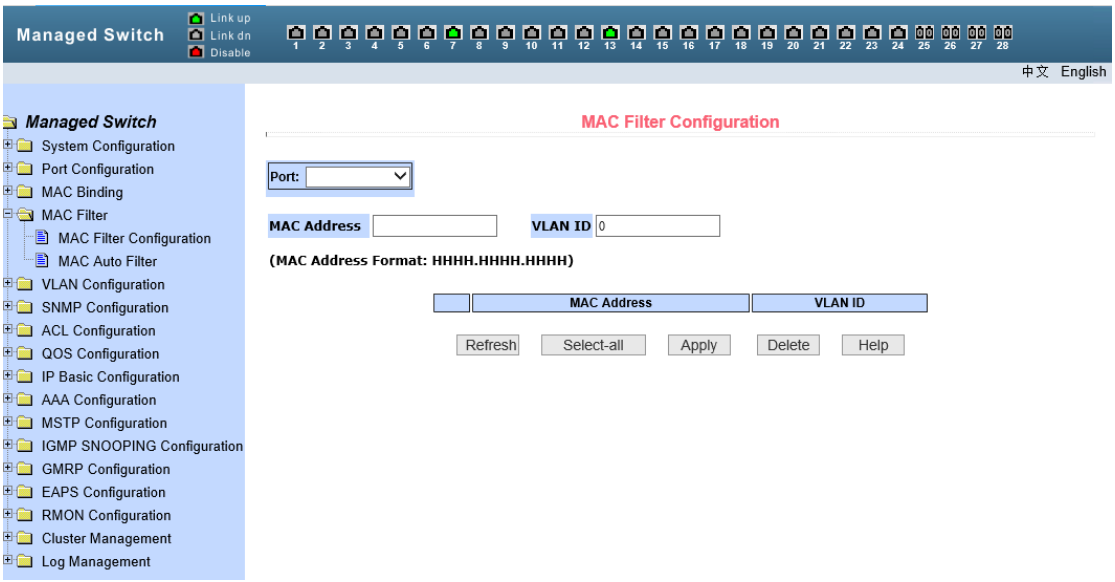


Рисунок 30 – Страница конфигурирования MAC-фильтра

(2) Страница автоматического MAC-фильтра

На рис. 31 показан MAC-фильтр, автоматически преобразующий страницу. Эта страница используется для реализации автоматической привязки MAC-адреса к порту.

Отображает динамический MAC-адрес и VLAN, связанные с портом, в таблице аппаратной переадресации уровня 2. Вы можете выбрать запись и преобразовать ее в конфигурацию статического фильтра.

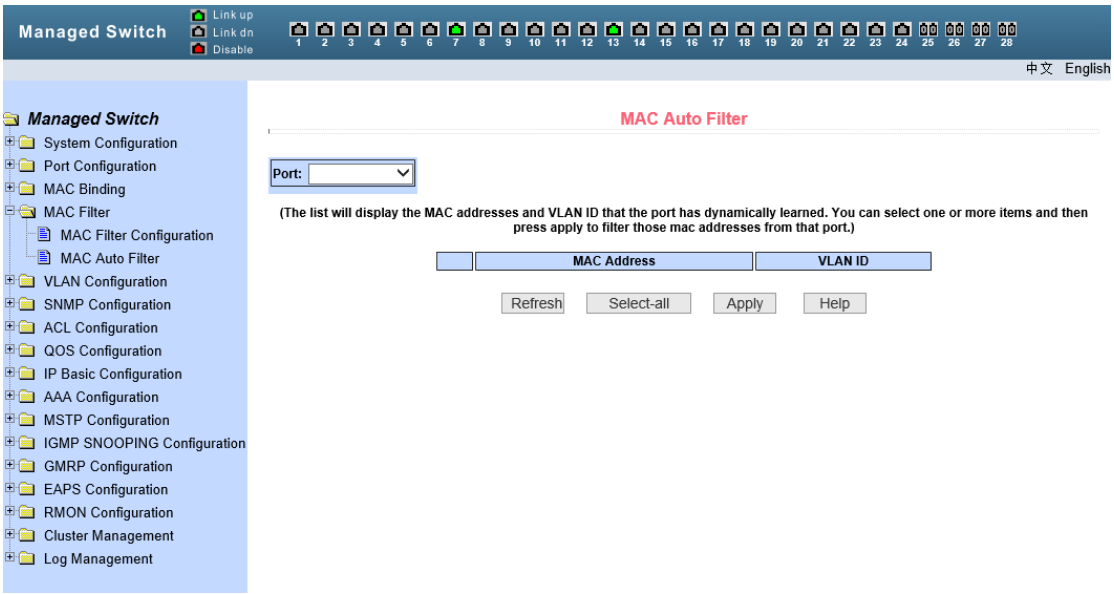


Рисунок 31 – Страница автоматического MAC-фильтра

7. Конфигурирование VLAN

(1) Страница со сведениями о VLAN

На рис. 32 показана страница с сведениями о текущей сети VLAN. Страница доступна только для чтения, на ней отображаются текущая сеть VLAN, состояние VLAN и порты в сети VLAN. В раскрывающемся списке отображаются все текущие сети VLAN, в списке отображается до 30 идентификаторов VLAN (VID), состояние сети и порты в ней. Выберите VLAN из выпадающего списка, и в списке отобразится информация по VID, для которого есть более 30 VLAN. Но если общее количество VLAN не более 30, независимо от выпадающего списка для выбора VLAN, вся информация о VLAN будет показана в списке.

Порт не может быть частью VLAN, независимо от наличия метки. На странице отображаются следующие символы:

t с меткой Порт является помеченным участником этой VLAN

u без метки Порт не является помеченным участником этой VLAN

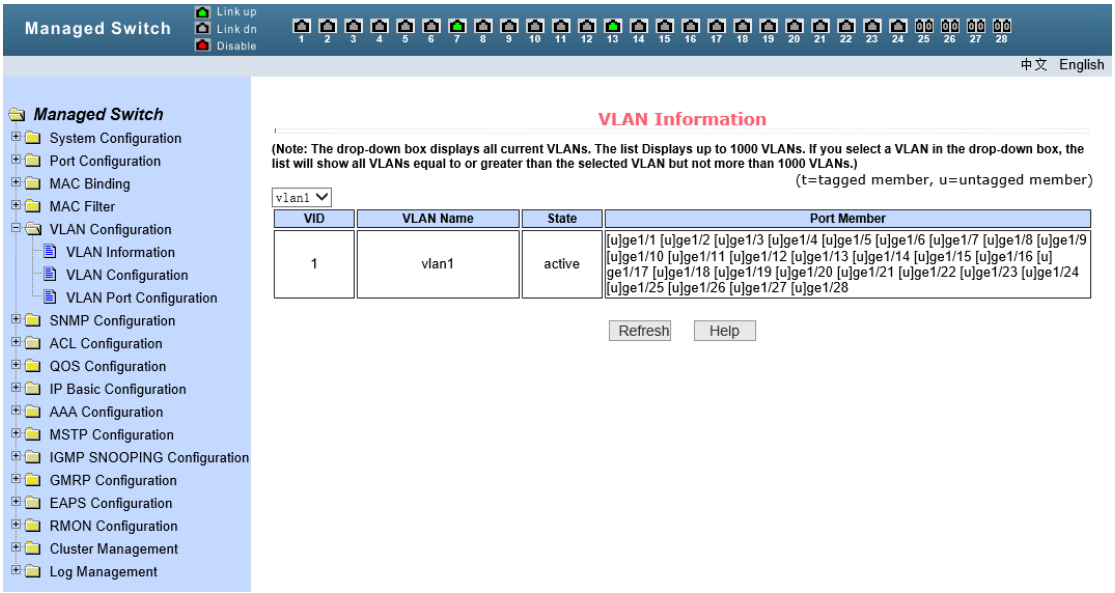


Рисунок 32 – Страница сведений о VLAN

(2) Страница соответствия статической VLAN

На рис. 33 показана страница конфигурации статической VLAN, которая позволяет пользователям создавать VLAN.

Если вы хотите создать новую VLAN, пользователь должен ввести VID в активной строке в диапазоне от 2 до 4094. Имя VLAN генерируется системой в соответствии с идентификатором VLAN и не может быть изменено. Нажмите кнопку "Применить" (Apply),

и в окне списка отобразится VID и имя VLAN, созданной пользователем. Коммутатор создает VLAN 1 по умолчанию, и VLAN 1 нельзя удалить.

Если вы хотите удалить VLAN, пользователь должен нажать на соответствующую VLAN в списке. VLAN будет отображаться в активной строке. Нажмите кнопку "Удалить" (Delete), чтобы удалить VLAN, и информация о VLAN будет удалена из списка.

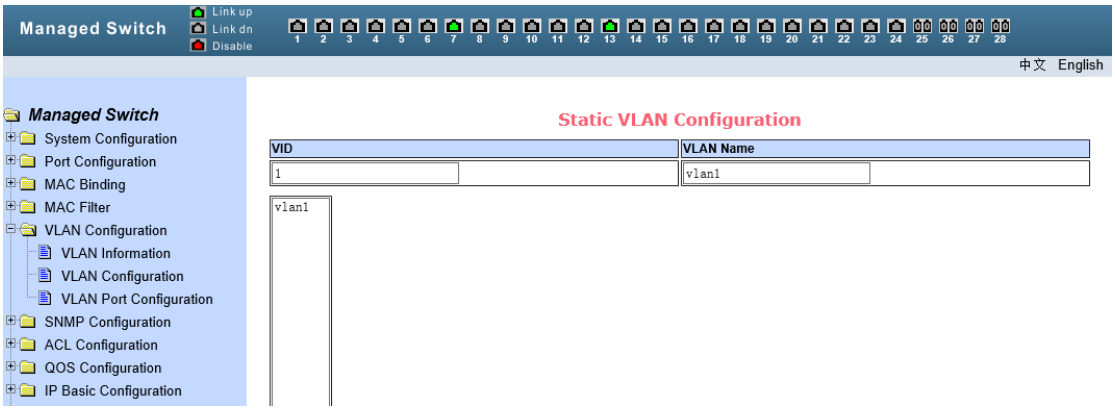


Рисунок 33 – Страница конфигурации статической VLAN

(3) Страница конфигурации порта VLAN

На рис. 34 показана страница конфигурации порта VLAN, которая используется для настройки VLAN на порту и отображения результатов настройки. Страница состоит из восьми частей: порт, режим, все текущие VLAN, порты, принадлежащие VLAN, "VLAN по умолчанию =>", "с меткой =", "без метки =>" и "не является участником <=".

Порт – это порт, который определяет VLAN, подлежащую настройке.

Режим. Порт определяет режим VLAN порта в качестве режима ДОСТУПА (ACCESS). В этом режиме VLAN порт по умолчанию используется для участников VLAN1 без меток. VLAN порта по умолчанию – 1. Режим VLAN гибридного порта - это ГИБРИДНЫЙ (HYBRID) режим. В этом режиме VLAN порт является участником VLAN1 без метки, а VLAN порта по умолчанию – 1. Режим VLAN объединенного порта — это режим объединения (TRUNK). В этом режиме VLAN порт по умолчанию является участником VLAN1 с меткой, а VLAN порта по умолчанию — 1.

Все текущие VLAN – это VLAN, которые могут быть созданы портом. Пользователи могут выбирать VLAN из списка.

Порт принадлежит VLAN, чтобы показать результат настройки порта VLAN. [P] указывает, что VLAN является VLAN порта по умолчанию. [T] указывает, что порт является участником VLAN с меткой. [U] указывает, что порт является участником VLAN без метки. Для удаления VLAN пользователю необходимо выбрать VLAN из списка.

Нажмите VLAN по умолчанию => Настройте VLAN порта по умолчанию и выберите VLAN из всех текущих VLAN.

Нажмите "С меткой =>" (Tagged =>), чтобы настроить порт как участника указанной VLAN с меткой, и выберите одну или несколько VLAN из всех текущих VLAN.

Нажмите "Без метки =>" (Untagged =>), чтобы настроить порт как участника указанной VLAN без метки, и выберите одну или несколько VLAN из всех текущих VLAN.

Кнопка "Удалить из участников <=" (Unmember <=) удаляет порт из указанной одной или нескольких VLAN таким образом, что он больше не является участников этих VLAN, и выбирает одну или несколько VLAN из VLAN, к которой принадлежит порт.

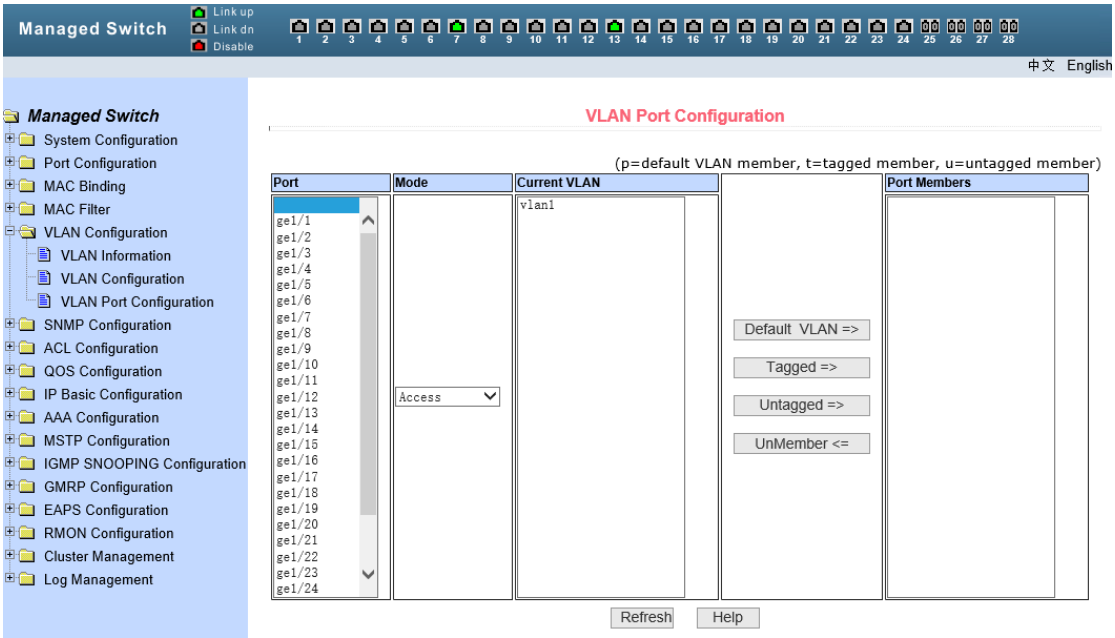


Рисунок 34 – Страница конфигурации порта VLAN

8. Конфигурация SNMP

(1) Страница конфигурации SNMP community

На рис. 35 показана страница конфигурации SNMP community, которая позволяет пользователю настраивать имя коммутатора и разрешения на чтение и запись. Всего можно настроить до восьми записей.

