

NIKOMAX

Руководство пользователя по Web-интерфейсу

Серия промышленных коммутаторов G207, G307



Оглавление

1. Web-интерфейс	5
1.1. Вход в Web-интерфейс	5
1.2. Выход из Web-интерфейса	5
1.3. Сохранение конфигурации	6
1.4. Перезагрузка устройства	6
1.5. Навигация в Web-интерфейсе	6
2. Monitor	8
2.1. Overview	8
2.2. Port Statistics	9
2.3. Loop Protection	10
2.4. Serial Server State	11
2.5. Security	12
2.6. PoE State	14
2.7. LLDP State	15
2.8. IGMP Snooping State	16
2.9. DHCP Snooping State	16
2.10. QinQ Information	17
3. Configuration	18
3.1. VLAN	18
3.1.1. Введение	18
3.1.2. Конфигурация VLAN	21
3.2. Port	23
3.2.1. Port Configuration	23
3.2.2. Port Extension	25
3.2.3. Port Mirroring	29
3.2.4. Port Aggregation	31
3.3. Spanning Tree	34
3.3.1. Введение	34
3.3.2. Конфигурация Spanning Tree	35
3.4. ERPS	37
3.4.1. Введение	37
3.4.2. Конфигурация ERPS	42
3.5. PoE Management	45
3.5.1. PoE Overview	45
	2

3.5.2.	Конфигурация PoE	46
3.6.	Security	49
3.6.1.	Port Security	49
3.6.2.	IP Source Guard	51
3.6.3.	Dot1X	55
3.6.4.	MAC Authentication	59
3.6.5.	RADIUS	60
3.7.	Control	63
3.7.1.	Serial Servers.....	63
3.7.2.	IO Control.....	66
4.	Advance.....	67
4.1.	LLDP	67
4.1.1.	Введение	67
4.1.2.	Конфигурация LLDP	67
4.2.	IGMP Snooping	72
4.2.1.	Принцип IGMP Snooping	72
4.2.2.	Конфигурация IGMP Snooping.....	73
4.3.	Управление MAC-адресами.....	75
4.3.1.	Введение	75
4.3.2.	Конфигурация MAC-адресов	76
4.4.	DHCP Snooping	78
4.4.1.	Введение	78
4.4.2.	Конфигурация DHCP Snooping.....	78
4.5.	QinQ.....	81
4.5.1.	Введение	81
4.5.2.	Конфигурация QinQ	82
4.6.	ACL	83
4.6.1.	Введение	84
4.6.2.	Конфигурация ACL	84
4.7.	QoS	89
4.7.1.	Введение	89
4.7.2.	Конфигурация QoS.....	89
5.	Maintenance	94
5.1.	Конфигурация системы.....	94
5.1.1.	Настройка имени хоста	94

5.1.2.	Включение сервисов	94
5.1.3.	IP-адрес управления	95
5.2.	Управление файлами	96
5.2.1.	Базовая информация.....	96
5.2.2.	Управление программным обеспечением.....	96
5.2.3.	Управление конфигурацией	97
5.2.4.	Управление сертификатами.....	98
5.2.5.	Управление пакетами.....	98
5.3.	Управление пользователями.....	99
5.4.	Управление системным временем.....	99
5.4.1.	Просмотр системного времени	99
5.4.2.	Конфигурация системного времени	100
5.4.3.	Конфигурация NTP сервера.....	100
5.5.	SNMP.....	101
5.5.1.	Конфигурация SNMP	101
6.	Diagnosis	102
6.1.	Network Utilities.....	102
6.1.1.	Инструменты диагностики	102
6.2.	Optical Transceiver Information.....	103
6.2.1.	Отображение информации оптического трансивера	103
6.2.2.	Отображение подробной информации	104
6.3.	One-click Collection	105
6.4.	Dying Gasp	105
6.4.1.	Введение	105
6.4.2.	Конфигурация Dying Gasp.....	105

1. Web-интерфейс

1.1. Вход в Web-интерфейс

Для первичного входа и конфигурирования устройства в Web-интерфейсе используется следующая информация по умолчанию:

- Имя пользователя: «**admin**»
- Пароль: «**admin**»
- IP-адрес устройства: «**192.168.56.166**»

Для первичного входа в Web-интерфейс выполните следующие шаги:

1. Осуществите прямое подключение сетевого порта компьютера к любому доступному порту коммутатора.
2. Измените IP-адрес компьютера на свободный в сегменте сети **192.168.56.0/24**, например, **192.168.56.2**
3. На компьютере откройте браузер, в адресную строку введите **192.168.56.166** и нажмите Enter.
4. На странице входа в Web-интерфейс, как показано на Рисунке 1. Введите имя пользователя - **admin** и пароль – **admin**, нажмите кнопку «Войти».

Managed Ethernet Switch

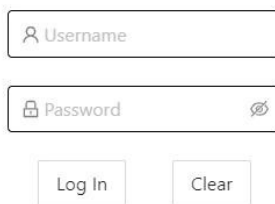


Рисунок 1 - Страница входа в Web-интерфейс

1.2. Выход из Web-интерфейса

Нажмите кнопку «Выход» в дополнительной области, чтобы выйти из Web-интерфейса, как показана на Рисунке 2.

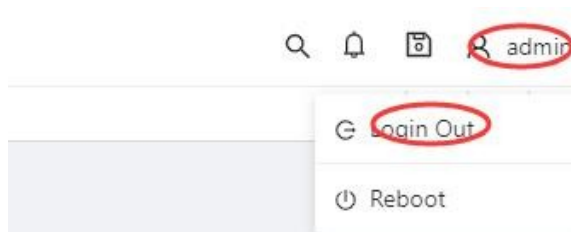


Рисунок 2 - Выход из Web-интерфейса

1.3. Сохранение конфигурации

Функция сохранения конфигурации предоставляет возможность сохранить текущие изменения настроек в файл конфигурации. Нажмите кнопку «Сохранить» для сохранения текущих настроек в файл конфигурации, как показано на Рисунке 3.

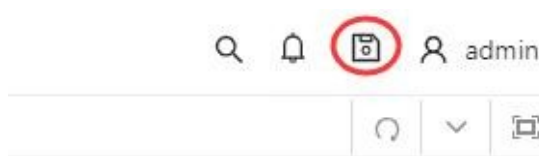


Рисунок 3 – Сохранение конфигурации

1.4. Перезагрузка устройства

Для выполнения перезагрузки устройства нажмите кнопку «Перезагрузить», как показано на Рисунке 4.

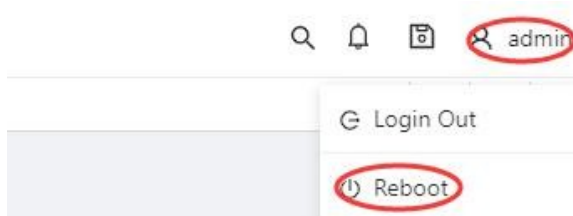


Рисунок 4 – Перезагрузка устройства

1.5. Навигация в Web-интерфейсе

Веб-интерфейс состоит из трех частей:

1. Основная область навигации
2. Вспомогательная область инструментов
3. Основная область настроек

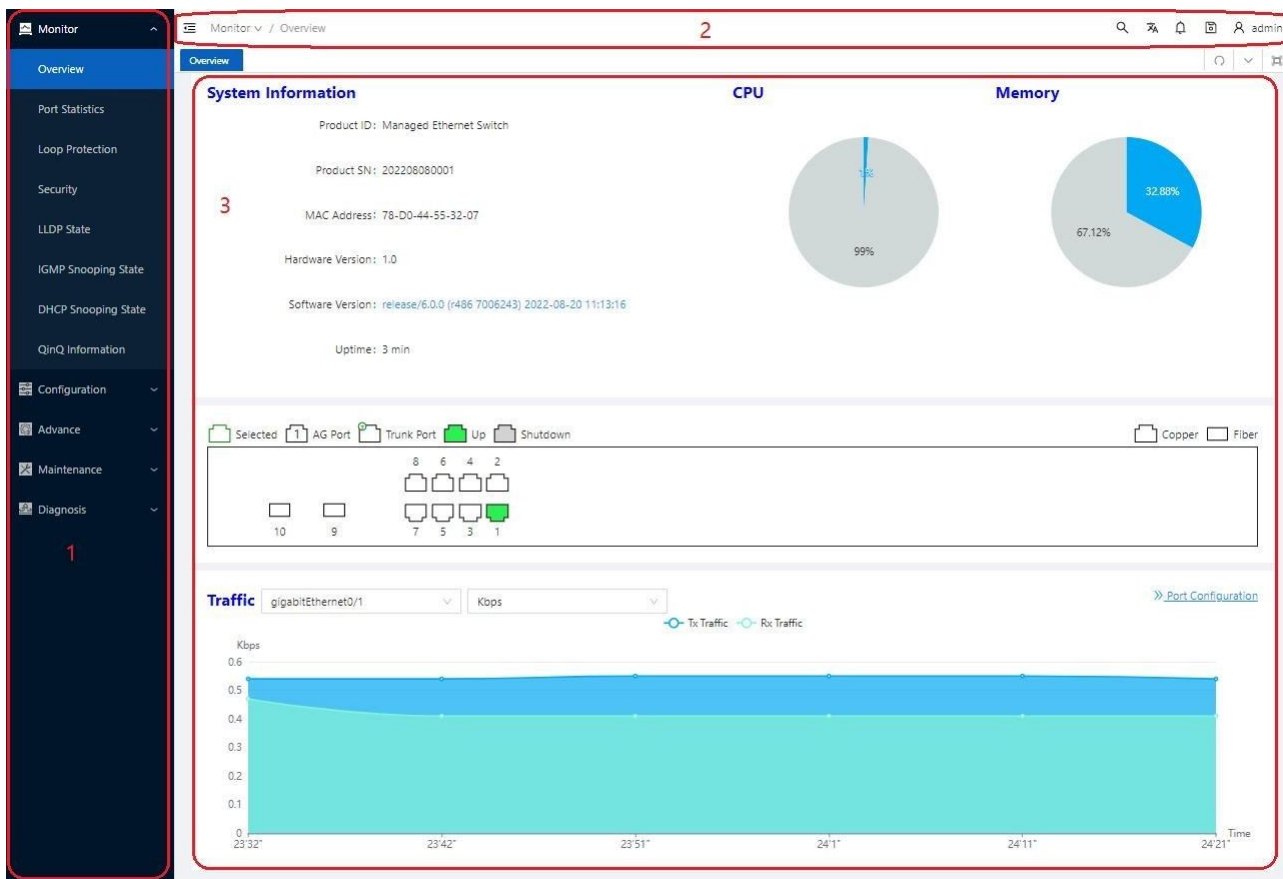


Рисунок 5 - Web-интерфейс

2. Monitor

2.1. Overview

Выберите «Monitor» - «Overview» в дереве навигации, чтобы перейти на страницу обзора информации о устройстве, как показано на Рисунке 6. Страница обзора информации о устройстве разделена на 3 области: «System Information», «Panel port» и «Traffic».

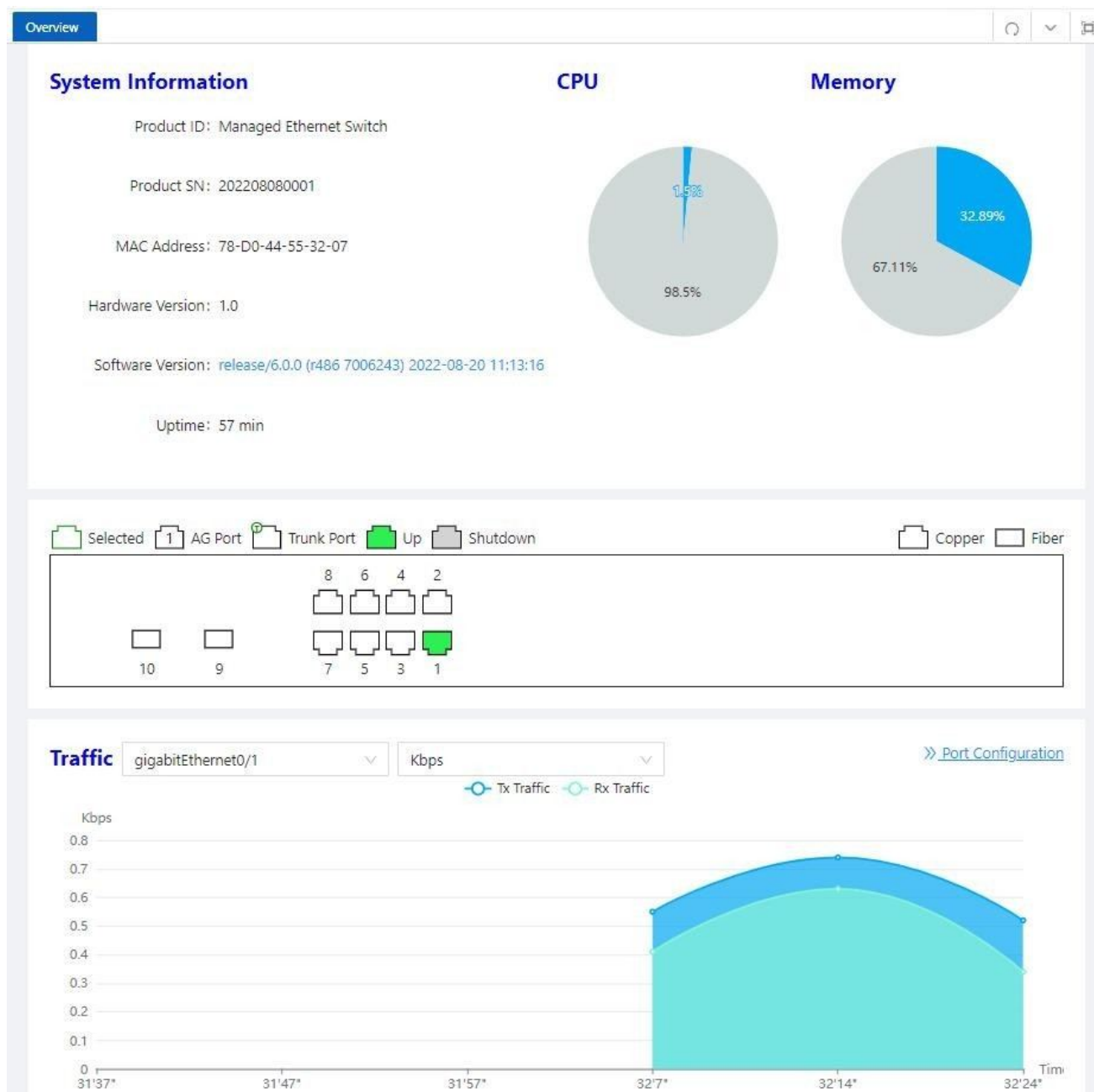


Рисунок 6 – Страница Overview

«System Information» отображает основную информацию о устройстве: product ID, serial number, MAC address, hardware version, software version и uptime.

Элемент	Описание
Product ID	Отображает имя устройства
Serial number	Отображает серийный номер устройства
MAC address	Отображает MAC-адрес устройства
Hardware version	Отображает аппаратную версию устройства
Software version	Отображает версию программного обеспечения устройства
Release Date	Отображает дату выпуска программного обеспечения устройства
CPU	Отображает состояние процессора устройства
Memory	Отображает состояние памяти устройства
Uptime	Отображает время с момента последнего запуска системы

«Panel port» отображает текущую информацию и статус портов.

«Traffic» отображает текущую информацию о входящем и исходящем трафике на выбранном порту.

2.2. Port Statistics

Страница «Port Statistics» отображает статистику о полученных и отправленных через интерфейсы пакетах.

Выберите «Monitor» - «Port Statistics» в дереве навигации, чтобы перейти на страницу, как показано на Рисунке 7.

Port Statistics								
Clear Auto Refresh		Port Configuration						
Port	Rx Load	Tx Load	Speed	Under Size	Over Size	CRC Error	Collision Count	Action
gigabitEthernet0/1	0 %	0 %	1000M	0	0	0	0	Clear

Рисунок 7 - Страница Port Statistics

«Port Statistics» отображает основную информацию о портах: Rx Load, Tx Load, Speed, Under size, Over size, CRC Error, Collision Count.

