Промышленный коммутатор серии SICOM3000A

Руководство по программной части

Версия 1.3

Сайт: https://kyland-rus.ru/

Эл. почта: sales@kyland-rus.ru
support@kyland-rus.ru

KYLAND

Содержание

Предисловие

В этом руководстве в основном представлены методы доступа и функции программного обеспечения промышленного Ethernet-коммутатора SICOM3000A, а также подробно описаны методы настройки через веб-интерфейс.

Структура материала

Руководство пользователя содержит следующий материал:

Основное содержание	**Пояснения**
1. Введение	➢ Обзор ➢ Функции программного обеспечения
2. Доступ к коммутатору	➢ Варианты представления ➢ Доступ к коммутатору через порт консоли ➢ Доступ к коммутатору через Telnet ➢ Доступ к коммутатору через веб-интерфейс
3. Обслуживание	➢ Перезагрузка ➢ Загрузка настроек по умолчанию ➢ Сохранение текущей конфигурации ➢ Выгрузка/загрузка файла конфигурации
4. Основная конфигурация	➢ Информация о системе ➢ Конфигурация системы ➢ Загрузка ЦП ➢ Обновление прошивки (по HTTP, SFTP) ➢ Активация версии прошивки
5. Настройка IP	➢ Настройка IP-адреса ➢ Настройка ARP ➢ Настройка DHCP
6. Система часов	➢ Настройка часов ➢ SNTP ➢ PTP
7. Настройка порта	➢ Настройка состояния порта

	➢ Статистика порта
8. Настройка QoS	➢ Сопоставление приоритетов очередей на основе портов ➢ Сопоставление приоритетов очередей на основе заголовков ➢ Перемаркировка IEEE802.1p ➢ Сопоставление приоритетов очередей на основе DSCP ➢ Повторное сопоставление DSCP ➢ Правило класса DSCP ➢ QCL ➢ Фиксация скорости доступа на основе портов ➢ Фиксация скорости доступа на основе очередей ➢ Планирование очередей на основе портов ➢ Формирование трафика на основе портов ➢ Подавление штормов
9. Безопасность	➢ Управление пользователями ➢ Настройка аутентификации при входе ➢ Настройка SSH ➢ Настройка SSL ➢ Управление доступом ➢ SNMP v1/v2c/v3 ➢ Настройка RMON ➢ Настройка TACACS+ ➢ Настройка RADIUS
10. Сеть	➢ Безопасность порта ➢ Настройка IEEE802.1X ➢ Настройка ACL
11. Агрегация портов	➢ Статическая агрегация ➢ Конфигурация LACP
12. Настройка обнаружения петель Loop Detect	
13. Промышленный протокол	➢ EtherNet/IP

	➢ ModbusTCP ➢ PROFINET
14. Многоадресная рассылка	➢ IGMP Snooping ➢ GMRP ➢ Действие при получении незарегистрированного многоадресного пакета
15. LLDP	
16. Настройка MAC-адреса	
17. VLAN	➢ Настройка VLAN ➢ Настройка PVLAN ➢ GVRP
18. Резервирование	➢ DT-Ring ➢ DRP/DHP ➢ RSTP/STP ➢ MSTP
19. Аварийная сигнализация	➢ Аварийная сигнализация по питанию ➢ Аварийная сигнализация по использованию памяти/ЦП ➢ Аварийная сигнализация по порту ➢ Аварийная сигнализация DT-Ring ➢ Аварийная сигнализация DRP ➢ Аварийная сигнализация по конфликту IP/MAC ➢ Аварийная сигнализация по CRC и потере пакетов ➢ Аварийная сигнализация по скорости порта ➢ Аварийная сигнализация по мощности SFP
20. Проверка канала связи	
21. Журнал	
22. Зеркалирование портов	
23. Диагностика	Ping

Условные обозначения в руководстве

1. Условные обозначения в тексте

Формат	Пояснения
< >	Текст в угловых скобках < > – это название кнопки. Например, щелкните кнопку <Apply>
[ ]	Текст в квадратных скобках [ ] – это название окна или меню. Например, щелкните пункт меню [File]
{ }	Текст в фигурных скобках { } – это сгруппированные элементы. Например, {IP-адрес, MAC-адрес} означает, что IP-адрес и MAC-адрес объединены в группу, и их можно настраивать и отображать совместно
→	Элементы многоуровневых меню разделяются знаком “→”. Например, Start → All Programs → Accessories. Щелкните меню [Start], щелкните подменю [All programs], затем щелкните подменю
/	Выбор одного из двух или нескольких вариантов, разделенных знаком “/”. Например: “Добавление/вычитание” означает добавление или вычитание.
~	Обозначает диапазон. Например, “1~255” означает диапазон от 1 до 255.

2. Условные обозначения в командной строке

Формат	Описание
Полужирный	Команды и ключевые слова, например, **show version**, выделяются **полужирным** шрифтом
Курсив	Парметры, для которых нужно задать значение, выделяются *курсивом*. Например, в команде **show vlan** *vlan-id* нужно задать фактическое значение *vlan-id*

3. Символы

Символ	Пояснения
Предостережение	На эти моменты следует обратить внимание при эксплуатации и настройке, они дополняют описание действий.
Примечание	Необходимые пояснения к описанию действий.
Предупреждение	Требует особого внимания. Некорректные действия могут привести к потере данных или повреждению оборудования

Документация по изделию

Документация к промышленному коммутатору SICOM3000A включает в себя:

Наименование документа	**Содержание**
SICOM3000A Series Industrial Ethernet Switches Hardware Installation Manual (Руководство пользователя по монтажу промышленного коммутатора серии SICOM3000A)	Описана конструкция оборудования, технические характеристики, способы монтажа и демонтажа.
SICOM3000A Industrial Ethernet Switch Web Operation Manual (Руководство пользователя по веб-интерфейсу промышленного коммутатора серии SICOM3000A)	Описаны функции ПО, способы настройки через веб-интерфейс и все функции.

Получение документации

Документацию по изделию можно получить:

- На сайте Kyland: https://kyland-rus.ru/

1 Введение

1.1 Обзор

SICOM3000A – это серия высокопроизводительных управляемых промышленных Ethernet-коммутаторов, применяемых в отрасли железнодорожного транспорта. SICOM3000A соответствует EN50155, EN50121 и другим промышленным стандартам. Коммутатор представляет собой коммутатор уровня 2, который поддерживает протоколы резервирования MSTP, RSTP, DT-Ring, IEC62439-6, гарантируя надежную работу системы. Он также поддерживает функцию цифровой диагностики оптического модуля SFP, что позволяет в реальном времени контролировать мощность приема и передачи оптического трансивера.

1.2 Функции программного обеспечения

SICOM3000A предоставляет обширный набор функций программного обеспечения, удовлетворяющих различные потребности заказчиков.

- Протоколы резервирования: STP/RSTP, MSTP, DT-Ring и DRP.
- Многоадресные протоколы: IGMP Snooping, статическая многоадресная рассылка и GMRP.
- Атрибуты коммутации: VLAN, PVLAN, GVRP, QoS, и ARP.
- Управление пропускной способностью: статическая агрегация портов, LACP, ограничение скорости порта и подавление широковещательных штормов.
- Безопасность: управление пользователями, управление доступом, SSH, SSL, TACACS+, RADIUS, IEEE802.1X и ACL.
- Протоколы синхронизации: SNTP, PTP.
- Управление устройством: обновление программного обеспечения, загрузка/выгрузка файла конфигурации, запись и выгрузка журнала, настройка U-диска.
- Диагностика устройства: зеркалирование портов, LLDP, проверка канала и защита от петель.
- Тревожное оповещение: питание, использование памяти/процессора, порт, кольцо, потеря CRC и Pkt, скорость порта, конфликт IP/MAC-адресов и мощность SFP.

- Управление сетью: командная строка, Telnet, веб-интрефейс и ПО Kyvision, DHCP и SNMP v1/v2c/v3.
- Промышленные протоколы: EtherNet/IP、ModbusTCP、Profinet；
- ……

2 Доступ к коммутатору

Доступ к коммутатору осуществляется через:

- Консольный порт
- Telnet/SSH
- Веб-браузер
- Программное обеспечение Kyvision

Программное обеспечение для управления сетью Kyvision разработано компанией Kyland. Подробная информация содержится в руководстве пользователя.

2.1 Варианты представления

При входе в интерфейс командной строки (CLI) через консольный порт или Telnet можно входить в различные представления или переключаться между представлениями с помощью следующих команд.

Таблица 1 Варианты представления

Приглашение	**Вариант представления**	**Функция**	**Команда для переключения представления**
SWITCH #	Привилегированный режим	Просмотр недавно использованных команд. Просмотр версии программного обеспечения. Просмотр информации об ответе на операцию ping. Выгрузка/загрузка файла конфигурации. Восстановление	Введите “**configure terminal**” для переключения из привилегированного режима в режим настройки. Введите “**exit**” для возврата в общий режим.

SWITCH（config） # 	Режим настройки	Настройка всех функций коммутатора.	Введите "**exit**" или "**end**" для возврата в привилегированный режим.

При настройке коммутатора через интерфейс командной строки для получения справки по командам можно использовать "?". В справочной информации используются различные форматы описания параметров. Например, <1, 255>

означает числовой диапазон; <xx:xx:xx:xx:xx:xx> означает MAC-адрес; <word31> означает диапазон строк 1~31. Кроме того, символы ↑ и ↓ могут использоваться для просмотра недавно использованных команд.

2.2 Доступ к коммутатору через консольный порт

Доступ к коммутатору можно получить через его консольный порт и гипертерминал операционной системы Windows или другое программное обеспечение, поддерживающее подключение через последовательный порт, например, HTT3.3. В следующем примере показано, как использовать HyperTerminal для доступа к коммутатору через консольный порт.

1. Подключите 9-контактный последовательный порт ПК к консольному порту коммутатора с помощью консольного кабеля DB9-RJ45.

2. Запустите HyperTerminal на рабочем столе Windows. Щелкните [Start] → [All Programs] → [Accessories] → [Communications] → [Hyper Terminal], как показано на рисунке 1.

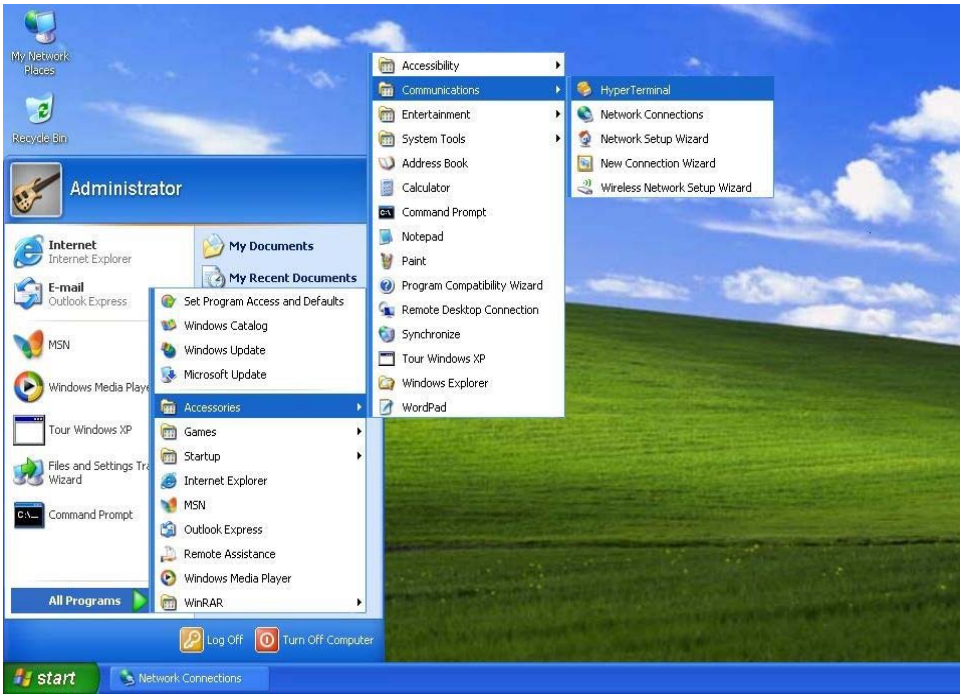


Рисунок 1 Запуск Hyper Terminal

3. Создайте новой подключение "Switch", как показано на рисунке 2.

Рисунок 2 Создание нового подключения

4. Выберите порт для подключения, как показано на рисунке 3.

Рисунок 3 Выбор порта для подключения

Примечание:

Чтобы убедиться, что порт выбран верно, щелкните правой кнопкой [My Computer] и щелкните [Property] →

[Hardware] → [Device Manager] → [Port].

5. Настройте параметры порта (Bits per second: 115200, Data bits: 8, Parity: None, Stop bits: 1, Flow control: None), как показано на рисунке 4.

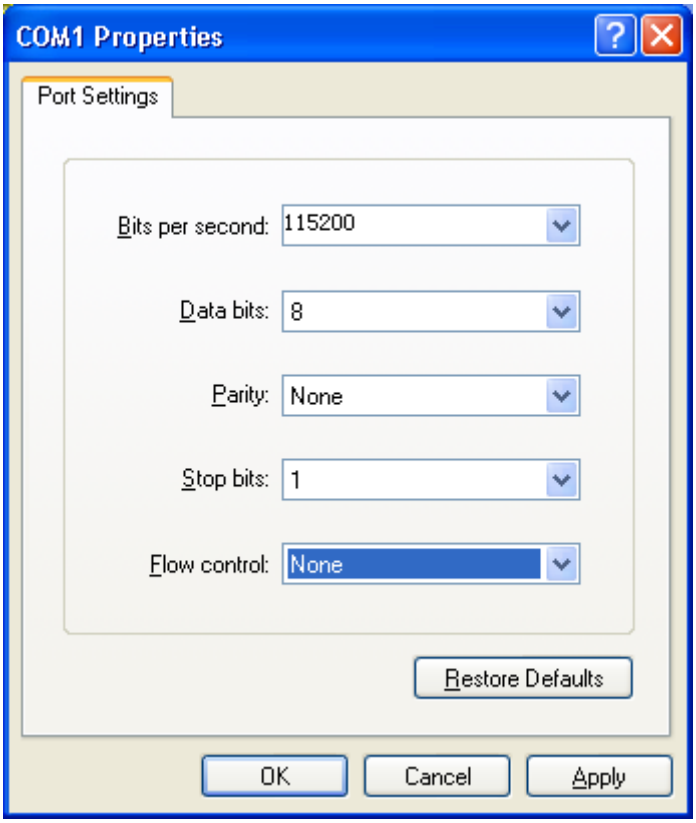


Рисунок 4 Настройка параметров порта

6. Щелкните кнопку <OK>, чтобы войти в интерфейс командной строки коммутатора. Введите имя пользователя по умолчанию "admin" и пароль "123" для входа в привилегированный режим. Можно также ввести другие созданные имя пользователя и пароль, как показано на рисунке 5.

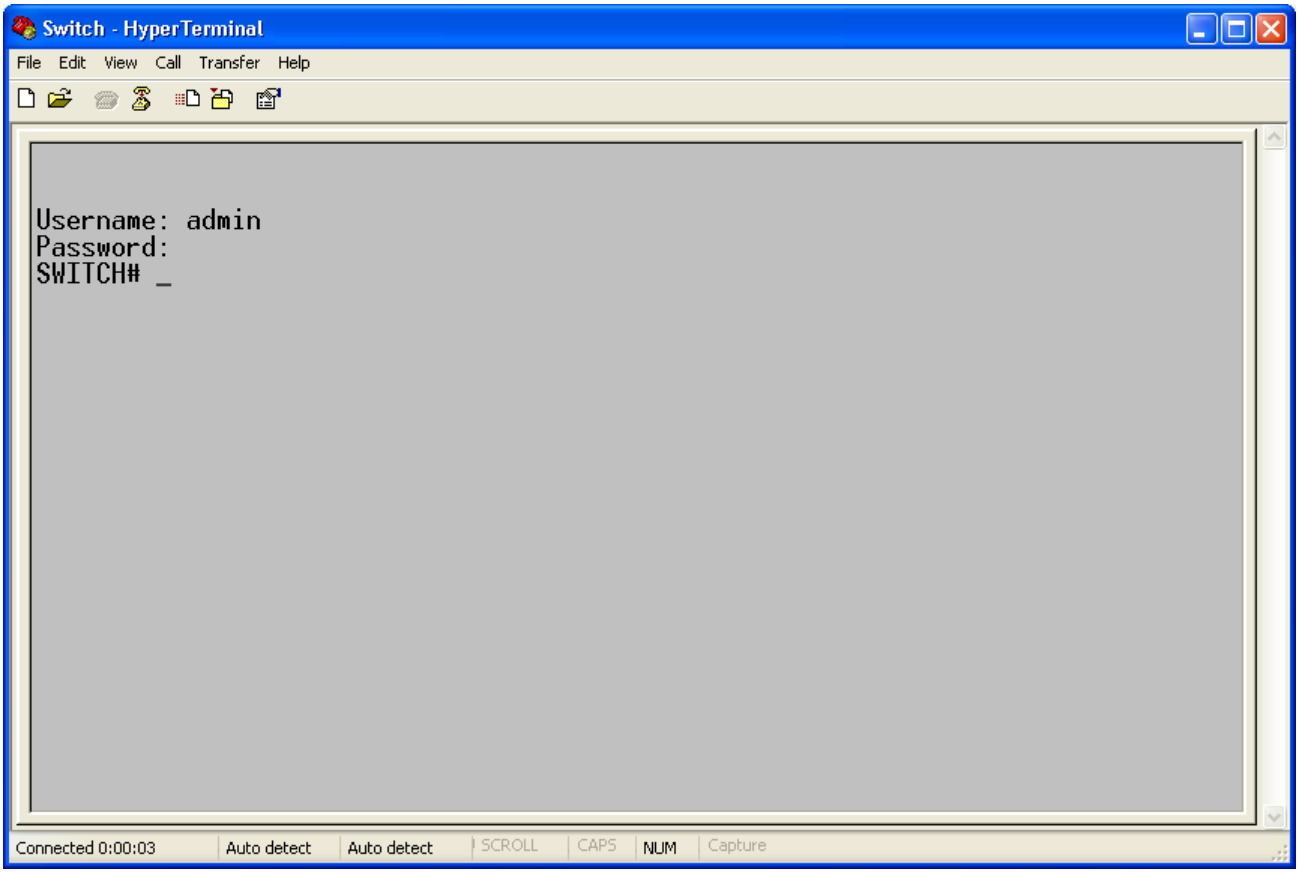


Рисунок 5 Интерфейс командной строки

2.3 Доступ к коммутатору через Telnet

Предварительным условием доступа к коммутатору по протоколу Telnet является нормальная связь между ПК и коммутатором.

1. Введите "**telnet** *IP address*" в диалоговом окне Run, как показано на рисунке 6. IP-адрес коммутатора Kyland по умолчанию 192.168.0.2.

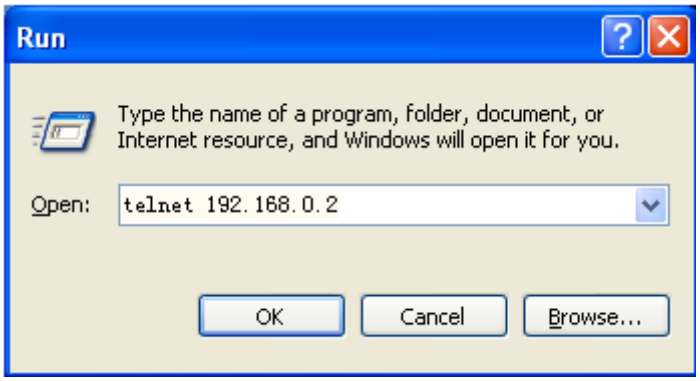


Рисунок 6 Доступ по Telnet

Примечание:

Для подтверждения IP-адреса обратитесь к разделу “5 Настройка IP”, чтобы узнать, как получить IP-адрес.

2. В интерфейсе Telnet введите имя пользователя "admin» и пароль "123" для подключения к коммутатору. Можно также ввести другие созданные имя пользователя и пароль, как показано на рисунке 7.

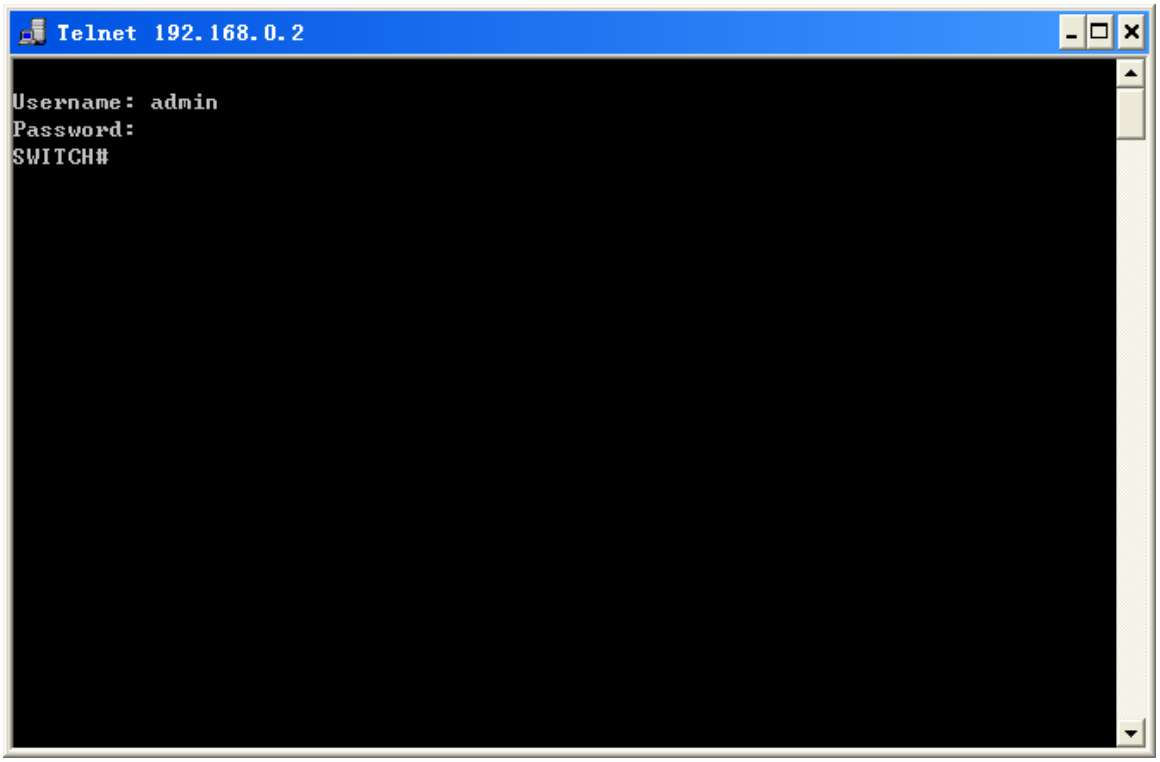


Рисунок 7 Интерфейс Telnet

2.4 Доступ к коммутатору через веб-интерфейс

Предварительным условием доступа к коммутатору через веб-интерфейс является нормальная связь между ПК и коммутатором.

Примечание:

Для наилучшего отображения доступа через веб-интерфейс рекомендуется использовать IE8.0 или более позднюю версию

1. Введите "*IP-адрес*" в адресной строке браузера. Отображается интерфейс для входа, как показано на рисунке 8. Введите имя пользователя по умолчанию "admin", пароль "123» или заданные имя пользователя и пароль. Щелкните <Login>. Можно

также ввести другие созданные имя пользователя и пароль.

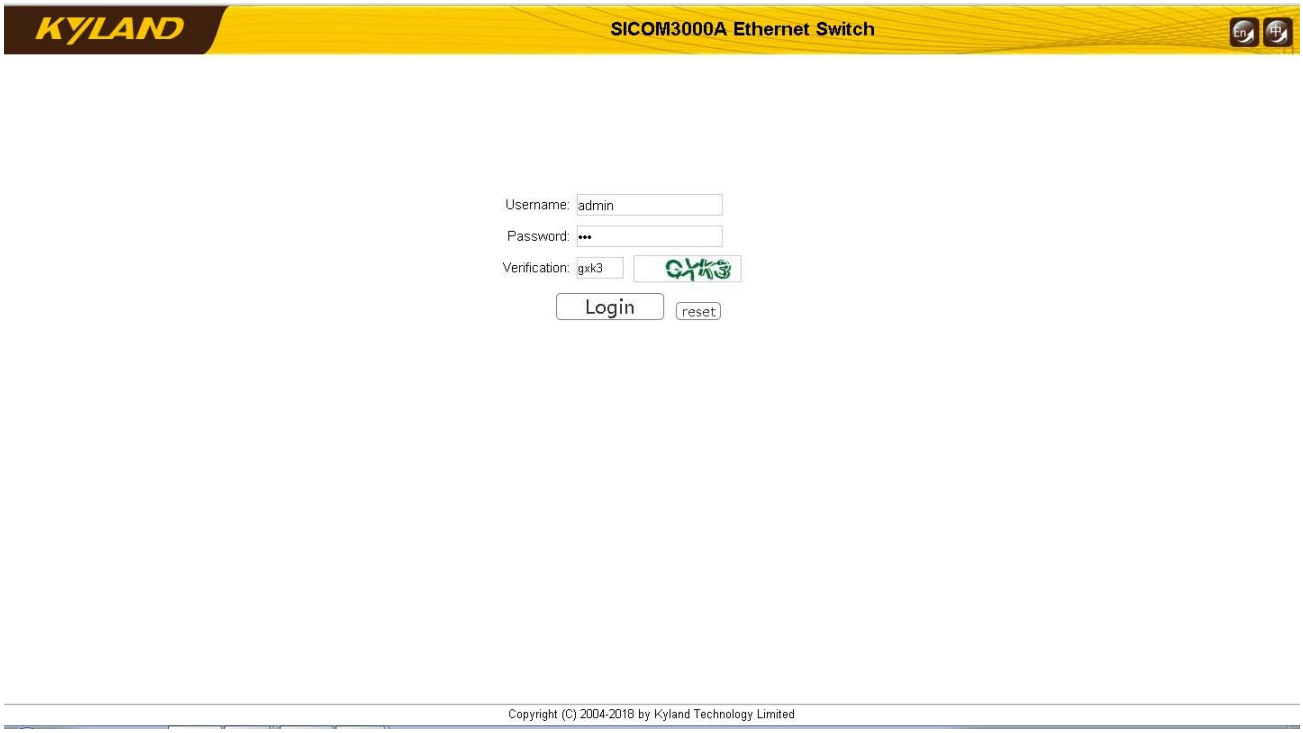


Рисунок 8 Вход через веб-интерфейс

Для переключения на английский или китайский интерфейс можно щелкнуть  или  . По умолчанию отображается английский интерфейс.

Примечание:

Для подтверждения IP-адреса обратитесь к разделу “5 Настройка IP”, чтобы узнать, как получить IP-адрес.

2. После успешного входа слева в окне интерфейса появится дерево навигации, как показано на рисунке 9.

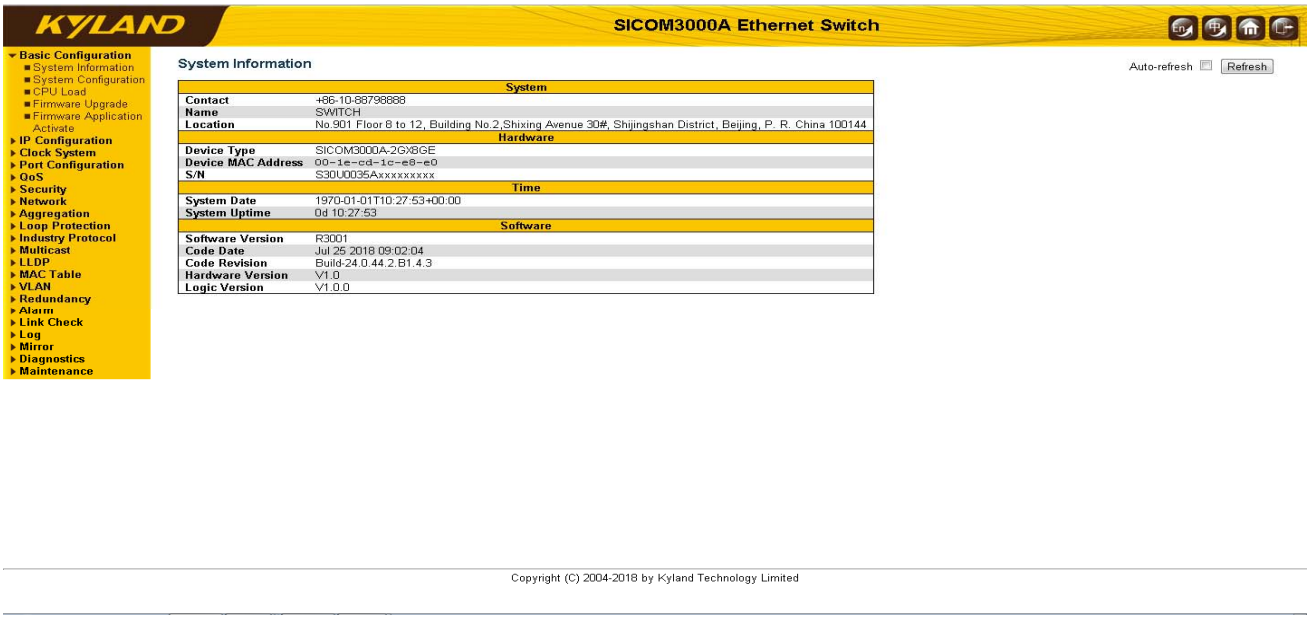


Рисунок 9 Веб-интерфейс

Щелкнув меню в дереве навигации, можно развернуть или свернуть дерево навигации. Можно щелкнуть для перехода в вид, показанный на рисунке 9,

, а для выхода из веб-интерфейса можно щелкнуть .

Как показано на рисунке 10, страница конфигурации/просмотра каждого модуля содержит несколько кнопок управления, и можно щелкнуть кнопку, чтобы выполнить соответствующую операцию на странице. Например, можно щелкнуть <Submit>, чтобы применить текущую конфигурацию, щелкнуть

<Reset>, чтобы отменить текущую конфигурацию и использовать примененную конфигурацию, щелкнуть <Cancel>, чтобы закрыть страницу конфигурации и вернуться на предыдущую страницу конфигурации, или щелкнуть <Refresh>, чтобы обновить информацию на странице. Можно также выбрать «Auto-refresh», чтобы информация обновлялась автоматически с интервалом 4 секунды, или щелкнуть

<Clear>, чтобы сбросить текущую статистику и перезапустить сбор статистики.

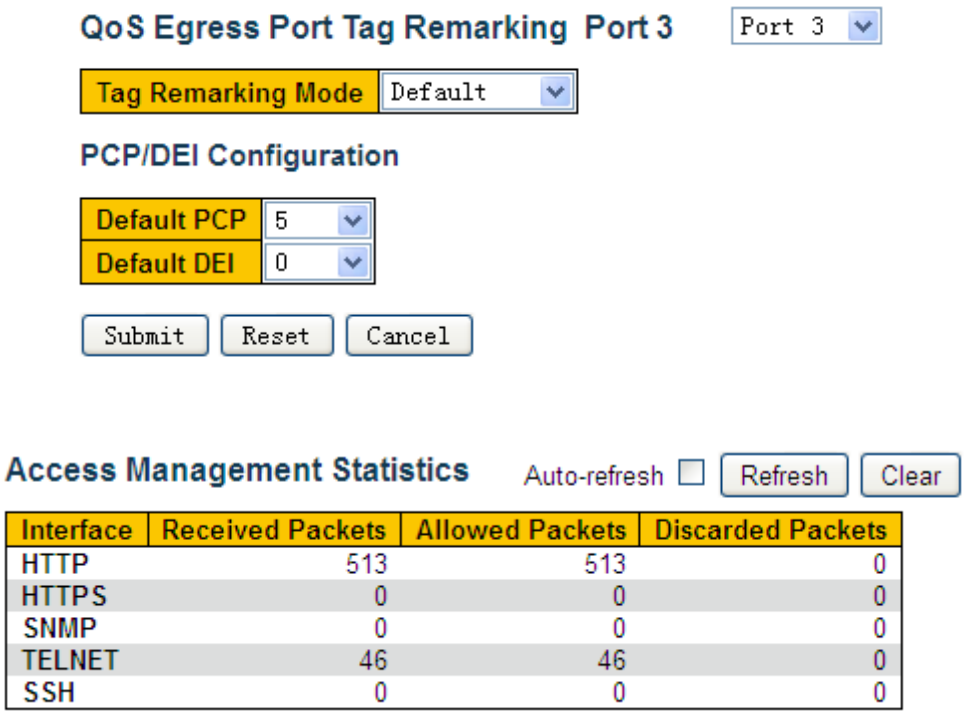


Рисунок 10 Интерфейс конфигурации/статистики

3 Обслуживание

1. Перезагрузите устройство, как показано на рисунке 11.

Рисунок 11 Перезагрузка

Перед перезагрузкой подтвердите сохранение текущей конфигурации. Если выбрать "Yes", после перезагрузки коммутатор запустит текущую конфигурацию. Если выбрать «No", коммутатор запустит последнюю сохраненную конфигурацию. Если сохраненных конфигураций нет, после перезагрузки коммутатор восстановит конфигурацию по умолчанию.

2. Восстановите конфигурацию по умолчанию, как показано на рисунке 12.

Рисунок 12 Восстановление конфигурации по умолчанию

Предупреждение:

После восстановления настроек по умолчанию необходимо перезагрузить устройство, чтобы настройки вступили в силу.

3. Сохраните текущую конфигурацию, как показано на рисунке 13.

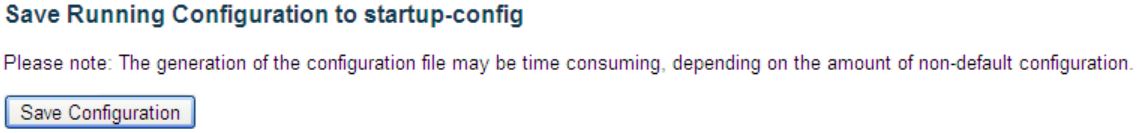


Рисунок 13 Сохранение текущей конфигурации

4. Выгрузите файл с коммутатора на локальный компьютер/сервер, как показано на рисунке 14 и рисунке 15.

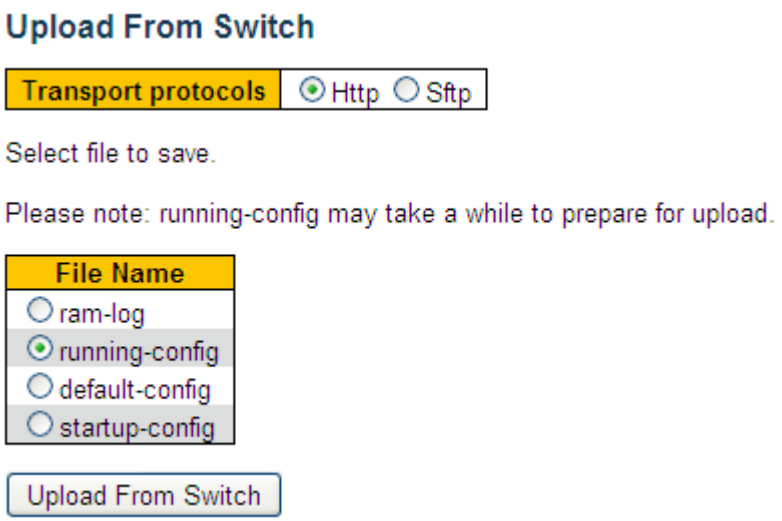


Рисунок 14 Выгрузка файла – HTTP

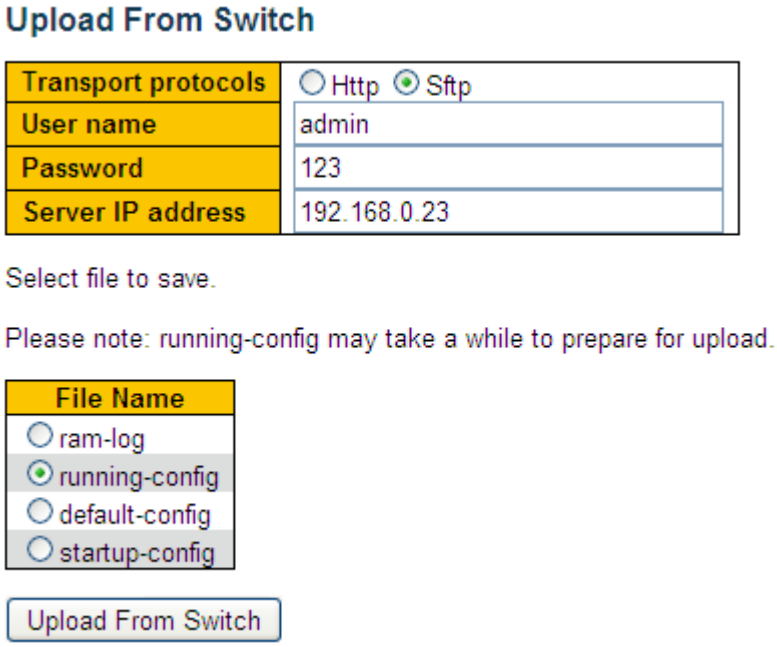


Рисунок 15 Выгрузка файла – SFTP

{User name, Password }

Диапазон: {1~63 символа, 1~63 символа}

Описание: Введите имя пользователя и пароль, созданные на сервере SFTP.

IP-адрес сервера

Формат: A.B.C.D

Описание: Настройте IP-адрес сервера SFTP.

Предупреждение:

- При передаче файлов по SFTP необходимо настроить имя пользователя, пароль и IP-адрес сервера SFTP.
- При передаче файла сервер SFTP должен находиться в рабочем состоянии.

Файл коммутатора можно сохранить на локальном компьютере/сервере. В файле **ram-log** хранится информация журнала, **running-config –** это файл текущей конфигурации коммутатора, **default-config** – файл конфигурации по умолчанию, а **startup-config** – файл запуска коммутатора. Выберите файл и щелкните <Upload From Switch>, чтобы сохранить файл на локальном компьютере/сервере.

5. Загрузите файл конфигурации с локального компьютера/сервера в качестве нового файла запуска коммутатора, как показано на рисунке 16 и рисунке 17.

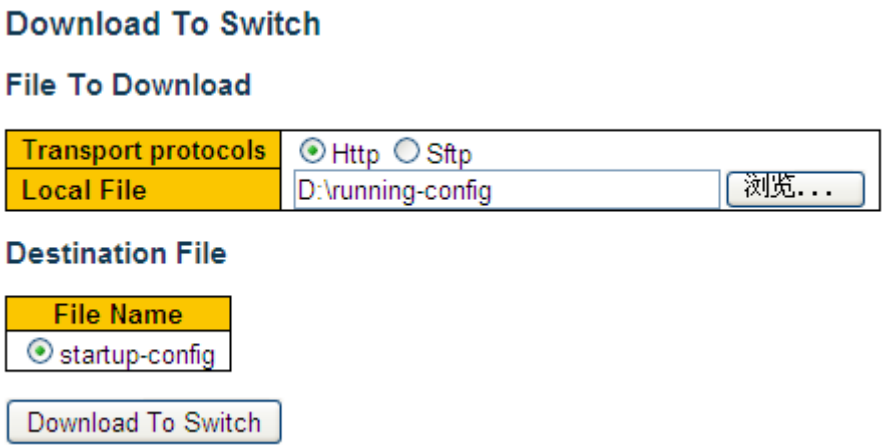


Рисунок 16 Загрузка файла конфигурации – HTTP

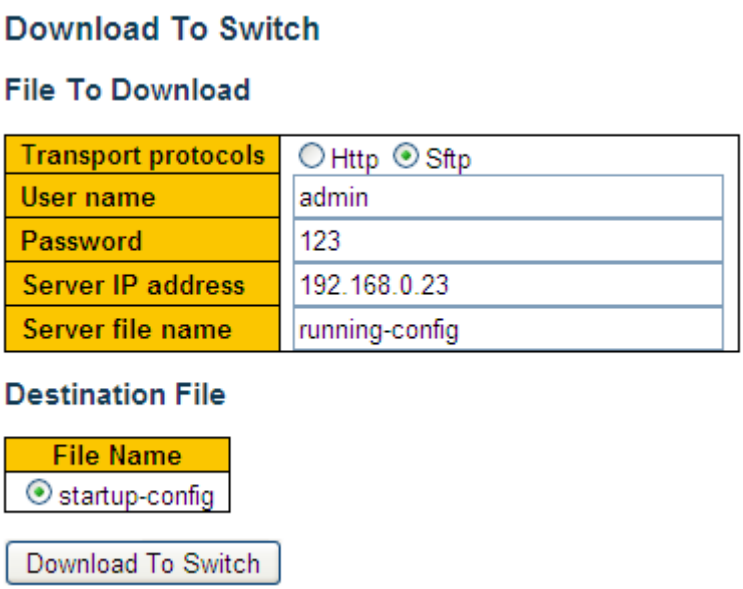


Рисунок 17 Загрузка файла конфигурации – SFTP

Локальный файл

Функция Выбор файла конфигурации, сохраненного локально.

{User name, Password }

Диапазон: {1~63 символа, 1~63 символа}

Описание: Введите имя пользователя и пароль, созданные на сервере SFTP.

IP-адрес сервера

Формат: A.B.C.D

Описание: Настройте IP-адрес сервера SFTP.

Имя файла на сервере

Диапазон: 1~63 символа

Описание: Укажите имя сохраненного на сервере SFTP файла конфигурации.

Предупреждение:

- При передаче файлов по SFTP необходимо настроить имя пользователя, пароль и IP-адрес сервера SFTP.
- При передаче файла сервер SFTP должен находиться в рабочем состоянии.

Можно загрузить в коммутатор файл конфигурации с локального компьютера/сервера в качестве нового файла запуска. Новый файл заменит исходный файл **startup-config**. Щелкните <Download

To Switch>, чтобы загрузить в коммутатор файл конфигурации с локального компьютера/сервера.

6. Настройка через USB

Загружайте и выгружайте файлы конфигурации, используя USB-накопитель, как показано на рисунке 18

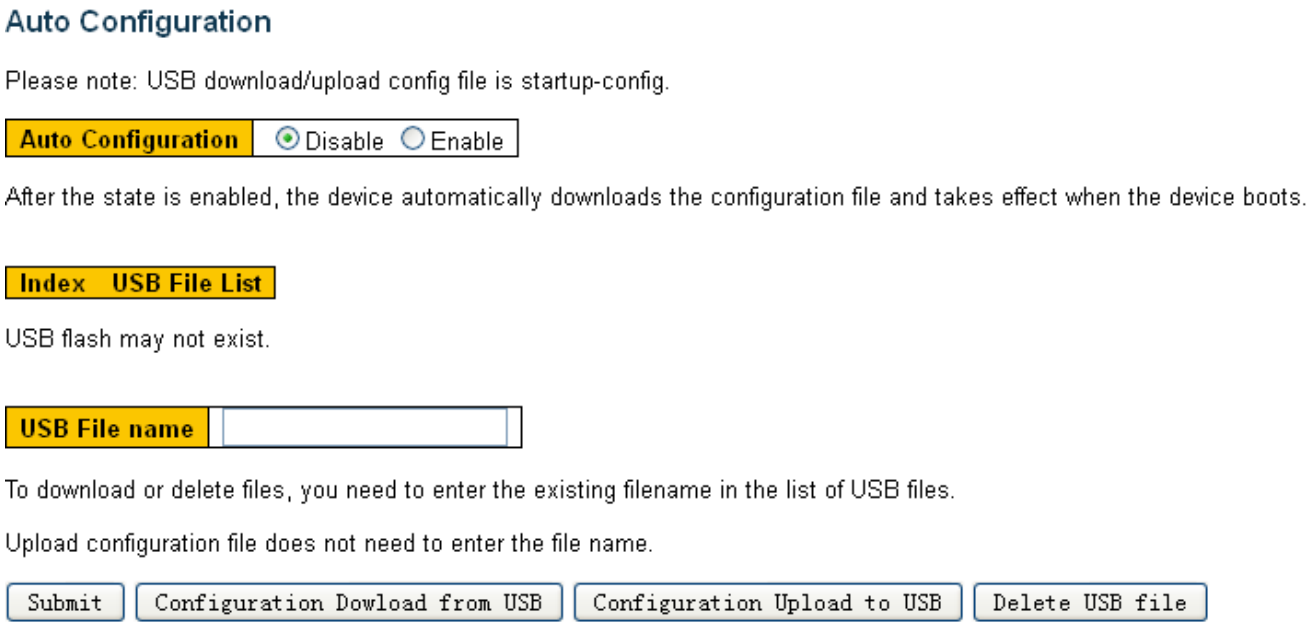


Рисунок 18 Настройка через USB

Automatic configuration: enable / disable

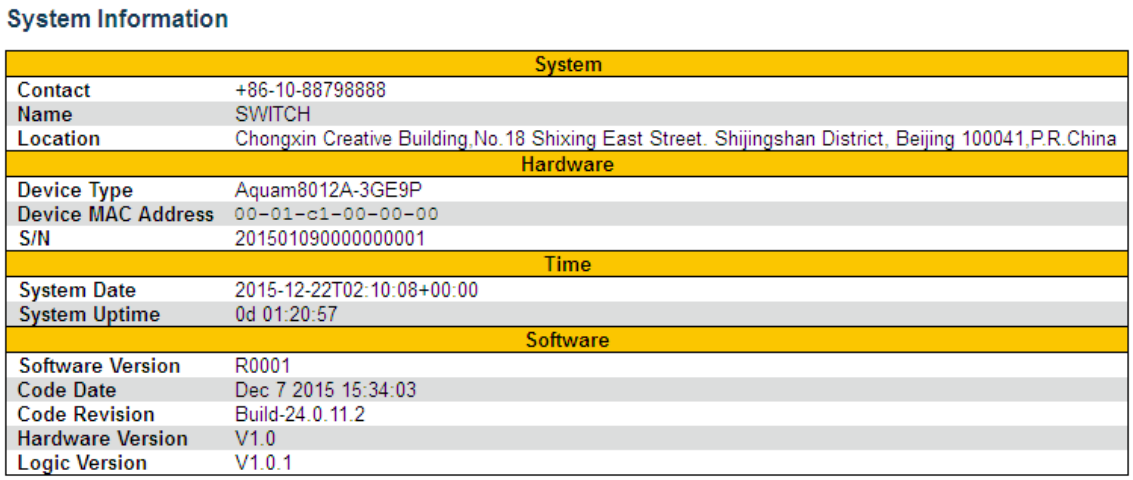
Описание: Если автоматическое конфигурирование включено, устройство автоматически загрузит файл конфигурации с USB-накопителя и применит его при запуске устройства.

Имя файла на USB-накопителе: Чтобы загрузить или удалить файл конфигурации, необходимо ввести имя файла, присутствующего в списке файлов на USB-накопителе. При выгрузке файла конфигурации нет необходимости вводить имя файла.

4 Основная конфигурация

4.1 Информация о системе

Информация о системе включает в себя контактные данные, имя системы, тип устройства, MAC-адрес, серийный номер, системное время и информацию о версии, как показано на рисунке 19.



System Information

System	
Contact	+86-10-88798888
Name	SWITCH
Location	Chongxin Creative Building,No.18 Shixing East Street. Shijingshan District, Beijing 100041,P.R.China
Hardware	
Device Type	Aquam8012A-3GE9P
Device MAC Address	00-01-c1-00-00-00
S/N	201501090000000001
Time	
System Date	2015-12-22T02:10:08+00:00
System Uptime	0d 01:20:57
Software	
Software Version	R0001
Code Date	Dec 7 2015 15:34:03
Code Revision	Build-24.0.11.2
Hardware Version	V1.0
Logic Version	V1.0.1

Рисунок 19 Информация о системе

4.2 Конфигурация системы

Конфигурация системы включает в себя контактные данные, имя системы и конфигурацию местоположения, как показано на рисунке 20.

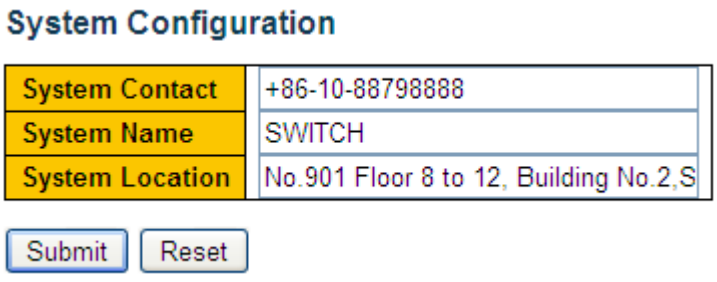


Рисунок 20 Конфигурация системы

Контактные данные

Диапазон: 0~255 символов (символы ASCII с 32 по 126)

Имя системы

Диапазон: 0~255 символов (буквы A~Z / a~z, цифры 0~9, знак минус sign -. Первый

символ должен быть буквой, а первый или последний символ не должен быть знаком минус.

Местоположение системы

Диапазон: 0~255 символов (символы ASCII с 32 по 126)

4.3 Загрузка ЦП

Загрузка измеряется как усредненная за последние 100 мс, 1 с и 10 с, как показано на рисунке 21.

CPU Load

Running Time	CPU Load
100ms	2%
1sec	0%
10sec	4%

Рисунок 21 Загрузка ЦП

4.4 Обновление прошивки

Обновление прошивки может помочь улучшить производительность коммутатора. Для коммутаторов этой серии обновление прошивки включает обновление версии загрузчика и обновление версии системного программного обеспечения. Версия загрузчика должна быть обновлена до обновления версии системного программного обеспечения. Если версия загрузчика не меняется, можно обновить только версию системного ПО. Для обновления прошивки необходимо использовать HTTP/SFTP.

4.4.1 Обновление прошивки по HTTP

1. Обновите прошивку, как показано на рисунке 22.

Firmware Upgrade

Transport protocols	(•) Http ( ) Sftp
Upgrade Target	(•) Application ( ) Bootloader
Upgrade Mode	(•) First ( ) Second ( ) All
Local File	D:\工作\工作\新建文件夹\SICOM300 浏览...

Submit

Рисунок 22 Обновление прошивки – HTTP

Цель обновления

Варианты: Приложение/загрузчик

Функция Выбор цели обновления.

Режим обновления

Варианты: Первый/второй/все

Описание: В коммутатор можно загрузить две версии ПО, одинаковые или разные. All означает версию 1 и версию 2

Локальный файл

Функция Выбор файла версии, сохраненного локально.

2. Когда обновление будет завершено, как показано на рисунке 23, активируйте версию программного обеспечения и перезагрузите устройство, откройте страницу информации о системе, чтобы проверить, успешно ли выполнено обновление и активна ли новая версия.

Рисунок 23 Обновление выполнено успешно

Внимание:

- По завершении обновления активируйте версию программного обеспечения и перезагрузите устройство, чтобы новая версия вступила в силу.
- Если обновление не удалось, не перезагружайте устройство, чтобы избежать потери файла программного обеспечения и запуска с ошибкой.

4.4.2 Обновление прошивки по SFTP

Протокол безопасной передачи файлов (SFTP) — это протокол передачи файлов на основе SSH. Он обеспечивает зашифрованную передачу файлов для гарантии безопасности.

В следующем примере MSFTP используется для описания конфигурации сервера

SFTP и процесса обновления прошивки.

1. Добавьте пользователя SFTP, как показано на рисунке 24. Введите пользователя и пароль, например, admin и 123. Установите номер порта 22. Введите путь для сохранения файла версии прошивки в поле Root path. Щелкните кнопку <Start>.

Рисунок 24 Добавление пользователя SFTP

2. Обновите прошивку, как показано на рисунке 25.

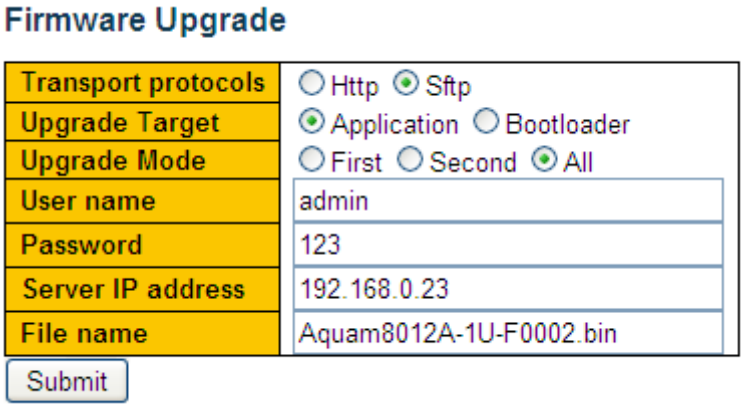


Рисунок 25 Обновление прошивки – SFTP

Цель обновления

Варианты: Приложение/загрузчик

Функция: Выбор цели обновления.

Режим обновления

Варианты: Первый/второй/все

Описание: В коммутатор можно загрузить две версии ПО, одинаковые или разные. All означает версию 1 и версию 2

{User name, Password }

Диапазон: {1~63 символа, 1~63 символа}

Описание: Введите имя пользователя и пароль, созданные на сервере SFTP.

IP-адрес сервера

Формат: A.B.C.D

Описание: Настройте IP-адрес сервера SFTP.

Имя файла

Диапазон: 1~63 символа

Описание: Укажите имя сохраненного на сервере SFTP файла прошивки.

Внимание:

Имя файла должно содержать расширение. В противном случае обновление может пройти неудачно.

3. Когда обновление будет завершено, как показано на рисунке 26, активируйте версию программного обеспечения и перезагрузите устройство, откройте страницу информации о системе, чтобы проверить, успешно ли выполнено обновление и активна ли новая версия.

Рисунок 26 Обновление выполнено успешно

Внимание:

- При обновлении прошивки сервер SFTP должен находиться в рабочем состоянии.
- По завершении обновления перезагрузите устройство для активации новой версии.
- Если обновление не удалось, не перезагружайте устройство, чтобы избежать потери файла программного обеспечения и запуска с ошибкой.

4.5 Активация версии прошивки

Активируйте версию прошивки, как показано на рисунке 27.

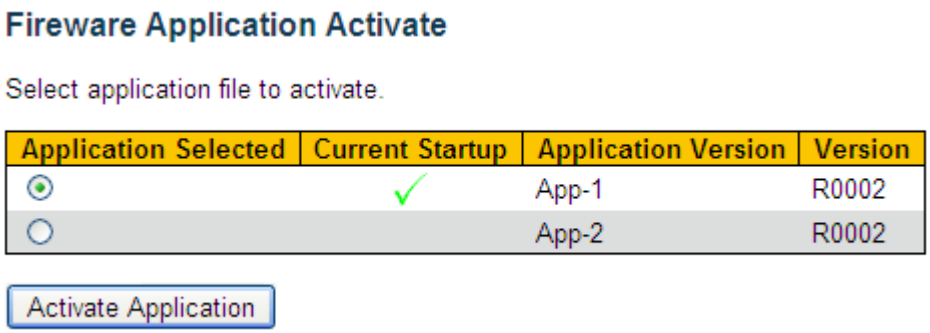


Рисунок 27 Активация версии прошивки

Выберите одну из версий и нажмите кнопку <Activate Application>, настроив версию, которая будет активной, то есть запустится при следующем запуске. Активной может быть только одна версия.

В поле Current Startup показана запущенная версия.

5 Настройка IP

5.1 Настройка IP-адреса

1. Просмотр IP-адреса коммутатора через порт консоли.

Войдите в интерфейс командной строки через порт консоли. Выполните команду "**show interface vlan 1**" в привилегированном режиме, чтобы увидеть IP-адрес коммутатор, как показано в красном круге на рисунке 28.

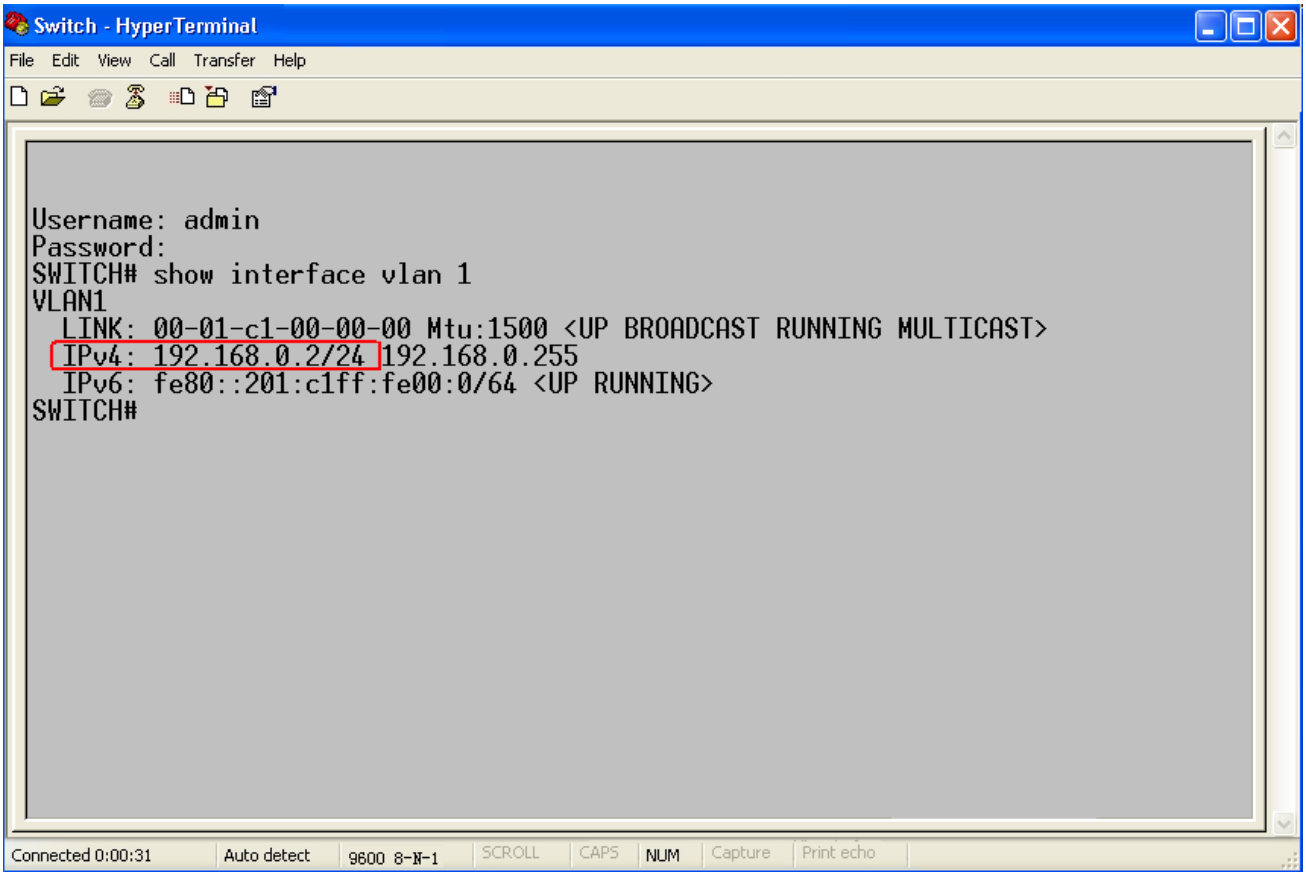


Рисунок 28 Отображение IP-адреса

2. Создание интерфейса IP.

Хосты в разных VLAN не могут связываться друг с другом. Их коммуникационные пакеты должны пересылаться маршрутизатором или коммутатором уровня 3 через IP-интерфейс. Коммутаторы данной серии поддерживают IP-интерфейсы, которые представляют собой виртуальные интерфейсы уровня 3, используемые для связи между VLAN. Для каждой VLAN можно создать один IP-интерфейс. Интерфейс используется для пересылки пакетов уровня 3 в VLAN.

3. Настройка IP-адреса

IP-адрес коммутатора можно настроить вручную или получить автоматически, как показано на рисунке 29.

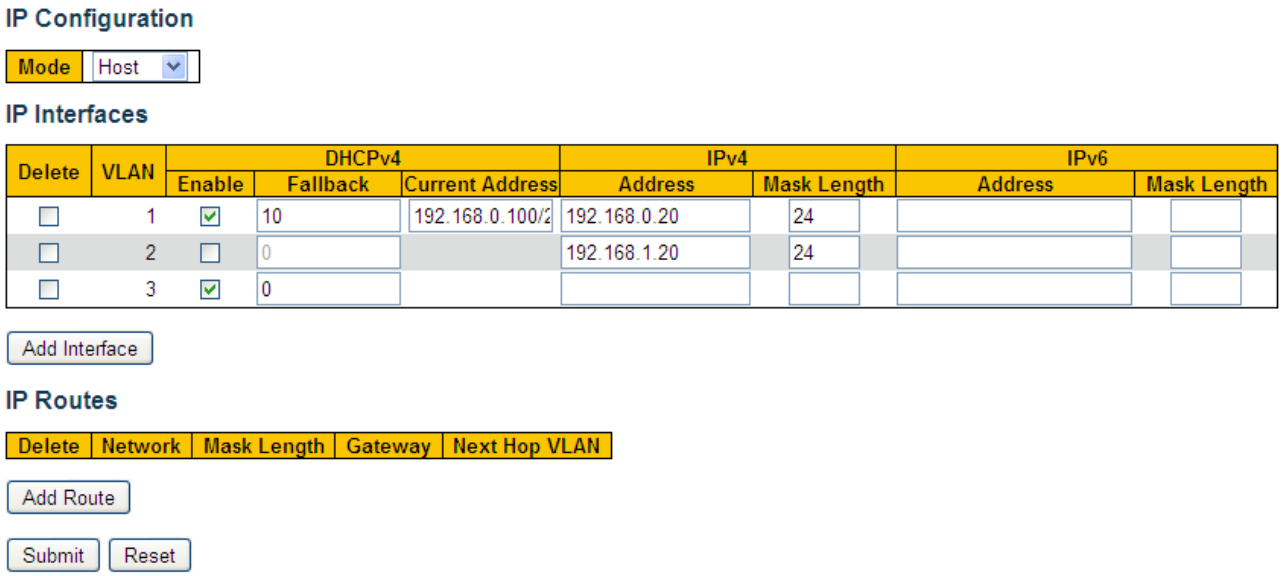


Рисунок 29 Настройка IP-адреса

VLAN

Функция Настройка атрибуте VLAN IP-интерфейса. Только порты этой VLAN получат доступ к IP-интерфейсу.

DHCPv4-Enable

Варианты: Enable/Disable

Функция Отключение DHCPv4, настройка IP-адреса и маски вручную; включение DHCPv4, коммутатор (как клиент DHCP) автоматически получает IP-адрес через DHCP. В сети должен быть DHCP-сервер для назначения клиентам IP-адресов и масок.

DHCPv4-Fallback

Диапазон: 0~4294967295s

Функция Если значение не равно нулю, коммутатор получает время для попытки получения IP-адреса по протоколу динамической конфигурации хоста (DHCP). В этом случае необходимо настроить IP-адрес вручную. По истечении времени попытки IP-адрес, настроенный вручную, вступает в силу. Если значение равно 0, коммутатор неоднократно пытается получить IP-адрес, пока не получит IP-адрес через DHCP. В этом случае нет необходимости настраивать IP-адрес вручную.

DHCPv4-Current Address

Функция Отображение IP-адреса и длины маски, автоматически получаемых от сервера DHCP. Если коммутатору не удается получить IP-адрес через DHCP в течение времени, отведенного на попытку, IP-адрес и длина маски, настроенные вручную, отображаются в поле **Current Address**.

IPv4-Address

Формат: A.B.C.D

Функция Задание IP-адреса вручную.

IPv4-Mask Length

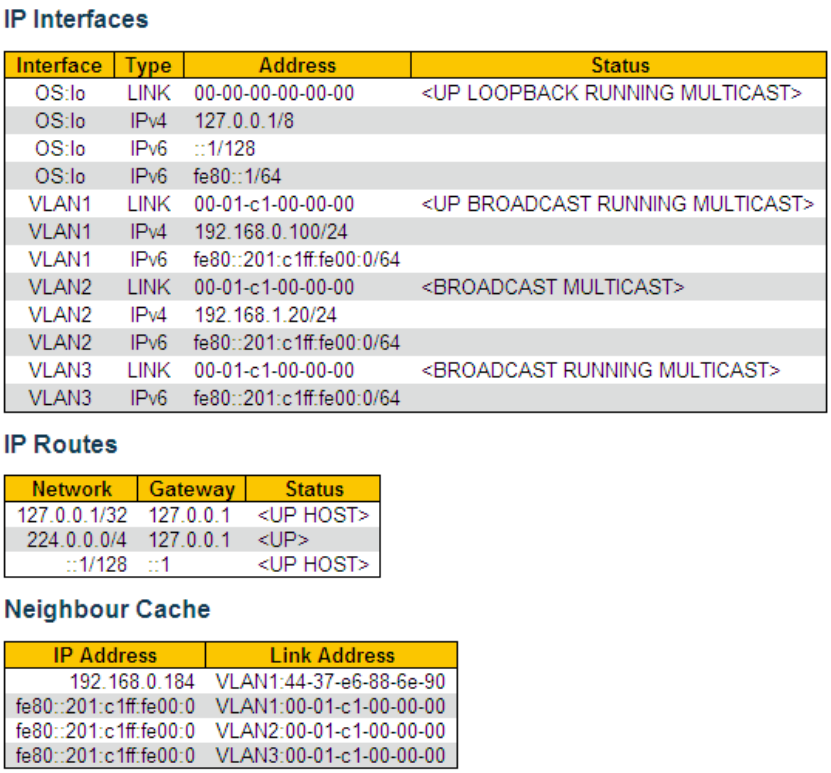
Функция Маска подсети представляет собой число длиной 32 бита, состоящее из строки 1 и строки 0. 1 соответствует полям номера сети и полям номера подсети, а 0 соответствует полям номера хоста. Длина маски — это количество 1 в маске подсети.

Щелкните <Add Interface>, чтобы добавить новый IP-интерфейс; поддерживается не более 8 интерфейсов.

Предупреждение:

- Каждый IP-интерфейс поддерживает один IP-адрес.
- IP-адреса разных сегментов сети должны быть настроены для разных IP-интерфейсов.

4. Просмотрите IP-интерфейсы, как показано на рисунке 30.



IP Interfaces

Interface	Type	Address	Status
OS:lo	LINK	00-00-00-00-00-00	<UP LOOPBACK RUNNING MULTICAST>
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	::1/128	
OS:lo	IPv6	fe80::1/64	
VLAN1	LINK	00-01-c1-00-00-00	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.0.100/24	
VLAN1	IPv6	fe80::201:c1ff:fe00:0/64	
VLAN2	LINK	00-01-c1-00-00-00	<BROADCAST MULTICAST>
VLAN2	IPv4	192.168.1.20/24	
VLAN2	IPv6	fe80::201:c1ff:fe00:0/64	
VLAN3	LINK	00-01-c1-00-00-00	<BROADCAST RUNNING MULTICAST>
VLAN3	IPv6	fe80::201:c1ff:fe00:0/64	

IP Routes

Network	Gateway	Status
127.0.0.1/32	127.0.0.1	<UP HOST>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

Neighbour Cache

IP Address	Link Address
192.168.0.184	VLAN1:44-37-e6-88-6e-90
fe80::201:c1ff:fe00:0	VLAN1:00-01-c1-00-00-00
fe80::201:c1ff:fe00:0	VLAN2:00-01-c1-00-00-00
fe80::201:c1ff:fe00:0	VLAN3:00-01-c1-00-00-00

Рисунок 30 Просмотр IP-интерфейсов

5.2 ARP

5.2.1 Введение

Протокол разрешения адресов (ARP) разрешает сопоставление между IP-адресами и MAC-адресами с помощью механизма запроса и ответа адреса. Коммутатор получает информацию о сопоставлении 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 реальными 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.

5.2.2 Настройка через веб-интерфейс

1. Настройте время старения ARP, как показано на рисунке 31.

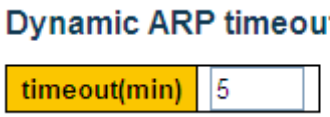


Рисунок 31 Настройка времени старения

timeout

Диапазон: 0 ~ 60 минут

По умолчанию: 5 минут

Функция Настройка времени старения ARP, если время старения установлено на 0, старение запрещено. Описание: Время старения ARP — это промежуток с момента добавления динамической записи ARP в таблицу до момента удаления записи из таблицы.

2. Добавьте статическую запись ARP, как показано на рисунке 32.

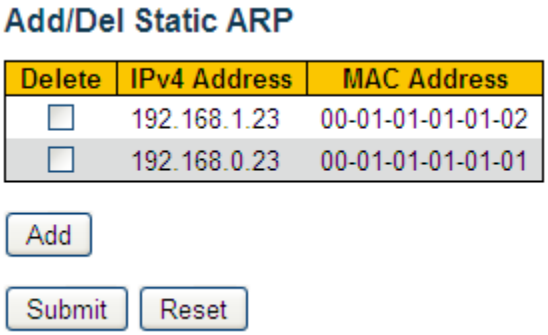


Рисунок 32 Добавление статической записи ARP

ARP

Группа: {IP address, MAC address}

Формат: {A.B.C.D, HHHHHHHHHHHH} (H – шестнадцатеричное число.)

Функция Настройка статической записи ARP.

Предупреждение:

Как правило, коммутатор автоматически запоминает записи ARP. Настройка вручную не требуется.

Щелкните <Add>, чтобы добавить новую статическую запись ARP; поддерживается не более 128 статических записей ARP.

5.3 Настройка DHCP

С непрерывным расширением масштаба и ростом сложности сети, в условиях частого перемещения компьютеров (таких как ноутбуки или беспроводная сеть) и числа компьютеров, превышающего выделяемые IP-адреса, протокол BootP, специально предназначенный для статической конфигурации хоста, оказывается неспособным 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. Для решения этих проблем был введен DHCP (протокол динамической конфигурации хоста).

DHCP использует модель взаимодействия клиент-сервер. Клиент отправляет запрос конфигурации на сервер, а затем сервер отправляет параметры конфигурации, такие как IP-адрес, клиенту, достигая динамической конфигурации IP-адресов. Структура типичного использования DHCP показана на рисунке 33.

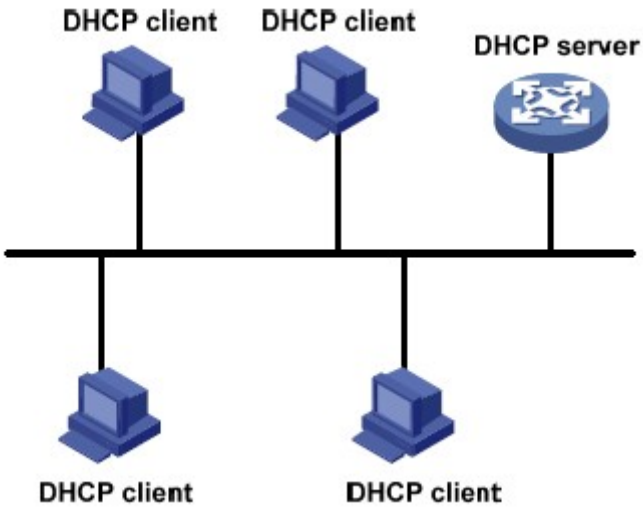


Рисунок 33 Типичное использование DHCP

Предупреждение:

В процессе динамического получения IP-адресов сообщения рассылаются путем 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 DHCP Relay, чтобы получить IP-адреса и 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 привязанные IP-адреса клиентам по DHCP. При статическом распределении адреса закрепляются постоянно.

Динамическое распределение: Сервер DHCP 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 запросить IP-адрес. Сетевой администратор может выбрать механизм распределения DHCP для каждого клиента.

5.3.1 Настройка сервера DHCP

5.3.1.1 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. DHCP-сервер обычно используется для выделения IP-адресов в следующих случаях.

- Большой масштаб сети. Трудоемкость ручной настройки велика, и трудно управлять всей сетью.
- Количество хостов превышает количество назначаемых IP-адресов, и нет возможности выделить фиксированный IP-адрес каждому хосту.
- Лишь несколько хостов в сети нуждаются в фиксированных IP-адресах.

5.3.1.2 Пул адресов HCP

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

1. IP-адрес статически привязан к MAC-адресу клиента.
2. Записанный на DHCP-сервере IP-адрес, который когда-либо был выделен клиенту.
3. IP-адрес, указанный в сообщении запроса, отправленном от клиента.
4. Первый доступный IP-адрес, найденный в пуле адресов.

5. Если нет доступного IP адреса, проверяется IP адрес, срок действия которого истекает, и у которого были конфликты в процессе использования. Если такой IP адрес найден, он присваивается клиенту. Если нет, то ничего не происходит.

5.3.1.3 Настройка через веб-интерфейс

1. Запустите сервер DHCP, как показано на рисунке 34.

