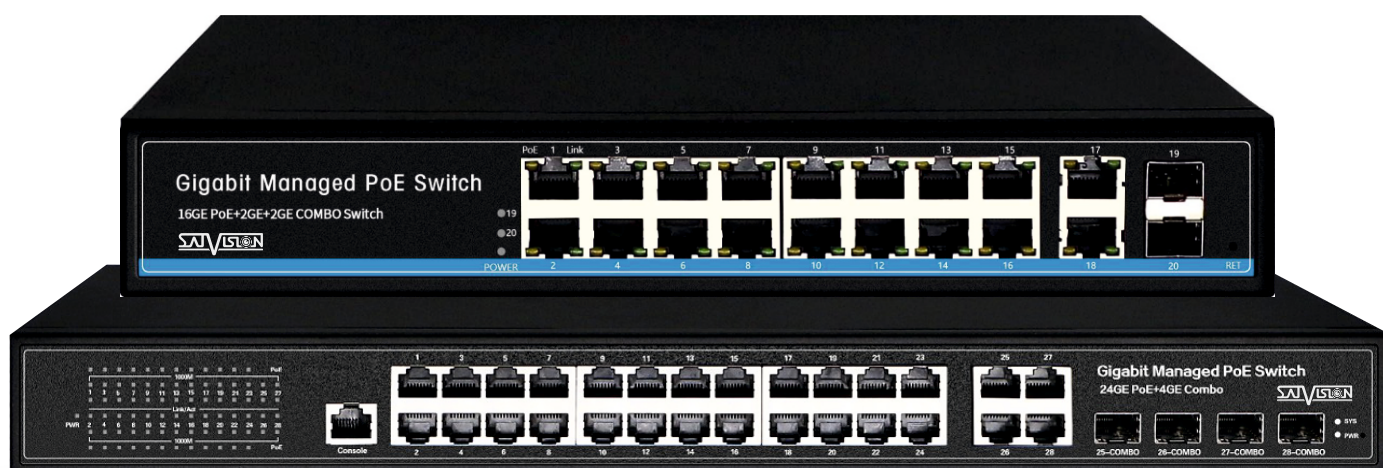


системы видеонаблюдения



ПОЛНОЕ РУКОВОДСТВО



УПРАВЛЯЕМЫЕ POE-КОММУТАТОРЫ

SVB-3316PC

SVB-3324PC WDT

Введение продукта

Коммутатор Ethernet разработан специально для обеспечения высокой безопасности и производительности сети. Система использует новую программную и аппаратную платформу, обеспечивает комплексную систему безопасности, совершенную стратегию QoS и расширенную функцию Vlan, простое управление и обслуживание, является идеальной офисной сетью, кампусной сетью и коммутатором конвергентного уровня для малых и средних предприятий и филиалов.

Функция 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, IEEE 802.1s
- Поддержка таблицы MAC-адресов 16К, автоматическое обновление, двустороннее обучение
- Поддержка VLAN на основе портов, до 4096 VLAN
- Поддержка VLAN стандарта 802.1Q
- Поддержка протокола связующего дерева STP
- Поддержка протокола быстрого связующего дерева RSTP
- Поддержка протокола быстрого связующего дерева MSTP
- Поддержка кольцевого сетевого протокола EPPS
- Поддержка кольцевого сетевого протокола EAPS
- Поддержка соглашения по аргументам 802.1x
- Поддержка 8 групп конвергенции, максимум с 8 портами в каждой группе
- Зеркала портов, поддерживающие двустороннюю связь приемопередатчика
- Поддержка функции защиты от замыкания, обнаружения в реальном времени, быстрой сигнализации, точного позиционирования, интеллектуальной блокировки, автоматического восстановления
- Поддержка нижестоящих портов для отделения друг от друга и связи с верхним портом
- Поддержка полудуплекса на основе управления обратным давлением
- Поддержка полного дуплекса на основе кадров ПАУЗЫ
- Управление пропускной полосы ввода/ вывода на основе портов
- Поддержка отслеживания IGMPv1/2/3 и MLDv1/2
- Поддержка регистрации протокола GMRP
- Поддержка управления адресами многоадресной рассылки, VLAN многоадресной рассылки, порт маршрутизации многоадресной рассылки, статического адреса многоадресной рассылки
- Поддержка перехвата DHCP

- Поддержка подавления шторма неизвестного одноадресного, многоадресного, неизвестного многоадресного, широковещательного типа
- Поддержка подавления штормов на основе регулирования полосы пропускания и штормфильтрации
- Поддержка пользовательского порта + IP-адреса + MAC-адреса
- Поддержка ACL на основе IP и MAC
- Свойства безопасности, поддерживающие количество MAC-адресов на основе портов
- Поддержка алгоритма приоритета очереди портов 802.1p
- Поддержка Cos/Tos, разметка QOS
- Поддержка WRR (Weighted Round Robin), алгоритма взвешенной ротации приоритетов
- Три режима планирования приоритетов, поддерживающие WRR, SP и WFQ
- Поддержка функции Auto-MDIX для автоматической идентификации по сетевым линиям и пересечения сетевых линий
- Порт поддержки поддерживает функцию автоматического согласования (скорость передачи с самостоятельным согласованием и дуплексный режим)
- Поддержка загрузки пакета обновления
- Поддержка просмотра системного журнала
- Поддержка ВЕБ-восстановления заводской конфигурации
- Поддержка открытия или закрытия порта
- Поддержка стандартного управления расписанием POE
- Поддержка автоматического определения функции сетевого оборудования (автоматически, без операции)
- 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

Содержание

ОБЗОР ВЕБ-СТРАНИЦЫ	5
1. Характеристики веб-доступа	5
2. Системные требования для просмотра веб-страниц	5
3. Вход в сеанс просмотра веб-страниц.....	5
4. Базовый состав веб-страницы.....	6
5. Древоподобная структура навигации.....	7
7. Сообщение об ошибке	9
8. Поле для ввода	9
ВВЕДЕНИЕ В ВЕБ-СТРАНИЦУ	11
1. Диалоговое окно входа в систему	11
2. Главная страница	12
3. Конфигурация системы	12
4. Конфигурация порта	20
5. Привязка к MAC	28
6. MAC-фильтр	30
7. Конфигурация VLAN	32
8. Конфигурация SNMP	35
9. Конфигурация ACL.....	37
10. Конфигурация QoS	43
11. Базовая конфигурация IP	45
12. Конфигурация AAA.....	48
13. Конфигурация MSTP	53
14. Конфигурация отслеживания IGMP	55
15. Конфигурация GMRP	57
16. Конфигурация EAPS.....	59
17. Конфигурация RMON.....	61
18. Конфигурация кластера	65
19. Конфигурация ERPS	68
20. Управление журналами.....	70
21. Конфигурация порта POE.....	71

ОБЗОР ВЕБ-СТРАНИЦЫ

1. Характеристики веб-доступа

Все коммутаторы Gigabit management Ethernet предоставляют пользователям веб-доступ. Пользователи могут получать доступ к коммутаторам через веб-браузеры для управления и настройки коммутаторов. Основными функциями веб-доступа являются:

- Простота доступа: пользователи могут легко получить 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 представлена пользователю в графическом и табличном виде.
- Коммутатор Gigabit management Ethernet предоставляет множество веб-страниц. Пользователи могут настраивать большинство функций этих коммутаторов и управлять ими с помощью этих веб-страниц.
- Классификация и интеграция функций веб-страницы, 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.

Аппаратное и программное обеспечение	Системные требования
ЦП	Pentium 586 и выше
ОЗУ	128 МБ и выше
Разрешение	800x600 и выше
Цвет	256 цветов и выше
Браузер	IE4.0 и выше или Netscape4.01 и выше
Операционная Система	Операционная система Microsoft ® , Windows95 ® , Windows98 ® , WindowsNT ® , Windows2000 ® , WindowsXP ® , WindowsME ® , WindowsVista ® , Windows7 ® , Windows8 ® , MAC, Linux, Unix

3. Вход в сеанс просмотра веб-страниц

Прежде чем начать сеанс просмотра веб-страниц, вам необходимо подтвердить:

- Что IP-адрес был настроен на коммутаторе. По умолчанию IP-адрес интерфейса VLAN1 коммутатора равен 192.168.0.1.
- Маска подсети 255.255.255.0.
- К сети подключен хост-компьютер с установленным веб-браузером, хост-компьютер может пинговаться через коммутатор.
- После выполнения двух вышеуказанных задач в адресной строке браузера введите адрес коммутатора и нажмите Enter, чтобы перейти на страницу веб-входа в коммутатор, как показано на рисунке 1. Когда многопользовательское управление не включено, пользователь вводит пароль по умолчанию admin.

Если в системе включено многопользовательское управление и настроены привилегированные пользователи, при подключении не выполняется проверка пароля, но выполняется проверка подлинности имени пользователя и пароля для многопользовательского управления.

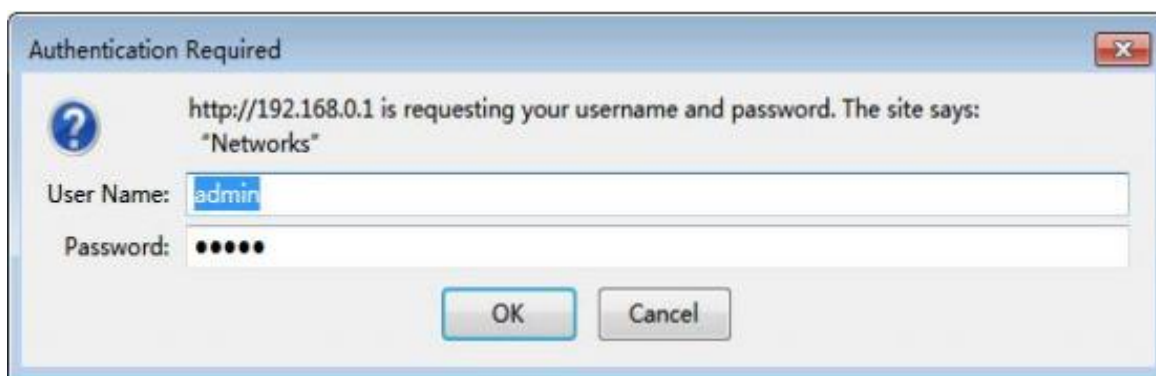


Рис. 1 Страница входа в систему для сеанса просмотра

4. Базовый состав веб-страницы

Рисунок 2. Веб-страница состоит из трех частей: титульной страницы, страницы дерева навигации и главной страницы.

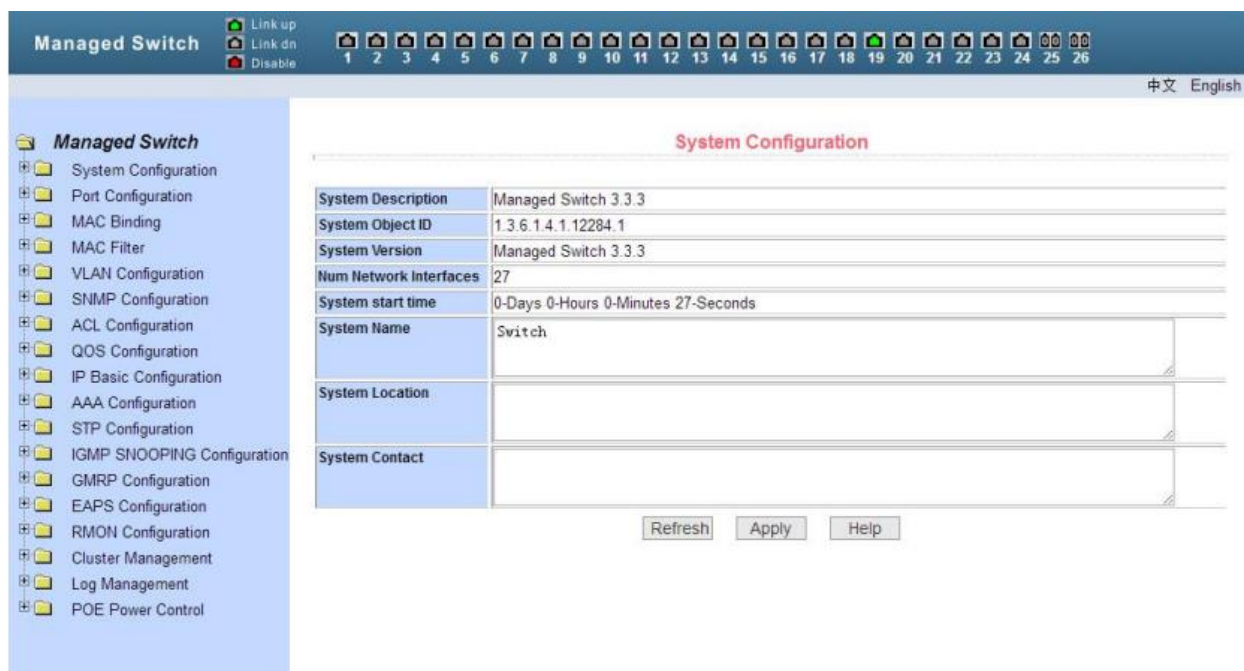


Рис. 2 Переключение веб-страницы на страницу базовой композиции

Титульная страница

Используется для отображения логотипа и состояния порта в режиме реального 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 рисунке 17)



Главная страница

используется для отображения страницы, выбранной пользователем из дерева навигации.

5. Древоподобная структура навигации

На рисунке 3 показана организация дерева навигации.

Дерево навигации расположено в левом нижнем углу каждой страницы, отображая узлы веб-страницы в виде дерева, пользователь может легко найти веб-страницу,

которой нужно управлять. В соответствии с различными функциями страница будет разделена на разные группы, каждая группа включает в себя одну или несколько страниц. Большинство веб-страниц в дереве навигации являются сокращениями названия страницы в верхней части соответствующей страницы.

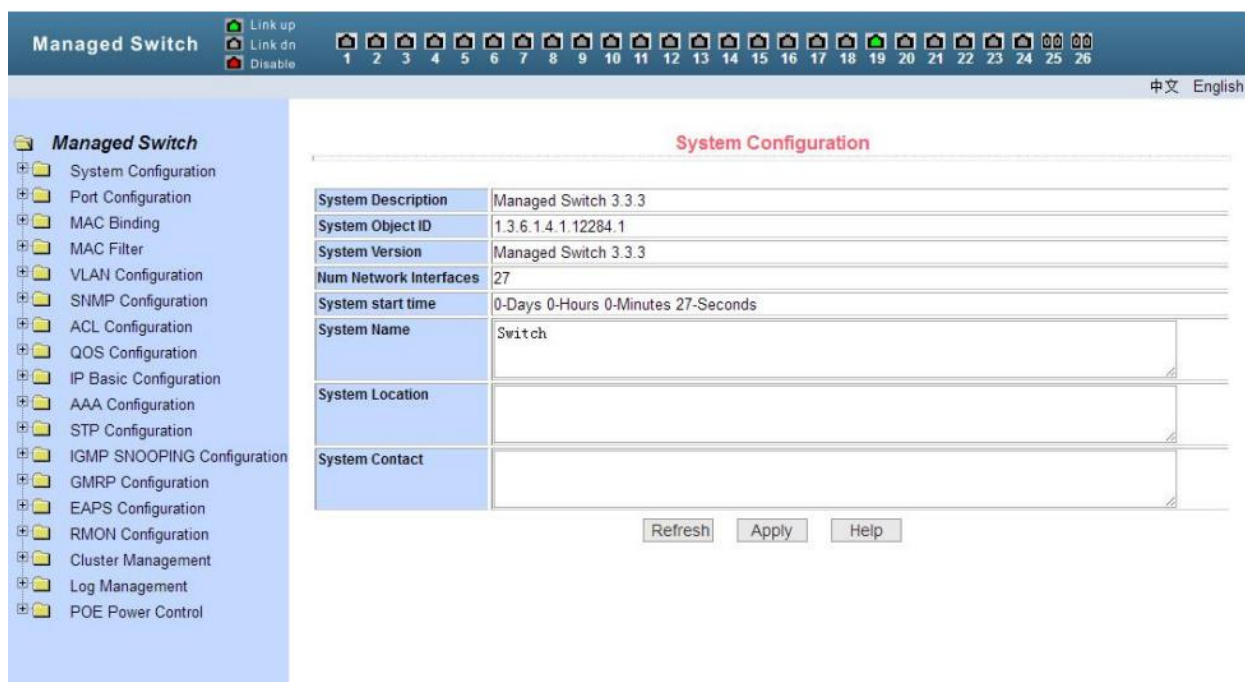


Рис. 3 Переключение страницы организации дерева навигации

6. Введение кнопки страницы

На странице есть несколько общих кнопок, роль этих кнопок в целом одинакова, в таблице 2 показаны роли этих кнопок для ознакомления.

Таблица 2:

Кнопка	Действие
Refresh	Обновить все поля на странице
Application	Сохранить обновленные значения в памяти. Поскольку проверка ошибок выполняется веб-сервером, проверка ошибок не выполнится до того, пока пользователь не нажмет кнопку
Delete	Удалить текущую запись
Help	Открыть страницу справки и просмотреть инструкции по настройке для каждой страницы

7. Сообщение об ошибке

Если коммутатор выдает ошибку при обработке пользовательских запросов, в диалоговом окне отображается соответствующее сообщение об ошибке. Например, на рисунке 4 показано диалоговое окно с сообщением об ошибке.



Рис. 4 Страница с сообщением об ошибке

8. Поле для ввода

В крайнем левом столбце таблицы есть несколько страниц, на которых есть поле ввода, как показано на рисунке 5, через которое вы можете получить доступ к различным разделам. Когда вы выбираете значение в поле ввода, соответствующая информация для этой строки отображается в первой строке, и редактировать можно только активную строку. При загрузке первой страницы в поле ввода отображается новая, пустая активная строка.

Если вы хотите добавить новую строку, выберите создать в выпадающем меню поля ввода, введите информацию о новой строке и нажмите клавишу «Применить».

Если вы хотите отредактировать существующую строку, выберите соответствующий номер строки в выпадающем меню поля ввода, отредактируйте строку по мере необходимости и нажмите клавишу «Применить». Вы увидите соответствующее изменение, отображаемое в таблице.

Если вы хотите удалить строку, выберите соответствующий номер строки из выпадающего меню в поле ввода и нажмите клавишу «Удалить», после чего строка исчезнет из таблицы.

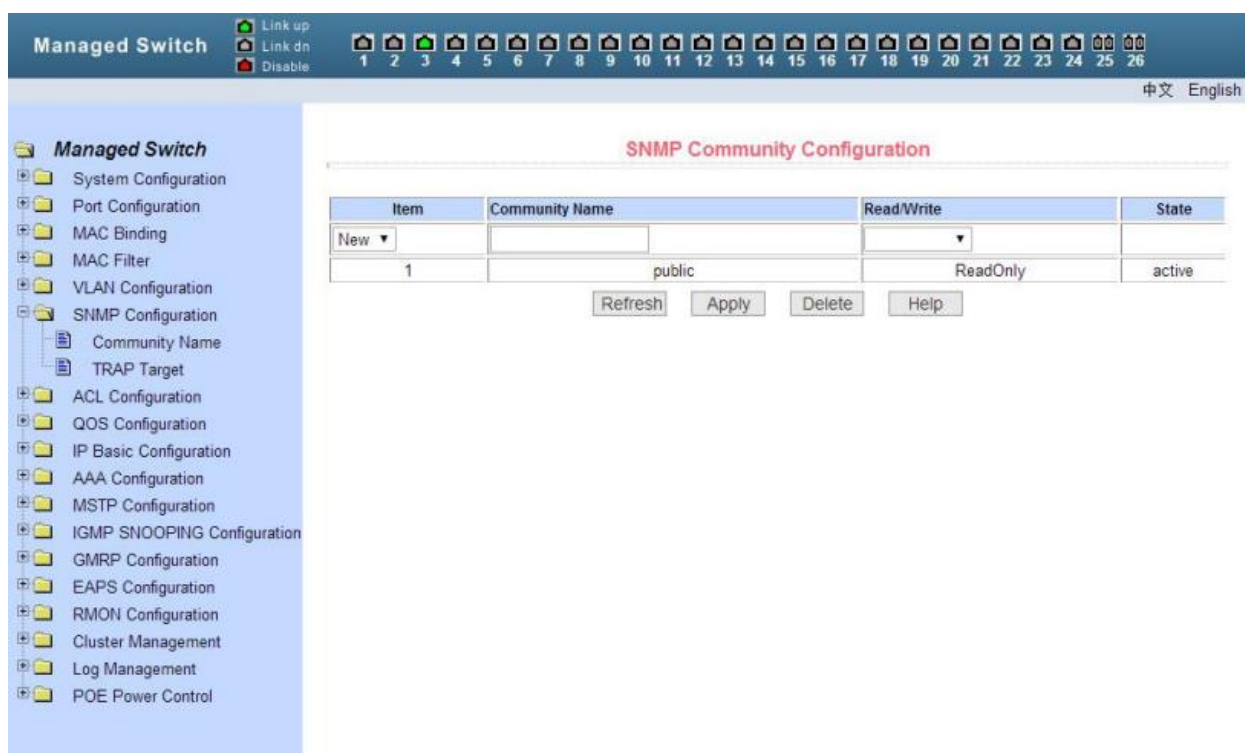


Рис. 5 Страница поля ввода

9. Поле состояния

В крайнем правом столбце таблицы есть несколько страниц, на которых есть поле состояния, как показано на рисунке 6, где поле показывает исходное состояние. Поскольку все изменения состояния строк обрабатываются внутри, поле состояния доступно только для чтения. Как только вся информация о домене в строке становится действительной, состояние строки автоматически становится активным.

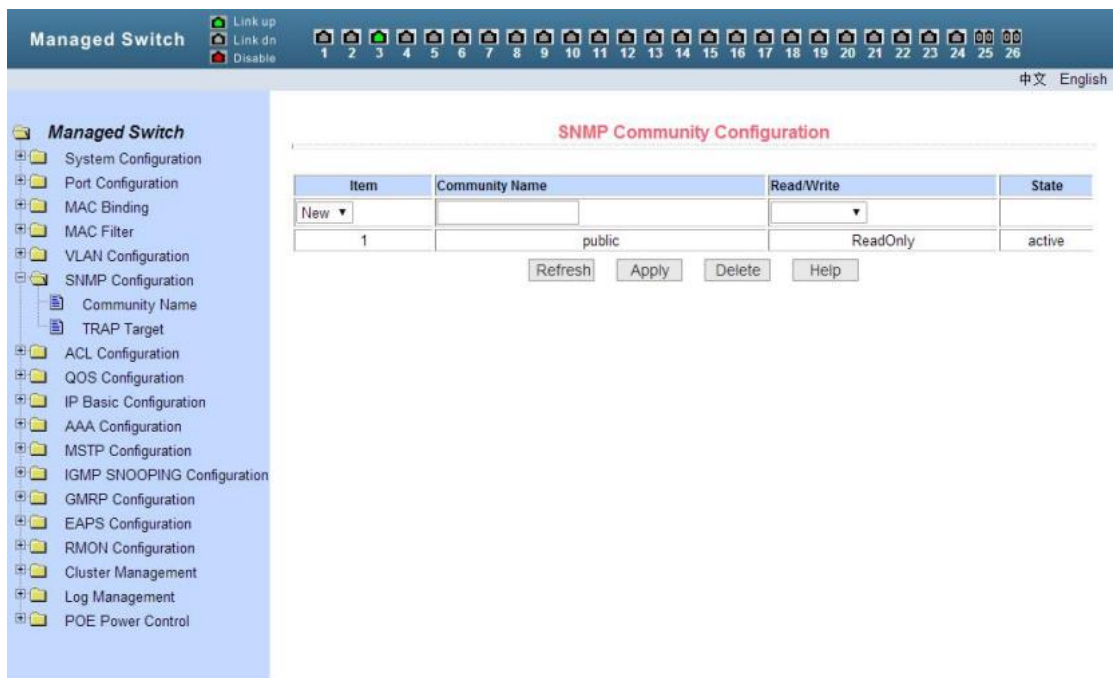


Рис. 6 Страница поля состояния

ВВЕДЕНИЕ В ВЕБ-СТРАНИЦУ

1. Диалоговое окно входа в систему

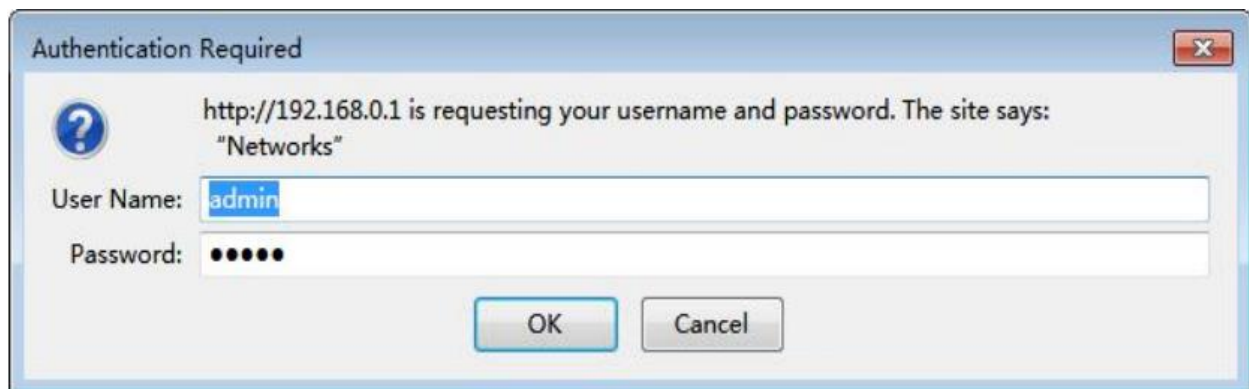


Рис. 7 Окно входа в систему

На рисунке 7 показано диалоговое окно входа в систему, которое отображается при первом входе пользователя на веб-страницу. Пользователь вводит имя пользователя и пароль в соответствующее поле, а затем нажимает клавишу «ОК» для входа на веб-сервер коммутатора. Пароль чувствителен к регистру, пароль может содержать до 16 символов, а имя пользователя и пароль для нескольких пользователей могут содержать до 16 символов.

Имя пользователя по умолчанию для коммутатора - «admin». Пароль по умолчанию пуст.

2. Главная страница

На рисунке 8 показана главная веб-страница коммутатора. Страница будет отображена после входа пользователя на страницу.

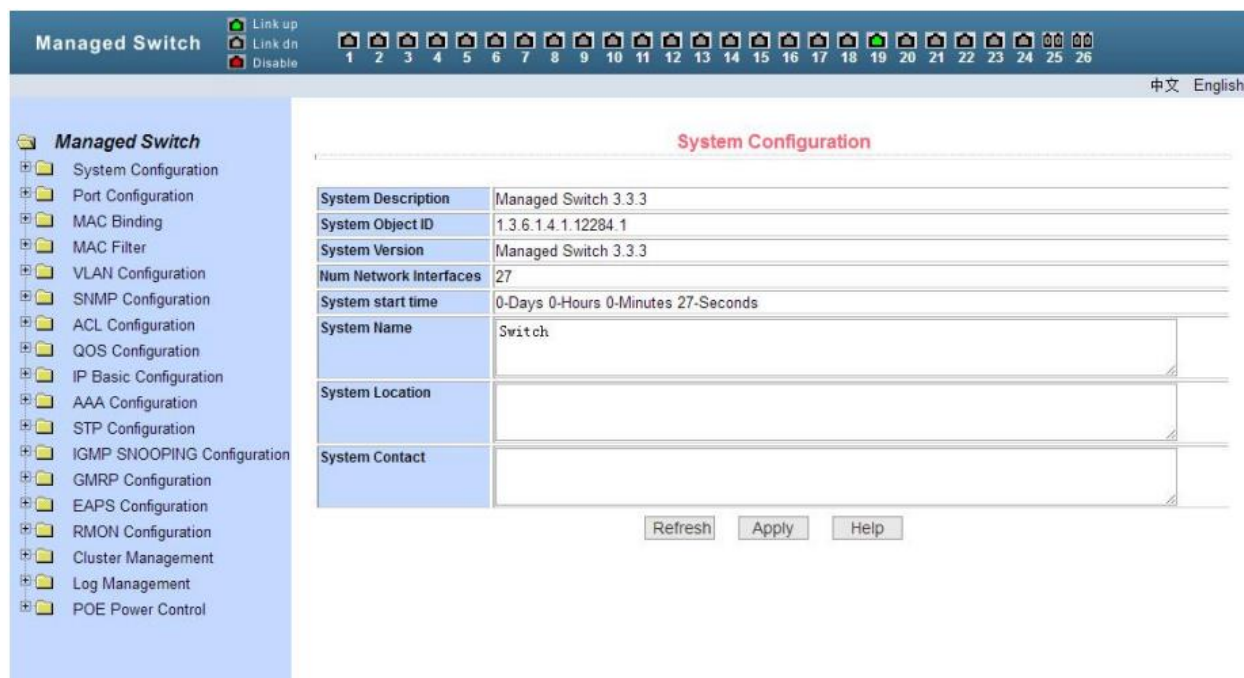


Рис. 8 Переключение главной страницы

3. Конфигурация системы

Переключение языков: кнопки в правом верхнем углу позволяют легко переходить между китайским и английским системными интерфейсами.



(1) Страница с основной информацией

На рисунке 9 показана страница конфигурации основной информации, где пользователь может настроить основную информацию для коммутатора. Описание системы: отображает описание параметров, связанных с системой. Идентификационный номер системного дескриптора указывает идентификатор системы в сетевом управлении. Номер версии системы показывает номер версии текущего программного обеспечения, используемого коммутатором.

Количество сетевых интерфейсов: отображает текущее количество сетевых интерфейсов в коммутаторе.

Время запуска системы: отображает время работы коммутатора с момента последнего включения.

Системные часы отображают текущее установленное время системы. Пользователь может его, изменить для этого необходимо ввести значения года, месяца, дня, часа, минуты и секунды.

Системное имя: отображает системное имя коммутатора в сети. Пользователь может изменить системное имя.

Системное местоположение отображает местоположение коммутатора в сети, и пользователь может изменить системное местоположение.

Системный контакт отображает управление текущими узловыми контактами и контактной информацией, пользователь может изменить системный контакт.

