Промышленный управляемый гигабитный PoE-коммутатор

ComOnyx CO-PF-8GP8SFP-P510

Руководство пользователя

Промышленный управляемый PoE-коммутатор предназначен для коммутации IP-устройств по проводной сети. Коммутатор оснащен восемью гигабитными LAN-портами с поддержкой питания PoE-устройств и восьмью оптическими SFP-портами. Исполнение в металлическом корпусе классом защиты IP40 с креплением на DIN-рейку. Питание от источника постоянного тока DC48-57В, с возможностью резервного питания.

Оглавление

1.1 Обзор

Благодарим за покупку нашей серии управляемых коммутаторов, всеми функциями программного обеспечения которого можно управлять, настраивать и контролировать через встроенный веб-интерфейс (HTML). С помощью стандартного браузера вы можете управлять коммутатором через любой удаленный сайт в сети. Браузер как универсальный инструмент доступа, использует протокол HTTP для связи с коммутатором напрямую.

1.2 Вход в веб-управление

Откройте установленный веб-браузер на вашем ПК, введите IP-адрес коммутатора, например http://xxx.xxx.xxx.xxx, затем откройте URL для входа в веб-управление.

Примечание. По умолчанию IP-адрес коммутатора - 192.168.2.1. Поэтому, пожалуйста, введите http://192.168.2.1 в браузере.

Когда появится окно входа в систему, введите имя пользователя - по умолчанию «admin» с паролем «system». Затем нажмите OK, чтобы войти.

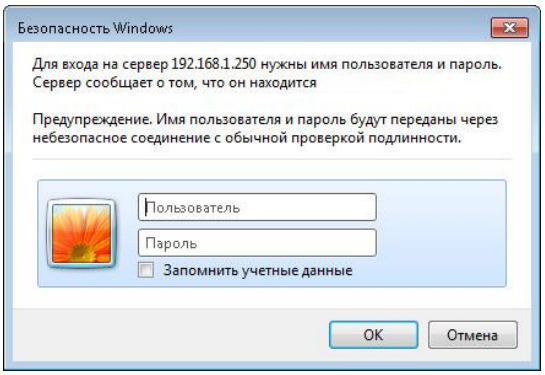


Рисунок 1-1 Окно входа в систему

1.3 Веб-интерфейс пользователя

После ввода имени пользователя и пароля появится главный экран, как показано на рисунке 1-2.

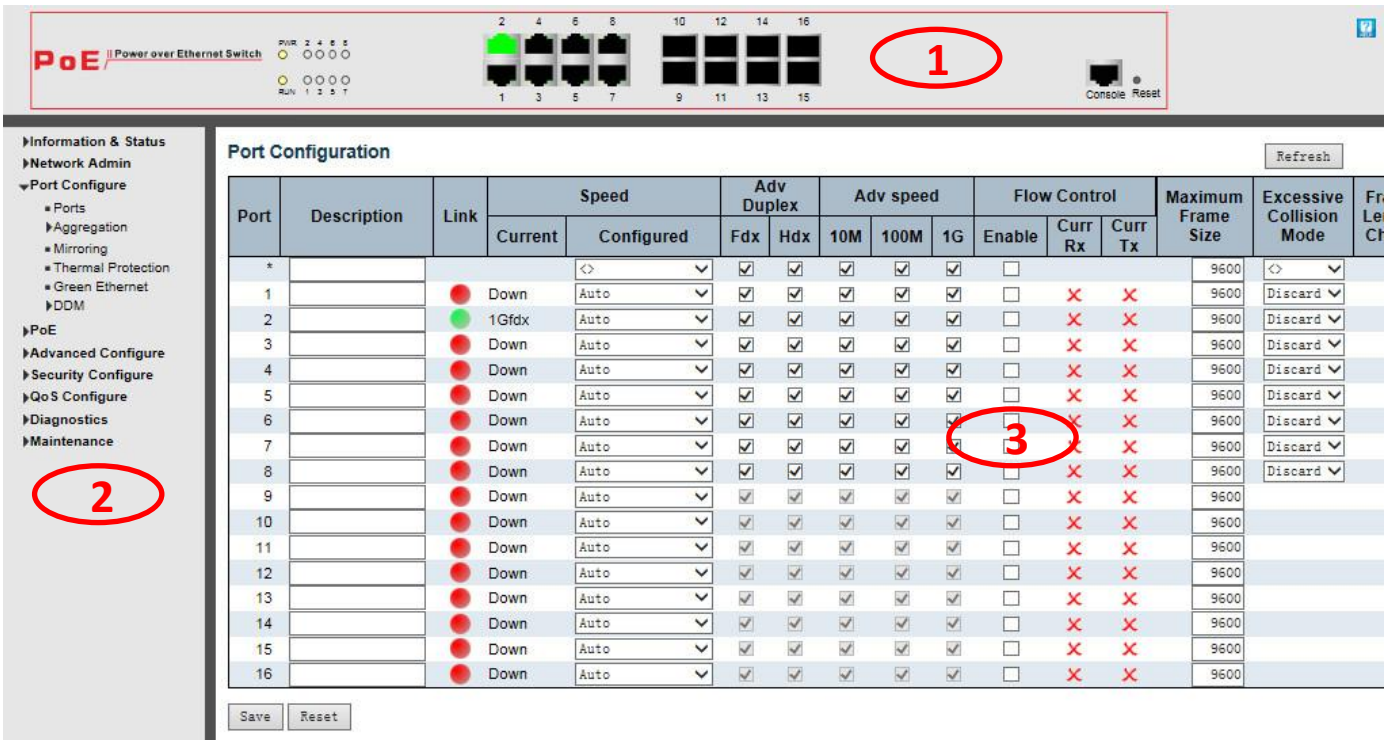


Рисунок 1-2 Интерфейс главной страницы веб-управления

Этот интерфейс главной страницы состоит в основном из 3 частей. Вот описание:

1. Панель дисплея; Индикаторы портов, включая PoE и рабочее состояние Link; Кнопка выбора языка; Help .
2. Главное меню, позволяет получить доступ ко всем командам и статистике.
3. Главный экран, показывающий детали конфигурации.

Веб-агент отображает изображение портов управляемого коммутатора. Разные цвета означают разные состояния, они иллюстрируются следующим образом:

100Mbps соединение 1000Mbps соединение нет соединения

Основное меню

Используя встроенный веб-агент, вы можете определять системные параметры, управлять и контролировать управляемый коммутатор и все его порты, или контролировать состояние сети. С помощью веб-управления администратор может настроить управляемый коммутатор, выбрав функции, перечисленные в главном меню. Ниже приводится краткое описание:

Information & Status (Информация и статус) - пользователи могут проверить информацию о коммутаторе и рабочее состояние в этом меню.
Network Admin (Администратор сети) - пользователи могут проверить и настроить связанные функции сети в этом меню.
Port Configure (Настройка портов) - пользователи могут проверить и настроить спецификации портов в этом меню.
PoE - пользователи могут проверять и настраивать связанные функции Power-over-Ethernet (PoE) в этом меню.
Advanced Configure (Расширенные настройки) - пользователи могут проверить и настроить расширенные функции L2 в этом меню.
Security Configure (Настройка безопасности) - пользователи могут проверить и настроить функции безопасности коммутатора в соответствии с этим меню.

QoS Configure - пользователи могут проверять и настраивать функции QoS коммутатора в этом меню.

2. Управление сетью
2.1 Конфигурация IP

Примечание. По умолчанию IP-адрес коммутатора составляет 192.168.2.1, а маска подсети по умолчанию - 255.255.255.0 (24).

Нажмите "Network Admin">"IP config", на экране отобразится следующее:

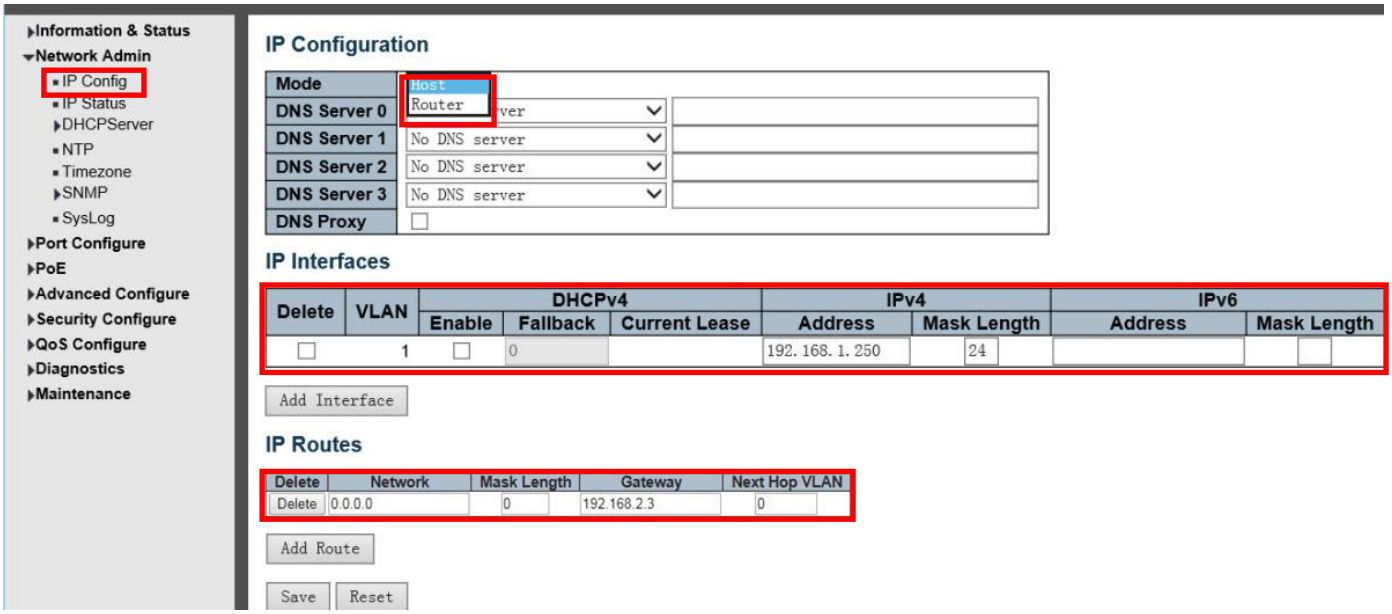


Рисунок 2-1 Экран конфигурации IP

Ниже приведено подробное описание конфигурации IP:

Port Name	Отображение имени порта системы
VLAN	VLAN для доступа и управления коммутатором
IPv4 DHCP	Если включено, это означает, что порт VLAN запускает IPv4 DHCP-клиента, чтобы динамически получать IPv4-адреса коммутатора. В противном случае он будет использовать статическую IP-конфигурацию коммутатора. Откат (в секундах) означает время ожидания переключения для получения динамического IP-адреса через DHCP. Значение «0» здесь означает, что никогда со временем. Текущий лизинг, означает, что IP-адрес получить от DHCP
IPv4	Address: статический IPv4-адрес, введенный пользователем. Mask Length(Длина маски): статическая маска IPv4, введенная пользователем.
IPv6	IP-адрес, пользователи могут вводить статический IPv6-адрес. IP Mask(IP-маска), пользователи могут вводить статическую маску IPv6-подсети.
IP Routes	Назначение, пользователи могут вводить IPv4-адрес назначения IP Mask(IP-маска), пользователи могут использовать статическую маску подсети IPv4 Next address, Следующий адрес, пользователи могут вводить следующий адрес IPv4

Нажмите "Add Interface" «Добавить интерфейс», чтобы создать новое управление для VLAN и IP-адреса. Нажмите «Сохранить», чтобы сохранить настройки.

Примечание. По умолчанию коммутатор создал только VLAN1. Если пользователю нужно использовать другую VLAN для управления коммутатором, сначала добавьте VLAN в модуль VLAN и добавьте соответствующий порт в VLAN.

Нажмите «Save», чтобы сохранить Ваши настройки.

2.2 IP статус

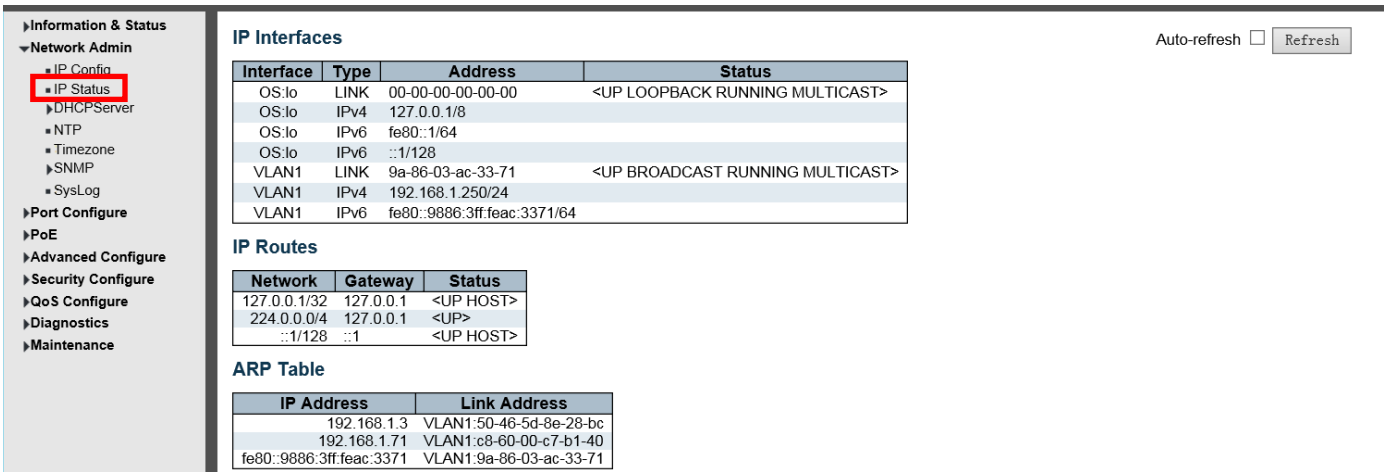


Рисунок 2-2 IP статус

На этой странице отображается состояние протокола IP. Статус определяется IP-интерфейсами, IP-маршрутами и состоянием соседнего кэша (ARP-кэша).

2.3 DHCP сервер
2.3.1 Mode Настройка режима DHCP-сервера

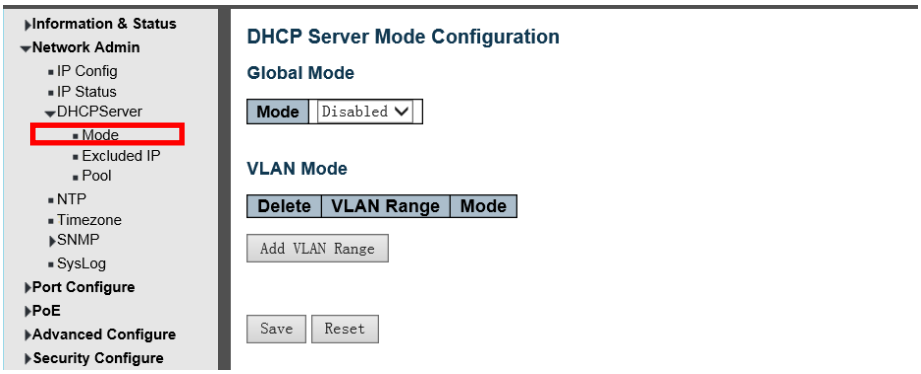


Рисунок 2-3-1 Настройка режима DHCP-сервера

На этой странице настраивается глобальный режим и режим VLAN для включения / отключения DHCP-сервера для системы и VLAN.

Глобальный режим
Настройте режим работы для включения / отключения DHCP-сервера для каждой системы.
Режим Настройте режим работы для каждой системы. Возможные режимы:
Включено: Включить DHCP-сервер для каждой системы.
Отключено: Отключить предварительную систему DHCP-сервера.

Режим VLAN
Настройте режим работы, чтобы включить / отключить DHCP-сервер для каждой VLAN.
Диапазон VLAN Укажите диапазон VLAN, в котором DHCP-сервер включен или отключен. Первый идентификатор VLAN должен быть меньше или равен второму идентификатору VLAN. НО, если диапазон VLAN содержит только 1 идентификатор VLAN, вы можете просто ввести его в один из первого и второго идентификатора VLAN или в оба.
С другой стороны, если вы хотите отключить существующий диапазон VLAN, вы можете выполнить следующие действия.
1. нажмите, чтобы добавить новый диапазон VLAN.
2. введите диапазон VLAN, который вы хотите отключить.
3. выберите режим для отключения.
4. нажмите, чтобы применить изменения.

Затем вы увидите, что отключенный диапазон VLAN удаляется со страницы конфигурации режима DHCP-сервера.

Режим Укажите режим работы для каждой VLAN. Возможные режимы:
Включено: Включить DHCP-сервер для каждой VLAN.
Отключено: отключить DHCP-сервер предварительно VLAN.
Нажмите «Save», чтобы сохранить Ваши настройки.

2.3.2 Excluded IP (Исключение IP-адресов для DHCP-сервера)

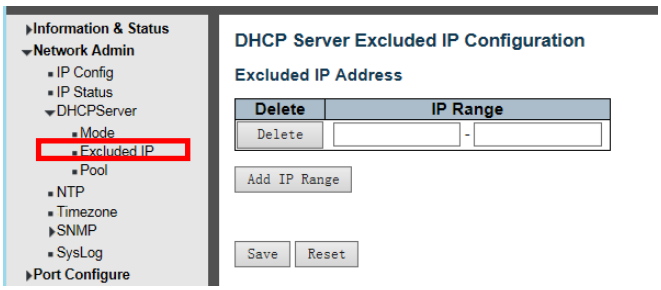


Рисунок 2-3-2 Экран конфигурации исключения IP-адресов для DHCP

На этой странице настраиваются исключенные IP-адреса. DHCP-сервер не будет выделять эти исключенные IP-адреса DHCP-клиенту.

Исключенный IP-адрес
Настройте исключенные IP-адреса.

IP Range(Диапазон IP-адресов) Определите диапазон IP-адресов, которые должны быть исключены. Первый исключенный IP-адрес должен быть меньше или равен второму исключенному IP-адресу. НО, если диапазон IP-адресов содержит только 1 исключенный IP-адрес, вы можете просто ввести его.
Нажмите «Save», чтобы сохранить Ваши настройки.

2.3.3 Pool (Конфигурация пула серверов DHCP)

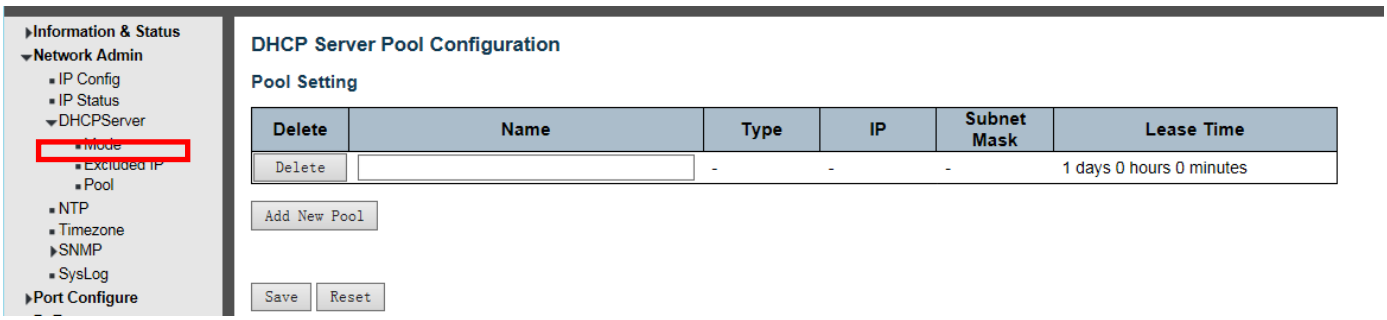


Рисунок 2-3-3Экран конфигурации пула серверов DHCP

Эта страница управляет пулами DHCP. В соответствии с пулом DHCP, DHCP-сервер будет выделять IP-адрес и передавать параметры конфигурации DHCP-клиенту.

Настройка пула

Добавить или удалить пулы.

Добавление пула и присвоение имени - это создание нового пула с конфигурацией «Default». Если вы хотите настроить все параметры, включая тип, маску IP-подсети и время аренды, вы можете щелкнуть имя пула, чтобы перейти на страницу конфигурации.
Name (Имя) Настройте имя пула, которое принимает все печатаемые символы, кроме пробелов. Если вы хотите настроить подробные параметры, вы можете щелкнуть имя пула, чтобы перейти на страницу конфигурации.
Type (Тип) Отображение типа пула.
Network(Сеть): пул определяет пул IP-адресов для обслуживания более одного DHCP-клиента.
Host(Хост): пул услуг для конкретного клиента DHCP, идентифицируемого по идентификатору клиента или аппаратному адресу.

Если отображается «-», это означает, что не определено. IPDisplay номер сети пула адресов DHCP.
Если отображается «-», это означает, что не определено. Subnet MaskDisplay маска подсети пула адресов DHCP.
Если отображается «-», это означает, что не определено. Lease TimeDisplay время аренды пула.

IP: Отображение номера сети пула адресов DHCP. Если отображается «-», это означает, что не определено.
Subnet Mask (Маска подсети): Отображение маски подсети пула адресов DHCP. Если отображается «-», это означает, что не определено.
Lease Time (Время аренды): Отображение времени аренды пула. Если отображается «-», это означает, что не определено.
Нажмите «Save», чтобы сохранить Ваши настройки.

2.4 конфигурация NTP

NTP является аббревиатурой от Simple Network Time Protocol, сетевого протокола для синхронизации часов компьютерных систем. Вы можете указать NTP-серверы и установить часовой пояс GMT. Экраны конфигурации NTP будут появляются после нажатия «Network Admin» (Сетевой администратор)> «NTP».

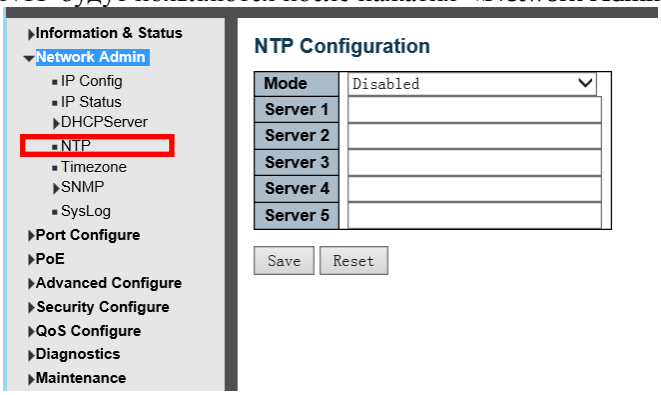


Рисунок 2-4 Экран настройки NTP

Конфигурация объекта и описание:
Mode(Режим)**:** Указывает на работу в режиме NTP. Возможные режимы:
Включено: Включить работу в режиме клиента NTP.
Отключено: отключить работу в режиме клиента NTP.
Сервер # Укажите IPv4 или IPv6-адрес NTP-сервера. Адрес IPv6 содержится в 128-битных записях, представленных в виде восьми полей длиной до четырех шестнадцатеричных цифр с двоеточием, разделяющим каждое поле (:). Например, 'fe80 :: 215: c5ff: fe03: 4dc7'. Символ «::» - это специальный синтаксис, который можно использовать как сокращенный способ представления нескольких 16-битных групп непрерывных нулей; но это может появиться только один раз. Он также может представлять юридически действительный адрес IPv4. Например, ':: 192.1.2.34'. Кроме того, он также может принять адрес доменного имени.
Нажмите «Save», чтобы сохранить Ваши настройки.

2.5 Timezone (Часовой пояс)

Timezone (Часовой пояс), чтобы установить время переключения, пользователи могут установить время в соответствии с их местоположением. Вы можете попасть в часовой пояс через нажатия «Network Admin» (Сетевой администратор)> «**Timezone**», как показано на рисунке 2-5

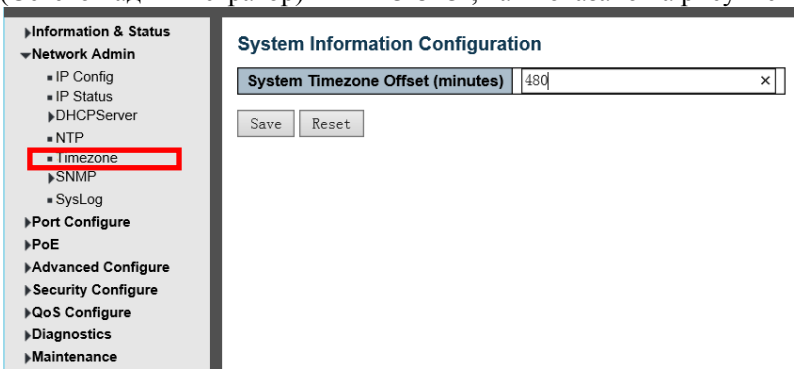


Рисунок 2-5 Настройка часового пояса

Нажмите «Save», чтобы сохранить Ваши настройки.

2.6 Конфигурация SNMP

Simple Network Management Protocol (SNMP) - это протокол прикладного уровня, который облегчает обмен информацией управления между сетевыми устройствами. Это часть протокола Transmission Control Protocol/Internet Protocol (TCP/IP). SNMP позволяет сетевым администраторам управлять производительностью сети, найти и решить проблемы с сетью, и планировать рост сети.

Этот коммутатор поддерживает SNMPv1, v2c, v3. Различные версии SNMP обеспечивают разный уровень безопасности для станций управления и сетевых устройств.
В SNMP v1 и v2c для аутентификации пользователей используется "Community String" («Строка сообщества»). Эта строка похожа на функцию пароля. Приложение SNMP удаленного пользователя и SNMP коммутатора должны использовать одну и ту же строку сообщества.
Пакеты SNMP любых неавторизованных сайтов будут игнорироваться (отбрасываться).

«Строка сообщества» по умолчанию для управления доступом коммутатора SNMPv1 и v2c:

1. public - разрешить станции управления аутентификацией считывать объекты MIB.
2. private - разрешить станции управления аутентификацией считывать, записывать и редактировать объекты MIB.

Trap (ловушка)
Используется агентом для асинхронного информирования NMS о каком-либо событии. Эти события могут быть очень серьезными, такими как перезагрузка (кто-то случайно выключил коммутатор) или просто общая информация, такая как изменение статуса порта.
В этом случае переключите созданую ловушкой информацию и затем отправьте получателю или администратору сети. Типичная ловушка включает: ошибки аутентификации, сетевые изменения и ловушка холодного / горячего запуска.

MIB
MIB - это коллекция управляемых объектов, находящихся в виртуальном хранилище информации. Коллекции связанных управляемых объектов определены в определенных модулях MIB. Коммутатор использует стандартный модуль управления информацией MIB-II. Так, значение объекта MIB может быть прочитано любым программным обеспечением SNMP, управляемым через Интернет.

2.6.1 SNMP System Configuration (Конфигурация системы SNMP)

Вы можете включить или отключить Конфигурация системы SNMP. Его экран появится после нажатия кнопки нажатия «Network Admin» (Сетевой администратор)>" SNMP ">" System"

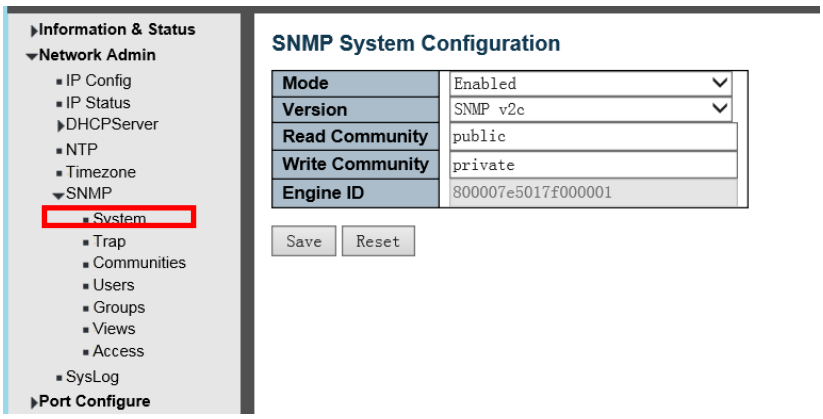


Рисунок 2-6-1 Экран настройки системы SNMP

Mode(Режим) Указывает на работу в режиме SNMP. Возможные режимы:
Enabled (Включено): Включить работу в режиме SNMP.
Disabled (Отключено): отключение режима SNMP.
Version(Версия) Указывает поддерживаемую версию SNMP. Возможные версии:
SNMP v1: установите поддерживаемую SNMP версию 1.
SNMP v2c: установите поддерживаемую SNMP версию 2c.
SNMP v3: установите поддерживаемую SNMP версию 3.
Read Community. (Сообщество чтения). Указывает строку доступа для чтения сообщества, чтобы разрешить доступ к агенту SNMP. Допустимая длина строки - от 0 до 255, а допустимым содержимым являются символы ASCII от 33 до 126. Поле применимо, только если версия SNMP - это SNMPv1 или SNMPv2c. Если версия SNMP - SNMPv3, строка сообщества будет связана с таблицей сообществ SNMPv3. Он обеспечивает большую гибкость настройки имени безопасности, чем строка сообщества SNMPv1 или SNMPv2c. В дополнение к строке сообщества, определенный диапазон адресов источника может использоваться для ограничения подсети источника.
Write Community (Сообщество записи). Указывает строку доступа для записи сообщества, чтобы разрешить доступ к агенту SNMP. Допустимая длина строки - от 0 до 255, а допустимым содержимым являются символы ASCII от 33 до 126. Поле применимо, только если версия SNMP - это SNMPv1 или SNMPv2c. Если версия SNMP - SNMPv3, строка сообщества будет связана с таблицей сообществ SNMPv3. Он обеспечивает большую гибкость настройки имени безопасности, чем строка сообщества SNMPv1 или SNMPv2c. В дополнение к строке сообщества, определенный диапазон адресов источника может использоваться для ограничения подсети источника.
Engine ID. Указывает идентификатор для механизма SNMPv3. Строка должна содержать четное число (в шестнадцатеричном формате) с количеством цифр от 10 до 64, но все нули и все -F не допускаются. Изменение идентификатора двигателя очистит всех оригинальных локальных пользователей.
Нажмите «Save», чтобы сохранить Ваши настройки.

2.6.2 Конфигурация SMNP Trap (SMNP ловушка)

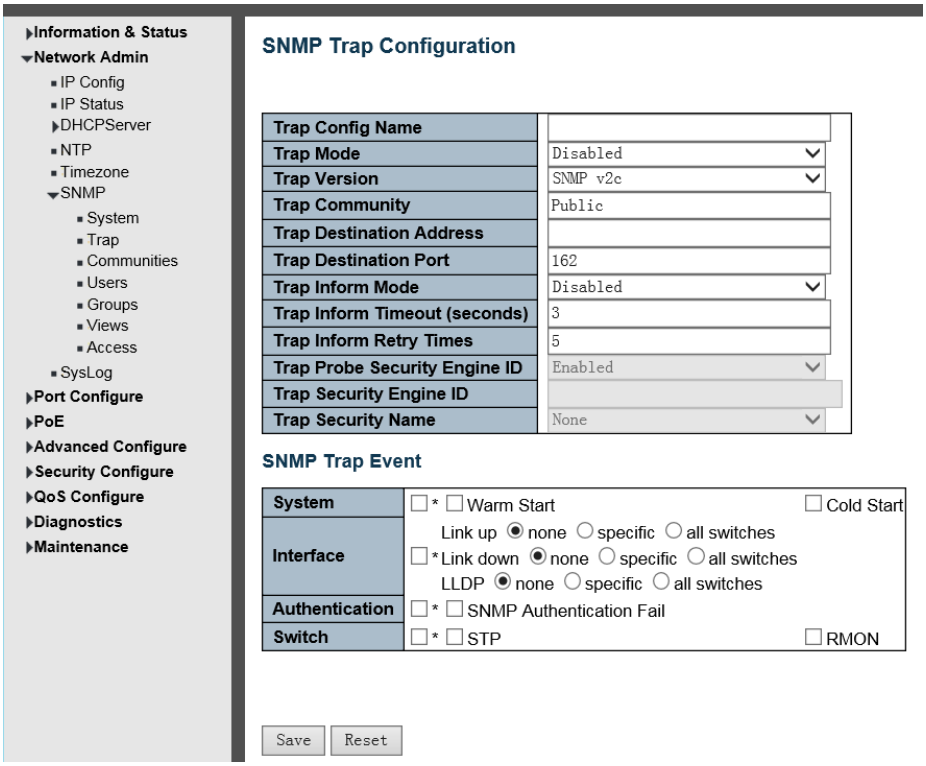


Рисунок 2-6-2

Нажмите «Save», чтобы сохранить Ваши настройки.

2.6.3 Communities Сообщества

Пользователи могут установить имя нового сообщества через «Network Admin» (Сетевой администратор)>" SNMP "> “Communities”, (Сообщества), как показано на рисунке ниже.

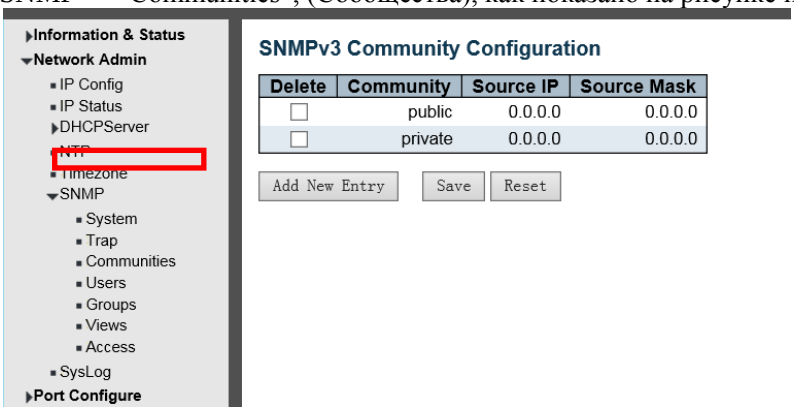


Рисунок 2-6-3 Добавление сообщества

Delete (Удалить) Проверьте для удаления записи. Она будет удалена во время следующего сохранения.
Community(Сообщество) Указывает строку доступа сообщества, чтобы разрешить доступ к агенту SNMPv3. Допустимая длина строки - от 1 до 32, а допустимое содержимое - символы ASCII от 33 до 126. Строка сообщества будет считаться именем безопасности и отображать строку сообщества SNMPv1 или SNMPv2c.
Source IP Указывает исходный адрес доступа SNMP. Определенный диапазон адресов источника может использоваться для ограничения исходной подсети в сочетании с маской источника.
Source Mask Указывает исходную маску адреса доступа SNMP.
Нажмите «Save», чтобы сохранить Ваши настройки.

2.6.4 Users (Пользователи)

SNMP v3 использует механизм аутентификации USM (User-Based Security Model). Администратор может установить функцию аутентификации и шифрования. Аутентификация проверяет правильность отправителя сообщения во избежание незаконного доступа пользователей. Шифрование предназначено для шифрования связи между NMS и агентами. Выбирая обе функции, обеспечивается большая безопасность для связи между NMS и Агентом.

Пользователи могут установить учетную запись SNMP v3 и EncryMode. Нажмите «Network Admin» (Сетевой администратор)>" SNMP "> «Users» (Пользователи), как показано ниже**:**

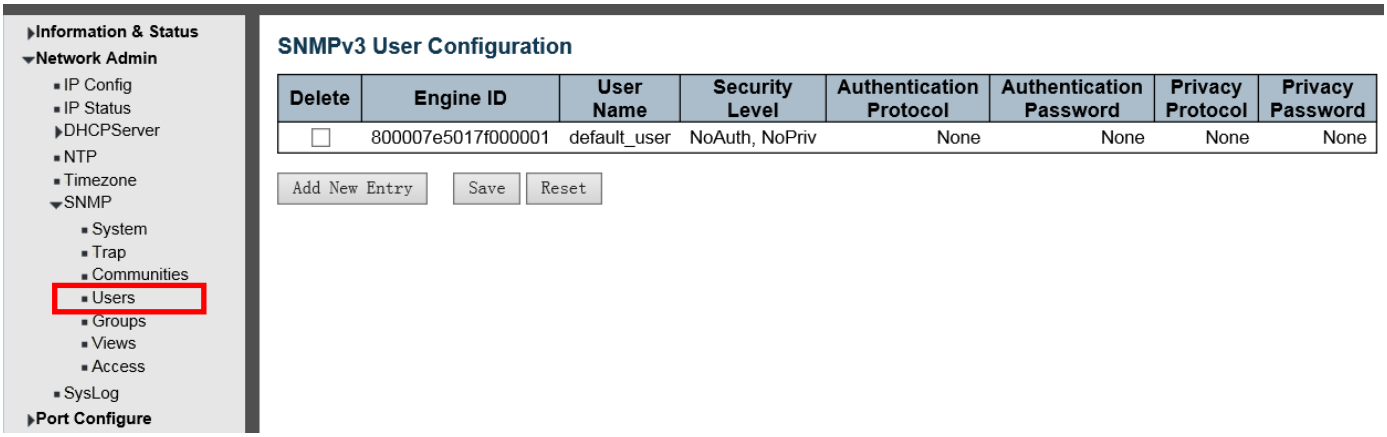


Рисунок 2-6-4 Пользователи

Engine ID Идентификатор двигателя	Значение по умолчанию 800007e5017f000001. Рекомендуется использовать значение по умолчанию
User Name Имя пользователя	Введите имя новой учетной записи SNMPv3.
Security Level Уровень безопасности	Три EncryModes, NoAuth, NoPriv , Auth, NoPriv , Auth, Priv, выбор из ниспадающего меню
Authentication Protocol Протокол аутентификации	Выберите для MD5 и SHA
Authentication Password Пароль аутентификации	Введите зашифрованный пароль
Privacy Protocol Протокол конфиденциальности	Выберите для DES и AES
Privacy Password Пароль конфиденциальности	Введите зашифрованный пароль

Нажмите «Save», чтобы сохранить Ваши настройки.

2.6.5 Groups(Группы)

Пользователи могут установить группы для загрузки встроенных Users (пользователей) и Access (доступа). Нажмите «Network Admin» (Сетевой администратор)>" SNMP "> «Groups»(Группы), как показано ниже

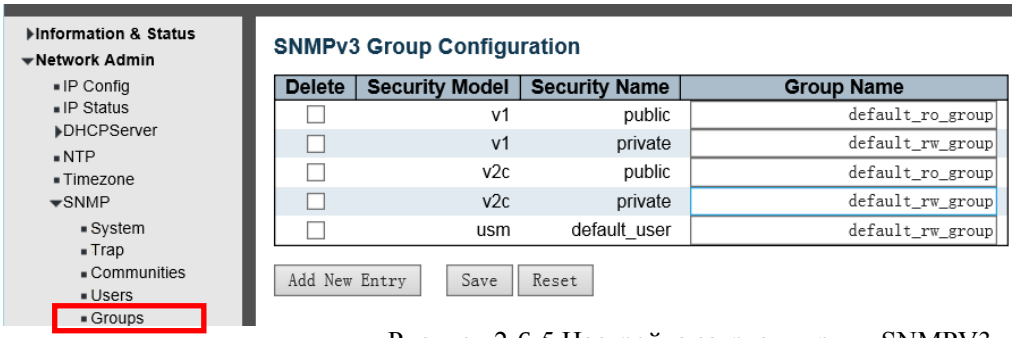


Рисунок 2-6-5 Настройка загрузки групп SNMPV3

Security Model Модель безопасности	Выберите для v1 v2c usm
Security Name Имя безопасности	Выберите имя встроенной учетной записи. Для имени встроенной команды под v1 v2c, имя встроенной учетной записи под usm
Group Name Имя группы	Имя группы Введите имя встроенной группы

Нажмите «Save», чтобы сохранить Ваши настройки.

2.6.6 Views(Виды)

Пользователи могут установить вид посещения SNMPv3. Нажмите «Network Admin» (Сетевой администратор)>" SNMP "> «Views» (Виды). Как показано ниже:

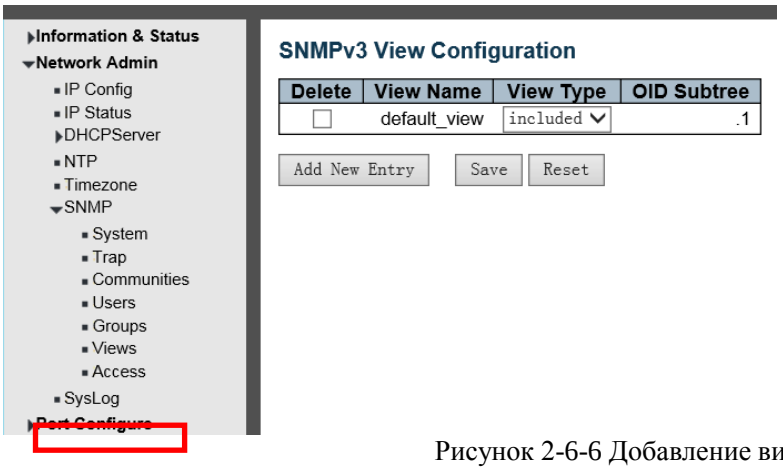


Рисунок 2-6-6 Добавление видов SNMPV3

Views Name (Имя просмотра)	Введите имя просмотра
Views Type (Тип просмотра)	Выберите для включенных и исключенных
OID Subtree (Поддерево OID)	Входное поддерево OID, например .1

Нажмите «Save», чтобы сохранить Ваши настройки.