Элемент	Описание
Port	Имя логического интерфейса
Rx Load	Исходящая загрузка порта
Tx Load	Входящая загрузка порта
Speed	Скорость работы порта
Under Size	Количество пакетов, полученных портом, меньше 64 байт
Over Size	Количество пакетов, полученных портом, превышающих максимальное значение MTU
CRC Error	Количество полученных пакетов с ошибкой проверки CRC
Collision Count	Количество конфликтующих пакетов, полученных портом
Clear	Кнопка очистки статистики

2.3. Loop Protection

Страница «Loop Protection» используется для отображения рабочего состояния кольцевых протоколов, использующийся для исключения образования колец в топологии, таких как протоколы ERPS и Spanning Tree.

1. Выберите «Monitor» - «Loop Protection» в дереве навигации для перехода на страницу состояния «Loop Protection», как показано на Рисунке 8.
2. Страница отображает статус включенных протоколов ERPS и Spanning Tree.
3. Нажмите кнопку «ERPS Configuration» или «Spanning Tree Configuration» для перехода в режим настройки параметров соответствующего протокола.

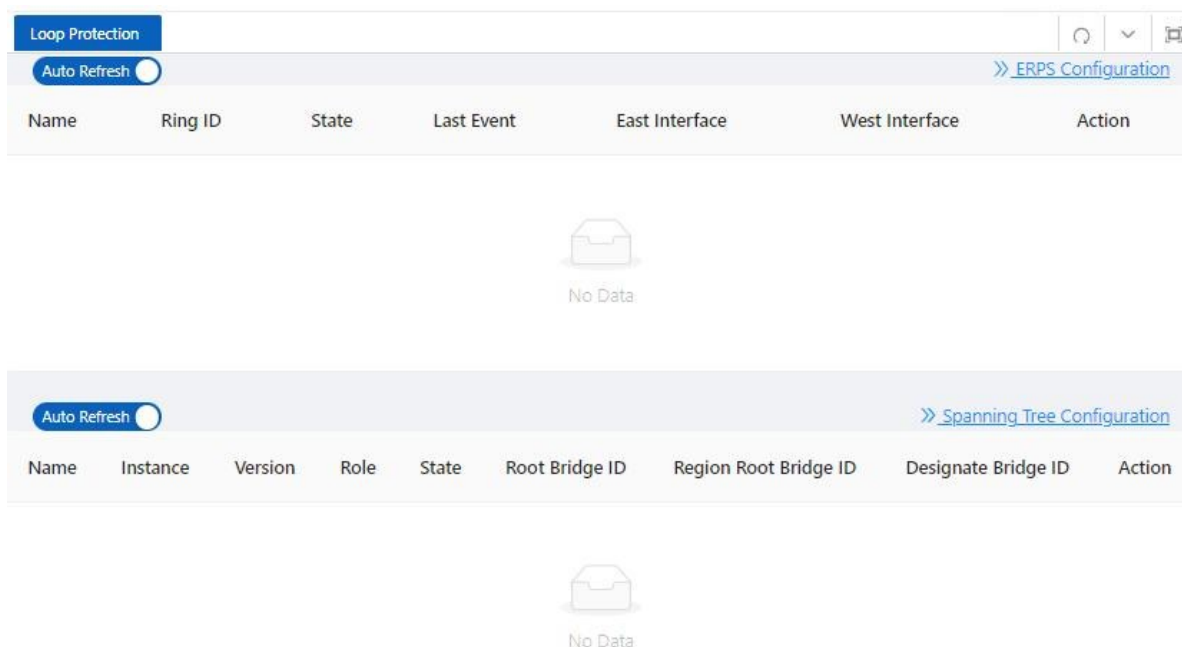


Рисунок 8 – Страница Loop Protection

2.4. Serial Server State

Страница «Serial Server State» используется для отображения состояния последовательного сервера.

1. Выберите «Monitor» - «Serial Server State» в дереве навигации для перехода на страницу состояния «Serial Server State», как показано на Рисунке 9.
2. Страница отображает статус состояния последовательного сервера.
3. Нажмите кнопку «Configuration» для перехода в режим настройки параметров соответствующего интерфейса.

Serial Server										
Statistics										
Auto Refresh										
ID	Net Octets Rx	Net Packets Rx	Net Octets Tx	Net Packets Tx	Serial Octets Rx	Serial Packets Rx	Serial Octets Tx	Serial Packets Tx	Net Connect Up/Down times	Serial Overload Drop Packets
1	0	0	0	0	0	0	0	0	0	0

Рисунок 9 – Страница Serial Server State

Элемент	Описание
ID	Идентификатор последовательного порта сервера
Net Octets Rx	Количество полученных байт, сеть
Net Packets Rx	Количество полученных пакетов, сеть
Net Octets Tx	Количество отправленных байт, сеть
Net Packets Tx	Количество отправленных пакетов, сеть
Serial Octets Rx	Количество полученных байт, последовательный порт
Serial Packets Rx	Количество полученных пакетов, последовательный порт
Serial Octets Tx	Количество отправленных байт, последовательный порт
Serial Packets Tx	Количество отправленных пакетов, последовательный порт
Net Connect Up/Down times	Количество сетевых подключений
Serial Overload Drop Packets	Количество пакетов, отброшенных из-за переполнения последовательного порта

2.5. Security

Страница «Security» используется для отображения состояния протоколов, связанных с безопасностью устройства, и состоит из трех частей: Port security, IP Source Guard и MAC authentication.

1. Выберите «Monitor» - «Security» в дереве навигации для перехода на страницу состояния «Security», как показано на Рисунке 10, 11, 12.

Port Security

Port State

Auto Refresh

[» Port Configuration](#)

Name	Total MAC Number	Configure MAC Number	Violation Count	Last Violate MAC	Last Violate Stamp
 No Data					

MAC State

MAC State

Auto Refresh

[» MAC Configuration](#)

Interface	VID	MAC Address	Type	Age Time Left(s)
 No Data				

Рисунок 10 - Страница состояния Port Security

IP Source Guard

User State

Auto Refresh

[» User Configuration](#)

Interface	Type	Filter	IP Address	MAC Address	VID
 No Data					

Рисунок 11 - Страница состояния IP Source Guard

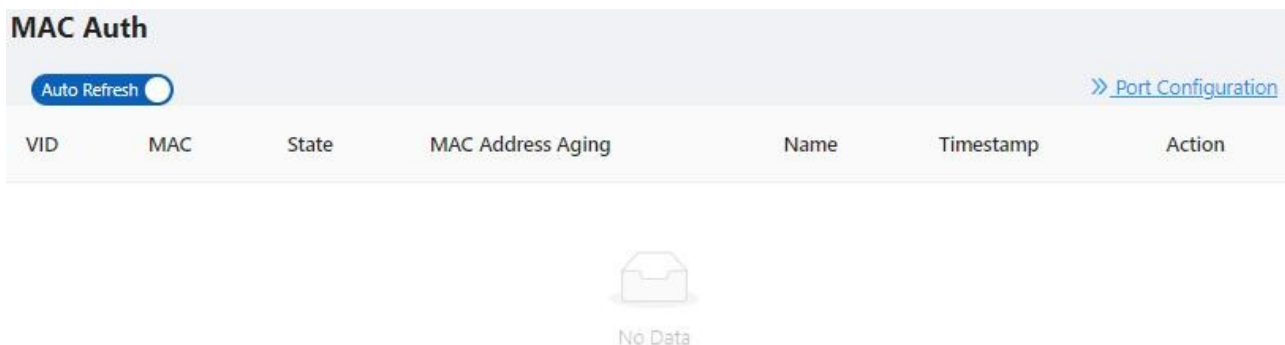


Рисунок 12 – Страница состояния MAC-аутентификации

2. На этой странице отображается состояние ERPS, Spanning tree, IP Source Guard и MAC authentication, для настройки соответствующего протокола безопасности нажмите кнопку «Configuration» для перехода в режим настройки параметров соответствующего протокола безопасности.

2.6. PoE State

Страница «PoE State» используется для отображения текущего состояния PoE устройства.

1. Выберите «Monitor» - «PoE State» в дереве навигации для перехода на страницу состояния «PoE State», как показано на Рисунке 13.

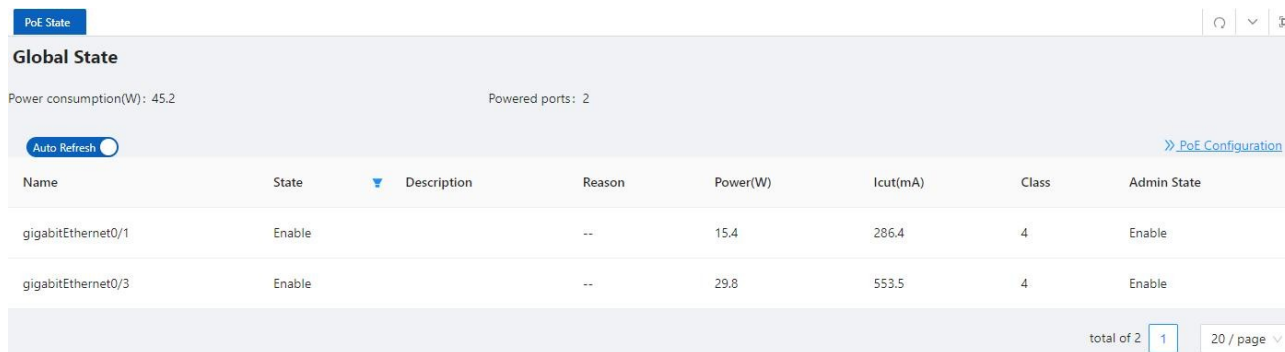


Рисунок 13 – Страница PoE State

2. На текущей странице отображена детальная информация о состоянии PoE питания устройств, описание параметров приведены в таблице ниже.

Элемент		Описание
Global state	Power Consumption (W)	Текущее потребление PoE
	Powered ports	Текущее общее количество включенных портов с PoE
Port	Name	Номер задействованного порта
	State	Текущее состояние PoE на порту: Disable: питание по PoE выключено Enable: питание по PoE включено
	Description	Описание порта
	Reason	Причина, по которой порт не может подавать питание. Short: короткое замыкание Management: недостаточная мощность
	Power(W)	Мощность, потребляемая текущим портом
	Icut(mA)	Рабочий ток текущего порта
	Class	Класс устройства PD, подключенного к этому порту
	Admin State	Отображает включена или отключена функция PoE этого порта

2.7. LLDP State

Страница «LLDP State» используется для отображения текущего состояния LLDP устройства.

1. Выберите «Monitor» - «LLDP State» в дереве навигации для перехода на страницу состояния «LLDP», как показано на Рисунке 14.
2. На странице отображен текущий статус включенного протокола LLDP, описание отображаемых элементов описаны в разделе настройки протокола LLDP.
3. Нажмите кнопку «LLDP Configuration» для перехода в режим настройки параметров LLDP.

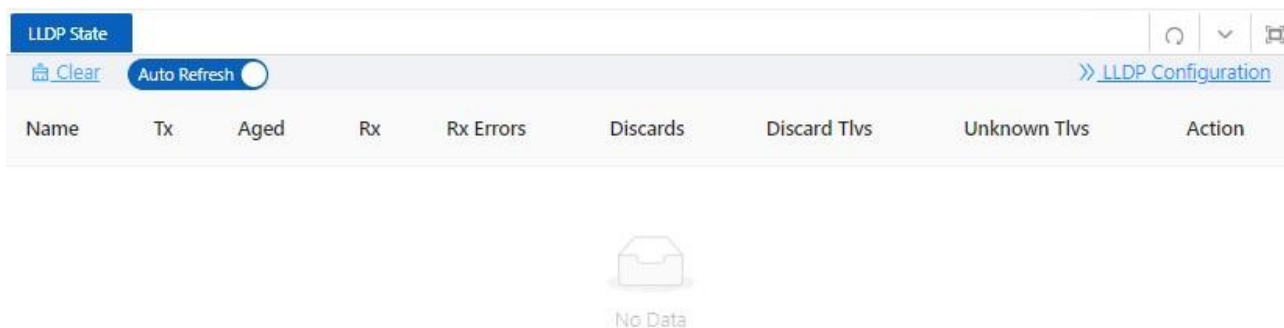


Рисунок 14 - Страница состояния LLDP

2.8. IGMP Snooping State

Страница «IGMP Snooping State» используется для отображения текущего состояния протокола IGMP Snooping.

1. Выберите «Monitor» - «IGMP Snooping State» в дереве навигации для перехода на страницу состояния «IGMP Snooping State», как показано на Рисунке 15.
2. На странице отображен текущий статус включенного протокола IGMP Snooping, описание отображаемых элементов описаны в разделе настройки протокола IGMP Snooping.
3. Нажмите кнопку «IGMP Snooping Configuration» для перехода в режим настройки параметров IGMP Snooping.

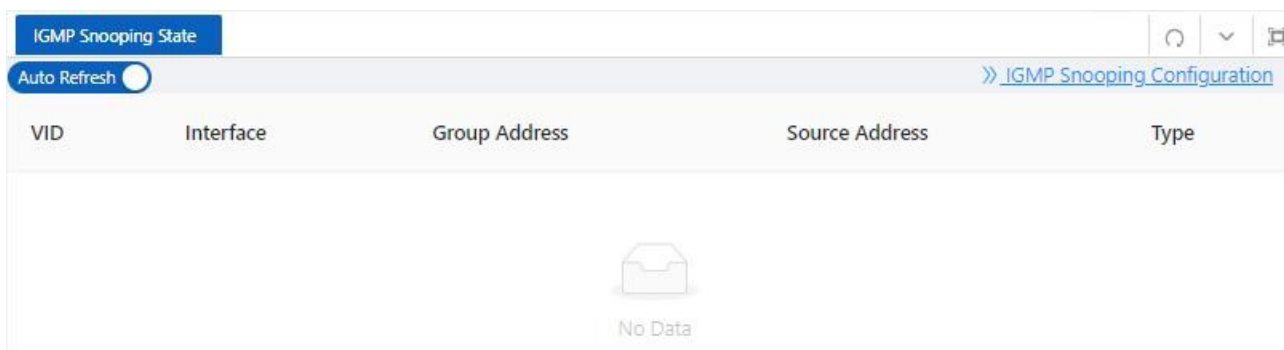


Рисунок 15 – Страница состояния IGMP Snooping

2.9. DHCP Snooping State

Страница «DHCP Snooping State» используется для отображения текущего состояния протокола DHCP Snooping.

1. Выберите «Monitor» - «DHCP Snooping State» в дереве навигации для перехода на страницу состояния «DHCP Snooping State», как показано на Рисунке 16.

2. На странице отображен текущий статус включенного протокола DHCP Snooping, описание отображаемых элементов описаны в разделе настройки протокола DHCP Snooping.
3. Нажмите кнопку «DHCP Snooping Configuration» для перехода в режим настройки параметров DHCP Snooping.

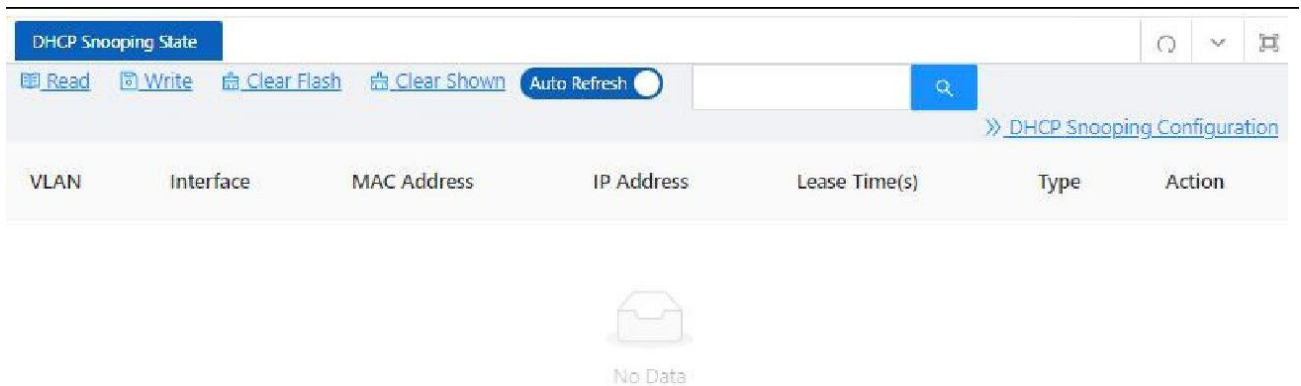


Рисунок 16 – Страница состояния DHCP Snooping

2.10.QinQ Information

Страница «QinQ Information» используется для отображения текущего состояния QinQ.

