Промышленные управляемые коммутаторы серии STEZ48xx

Руководство пользователя

Оглавление

1. Описание устройства

1.1. Введение

Коммутаторы серии STEZ48xx, являются промышленными Ethernet-коммутаторами, использующими технологию управления IEC61850 MMS, что обеспечивает унифицированное моделирование и управление. Коммутаторы, специально разработанные для интеллектуальных подстанций и подходящие для суровых условий. Кроме того, коммутаторы соответствуют стандартам электроэнергетики IEC61850-3 и IEEE1613.

Коммутаторы поддерживает подключение оптических модулей SFP с функцией цифровой диагностики, который используется для контроля температуры, напряжения питания, тока смещения лазера, передачи и приема оптической мощности. Ссылаясь на такие измеренные параметры, блок управления может быстро обнаруживать ошибки, возникающие в оптических каналах, что помогает упростить техническое обслуживание и повысить надежность системы.

1.2. Модели серии

В портфолио серии STEZ48xx входят следующие коммутаторы:

- **STEZ4824-4G** (артикул 70000003) – коммутатор L2 уровня, с поддержкой 24 медных RJ45 портов 10/100/1000 Мбит/с и 4 SFP порта 100/1000 Мбит/с, резервированные источники питания 85-264VAC / 77-300VDC;
- **STEZ4800-16SFP-4G** (артикул 70000001) - коммутатор L2 уровня, с поддержкой 16 SFP портов 100 Мбит/с и 4 SFP порта 100/1000 Мбит/с, резервированные источники питания 85-264VAC / 77-300VDC;
- **STEZ4800-16GSFP** (артикул 70000002) – коммутатор L2 уровня, с поддержкой 16 SFP портов 1000 Мбит/с, резервированные источники питания 85-264VAC / 77-300VDC.

1.3. Функции программного обеспечения

Коммутаторы серии STEZ48xx поддерживают множество программных функций, удовлетворяющих различные требования клиентов.

- Протоколы резервирования: RSTP/STP, MSTP, ST-Ring, STRP;
- Протоколы маршрутизации: OSPFv2, RIP, статическая маршрутизация
- Поддержка мультикаст протоколов: IGMP Snooping, GMRP и static multicast
- VLAN, PVLAN, QoS и ARP
- Управление шириной канала: port trunk, port rate limiting
- Протоколы синхронизации времени: SNTP, NTP, PTPv2
- Безопасность: ACL, port isolate, привязка MAC-адресов, управление пользователями, IEEE802.1x, TACACS+, RADIUS, SSH, SSL

- Управление устройством: обновление программного обеспечения через FTP/TFTP, загрузка / выгрузка конфигурационного файла через FTP/TFTP, запись и загрузка журнала;
- Диагностика: зеркалирование портов, LLDP, определение состояния соединения, обнаружение петель, защита CRC;
- Функции уведомления: port alarm, power alarm, ring alarm, конфликт IP/MAC адресов, temperature alarm и port traffic alarm, alarm CPU / RAM, alarm CRC;
- Управление устройством: CLI, Telnet (SSH), Web, SNMPv1/v2/v3.

2. Управление коммутатором

Управление коммутатором возможно посредством:

- Консольного порта
- Telnet/SSH
- Web браузера

2.1. Тип просмотра

После подключения в Command Line Interface (CLI) через консольный порт или Telnet (SSH), возможно получить различный доступ, переключение между ними можно получить с помощью следующих команд.

Таблица 1. Типы просмотра

Отображение	Тип	Доступный функционал	Команды для смены уровня привилегий
SWITCH>	Основной режим	Просмотр недавно использованных команд. Просмотр версии ПО. Просмотр информации об ответе на операцию ping.	Введите «enable», чтобы войти в привилегированный режим.
SWITCH#	Привилегированный режим	Загрузить/выгрузить файл конфигурации; восстановить конфигурацию по умолчанию; просмотр информации об ответе на операцию ping; перезапустить коммутатор; сохранить текущую конфигурацию; показать текущую конфигурацию; обновить программное обеспечение; и т.д.	Введите "configure terminal" или "config" для входа в режим конфигурации из привилегированного режима. Введите "exit" для возврата в основной режим.
SWITCH(config)#	Режим конфигурации	Конфигурирование функций коммутатора.	Введите "exit" для возврата в привилегированный режим.

Когда коммутатор конфигурируется через интерфейс командной строки, то можно использовать для получения справки по команде "?". В справочной информации есть разные форматы описания параметров. Например, <1, 255> означает диапазон чисел; <H.H.H.H> означает IP-адрес; <H:H:H:H:H:H> означает MAC-адрес; слово<1,31> означает диапазон строк. Кроме того, с помощью ↑ и ↓ можно делать прокрутку недавно использовавшихся команд.

2.2. Управление коммутатором через консольный порт

Доступ к коммутатору можно получить через его консольный порт и гипертерминал ОС Windows или другого программного обеспечения, поддерживающего подключение через последовательный порт. В качестве примера приведен пример подключения с помощью приложения PuTTY

RJ45 Connector

Подключите 9-пиновый консольный порт на PC в консольный кабель на коммутаторе с помощью консольного кабеля DB9-RJ45.

- Запустите приложение PuTTY или аналогичное приложение для эмуляции терминала;

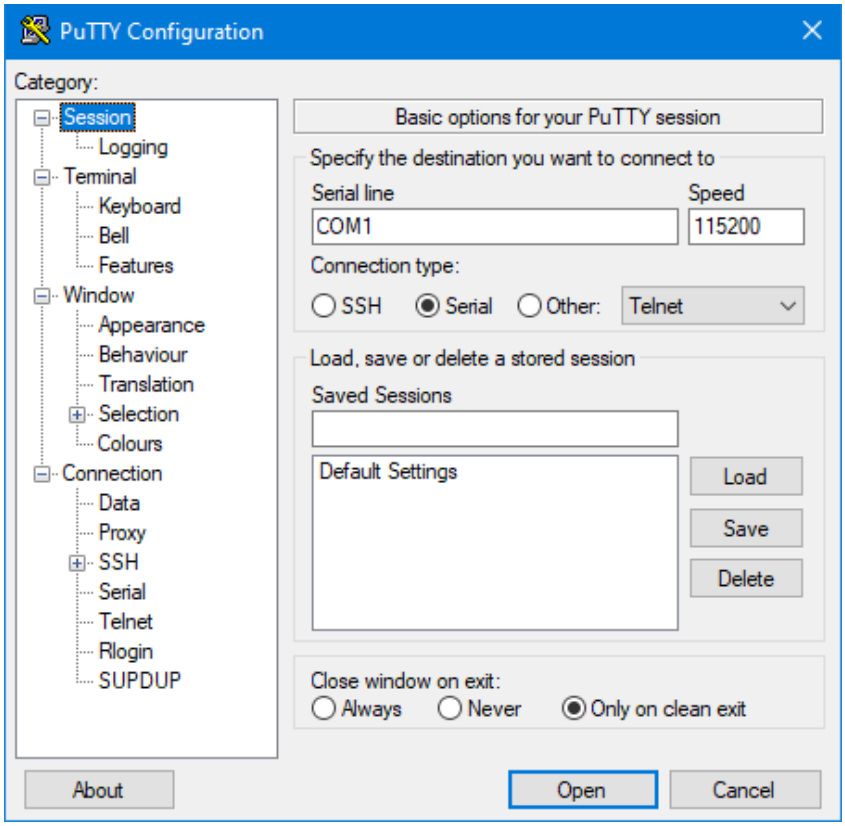


Рис. 1. Запуск Hyper Terminal

- Введите имя для нового соединения

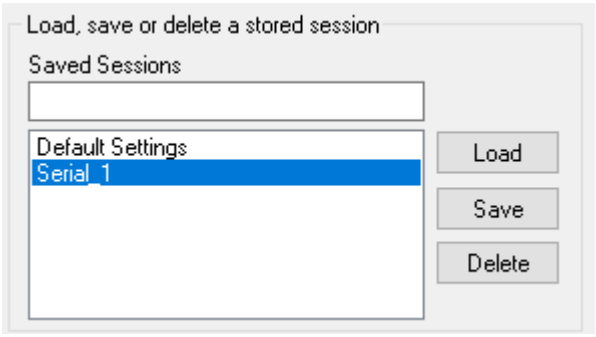


Рис. 2. Создание нового соединения

- Перейдите в категорию Serial и задайте параметры порта;

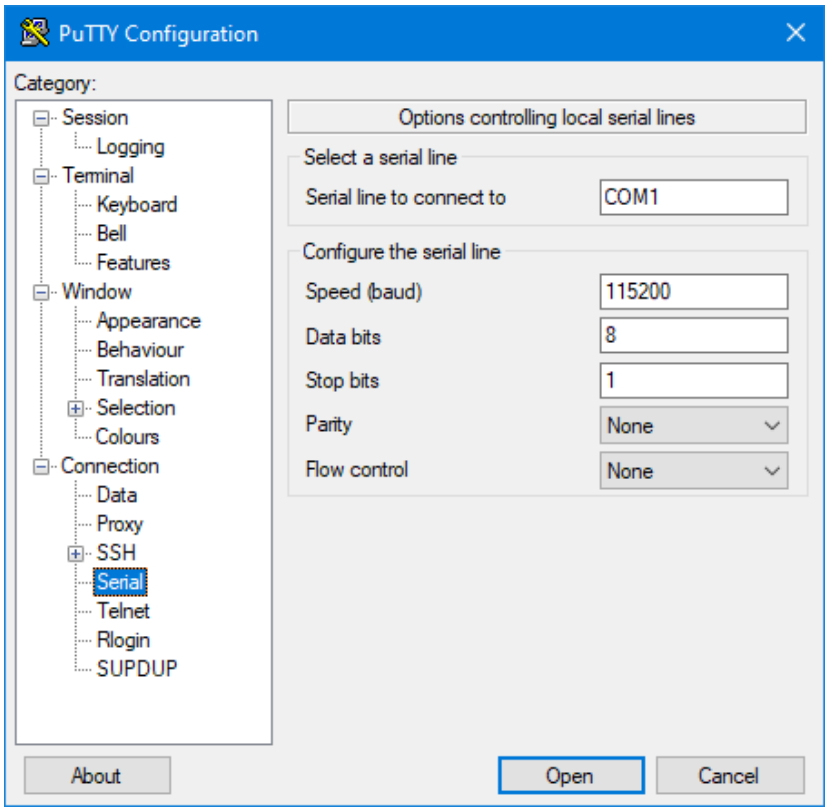


Рис. 3. Выбор порта для соединения

- Настройка свойств COM порта: 115200 для бит в секунду, 8 для бит данных, None для четности, 1 для стоповых битов и none для управления потоком.

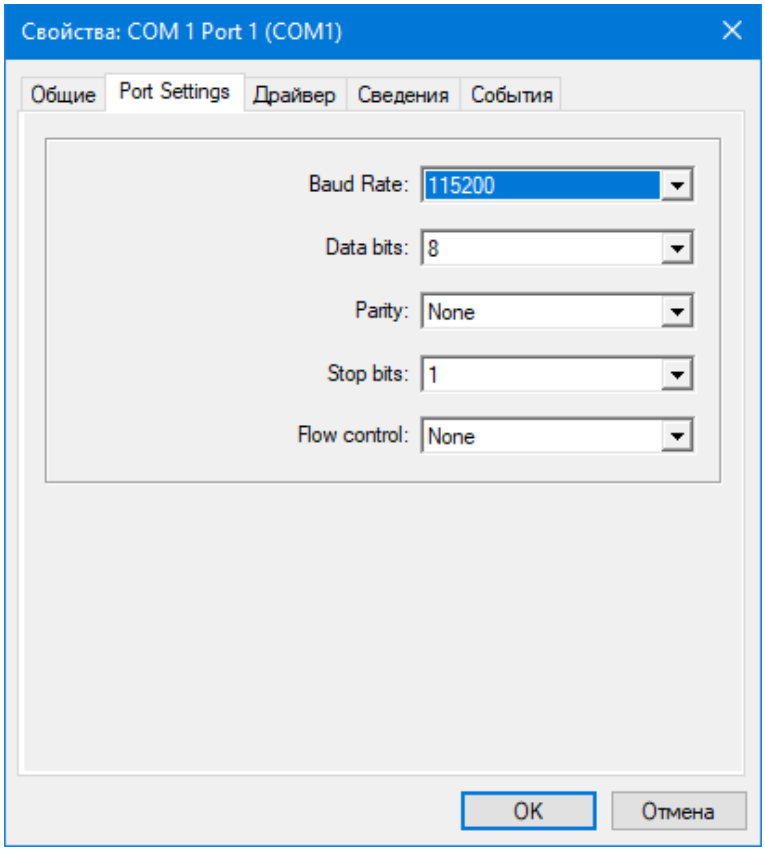


Рис. 4. Выбор параметров порта

- Появится окно входа в систему. Введите имя пользователя и пароль (пароль такой же, как и для Web браузера), затем нажмите enter.

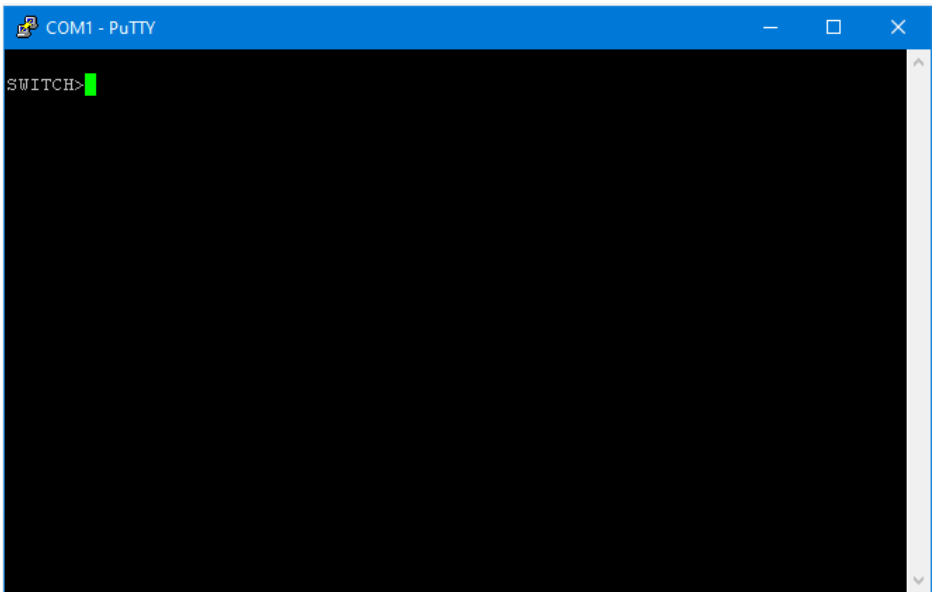


Рис. 5. CLI

- Введите команду “enable”, пользователь по умолчанию “admin” и пароль “STEZ” для доступа в привилегированный режим.

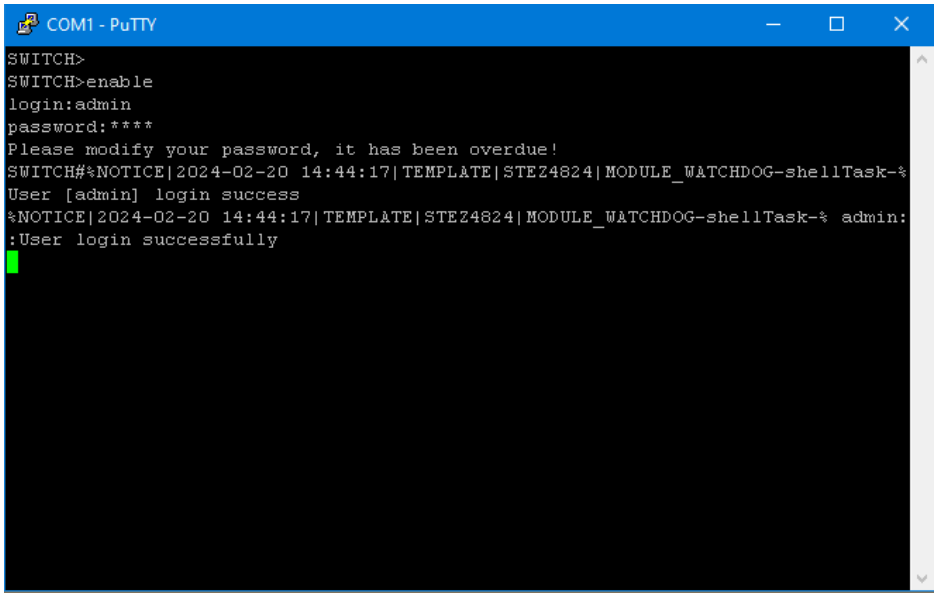


Рис. 6. Привилегированный режим

2.3. Управление коммутатором через Telnet

Пользователи могут использовать Telnet для настройки коммутаторов.

- Выбрать telnet, ввести *IP адрес коммутатора*, далее <Open>. По умолчанию адрес: 192.168.0.1.

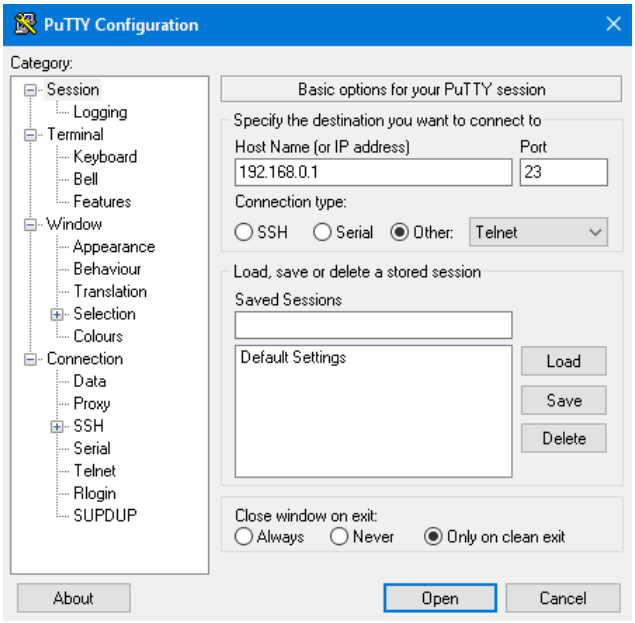


Рис. 7. Доступ через Telnet

- Появится окно входа в систему. Введите имя пользователя и пароль (“admin” / ”STEZ” по умолчанию), затем нажмите enter.

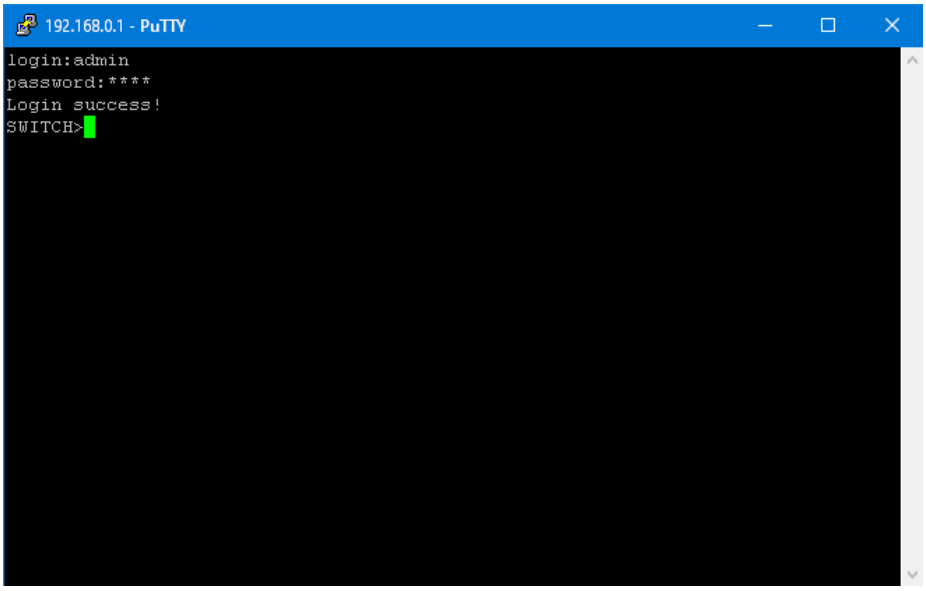


Рис. 8. Telnet интерфейс

2.4. Управление коммутатором через Web

- Запустите web-браузер
- Наберите http:// IP адрес коммутатора. Нажмите <Enter>
- Появится окно входа
- Введите имя пользователя и пароль. Имя пользователя и пароль по умолчанию – “admin” / “STEZ”
- Нажмите Enter или кнопку <OK>, затем появится главный интерфейс веб-управления
- При появлении запроса на смену пароля нажмите кнопку <OK>;
- Успешно войдите на веб-страницу управления коммутатором, дерево навигации по конфигурации находится слева.

Рекомендуется использовать браузер IE8.0 или выше, чтобы сделать интерфейс веб-управления более удобным.

3. Основная информация о коммутаторе

Основная информация о коммутаторе включает MAC-адрес, версию аппаратного обеспечения, версию программного обеспечения, версию BootROM, тип устройства, дату компиляции и время работы. Нажмите [Device Information] → [Switch Basic Information] в дереве навигации, чтобы отобразить основную информацию о коммутаторе, как показано на рис. 9.

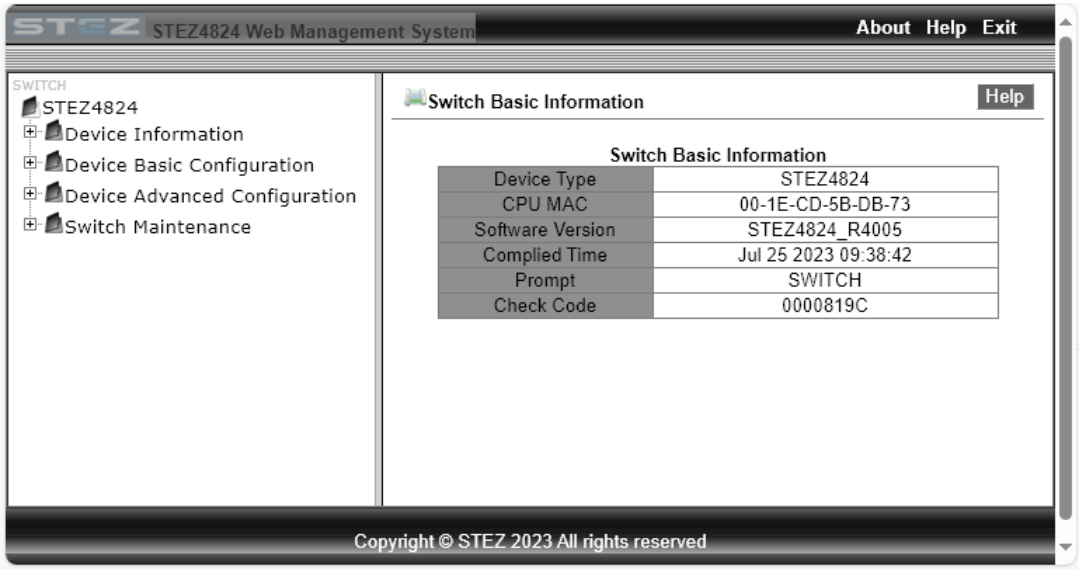


Рис. 9. Базовая информация о коммутаторе

4. Обслуживание коммутатора

В дереве навигации вы можете нажать [Save current running-config], чтобы сохранить текущую конфигурацию, или [Reboot With The Default Configuration], чтобы перейти на страницу, показанную на рис. 10. Затем вы можете нажать <Apply>, чтобы восстановить конфигурацию по умолчанию.

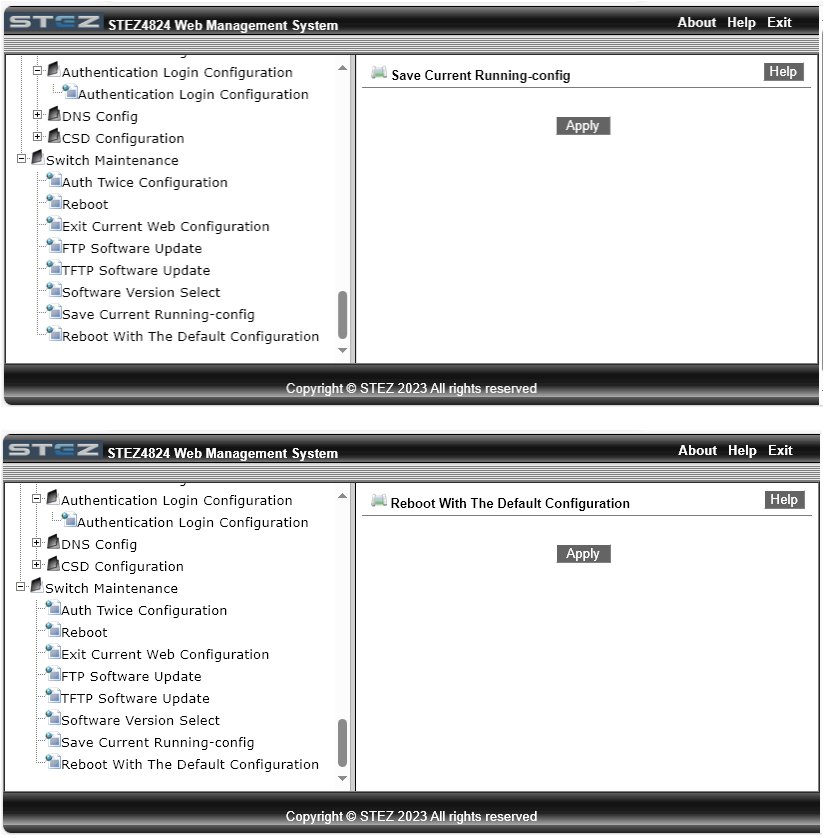


Рис. 10. Перезагрузка с конфигурацией по умолчанию

4.1. Перезагрузка

Чтобы перезагрузить устройство, нажмите [Switch maintenance] → [Reboot] в дереве навигации, чтобы войти в интерфейс перезагрузки, как показано на рис. 11.

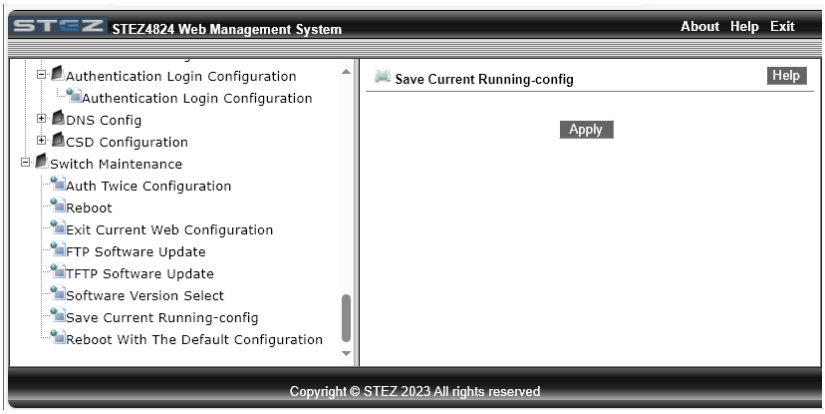


Рис. 11. Перезагрузка

Перед перезагрузкой подтвердите сохранение текущей конфигурации. Если вы выберете «Yes», коммутатор запустит текущую конфигурацию после перезагрузки. Если вы выберете «No», коммутатор использует предыдущую сохраненную конфигурацию. Если конфигурация не была сохранена, коммутатор восстановит конфигурацию по умолчанию после перезагрузки.

4.2. Обновление программного обсепечения (firmware)

Регулярные обновления программного обеспечения могут помочь уменьшить количество ошибок при работе коммутатора. Коммутаторам серии требуется обновить только один файл версии программного обеспечения. Он содержит не только версию системного программного обеспечения, но и версию программного обеспечения BootROM. Для обновления версии программного обеспечения требуется помощь сервера FTP / TFTP.

4.2.1. Обновление ПО через FTP

Установите FTP-сервер. Ниже в качестве примера используется программное обеспечение FileZilla_Server_1.8.1 для ознакомления с конфигурацией FTP-сервера и обновлением программного обеспечения.

Нажмите [Server] → [Configure]. Откроется диалоговое окно для настройки сервера. Нажмите <Add> для создания нового FTP пользователя, как показано на рис. 12. Создайте имя пользователя и пароль, для примера, имя пользователя "admin" и пароль "STEZ". Нажмите <Apply>.

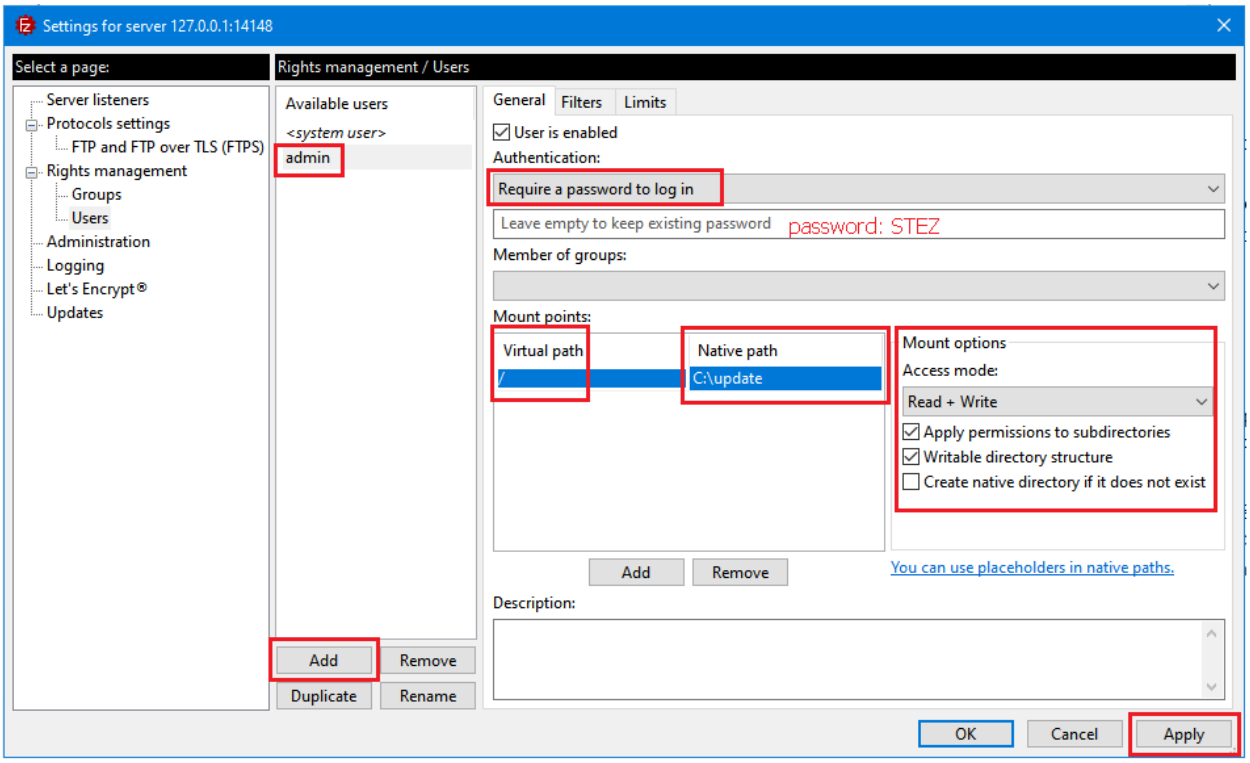


Рис. 12. Создание нового FTP пользователя

Введите путь хранения файла обновления, как показано на рис. 13. Нажмите <Apply>.

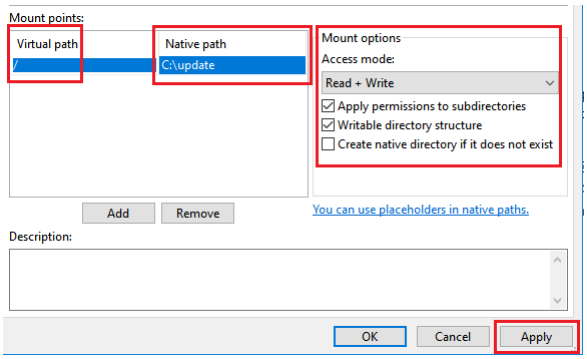


Рис. 13. Путь к файлу

Нажмите [Switch maintenance] → [FTP software update] в навигационном дереве для показа окна обновления ПО через FTP, как показано на рис. 14. Введите IP-адрес FTP сервера, имя FTP пользователя, пароль и имя файла на сервере. Нажмите <Update>.

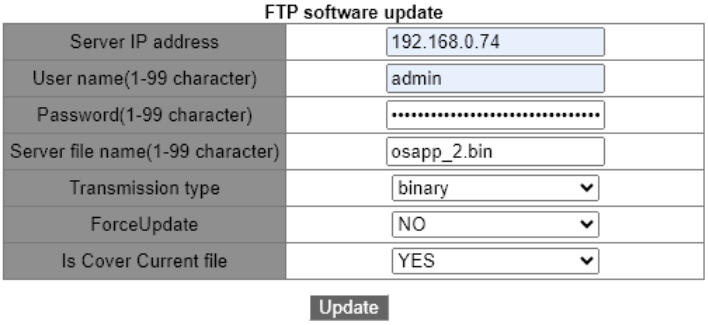


Рис. 14. Обновление ПО через FTP

- **Transmission type**
  Значения: binary / ascii
  По умолчанию: binary
  Функция: выбор стандарта передачи файлов.
  Описание: **ascii** означает использование стандарта ASCII для передачи файла; **binary** означает использование двоичного стандарта для передачи файла.
- **ForceUpdate**
  Значения: YES/NO
  По умолчанию: NO
  Функция: выберите метод обработки, если версия программного обеспечения не соответствует аппаратному обеспечению коммутатора.
  Описание: NO означает отмену обновления программного обеспечения, если программное и аппаратное обеспечение не совпадают. YES означает продолжение обновления программного обеспечения, даже если программное и аппаратное обеспечение не совпадают. Однако это может привести к системной аномалии или даже сбою загрузки.
- **Is Cover Current file**
  Параметры конфигурации: не перезаписывать текущую версию / перезаписывать текущую версию
  Конфигурация по умолчанию: перезаписать текущую версию
  Функция: заменять ли текущую версию программного обеспечения обновляемой версией программного обеспечения. Если это не предусмотрено, версия программного обеспечения не будет обновлена, и во флэш-памяти будет сохранена только версия программного обеспечения, подлежащая обновлению.

Имя файла должно иметь суффикс, иначе обновление не будет выполнено;
Файл версии программного обеспечения является нетекстовым файлом, и для передачи файла следует использовать двоичный стандарт;
Для обеспечения нормальной работы коммутатора выберите No Mandatory для параметра обязательного состояния, то есть отмените обновление программного обеспечения, если версия программного обеспечения не соответствует версии аппаратного обеспечения.

Убедитесь в нормальной связи между FTP-сервером и коммутатором, как показано на рис. 15.

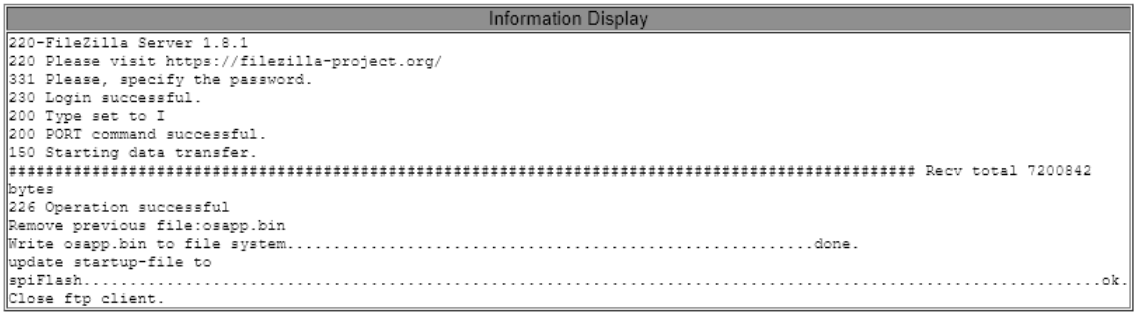


Рис. 15. Взаимодействие между коммутатором и FTP сервером

Дождитесь окончания обновления, как показано на рис. 16.

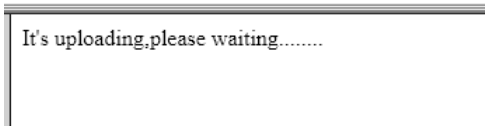


Рис. 16. Процесс обновления

Когда обновление будет завершено, перезагрузите устройство и откройте страницу основной информации о коммутаторе, чтобы проверить, успешно ли выполнено обновление и активна ли новая версия.

В процессе обновления программного обеспечения программное обеспечение FTP-сервера должно продолжать работать;
После успешного обновления ПО необходимо перезагрузить устройство, чтобы новая версия ПО вступила в силу.

4.2.2. Обновление ПО через TFTP

Установите TFTP-сервер. На рис. 17 в качестве примера используется программное обеспечение TFTPD для ознакомления с конфигурацией сервера TFTP.

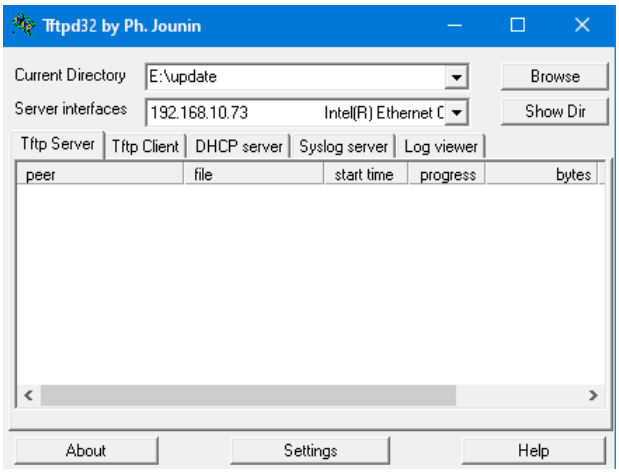


Рис. 17. Процесс обновления

В "Current Directory" выберите путь до обновляемого файла на сервере. Введите IP адрес сервера в "Server interface".

Нажмите [Switch maintenance] → [TFTP software update] в навигационном дереве, откроется окно обновления ПО через TFTP, как показано на рис. 18. Введите IP адрес TFTP сервера и имя файла на сервере. Нажмите <Update> и ожидайте окончания обновления.

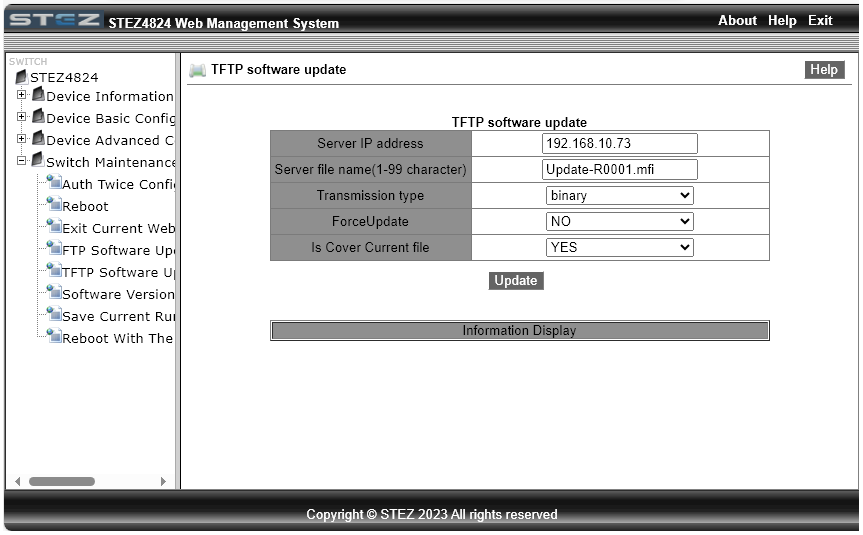


Рис. 18. Обновление ПО через TFTP

- **Transmission type**
  Значения: binary/ascii
  По умолчанию: binary
  Функция: выбор стандарта передачи файлов.
  Описание: **ascii** означает использование стандарта ASCII для передачи файла; **binary** означает использование двоичного стандарта для передачи файла.

- **ForceUpdate**
  Значения: YES/NO
  По умолчанию: NO
  Функция: выберите метод обработки, если версия программного обеспечения не соответствует аппаратному обеспечению коммутатора.
  Описание: NO означает отмену обновления программного обеспечения, если программное и аппаратное обеспечение не совпадают. YES означает продолжение обновления программного обеспечения, даже если программное и аппаратное обеспечение не совпадают. Однако это может привести к системной аномалии или даже сбою загрузки.

Имя файла должно иметь суффикс, иначе обновление не будет выполнено;
Файл версии программного обеспечения является нетекстовым файлом, и для передачи файла следует использовать двоичный стандарт;
Для обеспечения нормальной работы коммутатора выберите No Mandatory для параметра обязательного состояния, то есть отмените обновление программного обеспечения, если версия программного обеспечения не соответствует версии аппаратного обеспечения.

Убедитесь в нормальной связи между TFTP-сервером и коммутатором, как показано на рис. 19.

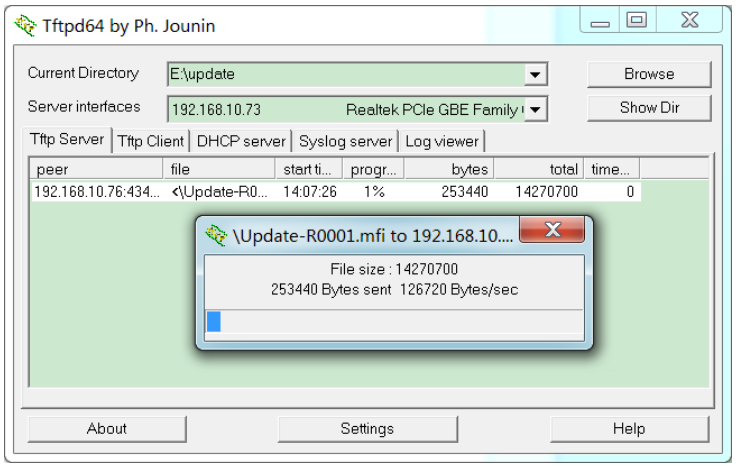


Рис. 19. Процесс обновления ПО через TFTP

Дождитесь окончания обновления.

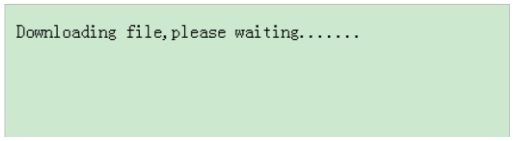


Рис. 20. Процесс обновления ПО через TFTP

Когда обновление будет завершено, перезагрузите устройство и откройте страницу основной информации о коммутаторе, чтобы проверить, успешно ли выполнено обновление и активна ли новая версия.

5. Базовая конфигурация коммутатора

5.1. Базовая конфигурация коммутатора

Базовая конфигурация коммутатора включает настройку имени хоста, отношения отображения между хостом и IP-адресом (mapping host), а также часов коммутатора.

5.1.1. Настройка имени хоста

Настройка имени хоста (hostname).

Нажмите [Device Basic Configuration] → [Switch Basic Configuration] → [Basic Config] для входа на страницу базовой конфигурации, как показано на рис. 21.

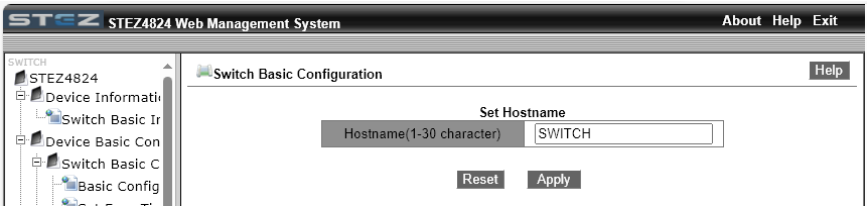


Рис. 21. Назначение имени коммутатора

- **Hostname**
  Диапазон: 1-30 символов
  По умолчанию: SWITCH
  Функция: Установите подсказку в интерфейсе командной строки коммутатора.
  Метод: Нажмите <Apply>, чтобы активировать новое имя хоста. Нажмите <Reset>, чтобы отменить текущую настройку и использовать предыдущее имя хоста.

Настройка сопоставления между именем хоста и IP-адресом, как показано на рис. 22.

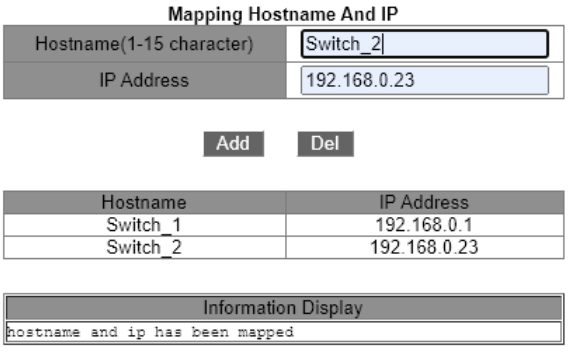


Рис. 22. Сопоставления между именем хоста и IP-адресом

- **{Host name, IP address}**
  Формат: {1–15 символов, A.B.C.D}
  Функция: в соответствии с сопоставлением используйте имя хоста для доступа к соответствующему устройству.
  Метод: введите правильное имя хоста и IP-адрес. Затем нажмите <Add>, чтобы установить запись сопоставления имени хоста и IP-адреса, или <Del>, чтобы удалить запись сопоставления.
  Пример. После успешной настройки сопоставления между именем хоста «Switch_2» и IP-адресом «192.168.0.23» вы можете пропинговать коммутатор с помощью команды ping host Switch_2 вместо ping 192.168.0.23.

5.1.2. Настройка часов

Вы можете установить системную дату и время. Коммутаторы этой серии поддерживают часы реального времени (RTC). Даже если они выключены, они продолжают синхронизироваться.

Чтобы в полной мере использовать время и экономить энергию, летом можно использовать летнее время (DST). Чтобы быть точным, переведите часы на один час вперед летом.

Нажмите [Device Basic Configuration] → [Switch Basic Configuration] → [Set Basic Clock], чтобы открыть страницу конфигурации часов, как показано на рис. 23.

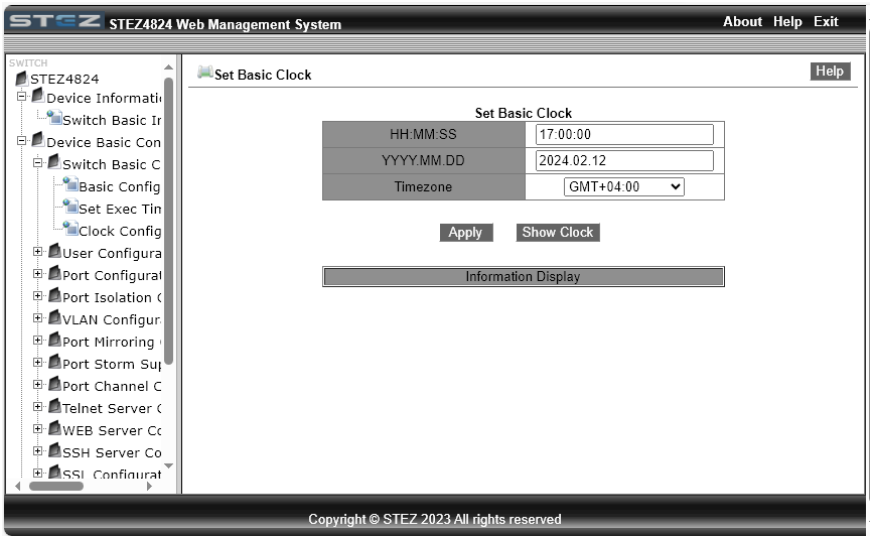


Рис. 23. Конфигурация часов

- **HH:MM:SS**
  Диапазон: значение HH находится в диапазоне от 0 до 23, а значение MM и SS — в диапазоне от 0 до 59.
- **YYYY.MM.DD.**
  Диапазон: значение YYYY находится в диапазоне от 1970 до 2099, значение MM — от 1 до 12, а значение DD — от 1 до 31.

Описание: Диапазон DD меняется в зависимости от месяца. Например, диапазон ДД для марта — от 1 до 31, а для апреля — от 1 до 30. Вы можете настроить его в соответствии с реальной ситуацией.

- **Timezone**
  Функция: выберите местный часовой пояс.

5.1.3. Управление конфигурациями пользователей

Чтобы избежать проблем с безопасностью, вызванных неавторизованным доступом пользователей к коммутатору, коммутаторы данной серии обеспечивают иерархическое управление пользователями. Коммутаторы обеспечивают различные права работы в зависимости от уровня пользователей, удовлетворяя разнообразные требования к управлению доступом. Доступны три уровня пользователя, как показано в таблице 2.

Таблица 2. Уровни пользователей

Уровень пользователя	Описание
Guest (Гость)	самый низкий уровень, пользователи “Гости” могут только просматривать конфигурацию коммутатора, но не могут выполнять настройку или модификацию. Пользователи “Guest” не могут получить доступ к следующим функциям: обновление программного обеспечения, управление пользователями, передача файлов, перезагрузка, сохранение текущей конфигурации и загрузка по умолчанию.
System (Системный уровень)	Средний уровень, пользователи “Системного уровня” имеют определенные права доступа и настройки. Пользователи “Системного уровня” не могут получить доступ к следующим функциям: обновление программного обеспечения, управление пользователями, передача файлов, перезагрузка и загрузка по умолчанию. Примечание. Пользователь “Системного уровня” может изменить пароль текущего пользователя.
Admin (Администратор)	Самый высокий уровень, пользователи с правами администратора имеют права на выполнение всех функций.
Audit (Пользователь Аудита)	Этот пользователь может только просматривать и настраивать журналы.

5.1.4. Веб конфигурирование

Конфигурирование пользователей.

Нажмите [Device Basic Configuration] → [User Configuration] → [User Configuration] для перехода на страницу конфигурирования, как показано ниже.

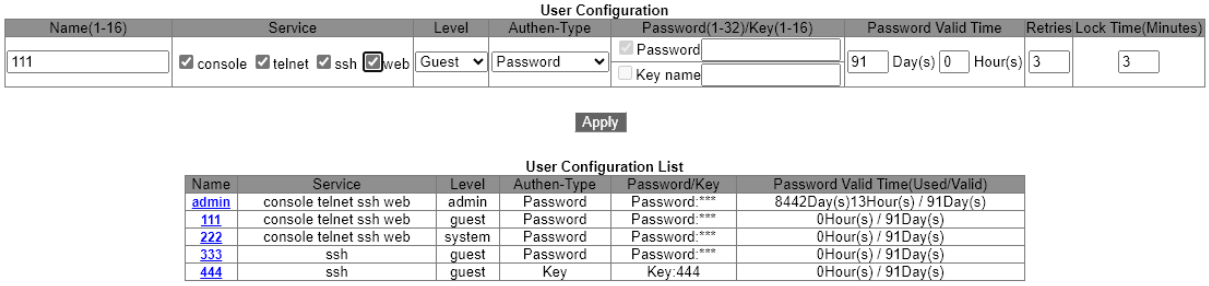


Рис. 24. Конфигурация пользователей

- **Name**
  Диапазон: 1~16 символов
- **Service**
  Опции: console/telnet/ssh/web
  Функция: выбор режима доступа переключения для текущего пользователя. Можно выбрать один или несколько режимов доступа.
- **Level**
  Опция: Guest/System/Admin
  По умолчанию: Guest
  Опция: Выберите уровень пользователя, пользователи разных уровней имеют разные права на операции.
- **Authen-Type**
  Опция: Password/Key/Password или Key
  По умолчанию: Password
  Функция: выбран тип аутентификации, который будет использоваться при доступе текущего пользователя к коммутатору. При выборе пароля необходимо настроить параметр «**Password**». При выборе ключа необходимо настроить **Key name**.
- **Password**
  Диапазон: 1~32 символа
  Функция: настройка пароля, который будет использоваться при доступе текущего пользователя к коммутатору.
- **Key name**
  Функция: выберите имя ключа, которое будет использоваться при доступе текущего пользователя к коммутатору в режиме ssh.
- **Password validity period**
  Диапазон по умолчанию: 91 день 0 часов
- **Repeat authentication times**
  Диапазон конфигурации: 1-10
  Конфигурация по умолчанию: 3

Функция: настройка количества последовательных неправильных вводов пароля при входе пользователя в систему, блокировка пользователя после достижения количества неправильных паролей, пользователю не разрешается входить в систему в течение времени блокировки после блокировки пользователя.

- **Authentication failure lockout time (minutes)**
  Конфигурация по умолчанию: 3
  Диапазон конфигурации: 1-5
  Функция: настроить время блокировки для сбоя аутентификации пользователя, и пользователю не разрешается входить в систему в течение времени блокировки.

console/telnet/web в настоящее время не поддерживает метод аутентификации по ключу, поэтому, если тип службы — console/telnet/web, не выбирайте ключ для типа аутентификации;
ssh поддерживает методы аутентификации по паролю и ключу;
Можно настроить до 9 пользователей;

Модификация и удаление пользователей.

Перейдите на запись пользователя в списке конфигурации пользователя. Вы можете изменить и удалить конфигурацию пользователя, как показано на рис. 25.

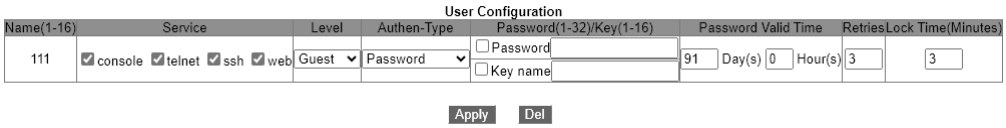


Рис. 25. Модификация и удаление информации пользователей

Изменение пароля у текущего пользователя.

Перейдите [Device Basic Configuration] → [User Configuration] → [Password] для входа на страницу с изменением пароля, как показано на рис. 26.

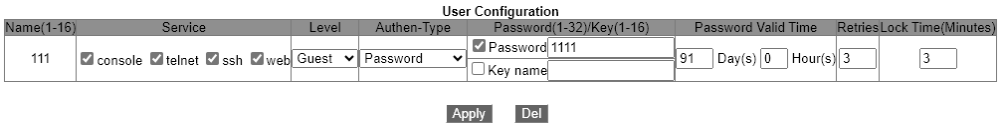


Рис. 26. Модификация пароля пользователя

- **Password**
  Диапазон: 1~32 символа

5.2. Конфигурация портов

5.2.1. Конфигурация физического порта

В конфигурации физического порта вы можете настроить тип подключения порта, состояние управления, скорость/режим и другую информацию.

Перейдите [Device Basic Configuration] → [Port configuration] → [Ethernet port configuration] → [Physical port configuration] для входа на страницу конфигурации, как показано на рисунке ниже.

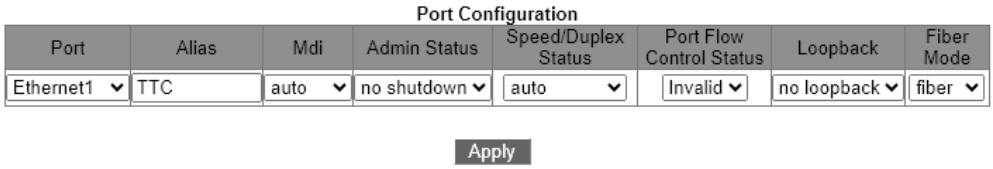


Рис. 27. Конфигурация порта

- **Port**
  Опции: все порты коммутатора
  Описание: Метки портов Ethernet (1, 2, 3...28).
- **Alias**
  Диапазон: 1~32 символа
  Функция: настроить псевдоним для описания порта.
- **mdi**
  Варианты: auto/normal/across
  По умолчанию: auto
  Функция: Настройка типа кабеля для порта Ethernet.
  Описание: auto означает автоматическое определение типа кабеля; cross означает, что порт поддерживает только перекрестный кабель; normal означает, что порт поддерживает только прямой кабель.

Пользователям рекомендуется использовать автоматическую идентификацию типов подключения.

- **Admin Status**
  Варианты: shutdown/no shutdown
  По умолчанию: no shutdown
  Функция: Разрешить передачу данных на порт или нет.
  Описание: no shutdown означает, что порт включен и разрешает передачу данных; shutdown указывает, что порт отключен и запрещает передачу данных. Эта опция напрямую влияет на аппаратное состояние порта и запускает аварийные сигналы порта.
- **Speed/duplex status**

Варианты: auto, 10M/половина, 10M/полный, 100M/половина, 100M/полный, 1000M/половина, 1000M/полный

По умолчанию: auto

Функция: настройка скорости порта и режима дуплекса.

Описание. Скорость порта и дуплексный режим поддерживают автосогласование и принудительную настройку. Если установлено значение «auto», скорость порта и режим дуплекса будут автоматически согласовываться в соответствии со статусом подключения порта. Когда режим дуплекса порта изменяется с автоматического согласования на принудительный полный дуплекс или полудуплекс, скорость порта также будет изменена на принудительный режим. Рекомендуется установить для параметра значение auto, чтобы избежать проблем с подключением, вызванных несогласованной конфигурацией портов на обоих концах канала. Если вы установили для порта принудительную скорость или дуплекс, убедитесь, что настройки скорости или режима дуплекса на обоих концах соединения одинаковы.

Вы можете просмотреть информацию о порте на основе конфигурации порта Ethernet и условий связи, как показано на рис. 28.

Port List

Port	Alias	Type	Mdi	Status	Admin Status	Speed	Mode	Flow Control	Loopback	Fiber Mode
Ethernet1	TTC	GE	auto	down	no shutdown	auto	auto	Invalid	no loopback	fiber
Ethernet2		GE	auto	up	no shutdown	auto	auto	Invalid	no loopback	fiber
Ethernet3		GE	auto	down	no shutdown	auto	auto	Invalid	no loopback	fiber
Ethernet4		GE	auto	down	no shutdown	auto	auto	Invalid	no loopback	fiber
Ethernet5		GE	auto	down	no shutdown	auto	auto	Invalid	no loopback	fiber
Ethernet6		GE	auto	down	no shutdown	auto	auto	Invalid	no loopback	fiber
Ethernet7		GE	auto	down	no shutdown	auto	auto	Invalid	no loopback	fiber
Ethernet8		GE	auto	down	no shutdown	auto	auto	Invalid	no loopback	fiber
Ethernet9		GE	auto	down	no shutdown	auto	auto	Invalid	no loopback	fiber
Ethernet10		GE	auto	down	no shutdown	auto	auto	Invalid	no loopback	fiber
Ethernet11		GE	auto	down	no shutdown	auto	auto	Invalid	no loopback	fiber
Ethernet12		GE	auto	down	no shutdown	auto	auto	Invalid	no loopback	fiber
Ethernet13		GE	auto	down	no shutdown	auto	auto	Invalid	no loopback	fiber
Ethernet14		GE	auto	down	no shutdown	auto	auto	Invalid	no loopback	fiber
Ethernet15		GE	auto	down	no shutdown	auto	auto	Invalid	no loopback	fiber
Ethernet16		GE	auto	down	no shutdown	auto	auto	Invalid	no loopback	fiber
Ethernet17		GE	auto	down	no shutdown	auto	auto	Invalid	no loopback	fiber
Ethernet18		GE	auto	down	no shutdown	auto	auto	Invalid	no loopback	fiber
Ethernet19		GE	auto	down	no shutdown	auto	auto	Invalid	no loopback	fiber
Ethernet20		GE	auto	down	no shutdown	auto	auto	Invalid	no loopback	fiber
Ethernet21		GE	auto	down	no shutdown	auto	auto	Invalid	no loopback	fiber
Ethernet22		GE	auto	down	no shutdown	auto	auto	Invalid	no loopback	fiber
Ethernet23		GE	auto	down	no shutdown	auto	auto	Invalid	no loopback	fiber
Ethernet24		GE	auto	down	no shutdown	auto	auto	Invalid	no loopback	fiber
Ethernet25		GX	auto	down	no shutdown	auto	auto	Invalid	no loopback	fiber
Ethernet26		GX	auto	down	no shutdown	auto	auto	Invalid	no loopback	fiber
Ethernet27		GX	auto	down	no shutdown	auto	auto	Invalid	no loopback	fiber
Ethernet28		GX	auto	down	no shutdown	auto	auto	Invalid	no loopback	fiber

Рис. 28. Информация о портах

5.2.2. Конфигурация ограничения полосы пропускания

Контролирует скорость исходящего или входящего информационного потока порта.

Перейдите [Device Basic Configuration] → [Port configuration] → [Ethernet port configuration] → [Bandwidth Control], чтобы войти в интерфейс конфигурации информации о физическом порте, как показано на рисунке ниже.

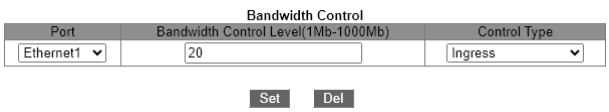


Рис. 29. Конфигурация ограничения полосы пропускания

- **Port**
  Варианты конфигурации: все порты на коммутаторе
  Описание: используйте одномерные порты (1, 2, 3...28) для представления меток портов.
- **Bandwidth Control**
  Уровень управления пропускной способностью
  Диапазон конфигурации: 1Mb-1000Mb
- **Control Type**
  Варианты конфигурации: Ingress/Egress/ Egress and Ingress
  Конфигурация по умолчанию: Ingress
  Функция: Ingress - ограничение входящего потока; Egress - ограничение исходящено потока; Egress and Ingress – ограничение входящего и исходящего потоков.

  В соответствии с конфигурацией порта и состоянием связи вся информация о порте отображается в «Списке портов», как показано на рисунке ниже.