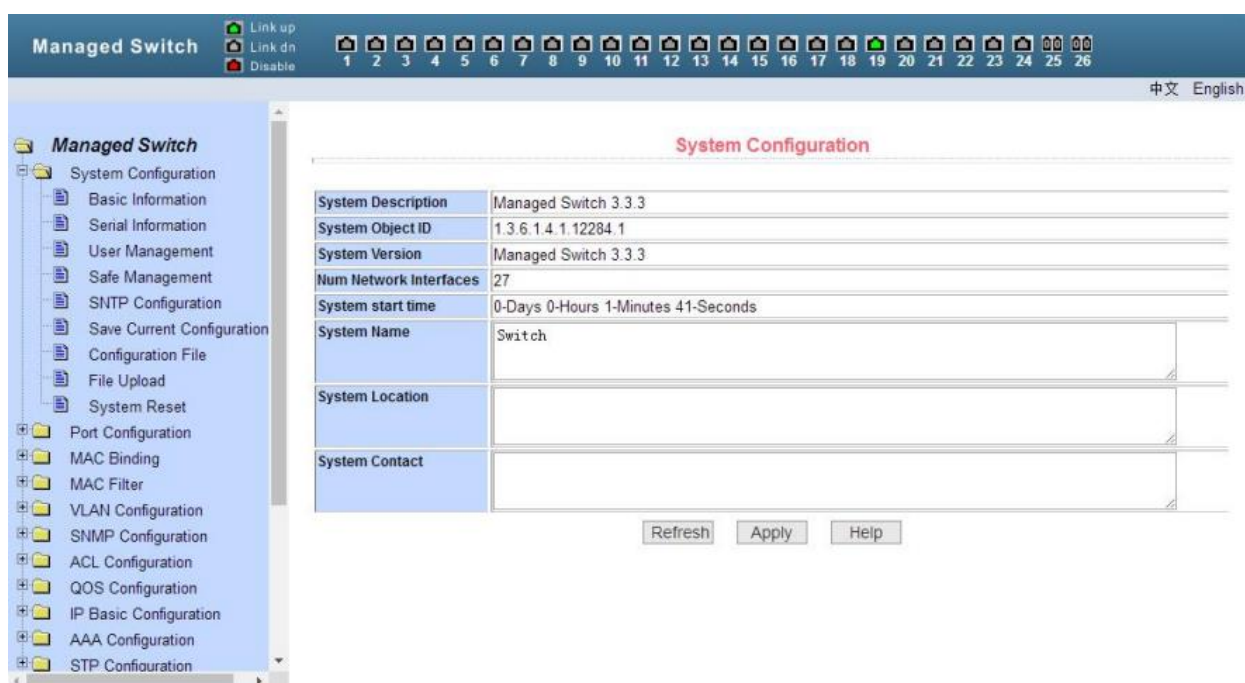


Рис. 9 Страница с основной информацией

(2) Страница конфигурации последовательного порта

На рисунке 10 показана страница конфигурации последовательного порта, на которой показана скорость передачи данных в бодах и другая информация, относящаяся к последовательному порту. Когда хост использует последовательный терминал (например, Windows HyperTerminal) для управления коммутатором, конфигурация терминала последовательного порта должна соответствовать информации на этой странице.

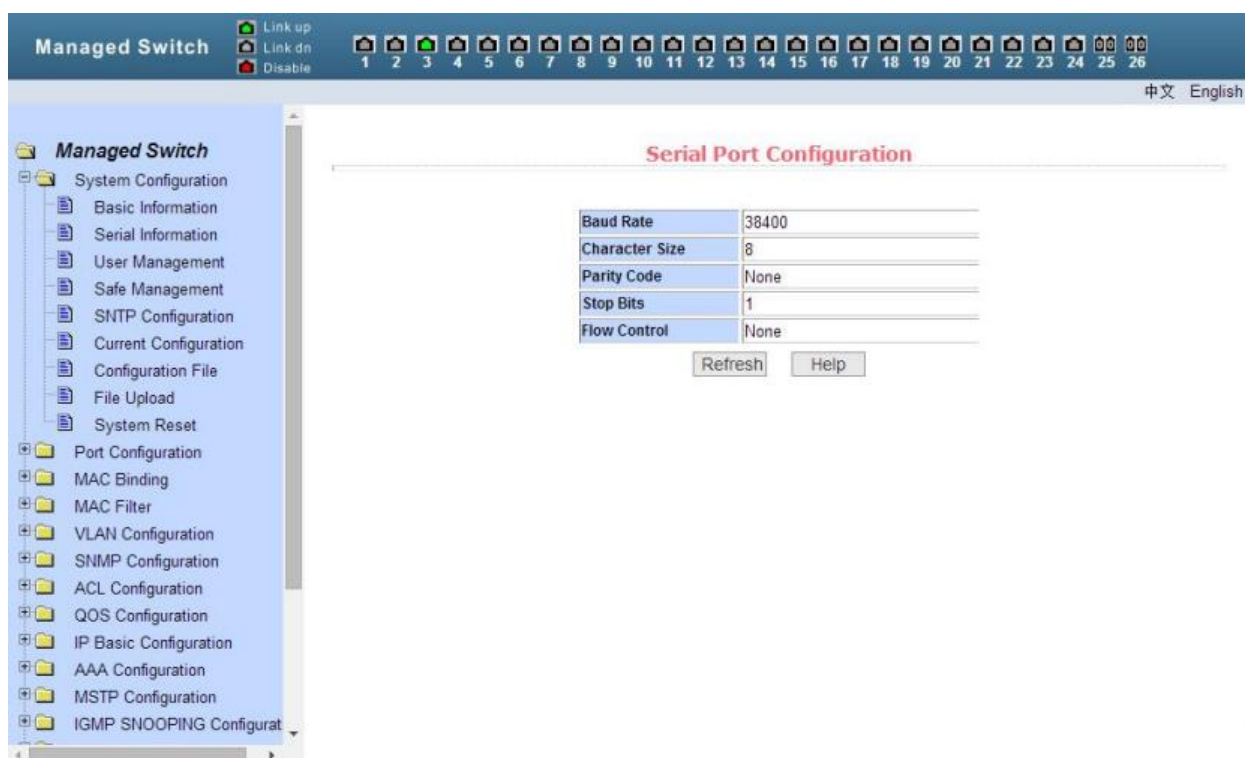


Рис. 10 Страница конфигурации последовательного порта

(3) Страница конфигурации многопользовательского управления

На рисунке 11 показана страница конфигурации многопользовательского управления, на которой пользователи могут изменять пароль анонимного пользователя коммутатора. Telnet и Web используют один и тот же пароль пользователя, когда не включены несколько пользователей. Пароли чувствительны к регистру, и вы можете ввести не более 16 символов. Если вы хотите изменить пароль, вам необходимо ввести новый пароль дважды, после чего активируется новый пароль, если коммутатор не включен в режиме многопользовательской работы, отобразится диалоговое окно входа в систему (показано на рисунке 7), вам необходимо повторно войти на страницу и ввести новый анонимный пароль.

В то же время через эту страницу пользователи могут настроить несколько пользователей, коммутатор по умолчанию находится в не многопользовательском режиме, то есть по умолчанию не включены функции многопользовательского управления, тогда 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 Интернета, когда имя пользователя добавлено и если вы являетесь привилегированным пользователем, функция многопользовательского управления включена, когда все привилегированные пользователи удаляются, функция многопользовательского управления снова отключается. Пока функция многопользовательского управления включена, система не будет запрашивать пароль, для входа в Telnet и Web требуется многопользовательская аутентификация по имени

пользователя и паролю. Когда функция многопользовательского управления выключена, в это время, если настроен пароль, для входа в Telnet и Web потребуется проверка пароля.

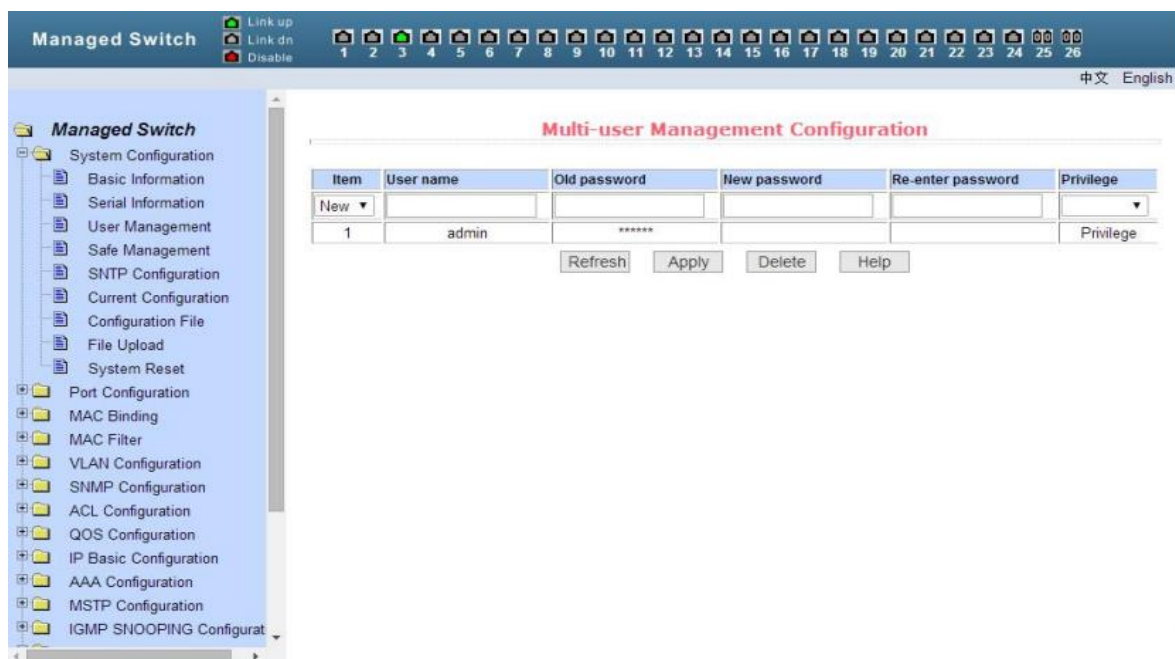


Рис. 11 Страница конфигурации многопользовательского управления

(4) Страница настройки безопасности пользователя

На рисунке 12 показана страница конфигурации безопасности пользователя, через конфигурацию страницы администратор может управлять службами сетевого управления TELNET, WEB и SNMPcontrol, вы можете открывать или закрывать эти службы, которые могут быть связаны с группой ACL IPstandard, реализацией контроля исходного IP-адреса, управлением хостом доступ к этим сервисам.

В коммутаторе по умолчанию службы TELNET, WEB и SNMP открыты и не выполняют фильтрацию ACL, то есть все хосты могут получить доступ к коммутатору этих трех служб. Если администратор по соображениям безопасности не хочет предоставлять другим пользователям одну или несколько из этих служб, он может отключить одну или несколько из этих служб. Если администратору нужно, чтобы доступ к одной или нескольким из этих служб имел только определенный хост, то одна или несколько из этих служб может выполнять фильтрацию ACL. Когда службе необходимо выполнить фильтрацию ACL, вам нужно открыть службу и выбрать стандартную группу ACL IP (1-99). Группа ACL должна существовать.

Следует отметить, что если администратор на этой странице управляет веб-службой (например, закрывает веб-службы), это может привести к тому, что пользователи больше не смогут использовать веб-страницу, в это время можно использовать другие способы входа на коммутатор и управления веб-службами, чтобы пользователи могли использовать веб-страницу (например, открыть веб-сервис).

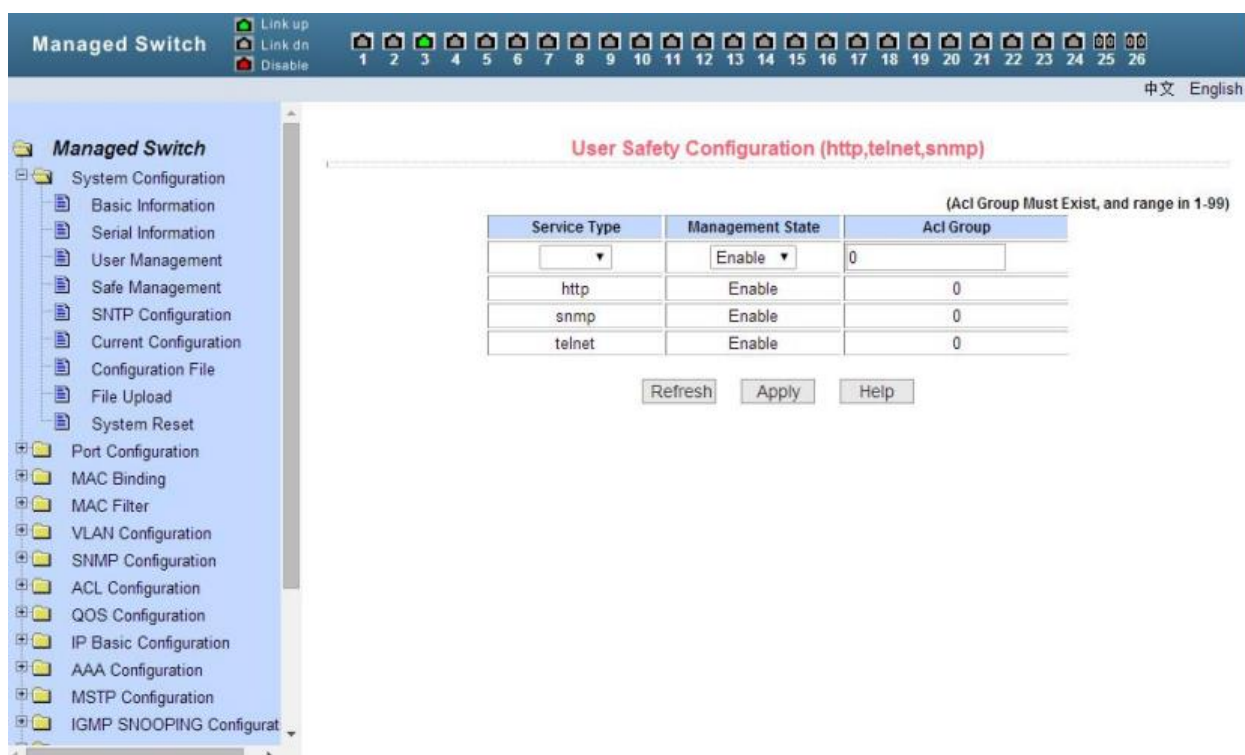


Рис. 12 Страница настройки безопасности пользователя

(5) Страница конфигурации SNMP

На рисунке 13 показана страница конфигурации SNTP, где администратор может настроить и просмотреть системные часы с помощью настройки страницы.

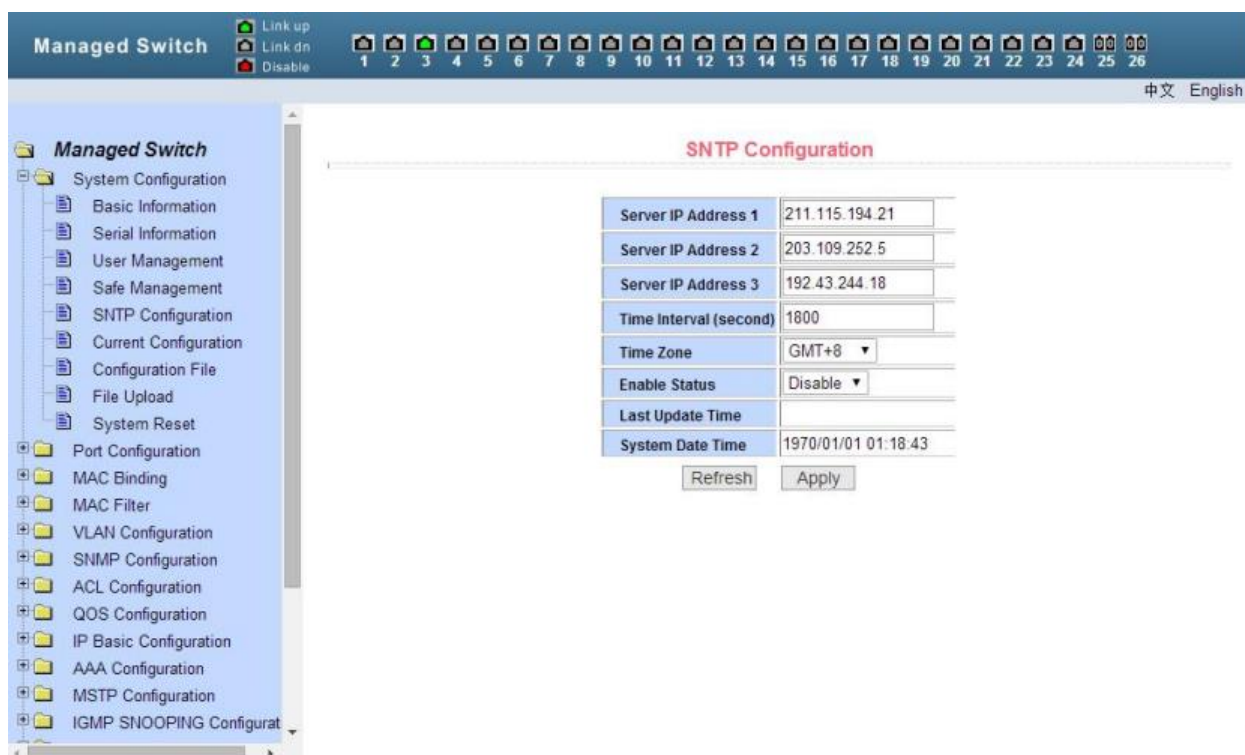


Рис. 13 Страница конфигурации SNTP

(6) Страница текущего конфигурационного файла

На рисунке 14 показана страница текущего файла конфигурации. На этой странице пользователь может просмотреть текущую конфигурацию коммутатора и сохранить текущую конфигурацию системы в файле конфигурации с помощью клавиши сохранения. Для операции сохранения необходимо стереть флэш-память, что займет определенное количество времени. Если пользователь настроил всё необходимое на странице и хочет, чтобы конфигурация не была потеряна после перезапуска коммутатора, необходимо нажать кнопку «Сохранить» перед выходом со страницы текущей конфигурации.

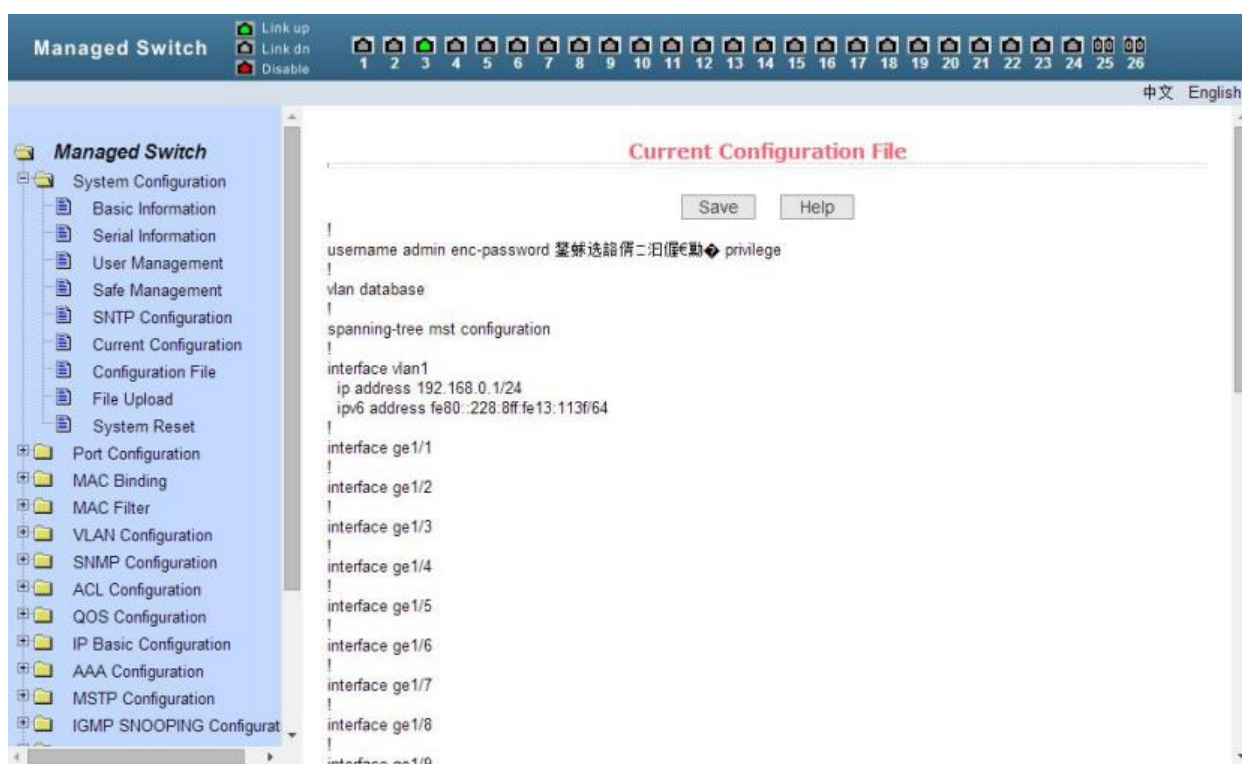


Рис. 14 Страница текущего конфигурационного файла

(7) Страница конфигурационного файла

На рисунке 15 показана страница файла конфигурации. Эта страница позволяет пользователю просмотреть начальную конфигурацию системы. Начальная конфигурация является файлом конфигурации во FLASH, когда файла конфигурации во FLASH нет, система запускается с конфигурацией по умолчанию. Клавиша «Удалить» для удаления файла конфигурации во FLASH. Нажмите кнопку «Удалить», появится диалоговое окно, в котором пользователю предлагается определить, следует ли удалять файл конфигурации, если да то нажмите кнопку «ОК», в противном случае нажмите кнопку «Отмена». Кнопка «Ключ загрузки» используется для загрузки файла конфигурации на ПК. Нажмите кнопку загрузки, появится диалоговое окно, пользователь должен выбирать путь к каталогу и сохранить файл конфигурации. Имя загруженного файла конфигурации - switch.cfg.

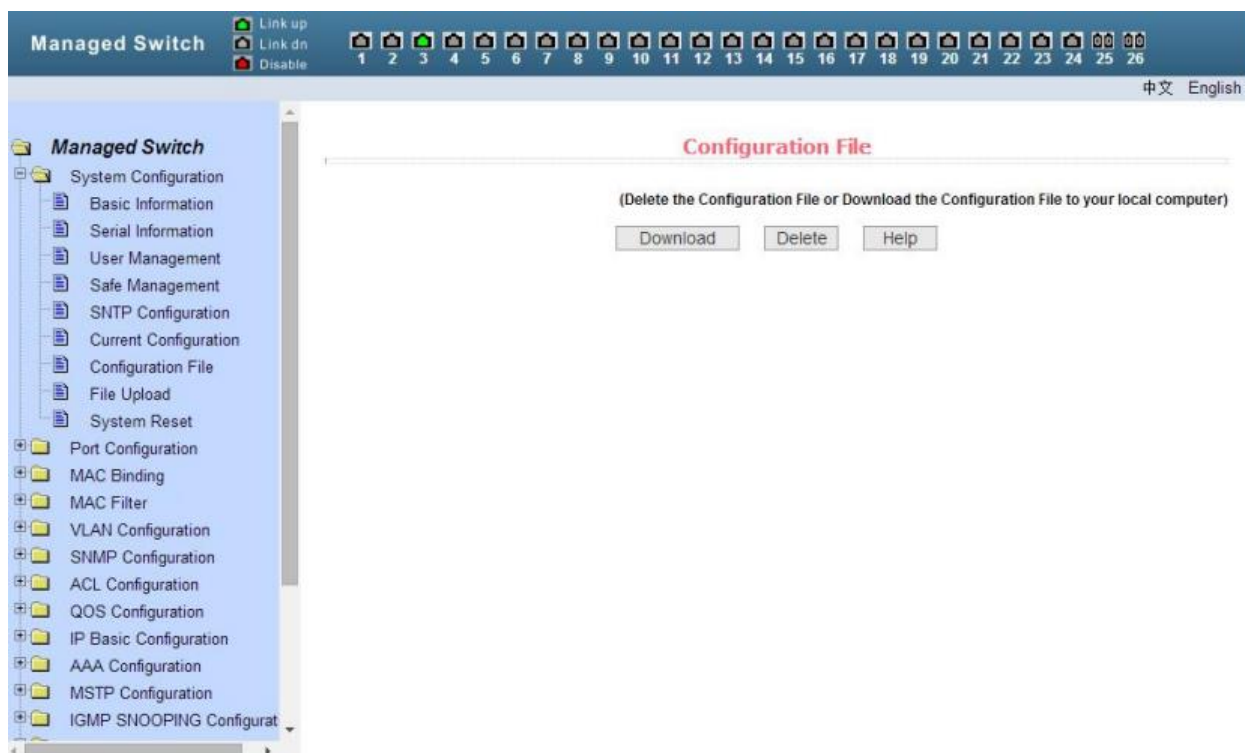


Рис. 15 Страница конфигурационного файла

(8) Страница загрузки файла

На рисунке 16 показана страница загрузки файлов, с помощью которой пользователи могут загружать файлы конфигурации и изображения на коммутатор. Нажмите кнопку «Обзор», чтобы выбрать путь к каталогу загруженного профиля или файла изображения на ПК. Нажмите кнопку «Загрузить», чтобы загрузить файл конфигурации или файл изображения. Окончание файла конфигурации должно 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 страницы результатов переноса. В противном случае сбой передачи файла приведет к аварийному завершению работы системы.



Рис. 16 Страница загрузки файла

(9) Страница сброса системы

На рисунке 17 показана страница сброса системы, с помощью которой пользователи могут перезапустить коммутатор. Когда вы нажмете кнопку перезапуска, появится диалоговое окно с запросом, уверен ли пользователь в перезапуске коммутатора. Если все в порядке, нажмите клавишу «ОК». В противном случае нажмите клавишу «Отмена». Веб-страница больше не будет открываться при ее перезапуске.

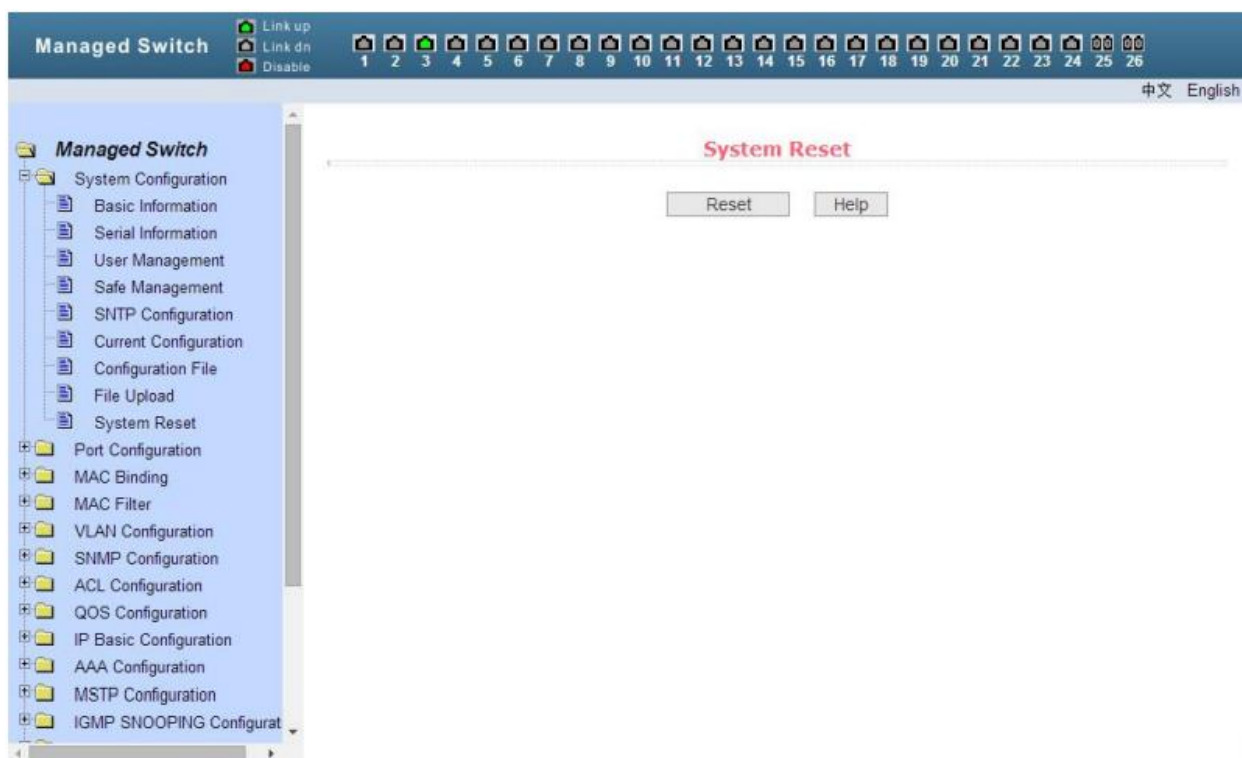


Рис. 17 Страница сброса системы

4. Конфигурация порта

(1) Конфигурация порта/показать страницу

На рисунке 18 показана страница настройки порта/отображения. Пользователь может включить или отключить порт на этой странице, установить скорость порта или просмотреть основную информацию обо всех портах. Чтобы задать определенный порт, выберите подходящее название порта в выпадающем меню для порта пользователя. Статус порта по умолчанию равен «up», и вы можете выбрать «down» в выпадающем меню, чтобы отключить порт. Пользователь также может выбрать настройку скорости в раскрывающемся меню, чтобы задать скорость порта, например, обязательную полудуплексную для порта, 10 М (половина 10) и т.д. Пользователи могут просмотреть другую основную информацию для всех портов на этой странице.

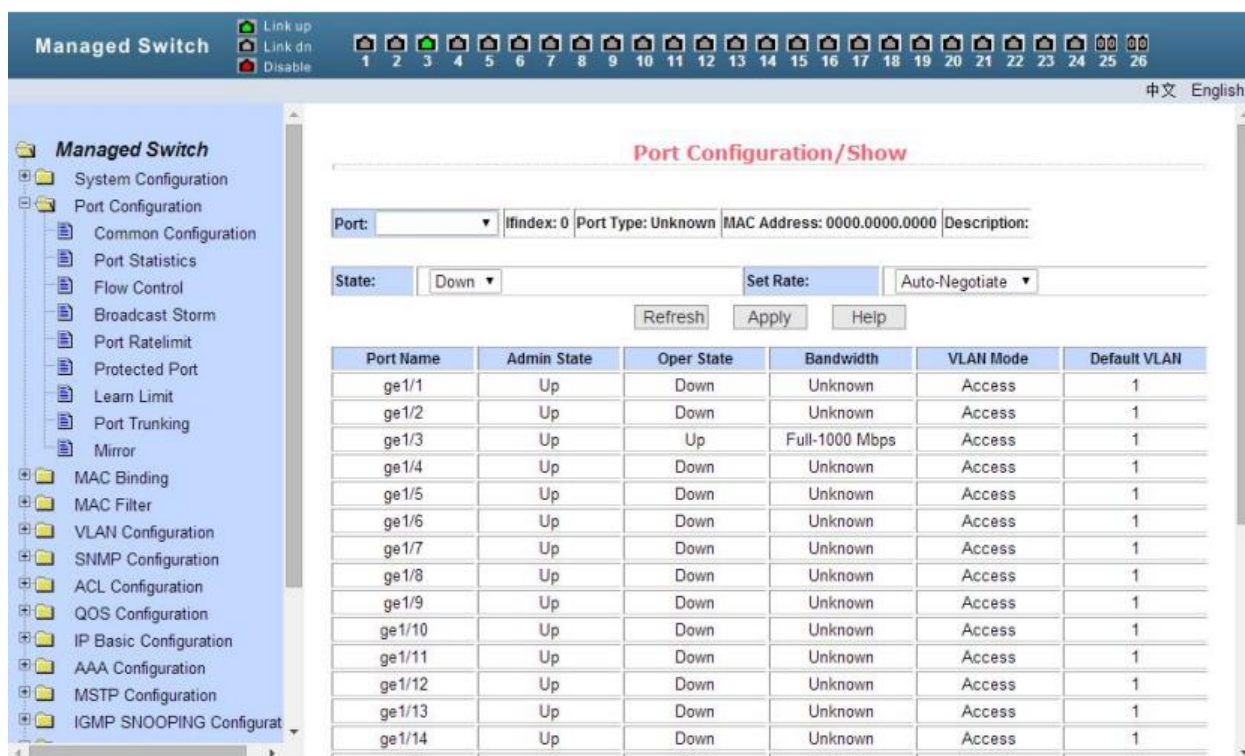


Рис. 18 Конфигурация порта/показать страницу

(2) Страница с информацией о статистике портов

На рисунке 19 показана страница информации о статистике портов. Чтобы просмотреть конкретный порт, выберите нужное название порта в выпадающем меню для порта пользователя. Пользователи могут просматривать статистику отправки и получения пакетов через порт на этой странице.

