iRN-618-2P48

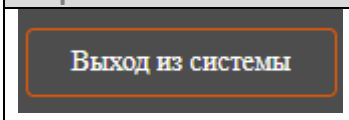
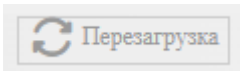
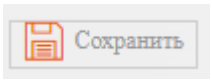
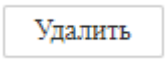
Управляемый промышленный коммутатор Ethernet

Руководство пользователя

Символы

Формат	Описание
 Уведомление	Неправильная эксплуатация может привести к потере данных.
 Внимание	Неправильная эксплуатация может привести к повреждению оборудования.
 Примечание	Пояснения к описанию операции
 Ключ	Ключевые советы по использованию оборудования
 Советы	Обратите внимание на информацию для успешной конфигурации оборудования

Обозначение кнопок

Формат	Описание
	На верхнем правом углу веб-страницы есть кнопка выхода. После её нажатия страница возвращается на страницу входа
	На верхнем правом углу веб-страницы есть кнопка перезагрузки. После её нажатия появится окно подтверждения перезагрузки. После подтверждения устройство будет перезагружено.
	На верхнем правом углу веб-страницы есть кнопка "Сохранить". Нажмите её, чтобы сохранить текущую конфигурацию устройства
	Нажмите кнопку "Добавить", чтобы добавить строку конфигурации. Обратите внимание, что повторная конфигурация может привести к перезаписи данных
	Выберите строку, которую нужно удалить, а затем нажмите кнопку "Удалить", чтобы деактивировать конфигурацию
	Выберите строку, которую нужно сконфигурировать, а затем нажмите кнопку "Конфигурация", чтобы перейти на страницу с выбором настроек
	Нажмите один раз что бы активировать конфигурацию Нажмите повторно что бы выключить конфигурацию 
	Нажмите кнопку "Применить", чтобы активировать текущую конфигурацию

Содержание

1. Вход в Web-панель

1.1 Выставление IP адреса на компьютере

По умолчанию на коммутаторе выставлен следующий адрес

IP Настройки	Адрес по умолчанию
IP Адрес	192.168.1.254
Маска подсети	255.255.255.0

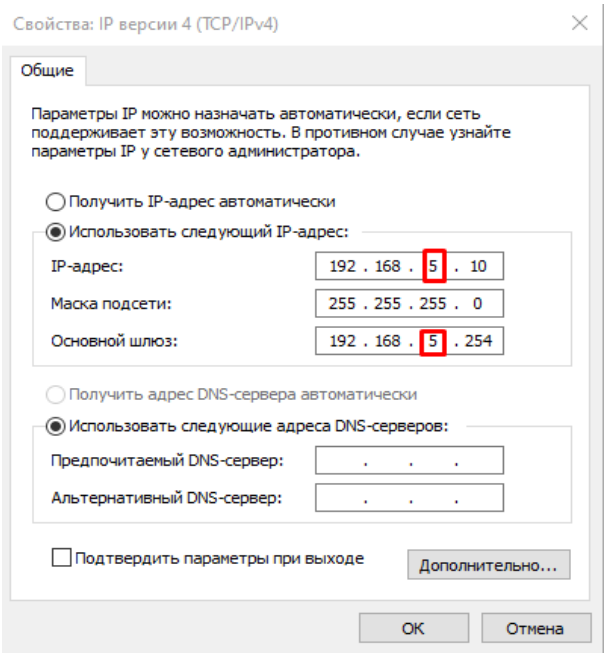
Перед конфигурацией коммутатора через Web-панель убедитесь:

- Что маршрут между компьютером и коммутатором доступен
- Что IP адрес компьютера находится в той же подсети, что и IP адрес коммутатора.

Примечание:
При первоначальной настройке коммутатора в локальном режиме убедитесь, что сегмент сети текущего компьютера равен 1.
Например: предположим, что IP-адрес текущего компьютера - 192.168.5.60, измените сегмент сети "5" на "1".

Шаги настройки компьютера

- Откройте Панель управления> Центр управления сетями и общим доступом> Изменение параметров адаптера, выберите ваш адаптер, нажмите правой кнопкой мыши на него и выберите свойства.
- Выберите пункт IP версии 4 (TCP/IPv4) и нажмите свойства.
- Далее в настройках поменяйте 5 на 1 или выставите IP адрес вручную (IP адрес не должен совпадать с IP адресом коммутатора)



- Нажмите ОК

1.2 Вход в Web-панель конфигурации

Шаги для входа в Web-панель конфигурации:

- Отройте браузер
- Введите в адресной строке «http://192.168.1.254»
- Нажмите Enter
- Появится страница для ввода логина и пароля

Примечание

Логин и пароль по умолчанию: admin

- Нажмите на кнопку «Вход в систему»

2. Системная информация

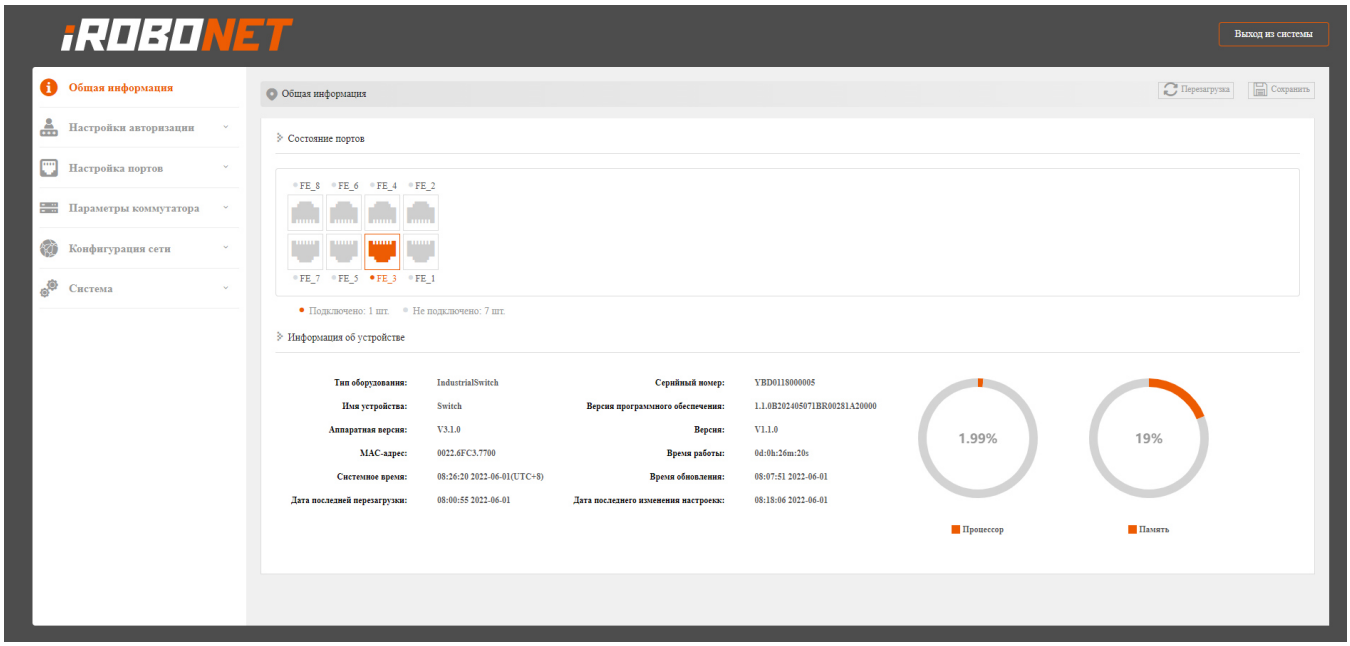
Описание функций:

Просмотр статуса портов, таких как тип порта и состояние подключения.

Проверка информации об устройстве, такой как модель продукта, версии программного и аппаратного обеспечения и т. д

Путь: Откройте на панели навигации: "Общая информация".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Статус порта	Отображение значка порта и статуса подключения порта устройства: Серый цвет обозначает что порт не активен  Оранжевый цвет означает что порт активен
Информация о девайсе	Базовая информация об устройстве • Тип оборудования • Имя устройства • Аппаратная версия • MAC-адрес • Системное время • Дата последней перезагрузки • Серийный номер • Версия программного обеспечения • Версия • Время работы • Время обновления • Дата последнего изменения настроек

3. Системная конфигурация

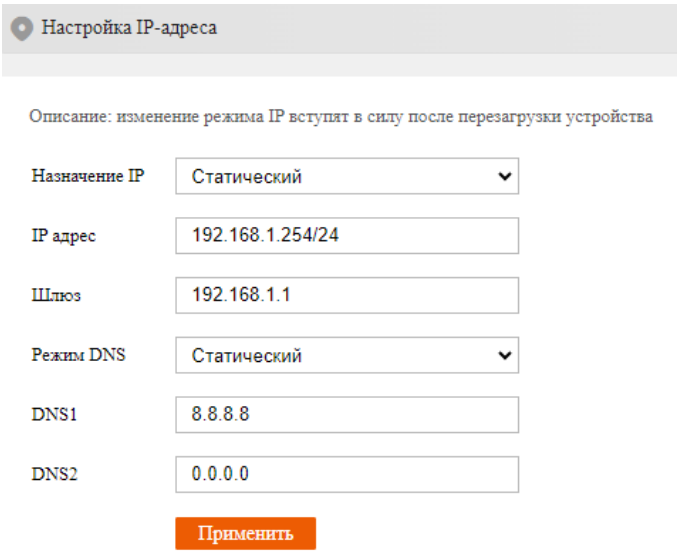
3.1 Конфигурация IP адреса

Описание функции:

Настройка статического или динамического IP-адреса.

Путь: Откройте панель навигации: "Настройка авторизации> IP-адрес".

Скриншот интерфейса конфигурации IP-адреса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Получение IP адреса	Установите режим получения IP-адреса: • Статический: IP-адрес системы настроен по умолчанию или вручную. • Динамический: система автоматически получает IP-адрес устройства. Примечание: IP-адрес, настроенный по умолчанию, - 192.168.1.254/24.
IP адрес	Отображается текущий IP адрес устройства
Шлюз	Отображается текущий шлюз устройства
Режим DNS	Установите режим получения DNS: • Статический: DNS адрес системы прописан по умолчанию или вручную. • Динамический: система автоматически получает DNS адрес устройства. Примечание: DNS1/DNS2 адрес, настроенный по умолчанию, 8.8.8.8/0.0.0.0.
DNS1	Отображается адрес DNS1
DNS2	Отображается адрес DNS2

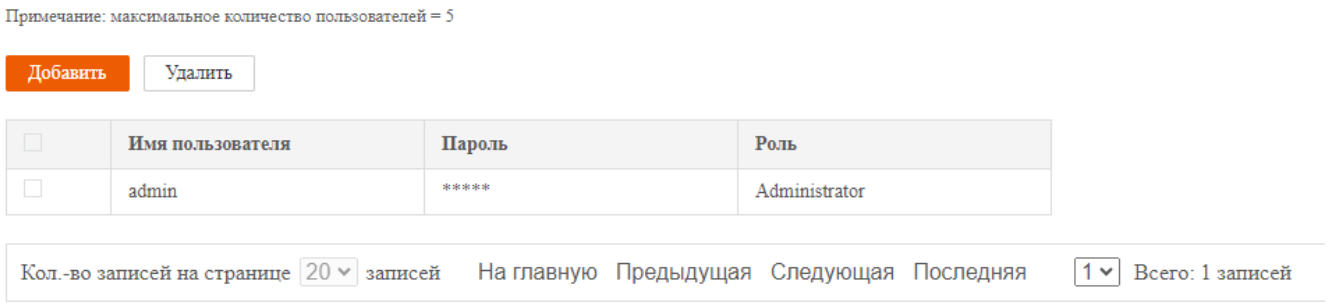
3.2 Конфигурация пользователя

Описание функции:

Добавление/удаление пользователей, получающих доступ к системе управления сетью.

Путь: Откройте панель навигации: "Настройка авторизации> Пользователи".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Пользователь	Имя пользователя для доступа к системе управления сетью. Примечание: • Имя пользователя - это комбинация букв, цифр и символов, не превышающая 20 байт. Пожалуйста, учитывайте регистр. • Поддерживается до 5 групп пользователей.
Пароль	Имя пользователя для доступа к системе управления сетью. Примечание: Пароль представляет собой комбинацию букв, цифр и символов, не превышающую 20 байт. Пожалуйста, учитывайте регистр.
Привилегии	• Observer: Информацию о конфигурации устройства можно просматривать, но конфигурация устройства не может быть изменена. • Administrator: Пользователь имеет все привилегии устройства, включая скачивание, загрузку, перезагрузку, изменение информации об устройстве и другие операции. Примечание: • Пользователи могут просматривать, удалять или добавлять других пользователей, приоритет которых не превышает их собственный. • Если добавленное имя пользователя уже существует, оригинальная информация о пользователе будет перезаписана.

Уведомление

Пожалуйста, запомните измененное имя пользователя и пароль для входа. Если вы забудете их, вы можете восстановить заводские настройки через DIP-переключатель. Имя пользователя и пароль по умолчанию для входа в веб-интерфейс конфигурации - "admin".

3.3 Авторизация через протокол

Описание функции:

Открывает протоколы безопасности доступа Telnet и SSH для удаленного сервисного входа.

Полное английское название SSH - Secure Shell. SSH - это протокол безопасности, основанный на прикладном и транспортном уровнях. SSH является надежным протоколом, обеспечивающим безопасность сеансов удаленного входа и других сетевых сервисов. Использование протокола SSH может эффективно предотвратить утечку информации в процессе удаленного управления, а также предотвратить подделку DNS и IP. Кроме того, передаваемые данные сжимаются, что позволяет увеличить скорость передачи. После включения функции SSH пользователи могут войти в интерфейс конфигурации командной строки для управления устройствами.

Telnet - это стандартный протокол и основной способ удаленного входа в Интернет. Он предоставляет пользователям возможность завершать работу с удаленным хостом на локальном компьютере. После включения функции TELNET пользователи могут войти в интерфейс конфигурации командной строки для управления устройством.

Путь: Откройте панель навигации: "Настройка авторизации> Протокол авторизации".

Скриншот интерфейса:

Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Telnet	После открытия, пользователи могут получить доступ к интерфейсу конфигурации командной строки через порт Ethernet.
SSH	После открытия пользователи могут получить доступ к интерфейсу конфигурации командной строки через консольный порт.

4. Настройка порта

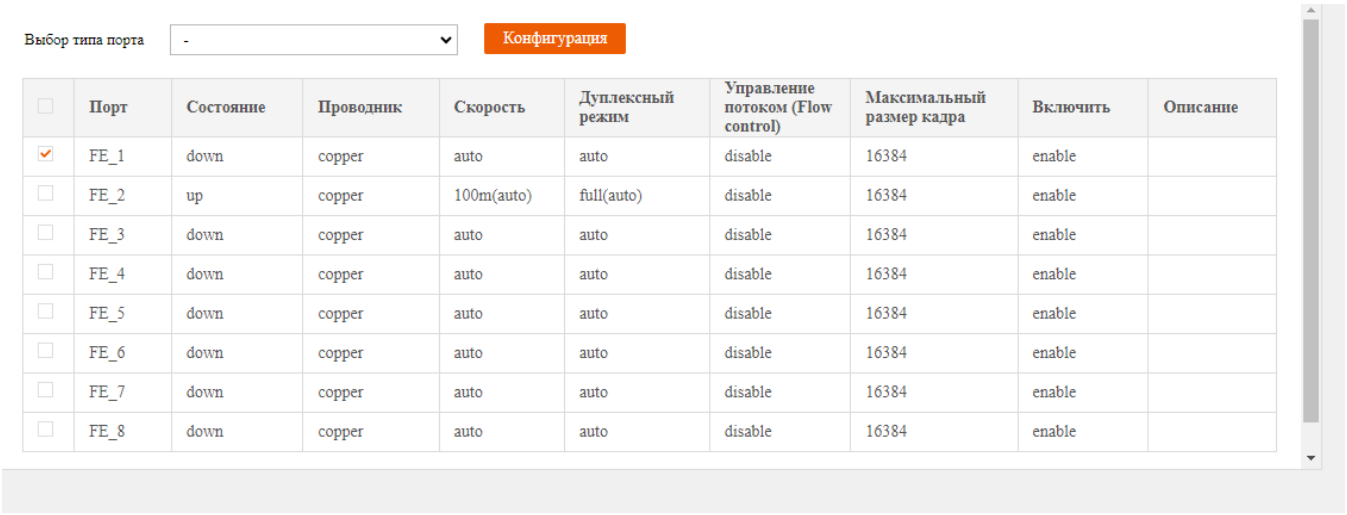
4.1 Настройка порта

Описание функции

Конфигурация параметров порта индивидуально или группой.

Путь: Откройте панель навигации: "Настройка портов> настройка порта".

Скриншот интерфейса:



Порт	Состояние	Проводник	Скорость	Дуплексный режим	Управление потоком (Flow control)	Максимальный размер кадра	Включить	Описание
FE_1	down	copper	auto	auto	disable	16384	enable	
FE_2	up	copper	100m(auto)	full(auto)	disable	16384	enable	
FE_3	down	copper	auto	auto	disable	16384	enable	
FE_4	down	copper	auto	auto	disable	16384	enable	
FE_5	down	copper	auto	auto	disable	16384	enable	
FE_6	down	copper	auto	auto	disable	16384	enable	
FE_7	down	copper	auto	auto	disable	16384	enable	
FE_8	down	copper	auto	auto	disable	16384	enable	

Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Порт	Отображение имени порта устройства
Состояние	Отображение состоянии порта • down: подключение отсутствует • up: подключение выполнено
Проводник	Подключение по типу BASE-TX
Скорость	Отображение скорости работы порта • auto • 10m • 100m
Дуплексный режим	Отображение дуплексного режима работы • auto • full-duplex • half-duplex
Управление потоком	Отображение режима контроля потоком • disable • enable
Макс. размер кадра	Отображение максимального размера передаваемого кадра
Включить	Включение порта Если порт будет выключен, вы не сможете к нему подключиться.
Описание	Поддерживается ввод описания порта длиной не более 40 символов.

4.2 Агрегация ссылок

Агрегация ссылок является важной технологией в сетевых коммуникациях, позволяющей объединить несколько физических портов в один логический канал. Это обеспечивает увеличение пропускной способности, повышение надежности и улучшение распределения нагрузки в сети.

Технология агрегации ссылок имеет следующие три преимущества:

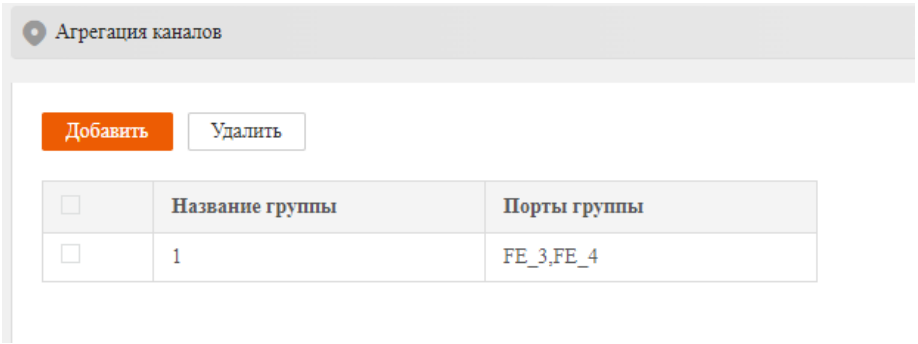
- Увеличение пропускной способности
  Максимальная пропускная способность интерфейса агрегации ссылок может достигать суммы пропускных способностей каждого из объединенных интерфейсов.
- Повышение надежности
  Когда активное соединение выходит из строя, трафик может быть переключен на другие доступные объединенные соединения, что улучшает надежность интерфейса агрегации ссылок.
- Распределение нагрузки
  В рамках группы агрегации ссылок распределение нагрузки может быть достигнуто на активных соединениях каждого объединенного интерфейса.