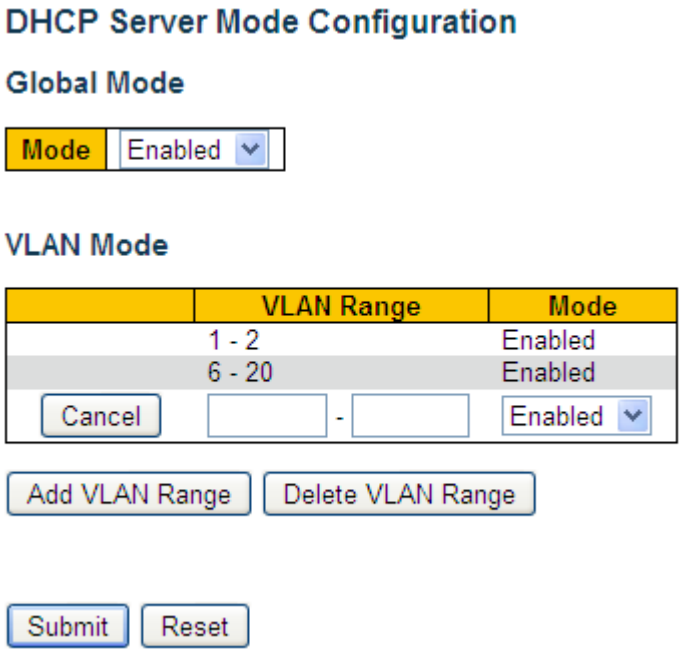


Рисунок 34 Запуск сервера DHCP

Режим Global Mode

Варианты: Включен/выключен

По умолчанию: Выключен

Функция Выбор текущего коммутатора как сервера DHCP, чтобы выделить или не выделять IP-адрес клиенту.

{VLAN Range, Mode}

Диапазон: {1~4095, Disabled/Enabled}

Функция Если для VLAN клиента, подающего заявку на получение IP-адреса, установлено значение Enabled, DHCP-сервер выделяет клиенту IP-адрес. В противном случае DHCP-сервер не выделяет клиенту IP-адрес.

2. Создайте пул адресов DHCP, как показано на рисунке 35.

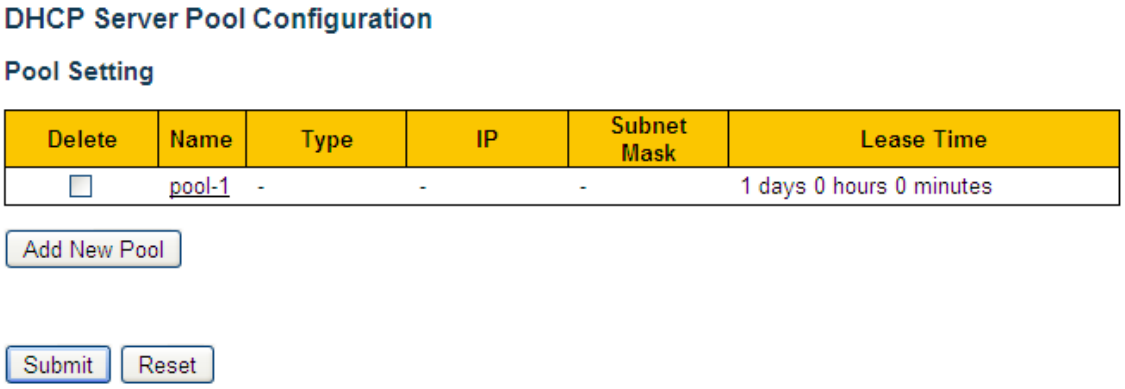


Рисунок 35 Создание пула адресов DHCP

Name

Диапазон: 1~32 символа

Функция: задание имени пула IP-адресов.

Щелкните <Add New Pool>, чтобы создать новый пул адресов DHCP.

3. Настройте пул адресов DHCP. Щелкните <Name> (см. Figure 35), чтобы настроить пул адресов DHCP, как показано на рисунке 36.

DHCP Pool Configuration

Pool

Name	pool-1

Setting

Pool Name	pool-1	
Type	Host	
IP	192.168.0.6	
Subnet Mask	255.255.255.0	
Lease Time	1	days (0-365)
	0	hours (0-23)
	0	minutes (0-59)
Domain Name	domain.com	
Broadcast Address		
Default Router	192.168.0.201	
	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
DNS Server	192.168.0.202	
	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
NTP Server	192.168.0.203	
	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
NetBIOS Node Type	None	
NetBIOS Scope		
NetBIOS Name Server	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
NIS Domain Name		
NIS Server	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
Client Identifier	MAC	
	00-11-22-33-44-55	
Hardware Address	00-11-22-33-44-55	
Client Name		
Vendor 1 Class Identifier		
Vendor 1 Specific Information		
Vendor 2 Class Identifier		
Vendor 2 Specific Information		
Vendor 3 Class Identifier		
Vendor 3 Specific Information		
Vendor 4 Class Identifier		
Vendor 4 Specific Information		

Save Reset

Рисунок 36 Настройка пула IP-адресов

Name

Функция: Выбор созданного имени пула.

Type

Варианты: None/Network/Host

По умолчанию: None

Функция Настройка типа пула адресов. Network: коммутатор динамически выделяет IP-адреса нескольким DHCP-клиентам. Host: коммутатор поддерживает статическое выделение IP-адресов специальным DHCP-клиентам.

{IP，Subnet Mask}

Функция Network означает, что можно настроить 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. Значение обычно настроено как 255.255.255.0.

Host указывает, что можно настроить статически привязанный IP-адрес клиента. Назначение статического IP-адреса 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.

Lease Time

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

По умолчанию: 1 день 0 часов 0 минут

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

Domain Name

Диапазон: 1~36 символов

Функция Функция: задание доменного имени пула IP-адресов. При выделении IP-адреса клиенту ему также отправляется суффикс доменного имени.

Broadcast Address

Формат: A.B.C.D

Функция Настройка широковещательного адреса клиента, выделенного DHCP-сервером.

Default Routing

Формат: A.B.C.D

Функция Настройка адреса клиентского шлюза, выделенного DHCP-сервером.

Пояснение: когда DHCP-клиент посещает хост, находящийся в другом сегменте, данные должны пересылаться через шлюзы. Когда DHCP-сервер выделяет клиентам IP-адреса, он может одновременно указывать адреса шлюза. Для пула адресов DHCP можно настроить не более 4 шлюзов.

DNS Server

Формат: A.B.C.D

Функция Настройка адреса сервера DNS, выделенного DHCP-сервером.

Пояснение: При посещении сетевого хоста через доменное имя доменное имя должно быть преобразовано в IP-адрес. Это реализуется DNS (системой доменных имен). Для того, чтобы DHCP-клиент мог посещать сетевой хост через доменное имя, при выделении IP-адресов клиентам DHCP-сервер может одновременно указывать IP-адреса серверов доменных имен. Для пула адресов DHCP можно настроить не более 4 серверов DNS.

NTP Server

Формат: A.B.C.D

Функция Настройка адреса сервера NTP, выделенного DHCP-сервером.

NetBIOS Node Type

Варианты: None/B-node/P-node/M-node/H-node

По умолчанию: None

Функция Настройка типа узла NetBIOS, выделенного DHCP-сервером. Когда DHCP-клиент использует протокол NetBIOS для связи в сети, необходимо установить соответствие между именем хоста и IP-адресом. Различные типы узлов получают сопоставление в разных режимах.

Описание: B-узел получает сопоставление посредством широковещательной рассылки. P-узел получает сопоставление путем отправки одноадресного пакета для связи с WINS-сервером. M-узел получает сопоставление, отправив

широковещательный пакет в первый раз. Если M-узел не может получить сопоставление в первый раз, он получает сопоставление, отправив одноадресный пакет для связи с WINS-сервером во второй раз. H-узел получает сопоставление, отправляя одноадресный пакет для связи с WINS-сервером в первый раз. Если H-узел не может получить сопоставление в первый раз, он получает сопоставление, отправив широковещательный пакет во второй раз.

NetBIOS Scope

Диапазон: 1~36 символов

Функция: Настройка имени NetBIOS.

NetBIOS Name Server

Формат: A.B.C.D

Функция: Настройка адреса сервера WINS, выделенного DHCP-сервером. Пояснение: 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 протокол NetBIOS для передачи данных. Поэтому для большинства клиентов на базе ОС Windows требуется настройка WINS. Чтобы DHCP-клиент мог преобразовать имя хоста в IP-адрес, следует указать адрес WINS-сервера, когда DHCP-сервер выделяет IP-адрес клиенту. Для пула адресов DHCP можно настроить не более 4 серверов WINS.

NIS Domain Name

Диапазон: 1~36 символов

Функция: Настройка адреса доменного имени NIS, выделенного DHCP-сервером.

NIS Server

Формат: A.B.C.D

Функция: Настройка адреса сервера NIS, выделенного DHCP-сервером.

Client Identifier

Варианты: None/FQDN/MAC

По умолчанию: None

Функция: Если тип пула - хост, необходимо указать уникальный идентификатор клиента.

Hardware Address

Формат: HH-HH-HH-HH-HH-HH (H – шестнадцатеричное число)

Функция: Если тип пула - хост, необходимо указать статически привязанный MAC-адрес.

Client Name

Диапазон: 1~32 символа

Функция: Если тип пула - хост, необходимо указать имя клиента.

Vendor i Class Identifier

Диапазон: 1~64 символа

Функция: Настройка идентификатора класса вендора, выделенного DHCP-сервером.

Vendor i Specific Information

Диапазон: 1~64 шестнадцатеричных числа

Функция: Настройка специфичной информации вендора, выданной DHCP-сервером.

4. Настройте исключенные IP-адреса (IP-адреса не выделяются динамически в пуле адресов DHCP), как показано на рисунке 37.

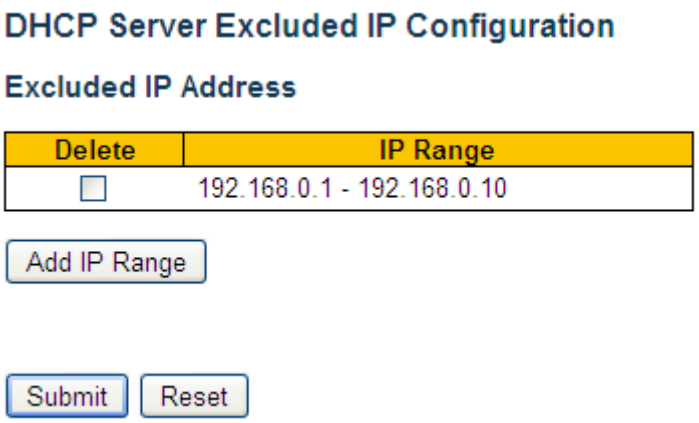


Рисунок 37 Настройка исключенных IP-адресов

IP Range

Функция: Настройка диапазона IP-адресов, которые не выделяются динамически в пуле адресов DHCP. При распределении IP-адресов DHCP-сервер должен исключить занятый 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.

Щелкните <Add IP Range>, чтобы настроить диапазон IP-адресов, которые не распределяются динамически.

5. Просмотрите статистику сервера DHCP, как показано на рисунке 38.

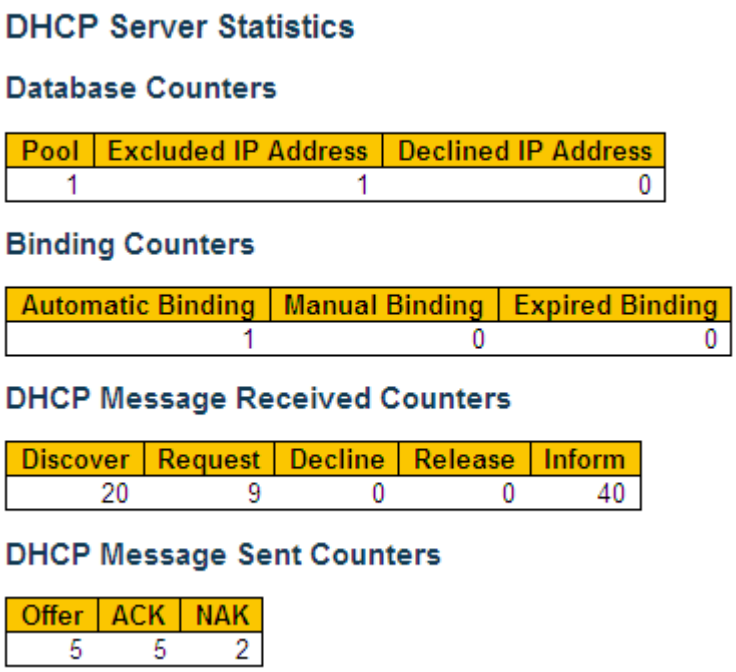


Рисунок 38 Просмотр статистики сервера DHCP

6. Просмотрите информацию об IP-адресах, выделенных сервером DHCP, как показано на рисунке 39.

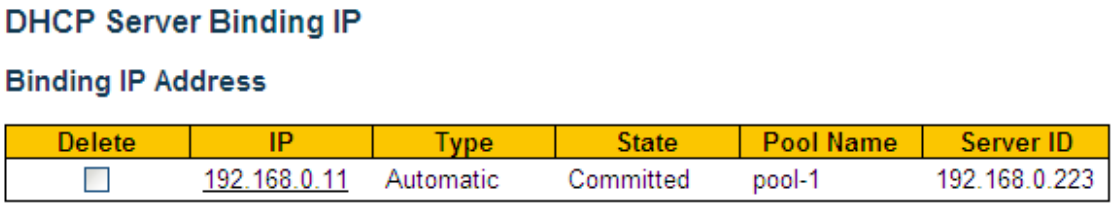


Рисунок 39 Просмотр информации об IP-адресах, выделенных сервером DHCP

7. Просмотрите IP-адреса, отклоненные DHCP-клиентами, как показано на рисунке 40.

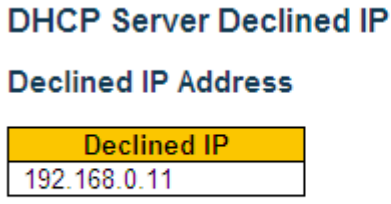


Рисунок 40 Просмотр IP-адресов, отклоненных DHCP-клиентами

Если клиент обнаруживает, что IP-адрес, выделенный сервером, конфликтует со статическим IP-адресом в том же сегменте сети, он отправляет на сервер пакет отклонения, чтобы отклонить этот IP-адрес. Сервер записывает IP-адрес,

отклоненный клиентом, и не будет выделять этот IP-адрес другим клиентам в течение определенного периода времени.

5.3.1.4 Пример типовой конфигурации

Как показано на рисунке 41, коммутатор A работает как сервер DHCP, а коммутатор B работает как DHCP-клиент. Порт 3 коммутатора A подключается к порту 4 коммутатора B. Клиент отправляет сообщения с запросом IP-адреса, и сервер может выделить IP-адрес клиенту двумя способами. Для динамического выделения IP-адресов диапазон исключенных адресов 192.168.0.1~192.168.0.10.

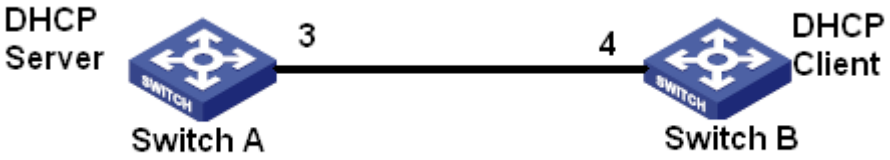


Рисунок 41 Пример типовой конфигурации DHCP

Статические IP-адреса

➢ Конфигурация коммутатора A:

1. Запустите сервер DHCP в соответствующих VLANs, как показано на рисунке 34.
2. Создайте IP-пул DHCP: pool-1, как показано на рисунке 35.
3. Установите тип пула Host; IP-адрес 192.168.0.6, маску 255.255.255.0. Привяжите MAC-адрес коммутатора B: 00-11-22-33-44-55, как показано на рисунке 36.

➢ Конфигурация коммутатора B:

1. Настройте коммутатор B для автоматического получения IP-адреса через DHCP.
2. Коммутатор B получает IP-адрес 192.168.0.6 и маску подсети 255.255.255.0 от DHCP-сервера, как показано на рисунке 42.

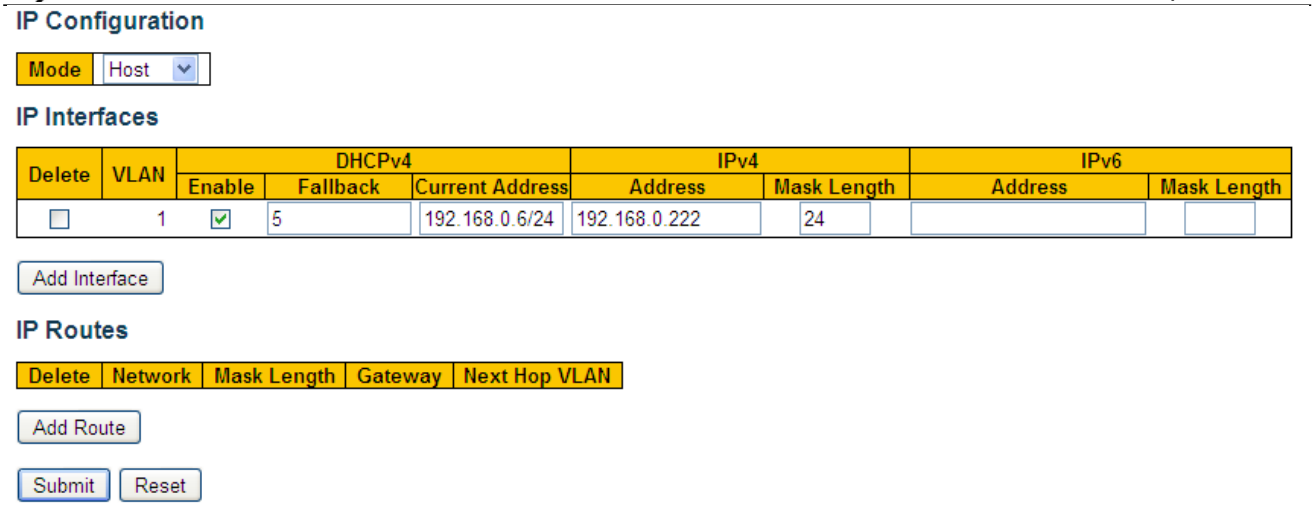


Рисунок 42 Клиент DHCP получает IP-адрес-1

Динамические IP-адреса

➢ Конфигурация коммутатора A:

1. Запустите сервер DHCP в соответствующих VLANs, как показано на рисунке 34.

2. Создайте IP-пул DHCP: pool-1, как показано на рисунке 35.

3. Установите тип пула Network; IP-адрес 192.168.0.6, маску 255.255.255.0, как показано на рисунке 36.

4. Настройте диапазон исключенных IP-адресов 192.168.0.1~192.168.0.10., как показано на рисунке 37.

➢ Конфигурация коммутатора B:

1. Настройте коммутатор B для автоматического получения IP-адреса через DHCP.

2. DHCP-сервер ищет доступные IP-адреса в пуле адресов по порядку и выделяет первый найденный доступный IP-адрес и другие сетевые параметры коммутатору B. Маска подсети 255.255.255.0, как показано на рисунке 43.

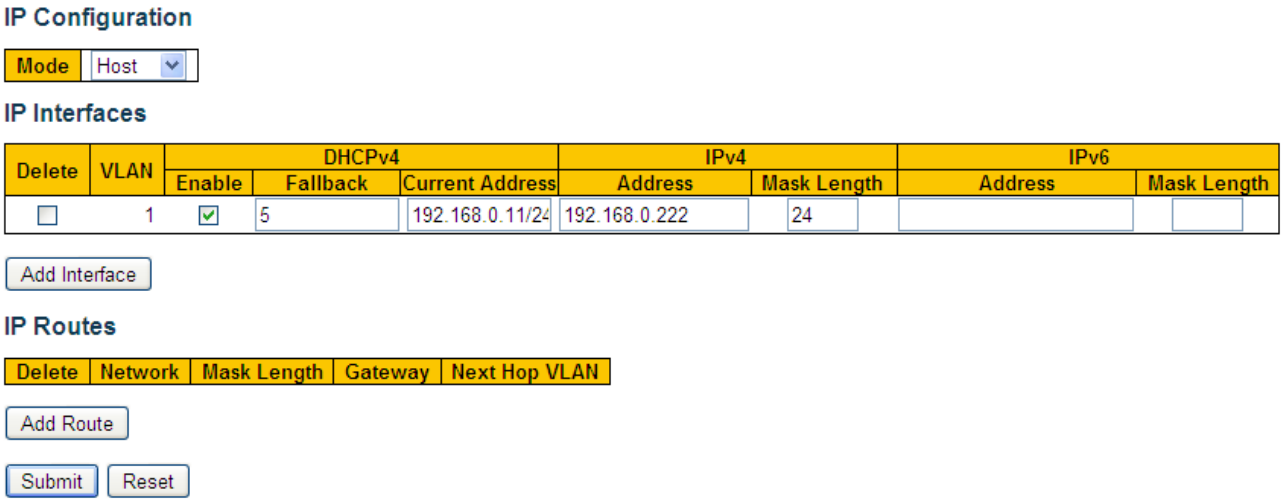


Рисунок 43 Клиент DHCP получает IP-адрес-2

5.3.2 DHCP Snooping

5.3.2.1 Введение

Отслеживание DHCP — это функция мониторинга служб DHCP на уровне 2 и функция безопасности DHCP, обеспечивающая дополнительную безопасность клиента. Механизм безопасности DHCP Snooping может контролировать, что только доверенный порт может пересылать сообщение запроса DHCP-клиента на легальный сервер, в то же время он может контролировать источник ответного сообщения DHCP-сервера, гарантируя, что клиент получит IP-адрес от действительного сервера, и предотвращая выделения IP-адресов или других параметров конфигурации другим хостам поддельным или недействительным DHCP-сервером.

Механизм безопасности DHCP Snooping делит порты на доверенные и ненадежные. Доверенный порт: порт, который прямо или косвенно подключается к действительному DHCP-серверу. Доверенный порт пересылает сообщения запросов DHCP-клиентов и ответные сообщения DHCP-серверов, чтобы гарантировать, что DHCP-клиенты могут получить допустимые IP-адреса. Ненадежный порт: это порт, который подключается к недействительному DHCP-серверу. Ненадежный порт не пересылает сообщения запросов DHCP-клиентов и ответные сообщения DHCP-серверов, чтобы предотвратить получение DHCP-клиентами недопустимых IP-адресов.

5.3.2.2 Настройка через веб-интерфейс

1. Включите функцию DHCP Snooping, как показано на рисунке 44.

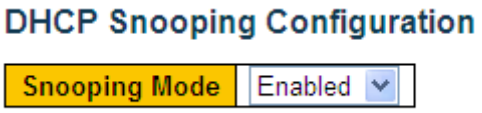


Рисунок 44 Состояние функции DHCP Snooping

DHCP Snooping Mode

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение функции DHCP Snooping

Предупреждение:

У коммутатора, который работает и как сервер DHCP и как клиент, нельзя включить функцию DHCP Snooping.

2. Настройте доверенные порты, как показано на рисунке 45.

Рисунок 45 Настройка доверенных портов

Mode

Варианты: Trusted/Untrusted

По умолчанию: Untrusted

Функция: настройка порта как доверенного или ненадежного. Порты, которые прямо или косвенно подключаются к действительному DHCP-серверу – это доверенные порты.

Предупреждение:

Назначение порта доверенным и транковым является взаимоисключающим. Порт, группу нельзя назначить доверенным. Доверенный порт не может входить в транковую группу.

5.3.2.3 Пример типовой конфигурации

Как показано на рисунке 46, DHCP-клиент запрашивает IP-адрес от сервера DHCP. В сети существует неавторизованный DHCP-сервер. Порт 1 настроен как доверенный порт с помощью DHCP Snooping, чтобы пересылать сообщение запроса DHCP-клиента на DHCP-сервер и пересылать ответное сообщение DHCP-сервера на DHCP-клиент. Порт 3 настроен в качестве ненадежного порта, который не может пересылать сообщение запроса DHCP-клиента и ответное сообщение неавторизованного DHCP-сервера, гарантируя, что клиент может получить действительный IP-адрес от действительного DHCP-сервера.

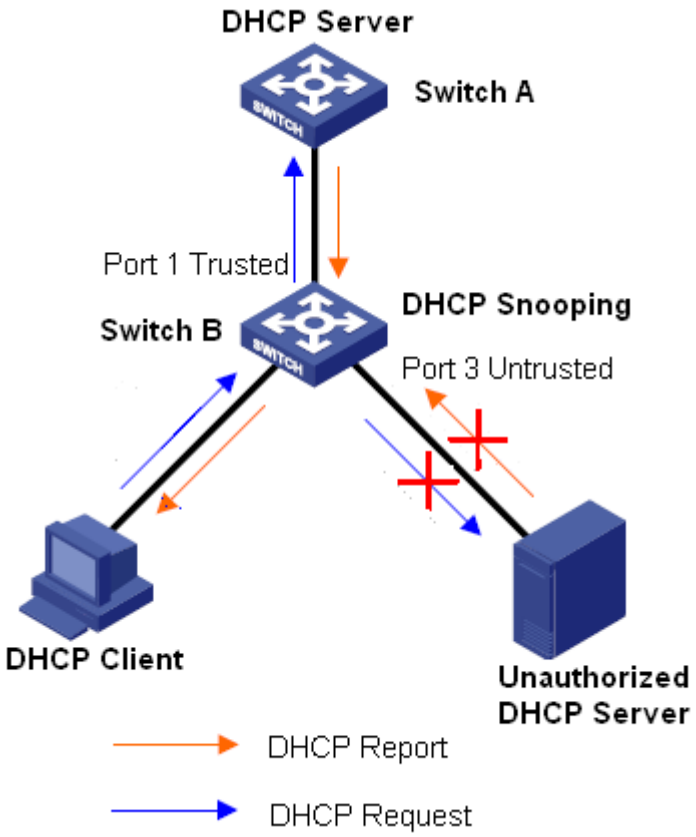


Рисунок 46 Пример типовой конфигурации DHCP Snooping

Конфигурация коммутатора B:

- Включите функцию DHCP Snooping, как показано на рисунке 44.
- Настройте порт 1 коммутатора B как доверенный порт, а порт 3 как ненадежный порт, как показано на рисунке 45. По умолчанию: Trusted

5.3.3 Конфигурация

Функция Option 82 (запись информации об агенте ретрансляции) записывает информацию о клиенте. Когда DHCP Snooping, поддерживаемый Option 82, получает сообщение запроса от DHCP-клиента, в сообщения добавляется соответствующее поле Option 82, а затем сообщение пересылается на DHCP-сервер. Сервер, поддерживающий Option 82, может гибко распределять адреса в соответствии с сообщением Option 82.

После включения функции Option 82 поле Option 82 будет добавлено в сообщение. Поле Option

82 коммутаторов этой серии содержит два параметра: параметр 1 (Circuit ID) и параметр 2 (Remote ID). Формат двух параметров показан ниже:

- Параметр 1 содержит идентификатор VLAN ID и номер порта, который получает сообщение запроса от DHCP-клиента, как показано в Таблице 2.

Таблица 2 Формат поля параметра 1

Тип параметра （0x01）	Длина （0x04）	VLAN ID	Номер порта
Один байт	Один байт	Два байта.	Два байта.

Тип параметра: Тип параметра 1 – 1.

Длина: количество байтов, которые занимают идентификатор VLAN и номер порта.

VLAN ID: На устройстве DHCP Snooping — идентификатор VLAN порта, который получает сообщение запроса от DHCP-клиента.

Номер порта: На устройстве DHCP Snooping — номер порта, который получает сообщение запроса от DHCP-клиента.

- Параметр 2 содержит MAC-адрес устройства DHCP Snooping, которое получает

сообщение запроса от DHCP-клиента, как показано в Таблице 3.

Таблица 3 Формат поля параметра 2 – MAC-адрес

Тип параметра （0x02）	Длина （0x06)	MAC-адрес
Один байт	Один байт	6 байт

Тип параметра: Тип параметра 2 – 2.

Длина: количество байтов, которые занимает содержание параметра 2. MAC-адрес занимает 6 байт, а строка символов занимает 16 байт.

MAC-адрес: содержимое параметра 2 — это MAC-адрес устройства DHCP Snooping, которое получает сообщение запроса от DHCP-клиента.

5.3.3.1 DHCP Snooping с поддержкой функцию Option 82

1 Введение

Если устройство DHCP Snooping поддерживает функцию Option 82, при получении DHCP Snooping сообщения запроса DHCP сообщение обрабатывается в соответствии с тем, содержит ли сообщение параметр 82 и политику клиента, а затем обработанное сообщение пересылается серверу DHCP. Метод обработки показан в таблице 4.

Таблица 4 Режимы обработки сообщений запроса (DHCP Snooping)

Получение сообщения	**Политика конфигурации**	**Обработка сообщения запроса на устройстве DHCP Snooping**
Сообщение запроса	Drop	Отклонить сообщение запроса
	Keep	Сохранить формат сообщения без изменений и переслать сообщение
	Replace	Заменить поле Option 82 в сообщении полем Option 82 устройства Snooping и переслать новое сообщение
Сообщение запроса не содержит Option 82	Drop/Keep/Replace	Добавить поле Option 82 устройства Snooping в сообщение и переслать его

Когда устройство DHCP Snooping получает сообщение запроса от DHCP-сервера, если сообщение содержит поле Option 82, удалить поле Option 82 и переслать сообщение клиенту.

2 Настройка через веб-интерфейс

Настройка DHCP Snooping Option 82 показана на рисунке 47.

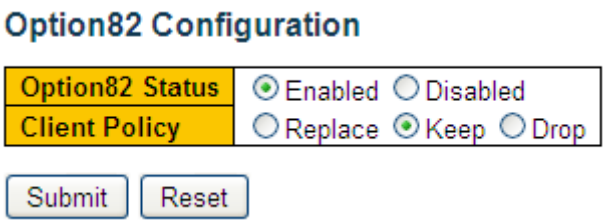


Рисунок 47 Настройка DHCP Snooping Option 82

Option82 Status

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение функции Option82 на устройстве DHCP Snooping.

Client Policy

Варианты: Drop/Replace/Keep

По умолчанию: Replace

Функция: Настройка политики клиента. Устройство DHCP Snooping обрабатывает сообщение запроса, отправленное от клиента, в соответствии с политикой клиента, как показано в таблице 4.

6 Система часов

6.1 Настройка часов

Настройте часовой пояс, как показано на рисунке 48.

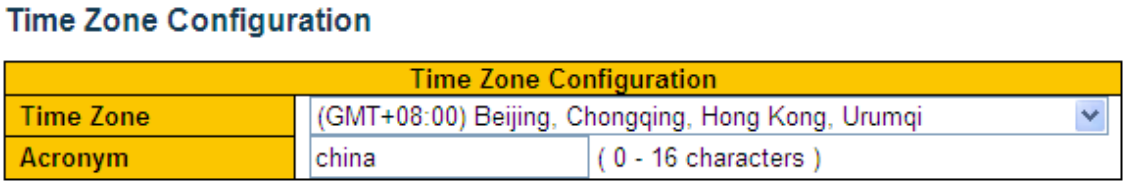


Рисунок 48 Настройка часового пояса

Time Zone

Функция: Выбор часового пояса.

Acronym

Функция: Описание часового пояса

Настройте летнее время, как показано на рисунке 49 и рисунке 50.

Чтобы в полной мере использовать время и экономить энергию, летом можно использовать летнее время (DST). Чтобы быть точным, переведите часы на какое-то время летом. Настройка DST включает в себя повторяющуюся и неповторяющуюся настройку.

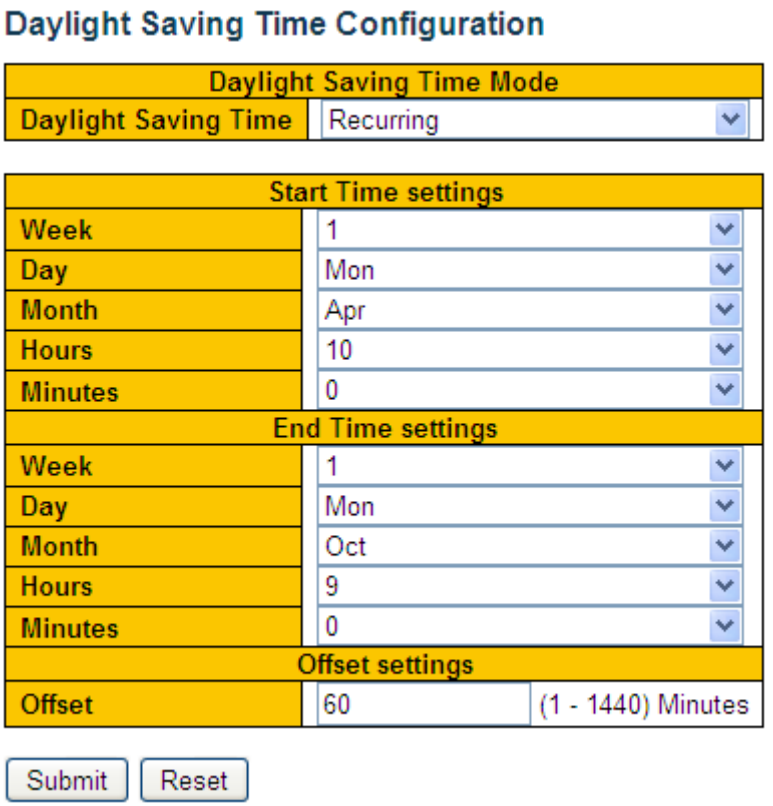


Рисунок 49 Повторяющаяся настройка DST

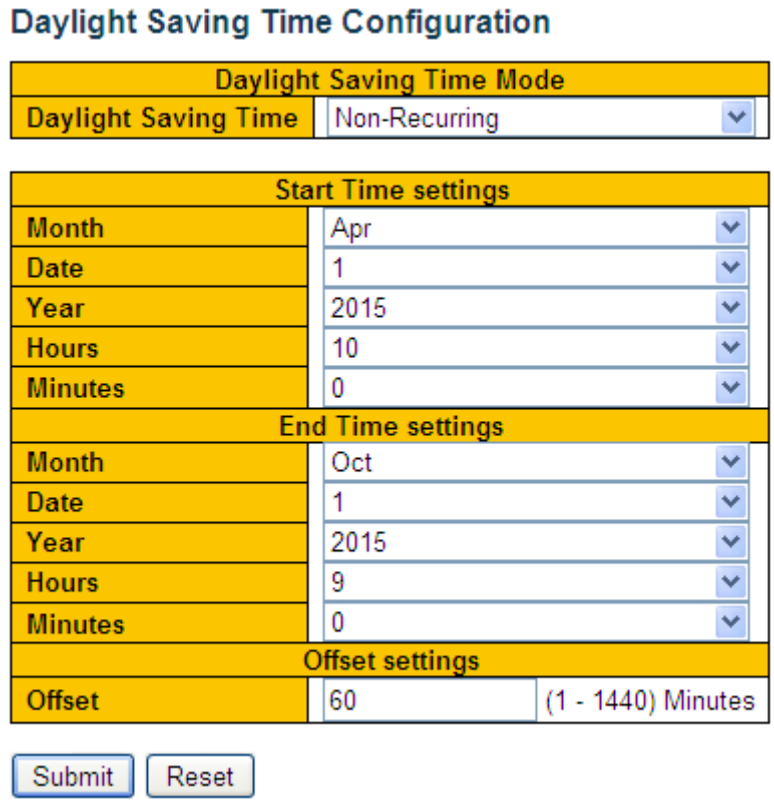


Рисунок 50 Неповторяющаяся настройка DST

Daylight Saving Time

Варианты: Disabled/Recurring/Non-Recurring

По умолчанию: Disabled

Функция: Включение или выключение DST После включения DST часы будут переведены летом на некоторое время вперед. Вариант Recurring означает повторение перехода на летнее время каждый год.

Start Time setting /End Time setting

Функция: Настройка отрезка времени для перехода на летнее время после включения DST. В режиме non-Recurring необходимо задать год, месяц, число, часы и минуты для указания отрезка времени для перехода на летнее время. Как показано на рисунке 50, переход на летнее время осуществляется с 10:00 1 апреля 2015 г. по 9:00 1 октября 2015 г. Можно задать месяц, неделю, день, час и минуту в режиме цикла, чтобы указать период применения летнего времени каждый год. Например, можно задать переход на летнее время с 10:00 первого понедельника апреля по 9:00 первого понедельника октября каждый год (см. рисунок 49).

Offset

Диапазон: 1~1440 минут

По умолчанию: 1 минута

Функция: Задание времени, на которое переводятся вперед часы при переходе на летнее время.

Предупреждение:

- Время начала должно отличаться от времени окончания.
- Время начала задается по зимнему времени. Время окончания задается по летнему времени.

Например, летнее время с 10:00:00 1 апреля до 9:00:00 1 октября. Часы переводятся на 60 минут. Зимнее время идет до 10:00:00 1 апреля. Затем часы переводятся на 11:00:00, и начинается летнее время. Летнее время идет до 9:00:00 1 октября. Затем часы переводятся назад на 8:00:00 зимнего времени.

6.2 SNTP

Простой протокол сетевого времени (SNTP) синхронизирует время между сервером и клиентом путем запросов и ответов. Как клиент коммутатор синхронизирует время с сервером по пакетам сервера.

Предупреждение:

- Для синхронизации времени по SNTP необходим активный SNTP-сервер.
- Вся информация о времени, передаваемая в протоколе SNTP, является стандартной информацией о времени часового пояса 0.

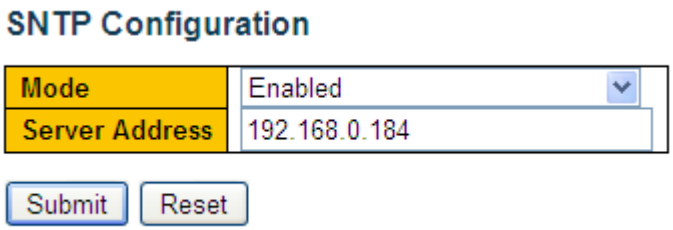


Рисунок 51 Включение SNTP

Mode

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Включение/выключение SNTP

Server Address

Формат: A.B.C.D

Функция: Настройка IP-адреса сервера SNTP. Клиенты будут синхронизировать время в соответствии с пакетами сервера.

Проверьте, синхронизируются ли часы с сервера.

Щелкните [Basic Configuration] →[System Information], чтобы просмотреть информацию о часах, как показано на рисунке 52.

System Information

System	
Contact	+86-10-88798888
Name	SWITCH
Location	No.901 Floor 8 to 12, Building No.2,Shixing Avenue 30#, Shijingshan District, Beijing, P. R. China 100144
Hardware	
Device Type	SICOM3000A-2GX8GE
Device MAC Address	00-1e-cd-1c-e8-e0
S/N	S30U0035Axxxxxxxxx
Time	
System Date	1970-01-02T00:30:08+00:00
System Uptime	1d 00:30:08
Software	
Software Version	R3001
Code Date	Jul 25 2018 09:02:04
Code Revision	Build-24.0.44.2.B1.4.3
Hardware Version	V1.0
Logic Version	V1.0.0

Рисунок 52 Просмотр информации о часах

Можно просмотреть информацию о времени коммутатора на основе времени сервера в сочетании с выбранным часовым поясом и конфигурацией перехода на летнее время.

6.3 PTP

6.3.1 Введение

Протокол точного времени (PTP) с высокой точностью синхронизирует независимые часы на распределенных узлах системы измерения и управления. Протокол синхронизирует фазу и частоту с точностью до ±100 нс.

Концепция PTP

1. Домен PTP

Сеть, в которой применяется PTP, является доменом PTP. Домен PTP имеет только одни главные часы. Все остальные устройства синхронизируют время по ним.

2. Порт PTP

Порт с поддержкой PTP называется портом PTP.

3. Узел часов

Узлы в домене PTP являются узлами часов. PTP определяет следующие узлы часов:

- Граничные часы (BC)

В домене PTP узел BC имеет один или несколько портов PTP, участвующих в синхронизации часов. Если толь
участвуют несколько портов PTP, один из этих портов синхронизирует время от узла синхронизации восходящей линии связи, а другие порты синхронизируют время с узлами синхронизации нисходящей линии связи. Когда BC служат источником синхронизации, они могут доставлять время на узлы синхронизации нисходящей линии связи через несколько портов PTP.

- Прозрачные часы (TC)

Узлу TC не нужно синхронизировать время с другими узлами часов. Он имеет несколько портов PTP. Эти порты только пересылают пакеты PTP и проверяют задержку пересылки, но не выполняют синхронизацию часов. Часы проз
Прозрачные часы End-to-End Transparent Clock (E2ETC): напрямую пересылают не-PTP-пакеты и участвуют в расчете задержки для всего канала.
Прозрачные часы Peer-to-Peer Transparent Clock (P2PTC): напрямую пересылают пакеты Sync, Follow_Up и Announce, завершают другие пакеты PTP и участвуют в расчете задержки каждого сегмента канала.
Связь между парой узлов синхронных часов:

- Узел, отправляющий информацию о синхронизации часов, находится в ведущем режиме (master), а узлы, получающие информацию, являются подчиненными (slave) узлами.
- Часы узла master являются ведущими часами, а часы узла slave — подчиненными.
- Порт, отправляющий информацию о синхронизации часов, находится в ведущем режиме (master), а порты, получающие информацию, являются подчиненными (slave) узлами.

6.3.2 Принципы синхронизации

1. Выбор гроссмейстерских часов

Все узлы часов выбирают гроссмейстерские часы в домене PTP, обмениваясь

пакетами Announce с информацией об уровне часов и идентификаторе часов. Затем определяются отношения ведущий/подчиненный между узлами и портами ведущий/подчиненный на узлах. С помощью этого процесса по всему домену PTP устанавливается связующее дерево с гроссмейстерскими часами в качестве корня. Затем главные часы периодически посылают пакеты Announce подчиненным часам. Если подчиненные часы не получают пакеты Announce от главных часов в течение определенного периода, главные часы считаются недействительными и начинается новый выбор.

Пакеты Announce содержат следующую информацию для выбора гроссмейстерских часов: гроссмейстерский приоритет 1, тактовый слой, точность часов, гроссмейстерский приоритет 2 и идентификатор часов. Информация сравнивается в следующей процедуре: часы с наименьшим гроссмейстерским приоритетом 1 выбираются в качестве гроссмейстерских часов; если часы имеют одинаковое значение гроссмейстерского приоритета 1, часы с наименьшим часовым слоем выбираются гроссмейстерскими часами; аналогичным образом, если часы имеют одинаковые значения для гроссмейстерского приоритета 1, слоя часов, точности часов, гроссмейстерского приоритета 2, часы с наименьшим идентификатором часов выбираются в качестве гроссмейстерских часов.

2. Принципы синхронизации

Главные и подчиненные часы обмениваются пакетами синхронизации, записывают время отправки и получения пакетов и вычисляют общую задержку между главными и подчиненными часами на основе разницы во времени. Если сетевой путь симметричен, однонаправленная задержка составляет половину общей задержки. Подчиненные часы настраивают местное время в соответствии с разницей во времени между главными и подчиненными часами и однонаправленной задержкой, реализуя синхронизацию времени от главных часов.

PTP поддерживает два механизма измерения задержки:

- Механизм запроса-ответа: используется для измерения сквозной задержки всего канала.
- Одноранговый механизм: используется для измерения задержки между двумя точками. По сравнению с механизмом запроса-ответа, одноранговый механизм

измеряет задержку каждого сегмента канала связи.

6.3.3 Настройка через веб-интерфейс

1. Настройка часов PTP показана на рисунке 53.

PTP Clock Configuration

Delete	Clock Instance	Device Type	Profile
☐	0	Ord-Bound	1588

Рисунок 53 Настройка часов PTP

Clock Instance:

Диапазон: 0~3

Функция: Настройка экземпляра PTP

Device Type:

Диапазон: Ord-Bound/P2pTransp/E2eTransp/Masteronly/Slaveonly

Функция: Настройка типа часов PTP

Profile:

Диапазон: No Profile/1588

Функция: Выбор файла описания PTP

Предупреждение:

➢Profile 1588 нельзя использовать с E2eTransp

2.Щелкните <Instance No.>, чтобы выполнить задать подробную настройку PTP, как показано на рисунке 54:

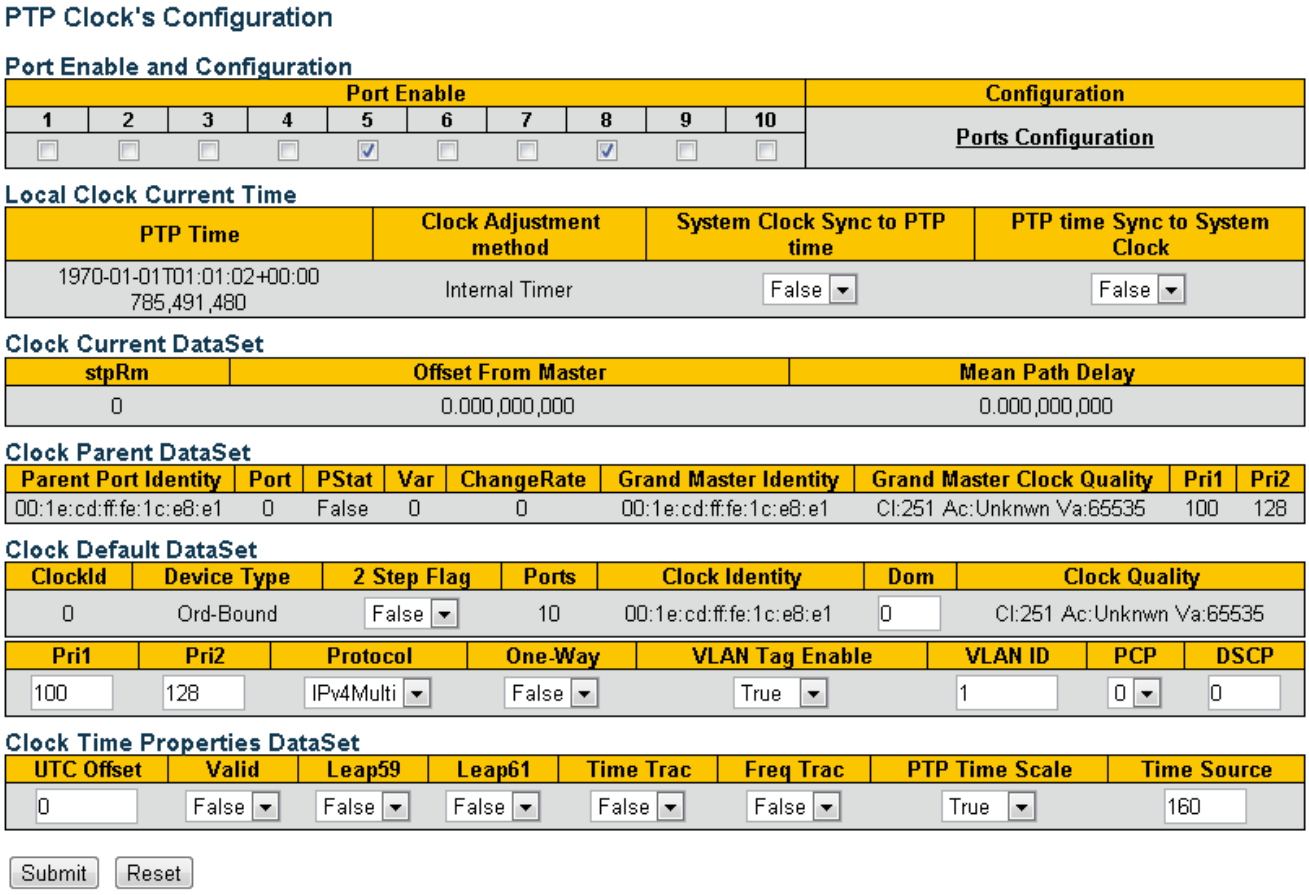


Рисунок 54 Подробная настройка экземпляра PTP

2.1 Port enable and configuration

Port Enable:

Функция: Выбор одного порта для включения PTP

Configuration:

Щелкните <Ports Configuration>, чтобы перейти на страницу настройки данных порта синхронизации PTP, как показано на рисунке 55.

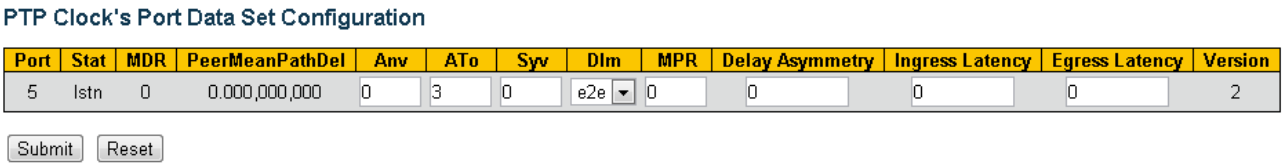


Рисунок 55 Настройка портов

Anv:

Диапазон:-3~4

Функция: Интервал времени для выдачи сообщений Announce в состоянии master.

ATo:

Диапазон:1~10

Функция: Тайм-аут для получения портом сообщений Announce.

Syv :

Диапазон:-7~4

Функция: Интервал времени для выдачи сообщений синхронизации в состоянии master.

Dlm:

Диапазон: p2p/e2e

Функция: Настраиваемый механизм задержки. Используемый для порта механизм

задержки: e2e измерение задержки End-to-end

p2p измерение задержки Peer-to-peer.

Может быть определен для каждого порта в обычных/граничных часах.

В прозрачных часах все порты используют один и тот же механизм задержки,

определяемый типом часов.

MPR:

Диапазон: -7~5

Функция: Интервал выдачи сообщений Delay_Req для порта в режиме E2e. Это значение объявляется от главного к подчиненному ведомому в сообщении Announce.

Значение отражается в поле MDR в Slave.

Интервал выдачи сообщений Pdelay_Req для порта в режиме P2P.

Delay Asymmetry:

Диапазон:-100000~100000ns

Функция: Компенсация задержки для несимметричных линий

Ingress latency:

Диапазон:-100000~100000ns

Функция: Задержка входящего трафика в наносекундахс, как определено в IEEE 1588, раздел 7.3.4.2.

Ingress latency:

Диапазон:-100000~100000ns

Функция: Задержка исходящего трафика в наносекундахс, как определено в IEEE 1588, раздел 7.3.4.2.

2.2 Текущий набор данных часов

Показывает фактическое время PTP с разрешением в наносекундах. Существует два метода: синхронизировать системные часы с временем PTP или синхронизировать время PTP с системными часами. Однако они являются взаимоисключающими и не могут быть выбраны одновременно.

2.3 Набор данных часов по умолчанию

2 Step Flag:

включение 2

step flag

Domain:

настройка идентификатора домена экземпляра PTP

Pri 1:

Приоритет часов 1 [0..255], используемый алгоритмом выбора главного устройства BMC.

Pri 2:

Приоритет часов 2 [0..255], используемый алгоритмом выбора главного устройства BMC.

Protocol:

Диапазон: Ethernet/IPv4Multi

Функция: Транспортный протокол, используемый ядром протокола PTP.

Описание: Ethernet PTP через многоадресную передачу Ethernet/IPv4Multi PTP через многоадресную передачу IPv4

One-Way:

Если значение true, используются односторонние измерения. Этот параметр применяется только к подчиненному устройству. В одностороннем режиме измерения задержки не выполняются, т. е. это применимо только в том случае, когда необходима частотная синхронизация. Главное устройство всегда отвечает на запросы задержки.

VLAN Tag Enable:

Включение тегирования VLAN для кадров PTP.

Примечание: Пакеты помечаются только в том случае, если порт настроен для

тегирования vlan для настроенной VLAN.

VlanID:

Диапазон:1-4094

PCP:

Диапазон：0~7

Описание: Значение Priority Code Point, используемое для кадров PTP.

DSCP:

Диапазон: 0~63

Описание: Значение Differentiated Services Code Point, используемое для кадров PTP.

2.3 Набор данных свойств времени часов

UTC Offset:

Диапазон: 0-

10000 **Valid:**

Диапазон: TRUE/FALSE

Leap59, Leap61:

Описание:

дополнительная секунда

Time Trac、Freq Trac:

Диапазон:

TRUE/FALSE **PTP**

Time Scale: Диапазон:

TRUE/FALSE **Time**

Source:

Набор данных свойств времени часов определен в стандарте IEEE 1588. Набор данных является как настраиваемым, так и динамическим, т.е. параметры могут быть настроены для гроссмейстерских часов. В ведомых часах параметры перезаписываются свойствами гроссмейстерских часов. Параметры не используются в текущей реализации PTP.

Допустимые значения параметра Time Source: 16

(0x10) ATOMIC_CLOCK

32 (0x20) GPS

48 (0x30) TERRESTRIAL_RADIO

64 (0x40) PTP

80 (0x50) NTP

96 (0x60) HAND_SET

144 (0x90) OTHER

160 (0xA0) INTERNAL_OSCILLATOR

3.Состояние PTP

Настройка часов PTP показана на рисунке 56.

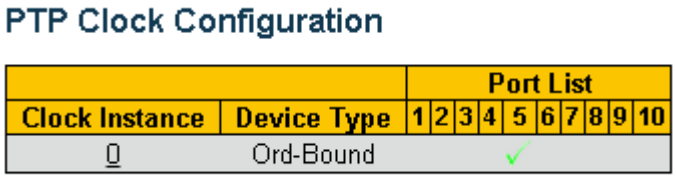


Рисунок 56 Настройка часов PTP

Подробная настройка экземпляра PTP показана на рисунке 57.

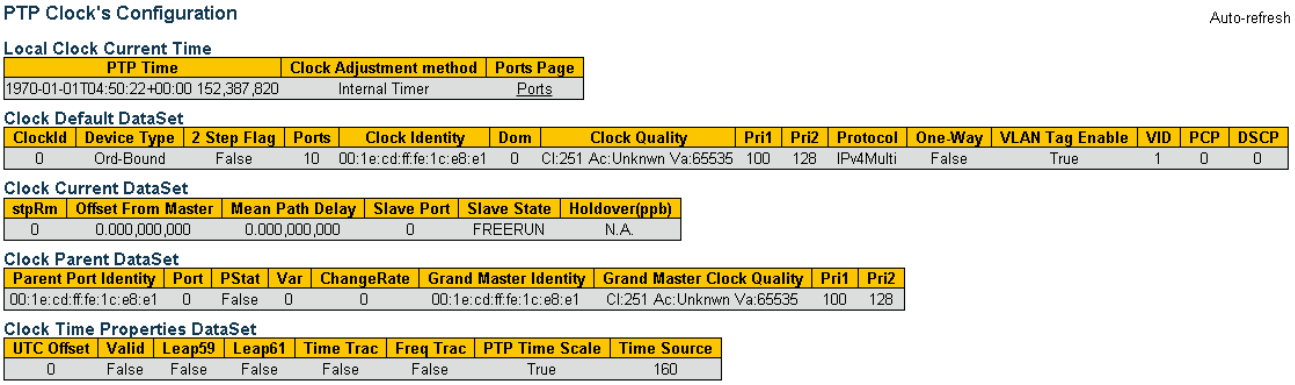


Рисунок 57 Подробная настройка экземпляра PTP

6.3.4 Пример типовой конфигурации

Как показано на рисунке 58, порт 1 коммутатора A подключен к порту 2 коммутатора B, а порт 3 коммутатора B подключен к порту 4 коммутатора C. Коммутатор A является ведущим (тип часов BC).

Коммутатор B использует тип часов P2PTC. Коммута

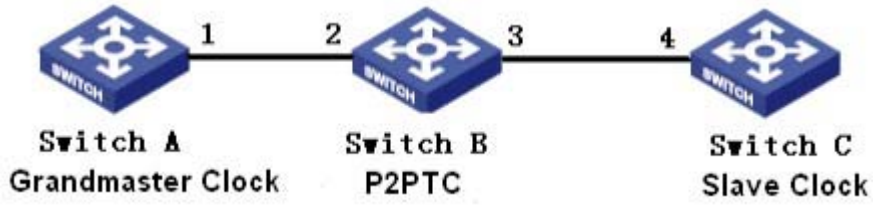


Рисунок 58 Пример настройки PTP

Конфигурация коммутатора A:

1. PTP включен на порту 1 коммутатора A.

2. Установите тип часов Boundary.Поскольку коммутатор A является ведущим, он должен иметь высший гроссмейстерский приоритет 1. В этом примере установите гроссмейстерский приоритет priority1 200, а механизм измерения задержки peer-to-peer, как показано на рисунке 53 и рисунке 54. Конфигурация коммутатора B:

3. PTP включен на порту 2 и порту 3 коммутатора B.

4. Set the clock type to P2PTC, the grandmaster priority1 to 210, and the delay measurement mechanism to peer-to-peer, as shown in Figure 53、Figure 54.Конфигурация коммутатора C:

5. PTP включен на порту 4 коммутатора C.

6. Установите тип часов Boundary, гроссмейстерский приоритет priority1 220, а механизм измерения задержки peer-to-peer, как показано на рисунке 53 и рисунке 54.

7 Настройка порта

1. Настройте состояние порта, скорость порта, управление потоком и другую информацию, как показано на рисунке 59.

Port Configuration

Port	Link	Speed		Adv Duplex		Adv Speed			Flow Control			Maximum Frame Size	Excessive Collision Mode	Reset
		Current	Configured	Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx			
*			<>	☑	☑	☑	☑	☑	☑			9600	<>	☐
1	●	100fdx	Auto	☑	☑	☑	☑	☑	☑	✓	✓	9600	Discard	☐
2	●	100fdx	Auto	☑	☑	☑	☑	☑	☑	✓	✓	9600	Discard	☐
3	●	100fdx	Auto	☑	☑	☑	☑	☑	☑	✓	✓	9600	Discard	☐
4	●	Down	10Mbps HDX	☐	☐	☐	☐	☐	☐	✗	✗	9600	Discard	☐
5	●	Down	10Mbps FDX	☐	☐	☐	☐	☐	☑	✓	✓	9600	Discard	☐
6	●	Down	100Mbps HDX	☐	☐	☐	☐	☐	☑	✓	✓	9600	Discard	☐
7	●	Down	100Mbps FDX	☐	☐	☐	☐	☐	☑	✓	✓	9600	Discard	☐
8	●	Down	Auto	☑	☑	☑	☑	☑	☑	✓	✓	9600	Discard	☐
9	●	Down	Auto	☑	☑	☑	☑	☑	☑	✓	✓	9600	Discard	☐
10	●	Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	9600	Discard	☐
11	●	Down	Auto	☑	☑	☑	☑	☑	☑	✓	✓	9600	Discard	☐
12	●	Down	Auto	☑	☑	☑	☑	☑	☑	✓	✓	9600	Discard	☐

Submit Reset

Рисунок 59 Настройка портов

Link

Отображение статуса соединения для портов.

Зеленый: Порт находится в состоянии LinkUp и может нормально передавать данные.

Красный: Порт находится в состоянии LinkDown и не может нормально передавать данные. **Speed-Current**

Отображение скорости связи и дуплексного режима портов.

Speed-Configuration

Варианты: Disabled/Auto/10Mbps HDX/10Mbps FDX/100Mbps HDX/100Mbps FDX//1Gbps FDX

По умолчанию: Auto

Функция: Настройка скорости связи и дуплексного режима портов. Disabled указывает на то, что порт отключен и запрещает передачу данных. Эта опция напрямую влияет на аппаратное состояние порта и запускает аварийные сигналы порта.

Описание: Скорость и дуплексный режим портов могут автоматически согласовываться или устанавливаться принудительно. Если установлено значение Auto, скорость порта и режим дуплекса согласовываются автоматически

в зависимости от состояния подключения порта. Рекомендуется включить автосогласование для каждого порта, чтобы избежать проблем с подключением, вызванных несоответствием конфигурации порта. Если вы хотите принудительно включить режим скорости/дуплекса порта, убедитесь, что конфигурация скорости/режима дуплекса одинакова для подключенных портов на обоих концах.

Предупреждение:

- Для порта 10/100Base-TX можно задать Auto, 10Mbps HDX/10Mbps FDX/100Mbps HDX/100Mbps FDX.
- Для порта 10/100/1000Base-TX можно задать Auto, 10Mbps HDX/10Mbps FDX/100Mbps HDX/100Mbps FDX/1Gbps FDX.

Adv Duplex

Варианты: Fdx/Hdx

Функция: Настройка дуплексного режима автоматического согласования портов.

Описание: Fdx указывает, что порт может одновременно принимать и передавать данные; Hdx указывает, что порт либо принимает, либо передает данные. Когда для режима порта установлено значение Auto, дуплексный режим порта по умолчанию определяется путем согласования с одноранговым узлом. Согласованный дуплексный режим может быть либо Fdx, либо Hdx. Параметр может быть настроен для порта на согласование только одного дуплексного режима, тем самым управляя согласованием дуплексного режима.

Adv Speed

Варианты: 10M/100M/1G

Функция: Настройка автосогласования скорости портов.

Описание: Когда для режима порта установлено значение Auto, скорость порта по умолчанию определяется путем согласования с одноранговым узлом. Согласованная скорость может быть любой в пределах допустимого диапазона скоростей порта. Параметр может быть настроен для порта на согласование только некоторых скоростей, тем самым управляя согласованием скорости.

Предупреждение:

Настройки Adv Duplex и Adv Speed действуют только в автоматическом режиме.

Flow Control

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Включение/выключение функции управления потоком на назначенном порту.

Описание: Как только функция управления потоком включена, порт сообщит отправителю о снижении скорости передачи, чтобы по алгоритму или протоколу избежать потери пакетов, когда поток, полученный портом, превышает размер кэша порта. Если устройства работают в разных дуплексных режимах (полу/полный), управление потоком у них реализуется по-разному. Если устройства работают в полнодуплексном режиме, принимающая сторона отправит специальный кадр (Pause frame), чтобы проинформировать отправляющую сторону о прекращении отправки пакетов. Когда отправитель получает кадр паузы, он прекращает отправку пакетов на период «времени ожидания», указанный в кадре паузы, и продолжает отправлять пакеты после окончания «времени ожидания». Если устройства работают в полудуплексном режиме, они поддерживают управление потоком методом обратного давления. Принимающая сторона создает конфликт или сигнал несущей. Когда отправитель обнаруживает конфликт или несущую, он формирует отсрочку, чтобы отложить передачу данных.

Curr Rx/Curr Tx

Функция: Отображение состояния управления потоком порта.

Maximum Frame Size

Диапазон: 1518~9600 байт

По умолчанию: 9600 байт

Функция: Задание максимального размера пакета, принимаемого портом. Пакеты, размер которых больше указанного значения, отбрасываются.

Reset

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Выполнить или нет сброс порта.

2. Просмотр статистики порта, как показано на рисунке 60.

Port Statistics Overview

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	1275387	11523	98799397	2629185	0	0	869612	0	609
2	184535	1092883	17294542	80989316	0	0	1226	0	125257
3	227	183345	26332	16672027	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0

Рисунок 60 Статистика порта

Port

Щелкните <port> для перехода на страницу подробной статистики порта.

Packets

Отображение количества пакетов, которые каждый порт отправляет/получает.

Bytes

Отображение количества байтов, которые каждый порт отправляет/получает.

Errors

Отображение количества ошибочных пакетов, которые каждый порт отправляет/получает.

Drops

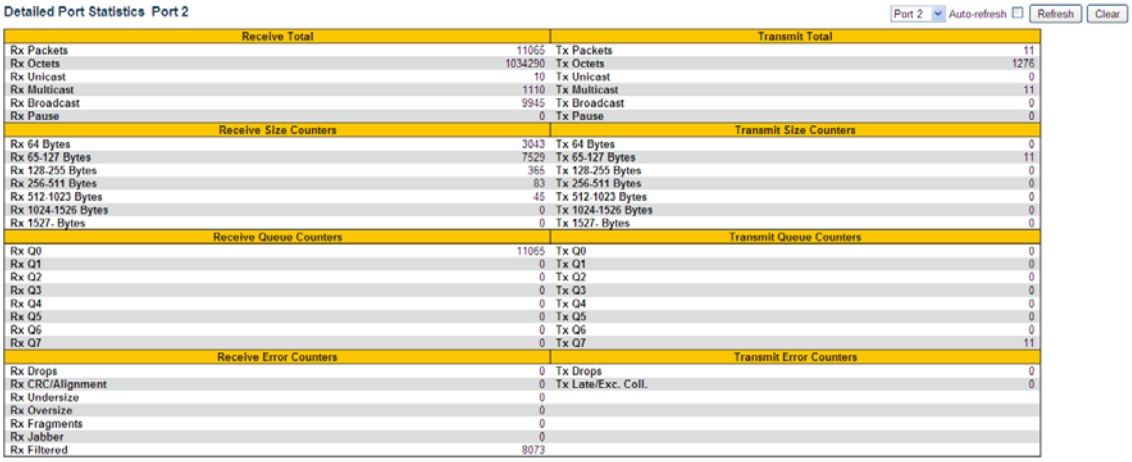
Отображение количества пакетов, отброшенных из-за конфликтов передачи/получения.

Filtered Received

Отображение количества пакетов, отфильтрованных принимающей стороной. Щелкните

<port> для перехода на страницу подробной статистики порта.

3. Просмотр подробной статистики порта, как показано на рисунке 61.



Detailed Port Statistics Port 2

Port 2 Auto-refresh Refresh Clear

Receive Total		Transmit Total	
Rx Packets	11065	Tx Packets	11
Rx Octets	1034290	Tx Octets	1276
Rx Unicast	10	Tx Unicast	0
Rx Multicast	1110	Tx Multicast	11
Rx Broadcast	9945	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	3043	Tx 64 Bytes	0
Rx 65-127 Bytes	7529	Tx 65-127 Bytes	11
Rx 128-255 Bytes	365	Tx 128-255 Bytes	0
Rx 256-511 Bytes	83	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	45	Tx 512-1023 Bytes	0
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	11065	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	11
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	8073		

Рисунок 61 Подробная статистика порта

Выберите порт и просмотрите подробную статистику порта.

8 Конфигурация QoS

8.1 Введение

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

Классификация трафика, контроль трафика, формирование трафика, управление перегрузками и предотвращение перегрузок являются основными концепциями развертывания QoS. В основном выполняются следующие функции:

Классификация трафика: идентифицирует объект на основе определенных правил сопоставления Это основа и предпосылка QoS.

Контроль трафика: контролирует скорость трафика пакетов, которые передаются на устройство. Когда скорость трафика превышает указанную скорость трафика, устройство принимает меры ограничения или штрафа для защиты сетевых ресурсов от повреждения. Контроль трафика подразделяется на контроль трафика на основе портов и контроль трафика на основе очередей.

Формирование трафика: проактивно регулирует скорость вывода трафика. Оно направлено на адаптацию трафика к доступным сетевым ресурсам нисходящего устройства, чтобы предотвратить ненужное отбрасывание пакетов и перегрузку. Формирование трафика подразделяется на формирование трафика на основе портов и формирование трафика на основе очередей.

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. Функция предотвращения перегрузки отслеживает использование сетевых ресурсов. При обнаружении увеличения перегрузки функция использует

упреждающее отбрасывание пакетов и настраивает объем трафика для устранения перегрузки.

Контроль трафика, формирование трафика, управление перегрузками и предотвращение перегрузок контролируют сетевой трафик и выделенные ресурсы с разных сторон. Они являются конкретным воплощением QoS. Например, коммутатор контролирует пакеты, которые передаются в сеть, на основе установленной скорости. Он формирует пакеты до того, как пакеты покинут коммутатор. Он управляет планированием очереди в случае перегрузки и принимает меры по предотвращению перегрузки, когда перегрузка усиливается.

8.2 Принцип работы

Каждый порт коммутаторов этой серии поддерживает 8 очередей кэширования, от 0 до 7 в порядке возрастания приоритета.

Когда кадр достигает порта, коммутатор определяет очередь для кадра в соответствии с информацией о кадре и портом. Коммутаторы этой серии поддерживают классификацию трафика в следующих режимах сопоставления очередей: порт, информация заголовка 802.1Q, кодовая точка дифференцированного обслуживания (DSCP) и контрольный список QoS (QCL) с приоритетом в порядке возрастания.

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: 6 Queues Weighted и SP (Strict Priority).

WRR (Weighted Round Robin) планирует потоки данных на основе соотношения весов. Очереди получают свою пропускную способность на основе соотношения весов. WRR отдает приоритет очередям с высоким весом. Больше пропускной способности выделяется очередям с более высоким весовым коэффициентом.

В режиме SP преимущественно пересылаются высокоприоритетные пакеты. Он в основном используется для передачи чувствительных сигналов. Если кадр поступает в очередь с высоким приоритетом, коммутатор прекращает планирование очередей с низким приоритетом и начинает обрабатывать данные очереди с высоким приоритетом. Когда очередь с высоким приоритетом не содержит данных, коммутатор начинает обрабатывать данные из очереди с более низким приоритетом.

6 Queues Weighted указывает, что очередь 6 и очередь 7 используют режим планирования Strict Priority, а очередь 0 ~ очередь 5 используют режим планирования WRR. Данные в очереди 7 обрабатываются раньше данных в очереди 6. Когда и очередь 7, и очередь 6 пусты, данные в очереди 0 ~ очереди 5 планируются на основе весовых коэффициентов.

8.3 Настройка через веб-интерфейс

1. Настройка режима сопоставления очередей на основе портов показана на рисунке 62.

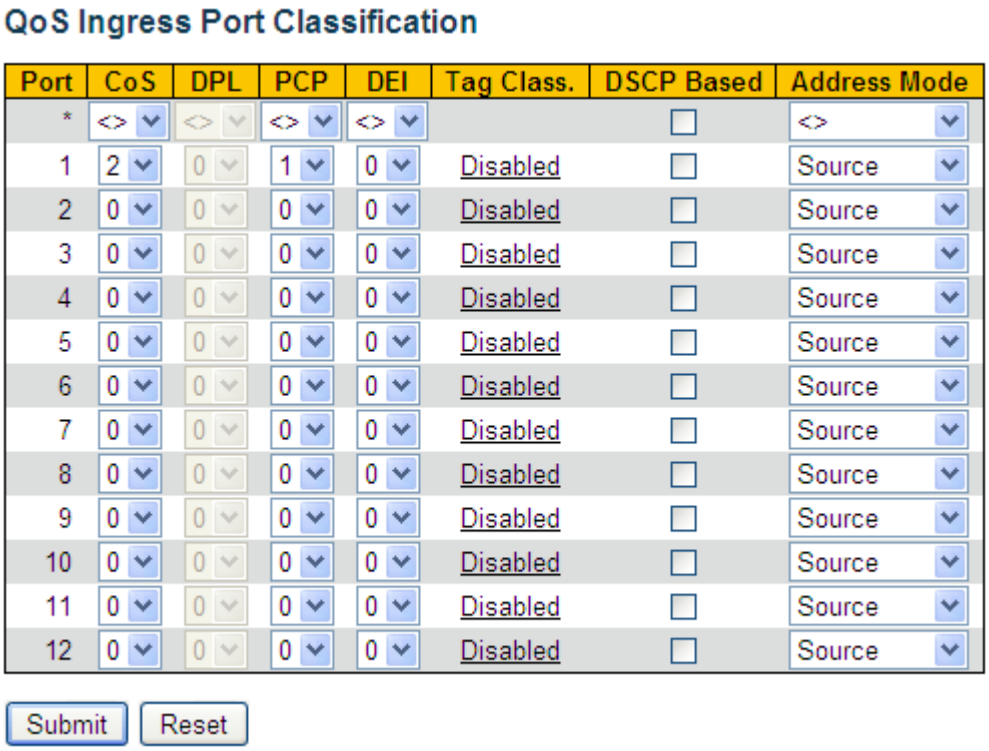


Рисунок 62 Настройка режима сопоставления очередей на основе портов

CoS

Диапазон: 0~7

По умолчанию: 0

Функция: Настройка значения CoS по умолчанию.

Описание: Значение CoS определяет очередь для хранения пакетов. Значение CoS находится в диапазоне от 0 до 7, что соответствует очереди от 0 до 7. После того, как пакет передан коммутатору, коммутатор присваивает пакету значение CoS. Если полученный пакет относится к типу тегированных, а классификация тегов отключена, или полученный пакет относится к типу без тегов, значением CoS в пакете является значение CoS по умолчанию для порта, принимающего пакет.

PCP

Диапазон: 0~7

По умолчанию: 0

Функция: Настройказначения PCP（Priority Code Point）по умолчанию для порта.

Пояснение: Когда пакет не помечен, приоритет в теге, добавленном к пакету, равен значению PCP по умолчанию для порта.

DEI

Диапазон: 0~1

По умолчанию: 0

Функция: Настройка значения DEI（Drop Eligible Indicator）по умолчанию для порта.

Пояснение: Когда пакет не помечен, CFI в теге, добавленном к пакету, является значением DEI по умолчанию для порта.

2. Настройка режима сопоставления очереди на основе заголовка кадра 802.1Q.

Щелкните <Tag Cliass> на рисунке 62, чтобы перейти на страницу настройки режима сопоставления очереди на основе заголовка кадра 802.1Q, как показано на рисунке 63.

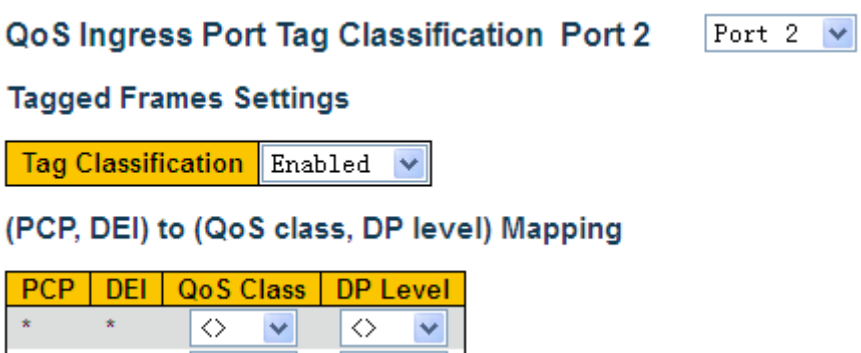


Рисунок 63 Настройка режима сопоставления очереди на основе заголовка кадра 802.1Q.