По умолчанию коммутатор имеет общедоступное имя общего тела, общее тело имеет разрешения только для чтения. В соответствии с этим на странице есть только одна активная запись, общее имя является общедоступным, а разрешения доступны только для чтения. Когда коммутатор необходимо подключить к сети через SNMP, вам необходимо настроить community (т. е. пароль), для доступа к чтению и записи.

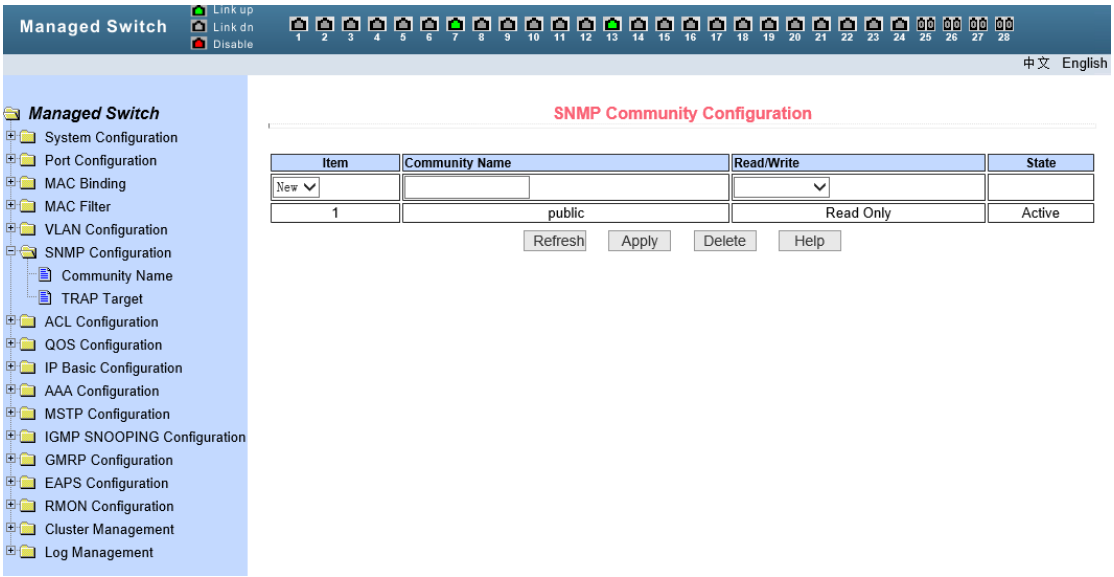


Рисунок 35 – Страница конфигурации SNMP community

(2) Страница конфигурации целей трапов

На рис. 36 показана страница конфигурации целей трапов (trap targets), которая позволяет пользователю настроить IP-адрес рабочей станции, получившей трап-сообщение, и

Некоторые параметры пакета протокола TRAP.

При настройке записи имя используется для ввода имени трапа. IP-адрес используется для ввода адреса назначения. Версия SNMP используется для выбора версии пакета-трапа. Если настройка выполнена успешно, статус в записи будет отображаться как активный. Если настройка выполнена успешно, функция SNMP TRAP активируется. В случае организации восходящего или нисходящего канала связи коммутатор автоматически отправит трап-пакет на адрес назначения.

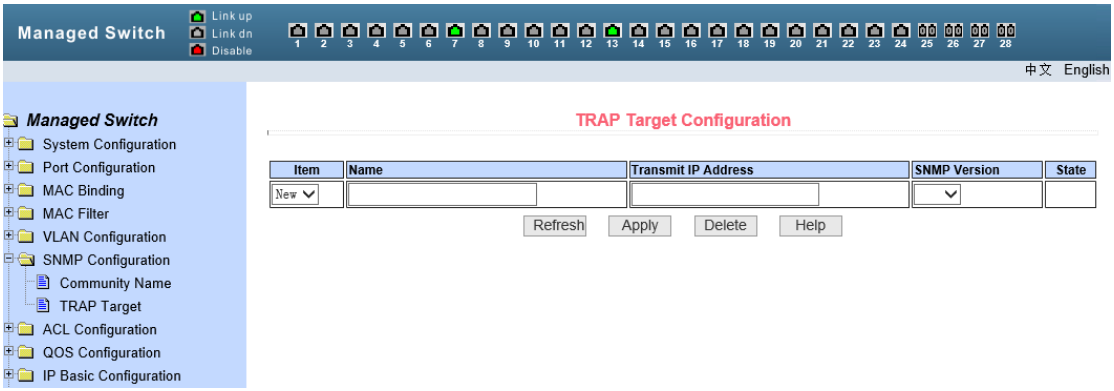


Рисунок 36 – Страница конфигурации целей трапов

9. Конфигурация ACL

(1) Страница конфигурации стандартного ACL по IP-адресам

На рис. 37 показана страница конфигурации стандартного ACL по IP-адресам. Вы можете использовать эту страницу для создания базы правил для стандартного ACL по IP-адресам. Пользователь может выбрать номер группы ACL (диапазон от 1–99 или 1300–1999), чтобы создать одно или несколько правил в группе. Поля, которые могут быть сопоставлены в правиле, имеют только IP-адреса источника (с маской).

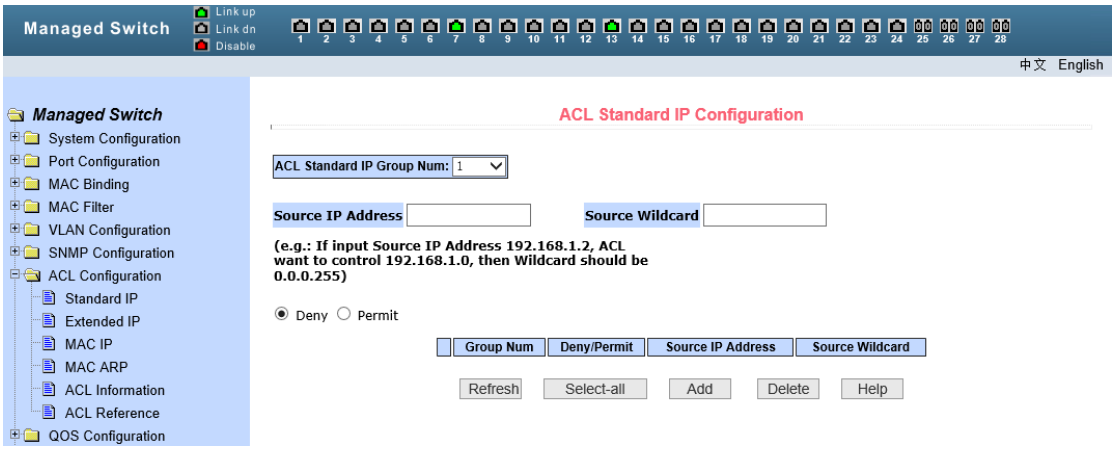


Рисунок 37 – Страница стандартной конфигурации ACL по IP-адресам

Когда пользователь настраивает правило, IP-адрес источника должен иметь маску. Правило может соответствовать набору IP-адресов. Адресная маска представлена антикодом. Если правило соответствует диапазону IP-адресов от 192.168.0.0 до 192.168.0.255, IP-адрес может быть 192.168.0.1, а его маска — 0.0.0.255.

Когда пользователь настраивает правило, каждое правило должно иметь режим фильтрации: разрешить или запретить.

Когда пользователь создает правило в группе правил, система автоматически присваивает правилу номер. Когда правило в группе правил удаляется, другие правила не изменяются, и система автоматически назначает правило для сортировки по группе правил. Если вы хотите удалить всю группу правил, вы можете выбрать все правила, нажав кнопку "Выбрать все" (Select all), а затем нажать кнопку "Удалить" (Delete).

(2) Страница расширенной конфигурации ACL по IP-адресам

На рис. 38 показана страница расширенной конфигурации ACL по IP-адресам. Вы можете использовать эту страницу для создания базы правил для расширения ACL по IP-адресам. Пользователь может выбрать номер группы ACL (между 100–199 или 2000–2699), чтобы создать одно или несколько правил в группе (например, ICMP, TCP, UDP и т.д.), порт источника и порт назначения (только TCP и UDP). IP-адрес источника (с маской), IP-адрес назначения (с маской), тип протокола (например, ICMP, TCP, UDP и т.д.) (допустимый протокол), флаг управления TCP.

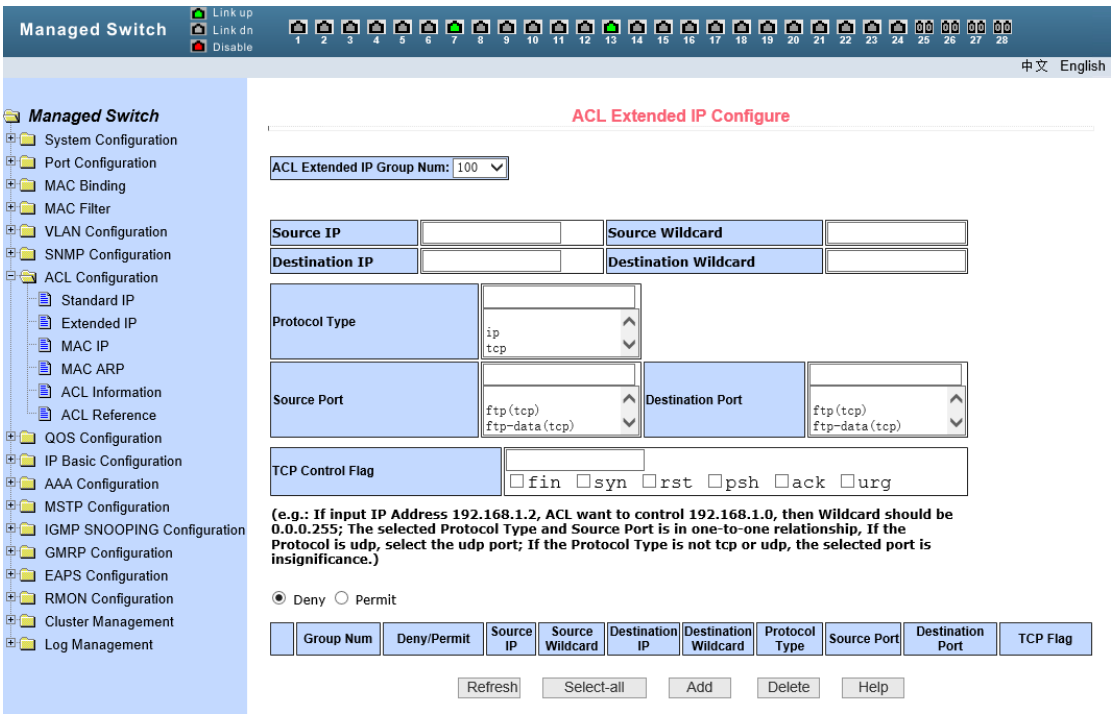


Рисунок 38 – Страница расширенной конфигурации ACL по IP-адресам

Когда пользователь настраивает правило, IP-адрес источника и IP-адрес назначения должны иметь маски. Правило может соответствовать набору IP-адресов.

Адресная маска представлена антикодом. Если правило соответствует диапазону IP-адресов от 192.168.0.0 до 192.168.0. 255, IP-адрес может быть 192.168.0.1, а маска — 0.0.0.255.

Когда пользователь настраивает правило, каждое правило должно иметь режим фильтрации: разрешить или запретить.

Когда пользователь создает правило в группе правил, система автоматически присваивает правилу номер. Когда правило в группе правил удаляется, другие правила не изменяются, и система автоматически назначает правило для сортировки по группе правил. Если вы хотите удалить всю группу правил, вы можете выбрать все правила, нажав кнопку "Выбрать все" (Select all), а затем нажать кнопку "Удалить" (Delete).

(3) Страница конфигурации ACL MAC IP

На рис. 39 показана страница конфигурации ACL MAC IP. Вы можете использовать эту страницу для создания базы правил для ACL по MAC-адресу. Пользователь может выбрать номер группы ACL (в диапазоне 700–799), чтобы создать одно или несколько правил в группе. Поля могут соответствовать активному MAC-адресу (с битами сопоставления адресов), IP-адресу источника (с битом сопоставления адресов), IP-адресу назначения (с битом сопоставления адресов) и идентификатору VLAN.

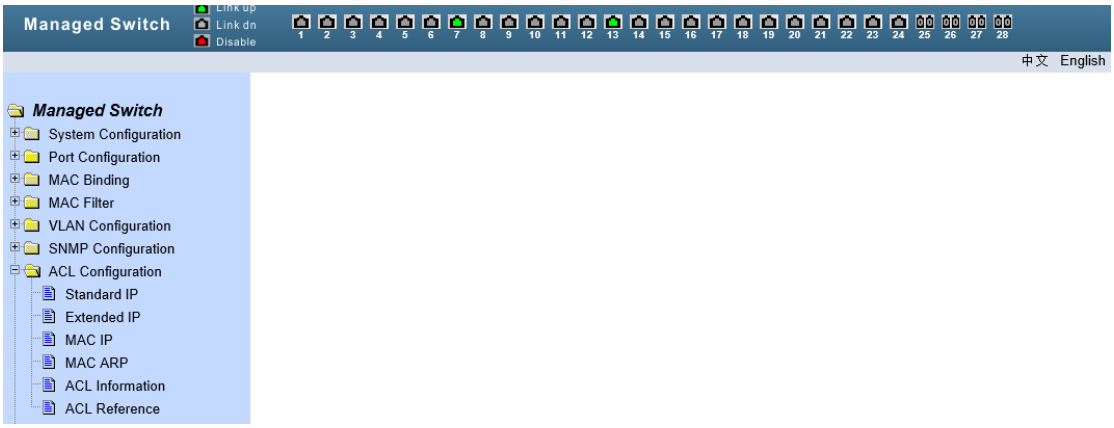


Рисунок 39 – Страница конфигурации ACL MAC IP

Когда пользователь настраивает правило, MAC-адрес источника, IP-адрес источника и IP-адрес назначения должны совпадать с адресом. Правило может соответствовать MAC-адресу и IP-адресу. Например, если правило соответствует диапазону IP-адресов от 192.168.0.0 до 192.168.0. 255, IP-адрес может быть 192.168.0.1, а его маска – 0.0.0.255.