Port List

Port	Ingress Bandwidth Threshold(Mb)	Outgress Bandwidth Threshold(Mb)
Ethernet1	20	No Limit
Ethernet2	No Limit	No Limit
Ethernet3	No Limit	No Limit
Ethernet4	No Limit	No Limit
Ethernet5	No Limit	No Limit
Ethernet6	No Limit	No Limit
Ethernet7	No Limit	No Limit
Ethernet8	No Limit	No Limit
Ethernet9	No Limit	No Limit
Ethernet10	No Limit	No Limit
Ethernet11	No Limit	No Limit
Ethernet12	No Limit	No Limit
Ethernet13	No Limit	No Limit
Ethernet14	No Limit	No Limit
Ethernet15	No Limit	No Limit
Ethernet16	No Limit	No Limit
Ethernet17	No Limit	No Limit
Ethernet18	No Limit	No Limit
Ethernet19	No Limit	No Limit
Ethernet20	No Limit	No Limit
Ethernet21	No Limit	No Limit
Ethernet22	No Limit	No Limit
Ethernet23	No Limit	No Limit
Ethernet24	No Limit	No Limit
Ethernet25	No Limit	No Limit
Ethernet26	No Limit	No Limit
Ethernet27	No Limit	No Limit
Ethernet28	No Limit	No Limit

Рис. 30. Состояние ограничения полосы пропускания

5.2.3. Конфигурация привязки портов

Перейдите [Device Basic Configuration] → [Port configuration] → [Ethernet port configuration] → [PortBind Configuration], чтобы войти в интерфейс конфигурации информации о физическом порте, как показано на рисунке ниже.

PortBind Configuration

Port	Ethernet1
IP Address	0.0.0.0
Mac Address	00-00-00-00-00-01
Operation Type	Add

Reset Apply

Рис. 31. Конфигурация привязки портов

- **Port**
  Варианты конфигурации: все порты на коммутаторе

Описание: используйте одномерные порты (1, 2, 3...28) для представления меток портов.

- **IP address**
  Формат конфигурации: A.B.C.D.
  Функция: Настройте IP-адрес, привязанный к порту, и установите отношение сопоставления между номером порта и IP-адресом.
- **MAC-address**
  Формат конфигурации: HH-HH-HH-HH-HH-HH (H — шестнадцатеричное число).
  Функция: настроить одноадресный MAC-адрес, младший бит старшего байта равен 0, и установить отношение отображения между конкретным MAC-адресом, номером порта и IP-адресом.
- **Operation Type**
  Параметры конфигурации: add /del
  Конфигурация по умолчанию: add
  Функция: выбор операции для текущей записи. Add – добавить запись; del – удалить запись.

5.2.4. Просмотр информации по порту.

Перейдите [Device Basic Configuration] → [Port configuration] → [Port debug and maintenance] → [Show port information] для перехода на страницу информации. Она содержит информацию о состоянии подключения порта, тип порта, статистику входящих/исходящих пакетов и другую информацию, как показано на рисунке ниже.

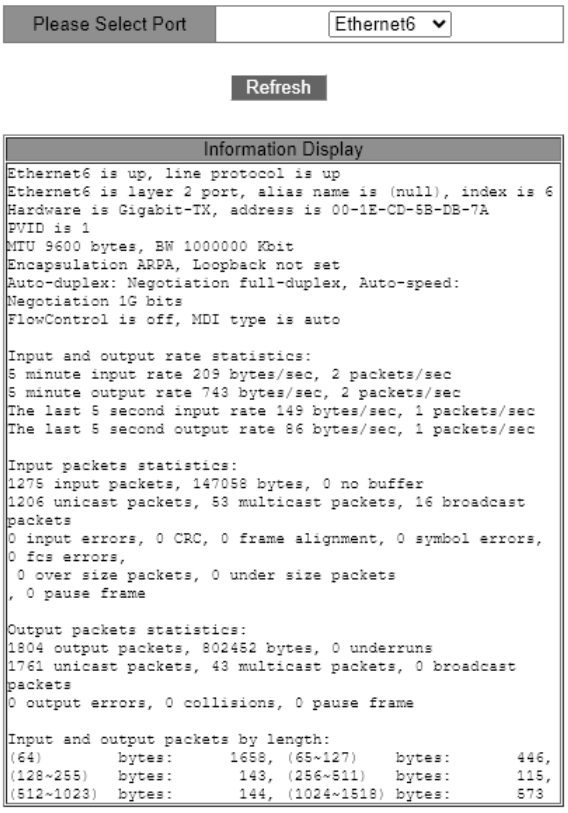


Рис. 32. Просмотр информации по порту

5.3. VLAN

Одна локальная сеть может быть разделена на несколько логических виртуальных локальных сетей (VLAN - Virtual Local Area Network). Устройство может обмениваться данными только с устройствами в той же VLAN. В результате широковещательные пакеты ограничиваются VLAN, что оптимизирует безопасность LAN. Раздел VLAN не ограничен физическим расположением. Каждая VLAN рассматривается как логическая сеть. Если хосту в одной VLAN необходимо отправить пакеты данных на хост в другой VLAN, должен быть задействован маршрутизатор или устройство уровня 3.

Чтобы сетевые устройства могли различать разные пакеты VLAN, необходимо добавить поле для идентификации VLAN в пакетах. В настоящее время наиболее распространенным протоколом для идентификации VLAN является протокол IEEE802.1Q. Структура кадра 802.1Q показана в таблице ниже.

Таблица 3. Структура кадра 802.1Q

<table>
<tr><td rowspan="2">DA</td><td rowspan="2">SA</td><td colspan="4">Информация о заголовке 802.1Q</td><td rowspan="2">Length/type</td><td rowspan="2">Data</td><td rowspan="2">FCS</td></tr>
<tr><td>Type</td><td>PRI</td><td>CFI</td><td>VID</td></tr>
</table>

4-байтовая информация заголовка 802.1Q вставляется в традиционную структуру кадра данных Ethernet, чтобы указать тег VLAN кадра:

Тип: 16 бит, указывающий, что этот кадр данных является данными с тегом VLAN, и значение равно 0x8100;

PRI: 3 бита, обозначающие приоритет сообщения 802.1p;

CFI: 1 бит, значение 0 указывает на Ethernet, значение 1 указывает на Token Ring;

VID: 12 бит, номер VLAN, диапазон значений 1~4093, 0, 4094, 4095 зарезервированы для протокола.

VLAN 1 является VLAN системы по умолчанию, и пользователи не могут создавать и удалять ее вручную;
Зарезервированные VLAN — это VLAN, зарезервированные системой для определенных функций, и пользователи не могут создавать или удалять их вручную.

Пакет с информацией заголовка 802.1Q является тегированным (Tag) пакетом, в противном случае он является нетегированным (Untag) пакетом, и все пакеты помечаются в коммутаторе 802.1Q.

5.3.1. Введение в VLAN на основе портов

Раздел VLAN может быть либо на основе порта, либо на основе MAC-адреса. Коммутаторы этой серии поддерживают разделение VLAN на основе портов. Члены VLAN могут быть определены на основе портов коммутатора. После добавления порта в указанную VLAN порт может пересылать пакеты с тегом для VLAN.

Тип порта

Порты делятся на два типа в зависимости от того, как они обрабатывают теги VLAN при пересылке пакетов.

- Untag port: пакеты, пересылаемые портом без тегов, не имеют тегов VLAN. Порты Untag обычно используются для подключения к терминалам, которые не поддерживают 802.1Q. По умолчанию все порты коммутатора являются портами без тегов и принадлежат VLAN1.
- Tag port: все пакеты, пересылаемые портом тега, содержат тег VLAN. Порты тегов обычно используются для подключения сетевых передающих устройств.

Режим порта

- Режим доступа (access): в режиме доступа порт должен быть добавлен в один VLAN с типом Untag и не может быть добавлены ни в один VLAN с типом Tag;
- Режим магистрали (trunk): в режиме магистрали порт добавляется в PVID VLAN с типом Untag; он добавляется к любой другой VLAN с типом Untag/Tag.

PVID

Каждый порт имеет PVID. При получении нетегированного пакета порт добавляет к пакету тег в соответствии с PVID. PVID по умолчанию для всех портов равен 1. PVID порта доступа — это идентификатор VLAN, к которой принадлежит порт, и его нельзя настроить. PVID магистрального порта может быть настроен как один из идентификаторов VLAN, разрешенных через порт. В таблице ниже показано, как коммутатор обрабатывает полученные и пересылаемые пакеты в зависимости от режима порта, типа порта и PVID.

Обработка полученных пакетов		**Обработка пакетов для пересылки**	
Untagged packets	**Tagged packets**	**Port Type**	**Packet Processing**
Добавить PVID tag к пакетам	➢ Если идентификатор VLAN в пакете есть в списке разрешенных VLAN, примите пакет. ➢ Если идентификатор VLAN в пакете находится в списке разрешенных VLAN, пакет отбрасывается.	Untag	Пересылать пакеты после удаления tag
		Tag	Сохранять tag и пересылать пакет

5.3.2. Веб конфигурирование

Создание и удаление VLAN

Перейти [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [Create/Remove VLAN] → [VID Allocation] для входа на страницу конфигурирования VLAN, как показано на рисунке ниже.

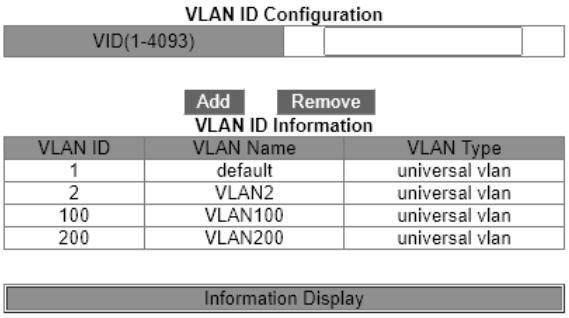


Рис. 33. Создание и удаление VLAN

- **VLAN ID**
  Диапазон: 2~4093.
  Функция: Используйте разные идентификаторы VLAN для различения VLANов.
  Описание: Коммутаторы этой серии поддерживают до 4094 VLAN.
  Метод: Нажмите <Add>, чтобы создать VLAN; нажмите <Remove>, чтобы удалить указанный VLAN.

Конфигурирование имени VLAN

Перейти [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [Create/Remove VLAN] → [VID Attribution Configuration] для входа на страницу конфигурирования имени VLAN, как показано на рисунке ниже.

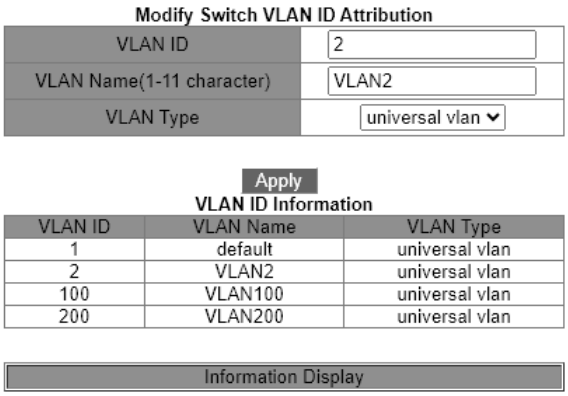


Рис. 34. Конфигурирование имени VLAN

- **VLAN ID**
  Диапазон: все созданные VLAN.
  Функция: введите идентификатор VLAN, имя которой необходимо изменить.

- **VLAN Name**
  Диапазон: 1~11 символов
  Функция: введите имя VLAN с указанным идентификатором.
- **VLAN Type**
  Опции: universal
  По умолчанию: universal

После завершения настройки на странице «Информация об идентификаторе VLAN» отображается информация об атрибутах всех созданных сетей VLAN, как показано на рисунке ниже:

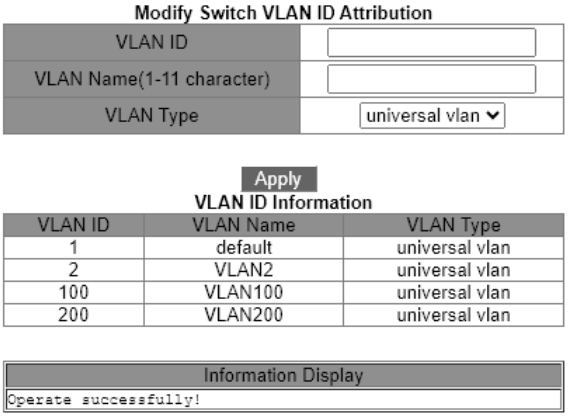
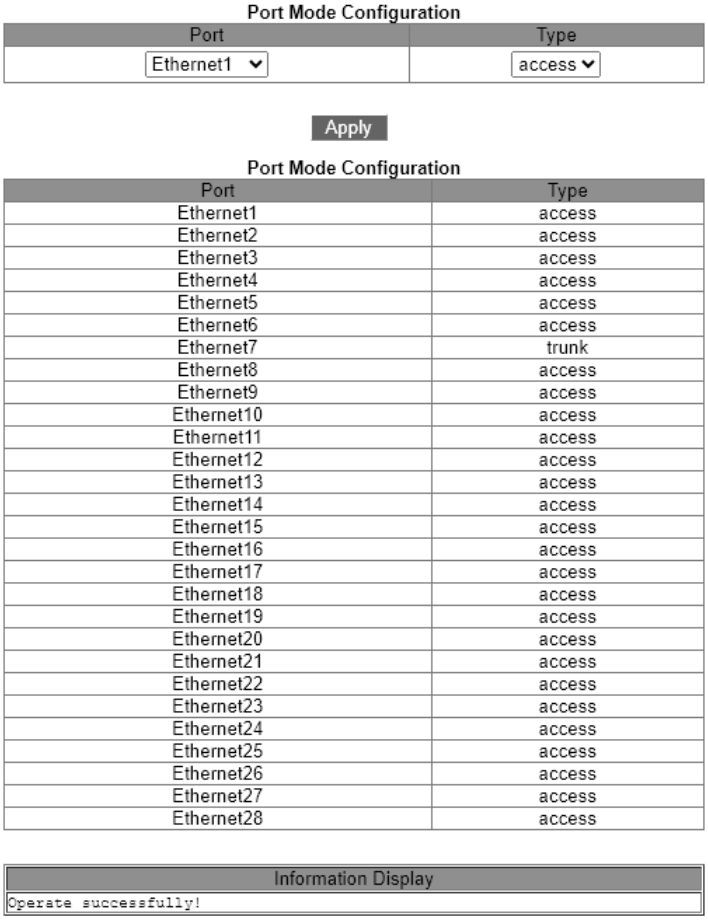


Рис. 35. Информация об идентификаторе VLAN

Конфигурирование режима порта

Перейти [Device Basic Configuration] → [VLAN configuration] → [Port type configuration] → [Set port mode (Trunk/Access)] для входа на страницу конфигурирования типа порта, как показано на странице ниже.



Port Mode Configuration

Port	Type
Ethernet1	access

Apply

Port Mode Configuration

Port	Type
Ethernet1	access
Ethernet2	access
Ethernet3	access
Ethernet4	access
Ethernet5	access
Ethernet6	access
Ethernet7	trunk
Ethernet8	access
Ethernet9	access
Ethernet10	access
Ethernet11	access
Ethernet12	access
Ethernet13	access
Ethernet14	access
Ethernet15	access
Ethernet16	access
Ethernet17	access
Ethernet18	access
Ethernet19	access
Ethernet20	access
Ethernet21	access
Ethernet22	access
Ethernet23	access
Ethernet24	access
Ethernet25	access
Ethernet26	access
Ethernet27	access
Ethernet28	access

Information Display
Operate successfully!

Рис. 36. Конфигурирование режима порта

- **Port**
  Опция: все порты коммутатора.
- **Type**
  Опция: access / trunk
  По умолчанию: access
  Функция: Выберите режим для указанного порта. Каждый порт поддерживает только один режим.

После завершения настройки на странице «Конфигурация режима порта» будут перечислены все типы портов, как показано на рисунке ниже.

Port Mode Configuration

Port	Type
Ethernet1	access

Apply

Port Mode Configuration

Port	Type
Ethernet1	access
Ethernet2	access
Ethernet3	access
Ethernet4	access
Ethernet5	access
Ethernet6	access
Ethernet7	trunk
Ethernet8	access
Ethernet9	access
Ethernet10	access
Ethernet11	access
Ethernet12	access
Ethernet13	access
Ethernet14	access
Ethernet15	access
Ethernet16	access
Ethernet17	access
Ethernet18	access
Ethernet19	access
Ethernet20	access
Ethernet21	access
Ethernet22	access
Ethernet23	access
Ethernet24	access
Ethernet25	access
Ethernet26	access
Ethernet27	access
Ethernet28	access

Information Display
Operate successfully!

Рис. 37. Конфигурация режима порта

Конфигурирование PVID для магистральный (trunk) портов

Перейти [Device Basic Configuration] → [VLAN configuration] → [Trunk Port Configuration]→ [VLAN Setting For Trunk Port] для входа на страницу конфигурирования trunk порта, как показано на странице ниже.

Set Trunk Native

Trunk Port	Ethernet12
Trunk Native VLAN(pvid)	

Рис. 38. Конфигурирование режима для Trunk порта

- **Trunk port**
  Опция: все trunk порты
- **Trunk Native VLAN (pvid)**
  Опция: все созданные VLANы
  По умолчанию: 1
  Функция: Конфигурирование PVID для trunk порта.
  Описание: Независимо от того, существует ли порт в VLAN или существует в VLAN в виде Untag/tag, после указания PVID этот порт будет добавлен в VLAN в виде Untag.
  Метод: Нажмите <Restore Default>, чтобы восстановить PVID выбранного trunk порта на 1.

Конфигурирование VLAN разрешенных для trunk портов показано на рисунке ниже.

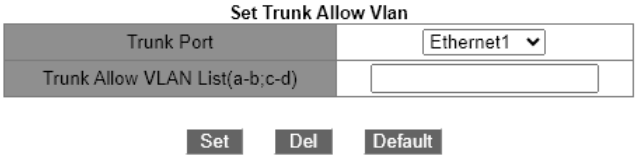


Рис. 39. Конфигурирование VLAN разрешенных для trunk портов

- **Trunk port**
  Опция: все trunk порты
- **Trunk Allow VLAN List**
  Опция: все созданные VLANы
  По умолчанию: все созданные VLANы
  Функция: Конфигурирование VLANов для выбора trunk порта.

После завершения настройки отображается информация о VLAN всех портов Trunk портов, как показано на рисунке ниже.

Trunk Port	Native Vlan	Allow Vlan List
Ethernet7	1	1 2 100 200

Рис. 40. Информация о VLAN всех портов Trunk портов

Назначение портов для созданных VLANов

Перейти [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [Allocate ports for VLAN] → [Allocate ports for VLAN] для входа на страницу конфигурирования портов для VLANов, как показано на рисунке ниже.

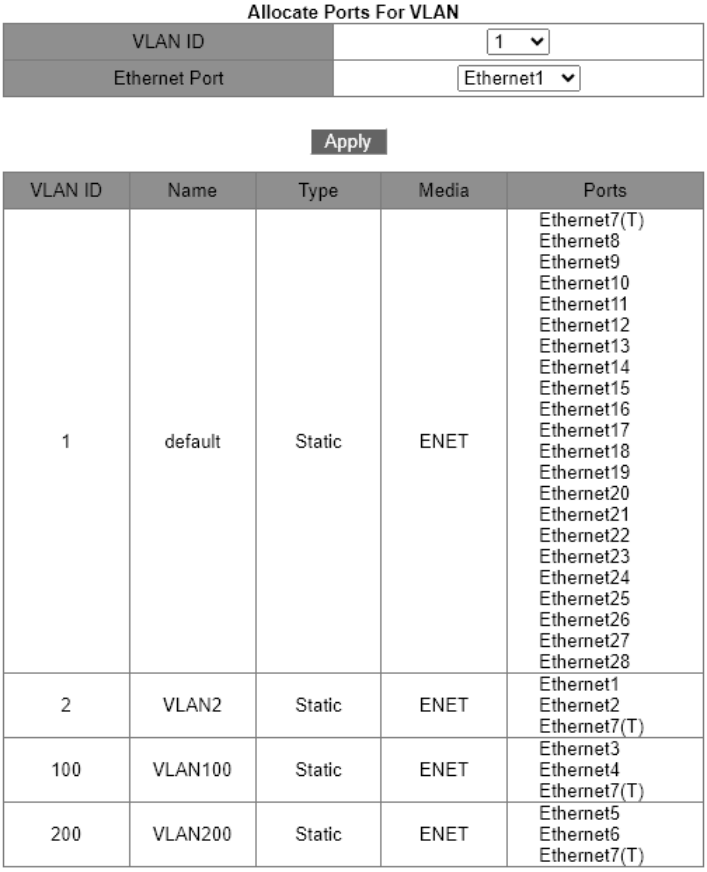


Рис. 41. Назначение портов для созданных VLAN

- **VLAN ID**
  Диапазон: все созданные VLAN.
  Функция: введите идентификатор VLAN, имя которой необходимо изменить.

Конфигурирование правила входа (ingress) VLAN порта.

Перейти [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [Enable/Disable VLAN ingress rule] → [Enable/Disable VLAN ingress rule] для входа на страницу конфигурации правила входа VLAN, как показано на рисунке ниже.

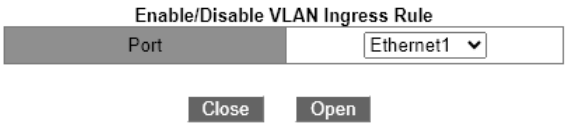


Рис. 42. Конфигурирование правила входа (ingress) VLAN порта

Опции: Enable / Disable
По умолчанию: Enable
Функция: Включить или отключить правило входа VLAN для порта.
Описание: если эта функция включена, порт сверяет идентификатор VLAN пакета с его разрешенным списком VLAN при получении пакета. Если совпадение найдено,

порт пересылает пакет; в противном случае пакет отбрасывается. Если эта функция отключена, порт пересылает все пакеты без проверки их идентификаторов VLAN. После завершения настройки отображается вся информация о правилах входа VLAN, как показано на рисунке ниже.

Port	Entrance Rule
Ethernet1	Open
Ethernet2	Open
Ethernet3	Open
Ethernet4	Open
Ethernet5	Open
Ethernet6	Open
Ethernet7	Open
Ethernet8	Open
Ethernet9	Close
Ethernet10	Open
Ethernet11	Open
Ethernet12	Open
Ethernet13	Open
Ethernet14	Open
Ethernet15	Open
Ethernet16	Open
Ethernet17	Open
Ethernet18	Open
Ethernet19	Open
Ethernet20	Open
Ethernet21	Open
Ethernet22	Open
Ethernet23	Open
Ethernet24	Close
Ethernet25	Open
Ethernet26	Open
Ethernet27	Open
Ethernet28	Open

Information Display

Рис. 43. Информация о правилах входа VLAN

Просмотр информации о всех созданных VLAN.

Перейти [Device Basic Configuration] → [VLAN configuration] → [Allocate Ports For VLAN] для входа на информационную страницу о VLANax, как показано на рисунке ниже.

Allocate Ports For VLAN

VLAN ID	1
Ethernet Port	Ethernet1

Apply

VLAN ID	Name	Type	Media	Ports
1	default	Static	ENET	Ethernet7(T) Ethernet8 Ethernet9 Ethernet10 Ethernet11 Ethernet12 Ethernet13 Ethernet14 Ethernet15 Ethernet16 Ethernet17 Ethernet18 Ethernet19 Ethernet20 Ethernet21 Ethernet22 Ethernet23 Ethernet24 Ethernet25 Ethernet26 Ethernet27 Ethernet28
2	VLAN2	Static	ENET	Ethernet1 Ethernet2 Ethernet7(T)
100	VLAN100	Static	ENET	Ethernet3 Ethernet4 Ethernet7(T)
200	VLAN200	Static	ENET	Ethernet5 Ethernet6 Ethernet7(T)

Рис. 44. Просмотр информации о всех созданных VLAN

5.3.3. Пример типовой конфигурации

Как показано на рисунке ниже, вся локальная сеть разделена на три VLAN: VLAN2, VLAN100 и VLAN200. Необходимо, чтобы устройства в одной VLAN могли взаимодействовать друг с другом, а разные VLAN были изолированы друг от друга. Терминальные ПК не распознают тегированные пакеты, поэтому настройте порты, соединяющие коммутаторы A и B с ПК, как порты доступа. Пакеты VLAN 2, VLAN 100 и VLAN 200 должны передаваться между коммутатором A и коммутатором B, поэтому настройте порт, подключенный к коммутатору A и коммутатору B, в качестве магистрального порта и разрешите прохождение VLAN 2, VLAN 100 и VLAN 200. Конкретная конфигурация показана в таблице 4.

Таблица 4. Типовая конфигурация

Элементы конфигурации	Описание конфигурации
VLAN2	Порты 1 и 2 коммутаторов A и B (типа Untag), порт 7 (типа Tag, PVID=1)
VLAN100	Порты 3 и 4 коммутаторов A и B (типа Untag), порт 7 (типа Tag, PVID=1)
VLAN200	Порты 5 и 6 коммутаторов A и B (типа Untag), порт 7 (типа Tag, PVID=1)

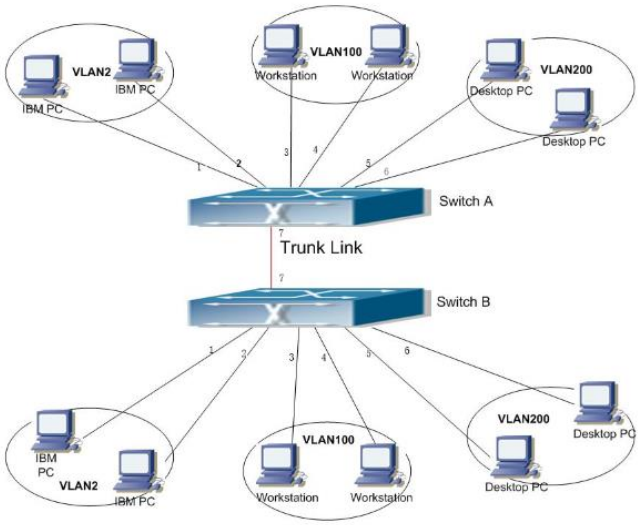


Рис. 45. Типовая конфигурация

Процесс настройки Switch A, B:

- Создайте VLAN2, VLAN 100 и VLAN 200, как показано на рис. 33;
- Настройте порты 1, 2, 3, 4, 5 и 6 как тип доступа, а порт 7 — как тип магистрали, как показано на рис. 36 и рис. 39;
- Настройте порты 1 и 2 для добавления в VLAN2 как Untag, порты 3 и 4 для добавления в VLAN100 как Untag, а порты 5 и 6 для добавления в VLAN200 как Untag. Порт 7 добавляется к VLAN2, VLAN100 и VLAN200 с типом Tag, как показано на рис. 41.

5.4. GVRP

5.4.1. Введение в GARP

GARP (Generic Attribute Registration Protocol, общий протокол регистрации атрибутов) используется для распространения, регистрации и отмены регистрации определенной информации (VLAN, групповой адрес и т. д.) между коммутаторами в одной сети. Приложения GARP делятся на GVRP и GMRP.

Через механизм GARP информация о конфигурации члена GARP будет быстро распространяться по всей коммутационной сети. Члены GARP уведомляют других членов GARP о необходимости зарегистрировать или отменить информацию об их собственных атрибутах посредством сообщений о присоединении/отмене, а также о регистрации или отмене информации об атрибутах друг друга в соответствии с сообщениями о присоединении/отмене других участников.

В GARP работают три типа сообщений: Join, Leave, LeaveAll.

Когда объект приложения GARP хочет, чтобы другие коммутаторы зарегистрировали некоторую атрибутивную информацию о себе, он отправляет наружу сообщение о присоединении. Сообщение Join делится на два типа: JoinEmpty и JoinIn. Отправка сообщения JoinIn используется для объявления атрибута, зарегистрированного сущностью приложения, отправка сообщения JoinEmpty используется для объявления атрибута, который не зарегистрирован сущностью приложения;

Когда объект приложения GARP хочет, чтобы другие коммутаторы аннулировали некоторую атрибутивную информацию о себе, он отправляет наружу сообщение Leave;

После того, как каждый объект приложения GARP запустится, он одновременно запустит таймер LeaveAll, и когда таймер истечет, объект приложения GARP отправит наружу сообщение LeaveAll.

Таймеры GARP включают в себя таймер Hold, таймер Join, таймер Leave и таймер LeaveAll:

Таймер Hold (удержания): когда объект приложения GARP получает определенную регистрационную информацию, он не сразу отправляет сообщение о присоединении во внешний мир, а запускает таймер удержания. Сообщения о присоединении рассылаются, поэтому уменьшение количества отправляемых сообщений способствует стабильности сети.

Таймер Join (присоединения): для того, чтобы гарантировать, что сообщение о присоединении может быть надежно передано другим объектам приложения, объект приложения GARP будет ждать интервал таймера присоединения после отправки первого сообщения о присоединении. сообщение.

Таймер Leave (выхода): когда объект приложения GARP хочет отменить определенную атрибутивную информацию, он отправляет сообщение «Выйти» наружу, и объект приложения GARP, получивший сообщение, запускает таймер «Выход». истекает, затем отмените регистрацию информации об атрибуте.

Таймер LeaveAll: после запуска каждого объекта приложения GARP одновременно запускается таймер LeaveAll. По истечении времени таймера объект приложения GARP отправит сообщение LeaveAll, чтобы другие объекты приложения GARP перерегистрировали всю атрибутивную информацию этого объекта. сущность. Затем снова запустите таймер LeaveAll, чтобы начать новый цикл.

5.4.2. Введение в GVRP

GVRP (протокол регистрации GARP VLAN, протокол регистрации GARP VLAN) — это приложение GARP, основанное на рабочем механизме GARP, которое поддерживает динамическую регистрационную информацию VLAN в устройстве и распространяет эту информацию на другие устройства.

После того как устройство запускает функцию GVRP, оно может получать регистрационную информацию VLAN от других устройств и динамически обновлять регистрационную информацию локальной VLAN. Кроме того, устройство может распространять регистрационную информацию локальной VLAN на другие устройства, чтобы сделать информацию VLAN всех устройств в одной и той же локальной сети. Регистрационная информация VLAN, распространяемая GVRP, включает в себя не только статическую регистрационную информацию, сконфигурированную вручную локально, но и динамическую регистрационную информацию от других устройств.

Порты GVRP и порты агрегации являются взаимоисключающими, то есть порты, поддерживающие GVRP, не должны добавляться в группу агрегации; порты, добавленные в группу агрегации, не должны включаться с помощью GVRP.

5.4.3. Веб конфигурирование

Глобальное включение протокола GVRP

Перейдите в дерево навигации [Device Basic Configuration] → [VLAN configuration] → [GVRP configuration] → [Enable Global GVRP], чтобы войти в интерфейс управления запуском глобальной конфигурации GVRP, как показано на рис. 46.

Рис. 46. Глобальное включение протокола GVRP

- **Включить/отключить глобальный GVRP**
  Варианты конфигурации: включить GVRP/отключить GVRP
  Функция: включение протокола GVRP.

Запуск GVRP на порту

Перейдите в дерево навигации [Device Basic Configuration] → [VLAN configuration] → [GVRP configuration] → [Enable Port GVRP], чтобы войти в интерфейс управления конфигурацией начального порта GVRP, как показано на рис. 47.

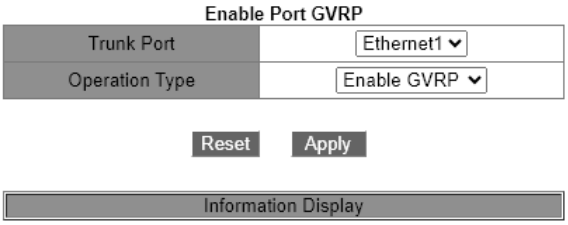


Рис. 47. Запуск GVRP на порту

- **Trunk**
  Конфигурация по умолчанию: Ethernet1
  Функция: настроить VLAN, разрешенный магистральным портом.
- **Operation Type**
  Варианты конфигурации: включить GVRP/отключить GVRP
  Функция: включение протокола GVRP на порту.

Конфигурация GVRP

Перейдите в дерево навигации [Device Basic Configuration] → [VLAN configuration] → [GVRP configuration] → [GVRP Configuration], чтобы войти в интерфейс управления конфигурацией GVRP, как показано на рис. 48.

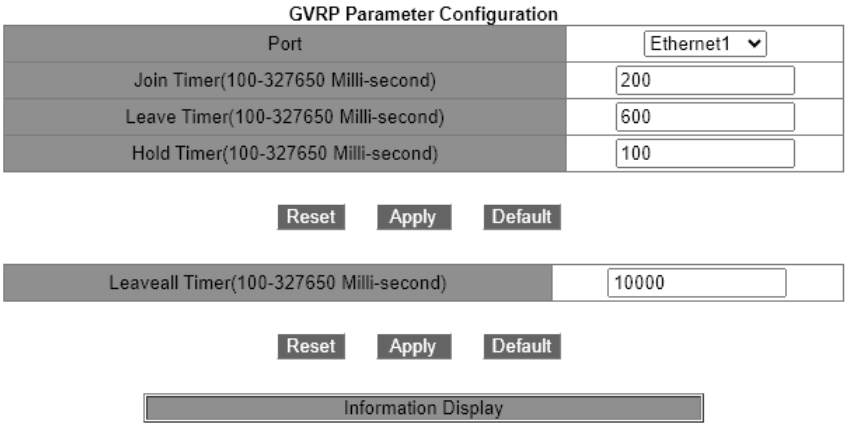


Рис. 48. Конфигурация GVRP

- **Join Timer**
  Диапазон конфигурации: 100-327650 (миллисекунд)
  Конфигурация по умолчанию: 200 (миллисекунд)
  Функция: настройка значения таймера присоединения.

- **Leave Timer**
  Диапазон конфигурации: 100-327650 (миллисекунд)
  Конфигурация по умолчанию: 600 (миллисекунд)
  Функция: Настройка значения таймера выхода.
- **Hold Timer**
  Диапазон конфигурации: 100-327650 (миллисекунд)
  Конфигурация по умолчанию: 100 (миллисекунд)
  Описание: Настройка значения таймера удержания.
- **Leaveall Timer**
  Диапазон конфигурации: 100-327650 (миллисекунд)
  Конфигурация по умолчанию: 1000 (миллисекунд)
  Функция: Настройка значения таймера «Выйти из всех».
  Описание: Если время действия таймеров Leaveall на разных устройствах истекает одновременно, одновременно будет отправлено несколько сообщений Leaveall, чтобы увеличить количество ненужных пакетов, чтобы предотвратить одновременное истечение времени ожидания таймеров Leaveall на разных устройствах фактическое текущее значение таймера «Выйти из всех» больше, чем значение таймера «Выйти из всех» — случайное значение, меньшее чем в 1,5 раза превышающее значение таймера «Выйти из всех».

Порт GVRP должен быть настроен как магистральный порт;
Порт GVRP распространяет атрибуты VLAN других портов GVRP в состоянии Up.

5.4.4. Пример типовой конфигурации

Как показано на рис. 49, для реализации динамической регистрации и обновления информации о VLAN между устройством A и устройством B на устройстве необходимо включить протокол GVRP.

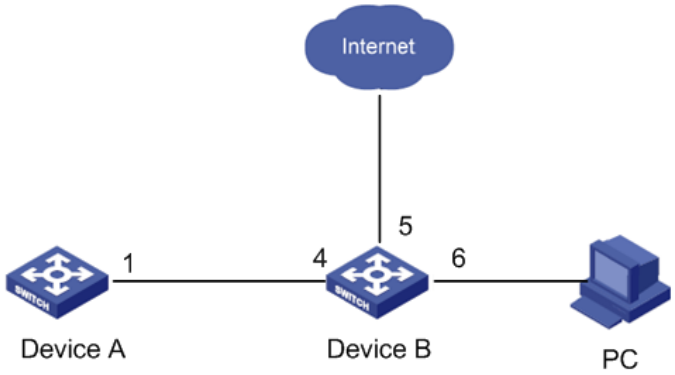


Рис. 49. Пример типовой конфигурации

Устройство A настроено следующим образом:

- Настройте порт 1 как режим Trunk;
- Глобально включить функцию GVRP, см. рис. 46;
- Включите функцию GVRP порта 1, см. рис. 47;

Устройство B настроено следующим образом:

- Настройте порт 4 в магистральном режиме, порт 6 в магистральном режиме и разрешенные для прохождения VLAN 1 и 6;
- Глобально включить функцию GVRP, см. рис. 46;
- Включите функцию GVRP портов 4, 5 и 6, см. рис. 47;

Порт 1 в коммутаторе A зарегистрирован в той же информации VLAN, что и порты 5 и 6 в коммутаторе B.

5.5. PVLAN конфигурация

5.5.1. Введение

PVLAN (private VLAN) использует двухуровневые технологии изоляции для реализации сложной функции изоляции трафика портов, обеспечения сетевой безопасности и изоляции широковещательного домена.

VLAN верхнего уровня — это VLAN с общим доменом, в которой порты являются восходящими портами. VLAN нижнего уровня — это VLAN изолированного домена, в которых порты являются портами нисходящей линии связи. Порты нисходящей линии связи могут быть назначены разным доменам изоляции, и они могут одновременно взаимодействовать с портом восходящей линии связи. Изолированные домены не могут взаимодействовать друг с другом.

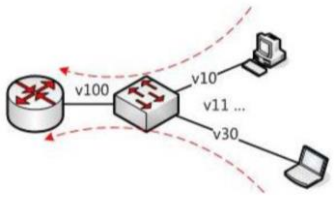


Рис. 50. PVLAN пример настройки

Как показано на рис. 50, общий домен — это VLAN100, а изолированные домены — это VLAN 10 и VLAN 30; устройства в изолированных доменах могут взаимодействовать с устройством в совместно используемом домене, например, VLAN 10 может взаимодействовать с VLAN 100; VLAN 30 также может взаимодействовать с VLAN 100, но устройства в разных изолированных доменах не могут взаимодействовать друг с другом, например, VLAN 10 не может взаимодействовать с VLAN 30.

Функцию PVLAN можно реализовать с помощью специальной конфигурации портов.

- PVID восходящих портов совпадает с общим идентификатором VLAN домена; PVID нисходящих портов совпадает с их собственным идентификатором VLAN домена изоляции.
- Для восходящих портов не используются теги, и они назначаются VLAN общего домена и всем изолированным доменам; для портов нисходящей линии связи не

используются теги, и они назначаются VLAN общего домена и собственному изолированному домену.

5.5.2. Пример типовой конфигурации

На рис. 51 показано PVLAN, VLAN300 — общий домен, порты 1 и 2 — восходящие порты, VLAN100 и VLAN200 — изолированные домены, а порты 3, 4, 5 и 6 — нисходящие порты.

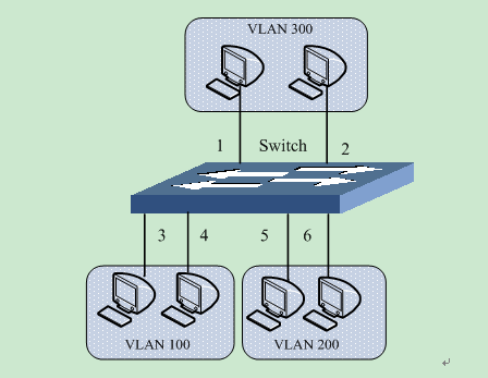


Рис. 51. Типовая конфигурация PVLAN

Конфигурация коммутатора:

- Создайте VLAN300, VLAN 100 и VLAN 200, как показано на рис. 33;
- Настройте порты 1, 2, 3, 4, 5 и 6 в режиме Trunk, как показано на рис. 36;
- Настройте порты 1~6 для добавления в VLAN300 как Untag, порты 1~4 для добавления в VLAN100 как Untag, порты 1, 2, 5 и 6 для добавления в VLAN200 как Untag, как показано на рис. 41;
- Настройте PVID портов 1 и 2 на 300, настройте PVID портов 3 и 4 на 100 и настройте PVID портов 5 и 6 на 200, как показано на рис. 38.

5.6. Зеркалирование

С функцией зеркального отображения портов коммутатор копирует все полученные или переданные кадры данных в одном порту (зеркальное отображение исходного порта) на другой порт (зеркальное отображение порта назначения). Порт назначения зеркалирования может быть подключен к анализатору протокола или монитору RMON для мониторинга сети, управления и диагностики неисправностей.

Коммутатор поддерживает только один порт назначения для зеркалирования, но несколько портов-источников. Несколько исходных портов могут находиться либо в одной VLAN, либо в разных VLAN. Порт источника и порт назначения зеркалирования могут находиться в одной и той же VLAN или в разных VLAN. Исходный порт и порт назначения не могут быть одним и тем же портом.

Порт назначения зеркалирования и port channel являются взаимоисключающими. Порт назначения зеркального отображения не может быть добавлен к port channel, и порт в port channel не может быть установлен в качестве порта назначения зеркального отображения.

5.6.1. Настройка через веб интерфейс

Выберите исходный порт зеркалирования и режим зеркалирования.

Перейти [Device Basic Configuration] → [Port mirroring configuration] → [Mirror configuration] для входа на страницу конфигурации порта источника зеркалирования, как показано на рисунке ниже.

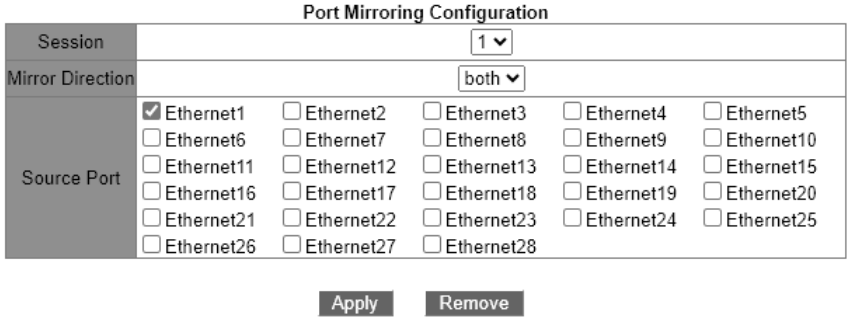


Рис. 52. Исходный порт зеркалирования и режим зеркалирования

- **Session**
  Опция: 1~7
  По умолчанию: 1
  Функция: Выберите группу зеркалирования.
- **Mirror Direction**
  Опция: rx/tx/both
  По умолчанию: rx
  Функция: Выберите данные для зеркального отображения в исходном порту зеркального отображения.
  Описание: rx указывает, что в исходном порту зеркалируются только полученные пакеты;
  tx указывает, что в исходном порту зеркалируются только передаваемые пакеты.
  both указывает, что и переданные, и полученные пакеты зеркально отражены в исходном порту.
- **Source port**
  Опции: все порты коммутатора
  Функция: Выберите исходный порт зеркалирования. Вы можете выбрать несколько исходных портов.

Выберите порт назначения зеркалирования, как показано на рисунке ниже.

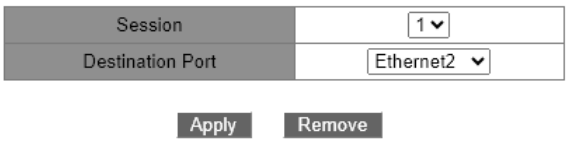


Рис. 53. Порт назначения для зеркалирования

- **Session**
  Опция: 1~7
  По умолчанию: 1
  Функция: Выбор группы зеркалирования
- **Destination port**
  Опция: все порты, кроме исходного порта.
  Функция: Выберите порт назначения зеркалирования.
  Описание: Установите порт в качестве порта назначения зеркалирования. Существует только один порт назначения зеркалирования. Порт назначения зеркального отображения не может быть членом канала порта. Лучше, чтобы пропускная способность порта назначения была больше или равна общей пропускной способности портов-источников.

5.6.2. Пример типовой конфигурации

Как показано на рис. 54, порт назначения зеркального отображения — 2, порт источника зеркального отображения — 1, а пакеты, полученные и отправленные портом 1, зеркалируются на порт 2.

Рис. 54. Пример конфигурации

Процесс настройки:

- Выберите порт 2 в качестве порта назначения зеркалирования, см. рис. 53;
- Выберите порт 1 в качестве исходного порта зеркалирования и выберите оба порта в качестве режима зеркалирования портов, как показано на рис. 52.

5.7. Port Storm Control

5.7.1. Введение

Port Storm Control предназначено для ограничения принимаемых портом широковещательных / многоадресных / неизвестных одноадресных пакетов. Когда скорость широковещательных / многоадресных / неизвестных одноадресных пакетов, полученных портом, превышает настроенный порог, система будет отбрасывать лишние широковещательные / многоадресные / неизвестные одноадресные пакеты, чтобы удерживать широковещательный / многоадресный / неизвестный одноадресный трафик в пределах допустимого диапазона, обеспечивая нормальную работу сети.

5.7.2. Настройка через веб интерфейс

Настройте пороговое значение port storm control.

Перейти [Device Basic Configuration] → [Port Storm Suppression configuration] → [Port Storm Suppression] для входа на страницу конфигурации, как показано на рисунке ниже.

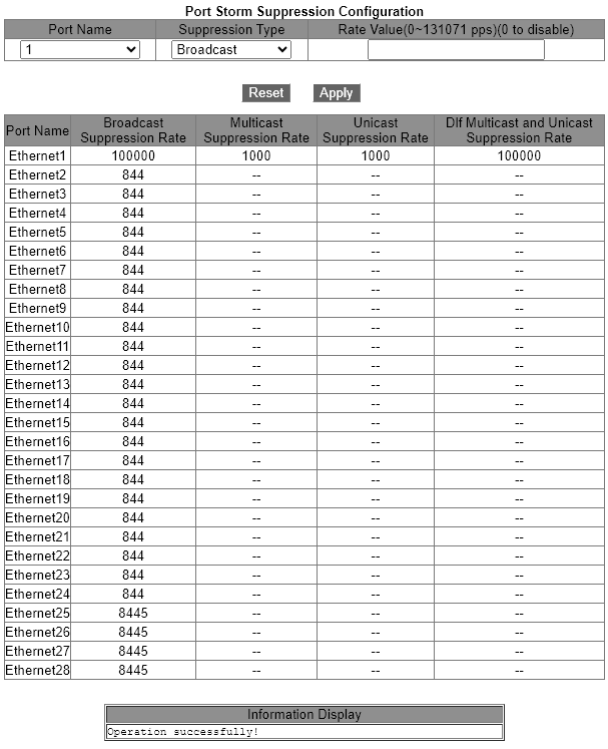


Рис. 55. Настройка port storm control

- **Port name**
  Опции: все порты, на которых включено port storm control

- **Suppression Type**
  Опции: Multicast / broadcast / dlf
  Функция: Выберите тип пакетов для управления.
- **Rate Value**
  Диапазон конфигурации: 1~ 131071 импульсов в секунду
  Конфигурация по умолчанию: 0, значение 0 означает, что подавление шторма отключено
  Функция: Настройте пороговое значение ограничения скорости порта, и пакетные данные, превышающие пороговое значение, будут потеряны.

Для каждого порта можно настроить только один порог. Порог влияет на настроенный тип пакета.

5.7.3. Пример типовой конфигурации

Включите подавление неизвестных многоадресных штормов на порту 1 и установите порог пропускной способности на 1000 пакетов в секунду.

Процесс настройки:

- Выберите порт 1, единица ограничения скорости: pps, значение скорости: 1000 pps, как показано на рис. 55;
- Выберите тип подавления: подавление многоадресных пакетов, как показано на рис. 55.

5.8. Изоляция портов (Port Isolation)

5.8.1. Введение

Чтобы реализовать изоляцию пакетов на уровне 2, вы можете добавить порты в разные VLAN. Однако этот метод приведет к пустой трате ограниченных ресурсов VLAN. Используя функцию изоляции портов, вы можете изолировать порты в одной и той же VLAN друг от друга. Пользователю нужно только добавить порт в группу изоляции, и будет реализована изоляция данных на уровне 2 среди портов группы изоляции, поскольку порты в группе изоляции не будут пересылать пакеты на другие порты группы изоляции. Функция изоляции портов предоставляет пользователям более безопасное и гибкое сетевое решение.

- *Порты группы изоляции могут быть только портами одного и того же коммутатора.*
- *Одно устройство поддерживает максимум 14 групп изоляции, и количество портов Ethernet в каждой группе не ограничено.*
- *После настройки группы изоляции только пакеты между портами группы изоляции не могли обмениваться друг с другом, связь между портами в группе изоляции и портами вне группы изоляции не пострадала бы.*

- *Изолированный порт и канал порта являются взаимоисключающими. Порт группы изоляции нельзя добавить в канал порта, а порт в канале порта нельзя добавить в группу изоляции.*

5.8.2. Настройка через веб интерфейс

Перейти [Device Basic Configuration] → [Port Isolate configuration] → [Port Isolation] для входа на страницу конфигурации, как показано на рисунке ниже.

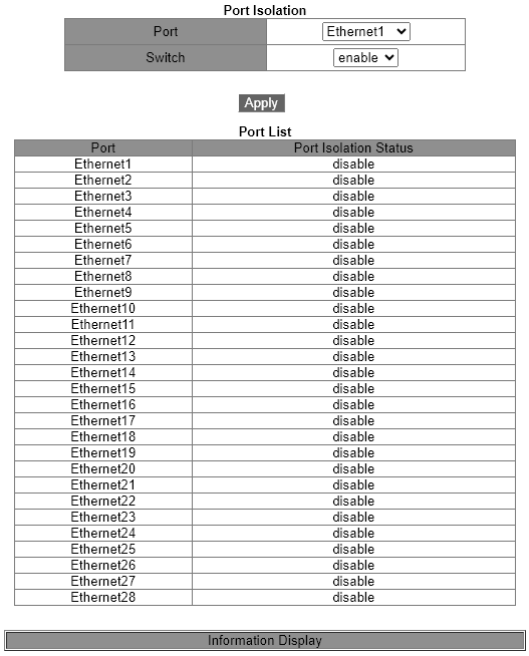


Рис. 56. Настройка изоляции портов

- **Port**
  Варианты конфигурации: все порты на коммутаторе
  Описание: используйте одномерные порты (1, 2, 3...28) для представления меток портов
- **Port Isolate**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: Включите или отключите изоляцию порта.

Один порт добавляется только в одну группу изоляции.

5.8.3. Пример типичной конфигурации

ПК1, ПК2 и ПК3 подключены к Ethernet-портам 1, 2 и 3 коммутатора, а порт 4 подключен к внешней сети. Все порты 1, 2, 3 и 4 находятся в сети VLAN 1. ПК1, ПК2 и ПК3 не могут взаимодействовать друг с другом, но все они могут получить доступ к внешней сети, как показано на рис. 57.

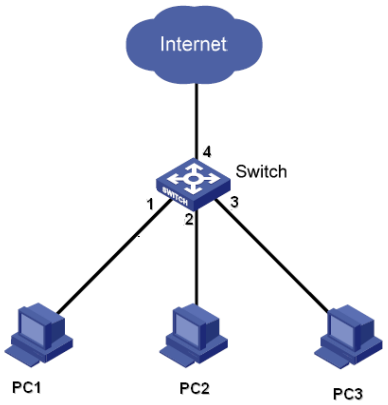


Рис. 57. Пример конфигурации

Добавьте порты 1, 2 и 3 в группу изоляции, как показано на рис. 56, чтобы обеспечить изоляцию между ПК1, ПК2 и ПК3.

5.9. Port Channel

5.9.1. Введение

Агрегация портов предназначена для привязки группы физических портов с одинаковой конфигурацией к логическому порту для увеличения пропускной способности и повышения скорости передачи. Порты-члены одной группы совместно используют трафик и служат друг для друга динамическими резервными копиями, повышая надежность соединения. Группа портов — это группа физических портов на уровне конфигурации. Только физические порты, входящие в группу портов, могут участвовать в агрегации каналов и становиться участниками канала портов. Когда физические порты в группе портов соответствуют определенным условиям, они могут выполнять агрегацию портов, формировать канал порта и становиться независимым логическим портом, тем самым увеличивая пропускную способность сети и обеспечивая резервирование канала.

5.9.2. Реализация

Как показано на рисунке ниже, три порта на коммутаторах A и B объединяются, образуя канал портов. Пропускная способность канала порта — это общая пропускная способность этих трех портов.

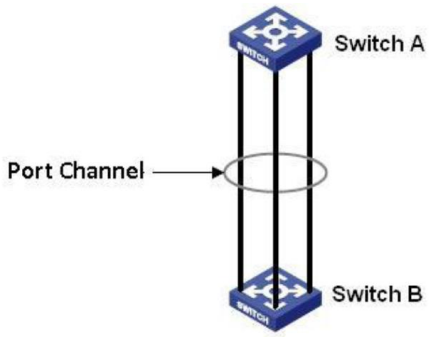


Рис. 58. Пример агрегации портов

Если коммутатор A отправляет пакеты коммутатору B через канал порта, коммутатор A определяет порт-участник для передачи трафика на основе результатов расчета распределения нагрузки. Когда один порт-член канала порта выходит из строя, трафик, передаваемый через порт, передается другому обычному порту на основе алгоритма распределения нагрузки.

Коммутаторы серии поддерживают не более 8 групп портов, и каждая группа содержит не более 8 портов-членов.

- *Порт можно добавить только в одну группу портов.*
- *Канал порта и изолированный порт являются взаимоисключающими. Порт в канале порта нельзя добавить в группу изоляции; порт группы изоляции не может быть добавлен к каналу порта.*
- *Канал порта и порт назначения зеркалирования являются взаимоисключающими. Порт в канале порта нельзя настроить как порт назначения зеркалирования; порт назначения зеркалирования не может быть добавлен к каналу порта.*

5.9.3. Настройка через веб интерфейс

Настроить режим распределения нагрузки канала порта.

Перейти [Device Basic Configuration] → [Port channel configuration] → [LACP Port Group Configuration] для входа на страницу конфигурации, как показано на рисунке ниже.

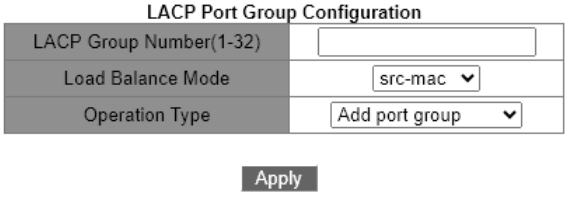


Рис. 59. Настройку группы портов для агрегации

- **Номер группы LACP (1-18)**
  Диапазон конфигурации: 1~18
  Функция: Настройка номера группы портов и поддержка до 18 групп агрегации.
- **Метод разделения трафика**
  Варианты конфигурации: src-mac/dst-mac/dst-src-ip/port
  Конфигурация по умолчанию: src-mac
  Функция: Настройка режима разделения трафика группы агрегации.
  Описание: src-mac выполняет распределение нагрузки на основе MAC-адреса источника, dst-mac выполняет распределение нагрузки на основе MAC-адреса назначения, dst-src-ip выполняет распределение нагрузки на основе результата исходного IP-адреса XOR IP-адреса назначения
- **Operation type**
  Опции: добавить группу портов/удалить группу портов
  По умолчанию: добавить группу портов
  Функция: создание или удаление группы портов.

После завершения настройки на странице «Таблица групп портов» перечислены все созданные группы портов и режимы распределения нагрузки, как показано на рисунке ниже.

port group table

port group	Load Balance
3	src-mac
2	src-mac
1	src-mac

Рис. 60. Таблица групп портов

Настройка члена группы портов

Перейти [Device Basic Configuration] → [Port channel configuration] → [LACP Port Configuration] для входа на страницу конфигурации, как показано на рисунке ниже.

LACP Port Configuration

LACP Group Number(1-32)	1
Port	Ethernet1
Port Mode	on
Operation Type	Add Port To Group

Apply

Рис. 61. Настройка члена группы портов

- **Номер группы LACP**
  Вариант конфигурации: номер созданной группы портов.
- **Port**
  Опции: все порты коммутатора
  Функция: Выберите порт, который необходимо добавить или удалить из группы портов.
  Описание: порты-участники одной и той же группы агрегации имеют одинаковые атрибуты портов, и в группу можно добавить не более 8 портов.

- **Operation type**
  Опции: Добавить порт в группу / Удалить порт из группы
  По умолчанию: добавить порт в группу
  Функция: добавить порт или удалить порт из группы портов.

5.9.4. Пример типовой конфигурации

Как показано на рис. 58, три порта (порт 1, 2 и 3) Switch A добавляются в группу портов 1, три порта (порт 1, 2 и 3) Switch B добавляются в группу портов 2;

Соответствующие порты выше с сетевыми кабелями формируется для разделения трафика между портами (при условии, что три порта агрегации коммутатора имеют одинаковые атрибуты).

Процесс настройки коммутатора:

- Добавьте группу портов 1 в Switch A, см. рис. 59;
- Выберите порты 1, 2 и 3, чтобы присоединиться к группе портов 1, как показано на рис. 61;
- Добавьте группу портов 2 в Switch B, см. рис. 59;
- Выберите порты 1, 2 и 3, чтобы присоединиться к группе портов 2, как показано на рис. 61.

5.10. Конфигурация Telnet Server

5.10.1. Введение

Telnet — это протокол для доступа к удаленным терминалам. Вы можете войти на удаленный хост, используя IP-адрес или имя хоста через Telnet. Telnet может передавать ваши команды на удаленный хост и возвращать вывод удаленного устройства на ваш дисплей через TCP.

Telnet работает в режиме клиент / сервер. Локальная система является клиентом, а удаленный хост — сервером. Коммутаторы этой серии могут служить в качестве сервера или клиента Telnet.

Когда коммутатор служит сервером Telnet, вы можете войти в коммутатор с помощью клиентского программного обеспечения Telnet в Windows или других операционных системах. Когда коммутатор служит сервером Telnet, он может устанавливать TCP-соединения максимум с 5 клиентами Telnet.

Когда коммутатор служит клиентом Telnet, вы можете использовать команды Telnet в общем виде для входа на другие удаленные хосты. При работе в качестве клиента Telnet коммутатор может устанавливать TCP-соединение только с одним удаленным хостом. Чтобы установить TCP-соединение с другим хостом, коммутатор должен сначала отключить подключенный хост.

5.10.2. Настройка через веб интерфейс

Перейти [Device Basic Configuration] → [Telnet server configuration] → [Telnet security IP] для входа на страницу конфигурации, как показано на рисунке ниже.

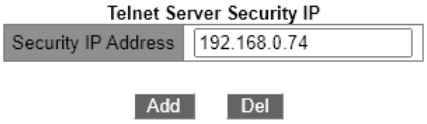


Рис. 62. Настройка Telnet Security IP

- **Security IP address**
  Формат: A.D.C.D
  Функция: Настройка безопасного IP-адрес для входа клиента Telnet, когда коммутатор работает как сервер Telnet.
  Описание: Если безопасный IP-адрес не установлен, ограничения на IP-адрес клиента Telnet отсутствуют.
  После установки безопасных IP-адресов только клиент с безопасным IP-адресом может войти в систему и настроить коммутатор с помощью Telnet.
  Коммутатор допускает до 32 безопасных IP-адресов. По умолчанию безопасный IP-адрес не настроен.
  После завершения настройки в «Списке IP-адресов безопасности сервера Telnet» отображаются IP-адреса клиентов Telnet, которые могут войти в коммутатор, как показано на рисунке ниже.

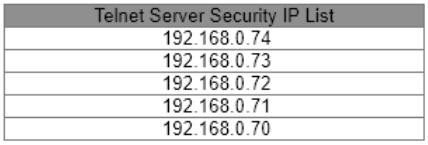


Рис. 63. Список IP-адресов безопасности сервера Telnet

5.11. Конфигурация SSH Server

5.11.1. Введение

SSH (Secure Shell) — это сетевой протокол для безопасного удаленного входа в систему. Он шифрует все передаваемые данные, чтобы предотвратить раскрытие информации. Когда данные шифруются SSH, пользователи могут использовать только командные строки для настройки коммутаторов. Коммутатор поддерживает функцию SSH-сервера и позволяет подключаться нескольким пользователям SSH, которые входят в коммутатор удаленно через SSH, но одновременно к коммутатору могут подключаться не более двух пользователей.

Незашифрованное сообщение называется открытым текстом, а зашифрованное сообщение называется зашифрованным текстом. Шифрование или дешифрование находится под контролем секретного ключа. Секретный ключ представляет собой определенную строку символов и является единственным параметром, управляющим

преобразованием между обычным текстом и зашифрованным текстом, работающим как ключ. Шифрование может превратить обычный текст в зашифрованный текст, а дешифрование может превратить зашифрованный текст в обычный текст. Аутентификация безопасности на основе ключей требует секретных ключей, и каждый конец связи имеет пару секретных ключей, закрытый ключ и открытый ключ. Открытый ключ используется для шифрования данных, а законный владелец закрытого ключа может использовать закрытый ключ для расшифровки даты, чтобы гарантировать безопасность данных.

Чтобы реализовать безопасное соединение SSH в процессе связи, сервер и клиент проходят следующие пять этапов: Стадия согласования версии: в настоящее время SSH состоит из двух версий: SSH1 и SSH2. Две стороны договариваются об используемой версии. Этап согласования ключа и алгоритма: SSH поддерживает несколько типов алгоритмов шифрования. Две стороны согласовывают алгоритм для использования. Состояние аутентификации: клиент SSH отправляет запрос на аутентификацию на сервер, и сервер аутентифицирует клиента. Этап запроса сеанса: клиент отправляет запрос сеанса на сервер после прохождения аутентификации. Стадия сеанса: клиент и сервер начинают общение после передачи запроса сеанса.

5.11.2. Настройка через веб интерфейс

Этапы настройки SSH-сервера.

Перейти [Device Basic Configuration] → [SSH Server Config] → [SSH Server Config] для входа на страницу конфигурации, как показано на рисунке ниже.

- Отключить статус SSH.
- Нажмите <Destroy>, чтобы уничтожить старую пару ключей, как показано на рисунке ниже.

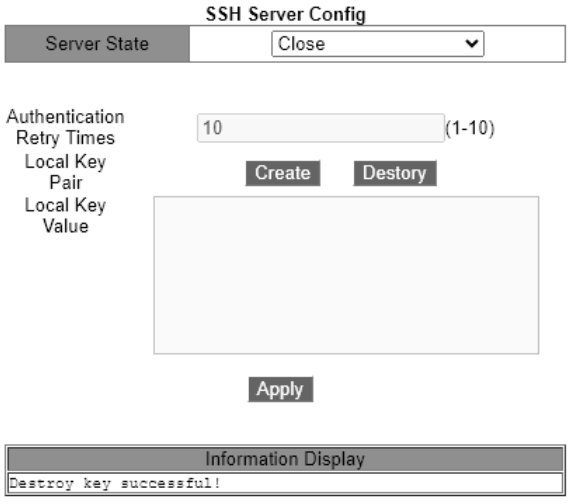


Рис. 64. Начальная настройка SSH сервера

- Нажмите <Create>, чтобы создать новую пару ключей.
- Включите протокол SSH и настройте сервер SSH, как показано на рис. 65.