2.6.7 Access(Доступ)

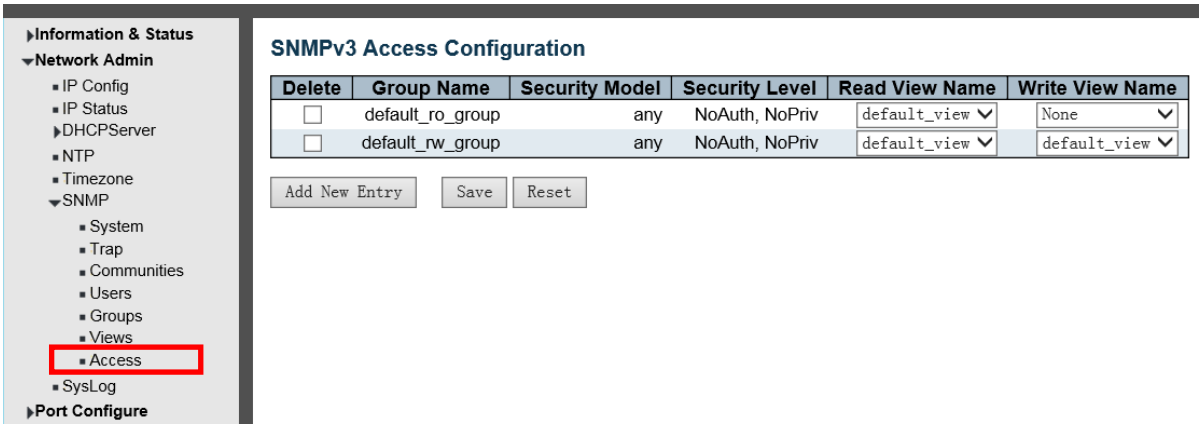


Рисунок 2-6-7 Настройка доступа SNMPv3

Group Name Имя группы	Введите название группы
Security Model Модель безопасности	Выберите для любого v1 v2c usm
Security Level Уровень безопасности	Три EncryModes, NoAuth, NoPriv , Auth, NoPriv , Auth, Priv, выбор из ниспадающего меню
Read View Name Прочитать имя вида	Выбрать встроенные виды
Write View Name Написать имя вида	Выбрать встроенные виды

Нажмите «Save», чтобы сохранить Ваши настройки.

2.7 SysLog (системный журнал)

Нажмите «Network Admin» (Сетевой администратор)>" SysLog"

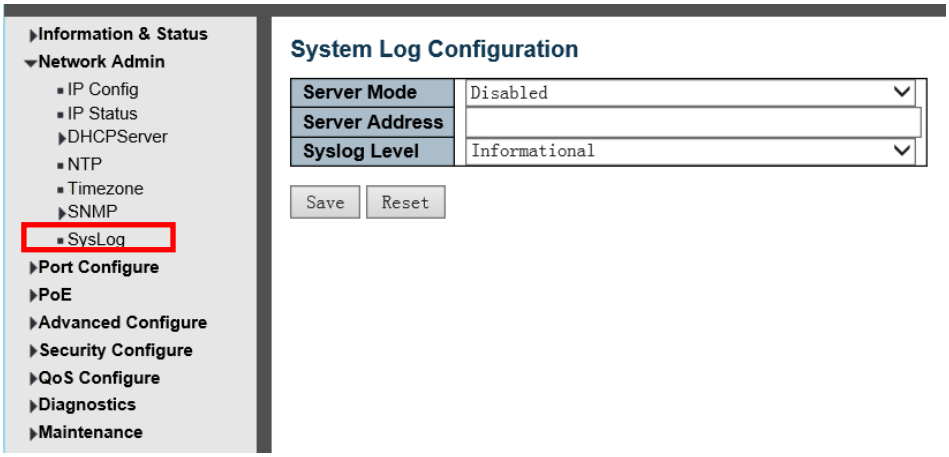


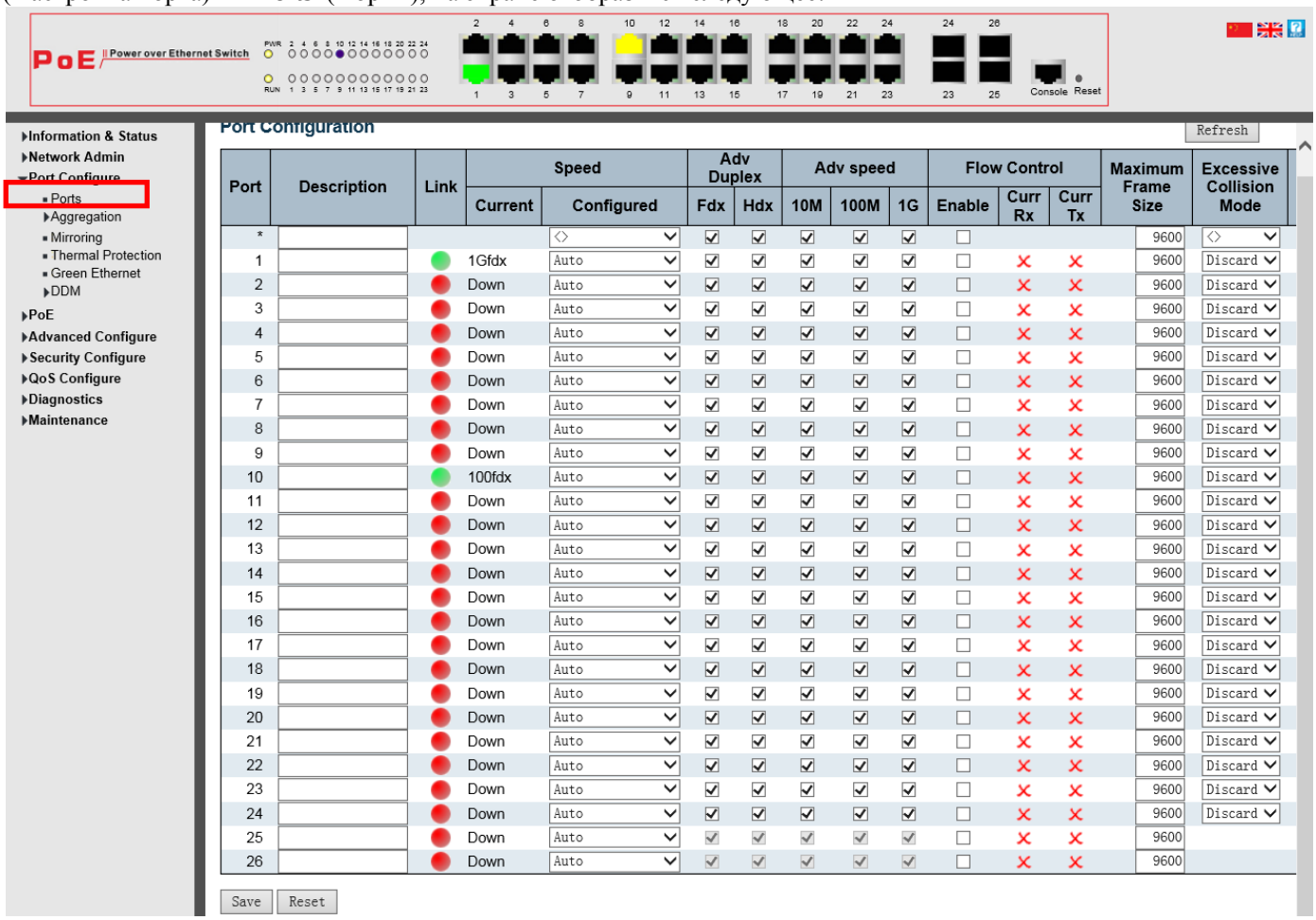
Рисунок 2-4 Экран конфигурации системного журнала

Конфигурация системного журнала

Настройте системный журнал на этой странице.
Server Mode Режим сервера Указывает работу режима сервера. Когда режим работы включен, сообщение системного журнала будет отправлено на сервер системного журнала. Протокол системного журнала основан на связи UDP и получен через UDP-порт 514, и сервер системного журнала не будет отправлять подтверждения отправителю, поскольку UDP является протоколом без установления соединения и не предоставляет подтверждения. Пакет системного журнала будет отправляться всегда, даже если сервер системного журнала не существует. Возможные режимы:
Enabled: Включено: Включить работу в режиме сервера.
Disabled: Отключено: отключить работу в режиме сервера.
Server Address Адрес сервера: Указывает адрес хоста IPv4 сервера системного журнала. Если коммутатор предоставляет функцию DNS, это также может быть доменное имя.
Syslog Level Уровень системного журнала: Указывает, какое сообщение будет отправлено на сервер системного журнала. Возможные режимы:
Error Ошибка: отправьте конкретные сообщения, код серьезности которых меньше или равен ошибке (3).
Warning Предупреждение: Отправьте конкретные сообщения, код серьезности которых меньше или равен значению «Предупреждение» (4).
Notice Уведомление: Отправьте конкретные сообщения, код серьезности которых меньше или равен Уведомлению (5).
Informational Информационный: Отправьте конкретные сообщения, код серьезности которых меньше или равен информационному (6).
Нажмите «Save», чтобы сохранить Ваши настройки.

3.Port Configure (Настройка порта)
3.1 Port Configuration (Настройка порта)

Эта страница предназначена для настройки параметров порта коммутатора. После нажатия «Port Configure (Настройка порта)»> «Ports»(Порты), на экране отобразится следующее:



Port	Description	Link	Speed		Adv Duplex		Adv speed			Flow Control			Maximum Frame Size	Excessive Collision Mode
			Current	Configured	Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx		
*				◇	☑	☑	☑	☑	☑	☐			9600	◇
1			1Gfdx	Auto	☑	☑	☑	☑	☑	☐	✕	✕	9600	Discard
2			Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	9600	Discard
3			Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	9600	Discard
4			Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	9600	Discard
5			Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	9600	Discard
6			Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	9600	Discard
7			Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	9600	Discard
8			Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	9600	Discard
9			Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	9600	Discard
10			100fdx	Auto	☑	☑	☑	☑	☑	☐	✕	✕	9600	Discard
11			Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	9600	Discard
12			Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	9600	Discard
13			Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	9600	Discard
14			Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	9600	Discard
15			Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	9600	Discard
16			Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	9600	Discard
17			Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	9600	Discard
18			Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	9600	Discard
19			Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	9600	Discard
20			Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	9600	Discard
21			Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	9600	Discard
22			Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	9600	Discard
23			Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	9600	Discard
24			Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	9600	Discard
25			Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	9600	
26			Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	9600	

Рисунок 3-1. Экран настройки порта

Link Красный цвет означает Link Down, зеленый цвет означает Link Up

Speed Выберите скорость порта и полный / полудуплексный режим. «Disabled» (Отключено) означает, что порт отключен. «Авто» означает в полнодуплексном (FDX) или полудуплексном режиме (HDX) (1000 Мбит / с всегда в полнодуплексном режиме) автоматическое согласование между 10 100 000 Мбит / с устройствами. Настройка «Авто» позволяет порту автоматически определять самые быстрые настройки для подключенного устройства и применять эти настройки. «1000-X_AMS» означает, что порт является комбинированным портом Ethernet / Optical, и оптический порт имеет приоритет. Другие варианты: 10M HDX, 10M FDX, 100M HDX, 100M FDX, 1000M FDX, 1000-X

Flow Control Управление потоком. Это механизм управления потоком для различных конфигураций портов. Полнодуплексные порты используют управление потоком 802.3x, полудуплексные порты используют управление потоком противодавления. По умолчанию отключено. Установите флажок, чтобы включить управление потоком.

Maximum Frame Size Максимальный размер кадра. Используется для установки максимального размера кадра для Ethernet. Настройка по умолчанию - 9600, которая должна поддерживать Jumbo-кадры.

Нажмите «Save», чтобы сохранить Ваши настройки.

3.2. Link Aggregation (Агрегация ссылок)

Пользователи могут установить несколько ссылок между несколькими коммутаторами. Агрегация ссылок, это метод, который связывает некоторые физические порты вместе как один логический порт, чтобы увеличить пропускную способность. Этот коммутатор поддерживает до 13 групп Link Aggregation, от 2 до 8 портов в одной группе.

Примечание. Если какой-либо порт в группе агрегации каналов отключен, пакет данных, отправленный на отключенный порт, будет распределять нагрузку с другим подключенным портом в этой группе агрегации.

3.2.1 Статическая агрегация

После нажатия «Port Configure (Настройка порта)»> " Aggregation " (Агрегация)>"Static"(Статический), появится окно с настройками статического агрегирования.

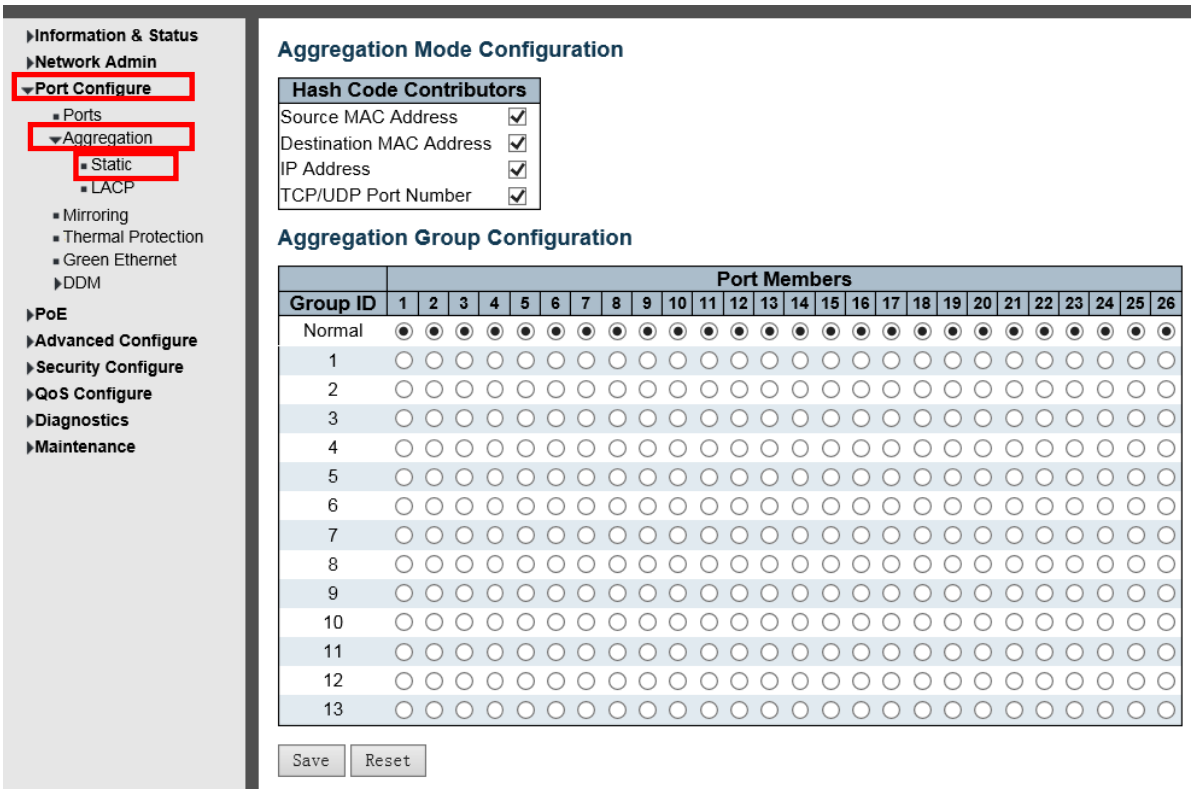


Рисунок 3-2-1. Экран конфигурации статического агрегирования портов

Aggregation Mode Configuration	Конфигурация режима агрегации. Этот параметр является алгоритмом хеширования потока между портами LAG (Link Aggregated Group).
Group ID	Идентификатор группы. Статический идентификатор группы агрегации
Port Members	Участники порта. Этот коммутатор поддерживает до 13 групп Link Aggregation, от 2 до 8 портов в одной группе.

Нажмите «Save», чтобы сохранить Ваши настройки.

Примечание. Допустимо одновременно объединять не более 8 портов в одну статическую группу.

3.2.2 LACP Aggregation

Протокол управления агрегацией каналов Link Aggregation Control Protocol (LACP) предоставляет стандартизированные средства для обмена информацией между партнерскими системами, для которых требуются высокоскоростные резервные каналы. Агрегация каналов позволяет группировать до восьми последовательных портов в одно выделенное соединение. Эта функция может расширить полосу пропускания для устройства в сети.

LACP операция требует полнодуплексного режима. Для получения более подробной информации обратитесь к стандарту IEEE 802.3ad.

Пользователи могут создавать динамические группы агрегации для коммутаторов. После нажатия «Port Configure (Настройка порта)»> " Aggregation " (Агрегация)> «LACP» пользователи могут настроить конфигурацию LACP на следующем экране.

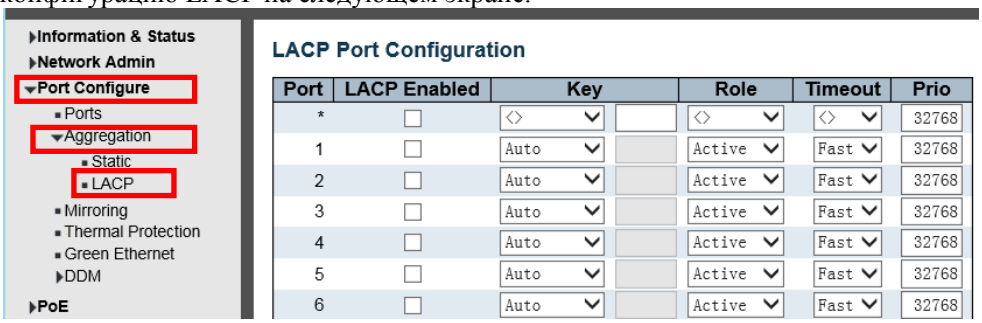


Рисунок 3-2-2. Экран конфигурации LACP

LACP Включение или отключение функции LACP для этого порта.

Key Ключ. Значение ключа, полученное портом, находится в диапазоне 1-65535. Автоматическая настройка установит ключ в зависимости от скорости физической линии: 10 МБ = 1, 100 МБ = 2, 1 ГБ = 3. Используя параметр «Конкретный», можно ввести пользовательское значение. Порты с одинаковым значением ключа могут участвовать в одной группе агрегации, а порты с разными ключами - нет.

Role Роль показывает статус активности LACP. Active будет передавать пакеты LACP каждую секунду, в то время как Passive будет ожидать пакета LACP от партнера (говорить, если с ним говорят).

Timeout Тайм-аут. Тайм-аут контролирует период между передачами BPDU. Fast будет передавать пакеты LACP каждую секунду, а Slow будет ждать 30 секунд перед отправкой пакета LACP.

Prio Контролирует приоритет порта. Если партнер LACP хочет сформировать большую группу, чем поддерживается этим устройством, этот параметр будет контролировать, какие порты будут активными, а какие будут выполнять роль резервного копирования. Меньшее число означает больший приоритет.

Нажмите «Save», чтобы сохранить Ваши настройки.

3.3 Mirroring (Зеркалирование портов)

Настройте зеркальное отображение портов на этой странице. Эта функция обеспечивает мониторинг сетевого трафика, который пересылает копию каждого входящего или исходящего пакета с одного порта сетевого коммутатора на другой порт, где пакет может быть изучен. Это позволяет менеджеру следить за производительностью коммутатора и при необходимости изменять его.

Чтобы настроить параметры зеркала, нажмите «Port Configure (Настройка порта)»> «Mirroring (Зеркалирование)». Тогда следующий экран будет выглядеть так:

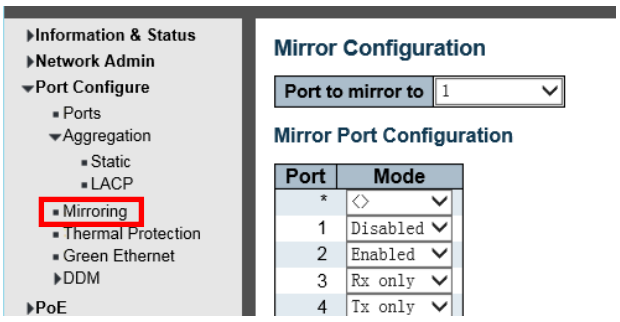


Рисунок 3-3. Экран настройки зеркала

Port mirror to Кадры из портов, для которых включено зеркалирование источника (rx) или назначения (tx), отражаются на этом порту. Отключено(Disabled) отключает зеркалирование.

Mode	Выберите режим зеркала исходного порта. **Rx only Кадры**, полученные на этот порт, отражаются на зеркальном порту. Переданные кадры не отражаются. **Tx only Кадры**, передаваемые через этот порт, отражаются на зеркальном порту. Полученные кадры не отражаются. **Disabled** Отключено Ни переданные, ни принятые кадры не отражаются. **Enabled** Включено Полученные кадры и переданные кадры отражаются на зеркальном порту. **Примечание.**. Для данного порта кадр передается только один раз. Поэтому невозможно зеркально отразить кадры Tx порта зеркала. Из-за этого режим для выбранного зеркального порта ограничен только **Disabled** или **Rx only**.

Нажмите «Save», чтобы сохранить Ваши настройки.

Примечание: Вы не можете установить зеркало для высокоскоростного порта на низкоскоростной порт. Например, существует проблема, если вы попытаетесь отразить порт (ы) 100 Мбит / с на порт 10 Мбит / с. Таким образом, порт назначения должен иметь равную или более высокую скорость по сравнению с портом источника. Кроме того, порт источника и порт назначения не должны совпадать.

3.4 Thermal Protection (Конфигурация тепловой защиты)

Тепловая защита предназначена для обнаружения и защиты рабочего выключателя. Когда коммутатор обнаружил температуру порта выше заданной температуры, система отключит порт, чтобы защитить сам коммутатор.

После нажатия «Port Configure (Настройка порта)»> «Thermal Protection (Тепловая защита)», следующий экран будет выглядеть так:

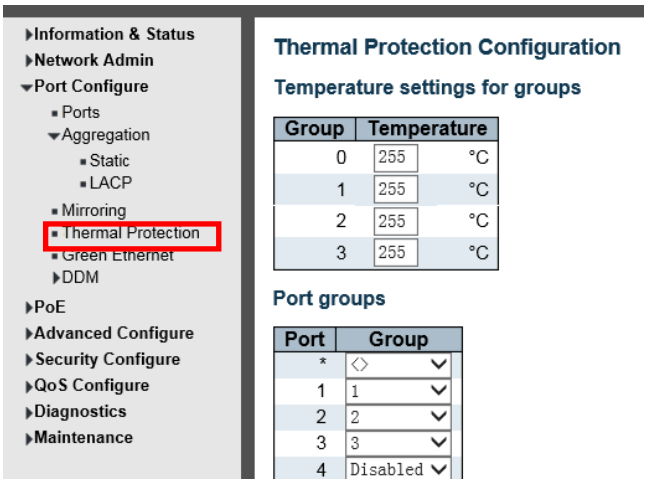


Рисунок 3-4. Экран настройки термозащиты

Temperature settings for groups	Настройки температуры для групп. Температура, при которой порты соответствующей группы будут отключены. Поддерживаются температуры от 0 до 255 ° C.
Port groups	Группы портов. Группа, к которой принадлежит порт. Поддерживаются 4 группы.

Нажмите «Save», чтобы сохранить Ваши настройки.

Примечание. По умолчанию все порты коммутатора относятся к группе приоритетов 0 с защищенной температурой 225 градусов C.

3.5 Green Ethernet (Зеленый Ethernet)

После нажатия «Port Configure (Настройка порта)»> «Green Ethernet» появится окно:

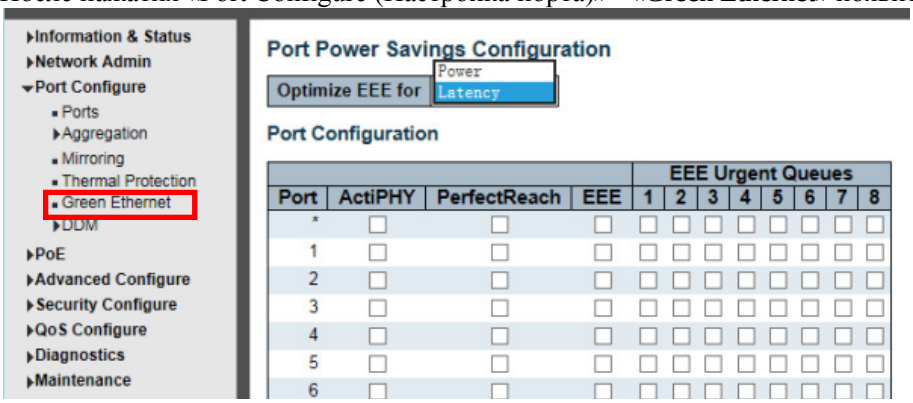


Рисунок 3-5. Экран настройки функции энергосбережения порта

Port Power Savings Configuration

Эта страница позволяет пользователю настроить функции энергосбережения порта.

Что такое EEE

EEE - это опция энергосбережения, которая снижает энергопотребление при низкой или нулевой загрузке трафика.

EEE работает, отключая цепи, когда нет трафика. Когда порт получает данные для передачи, все каналы включаются. Время включения цепей называется временем пробуждения. Время пробуждения по умолчанию составляет 17 мкс для 1-гигабитных ссылок и 30 мкс для других скоростей. Устройства EEE должны согласовать значение времени пробуждения, чтобы убедиться, что на приемном и передающем устройстве все цепи включены при передаче трафика. Устройства могут обмениваться информацией о времени пробуждения, используя протокол LLDP.

EEE работает для портов в режиме автосогласования, где порт согласовывается либо в полнодуплексном режиме 1G, либо в 100 Мбит.

Для портов, которые не поддерживают EEE, соответствующие флажки EEE выделены серым цветом и, следовательно, невозможно включить EEE.

Когда порт отключается для экономии энергии, исходящий трафик сохраняется в буфере до следующего включения порта. Поскольку при переключении порта вниз и вверх возникают некоторые издержки, можно сэкономить больше энергии, если трафик может быть буферизован до тех пор, пока не будет передан большой пакет трафика. Буферизация трафика даст некоторую задержку в трафике.

Optimize EEE for (Оптимизировать EEE для)

Коммутатор может быть настроен на оптимизацию EEE для наилучшего энергосбережения или минимальной задержки трафика.

Port Configuration (Конфигурация порта)

Port Номер порта коммутатора логического порта.
ActiPHY
Сброс энергосбережения включен.
ActiPHY работает, уменьшая мощность для порта, когда нет связи. Порт на короткое время включается, чтобы определить, подключен ли кабель.
PerfectReach
Длина энергосбережения включена.
PerfectReach работает путем определения длины кабеля и снижения мощности для портов с короткими кабелями.
EEE Управляет включением EEE для этого порта коммутатора.

Для обеспечения максимальной экономии энергии схема не запускается сразу, когда данные передаются для порта, а вместо этого ставится в очередь, пока пакет данных не будет готов к передаче. Это даст некоторую задержку трафика.

При желании можно минимизировать задержку для определенных кадров путем сопоставления кадров с определенной очередью (выполненной с помощью QOS), а затем пометить очередь как срочную очередь. Когда срочная очередь получает данные для передачи, каналы сразу включаются, и задержка уменьшается до времени пробуждения.
EEE Urgent Queues (Набор очередей EEE) Urgent Queues активирует передачу кадров, как только данные станут доступны. В противном случае очередь отложит передачу до тех пор, пока не будет передан пакет кадров.

3.6 DDM

DDM(Digital Diagnostics Monitoring) — функция цифрового контроля параметров производительности SFP трансивера (а также SFP+ и XFP). Позволяет отслеживать в реальном времени такие параметры как: напряжение, температуру модуля...

3.6.1 DDM Configuration

После нажатия «Port Configure (Настройка порта)»> «DDM Configuration » появится окно:

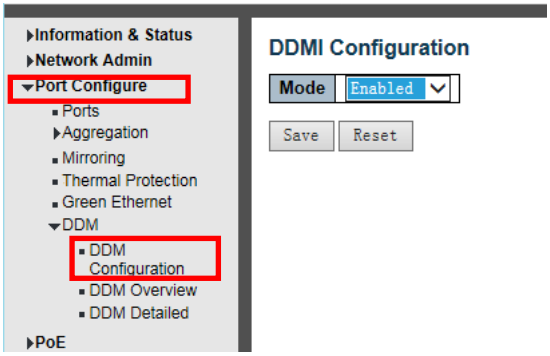


Рисунок 3-6-1. Экран настройки **DDM**

DDM Configuration (Конфигурация DDM)

Настройте DDMI на этой странице.
Mode (Режим) Указывает на работу в режиме DDMI.
Возможные режимы:
Enable Включено: Включить работу в режиме DDMI.
Disable Отключено: отключить работу в режиме DDMI.

3.6.2 DDM Overview

После нажатия «Port Configure (Настройка порта)»> «DDM Overview » появится окно:

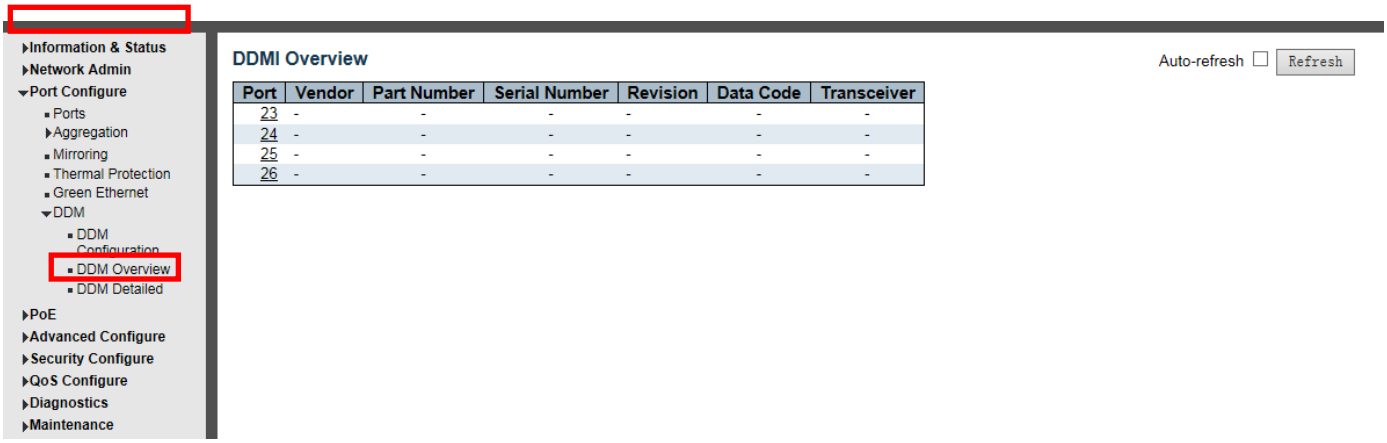


Рисунок 3-6-2. Экран обзорной информации **DDM**

На этой странице показана обзорная информацию DDMI.
Port DDM - порт.
Vendor Поставщик Указывает имя поставщика Имя поставщика SFP.
Part Number Номер детали Указывает поставщика PN Номер детали, предоставленный поставщиком SFP.
Serial Number Серийный номер Указывает серийный номер поставщика, предоставленный поставщиком.
Редакция Указывает ревизию поставщика Уровень ревизии для номера детали, предоставленного поставщиком.
Data Code Код данных Указывает код даты Код даты изготовления поставщика.
Transeiver Указывает на совместимость с трансивером.

3.6.3 DDM Detailed (DDM Подробно)

После нажатия «Port Configure (Настройка порта)»> «DDM Detailed » появится окно:

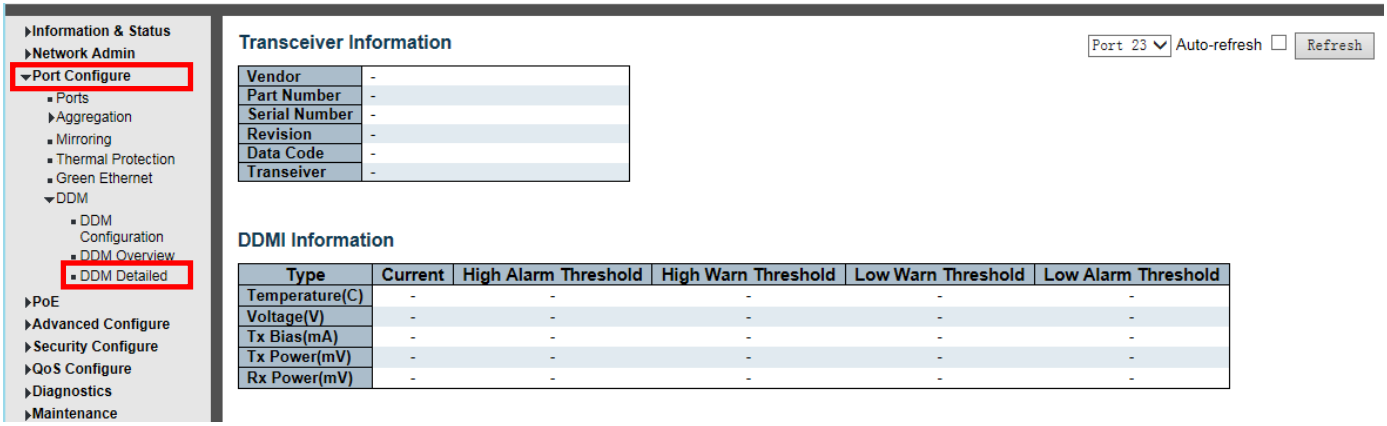


Рисунок 3-6-3. Экран подробной информации **DDM**

На этой странице показана информацию о трансивере.

Transceiver Information

Vendor Поставщик Указывает имя поставщика Имя поставщика SFP.
Part Number Номер детали Указывает поставщика PN Номер детали, предоставленный поставщиком SFP.
Serial Number Серийный номер Указывает серийный номер поставщика, предоставленный поставщиком.
Редакция Указывает ревизию поставщика Уровень ревизии для номера детали, предоставленного поставщиком.
Data Code Код данных Указывает код даты Код даты изготовления поставщика.
Transeiver Указывает на совместимость с трансивером.

DDMI Information

Current Текущее значение температуры, напряжения, смещения TX, мощности TX и мощности RX.
High Alarm Threshold Высокий порог тревоги: температура, напряжение, смещение передачи, мощность передачи и мощность приема.
High Warn Threshold Пороговое значение для высокого предупреждения о температуре, напряжении, смещении TX, мощности TX и мощности RX.
Low Warn Threshold Пороговое значение для низкого предупреждения о температуре, напряжении, смещении TX, мощности TX и мощности RX.
Low Alarm Threshold Низкое пороговое значение тревоги температуры, напряжения, смещения TX, мощности TX и мощности RX.

4. PoE Configuration(Конфигурация PoE)

4.1 PoE Setting (Настройка PoE)

После нажатия «PoE)»> «PoE Setting» появится окно:

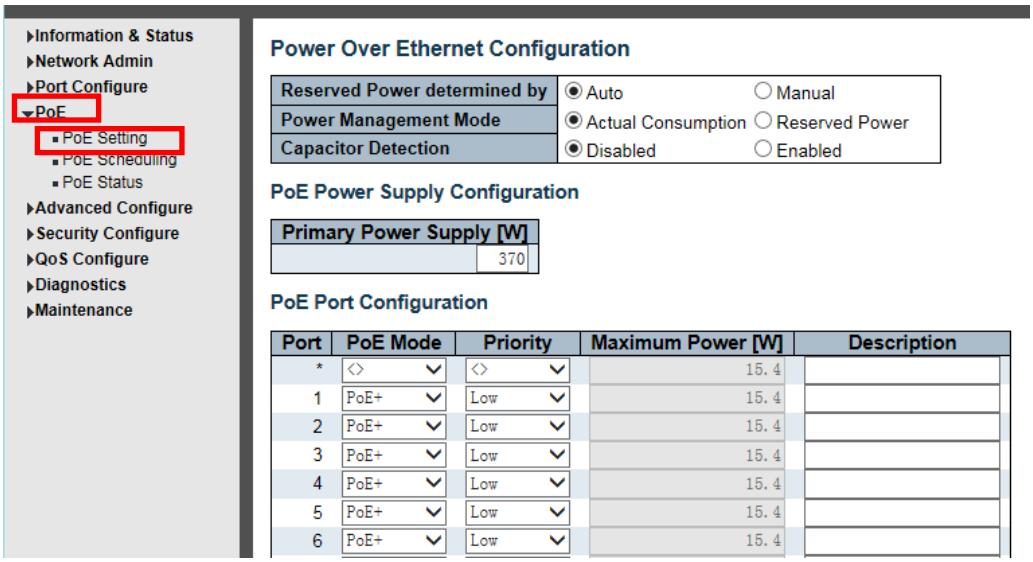


Рисунок 4-1 Экран настроек PoE

Power Over Ethernet Configuration (Конфигурация питания через Ethernet)

Reserved Power determined by Зарезервированная мощность определяется тремя способами для настройки того, как порты / PD(Power device) могут резервировать мощность.
1. Распределенный режим: в этом режиме пользователь распределяет количество энергии, которое может зарезервировать каждый порт. Выделенная / зарезервированная мощность для каждого порта / PD указана в полях Maximum Power.
2. Режим класса: в этом режиме каждый порт автоматически определяет, сколько энергии резервировать в соответствии с классом, к которому принадлежит подключенный PD, и соответственно резервирует мощность. Существует четыре различных класса портов, один на 4, 7, 15,4 или 30 Вт. В этом режиме поля максимальной мощности не действуют.
3. Режим LLDP-MED: этот режим аналогичен режиму класса, в котором каждый порт определяет величину мощности, которую он резервирует, путем обмена информацией PoE с использованием протокола LLDP и резервирует мощность соответственно. Если информация о LLDP недоступна для порта, порт будет резервировать питание с использованием режима класса. В этом режиме поля максимальной мощности не действуют для всех режимов: если порт использует больше мощности, чем зарезервированная мощность для порта, порт отключается.

Power Management Mode Режим управления питанием Есть 2 режима для настройки времени отключения портов:
1. Фактическое потребление: в этом режиме порты отключаются, когда фактическое энергопотребление для всех портов превышает количество энергии, которое может доставить источник питания, или если фактическое энергопотребление для данного порта превышает зарезервированную мощность для этого порта. Порты отключены в соответствии с приоритетом портов. Если два порта имеют одинаковый приоритет, порт с наибольшим номером порта отключается.
2. Зарезервированная мощность: в этом режиме порты отключаются, когда общее резервное питание превышает количество энергии, которое может обеспечить источник питания. В этом режиме питание порта не включается, если PD запрашивает больше энергии, чем доступно от источника питания.
Capacitor Detection Обнаружение конденсатора Управляет обнаружением конденсатора для устаревших устройств PD.
Disabled Отключено: эта функция отключена.
Enabled Включено: эта функция включена.

Power Supply Configuration Конфигурация источника питания
Источник питания Чтобы определить количество энергии, которое может использовать ПД, необходимо определить, какое количество энергии может выдавать источник питания.
Допустимые значения находятся в диапазоне от 0 до 2000 Вт.

Port Configuration Конфигурация порта
Port Это логический номер порта для этой строки.
Порты, которые не поддерживают PoE, выделены серым цветом и, следовательно, невозможно настроить PoE для.

PoE Mode Режим PoE представляет режим работы PoE для порта.

Disabled Отключено: PoE отключено для порта.
PoE: включает PoE IEEE 802.3af (PD класса 4 ограничен 15,4 Вт)
PoE +: включает PoE + IEEE 802.3at (PD класса 4 ограничены 30 Вт)

Priority Приоритет представляет приоритет портов. Существует три уровня приоритета мощности: Low Низкий, Hi Высокий и Critical Критический.
Приоритет используется в случае, когда удаленным устройствам требуется больше энергии, чем может обеспечить источник питания. В этом случае порт с самым низким приоритетом будет отключен, начиная с порта с наибольшим номером порта.
Maximum Power Максимальная мощность
Значение максимальной мощности содержит числовое значение, которое указывает максимальную мощность в ваттах, которую можно доставить на удаленное устройство.
Максимально допустимое значение составляет 30 Вт.

4.2 PoE Scheduling (планирования PoE)

Коммутатор поддерживает планирование PoE, пользователи могут устанавливать время перезагрузки PoE и включать / отключать PoE по расписанию.
После нажатия «PoE»> «PoE Scheduling» появится окно:

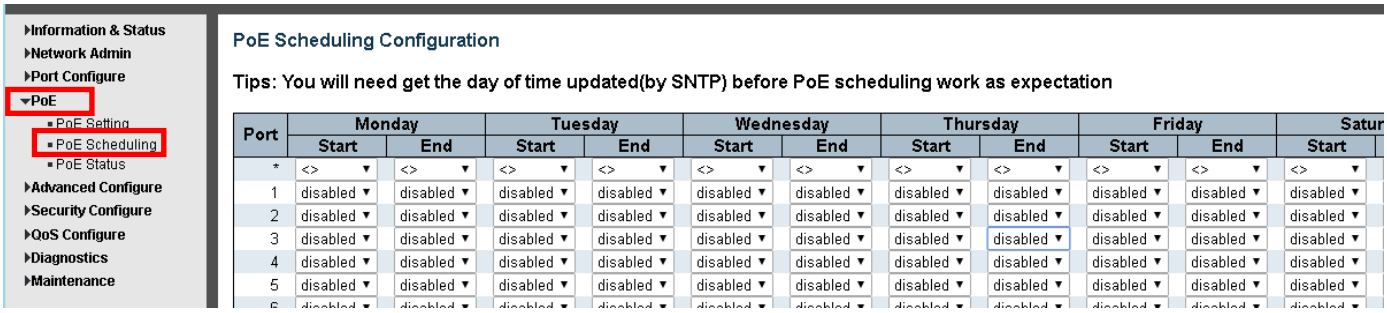


Рисунок 4-2 Экран планирования PoE

Советы: вам нужно будет обновить день (по SNTP) перед планированием работы PoE.