Когда пользователь настраивает правило, каждое правило должно иметь режим фильтрации: разрешить или запретить.

Когда пользователь создает правило в группе правил, система автоматически присваивает правилу номер. Когда правило в группе правил удаляется, другие правила не изменяются, и система автоматически назначает правило для сортировки по группе правил. Если вы хотите удалить всю группу правил, вы можете выбрать все правила, нажав кнопку "Выбрать все" (Select all), а затем нажать кнопку "Удалить" (Delete).

Когда пользователь настраивает правило, идентификатор VLAN должен находиться в диапазоне от 0 до 4094, включая 0 и 4094, где 0 представляет все.

(4) Страница конфигурации ACL MAC ARP

На рис. 40 показана страница конфигурации ACL MAC ARP. Вы можете использовать эту страницу для создания базы правил для ACL MAC ARP. Пользователь может выбрать номер группы ACL (в диапазоне 1100–1199), чтобы создать одно или несколько правил в группе. Поля, которые могут быть сопоставлены в правиле, имеют тип операции ARP, отправляют MAC-адрес (с битом сопоставления адресов), и отправляют IP-адрес (с битом сопоставления адресов).

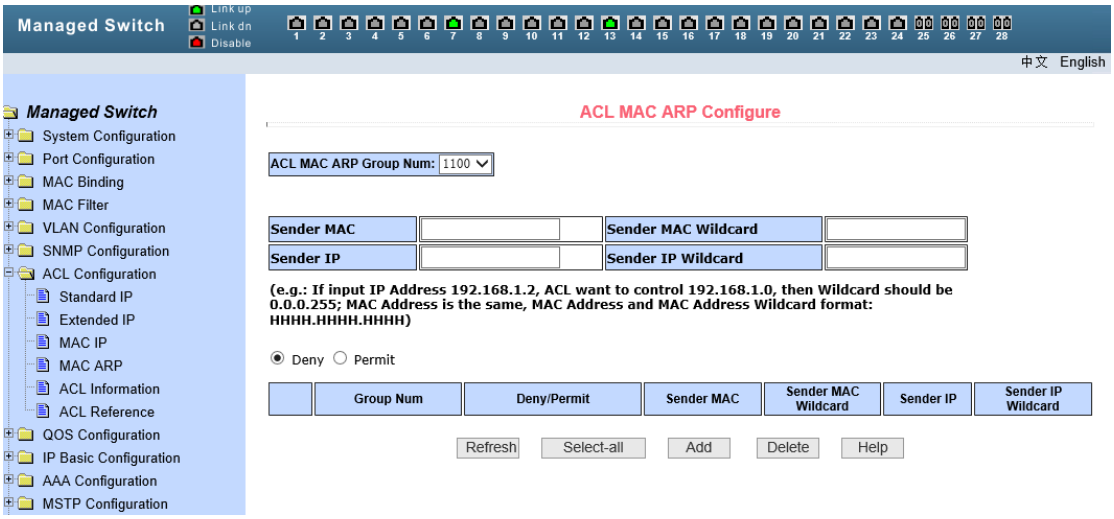


Рисунок 40 – Страница конфигурации ACL MAC ARP

Когда пользователь настраивает правило, MAC-адрес и IP-адрес отправляются с битом сопоставления адресов. Правило может соответствовать набору MAC-адреса и IP-адреса. Например, если правило соответствует диапазону IP-адресов от 192.168.0.0 до 192.168.0. 255, IP-адрес может быть 192.168.0.1, а его маска – 0.0.0.255.

Когда пользователь настраивает правило, каждое правило должно иметь режим фильтрации: разрешить или запретить.

Когда пользователь создает правило в группе правил, система автоматически присваивает правилу номер. Когда правило в группе правил удаляется, другие правила не изменяются, и система автоматически назначает правило для сортировки по группе правил. Если вы хотите удалить всю группу правил, вы можете выбрать все правила, нажав кнопку "Выбрать все" (Select all), а затем нажать кнопку "Удалить" (Delete).

(5) Страница информации о ресурсах ACL

На рис. 41 показана страница информации о ресурсах ACL, на которой отображаются все правила и ссылки, настроенные в текущем ACL.

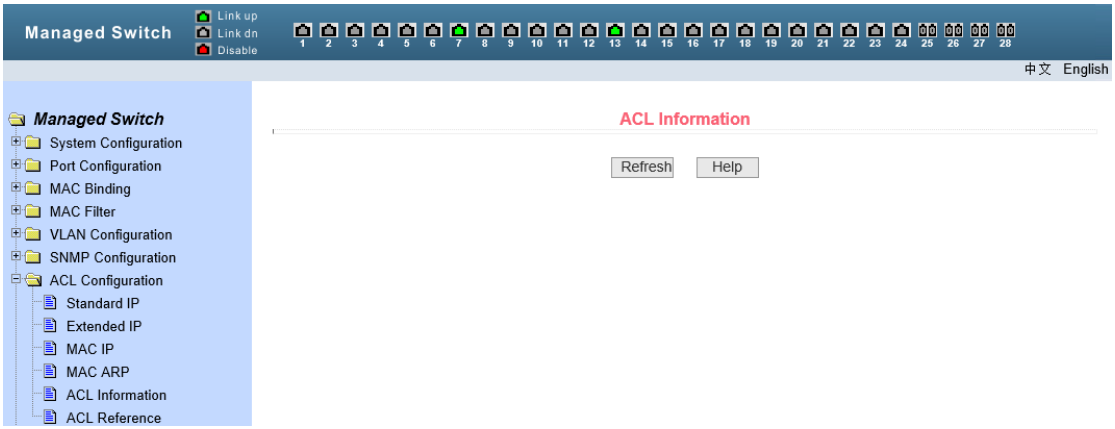


Рисунок 41 – Страница информации о ресурсах ACL

(6) Страница референса конфигурации ACL

На рис. 42 показана страница референса конфигурации ACL. Вы можете использовать эту страницу, чтобы выбрать группу ACL для порта и записать правила в этой группе ACL в аппаратную логику порта, чтобы порт мог выполнять фильтрацию по ACL для полученных пакетов в соответствии с этими правилами.

При выборе группы ACL для порта вы можете выбрать стандарт IP, расширение IP, MAC IP и ACL MAC ARP. Выбранная группа ACL должна существовать. Выберите список групп правил ACL и нажмите кнопку "Добавить" (Add). Для удаления группы ACL выберите группу ACL из списка групп референсных правил, и нажмите кнопку "Удалить" (Delete).

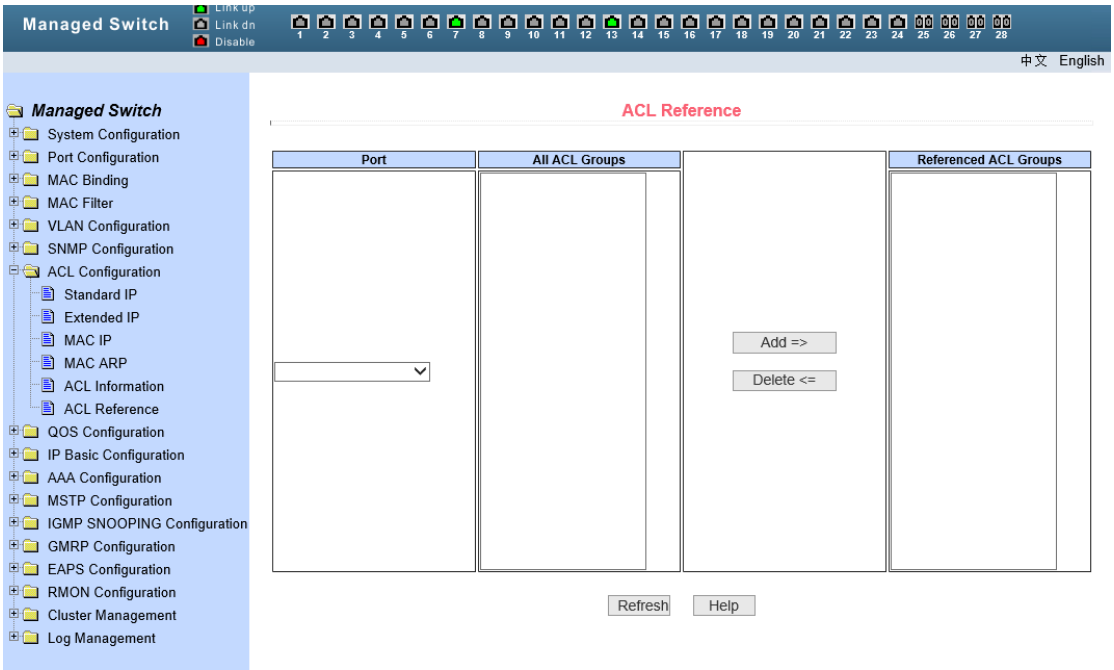


Рисунок 42 – Страница референса конфигурации ACL

10. Конфигурация QOS

(1) Страница применения QOS

На рис. 43 показана страница применения QOS, пользователь может использовать эту страницу для настройки типа QOS порта, а также может изменять на ней приоритет пользователя по умолчанию. В списке в реальном времени отображается тип QOS порта и приоритет пользователя по умолчанию.

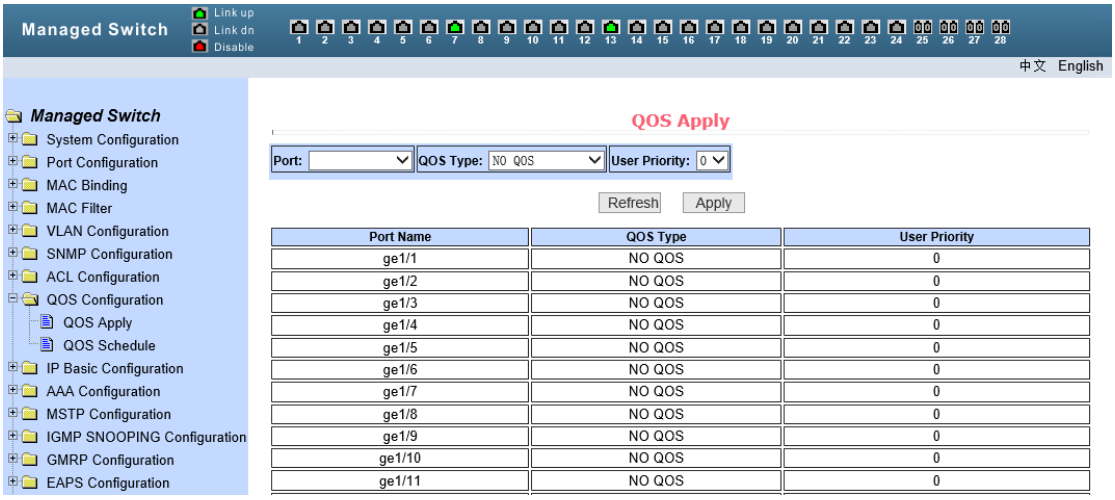


Рисунок 43 – Страница применения QOS

(2) Страница расписания QOS

На рис. 44 показана страница планирования Qos, пользователь может использовать эту страницу для настройки типа планирования QOS порта, а также может изменять приоритет очереди. Список представляет собой режим планирования портов отображения в реальном времени и значение веса каждой очереди.

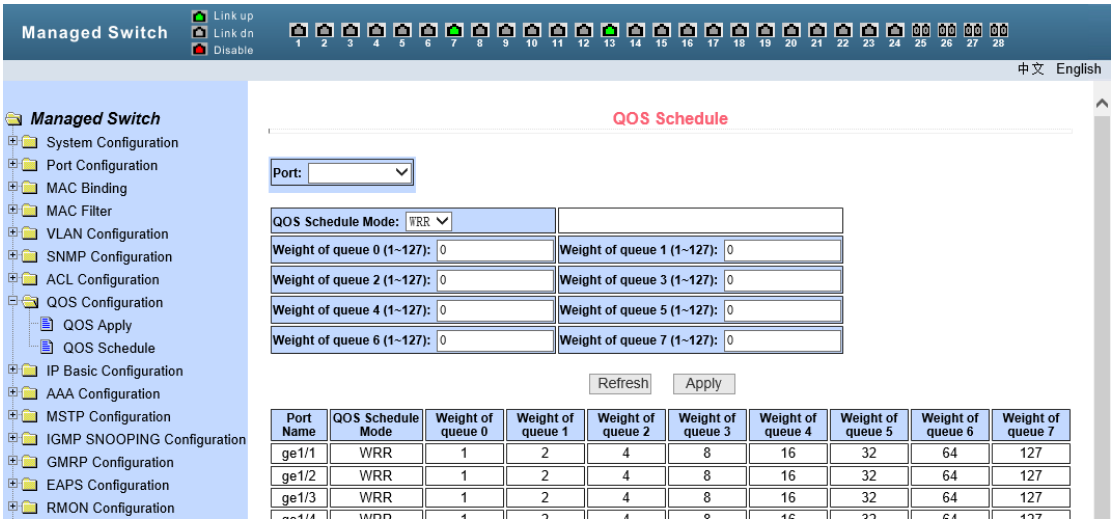


Рисунок 44 – Страница расписания QOS

11. Базовая конфигурация IP

(1) Страница конфигурации интерфейса VLAN

На рис. 45 показана страница конфигурации интерфейса VLAN. Вы можете настроить интерфейс VLAN, удалить интерфейс VLAN, настроить IP-адрес интерфейса, удалить IP-адрес интерфейса и просмотреть информацию об интерфейсе. VLAN можно установить в качестве интерфейса, когда она уже существует. На настроенном интерфейсе можно настроить только адрес интерфейса.