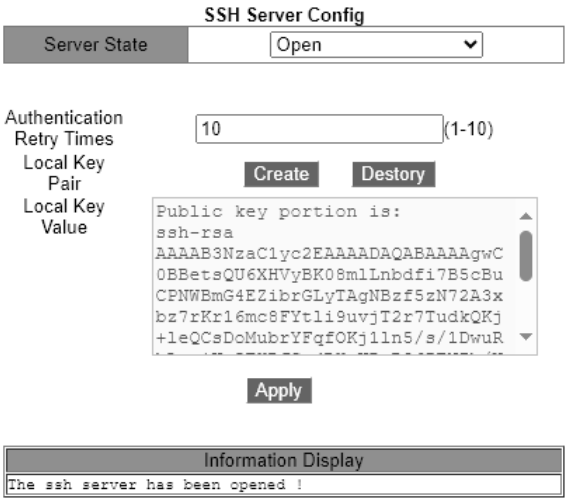


Рис. 65. Включение SSH сервера

- **Server state**
  Опции: open / close.
  По умолчанию: close
  Функция: включить/отключить протокол SSH. Если он включен, коммутатор работает как SSH-сервер.
- **Authentication Retry Times**
  Диапазон конфигурации: 1~10
  По умолчанию: 10
  Функция: установить количество попыток входа на сервер SSH.
- **Local Key Pair**
  Опции: Создать / Удалить
  Функция: создать или уничтожить локальную пару ключей SSH-сервера. Перед включением SSH-сервера создайте локальную пару ключей; уничтожьте старую пару ключей перед созданием новой пары ключей.
- **Local Key Value**
  Функция: показать значение локального ключа. Нажмите <Generate>, чтобы автоматически сгенерировать значение ключа.

5.12. SSL конфигурация

5.12.1. Введение

SSL (Secure Socket Layer) — это протокол безопасности, обеспечивающий безопасный канал для протокола прикладного уровня на основе TCP, такого как HTTPS. SSL шифрует сетевое соединение на транспортном уровне и использует алгоритм симметричного шифрования для обеспечения безопасности данных, а также использует код аутентификации с секретным ключом для обеспечения надежности информации. Этот протокол широко используется в веб-браузерах, для получения и отправки электронной почты, сетевого факса, связи в реальном времени и т. д., обеспечивая протокол шифрования для безопасной передачи в сети. Когда коммутатор включает SSL, пользователи должны использовать безопасную ссылку https, например, https://192.168.0.1, для доступа к коммутатору.

5.12.2. Настройка через веб интерфейс

Включение HTTPS протокола.

Перейти [Device Basic Configuration] → [SSL Configuration] → [SSL Configuration] для входа на страницу конфигурации, как показано на рисунке ниже.

Рис. 66. Настройка SSL

- **Server state**
  Опция: Enable / Disable
  По умолчанию: Disable
  Функция: включить или отключить протокол SSL.
  Объяснение: После включения SSL пользователи должны использовать безопасную ссылку https://ip-адрес для доступа к коммутатору.
- **Certificate/Private key**
  Функция: введите правильный сертификат и закрытый ключ, затем нажмите кнопку <Add>, чтобы импортировать их для переключения.

Сертификат по умолчанию и закрытый ключ, предоставленные компанией, уже импортированы в коммутатор. Пользователи могут напрямую включить протокол SSL и получить доступ к коммутатору в режиме HTTPS.

Введите имя пользователя и пароль для успешного входа в коммутатор через HTTPS.

5.13. Служба передачи файлов

Служба передачи файлов обеспечивает взаимное резервное копирование файлов между сервером и клиентом. При изменении файла на сервере (или клиенте) вы можете получить файл резервной копии с клиента (или сервера) через FTP / TFTP / SFTP. Коммутатор может служить клиентом или сервером для загрузки и выгрузки файлов через FTP / TFTP / SFTP.

Для службы SFTP этот коммутатор поддерживает только службу клиента SFTP, что означает, что этот коммутатор может служить клиентом для загрузки и скачивания файлов через SFTP.

5.13.1. Служба TFTP

Коммутатор работает как TFTP-клиент

Сначала установите TFTP-сервер, как показано на рисунке ниже. В Current Directory найдите используемый путь к хранилищу файлов. Введите IP-адрес сервера в интерфейсе сервера.

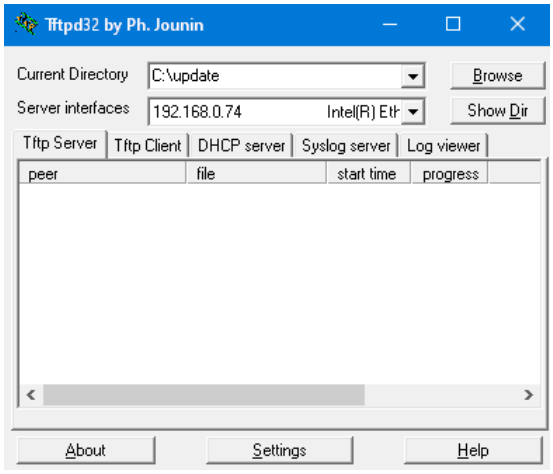


Рис. 67. Настройка TFTP сервера

Перейти [Device Basic Configuration] → [File transmit] → [TFTP Service] → [TFTP client service] для входа на страницу конфигурации TFTP клиента, как показано на рисунке ниже.

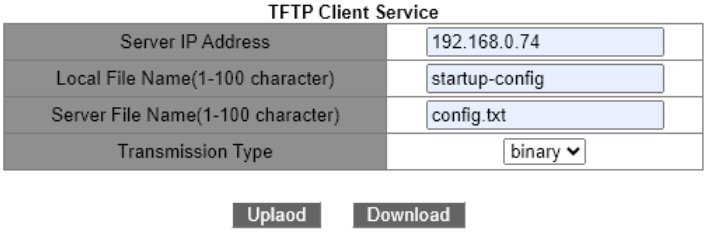


Рис. 68. Настройка TFTP клиента

- **Server IP address**
  Формат: A.D.C.D.
  Описание: Ввод IP адреса сервера
- **Local file name**
  Диапазон: 1 ~ 50 символов
  Описание: Введите имя файла коммутатора.
- **Server file name**
  Диапазон: 1 ~ 50 символов
  Описание: Введите имя файла сервера.
- **Transmission type**
  Элементы конфигурации: binary / ascii
  По умолчанию: binary
  Функция: выбор стандарта передачи файлов.
  Описание: ascii означает использование стандарта ASCII для передачи файла; двоичный означает использование двоичного стандарта для передачи файла.
  Использование: Нажмите <Upload>, чтобы загрузить файл с коммутатора на сервер, или <Download>, чтобы загрузить файл с сервера на коммутатор.
  После успешной передачи файла в веб-интерфейсе появляется следующая информация, как показано на рисунке ниже.

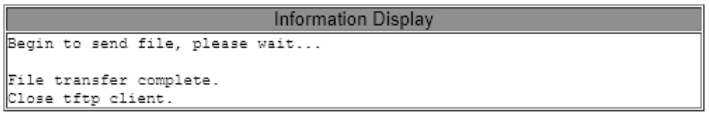


Рис. 69. Сообщения TFTP клиента

- *В процессе передачи файлов поддерживает работу TFTP-сервера.*
- *Файл версии программного обеспечения не является текстовым файлом и должен принимать двоичный стандарт для передачи.*

Коммутатор работает как TFTP-сервер

Перейти [Device Basic Configuration] → [File transmit] → [TFTP Service] → [TFTP sever service] для входа на страницу конфигурации TFTP сервера, как показано на рисунке ниже.

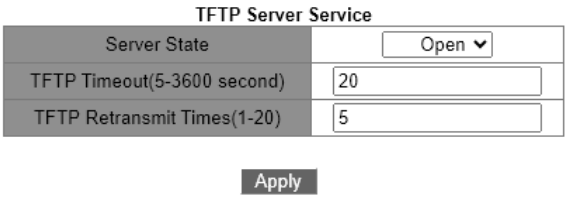


Рис. 70. Настройка TFTP сервера

- **Server state**
  Элементы конфигурации: Close / Open
  По умолчанию: Close
  Функция: включение/выключение функции сервера TFTP.
- **TFTP Timeout**
  Диапазон: 5~3600 с
  По умолчанию: 20 с.
  Функция: Настройка тайм-аута подключения к серверу TFTP.
- **TFTP Retransmit times**
  Диапазон: 1~20
  По умолчанию: 5
  Функция: настройка времени повторной передачи сервера TFTP во время тайм-аута.
  Установите клиентское программное обеспечение TFTP, как показано на рисунке ниже. Введите IP-адрес коммутатора в Host; выберите путь хранения файлов клиента в Local File; введите имя файла, сохраненного в коммутаторе в удаленном файле; нажмите <Get>, чтобы загрузить файл с коммутатора на клиента; нажмите <Put>, чтобы загрузить файл клиента для переключения.

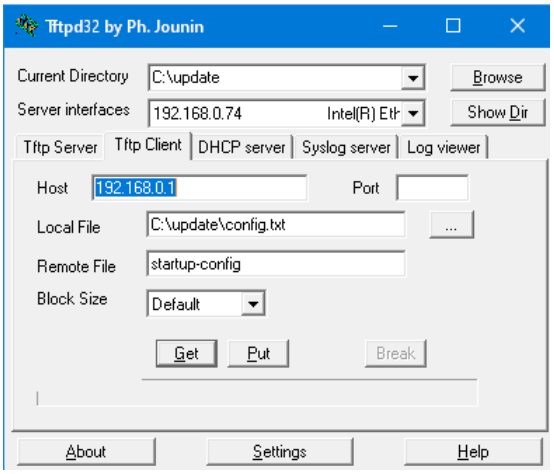


Рис. 71. Настройка TFTP клиента

➢ *Во время передачи файлов не отключайте программное обеспечение клиента TFTP.*

5.13.2. FTP Service

Коммутатор работает как FTP-клиент

Сначала установите FTP-сервер. Перейти [Security] → [users/rights] для открытия диалогового окна. Нажмите <новый пользователь>, чтобы создать нового пользователя FTP, как показано на рис. 72. Введите имя пользователя (username) и пароль (password), например, имя пользователя: admin; пароль: STEZ. Нажмите <OK>.

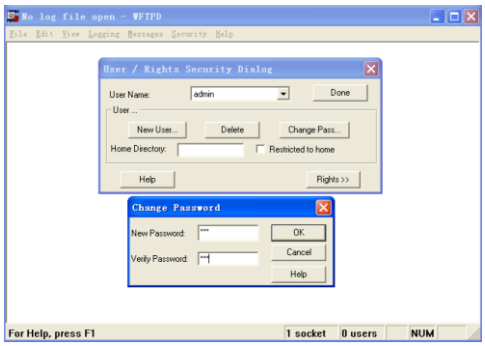


Рис. 72. Настройка FTP сервера

Введите путь к хранилищу файлов на сервере в домашнем каталоге, как показано на рисунке ниже. Нажмите <Done>.

Рис. 73. Настройка доступа к FTP серверу

Перейти [Device Basic Configuration] → [File transmit] → [FTP Service] → [FTP Client Service] для входа на страницу конфигурации FTP клиента, как показано на рисунке ниже.

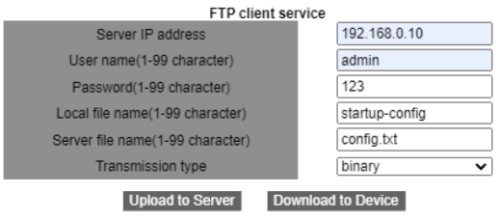


Рис. 74. Настройка FTP клиента

- **Server IP address**
  Формат: A.B.C.D.
  Описание: указывает IP-адрес сервера.
- **{User name, Password}**
  Диапазон: {1~100 символов, 1~100 символов}
  Описание: указывает имя пользователя и пароль, созданные на FTP-сервере.

- **Local file name.**
  Диапазон: 1~100 символов
  Описание: указывает имя файла в коммутаторе.
- **Server file name**
  Диапазон: 1~100 символов
  Описание: указывает имя файла на сервере.
- **Transmission type**
  Элементы конфигурации: binary / ascii
  По умолчанию: binary
  Функция: выбор стандарта передачи файлов.
  Объяснение: ascii означает использование стандарта ASCII для передачи файла; binary означает использование двоичного стандарта для передачи файла.
  Метод: Нажмите <Upload>, чтобы загрузить файл с коммутатора на сервер. Нажмите <Download>, чтобы загрузить файл с сервера для переключения.

  После успешной передачи файла в веб-интерфейсе появляется следующая информация, как показано на рисунке ниже.

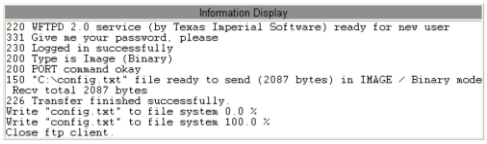


Рис. 75. Сообщения FTP клиента

- *В процессе передачи файлов не отключайте программное обеспечение FTP-сервера.*
- *Файл версии программного обеспечения не является текстовым файлом, и для передачи он должен принимать двоичный стандарт.*

Коммутатор работает как FTP-сервер

Перейти [Device Basic Configuration] → [File transmit] → [FTP Service] → [FTP Server Service] для входа на страницу конфигурации FTP сервера, как показано на рисунке ниже.

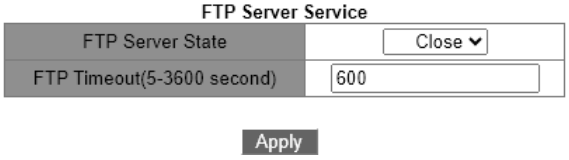


Рис. 76. Настройка FTP сервера

- **FTP Server state**
  Формат: Close / Open.
  По умолчанию: Close
  Функция: включение или отключение функции FTP-сервера.
- **FTP Timeout**
  Диапазон: 5~3600 с

По умолчанию: 600 с

Функция: настройка времени ожидания подключения к FTP-серверу.

Описание: Если в течение тайм-аута между FTP-сервером и клиентом не передаются данные, соединение между ними разрывается.

Настройте имя пользователя и пароль, используемые для входа на FTP-сервер, как показано на рисунке ниже.

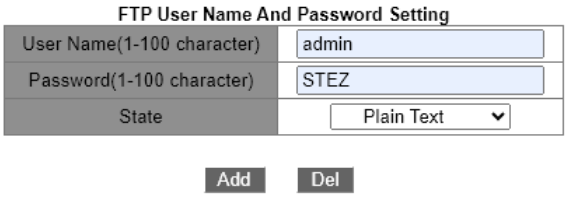


Рис. 77. Настройка доступа к FTP серверу

- **{Username, Password}**
  Диапазон: {1~16 символов, 1~16 символов}
  Функция: Настройка имени пользователя и пароля для входа на FTP-сервер.
  Описание: Когда коммутатор работает как FTP-сервер, он может одновременно подключаться к нескольким FTP-клиентам.
- **State**
  Опции: Простой текст / Зашифрованный текст
  По умолчанию: обычный текст
  Функция: Выберите режим отображения пароля.

Перейти [Пуск] → [Выполнить] в Windows. Отображается диалоговое окно «Выполнить». Введите «cmd» и нажмите Enter. Отображается следующая страница.

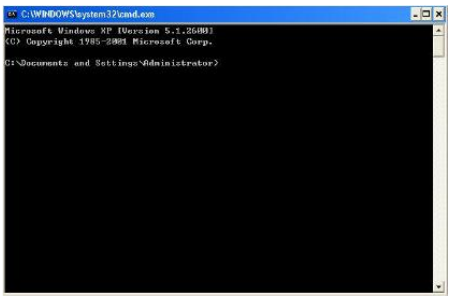


Рис. 78. Настройка доступа к FTP серверу

Путь передачи файла можно изменить. Войдите на FTP-сервер, как показано на рисунке:

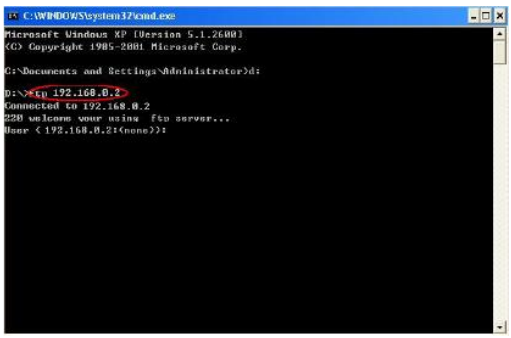


Рис. 79. Настройка доступа к FTP серверу

Используйте настроенное имя пользователя «admin» и пароль «STEZ» для входа на FTP-сервер, как показано на рисунке ниже:

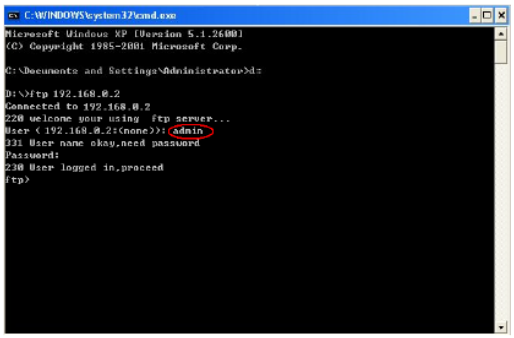


Рис. 80. Настройка доступа к FTP серверу

Используйте команду «get», чтобы загрузить файл по указанному пути на клиенте, как показано на рисунке. Введите команду «get» и нажмите Enter. Введите имя файла на коммутаторе для загрузки в удаленный файл и имя файла, сохраненного на клиенте, в локальный файл.

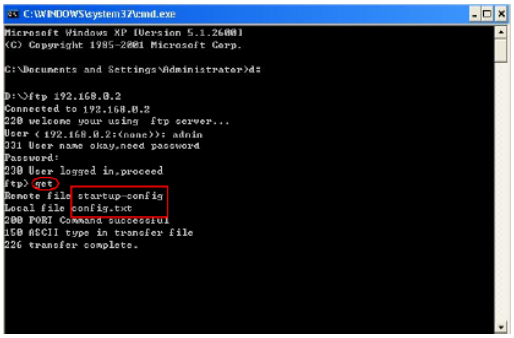


Рис. 81. Загрузка файла в ПК по FTP

Используйте команду «put», чтобы загрузить файл по указанному пути в клиенте на сервер, как показано на рисунке ниже. Запустите команду «put» и нажмите Enter. Введите имя файла в коммутаторе в удаленном файле и имя файла в клиенте, который будет загружен в локальный файл.

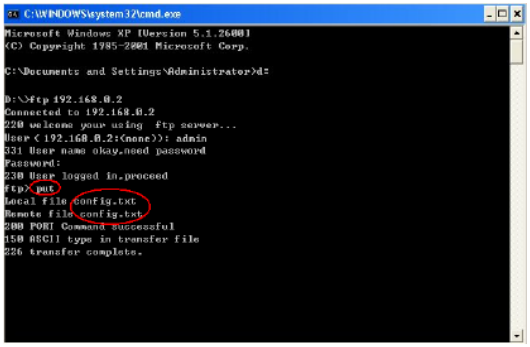


Рис. 82. Выгрузка файла из ПК по FTP

5.14. Конфигурация MAC Address

5.14.1. Введение

Когда коммутатор пересылает сообщение, он проверяет номер порта, соответствующий MAC-адресу получателя в сообщении, в соответствии с таблицей MAC-адресов и пересылает сообщение через порт.

MAC-адреса делятся на статические MAC-адреса и динамические MAC-адреса.

Статический MAC-адрес настраивается пользователем, имеет наивысший приоритет (не распространяется на динамический MAC-адрес) и действует постоянно.

Динамический MAC-адрес запоминается коммутатором в процессе пересылки кадров данных и вступает в силу в течение ограниченного времени, а таблица MAC-адресов регулярно обновляется. Когда коммутатор получает кадр данных, который необходимо переслать, он сначала узнает MAC-адрес источника кадра данных и устанавливает связь с принимающим портом, а затем запрашивает таблицу MAC-адресов в соответствии с MAC-адресом получателя. в противном случае коммутатор передает кадр данных в своем собственном широковещательном домене.

Время устаревания относится к времени, когда динамический MAC-адрес добавляется в таблицу адресов. Если каждый порт не получит кадр с исходным адресом этого MAC-адреса в течение 1-2 раз по истечении времени старения, запись будет удалена. из динамической таблицы адресов переадресации. Статическая таблица MAC-адресов не зависит от времени устаревания.

Эта серия коммутаторов может настраивать до 1024 статических одноадресных записей.

5.14.2. Веб конфигурирование

Добавление статического MAC-адреса

Перейти [Device Basic Configuration] → [MAC address table configuration] → [Unicast Address Configuration] для входа на страницу конфигурации, как показано на рисунке ниже.

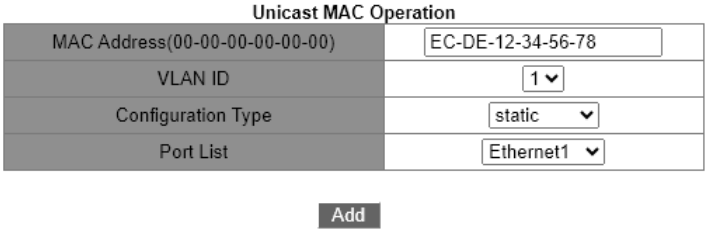


Рис. 83. Добавление статического MAC-адреса

- **MAC address**
  Формат: HH-HH-HH-HH-HH-HH (H — шестнадцатеричное число)
  Функция: Настройка одноадресного MAC-адреса. Младший бит в первом байте равен 0.
- **VLAN ID**
  Опции: все созданные идентификаторы VLAN.
  По умолчанию: VLAN1
- **Configuration type**
  Варианты: static / blackhole
  По умолчанию: static
  Функция: выберите тип записи MAC-адреса.
  Описание: Статический означает установление соответствия между назначенным MAC-адресом и номером порта или идентификатором VLAN. Blackhole должен отбросить пакет, исходный MAC-адрес которого или MAC-адрес назначения является назначенным MAC-адресом.
- **Port**
  Опции: все порты коммутатора
  Функция: выберите порт для пересылки пакетов с этим MAC-адресом назначения. Выбранный порт должен находиться в указанной сети VLAN.

Удаление статического MAC-адреса

Перейти [Device Basic Configuration] → [MAC address table configuration] → [Delete Unicast Address] для входа на страницу конфигурации, как показано на рисунке ниже.

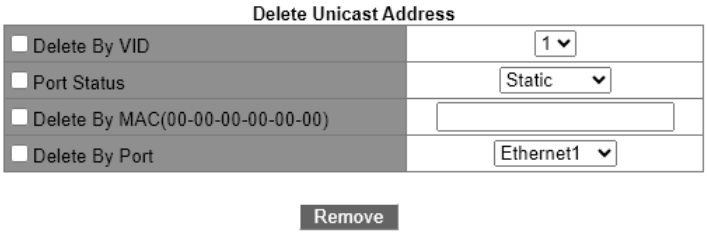


Рис. 84. Удаление статического MAC-адреса

Выберите критерий для удаления индивидуального адреса. Если выбрано несколько критериев, их взаимосвязь является логическим «И».

Настройка времени устаревания MAC-адреса

Перейти [Device Basic Configuration] → [MAC address table configuration] → [Address Aging-time] для входа на страницу конфигурации, как показано на рисунке ниже.

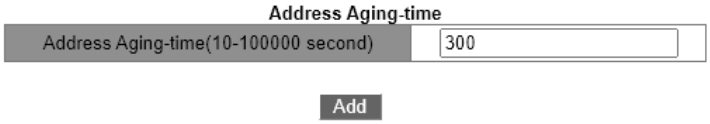


Рис. 85. Настройка времени устаревания MAC-адреса

- **Aging time**
  Диапазон: 10~100000c
  По умолчанию: 300 с
  Функция: Установите время устаревания для записи динамического MAC-адреса.
  Описание: Когда время старения установлено на 0, старение запрещено. В этом случае адрес, полученный динамически, не устаревает со временем.

Запрос unicast MAC-адреса

Перейти [Device Basic Configuration] → [MAC address table configuration] → [MAC address query] для входа на страницу конфигурации, как показано на рисунке ниже.

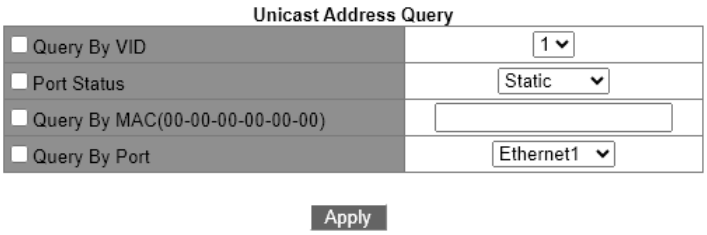


Рис. 86. Запрос unicast MAC-адреса

Выберите критерий для unicast запроса MAC-адреса. Если выбрано несколько критериев, их взаимосвязь является логическим «И». Например, если вы запрашиваете unicast адрес порта Ethernet 1/1, отображается следующая страница.

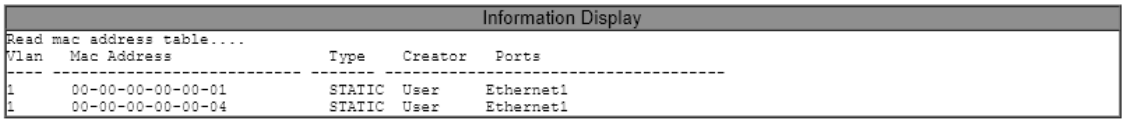


Рис. 87. Отображение результата unicast запроса

Просмотр записей MAC адресов

Перейти [Device Basic Configuration] → [MAC address table configuration] → [Show mac-address table] для входа на страницу конфигурации, как показано на рисунке ниже.

Information Display

```
Read mac address table....
Vlan   Mac Address                Type    Creator   Ports
---- -------------------------- ------- ---------- ------------------------------------
1      00-00-00-00-00-01          STATIC  User      Ethernet1
1      00-00-00-00-00-04          STATIC  User      Ethernet1
1      68-84-7e-36-44-4f          DYNAMIC Hardware  Ethernet2
```

Рис. 88. Просмотр записей MAC адресов

5.15. Информация об обслуживании и отладке базовой конфигурации

При настройке коммутатора может потребоваться проверка правильности различных конфигураций для обеспечения нормальной работы; или при возникновении определенных аномалий может потребоваться локализация неисправности. В этих случаях вы можете выполнить следующие операции для просмотра конфигурации системы и рабочего состояния.

Ping

Перейти [Device Basic Configuration] → [Basic configuration debug] → [Ping and Traceroute] для входа на страницу конфигурации ping, как показано на рисунке ниже.

Ping

IP Address	192.168.0.2
Hostname	Switch

Рис. 89. Команда Ping

- **IP address**
  Формат: A.B.C.D.
  Описание: Введите IP-адрес удаленного устройства.
- **Hostname**
  Диапазон: 1~30 символов
  Функция: Если сопоставление между удаленным хостом и IP-адресом установлено, просто введите имя удаленного хоста и выполните операцию Ping.
  Описание: Коммутатор отправляет пакеты запросов ICMP на удаленное устройство для обнаружения связи между коммутатором и удаленным устройством.

Traceroute

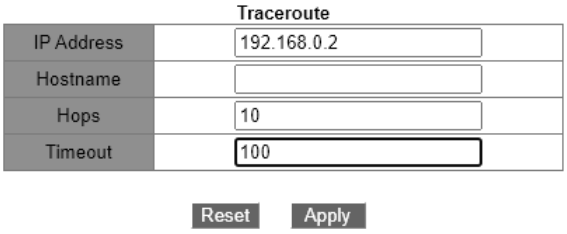


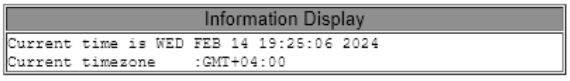
Рис. 90. Команда Traceroute

- **IP address**
  Формат: A.B.C.D.
  Описание: Введите IP-адрес удаленного устройства.
- **Hostname**
  Диапазон: 1~30 символов
  Функция: Если сопоставление между удаленным хостом и IP-адресом установлено, вам нужно ввести только имя удаленного хоста для выполнения операции Traceroute.
- **Hops**
  Опции: 1~255
  Функция: проверка количества шлюзов, через которые проходят пакеты от отправляющего устройства к целевому.
- **Timeout**
  Опции: 100~10000 мс
  Функция: Настройка тайм-аута. Если отправляющее устройство не получает ответный пакет от принимающего устройства в течение этого времени, считается, что связь не удалась.

Просмотр системной даты и времени.

Коммутаторы этой серии поддерживают RTC. Даже питание отключено, хронометраж продолжается.

Перейти [Device Basic Configuration] → [Basic configuration debug] → [show clock] для входа на страницу информации, как показано на рисунке ниже.



Просмотр информацию о файлах на flash

Перейти [Device Basic Configuration] → [Basic configuration debug] → [show flash] для входа на страницу информации, как показано на рисунке ниже.

Information Display

```
[NO.1]    d    2048 bytes    log
[NO.2]    -    3808 bytes    ssl.cky
[NO.3]    -    7200842 bytes    osapp.bin * #
[NO.4]    -    8968 bytes    edrLog2.txt
[NO.5]    -    8968 bytes    edrLog3.txt
[NO.6]    -    8968 bytes    edrLog4.txt
[NO.7]    -    427 bytes    rsa_key
[NO.8]    -    8968 bytes    edrLog5.txt
[NO.9]    -    1 bytes    edrLogNum.txt
[NO.10]    -    8968 bytes    edrLog1.txt
[NO.11]    -    313181 bytes    log/buf.log
[NO.12]    -    1048640 bytes    log/syslocal.log
[NO.13]    -    312765 bytes    log/systemlog.log
[NO.14]    -    3296 bytes    log/alarmlog.log
```

Рис. 91. Просмотр информацию о файлах на flash

Просмотр информации о конфигурации: running-config

Перейти [Device Basic Configuration] → [Basic configuration debug] → [show running-config] для входа на страницу информации, как показано на рисунке ниже.

Information Display

```
Current configuration:
!
   hostname SWITCH
   user add admin level admin service console telnet ssh
web authen-type password **** pwdvalidtime 2184
authentication-retries 3 unauth-locked-times 3
   clock timezone add 04:00
!
   ip ftp admin password 0 123 userpath /yaffs2/
   ftp-server enable
!
   authentication dot1x local
   authentication telnet login local
   authentication web login local
   authentication ssh login local
!
!
Vlan 1
   vlan 1
!
Interface Ethernet1
!
   lldp enable
!
```

Рис. 92. Просмотр информации о конфигурации

Просмотр информации о порте

Перейти [Device Basic Configuration] → [Basic configuration debug] → [show switchport interface] для входа на страницу информации, как показано на рисунке ниже.

Port Ethernet1

Reset Apply

Information Display

```
Ethernet1
Type :Universal
Mode :Access
Port VID :1
```

Рис. 93. Просмотр информации о порте

- **Type**
  Описание: тип VLAN.
- **Mode**
  Описание: режим порта.

- **Port VID**
  Описание: порт PVID

Просмотр состояния TCP-соединения

Перейти [Device Basic Configuration] → [Basic configuration debug] → [show tcp] для входа на страницу информации, как показано на рисунке ниже.

Information Display

LocalAddress	LocalPort	ForeignAddress	ForeignPort	State
192.168.0.1	80	192.168.0.74	64882	ESTABLISH
192.168.0.1	80	192.168.0.74	64881	TIMEWAIT
192.168.0.1	80	192.168.0.74	64880	TIMEWAIT
192.168.0.1	80	192.168.0.74	64879	TIMEWAIT
192.168.0.1	80	192.168.0.74	64878	TIMEWAIT
192.168.0.1	80	192.168.0.74	64877	TIMEWAIT
192.168.0.1	80	192.168.0.74	64876	TIMEWAIT
192.168.0.1	80	192.168.0.74	64875	TIMEWAIT
192.168.0.1	80	192.168.0.74	64874	TIMEWAIT
192.168.0.1	80	192.168.0.74	64873	TIMEWAIT
192.168.0.1	80	192.168.0.74	64872	TIMEWAIT
192.168.0.1	80	192.168.0.74	64871	TIMEWAIT
0.0.0.0	21	0.0.0.0	0	LISTEN
0.0.0.0	443	0.0.0.0	0	LISTEN
0.0.0.0	80	0.0.0.0	0	LISTEN
0.0.0.0	23	0.0.0.0	0	LISTEN

Рис. 94. Просмотр состояния TCP-соединения

- **Local Address**
  Описание: указывает локальный адрес TCP-соединения.
- **Local Port**
  Описание: указывает номер локального порта TCP-соединения.
- **Foreign Address**
  Описание: указывает адрес на другом конце TCP-соединения.
- **Foreign Port**
  Описание: указывает номер порта на другом конце соединения TCP.
- **State**
  Описание: указывает текущий статус TCP-соединения.

Просмотр состояния UDP-соединения

Перейти [Device Basic Configuration] → [Basic configuration debug] → [show udp] для входа на страницу информации, как показано на рисунке ниже.

Information Display

LocalAddress	LocalPort	ForeignAddress	ForeignPort	State
0.0.0.0	2012	0.0.0.0	0	CLOSED
0.0.0.0	161	0.0.0.0	0	CLOSED

Рис. 95. Просмотр состояния UDP-соединения

- **Local Address**
  Описание: указывает локальный адрес UDP-соединения.
- **Local Port**
  Описание: указывает номер локального порта UDP-соединения.
- **Foreign Address**
  Описание: указывает адрес на другом конце UDP-соединения.

- **Foreign Port**
  Описание: указывает номер порта на другом конце соединения UDP.
- **State**
  Описание: указывает текущий статус UDP-соединения.

Просмотр информации об онлайн Telnet пользователях

Перейти [Device Basic Configuration] → [Basic configuration debug] → [Show Telnet Login] для входа на страницу информации, как показано на рисунке ниже.

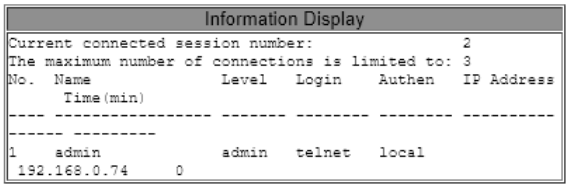


Рис. 96. Просмотр информации об онлайн Telnet пользователях

6. Расширенная конфигурация

6.1. ARP конфигурация

6.1.1. Введение

Address Resolution Protocol (ARP, протокол разрешения адресов) разрешает сопоставление между IP-адресами и MAC-адресами с помощью механизма запроса и ответа адреса. Коммутатор может узнать сопоставление между IP-адресами и MAC-адресами других хостов в том же сегменте сети. Он также поддерживает статические записи ARP для определения соответствия между IP-адресами и MAC-адресами.

Динамические записи ARP периодически устаревают, обеспечивая согласованность между записями ARP и фактическими приложениями. Коммутаторы этой серии обеспечивают не только функцию коммутации уровня 2, но и функцию ARP для разрешения IP-адресов других хостов в том же сегменте сети, обеспечивая связь между NMS и управляемыми хостами.

6.1.2. Описание

Записи ARP делятся на динамические и статические. Динамические записи генерируются и поддерживаются на основе обмена пакетами ARP. Динамические записи могут устаревать, обновляться новым пакетом ARP или перезаписываться статической записью ARP. Статические записи настраиваются, поддерживаются вручную и никогда не устаревают, и не перезаписываются динамическими записями ARP. Коммутатор поддерживает до 8192 записей ARP. Когда количество записей ARP превышает 8192, новые записи автоматически перезаписывают старые динамические.

6.1.3. Proxy-ARP

Если запрос ARP отправляется с хоста на другой хост, который находится в том же сетевом сегменте, но в другой физической сети, шлюз, находящийся в прямом соединении с хостом-источником и с функцией прокси-ARP, может ответить на это сообщение запроса. Этот процесс называется прокси-ARP.

Процесс прокси-ARP выглядит следующим образом:

- Хост-источник отправляет запрос ARP на другой хост в другой физической сети.
- Функция proxy ARP на этом интерфейсе VLAN была включена на шлюзе в прямом соединении с хостом-источником.
- Если нормальный маршрут к целевому хосту существует, шлюз отвечает своим собственным MAC-адресом для целевого хоста.
- IP-пакеты, отправленные с исходного узла на узел назначения, отправляются на устройство с включенным прокси-ARP.
- Шлюз выполняет обычную IP-маршрутизацию и пересылку пакетов.
- IP-пакеты, которые должны быть отправлены на узел назначения, наконец достигают узла назначения через сеть.

Прокси не выполняется для запросов ARP, соответствующих маршрутизации по умолчанию.

6.1.4. Веб конфигурирование

Добавить или удалить статическую запись ARP

Перейти [Device Advanced Configuration] → [ARP configuration] → [ARP configuration] для входа на страницу информации о ARP, как показано на рисунке ниже.

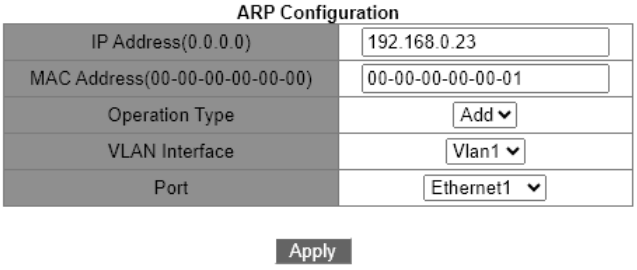


Рис. 97. Добавить или удалить статическую запись ARP

- **IP address**
  Формат: A.B.C.D.
  Функция: Настройка IP-адреса статической записи ARP.
- **MAC address**
  Формат: HH-HH-HH-HH-HH-HH (H — шестнадцатеричное число)
  Функция: Настройка MAC-адреса статической записи ARP.

- **Operation type**
  Опции: add / del
  По умолчанию: add
  Функция: добавить или удалить запись ARP.
- **L3 interface**
  Опции: все созданные интерфейсы VLAN уровня 3.
  По умолчанию: VLAN1
  Функция: выберите интерфейс VLAN уровня 3 для текущей записи ARP.
- **Ethernet Port**
  Опции: все порты в назначенной VLAN
  Функция: выберите выход, соответствующий текущей записи ARP.

IP-адрес, связанный со статической записью ARP, не может быть IP-адресом коммутатора.
К одному MAC-адресу можно привязать разные IP-адреса.
В VLAN запись ARP может соответствовать только одному порту пересылки.
Как правило, коммутатор автоматически запоминает записи ARP без вмешательства администратора.

Просмотр записей адресов ARP

Перейти [Device Advanced Configuration] → [ARP configuration] → [Show ARP] для входа на страницу информации о ARP, как показано на рисунке ниже.

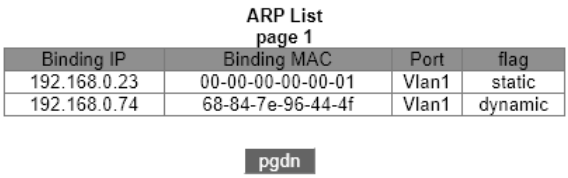


Рис. 98. Просмотр записей адресов ARP

- **ARP list**
  Портфолио: {IP-адрес, MAC-адрес, интерфейс L3, порт Ethernet, тип}
  Функция: просмотр записей ARP.
  Описание: Список ARP показывает все записи ARP, соответствующие портам LinkUp, включая статические записи и динамические записи.

Очистка кэша ARP

Перейти [Device Advanced Configuration] → [ARP configuration] → [Clear ARP cache] для очистки кэша ARP, как показано на рисунке ниже.

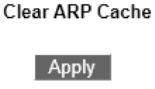


Рис. 99. Очистка кэша ARP

Нажмите <Apply>, чтобы очистить динамические записи ARP в кэше.

Включение прокси-ARP

Перейти [Device Advanced Configuration] → [ARP configuration] → [Proxy ARP configuration] для конфигурирования кеша ARP, как показано на рисунке ниже.

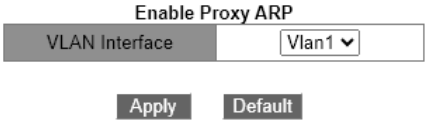


Рис. 100. Включение прокси-ARP

- **VLAN interface**
  Функция: выберите 3-уровневый интерфейс VLAN для включения прокси-ARP.

6.1.5. Пример типовой конфигурации

Как показано на рис ниже, PC1, PC2 и PC3 принадлежат хостам в одном сегменте сети и принадлежат к разным подсетям VLAN1, VLAN2 и VLAN4 соответственно.

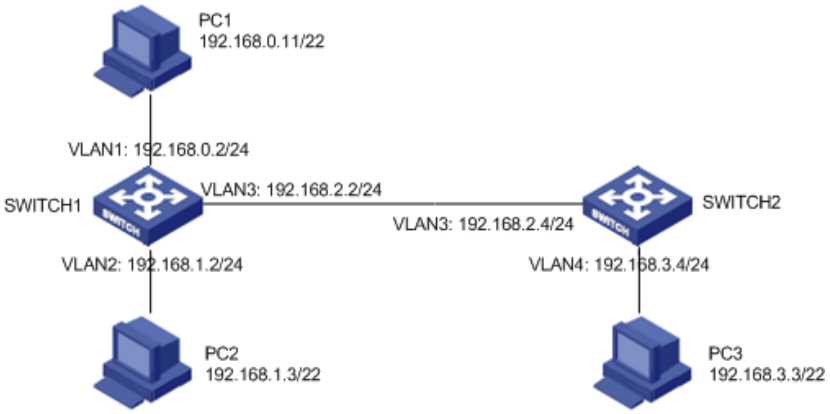


Рис. 101. Пример конфигурации

PC1 передает запрос ARP для запроса MAC-адресов PC2 и PC3.

- Когда функция прокси-ARP интерфейса VLAN1 коммутатора SWITCH1 не включена, поскольку они находятся в разных VLAN, запрос ARP не может достичь PC2 и PC3, и две стороны не могут обмениваться данными;
- Когда функция прокси-ARP интерфейса VLAN1 для SWITCH1 включена, после того, как интерфейс VLAN1 получит запрос ARP, он обнаружит, что существует маршрут к PC2 и PC3, путем поиска записей в таблице маршрутизации, затем SWITCH1 использует MAC-адрес интерфейса VLAN1. для отправки ответного сообщения ARP (ответ Исходный IP-адрес в сообщении является IP-адресом PC2 и PC3). После того как PC1 получает ответное сообщение, он создает запись ARP, а последующие IP-сообщения, отправляемые с PC1 на PC2 и PC3, отправляются на интерфейс VLAN1 коммутатора SWITCH1, а затем пересылаются коммутатором SWITCH1.

6.2. Layer 3 конфигурация интерфейса

6.2.1. Просмотр IP адреса коммутатора

Войдите в CLI коммутатора через консольный порт. Запустите команду enable в общем виде, чтобы войти в привилегированный вид. Запустите команду show interface vlan 1, чтобы просмотреть IP-адрес коммутатора, как показано в красном круге на рисунке ниже.

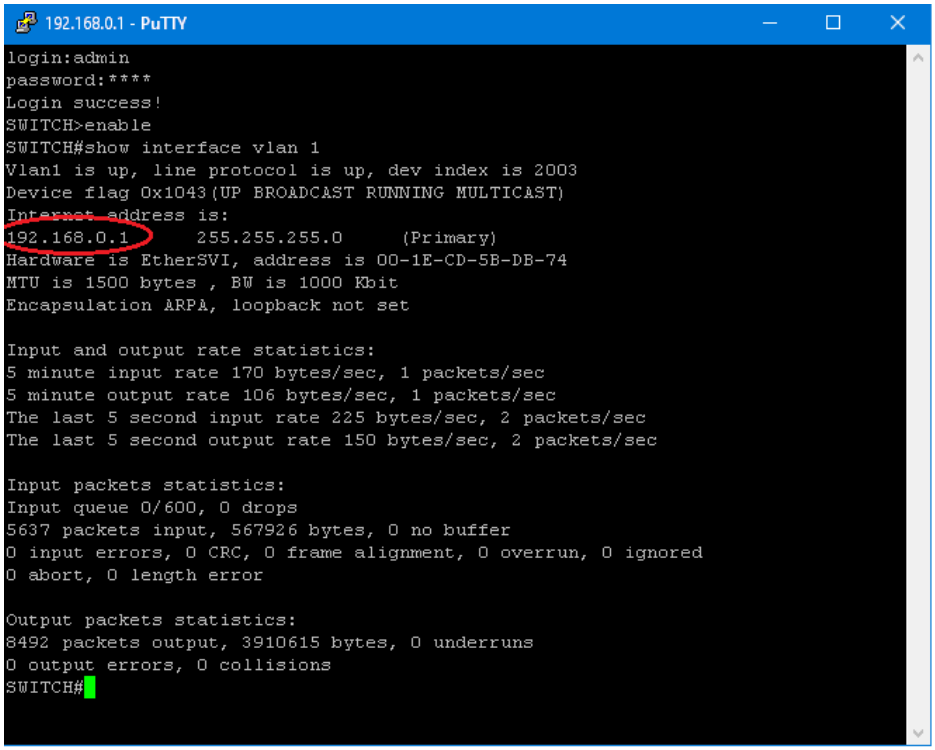


Рис. 102. Просмотр IP адреса коммутатора

6.2.2. Конфигурирование IP адреса

Создайте интерфейс VLAN уровня 3

Хосты в разных VLAN не могут взаимодействовать друг с другом. Их коммуникационные пакеты должны пересылаться маршрутизатором или коммутатором уровня 3 через интерфейс VLAN.

Коммутаторы этой серии поддерживают интерфейсы VLAN, которые представляют собой виртуальные интерфейсы уровня 3, используемые для обмена данными между VLAN. Вы можете создать один интерфейс VLAN для каждой VLAN. Интерфейс используется для пересылки пакетов уровня 3 портов в VLAN.

Перейдите в дерево навигации [Device Advanced Configuration] → [L3 Interface Configuration] → [Add Interface VLAN], чтобы войти в интерфейс создания интерфейса VLAN, как показано на рис. 103.

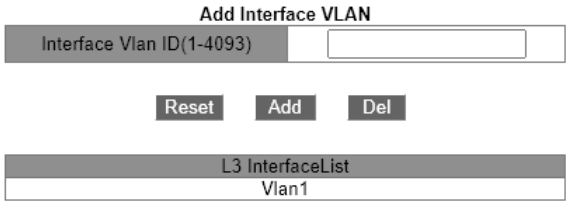


Рис. 103. Создайте интерфейс VLAN уровня 3

- **Interface vlan ID**
  Опции: все созданные номера VLAN.
  Функция: создание интерфейса VLAN уровня 3.

Коммутатор поддерживает максимум 128 интерфейсов VLAN уровня 3.
Перед созданием интерфейса VLAN убедитесь в наличии соответствующей VLAN. Если VLAN не существует, ее интерфейс VLAN не может быть создан.
Вы не можете удалить интерфейс VLAN, соответствующий IP-адрес которого используется для доступа к коммутатору через web.

Ручная настройка IP address

Перейти [Device Advanced Configuration] → [L3 interface configuration] → [Allocate IP address for L3 port] для ручного назначения IP Address для L3 интерфейса, как показано на рисунке ниже.

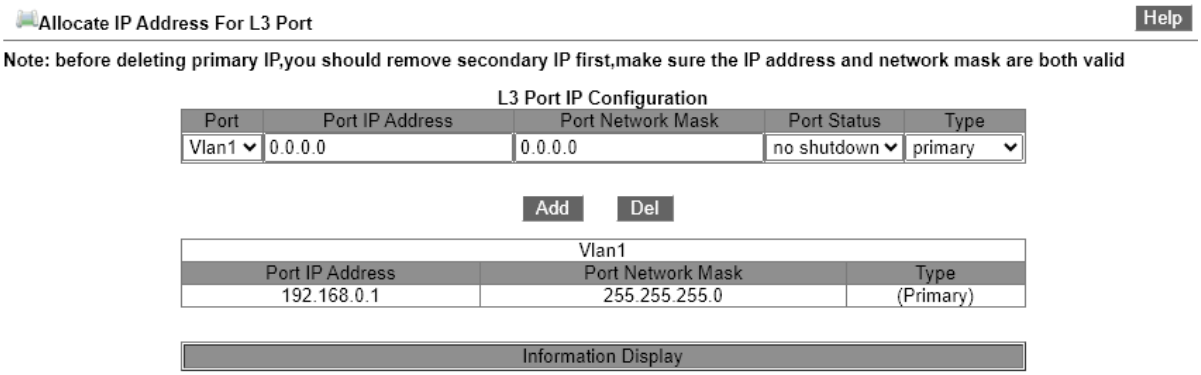


Рис. 104. Ручная настройка IP address

- **IP Address**
  Формат конфигурации: A.B.C.D.
  Функция: Настройте IP-адрес для указанного интерфейса VLAN уровня 3.
- **Subnet mask**
  Маска подсети представляет собой число длиной 32 бита, состоящее из строки 1 и строки 0. «1» соответствует полям номера сети и полям номера подсети, а «0» соответствует полям номера хоста. Обычно он настроен как 255.255.255.0.
- **Status**
  Опции: no shutdown / shutdown
  По умолчанию: no shutdown

Функция: настройка состояния интерфейса VLAN уровня 3.
Описание: без выключения: открывает интерфейс VLAN уровня 3. Завершение работы: закрывает интерфейс VLAN уровня 3.

- **Type**
  Опции: secondary / primary
  По умолчанию: primary
  Функция: В одном и том же порту можно установить более двух IP-адресов разных сетевых сегментов для реализации связи между разными сетевыми сегментами в одной и той же локальной сети. Как правило, поскольку сегмента сети пользователю недостаточно, можно использовать этот метод.
  Описание: вторичный IP-адрес может решить проблему агрегации маршрутизации в RIP v1. Его можно использовать для NAT, после преобразования он не является адресом прямого подключения маршрутизатора.
  Нажмите <Add>, чтобы настроить IP-адрес для интерфейса VLAN; нажмите <Del>, чтобы удалить текущий IP-адрес, вы должны сначала удалить дополнительный IP-адрес, прежде чем удалять основной IP-адрес; нажмите <Update>, чтобы изменить основной IP-адрес интерфейса VLAN.

Каждый интерфейс VLAN уровня 3 поддерживает максимум 32 IP-адреса.
Для каждого интерфейса VLAN можно настроить IP-адреса одного и того же сегмента сети или разных сегментов сети.
IP-адреса разных сегментов сети должны быть настроены для разных интерфейсов VLAN.

Варианты присвоения IP адреса

Перейти [Device Advanced Configuration] → [L3 interface configuration] → [L3 Port IP Address Mode Configuration] для назначения IP Address для L3 интерфейса, как показано на рисунке ниже.

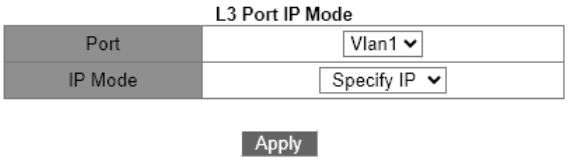


Рис. 105. Варианты присвоения IP адреса

- **Interface**
  Опции: все созданные интерфейсы VLAN уровня 3.
  По умолчанию: VLAN1.
- **IP Mode**
  Опции: bootp-client / dhcp-client / Specify IP
  По умолчанию: Specify IP
  Функция: Выберите режим получения IP-адреса.
  Описание: Указать IP-адрес — настроить IP-адрес вручную; bootp-client / dhcp-client заключается в том, что коммутатор автоматически получает IP-адрес через DHCP / BOOTP. В сети должен быть сервер DHCP / BOOTP для назначения IP-адресов клиентам.

6.3. SNMPv2c

6.3.1. Введение

Простой протокол управления сетью (Simple Network Management Protocol - SNMP) — это структура, использующая TCP/IP для управления сетевыми устройствами. С помощью функции SNMP администратор может запрашивать информацию об устройстве, изменять настройки параметров, отслеживать состояние устройства и обнаруживать сбои в сети.

6.3.2. Реализация

SNMP принимает режим станции управления / агента. Таким образом, SNMP включает в себя два типа сетевых элементов: NMS и агент.

- Станция управления сетью (NMS) — это станция, на которой работает программный клиент управления сетью с поддержкой SNMP. Это ядро для сетевого управления сетью SNMP.
- Агент — это процесс в управляемых сетевых устройствах. Он получает и обрабатывает пакеты запросов от NMS. Когда возникает тревога, агент заблаговременно сообщает об этом в NMS.

NMS является менеджером сети SNMP, а агент — управляемым устройством сети SNMP. NMS и агенты обмениваются пакетами управления через SNMP. SNMP включает в себя следующие основные операции:

- Get-Request
- Get-Response
- Get-Next-Request
- Set-Request
- Trap

NMS отправляет пакеты Get-Request, Get-Next-Request и Set-Request агентам для запроса, настройки и управления переменными. После получения этих запросов агенты отвечают пакетами Get-Response. Когда возникает тревога, агент заранее сообщает об этом в NMS с помощью пакета trap.

6.3.3. Описание

Коммутаторы этой серии поддерживают SNMPv2c и SNMPv3, SNMPv2c совместим с SNMPv1. SNMPv1 использует community name для аутентификации. Community name действует как пароль, ограничивая доступ NMS к агентам. Если community name, переносимое пакетом SNMP, не подтверждается коммутатором, запрос завершается неудачно и возвращается сообщение об ошибке.

SNMPv2c также использует community name для аутентификации. Он совместим с SNMPv1 и расширяет функции SNMPv1.

Чтобы обеспечить связь между NMS и агентом, их версии SNMP должны совпадать. На агенте можно настроить разные версии SNMP, чтобы он мог использовать разные версии для связи с разными NMS.

6.3.4. Введение в MIB

Любой управляемый ресурс называется управляемым объектом. База управляющей информации (Management Information Base - MIB) хранит управляемые объекты. Он определяет иерархические отношения управляемых объектов и атрибутов объектов, таких как имена, разрешения на доступ и типы данных. У каждого агента есть своя MIB. NMS может читать / записывать MIB на основе разрешений. На рисунке ниже показаны взаимосвязи между NMS, агентом и MIB.

Рис. 106. Взаимосвязи между NMS, агентом и MIB

MIB определяет древовидную структуру. Узлы дерева являются управляемыми объектами. Каждый узел имеет уникальный идентификатор объекта (OID), указывающий расположение узла в структуре MIB. Как показано на рисунке ниже, OID объекта A равен 1.2.1.1.

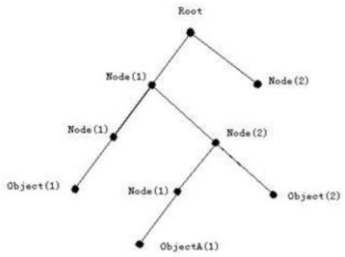


Рис. 107. Струрктура MIB

6.3.5. Веб конфигурирование

Конфигурирование SNMPv2

Перейти [Device Advanced Configuration] → [SNMP Configuration] → [SNMP Base Configuration] для конфигурирования SNMPv2, как показано на рисунке ниже.

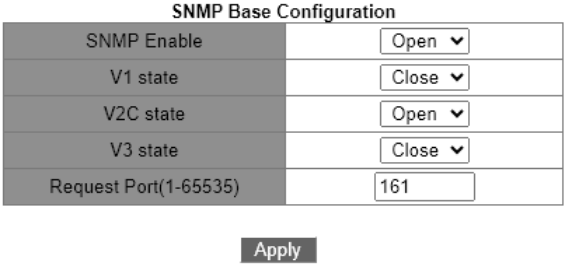


Рис. 108. Конфигурирование SNMPv2

- **Snmp Agent state**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включить / отключить SNMP.
- **V1/V2C/V3 state**
  Опции: Enable / Disable
  Функция: выберите версию SNMP.
- **Request Port**
  Диапазон: 1~65535
  По умолчанию: 161
  Функция: Настройка номера порта для приема SNMP-запросов.

Настройка режима управления SNMP

Перейдите в дерево навигации [Device Advanced Configuration] → [SNMP Configuration] → [SNMP Manager Configuration], чтобы войти в интерфейс конфигурации SNMP v2, как показано на рис. 109.

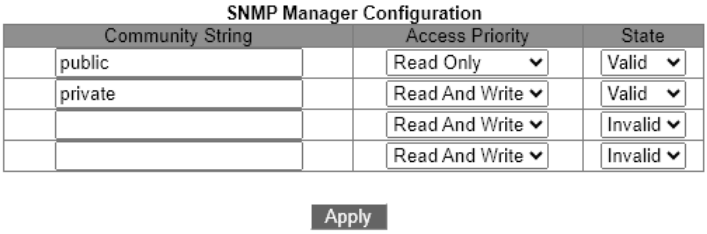


Рис. 109. Настройка режима управления SNMP

- **Community**
  Диапазон: 4~16 символов
  Функция: Настройка сообщества коммутаторов.
  Описание: пакет может получить доступ к MIB коммутатора только в том случае, если имя сообщества, передаваемое в пакете SNMP, совпадает с этой строкой сообщества.
- **Access Permission**
  Варианты: Read Only / Read And Write
  По умолчанию: Read Only
  Функция: Настройка режима доступа к MIB.

Описание: Read Only: считывает только информацию MIB. Read And Write: чтение и запись информации MIB.

- **State**
  Варианты конфигурации: Valid / Invalid
  Функция: Только когда конфигурация действительна, слово сообщества может быть успешно настроено. Если выбор недействителен, конфигурация не будет активна.

Настройка безопасных IP-адресов

Перейти [Device Advanced Configuration] → [SNMP Configuration] → [IP Address of SNMP Manager] для конфигурирования безопасных IP-адресов, как показано на рисунке ниже.

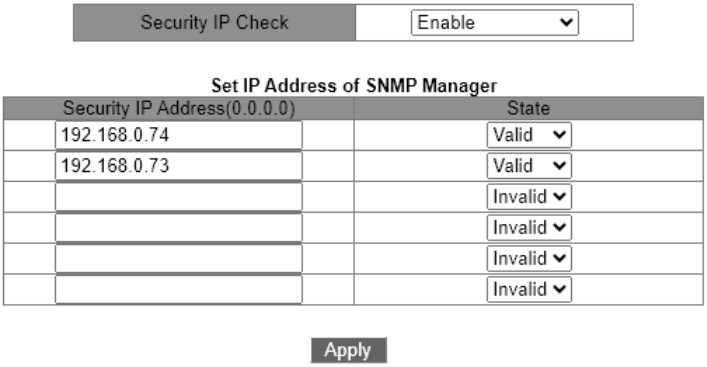


Рис. 110. Настройка безопасных IP-адресов

- **Security IP Check**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включить или отключить проверку безопасности IP. Если проверка безопасности IP отключена, нет ограничений на IP-адрес NMS, любая NMS, подключенная к коммутатору, может получить доступ к информации MIB коммутатора. После того, как проверка IP-адреса безопасности включена, вам необходимо установить IP-адрес безопасности, и только NMS с IP-адресом безопасности может получить доступ к информации MIB коммутатора.
- **IP Address**
  Формат: A.B.C.D.
  Функция: настроить безопасный IP-адрес NMS.
  Описание: Только NMS, чей IP-адрес соответствует IP-адресу безопасности, может получить доступ к информации MIB коммутатора. Коммутатор позволяет использовать максимум 6 IP-адресов безопасности NMS.
  Можно настроить до 6 IP-адресов менеджера безопасности.
- **State**
  Варианты конфигурации: активный/неактивный

Конфигурирование trap

Перейти [Device Advanced Configuration] → [SNMP Configuration] → [TRAP Manager Configuration] для конфигурирования trap, как показано на рисунке ниже.

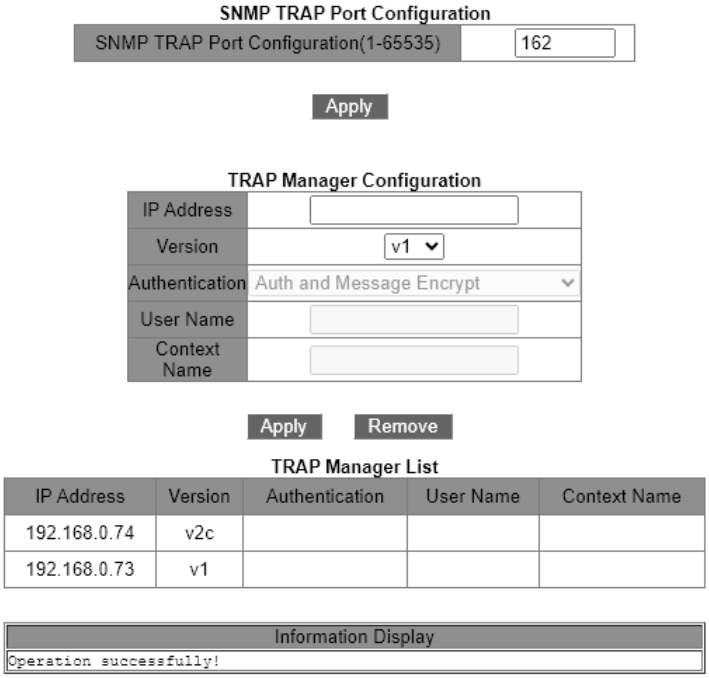


Рис. 111. Конфигурирование trap

- **TRAP Port**
  Опции: 1~65535
  По умолчанию: 162
  Функция: Настройка номера порта для отправки сообщений- trap.
- **Version**
  Опция: V1 / V2C / V3
  Функция: V1 / V2C указывает, что коммутатор отправляет сообщения- trap версии 1 / версии 2C на сервер. V3 указывает, что коммутатор отправляет на сервер сообщения- trap версии 3. Если вы выберете V1 / V2C, необходимо настроить только IP-адрес назначения.
- **Destination IP Address**
  Формат: A.B.C.D.
  Функция: Настройка адреса сервера для получения сообщений- trap. Вы можете настроить максимум 8 серверов, то есть 8 записей- trap.