4.3 PoE Status(Состояние PoE)

После нажатия «PoE)»> «PoE Status» появится окно:

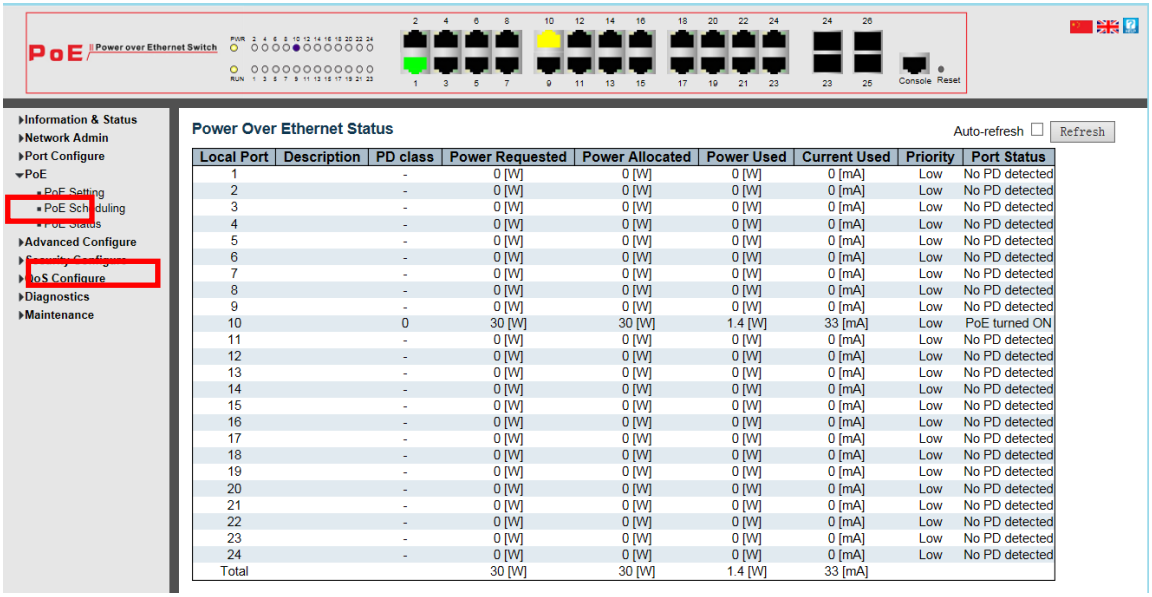


Рисунок 4-3 Экран состояния PoE

5. Advanced Configure (Расширенная настройка)

5.1 VLAN

VLAN (виртуальная локальная сеть) логически делит одну LAN (локальную сеть) на множество подмножеств, и каждое подмножество образует собственную широковещательную сеть. Короче говоря, VLAN - это технология связи, которая логически разделяет одну физическую локальную сеть на несколько широковещательных сетей (несколько VLAN). Хосты внутри VLAN могут общаться напрямую. Но группы VLAN не могут напрямую общаться друг с другом. Так что это ограничит широковещательные пакеты в VLAN. Поскольку отсутствует прямой доступ между группами VLAN, это повышает безопасность сети.

Нажмите «Advanced Configure»> «VLAN», чтобы увидеть экран конфигурации 802.1Q VLAN следующим образом:

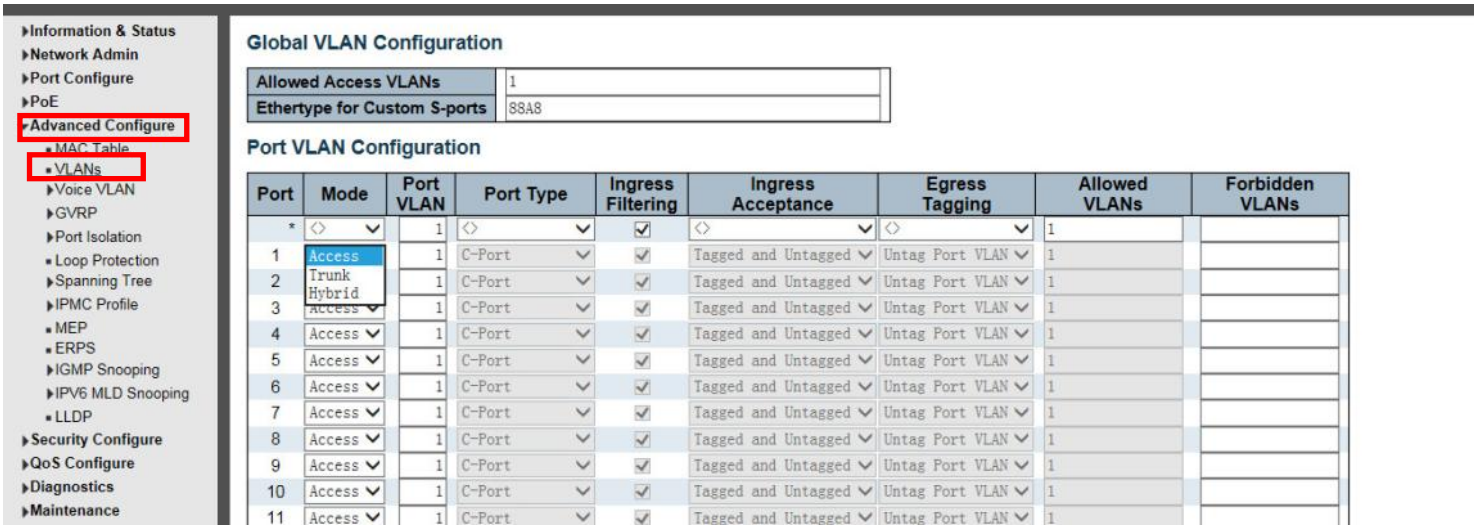


Рисунок 5-1 Экран конфигурации VLAN

Global VLAN Configuration Глобальная конфигурация VLAN

Allowed Access VLANs VLAN разрешенного доступа. В этом поле отображаются разрешенные VLAN доступа, т. Е. Оно влияет только на порты, настроенные как порты доступа. Порты в других режимах являются членами VLAN, указанными в поле Allowed VLAN. По умолчанию включена только VLAN 1. Больше VLAN может быть создано с использованием синтаксиса списка, где отдельные элементы разделены запятыми. Диапазоны указаны с дефисом, разделяющим нижнюю и верхнюю границы.
В следующем примере будут созданы VLAN 1, 10, 11, 12, 13, 200 и 300: 1,10-13,200,300. Между разделителями допускаются пробелы.
Ethertype for Custom S-ports Ethertype для пользовательских S-портов. В этом поле указывается ethertype / TPID (указанный в шестнадцатеричном формате), используемый для пользовательских S-портов. Этот параметр действует для всех портов, для которых в качестве типа порта установлено значение S-Custom-Port.

Port VLAN Configuration Конфигурация порта VLAN

Port - логический номер порта этой строки.

Mode Режим порта (по умолчанию Access) определяет основное поведение рассматриваемого порта. Порт может находиться в одном из трех режимов, как описано ниже.
Всякий раз, когда выбран конкретный режим, остальные поля в этой строке будут либо выделены серым цветом, либо изменены в зависимости от рассматриваемого режима.
Затененные поля показывают значение, которое порт получит при применении режима.

Access Доступ:
Порты доступа обычно используются для подключения к конечным станциям. Динамические функции, такие как Voice VLAN, могут добавить порт к большему количеству VLAN за кулисами. Порты доступа имеют следующие характеристики:
• Участник ровно одной VLAN, VLAN порта (a.k.a. VLAN доступа), которая по умолчанию равна 1
• Принимает кадры без тегов и C-tagged

• Сбрасывает все кадры, не классифицированные в Access VLAN
• На выходе все кадры передаются без тегов

Trunk Магистральный:

Магистральные порты могут одновременно передавать трафик по нескольким сетям VLAN и обычно используются для подключения к другим коммутаторам. Магистральные порты имеют следующие характеристики:
• По умолчанию магистральный порт является членом всех VLAN (1-4095).
• Сети VLAN, членом которых является магистральный порт, могут быть ограничены использованием разрешенных сетей VLAN.
• Кадры, классифицированные для VLAN, членом которой порт не является, отбрасываются
• По умолчанию все кадры, кроме кадров, отнесенных к порту VLAN (например, собственная VLAN), помечаются на выходе. Кадры, отнесенные к порту VLAN, не имеют C-тегов на выходе
• Выходную метку можно изменить, чтобы пометить все кадры, и в этом случае только входные метки принимаются на входе.

Hybrid Гибридный:

Гибридные порты во многом напоминают магистральные порты, но добавляют дополнительные функции конфигурации портов. В дополнение к характеристикам, описанным для магистральных портов, гибридные порты имеют следующие возможности:
• Может быть настроен так, чтобы тег VLAN не распознавался, распознавал C-тег, распознавал S-тег или распознавал S-custom-тег
• Входная фильтрация может контролироваться
• Входной прием кадров и конфигурация выходной маркировки могут быть настроены независимо

Port VLAN

Порт VLAN определяет идентификатор VLAN порта (например, PVID). Допустимые VLAN находятся в диапазоне от 1 до 4095, по умолчанию 1.

При входе кадры классифицируются как порт VLAN, если порт настроен как не осведомленный о VLAN, кадр не помечен или в нем включена поддержка VLAN, но кадр помечен как приоритетный (VLAN ID = 0).

На выходе кадры, классифицированные для VLAN порта, не помечаются, если для конфигурации исходящей метки установлено значение Untag Port VLAN.

VLAN для портов называется «Access VLAN» для портов в режиме доступа, и «Native VLAN» для портов в магистральном или гибридном режиме.

Port Type

Порты в гибридном режиме позволяют изменять тип порта, то есть используется ли тег VLAN кадра для классификации кадра при входе в конкретную VLAN и, если да, то на какой TPID он реагирует. Аналогично, на выходе тип порта определяет TPID тега, если тег требуется.

Unaware Неподозревающий:

При входе все кадры, независимо от того, несут ли они тег VLAN, классифицируются как порт VLAN, и возможные теги не удаляются на выходе.

C-***Port:***

При входе кадры с тегом VLAN с TPID = 0x8100 классифицируются по идентификатору VLAN, встроенному в тег.

Если кадр не помечен или помечен как приоритетный, кадр классифицируется как порт VLAN.

Если кадры должны быть помечены на выходе, они будут помечены C-меткой.

S-Port:

При входе кадры с тегом VLAN с TPID = 0x88A8 классифицируются по идентификатору VLAN, встроенному в тег.

Кадры с тегами приоритета классифицируются как порт VLAN.

Если порт настроен на прием только **Tagged Only** помеченных кадров (см. Прием входных данных ниже), кадры без этого TPID отбрасываются.

Если порт настроен на прием **Untagged Only** или **Tagged and Untagged** (только кадров без тегов или с тегами и без тегов) (см. Приемка ниже), кадры с C-тегом обрабатываются как кадры с S-тегом.

Если кадры должны быть помечены на выходе, они будут помечены S-меткой.

S-Custom-Port:

При входе кадры с тегом VLAN с TPID, равным Ethertype, настроенному для портов Custom-S, классифицируются по идентификатору VLAN, встроенному в тег.

Кадры с тегами приоритета классифицируются как порт VLAN.

Если порт настроен на прием только помеченных кадров (см. Прием входных данных ниже), кадры без этого TPID отбрасываются.
Если порт настроен на прием только кадров без тегов или с тегами и без тегов (см. Приемка ниже), кадры с C-тегом обрабатываются как кадры с пользовательским S-тегом.
Если кадры должны быть помечены на выходе, они будут помечены пользовательским S-тегом.

Ingress Filtering Входная фильтрация
Hybrid port гибридный порт позволяет изменить входную фильтрацию. Access port и Trunk порт (Порты доступа и магистральный) всегда имеют входную фильтрацию.
Если входная фильтрация включена (флажок установлен), кадры, классифицированные для VLAN, к которой порт не принадлежит, отбрасываются.
Если входная фильтрация отключена, кадры, классифицированные для VLAN, к которой порт не принадлежит, принимаются и пересылаются в коммутатор. Однако порт никогда не будет передавать кадры, классифицированные в VLAN, членом которых он не является.

Ingress Acceptance Входной прием
Гибридные порты позволяют изменять тип кадров, которые принимаются на входе.

Tagged and Untagged С тегом и без тега
Принимаются как теговые, так и нетегированные кадры. См. Тип порта для описания того, когда кадр считается помеченным.
Tagged Only Помечено только
На вход принимаются только кадры, помеченные соответствующим тегом типа порта.

Untagged Only Только без тегов
На вход принимаются только нетегированные кадры. См. Тип порта для описания того, когда кадр считается не маркированным.

Egress Tagging Выходная маркировка
Выходные теговые порты в магистральном и гибридном режимах могут контролировать тегирование кадров на выходе.

Untag Port VLAN Отключить порт VLAN
Кадры, отнесенные к порту VLAN, передаются без тегов. Другие кадры передаются с соответствующим тегом.

Tag All Пометить все
Все кадры, независимо от того, отнесены ли они к порту VLAN или нет, передаются с тегом.

Untag All Снять пометки со всех
Все кадры, независимо от того, отнесены ли они к порту VLAN или нет, передаются без тега.
Эта опция доступна только для портов в гибридном режиме.

Allowed VLANs Разрешенные VLANs порты в магистральном и гибридном режимах могут контролировать, в какие VLAN они могут входить. Порты доступа могут быть только членами одной VLAN, Access VLAN.
Синтаксис поля идентичен синтаксису, используемому в поле Enabled VLANs. По умолчанию магистральный или гибридный порт становится участником всех VLAN, поэтому для него установлено значение 1-4095.
Поле может быть оставлено пустым, это означает, что порт не станет членом каких-либо VLAN.

Forbidden VLANs Запрещенные VLAN
Порт может быть настроен так, чтобы никогда не становиться членом одной или нескольких VLAN. Это особенно полезно, когда динамические протоколы VLAN, такие как MVRP и GVRP, не должны динамически добавлять порты в VLAN.
Хитрость заключается в том, чтобы пометить такие VLAN как запрещенные на рассматриваемом порту.
Синтаксис идентичен синтаксису, используемому в поле Enabled VLANs.
По умолчанию поле остается пустым, что означает, что порт может стать участником всех возможных VLAN.

Нажмите «Save», чтобы сохранить Ваши настройки.

5.2 Port Isolation (Изоляция порта)

Изоляция портов предназначена для ограничения данных между портами. Это похоже на VLAN, но более строгое.

5.2.1 Port Group (Группа портов)

Этот коммутатор поддерживает группы портов. Члены группы портов могут пересылать дату.
Примечание: порт может принадлежать нескольким группам портов. Данные могут быть перенаправлены между любыми портами, которые принадлежат одной группе портов.

После нажатия «Advanced Configure»> «Port Isolation»> «Port Group» появится экран для создания группы портов.

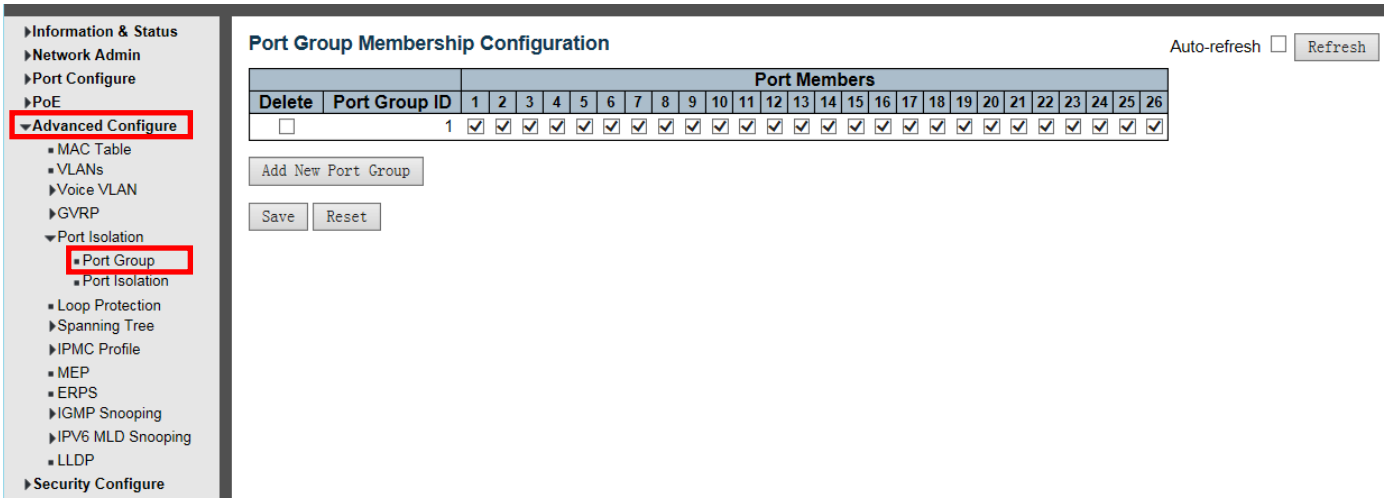


Рисунок 5-2-1 Экран конфигурации группы портов

Члены порта
Ряд флажков для каждого порта отображается для каждого идентификатора группы. Чтобы включить порт в группу, установите флажок.
Чтобы удалить или исключить порт из группы, убедитесь, что флажок снят. По умолчанию никакие порты не являются членами, и все поля сняты.

Нажмите «Save», чтобы сохранить Ваши настройки.

5.2.2 Port Isolation (Изоляция порта)

После нажатия "Advanced Configure">"Port Isolation">"Port Isolation", появится экран для выполнения настройки изоляции портов.

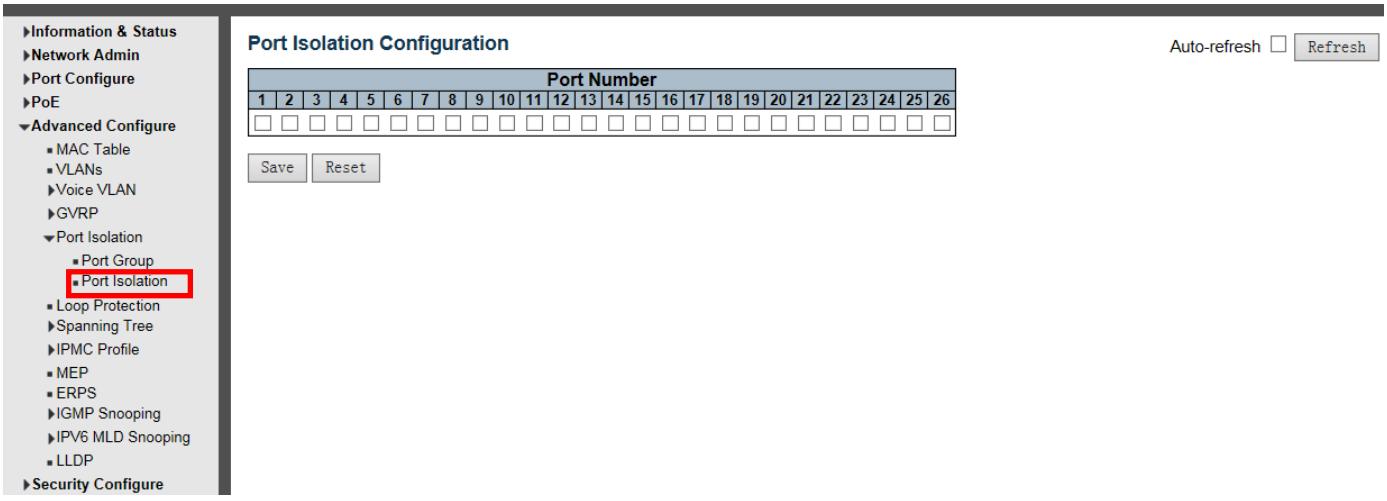


Рисунок 5-2-2 Экран конфигурации изоляции портов

Port Number Номер порта отметьте флажок, чтобы установить соответствующий порт в качестве изолированного порта, чтобы он не мог пересылать поток данных.
Нажмите «Save», чтобы сохранить Ваши настройки.

5.3 STP

Spanning Tree Protocol (STP)Протокол связующего дерева может использоваться для обнаружения и отключения сетевых петель, а также для обеспечения резервных каналов связи между коммутаторами, мостами или маршрутизаторами. Это позволяет коммутатору взаимодействовать с другими мостовыми устройствами в вашей сети, чтобы гарантировать, что между любыми двумя станциями в сети существует только один маршрут, и предоставлять резервные каналы, которые автоматически вступают во владение, когда основной канал отключается.

5.3.1 STP Bridge Settings (Настройки моста STP)

Эта страница позволяет вам настроить параметры порта STP. После нажатия «Advanced Configure»> «Spanning Tree»> «Bridge Settings» появится следующий экран.

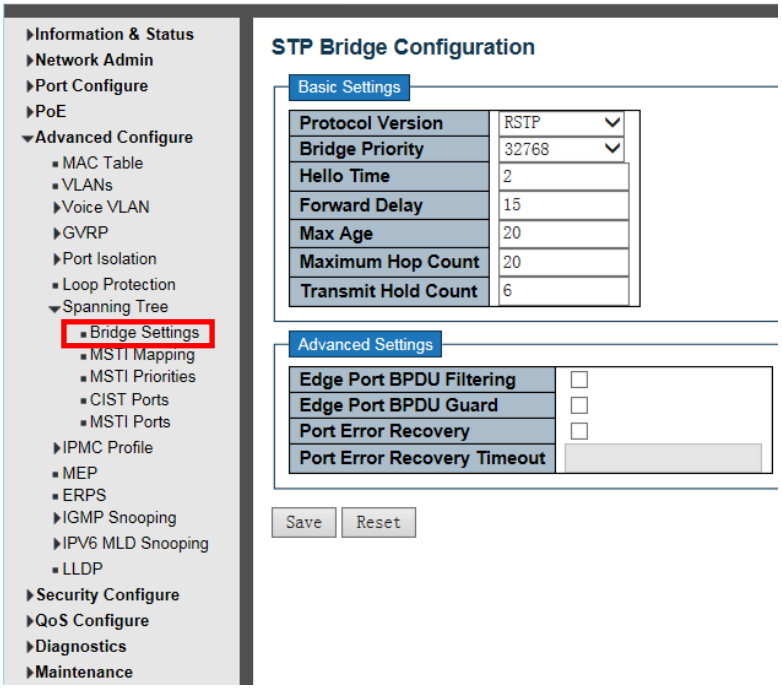


Рисунок 5-3-1 Экран конфигурации изоляции портов

На этой странице вы можете настроить параметры системы STP. Настройки используются всеми видами мостов STP Bridge в Коммутаторе.

Основные настройки

Protocol Version Версия протокола
Настройка версии протокола . Допустимые значения MSTP, RSTP и STP.
STP - Spanning Tree Protocol (IEEE802.1D);
RSTP - Rapid Spanning Tree Protocol (IEEE802.1w)
MSTP- Multiple Spanning Tree Protocol (IEEE802.1s)

Bridge Priority Приоритет моста
Управляет приоритетом моста. Более низкие числовые значения имеют лучший приоритет. Приоритет моста плюс номер экземпляра MSTI(, объединенный с 6-байтовым MAC-адресом коммутатора, образует идентификатор моста.

Для операции MSTP это приоритет CIST. В противном случае это приоритет моста STP / RSTP.

Hello Time Время приветствия
Интервал между отправкой STP BPDU. Допустимые значения находятся в диапазоне от 1 до 10 секунд, по умолчанию - 2 секунды.

Примечание. Изменение этого параметра по умолчанию не рекомендуется и может отрицательно повлиять на вашу сеть.

Forward Delay Задержка пересылки
Задержка, используемая мостами STP для транзита Root и Designated (корневого и назначенного) портов в переадресацию (используется в режиме, совместимом с STP). Допустимые значения находятся в диапазоне от 4 до 30 секунд.

Max Age Макс возраст
Максимальный возраст информации, передаваемой мостом, когда он является Root Bridge (корневым мостом). Допустимые значения находятся в диапазоне от 6 до 40 секунд, и MaxAge должно быть <= (FwdDelay-1) * 2.

Maximum Hop Count Максимальное количество прыжков
Это определяет начальное значение оставшихся переходов для информации MSTI, сгенерированной на границе области MSTI. Оно определяет, на сколько мостов корневой мост может распространять свою информацию BPDU. Допустимые значения находятся в диапазоне от 6 до 40 прыжков.

Transmit Hold Count Передача Hold Count
Количество BPDU, которые может послать мостовой порт в секунду. При превышении передача следующего BPDU будет отложена. Допустимые значения находятся в диапазоне от 1 до 10 BPDU в секунду.

Advanced Settings Расширенные настройки

Edge Port BPDU Filterin Фильтрация
Определите, будет ли порт, явно настроенный как Edge, передавать и получать BPDU.

Edge Port BPDU Guarв Охрана пограничного порта BPDU
Управляйте тем, будет ли порт, явно настроенный как Edge, отключаться при получении BPDU. Порт перейдет в состояние отключения по ошибке и будет удален из активной топологии.

Port Error Recovery Восстановление порта при ошибке
Определите, будет ли порт в состоянии отключения по ошибке автоматически включен через определенное время. Если восстановление не включено, порты должны быть отключены и повторно включены для нормальной работы STP. Условие также очищается перезагрузкой системы.

Port Error Recovery Timeout Тайм-аут восстановления порта при ошибке
. Время, по истечении которого порт может быть отключен из-за ошибки. Допустимые значения: от 30 до 86400 секунд (24 часа).

Нажмите «Save», чтобы сохранить Ваши настройки.

5.3.2 MSTI Mapping

Пользователи могут установить сопоставление. Нажмите «Advanced Configure»> «Spanning Tree»> «MSTI Mapping».

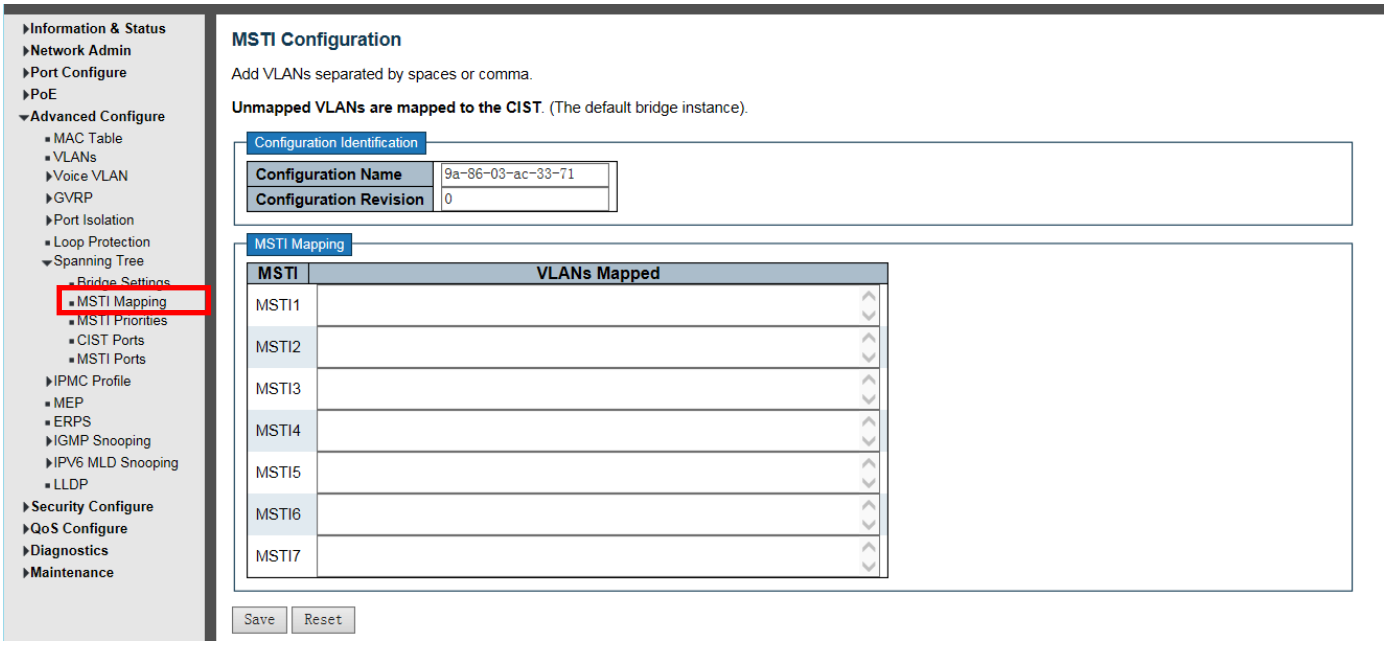


Рисунок 5-3-2 Экран конфигурации MSTI сопоставления

Configuration Name Имя конфигурации
Установить доменное имя MSTP

Configuration Revision Версия конфигурации
Установить ревизию конфигурации

MSTI Mapping MSTI сопоставление
Введите VLAN, которая требует сопоставления

Нажмите «Save», чтобы сохранить Ваши настройки.

5.3.3 MSTI Priorities Приоритеты MSTI

Пользователи могут устанавливать приоритеты MSTI, нажимая «Advanced Configure»> «Spanning Tree»> «MSTI Priorities»

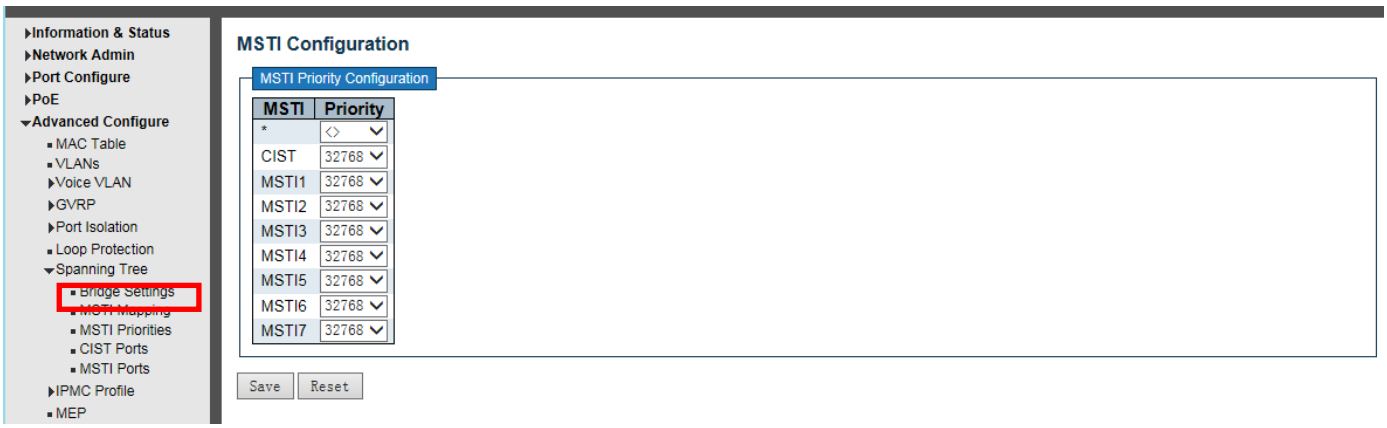


Рисунок 5-3-3 Экран конфигурации MSTI приоритетов

Эта страница позволяет пользователю проверить текущие конфигурации приоритетов экземпляра моста STP MSTI и, возможно, изменить их.

MSTI - Multiple Spanning-Tree Instances
Экземпляр моста. CIST является экземпляром по умолчанию, который всегда активен.

Priority Приоритет
Управляет приоритетом моста. Более низкие числовые значения имеют лучший приоритет. Приоритет моста плюс номер экземпляра MSTI, объединенный с 6-байтовым MAC-адресом коммутатора, образует идентификатор моста.

Примечание: значение приоритета должно быть кратно 4094, в диапазоне 0-61440

Нажмите «Save», чтобы сохранить Ваши настройки.

5.3.4 Порты CIST

Пользователи могут установить порты CIST, щелкнув «Advanced Configure»> «Spanning Tree»> « CIST Ports».
После нажатия «Advanced Configure»> «Spanning Tree»> «CIST Ports» появится следующий экран.

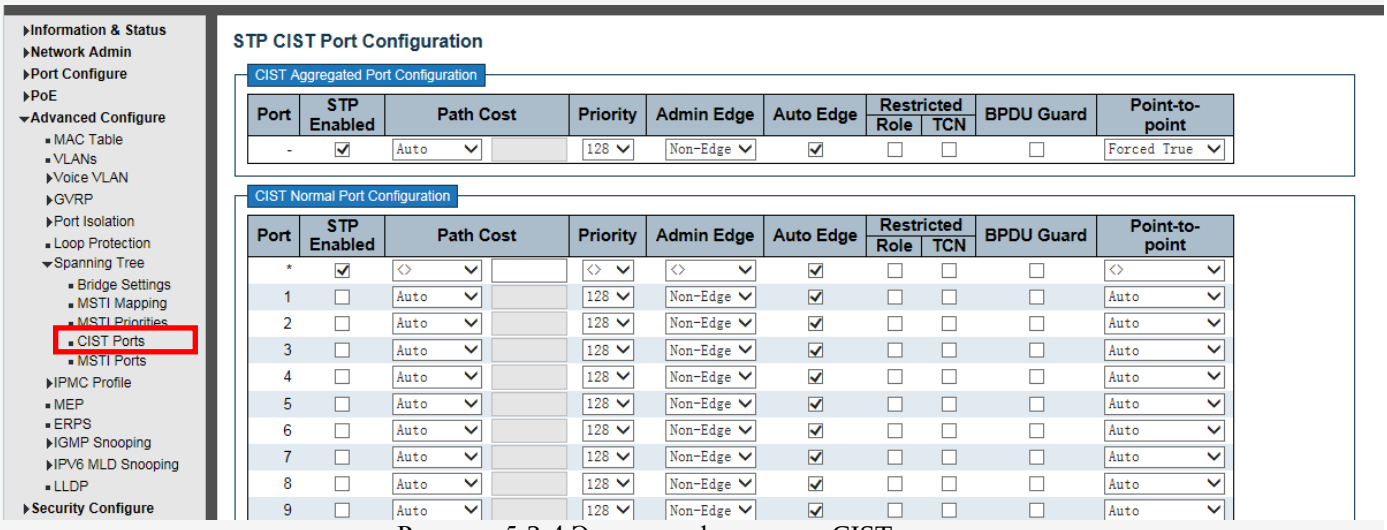


Рисунок 5-3-4 Экран конфигурации CIST портов

Эта страница позволяет пользователю проверить текущие конфигурации порта STP CIST и, возможно, изменить их.Эта страница содержит настройки для физических и агрегированных портов.

Port порт
Номер порта коммутатора логического порта STP.

STP Enabled включен
Управляет включением STP на этом порту коммутатора.

Path Cost Стоимость пути
Управляет стоимостью пути, который несет порт. Параметр Авто установит стоимость пути в зависимости от скорости физического канала, используя рекомендованные значения 802.1D. Используя параметр Specific, можно ввести пользовательское значение. Стоимость пути используется при установлении активной топологии сети. Порты с более низкой стоимостью пути выбираются в качестве портов переадресации в пользу портов с более высокой стоимостью пути. Допустимые значения находятся в диапазоне от 1 до 200000000.

Priority приоритет

Управляет приоритетом порта. Это может использоваться для контроля приоритета портов с одинаковой стоимостью порта. (См. Выше).

operEdge (флаг)
Операционный флаг, описывающий, подключен ли порт напрямую к периферийным устройствам. (Мосты не прилагаются). Переход в состояние пересылки происходит быстрее для пограничных портов (имеющих значение operEdge true), чем для других портов. Значение этого флага основано на полях AdminEdge и AutoEdge. Этот флаг отображается как Edge в Monitor-> Spanning Tree -> STP Детальный статус моста.

AdminEdge
Определяет, должен ли флаг operEdge начинаться как установленный или очищенный. (Начальное состояние operEdge при инициализации порта).

AutoEdge
Управляет тем, должен ли мост активировать автоматическое определение края на порте моста. Это позволяет получать operEdge из того, получены ли BPDU на порт или нет.

Restricted Role Ограниченная роль
Если этот параметр включен, порт не будет выбран в качестве корневого порта для CISTor для любого MSTI, даже если он имеет лучший вектор приоритета связующего дерева. Такой порт будет выбран в качестве альтернативного порта после выбора корневого порта. Если установлено, это может привести к отсутствию связности связующего дерева. Сетевой администратор может установить, чтобы мосты, внешние по отношению к основной области сети, не влияли на активную топологию связующего дерева, возможно, потому что эти мосты не находятся под полным контролем администратора. Эта функция также известна как Root Guard.

Restricted TCN Ограниченный TCN
Если этот параметр включен, порт не будет распространять полученные уведомления об изменении топологии и изменения топологии на другие порты. Если установлено, это может вызвать временную потерю соединения после изменений в активной топологии связующего дерева в результате постоянно неверной информации о местоположении изученной станции. Он устанавливается сетевым администратором для предотвращения внешних мостов по отношению к основной области сети, что приводит к сбросу адресов в этой области, возможно, из-за того, что эти мосты не находятся под полным контролем администратора или состояние физического канала подключенных локальных сетей часто проходит ,

BPDU Guard
Если включено, порт отключается при получении действительных BPDU. В отличие от аналогичного параметра моста, статус пограничного порта не влияет на этот параметр.
Порт, входящий в отключенное из-за ошибки состояние из-за этого параметра, также является объектом настройки восстановления порта моста.

Point-to-Point Точка-точка
Управляет подключением порта к локальной сети «точка-точка», а не к общей среде. Это может быть определено автоматически или принудительно, либо истинно, либо ложно. Переход в состояние пересылки происходит быстрее для двухточечных локальных сетей, чем для совместно используемых сред.

Нажмите «Save», чтобы сохранить Ваши настройки.

5.3.5 Порты MSTI

Пользователи могут установить порты MSTI, щелкнув «Advanced Configure»> «Spanning Tree»> « MSTI Ports». После нажатия «Advanced Configure»> «Spanning Tree»> « MSTI Ports» появится следующий экран.

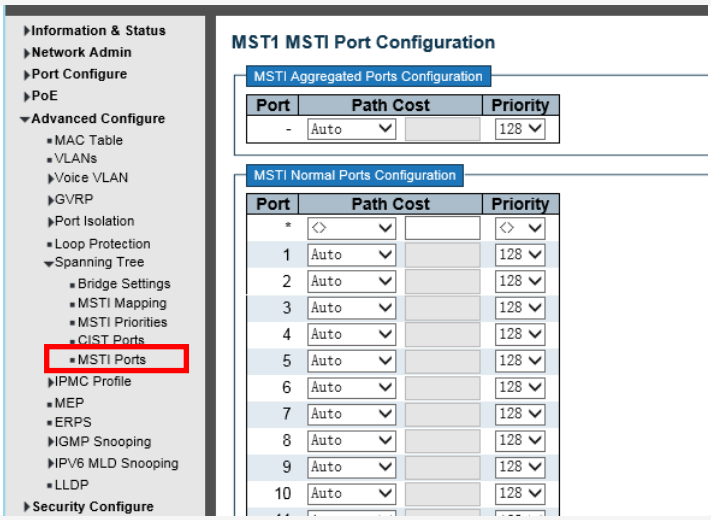


Рисунок 5-3-5 Экран конфигурации MSTI портов

Эта страница позволяет пользователю проверить текущие конфигурации порта STP MSTI и, возможно, изменить их.

Порт MSTI - это виртуальный порт, который создается отдельно для каждого активного (физического) порта CIST для каждого экземпляра MSTI, настроенного и применимого к порту. Экземпляр MSTI должен быть выбран перед отображением фактических параметров конфигурации порта MSTI.

Эта страница содержит настройки порта MSTI для физических и агрегированных портов.

Port порт

Номер порта коммутатора, соответствующего портам STP CIST (и MSTI).

Path Cost Стоимость пути

Управляет стоимостью пути, который несет порт. Параметр Авто установит стоимость пути в зависимости от скорости физического канала, используя рекомендованные значения 802.1D. Используя параметр Specific, можно ввести пользовательское значение. Стоимость пути используется при установлении активной топологии сети. Порты с более низкой стоимостью пути выбираются в качестве портов переадресации в пользу портов с более высокой стоимостью пути. Допустимые значения находятся в диапазоне от 1 до 200 000 000.

Priority приоритет

Управляет приоритетом порта. Это может использоваться для контроля приоритета портов с одинаковой стоимостью порта. (См. Выше).

Нажмите «Save», чтобы сохранить Ваши настройки.

5.3.6 MAC Address Table

На этой странице вы можете настроить параметры таблицы MAC адресов. После нажатия «Advanced Configure»> «Mac Table» появится экран, показанный ниже.