1. Выберите «Monitor» - «QinQ Information» в дереве навигации для перехода на страницу состояния «QinQ Information», как показано на Рисунке 17.
2. На странице отображен текущий статус включенного QinQ, описание отображаемых элементов описаны в разделе настройки QinQ.
3. Нажмите кнопку «QinQ Configuration» для перехода в режим настройки параметров QinQ.

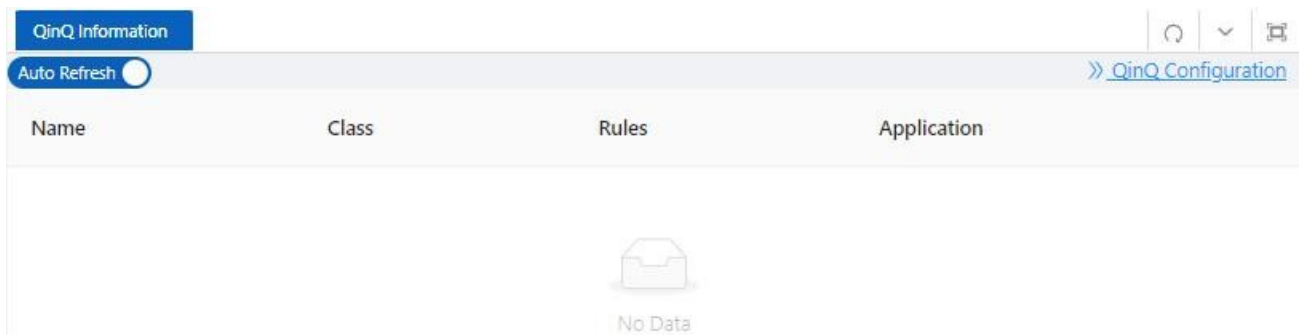


Рисунок 17 – Страница состояния QinQ

3. Configuration

3.1. VLAN

3.1.1. Введение

Ethernet – семейство технологий пакетной передачи данных между устройствами для компьютерных и промышленных сетей. Это самый распространенный протокол в мире, используемый для построения локальных сетей (LAN) и городских сетей (MAN). Протоколы Ethernet работают на физическом уровне модели OSI, предоставляя средства для передачи данных между устройствами.

Поскольку в Ethernet распространены коллизии и широковещательный трафик, для решения этой проблемы была введена виртуальная локальная сеть (VLAN). Идея состоит в том, чтобы разбить локальную сеть на отдельные VLAN, то есть широковещательные домены уровня 2. Таким образом каждый порт имеет PVID (port vlan identifier). Этот трафик может в дальнейшем проходить через другие порты коммутаторов, которые находятся в этом VLAN и не пройдут через все остальные порты. В итоге, создается изолированная среда (подсеть), которая без дополнительного устройства (маршрутизатора) не может взаимодействовать с другими подсетями, как показано на Рисунке 18.

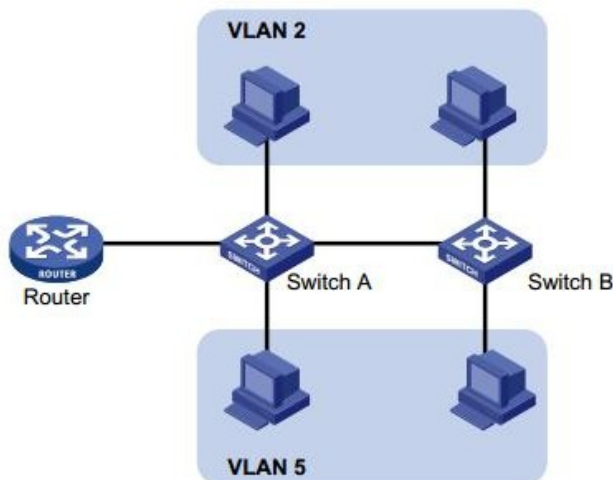


Рисунок 18 - Схема VLAN

VLAN предоставляет возможность построения сети, логическая структура которой не зависит от физической. То есть, топология сети на канальном уровне строится независимо от географического расположения составляющих компонентов сети.

Технология VLAN обеспечивает следующие преимущества:

- Ограничение широковещательного трафика внутри отдельных VLAN. Это уменьшает потери пропускной способности и повышает производительность сети;

- Улучшение безопасности локальной сети. Назначая группы пользователей разным VLAN, вы можете изолировать их на уровне 2. Для связи хостов в разных VLAN необходимы маршрутизаторы или коммутаторы уровня 3;
- Гибкое создание виртуальных рабочих групп. Поскольку пользователи из одной рабочей группы могут быть назначены в одну и ту же VLAN независимо от их физического местоположения, построение и обслуживание сети становится более гибким и простым.

Типы VLAN:

- VLAN на основе портов (Port-based VLAN) — каждый порт коммутатора назначается в определенную VLAN и любое сетевое устройство, подключенное в данный порт, будет находиться в назначенной виртуальной сети;
- VLAN на основе MAC-адресов (MAC-based VLAN) — членство в VLAN основывается на MAC-адресе рабочей станции. В этом случае на коммутаторе необходимо создать привязку MAC-адресов всех устройств к VLAN;
- VLAN на основе портов и протоколов IEEE 802.1v — тип протокола используется для определения членства в VLAN;
- VLAN на основе стандарта IEEE 802.1Q — поле принадлежности VLAN, интегрируется в структуру кадра Ethernet, что позволяет передавать данную информацию по сети. Преимуществом является гибкость настройки, использование не только на одном коммутаторе, но и в пределах всей коммутируемой сети; возможность использования оборудования разных производителей при организации сети. Данный тип VLAN используется чаще остальных.

Поскольку в веб-интерфейсе доступна только конфигурация VLAN на основе портов, в этой главе будет рассмотрен VLAN на основе портов.

3.1.1.1. VLAN Mode

В зависимости от режима обработки тегов режим VLAN порта может быть одним из следующих трех:

- **Access:**

Порт, находящийся в определенном VLAN и передающий не тегированные кадры. Как правило, это порт, смотрящий на пользовательское устройство.

- **Trunk:**

Порт, передающий тегированный трафик. Как правило, этот порт поднимается между сетевыми устройствами.

- **Hybrid:**

Порт может объединять несколько VLAN для получения и отправки трафика для них. Он может подключаться как к пользовательскому устройству, так и к сетевому устройству.

Гибридный порт отличается от магистрального порта тем, что позволяет трафику нескольких VLAN проходить без тегов, в отличие от магистрального порта, который пропускает без тегов только трафик VLAN по умолчанию.

3.1.1.2. Port link type

По умолчанию VLAN 1 является VLAN по умолчанию для всех портов. Однако при необходимости вы можете изменить VLAN по умолчанию для порта. При этом следуйте следующим рекомендациям:

- Поскольку Access порт может присоединяться только к одной VLAN, его VLAN по умолчанию — это VLAN, которому он принадлежит, и его нельзя настроить;
- Поскольку магистральный или гибридный порт может присоединяться к нескольким VLAN, вы можете настроить для этого порта VLAN по умолчанию.

3.1.1.3. Frame handling methods

Порт, настроенный с использованием VLAN по умолчанию, обрабатывает кадр следующим образом:

Тип порта	Действие (входящий кадр)		Действие (исходящий кадр)
	Untagged frame	Tagged frame	
Access	Помечает кадр тегом VLAN по умолчанию	• Получает кадр, если его VLAN ID совпадает с VLAN ID по умолчанию • Отбрасывает кадр, если его VLAN ID отличается от VLAN ID по умолчанию	Удаляет тег VLAN по умолчанию и отправляет кадр
Trunk	Проверяет, используется ли на порту VLAN по умолчанию: • Если да, помечает кадр тегом VLAN по умолчанию • Если нет, отбрасывает кадр	• Получает кадр, если его VLAN передается через порт • Отбрасывает кадр, если его VLAN не передается через порт	• Удаляет тег и отправляет кадр, если кадр содержит тег VLAN по умолчанию • Отправляет кадр не удаляя тег, если его VLAN передается на порт, но отличается от сети по умолчанию

Hybrid			Отправляет кадр, если его VLAN передается через порт. Кадр отправляется с удаленным или неизменным тегом VLAN в зависимости от вашей конфигурации
--------	--	--	---

3.1.2. Конфигурация VLAN

3.1.2.1. Создание VLAN

Выберите «Configuration» - «VLAN» в дереве навигации для перехода на страницу VLAN, как показано на Рисунке 19.

VLAN Configuration

[+ Add](#)
[X Delete](#)

☐	ID	Name	Type	Member	Action
☐	1	default	Static	gigabitEthernet0/1, gigabitEthernet0/2, gigabitEthernet0/3, gigabitEthernet0/4, gigabitEthernet0/5, gigabitEthernet0/6, gigabitEthernet0/7, gigabitEthernet0/8, gigabitEthernet0/9, gigabitEthernet0/10	Edit

Рисунок 19 - Страница конфигурации VLAN

Элемент	Описание
ID	Идентификатор VLAN
Name	Описания VLAN
Members	Указывает, что порт отправляет трафик VLAN без удаления тега VLAN
Edit	Редактирование VLAN
Add	Добавление VLAN
Delete	Удаление выбранного VLAN

Нажмите кнопку «Add», чтобы перейти на страницу создания VLAN, как показано на Рисунке 20.

Введите номер VLAN в поле ID, выберите тегированных участников на панели портов, которым будет назначен этот VLAN ID.

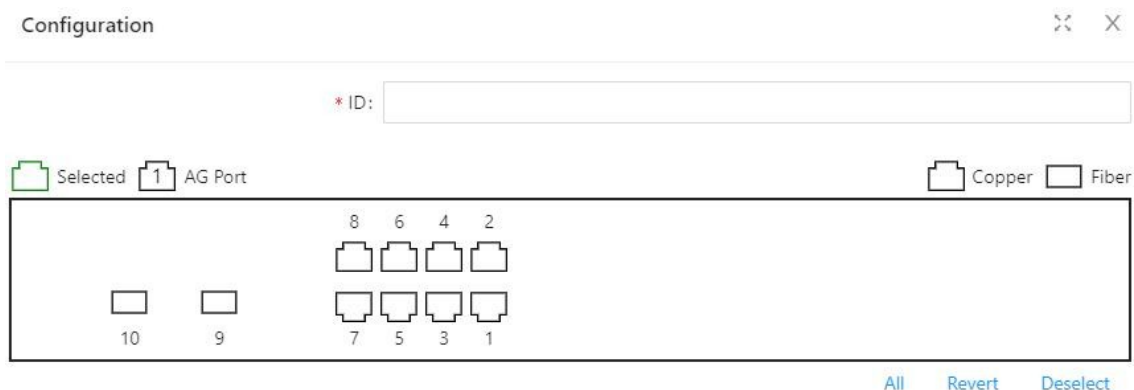


Рисунок 20 - Создание VLAN

Нажмите кнопку «Save» во вспомогательной области инструментов, чтобы сохранить конфигурацию.

3.1.2.2. Конфигурация Trunk порта

Выберите «Configuration» - «VLAN» в дереве навигации для перехода на страницу VLAN, как показано на Рисунке 21.

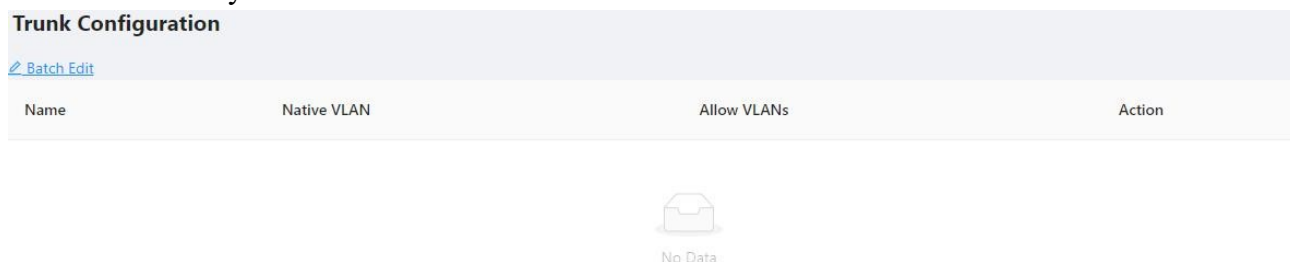


Рисунок 21 - Страница конфигурации Trunk порта

Нажмите кнопку «Batch Edit» под «Trunk Configuration», чтобы перейти на страницу конфигурации trunk, как показано на Рисунке.22.

Элемент		Описание
Mode	Access	Режим VLAN порта access
	Trunk	Режим VLAN порта trunk
PVID		VLAN ID порта по умолчанию, который существует только в режиме access. Trunk порты на двух концах канала должны иметь одинаковый PVID. В противном случае канал не сможет правильно передавать пакеты
Native Vlan		VLAN (Native Vlan) существует только в режиме trunk
Allow VLANs		Разрешенные VLAN к передаче через порт

Configuration

* Mode:

Access

Trunk

* PVID/Native VLAN:

1

* Allow VLANs:

all

Selected

1

AG Port

Copper

Fiber

10

9

8

6

4

2

7

5

3

1

All

Revert

Deselect

Рисунок 22 - Страница конфигурации интерфейса

Выберите режим VLAN, введите номер VLAN в поле PVID и Allow VLANs, нажмите кнопку «OK», чтобы завершить настройку. Нажмите кнопку «Save» во вспомогательной области инструментов, чтобы сохранить конфигурацию.

3.2. Port

3.2.1. Port Configuration

Вы можете использовать функцию управления интерфейсом для просмотра информации об интерфейсе, создания/удаления логических интерфейсов, изменения состояния интерфейса и сброса параметров интерфейса, как показано на Рисунке 23.

L2 Port

[Batch Edit](#)
[Port Statistics](#)

Name	Admin State	Port Mode	PVID/Native VLAN	Allow VLANs	Speed	Duplex/Auto-Neg	Flow Control	MTU	Description	Action
gigabitEthernet0/1	No shutdown	Access	1		AUTO	AUTO	OFF	1500		Edit
gigabitEthernet0/2	No shutdown	Access	1		AUTO	AUTO	OFF	1500		Edit
gigabitEthernet0/3	No shutdown	Access	1		AUTO	AUTO	OFF	1500		Edit
gigabitEthernet0/4	No shutdown	Access	1		AUTO	AUTO	OFF	1500		Edit

Рисунок 23 - Страница конфигурации порта

Конфигурация интерфейса:

1. Выберите «Configuration» - «Port» - «Port Configuration» в дереве навигации для перехода на страницу конфигурации порта, как показано на Рисунке 23.
2. Выберите порты для настройки, нажмите кнопку «Edit», чтобы перейти на страницу настройки интерфейса, как показано на Рисунке 24.

Port Configuration

✕
✕

* Admin State:

No Change
Shutdown
No shutdown

Description:

* Port Mode:

No Change
Access
Trunk

* PVID/Native VLAN:

1

Advanced Setting

* Media Type:

No Change
RJ45

* Speed:

No Change
AUTO
10M
100M
1000M

* Duplex:

No Change
AUTO
FULL
HALF

* Flow Control:

No Change
ON
OFF

* MTU:

1500

Рисунок 24 - Страница конфигурации порта

Элемент	Описание
Admin State	Выключение/включение порта
Description	Описание логического интерфейса
Port Mode	Режим VLAN порта, access или trunk
PVID/Native VLAN	PVID или Native VLAN порта
Media type	Тип комбинированных портов: - RJ45: режим порта 10/100/1000BASE-T. - SFP: режим порта 1000BASE-X. Примечание: только для комбинированных портов
Speed (copper)	Скорость передачи порта: 10: 10 Мбит/с. 100M: 100 Мбит/с. 1000M: 1000 Мбит/с. - Авто: автосогласование.