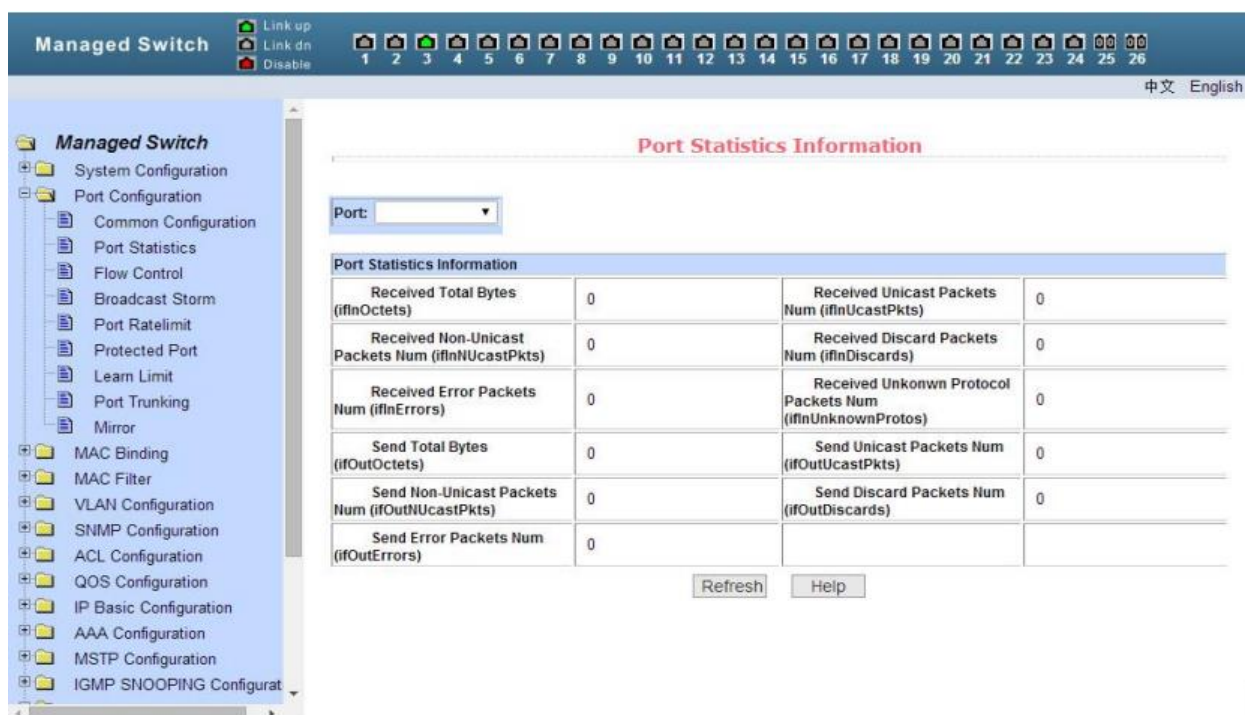


Рис. 19 Страница с информацией о статистике портов

(3) Страница управления потоком

На рисунке 20 показана страница управления потоком. Пользователь может использовать эту страницу для открытия или закрытия управления потоком для каждого порта.

С помощью раскрывающегося списка «Включить» или «Выключить» управления потоком можно открыть или закрыть управление потоком порта. В то же время на этой странице вы можете просмотреть состояние управления потоком всех портов.

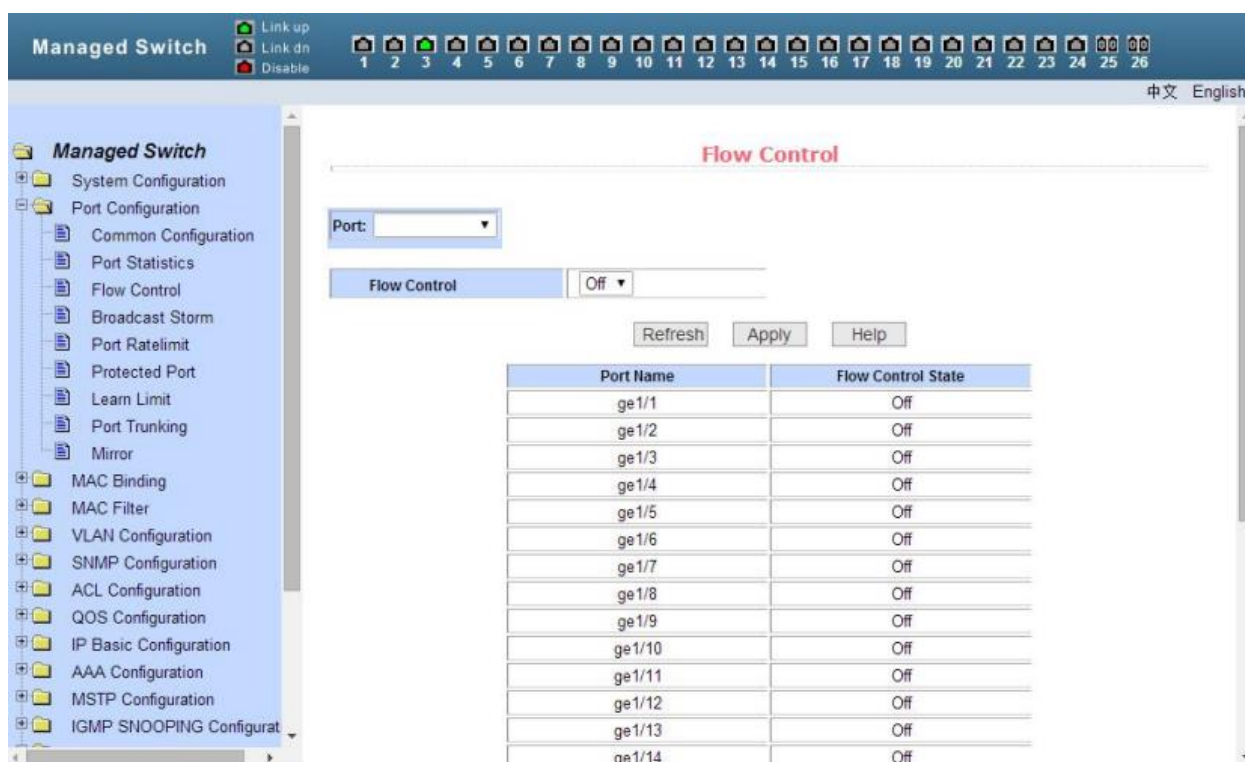


Рис. 20 Страница управления потоком

(4) Страница управления широковещательным штормом

На рисунке 21 показана страница управления широковещательным штормом. Эта страница используется для настройки подавления широковещательных пакетов, многоадресных пакетов и пакетов DLF на порту.

Выберите порт, который нужно настроить, из выпадающего списка порта. «Вкл.» и «Выкл.», чтобы включить или отключить подавление широковещательной рассылки, подавление многоадресной рассылки и подавление DLF порта. Термин "скорость подавления" используется для настройки скорости подавления порта в диапазоне 1-1024000 в кбит. Скорости подавления широковещательной рассылки, групповой рассылки и самоподавления на одном и том же порту равны. В то же время, на этой странице вы можете просмотреть конфигурацию управления широковещательным штормом всех портов.

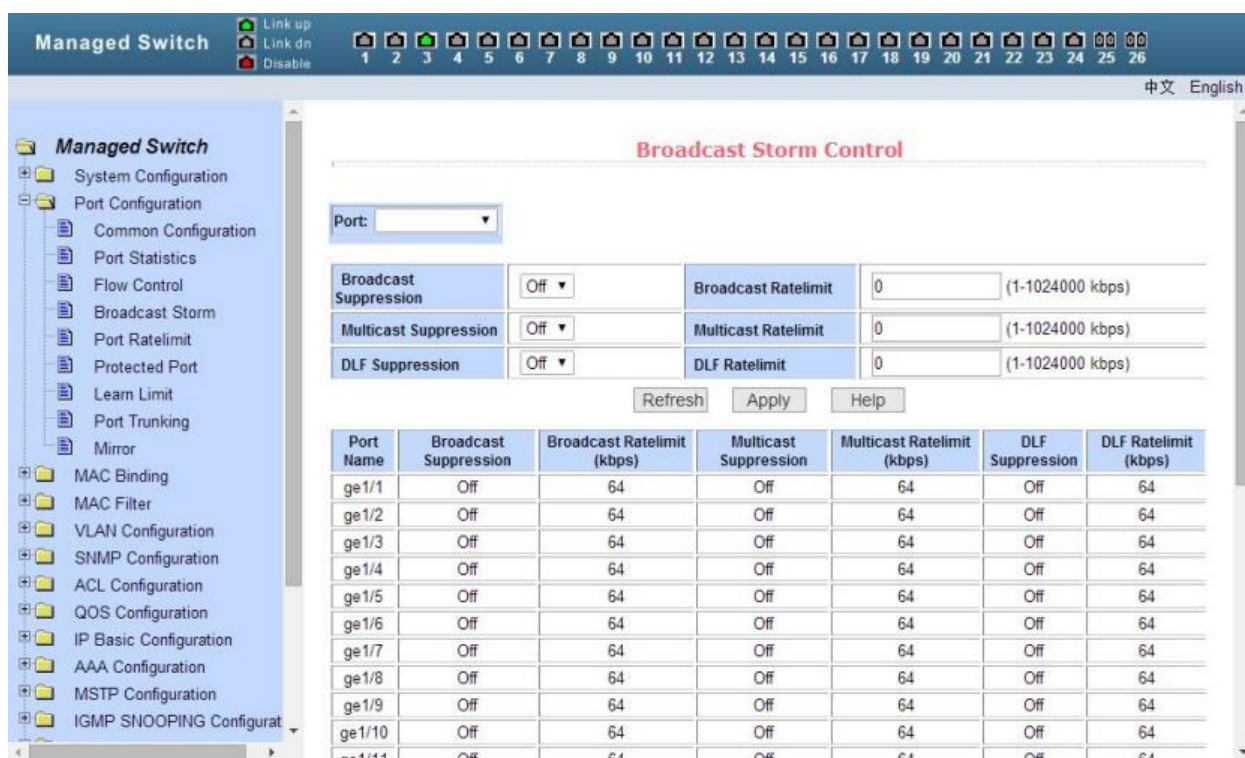


Рис. 21 Страница управления ширококвещательным штормом

(5) Страница ограничения скорости порта

На рисунке 22 показана страница ограничения скорости порта. Эта страница используется для настройки скорости, с которой отправляются и принимаются порты.

Выберите порт, который нужно настроить, из выпадающего списка порта. Управление полосой пропускания передаваемого пакета используется для настройки и отображения управления полосой пропускания отправляемого пакета данных в диапазоне 1-1024000 кбит. После ввода нажмите клавишу «Продолжить», чтобы настройки вступили в силу. Если порт не настроен для управления пропускной полосой, он отображается как выключенный. Соответствующая клавиша отмены используется для отмены управления пропускной полосой отправляющего пакета данных. Управление пропускной полосой принимающего пакета данных используется для настройки и отображения управления пропускной полосой отправляющего пакета данных. Полученный пакет, в диапазоне 1-1024000 кбит, после ввода доступен для сохранения. Если порт не настроен для управления полосой пропускания, он отображается как выключенный. Соответствующая клавиша отмены используется для отмены управления полосой пропускания принимаемого пакета данных.

Если порт настроен с возможностью управления пропускной полосой, он будет отображен в списке.

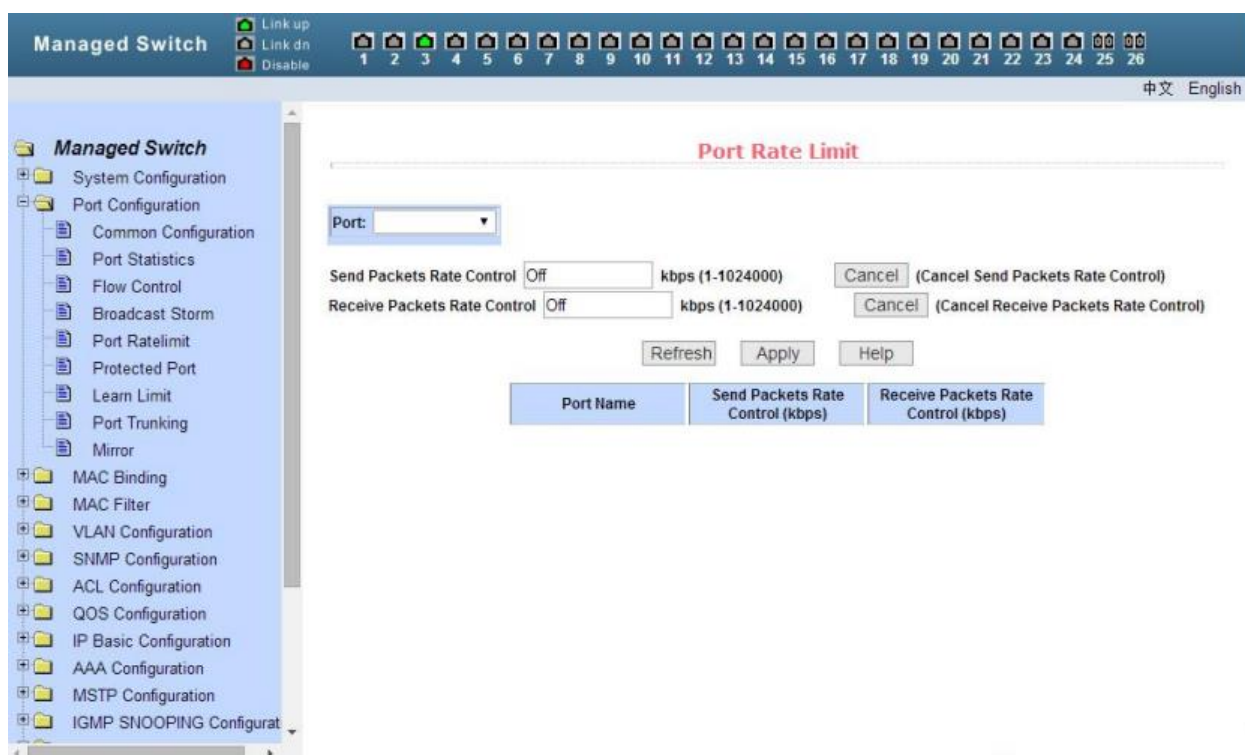


Рис. 22 Страница ограничения скорости порта

(6) Страница защищенного порта

На рисунке 23 показана страница защищенного порта, используемая для его настройки.

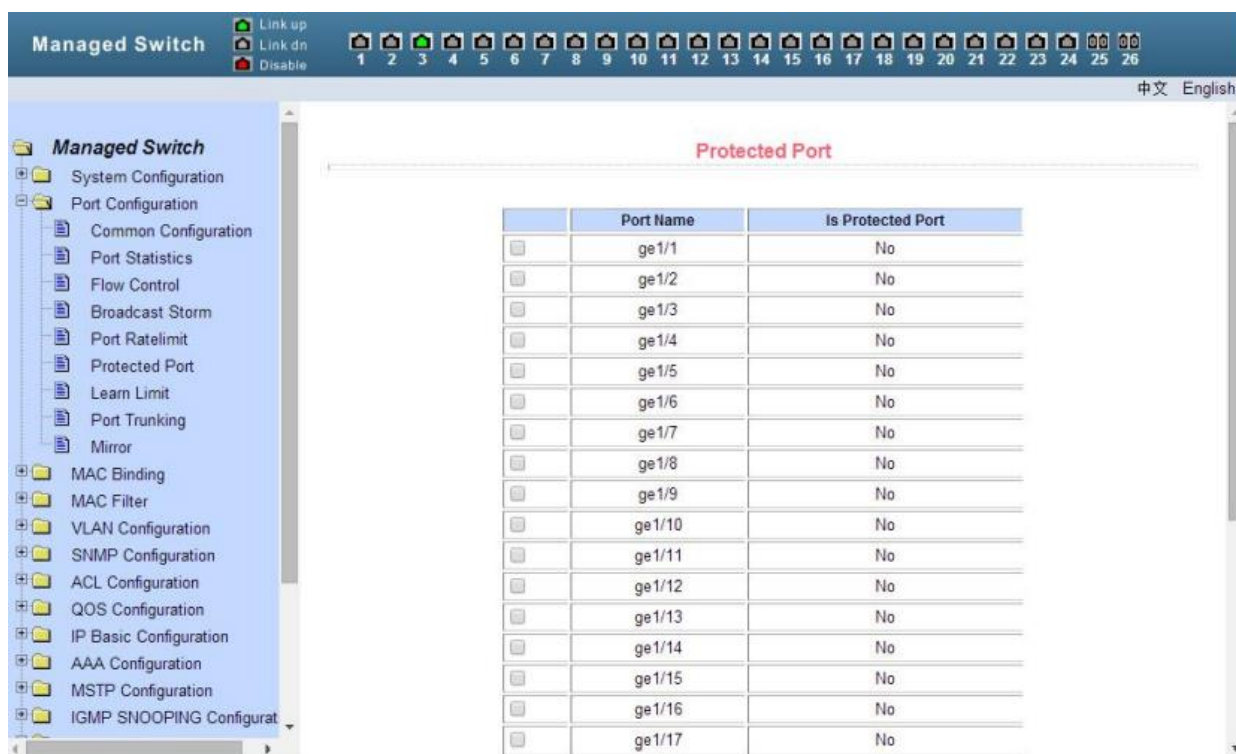


Рис. 23 Страница защищенного порта

(7) Страница ограничения для изучения порта

На рисунке 24 показана страница ограничения для изучения порта. Она используется для ограничения количества MAC-адресов, которые могут узнать порт. Диапазон 0-8191. Значение по умолчанию равно 8191, что также является максимальным значением, указывающим на то, что порт не настроен с ограничениями для обучения. В списке показаны ограничения для обучения для всех портов.

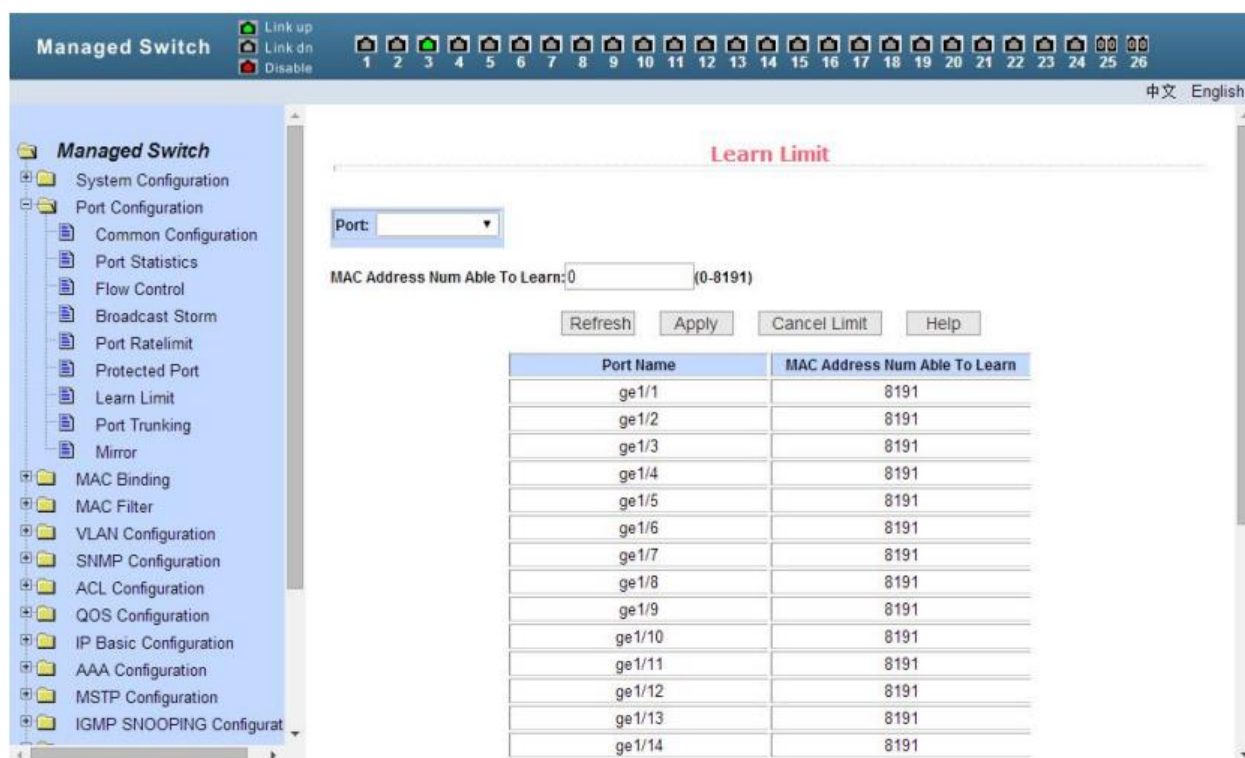


Рис. 24 Страница изучения ограничений порта

(8) Страница конфигурации транкинга портов

На рисунке 25 показана страница конфигурации транкинга портов, которая позволяет настроить агрегацию портов. Страница состоит из четырех частей: выбор идентификатора группы транкинга, установка метода агрегации, настраиваемый порт и порт участника группы.

Чтобы создать или изменить агрегацию портов, пользователю необходимо выбрать идентификатор группы магистралей ID от 1 до 8 в окне списка. Информация о группе магистралей отображается в порту участника группы. Чтобы создать группу магистралей, выберите соответствующий из идентификатора группы магистралей, нажмите кнопку "Создать группу магистралей", в случае успеха на панели отображения идентификатора будет создана аннотация в виде скобки. Если группа магистралей не создана, скобка аннотации не появится в строке отображения идентификатора. Чтобы задать метод агрегации портов, выберите нужный в раскрывающемся списке и нажмите кнопку "Настроить метод агрегации". Чтобы добавить агрегированный порт, выберите нужный порт в настраиваемом порту и нажмите кнопку "Порт участника =>". Чтобы

удалить порт, выберите объединенный порт в порту участника группы и нажмите клавишу "Порт, не являющийся членом группы <=". Чтобы удалить всю группу магистралей, нажмите клавишу «Удалить группу магистралей».

В процессе настройки страницы метод агрегации настраивается так, чтобы он соответствовал выбранному идентификатору группы магистральных каналов. Существующая группа магистральных каналов может настроить метод агрегации. Вы можете добавлять или удалять порты-участники существующей магистрали.

Коммутатор обеспечивает шесть типов агрегации 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 агрегирования портов. Каждая группа агрегирования портов поддерживает до восьми портов. Каждая магистральная группа может настроить свой собственный метод агрегирования портов.

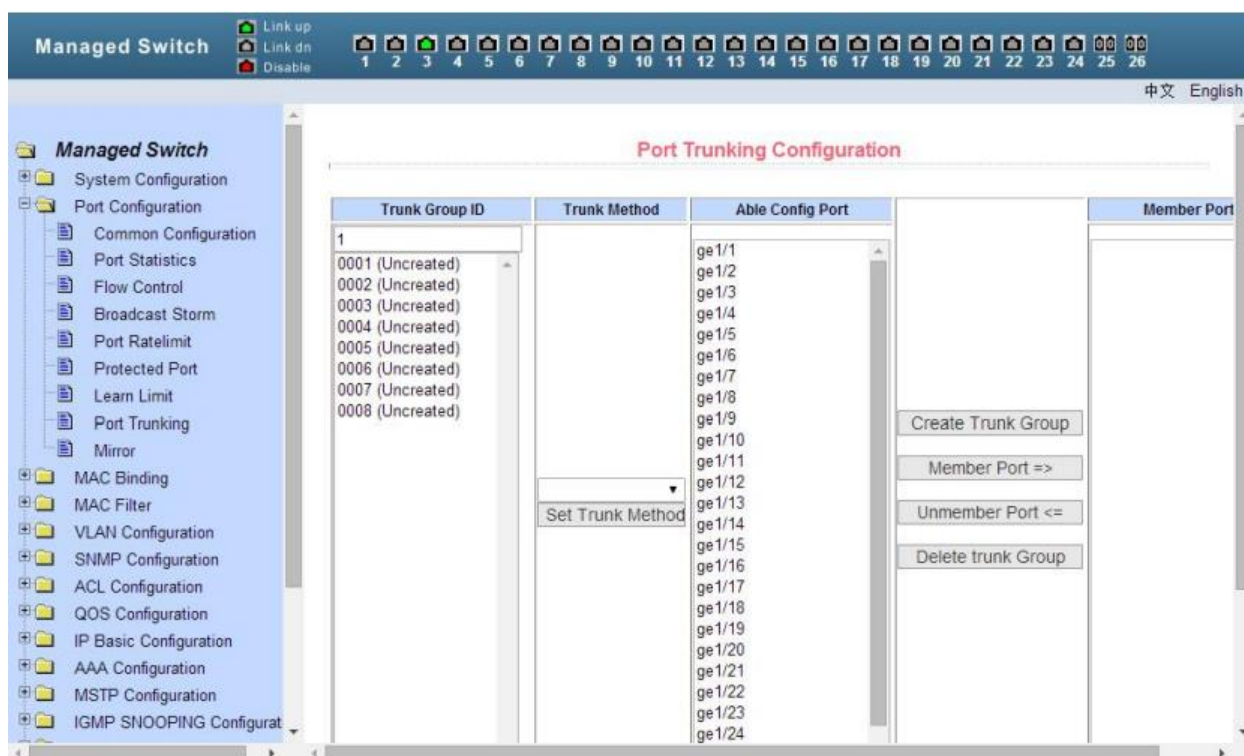


Рис. 25 Страница конфигурации транкинга портов

(9) Страница конфигурации зеркального отображения порта

На рисунке 26 показана страница конфигурации зеркального отображения портов, которая настраивает зеркальное отображение портов. Зеркальное отображение портов осуществляется через зеркальный порт для мониторинга выходных данных зеркального порта вывода и входных пакетов зеркального порта ввода. Зеркальный порт можно выбрать только один, а порты зеркального вывода и ввода несколько. Страница состоит из четырех частей: порт прослушивания, настраиваемый порт, направление прослушивания и конфигурация зеркального отображения информации. В разделе

«порт прослушивания» можно выбрать только один порт. Выберите зеркальный порт из настраиваемого порта, выберите направление прослушивания и нажмите клавишу «Применить». Результатом будет отображение информации о конфигурации зеркального порта.

Когда выбран RECEIVE в направлении прослушивания, это указывает на то, что пакет получен, TRANSMIT указывает на пакет, который должен быть отправлен, BOTH указывают на все пакеты, которые отправляются и принимаются, NOT_RECEIVE указывает на то, что полученный пакет отменен, NOT_TRANSMIT указывает на то, что пакет отменен, NEITHER отменяет получение и отправку пакета, то есть отменяет прослушивающий порт.

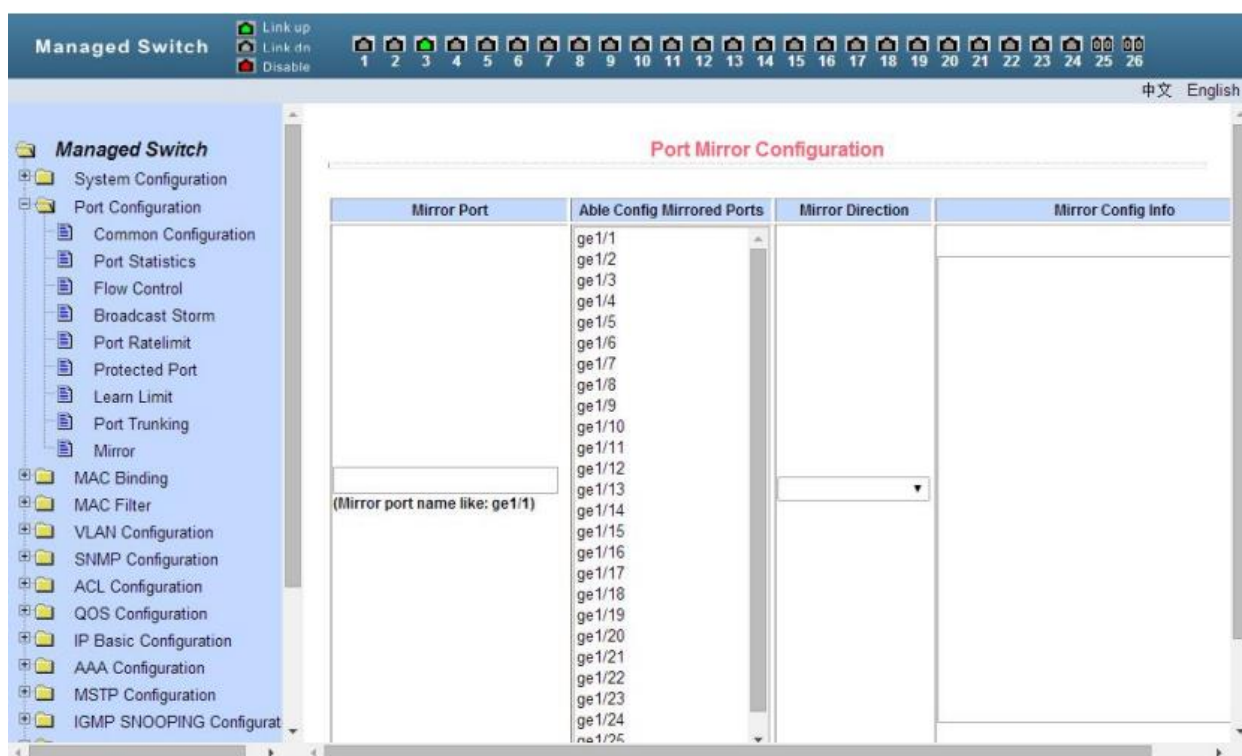


Рис. 26 Страница конфигурации зеркального отображения порта

5. Привязка к MAC

(1) Страница конфигурации привязки MAC

На рисунке 27 показана страница конфигурации привязки MAC. Эта страница используется для привязки порта к MAC-адресу.

MAC-адрес на странице используется для ввода привязанного MAC-адреса. Запись идентификатора VLAN используется для ввода VLAN, к которой принадлежит MAC-адрес.

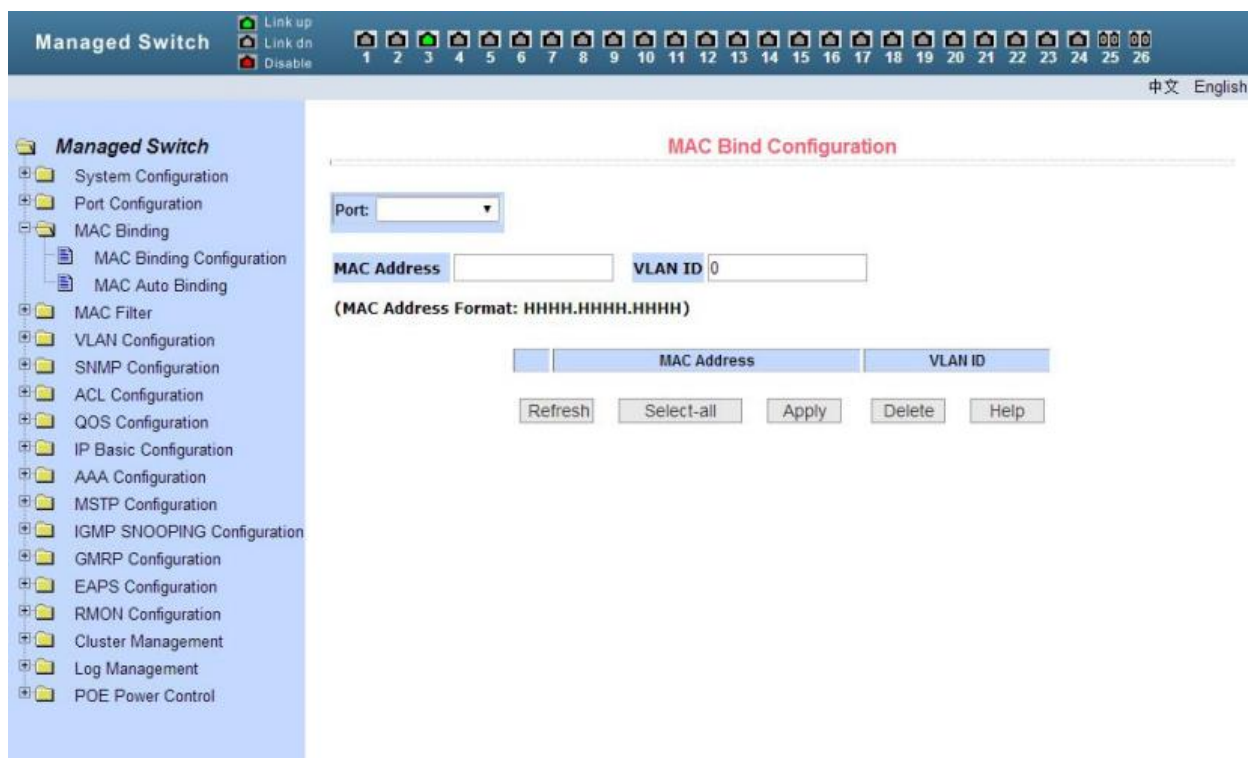


Рис. 27 Страница конфигурации привязки MAC

(2) Страница автоматической привязки MAC

На рисунке 28 показана страница автоматического преобразования привязки MAC, которая используется для реализации автоматической привязки MAC-адреса порта.