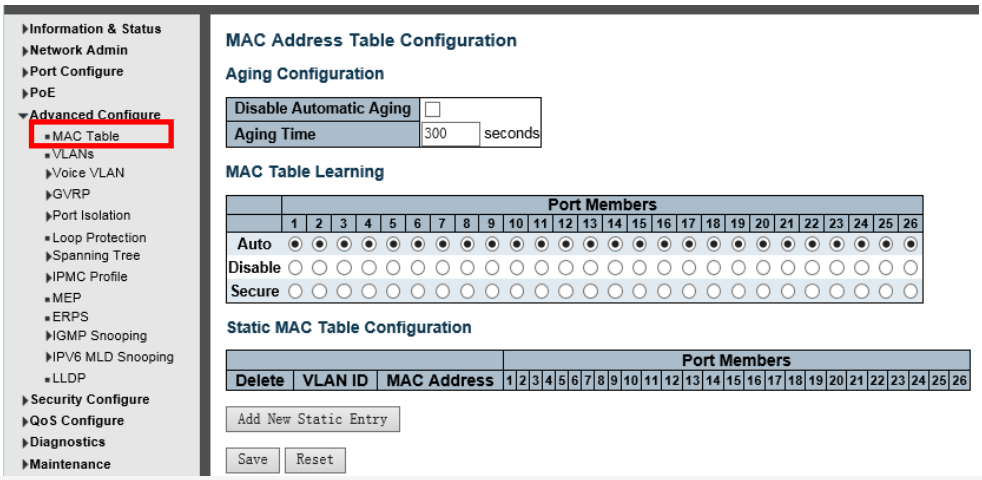


Рисунок 5-3-6 Экран конфигурации параметров таблицы MAC адресов

Таблица MAC-адресов настроена на этой странице. Установите таймауты для записей в динамической таблице MAC и настройте статическую таблицу MAC здесь.

Aging Configuration Конфигурация старения

По умолчанию динамические записи удаляются из таблицы MAC через 300 секунд. Это удаление также называется старением. Настройте время старения, введя значение здесь в секундах. Допустимый диапазон от 10 до 1000000 секунд. Отключите автоматическое устаревание динамических записей, установив флажок Disable automatic aging (Отключить автоматическое устаревание).

MAC Table Learning (Изучение таблицы MAC)

Если режим обучения для данного порта неактивен, другой модуль контролирует этот режим, поэтому пользователь не может его изменить. Примером такого модуля является Аутентификация на основе MAC под 802.1X.

Каждый порт может выполнять обучение на основе следующих настроек:

AutoАвто

Обучение выполняется автоматически, как только получен кадр с неизвестным SMAC.

Disable Отключить

Нет обучения не сделано.

Secure Безопасный

Изучаются только статические записи MAC, все остальные кадры отбрасываются.

Примечание. Перед переходом в безопасный режим обучения убедитесь, что ссылка, используемая для управления коммутатором, добавлена в таблицу Static Mac. В противном случае канал управления теряется и может быть восстановлен только с помощью другого незащищенного порта или подключения к коммутатору. через последовательный интерфейс.

Конфигурация статической таблицы MAC

Статические записи в таблице MAC показаны в этой таблице. Статическая таблица MAC может содержать 64 записи.

Таблица MAC сортируется сначала по идентификатору VLAN ID, а затем по MAC-адресу.

Delete Удалить

Проверьте, чтобы удалить запись. Он будет удален во время следующего сохранения.

VLAN ID

Идентификатор VLAN записи.

MAC-адрес

MAC-адрес записи.

Port Members Члены порта

Галочки указывают, какие порты являются членами записи. Установите или снимите флажок, если необходимо изменить запись.

Adding a New Static Entry Добавление новой статической записи

Нажмите, чтобы добавить новую запись в статическую таблицу MAC. Укажите идентификатор VLAN, MAC-адрес и Port Members для новой записи.

Нажмите «Save», чтобы сохранить Ваши настройки.

5.4 IGMP Snooping (Отслеживание IGMP)

Internet Group Management Protocol (IGMP) Протокол управления группами Интернета (IGMP) позволяет хосту и маршрутизаторам обмениваться информацией о членстве в многоадресных группах. Отслеживание IGMP - это функция переключения, которая контролирует обмен сообщениями IGMP и копирует их в ЦПУ для обработки функций. Общая цель IGMP Snooping - ограничить пересылку многоадресных кадров только на порты, которые являются членами многоадресной группы..

5.4.1 Базовая конфигурация

После нажатия «Advanced Configure»> «IGMP Snooping»> «Basic Configuration» появится следующий экран.

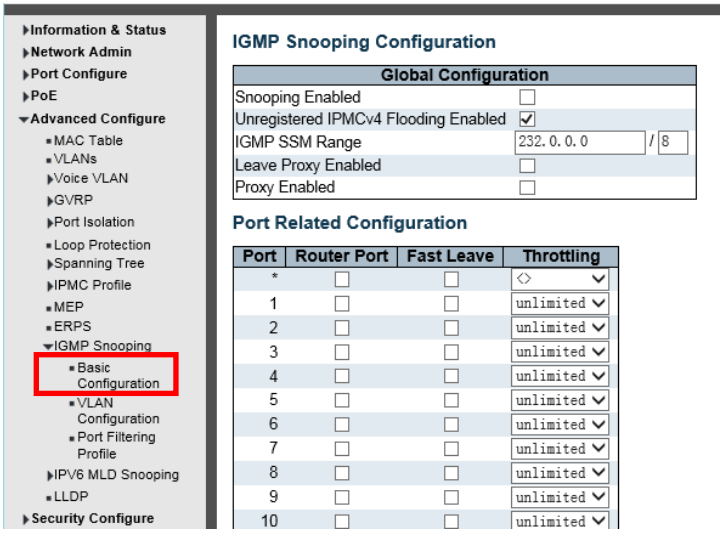


Рисунок 5-4-1 Экран базовой конфигурации IGMP Snooping

Snooping Enabled Отслеживание включено

Включить Global IGMP Snooping.

Незарегистрированное наводнение IPMCv4 включено

Включить незарегистрированный поток трафика IPMCv4.

Контроль затопления вступает в силу только тогда, когда IGMP Snooping включен. Когда IGMP Snooping отключен, незарегистрированный поток трафика IPMCv4 всегда активен, несмотря на этот параметр.

IGMP SSM Range

Диапазон SSM (Source-Specific Multicast) позволяет хостам и маршрутизаторам с поддержкой SSM запускать модель обслуживания SSM для групп в диапазоне адресов. В качестве префикса назначьте действительный адрес многоадресной рассылки IPv4 с длиной префикса (от 4 до 32) для диапазона.

Leave Proxy Enabled Оставьте прокси включенным

Включить IGMP Leave Proxy. Эту функцию можно использовать, чтобы избежать пересылки ненужных сообщений о выходе на сторону маршрутизатора.

Proxy Enabled Прокси включен

Включить IGMP Proxy. Эту функцию можно использовать, чтобы избежать пересылки ненужного соединения и оставлять сообщения на стороне маршрутизатора.

Router Port Порт маршрутизатора

Укажите, какие порты действуют как порты маршрутизатора. Порт маршрутизатора - это порт на коммутаторе Ethernet, который ведет к устройству многоадресной рассылки уровня 3 или к IGMP-запросу.
Если порт участника агрегации выбран в качестве порта маршрутизатора, вся агрегация будет действовать как порт маршрутизатора.

Fast Leave Быстрый выход
Включите быстрый выход в порт.
Система удалит групповую запись и прекратит пересылку данных после получения сообщения о выходе, не отправляя сообщения запроса последнего участника. Рекомендуется включать эту функцию только в том случае, если к конкретному порту подключен один хост IGMPv2.

Throttling
Включите, чтобы ограничить количество групп многоадресной рассылки, к которым может принадлежать порт коммутатора.

Нажмите «Save», чтобы сохранить Ваши настройки.

5.4.2 IGMP Snooping VLAN Configuration (конфигурация VLAN отслеживания IGMP)

После нажатия «Advanced Configure»> «IGMP Snooping»> «VLAN Configuration», появится следующий экран.

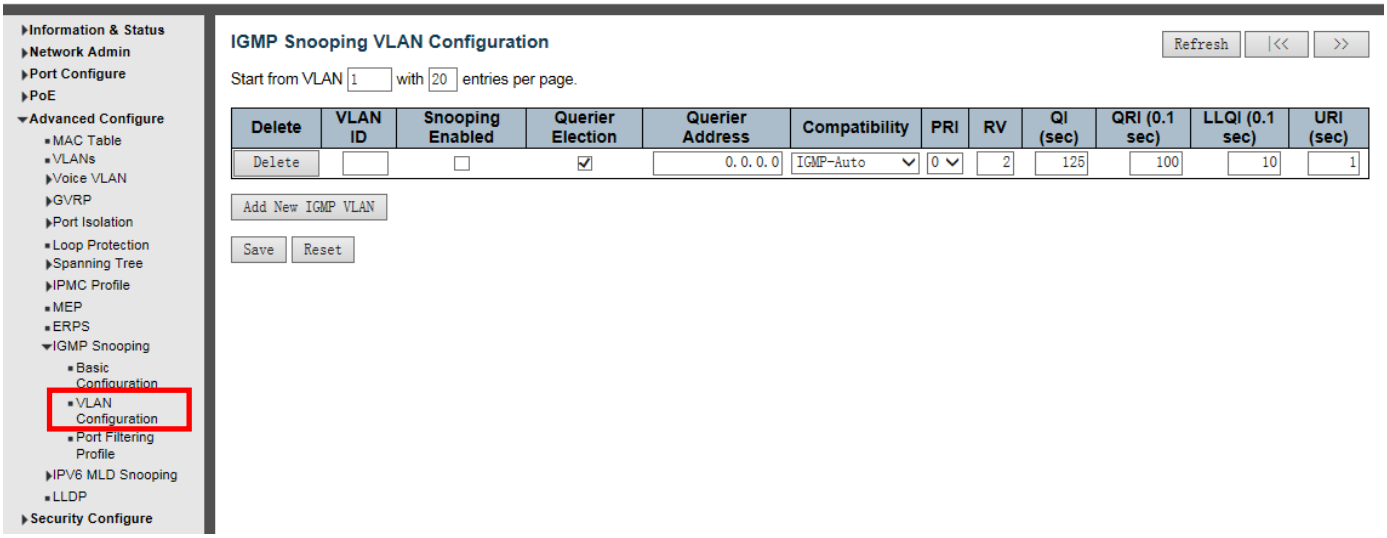


Рисунок 5-4-2 Экран конфигурации VLAN IGMP Snooping

На каждой странице отображается до 99 записей из таблицы VLAN, по умолчанию 20, выбираемых через поле ввода «записей на страницу». При первом посещении веб-страницы будут отображаться первые 20 записей в начале таблицы VLAN. Первым будет отображаться тот, у которого в таблице VLAN найден самый низкий VLAN ID.
Поля ввода «VLAN» позволяют пользователю выбрать начальную точку в таблице VLAN. Нажатие на кнопку обновит отображаемую таблицу, начиная с этого или следующего ближайшего соответствия таблицы VLAN. Последняя будет использовать последнюю отображаемую запись в качестве основы для следующего поиска. Когда достигнут конец, в отображаемой таблице появится текст «Больше нет записей». Используйте кнопку, чтобы начать все сначала.

IGMP Snooping VLAN Столбцы таблицы

DeleteУдалить
Проверьте, чтобы удалить запись. Назначенная запись будет удалена при следующем сохранении.

VLAN ID
Идентификатор VLAN записи.

IGMP Snooping enabled включен

Включите отслеживание IGMP для каждой VLAN. Для отслеживания IGMP можно выбрать до 32 VLAN.

Querier Election Выбор главного маршрутизатора
Включите, чтобы присоединиться к выборам IGMP Querier в VLAN. Отключите если действовать в качествк IGMP-незапрашивающего.

Querier Address Адрес главного маршрутизатора
Определите адрес IPv4 как адрес источника, используемого в заголовке IP для IGMP Querier Election. Если адрес Querier не задан, система использует IPv4-адрес управления IP-интерфейса, связанного с этой VLAN.
Если адрес управления IPv4 не задан, система использует первый доступный адрес управления IPv4.
В противном случае система использует предопределенное значение. По умолчанию это значение будет 192.0.2.1.

Compatibility Совместимость
Совместимость поддерживается хостами и маршрутизаторами, выполняющими соответствующие действия в зависимости от версий IGMP, работающих на хостах и маршрутизаторах в сети.
Разрешенный выбор: IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3, значение совместимости по умолчанию - IGMP-Auto.

PRI
Priority of Interface. Приоритет интерфейса.
Указывает уровень приоритета кадра управления IGMP, сгенерированный системой. Эти значения могут использоваться для определения приоритетов разных классов трафика.
Допустимый диапазон - от 0 (максимальное усилие) до 7 (максимальное), значение приоритета интерфейса по умолчанию - 0.

R.V.(Robustness Variable Переменная надежности)
Переменная Robustness Variable позволяет настраивать ожидаемую потерю пакетов в сети.
Допустимый диапазон - от 1 до 255, значение переменной устойчивости по умолчанию - 2.

QI (Query Interval Интервал запроса)
Интервал запроса - это интервал между общими запросами, отправляемыми запрашивающим.
Допустимый диапазон - от 1 до 31744 секунд, интервал запроса по умолчанию - 125 секунд.

QRI (Query Response Interval Интервал ответа на запрос)
Максимальная задержка ответа, используемая для расчета максимального кода ответа, вставляемого в периодические общие запросы.
Допустимый диапазон от 0 до 31744 за десятые секунды, интервал ответа на запрос по умолчанию - 100 за десятые секунды (10 секунд).

LLQI (LMQI для IGMP) Last Member Query Interval Интервал запроса последнего участника.
Время запроса последнего участника - это значение времени, представленное интервалом последнего запроса участника, умноженное на количество последнего запроса участника.
Допустимый диапазон - от 0 до 31744 в десятых долях секунды, интервал запроса последнего участника по умолчанию - 10 в десятых долях секунды (1 секунда).

URI (Unsolicited Report Interval Интервал незапрашиваемых отчетов).
Интервал незапрашиваемых отчетов - это время между повторениями первоначального отчета хоста о членстве в группе.
Допустимый диапазон - от 0 до 31744 секунд, интервал незапрашиваемых отчетов по умолчанию - 1 секунда.

Нажмите «Save», чтобы сохранить Ваши настройки.

5.4.3 Port Filtering Profile Профиль фильтрации портов

Установите профиль фильтрации портов, нажмите “Advanced Configure”>“IGMP Snooping”>“Port Filtering Profile”

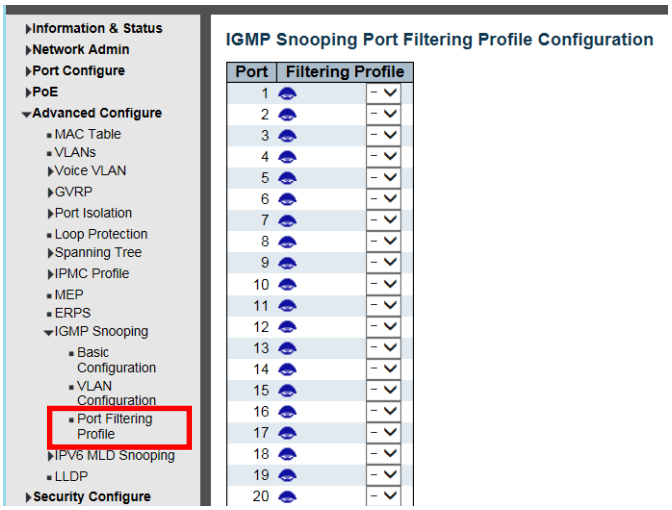


Рисунок 5-4-3 Экран настройки профиля фильтрации портов

Port порт
Логический порт для настроек.

Filtering Profile Профиль фильтрации
Выберите профиль IPMC в качестве условия фильтрации для определенного порта. Сводка о назначенном профиле будет отображаться при нажатии на кнопку просмотра.

Profile Management Button Кнопка управления профилем
Вы можете проверить правила назначенного профиля с помощью следующей кнопки: 

Нажмите «Save», чтобы сохранить Ваши настройки.

5.5 IPMC Profile (Профиль IPMC)

Пользователи могут установить фильтр многоадресного списка, нажмите “Advanced Configure” > “IPMC Profile” > “Address Entry”

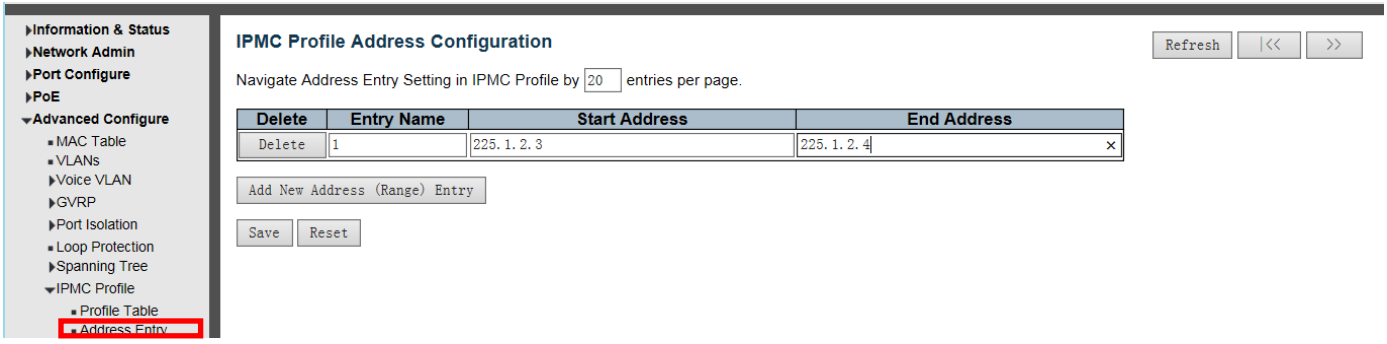


Рисунок 5-5-1 Экран настройки профиля адресов IPMC

Entry Name Имя входа Введите имя группы для фильтрации
Start Address Начальный адрес Введите адрес стартовой группы
End Address Конечный адрес Введите адрес конечной группы

Нажмите «Save», чтобы сохранить Ваши настройки.

Свяжите список многоадресной рассылки фильтра, нажмите “Advanced Configure”>“IPMC Profile”>“ Profile Table

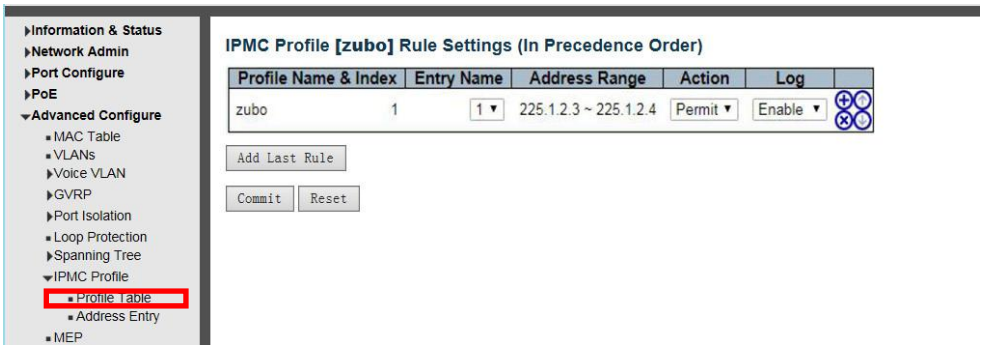


Рисунок 5-5-2 Экран настройки правила фильтрации для определенного профиля IPMC.

Profile Name Имя профиля
Имя назначенного профиля, который будет связан. Это поле не доступно для редактирования.

Entry Name Имя входа
Имя, используемое при указании диапазона адресов, используемого для этого правила.
Только выбранные записи адреса профиля будут выбраны в выбранном поле. Это поле не может быть выбрано как none ("-"), пока таблица настроек правила зафиксирована.

Address Range Диапазон адресов
Соответствующий диапазон адресов выбранной записи профиля. Это поле недоступно для редактирования и будет корректироваться автоматически в соответствии с выбранной записью профиля.

Action действие
Указывает обучающее действие при получении фрейма Join / Report, в котором групповой адрес соответствует диапазону адресов правила.

Permit Разрешить: групповой адрес соответствует диапазону, указанному в правиле.
Deny Запретить: адрес группы, соответствующий диапазону, указанному в правиле, будет удален.

Log Журнал
Указывает предпочтение ведения журнала после получения фрейма Join / Report, в котором групповой адрес соответствует диапазону адресов правила.

Enable Включить: Будет записана информация о групповом адресе, соответствующая диапазону, указанному в правиле.
Disable Отключить: Информация о групповом адресе, соответствующая диапазону, указанному в правиле, не будет регистрироваться.

Rule Management Buttons Кнопки управления правилами
Вы можете управлять правилами и соответствующим порядком приоритета, используя следующие кнопки:

: вставить новое правило перед текущей записью правила.
: Удалить текущую запись правила.
: перемещает текущую запись правила вверх в списке.
: перемещает текущую запись правила вниз по списку

5.6 IPV6 MLD Snooping

IPV6 MLD Snooping - это механизм многоадресного управления и контроля, работающий на коммутаторе Ethernet уровня 2

При включении отслеживания MLD IPV6 коммутатор получает сообщение MLD IPV6 путем прослушивания каждого интерфейса, для обмена интерфейса и группы многоадресной рассылки отношениями сопоставления адресов интерфейса и, в соответствии с этим, устанавливает отношения сопоставления для пересылки потока многоадресных данных.

5.6.1 Basic Configuration (Базовая конфигурация)

Нажмите «Advanced Configure»> «IPv6 MLD Snooping»> «Basic Configuration», чтобы проверить информацию о конфигурации IPv6 MLD Snooping.

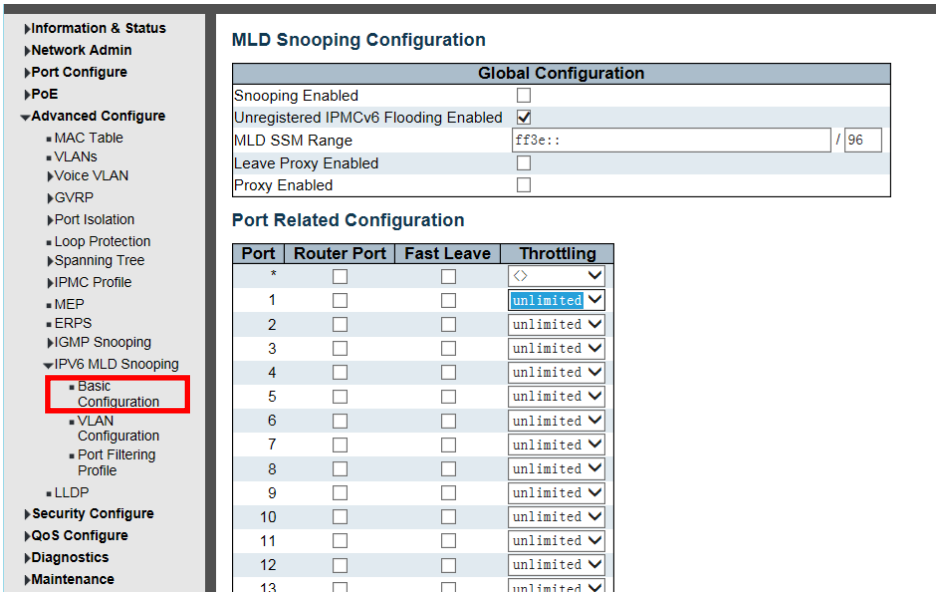


Рисунок 5-6-1 Базовая настройка IGMP Snooping

Snooping Enabled Отслеживание включено

Включить Global IGMP Snooping.

Незарегистрированное наводнение IPMCv6 включено

Включить незарегистрированный поток трафика IPMCv6.

Контроль затопления вступает в силу только тогда, когда MLD Snooping включен. Когда MLD Snooping отключен, незарегистрированный поток трафика IPMCv6 всегда активен, несмотря на этот параметр.

MLD SSM Range

Диапазон SSM (Source-Specific Multicast) позволяет хостам и маршрутизаторам с поддержкой SSM запускать модель обслуживания SSM для групп в диапазоне адресов. В качестве префикса назначьте действительный адрес многоадресной рассылки IPv6 с длиной префикса (от8 до 32) для диапазона.

Leave Proxy Enabled Оставьте прокси включенным

Включить MLD Leave Proxy. Эту функцию можно использовать, чтобы избежать пересылки ненужных сообщений о выходе на сторону маршрутизатора.

Proxy Enabled Прокси включен

Включить MLD Proxy. Эту функцию можно использовать, чтобы избежать пересылки ненужного соединения и оставлять сообщения на стороне маршрутизатора.

Router Port Порт маршрутизатора

Укажите, какие порты действуют как порты маршрутизатора. Порт маршрутизатора - это порт на коммутаторе Ethernet, который ведет к устройству многоадресной рассылки уровня 3 или к MLD-запросу.

Если порт участника агрегации выбран в качестве порта маршрутизатора, вся агрегация будет действовать как порт маршрутизатора.

Fast Leave Быстрый выход
Включите быстрый выход в порт.
Система удалит групповую запись и прекратит пересылку данных после получения сообщения о выходе, не отправляя сообщения запроса последнего участника. Рекомендуется включать эту функцию только в том случае, если к конкретному порту подключен один хост MLDv1.

Throttling
Включите, чтобы ограничить количество групп многоадресной рассылки, к которым может принадлежать порт коммутатора.

Нажмите «Save», чтобы сохранить Ваши настройки.

5.6.2 VLAN Configuration (конфигурация VLAN)

Нажмите «Advanced Configure»> «IPv6 MLD Snooping»> «VLAN Configuration», чтобы проверить информацию о конфигурации IPv6 MLD Snooping.

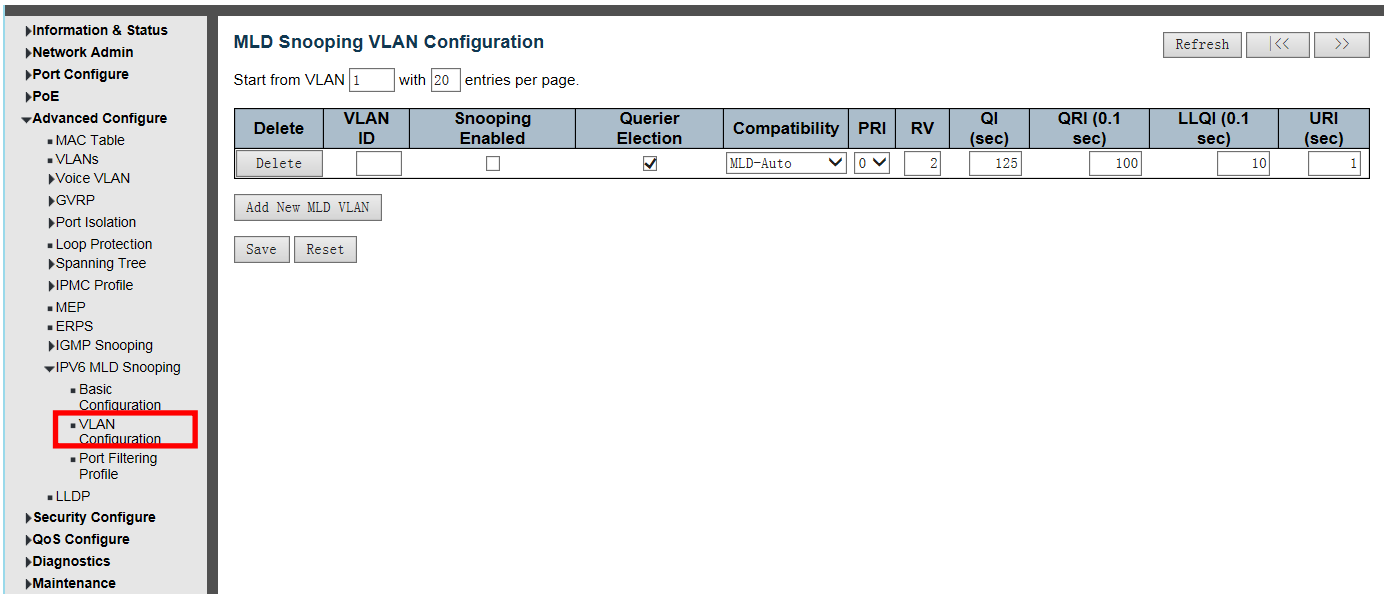


Рисунок 5-6-2 Экран конфигурации IPV6 MLD Snooping

MLD Snooping VLAN Столбцы таблицы

DeleteУдалить
Проверьте, чтобы удалить запись. Назначенная запись будет удалена при следующем сохранении.

VLAN ID
Идентификатор VLAN записи.

MLD Snooping enabled включен
Включите отслеживание MLD для каждой VLAN. Для отслеживания MLD можно выбрать до 32 VLAN.

Querier Election Выбор главного маршрутизатора
Включите, чтобы присоединиться к выборам MLD Querier в VLAN. Отключите если действовать в качествк MLD-незапрашивающего.

Compatibility Совместимость

Совместимость поддерживается хостами и маршрутизаторами, выполняющими соответствующие действия в зависимости от версий MLD, работающих на хостах и маршрутизаторах в сети.
Разрешенный выбор: MLD-Auto, Forced MLDv1, Forced MLDv2, значение совместимости по умолчанию - MLD-Auto.

PRI Priority of Interface. Приоритет интерфейса.
Указывает уровень приоритета кадра управления MLD, сгенерированный системой. Эти значения могут использоваться для определения приоритетов разных классов трафика.
Допустимый диапазон - от 0 (максимальное усилие) до 7 (максимальное), значение приоритета интерфейса по умолчанию - 0.

R.V.(Robustness Variable Переменная надежности)
Переменная Robustness Variable позволяет настраивать ожидаемую потерю пакетов в сети.
Допустимый диапазон - от 1 до 255, значение переменной устойчивости по умолчанию - 2.

QI (Query Interval Интервал запроса)
Интервал запроса - это интервал между общими запросами, отправляемыми запрашивающим.
Допустимый диапазон - от 1 до 31744 секунд, интервал запроса по умолчанию - 125 секунд.

QRI (Query Response Interval Интервал ответа на запрос)
Максимальная задержка ответа, используемая для расчета максимального кода ответа, вставляемого в периодические общие запросы.
Допустимый диапазон от 0 до 31744 за десятые секунды, интервал ответа на запрос по умолчанию - 100 за десятые секунды (10 секунд).

LLQI Last Listener Query Interval Интервал запроса последнего прослушивателя.
Интервал запроса последнего прослушивателя - это максимальная задержка ответа, используемая для расчета максимального кода ответа, вставленного в запросы на адрес многоадресной рассылки, отправленные в ответ на сообщения прослушивателя многоадресной рассылки версии 1. Это также Максимальная задержка ответа, используемая для расчета максимального кода ответа, вставленного в сообщения многоадресного адреса и запроса конкретного источника.
Допустимый диапазон: от 0 до 31744 в десятых долях секунды, по умолчанию интервал последнего прослушивателя составляет 10 в десятых долях секунды (1 секунда).
URI (Unsolicited Report Interval Интервал незапрашиваемых отчетов).
Интервал незапрашиваемых отчетов - это время между повторениями первоначального отчета хоста о членстве в группе.
Допустимый диапазон - от 0 до 31744 секунд, интервал незапрашиваемых отчетов по умолчанию - 1 секунда.

Нажмите «Save», чтобы сохранить Ваши настройки.

5.7 ERPS

ERPS (Ethernet Ring Protection Switching), он объединяет функцию OAM и протокол APS. Он обеспечивает быструю защиту и восстановление коммутации трафика Ethernet в кольцевой топологии, а также гарантирует отсутствие петель на уровне Ethernet. Если кольцевая сеть была случайно прервана, время восстановления после сбоя может составить менее 50 мс, чтобы быстро вернуть сеть в нормальное состояние. ITU-T G.8032 является первым отраслевым стандартом для ERPS.

Примечание. Перед включением ERPS STP кольцевого порта должен быть отключен. ,

После нажмите "Advanced Configure">"ERPS ", после чего появится экран.

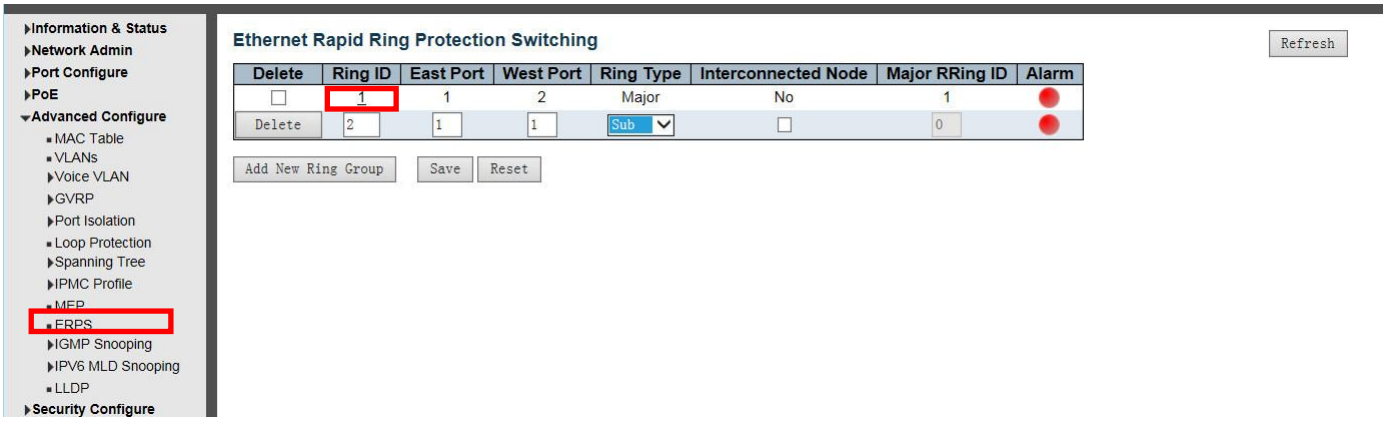


Рисунок 5-7-1 Конфигурация EPRS

Ring ID ERPS Ring ID Идентификатор созданной группы защиты. Это должно быть целочисленное значение от 1 до 64. Максимальное число групп защиты ERPS, которое можно создать, составляет 64.

East Port Восточный Порт
Номер порта, который участвует в защите этого кольца.

West Port Западный Порт
Номер другого порта, который участвует в защите этого кольца.

Ring Type Тип кольца
Доступный выбор: " Major Ring " или " Sub Ring ". «Sub Ring» требуется для настройки только в случае применения Multi Ring,. Ring Type по умолчанию: " Major Ring ".

Interconnected Node Взаимосвязанный узел
В случае применения Multi Ring Interconnected Node - это узел, который соединяет 2 или более колец.

Major Ring ID
В случае применения Single Ring идентификатор Major Ring совпадает с идентификатором кольца. В приложении Multi Ring Sub Ring должен быть введен как Major Ring ID.
Идентификатор главной кольцевой группы для взаимосвязанного подкольца. Он используется для отправки обновлений об изменениях топологии на основном кольце. Если кольцо является основным, это значение совпадает с идентификатором группы защиты этого кольца.

Нажмите «Save», чтобы сохранить Ваши настройки.

После щелчка по номеру под «Ring ID» откроется страница для Ring Configuration, как показано на следующем экране:

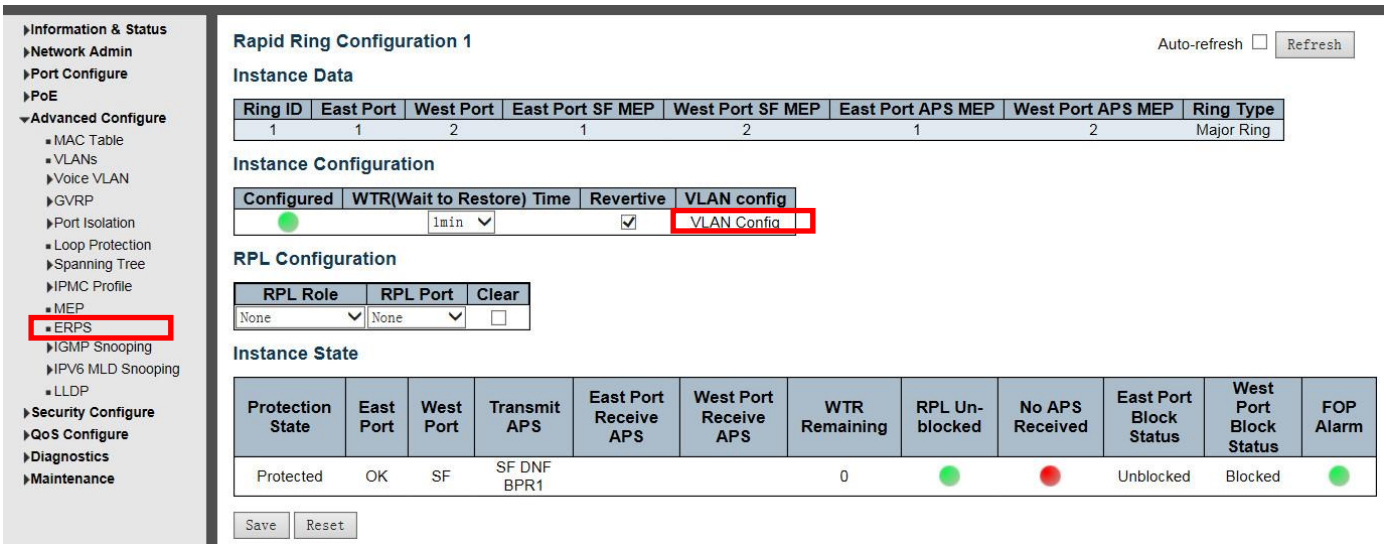


Рисунок 5-7-2 Конфигурация кольца

Время WTR (ожидание восстановления) (1-12)
Щелкните раскрывающееся меню, чтобы выбрать время WTR для R-APS. Доступный выбор: 1-12 мин. По умолчанию: 1 мин.
Revertive Установите этот флажок, чтобы включить реверсивный статус R-APS.
VLAN config Конфигурация VLAN
После нажатия «Конфигурация VLAN» откроется страница Rapid Ring VLAN Configuration.
RPLRole
Щелкните раскрывающееся меню, чтобы выбрать роль "None", "RPL Owner", or "RPL Neighbor" role(«No», «Владелец RPL» или «Сосед RPL»).
RPL Port Порт RPL
Щелкните раскрывающееся меню, чтобы выбрать "None", "East Port", or "West Port". («No», «Восточный порт» или «Западный порт»).

Нажмите «Save», чтобы сохранить активные настройки.

После нажатия кнопки «VLAN config» откроется страница Rapid Ring VLAN Configuration, как показано на следующем экране:

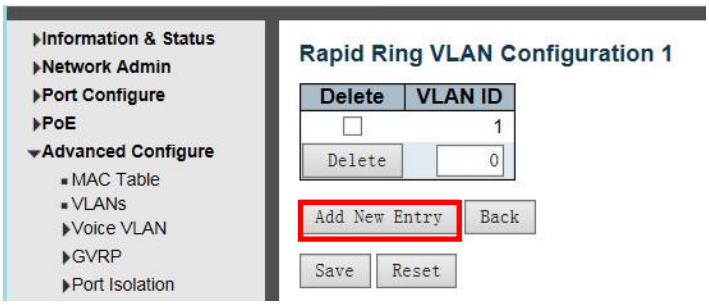


Рисунок 5-7-3 Конфигурация быстрой настройки кольца VLAN

Нажмите «Add New Entry», чтобы создать новую запись.
Нажмите «Save», чтобы сохранить активные настройки.

5.8 LLDP (Link Layer Discovery Protocol)

Протокол обнаружения канального уровня (LLDP) используется для обнаружения основной информации о соседних устройствах на локальных доменах широковещательной передачи. LLDP - это протокол уровня 2, который использует периодические широковещательные рассылки для рекламы информация об отправляющем

устройстве. Объявленная информация представлена в формате Type Length Value (TLV) (значение длины типа (TLV) в соответствии со стандартом IEEE 802.1ab и может включать такие детали, как идентификация устройства, возможности и параметры конфигурации. LLDP также определяет, как хранить и поддерживать собранную информацию о соседних узлах сети, которые он обнаруживает.

После нажатия «Advanced Configure»> «LLDP» появится следующий экран.

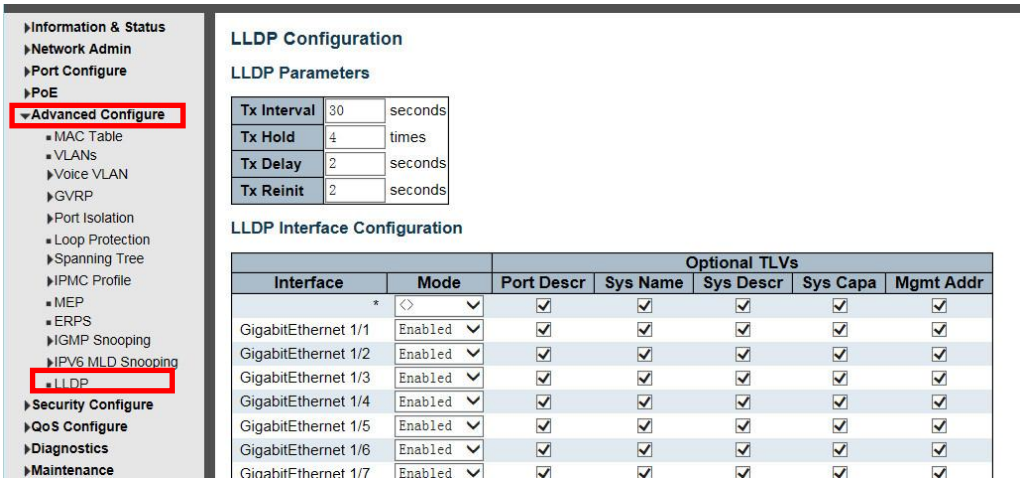


Рисунок 5-8 Экран конфигурации LLDP

Параметры LLDP

Tx Interval

Коммутатор периодически передает кадры LLDP своим соседям, чтобы информация об обнаружении сети была актуальной. Интервал между каждым кадром LLDP определяется значением Tx Interval. Допустимые значения ограничены 5–32768 секундами.