Описание функции

Связывание нескольких физических портов в один логический канал.

Путь: Откройте панель навигации: "Настройка портов> Агрегация каналов".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Название группы	Номер группы агрегации
Порты группы	Входящие в нее порты

Примечание

- Атрибуты всех объединенных портов в группе агрегации должны быть одинаковыми, включая тип среды, скорость и режим дуплекса и т.д.
- Настройка одного порта одновременно как порта кольцевой сети и порта агрегации не поддерживается.
- Один порт может быть включен только в одну группу агрегации.

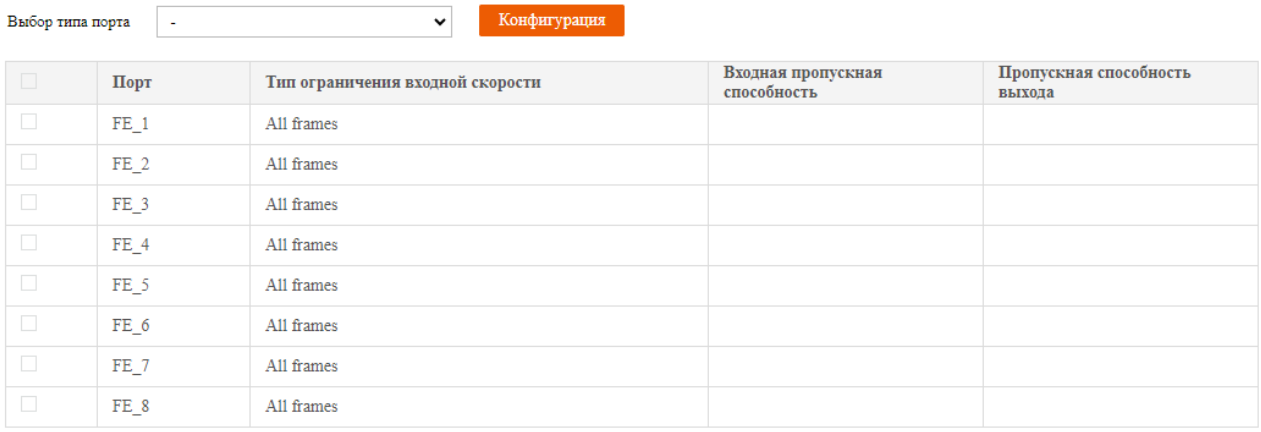
4.3 Ограничение скорости порта

Описание функции

Ограничение входящей и исходящей пропускной способности для широковещательных, многоадресных и одноадресных пакетов, принимаемых портом, как в одиночном порядке, так и группой.

Путь: Откройте панель навигации: "Настройка портов> Ограничение скорости порта".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Выбор типа порта	Выбор отдельного порта, либо всю группу
☐	Выбор отдельного порта
Порт	Номер порта устройства
Тип ограничения скорости	Ограничение пропускной способности всех кадров
Входная пропускная способность	Ограничение скорости входящих данных • 128/256/512Kbps • 1/2/4/8/16/64Mbps
Выходная пропускная способность	Ограничение скорости исходящих данных • 128/256/512Kbps • 1/2/4/8/16/64Mbps

Примечание

Ограничение скорости порта предъявляет высокие требования к качеству сетевого кабеля. Если качество кабеля не соответствует стандартам, может появиться множество конфликтных и поврежденных пакетов.

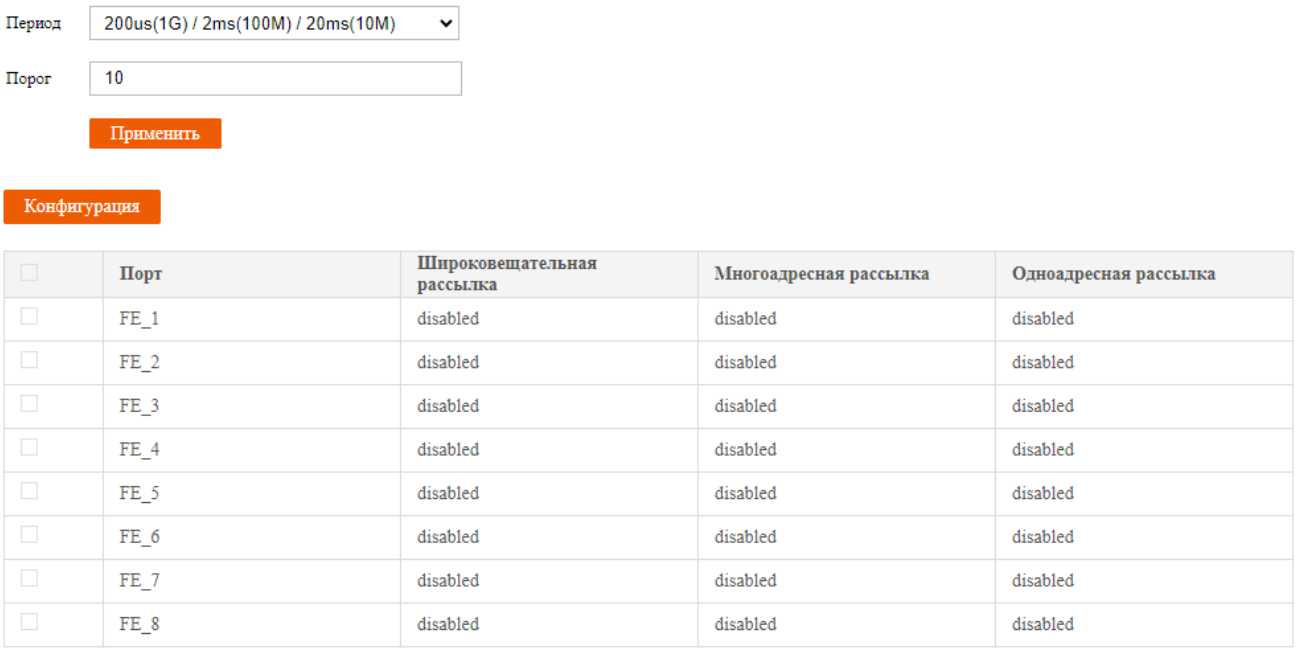
4.4 Подавление шторма

Описание функции

Ограничивает максимальный поток пакетов широковещательной рассылки, многоадресной передачи или неизвестного одноадресного назначения, который разрешен портом. Когда суммарный поток для каждого порта достигает значения, установленного пользователем, система отбрасывает пакеты, превышающие этот предел. Это помогает снизить долю общего потока до определенного диапазона, обеспечивая тем самым нормальную работу сетевых служб.

Путь: Откройте панель навигации: "Настройка портов> Повышение отказоустойчивости".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Период обнаружения	Период обнаружения для портов с различной пропускной способностью для широковещательных, неизвестных многоадресных или неизвестных одноадресных пакетов может быть выбран следующим образом: • 200us (1G) / 2ms (100M) / 20ms (10M) • 1ms (1G) / 10ms (100M) / 100ms (10M) • 10ms (1G) / 10ms (100M) / 10ms (10M) • 100ms (1G) / 100ms (100M) / 100ms (10M)
Порог обнаружения	Ограничение количества обнаруженных широковещательных, неизвестных многоадресных или неизвестных одноадресных пакетов за указанный период, с диапазоном значений от 1 до 255;

	при превышении порога подавления шторма превышенные сообщения будут отброшены.
Порт	Номер порта устройства
Широковещательная рассылка	Статус ограничения широковещательной рассылки • enable • disabled
Многоадресная рассылка	Статус ограничения многоадресной рассылки • enable • disabled
Одноадресная рассылка	Статус ограничения одноадресной рассылки • enable • disabled

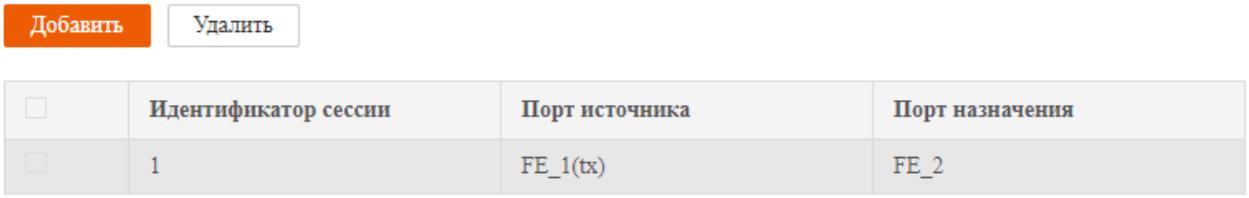
4.5 Зеркалирование портов

Описание функции

Копирование данных с исходного порта на назначенный порт для анализа и мониторинга.

Путь: Откройте панель навигации: "Настройка портов> Зеркалирование портов".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Идентификатор сессии	Номер идентификатора зеркалирования устройства, значение - 1. Примечание: Поддерживается только 1 сессия зеркалирования. Если зеркалирование настроено несколько раз, будут сохранены только данные последней конфигурации.
Порт источник	Порт с которого будет собираться информация. Может быть один или несколько портов
Порт назначения	Порт мониторинга для сбора информации с источника

Добавить	Щелкните "Добавить", чтобы перенастроить зеркалирование и настроить направление данных для зеркала. Опции направления данных следующие: • Отправка: сообщение, отправленное исходным портом, будет отражено на целевой порт • Получение: сообщение, полученное исходным портом, будет отражено на целевой порт • Двунаправленный: сообщения, получаемые и отправляемые исходным портом одновременно, отображаются на целевой порт

4.6 Статистика порта

4.6.1 Статистика порта – Обзор

Описание функции

Просмотр информации о данных на каждом порту:

- Количество отправленных и принятых сообщений и количество байт сообщений
- Количество отброшенных и сообщений с ошибками

Путь: Откройте панель навигации: "Настройка портов> Статистика портов> Статистика портов - Обзор".

Скриншот интерфейса:

4.6.2 Статистика порта – Порт

Описание функции

Просмотр статистики классификации общего количества отправленных и принятых сообщений, а также количества байт сообщений по заданному порту.

Путь: Откройте панель навигации: "Настройка портов> Статистика портов> Статистика портов - Порт".

Скриншот интерфейса:

	Направление входа	Направление выхода
Статистика (кол.-во)		
Количество пакетов	261	68
Количество байтов	46569	6058
Одноадресный номер	1	4
Номер многоадресной рассылки	225	45
Широковещательный номер	35	19
Кадр паузы	0	0
ошибки с вычисляемой суммой контроля кадра	0	0
Кадры < минимального размера	0	-
Flagments	0	-
Кадры > максимального размера	0	-
Jabber	0	-
Ошибки при приеме	0	-
Избыточные	-	0
Коллизии	-	0

5. Параметры коммутатора

5.1 VLAN конфигурация

VLAN (Virtual Local Area Network) - это технология коммуникации, которая логически делит физическую локальную сеть на несколько доменов широковещания. Хосты в VLAN могут напрямую общаться друг с другом, но два VLAN не могут напрямую обмениваться данными, что позволяет ограничить передачу широковещательных сообщений в VLAN. Использование VLAN предоставляет следующие преимущества для пользователей:

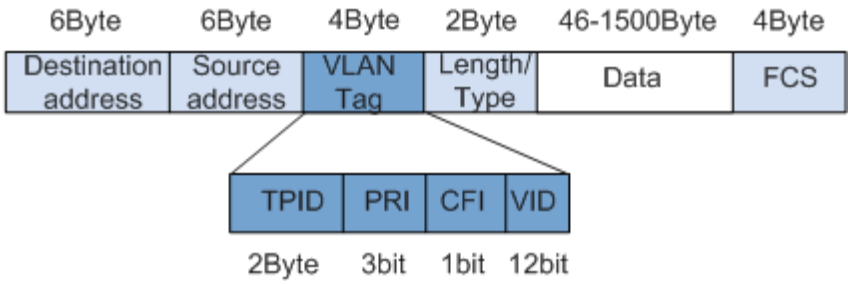
- Ограничение домена широковещания;
- Повышение безопасности локальной сети;
- Улучшение стабильности сети;
- Гибкое формирование виртуальных рабочих групп.

Порт VLAN

Порт VLAN использует различные идентификаторы для различия между разными VLAN. Использование одного и того же идентификатора приведет к замене внутренних групп членов, новый идентификатор установит новые правила пересылки, и все порты должны принадлежать одной или нескольким VLAN.

IEEE802.1Q VLAN

В соответствии с протоколом IEEE 802.1Q устройство может добавлять 4-байтовый тег VLAN (сокращенно тег) между полем исходного адреса и полями длины/типа кадра данных Ethernet, идентифицируя информацию VLAN.



- TPID (Tag Protocol Identifier) – Тег идентификатор протокола. Значение 0x8100 указывает на кадр данных VLAN стандарта IEEE 802.1Q.
- PRI (Priority) - Приоритет. Представляет приоритет кадра данных по стандарту 802.1p. Диапазон значений: 0-7, где большее значение соответствует более высокому приоритету. Во время сетевой перегрузки коммутатор будет предпочтительно передавать кадры данных с более высоким приоритетом.
- CFI (Canonical Format Indicator) - Индикатор канонического формата. Определяет, упакован ли MAC-адрес в стандартный формат для различных сред передачи. Значение 0 указывает на то, что MAC-адрес упакован в стандартный формат.
- VID (VLAN ID) - Идентификатор VLAN. Представляет номер VLAN кадра данных. Диапазон значений VLAN ID: 0-4095. Значения 0 и 4095 являются зарезервированными, поэтому допустимый диапазон VLAN ID составляет 1-4094.

5.1.1 Глобальная конфигурация

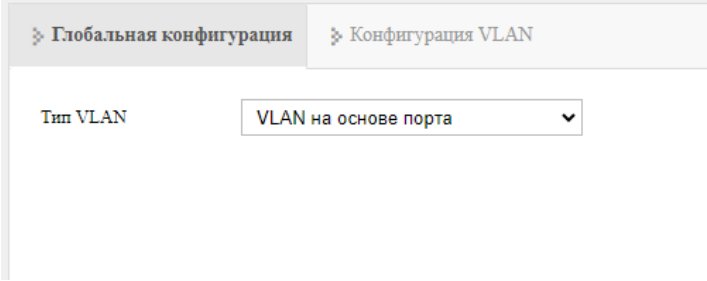
Описание функции

Глобальная конфигурация позволяет:

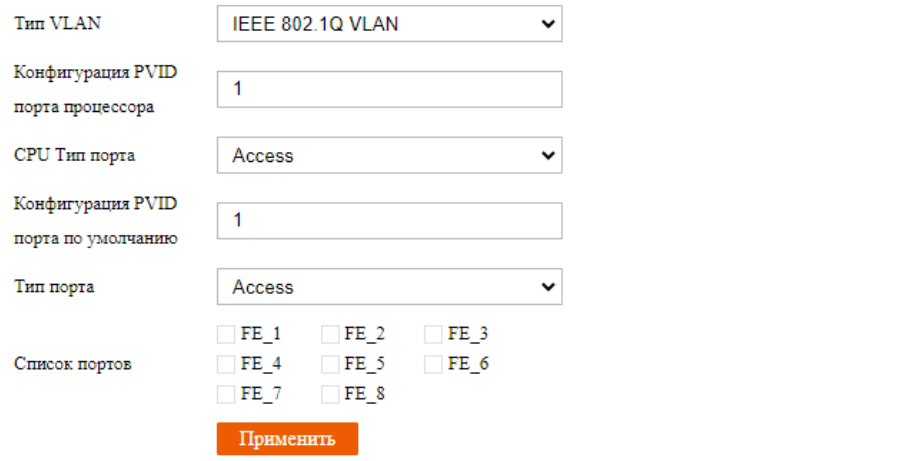
- Установить тип VLAN
- Установить PVID CUP
- Установить PVID порта по умолчанию
- Установить тип порта

Путь: Откройте панель навигации: "Параметры коммутатора> VLAN> Глобальная конфигурация".

Тип 1: VLAN на основе порта



Тип 2: IEEE 802.1Q VLAN



Порты группы	PVID	Тип участника
cpu	1	trunk
FE_1	1	access
FE_2	1	access
FE_3	1	access
FE_4	1	access
FE_5	1	access
FE_6	1	access

Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Тип VLAN	Переключение между двумя типами работы • VLAN на основе порта • IEEE 802.1Q VLAN
Конфигурация PVID порта процессора	По умолчанию конфигурация равна 1, а допустимый диапазон составляет от 1 до 4094
CPU Тип порта	Настроить тип связи порта можно двумя способами: • Доступ (Access): Сообщение, входящее в коммутатор с порта Access, принудительно использует PVID порта в качестве идентификатора VLAN. • Транк (Trunk): Сообщение, входящее в коммутатор с порта Trunk. Если в сообщении уже есть тег VLAN, используется идентификатор VLAN из тега VLAN сообщения; в противном случае используется PVID этого порта в качестве идентификатора VLAN.
Конфигурация PVID порта по умолчанию	Конфигурация по умолчанию равна 1, а допустимый диапазон значений составляет от 1 до 4094
Тип порта	Настройка типа соединения порта включает два типа • Access • Trunk
Список портов	Выбор необходимого порта для конфигурации

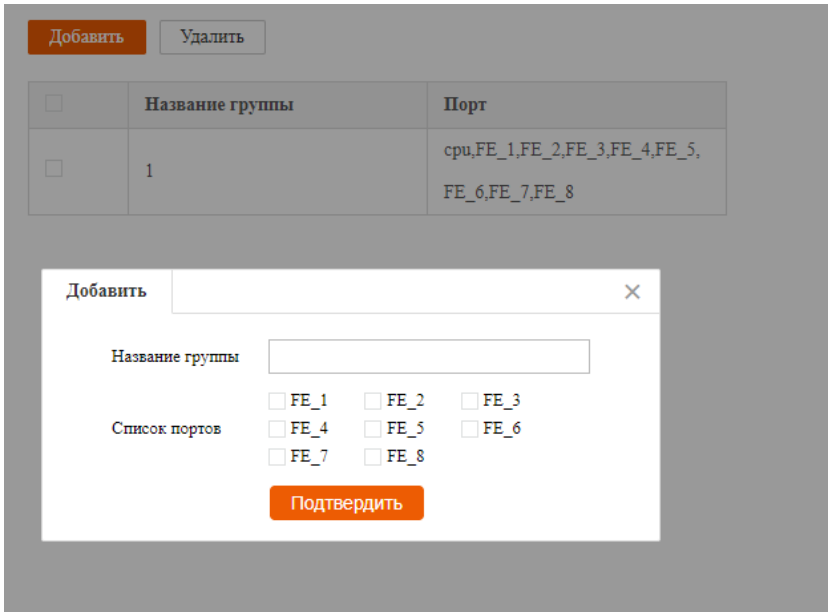
5.1.2 Конфигурация VLAN

Описание функции:

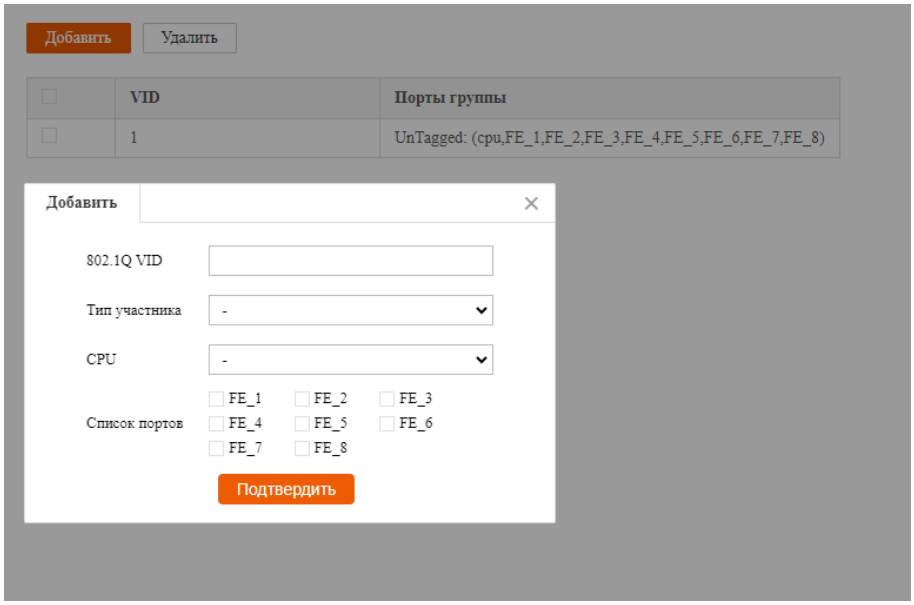
Добавление VLAN на основе порта или 802.1Q

Путь: Откройте панель навигации: "Параметры коммутатора> VLAN> Конфигурация VLAN".