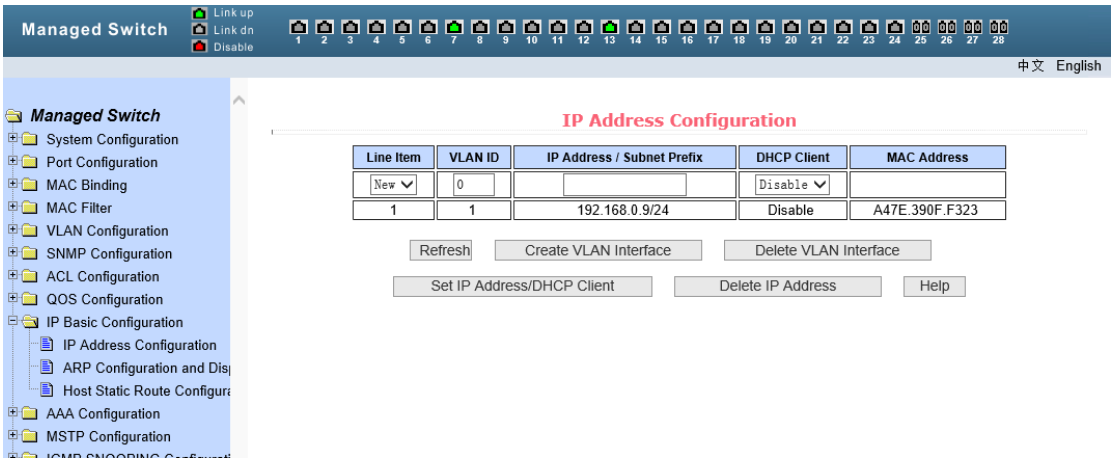


Рисунок 45 – Страница конфигурации интерфейса VLAN

Коммутатор по умолчанию имеет интерфейс VLAN1, и этот интерфейс нельзя удалить. Для одной VLAN может быть настроен только один интерфейс.

(2) Конфигурация ARP и страница отображения

На рис. 46 показана конфигурация ARP и страница отображения. На этой странице отображается вся информация из таблицы ARP коммутатора. Вы можете использовать эту страницу для настройки статических записей ARP, удаления записей ARP и изменения динамических записей ARP на статические записи ARP.

Для настройки статической записи ARP необходимо ввести IP-адрес и MAC-адрес. MAC-адрес должен быть MAC-адресом одноадресной рассылки. Затем нажмите кнопку "Добавить" (Add).

При удалении пользователем записи ARP можно выбрать удаление записи ARP с одного IP-адреса, удаление записи ARP из одного сегмента сети, удаление всех записей ARP, удаление всех динамических записей ARP и удаление всех статических записей ARP. Чтобы удалить запись IP ARP или удалить запись ARP из сегмента сети, введите указанный IP-адрес или IP-сегмент в поле ввода. Затем нажмите кнопку "Удалить" (Delete).

Динамическую запись ARP можно заменить на статическую запись ARP в сетевом сегменте. Для сегмента сети введите указанный сегмент сети в поле ввода. А затем нажмите кнопку "Применить" (Apply).

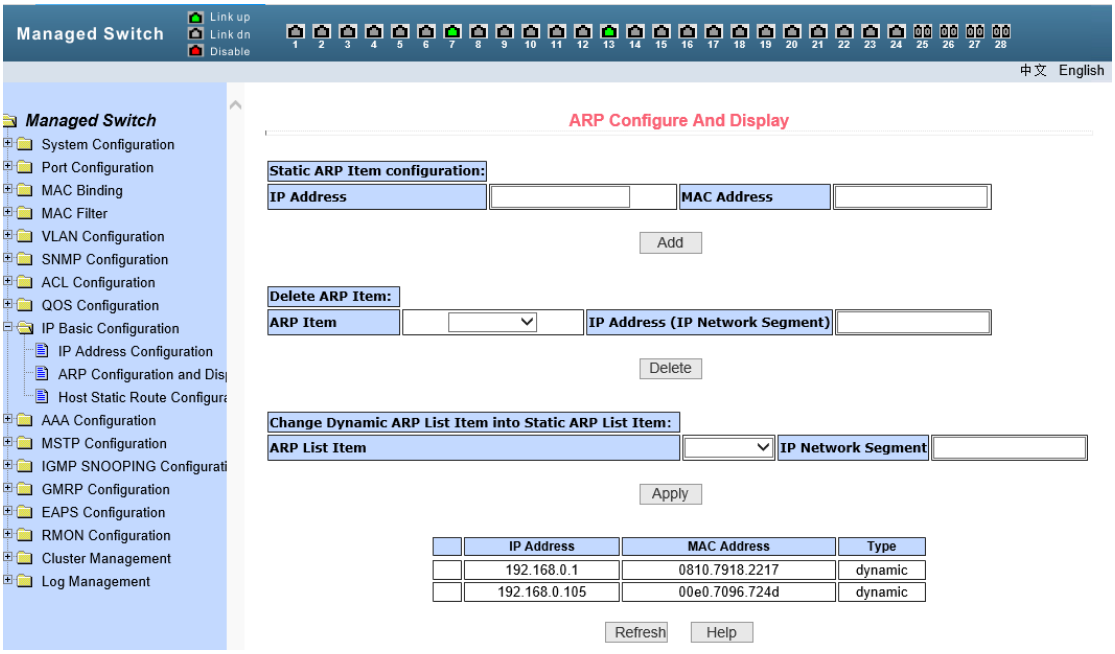


Рисунок 46 – Страница конфигурации и отображения ARP

(3) Страница конфигурации статического маршрута хоста

На рис. 47 показана страница конфигурации статической маршрутизации хоста, на которой пользователь может добавлять и удалять статические маршруты хоста коммутатора. По умолчанию статический маршрут на коммутаторе не настроен. Вы можете использовать эту страницу для настройки маршрута по умолчанию, то есть префикс назначения / подсети — 0.0.0.0/0.

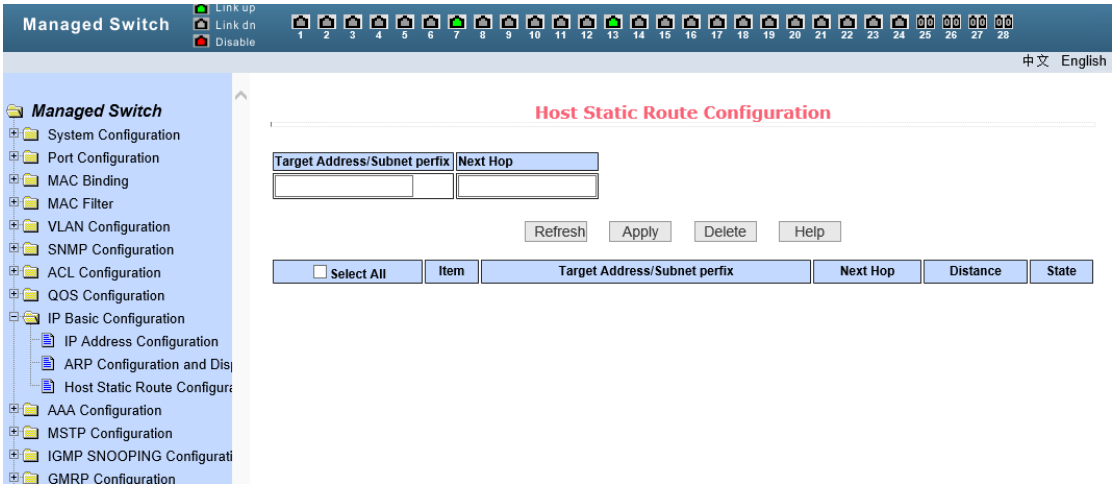


Рисунок 47 – Страница конфигурации статического маршрута хоста

12. Конфигурация AAA

(1) Страница конфигурации Tacacs+

На рис. 48 показана страница конфигурации Tacacs +. Пользователь может настроить информацию, относящуюся к Tacacs +. Можно задать следующую информацию: активировать функцию Tacacs +, настроить IP-адрес сервера Tacacs +, тип аутентификации и общий секретный ключ.

Перед использованием функции Tacacs + необходимо включить функцию Tacacs +, которая настроена по умолчанию.

Настройте IP-адрес сервера Tacacs +, который необходимо задать при использовании функции Tacacs +.

Тип аутентификации, предоставляющий типы аутентификации PAP и CHAP. По умолчанию используется аутентификация по протоколу PAP.

При авторизации необходимо ввести общий ключ, используемый для настройки коммутатора и сервера Tacacs + в качестве зашифрованного общего пароля. Он должен совпадать с настройками сервера Tacacs +.

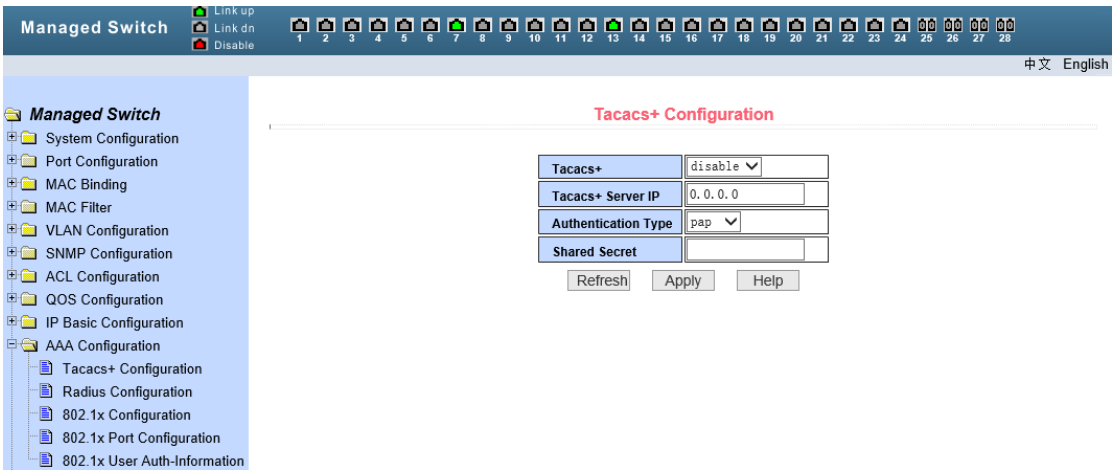


Рисунок 48 – Страница конфигурации Tacacs+.

(2) Страница конфигурации Radius

На рис. 49 показана страница конфигурации Radius, на которой пользователь может настроить информацию, связанную с Radius, задав следующие данные:

- В поле Primary Server должен быть указан IP-адрес сервера Radius, заданный для аутентификации и тарификации.

- Option Server –дополнительный IP-адрес сервера Radius, который можно задать при наличии альтернативного сервера Radius.
- UDP port — UDP-порт аутентификации, значение по умолчанию равно 1812, пользователю, как правило, не требуется изменять это поле.
- Accounting — для тарификации по умолчанию используется значение "Активировать" (Enable) при выполнении условий аутентификации и тарификации для начала тарификации.
- Accounting UDP port — Для UDP-порта тарификации значение по умолчанию — 1813.
- Shared key — общий ключ, используемый для настройки коммутатора и шифрования сервера Radius в качестве общего пароля для аутентификации и тарификации, необходимо указать в этом поле, Он должен совпадать с настройкам на сервере Radius.
- Vendor — информация, относящаяся к конкретному поставщику. Пользователям, как правило, не требуется изменять это поле.
- Порт NAS (NAS Port), тип порта NAS (NAS Port Type), тип службы NAS (NAS Service Type) — эти три значения пользователям, как правило, не требуется изменять.
- Roaming — активация или отключение функции роуминга Radius.

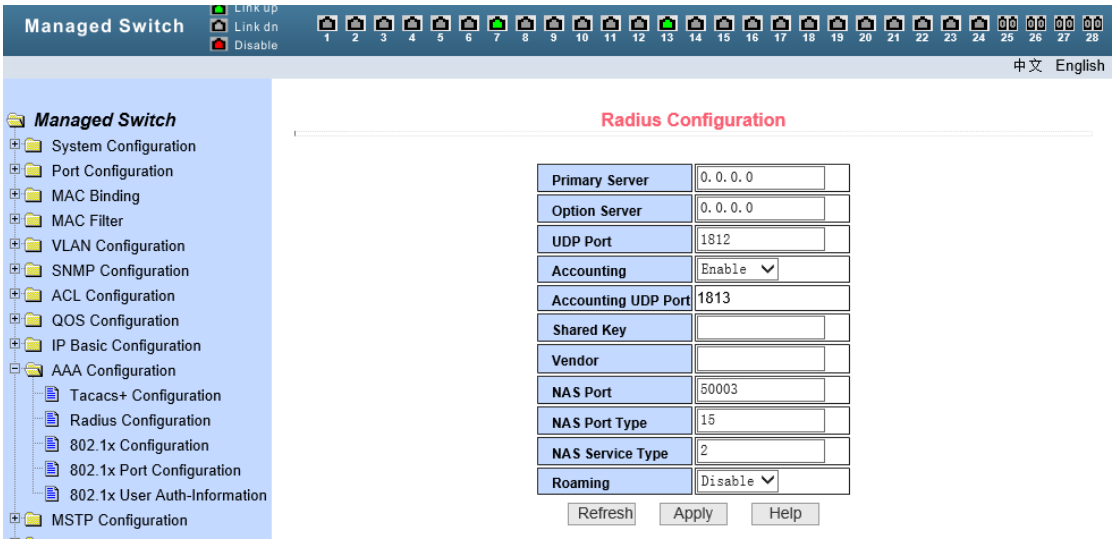


Рисунок 49 – Страница конфигурации Radius

(3) Страница конфигурации 802.1x

На рис. 50 показана страница конфигурации 802.1x. Вы можете настроить информацию, связанную с 802.1x, на этой странице, включая:

- Следует ли запускать протокол 802.1x. Обязательно запустите протокол 802.1x при выполнении аутентификации и тарификации.
- Независимо от того, использует ли коммутатор обычный или расширенный метод аутентификации.
- Следует ли активировать функцию повторной аутентификации (Reauthentication). По умолчанию она не активирована. При выполнении аутентификации и тарификации решение принимается в соответствии с фактической ситуацией. Включение функции повторной аутентификации обеспечить пользователю более высокую надежность при выполнении аутентификации и такрификации, но немного увеличит трафик в сети.
- Интервал повторной аутентификации (Reauthentication Period) может быть задан, только в том случае, если включена функция повторной аутентификации. По умолчанию интервал составляет 3600 секунд. При выполнении аутентификации и тарификации в соответствии с фактической ситуацией необходимо установить значение, однако значение не должно быть слишком маленьким.
- Таймер периода бездействия (Quiet Period) — пользователю, как правило, не требуется изменять это поле.
- Таймер периода Tx (Tx-Period) — пользователю, как правило, не требуется изменять это поле.
- Таймер тайм-аута сервера (Server Timeout) — пользователю, как правило, не требуется изменять это поле.
- Таймер тайм-аута запрашивающего устройства (Supplicant Timeout) — пользователю, как правило, не требуется изменять это поле.
- Количество запросов (Max Reqest) — пользователю, как правило, не требуется изменять это поле.
- Reauth Max — показывать максимальное количество попыток повторной аутентификации.