Tx Hold

Каждый кадр LLDP содержит информацию о том, как долго информация в кадре LLDP должна считаться действительной. Период действия информации LLDP устанавливается равным Tx Hold, умноженному на Tx Interval в секундах. Допустимые значения ограничены 2 - 10 разами.

Tx Delay Задержка передачи

Если некоторая конфигурация изменена (например, IP-адрес), передается новый кадр LLDP, но время между кадрами LLDP всегда будет не меньше значения секунд задержки передачи. Задержка передачи не может быть больше 1/4 значения интервала передачи. Допустимые значения ограничены 1-8192 секундами.

Tx Reinit

Когда интерфейс отключен, LLDP отключен или коммутатор перезагружается, кадр завершения LLDP передается соседним устройствам, сигнализируя, что информация LLDP больше не действительна. Tx Reinit контролирует количество секунд между кадром выключения и новой инициализацией LLDP. Допустимые значения ограничены 1–10 секундами.

LLDP Interface Configuration Конфигурация интерфейса LLDP

Interface Интерфейс

Имя интерфейса коммутатора логического интерфейса LLDP.

Mode Режим

Выберите режим LLDP.

Rx only Только Rx Коммутатор не будет отправлять информацию LLDP, но информация LLDP от соседних устройств анализируется.

Tx only Только Tx Коммутатор отбрасывает информацию LLDP, полученную от соседей, но отправляет информацию LLDP.

Disabled Отключено Коммутатор не отправляет информацию LLDP и отбрасывает информацию LLDP, полученную от соседей.

Enabled Включено Коммутатор будет отправлять информацию LLDP и анализировать информацию LLDP, полученную от соседей.

Port Descr Порт Описание

Optional TLV Необязательный TLV: если этот флажок установлен, «описание порта» включается в передаваемую информацию LLDP.

Sys Name Имя системы

Optional TLV Необязательный TLV: если этот флажок установлен, «описание имени системы» включается в передаваемую информацию LLDP.

Sys Descr

Optional TLV Необязательный TLV: если этот флажок установлен, «описание системы» включается в передаваемую информацию LLDP.

Sys Capa

Optional TLV Необязательный TLV: если этот флажок установлен, «возможности системы» включается в передаваемую информацию LLDP.

Mgmt Addr

Optional TLV Необязательный TLV: если этот флажок установлен, «адрес управления» включается в передаваемую информацию LLDP.

Нажмите «Save», чтобы сохранить Ваши настройки.

5.9 Loop Protection (Защита от петель)

Защита от петель предназначена для предотвращения петель вещания.
Нажмите "Advanced Configure">"Loop Protection" , появится экран.

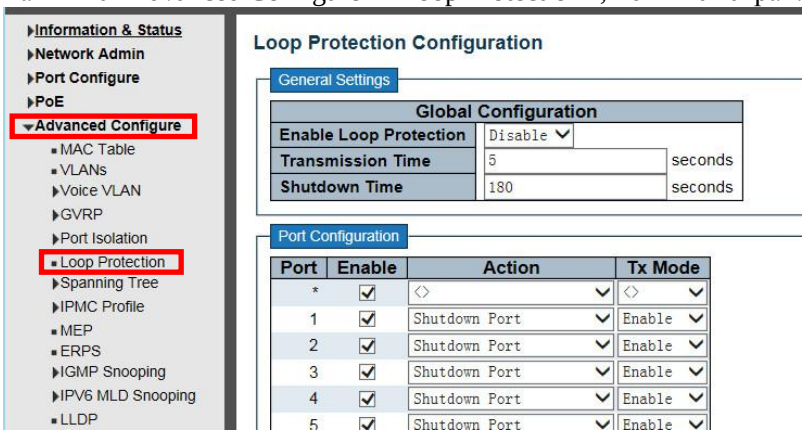


Рисунок 5-9 Экран настройки защиты от петель

General Settings общие настройки

Enable Loop Protection

Включить защиту от петель

Контролирует, включена ли защита от петель (в целом).

Transmission Time Время передачи

Интервал между каждым PDU защиты от петель, отправленным на каждый порт. Допустимые значения: от 1 до 10 секунд. Значение по умолчанию - 5 секунд.

Shutdown Time Время выключения

Период (в секундах), в течение которого порт будет отключен в случае обнаружения петли (и действие порта отключает порт). Допустимые значения: от 0 до 604800 секунд (7 дней). При нулевом значении порт будет отключен (до следующего перезапуска устройства). Значение по умолчанию - 180 секунд.

Port Configuration Конфигурация порта

Port порт

Номер порта коммутатора порта.

Enable включить

Управляет включением защиты от петель на этом порту коммутатора.

Action действие

Настраивает действие, выполняемое при обнаружении петли на порту. Допустимые значения: Порт выключения, Порт выключения и Журнал или Только журнал.

Tx Mode Режим Tx
Определяет, активно ли порт генерирует PDU защиты от петель или просто пассивно ищет PDU с петлей.

Нажмите «Save», чтобы сохранить Ваши настройки.

6. QoS Configure

Quality of Service (QoS) (англ. quality of service «качество обслуживания») — технология предоставления различным классам трафика различных приоритетов в обслуживании(таким как мультимедийный, видео, зависящий от протокола, критичный по времени и трафик резервного копирования файлов), также этим термином в области компьютерных сетей называют вероятность того, что сеть связи соответствует заданному соглашению о трафике, или же, в ряде случаев, неформальное обозначение вероятности прохождения пакета между двумя точками сети.

Что можно литературно перевести как: «QoS — способность сети обеспечить необходимый сервис заданному трафику в определенных технологических рамках».
В узком техническом значении, этот термин означает набор методов для управления ресурсами пакетных сетей.

6.1 QoS Port Classification (Классификация портов QoS)

После нажатия "QoS Configure">"Port Classification" , появится следующий экран.

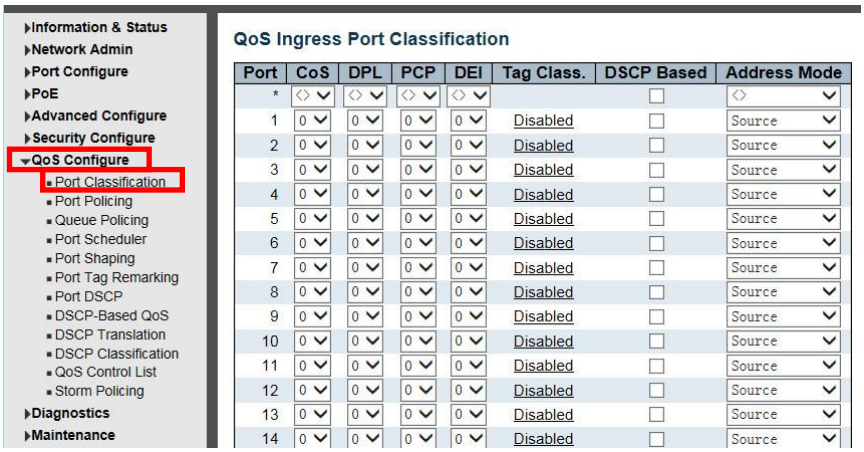


Рисунок 6-1 Экран конфигурации классификации портов

Port порт
Номер порта, для которого применяется приведенная ниже конфигурация.

CoS
Управляет классом обслуживания по умолчанию.
Все кадры классифицируются как CoS. Между CoS, очередью и приоритетом существует взаимно однозначное соответствие. CoS 0 (ноль) имеет самый низкий приоритет.
Если порт поддерживает VLAN, кадр помечается тегами и классом тегов. включен, то кадр классифицируется как CoS, который отображается из значений PCP и DEI в теге. В противном случае кадр классифицируется как CoS по умолчанию.
Классифицированный CoS может быть отменен записью QCL.
Примечание: Если CoS по умолчанию был динамически изменен, то фактический CoS по умолчанию показан в скобках после настроенного CoS по умолчанию.

DPL Drop Precedence Level(Отбросить уровень приоритета)
Управляет значением «Отбросить уровень приоритета» по умолчанию.
Все кадры классифицируются по уровню приоритета отбрасывания. Все кадры классифицируются по уровню приоритета отбрасывания.Классифицированный DPL может быть отменен записью QCL.

PCP Priority Code Point (Код приоритета)
Управляет значением PCP по умолчанию.
Все кадры классифицируются по значению PCP.

Если порт поддерживает VLAN и фрейм помечен, тогда фрейм классифицируется по значению PCP в тэге. В противном случае кадр классифицируется по значению PCP по умолчанию.

DEI Drop Eligible Indicator (Отбросить индикатор соответствия)
Управляет значением DEI по умолчанию.
Все кадры классифицируются по значению DEI.
Если порт поддерживает VLAN и фрейм помечен, тогда фрейм классифицируется по значению DEI в тэге. В противном случае кадр классифицируется по значению DEI по умолчанию.

Tag Class Класс тега.
Показывает режим классификации для помеченных кадров на этом порту.
Disabled Отключено: использовать CoS и DPL по умолчанию для помеченных кадров.
Enabled Включено: использовать сопоставленные версии PCP и DEI для кадров с тегами.
Щелкните режим, чтобы настроить режим и / или отображение.

Примечание. Этот параметр не действует, если порт не поддерживает VLAN. Тегированные кадры, полученные на портах, не поддерживающих VLAN, всегда классифицируются как CoS и DPL по умолчанию.

DSCP Based На основе DSCP
Щелкните, чтобы включить классификацию входного порта QoS на основе DSCP.

Address Mode Адресный режим
Режим IP / MAC-адреса, определяющий, должна ли классификация QCL основываться на адресах источника (SMAC / SIP) или назначения (DMAC / DIP) на этом порту. Допустимые значения:
Source Источник: включить сопоставление SMAC / SIP.
Destination Назначение: включить сопоставление DMAC / DIP.

Нажмите «Save», чтобы сохранить активные настройки.

6.2 Port Policing Контроль за портом

После нажатия «QoS Configure»> «Port Policing» появится следующий экран.

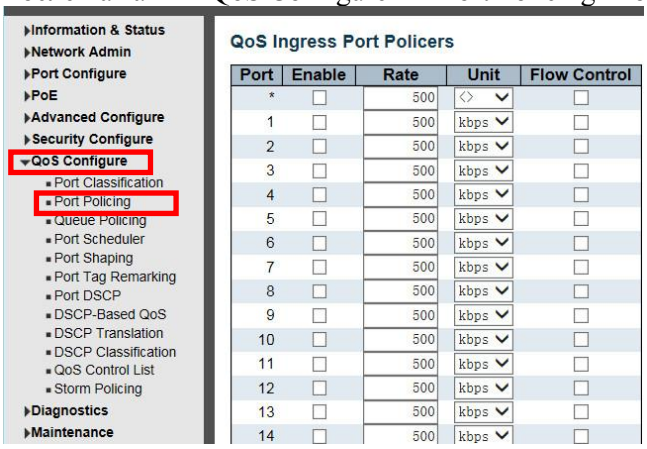


Рисунок 6-2 Экран настройки политики порта

Enabled Включено Установите флажок, чтобы включить политику порта.
Rate Скорость Управляет скоростью для ограничителя. Значение по умолчанию - 500. Это значение ограничено 100-1000000, когда «Unit» - это «кбит / с» или «fps», и ограничено 1-3300, когда «Unit» - «Mbps» или «kfps».

Unit (Единица) Управляет единицей измерения скорости ограничителя: кбит / с, Мбит / с, кадр / с или kfps, значение по умолчанию - «кбит / с». ,
Flow Control Управление потоком Если управление потоком включено и порт находится в режиме управления потоком, то вместо отбрасывания кадров отправляются кадры паузы.
Нажмите «Save», чтобы сохранить активные настройки.

6.3 QoS Ingress Queue Policer Config

После нажатия «QoS Configure»> «Queue Policing» появится следующий экран.

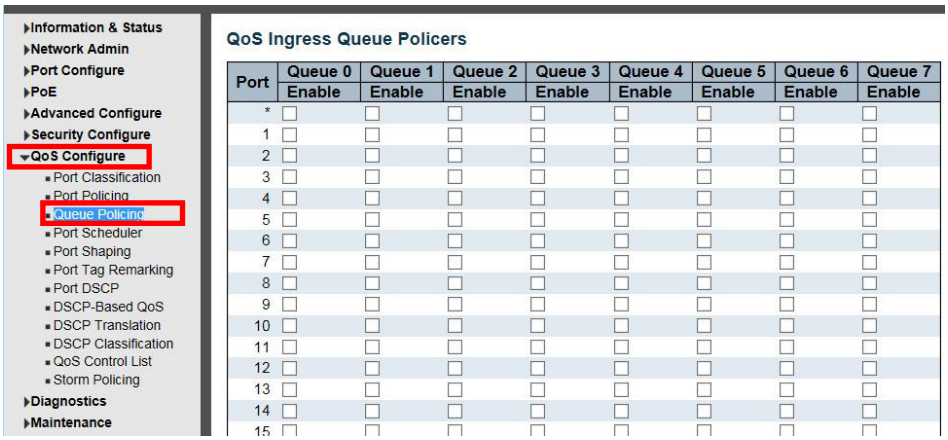


Рисунок 6-3 Экран конфигурации ограничителя очереди входящего трафика QoS

Эта страница позволяет настроить параметры ограничителя очереди для всех портов коммутатора.
Отображаемые настройки:
Port порт
Номер порта, для которого применяется приведенная ниже конфигурация.
Enable Включить (E)
Включите или отключите ограничитель очереди для этого порта коммутатора.
Нажмите «Save», чтобы сохранить активные настройки.

6.4 Port Scheduler (Планировщик портов)

После нажатия «QoS Configure»> «Port Scheduler» появится следующий экран.

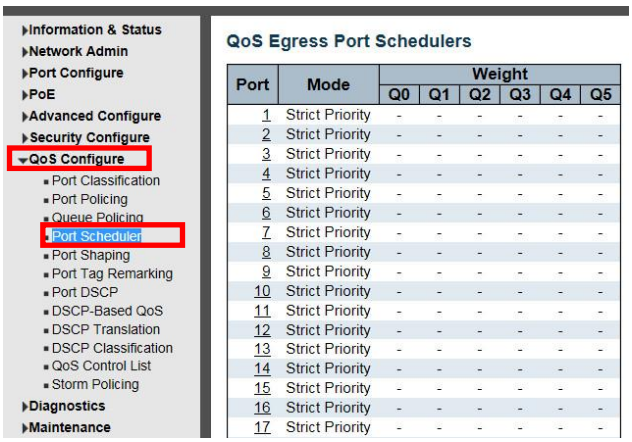


Рисунок 6-4 Экран планировщика портов

Port порт
Логический порт для настроек, содержащихся в той же строке.
Щелкните номер порта, чтобы настроить планировщики.
Mode Режим
Показывает режим планирования для этого порта.
Qn Показывает вес этой очереди и порта.

6.5 Port Shaping (Формирование порта)

После нажатия «QoS Configure»> «Port Shaping» появится следующий экран.

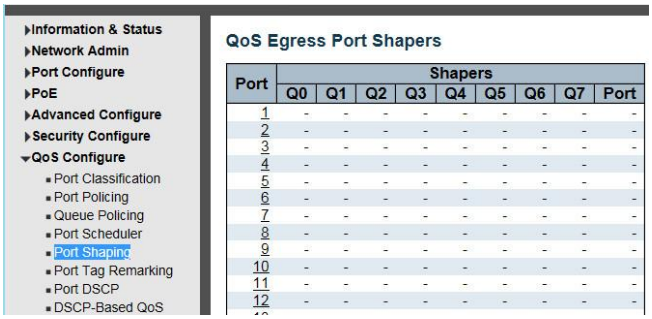


Рисунок 6-5 Экран формирования портов

Port порт

Логический порт для настроек, содержащихся в той же строке.

Щелкните номер порта, чтобы настроить формирователи.

Qn

Показывает "-" для отключенной или фактической скорости формирования очереди - например, «800 Мбит / с».

6.6 Port Tag Remarking (Маркировка тега порта)

После нажатия «QoS Configure»> «Port Tag Remarking» появится следующий экран.

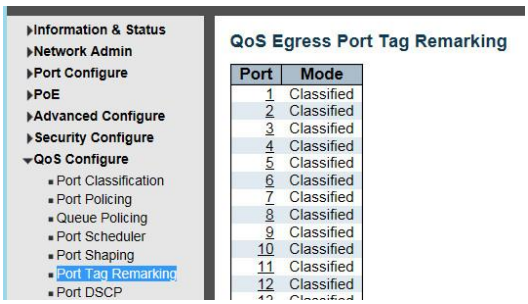


Рисунок 6-6 Экран маркировки тега порта

Port порт

Логический порт для настроек, содержащихся в той же строке.

Щелкните номер порта, чтобы настроить перемаркировку тегов.

Mode Режим

Показывает режим пометки тегов для этого порта.

Classified Классифицировано: используйте классифицированные значения PCP / DEI.

Default По умолчанию: использовать значения PCP / DEI по умолчанию.

Mapped Сопоставлено: используйте сопоставленные версии класса QoS и уровня DP.

6.7 Port DSCP

После нажатия «QoS Configure»> «Port DSCP » появится следующий экран.

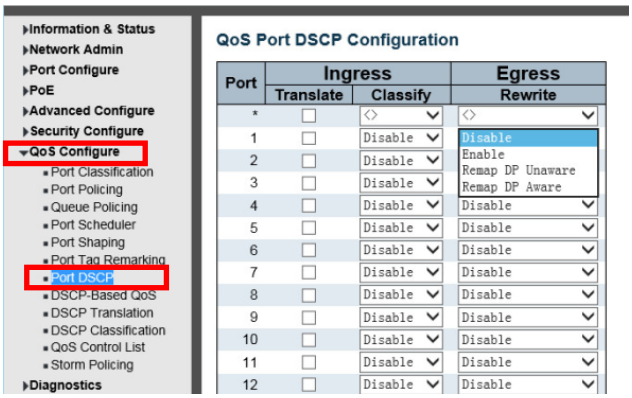


Рисунок 6-7 Экран DSCP Конфигурации порта

На этой странице можно настроить основные параметры конфигурации DSCP (Differentiated Services Code Point) (Кодовый пункт дифференцированных услуг)порта QoS для всех портов коммутатора. Это поле в заголовке IP-пакетов для целей классификации пакетов.

Отображаемые настройки:

Port порт

В столбце Port отображается список портов, для которых вы можете настроить параметры входа и выхода dscp.

Ingress вход

В настройках Ingress вы можете изменить настройки преобразования и классификации входящего трафика для отдельных портов.

В Ingress доступны два параметра конфигурации:

1. Translate Перевести
2. Classify Классифицировать

1. Translate Перевести

Чтобы включить перевод Ingress, установите флажок.

2. Classify Классифицировать

Классификация порта имеет 4 различных значения.

• Disable Отключить: нет классификации входящего DSCP.

• DSCP = 0: классифицировать, если входящий (или переведенный, если включен) DSCP равен 0.

• Selected Выбрано: классифицировать только выбранный DSCP, для которого включена классификация, как указано в окне «Трансляция DSCP» для конкретного DSCP.

• All Все: классифицировать все DSCP.

Egress выход

Перезапись порта выхода может быть одним из -

• Disable Отключить: перезапись на выходе запрещена.

• EnableВключить: перезапись включена без переназначения.

• Remap DP Unaware: DSCP от анализатора переназначается, и кадр помечается с переназначенным значением DSCP. Переназначенное значение DSCP всегда берется из таблицы «DSCP Translation-> Egress Remap DP0».

• Remap DP Aware: DSCP из анализатора переназначается, и кадр помечается с переназначенным значением DSCP. В зависимости от уровня DP кадра переназначенное значение DSCP берется либо из таблицы «Трансляция DSCP-> Egress Remap DP0», либо из таблицы «Трансляция DSCP-> Egress Remap DP1».

Нажмите «Save», чтобы сохранить активные настройки.

6.8 DSCP-Based QoS

После нажатия «QoS Configure»> «DSCP-Based QoS» появится следующий экран.

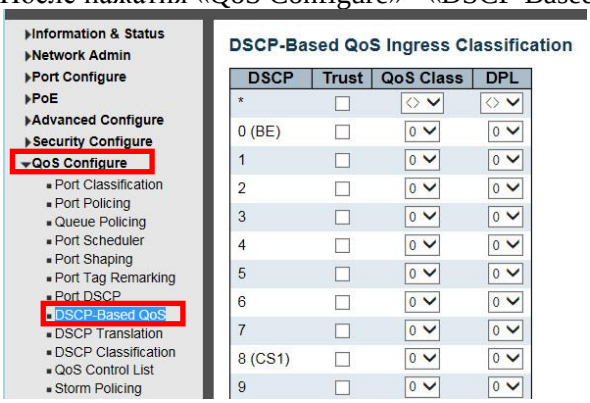


Рисунок 6-8 Экран конфигурации DSCP-Based QoS

Эта страница позволяет настроить базовые параметры классификации входящего трафика QoS на основе DSCP для всех коммутаторов.

Отображаемые настройки:

DSCP

Максимальное количество поддерживаемых значений DSCP - 64.

Trust Доверять

Определяет, является ли определенное значение DSCP доверенным. Только кадры с доверенными значениями DSCP отображаются на определенный класс QoS и уровень приоритета отбрасывания. Кадры с ненадежными значениями DSCP обрабатываются как кадры без IP.

QoS Class Класс QoS

Значение класса QoS может быть любым из (0-7)

DPL

Уровень приоритета выпадения (0-1)

Нажмите «Save», чтобы сохранить активные настройки.

6.9 DSCP Translation

После нажатия «QoS Configure»> «DSCP Translation» появится следующий экран.

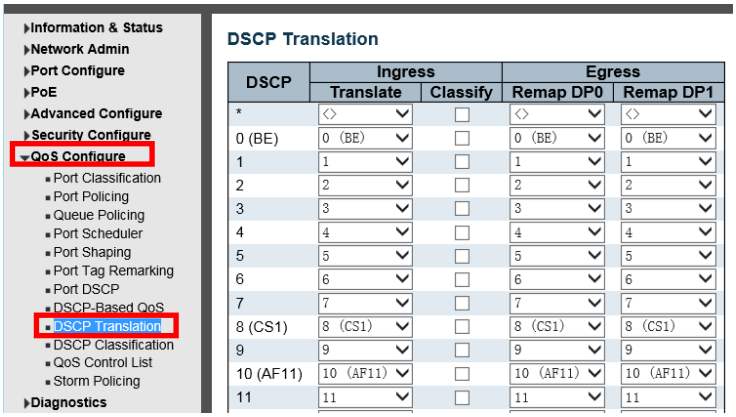


Рисунок 6-9 Экран конфигурации DSCP трансляции

На этой странице можно настроить основные параметры трансляции QoS DSCP для всех коммутаторов. Трансляция DSCP может выполняться на входящем или исходящем уровне.

DSCP

Максимальное количество поддерживаемых значений DSCP - 64, а допустимое значение DSCP находится в диапазоне от 0 до 63.

Ingress вход
DSCP на входящей стороне можно сначала преобразовать в новый DSCP перед использованием DSCP для класса QoS и карты DPL.
Есть два параметра конфигурации для трансляции DSCP:
1. Translate Перевести
2. Classify Классифицировать
1. Translate Перевести
DSCP на входящей стороне можно преобразовать в любое из (0-63) значений DSCP ***2. Classify Классифицировать***
Щелкните, чтобы включить классификацию на стороне входа.
Egress выход
Для исходящей стороны есть следующие настраиваемые параметры -
1. Remap DP0 Управляет повторным отображением для кадров с уровнем DP 0.
2. Remap DP1 Управляет повторным отображением для кадров с DP уровня 1.

1. Remap DP0 Переназначить DP0
Выберите значение DSCP из меню выбора, на которое вы хотите переназначить. Диапазон значений DSCP от 0 до 63.
2. Remap DP1 Переназначить DP1
Выберите значение DSCP из меню выбора, на которое вы хотите переназначить. Диапазон значений DSCP от 0 до 63.

Нажмите «Save», чтобы сохранить активные настройки.

6.10 DSCP Classification

После нажатия «QoS Configure»> «DSCP Classification» появится следующий экран.

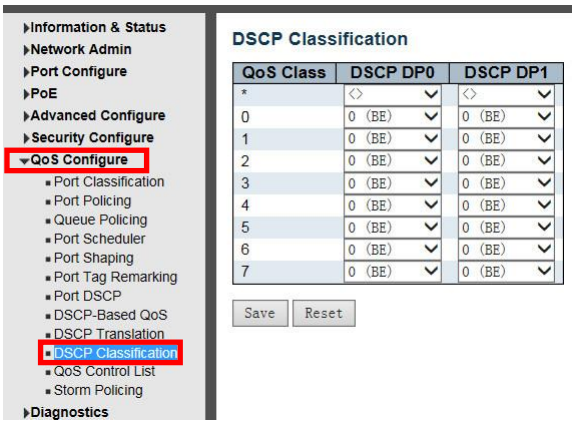


Рисунок 6-10 Экран конфигурации DSCP классификации

На этой странице можно настроить сопоставление класса QoS и уровня приоритета отбрасывания со значением DSCP.

Класс QoS
Фактический класс QoS.

DSCP DP0
Выберите классифицированное значение DSCP (0-63) для уровня приоритета отбрасывания 0.

DSCP DP1
Выберите классифицированное значение DSCP (0-63) для уровня приоритета отбрасывания 1.

Нажмите «Save», чтобы сохранить активные настройки.

6.11 QoS Control List

После нажатия «QoS Configure»> «QoS Control List» появится следующий экран.

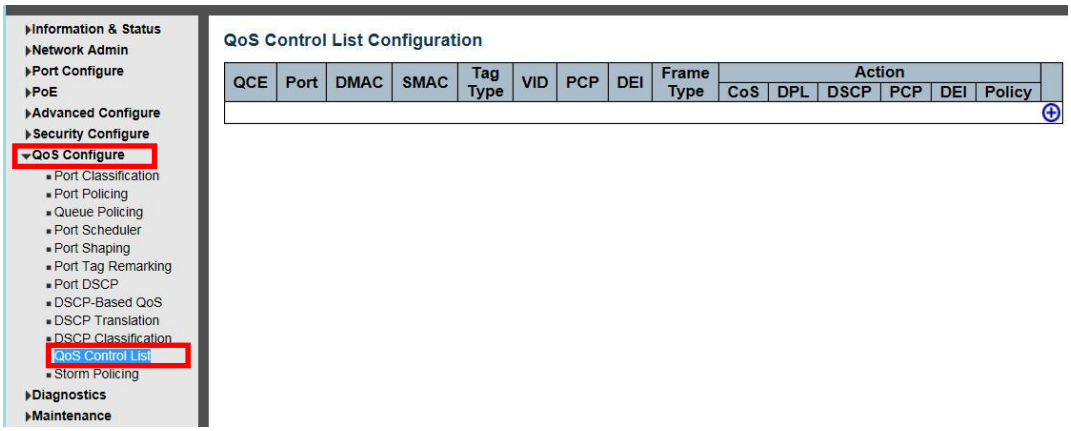


Рисунок 6-11-1 Экран конфигурации списка управления QoS (QCL)

На этой странице показан список управления QoS (QCL), который состоит из QCE. Каждая строка описывает определенный QCE. Максимальное количество QCE - 256 на каждом коммутаторе.
Нажмите на самый нижний знак плюса, чтобы добавить новый QCE в список.

QCE
Указывает идентификатор QCE.

Port порт
Указывает список портов, настроенных с помощью QCE или «Any».

DMAC
Указывает MAC-адрес назначения. Возможные значения:
Любой: соответствует любому DMAC.
Одноадресный: сопоставление одноадресного DMAC.
Multicast: соответствует многоадресному DMAC.
Трансляция: Матч трансляции DMAC.
Значение по умолчанию - «Any».

SMAC
Соответствует определенному MAC-адресу источника или «Any». Если порт настроен для сопоставления по адресам назначения, в этом поле указывается DMAC.

Tag Type Тип тега
Указывает тип тега. Возможные значения:
Любой: сопоставление кадров с тегами и без тегов.
Без тегов: соответствие немаркированным кадрам.
С тегами: сопоставление кадров с тегами.
Значение по умолчанию - «Any».

VID
Указывает (VLAN ID) либо конкретный VID, либо диапазон VID. VID может быть в диапазоне 1-4095 или «Any».

PCP
Точка кода приоритета: допустимые значения PCP являются конкретными (0, 1, 2, 3, 4, 5, 6, 7) или диапазоном (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) или «Any».

DEI
Отбросить индикатор соответствия: допустимые значения DEI - 0, 1 или «Any».

Frame Type Тип кадра
Указывает тип рамки. Возможные значения:
Любой: соответствует любому типу кадра.
Ethernet: сопоставление кадров EtherType.
OOO: Матч (OOO) кадры.
SNAP: совпадают (SNAP) кадры.
IPv4: соответствие фреймов IPv4.
IPv6: соответствие кадров IPv6.

Action действие
Указывает действие классификации, предпринимаемое для входящего кадра, если настроенные параметры совпадают с содержимым кадра.
Возможные действия:
CoS: классифицируйте класс обслуживания.
DPL: классифицируйте уровень приоритета отбрасывания.
DSCP: классифицируйте значение DSCP.
PCP: классифицируйте значение PCP.
DEI: классифицируйте значение DEI.
Политика: классифицируйте номер политики ACL.

Modification Buttons Кнопки модификации
Вы можете изменить каждый QCE (QoS Control Entry) в таблице с помощью следующих кнопок:

- Добавить: вставляет новый QCE перед текущей строкой.
- : Изменить: редактирует QCE.
- : Вверх: перемещает QCE вверх по списку.
- : Вниз: перемещает QCE вниз по списку.
- : Удалить: удаляет QCE.
- : Добавить: самый нижний знак плюса добавляет новую запись внизу списков QCE.

При нажатии на значок появится следующий экран

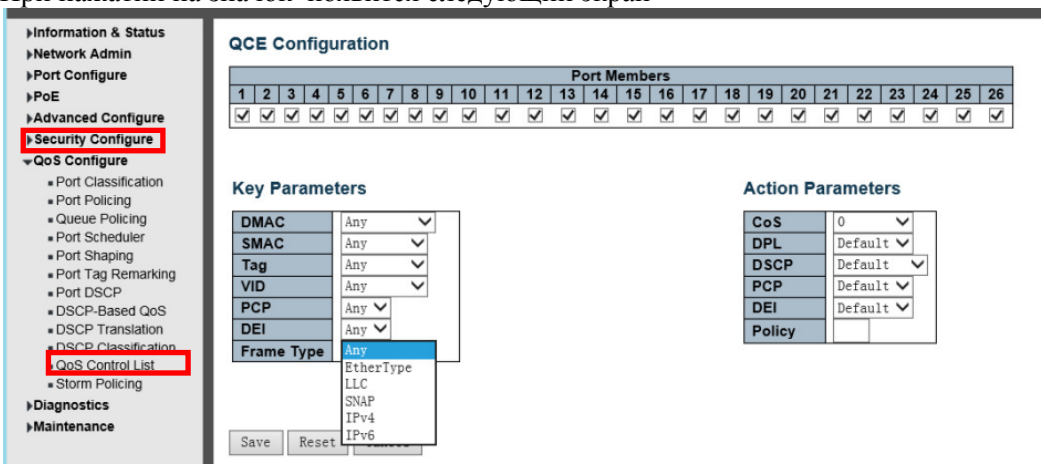


Рисунок 6-11-2 Экран конфигурации списка управления QoS (QCL)

Эта страница позволяет редактировать | вставлять по одной записи управления QoS за раз. QCE состоит из нескольких параметров. Эти параметры различаются в зависимости от выбранного вами типа кадра.

Port Members Члены порта
Установите флажок, чтобы включить порт в запись QCL. По умолчанию включены все порты.

Key Parameters Ключевые параметры

Ключевая конфигурация описана ниже:
MAC-адрес назначения DMAC: Возможные значения: «Unicast», «Multicast», «Broadcast» или «Any».
Исходный MAC-адрес SMAC: xx-xx-xx-xx-xx-xx или «Any». Если порт настроен для соответствия DMAC / DIP, это поле является MAC-адресом назначения.
Значение тега в поле Tag может быть «Без тегов», «Теги», «C-Tagged», «S-Tagged» или «Любые».
VID Допустимым значением VLAN ID может быть любое значение в диапазоне 1-4095 или «Any»; пользователь может ввести либо конкретное значение, либо диапазон VID.
PCP Допустимые значения PCP являются конкретными (0, 1, 2, 3, 4, 5, 6, 7) или диапазонами (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) или «Any».
DEI Допустимое значение DEI может быть «0», «1» или «Любое».
Тип кадра Тип кадра может иметь любое из следующих значений:
1.Any
2.EtherType
3.LLC
4.SNAP
5.IPv4
6.IPv6
Примечание. Ниже описаны все типы кадров.

1. Любой
Разрешить все типы рамок.
2. EtherType
Тип эфира. Действительный тип эфира может быть 0x600-0xFFFF, за исключением 0x800 (IPv4) и 0x86DD (IPv6) или «Any».
3. LLC
Действительный адрес DSAP DSAP (конечная точка доступа к услуге) может варьироваться от 0x00 до 0xFF или «Any».
Действительный адрес SSAP SSAP (исходная точка доступа к сервису) может варьироваться от 0x00 до 0xFF или «Any».
Контрольное поле Действительное Контрольное поле может быть от 0x00 до 0xFF или «Любое».
4. SNAP
PID Действительный PID (он же Ether Type) может иметь значение 0x0000-0xFFFF или «Any».

5. IPv4
Protocol IP Номер протокола IP: (0–255, «TCP» или «UDP») или «Any» (Любой).
Source IP Исходный IP Определенный исходный IP-адрес в формате значения / маски или «Any» IP и маска имеют формат xyzw, где x, y, z и w - десятичные числа от 0 до 255. Когда маска преобразуется в 32-битную двоичную строку и читается слева направо, все биты, следующие за первым нулем, должны также равняться нулю. Если порт настроен для соответствия DMAC / DIP, это поле является IP-адресом назначения.

IP Fragment IP-фрагмент Параметр фрагментации кадра IPv4: «Yes», «No» или «Any».
DSCP Diffserv Code Point value (DSCP): Это может быть конкретное значение, диапазон значений или «Any». Значения DSCP находятся в диапазоне 0-63, включая BE, CS1-CS7, EF или AF11-AF43.
Порт TCP / UDP источника
Sport: (0-65535) или «Any», конкретный или диапазон портов, применимый для IP-протокола UDP / TCP.
Dport Destination TCP / UDP port: (0-65535) или «Any», конкретный или диапазон портов, применимый для IP-протокола UDP / TCP.

6. IPv6
Protocol IP Номер протокола IP: (0–255, «TCP» или «UDP») или «Any».
Source IP Исходный IP-адрес 32 LS-бита исходного IPv6-адреса в формате «значение / маска» или «Any». Если порт настроен для соответствия DMAC / DIP, это поле является IP-адресом назначения.
DSCP Diffserv Code Point value (DSCP): Это может быть конкретное значение, диапазон значений или «Any». Значения DSCP находятся в диапазоне 0-63, включая BE, CS1-CS7, EF или AF11-AF43.
Порт TCP / UDP источника Sport: (0-65535) или «Any», конкретный или диапазон портов, применимый для IP-протокола UDP / TCP.
Dport Destination TCP / UDP port: (0-65535) или «Any», конкретный или диапазон портов, применимый для IP-протокола UDP / TCP.

Action Parameters Параметры действия
Класс обслуживания CoS: (0-7) или «Default».
Уровень приоритета сброса DP: (0–1) или «Default».
DSCP DSCP: (0-63, BE, CS1-CS7, EF или AF11-AF43) или «Default».
PCP PCP: (0-7) или «Default». Примечание: PCP и DEI не могут быть установлены индивидуально.
DEI DEI: (0-1) или «Default».
ACL политики Номер политики: (0–255) или «Default» (пустое поле).

«Default» означает, что классифицированное значение по умолчанию не изменяется этим QCE.

Нажмите «Save», чтобы сохранить активные настройки.

6.12 Storm Policing (Ограничение шторма)

После нажатия «QoS Configure»> «Storm Policing» появится следующий экран.

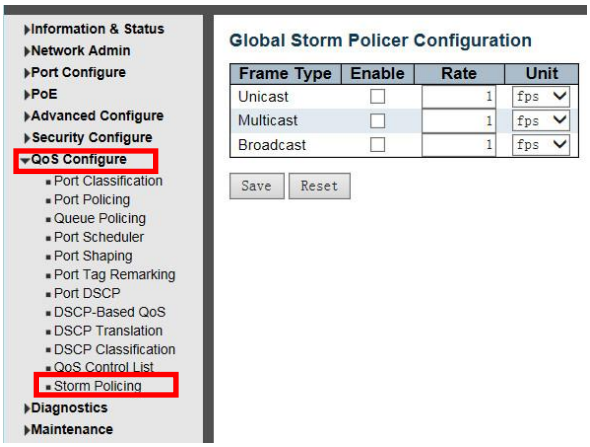


Рисунок 6-12 Экран конфигурации ограничения шторма

На этой странице настраиваются глобальные ограничители шторма для коммутатора.

Существует ограничитель шторма одноадресной рассылки, ограничитель шторма многоадресной рассылки и ограничитель широковещательного шторма.
Они влияют только на заправленные кадры, то есть кадры с парой (VLAN ID, DMAC), отсутствующей в таблице MAC-адресов.

Отображаемые настройки:
Frame Type Тип кадра
Тип кадра, для которого применяется приведенная ниже конфигурация.

Enable включить
Включите или отключите глобальный ограничитель шторма для данного типа кадра.

Rate скорость
Управляет скоростью глобального ограничителя шторма. Это значение ограничено 1-1024000, когда "Unit" - это fps, и 1-1024, когда "Unit" - kfps. Скорость внутренне округляется до ближайшего значения, поддерживаемого глобальным ограничителем шторма.

Unit Ед. изм
Управляет единицей измерения для глобальной скорости ограничителя шторма как fps или kfps.

Нажмите «Save», чтобы сохранить активные настройки

7. Security Configure (Настройка безопасности)

7.1 Users (Пользователи)

Чтобы изменить пароль для входа в систему коммутатора, нажмите «Security Configure»> «Users».

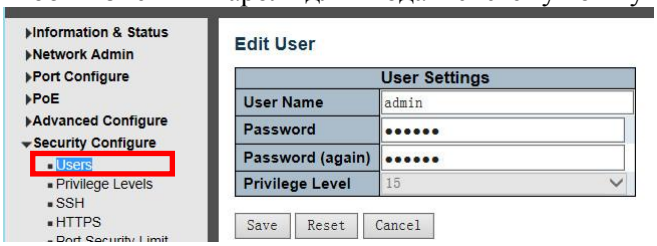


Рисунок 7-1 Экран конфигурации пользователей

На этой странице представлен обзор текущих пользователей. В настоящее время единственный способ войти в систему как другой пользователь на веб-сервере - закрыть и снова открыть браузер.

Отображаемые значения для каждого пользователя:

User Name Имя пользователя

Имя, идентифицирующее пользователя. Это также ссылка для добавления / редактирования пользователя.

Privilege Level Уровень привилегий

Уровень привилегий пользователя. Допустимый диапазон - от 0 до 15. Если значение уровня привилегии равно 15, он может получить доступ ко всем группам, то есть ему предоставляется полный контроль над устройством. Но другие ценят необходимость ссылаться на каждый уровень привилегий группы. Привилегия пользователя должна быть такой же или больше, чем уровень привилегий группы, чтобы иметь доступ к этой группе. По умолчанию большинство групп с уровнем привилегий 5 имеют доступ только для чтения, а уровень привилегий 10 имеет доступ для чтения и записи. А для обслуживания системы (загрузка программного обеспечения, заводские настройки по умолчанию и т. д.) требуется уровень прав пользователя 15. Как правило, уровень привилегий 15 может использоваться для учетной записи администратора, уровень привилегий 10 для стандартной учетной записи пользователя и уровень привилегий 5 для гостевой учетной записи.