	Примечание: только для медных портов
Duplex (copper)	Дуплексный режим порта: • ABTO: автосогласование. • FULL: полнодуплексный режим. • HALF: полудуплекс. Примечание: только для медных портов
Speed (fiber)	Режим порта: • 100BASE-FX: режим порта — 100BASE-FX. • 1000BASE-X: режим порта — 1000BASE-X. • 2500BASE-X: режим порта — 2,5G BASE-X. • 10G BASE-X: режим порта — 10G BASE-X. Примечание: только для оптоволоконных портов
Autoneg (fiber)	Включает или отключает автосогласование порта. Функцию автосогласования необходимо включать или отключать одновременно на двух концах канала, иначе произойдет сбой канала. Примечание: только для оптических портов
Flow control	Включает или отключает управление потоком порта
MTU	Разрешает или запрещает прохождение больших кадров через порт. Длина пакетов по умолчанию составляет 46–1500 байт
Admin Shutdown	Выключение/включение порта

3.2.2. Port Extension

3.2.2.1. Rate Limiting

Ограничение скорости на основе порта позволяет ограничить скорость, с которой сетевой трафик отправляется или принимается устройством, подключенным к порту вашего коммутатора. В отличие от качества обслуживания (QoS) 802.1p, ограничение скорости на основе порта не определяет приоритет информации в зависимости от типа. Ограничение скорости просто означает, что коммутатор будет замедлять трафик на порту, чтобы он не превышал установленный вами предел. Если вы установите слишком низкое ограничение скорости для порта, вы можете столкнуться с ухудшением качества видеопотока, замедлением времени отклика во время онлайн-активности и другими проблемами.

Лучшее использование ограничения скорости — не допускать, чтобы устройства с низким приоритетом, подключенные к вашему коммутатору, использовали слишком большую часть вашей пропускной способности и замедляли работу других подключенных устройств. Сочетание ограничения скорости и качества обслуживания может помочь вам максимизировать эффективность вашей сети и расставить приоритеты для устройств.

Конфигурация Port Ratelimit:

1. Выберите «Configuration» - «Port» - «Port Extension» - «Rate Limiting» в дереве навигации для перехода на страницу ограничения скорости порта, как показано на Рисунке 25.
2. Нажмите кнопку «Batch Edit» под «Rate Limiting», чтобы перейти на страницу настройки ограничения скорости, как показано на Рисунке 26.
3. Нажмите кнопку «OK».
4. Нажмите кнопку «Save» в вспомогательной области инструментов.

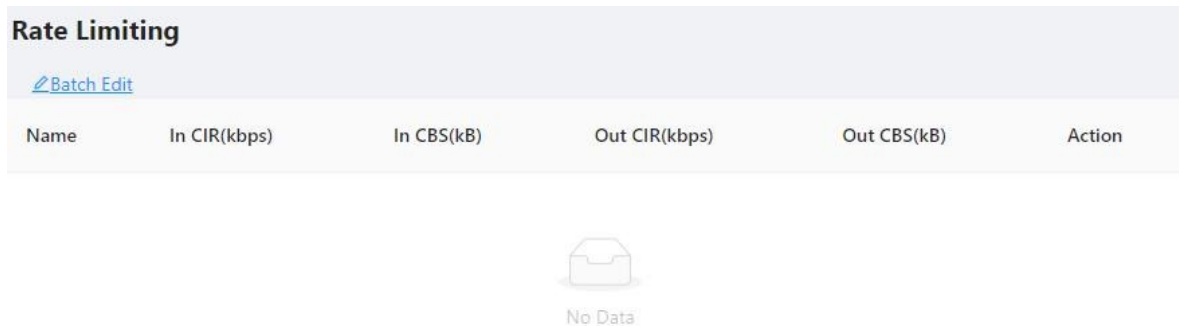


Рисунок 25 - Страница Port Ratelimit

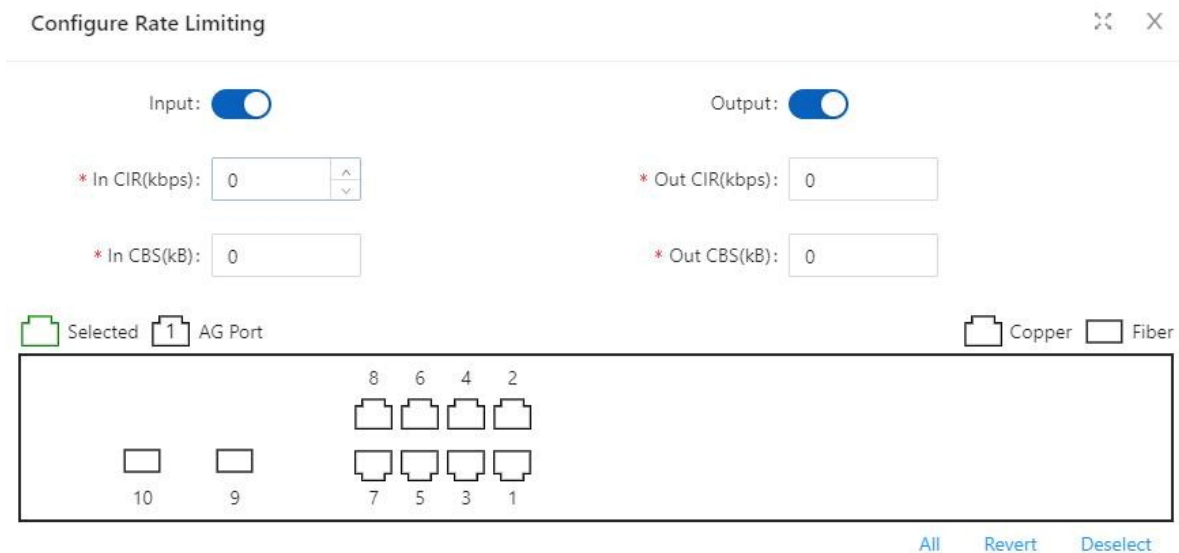


Рисунок 26 - Страница настройки Port Ratelimit

Элемент	Описание
In CIR (kbps)	Ограничение скорости во входящем направлении (Кбит)
In CBS (KB)	Размер пакета во входящем направлении (Кбит)
Out CIR (kbps)	Ограничение скорости в исходящем направлении (Кбит)
Out CBS (KB)	Размер пакета в исходящем направлении (Кбит)

3.2.2.2. Storm Control

Шторм трафика возникает, когда большое количество широковещательных, многоадресных или одноадресных пакетов перегружает сеть.

Вы можете использовать функцию подавления шторма, чтобы ограничить размер определенного типа трафика (широковещательного, многоадресного и неизвестного одноадресного трафика) для каждого интерфейса в представлении порта Ethernet или представлении группы портов.

В представлении интерфейса или группы портов вы устанавливаете максимальный широковещательный, многоадресный или неизвестный одноадресный трафик, разрешенный для прохождения через интерфейс или каждый интерфейс в группе портов. Когда широковещательный, многоадресный или неизвестный одноадресный трафик на интерфейсе превышает пороговое значение, система отбрасывает пакеты до тех пор, пока трафик не упадет ниже порогового значения.

Конфигурация Storm Control:

1. Выберите «Configuration» - «Port» - «Port Extension» - «Storm Control» в дереве навигации для перехода на страницу управления штормом, как показано на Рисунке 27.

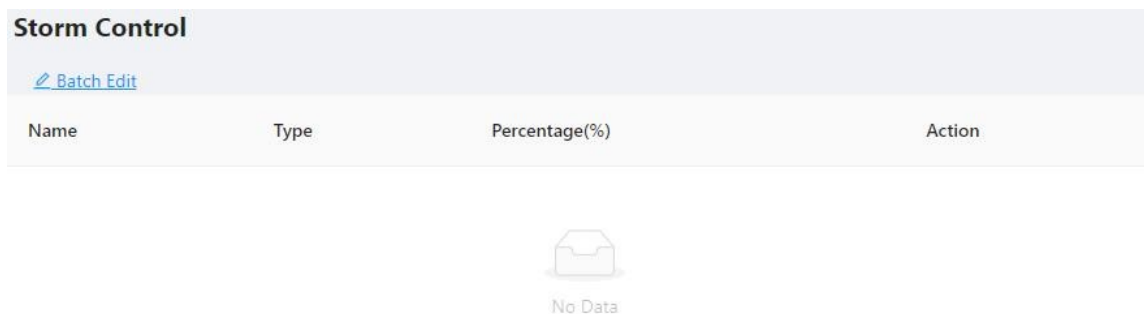


Рисунок 27 - Страница Storm Control

2. Выберите тип, введите в поле «Percentage» требуемое значение, выберите порты для настройки на панели портов, как показано на Рисунке 28.
3. Нажмите кнопку «OK».
4. Нажмите кнопку «Save» в вспомогательной области инструментов.

Configure Storm Control

* Type:

Disabled

Broadcast

Multicast

Unicast

Multicast+Broadcast

Unicast+Broadcast

All

* Percentage(%):

Selected

1 AG Port

Copper

Fiber

10

9

8

6

4

2

7

5

3

1

All

Revert

Deselect

Рисунок 28 - Страница настройки Storm Control

Элемент		Описание
Type	Disabled	Отключение контроля шторма
	Broadcast	Параметр, используемый при подавлении широковещательной рассылки
	Multicast	Параметр, используемый при подавлении многоадресной рассылки
	Unicast	Параметр, используемый при подавлении одноадресной рассылки
	multicast-broadcast	Параметр, используемый при подавлении многоадресной и широковещательной рассылки
	unicast-broadcast	Параметр, используемый при подавлении одноадресной и широковещательной передаче
	All	Параметр, используемый при подавлении в одноадресной, многоадресной, широковещательной рассылке
Percentage (%)		Максимальный процент трафика от общей пропускной способности интерфейса Ethernet

3.2.2.3. Isolation

Изоляция - это независимый функционал, который ограничивает передачу пакетов между определенными портами. Коммутаторы поддерживают как полную изоляцию трафика между портами, так и изоляцию трафика в рамках определенного VLAN. Настройка функционала сводится к добавлению Ethernet интерфейсов в одну или несколько групп.

Порты внутри одной группы изолируются, то есть трафик между ними не передается.

Порты, принадлежащие разным группам или не добавленные ни в одну группу, могут коммутировать пакеты между собой. Изоляция портов внутри VLAN выполняется аналогично, только применяется к трафику в данном VLAN.

Конфигурация Isolation Group:

1. Выберите «Configuration» - «Port» - «Port Extension» - «Isolation» в дереве навигации для перехода на страницу изоляции порта, как показано на Рисунке 29.
2. Выберите порт, который необходимо изолировать, нажмите кнопку «ОК».
3. Нажмите кнопку «Save» в вспомогательной области инструментов.

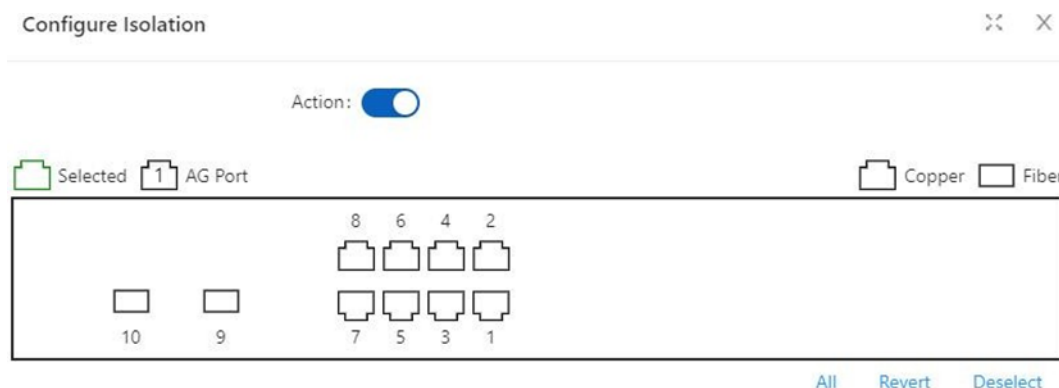


Рисунок 29 – Страница Port Isolate

3.2.3. Port Mirroring

Зеркалирование портов заключается в копировании пакетов, проходящих через один или несколько портов (называемых исходным интерфейсом), в порт (называемый интерфейсом назначения) на локальном устройстве. Исходный интерфейс подключен к устройству мониторинга. Анализируя на устройстве мониторинга пакеты, зеркально отраженные на интерфейсе назначения, вы можете отслеживать сеть и устранять возможные сетевые проблемы.

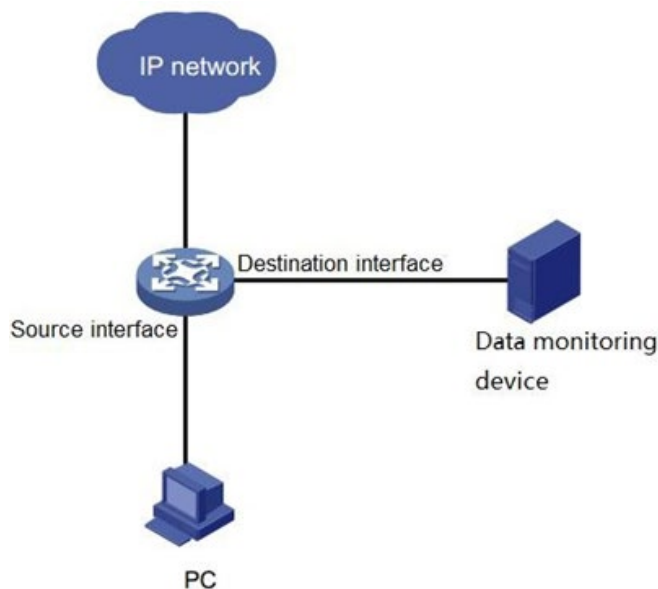


Рисунок 30 - Реализация зеркалирования портов

Создание группы зеркалирования:

1. Выберите «Configuration» - «Port» - «Port Mirror» в дереве навигации для перехода на страницу зеркалирования порта, как показано на Рисунке 31.

Port Mirroring			
ID	Destination Interface	Source Interfaces	Action
1			Edit Delete
2			Edit Delete
3			Edit Delete

Рисунок 31 - Страница Port Mirroring

2. Нажмите кнопку «Edit» для соответствующего идентификатора и выберите интерфейс назначения или интерфейс источника, как показано на Рисунке 32.

Элемент	Описание
Session	Идентификатор создаваемой группы зеркалирования
Destination Interface	Интерфейс назначения трафика зеркала для сессии, может быть только один
Source Interface	Интерфейс источника трафика зеркала для сессии, их может быть более одного

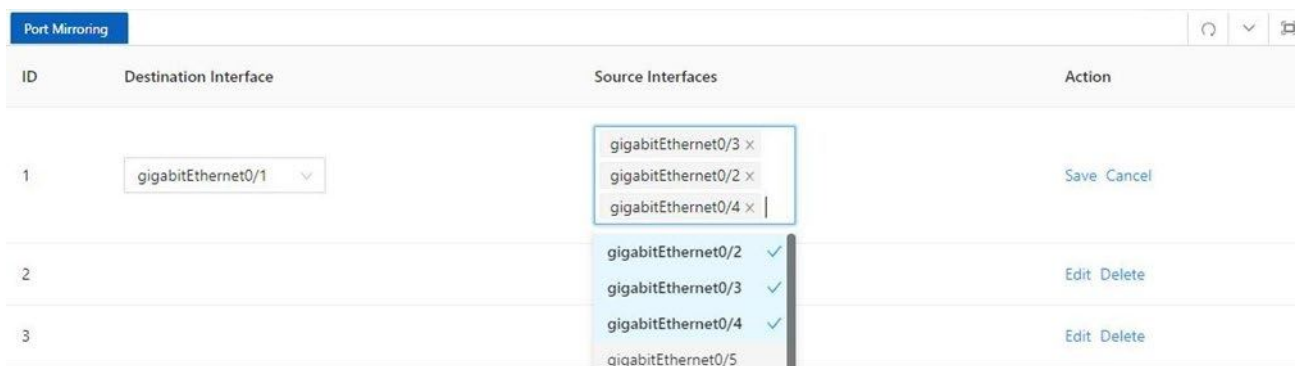


Рисунок 32 - Страница создания группы зеркалирования

3. Нажмите кнопку «Save» для соответствующего идентификатора.
4. Нажмите кнопку «OK».
5. Нажмите кнопку «Save» в вспомогательной области инструментов.

3.2.4. Port Aggregation

3.2.4.1. Введение

Link Aggregation.