Просмотр SNMP статистики

Перейти [Device Advanced Configuration] → [SNMP Configuration] → [SNMP Statistics] для просмотра SNMP, как показано на рисунке ниже.

SNMP Statistics	Number
Incoming Snmp Packet	2
Version Error Snmp Packet	0
Received Snmp GetNext Packet	0
Received SET Request Packet	0
Outgoing Snmp Packet	2
Too_big Error Snmp Packet	0
Max-Length of Snmp Datagram	1500
Snmp Request for Inexistent MIB Object	0
Bad_value Error Snmp Packet	0
General_error Snmp Packet	0
Transmitting Response Packet	2
Transmitting TRAP Packet	0
Nms SET Request Packet	0
Communitry String Error Snmp Packet	0
Communitry String Priority Error	0
Coding Error Snmp Packet	0

Show

Рис. 112. Просмотр SNMP статистики

6.3.6. Пример типовой конфигурации

Станция управления SNMP подключена к коммутатору через Ethernet, IP-адрес станции управления — 192.168.0.23, а IP-адрес коммутатора — 192.168.0.2. NMS отслеживает и управляет агентом через SNMPv2c, считывает и записывает информацию об узле MIB агента и активно отправляет сообщение Trap в NMS, когда агент выходит из строя или совершает ошибку, как показано на рис. 113.

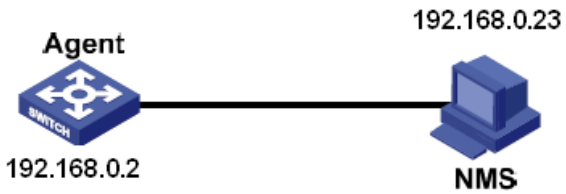


Рис. 113. Пример конфигурации

Процесс настройки агента:

- Включить протокол SNMP и статус V2C, настроить права доступа, сообщество только для чтения называется public, а сообщество для чтения и записи именуется private, см. рис. 109;
- Настройте безопасный IP-адрес как 192.168.0.23, см. рис. 110;
- Включите состояние Trap, выберите версию V2C и адрес сервера 192.168.0.23, см. рис. 111.

Если вы хотите контролировать и управлять состоянием агента, вам необходимо запустить соответствующее программное обеспечение для управления на стороне NMS.

6.4. SNMPv3

6.4.1. Введение

SNMPv3 обеспечивает механизм аутентификации модели безопасности на основе пользователей (User-Based Security Model - USM). Вы можете настроить функции аутентификации и шифрования. Аутентификация используется для проверки подлинности отправителя пакета, предотвращая доступ незаконных пользователей. Шифрование используется для шифрования пакетов, передаваемых между NMS и агентом, во избежание перехвата. Функции аутентификации и шифрования могут повысить безопасность связи между SNMP NMS и SNMP-агентом.

6.4.2. Реализация

SNMPv3 предоставляет пять таблиц конфигурации. Каждая таблица может содержать 16 записей. Эти таблицы определяют, могут ли определенные пользователи получать доступ к информации MIB.

Вы можете создать несколько пользователей в таблице пользователей. Каждый пользователь использует разные политики безопасности для аутентификации и шифрования.

Групповая таблица — это совокупность нескольких пользователей. В таблице групп права доступа определяются на основе групп пользователей. Все пользователи группы имеют права группы.

Таблица контекста идентифицирует строки, которые могут быть прочитаны пользователями, независимо от моделей безопасности.

Таблица представления относится к информации представления MIB, которая определяет информацию MIB, к которой могут обращаться пользователи. Представление MIB может содержать все узлы определенного поддерева MIB (т. е. пользователям разрешен доступ ко всем узлам поддерева MIB) или не содержать ни одного из узлов определенного поддерева MIB (т. е. узел поддерева MIB).

Вы можете определить права доступа MIB в таблице доступа по имени группы, имени контекста, модели безопасности и уровню безопасности.

6.4.3. Веб конфигурирование

Настройка таблицы пользователей

Перейти [Device Advanced Configuration] → [SNMP Configuration] → [V3 User Table Configuration] для конфигурации пользователей для V3, как показано на рисунке ниже.

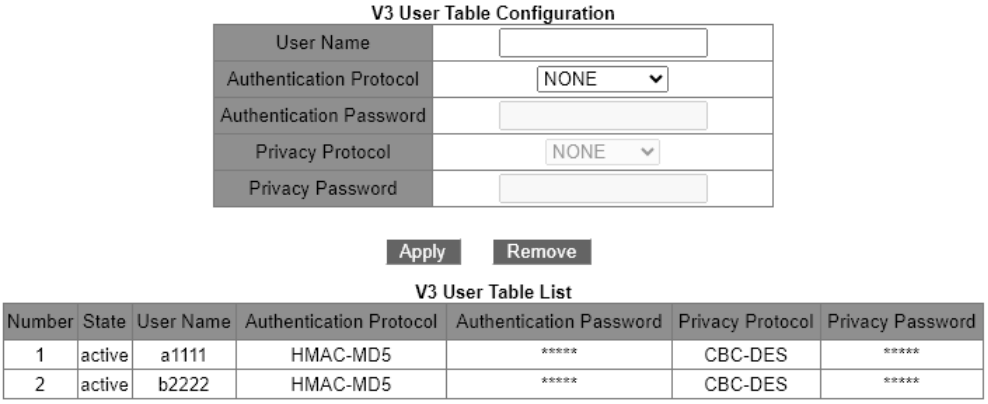


Рис. 114. Настройка таблицы пользователей

- **User Name**
  Диапазон: 4~16 символов
  Функция: Создать имя пользователя.
- **Authentication protocol**
  Опции: NONE / HMAC-MD5 / HMAC-SHA
  По умолчанию: NONE
  Функция: выбор алгоритма аутентификации.
- **Authentication password**
  Диапазон: 4~16 символов
  Функция: Создать пароль аутентификации.
- **Privacy protocol**
  Опции: NONE / HMAC-DES
  По умолчанию: NONE
  Функция: выберите протокол шифрования пакетов.
- **Privacy password**
  Диапазон: 4~16 символов
  Функция: создание пароля для шифрования пакетов.

Настроить групповую таблицу

Перейти [Device Advanced Configuration] → [SNMP Configuration] → [V3 Group Table Configuration] для конфигурации групп для V3, как показано на рисунке ниже.

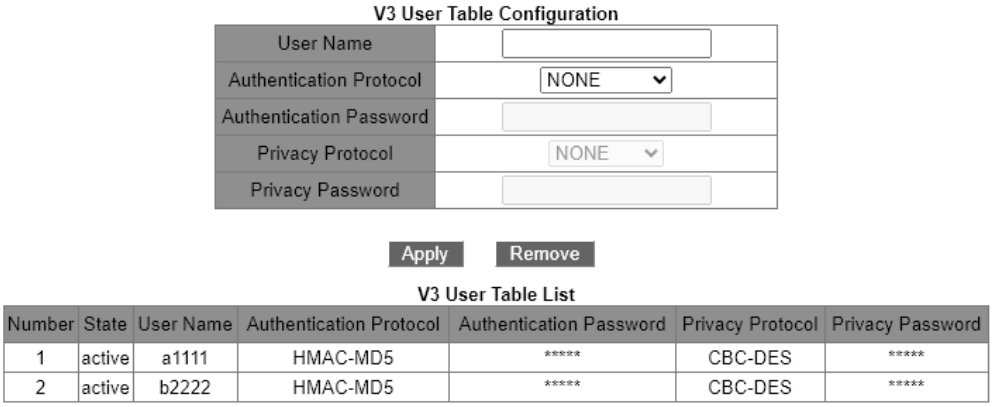


Рис. 115. Настроить групповую таблицу

- **Group Name**
  Диапазон: 4~16 символов
  Функция: Настройка имени групповой таблицы.
- **Security Name**
  Диапазон: все существующие имена пользователей, 4~16 символов.
  Функция: Настройка имени безопасности. Имя безопасности должно совпадать с именем пользователя в пользовательской таблице. Пользователи с одинаковым именем группы принадлежат к одной группе.
- **Security Model**
  По умолчанию: SNMPv3
  Описание: SNMPv3 указывает, что принята модель безопасности на основе пользователей (USM). В настоящее время значение должно быть SNMPv3.

Настройка контекстной таблицы

Перейти [Device Advanced Configuration] → [SNMP Configuration] → [V3 Context Table Configuration] для конфигурации контекстной таблицы для V3, как показано на рисунке ниже.

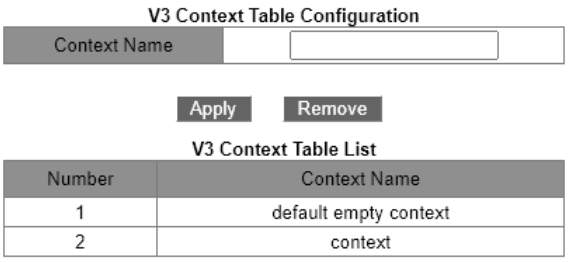
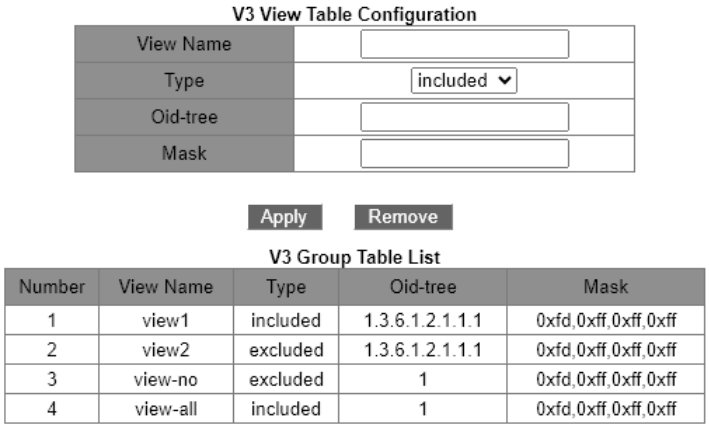


Рис. 116. Настройка контекстной таблицы

- **Context Name**
  Диапазон: 4~16 символов
  Функция: настроить имя контекста.
  Описание: Имя первого контекста должно быть пустым.

Настройка таблицы просмотра

Перейти [Device Advanced Configuration] → [SNMP Configuration] → [V3 View Table Configuration] для конфигурации таблицы просмотра для V3, как показано на рисунке ниже.



Number	View Name	Type	Oid-tree	Mask
1	view1	included	1.3.6.1.2.1.1.1	0xfd,0xff,0xff,0xff
2	view2	excluded	1.3.6.1.2.1.1.1	0xfd,0xff,0xff,0xff
3	view-no	excluded	1	0xfd,0xff,0xff,0xff
4	view-all	included	1	0xfd,0xff,0xff,0xff

Рис. 117. Настройка таблицы просмотра

- **View Name**
  Диапазон: 4~16 символов
  Функция: Настройка имени представления.
- **Type**
  Опции: included / excluded
  По умолчанию: included
  Функция: Included указывает, что текущее представление включает все узлы дерева MIB. Excluded указывает, что текущее представление не включает узлы дерева MIB.
- **oid-tree**
  Функция: MIB-дерево, обозначенное OID корневого узла дерева.
- **Mask**
  Функция: Маска дерева MIB. Oid-дерево и маска вместе определяют информацию об узле MIB текущего представления. Например, на рисунке имя представления «view1» может иметь доступ только к информации узла 1.3.6.1.2.1.1.1, 1.3.6.1.2.1.2.1, 1.3.6.1.2.1.3.1 и 1.3.6.1. 2.1.4.1… 1.3.6.1.2.1.n.1.

Конфигурирование таблицы доступа

Перейти [Device Advanced Configuration] → [SNMP Configuration] → [V3 Access Table Configuration] для конфигурации таблицы доступа для V3, как показано на рисунке ниже.

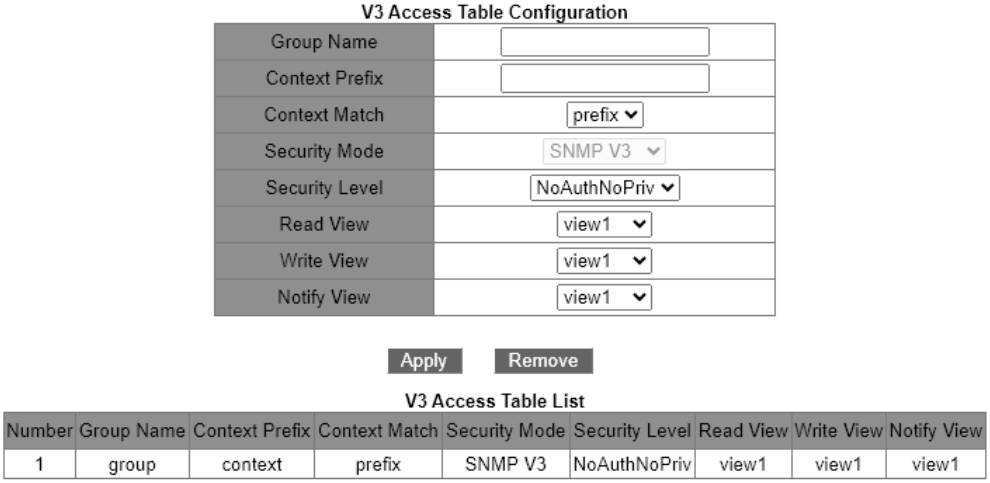


Рис. 118. Конфигурирование таблицы доступа

- **Group Name**
  Диапазон: все существующие имена групп, 4~16 символов
  Функция: Пользователи в группе имеют одинаковые права доступа.
- **Context Prefix**
  Диапазон: все существующие имена контекстов, 4~16 символов
  Функция: настроить имя контекста. Имя группы и имя контекста вместе определяют права доступа группы. Поскольку первое имя контекста в таблице контекстов должно быть пустым, префикс контекста может быть пустым.
- **Context Match**
  Опции: exact / prefix
  По умолчанию: exact
  Функция: выберите режим соответствия имени контекста. Exact указывает, что значение префикса контекста должно совпадать с именем контекста. Префикс указывает, что значение префикса контекста должно совпадать с первыми 4–16 символами имени контекста. В этом случае имена контекстов с одинаковым префиксом имеют одинаковые права доступа.
- **Security Model**
  По умолчанию: SNMP версии 3.
  Описание: SNMPv3 указывает, что принята модель безопасности на основе пользователей (USM). В настоящее время значение должно быть SNMPv3.
- **Security Level**
  Опции: NoAuthNoPriv / AuthNoPriv / AuthPriv
  По умолчанию: NoAuthNoPriv
  Функция: Выберите права доступа к информации MIB.
  Описание: NoAuthNoPriv указывает, что не требуется ни аутентификация, ни шифрование пакетов. AuthNoPriv указывает, что требуется аутентификация, но не шифрование пакетов. AuthPriv указывает, что требуется как аутентификация, так и шифрование пакетов. Когда требуется шифрование, пользователь может получить доступ к указанной информации MIB только в том случае, если алгоритм шифрования и пароль идентичны настроенным в пользовательской таблице.
- **read View**
  Опции: все существующие имена видов
  Функция: Выберите имя представления только для чтения

- **write View**
  Опции: все существующие имена видов
  Функция: Выберите имя представления записи.
- **notify View**
  Опции: все существующие имена видов
  Функция: Выберите имя представления, которое может отправлять сообщение-trap.

Настройка безопасных IP-адресов

Перейти [Device Advanced Configuration] → [SNMP Configuration] → [IP Address of SNMP Manager] для конфигурации безопасных IP-адресов, как показано на рисунке ниже.

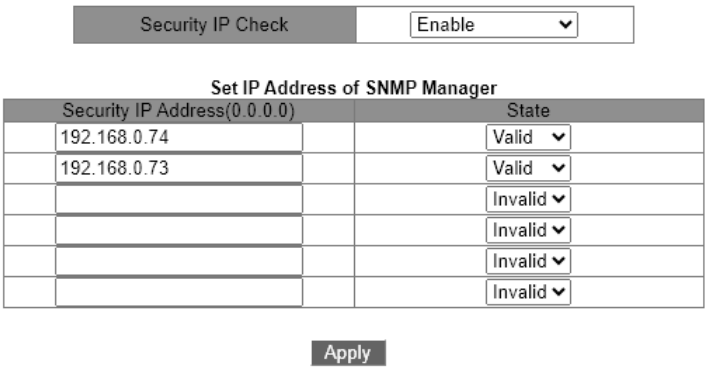


Рис. 119. Настройка безопасных IP-адресов

- **Security IP Check**
  Опция: Enable / Disable
  По умолчанию: Disable
  Функция: включить или отключить проверку безопасности IP. Если проверка безопасности IP отключена, нет ограничений на IP-адрес NMS, любая NMS, подключенная к коммутатору, может получить доступ к информации MIB коммутатора. После того, как проверка IP-адреса безопасности включена, вам необходимо установить IP-адрес безопасности, и только NMS с IP-адресом безопасности может получить доступ к информации MIB коммутатора.
- **IP Address**
  Формат: A.B.C.D.
  Функция: настроить безопасный IP-адрес NMS.
  Описание: Только NMS, чей IP-адрес соответствует IP-адресу безопасности, может получить доступ к информации MIB коммутатора. Коммутатор позволяет использовать максимум 6 IP-адресов безопасности NMS.

Конфигурирование trap

Перейти [Device Advanced Configuration] → [SNMP Configuration] → [TRAP Manager Configuration] для конфигурации trap, как показано на рисунке ниже.

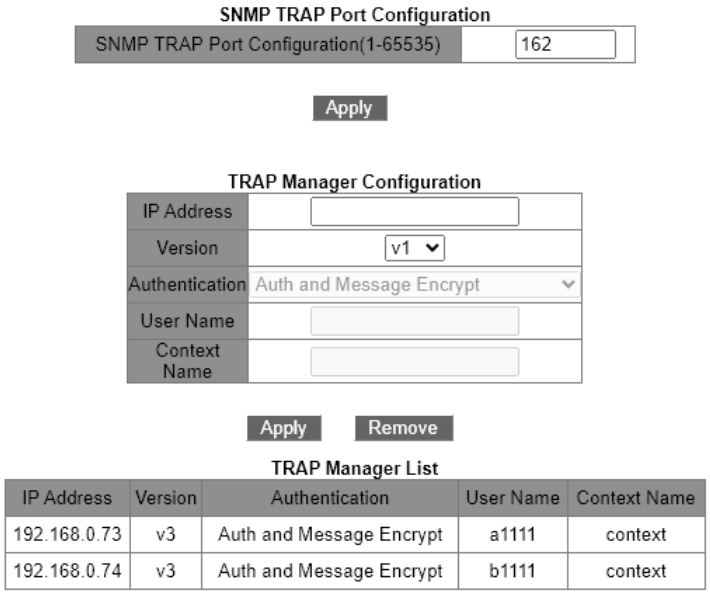


Рис. 120. Конфигурирование trap

- **TRAP Port**
  Опции: 1~65535
  По умолчанию: 162
  Функция: Настройка номера порта для отправки сообщений- trap.
- **Version**
  Опция: V1 / V2C / V3
  Функция: V1 / V2C указывает, что коммутатор отправляет сообщения- trap версии 1 / версии 2C на сервер. V3 указывает, что коммутатор отправляет на сервер сообщения- trap версии 3.
- **Destination IP Address**
  Формат: A.B.C.D.
  Функция: Настройка адреса сервера для получения сообщений- trap. Вы можете настроить максимум 8 серверов, то есть 8 записей- trap.
- **{Security Level, Security Name, Context Name}**
  Опции: {NoAuthNoPriv / AuthNoPriv / AuthPriv, 4~16 символов, 4~16 символов}
  Функция: Эти три параметра необходимо настраивать только при выборе V3. Эти конфигурации должны соответствовать конфигурациям в таблице доступа. Уровень безопасности может быть равен или выше, чем в таблице доступа. Например, когда право доступа пользователя 1111 установлено на AuthNoPriv, коммутатор может отправлять trap на сервер только в том случае, если уровень безопасности имени безопасности 1111 — AuthNoPriv или AuthPriv. Имя контекста должно совпадать с префиксом контекста в таблице доступа.

6.4.4. Типовой пример конфигурации

Станция управления SNMP подключена к коммутатору через Ethernet, IP-адрес станции управления — 192.168.0.23, а IP-адрес коммутатора — 192.168.0.2. Пользователь a1111 и пользователь b2222 контролируют и управляют агентом через SNMPv3, а уровень безопасности принимает AuthNoPriv, который может выполнять операции только для чтения со всей информацией об узле в агенте; когда агент получает сигнал тревоги, он активно отправляет сообщение trap v3 в NMS, как показано на рис. 121;

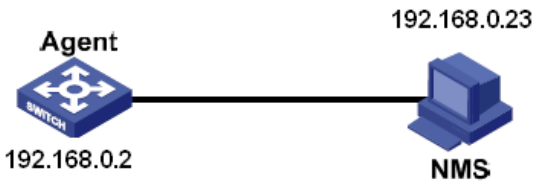


Рис. 121. Пример конфигурации

Конфигурация агента:

- Настройте таблицу пользователей SNMPv3, имя пользователя: a1111, шифрование аутентификации: HMAC-MD5, пароль шифрования аутентификации: aaaa, протокол шифрования сообщений: HMAC-DES, пароль шифрования сообщений: xxxx, имя пользователя: b2222, шифрование аутентификации: HMAC - SHA, пароль шифрования аутентификации: bbbb, протокол шифрования сообщений: HMAC-DES, пароль шифрования сообщений: yyyy, см. рис. 114;
- Создайте групповую таблицу, включающую пользователей a1111 и b2222, см. рис. 115;
- Создайте контекстную таблицу, имя контекста: context, см. рис. 116;
- Создайте представление view-all, включая все узлы, view-no, не включая узлы, см. рис. 117;
- Настройте таблицу доступа SNMPv3, имя группы: group, имя контекста: context, метод сопоставления контекста: prefix, уровень безопасности: AuthNoPriv, представление чтения: view-all, представление записи: view-no, представление уведомлений: view-all, см. рис. 118;
- Включите trap. Настройте запись- trap, версия: V3, IP-адрес назначения: 192.168.0.23, уровень безопасности: AuthPriv, имя безопасности: a1111, имя контекста: context, см. рис. 120.

Если вы хотите контролировать и управлять состоянием агента, вам необходимо запустить соответствующее программное обеспечение для управления на стороне NMS.

6.5. ST-ring

6.5.1. Введение

ST-Ring и ST-Ring+ — это проприетарные протоколы резервирования ООО "Ступинский Электротехнческий Завод ". Время восстановления сети в течение 20 - 50 мс при сбое канала, обеспечивая стабильную и надежную связь. Типы колец ST-ring делятся на два типа: на основе портов (ST-Ring-Port) и на основе VLAN (ST-Ring-VLAN).

- ST-Ring-Port: указывает порт для пересылки или блокировки пакетов.
- ST-Ring-VLAN: указывает порт для пересылки или блокировки пакетов определенной VLAN. Это позволяет использовать несколько VLAN на касательном порту, то есть один порт является частью разных резервных колец, основанных на разных VLAN.

6.5.2. Концепция

- Мастер: У одного кольца есть только один мастер. Мастер отправляет пакеты протокола ST-Ring и определяет состояние кольца. Когда кольцо закрыто, два кольцевых порта на ведущем устройстве находятся в состоянии пересылки (Forwarding) и блокировки (Blocking) соответственно.

Первый порт, статус связи которого меняется на up при закрытии кольца, находится в состоянии пересылки (Forwarding). Другой кольцевой порт находится в состоянии блокировки (Blocking).

- Ведомый: Кольцо может включать в себя несколько ведомых устройств. Подчиненные устройства прослушивают и пересылают пакеты протокола ST-Ring и сообщают информацию об ошибках ведущему устройству.
- Резервный порт: Порт для связи между кольцами ST называется резервным портом.
- Основной резервный порт: если кольцо имеет несколько резервных портов, резервный порт с большим MAC-адресом является основным резервным портом. Он находится в состоянии пересылки.
- Подчиненный резервный порт: если в кольце имеется несколько резервных портов, все резервные порты, кроме основного резервного порта, являются подчиненными резервными портами. Они находятся в состоянии блокировки.
- Состояние пересылки: если порт находится в состоянии пересылки, порт может как получать, так и отправлять данные.
- Состояние блокировки: если порт находится в состоянии блокировки, порт может получать и пересылать только пакеты протокола ST -Ring, но не другие пакеты.

6.5.3. Реализация

6.5.3.1. ST-Ring-Port

Порт пересылки на ведущем устройстве периодически отправляет пакеты протокола ST-Ring для определения состояния кольца. Если блокирующий порт мастера получает пакеты, кольцо замыкается; в противном случае кольцо разомкнуто.

Рабочий процесс коммутатора A, коммутатора B, коммутатора C и коммутатора D:

- Настройте коммутатор A как ведущий, а остальные коммутаторы — как ведомые.
- Кольцевой порт 1 на ведущем устройстве находится в состоянии пересылки, а кольцевой порт 2 — в состоянии блокировки. Оба порта подчиненного устройства находятся в состоянии пересылки.
- Если линк CD неисправен, как показано на следующем рисунке:
  - Когда канал связи CD неисправен, порты 6 и 7 подчиненного устройства находятся в состоянии блокировки. Порт 2 на ведущем устройстве переходит в состояние пересылки, обеспечивая нормальную связь по каналу.
  - Когда неисправность устранена, порты 6 и 7 подчиненного устройства находятся в состоянии пересылки. Порт 2 на ведущем устройстве переходит в состояние блокировки. Происходит переключение каналов, и каналы восстанавливаются до состояния, предшествующего отказу CD.

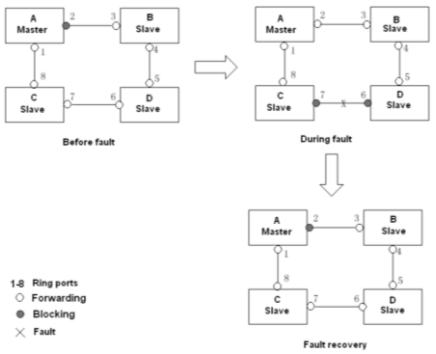


Рис. 122. Пример работы ST-Ring

- Если канал AC неисправен, как показано на следующем рисунке:
  - Когда канал AC неисправен, порт 1 находится в состоянии блокировки, а порт 2 переходит в состояние пересылки, обеспечивая нормальную связь по каналу.
  - После устранения неисправности,
    - Если на ведущем устройстве A не настроен основной порт, порт 1 все еще находится в состоянии блокировки, а порт 8 — в состоянии пересылки. Переключения не происходит.
    - Если порт 1 на мастере A настроен как основной порт. Когда кольцо замкнуто, основной порт должен находиться в состоянии пересылки. Поэтому порт 1 переходит в состояние пересылки. Порт 8 находится в состоянии пересылки, а порт 2 — в состоянии блокировки. Происходит переключение каналов.

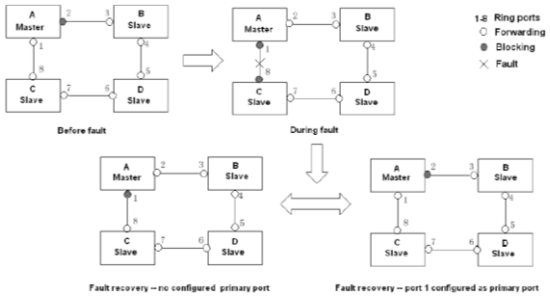


Рис. 123. Пример работы ST-Ring

Изменение статуса канала влияет на статус портов кольца

6.5.3.2. ST-RING-VLAN

ST-Ring-VLAN позволяет пересылать пакеты из разных VLAN по разным путям. Каждый путь пересылки для VLAN образует ST-Ring-VLAN. У разных колец ST-VLAN-Ring могут быть разные мастера. Как показано на следующем рисунке, настроены две ST-Ring-VLAN.

Кольцевые звенья ST-Ring-VLAN 10: AB-BC-CD-DE-EA.

Кольцевые звенья ST-Ring-VLAN 20: FB-BC-CD-DE-EF.

Два кольца касаются звеньев BC, CD и DE. Коммутатор C и коммутатор D используют одни и те же порты в двух кольцах, но используют разные логические каналы на основе VLAN.

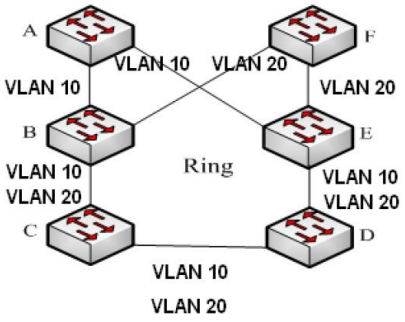


Рис. 124. Пример ST-Ring VLAN

В каждом логическом кольце ST-Ring-VLAN реализация идентична реализации ST-Ring-Port.

6.5.3.3. ST -RING+ реализация

ST-Ring+ может обеспечить резервирование двух колец ST, как показано на следующем рисунке. Один резервный порт настроен соответственно на коммутаторе C и коммутаторе D. Какой порт является основным резервным портом, зависит от MAC-адресов двух портов. Если главный резервный порт или его канал выходят из строя,

подчиненный резервный порт будет пересылать пакеты, предотвращая образование петель и обеспечивая нормальную связь между резервными кольцами.

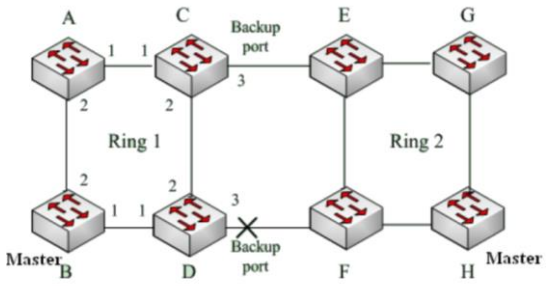


Рис. 125. Пример реализации ST-Ring VLAN

Изменение статуса канала влияет на статус резервных портов.

6.5.4. Описание

Конфигурации ST-Ring должны соответствовать следующим условиям:

- Все коммутаторы в одном кольце должны иметь одинаковый номер домена.
- Каждое кольцо может иметь только одного ведущего и несколько ведомых.
- На каждом коммутаторе можно настроить только два порта для кольца.
- Для двух связанных колец резервные порты можно настроить только в одном кольце.
- В одном кольце можно настроить не более двух резервных портов.
- На коммутаторе для одного кольца можно настроить только один резервный порт.
- ST-Ring-Port и ST-Ring-VLAN нельзя настроить на одном коммутаторе одновременно.

6.5.5. Веб конфигурирование

Конфигурирование кольцевой топологии

Перейти [Device Advanced Configuration] → [ST-Ring Configuration] → [ST-Ringlink_Mode] для конфигурации кольцевой топологии, как показано на рисунке ниже.

Рис. 126. Конфигурирование кольцевой топологии

- **Redundancy Mode Set**
  Опции: DISABLE / ST-PORT / ST-VLAN
  По умолчанию: ST-PORT

Функция: следует ли включить протокол ST-Ring и выбрать режим резервного звонка.

Кольцевые протоколы на основе портов включают RSTP, ST-Ring-Port и STRP-Port, а кольцевые протоколы на основе VLAN включают MSTP, ST-Ring-VLAN и STRP-VLAN. Кольцевые протоколы на основе VLAN являются взаимоисключающими, и для одного устройства можно настроить только тип кольцевого протокола на основе VLAN. Кольцевой протокол на основе портов и кольцевой протокол на основе VLAN являются взаимоисключающими, и для одного устройства можно выбрать только один режим кольцевого протокола.

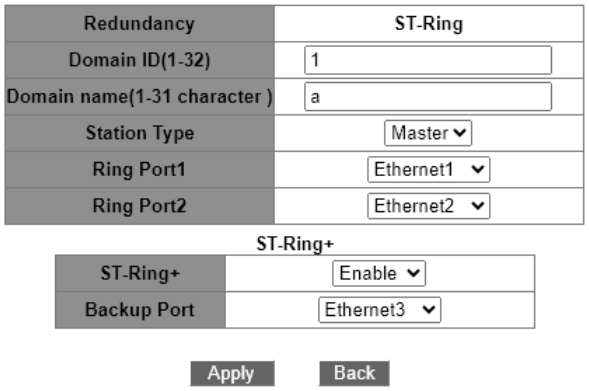
Создание ST-Ring

Перейти [Device Advanced Configuration] → [ST-Ring Configuration] → [ST-Ringlink_configure] для конфигурации ST-Ring, как показано на рисунке ниже.

Рис. 127. Создание ST-Ring

Нажмите <Add>, чтобы создать ST-Ring.

Конфигурирование ST-ring и ST-VLAN-Ring, как показано на рисунке ниже.



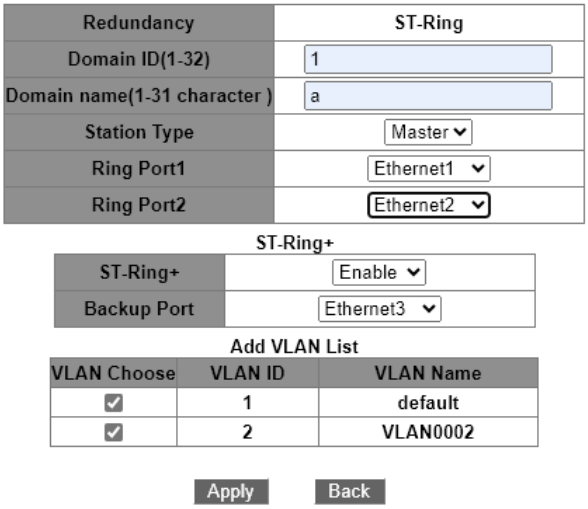


Рис. 128. Конфигурирование ST-Ring и ST-VLAN-Ring

- **Redundancy**
  Принудительная настройка: ST-Ring
- **Domain ID**
  Диапазон конфигурации: 1~32
  Функция: Идентификатор домена используется для различения различных колец. Один коммутатор поддерживает максимум 16 колец на основе портов или 8 колец на основе VLAN.
- **Domain name**
  Диапазон: 1~31 символ
  Функция: настроить доменное имя.
- **Station Type**
  Варианты: Master / Slave
  По умолчанию: Master
  Функция: выберите роль коммутатора в кольце.
- **Ring port 1/Ring port 2**
  Опции: все порты коммутатора
  Функция: выберите два кольцевых порта.

Кольцевой порт ST-Ring, резервный порт и канал агрегации являются взаимоисключающими. Кольцевой порт ST-Ring или резервный порт нельзя добавить к группе агрегации; порты, добавленные в группу агрегации, не могут быть настроены как кольцевые порты ST-Ring и резервные порты.

Кольцевой порт ST-Ring, резервный порт и порт для зеркалирования являются взаимоисключающими. Кольцевой порт ST-Ring или резервный порт нельзя настроить в качестве зеркального порта назначения; порт назначения зеркалирования не может быть настроен в качестве кольцевого порта ST-Ring или резервного порта.

Кольцевые порты между кольцевыми протоколами на основе портов RSTP, ST-Ring-Port и STRP-Port являются взаимоисключающими, то есть кольцевой порт и резервный порт ST-Ring-Port не могут быть настроены как порт RSTP, кольцо STRP-Port. порт или резервный порт STRP-Port; Порт RSTP, кольцевой порт STRP-Port и резервный порт STRP-Port нельзя настроить как кольцевой порт ST-Ring-Port или резервный порт.

Не рекомендуется одновременно настраивать порты в той же группе изоляции, что и кольцевые порты ST-Ring и резервные порты, а порты ST-Ring и резервные порты не следует добавлять в одну и ту же группу изоляции.

- **ST-RING+**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: Включить / выключить ST-Ring+.
- **Backup port**
  Опции: все порты коммутатора
  Функция: Установите порт в качестве резервного порта.
  Объяснение: Включите ST-Ring+ перед настройкой резервного порта.
- **Add VLAN list**
  Опции: все созданные VLAN
  Функция: выберите VLAN для кольцевого порта.

  После завершения настройки в списке ST-Ring List отображаются все созданные кольца, как показано на рисунке ниже.

Рис. 129. Список колец ST-Ring

Просмотр и изменение конфигурации ST-Ring

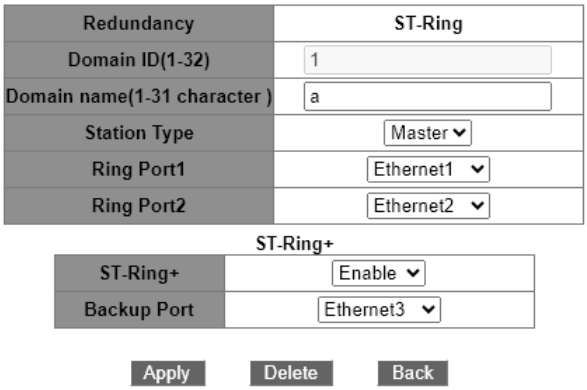


Рис. 130. Просмотр и изменение конфигурации ST-Ring

Нажмите <Apply>, чтобы изменения вступили в силу после внесения изменений. Нажмите <Delete>, чтобы удалить запись конфигурации ST-Ring.

Просмотр ST-Ring и статус порта

ST-Ring State List

Redundancy	ST-Ring
Ring Port1	forwarding
Ring Port2	blocking
Ring State	RING-CLOSE

Redundancy	ST-Ring+
Equipment IP	192.168.0.1
Equipment MAC	00-1e-cd-5b-db-73
BackupPort Status	blocking

Рис. 131. Просмотр ST-Ring и статус порта

6.5.6. Пример типовой конфигурации

Как показано на рис. 125, A, B, C и D образуют кольцо Ring1, E, F, G и H образуют кольцо Ring2, а CE и DF являются резервными соединениями между Ring1 и Ring2.

Процесс настройки коммутатора A:

- Идентификатор домена: 1, имя домена: Ring, выбор порта кольца 1 и 2, тип станции: подчиненная станция, ST-Ring+ отключен, нет необходимости настраивать резервный порт, см. рис. 128;

Процесс настройки коммутатора B:

- Идентификатор домена: 1, имя домена: Ring, выбор портов кольца 1 и 2, тип станции: главная станция, ST-Ring+ не включен, нет необходимости настраивать резервный порт, см. рис. 128;

Процесс настройки коммутатора C, D:

- Идентификатор домена: 1, имя домена: Ring, выбор портов кольца 1 и 2, тип станции: ведомая станция, включение ST-Ring+, выбор резервного порта 3, см. рис. 128;

Процесс настройки коммутатора E, F, G:

- ID домена: 2, имя домена: Ring, выбор порта кольца 1 и 2, тип станции: подчиненная станция, ST-Ring+ не включен, нет необходимости настраивать резервный порт, см. рис. 128;

Процесс настройки коммутатора H:

- Идентификатор домена: 2, имя домена: Ring, выбор портов кольца 1 и 2, тип станции: главная станция, ST-Ring+ отключен, нет необходимости настраивать резервный порт, см. рис. 128.

6.6. STP / RSTP

6.6.1. Введение

Стандартизированный в IEEE802.1D протокол связующего дерева (Spanning Tree Protocol - STP) представляет собой протокол локальной сети, используемый для предотвращения широковещательных штормов, вызванных петлями канала, и обеспечения резервирования канала. Устройства с поддержкой STP обмениваются пакетами и блокируют определенные порты, чтобы сократить «петли» на «деревья», предотвращая распространение и бесконечные петли. Недостаток STP заключается в том, что порт должен ждать в два раза больше задержки пересылки, чтобы перейти в состояние пересылки.

Чтобы преодолеть этот недостаток, IEEE создал стандарт 802.1w в дополнение к 802.1D. IEEE802.1w определяет протокол быстрого связующего дерева (Rapid Spanning Tree Protocol - RSTP). По сравнению с STP, RSTP достигает гораздо более быстрой конвергенции, добавляя альтернативный порт и резервный порт для корневого порта и назначенного порта соответственно. Если корневой порт недействителен, альтернативный порт может быстро войти в состояние пересылки.

6.6.2. Основные понятия

- Root bridge: служит root для сети. Сеть имеет только один root bridge. Root bridge меняется в зависимости от топологии сети. Root bridge периодически отправляет BPDU другим устройствам, которые пересылают BPDU для обеспечения стабильности топологии.
- Root port: указывает наилучший порт для передачи от некорневых мостов к корневому мосту. Лучший порт — это порт с наименьшей стоимостью для корневого моста. Non-root bridge взаимодействует с root bridge через root port. Non-root bridge имеет только один root port. Root bridge не имеет root port.
- Designated port: указывает порт для пересылки BPDU на другие устройства или локальные сети. Все порты root bridge являются designated port.
- Alternate port: указывает резервный порт root port. Если root port выходит из строя, alternate port становится новым root port.
- Backup port: указывает backup port назначенного порта. Когда designated port выходит из строя, backup port становится новым designated port и пересылает данные.

6.6.3. BPDU

Для предотвращения образования петель все мосты локальной сети вычисляют связующее дерево. Процесс вычисления включает в себя передачу BPDU между устройствами для определения топологии сети. В таблице ниже показана структура данных BPDU.

Таблица 5. Структура данных BPDU

…	Root bridge ID	Root path cost	Designated bridge ID	Designated port ID	Message age	Max age	Hello time	Forward delay	…
…	8 bytes	4 bytes	8 bytes	2 bytes	2 bytes	2 bytes	2 bytes	2 bytes	…

- Root bridge: приоритет корневого моста (2 байта) + MAC-адрес корневого моста (6 байт).
- Root path: стоимость пути к корневому мосту.
- Designation bridge ID: приоритет назначенного моста (2 байта) + MAC-адрес назначенного моста (6 байт).
- Designation port ID: приоритет порта + номер порта.
- Message age: время, в течение которого BPDU может распространяться по сети.
- Max age: максимальная продолжительность хранения BPDU на устройстве. Когда возраст сообщения превышает максимальный возраст, BPDU отбрасывается.
- Hello time: интервал для отправки BPDU.
- Forward delay: задержка изменения статуса (отбрасывание-обучение-пересылка).

6.6.4. Процесс реализации

Конкретный процесс для всех мостов, вычисляющий связующее дерево с помощью BPDU, выглядит следующим образом:

Начальная фаза - каждый порт всех устройств генерирует конфигурационное сообщение (BPDU) с самим собой в качестве корневого моста, идентификатор корневого моста — это собственный идентификатор устройства, стоимость корневого пути равна 0, идентификатор назначенного моста — это идентификатор его собственного устройства, а назначенный порт есть собственный порт.

- Выбор лучшего BPDU - все устройства отправляют свои собственные BPDU и получают BPDU от других устройств. При получении BPDU каждый порт сравнивает полученный BPDU со своим.
  - если приоритет собственного BPDU выше, то порт не выполняет никаких операций;
  - если приоритет полученного BPDU выше, то порт заменяет локальный BPDU полученным.

Устройства сравнивают BPDU всех портов и определяют лучший BPDU. Принципы сравнения BPDU следующие:

- BPDU с меньшим идентификатором корневого моста имеет более высокий приоритет.
- Если идентификаторы корневого моста двух BPDU совпадают, сравнивается их стоимость корневого пути. Если стоимость корневого пути в BPDU плюс стоимость пути локального порта меньше, приоритет BPDU выше.

- Если стоимость корневого пути двух BPDU также одинакова, назначенные идентификаторы моста, назначенные идентификаторы портов и идентификаторы порта, получающего BPDU, дополнительно сравниваются по порядку. BPDU с меньшим идентификатором имеет более высокий приоритет. BPDU с меньшим идентификатором корневого моста имеет более высокий приоритет.

- Выбор root bridge - root bridge связующего дерева является мост с наименьшим идентификатором моста.
- Выбор root port - устройство без корневого моста выбирает порт, получающий лучший BPDU, в качестве корневого порта.
- Расчет BPDU designated port - на основе BPDU корневого порта и стоимости пути корневого порта устройство вычисляет BPDU designated port для каждого порта следующим образом:
  - Замените идентификатор корневого моста идентификатором корневого моста BPDU корневой порт.
  - Замените стоимость корневого пути на стоимость корневого пути BPDU корневого порта плюс стоимость пути корневого порта.
  - Замените назначенный идентификатор моста идентификатором локального устройства.
  - Замените назначенный идентификатор порта идентификатором локального порта.
- Выбор designated port - Если рассчитанный BPDU лучше, то устройство выбирает порт в качестве назначенного порта, заменяет BPDU порта рассчитанным BPDU и отправляет рассчитанный BPDU. Если BPDU порта лучше, то устройство не обновляет BPDU порта и блокирует порт. Заблокированные порты могут получать и пересылать только пакеты RSTP, но не другие пакеты.

6.6.5. Веб конфигурирование

Включение RSTP

Перейти [Device Advanced Configuration] → [RSTP configuration] → [RSTP configuration] для конфигурации RSTP, как показано на рисунке ниже.

RSTP Configuration

Protocol Status	Disable	
Bridge Priority	32768	(0-65535)
Hello Time(s)	2	(1-10)
Max Age Time(s)	20	(6-40)
Forward Delay Time(s)	15	(4-30)
Message-age Increment	Default	

Apply

Рис. 132. Включение RSTP

- **Protocol Status**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: выключение или включение протокола RSTP.

Кольцевые протоколы на основе портов включают RSTP, ST-Ring-Port и STRP-Port, а кольцевые протоколы на основе VLAN включают MSTP, ST-Ring-VLAN и STRP-VLAN. Кольцевой протокол на основе портов и кольцевой протокол на основе VLAN являются взаимоисключающими, и для одного устройства можно выбрать только один режим кольцевого протокола.

Установка временных параметров сетевого моста

- **Bridge Priority**
  Диапазон: 0~65535. Шаг 4096.
  По умолчанию: 32768
  Функция: настройка приоритета сетевого моста.
  Описание: Приоритет используется для выбора корневого моста. Чем меньше значение, тем выше приоритет.
- **Hello time**
  Диапазон: 1~10 с
  По умолчанию: 2 с
  Функция: Настройка интервала отправки BPDU.
- **Max age time**
  Диапазон: 6~40 с
  По умолчанию: 20 с
  Описание: Если значение возраста сообщения в BPDU превышает указанное значение, то BPDU отбрасывается.
- **Forward Delay Time**
  Диапазон: 4~30 с
  По умолчанию: 15 с
  Функция: настройка времени изменения статуса с «Discarding» на «Learning» или с «Learning» на «Forwarding».
- **Message-age Increment**
  Варианты: Compulsion / Default
  По умолчанию: Default
  Функция: Настройте значение, которое будет добавляться к возрасту сообщения, когда BPDU проходит через сетевой мост.
  Описание: В принудительном режиме значение равно 1.
  В режиме по умолчанию значение равно max (max age time / 16, 1).
  Forward Delay Time, Max Age Time и Hello Time должны соответствовать следующим требованиям: 2 x (Forward Delay Time — 1,0 секунды) ≥ Max Age Time;
  Max Age Time ≥ 2 x (Hello Time + 1,0 секунды).

Включение RSTP на портах, показано на рисунке ниже.

Port Configuration

Port	Type	Protocol Status	Port Priority(0~255)	Auto Cost Count	Path Cost(1~200000000)
Ethernet1	GE	☑	128	☑	20000
Ethernet2	GE	☑	128	☑	20000
Ethernet3	GE	☑	128	☑	2000000
Ethernet4	GE	☑	128	☑	2000000
Ethernet5	GE	☐	128	☑	2000000
Ethernet6	GE	☐	128	☑	2000000
Ethernet7	GE	☐	128	☑	2000000
Ethernet8	GE	☐	128	☑	2000000
Ethernet9	GE	☐	128	☑	2000000
Ethernet10	GE	☐	128	☑	2000000
Ethernet11	GE	☐	128	☑	2000000
Ethernet12	GE	☐	128	☑	2000000
Ethernet13	GE	☐	128	☑	2000000
Ethernet14	GE	☐	128	☑	2000000
Ethernet15	GE	☐	128	☑	2000000
Ethernet16	GE	☐	128	☑	2000000
Ethernet17	GE	☐	128	☑	2000000
Ethernet18	GE	☐	128	☑	2000000
Ethernet19	GE	☐	128	☑	2000000
Ethernet20	GE	☐	128	☑	2000000
Ethernet21	GE	☐	128	☑	2000000
Ethernet22	GE	☐	128	☑	2000000
Ethernet23	GE	☐	128	☑	2000000
Ethernet24	GE	☐	128	☑	2000000
Ethernet25	GX	☐	128	☑	2000000
Ethernet26	GX	☐	128	☑	2000000
Ethernet27	GX	☐	128	☑	2000000
Ethernet28	GX	☐	128	☑	2000000

Apply

Рис. 133. Включение RSTP на портах

- **Protocol Status**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: Включение / выключение STP / RSTP на портах

Порт RSTP и channel порт являются взаимоисключающими. Порт RSTP нельзя добавить в группы агрегации; порт, добавленный в группу агрегации не может быть настроен как порт RSTP.
Порт RSTP и порт назначения зеркалирования являются взаимоисключающими. Порт RSTP нельзя настроить как порт назначения зеркалирования; порт назначения зеркалирования не может быть настроен как порт RSTP.
Кольцевые порты между кольцевыми протоколами на основе портов RSTP, ST-Ring-Port и STRP-Port являются взаимоисключающими, то есть порт RSTP нельзя настроить как кольцевой порт STRP-Port / ST-Ring-Port или STRP-Port / ST-Ring-Port резервный порт; Кольцевой порт STRP-Port / ST-Ring-Port и резервный порт STRP-Port / ST-Ring-Port нельзя настроить как порт RSTP.
Не рекомендуется одновременно настраивать порты в группе изоляции как порты RSTP, а порты RSTP нельзя добавлять в группу изоляции.

- **Port Priority**
  Диапазон: 0~255. Шаг 16.

По умолчанию: 128

Функция: Настройка приоритета порта, который определяет роли портов.

- **Path Cost**

  Диапазон: 1~200000000

  По умолчанию: 2000000 (порт 10M), 200000 (порт 100M), 20000 (порт 1000M)

  Описание: Стоимость пути порта используется для расчета наилучшего пути. Значение параметра зависит от пропускной способности. Чем больше значение, тем ниже стоимость. Вы можете изменить роль порта, изменив значение параметра стоимости пути. Чтобы настроить значение вручную, выберите No для счетчика затрат.

- **Auto Cost Count**

  Диапазон: Yes / No

  По умолчанию: Yes

  Описание: Yes указывает, что стоимость пути порта принимает значение по умолчанию. No означает, что вы можете настроить стоимость пути.

Просмотр RSTP статуса, показано на рисунке ниже.

Root Info

Root MAC	0:1e:cd:5b:db:73
Root Priority	32768
Root Path Cost	0
Root Port	None
Max Age(s)	20
Hello Time(s)	2
Forward Delay(s)	15

Bridge Info

Bridge MAC	0:1e:cd:5b:db:73
Bridge Priority	32768
Bridge Version	2
Max Age(s)	20
Hello Time(s)	2
Forward Delay(s)	15

Port Info

Port	Priority	Path Cost	Role	State	Link State
1	128	20000	Designated	Forwarding	Up
2	128	20000	Backup	Discarding	Up
3	128	2000000	Disabled	Discarding	Down
4	128	2000000	Disabled	Discarding	Down

Рис. 134. Просмотр RSTP статуса

6.6.6. Пример типовой конфигурации

Приоритеты коммутаторов A, B и C равны 0, 4096 и 8192 соответственно, а стоимость пути каждого канала равна 4, 5 и 10, как показано на рис. 135;

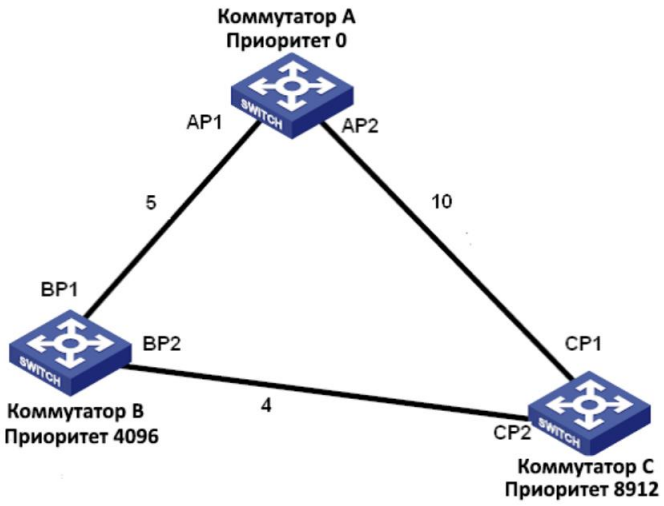


Рис. 135. Пример конфигурации

Конфигурация коммутатора A:

- Приоритет равен 0, а для параметра времени установлено значение по умолчанию, см. рис. 132;
- Стоимость пути порта 1 равна 5, а стоимость пути порта 2 равна 10, см. рис. 133;

Конфигурация коммутатора B:

- Приоритет равен 4096, а для параметра времени установлено значение по умолчанию, см. рис. 132;
- Стоимость пути порта 1 равна 5, а стоимость пути порта 2 равна 4, см. рис. 133;

Конфигурация коммутатора C:

- Приоритет равен 8192, а для параметра времени установлено значение по умолчанию, как показано на рис. 132;
- Стоимость пути порта 1 равна 10, а стоимость пути порта 2 равна 4, см. рис. 133;

Приоритет коммутатора A равен 0, идентификатор моста наименьший, и он выбран в качестве корневого моста;

Стоимость пути от AP1 к BP1 равна 5, а стоимость пути от AP2 к BP2 равна 14, поэтому BP1 выбран в качестве корневого порта;

Стоимость пути от AP1 до CP2 равна 9, а стоимость пути от AP2 до CP1 равна 10, поэтому выберите CP2 в качестве корневого порта и BP2 в качестве назначенного порта.

6.7. STRP

6.7.1. Введение

STRP — это протокол защиты от избыточности при передаче данных, предложенный нашей компанией для кольцевой топологии. Когда кольцо Ethernet закрыто, протокол может предотвратить широковещательный шторм, вызванный кольцом данных, и отказ канала или отказ узла происходит в кольцевой сети.В случае сбоя он может переключиться на резервный канал в режиме реального времени, чтобы обеспечить нормальную передачу пакетов данных.

В соответствии со стандартом IEC 62439-6 STRP использует механизм выбора мастера без фиксированного мастера. STRP предоставляет следующие возможности:

- Время восстановления, не зависящее от масштаба сети.
  STRP обеспечивает время восстановления, не зависящее от масштаба сети, за счет оптимизации механизма пересылки пакетов обнаружения кольца. STRP позволяет сетям восстанавливаться в течение 20 мс благодаря введению прерывания отчетов в реальном времени, что повышает надежность передачи данных в реальном времени. Эта функция позволяет коммутаторам обеспечивать более высокую надежность для приложений в энергетике, железнодорожном транспорте и многих других отраслях, требующих управления в режиме реального времени.

- Разнообразные функции обнаружения ссылок.
  Для повышения стабильности сети STRP предоставляет разнообразные функции обнаружения каналов для типичных сетевых сбоев, включая обнаружение быстрого отключения, обнаружение однонаправленных каналов оптоволокна, проверку качества каналов и проверку работоспособности оборудования, обеспечивая надлежащую передачу данных.

- Применимо к нескольким сетевым топологиям.
  Помимо быстрого восстановления для простых кольцевых сетей, STRP также поддерживает сложные кольцевые топологии, такие как пересекающиеся кольца и касательные кольца. Кроме того, STRP поддерживает несколько экземпляров на основе VLAN, что подходит для различных сетевых приложений с гибкой сетью.

- Мощные функции диагностики и обслуживания.
  STRP предоставляет мощные механизмы запросов о состоянии и сигналов тревоги для диагностики и обслуживания сети, а также механизм предотвращения непреднамеренных операций и неправильных конфигураций, которые могут привести к кольцевым сетевым штормам.

6.7.2. Концепция

STRP включает два режима: STRP-Port-Based и STRP-VLAN-Based.

STRP-Port-Based: перенаправляет или блокирует пакеты на основе определенных портов.

STRP-VLAN-Based: перенаправляет или блокирует пакеты на основе VLAN. Если порт находится в состоянии блокировки, блокируются только пакеты данных указанной сети VLAN. Таким образом, на портах касательного кольца можно настроить несколько VLAN. Порт может принадлежать разным кольцам STRP в соответствии с конфигурациями VLAN.

6.7.3. Состояние портов STRP

Forwarding state: если порт находится в состоянии пересылки, он может получать и пересылать пакеты данных.
Blocking state: если порт находится в состоянии блокировки, он может получать и пересылать пакеты STRP, но не другие пакеты данных.
Primary port: указывает кольцевой порт (в корневом каталоге), состояние которого настроено как принудительная переадресация пользователем, когда кольцо закрыто.

6.7.4. Роль устройства STRP

STRP определяет роли коммутаторов, пересылая пакеты Announce, предотвращая образование петель в кольцах избыточности.

INIT: указывает устройство, на котором включен STRP, а два кольцевых порта находятся в состоянии Link down.

ROOT: указывает устройство, на котором включен STRP, и по крайней мере один кольцевой порт находится в состоянии соединения. В кольце root выбирается в соответствии с векторами пакетов Announce. Это может измениться в зависимости от топологии сети. Root периодически отправляет свои собственные пакеты Announce на другие устройства. Статусы кольцевых портов: Один кольцевой порт находится в состоянии пересылки, а другой — в состоянии блокировки. Получив пакет Announce от другого устройства, Root сравнивает вектор пакета с вектором своего собственного пакета Announce. Если вектор полученного пакета больше, Root меняет свою роль на Normal или B-Root в зависимости от состояния канала и ухудшения CRC портов.

B-Root: указывает устройство, на котором включен STRP, отвечающее хотя бы одному из следующих условий: один кольцевой порт находится в состоянии соединения, а другой — в состоянии соединения, деградация CRC, приоритет не менее 200. B-Root сравнивает и пересылает пакеты Announce. Если вектор полученного пакета Announce меньше вектора его собственного пакета Announce, B-Root меняет свою роль на Root; в противном случае он пересылает полученный пакет и не меняет свою роль. Статусы портов кольца: Один порт кольца находится в состоянии пересылки.

Normal: указывает устройство, на котором включен STRP, и оба кольцевых порта находятся в состоянии соединения без ухудшения CRC, а приоритет выше 200. Нормальный только пересылает пакеты Announce, но не проверяет содержимое

пакетов. Статусы кольцевых портов: Оба кольцевых порта находятся в состоянии пересылки.

Ухудшение CRC: указывает, что количество пакетов CRC превышает пороговое значение за 15 минут.

6.7.5. Реализация

Каждый коммутатор поддерживает свой собственный вектор пакета Announce. Коммутатор с большим вектором будет выбран корневым.

Вектор пакета Announce содержит следующую информацию для назначения роли.

Таблица 6. Вектор пакета Announce

Link status	CRC degradation		Role priority	IP address of the device	MAC address of the device
	CRC degradation status	CRC degradation rate			

Link status: Значение устанавливается равным 1, если один кольцевой порт находится в состоянии Link down, и устанавливается в 0, если оба кольцевых порта находятся в состоянии Link up.

Статус деградации CRC: если деградация CRC происходит на одном порту, значение устанавливается равным 1. Если деградация CRC не происходит на двух кольцевых портах, значение устанавливается равным 0.

Скорость деградации CRC: отношение количества пакетов CRC к порогу за 15 минут. Role priority: значение можно установить в веб-интерфейсе.

Параметры в табл. 6 сравниваются в следующей процедуре:

- Сначала проверяется значение статуса канала. Устройство с большим значением статуса канала считается имеющим больший вектор.
- Если два сравниваемых устройства имеют одинаковое значение состояния канала, сравниваются значения состояния ухудшения CRC. Устройство с большим значением статуса деградации CRC считается имеющим больший вектор.
- Если значение статуса деградации CRC всех сравниваемых устройств равно 1, считается, что устройство с большим значением скорости деградации CRC имеет больший вектор. Если два сравниваемых устройства имеют одинаковое значение состояния канала и значение деградации CRC, значения приоритета ролей, IP-адресов и MAC-адресов сравниваются последовательно. Устройство с большим значением считается имеющим больший вектор.
- Устройство с большим вектором выбирается корневым.

Только когда значение состояния деградации CRC равно 1, значение скорости деградации CRC участвует в сравнении векторов. В противном случае векторы сравниваются независимо от значения скорости деградации CRC.

Реализация режима STRP-Port-Based.

Процесс выбора роли коммутатора выглядит следующим образом:

- В исходном состоянии все коммутаторы находятся в состоянии INIT. Когда порт Linked, роль переключается на Root, Root отправляет и получает сообщения Announce для выборов, а роль порта выбирается путем сравнения векторов Announce сообщения;
- Коммутатор, который подключается к кольцевому сетевому соединению и имеет наибольший вектор сравнения сообщений Announce, выбирается корневым, среди остальных коммутаторов, если кольцевой порт коммутатора находится в состоянии Link down или CRC ухудшен, роль устройство является корневым B. Если у коммутатора оба кольцевых порта подключены и нет ухудшения CRC, роль устройства Normal.

Процесс восстановления после сбоя коммутатора показан на рис. 136:

- В исходной топологии A является корнем; порт 1 находится в состоянии пересылки, а порт 2 в состоянии блокировки. B, C и D являются нормальными, и их кольцевые порты находятся в состоянии пересылки.
- При отключении линка CD по протоколу STRP кольцевые порты 6 и 7 коммутаторов C и D устанавливаются в состояние блокировки, а роли C и D переключаются на Root, Root A, Root C и корень D все рассылают Для каждого сообщения Announce, поскольку связь между корнем C и корнем D отключена, вектор сравнения в это время должен быть больше, чем вектор сравнения корня A. Предполагая, что вектор сравнения D больше, чем C, D выбирается корневым, а роль C переключается на B-Root, после получения сообщения Announce от D, A обнаруживает, что он больше, чем его собственный вектор сравнения, и все его кольцевые порты подключены, поэтому он переключает роль на Обычную и переводит кольцевой порт 2 в состояние пересылки.
- После восстановления канала CD вектор сравнения Root D все еще больше, чем у B-Root C, а роль коммутатора D остается как Root.

    - Если на D не настроен основной порт, порт 7 по-прежнему находится в состоянии блокировки, а порт 8 — в состоянии пересылки.
    - Если порт 7 на D настроен как основной порт, порт 7 переходит в состояние пересылки, а порт 8 — в состояние блокировки.