Нажмите «Save», чтобы сохранить активные настройки

7.2 Privilege Level (Уровень привилегий)

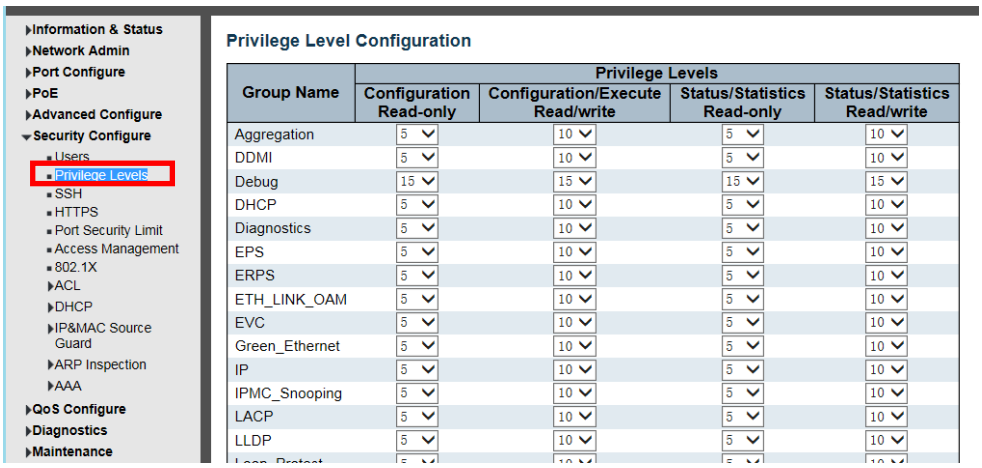


Рисунок 7-1 Экран конфигурации уровня привилегий

Group Name Название группы

Имя, определяющее группу привилегий. В большинстве случаев группа уровня привилегий состоит из одного модуля (например, LACP, RSTP или QoS), но некоторые из них содержат более одного модуля. Следующее описание подробно описывает эти группы уровней привилегий:

System: Contact, Name, Location, Timezone, Log Система: контакт, имя, местоположение, часовой пояс, журнал.
Security Безопасность: аутентификация, управление доступом к системе, порт (содержит порт Dot1x, на основе MAC и ограничение MAC-адреса), ACL, HTTPS, SSH, проверка ARP, защита источника IP.
IP: Все, кроме пинга.
Port: все, кроме VeriPHY.
Diagnostics Диагностика: «ping» и «VeriPHY».
Maintenance Обслуживание: CLI - перезагрузка системы, восстановление системы по умолчанию, системный пароль, сохранение конфигурации, загрузка конфигурации и загрузка прошивки. Веб-пользователи, уровни привилегий и все необходимое для обслуживания.
Debug Отладка: присутствует только в CLI.

Privilege Levels Уровни привилегий
Каждая группа имеет уровень привилегий авторизации для следующих подгрупп: конфигурация только для чтения, конфигурация / выполнение для чтения-записи, статус / статистика только для чтения, статус / статистика для чтения-записи (например, для очистки статистики). Привилегия пользователя должна быть такой же или больше, чем уровень привилегий авторизации, чтобы иметь доступ к этой группе.

Нажмите «Save», чтобы сохранить активные настройки

7.3 SSH

Конфигурация SSH

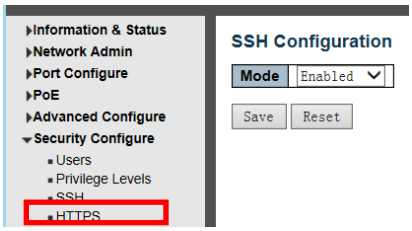


Рисунок 7-3 Экран конфигурации SSH

Настройте SSH на этой странице.
Mode Указывает на работу в режиме SSH. Возможные режимы:
Enable Включено: включить режим SSH.
Disabled Отключено: отключить режим SSH.

Нажмите «Save», чтобы сохранить активные настройки

7.4 HTTPS

Конфигурация HTTPS

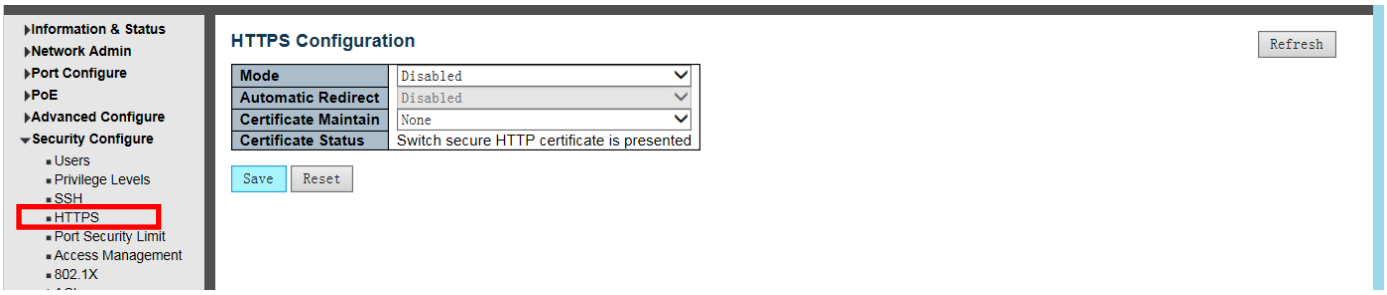


Рисунок 7-4 Экран конфигурации HTTPS

Эта страница позволяет вам настроить параметры HTTPS и поддерживать текущий сертификат на коммутаторе.
Mode Режим

Укажите режим работы HTTPS.
Возможные режимы:
Enabled: включить режим HTTPS.
Disabled : отключить режим HTTPS.

Automatic RedirectАвтоматическое перенаправление
Укажите режим перенаправления HTTPS. Это имеет значение только при выборе «HTTPS Mode Enabled». Когда включен режим перенаправления, HTTP-соединение будет автоматически перенаправлено на HTTPS-соединение.
Обратите внимание, что браузер может не разрешить операцию перенаправления из соображений безопасности, если сертификат коммутатора не является доверенным для браузера. В этом случае вам необходимо инициализировать HTTPS-соединение вручную.
Возможные режимы:
Enabled: включить режим перенаправления HTTPS.
Disabled: отключить режим перенаправления HTTPS.

Certificate Maintain Обслуживание сертификата
Операция по обслуживанию сертификата.
Возможные операции:
None: нет операции.
Delete: удалить текущий сертификат.
Upload: загрузить файл PEM сертификата. Возможные методы: веб-браузер или URL.
Generate: создание нового самозаверяющего сертификата RSA.

Certificate Pass Phrase Контрольная фраза
Введите парольную фразу в это поле, если ваш сертификат загрузки защищен определенной парольной фразой.

Certificate Upload Загрузить сертификат
Загрузите файл PEM сертификата в коммутатор. Файл должен содержать сертификат и закрытый ключ вместе. Если у вас есть два отдельных файла для сохранения сертификата и закрытого ключа, используйте команду Linux cat, чтобы объединить их в один файл PEM. Например, cat my.cert my.key> my.pem
Обратите внимание, что рекомендуется использовать сертификат RSA, поскольку в большинстве новых версий браузеров удалена поддержка DSA в сертификате, например Firefox v37 и Chrome v39.
Возможные методы:
Веб-браузер: загрузите сертификат через веб-браузер.
URL-адрес: загрузите сертификат через URL-адрес, поддерживаемые протоколы: HTTP, HTTPS, TFTP и FTP. Формат URL-адреса следующий: <протокол>: // [<имя пользователя> [: <пароль>] @] <хост> [: <порт>] [/ <путь>] / <имя_файла>. Например, tftp: //10.10.10.10/new_image_path/new_image.dat, http: // имя пользователя: пароль@10.10.10.10: 80 / new_image_path / new_image.dat. Допустимое имя файла - это текстовая строка, состоящая из букв (A-Za-z), цифр (0-9), точки (.), Дефиса (-), под знаком (_). Максимальная длина - 63, дефис не должен быть первым символом. Содержимое имени файла, которое содержит только "." не допускается.

Certificate Status Статус сертификата
Отобразите текущий статус сертификата на коммутаторе.
Возможные статусы:
Switch secure HTTP certificate is presented. Представлен сертификат безопасности коммутатора HTTP.
Switch secure HTTP certificate is not presented. Сертификат безопасности коммутатора HTTP не представлен.
Switch secure HTTP certificate is generating ....Создается сертификат безопасности коммутатора HTTP ....

Нажмите «Save», чтобы сохранить активные настройки

7.5 Port Security Limit (Ограничение безопасности порта)

Конфигурация ограничения безопасности порта

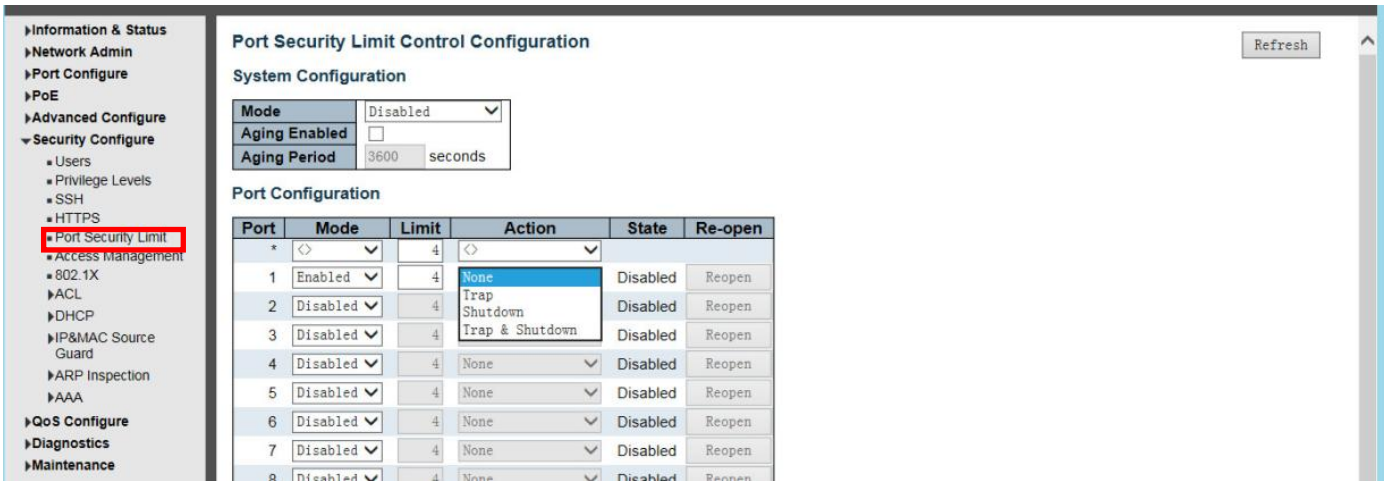


Рисунок 7-5 Экран конфигурации ограничения безопасности порта

На этой странице вы можете настроить систему ограничения безопасности порта и параметры порта.

Limit Control позволяет ограничить количество пользователей на данном порту. Пользователь идентифицируется по MAC-адресу и идентификатору VLAN. Если для порта включен контроль пределов, это ограничение определяет максимальное количество пользователей на порту. Если это число превышено, предпринимается действие. Действие может быть одним из четырех различных действий, описанных ниже.
Модуль управления лимитами использует модуль нижнего уровня, модуль безопасности порта, который управляет MAC-адресами, полученными на порте.

Конфигурация Limit Control состоит из двух разделов: Конфигурация системы и Конфигурация порта.

System Configuration Конфигурация системы

Mode Режим

Указывает, включено или отключено управление ограничениями на коммутаторе. При глобальном отключении другие модули могут по-прежнему использовать базовые функции, но проверки ограничений и соответствующие действия отключены.

Aging Enabled Старение включено

Если этот флажок установлен, защищенные MAC-адреса подлежат устареванию, как описано в разделе «Aging Period».

Aging Period Период старения

Если установлен флажок Aging Enabled, то с помощью этого входа контролируется период устаревания. Если другие модули используют безопасность базового порта для защиты MAC-адресов, у них могут быть другие требования к периоду устаревания. Базовая защита порта будет использовать более короткий запрошенный период устаревания всех модулей, которые используют эту функциональность.
Период выдержки может быть установлен в диапазоне от 10 до 10 000 000 секунд.
Чтобы понять, почему старение может быть желательным, рассмотрим следующий сценарий: Предположим, что конечный хост подключен к стороннему коммутатору или концентратору, который, в свою очередь, подключен к порту на этом коммутаторе, на котором включен контроль ограничений. Конечному хосту будет разрешено пересылать, если лимит не превышен. Теперь предположим, что конечный хост выходит из системы или отключается. Если бы не устаревание, конечный хост по-прежнему занимал бы ресурсы на этом коммутаторе и ему разрешили бы пересылку. Чтобы преодолеть эту ситуацию, включите старение. При включенном устаревании таймер запускается после защиты конечного хоста. Когда таймер истекает, коммутатор начинает поиск кадров от конечного хоста, и если такие кадры не видны в течение следующего периода устаревания, конечный узел считается отключенным, и соответствующие ресурсы на коммутаторе освобождаются.

Port Configuration Конфигурация порта
В таблице есть по одной строке для каждого порта коммутатора и несколько столбцов:

Port Порт
Номер порта, к которому применяется приведенная ниже конфигурация.

Mode Режим
Управляет включением ограничения на этом порте. И этот, и глобальный режим должны быть установлены на «Включено», чтобы управление ограничениями действовало. Обратите внимание, что другие модули могут по-прежнему использовать базовые функции безопасности порта без включения контроля ограничений для данного порта.

Limit Предел
Максимальное количество MAC-адресов, которые можно защитить на этом порте. Это число не может превышать 1024. При превышении лимита выполняется соответствующее действие.
Коммутатор «рожден» с общим количеством MAC-адресов, из которых все порты получают каждый раз, когда новый MAC-адрес обнаруживается на порте с включенной защитой порта. Поскольку все порты берутся из одного пула, может случиться так, что сконфигурированный максимум не может быть предоставлен, если оставшиеся порты уже использовали все доступные MAC-адреса.

Action Действие
Если предел достигнут, переключатель может выполнить одно из следующих действий:
Нет: не разрешайте на порт больше MAC-адресов, но не предпринимайте дальнейших действий.
Ловушка: если на порте видны MAC-адреса Limit + 1, отправьте прерывание SNMP. Если устаревание отключено, будет отправлено только одно прерывание SNMP, но при включенном устаревании новые прерывания SNMP будут отправляться каждый раз при превышении лимита.
Завершение работы: если на порте видны MAC-адреса Limit + 1, выключите порт. Это означает, что все защищенные MAC-адреса будут удалены из порта, и новый адрес не будет изучен. Даже если соединение физически отключено и повторно подключено к порту (путем отсоединения кабеля), порт останется выключенным. Открыть порт можно тремя способами:
1) Загрузите переключатель,
2) Отключите и снова включите Limit Control на порту или коммутаторе,
3) Нажмите кнопку «Открыть».
Прерывание и завершение работы: если на порту видны MAC-адреса с ограничением + 1, будут выполнены действия как «Прерывание», так и «Завершение работы», описанные выше.

State Состояние
В этом столбце показано текущее состояние порта с точки зрения элемента управления пределами.
Состояние принимает одно из четырех значений:
Disabled Отключено: Контроль пределов либо отключен глобально, либо отключен для порта.
Ready Готово: предел еще не достигнут. Это может быть показано для всех действий.
Limit Reached Достигнут предел: указывает, что на этом порте достигнут предел. Это состояние может отображаться, только если для параметра Действие Action Действие установлено значение «None Нет» или «Trap Ловушка».
Shutdown Завершение работы: указывает, что порт отключен модулем контроля пределов. Это состояние может отображаться только в том случае, если для параметра Action установлено значение «Shutdown Выключение» или «Trap & Shutdown Прерывание и выключение».

Re-open ButtonКнопка повторного открытия
Если порт отключен этим модулем, вы можете снова открыть его, нажав эту кнопку, которая будет активирована только в этом случае. О других методах см. В разделе «Завершение работы» в разделе «Действие».
Обратите внимание, что нажатие кнопки «Открыть заново» приводит к обновлению страницы, поэтому незавершенные изменения будут потеряны.

Нажмите «Save», чтобы сохранить активные настройки.

7.6 Access Management (Управление доступом)

Конфигурация управления доступом

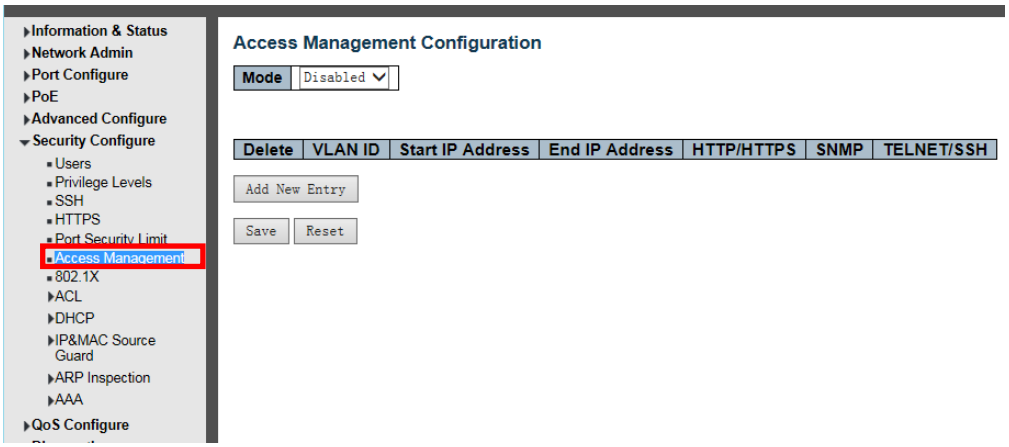


Рисунок 7-6 Экран конфигурации управления доступом

Настройте таблицу управления доступом на этой странице. Максимальное количество записей - 16. Если тип приложения соответствует любой из записей управления доступом, он разрешит доступ к коммутатору.

Mode Режим

Указывает на работу режима управления доступом. Возможные режимы:
Enabled Включено: включить режим управления доступом.
Disabled: отключить режим управления доступом.

Delete Удалить

Отметьте, чтобы удалить запись. Она будет удалена при следующем сохранении.

VLAN ID

Указывает идентификатор VLAN для записи управления доступом.

Start IP address Начальный IP-адрес

Указывает начальный IP-адрес для записи управления доступом.

End IP address Конечный IP-адрес

Указывает конечный IP-адрес для записи управления доступом.

HTTP / HTTPS

Указывает, что хост может получить доступ к коммутатору через интерфейс HTTP / HTTPS, если IP-адрес хоста соответствует диапазону IP-адресов, указанному в записи.

SNMP

Указывает, что хост может получить доступ к коммутатору через интерфейс SNMP, если IP-адрес хоста совпадает с диапазоном IP-адресов, указанным в записи.

ТЕЛНЕТ / SSH

Указывает, что хост может получить доступ к коммутатору через интерфейс TELNET / SSH, если IP-адрес хоста совпадает с диапазоном IP-адресов, указанным в записи.

Нажмите «Save», чтобы сохранить активные настройки.

7.7 802.1x Протокол проверки подлинности IEEE

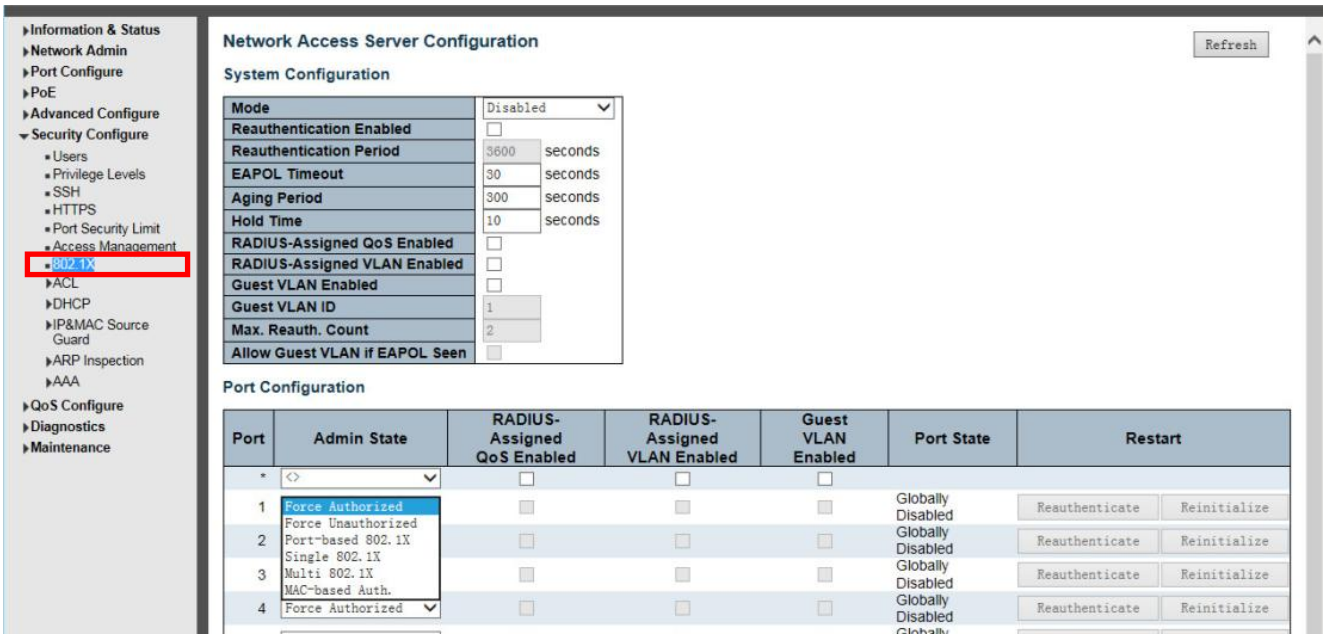


Рисунок 7-7 Экран конфигурации системы аутентификации IEEE 802.1X

Справка по конфигурации NAS

Эта страница позволяет вам настроить IEEE 802.1X и систему аутентификации на основе MAC, а также параметры порта.

Стандарт IEEE 802.1X определяет процедуру управления доступом на основе портов, которая предотвращает несанкционированный доступ к сети, требуя от пользователей сначала предоставить учетные данные для аутентификации. Один или несколько центральных серверов, бэкэнд-серверов, определяют, разрешен ли пользователю доступ к сети. Эти внутренние (RADIUS) серверы настраиваются на странице «Конфигурация → Безопасность → AAA». Стандарт IEEE802.1X определяет работу на основе порта, но нестандартные варианты преодолевают ограничения безопасности, которые будут рассмотрены ниже.

Аутентификация на основе MAC позволяет аутентифицировать более одного пользователя на одном и том же порте и не требует от пользователя установки в его системе специального программного обеспечения соискателя 802.1X. Коммутатор использует MAC-адрес пользователя для аутентификации на внутреннем сервере. Злоумышленники могут создавать поддельные MAC-адреса, что делает аутентификацию на основе MAC менее безопасной, чем аутентификация 802.1X.

Конфигурация NAS состоит из двух разделов: системного и портового.

Конфигурация системы

Mode Режим Указывает, включен или выключен NAS на коммутаторе на глобальном уровне. Если глобально отключено, всем портам разрешена пересылка кадров.

Reauthentication Enabled Если этот флажок установлен, успешно прошедшие аутентификацию соискатели / клиенты проходят повторную аутентификацию по истечении интервала, указанного в Периоде повторной аутентификации. Повторная аутентификация для портов с поддержкой 802.1X может использоваться для определения того, подключено ли новое устройство к порту коммутатора или запрашивающее устройство больше не подключено. Для портов на основе MAC повторная аутентификация полезна только в том случае, если конфигурация сервера RADIUS изменилась. Это не связано с обменом данными между коммутатором и клиентом и, следовательно, не означает, что клиент все еще присутствует на порту (см. «Период устаревания» ниже).

Reauthentication Period Определяет период в секундах, по истечении которого подключенный клиент должен быть повторно аутентифицирован. Он активен, только если установлен флажок «Повторная проверка подлинности». Допустимые значения находятся в диапазоне от 1 до 3600 секунд.

EAPOL Timeout Определяет время для повторной передачи кадров EAPOL запроса идентификации.

Допустимые значения находятся в диапазоне от 1 до 65535 секунд. Это не влияет на порты на основе MAC.

Aging Period Этот параметр применяется к следующим режимам, то есть к режимам, использующим функцию Port Security для защиты MAC-адресов:

• Single 802.1X
• Multi 802.1X
• Аутентификация на основе MAC.

Когда модуль NAS использует модуль безопасности порта для защиты MAC-адресов, модуль безопасности порта должен регулярно проверять активность на соответствующем MAC-адресе и освобождать ресурсы, если в течение заданного периода времени не наблюдается никакой активности. Этот параметр контролирует именно этот период и может иметь значение от 10 до 1000000 секунд.

Если повторная аутентификация включена и порт находится в режиме на основе 802.1X, это не так критично, поскольку соискатели, которые больше не подключены к порту, будут удалены при следующей повторной аутентификации, которая завершится ошибкой. Но если повторная аутентификация не включена, единственный способ освободить ресурсы - это устаревание записей.

Для портов с аутентификацией на основе MAC. В этом режиме повторная проверка подлинности не вызывает прямой связи между коммутатором и клиентом, поэтому он не определяет, подключен ли клиент по-прежнему или нет, и единственный способ освободить ресурсы - это сделать запись устаревшей. Время удержания Этот параметр применяется к следующим режимам, т. е. к режимам, использующим функцию защиты порта для защиты MAC-адресов:

• Single 802.1X
• Multi 802.1X
• Аутентификация на основе MAC.

Если клиенту отказано в доступе - либо из-за того, что сервер RADIUS отказывает клиенту в доступе, либо из-за тайм-аута запроса сервера RADIUS (в соответствии с тайм-аутом, указанным на странице «Конфигурация → Безопасность → AAA»), клиент приостанавливается в Несанкционированное состояние. Таймер удержания не учитывается во время текущей аутентификации.

В аутентификации на основе MAC. В режиме ожидания коммутатор будет игнорировать новые кадры, поступающие от клиента.

Hold Time Время удержания может быть установлено от 10 до 1000000 секунд. QoS, назначенное RADIUS, QoS, назначенное RADIUS, обеспечивает средства для централизованного управления классом трафика, которому на коммутаторе назначается трафик, исходящий от успешно аутентифицированного соискателя. Сервер RADIUS должен быть настроен для передачи специальных атрибутов RADIUS, чтобы воспользоваться этой функцией (подробное описание см. Ниже в разделе «QoS-Assigned QoS Enabled»).

Флажок «RADIUS-Assigned QoS Enabled» обеспечивает быстрый способ глобального включения / отключения функциональности класса QoS, назначенного RADIUS-сервером. Если этот флажок установлен, то же значение параметра отдельных портов определяет, включен ли для этого порта назначенный RADIUS класс QoS. Если этот флажок не установлен, класс QoS, назначенный RADIUS-сервером, отключен на всех портах.

RADIUS-Assigned VLAN Enabled

VLAN, назначенная RADIUS, предоставляет средства для централизованного управления VLAN, в которой успешно аутентифицированный соискатель размещается на коммутаторе. Входящий трафик будет классифицироваться и коммутироваться в VLAN, назначенной RADIUS. Сервер RADIUS должен быть настроен для передачи специальных атрибутов RADIUS, чтобы воспользоваться этой функцией (подробное описание см. Ниже в разделе «VLAN, назначенная RADIUS»).

Флажок «RADIUS-Assigned VLAN Enabled» обеспечивает быстрый способ глобального включения / выключения функций VLAN, назначенных RADIUS-сервером. Если этот флажок установлен, настройка отдельных портов определяет, включена ли для этого порта VLAN, назначенная RADIUS. Если этот флажок не установлен, VLAN, назначенная RADIUS-сервером, отключена на всех портах.

Guest VLAN Enabled

Гостевая VLAN - это специальная VLAN, обычно с ограниченным доступом к сети, в которую клиенты, не осведомленные о 802.1X, помещаются после тайм-аута, определенного сетевым администратором. Коммутатор следует набору правил для входа в гостевую VLAN и выхода из нее, как указано ниже.

Флажок «Guest VLAN Enabled» обеспечивает быстрый способ глобального включения / отключения функциональности гостевой VLAN. Если этот флажок установлен, то же значение настройки отдельных

портов определяет, можно ли переместить порт в гостевую VLAN. Если флажок снят, возможность перехода к

Гостевая VLAN отключена на всех портах.

Guest VLAN ID

Это значение, которое устанавливается для идентификатора VLAN порта порта, если порт перемещается в гостевую VLAN. Его можно изменить только в том случае, если опция Guest VLAN включена глобально.

Допустимые значения находятся в диапазоне [1; 4095].

Max. Reauth. Count

Количество раз, когда коммутатор передает кадр идентификации запроса EAPOL без ответа до рассмотрения возможности входа в гостевую VLAN, регулируется этим параметром. Значение может быть изменено только в том случае, если опция Guest VLAN включена глобально.

Допустимые значения находятся в диапазоне [1; 255].

Allow Guest VLAN if EAPOL Seen

Коммутатор запоминает, был ли получен кадр EAPOL на порте в течение всего срока службы порта. Как только коммутатор решит, следует ли входить в гостевую VLAN, он сначала проверит, включен или выключен этот параметр. Если этот параметр отключен (не установлен; по умолчанию), коммутатор будет входить в гостевую VLAN только в том случае, если на порт не был получен кадр EAPOL в течение всего срока его службы. Если этот параметр включен (отмечен), коммутатор будет рассматривать возможность входа в гостевую VLAN, даже если на порт был получен кадр EAPOL в течение всего срока службы порта.

Значение может быть изменено только в том случае, если опция Guest VLAN включена глобально.

Port Configuration Конфигурация порта

В таблице есть по одной строке для каждого порта коммутатора и несколько столбцов:

Port Порт

Номер порта, для которого применяется приведенная ниже конфигурация.

Admin State

Если NAS включен глобально, этот выбор управляет режимом аутентификации порта. Доступны следующие режимы:

Force Authorized

В этом режиме коммутатор отправит один кадр успеха EAPOL при подключении порта, и любому клиенту на порту будет разрешен доступ к сети без аутентификации.

Force Unauthorized

В этом режиме коммутатор отправит один кадр сбоя EAPOL при подключении порта, и любому клиенту на порту будет запрещен доступ к сети.

Port-based 802.1X

В мире 802.1X пользователя называют соискателем, коммутатор - аутентификатором, а сервер RADIUS - сервером аутентификации. Аутентификатор действует как посредник, пересылающий запросы и ответы между соискателем и сервером аутентификации. Кадры, передаваемые между запрашивающей стороной и коммутатором, представляют собой специальные кадры 802.1X, известные как кадры EAPOL (EAP Over LAN). Кадры EAPOL инкапсулируют PDU EAP (RFC3748). Кадры, передаваемые между коммутатором и сервером RADIUS, являются пакетами RADIUS. Пакеты RADIUS также инкапсулируют PDU EAP вместе с другими атрибутами, такими как IP-адрес коммутатора, имя и номер порта соискателя на коммутаторе. EAP очень гибок, поскольку позволяет использовать различные методы аутентификации, такие как MD5-Challenge, PEAP и TLS. Важно то, что аутентификатору (коммутатору) не нужно знать, какой метод аутентификации используют запрашивающий и сервер аутентификации, или сколько кадров обмена информацией необходимо для определенного метода. Коммутатор просто инкапсулирует часть кадра EAP в соответствующий тип (EAPOL или RADIUS) и пересылает его.

По завершении аутентификации сервер RADIUS отправляет специальный пакет, содержащий индикацию успеха или неудачи. Помимо пересылки этого решения запрашивающей стороне, коммутатор использует его для открытия или блокировки трафика на порте коммутатора, подключенном к запрашивающей стороне.

Примечание. Предположим, что два внутренних сервера включены и тайм-аут сервера настроен на X секунд (с использованием страницы конфигурации AAA), и предположим, что первый сервер в списке в настоящее время не работает (но не считается мертвым). Теперь, если соискатель повторно передает

стартовые кадры EAPOL со скоростью, превышающей X секунд, он никогда не будет аутентифицирован, потому что коммутатор будет отменять текущие запросы внутреннего сервера аутентификации всякий раз, когда он получает новый начальный кадр EAPOL от соискателя. И поскольку сервер еще не отказал (поскольку X секунд еще не истекли), с тем же сервером свяжутся при следующем запросе серверной аутентификации от коммутатора. Этот сценарий будет повторяться вечно. Следовательно, тайм-аут сервера должен быть меньше, чем скорость повторной передачи начального кадра EAPOL запрашивающей стороны.

Single 802.1X

При аутентификации 802.1X на основе портов после успешной аутентификации соискателя на порте весь порт открывается для сетевого трафика. Это позволяет другим клиентам, подключенным к порту (например, через концентратор), подключаться к успешно аутентифицированному клиенту и получать доступ к сети, даже если они действительно не аутентифицированы. Чтобы преодолеть это нарушение безопасности, используйте вариант Single 802.1X.

Single 802.1X на самом деле не является стандартом IEEE, но имеет многие из тех же характеристик, что и 802.1X на основе портов. В Single 802.1X максимум один соискатель может пройти аутентификацию на порту за раз. Обычные кадры EAPOL используются при обмене данными между запрашивающей стороной и коммутатором. Если к порту подключено более одного соискателя, то первым будет рассмотрен тот, который появится первым при подключении порта. Если этот соискатель не предоставит действительные учетные данные в течение определенного периода времени, другой соискатель получит шанс. После успешной аутентификации соискателя доступ будет разрешен только этому соискателю. Это самый безопасный из всех поддерживаемых режимов. В этом режиме модуль безопасности порта используется для защиты MAC-адреса соискателя после успешной аутентификации.

Multi 802.1X

Multi 802.1X, как и Single 802.1X, не является стандартом IEEE, а является вариантом, который имеет многие из тех же характеристик. В Multi 802.1X один или несколько соискателей могут пройти аутентификацию на одном и том же порте одновременно. Каждый соискатель аутентифицируется индивидуально и защищается в таблице MAC-адресов с помощью модуля безопасности порта.

В Multi 802.1X невозможно использовать MAC-адрес многоадресного BPDU в качестве MAC-адреса назначения для кадров EAPOL, отправляемых от коммутатора к запрашивающему, так как это заставит всех соискателей, подключенных к порту, отвечать на запросы, отправленные с коммутатора. Вместо этого коммутатор использует MAC-адрес соискателя, который получается из первого кадра EAPOL Start или EAPOL Response Identity, отправленного соискателем. Исключение составляют случаи, когда просители не прикреплены. В этом случае коммутатор отправляет кадры EAPOL Request Identity, используя MAC-адрес многоадресной рассылки BPDU в качестве пункта назначения - чтобы разбудить любых соискателей, которые могут быть на порту.

Максимальное количество соискателей, которые могут быть подключены к порту, можно ограничить с помощью функции управления ограничениями безопасности порта.

MAC-based Auth

В отличие от 802.1X на основе портов, аутентификация на основе MAC-адресов не является стандартом, а всего лишь передовым методом, принятым в отрасли. При аутентификации на основе MAC пользователи называются клиентами, а коммутатор действует как запрашивающий от имени клиентов. Первоначальный кадр (любой вид кадра), отправленный клиентом, отслеживается коммутатором, который, в свою очередь, использует MAC-адрес клиента как имя пользователя и пароль в последующем обмене EAP с сервером RADIUS. 6-байтовый MAC-адрес преобразуется в строку следующего вида «xx-xx-xx-xx-xx-xx», то есть тире (-) используется в качестве разделителя между шестнадцатеричными цифрами в нижнем регистре. Коммутатор поддерживает только метод аутентификации MD5-Challenge, поэтому сервер RADIUS должен быть настроен соответствующим образом.

Когда проверка подлинности завершена, сервер RADIUS отправляет сообщение об успешном или неудачном завершении работы, что, в свою очередь, заставляет коммутатор открывать или блокировать трафик для этого конкретного клиента с помощью модуля безопасности порта. Только после этого кадры от клиента будут перенаправлены на коммутатор. В этой аутентификации не используются кадры EAPOL, и поэтому аутентификация на основе MAC не имеет ничего общего со стандартом 802.1X.

Преимущество аутентификации на основе MAC перед аутентификацией на основе 802.1X заключается в том, что клиентам не требуется специальное программное обеспечение соискателя для аутентификации. Недостатком является то, что MAC-адреса могут быть подменены злоумышленниками - оборудование, MAC-адрес которого является действительным пользователем RADIUS, может использоваться кем угодно. Также поддерживается только метод MD5-Challenge. Максимальное количество клиентов, которые могут быть подключены к порту, может быть ограничено с помощью функции управления ограничениями безопасности порта.

RADIUS-Assigned QoS Enabled

Когда QoS, назначенное RADIUS, одновременно включено и включено (проверено) на заданном порту, коммутатор реагирует на информацию о классе QoS, передаваемую RADIUS-пакетом Access-Accept, передаваемым сервером RADIUS, после успешной аутентификации соискателя. Если он присутствует и действителен, трафик, полученный через порт запрашивающей стороны, будет классифицирован по данному классу QoS. Если (повторная) аутентификация завершилась неудачно, или пакет RADIUS Access-Accept больше не содержит класс QoS, или он недействителен, или если запрашивающий больше не присутствует на порте, класс QoS порта немедленно возвращается к исходному классу QoS (который может быть изменен администратором, не влияя на назначенный RADIUS).

Эта опция доступна только для однопользовательских режимов, т.е.

• 802.1X на основе портов

• Один 802.1X

Атрибуты RADIUS, используемые при идентификации класса QoS:

Атрибут User-Priority-Table, определенный в RFC4675, формирует основу для идентификации класса QoS в пакете Access-Accept.

Будет рассматриваться только первое появление атрибута в пакете, и чтобы он был действительным, он должен соответствовать следующему правилу:

• Все 8 октетов в значении атрибута должны быть идентичны и состоять из символов ASCII в диапазоне «0» - «7», что соответствует желаемому классу QoS в диапазоне [0; 7].

RADIUS-Assigned VLAN Enabled

Когда VLAN, назначенная RADIUS, глобально включена и включена (проверена) для данного порта, коммутатор реагирует на информацию идентификатора VLAN, содержащуюся в пакете RADIUS Access-Accept, передаваемом сервером RADIUS, когда запрашивающая сторона успешно аутентифицирована. Если присутствует и действителен, порт VLAN ID порта будет изменен на этот VLAN ID, порт будет установлен как член этого VLAN ID, и порт будет принудительно переведен в режим отсутствия информации о VLAN. После назначения весь трафик, поступающий на порт, будет классифицироваться и переключаться на идентификатор VLAN, назначенный RADIUS.

Если (повторная) аутентификация завершается неудачно, или пакет RADIUS Access-Accept больше не содержит идентификатор VLAN, или он недействителен, или запрашивающее лицо по иным причинам больше не присутствует на порте, идентификатор VLAN порта немедленно возвращается к исходному идентификатору VLAN (который может быть изменен администратором, не влияя на назначенный RADIUS).

Эта опция доступна только для однопользовательских режимов, т.е.

• 802.1X на основе портов

• Один 802.1X

Для устранения проблем с назначением VLAN используйте страницы «Монитор → VLAN → Членство в VLAN и порт VLAN». На этих страницах показано, какие модули (временно) переопределили текущую конфигурацию VLAN порта.

Атрибуты RADIUS, используемые при идентификации идентификатора VLAN:

RFC2868 и RFC3580 формируют основу для атрибутов, используемых при идентификации идентификатора VLAN в пакете Access-Accept. Используются следующие критерии:

• Атрибуты Tunnel-Medium-Type, Tunnel-Type и Tunnel-Private-Group-ID должны присутствовать хотя бы один раз в пакете Access-Accept.

• Коммутатор ищет первый набор этих атрибутов, которые имеют одинаковое значение тега и удовлетворяют следующим требованиям (если используется Tag == 0, Tunnel-Private-Group-ID не должен включать тег):

- Значение Tunnel-Medium-Type должно быть установлено на «IEEE-802» (порядковый номер 6).

- Значение Tunnel-Type должно быть установлено на «VLAN» (порядковый номер 13).

- Значение Tunnel-Private-Group-ID должно быть строкой символов ASCII в диапазоне «0» - «9», которая интерпретируется как десятичная строка, представляющая идентификатор VLAN. Начальные "0" отбрасываются. Окончательное значение должно быть в диапазоне [1; 4095]. Guest VLAN Enabled Когда гостевая VLAN включена и включена (отмечена) глобально для данного порта, коммутатор рассматривает возможность перемещения порта в гостевую VLAN в соответствии с правилами, описанными ниже.

Эта опция доступна только для режимов на основе EAPOL, а именно:

• 802.1X на основе портов

• Один 802.1X

• Мульти 802.1X

Для устранения проблем с назначением VLAN используйте страницы «Монитор → VLAN → Членство в VLAN и порт VLAN». На этих страницах показано, какие модули (временно) переопределили текущую конфигурацию VLAN порта.

Guest VLAN Operation:

Когда подключается порт с активированной гостевой VLAN, коммутатор начинает передавать кадры идентификации запроса EAPOL. Если количество передач таких кадров превышает Макс. Реаут. В это время не было получено ни одного кадра EAPOL, коммутатор рассматривает возможность входа в гостевую VLAN. Интервал между передачей кадров EAPOL Request Identity настраивается с помощью EAPOL Timeout. Если разрешить гостевую VLAN, если включен EAPOL Seen, порт теперь будет помещен в гостевую VLAN. Если этот параметр отключен, коммутатор сначала проверит свою историю, чтобы увидеть, был ли ранее получен кадр EAPOL на порт (эта история очищается, если канал порта выходит из строя или состояние администратора порта изменяется), а если нет, порт будет быть помещенным в гостевую VLAN. В противном случае он не переместится в гостевую VLAN, а продолжит передачу кадров идентификации запроса EAPOL со скоростью, заданной тайм-аутом EAPOL.

Попав в гостевую VLAN, порт считается аутентифицированным, и всем подключенным к порту клиентам разрешен доступ к этой VLAN. Коммутатор не будет передавать кадр успеха EAPOL при входе в гостевую VLAN.

Находясь в гостевой VLAN, коммутатор отслеживает ссылку на фреймы EAPOL, и если один такой фрейм получен, коммутатор немедленно выводит порт из гостевой VLAN и начинает аутентификацию запрашивающего в соответствии с режимом порта. Если получен кадр EAPOL, порт никогда не сможет вернуться в гостевую VLAN, если отключен параметр «Разрешить гостевую VLAN при обнаружении EAPOL».