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

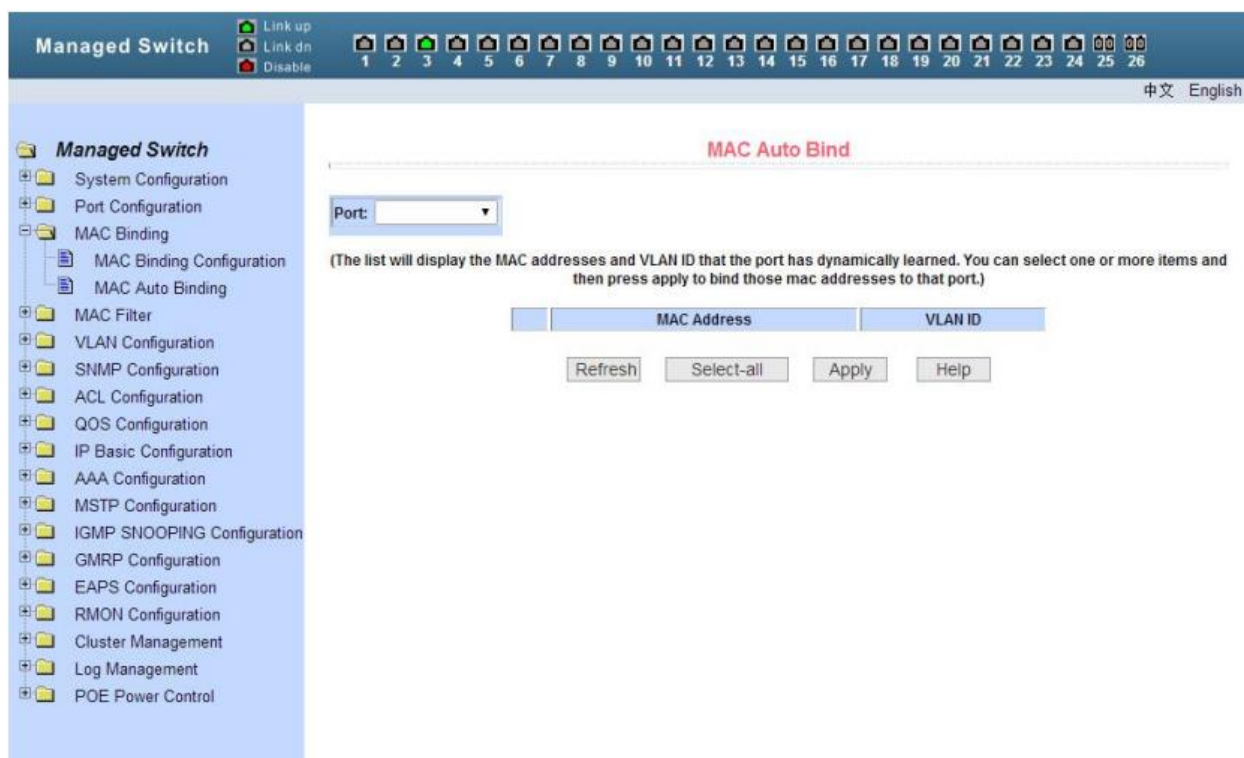


Рис. 28 Страница автоматической привязки MAC

6. MAC-фильтр

(1) Страница конфигурации MAC-фильтра

На рисунке 29 показана страница настройки MAC-фильтра, которая используется для настройки порта для фильтрации MAC-адреса.

MAC-адрес на странице используется для ввода отфильтрованного MAC-адреса. Запись идентификатора VLAN используется для ввода VLAN, к которой принадлежит MAC-адрес.

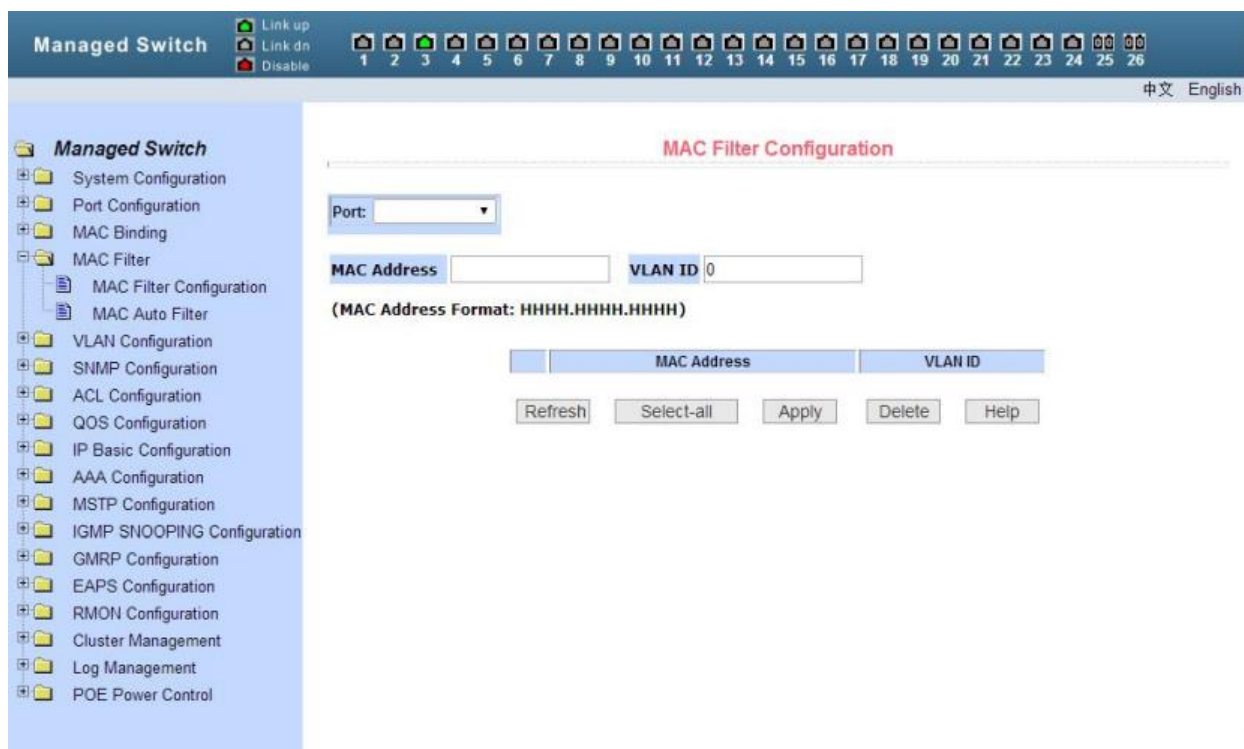


Рис. 29 Страница настройки MAC-фильтра

(2) Страница автоматического фильтра MAC

На рисунке 30 показан MAC-фильтр, автоматически преобразующий страницу, которая используется для реализации автоматической привязки MAC-адреса к порту.

Отобразите динамический MAC-адрес и VLAN, связанные с портом, на уровне 2 таблицы аппаратной переадресации. Вы можете выбрать запись и преобразовать ее в конфигурацию статического фильтра.

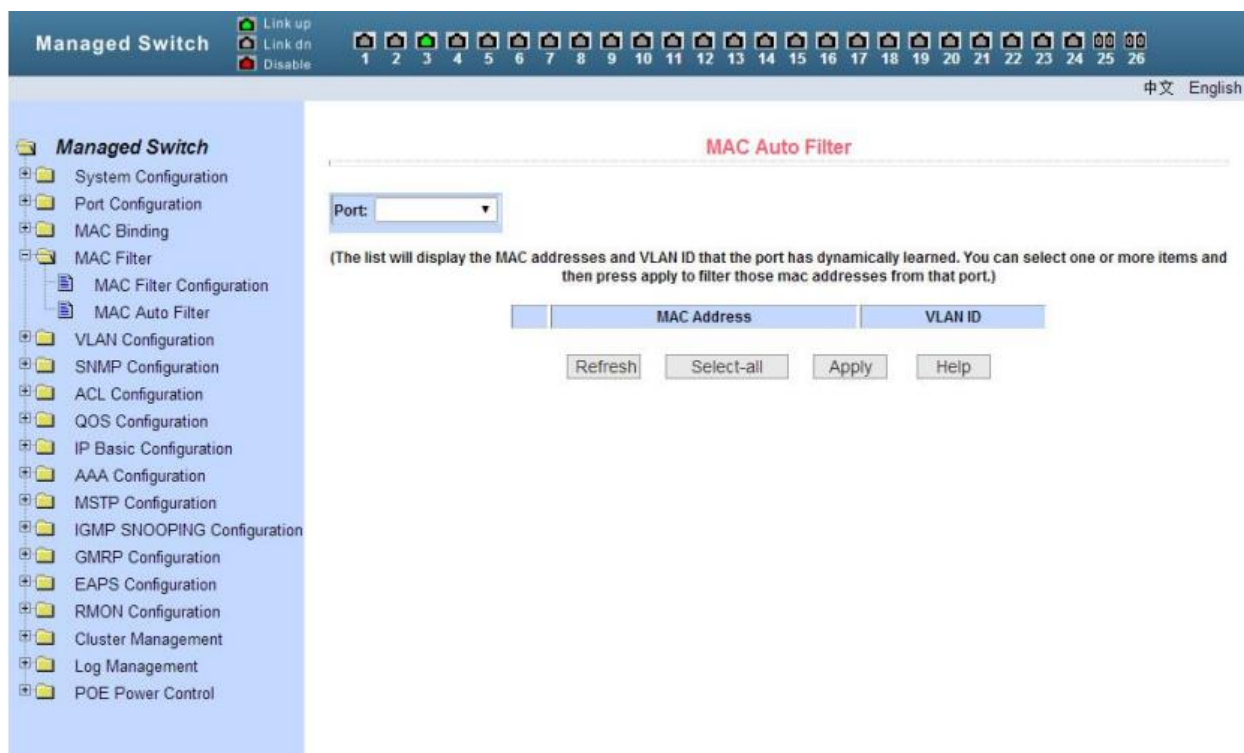


Рис. 30 Страница автоматического фильтра MAC

7. Конфигурация VLAN

(1) Информационная страница VLAN

На рисунке 31 показана страница с текущей информацией о VLAN. Страница доступна только для чтения и отображает текущие статус и члены порта VLAN. В раскрывающемся списке будут показаны все текущие VLAN, в списке отображается до 30 VID VLAN, состояние и порты участников. Выберите VLAN из выпадающего списка, и в списке отобразится информация с VID, превышающим 30 VLAN для этой VLAN. Но если всех VLAN не более 30, независимо от выпадающего списка для выбора VLAN, в списке будет отображена вся информация о VLAN.

Порт не может быть членом VLAN, ни помеченным, ни не помеченным членом VLAN. Символы в начале страницы следующие:

t - помеченный порт - является помеченным членом этой VLAN

u - не помеченный порт - является не помеченным членом этой VLAN

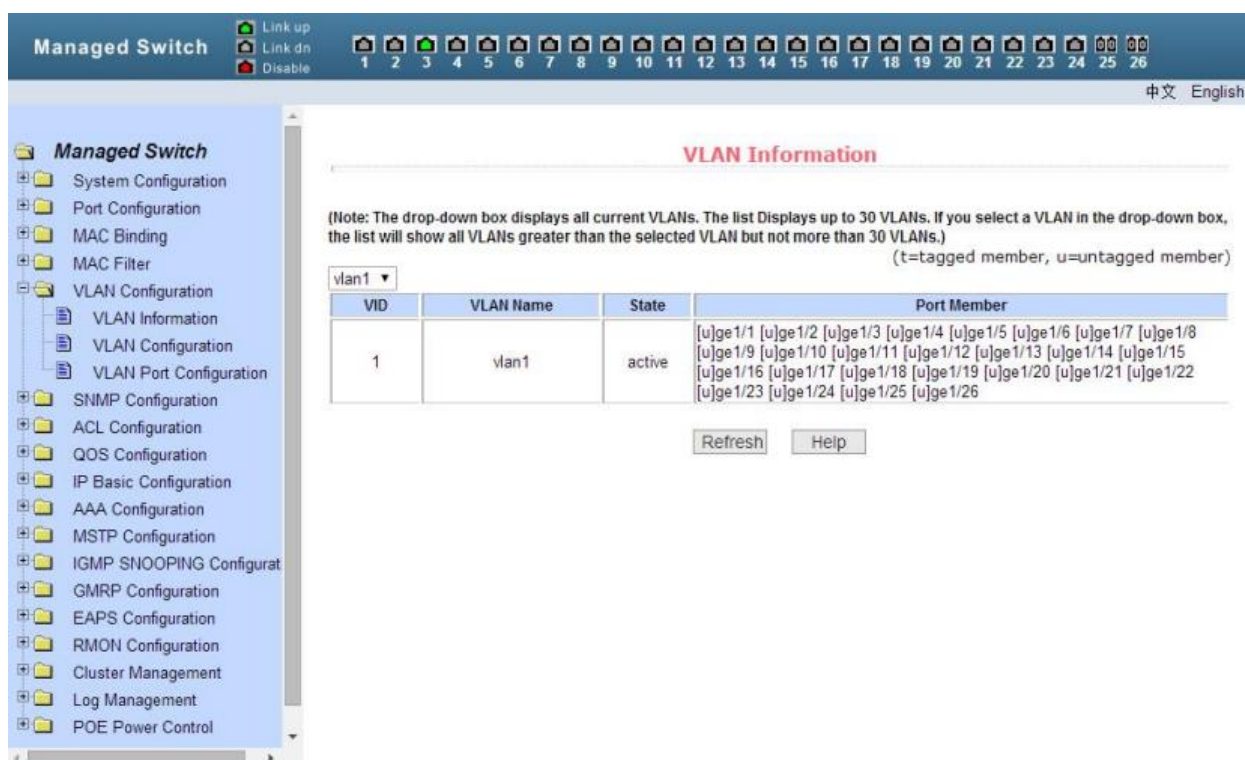


Рис. 31 Информационная страница VLAN

(2) Страница настройки статической VLAN

На рисунке 32 показана страница конфигурации статической VLAN, которая позволяет пользователям создавать VLAN.

Если вы хотите создать новую VLAN, введите в активную строку VID в диапазоне от 2 до 4094. Имя VLAN генерируется системой в соответствии с идентификатором VLAN и не может быть изменено. Нажмите кнопку «Применить», и в окне списка отобразятся VID и имя VLAN, созданные пользователем. Коммутатор создает VLAN 1 по умолчанию, и VLAN 1 нельзя удалить.

Если вы хотите удалить VLAN, пользователю необходимо выбрать соответствующую VLAN в окне списка. VLAN отобразится в активной строке, нажмите кнопку «Удалить», чтобы удалить VLAN, и информация о VLAN будет удалена из окна списка.

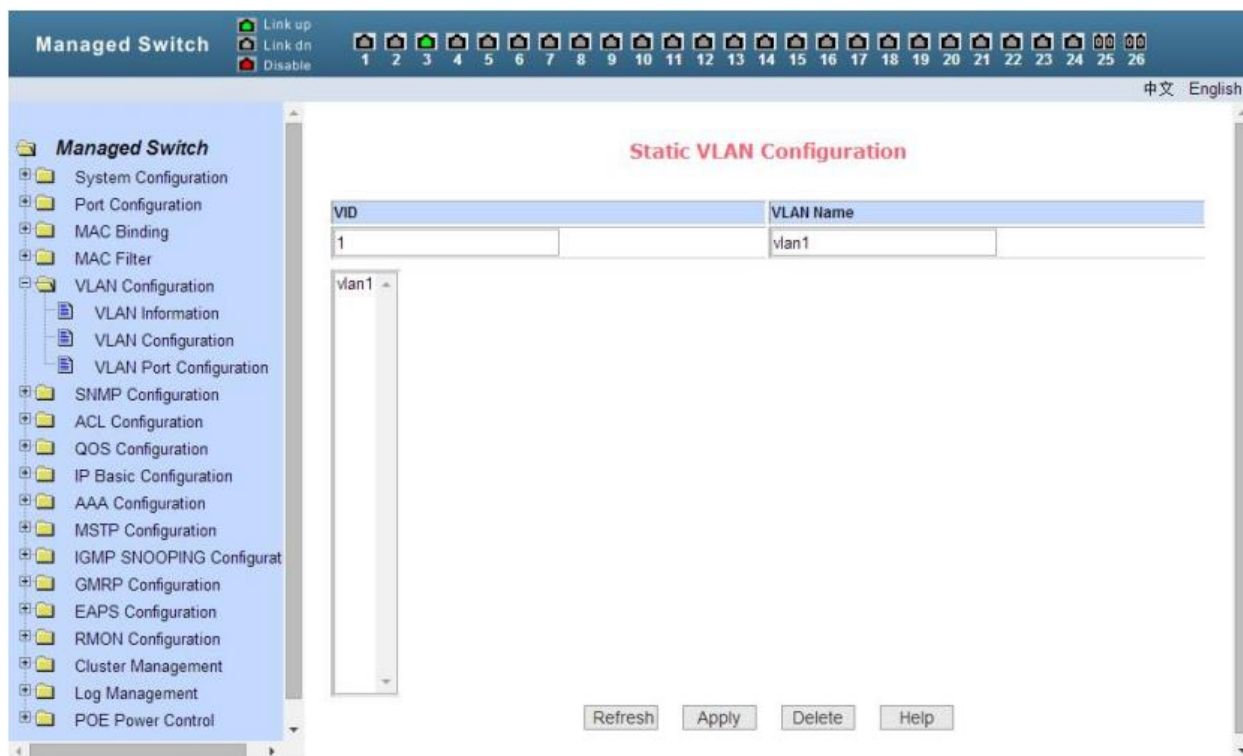


Рис. 32 Страница конфигурации статической VLAN

(3) Страница конфигурации порта VLAN

На рисунке 33 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, "default VLAN =>", "tagged =", "untagged =>" и "non-member <=".

Порт - это порт, который указывает VLAN, подлежащую настройке.

Режим «Порт» определяет режим VLAN порта в качестве режима доступа. В этом режиме VLAN порт по умолчанию использует не помеченные тегами элементы VLAN1. VLAN порта по умолчанию равна 1. Режим VLAN гибридного порта - ГИБРИДНЫЙ режим. В этом режиме VLAN порт является не помеченным членом VLAN1, а VLAN порта по умолчанию равна 1. Режим VLAN магистрального порта - это режим магистральной сети, в котором VLAN портом по умолчанию является помеченный элемент VLAN1, а значение по умолчанию VLAN порта равно 1.

Все текущие VLAN - это VLAN, которые могут быть созданы портом. Пользователи могут выбрать 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 помеченным членом VLAN. [U] указывает, что порт является членом VLAN без тегов. При удалении VLAN пользователь выбирает VLAN из списка.

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

Нажмите "tagged =>", чтобы настроить порт как помеченный элемент указанной VLAN, и выберите одну или несколько VLAN из всех текущих.

Нажмите "untagged =>", чтобы настроить порт как не помеченный член указанной VLAN, и выберите одну или несколько VLAN из всех текущих.

Ключ "Non-member <=" удаляет порт из указанной одной или нескольких VLAN, он больше не является членом этих VLAN и выбирает одну или несколько VLAN из тех, к которым принадлежит порт.

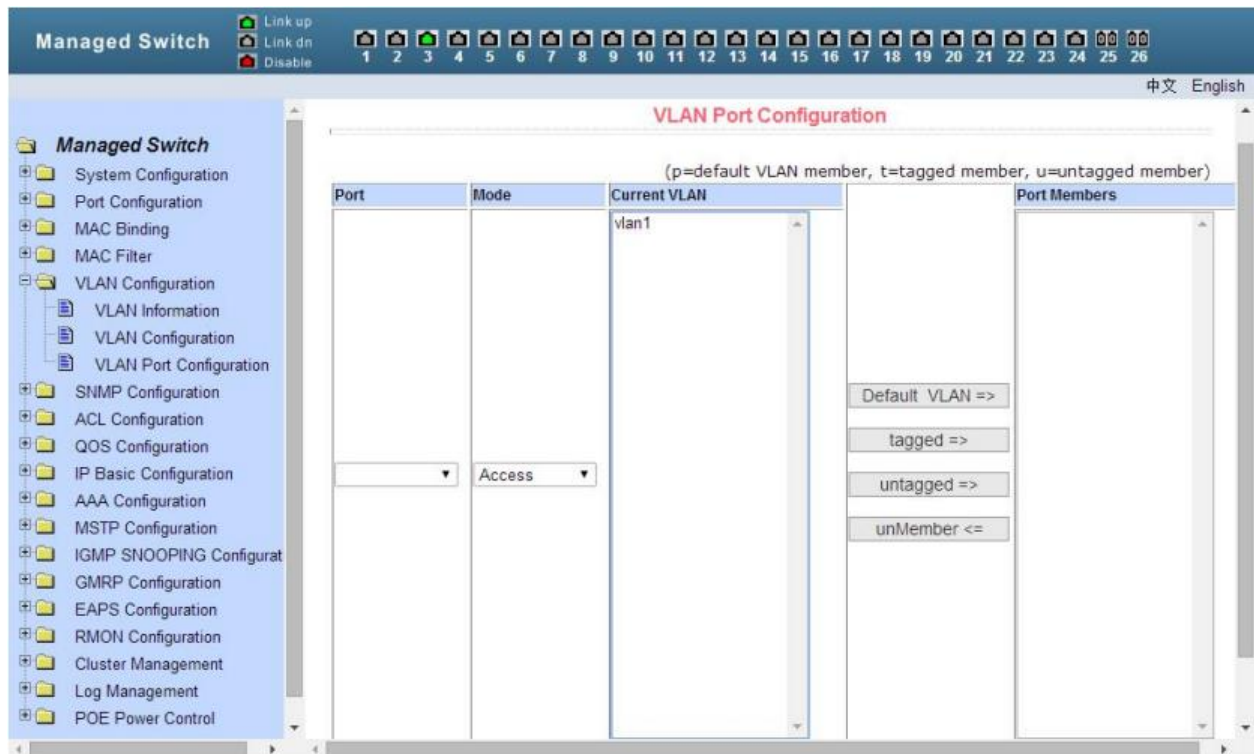


Рис. 33 Страница конфигурации порта VLAN

8. Конфигурация SNMP

(1) Страница конфигурации сообщества SNMP

На рисунке 34 показана страница конфигурации сообщества SNMP, которая позволяет пользователю настроить имя коммутатора и разрешения на чтение и запись, и в общей сложности можно настроить восемь записей.

По умолчанию переключатель имеет общедоступное имя общего тела, общим телом являются 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 сообщество, доступное для чтения и записи.



Рис. 34 Страница конфигурации сообщества SNMP

(2) Страница конфигурации целевой ловушки

На рисунке 35 показана страница конфигурации цели TRAP, которая позволяет настроить IP-адрес рабочей станции, получившей сообщение TRAP, и некоторые параметры пакета протокола TRAP.

При настройке записи имя используется для ввода имени TRAP. IP-адрес используется для ввода адреса назначения. Версия SNMP используется для выбора версии пакета TRAP. Если настройка выполнена успешно, статус записи будет отображаться как активный. Если конфигурация выполнена успешно, функция SNMP TRAP вступит в силу. В случае подключения вверх или вниз коммутатор автоматически отправит пакет TRAP на адрес назначения.

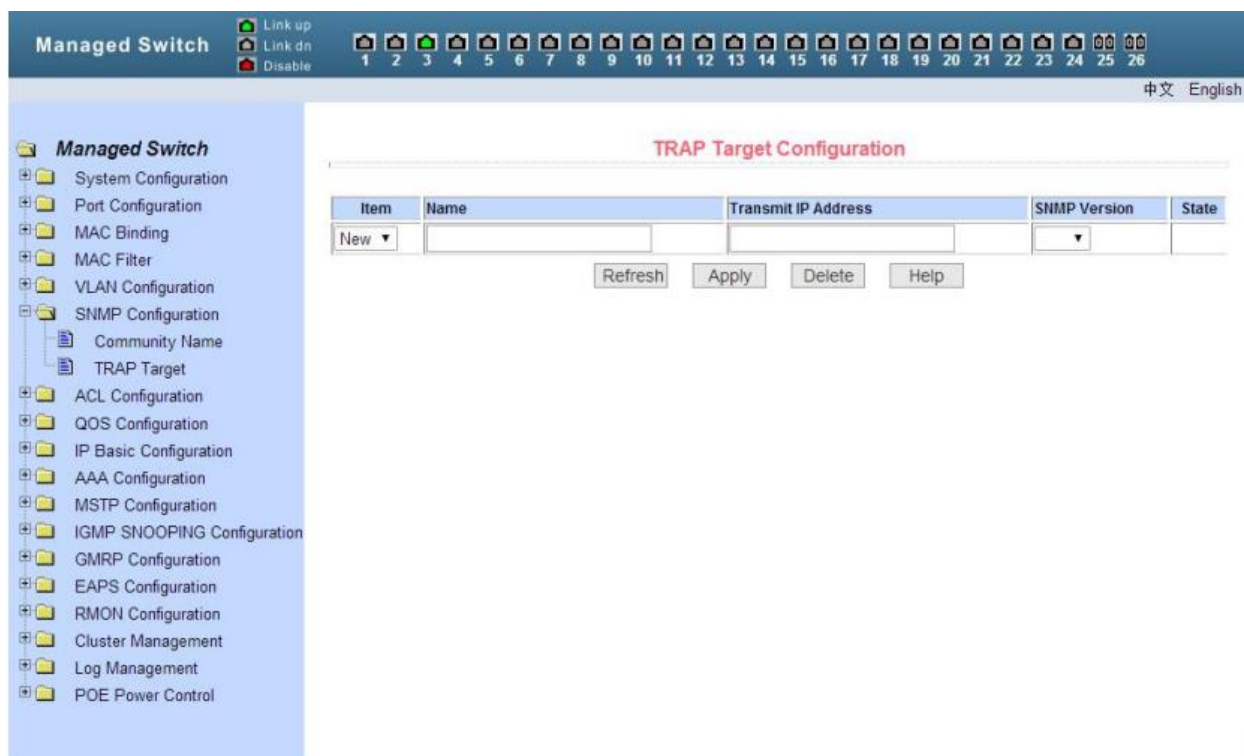


Рис. 35 Страница конфигурации целевой ловушки

9. Конфигурация ACL

(1) Страница стандартной конфигурации IP-адреса ACL

На рисунке 36 показана страница конфигурации ACL standard IP. Вы можете использовать эту страницу для создания базы правил для ACL standard IP. Пользователь может выбрать номер группы ACL (диапазон от 1 до 99 или 1300-1999), чтобы создать одно или несколько правил в группе. Поля, которые могут быть сопоставлены в правиле, содержат только исходные IP-адреса (с маской).

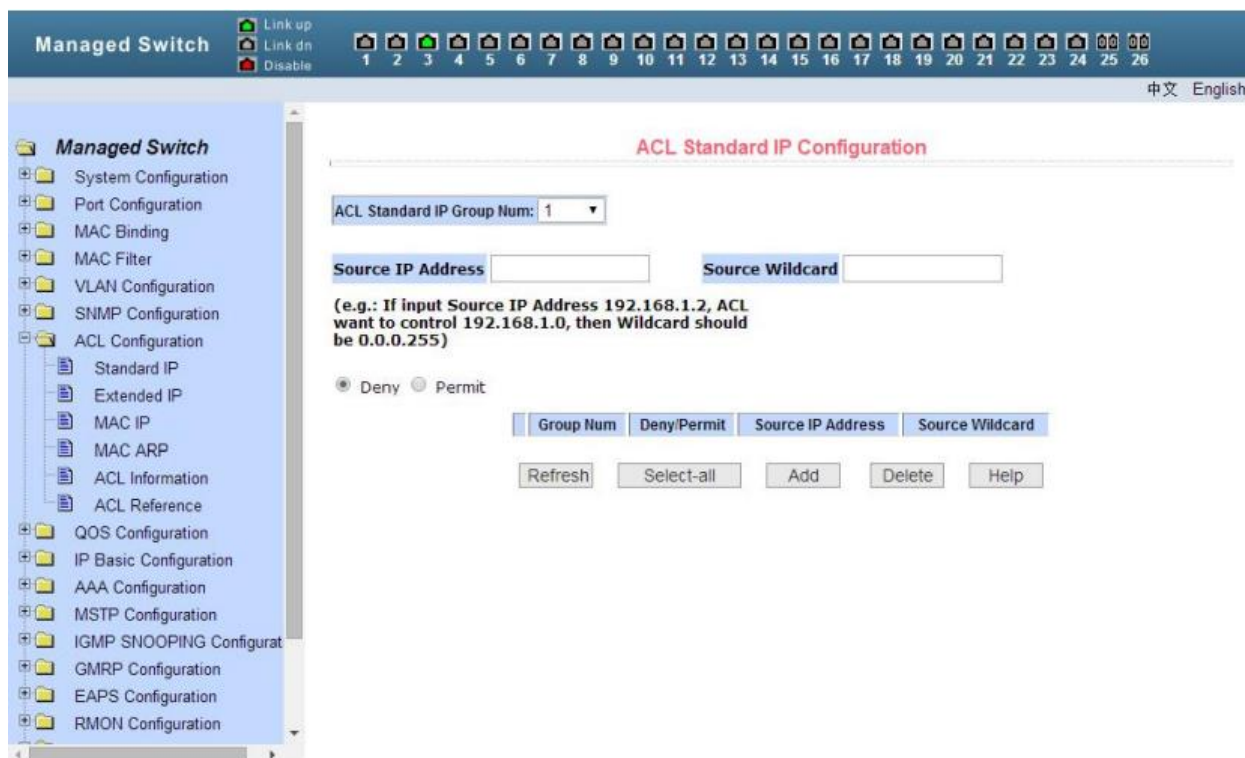


Рис. 36 Страница стандартной конфигурации IP-адреса ACL

Когда пользователь настраивает правило, исходный IP-адрес должен быть замаскирован. Правило может соответствовать набору IP-адресов. Маска адреса 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 равна 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 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, а затем нажать клавишу «Удалить».

(2) Страница конфигурации расширенного IP-адреса ACL

На рисунке 37 показана страница конфигурации IP-адреса расширения ACL. Вы можете использовать эту страницу для создания базы правил для IP-адреса расширения ACL. Пользователь может выбрать номер группы ACL (в диапазоне 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 (замаскированный), IP-адрес назначения (замаскированный), тип протокола (например, ICMP, TCP, UDP и т.д.) (Допустимый протокол), флаг управления TCP.