Агрегирование портов - это процесс объединения нескольких портов с одинаковой конфигурацией и для использования их логически в качестве одного физического порта (Port-Channel), что позволяет суммировать полосу пропускания в одном логическом линке и использовать резервирование, как показано на Рисунке 33.

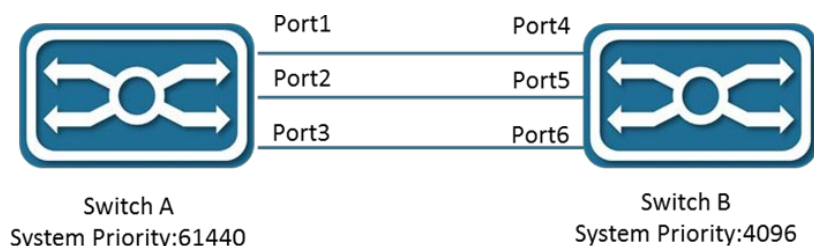


Рисунок 33 – Схема агрегирования портов

LACP.

LACP (Link Aggregation Control Protocol) - протокол управления агрегацией каналов IEEE 802.3ad. (LACP) обеспечивает динамическое агрегирование физических каналов и использует LACPDU сообщения для обмена информацией с соседней стороной.

После включения LACP порт посылает LACPDU, уведомляя ответную сторону о приоритете и MAC адресе системы, приоритете и адресе порта, и ключе операции. Когда ответный порт получает эту информацию, он сравнивает её с информацией о своих портах, настроенных на агрегацию. Таким образом обе стороны достигают соглашения о включении или исключении порта из динамической группы агрегации.

В динамической группе агрегации порты имеют 2 статуса - выбранный (selected) и в ожидании (standby). Порты могут посылать и принимать LACPDU находясь в любом статусе, но в статусе standby порт не может передавать данные.

3.2.4.2. Конфигурация Aggregation Group

Конфигурация Aggregation Group:

1. Выберите «Configuration» - «Port» - «Port Aggregation» в дереве навигации для перехода на страницу агрегации каналов, как показано на Рисунке 34.

Рисунок 34 – Страница Global Configuration

Элемент	Описание	
Load balancing method	dst-mac	Выравнивание в соответствии с MAC-адресом назначения
	src-mac	Выравнивание в соответствии с MAC-адресом источника
	src-dst-mac	Выравнивание в соответствии с MAC-адресом назначения и MAC-адресом источника
	dst-ip	Выравнивание в соответствии с IP-адресом назначения
	srt-ip	Выравнивание в соответствии с IP-адресом источника
	src-dst-ip	Выравнивание в соответствии с IP-адресом назначения и IP-адресом источника
	dst-port	Выравнивание в соответствии с номером порта назначения TCP/UDP L4
	src-port	Выравнивание в соответствии с номером порта источника TCP/UDP L4
	src-dst-port	Выравнивание в соответствии с номером порта назначения и источника TCP/UDP L4

2. На странице «Aggregation ports» нажмите кнопку «+Add», чтобы перейти на страницу конфигурации портов, как показано на Рисунке 35.

Элемент	Описание		
Port configuration	ID	Идентификатор участника агрегации	
	Type	Manual	Ручной режим
		Active	В этом режиме порты через регулярные промежутки времени отправляют пакеты LACP на ответные порты
		Passive	В этом режиме порты не отправляют пакеты LACP до тех пор, пока ответный порт не отправит пакеты LACP. После получения пакетов LACP от ответного порта, порты отправляют пакеты LACP на ответный порт

Port Configuration ✕ ✕

* Type: **Manual** Active Passive

* ID: 1

☒ Selected ☐ 1 AG Port ☐ Copper ☐ Fiber

10 9

8 6 4 2

7 5 3 1

[All](#) [Revert](#) [Deselect](#)

Рисунок 35 – Страница Aggregation port configuration

3. Выберите тип агрегации и порты на панели портов, введите значение в поле «ID», нажмите кнопку «ОК».
4. После завершения настройки созданный порт агрегации отображается на странице «Aggregation Port», как показано на Рисунке 36.

Aggregate Ports				
+Add				
ID	Name	Type	Member	Action
1	po1	Manual	gigabitEthernet0/3, gigabitEthernet0/4	Edit Delete

Рисунок 36 – Страница Aggregation port

Элемент	Описание	
Aggregation port	ID	Идентификатор порта агрегации
	Name	Имя порта агрегации
	Type	Режим порта агрегации
	Member	Порты-члены агрегации

3.3. Spanning Tree

3.3.1. Введение

Spanning Tree Protocol (STP) — канальный протокол. Основной задачей STP является устранение петель в топологии произвольной сети Ethernet, в которой есть один или более сетевых мостов, связанных избыточными соединениями. STP решает эту задачу, автоматически блокируя соединения, которые в данный момент для полной связности коммутаторов являются избыточными.

Необходимость устранения топологических петель в сети Ethernet следует из того, что их наличие в реальной сети Ethernet с коммутатором с высокой вероятностью приводит к бесконечным повторам передачи одних и тех же кадров Ethernet одним и более коммутатором, отчего пропускная способность сети оказывается почти полностью занятой этими бесполезными повторами; в этих условиях, хотя формально сеть может продолжать работать, на практике её производительность становится настолько низкой, что может выглядеть как полный отказ сети.

STP относится ко второму уровню модели OSI. Протокол описан в стандарте IEEE 802.1D, выработанном рабочей группой IEEE 802.1 по межсетевому взаимодействию.

Если в сети с мостовыми подключениями (в сегменте сети из коммутаторов) имеется несколько путей, могут образоваться циклические маршруты, и следование простым правилам пересылки данных через мост (коммутатор) приведёт к тому, что один и тот же пакет будет бесконечно передаваться с одного моста на другой (передаваться по кольцу из коммутаторов).

Алгоритм связующего дерева позволяет по мере необходимости автоматически отключать передачу через мост (коммутатор) в отдельных портах (блокировать порты коммутатора), чтобы предотвратить заикливание в топологии маршрутов пересылки пакетов. Для использования алгоритма связующего дерева в сетевом мосте никакой дополнительной настройки не требуется.

Rapid STP (RSTP) является значительным усовершенствованием STP. В первую очередь необходимо отметить уменьшение времени сходимости и более высокую устойчивость. Rapid STP совместим с STP — если некое устройство использует STP, то RSTP тоже будет

использовать STP с этим устройством, но в этом режиме может оказаться, что наличие RSTP на остальных устройствах не дает преимуществ по сравнению с STP.

Multiple Spanning Tree Protocol (MSTP) является расширением протокола RSTP, который позволяет настраивать отдельное связующее дерево для любой VLAN или группы VLAN, создавая множество маршрутов передачи трафика и позволяя осуществлять балансировку нагрузки.

Протокол MSTP делит коммутируемую сеть на регионы MST (Multiple Spanning Tree (MST) Region), каждый из которых может содержать множество копий связующих деревьев (Multiple Spanning Tree Instance, MSTI) с независимой друг от друга топологией.

3.3.2. Конфигурация Spanning Tree

Конфигурация Spanning Tree:

Выберите «Configuration» - «Spanning Tree» - «Global Configuration» в дереве навигации для перехода на страницу глобальной конфигурации, как показано на Рисунке 37.

The screenshot shows the 'Spanning Tree' configuration page. At the top, there's a 'Spanning Tree' tab. Below it, the 'Global Configuration' section is active. The settings are as follows:

- Mode:** RSTP (dropdown menu)
- State:** Enabled (toggle switch)
- Priority:** 32768 (dropdown menu)
- Advanced Setting:** Link to expand more options
- Hello Time(s):** 2 (input field)
- Error Disable Timeout:** Enabled (toggle switch)
- Forward Delay(s):** 15 (input field)
- Transmit Hold Count:** 6 (input field)
- Error Disable Timeout Int:** 300 (input field)
- Max Age(s):** 20 (input field)
- Buttons:** Apply (with checkmark icon) and Reset (with trash icon)

Рисунок 37 – Страница Spanning Tree Global Configuration

Элемент	Описание	
Global Configuration	Mode	Режим STP включает STP/RSTP/MSTP STP: в режиме STP каждый порт устройства отправляет STP BPDU RSTP: в режиме RSTP каждый порт устройства будет отправлять RSTP BPDU. При подключении к устройству, работающему по протоколу STP, порт автоматически перейдет в режим STP MSTP: в режиме MSTP каждый порт устройства отправляет MSTP BPDU. При подключении к устройству, работающему по протоколу STP, порт автоматически перейдет в режим STP
	State	Включение STP

	Hello Time	Интервал Hello Time
	Priority	Приоритет моста
	Forward Delay	Время задержки перед изменением интерфейса на пересылку
	Transmit Hold Count	Максимальное количество BPDU, отправляемых мостом в секунду
	Max Age	Максимальная продолжительность хранения сообщений на устройстве
	Error Disable Timeout	Автоматическое отключения порта при ошибке конфигурации
	Error Disable Timeout Interval	Ошибка конфигурации: порт автоматически отключается по тайм-ауту

Конфигурация экземпляра:

Выберите «Configuration» - «Spanning Tree» - «Instance Configuration» в дереве навигации для перехода на страницу конфигурации экземпляра, как показано на Рисунке 38.

Instance Configuration

+Add			» Spanning Tree State
ID	VLAN List	Priority	Action



No Data

Рисунок 38 – Страница Spanning Tree Instance Configuration

Элемент	Описание	
Instance Configuration	ID	Идентификатор экземпляра
	VLAN List	Список VLAN связанных с экземпляром
	Priority	Приоритет моста
	Action	Удалить запись

Конфигурация порта:

Выберите «Configuration» - «Spanning Tree» - «Port Configuration» в дереве навигации для перехода на страницу конфигурации порта, как показано на Рисунке 39.

Port Configuration

[Batch Edit](#) [Spanning Tree State](#)

Name	State	Path Cost	Link Type	Root Guard	Auto Edge	Edge Port	Port Fast	BPDU Guard	BPDU Filter	Instance/Priority/TCN Restrict	Action
gigabitEthernet0/1	Enable	20000000	P2P	Disable	Disable	Disable	Disable	Default	Default	0 128 Disable	Edit
gigabitEthernet0/2	Enable	20000000	P2P	Disable	Disable	Disable	Disable	Default	Default	0 128 Disable	Edit

Рисунок 39 – Страница Spanning Tree Port Configuration

Элемент	Описание	
Port Configuration	Name	Имя интерфейса
	State	Статус STP
	Path Cost	Настройка стоимости пути интерфейса
	Link Type	Настройка типа подключенной к порту сети
	Root Guard	Настройка интерфейса для включения защиты от root
	Auto Edge	Настройка интерфейса для автоматического распознавания пограничного порта
	Edge Port	Настройте интерфейс как пограничный порт
	Port Fast	Настройте интерфейс как быстрый порт
	BPDU Filter	Настройка интерфейса для включения фильтрации BPDU
	BPDU Guard	Настройка интерфейса для включения защиты BPDU
	Instance/Priority/TCN restrict	Настройка экземпляра, приоритет и ограничение TCN

3.4. ERPS

3.4.1. Введение

ERPS (Ethernet Ring Protection Switching) - протокол, позволяющий осуществлять резервирование канала на втором уровне модели OSI путем физического создания петель и их логической блокировки, также известный как G.8032. Он оптимизирует механизм обнаружения петли и может определить двунаправленную/однонаправленную неисправность, поддерживает многокольцевую и многодоменную структуры. Время сходимости достигает 50 мс.

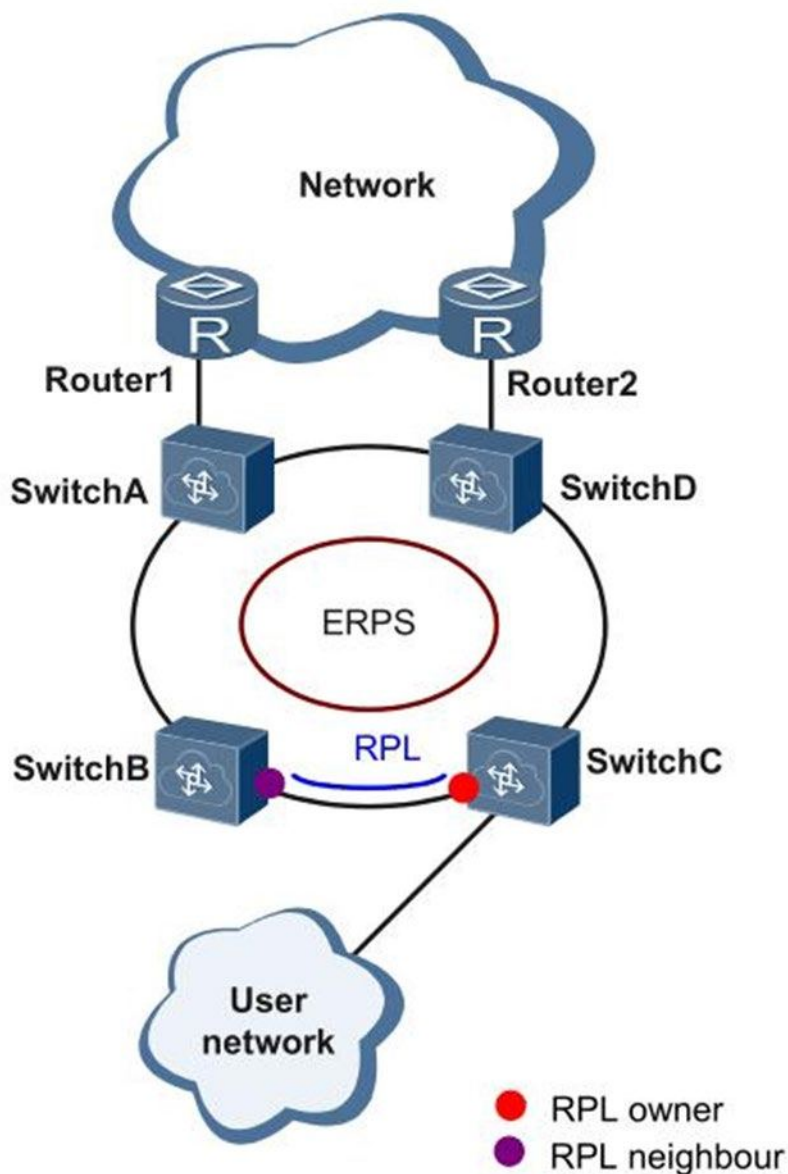


Рисунок 40 – Initial State

Initial State

Как показано на Рисунке 40, устройства на кольце настроены, и все соединения находятся в рабочем состоянии.

Интерфейс владельца RPL будет заблокирован протоколом ERPS для предотвращения петель. Если настроен соседний интерфейс RPL, он также будет заблокирован. Другие интерфейсы находятся в состоянии пересылки и могут пересылать трафик.

Link failure

При сбое канала между коммутаторами D и E два интерфейса на канале будут заблокированы протоколом ERPS, интерфейс владельца RPL будет перенаправлен, как показано на Рисунке 41.