Port State

Текущее состояние порта. Он может принимать одно из следующих значений:

Globally Disabled Глобально отключено: NAS отключен глобально.

Link Down Link Down: NAS включен глобально, но на порту нет ссылки.

Authorized Авторизовано: порт находится в режиме принудительной авторизации или в режиме единственного соискателя, и соискатель авторизован.

Unauthorized Неавторизованный: порт находится в режиме принудительного несанкционированного доступа или в режиме единственного соискателя, и соискатель не авторизован на сервере RADIUS.

X Auth / Y Unauth: порт находится в режиме множественных запросов. В настоящее время X клиентов авторизованы, а Y не авторизованы.

Начать сначала

Для каждой строки доступны две кнопки. Кнопки доступны только в том случае, если аутентификация включена глобально и порт Admin State находится в режиме на основе EAPOL или MAC.

Нажатие этих кнопок не приведет к вступлению в силу настроек, измененных на странице.

Reauthenticate: планирует повторную проверку подлинности всякий раз, когда истекает период молчания порта (проверка подлинности на основе EAPOL). При аутентификации на основе MAC будет предпринята попытка повторной аутентификации немедленно.

Кнопка действует только для клиентов, успешно прошедших проверку подлинности на порту, и не приводит к временной несанкционированной авторизации клиентов.

Reinitialize: вызывает повторную инициализацию клиентов на порту и, следовательно, немедленную повторную аутентификацию. Во время повторной аутентификации клиенты перейдут в неавторизованное состояние.

Нажмите «Save», чтобы сохранить активные настройки.

7.8 ACL (Access control list) - списки контроля доступа.

ACL - это аббревиатура от Access Control List. Это таблица списков ACE, содержащая записи управления доступом, которые определяют отдельных пользователей или группы, которым разрешено или запрещено использование определенных объектов трафика, таких как процесс или программа.
Каждый доступный объект трафика содержит идентификатор своего ACL. Привилегии определяют наличие определенных прав доступа к объекту трафика.
Реализации ACL могут быть довольно сложными, например, когда ACE имеют приоритет для различных ситуаций.
В сети ACL относится к списку сервисных портов или сетевых сервисов, доступных на хосте или сервере, каждый со списком хостов или серверов, которым разрешено или запрещено использовать сервис. ACL обычно можно настроить для управления входящим трафиком, и в этом контексте они похожи на брандмауэры.

7.8.1 ACL Ports Configure

После нажатия «Security Configure»> «ACL»> «Ports» появится следующий экран.

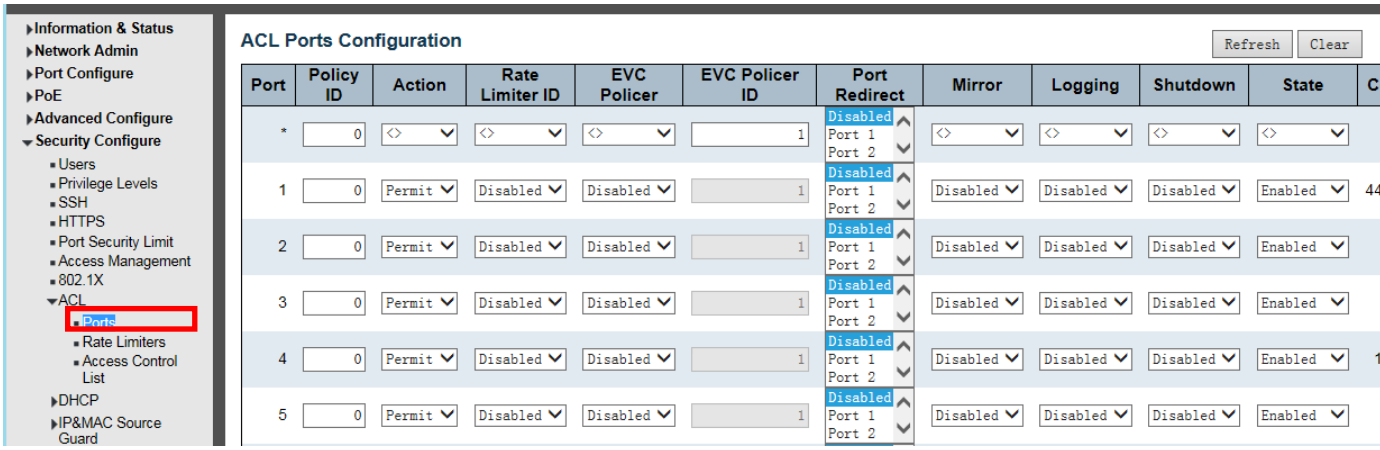


Рисунок 7-8-1 Экран настройки портов ACL

Action Действие Есть 2 доступных варианта: Разрешить: этот конкретный порт позволяет передавать данные. Запретить: этот конкретный порт запрещает прохождение данных.

Rate LimiterID Фиксированный идентификатор ограничителя скорости порта. Для получения дополнительных сведений перейдите в раздел «Конфигурация ограничителя скорости».

Port Redirect Перенаправление порта Выберите, на какой порт будет перенаправляться фрейм. Допустимые значения: Disabled или определенный номер порта, и его нельзя установить, если действие разрешено. Значение по умолчанию - «Отключено».

Mirror Зеркало Укажите операцию зеркалирования этого порта. Допустимые значения: Включено: кадры, полученные через порт, зеркалируются. Отключено: кадры, полученные через порт, не зеркалируются. Значение по умолчанию - «Отключено».

Logging Ведение журнала включено или отключено Журнал

Shut Down Завершение работы Укажите операцию отключения порта для этого порта. Допустимые значения: Включено: если через порт получен кадр, порт будет отключен. Отключено: отключение порта отключено. Значение по умолчанию - «Отключено». Примечание. Функция выключения работает только при длине пакета менее 1518 (без тегов VLAN).

State Укажите состояние порта для этого порта. Допустимые значения: Включено: повторное открытие портов путем изменения изменчивой конфигурации порта пользовательского модуля ACL. Отключено: закрытие портов путем изменения нестабильной конфигурации порта пользовательского модуля ACL. Значение по умолчанию - «Включено».

Counter Счетчик Подсчитывает количество кадров, соответствующих этому правилу.

Нажмите «Save», чтобы сохранить активные настройки.

7.8.2 Rate Limiter Configuration

Пользователь может настроить ограничитель скорости ACL на этой странице. После нажатия "Security Configure">"ACL">"Rate Limiter",появится следующий экран.

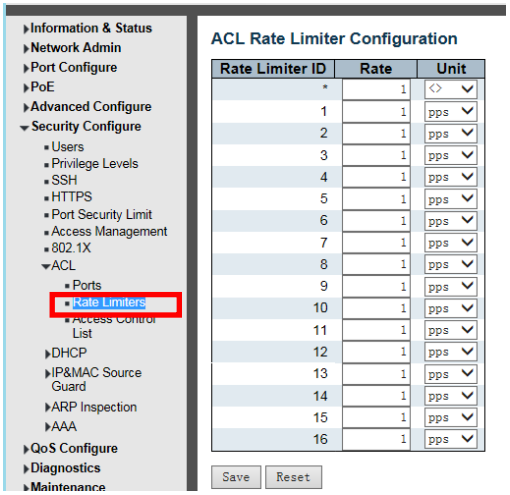


Рисунок 7-8-2 Экран настройки ограничителя скорости ACL

Нажмите «Save», чтобы сохранить активные настройки.

7.8.3 Access Control List Configuration

Пользователь может настроить список управления доступом на этой странице. После нажатия «Security Configure»> «ACL»> «Access Control List» появится следующий экран.

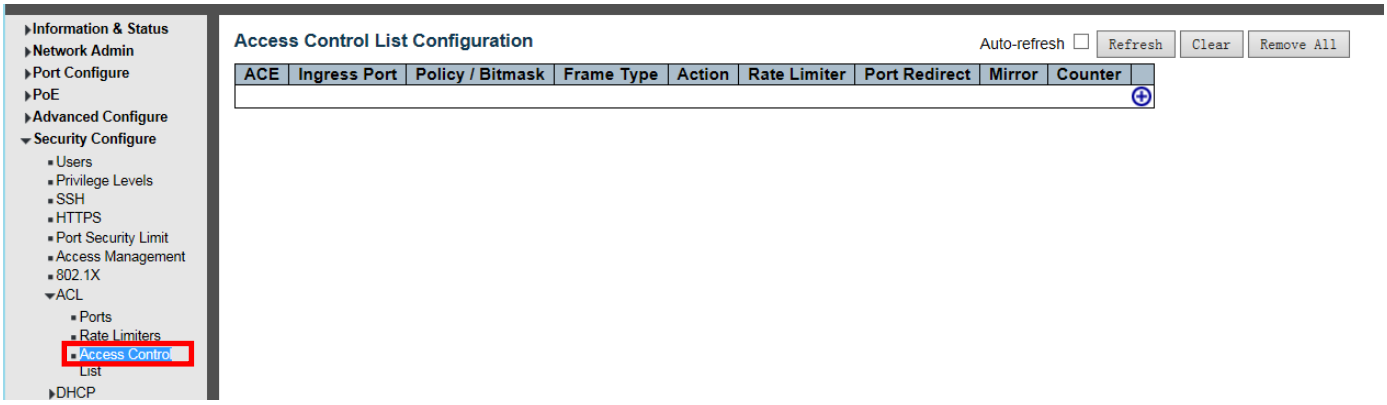


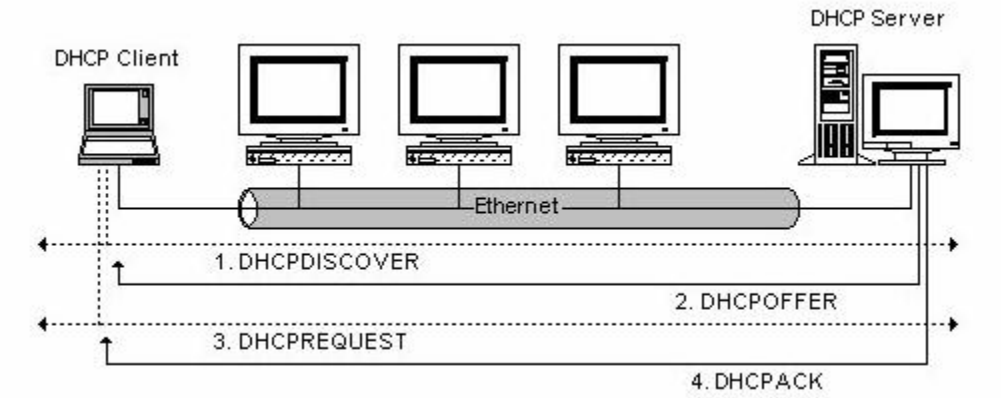
Рисунок 7-8-3 Экран конфигурации списка контроля доступа

Нажмите кнопку ⊕, чтобы перейти к списку контроля доступа и отредактировать его. Нажмите «Save», чтобы сохранить активные настройки.

7.9 DHCP

7.9.1 Обзор DHCP

Протокол DHCP широко используется для динамического выделения повторно используемых сетевых ресурсов, таких как IP-адрес. Процесс DHCP для получения IP выглядит следующим образом:



DHCP-клиент отправляет сообщение DHCP DISCOVER на DHCP-сервер. Если клиент не получил ответа от сервера в течение определенного периода времени, он повторно отправит сообщение DHCP DISCOVER.

После получения сообщения DHCP DISCOVER DHCP-сервер назначит клиенту источники (например, IP-адрес), а затем отправит DHCP-клиенту сообщение DHCP OFFER.

После получения сообщения DHCP OFFER, DHCP-клиент отправляет DHCP REQUEST, чтобы запросить аренду сервера, и уведомляет другие серверы о том, что он принял этот сервер для назначения адресов.

После получения ЗАПРОСА DHCP сервер проверит, можно ли выделить ресурс. Если все в порядке, он отправит сообщение DHCP ACK; Если не в порядке, он отправит сообщение DHCP NAK. После получения сообщения DHCP ACK начните использовать источник, назначенный сервером. Если получено DHCP NAK, DHCP-клиент повторно отправит сообщение DHCP DISCOVER.

7.9.2 DHCP Snooping

Адреса, назначенные клиентам DHCP на незащищенных портах, можно тщательно контролировать с помощью динамических привязок, зарегистрированных с помощью DHCP Snooping. Отслеживание DHCP позволяет коммутатору защищать сеть от мошеннических серверов DHCP или других устройств, которые отправляют информацию о портах на сервер DHCP. Эта информация может быть полезна при отслеживании IP-адреса до физического порта.

Использование команд

- Сетевой трафик может быть нарушен при получении вредоносных сообщений DHCP от внешнего источника.
- Отслеживание DHCP используется для фильтрации сообщений DHCP, полученных на незащищенном интерфейсе извне сети или межсетевого экрана. Когда отслеживание DHCP включено глобально и включено на интерфейсе VLAN, DHCP.
- сообщения, полученные на ненадежном интерфейсе от устройства, не указанного в таблице отслеживания DHCP, будут отброшены.
- Записи в таблице изучаются только для доверенных интерфейсов. Запись динамически добавляется или удаляется в таблицу отслеживания DHCP, когда клиент получает или освобождает IP-адрес от DHCP-сервера. Каждая запись включает MAC-адрес, IP-адрес, время аренды, идентификатор VLAN и идентификатор порта.
- Когда отслеживание DHCP включено, сообщения DHCP, поступающие на ненадежный интерфейс, фильтруются на основе динамических записей, полученных с помощью отслеживания DHCP.

- Если пакет DHCP от клиента соответствует критериям фильтрации, он будет перенаправлен только на доверенные порты в той же VLAN.
- Если DHCP-пакет от сервера получен через доверенный порт, он будет перенаправлен как на доверенные, так и на ненадежные порты в одной и той же VLAN.
- Если отслеживание DHCP отключено глобально, все динамические привязки удаляются из таблицы привязок.

7.9.3 Настройка отслеживания DHCP

После нажатия «Security Configure»> «DHCP»> «Snooping Setting» появится следующий экран.

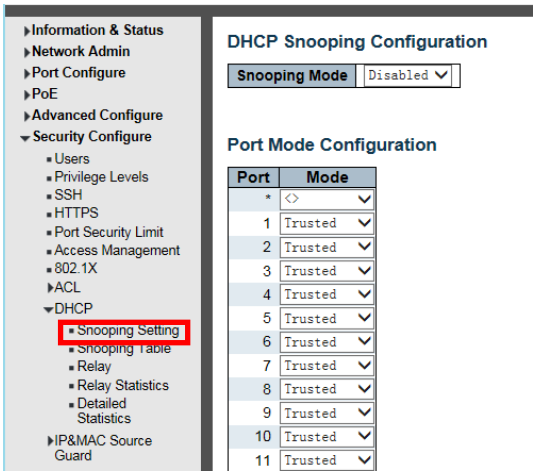


Рисунок 7-9-3 Экран конфигурации DHCP Snooping

DHCP Snooping Mode
Указывает на работу режима отслеживания DHCP. Возможные режимы:
Включено: включить режим отслеживания DHCP. Когда включен режим отслеживания DHCP, сообщения с запросами DHCP будут пересылаться на доверенные порты и разрешать ответные пакеты только от доверенных портов.
Отключено: отключение режима отслеживания DHCP.
Port Mode Configuration
Указывает режим порта отслеживания DHCP.
Возможные режимы порта:
Trusted: настраивает порт как надежный источник сообщений DHCP.
Untrusted: настраивает порт как ненадежный источник сообщений DHCP.

Нажмите «Save», чтобы сохранить активные настройки

7.9.4 Snooping Table Таблица слежения

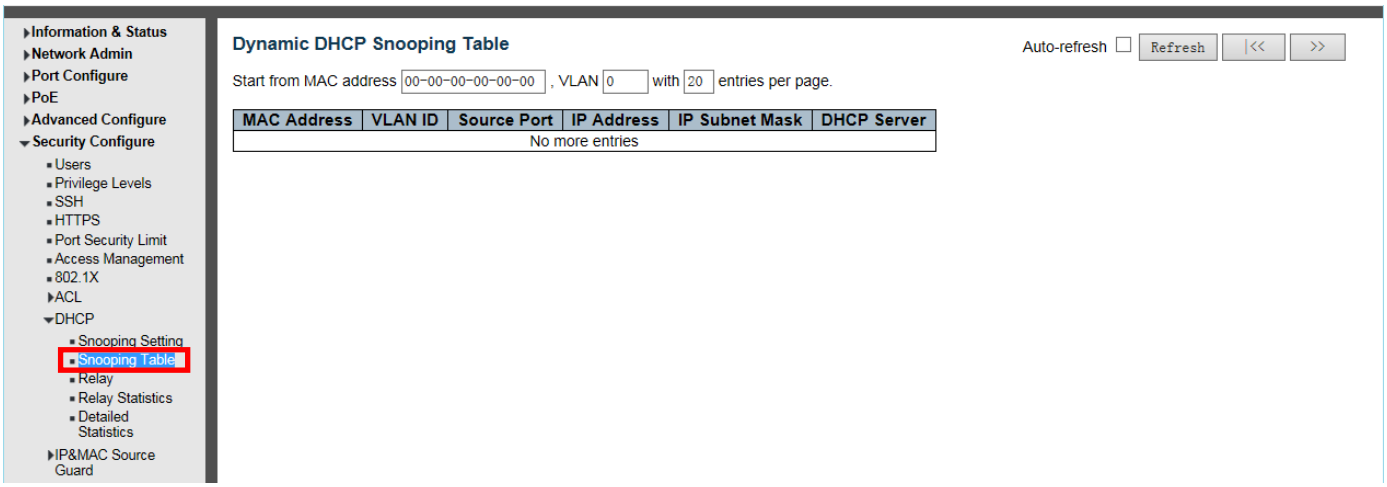


Рисунок 7-9-4 Экран конфигурации Таблицы слежения

На этой странице отображается информация о назначении динамического IP-адреса после отключения режима DHCP Snooping. Все клиенты DHCP, получившие динамический IP-адрес от DHCP-сервера, будут перечислены в этой таблице, за исключением IP-адресов локального интерфейса VLAN. На этой странице показаны записи в таблице динамического отслеживания DHCP.

Перемещение по таблице отслеживания DHCP

На каждой странице отображается до 99 записей из таблицы динамического отслеживания DHCP, по умолчанию 20, выбираемых в поле ввода «записей на страницу». При первом посещении веб-страница покажет первые 20 записей с начала таблицы динамического отслеживания DHCP.
Поля ввода «MAC-адрес» и «VLAN» позволяют пользователю выбрать начальную точку в таблице динамического отслеживания DHCP. Нажатие кнопки обновит отображаемую таблицу, начиная с этого или ближайшего следующего совпадения с таблицей динамического отслеживания DHCP. Кроме того, два поля ввода - при нажатии кнопки - принимают значение первой отображаемой записи, обеспечивая непрерывное обновление с тем же начальным адресом.
В качестве основы для следующего поиска будет использоваться последняя запись текущей отображаемой таблицы. По достижении конца в отображаемой таблице отображается текст «Больше записей нет». Используйте кнопку, чтобы начать заново.

Столбцы таблицы отслеживания DHCP
MAC Address
MAC-адрес пользователя записи.
ID VLAN
ID VLAN, в котором разрешен трафик DHCP.
Source Port
Номер порта коммутатора, для которого отображаются записи.
IP- Address
IP-адрес пользователя записи.
IP Subnet Mask
Маска IP-подсети пользователя записи.
DHCP
Адрес сервера DHCP Адрес сервера записи.

7.9.5 Relay (DHCP-ретрансляция)

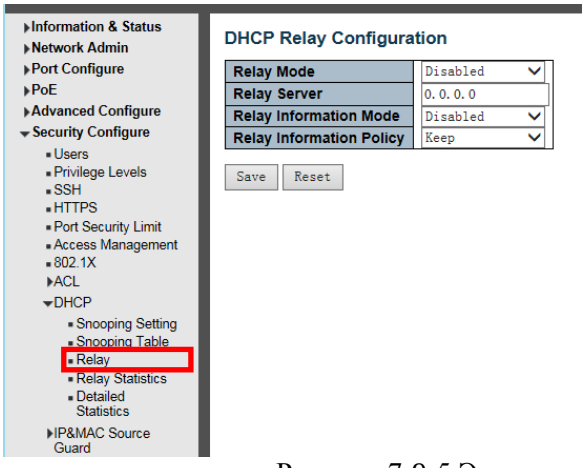


Рисунок 7-9-5 Экран конфигурации Таблицы DHCP-ретрансляции

DHCP Relay Configuration Конфигурация DHCP-ретрансляции

Агент ретрансляции DHCP используется для пересылки и передачи сообщений DHCP между клиентами и сервером, когда они не находятся в одном домене подсети. Он сохраняет IP-адрес входящего интерфейса в поле GIADDR пакета DHCP. Сервер DHCP может использовать значение поля GIADDR для определения

назначенной подсети. В таком случае убедитесь, что коммутатор правильно настроил IP-адрес интерфейса VLAN и PVID (идентификатор порта VLAN).

Relay Mode Режим ретрансляции
Указывает на работу режима ретрансляции DHCP.
Возможные режимы:
Включено: включить режим ретрансляции DHCP. Когда включен режим ретрансляции DHCP, агент пересылает и передает сообщения DHCP между клиентами и сервером, когда они не находятся в одном домене подсети. И широковещательное сообщение DHCP не будет переполнено из соображений безопасности.
Отключено: отключение режима ретрансляции DHCP.

Relay Server Сервер ретрансляции
Указывает IP-адрес сервера ретрансляции DHCP.

Relay Information Mode Информационный режим ретрансляции

Указывает на работу опции режима передачи информации DHCP. Формат идентификатора цепи опции 82 как "[vlan_id] [module_id] [port_no]". Первые четыре символа представляют собой идентификатор VLAN, пятый и шестой символы - это идентификатор модуля (в автономном устройстве он всегда равен 0, в наращиваемом устройстве это означает идентификатор коммутатора), а последние два символа - это номер порта. Например, «00030108» означает, что сообщение DHCP получено с идентификатора VLAN 3, идентификатора коммутатора 1, порта № 8. А значение удаленного идентификатора опции 82 равно MAC-адресу коммутатора.
Возможные режимы:
Enabled Включено: Включение режима передачи информации DHCP. Когда включен режим передачи информации DHCP, агент вставляет определенную информацию (параметр 82) в сообщение DHCP при пересылке на сервер DHCP и удаляет ее из сообщения DHCP при передаче на клиент DHCP. Работает только при включенном режиме работы DHCP- ретрансляции.
Отключено: отключение работы в информационном режиме DHCP-реле.

Relay Information Policy Информационная политика реле
Указывает политику параметра информации о ретрансляции DHCP. При включении режима передачи информации DHCP, если агент получает сообщение DHCP, которое уже содержит информацию агента ретрансляции, он применяет политику. Политика «Replace» недействительна, если режим информации реле отключен.
Возможные политики:
Replace: заменить исходную информацию о реле при получении сообщения DHCP, которое уже содержит ее.
Keep: сохранить исходную информацию о реле при получении сообщения DHCP, которое уже содержит ее.
Drop: отбросить пакет, когда получено сообщение DHCP, которое уже содержит информацию о ретрансляции.

Нажмите «Save», чтобы сохранить активные настройки

7.9.6 Relay Statistics (Статистика ретрансляций DHCP)

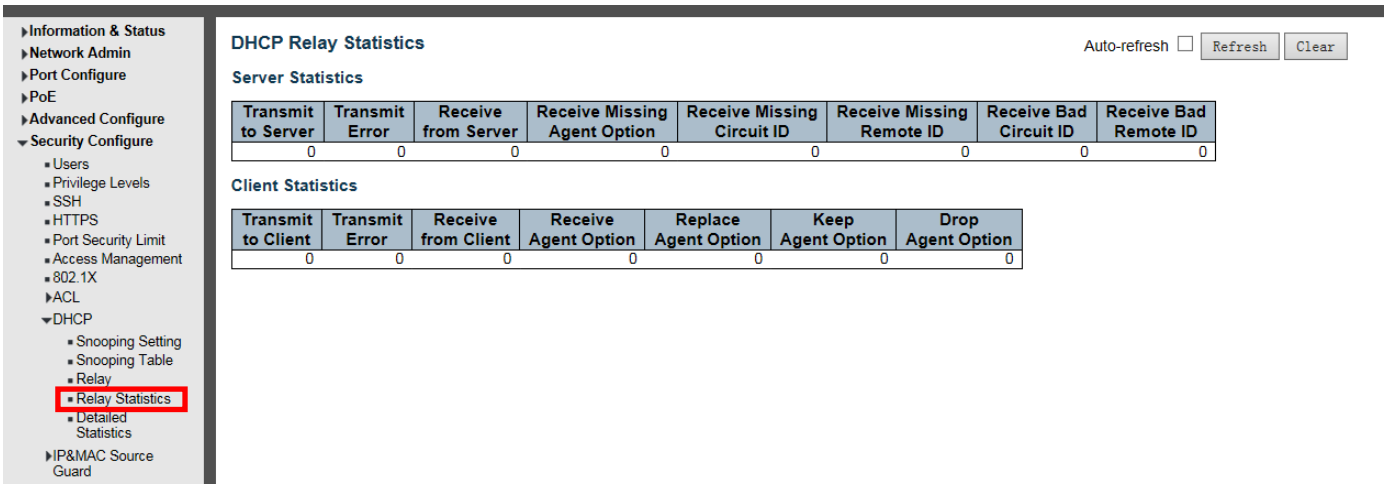


Рисунок 7-9-6 Экран конфигурации статистики DHCP-ретрансляции

Server Statistics

Transmit to Server

Количество пакетов, передаваемых от клиента к серверу.

Transmit Error

Количество пакетов, которые привели к ошибкам при отправке клиентам.

Receive from Server

Количество пакетов, полученных от сервера.

Receive Missing Agent Option

Количество пакетов, полученных без параметров информации агента.

Receive Missing Circuit ID

Количество пакетов, полученных с отсутствующей опцией Circuit ID.

Receive Missing Remote ID

Количество пакетов, полученных с отсутствующей опцией Remote ID.

Receive Bad Circuit ID

Количество пакетов, для которых параметр Circuit ID не соответствует известному идентификатору канала.

Receive Bad Remote ID

Количество пакетов, для которых параметр удаленного идентификатора не соответствует известному удаленному идентификатору.

Client Statistics

Transmit to Client

Количество ретранслируемых пакетов от сервера к клиенту.

Transmit Error

Количество пакетов, которые привели к ошибке при отправке на серверы.

Receive from Client

Количество пакетов, полученных от сервера.

Receive Agent Option

Количество полученных пакетов с опцией информации агента ретрансляции.

Replace Agent Option

Количество пакетов, которые были заменены опцией информации агента ретрансляции.

Keep Agent Option

Количество пакетов, для которых сохранена информация агента ретрансляции.

Drop Agent Option

Количество отброшенных пакетов, полученных с информацией агента ретрансляции.

7.9.7 Detailed Statistics (Подробная статистика)

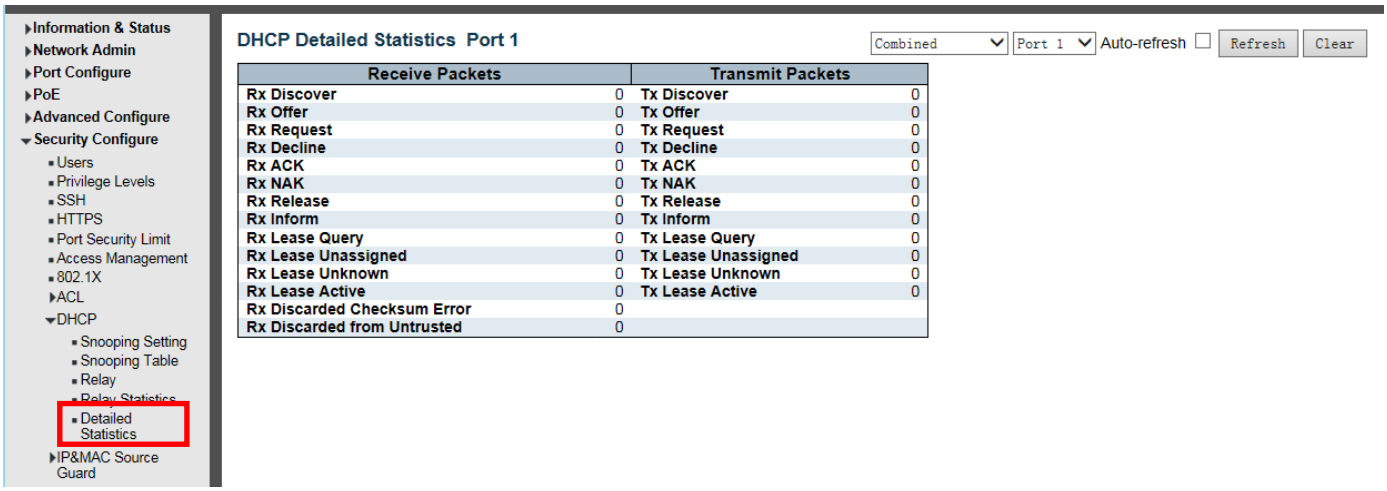


Рисунок 7-9-7 Экран подробной статистики DHCP

DHCP Detailed Statistics

На этой странице представлена статистика отслеживания DHCP. Обратите внимание, что обычная статистика пересылки для каждого порта не увеличивается, если входящий пакет DHCP выполняется с помощью механизма пересылки L3. И очистка статистики для определенного порта может не повлиять на глобальную статистику, поскольку она собирает обзор различных уровней.

Receive and Transmit Packets Прием и передача пакетов

Rx и Tx Discover -Количество полученных и переданных пакетов обнаружения (опция 53 со значением 1).
Rx и Tx Offer -Количество полученных и переданных пакетов предложений (опция 53 со значением 2). Rx и Tx Request - количество принятых и переданных пакетов запроса (опция 53 со значением 3).
Rx and Tx Decline - количество принятых и переданных пакетов отклонения (опция 53 со значением 4).
Rx и Tx ACK - количество принятых и переданных пакетов ACK (опция 53 со значением 5).
Rx и Tx NAK - количество принятых и переданных пакетов NAK (опция 53 со значением 6).
Rx и Tx Release -Количество полученных и переданных пакетов Release (опция 53 со значением 7).
Rx и Tx Inform - количество принятых и переданных пакетов inform (опция 53 со значением 8).
Rx и Tx Lease Query -Количество полученных и переданных пакетов запроса аренды (опция 53 со значением 10).
Rx и Tx Lease Unassigned- Количество полученных и переданных пакетов без назначения аренды (опция 53 со значением 11).
Rx и Tx Lease Unknown - Количество полученных и переданных пакетов с неизвестной арендой (опция 53 со значением 12).
Rx и Tx Lease Active - Количество принятых и переданных пакетов аренды (опция 53 со значением 13). Rx Discarded checksum error - Число отклоненных пакетов, для которых контрольная сумма IP / UDP является ошибочной.
Rx Discarded from Untrusted -Количество отброшенных пакетов, приходящих с ненадежного порта.

7.10 IP&MAC Source Guard(Защита источника IP и MAC)

7.10.1 IP Source Guard Configuration

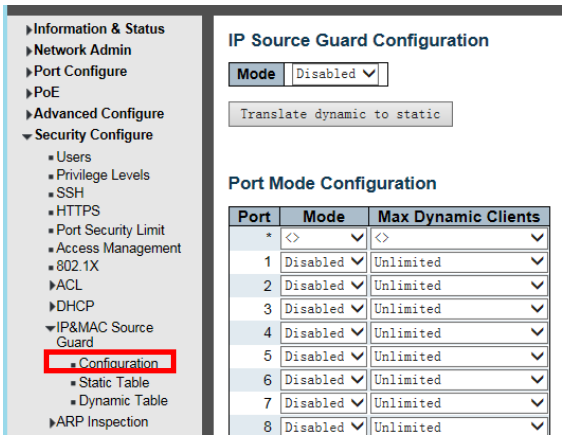


Рисунок 7-10-1 Экран конфигурации защиты источника IP и MAC

На этой странице представлена конфигурация, относящаяся к IP Source Guard.

Режим конфигурации IP Source Guard

Включите Global IP Source Guard или отключите Global IP Source Guard. Все настроенные ACE будут потеряны при включении режима.

Конфигурация режима порта

Укажите, на каких портах включена защита IP-источника. Только тогда, когда для данного порта включены и глобальный режим, и режим порта, IP Source Guard включен для этого данного порта.

Max Dynamic Clients Максимальное количество динамических клиентов

Укажите максимальное количество динамических клиентов, которые могут быть изучены на данном порту. Это значение может быть 0, 1, 2 или неограниченно. Если режим порта включен и значение max dynamic client равно 0, это означает, что разрешена пересылка только IP-пакетов, которые совпадают в статических записях на конкретном порту.

Нажмите «Save», чтобы сохранить активные настройки

7.10.2 Static IP Source Guard Table

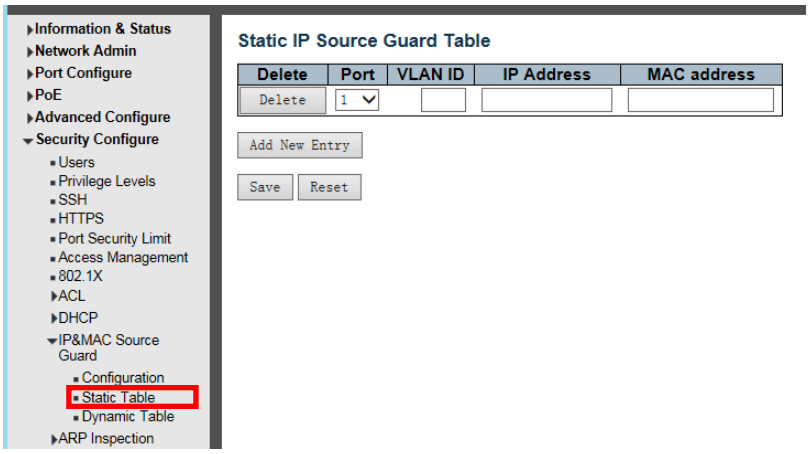


Рисунок 7-10-2 Экран Таблица защиты источника статического IP-адреса

На этой странице показаны правила защиты источника для статических IP адресов. Максимальное количество правил на коммутаторе - 112.

Delete - Отметьте, чтобы удалить запись. Он будет удален при следующем сохранении.

Port - Логический порт для настроек.

VLAN ID - идентификатор VLAN для настроек.

IP Address -Разрешенный исходный IP-адрес.

MAC address - Разрешенный исходный MAC-адрес

Нажмите «Save», чтобы сохранить активные настройки

7.10.3 Dynamic IP Source Guard Table

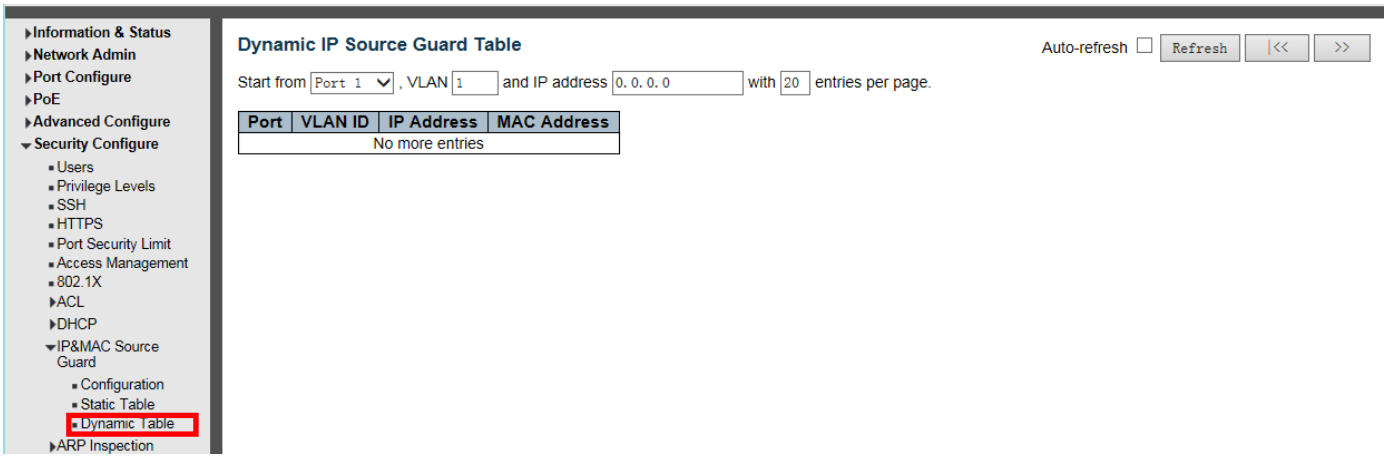


Рисунок 7-10-3 Экран Таблица защиты источника динамического IP-адреса

На этой странице показаны записи в таблице защиты источника динамических IP-адресов. Таблица защиты источника динамического IP-адреса сортируется сначала по портам, затем по идентификатору VLAN, затем по IP-адресу, а затем по MAC-адресу.

Навигация по таблице защиты IP-источника

На каждой странице отображается до 99 записей из таблицы защиты источника динамического IP-адреса, значение по умолчанию - 20, выбираемых с помощью поля ввода «записей на страницу». При первом посещении веб-страница покажет первые 20 записей с начала таблицы защиты источника динамического IP-адреса.
Поля ввода «Начать с адреса порта», «VLAN» и «IP-адрес» позволяют пользователю выбрать начальную точку в таблице защиты источника динамического IP-адреса. Нажатие кнопки обновит отображаемую таблицу, начиная с этого или ближайшего следующего совпадения с таблицей защиты источника динамического IP-адреса. Кроме того, два поля ввода - при нажатии кнопки - принимают значение первой отображаемой записи, обеспечивая непрерывное обновление с тем же начальным адресом.
В качестве основы для следующего поиска будет использоваться последняя запись текущей отображаемой таблицы. По достижении конца в отображаемой таблице отображается текст «Больше записей нет». Используйте кнопку, чтобы начать заново.

Столбцы таблицы IP Source Guard
PortSwitch -Номер порта, для которого отображаются записи.
ID VLAN - ID VLAN, в котором разрешен IP-трафик.
P-адрес - IP-адрес пользователя записи.
MAC-адрес - MAC-адрес источника.

7.11 ARP Inspection Проверка ARP

Динамическая проверка ARP (DAI) - это функция безопасности. На хост или устройства, подключенные к сетям уровня 2, могут быть запущены несколько типов атак путем «отравления» кэшей ARP. Эта функция используется для блокировки таких атак. Только действительные запросы и ответы ARP могут проходить через DUT. Динамический ARP предотвращает ненадежные пакеты ARP на основе базы данных отслеживания DHCP. На этой странице представлена конфигурация, относящаяся к проверке ARP.

7.11.1 Port Configuration

Пользователь может настроить порт на этой странице. После нажатия «Security Configure»> «ARP Inspection»> «Port Configuration» появится следующий экран.

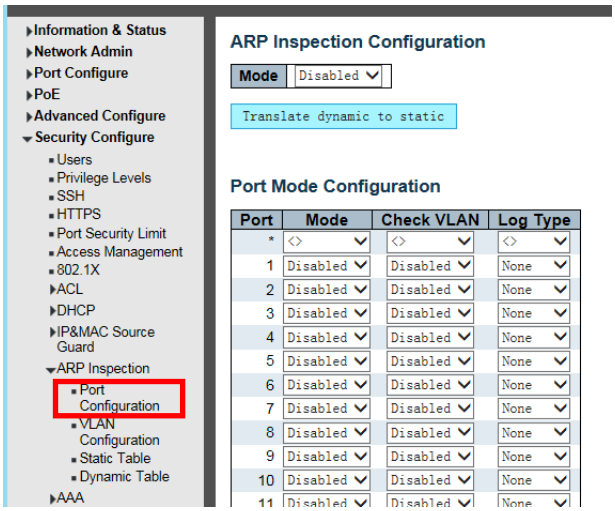


Рисунок 7-11-1 Экран конфигурации проверки ARP порта

Режим конфигурации проверки ARP Включите глобальную проверку ARP или отключите глобальную проверку ARP. Конфигурация режима порта Укажите, на каких портах включена проверка ARP. Только тогда, когда на данном порте включены и глобальный режим, и режим порта, для данного порта включается проверка ARP. Возможные режимы:
Enabled:включить операцию проверки ARP.
Disabled: отключить операцию проверки ARP.

Если вы хотите проверить конфигурацию VLAN, вы должны включить настройку «Проверить VLAN». По умолчанию параметр «Проверить VLAN» отключен. Когда параметр «Проверить VLAN» отключен, тип журнала проверки ARP будет относиться к настройке порта. Когда параметр «Проверить VLAN» включена, тип журнала проверки ARP будет относиться к настройке VLAN.
Возможные настройки «Проверить VLAN»:
Enabled: Включить проверку работы VLAN.
Disabled: отключить проверку работы VLAN.
Только когда глобальный режим и режим порта для данного порта включены, а настройка «Проверка VLAN» отключена, тип журнала проверки ARP будет относиться к настройке порта. Существует четыре типа журналов:
None: ничего не записывать.
Deny: записывать отклоненные записи.
Permit: регистрировать разрешенные записи.
All: записывать все записи.

Нажмите «Save», чтобы сохранить активные настройки

7.11.2 VLAN Configuration

После нажатия «Security Configure»> «ARP Inspection»> «VLAN Configuration» появится следующий экран.