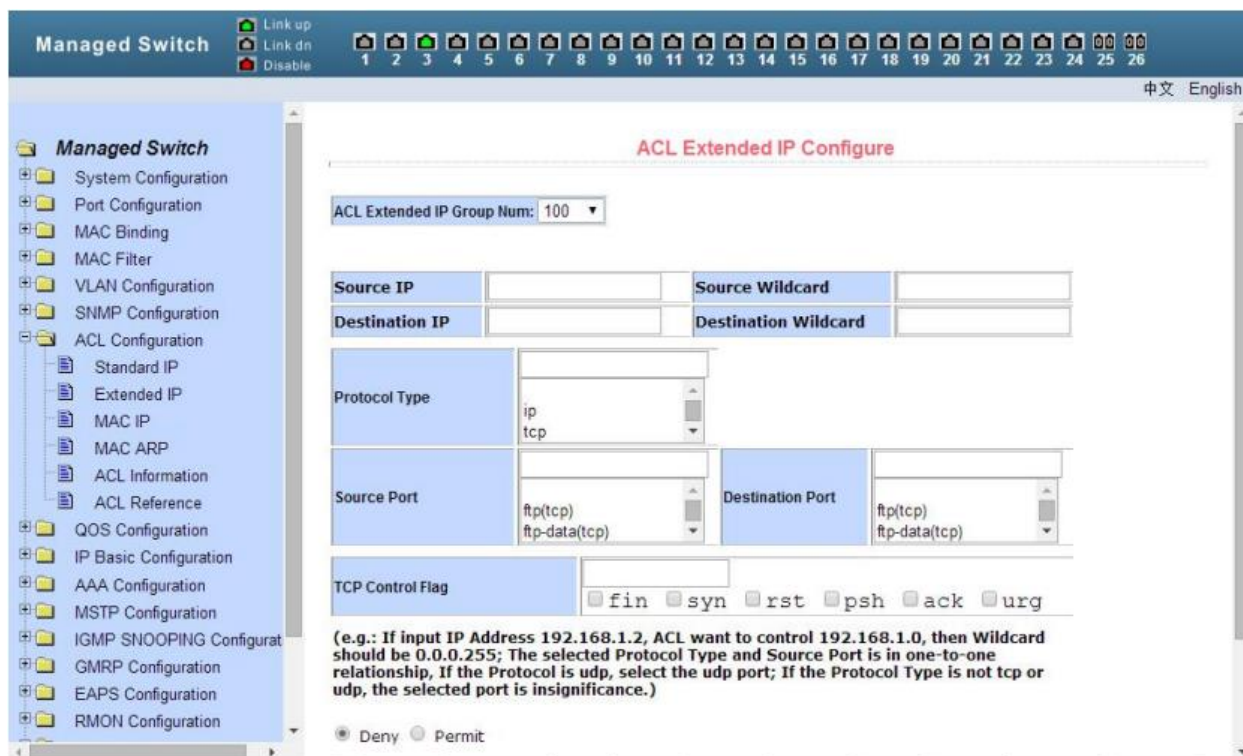


Рис. 37 Страница конфигурации расширенного IP-адреса ACL

Когда пользователь настраивает правило, IP-адрес источника и IP-адрес назначения должны быть замаскированы. Правило может соответствовать набору IP-адресов. Маска адреса 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 его номер. Когда правило в группе 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, а затем нажать клавишу «Удалить».

(3) Страница конфигурации ACL MAC IP

На рисунке 38 показана страница настройки MAC-IP ACL. Вы можете использовать эту страницу для создания базы правил для MAC-адресов ACL. Пользователь может выбрать номер группы ACL (в диапазоне 700-799), чтобы создать одно или несколько правил в группе. Поля, которые могут соответствовать активному MAC-адресу (с битами совпадения адресов), IP-адресу источника (с битом совпадения адресов), IP-адресу назначения (с битом совпадения адресов) и идентификатору VLAN.

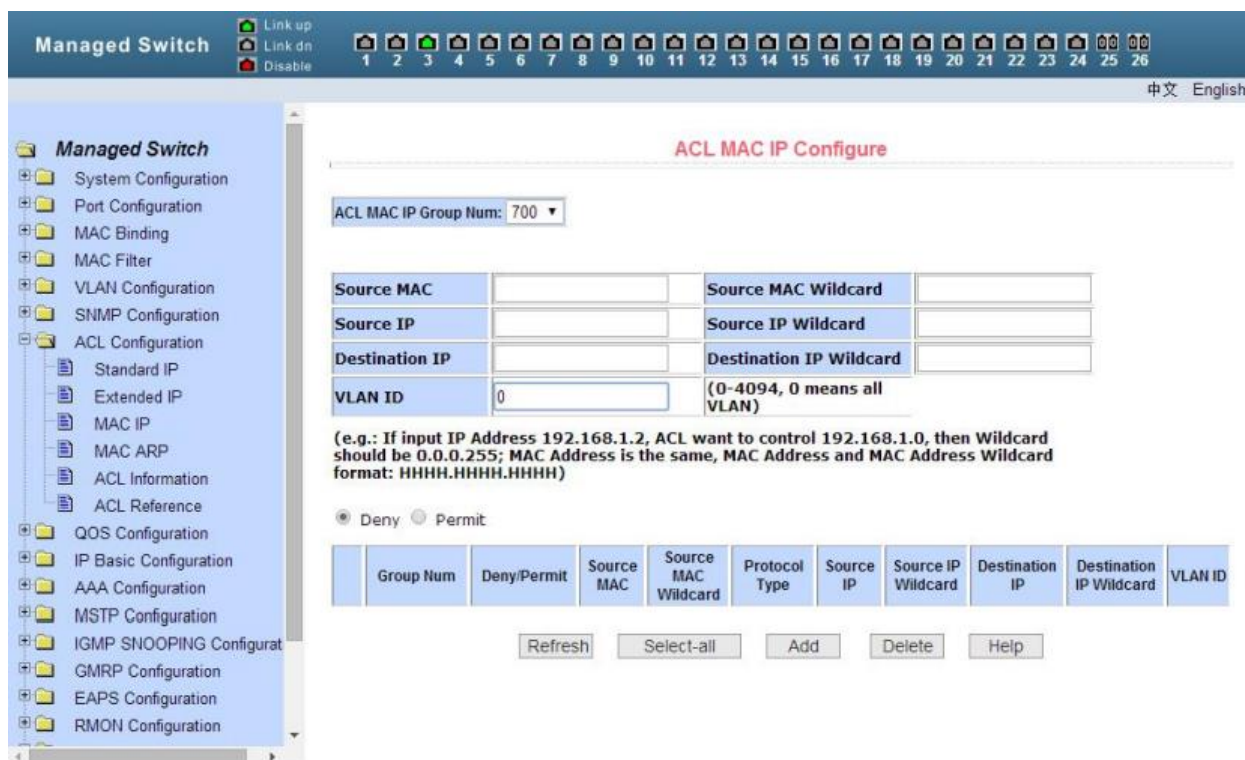


Рис. 38 Страница конфигурации ACL MAC IP

Когда пользователь настраивает правило, MAC-адрес источника, IP-адрес источника и IP-адрес назначения должны совпадать с адресом. Правило может совпадать с MAC-адресом и IP-адресом. 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 из них должно иметь режим фильтрации: разрешить или запретить.

Когда пользователь создает правило в группе правил, система автоматически присваивает правилу его номер. Когда правило в группе 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, а затем нажать клавишу «Удалить».

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

(4) Страница конфигурации ACL MAC ARP

На рисунке 39 показана страница конфигурации ACL MAC ARP. Вы можете использовать её 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 соответствия адреса), отправляют IP-адрес (с битом соответствия адреса).

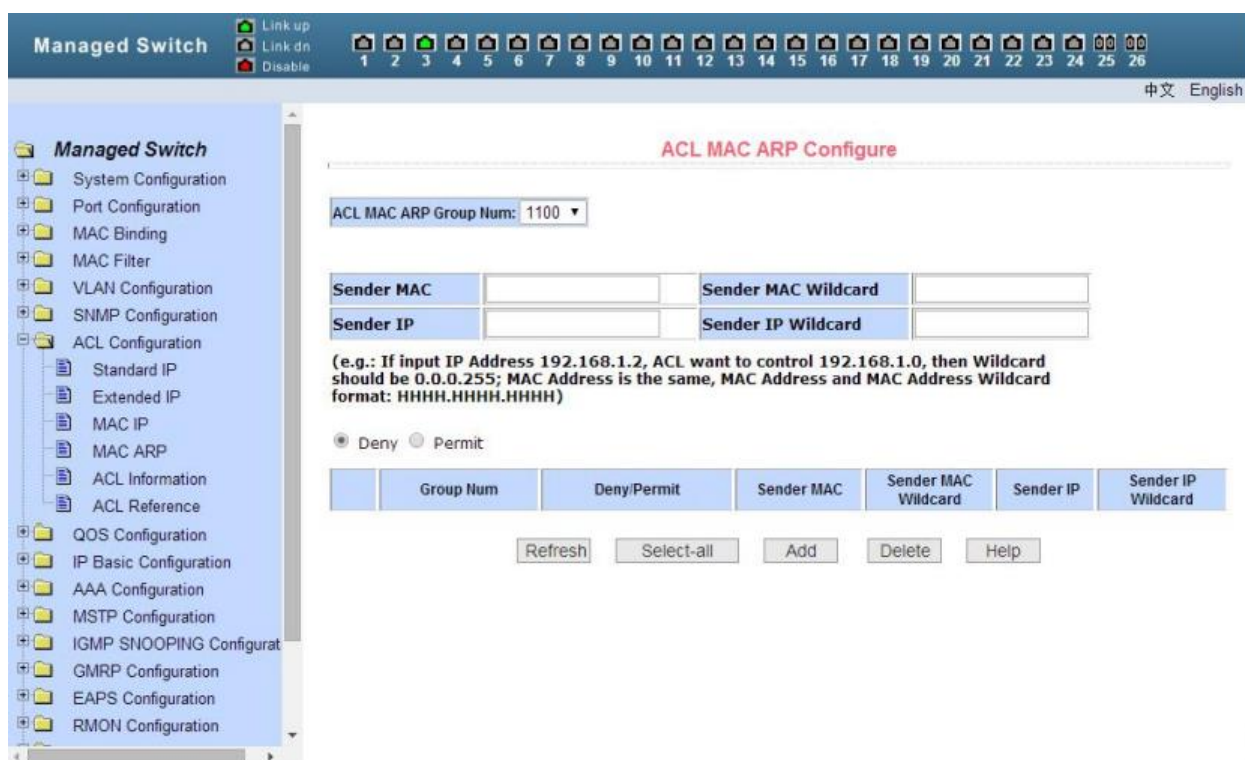


Рис. 39 Страница конфигурации ACL MAC ARP

Когда пользователь настраивает правило, MAC-адрес и IP-адрес отправляются с битом соответствия адреса. 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 из них должно иметь режим фильтрации: разрешить или запретить.

Когда пользователь создает правило в группе правил, система автоматически присваивает правилу номер. Когда правило в группе 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, а затем нажать клавишу «Удалить».

(5) Страница с информацией о ресурсах ACL

На рисунке 40 показана страница информации о ресурсах ACL, на которой отображаются все правила и ссылки, настроенные в текущем ACL.

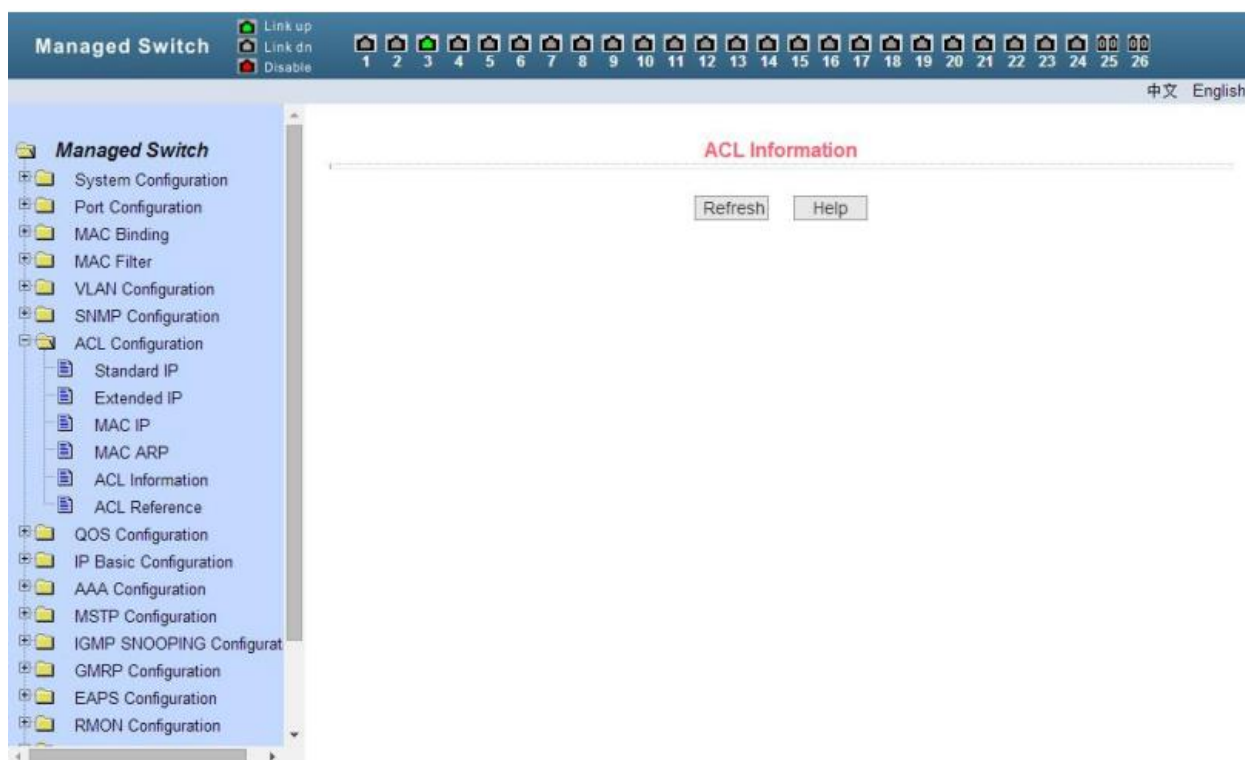


Рис. 40 Страница с информацией о ресурсах ACL

(6) Справочная страница конфигурации ACL

На рисунке 41 показана страница конфигурации ACL reference. 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 ACL для принимаемых пакетов в соответствии с этими правилами.

При выборе группы ACL для порта вы можете выбрать стандарт IP, расширение IP, MAC IP и MAC ARP ACL. Выбранная группа ACL должна существовать. Выберите список групп правил ACL и нажмите клавишу «Добавить». При удалении группы ACL выберите группу ACL из списка связанных групп правил и нажмите клавишу «Удалить».

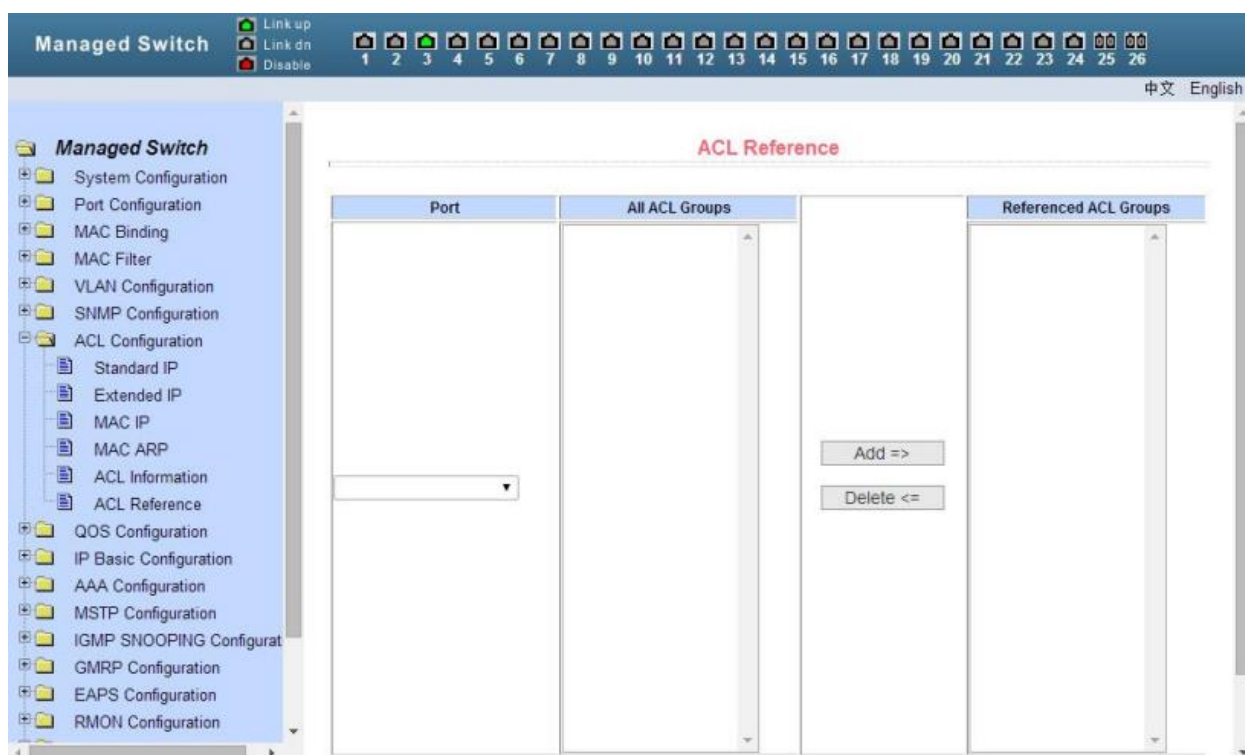


Рис. 41 Справочная страница конфигурации ACL

10. Конфигурация QoS

(1) Страница применения QoS

На рисунке 42 показана страница приложения QoS, пользователь может использовать эту страницу для настройки типа QoS порта, но также может изменить приоритет пользователя по умолчанию. Список отображает тип QoS порта в реальном времени и приоритет пользователя по умолчанию.

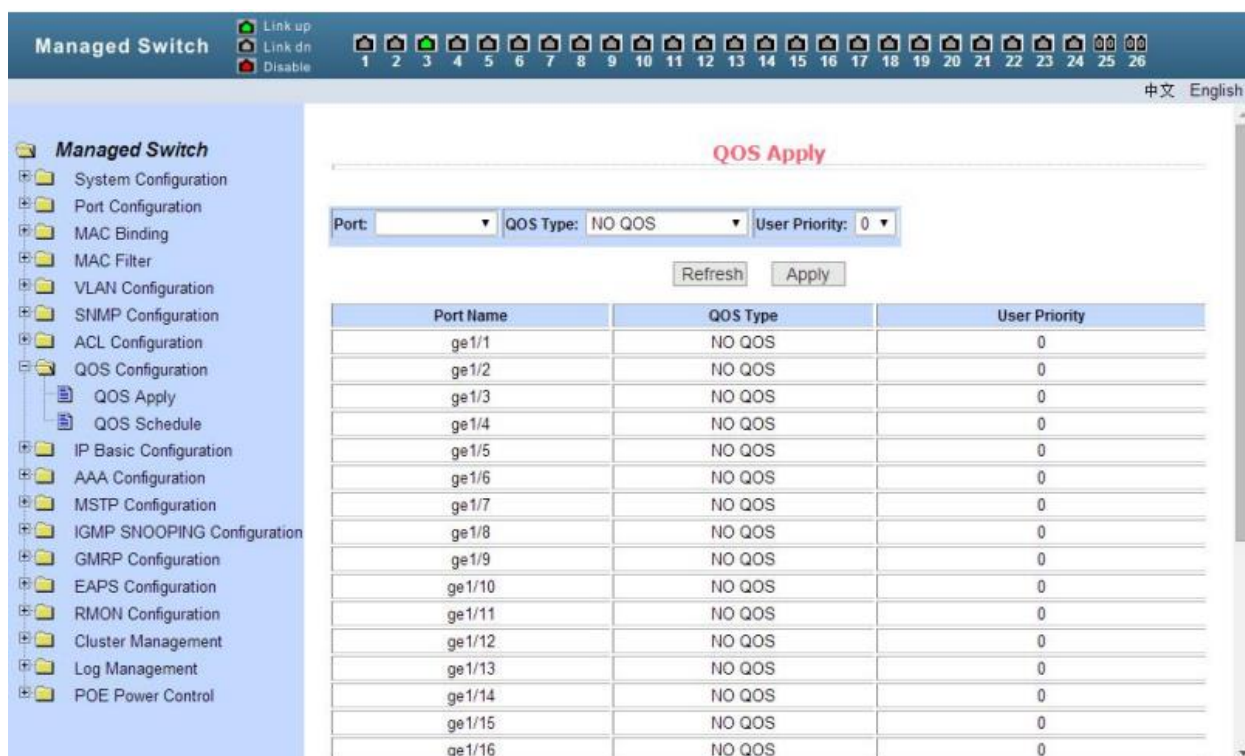


Рис. 42 Страница применения QoS

(2) Страница расписания QoS

На рисунке 43 показана страница планирования QoS, пользователь может использовать эту страницу для настройки типа планирования QoS порта, но также может изменять приоритет очереди. Список отображает режим планирования портов в реальном времени и значение веса каждой очереди.

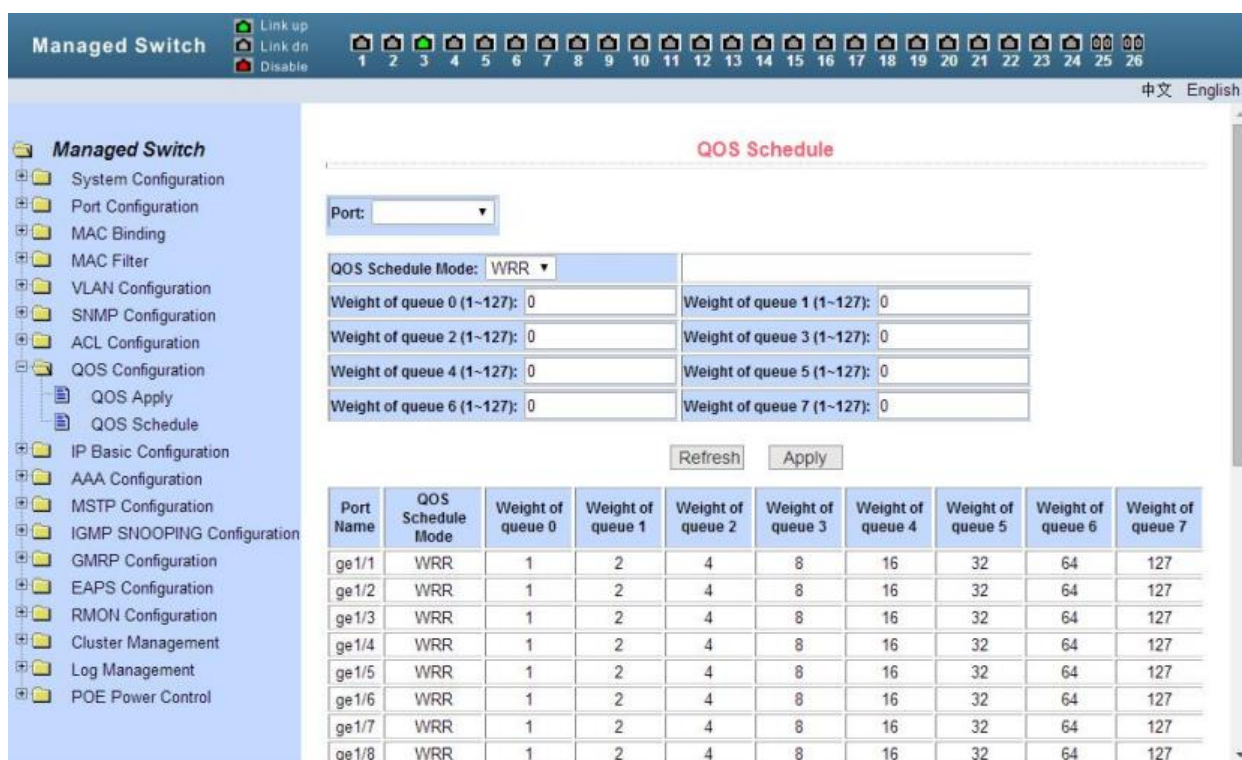


Рис. 43 Страница расписания Qos

11. Базовая конфигурация IP

(1) Страница конфигурации интерфейса VLAN

На рисунке 44 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. Только если VLAN уже существует, ее можно установить в качестве интерфейса. В сконфигурированном интерфейсе можно настроить только адрес интерфейса.

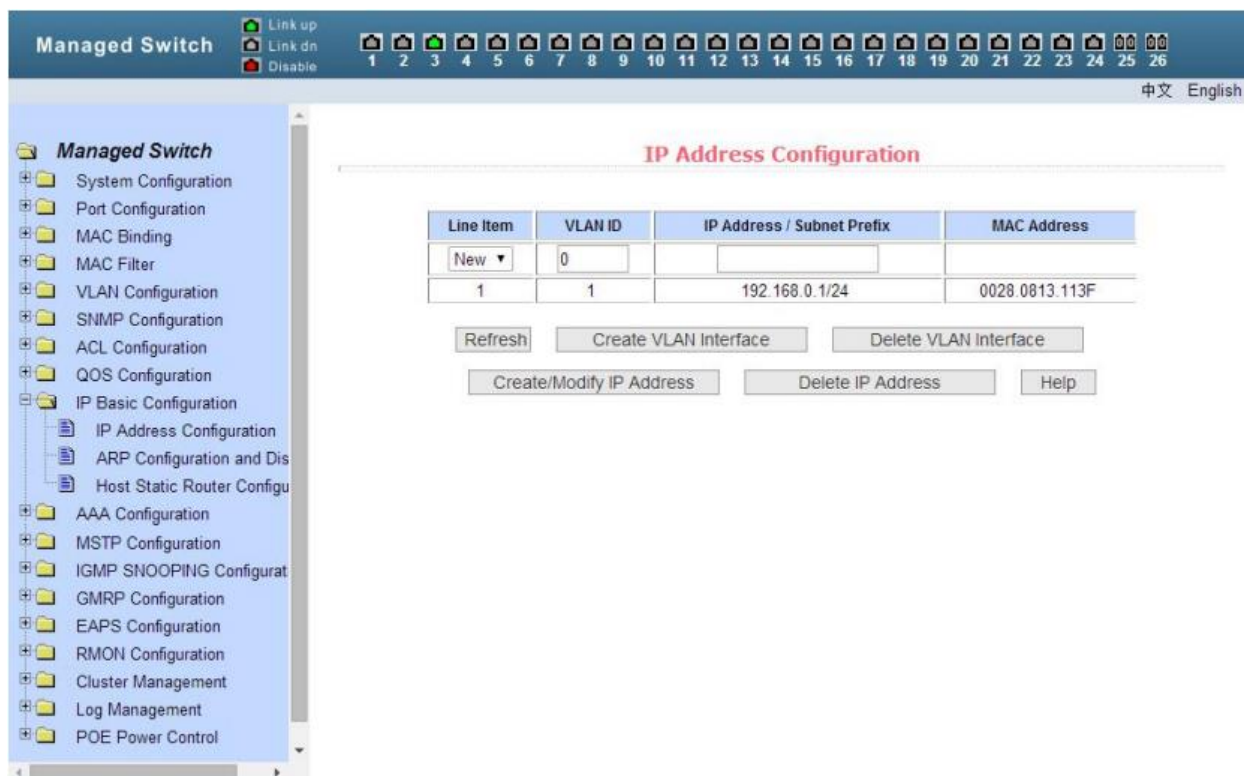


Рис. 44 Страница конфигурации интерфейса VLAN

Коммутатор по умолчанию имеет интерфейс VLAN1, и этот интерфейс нельзя удалить. Для одной VLAN можно настроить только один интерфейс.

(2) Страница настройки ARP и отображения

На рисунке 45 показана страница конфигурации и отображения ARP, на которой отображается вся информация 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.

При настройке статической записи ARP вам необходимо ввести IP-адрес и MAC-адрес. MAC-адрес должен быть одноадресным MAC-адресом, а затем нажмите клавишу «Добавить».

Когда пользователь удаляет запись ARP, вы можете 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 сегмент IP в поле ввода. Затем нажмите клавишу «Удалить».

Когда динамическая запись ARP изменяется на статическую запись ARP, вы можете выбрать изменение динамической записи ARP в сегменте сети на статическую. Для сегмента сети введите указанный сегмент сети в поле ввода, а затем нажмите кнопку «Применить».

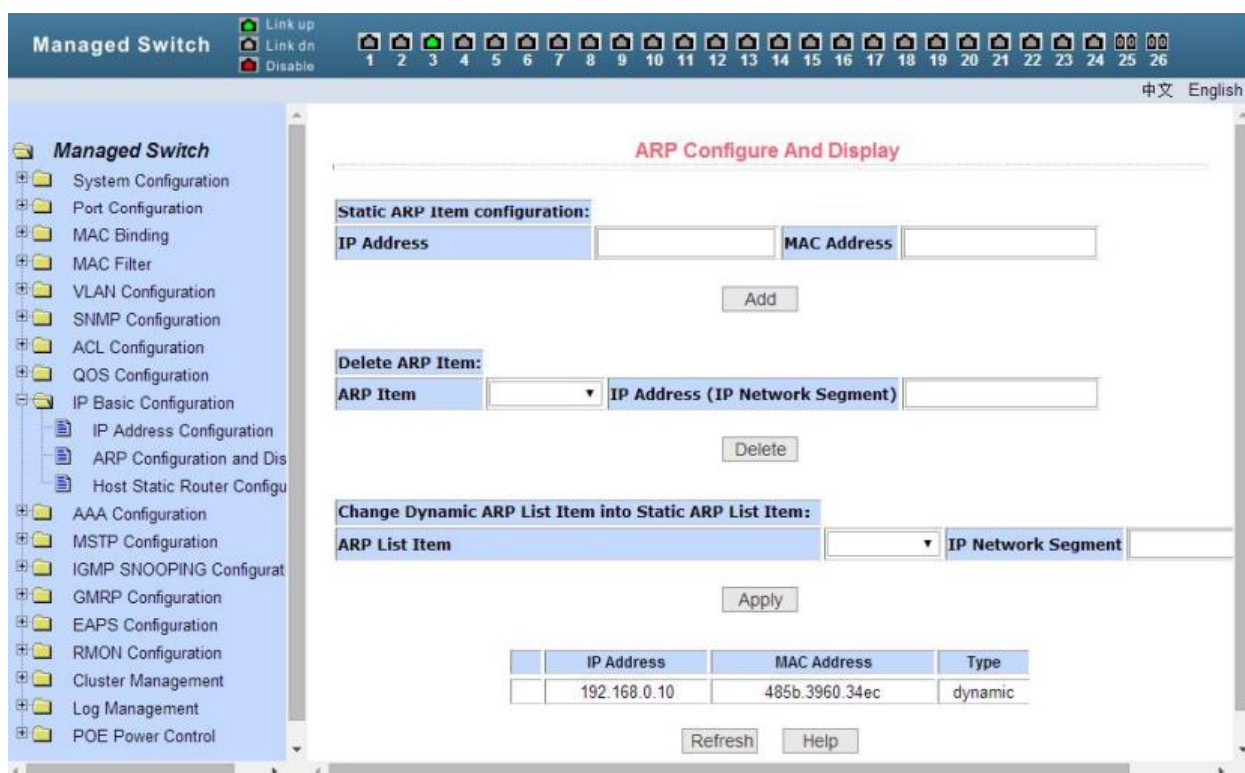


Рис. 45 Конфигурация ARP и страница отображения

(3) Страница конфигурации статического маршрута хоста

На рисунке 46 показана страница конфигурации статической маршрутизации узла, пользователь может добавлять и удалять статический маршрут узла коммутатора. По умолчанию статический маршрут на коммутаторе не настроен. Вы можете использовать эту страницу для настройки маршрута по умолчанию, то есть префикс назначения / подсети равен 0.0.0.0/0.