STRP изменяет состояние порта 6 на пересылку. В результате C становится Normal. Поэтому роли коммутаторов не меняются при восстановлении канала.

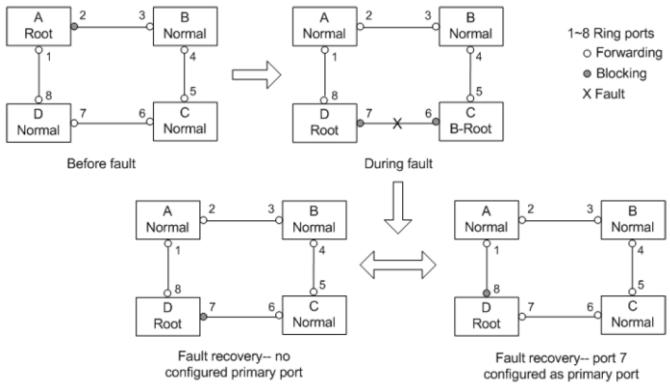


Рис. 136. Процесс восстановления после сбоя

В кольцевой сети STRP роли коммутаторов меняются при сбое канала, но не меняются при восстановлении канала. Этот механизм повышает безопасность сети и надежность передачи данных.

Реализация режима STRP-VLAN-Based

STRP-VLAN-Based устанавливает сопоставление между VLAN и экземпляром STG. Одна или несколько сетей VLAN могут быть сопоставлены с одним экземпляром STG. Экземпляр STG: каждый экземпляр STG соответствует одному кольцу на основе STRP-VLAN. С помощью STRP экземпляр STG записывает роли устройств и состояние порта. После получения пакета коммутатор определяет сопоставленный экземпляр STG на основе атрибута VLAN пакета. Коммутатор обрабатывает пакет в соответствии с ролями устройства и статусом порта экземпляра.

При настройке кольца на основе STRP-VLAN пакеты из разных VLAN могут пересылаться по разным путям. Как показано на рисунке ниже, сопоставление экземпляров STG и VLAN одинаково для всех устройств.

Кольцевая ссылка на базе STG1: AB-BC-CD-DE-EA. Пакеты VLAN10 и VLAN20 пересылаются по каналу A — root.

Кольцевая ссылка на базе STG2: FB-BC-CD-DE-EF. Пакеты VLAN30 пересылаются по каналу F — root.

Два кольца касаются звеньев BC, CD и DE. Коммутатор C и коммутатор D используют одни и те же порты в двух кольцах, но используют разные логические каналы на основе VLAN.

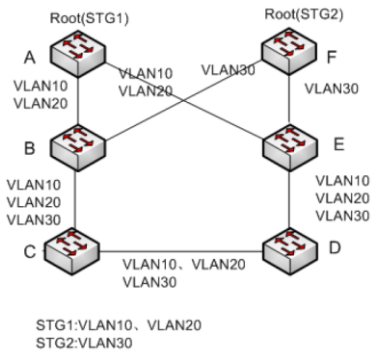


Рис. 137. Пересылка пакетов по разным VLAN

Состояние порта и назначение ролей для каждого кольца на основе STRP-VLAN такие же, как и для кольца на основе порта STRP.

STRP Backup

STRP также может обеспечивать резервирование двух колец STRP, предотвращая образование петель и обеспечивая нормальную связь между кольцами.

Backup port: указывает порт связи между кольцами STRP. Можно настроить несколько резервных портов, но они должны находиться в одном кольце. Первый резервный порт, который подключается, является основным резервным портом,

который находится в состоянии пересылки. Все остальные резервные порты являются подчиненными. Они находятся в состоянии блокировки.

Как показано на следующем рисунке, на каждом коммутаторе можно настроить один резервный порт. Главный резервный порт находится в состоянии пересылки, а другие резервные порты — в состоянии блокировки. Если главный резервный порт или его канал неисправен, для пересылки данных будет выбран подчиненный резервный порт.

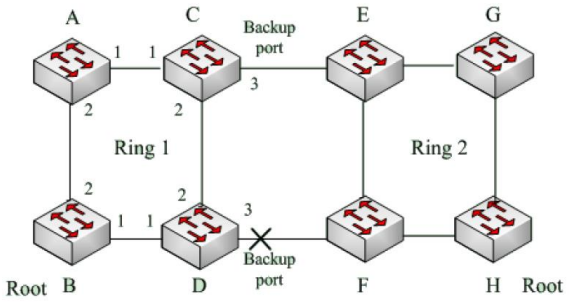


Рис. 138. Резервирование двух колец

Изменение статуса канала влияет на статус резервных портов.

6.8. DHP

6.8.1. Введение

DHP (Dual Homing Protocol - протокол двойного подключения): это протокол канала двойного подключения. Как показано на следующем рисунке, A, B, C и D смонтированы на кольце. DHP реализует следующие функции, если он включен на A, B, C и D.

- A, B, C и D могут взаимодействовать друг с другом, не влияя на правильную работу устройств в кольце.
- Когда линия между соединительными устройствами AB отключена, устройство A все еще может обеспечить нормальную передачу данных с B, C и D через соединение между 1 и 2 в кольцевой сети и реализовать связь между A, B и D. Функция резервного копирования для ссылок C и D.

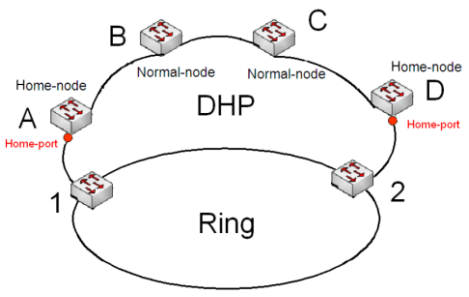


Рис. 139. Пример применения DHP

6.8.2. Концепция

Реализация DHP основана на STRP. Механизм выбора и назначения ролей в DHP такой же, как и в STRP. DHP обеспечивает резервное копирование канала посредством конфигурации Home-node, Normal-node и Home-port.
Home-node: указывает устройства на обоих концах канала DHP и завершает пакеты STRP. Home-node: указывает порт, соединяющий домашний узел с внешней сетью. Домашний порт обеспечивает следующие функции:

- Отправка ответных пакетов в корневой узел после получения пакетов оповещения из корневого узла. Корень идентифицирует состояние кольца как закрытое, если он получает ответные пакеты. Если корень не получает ответные пакеты, он идентифицирует состояние кольца как открытое.
- Блокировка пакетов STRP внешних сетей и изоляция канала DHP от внешних сетей. Отправка пакетов очистки входа на подключенные устройства во внешних сетях при изменении топологии канала DHP.

Normal-node: указывает устройства в канале DHP, исключая устройства на обоих концах. Normal-node передают ответные пакеты домашних узлов.

6.8.3. Реализация

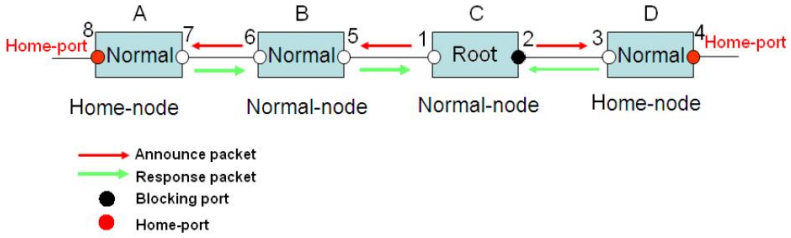


Рис. 140. Реализация DHP

Как показано на предыдущем рисунке, конфигурации A, B, C и D на рисунке следующие:

- Конфигурация STRP: C — Root; порт 2 находится в состоянии блокировки; A, B и D являются нормальными; все остальные кольцевые порты находятся в состоянии пересылки.
- Конфигурация DHP: A и D — Home-nodes; порт 8 и порт 4 — Home-ports; B и C являются Normal-nodes.

- C, Root, отправляет пакеты Announce через два своих кольцевых порта. Домашний порт 8 и домашний порт 4 завершают полученные пакеты Announce и отправляют ответные пакеты на C. C идентифицирует состояние кольца как закрытое. Порт 2 находится в состоянии блокировки.
- Когда канал между A и B заблокирован, топология включает два канала: A и B-C-D. A избирается корнем. Порт 7 находится в состоянии блокировки.
- B ссылке B-C-D B выбран в качестве корня. Порт 6 находится в состоянии блокировки. C становится нормальным. Порт 2 находится в состоянии пересылки. A

может связываться с B, C и D через устройство 1 и устройство 2, как показано на следующем рисунке.

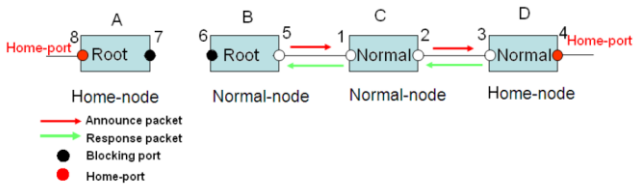


Рис. 141. Реализация DHP

6.8.4. Описание

Конфигурации STRP отвечают следующим требованиям:

- Все коммутаторы в одном кольце должны иметь одинаковый номер домена.
- Одно кольцо содержит только один корень, но может содержать несколько корней B или нормалей.
- На каждом коммутаторе можно настроить только два порта для кольца.
- Для двух связанных колец резервные порты можно настроить только в одном кольце.
- В одном кольце можно настроить несколько резервных портов.
- На коммутаторе для одного кольца можно настроить только один резервный порт.

6.8.5. Веб конфигурация

Конфигурирование STRP mode

Перейти [Device Advanced Configuration] → [STRP configuration] → [STRP Mode] для конфигурации STRP mode, как показано на рисунке ниже.

Рис. 142. Конфигурирование STRP mode

- **STRP Mode**
  Опции: Port Based / VLAN Based
  По умолчанию: Port Based
  Функция: Конфигурирование STRP mode

Кольцевые протоколы на основе портов включают RSTP, ST-Ring-Port и STRP-Port, а кольцевые протоколы на основе VLAN включают MSTP, ST-Ring-VLAN и STRP-VLAN.
Кольцевые протоколы на основе VLAN являются взаимоисключающими, и только тип кольцевого протокола на основе VLAN может быть настроен для одного устройства.
Кольцевой протокол на основе порта и кольцевой протокол на основе VLAN являются взаимоисключающими, и только один режим кольцевого протокола может быть выбран для одно устройство.

Создание STRP-Port-Based записи

Перейти [Device Advanced Configuration] → [STRP configuration] → [Port-Based STRP Configuration] для входа на страницу создание STRP-Port-Based записи, как показано на рисунке ниже.

Рис. 143. Создание STRP-Port-Based записи

Нажмите <Add>, чтобы создать запись STRP.

Установите параметры для записи STRP-Port-Based, как показано на следующем рисунке.

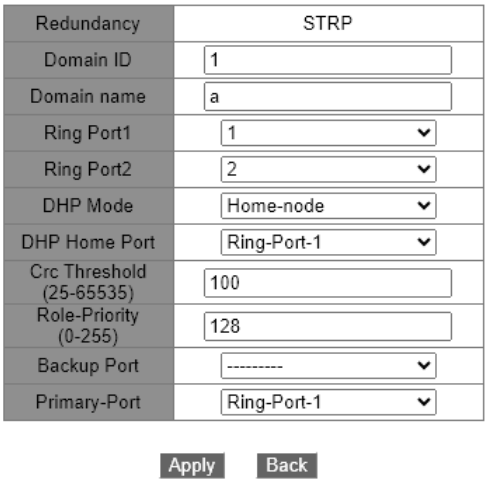


Рис. 144. Настройка записи STRP

- **Redundancy**
  Обязательная конфигурация: STRP
- **Domain ID**
  Диапазон: 1~32
  Описание: Каждое кольцо имеет уникальный идентификатор домена. На одном коммутаторе можно настроить максимум 16 колец STRP.
- **Domain name**
  Диапазон: 1~31 символ
  Функция: настроить доменное имя.
- **Ring Port 1/Ring Port 2**
  Опции: все порты коммутатора
  Функция: выберите два кольцевых порта.
- **DHP Mode**
  Опции: Disable / Normal-node / Home-node
  По умолчанию: Disable
  Функция: отключить DHP или настроить режим DHP.
- **DHP Home Port**
  Варианты: Ring-Port-1 / Ring-Port-2 / Ring-Port-1-2
  Функция: настроить Home-port для Home-node DHP.
  Описание: Если в канале DHP есть только одно устройство, оба кольцевых порта домашнего узла должны быть настроены как домашние порты.
- **Crc Threshold**
  Диапазон: 25~65535
  По умолчанию: 100
  Функция: настроить пороговое значение CRC.
  Описание: Этот параметр используется при выборе root. Система подсчитывает количество полученных CRC. Если количество CRC одного кольцевого порта превышает пороговое значение, система считает, что порт имеет ухудшение CRC. В результате значение деградации CRC устанавливается равным 1 в векторе пакета Announce порта.
- **Role-Priority**
  Диапазон: 0~255
  По умолчанию: 128

Функция: Настройка приоритета коммутатора.

- **Backup Port**
  Опции: все порты коммутатора
  Функция: Настройка резервного порта.

Не настраивайте кольцевой порт в качестве резервного порта.

- **Primary-Port**
  Опции: --/Ring-Port-1 / Ring-Port-2
  По умолчание: --
  Функция: Настройка основного порта. Когда кольцо замкнуто, основной порт root находится в состоянии пересылки.
  После завершения настройки параметров созданная запись будет отображаться в списке STRP, как показано на следующем рисунке.

Рис. 145. Список записей STRP

Кольцевой порт STRP или резервный порт и канал порта являются взаимоисключающими. Кольцевой порт STRP или резервный порт нельзя добавить к каналу порта; порт в канале порта не может быть настроен в качестве кольцевого порта STRP или резервного порта.
Кольцевой или резервный порт STRP и пункт назначения зеркалирования являются взаимоисключающими. Кольцевой порт STRP или резервный порт нельзя настроить в качестве порта назначения зеркалирования; порт назначения зеркального отображения нельзя настроить в качестве кольцевого порта STRP или резервного порта.
Кольцевые порты между кольцевыми протоколами на основе портов RSTP, ST-Ring-Port и STRP-Port являются взаимоисключающими, то есть кольцевой порт и резервный порт STRP-Port не могут быть настроены как порт RSTP, кольцо ST-Ring-Port. порт или резервный порт ST-Ring-Port; Порт RSTP, кольцевой порт ST-Ring-Port и резервный порт ST-Ring-Port нельзя настроить как кольцевой порт STRP-Port или резервный порт.
Не рекомендуется, чтобы порты в группе изоляции настраивались одновременно как порты STRP и резервные порты, а порты STRP и резервные порты не могут быть добавлены в группу изоляции.

Просмотр настроек параметров записи STRP-Port-Based

Щелкнув запись STRP и можно просматривать, и изменять настройки параметров записи, как показано на следующем рисунке.

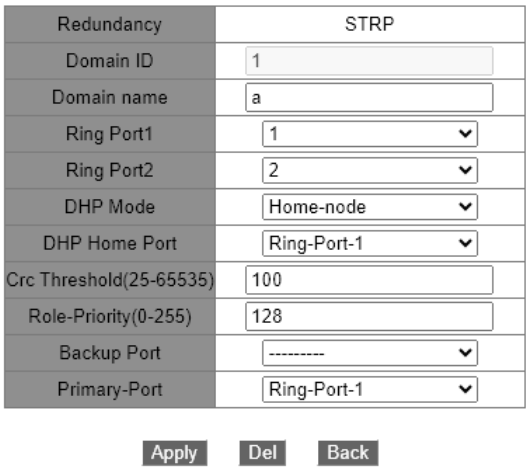


Рис. 146. Настройка параметров для записи STRP

После завершения изменения нажмите <Apply>, чтобы изменение вступило в силу. Вы можете удалить запись STRP, нажав <Delete>.

Просмотр роли и статус порта кольца STRP возможен, как показано на следующем рисунке.

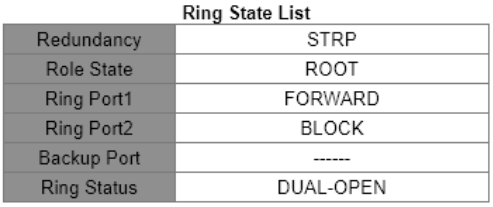


Рис. 147. Состояние кольца STRP

Конфигурация на основе STRP-VLAN

Перейти [Device Advanced Configuration] → [STRP configuration] → [STRP Mode] для входа на страницу конфигурации STRP mode. Выберите Vlan Based.

Конфигурация экземпляра STRP

Перейти [Device Advanced Configuration] → [STRP configuration] → [VLAN-Based STRP Configuration] → [STRP STG Instance Configuration] для входа на страницу конфигурации экземпляра STRP STG, как показано на следующем рисунке.

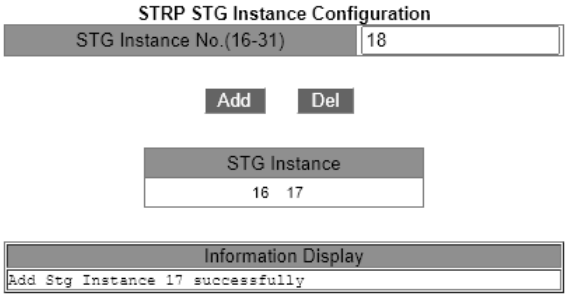


Рис. 148. Конфигурация экземпляра STRP

- **STG Instance No. (16-31)**
  Диапазон: 16 ~ 31
  Функция: Настройка идентификатора экземпляра STRP.

Конфигурация VLAN в экземпляре STRP

Перейти [Device Advanced Configuration] → [STRP configuration] → [VLAN-Based STRP Configuration] → [STG Instance Protocol VLAN] для входа на страницу конфигурации VLAN экземпляра STRP, как показано на следующем рисунке.

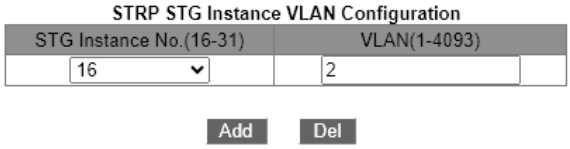


Рис. 149. Конфигурация VLAN в экземпляре STRP

- **STRP STG Instance VLAN Configuration**
  Портфолио: {идентификатор экземпляра STG, идентификатор VLAN}
  Диапазон: {16~31, 1~4093}
  Функция: Настройте идентификатор VLAN для экземпляра STRP.
  Описание: один экземпляр может соответствовать нескольким идентификаторам VLAN, но один идентификатор VLAN может соответствовать только одному экземпляру.

Просмотрите информацию об экземплярах STRP

Перейти [Device Advanced Configuration] → [STRP configuration] → [VLAN-Based STRP Configuration] → [STG Instance Information] для входа на страницу информации об экземпляре STRP, как показано на следующем рисунке.

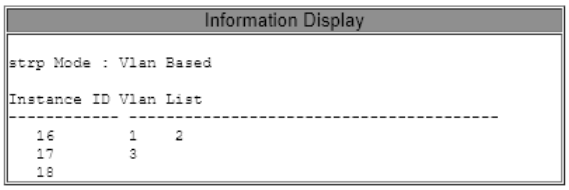


Рис. 150. Просмотр информации об экземплярах STRP

Конфигурация STRP-VLAN-Based

Перейти [Device Advanced Configuration] → [STRP configuration] → [VLAN-Based STRP Configuration] → [Ring Configuration] для входа на страницу создания STRP-VLAN-Based, как показано на следующем рисунке.

Рис. 151. Конфигурация STRP-VLAN-Based

Нажмите <Add>, чтобы создать запись STRP. Установите параметры для записи, как показано на следующем рисунке.

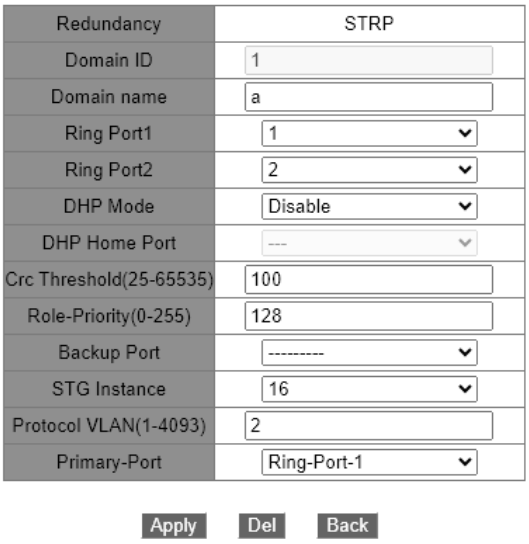


Рис. 152. Параметры записи STRP

- **Redundancy**
  Обязательная настройка: STRP
- **Domain ID**
  Диапазон: 1~32
  Функция: Каждое кольцо имеет уникальный идентификатор домена. На одном коммутаторе можно настроить максимум 8 колец STRP.

- **Domain name**
  Диапазон: 1~31 символ
  Функция: настроить доменное имя.
- **Ring Port 1/Ring Port 2**
  Опции: все порты коммутатора
  Функция: выберите два кольцевых порта.
- **DHP Mode**
  Опции: Disable / Normal-node / Home-node
  По умолчанию: Disable
  Функция: отключить DHP или настроить режим DHP.
- **DHP Home Port**
  Варианты: Ring-Port-1 / Ring-Port-2 / Ring-Port-1-2
  Функция: настроить домашний порт для домашнего узла DHP.
  Описание: Если в канале DHP есть только одно устройство, оба кольцевых порта домашнего узла должны быть настроены как домашние порты.
- **Crc Threshold**
  Диапазон: 25~65535
  По умолчанию: 100
  Функция: настроить пороговое значение CRC.
  Описание: Этот параметр используется при выборе root. Система подсчитывает количество полученных CRC. Если количество CRC одного кольцевого порта превышает пороговое значение, система считает, что порт имеет ухудшение CRC. В результате значение деградации CRC устанавливается равным 1 в векторе пакета Announce порта.
- **Role-Priority**
  Диапазон: 0~255
  По умолчанию: 128
  Функция: Настройка приоритета коммутатора.

Кольцевой порт STRP или резервный порт и канал порта являются взаимоисключающими. Кольцевой порт STRP или резервный порт нельзя добавить к каналу порта; порт в канале порта не может быть настроен в качестве кольцевого порта STRP или резервного порта.

Кольцевой или резервный порт STRP и пункт назначения зеркалирования являются взаимоисключающими. Кольцевой порт STRP или резервный порт нельзя настроить в качестве порта назначения зеркалирования; порт назначения зеркального отображения нельзя настроить в качестве кольцевого порта STRP или резервного порта.

Не рекомендуется, чтобы порты в группе изоляции настраивались одновременно как порты STRP и резервные порты, а порты STRP и резервные порты не могут быть добавлены в группу изоляции.

- **Backup Port**
  Опции: все порты коммутатора
  Функция: Конфигурирование резервного порта

Не настраивайте кольцевой порт в качестве резервного порта.

- **STG Instance**
  Опции: созданные экземпляры STRP
  Функция: настроить экземпляр для кольца.
  Описание: блокирующий порт в кольце будет блокировать пакеты данных всех VLAN, соответствующих экземпляру.
- **Protocol VLAN (1~4093)**
  Диапазон: 1~4093
  Описание: идентификатор VLAN должен быть одним из тех, которые соответствуют экземпляру STG. Функция: пакеты STRP с идентификатором VLAN служат основой для диагностики и обслуживания кольца на основе STRP-VLAN.
- **Primary-Port**
  Опции: -- / Ring-Port-1 / Ring-Port-2
  По умолчанию: --
  Функция: Настройка основного порта. Когда кольцо замкнуто, основной порт root находится в состоянии пересылки.

  После завершения настройки созданные кольца отображаются в списке STRP List, как показано на следующем рисунке.

Рис. 153. Список STRP List

Перейдите в соответствующий параметр STRP, чтобы просмотреть конфигурацию кольца и изменить ее, как показано на рис. 154.

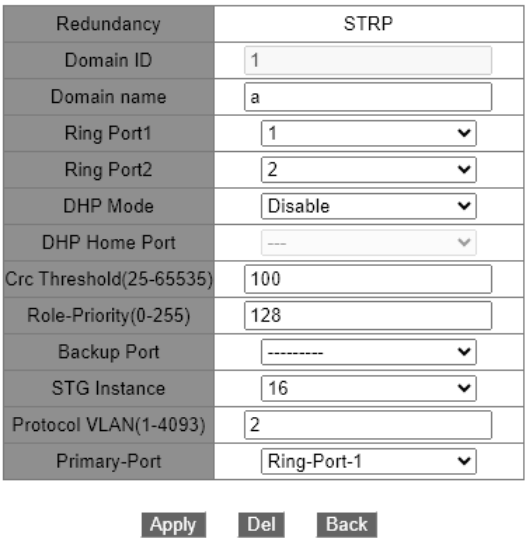


Рис. 154. Просмотр конфигурации для записи STRP

После завершения изменения нажмите <Apply>, чтобы изменение вступило в силу. Вы можете удалить запись STRP, нажав <Delete>.

Просмотр роли и статус порта кольца STRP, как показано на следующем рисунке.

Ring State List

Redundancy	STRP
Role State	ROOT
Ring Port1	FORWARD
Ring Port2	BLOCK
Backup Port	------
Ring Status	RING-OPEN

Рис. 155. Просмотр роли и статуса портов для кольца STRP

6.8.6. Пример типовой конфигурации

Как показано на рис. 138, A, B, C и D образуют кольцо Ring1, E, F, G и H образуют кольцо Ring2, а CE и DF являются резервными соединениями между Ring1 и Ring2.

Процесс настройки коммутатора A, B:

- Идентификатор домена: 1, имя домена: Ring, приоритет порта принимает значение по умолчанию, выберите кольцевой порт 1 и 2, резервный порт выбрать нельзя, см. рис. 144;

Конфигурация коммутаторов C и D:

- Идентификатор домена: 1, имя домена: Ring, приоритет порта принимает значение по умолчанию, выберите 1 и 2 для кольцевого порта и выберите 3 для резервного порта, см. рис. 144;

Конфигурация коммутаторов E, F, G, H:

- Идентификатор домена: 2, имя домена: Ring, приоритет порта принимает значение по умолчанию, выберите кольцевой порт 1 и 2, резервный порт выбрать нельзя, см. рис. 144.

6.9. Конфигурирование MSTP

6.9.1. Введение

Хотя протокол RSTP обеспечивает быструю конвергенцию, у него, как и у STP, есть следующий недостаток: все мосты в локальной сети совместно используют одно связующее дерево, и пакеты всех VLAN пересылаются по связующему дереву. Как показано на рисунке ниже, некоторые конфигурации могут блокировать соединение между коммутатором A и коммутатором C. Поскольку коммутатор B и коммутатор D не входят в сеть VLAN 1, они не могут пересылать пакеты сети VLAN 1. В результате порт VLAN 1 коммутатора A не может связаться с коммутатором C.

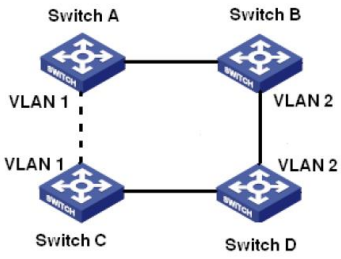


Рис. 156. Пример подключения

Чтобы решить эту проблему, появился протокол Multiple Spanning Tree Protocol (MSTP). Он обеспечивает как быструю конвергенцию, так и отдельные пути пересылки для трафика разных VLAN, обеспечивая лучший механизм распределения нагрузки для избыточных каналов.

MSTP отображает одну или несколько VLAN в один экземпляр. Коммутаторы с одинаковой конфигурацией образуют домен. В каждом домене формируется несколько связующих деревьев. Связующие деревья не зависят друг от друга. Этот домен эквивалентен узлу коммутатора и другим доменам. Затем выполнить операцию алгоритма связующего дерева, чтобы получить полное связующее дерево. В соответствии с этим алгоритмом сеть, показанная на рис. 156, образует топологию, показанную на рис. 157. Оба коммутатора A и C находятся в регионе 1. В этом домене нет петли, поэтому блок каналов не теряется, то же верно и для региона 2. Region1 и Region2 эквивалентны узлам коммутатора. Между двумя коммутаторами есть петля, поэтому пересылка должна быть заблокирована.

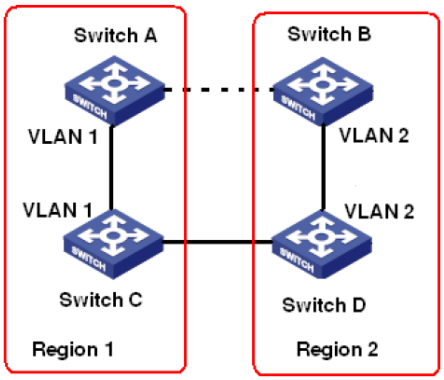


Рис. 157. Пример подключения

6.9.2. Основные понятия

В сочетании с рис. 158 – рис. 161 для понимания связанных концепций MSTP:

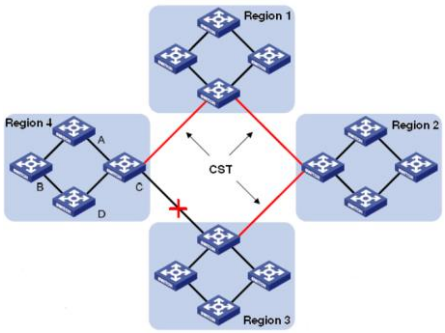


Рис. 158. MSTP концепция

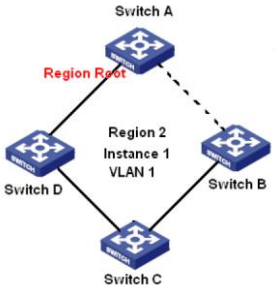


Рис. 159. Mapping to Instance 1

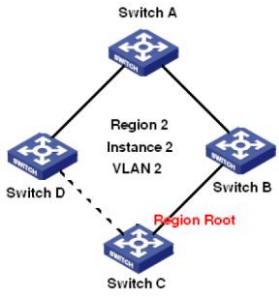


Рис. 160. Mapping to Instance 2

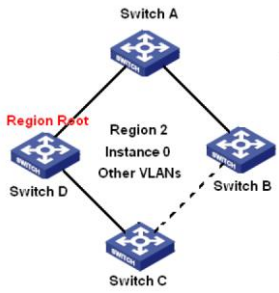


Рис. 161. Другие VLAN Mapping to Instance 0

Экземпляр: набор из нескольких VLAN. Одна сеть VLAN может быть сопоставлена с одним экземпляром (одна сеть VLAN образует одно связующее дерево), как показано на рис. 159 и 160; несколько сетей VLAN с одинаковой топологией также могут быть

сопоставлены с одним экземпляром (несколько сетей VLAN совместно используют одно связующее дерево), как показано на рис. 161. Разные экземпляры сопоставляются с разными связующими деревьями. Экземпляр 0 является связующим деревом для устройств всех регионов, а остальные экземпляры — связующим деревом для устройств определенного региона.

Домен MST (несколько регионов связующего дерева, несколько регионов связующего дерева): имя домена MSTP, уровень версии, конфигурация сопоставления VLAN и экземпляра связующего дерева одинаковы, а взаимосвязанные коммутаторы находятся в одном домене, как показано на рис. 158. Region1, Region2, Region3, Region4 — это четыре разных домена MST.

Таблица сопоставления VLAN: состоит из сопоставления между VLAN и связующими деревьями. Таблица сопоставления VLAN региона 2 представляет собой сопоставление между VLAN 1 и экземпляром 1, как показано на рис. 159; VLAN 2 сопоставляется с экземпляром 2, как показано на рис. 160. Другие VLAN сопоставляются с экземпляром 0, как показано на рис. 161.

IST (Common and Internal Spanning Tree, общедоступное и внутреннее связующее дерево): то есть экземпляр связующего дерева 0, который относится к одному связующему дереву, соединяющему все устройства в коммутируемой сети. Как показано на рис. 158, оно состоит из IST и КНТ.

IST (Internal Spanning Tree, внутреннее связующее дерево): фрагмент CIST в домене MST, то есть экземпляр 0 в каждом домене, как показано на рис. 161;

CST (Common Spanning Tree, общедоступное связующее дерево): единое связующее дерево, соединяющее все домены MST в коммутируемой сети. Если каждый домен MST рассматривается как «узел устройства», CST представляет собой связующее дерево, вычисляемое этими узлами по протоколу STP/RSTP, такое как связующее дерево, состоящее из красных линий на рис. 158.

MSTI (Multiple Spanning Tree Instance, Multiple Spanning Tree Instance): несколько связующих деревьев могут быть созданы в одном домене MST, каждое связующее дерево не зависит друг от друга, и каждое связующее дерево является MSTI, как показано на рис. 159 и рис. 160; IST также является специальным MSTI.

Общий корень: указывает корневой мост CIST. Коммутатор с наименьшим идентификатором корневого моста в сети является общим корнем. В регионе MST остовные деревья имеют разную топологию, и их региональные корни также могут быть разными, три экземпляра имеют разные региональные корни. Корневой мост MSTI рассчитывается на основе STP/RSTP в текущем регионе MST. Корневой мост IST — это устройство, которое подключено к другому региону MST и выбрано на основе полученной информации о приоритете. Граничный порт: указывает порт, который соединяет регион MST с другим регионом MST, рабочим регионом STP или рабочим регионом RSTP. Состояние порта. Порт может находиться в одном из следующих состояний в зависимости от того, изучает ли он MAC-адреса и пересылает ли трафик.

Forwarding state: указывает, что порт изучает MAC-адреса и пересылает трафик.

Learning state: указывает, что порт изучает MAC-адреса, но не пересылает трафик.

Discarding state: указывает, что порт не изучает MAC-адреса и не пересылает трафик.

Root port: указывает лучший порт от некорневого моста к корневому мосту, то есть порт с наименьшей стоимостью для корневого моста. Некорневой мост взаимодействует с корневым мостом через корневой порт. Некорневой мост имеет только один корневой порт. Корневой мост не имеет корневого порта. Корневой порт может находиться в состоянии пересылки, обучения или сброса.

Назначенный порт: указывает порт для пересылки BPDU на другие устройства или локальные сети. Все порты корневого моста являются назначенными портами. Назначенный порт может находиться в состоянии пересылки, обучения или сброса.

Главный порт: указывает порт, который соединяет регион MST с общим корнем. Порт находится на кратчайшем пути к общему корню. В CST главный порт является корневым портом региона (как узла). Мастер-порт — это специальный пограничный порт. Это корневой порт для CIST и главный порт для других экземпляров. Главный порт может находиться в состоянии пересылки, обучения или сброса.

Альтернативный порт: указывает резервный порт корневого порта или основного порта. При сбое корневого или главного порта альтернативный порт становится новым корневым или главным портом. Главный порт может находиться только в состоянии отбрасывания.

Резервный порт: указывает резервный порт назначенного порта. Когда назначенный порт выходит из строя, резервный порт становится назначенным портом и пересылает данные без каких-либо задержек. Резервный порт может находиться только в состоянии отбрасывания.

6.9.3. Реализация MSTP

MSTP делит сеть на несколько регионов MST. CST рассчитывается между регионами. Несколько остовных деревьев рассчитываются в регионе. Каждое связующее дерево является MSTI. Экземпляр 0 — это IST, а остальные экземпляры — это MSTI.

- Расчет CIST
  - Устройство отправляет и получает пакеты BPDU. На основе сравнения сообщений конфигурации MSTP устройство с наивысшим приоритетом выбирается в качестве общего корня CIST.
  - IST рассчитывается в каждом домене MST.
  - Каждый домен MST рассматривается как отдельное устройство, и CST рассчитывается между доменами.
  - CST и IST составляют CIST всей сети.

- Расчет MSTI
  - В регионе MST MSTP создает различные связующие деревья для VLAN на основе сопоставления между VLAN и связующими деревьями. Каждое остовное дерево рассчитывается независимо. Процесс расчета подобен тому, что в STP.
  - Внутри домена MST пакеты VLAN пересылаются по соответствующим MSTI. Между регионами MST пакеты VLAN пересылаются по CST.

6.9.4. Веб конфигурирование

Глобальное включение MSTP протокола

Перейти [Device Advanced Configuration] → [MSTP configuration] → [Enable MSTP] для входа на страницу конфигурации протокола MSTP, как показано на рисунке ниже.

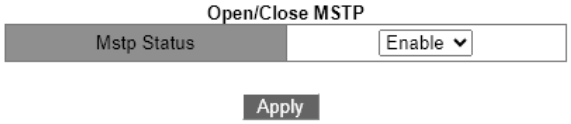


Рис. 162. Глобальное включение MSTP протокола

- **Mstp status**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: Включение / Выключение MSTP

Кольцевые протоколы на основе портов включают RSTP, ST-Ring-Port и STRP-Port, а кольцевые протоколы на основе VLAN включают MSTP, ST-Ring-VLAN и STRP-VLAN.
Кольцевые протоколы на основе VLAN являются взаимоисключающими, и для одного устройства можно настроить только тип кольцевого протокола на основе VLAN.
Кольцевой протокол на основе портов и кольцевой протокол на основе VLAN являются взаимоисключающими, и для одного устройства можно выбрать только один режим кольцевого протокола.

Включение порта в режиме MSTP, как показано на рисунке ниже.

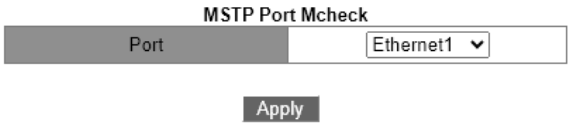


Рис. 163. Включение порта в режиме MSTP

- **Port**
  Опции: все порты коммутатора
  По умолчанию: Disable
  Функция: Когда порт с поддержкой MSTP подключен к устройству с поддержкой STP, этот порт будет автоматически изменен для работы в режиме STP. Если устройство с поддержкой STP будет удалено, этот порт не вернется автоматически к работе в режиме MSTP. Если вы хотите вернуться к работе в режиме MSTP в этом состоянии, установите эту функцию для порта. Как только порт снова получит STP-сообщение, он автоматически переключится на работу в режиме STP.

Эта конфигурация вступит в силу, только если коммутатор работает в режиме MSTP; в противном случае это бесполезно.

Установите режим работы MSTP, как показано на рис. 164;

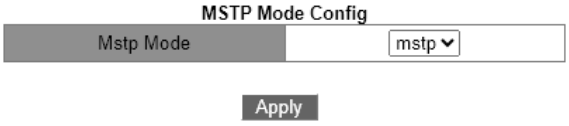


Рис. 164. Режим работы MSTP

- **MSTP Mode Config**
  Варианты конфигурации: mstp/rstp
  Конфигурация по умолчанию: mstp
  Функция: выберите протокол связующего дерева.

Настройка состояния MSTP порта

Перейти [Device Advanced Configuration] → [MSTP configuration] → [Enable Port MSTP] для входа на страницу конфигурации протокола MSTP, как показано на рисунке ниже.

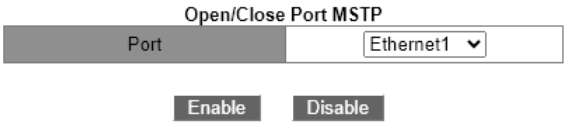


Рис. 165. Настройка состояния MSTP порта

- **Port**
  Опции: все порты коммутатора
  По умолчанию: если включен глобальный протокол MSTP, состояние MSTP всех портов открыто.
  Функция: включить / отключить MSTP на порту.

Настройка параметров домена MSTP

Перейти [Device Advanced Configuration] → [MSTP configuration] → [MSTP Region Config] для входа на страницу конфигурации параметров региона MST, как показано на рисунке ниже.

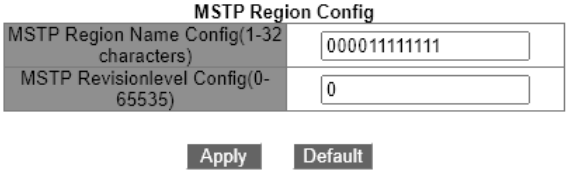


Рис. 166. Настройка параметров домена MSTP

- **MSTP Region Name config**
  Диапазон: 1-32 символа
  По умолчанию: MAC-адрес устройства.
  Функция: Настройка имени региона MST.
- **MSTP Revision level config**
  Опции: 0~65535
  По умолчанию: 0
  Функция: Настройка параметра версии для региона MSTP.
  Описание: Параметр версии, имя региона MST и таблица сопоставления VLAN определяют регион MST, к которому принадлежит устройство. Когда все конфигурации одинаковы, устройства находятся в одном регионе MST.

Настройка таблицы сопоставления VLAN, как показано на рисунке ниже.

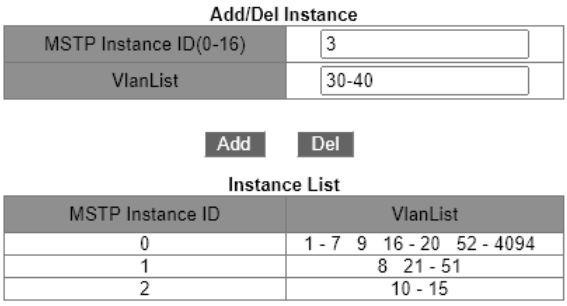


Рис. 167. Настройка таблицы сопоставления VLAN

- **{MSTP Instance ID, VLAN list}**
  Диапазон: {0~16, 1~4094}
  По умолчанию: {0, 1~4094}.
  Функция: Настройте таблицу сопоставления VLAN в регионе MST.
  Описание. По умолчанию все VLAN сопоставляются с экземпляром 0. VLAN можно сопоставить только с одним экземпляром связующего дерева. Если VLAN с установленным отношением сопоставления повторно сопоставляется с другим экземпляром, исходное отношение сопоставления будет отменено. Если отношение сопоставления между указанными VLAN и экземплярами связующего дерева удалено, эти VLAN будут повторно сопоставлены с экземпляром 0.

<Del> не может удалить список VLAN экземпляра 0

После завершения настройки «Список экземпляров» покажет сопоставление между VLAN и экземпляром.

Настройте приоритет моста коммутатора в указанном экземпляре

Перейти [Device Advanced Configuration] → [MSTP configuration] → [MSTP Instance Config] для входа на страницу конфигурации параметров экземпляра MSTP, как показано на рисунке ниже.

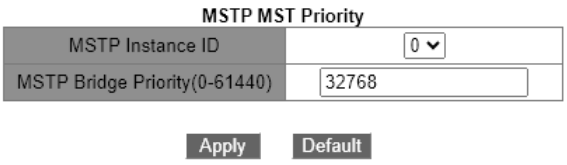


Рис. 168. Приоритет моста коммутатора

- **MSTP Instance ID**
  Опции: все созданные экземпляры
- **MSTP Bridge Priority**
  Диапазон: 0~61440 с шагом 4096
  По умолчанию: 32768
  Функция: настроить приоритет моста коммутатора в назначенном экземпляре.
  Описание: Приоритет моста определяет, может ли коммутатор быть выбран в качестве регионального корня экземпляра связующего дерева. Чем меньше значение, тем выше приоритет. Установив более низкий приоритет, определенное устройство может быть назначено корневым мостом связующего дерева. Устройство с поддержкой MSTP можно настроить с разными приоритетами в разных экземплярах связующего дерева.

Настройка приоритета порта и стоимости пути в назначенном экземпляре, как показано на рисунке ниже.

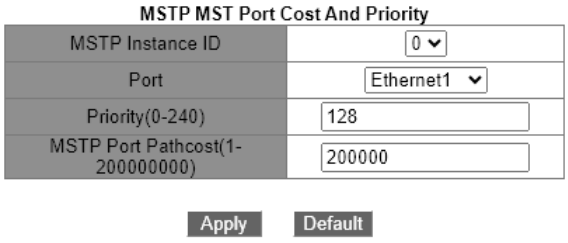


Рис. 169. Настройка приоритета порта и стоимости пути

- **MSTP Instance ID**
  Опции: все созданные экземпляры
- **Port**
  Опции: все порты коммутатора
- **Priority**
  Диапазон: 0~240 с шагом 16
  По умолчанию: 128
  Функция: настроить приоритет порта в назначенном экземпляре.
  Описание: Приоритет порта определяет, будет ли он выбран в качестве корневого порта. В том же состоянии порт с более низким приоритетом будет выбран в качестве корневого порта. Порты с поддержкой MSTP можно настроить с разными приоритетами и играть разные роли портов в разных экземплярах связующего дерева.

- **MSTP Port Path cost**
  Диапазон: 1~200000000
  По умолчанию: как указано в таблицах ниже.

Таблица 7. Расчет MSTP Port Path cost

Port Type	Default Path Cost	Recommended Range
10Mbps	2000000	2000000~20000000
100Mbps	200000	200000~2000000
1Gbps	20000	20000~200000

Таблица 8. Расчет MSTP Port Path cost

Port Type	Number of Aggregation Ports (in Allowed Aggregation Range)	Recommended Range
10Mbps	N	2000000/N
100Mbps	N	200000/N
1Gbps	N	20000/N

Функция: Настройка стоимости пути порта в назначенном экземпляре.
Описание: Стоимость пути порта используется для расчета оптимального пути. Этот параметр зависит от пропускной способности. Чем больше пропускная способность, тем ниже стоимость. Изменение стоимости пути порта может изменить путь передачи между устройством и корневым мостом, тем самым изменив роль порта. Порт с поддержкой MSTP можно настроить с различной стоимостью пути в разных экземплярах связующего дерева.

Конфигурирование параметров MSTP времени

Перейти [Device Advanced Configuration] → [MSTP configuration] → [MSTP Time Config] для входа на страницу настройки параметров времени MSTP, как показано на рисунке ниже.

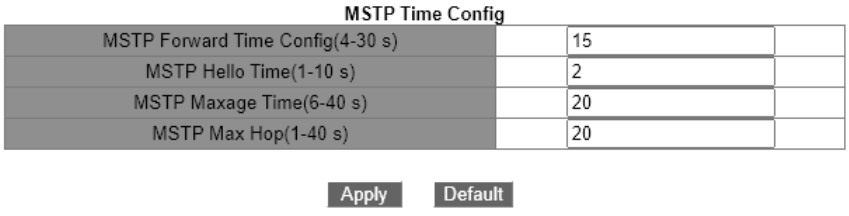


Рис. 170. Конфигурирование параметров MSTP времени

- **MSTP Forward Time Config**
  Опции: 4~30 с
  По умолчанию: 15 с

Функция: Настройка временного интервала для смены состояния порта (Discarding – Learning или Learning – Forwarding).

- **MSTP Hello Time**
  Диапазон: 1~10 с
  По умолчанию: 2 с
  Функция: Настройка временного интервала для отправки BPDU.
- **MSTP Max Age Time**
  Диапазон: 6~40 с
  По умолчанию: 20 с
  Функция: Установите максимальный возраст пакетов BPDU.

*Значения Forward Delay Time, Hello Time и Max Age Time должны соответствовать следующим требованиям: 2 * (Forward Delay Time – 1,0 секунды) >= Max Age Time; Max Age Time >= 2 * (Hello Time + 1,0 секунды).*
Рекомендуется установка по умолчанию.

- **MSTP Max Hop**
  Диапазон: 1~40
  По умолчанию: 20
  Функция: настроить максимальное количество переходов для региона MST. Максимальные прыжки области MST ограничивают масштаб области MST; максимальное количество переходов регионального корня равно максимальному количеству переходов региона MST.
  Описание: Начиная с корневого моста связующего дерева в регионе MST, номер перехода вычитает 1, когда BPDU проходит через устройство в регионе. Устройство отбрасывает BPDU с номером перехода 0.

Действительна только максимальная конфигурация переходов корневого моста в регионе MST. Устройство некорневого моста принимает конфигурацию максимального прыжка корневого моста.
Рекомендуется установка по умолчанию.

Настройка функции быстрого перехода состояния MSTP

Перейти [Device Advanced Configuration] → [MSTP configuration] → [MSTP Fast Transfer Config] для входа на страницу конфигурации, как показано на рисунке ниже.

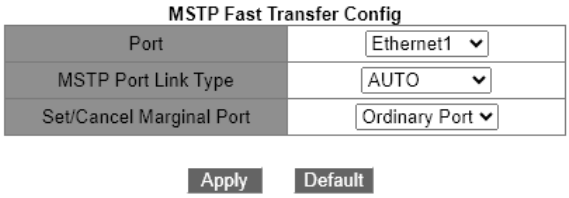


Рис. 171. Настройка функции быстрого перехода состояния MSTP

- **MSTP Port Link Type**
  Опции: AUTO / Force True / Force False

По умолчанию: АВТО

Функция: Установите тип соединения порта. Если порт подключен к каналу «точка-точка», состояние порта может быть быстро передано.

Описание: **AUTO** означает, что коммутатор автоматически определяет тип соединения в соответствии с состоянием дуплекса порта. Когда порт работает в полнодуплексном режиме, протокол MSTP автоматически предполагает, что канал, подключенный к порту, является каналом «точка-точка». Когда порт работает в полудуплексном режиме, протокол MSTP автоматически предполагает, что канал, подключенный к порту, является общим каналом. **Force True** означает, что ссылка, подключенная к локальному порту, является двухточечной. **Force False** означает, что ссылка, подключенная к локальному порту, является общей ссылкой.

- **Set/Cancel Edge Port**

  Варианты: Edge port / Ordinary port

  По умолчанию: Ordinary port

  Функция: Настройте порт как порт Edge или обычный порт.

  Описание: когда порт напрямую подключен к конечным устройствам, но не подключен к другим устройствам или общим сегментам, этот порт является граничным портом. Пограничный порт может быстро перейти от блокировки к пересылке без задержки. Как только пограничный порт получит сообщение BPDU, этот порт снова изменится на обычный порт.

Просмотр MSTP конфигурации

Перейти [Device Advanced Configuration] → [MSTP configuration] → [MSTP Information] для входа просмотра MSTP конфигурации, как показано на рисунке ниже.

Information Display

```
                -- MSTP Bridge Config Info --

Bridge MAC    :  00:1e:cd:5b:db:73
Bridge Times :  Max Age 20, Hello Time 2, Forward Delay 15
Force Version:  3

############################ Instance 0 ############################
Self Bridge Id    : 32768 -  00:1e:cd:5b:db:73
Root Id           : this switch
Ext.RootPathCost : 0
Region Root Id    : this switch
Int.RootPathCost : 0
Root Port ID      : 0
Current port list in Instance 0:
Ethernet12 Ethernet2 Ethernet1 (Total 3)

   PortName      ID      ExtRPC   IntRPC  State Role     DsgBridge     DsgPort
-------------- ------- --------- --------- --- ---- ------------------ -------
    Ethernet12 128.012         0         0 FWD DSGN 32768.001ecd5bdb73 128.012
     Ethernet2 128.002         0     20000 BLK BKUP 32768.001ecd5bdb73 128.001
     Ethernet1 128.001         0         0 BLK DSGN 32768.001ecd5bdb73 128.001

############################ Instance 1 ############################
Self Bridge Id    : 32768.00:1e:cd:5b:db:73
Region Root Id    : this switch
Int.RootPathCost : 0
Root Port ID      : 0
Current port list in Instance 1:
(Total 0)

   PortName      ID    IntRPC   State Role     DsgBridge     DsgPort
-------------- ------- --------- --- ---- ------------------ -------

############################ Instance 2 ############################
Self Bridge Id    : 32768.00:1e:cd:5b:db:73
Region Root Id    : this switch
Int.RootPathCost : 0
Root Port ID      : 0
Current port list in Instance 2:
(Total 0)

   PortName      ID    IntRPC   State Role     DsgBridge     DsgPort
-------------- ------- --------- --- ---- ------------------ -------
```

Рис. 172. Просмотр MSTP конфигурации

6.9.5. Пример типовой конфигурации

Коммутаторы A, B, C и D в сети, показанной на рис. 173, принадлежат домену MST, а красные метки обозначают пакеты VLAN, которым разрешено проходить по этому каналу. Благодаря настройке пакеты разных VLAN пересылаются по разным экземплярам связующего дерева: пакеты VLAN 10 пересылаются по экземпляру 1, а корневым мостом экземпляра 1 является коммутатор A; пакеты VLAN 30 пересылаются по экземпляру 3, а корневой мост экземпляра 3 — SwitchB; пакеты VLAN 40 пересылаются через экземпляр 4, а корневой мост экземпляра 4 — это Switch C; пакеты VLAN 20 пересылаются через экземпляр 0, а корневой мост экземпляра 0 — это Switch B.

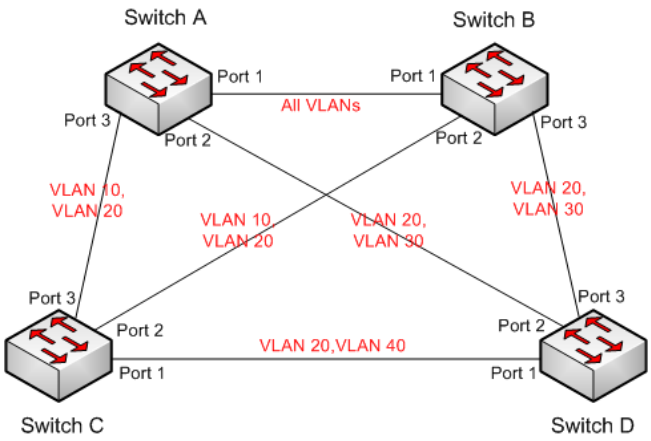


Рис. 173. Пример конфигурации

Процесс настройки **коммутатора A:**

1. Создайте виртуальные локальные сети 10, 20 и 30 на коммутаторе A и настройте порты, чтобы разрешить прохождение через соответствующие виртуальные локальные сети;

2. Включите протокол MSTP глобально, как показано на рис. 162;

3. Настройте имя домена MST как «Регион» и измените параметр на 0, как показано на рис. 166;

4. Создайте экземпляры 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с экземплярами 1, 3 и 4 соответственно, как показано на рис. 167;

5. Настройте приоритет моста коммутатора в экземпляре 1 на 4096 и значение по умолчанию в других экземплярах, как показано на рис. 168;

Коммутатор B настроен следующим образом:

6. Создайте VLAN 10, 20 и 30 на коммутаторе B, настройте соответствующие порты как транковые порты и разрешите прохождение соответствующих VLAN;

7. Включите протокол MSTP глобально, как показано на рис. 162;

8. Настройте имя домена MST как «Регион» и измените параметр на 0, как показано на рис. 166;

9. Создайте экземпляры 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с экземплярами 1, 3 и 4 соответственно, как показано на рис. 167;

10. Настройте приоритет моста коммутатора в экземплярах 3 и 0 на 4096 и значение по умолчанию в других экземплярах, как показано на рис. 168;

Коммутатор C настроен следующим образом:

11. Создайте VLAN 10, 20 и 40 на коммутаторе C, настройте соответствующие порты как транковые порты и разрешите прохождение соответствующих VLAN;

12. Включите протокол MSTP глобально, как показано на рис. 162;

13. Настройте имя домена MST как «Регион» и измените параметр на 0, как показано на рис. 166;

14. Создайте экземпляры 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с экземплярами 1, 3 и 4 соответственно, как показано на рис. 167;

15. Настройте приоритет моста коммутатора в экземпляре 4 на 4096 и значение по умолчанию в других экземплярах, как показано на рис. 168;

Коммутатор D настроен следующим образом:

16. Создайте VLAN 20, 30 и 40 на коммутаторе D, настройте соответствующие порты как транковые порты и разрешите прохождение соответствующих VLAN;

17. Включите протокол MSTP глобально, как показано на рис. 162;

18. Настройте имя домена MST как «Регион» и измените параметр на 0, как показано на рис. 166;

19. Создайте экземпляры 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с экземплярами 1, 3 и 4 соответственно, как показано на рис. 167;

После того, как вычисление MSTP завершено, MSTI, соответствующий каждой VLAN, показан на рис. 174;

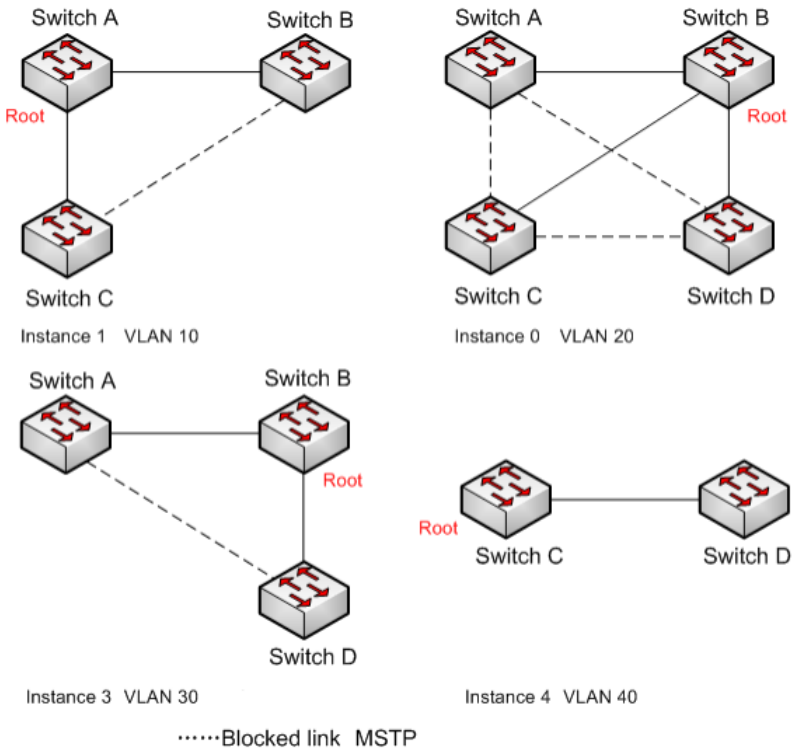


Рис. 174. STP для каждой VLAN

6.10. Alarm

6.10.1. Введение

Коммутаторы этой серии поддерживают следующие типы аварийных сигналов:

- Аварийный сигнал использования памяти / ЦП: Если эта функция включена, сигнал тревоги генерируется, когда использование ЦП / памяти превышает указанный порог.
- Аварийный сигнал конфликта IP и MAC адреса.
- Аварийный сигнал порта: если эта функция включена, аварийный сигнал срабатывает, когда порт находится в состоянии отсутствия соединения.
- Аварийный сигнал питания: он применим к продуктам с двойным источником питания. Если эта функция включена, тревога срабатывает при отключении питания или отклонении от нормы.
- Тревога кольцевой топологии: Если эта функция включена, тревога срабатывает, когда кольцо разомкнуто.
- Аварийный сигнал высокой температуры: если эта функция включена, аварийный сигнал срабатывает, когда температура коммутатора превышает пороговое значение высокой температуры.

  Диапазон общего порога высокой температуры (T-high) составляет от 85 ^{0}C до 94 ^{0}C с настройкой по умолчанию 85 ^{0}C.

  Диапазон опасного высокотемпературного порога (T-Max) составляет от 95^{0}C до 100^{0}C с настройкой по умолчанию 95^{0}C.

  Общий аварийный сигнал высокой температуры срабатывает, когда температура коммутатора (T-cur) выше порога T-high и ниже порога T-Max (T-high <T-cur<T-max).

  Аварийный сигнал опасной высокой температуры срабатывает, когда температура коммутатора равна или превышает пороговое значение T-Max (T-cur>=T-max).
- Аварийный сигнал низкой температуры: если эта функция включена, аварийный сигнал срабатывает, когда температура коммутатора превышает пороговое значение низкой температуры.

  Диапазон порога низкой температуры (T-low) составляет от -40 ^{0}C до 10 ^{0}C с настройкой по умолчанию -40 ^{0}C.

  Аварийный сигнал низкой температуры срабатывает, когда температура коммутатора (T-cur) ниже порогового значения T-low (T-cur<T-low).
- Аварийный сигнал трафика порта: если эта функция включена, аварийный сигнал генерируется, когда скорость входящего/исходящего трафика порта превышает указанный порог.
- Аварийный сигнал ошибки CRC / потери пакета: Если эта функция включена, аварийный сигнал генерируется, когда количество ошибок CRC / потери пакета порта превышает указанный порог.

Когда функция тревоги включена, режимы тревоги включают запись в журнал, мигание светодиода тревоги на передней панели, срабатывание клеммного блока тревоги и отправку пакетов trap SNMP.

Только главная станция кольца ST-Ring и STRP root поддерживают функцию кольцевой сигнализации.

6.10.2. Веб конфигурация

Настройка и отображения предупреждений об использовании памяти/ЦП.

Перейти [Device Advanced Configuration] → [Alarm Control] → [Basic Alarm] для входа на страницу конфигурации аварийного сигнала использования памяти/ЦП, как показано на рисунке ниже.

Mem and CPU Usage Alarm

Enable	☐ Mem Usage Alarm	☐ CPU Usage Alarm
Threshold	85 (50~100)	85 (50~100)
Margin Value	5 (1~20)	5 (1~20)
Alarm Status	Disable	Disable

Apply

Рис. 175. Настройка аларма памяти/ЦП

- **Mem Usage Alarm/CPU Usage Alarm**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включить / выключить сигнализацию использования памяти / процессора.
- **Threshold (%)**
  Диапазон: 50~100
  По умолчанию: 85
  Функция: установка порога использования памяти/ЦП. Когда использование памяти/ЦП коммутатора превышает пороговое значение, генерируется аварийный сигнал.
- **Margin Value (%)**
  Диапазон: 1~20
  По умолчанию: 5
  Функция: Установите значение запаса использования памяти / ЦП.
  Описание: Если использование памяти / ЦП колеблется около порогового значения, аварийные сигналы могут генерироваться и сбрасываться неоднократно. Чтобы предотвратить это явление, вы можете указать значение маржи (по умолчанию 5%). Аварийный сигнал будет сброшен только в том случае, если использование памяти / ЦП ниже порогового значения на величину запаса или более. Например, порог использования памяти установлен на 60%, а значение поля установлено на 5%. Если использование памяти коммутатора меньше или равно 60 %, аварийный сигнал не генерируется. Если использование памяти превышает 60%, будет сгенерирован

сигнал тревоги. Аварийный сигнал будет сброшен только в том случае, если использование памяти равно или ниже 55%.