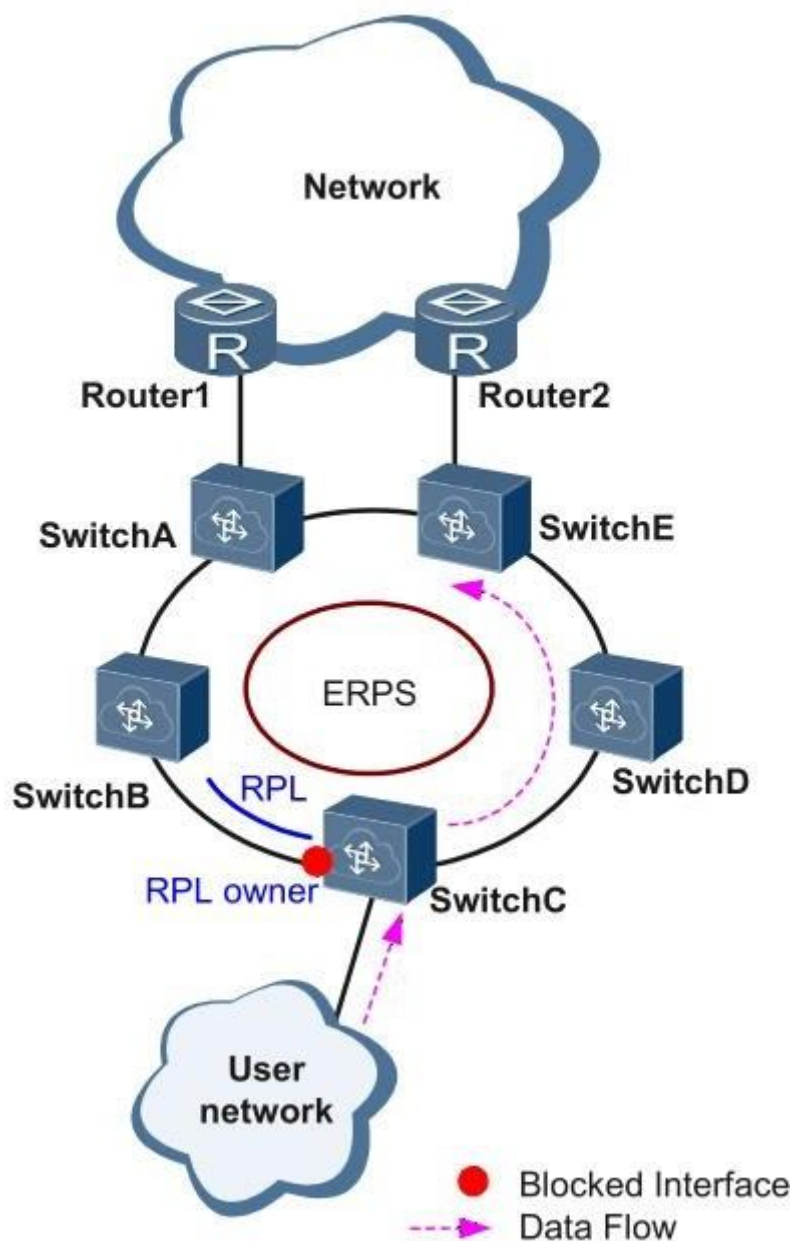


Рисунок 41 – Link failure

Link restores

При сбое, линк восстанавливается. Когда кольцо ERPS настроено на возвратный режим, интерфейс владельца RPL будет заблокирован протоколом ERPS, восстановленный канал будет настроен в состояние пересылки для пересылки трафика, как показано на Рисунке 42.

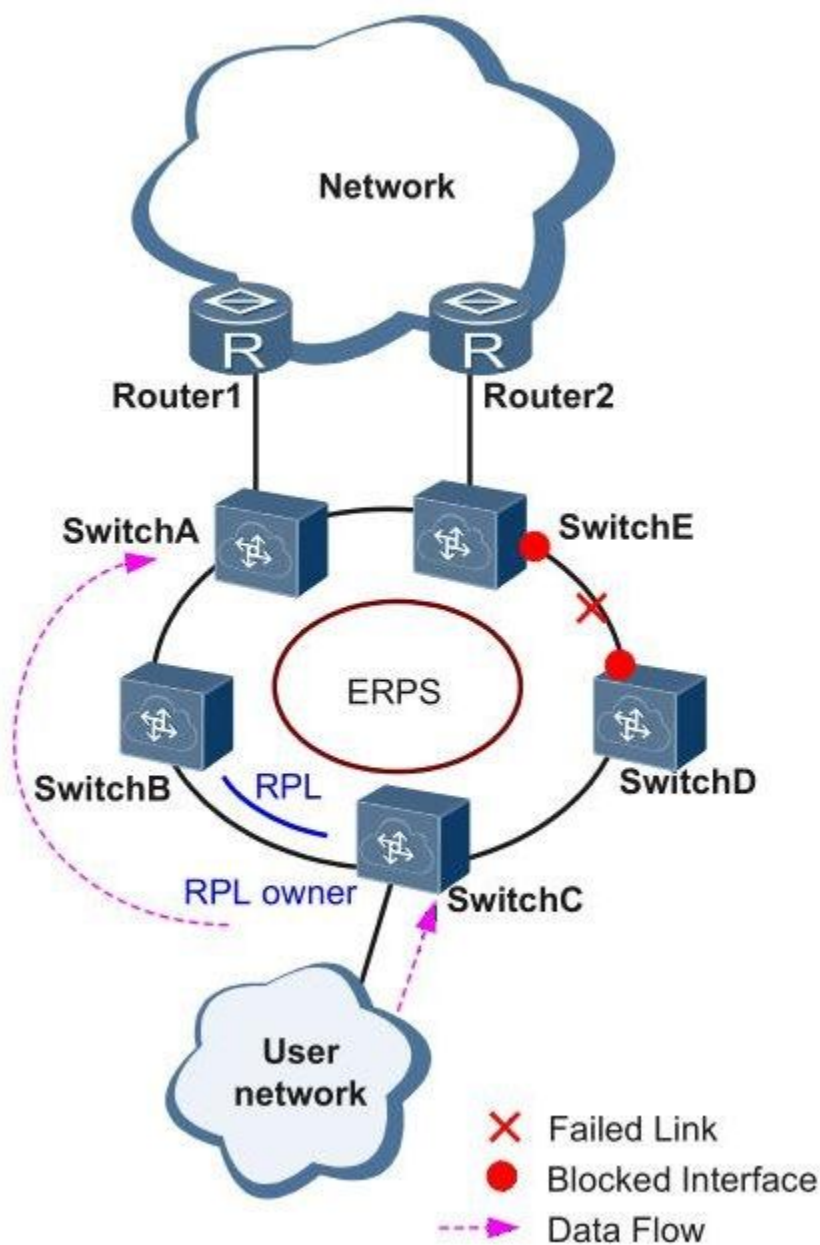


Рисунок 42 – Link restores

Single-Ring:

На Рисунке 43 топология сети имеет только одно кольцо, один узел-владелец RPL и один RPL. Все узлы должны принадлежать к одной и той же виртуальной локальной сети (VLAN) с автоматической защитной коммутацией (R-APS).

Все устройства в кольцевой сети должны поддерживать ERPS. Каналы между устройствами в кольцевой сети должны быть соединены напрямую, и не должно быть никаких промежуточных устройств.

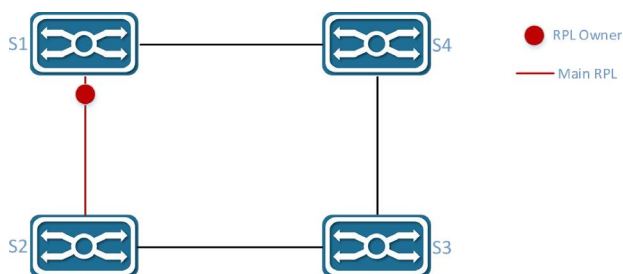


Рисунок 43 –ERPS Single-Ring

Tangent Rings:

На Рисунке 44 два кольца в сетевой топологии используют одно устройство. Каждое кольцо имеет только один узел-владелец PRL и один RPL. Два кольца принадлежат разным VLAN R-APS. Все устройства в кольцевой сети должны поддерживать ERPS. Каналы между устройствами в кольцевой сети должны быть соединены напрямую, и не должно быть никаких промежуточных устройств.

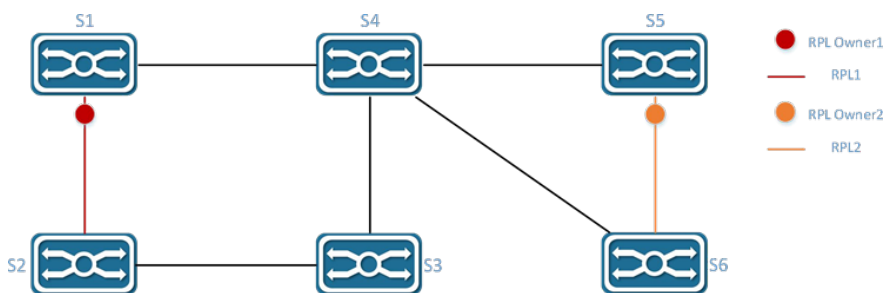


Рисунок 44 –ERPS Tangent Rings

Intersecting Rings:

На Рисунке 45 в топологии сети существует четыре кольца. Каждое кольцо имеет только один узел-владелец PRL и один RPL. Четыре кольца принадлежат разным VLAN R-APS. Все устройства в кольцевой сети должны поддерживать ERPS. Каналы между устройствами в кольцевой сети должны быть соединены напрямую, и не должно быть никаких промежуточных устройств.

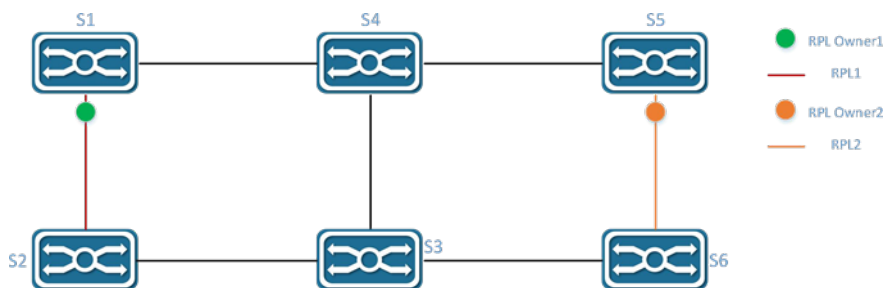


Рисунок 45 –ERPS Intersecting Rings

3.4.2. Конфигурация ERPS

Конфигурация кольца:

Выберите «Configuration» - «ERPS» - «Ring Configuration» в дереве навигации для перехода на страницу конфигурации кольца, как показано на Рисунке 46.

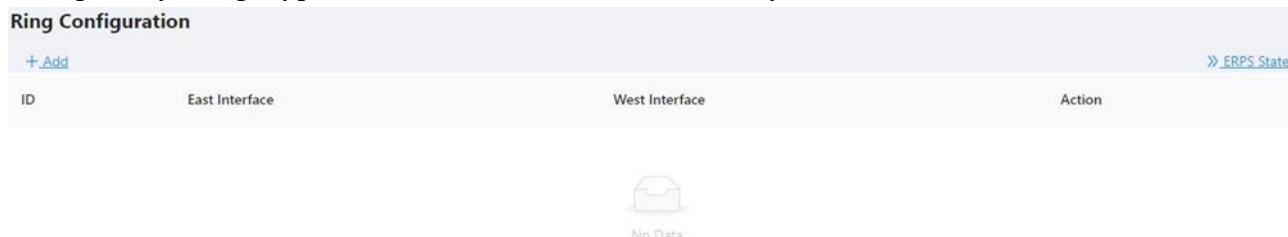


Рисунок 46 – Страница ERPS Ring Configuration

Элемент	Описание
Ring ID	Может быть любое число. Номер кольца ERPS должен быть уникальным
East Interface	Восточный интерфейс кольца ERPS
West Interface	Западный интерфейс кольца ERPS
Action	Удалить кольцо ERPS

Конфигурация экземпляра ERPS:

Выберите «Configuration» - «ERPS» - «Instance Configuration» в дереве навигации для перехода на страницу конфигурации экземпляра ERPS, как показано на Рисунке 47.

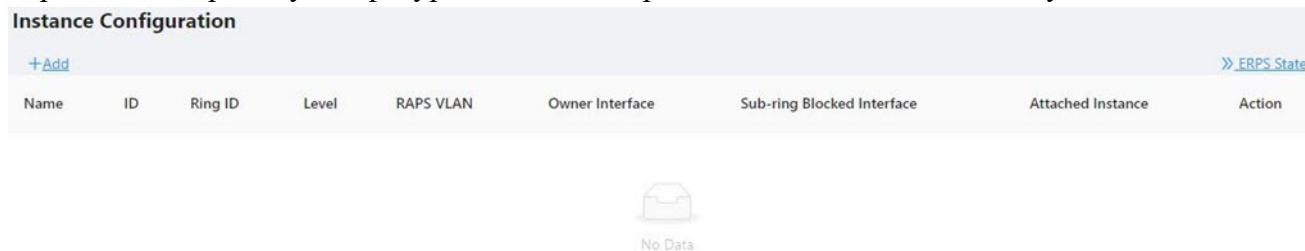


Рисунок 47 – Страница ERPS Instance Configuration

Нажмите кнопку «+Add» под «Instance Configuration», чтобы создать экземпляр ERPS, как показано на Рисунке 48.

Элемент	Описание
Ring Configuration	Создание нового или ссылки на созданное кольцо ERPS
Ring ID	Связанный ID кольца должен быть созданным кольцом

East Interface	Восточный интерфейс кольца ERPS
West Interface	Западный интерфейс кольца ERPS
RAPS VLAN	Каждый коммутатор в одном кольце должен быть настроен с использованием одной и той же VLAN управления RAPS для передачи пакетов протокола ERPS. VLAN управления RAPS может быть виртуальным VLAN, и его необходимо изолировать от VLAN данных
Owner interface	Интерфейс владельца ERPS может выбрать в качестве узла владельца восточный или западный интерфейс. Каждое кольцо ERPS имеет один и только один интерфейс, настроенный как интерфейс владельца RPL, который управляет портами, которые необходимо заблокировать
Sub-ring Block Interface	Блокированный интерфейс подкольца, одно подкольцо имеет только один блокирующий порт. Вы можете выбрать восточный или западный интерфейс. Этот параметр необходимо настроить только для касательного кольца. Подкольца двух устройств по касательной к кольцу должны быть настроены с портом блокировки подкольца
Attached Instance	Необходимо устанавливать только в том случае, если необходимо настроить блокирующий порт подкольца, и для него устанавливается ID кольца, касательный к текущему подкольцу

ERPS Configuration

* Ring Configuration:

Create

Link

* Ring ID: 1

* East Interface: gigabitEthernet0/9

* West Interface: gigabitEthernet0/10

* RAPS VLAN: 1000

Advanced Setting

Name:

* ID: 0

* Level: 0

* Owner Interface:

None

East

West

* Sub-ring Blocked Interface:

None

East

West

Рисунок 48 – Страница ERPS Instance Configuration

Просмотр состояния ERPS:

Нажмите кнопку «ERPS State», чтобы перейти на страницу «ERPS State», как показано на Рисунке 49.

Auto Refresh

» ERPS Configuration

Name	Ring ID	State	Last Event	East Interface	West Interface	Action
No Data						

Рисунок 49 – Страница ERPS State

Элемент	Описание
Name	Название кольца ERPS
Ring ID	Номер кольца ERPS
State	Статус кольца ERPS, включая:

	Idle: Стабильное состояние, когда доступны все линки, не относящиеся к RPL. В этом состоянии узел-владелец блокирует порт RPL и периодически отправляет пакеты NR-RB. Соседний узел блокирует порт RPL. Все узлы переходят в состояние ожидания после того, как узел-владелец переходит в состояние ожидания. Pending: Переходное состояние между предыдущими состояниями. Protection: Состояние, когда канал, не поддерживающий RPL, неисправен. В этом состоянии канал RPL разблокирован для пересылки трафика. Все узлы переходят в состояние защиты после того, как узел входит в состояние защиты
Last Event	События: RAPS-NR: удаленное восстановление после сбоя RAPS-NR-RB: дистанционное обратное переключение RAPS-SF: удаленная неисправность LOCAL-SF: местная неисправность LOCAL-CLEAR-SF: восстановление после локального сбоя WTR-EXP: местное обратное переключение
East Interface	Восточный интерфейс кольца ERPS
West Interface	Западный интерфейс кольца ERPS
Action	Когда неисправный линк будет восстановлен, вы можете немедленно выполнить возврат вручную, в противном случае система автоматически выполнит возврат через 5 минут

3.5. PoE Management

3.5.1. PoE Overview

Power over Ethernet (PoE) - технология, позволяющая передавать удалённому устройству электрическую энергию вместе с данными через стандартную витую пару в сети Ethernet.

Данная технология предназначена для IP-телефонии, точек доступа беспроводных сетей, IP-камер, сетевых концентраторов и других устройств, к которым нежелательно или невозможно проводить отдельный электрический кабель.

Технология PoE описана стандартами IEEE 802.3af-2003, IEEE 802.3at-2009 и IEEE 802.3bt-2018.

3.5.2. Конфигурация PoE

1. Выберите «Configuration» - «PoE» в дереве навигации для перехода на страницу управления PoE, как показано на Рисунке 50.
2. Введите значения в поля «Power supply» и «Power reserved» и нажмите кнопку «Apply».