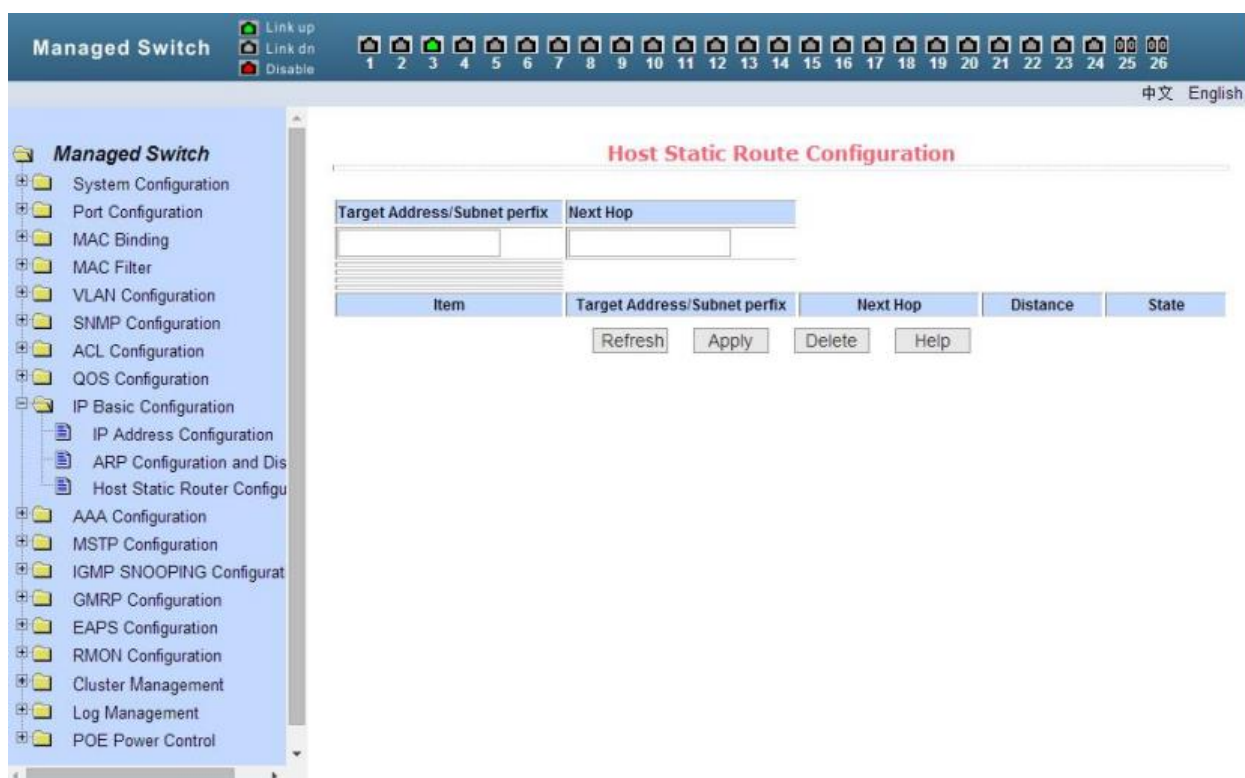


Рис. 46 страница конфигурации статического маршрута хоста

12. Конфигурация AAA

(1) Страница конфигурации Tacsacs+

На рисунке 47 показана страница конфигурации Tacsacs +. Пользователь может настроить информацию, относящуюся к Tacsacs +. Можно задать следующую информацию: Включить функцию Tacsacs +, настроить IP-адрес сервера Tacsacs +, тип аутентификации и общий секретный ключ.

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

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

Тип аутентификации, обеспечивающий типы аутентификации PAP и CHAP. По умолчанию используется аутентификация PAP.

Общий ключ, используемый для настройки коммутатора и сервера Tacsacs + между зашифрованным общим паролем, в поле авторизации/аутентификации необходимо установить значение, совпадающее с настройками сервера Tacsacs +.

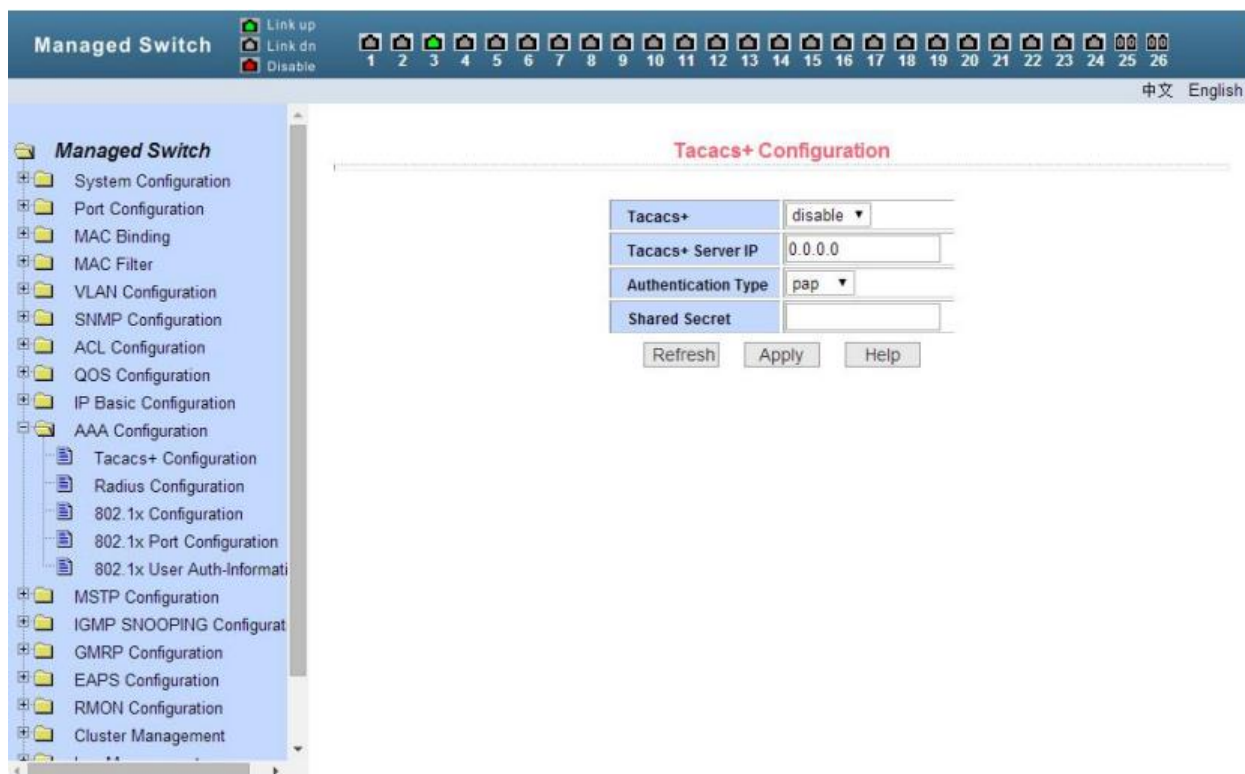


Рис. 47 Страница конфигурации Tacacs+.

(2) Страница конфигурации Radius

На рисунке 48 показана страница конфигурации Radius, пользователь может настроить информацию, относящуюся к Radius, может установить, что информация включает:

- IP-адрес сервера Radius, в поле аутентификации и выставления счетов необходимо указать IP-адрес.
- Необязательный IP-адрес сервера Radius, который можно задать, если есть альтернативный сервер Radius.
- Порт аутентификации UDP, значение по умолчанию - 1812, пользователю обычно не нужно изменять это поле.
- Запускать ли выставление счетов, по умолчанию используется значение "Начать" при выполнении аутентификации и выставлении счетов.
- Порт UDP для выставления счетов, значение по умолчанию - 1813.
- Общий ключ, используемый для настройки коммутатора и шифрования сервера Radius между общим паролем, в поле аутентификации и выставления счетов должно быть указано это поле, а также те же настройки на сервере Radius.
- Информация о поставщике, пользователям обычно не нужно изменять это поле.
- Порт NAS, тип порта NAS, тип службы NAS, эти три значения пользователям, как правило, изменять не нужно.
- Следует ли запускать или выключать функцию перемещения в Radius.

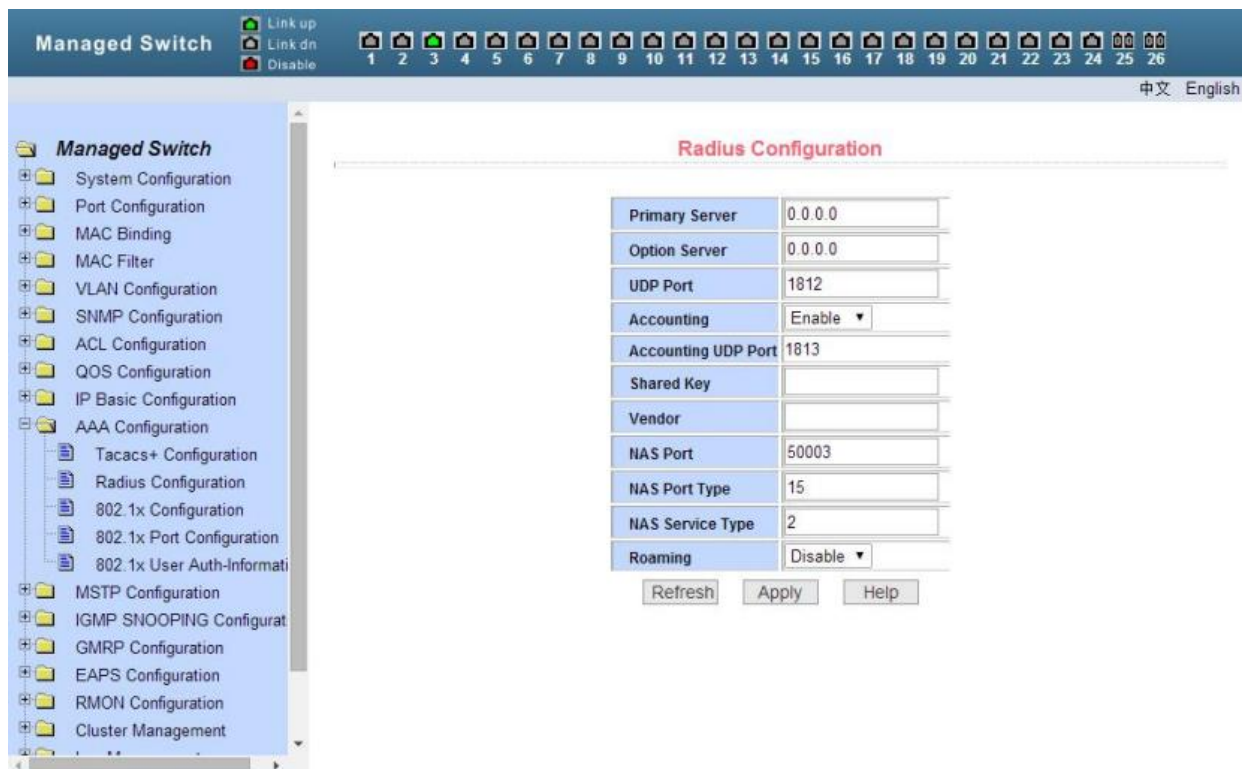


Рис. 48 Страница конфигурации Radius

(3) Страница конфигурации 802.1x

На рисунке 49 показана страница конфигурации 802.1x. На этой странице вы можете настроить информацию, связанную с 802.1x, включая:

- Независимо от того, следует ли запускать протокол 802.1x, обязательно запускайте протокол 802.1x при выполнении аутентификации и учета.
- Является ли переключатель обычным методом аутентификации или методом расширенной аутентификации.
- Следует ли открывать функцию повторной аутентификации, по умолчанию она не открыта, при выполнении аутентификации и выставлении счета необходимо принимать решение в соответствии с реальной ситуацией. Включение функции повторной аутентификации сделает пользователя более надежным при использовании аутентификации и выставлении счетов, но немного увеличит трафик в сети.
- Установите интервал повторной аутентификации, только в случае, если функция повторной аутентификации включена, значение по умолчанию равно 3600 секундам, при выполнении аутентификации и выставлении счета в соответствии с фактической ситуацией установите значение, но значение не должно быть слишком маленьким.
- Таймер периода ожидания, пользователю обычно не нужно изменять это поле.
- Таймер тайм-аута сервера, пользователям обычно не нужно изменять это поле.

- Таймер ожидания запроса, пользователю, как правило, не нужно изменять это поле.
- Количество запросов, пользователям, как правило, не нужно изменять это поле.
- Показывать максимальный размер Reauth.
- Версия клиента, номер версии клиента.
- Проверить пакет временного трафика клиента после прохождения аутентификации.

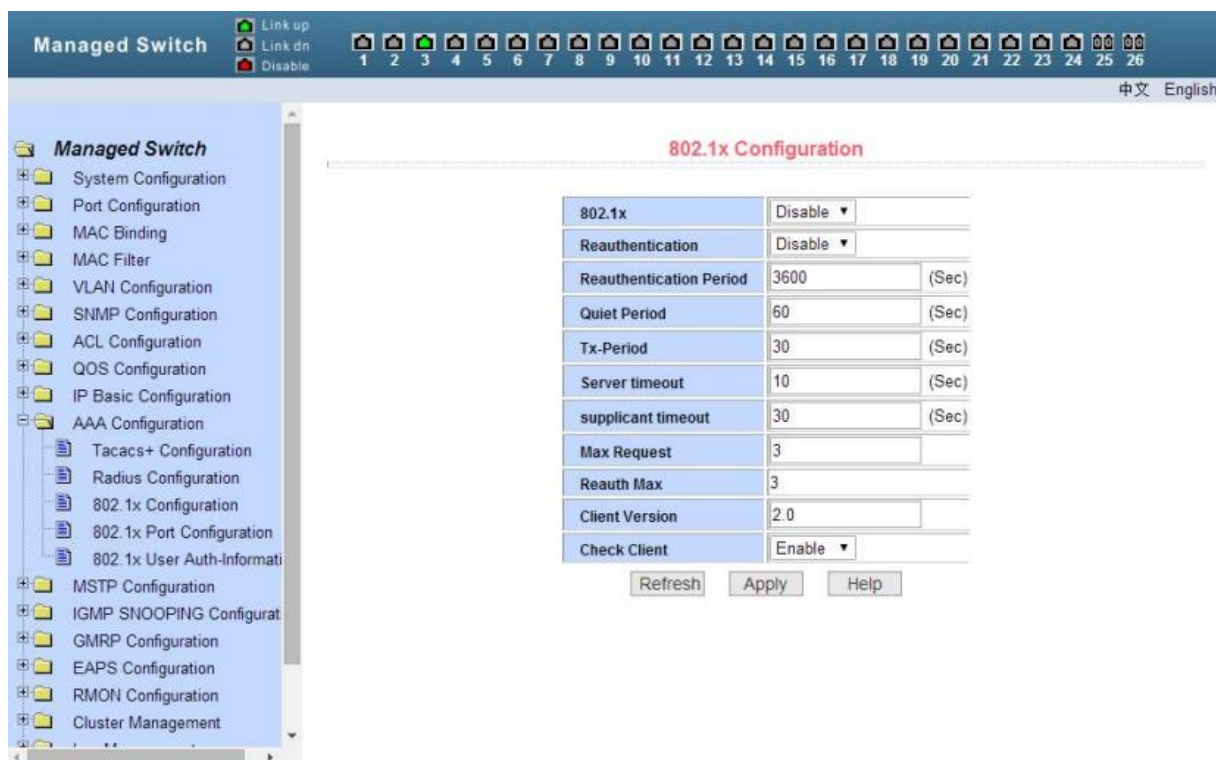


Рис. 49 Страница конфигурации 802.1x

(4) страница конфигурации порта 802.1x

На рисунке 50 показана страница конфигурации порта 802.1x. Вы можете настроить режим порта 802.1x и максимальное количество хостов. Вы также можете просмотреть конфигурацию 802.1x каждого порта. Режим порта 802.1x включает в себя четыре типа: статус отсутствия доступа, автоматическое состояние, статус принудительной авторизации и статус принудительной авторизации без разрешения. Когда необходимо выполнить аутентификацию на порту 802.1 x, для состояния порта устанавливается значение Auto, для получения доступа к сети необходимо выполнить сертификацию, для состояния порта устанавливается значение N/A, два других состояния редко используются на практике.

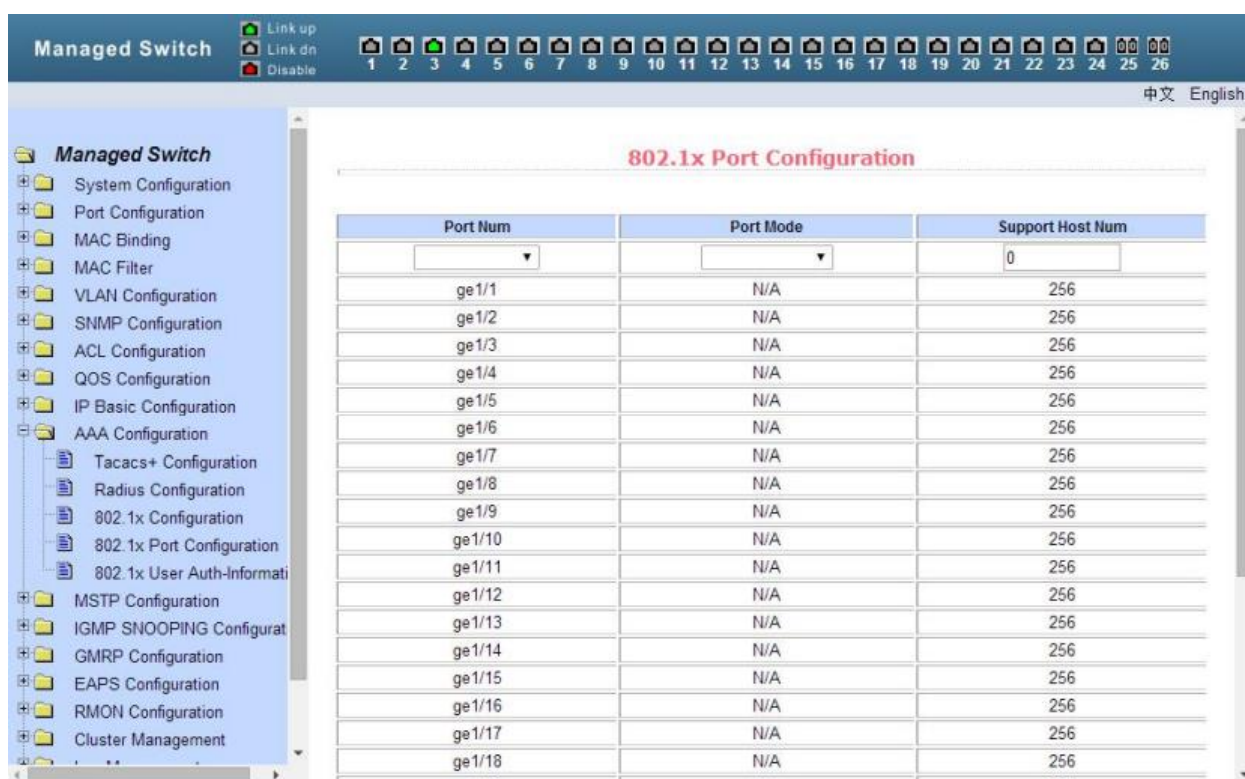


Рис. 50 Страница конфигурации порта 802.1x.

Когда включена аутентификация 802.1x, максимальное количество хостов, к которым может быть получен доступ через порт, равно 256, пользователь может изменить это значение.

(5) страница с информацией об авторизации пользователя 802.1x

На рисунке 51 показана страница с информацией об авторизации пользователя 802.1x. На этой странице вы можете просмотреть информацию о статусе всех пользователей, получающих доступ к порту.

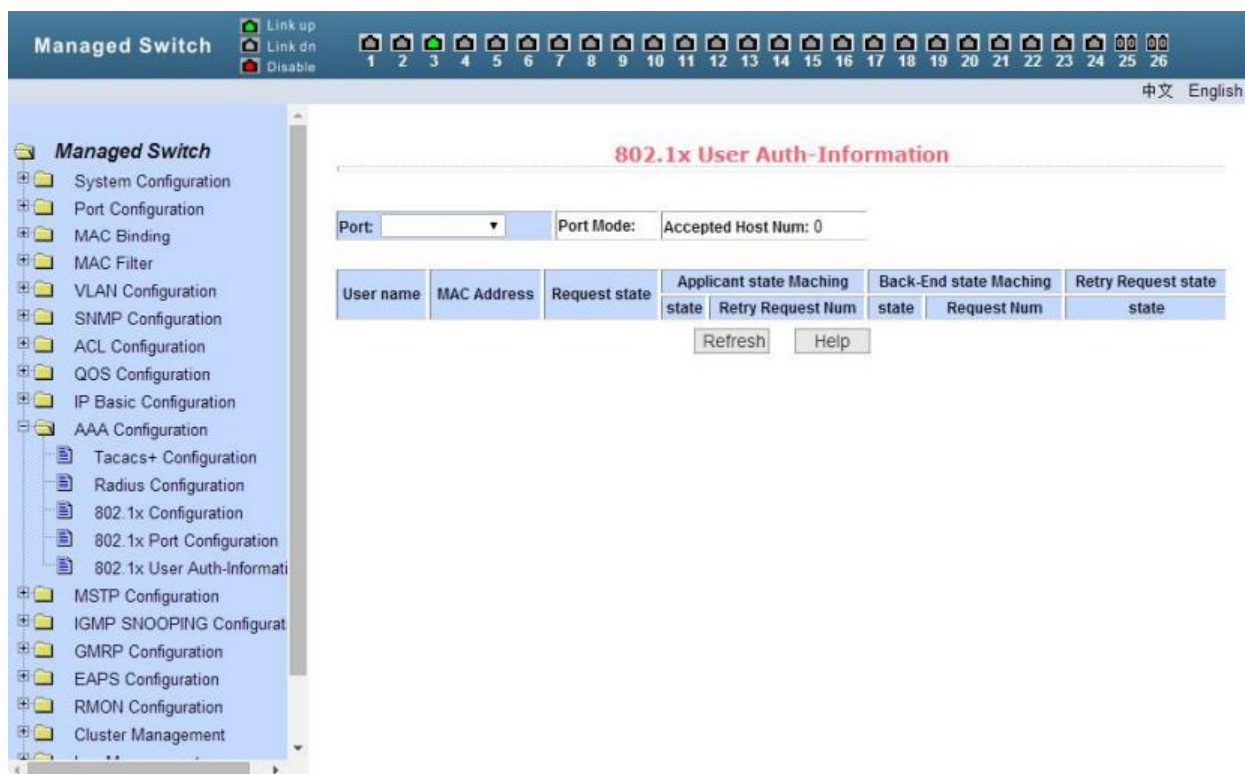


Рис. 51 Страница с информацией об авторизации пользователя 802.1x

13. Конфигурация MSTP

(1) Страница глобальной конфигурации MSTP

На рисунке 52 показана страница глобальной конфигурации MSTP. На этой странице вы можете настроить глобальные параметры MSTP.

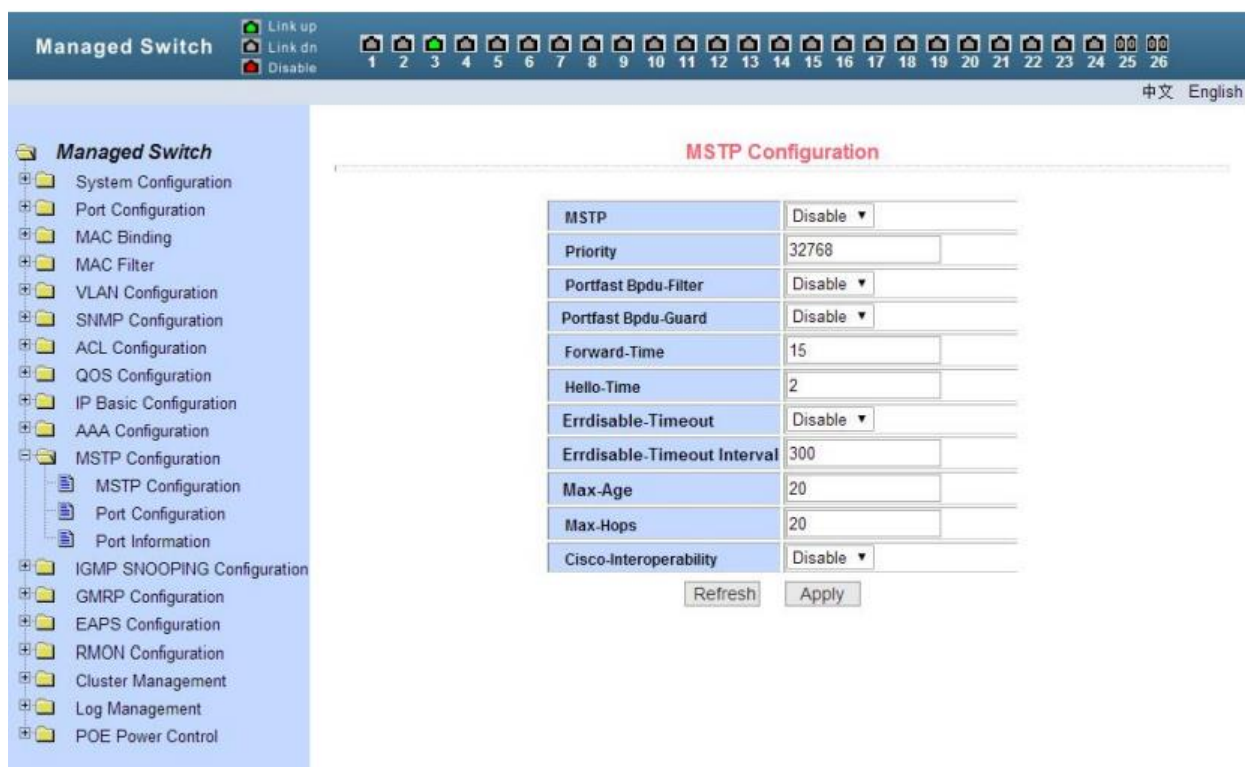


Рис. 52 Страница глобальной конфигурации MSTP

(2) Страница конфигурации порта MSTP

На рисунке 53 показана страница конфигурации порта MSTP. Вы можете использовать эту страницу для настройки параметров порта MSTP.

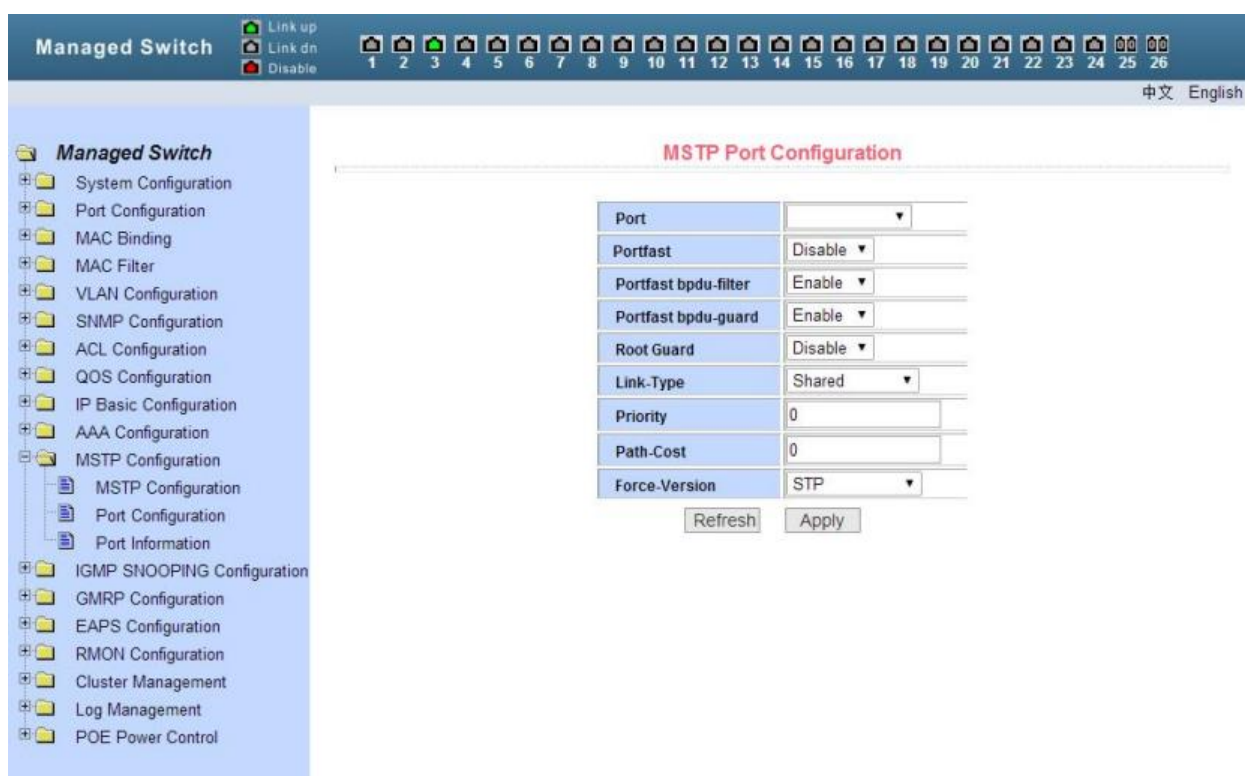
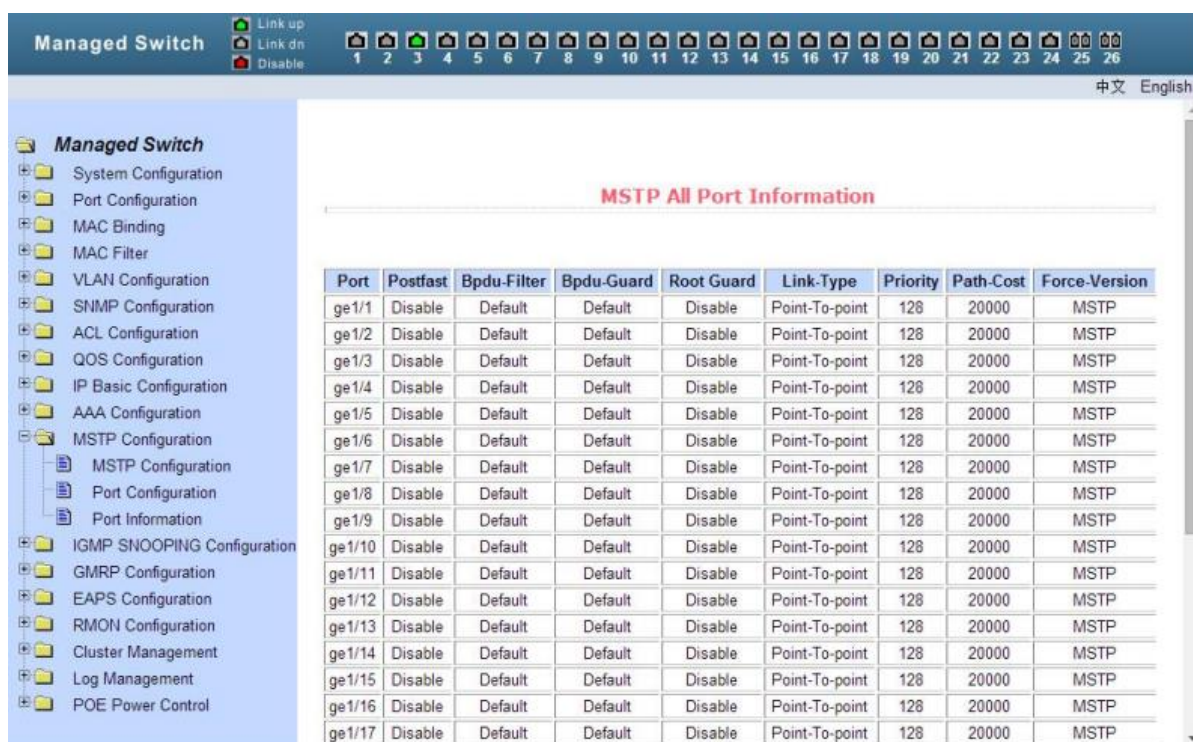


Рис. 53 Страница конфигурации порта MSTP

(3) Страница с информацией о порте MSTP

На рисунке 54 показана страница с информацией о порте MSTP. Вы можете просмотреть статус порта MSTP на этой странице.