Tag Classification

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Включить ли режим сопоставления очередей на основе информации заголовка 802.1Q. Этот режим сопоставления очередей имеет более высокий приоритет по сравнению с режимом сопоставления очередей на основе портов.

Предупреждение:

Режим сопоставления очереди на основе информации о заголовке 802.1Q применим только к тегированным пакетам, полученным портом.

(PCP, DEI) to (QoS class, DP level) Mapping

Диапазон: 0~7 (QoS class) 0~1 (DP Level)

По умолчанию: Диапазон значений PCP составляет 0, 1, 2, 3, 4, 5, 6 и 7, которые соответствуют классам QoS 1, 0, 2, 3, 4, 5, 6 и 7. Диапазон значений DEI составляет 0 и 1, которые соответствуют уровням DP 0 и 1.

Функция: Задать сопоставление с (PCP, DEI) на (CoS, DPL) на основе значений PCP и DEI в пакетах.

Описание: Класс QoS эквивалентен значению CoS. Значение CoS определяет очередь для хранения пакетов, а значения CoS 0-7 соответствуют очередям 0-7. После того, как пакет передан коммутатору, коммутатор присваивает пакету значение CoS и DPL. Значение CoS и значение DPL пакета (CoS, DPL) сопоставляются с (PCP, DEI), если полученный пакет тегированный и включена классификация тегов.

Можно выбрать порт для настройки режима сопоставления очередей на основе информации заголовка 802.1Q в правом верхнем углу страницы.

3. Настройка перемаркировки 802.1p показана на рисунке 64.

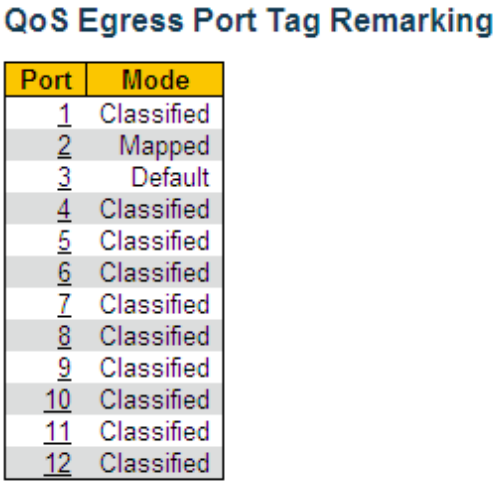


Рисунок 64 Настройка перемаркировки 802.1p

Mode

Варианты: Classified/Mapped/Default

Функция: Отображает режим перемаркировки 802.1p, когда исходящий порт пересылает пакеты. Перемаркировка 802.1p используется для обновления значения PCP и значения DEI в пакетах, когда выходной порт пересылает пакеты.

Предупреждение:

Если пакеты, пересылаемые выходным портом, не помечены, функция перемаркировки 802.1p недоступна.

Щелкните <Port>, чтобы перейти на страницу настройки перемаркировки 802.1p.

- Установите режим перемаркировки 802.1p Classified, как показано на рисунке 65.

Рисунок 65 Настройка режима перемаркировки 802.1p Classified

Tag Remarking Mode

Варианты: Classified/Mapped/Default

По умолчанию: Classified

Функция: Настройка режима перемаркировки 802.1p Classified: Значение PCP и значение DEI в пакетах не обновляются, когда выходной порт пересылает пакеты. Можно выбрать порт для настройки режима перемаркировки 802.1p в правом верхнем углу страницы.

- Настройте режим перемаркировки 802.1p Default, как показано на рисунке 66.

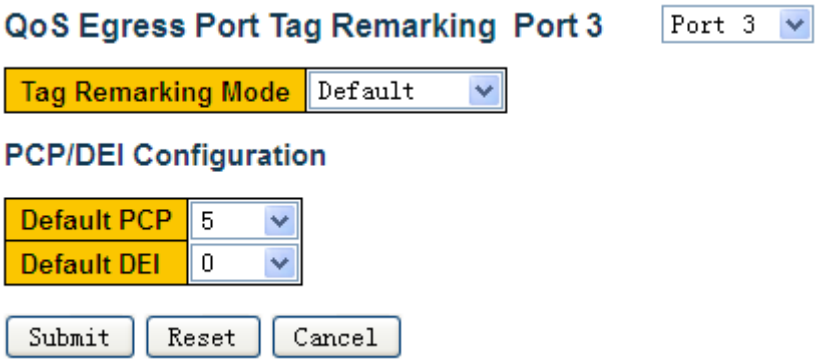


Рисунок 66 Настройка режима перемаркировки 802.1p Default

Tag Remarking Mode

Варианты: Classified/Mapped/Default

По умолчанию: Classified

Функция: Настройка режима перемаркировки 802.1p

По умолчанию: Значение PCP и значение DEI в пакетах обновляются до значений по умолчанию (установленных в нижней части страницы) выходного порта, когда выходной порт пересылает пакеты.

Default PCP

Диапазон: 0~7

По умолчанию: 0

Функция: Задание значения PCP по умолчанию для выходного порта.

Default DEI

Диапазон: 0~1

По умолчанию: 0

Функция: Задание значения DEI по умолчанию для выходного порта.

Можно выбрать порт для настройки режима перемаркировки 802.1p в правом верхнем углу страницы.

- Настройте режим перемаркировки 802.1p Mapped, как показано на рисунке 67.

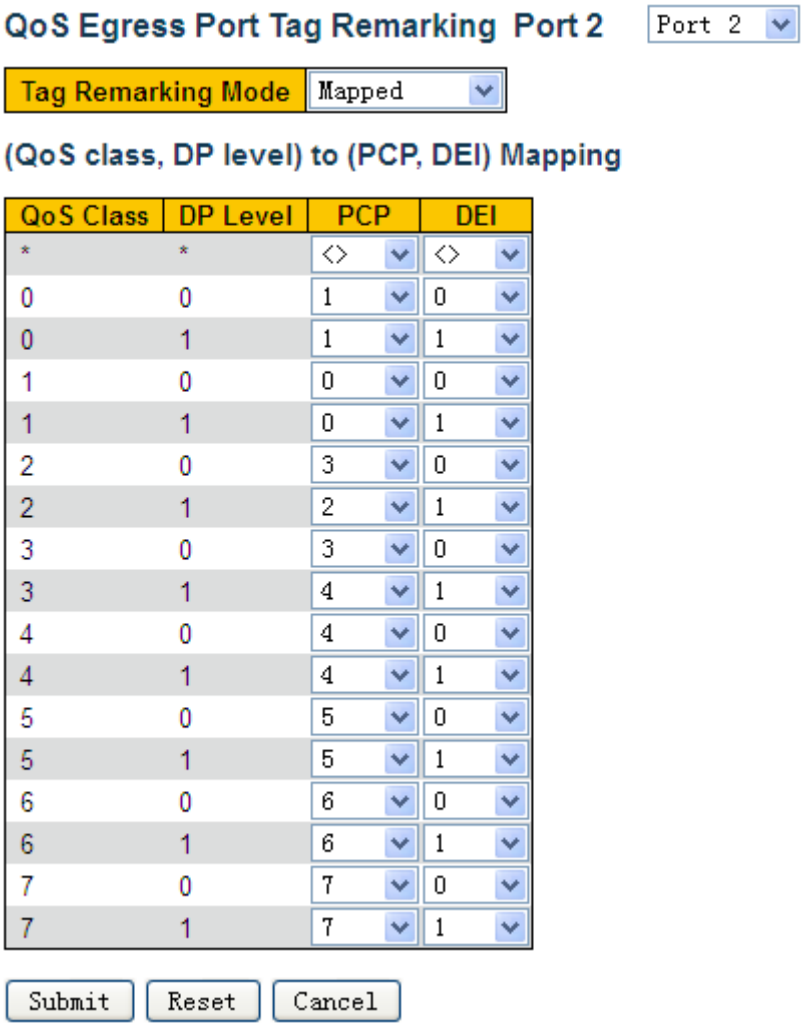


Рисунок 67 Настройка режима перемаркировки 802.1p Mapped

Tag Remarking Mode

Варианты: Classified/Mapped/Default

По умолчанию: Classified

Функция: Настройка режима перемаркировки 802.1p Mapped: Значение PCP и значение DEI в пакетах обновляются до (PCP, DEI), сопоставленного с (CoS, DPL), когда выходной порт пересылает пакеты. Сопоставление настраивается в нижней части страницы.

(QoS class, DP level) to (PCP, DEI) Mapping

Диапазон: 0~7 (PCP) 0~1 (DEI)

По умолчанию: Диапазон классов QoS составляет 0, 1, 2, 3, 4, 5, 6 и 7, которые сопоставляются значениям PCP 1, 0, 2, 3, 4, 5, 6 и 7. Диапазон значений уровня DP составляет 0 и 1, которые сопоставляются значениям DEI 0 и 1.

Функция: Настройка сопоставления (CoS, DPL) и (PCP, DEI) на основе значений CoS и DPL в пакетах.

Можно выбрать порт для настройки режима перемаркировки 802.1p в правом верхнем углу страницы.

4. Включите режим сопоставления очередей на основе DSCP, как показано на рисунке 68.

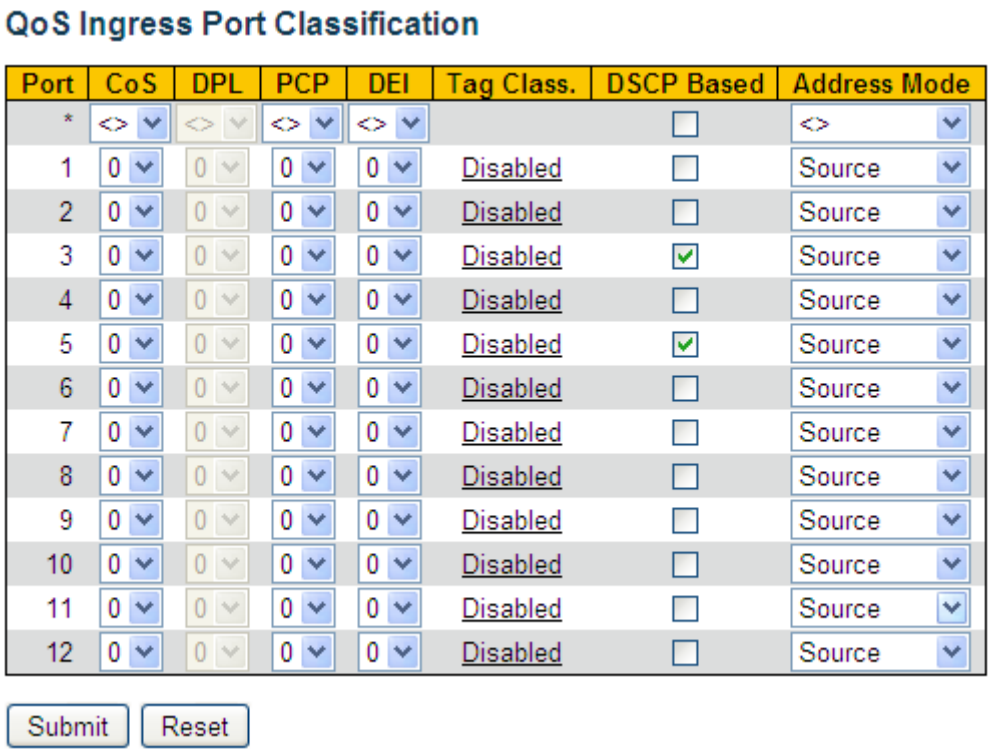


Рисунок 68 Включение режима сопоставления очередей на основе DSCP

DSCP-Based

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Включить ли режим сопоставления очередей на основе DSCP Этот режим сопоставления очередей имеет более высокий приоритет по сравнению с режимом сопоставления очередей на основе информации заголовка 802.1Q.

5. Включите трансляцию DSCP для входного порта и функцию перезаписи DSCP для выходного порта, как показано на рисунке 69.

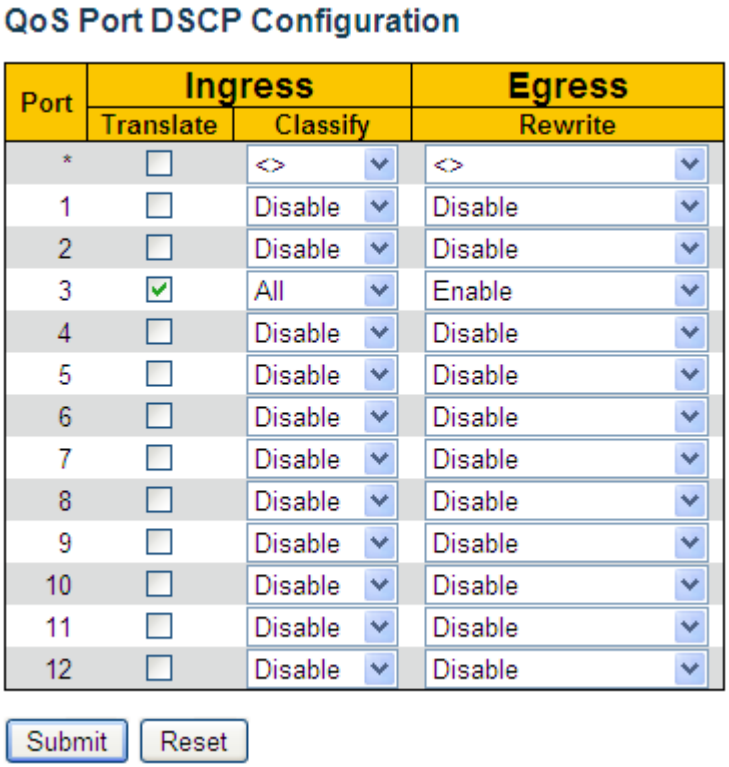


Рисунок 69 Настройка функции DSCP

Translate

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Включение и выключение преобразования значения DSCP в пакете, полученном входным портом. Если установлено значение Enable, значение DSCP преобразуется в соответствии с таблицей преобразования DSCP (столбец Translate на рисунке 71).

Classify

Варианты: Disable/DSCP=0/Selected/All

По умолчанию: Disable

Функция: Выбор перезаписанного значения DSCP для выходного порта, когда для параметра Rewrite установлено значение Enable. Disable: Значение DSCP в пакетах не перезаписывается, когда выходной порт пересылает пакеты.

DSCP=0: Когда выходной порт пересылает пакеты, если значения DSCP в пакетах равны 0, значения DSCP в пакетах перезаписываются в соответствии с классификацией на рисунке 72.

Selected: Когда выходной порт пересылает пакеты, если значения DSCP в пакетах являются выбранным значением (столбец Classify на рисунке 71), значения DSCP в пакетах перезаписываются в соответствии с классификацией на рисунке 72.

All: Когда выходной порт пересылает пакеты, значения DSCP в пакетах перезаписываются в соответствии с классификацией на рисунке 72.

Rewrite

Варианты: Disable/Enable/Remap DP Unaware/Remap DP Aware

По умолчанию: Disable

Функция: Установка режима перезаписи значения DSCP в пакетах, когда выходной порт пересылает пакеты.

Disable: Значения DSCP в пакетах не перезаписывается, когда выходной порт пересылает пакеты.

Enable: Перезапись значений DSCP в пакетах определяется на основе конфигурации классификации, когда выходной порт пересылает пакеты.

Remap DP Unaware: Значения DSCP в пакетах перезаписываются на основе сопоставления (столбец Remap DP0 на рисунке 71) из (DSCP, DPL=0) в DSCP, когда выходной порт пересылает пакеты.

Remap DP Aware: Значения DSCP в пакетах перезаписываются на основе сопоставления (столбцы Remap DP0 и Remap DP1 на рисунке 71) из (DSCP, DPL) в DSCP, когда выходной порт пересылает пакеты.

6. Настройте режим сопоставления очередей на основе DSCP, как показано на рисунке 70.

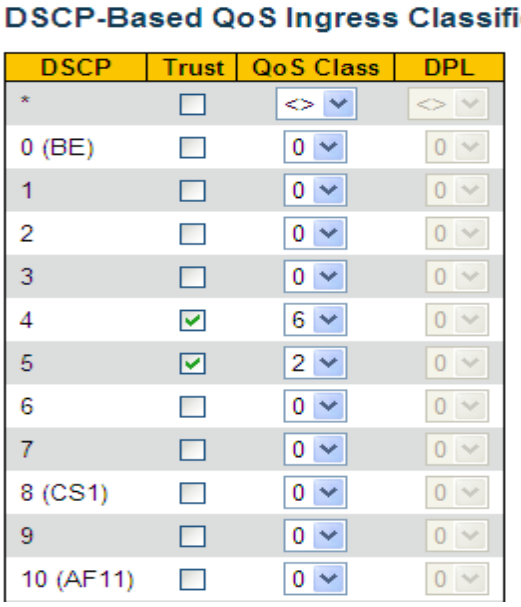


Рисунок 70 Настройка режима сопоставления очередей на основе DSCP

Trust

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Включение и выключение доверенного режима значения DSCP

Предупреждение:

Режим сопоставления очередей на основе DSCP применим только к доверенным значениям DSCP в пакетах, полученных портом.

QoS Class

Диапазон: 0~7

По умолчанию: 0

Функция: Настройка сопоставления DSCP и CoS.

Описание: Класс QoS эквивалентен значению CoS. Значение CoS определяет очередь для хранения пакетов, а значения CoS 0~7 соответствуют очередям 0~7. После того как пакет со значением DSCP, являющимся доверенным значением, передан коммутатору, коммутатор выделяет значение CoS пакету в соответствии с сопоставлением DSCP и CoS.

Предупреждение:

Если для входного порта включено преобразование, коммутатор выделяет значение CoS на основе преобразованного значения DSCP. В противном случае коммутатор выделяет значение CoS на основе исходного значения DSCP в пакетах.

7. Настройка преобразования и перезаписи DSCP показана на рисунке 71.

DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<>	☑	<>	<>
0 (BE)	7	☑	0 (BE)	0 (BE)
1	5	☑	1	1
2	8 (CS1)	☑	2	2
3	3	☐	3	3
4	4	☐	8 (CS1)	4
5	5	☐	9	5
6	6	☐	6	6
7	7	☐	7	7
8 (CS1)	8 (CS1)	☐	8 (CS1)	8 (CS1)
9	9	☐	9	9
10 (AF11)	10 (AF11)	☐	10 (AF11)	10 (AF11)

Рисунок 71 Настройка преобразования и перезаписи DSCP

Translate

Диапазон: 0~63

Функция: Задание таблицы преобразования значений DSCP

Classify

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Когда для параметра Classify установлено значение Selected рисунок 69, этот параметр используется для установки выбранного значения DSCP.

Предупреждение:

Когда для входного порта включено преобразование, выбранное значение DSCP

является значением DSCP после преобразования. В противном случае выбранное значение DSCP является исходным значением DSCP в пакетах.

Remap DP0/ Remap DP1

Диапазон: 0~63

Функция: Настройка сопоставления (DSCP, DPL) и DSCP.

8. Настройте классификацию DSCP, как показано на рисунке 72.

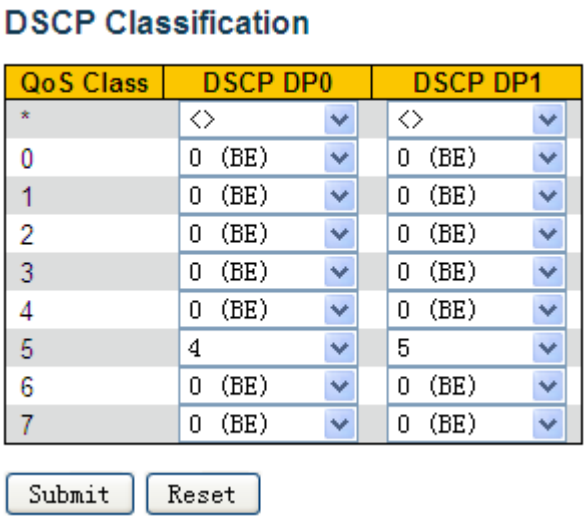


Рисунок 72 Настройка классификации DSCP

DSCP DP0/DSCP DP1

Диапазон: 0~63

Функция: Настройка сопоставления (CoS, DPL) и DSCP. Класс QoS эквивалентен значению CoS. Значение CoS определяет очередь для хранения пакетов, а значения CoS 0-7 соответствуют очередям 0-7.

9. Настройте запись QCL, как показано на рисунке 73.

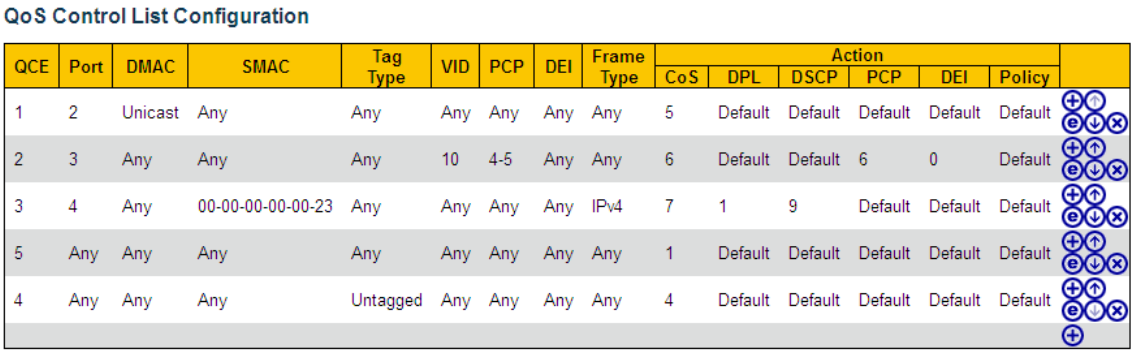


Рисунок 73 Настройка записи QCL

Сопоставление очереди пакетов реализуется путем сопоставления записей QCL. Каждая запись состоит из нескольких условий в логической связи И. Считается, что пакет, полученный портом-участником, соответствует записи QCL только тогда, когда пакет удовлетворяет всем условиям. Записи QCL не зависят друг от друга.

При наличии нескольких записей QCL устройство последовательно сравнивает пакет с записями QCL (сверху вниз). Как только совпадение найдено, действие выполнено, и дальнейшее сравнение не проводится. Click <○+ >, чтобы добавить новую запись QCL;

щелкните <○e >, чтобы редактировать запись QCL; щелкните <○x >, чтобы удалить запись QCL, щелкните <○↑ >, чтобы переместить текущую запись вверх; щелкните <○↓ > чтобы переместить текущую запись вниз.

QCE — это идентификатор записи QCL, который нумеруется на основе временной последовательности создания записи.

10. Настройка параметром записи QCL

- Выберите порт, на котором действует текущая запись QCL, как показано на рисунке 74.

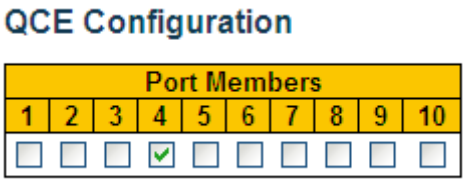


Рисунок 74 Выбор порта

Port members

Функция: Выбор порта, на котором действует текущая запись QCL

По умолчанию все порты являются портами-участниками.

- Настройте параметры записи QCL, как показано на рисунке 75.

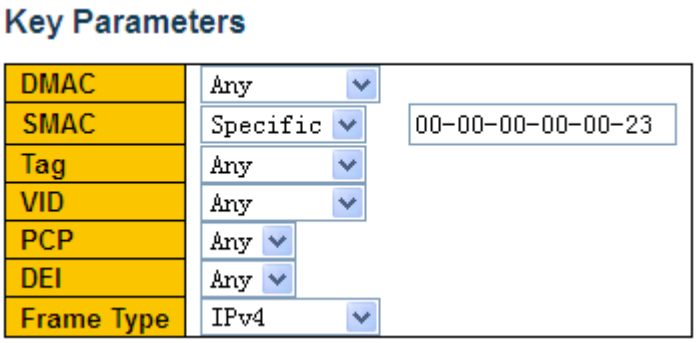


Рисунок 75 Настройка записи QCL

DMAC

Варианты: Any/ Unicast/ Multicast / Broadcast

По умолчанию: Any

Функция: Задание условий для MAC-адреса назначения Когда MAC-адрес назначения в пакете, полученном портом, соответствует настройкам этого параметра, условие успешно выполнено.

SMAC

Варианты: Any/ Specific

По умолчанию: Any

Функция: Задание условий для MAC-адреса источника Если установлено значение Specific, нужно назначить MAC-адрес. Когда MAC-адрес источника в пакете, полученном портом, соответствует настройкам этого параметра, условие успешно выполнено.

Tag

Варианты: Any/ Untagged/ Tagged

По умолчанию: Any

Функция: Задание условий для тегированных пакетов Когда пакет, полученный портом, соответствует настройкам этого параметра, условие успешно выполнено.

VID

Варианты: Any/ Specific（1~4095）/ Range（1~4095）

По умолчанию: Any

Функция: Задание условий для VID. Если установлено значение Specific, нужно назначить значение VID. Если установлено значение Range, нужно назначить диапазон VID. Когда VID в пакете, полученном портом, соответствует настройкам этого параметра, условие успешно выполнено. Этот параметр недоступен, если для параметра Tag задано значение Untagged.

PCP

Варианты: Any/0/1/2/3/4/5/6/7/0-1/2-3/4-5/6-7/0-3/4-7

По умолчанию: Any

Функция: Задание условий для PCP. Когда значение PCP в пакете, полученном портом, соответствует настройкам этого параметра, условие успешно выполнено. Этот параметр недоступен, если для параметра Tag задано значение Untagged.

DEI

Варианты: Any/0/1

По умолчанию: Any

Функция: Задание условий для DEI Когда значение DEI в пакете, полученном портом, соответствует настройкам этого параметра, условие успешно выполнено. Этот параметр недоступен, если для параметра Tag задано значение Untagged.

Frame Type

Варианты: Any/ EtherType/ LLC/ SNAP/ IPv4/ IPv6

По умолчанию: Any

Функция: Выбор типа кадра.

➢ Настройте параметры кадра EtherType, как показано на рисунке 76.

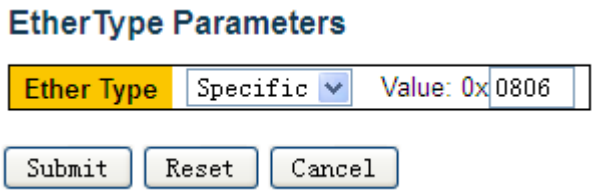


Рисунок 76 Настройка параметров кадра EtherType

EtherType

Варианты: Any/

Specific（0x0600~0xFFFF）

По умолчанию: Any

Функция: Задание условий для типа Ethernet. Если установлено значение Specific, нужно назначить тип Ethernet. Когда пакет Ethernet, полученный портом, соответствует настройкам этого параметра, условие успешно выполнено.

➢ Настройте параметры кадра LLC, как показано на рисунке 77.

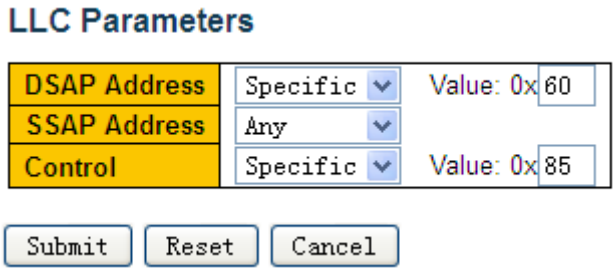


Рисунок 77 Настройка параметров кадра LLC

DSAP Address/SSAP Address/Control

Варианты: Any/Specific（0x00~0xFF）

По умолчанию: Any

Функция: Задание условий для параметров пакета LLC Если для параметра DSAP Address, SSAP Address или Control установлено значение Specific, необходимо ввести конкретное значение. Когда пакет LLC, полученный портом, соответствует настройкам этого параметра, условие успешно выполнено.

➢ Настройте параметры кадра SNAP, как показано на рисунке 78.

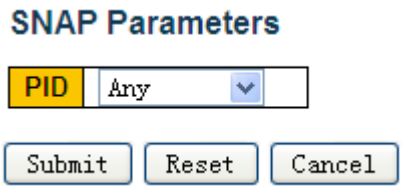


Рисунок 78 Настройка параметров кадра SNAP

PID

Варианты: Any/ Specific（0x0000~0xFFFF）

По умолчанию: Any

Функция: Задание условий для параметров пакета SNAP Если установлено значение Specific, нужно назначить значение PID. Когда PID в пакете SNAP, полученном портом, соответствует настройкам этого параметра, условие успешно выполнено.

➢ Настройте параметры кадра IPv4/ IPv6, как показано на рисунке 79.

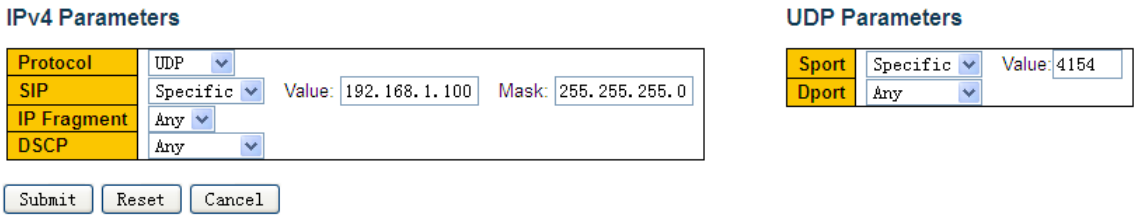


Рисунок 79 Настройка параметров кадра IPv4

Protocol

Варианты: Any/ UDP/ TCP/ Other（0~255）

По умолчанию: Any

Функция: Задание условий для типа протокола пакета IPv4 Если установлено значение UDP или TCP, необходимо установить ID исходного порта и ID порта назначения. Если установлено значение Other, нужно назначить ID протокола. Когда тип протокола в пакете, полученном портом, соответствует настройкам этого параметра, условие успешно выполнено.

Sport/ Dport

Варианты: Any/ Specific（0~65535）/ Range（0~65535）

По умолчанию: Any

Функция: Задание условий для ID исходного порта TCP/UDP и ID порта назначения Если установлено значение Specific, нужно назначить ID порта. Если установлено значение Range, нужно назначить диапазон ID порта.

Когда ID порта в пакете IP, полученном портом, соответствует настройкам этого параметра, условие успешно выполнено.

SIP

Варианты: Any/ Specific

По умолчанию: Any

Функция: Задание условий для IP-адреса источника и маски IP-адреса источника. Если установлено значение Specific, нужно назначить IP-адрес источника и маску IP-адреса источника. Когда SIP в пакете IP, полученном портом, соответствует настройкам этого параметра, условие успешно выполнено.

IP Fragment

Варианты: Any/ Yes/ No

По умолчанию: Any

Функция: Задание условий для для пакета IP-фрагмента. Когда фрагмент в пакете Ipv4, полученном портом, соответствует настройкам этого параметра, условие успешно выполнено.

DSCP

Варианты: Any/ Specific（0~63）/ Range（0~63）

По умолчанию: Any

Функция: Задание условий для значения DSCP. Если установлено значение Specific, нужно назначить значение DSCP. Если установлено значение Range, нужно назначить диапазон DSCP. Когда DSCP в пакете IP, полученном портом, соответствует настройкам этого параметра, условие успешно выполнено.

- Настройте действие QCL, как показано на рисунке 80.

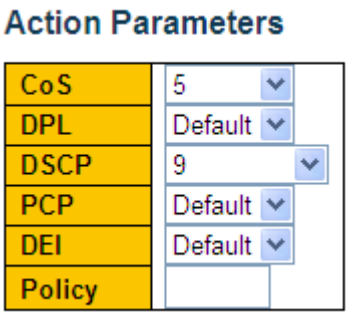


Рисунок 80 Настройка действия QCL

CoS

Варианты: 0~7/ Default

По умолчанию: 0

Функция: Значение CoS определяет очередь для хранения пакетов. Значение CoS находится в диапазоне от 0 до 7, что соответствует очереди от 0 до 7. Значение Default указывает на то, что значение CoS равно 0. Когда пакет, полученный портом, совпадает с записью QCL, коммутатор назначает пакету значение CoS.

DPL

Варианты: Default/ 0/ 1

По умолчанию: Default

Функция: Изменить значение DPL в пакете, полученном портом-участником, на значение этого параметра, если пакет соответствует записи QCL. Значение Default указывает, что значение DPL в пакете не изменяется.

DSCP

Варианты: Default/ 0~63

По умолчанию: Default

Функция: Изменить значение DSCP в пакете, полученном портом-участником, на значение этого параметра, если пакет соответствует записи QCL. Значение Default указывает, что значение DSCP в пакете не изменяется.

PCP

Варианты: Default/ 0~7

По умолчанию: Default

Функция: Изменить значение PCP в пакете, полученном портом-участником, на значение этого параметра, если пакет соответствует записи QCL. Значение Default

указывает, что значение PCP в пакете не изменяется.

DEI

Варианты: Default/ 0/ 1

По умолчанию: Default

Функция: Изменить значение DEI в пакете, полученном портом-участником, на значение этого параметра, если пакет соответствует записи QCL. Значение Default указывает, что значение DEI в пакете не изменяется.

Предупреждение:

Значение PCP и значение DEI в пакете не могут быть изменены по отдельности. То есть значение PCP и значение DEI должны изменяться одновременно или сохранять свои первоначальные значения.

- Просмотрите записи QCL, как показано на рисунке 81.

QoS Control List Status

User	QCE	Port	Frame Type	Action						Conflict
				CoS	DPL	DSCP	PCP	DEI	Policy	
Static	1	2	Any	5	Default	Default	Default	Default	Default	No
Static	2	3	Any	6	Default	Default	6	0	Default	No
Static	3	4	IPv4	7	1	9	Default	Default	Default	No
Static	5	Any	Any	1	Default	Default	Default	Default	Default	No
Static	4	Any	Any	2	Default	Default	Default	Default	Default	No

Рисунок 81 Просмотр записей QCL

Conflict

Варианты: No/Yes

Функция: Отображение статуса конфликта записи QCL. Если ресурсов для создания записи QCL недостаточно, для параметра **Conflict** для этой записи устанавливается значение **Yes**. В противном случае для параметра **Conflict** для этой записи установлено значение **No.**

Щелкните <Resolve Confilct>, чтобы освободить ресурсы, необходимые для конфликтующей записи QCL, чтобы разрешить конфликт ресурсов.

11. Настройте ограничители входящего порта, как показано на рисунке 82.

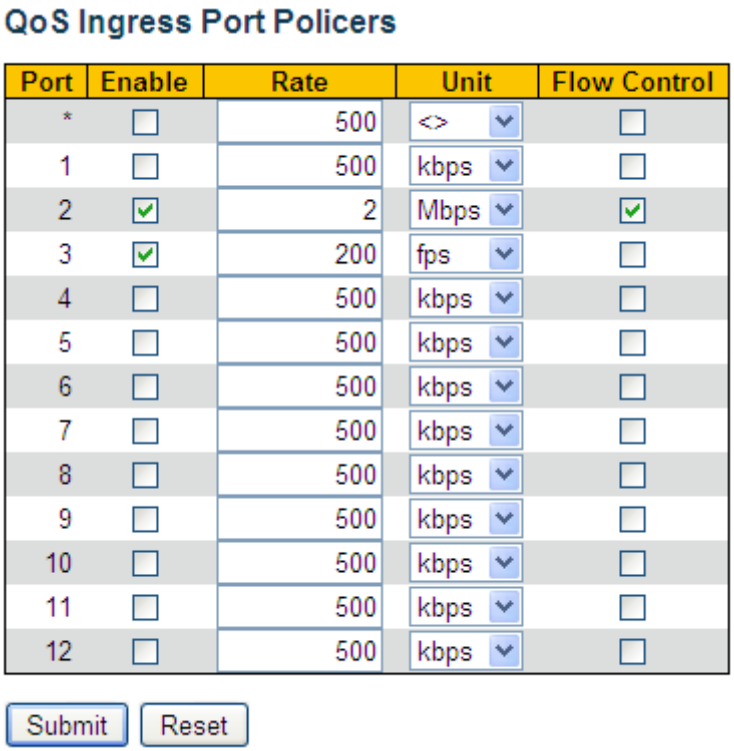


Рисунок 82 Настройка ограничителей входящего порта

Enable

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Включение или выключение ограничителей входящего порта Контроль трафика порта реализуется путем ограничения скорости порта или управления потоком порта.

Rate, Unit

Диапазон: 100~3276700kbps/ 1~3276Mbps/ 100~3276700fps/ 1~3276Kfps

По умолчанию: 500 kbps

Функция: Ограничить скорость пакетов, принимаемых портом. Пакеты, скорость которых больше указанного значения, отбрасываются.

Flow Control

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Включение и выключение управления потоком для порта. После включения управления потоком для порта, когда трафик, полученный портом, превышает

предельное значение, отправитель получает указание замедлить передачу, чтобы предотвратить потерю пакетов с помощью алгоритмов или протоколов.

Примечание:

Предварительным условием для того, чтобы функция управления потоком вступила в Port Configuration (порт должен находиться в состоянии LinkUp).

12. . Настройте ограничители входящего порта, как показано на рисунке 83.

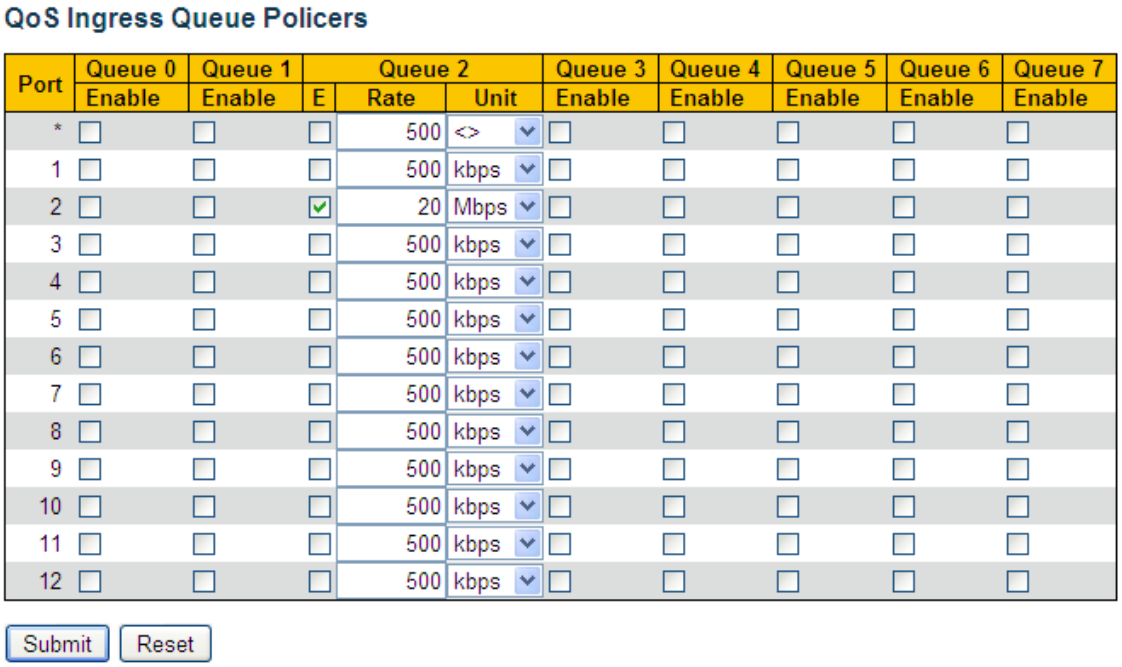


Рисунок 83 Настройка ограничителей входящего порта

Enable (E)

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Включение или выключение ограничителей входящей очереди После включения ограничения трафика для очереди необходимо установить скорость и единицу измерения.

Rate, Unit

Диапазон: 100~3276700kbps/ 1~3276Mbps

По умолчанию: 500 kbps

Функция: Ограничить скорость пакетов, принимаемых очередью порта. Пакеты,

скорость которых больше указанного значения, отбрасываются.

13. . Настройте режим планирования очереди портов, как показано на рисунке 84 и рисунке 85.

QoS Egress Port Schedulers

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	6 Queues Weighted	13%	25%	25%	13%	13%	13%
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-
11	Strict Priority	-	-	-	-	-	-
12	Strict Priority	-	-	-	-	-	-

Рисунок 84 Просмотр режима планирования очереди портов

Щелкните <Port>, чтобы перейти на страницу настройки режима планирования очереди портов.

QoS Egress Port Scheduler and Shapers Port 6

Scheduler Mode: 6 Queues Weighted

Queue Shaper					Queue Scheduler	
Queue	Enable	Rate	Unit	Excess	Weight	Percent
Q7	☐	500	kbps	☐	--	--
Q6	☐	500	kbps	☐	--	--
Q5	☐	500	kbps	☐	20	13%
Q4	☐	500	kbps	☐	20	13%
Q3	☐	500	kbps	☐	20	13%
Q2	☐	500	kbps	☐	40	25%
Q1	☐	500	kbps	☐	40	25%
Q0	☐	500	kbps	☐	20	13%

Рисунок 85 Настройка режима планирования очереди портов

Scheduler Mode

Варианты: Strict Priority/6 Queues Weighted

По умолчанию: Strict Priority

Функция: Настройка режима исходящей очереди для выбранного порта.

Queue Weight

Диапазон: 1~100
По умолчанию: 17

Функция: Настройка значений веса для очереди.

Можно выбрать порт для настройки режима планирования очереди портов в правом верхнем углу страницы.

14. . Настройте шейперы выходного порта, как показано на рисунке 86.

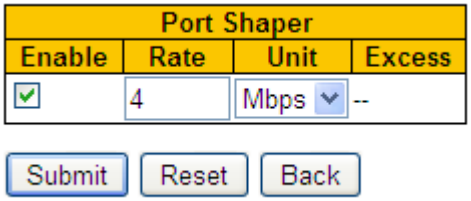


Рисунок 86 Настройка шейперов выходного порта

Enable

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Включение или выключение шейперов выходного порта. Формирование трафика порта осуществляется ограничением скорости порта.

Rate, Unit

Диапазон: 100~3281943kbps/ 1~3281Mbps

По умолчанию: 500 kbps

Функция: Ограничить скорость пакетов, отправляемых портом. Пакеты, скорость которых больше указанного значения, отбрасываются.

Щелкните <Back>, чтобы закрыть страницу конфигурации и вернуться на предыдущую страницу конфигурации.

Можно выбрать порт для настройки формирования трафика в правом верхнем углу страницы.

15. Настройте шейперы очереди, как показано на рисунке 87.

Queue Shaper					Queue Scheduler	
Queue	Enable	Rate	Unit	Excess	Weight	Percent
Q7	☐	500	kbps	☐	--	--
Q6	☑	4	Mbps	☐	--	--
Q5	☑	8	Mbps	☑	20	13%
Q4	☐	500	kbps	☐	20	13%
Q3	☐	500	kbps	☐	20	13%
Q2	☐	500	kbps	☐	40	25%
Q1	☐	500	kbps	☐	40	25%
Q0	☐	500	kbps	☐	20	13%

Рисунок 87 Настройка шейперов очереди

Enable

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Включение или выключение шейперов очереди

Rate, Unit

Диапазон: 100~3281943kbps/ 1~3281Mbps

По умолчанию: 500 kbps

Функция: Ограничить скорость пакетов, отправляемых очередью порта. Пакеты, скорость которых больше указанного значения, отбрасываются.

Щелкните <Back>, чтобы закрыть страницу конфигурации и вернуться на предыдущую страницу конфигурации.

Можно выбрать порт для настройки формирования трафика в правом верхнем углу страницы.

16. Настройте управление штормом порта, как показано на рисунке 88.

Global Storm Policer Configuration

Frame Type	Enable	Rate	Unit
Unicast	☑	1	kfps
Multicast	☐	1	fps
Broadcast	☐	1	fps

Submit Reset

Рисунок 88 Настройка управления штормом порта

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

Enable

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Включение или выключение управления штормом порта

Rate, Unit

Диапазон: 1~1024000fps/ 1~1024kfps

По умолчанию: 1fps

Функция: Настройка порогового значения для ограничения скорости порта. Пакеты, превышающие пороговое значение, будут отброшены.

17. Просмотрите счетчики очереди, как показано на рисунке 89.

Queuing Counters

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	1328270	897	0	0	0	0	0	0	0	0	0	0	0	0	0	6852
2	236399	1092247	0	0	0	0	0	0	0	0	0	0	0	0	0	693
3	284	222112	0	0	0	0	0	0	0	0	0	0	0	0	0	13096
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Рисунок 89 Просмотр счетчиков очереди

Отображение количества пакетов, которые каждая очередь отправляет/получает.

Щелкните <port> для перехода на страницу подробной статистики порта, как показано на рисунке 61.

8.4 Пример типовой конфигурации

Как показано на рисунке 90, порты 1-5 пересылают сообщения в порт 6. Среди них

Пакеты, полученные портом 1, имеют статус Untag, а пакеты, поступающие в порт 1, сопоставляются с очередью 2.

Значение PCP принятого пакета порта 2 равно 0, значение DEI равно 1, а пакеты,

поступающие на порт 2, сопоставляются с очередью 3.

Значение DSCP принятого пакета порта 3 равно 4, а пакеты, поступающие в порт 3,

сопоставляются с очередью 6.

Порт 4 отображает все полученные пакеты с исходным MAC-адресом 00-00-00-00-00-

23 в очередь 5 и изменяет значение DSCP в этих пакетах на 9 для пересылки.

Значение DSCP принятого пакета порта 5 равно 5, а пакеты, поступающие в порт 5,

сопоставляются с очередью 2.

Порт 6 использует режим планирования SP+WRR.

Процесс настройки коммутатора:

1. Установите значение CoS порта 1 равным 2, как показано нарисунке 62.
2. Включите режим классификации тега порта 2 и сопоставьте (PCP=0, DEI=1) с CoS=3, как показано на рисунке 63.
3. Включите сопоставление на основе DSCP портов 3 и 5, как показано нарисунке 68.
4. Установите значения 4 и 5 DSCP как «доверенные» и сопоставьте значение 4

DSCP с очередью 6, а значение 5 DSCP с очередью 2, как показано на рисунке

70.

5. Настройте запись QCL порта 4, как показано на рисунке 74.
6. Настройте параметры записи QCL: установите MAC-адрес источника на 00-00-00-

00-00-23 и тип кадра на IPv4., как показано на рисунке 75.

7. Настройте параметры действия записи QCL: установите значение CoS на 5 и

значение DSCP на 9, как показано на рисунке 80.

8. Настройте режим планирования очереди порта 6 на 6 Queues Weighted, вес

очереди от Q0~Q5 до 20, 40, 40, 20, 20, 20., как показано на рисунке 80.

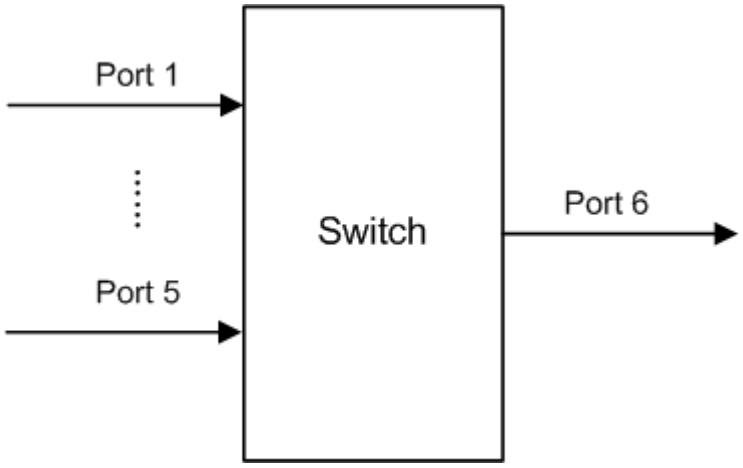


Рисунок 90 Пример настройки QoS

Пакеты порта 1 и порта 5 попадают в очередь 2, пакеты порта 2 попадают в очередь 3, пакеты порта 3 попадают в очередь 6, пакеты порта 4 попадают в очередь 5.

Очередь 6 и очередь 7 используют режим планирования со строгим приоритетом, а очереди с 0 по 5 используют режим планирования WRR. Данные в очереди 6 обрабатываются первыми, когда очередь 6 пуста, данные в очередях с 0 по 5 планируются по весовому соотношению.

Вес очереди 20, 40, 40, 20, 20, 20. Таким образом, полоса пропускания, выделенная пакетам во входной очереди 2, составляет 40（/20+40+40+20+20+20）=25%, полоса пропускания, выделенная пакетам во входной очереди 3 – 20/（20+40+40+20+20+20）=13%, полоса пропускания, выделенная пакетам во входной очереди 5, составляет 20（/20+40+40+20+20+20）=13%. Среди них пакеты портов 1 и 5. оба помещаются в очередь 2, поэтому они пересылаются в соответствии с правилом «первым пришел — первым обслужен» (FIFO), но общая доля пропускной способности порта 1 и порта 5 должна составлять 25 %.

9 Безопасность

9.1 Управление пользователями

9.1.1 Введение

Чтобы избежать проблем с безопасностью, вызванных незаконными пользователями, коммутаторы данной серии обеспечивают иерархическое управление пользователями. Коммутатор обеспечивает различные права работы в зависимости от уровня пользователя, удовлетворяя разнообразные требования к управлению доступом. Доступны три уровня пользователя, как показано в таблице 5.

Таблица 5 Уровень пользователей

Уровень пользователей	**Уровень привилегий**	**Описание**
Guest	5~9	Самый низкий уровень, гостевые пользователи могут только просматривать конфигурацию коммутатора.
System	10~14	Средний уровень, пользователи с уровнем System имеют определенные права для доступа и настройки. Пользователи с уровнем System не могут получить доступ к следующим функциям: управление пользователями, обновление программного обеспечения, перезагрузка, загрузка параметров по умолчанию и передача файлов.
Admin	15	Самый высокий уровень, пользователи с уровнем Admin имеют права на выполнение всех функций.

9.1.2 Настройка через веб-интерфейс

1. Создайте нового пользователя, как показано на рисунке 91.

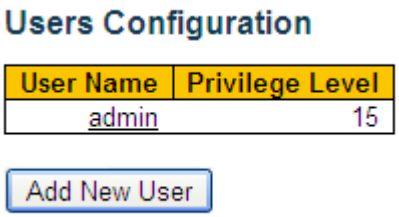


Рисунок 91 Создание нового пользователя

Нажмите <Add New User>, чтобы настроить пользователя другого уровня.

Коммутатор поддерживает до 20 пользователей.

2. Настройте уровень доступа пользователя, как показано на рисунке 92.

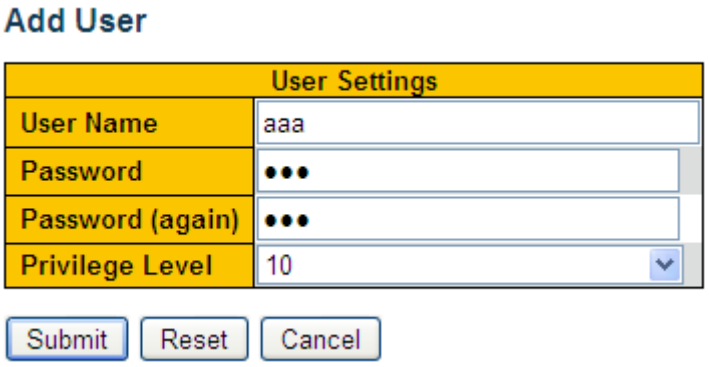


Рисунок 92 Настройка уровень доступа пользователя

User Name

Диапазон: 1~31 символ

Функция: Настройка имени пользователя

Password

Диапазон: 1~31 символ

Функция: Настройка пароля, который будет использоваться при доступе текущего пользователя к коммутатору.

Password (again)

Диапазон: 1~31 символ

Функция: Подтверждение пароль доступа.

Уровень привилегий

Диапазон: 0~15

Функция: Настройте уровень пользователя, пользователи разных уровней имеют разные права.

3. Просмотрите список пользователей, как показано на рисунке 93.

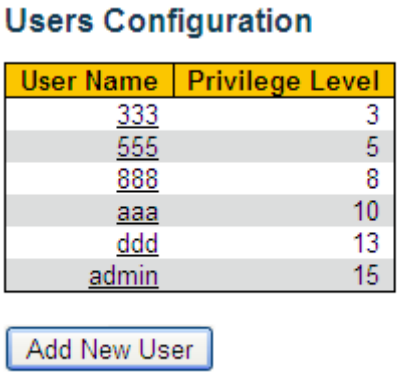


Рисунок 93 Список пользователей

Щелкните <User Name>, чтобы изменить настройки текущего пользователя.

4. Отредактируйте настройки пользователя, как показано на рисунке 94.

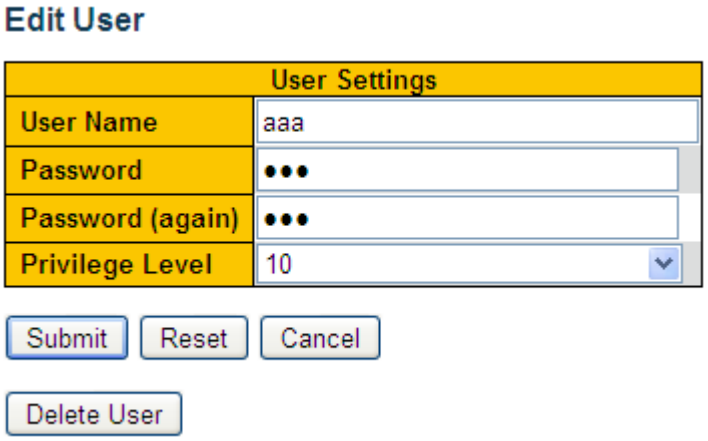


Рисунок 94 Изменение настроек пользователя

Можно изменить пароль пользователя и уровень привилегий. Щелкните <Delete User>, чтобы удалить текущего пользователя.

Примечание:

- Пользователя по умолчанию admin удалить нельзя.
- Уровень привилегий пользователя admin принудительно установлен на 15, изменить его нельзя; но пароль по умолчанию (123) можно изменить.

5. Настройте уровень привилегий групп, как показано на рисунке 95.

Privilege Level Configuration

Group Name	Privilege Level			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
ALARM	5	10	5	10
Debug	15	15	15	15
DHCP	5	10	5	10
DHCPv6_Client	5	10	5	10
Diagnostics	5	10	5	10
DT-RING	5	10	5	10
IP	5	10	5	10
IPMC_Snooping	5	10	5	10
LACP	5	10	5	10
LINKCHECK	5	10	5	10
LLDP	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
Maintenance	15	15	15	15
Ports	5	10	1	10
QoS	5	10	5	10
RMirror	5	10	5	10
Security	5	10	5	10
SNTP	5	10	5	10
Spanning_Tree	5	10	5	10
System	5	10	1	10
VLANs	5	10	5	10

Submit Reset

Рисунок 95 Настройка уровня привилегий групп

Когда уровень привилегий пользователя такой же или выше, чем уровень привилегий группы, пользователь может получить доступ к группе или настроить ее. Право доступа или настройки зависит от уровня привилегий пользователя.

9.2 Настройка аутентификации при входе

Настройте режим доступа к коммутатору, режим аутентификации и порядок аутентификации, как показано на рисунке 96.

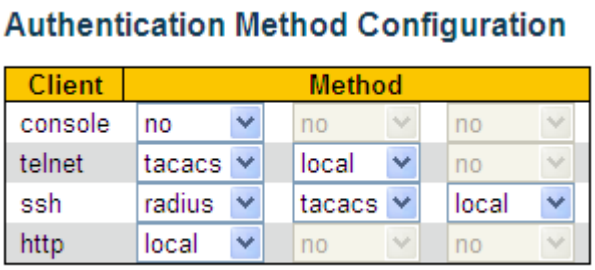


Рисунок 96 Настройка аутентификации при входе

Client

Варианты: console/telnet/ssh/http Функция:

Выбор режима доступа к коммутатору.

Method 1/Method 2/Method 3

Варианты: no/local/tacacs/radius

По умолчанию: local

Функция: Методы слева направо method 1, method 2 и method 3. Выбор порядка аутентификации. Сначала выполняется метод аутентификации method 1. Если аутентификация не удалась, применяется метод аутентификации method 2. Если и метод аутентификации 1, и метод аутентификации 2 неудачны, выполняется метод аутентификации method 3.

Описание: **no** означает, что аутентификация отключена и вход в систему невозможен. local означает использование имени пользователя и пароля, установленных в локальном компьютере, для выполнения аутентификации. **tacacs** означает использование имени пользователя и пароля, установленных на сервере TACACS+ для аутентификации.

Предупреждение:

Если для method 1 и method 2 выбрано значение tacacs/radius, рекомендуется настроить method 3 как local. Это позволит клиенту управления войти в систему через локального пользователя, если ни один из настроенных удаленных серверов аутентификации не активен.

radius означает использование имени пользователя и пароля, установленных на сервере RADIUS для аутентификации.

9.3 Настройка SSH

9.3.1 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 командную строку для настройки коммутаторов.

Серия коммутаторов поддерживает функцию SSH-сервера и позволяет подключаться нескольким пользователям SSH, которые удаленно входят в коммутатор через SSH.

9.3.2 Реализация

Чтобы осуществить безопасное SSH подключение, сервер и клиент должны пройти следующие пять этапов:
Этап согласования версий: в настоящее время SSH состоит из двух версий: SSH1 и SSH2. Обе стороны должны согласовать версию для использования.
Этап согласования ключей и алгоритмов. SSH поддерживает несколько типов алгоритмов шифрования. Обе стороны должны согласовать, какой алгоритм будет использоваться.
Этап аутентификации: клиент SSH отправляет на сервер запрос на аутентификацию, после чего сервер должен аутентифицировать клиента.
Этап запроса сеанса: после прохождения аутентификации клиент отправляет запрос на сеанс к серверу.
Этап сеанса: после передачи запроса на сеанс клиент и сервер начинают обмен данными.

9.3.3 Настройка через веб-интерфейс

1. Включите протокол SSH, как показано на рисунке 97.

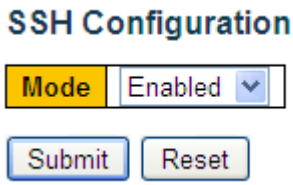


Рисунок 97 Включение протокола SSH

Mode

Варианты: Enable/Disable

По умолчанию: Enable

Функция: Включение/отключение протокола SSH Если протокол включен, коммутатор работает как сервер SSH.

9.3.4 Пример типовой конфигурации

Хост работает как SSH-клиент для установления локального соединения с коммутатором, как показано на Рисунке 98.

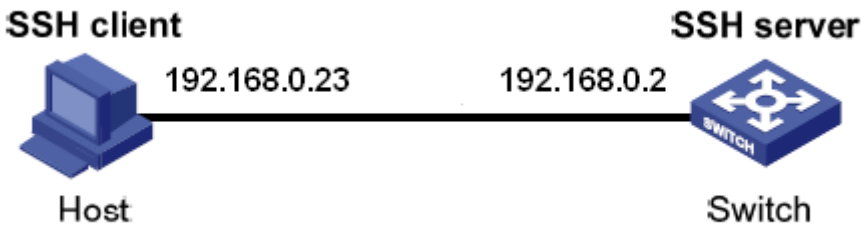


Рисунок 98 Пример настройки SSH

1. Включите протокол SSH, как показано на рисунке 97.

2. Установите соединение с сервером SSH. Сначала запустите программу PuTTY.exe, как показано на рисунке 99; введите IP-адрес SSH-сервера 192.168.0.2 в поле Host Name (или IP address).

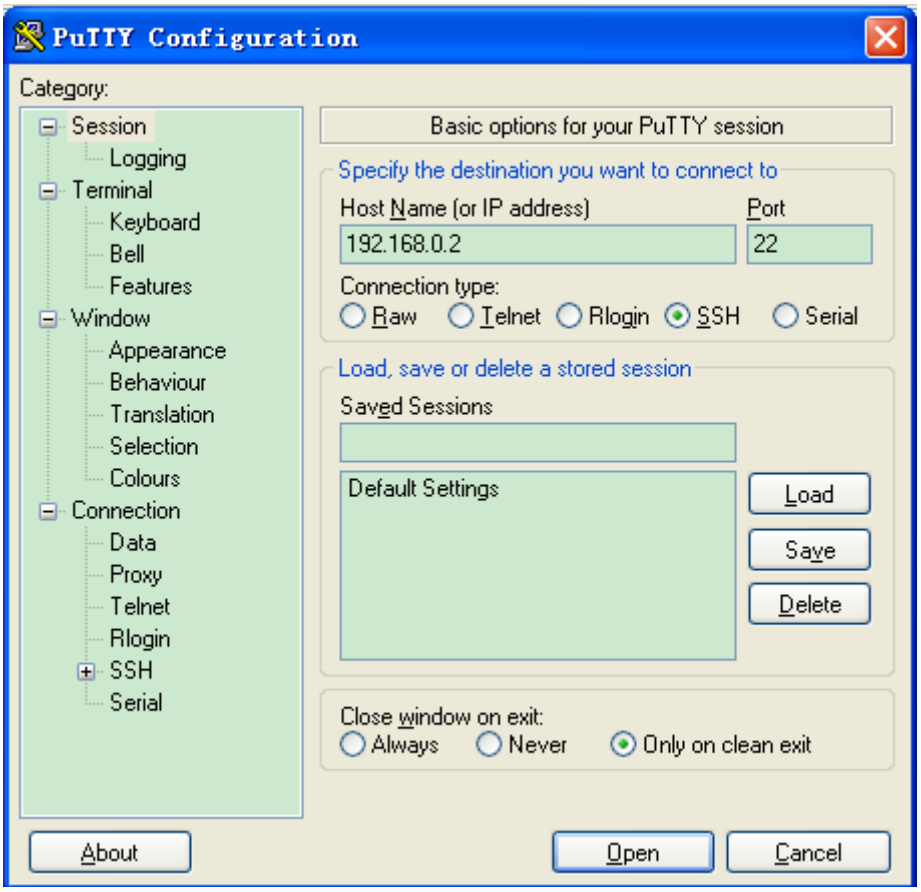


Рисунок 99 Настройка клиента SSH

3. Щелкните кнопку <Open>, появится предупреждающее сообщение, показанное на рисунке 100, щелкнитекнопку<是(Y)>.

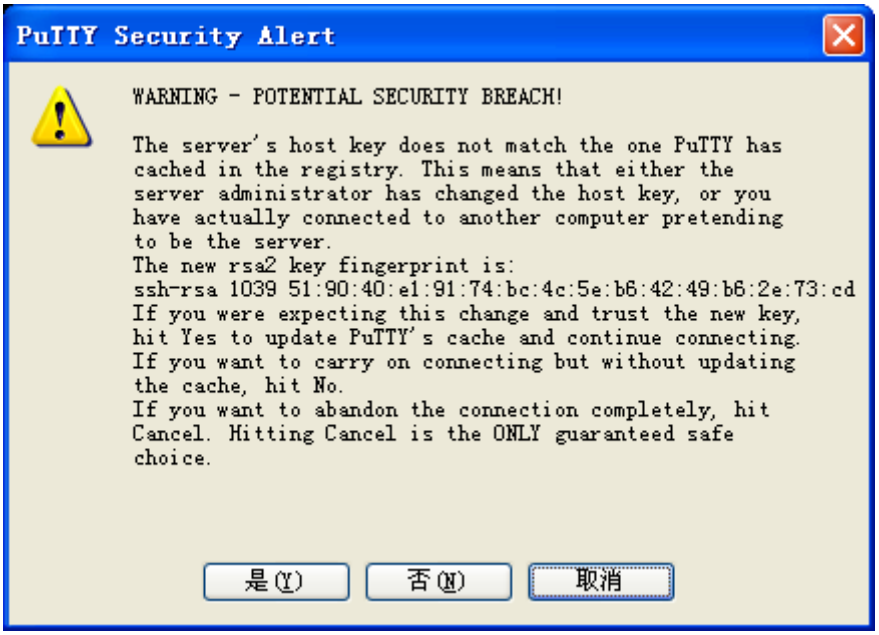


Рисунок 100 Предупреждающее сообщение

4. Введите имя пользователя admin и пароль 123, чтобы войти в интерфейс настрйки коммутатора, как показано на рисунке 101.

Рисунок 101 Интерфейс входа в SSH-аутентификацию

9.4 Настройка SSL

9.4.1 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 данных в сети.

После того, как коммута

9.4.2 Настройка через веб-интерфейс

1. Включите протокол HTTPS, как показано на рисунке 102.

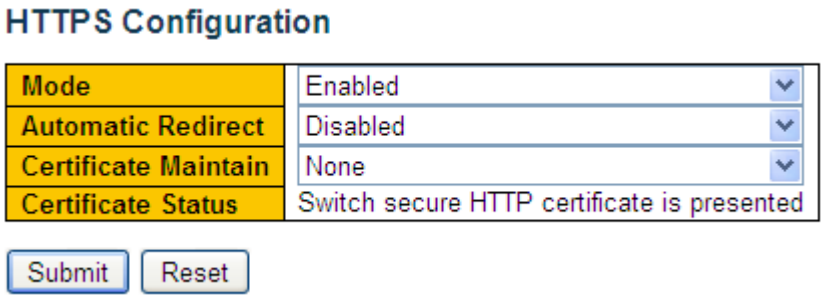


Рисунок 102 Включение протокола HTTPS

Mode

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Включение или выключение протокола HTTPS. После включения HTTPS пользователи могут использовать адрес http://ip и безопасное подключение https://ip-адрес для доступа к коммутатору.

Automatic Redirect

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Enabled означает, что пользователи могут использовать безопасное подключение https://*ip-адрес* для доступа к коммутатору. Disabled означает, что пользователи могут использовать адрес http://ip и безопасное подключение https://ip-адрес для доступа к коммутатору. Параметр Automatic Redirect можно настроить только если для Mode выбрано значение enabled.

Certificate Maintain

Варианты:

None/Delete/Upload/Generate

По умолчанию: None

Функция: Управление сертификатом HTTPS. Параметр Certificate Maintain можно настроить только если для Mode выбрано значение disabled. **Delete** используется для удаления существующего сертификата HTTPS из коммутатора. **Upload** используется для загрузки правильного сертификата HTTPS в коммутатор с помощью веб-браузера или URL-адреса. **Generate** указывает, что коммутатор автоматически создает правильный сертификат HTTPS.

Certificate Status

Варианты: Switch secure HTTP certificate is presented/Switch secure HTTP certificate is not presented/Switch secure HTTP certificate is generating

Функция: Отображение статуса сертификата HTTPS для коммутатора. **Switch secure HTTP certificate is presented** означает, что сертификат доступен. В этом случае можно войти на веб-страницу коммутатора через HTTPS. **Switch secure HTTP certificate is not presented** означает, что в коммутаторе нет доступного сертификата. В этом случае нельзя войти на веб-страницу коммутатора через HTTPS. **Switch secure HTTP certificate is generating** указывает, что сертификаты HTTPS создаются.

2. Создайте сертификат HTTPS, как показано на рисунке 103.

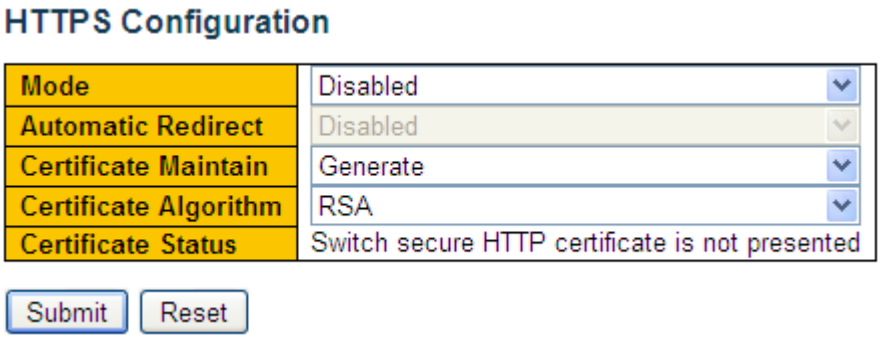


Рисунок 103 Создание сертификата

Certificate Algorithm

Варианты: RSA/DSA

По умолчанию: RSA

Функция: Выбор алгоритма для создания сертификата HTTPS.

3. Загрузите сертификат HTTPS, как показано на рисунке 104 и рисунке 105.

Рисунок 104 Загрузка сертификата – браузер

Рисунок 105 Загрузка сертификата – URL

Pass Phrase

Функция: Используется для шифрования сертификата.

Certificate Upload

Варианты: Web

Browser/URL

По умолчанию: Web Browser

Функция: Выбор метода загрузки сертификата.

File Upload

Функция: Выбор файла сертификата HTTPS, сохраненного локально.

URL

Функция: Настройка пути хранения файла сертификата HTTPS. Поддерживаются протоколы HTTP, HTTPS, TFTP и FTP, формат::

http://10.10.10.10:80/new_image_path/new_image.dat или

FTP://username:password@10.10.10.10/new_image_path/new_image.dat.

4. Когда сертификат HTTPS представлен в коммутаторе, введите имя пользователя и пароль для успешного входа в коммутатор через HTTPS.

9.5 Управление доступом

9.5.1 Введение

Для управления доступом к коммутатору можно настроить записи доступа, чтобы ограничить хосты, которые могут получить доступ к коммутатору, а также режим доступа. Можно настроить не более 16 записей доступа. Хост, который соответствует любой из записей доступа, может успешно получить доступ к коммутатору.

9.5.2 Настройка через веб-интерфейс

1. Настройте запись управления доступом, как показано на рисунке 106.

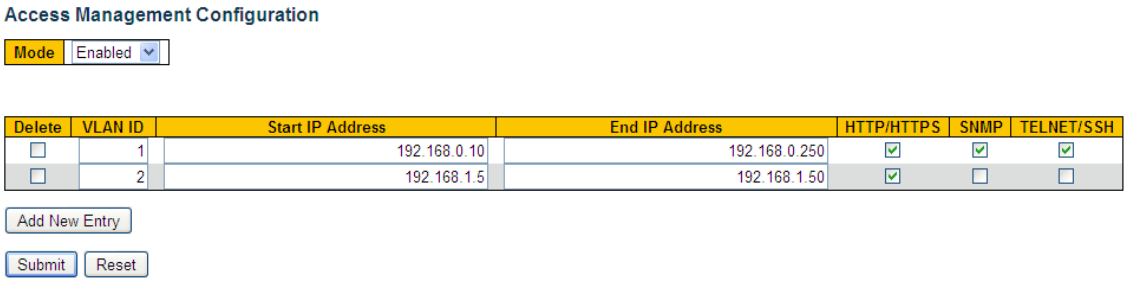


Рисунок 106 Настройка записи управления доступом

Mode

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Включение или выключение управления доступом. Disable: доступ к коммутатору не ограничен.

VLAN ID

Диапазон: 1~4094
Функция: Настройка VLAN ID записи управления доступом.

Start IP Address/End IP Address

Функция: Настройка диапазона IP-адресов записи управления доступом.

HTTP/HTTPS

Функция: При выборе HTTP/HTTPS, хост, который соответствует идентификатору VLAN и IP-адресу в записи доступа, может получить доступ к коммутатору через HTTP/HTTPS.

SNMP

Функция: При выборе SNMP, хост, который соответствует идентификатору VLAN и IP-адресу в записи доступа, может получить доступ к коммутатору через SNMP.

TELNET/SSH

Функция: При выборе TELNET/SSH, хост, который соответствует идентификатору VLAN и IP-адресу в записи доступа, может получить доступ к коммутатору через TELNET/SSH.

Нажмите <Add New Entry>, чтобы настроить запись управления доступом.

Коммутатор поддерживает не более 16 записей управления доступом.

2. Просмотрите статистику управления доступом, как показано на рисунке 107.

Access Management Statistics Auto-refresh ☐ Refresh Clear

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	513	513	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	46	46	0
SSH	0	0	0

Рисунок 107 Просмотр статистики управления доступом

3. Настройте таймауты для режимов доступа к коммутатору, как показано на рисунке 108.

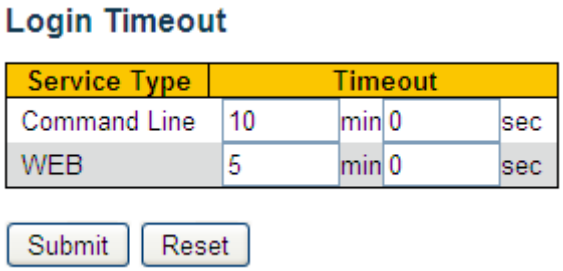


Рисунок 108 Настройка таймаутов для режимов доступа к коммутатору

Timeout

Диапазон: (0~1440) мин (0~3600) с

По умолчанию: 10 мин для командной строки, 5 мин для веб-интерфейса

Функция: Настройка времени ожидания входа пользователя и времени отключения. Отсчет времени начинается, когда пользователь завершит все настройки, и система автоматически выйдет из режима доступа, когда время истечет. Когда время установлено на 0, пользовательская функция тайм-аута и отключения выключена. В этом случае сервер не будет определять, истекло ли время входа пользователя в систему, и поэтому пользователь не выйдет из текущего режима входа.

9.6 SNMP v1/SNMP v2c

9.6.1 Введение

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

9.6.2 Реализация

SNMP использует 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 управления сетью SNMP.

Агент — это процесс в управляемых сетевых устройствах. Он получает и обрабатывает пакеты запросов от NMS. Когда возникает сигнал тревоги, агент сообщает об этом в NMS. NMS является средством управления сетью SNMP, а агент управляется сетью 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 упреждающе сообщает об этом в NMS с помощью пакета Trap.