- Версия клиента (Client Version) — номер версии клиента.
- Проверка клиента (Check Client) — следует ли проверять пакет временного трафика клиента после прохождения аутентификации.

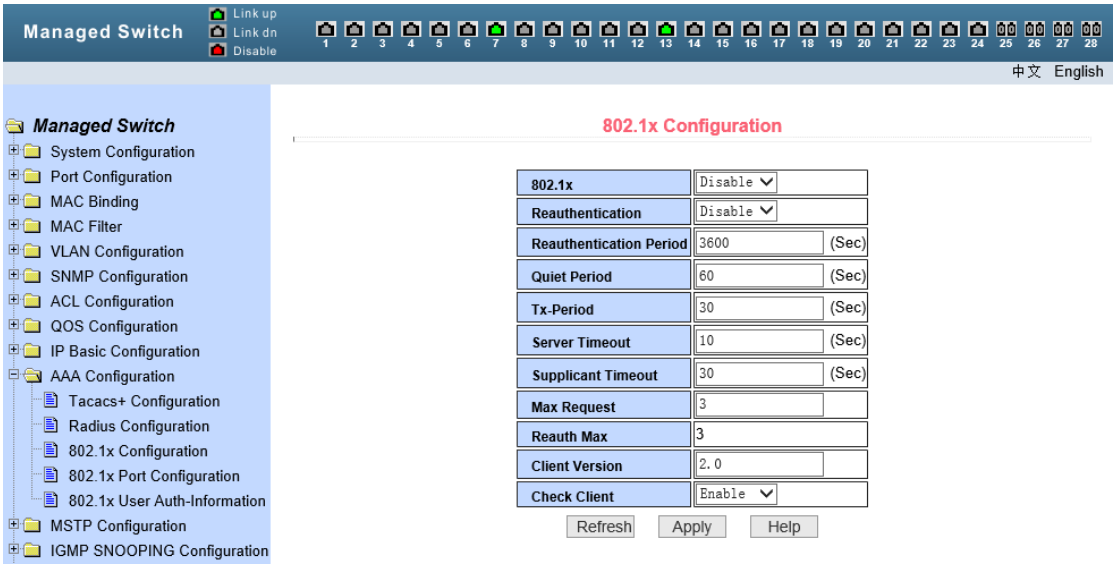


Рисунок 50 – Страница конфигурации 802.1x

(4) страница конфигурации порта 802.1x

На рис. 51 показана страница конфигурации порта 802.1x. Вы можете настроить режим порта 802.1x и максимальное количество хостов, которые можно настроить. Вы также можете просмотреть конфигурацию 802.1x каждого порта. Режим порта 802.1x включает четыре типа состояния: н/д (N/A), авто (Auto), принудительная авторизация (Force-authorized) и принудительное отключение авторизации (Force-unauthorized).当

Когда для порта необходимо выполнить аутентификацию 802.1 x, для состояния порта устанавливается значение "авто" (Auto). Если доступ к сети можно получить, не выполняя аутентификацию, состояние порта устанавливается на н/д (N/A). Два других состояния редко используются в практическом применении.

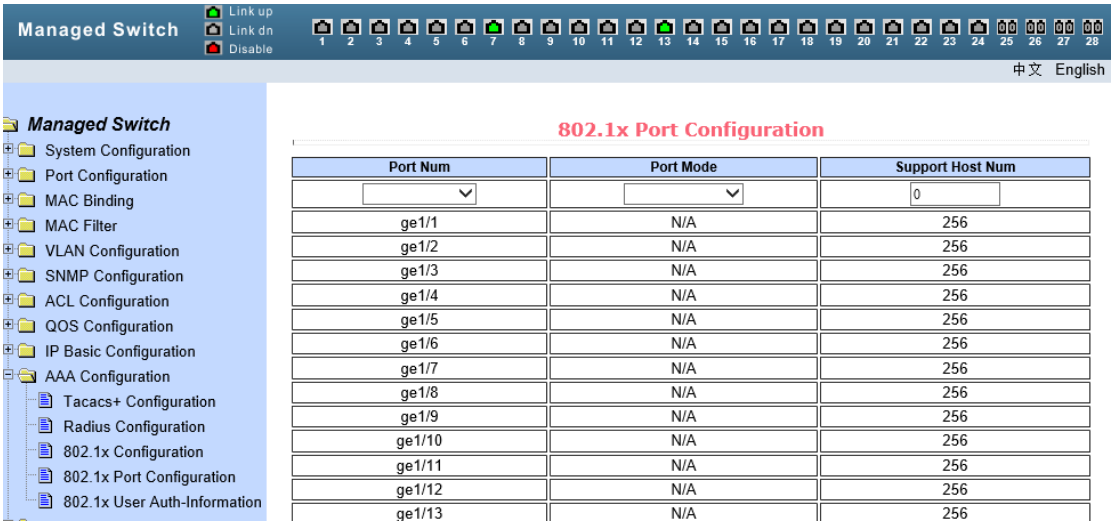


Рисунок 51 – Страница конфигурации порта 802.1x.

Когда включена проверка подлинности 802.1x, максимальное количество узлов, к которым может быть получен доступ через порт — 256, и пользователь может изменить это поле для поддержки до 256 узлов.

(5) Страница информации об авторизации пользователя 802.1x

На рис. 52 показана страница с информацией об авторизации пользователя 802.1x. Вы можете просматривать информацию о статусе всех пользователей, получающих доступ к порту, на этой странице.

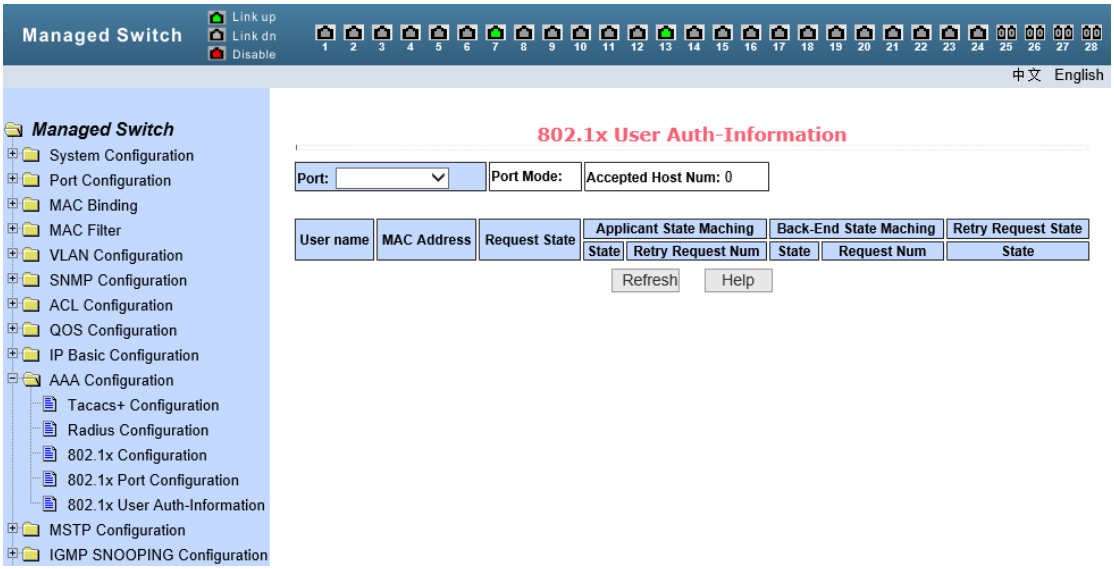


Рисунок 52 – Страница информации об авторизации пользователя 802.1x

13. Конфигурация MSTP

(1) Страница глобальной конфигурации MSTP

На рис. 53 показана страница глобальной конфигурации MSTP. Вы можете настраивать глобальные параметры MSTP на этой странице.

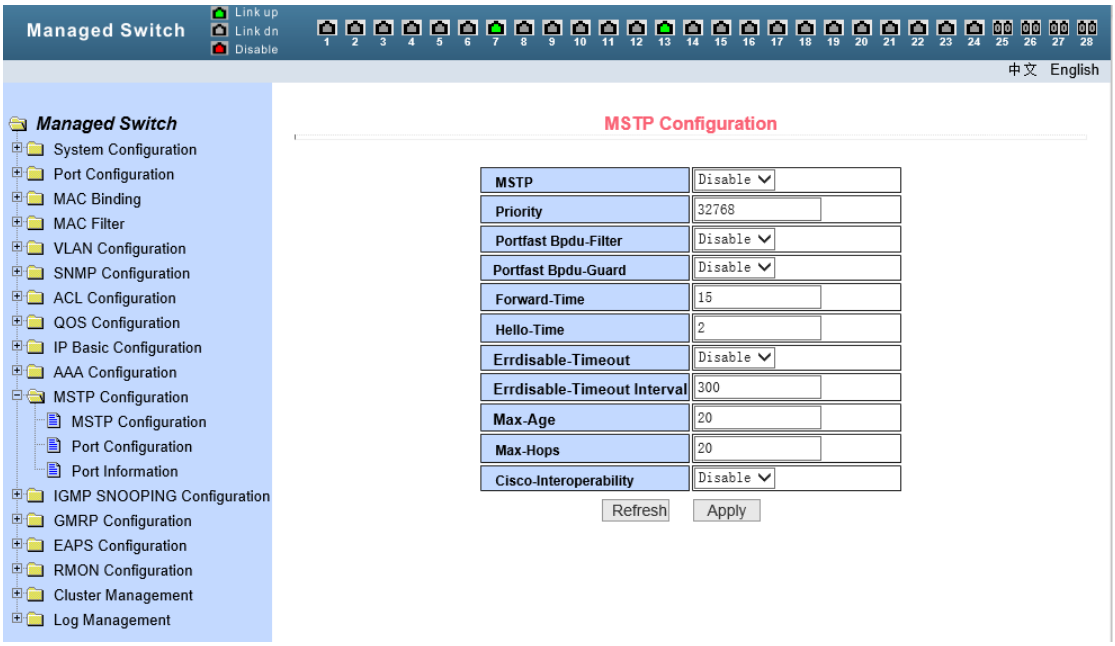


Рисунок 53 – Страница глобальной конфигурации MSTP

(2) Страница конфигурации порта MSTP

На рис. 54 показана страница конфигурации порта MSTP. Вы можете использовать эту страницу для настройки параметров порта MSTP.

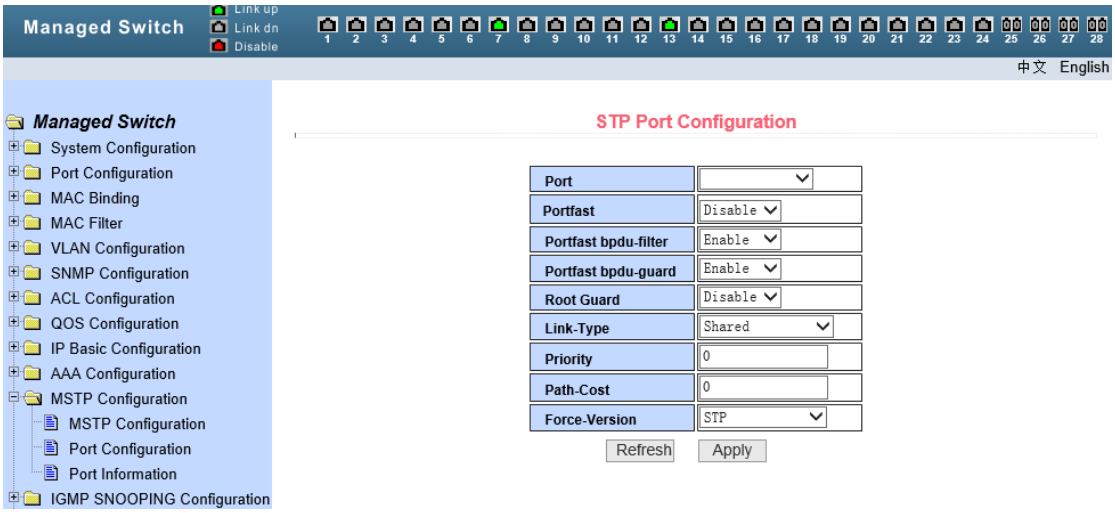
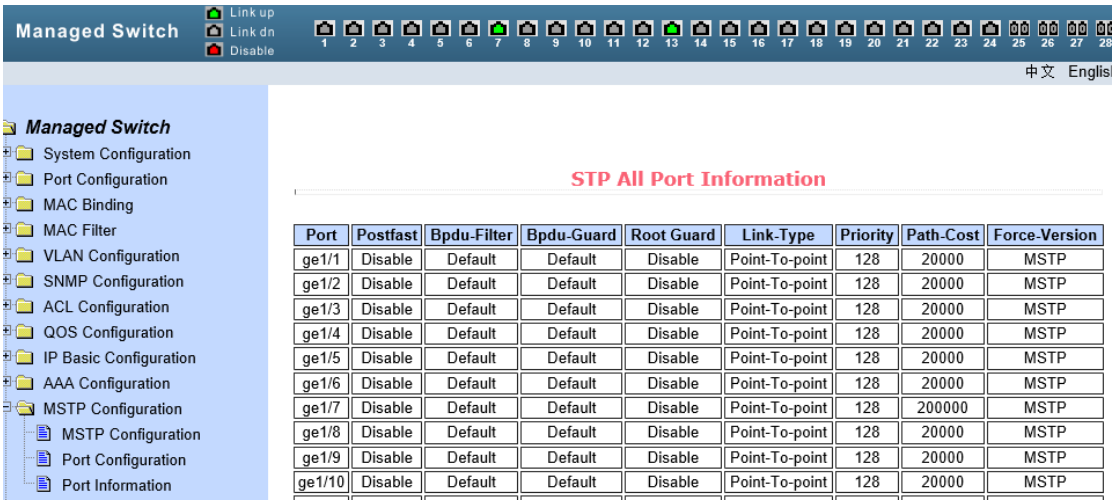


Рисунок 54 – Страница конфигурации порта MSTP

(3) Страница информации о порте MSTP

На рис. 55 показана страница информации о порте MSTP. Вы можете просмотреть статус порта MSTP на этой странице.



Port	Postfast	Bpdu-Filter	Bpdu-Guard	Root Guard	Link-Type	Priority	Path-Cost	Force-Version
ge1/1	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/2	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/3	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/4	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/5	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/6	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/7	Disable	Default	Default	Disable	Point-To-point	128	200000	MSTP
ge1/8	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/9	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/10	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP

Рисунок 55 – Страница информации о порте MSTP

14. Конфигурация IGMP SNOOPING

(1) Страница глобальной конфигурации IGMP snooping

На рис. 56 показана страница глобальной конфигурации IGMP snooping. Вы можете включить IGMP snooping на этой странице.