- **Alarm Status**
  Опции: Disable / Normal
  Функция: просмотр состояния использования памяти / ЦП коммутатора. Тревога означает, что использование памяти / ЦП превышает пороговое значение и вызывает тревогу.

Загрузка ЦП в этом документе относится к средней загрузке ЦП за пять минут.

Настройка и отображение сигналов тревоги по источнику питания и температуре, как показано на рисунке ниже.

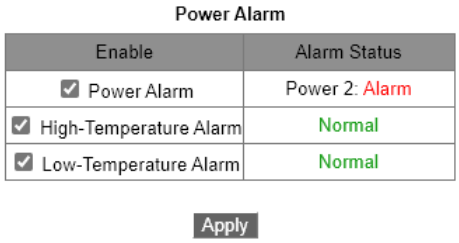


Рис. 176. Настройка алармов по питанию и температуре

- **Power Alarm/High-Temperature Alarm/Low-Temperature Alarm**
  Опции: Disable / Enable
  По умолчанию: Disable
  Функция: включить / отключить сигнализацию питания / сигнализацию высокой температуры / сигнализацию низкой температуры.
- **Power Alarm Status**
  Варианты: Normal / Alarm
  Функция: просмотр состояния аварийного сигнала питания.
  Аварийный сигнал: для продуктов с резервным питанием один из модулей питания выходит из строя или работает ненормально, и срабатывает аварийный сигнал.
  Нормальный: для продуктов с одним источником питания модуль питания подает питание в обычном режиме; для продукта с резервным питанием два силовых модуля обычно обеспечивают питание.
  High-Temperature Alarm Status / Low-Temperature Alarm Status
  Варианты: Normal / Alarm
  Функция: просмотр рабочей температуры коммутатора. Тревога означает, что температура коммутатора превышает пороговое значение высокой/низкой температуры и вызывает тревогу. Нормальный означает, что рабочая температура коммутатора нормальная.

Настройка и отображение оповещения о конфликте IP, MAC, как показано на рисунке ниже.

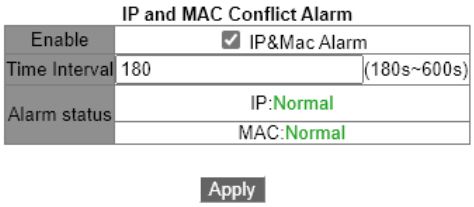


Рис. 177. Настройка алармов о конфликте IP, MAC

- **IP and MAC conflict alarm**
  Опции: Enable / disable
  Конфигурация по умолчанию: disable
  Функция: включить ли сигнализацию о конфликте адресов.
- **Time Interval**
  Диапазон конфигурации: 180 с ~ 600 с
  По умолчанию: 180 с
  Функция: Настройка временного интервала для обнаружения конфликтов адресов.

Настройка и отображение сигналов тревоги порта

Перейти [Device Advanced Configuration] → [Alarm Control] → [Set Port Alarm] для входа на страницу конфигурирования тревоги, как показано на рисунке ниже.

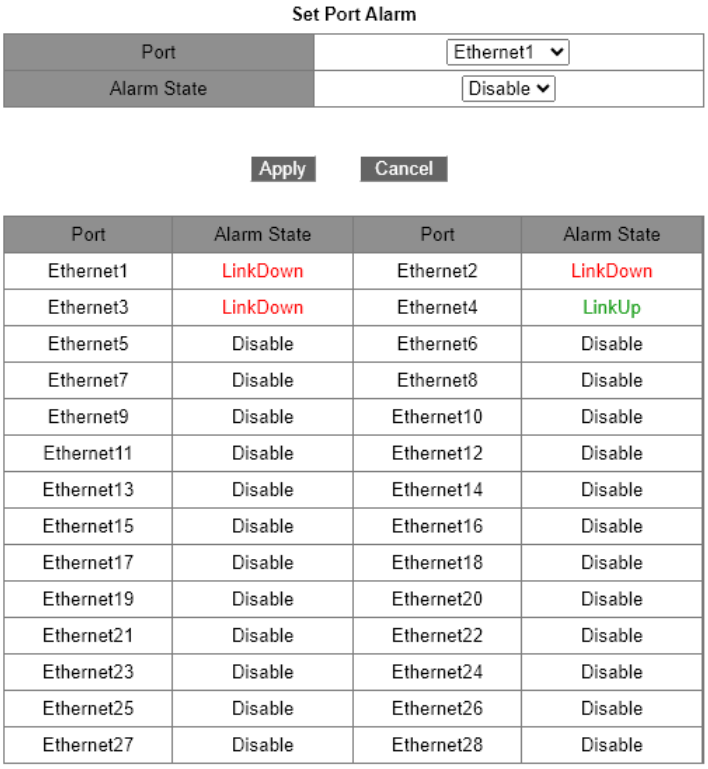


Рис. 178. Настройка и отображение сигналов тревоги порта

- **Port**
  Опции: Disable / Enable
  По умолчанию: Отключить
  Функция: включить / выключить тревогу порта.
- **Alarm Status**
  Опции: LinkDown / LinkUp
  Функция: просмотр состояния подключения порта. LinkUp означает, что порт находится в состоянии подключения и поддерживает нормальную связь. LinkDown означает, что порт отключен или находится в ненормальном соединении (сбой связи), и будет сгенерирован аварийный сигнал.

Настройка и отображение аварийного сигнал трафика порта

Перейти [Device Advanced Configuration] → [Alarm Control] → [AlarmPortRate] для входа на страницу конфигурации оповещения о трафике портов, как показано на рисунке ниже.

Set Port Rate Alarm

Port	input rate alarm			output rate alarm		
	Enable	Threshold	Alarm Status	Enable	Threshold	Alarm Status
1	☐	0 bps	Disable	☐	0 bps	Disable
2	☐	0 bps	Disable	☐	0 bps	Disable
3	☐	0 bps	Disable	☐	0 bps	Disable
4	☑	10 bps	Alarm	☑	10 kbps	Normal
5	☐	0 kbps	Disable	☐	0 kbps	Disable
6	☑	1000000000 bps	Normal	☑	1000000 kbps	Normal
7	☐	0 kbps	Disable	☐	0 kbps	Disable
8	☐	0 kbps	Disable	☐	0 kbps	Disable
9	☐	0 kbps	Disable	☐	0 kbps	Disable
10	☐	0 kbps	Disable	☐	0 kbps	Disable
11	☐	0 kbps	Disable	☐	0 kbps	Disable
12	☐	0 kbps	Disable	☐	0 kbps	Disable
13	☐	0 kbps	Disable	☐	0 kbps	Disable
14	☐	0 kbps	Disable	☐	0 kbps	Disable
15	☐	0 kbps	Disable	☐	0 kbps	Disable
16	☐	0 kbps	Disable	☐	0 kbps	Disable
17	☐	0 kbps	Disable	☐	0 kbps	Disable
18	☐	0 kbps	Disable	☐	0 kbps	Disable
19	☐	0 kbps	Disable	☐	0 kbps	Disable
20	☐	0 kbps	Disable	☐	0 kbps	Disable
21	☐	0 kbps	Disable	☐	0 kbps	Disable
22	☐	0 kbps	Disable	☐	0 kbps	Disable
23	☐	0 kbps	Disable	☐	0 kbps	Disable
24	☐	0 kbps	Disable	☐	0 kbps	Disable
25	☐	0 kbps	Disable	☐	0 kbps	Disable
26	☐	0 kbps	Disable	☐	0 kbps	Disable
27	☐	0 kbps	Disable	☐	0 kbps	Disable
28	☐	0 kbps	Disable	☐	0 kbps	Disable

Apply

Рис. 179. Настройка аларма трафика порта

- **input rate alarm/output rate alarm**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включить / отключить сигнализацию трафика порта.
- **Threshold**
  Диапазон: от 1 до 1000000000 бит/с или от 1 до 1000000 кбит/с.
  Функция: настроить пороговое значение для трафика порта.
- **Alarm Status**
  Варианты: Alarm / Normal
  Функция: просмотр состояния трафика порта. Тревога означает, что скорость входящего / исходящего трафика превышает пороговое значение и и генерируется аварийный сигнал.

Настройка и отображение сигнала ошибки CRC / потери пакета.

Перейти [Device Advanced Configuration] → [Alarm Control] → [Alarm about CRC/ Pkt Loss] для входа на страницу конфигурации аварийного сигнала ошибки CRC / потери пакета, как показано на рисунке ниже.

Alarm about CRC/Pkt Loss

Port	CRC			Pkt Loss Alarm		
	Enable	Threshold	Alarm Status	Enable	Threshold	Alarm Status
1	☐	0 pps	Disable	☐	0 pps	Disable
2	☐	0 pps	Disable	☐	0 pps	Disable
3	☐	0 pps	Disable	☐	0 pps	Disable
4	☑	1 pps	Normal	☑	1 pps	Normal
5	☐	0 pps	Disable	☐	0 pps	Disable
6	☑	1000000 pps	Normal	☑	1000000 pps	Normal
7	☐	0 pps	Disable	☐	0 pps	Disable
8	☐	0 pps	Disable	☐	0 pps	Disable
9	☐	0 pps	Disable	☐	0 pps	Disable
10	☐	0 pps	Disable	☐	0 pps	Disable
11	☐	0 pps	Disable	☐	0 pps	Disable
12	☐	0 pps	Disable	☐	0 pps	Disable
13	☐	0 pps	Disable	☐	0 pps	Disable
14	☐	0 pps	Disable	☐	0 pps	Disable
15	☐	0 pps	Disable	☐	0 pps	Disable
16	☐	0 pps	Disable	☐	0 pps	Disable
17	☐	0 pps	Disable	☐	0 pps	Disable
18	☐	0 pps	Disable	☐	0 pps	Disable
19	☐	0 pps	Disable	☐	0 pps	Disable
20	☐	0 pps	Disable	☐	0 pps	Disable
21	☐	0 pps	Disable	☐	0 pps	Disable
22	☐	0 pps	Disable	☐	0 pps	Disable
23	☐	0 pps	Disable	☐	0 pps	Disable
24	☐	0 pps	Disable	☐	0 pps	Disable
25	☐	0 pps	Disable	☐	0 pps	Disable
26	☐	0 pps	Disable	☐	0 pps	Disable
27	☐	0 pps	Disable	☐	0 pps	Disable
28	☐	0 pps	Disable	☐	0 pps	Disable

Apply

Рис. 180. Настройка аларма ошибки CRC / потери пакета

- **CRC/Pkt Loss Alarm**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включение/отключение CRC/сигнала потери Pkt.
- **Threshold**
  Диапазон: от 1 до 1000000pps.
  Функция: Настройте пороговое значение для аварийного сигнала потери портов CRC/Pkt.

- **Alarm Status**
  Варианты: Alarm / Normal
  Функция: просмотр статуса потери портов CRC / Pkt. Аварийный сигнал означает, что потеря CRC / Pkt порта превышает пороговое значение и вызывает аварийный сигнал.

Настройка и отображение сигнала тревоги ST-Ring

Перейти [Device Advanced Configuration] → [Alarm Control] → [Set Ring Alarm] для входа на страницу конфигурации тревоги ST-Ring, как показано на рисунке ниже.

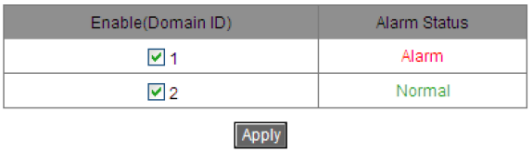


Рис. 181. Настройка и отображение сигнала тревоги ST-Ring

- **Alarm About ST-Ring**
  Опции: Disable / Enable
  По умолчанию: Disable
  Функция: включить / отключить сигнал ST-Ring.
- **Alarm Status**
  Варианты: Alarm / Normal
  Функция: просмотр состояния ST-Ring. Нормальный означает, что кольцо ST закрыто. Аварийный сигнал означает, что ST-Ring разомкнут или, находится в ненормальном состоянии.

Конфигурирование и отображение SFP порта RX тревоги

Перейти [Device Advanced Configuration] → [Alarm Control] → [Sfp Port Rx Power Alarm] для входа на страницу конфигурации аварийного сигнала питания порта SFP RX, как показано на рисунке ниже.

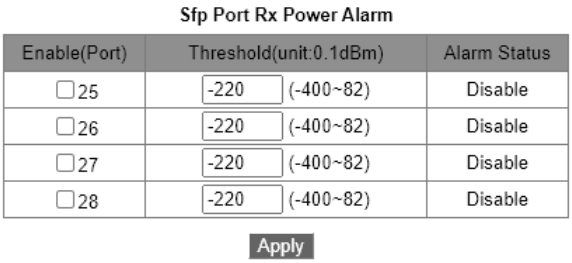


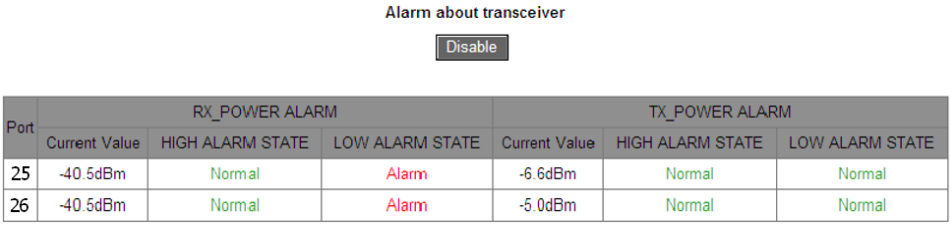
Рис. 182. Настройка аларма SFP порта RX

- **Sfp Port Rx Power Alarm**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включение / отключение сигнала тревоги питания RX порта SFP.

- **Threshold**
  Диапазон: -400~82 (единица измерения: 0,1 дБм)
  По умолчанию: -220 (-22,0 дБм)
  Функция: Настройка порога для сигнала тревоги мощности RX порта SFP.
- **Alarm Status**
  Варианты: Alarm / Normal
  Функция: после включения функции тревога означает, что мощность Rx для порта SFP меньше указанного порога и вызывает тревогу.

Настройка и отображение сигнала тревоги оптического модуля (трансивера).

Перейти [Device Advanced Configuration] → [Alarm Control] → [Alarm about transceiver] для входа на страницу конфигурации тревог трансивера, как показано на рисунке ниже.



Port	RX_POWER ALARM			TX_POWER ALARM		
	Current Value	HIGH ALARM STATE	LOW ALARM STATE	Current Value	HIGH ALARM STATE	LOW ALARM STATE
25	-40.5dBm	Normal	Alarm	-6.6dBm	Normal	Normal
26	-40.5dBm	Normal	Alarm	-5.0dBm	Normal	Normal

Рис. 183. Настройка и отображение сигнала тревоги оптического модуля

- **Alarm about transceiver**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включить / выключить сигнализацию приемопередатчика. Аварийный сигнал о низком уровне оптической мощности генерируется, когда отслеживаемое значение оптической мощности на порту SFP меньше нижнего порога аварийного сигнала; тревога высокой оптической мощности генерируется, когда отслеживаемое значение оптической мощности на порту SFP превышает пороговое значение верхней тревоги.

Низкий и высокий порог оптической мощности определяются аппаратным обеспечением и не могут быть настроены программно.

6.11. Конфигурация журнала

6.11.1. Введение

Функция журнала коммутатора в основном записывает такую информацию, как изменения состояния, неисправности, отладка и ошибки системы коммутатора. С помощью конфигурации информация журнала может быть загружена на сервер, поддерживающий протокол Syslog, в режиме реального времени. Информация журнала разделена на 3 уровня важности, от низкого к высокому: ERROR (ОШИБКА), WARNNING (ПРЕДУПРЕЖДЕНИЕ), NOTICE (УВЕДОМЛЕНИЕ)

информационный уровень	Описание
ERROR	Аномальный процесс неправильной работы или оборудования требует внимания и анализа причин
WARNNING	Аномальные моменты в ненормальной работе оборудования и процессов, которые могут привести к сбоям, требуют внимания
NOTICE	Критическая оперативная информация для правильного функционирования оборудования

6.11.2. Веб конфигурирование

Настроика функции журнала

Перейти [Device Advanced Configuration] → [Logging Configuration] → [Logging Configuration] для входа на страницу конфигурирование журнала, как показано на рисунке ниже.

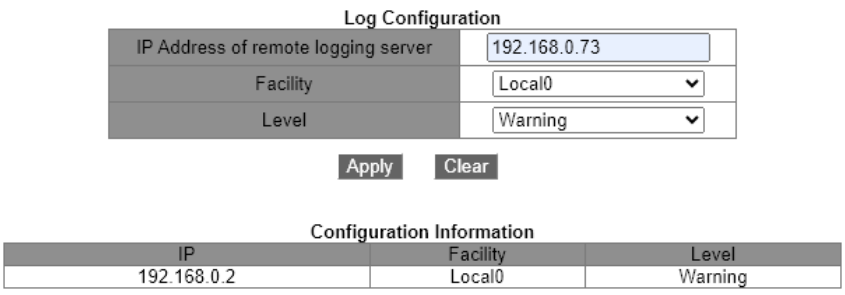


Рис. 184. Настроика функции журнала

- **IP Address of remote logging server**
  Настройте IP-адрес сервера, на который загружается информация журнала.
- **Facility**
  Опции: Local0 - Local7

По умолчанию: Local0

Описание: Средство используется для идентификации различных источников журналов на сервере журналов.

- **Level**

  Варианты: ERROR / WARNNING / NOTICE

  По умолчанию: Warning

  Функция: Выберите уровень записываемой информации журнала.

  Описание: Информация журнала может быть отфильтрована по уровням.

Вы можете установить программное обеспечение Syslog Server, например, Tftp32, на ПК для создания «Syslog Server». Информация журнала может отображаться в режиме реального времени на сервере Syslog, как показано на рисунке ниже.

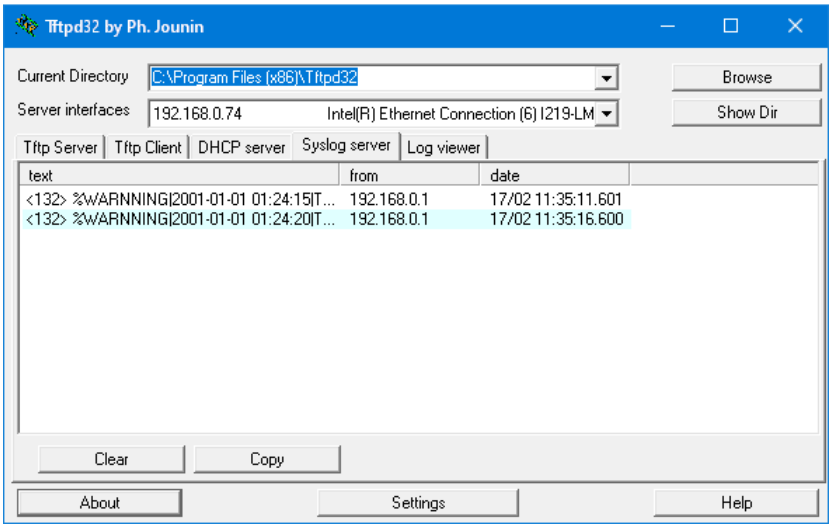


Рис. 185. Отображение информации в Syslog Server

Просмотр конфигурации журнала

Перейти [Device Advanced Configuration] → [Logging Configuration] → [showLogInfo] для входа на страницу просмотра лога, как показано на рисунке ниже.

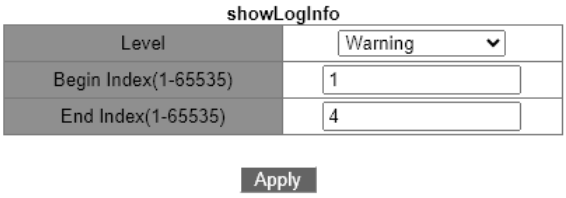


Рис. 186. Просмотр конфигурации журнала

- **Level**

  Опции: ERROR / WARNNING / NOTICE

  По умолчанию: Warning

  Функция: выберите уровень отображаемой информации журнала.

- **Begin Index/End Index**

  Диапазон: 1~65535

Функция: просмотр указанной информации журнала в буфере, и одна строка указывает на одну запись. На рисунке ниже показана указанная информация журнала в буфере.

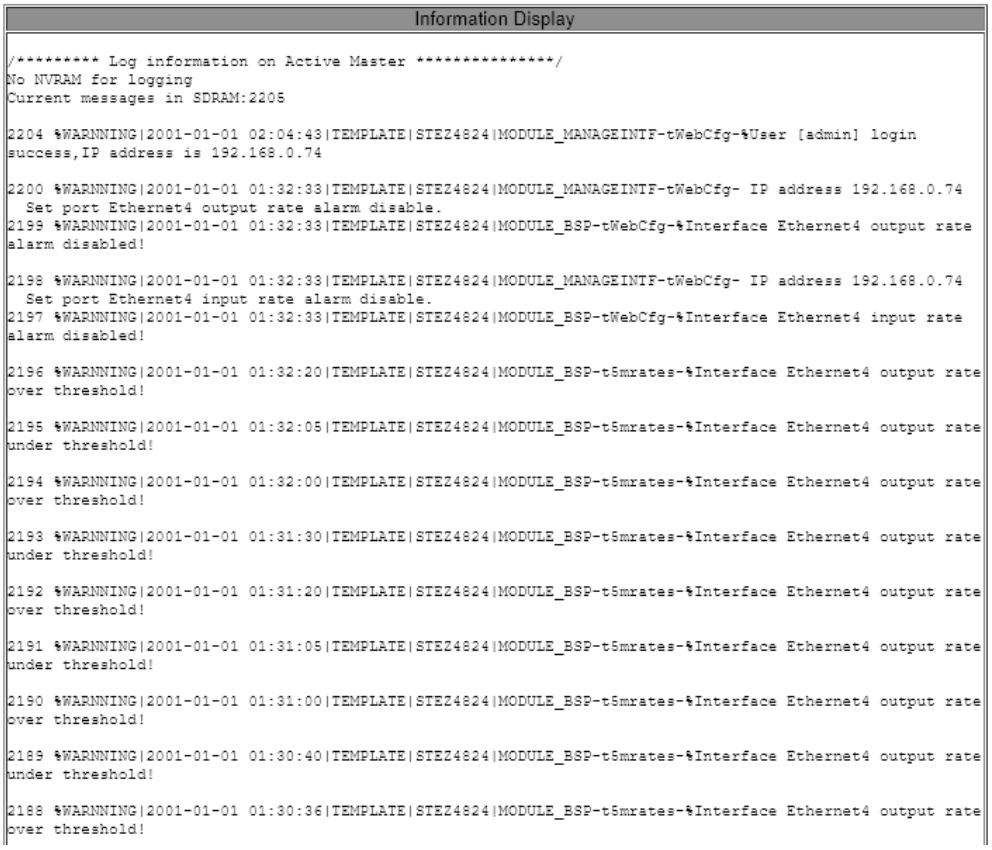


Рис. 187. Отображение журнала

Загрузка журнала с помощью FTP

Перейти [Device Advanced Configuration] → [Log Configuration] → [Log Transmit] для входа на страницу загрузки журнала, как показано на рисунке ниже.

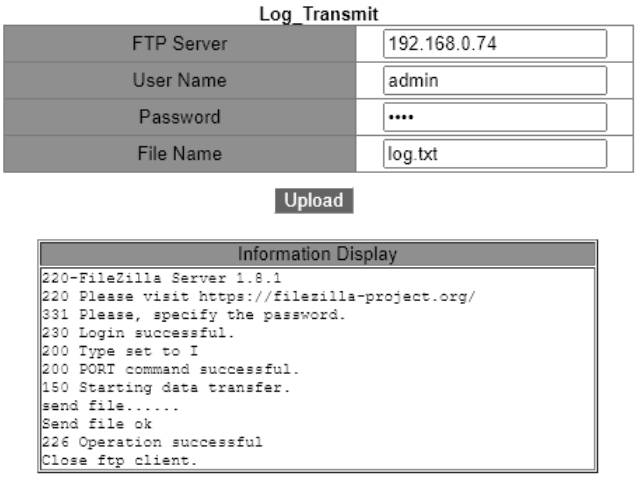


Рис. 188. Загрузка журнала с помощью FTP

- **FTP Server**
  Формат: A.B.C.D.
  Функция: Установите IP-адрес FTP-сервера.
- **User Name**
  Функция: Настройка имени пользователя FTP.
- **Password**
  Функция: Настройка пароля пользователя FTP.
- **File Name**
  Диапазон: 1~32 символа
  Функция: установить имя файла, сохраненного на сервере.

FTP-сервер должен оставаться в онлайн-состоянии во время загрузки журналов.

6.12. Конфигурация DHCP

С постоянным расширением масштаба сети и ростом сложности сети, в условиях частого перемещения компьютеров (таких как ноутбуки или беспроводная сеть) и количества компьютеров, превышающих выделяемые IP-адреса, протокол BootP, специально предназначенный для статического хоста. конфигурация становится все более неспособной удовлетворить фактические потребности. Для быстрого доступа и выхода из сети и улучшения коэффициента использования ресурсов IP-адресов нам необходимо разработать автоматический механизм на основе BootP для назначения IP-адресов. DHCP (протокол динамической конфигурации хоста) был введен для решения этих проблем. DHCP использует модель связи клиент-сервер. Клиент отправляет запрос конфигурации на сервер, а затем сервер отвечает на параметры конфигурации, такие как IP-адрес, клиенту, достигая динамической конфигурации IP-адресов. Структура типичного приложения DHCP показана на рисунке ниже.

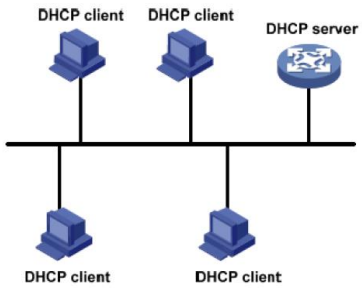


Рис. 189. Структура типичного приложения DHCP

В процессе динамического получения IP-адресов сообщения передаются способом широковещательной рассылки, поэтому требуется, чтобы DHCP-клиент и DHCP-сервер находились в одном сегменте. Если они находятся в разных сегментах, клиент может связаться с сервером через ретранслятор DHCP, чтобы получить IP-адреса и другие параметры конфигурации.

DHCP поддерживает два типа механизмов распределения IP-адресов.

Статическое распределение: сетевой администратор статически привязывает фиксированные IP-адреса к нескольким конкретным клиентам, таким как WWW-сервер, и отправляет связывающие IP-адреса клиентам по DHCP.

Динамическое выделение: DHCP-сервер динамически выделяет IP-адрес клиенту. Этот механизм выделения может выделить клиенту постоянный IP-адрес или IP-адрес с ограниченным сроком аренды. Когда срок аренды истекает, клиенту необходимо повторно применить IP-адрес.

Сетевой администратор может выбрать механизм распределения DHCP для каждого клиента.

6.12.1. Конфигурация DHCP Server

6.12.1.1. Введение

DHCP-сервер — поставщик услуг DHCP. Он использует DHCP-сообщения для связи с DHCP-клиентом, чтобы выделить клиенту, подходящий IP-адрес и при необходимости назначить ему другие сетевые параметры. В следующих случаях DHCP-сервер обычно используется для выделения IP-адресов.

- Большой масштаб сети. Рабочая нагрузка ручной настройки велика, и трудно управлять всей сетью.
- Количество хостов превышает количество назначаемых IP-адресов, и он не может выделить фиксированный IP-адрес каждому хосту.
- Только несколько хостов в сети нуждаются в фиксированных IP-адресах.

6.12.1.2. Пул адресов

DHCP-сервер выбирает IP-адрес из пула адресов и выделяет его вместе с другими параметрами клиенту. Последовательность распределения IP-адресов следующая:

- IP-адрес статически привязан к MAC-адресу клиента.
- IP-адрес, записанный на DHCP-сервере, который когда-либо был выделен клиенту.
- IP-адрес, указанный в сообщении запроса, отправленном от клиента.
- Первый выделяемый IP-адрес, найденный в пуле адресов.
- Если нет доступного IP-адреса, проверьте IP-адрес, срок аренды которого истекает и который имел конфликты по порядку. Если найдено, выделите IP-адрес. Если нет, то нет процесса.

6.12.1.3. Веб конфигурирование

Включение DHCP сервера

Перейти [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Enable DHCP] для входа на страницу включения DHCP сервера, как показано на рисунке ниже.

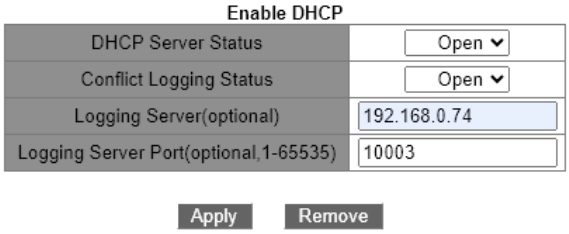


Рис. 190. Включение DHCP сервера

- **Состояние DHCP-сервера**
  Варианты конфигурации: Enable / Disable
  Конфигурация по умолчанию: Disable
  Функция: следует ли выбирать текущий коммутатор в качестве DHCP-сервера для назначения IP-адресов клиентам.
- **Статус журнала конфликтов адресов**
  Варианты конфигурации: Enable / Disable
  Конфигурация по умолчанию: открытая
  Функция: когда IP-адрес, примененный клиентом, конфликтует с другими выделенными IP-адресами, соответствующие журналы могут быть записаны.
- **Адрес сервера журналов (необязательно)**
  Диапазон конфигурации: Настройте IP-адрес сервера для загрузки информации журнала.
  Функция: IP-адрес сервера лог-информации
- **Порт сервера журнала (необязательно, 1~65535)**
  Диапазон конфигурации: 1~65535
  Функция: настроить порт сервера для загрузки информации журнала.

Выделение статического IP адреса

Перейти [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Address pool configuration] для создания DHCP адресного пула, как показано на рисунке ниже.

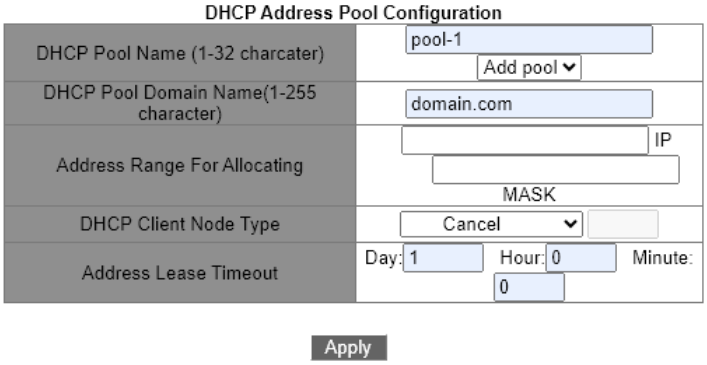


Рис. 191. Создание DHCP адресного пула

- **DHCP pool name**
  Диапазон: 1~32 символа
  Функция: настроить имя пула IP-адресов.
- **DHCP pool domain name**
  Диапазон: 1~255 символов
  Функция: настроить доменное имя пула IP-адресов. При назначении IP-адреса клиенту также отправьте клиенту суффикс доменного имени.
- **Address lease timeout**
  Диапазон: 0 дней 0 часов 0 минут ~ 365 дней 23 часов 59 минут
  Описание. Тайм-аут аренды статического выделения бесконечен. Конфигурация этого параметра недопустима для статического распределения.

Статическое выделение IP-адреса можно рассматривать как получение IP-адреса из специального пула адресов, который содержит только один конкретный IP-адрес. Следовательно, пул адресов DHCP должен быть создан перед статически выделенным IP-адресом.
Для каждого пула адресов DHCP можно настроить только один тип механизма распределения IP-адресов.

Перейти [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Manual address pool configuration] для входа на страницу назначения статического адреса, как показано на рисунке ниже.

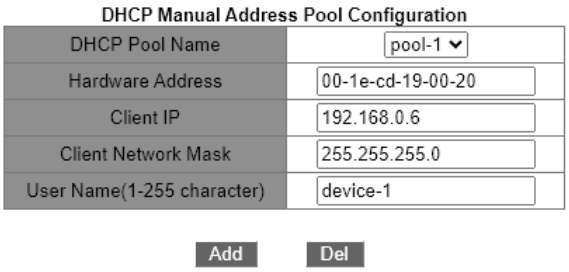


Рис. 192. Назначение статического адреса

- **DHCP pool name**
  Функция: выбрать имя созданного пула.
- **Hardware address**
  Формат: HH-HH-HH-HH-HH-HH (H — шестнадцатеричное число)
  Функция: Настройка MAC-адреса клиента со статическим ограничением.
- **Client IP**
  Формат: A.B.C.D.
  Функция: Настройка IP-адреса клиента со статическим ограничением.
  Описание. Статическое выделение IP-адресов реализовано путем связывания MAC-адреса и IP-адреса клиента. Когда клиент с этим MAC-адресом запрашивает IP-адрес, DHCP-сервер находит IP-адрес, соответствующий MAC-адресу клиента, и выделяет IP-адрес клиенту. Приоритет этого режима выделения выше, чем у динамического выделения IP-адресов, а срок аренды является постоянным.

- **Client network mask**
  Маска подсети представляет собой число длиной 32 бита, состоящее из строки 1 и строки 0. «1» соответствует полям номера сети и полям номера подсети, а «0» соответствует полям номера хоста. Обычно он настроен на 255.255.255.0.
- **User name**
  Диапазон: 1~255 символов
  Функция: Настройка имени пользователя клиента.

Динамическое назначение IP адреса

Перейти [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Address pool configuration] для входа на страницу конфигурации динамического распределения, как показано на рисунке ниже.

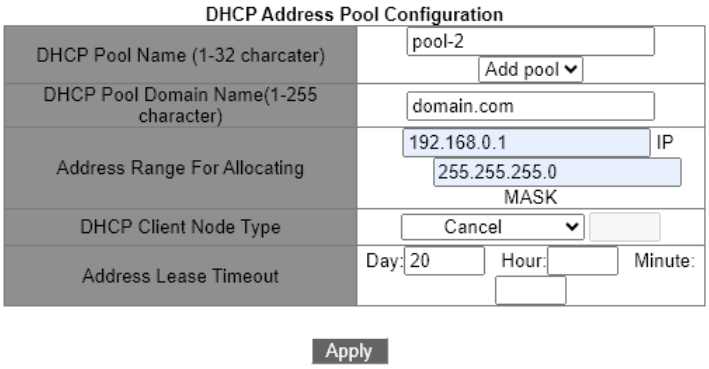


Рис. 193. Динамическое назначение IP адреса

- **DHCP pool name**
  Диапазон: 1~32 символа
  Функция: настроить имя пула IP-адресов.
- **DHCP pool domain name**
  Диапазон: 1~255 символов
  Функция: настроить доменное имя пула IP-адресов. При назначении IP-адреса клиенту также отправьте клиенту суффикс доменного имени.
- **Address range of allocating {IP, MASK}**
  Функция: Настройте диапазон пула IP-адресов, а диапазон адресов определяется маской подсети. Маска подсети представляет собой число длиной 32 бита, состоящее из строки 1 и строки 0. «1» соответствует полям номера сети и полям номера подсети, а «0» соответствует полям номера хоста. Обычно он настроен на 255.255.255.0.

В каждом пуле адресов можно настроить только один сегмент адреса.

- **DHCP client node type**
  Опция: Cancel / Broadcast node / Peer-to-peer node / Mixed node / Hybrid node
  По умолчанию: Cancel
  Функция: Настройка типа клиентского узла NetBIOS, выделенного DHCP-сервером. Когда DHCP-клиент использует протокол NetBIOS для связи в сети, необходимо

установить сопоставление между именем хоста и IP-адресом. Различные типы узлов получают отображение в разных режимах.

Описание: Широковещательный узел получает отображение в широковещательном режиме. Одноранговый узел получает сопоставление, отправляя одноадресный пакет для связи с WINS-сервером. Смешанный узел получает отображение, посылая широковещательный пакет в первый раз. Если смешанный узел не может получить сопоставление в первый раз, он получает сопоставление, отправляя одноадресный пакет для связи с WINS-сервером во второй раз. Гибридный узел получает сопоставление, отправляя одноадресный пакет для связи с WINS-сервером в первый раз. Если гибридному узлу не удается получить сопоставление в первый раз, он получает сопоставление, отправив широковещательный пакет во второй раз.

- **Address lease timeout**

  Диапазон: 0 дней 0 часов 0 минут ~ 365 дней 23 часов 59 минут

  Описание: Настройка тайм-аута аренды динамического распределения. Для разных пулов адресов сервер DHCP может установить разное время аренды адреса, но адреса в одном пуле адресов DHCP имеют одинаковое время аренды.

Конфигурирование DHCP шлюза клинета

Перейти [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Client's Default Gateway Configuration] для входа на страницу конфигурации шлюза DHCP-клиента, как показано на рисунке ниже.

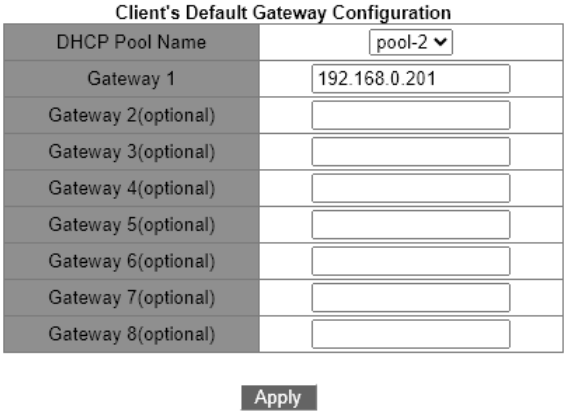


Рис. 194. Конфигурирование DHCP шлюза клинета

- **DHCP pool name**

  Функция: выбрать имя созданного пула.

- **Gateway 1~Gateway 8**

  Функция: настроить адрес клиентского шлюза, выделенный DHCP-сервером.

  Объяснение: когда DHCP-клиент посещает хост, находящийся в другом сегменте, данные должны пересылаться через шлюзы. Когда DHCP-сервер выделяет IP-адреса клиентам, он может одновременно указывать адреса шлюза. Пул адресов DHCP может настроить до 8 шлюзов. Шлюз 1 имеет наивысший приоритет, а шлюз 8 - наименьший.

Конфигурирование DHCP-клиента DNS-сервера

Перейти [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Client DNS server configuration] для входа на страницу конфигурации DNS-сервера DHCP-клиента, как показано на рисунке ниже.

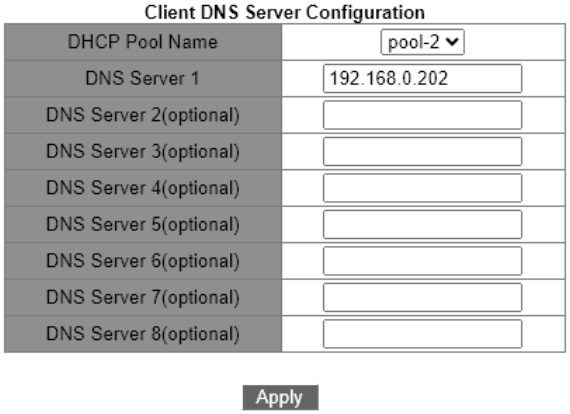


Рис. 195. Конфигурирование DHCP-клиента DNS-сервера

- **DHCP pool name**
  Функция: выбрать имя созданного пула.
- **DNS server 1~DNS server 8**
  Функция: Настройка адреса клиентского DNS-сервера, назначенного DHCP-сервером.
  Объяснение: При посещении сетевого узла через доменное имя доменное имя должно быть преобразовано в IP-адрес, который реализуется DNS (системой доменных имен). Чтобы DHCP-клиент мог посещать сетевой хост через доменное имя, когда DHCP-сервер выделяет IP-адреса клиентам, он может одновременно указывать IP-адреса серверов доменных имен. Пул адресов DHCP может настроить максимум 8 DNS-серверов. DNS-сервер 1 имеет наивысший приоритет, а DNS-сервер 8 — самый низкий приоритет.

Конфигурирование DHCP-клиента WINS-сервера

Перейти [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Client WINS server configuration] для входа на страницу конфигурации WINS-сервера DHCP-клиента, как показано на рисунке ниже.

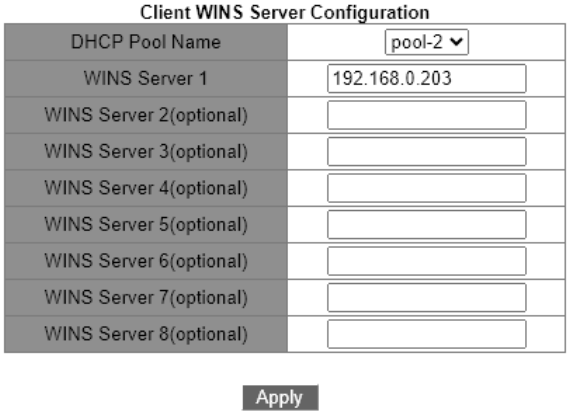


Рис. 196. Конфигурирование DHCP-клиента WINS-сервера

- **DHCP pool name**
  Функция: выбрать имя созданного пула.
- **WINS server 1~WINS server 8**
  Функция: Настройка адреса клиентского WINS-сервера, выделенного DHCP-сервером.
  Описание: Для клиента, работающего под управлением операционной системы (ОС) Microsoft Windows, сервер Windows Internet Naming Service (WINS) предоставляет услугу преобразования имени хоста в IP-адрес для хоста, использующего для связи протокол NetBIOS. Поэтому для большинства клиентов на базе ОС Windows требуется настройка WINS. Чтобы DHCP-клиент мог преобразовать имя хоста в IP-адрес, укажите адрес WINS-сервера, когда DHCP-сервер выделяет IP-адрес клиенту. Пул адресов DHCP может настроить до 8 серверов WINS. WINS-сервер 1 имеет наивысший приоритет, а WINS-сервер 8 — самый низкий приоритет.

Настройка DHCP-клиента, адреса TFTP-сервера и имени загрузочного файла

Перейти [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [DHCP file server address configuration] для ввода адреса DHCP-клиента TFTP-сервера и страницы конфигурации имени загрузочного файла, как показано на рисунке ниже.

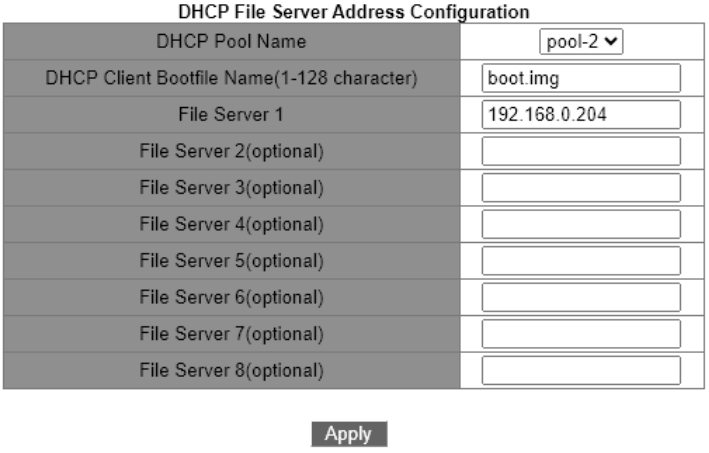


Рис. 197. Настройка DHCP-клиента, адреса TFTP-сервера и имени загрузочного файла

- **DHCP pool name**
  Функция: выбрать имя созданного пула.
- **DHCP client bootfile name**
  Имя загрузочного файла DHCP-клиента
  Диапазон: 1~128 символов
  Функция: Настройка имени файла запуска клиента, назначенного DHCP-сервером. При запуске бездискового устройства файл запуска должен быть загружен с сервера, а затем импортирован.
- **File server 1~File server 8**
  Функция: Настройка адреса клиентского TFTP-сервера, выделенного DHCP-сервером. Пул адресов DHCP может настроить до 8 файловых серверов. Файловый сервер 1 имеет наивысший приоритет, а файловый сервер 8 — самый низкий.

Конфигурирование сетевых параметров пула адресов DHCP

Перейти [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [DHCP network parameter configuration] для входа на страницу конфигурации сетевых параметров DHCP, как показано на рисунке ниже.

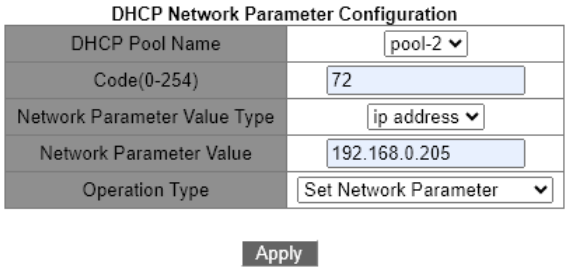


Рис. 198. Конфигурирование сетевых параметров пула адресов DHCP

- **DHCP pool name**
  Функция: выбрать имя созданного пула.
- **Code**
  Диапазон: 0~254
  Функция: настройка опции DHCP. DHCP сохраняет формат сообщения BootP для совместимости с BootP. Недавно добавленная функция BootP реализуется через поле **Option**. DHCP передает управляющую информацию и параметры конфигурации сети через поле **Option**, реализуя распределение IP-адресов и предоставляя клиенту более подробную информацию о конфигурации. Например, Option72 — это параметр WWW-сервера, который используется для указания адреса WWW-сервера, выделяемого клиенту.

Дополнительные сведения об опциях DHCP см. в документе RFC2132.
Веб-страница обеспечивает настройку общих параметров (например, адрес шлюза, адрес DNS-сервера и адрес WINS-сервера). Коды сетевых параметров не могут быть настроены как эти общие параметры.

- **Network parameter value type**
  Опции: ascii / hex / ip-адрес
  Функция: Настройка типа значения сетевого параметра. ascii — это строка символов ascii, и ее диапазон конфигурации составляет от 1 до 255 символов. Hex — это шестнадцатеричное число, и длина его конфигурации должна быть четным числом в диапазоне от 1 до 510.
- **Network parameter value**
  Функция: Настройка соответствующего значения сетевого параметра на основе типа значения сетевого параметра.

Настройка диапазона IP-адресов, не выделяемых динамически в DHCP-адрес пуле

Перейти [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Excluded address configuration] для входа в конфигурацию исключенного адреса на странице, как показано на рисунке ниже.

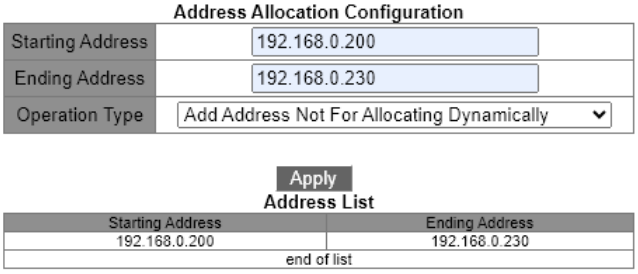


Рис. 199. Настройка нераспределямых адресов

- **Starting address/Ending address**
  Функция: настроить диапазон IP-адресов, которые не распределяются динамически в DHCP. пул адресов. При распределении IP-адресов DHCP-сервер должен устранять занятые IP-адрес (например, IP-адреса шлюза и DNS-сервера). В противном случае один и тот же IP-адрес может быть назначен двум клиентам, что приведет к конфликту IP-адресов.

Просмотр статитстики DHCP пакетов

Перейти [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [DHCP packet statistics] для просмотра DCHP статитстики, как показано на рисунке ниже.

DHCP Packet Statistics

Memory Usage Rate	741
Address Pool	2
Proxy Database	0
Dynamical Allocated Address	1
Manual Binded Address	1
Address Conflict	0
Binding Exceeding Lease Time	2
Errors	0

Received DHCP Packet Statistics

Received	7
DHCPDISCOVER	2
DHCPREQUEST	4
DHCPDECLINE	0
DHCPRELEASE	1
DHCPINFORM	0

Transmitted DHCP Packet Statistics

Transmitted	6
DHCPOFFER	0
DHCPACK	0
DHCPNAK	2
DHCPRELAY	4
DHCPFORWARD	0
DHCP Server Option82 Error Packet Count	0
DHCP Relay Option82 Error Packet Count	0

Clear Show

Рис. 200. Просмотр статитстики DHCP пакетов

Вы можете нажать кнопку <Show>, чтобы обновить статистику пакетов данных DHCP в режиме реального времени, и вы можете нажать кнопку <Clear>, чтобы очистить статистику полученных / отправленных пакетов данных DHCP.

Конфигурация DHCP-сервера Option82

Перейдите в дерево навигации в меню [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration]→[DHCP Server Option82 Config], чтобы войти в интерфейс конфигурации DHCP-сервера Option82, как показано на рис. ниже

Server Option82 Configuration

Status	Enable

Apply

Рис. 201. Конфигурация DHCP-сервера Option82

- **Status**
  Диапазон конфигурации: Disable / Enable
  Функция: следует ли включить функцию Option82 устройства DHCP.

Пул адресов DHCP Конфигурация Option82

Перейдите в дерево навигации меню [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [DHCP Pool Option82 Configuration], чтобы войти в интерфейс настройки пула адресов DHCP Option82, как показано на рис. Ниже

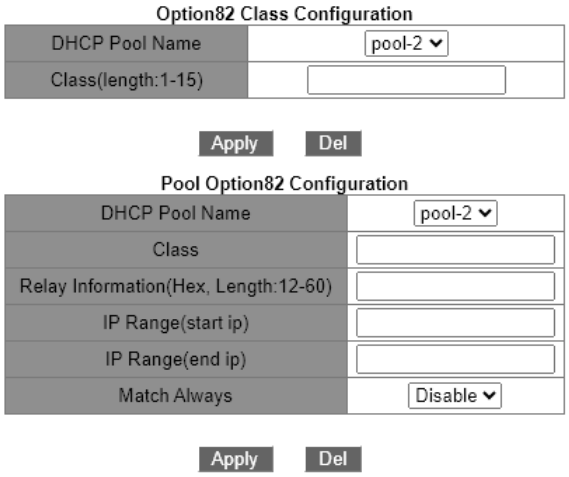


Рис. 202. Пул адресов DHCP Конфигурация Option82

- **Class**
  Диапазон конфигурации: 1-15
- **Relay Information**
  Диапазон конфигурации: шестнадцатеричное число, длина: 12-60
  Функция: информация, которую необходимо сопоставить.
- **IP Range(start ip)**
  Функция: назначить диапазон IP-адресов.
- **IP Range(end ip)**
  Функция: назначить диапазон IP-адресов.
- **Match Always**
  Диапазон конфигурации: Disable / Enable
  Функция: выполнять ли функцию сопоставления присваивания

Конфигурация DHCP-ретранслятора

Перейдите в дерево навигации меню [Device Advanced Configuration]→[DHCP configuration]→[DHCP server configuration]→[DHCP Relay Configuration]→[DHCP Relay Configuration], чтобы войти в интерфейс настройки DHCP-ретрансляции, как показано на рисунке ниже.

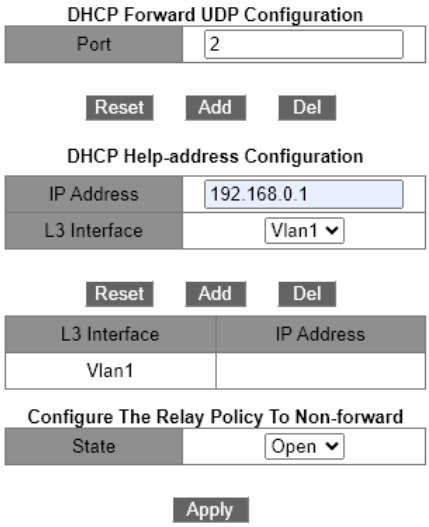


Рис. 203. Конфигурация DHCP-ретранслятора

- **Port**
  Функция: настроить порт для пересылки сообщений DHCP UDP, общий порт DHCP UDP (67/68)
- **IP Address**
  Диапазон конфигурации: IP-адрес DHCP-сервера.
- **L3 Interface**
  Диапазон конфигурации: 1-4094
  Функция: виртуальный интерфейс уровня 3, на котором находится DHCP-сервер.
- **State**
  Диапазон конфигурации: вкл./выкл.
  Функция: пересылает ли реле сообщения DHCP.

Устранение неполадок DHCP, удаление записей привязки

Перейдите в дерево навигации [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [DHCP Debugging] → [Delete Binding Log], чтобы войти в интерфейс удаления записи привязки, как показано на рисунке ниже.

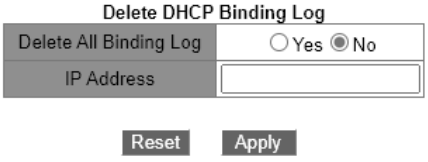


Рис. 204. Удаление записей привязки DHCP

- **Delete All Binding Log**
  Варианты конфигурации: да/нет
- **IP Address**
  Функция: удалить назначенную запись IP-адреса.

Устранение неполадок DHCP, удаление записей о конфликтах

Перейдите в дерево навигации [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [DHCP Debugging] → [Delete Conflict Log], чтобы войти в интерфейс удаления записи о конфликте, как показано на рисунке ниже;

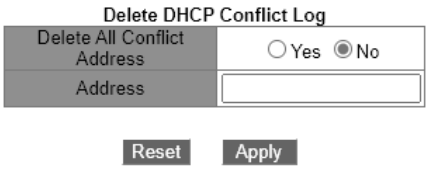


Рис. 205. Удаление записей о конфликтах DHCP

- **Delete All Conflict Address**
  Варианты конфигурации: да/нет
- **Address**
  Функция: удалить назначенный конфликтующий IP-адрес.

Удалить статистические записи DHCP-сервера

Перейдите в дерево навигации меню [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [DHCP Debugging] → [Delete DHCP Server Statistics Log], чтобы войти в интерфейс удаления статистических записей DHCP-сервера, как показано на рисунке ниже;

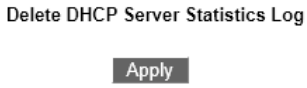


Рис. 206. Удаление статистических записей DHCP-сервера

Функция: очистить записи DHCP-сервера.

Просмотр инфомрациии о привязке IP-MAC

Перейдите в [Device Basic Configuration] → [DHCP configuration] → [DHCP debugging] → [Show IP-MAC binding] просмотеть информации о приязке IP-MAC можно, как показано на рисунке ниже.

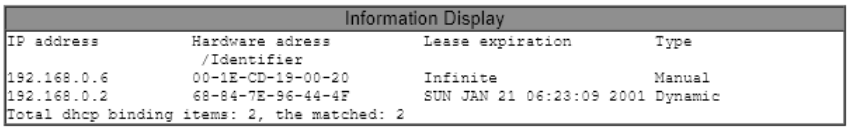


Рис. 207. Просмотр инфомрациии о привязке IP-MAC

Отображение информации журнала конфликтов

Перейдите в дерево навигации [Device Basic Configuration] → [DHCP configuration] → [DHCP debugging] → [Show Conflict-logging], чтобы войти в интерфейс отображения привязки IP-адресов и MAC-адресов, как показано на рис. ниже

```
                    Information Display
IP Address          Detection method    Detection Time
192.168.0.1         Ping                MON JAN 01 06:16:34 2001
```

Рис. 208. Отображение информации журнала конфликтов

6.12.1.4. Типовой пример конфигурации

Как показано на рис. ниже, коммутатор A действует как сервер DHCP, коммутатор B действует как клиент DHCP, а порт 3 коммутатора A подключен к порту 4 коммутатора B. Клиент отправляет сообщение запроса приложения IP-адреса, и сервер может назначить IP-адрес клиенту двумя способами. Когда DHCP-сервер динамически выделяет IP-адреса, IP-адреса в диапазоне от 192.168.0.1 до 192.168.0.9 не участвуют в динамическом распределении.

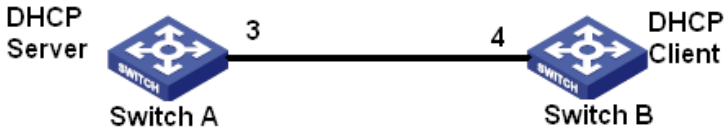


Рис. 209. Пример конфигурации

Статическое выделение IP-адресов

- Конфигурация коммутатора A:
  1. Откройте статус DHCP-сервера, см. рис. 190;
  2. Создать пул адресов pool-1, см. рис. 191;
  3. Привязать MAC-адрес коммутатора B: 00-1e-cd-19-00-02 и IP-адрес: 192.168.0.6, маска: 255.255.255.0, см. рис. 192;

- Конфигурация коммутатора B:
  1. Коммутатор B получает IP-адрес через bootp-client или dhcp-client, см. рис. 105;
  2. Коммутатор B получает от DHCP-сервера IP-адрес: 192.168.0.6, маска подсети: 255.255.255.0;

Динамическое выделение IP-адресов

- Конфигурация коммутатора A:
  1. Откройте статус DHCP-сервера, см. рис. 190;
  2. Создайте пул адресов pool-2, настройте доменное имя пула адресов как domain.com и диапазоны адресов, которые могут быть выделены: 192.168.0.3 (IP) и 255.255.255.0 (MASK), срок аренды 20 дней, как показано на рис. 193;
  3. Настройте диапазон IP-адресов 192.168.0.1~192.168.0.9, который не участвует в динамическом распределении, см. рис. 199;

- Конфигурация коммутатора B:
  1. Коммутатор B получает IP-адрес через bootp-client или dhcp-client, см. рис. 105;
  2. DHCP-сервер последовательно ищет доступные IP-адреса из пула адресов и назначает первый найденный IP-адрес: 192.168.0.10, маска подсети: 255.255.255.0 коммутатору B.

6.13. Конфигурация IEC61850

6.13.1. Введение

В настоящее время коммутаторы прозрачны для других функциональных объектов в сетях подстанций. Для мониторинга коммутаторов необходимы инструменты, отличные от IEC61850, такие как EMS, Web, CLI и OPC, что приводит к несогласованности и неудобству настройки сети и управления ею. Чтобы решить эти проблемы, мы создаем модели для коммутаторов в соответствии со стандартом IEC61850 и вводим коммутаторы в системы автоматизации подстанций в качестве интеллектуальных электронных устройств (IED), обеспечивая единое представление мониторинга автоматизации подстанции, облегчая планирование интеграции и управления, а также экономя строительство и затраты на техническое обслуживание.

Файл моделирования по умолчанию switch.cid, предоставленный компанией, уже импортирован в коммутатор. Если заказчик хочет импортировать другие файлы моделирования, обратитесь к разделу «Служба передачи файлов».

6.13.2. Веб конфигурирование

Включение IEC61850

Перейти [Device Advanced Configuration] → [IEC 61850 Function] → [IEC 61850 Function] для входа на страницу конфигурации IEC61850, как показано на рисунке ниже.

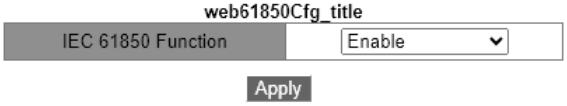


Рис. 210. Включение IEC61850

- **IEC61850 Function**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включение / выключение IEC61850 функции

Настройка параметров IEC61850

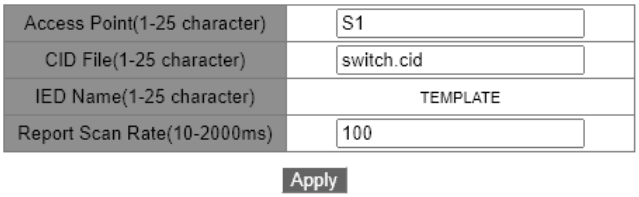


Рис. 211. Настройка параметров IEC61850

- **Access Point**
  Диапазон: 1~25 символов
  По умолчанию: S1
  Функция: Настройка имени точки доступа, соответствующей IED, в файле CID.
- **CID File**
  Диапазон: 1~25 символов
  По умолчанию: switch.cid
  Функция: Настройка имени действительного файла моделирования CID при запуске функции IEC61850.
- **IED Name**
  Диапазон: 1~25 символов
  По умолчанию: TEMPLATE
  Функция: Настройка имени логического устройства, соответствующего IED, в файле CID.
- **Report Scan Rate**
  Диапазон: 10~2000 мс
  По умолчанию: 100 мс
  Функция: настройка интервала сканирования информации об узле устройства.

Конфигурации имени точки доступа и устройства IED должны соответствовать имени точки доступа и устройства IED в указанном файле моделирования. В противном случае функция IEC61850 не может быть активирована.

6.14. Конфигурация GOOSE

GOOSE-Trigger определяет, следует ли подписываться на GOOSE-пакет, в соответствии с MAC-адресом получателя и идентификатором приложения GOOSE-пакета. Если устройство подписалось на пакет GOOSE, GOOSE-Trigger получает текущее время и информацию о состоянии коммутатора, содержащуюся в пакете (IEC61850 периодически запрашивает значение состояния коммутатора в режиме опроса. Если статус коммутатора переключается, он сообщает MMS REPORT).

Глобальная конфигурация Goose-sv

Перейдите [Device Advanced Configuration] → [Goose configuration] → [Goose-sv Global Configuration] для входа на страницу конфигурации Goose-sv qos, как показано на рисунке ниже.

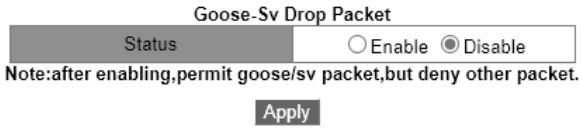


Рис. 212. Глобальная конфигурация Goose-sv

- **Goose Function**
  Опции: Включить/Выключить
  По умолчанию: Отключить
  Функция: включение/выключение функции триггера GOOSE. Устройство может подписываться на пакеты GOOSE после включения функции Goose.

Конфигурация GOOSE

Перейдите в дерево навигации [Device Advanced Configuration] → [Goose configuration] → [Goose-sv Qos Priority Configuration], чтобы войти в интерфейс настройки приоритета Goose-sv qos, как показано на рис. 213;

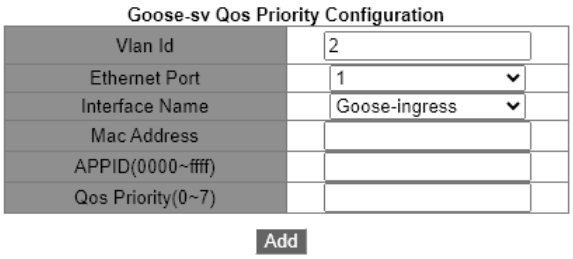


Рис. 213. Конфигурация GOOSE

- **VLAN ID**
  Диапазон конфигурации: 1-4094
  Функция: Установите соответствующее значение VLAN.
- **Ethernet Port**
  Объем конфигурации: все порты устройства
  Функция: Установите соответствующее значение порта.
- **Interface Name**
  Варианты конфигурации: входящее направление Goose-пакета/исходящее направление Goose-пакета/исходящее направление Sv-пакета/исходящее направление Sv-пакета
  Функция: Установить условия соответствия.
- **APP ID**
  Параметры: 0x0000~0xffff
  По умолчанию: 0x10ff

Функция: Настройка идентификатора приложения GOOSE-пакетов, на которые необходимо подписаться. После включения триггера GOOSE устройство подпишется на пакеты GOOSE с идентификатором приложения, соответствующим конфигурации.