Тип 1: VLAN на основе порта



Тип 2: IEEE 802.1Q VLAN



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
802.1Q VID	Введите идентификатор для добавления VLAN. Примечание: Если идентификатор VLAN уже существует, то после сохранения новая конфигурация идентификатора VLAN заменит существующую.
Тип участника	Существуют три типа "VLAN ID" для кадров данных, отправляемых из порта: • Неизменный (Unmodified): при отправке кадра данных из порта восстанавливается "VLAN ID", используемый для доступа к коммутатору. • Не помеченный (Untagged): удаляются поля "VLAN ID" при отправке кадра данных из порта. • Помеченный (Tagged): при отправке кадра данных из порта поля "VLAN ID" сохраняются.
CPU	Существуют три типа "VLAN ID" для кадров данных, отправляемых на CPU: • Неизменный (Unmodified): когда кадр данных отправляется на CPU, он восстанавливает "VLAN ID", используемый для доступа к коммутатору. • Не помеченный (Untagged): при отправке кадра данных на CPU удаляются поля "VLAN ID". • Помеченный (Tagged): при отправке кадра данных на CPU сохраняются поля "VLAN ID"
Список портов	Список портов доступных для добавления конфигурации

5.2 MAC конфигурация

MAC-адрес (Media Access Control) — это уникальный аппаратный идентификатор сетевого устройства. Коммутаторы используют эти адреса для эффективной маршрутизации сообщений в сети. Внутренняя уникальность MAC-адреса обеспечивает правильную доставку и повторную передачу сообщений.

5.2.1 Таблица MAC адресов

Каждый порт коммутатора оснащен функцией автоматического обучения адресов. Эта функция позволяет коммутатору хранить в адресной таблице информацию об отправителе (исходный MAC-адрес и номер порта коммутатора) для каждого кадра, который данный порт отправляет или получает. Время старения (Ageing Time) - это параметр, влияющий на процесс обучения коммутатора. Значение по умолчанию обычно составляет 300 секунд (5 минут). После добавления записи адреса в адресную таблицу начинается отсчет времени старения. Если в течение этого периода на порту не будет получено ни одного кадра, у которого исходный MAC-адрес совпадает с сохраненным в таблице, то такая запись будет удалена из таблицы динамической маршрутизации (таблица содержит исходный MAC-адрес, адрес назначения и соответствующий им номер порта коммутатора).

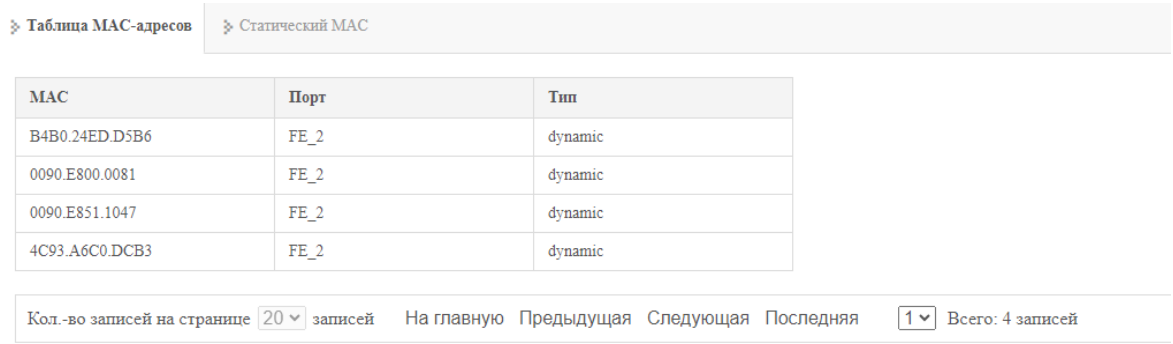
Описание функции

Просмотр MAC адресов, включая:

- MAC-адреса устройств в одной подсети.
- Вручную добавленный MAC адрес

Путь: Откройте панель навигации: "Параметры коммутатора> MAC> Таблица MAC адресов".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
MAC	Отображение MAC адресов обнаруженные устройством и добавленные вручную
Порт	Доступ к номеру порта источника данных соответствующего MAC-адреса
Тип	Тип MAC-адреса, отображается следующим образом: • dynamic: динамический MAC-адрес; • static: статический MAC-адрес.

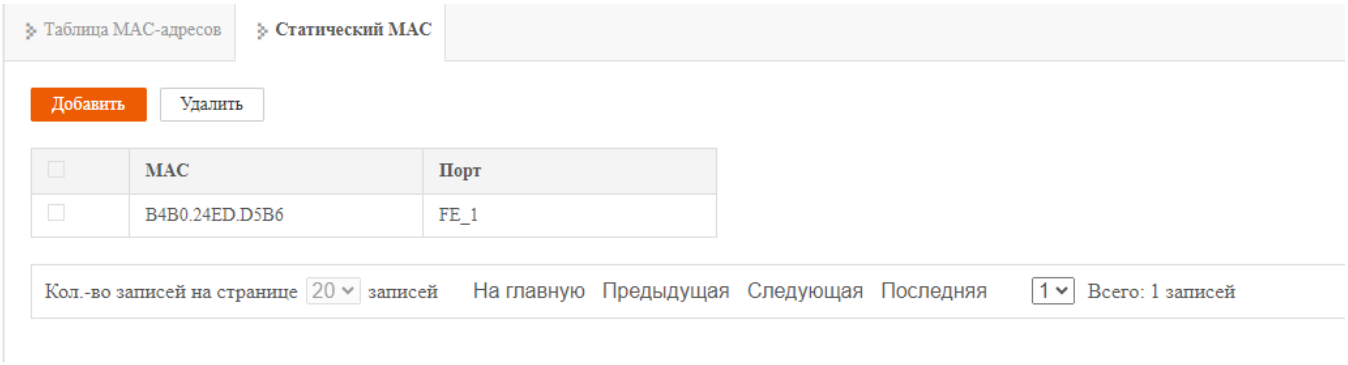
5.2.2 Статический MAC адрес

Описание функции

Поддержка ручной привязки одноадресных (unicast) MAC-адресов. Одноадресный адрес после привязки становится статическим MAC-адресом, который не устаревает.

Путь: Откройте панель навигации: "Параметры коммутатора> MAC> Статический MAC".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
MAC	Заполните одноадресный (unicast) MAC-адрес, который нужно привязать к интерфейсу, например, 0001.0001.0001.
Порт	Порт к которому привязан MAC адрес

Примечание

- Эта функция является своего рода механизмом безопасности. Пожалуйста, внимательно проверьте настройки, иначе часть устройств не сможет общаться друг с другом.
- Не используйте мультикаст-адрес в качестве входного адреса.
- Не вводите зарезервированный MAC-адрес, например, локальный MAC-адрес.

5.3 Spanning-tree конфигурация

Примечание

Нельзя одновременно включить протоколы Spanning Tree и Ring. Пожалуйста, отключите режим Ring, если он включен, перед настройкой протокола Spanning Tree.

Протокол Spanning Tree (STP) — это сетевой протокол второго уровня, который помогает устранить петли второго уровня в сети путем выборочной блокировки резервных сетевых каналов. При этом он обеспечивает резервирование каналов связи. Существует три основных типа протоколов Spanning Tree:

- STP (Spanning Tree Protocol) - базовый протокол Spanning Tree.
- RSTP (Rapid Spanning Tree Protocol) - усовершенствованный протокол Spanning Tree с более быстрой конвергенцией.

Протокол Spanning Tree выполняет две основные функции:

- Предотвращение петель: STP использует алгоритм построения дерева (spanning tree), чтобы создать топологию сети без петель. В этом дереве выбирается один порт коммутатора в качестве корневого, а остальные порты настраиваются таким образом, чтобы избежать образования петель.
- Быстрое восстановление сети: В случае изменения топологии сети (например, отключения кабеля) протокол Spanning Tree быстро перестраивает подлючение, чтобы восстановить нормальную работу сети.

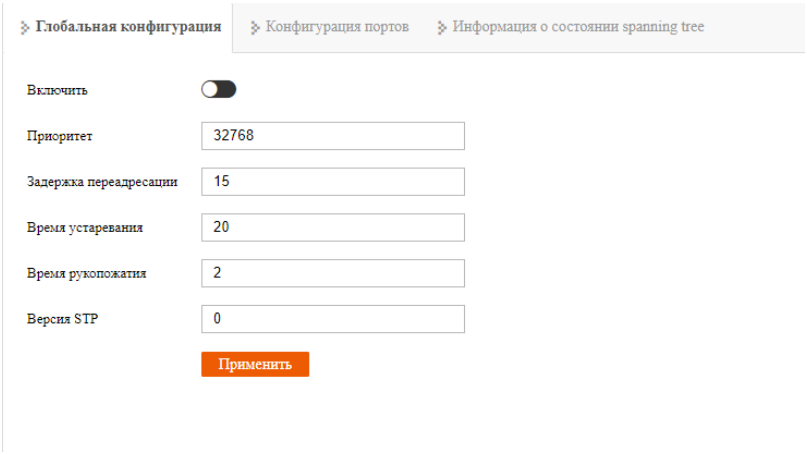
5.3.1 Глобальная конфигурация

Описание функции

На странице "Глобальная конфигурация" пользователь может настраивать параметры протокола STP.

Путь: Откройте панель навигации: "Параметры коммутатора> Spanning-tree> Глобальная конфигурация".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Включить	Включение протокола STP. По умолчанию он выключен
Приоритет	Уровень приоритета моста по умолчанию равен 32768, диапазон значений составляет от 0 до 61440. Примечание: Чем меньше значение уровня приоритета, тем выше уровень приоритета.
Задержка переадресации	При обнаружении изменения топологии порт первоначально переводится в состояние блокировки, чтобы предотвратить образование петель. По умолчанию выставлено 15 секунд. Диапазон от 4 до 30 секунд
Время устаревания	Оно по умолчанию равно 20 секундам, а допустимый диапазон значений - от 6 до 40 секунд. Этот параметр определяет, как долго коммутатор хранит полученное сообщение BPDU (Bridge Protocol Data Unit) от соседнего коммутатора, прежде чем считать его устаревшим.
Время рукопожатия	Интервал отправки сообщений - это параметр протокола Spanning Tree (STP), который определяет, как часто коммутатор отправляет сообщения другим коммутаторам в сети. Значение по умолчанию составляет 2 секунды, а допустимый диапазон - от 1 до 10 секунд.
Версия STP	STP версия. По умолчанию установлена версия 0. Диапазон от 0 до 1: • 0 – STP • 1 – RSTP

5.3.2 Конфигурация портов

Описание функции

На странице "Конфигурация портов" пользователи могут включить порты для участия в протоколе связующего дерева и настроить тип соединения, приоритет и другие атрибуты.

Путь: Откройте панель навигации: "Параметры коммутатора> Spanning-tree> Конфигурация портов".

Скриншот интерфейса:

Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Порт	Номер порта устройства
Включить	Включение протокола STP на данном порту
Пограничный порт	Позволяет управлять участием портов соседних коммутаторов в протоколе Доступны значения: • enable • disable
Тип соединения	Этот параметр позволяет выбрать тип соединения для порта коммутатора. Доступны значения: • auto • point-to-point • shared
Приоритет	Приоритет порта, допустимые значения: 0/16/32/48/64/80/96/112/128/144/160/176/192/208/224/240. Примечание: Уровень приоритета порта выше, когда значение меньше. Чем выше приоритет, тем вероятнее, что он будет корневым портом.
Стоимость конфигурации	Это параметр используется для определения наилучшего пути передачи данных в сети. Он указывает на общую стоимость (с точки зрения задержки или других факторов) достижения корневого моста от любого другого коммутатора в сети. Доступны значения: 1-200000000.

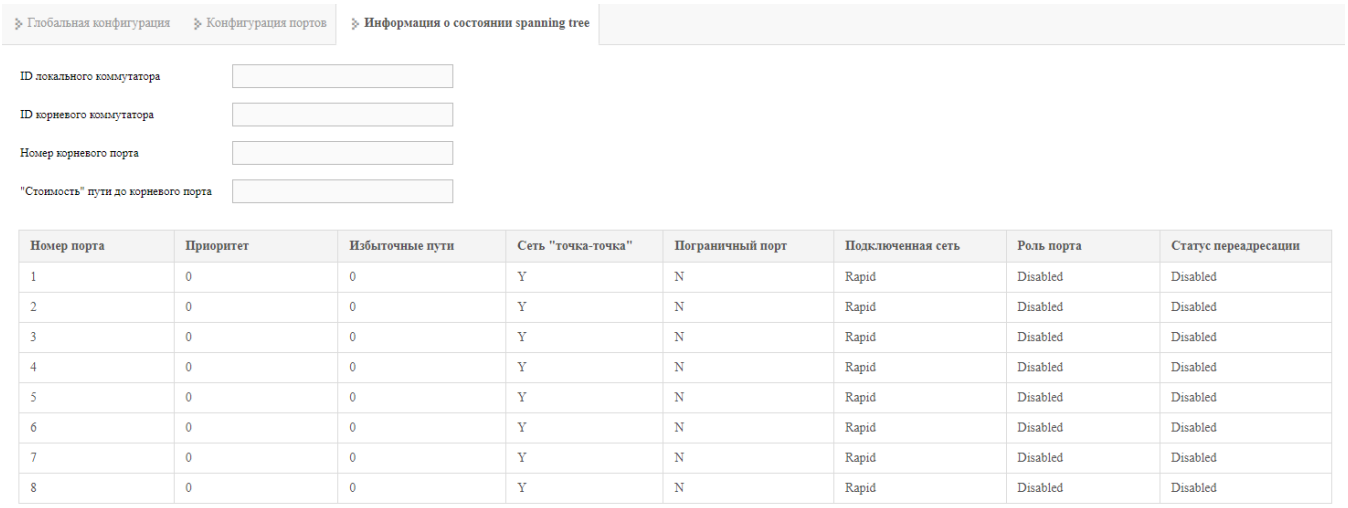
5.3.3 Информация о состоянии STP

Описание функции:

Отображение информации о Spanning Tree.

Путь: Откройте панель навигации: "Параметры коммутатора> Spanning-tree> Информация о состоянии spanning-tree".

Скриншот интерфейса:



Номер порта	Приоритет	Избыточные пути	Сеть "точка-точка"	Пограничный порт	Подключенная сеть	Роль порта	Статус переадресации
1	0	0	Y	N	Rapid	Disabled	Disabled
2	0	0	Y	N	Rapid	Disabled	Disabled
3	0	0	Y	N	Rapid	Disabled	Disabled
4	0	0	Y	N	Rapid	Disabled	Disabled
5	0	0	Y	N	Rapid	Disabled	Disabled
6	0	0	Y	N	Rapid	Disabled	Disabled
7	0	0	Y	N	Rapid	Disabled	Disabled
8	0	0	Y	N	Rapid	Disabled	Disabled

Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
ID локального коммутатора	Отображается приоритет этого коммутатора и информация об идентификаторе MAC-адреса
ID корневого коммутатора	Отображается приоритет корневого коммутатора и информация об идентификаторе MAC-адреса.
Номер корневого порта	Это порт на некорневом коммутаторе, который напрямую подключен к корневому мосту в сети Spanning Tree
"Стоимость" пути до корневого порта	Корневая стоимость некорневого моста отражает стоимость этого выбранного корневого порта
Номер порта	Отображение номера порта устройства
Приоритет	Приоритет порта может принимать значения от 0 (наивысший приоритет) до 240 (низший приоритет)
Избыточные пути	это дополнительный трафик, генерируемый протоколом в сети. Этот трафик необходим для работы STP и поддержания топологии без петель. Однако он также может потреблять часть ресурсов полосы пропускания
Сеть "точка-точка"	Канал прямого подключения к коммутатору
Пограничный порт	Порт, который напрямую подключен к конечному устройству, а не к другим коммутаторам.
Подключенная сеть	Отображается сетевой протокол устройств с подключенными портами
Роль порта	Корневой порт (Root port), указанный порт (Specified port), Альтернативный порт (Alternate port) и Резервный порт (Backup port)

Статус переадресации	Разделение происходит в зависимости от того, пересылает ли порт пользовательский трафик и изучает ли MAC-адреса. • Отбрасывание (Discarding): не пересылает пользовательский трафик и не изучает MAC-адреса; • Изучение (Learning): не пересылает пользовательский трафик, но изучает MAC-адреса; • Пересылка (Forwarding): пересылает пользовательский трафик и изучает MAC-адреса; • Прослушивание (Listening): не пересылает пользовательский трафик и не изучает MAC-адреса, но может получать и отправлять сообщения конфигурации; • Блокировка (Blocking): порт только получает и обрабатывает BPDU, не пересылает пользовательский трафик; • Отключено (Disabled): заблокировано или физически отключено.

5.4 Ring

Примечание

Нельзя одновременно включить протоколы Spanning Tree и Ring. Пожалуйста, отключите режим Spanning Tree, если он включен, перед настройкой протокола Ring.

Кольцевая сеть с протоколом SW-Ring - это тип технологии Ethernet-сети, разработанный для промышленных сетей управления, требующих высокой надежности и быстрого восстановления в случае сбоев связи. Она использует кольцевую топологию с резервными путями для передачи данных и применяет протокол SW-Ring для автоматического переключения и восстановления сети.

Ключевые характеристики:

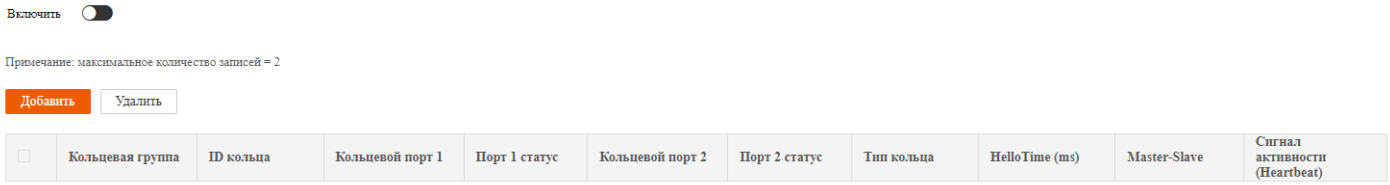
- Резервирование линий связи Ethernet: обеспечивает резервные пути для данных, гарантируя бесперебойную работу сети.
- Быстрое автоматическое восстановление: Сеть быстро восстанавливается после прерываний связи.
- Отсутствие главной станции: Децентрализованная конструкция исключает единую точку отказа.
- Поддержка многокольцевых сетей: до 250 коммутаторов могут быть объединены в самовосстанавливающуюся сеть с временем восстановления менее 20 миллисекунд.
- Гибкое использование портов: Любой порт на коммутаторе может быть использован как кольцевой порт для подключения.