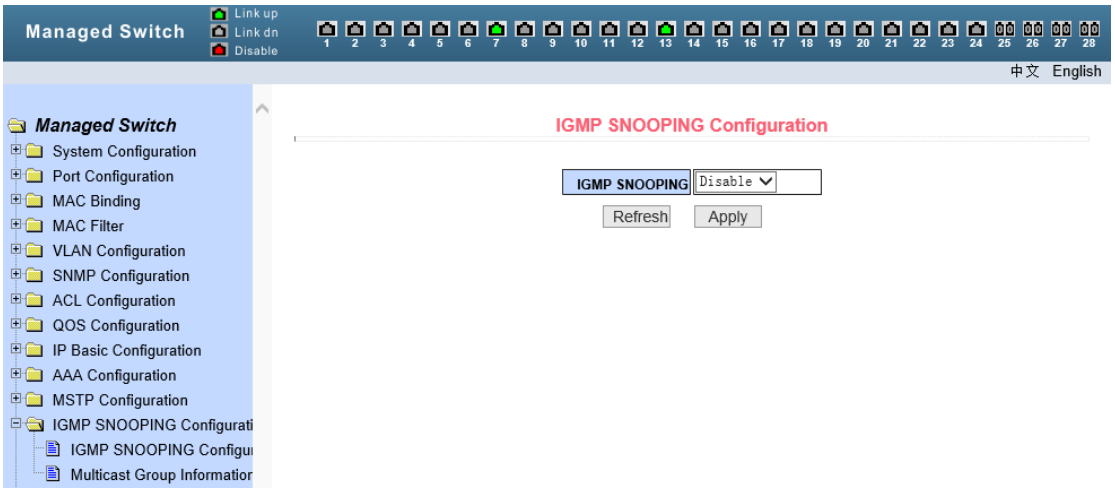


Рисунок 56 – Страница глобальной конфигурации IGMP snooping

(2) Страница информации о группе многоадресной рассылки

На рис. 57 показана страница информации о группе многоадресной рассылки. Вы можете просмотреть информацию о программе многоадресной рассылки IGMP snooping с этой страницы.

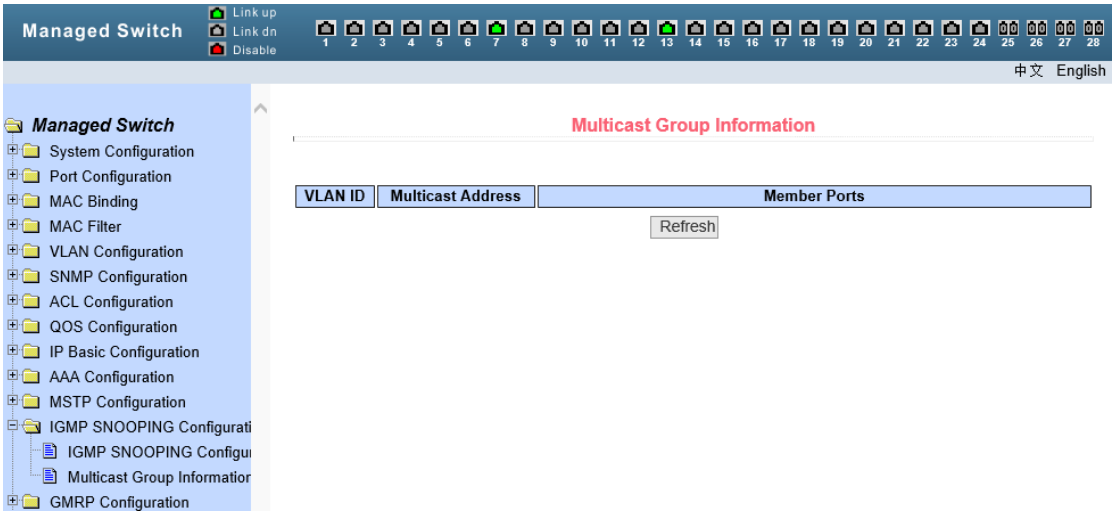


Рисунок 57 – Страница информации о группе многоадресной рассылки

15. Конфигурация GMRP

(1) Страница глобальной конфигурации GMRP

На рис. 58 показана страница глобальной конфигурации GMRP. Пользователи могут включать GMRP на этой страницу.

Рисунок 58 – Страница глобальной конфигурации GMRP

(2) Страница конфигурации порта GMRP

На рис. 59 показана страница конфигурации порта GMRP. Пользователи могут использовать эту страницу, чтобы включить порт GMRP, а также просматривать информацию о порте.

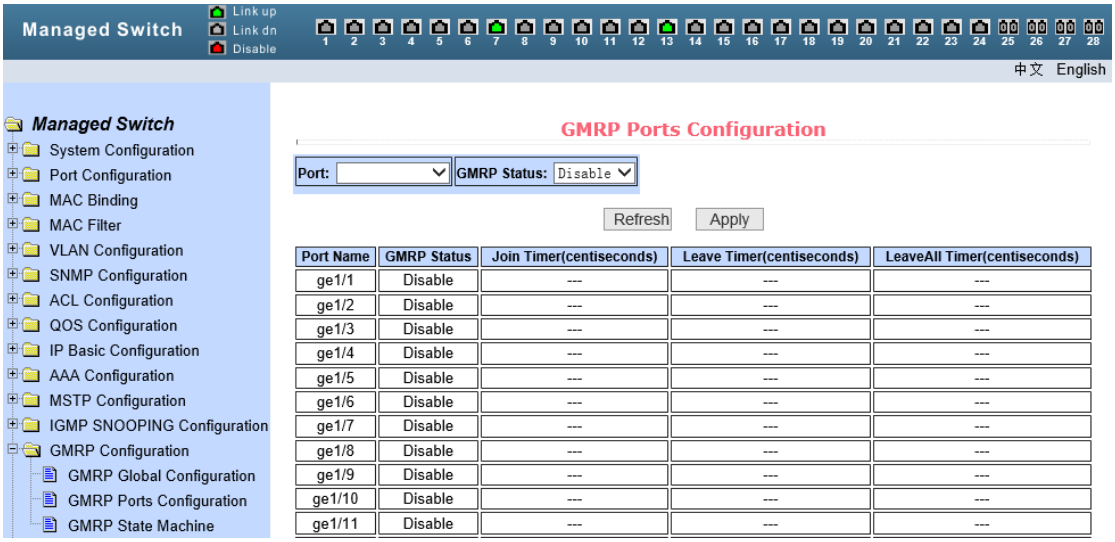


Рисунок 59 — Страница конфигурации порта GMRP

(3) Страница конечного автомата GMRP

Рисунок 60 - страница конечного автомата GMRP. Пользователи могут просматривать информацию о конечном автомате GMRP с этой страницы.

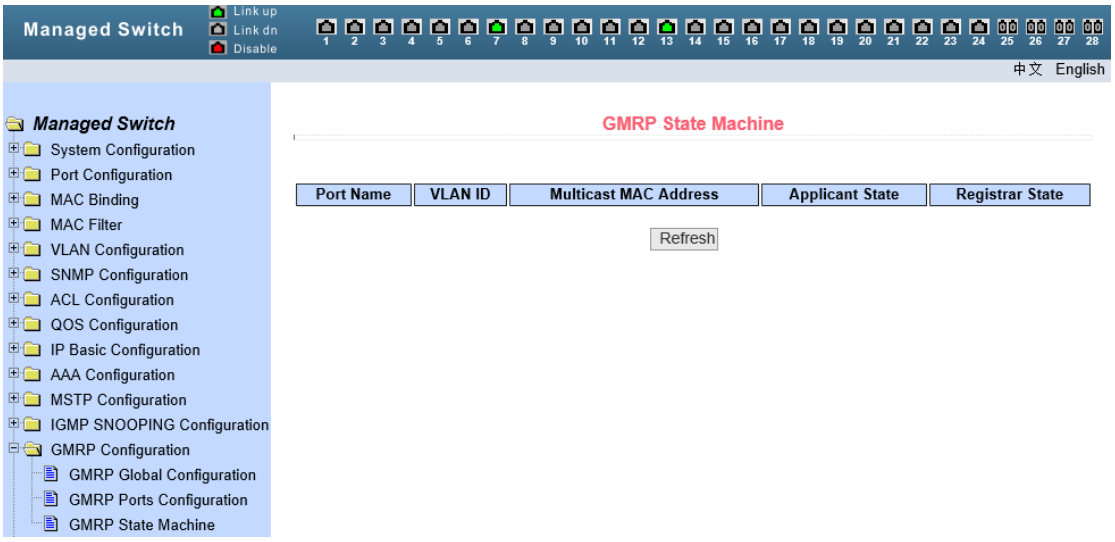


Рисунок 60 — Страница конечного автомата GMRP

16. Конфигурация EAPS

(1) Страница конфигурации EAPS

Эта страница используется для создания и настройки данных EAPS, а также может использоваться для удаления и отображения данных EAPS.

Идентификатор EAPS-кольца (EAPS Ring ID) — конкретный идентификатор кольца в диапазоне от 1 до 16, можно выбрать в соответствии с раскрывающимся списком

Два варианта статуса создания (Create Status): "Не созданный" (Not Created) и "Созданный" (Created). Если он не создан, необходимо создать шаблон Master и Transit. Соответствующий режим может быть настроен в соответствии с конкретными потребностями

Главный порт (Primary Port) — основной порт EAPS, такой как: fe1/1, ge1/1

Альтернативный порт EAPS (Secondary Port) — второй порт

Управляющая VLAN (Control VLAN) — Управляющая VLAN EAPS-кольца, значение 2–4094

Защитные VLAN (Protected VLANs) — защитные VLAN EAPS-кольца

Интервал времени приветствия (Hello Time Interval) — интервал отправки приветственного сообщения по умолчанию составляет 1 сек.

Время сбоя (Fail Time) — время обнаружения неисправности по умолчанию равно 3 секундам

Data Span — Данные передаются по кольцу, в случае нескольких колец эта функция требуется, когда необходимо передать данные по кольцу. Значение по умолчанию – отключено

Extreme interoperability — Совместимость с крайними сетевыми устройствами, включенными по умолчанию

Состояние активации (Enabled State) Включено последнее EAPS-кольцо

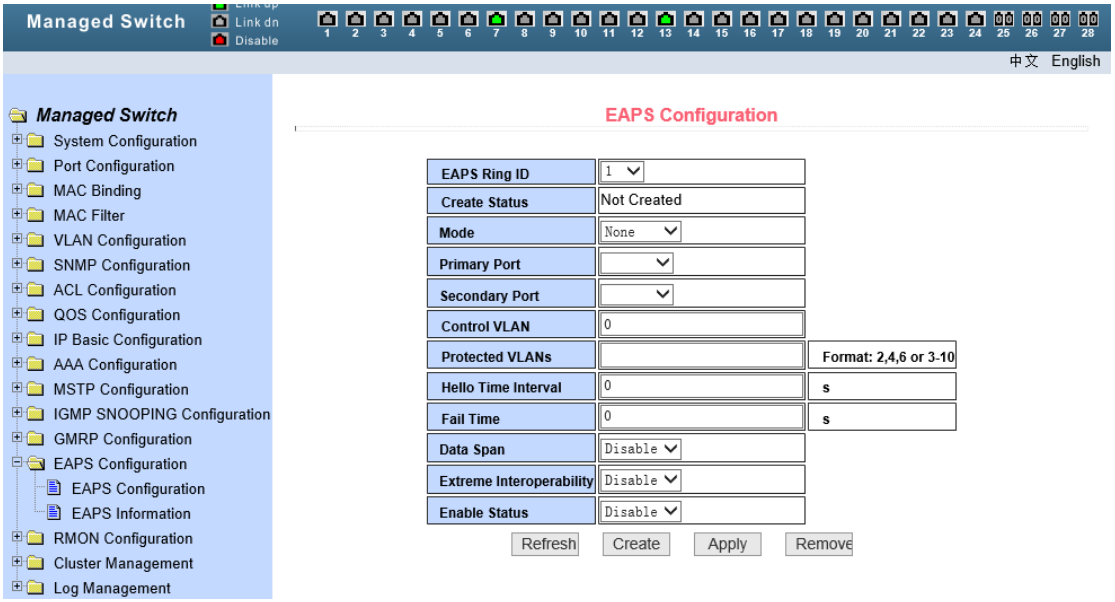


Рисунок 61 — Страница конфигурации EAPS

(2) Страница сведений EAPS

На рис. 62 показана страница сведений EAPS. Пользователи могут просматривать информацию о конфигурации EAPS на этой странице.

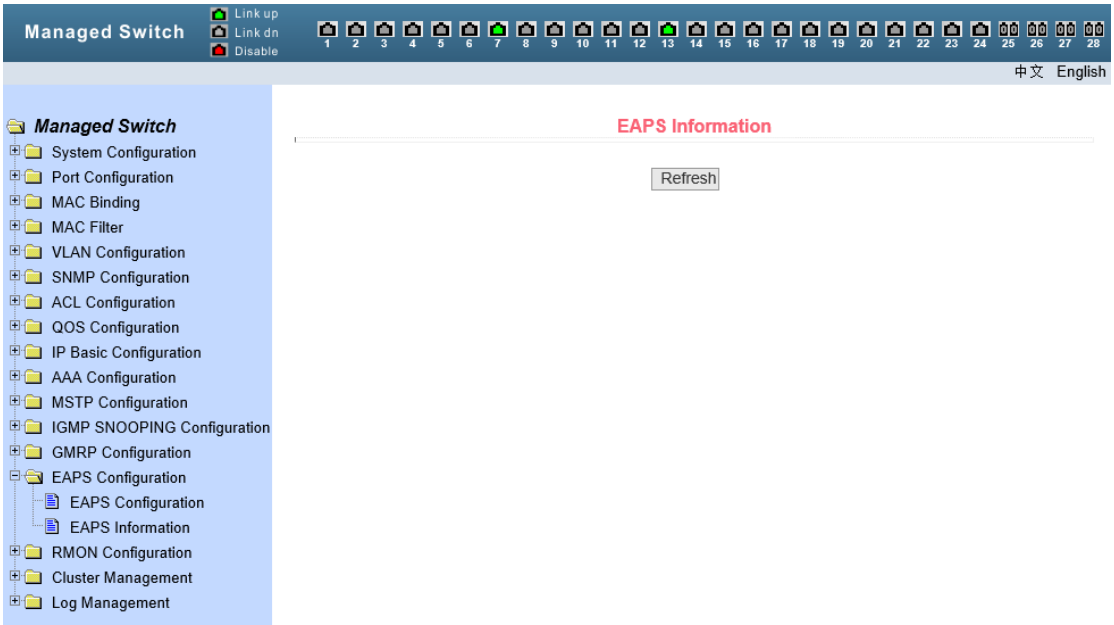


Рисунок 62 — Страница сведений EAPS

17. Конфигурация RMON

(1) Страница конфигурации группы статистики RMON

На рис. 63 показана страница конфигурации группы статистики RMON. Пользователь может настроить группу статистики RMON на этой странице. Выберите порт из выпадающего списка, чтобы просмотреть или настроить конфигурацию группы статистики RMON для этого порта. Если номер индекса (Index) равен 0, заполняется правильный номер индекса (в диапазоне от 1 до 100), а поле "Владелец" (Owner) является необязательным. Вы можете настроить группу статистики RMON для порта. В таблице статистики показана статистика портов, полученная в результате успешной настройки.