- **Qos Priority(0~7)**
  Диапазон конфигурации: 0~7
  Функция: изменение соответствующего сообщения goose или sv на указанный приоритет (по умолчанию исходный приоритет сообщения goose равен 7).

6.15. ACL

6.15.1. Введение

Список управления доступом (Access Control List - ACL) позволяет пользователям настраивать правила сопоставления и режим обработки для пакетов во входящем направлении порта коммутатора для фильтрации пакетов. Он направлен на эффективное предотвращение доступа неавторизованных пользователей к сети, контроль трафика и экономию сетевых ресурсов.

6.15.2. Записи и правила

Запись ACL может содержать несколько правил, и в каждом правиле можно указать параметры сопоставления пакетов и обработки пакетов. Перед настройкой правила необходимо создать запись ACL. В нескольких правилах в одной записи ACL правило с меньшим идентификатором правила предшествует правилу с большим идентификатором правила. Действие сопоставления пакетов начинается с первого правила до тех пор, пока пакеты не будут соответствовать правилу, а последующие правила не будут использоваться для сопоставления.

Записи ACL могут применяться к портам, виртуальным локальным сетям и глобально. Когда несколько записей конфликтуют друг с другом, ACL, примененный к порту, имеет наивысший приоритет, тогда как ACL, примененный глобально, имеет самый низкий приоритет. Например, ACL1 (пакеты с IP-адресом назначения 192.168.0.3 будут отбрасываться) настроен на глобальное применение, ACL2 (пакеты с IP-адресом назначения 192.168.0.3 будут получены) настроен на применение к VLAN1, и ACL3 (пакеты с IP-адресом назначения 192.168.0.3 будут зеркалироваться) настроен для применения к порту 2/1. Порт 2/1 принадлежит VLAN1. ACL, применяемый к порту, предшествует ACL, применяемому к VLAN. Поэтому порт 2/1 зеркалирует пакеты с IP-адресом назначения 192.168.0.3. ACL, применяемый к VLAN, предшествует глобальному ACL. Таким образом, VLAN1 получает пакеты с IP-адресом назначения 192.168.0.3. В остальных случаях пакеты с IP-адресом назначения 192.168.0.3 отбрасываются.

Запись ACL представляет собой набор из одного или нескольких правил. Следовательно, после применения записи ACL к порту / VLAN / глобально все правила, содержащиеся в этой записи ACL, будут применяться к порту / VLAN / глобально.

По умолчанию ACL, применяемый к порту / VLAN / глобально, вступает в силу раньше, чем ACL, который должен применяться к тому же порту / VLAN / глобально, но

выдается позже. Пользователи могут настроить приоритет записей ACL по мере необходимости.

6.15.3. Веб конфигурация

Конфигурирование записи ACL

Перейти [Device Advanced Configuration] → [ACL configuration] → [ACL Base Configuration] для конфигурирования записи ACL, как показано на рисунке ниже.

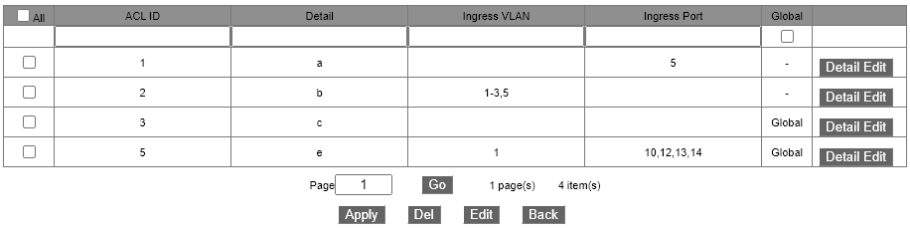


Рис. 214. Конфигурирование записи ACL

- **ACL ID**
  Диапазон: 1~1024
  Функция: Настройка идентификатора ACL. Данный тип коммутатора поддерживает до 512 записей ACL. Если запись ACL применяется к нескольким портам, она применяется к каждому из портов. Аналогичным образом, если запись ACL применяется к нескольким VLAN, она применяется к каждой из VLAN.
  Описание. Если запись ACL применяется к нескольким непрерывным портам или сетям VLAN, порты или сети VLAN могут быть разделены дефисом (-). Если запись ACL применяется к нескольким прерывистым портам или сетям VLAN, порты или сети VLAN могут быть разделены запятой (,).

Существуют некоторые системные записи ACL, и пользователи фактически могут настроить менее 512 записей ACL.

- **Detail**
  Диапазон: 1~127 символов
  Функция: Настройка информации описания для записи ACL.
- **Ingress VLAN / Ingress Port/ Global**
  Функция: Настройка области применения записи ACL.

Редактирование ACL записи показано на рисунке ниже

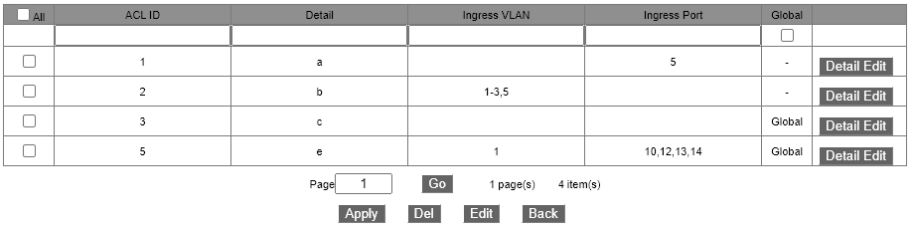


Рис. 215. Редактирование ACL записи

Выберите запись ACL, нажмите <Del>, чтобы удалить запись ACL; нажмите <Edit>, чтобы изменить конфигурацию записи ACL.

Добавление правила в ACL запись

Перейдите в созданную запись ACL чтобы открыть возможность добавление правил (смотри рисунок ниже), нажмите <Add Rule>, чтобы настроить правило для записи ACL.

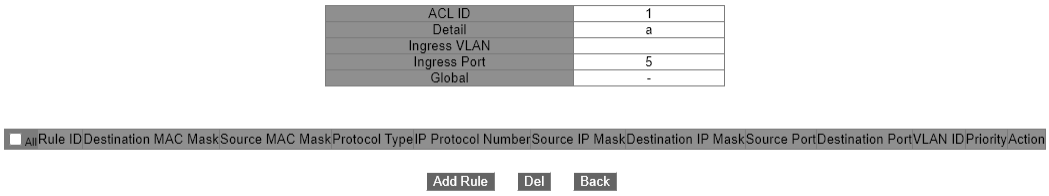


Рис. 216. Добавление правила в ACL запись

Настройка правил для записи ACL, как показано на рисунке ниже

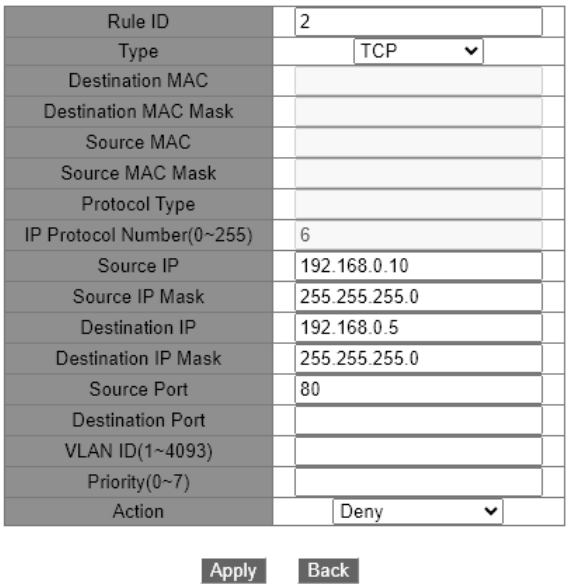


Рис. 217. Настройка правил для записи ACL

- **Rule ID**
  Диапазон: 1~1024
  Функция: Настройка идентификатора правила для записи ACL.
  Описание: Каждая запись ACL поддерживает максимум 512 правил, а общее количество правил во всех ACL не может превышать 512.
- **Type**
  Варианты: Customized/IGMP/ICMP/TCP/UDP/MAC
  По умолчанию: Customized
  Функция: Настройка типа пакета правила ACL.

- **Destination MAC/ Destination MAC Mask**
  Функция: Настройка MAC-адреса назначения. В маске MAC-адреса получателя **1** указывает на cared бит MAC-адреса получателя, а **0** указывает на игнорируемый бит MAC-адреса получателя.
- **Source MAC/ Source MAC Mask**
  Функция: Настройка исходного MAC-адреса. В маске MAC-адреса источника **1** указывает на cared бит MAC-адреса источника, а **0** указывает на игнорируемый бит MAC-адреса источника.
- **Protocol Type**
  Диапазон: 5DD-FFFF
  Функция: настройка типа протокола.
- **IP Protocol Number**
  Диапазон: 0~255
  Функция: настройка номера IP-протокола.
- **Source IP/ Source IP Mask**
  Функция: настройка исходного IP-адреса. В маске исходного IP-адреса 1 указывает на заботливый бит IP-адреса источника, а 0 указывает на игнорируемый бит исходного IP-адреса.
- **Destination IP/ Destination IP Mask**
  Функция: настройка IP-адреса назначения. В маске IP-адреса назначения 1 указывает на заботливый бит IP-адреса назначения, а 0 указывает на игнорируемый бит IP-адреса назначения.
- **Source Port**
  Диапазон: 0~65535
  Функция: Настройка номера исходного порта.
- **Destination Port**
  Диапазон: 0~65535
  Функция: Настройка номера порта назначения.
- **VLAN ID**
  Диапазон: 1~4093
  Функция: Настройка идентификатора VLAN.
- **Action**
  Опции: Permit / Deny / Mirror to CPU / Mirror to Port / Redirect to CPU / Redirect to Port
  По умолчанию: Permit
  Функция: настроить режим обработки пакетов для успешно сопоставленных пакетов.
  Описание: **Permit** указывает на получение успешно согласованных пакетов; **Deny** указывает на отбрасывание успешно сопоставленных пакетов; **Mirror to CPU** указывает на получение успешно сопоставленных пакетов и их зеркалирование на ЦП; **Mirror to Port** указывает на получение успешно сопоставленных пакетов и их зеркалирование на указанный порт; **Redirect to CPU** указывает на перенаправление успешно сопоставленных пакетов на ЦП; **Redirect to Port** указывает на перенаправление успешно сопоставленных пакетов на указанный порт.

Запрос записи ACL

Перейти [Device Advanced Configuration] → [ACL configuration] → [ACL Search] для запроса записи ACL, как показано на рисунке ниже.

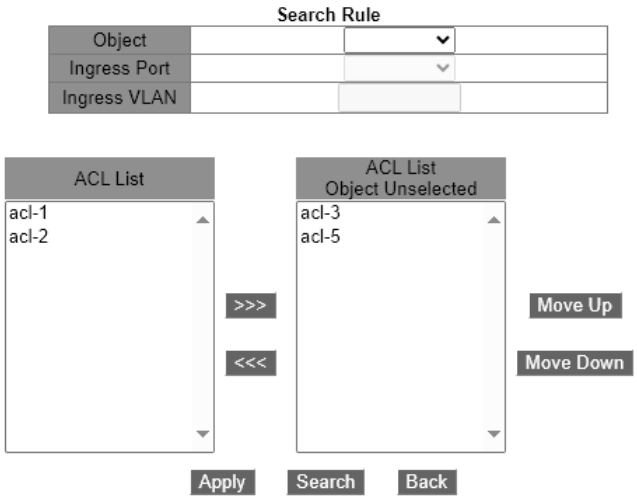


Рис. 218. Запрос записи ACL

- **Object**
  Опции: Global / Port / VLAN
  Функция: выберите область применения запрашиваемых записей ACL.
- **Ingress Port**
  Функция: выберите порт приложения для записей ACL, которые будут запрашиваться, когда для параметра «**Object**» установлено значение «**Port**».
- **Ingress VLAN**
  Функция: выберите прикладную VLAN из записей ACL, которые будут запрашиваться, когда для параметра **Object** установлено значение **VLAN**.

Список ACL в нижней правой части показывает найденные записи ACL.

Доставьте записи ACL в объект и настройте приоритет для записей ACL, как показано на рисунке.

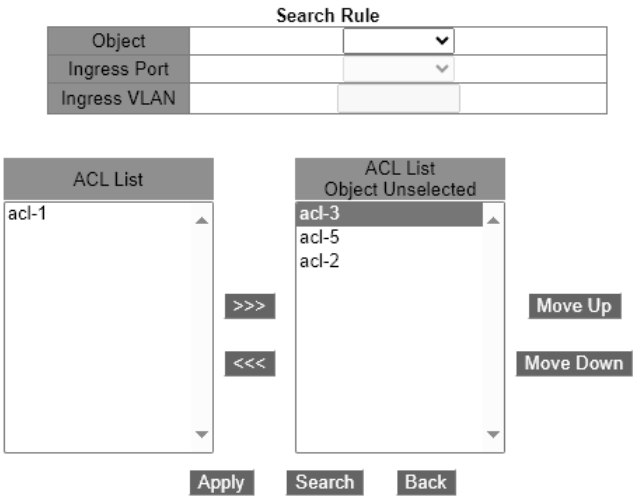


Рис. 219. Настройка приоритета записей ACL

Переместите запись ACL, которую нужно применить к объекту, в список ACL справа. Выберите запись и нажмите <Переместить вверх> или <Переместить вниз>, чтобы изменить приоритет записей ACL, применяемых к объекту. Записи ACL сверху вниз в списке расположены в порядке убывания.

6.15.4. Пример типовой конфигурации

Порт 2: Хост сегмента сети 192.168.1.0 отправляет TCP-пакеты с исходным номером порта 80 на хост сегмента сети 192.168.0.0.

Конфигурация выглядит следующим образом:

1. Настройте запись ACL 1 для применения к порту 2, как показано на рис. 214.

2. Настройте правила ACL и выберите тип TCP; исходный IP-адрес - 192.168.1.5, а маска IP-адреса источника - 255.255.255.0; целевой IP-адрес - 192.168.0.5, а маска IP-адреса назначения - 255.255.255.0; номер порта источника - 80; действие сопоставления - запретить, как показано на рис. 217.

6.16. QoS

6.16.1. Введение

Качество обслуживания (Quality of Service - QoS) позволяет предоставлять дифференцированные услуги на основе различных требований при ограниченной пропускной способности посредством управления трафиком и распределения ресурсов в IP-сетях. QoS пытается удовлетворить передачу различных услуг, чтобы уменьшить перегрузку сети и свести к минимуму влияние перегрузки на услуги с высоким приоритетом.

QoS в основном включает в себя идентификацию услуг, управление перегрузками и предотвращение перегрузок.

Идентификация службы: объекты идентифицируются на основе определенных правил соответствия. Например, объекты могут быть тегами приоритета, переносимыми пакетами, приоритетом, отображаемым портами и виртуальными локальными сетями, или

информацией о приоритете, отображаемой пятерками. Идентификация услуги является предварительным условием для QoS. Управление перегрузками: это обязательно для решения проблемы конкуренции за ресурсы. Управление перегрузками кэширует пакеты в очередях и определяет последовательность пересылки пакетов на основе определенного алгоритма планирования, обеспечивая приоритетную пересылку для ключевых служб. Предотвращение перегрузки: Чрезмерная перегрузка может привести к повреждению сетевых ресурсов. Предотвращение перегрузки отслеживает использование сетевых ресурсов. При обнаружении увеличения перегрузки функция использует упреждающее отбрасывание пакетов и настраивает объем трафика для решения проблемы перегрузки.

6.16.2. QoS CAR

Гарантированная скорость доступа QoS (Committed Access Rate - CAR) — это тип политики ограничения скорости. Эта политика цитирует правило ACL для идентификации потока, ограничивает скорость порта для соответствующего пакета и отбрасывает поток, выходящий за пределы диапазона (ширина и значение пакета), предусмотренного политикой QoS в пакете.

6.16.3. QoS Remark

QoS Remark цитирует правило ACL для идентификации потока и снова указывает приоритет (значение DSCP или COS) для соответствующего пакета.

6.16.4. Принципы

Каждый порт коммутаторов этой серии поддерживает 8 очередей кэширования, от 0 до 7 в порядке возрастания приоритета. Вы можете настроить сопоставление между приоритетом и очередями. Когда кадр достигает порта, коммутатор определяет очередь для кадра в соответствии с информацией в заголовке кадра. Коммутатор поддерживает два режима отображения очереди для определения приоритета: CoS и DSCP.

- Значение CoS зависит от приоритета тега 802.1Q в пакете. Сопоставление между значением CoS и очередью можно настроить.
- Значение DSCP зависит от части пакета TOD/DSCP. Сопоставление между значением DSCP и очередью можно настроить.

При пересылке данных порт использует режим планирования для планирования данных в 8 очередях и пропускной способности каждой очереди. Коммутаторы этой серии поддерживают два режима планирования: WRR (взвешенный циклический алгоритм) и очередь с приоритетом.

- WRR планирует потоки данных на основе коэффициента веса. Очереди получают свою пропускную способность на основе соотношения весов. WRR отдает приоритет очередям с высоким соотношением веса. Больше пропускной способности выделяется очередям с более высоким коэффициентом веса.
- Режим планирования очереди с приоритетом может строго гарантировать наивысший приоритет пересылки для пакета с наивысшим приоритетом, который в основном используется при передаче конфиденциального сигнала. Как только кадр попадает в очередь с высоким приоритетом, система останавливает

планирование данных очереди с низким приоритетом и обрабатывает данные в очереди с высоким приоритетом. Только когда очередь с высоким приоритетом пуста, она может начать обработку данных в очереди с более низким приоритетом.

6.16.5. Веб конфигурирование

Добавить / удалить policy-map

Перейти [Device Advanced Configuration] → [QoS configuration] → [Policy-map configuration] –> [Add/Remove policy-map] чтоб добавить / удалить police-map, как показано на рисунке ниже.

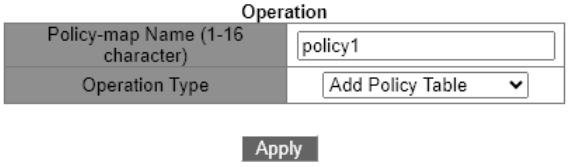


Рис. 220. Добавить / удалить policy-map

- **Policy-map name**
  Диапазон: 1~16 символов
  Функция: Настройка имени карты политик. Нажмите <Add>/<Del>, чтобы создать/удалить таблицу политик.

Настройка приоритетной перемаркировки policy-map

Перейти [Device Advanced Configuration] → [QoS configuration] → [Policy-map configuration] → [Policy-map Configuration] для входа на страницу настройки приоритета policy-map, как показано на рисунке ниже.

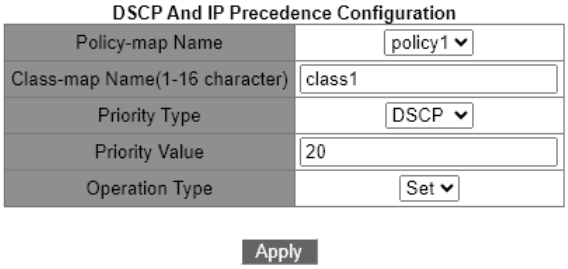


Рис. 221. Настройка приоритетной перемаркировки policy-map

- **Policy-map name**
  Опции: Все созданные карты политик.
- **Class-map name**
  Опции: Все созданные карты классов.
- **Priority type**

Опции: значение DSCP / значение COS
Функция: выберите тип приоритета, который необходимо отметить.

- **Priority value**
  Опции: 0–63 (значение DSCP) / 0–7 (значение COS)
  Функция: Настройка значения перемаркировки приоритета.
  Описание: Выполнение политики перемаркировки для значения приоритета в действии сопоставления пакетов на карте классов.
- **Operation type**
  Опции: Set/Del
  Функция: установка/удаление примечания приоритета карты политик.

Применение policy-map для порта

Перейти [Device Advanced Configuration] → [QoS configuration] → [Apply QoS To Port] –> [Apply policy-map to port] чтобы применить policy-map на порт, как показано на рисунке ниже.

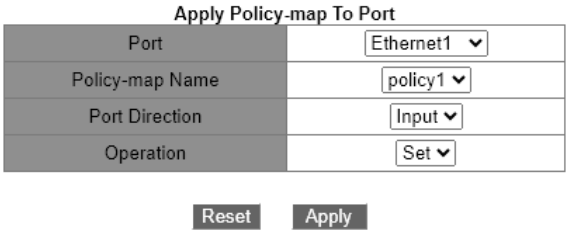


Рис. 222. Применение policy-map для порта

- **Policy-map name**
  Опции: Все созданные карты политик.
- **Port direction**
  Опции: ввод
  Функция: Примените эту таблицу политик во входном направлении порта, чтобы реализовать ограничение скорости или перемаркировку приоритета для пакета, полученного через порт.
- **Operation type**
  Опции: Set / Del
  Функция: установить/удалить карту политик приложения на порт.

Примените к порту только одну карту политик.
Конфигурация режима доверия порта и сопоставление политики приложения с портом являются взаимоисключающими.

Конфигурирование trust mode на порту

Перейти [Device Advanced Configuration] → [QoS configuration] → [Apply QoS to port] → [Port trust mode configurationion] для входа на страницу конфигурации режима доверия порта, как показано на рисунке ниже.

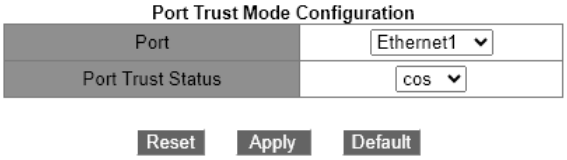


Рис. 223. Конфигурирование trust mode на порту

- **Port**
  Опции: все порты коммутатора
- **Port trust status**
  Варианты: cos /dscp / port
  По умолчанию: если полученный портом пакет является IP-пакетом, по умолчанию используется dscp; если это не IP-пакет, а тегированный пакет, по умолчанию используется значение cos. Если это не IP-пакет, а нетегированный пакет, порт не имеет режима доверия по умолчанию и сохранит пакет в очереди 0.
  Функция: настроить статус доверия портов коммутатора.
  Описание: COS относится к значению COS порта, и очередь, в которой должны храниться пакеты, полученные портом, определяется в соответствии с отношением сопоставления между значением COS и очередью. Если в пакете нет значения COS, сопоставление выполняется в соответствии со значением cos равно 0. Разница в том, что: COS относится к соотношению отображения между значением COS и значением DSCP при пересылке пакета значение DSCP в пакете изменяется на значение DSCP, отображаемое значением COS.
  DSCP ссылается на значение DSCP порта, и очередь, в которой должны храниться пакеты, полученные портом, определяется в соответствии с отношением сопоставления между значением DSCP и очередью. Если в пакете нет значения DSCP, сопоставление выполняется в соответствии со значением DSCP, равным 0. Разница заключается в том, что: DSCP ссылается на соотношение отображения между значением DSCP и значением COS при пересылке пакета значение COS в пакете изменяется на значение COS, отображаемое значением DSCP.
  Port priority
  Варианты: 0~7
  По умолчанию: 0
  Функция: назначить приоритет физическому порту. Пакеты, полученные от порта, ставятся в очередь в соответствии с назначенным приоритетом, но не в соответствии с приоритетом, переносимым пакетами. Пакеты, полученные от порта с приоритетом 0, помещаются в очередь 0, а пакеты, полученные от порта с приоритетом 1, помещаются в очередь 1. Остальное можно сделать таким же образом.

Настройте значение CoS порта по умолчанию

Перейти [Device Advanced Configuration] → [QoS configuration] → [Apply QoS to port] → [Port default CoS configuration] для входа на страницу конфигурации CoS порта по умолчанию, как показано на рисунке ниже.

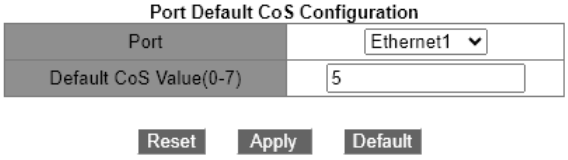


Рис. 224. Настройте значение CoS порта по умолчанию

- **Port**
  Опции: все порты коммутатора
  Значение CoS по умолчанию
  Варианты: 0~7
  По умолчанию: 0
  Функция: Настройка значения CoS по умолчанию для порта.
  Объяснение: Когда пакет не помечен, приоритет в теге, добавленном к пакету, равен значению CoS по умолчанию для порта.

Настройка веса WRR очереди порта

Перейти [Device Advanced Configuration] → [QoS configuration] → [Egress-queue configuration] –> [Port Egress-queue wrr weight configuration] для входа на страницу конфигурации веса WRR, как показано на рисунке ниже.

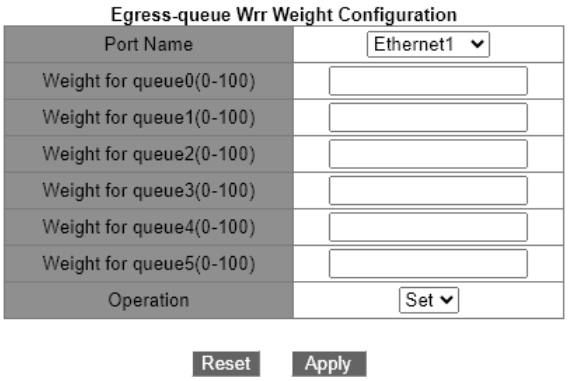


Рис. 225. Настройка веса WRR очереди порта

- **Port Name**
  Опции: все порты коммутатора

- **Weight for queue**
  Варианты: 0~100
  По умолчанию: 0
  Объяснение: Коммутатор поддерживает не более 6 групп значений веса.
  Функция: Настройка значений веса. Абсолютное значение веса не имеет смысла. WRR распределяет полосу пропускания в соответствии с соотношениями весовых значений.

Настройки сопоставления между значением DSCP и очередью

Перейти [Device Advanced Configuration] → [QoS configuration] → [QoS Mapping Configuration] → [DSCP-to-Queue Mapping] для входа на страницу конфигурации DSCP и сопоставления очередей, как показано на рисунке ниже.

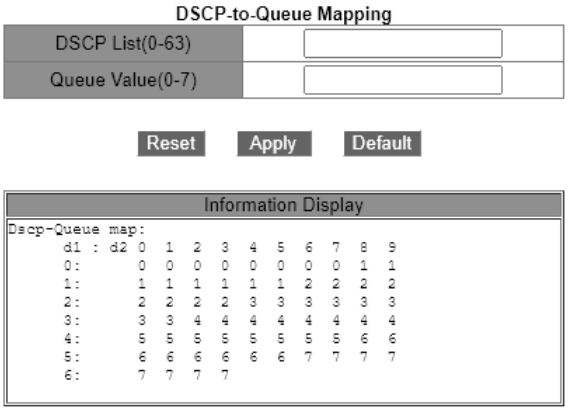


Рис. 226. Настройки сопоставления между значением DSCP и очередью

- **{DSCP, Queue value}**
  Опции: {0~63, 0~7}
  По умолчанию:
  Значение DSCP 0–7 отображается в очередь 0; Значение DSCP 8~15 сопоставляется с очередью 1;
  Значение DSCP 16~23 сопоставлено с очередью 2; Значение DSCP 24~31 сопоставляется с очередью 3; Значение DSCP 32~39 сопоставлено с очередью 4; Значение DSCP 40~47 сопоставлено с очередью 5; Значение DSCP 48~55 сопоставлено с очередью 6; Значение DSCP 56~63 сопоставляется с очередью 7.
  Функция: Настройка сопоставления между значением DSCP и очередью.
  Объяснение: Каждое значение DSCP можно сопоставить только с одной очередью. Несколько значений DSCP могут быть сопоставлены с одной очередью.

Настройка сопоставление между значением CoS и значением DSCP

Перейти [Device Advanced Configuration] → [QoS configuration] → [QoS mapping configuration] –> [CoS-to-DSCP mapping] для входа на страницу конфигурации сопоставления CoS и DSCP, как показано на рисунке ниже.

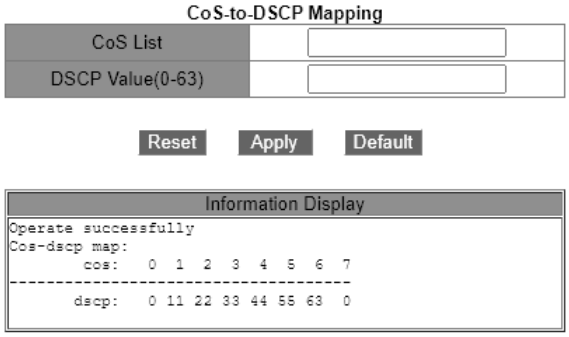


Рис. 227. Настройка сопоставление между значением CoS и значением DSCP

- **DSCP value**
  Варианты: 0~63
  По умолчанию:
  Значение CoS 0 отображается на значение 0 DSCP; Значение CoS 1 отображается на значение 8 DSCP; Значение CoS 2 отображается на значение 16 DSCP; Значение CoS 3 отображается на значение DSCP 24; Значение CoS 4 отображается на значение DSCP 32; Значение CoS 5 отображается на значение DSCP 40; Значение CoS 6 отображается на значение 48 DSCP; Значение CoS 7 сопоставляется со значением DSCP 56.
  Функция: настроить отображение между CoS и DSCP. Когда режим доверия порта — CoS, значение DSCP пакета может быть изменено в соответствии с этим отображением.
  Объяснение: Одному значению DSCP можно сопоставить несколько значений CoS.

Настройка сопоставление между значением DSCP и значением DSCP

Перейти [Device Advanced Configuration] → [QoS configuration] → [QoS mapping configuration] → [DSCP Mutation Mapping] для входа на страницу конфигурации сопоставления DSCP и DSCP, как показано на рисунке ниже.

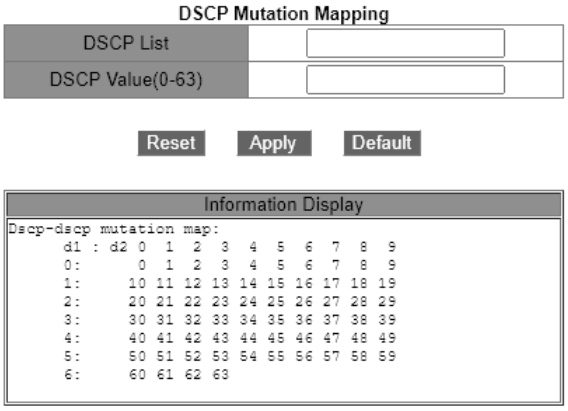


Рис. 228. Настройка сопоставление между значением DSCP и значением DSCP

- **DSCP List**
  Функция: Установить имя для мутации DSCP.
- **DSCP Value{ In , Out }**
  Опции: {0~63, 0~63}
  Функция: настроить сопоставление между DSCP и DSCP. Чтобы изменить значение DSCP пакета, используйте это сопоставление, когда выход пересылает пакет.
  Объяснение: Коммутаторы этой серии поддерживают до 28 сопоставлений мутаций DSCP.

Очередь для сохранения пакетов определяется исходным сопоставлением между значением DSCP и очередью.

Применение сопоставления mutation DSCP на порту

Перейти [Device Advanced Configuration] → [QoS configuration] → [Apply QoS to port] → [Apply DSCP mutation mapping] для входа на страницу конфигурации, как показано на рисунке ниже.

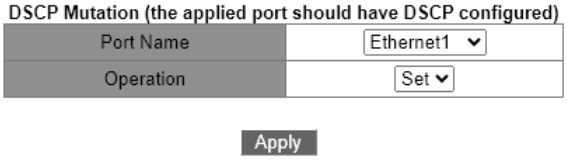


Рис. 229. Применение сопоставления mutation DSCP на порту

- **Port name**
  Опции: все порты коммутатора
  Функция: выберите порт для использования картирования мутаций DSCP.
- **DSCP mutation name**
  Параметры: Имя DSCP для сопоставления DSCP.
  Функция: Настройка отображения mutation DSCP, используемого портом.
- **Operation**
  Опции: Set/Del
  Функция: добавление/удаление сопоставления мутаций DSCP, используемого портом.

6.17. IGMP Snooping

6.17.1. Введение

Отслеживание протокола группового управления Интернетом (Internet Group Management Protocol Snooping – IGMP Snooping) — это протокол многоадресной рассылки на канальном уровне. Он используется для управления и контроля групп многоадресной рассылки. Коммутаторы с поддержкой IGMP Snooping анализируют полученные пакеты IGMP, устанавливают сопоставление между портами и MAC-адресами многоадресной рассылки и пересылают многоадресные пакеты в соответствии с сопоставлением.

6.17.2. Основные понятия

Querier: периодически отправляет пакеты общего запроса IGMP для запроса статуса членов в группе многоадресной рассылки, сохраняя информацию о группе многоадресной рассылки. Когда в сети существует несколько запрашивающих, они автоматически выбирают тот, у которого наименьший IP-адрес, в качестве запрашивающего. Только выбранный запросчик периодически отправляет пакеты общего запроса IGMP. Другие запрашивающие только получают и пересылают пакеты запросов IGMP.

Router port: получает пакеты общего запроса (на коммутаторе с поддержкой IGMP) от запрашивающего. После получения отчета IGMP коммутатор устанавливает многоадресную запись и добавляет порт, который получает отчет IGMP, в список портов-членов. Если порт маршрутизатора существует, он также добавляется в список портов-членов. Затем коммутатор пересылает отчет IGMP другим устройствам через порт маршрутизатора, чтобы другие устройства установили ту же запись многоадресной рассылки.

6.17.3. Принцип

IGMP Snooping управляет и поддерживает членов группы многоадресной рассылки путем обмена связанными пакетами между устройствами с поддержкой IGMP. Связанные пакеты следующие: Пакет общего запроса: запрашивающий периодически отправляет пакеты общего запроса (IP-адрес назначения: 224.0.0.1), чтобы подтвердить, есть ли в группе многоадресной рассылки порты-члены. После получения пакета запроса устройство, не являющееся запросчиком, пересылает пакет на все подключенные к нему порты.

Specific query packet: если устройство хочет выйти из группы многоадресной рассылки, оно отправляет пакет выхода IGMP. После получения пакета leave запрашивающий отправляет определенный пакет запроса (IP-адрес назначения: IP-адрес группы многоадресной рассылки), чтобы подтвердить, содержит ли группа другие порты-члены.

Membership report packet: если устройство хочет получить данные группы многоадресной рассылки, оно немедленно отправляет пакет отчета IGMP (IP-адрес назначения: IP-адрес группы многоадресной рассылки), чтобы ответить на пакет запроса IGMP группы. Пакет выхода: если устройство хочет покинуть группу многоадресной рассылки, оно отправит пакет выхода IGMP (IP-адрес назначения: 224.0.0.2).

6.17.4. Веб конфигурация

Включение IGMP Snooping

Перейти [Device Advanced Configuration] → [Multicast protocol configuration] → [IGMP Snooping configuration] → [Enable IGMP Snooping] для входа на страницу глобальной конфигурации IGMP Snooping, как показано на рисунке ниже.

Рис. 230. Включение IGMP Snooping

- **IGMP Snooping**
  Опции: Open / Close
  По умолчанию: Close
  Функция: Включить или отключить глобальный протокол IGMP Snooping. IGMP Snooping и GMRP нельзя включить одновременно.

Конфигурирование IGMP Snooping параметров

Перейти [Device Advanced Configuration] → [Multicast protocol configuration] → [IGMP Snooping configuration] → [IGMP Snooping configuration] для входа на страницу конфигурации IGMP Snooping, как показано на рисунке ниже.

Рис. 231. Конфигурирование IGMP Snooping параметров

- **VLAN ID**
  Опции: все созданные идентификаторы VLAN.
- **Snooping state**
  Опции: Open / Close
  По умолчанию: Close
  Функция: включение или выключение функции отслеживания IGMP VLAN. Предпосылкой этого
  Функция состоит в том, чтобы включить глобальную функцию IGMP Snooping.
- **Static IP**
  Формат: A.B.C.D.
  По умолчанию: 192.168.0.2
  Функция: настроить исходный IP-адрес отправки пакетов.

Настройте параметры запроса IGMP, как показано на рисунке ниже.

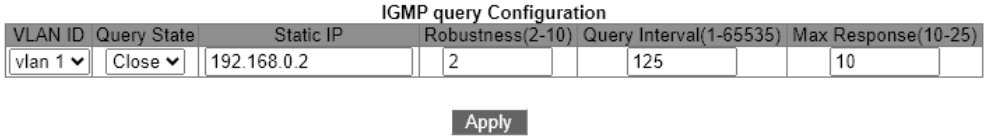


Рис. 232. Параметры запроса IGMP

- **VLAN ID**
  Опции: Все созданные идентификаторы VLAN.
  Функция: выберите идентификатор VLAN, чтобы включить функцию запроса IGMP.
- **Query State**
  Опции: Open / Close
  По умолчанию: Close
  Функция: включение или отключение функции запроса IGMP для выбранной VLAN. предварительным условием этой функции является включение глобальной функции IGMP Snooping.
  Описание: Если в сети есть несколько запрашивающих, они автоматически выберут тот, у которого наименьший IP-адрес, в качестве запрашивающего. Если есть только одно устройство, которое позволяет функцию запроса IGMP, это будет querier.

Функции Query и Snooping являются взаимоисключающими в VLAN. Это означает, что если запрос открыт, snooping должен быть закрыт в одном VLAN; если отслеживание открыто, запрос должен быть закрыт.

- **Static IP**
  Формат: A.B.C.D.
  По умолчанию: 192.168.0.2
  Функция: настроить исходный IP-адрес отправки пакета запроса.
- **Robustness**
  Диапазон: 2~10
  По умолчанию: 2
  Функция: укажите параметр надежности функции запроса IGMP.
  Описание: Чем больше параметр, тем хуже сетевое окружение. Пользователь может установить
  подходящий параметр надежности в соответствии с реальной сетью.
- **Query Interval**
  Диапазон: 1~65535 с
  По умолчанию: 125 с
  Функция: Настройка интервала отправки пакета запроса.
- **Max Response**
  Диапазон: 10 ~ 25 с
  По умолчанию: 10 с
  Функция: настроить максимальное время ответа на запрос пакета.
  Опции: Все созданные идентификаторы VLAN.

После завершения настройки в разделе «Конфигурация IGMP» отображается информация о конфигурации IGMP, показано на рисунке ниже.

IGMP Configuration

VLAN ID	Snooping State	Query State	Static IP	Robustness	Query Interval	Max Response
1	Close	Open	192.168.0.2	2	125	10
2	Open	Close	192.168.0.2	0	0	0

Рис. 233. Информация о конфигурации IGMP

Настройка статическискиx параметров многоадресной рассылки IGMP Snooping

Перейти [Device Advanced Configuration] → [Multicast protocol configuration] → [IGMP Snooping configuration] → [IGMP Snooping static multicast configuration] для входа на страницу статической конфигурации IGMP Snooping, как показано на рисунке ниже.

IGMP Snooping Static Multicast Configuration

VLAN ID	1
Operation Type	Add
Multicast Group Member Port	Ethernet1
Multicast Address	224.0.1.0

Apply

Рис. 234. Настройка статическискиx параметров IGMP Snooping

- **VLAN ID**
  Опции: все созданные идентификаторы VLAN.
- **Operation type**
  Опции: Add / Del
  По умолчанию: Add
  Функция: Добавить / удалить порт участника группы многоадресной рассылки.
- **Multicast group member port**
  Опции: все порты коммутатора
  Функция: выберите порт-член, который необходимо добавить или удалить из группы многоадресной рассылки. Если
  порт подключен к хосту и хост получает данные определенной мультикаст-группы, этот порт
  может быть настроен для присоединения к статической группе многоадресной рассылки и становится статическим портом-участником.
- **Multicast address**
  Диапазон: 224.0.1.0~239.255.255.255
  Функция: Введите адрес группы многоадресной рассылки.
  Описание: при динамическом изучении вновь добавленного статического адреса многоадресной рассылки этот статический адрес многоадресной рассылки будет охватывать динамический адрес многоадресной рассылки.

Просмотр многоадресных записей

Перейти [Device Advanced Configuration] → [Multicast protocol configuration] → [IGMP Snooping configuration] → [Show IGMP Snooping information] для отображения многоадресных записей, как показано на рисунке ниже.

Рис. 235. Просмотр многоадресных записей

6.17.5. Типовые примеры применения

Как показано на рис. 236, Switch1, Switch2 и Switch3 включены с функцией отслеживания IGMP, а Switch2 и Switch3 включены с автоматическим запросом. IP-адрес Switch2: 192.168.1.2 IP-адрес Switch3: 192.168.0.2. Поэтому в качестве запрашивающего был выбран Switch3.

- Включите функцию IGMP Snooping для Switch 1;
- Включите функции IGMP Snooping и автоматических запросов Switch2;
- Включите функции IGMP Snooping и автоматических запросов Switch3;

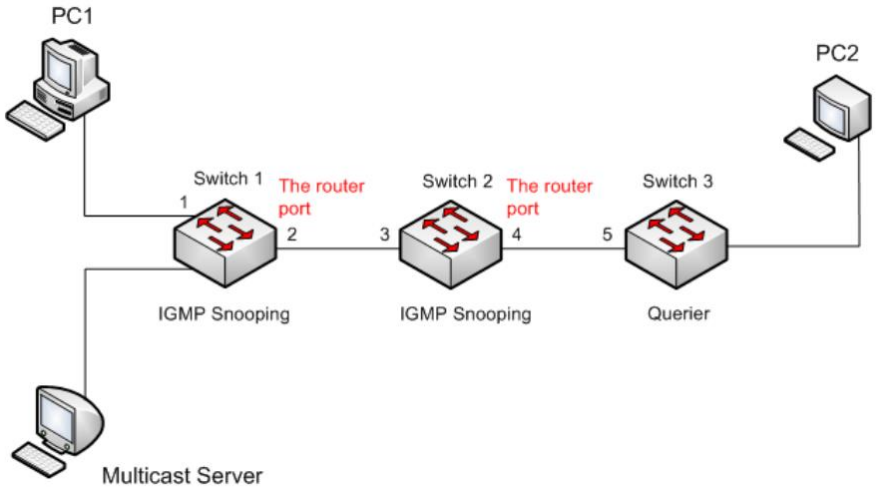


Рис. 236. Пример применения

- Поскольку Switch 3 выбран в качестве запрашивающего, он периодически отправляет общие пакеты запросов, а порт 4 Switch 2 получает пакеты запросов, поэтому он выбирается в качестве порта маршрутизации, а Switch 2 также будет пересылать пакеты запросов с порта 3, а Switch 1 Порт 2 выбирается в качестве порта маршрутизации после его получения.
- Когда ПК1 присоединяется к группе многоадресной рассылки 225.1.1.1, он отправляет отчетное сообщение igmp этой группы. В это время как порт 1, так и порт маршрутизации 2 Switch 1 присоединятся к группе многоадресной рассылки 225.1.1.1. Сообщение отчета igmp проходит через маршрутизатор Порт 2 перенаправляется на Switch 2, а порты 3 и 4 коммутатора 2 также добавляются к 225.1.1.1 В то же время сообщение отчета igmp пересылается на Switch 3 через порт маршрутизации 4 и порт 5. Switch3 также добавлен в 225.1.1.1.

- Когда мультикаст-данные с мультикаст-сервера поступят на Switch1, они будут перенаправлены на pc1 через порт 1. В то же время, поскольку маршрутизирующий порт 2 также является членом мультикаст-группы, мультикаст-данные также будут перенаправлены через порт 1, порт маршрутизации и т. д. Порт 5 коммутатора 3 прекращает пересылку, потому что нет приемника, но, если pc2 также присоединится к 225.1.1.1, то данные многоадресной рассылки также будут перенаправлены на pc2.

6.18. GMRP

6.18.1. Введение в GARP

Общий протокол регистрации атрибутов (Generic Attribute Registration Protocol - GARP) используется для распространения, регистрации и отмена определенной информации (VLAN, многоадресный адрес) среди коммутаторов на одном и том же сеть.

При использовании GARP информация о конфигурации члена GARP будет распространяться на всю коммутационную сеть. Член GARP инструктирует других членов GARP зарегистрироваться или отменить свою собственную информацию о конфигурации с помощью сообщения о присоединении/отключении соответственно. Участник также регистрирует или отменяет информацию о конфигурации других участников на основе в сообщениях о присоединении / выходе, отправленных другими участниками.

GARP включает три типа сообщений: Join, Leave и LeaveAll.

- Когда объект приложения GARP хочет зарегистрировать свою собственную информацию на других коммутаторах, объект отправляет сообщение о присоединении. Сообщения о присоединении делятся на два типа: JoinEmpty и JoinIn. Сообщение JoinIn отправляется для объявления зарегистрированного атрибута, а сообщение JoinEmpty отправляется для объявления атрибута, который еще не зарегистрирован.
- Когда объект приложения GARP хочет аннулировать свою собственную информацию о других коммутаторах, объект отправляет сообщение о выходе. Сообщения о выходе делятся на два типа: LeaveEmpty и LeaveIn. Сообщение LeaveIn отправляется для отмены зарегистрированного атрибута, а сообщение LeaveEmpty отправляется сообщение для отмены еще не зарегистрированного атрибута.
- После запуска объекта GARP он запускает таймер LeaveAll. Когда таймер истекает, объект отправляет сообщение LeaveAll.

Сущность приложения указывает на порт с поддержкой GARP.

Таймеры GARP включают Hold timer, Join timer, Leave timer и LeaveAll timer.

Hold timer: при получении регистрационного сообщения объект GARP не отправляет сообщение о присоединении. сообщение немедленно, но запускает таймер удержания. Когда таймер истекает, объект отправляет все сообщений о регистрации, полученных в течение предшествующего периода, в одном сообщении о присоединении, отправка пакетов для лучшей стабильности сети.

Join time: чтобы убедиться, что сообщения о присоединении принимаются другими объектами приложения, Сущность приложения GARP запускает таймер присоединения после отправки сообщения присоединения. Если не получено JoinIn сообщения до истечения времени таймера присоединения объект снова отправляет сообщение о присоединении. Если вы получаете Сообщение JoinIn до истечения времени таймера объект не отправляет второе сообщение Join.
Leave timer: когда объект приложения GARP хочет отменить информацию о атрибут, объект отправляет сообщение о выходе. Сущность, получившая сообщение, начинает оставить таймер. Если сообщение о присоединении не получено до истечения таймера, объект, получивший сообщение, отменяет информацию об атрибуте.
LeaveAll timer: Когда объект приложения GARP запускается, он запускает таймер LeaveAll. Когда таймер истекает, объект отправляет сообщение LeaveAll, чтобы другие объекты приложения GARP перерегистрировать все атрибуты. Затем объект снова запускает таймер LeaveAll для нового цикла.

6.18.2. GMRP протокол

Протокол регистрации многоадресной рассылки GARP (GARP Multicast Registration Protocol - GMRP) — это протокол регистрации многоадресной рассылки, основанный на на ГАРП. Он используется для поддержки регистрационной информации многоадресной рассылки коммутаторов. Все Коммутаторы с поддержкой GMRP могут получать информацию о регистрации многоадресной рассылки от других коммутаторов. динамически обновлять информацию о регистрации локальной многоадресной рассылки и распространять локальную многоадресную рассылку регистрационную информацию другим коммутаторам. Этот механизм обмена информацией обеспечивает непротиворечивость многоадресной информации, поддерживаемой всеми коммутаторами с поддержкой GMRP на сеть.

Если коммутатор или терминал хочет присоединиться к группе многоадресной рассылки или выйти из нее, порт с поддержкой GMRP передает информацию на все порты в той же VLAN.

6.18.3. Описание

Agent port: указывает порт, на котором включены GMRP и функция агента.
Propagation port: указывает порт, на котором включен только GMRP, но не прокси. функция.
Динамически изученная многоадресная запись GMRP и запись агента пересылаются порт распространения к портам распространения устройств более низкого уровня.
Все таймеры GMRP в одной сети должны поддерживать согласованность во избежание взаимных помех. Таймеры должны соответствовать следующим правилам: Hold timer < Join timer, 2*Join timer < Leave timer, and Leave timer < LeaveAll timer.

6.18.4. Веб конфигурирование

Глобальное включение GMRP протокола

Перейти [Device Advanced Configuration] → [Multicast protocol configuration] → [GMRP configuration] → [Enable Global GMRP] для входа на страницу конфигурации GMRP, как показано на рисунке ниже.

Рис. 237. Глобальное включение GMRP протокола

- **GMRP function**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включение / выключение глобальной функции GMRP. Функцию нельзя использовать вместе с функцией IGMP Snooping.

Добавить запись прокси GMRP

Перейдите в дерево навигации меню [Device Advanced Configuration] → [Multicast protocol configuration] → [GMRP configuration]→[GMRP Global Agent Configuration], чтобы войти в интерфейс настройки записи прокси-сервера GMRP, как показано на рис. 238;

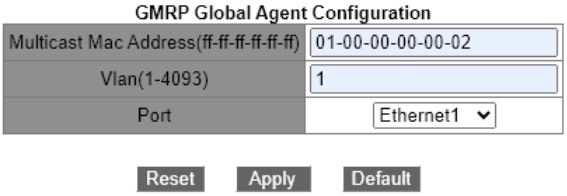


Рис. 238. Добавить запись прокси GMRP

- **Port**
  Параметры конфигурации: настроенные порты прокси
- **MAC-адрес**
  Формат конфигурации: HH-HH-HH-HH-HH-HH (H — шестнадцатеричное число)
  Функция: настроить MAC-адрес группы многоадресной рассылки, младший бит старшего байта равен 1.
- **VLAN (1-4093)**
  Параметры конфигурации: созданные номера VLAN
  Функция: Настройка идентификатора VLAN для записи прокси-сервера GMRP.
  Описание: Запись прокси-сервера GMRP перенаправляется только из порта мультикаст рассылки с тем же идентификатором VLAN, что и запись.

Настройте GMRP, как показано на рисунке;

[Device Advanced Configuration] → [Multicast protocol configuration] → [GMRP configuration] → [GMRP Port Configuration]

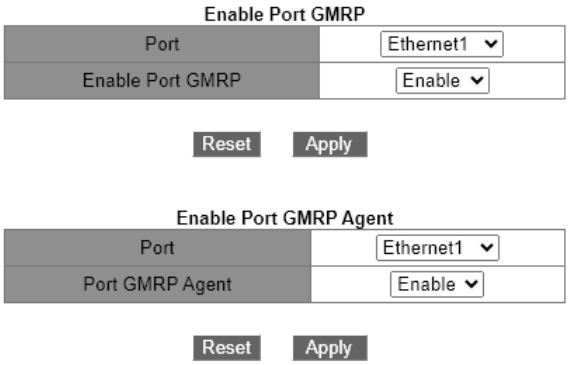


Рис. 239. Настройте GMRP порт

- **Port**
  Варианты конфигурации: все порты на коммутаторе
  Включить / отключить порт GMRP
  Параметры конфигурации: включить / отключить
  Конфигурация по умолчанию: старт
  Функция: следует ли включить функцию GMRP порта.
  Стартовый порт GMRP-прокси
  порт
  Варианты конфигурации: все порты на коммутаторе
  Параметры конфигурации: включить/отключить
  Конфигурация по умолчанию: старт
  Функция: следует ли включить функцию прокси-сервера GMRP для порта.

Настройка функции GMPR на порту, как показано на рисунке.

[Device Advanced Configuration] → [Multicast protocol configuration] → [GMRP configuration] → [GMRP Timer Configuration]

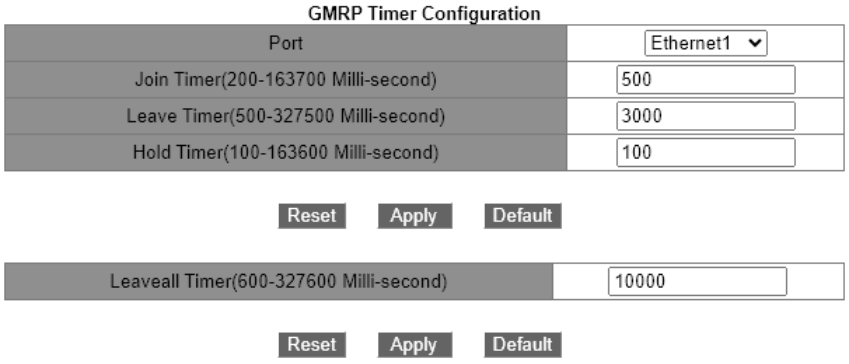


Рис. 240. Настройка функции GMPR на порту

- **Port name**
  Опции: все порты коммутатора

- **GMRP Function**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включить функцию GMRP на порту или отключить
- **GMRP Agent Function**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: Включить функцию агента GMRP на порту или нет.
- **Hold Timer**
  Диапазон: 100-163600 мс
  По умолчанию: 100 мс
  Описание: Это значение должно быть кратно 100. Лучше установить одинаковое время таймеров Hold на всех портах с поддержкой GMRP.
- **Join Timer**
  Диапазон: 200-163700 мс
  По умолчанию: 500 мс
  Это значение должно быть кратно 100. Лучше установить одинаковое время таймеров присоединения на всех портах с поддержкой GMRP.
- **Leave Timer**
  Диапазон: 500 мс~327500 мс
  По умолчанию: 3000 мс
  Это значение должно быть кратно 100. Лучше установить одинаковое время таймеров выхода на всех портах с поддержкой GMRP.

Просмотр GMRP конфигурации

Перейти [Device Advanced Configuration] → [Multicast protocol configuration] → [GMRP configuration] → [Show GMRP configuration] для отображения информации о конфигурации GMRP, как показано на рисунке ниже.

Information Display

```
---------------- Gmrp Information ------------------
Gmrp status : enable
Gmrp Timers(milliseconds)
LeaveAll    :  10000  [default : 10000]


Interface Ethernet4 status    : Gmrp Enable
                              : Gmrp Agent Enable
     Gmrp Timers(milliseconds)
        Hold  :   100  [default :   100]
        Join  :   500  [default :   200]
        Leave :  3000  [default :   600]

     Gmrp last PDU Origin:
        00-00-00-00-00-00

Interface Ethernet1 status    : Gmrp Enable
                              : Gmrp Agent Enable
     Gmrp Timers(milliseconds)
        Hold  :   100  [default :   100]
        Join  :   500  [default :   200]
        Leave :  3000  [default :   600]

     Gmrp last PDU Origin:
        00-00-00-00-00-00
```

Рис. 241. Просмотр GMRP конфигурации

6.18.5. Пример типовой конфигурации

Как показано на рисунке ниже, коммутаторы A и B подключены через порт 2, а порт 1 в коммутаторе A настроен как прокси-порт, и он действует как прокси для двух многоадресных записей: MAC-адрес: 01-00-00-00-00-01 VLAN: 1 MAC-адрес: 01-00-00-00-00-02 VLAN: 2 Наблюдайте за динамической регистрацией и обновлением информации о многоадресной рассылке между коммутаторами, настраивая различные атрибуты портов VLAN.

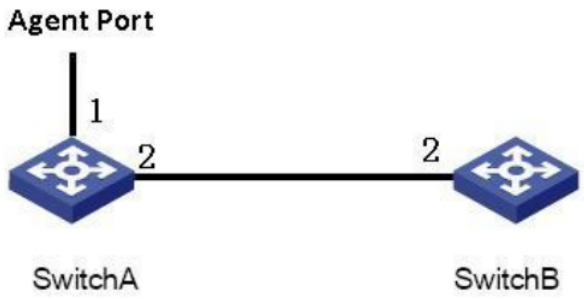


Рис. 242. Пример конфигурации

Процесс настройки коммутатора A:

1. Включите глобальную функцию GMRP коммутатора A, см. рис. 237;
2. Включите функцию GMRP и функцию прокси порта 1, включите функцию GMRP порта 2, и значения таймера примут значения по умолчанию, как показано на рис. 239, 240;
3. Настройте запись многоадресной рассылки прокси-сервера, <MAC-адрес, идентификатор VLAN, членский порт>, настроенный как <01-00-00-00-00-01, 1, 1> и <01-00-00-00-00-02, 2, 1>, см. рис. 238;

Процесс настройки коммутатора B:

4. Включите глобальную функцию GMRP коммутатора B, см. рис. 237;
5. Включите функцию GMRP порта 2, и значение таймера примет значение по умолчанию, как показано на рис. 239, 240.

6.19. Конфигурация static multicast

Таблица многоадресных адресов может быть настроена статически. В таблицу многоадресных адресов добавляется запись в виде {VLAN ID, MAC-адрес многоадресной рассылки, порт-участник многоадресной рассылки}, и сообщение многоадресной рассылки будет перенаправлено на соответствующий порт-участник в соответствии с записью.

6.19.1. Веб конфигурирование

Добавление static multicast записи

Перейти [Device Advanced Configuration] → [Multicast protocol configuration] → [Static Multicast Configuration], для входа на страницу конфигурации статической многоадресной рассылки, как показано на рисунке ниже.

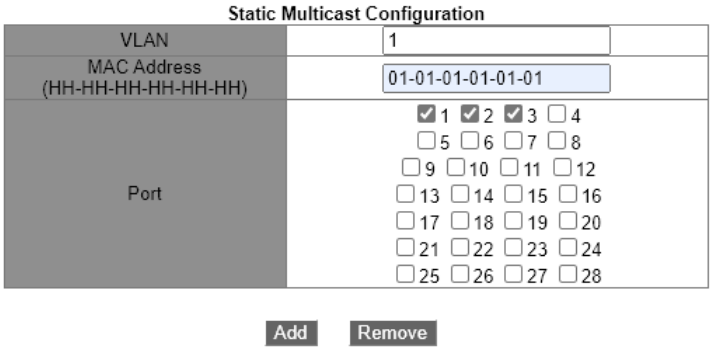


Рис. 243. Добавление static multicast записи

- **VLAN**
  Опции: Все существующие идентификаторы VLAN.
  Функция: установить идентификатор VLAN для статической многоадресной записи. Только порты-члены VLAN могут пересылать это многоадресное сообщение.
- **MAC Address**
  Формат: HH-HH-HH-HH-HH-HH (H — шестнадцатеричное число)
  Функция: настройка группового адреса многоадресной рассылки. Младший бит старшего байта равен 1.
- **Port**
  Функция: выберите порты-члены многоадресного адреса. Если хост, подключенный к порту, хочет получать определенные данные группы многоадресной рассылки, статически добавьте этот порт в группу многоадресной рассылки и станьте статическим портом-участником.
  Нажмите кнопку <Add>, чтобы добавить статическую многоадресную запись; нажмите кнопку <Delete>, чтобы удалить статическую запись многоадресной рассылки.

6.20. Конфигурация ограничения скорости многоадресной рассылки

6.20.1. Введение в ограничение скорости многоадресной рассылки

Чтобы повысить надежность передачи сетевых сообщений GOOSE и SV и разрешить ситуацию, когда сбой одного сообщения GOOSE или SV приводит к ненормальному состоянию всей сети, управление потоком выполняется для каждого канала сообщений GOOSE и SV, чтобы гарантировать что бурные сообщения GOOSE/SV занимают лишь небольшую часть полосы пропускания сети, чтобы гарантировать, что другие полосы пропускания сети могут по-прежнему нормально передавать сообщения GOOSE/SV. Инструкции по настройке топологии и управления потоком см. на рис. 244.

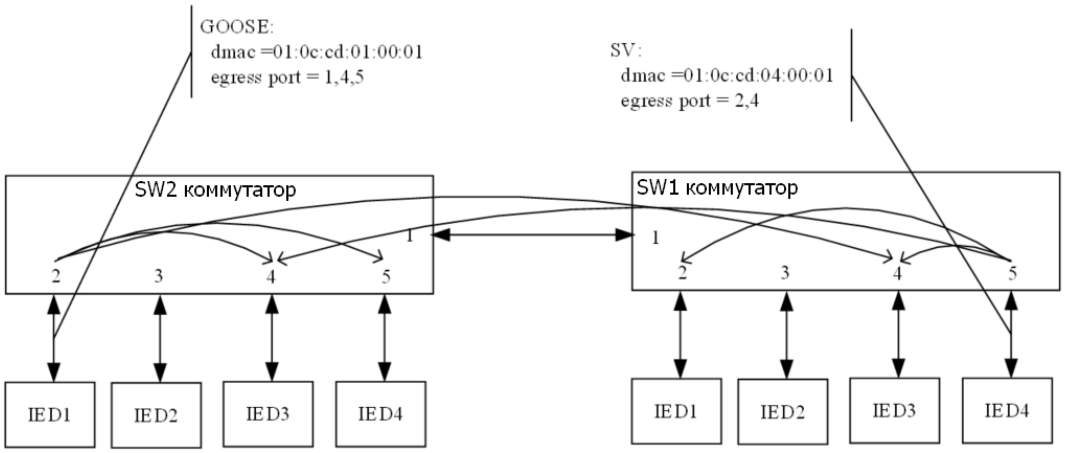


Рис. 244. Пример топологии

Коммутаторы SW1 и SW2 соответственно настроены на значения управления потоком согласно таблице 9, 10.

Таблица 9. Упрваление потоком SW1

Блок управления потоком	Порог регулирования (Mbit/s)
Управление потоком GOOSE	2
Управление потоком SV	15

Таблица 10. Управление потоком SW2

Блок управления потоком	Порог регулирования (Mbit/s)
Управление потоком GOOSE	2
Управление потоком SV	15

После настройки управления потоком, см. табл. 11, 12 для настройки выходного потока GOOSE/SV для каждого порта коммутаторов SW1 и SW2.