Описание функции

Быстрая настройка конфигурации Ring.

Путь: Откройте панель навигации: "Параметры коммутатора> Ring".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

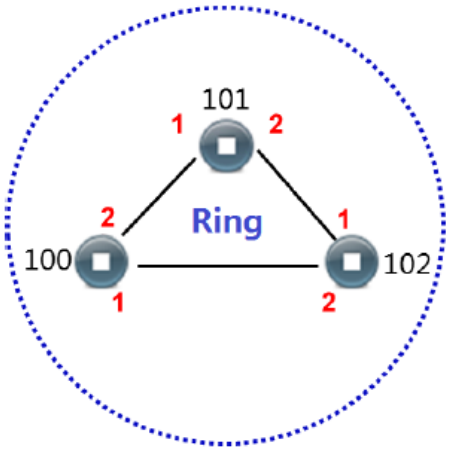
Элемент интерфейса	Описание
Включить	Включение функции Ring
Кольцевая группа	Поддержка протокола Ring 1 и 2 версии
ID кольца	Когда несколько коммутаторов формируют кольцо, текущий идентификатор кольца будет идентификатором сети. У разных кольцевых сетей разные идентификаторы. Диапазон значений составляет от 1 до 255. Примечание: Идентификация кольцевой сети должна оставаться одинаковой в одной кольцевой сети.
Кольцевой порт 1	В коммутаторе порт 1 может быть предназначен для участия в топологии кольцевой сети. Эта кольцевая сеть позволяет данным передаваться по замкнутому контуру через взаимосвязанные коммутаторы, повышая избыточность и надежность. когда тип кольцевой сети является "Couple" (также потенциально обозначаемым как "Coupled" или "Paired"), порт 1 принимает на себя специфическую роль, называемую "Сцепленный порт". Этот Сцепленный порт служит точкой соединения между различными сегментами сети или идентификаторами сети
Порт 1 статус	Состояние порта: • block • forward
Кольцевой порт 2	Порт номер 2 на коммутаторе используется для образования кольца. Примечание: • Когда тип кольцевой сети установлен в "Couple" (пара), порт 2 является "консольным портом". Консольный порт - это порт в цепочке, где пересекаются два кольца. • "Порт 1" и "Порт 2" не могут быть назначены на один и тот же порт. Номер порта, который вы устанавливаете, должен совпадать с фактически подключенным портом, без учета последовательности.
Порт 2 статус	Состояние порта:

	• block • forward
Тип кольца	Типы колец в соответствии с требованиями В зависимости от сценария использования, пользователь может выбрать различные типы колец. • Одиночное кольцо (Single): Представляет собой единое кольцо, которое соединяет все устройства последовательно. • Парное кольцо (Couple): Резервная структура, используемая для соединения двух независимых сетей. • Цепочка (Chain): Позволяет пользователям гибко строить различные топологии резервных сетей с помощью специального программного обеспечения. • Двойное кольцо (Dual): Два соседних кольца используют один коммутатор. Пользователи могут подключить один коммутатор к двум разным сетям или два разных коммутатора к одной сети.
HelloTime (ms)	Hello_time - это интервал отправки пакета Hello; через кольцевой порт ЦПУ отправляет информационный пакет смежному устройству для подтверждения, является ли соединение нормальным или нет. Диапазон ввода составляет от 0 до 100. Примечание: Когда значение Hello Time равно 0, это означает, что запросный пакет не отправляется.
Master-Slave	Сеть с одиночным кольцом поддерживает структуры без ведущей станции и с одной ведущей станцией и несколькими ведомыми. • Без ведущей станции: Все устройства в одиночном кольце являются ведомыми станциями. • С одной ведущей станцией: Одно устройство назначается ведущим, остальные - ведомыми. Один конец основного устройства кольца является резервным каналом. При сбое кольца резервный канал активируется с ведущей станции, обеспечивая нормальную работу сети.
Сигнал активности	Механизм обнаружения активности - это функция, повышающая надежность сети. При включении данной конфигурации сетевое объединение периодически отправляет сообщения активности для проверки того, находятся ли соответствующие устройства в активном состоянии. Настройки: • Включить (Enable). • Выключить (Disable).

Примечание

- Порт, который был настроен как порт Trank, не может быть установлен как порт быстрого кольца. Один порт не может принадлежать к нескольким кольцевым сетям.
- Идентификатор в одном и том же одиночном кольце должен быть одинаковым; в противном случае он не может сформировать кольцо и обеспечить нормальную связь.
- Для обеспечения связи кольцевой сети рекомендуется установить "Тип" портов, которые уже были настроены как кольцевая сеть, как Trank и "отношение участников" как "Отмеченный".
- При формировании сложных кольцевых сетей, таких как касательное кольцо, убедитесь, что идентификатор соответствует единству идентификатора одиночного кольца. Идентификатор сети разных одиночных колец должен быть разным.

5.4.1 Создание одиночного кольца



Кольцевые порты устройств 100, 101 и 102 — это порт 1 и порт 2. Следовательно, порты 1 и 2 устанавливаются как кольцевые порты каждого устройства.

Шаги настройки

Для настройки устройств 100, 101 и 102 выполните следующие действия:

- Включите переключатель "Включить".
- В текстовое поле "ID кольца" группы 1 введите значение "1".
- Выберите "Single" (Одиночное) в раскрывающемся списке "Тип кольца" группы 1.
- Установите для "Порта 1" значение "fe1", а для "Порта 2" - "fe2". Обратите внимание: "Порт 1" и "Порт 2" нельзя назначать одному и тому же физическому порту.
- В текстовое поле "HelloTime" группы 1 введите значение "0" (время приветствия).
- (Для устройств 100 и 101)
- Выберите "Slave" (Ведомый) в раскрывающемся списке "Master-slave" группы 1.
- (Для устройства 102)
- Выберите "Master" (Ведущий) в раскрывающемся списке "Master-slave" группы 1.
- Нажмите кнопку "OK"

5.5 Конфигурация IGMP Snooping

IGMP Snooping (Протокол контроля управления группами IPv4)

IGMP Snooping (Протокол контроля управления группами IPv4) - это сетевой протокол второго уровня для IPv4, предназначенный для многоадресной передачи данных. Он отслеживает (snooping) сообщения многоадресного протокола, передаваемые между маршрутизатором верхнего уровня и пользовательскими устройствами, для управления и контроля пересылки многоадресных пакетов на канальном уровне.

Принцип работы:

После настройки IGMP Snooping коммутатор второго уровня перехватывает и анализирует сообщения IGMP между многоадресными устройствами и маршрутизатором верхнего уровня. На основе этой информации он создает записи для пересылки многоадресного трафика на канальном уровне, что позволяет контролировать доставку данных. Таким образом, IGMP Snooping предотвращает широковещательную рассылку многоадресного трафика в сети второго уровня.

Обработка различных сообщений IGMP Snooping:

- Запрос универсальной группы IGMP: Это сообщение периодически рассылается всем устройствам и маршрутизаторам в локальном сетевом сегменте, чтобы узнать, какие участники многоадресной группы присутствуют в этом сегменте.
- Сообщение отчета IGMP: Устройство-участник, получив запрос универсальной группы IGMP, отвечает сообщением отчета IGMP. Участник активно отправляет сообщение отчета в ответ на запрос IGMP, чтобы сообщить о присоединении к многоадресной группе.
- Сообщение выхода IGMP: Устройство, использующее IGMPv2, отправляет сообщение выхода IGMP, чтобы уведомить службу запросов IGMP о том, что оно покинуло многоадресную группу

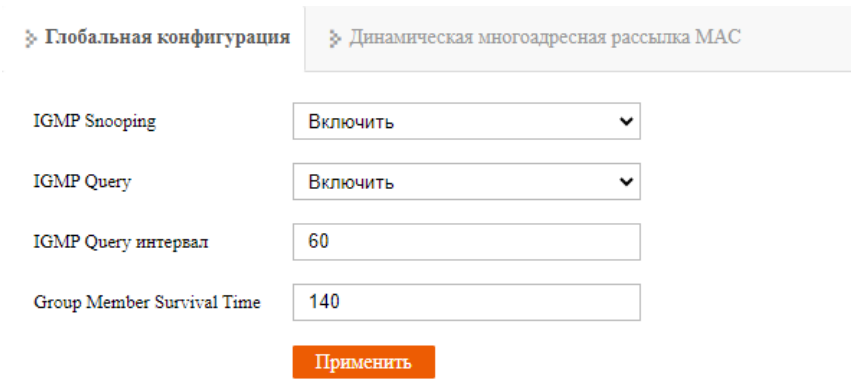
5.5.1 Создание одиночного кольца

Описание функции

Включение и выключение IGMP Snooping.

Путь: Откройте панель навигации: "Параметры коммутатора> IGMP-Snooping".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
IGMP Snooping	Функция IGMP Snooping: • Включить • Отключить Примечание: Функция IGMP Snooping подразумевает перехват сообщений между пользовательскими устройствами и маршрутизатором. На основании этой информации коммутатор отслеживает данные о многоадресных группах и портах, задействованных в их работе.
IGMP Query	Функция запроса IGMP: • Включить • Отключить Примечание: Запрос IGMP - это сообщение, которое маршрутизатор периодически отправляет всем устройствам в подсети, чтобы узнать, присоединились ли они к каким-либо многоадресным группам. Коммутатор, использующий IGMP Snooping, не отправляет запросы IGMP напрямую, а полагается на запросы, отправляемые маршрутизатором
IGMP Query интервал	Интервал запроса IGMP — это временной интервал, с которым маршрутизатор отправляет запросы IGMP всем устройствам в подсети. Допустимый диапазон значений: 60-300 секунд
Group Member Survival Time	Временем существования участника многоадресной группы: максимальный интервал, в течение которого коммутатор будет продолжать пересылать многоадресный трафик на порт, связанный с этой группой, после того, как участник группы перестанет отправлять отчеты IGMP. Примечание: • Функция IGMP Snooping должна быть включена на коммутаторе. • Допустимый диапазон значений: 120-300 секунд

Примечание

Вам нужно сначала установить источник и порт multicast в одной VLAN, чтобы включить функцию IGMP Snooping.

- Следует избегать наличия нескольких запросов IGMP в сети, чтобы не тратить ресурсы впустую. Пожалуйста, выберите все порты, если отношение пересылки неизвестной multicast-группы не определено.

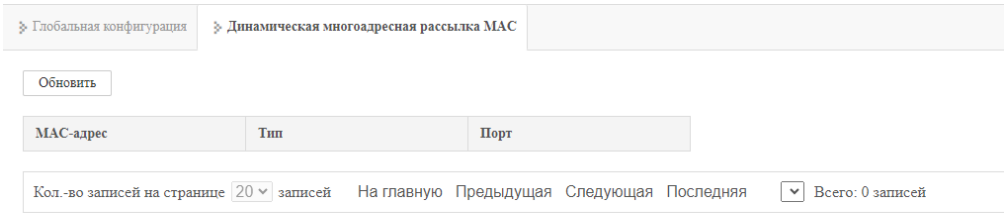
5.5.2 Динамическая многоадресная рассылка MAC

Описание функции

Отображает динамическую информацию multicast, полученную интерфейсом устройства.

Путь: Откройте панель навигации: "Параметры коммутатора> IGMP-Snooping> Динамическая многоадресная рассылка MAC".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
MAC-адрес	Multicast адрес, полученный интерфейсом
Тип	Multicast тип: • Динамический • Статический
Порт	Порт устройства

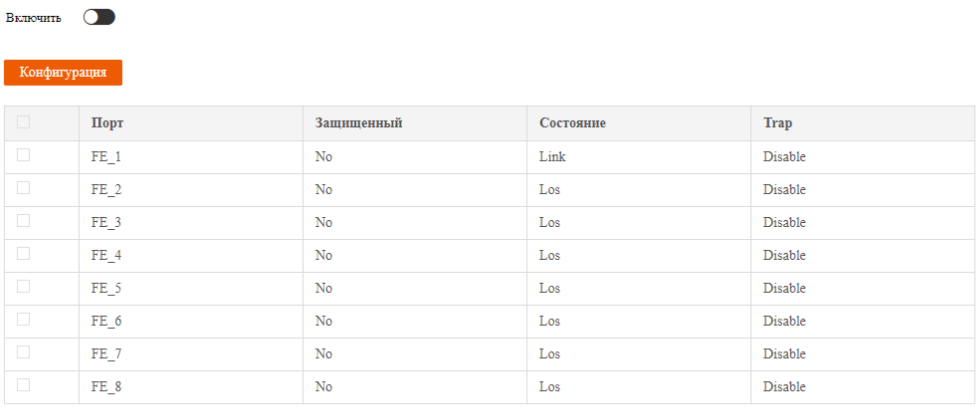
5.6 Обнаружение петель

Описание функции

Защита от петель может быть настроена для предотвращения шторма в кольцевой сети.

Путь: Откройте панель навигации: "Параметры коммутатора> Обнаружение петель".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Включить	Включение или выключение функции обнаружения петель
Порт	Порт устройства
Защищенный	Состояние порта, защищенного от петель. После включения, при обнаружении петли порта, петля может быть быстро разорвана, и статус порта может быть установлен в режим блокировки или пересылки для предотвращения сетевых штормов
Состояние	Состояние подключения этого порта, возможные значения: • Los: порт физически отключен • Link: порт не имеет петель и подключен • Block: функция защиты от петель включена, петля обнаружена, порт перешел в состояние защиты • Forward: порт подключен, защита от петель включена, петля не обнаружена
Trap	Переключатель Trap используется для отправки или блокировки информации Trap при обнаружении петли порта. Варианты: • Включить • Отключить

5.7 ERPS

Переключение защиты кольца Ethernet (ERPS) — это технология канального уровня сети Ethernet с высокой надежностью и стабильностью. ERPS — это протокол, определенный Сектором стандартизации электросвязи Международного союза электросвязи (ITU-T) для устранения петель на втором уровне. Поскольку номер стандарта — ITU-T G.8032/Y1344, ERPS также называют G.8032. ERPS определяет сообщения протокола Ring Auto Protection Switching (RAPS) и механизмы переключения защиты. Он может предотвратить штормы широковещательных рассылок, вызванные петлей данных, когда кольцо Ethernet целое. При отказе соединения кольца Ethernet имеет высокую скорость сходимости, что позволяет быстро восстановить путь связи между каждым узлом в кольцевой сети.

5.7.1 Конфигурация таймера

Описание функции

Настройка параметров таймера кольцевой сети ERPS после восстановления узлового устройства или соединения в кольце ERPS позволяет предотвратить колебания и помогает уменьшить время прерывания потока трафика. В протоколе ERPS основные используемые таймеры включают WTR (Wait to Restore) таймер, Guard таймер и Hold таймер.

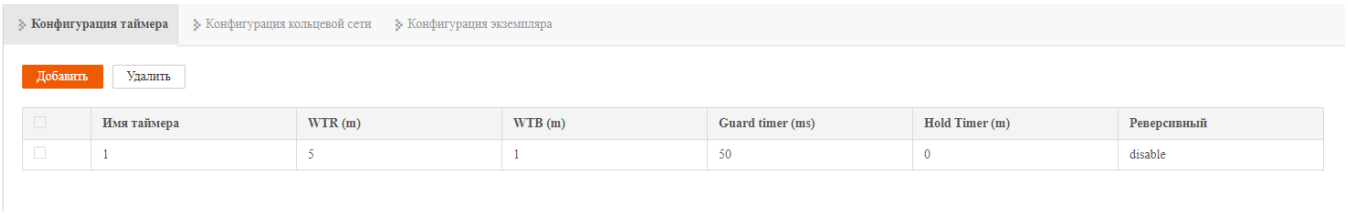
- WTR таймер
  Если порт владельца RPL разблокируется из-за неисправности соединения или узла, вовлеченный порт может не восстановиться сразу после восстановления соединения или узла. Блокировка порта владельца RPL может вызвать колебания сети. Чтобы предотвратить эту проблему, узел, на котором находится порт владельца RPL, запускает

таймер ожидания восстановления (WTR) после получения сообщения RAPS (NR). Таймер WTR будет отключен, если сообщения RAPS (SF) будут получены с других портов до истечения таймера. Если узел не получит никаких сообщений RAPS (SF) до истечения таймера, он блокирует порт владельца RPL по истечении таймера и отправляет сообщение NR-RB (RPL Block, RPL) RAPS. После получения этого сообщения RAPS (NR, RB) узлы устанавливают свои восстановленные порты в кольце в состояние Forwarding.

- Guard таймер
  Устройство, вовлеченное в сбой соединения или узла, отправляет сообщение NR (No Request) RAPS другим устройствам после восстановления сбоя или очистки операции, и одновременно запускает Guard таймер, и не обрабатывает сообщения NR RAPS до истечения таймера, чтобы предотвратить получение устаревшего сообщения NR RAPS. До истечения Guard таймера устройство не обрабатывает сообщения RAPS (NR) для предотвращения получения устаревших сообщений RAPS (NR). После истечения Guard таймера, если устройство всё еще получает сообщение RAPS (NR), локальный порт переходит в состояние Forwarding.
- Hold таймер
  В сетях второго уровня, работающих под управлением ERPS, могут быть разные требования к переключению защиты. Например, в сети, где предоставляются многоуровневые услуги, после сбоя сервера пользователям может потребоваться некоторое время для устранения неисправности сервера, чтобы клиенты не заметили сбой. Пользователи могут установить Hold таймер. Если происходит сбой, информация о сбое не отправляется сразу в ERPS до истечения таймера Hold, и если сбой не устранен, он отправляется после истечения таймера.

Путь: Откройте панель навигации: "Параметры коммутатора> ERPS> Конфигурация таймера".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Имя таймера	Имя таймера ERPS, поддерживающее от 1 до 32 символов и состоящее из заглавных букв, строчных букв, цифр или специальных символов (! @ _-).
WTR	WTR таймер, диапазон значений от 1 до 12 минут
Guard Timer	Guard таймер, его диапазон значений от 1 до 200мс
Hold Timer	Hold таймер, его диапазон значений от 0 до 100мс
Реверсивный	Статус обратимого режима ERPS, варианты следующие: • Включить: если восстанавливается отказавшее соединение, порт владельца RPL снова будет

	заблокирован после ожидания времени WTR. Заблокированные соединения переключаются обратно на RPL. • Отключить: если восстанавливается отказавшее соединение, таймер WTR не запускается, и исходное неисправное соединение остается заблокированным и будет переключено на RPL.