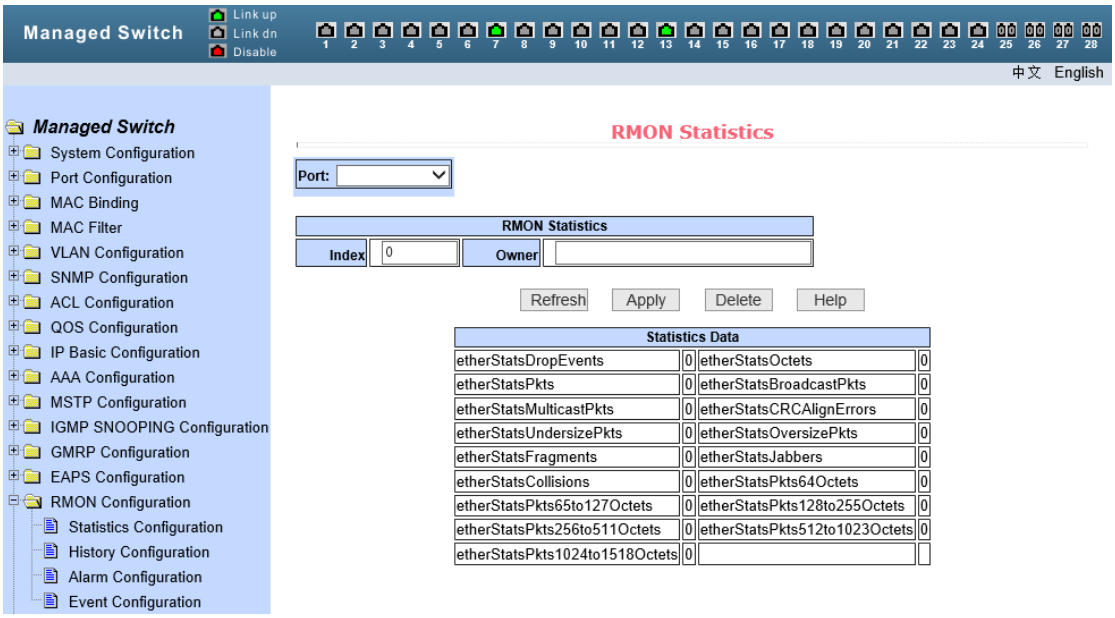


Рисунок 63 — Страница конфигурации группы статистики RMON

(2) Страница конфигурации группы истории RMON

На рис. 64 показана страница конфигурации группы истории RMON. Пользователь может настроить группу истории RMON на этой странице. Выберите порт из выпадающего списка, чтобы просмотреть или настроить конфигурацию группы истории RMON для этого порта. Если номер индекса равен 0, то указывается правильный номер индекса (в диапазоне от 1 до 100), Поля "Интервал", "Сегменты запроса" (Request Buckets) и "Владелец" (Owner) являются необязательными. Вы можете настроить группу истории RMON для этого порта. Интервал относится к временному интервалу для сбора данных в секундах в диапазоне 1–3600; сегменты запросов - это выделенный размер хранилища, указывающий, сколько записей хранится, диапазон: 1–100. В таблице статистики показаны исторические данные, полученные с момента успешного выполнения конфигурации.

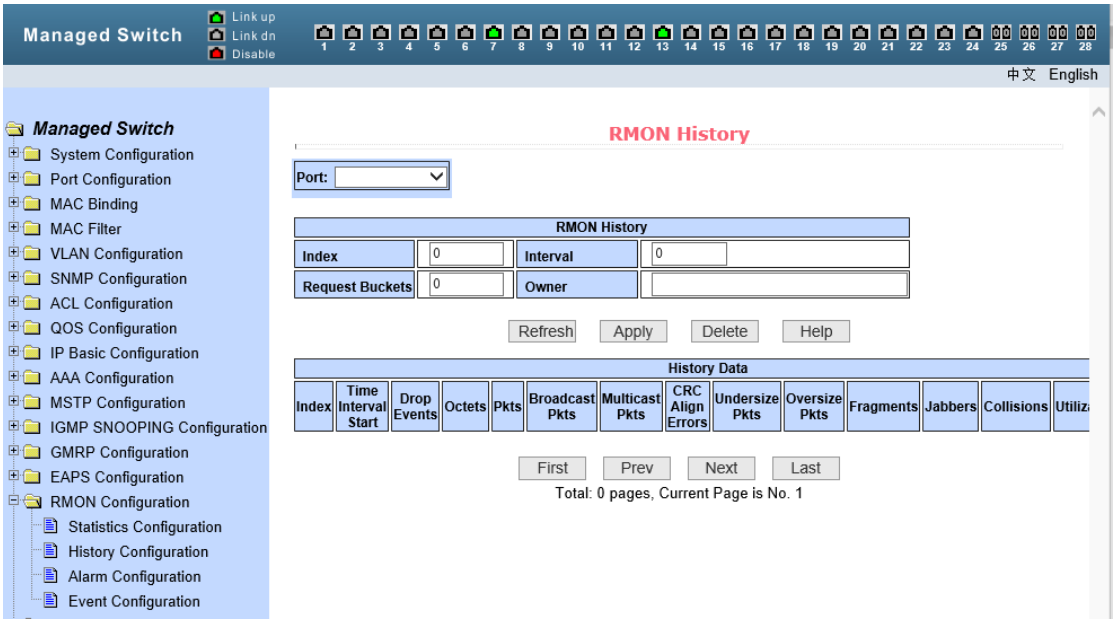


Рисунок 64 — Страница конфигурации группы истории RMON

(3) Страница конфигурации группы аварийных сигналов RMON

На рис. 65 показана страница конфигурации группы аварийных сигналов RMON, на которой пользователи могут создавать или изменять группу аварийных сигналов RMON. Выберите настроенную группу сигнализации из выпадающего списка, чтобы просмотреть или настроить ее информацию, и выберите "Создать" (New), чтобы создать ее. Диапазон индексов от 1 до 60, интервал от 1 до 3600, в секундах, в качестве объекта мониторинга должен быть указан узел MIB, контраст: абсолютный или дельта. Также необходимо заполнить верхний и нижний порог, а также индекс события. Поле "Владелец" (Owner) является необязательным. Значение сигнала тревоги доступно только для чтения и показывает выбранное значение, когда был выдан последний сигнал тревоги. Индекс события относится к номеру индекса группы событий RMON и должен быть настроен заранее.

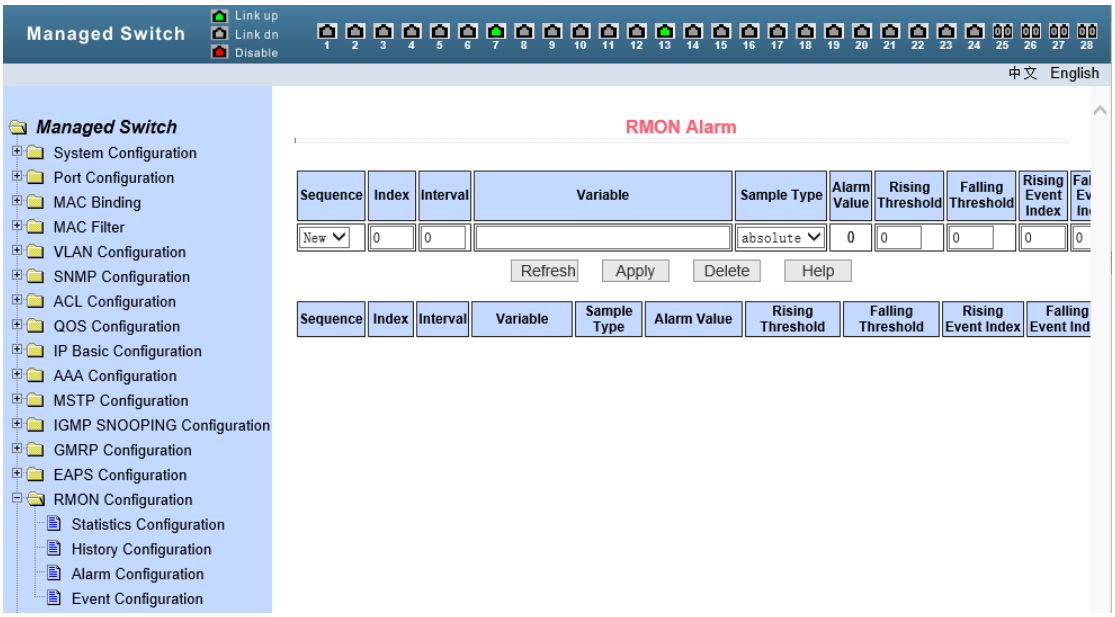


Рисунок 65 — Страница конфигурации группы аварийных сигналов RMON

(4) Страница конфигурации группы событий RMON

На рис. 66 показана страница конфигурации группы событий RMON, на которой пользователи могут создавать или изменять группы событий RMON. Выберите настроенную группу событий из выпадающего списка, чтобы просмотреть или настроить ее информацию, и выберите "Создать" (New), чтобы создать ее. Диапазон индексов составляет от 1 до 60, а описание представляет собой строку. Доступные действия: нет (none) (отсутствие операций), журнал (log), SNMP-трап (SNMP-trap) или журнал и трап (log-and-trap). Общее имя не работает на этом устройстве, а поле "Владелец" (Owner) является необязательным. Время последней отправки доступно только для чтения и показывает время последней отправки события.

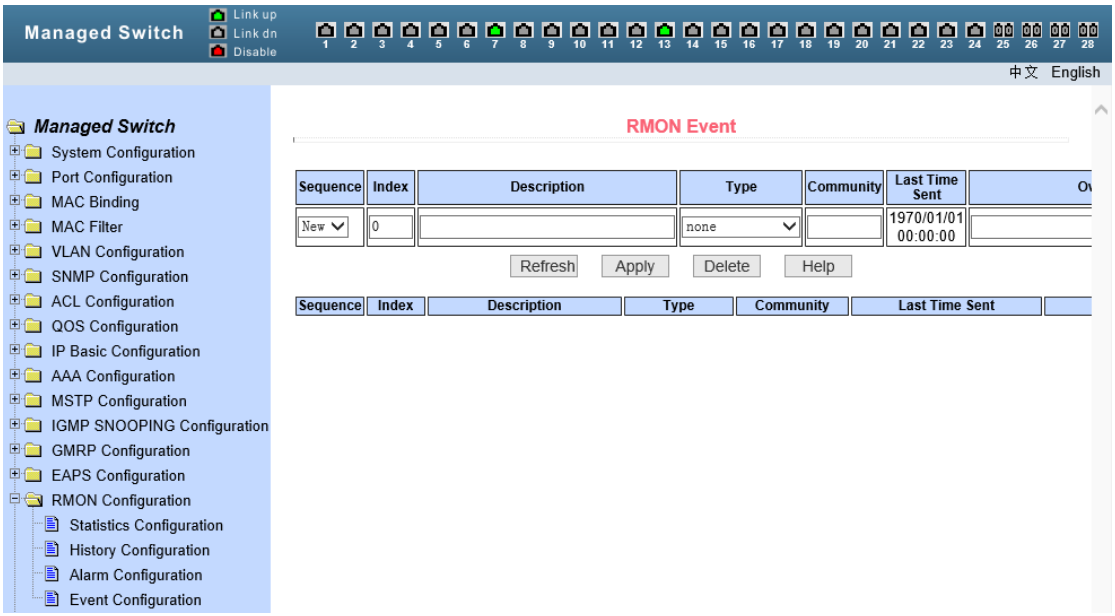


Рисунок 66 — Страница конфигурации группы событий RMON

18. Конфигурация кластера

(1) Страница конфигурации NDP

На рис. 66 показана страница конфигурации NDP, на которой пользователи могут настроить NDP. Информация, которую можно задать, включает в себя: выбор порта, функцию NDP порта, глобальную функцию NDP, интервал отправки пакетов NDP и время старения пакетов NDP на принимающем устройстве.

Выбор порта — выберите необходимый порт и включите функцию NDP порта. NDP должен выполняться нормально, и функции глобального NDP и NDP порта должны быть включены одновременно.

Настройте время старения пакетов NDP, отправляемых устройством, на принимающем устройстве. Действительный диапазон времени составляет 1–4096 секунд. Конфигурация по умолчанию составляет 180 секунд.

Настройте интервал для отправки пакетов NDP, допустимый диапазон времени составляет 1–4096 секунд, по умолчанию – 60 секунд.