Рисунок 50 – Страница PoE Global Configuration

Элемент	Описание
Power supply (W)	Введите в поле значение соответствующее мощности внешнего источника питания
Power reserved (%)	Резервная мощность выделяемая для работы основной платы коммутатора, рекомендуется указывать потребляемую мощность основной платы
Power management	Отображение режима управления питанием энергосбережения. В этом режиме мощность, запрашиваемая и выделяемая порту, основана на фактическом энергопотреблении порта в реальном времени
Disconnect mode	Отображение режима отключения постоянного тока
Alarm state	Включение/выключение логирования при недостаточном питании
Power alarm (%)	Настройка ограничения мощности: когда потребляемая мощность PoE превышает это значение, система автоматически оповещает и записывает событие в журнал

3. Нажмите «Batch Edit» под «Port Configuration», чтобы перейти на страницу конфигурации PoE порта. Выберите порт для настройки, как показано на Рисунке 51.

Port Configuration

* Admin State: ☐ Disabled ☒ Enable ☐ Force_on

Description:

Max power(W):

* Priority: ☒ Low ☐ Medium ☐ High

* Mode: ☒ None ☐ Flow ☐ Ping

Legacy mode: ☐

☒ Selected ☐ AG Port ☐ Copper ☐ Fiber

[All](#) [Revert](#) [Deselect](#)

Рисунок 51 – Страница PoE Interface Configuration

- Нажмите кнопку «OK», чтобы завершить операцию, после чего страница вернется на страницу PoE Interface Configuration, как показано на Рисунке 52.

Port Configuration

[Batch Edit](#) [PoE State](#)

Name	Admin State	Description	Max power(W)	Priority	Mode	IP address	Interval	Times	Legacy mode	Action
gigabitEthernet0/1	Enable		--	Low	None		30	10	Disable	Edit
gigabitEthernet0/2	Force_on	111	30	Low	Flow		30	10	Disable	Edit
gigabitEthernet0/3	Enable		--	Low	None		30	10	Disable	Edit
gigabitEthernet0/4	Enable		--	Low	None		30	10	Disable	Edit

Рисунок 52 – Страница PoE Interface Configuration

- Нажмите кнопку «Save» во вспомогательной области инструментов, чтобы сохранить конфигурацию.

Элемент	Описание
Name	Номер порта
Admin State	Включение/выключение PoE порта. Disabled: отключить питание PoE. Enable: включить питание PoE. Force_on: принудительно включить питание PoE. В этом режиме максимальная мощность нагрузки по умолчанию составляет 15 Вт. Если вам необходимо обеспечить мощность устройства выше 15 Вт, одновременно необходимо настроить параметр максимальной мощности
Description	Описание PoE порта
Max Power (W)	Максимальная мощность PoE порта.

	Для портов AF/AT максимальный диапазон мощности порта составляет 1–30. Для портов BT максимальный диапазон мощности порта составляет 1–90. В режиме по умолчанию порт будет управлять питанием в соответствии с классом PD
Priority	Настройка приоритета порта. В случае, когда общего бюджета PoE недостаточно, порты с более низким приоритетом будут отключены в первую очередь. Порты с одинаковым приоритетом располагаются в порядке номера порта, причем приоритет порта с меньшим номером порта выше. Например, приоритет порта 0/1 выше, чем портов 0/2 и 0/3
Mode	None: отключает функцию обнаружения PD. Flow: включает функцию обнаружения PD в режиме потока. Эта функция реализуется путем мониторинга счетчика порта: если счетчик пакетов порта не изменяется, считается, что устройство PD подключенное к порту находится в ненормальном состоянии, после чего происходит отключение и включение PoE на порту. Ping: Включает функцию обнаружения PD в режиме Ping. Эта функция реализуется путем непрерывной отправки запросов к PD. Если в течение определенного периода времени заданный узел недоступен, считается, что устройство PD подключенное к порту находится в ненормальном состоянии, после чего происходит отключение и включение PoE на порту
IP address	В режиме Ping, IP-адрес устройства PD и коммутатора должны находиться в одном сегменте сети
Interval	Интервал времени обнаружения
Times	Время обнаружения. Время запуска PD должно быть меньше интервала обнаружения * время обнаружения, в противном случае устройство PD всегда будет находиться в состоянии запуска
Legacy mode	ON/OFF, по умолчанию OFF. OFF: поддерживаются только стандартные устройства PD, сопротивление которых составляет от 19 до 26,5 кОм с параллельно подключенным конденсатором емкостью от 0 до 150 нФ. ON: поддержка нестандартных устройств PD, значение сопротивления и емкости которых превышают стандартные значения

3.6. Security

3.6.1. Port Security

3.6.1.1. Введение

Port-Security - механизм обеспечения безопасности и контроля доступа, основанный на контроле изучаемых MAC-адресов. Может использоваться как дополнение существующей аутентификации 802.1x и аутентификации MAC. Port-security контролирует доступ неавторизованных устройств к сети, проверяя MAC-адрес источника принятого кадра и доступ к неавторизованным устройствам, проверяя MAC-адрес назначения отправленного кадра.

Если функционал port-security настроен на портах коммутатора, при получении кадра с неверным MAC-адресом, коммутатор запускает заданную пользователем функцию защиты порта и автоматически выполняет заданное действие.

3.6.1.2. Конфигурация Port Security

Port Configuration:

1. Выберите «Configuration» - «Security» - «Port security» в дереве навигации для перехода на страницу Port security, как показано на Рисунке 53.

Port Configuration							
Batch Edit		Port State					
Name	State	Max MAC Number	Sticky	Aging Time(min.)	Aging Static	Violation Mode	Action
 No Data							

Рисунок 53 – Страница статистики Port Security

2. Нажмите кнопку «Batch Edit» под «Port Configuration», чтобы перейти на страницу Port Configuration, как показано на Рисунке 54.

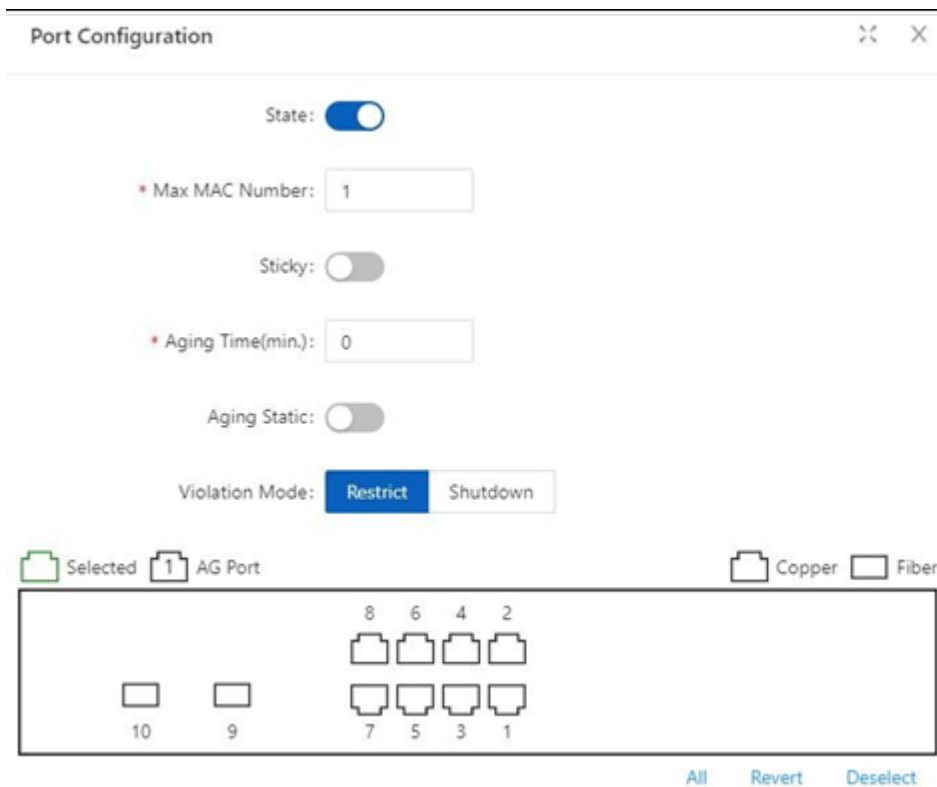


Рисунок 54 – Страница конфигурации Port Security

Элемент		Описание
Port Configuration	State	Включить/выключить Port security на порту
	Max MAC Number	Настройка максимального количества MAC-адресов для порта, по умолчанию максимальное количество MAC-адресов — 1, диапазон — <1-1024>
	Sticky	Включить/выключить функцию Sticky (статический MAC-адрес)
	Aging Time(min)	Настройка времени жизни MAC-адресов в минутах. По умолчанию 0, что означает, что функция отключена. Диапазон времени жизни <0-1440>. По умолчанию функция времени жизни MAC-адресов применяется для динамических и статических адресов
	Aging Static	Включает функцию времени жизни статического адреса
	Violation Mode	Выберите действие при изучении нового MAC-адреса, если превышено заданное максимальное число адресов. Restrict - не изучать новый MAC. Shutdown - выключить порт

MAC Configuration:

1. Выберите «Configuration» - «Security» - «MAC Configuration» в дереве навигации для перехода на страницу MAC Configuration, как показано на Рисунке 55.

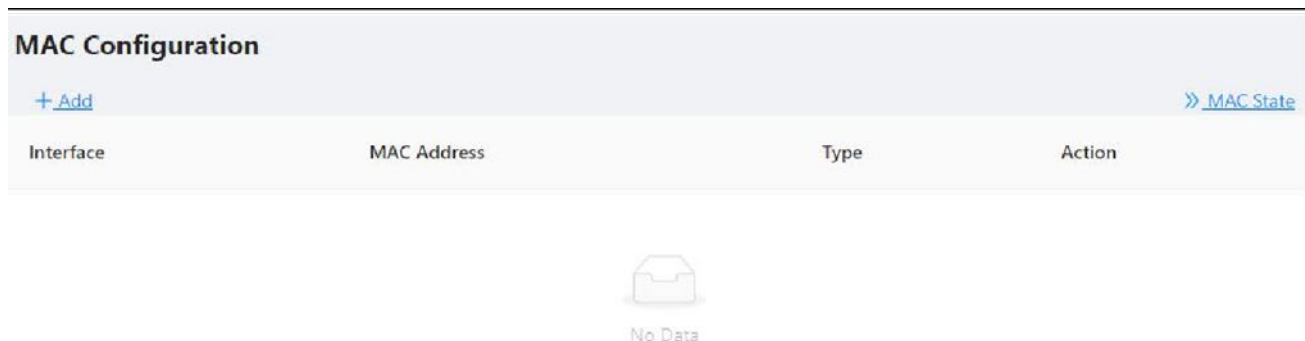


Рисунок 55 – Страница информации о MAC Configuration

2. Нажмите кнопку «+Add» чтобы перейти на страницу MAC Configuration, как показано на Рисунке 56.

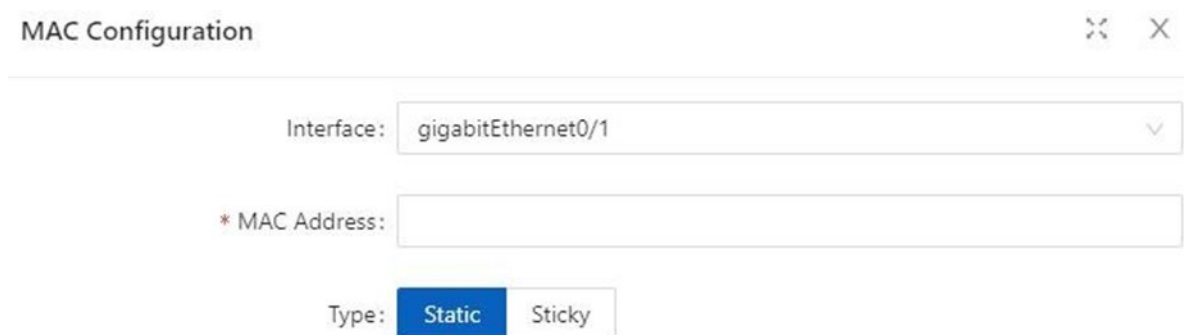


Рисунок 56 – Страница MAC Configuration

Элемент		Описание
MAC Configuration	Interface	Выберите интерфейс для настройки.
	MAC Address	Введите статический MAC-адрес в формате: XXXX.XXXX.XXXX. MAC-адрес не может быть широковещательным или многоадресным адресом.
	Type	Выберите тип MAC-адреса: динамический или статический

3.6.2. IP Source Guard

3.6.2.1. Введение

IP Source Guard это механизм коммутатора, который ограничивает прохождение трафика через интерфейс коммутатора, если он не входит в таблицу привязок DHCP Snooping или не указан статически.

Если для интерфейса настроен IP Source Guard, то ПК не сможет взаимодействовать с сетью пока он не получит адрес по DHCP или его IP+MAC адрес не будет включен в статическую таблицу.

Функция **ARP-Check** (проверка ARP пакетов) фильтрует ARP пакеты и отбрасывает все ложные ARP пакеты на основе информации IP+MAC, что позволяет эффективно предотвратить подделку ARP пакета и повысить стабильность сети.

3.6.2.2. Конфигурация IP Source Guard

1. Выберите «Configuration» - «Security» - «IP Source Guard» в дереве навигации для перехода на страницу IP Source Guard, как показано на Рисунке 57.

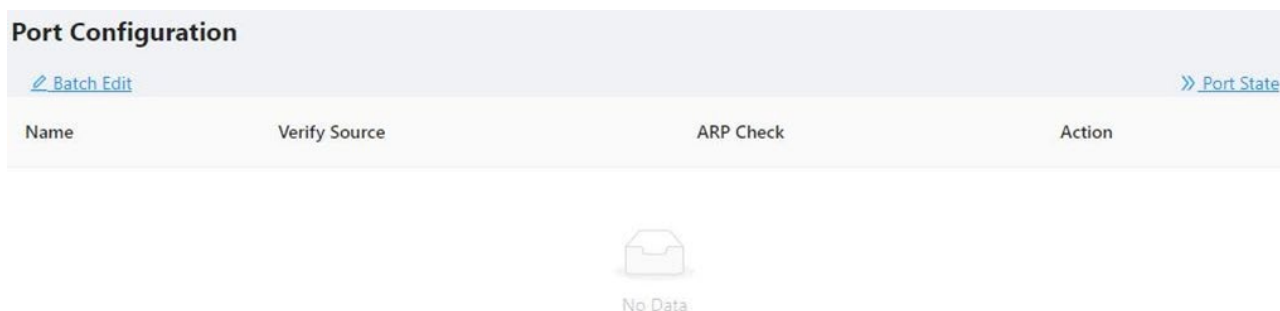


Рисунок 57 – Страница информации о IP Source Guard

2. Нажмите кнопку «Batch Edit» под «Port Configuration» на текущей странице, выберите интерфейс для настройки на панели порта, нажмите кнопку «Verify Source», как показано на Рисунке 58.

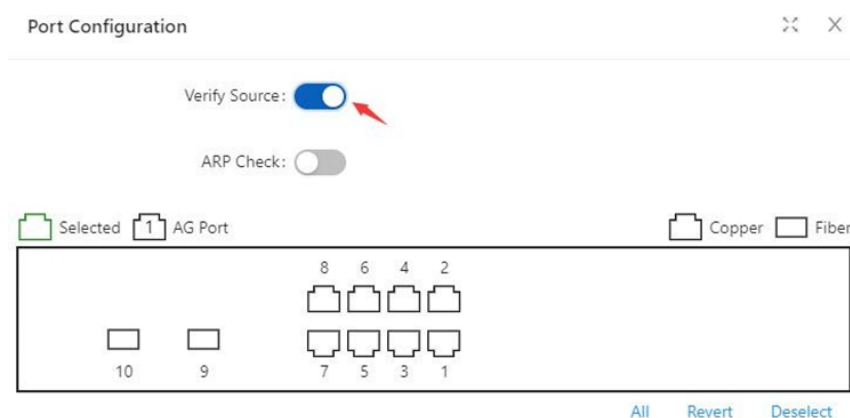


Рисунок 58 – Страница IP Source Guard port configuration

3. Нажмите кнопку «ОК», созданные правила отобразятся на сводной странице, как показано на Рисунке 59.