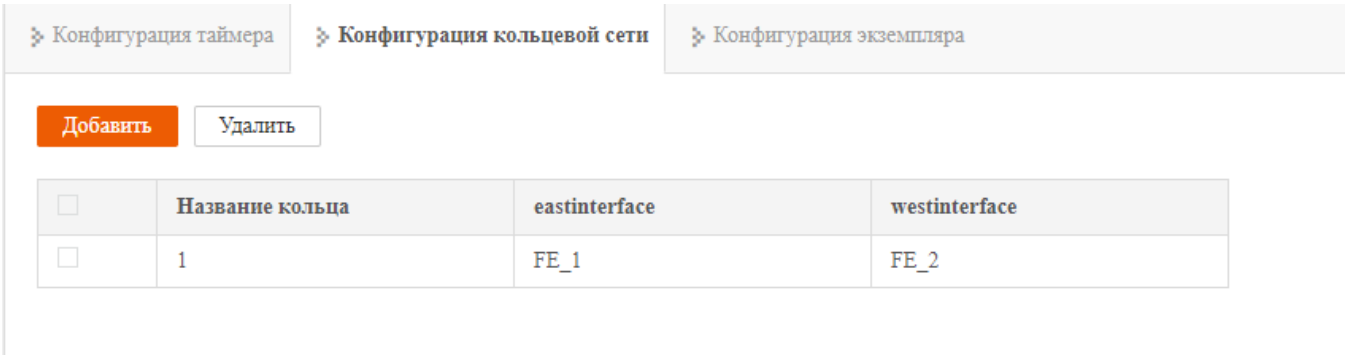
5.7.2 Конфигурация кольцевой сети

Описание функции

Конфигурация ERPS кольцевого порта.

Путь: Откройте панель навигации: "Параметры коммутатора> ERPS> Конфигурация кольцевой сети".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Название кольца	Название кольцевой сети ERPS, которое поддерживает от 1 до 32 символов, может состоять из заглавных букв, строчных букв, цифр или специальных символов (! @ _ -).
eastinterface	ERPS кольцевой порт
westinterface	ERPS кольцевой порт Примечание: • Порты кольцевой сети ERPS могут быть обычными физическими портами. • Порты кольцевой сети ERPS не могут быть включены в другие протоколы кольцевых сетей уровня 2 одновременно. • Порты кольцевой сети ERPS не могут быть одним и тем же портом. • Порты кольцевой сети ERPS должны быть trank-портами и разрешать проход тегированных кадров VLAN кольцевого экземпляра.

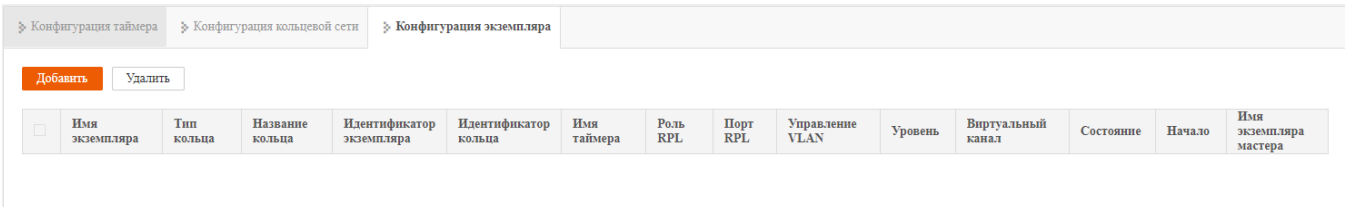
5.7.3 Конфигурация экземпляра

Описание функции

Настройка экземпляра кольцевой сети ERPS.

Путь: Откройте панель навигации: "Параметры коммутатора> ERPS> Конфигурация экземпляра".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Имя экземпляра	Название экземпляра кольцевой сети ERPS, которое может содержать от 1 до 32 символов, может состоять из заглавных букв, строчных букв, цифр или специальных символов (! @ _ -)
Тип кольца	Тип кольцевой сети экземпляра ERPS, варианты следующие: • Основное кольцо, замкнутое кольцо. • Дополнительное кольцо, незамкнутое кольцо, формирует многоуровневую сеть, такую как пересекающееся кольцо с основным кольцом.
Название кольца	Название кольцевой сети ERPS. Примечание: Название кольца должно быть создано заранее в разделе "Конфигурация кольцевой сети" ERPS, и порт кольцевой сети должен быть указан
Идентификатор экземпляра	Идентификатор защитного экземпляра ERPS, значение по умолчанию - 0.
Идентификатор кольца	Идентификатор кольцевой сети ERPS, его диапазон значений от 1 до 239. Идентификатор кольца используется для уникальной идентификации кольцевой сети ERPS, и все узлы в одной и той же кольцевой сети ERPS должны быть настроены с одним и тем же идентификатором кольца. Примечание: Идентификатор кольца ERPS будет последним байтом MAC-адреса назначения сообщения RAPS.
Имя таймера	Название таймера, которое поддерживает параметр таймера по умолчанию или настраивается при настройке таймера.
Роль RPL	Каждое устройство в кольцевой сети ERPS называется узлом. Роль узла определяется пользовательской конфигурацией и может быть следующего типа:

	• ВЛАДЕЛЕЦ-RPL (RPL-OWNER): Владелец узла отвечает за блокировку и разблокировку портов в RPL узла для предотвращения образования петель и выполнения переключения соединения. • СОСЕД-RPL (RPL-NEIGHBOR): Соседний узел подключен к Владельцу на RPL. Сотрудничая с Владельцем, он блокирует и разблокирует порты на RPL узла и выполняет переключение соединения. • ПЕРЕКРЕСТНОЕ СОЕДИНЕНИЕ (INTERCONNECTION): Перекрестное соединение представляет собой узел, который подключает несколько колец в множественной кольцевой модели. Он принадлежит вторичному кольцу, и в основном кольце нет перекрестных соединений. В режиме передачи пакетов протокола между двумя узлами перекрестного соединения вторичного кольца протокол вторичного кольца заканчивается в перекрестном узле, но пакет данных не завершается. • ДРУГОЕ (OTHER): Обычный узел представляет собой любой другой узел, помимо вышеперечисленных трех типов. Обычный узел отвечает за прием и пересылку протокольного пакета и пакета данных в соединении.
Порт RPL	Порт, подключенный по RPL-соединению, варианты следующие: • Западный интерфейс (West-interface) • Восточный интерфейс (East-interface)
Управление VLAN	Канал VLAN протокольного пакета, его диапазон значений от 1 до 4094
Уровень	Уровень кольцевой сети ERPS, диапазон значений от 0 до 7. Чем выше уровень кольцевой сети, тем больше значение. Когда сообщение R-APS должно быть передано по всему кольцу, оно может пересекать только кольца с высоким уровнем на низкий уровень.
Виртуальный канал	После включения виртуального канала, протокольный пакет вторичного кольца может передаваться по основному кольцу; в противном случае, протокольный пакет вторичного кольца может передаваться только в пределах кольца. Варианты: • ВИРТУАЛЬНЫЙ КАНАЛ: виртуальный канал активирован • НЕ ВИРТУАЛЬНЫЙ КАНАЛ: виртуальный канал не активирован
Состояние	Состояния экземпляра ERPS имеют следующие значения: • ERPS_INIT: начальное состояние, которое является состоянием инициализации при запуске протокола. • ERPS_IDLE: состояние ожидания, в которое он входит, когда топология кольца завершена.

	ERPS_FS: состояние принудительного переключения, в которое устройство входит при выполнении команды принудительного переключения. • ERPS_MS: состояние ручного переключения, в которое устройство входит при выполнении команды ручного переключения. • ERPS_PROTECTION: состояние защиты, в которое устройство входит при отказе соединения в кольце. • ERPS_PENDING: состояние ожидания, в которое устройство входит, когда соединение в кольце восстановлено после отказа.
Начало	Состояние запуска экземпляра ERPS: • start (запустить) • stop (остановить)
Имя экземпляра мастера	Имя основного экземпляра ERPS является именем экземпляра основного кольца, связанного с вторичным кольцом. Когда роль кольцевой сети – вторичное кольцо, а роль RPL - Перекрестное соединение, имя основного экземпляра может быть установлено только один раз и должно быть установлено как имя экземпляра ERPS.

6. Конфигурация сети

6.1 SNMP конфигурация

В настоящее время самым распространенным протоколом управления сетью является SNMP (Simple Network Management Protocol - простой протокол управления сетью). SNMP - это широко признанный и используемый промышленный стандарт, применяемый для обеспечения передачи управляющей информации между двумя точками в сети. Он удобен для сетевых администраторов, позволяя им искать информацию, изменять ее, обнаруживать неисправности, проводить диагностику, планировать емкость сети и создавать отчеты. SNMP использует механизм опроса и предоставляет только самые базовые библиотеки функций, что делает его особенно подходящим для использования в компактных, быстро развертываемых и экономичных средах. Реализация SNMP основана на протоколе UDP без установления соединения, поэтому он может устанавливать безусловные соединения со многими другими устройствами.

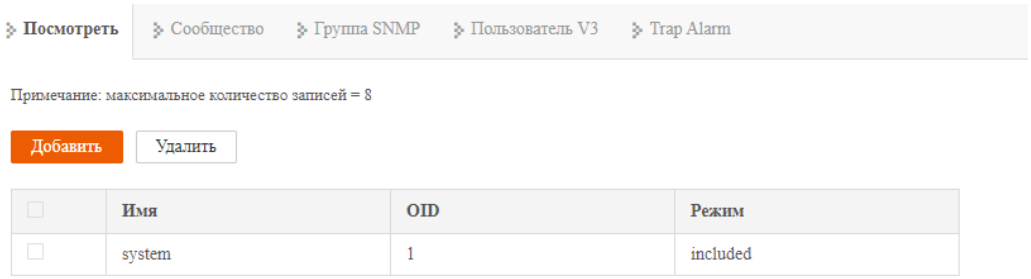
6.1.1 Просмотр

Описание функции

Добавление и удаление SNMP просмотра.

Путь: Откройте панель навигации: "Конфигурация сети> SNMP> Посмотреть".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Имя	Длина имени должна составлять от 1 до 32 символов. Имя может содержать только алфавитно-цифровые символы (a-z, A-Z и 0-9).
OID	Информация о расположении узла в дереве MIB, где находится устройство. Примечание: • Идентификатор объекта OID, компонентный узел MIB, уникально идентифицируется строкой чисел, представляющих путь. • Информацию об OID можно просмотреть с помощью стороннего программного обеспечения MG-SOFT MIB Browser.
Режим	Метод обработки узла OID, варианты следующие: • Included: содержит все объекты под поддеревом узла; • Excluded: исключает все объекты за пределами поддерева узла.

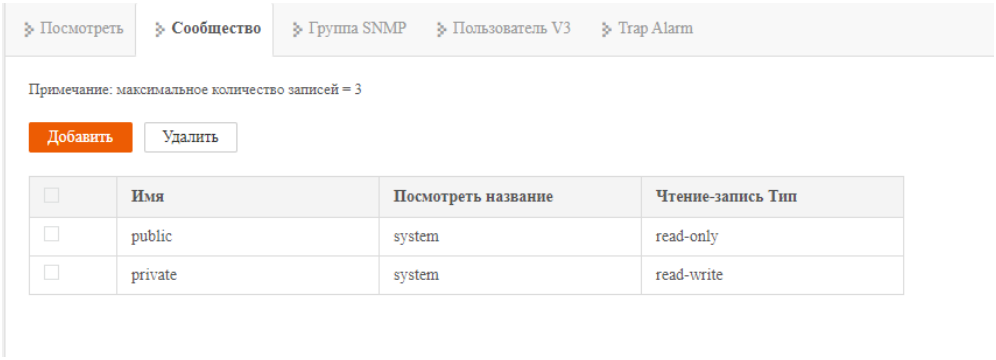
6.1.2 Сообщество

Описание функции

Добавление SNMP-сообществ, определение представления MIB, к которому данное сообщество может получить доступ, установить права доступа к объектам MIB для сообщества (чтение или запись).

Путь: Откройте панель навигации: "Конфигурация сети> SNMP> Сообщество".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Имя	Имя группы, включающее цифры или буквы, длиной не более 32 символов.
Посмотреть название	Определение имени представления SNMP, которое было настроено на странице Представления (View)
Чтение-запись Тип	Выбор имени представления с правами чтения-записи, варианты: • Только чтение (Read-only) • Чтение-запись (Read-write)

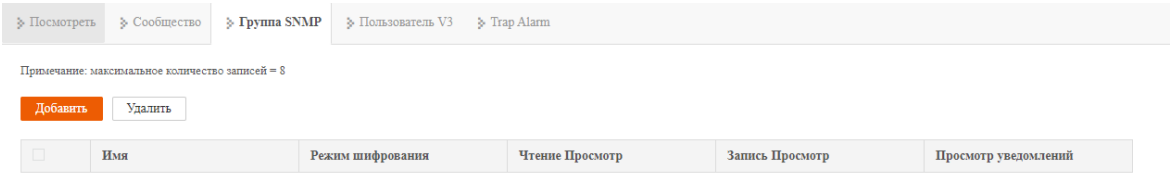
6.1.3 Группа SNMP

Описание функции

Настройка новой группы SNMP и установка режима безопасности и соответствующее представление SNMP для этой группы SNMP.

Путь: Откройте панель навигации: "Конфигурация сети> SNMP> Группа SNMP".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Имя	Имя группы SNMP, длина от 1 до 32 байт
Режим шифрования	Будет ли сообщение аутентифицироваться и шифроваться, варианты: • noauth: сообщение не аутентифицируется и не шифруется • auth: сообщение аутентифицируется, но не шифруется • priv: сообщение аутентифицируется и шифруется
Чтение просмотр	Укажите представление для чтения группы. Примечание: Представление должно быть настроено в интерфейсе представлений (View).
Запись просмотр	Укажите представление для записи и чтения группы. Примечание: Представление может совпадать или не совпадать. Для настройки представления необходимо его настроить через интерфейс представлений (View)
Просмотр уведомлений	Укажите представление для уведомлений группы. Примечание: Представление может совпадать или не совпадать. Для настройки представления необходимо использовать представление, настроенное через интерфейс представлений (View)

6.1.4 Пользователь V3

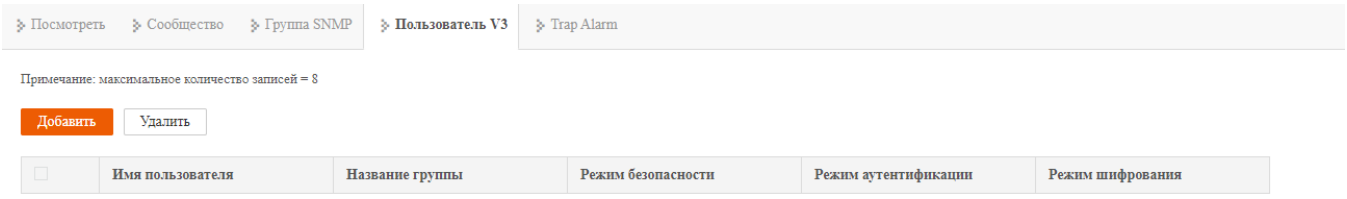
Описание функции

SNMPv3 использует модель безопасности на основе пользователей (User-Based Security Model, USM) для аутентификации.

Сетевой менеджер может настроить функции аутентификации и шифрования. Аутентификация используется для проверки подлинности отправителя пакета и предотвращения доступа неавторизованных пользователей. Шифрование шифрует передаваемый пакет между системой управления сетью (Network Management System, NMS) и агентом для предотвращения подслушивания. Использование функций аутентификации и шифрования обеспечивает более высокий уровень безопасности при коммуникации между NMS и агентом.

Путь: Откройте панель навигации: "Конфигурация сети> SNMP> Пользователь V3".

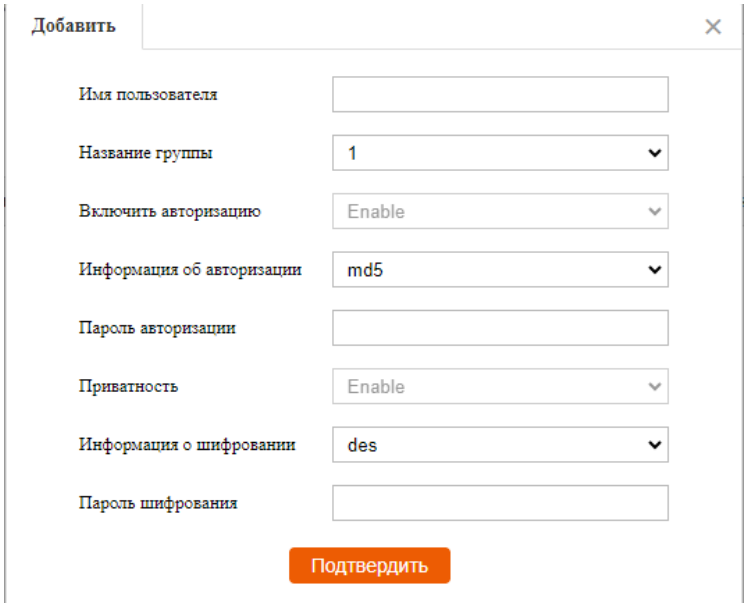
Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Имя пользователя	Определение имени пользователя SNMP v3, которое может содержать только цифры, буквы или символы @_!, длиной не более 32 символов
Название группы	Имя группы, длиной от 1 до 32 байт. Примечание: Имя группы должно быть создано в группе SNMP, и только созданная группа может создать пользователей SNMP v3
Режим безопасности	Будет ли аутентифицироваться и шифроваться сообщение, значения: • auth: указывает, что сообщение аутентифицировано, но не зашифровано; • noauth: указывает, что сообщение не аутентифицировано и не зашифровано; • priv: указывает, что сообщение аутентифицировано и зашифровано.
Режим аутентификации	Тип аутентификации, принимаемые значения: • MD5: Алгоритм абстрактного хеширования 5; • SHA: Алгоритм безопасного хеширования.
Режим шифрования	Алгоритм шифрования данных пользователя SNMP v3, варианты следующие: • DES: принять алгоритм шифрования данных; • AES: принять стандарт шифрования.

Добавление пользователя



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Имя пользователя	Определение имени пользователя SNMP v3, которое может содержать только цифры, буквы или символы @_!, длиной не более 32 символов
Название группы	Список групп SNMP
Включить авторизацию	Укажите, что режим безопасности требует аутентификации. Если выбрано "disable", то по умолчанию будет установлен режим без аутентификации и без шифрования.
Информация об авторизации	Тип информации для аутентификации, допустимые значения: • Md5: Алгоритм абстрактного хеширования 5; • Sha: Безопасный хеш-алгоритм.
Пароль авторизации	Пароль аутентификации — строка символов, длина которой больше или равна 8 байтам
Приватность	Укажите, что режим безопасности требует шифрования
Информация о шифровании	Алгоритм шифрования данных пользователя SNMP v3, варианты следующие: • DES: принять алгоритм шифрования данных; • AES: принять стандарт шифрования.
Пароль шифрования	Зашифрованный пароль — строка символов, длина которой больше или равна 8 байтам.