9.6.3 9.6.3 Пояснения

Эта серия коммутаторов поддерживает SNMP v2c. SNMP v2c совместим с SNMPv1. SNMP v1 использует для аутентификации имя сообщества. Имя сообщества действует как пароль, ограничивая доступ NMS к агентам. Если имя сообщества, переносимое пакетом SNMP, не подтверждается коммутатором, запрос завершается неудачно и возвращается сообщение об ошибке.

SNMP v2c также использует для аутентификации имя сообщества. Он совместим с SNMPv1 и расширяет функционал SNMP v1.

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

9.6.4 Знакомство с MIB

Любой управляемый ресурс называется управляемым объектом. Management Information Base (MIB) хранит управляемые объекты. Она 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 109 показаны взаимоотношения между NMS, агентом и MIB.

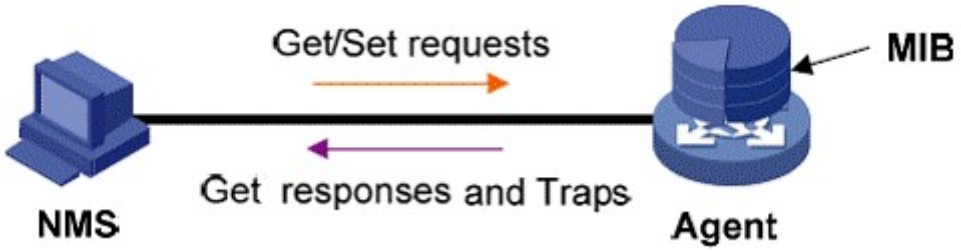


Рисунок 109 Взаимоотношения между NMS, агентом и MIB

MIB определяет древовидную структуру. Узлы дерева являются управляемыми объектами. Каждый узел имеет уникальный идентификатор Object Identifier (OID), который указывает расположение узла в структуре MIB. Как показано на рисунке 110, OID объекта A – 1.2.1.1.

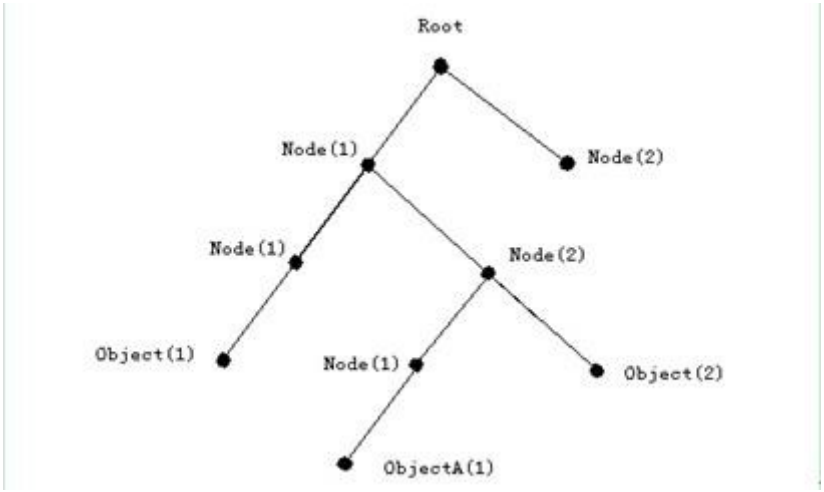


Рисунок 110 Структура MIB

9.6.5 Настройка через веб-интерфейс

1. Включите протокол SNMP и выберите версию SNMP, как показано на рисунке 111.

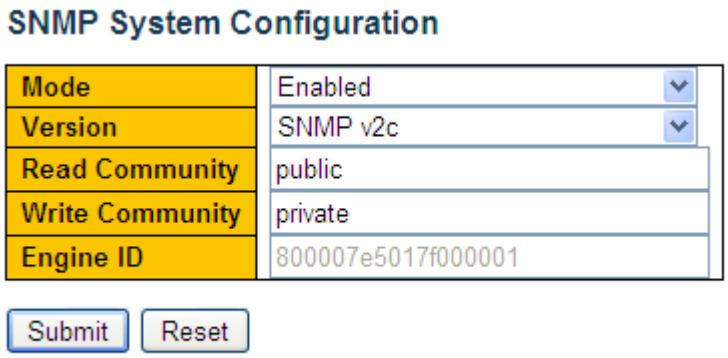


Рисунок 111 Включение протокола SNMP и выбор версии SNMP

Mode

Варианты: Enable/Disable

По умолчанию: Enable

Функция: Включение/выключение SNMP.

Version

Варианты: SNMP v1/SNMP v2c/SNMP v3

По умолчанию: SNMP v2c

Функция: Выбор версии SNMP. SNMP v2c совместим с SNMPv1; SNMP v3 совместим с SNMPv1 и SNMP v2c.

Read-only Community

Диапазон: 0~255 символов

По умолчанию: public

Функция: Задание имени сообщества «Только чтение».

Описание: Информация MIB коммутатора может быть прочитана только в том случае, если имя сообщества, передаваемое пакетом SNMP, совпадает с именем, настроенным на коммутаторе.

Read&write Community

Диапазон: 0~255 символов

По умолчанию: private

Функция: Задание имени сообщества «Чтение-запись».

Описание: Информация MIB коммутатора может быть прочитана и записана только в том случае, если имя сообщества, передаваемое пакетом SNMP, совпадает с именем, настроенным на коммутаторе.

2. Настройте глобальный режим Trap, как показано на рисунке 112.

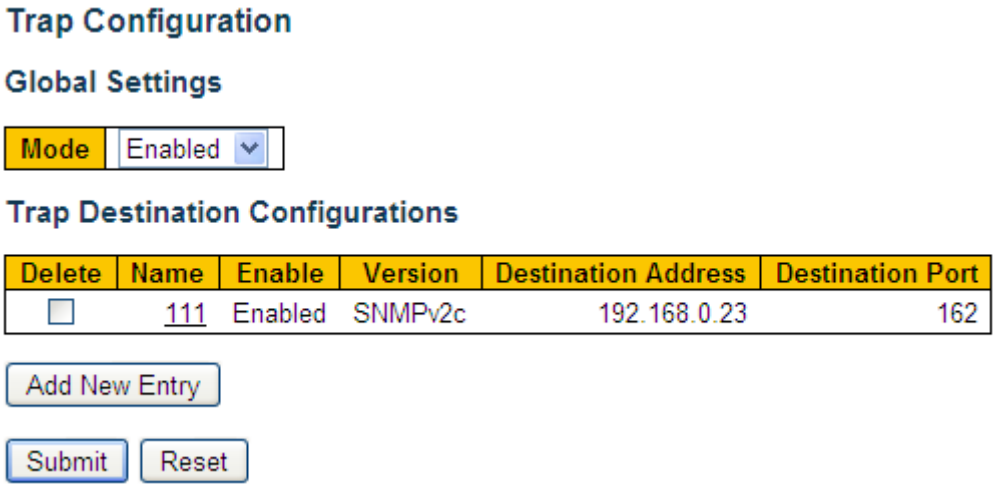


Рисунок 112 Настройка глобального режим Trap

Mode

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Включение/выключение глобального режим Trap.

Щелкните <Add New Entry>, чтобы настроить запись Trap. Коммутатор поддерживает не более 4 записей Trap. Щелкните <Name>, чтобы изменить запись Trap.

3. Настройте запись Trap, как показано на рисунке 113.

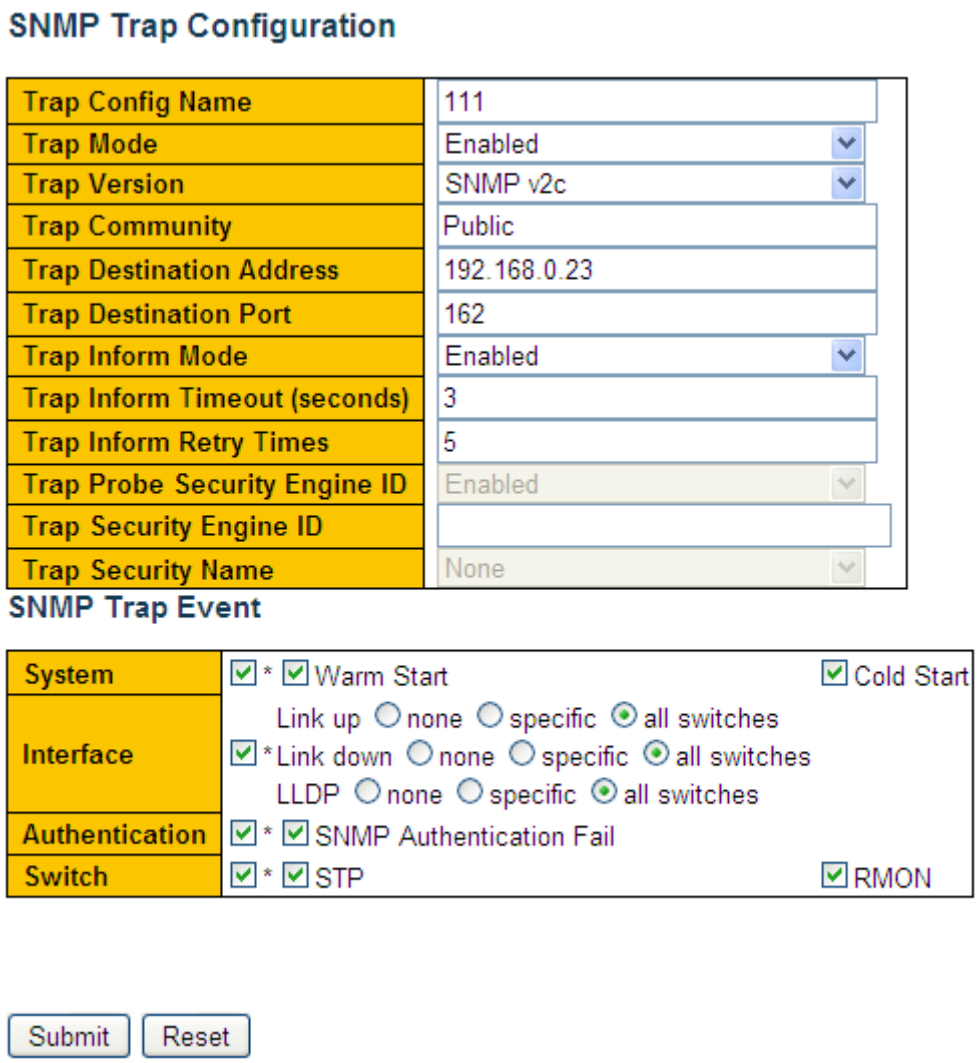


Рисунок 113 Настройка записи Trap

Trap Config Name

Диапазон: 1~255 символов

Функция: Настройка имени записи Trap.

Trap Mode

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Включение/выключение записи Trap. После включения режима Trap коммутатор может отправить сообщение Trap в NMS.

Trap Version

Варианты: SNMP v1/SNMP v2c/SNMP v3

По умолчанию: SNMP v2c

Функция: Задание версии пакетов Trap, отправляемых с коммутатора на сервер.

Trap Community

Диапазон: 0~255 символов

По умолчанию: public

Функция: Настройка сообщества, переносимого сообщением Trap.

Trap Destination Address

Формат: A.B.C.D

Функция: Настройка адреса сервера для приема сообщений Trap.

Trap Destination Port

Диапазон: 1~65535

По умолчанию: 162

Функция: Настройка номера порта для отправки сообщений Trap.

Trap Inform Mode

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Отправлять ли ответ коммутатору после того, как сервер получит trap-пакет.

Trap Inform Timeout

Диапазон: 0~2147 с

По умолчанию: 3 с

Функция: Настройка времени ожидания для отправки пакетов с сообщениями Trap. После отправки пакета на сервер коммутатор повторно передает пакет с сообщениями Trap, если он не получает ответа от сервера в течение данного периода.

Trap Inform Retry Times

Диапазон: 0~255

По умолчанию: 5

Функция: Настройка времени ожидания для отправки пакетов с сообщениями Trap. Если накопленное количество раз передачи превышает значение этого параметра, а сервер еще не отвечает, считается, что передача trap-пакета не удалась.

Warm Start/ Cold Start

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: включение/выключение передачи пакетов с сообщениями Trap при выполнении «горячего»/«холодного» старта коммутатора.

Link up/ Link down

Варианты: none/specific/all switches

По умолчанию: none

Функция: Настройка передачи пакетов с сообщениями Trap при изменении статуса порта.

LLDP

Варианты: none/specific/all switches

По умолчанию: none

Функция: Настройка передачи пакетов Trap протокола обнаружения канального

уровня (LLDP) при изменении статуса соседа.

SNMP Authentication Fail

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Настройка отправки сообщений Trap при ошибке аутентификации SNMP.

STP

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Настройка отправки сообщений Trap при изменении статуса STP.

9.6.6 Пример типовой конфигурации

Управляющий сервер SNMP подключается к коммутатору через Ethernet. IP-адрес управляющего сервера 192.168.0.23, а IP-адрес коммутатора 192.168.0.2. NMS отслеживает и управляет агентом через SNMP v2c, а также считывает и записывает информацию узла MIB агента. Когда агент неисправен, он упреждающе отправляет пакеты Trap в NMS, как показано на рисунке 114.

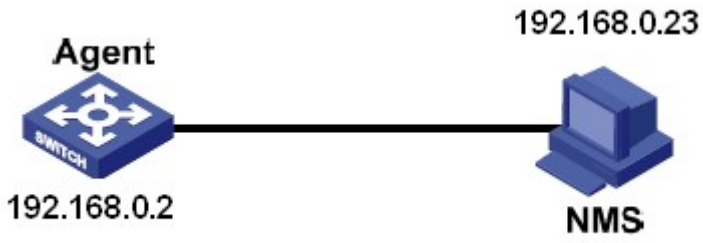


Рисунок 114 Пример конфигурации

Настройка агента:

1. Включите состояние SNMP и v2c; настройте права доступа сообщества Read only – public и сообщества Read and write – private, как показано на рисунке 111.

2. Настройте глобальный режим Trap, как показано на рисунке 112.

3. Создайте запись Trap 111, включите режим Trap; установите версию trap SNMP v2c, IP-адрес назначения 192.168.0.23. Выберите систему, интерфейс, аутентификацию и все сообщения Trap для коммутатора, а также установите настройки по умолчанию для других параметров, как показано на рисунке 113.

При необходимости отслеживание и управление агентами запустите соответствующее программное обеспечение для управления в NMS, например, Kyvision, разработанное Kyland.

Подробные сведения о работе Kyvision приведены в *Руководстве пользователя Kyvision*.

9.7 SNMPv3

9.7.1 Введение

SNMP v3 обеспечивает механизм аутентификации модели безопасности на основе пользователей (USM). Можно 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.

Чтобы обеспечить связь между NMS и агентом, их версии SNMP должны совпадать.

Для агента можно настроить разные версии SNMP, чтобы он мог использовать разные версии для связи с разными NMS.

9.7.2 Реализация

SNMP v3 предоставляет четыре таблицы конфигурации. Каждая таблица может содержать 16 записей. Эти таблицы определяют, могут ли конкретные пользователи получать доступ к информации MIB.

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

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

Таблица просмотра относится к информации просмотра MIB, которая указывает информацию MIB, к которой могут обращаться пользователи. Представление MIB может содержать все узлы определенного поддерева MIB (то есть пользователям разрешен доступ ко всем узлам поддерева MIB) или не содержать ни одного из узлов определенного поддерева MIB (то есть пользователям не разрешен доступ ни к одному из узлов поддерева MIB).

Можно определить права доступа MIB в таблице доступа по имени группы, модели безопасности и уровню безопасности.

9.7.3 Настройка через веб-интерфейс

1. Включите протокол SNMP и выберите версию SNMP, как показано на рисунке 115.

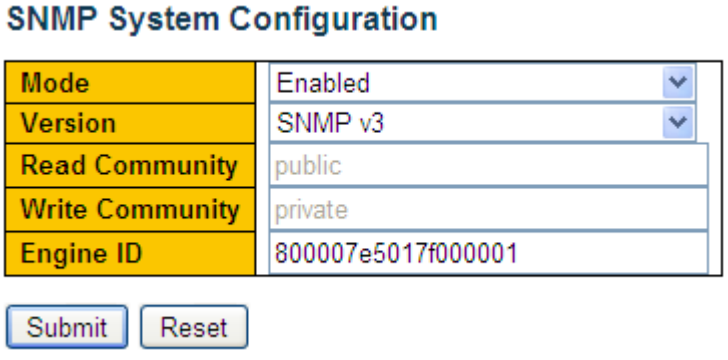


Рисунок 115 Включение протокола SNMP и выбор версии SNMP

Mode

Варианты: Enable/Disable

По умолчанию: Enable

Функция: Включение/выключение SNMP.

Version

Варианты: SNMP v1/SNMP v2c/SNMP v3

По умолчанию: SNMP v2c

Функция: Выбор версии SNMP. SNMP v2c совместим с SNMP v1; SNMP v3 совместим с SNMPv1 и SNMP v2c.

Engine ID

Диапазон: Engine ID – это набор из четного числа шестнадцатеричных цифр, которые не может содержать только 0 или только F. Цифр может быть от 10 до 64.

Функция: Настройка Engine ID для системы SNMP v3. При изменении Engine ID пользователи, соответствующие идентификаторам устройств в таблице пользователей, удаляются.

2. Настройте глобальный режим Trap, как показано на рисунке 116.

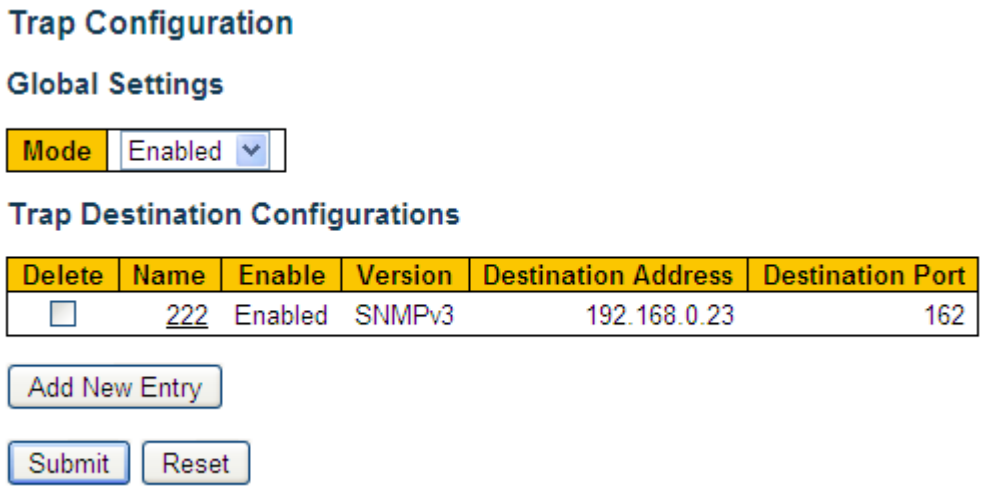


Рисунок 116 Настройка глобального режим Trap

Mode

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Включение/выключение глобального режим Trap.

Щелкните <Add New Entry>, чтобы настроить запись Trap. Коммутатор поддерживает не более 4 записей Trap. Щелкните <Name>, чтобы изменить запись Trap.

3. Настройте запись Trap, как показано на рисунке 117.

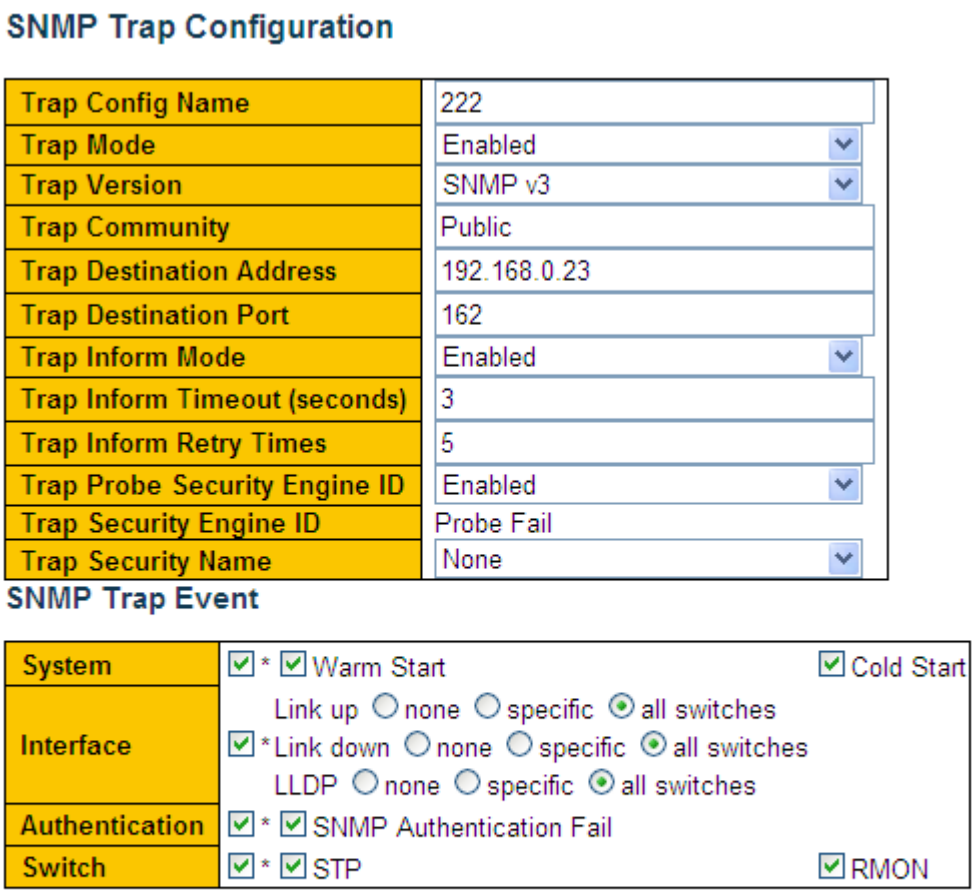


Рисунок 117 Настройка записи Trap

Trap Config Name

Диапазон: 1~255 символов

Функция: Настройка имени записи Trap.

Trap Mode

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Включение/выключение записи Trap. После включения режима Trap коммутатор может отправить сообщение Trap в NMS.

Trap Version

Варианты: SNMP v1/SNMP v2c/SNMP v3

По умолчанию: SNMP v2c

Функция: Задание версии пакетов Trap, отправляемых с коммутатора на сервер.

Trap Community

Диапазон: 0~255 символов

По умолчанию: public

Функция: Настройка сообщества, переносимого сообщением Trap.

Trap Destination Address

Формат: A.B.C.D

Функция: Настройка адреса сервера для приема сообщений Trap.

Trap Destination Port

Диапазон: 1~65535

По умолчанию: 162

Функция: Настройка номера порта для отправки сообщений Trap.

Trap Inform Mode

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Отправлять ли ответ коммутатору после того, как сервер получит trap-пакет.

Trap Inform Timeout

Диапазон: 0~2147 с

По умолчанию: 3 с

Функция: Настройка времени ожидания для отправки пакетов с сообщениями Trap. После отправки пакета на сервер коммутатор повторно передает пакет с сообщениями Trap, если он не получает ответа от сервера в течение данного периода.

Trap Inform Retry Times

Диапазон: 0~255

По умолчанию: 5

Функция: Настройка времени ожидания для отправки пакетов с сообщениями Trap.

Если накопленное количество раз передачи превышает значение этого параметра, а сервер еще не отвечает, считается, что передача trap-пакета не удалась.

Trap Probe Security Engine ID

Варианты: Enable/Disable

По умолчанию: Enable

Функция: Настройка идентификатора механизма безопасности, передаваемый в пакетах Trap SNMP v3. Если для него установлено значение Enabled, коммутатор автоматически проверяет и получает идентификатор Engine ID. Если для него установлено значение Disabled, идентификатор механизма безопасности Engine ID получается из значения Trap Security Engine ID. **Trap Probe Security Engine ID**

Диапазон: Engine ID – это набор из четного числа шестнадцатеричных цифр, которые не может содержать только 0 или только F. Цифр может быть от 10 до 64.

Функция: Настройка Trap Security Engine ID, переносимого сообщением Trap.

Warm Start/ Cold Start

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: включение/выключение передачи пакетов с сообщениями Trap при выполнении «горячего»/»холодного» старта коммутатора.

Link up/ Link down

Варианты: none/specific/all switches

По умолчанию: none

Функция: Настройка передачи пакетов с сообщениями Trap при изменении статуса порта.

LLDP

Варианты: none/specific/all switches

По умолчанию: none

Функция: Настройка передачи пакетов Trap LLDP при изменении статуса соседа.

SNMP Authentication Fail Варианты:

Enable/Disable

По умолчанию: Disabled

Функция: Настройка отправки сообщений Trap при ошибке аутентификации SNMP.

STP

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Настройка отправки сообщений Trap при изменении статуса STP.

4. Настройте сообщество, как показано на рисунке 118.

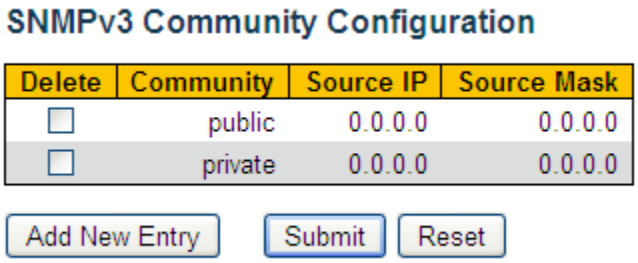


Рисунок 118 Настройка сообщества

Сообщество

Диапазон: 1~32 символа

Функция: Задание имени сообщества на стороне коммутатора

Если выбран SNMP v3, можно задать имя сообщества, чтобы разрешить системе управления сетью (NMS) доступ к коммутатору через SNMPv1 и SNMPv2. В этом случае имя сообщества в NMS должно совпадать с именем на коммутаторе. Права доступа для имени сообщества зависят от конфигурации таблицы групп и таблицы доступа.

Source IP

Формат: A.B.C.D

Функция: Настройка IP-адреса NMS

Source Mask

Функция: Network означает, что можно настроить 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. IP-адрес NMS определяется параметрами Source IP и Source Mask.

Щелкните <Add New Entry>, чтобы настроить сообщества. Коммутатор поддерживает не более 16 сообществ.

Примечание:

По умолчанию существуют имена сообществ Public и Private. Нет ограничений по IP-адресу в NMS

4. Настройте таблицу пользователей, как показано на рисунке 119.

SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
☐	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None
☐	800007e5017f000001	1111	Auth, Priv	MD5	••••••••	DES	••••••••
☐	800007e5017f000001	2222	Auth, Priv	SHA	••••••••	AES	••••••••

Add New Entry | Submit | Reset

Рисунок 119 Настройка таблицы пользователей SNMP v3

Engine ID

Диапазон: Engine ID – это набор из четного числа шестнадцатеричных цифр, которые не может содержать только 0 или только F. Цифр может быть от 10 до 64.

Функция: Задание Engine ID пользователя. Если Engine ID пользователя отличается от Engine ID системы SNMPv3, пользователь в настоящее время неэффективен.

User Name

Диапазон: 1~32 символа

Функция: Создание имени пользователя.

Security Level

Варианты: NoAuth,NoPriv/Auth,NoPriv/Auth,Priv

Функция: Настройка уровня безопасности текущего пользователя.

Описание: NoAuth,NoPriv указывает, что ни аутентификация, ни шифрование не требуются. Auth,NoPriv указывает, что требуется аутентификация, но не требуется шифрование. Auth,Priv указывает, что требуется и аутентификация, и шифрование.

Authentication Protocol

Варианты: MD5/SHA

Функция: Выбор алгоритма аутентификации. Протокол аутентификации и пароль аутентификации должны быть установлены, когда уровень безопасности установлен на Auth, NoPriv или NoAuth, Priv.

Authentication Password

Диапазон: 8~32 символа (MD5) 8~40 символов (SHA)

Функция: Создание пароля аутентификации

Privacy Protocol

Варианты: DES/AES

Функция: Выбор протокола шифрования. Протокол конфиденциальности и пароль конфиденциальности должны быть установлены, когда уровень безопасности установлен на Auth, Priv.

Privacy Password

Диапазон: 1~32 символа

Функция: Создание пароля шифрования.

Щелкните <Add New Entry>, чтобы настроить запись пользователя. Поддерживается не более 16 пользователей.

NOTE

Примечание:

По умолчанию в коммутаторе существует пользователь default_user и уровень безопасности NoAuth, NoPriv.

5. Настройте таблицу групп, как показано на рисунке 120.

SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
☐	v1	public	default_ro_group
☐	v1	private	default_rw_group
☐	v2c	public	default_ro_group
☐	v2c	private	default_rw_group
☐	usm	default_user	default_rw_group
☐	usm	1111	group
☐	usm	2222	group

Add New Entry Submit Reset

Рисунок 120 Настройка таблицы групп SNMP v3

Security Model

По умолчанию: v1/v2/usm

Описание: Выбор модели безопасности текущей группы (версия SNMP). SNMP v3 использует модель безопасности на основе пользователей (USM).

Security Name

Диапазон: все существующие сообщества/имена пользователей, 1~32 символа

Функция: Настройка имени безопасного пользователя. Если используется модель безопасности v1/v2, имя должно совпадать с именем Community. Если используется модель безопасности v1/v2, имя должно совпадать с именем пользователя в таблице пользователей.

Group Name

Диапазон: 1~32 символа

Функция: Настройка имени таблицы группы, пользователи с одинаковым именем группы принадлежат к одной группе.

Щелкните <Add New Entry>, чтобы настроить таблицу группы. Поддерживается не более 16 групп.

Примечание:

По умолчанию в коммутаторе существуют следующие групповые таблицы: {v1,private,default_rw_group}, {v2c,public,default_ro_group}, {v2c,private,default_rw_group}, {usm,default_user,default_rw_group}.

6. Настройте таблицу представления, как показано на рисунке 121.

SNMPv3 View Configuration

Delete	View Name	View Type	OID Subtree
☐	default_view	included	.1
☐	view1	included	.1.3.6.1.2.1.1.1

Add New Entry | Submit | Reset

Рисунок 121 Настройка таблицы представления SNMP v3

View Name

Диапазон: 1~32 символа

Функция: Настройка имени представления

View Type

Варианты: 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 Subtree**

Функция: Дерево MIB, указанное OID корневого узла дерева.

Щелкните <Add New Entry>, чтобы настроить таблицу представлений.

Поддерживается не более 16 записей.

Примечание:

По умолчанию в коммутаторе существует представление default_view, и это представление охватывает все узлы в поддереве

7. Настройте таблицу доступа, как показано на рисунке 122.

SNMPv3 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
☐	default_ro_group	any	NoAuth, NoPriv	default_view	None
☐	default_rw_group	any	NoAuth, NoPriv	default_view	default_view
☐	group	usm	Auth, NoPriv	default_view	None

Add New Entry | Submit | Reset

Рисунок 122 Настройка таблицы доступа SNMP v3

Group Name

Диапазон: все существующие имена групп, 1~32 символа

Функция: Пользователи в группе имеют одинаковые права доступа.

Security Model

Варианты: any/v1/v2/usm

Функция: Задание модели безопасности (т. е. номера версии SNMP), используемой при доступе текущей группы к коммутатору. SNMPv3 принимает модель безопасности на основе пользователя (USM), и значение any указывает, что может быть принята любая модель безопасности. Имя группы и значение Security Model в таблице доступа должны совпадать с таковыми в таблице групп.

Security Level

Варианты: NoAuth,NoPriv/Auth,NoPriv/Auth,Priv

Функция: Настройка уровня безопасности текущей группы.

Описание: NoAuth,NoPriv указывает, что ни аутентификация, ни шифрование не требуются. Auth,NoPriv указывает, что требуется аутентификация, но не требуется шифрование. Auth,Priv указывает, что требуется и аутентификация, и шифрование. Когда требуется аутентификация/шифрование, пользователь может получить доступ к указанной информации MIB только в том случае, если протокол аутентификации/шифрования и пароль аутентификации/шифрования идентичны настроенным в пользовательской таблице.

Уровни безопасности: NoAuth,NoPriv, Auth,NoPriv и Auth,Priv в порядке возрастания. Доступ к содержимому с более низким уровнем безопасности разрешен с более высоким уровнем безопасности.

Например, если и протокол аутентификации/шифрования, и пароль аутентификации/шифрования верны, уровень безопасности настроен как Auth, NoPriv, к содержимому можно успешно получить доступ с уровнями безопасности Auth,NoPriv и Auth,Priv, но нельзя получить доступ с уровнями безопасности NoAuth,NoPriv.

Read View Name

Варианты: default_view/None/all existing view names

Функция: Задание имени представления «Только чтение».

Write View Name

Варианты: default_view/None/all existing view names

Функция: Задание имени представления «Запись».

Щелкните <Add New Entry>, чтобы настроить таблицу доступа. Поддерживается не более 16 записей доступа.

Примечание:

По умолчанию в коммутаторе существуют следующие таблицы доступа: NoAuth,NoPriv, default_view, None} and {default_rw_group, any, NoAuth,NoPriv, default_view, default_view}.

9.7.4 Пример типовой конфигурации

Управляющий сервер SNMP подключается к коммутатору через Ethernet. IP-адрес управляющего сервера 192.168.0.23, а IP-адрес коммутатора 192.168.0.2. Пользователь 1111 и пользователь 2222 управляют Агентом через SNMP v3. Уровень безопасности установлен на AuthNoPriv, и коммутатор может выполнять операцию только для чтения со всей информацией об узле Агента. При возникновении тревоги агент заранее отправляет сообщения trap v3 в NMS, как показано на рисунке 123.

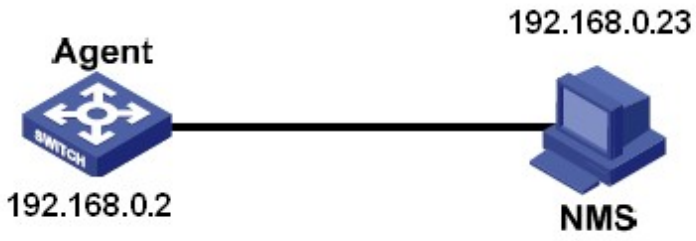


Рисунок 123 Пример конфигурации SNMP v3

Настройка агента:

1. Включите протокол SNMP v3, как показано на рисунке 115.

2. Настройте таблицу пользователей SNMP v3.

Задайте имя пользователя 1111, уровень безопасности Auth, Priv, протокол аутентификации MD5, пароль аутентификации aaaaaaaa, протокол конфиденциальности DES и пароль конфиденциальности xxxxxxxx.

Задайте другое имя пользователя 2222, уровень безопасности Auth, Priv, протокол аутентификации SHA, пароль аутентификации bbbbbbbb, протокол конфиденциальности AES и пароль конфиденциальности yyyyyyyy, как показано на рисунке 119.

3. Создайте группу, установите модель безопасности usm и добавьте пользователей 1111 и 2222 в группу, как показано на рисунке 120.

4. Настройте таблицу доступа SNMP v3.

Задайте имя группы group, модель безопасности usm, уровень безопасности Auth,NoPriv, значение default_view для параметра read view, значение None для параметра write view, как показано на рисунке 122.

5. Включите глобальный режим Trap, как показано на рисунке 116.

6. Создайте запись trap 222, включите режим trap; установите версию trap SNMP v3, IP-

адрес назначения 192.168.0.23. Выберите систему, интерфейс, аутентификацию и все сообщения Trap для коммутатора, а также установите настройки по умолчанию для других параметров, как показано на рисунке 117.

При необходимости отслеживание и управление агентами запустите соответствующее программное обеспечение для управления в NMS.

9.8 RMON

9.8.1 Введение

Основанный на архитектуре SNMP, удаленный мониторинг сети (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.

9.8.2 Группы RMON

RMON (RFC2819) определяет несколько групп RMON. Устройства серии поддерживают группу статистики, группу истории, группу событий и группу сигналов тревоги в общедоступной MIB.

- Группа статистики

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.

- Группа истории

Группа истории 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.

- Группа событий

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 обрабатываются следующими способами:

Log: регистрирует события и соответствующую информацию в таблице журнала событий.

Trap: отправляет сообщение Trap в NMS и информирует NMS о событии.

Trap: отправляет сообщение Trap в NMS и информирует NMS о событии. None: указывает на отсутствие действий.

- Группа тревоги

Управление сигналами тревоги RMON может отслеживать указанные переменные аварийных сигналов тревоги. 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 событие роста значения. Когда значение переменной тревоги меньше или равно нижнему пределу, инициируется событие падения значения. Сигналы тревоги будут обрабатываться в соответствии с определением события.

Предупреждение:

Если выбранное значение переменной тревоги превышает пороговое значение несколько раз в одном и том же направлении, то событие тревоги срабатывает только в первый раз.

Таким образом, попеременно генерируются сигналы повышения и падения значения.

9.8.3 Настройка через веб-интерфейс

1. Настройте таблицу статистики, как показано на рисунке 124.

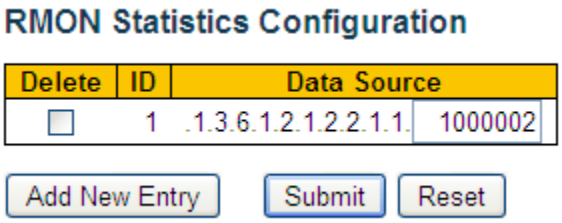


Рисунок 124 Настройка таблицы статистики RMON

ID

Диапазон: 1~65535

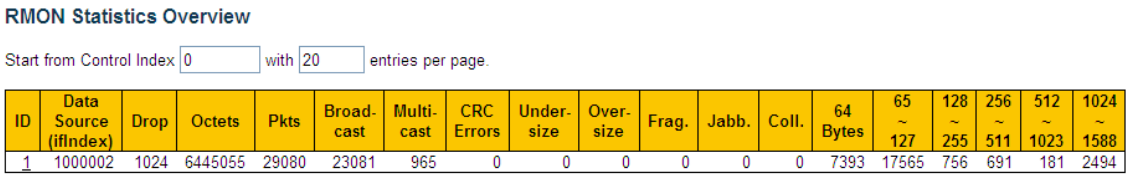
Функция: Настройка номера записи статистики. Группа статистики поддерживает до 128 записей.

Data Source

Диапазон: 100000portid

Функция: Выбор порта для сбора статистики.

2. Просмотрите статус группы статистики, как показано на рисунке 125.



ID	Data Source (ifIndex)	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1588
1	1000002	1024	6445055	29080	23081	965	0	0	0	0	0	0	7393	17565	756	691	181	2494

Рисунок 125 Просмотр статуса группы статистики

Drop: количество пакетов, отброшенных портом. Octets: количество байтов, полученных портом.

Pkts: количество пакетов, полученных портом.

Broadcast: количество широковещательных пакетов, полученных портом. Multicast: количество многоадресных пакетов, полученных портом.

CRC Errors: количество пакетов с ошибками CRC длиной от 64 до 9600 байт, полученных портом.

Undersize: количество пакетов размером менее 64 байт, полученных портом.

Oversize: количество пакетов размером более 9600 байт, полученных портом.

Frag.: количество пакетов с ошибками CRC размером менее 64 байт, полученных портом.

Jabb.: количество пакетов ошибок CRC размером более 9600 байт, полученных портом.

Coll.: количество коллизий, полученных портом в полудуплексном режиме.

64 Bytes: количество пакетов длиной 64 байта, полученных портом.

65~127: количество пакетов длиной от 65 до 127 байт, полученных портом.

128~255: количество пакетов длиной от 128 до 255 байт, полученных портом.

256~511: количество пакетов длиной от 256 до 511 байт, полученных портом.

512~1023: количество пакетов длиной от 512 до 1023 байт, полученных портом.

1024~1588: количество пакетов длиной от 1024 до 1588 байт, полученных портом.

Примечание:

Значение oversize зависит от параметра Maximum Frame Size в настройке порта. Связь нормальная, когда порт находится в состоянии LinkUP. В этом примере значение oversize 9600 байт.

3. Настройте таблицу истории, как показано на рисунке 126.

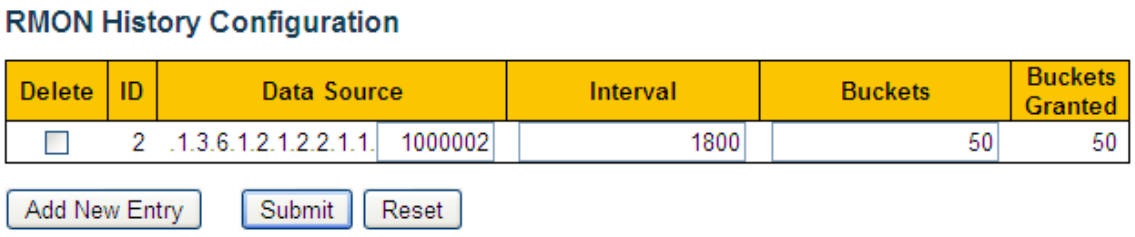


Рисунок 126 Настройка таблицы истории

ID

Диапазон: 1~65535

Функция: Настройка номера записи истории. Группа истории поддерживает до 256 записей.

Data Source

Варианты: 100000portid

Функция: Выбор порта для сбора информации.

Interval

Диапазон: 1~3600 с

По умолчанию: 1800 с

Функция: Настройка периода выборки для порта.

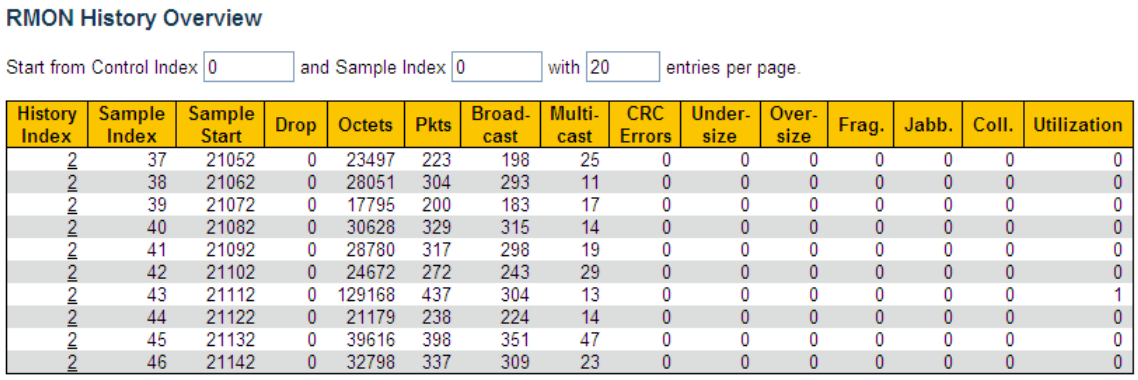
Buckets

Диапазон: 1~65535

По умолчанию: 50

Функция: Настройка количества последних значений выборки информации о порте, хранящейся в RMON.

4. Просмотрите статус группы истории, как показано на рисунке 127.



History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
2	37	21052	0	23497	223	198	25	0	0	0	0	0	0	0
2	38	21062	0	28051	304	293	11	0	0	0	0	0	0	0
2	39	21072	0	17795	200	183	17	0	0	0	0	0	0	0
2	40	21082	0	30628	329	315	14	0	0	0	0	0	0	0
2	41	21092	0	28780	317	298	19	0	0	0	0	0	0	0
2	42	21102	0	24672	272	243	29	0	0	0	0	0	0	0
2	43	21112	0	129168	437	304	13	0	0	0	0	0	0	1
2	44	21122	0	21179	238	224	14	0	0	0	0	0	0	0
2	45	21132	0	39616	398	351	47	0	0	0	0	0	0	0
2	46	21142	0	32798	337	309	23	0	0	0	0	0	0	0

Рисунок 127 Просмотр статуса группы истории

5. Настройте таблицу событий, как показано на рисунке 128.

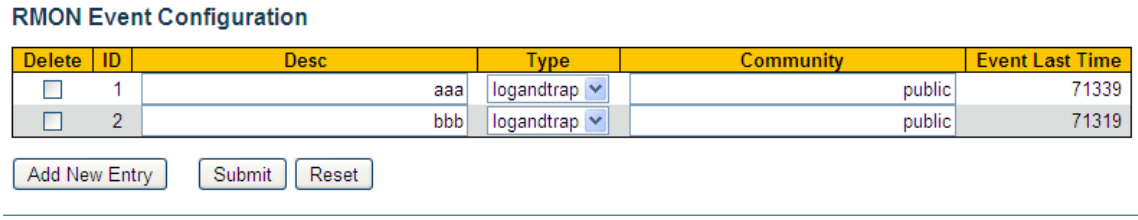


Рисунок 128 Настройка таблицы событий

ID

Диапазон: 1~65535

Функция: Настройка порядкового номера записи событий. Группа событий поддерживает до 128 записей.

Desc

Диапазон: 1~127 символов

Функция: Описание события.

Type

Варианты: none/log/snmptrap/logandtrap

По умолчанию: none

Функция: Настройка типа события для сигналов тревоги, то есть режима обработки сигналов тревоги.

Community

Диапазон: 0~127 символов

По умолчанию: public

Функция: Задание имени сообщества для отправки события trap. Значение должно совпадать со значением в SNMP.

Last Event

Функция: Отображает значение sysUpTime, когда событие использовалось в последний раз.

6. Просмотрите статус группы событий, как показано на рисунке 129.

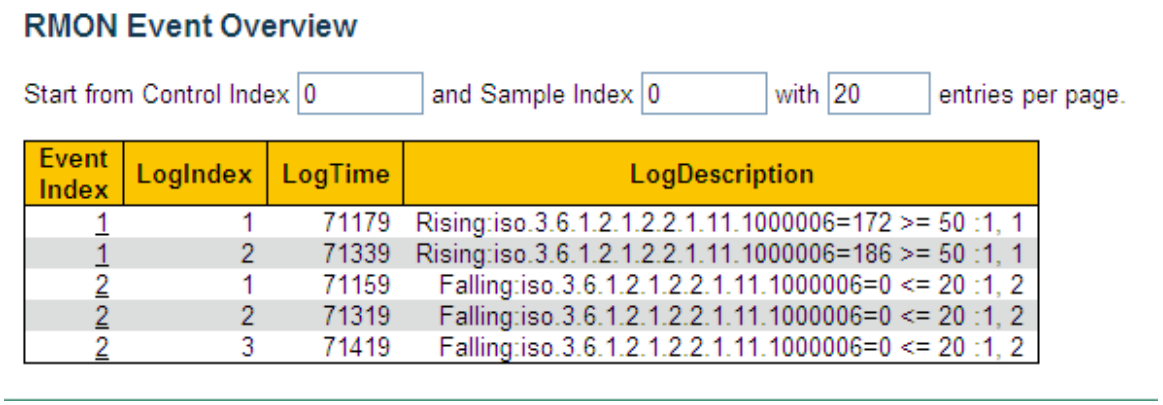


Рисунок 129 Просмотр статуса группы событий

7. Настройте таблицу сигналов тревоги, как показано на рисунке 130.

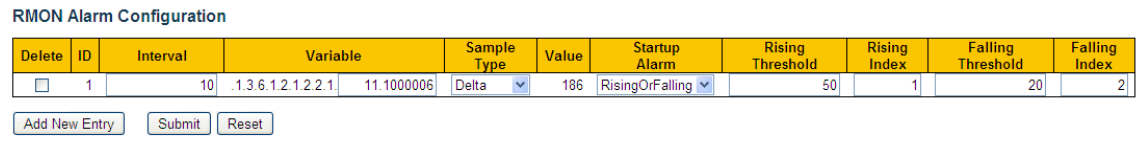


Рисунок 130 Настройка таблицы сигналов тревоги

ID

Диапазон: 1~65535

Функция: Настройка номера записи сигнала тревоги. Группа сигналов тревоги поддерживает до 256 записей.

Interval

Диапазон: 1~2147483647 с

По умолчанию: 30 с

Функция: Настройка периода выборки.

Variable

Формат: A.100000portid

Диапазон: A：10~21

Функция: Выбор информации MIB порта для мониторинга.

InOctets: A=10, количество байтов, полученных портом.

InUcastPkts: A=11, количество одноадресных пакетов, полученных портом.

InNUcastPkts: A=12, количество широковещательных и многоадресных пакетов, полученных портом.

InDiscards: A=13, количество пакетов, отброшенных портом.

InErrors: A=14, количество пакетов с ошибками, полученных портом.

InUnknownProtos: A=15, количество неизвестных пакетов, полученных

портом. OutOctets: A=16, количество байтов, отправленных портом.

OutUcastPkts: A=17, количество одноадресных пакетов, отправленных портом.

OutNUcastPkts: A=18, количество широковещательных и многоадресных пакетов,

отправленных портом. OutDiscards: A=19, количество отброшенных пакетов,

отправленных портом.

OutErrors: A=19, количество пакетов с ошибками, отправленных портом.

OutQLen: A=21, длина пакетов в выходной очереди порта.

Sample Type

Варианты: Absolute/Delta

По умолчанию: Delta

Функция: выбор метода сравнения значения выборки и порога.

Описание: Absolute: прямое сравнение каждого значения выборки с пороговым значением; Delta: значение выборки минус предыдущее значение выборки, затем разница используется для сравнения с порогом.

Startup Alarm

Варианты: Rising/Falling/RisingOrFalling

По умолчанию: RisingOrFalling

Функция: выбор типа сигнала тревоги.

Rising Threshold

Диапазон: 1~2147483647

Функция: Задание порога повышения. Когда значение выборки превышает порог повышения и типом тревоги является RisingAlarm или RisOrFallAlarm, срабатывает тревога и активируется индекс событий повышения.

Rising Index

Диапазон: 1~65535

Функция: Задание индекса события повышения. Это способ обработки сигнала тревоги при повышении значения.

Falling Threshold

Диапазон: 1~2147483647

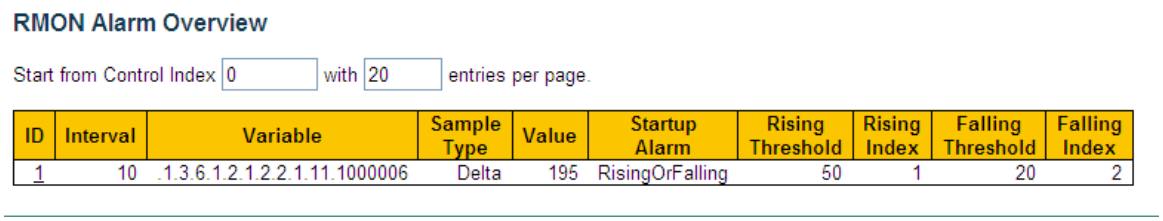
Функция: Задание порога понижения. Когда значение выборки ниже порога понижения и типом тревоги является RisingAlarm или RisOrFallAlarm, срабатывает тревога и активируется индекс событий понижения.

Falling Index

Диапазон: 1~65535

Функция: Задание индекса события понижения. Это способ обработки сигнала тревоги при понижении значения.

8. Просмотрите статус группы тревоги, как показано на рисунке 131.


RMON Alarm Overview

Start from Control Index 0 with 20 entries per page.

ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
1	10	.1.3.6.1.2.1.2.2.1.11.1000006	Delta	195	RisingOrFalling	50	1	20	2

Рисунок 131 Просмотр статуса группы тревоги

9.9 Настройка TACACS+

9.9.1 Введение

TACACS+ (Terminal Access Controller Access Control System) представляет собой приложение на основе TCP. Оно использует 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.

На рисунке 132 показана структура.

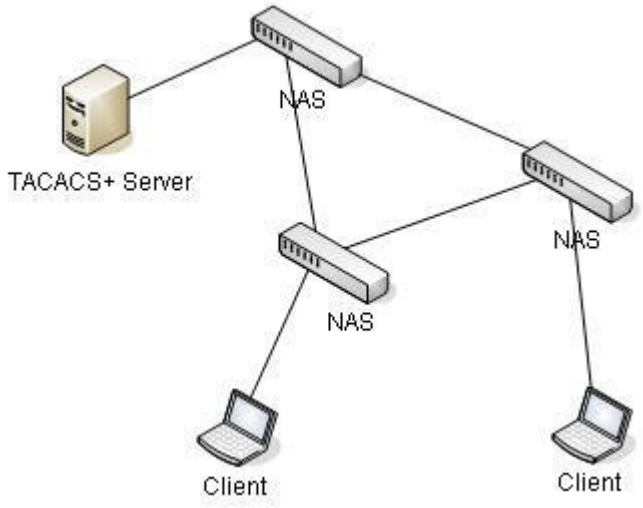


Рисунок 132 Структура TACACS+

Протокол аутентифицирует, авторизует и учитывает 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 выполнения операций.

9.9.2 Настройка через веб-интерфейс

1. Настройте глобальные параметры TACACS+, как показано на рисунке 133.

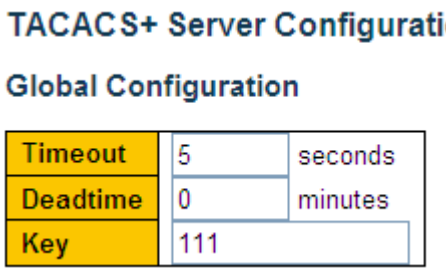


Рисунок 133 Настройка глобальных параметров TACACS+

Timeout

Диапазон: 1~1000 с

По умолчанию: 5 с

Функция: Настройка времени для получения отклика от сервера TACACS+. Если после отправки пакета запроса TACACS+ устройство не получает ответа от сервера TACACS+ по истечении указанного времени, аутентификация завершается неудачно, и устройство считает сервер TACACS+ недействительным.

Deadtime

Диапазон: 0~1440 мин

По умолчанию: 0 минут

Функция: Настройка периода, в течение которого сервер не действует. В течение этого периода устройство не отправляет сообщения запроса TACACS+ на сервер. Значение 0 означает выключение функции. Можно включить эту функцию, только если настроено более одного сервера TACACS+.

Key

Диапазон: 1~63 символа

Функция: Задание ключа 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 нужно, чтобы настроенный ключ совпадал с ключом на сервере TACACS+.

2. Настройте сервер TACACS+, как показано на рисунке 134.

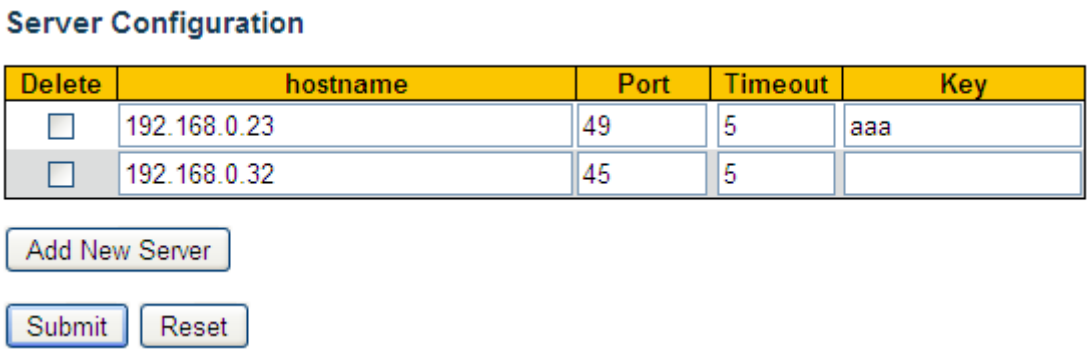


Рисунок 134 Конфигурация сервера TACACS+

Hostname

Функция: Настройка IP-адреса или имени хоста сервера TACACS+. Можно настроить не более 5 серверов TACACS+.

Port

Диапазон: 0~65535

По умолчанию: 49

Функция: Назначение порта TCP сервера TACACS+ для аутентификации.

Timeout

Диапазон: 1~1000 с

Функция: Настройка времени для получения отклика от сервера TACACS+. Если после отправки пакета запроса TACACS+ устройство не получает ответа от сервера TACACS+ по истечении указанного времени, аутентификация завершается неудачно, и устройство считает сервер TACACS+ недействительным.

Key

Диапазон: 1~63 символа

Функция: Задание ключа 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 нужно, чтобы настроенный ключ совпадал с ключом на сервере TACACS+.

Примечание:

Приоритет параметров Timeout и Key в конфигурации сервера TACACS+ выше, чем в глобальной конфигурации.

9.9.3 Пример типовой конфигурации

Как показано на рисунке 135, сервер TACACS+ может выполнять аутентификацию и авторизацию пользователей с помощью коммутатора. IP-адрес сервера — 192.168.0.23, а общий ключ, используемый при обмене пакетами между коммутатором и сервером, — aaa.

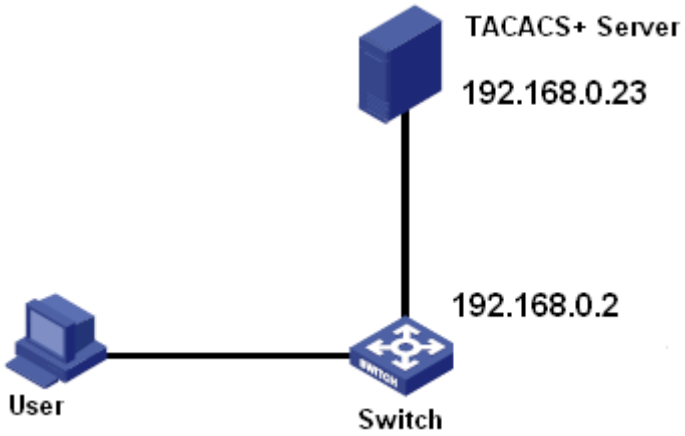


Рисунок 135 Пример аутентификации TACACS+

1. Настройка сервера TACACS+. Задайте IP-адрес сервера 192.168.0.23 и значение ключа aaa, как показано на рисунке 134.
2. При входе в коммутатор через веб-интерфейс выберите Local, при входе в коммутатор через telnet выберите Tacacs+, как показано на рисунке 96.
3. Настройте имя пользователя и пароль bbb, зашифруйте ключ aaa на сервере TACACS+.
4. При входе в коммутатор через веб-интерфейс введите имя пользователя admin и пароль 123, чтобы пройти локальную аутентификацию.
5. При входе в коммутатор через Telnet введите имя пользователя и пароль bbb, чтобы пройти аутентификацию TACACS+.

9.10 Настройка RADIUS

9.10.1 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 — это сервер для пользователей, но клиент для сервера RADIUS. На рисунке 136 показана структура.

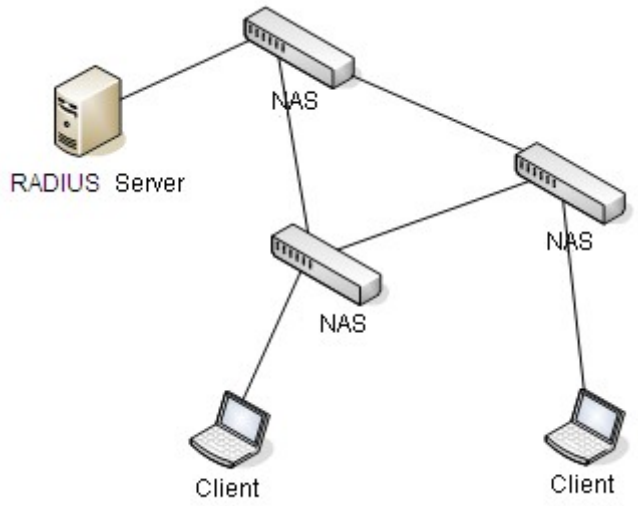


Рисунок 136 Структура RADIUS

Протокол аутентифицирует пользователей терминалов, которым необходимо войти в устройство для выполнения операций. 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 аутентификации.

9.10.2 Настройка через веб-интерфейс

1. Настройте глобальные параметры RADIUS, как показано на рисунке 137.

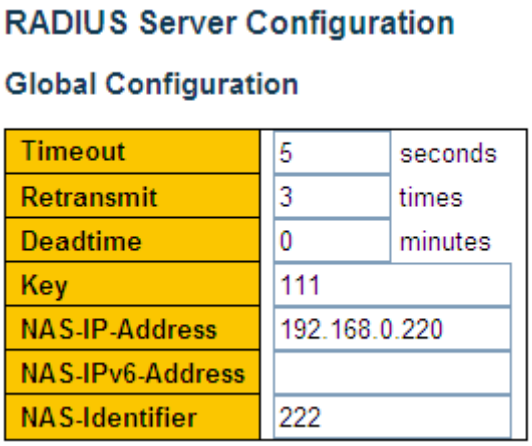


Рисунок 137 Настройка глобальных параметров RADIUS

Timeout

Диапазон: 1~1000 с

По умолчанию: 5 с

Функция: Настройка времени для получения отклика 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.

Retransmit

Диапазон: 1~1000

По умолчанию: 3

Функция: Задание максимального количества попыток повторной передачи для пакетов запросов RADIUS. Если устройство по-прежнему не получает ответные пакеты от сервера RADIUS после максимального числа попыток повторной передачи, аутентификация завершается ошибкой, и устройство считает, что сервер RADIUS недействителен.

Deadtime

Диапазон: 0~1440 мин

По умолчанию: 0 минут

Функция: Настройка периода, в течение которого сервер не действует. В течение этого периода устройство не отправляет сообщения запроса RADIUS на сервер. Значение 0 означает выключение функции. Можно включить эту функцию, только если настроено более одного сервера RADIUS.

Key

Диапазон: 1~63 символа

Функция: Задание ключа для повышения безопасности связи между клиентом и сервером RADIUS. Две стороны совместно используют ключ для проверки легитимности пакетов. Обе стороны могут получать пакеты друг от друга только тогда, когда ключи совпадают. Поэтому нужно, чтобы настроенный ключ совпадал с ключом на сервере RADIUS.

NAS-IP-Address

Функция: Настройка адреса источника, используемого для отправки оборудованием запросов RADIUS. Если адрес источника не указан, то в качестве адреса источника будет рассматриваться адрес интерфейса для отправки сообщений.

NAS-Identifier

Диапазон: 1~253 символа

Функция: Настройка идентификатора, используемого для отправки оборудованием запросов RADIUS.

2. Настройте сервер RADIUS, как показано на рисунке 138.

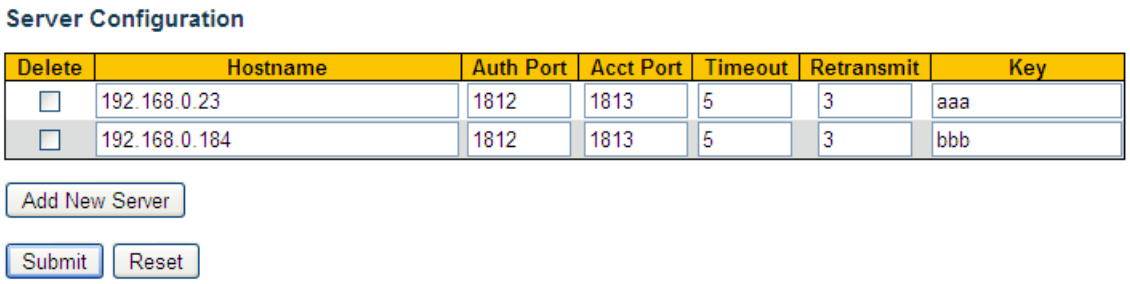


Рисунок 138 Настройка сервера RADIUS

Hostname

Функция: Настройка IP-адреса или имени хоста сервера RADIUS. Можно настроить не более 5 серверов RADIUS.

Auth Port

Диапазон: 0~65535

По умолчанию: 1812

Функция: Задание порта UDP сервера RADIUS для аутентификации.

Acct Port

Диапазон: 0~65535

По умолчанию: 1813

Функция: Задание порта UDP сервера RADIUS для учета. Поскольку RADIUS использует разные порты UDP для получения и отправки сообщений аутентификации и учета, необходимо настроить разные номера портов для аутентификации и учета.

Timeout

Диапазон: 1~1000 с

Функция: Настройка времени для получения отклика 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.

Retransmit

Диапазон: 1~1000

Функция: Задание максимального количества попыток повторной передачи для пакетов запросов RADIUS. Если устройство по-прежнему не получает ответные пакеты от сервера RADIUS после максимального числа попыток повторной передачи, аутентификация завершается ошибкой, и устройство считает, что сервер RADIUS недействителен.

Key

Диапазон: 1~63 символа

Функция: Задание ключа для повышения безопасности связи между клиентом и сервером RADIUS. Две стороны совместно используют ключ для проверки легитимности пакетов. Обе стороны могут получать пакеты друг от друга только тогда, когда ключи совпадают. Поэтому нужно, чтобы настроенный ключ совпадал с ключом на сервере RADIUS.

Примечание:

Приоритет параметров Timeout, Retransmit и Key в конфигурации сервера RADIUS выше, чем в глобальной конфигурации.

3. Просмотрите статус сервера RADIUS, как показано на рисунке 139.

RADIUS Server Status Overview

#	IP Address	Authentication Port	Authentication Status	Accounting Port	Accounting Status
1	192.168.0.23	1812	Ready	1813	Ready
2	192.168.0.184	1812	Ready	1813	Ready
3			Disabled		Disabled
4			Disabled		Disabled
5			Disabled		Disabled

Рисунок 139 Просмотр статуса сервера RADIUS

Щелкните номер для перехода на страницу подробной статистики сервера RADIUS.

4. Просмотрите подробную статистику сервера RADIUS, как показано на рисунке 140.

RADIUS Authentication Statistics for Server #1 Server #1 Auto-refresh Refresh Clear

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
IP Address		192.168.0.23:1812	
State		Ready	
Round-Trip Time		0 ms	

RADIUS Accounting Statistics for Server #1

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
IP Address		192.168.0.23:1813	
State		Ready	
Round-Trip Time		0 ms	

Рисунок 140 Просмотр подробной статистики сервера RADIUS

Выберите сервер и просмотрите подробную статистику назначенного сервера.

9.10.3 Пример типовой конфигурации

Как показано на рисунке 141, IEEE802.1X включен на порту 1 коммутатора.

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 — aaa.

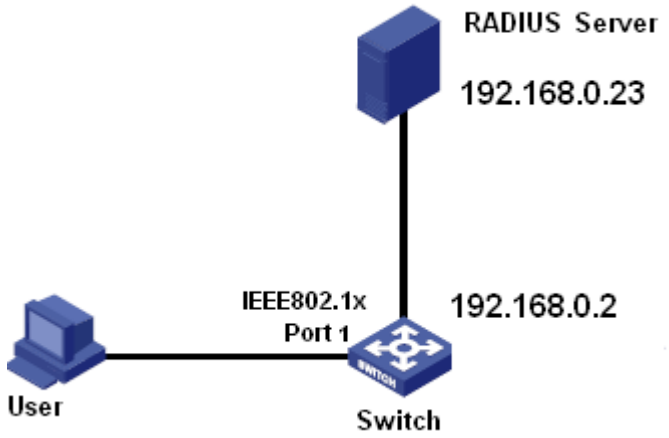


Рисунок 141 Пример аутентификации RADIUS

1. Задайте IP-адрес сервера аутентификации 192.168.0.23 и пароль aaa, как показано на рисунке 138.

2. Настройки IEEE802.1x: включить IEEE802.1X глобально. Установите тип аутентификации radius, состояние администратора порта 1 802.1X на основе порта, оставьте настройки по умолчанию для других параметров. Подробности см. в разделе 10.2Настройка IEEE802.1X.

3. Установите для имени пользователя и пароля на сервере RADIUS значение ccc, для ключа шифрования — aaa.

4. Установите и запустите клиентское ПО 802.1x на ПК. Введите ccc в качестве имени пользователя и пароля. Затем пользователь может пройти аутентификацию и получить доступ к коммутатору.

10 Сеть

10.1 Безопасность порта

10.1.1 Введение

Безопасность портов ограничивает максимальное количество пользователей на порт, которые однозначно идентифицируются по MAC-адресам и идентификатору vlan. Если ограничение MAC-адресов для порта включено, максимальное количество пользователей на порту – это ограничение MAC-адресов. Если количество MAC-адресов на порту превышает максимальный предел, запускается соответствующее действие.

10.1.2 Настройка через веб-интерфейс

Настройте ограничения MAC-адресов для безопасности порта, как показано на рисунке 142.

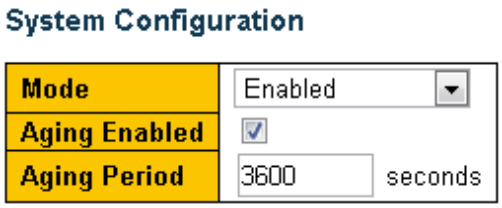


Рисунок 142 Конфигурация системы

Mode:

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение и выключение глобального режима ограничения MAC-адресов.

Aging Enable:

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение и выключение глобальной функции старения MAC-адресов.

Aging Period:

Диапазон：10~10000000 с

По умолчанию: 3600 с

Функция: MAC-адреса могут устаревать в течение данного периода

1. Настройка ограничения MAC-адресов для порта показана на рисунке 143.

Port Configuration

Port	Mode	Limit	Action	State	Reopen
*	<>	4	<>		
1	Disabled	4	None	Disabled	Reopen
2	Disabled	4	None	Disabled	Reopen
3	Disabled	4	None	Disabled	Reopen
4	Enabled	4	None	Ready	Reopen
5	Disabled	4	None	Disabled	Reopen
6	Disabled	4	None	Disabled	Reopen
7	Disabled	4	None	Disabled	Reopen
8	Disabled	4	None	Disabled	Reopen
9	Disabled	4	None	Disabled	Reopen
10	Disabled	4	None	Disabled	Reopen

Рисунок 143 Настройка порта

Mode:

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение и выключение функции ограничения MAC-адресов.

Limit:

Диапазон:1~1024

По умолчанию:4

Функция: Настройка максимального количества MAC-адресов для ограничения

Action:

Варианты: None/Trap/Shutdown/Trap&Shutdown

По умолчанию: None

Функция: Настройка действия при превышении предельного числа MAC-адресов.

State:

Варианты: Disabled/Ready/Limit Reached/Shutdown

Reopen:

Если порт отключен этим модулем, можно снова открыть его, щелкнув эту кнопку.

Предупреждение:

1Для параметров Port Mode и Global Mode должно быть установлено значение Enabled. чтбы фvнкция Limit Control действовала.

2、Обратите внимание, что щелчок кнопки Reopen приведет к обновлению страницы, так что неподтвержденные изменения будут потеряны.

3.Состояние безопасности портов коммутатора показано на рисунке 144.

Port Security Switch Status

User Module Legend

User Module Name	Abbr
Limit Control	L
802.1X	8
Voice VLAN	V

Port Status

Port	Users	State	MAC Count	
			Current	Limit
1	---	Disabled	-	-
2	---	Disabled	-	-
3	---	Disabled	-	-
4	L--	Ready	0	4
5	---	Disabled	-	-
6	---	Disabled	-	-
7	---	Disabled	-	-
8	---	Disabled	-	-
9	---	Disabled	-	-
10	---	Disabled	-	-

Рисунок 144 Состояние безопасности портов коммутатора

4.Состояние безопасности порта рисунке 145.

Port Security Status Port 5

MAC Address	VLAN ID	State	Time of Addition	Ageing Time(s)
54-e6-fc-6a-fe-a0	1	Forwarding	1970-01-01T07:19:41+00:00	3597

Рисунок 145 Состояние порта

10.2 Настройка IEEE802.1X

10.2.1 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 проходит аутентификацию, он не может получить доступ к ресурсам в локальной сети.

Системы 802.1X используют структуру клиент/сервер, как показано на рисунке 146. Аутентификация и авторизация пользователя при управлении доступом на основе порта требуют следующих элементов:

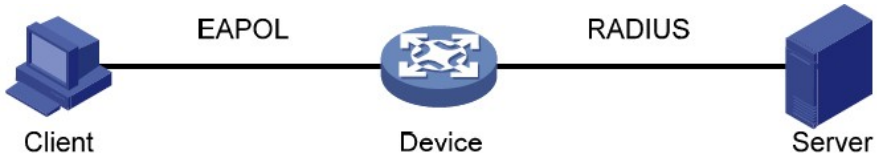


Рисунок 146 Структура IEEE802.1X

Клиент: обычно указывает пользовательский терминал. Когда пользователь хочет выйти в Интернет, он запускает клиентскую программу и вводит необходимое имя пользователя и пароль. Клиентская программа отправляет запрос на соединение. Клиент должен поддерживать EAPOL (Extensible Authentication Protocol over LAN).

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 службу 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.

10.2.2 Настройка через веб-интерфейс

1. Настройте глобальные параметры IEEE802.1X, как показано на рисунке 147.

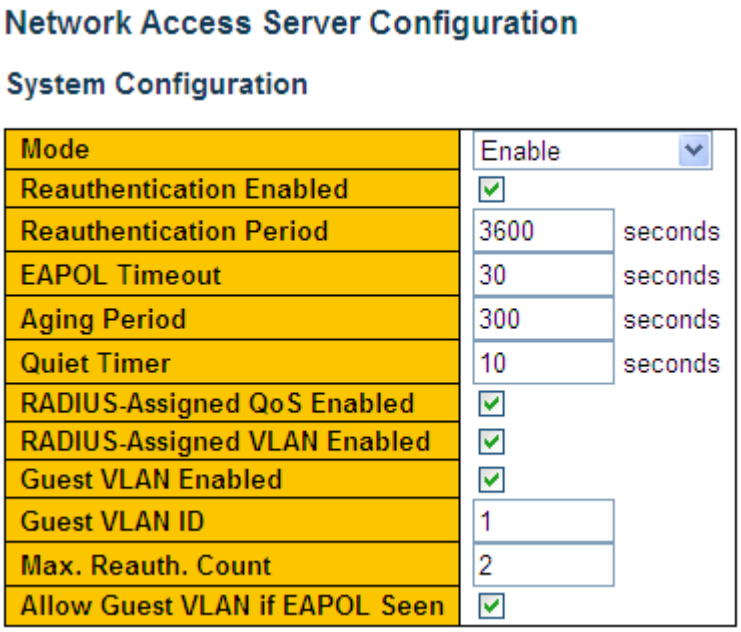


Рисунок 147 Настройка глобальных параметров IEEE802.1X

Mode

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение глобальных функций безопасности IEEE802.1x.