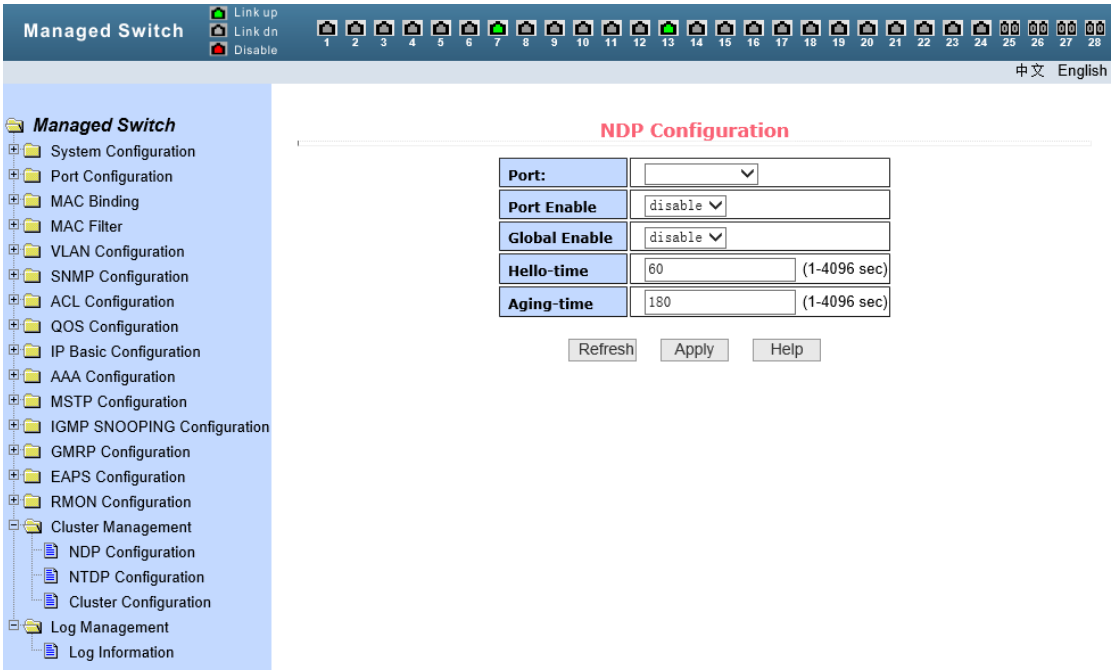


Рисунок 66 — Страница конфигурации NDP

(2) Страница конфигурации NTDP

На рис. 67 показана страница конфигурации NTDP, где пользователи могут настроить NTDP. Информация, которую можно задать, включает: выбор порта, включение функции NTDP порта, включение функции глобального NTDP, диапазон

сбора топологии, временной интервал сбора топологии, время задержки пакета переадресации первого порта и задержка других пакетов переадресации порта.

Выбор порта — выберите необходимый порт и включите функцию порта NTDP. Для нормальной работы NTDP необходимо также включить функцию глобального NTDP и NTDP порта.

Настройте диапазон коллекции топологий. Действительный диапазон составляет 1—6. В топологии по умолчанию максимальное количество переходов устройства равно 3.

Настройте интервал для сбора информации о топологии. Действительный диапазон составляет 0—65535 минут. Конфигурация по умолчанию составляет 1 минуту.

Настройте время задержки для пересылки пакетов на первый порт. Действительный диапазон составляет 1—1000 миллисекунд. Конфигурация по умолчанию составляет 200 миллисекунд.

Настройте время задержки для пересылки пакетов на первый порт. Действительный диапазон составляет 1—100 миллисекунд. Конфигурация по умолчанию составляет 20 миллисекунд.

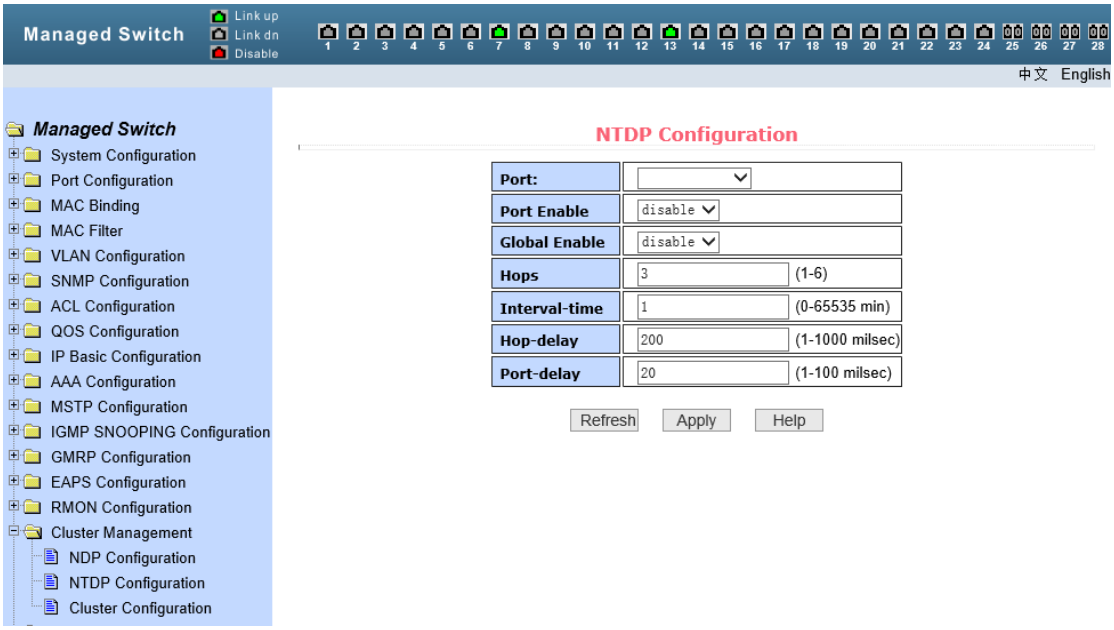


Рисунок 67 — Страница конфигурации NTDP

(3) Страница конфигурации кластера

На рис. 68 показана страница конфигурации кластера. Пользователь может настроить кластер на этой странице и просматривать таблицу участников кластера. Информация, которую можно задать, включает функции включения кластера, настройки VLAN управления, пула адресов кластера, интервала отправки пакетов квитирования, эффективного времени хранения устройства, имени кластера, способа присоединения к кластеру и удаления кластера.

Включите функцию Cluster Enable для нормальной работы. Сначала вы должны включить функцию кластера.

Настройте VLAN управления с допустимым диапазоном 1—4094 и значением по умолчанию VLAN1.

Настройте диапазон частных IP-адресов, используемых устройствами в кластере. Действительный диапазон IP-адресов составляет 0.0.0.0 ~ 255.255.255.255. Действительный диапазон длины маски составляет 0 ~ 32.

Интервал для отправки пакетов квитирования составляет 1—255 секунд, а значение по умолчанию равно 10 секундам.

Настройте эффективное время хранения устройства. Действительный диапазон составляет 1—255 секунд. Конфигурация по умолчанию составляет 60 секунд.

Чтобы создать кластер, вам необходимо настроить имя кластера, выбрать способ добавления в кластер. Способ добавления может быть, как ручной, так и автоматический. После настройки кластера его можно автоматически переключить в ручной режим, но ручной режим нельзя переключить в автоматический. В ручном режиме можно изменять имя кластера.

После создания кластера вы можете просматривать устройства в кластере и устройства-кандидаты в таблице участников кластера. Вы можете добавить устройство в кластере или добавить устройство-кандидат к устройству в кластере в зависимости от роли.

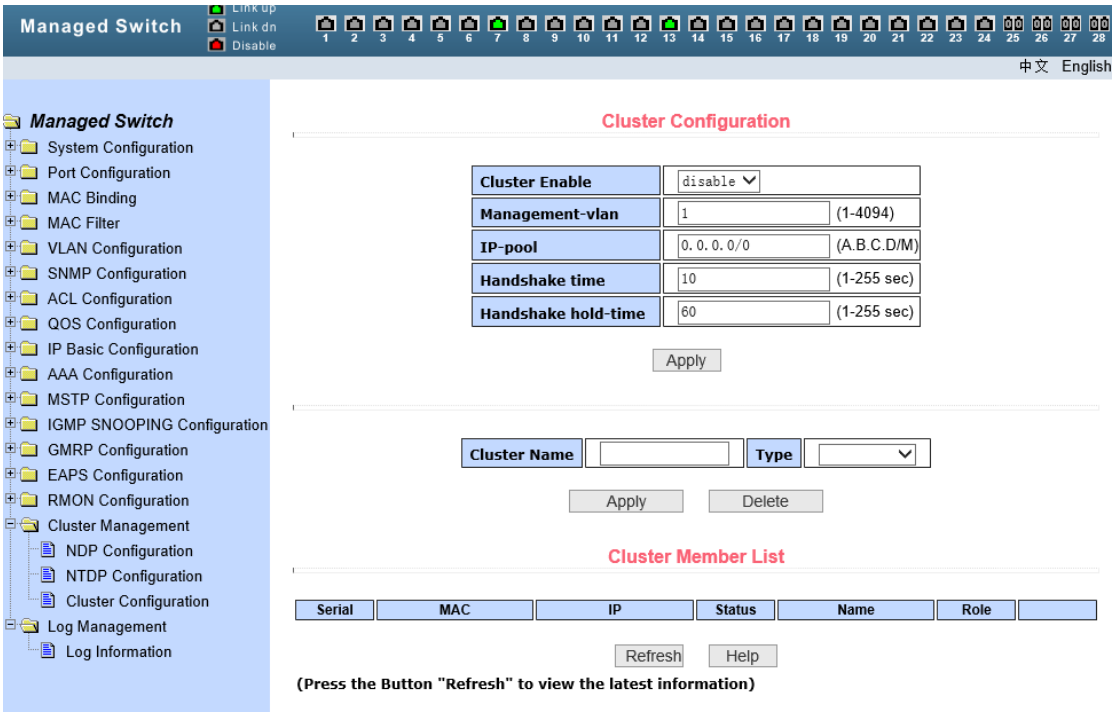


Рисунок 68 — Страница конфигурации кластера

19. Конфигурация ERPS

(1) Страница конфигурации EAPS

На рис. 69 показана страница конфигурации EAPS. Пользователи могут использовать эту страницу для включения функции ERPS, настройки параметров ERPS, создания и удаления экземпляра ERPS, ERPS-кольца и других действий.

Экземпляр ERPS (ERPS instance) – Создание и удаление экземпляров ERPS (<1–8>)

Роль узла (Node role) – Настройте роль узла в ERPS-кольце, узла сети или не связанного узла

ERPS-кольцо (ERPS ring) — Создание и удаление ERPS-колец (<1–32>)

Режим кольца (Ring mode) — Настройка режима ERPS-кольца: основное кольцо или дополнительное кольцо

Режим узла (Node mode) — конфигурация режима узла ERPS-кольца, узел-владелец RPL, соседний узел RPL или общий узел кольца

Протокол VLAN (Protocol VLAN) — конфигурация протокола, удаление протокола VLAN ERPS-кольца (<2–4094>)

VLAN данных (Data VLAN) —конфигурация VLAN данных ERPS-кольца (<1–4094>)

Порт кольца (Ring port) — конфигурация порта ERPS-кольца, удаление порта ERPS-кольца, порта RPL или общего порта кольца

Восстановить поведение (Restore Behavior) — настройка восстановления поведения ERPS-кольца: восстанавливаемое или невосстанавливаемое

Время задержки (Hold-Off Time)Настройте время задержки цикла ERPS (<0–10000>) в мс, значение по умолчанию равно 0

Время защиты (Guard Time) — Настройка времени защиты ERPS-кольца (<10–2000>) в мс, по умолчанию равно 500

Время WTR (WTR Time) — Настройка времени WTR ERPS-кольца (<1–12>) в минутах, по умолчанию 5

Время WTB (WTB Time) — Настройка времени WTB ERPS-кольца (<1–10>) в секундах, значение по умолчанию равно 5

Время передачи пакетов протокола Настройка времени отправки пакетов протокола ERPS-кольца (<1–10>) в секундах, значение по умолчанию равно 5

Включить ERPS-кольцо (Enable ERPS ring) — включение или выключение ERPS-кольца

Принудительно переключить порт ERPS-кольца (Force to switch ERPS ring port) —принудительное переключение, снять принудительное переключение порта ERPS-кольца

Принудительный ручной режим порта ERPS-кольца (Force manual ERPS ring port)— Снять принудительный ручной режим порта ERPS-кольца

Ручное восстановление (Manual recovery) — Обрабатывать восстановление невосстанавливаемого поведения ERPS-кольца или восстановление вручную до истечения времени WTR/WTB

To be updated.....

Рисунок 69 — Страница конфигурации EAPS

(2) Страница сведений о ERPS

На рис. 70 показана страница сведений о ERPS, на которой пользователи могут просматривать информацию о конфигурации ERPS.

To be updated.....

Рисунок 70 — Страница сведений о ERPS

20. Управление журналами

(1) Данные журнала

На рис. 71 показана страница данных журнала, пользователь может просматривать журнал на этой странице. Выберите приоритет из выпадающего списка. Вы можете просмотреть журнал этого уровня. Нажмите "Обновить" (Refresh) для просмотра последнего журнала.

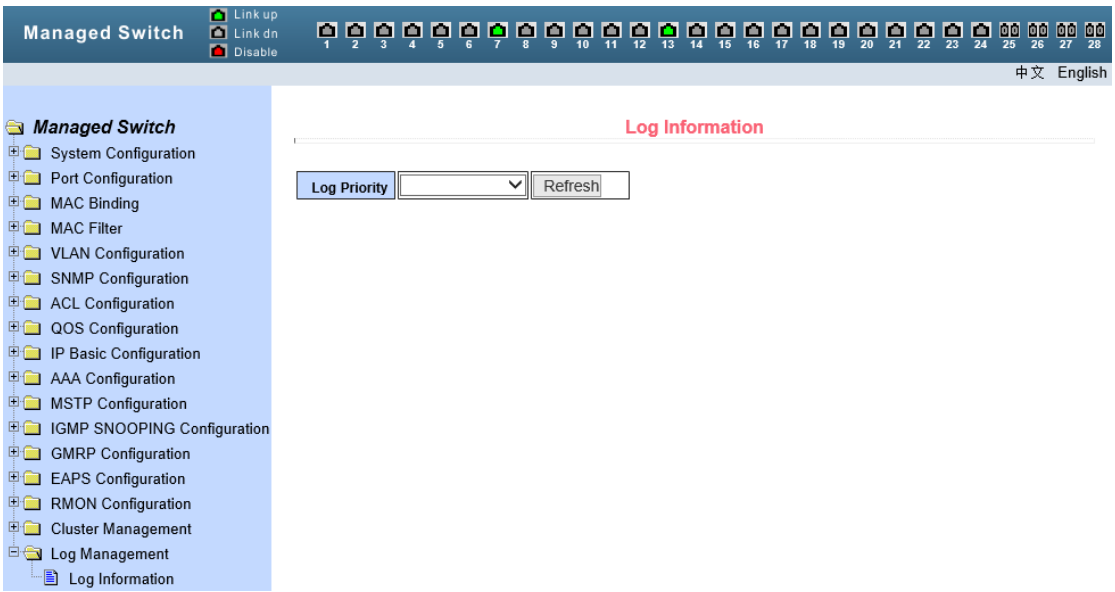


Рисунок 71 — Страница данных журнала