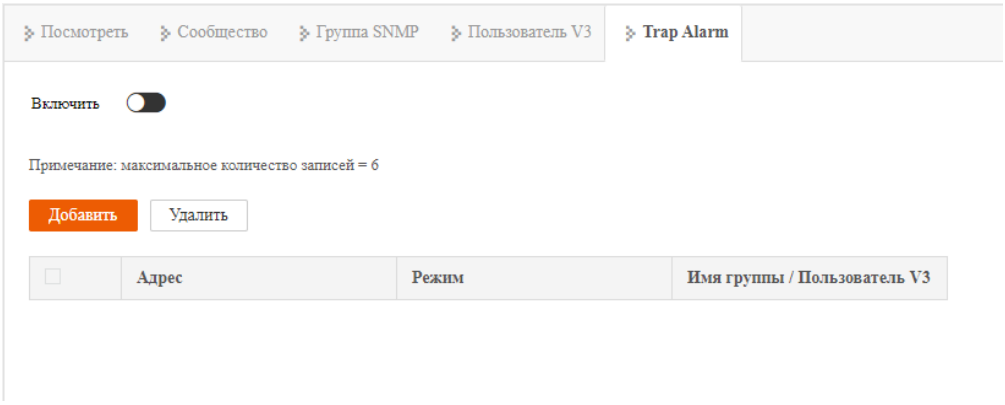
6.1.5 Trap Alarm

Описание функции

На основе протокола TCP/IP, SNMP обычно использует UDP порты 161 (SNMP) и 162 (SNMP-traps). Агент протокола SNMP существует в сетевом устройстве и использует информацию, специфичную для устройства (MIBs), в качестве интерфейса устройства; эти сетевые устройства могут быть мониториться или управляться через агента. Когда происходит событие trap, сообщение передается через SNMP Trap. В этом случае доступный получатель trap может получить сообщение trap.

Путь: Откройте панель навигации: "Конфигурация сети> SNMP> Trap Alarm".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Адрес	IP-адрес устройства управления SNMP, используемого для получения информации об аварийных ситуациях, например, ПК
Режим	Управляемое устройство, которое отправляет активное оповещение в NMS. После отправки аварийного сообщения inform устройство будет ждать подтверждающее сообщение от NMS. Если подтверждающее сообщение не будет получено, оно повторно отправит сообщение inform; сообщение Trap не имеет процесса подтверждения. Типы аварийных сообщений включают: • trapV1: отправить trap snmpV1 • trapV2c: отправить trap snmpV2c • trapV3: отправить trap snmpV3 • informV2c: отправить inform snmpV2c • informV3: отправить inform snmpV3
Имя группы/ Пользователь V3	Имя сообщества или имя пользователя snmpv3.

6.2 LLDP конфигурация

LLDP (Link Layer Discovery Protocol) — это протокол обнаружения топологии второго уровня. Его основной принцип заключается в следующем: устройства в сети отправляют сообщения с информацией о состоянии на соседние устройства, и каждый порт устройства хранит свою собственную информацию. Если статус локального устройства изменяется, оно может отправить обновленную информацию на непосредственно подключенное соседнее устройство. Соседние устройства будут хранить информацию в стандартном банке MIB SNMP. Система управления сетью может запрашивать состояние соединения текущего второго уровня из банка MIB SNMP. Следует отметить, что LLDP является протоколом только для обнаружения информации о состоянии удаленного устройства и не может выполнять конфигурацию сетевого устройства, управление портами и другие функции.

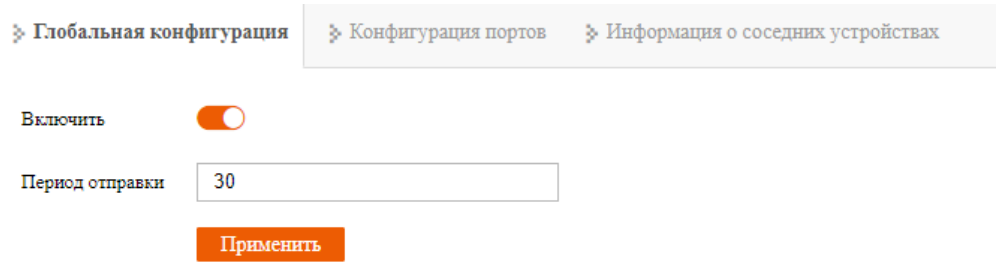
6.2.1 Глобальная конфигурация

Описание функции

Включение и настройка LLDP

Путь: Откройте панель навигации: "Конфигурация сети> LLDP> Глобальная конфигурация".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Включить	Включение функции LLDP
Период отправки	Период передачи LLDP, диапазон 5-300, единица измерения: секунда, по умолчанию: 30. Примечание: Когда статус устройства не меняется, устройство периодически отправляет LLDP пакеты на свои соседние узлы. Этот интервал называется периодом отправки LLDP пакетов.
Применить	Нажмите «Применить» для сохранения

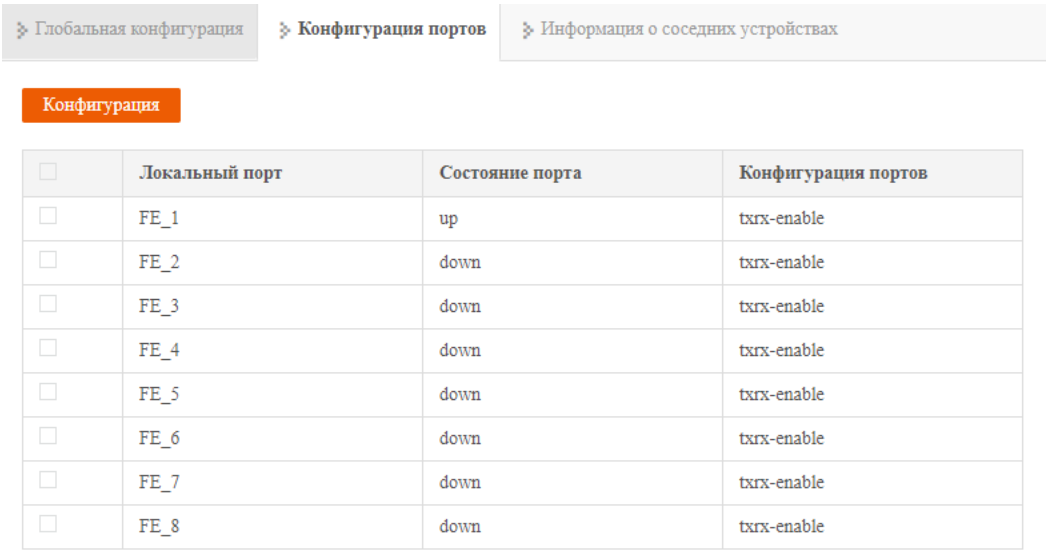
6.2.2 Конфигурация портов

Описание функции

Конфигурация работы LLDP на каждом порту

Путь: Откройте панель навигации: "Конфигурация сети> LLDP> Конфигурация портов".

Скриншот интерфейса:



	Локальный порт	Состояние порта	Конфигурация портов
	FE_1	up	txrx-enable
	FE_2	down	txrx-enable
	FE_3	down	txrx-enable
	FE_4	down	txrx-enable
	FE_5	down	txrx-enable
	FE_6	down	txrx-enable
	FE_7	down	txrx-enable
	FE_8	down	txrx-enable

Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Локальный порт	Порт устройства
Состояние порта	Состояние порта: • UP • down
Конфигурация портов	Опции режимов работы LLDP для порта устройства следующие: • tx-enable: режим работы Tx, только отправка и не прием LLDP сообщений. • rx-enable: режим работы Rx, только прием и не отправка LLDP сообщений. • txrx-enable: режим работы TxRx, как отправка, так и прием LLDP сообщений. • disable: режим работы Disable, ни прием, ни отправка LLDP сообщений. Примечание: Когда глобальный LLDP включен, по умолчанию режим работы LLDP - TxRx.

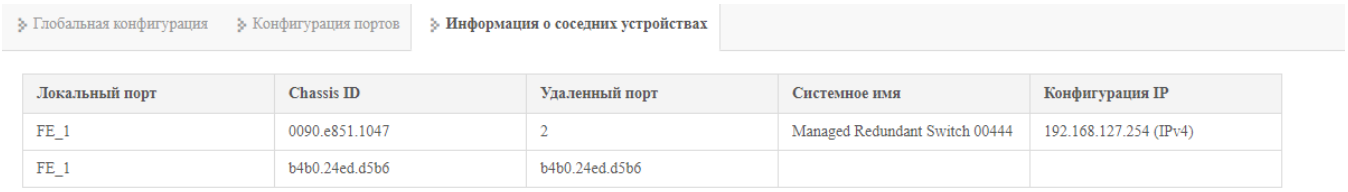
6.2.3 Информация о соседних устройствах

Описание функции

Просмотр информации о соседних устройствах

Путь: Откройте панель навигации: "Конфигурация сети> LLDP> Информация о соседних устройствах".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Локальный порт	Локальный порт к которому подключено устройство
Chassis ID	MAC-адрес моста соседнего устройства или порта.
Удаленный порт	Номер порта соседнего устройства
Системное имя	Системное имя соседнего устройства.
Конфигурация IP	IP-адрес управления соседнего устройства или порта.

6.3 DHCP-сервер

DHCP (Dynamic Host Configuration Protocol) обычно применяется в крупных локальных сетях (LAN). Его основные функции включают централизованное управление и распределение IP-адресов, что позволяет хосту в сети динамически получать IP-адрес, адрес шлюза и адрес DNS-сервера, а также улучшать использование адресов.

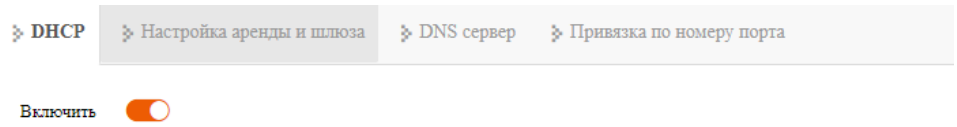
6.3.1 Настройка DHCP-сервера

Описание функции

Включение и отключение DHCP-сервера

Путь: Откройте панель навигации: "Конфигурация сети> DHCP-сервер> DHCP".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Включить	После включения, устройство выступающее в роли DHCP-сервера, может распределять IP-адреса для подключенных к нему устройств путем настройки таблицы статического распределения адресов.

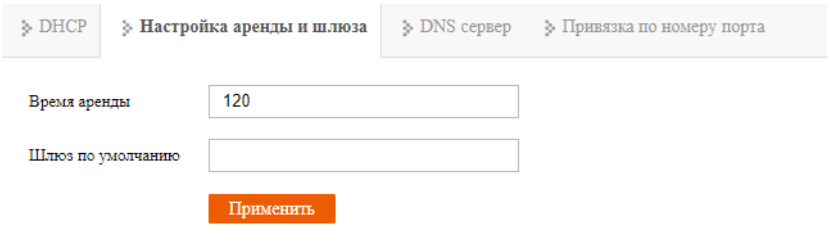
6.3.2 Настройка аренды шлюза

Описание функции

Установите время аренды и шлюз по умолчанию для IP-адреса клиента

Путь: Откройте панель навигации: "Конфигурация сети> DHCP-сервер> Настройка аренды шлюза".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Время аренды	Время аренды IP-адреса клиента. Значение по умолчанию — 120, единица измерения — минуты, диапазон значений — от 1 до 65535. Примечание: Когда время аренды IP-адреса, полученного клиентом DHCP, достигает срока аренды, его необходимо продлить, иначе IP-адрес станет недействительным, и клиенту DHCP нужно будет запрашивать IP-адрес снова
Шлюз по умолчанию	Адрес шлюза клиента по умолчанию, пример: 255.255.255.0

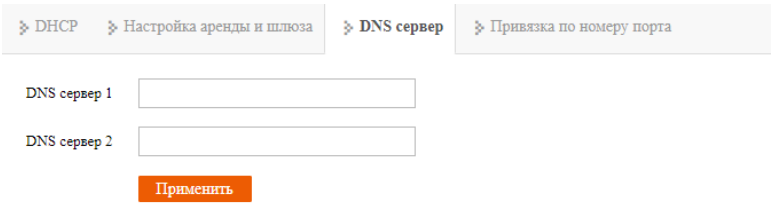
6.3.3 DNS сервер

Описание функции

Указание DNS-серверов

Путь: Откройте панель навигации: "Конфигурация сети> DHCP-сервер> DNS-сервер".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
DNS сервер 1	IP адрес DNS сервера 1
DNS сервер 2	IP адрес DNS сервера 2

6.3.4 Привязка по номеру порта

Описание функции

Установка соответствия IP-адресов, назначенных портам.

Возьмем в качестве примера устройство A и устройство B.

Если функция DHCP-сервера включена на устройстве A и установлены две таблицы статического выделения адресов:

192.168.1.19 соответствует порту 1;

192.168.1.20 соответствует порту 2.

После включения функции автоматического получения IP-адреса на устройстве B,

Если устройство A подключено к устройству B через порт 1, устройство B может автоматически получить IP-адрес 192.168.1.19;

Если устройство A подключено к устройству B через порт 2, устройство B может автоматически получить IP-адрес 192.168.1.20.

Путь: Откройте панель навигации: "Конфигурация сети> DHCP-сервер> Привязка по номеру порта".

Скриншот интерфейса:

Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
IP-адрес	IP адрес который указывается вручную
Порт	Порт на который закрепляется IP-адрес

6.4 Контроль доступа

6.4.1 Аутентификация порта

Протокол IEEE 802.1X представляет собой протокол управления доступом к сети на основе портов, то есть устройства пользователей аутентифицируются на портах устройств доступа к LAN, чтобы устройства пользователей могли контролировать доступ к сетевым ресурсам.

IEEE 802.1X принимает логические функции "управляемого порта" и "неконтролируемого порта" в архитектуре аутентификации, таким образом, реализуя разделение бизнеса и аутентификации. После прохождения пользователя аутентификации потоки бизнеса и аутентификации реализуют разделение. У него нет специальных требований к последующей обработке пакетов, сервис может быть очень гибким, и имеет большое преимущество в бизнесе, особенно в области многоадресной широкополосной передачи, все услуги не ограничены методом аутентификации.

Структура 802.1X включает в себя три основных компонента:

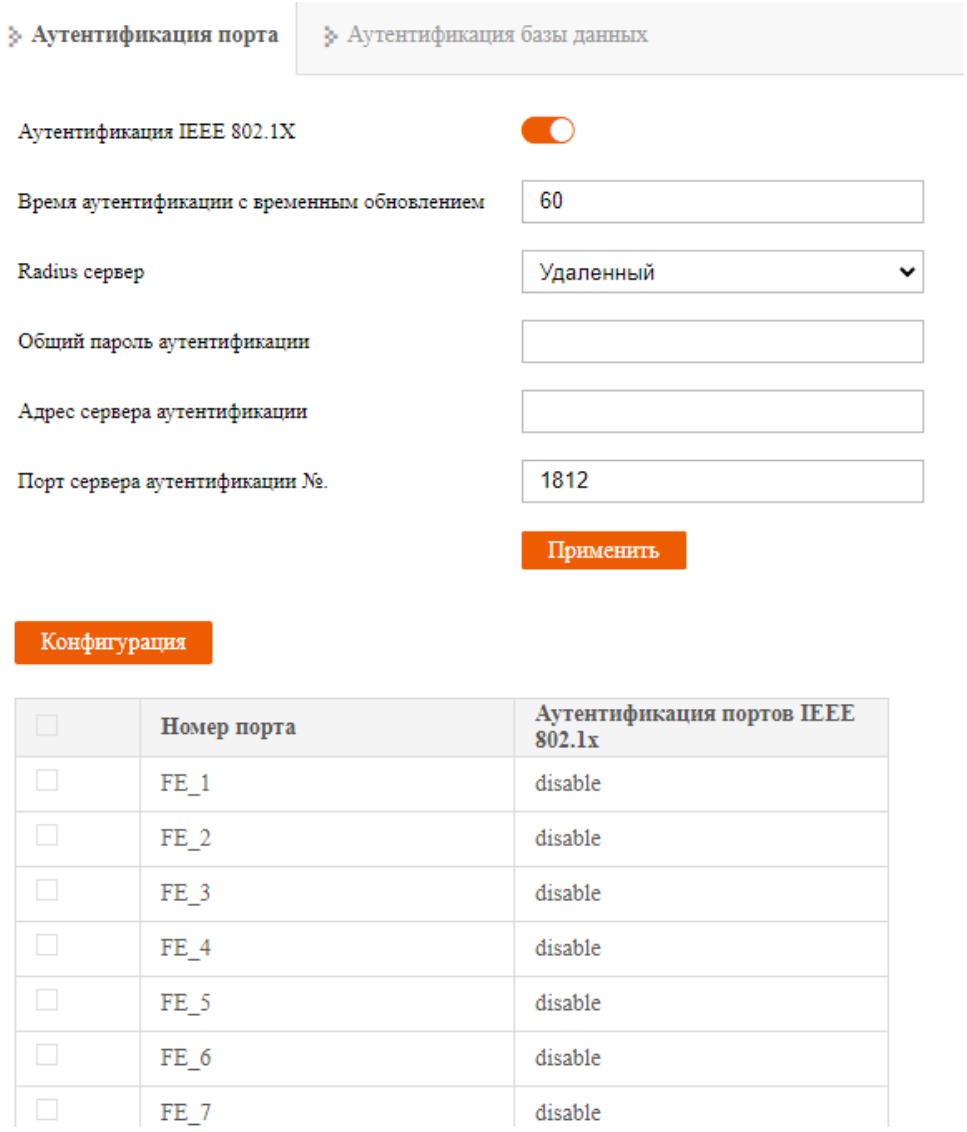
- Станция (Supplicant): пользователь или клиент, который хочет пройти аутентификацию;
- Сервер аутентификации: типичным примером является сервер RADIUS;
- Аутентификатор: устройства доступа, такие как беспроводные точки доступа, коммутаторы и т. д.

Описание функции

Включение и конфигурация функции 802.1X

Путь: Откройте панель навигации: "Конфигурация сети> Контроль доступа> Аутентификация порта".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Аутентификация IEEE 802.1X	Включение и отключение функции
Время аутентификации с временным обновлением	Диапазон интервала обновления аутентификации составляет от 60 до 4095 секунд. Единица измерения - секунда. Период повторной аутентификации 802.1X используется для укрепления безопасности аутентификации.
Radius сервер	Конфигурация локального внутреннего RADIUS-сервера и внешнего RADIUS-сервера:

	• Локальный: встроенный RADIUS-сервер. При выборе внутреннего RADIUS-сервера заявитель будет использовать только имя пользователя и пароль внутренней базы данных RADIUS. • Удаленный: укажите IP-адрес, номер порта и общий пароль для аутентификации на сервере аутентификации при использовании внешнего RADIUS-сервера.
Общий пароль аутентификации	Общий пароль - это строка символов, используемая для доступа устройства к серверу Radius. Поддерживаются комбинации букв, цифр и символов длиной не более 50 символов.
Адрес сервера аутентификации	IP адрес сервера аутентификации
Порт сервера аутентификации	Порт сервера аутентификации. По умолчанию порт 1812. Диапазон портов 1-65535
Номер порта	Порт устройства
Аутентификация портов IEEE 802.1X	Статус функции IEEE 802.1X порта: • Enable • Disable

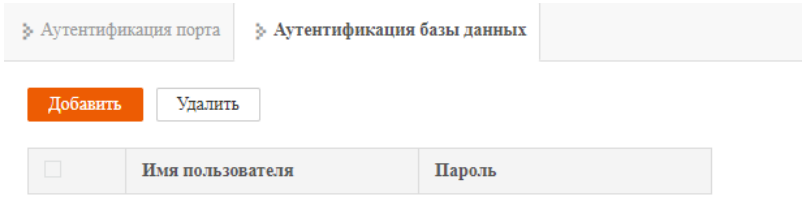
6.4.2 Аутентификация базы данных

Описание функции

Добавление локального имени пользователя и пароля для аутентификации по протоколу 802.1X, а также добавление, удаление и сохранение пользователей

Путь: Откройте панель навигации: "Конфигурация сети> Контроль доступа> Аутентификация базы данных".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Имя пользователя	Имя пользователя для аутентификации
Пароль	Пароль для аутентификации

6.5 QoS

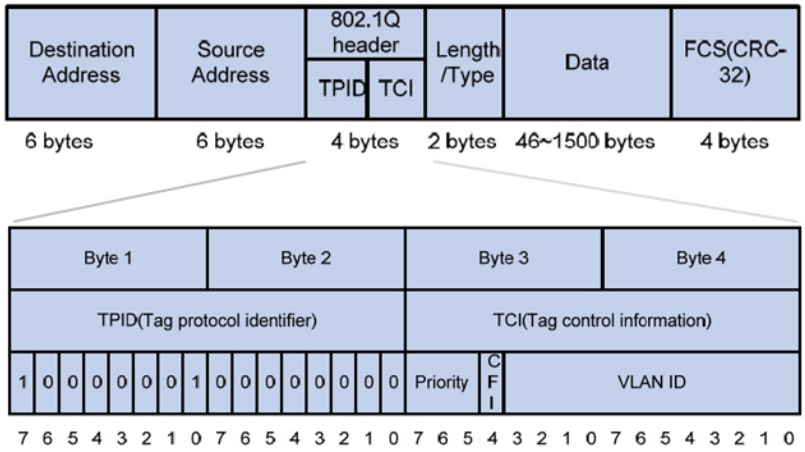
6.5.1 QoS Классификация

QoS (Quality of Service) используется для оценки способности поставщика услуг удовлетворять потребности клиентов в обслуживании. Что касается сетевого бизнеса, то качество услуг включает в себя пропускную способность передачи данных, задержку передачи, скорость потери пакетов данных и т.д.