Reauthentication Enabled

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Требуется ли регулярная повторная аутентификация при успешной проверке аутентификации.

Reauthentication Period

Диапазон: 1~3600 с

По умолчанию: 3600 с

Функция: Установка временного интервала для повторной аутентификации после успешной аутентификации. Параметр Reauthentication Period можно настроить только тогда, когда параметр Reauthentication Enabled имеет значение Enable. **EAPOL**

Timeout

Диапазон: 1~65535 с

По умолчанию: 30 с

Функция: Настройка времени для получения отклика от клиента. После отправки пакета запроса идентификации EAPOL устройство повторит передачу пакета запроса идентификации EAPOL, если оно по-прежнему не получит ответа от клиента по истечении указанного времени.

Aging Period

Диапазон: 10~1000000 с

По умолчанию: 300 с

Функция: Настройка периода старения. Когда повторная аутентификация отключена, временной интервал для повторной аутентификации равен удвоенному периоду старения.

Quiet Timer

Диапазон: 10~1000000 с

По умолчанию: 10 с

Функция: Если аутентификация не удалась, устройство переходит в режим молчания. В период молчания устройство не отвечает на запросы аутентификации от клиента.

RADIUS-Assigned QoS Enabled

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Если этот параметр включен, после прохождения клиентом аутентификации сервер передает на устройство информацию об авторизации. Если на сервере установлен флаг RADIUS-Assigned QoS Enabled, информация авторизации включает информацию CoS, назначенную для авторизации. Оборудование изменит значение CoS порта аутентификации клиента на основе присвоенного значения.

RADIUS-Assigned VLAN Enabled

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Если этот параметр включен, после прохождения клиентом аутентификации сервер передает на устройство информацию об авторизации. Если на сервере

установлен флаг **RADIUS-Assigned VLAN Enabled**, информация авторизации включает информацию VLAN, назначенную для авторизации. Оборудование изменит значение VLAN порта аутентификации клиента на основе присвоенного значения.

Guest VLAN Enabled

Варианты: Enable/Disable

По умолчанию: Disable

Функция: При значении Enable, если пользователь не прошел аутентификацию или в аутентификации отказано, устройство добавляет порт аутентификации клиента в гостевую VLAN. Все пользователи, имеющие доступ к этому порту, имеют право доступа к ресурсам в гостевой VLAN.

Guest VLAN ID

Диапазон: 1~4095

По умолчанию: 1

Функция: Настройка VLAN ID гостевой сети.

Max. Reauth.

Count Диапазон:

1~255

По умолчанию: 2

Функция: Задание максимального количества попыток повторной передачи для пакетов запроса Identity EAPOL. Если устройство по-прежнему не получает ответных пакетов от клиента после максимальных попыток повторной передачи, устройство будет считать аутентификацию неудачной.

Allow Guest VLAN if EAPOL Seen

Варианты: Enable/Disable

По умолчанию: Disable

Функция: При значении Enable, если пользователь не прошел аутентификацию или в аутентификации отказано, устройство добавляет порт аутентификации клиента в гостевую VLAN. При значении Disable устройство добавляет порт в гостевую VLAN только в том случае, если этот порт не имеет записи кадра EAPOL.

Предупреждение:

- Предварительным условием для настройки параметров Guest VLAN ID, Max. Reauth. Count и Allow Guest VLAN if EAPOL Seen является задание значения Enable для параметра Guest VLAN ID.
- Если тип порта аутентификации Trunk или Hybrid для параметров RADIUS-Assigned VLAN Enabled и Guest VLAN ID задать значение Disable.
- Значение CoS, назначенное для авторизации, не меняет и не влияет на конфигурацию порта. Однако приоритет значения COS, назначенного для авторизации, выше, чем приоритет значения COS, настроенного пользователем. Иными словами, действительным после аутентификации является значение CoS, назначенное для авторизации. Если пользователь не проходит аутентификацию или выходит из сети, значение CoS, настроенное пользователем, вступает в силу.
- Назначенная для авторизации VLAN или гостевая VLAN не меняют и не влияют на конфигурацию порта. Однако назначенная для авторизации VLAN или гостевая VLAN имеет более высокий приоритет, чем VLAN, настроенная пользователем.

После того, как пользователь инициирует аутентификацию, и если аутентификация прошла успешно:

Если на порту включен режим **RADIUS-Assigned VLAN**, порт добавляется в VLAN, назначенную сервером RADIUS.

Если на порту не включен режим **RADIUS-Assigned VLAN**, порт добавляется в VLAN, настроенную пользователем.

Если пользователь не проходит аутентификацию или выходит из сети:

Если для порта включен режим **Guest VLAN** и **Allow Guest VLAN if EAPOL Seen**, порт добавляется в VLAN.

Если для порта включен режим **Guest VLAN**, но не включен режим **Allow Guest VLAN if EAPOL Seen,** порт добавляется в гостевую VLAN, если нет доступной записи кадра EAPOL, и добавляется в VLAN, настроенную пользователем, если запись кадра EAPOL доступна.

Если на порту не включен режим **Guest VLAN**, порт добавляется в VLAN, настроенную пользователем.

2. Настройте порт IEEE802.1X, как показано на рисунке 148.

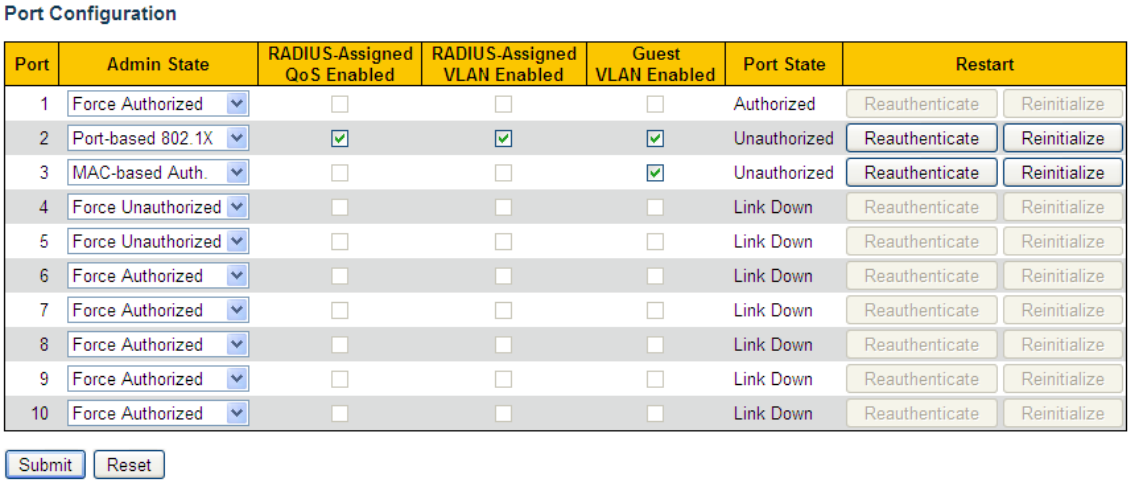


Рисунок 148 Настройка порта IEEE802.1X

Port

Варианты: все порты коммутатора.

Admin State

Варианты: Force Authorized/Force Unauthorized/Port-based 802.1X/MAC-based Auth.

По умолчанию: Force Authorized

Функция: Выбор режима аутентификации для порта.

Описание: **Force Authorized** означает, что порт всегда находится в авторизованном состоянии и позволяет пользователям получать доступ к сетевым ресурсам без аутентификации.

Force Unauthorized 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 через этот порт. **MAC-based Auth** указывает, что пользователи, использующие порт, должны пройти соответствующую аутентификацию. Когда пользователь находится в автономном режиме, только этот пользователь не может использовать сеть. **Port-based 802.1X** указывает, что пользователи проходят аутентификацию 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.

RADIUS-Assigned QoS Enabled

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение или выключение назначенного RADIUS QoS для порта.

RADIUS-Assigned VLAN Enabled

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение или выключение назначенной RADIUS VLAN для порта.

Guest VLAN Enabled

Enable/Disable

По умолчанию: Disable

Функция: Включение или выключение гостевой VLAN для порта.

Примечание:
Эта функция доступна только тогда, когда параметры **RADIUS-Assigned QoS**/**RADIUS-Assigned VLAN**/**Guest VLAN** включены и на глобальном уровне, и на уровне порта.

Port State

Варианты: Globally Disabled, Authorized, Unauthorized, Link Down, x Auth/y Unauth

Function: Отображение состояния аутентификации для порта. **Globally Disabled** указывает, что IEEE802.1X отключен глобально; **Authorized** указывает, что пользователь, подключенный к порту, проходит аутентификацию; **Unauthorized** указывает, что пользователь, подключенный к порту, не может пройти аутентификацию; **Link Down** указывает, что порт не работает; **x Auth/y Unauth** указывает, что x пользователей авторизованы, а y пользователей не авторизованы, когда режим аутентификации порта MAC-based Auth.

Если режим аутентификации порта MAC-based Auth или Port-based 802.1X, можно нажать кнопку <Reauthenticate>/<Reinitialize> для повторной аутентификации. В процессе повторной аутентификации состояние порта изменяется на **Unauthorized**.

3. Просмотрите настройки IEEE802.1X, как показано на рисунке 149.

Network Access Server Switch Status

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Authorized			-	
2	Port-based 802.1X	Unauthorized			-	
3	MAC-based Auth.	Unauthorized			-	
4	Force Unauthorized	Link Down			-	
5	Force Unauthorized	Link Down			-	
6	Force Authorized	Link Down			-	
7	Force Authorized	Link Down			-	
8	Force Authorized	Link Down			-	
9	Force Authorized	Link Down			-	
10	Force Authorized	Link Down			-	

Рисунок 149 Просмотр настроек IEEE802.1X

Щелкните <port> для перехода на страницу статистики IEEE802.1X.

4. Просмотрите статистику IEEE802.1X, как показано на рисунке 150.

NAS Statistics Port 1 Auto-refresh Refresh Clear All Clear This

Port State

Admin State	Port-based 802.1X
Port State	Authorized
QoS Class	-
Port VLAN ID	

Port Counters

Receive EAPOL Counters		Transmit EAPOL Counters	
Total	4	Total	5
Response ID	1	Request ID	3
Responses	1	Requests	1
Start	1		
Logoff	1		
Invalid Type	0		
Invalid Length	0		
Receive Backend Server Counters		**Transmit Backend Server Counters**	
Access Challenges	1	Responses	2
Other Requests	4		
Auth. Successes	1		
Auth. Failures	0		
Last Supplicant Info			
MAC Address		44-37-e6-88-6e-90	
VLAN ID		1	
Version		1	
Identity		ccc	

Рисунок 150 Просмотр статистики IEEE802.1X

Выберите порт и просмотрите статистику IEEE802.1X для выбранного порта.

10.2.3 Пример типовой конфигурации

Как показано на рисунке 151, клиент подключен к порту 1 коммутатора. Включите IEEE802.1x для порта 1 и выберите режим аутентификации Port-based 802,1X. Имя пользователя и пароль для удаленной аутентификации ddd.

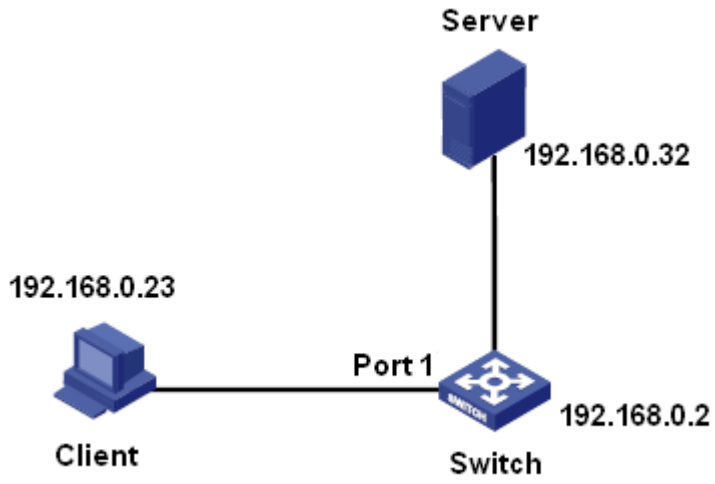


Рисунок 151 Пример настроек IEEE802.1X

Можно ознакомиться с примером типовой конфигурации в 9.10 Настройка RADIUS.

10.3 ACL

10.3.1 Обзор

С развитием сетевых технологий вопросы безопасности становятся все более заметными, что требует механизма контроля доступа. Благодаря функции списка управления доступом Access Control List (ACL) коммутатор сопоставляет пакеты со списком для реализации контроля доступа.

10.3.2 Реализация

Коммутаторы серии осуществляют фильтрацию пакетов в соответствии с согласованным ACL. Каждая запись состоит из нескольких условий в логической связи И. Записи ACL не зависят друг от друга.

Коммутатор сравнивает пакет с записями ACL в порядке возрастания идентификаторов записей. Как только совпадение найдено, действие выполнено, и дальнейшее сравнение не проводится, как показано на следующем рисунке.

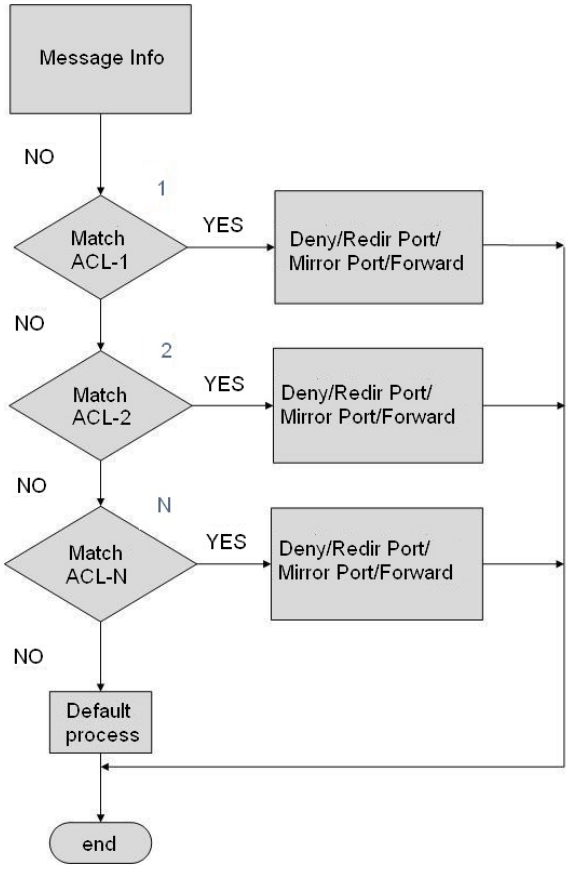


Рисунок 152 Схема обработки ACL

Примечание:

Процесс по умолчанию указывает режим обработки пакетов, не соответствующих записи ACL.

10.3.3 Настройка через веб-интерфейс

1. Настройте порты ACL, как показано на рисунке 153.

Предупреждение:

Конфигурация порта ACL указывает способ обработки принятых портом пакетов, не соответствующих ни одной записи ACL.

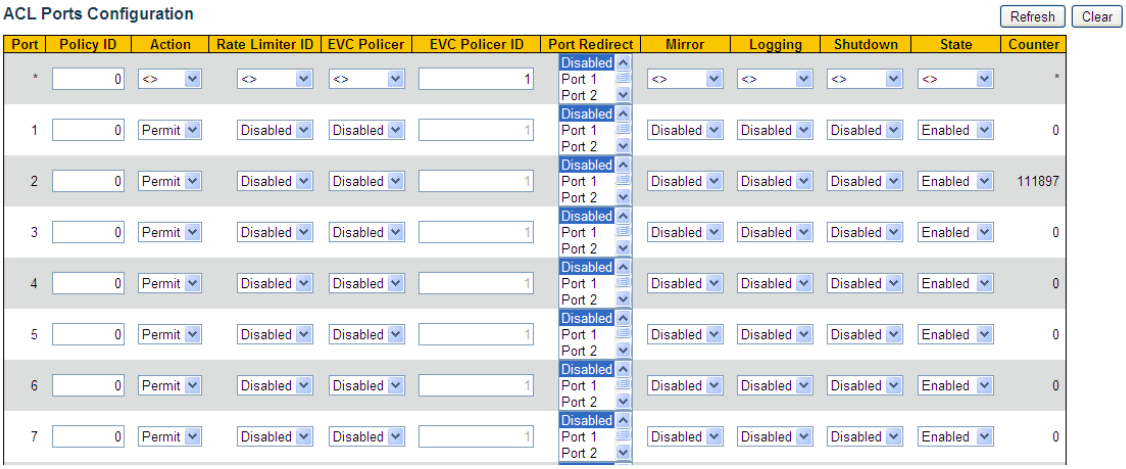


Рисунок 153 Настройка портов ACL

Policy ID

Диапазон: 0~255

По умолчанию: 0

Функция: Настройка ID политики порта.

Action

Варианты: Deny/Permit

По умолчанию: Permit

Функция: Настройка действия по отношению к пакету, который не соответствует какой-либо записи ACL. Deny: Пакеты, не соответствующие какой-либо записи, будут отклонены. Permit: Пакеты, не соответствующие какой-либо записи, будут переадресованы.

Rate Limiter ID

Диапазон: Disabled/1~16

По умолчанию: Disabled

Функция: отключить функцию ограничения скорости порта и выбрать ID ограничителя скорости.

EVC Policer

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Включить/выключить ограничитель EVC порта.

EVC Policer ID

Диапазон: 1~256

По умолчанию: 1

Функция: После включения ограничителя EVC настроить ID ограничителя EVC порта.

Предупреждение:

Ограничение скорости порта и политика EVC не могут быть включены одновременно.

Port Redirect

Варианты: Disabled/ любой порт

По умолчанию: Disabled

Функция: Включение/выключение функции перенаправления портов. После включения функции перенаправления портов пакеты, не соответствующие какой-либо записи ACL, будут перенаправлены на указанный порт.

Предупреждение:

Функцию перенаправления портов можно включить только если для параметра Action установлено значение Deny.

Mirroring

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Включение/выключение функции зеркалирования портов. После включения функции зеркалирования портов пакеты, не соответствующие какой-либо записи ACL, будут пересылаться как на порт назначения, так и на порт назначения зеркалирования.

Предупреждение:

Условием для включения зеркалирования портов ACL является наличие зеркального порта назначения.

Logging

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Включение/выключение функции регистрации порта. Enabled: если порт получает пакет, который не соответствует ни одной записи ACL, пакет записывается в системный журнал. Disabled: если порт получает пакет, который не соответствует ни одной записи ACL, пакет записывается в системный журнал.

Shutdown

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: отключение порта. Enabled: если порт получает пакет, который не соответствует ни одной записи ACL, порт отключается. Disabled: если порт получает пакет, который не соответствует ни одной записи ACL, порт не отключается.

Counter

Функция: Отображение количества полученных каждым портом пакетов, не соответствующих какой-либо записи ACL.

2. Настройте ограничитель скорости ACL, как показано на рисунке 154.

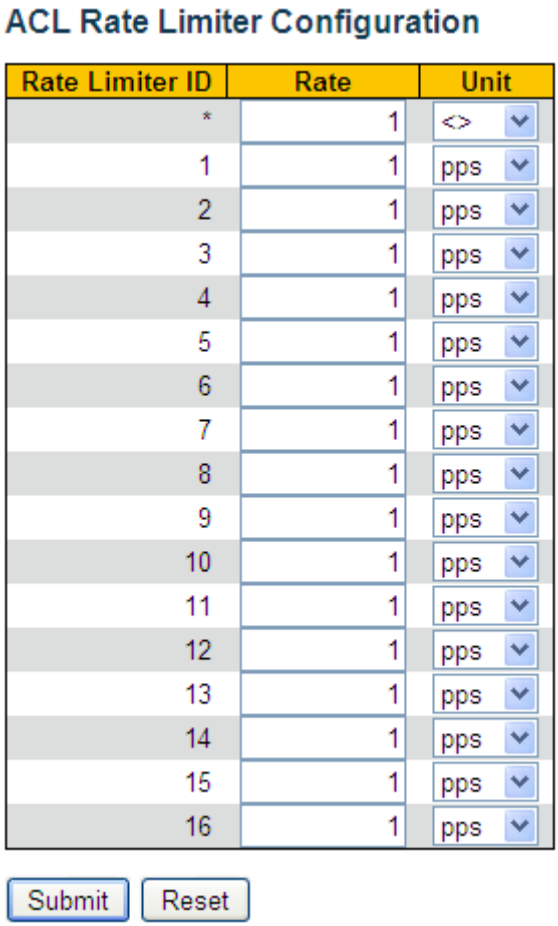


Рисунок 154 Настройка ограничителя скорости ACL

Rate Unit

Диапазон: 0~3276700 pps/ 0~1000000 Kbps (шаг 100)

По умолчанию: 1 pps

Функция: Настройка ограничения скорости по идентификатору ограничителя скорости

3. Настройте запись ACL, как показано на рисунке 155.

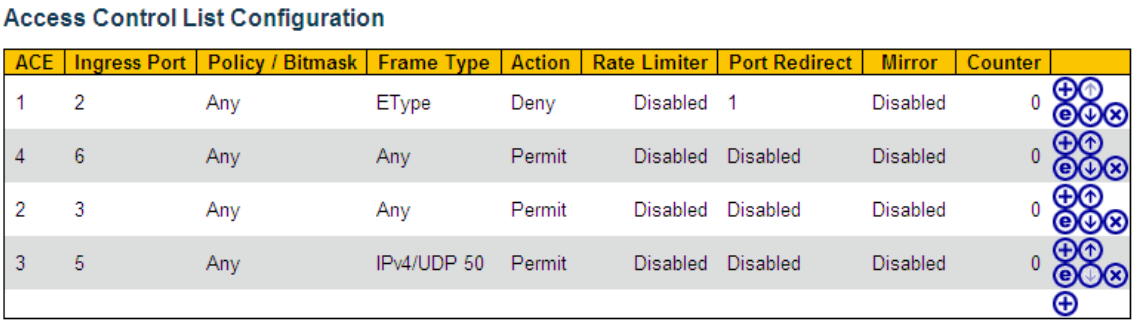


Рисунок 155 Настройка записи ACL

При наличии нескольких записей ACL устройство последовательно сравнивает пакет с записями ACL (сверху вниз). Как только совпадение найдено, действие выполнено,

и дальнейшее сравнение не проводится.

Щелкните <○+ >, чтобы добавить новую запись ACL; щелкните <○e >, чтобы редактировать запись ACL; щелкните <○x >, чтобы удалить запись ACL, щелкните <○↑ >, чтобы переместить текущую запись вверх; щелкните <○↓ > чтобы переместить текущую запись вниз.

ACE — это идентификатор записи ACL, который нумеруется на основе временной последовательности создания записи.

4. Настройка параметров записи ACL

➢ Настройте параметры записи ACL, как показано на рисунке 156.

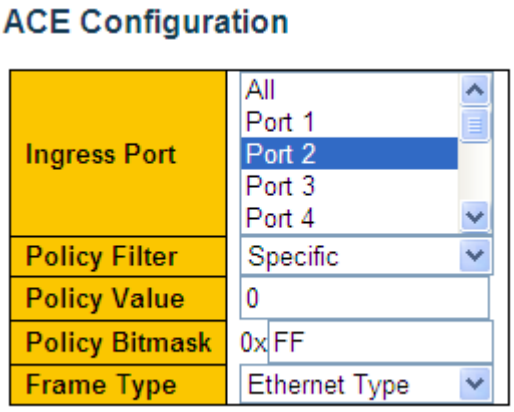


Рисунок 156 Настройка параметров записи ACL

Ingress Port

Варианты: All/ любой порт

По умолчанию: All

Функция: Выбор порта, на котором действует запись контроля доступа (ACE).

Policy Filter

Варианты: Any/ Specific

По умолчанию: Any

Функция: Настройка условия ACE – ID политик. Если установлено значение Specific, нужно назначить значение и битовую маску политики. Когда значение политики пакета, полученного входным портом, соответствует настройкам этого параметра, условие успешно соблюдено.

Policy Value

Диапазон: 0~255

Функция: Настройка значения политики.

Policy Bitmask

Диапазон: 0x0~0xFF

Функция: Настройка битовой маски политики. Значение политики и битовая маска политики используются для сопоставления при фильтрации политики. Битовая маска политики преобразуется в двоичные числа, а затем выравнивается по правому краю со значением политики (в двоичном режиме). Значение 1 указывает на то же самое, а значение 0 указывает на то, что разрешено любое значение.

Frame Type

Варианты: Any/Ethernet Type/IPv4

По умолчанию: Any

Функция: Задание условий – тип пакета. Когда тип пакета, полученного входным портом, соответствует настройкам этого параметра, условие выполняется успешно.

- Настройте параметры VLAN, как показано на рисунке 157.

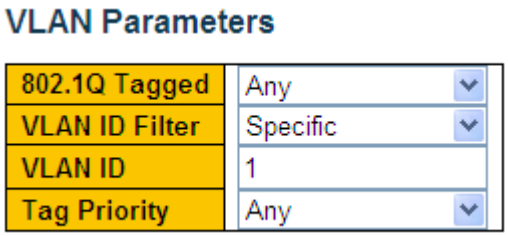


Рисунок 157 Настройка параметров VLAN

802.1Q Tagged

Варианты: Any/ Disabled/ Enabled
По умолчанию: Any

Функция: Задание условий – тег 802.1Q Значение Disabled указывает на нетегированные пакеты, а значение Enabled указывает на тегированные пакеты. Когда пакет, полученный входным портом, соответствует настройкам этого параметра, условие выполняется успешно.

VLAN ID Filter

Варианты: Any/ Specific（1~4095）

По умолчанию: Any

Функция: Задание условий для VID. Если установлено значение Specific, нужно назначить значение VID. Когда VID пакета, полученного входным портом, соответствует настройкам этого параметра, условие выполняется успешно. Если для параметра 802.1Q задано значение Disabled, для данного параметра необходимо задать значение Any.

Tag Priority

Варианты: Any/0/1/2/3/4/5/6/7/0-1/2-3/4-5/6-7/0-3/4-7

По умолчанию: Any

Функция: Задание условий – приоритет тега. Когда приоритет в пакете, полученном входным портом, соответствует настройкам этого параметра, условие выполняется успешно. Если для параметра 802.1Q задано значение Disabled, для данного параметра необходимо задать значение Any.

- Настройте параметры кадра EtherType, как показано на рисунке 158.

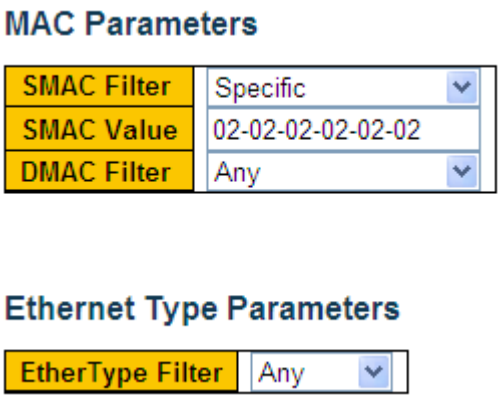


Рисунок 158 Настройка параметров кадра EtherType

SMAC Filter

Варианты: Any/ Specific

По умолчанию: Any

Функция: Задание условий для MAC-адреса источника Если установлено значение Specific, нужно назначить MAC-адрес источника. Когда MAC-адрес источника в пакете, полученном входным портом, соответствует настройкам этого параметра, условие успешно выполнено.

DMAC Filter

Варианты: Any/ UC/ MC / BC/ Specific

По умолчанию: Any

Функция: Задание условий для MAC-адреса назначения Если установлено значение Specific, нужно назначить MAC-адрес назначения. Когда MAC-адрес назначения в пакете, полученном входным портом, соответствует настройкам этого параметра, условие успешно выполнено.

Ether Type Filter

Варианты: Any/ Specific (0x600~0xFFFF，исключая 0x800(IPv4), 0x806(ARP), 0x86DD(IPv6))

По умолчанию: Any

Функция: Задание условий для типа Ethernet. Если установлено значение Specific, нужно назначить тип Ethernet. Когда пакет Ethernet, полученный входным портом, соответствует настройкам этого параметра, условие выполняется успешно.

- Настройте параметры кадра IPv4, как показано на рисунке 159.

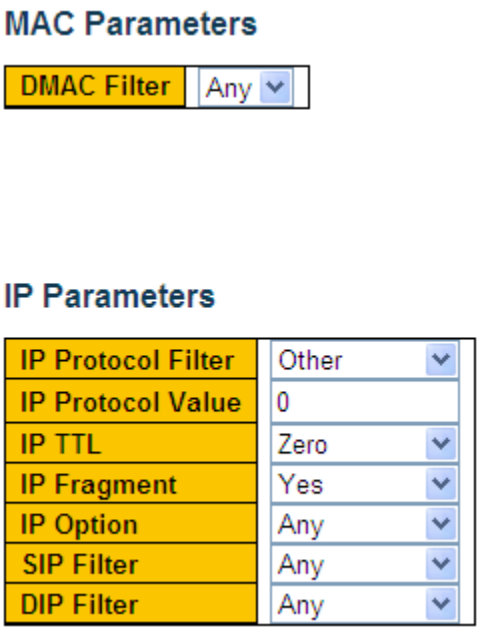


Рисунок 159 Настройка параметров кадра IPv4

DMAC Filter

Варианты: Any/ UC/ MC / BC

По умолчанию: Any

Функция: Задание условий для MAC-адреса назначения Когда MAC-адрес назначения в пакете, полученном входным портом, соответствует настройкам этого параметра, условие успешно выполнено.

IP Protocol Filter

Варианты: Any/ ICMP/ UDP/ TCP/ Other（0~255）

По умолчанию: Any

Функция: Задание условий для типа протокола пакета IPv4 Если для него установлено значение ICMP, UDP или TCP, необходимо задать соответствующие параметры. Если установлено значение Other, нужно назначить ID протокола. Когда тип протокола в пакете IPv4, полученном входным портом, соответствует настройкам этого параметра, условие выполняется успешно.

IP TTL

Варианты: Any/Non-zero/zero

По умолчанию: Any

Функция: Задание условий – поле TTL в IP-пакетах. Значение Non-zero указывает, что условие выполняется, когда IP TTL в пакете IPv4 больше 0, а значение Zero указывает, что условие не выполняется, когда IP TTL в пакете IPv4 больше 0.

IP Fragment

Варианты: Any/ Yes/ No

По умолчанию: Any

Функция: Задание условий – IP-фрагмент. Когда IP-фрагмент в пакете IPv4, полученном входным портом, соответствует настройкам этого параметра, условие выполняется успешно.

IP Option

Варианты: Any/ Yes/ No

По умолчанию: Any

Функция: Задание условий – IP-опция. Когда IP-опция в пакете IPv4, полученном

входным портом, соответствует настройкам этого параметра, условие выполняется успешно.

SIP Filter

Варианты: Any/Host/Network
По умолчанию: Any

Функция: Задание условий для IP-адреса источника Если установлено значение Host, нужно назначить IP-адрес. Если установлено значение Network, нужно назначить IP-адрес и маску подсети. Когда IP-адрес источника в пакете IPv4, полученном входным портом, соответствует настройкам этого параметра, условие выполняется успешно.

DIP Filter

Варианты: Any/Host/Network

По умолчанию: Any

Функция: Задание условий для IP-адреса назначения Если установлено значение Host, нужно назначить IP-адрес. Если установлено значение Network, нужно назначить IP-адрес и маску подсети. Когда IP-адрес назначения в пакете IPv4, полученном входным портом, соответствует настройкам этого параметра, условие выполняется успешно.

- Настройте параметры ICMP, как показано на рисунке 160.

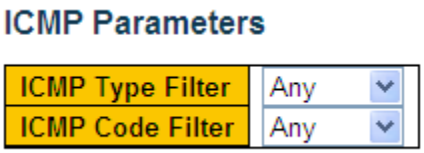


Рисунок 160 Настройка параметров ICMP

ICMP Type Filter

Варианты: Any/Specific（0~255）

По умолчанию: Any

Функция: Задание условий – тип ICMP. Если установлено значение Specific, нужно назначить тип ICMP. Когда тип ICMP в пакете IPv4, полученном входным портом, соответствует настройкам этого параметра, условие выполняется успешно.

ICMP Code Filter

Варианты: Any/Specific（0~255）

По умолчанию: Any

Функция: Задание условий – код ICMP. Если установлено значение Specific, нужно назначить код ICMP. Когда код ICMP в пакете IPv4, полученном входным портом, соответствует настройкам этого параметра, условие выполняется успешно.

➢ Настройте параметры UDP, как показано на рисунке 161.

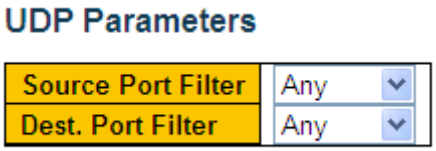


Рисунок 161 Настройка параметров UDP

Source Port Filter/ Destination Port Filter

Варианты: Any/ Specific（0~65535）/ Range（0~65535）

По умолчанию: Any

Функция: Задание условий для ID исходного порта UDP и ID порта назначения. Если установлено значение Specific, нужно назначить ID порта. Если установлено значение Range, нужно назначить диапазон ID порта. Когда ID порта UDP в пакете IPv4, полученном входным портом, соответствует настройкам этого параметра, условие выполняется успешно.

➢ Настройте параметры TCP, как показано на рисунке 162.

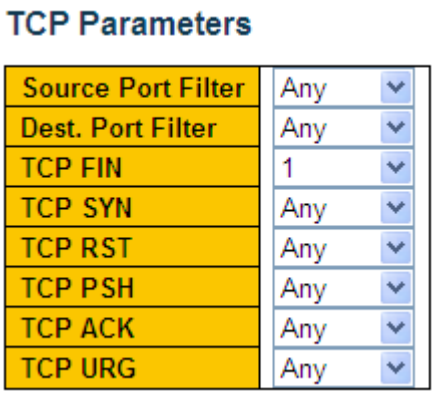


Рисунок 162 Настройка параметров TCP

Source Port Filter/ Destination Port Filter

Варианты: Any/ Specific（0~65535）/ Range（0~65535）

По умолчанию: Any

Функция: Задание условий для ID исходного порта TCP и ID порта назначения Если установлено значение Specific, нужно назначить ID порта. Если установлено значение Range, нужно назначить диапазон ID порта. Когда ID порта TCP в пакете IPv4, полученном входным портом, соответствует настройкам этого параметра, условие выполняется успешно.

TCP FIN/SYN/RST/PSH/ACK/URG

Варианты: Any/1/0

По умолчанию: Any

Функция: Задание условий для контрольных полей TCP. Когда контрольные поля TCP в пакете IPv4, полученном входным портом, соответствуют настройкам этого параметра, условие выполняется успешно.

- Настройте запись ACL, как показано на рисунке 163.

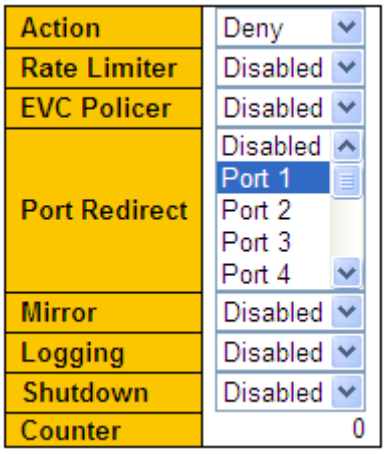


Рисунок 163 Настройка записи ACL

Action

Варианты: Deny/Permit/Filter

По умолчанию: Permit

Функция: Задать режим обработки входным портом пакета, соответствующего ACE. Значение Deny указывает на отбрасывание пакета, значение Permit указывает на пересылку пакета, а значение Filter указывает на фильтрацию пакета и необходимость выбора порта фильтрации.

Rate Limiter

Варианты: Disabled/1~16

По умолчанию: Disabled

Функция: отключить функцию ограничения скорости порта и выбрать ID ограничителя скорости.

EVC Policer

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Включить/выключить ограничитель EVC порта.

EVC Policer ID

Диапазон: 1~256

По умолчанию: 1

Функция: После включения ограничителя EVC настроить ID ограничителя EVC порта.

Предупреждение:

Ограничение скорости порта и политика EVC не могут быть включены одновременно.

Port Redirect

Варианты: Disabled/ любой порт

По умолчанию: Disabled

Функция: Включение/выключение функции перенаправления портов. После включения функции перенаправления портов пакеты, соответствующие какой-либо записи, будут перенаправлены на указанный порт.

Предупреждение:

Функцию перенаправления портов можно включить только если для параметра Action установлено значение Deny.

Mirroring

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Включение/выключение функции зеркалирования портов. После включения функции зеркалирования портов пакеты, соответствующие какой-либо

записи ACL, будут пересылаться как на порт назначения, так и на порт назначения зеркалирования.

Предупреждение:

Условием для включения зеркалирования портов ACL является наличие зеркального порта назначения.

Logging

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Включение/выключение функции регистрации порта.

Функция: Включение/выключение функции регистрации порта. Enabled: если порт получает пакет, который соответствует какой-либо записи ACL, пакет записывается в системный журнал.

Disabled: если порт получает пакет, который соответствует какой-либо записи ACL, пакет не записывается в системный журнал.

Shutdown

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: отключение порта. Enabled: если порт получает пакет, который соответствует какой-либо одной записи ACL, порт отключается. Disabled: если порт получает пакет, который не соответствует ни одной записи ACL, порт не отключается.

Counter

Функция: Отображение количества соответствующих ACE пакетов, которые каждый порт получает.

- Просмотрите записи ACL, как показано на рисунке 164.

ACL Status

User	ACE	Frame Type	Action	Rate Limiter	Mirror	CPU	Counter	Conflict
rp_mirror_cpu	1	EType	Filter	Disabled	Enabled	Yes	0	No
devSmacDrop	1	EType	Deny	Disabled	Disabled	No	0	No
bootp	1	IPv4/UDP 67-68	Filter	Disabled	Enabled	Yes	298	No
arp	1	ARP	Filter	Disabled	Enabled	Yes	199870	No
static	1	EType	Deny	Disabled	Disabled	No	0	No
static	4	Any	Permit	Disabled	Disabled	No	0	No
static	2	Any	Permit	Disabled	Disabled	No	0	No
static	3	IPv4/UDP 50	Permit	Disabled	Disabled	No	0	No
static	5	EType	Permit	Disabled	Disabled	No	0	No
static	6	IPv4/Other 0	Permit	Disabled	Disabled	No	0	No

Рисунок 164 Просмотр статистики ACL

Conflict

Варианты: No/Yes

Функция: Отображение статуса конфликта записи ACL. Если ресурсов для создания записи ACL недостаточно, для параметра **Conflict** для этой записи устанавливается значение **Yes**. В противном случае для параметра **Conflict** для этой записи установлено значение **No.**

10.3.4 Пример типовой конфигурации

Подключите порт 2 коммутатора. Настройте порт для получения пакетов только с исходного MAC-адреса 02-02-02-02-02-02 и пересылки пакетов через порт 1.

Этапы настройки:

1. Настройте действие порта Deny, как показано на рисунке 153.

2. Настройте запись ACL, установите входной порт 2, тип кадра Ethernet, как показано на рисунке 156.
3. Установите фильтр SMAC 02-02-02-02-02-02, как показано на рисунке 158.
4. Настройте действие записи ACL Deny, переадресацию на порт 1, как показано на рисунке 163.
5. Оставьте все остальные параметры со значениями по умолчанию или пустыми.

11 Агрегация портов

11.1 Статическая агрегация

11.1.1 Введение

Канал порта предназначен для привязки группы физических портов с одинаковой конфигурацией к логическому порту для увеличения пропускной способности и повышения скорости передачи. Порты-участники 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 агрегированный канал и становиться независимым логическим портом, тем самым увеличивая пропускную способность сети и обеспечивая резервирование канала.

11.1.2 Реализация

Как показано на рисунке 165, три порта на коммутаторах A и B объединяются, образуя канал портов. Пропускная способность канала портов — это общая пропускная способность этих трех портов.

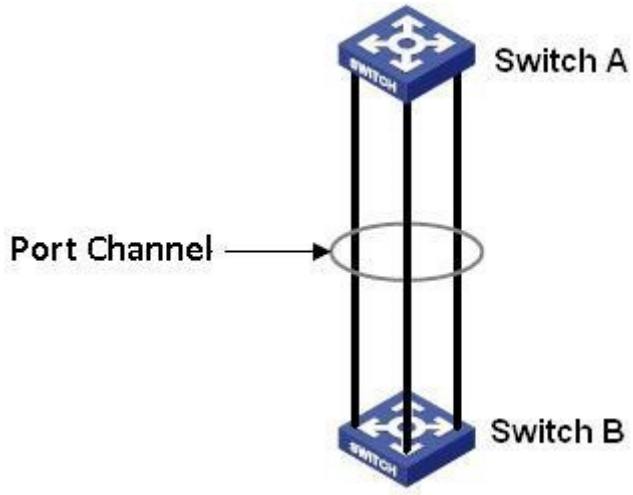


Рисунок 165 Канал портов

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

Предупреждение:

- Порт можно добавить только в одну группу портов.
- Только полнодуплексные порты могут присоединиться к агрегации.
- Для порта в канале портов нельзя включить LACP, а порт с включенным LACP нельзя добавить в канал портов.
- Канал портов и резервный порт являются взаимоисключающими. Порт в канале портов нельзя настроить как резервный порт, а резервный порт нельзя добавить в канал портов.
- Термин «резервный порт» в этом документе относится к кольцевому порту DT-Ring, резервному порту DT-Ring, кольцевому порту DRP, резервному порту DRP, порту RSTP и порту MSTP.

11.1.3 Настройка через веб-интерфейс

1. Настройте режим распределения нагрузки канала портов, как показано на рисунке 166.

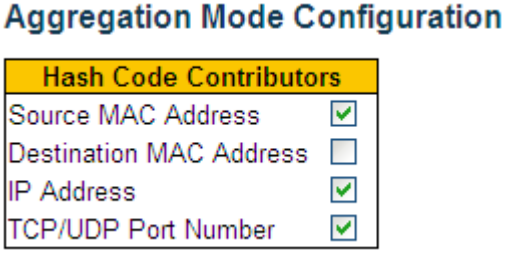


Рисунок 166 Настройка режима распределения нагрузки

Режим распределения нагрузки

Варианты: Source MAC Address/Destination MAC Address/IP Address/ TCP/UDP Port Number

По умолчанию: Source MAC Address/IP Address/ TCP/UDP Port Number

Функция: Задайте режим распределения нагрузки канала портов.

Описание: Source MAC Address указывает на распределение нагрузки на основе исходного MAC-адреса. Destination MAC Address указывает на распределение нагрузки на основе MAC-адреса назначения. IP Address указывает на распределение нагрузки на основе IP-адреса. TCP/UDP указывает на распределение нагрузки на основе номера порта TCP/UDP.

2. Настройте порты-участники группы агрегации, как показано на рисунке 167.

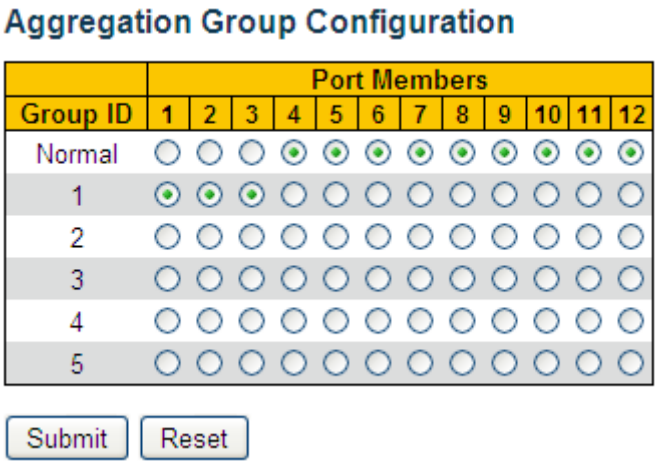


Рисунок 167 Настройка портов-участников группы агрегации

Port members

Функция: Выбор портов-участников группы агрегации.

Описание: Все порты в одной группе агрегации имеют одинаковую конфигурацию. Количество транковых групп зависит от количества портов коммутатора. Каждая группа включает в себя не более 8 портов.

11.1.4 Пример типовой конфигурации

Как показано на рисунке 165, добавьте три порта (порты 1, 2 и 3) коммутатора A в группу портов 1 и три порта (порты 1, 2 и 3) коммутатора B в группу портов 1. Используйте сетевые кабели, чтобы соединить эти порты, чтобы сформировать канал портов, реализуя распределение нагрузки между портами. (Предполагается,

что три порта на коммутаторах A и B имеют одинаковые атрибуты соответственно).

Настройка на коммутаторах:

1. Добавьте порты 1, 2 и 3 коммутатора A в группу портов 1, как показано на рисунке 167.
2. Добавьте порты 1, 2 и 3 коммутатора B в группу портов 1, как показано на рисунке 167.

11.2 LACP

11.2.1 Введение

Протокол управления агрегацией каналов Link Aggregation Control Protocol (LACP) основан на стандарте IEEE802.3ad. Он используется для обмена информацией с одноранговым портом через блок данных протокола управления агрегацией каналов (LACPDU), чтобы выбрать порт-участник в группе динамического агрегирования.

11.2.2 Реализация

Порт с поддержкой LACP информирует одноранговый порт о своем приоритете LACP локального оборудования, MAC-адресе оборудования, приоритете LACP порта, номере порта и значении ключа, отправляя сообщение LACPDU. Одноранговый порт согласовывает с локальным портом после получения сообщения LACPDU:

1. Сравнивает идентификаторы оборудования на обоих концах (идентификатор оборудования = приоритет оборудования LACP + MAC-адрес оборудования). Сначала сравниваются приоритеты LACP. Если приоритеты LACP совпадают, сравниваются MAC-адреса. В качестве основного (master) выбирается оборудование с наименьшим идентификатором.

2. Сравниваются идентификаторы портов оборудования master (идентификатор порта = приоритет порта LACP + номер порта). Сначала сравниваются приоритеты LACP. Если приоритеты LACP совпадают, сравниваются номера портов. Порт с меньшим идентификатором выбирается в качестве ссылочного порта.

3. Если этот порт и ссылочный порт имеют одинаковые значения ключей и одинаковые конфигурации атрибутов порта в состоянии Up, а одноранговые порты этого порта и ссылочного порта имеют одинаковые значения ключей и конфигурации атрибутов порта, этот порт может стать портом-участником группы динамической

агрегации.

11.2.3 Настройка через веб-интерфейс

1. Настройте порт LACP, как показано на рисунке 168.

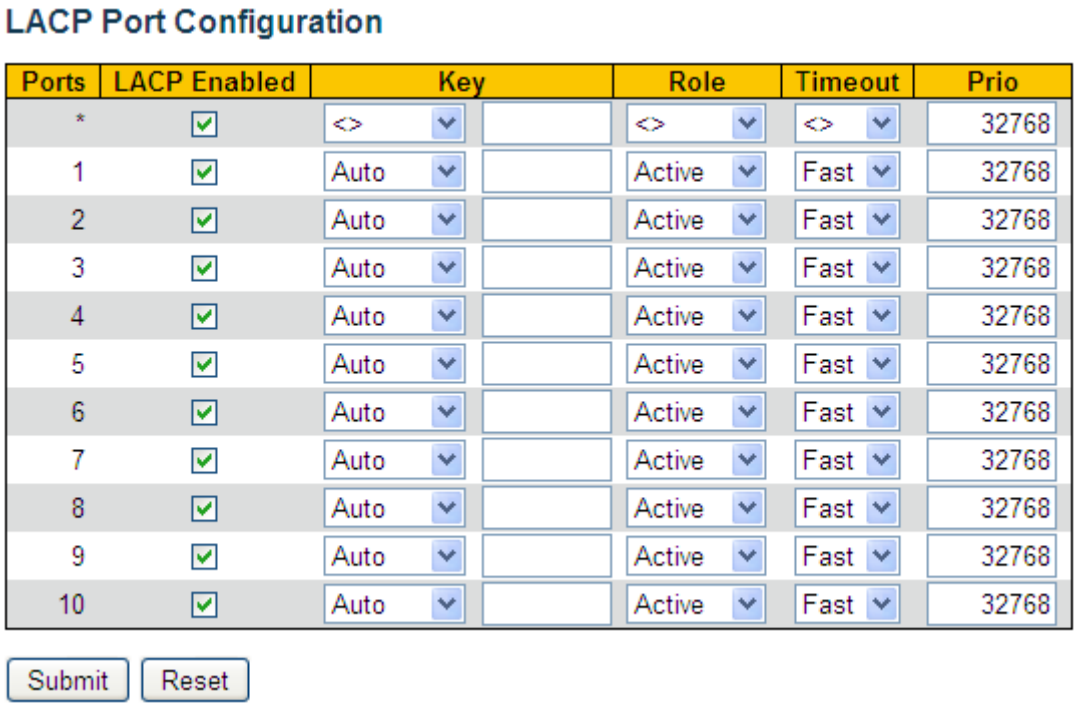


Рисунок 168 Настройка порта LACP

LACP Enabled

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение или выключение LACP для порта.

Key

Варианты: Auto/Specific (1~65535)

По умолчанию: Auto

Функция: Настройка значения ключа порта. Auto означает, что значение ключа зависит от скорости порта, ключ=1 (10 Мб), ключ=2 (100 Мб), ключ=3 (1000 Мб). Порты с разными значениями ключей не могут быть добавлены в группу агрегации.

Role

Варианты: Active/Passive

По умолчанию: Active

Функция: Выбор состояние роли LACP. Активный порт будет активно отправлять сообщения LACPDU на одноранговый порт. Пассивный порт будет отправлять сообщения LACPDU на одноранговый порт после получения сообщений LACPDU от однорангового порта.

Предупреждение:

Для двух подключенных портов как минимум один порт должен быть активным; в обмениваться информацией друг с другом.

Timeout

Варианты: Fast/Slow

По умолчанию: Fast

Функция: Настраивает интервал для активного порта для отправки сообщений LACPDU.

Fast указывает, что интервал равен 1 с. **Slow** Указывает, что интервал равен 30 с.

Prio

Варианты: 1~65535

По умолчанию: 32768

Функция: Настраивает приоритет LACP порта, который используется для выбора ссылочного порта. В качестве ссылочного порта выбирается порт с более низким приоритетом в ведущем оборудовании.

2. Просмотрите статус LACP системы, как показано на рисунке 169.

LACP System Status

Aggr ID	Partner System ID	Partner Key	Partner Prio	Last Changed	Local Ports
LLAG1	00-01-c1-01-00-02	2	32768	0d 00:00:28	1,2

Рисунок 169 Просмотр статуса LACP системы

3. Просмотрите статус LACP порта, как показано на рисунке 170.

LACP Status

Ports	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	Yes	2	LLAG1	00-01-c1-01-00-02	1	32768
2	Yes	2	LLAG1	00-01-c1-01-00-02	2	32768
3	Yes	2	-	-	-	-
4	Yes	2	-	-	-	-
5	No	-	-	-	-	-
6	No	-	-	-	-	-
7	No	-	-	-	-	-
8	No	-	-	-	-	-
9	No	-	-	-	-	-
10	No	-	-	-	-	-

Рисунок 170 Просмотр статуса LACP порта

LACP

Варианты: Yes/No

Функция: Просмотр статуса LACP для портов. Yes означает, что LACP включен, а порт в состоянии LinkUp. No означает, что LACP не включен, а порт в состоянии LinkDown.

4. Просмотрите статистику LACP порта, как показано на рисунке 171.

LACP Statistics

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	333	326	0	0
2	222	221	0	0
3	0	7	0	0
4	0	7	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0

Рисунок 171 Просмотр статистики LACP порта

11.2.4 Пример типовой конфигурации

Как показано на рисунке 165, добавьте три порта (порты 1, 2 и 3) коммутатора A в группу портов 1 и три порта (порты 1, 2 и 3) коммутатора B в группу портов 1. Используйте сетевые кабели, чтобы соединить эти порты, чтобы сформировать канал портов, реализуя распределение нагрузки между портами. (Предполагается,

что три порта на коммутаторах A и B имеют одинаковые атрибуты соответственно).

Настройка на коммутаторах:

1. Включите LACP на портах 1, 2 и 3 коммутатора A, как показано на рисунке 168.
2. Включите LACP на портах 1, 2 и 3 коммутатора B, как показано на рисунке 168.

12 Настройка обнаружения петель Loop Detect

12.1 Обзор

После того, как обнаружение петель включено для порта, пакеты обнаружения петель будут отправлены через порт, чтобы определить, существуют ли петли в сети, подключенной к порту. ЦП периодически отправляет в порт пакеты обнаружения петель. Если какой-либо порт коммутатора получает пакеты обнаружения петель, определяется, что в сети существуют петли. Отключите порт, который отправляет пакеты обнаружения петли, и через некоторое время порт автоматически подключится и продолжит обнаружение. Интервал времени для отправки пакетов обнаружения петель и время восстановления порта можно настроить в программном обеспечении.

Примечание:

Обнаружение петель и DT-Ring/DRP/RSTP/MSTP являются взаимоисключающими. Порт, для которого включено обнаружение петель, не может быть настроен как резервный порт; резервный порт не может быть включен для обнаружения петель.

12.2 Настройка через веб-интерфейс

1. Настройте функцию обнаружения петель для порта, как показано на рисунке 172.

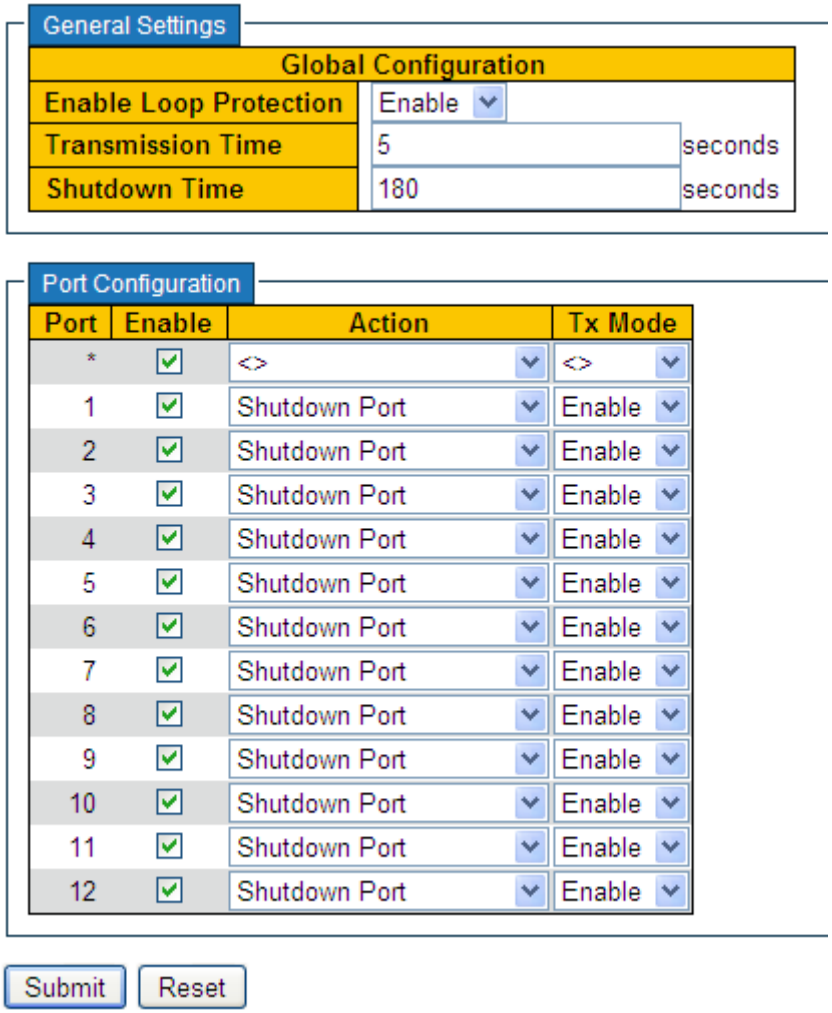


Рисунок 172 Настройка функции обнаружения петель для порта

Enable Loop Protection

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение или выключение глобальной функции обнаружения петель для порта

Transmission Time

Диапазон: 1~10 с

По умолчанию: 5 с

Функция: Настройка интервала времени для отправки пакетов обнаружения петель.

Shutdown Time

Диапазон: 0~604800 с

По умолчанию: 180 с

Функция: Настройка времени восстановления порта, 0 указывает, что порт не может быть подключен автоматически до перезапуска устройства.

Enable

Варианты: Enable/Disable

По умолчанию: Enable

Функция: Включение или выключение функции обнаружения петель для порта.

Action

Варианты: Shutdown Port/Shutdown Port and Log/Log Only

По умолчанию: Shutdown Port

Функция: Действие, которое будет выполняться, когда порт обнаружит наличие петли.

Tx Mode

Варианты: Enable/Disable

По умолчанию: Enable

Функция: Отправлять ли пакеты обнаружения петель или нет.

Предупреждение:

Порт может точно определить, существует ли петля, только после того, как защита от глобально, защита от петель и режим Tx включены на порту.

2. Просмотрите статус защиты от петель, как показано на рисунке 173.

Loop Protection Status

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Shutdown	Enabled	0	Up	-	-
2	Shutdown	Enabled	14	Down	-	2015-11-14T13:29:24+08:00
3	Shutdown	Enabled	8	Disabled	Loop	2015-11-14T13:30:55+08:00
4	Shutdown	Enabled	1	Down	-	2015-11-14T13:26:33+08:00
5	Shutdown	Enabled	0	Down	-	-
6	Shutdown	Enabled	0	Down	-	-
7	Shutdown	Enabled	0	Down	-	-
8	Shutdown	Enabled	0	Down	-	-
9	Shutdown	Enabled	0	Down	-	-
10	Shutdown	Enabled	0	Down	-	-
11	Shutdown	Enabled	0	Down	-	-
12	Shutdown	Enabled	0	Down	-	-

Рисунок 173 Просмотр статуса защиты от петель

Loop Protection Status

Варианты: --/Loop

Функция: Показать наличие петель в сети, когда функция обнаружения петель порта включена. Loop указывает на наличие петель, а -- указывает на отсутствие петель.

12.3 Пример типовой конфигурации

Требования к сети

Порт 3 коммутатора подключен к внешней сети. При наличии петель в сети отключите порт 3, как показано на рисунке 174.

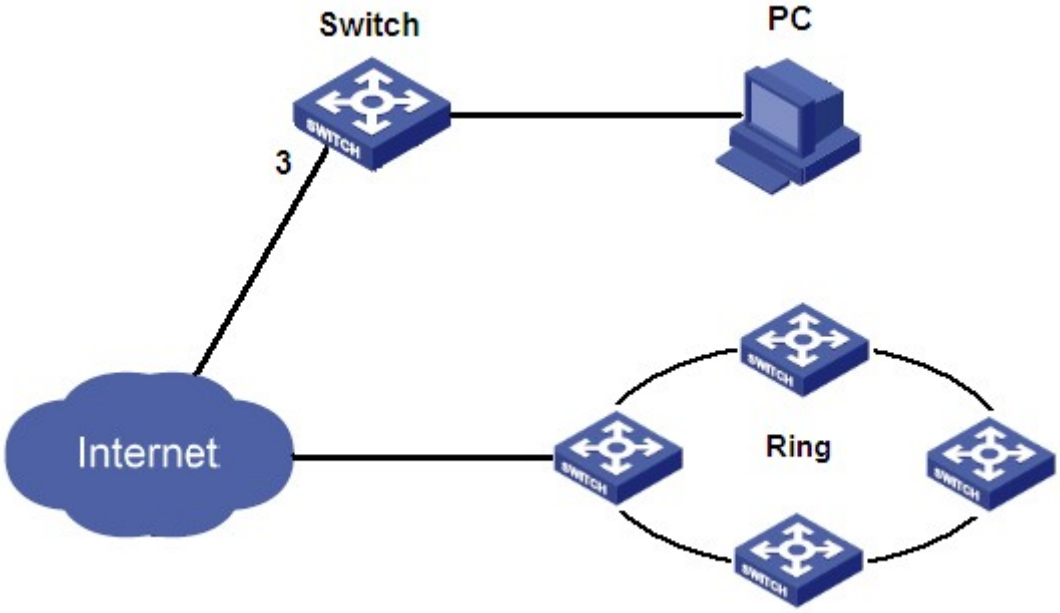


Рисунок 174 Пример обнаружения петли

Конкретная конфигурация:

Включите функцию обнаружения петель для порта 3, как показано на рисунке 172.

13 Промышленный протокол

13.1 EtherNet/IP

13.1.1 Введение

EtherNet/IP — это промышленный протокол прикладного уровня для приложений промышленной автоматизации. Он основан на стандартных протоколах TCP/IP и UDP/IP и использует стандартное аппаратное и программное обеспечение Ethernet для определения протокола прикладного уровня для настройки, доступа и управления устройствами промышленной автоматизации.

Эта серия коммутаторов позволяет пользователям устанавливать состояние порта (включить/отключить) с помощью протокола EtherNet/IP

для получения информации об устройстве, информации о инфо информаци инфор

и информации RSTP.

13.1.2 Настройка через веб-интерфейс

Настройте протокол EtherNet/IP, как показано на рисунке

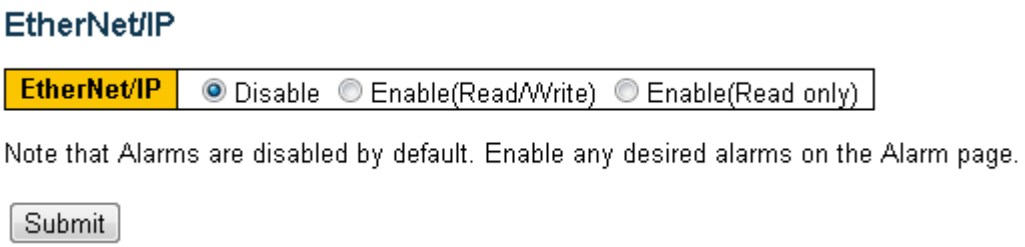


Рисунок 175 Настройка EtherNet/IP

Варианты**:** Disable/Enable(Read/Write)/Enable(Read Only)

По умолчанию**:** Disable

Функция: Включение EtherNet/IP и использование протокола EtherNet/IP для настройки состояния устройства.

13.2 ModbusTCP

13.2.1 Введение

Протокол ModbusTCP – это Modbus, основанный на Ethernet TCP/IP. Modbus — это протокол передачи сообщений прикладного уровня, который использует для связи Master/Slave (Master/Slave). Modbus — это простой прикладной протокол клиент/сервер. Сервер анализирует, обрабатывает запросы и отправляет ответы клиенту.

Эта серия коммутаторов позволяет пользователям устанавливать состояние порта (включить/отключить) с помощью протокола ModbusTCP для получения информации об устройстве, информации о порте, информации о тревоге, информации DT-ring, информации DRP и информации RSTP.

13.2.2 Настройка через веб-интерфейс

Настройте Включите протокол ModbusTCP, как показано на рисунке 176.

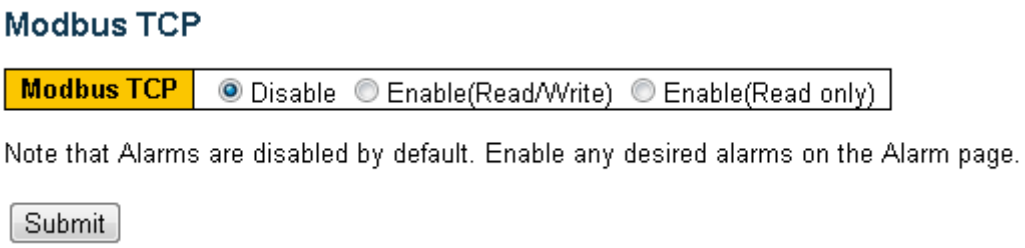


Рисунок 176 Настройка ModbusTCP

Варианты**:** Disable/Enable(Read/Write)/Enable(Read Only)

По умолчанию**:** Disable

Функция: Включение ModbusTCP и использование протокола ModbusTCP для настройки состояния устройства.

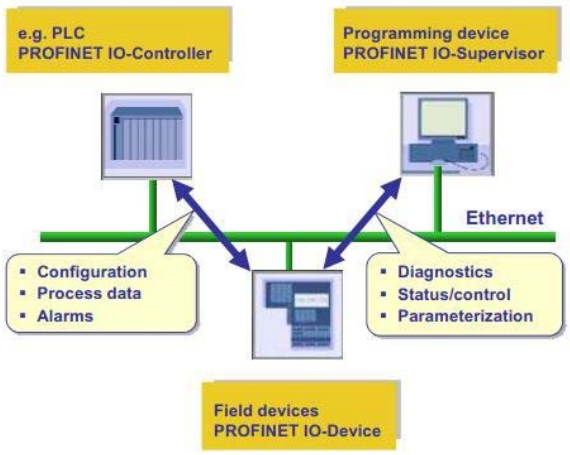
13.3 PROFINET

13.3.1 Введение

PROFINET — это промышленная коммуникационная сеть на основе Ethernet для всех видов приложений от PROFIBUS International (PI). Она охватывает как нынешние, так и перспективные ключевые рынки, и ключевые технологии

автоматизации. Благодаря реализации PROFINET I/O можно легко автоматизировать производство и процессы. Кроме того, обмен данными по PROFINET I/O осуществляется между контроллером ввода/вывода (ПЛК и т. д.) и устройствами ввода/вывода (полевыми устройствами).

В сетевой структуре PROFINET I/O есть три основные роли. Это контроллер ввода/вывода, супервизор ввода/вывода и устройства ввода/вывода. Реализуется модель поставщика и потребителя для обмена данными. Подробное описание приведено ниже.



Контроллер ввода/вывода

Контроллер ввода/вывода – это роль для управления устройством ввода/вывода. В сети PROFINET I/O может существовать ровно один контроллер. Однако это позволяет нескольким контроллерам реализовать резервирование системы. Типичным контроллером является программируемый логический контроллер (ПЛК), на котором выполняется программа автоматизации.

Супервизор ввода/вывода

Супервизор ввода-вывода может быть устройством программирования, которое управляет контроллером ввода-вывода, персональным компьютером или устройством HMI для ввода в эксплуатацию или диагностики.

Устройство ввода/вывода

Устройство ввода-вывода — это распределенное полевое устройство, которое подключено к одному или нескольким контроллерам ввода-вывода через PROFINET I/O. Оно периодически отправляет данные коммутатора на контроллер в соответствии

с поддерживаемым временем цикла.

Коммутатор PROFINET работает как устройство PROFINET I/O. Он поддерживает множество полезных атрибутов для настройки или мониторинга контроллера ввода-вывода. Атрибуты подробно описаны в файле GSD и в следующей теме.

GSD

Коммутатор PROFINET в качестве устройства ввода-вывода должен предоставить описание файла GSD, чтобы гарантировать, что устройство может быть идентифицировано контроллером. Файл GSD I/O моделирует коммутационное оборудование PROFINET и использует язык GSDML для формирования файла. Таким образом, устройство можно настроить и смоделировать с помощью программного обеспечения STEP7 или TIA PORTAL. Файл GSD подробно описывает функции, поддерживаемые устройством.

13.3.2 Настройка через веб-интерфейс

Настройте протокол PROFINET, как показано на рисунке 177.

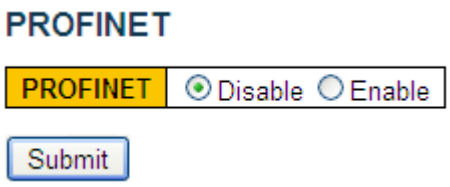


Рисунок 177 Настройка PROFINET

Варианты: Disable/Enable

По умолчанию: Disable

Функция: Включение/отключение протокола PROFINET

14 Многоадресная рассылка

14.1 IGMP Snooping

14.1.1 Введение

Отслеживание IGMP — 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.

Есть три версии протокола IGMP: IGMPv1, IGMPv2 и IGMPv3. Версия IGMPv1 определена в RFC1112, IGMPv2 определена в RFC2236, а IGMPv3 определена в RFC3376.

IGMPv1 поддерживает два типа пакетов (пакеты отчетов и запросов) и определяет базовый процесс запроса и отчета члена группы.

Протокол IGMPv2, построенный на основе IGMPv1, предоставляет пакет выхода механизма быстрого выхода для членов группы. При использовании этого механизма, когда последний участник покидает группу многоадресной рассылки, маршрутизатор получает указание провести быструю конвергенцию. По сравнению с IGMPv1, IGMPv2 поддерживает два типа пакетов запросов: общий пакет запроса и пакет запроса для конкретной группы. Коммутатор периодически отправляет пакет общего запроса для запроса членства. Когда хост покидает группу многоадресной рассылки, после получения коммутатором сообщения о выходе коммутатор отправляет пакет запроса для конкретной группы, чтобы определить, все ли члены покидают группу многоадресной рассылки.

В IGMPv3 добавлена функция фильтрации источника хоста. Эта функция позволяет хосту указать, следует ли принимать или отклонять пакеты от определенных источников группы многоадресной рассылки.

14.1.2 Основная концепция

Генератор запросов 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 генераторов запросов, автоматически выбирается тот, у которого наименьший IP-адрес, в качестве запрашивающего. Только выбранный генератор запросов периодически отправляет пакеты общего запроса IGMP. Другие генераторы запросов только получают и пересылают пакеты запросов IGMP.

Маршрутизирующий порт: получает пакеты общего запроса (на коммутаторе с поддержкой IGMP) от генератора запросов. После получения ответа IGMP коммутатор создает запись многоадресной рассылки и добавляет порт, который получает отчет IGMP, в список портов-участников. Если маршрутизирующий порт существует, он также добавляется в список портов-участников. Затем коммутатор пересылает отчет IGMP другим устройствам через маршрутизирующий порт, чтобы другие устройства создали ту же запись многоадресной рассылки.

Прокси IGMP Snooping: Функция прокси-сервера IGMP snooping настраивается на граничном устройстве, чтобы уменьшить количество пакетов отчетов IGMP и оставить пакеты, полученные вышестоящим устройством, тем самым повышая общую производительность вышестоящего устройства. Устройство, на котором настроена функция прокси-сервера IGMP snooping, работает как хост для вышестоящего устройства и работает как генератор запросов для нижестоящего хоста.

14.1.3 Принцип работы

IGMP Snooping управляет и поддерживает членов группы многоадресной рассылки путем обмена пакетами related между устройствами с поддержкой IGMP. Пакеты related следующие:

Пакет общего запроса: Генератор запросов периодически отправляет пакеты общего запроса (IP-адрес назначения 224.0.0.1) чтобы подтвердить, есть ли в группе многоадресной рассылки порты-участники. После получения пакета запроса устройство, не являющееся генератором запросов, пересылает пакет на все подключенные к нему порты.

Пакет конкретного запроса: Если устройство хочет выйти из группы многоадресной рассылки, оно отправляет пакет IGMP leave. После получения пакета leave

запрашивающая сторона отправляет пакет конкретного запроса(IP-адрес назначения: IP-адрес группы многоадресной рассылки), чтобы убедиться, что группа содержит другие порты-участники.

Пакет с отчетом участника: Если устройство хочет получить данные группы многоадресной рассылки, оно отправляет пакет IGMP report (IP-адрес назначения: IP-адрес группы многоадресной рассылки) немедленно в ответ на пакет запроса IGMP группы.

Пакет выхода: Если устройство хочет выйти из группы многоадресной рассылки, оно отправляет пакет IGMP leave (IP-адрес назначения: 224.0.0.2).

14.1.4 Настройка через веб-интерфейс

1. Включите IGMP Snooping, как показано на рисунке 177.

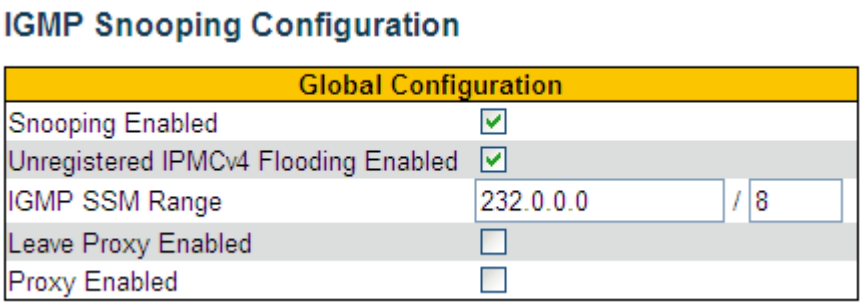


Рисунок 177 Включение IGMP Snooping

Snooping Enabled

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение или выключение глобального протокола IGMP Snooping.

Unregistered IPMCv4 Flooding Enabled

Варианты: Enable/Disable

По умолчанию: Enable

Функция: Настройка действия при получении незарегистрированного многоадресного пакета. Enable: при получении незарегистрированного многоадресного пакета коммутатор транслирует пакет в пределах VLAN (все порты, кроме входного). Disable: при получении незарегистрированного многоадресного пакета коммутатор отбрасывает его. Незарегистрированные многоадресные пакеты относятся к многоадресным пакетам без соответствующих записей о пересылке на коммутаторе.

IGMP SSM Range

Формат: A.B.C.D/ 4~32

По умолчанию: 232.0.0.0/8

Функция: Только хосты и маршрутизаторы с адресом в пределах значения этого параметра могут запускать модель службы многоадресной рассылки IGMP (SSM) при условии, что хосты и маршрутизаторы поддерживают модель службы IGMP SSM. Модель службы SSM предоставляет пользователям услугу передачи, определяющую источники многоадресной рассылки для клиента.