The screenshot shows a network management interface for a 'Managed Switch'. The left sidebar contains a navigation tree with categories like System Configuration, Port Configuration, MAC Binding, etc. The main area displays 'MSTP All Port Information' as a table with the following data:

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	20000	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
ge1/11	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/12	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/13	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/14	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/15	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/16	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/17	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP

Рис. 54 Страница с информацией о порте MSTP

14. Конфигурация отслеживания IGMP

(1) Страница глобальной конфигурации отслеживания IGMP

На рисунке 55 показана страница глобальной конфигурации отслеживания IGMP. Вы можете включить отслеживание IGMP на этой странице.

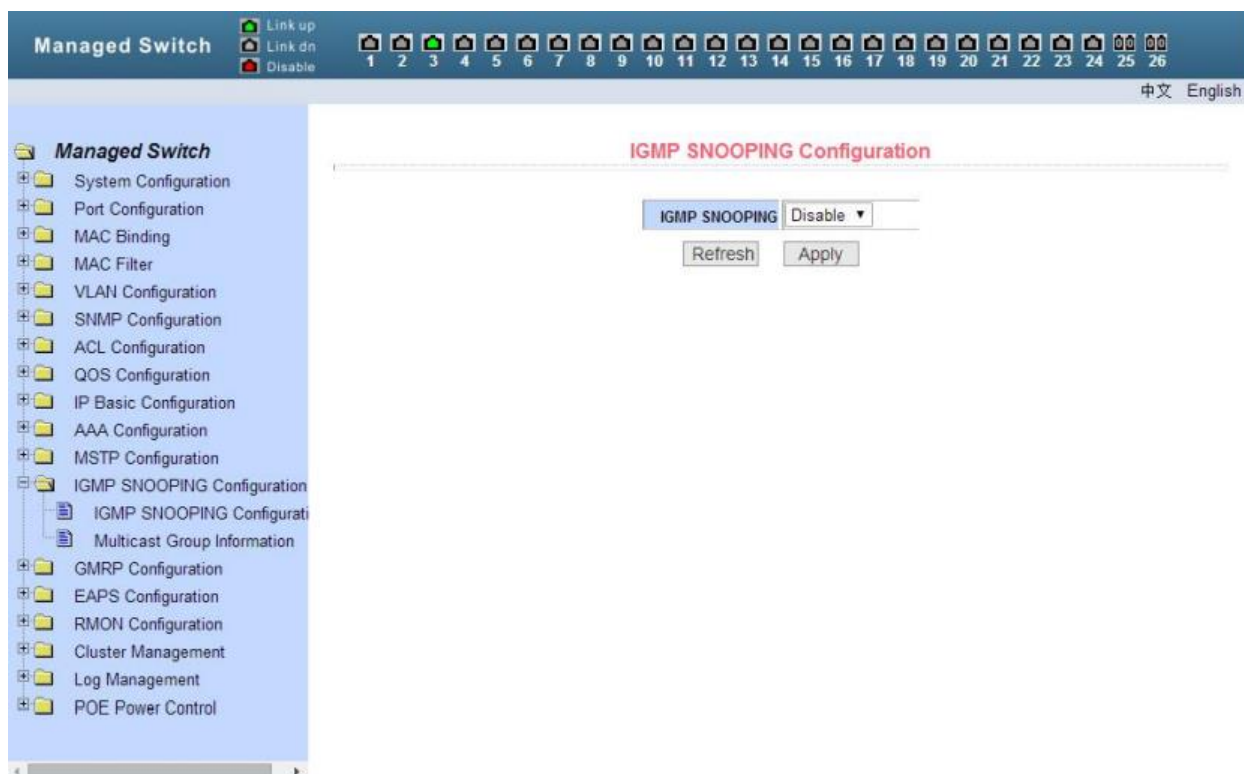


Рис. 55 Страница глобальной конфигурации отслеживания IGMP

(2) Страница информации о группе многоадресной рассылки

На рисунке 56 показана страница информации о группе многоадресной рассылки, на которой вы можете просмотреть информацию о программе многоадресной рассылки igmp snooping.

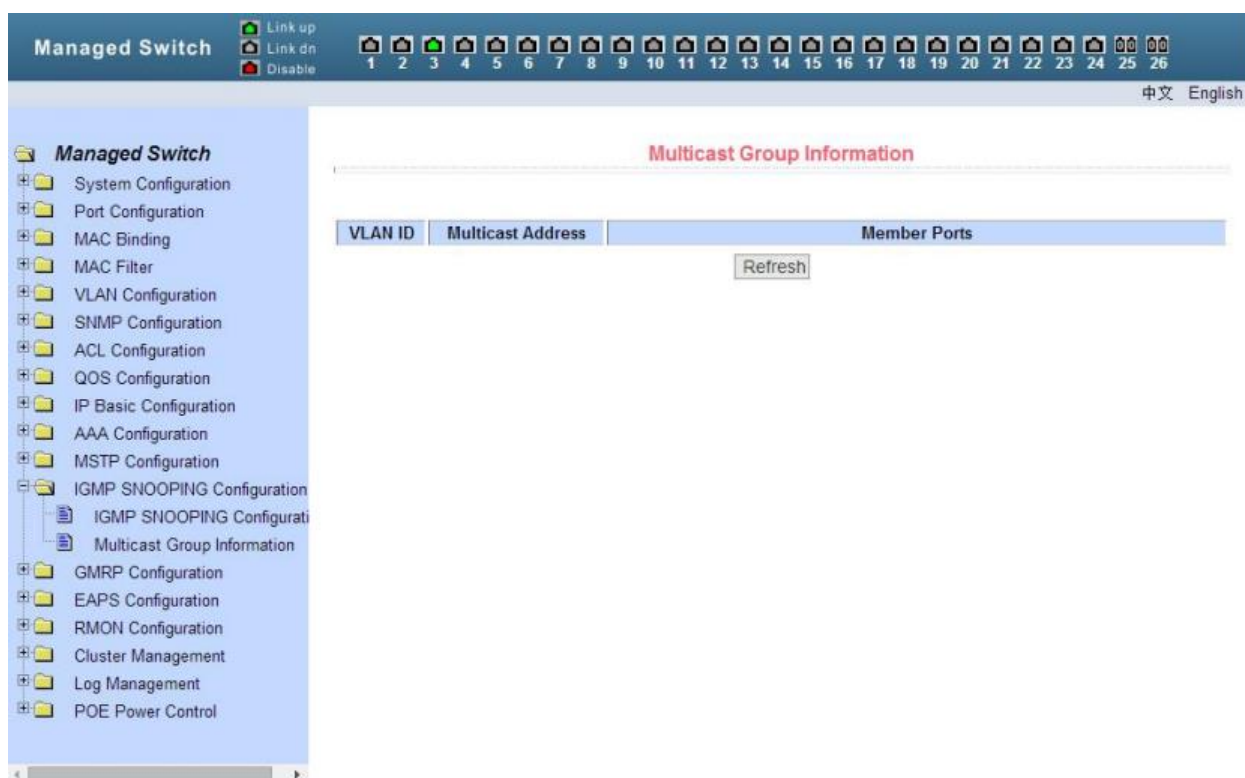


Рис. 56 Информационная страница группы многоадресной рассылки

15. Конфигурация GMRP

(1) Страница глобальной конфигурации GMRP

На рисунке 57 показана страница глобальной конфигурации GMRP. Пользователи могут включить GMRP на этой странице.



Рис. 57 Страница глобальной конфигурации GMRP

(2) Страница конфигурации порта GMRP

На рисунке 58 показана страница конфигурации порта GMRP. Пользователи могут использовать эту страницу для включения порта GMRP и просмотра информации о порте.

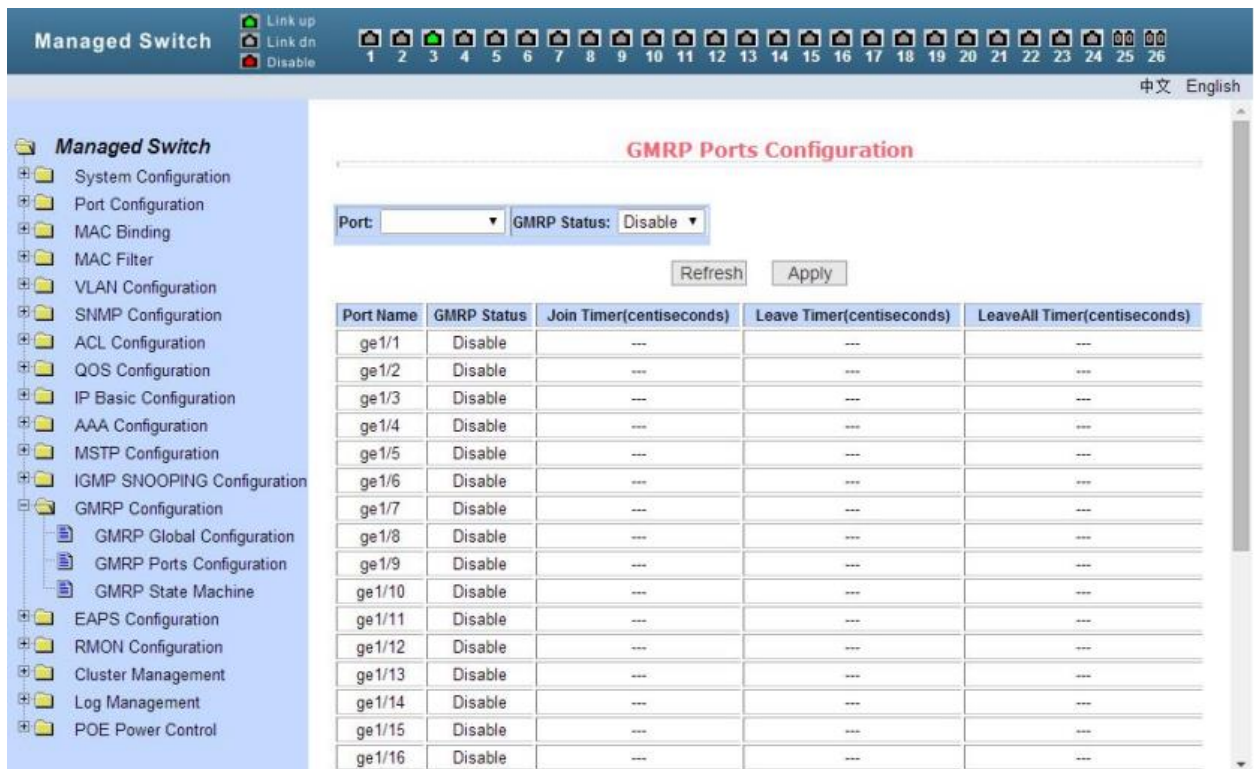


Рис. 58 Страница конфигурации порта GMRP

(3) Страница конечного автомата GMRP

Рисунок 59 - страница конечного автомата GMRP. Пользователи могут просматривать информацию о конечном автомате GMRP на этой странице.

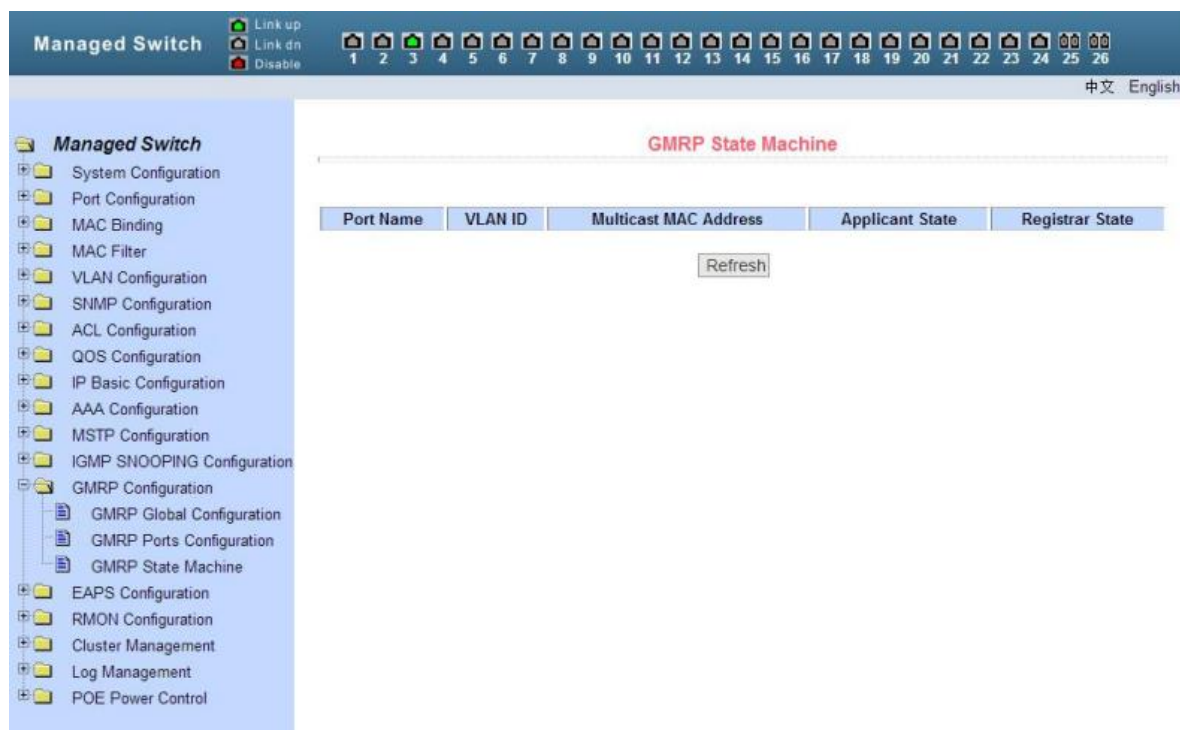


Рис. 59 Страница конечного автомата GMRP

16. Конфигурация EAPS

(1) Страница конфигурации EAPS

Эта страница используется для создания и настройки информации EAPS, а также для удаления и отображения информации EAPS.

Идентификатор кольца EAPS: конкретный идентификатор кольца в диапазоне от 1 до 16 может быть выбран в соответствии с раскрывающимся списком.

Создайте два типа, «Not Created» и «Created», если вы не можете их создать, создайте шаблон «Master» и «Transit», соответствующий режим может быть настроен по конкретным потребностям.

Основной порт EAPS: основной порт, такой как: fe 1/1, ge1/ 1.

Альтернативный порт EAPS: второй порт.

Управляющая vlan: EAPS кольцевая управляющая vlan, значение 2-4094.

Защищенная vlan: EAPS кольцевая защитная vlan

Временной интервал приветствия: приветственное сообщение для отправки временного интервала, значение по умолчанию равно 1с.

Время сбоя: определение времени сбоя, значение по умолчанию равно 3с.

Передача данных по кольцу: в случае нескольких колец эта функция требуется, когда необходимо передать данные по кольцу. По умолчанию не включена.

Исключительная совместимость с устройствами: radical network, включена по умолчанию.

Включено состояние: включено последнее кольцо EAPS.

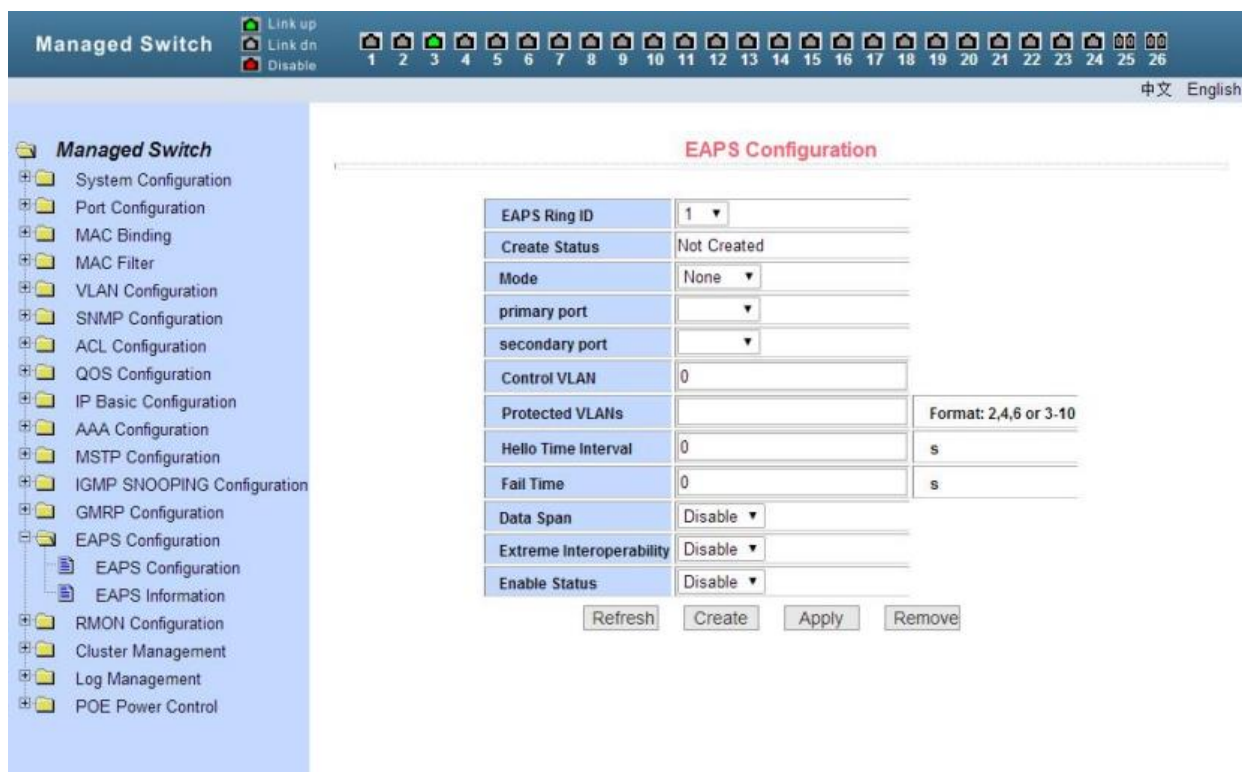


Рис. 60 Страница конфигурации EAPS

(2) Информационная страница EAPS

На рисунке 61 показана информационная страница EAPS. Пользователи могут просматривать информацию о конфигурации EAPS на этой странице.

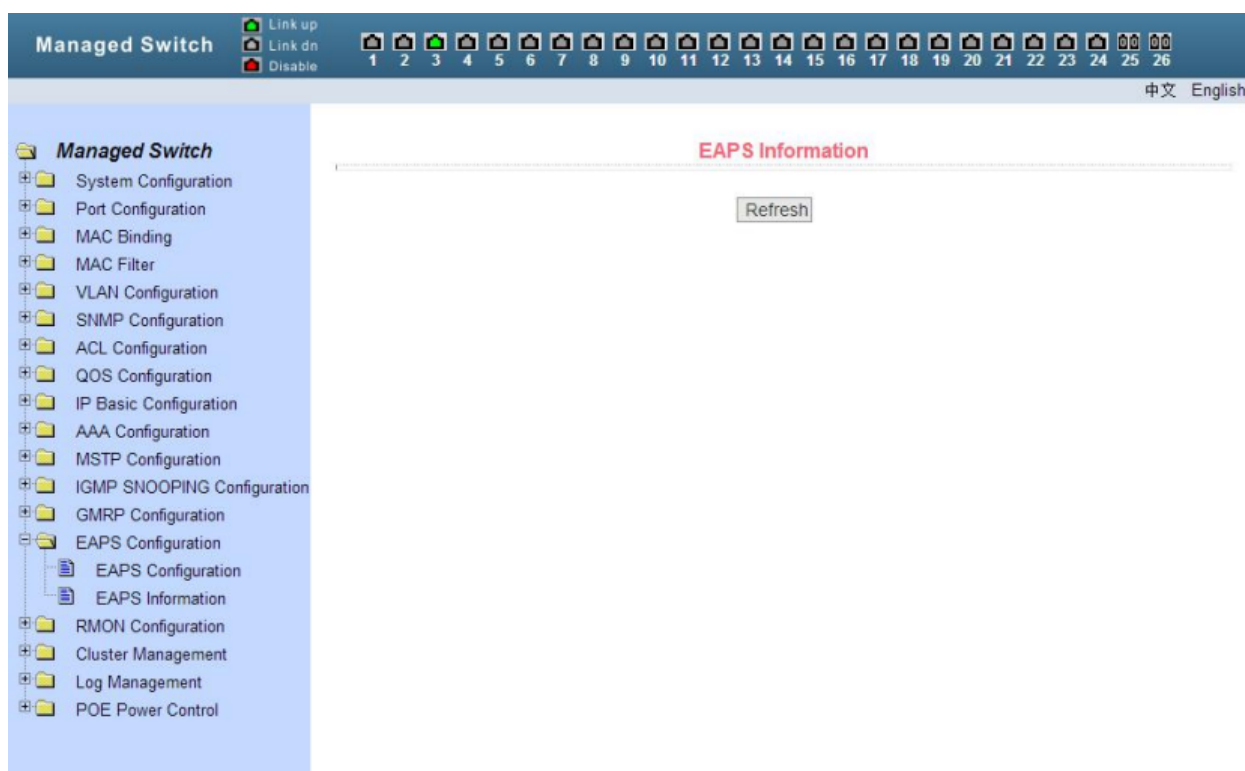


Рис. 61 Информационная страница EAPS

17. Конфигурация RMON

(1) Страница настройки группы статистики RMON

На рисунке 62 показана страница конфигурации группы статистики RMON. Пользователь может настроить группу статистики RMON на этой странице. Выберите порт из выпадающего списка для просмотра и настройте конфигурацию группы статистики RMON для этого порта. Если номер индекса равен 0, то вводится правильный номер индекса (в диапазоне от 1 до 100), владелец необязателен. Вы можете настроить группу статистики RMON для порта. В таблице статистики отображается статистика порта после успешной настройки.

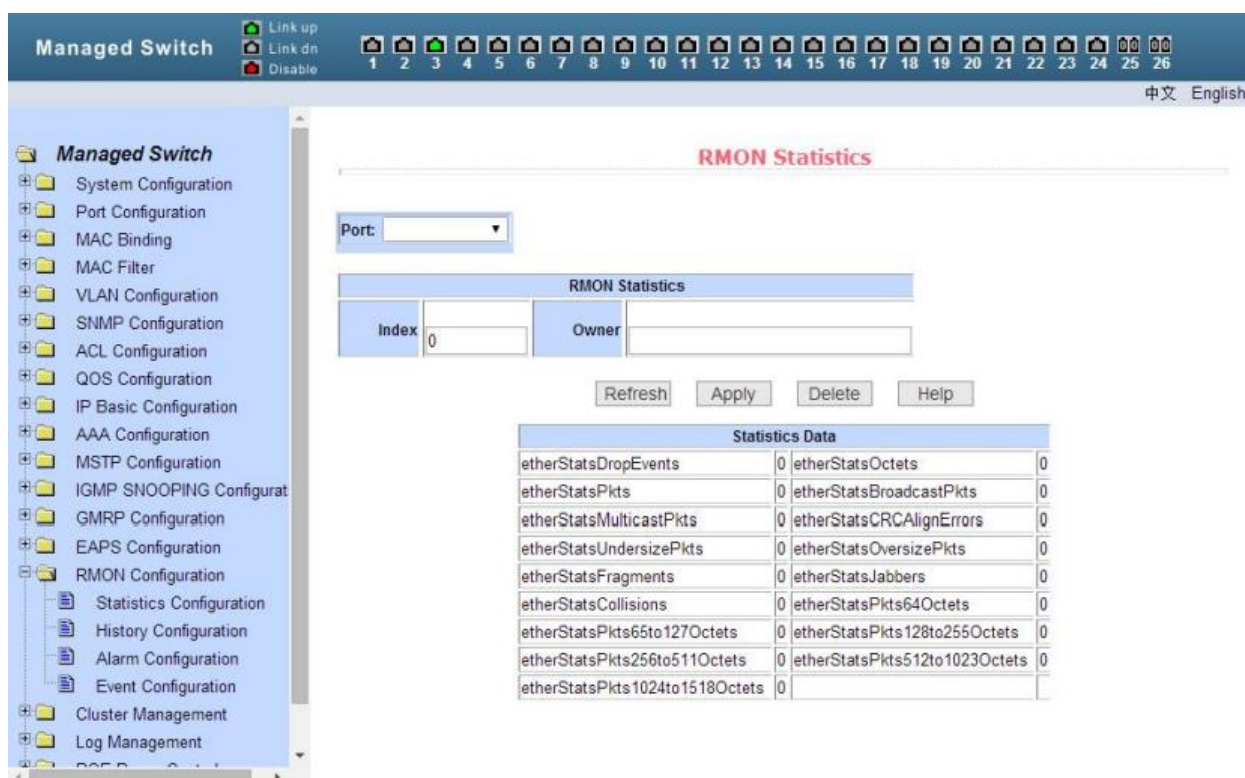


Рис. 62 Страница конфигурации группы статистики RMON

(2) Страница конфигурации группы истории RMON

На рисунке 63 показана страница конфигурации группы истории RMON. Пользователь может настроить группу истории RMON на этой странице. Выберите порт из выпадающего списка, чтобы просмотреть/настроить конфигурацию группы истории RMON для этого порта. Если номер индекса равен 0, то установите правильный номер индекса (в диапазоне от 1 до 100), интервал, сегменты запросов и владелец необязательны. Вы можете настроить группу журнала RMON для порта. Интервал относится к временному интервалу для сбора данных в секундах в диапазоне от 1 до 3600; сегменты запроса - это выделенный размер хранилища, указывающий, сколько записей хранится, диапазон составляет 1-100. В таблице статистики показаны прошлые данные, которые были получены с момента успешной настройки.

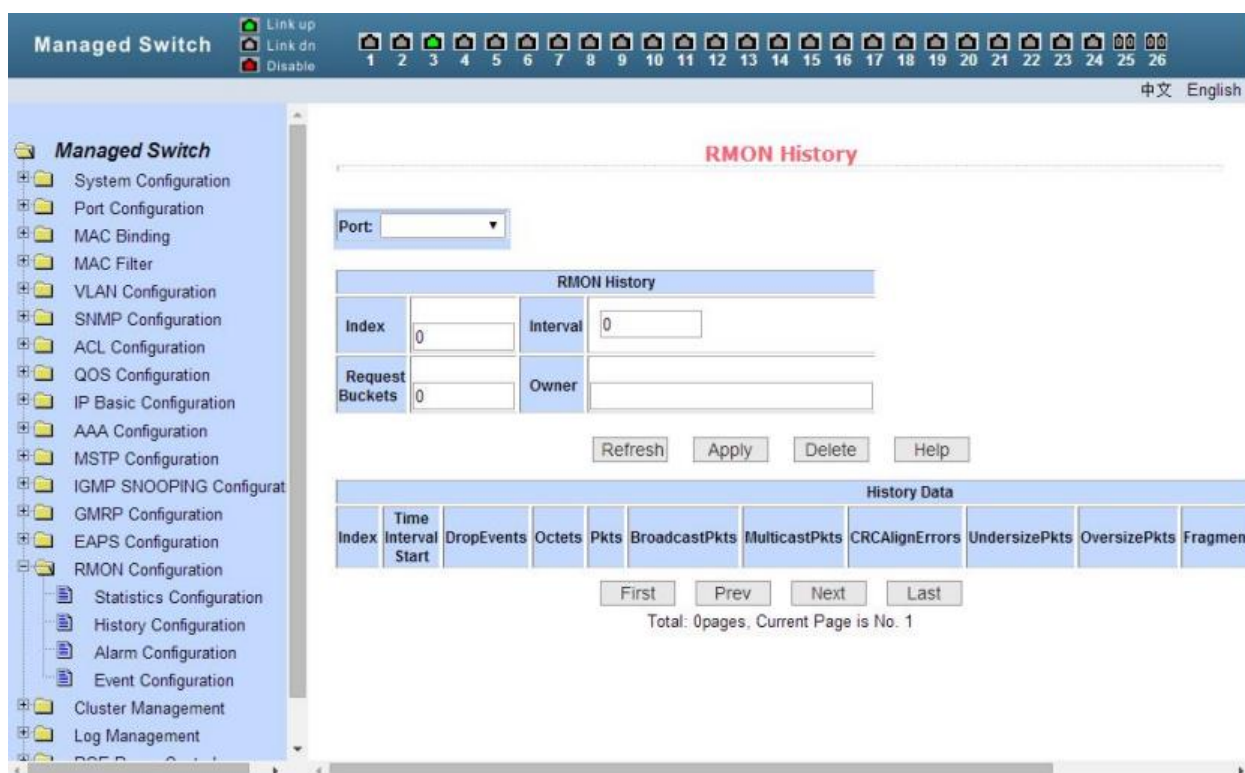


Рис. 63 Страница конфигурации группы RMON history

(3) Страница конфигурации группы аварийных сигналов RMON

На рисунке 64 показана страница конфигурации группы аварийных сигналов RMON, где пользователи могут создавать или изменить группу аварийных сигналов RMON. Выберите настроенную группу аварийных сигналов из выпадающего списка, чтобы просмотреть или настроить ее информацию, и выберите «Создать», чтобы создать ее. Диапазон индексов от 1 до 60, интервал от 1 до 3600 (в секундах), объект мониторинга должен заполнить узел MIB, также необходимо заполнить верхний и нижний пороговые значения, индекс события, владелец заполнять не обязательно. Значение аварийного сигнала доступно только для чтения и показывает выбранное значение на момент выдачи последнего аварийного сигнала. Индекс события относится к индексному номеру группы событий RMON и должен быть настроен заранее.