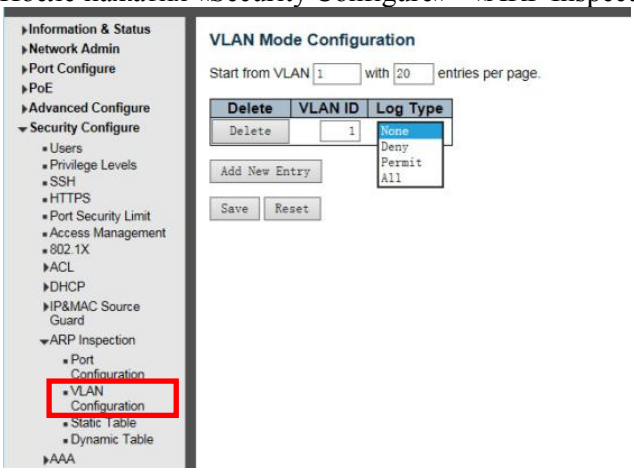


Рисунок 7-11-2 Экран конфигурации проверки ARP VLAN

Навигация по конфигурации VLAN

На каждой странице отображается до 9999 записей из таблицы VLAN, по умолчанию - 20, выбранных в поле ввода «записей на страницу». При первом посещении веб-страница покажет первые 20 записей с начала таблицы VLAN. Первым отображается тот, у которого самый низкий идентификатор VLAN из таблицы VLAN.

Поля ввода «VLAN» позволяют пользователю выбрать начальную точку в таблице VLAN. Нажатие кнопки Refresh обновит отображаемую таблицу, начиная с этой или ближайшей следующей таблицы VLAN.

Конфигурация режима VLAN - Укажите, в каких сетях VLAN включена проверка ARP. Во-первых, вы должны включить настройку порта на веб-странице конфигурации режима порта. Только тогда, когда на данном порте включены и глобальный режим, и режим порта, для данного порта включается проверка ARP. Во-вторых, вы можете указать, какая VLAN будет проверяться на веб-странице конфигурации режима VLAN. Тип журнала также можно настроить для каждой настройки VLAN.

Возможные типы:

None: ничего не записывать.

Deny: записывать отклоненные записи.

Permit: регистрировать разрешенные записи.

All: записывать все записи.

Нажмите «Save», чтобы сохранить активные настройки

7.11.3 Static Table

Пользователь может вручную настроить статическую таблицу проверки ARP для управления портом. После нажатия «Security Configure»> «ARP Inspection»> «Static Table» появится следующий экран.

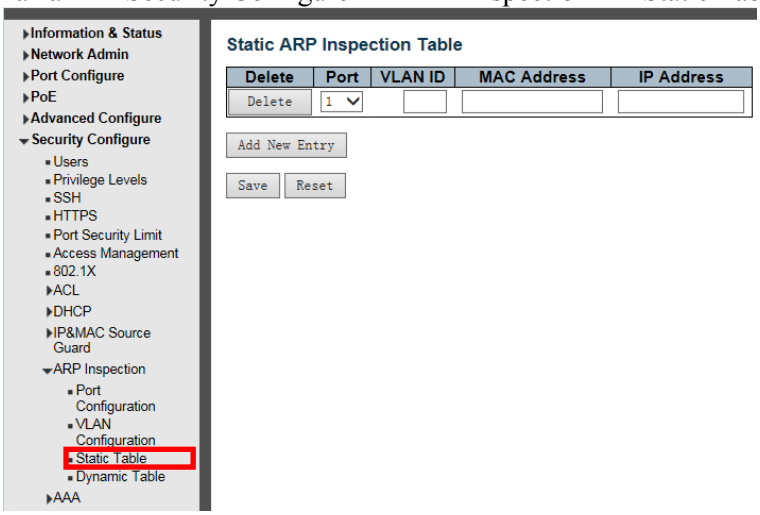


Рисунок 7-11-3 Экран конфигурации статической проверки ARP

На этой странице показаны статические правила проверки ARP.
Максимальное количество правил на коммутаторе - 256.
Delete - Отметьте, чтобы удалить запись. Он будет удален при следующем сохранении.
Port - Логический порт для настроек.
VLAN ID - Идентификатор vlan для настроек.
MAC Address - Разрешенный MAC-адрес источника в пакетах запроса ARP.
IP Address -Разрешенный IP-адрес источника в пакетах запроса ARP.

Нажмите «Save», чтобы сохранить активные настройки

7.11.4 Dynamic Table

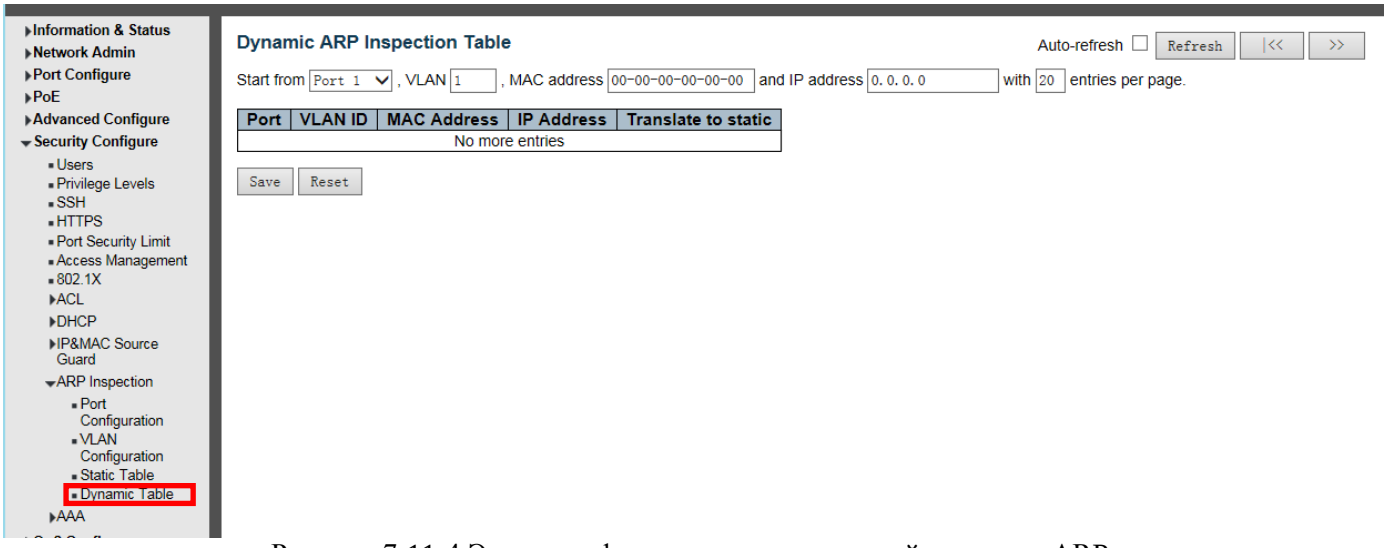


Рисунок 7-11-4 Экран конфигурации динамической проверки ARP

На этой странице показаны записи в таблице динамической проверки ARP. Таблица динамической проверки ARP содержит до 256 записей и сортируется сначала по портам, затем по идентификатору VLAN, затем по MAC-адресу, а затем по IP-адресу. Все динамические записи обучаются с помощью DHCP Snooping.

Навигация по таблице проверки ARP

На каждой странице отображается до 99 записей из таблицы динамической проверки ARP (по умолчанию 20), выбранных в поле ввода «записей на страницу». При первом посещении веб-страница покажет первые 20 записей с начала таблицы динамической проверки ARP.

Поля ввода «Начать с адреса порта», «VLAN», «MAC-адрес» и «IP-адрес» позволяют пользователю выбрать начальную точку в таблице динамической проверки ARP. Нажатие на кнопку обновит отображаемую таблицу, начиная с этого или ближайшего следующего совпадения с таблицей динамической проверки ARP. Кроме того, два поля ввода - при нажатии кнопки - принимают значение первой отображаемой записи, обеспечивая непрерывное обновление с тем же начальным адресом.

В качестве основы для следующего поиска будет использоваться последняя запись текущей отображаемой таблицы. По достижении конца в отображаемой таблице отображается текст «Больше записей нет». Используйте кнопку, чтобы начать заново.

Столбцы таблицы проверки ARP
PortSwitch - Номер порта, для которого отображаются записи.
VLAN ID - VLAN-ID, в котором разрешен трафик ARP.
MAC Address - MAC-адрес пользователя записи.
IP Address - IP-адрес пользователя записи.
Translate to static - Установите флажок, чтобы преобразовать запись в статическую запись.

Нажмите «Save», чтобы сохранить активные настройки

7.12 AAA

AAA (Authentication, Authorization, Accounting)- аутентификация, авторизация и учет.
Простым языком принцип AAA можно описать так: для совершения какого-либо действия в сети мы должны проследить, кто инициирует это действие (authentication), имеет ли он право на выполнение этого действия (authorization) и что в журнал записаны все действия, которые он совершил (accounting).

7.12.1 RADIUS Server Configuration

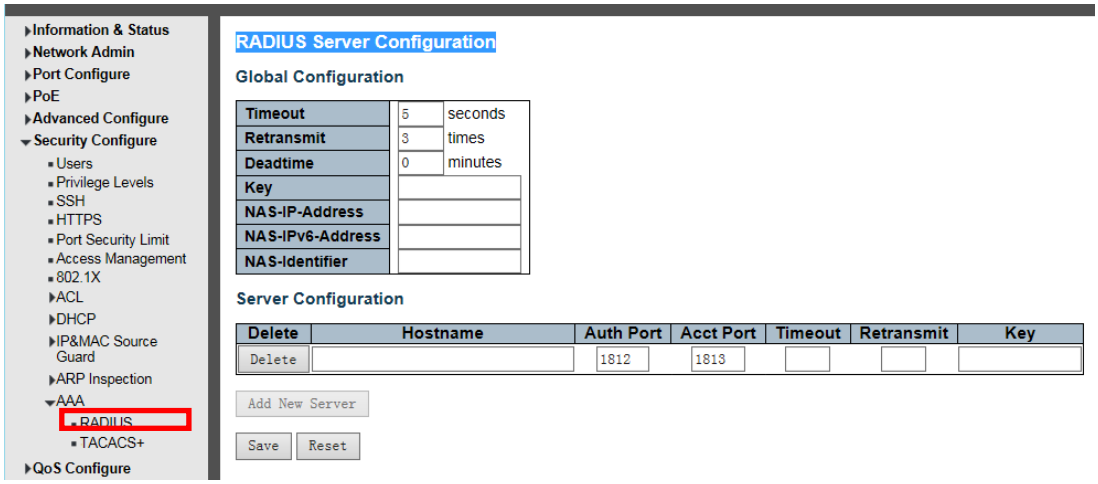


Рисунок 7-12-1 Экран настройки серверов RADIUS.

Эта страница позволяет вам настроить серверы RADIUS.

Global Configuration Глобальная конфигурация

Эти настройки являются общими для всех серверов RADIUS.
Timeout Тайм-аут - это количество секунд в диапазоне от 1 до 1000 для ожидания ответа от сервера RADIUS перед повторной передачей запроса.
Retransmit Повторная передача - это количество раз в диапазоне от 1 до 1000, когда запрос RADIUS повторно передается на сервер, который не отвечает. Если сервер не ответил после последней повторной передачи, он считается мертвым.

Deadtime Мертвое время, которое может быть установлено в диапазоне от 0 до 1440 минут, - это период, в течение которого коммутатор не будет отправлять новые запросы на сервер, который не смог ответить на предыдущий запрос. Это предотвратит постоянные попытки коммутатора связаться с сервером, который он уже определил как неработающий.
Установка Deadtime на значение больше 0 (ноль) включит эту функцию, но только если настроено более одного сервера.
Key - Секретный ключ длиной до 63 символов, совместно используемый сервером RADIUS и коммутатором.
NAS-IP-Address (Attribute 4) - Адрес IPv4, который будет использоваться как атрибут 4 в пакетах запроса доступа RADIUS. Если это поле оставлено пустым, используется IP-адрес исходящего интерфейса.
NAS-IPv6-Address (Attribute 95) - Адрес IPv6, который будет использоваться в качестве атрибута 95 в пакетах запроса доступа RADIUS. Если это поле оставлено пустым, используется IP-адрес исходящего интерфейса.
NAS-Identifier (Attribute 32) - Идентификатор длиной до 253 символов, который будет использоваться как атрибут 32 в пакетах запроса доступа RADIUS. Если это поле оставить пустым, NAS-идентификатор не включен в пакет.

Конфигурация сервера

В таблице есть одна строка для каждого сервера RADIUS и несколько столбцов, а именно:
Delete - Установите этот флажок, чтобы удалить запись сервера RADIUS. Запись будет удалена при следующем сохранении.
Hostname - IP-адрес или имя хоста сервера RADIUS.
Auth Port - Порт UDP для использования на сервере RADIUS для аутентификации. Установите 0, чтобы отключить аутентификацию.
Auth Port - Порт UDP, используемый на сервере RADIUS для учета. Установите 0, чтобы отключить учет.
Timeout - Этот необязательный параметр переопределяет значение глобального тайм-аута. Если оставить поле пустым, будет использоваться значение глобального тайм-аута.
Retransmit - Этот необязательный параметр отменяет глобальное значение повторной передачи. Если оставить это поле пустым, будет использоваться значение глобальной повторной передачи.
Key - Этот необязательный параметр имеет приоритет над глобальным ключом. Если оставить поле пустым, будет использоваться глобальный ключ.

Нажмите «Save», чтобы сохранить активные настройки

7.12.2 TACACS+ Server Configuration

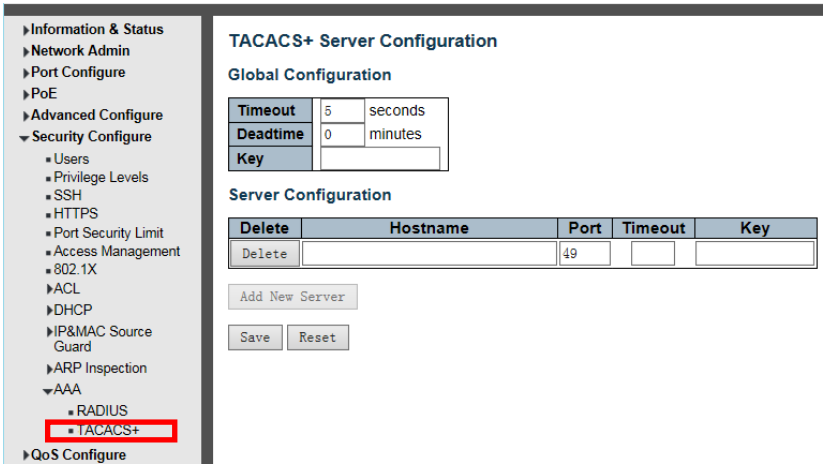


Рисунок 7-12-2 Экран настройки серверов TACACS+

Эта страница позволяет вам настроить серверы TACACS +.

Global Configuration Глобальная конфигурация
Эти настройки являются общими для всех серверов TACACS +.
Timeout - это количество секунд в диапазоне от 1 до 1000 для ожидания ответа от сервера TACACS +, прежде чем он будет считаться неработающим.

Deadtime - Deadtime, который может быть установлен в диапазоне от 0 до 1440 минут, - это период, в течение которого коммутатор не будет отправлять новые запросы на сервер, который не смог ответить на предыдущий запрос. Это предотвратит постоянные попытки коммутатора связаться с сервером, который он уже определил как неработающий.
Установка Deadtime на значение больше 0 (ноль) включит эту функцию, но только если настроено более одного сервера.
Key - Секретный ключ длиной до 63 символов, совместно используемый сервером TACACS + и коммутатором.

Server Configuration Конфигурация сервера

В таблице есть одна строка для каждого сервера TACACS + и несколько столбцов, а именно:
Delete -Установите этот флажок, чтобы удалить запись сервера TACACS +. Запись будет удалена при следующем сохранении.
Hostname - IP-адрес или имя хоста сервера TACACS +.
Port Порт TCP, используемый на сервере TACACS + для аутентификации.
Timeout - Этот необязательный параметр переопределяет значение глобального тайм-аута. Если оставить поле пустым, будет использоваться значение глобального тайм-аута.
Key - Этот необязательный параметр имеет приоритет над глобальным ключом. Если оставить поле пустым, будет использоваться глобальный ключ.

Нажмите «Save», чтобы сохранить активные настройки

8. Diagnostics
8.1 Ping

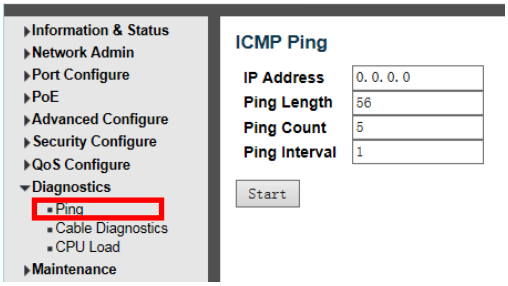


Рисунок 8-1 Экран настройки Ping

Эта страница позволяет отправлять пакеты ICMP PING для устранения проблем с подключением по IP. ICMP - это аббревиатура от Internet Control Message Protocol. Это протокол, который генерирует сообщения об ошибках, диагностику или маршрутизацию. Сообщения ICMP обычно содержат информацию о трудностях маршрутизации или простых обменах, таких как временные метки или эхо-транзакции.

IP Address - IP-адрес назначения, необходимый для проверки связи.
Ping Length - Введите число от 1 до 1452. По умолчанию: 56.
Ping Count - Количество пакетов ICMP. Значения варьируются от 1 раза до 60.
Ping Interval - Интервал времени для Ping (интервал отправки для каждого пакета ICMP)

8.2 Cable Diagnostics

Программа диагностики кабеля выполняет тесты медных кабелей 10/100 / 1000BASE-T. Эти функции позволяют определять длину кабеля и условия эксплуатации, а также изолировать множество распространенных неисправностей, которые могут возникнуть в кабельной разводке витой пары Cat5. После нажатия «Диагностика»> «Диагностика кабеля» появится следующий экран.

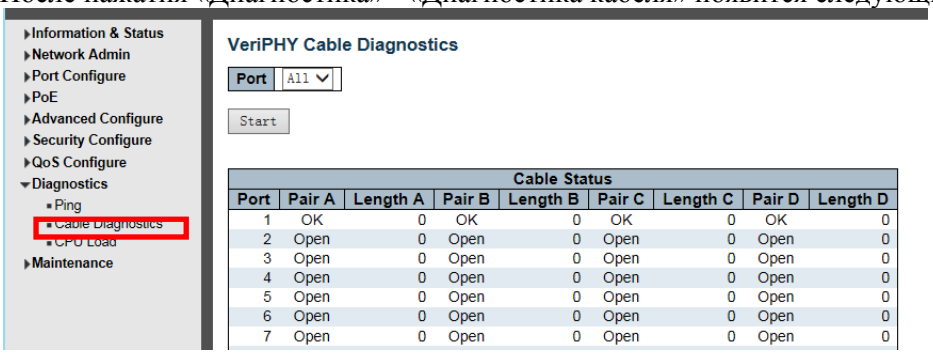


Рисунок 8-2 Экран настройки Ping

Эта страница используется для запуска VeriPHY Cable Diagnostics для медных портов 10/100 и 1G.

Нажмите S tart чтобы запустить диагностику. Это займет примерно 5 секунд. Если выбраны все порты, это может занять около 15 секунд. По завершении страница обновится автоматически, и вы сможете просмотреть результаты диагностики кабеля в таблице состояния кабеля. Обратите внимание, что VeriPHY точен только для кабелей длиной от 7 до 140 метров.
Порты 10 и 100 Мбит / с будут отключены во время работы VeriPHY. Следовательно, запуск VeriPHY на порту управления 10 или 100 Мбит / с приведет к тому, что коммутатор перестанет отвечать, пока VeriPHY не будет завершен.

Port - Порт, через который вы запрашиваете диагностику кабеля VeriPHY.

Состояние кабеля
Port: Номер порта.
Pair: Состояние кабельной пары.
OK - правильно завершенная пара
Open - Открытая пара
Short - короткая пара
Short A - перекрестная короткая пара на пару A
Short B - перекрестная короткая пара на пару B
Short C - перекрестная короткая пара на пару C
Short D - перекрестное короткое замыкание пары на пару D
Cross A - ненормальное соединение пары с парой A
Cross B - ненормальное соединение пары с парой B
Cross C - ненормальное соединение пары с парой C
Cross D - ненормальное соединение пары с парой D
Length: Длина (в метрах) кабельной пары. Разрешение 3 метра

8.3 CPU Load (загрузка ЦП)

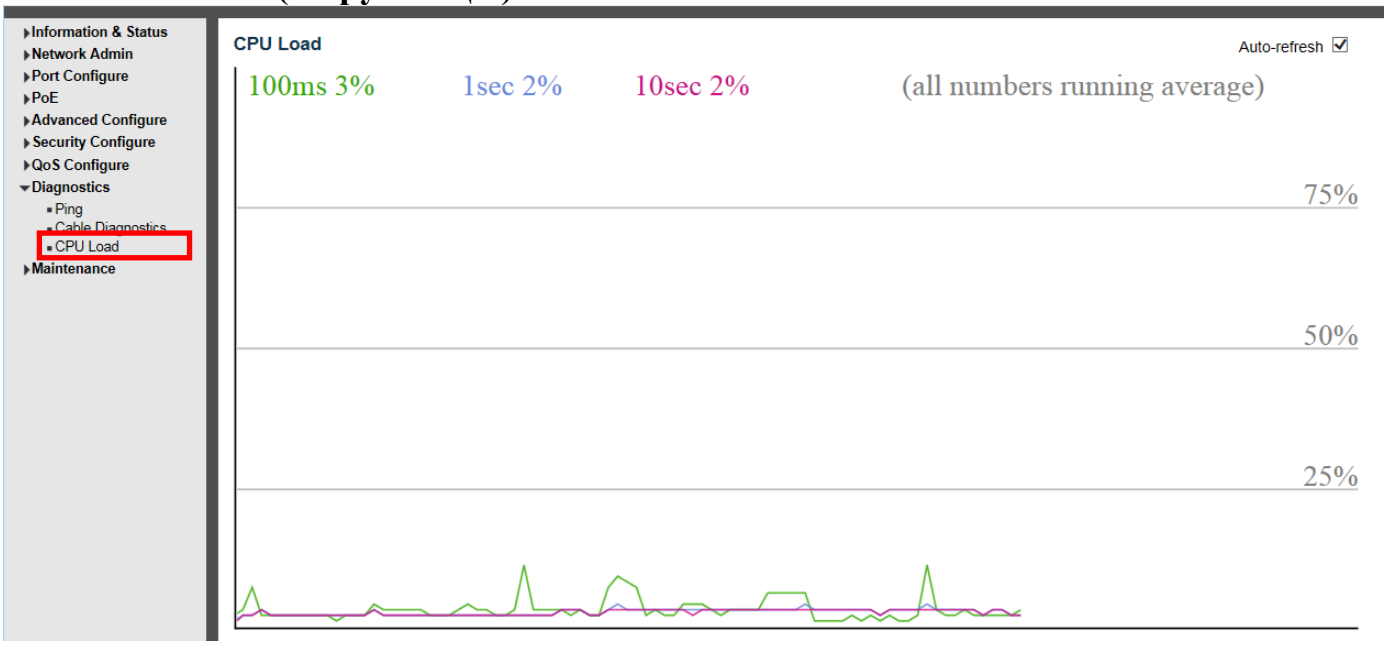


Рисунок 8-3 Экран загрузки ЦП

На этой странице отображается загрузка ЦП с использованием графика SVG.

Нагрузка измеряется как среднее значение за последние 100 мс, 1 с и 10 секунд. Последние 120 образцов отображаются в виде графика, а последние числа также отображаются в виде текста.

Для отображения графика SVG ваш браузер должен поддерживать формат SVG. Обратитесь к SVG Wiki для получения дополнительной информации о поддержке браузеров. В частности, на момент написания в Microsoft Internet Explorer должен быть установлен плагин для поддержки SVG.

9.Maintenance Обслуживание

9.1 Restart Device

Эта страница предназначена для перезапуска коммутатора. После нажатия "Maintenance ">"Restart Device" появится следующий экран.

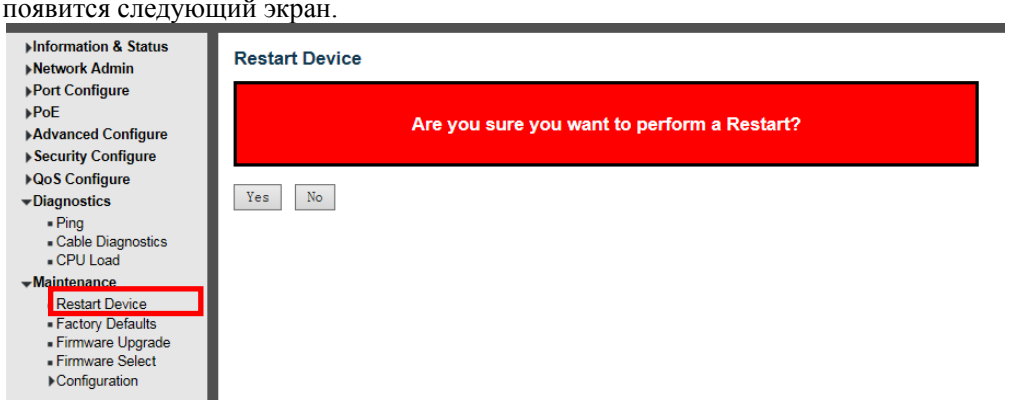


Рисунок 9-1 Экран перезапуска коммутатора

Нажмите «Yes», чтобы перезапустить коммутатор.

9.2 Factory Defaults

Эта страница предназначена для восстановления заводских настроек по умолчанию. После нажатия "Maintenance ">"Factory Defaults" появится экран:

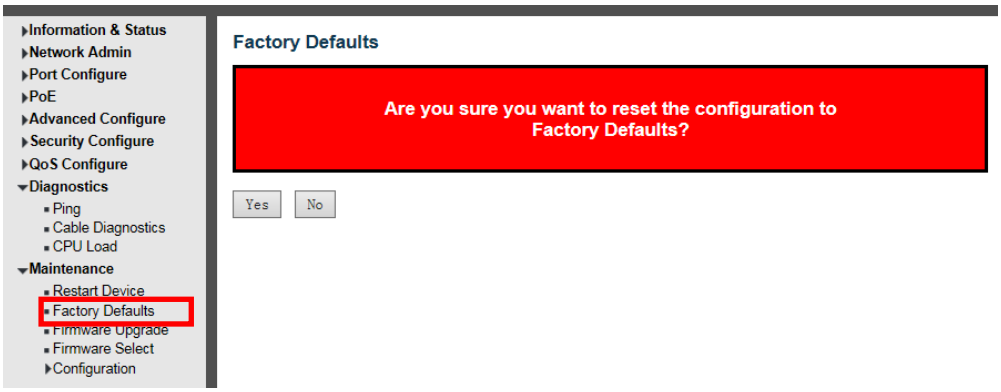


Рисунок 9-2 Экран сброса в заводские установки коммутатора

Нажмите «Yes», чтобы восстановить заводские настройки по умолчанию

9.3 Firmware Upgrade

Эта страница предназначена для обновления прошивки системы. После нажатия "Maintenance ">"Firmware Upgrade",появится экран.

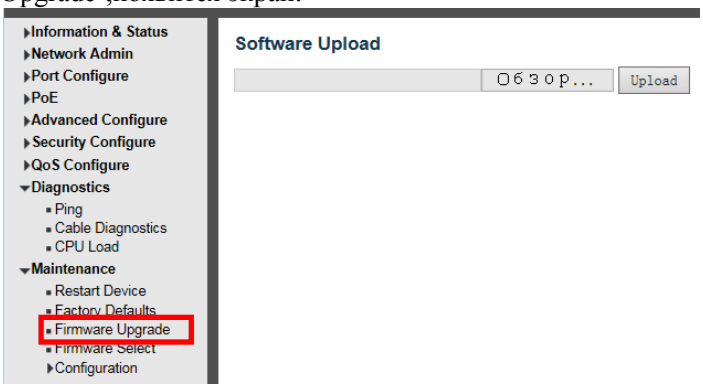


Рисунок 9-3 Экран обновления прошивки

Нажмите "Обзор", чтобы выбрать прошивку, которую необходимо обновить. Затем нажмите «Upload», чтобы начать обновление.

9.4 Firmware Select

Эта страница предназначена для выбора прошивки системы. После нажатия "Maintenance ">"Firmware Select" появится экран:

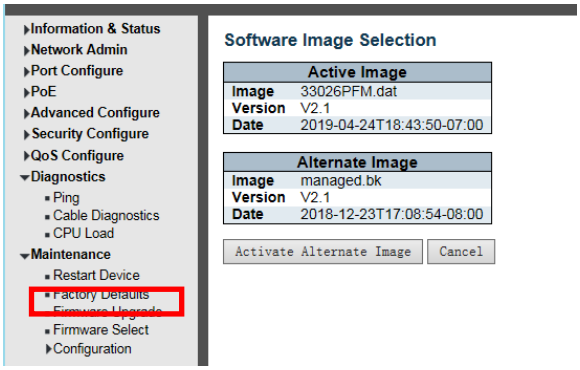


Рисунок 9-4 Экран выбора прошивки системы

На этой странице представлена информация об активных и альтернативных (резервных) образах микропрограмм в устройстве, а также можно вернуться к альтернативному образу.

На веб-странице отображаются две таблицы с информацией об активных и альтернативных образах прошивки.

Примечание:
1. Если активный образ встроенного ПО является альтернативным, отображается только таблица «Active Image». В этом случае кнопка "Activate Alternate Image" также неактивна.
2. Если альтернативный образ активен (из-за повреждения основного образа или из-за ручного вмешательства), загрузка нового образа микропрограммы на устройство автоматически использует слот основного образа и активирует его.
3. Информация о версии и дате прошивки может быть пустой для более старых версий прошивки. Это не является ошибкой.

Image Information Информация об образе
Image - Имя файла образа прошивки с момента последнего обновления образа.
Version - Версия образа прошивки.
Date - Дата выпуска прошивки.

9.5 Configuration

Коммутатор хранит свою конфигурацию в нескольких текстовых файлах в формате CLI. Файлы являются виртуальными (в ОЗУ) или хранятся во флэш-памяти на коммутаторе.

Доступные файлы:
• running-config: виртуальный файл, представляющий текущую активную конфигурацию коммутатора. Этот файл непостоянен.
• startup-config: стартовая конфигурация коммутатора, считываемая во время загрузки. Если этот файл не существует во время загрузки, коммутатор запустится в конфигурации по умолчанию.
• default-config: файл только для чтения с конфигурацией, зависящей от поставщика. Этот файл читается при восстановлении системы до настроек по умолчанию.
• До 31 других файлов, обычно используемых для резервного копирования конфигурации или альтернативных конфигураций.

Сохранить загрузочную конфигурацию
Скопировать running-config в startup-config, тем самым гарантируя, что текущая активная конфигурация будет использоваться при следующей перезагрузке.

9.5.1 Download Configuration File

После нажатия "Maintenance ">"Download" появится экран:

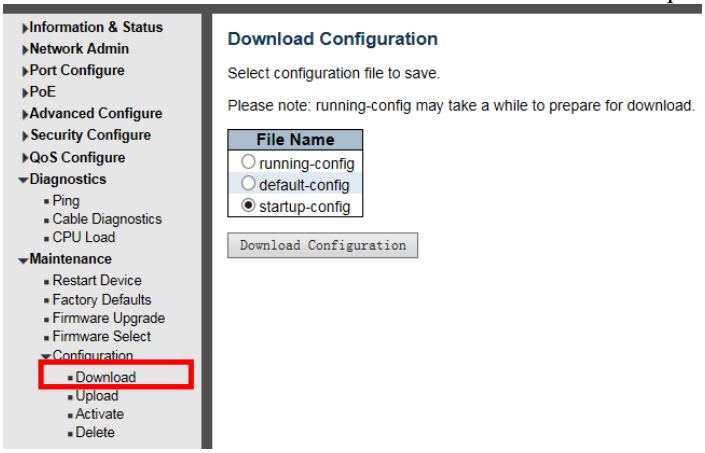


Рисунок 9-5-1 Экран скачивания файлов конфигурации

Пожалуйста, выберите файл и нажмите кнопку "Download Configuration"для загрузки.

9.5.2 Upload Configuration File

После нажатия "Maintenance ">"Upload" появится следующий экран. Затем пользователь может загрузить файл конфигурации.

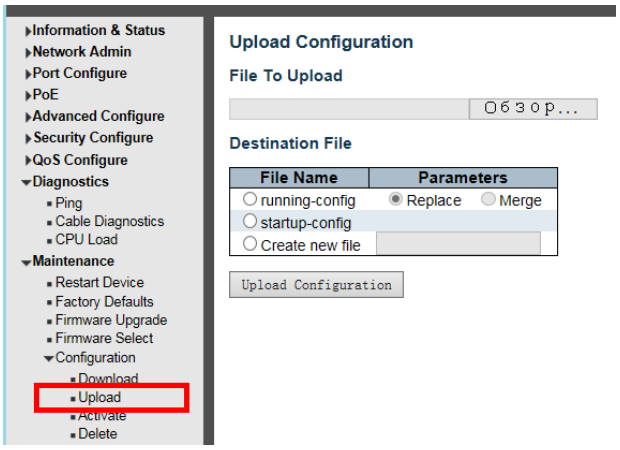


Рисунок 9-5-2 Экран загрузки файлов конфигурации

9.5.3 Activate Configuration

После нажатия "Maintenance ">"Activate"появится следующий экран. Затем пользователь может активировать файл конфигурации.

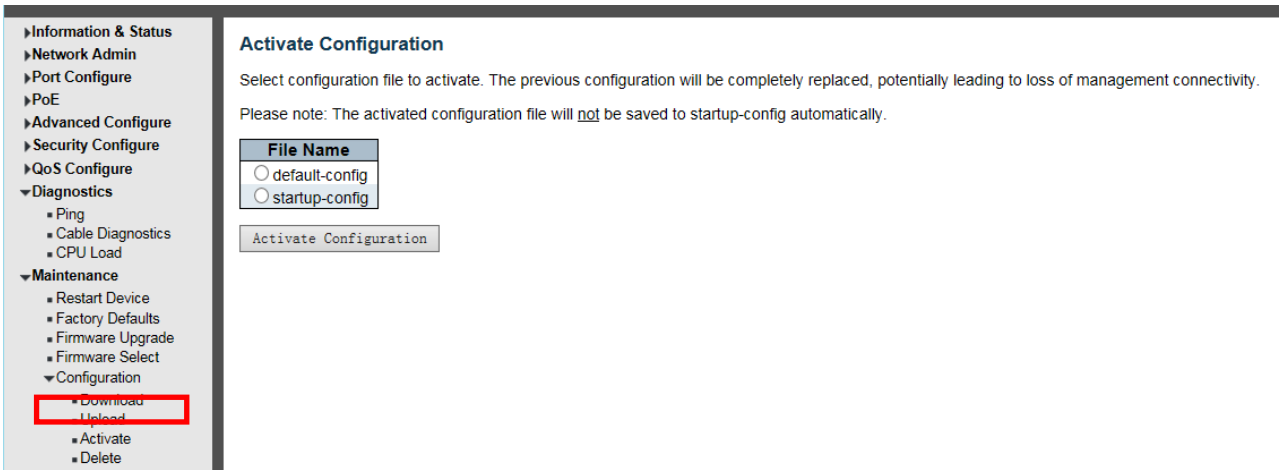


Рисунок 9-5-3 Экран активирования файлов конфигурации

9.5.4 Delete Configuration File

После нажатия "Maintenance ">"Delete" появится следующий экран. Затем пользователь может удалить файл конфигурации.

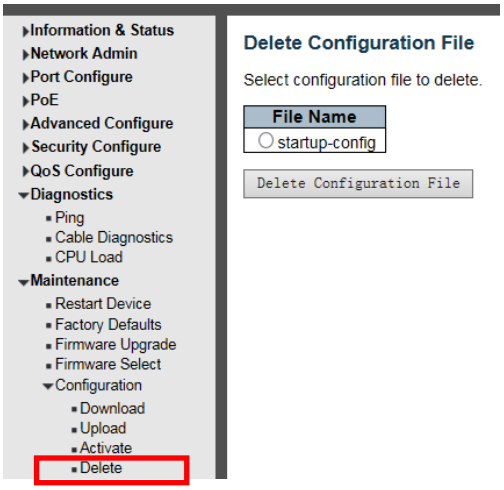


Рисунок 9-5-3 Экран удаления файла конфигурации

Приложение 1

Термины

	English Name	Description
A	ARP（Address Resolution Protocol）(протокол разрешения адресов)	Протокол, преобразующий IP-адрес в физический.
	Auto-Negotiation Автосогласование	Для автоматического согласования скорости работы и дуплексного режима на обоих концах коммутатора и другого оборудования.
B	Broadcast Storm Широковещательный шторм	По сети передается слишком много широковещательных кадров через один порт. Ответ на пересылку информации будет накапливаться в сети, потреблять чрезмерные сетевые ресурсы или вызывать сетевые тайм-ауты.
	Broadcasting Вещание	Передача данных на все узлы в сети.
C	CoS（Class of Service）(класс обслуживания)	Схема приоритета 802.1 p. CoS обеспечивает способ добавления метки приоритета к пакету и делит сообщение на восемь уровней. Диапазон значений: 0 ~ 7
D	DHCP（Dynamic Host Configuration Protocol）	IP-адрес, маска подсети, шлюз и другая информация
	DSCP（DiffServe Code Point）	В шестибитном домене, инкапсулированном в IP-заголовок, сообщение может быть разделено на 64 уровня. Диапазон значений: 0 ~ 63
E	Ethernet	Ethernet ИСПОЛЬЗУЕТ общую линейную или звездообразную топологию и поддерживает скорость передачи 10 Мбит / с. Новая версия, называемая Fast Ethernet, может достигать 100 Мбит / с.
F	Flow Control	Управление потоком позволяет низкоскоростному оборудованию обмениваться данными с высокоскоростными устройствами. Этот вид управления потоком позволяет приостанавливать пакет через высокоскоростной порт, чтобы обеспечить соответствие скорости высокоскоростного порта и скорости низкоскоростного. порт
	Frame	Пакет, содержащий информацию заголовка и хвоста, необходимую для физического уровня среды.
	Full-Duplex Полнодуплексный режим	Используя стандарт IEEE802.3 x, вы можете одновременно получать и отправлять данные в обоих направлениях одновременно
H	Half-Duplex Полудуплекс	Используя стандарт обратного давления, вы можете получать или отправлять данные только в одном направлении за раз.
I	IGMP（Internet Group Management	Обеспечивается механизм установления и поддержания связи между хостом и трехуровневым оборудованием многоадресной передачи.

	Protocol)	
	IEEE 802.1p	
	IEEE 802.1q	
Q	QoS (Quality of Service) Качество обслуживания	Метод, используемый для решения таких проблем, как задержка в сети и перегрузка.
T	Trunking	Т-транкинг Группа портов объединяется в агрегированную группу для увеличения пропускной способности и повышения надежности соединения.
	ToS (Type of Service)	In an 8-bit domain encapsulated in the IP header, a message representing different priority characteristics is represented
U	UDP (User Datagram Protocol)	UDP - это транспортный протокол передачи данных. Чтобы передать пакеты, ему не нужно заранее ничего устанавливать. Отправил пакеты, а что дальше с ними будет - без разницы. Ничего не контролирует, ничего не просит взамен, не гарантирует доставку пакета. Естественно, менее надежен, но поэтому более быстрый. Поэтому его используют для передачи больших данных, где допускаются "помехи". Например, фото, видео, аудио информация, клиент онлайн игры.
	UTP(Unshielded Twisted Pair)	Витая пара неэкранированная (без защиты

Приложение 2

FAQ

1. Почему отображение WEB страницы ненормально?
A: Перед доступом к WEB удалите кеш и файлы cookie IE. В противном случае это может вызвать неправильное отображение.
2. Забыли пароль?
A: Восстановите заводские настройки.
Нажимаем кнопку RESET на 10с. Начальное имя пользователя «admin» и пароль «system».
3. Работают ли оба способа настройки - через WEB браузер и через интерфейс командной строки?
A: Да, работают оба способа.
4. Почему не удается увеличить пропускную способность после настройки Trunking ?
A: Пожалуйста, проверьте, совпадает ли информация о порте транкинговой связи, включая скорость, дуплексный режим и VLAN и т. д.
5. Как решить проблему нерабочих портов коммутатора?
A: Когда некоторые порты на коммутаторе заблокированы, это может быть неисправность сетевого кабеля, неисправность сетевой карты или неисправность порта коммутатора, пользователи могут проверить, выполнив следующие действия:

Проверить отказ:

1. Соединение портов компьютера и коммутатора остается неизменным и заменять другие сетевые кабели.
2. Сетевой кабель и порт коммутатора остаются без изменений и поменять компьютер.
3. Сетевой кабель и компьютер остаются без изменений и заменять порты коммутатора.
4. Если выяснено, что это вызвано отказом порта коммутатора, обратитесь к поставщику для обслуживания.

6. В каком порядке происходит самоадаптивное определение статуса порта?
A: Тестирование состояния порта проводится в следующем порядке: 1000 Мбит / с дуплексный режим, 100 Мбит / с дуплекс, 100 Мбит / с полудуплекс, 10 Мбит / с дуплекс, 10 Мбит / с полудуплекс. И автоматически подключается с максимальной скоростью.