Таблица 11. Настройка выходного потока SW1

Блок управления потоком	Выходной порт	Скорость потока (Mbit/s)
01:0C:CD:01:00:01	4	2
01:0C:CD:04:00:01	1	15
01:0C:CD:04:00:01	2	15
01:0C:CD:04:00:01	4	15

Таблица 12. Настройка выходного потока SW2

Блок управления потоком	Выходной порт	Скорость потока (Mbit/s)
01:0C:CD:01:00:01	1	2
01:0C:CD:01:00:01	4	2
01:0C:CD:01:00:01	5	2
01:0C:CD:04:00:01	4	15

6.20.2. Конфигурация веб-страницы

Конфигурация правила ограничения скорости GOOSE-SV, поддерживает настройку ограничения скорости для определенных пакетов GOOSE-SV, точное ограничение скорости для определенных пакетов GOOSE-SV в соответствии с конфигурацией правил пользователя, обеспечивая высокую гибкость и большую свободу.

Перейдите в дерево навигации [Device Advanced Configuration] → [Multicast Limit Configuration] → [Limit Rule Configuration], чтобы войти в интерфейс настройки правила ограничения скорости, как показано на рис. 245;

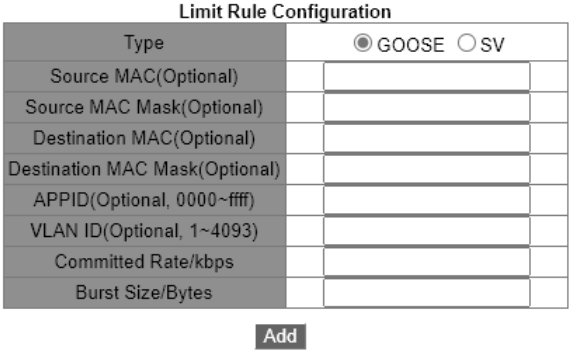


Рис. 245. Конфигурация правила ограничения скорости GOOSE-SV

- **GOOSE/SV: тип сообщения**
  MAC-адрес источника, MAC-адрес назначения, APPID необязательно
- **VLAN ID**
  Диапазон конфигурации: 1-4093

  Фиксированная скорость/кбит/с
  Диапазон конфигурации: 0-100000 Кбит/с

  Функция: CIR (согласованная скорость передачи данных), скорость, которая может передаваться в секунду, единица измерения — кбит/с, используется для ограничения скорости определенных пакетов GOOSE.
  пиковые байты/байты
  Диапазон конфигурации: 11000-1000000 байт
  Конфигурация по умолчанию: нет

Функция: CBS (Committed Burst Size, согласованный размер пакета), емкость корзины маркеров, то есть максимальный размер трафика, разрешенный для каждого пакета. Установленный размер пакета должен быть больше максимальной длины пакета. Единицей измерения является байт (byte).
Добавить: отправить информацию о конфигурации.

Управление многоадресным потоком GOOSE-SV, после включения этой конфигурации он настроит глобальное ограничение скорости для пакетов GOOSE-SV в качестве примера.

Перейдите в дерево навигации меню [Device Advanced Configuration] → [Multicast Limit Configuration] → [Multicast Limit Enable], чтобы войти в интерфейс включения ограничения скорости многоадресной передачи, как показано на рис. 246;

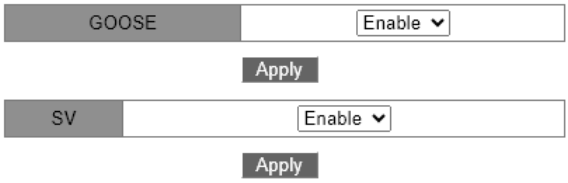


Рис. 246. Включение ограничения скорости многоадресной передачи

- **GOOSE**
  Объем настройки: вкл./выкл.
  Конфигурация по умолчанию: выключено
  Функция: после включения этой конфигурации глобальное ограничение скорости для пакетов GOOSE-SV будет ограничено 2 Мбит/с для пакетов типа GOOSE и 15 Мбит/с для пакетов типа SV.
- **SV**
  Объем настройки: вкл./выкл.
  Конфигурация по умолчанию: выключено
  Функция: после включения этой конфигурации глобальное ограничение скорости для пакетов GOOSE-SV будет ограничено 2 Мбит/с для пакетов типа GOOSE и 15 Мбит/с для пакетов типа SV.

Сообщение об ограничении скорости «GOOSE-SV»;

Перейдите в дерево навигации в меню меню [Device Advanced Configuration] → [Multicast Limit Configuration] → [Goose-sv Default Limit Configuration], чтобы войти в интерфейс включения ограничения скорости многоадресной рассылки, как показано на рис. 247;

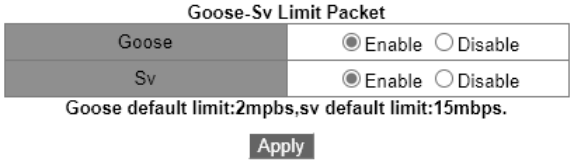


Рис. 247. Включение ограничения скорости многоадресной рассылки

- **{GOOSE, SV}**
  Параметры конфигурации: включить/отключить
  Функция: после включения этой конфигурации глобальное ограничение скорости для пакетов GOOSE-SV будет ограничено 2 Мбит/с для пакетов типа GOOSE и 15 Мбит/с для пакетов типа SV.

6.21. LLDP

6.21.1. Введение

Протокол обнаружения канального уровня (Link Layer Discovery Protocol - LLDP) предоставляет стандартный механизм обнаружения канального уровня. Он инкапсулирует информацию об устройстве, такую как возможности, адрес управления, идентификатор устройства и идентификатор интерфейса, в блок данных протокола обнаружения канального уровня (LLDPDU) и объявляет LLDPDU своим непосредственно подключенным соседям. Получив LLDPDU, соседи сохраняют эту информацию в MIB для запроса и проверки состояния канала NMS.

6.21.2. Веб конфигуирование

Включение LLDP

Перейти [Device Advanced Configuration] → [LLDP configuration] → [LLDP configuration] для входа на страницу конфигурации LLDP, как показано на рисунке ниже.

Рис. 248. Включение LLDP

- **LLDP configuration**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: Включение LLDP

Включить функцию адреса управления TLV можно, как показано на рисунке ниже.

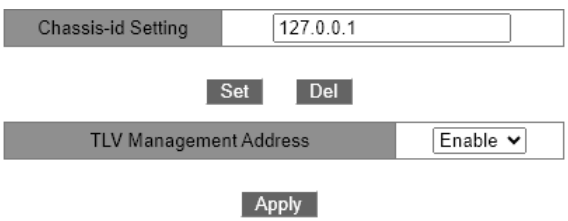


Рис. 249. Включение функции TLV

- **TLV Management Address**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: отправка IP-адреса интерфейса (то есть основного IP-адреса первого интерфейса VLAN, в котором находится этот порт) на подключенное устройство, когда эта функция отключена. Если IP-адрес не настроен для интерфейса VLAN, где находится этот порт, IP-адрес интерфейса — 127.0.0.1. Отправьте IP-адрес интерфейса и все IP-адреса, настроенные для текущего устройства, на подключенное устройство, когда эта функция включена. Можно отправить максимум 64 адреса управления TLV.

Когда на локальном устройстве включена функция управления адресом TLV и подключающееся соседнее устройство может анализировать функцию TLV, оно может правильно отображать все настроенные IP-адреса локального коммутатора.

Просмотр LLDP информации

Перейти [Device Advanced Configuration] → [LLDP configuration] → [Show lldp] для отображения информации LLDP, как показано на рисунках ниже.

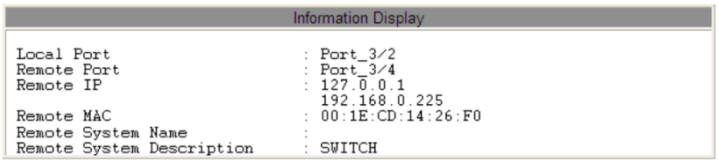


Рис. 250. Просмотр LLDP информации

На предыдущем рисунке показано условие, при котором IP-адрес не настроен для первого интерфейса VLAN, где находится порт 3/4.

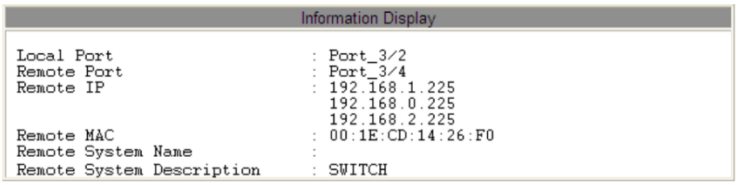


Рис. 251. Просмотр LLDP информации

На предыдущем рисунке показано условие, при котором первичный IP-адрес первого интерфейса VLAN, в котором находится порт 3/4, равен 192.168.1.225. Когда адрес управления TLV включен, отображаемая информация LLDP включает в себя подключенный локальный порт коммутатора и удаленный порт соседнего устройства, IP-адрес интерфейса, все настроенные IP-адреса, MAC-адрес и системную информацию соседнего устройства.

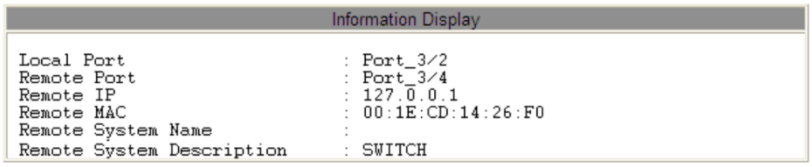


Рис. 252. Просмотр LLDP информации

На предыдущем рисунке показано условие, при котором IP-адрес не настроен для первого интерфейса VLAN, где находится порт 3/4.

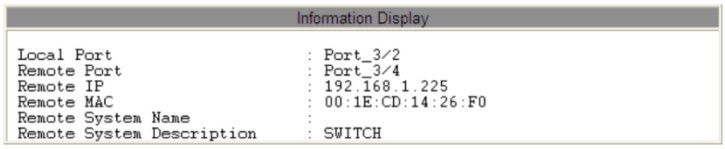


Рис. 253. Просмотр LLDP информации

На предыдущем рисунке показано условие, при котором первичный IP-адрес первого интерфейса VLAN, в котором находится порт 3/4, равен 192.168.1.225. Когда адрес управления TLV отключен, отображаемая информация LLDP включает в себя подключенный локальный порт коммутатора и удаленный порт соседнего устройства, IP-адрес интерфейса, MAC-адрес и системную информацию соседнего устройства.

Предпосылкой для отображения информации LLDP является то, что устройства с поддержкой LLDP подключены друг к другу.

6.22. RMON

6.22.1. Введение

Основанный на архитектуре SNMP, удаленный мониторинг сети (Remote Network Monitoring - RMON) позволяет устройствам управления сетью осуществлять упреждающий мониторинг и управление управляемыми устройствами. Сеть RMON обычно включает в себя станцию управления сетью и агенты. NMS управляет агентами, а агенты могут собирать статистику по различным типам трафика на этих портах. RMON в основном обеспечивает статистику и функции сигнализации. С помощью функции статистики Агенты могут периодически собирать статистику по различным типам трафика на этих портах, например, количество пакетов, полученных из определенного сегмента сети за определенный период. Функция тревоги заключается в том, что агенты могут отслеживать значения указанных переменных MIB. Когда значение достигает порога тревоги (например, количество пакетов достигает указанного значения), агент может автоматически записывать события тревоги в журнал RMON или отправлять сообщение Trap на управляющее устройство.

6.22.2. Группы RMON

RMON (RFC2819) определяет несколько групп RMON. Устройства серии поддерживают группу статистики, группу истории, группу событий и группу сигналов тревоги в общедоступной MIB. Каждая группа поддерживает до 32 записей.

- Statistics group

  С помощью группы статистики система собирает статистику по всем типам трафика на портах и сохраняет статистику в таблице статистики Ethernet для дальнейшего запроса управляющим устройством. Статистика включает в себя количество сетевых коллизий, пакетов с ошибками CRC, пакетов меньшего или большего размера, широковещательных и многоадресных пакетов, полученных байтов и полученных пакетов. После успешного создания записи статистики на указанном порту группа статистики подсчитывает количество пакетов на порту, и статистика представляет собой постоянно накапливаемое значение.
- History group

  Группа History требует, чтобы система периодически отбирала все виды трафика на портах и сохраняла значения выборки в таблице записей истории для дальнейшего запроса устройством управления. Группа истории подсчитывает статистические значения всех видов данных в интервале выборки.
- Event group

  Группа событий используется для определения индексов событий и методов обработки событий. События, определенные в группе событий, используются в элементе конфигурации группы тревог. Событие запускается, когда контролируемое устройство соответствует условию тревоги. События рассматриваются следующими способами:

  Log: регистрирует событие и связанную с ним информацию в таблице журнала событий.

  Trap: отправляет сообщение Trap в NMS и информирует NMS о событии.

  Log-Trap: регистрирует событие и отправляет сообщение Trap в NMS.

  None: указывает на отсутствие действий.
- Alarm group

  Управление аварийными сигналами RMON может отслеживать указанные переменные аварийных сигналов. После того, как записи сигналов тревоги определены, система получит значения контролируемых переменных сигналов тревоги за определенный период. Когда значение переменной тревоги больше или равно верхнему пределу, инициируется нарастающее событие тревоги. Когда значение тревожной переменной меньше или равно нижнему пределу, запускается падающее тревожное событие. Аварийные сигналы будут обрабатываться в соответствии с определением события.

Если выбранное значение переменной тревоги превышает пороговое значение несколько раз в одном и том же направлении, то событие тревоги запускается только в первый раз. Таким образом, попеременно генерируются сигналы повышения и снижения.

6.22.3. Веб конфигурирование

Перейти [Device Advanced Configuration] → [RMON configuration] → [RMON Statistics] для входа на страницу статистики RMON, как показано на рисунке ниже.

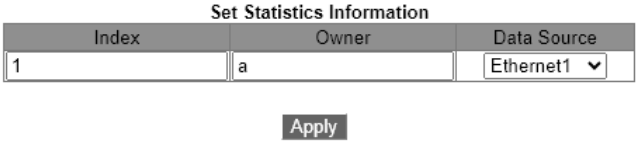


Рис. 254. Вход на страницу статистики RMON

- **Index**
  Диапазон: 1~65535
  Функция: Настройка номера записи статистики.
- **Ower**
  Диапазон: 1~32 символа
  Функция: Настройка имени записи статистики.
- **DataSource**
  Функция: Выберите порт, статистика которого должна быть собрана.

Перейти [Device Advanced Configuration] → [RMON configuration] → [RMON History] для входа на страницу RMON History, как показано на рисунке ниже.

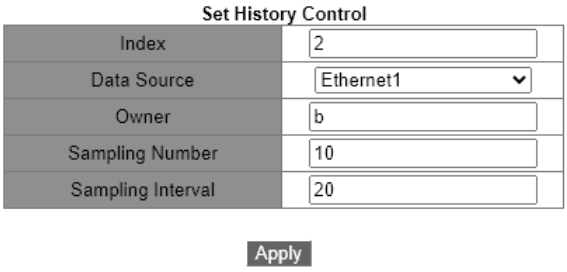


Рис. 255. Вход на страницу RMON History

- **Index**
  Диапазон: 1~65535
  Функция: Настройка номера записи истории.
- **DataSource**
  Функция: Выберите порт, информация которого должна быть запрошена.
- **Owner**
  Диапазон: 1~32 символа
  Функция: Настройка имени записи истории.
- **Sampling Number**
  Диапазон: 1~65535
  Функция: настроить время выборки порта.
- **Sampling Space**
  Диапазон: 1~3600 с
  Функция: Настройка периода выборки порта.

Перейти [Device Advanced Configuration] → [RMON configuration] → [RMON Event] для входа на страницу RMON Event, как показано на рисунке ниже.

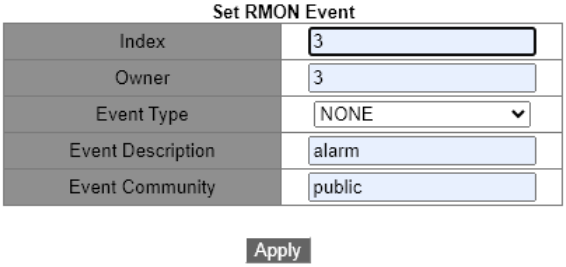


Рис. 256. Вход на страницу RMON Event

- **Index**
  Диапазон: 1~65535
  Функция: Настройка порядкового номера записи события.
- **Owner**
  Диапазон: 1~30 символов
  Функция: Настройка имени записи события.
- **Event Type**
  Варианты: NONE / LOG / Snmp-Trap/ Log and Trap
  По умолчанию: NONE
  Функция: Настроить тип события для аварийных сигналов, то есть режим обработки аварийных сигналов.
- **Event Description**
  Диапазон: 1~126 символов
  Функция: Опишите событие.
- **Event Community**
  Диапазон: 1~126 символов
  Функция: настроить имя сообщества для отправки события trap. Значение должно быть таким же, как в SNMP.

Перейти [Device Advanced Configuration] → [RMON configuration] → [RMON Alarm] для входа на страницу RMON Alarm, как показано на рисунке ниже.

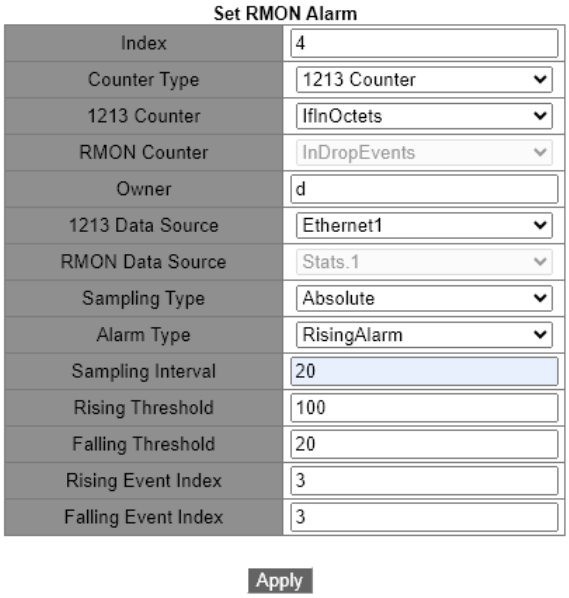


Рис. 257. Вход на страницу RMON Alarm

- **Index**
  Диапазон: 1~65535
  Функция: Настройка номера записи тревоги.
- **Counter Type**
  Опции: Счетчик 1213/ Счетчик RMON
  Функция: Выберите тип узла MIB.
- **1213 Counter/RMON Counter**
  Функция: Установите тип тревоги RMON.
- **Owner**
  Диапазон: 1~31 символ
  Функция: Настройка имени записи тревоги.
- **1213 DataSource**
  Функция: Выберите порт, информация о котором должна отслеживаться.
- **RMON DataSource**
  Параметры: Идентификатор индекса записи статистики в таблице статистики RMON.
  Функция: контролировать информацию о порте в таблице статистики RMON.
- **Sampling Type**
  Опции: Абсолют/Дельта
  По умолчанию: Абсолютный
  Функция: Absolute указывает на выборку на основе абсолютного значения. Значение переменной извлекается напрямую, когда приближается конец периода выборки. Дельта указывает выборку на основе изменения значения. Значение изменения переменной в периоде выборки извлекается, когда приближается конец периода.
- **Alarm Type**
  Опции: RisingAlarm / FallingAlarm / RisOrFallAlarm
  По умолчанию: RisingAlarm
  Функция: Выберите тип тревоги, включая тревогу по нарастающему фронту, тревогу по заднему фронту, а также тревогу по нарастающему и заднему фронту.

- **Sampling Space**
  Диапазон: 1~65535
  Функция: Настройка периода выборки.
- **Rising Threshold**
  Диапазон: 0~65535
  Функция: Настройка порога нарастания фронта. Когда значение выборки превышает пороговое значение, а тип сигнала тревоги установлен на RisingAlarm или RisOrFallAlarm, генерируется сигнал тревоги и запускается индекс события нарастания.
- **Falling Threshold**
  Диапазон: 0~65535
  Функция: Настройка порога заднего фронта. Когда значение выборки ниже порогового значения, а тип сигнала тревоги установлен на FallingAlarm или RisOrFallAlarm, генерируется сигнал тревоги и запускается индекс события падения.
- **Rising EventIndex**
  Диапазон: 0~65535
  Функция: Настройте индекс нарастающего события, т. е. режим обработки сигналов тревоги нарастающего фронта.
- **Falling EventIndex**
  Диапазон: 0~65535
  Функция: Сконфигурируйте индекс падающего события, т. е. режим обработки аварийных сигналов заднего фронта.

6.23. SNTP конфигурация

6.23.1. Введение

Простой протокол сетевого времени (Simple Network Time Protocol - SNTP) синхронизирует время между сервером и клиентом с помощью запросов и ответов. Как клиент коммутатор синхронизирует время с сервером по пакетам сервера. Для одного коммутатора можно настроить несколько серверов SNTP, но только один из них может быть активен одновременно. Клиент SNTP отправляет запрос на каждый сервер один за другим через одноадресную рассылку. Сервер, который первым дает ответ, находится в активном состоянии. Остальные серверы находятся в неактивном состоянии.

Для синхронизации времени по SNTP должен быть активный SNTP-сервер.
Вся информация о времени, передаваемая в протоколе SNTP, является стандартной информацией о времени для часового пояса 0.

6.23.2. Веб конфигурация

Включение SNTP протокола

Перейти [Device Advanced Configuration] → [SNTP configuration] → [Enable SNTP] для входа на страницу конфигурации SNTP, как показано на рисунке ниже.

Рис. 258. Включение SNTP протокола

- **SNTP State**
  Параметры: Enable / Disable
  По умолчанию: Disable
  Функция: включить / отключить SNTP

Настройте сервер SNTP, как показано на рис. ниже;
Перейти [Device Advanced Configuration] → [SNTP configuration] → [NTP/NTP Server Configuration]

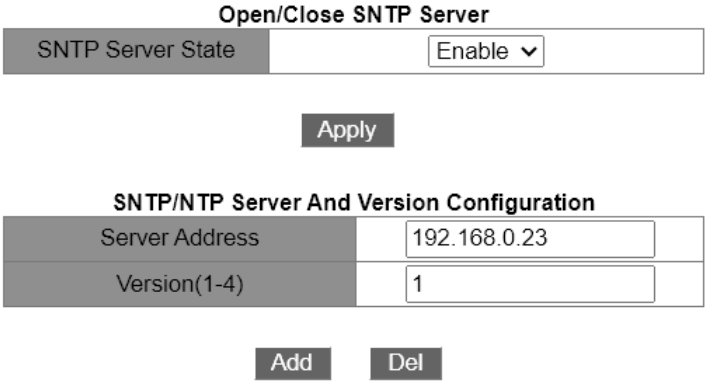


Рис. 259. Настройка сервера SNTP

- **Состояние SNTP-сервера**
  Объем настройки: вкл./выкл. адрес сервера
  Формат конфигурации: A.B.C.D.
  Функция: Настройте IP-адрес сервера SNTP, и клиент будет калибровать время в соответствии с сообщением сервера.
- **Версия**
  Варианты конфигурации: 1~4
  Функция: настройка номера текущей версии протокола SNTP.

Настройте интервал времени, в течение которого клиент SNTP будет отправлять запросы на синхронизацию, как показано на рис. 260;

Перейти [Device Advanced Configuration] → [SNTP configuration] → [Request Interval Configuration]

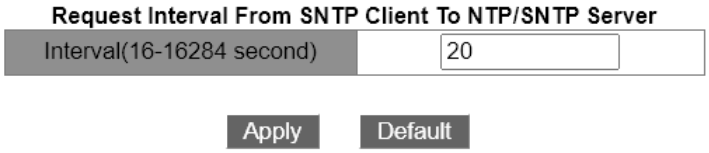
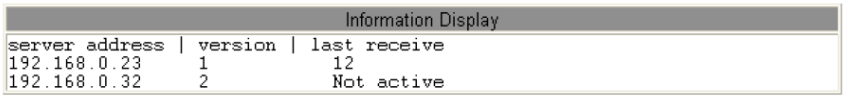


Рис. 260. Настройка интервала для запросов SNTP

- **временной интервал**
  Варианты конфигурации: 16~16284 с
  Функция: Настройка интервала времени, в течение которого клиент SNTP отправляет запрос на синхронизацию на сервер SNTP.

Просмотр информации о конфигурации SNTP

Перейти [Device Advanced Configuration] → [SNTP configuration] → [Show SNTP] для входа на страницу конфигурации SNTP, как показано на рисунке ниже.



6.24. NTP конфигурация

6.24.1. Введение

NTP (Network Time Protocol, сетевой протокол времени) используется для синхронизации времени между распределенными серверами времени и клиентами. NTP может синхронизировать часы всех устройств с часами в сети, чтобы синхронизировать часы всех устройств в сети, чтобы устройства могли предоставлять несколько приложений на основе одного и того же времени. Для локальной системы, на которой работает NTP, он может не только получать синхронизацию от других источников синхронизации, но и выступать в качестве источника синхронизации для синхронизации других часов.

Как показано на рис. 261, двусторонняя задержка Delay=(T4-T1)-(T3-T2) и смещение часов устройства Offset=((T2-T1)+(T3-T4))/2, чтобы добиться высокоточной синхронизации времени устройств в сети.

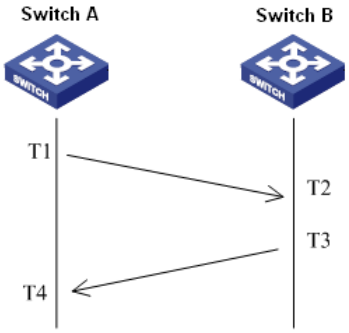


Рис. 261. Пример работы NTP

6.24.2. Рабочий режим NTP

Протокол NTP может использовать следующие рабочие режимы для синхронизации времени, и пользователи могут выбрать подходящий рабочий режим в соответствии со своими потребностями.

Режим клиент/сервер: в этом режиме клиент отправляет сообщение синхронизации часов на сервер (режим клиента); сервер автоматически работает в режиме сервера после получения сообщения и отправляет ответное сообщение (режим сервера); после получения ответного сообщения, синхронизироваться с оптимальными часами сервера.

Одноранговый режим: в этом режиме активный одноранговый узел отправляет сообщение синхронизации часов пассивному одноранговому узлу (режим активного однорангового узла), а пассивный одноранговый узел после получения сообщения работает в режиме пассивного однорангового узла и отправляет ответное сообщение (режим пассивного однорангового узла). После обмена сообщениями устанавливается одноранговый режим, и активный и пассивный одноранговые узлы могут синхронизироваться друг с другом, если они были синхронизированы, то приоритет имеют часы с меньшим количеством уровней.

Широковещательный режим: в этом режиме широковещательный сервер периодически рассылает пакеты синхронизации часов (режим широковещания), а широковещательный клиент отправляет пакеты синхронизации часов на сервер после получения широковещательных пакетов (режим клиента), и сервер получает после сообщения запроса, отправить ответное сообщение (режим сервера). Сервер и клиент завершают синхронизацию системных часов посредством взаимодействия 8 сообщений запроса и ответа.

Многоадресный режим: многоадресный клиент периодически отправляет многоадресное сообщение запроса синхронизации часов на многоадресный сервер (режим клиента), а сервер отправляет одноадресное ответное сообщение после получения сообщения (режим сервера). После этого сервер и клиент обмениваются одноадресными запросами синхронизации часов и ответными сообщениями, чтобы завершить синхронизацию часов.

6.24.3. Веб конфигурация

Включение NTP

Перейдите [Device Advanced Configuration] → [NTP configuration] → [confignt pServer] для входа в глобальную конфигурацию NTP как показано на рисунке ниже.

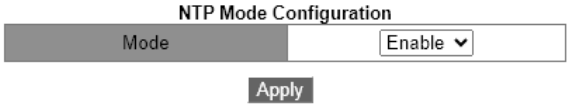


Рис. 262. Включение NTP

- **Mode**
  Опции: Enable / Disable
  По умолчанию: Disable.
  Фунция: Включение или выключение NTP.

NTP и SNTP нельзя использовать одновременно, так как они используют один и тот же порт UDP.
Вы также можете настроить службу NTP и сохранить конфигурацию, когда служба NTP неполноценный. Включена ли служба NTP, это не влияет на конфигурацию NTP.

Конфигурирование NTP unicast, как показано на рисунке ниже.

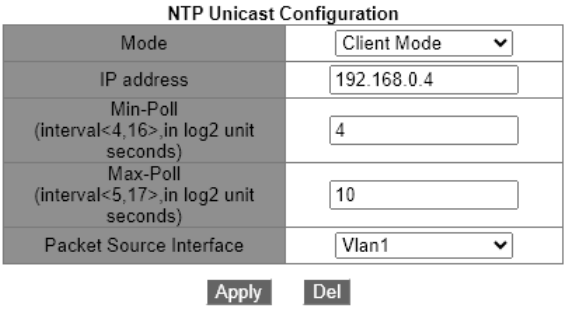


Рис. 263. Конфигурирование NTP unicast

- **NTP State**
  Опции: Client Mode / Peer Mode
  Фунция: Выбор NTP режима.
  Описание: Режим клиента указывает, что рабочий режим NTP является режимом клиент/сервер; одноранговый режим указывает, что рабочий режим NTP является равноправным.
- **IP address**
  Формат: A.B.C.D.
  Описание: Когда принимается режим клиент/сервер, IP-адрес совпадает с адресом NTP-сервера. Когда принимается одноранговый режим, IP-адрес является адресом пассивного однорангового узла.

- **MIN-Poll**
  Диапазон: от 4 до 16. Интервал=2n с («n» — значение этого параметра)
  По умолчанию: 4. В этом случае интервал равен 16 с (24).
  Функция: Настройка минимального интервала запросов для обмена пакетами NTP между локальным устройством и сервером.
- **MAX-Poll**
  Диапазон: от 5 до 17. Интервал=2n с («n» — значение этого параметра)
  По умолчанию: 10. В данном случае интервал равен 1024 с (210).
  Функция: Настройка максимального интервала запросов для обмена пакетами NTP между локальным устройством и сервером.
- **Packet source interface**
  Функция: укажите порт для отправки пакетов NTP.
  Описание: Когда используется режим клиент/сервер, локальное устройство отправляет пакеты NTP на сервер. IP-адрес источника в пакетах является основным IP-адресом порта.
  Когда принимается одноранговый режим, локальное устройство отправляет пакеты NTP одноранговому узлу. IP-адрес источника в пакетах является основным IP-адресом порта.

Если принят режим клиент/сервер, вам нужно только выполнить предыдущую настройку на клиенте.
Настроенные часы сервера NTP должны быть синхронизированы, прежде чем обеспечивать синхронизацию времени для других устройств.
Если выбран одноранговый режим, вам нужно выполнить предыдущую настройку только на активном одноранговом устройстве.
Min-Poll ≤ Max-Poll.
Значения Min-Poll узлов NTP должны быть одинаковыми.

Настройте сервер многоадресной рассылки NTP

Нажмите [Device Advanced Configuration] → [NTP configuration] → [Multicast Server Configuration], чтобы открыть страницу конфигурации сервера многоадресной рассылки, как показано на рис. 264.

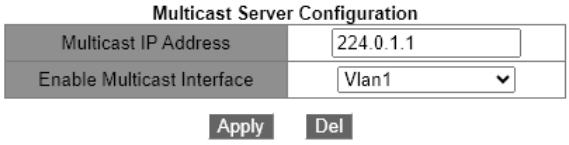


Рис. 264. Сервер многоадресной рассылки NTP

- **Multicast IP Address**
  Формат: A.B.C.D.
  Функция: Настройка многоадресного IP-адреса. Если указанный многоадресный IP-адрес недоступен, по умолчанию принимается 224.0.1.1.
- **Enable Multicast Interface**
  Функция: укажите многоадресный порт.

Настройка многоадресного клиента NTP

Нажмите [Device Advanced Configuration] → [NTP configuration] → [Multicast Client Configuration], чтобы открыть страницу конфигурации клиента многоадресной рассылки, как показано на рис. 265.

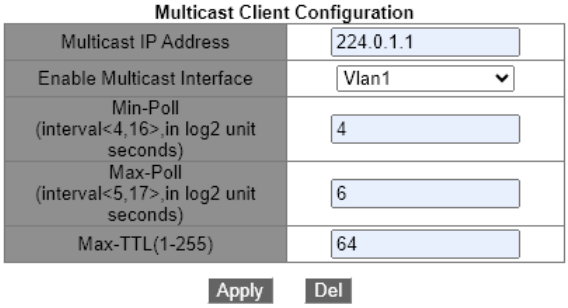


Рис. 265. Настройка многоадресного клиента NTP

- **Multicast IP Address**
  Формат: A.B.C.D.
  Функция: Настройка IP-адреса, используемого в многоадресном режиме. Если указанный многоадресный IP-адрес недоступен, по умолчанию принимается 224.0.1.1.
- **Enable Multicast Interface**
  Функция: укажите многоадресный порт.
- **Min-Poll**
  Диапазон: от 4 до 16. Интервал=2n с («n» — значение этого параметра)
  По умолчанию: 4. В этом случае интервал равен 16 с (24).
  Функция: Настройка минимального интервала запросов для обмена пакетами NTP между локальным устройством и сервером.
- **Max-Poll**
  Диапазон: от 5 до 17. Интервал=2n с («n» — значение этого параметра)
  По умолчанию: 10. В данном случае интервал равен 1024 с (210).
- **Max-TTL**
  Диапазон: 1~255
  По умолчанию: 64
  Функция: Настройка максимального TTL для запросов многоадресной рассылки, отправляемых клиентом многоадресной рассылки.

Настройка широковещательного сервера NTP

Нажмите [Device Advanced Configuration] → [NTP configuration] → [Broadcast Server Configuration], чтобы открыть страницу конфигурации сервера вещания, как показано на рис. 266.

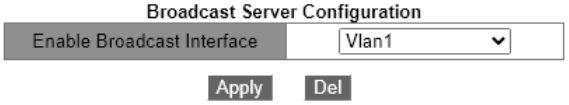


Рис. 266. Настройка широковещательного сервера NTP

- **Enable Broadcast Interface**
  Функция: Указать широковещательный порт

Настройка эталонных часов

Нажмите [Device Advanced Configuration] → [NTP configuration] → [Reference Clock Configuration], чтобы открыть страницу конфигурации эталонных часов, как показано на рис. 267.

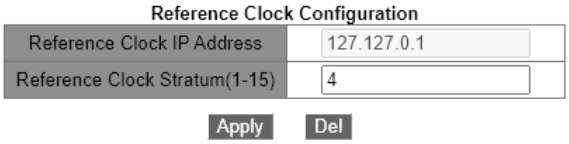


Рис. 267. Настройка эталонных часов

- **Reference Clock IP Address**
  Формат: 127.127.t.u.
  По умолчанию: 127.127.0.1
  Описание: "t" в 127.127.0.1 указывает тип опорных часов, а "u" указывает идентификатор экземпляра. В настоящее время поддерживается только 127.127.0.1. То есть системные часы служат опорными часами.
- **Reference Clock Stratum**
  Диапазон: 1~15
  По умолчанию: 4
  Функция: Настройте уровень эталонных часов.
  Описание: Уровень часов показывает точность часов. Чем больше число, тем ниже точность. Если уровень равен 16, часы не синхронизированы и, следовательно, не могут служить эталонными часами.

В настоящее время эталонными часами может служить только сам коммутатор. Перед настройкой этого элемента Вы должны подтвердить требования синхронизации времени системы.

6.24.4. Пример типовой конфигурации

Настройка однорангового режима:

Как показано на рис. 268, необходимо настроить локальные часы на коммутаторе D в качестве эталонных часов и установить для его страты значение 2. Коммутатор A работает в режиме клиента, а коммутатор D служит NTP-сервером. Коммутатор A является его партнером, коммутатор B — активным партнером, а коммутатор A — пассивным партнером.

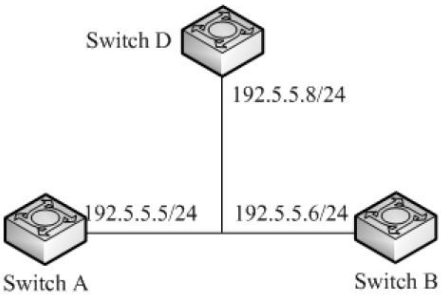


Рис. 268. Пример конфигурации

Конфигурация на коммутаторе D:

1. Включить NTP, как показано на рис. 262.
2. Установите IP-адрес эталонных часов на 127.127.0.1 и уровень часов на 2, как показано на рис. 267.

Конфигурация коммутатора A:

3. Включите NTP, как показано на рис. 262.
4. Установите IP-адрес NTP-сервера на 192.5.5.8, Min-Poll на 4, Max-Poll на 10 и NTP Source на VLAN 1, как показано на рис. 263.

Конфигурация на коммутаторе B:

5. Включите NTP, как показано на рис. 262.
6. Установите IP-адрес однорангового узла NTP на 192.5.5.5, Min-Poll на 4, Max-Poll на 10 и NTP Source на VLAN 1, как показано на рис. 263.

Настройка многоадресного режима:

Как показано на рис. 269, необходимо настроить локальные часы на коммутаторе D в качестве эталонных часов и установить уровень 2. Коммутатор D работает в режиме многоадресного сервера. Режим многоадресного сервера настроен на порте VLAN 2. Коммутатор A и коммутатор B работают в режиме клиента многоадресной рассылки Режим клиента многоадресной рассылки настроен на VLAN 2.

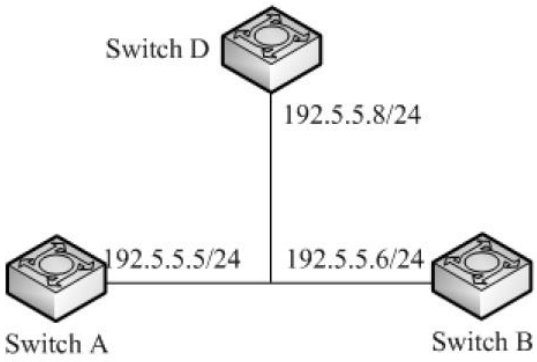


Рис. 269. Настройка многоадресного режима

Конфигурация на коммутаторе D:

1. Включите NTP, как показано на рис. 262.
2. Установите IP-адрес эталонных часов на 127.127.0.1 и уровень часов на 2, как показано на рис. 267.
3. Настройте сервер многоадресной рассылки: установите IP-адрес многоадресной рассылки на 224.0.1.1 и порт на VLAN 2, как показано на рис. 264.

Конфигурации коммутатора A и коммутатора B:

4. Включите NTP, как показано на рис. 262.
5. Настройте многоадресный клиент: установите многоадресный IP-адрес на 224.0.1.1, порт на VLAN 2, Min-Poll на 4, Max-Poll на 10 и Max-TTL на 64, как показано на рис. 265.

Настройка режима трансляции:

Как показано на рис. 270, необходимо настроить локальные часы на коммутаторе D в качестве эталонных часов и установить уровень 2. Коммутатор D работает в режиме широковещательного сервера. Режим широковещательного сервера настроен на порте VLAN 2. Коммутатор A и коммутатор B работают в режиме широковещательного клиента. Режим широковещательного клиента настроен на VLAN 2.

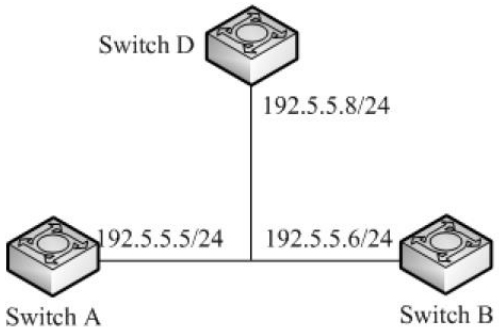


Рис. 270. Настройка режима трансляции

Конфигурация на коммутаторе D:

1. Включите NTP, как показано на рис. 262.

2. Установите IP-адрес эталонных часов на 127.127.0.1 и уровень часов на 2, как показано на рис. 267.
3. Настройте широковещательный сервер: установите широковещательный порт на VLAN 2, как показано на рис. 266.
   Конфигурации на коммутаторе A и коммутаторе B:
4. Включите NTP, как показано на рис. 262.
5. Настройте широковещательный клиент: установите широковещательный порт на VLAN 2, как показано на рис. 266.

6.25. Конфигурация TACACS+

6.25.1. Введение

Система управления доступом к контроллеру доступа к терминалу (TACACS+) представляет собой приложение на основе TCP. Он принимает режим клиент/сервер для реализации связи между сервером доступа к сети (NAS) и сервером TACACS+. Клиент работает на NAS, а информация о пользователях управляется централизованно на сервере. NAS — это сервер для пользователей, но клиент для сервера. Рис. 271 показывает структуру.

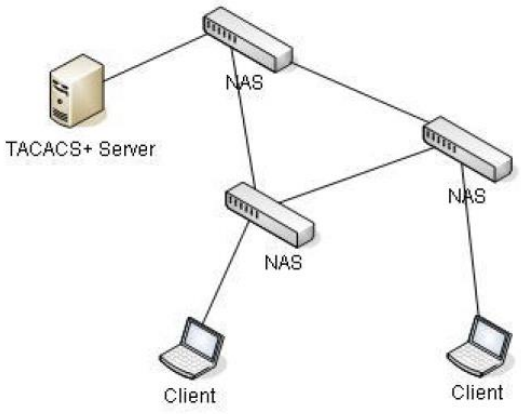


Рис. 271. Структура TACACS+

Протокол аутентифицирует, авторизует пользователей терминалов, которым необходимо войти на устройство для выполнения операций. Устройство служит клиентом TACACS+ и отправляет имя пользователя и пароль на сервер TACACS+ для аутентификации. Сервер получает запросы TCP-соединения от пользователей, отвечает на запросы аутентификации и проверяет легитимность пользователей. Если пользователь проходит аутентификацию, он может войти на устройство для операций.

6.25.2. Веб конфигурация

Включение TACACS+

Перейдите [Device Advanced Configuration] → [TACACS-PLUS Configuration] → [TACACS-PLUS configuration], чтобы открыть страницу конфигурации TACACS+, как показано на рис. 272.

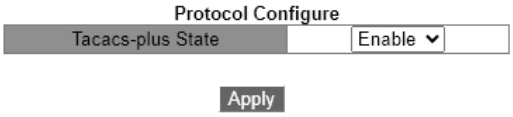


Рис. 272. Включение TACACS+

- **Tacacs-plus State**
  Опции: Enable/Disable
  По умолчанию: Disable
  Функция: Включение/Выключение TACACS+.

Конфигурация TACACS+ сервера как показно на рисунке ниже

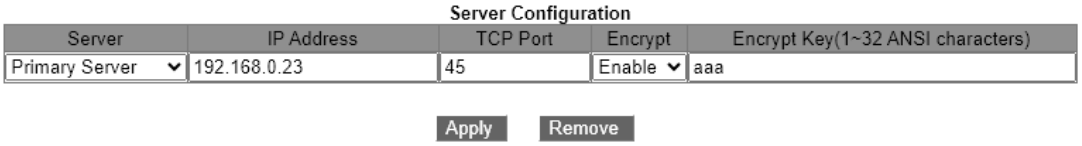


Рис. 273. Конфигурация TACACS+ сервера

- **Server**
  Опции: основной / вторичный
  По умолчанию: основной
  Функция: выберите тип сервера.
- **IP Address**
  Формат: A.B.C.D.
  Функция: введите IP-адрес сервера.
- **TCP-port**
  Диапазон: 1~65535
  По умолчанию: 49
  Функция: Установите количество портов, которые получают запросы аутентификации NAS.
- **Encrypt**
  Опции: включить/отключить
  По умолчанию: Отключить
  Функция: Шифровать пакет или нет. Если он включен, требуется ключ.
- **Encrypt key**
  Диапазон: 1~32 символа

Описание: Установите ключ для повышения безопасности связи между клиентом и сервером TACACS+. Две стороны совместно используют ключ для проверки легитимности пакетов. Обе стороны могут получать пакеты друг от друга только тогда, когда ключи совпадают. Поэтому убедитесь, что настроенный ключ совпадает с ключом на сервере TACACS+.

После завершения настройки в следующем разделе «Sever Configured» отображается информация о конфигурации сервера, как показано на рис. 274.

Server List				
Primary Server	192.168.0.23	45	Encrypt	aaa
Secondary Server	192.168.0.32	45	Unencrypt	-

Рис. 274. Информация о конфигурации сервера

6.25.3. Типовая конфигурация.

Как показано на рис. 275, сервер TACACS+ может аутентифицировать и авторизовать пользователей с помощью коммутатора. IP-адрес сервера — 192.168.0.23, а общий ключ, используемый при обмене пакетами между коммутатором и сервером, — aaa.

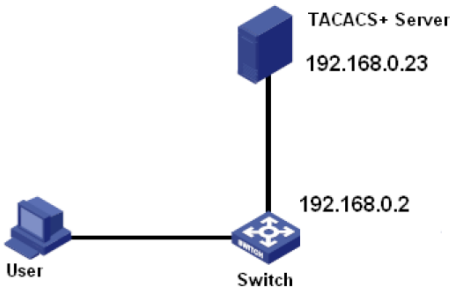


Рис. 275. Пример конфигурации

1. Включите TACACS+, как показано на рис. 272.
2. Настройка сервера TACACS+. Установите IP-адрес сервера на 192.168.0.23 и ключ шифрования на aaa и включите шифрование, как показано на рис. 273.
3. При входе в коммутатор через Интернет выберите «Локальный», при входе в коммутатор через telnet выберите «Tacacs+», как показано на рис. 276.

   Перейдите [Device Advanced Configuration] → [Authentication Login Configuration] → [Authentication Login Configuration], как показано далее.

Authentication Login Configuration

Login Method	Authentication Method1	Authentication Method2	Authentication Method3
Telnet	Local	Tacacs+	Radius

Apply

Рис. 276. Выбор режима аутентификации

4. Настройте имя пользователя и пароль «bbb», зашифруйте ключ «aaa» на сервере TACACS+.
5. При входе в коммутатор через Интернет введите имя пользователя «admin» и пароль «STEZ», чтобы пройти локальную аутентификацию.
6. При входе в коммутатор через Telnet введите имя пользователя и пароль «bbb», чтобы пройти аутентификацию TACACS+.

6.26. Конфигурация RADIUS

6.26.1. Введение

RADIUS (Remote Authentication Dial-In User Service) — это распределенный протокол обмена информацией. Он определяет формат кадра RADIUS на основе UDP и механизм передачи информации, защищая сети от несанкционированного доступа. RADIUS обычно используется в сетях, требующих высокой безопасности и удаленного доступа пользователей. RADIUS использует режим клиент / сервер для обеспечения связи между NAS (сервером доступа к сети) и сервером RADIUS. Клиент RADIUS работает на NAS. Сервер RADIUS обеспечивает централизованное управление пользовательской информацией. NAS является сервером для пользователей, но клиентом для сервера RADIUS. Рисунок 353 показывает структуру.

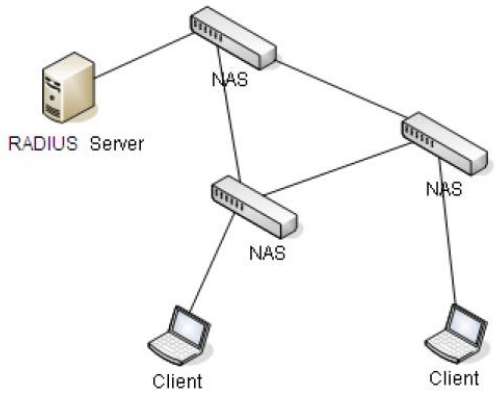


Рис. 277. Струкутура RADIUS

Протокол аутентифицирует пользователей терминалов, которым для работы необходимо войти в систему. Выступая в качестве клиента RADIUS, устройство отправляет информацию о пользователе на сервер RADIUS для аутентификации и разрешает или запрещает пользователям входить в систему в соответствии с результатами проверки подлинности.

6.26.2. Веб конфигурация

Конфигурация параметров RADIUS

Нажмите [Device Advanced Configuration] → [RADIUS configuration] → [RADIUS configuration] для хода на страницу конфигурации RADIUS как показано на рис. 278.

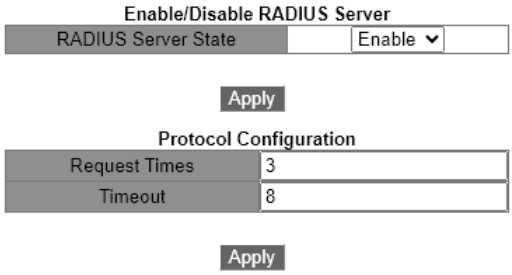


Рис. 278. Конфигурация параметров RADIUS

- **Request Times**
  Диапазон: 1~3
  По умолчанию: 3
  Функция: Установите максимальное количество попыток повторной передачи для пакетов запроса RADIUS. Если устройство по-прежнему не получает ответные пакеты от сервера RADIUS после максимального количества попыток повторной передачи, устройство считает, что аутентификация не удалась.
- **Timeout**
  Диапазон: 1~3
  По умолчанию: 3
  Функция: Установите дополнительное время для ответа от сервера RADIUS. После отправки пакета запроса RADIUS устройство повторит передачу пакета запроса RADIUS, если оно по-прежнему не получит ответа от сервера RADIUS по истечении указанного времени.

Настройте RADIUS-сервер, как показано на рис. 279.

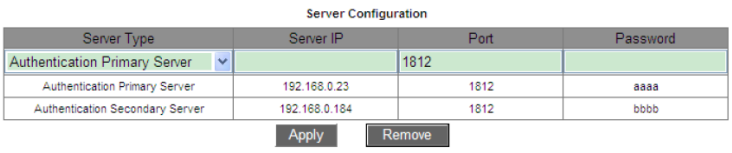


Рис. 279. Настройка RADIUS-сервера

- **Server Type**
  Опции: первичный сервер аутентификации/вторичный сервер аутентификации
  Функция: настроить первичный или вторичный сервер RADIUS. Если первичный сервер недоступен, для аутентификации будет использоваться вторичный сервер.
- **Server IP**
  Формат: A.B.C.D.

Функция: Установите IP-адрес сервера RADIUS.

- **Port**
  Диапазон: 1~65535
  По умолчанию: 1812
  Функция: Установите UDP-порт RADIUS-сервера.
  PasswordПароль
  Диапазон: 1~32 символа
  Функция: Настройка пароля сервера RADIUS.

6.26.3. Типовая конфигурация

Как показано на рис. 280, IEEE802.1x включен на порту 1 коммутатора. Затем пользователи могут войти в коммутатор через порт 1 после прохождения аутентификации на сервере RADIUS. IP-адрес сервера 192.168.0.23. Ключ для обмена пакетами между коммутатором и сервером — аааа.

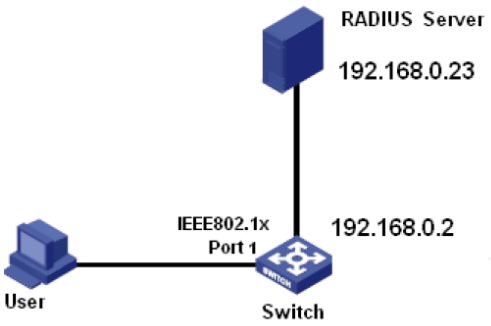


Рис. 280. Типовая конфигурация

1. Установите IP-адрес основного сервера аутентификации на 192.168.0.23 и пароль на аааа, как показано на рис. 278, 279.
2. Настройки IEEE802.1x: глобально включить IEEE802.1x. Включите IEEE802.1x на порту 1. Оставьте значения по умолчанию для других параметров. Подробнее см. в разделе «IEEE802.1x».
3. Установите аутентификацию по радиусу, как показано на рис. 276.
4. Установите для имени пользователя и пароля на сервере RADIUS значение ссс, ключ шифрования — аааа.
5. Установите и запустите клиентское программное обеспечение 802.1x на ПК. Введите ссс в качестве имени пользователя и пароля. Затем пользователь может пройти аутентификацию и получить доступ к коммутатору через порт 1.

6.27. Конфингурация IEEE802.1x

6.27.1. Введение

Для обеспечения безопасности WLAN комитет IEEE802 LAN/WAN предложил протокол 802.1x. Как общий механизм управления доступом к портам LAN в Ethernet, 802.1x реализует аутентификацию и безопасность Ethernet. 802.1x — это управление доступом к сети на основе портов. Управление доступом к сети на основе портов предназначено для реализации аутентификации и управления портами устройств доступа к локальной сети. Если пользователь проходит аутентификацию, он может получить доступ к ресурсам в локальной сети. Если он не может пройти аутентификацию, он не может получить доступ к ресурсам в локальной сети. Системы 802.1x используют структуру клиент/сервер. Аутентификация пользователя и авторизация управления доступом на основе порта требуют следующих элементов: Клиент: обычно указывает пользовательский терминал. Когда пользователь хочет выйти в Интернет, он запускает клиентскую программу и вводит необходимое имя пользователя и пароль. Клиентская программа отправит запрос на соединение. Устройство: указывает коммутатор аутентификации в системе Ethernet. Он загружает и доставляет информацию об аутентификации пользователя, а также включает или отключает порт в зависимости от результата аутентификации.

Сервер аутентификации: указывает объект, предоставляющий сервис аутентификации для устройств. Он проверяет, есть ли у пользователей разрешения на использование сетевых служб в соответствии с идентификаторами (именами пользователей и паролями), отправленными клиентами, и включает или отключает порты в соответствии с результатами аутентификации.

6.27.2. Веб конфигурирование

Глобальное включение IEEE802.1x протокола

Нажмите [Device Advanced Configuration] → [IEEE802.1x configuration] → [IEEE802.1x configuration], для входа на страницу конфигурации IEEE802.1x как показано на рисунке ниже.

Рис. 281. Включение IEEE802.1x протокола

- **IEEE802.1x State**
  Опции: включить/отключить
  По умолчанию: Отключить
  Функция: включение/отключение глобальной функции безопасности IEEE802.1x.

Настройте время ожидания сервера, как показано на рис. 282.

Рис. 282. Время ожидания сервера

- **Server Timeout**
  Диапазон: 100~ 30 с
  По умолчанию: 10 с
  Функция: Настройка тайм-аута сервера.

Настройте порт, на котором включен IEEE802.1x, как показано на рис. 283.

Рис. 283. Настройка порта IEEE802.1x

- **PortId**
  Опции: все порты коммутатора.
- **IEEE802.1x State**
  Опции: Включить/Выключить.
  По умолчанию: Отключить
  Функция: включение/отключение IEEE802.1x на порту.
  Описание: Когда эта функция включена, связь пользователей через порт зависит от режима порта IEEE802.1x.
- **Port Mode**
  Варианты: Unauthorized-force / Auto / Authorized-force
  По умолчанию: Авто
  Функция: выберите режим аутентификации порта.
  Описание: **Unauthorized-force** означает, что порт всегда находится в неавторизованном состоянии и не позволяет пользователям проводить аутентификацию, а коммутатор не предоставляет услуги аутентификации клиентам, которые получают доступ к коммутатору с этого порта. **Auto** означает, что начальное состояние порта неавторизовано, и порт не позволяет пользователям получать доступ к сетевым ресурсам. Если пользователь проходит аутентификацию, порт переходит в авторизованное состояние и позволяет пользователям получать доступ к сетевым ресурсам. Если пользователю не удастся пройти аутентификацию, порт перейдет в неавторизованное состояние и не позволит пользователям получить доступ к сетевым ресурсам. **Authorized-force** означает, что порт всегда находится в авторизованном состоянии и позволяет пользователям получать доступ к сетевым ресурсам без аутентификации.
- **ReAuth**

Опции: включить/отключить
По умолчанию: Отключить
Функция: Настройка необходимости регулярной повторной аутентификации при успешном выполнении аутентификации.

- **ReAuth Timer**
  Диапазон: 60~7200 с
  По умолчанию: 3600 с
  Функция: при успешной аутентификации установите временной интервал для повторной аутентификации.
- **Quiet Timer**
  Диапазон: 10~120 с
  По умолчанию: 60 сек.
  Функция: если аутентификация не удалась, начинается период молчания (QuietPeriod). В течение периода молчания сервер не отвечает на запросы аутентификации от клиента. После окончания периода молчания сервер снова начинает принимать запросы аутентификации.
- **Port-Method**
  Варианты: на основе порта/на основе MAC-адреса
  По умолчанию: на основе порта
  Функция: настройка режима управления доступом к портам с поддержкой IEEE802.1x.
  Описание: MAC_Based указывает, что пользователи, использующие порт, должны пройти аутентификацию соответственно. Когда пользователь находится в автономном режиме, только пользователь не может использовать сеть. Port_Based указывает, что пользователи аутентифицируются на основе порта. После того как первый пользователь, использующий порт, проходит аутентификацию, всем другим пользователям, использующим порт, аутентификация не требуется. Однако, когда первый пользователь находится в автономном режиме, порт отключается, и все остальные пользователи, использующие этот порт, не могут использовать сеть.
- **Max User Number**
  Диапазон: 1~128
  По умолчанию: 128
  Функция: настроить максимальное количество пользователей доступа, использующих порт с поддержкой IEEE802.1x.
  Описание: Конфигурация действительна только для портов с управлением доступом на основе MAC-адресов.

Просмотр конфигурации IEEE802.1x

Нажмите [Device Advanced Configuration] → [IEEE802.1x configuration] → [IEEE802.1x information], чтобы просмотреть конфигурацию IEEE802.1x, как показано на рис. 284.

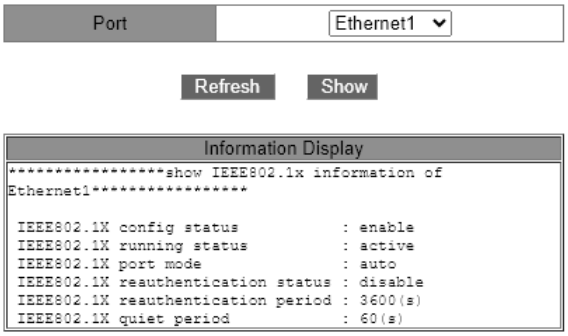


Рис. 284. Просмотр конфигурации IEEE802.1x

7. Приложение: принятые сокращения

Сокращение	Полное обозначение	Полное обозначение
ACE	Access Control Entry	Запись для списка контроля доступа
ACL	Access Control List	Список контроля доступа
ARP	Address Resolution Protocol	Протокол разрешения адресов
BootP	Bootstrap Protocol	Протокол получения IP адреса
BPDU	Bridge Protocol Data Unit	Блок данных протокола Spanning Tree
CIST	Common and Internal Spanning Tree	Общее и внутреннее связующее дерево
CLI	Command Line Interface	Интерфейс командной строки
CoS	Class of Service	Класс сервиса
CST	Common Spanning Tree	Общее связующее дерево
DHCP	Dynamic Host Configuration Protocol	Протокол динамического конфигурирования узлов
DHP	Dual Homing Protocol	Протокол двойной обратной связи
DNS	Domain Name System	Система доменных имен
DSCP	Differentiated Services CodePoint	Точка кода дифференцированных сервисов
DST	Daylight Saving Time	Переход на летнее время
EAPOL	Extensible Authentication Protocol over LAN	Протокол пердачи пакетов EAP через локальную сеть
GARP	Generic Attribute Registration Protocol	Протокол регистрации основных атрибутов
GMRP	GARP Multicast Registration Protocol	GARP протокол регистрации многоадресной рассылки
GVRP	GARP VLAN Registration Protocol	GARP ротокол регистрации VLAN
HTTP	Hyper Text Transfer Protocol	Протокол передачи гипертекста
ICMP	Internet Control Message Protocol	Протокол управляющих сообщений в сети
IGMP	Internet Group Management Protocol	Протокол управления групповой (multicast) передачей данных в сетях
IGMP Snooping	Internet Group Management Protocol Snooping	Протокол отслеживания IGMP
IST	Internal Spanning Tree	Внутреннее связующее дерево
LACP	Link Aggregation Control Protocol	Протокол управления агрегацией каналов
LACPDU	Link Aggregation Control Protocol Data Unit	Блок данных LACP
LLDP	Link Layer Discovery Protocol	Протокол обнаружения канального уровня

LLDPDU	Link Layer Discovery Protocol Data Unit	Блок данных LLDP
MIB	Management Information Base	База сведений об управлении
MSTI	Multiple Spanning Tree Instance	Экземпляр (инстанс) множественного связующего дерева
MSTP	Multiple Spanning Tree Protocol	Протокол множественного связующего дерева
NAS	Network Access Server	Сервер сетевого доступа
NetBIOS	Network Basic Input/Output System	Сетевая базовая система Ввода/Вывода
NMS	Network Management Station	Станция управления сетью
NTP	Network Time Protocol	Протокол сетевого времени
OID	Object Identifier	Идентификатор объекта
PCP	Priority Code Point	Код приоритета
PVLAN	Private VLAN	Частная VLAN
QCL	QoS Control List	Список управления QoS
QoS	Quality of Service	Качество обслуживания
RADIUS	Remote Authentication Dial-In User Service	Система аутентификации удаленных пользователей
RMON	Remote Network Monitoring	Дистанционный мониторинг сети
RSTP	Rapid Spanning Tree Protocol	Быстрый протокол связующего дерева
SFTP	Secure File Transfer Protocol	Защищенный протокол передачи файлов на основе SSH
SNMP	Simple Network Management Protocol	Простой протокол сетевого управления
SNTP	Simple Network Time Protocol	Простой протокол синхронизации времени
SP	Strict Priority	Строгий приоритет
SSH	Secure Shell	Протокол защищенной оболочки
SSL	Secure Sockets Layer	Уровень защищенных сокетов, протокол шифрования
SSM	Source Specific Multicast	Многоадресная рассылка для конкретных источников
STP	Spanning Tree Protocol	Протокол связующего дерева
TACACS+	Terminal Access Controller Access Control System	Система контроля доступа контроллера для терминалов
TCP	Transmission Control Protocol	Протокол управления передачей
UDP	User Datagram Protocol	Протокол пользовательских датаграмм
USM	User-Based Security Model	Модель безопасности на основе пользователей
VLAN	Virtual Local Area Network	Виртуальная локальная сеть
WINS	Windows Internet Naming Service	служба Internet имен
WRR	Weighted Round Robin	Взвешенный циклический перебор