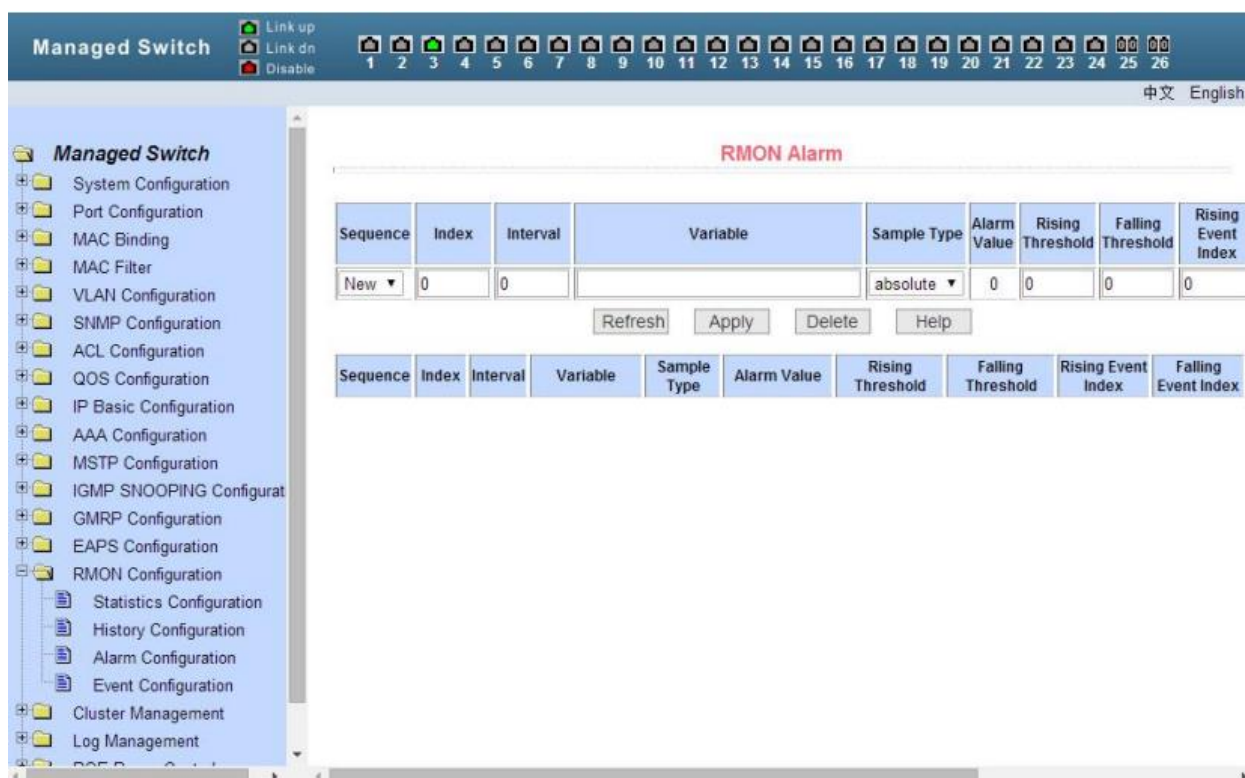


Рис. 64 Страница конфигурации группы аварийных сигналов RMON

(4) Страница конфигурации группы событий RMON

На рисунке 65 показана страница конфигурации группы событий RMON, где пользователи могут создавать и изменять группы событий RMON. Выберите настроенную группу событий из выпадающего списка для просмотра, настройте ее информацию и выберите «Создать», чтобы создать ее. Диапазон индексов от 1 до 60, а описание представляет собой строку. В качестве действия можно выбрать none (нет операции), log (журнал регистрации), SNMP-traplog-and-trap, общее имя не работает на этом устройстве, владелец необязателен. Время последней отправки доступно только для чтения и показывает время последней отправки события.

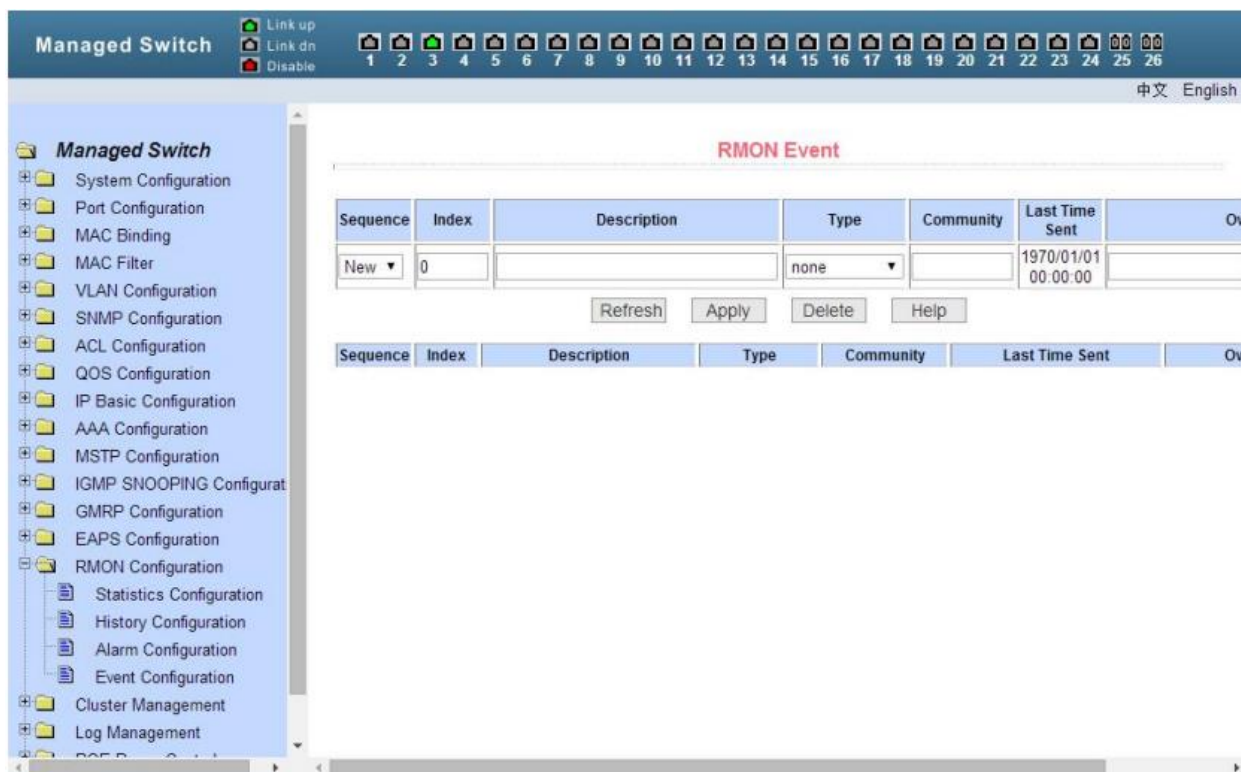


Рис. 65 Страница конфигурации группы событий RMON

18. Конфигурация кластера

(1) Страница конфигурации NTP

На рисунке 66 показана страница конфигурации NTP, где пользователи могут настроить NTP. Информация, которую можно настроить, включает в себя: выбор порта, функцию NTP порта, глобальную функцию BP, интервал отправки пакетов UDP и время ожидания пакетов NDP на принимающем устройстве.

Выберите порт по мере необходимости и включите функцию определения местоположения порта. NDP должен работать корректно, и функция определения местоположения глобального и порта должна быть включена.

Настройте время ожидания UDP-пакетов, отправляемых устройством, на принимающем устройстве. Диапазон эффективного времени составляет 1-4096 секунд. Конфигурация по умолчанию - 180 секунд.

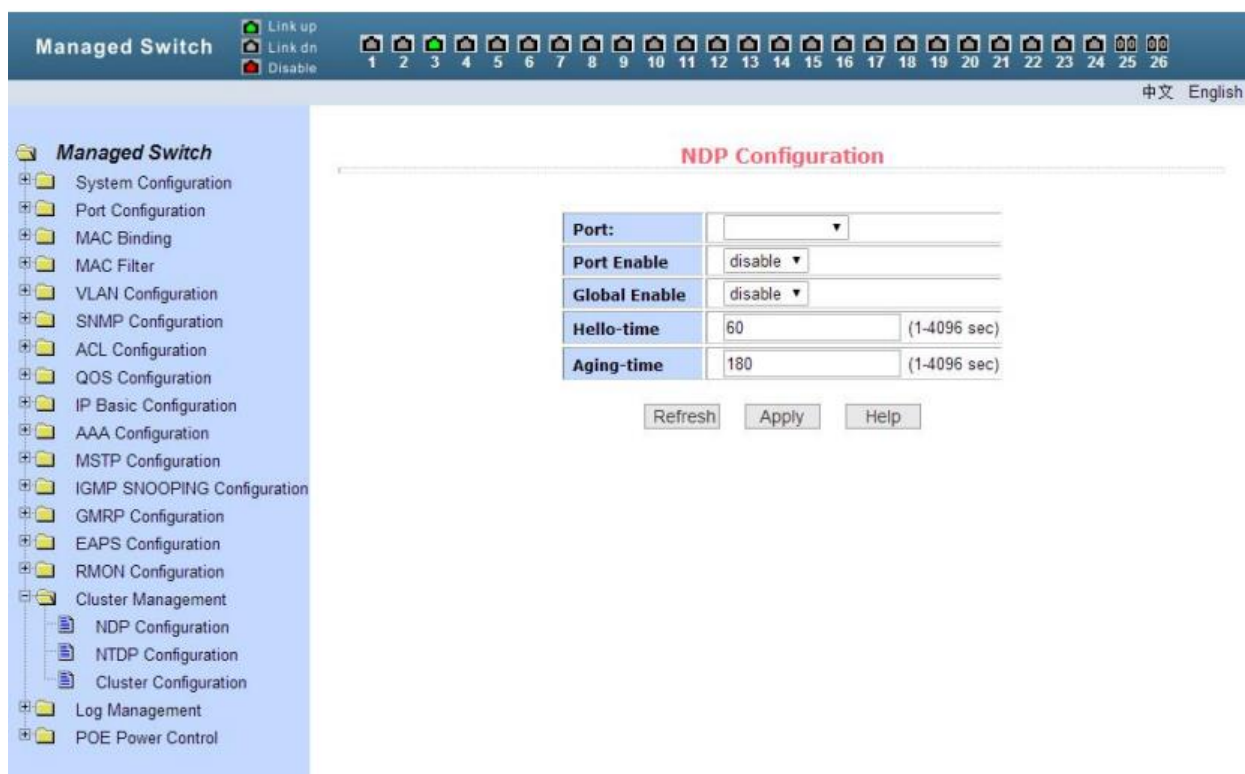


Рис. 66 Страница конфигурации NDP

(2) Страница конфигурации NTP

На рисунке 67 показана страница конфигурации NTDP, где пользователи могут настроить NTDP. Информация, которую можно задать, включает в себя: Выбор порта, включение функции NTDP порта, включение глобальной функции NTDP, диапазон сбора топологии, временной интервал сбора топологии, время задержки первого пакета переадресации порта и задержки других пакетов переадресации порта.

Выбор порта, вы можете выбрать порт по мере необходимости и включить функцию port NTDP. Для нормальной работы NTDP необходимо также включить функцию global и port NTDP.

Настройте диапазон сбора топологии. Эффективный диапазон составляет 1-6. В топологии по умолчанию максимальное количество переходов устройства равно 3.

Настройте интервал для сбора информации о топологии. Эффективный диапазон составляет 0-65535 минут. Конфигурация по умолчанию - 1 минута.

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

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

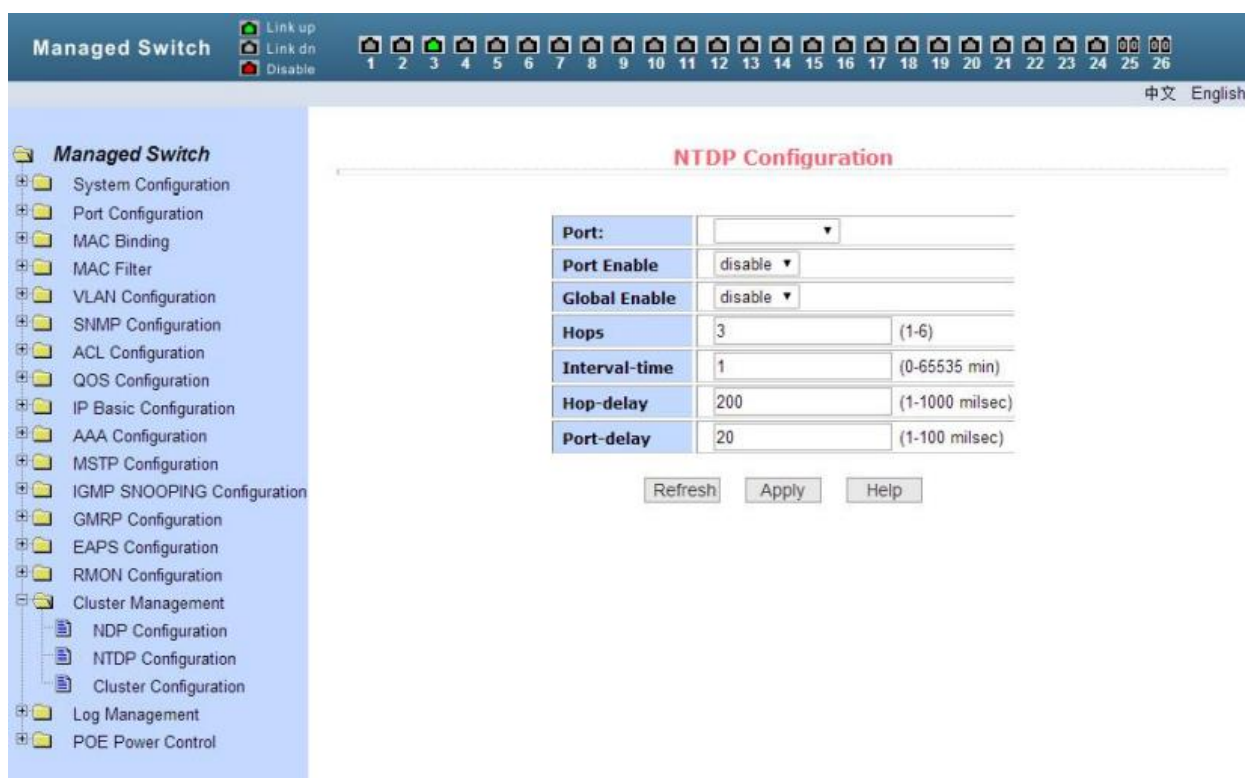


Рис. 67 Страница конфигурации NTDP

(3) Страница конфигурации кластера

На рисунке 68 показана страница конфигурации кластера, пользователь может настроить кластер через эту страницу и просмотреть таблицу элементов кластера. Информация, которую можно задать, содержит функции включения кластера, настройки управляющей VLAN, пула адресов кластера, интервала отправки пакетов подтверждения, эффективного времени хранения устройства, имени кластера, способа присоединения к кластеру и удаления кластера.

Включите функцию cluster.

Настройте VLAN управление с допустимым диапазоном 1-4094 и значением по умолчанию vlan1.

Настройте диапазон частных IP-адресов, используемых устройствами-членами кластера. Диапазон IP-адреса составляет 0.0.0.0 ~ 255.255.255.255. Диапазон длины маски составляет 0 ~ 32.

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

Настройте время удержания устройства. Диапазон составляет 1-255 секунд. Конфигурация по умолчанию - 60 секунд.

Чтобы создать кластер, вам необходимо настроить имя кластера, выбрать присоединение к кластеру, способ присоединения как ручной, так и автоматический. После настройки кластера его можно автоматически переключить на ручной, но ручной режим нельзя переключить на автоматический. В ручном режиме можно изменить название кластера.

После создания кластера вы можете просмотреть устройства-участники и устройства-кандидаты в таблице участников кластера, вы можете добавить устройство-участник или добавить устройство-кандидат к устройству-участнику в зависимости от роли.

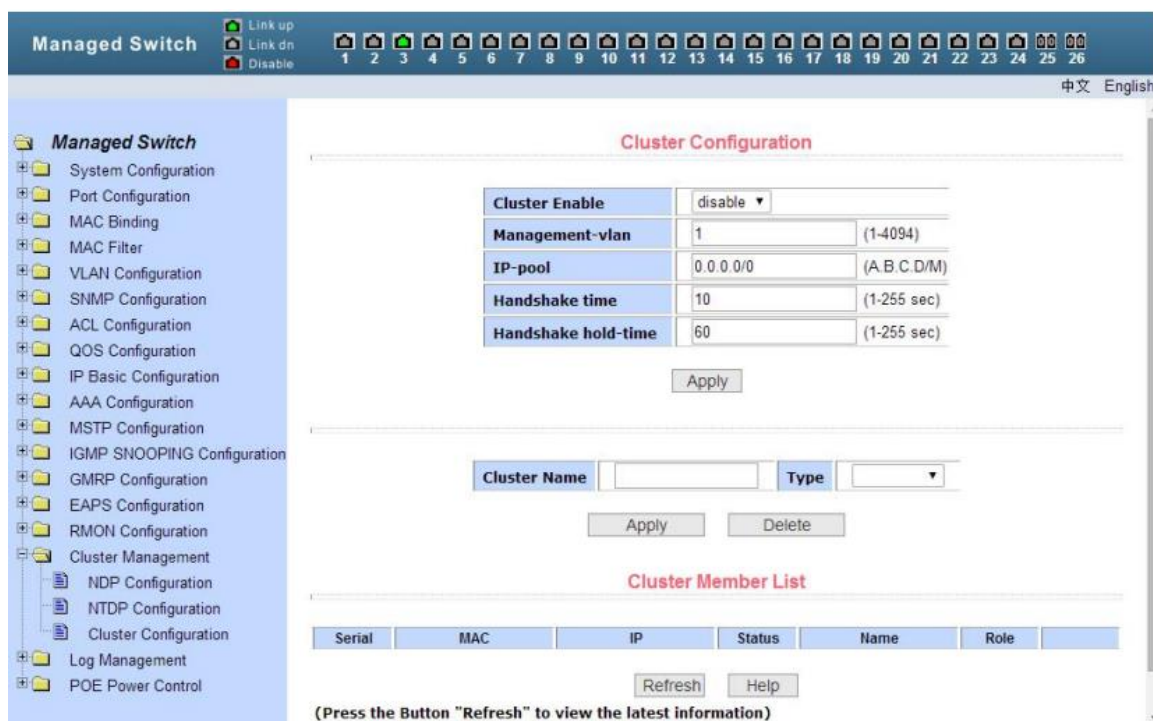


Рис. 68 страница конфигурации кластера

19. Конфигурация ERPS

(1) Страница конфигурации EAPS

На рисунке 69 показана страница конфигурации EAPS, пользователи могут использовать эту страницу для включения функции ERPS, настройки параметров ERPS, создания и удаления экземпляра ERPS, ERPS ring и других приложений.

Экземпляр ERPS: создание и удаление экземпляров ERPS (<1-8>).

Роль узла: настройте роль узла в кольце ERPS, узла межсетевого взаимодействия или несвязанного узла.

Кольцо ERPS: создание и удаление колец ERPS (<1-32>).

Режим кольца: настройка режима кольца ERPS, основного кольца или вспомогательного кольца.

Настройка режима узла: режим кольцевого узла ERPS, узел владельца RPL, соседний узел RPL или общий кольцевой узел.

Конфигурация протокола VLAN: удаление ERPS ring protocol VLAN (<2-4094>).

Конфигурация VLAN данных ERPS Ring Data VLAN (<1-4094>).

Конфигурация кольцевого порта: удаление ERPS ring port, RPL-порта или общего кольцевого порта.

Поведение восстановления: настройте поведение восстановления ERPS ring, восстанавливаемое или невозстановимое.

Wtr Time: настройка времени задержки цикла ERPS (<0-10000>), в мс, значение по умолчанию - 0. Время защиты кольца ERPS (<10-2000>), в мс, значение по умолчанию 500 втр. Настройка времени wtr кольца ERPS (<1-12>), в мин, значение по умолчанию — 5.

Wtb Time: настройте время wtb вызова ERPS (<1-10>), в секундах, значение по умолчанию - 5.

Время передачи пакетов протокола: настройте время отправки пакетов протокола ERPS ring (<1-10>), в секундах, значение по умолчанию - 5.

Включить кольцо ERPS: включите или выключите кольцо ERPS.

Принудительное переключение порта ERPS ring: принудительно, снимите флажок для переключения порта ERPS ring.

Принудительное включение порта ERPS ring вручную, снимите ручной порт ERPS ring.

Ручное восстановление: управляет восстановлением ERPS ring или ручным восстановлением до истечения срока действия WTR / WTB.



Through the serial line adjustment

Рис. 69 Страница конфигурации EAPS

(2) Информационная страница ERPS

На рисунке 70 показана информационная страница ERPS, где пользователи могут просматривать информацию о конфигурации ERPS.

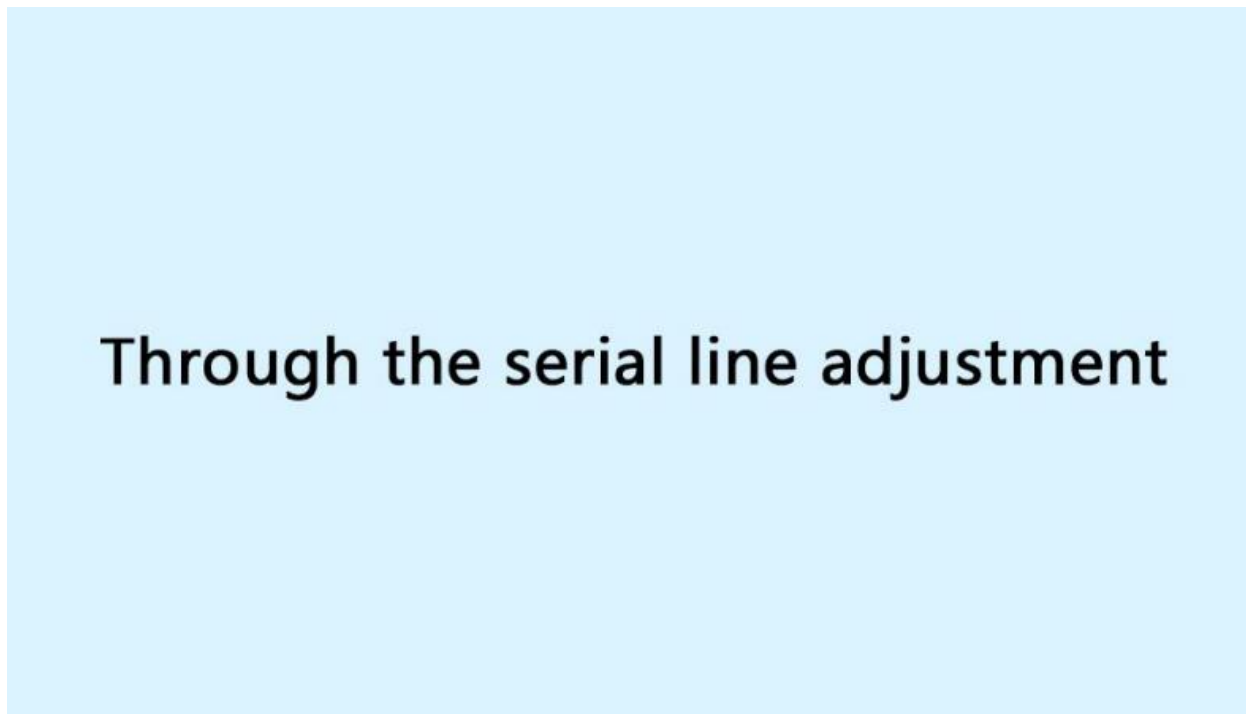


Рис. 70 Информационная страница EAPS

20. Управление журналами

(1) Информация о журнале регистрации

На рисунке 71 показана страница с информацией о журнале, пользователь может просмотреть журнал через эту страницу. Выберите приоритет из выпадающего списка, вы можете просмотреть журнал этого уровня, нажмите «Обновить», чтобы просмотреть последний журнал.

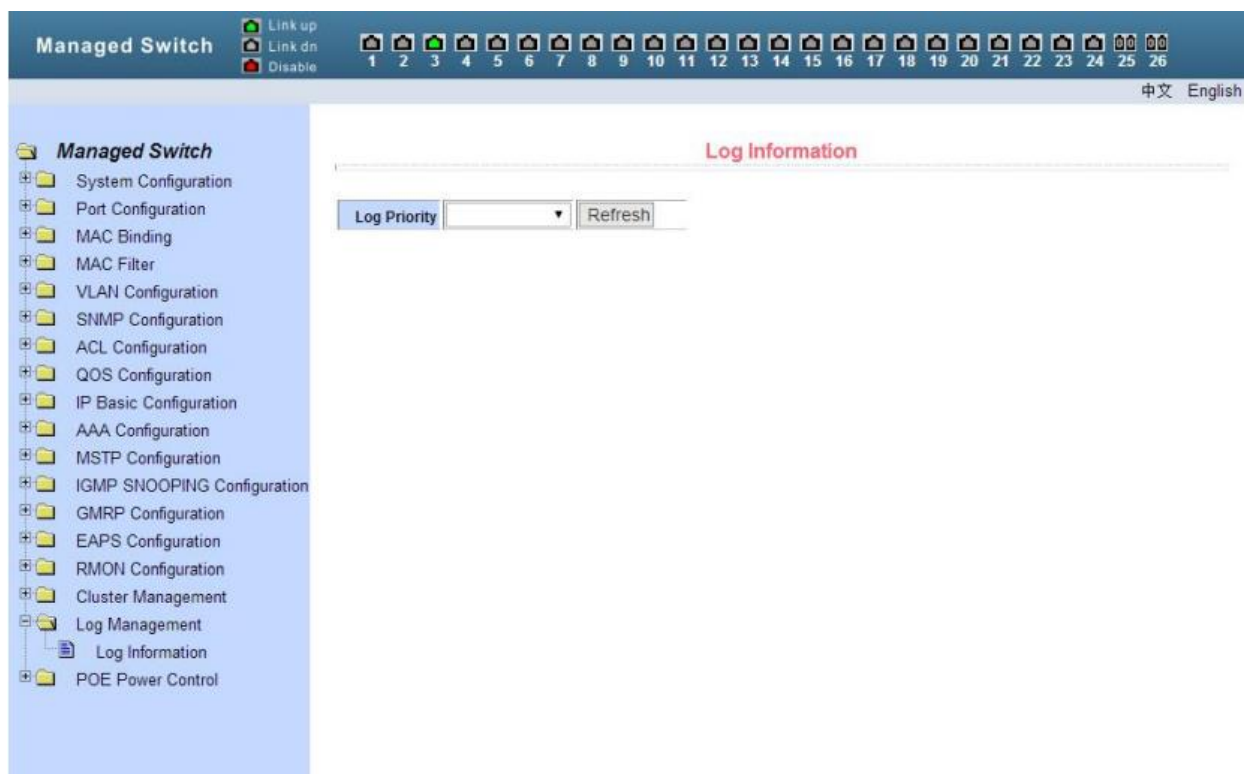


Рис. 71 Информационная страница журнала

21. Конфигурация порта POE

(1) Конфигурация порта POE

На рисунке 72 показана страница конфигурации устройства POE. Вы можете настроить общую мощность устройства POE (для обновления), мощность одного порта POE (для обновления), включение или выключение питания. Эта страница позволяет просмотреть информацию о текущем устройстве POE.

Порт POE: выберите номер порта источника питания (1-24).

Статус товара POE: включить или выключить.



Рис. 72 Страница конфигурации продукта POE

(2) Настройка расписания POE

На рисунке 73 показана страница настройки расписания POE. С помощью управления расписанием вы можете включать или отключать питание POE в соответствии с фактическими требованиями. Режим управления - режим "час + неделя".

Порт управления: используется для выбора портов, которым требуется управление по расписанию (1-24).

Функция управления: включение или выключение.

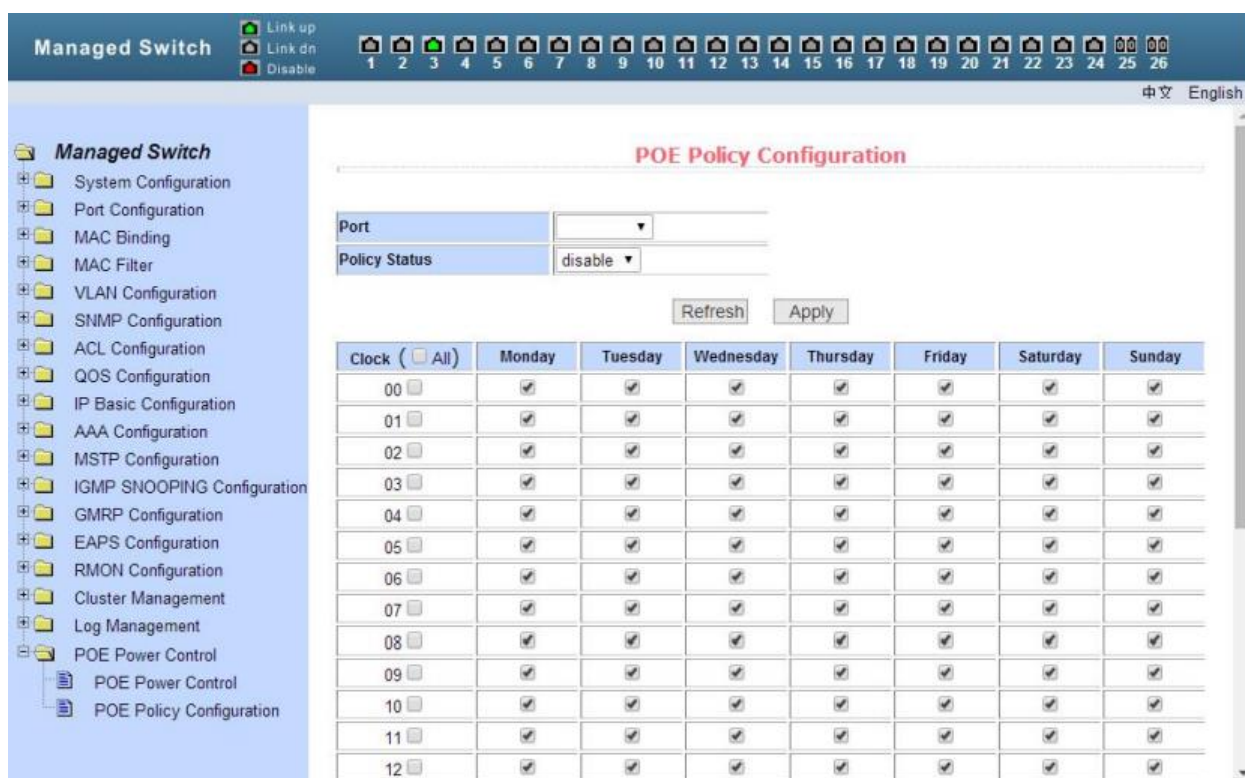


Рис. 73 Страница настройки расписания POE

(3) Конфигурация запроса PD

На рисунке 74 показана страница конфигурации запроса PD, и определение состояния устройства PD online может быть реализовано с помощью конфигурации запроса PD.

Порт POE: для выбора порта для подключения к устройству PD, которое необходимо запросить

IP-адрес PD: IP-адрес устройства PD.

Временной интервал запроса PD: интервал времени для запроса устройств PD (по умолчанию 5 секунд).

Максимальное количество не отвечающих запросов PD: максимальное количество раз, используемых для запроса устройств PD без ответа (по умолчанию 3 раза).

Максимальное время, необходимое для запуска PD: максимальное время, необходимое для запроса запуска.

Устройство PD (по умолчанию 120 секунд).

Managed Switch Link up
Link on
Disable

中文 English

PD Query Configuration

POE Port	<input type="text"/>	
PD IP Address	<input type="text"/>	
PD Query Interval	<input type="text" value="0"/>	(2~30 Sec)
PD Timeout Number	<input type="text" value="0"/>	(2~10)
PD Boot Time	<input type="text" value="0"/>	(30~600 Sec)

POE Port	PD IP Address	PD Query Interval (Sec)	PD Timeout Number	PD Boot Time (Sec)	PD Reboot Times
ge1/1	N/A	5	3	120	0
ge1/2	N/A	5	3	120	0
ge1/3	N/A	5	3	120	0
ge1/4	N/A	5	3	120	0
ge1/5	N/A	5	3	120	0
ge1/6	N/A	5	3	120	0
ge1/7	N/A	5	3	120	0
ge1/8	N/A	5	3	120	0
ge1/9	N/A	5	3	120	0

Рисунок 74 Страница конфигурации запроса PD