Leave Proxy Enabled

Варианты: Enabled/Disabled
По умолчанию: Disabled

Функция: Включение/выключение функции пересылки пакетов leave генератору запросов. Когда функция включена, пакеты leave не пересылаются.

Proxy Enabled

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Включение/выключение функции пересылки пакетов leave и пакетов отчетов участников генератору запросов. Когда функция включена, пакеты leave и пакеты отчетов участников не пересылаются.

2. Настройте порт IGMP, как показано на рисунке 178.

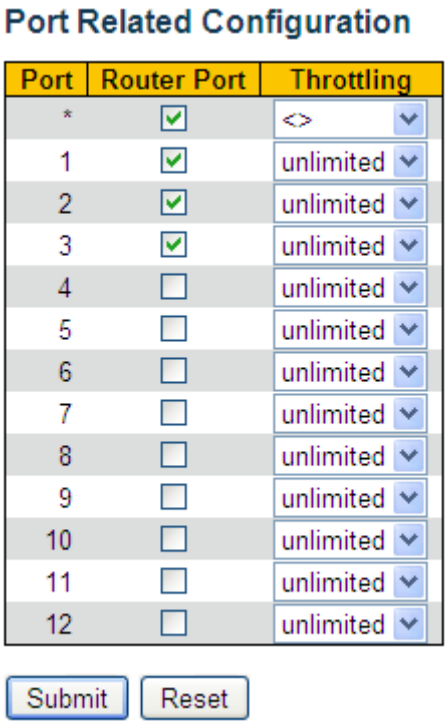


Рисунок 178 Настройка порта IGMP

Маршрутизирующий порт

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Настройка порта маршрутизатора.

Throttling

Варианты: unlimited/1~10

По умолчанию: unlimited

Функция: Включение/выключение функции ограничения количества записей многоадресной рассылки, полученных портом.

3. Настройте IGMP Snooping VLAN, как показано на рисунке 179.

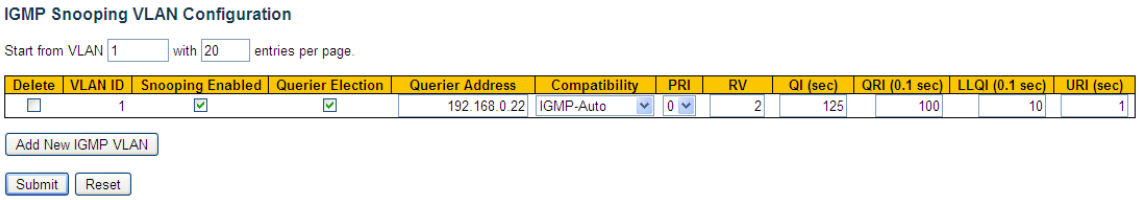


Рисунок 179 Настройка IGMP Snooping VLAN

VLAN ID

Варианты: все созданные VLAN ID

Snooping Enabled

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение или выключение функции VLAN IGMP Snooping.

Предварительным условием для этой функции является включение глобальной функции IGMP Snooping.

Querier Election

Варианты: Enable/Disable

По умолчанию: Enable

Функция: Включение или выключение функции IGMP query для выбранной VLAN. Предварительным условием для этой функции является включение глобальной функции IGMP Snooping и функции VLAN IGMP Snooping.

Описание: Когда в сети существует несколько генераторов запросов, автоматически выбирается тот, у которого наименьший IP-адрес, в качестве запрашивающего. Если есть только одно устройство, на котором включена функция IGMP query , оно будет генератором запросов.

Querier Address

Формат: A.B.C.D

Функция: Настройка исходящего IP-адреса для отправки пакетов с запросом. Если адрес генератора запросов не задан, в качестве адреса генератора запросов используется IP-адрес порта VLAN.

Compatibility

Варианты: IGMP-Auto/Forced IGMPv1/Forced IGMPv2/Forced IGMPv3

По умолчанию: IGMP-Auto

Функция: Настройка версии IGMP.

PRI (Priority of Interface)

Диапазон: 0~7

По умолчанию: 0

Функция: Настройка приоритета пакета управления IGMP.

RV (Robustness Variable)

Диапазон: 1~255

По умолчанию: 2

Функция: Настройка параметра надежности функции IGMP query.

Описание: Чем больше параметр, тем хуже сетевое окружение. Пользователь может установить подходящий параметр надежности в соответствии с реальной сетью.

QI (Query Interval)

Диапазон: 1~31744 с

По умолчанию: 125 с

Функция: Настройка интервала отправки пакета общего запроса.

QRI (Query Response Interval)

Диапазон: 0~31744（ед.: 0,1 с）

По умолчанию: 100

Функция: Настройка максимального времени ответа на пакет общего запроса.

LLQI (Last Member Query Interval)

Диапазон:0~31744（ед.: 0,1 с）

По умолчанию:10

Функция: Настройка максимального времени ответа на пакет конкретного запроса.

Предупреждение:

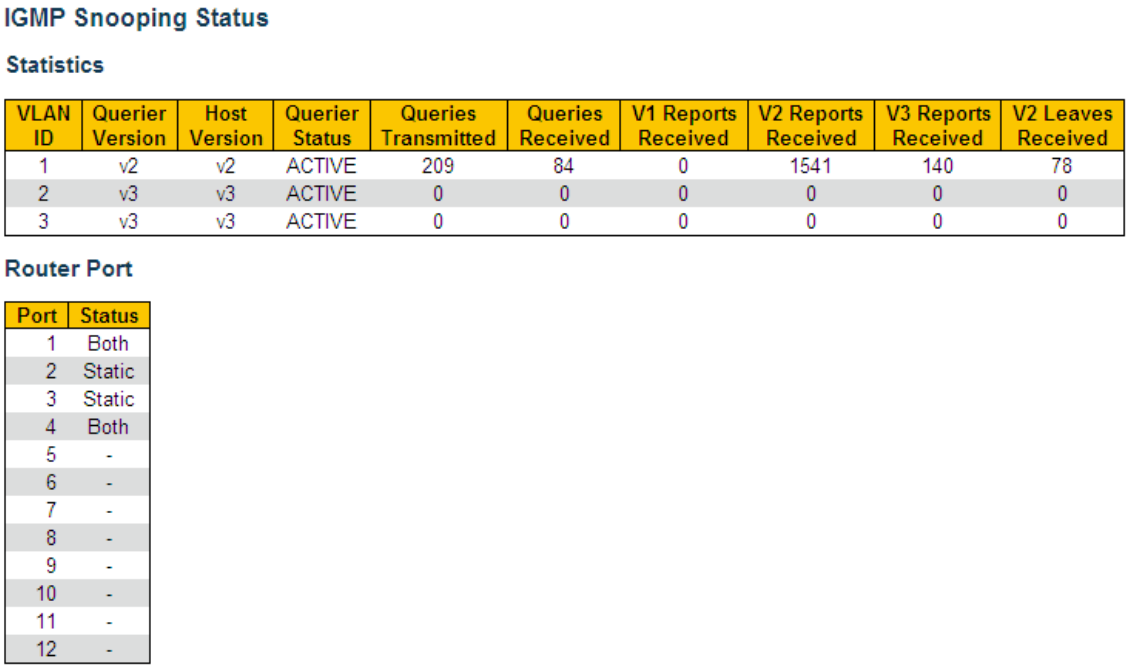
Конфигурация QI, QRI и LLQI действительна только для генератора запросов.

URI (Unsolicited Report Interval)

Диапазон: 0~31744 с
По умолчанию: 1 с

Функция: Задание интервала повторной отправки хостом пакета отчета для присоединения к группе многоадресной рассылки. Щелкните <Add New IGMP VLAN>, чтобы настроить запись IGMP Snooping VLAN. Поддерживается не более 32 записей IGMP Snooping VLAN.

4. Просмотрите статус IGMP Snooping, как показано на рисунке 180.



IGMP Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
1	v2	v2	ACTIVE	209	84	0	1541	140	78
2	v3	v3	ACTIVE	0	0	0	0	0	0
3	v3	v3	ACTIVE	0	0	0	0	0	0

Router Port

Port	Status
1	Both
2	Static
3	Static
4	Both
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-

Рисунок 180 Просмотр статуса IGMP Snooping

Router Port Status

Варианты: Both/Static/Dynamic

Функция: Отображение состояния порта маршрутизатора. Static указывает, что порт статически настроен как маршрутизирующий порт, Dynamic указывает, что порт динамически определяется как маршрутизирующий порт, а Both указывает, что порт статически настраивается как маршрутизирующий порт или динамически определяется как маршрутизирующий порт.

5. Просмотрите список участников многоадресной рассылки, как показано на рисунке 181.

VLAN ID	Groups	Port Members											
		1	2	3	4	5	6	7	8	9	10	11	12
1	224.0.1.1	✓		✓									
1	225.10.24.3	✓		✓									
1	226.81.9.8	✓		✓									
1	239.2.11.71	✓		✓									
1	239.5.5.5	✓		✓									
1	239.77.124.213	✓		✓									
1	239.255.255.250	✓		✓									
1	239.255.255.254	✓		✓									

Рисунок 181 Список участников многоадресной рассылки

14.1.5 Пример типового использования

Как показано на рисунке 182, включите IGMP Snooping на коммутаторе 1, коммутаторе 2 и коммутаторе 3. Включите функцию автоматического запроса на коммутаторе 2 и коммутаторе 3. IP-адрес коммутатора 2 192.168.1.2, а IP-адрес коммутатора 3 192.168.0.2, таким образом коммутатор 3 выбран в качестве генератора запросов.

1. Включите IGMP Snooping.
2. Включите IGMP Snooping и автозапрос.
3. Включите IGMP Snooping и автозапрос.

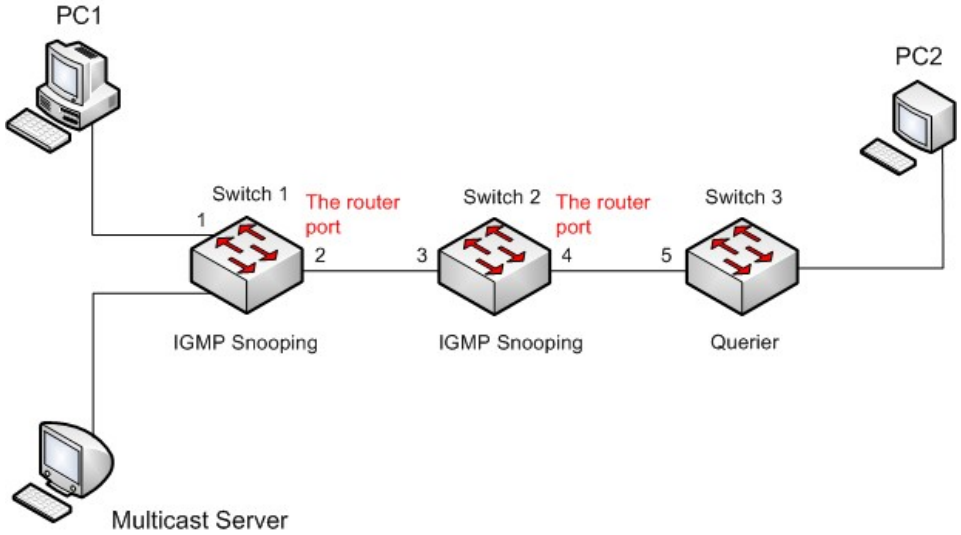


Рисунок 182 Пример использования IGMP Snooping

➢ Поскольку коммутатор 3 выбран в качестве генератора запросов, он периодически

отправляет сообщение общего запроса.

- Порт 4 коммутатора 2 получает сообщение запроса. Он становится портом маршрутизатора. Между тем, коммутатор 2 пересылает сообщение запроса с порта 3. Затем порт 2 коммутатора 1 выбирается в качестве порта маршрутизатора, как только он получает запрос от коммутатора 2.
- Когда ПК 1 присоединяется к группе многоадресной рассылки 225.1.1.1, он отправляет сообщение отчета IGMP, поэтому порт 1 и маршрутизирующий порт 2 коммутатора 1 также присоединяются к группе многоадресной рассылки 225.1.1.1. Затем сообщение с отчетом IGMP будет перенаправлено на коммутатор 2 через маршрутизирующий порт 2, поэтому порт 3 и порт 4 коммутатора 2 также присоединятся к 225.1.1.1, а затем сообщение с отчетом IGMP будет перенаправлено на коммутатор 3 через маршрутизирующий порт 4, поэтому порт 5 коммутатора 3 также присоединится к 225.1.1.1.
- Когда многоадресные данные сервера многоадресной рассылки достигают коммутатора 1, данные будут перенаправлены на ПК1 через порт 1; поскольку маршрутизирующий порт 2 также является участником группы многоадресной рассылки, данные многоадресной рассылки будут пересылаться маршрутизирующим портом. Таким образом, когда данные достигнут порта 5 коммутатора 3, их пересылка прекратится, поскольку приемника больше нет, но если ПК2 также присоединится к группе 255.1.1.1, данные многоадресной рассылки будут перенаправлены на ПК2.

14.2 GMRP

14.2.1 GARP. Введение

Протокол GARP (Generic Attribute Registration Protocol) используется для распространения, регистрации и отмены определенной информации (VLAN, адрес многоадресной рассылки) между коммутаторами в одной сети. При использовании GARP информация о конфигурации участника GARP будет распространяться по всей сети коммутатора. Устройства, поддерживающие GARP, передают друг другу инструкции о регистрации или отмене тех или иных настроек путём отправки соответствующих сообщений join/leave. Участник также регистрирует или отменяет информацию о конфигурации других участников на основе сообщений join/leave,

отправленных другими участниками.

GARP включает в себя три типа сообщений: Join, Leave и LeaveAll.

- Когда прикладной объект GARP хочет зарегистрировать свою собственную информацию на других коммутаторах, объект отправляет сообщение Join. Сообщения Join делятся на два типа: JoinEmpty и JoinIn. Сообщение JoinIn отправляется для объявления зарегистрированного атрибута, а сообщение JoinEmpty отправляется для объявления еще не зарегистрированного атрибута.
- Когда прикладной объект GARP хочет удалить свою собственную информацию на других коммутаторах, объект отправляет сообщение Leave.
- После запуска объекта GARP он запускает таймер LeaveAll. Когда период таймера истекает, объект отправляет сообщение LeaveAll.

Предупреждение:

Объект указывает порт с поддержкой GARP.

Таймеры GARP – это таймер Hold, таймер Join, таймер Leave и таймер LeaveAll.

- Таймер Hold: При получении регистрационного сообщения объект GARP не сразу отправляет сообщение о присоединении, а запускает таймер Hold. Когда период таймера истекает, объект отправляет все регистрационные сообщения, полученные в течение предшествующего периода, в одном сообщении о присоединении, сокращая отправку пакетов для повышения стабильности сети.
- Таймер Join: Чтобы гарантировать получение сообщений Join другими прикладными объектами, прикладной объект GARP запускает таймер Join после отправки сообщения Join. Если сообщение JoinIn не получено до истечения периода таймера Join, объект снова отправляет сообщение Join. Если сообщение JoinIn получено до истечения периода таймера Join, объект не отправляет второе сообщение Join.
- Таймер Leave: Когда прикладной объект GARP хочет удалить информацию об атрибуте, объект отправляет сообщение Leave. Объект, получивший сообщение, запускает таймер Leave. Если сообщение Join не получено до истечения периода таймера, объект, получивший сообщение, удаляет информацию об атрибуте.
- Таймер LeaveAll: После запуска объекта GARP он запускает таймер LeaveAll. Когда период таймера истекает, объект отправляет сообщение LeaveAll, чтобы другие

прикладные объекты GARP перерегистрировали все атрибуты. Затем объект снова запускает таймер LeaveAll для нового цикла.

14.2.2 Протокол GMRP

GARP Multicast Registration Protocol (GMRP) – это протокол регистрации многоадресной передачи, основанный на GARP. 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 информацию о регистрации локальной многоадресной рассылки на другие коммутаторы. Этот механизм обмена информацией обеспечивает согласованность многоадресной информации, поддерживаемой всеми коммутаторами с поддержкой GMRP в сети.

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.

Пояснение:

Порт агента:указывает порт, на котором включены GMRP и функция агента. Порт распространения: указывает порт, на котором включен только GMRP, но не функция прокси.

Для GMRP необходимо наличие одного и нескольких портов агента. Динамически изученная запись многоадресной рассылки GMRP и запись агента перенаправляются портом распространения на порты распространения устройств более низкого уровня.

Все таймеры GMRP в одной сети должны поддерживать согласованность во избежание взаимных помех. Таймеры должны соответствовать следующим правилам: Таймер Hold < таймер Join, 2*таймер Join < таймер Leave, таймер Leave <таймер LeaveAll.

14.2.3 Настройка через веб-интерфейс

1.Глобальная настройка GMRP показана на рисунке 183.

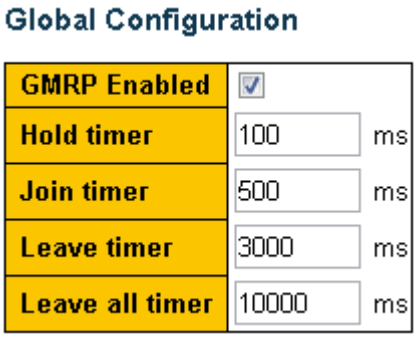


Рисунок 183 Глобальная настройка GMRP

GMRP Enabled:

Варианты: Enable/Disabled

По умолчанию: Disabled

Функция: Включение глобальной функции GMRP

Timer:

Варианты: Таймер Hold/таймер Join/таймер Leave/таймер Leave all

По умолчанию: 100/500/3000/10000 мс

Функция: Задание значения глобального таймера GMRP.

2.Настройка порта GMRP показана на рисунке 184.

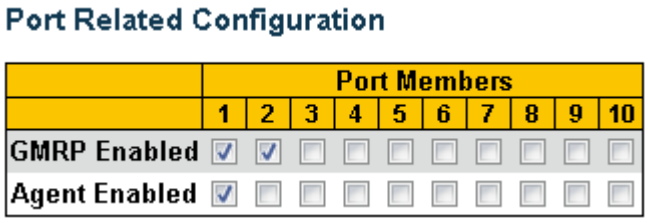


Рисунок 184 Настройка порта GMRP

GMRP Enabled:

Варианты: Enable/Disable

По умолчанию: Disabled

Функция: Включение GMRP для порта

Agent Enabled:

Варианты: Enabled/Disabled

По умолчанию: Disabled

Функция: Включение агента GMRP для порта.

3.Конфигурация таблицы MAC-адресов агента показана на рисунке 185.

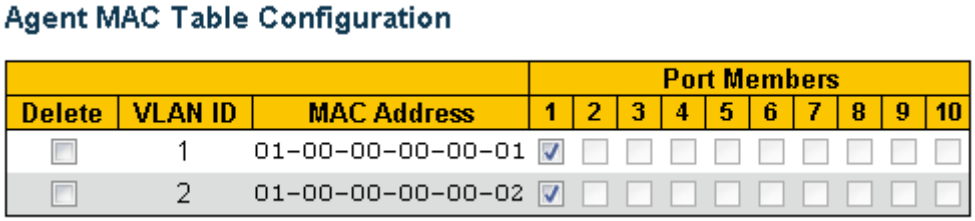


Рисунок 185 Конфигурация таблицы MAC-адресов агента

Функция: Настройка статического MAC-адрес агента многоадресной рассылки, привязанный к порту и VLAN.

Примечание: Для настройки этого элемента необходимо одновременно включить глобальный GMRP, порт GMRP и порт GMRP proxy.

4.Состояние таблицы MAC-адресов GMRP показана на рисунке 186.

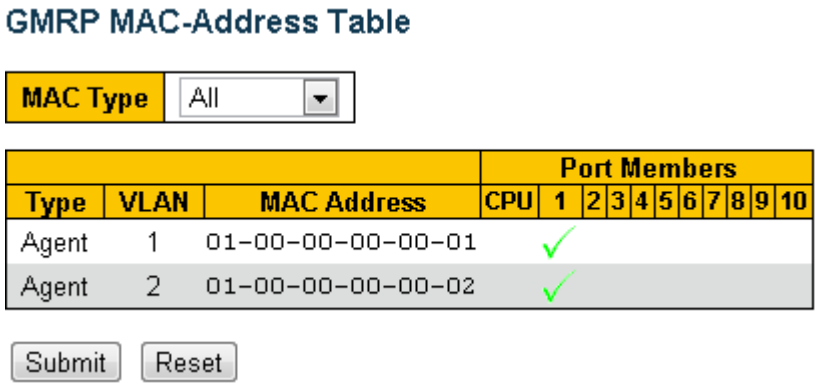


Рисунок 186 Состояние таблицы MAC-адресов GMRP

MAC Type:

Варианты: All/Agent/Dynamic

По умолчанию: All

14.2.4 Пример типового использования

Как показано на рисунке 187, коммутатор A и коммутатор B соединены через порты 2. Порт 1 коммутатора A настроен как порт-агент и содержит две записи многоадресной рассылки:

- MAC-адрес: 01-00-00-00-00-01, VLAN: 1
- MAC-адрес: 01-00-00-00-00-02, VLAN: 2

После настройки различных атрибутов VLAN на портах наблюдайте за динамической регистрацией между коммутаторами и обновлением информации о многоадресной рассылке.

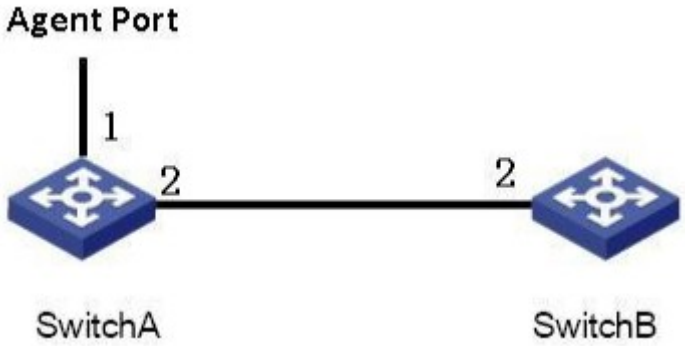


Рисунок 187 Сеть GMRP

Конфигурация коммутатора A:

1. Включите глобальную функцию GMRP на коммутаторе A; установите для таймера LeaveAll значение по умолчанию, как показано на рисунке 183.
2. Включите функцию GMRP и функцию агента на порту 1; включите только функцию GMRP на порту 2; установите таймеры на значения по умолчанию, как показано на рисунке 184.
3. Настройте запись агента многоадресной рассылки.
   Установите <MAC address, VLAN ID, Member port> <01-00-00-00-00-01, 1, 1> и <01-00-00-00-00-02, 2, 1>, как показано на рисунке 185.

Конфигурация коммутатора B:

1. Включите глобальную функцию GMRP на коммутаторе B; установите для таймера LeaveAll значение по умолчанию, как показано на рисунке 183.
2. Включите функцию GMRP на порту 2; установите таймеры на значения по умолчанию, как показано на рисунке 184. В таблице 6 перечислены динамически полученные записи многоадресной рассылки GMRP на коммутаторе B.

Таблица 6 Динамические записи многоадресной рассылки

Приглашение	**Вариант представления**	**Функция**	**Команда для переключения представления**
SWITCH #	Привилегированный режим	Просмотр недавно использованных команд. Просмотр версии программного обеспечения. Просмотр информации об ответе на операцию ping. Выгрузка/загрузка файла конфигурации. Восстановление конфигурации по умолчанию. Перезагрузка коммутатора.	Введите “**configure terminal**” для переключения из привилегированного режима в режим настройки. Введите “**exit**” для возврата в общий режим.
SWITCH（config）#	Режим настройки	Настройка всех функций коммутатора.	Введите "**exit**" или "**end**" для возврата в привилегированный режим.

14.3 Действие при получении незарегистрированного многоадресного пакета

Настройка через WEB-интерфейс показана на рисунке 188.

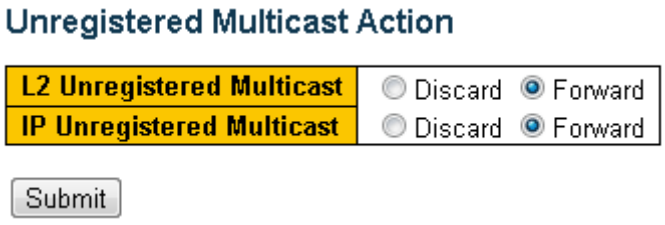


Рисунок 188 Действие при получении незарегистрированного многоадресного пакета

L2 Unregistered Multicast:

Варианты: Discard/Forward

По умолчанию: Forward

IP Unregistered Multicast:

Варианты: Discard/Forward

По умолчанию: Forward

15 LLDP

15.1 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.

15.2 Настройка через веб-интерфейс

1. Настройте LLDP, как показано на рисунке 189.

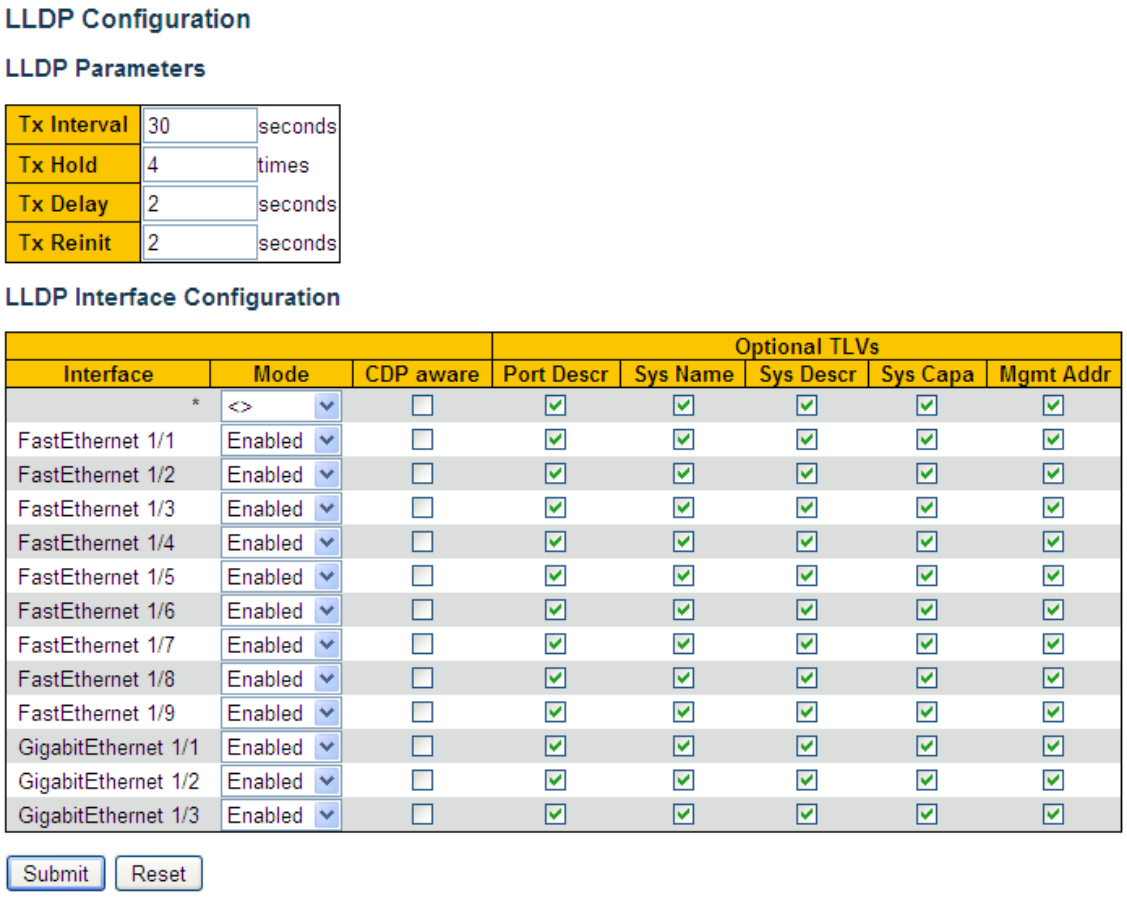


Рисунок 189 Настройка LLDP

Tx Interval

Диапазон: 5~32768 с

По умолчанию: 30 с

Функция: Настройка интервала времени для отправки пакетов LLDP.

Tx Hold

Диапазон: 2~10 раз

По умолчанию: 4 раза

Функция: Настройка количества удержаний Tx. Эффективная длительность пакета LLDP = Tx Interval x Tx Hold.

Tx Delay

Диапазон: 1~8192 с

По умолчанию: 2 с

Функция: Задание интервала передачи между новым пакетом LLDP и предыдущим пакетом LLDP после изменения информации о конфигурации. Значение Tx Delay не может превышать 1/4 значения Tx Interval.

Tx Reinit

Диапазон: 1~10 с

По умолчанию: 2 с

Функция: После отключения LLDP на порту или перезапуска коммутатора коммутатор отправляет кадр отключения LLDP соседнему узлу, чтобы объявить, что предыдущий пакет LLDP недействителен.

Tx Reinit относится к интервалу между передачей кадра выключения LLDP и повторной инициализацией пакета LLDP.

Mode

Варианты: Enabled/Disabled/Rx only/Tx only

По умолчанию: Enabled

Функция: Настройка режима пакетов LLDP. Режим Enabled указывает, что коммутатор может отправлять пакеты LLDP, а также получать и идентифицировать пакеты LLDP; режим Disabled указывает, что коммутатор не отправляет пакеты LLDP и не принимает

пакеты LLDP; режим only Rx указывает, что коммутатор только принимает и идентифицирует пакеты LLDP; единственный Tx only указывает, что коммутатор только отправляет пакеты LLDP.

Port Descr

Варианты: Enabled/Disabled

По умолчанию: Enabled

Функция: Enable указывает, что пакеты LLDP будут содержать описание порта.

Sys Name

Варианты: Enabled/Disabled

По умолчанию: Enabled

Функция: Enable указывает, что пакеты LLDP будут содержать имя системы.

Sys Descr

Варианты: Enabled/Disabled

По умолчанию: Enabled

Функция: Enable указывает, что пакеты LLDP будут содержать описание системы.

Sys Capa

Варианты: Enabled/Disabled

По умолчанию: Enabled

Функция: Enable указывает, что пакеты LLDP будут содержать возможности системы.

Mgmt Addr

Варианты: Enabled/Disabled

По умолчанию: Enabled

Функция: Enable указывает, что пакеты LLDP будут содержать адрес управления.

2. Просмотрите информацию о соединениях LLDP, как показано на рисунке 190.

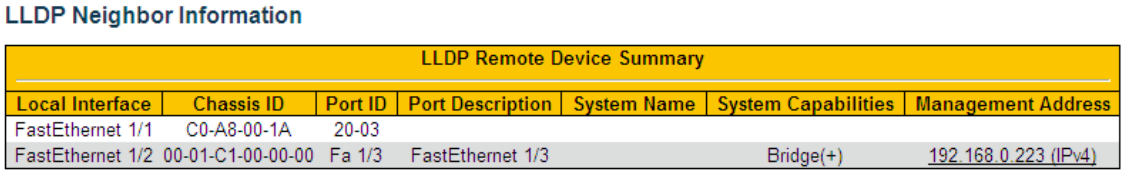


Рисунок 190 Информация LLDP

Предупреждение:

Для отображения информации LLDP необходимо включить LLDP на двух подключенных устройствах.

16 Настройка MAC-адреса

16.1 Введение

При пересылке пакета коммутатор ищет порт пересылки в таблице MAC-адресов на основе MAC-адреса получателя пакета.

MAC-адрес может быть как статическим, так и динамическим.

Статический MAC-адрес настраивается пользователем. Он имеет наивысший приоритет (не переопределяется динамическими MAC-адресами) и действует постоянно.

Динамические MAC-адреса коммутатор узнает при пересылке данных. Они действительны только в течение определенного периода. Коммутатор периодически обновляет свою таблицу MAC-адресов. При получении кадра данных для пересылки коммутатор узнает исходный MAC-адрес кадра, устанавливает сопоставление с принимающим портом и запрашивает порт пересылки в таблице MAC-адресов на основе MAC-адреса получателя кадра. Если совпадение найдено, коммутатор пересылает кадр данных с соответствующего порта. Если совпадений не найдено, коммутатор передает кадр в своем широковещательном домене.

Время устаревания начинается с момента добавления динамического MAC-адреса в таблицу MAC-адресов. Если ни один порт не получает кадр с MAC-адресом в течение времени, в 1-2 раза превышающего время устаревания, коммутатор удаляет запись MAC-адреса из таблицы динамических адресов пересылки. Статические MAC-адреса не включают понятие времени устаревания.

16.2 Настройка через веб-интерфейс

1. Настройте время устаревания MAC-адреса, как показано на рисунке 191.

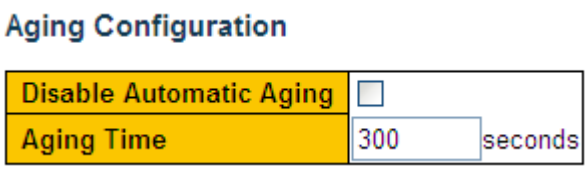


Рисунок 191 Настройка времени устаревания MAC-адреса

Disable Automatic Aging

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение устаревания MAC-адреса Enable означает, что необходимо настроить время устаревания. Disable указывает, что динамические адреса не устаревают со временем.

Aging Time

Диапазон: 10~1000000 с

По умолчанию: 300 с

Функция: Задание времени устаревания для записи динамического MAC-адреса.

2. Настройте динамический MAC-адрес, как показано на рисунке 192.

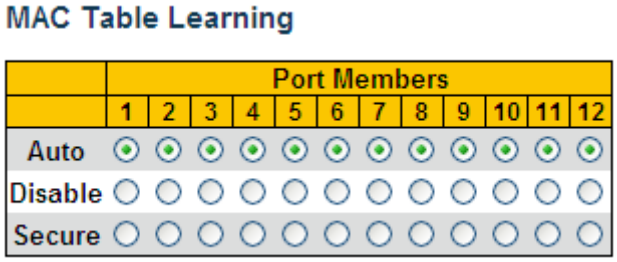


Рисунок 192 Настройка динамического MAC-адреса

Port members

Варианты: Auto/Disable

По умолчанию: Auto

Функция: Настройка функции динамического изучения портом таблицы MAC-адресов. Auto означает, что порт может динамически изучать таблицу MAC-адресов. Disable означает, что порту запрещено динамически изучать таблицу MAC-адресов. Secure: Включить безопасное изучение таблицы MAC-адресов. Изучаются только статические записи MAC, все остальные кадры отбрасываются.

3. Настройте динамический MAC-адрес, как показано на рисунке 193.

Static MAC Table Configuration

Delete	VLAN ID	MAC Address	Port Members 1	2	3	4	5	6	7	8	9	10	11	12
☐	1	00-12-34-56-78-90	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐	1	01-01-01-01-01-01	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐
☐	2	00-11-22-33-44-55	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐

Add New Static Entry

Submit Reset

Рисунок 193 Настройка динамического MAC-адреса

VLAN ID

Варианты: все созданные VLAN ID

По умолчанию: VLAN 1

Функция: Настройка VLAN ID статического MAC-адреса.

MAC address

Формат: HH-HH-HH-HH-HH-HH (H – шестнадцатеричное число)

Функция: Настройка MAC-адреса. Для MAC-адреса одноадресной рассылки младший бит в первом байте равен 0. Для MAC-адреса многоадресной рассылки младший бит в первом байте равен 1.

Port members

Функция: Выбор портов для пересылки пакетов с этим MAC-адресом назначения.

Щелкните <Add New Static Entry>, чтобы настроить запись статического MAC-адреса.

Поддерживается не более 64 записей статического MAC-адреса.

4. Просмотрите таблицу MAC-адресов, как показано на рисунке 194.

Type	VLAN	MAC Address	Port Members CPU	1	2	3	4	5	6	7	8	9	10	11	12
Static	1	00-01-C1-00-00-00	✓												
Dynamic	1	00-01-C1-00-00-02					✓								
Static	1	00-12-34-56-78-90			✓										
Dynamic	1	00-1E-CD-11-01-B1		✓											
Static	1	01-01-01-01-01-01		✓	✓	✓	✓								
Static	2	00-11-22-33-44-55						✓							
Static	2	01-01-01-01-01-02				✓	✓	✓							

Рисунок 194 Просмотр таблицы MAC-адресов

17 VLAN

17.1 Настройка VLAN

17.1.1 Введение

Одна локальная сеть может быть разделена на несколько логических виртуальных локальных сетей (VLAN). Устройство может обмениваться данными только с устройствами в той же VLAN. В результате широковещательные пакеты ограничиваются VLAN, что повышает 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.

17.1.2 Принцип работы

Чтобы сетевые устройства могли различать пакеты из разных VLAN, в пакеты необходимо добавить поля для идентификации VLAN. В настоящее время для идентификации VLAN чаще всего используется протокол IEEE802.1Q. В таблице 7 показана структура кадра 802.1Q.

Таблица 7 Структура кадра 802.1Q

DA	SA	Заголовок				Длина/тип	Данные	FCS
		TPID	PRI	CFI	VID			

4-байтовый заголовок 802.1Q в качестве тега VLAN добавляется к традиционному кадру данных Ethernet. TPID: 16 бит. Используется для идентификации кадра данных, несущего тег VLAN. Значение равно 0x8100. Значение TPID, указанное в протоколе 802.1Q, равно 0x8100.

PRI: три бита, определяющие приоритет пакета 802.1p.

CFI: 1 бит, указывает, инкапсулируется ли MAC-адрес в стандартном формате в

различных средах передачи. Значение 0 указывает, что MAC-адрес инкапсулирован в стандартном формате, а значение 1 указывает, что MAC-адрес инкапсулирован в нестандартном формате.

VID: 12 бит, обозначающих номер VLAN. Диапазон значений от 1 до 4093. 0, 4094 и 4095 являются зарезервированными значениями.

Примечание:

- VLAN 1 является VLAN по умолчанию, и ее нельзя создать или удалить вручную.
- Зарезервированные VLAN зарезервированы для реализации системой определенных функций и их нельзя создать или удалить вручную.

Пакет, содержащий заголовок 802.1Q, является тегированным пакетом; пакет без заголовка 802.1Q является нетегированным пакетом. Все пакеты, передаваемые коммутатором, содержат тег 802.1Q.

17.1.3 VLAN на основе порта

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

1. Режим порта

Порты делятся на два типа в зависимости от того, как они обрабатывают теги VLAN при отправке пакетов. Access: В режиме Access порт можно добавить только в одну VLAN. По умолчанию все порты коммутатора являются портами в режиме Access и принадлежат VLAN1. Пакеты, пересылаемые портом в режиме Access, не имеют тегов VLAN. Порты в режиме Access обычно используются для подключения к терминалам, не поддерживающим 802.1Q.

Trunk：В режиме Trunk порт можно добавить в несколько VLAN. Порт в режиме Trunk принимает пакеты с тегами и

без тегов. При отправке пакетов PVID для порта в режиме Trunk можно указать, следует ли передавать тег. Он передает тег при отправке других пакетов. Порты в режиме Trunk обычно используются для подключения сетевых передающих устройств.

Hybrid：В режиме Hybrid порт можно добавить в несколько VLAN. Можно указать тип пакетов, которые должны быть получены портом в режиме Hybrid, и указать, передается ли тег, когда порт в режиме Hybrid отправляет пакеты. Порт в режиме Hybrid можно использовать для подключения сетевых устройств и пользовательских устройств. Разница между портом в режиме Hybrid и портом в режиме Trunk заключается в следующем: Порт в режиме Hybrid не передает тег при отправке пакетов из нескольких VLAN, а порт в режиме Trunk не передает тег только при отправке пакетов PVID.

2. 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.

Предупреждение:

- При настройке PVID порта выберите один из идентификаторов VLAN, разрешенных для порта; в противном случае порт может не пересылать пакеты.
- Когда тег PVID добавляется к нетегированным пакетам, можно обратиться к настройкам PCP и DEI на рисунке 62 для значений PRI и CFI по умолчанию для порта.

Таблица 8 показывает, как коммутатор обрабатывает полученные и пересылаемые пакеты в зависимости от режима порта и PVID.

Таблица 8 Различные режимы обработки пакетов

<table>
<tr><th colspan="2">Обработка полученных пакетов</th><th colspan="2">Обработка пакетов для пересылки</th></tr>
<tr><th>Нетегированные пакеты</th><th>Тегированные пакеты</th><th>Режим порта</th><th>Обработка пакетов</th></tr>
<tr><td rowspan="2">Добавить теги PVID в пакеты:
➢ Если PVID находится в списке разрешенных VLAN, принять пакет.
➢ Если PVID не находится в списке разрешенных VLAN, отклонить пакет.</td><td rowspan="2">➢ Если VLAN ID находится в списке разрешенных VLAN, принять пакет.
➢ Если VLAN ID не находится в списке разрешенных VLAN, отклонить пакет.</td><td>Access</td><td>Переслать пакет после удаления тега.</td></tr>
<tr><td>Trunk</td><td>Переслать пакет в соответствии с конфигурацией Egress Tagging:
➢ Untag порт VLAN: Если VLAN ID в пакете совпадает с PVID и находится в списке разрешенных VLAN, перенаправить пакет после удаления тега. Если VLAN ID в пакете отличается от PVID и в списке разрешенных VLAN, сохранить тег и перенаправить пакет.
➢ Tag All: Если VLAN ID в пакете находится в списке разрешенных VLAN, сохранить тег и перенаправить пакет.</td></tr>
</table>

		Hybrid	Переслать пакет в соответствии с конфигурацией Egress Tagging: ➢ Untag Port VLAN: как указано выше. ➢ Tag All: как указано выше. ➢ Untag All: Если VLAN ID в пакете находится в списке разрешенных VLAN, переслать пакет после удаления тега.

17.1.4 Настройка через веб-интерфейс

1. Созданная конфигурация VLAN показана на рисунке 195.

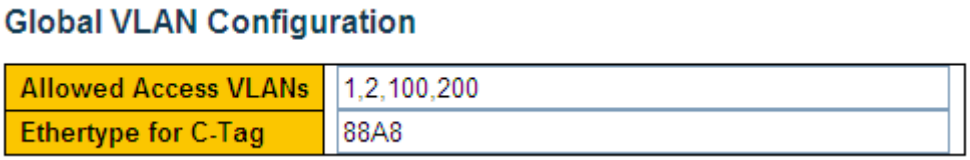


Рисунок 195 Созданная конфигурация VLAN

Allowed Access VLANs

Варианты: 1~4093

По умолчанию: 1

Функция: Настройка разрешенных VLAN для порта доступа. При наличии нескольких VLAN их можно разделить запятой (,) и дефисом (-), где дефис используется для разделения двух последовательных идентификаторов VLAN, а запятая — для разделения двух непоследовательных идентификаторов VLAN.

Ethertype for C-Tag

Варианты: 600-FFFF

По умолчанию: 88A8

Функция: Когда сообщение содержит двойные теги, значение TPID внешнего тега изменяется в соответствии с конфигурацией.

2. Настройте VLAN порта, как показано на рисунке 196.

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	2	<>	☑	<>	<>	2	1
1	Access	2	C-Port	☑	Tagged and Untagged	Untag All	2	1
2	Access	2	C-Port	☑	Tagged and Untagged	Untag All	2	
3	Access	100	C-Port	☑	Tagged and Untagged	Untag All	100	
4	Access	100	C-Port	☑	Tagged and Untagged	Untag All	100	
5	Access	200	C-Port	☑	Tagged and Untagged	Untag All	200	
6	Access	200	C-Port	☑	Tagged and Untagged	Untag All	200	
7	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1,2,100,200	
8	Hybrid	1	C-Port	☐	Tagged and Untagged	Untag Port VLAN	1-3	2
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

Submit Reset

Рисунок 196 Настройка VLAN порта

Mode

Варианты: Access/Trunk/Hybrid

По умолчанию: Access

Функция: Выбор режима для указанного порта. Каждый порт поддерживает только один режим.

Port

VLAN (PVID)

Диапазон: 1~4094

По умолчанию: 1

Функция: Каждый порт имеет PVID. При получении нетегированного пакета порт добавляет к пакету тег в соответствии с PVID.

Предупреждение:

- PVID порта доступа следует выбирать из списка VLAN, разрешенных портом доступа, см.
  - Варианты конфигурации: 1 ~ 4093
  - Конфигурация по умолчанию: 1
  - Функция: Настройка параметра Allowed VLAN в конфигурации;
  - PVID порта Trunk/Hybrid следует выбирать из списка VLAN, разрешенных портом, см. настройку параметра Allow VLAN ниже.

Тип порта

C-Port: На входе кадры с тегом VLAN с TPID = 0x8100 классифицируются по VLAN ID, встроенному в тег. Если кадр не имеет тега или имеет тег приоритета, он

классифицируется по Port VLAN. Если кадры должны быть тегированы на выходе, они будут тегированы тегом C-tag.

S-Port: На входе кадры с тегом VLAN с TPID = 0x8100 или 0x88A8 классифицируются по VLAN ID, встроенному в тег. Если кадр не имеет тега или имеет тег приоритета, он классифицируется по Port VLAN. Если кадры должны быть тегированы на выходе, они будут тегированы тегом S-tag.

S-Custom-Port: При входе кадры с тегом VLAN с TPID = 0x8100 или равным Ethertype, настроенному для портов Custom-S, классифицируются по идентификатору VLAN, встроенному в тег. Если кадр не имеет тега или имеет тег приоритета, он классифицируется по Port VLAN. Если кадры должны быть тегированы на выходе, они будут тегированы тегом S-tag Custom.

Ingress Filtering

Варианты:

Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение функции фильтрации входящего трафика гибридного порта. Входная фильтрация включена принудительно для порта доступа и порта Trunk, настроить параметр нельзя. Enable: Если VLAN ID в пакете не находится в списке разрешенных VLAN, отклонить пакет. Disable: Если VLAN ID находится в списке разрешенных VLAN, принять пакет и передать механизму MAC-адресов.

Ingress Acceptance

Варианты: Tagged and Untagged/ Tagged Only/ Untagged Only

По умолчанию: Tagged and Untagged

Функция: Настройка типа пакетов, которые должны быть получены портом в режиме Hybrid. Для порта Access и порта Trunk принудительно устанавливается значение Tagged and Untagged, и его нельзя изменить. Значение Tagged and Untagged указывает, что порт Hybrid может принимать пакеты с тегами и пакеты без тегов; значение Tagged Only указывает, что порт Hybrid принимает только тегированные пакеты и отбрасывает нетегированные пакеты; значение Untagged Only указывает, что порт Hybrid принимает только нетегированные пакеты и отбрасывает тегированные пакеты.

Egress Tagging

Варианты: Untag Port VLAN/ Unatg All/ Tag All

По умолчанию: Untag порт VLAN

Функция: Настройка обработки передачи пакетов для портов Trunk или Hybrid.

Значение Egress Tagging настроено на Unatg All принудительно для порта доступа, и его нельзя изменить этот параметр. Untag порт VLAN: Если VLAN ID в пакете совпадает с PVID и находится в списке разрешенных VLAN, перенаправить пакет после удаления тега. Если VLAN ID в пакете отличается от PVID и в списке разрешенных VLAN, сохранить тег и перенаправить пакет. Tag All: Если VLAN ID в пакете находится в списке разрешенных VLAN, сохранить тег и перенаправить пакет. Untag All: Если VLAN ID в пакете находится в списке разрешенных VLAN, переслать пакет после удаления тега.

Allowed VLANs

Диапазон: 1-4094

Диапазон: 1-4094

Функция: Настройка разрешенных VLAN для порта Trunk/Hybrid. Когда порт Access допускает только одну VLAN, значение этого параметра соответствует значению порта VLAN и не может быть изменено. Когда этот параметр установлен на несколько VLAN, их можно разделить запятой (,) и дефисом (-), где дефис используется для разделения двух последовательных идентификаторов VLAN, а запятая — для разделения двух непоследовательных идентификаторов VLAN.

Forbidden VLANs

Диапазон: 1-4094

Функция: Настройка запрещенных VLAN для порта. После установки этого параметра для порта порт никогда не станет портом-участником VLAN, включая динамически зарегистрированную VLAN через GVRP. Когда этот параметр установлен на несколько VLAN, их можно разделить запятой (,) и дефисом (-), где дефис используется для разделения двух последовательных идентификаторов VLAN, а запятая — для разделения двух непоследовательных идентификаторов VLAN.

3. Просмотрите все созданные VLAN и порты-участники, как показано на рисунке 197.

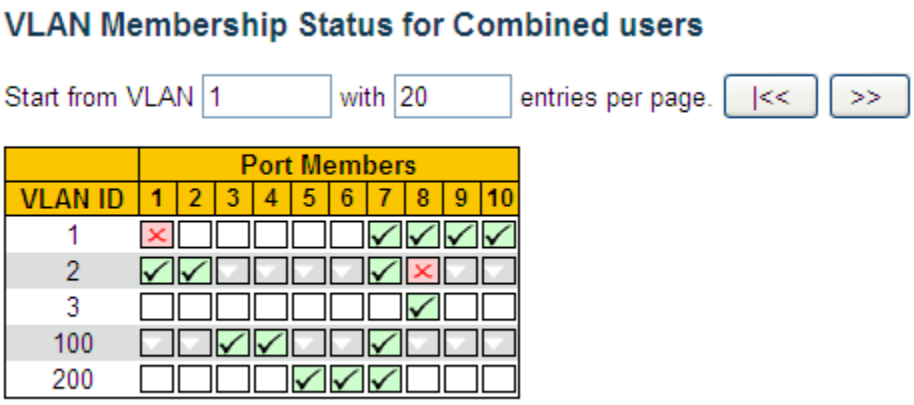
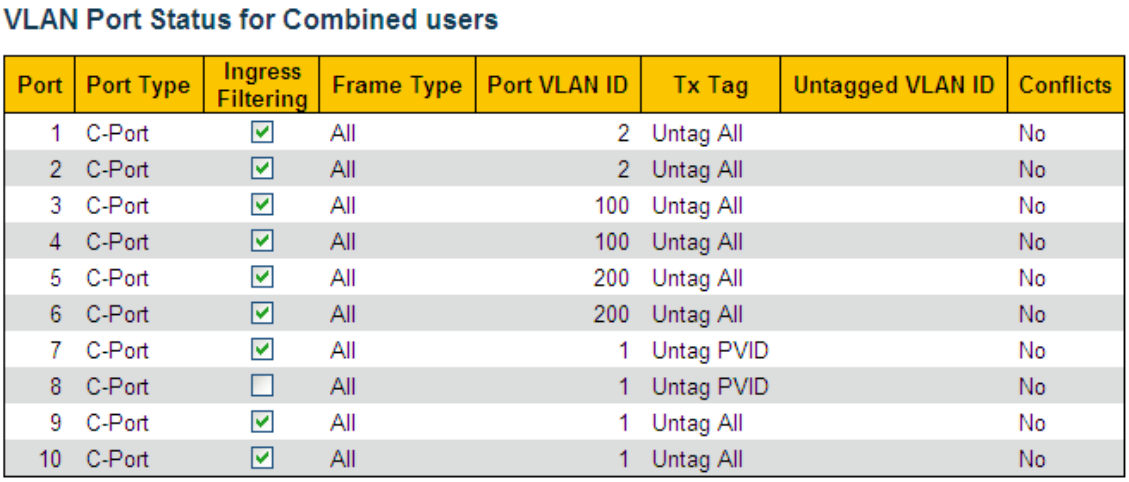


Рисунок 197 Просмотр всех созданных VLAN и портов-участников

☑ указывает, что порт является портом-участником текущей VLAN; ☒ указывает, что текущая VLAN принадлежит к запрещенным VLAN порта.

На каждой странице может отображаться от 1 до 99 записей VLAN, по умолчанию отображается 20 записей VLAN. На первой странице можно указать идентификатор первой записи VLAN.

4. Просмотрите настройки Port VLAN, как показано на рисунке 198.



Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	☑	All	2	Untag All		No
2	C-Port	☑	All	2	Untag All		No
3	C-Port	☑	All	100	Untag All		No
4	C-Port	☑	All	100	Untag All		No
5	C-Port	☑	All	200	Untag All		No
6	C-Port	☑	All	200	Untag All		No
7	C-Port	☑	All	1	Untag PVID		No
8	C-Port	☐	All	1	Untag PVID		No
9	C-Port	☑	All	1	Untag All		No
10	C-Port	☑	All	1	Untag All		No

Рисунок 198 Просмотр настроек Port VLAN

17.1.5 Пример типовой конфигурации

Как показано на рисунке 199, сеть разделена на 3 VLAN: VLAN2, VLAN100 и VLAN200. Требуется, чтобы устройства в одной VLAN могли осуществлять обмен данными друг с другом, но разные VLAN были изолированы. Терминальные ПК не могут различать тегированные пакеты, поэтому порты, соединяющие коммутатор A и коммутатор B с ПК, настроены на порт Access. Пакеты VLAN2, VLAN100 и VLAN200 должны

передаваться между коммутатором A и коммутатором B, поэтому порты, соединяющие коммутатор A и коммутатор B, должны быть настроены на порт Trunk, что позволит пропускать пакеты VLAN 2, VLAN 100 и VLAN 200. В таблице 9 показана конкретная конфигурация.

Таблица 9 Конфигурация VLAN

VLAN	**Конфигурация**
VLAN2	Настройте порты 1 и 2 на коммутаторах A и B как порты Access, а порт 7 как порт Trunk
VLAN100	Настройте порты 3 и 4 на коммутаторах A и B как порты Access, а порт 7 как порт Trunk
VLAN200	Настройте порты 5 и 6 на коммутаторах A и B как порты Access, а порт 7 как порт Trunk

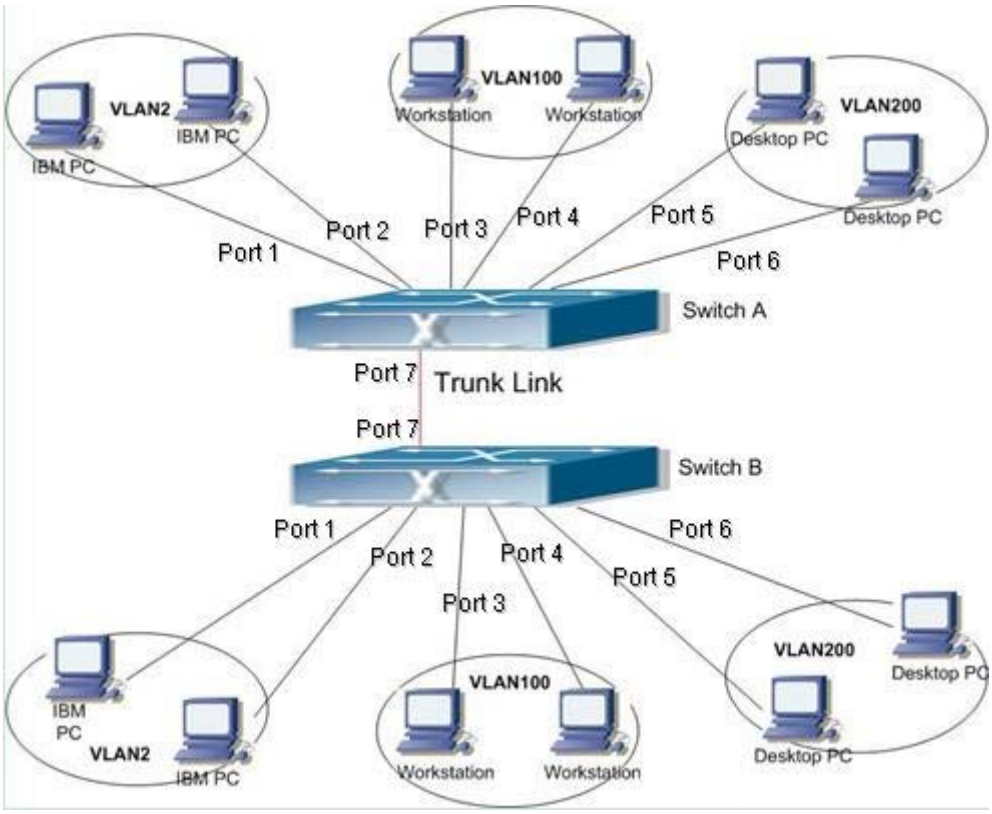


Рисунок 199 Использование VLAN

Конфигурация коммутатора A и коммутатора B:

1. Настройте VLAN с разрешенным доступом 1, 2, 100, 200, как показано на рисунке 195.

2. Настройте порты 1, 2 как порты Access, порт VLAN как 2. Настройте порты 3, 4 как порты Access, порт VLAN как 100. Настройте порты 5, 6 как порты Access, порт VLAN как 200. Настройте порт 7 как порт Trunk, порт VLAN как 1, разрешенные VLAN как 1, 2, 100, 200, как показано на рисунке 196.

3. Оставьте все остальные параметры со значениями по умолчанию.

17.2 Настройка PVLAN

17.2.1 Введение

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

Верхняя VLAN — это VLAN с общим доменом, в которой порты являются портами Uplink. Нижние VLAN являются изолированными доменами, в которых порты являются портами Downlink. Порты Downlink связи могут быть назначены разным доменам изоляции, и они могут одновременно взаимодействовать с портом Uplink. Изолированные домены не могут взаимодействовать друг с другом.

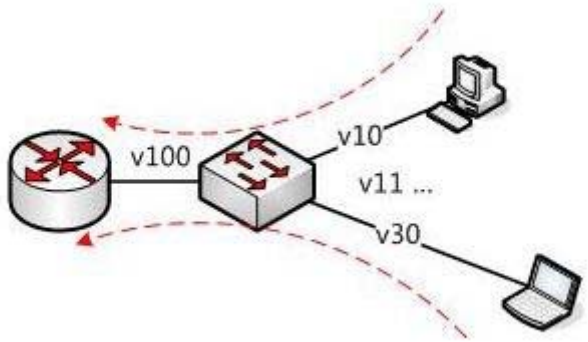


Рисунок 200 Использование PVLAN

Как показано на рисунке 200, общим доменом является VLAN100, а изолированными доменами являются 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.

17.2.2 17.2.2 Пояснения

Функцию PVLAN можно реализовать с помощью специальной настройки портов.

- PVID портов Uplink совпадает с общим идентификатором VLAN домена; PVID

портов Downlink совпадает с их собственным идентификатором VLAN домена изоляции.

- Порты Uplink настроены на режим Hybrid и назначены VLAN домена общего доступа и всем доменам изоляции; порты Downlink настроены на режим Hybrid и назначены VLAN с общим доменом и собственному изолированному домену.
- Пакеты, отправляемые портами-участниками PVLAN, имеют тип Untag.

17.2.3 Пример типовой конфигурации

Рисунок 201 показывает использование PVLAN. VLAN300 — это общий домен, а порты 1 и 2 — порты Uplink; VLAN100 и VLAN200 являются изолированными доменами, а порты 3, 4, 5 и 6 — портами Downlink.

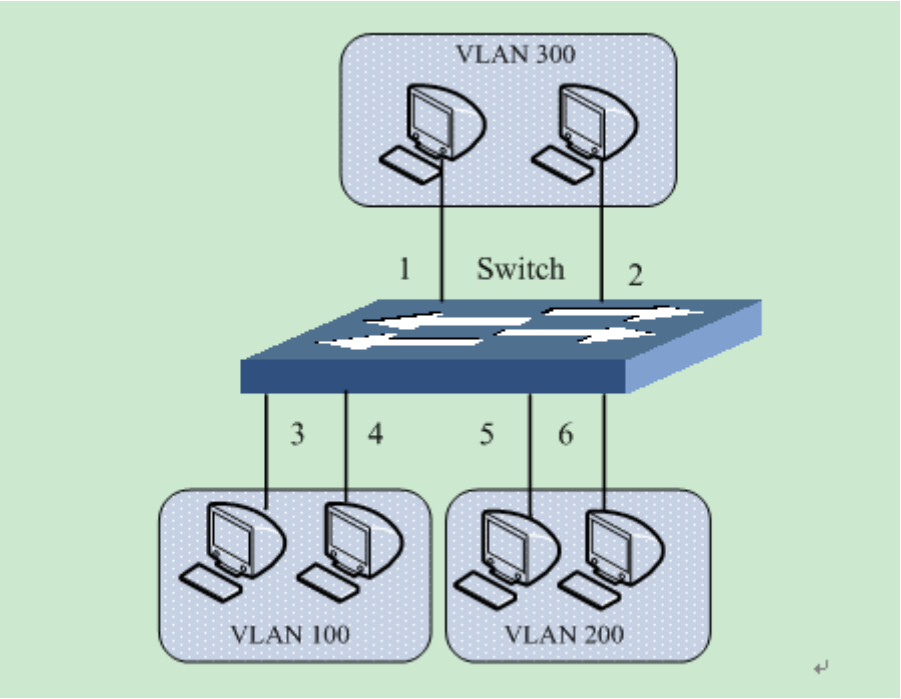
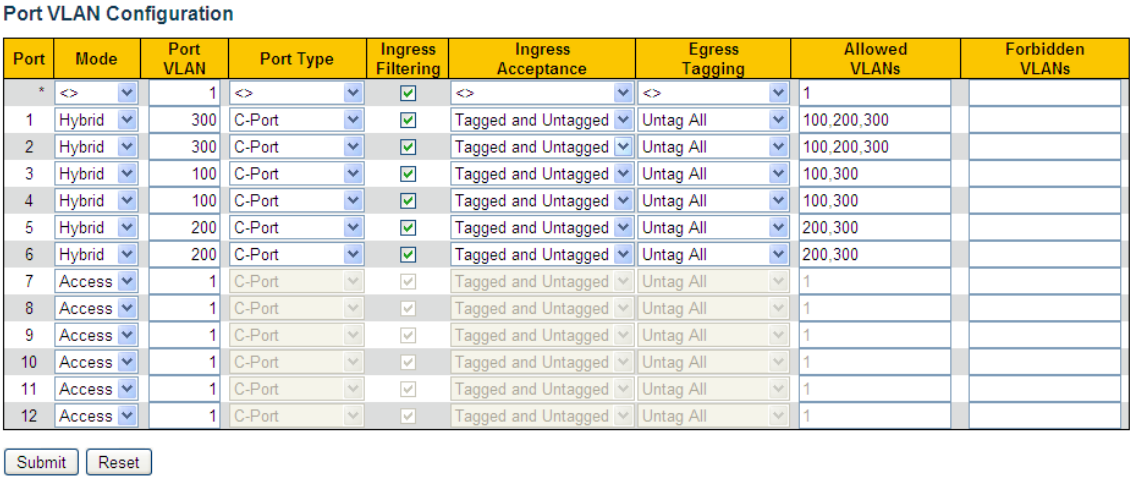


Рисунок 201 Пример настроек PVLAN

Настройка коммутатора:

1. Настройте порты 1, 2 как Hybrid, порт VLAN 300, тегирование исходящего трафика Untag All, разрешенные VLAN 100, 200, 300.
2. Настройте порты 3, 4 как Hybrid, порт VLAN 100, тегирование исходящего трафика Untag All, разрешенные VLAN 100, 300.
3. Настройте порты 5, 6 как Hybrid, порт VLAN 200, тегирование исходящего трафика Untag All, разрешенные VLAN 100, 300 как показано на рисунке 202.

4. Оставьте все остальные параметры со значениями по умолчанию.



Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Hybrid	300	C-Port	☑	Tagged and Untagged	Untag All	100,200,300	
2	Hybrid	300	C-Port	☑	Tagged and Untagged	Untag All	100,200,300	
3	Hybrid	100	C-Port	☑	Tagged and Untagged	Untag All	100,300	
4	Hybrid	100	C-Port	☑	Tagged and Untagged	Untag All	100,300	
5	Hybrid	200	C-Port	☑	Tagged and Untagged	Untag All	200,300	
6	Hybrid	200	C-Port	☑	Tagged and Untagged	Untag All	200,300	
7	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
8	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
11	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
12	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

Submit Reset

Рисунок 202 Настройка портов PVLAN

17.3 GVRP

17.3.1 GARP. Введение

Протокол GARP (Generic Attribute Registration Protocol) используется для распространения, регистрации и отмены определенной информации (VLAN, адрес многоадресной рассылки) между коммутаторами в одной сети.

При использовании GARP информация о конфигурации участника GARP будет распространяться по всей сети коммутатора. Устройства, поддерживающие GARP, передают друг другу инструкции о регистрации или отмене тех или иных настроек путём отправки соответствующих сообщений join/leave. Участник также регистрирует или отменяет информацию о конфигурации других участников на основе сообщений join/leave, отправленных другими участниками.

GARP включает в себя три типа сообщений: Join, Leave и LeaveAll.

Когда прикладной объект GARP хочет зарегистрировать свою собственную информацию на других коммутаторах, объект отправляет сообщение Join. Сообщения Join делятся на два типа: JoinEmpty и JoinIn. Сообщение JoinIn отправляется для объявления зарегистрированного атрибута, а сообщение JoinEmpty отправляется для объявления еще не зарегистрированного атрибута.

Когда прикладной объект GARP хочет удалить свою собственную информацию на других коммутаторах, объект отправляет сообщение Leave.

После запуска объекта GARP он запускает таймер LeaveAll. Когда период таймера истекает, объект отправляет сообщение LeaveAll.

Примечание:

Объект указывает порт с поддержкой GARP.

Таймеры GARP – это таймер Hold, таймер Join, таймер Leave и таймер LeaveAll.

Таймер Hold: когда коммутатор с поддержкой GARP получает сообщение о регистрации, он запускает таймер Hold, а не сразу отправляет сообщение Join. По истечении времени ожидания таймера Hold вся регистрационная информация, полученная за это время, будет помещена в одно и то же сообщение Join и отправлена, что уменьшит количество сообщений для стабильности сети.

Таймер Join: для того, чтобы гарантировать, что сообщение Join может быть надежно передано другим коммутаторам, коммутатор с поддержкой GARP будет ждать в течение временного интервала таймера Join после отправки первого сообщения Join. Если коммутатор не получит сообщение Join в течение этого времени, он снова отправит сообщение Join, в противном случае он не отправит второе сообщение.

Таймер Leave: когда коммутатор с поддержкой GARP желает, чтобы другие коммутаторы аннулировали его атрибутивную информацию, он отправляет сообщение Leave. Другие коммутаторы с поддержкой GARP, получившие это сообщение, включат таймер Leave. Если они не получат сообщение Join до истечения времени таймера, они аннулируют эту атрибутивную информацию.

Таймер LeaveAll: Когда коммутатор включает GARP, он одновременно запускает таймер LeaveAll. По истечении времени таймера коммутатор отправит сообщение LeaveAll другим коммутаторам с поддержкой GARP и позволит им повторно зарегистрировать всю информацию об атрибутах, а затем перезапустит таймер LeaveAll, чтобы начать новый цикл.

17.3.2 Введение

GVRP (протокол регистрации GARP VLAN) — это приложение GARP, основанное на

рабочем механизме GARP для поддержки динамической регистрационной информации VLAN устройства и распространения этой информации на другие устройства.

Устройство с поддержкой GVRP может получать регистрационную информацию VLAN от других устройств и динамически обновлять регистрационную информацию локальной VLAN, а также устройство может распространять регистрационную информацию локальной VLAN на другие устройства, достигая согласованности информации VLAN на всех устройствах в одной и той же локальной сети. Регистрационная информация VLAN, распространяемая GVRP, содержит не только локальную статическую регистрационную информацию, сконфигурированную вручную, но также динамическую регистрационную информацию от других устройств.

Предупреждение:

Канал портов и порт GVRP являются взаимоисключающими. Порты в канале портов

17.3.3 Настройка через веб-интерфейс

1. Включите протокол GVRP и настройте соответствующие таймеры, как показано на рисунке 203.

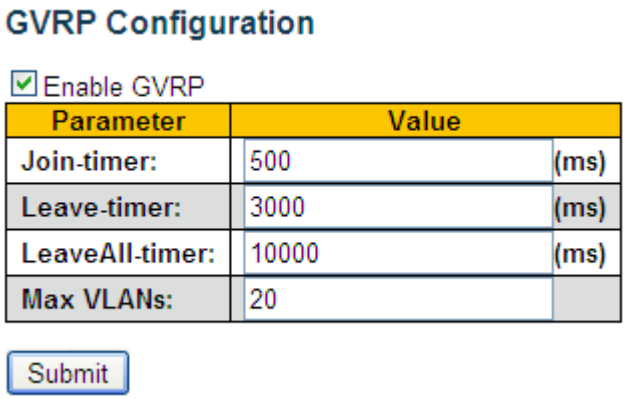


Рисунок 203 Настройка протокола GVRP

Enable GVRP

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/отключение протокола GVRP

Join-timer

Диапазон: 100 мс~327600 мс

По умолчанию: 500 мс

Функция: Настройка значения таймера Join Значение должно быть кратно 100.

Leave-timer

Диапазон: 100 мс~327600 мс

По умолчанию: 3000 мс

Функция: Настройка значения таймера Leave Значение должно быть кратно 100.

LeaveAll-timer

Диапазон: 100 мс~327600 мс
По умолчанию: 10000 мс

Функция: Настройка значения таймера LeaveAll. Значение должно быть кратно 100.

Пояснение: Если таймеры LeaveAll на разных устройствах истекают одновременно, устройства отправят сообщение LeaveAll одновременно, что увеличит количество сообщений. Чтобы избежать этого, фактическое время работы таймера LeaveAll является случайным значением и больше, чем значение таймера LeaveAll, и меньше чем 1,5 значения таймера LeaveAll.

Max VLANs

Диапазон: 1~4094

По умолчанию: 20

Функция: Задание максимального количества VLAN, которые динамически регистрируются с портом GVRP. Для настройки этого параметра необходимо отключить функцию GVRP.

2. Настройте порт GVRP, как показано на рисунке 204.

Рисунок 204 Настройка порта GVRP

Mode

Варианты: Enabled/Disabled

По умолчанию: Disabled

Функция: Включение/выключение функции GVRP для порта.

Предупреждение:

- Порт GVRP должен быть сконфигурирован как порт Trunk.
- Порт GVRP используется для передачи атрибутов VLAN других портов GVRP в рабочем состоянии.

3. Отображение информации о настроенных статически или зарегистрированных динамически VLAN показано на рисунке 205.

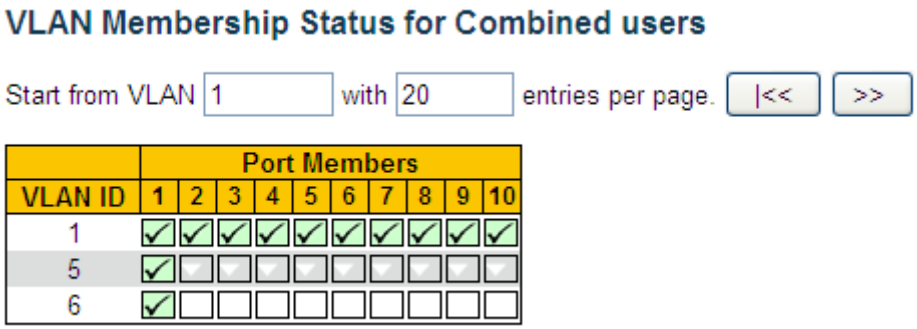


Рисунок 205 Информация VLAN

17.3.4 Пример типовой конфигурации

Как показано на рисунке 206, на устройствах необходимо включить GVRP, чтобы

информация VLAN динамически регистрировалась и обновлялась между устройством A и устройством B.

Рисунок 206 Пример настроек GVRP

Настройки устройства A:

1. Настройте порт 1 как порт Trunk, разрешенные VLAN на 1.

2. Включите глобальный GVRP, как показано на рисунке 203.

3. Включите GVRP на порту 1, как показано на рисунке 204. Настройки устройства B:

1. Настройте порт 4 как порт Trunk, разрешенные VLAN на 1; настройте порт 5 как порт Access, разрешенные VLAN на 5; настройте порт 6 как порт Trunk, разрешенные VLAN на 1, 6.

2. Включите глобальный GVRP, как показано на рисунке 203.

3. Включите GVRP на портах 4, 5, 6, как показано на рисунке 204.

Порт 1 коммутатора A может регистрировать ту же информацию о VLAN, что и порт 5 и 6 коммутатора B, как показано на рисунке 205.

18 Резервирование

18.1 DT-Ring

18.1.1 Введение

DT-Ring и DT-Ring+ — это собственные протоколы резервирования компании Kyland. Они позволяют сети восстанавливаться в течение 50 мс при сбое канала, обеспечивая стабильную и надежную связь.

Кольца DT делятся на два типа: на основе портов (DT-Ring-Port) и на основе VLAN (DT-Ring-VLAN). DT-Ring-Port: указывает порт для пересылки или блокировки пакетов.

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

DT-Ring-Port и DT-Ring-VLAN нельзя использовать вместе.

18.1.2 Основные концепции

Master: Одно кольцо может иметь только один узел в статусе Master. Узел в статусе Master отправляет пакеты протокола DT-Ring и определяет состояние кольца. Когда кольцо замкнуто, из двух портов, которые включены в кольцо, один находится в состоянии пересылки, а другой в состоянии блокировки, соответственно.

Примечание:

Первый порт, статус связи которого меняется на up при замыкании кольца, находится в состоянии пересылки.

Остальные кольцевые порты находятся в состоянии блокировки.

Slave: Кольцо может включать в себя несколько устройств Slave. Устройства Slave прослушивают и пересылают пакеты протокола DT-Ring и сообщают информацию об ошибках устройству Master.

Резервный порт: Порт для связи между кольцами DT называется резервным

портом. Резервный порт Master: Когда кольцо имеет несколько резервных портов, резервный порт с большим MAC-адресом является резервным портом Master. Он находится в состоянии пересылки.