Проблемы с качеством обслуживания, с которыми сталкиваются традиционные сети, возникают из-за сетевой перегрузки. Под перегрузкой понимается явление, при котором скорость передачи данных снижается, а дополнительные задержки возникают из-за относительной нехватки ресурсов, что приводит к снижению качества обслуживания. Для управления перегрузкой обычно применяется технология очередей. Она использует алгоритм очереди для классификации потоков, а затем использует некоторый алгоритм приоритетов для их отправки. Приоритет используется для маркировки важности передачи сообщения.

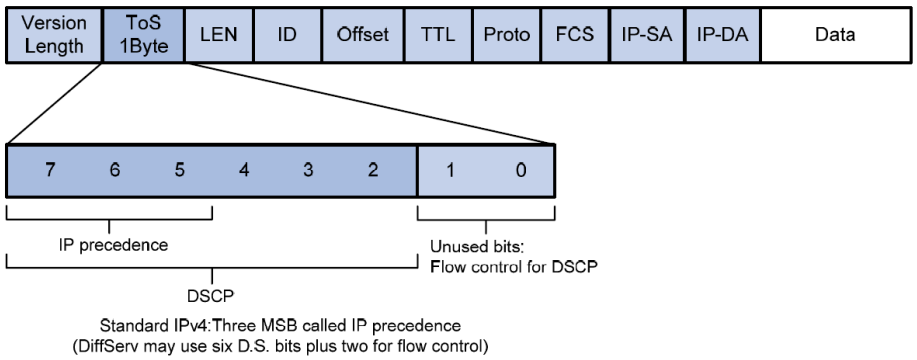
CoS

Ethernet определяет 8 приоритетов обслуживания (CoS, Class of Service) в теге VLAN заголовка фрейма Ethernet. 4-байтовый заголовок метки 802.1Q включает 2-байтовый TPID (Tag Protocol Identifier) и 2-байтовый TCI (Tag Control Information), TPID имеет значение 0x8100, на следующем рисунке показаны детали заголовка метки 802.1Q, поле приоритета - это приоритет 802.1p.



ToS

Поле ToS (Type of Service) в заголовке IP-сообщения называется доменом DS (differential Services), в котором приоритет DSCP представлен первыми 6 битами (от 0 до 5) этого поля, со значением от 0 до 63, а последние 2 бита (6 и 7) зарезервированы. Чем выше значение уровня приоритета, тем выше уровень приоритета.

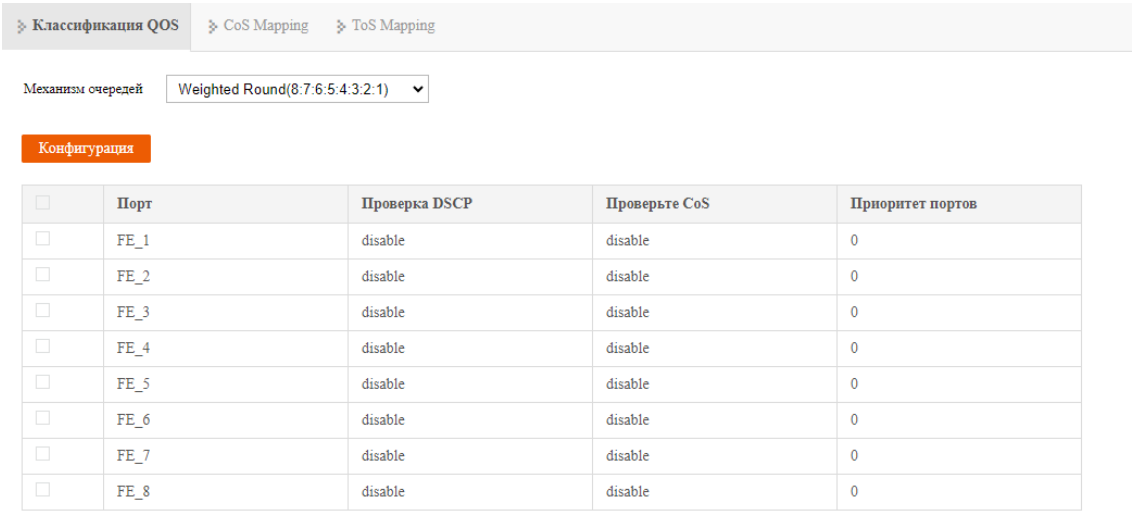


Описание функции

Настройте механизм очереди устройства и параметры приоритета каждого порта.

Путь: Откройте панель навигации: "Конфигурация сети> QoS> Классификация QOS".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Механизм очередей	Настройки планирования очередей: • Weighted Fair (8:4:2:1): Этот метод использует алгоритм планирования Weighted Round Robin (WRR) где каждой очереди назначены разные веса (8:4:2:1) • Strict (Strict Priority): Этот метод явно расставляет приоритеты между очередями. Обычно существует четыре очереди (хотя точное число может меняться). Пакеты обслуживаются в соответствии с назначенным им приоритетом, от самого высокого к самому низкому.
Порт	Порт устройства
Проверка DSCP	После установки флажка при планировании очереди будет проверяться приоритет ToS.

Проверьте CoS	После установки флажка при планировании очереди будет проверяться приоритет CoS.
Приоритет портов	Чтобы настроить приоритет порта по умолчанию для портов, которые не включили приоритет ToS и CoS. Диапазон значений составляет 0-7. Чем выше значение, тем выше приоритет. Примечание: По умолчанию коммутатор будет использовать приоритет порта вместо приоритета 802.1p, установленного на порте при получении сообщения, для управления качеством обслуживания сообщений.

Примечание

- Когда ToS и CoS не активированы, очередь и планирование осуществляются в порядке приоритета порта.
- Когда активированы ToS или CoS, очередь и планирование осуществляются в соответствии с ToS или CoS, а не с учетом приоритета порта.
- Если ToS и CoS активированы одновременно, очередь формируется в соответствии с приоритетом ToS. Когда значения ToS одинаковы, очередь формируется в соответствии с приоритетом CoS.

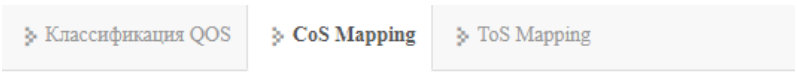
6.5.2 CoS Mapping

Описание функции

На странице "Отображение CoS" пользователь может настроить отображение между значением CoS и приоритетными очередями.

Путь: Откройте панель навигации: "Конфигурация сети> QoS> CoS Mapping".

Скриншот интерфейса:



Значение CoS	Приоритет очереди
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Значение CoS	Отображение значении CoS
Приоритет очереди	Установите отображение между значением CoS и приоритетной очередью. Приоритетная очередь представлена следующим образом: • Низкий: очередь с низким приоритетом • Обычный: обычная приоритетная очередь • Средний: средняя приоритетная очередь • Высокий: очередь с высоким приоритетом

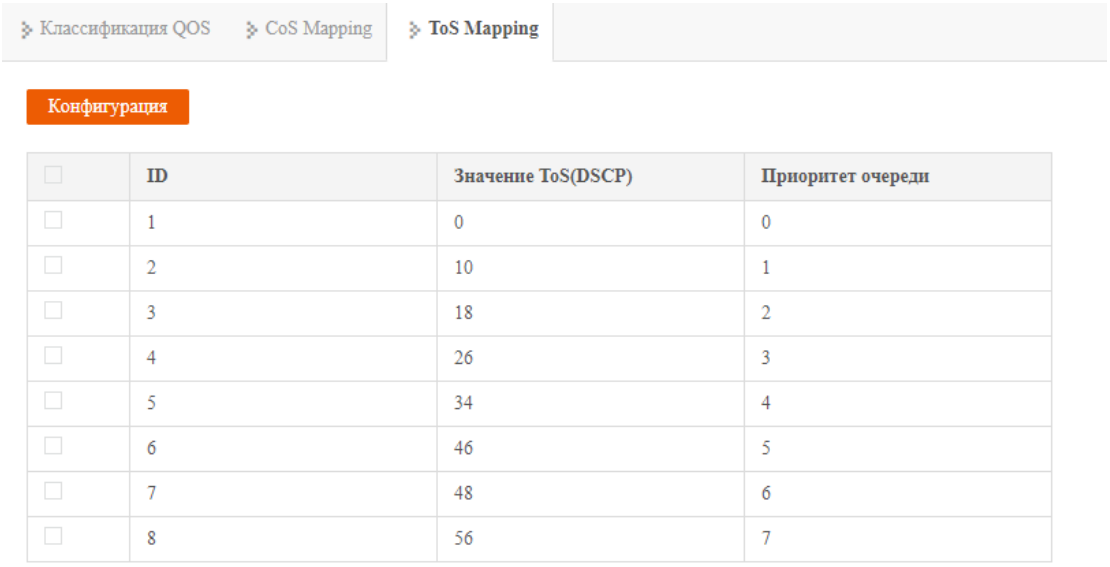
6.5.3 ToS Mapping

Описание функции

На странице "Отображение ToS", пользователь может настроить отображение между значением ToS и приоритетной очередью.

Путь: Откройте панель навигации: "Конфигурация сети> QoS> ToS Mapping".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Значение ToS (DSCP)	Он отображает значение ToS (DSCP) одновременно в шестнадцатеричном и десятичном форматах.
Приоритет очереди	Установите отображение между значением ToS и приоритетной очередью, варианты следующие: • Низкий: очередь с низким приоритетом • Обычный: обычная приоритетная очередь • Средний: средняя приоритетная очередь • Высокий: очередь с высоким приоритетом

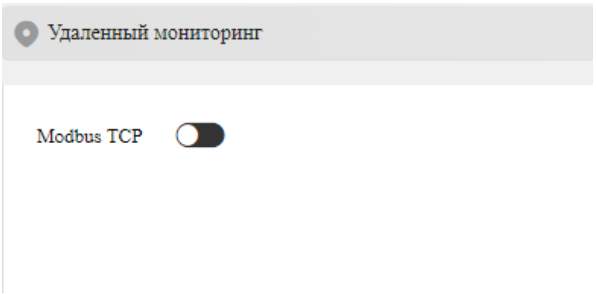
6.6 Modbus TCP

Описание функции

Устройство поддерживает функцию мониторинга Modbus TCP. Можно считывать информацию о системе коммутатора, портах, кольцевой сети, статистике кадров и другие параметры через протокол Modbus TCP, что удобно для различных интегрированных систем для мониторинга и управления устройством.

Путь: Откройте панель навигации: "Конфигурация сети> Modbus TCP".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Modbus TCP	Включение мониторинга Modbus TCP, который по умолчанию отключен. После включения функции мониторинга Modbus TCP клиент может считывать информацию об устройстве

Modbus TCP спецификация

Информация об адресах регистров коммутатора только для чтения и сохраненная информация об устройстве представлена в таблице ниже:

Примечание

- Адрес в следующей таблице представлен в шестнадцатеричном формате. Пожалуйста, преобразуйте его в подходящий формат в соответствии с требованиями текущего инструмента отладки
- Коммутатор может одновременно устанавливать 4 мониторинговых соединения по Modbus TCP.

Тип информации	Адрес (HEX)	Тип данных	Описание
Системная информация	0x0000	2 слова	Идентификатор устройства
	0x0002	16 слов	Имя (отображение ASCII)
	0x0012	16 слов	Описание (отображение ASCII)
	0x0022	3 слова	MAC-адрес (отображение HEX)
	0x0025	2 слова	IP-адрес
	0x0027	16 слов	Контактная информация
	0x0037	16 слов	Версия прошивки (отображение ASCII)
	0x0047	16 слов	Версия оборудования (отображение ASCII)
	0x0057	16 слов	Серийный номер
	0x0067	1 слово	Статус питания 1 • 0x0000: ВЫКЛ • 0x0001: ВКЛ
	0x0068	1 слово	Статус питания 2: • 0x0000: ВЫКЛ • 0x0001: ВКЛ
Информация о портах	0x1000-0x101B	1 слово	Статус соединения порта: • 0x0000: Соединение разорвано • 0x0001: Соединение установлено • 0x0002: Отключено • 0xFFFF: Нет порта
	0x101D-0x1038	1 слово	Режим работы порта: • 0x0000: 10M-Half • 0x0001: 10M-Full • 0x0002: 100M-Half • 0x0003: 100M-Full • 0x0004: 1G-Half • 0x0005: 1G-Full • 0xFFFF: Нет порта
	0x1039-0x1054	1 слово	Статус контроля потока порта: • 0x0000: ВЫКЛ • 0x0001: ВКЛ • 0xFFFF: Нет порта
	0x1056-0x1071	1 слово	Тип интерфейса порта: • 0x0000: Медный порт • 0x0001: Оптический порт • 0x0002: Комбинированный порт • 0xFFFF: Нет порта

7. Система

7.1 Диагностика сети

7.1.1 Ping

Описание функции

Команда Ping используется для проверки открыт ли сетевой доступ или для оценки скорости сетевого соединения. Команда Ping использует уникальность IP-адресов машин в сети для отправки пакета на целевой IP-адрес, после чего запрашивает противоположный конец вернуть пакет с таким же размером, чтобы определить состояние соединения и задержку между двумя сетевыми устройствами.

Путь: Откройте панель навигации: "Система> Диагностика сети".

Скриншот интерфейса:

Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Адрес	IP-адрес обнаруженного устройства, то есть адрес назначения. Устройство может проверить сетевое взаимодействие с другими устройствами с помощью команды ping

7.2 NTP

7.2.1 Конфигурация NTP

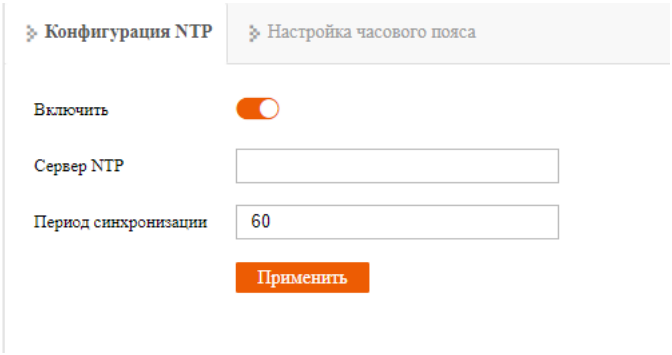
Полное название протокола NTP — Протокол сетевого времени (Network Time Protocol). Его целью является обеспечение единообразного, стандартизированного времени в Интернете. Конкретная схема реализации заключается в назначении нескольких веб-сайтов источников времени в сети для предоставления пользователям службы синхронизации времени. Эти веб-сайты должны иметь возможность сравниваться друг с другом для повышения точности. Протокол может обеспечивать коррекцию времени до миллисекунд и подтверждается зашифрованным способом для предотвращения злонамеренных атак на протокол.

Описание функции

Включение и конфигурация NTP сервера.

Путь: Откройте панель навигации: "Система> NTP> Конфигурация NTP".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Включить	Включение и отключение NTP конфигурации
Сервер NTP	IP Адрес сервера NTP
Период сканирования	Период синхронизации с сервером NTP

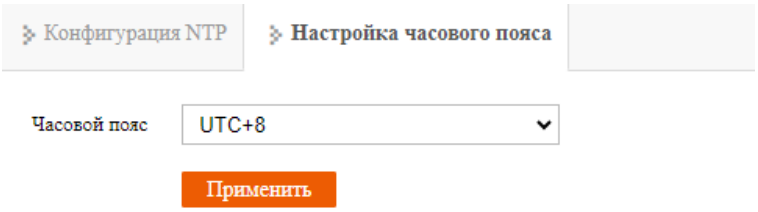
7.2.2 Настройка часового пояса

Описание функции

Настройка часового пояса.

Путь: Откройте панель навигации: "Система> NTP> Конфигурация часового пояса".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Часовой пояс	Временная зона UTC (Всемирное координированное время). Благодаря различным регионам, пользователи могут свободно устанавливать системные часы в соответствии с правилами своей страны или региона.

7.3 Сигнал тревоги

После включения сигнализации, при возникновении нештатной ситуации на порту устройства, пользователь может быть своевременно оповещен, а состояние устройства быстро восстановлено.

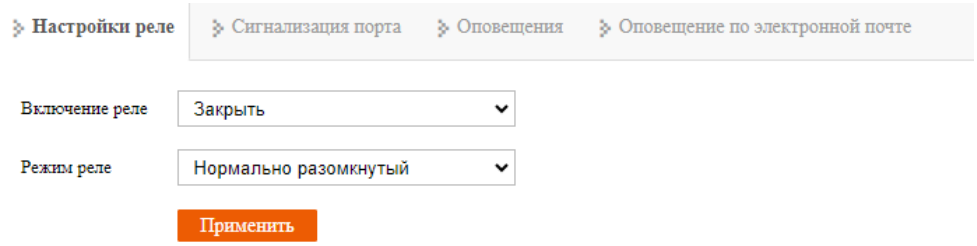
7.3.1 Настройки реле

Описание функции

Включение реле и настройка его работы.

Путь: Откройте панель навигации: "Система> Сигнал тревоги> Настройки реле".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Включение реле	Включение/выключение реле
Режим реле	Установите режим работы реле: • Нормально закрытый: В обычном состоянии, без срабатывания сигнализации, реле находится во включенном (замкнутом) состоянии. При срабатывании сигнализации реле переходит в разомкнутое состояние. • Нормально открытый: В обычном состоянии, без срабатывания сигнализации, реле находится в разомкнутом состоянии. При срабатывании сигнализации реле переходит во включенное (замкнутое) состояние.