Резервный порт Slave: Когда кольцо имеет несколько резервных портов, все резервные порты, кроме резервного порта Master, являются резервными портами Slave. Они находятся в состоянии блокировки.

Состояние пересылки: Если порт находится в состоянии пересылки, порт может и принимать, и отправлять данные.

Состояние блокировки: Если порт находится в состоянии блокировки, он может принимать и пересылать только пакеты протокола DT-Ring.

18.1.3 Реализация

Реализация DT-Ring-Port

Порт пересылки на устройстве Master периодически отправляет пакеты протокола DT-Ring для определения состояния кольца. Если блокирующий порт устройства Master получает пакеты, кольцо замкнуто; в противном случае кольцо разомкнуто.

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

1. Настройте коммутатор A как Master, а остальные коммутаторы — как Slave.

2. Кольцевой порт 1 на Master находится в состоянии пересылки, а кольцевой порт 2 находится в состоянии блокировки. Оба порта на Slave находятся в состоянии пересылки.

3. Если линия связи CD неисправна, как показано на рисунке 207.

a) Когда линия связи CD неисправна, порт 6 и порт 7 на устройстве Slave находятся в состоянии блокировки. Порт 2 устройства Master переходит в состояние пересылки, обеспечивая работающую линию связи.

b) Когда неисправность устранена, порт 6 и порт 7 устройства Slave находятся в состоянии пересылки. Порт 2 устройства Master переходит в состояние блокировки. Происходит переключение каналов, и каналы восстанавливаются до состояния, предшествующего отказу линии CD.

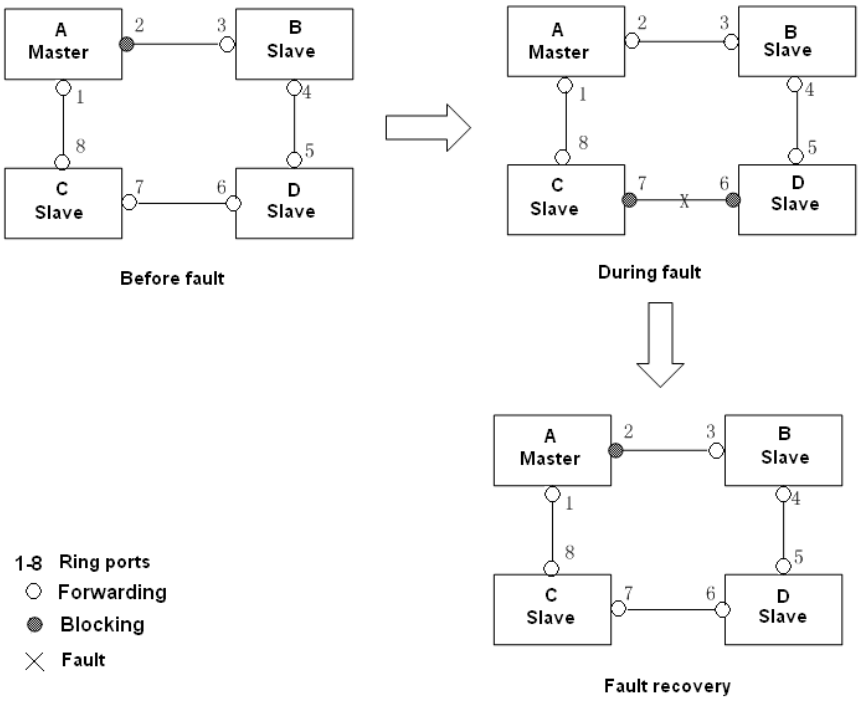


Рисунок 207 Отказ линии CD

4. Если линия связи AC неисправна, как показано на рисунке 208.

a) Если линия связи AC неисправна, порт 1 находится в состоянии блокировки, а порт 2 переходит в состояние пересылки, обеспечивая работающую линию связи.

b) Когда неисправность устранена, порт 1 по-прежнему находится в состоянии блокировки, а порт 8 находится в состоянии пересылки. Переключение не происходит.

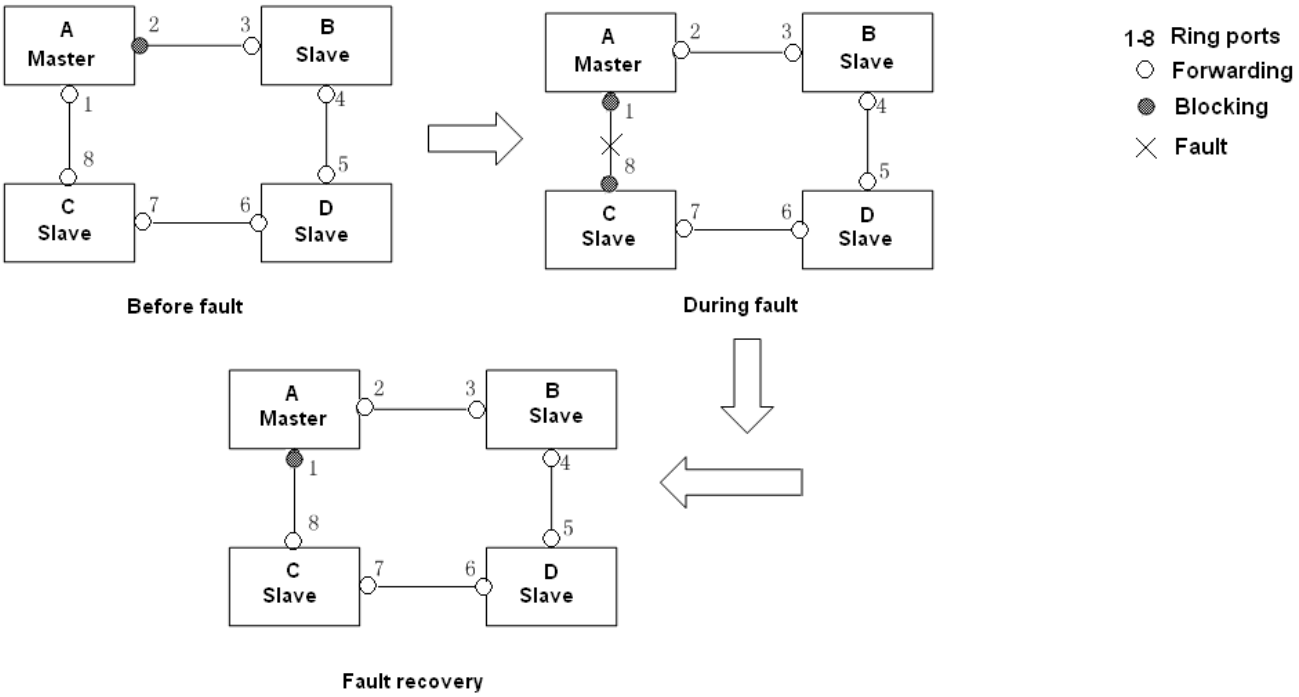


Рисунок 208 Отказ линии DT-Ring

Предупреждение:

Изменение статуса соединения влияет на статус кольцевых портов.

Реализация DT-Ring-VLAN

DT-Ring-VLAN позволяет пересылать пакеты из разных VLAN по разным путям. Каждый путь пересылки для VLAN образует DT-Ring-VLAN. Различные DT-VLAN-Rings могут иметь разные устройства Master. Как показано на рисунке 209, настроено 2 DT-Ring-VLAN.

Линии связи DT-Ring-VLAN 10: AB-BC-CD-DE-EA.

Линии связи DT-Ring-VLAN 20: FB-BC-CD-DE-EF.

Два кольца соприкасаются линиями связи 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.

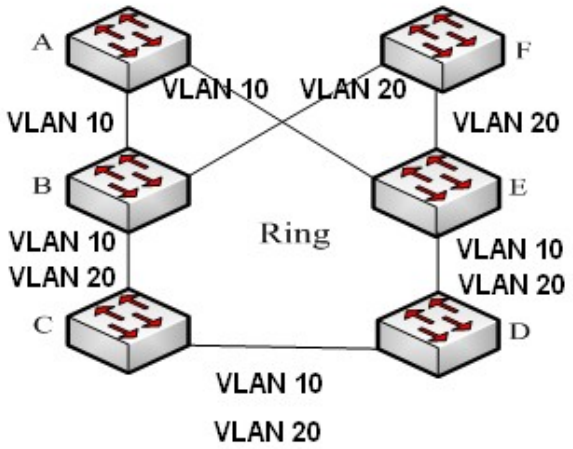


Рисунок 209 DT-Ring-VLAN

Примечание:

В каждом логическом кольце DT-Ring-VLAN реализация идентична таковой для DT-Ring-Port.

Реализация DT-Ring+

DT-Ring+ обеспечивает резервирование для двух колец DT, как показано на рисунке 210. Один резервный порт настроен соответственно на коммутаторе C и коммутаторе D. Какой порт является резервным портом Master, зависит от MAC-адресов двух портов. Если резервный порт Master или его канал выходят из строя,

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

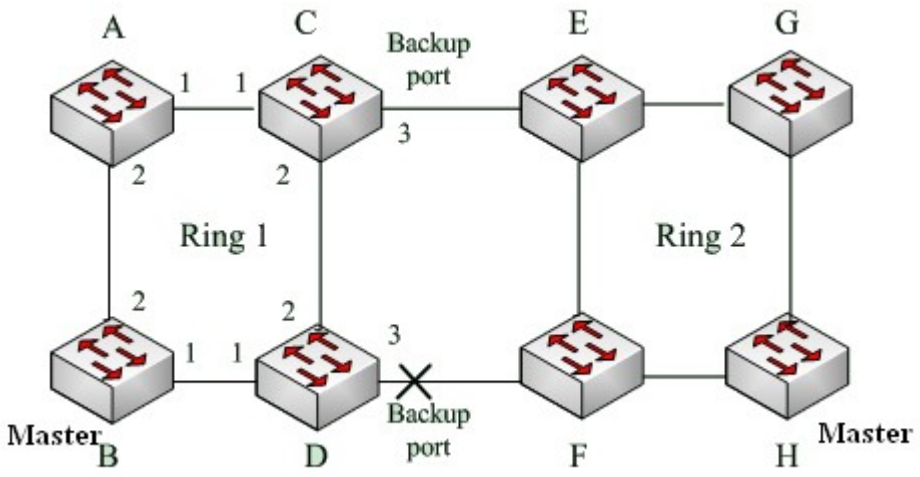


Рисунок 210 Торология Состояние DT-Ring+

Предупреждение:

Изменение статуса соединения влияет на статус резервных портов.

18.1.4 18.1.4 Пояснения

Конфигурация DT-Ring должны удовлетворять следующим условиям:

- Все коммутаторы в одном кольце должны иметь одинаковый номер домена.
- В каждом кольце может быть только один Master и несколько Slave.
- На каждом коммутаторе можно настроить только два порта для кольца.
- Для двух объединенных колец резервные порты можно настроить только в одном кольце.
- В одном кольце можно настроить не более двух резервных портов.
- На коммутаторе в одном кольце может быть настроен только один резервный порт.
- DT-Ring-Port и DT-Ring-VLAN нельзя настроить на одном коммутаторе одновременно.

18.1.5 Настройка через веб-интерфейс

1. Настройте режим резервирования DT-Ring, как показано на рисунке 211.

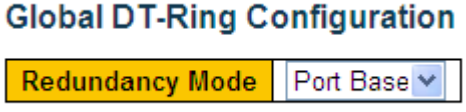


Рисунок 211 Настройка режима резервирования DT-Ring

Режим резервирования

Варианты: Port Based/Vlan Based

По умолчанию: Port Based

Функция: Выбор режима резервирования DT-Ring

Предупреждение:

- К кольцевым протоколам на основе портов относятся RSTP, DT-Ring-Port и DRP-Port, к протоколам на основе VLAN – MSTP, DT-Ring-VLAN и DRP-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 порта и кольцевой протокол на основе VLAN являются взаимоисключающими, и для одного устройства можно выбрать только один режим кольцевого протокола.

2. Настройте DT-Ring-Port и DT-Ring-VLAN, как показано на рисунке 212 и рисунке 213.

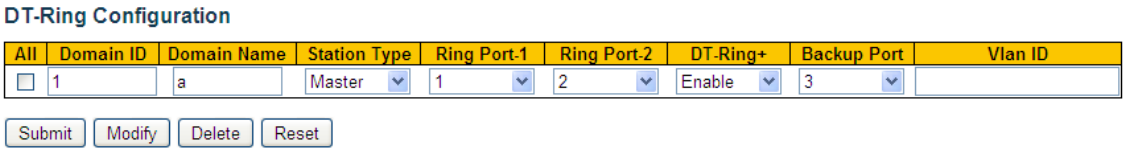


Рисунок 212 Настройка DT-Ring-Port

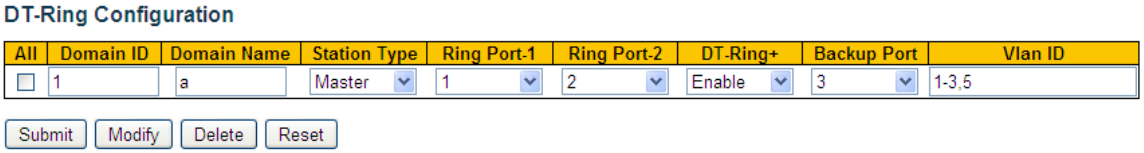


Figure 213 Настройка DT-Ring-VLAN

Domain ID

Диапазон: 1~32

Функция: Идентификатор домена используется, чтобы различать разные кольца. Один коммутатор поддерживает максимум 16 колец на основе VLAN, количество колец на основе портов зависит от количества портов коммутатора.

Domain Name

Диапазон: 1~31 символ

Функция: Задание доменного имени.

Station Type

Варианты: Master/Slave

По умолчанию: Master

Функция: Выбор роли коммутатора в кольце.

Ring Port-1/Ring Port-2

Варианты: все порты коммутатора

Функция: Выбор двух кольцевых портов.

Предупреждение:

- Кольцевой порт DT-Ring или резервный порт и канал портов являются

  или резервный порт не могут быть добавлены к каналу портов; порт в канале портов не может быть настроен в качестве кольцевого порта DT-Ring или резервного порта.

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

  DRP-Port нельзя настроить как кольцевой порт DT-Ring-Port или резервный порт.

- Не рекомендуется одновременно настраивать порты в изолированной группе как порты DT-Ring и резервные порты, а порты DT-Ring и резервные порты нельзя добавлять в изолированную группу.

DT-Ring+

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение DT-Ring+.

Резервный порт

Варианты: все порты коммутатора.

Функция: Настройка порта как резервного.

Пояснение: Включите DT-Ring+ прежде чем настраивать резервный порт.

Предупреждение:

Не следует настраивать кольцевой порт в качестве резервного.

VLAN ID

Варианты: все созданные VLAN

Функция: Выбор VLAN для кольцевого порта. При наличии нескольких VLAN их можно разделить запятой (,) и дефисом (-), где дефис используется для разделения двух последовательных идентификаторов VLAN, а запятая — для разделения двух непоследовательных идентификаторов VLAN.

3. Просмотрите и измените конфигурацию DT-Ring, как показано на рисунке 214.

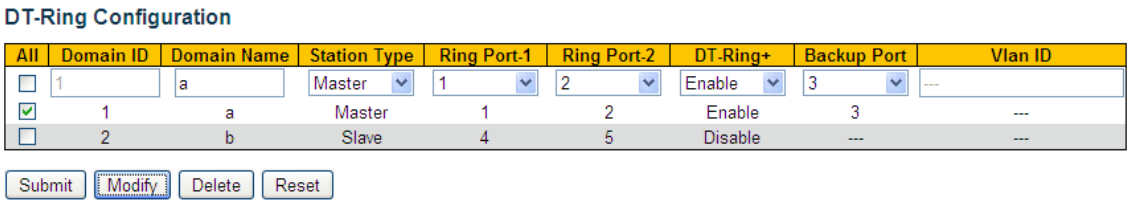


Рисунок 214 Конфигурация DT-Ring

Выберите запись DT-Ring, щелкните <Modify>, чтобы редактировать конфигурацию DT-Ring; щелкните <Delete>, чтобы удалить выбранную запись DT-Ring.

4. Щелкните запись DT-Ring на рисунке 214, чтобы отобразить состояние DT-Ring и порта, как показано на рисунке 215.

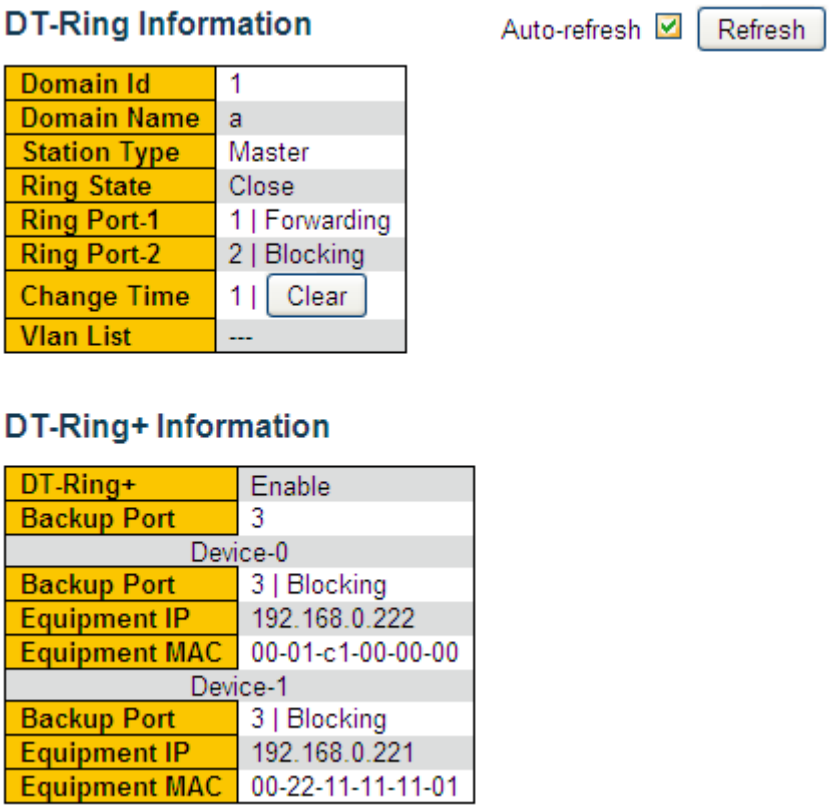


Рисунок 215 Состояние DT-Ring

18.1.6 Пример типовой конфигурации

Как показано на рисунке 210, коммутаторы A, B, C и D образуют кольцо 1; коммутаторы E, F, G и H образуют кольцо 2. Каналы CE и DF являются резервными каналами между кольцом 1 и кольцом 2.

Конфигурация коммутатора A:

1. Настройте Domain ID 1, имя домена a, кольцевые порты 1, 2, тип узла Slave, DT-Ring+ Disable, резервный порт не установлен, как показано на рисунке 212.

Конфигурация коммутатора B:

2. Настройте Domain ID 1, имя домена a, кольцевые порты 1, 2, тип узла Master, DT-Ring+ Disable, резервный порт не установлен, какпоказано на рисунке 212.

Конфигурация коммутатора C:

3. Настройте Domain ID 1, имя домена a, кольцевые порты 1, 2, тип узла Slave, DT-Ring+ Enable, резервный порт 3, как показано на рисунке 212.

Конфигурация коммутатора E, коммутатора F и коммутатора G:

4. Настройте Domain ID 2, имя домена b, кольцевые порты 1, 2, тип узла Slave, DT-Ring+ Disable, резервный порт не установлен, как показано на рисунке 212.

Конфигурация коммутатора H:

5. Настройте Domain ID 2, имя домена b, кольцевые порты 1, 2, тип узла Master, DT-Ring+ Disable, резервный порт не установлен, как показано на рисунке 212.

18.2 DRP

18.2.1 Обзор

Компания Kyland разрабатывает протокол распределенного резервирования (DRP) для передачи данных в сетях кольцевой топологии. Это может предотвратить широковещательные штормы для кольцевых сетей. Когда канал или узел неисправен, резервный канал может взять на себя обслуживание в режиме реального времени, чтобы обеспечить непрерывную передачу данных.

В соответствии со стандартом IEC 62439-6 DRP использует механизм выбора устройства Master без его фиксации. DRP обеспечивает следующие функции:

- Время восстановления, не зависящее от масштаба сети.

DRP обеспечивает время восстановления, не зависящее от масштаба сети, за счет оптимизации механизма пересылки пакетов обнаружения кольца. DRP позволяет сетям восстанавливаться в течение 20 мс благодаря введению отчетов о прерывании 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.

- Различные функции проверки линии связи

Для повышения стабильности сети DRP 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 правильную передачу данных.

- Применимость к нескольким сетевым топологиям

Помимо быстрого восстановления для простых кольцевых сетей, DRP также поддерживает сложные кольцевые топологии, такие как пересекающиеся кольца и соприкасающиеся кольца. Кроме того, DRP поддерживает многовариантные решения на основе VLAN, что подходит для различных сетевых приложений с гибкой сетью.

- Мощные функции диагностики и обслуживания

DRP 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.

18.2.2 Основные концепции

1. Режимы DRP

DRP имеет два режима: DRP-Port-Based и DRP-VLAN-Based.

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

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

2. Состояния порта DRP

Состояние пересылки: Если порт находится в состоянии пересылки, порт может и принимать, и отправлять пакеты данных. Состояние блокировки: Если порт находится в состоянии блокировки, порт может и принимать пакеты DRP, но не другие пакеты данных.

Основной порт: указывает кольцевой порт (для коммутатора Root), состояние которого настроено как принудительная переадресация пользователем, когда

кольцо

замкнуто.

Предупреждение:

- Если для коммутатора Root не настроен основной порт, им будет первый порт, состояние связи которого изменилось на «работает» (когда кольцо замкнуто), и он будет состоянии пересылки. Остальные кольцевые порты находятся в состоянии блокировки.
- Порт на устройстве Root в состоянии блокировки может активно отправлять пакеты DRP.

3. Режимы DRP

DRP определяет роли коммутаторов, пересылая пакеты Announce, предотвращая образование петель в кольцах резервирования.

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

INIT: указывает устройство, на котором включен DRP, а хотя бы один кольцевой порт находится в состоянии Link up. 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. Состояния 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 DRP, отвечающее хотя бы одному из следующих условий: один кольцевой порт находится в состоянии Link up, а другой — в состоянии Link down, 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. Состояния кольцевых портов: Один кольцевой порт находится в

состоянии пересылки.

Normal: указывает устройство, на котором включен DRP, и оба кольцевых порта находятся в состоянии Link up без ухудшения CRC, а приоритет меньше 200. Normal только пересылает пакеты Announce, но не проверяет содержимое пакетов.

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

Состояния кольцевых портов: Оба кольцевых порта находятся в состоянии пересылки.

18.2.3 Реализация

Каждый коммутатор поддерживает свой собственный вектор пакета Announce.

Коммутатор с большим вектором будет выбран в качестве Root.

Вектор пакета Announce содержит следующую информацию для назначения роли.

Таблица 10 Вектор пакета Announce

Состояние канала	Ухудшение CRC		Приоритет роли	IP-адреса устройства	MAC-адрес устройства
	Состояние ухудшения CRC	Скорость ухудшения CRC			

Состояние канала: 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.

Состояние ухудшения CRC: Если ухудшение CRC происходит на одном порту, значение устанавливается равным 1. Если ухудшение CRC не происходит на двух кольцевых портах, значение устанавливается равным 0.

Скорость ухудшения CRC: Соотношение количества пакетов CRC и порогового значения за 15 минут.

Приоритет роли: Значение можно задать через веб-интерфейс.

Параметры в таблице 10 сравниваются в следующей процедуре:

1. Сначала проверяется значение состояния канала. Устройство с большим значением состояния канала считается имеющим больший вектор.
2. Если два сравниваемых устройства имеют одинаковое значение состояния канала, сравниваются значения состояния ухудшения CRC. Устройство с большим значением состояния ухудшения CRC считается имеющим больший вектор. Если значение состояния ухудшения CRC всех сравниваемых устройств равно 1, считается, что устройство с большим значением скорости ухудшения CRC имеет больший вектор.
3. Если два сравниваемых устройства имеют одинаковое значение состояния канала и значение ухудшения CRC, значения приоритета ролей, IP-адресов и MAC-адресов сравниваются последовательно. Устройство с большим значением считается имеющим больший вектор.
4. Устройство с большим вектором будет выбрано в качестве Root.

Примечание:

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

- Реализация режима DRP-Port-Based

Роли коммутаторов следующие:

1. При запуске все коммутаторы находятся в состоянии INIT. Когда состояние одного порта изменяется на Link up, коммутатор становится коммутатором Root и отправляет пакеты Announce другим коммутаторам в кольце для выбора.
2. Коммутатор с большим вектором пакета Announce будет выбран в качестве Root. Кольцевой порт, который первым на Root переходит в состояние Link up, находится в состоянии пересылки, а другой кольцевой порт находится в состоянии блокировки. Среди других коммутаторов в кольце коммутатор с одним кольцевым портом в состоянии Link down или ухудшения CRC является коммутатором B-Root. Коммутатор с обоими кольцевыми портами в состоянии Link up и без ухудшения CRC является коммутатором Normal.

Процедура устранения отказов показана на следующем рисунке:

1. В исходной топологии A является Root; порт 1 находится в состоянии пересылки, а

порт 2 в состоянии блокировки. B, C и D – коммутаторы Normal, и их кольцевые порты находятся в состоянии пересылки.

2. Когда линия связи CD неисправна, DRP изменяет состояние порта 6 и порта 7 на состояние блокировки. В результате C и D становятся коммутаторами Root. Поскольку коммутаторы A, C и D в настоящий момент являются коммутаторами Root, все они отправляют пакеты Announce. Векторы C и D больше, чем векторы A, потому что порты 7 и 6 находятся в состоянии Link down. В этом случае, если вектор D больше, чем вектор C, D выбирается в качестве Root, а C становится B-Root. При получении пакета Announce от D, A обнаруживает, что вектор D больше, чем его собственный вектор, и оба его кольцевых порта находятся в состоянии Link up. Таким образом, A становится Normal и меняет статус порта 2 на пересылку.

3. Когда связь CD восстанавливается, D по-прежнему является Root, поскольку его вектор больше, чем вектор C.

- 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.

DRP меняет статус порта 6 на пересылку. В результате C становится коммутатором Normal. Поэтому корневой узел этой сети не меняется для восстановления связи.

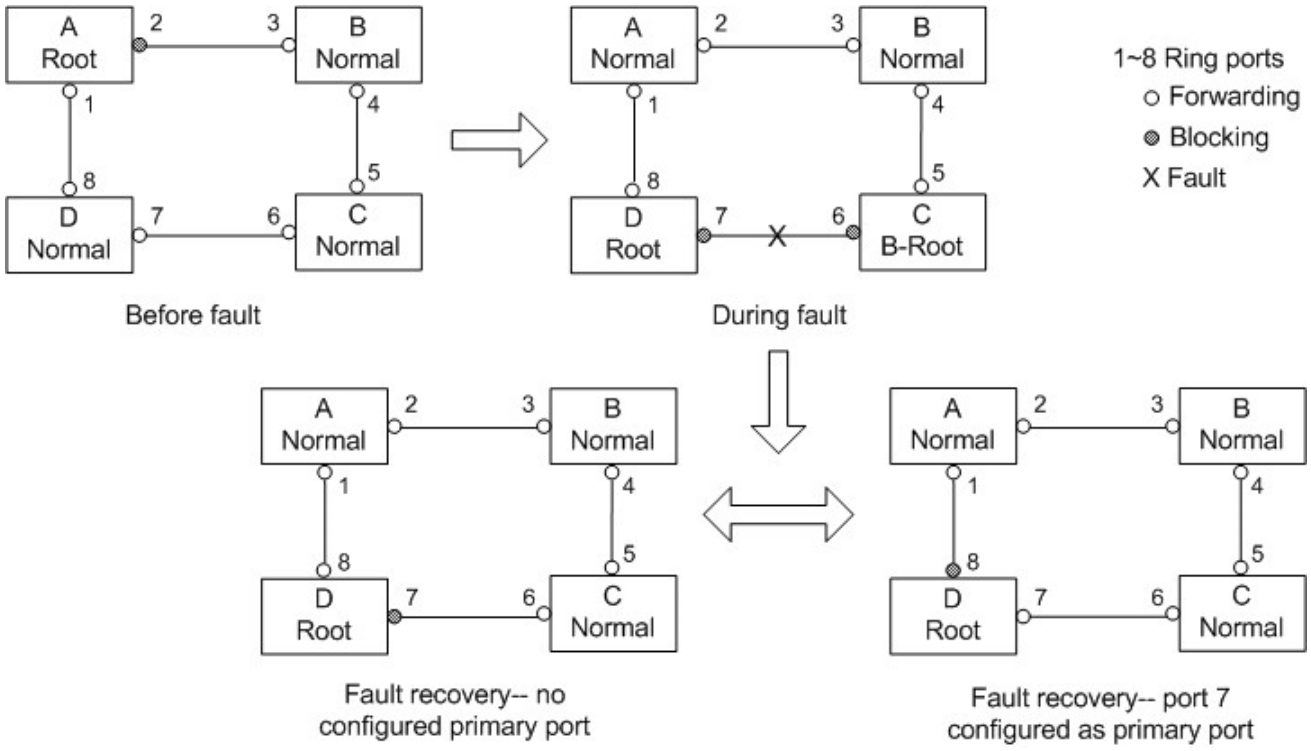


Рисунок 216 Отказ канала DRP

Примечание:

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

➢ Реализация режима DRP-VLAN-Based

Кольцо DRP-VLAN-Based позволяет пересылать пакеты из разных VLAN по разным путям. Каждый путь пересылки для VLAN образует DRP-VLAN-Based. Различные кольца на основе DRP-VLAN могут иметь разные корневые коммутаторы. Нак показано на следующем рисунке, сконфигурированы два кольца DRP-VLAN-Based.

Линии связи DRP-VLAN10/20-Based: AB-BC-CD-DE-EA.

Линии связи DRP-VLAN30-Based: FB-BC-CD-DE-EF.

Два кольца соприкасаются линиями связи 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.

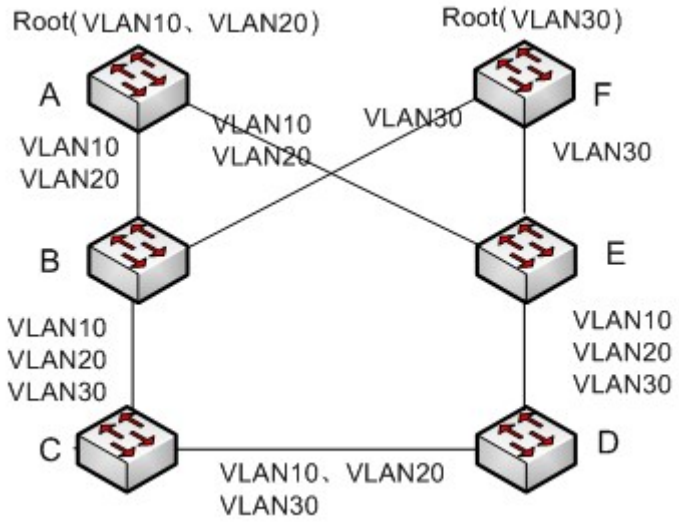


Рисунок 217 DRP-VLAN-Based

Примечание:

Статус порта и назначение ролей для каждого кольца на DRP-VLAN-Based такие же, как и DRP-Port-Based.

➢ Резервирование DRP

DRP также может обеспечивать резервирование двух колец DRP, предотвращая образование петель и обеспечивая нормальный обмен данными между кольцами.

Порт резервирования: указывает порт связи между кольцами DRP. Можно настроить несколько портов резервирования, но они должны находиться в одном кольце. Первый резервный порт в состоянии Link up – это резервный порт Master, который находится в состоянии пересылки. Все остальные порты являются портами Slave. Они находятся в состоянии блокировки.

Как показано на рисунке 218, на каждом коммутаторе можно настроить один резервный порт. Резервный порт Master находится в состоянии пересылки, а другие резервные порты — в состоянии блокировки. Если резервный порт Master или его канал выходят из строя, для пересылки данных будет выбран резервный порт Slave.

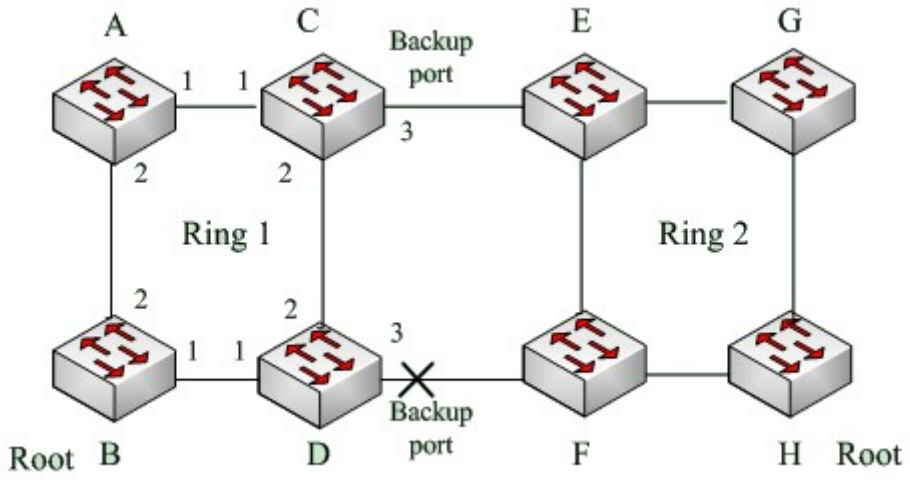


Рисунок 218 Резервирование DRP

Предупреждение:

Изменение статуса соединения влияет на статус резервных портов.

18.3 DHP

18.3.1 Обзор

Как показано на рисунке 219, коммутаторы A, B, C и D подключены к кольцу. Протокол Dual Homing (DHP) выполняет 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.
- Если связь между A и B неисправна, A все еще может обмениваться данными с B, C и D через Устройство 1 и Устройство 2.

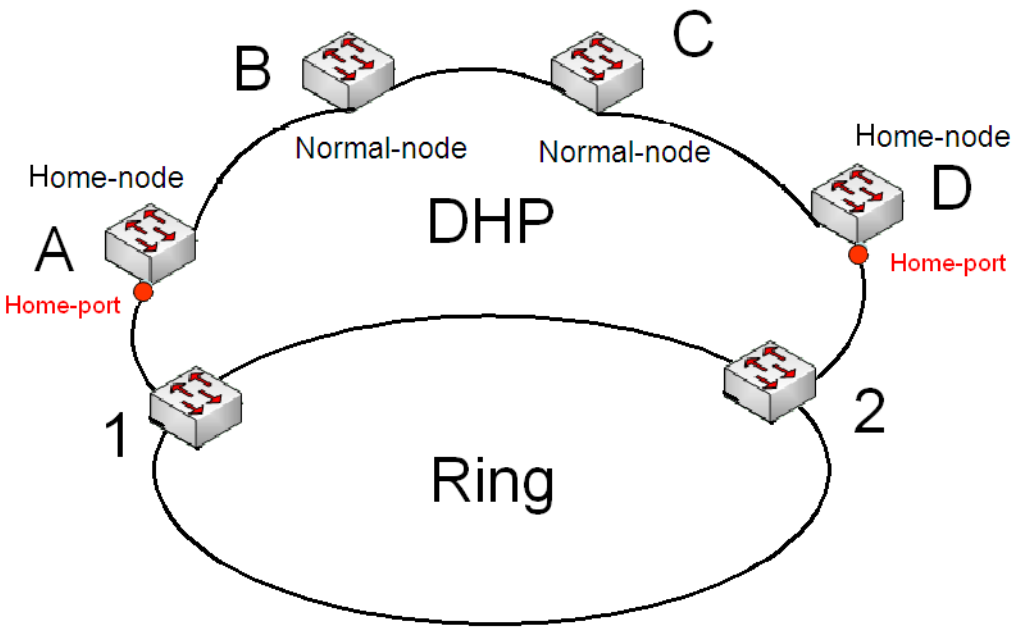


Рисунок 219 Использование DHP

18.3.2 Основные концепции

Реализация DHP основана на DRP. Механизм выбора и назначения ролей в DHP такой же, как и в DRP. DHP обеспечивает резервирование канала посредством настройки узла Home, узла Normal и порта Home.

Узел Home: указывает устройства на обоих концах канала DHP и завершает пакеты DRP.

Порт Home: указывает порт, соединяющий узел Home с внешней сетью. Порт Home обеспечивает следующие функции:

- Отправка ответных пакетов Root после получения пакетов Announce от Root. Если Root получает ответные пакеты, состояние кольца идентифицируется как замкнутое. Если Root получает не ответные пакеты, состояние кольца идентифицируется как разомкнутое.
- Блокировка пакетов DRP внешних сетей и изоляция канала DHP от внешних сетей.
- Отправка пакетов очистки входа на подключенные устройства во внешних сетях при изменении топологии канала DHP.

Узел Normal: указывает устройства в канале DHP, за исключением устройств на обоих концах. Узлы Normal передают ответные пакеты домашних узлов Home.

18.3.3 Реализация

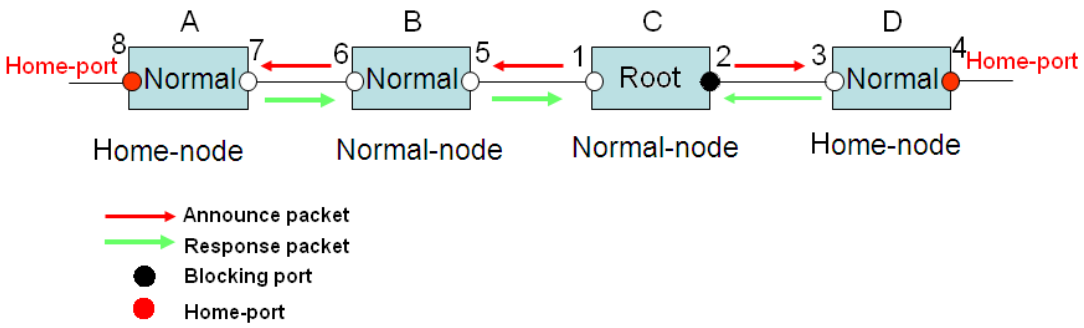


Рисунок 220 Конфигурация DHP

Как показано на рисунке 219, конфигурации A, B, C и D на рисунке 220 следующие:

- Конфигурация DRP: C — Root; порт 2 находится в состоянии блокировки; A, B и D являются узлами Normal; все остальные порты кольца находятся в состоянии пересылки.
- Конфигурация DHP A и D — узлы Home; порт 8 и порт 4 — порты Home; B и C являются узлами Normal.

Реализация:

1. C, Root, отправляет пакеты Announce через два своих кольцевых порта. Порт Home 8 и порт Home 4 завершают полученные пакеты Announce и отправляют ответные пакеты на C. C идентифицирует состояние кольца как замкнутое. Порт 2 находится в состоянии блокировки.

2. Когда канал между A и B заблокирован, топология включает два канала: A и B-C-D.

- A выбран в качестве Root. Порт 7 находится в состоянии блокировки.
- B канале B-C-D B выбран в качестве Root. Порт 6 находится в состоянии блокировки. C становится узлом Normal. Порт 2 находится в состоянии пересылки. A может обмениваться данными с B, C и D через Устройство 1 и Устройство 2, как показано на рисунке 221.

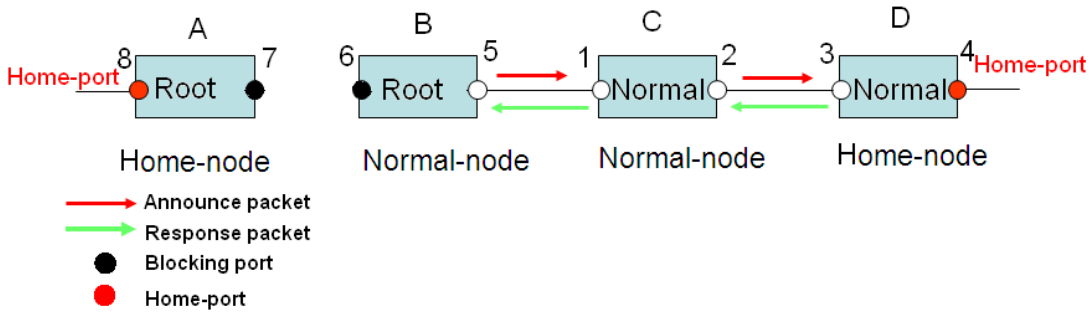


Рисунок 221 Устранение отказа DHP

18.3.4 Описание

Конфигурации DRP отвечают следующим требованиям:

- Все коммутаторы в одном кольце должны иметь одинаковый номер домена.
- Одно кольцо содержит только один узел Root, но может содержать несколько узлов B-Root или Normal.
- На каждом коммутаторе можно настроить только два порта для кольца.
- Для двух объединенных колец резервные порты можно настроить только в одном кольце.
- В одном кольце можно настроить несколько портов резервирования.
- На коммутаторе в одном кольце может быть настроен только один резервный порт.

18.3.5 Настройка через веб-интерфейс

1. Настройте режим резервирования DRP, как показано на рисунке 222.

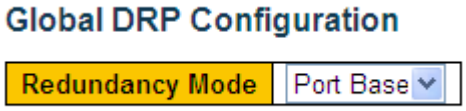


Рисунок 222 Настройка режима резервирования DRP

Режим резервирования

Варианты: Port Based/Vlan Based

По умолчанию: Port Based

Функция: Настройка режима резервирования DRP

Предупреждение:

- К кольцевым протоколам на основе портов относятся RSTP, DT-Ring-Port и DRP-Port, к протоколам на основе VLAN – MSTP, DT-Ring-VLAN и DRP-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 порта и кольцевой протокол на основе VLAN являются взаимоисключающими, и для одного устройства можно выбрать только один режим кольцевого протокола.

---

2. НастройтеDRP-Port-Based и DRP-VLAN-Based, как показано на рисунке 223 и рисунке 224.

Рисунок 223 Настройка DRP-Port-Based

Рисунок 224 Настройка DRP-VLAN-Based

Domain ID

Диапазон: 1~32

Функция: Каждое кольцо имеет уникальный идентификатор домена. Один коммутатор поддерживает максимум 8 колец на основе VLAN, количество колец на основе портов зависит от количества портов коммутатора.

Domain Name

Диапазон: 1~31 символ

Функция: Задание доменного имени.

Ring Port-1/Ring Port-2

Варианты: все порты коммутатора

Функция: Выбор двух кольцевых портов.

Предупреждение:

- Кольцевой порт DRP или резервный порт и канал портов являются взаимоисключающими. Кольцевой порт DRP или резервный порт не могут быть добавлены к каналу портов; порт в канале портов не может быть настроен в качестве кольцевого порта DRP или резервного порта.

- Кольцевые порты между кольцевыми протоколами на основе портов RSTP, DT-Ring-Port и DRP-Port являются взаимоисключающими, то есть кольцевой порт и резервный порт DRP-Port не могут быть настроены как порт RSTP, DRP-Port. кольцевой порт DT-Ring-Port или резервный порт DT-Ring-Port; Порт RSTP, кольцевой порт DT-Ring-Port и резервный порт DT-Ring-Port нельзя настроить как кольцевой порт DRP-Port ring или резервный порт.
- Не рекомендуется одновременно настраивать порты в изолированной группе как порты DRP и резервные порты, а порты DRP и резервные порты нельзя добавлять в изолированную группу.

Основной порт

Варианты: --/Ring Port-1/Ring Port-2

По умолчанию: --

Функция: Настройка основного порта. Когда кольцо замкнуто, основной порт коммутатора Root находится в состоянии пересылки.

Режим DHP

Варианты: Disable/Normal-Node/Home-Node

По умолчанию: Disable

Функция: Отключение DHP или настройка режима DHP.

DHP Home Port

Варианты: Ring-Port-1/Ring-Port-2/Ring-Port-1-2

Функция: Настройка порта Home для узла Home DHP.

Описание: Если в канале DHP есть только одно устройство, оба кольцевых порта узла Home должны быть настроены как порты Home.

CRC Threshold

Диапазон: 25~65535

По умолчанию: 100

Функция: Настройка порогового значения CRC.

Описание: Этот параметр используется при выборе коммутатора Root. Система подсчитывает количество полученных CRC. Если количество CRC одного

кольцевого порта превышает пороговое значение, система считает, что порт имеет ухудшение CRC. В результате в векторе пакета Announce порта значение ухудшения CRC устанавливается равным 1.

Role Priority

Диапазон: 0~255

По умолчанию: 128

Функция: Настройка приоритета коммутатора.

Резервный порт

Варианты: все порты коммутатора.

Функция: Настройка резервного порта.

Предупреждение:

Не следует настраивать кольцевой порт в качестве резервного.

VLAN List

Варианты: Все созданные VLAN

Функция: Выбор VLAN, управляемой данным кольцом DRP-VLAN-Based

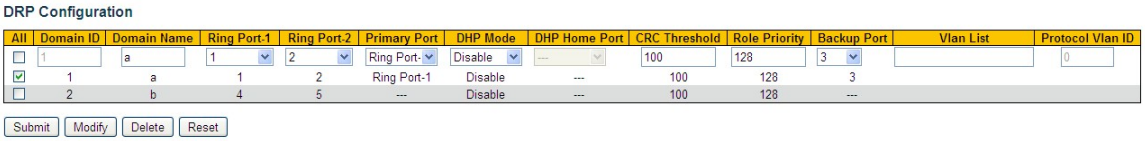
Protocol Vlan ID

Диапазон: 1~4093

Описание: VLAN ID должен быть идентификатором сервисной VLAN.

Функция: Пакеты DRP с VLAN ID служат основой для диагностики и обслуживания кольца DRP-VLAN-Based.

3. Просмотрите и измените конфигурацию DRP, как показано на рисунке 225.



Просмотрите и измените конфигурацию DRP, как показано на рисунке 225.

Выберите запись DRP, щелкните <Modify>, чтобы редактировать конфигурацию DRP; щелкните <Delete>, чтобы удалить выбранную запись DRP.

4. Щелкните запись DRP на рисунке 225, чтобы отобразить состояние DRP и порта, как показано на рисунке 226.

DRP Information

Domain ID	1
Domain Name	a
Role State	ROOT
Ring State	Close
Ring Port-1	1 | FORWARD
Ring Port-2	2 | BLOCK
Primary Port	Ring Port-1
DHP Mode	Disable
DHP Home Port	---
CRC Threshold	100
Role Priority	128
Backup Port	3 | INIT

Рисунок 226 Состояние DRP

18.3.6 Пример типовой конфигурации

Как показано на рисунке 218, A, B, C и D образуют кольцо 1; E, F, G и H образуют кольцо 2; CE и DF являются резервными каналами Ring 1 и Ring 2.

Конфигурация коммутатора A и коммутатора B:

1. Установите Domain ID 1 и Domain name a. Выберите кольцевой порт 1 и кольцевой порт 2. Сохраните значения по умолчанию для приоритета роли и резервного порта, как показано на рисунке 223.

Конфигурация коммутатора C и коммутатора D:

2. Установите Domain ID 1, Domain name a, резервный порт 3.Выберите кольцевой порт 1 и кольцевой порт 2. Сохраните значения по умолчанию для приоритета роли, как показано на рисунке 223.

Конфигурация коммутаторов E, F, G и H:

3. Установите Domain ID 2 и Domain name b. Выберите кольцевой порт 1 и кольцевой порт 2.Сохраните значения по умолчанию для приоритета роли и резервного порта, как показано на рисунке 223.

18.4 RSTP/STP

18.4.1 Введение

Стандартизированный в IEEE802.1D протокол 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, чтобы перейти в состояние пересылки, должен ждать в два раза дольше, чем задержка пересылки.

Чтобы преодолеть этот недостаток, IEEE создает стандарт 802.1w в дополнение к 802.1D. IEEE802.1w определяет протокол 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. Когда корневой порт выходит из строя, альтернативный порт может быстро войти в состояние пересылки.

18.4.2 Основные концепции

Корневой мост: служит корнем дерева. Сеть имеет только один корневой мост. Корневой мост меняется в зависимости от топологии сети. Корневой мост периодически отправляет BPDU другим устройствам, которые пересылают BPDU для обеспечения стабильности топологии.

Корневой порт: указывает наилучший порт для передачи от некорневых мостов к корневому мосту. Лучший порт — это порт с наименьшей стоимостью пути до корневого моста. Некорневой мост взаимодействует с корневым мостом через корневой порт. Некорневой мост имеет только один корневой порт. Корневой мост не имеет корневого порта.

Назначенный порт: указывает порт для пересылки BPDU на другие устройства или локальные сети. Все порты корневого моста являются назначенными портами.

Альтернативный порт: указывает резервный порт корневого порта. Если корневой порт выходит из строя, альтернативный порт становится новым корневым портом.

Резервный порт: указывает резервный порт назначенного порта. Когда назначенный порт выходит из строя, резервный порт становится новым назначенным портом и пересылает данные.

18.4.3 18.4.3 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 таблице11 показана структура данных BPDU.

Таблица 11 BPDU

…	ID корн. моста	Стоим. корн. пути	ID назн. моста	ID назн. порта	Возр. сообщ.	Макс. возр.	Инт. Hello	Задерж. отпр.	…
…	8 байт	4 байта	8 байт	2 байта	2 байта	2 байта	2 байта	2 байта	…

ID корневого моста: приоритет корневого моста (2 байта) +MAC-адрес корневого моста (6 байт).

Стоимость корневого пути: стоимость пути к корневому мосту.

ID назначенного моста: приоритет назначенного моста (2 байта) +MAC-адрес назначенного моста (6 байт).

ID назначенного порта: приоритет порта + номер порта.

Возраст сообщения: продолжительность распространения BPDU по сети.

Макс. возраст: максимальная продолжительность хранения BPDU на устройстве.

Когда возраст сообщения больше чем макс. возраст, BPDU отбрасывается.

Интервал Hello: интервал времени для отправки BPDU.

Задержка отправки: задержка изменения статуса (отбрасывание--обнаружение--пересылка).

18.4.4 Реализация

Процесс вычисления связующего дерева с помощью BPDU для всех мостов выглядит следующим образом:

1. В начальной фазе

Каждый порт всех устройств генерирует BPDU с самим собой в качестве корневого моста; и идентификатор корневого моста, и идентификатор назначенного моста являются идентификатором локального устройства; стоимость корневого пути равна 0; назначенный порт является локальным портом.

2. 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, идентификаторы назначенного моста, идентификаторы назначенного порта 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.

3. Выбор корневого моста

Корневой мост связующего дерева — это мост с наименьшим идентификатором моста.

4. Выбор корневого порта

Устройство без корневого моста выбирает порт, получающий лучший BPDU, в качестве корневого порта.

5. Расчет BPDU назначенного порта

На основе BPDU корневого порта и стоимости пути корневого порта устройство вычисляет BPDU назначенного порта для каждого порта следующим образом:

- Идентификатор корневого моста заменяется идентификатором корневого моста BPDU корневого порта.
- Стоимость корневого пути заменяется на стоимость корневого пути BPDU корневого порта плюс стоимость пути корневого порта.
- Идентификатор назначенного моста заменяется идентификатором локального устройства.
- Идентификатор назначенного порта заменяется идентификатором локального

порта.

6. Выбор назначенного порта.

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.

18.4.5 Настройка через веб-интерфейс

1. Задайте параметры времени сетевого моста, как показано на рисунке 227.

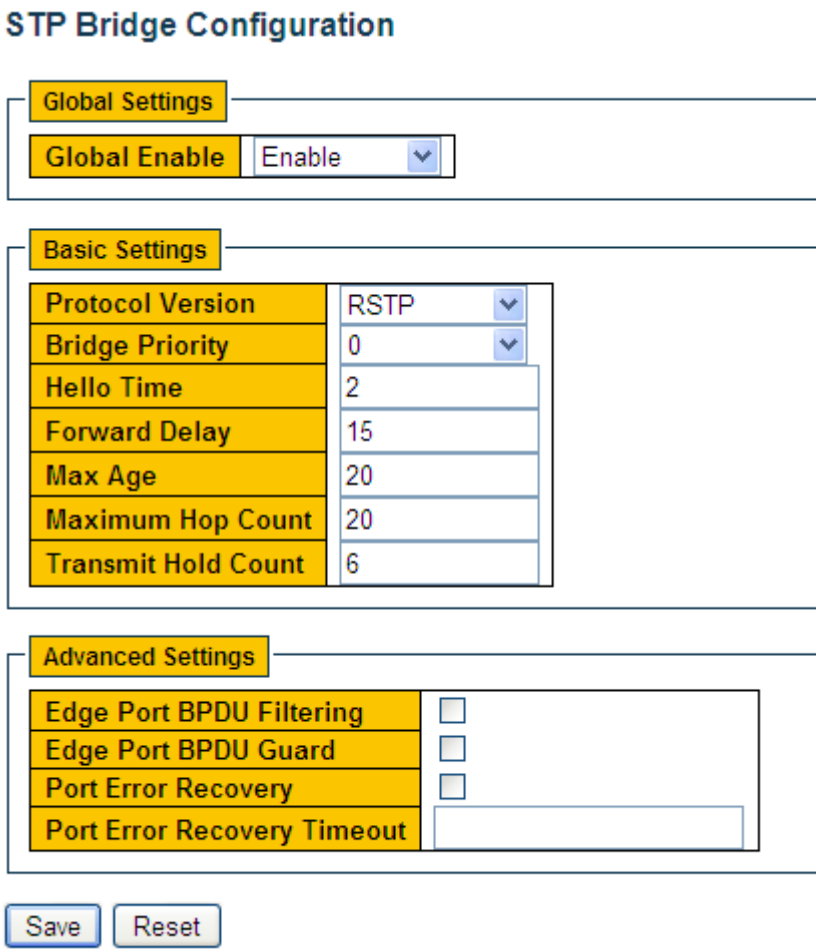


Рисунок 227 Задание параметров времени сетевого моста

Global Enable

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включить или выключить связующее дерево.

Предупреждение:

- К кольцевым протоколам на основе портов относятся RSTP, DT-Ring-Port и DRP-Port, к протоколам на основе VLAN – MSTP, DT-Ring-VLAN и DRP-VLAN.
- Кольцевой протокол на основе порта и кольцевой протокол на основе VLAN являются взаимоисключающими, и для одного устройства можно выбрать только один режим кольцевого протокола.

Protocol Priority

Варианты: MSTP/RSTP/STP
По умолчанию: MSTP

Функция: Выбор протокола связующего дерева.

Bridge Priority

Диапазон: 0~61440. Шаг составляет 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 времени для отправки BPDU.

Forward Delay

Диапазон: 4~30 с

По умолчанию: 15 с

Функция: Настройте время изменения статуса с Discarding на Learning или с Learning на Forwarding.

Max Age

Диапазон: 6~40 с

По умолчанию: 20 с

Функция: Максимальная продолжительность хранения BPDU на устройстве.

Описание: Если значение возраста сообщения в BPDU больше указанного значения, то BPDU отбрасывается.

Предупреждение:

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

Transmit Hold Count

Диапазон: 1~10

По умолчанию: 6

Функция: Задание максимального количества пакетов BPDU, которое может быть отправлено портом в течение каждого промежутка Hello Time.

Edge Port BPDU Filtering

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение и выключения режима получения и отправки граничным портом пакетов BPDU.

Edge Port BPDU Guard

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Режим контроля перехода граничного порта в состояние Error-Disable и закрытия при получении пакетов BPDU.

Port Error Recovery

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Контроль возможности порта автоматически восстанавливаться из состояния ошибки в нормальное состояние.

Port Error Recovery Timeout

Диапазон: 30~86400 c

Функция: Задание для порта времени для восстановления из состояния ошибки в нормальное состояние.

2. Настройте порт RSTP, как показано на рисунке 228.

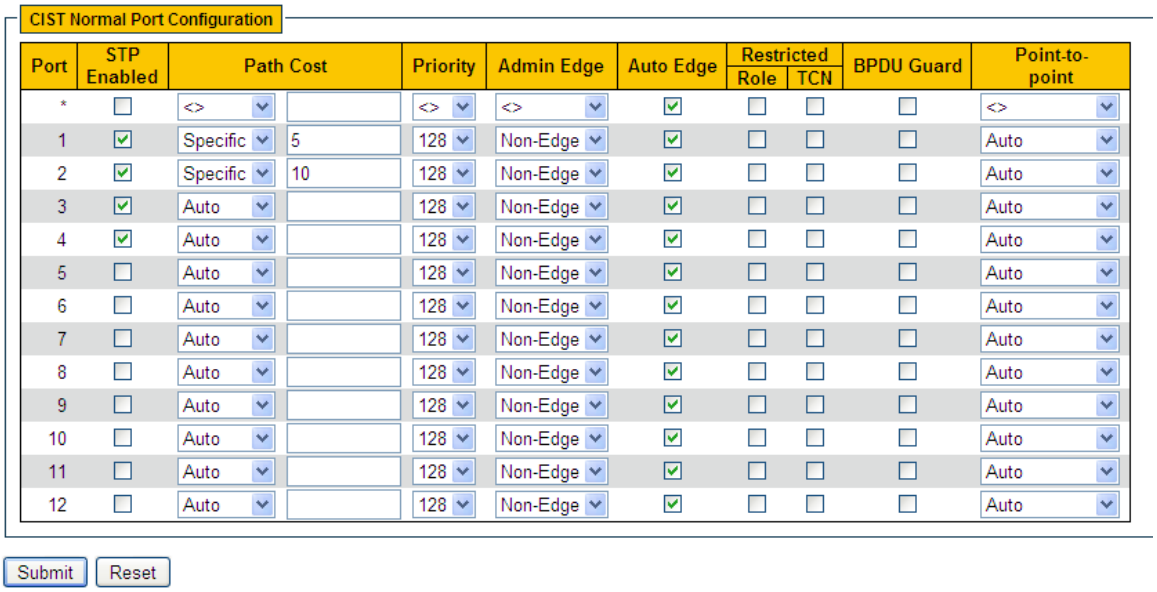


Рисунок 228 Настройка порта RSTP

STP Enabled

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение или выключение STP/RSTP для порта.

Предупреждение:

- Канал портов и порт RSTP являются взаимоисключающими. Порты в канале портов нельзя настроить как порт RSTP, а порт RSTP нельзя добавить в канал портов.
- Кольцевые порты между кольцевыми протоколами на основе портов RSTP, DT-Ring-Port и DRP-Port являются взаимоисключающими, то есть порт RSTP нельзя настроить как кольцевой порт DRP-Port/DT-Ring-Port или резервный порт DRP-Port/DT-Ring-Port; Кольцевой порт DRP-Port/DT-Ring-Port и резервный порт DRP-Port/DT-Ring-Port нельзя настроить как порт RSTP.
- Не рекомендуется одновременно настраивать порты в изолированной группе как порты RSTP, а порты RSTP нельзя добавлять в изолированную группу.

Path Cost

Варианты: Auto/Specific (1~200000000)

По умолчанию: Auto

Описание: Стоимость пути порта используется для расчета наилучшего пути. Значение параметра зависит от полосы пропускания. Чем больше значение, тем ниже стоимость. Можно изменить роль порта, изменив значение параметра стоимости пути. Чтобы настроить значение вручную, выберите значение No для параметра Cost Count.

Priority

Диапазон: 0~240. Шаг составляет 16.

По умолчанию: 128

Функция: Настройка приоритета порта, определяющего роли портов.

Admin Edge

Варианты: Non-Edge/Edge

По умолчанию: Non-Edge

Функция: Настройка порта в режим граничного порта.

Описание: Когда порт напрямую подключен к терминалу и не подключен к другим устройствам или общему сегменту сети, этот порт считается граничным портом. Граничный порт может быстро перейти из состояния блокировки в состояние пересылки без задержки ожидания. После того как граничный порт получает пакеты BPDU, он перестает быть граничным портом.

Auto Edge

Варианты: Enable/Disable

По умолчанию: Enable

Функция: Включение функции автоматического обнаружения граничного порта.

Restricted Role

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Порт с ограничением роли никогда не будет выбран в качестве корневого узла, даже если ему предоставлен наивысший приоритет.

Restricted TCN

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Порт с ограниченным TCN не будет активно отправлять сообщения TCN.

BPDU Guard

Варианты: Enable/Disable
По умолчанию: Disable

Функция: Режим контроля перехода граничного порта в состояние Error-Disable и закрытия при получении пакетов BPDU.

Point-to-point

Варианты: Auto/Forced True/Forced False

По умолчанию: Auto

Функция: Настройка типа соединения для порта. Если порт подключен к каналу «точка-точка», порт может быстро перейти в другое состояние.

Описание: **Auto** указывает, что коммутатор автоматически определяет тип канала на основе того, что порт работает в дуплексном режиме. Когда порт работает в полнодуплексном режиме, коммутатор считает, что тип соединения, подключенного к порту, — точка-точка; когда порт работает в полудуплексном режиме, коммутатор считает, что тип соединения, подключенного к порту, является общим. Принудительное задание соединения «точка-точка» означает, что соединение, подключенное к порту, является соединением «точка-точка», а принудительное задание совместного использования означает, что соединение, подключенное к порту, является общим соединением.

18.4.6 Пример типовой конфигурации

Приоритеты коммутаторов A, B и C: 0, 4096 и 8192. Стоимость пути для соединений составляет 4, 5 и 10, как показано на рисунке 229.

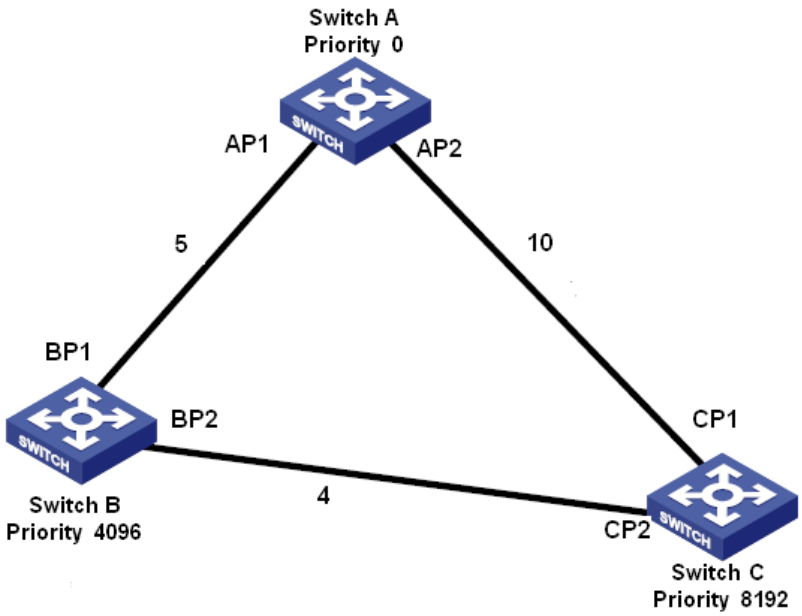


Рисунок 229 Пример настроек RSTP

Конфигурация коммутатора A:

1. Установите приоритет моста 0 и значения по умолчанию для временных параметров, как показано на рисунке 227.

2. Установите стоимость пути для порта 1 – 5 и для порта 2 – 10, как

показано нарисунке 228. Конфигурация коммутатора B:

1. Установите приоритет моста 4096 и значения по умолчанию для временных параметров, как показано на рисунке 227.

2. Установите стоимость пути для порта 1 – 5 и для порта 2 – 4, как

показано нарисунке 228. Конфигурация коммутатора C:

1. Установите приоритет моста 8192 и значения по умолчанию для временных параметров, как показано на рисунке 227.

2. Установите стоимость пути для порта 1 – 10 и для порта 2 – 4, как показано нарисунке 228.

- Приоритет коммутатора A равен 0, а его корневой идентификатор наименьший. Таким образом, коммутатор A является корневым мостом.
- Стоимость пути от AP1 к BP1 равна 5, а от AP2 к BP2 равна 14. Таким образом, BP1 является корневым портом.
- Стоимость пути от AP1 к CP2 равна 9, а от AP2 к CP1 равна 10. Таким образом, CP2 является корневым портом, а BP2 является назначенным портом.

18.5 Настройка MSTP

18.5.1 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 Рисунок 230, 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 обмениваться данными с портом коммутатора C.

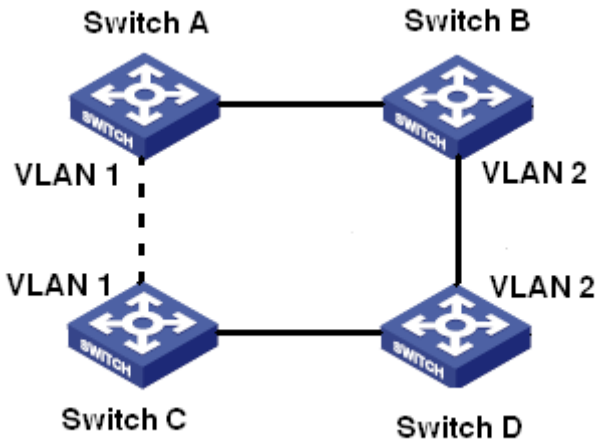


Рисунок 230 Недостатки RSTP

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 регион. Каждый регион содержит несколько взаимно независимых связующих деревьев. Регион выступает коммутационным узлом. Он участвует в вычислении с другими регионами на основе алгоритма связующего дерева, вычисляя общее связующее дерево. На основе этого алгоритма сеть на рисунке 230 формирует топологию, показанную на рисунке 231. Коммутатор A и коммутатора B находятся в Region1. Ни одна связь не заблокирована, так как регион не содержит петель. То же самое и с Region2. Region1 и Region2 аналогичны узлам коммутатора. Эти два «коммутатора» образуют петлю. Таким образом, связь должна быть заблокирована.

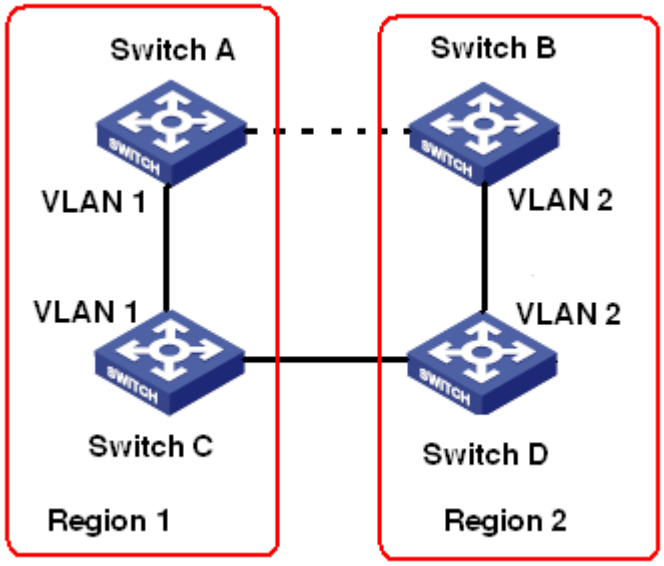


Рисунок 231 Топология MSTP

18.5.2 Основная концепция

Ознакомьтесь с концепцией MSTP, показанной на рисунке 232 и рисунке 235.

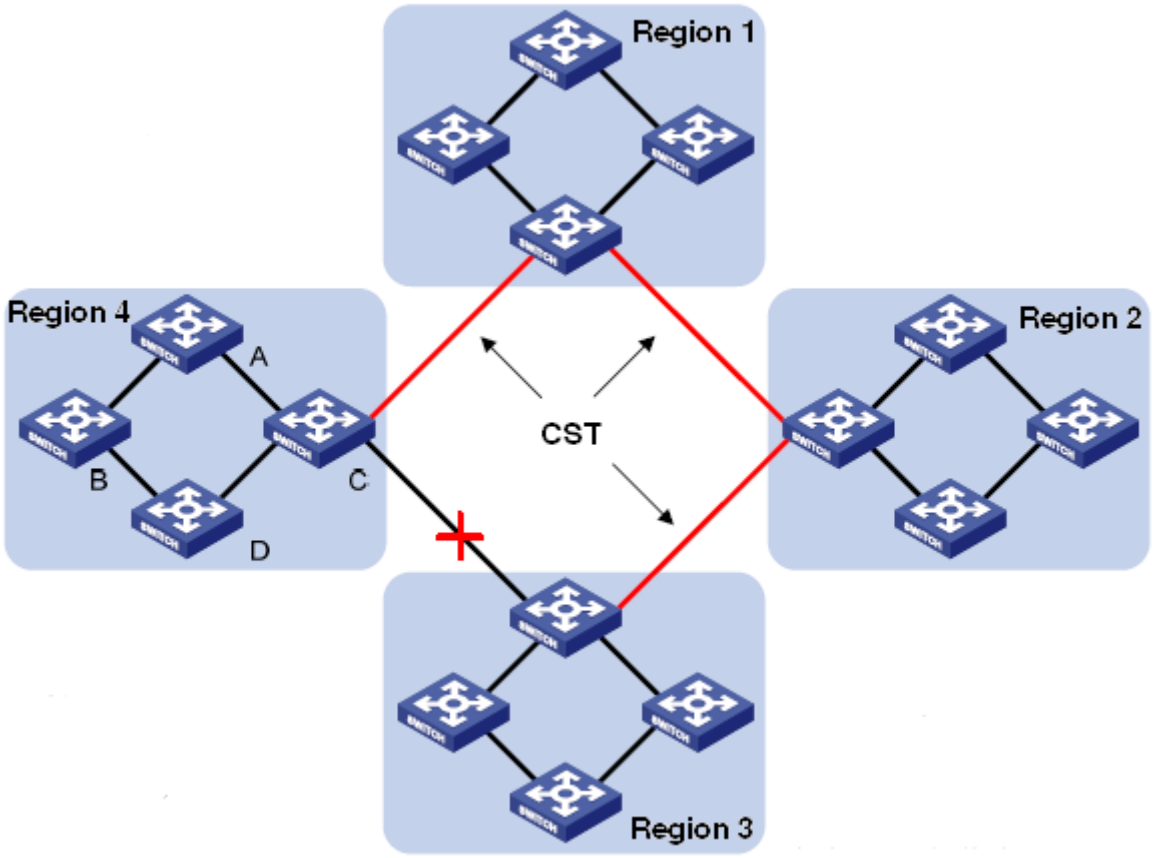


Рисунок 232 Концепция MSTP

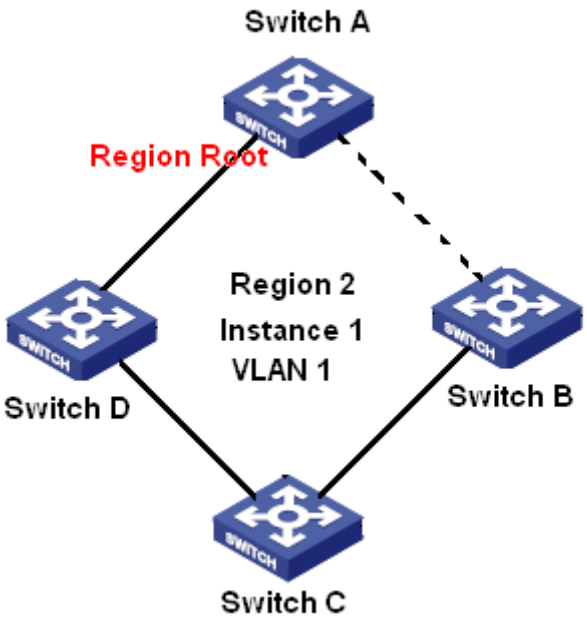


Рисунок 233 Сопоставление VLAN 1 с экземпляром 1

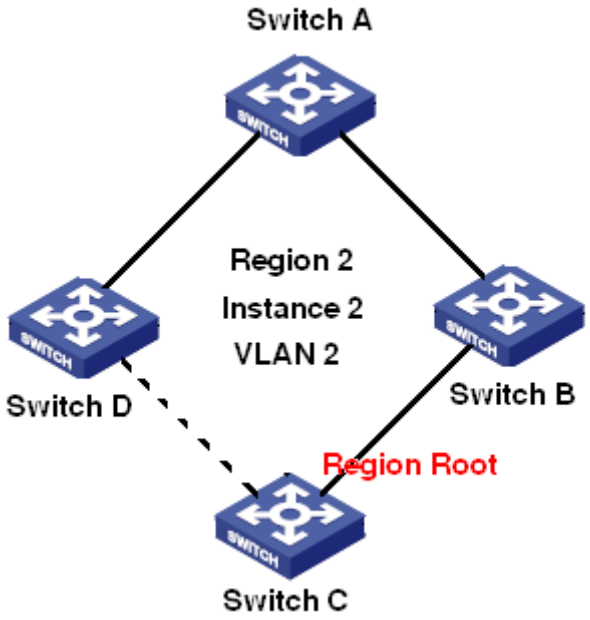


Рисунок 234 Сопоставление VLAN 2 с экземпляром 2

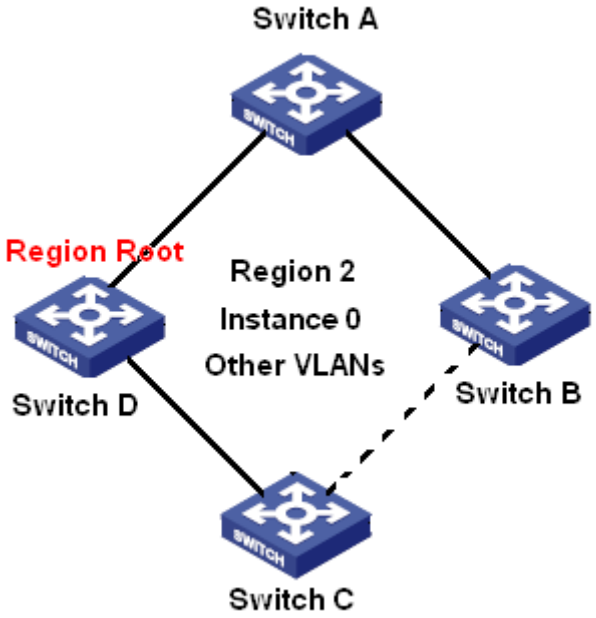


Рисунок 235 Сопоставление другой VLAN с экземпляром 0

Экземпляр: набор из нескольких VLAN. Одна VLAN (как показано на рисунке 233 и рисунке 234) или несколько VLAN с одинаковой топологией (как показано на рисунке 235) могут быть сопоставлены с одним экземпляром; то есть одна VLAN может образовывать связующее дерево, а несколько VLAN могут совместно использовать одно связующее дерево. Разные экземпляры сопоставляются с разными связующими деревьями. Экземпляр 0 – это связующее дерево для устройств всех регионов, в то время как остальные экземпляры – это связующие деревья для устройств

конкретного региона.

Multiple Spanning Tree Region (регион MST): Коммутаторы с одинаковым именем региона MSTP, уровнем версии и сопоставлением VLAN–экземпляр принадлежат одному региону MST. Как показано на рисунке 232, регион 1, регион 2, регион 3 и регион 4 – это четыре различных региона MST.

Таблица сопоставления VLAN: состоит из сопоставления VLAN и связующих деревьев. На рисунке 232 , таблица сопоставления VLAN региона 2 – это сопоставление VLAN 1 и экземпляра 1, как показано на рисунке 233; VLAN 2 сопоставляется с экземпляром 2, как показано на рисунке 234.. Другие VLAN сопоставляются с экземпляром 0, как показано на рисунке 235.

Общее и внутреннее связующее дерево (CIST): указывает экземпляр 0, то есть связующее дерево, охватывающее все устройства в коммутируемой сети. Как показано на рисунке 232, CIST состоит из IST и CST.

Внутреннее связующее дерево (IST): указывает сегмент CIST в регионе MST, то есть экземпляр 0 каждого региона, как показано на рисунке 235.

Общее связующее дерево (CST): указывает связующее дерево, соединяющее все регионы MST в коммутируемой сети. Если каждый регион MST является узлом, CST - это связующее дерево, вычисленное этими узлами на основе STP/RSTP. Как показано на рисунке 232, красные линии обозначают связующее дерево.

MSTI (Несколько экземпляров связующего дерева): один регион MST может образовывать несколько связующих деревьев, и они не зависят друг от друга. Каждое связующее дерево является MSTI, как показано на рисунке 233 и рисунке 234. IST также является специальным MSTI.

Общий корень: указывает корневой мост CIST. Коммутатор с наименьшим идентификатором корневого моста в сети является общим корневым коммутатором. В регионе MST связующие деревья имеют разную топологию и их корни регионов также могут быть разными. Как показано на рисунке 233, рисунке 234 и рисунке 235, эти три экземпляра имеют разные корни региона. 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.

Состояние Forwarding: указывает, что порт изучает MAC-адреса и пересылает трафик. Состояние Learning: указывает, что порт изучает MAC-адреса, но не пересылает трафик. Состояние Discarding: указывает, что порт не изучает MAC-адреса и не пересылает трафик. Корневой порт: 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 Forwarding, Learning или Discarding.

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 Forwarding, Learning или Discarding.

Главный порт: указывает порт, который соединяет регион MST с общим корнем. Порт имеет кратчайший путь к общему корню. Исходя из CST, главный порт - это корневой порт региона (как узел). Главный порт - это специальный граничный порт. Это корневой порт для CIST и главный порт для других экземпляров. Главный порт может находиться в состоянии Forwarding, Learning или Discarding.

Альтернативный порт: указывает резервный порт корневого порта или главного порта. Если корневой порт или главный порт выходит из строя, альтернативный порт становится новым корневым портом или главным портом. Главный порт может находиться в только состоянии Discarding.

Резервный порт: указывает резервный порт назначенного порта. Когда назначенный порт выходит из строя, резервный порт становится новым назначенным портом и пересылает данные без задержки. Резервный порт может находиться в только состоянии Discarding.

18.5.3 Реализация MSTP

MSTP делит сеть на несколько регионов MST. CST рассчитывается между регионами. Для региона рассчитывается несколько связующих деревьев. Каждое связующее

дерево – это MSTI. Экземпляр 0 – это IST, остальные экземпляры – MSTI.

1. 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 вычисляется в каждом регионе MST.
- Каждый регион MST рассматривается как отдельное устройство, и CST рассчитывается между регионами.
- CST и IST составляют CIST всей сети.

2. Расчет MSTI

В регионе MST MSTP создает различные связующие деревья для VLAN на основе сопоставления между VLAN и связующими деревьями. Каждое связующее дерево рассчитывается независимо. Процесс расчета подобен процессу в STP.

В регионе MST пакеты VLAN пересылаются по соответствующим MSTI. Между регионами MST пакеты VLAN пересылаются по CST.

18.5.4 Настройка через веб-интерфейс

1. Задайте параметры времени сетевого моста, как показано на рисунке 236.

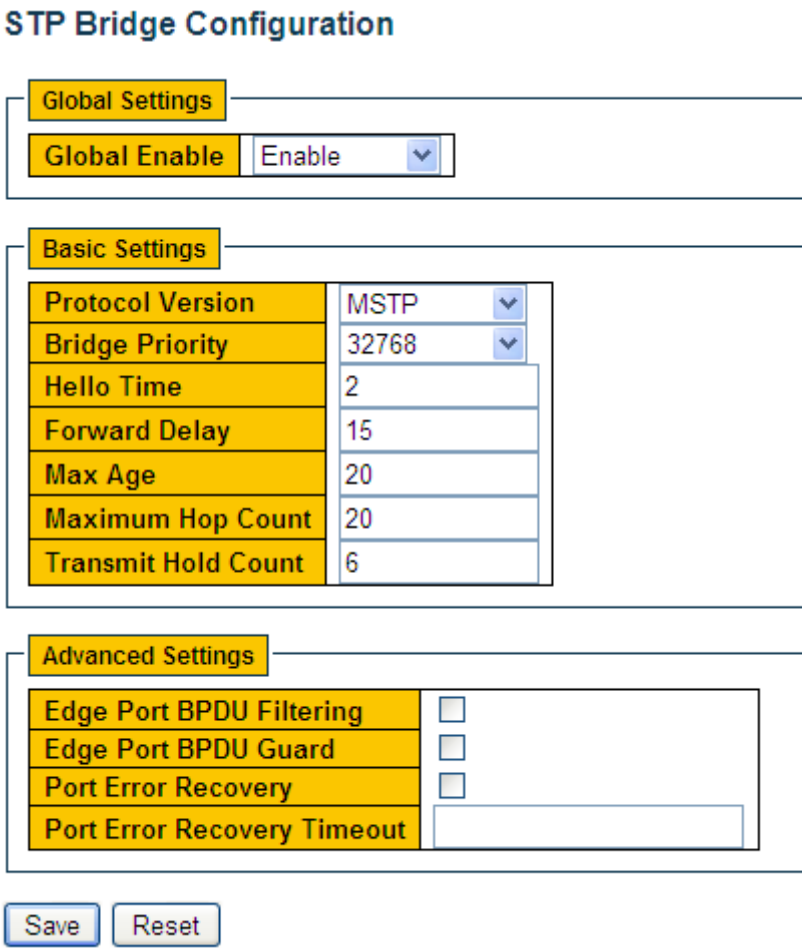


Рисунок 236
Задание параметров времени сетевого моста

Global Enable

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включить или выключить связующее дерево.

Предупреждение:

- К кольцевым протоколам на основе портов относятся RSTP, DT-Ring-Port и DRP-Port, к протоколам на основе VLAN – MSTP, DT-Ring-VLAN и DRP-VLAN.
- Кольцевой протокол на основе порта и кольцевой протокол на основе VLAN являются взаимоисключающими, и для одного устройства можно выбрать только один режим кольцевого протокола.

Protocol Priority

Варианты: MSTP/RSTP/STP

По умолчанию: MSTP

Функция: Выбор протокола связующего дерева.

Bridge Priority

Диапазон: 0~61440. Шаг составляет 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 времени для отправки BPDU.

Forward Delay

Диапазон: 4~30 с

По умолчанию: 15 с

Функция: Настройте время изменения статуса с Discarding на Learning или с Learning на Forwarding.

Max Age

Диапазон: 6~40 с

По умолчанию: 20 с

Функция: Максимальная продолжительность хранения BPDU на устройстве.

Описание: Если значение возраста сообщения в BPDU больше указанного значения, то BPDU отбрасывается.

Предупреждение:

- Значения Forward Delay Time, Hello Time и Max Age Time должны соответствовать следующим требованиям: 2 * (Forward Delay Time–1,0 с) >= Max Age Time; Max Age Time >= 2 * (Hello Time + 1,0 с).

- Рекомендуется использовать настройки по умолчанию.

Maximum Hop Count

Диапазон: 6~40

По умолчанию: 20

Функция: Настройка максимального числа транзитных участков региона MST. Максимальное число транзитных участков региона MST ограничивает масштаб региона MST; максимальное количество транзитных участков регионального корня равно максимальному количеству транзитных участков региона MST.

Описание: Начиная с корневого моста связующего дерева в регионе MST, из числа транзитных участков вычитается 1, когда BPDU проходит через устройство в регионе. Устройство отбрасывает BPDU с количеством транзитных участков 0.

Предупреждение:

- Действительна конфигурация только с максимальным количеством транзитных участков корневого моста в регионе MST. Устройство, не являющее корневым, использует конфигурацию транзитных участков корневого моста.
- Рекомендуется использовать настройки по умолчанию.

Transmit Hold Count

Диапазон: 1~10

По умолчанию: 6

Функция: Задание максимального количества пакетов BPDU, которое может быть отправлено портом в течение каждого промежутка Hello Time.

Edge Port BPDU Filtering

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение и выключения режима получения и отправки граничным портом пакетов BPDU.

Edge Port BPDU Guard

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Режим контроля перехода граничного порта в состояние Error-Disable и закрытия при получении пакетов BPDU.

Port Error Recovery

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Контроль возможности порта автоматически восстанавливаться из состояния ошибки в нормальное состояние.

Port Error Recovery Timeout

Диапазон: 30~86400 с

Функция: Задание для порта времени для восстановления из состояния ошибки в нормальное состояние.

2. Настройте сопоставление MSTI, как показано на рисунке 237.

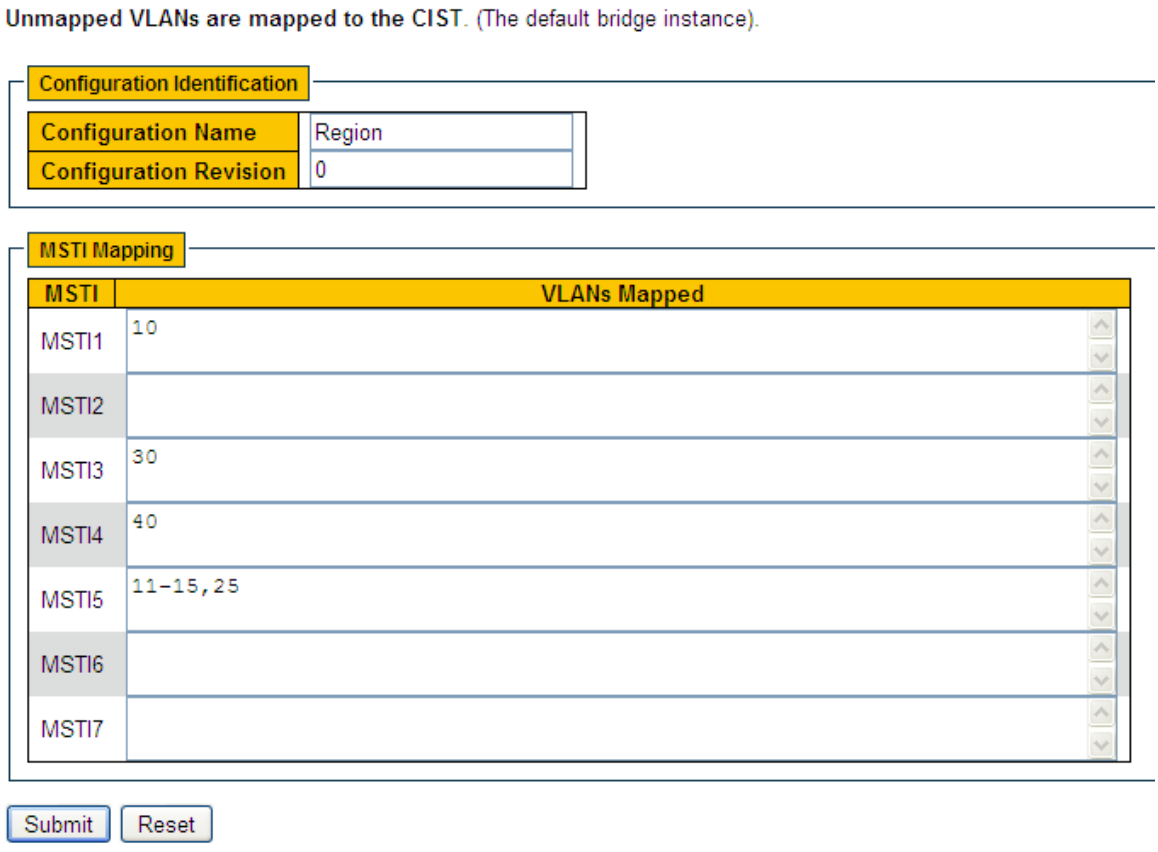


Рисунок 237 Настройка сопоставления MSTI

Configuration Name

Диапазон: 1-32 символа

По умолчанию: MAC-адрес устройства

Функция: Задание имени региона MST.

Configuration Revision

Варианты: 0~65535
По умолчанию: 0
Функция: Настройка параметра версии региона MSTP.

Описание: Параметр версии, имя региона MST и таблица сопоставления VLAN определяют регион MST, к которому принадлежит устройство. Когда все конфигурации совпадают, устройства находятся в одном регионе MST.

VLANs Mapped

Диапазон: 1~4094

Функция: Настройка таблицы сопоставления VLAN в регионе MST. При наличии нескольких VLAN их можно разделить запятой (,) и дефисом (-), где дефис используется для разделения двух последовательных идентификаторов VLAN, а запятая — для разделения двух непоследовательных идентификаторов VLAN.

Описание: По умолчанию все VLAN сопоставлены экземпляру 0. Одна VLAN сопоставляется только одному экземпляру связующего дерева. Если VLAN с существующим сопоставлением сопоставляется с другим экземпляром, предыдущее сопоставление отменяется. Если сопоставление между назначенной VLAN и экземпляром удалено, эта VLAN будет сопоставлена с экземпляром 0.

3. Настройте приоритет моста коммутатора в назначенном экземпляре, как показано на рисунке 238.

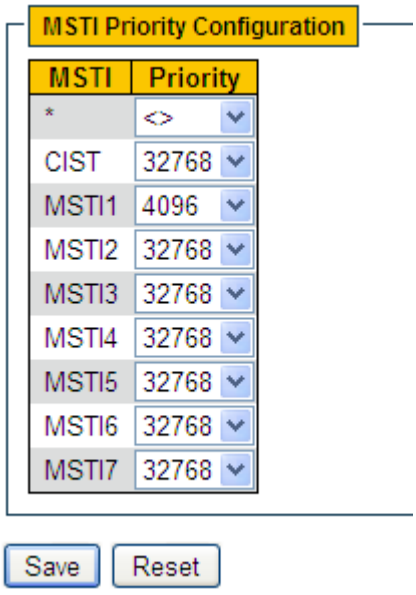


Рисунок 238 Настройка приоритета моста коммутатора в назначенном экземпляре

Priority

Диапазон: 0~61440 с шагом 4096
По умолчанию: 32768

Функция: Настройка приоритета 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, можно назначить определенное устройство корневым мостом связующего дерева. Устройство с поддержкой MSTP можно настроить с разными приоритетами в разных экземплярах связующего дерева.

Щелкните <Save>, чтобы текущие настройки вступили в силу.

4. Настройте порты CIST, как показано на рисунке 239.

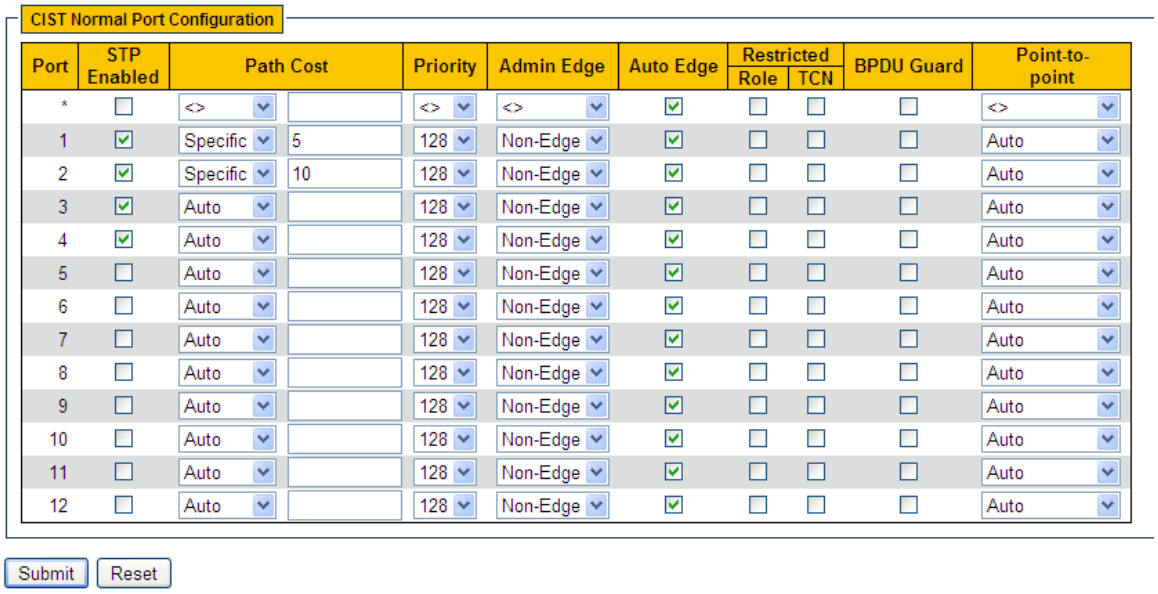


Рисунок 239 Настройка портов CIST

STP Enabled

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение или выключение STP/RSTP для порта.

Предупреждение:

- Канал портов и порт MSTP являются взаимоисключающими. Порты в канале портов нельзя настроить как порт MSTP, а порт MSTP нельзя добавить в канал портов.
- Не рекомендуется одновременно настраивать порты в изолированной группе как порты MSTP, а порты MSTP нельзя добавлять в изолированную группу.

Path Cost

Варианты: Auto/Specific (1~200000000)

По умолчанию: Auto

Описание: Стоимость пути порта используется для расчета наилучшего пути. Значение параметра зависит от полосы пропускания. Чем больше значение, тем ниже стоимость. Можно изменить роль порта, изменив значение параметра стоимости пути. Чтобы настроить значение вручную, выберите значение No для параметра Cost Count.

Priority

Диапазон: 0~240. Шаг составляет 16.

По умолчанию: 128

Функция: Настройка приоритета порта, определяющего роли портов.

Admin Edge

Варианты: Non-Edge/Edge

По умолчанию: Non-Edge

Функция: Настройка порта в режим граничного порта.

Описание: Когда порт напрямую подключен к терминалу и не подключен к другим устройствам или общему сегменту сети, этот порт считается граничным портом. Граничный порт может быстро перейти из состояния блокировки в состояние пересылки без задержки ожидания. После того как граничный порт получает пакеты BPDU, он перестает быть граничным портом.

Auto Edge

Варианты: Enable/Disable

По умолчанию: Enable

Функция: Включение функции автоматического обнаружения граничного порта.

Restricted Role

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Порт с ограничением роли никогда не будет выбран в качестве корневого узла, даже если ему предоставлен наивысший приоритет.

Restricted TCN

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Порт с ограниченным TCN не будет активно отправлять сообщения TCN.

BPDU Guard

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Режим контроля перехода граничного порта в состояние Error-Disable и закрытия при получении пакетов BPDU.

Point-to-point

Варианты: Auto/Forced True/Forced False

По умолчанию: Auto

Функция: Настройка типа соединения для порта. Если порт подключен к каналу «точка-точка», порт может быстро перейти в другое состояние.

Описание: Auto указывает, что коммутатор автоматически определяет тип канала на основе того, что порт работает в дуплексном режиме. Когда порт работает в полнодуплексном режиме, коммутатор считает, что тип соединения, подключенного к порту, — точка-точка; когда порт работает в полудуплексном режиме, коммутатор считает, что тип соединения, подключенного к порту, является общим. Принудительное задание соединения «точка-точка» означает, что соединение, подключенное к порту, является соединением «точка-точка», а принудительное задание совместного использования означает, что соединение, подключенное к порту, является общим соединением.

5. Настройте порты MSTI, как показано на рисунке 240.

Рисунок 240 Выбор MSTI

Select MSTI

Диапазон: MST1~MST7

По умолчанию: MST1

Функция: Выбор MSTI, Щелкните <Get>, чтобы перейти на станицу настройки портов MSTI, как показано на следующем рисунке.

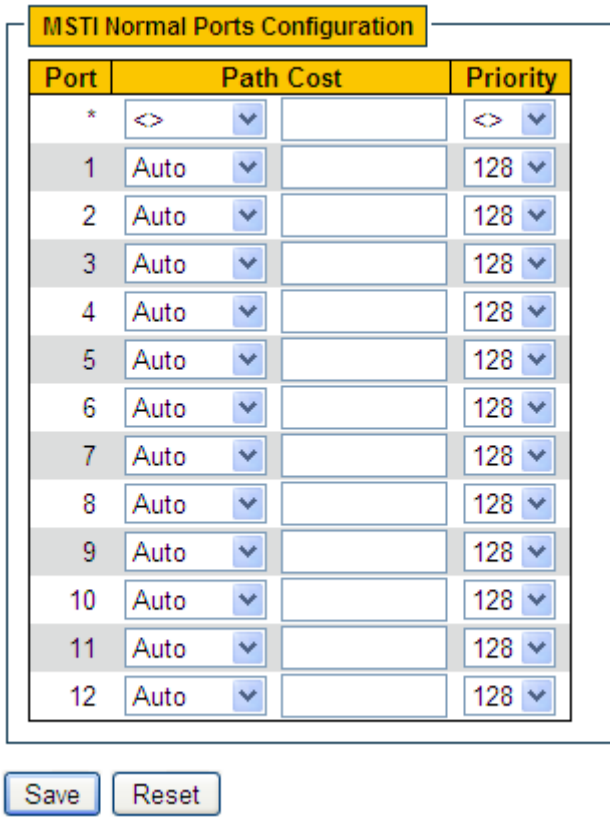


Рисунок 241 Настройка портов MSTI

Path Cost

Варианты: Auto/Specific (1~200000000)

По умолчанию: Auto

Функция: Настройка стоимости пути для порта в назначенном экземпляре.

Описание: Стоимость пути порта используется для расчета наилучшего пути. Этот параметр зависит от полосы пропускания. Чем гире полоса пропускания, тем ниже стоимость. Изменение стоимости пути порта может изменить путь передачи между устройством и корневым мостом, тем самым изменив роль порта. Устройство с поддержкой MSTP можно настроить с разными стоимостями пути в разных

экземплярах связующего дерева.

Priority

Диапазон: 0~240. Шаг составляет 16.

По умолчанию: 128

Функция: Настройка приоритета для порта в назначенном экземпляре.

Описание: Приоритет порта определяет, будет ли он выбран в качестве корневого порта. В том же состоянии в качестве корневого порта будет выбран порт с более низким приоритетом. Порты с поддержкой MSTP могут быть настроены с разными приоритетами и играть разные роли портов в разных экземплярах связующего дерева.

6. Просмотрите состояние моста, как показано на рисунке 242.

STP Bridges

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-01-C1-00-00-00	32768.00-01-C1-00-00-00	-	0	Steady	-
MSTI1	32769.00-01-C1-00-00-00	32769.00-01-C1-00-00-00	-	0	Steady	-
MSTI3	32771.00-01-C1-00-00-00	32771.00-01-C1-00-00-00	-	0	Steady	-
MSTI4	32772.00-01-C1-00-00-00	32772.00-01-C1-00-00-00	-	0	Steady	-
MSTI5	32773.00-01-C1-00-00-00	32773.00-01-C1-00-00-00	-	0	Steady	-

Рисунок 242 Просмотр состояния моста

7. Просмотрите статус портов STP, как показано на рисунке 243.

STP Port Status

Port	CIST Role	CIST State	Uptime
1	DesignatedPort	Forwarding	0d 01:03:13
2	DesignatedPort	Forwarding	0d 00:03:32
3	BackupPort	Discarding	0d 00:03:32
4	Disabled	Discarding	-
5	Non-STP	Discarding	-
6	Non-STP	Discarding	-
7	Non-STP	Discarding	-
8	Non-STP	Discarding	-
9	Non-STP	Discarding	-
10	Non-STP	Discarding	-
11	Non-STP	Discarding	-
12	Non-STP	Discarding	-

Рисунок 243 Просмотр статуса портов STP

8. Просмотрите статистику пакетов портов STP, как показано на рисунке 244.

STP Statistics

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1	1960	1180	0	0	0	0	0	0	0	0
2	164	0	0	0	3	0	0	0	0	0
3	3	0	0	0	164	0	0	0	0	0

Рисунок 244 Просмотр статистики пакетов портов STP

18.5.5 Пример типовой конфигурации

Как показано на рисунке 245, коммутаторы A, B, C и D принадлежат одному региону MST. Сети VLAN, отмеченные красным, указывают, что пакеты VLAN могут передаваться по линиям связи. После завершения настройки пакеты VLAN можно пересылать 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 — это коммутатор B. Пакеты VLAN 40 пересылаются по экземпляру 4, а корневой мост экземпляра 4 — это коммутатор C. Пакеты VLAN 20 пересылаются по экземпляру 0, а корневым мостом экземпляра 0 является коммутатор B.

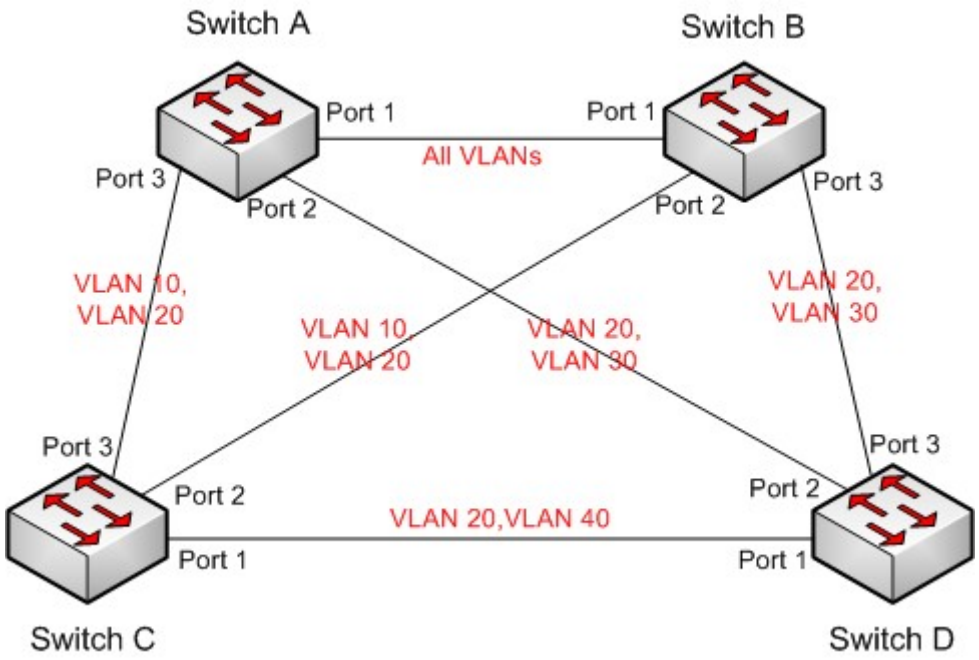


Рисунок 245 Пример типовой конфигурации

Конфигурация коммутатора A:

1. Создайте VLAN 10, 20 и 30 на коммутаторе A; настройте порты и

разрешите прохождение пакетов соответствующих VLAN.

2. Включите глобальный протокол MSTP, как показано на рисунке 236.

3. Установите имя региона MST Region, а параметр версии 0, как показано на рисунке 237.

4. Создайте MSTI 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с экземплярами 1, 3 и 4 соответственно, как показано на рисунке 237.

5. Установите приоритет моста коммутатора в MSTI 1 равным 4096 и сохраните приоритет по умолчанию в других экземплярах, как показано на рисунке 238.

Конфигурация коммутатора B:

1. Создайте VLAN 10, 20 и 30 на коммутаторе B; настройте порты и разрешите прохождение пакетов соответствующих VLAN.

2. Включите глобальный протокол MSTP, как показано на рисунке 236.

3. Установите имя региона MST Region, а параметр версии 0, как показано на рисунке 237.

4. Создайте MSTI 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с экземплярами 1, 3 и 4 соответственно, как показано на рисунке 237.

5. Установите приоритет моста коммутатора в MSTI 3 равным 4096 и сохраните приоритет по умолчанию в других экземплярах, как показано на рисунке 238.

Конфигурация коммутатора C:

1. Создайте VLAN 10, 20 и 40 на коммутаторе C; настройте порты и разрешите прохождение пакетов соответствующих VLAN.

2. Включите глобальный протокол MSTP, как показано на рисунке 236.

3. Установите имя региона MST Region, а параметр версии 0, как показано на рисунке 237.

4. Создайте MSTI 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с экземплярами 1, 3 и 4 соответственно, как показано на рисунке 237.

5. Установите приоритет моста коммутатора в MSTI 4 равным 4096 и сохраните приоритет по умолчанию в других экземплярах, как показано на рисунке 238.

Конфигурация коммутатора B:

1. . Создайте VLAN 20, 30 и 40 на коммутаторе D; настройте порты и разрешите прохождение пакетов соответствующих VLAN.

2. Включите глобальный протокол MSTP, как показано на рисунке 236.

3. Установите имя региона MST Region, а параметр версии 0, как показано на рисунке 237.

4. Создайте MSTI 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с экземплярами 1, 3 и 4 соответственно, как показано на рисунке 237.

Когда расчет MSTP завершен, MSTI каждой VLAN выглядит следующим образом:

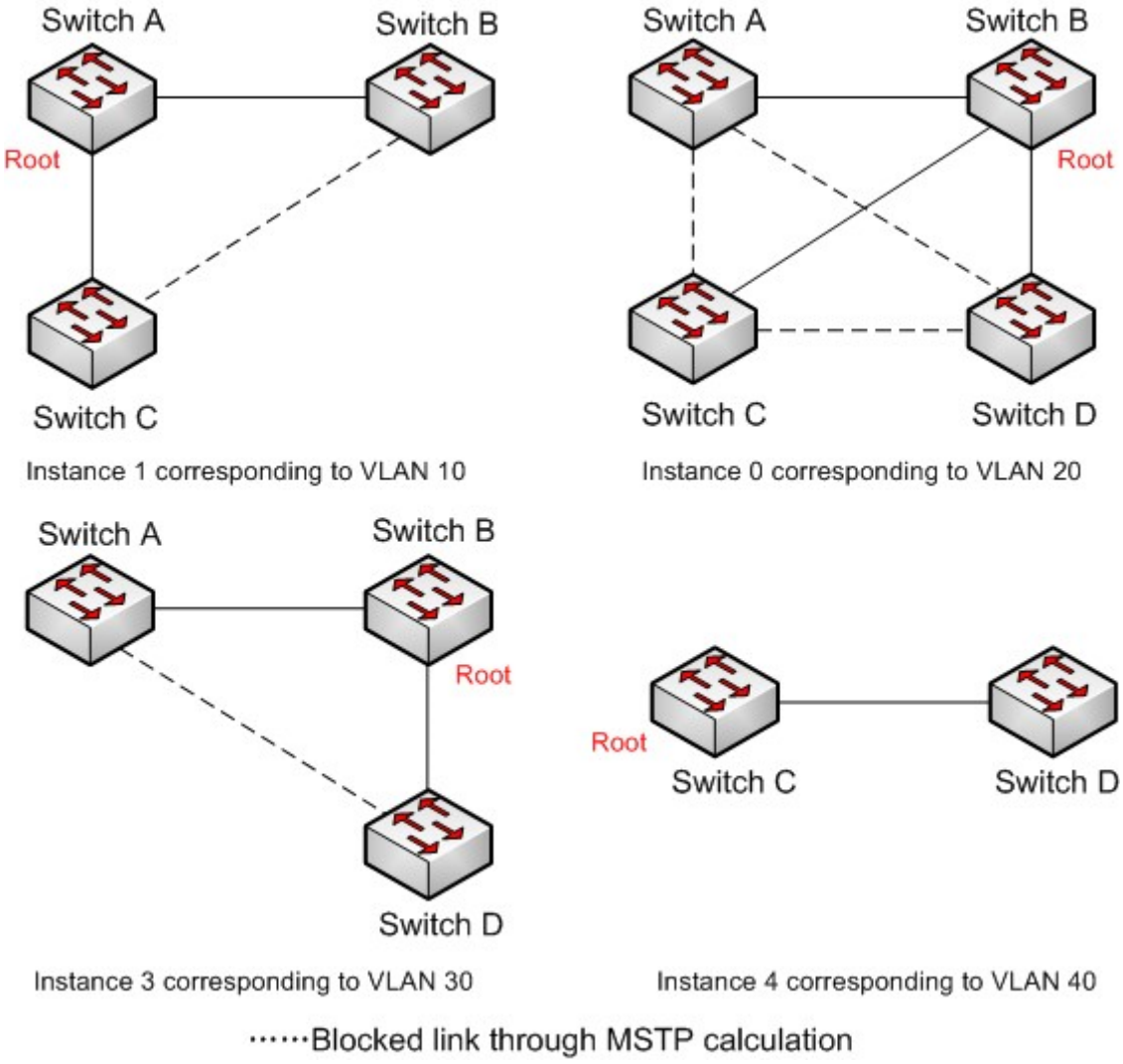


Рисунок 246 Экземпляры связующего дерева для каждой VLAN

19 Аварийная сигнализация

19.1 Введение

Коммутаторы этой серии поддерживают следующие типы аварийной сигнализации:

- Аварийная сигнализация по электропитанию: Если функция включена, то для отдельного источника питания будет генерироваться аварийный сигнал.
- Аварийная сигнализация по использованию памяти/ЦП: Если эта функция включена, аварийный сигнал генерируется, когда использование ЦП/памяти превышает указанный порог.
- Аварийная сигнализация по конфликту IP/MAC Если функция включена, то будет генерироваться аварийный сигнал при возникновении конфликта IP/MAC-адресов.
- Аварийная сигнализация по порту: Если эта функция включена, аварийный сигнал генерируется, когда порт находится в состоянии Link Down.
- Аварийная сигнализация по кольцу: Если эта функция включена, аварийный сигнал генерируется, когда кольцо разомкнуто.
- Аварийная сигнализация по CRC и потере пакетов: Если эта функция включена, аварийный сигнал генерируется, когда число ошибок CRC/потерь пакетов превышает указанный порог.
- Аварийная сигнализация по скорости порта: Если эта функция включена, аварийный сигнал генерируется, когда скорость входящего/исходящего трафика порта превышает указанный порог.
- Аварийная сигнализация по мощности SFP:

Предупреждение:

Только главное устройство станция кольца DT и корень DRP поддерживают функцию аварийной сигнализации кольца.

19.2 Настройка через веб-интерфейс

1. Настройте и отобразите аварийную сигнализацию по питанию и использованию памяти/ЦП, как показано на рисунке 247.

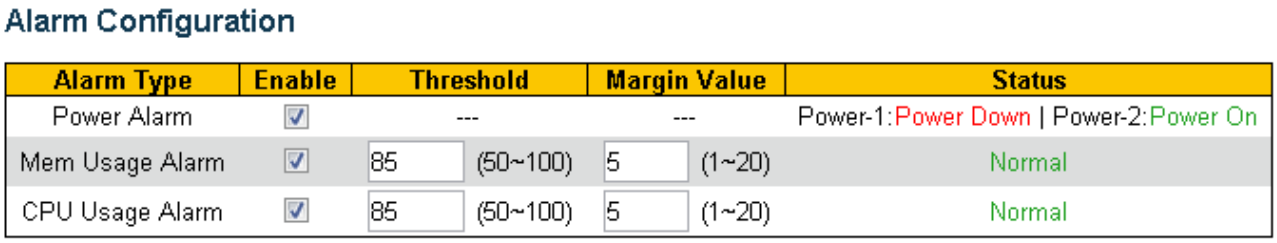


Рисунок 247 Настройка аварийной сигнализация

Power Alarm

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение аварийной сигнализации по питанию.

Status

Варианты: Power On/Power Down

Описание: Power On означает, что питание подключено и работает нормально. Power Down означает, что питание не подключено или не работает нормально.

Mem/CPU Usage Alarm

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение аварийной сигнализации по использованию памяти.

Threshold (%)

Диапазон: 50~100

По умолчанию: 85

Функция: Задание порога использования памяти/ЦП. Когда использование памяти/ЦП коммутатора превышает пороговое значение, генерируется аварийный сигнал.

Значение допуска (%)

Диапазон: 1~20

По умолчанию: 5

Функция: Задание значения допуска для порога использования памяти/ЦП.

Описание: Если использование памяти/ЦП колеблется около порогового значения,

аварийные сигналы могут генерироваться и сбрасываться неоднократно. Чтобы предотвратить это явление, можно указать значение допуска (по умолчанию 5 %). Аварийный сигнал будет сброшен только в том случае, если использование памяти/ЦП ниже порогового значения на величину допуска или более. Например, пороговое значение использования памяти равно 60 %, а значение допуска равно 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

Варианты: Normal /Alarm

Функция: Отображение состояния использования памяти/ЦП коммутатора. Alarm означает, что использование памяти/ЦП превышает пороговое значение и вызывает сигнал тревоги.

2. Настройте и отобразите аварийную сигнализацию по конфликту IP/MAC, как показано на рисунке 248.

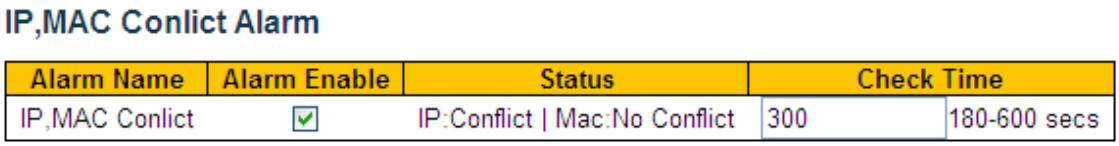


Рисунок 248 Аварийная сигнализация по конфликту IP/MAC

IP, MAC Conflict

Варианты: Enable/Disable

По умолчанию: Enable

Функция: Включение/выключение аварийной сигнализации по конфликту IP/MAC.

Status

Варианты: Conflict / No Conflict

Описание: Когда возникает конфликт IP/MAC, отображается Conflicts; в противном случае отображается No Conflicts.

Check Time

Диапазон: 180~600 с

По умолчанию: 300 с

Функция: Настройка интервала времени для обнаружения конфликтов IP/MAC.

3. Настройте и отобразите аварийную сигнализацию по кольцу DT-Ring, как показано на рисунке 249.

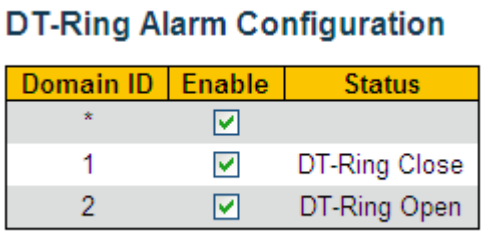


Рисунок 249 Аварийная сигнализация DT-Ring

DT-Ring Alarm Configuration

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение аварийной сигнализации DT-Ring.

Status

Варианты: DT-Ring Close / DT-Ring Open

Описание: DT-Ring Close означает, что DT-Ring замкнуто. DT-Ring Open означает, что

DT-Ring разомкнуто или находится в ненормальном состоянии.

4. Настройте и отобразите аварийную сигнализацию по кольцу DRP, как показано на рисунке 250.

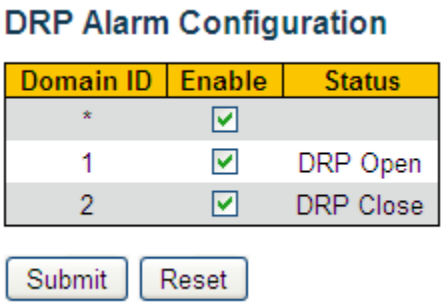


Рисунок 250 Аварийная сигнализация DRP

DRP Alarm Configuration

Варианты: Disable/Enable

По умолчанию: Disable

Функция: Включение/выключение аварийной сигнализации DRP.

Status

Варианты: DRP Close / DRP Open

Описание: DRP Close означает, что DRP замкнуто. DRP Open означает, что DRP

разомкнуто или находится в ненормальном состоянии.

5. Настройте и отобразите аварийную сигнализацию по порту, как показано на рисунке 251.

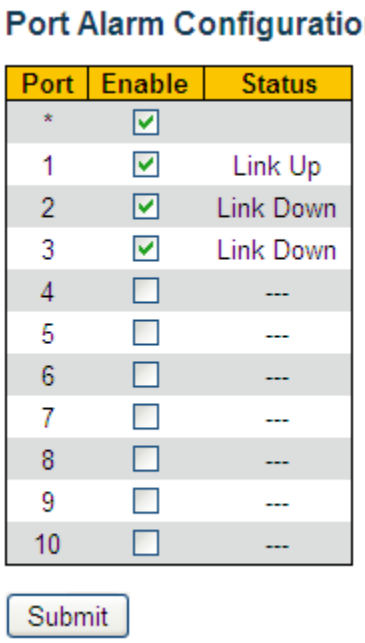


Рисунок 251 Аварийная сигнализация по порту

Port Alarm Configuration

Варианты: Disable/Enable

По умолчанию: Disable

Функция: Включение/выключение аварийной сигнализации по порту.

Status

Варианты: Link up/ Link down

Описание: Link Up означает, что порт находится в состоянии подключения и поддерживает нормальный обмен данными. Link Down означает, что порт отключен или находится в ненормальном состоянии (сбой обмена данными).

6. Настройте и отобразите аварийную сигнализацию по CRC и потере пакетов, как показано на рисунке 252.

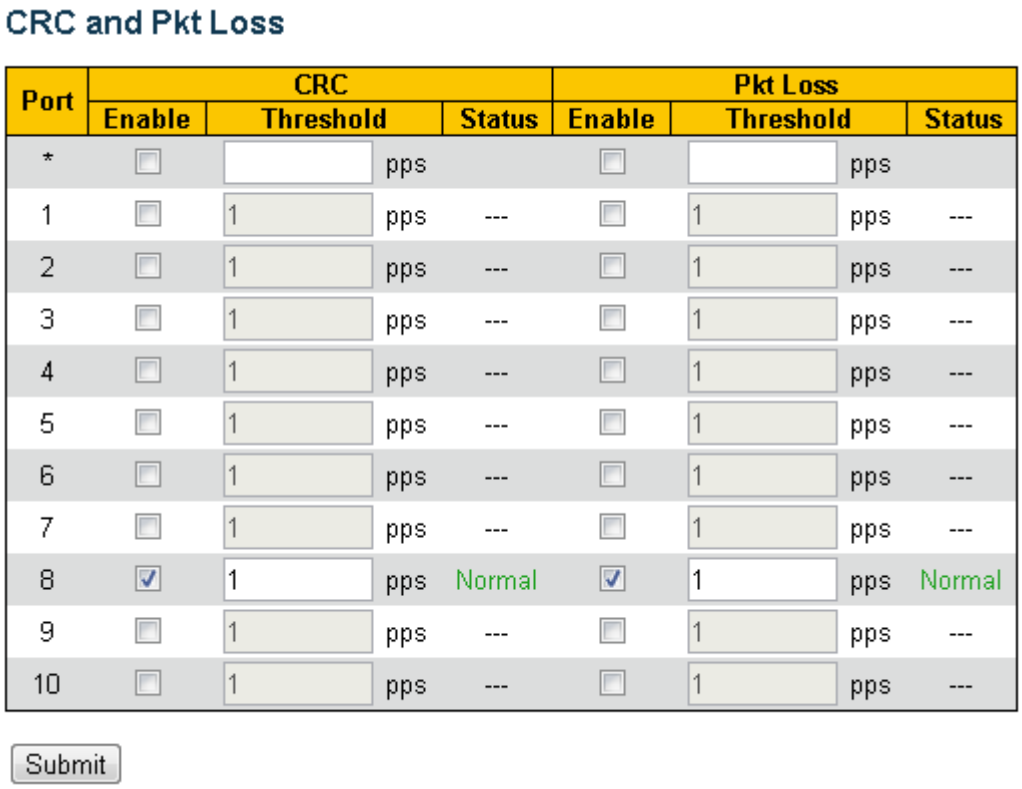


Рисунок 252 Аварийная сигнализация по CRC и потере пакетов

CRC/Pkt Loss Alarm

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение аварийной сигнализации по CRC и потере пакетов.

Threshold

Диапазон: от 1 до 1000000 pps

Функция: Задание порогового значения для аварийной сигнализации по CRC и потере пакетов для порта.

Alarm Status

Варианты: Alarm/ Normal

Функция: Просмотр состояния аварийной сигнализации по CRC и потере пакетов для порта. Alarm означает, что CRC/потеря пакетов для порта превышает пороговое значение и вызывает сигнал тревоги.

7. Настройте и отобразите аварийную сигнализацию по скорости порта, как показано на рисунке 253.

Port Rate Alarm

Port	Input Rate Alarm				Output Rate Alarm			
	Enable	Threshold	Unit	Status	Enable	Threshold	Unit	Status
*	☐		<>		☐		<>	
1	☐	1	bps	---	☐	1	bps	---
2	☐	1	bps	---	☐	1	bps	---
3	☐	1	bps	---	☐	1	bps	---
4	☐	1	bps	---	☐	1	bps	---
5	☐	1	bps	---	☐	1	bps	---
6	☐	1	bps	---	☐	1	bps	---
7	☐	1	bps	---	☐	1	bps	---
8	☐	1	bps	---	☐	1	bps	---
9	☐	1	bps	---	☐	1	bps	---
10	☐	1	bps	---	☐	1	bps	---

Submit

Рисунок 253 Аварийная сигнализация по скорости порта

Input rate alarm/output rate alarm

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение аварийной сигнализации по трафику порта.

Threshold

Диапазон: от 1 до 1000000000 bps или от 1 до 1000000 kbps.

Функция: Задание порогового значения для трафика порта.

Alarm Status

Варианты: Alarm/ Normal

Функция: Просмотр состояния трафика порта. Alarm означает, что входящий/исходящий трафик превышает пороговое значение и вызывает сигнал тревоги.

8. Настройте и отобразите аварийную сигнализацию по мощности порта RX SFP, как показано на рисунке 254.

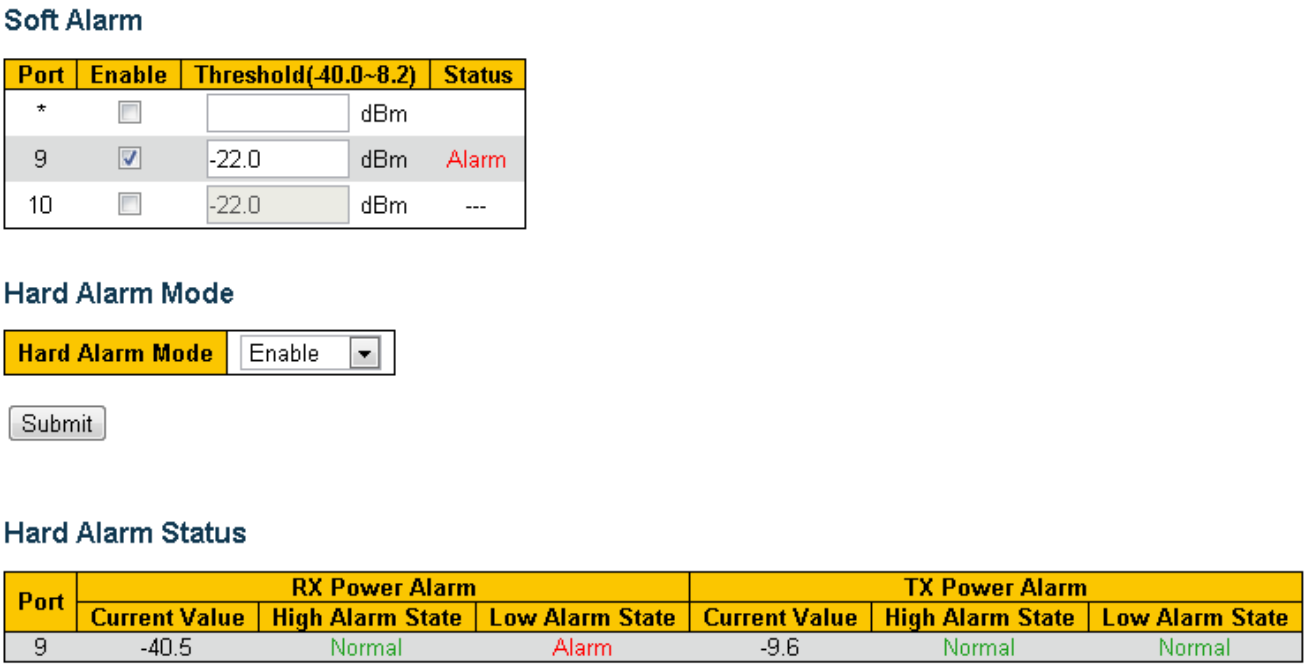


Рисунок 254 Аварийная сигнализация по мощности порта RX SFP

Software Alarm

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение аварийной сигнализации по мощности RX SFP.

Threshold

Диапазон: -40~8,2 (ед. изм: dBm)

По умолчанию: -22,0 dBm

Функция: Настройка порогового значения для аварийной сигнализации по мощности порта RX SFP.

Alarm Status

Варианты: NotSupportDDM/NotExist/Normal/Alarm

Описание: программный сигнал тревоги относится к порту, принимающему сигнал оптической мощности, и требует, чтобы SFP поддерживал функцию DDM. Если SFP не вставлен в порт, статус будет NotExist. Если SFP вставлен, но DDM не поддерживается, статус NotSupportDDM. Если вставлен SFP с поддержкой DDM, а принимаемая оптическая мощность ниже порогового значения, то будет сгенерирован сигнал тревоги, состояние Alarm. Если вставлен SFP с поддержкой DDM, а принимаемая оптическая мощность не ниже порогового значения, то состояние Normal.

Hardware Alarm

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение аппаратного аварийного сигнала мощности SFP.

Alarm Status

Варианты: Alarm/ Normal

Функция: Просмотр состояния аппаратного аварийного сигнала мощности SFP.

Поддерживает аварийный сигнал мощности SFP Tx/Rx, но пороговое значение аварийного сигнала мощности SFP Tx не настраивается.

20 Проверка канала связи

20.1 Введение

Проверка канала использует периодическое взаимодействие пакетов протокола для оценки подключения канала и отображения состояния связи порта. В случае неисправности проблема может быть обнаружена и устранена вовремя.

Порт, для которого включена проверка состояния соединения, периодически (каждую 1 с) отправляет пакеты для проверки состояния соединения. Если порт не получает пакет проверки канала от одноранговой стороны в течение времени ожидания приема (5 с), это означает, что канал неисправен, и порт отображает состояние ошибки Rx. Если порт получает пакет проверки канала от одноранговой стороны, и пакет показывает, что пакет проверки канала получен от локального узла в течение периода ожидания приема (5 с), порт отображает нормальное состояние. Если порт получает пакет проверки канала от одноранговой стороны, но пакет показывает, что пакет проверки канала не получен от локального узла в течение периода ожидания приема (5 с), порт отображает состояние ошибки Tx. Если связь с портом не работает, порт отображает состояние Link Down.

Порт, для которого отключена проверка состояния канала, работает в пассивном режиме. Это значит, что он не отправляет пакет проверки связи в активном режиме. Однако после получения пакета проверки канала от удаленного узла этот порт немедленно возвращает пакет проверки канала, чтобы проинформировать удаленный узел о том, что он получил пакет проверки канала.

20.2 Настройка через веб-интерфейс

Настройте проверку канала связи, как показано на рисунке 255.

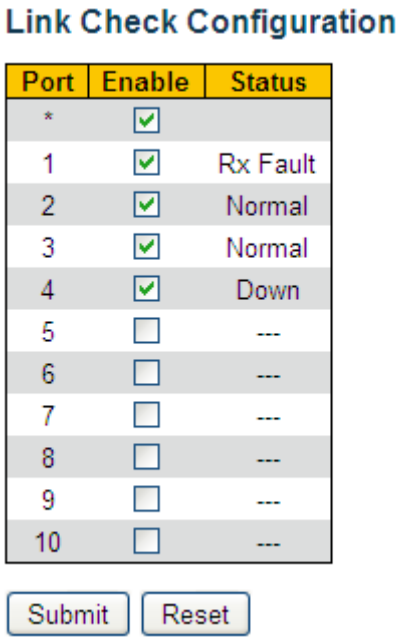


Рисунок 255 Проверка канала связи

Enable

Варианты: Disable/Enable

По умолчанию: Disable

Функция: Включение/выключение проверки канала связи для порта.

Предупреждение:

Если одноранговое устройство не поддерживает эту функцию, функция должна быть отключена на подключенном порту локального устройства.

Status

Варианты: Up/Normal/--/Rx Fault/Tx Fault/Down

Описание: Если для порта включена функция Link Check и порт нормально отправляет и принимает данные, отображается Normal. Если одноранговое устройство не получает пакеты обнаружения от устройства, отображается Tx Fault. Если устройство не получает пакеты обнаружения от однорангового устройства, отображается Rx Fault. Если порт отключен, отображается Down. Если функция Link Check не включена для порта, отображается --. В момент включения функции Link Check на подключенном порту Up.

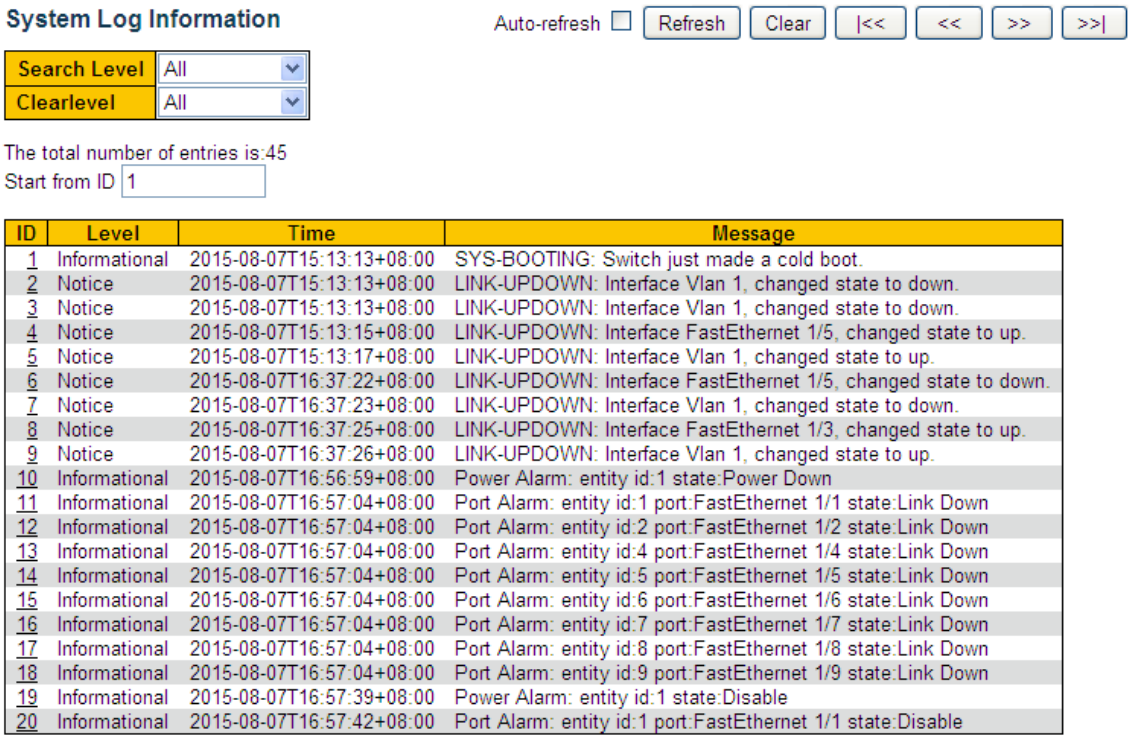
21 Журнал

21.1 Введение

Функция журнала в основном записывает состояние системы, ошибки, отладку, аномалии и другую информацию. При соответствующей настройке коммутатор может загружать журналы на сервер с поддержкой Syslog в режиме реального времени. Журнал содержит информацию о сигналах тревоги, широковещательном шторме, перезагрузке, памяти и информацию об операциях пользователей.

21.2 Настройка через веб-интерфейс

1. Настройте системный журнал, как показано на рисунке 256.



ID	Level	Time	Message
1	Informational	2015-08-07T15:13:13+08:00	SYS-BOOTING: Switch just made a cold boot.
2	Notice	2015-08-07T15:13:13+08:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
3	Notice	2015-08-07T15:13:13+08:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
4	Notice	2015-08-07T15:13:15+08:00	LINK-UPDOWN: Interface FastEthernet 1/5, changed state to up.
5	Notice	2015-08-07T15:13:17+08:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.
6	Notice	2015-08-07T16:37:22+08:00	LINK-UPDOWN: Interface FastEthernet 1/5, changed state to down.
7	Notice	2015-08-07T16:37:23+08:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
8	Notice	2015-08-07T16:37:25+08:00	LINK-UPDOWN: Interface FastEthernet 1/3, changed state to up.
9	Notice	2015-08-07T16:37:26+08:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.
10	Informational	2015-08-07T16:56:59+08:00	Power Alarm: entity id:1 state:Power Down
11	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:1 port:FastEthernet 1/1 state:Link Down
12	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:2 port:FastEthernet 1/2 state:Link Down
13	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:4 port:FastEthernet 1/4 state:Link Down
14	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:5 port:FastEthernet 1/5 state:Link Down
15	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:6 port:FastEthernet 1/6 state:Link Down
16	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:7 port:FastEthernet 1/7 state:Link Down
17	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:8 port:FastEthernet 1/8 state:Link Down
18	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:9 port:FastEthernet 1/9 state:Link Down
19	Informational	2015-08-07T16:57:39+08:00	Power Alarm: entity id:1 state:Disable
20	Informational	2015-08-07T16:57:42+08:00	Port Alarm: entity id:1 port:FastEthernet 1/1 state:Disable

Рисунок 256 Настройка системного журнала

Search Level

Варианты: Error/Warning/Notice/Information/All

По умолчанию: all

Функция: Выбор уровня отображаемой информации журнала.

Clear level

Варианты: Error/Warning/Notice/Information/All

По умолчанию: all

Функция: Выбор уровня отображаемой информации журнала для удаления. Щелкните <Clear>, чтобы удалить информацию выбранного уровня журнала.

The total number

Функция: **Отображает количество журналов, соответствующих условиям запроса.**

Start from ID

Функция: установить начальный идентификатор записей журнала на текущей странице. Можно щелкнуть <Refresh>, чтобы обновить записи журнала на текущей странице. На каждой странице может отображаться 20 записей журнала.

Щелкните [>>] , чтобы просмотреть записи журнала на следующей странице. Идентификатор начала следующей страницы — это идентификатор последней записи журнала на текущей странице.

Щелкните [<<] , чтобы просмотреть записи журнала на предыдущей странице.

Щелкните [>>|] , чтобы просмотреть записи журнала на последней странице. Конечный идентификатор — это идентификатор последней записи журнала.

Щелкните [|<<] , чтобы просмотреть записи журнала на первой странице. Начальный идентификатор — это идентификатор первой записи журнала.

2. Выгрузите журнал на сервер в реальном времени, как показано на рисунке 257.

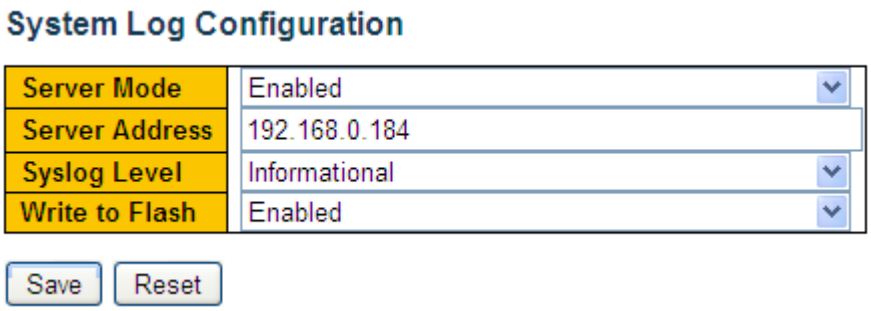


Рисунок 257 Выгрузка журнала в реальном времени

Server Mode

Варианты: Disable/Enable

По умолчанию: Disable

Функция: Включение/выключение функции выгрузки журнала на сервер в реальном времени.

Server Address

Функция: Настройка IP-адреса сервера для выгрузки информации журнала.

Syslog Level

Варианты: Error/Warning/Notice/Information

Default: Information

Функция: Выбор уровня информации журнала для выгрузки на сервер.

Write to Flash

Варианты: Enabled/Disabled

По умолчанию: Disabled

Функция: включение/выключение записи журнала во флэш-память

Можно 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 258.

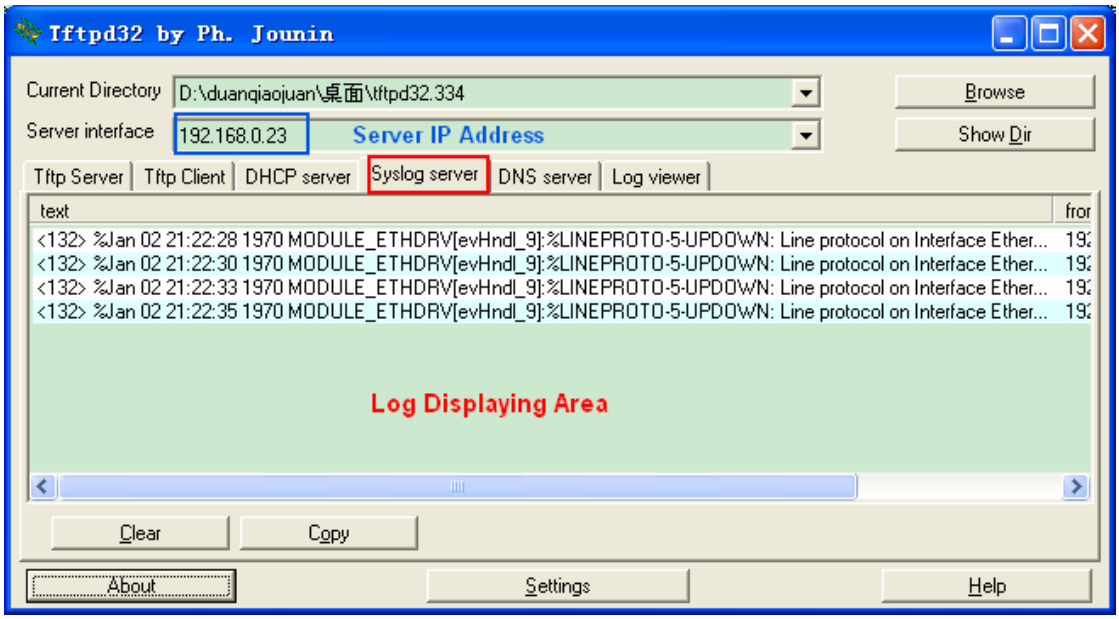


Рисунок 258 Выгрузка информации журнала в реальном времени

22 Зеркалирование портов

22.1 Введение

С функцией зеркалирования портов коммутатор копирует все полученные или переданные кадры данных в одном порту (исходный порт зеркалирования) на другой порт (порт назначения зеркалирования). Порт назначения зеркалирования подключается к анализатору протокола или монитору RMON для мониторинга сети, управления и диагностики неисправностей.

22.2 Пояснения

Коммутатор поддерживает только один порт назначения 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.

Предупреждение:

Динамическое изучение MAC-адресов должно быть отключено на порту назначения.

22.3 Настройка через веб-интерфейс

1. Настройте функцию зеркалирования порта, как показано на рисунке 259.

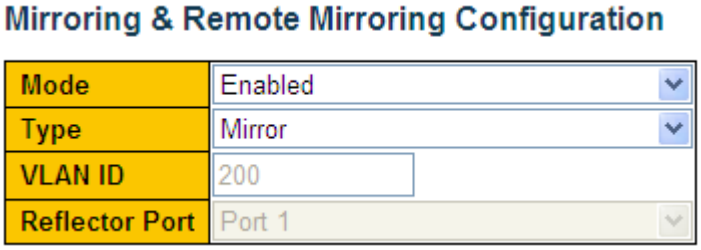


Рисунок 259 Настройка функции зеркалирования порта.

Mode

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение функции зеркалирования портов.

Type

Варианты: Mirror

Функция: Использовать функцию зеркалирования портов.

2. Выберите порт назначения зеркалирования и исходный порт, как показано на рисунке 260.

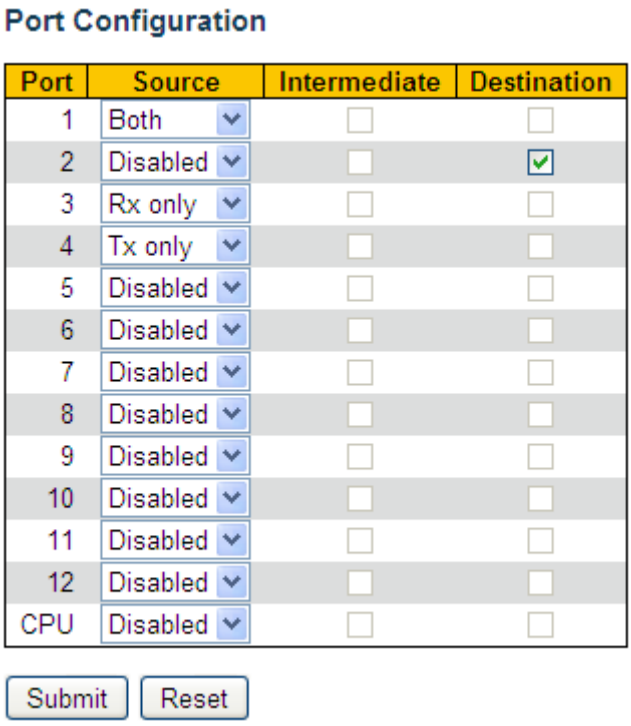


Рисунок 260 Выбор порта назначения зеркалирования и исходный порта

Source

Варианты: Rx only/Tx only /Both

Функция: Выбор данных для зеркалирования в исходном порту зеркалирования.

Rx only: указывает, что в исходном порту зеркалируются только

полученные пакеты. Tx only: указывает, что в исходном порту

зеркалируются только отправленные пакеты.

Both: указывает, что в исходном порту зеркалируются полученные и отправленные пакеты.

Destination

Функция: Выбор порта, который будет портом назначения зеркалирования.

Существует один и только один порт назначения зеркалирования.

22.4 Пример типовой конфигурации

Как показано на рисунке 261, порт назначения зеркалирования — это порт 2, а

исходный порт источника зеркалирования — порт 1. Как переданные, так и полученные пакеты порта 1 зеркалируются на порт 2.

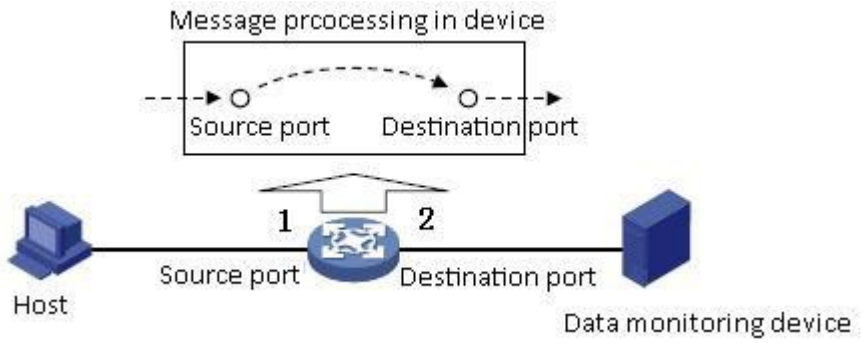


Рисунок 261 Пример зеркалирования порта

Процесс настройки:

1. Включите функцию зеркалирования порта, как показано на рисунке 259.

2. Установите порт 2 в качестве порта назначения зеркалирования , порт 1 в качестве исходного порта зеркалирования и режим зеркального отображения Both, как показано на рисунке 260.

23 Диагностика

23.1 Ping

Пользователи могут запустить команду ping, чтобы проверить, доступно ли устройство с указанным адресом и не повреждено ли сетевое подключение во время планового обслуживания системы.

1. Настройте команду ping, как показано на рисунке 262.

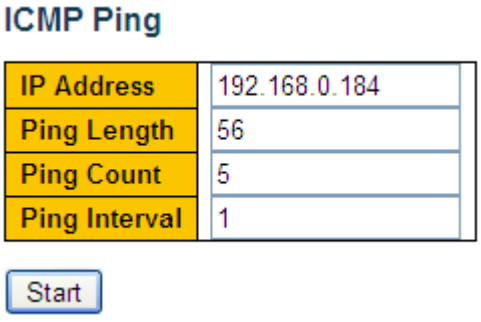


Рисунок 262 Настройка команды ping

IP Address

Формат: A.B.C.D

Описание: Ввод IP-адреса устройства назначения.

Ping Length

Диапазон: 2~1452 байт

По умолчанию: 56 байт

Функция: Указание длины запроса ICMP (исключая заголовок IP и ICMP-пакета) для передачи.

Ping Count

Диапазон: 1~60

По умолчанию: 5

Функция: Задание количества раз отправки ICMP-запроса.

Ping Interval

Диапазон: 0~30 с

По умолчанию: 1 с

Функция: Задание интервала отправки ICMP-запроса.

2. Просмотрите результаты ping, как показано на рисунке 263.

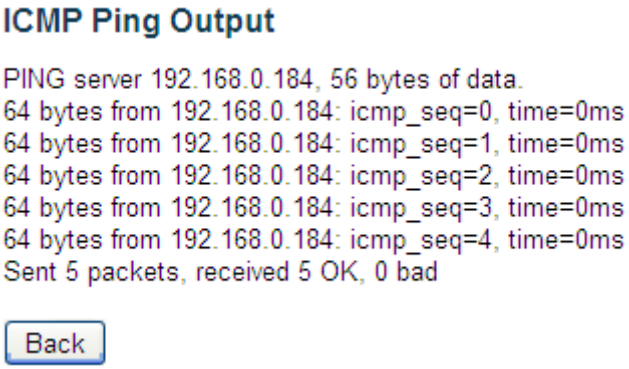


Рисунок 263 Просмотр результатов ping

Результаты команды ping включают в себя ответ целевого устройства на каждый пакет запроса ICMP и статистику пакетов, собранную во время выполнения команды ping.

Приложение: Аббревиатуры

Аббревиатура	Полное написание
ACE	Access Control Entry
ACL	Access Control List
ARP	Address Resolution Protocol
BootP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
CIST	Common and Internal Spanning Tree
CLI	Command Line Interface
CoS	Class of Service
CST	Common Spanning Tree
DHCP	Dynamic Host Configuration Protocol
DHP	Dual Homing Protocol
DNS	Domain Name System
DRP	Distributed Redundancy Protocol
DSCP	Differentiated Services CodePoint
DST	Daylight Saving Time
EAPOL	Extensible Authentication Protocol over LAN
GARP	Generic Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
GVRP	GARP VLAN Registration Protocol
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IGMP Snooping	Internet Group Management Protocol Snooping
IST	Internal Spanning Tree
LACP	Link Aggregation Control Protocol
LACPDU	Link Aggregation Control Protocol Data Unit

LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit
MIB	Management Information Base
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
NAS	Network Access Server
NetBIOS	Network Basic Input/Output System
NMS	Network Management Station
NTP	Network Time Protocol
OID	Object Identifier
PCP	Priority Code Point
PD	Powered Device
POE	Power Over Ethernet
PSE	Power Sourcing Equipment
PVLAN	Private VLAN
QCL	QoS Control List
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RMON	Remote Network Monitoring
RSTP	Rapid Spanning Tree Protocol
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SP	Strict Priority
SSH	Secure Shell
SSL	Secure Sockets Layer
SSM	Source Specific Multicast
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System

TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USM	User-Based Security Model
VLAN	Virtual Local Area Network
WINS	Windows Internet Naming Service
WRR	Weighted Round Robin

Контакты

Для получения технической поддержки пишите на наш адрес электронной почты: support@kyland-rus.ru
Офис продаж: sales@kyland-rus.ru

Для получения информации об оборудовании, документации, актуальной информации обращайтесь на сайт: https://kyland-rus.ru/