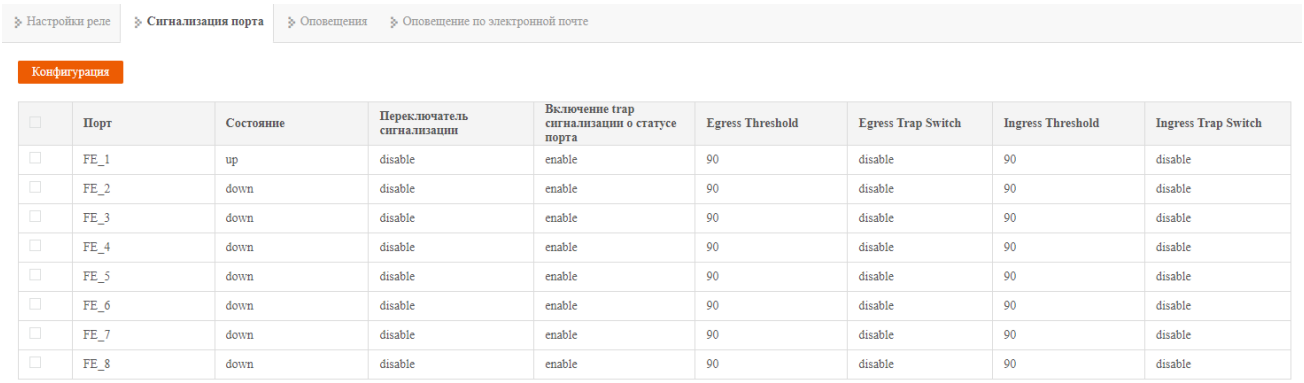
7.3.2 Сигнализация порта

Описание функции

При включении сигнализации, система сможет своевременно оповестить администратора о возникшей неисправности на порту устройства.

Путь: Откройте панель навигации: "Система> Сигнал тревоги> Сигнализация порта".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Порт	Порт устройства
Состояние	Состояние порта • Up • Down
Переключатель сигнализации	Состояние функции сигнализации порта • Enable • Disable
Включение trap сигнализации о статусе порта	Сигнализация о состоянии порта • Enable • Disable
Egress Threshold	При достижении порогового значения будет отправляться информация о ловушке. Варианты ловушки исходящего трафика: • Включить (Enable) - Ловушка исходящего трафика будет активирована. При достижении порогового значения трафика будет отправлено сообщение о ловушке. • Отключить (Disable) - Ловушка исходящего трафика будет отключена. Сообщения о ловушке отправляться не будут, даже если трафик превысит пороговое значение.
Egress Trap Switch	При достижении порогового значения исходящего трафика на порту, программное обеспечение NMS (сетевая система управления) срабатывает и выдает тревогу. Значение порогового значения может находиться в диапазоне от 5 до 95 процентов.

Ingress Threshold	Включение входящей ловушки. Отправка информации при достижении порогового значения. • Включить • Отключить
Ingress Trap Switch	Когда входящий порт достигает порогового значения, программное обеспечение NMS выдает сигнал тревоги. Диапазон значений порога: 5-95, единица измерения: %.

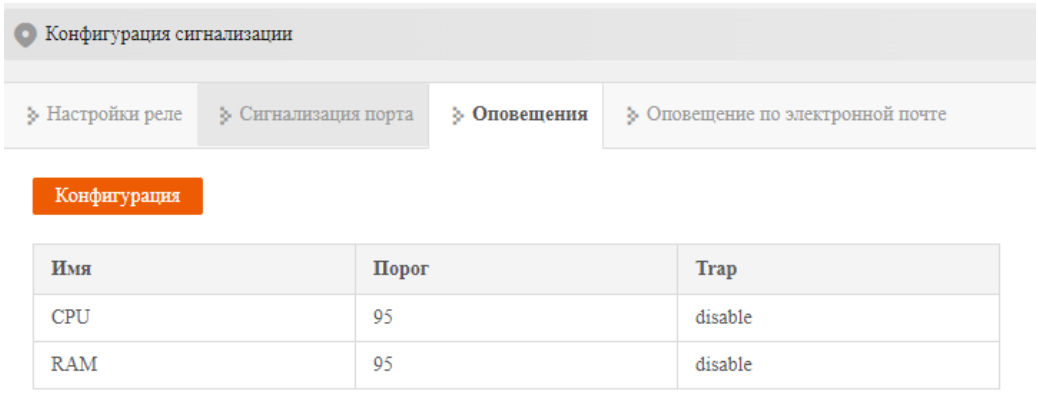
7.3.3 Оповещения

Описание функции

Настройка события сигнализации для использования ЦПУ и памяти. Когда значение параметра события сигнализации превышает установленный порог, устройство будет непрерывно отправлять информацию Trap. Когда значение параметра события сигнализации опускается ниже установленного порога, устройство отправит соответствующее сообщение Trap.

Путь: Откройте панель навигации: "Система> Сигнал тревоги> Оповещения".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
CPU Порог	Порог использования ЦПУ: когда использование ЦПУ достигает порогового значения, будет сгенерирован сигнал тревоги. Диапазон значений порога: 5-95%
CPU Trap	Отправлять информацию Trap, когда использование ЦПУ достигает порогового значения. • Включить • Отключить
RAM Порог	Порог использования памяти: когда использование памяти достигает порогового значения, будет сгенерирован сигнал тревоги. Диапазон значений порога: 5-95%

RAM Trap	Отправлять информацию Trap, когда использование памяти достигает порогового значения. • Включить • Отключить

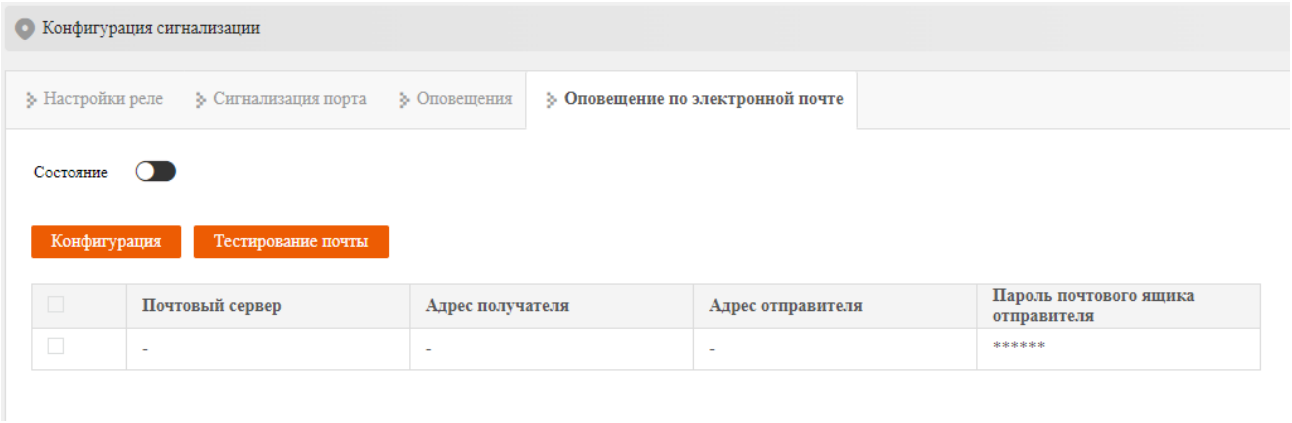
7.3.4 Оповещение по электронной почте

Описание функции

Включение и настройка оповещения по электронной почте.

Путь: Откройте панель навигации: "Система> Сигнал тревоги> Оповещение по электронной почте".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Состояние	Включение/выключение функции
Почтовый сервер	Адрес сервера используемой электронной почты должен быть заполнен в соответствии с учетной записью используемого адреса электронной почты. IP-адрес хоста или используемое имя хоста, которое предоставляет услугу доставки электронной почты для устройства.
Адрес получателя	Адрес электронной почты, используемый получателем уведомлений о нештатных событиях.
Адрес отправителя	Адрес электронной почты отправителя, имя учетной записи, используемое для входа на почтовый сервер.
Пароль почтового ящика отправителя	Пароль электронной почты отправителя, соответствующий пароль, используемый для входа в учетную запись электронной почты.

Примечание

При использовании сигнализации по электронной почте пользователь должен убедиться, что коммутатор нормально подключен к сети и шлюз коммутатора такой же, как и шлюз локальной сети.

7.4 Конфигурационный файл

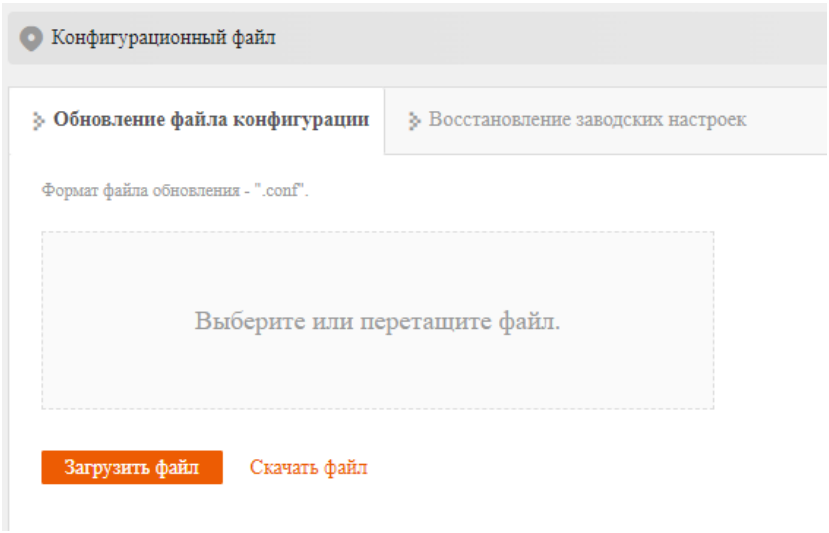
7.4.1 Обновление файла конфигурации

Описание функции

Загрузка и выгрузка конфигурационного файла.

Путь: Откройте панель навигации: "Система> Конфигурационный файл> Обновление файла конфигурации ".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Загрузить файл	Формат файла конфигурации - ".conf". Перетащите файл в поле обновления или нажмите "Нажмите для загрузки", чтобы выбрать файл.
Скачать файл	Загрузить файлы конфигурационной информации текущего коммутатора. Совет: Загруженные файлы конфигурации можно загрузить на другие идентичные устройства, обеспечивая повторное использование после однократной настройки.

Внимание
В процессе загрузки файлов конфигурации или обновления программного обеспечения обновляйте и не переходите на другую WEB-страницу коммутатора, так же не перезагружайте устройство; в противном случае это приведет к сбою загрузки файлов конфигурации или обновлению программного обеспечения, что в свою очередь приведет к поломке устройства.

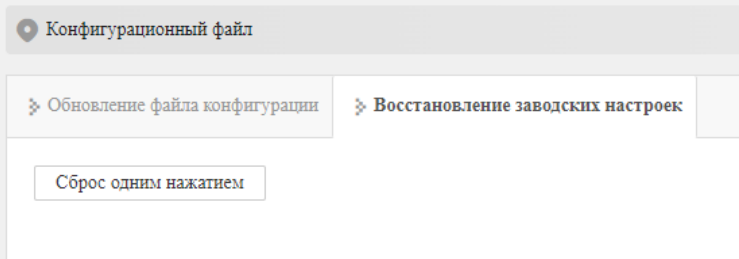
7.4.2 Восстановление заводских настроек

Описание функции

Восстановление заводских настроек устройства.

Путь: Откройте панель навигации: "Система> Конфигурационный файл> Восстановление заводских настроек ".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Сброс одним нажатием	Восстановление заводских настроек коммутатора. Примечание: Восстановление заводских настроек приведет к тому, что устройство будет восстановлено до заводских настроек. IP-адрес по умолчанию — «192.168.1.254».

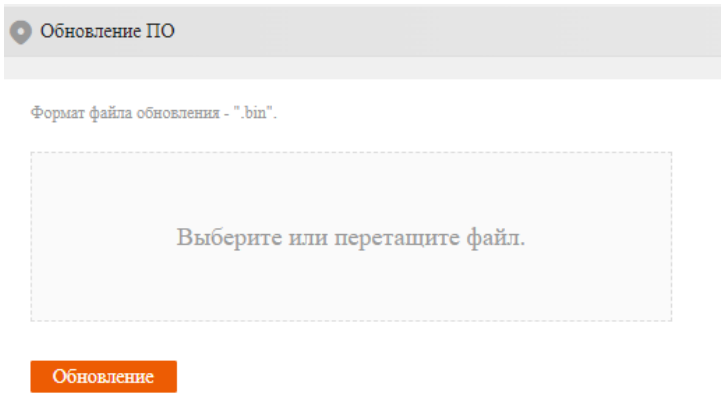
7.5 Обновление ПО

Описание функции

Обновление программного обеспечения устройства.

Путь: Откройте панель навигации: "Система> Обновление ПО".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Обновление	Перетащите файл обновления в поле обновления или нажмите «Нажмите Загрузить», чтобы выбрать обновленный файл в формате «.bin».

7.6 Логи

7.6.1 Информация о логировании

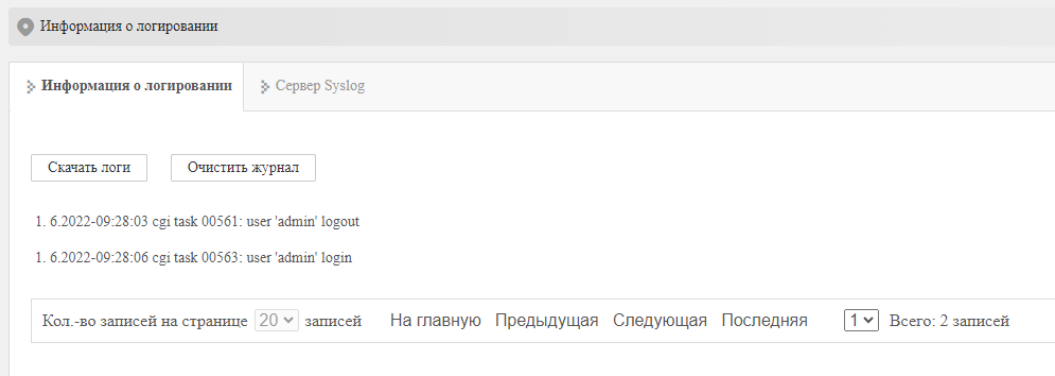
Описание функции

Информация о логировании записывает операции пользователя, сбои системы, информацию о безопасности системы и другую информацию, включая журнал пользователя, журнал безопасности и диагностический журнал.

- Журнал пользователя: записывает операции пользователя и информацию о работе системы.
- Журнал безопасности: записывает информацию, включающую управление учетными записями, протоколы, защиту от атак и статус.
- Диагностический журнал: записывает информацию, помогающую в идентификации проблем.

Путь: Откройте панель навигации: "Система> Логи> Информация о логировании ".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Скачать логи	Скачивание информации в текстовом файле
Очистить журнал	Очистка всей информации

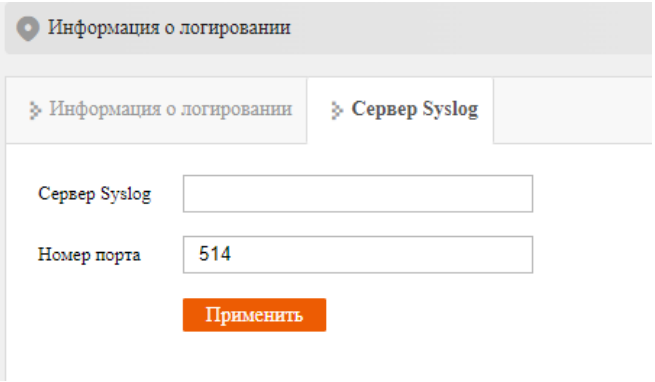
7.6.2 Сервер syslog

Описание функции

Конфигурация сервера для отправки логов с устройства на сервер.

Путь: Откройте панель навигации: "Система> Логи> Сервер Syslog".

Скриншот интерфейса:



Описание основных элементов конфигурации интерфейса:

Элемент интерфейса	Описание
Сервер Syslog	IP адрес сервера
Номер порта	Порт сервера

8. FAQ

8.1 Проблема при входе

8.2

1. Почему веб-страница отображается некорректно при просмотре конфигурации через WEB?

   Перед доступом к WEB очистите кэш и куки IE. В противном случае веб-страница будет отображаться некорректно.

8.3 Проблемы с конфигурацией

1. Как восстановить заводские настройки устройства через DIP-переключатель?

   Переведите DIP-переключатель 2 в положение ON и после повторного включения питания восстановите заводские настройки.

2. Почему после настройки функции объединения портов (Trunking) не увеличивается пропускная способность?

   Проверьте, совпадают ли атрибуты портов, установленные для Trunking, такие как скорость, дуплексный режим, VLAN и другие атрибуты.

3. Как решить проблему, когда часть портов коммутатора непроходима?

   Если некоторые порты на коммутаторе непроходимы, возможно, есть неисправности в сетевом кабеле, сетевом адаптере или самом порте коммутатора. Пользователь может определить неисправности, выполнив следующие тесты:
   - Оставьте подключенный компьютер и порты коммутатора без изменений, поменяйте другие сетевые кабели;
   - Оставьте подключенный сетевой кабель и порт коммутатора без изменений, поменяйте другие компьютеры;
   - Оставьте подключенный сетевой кабель и компьютер без изменений, поменяйте другой порт коммутатора;
   - Если подтверждены неисправности порта коммутатора, обратитесь к поставщику для технического обслуживания.

4. В каком порядке происходит обнаружение состояния самонастройки портов?

   Обнаружение состояния самонастройки портов происходит в следующем порядке: 1000Мбит/с полный дуплекс, 100Мбит/с полный дуплекс, 100Мбит/с полудуплекс, 10Мбит/с полный дуплекс, 10Мбит/с полудуплекс, подключение автоматически в поддерживаемой наивысшей скорости.

8.4 Проблемы с индикаторами

1. Почему индикатор питания не светится?

Возможные причины:

- Не подключен к сетевой розетке; устраните проблему, подключив к сетевой розетке.
- Неисправность в источнике питания или самом индикаторе; устраните проблему, заменив источник питания или проверив устройство.
- Напряжение питания не соответствует требованиям устройства; устраните проблему, настроив напряжение питания в соответствии с руководством устройства.

2. Почему индикатор Link/Act не горит?

Возможные причины:

- Сетевой кабель в части Ethernet медного порта отключен или есть плохой контакт; устраните проблему, проверив и подключив сетевой кабель снова.
- Аберрации в работе сетевого устройства или сетевой карты Ethernet; устраните проблему, исключив неисправность терминального устройства.
- Не подключен к сетевой розетке; устраните проблему, подключив к сетевой розетке.
- Скорость интерфейса не соответствует режиму работы; устраните проблему, проверив, соответствует ли скорость передачи данных устройства дуплексному режиму.

3. Индикаторы Ethernet медного порта и оптического порта подключены нормально, но данные не передаются. В чем причина?

   При включении системы или изменении конфигурации сети устройству и коммутатору требуется некоторое время. Устраните проблему, дождавшись завершения конфигурации устройства и коммутатора. Если проблема сохраняется, выключите систему и снова включите ее.

4. Почему происходят сбои в коммуникации после некоторого времени, то есть нет возможности связаться, и после перезагрузки все возвращается к нормальному состоянию?

Причины могут включать:

- Влияние окружающей среды на устройство; устраните проблему, используя заземление продукции или экранирование источников помех.
- Ненормативная разводка на месте; устраните проблему, размещая оптоволоконные и сетевые кабели так, чтобы они не пересекались с силовыми и высоковольтными линиями.
- Сетевой кабель подвергается воздействию статического электричества или скачков напряжения; устраните проблему, заменив экранированный кабель или установив молниезащиту.
- Влияние высоких и низких температур; устраните проблему, проверив диапазон рабочих температур устройства.

Контактная информация

109380, Россия, Москва
Ул. Ставропольская, д. 84, стр. 1

ООО "АйПиСи2Ю"
ИНН: 7721557513

+7 495 232-02-07
+7 495 642-82-44 (многоканальный)

support@ipc2u.ru
sales@ipc2u.ru

Ссылка на оборудование