Port Configuration			
Batch Edit		Port State	
Name	Verify Source	ARP Check	Action
gigabitEthernet0/1	Enable	Disable	Edit

Рисунок 59 – Страница IP Source Guard configuration port configuration

- Нажмите кнопку «+Add» под «User Configuration» на текущей странице, чтобы перейти на страницу конфигурации пользователя. Выберите порт, введите VID, IP-адрес и MAC-адрес, как показано на Рисунке 60.

User Configuration

Interface: gigabitEthernet0/1

VID: 1

* IP Address: 192.168.56.20

* MAC Address: 00-0E-C6-C1-37-89

Рисунок 60 – Страница IP Source Guard user configuration

- Нажмите кнопку «OK», созданные правила отобразятся на сводной странице, как показано на Рисунке 61.

User Configuration						
+ Add						User State
Interface	VID	IP Address	MAC Address	Lease	Type	Action
gigabitEthernet0/1	1	192.168.56.20	00-0E-C6-C1-37-89	Infinite	Static	Delete

Рисунок 61 – Страница IP Source Guard rules

3.6.2.3. Конфигурация ARP Check

- Выберите «Configuration» - «Security» - «IP Source Guard» в дереве навигации для перехода на страницу IP Source Guard, как показано на Рисунке 57.
- Нажмите кнопку «Batch Edit» под «Port Configuration» на текущей странице, выберите интерфейс для настройки на панели порта, нажмите кнопку «ARP Check», как показано на Рисунке 62.

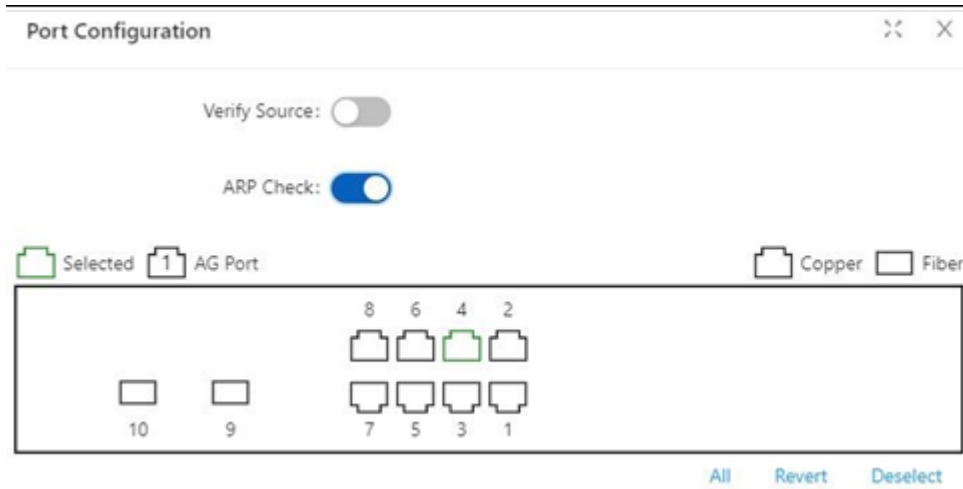


Рисунок 62 – Страница IP Source Guard ARP Check

3. Нажмите кнопку «+Add» под «User Configuration» на текущей странице, чтобы перейти на страницу конфигурации пользователя, как показано на Рисунке 63.

Рисунок 63 – Страница IP Source Guard User Configuration

4. Нажмите кнопку «Apply», созданные правила отобразятся на сводной странице, как показано на Рисунке 64.

User Configuration						
+ Add » User State						
Interface	VID	IP Address	MAC Address	Lease	Type	Action
gigabitEthernet0/4	1	192.168.56.20	00-0E-C6-C1-37-89	Infinite	Static	Delete

Рисунок 64 – Страница ARP Check rules

3.6.3. Dot1X

3.6.3.1. Введение

Стандарт IEEE 802.1x определяет метод управления доступом к сети, он управляет аутентификацией и устройствами доступа на физическом уровне (порты коммутатора). Если пользовательские устройства, подключенные к этим портам, удастся аутентифицировать, они получают доступ к ресурсам локальной сети, в противном случае доступ будет запрещен.

Стандарты IEEE 802.1x определяют протокол управления доступом к сети на основе портов. Протокол применим к соединению точка-точка между устройством доступа и портом доступа, при этом порт может быть логическим или физическим. В типичном случае один физический порт коммутатора присоединен только к одному терминирующему устройству (имеющему физические порты).

Архитектура IEEE 802.1X включает в себя следующие обязательные логические элементы: клиент, сервер аутентификации, аутентификатор, как показано на Рисунке 65.

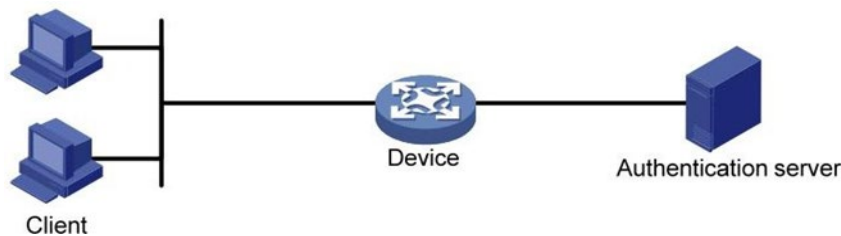


Рисунок 65 – Архитектура IEEE 802.1X

- Клиент (Client) находится в операционной системе абонента, обычно это рабочая станция, которая запрашивает доступ к локальной сети и сервисам коммутатора и отвечает на запросы от коммутатора. На рабочей станции должно быть установлено клиентское ПО для 802.1X, например то, которое встроено в ОС Microsoft Windows;
- Сервер аутентификации (Authentication Server) выполняет фактическую аутентификацию клиента. Он проверяет подлинность клиента и информирует коммутатор, предоставлять или нет клиенту доступ к локальной сети. RADIUS (Remote Authentication Dial-In User Service) работает в модели "клиент/сервер", в которой информация об аутентификации передается между сервером RADIUS и клиентами RADIUS;
- Аутентификатор (Device) управляет физическим доступом к сети, основываясь на статусе аутентификации клиента. Эту роль выполняет коммутатор. Он работает как посредник (Проху) между клиентом и сервером аутентификации: получает запрос на проверку подлинности от клиента, проверяет данную информацию при помощи сервера аутентификации и пересылает ответ клиенту. Коммутатор поддерживает клиент RADIUS, который отвечает за инкапсуляцию и деинкапсуляцию кадров EAP, и взаимодействие с сервером аутентификации.

Взаимодействие устройства, запрашивающего доступ, и устройства управления доступом (коммутатором доступа) происходит по протоколу EAPOL, определенного стандартами IEEE 802.1x. Взаимодействие сервера аутентификации с устройством управления доступом происходит по протоколу EAP. Данные аутентификации инкапсулируются в пакеты EAP. Пакет EAP передается в пакетах протоколов более высоких уровней, например, RADIUS (EAPOR - EAP over RADIUS).

Система аутентификации (коммутатор доступа) предоставляет порты для доступа к сети запрашивающим пользовательским системам. Эти порты логически можно разделить на два вида: контролируемые и неконтролируемые:

- Неконтролируемый порт всегда находится в режиме двунаправленного соединения и в основном используется для передачи пакетов протокола EAPOL, чтобы гарантировать, что запрашивающие системы всегда могут отправлять или получать сообщения аутентификации.
- Контролируемый порт связан с состоянием аутентификации. При отсутствии аутентификации данные из запрашивающих доступ систем передаваться не могут. Данный коммутатор может осуществлять контроль только одного направления трафика.
- Управляемые и неконтролируемые порты представляют собой две логические части одного физического порта.

Контролируемый порт может находиться в авторизованном, либо в неавторизованном состоянии, в зависимости от результата аутентификации, как показано на Рисунке 66.

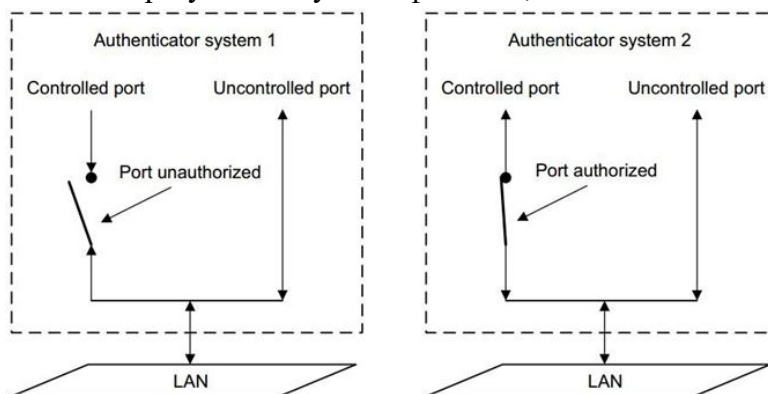


Рисунок 66 – Авторизованное/неавторизованное состояние контролируемого порта

И коммутатор, и клиент могут инициировать аутентификацию. Коммутатор делает это, когда состояние порта меняется с DOWN на UP или периодически, пока клиент за портом не аутентифицирован. Для этих задач коммутатор использует протоколы EAPOL (extensible authentication protocol over LAN) и RADIUS (remote authentication in dial-in user service). На Рисунке 67 рассмотрим, что происходит, когда новое сетевое устройство с поддержкой 802.1X подключается к порту коммутатора.

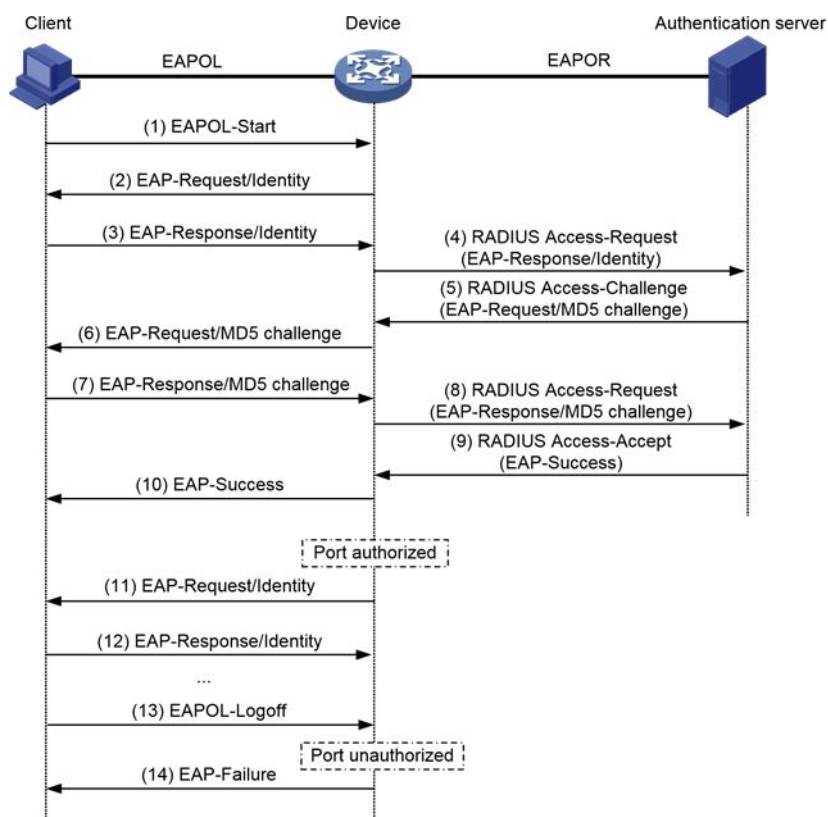


Рисунок 67 – Принцип обмена сообщениями с EAP-MD5

1. Устройство (Client) инициирует аутентификацию, посылая EAPOL-Start-фрейм на мультикастовый MAC-адрес 01:80:c2:00:00:03.
2. Коммутатор получает этот кадр, с этого момента он начинает выступать в роли промежуточного устройства (Device) между клиентом и сервером аутентификации (RADIUS). В ответ посылается EAP-фрейм Request/Identity, предлагающий клиенту представиться.
3. Клиент отвечает EAP-фреймом Response/Identity, содержащим имя пользователя. Эта информация добавляется в пакет протокола RADIUS Access-Request и в числе прочих атрибутов пересылается серверу аутентификации.
4. Сервер аутентификации отправляет на IP-адрес коммутатора RADIUS-пакет Access-Challenge с запросом пароля для данного имени пользователя. Коммутатор отправляет этот запрос клиенту EAP-фрейм с запросом пароля.
5. Клиент отправляет в ответ EAP-фрейм со своим паролем, который пересылается коммутатором серверу аутентификации в Access-Request пакете. Если клиент идентифицирован, то в ответ посылается пакет Access-Accept.
6. Коммутатор посылает клиенту EAP-фрейм EAP-Success. На этом этапе порт аутентифицирован. В случае, если устройство пришлет EAP-фрейм Logoff, порт вернется в исходное состояние.

3.6.3.2. Конфигурация Dot1X

Выберите «Security» - «Dot1x» - «Configuration» в дереве навигации для перехода на страницу отображения 802.1X Global Configuration и Port Configuration, как показано на Рисунке 68, 69.

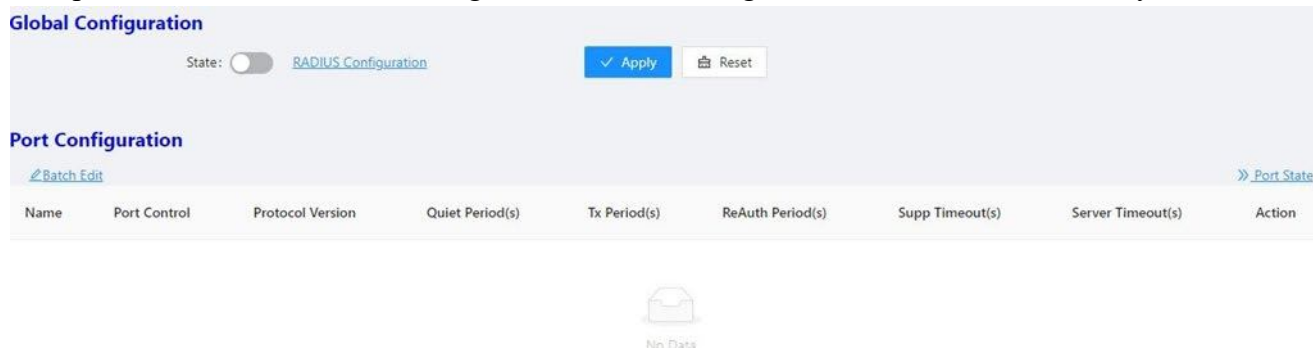


Рисунок 68 – Страница 802.1X Global Configuration

Элемент		Описание
Global Configuration	State	Включает функцию 802.1X
	RADIUS Configuration	Переход к интерфейсу настройки RADIUS

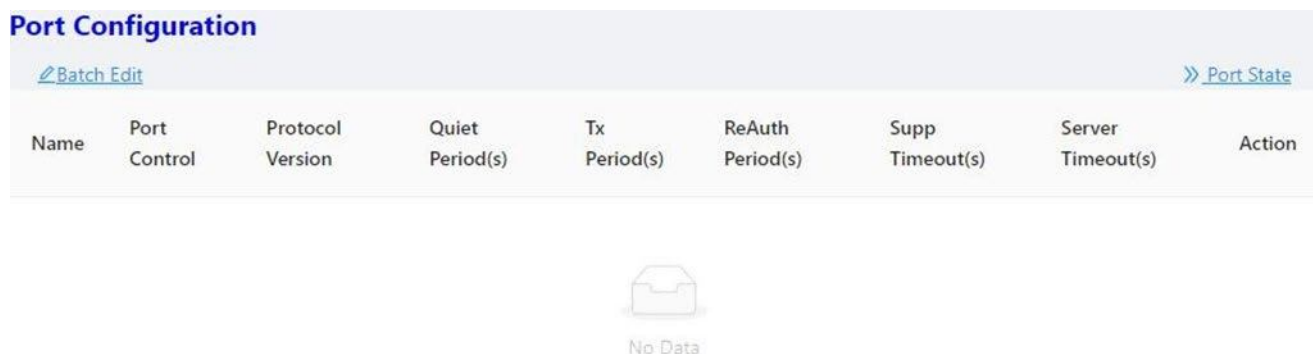


Рисунок 69 – Страница 802.1X Port Configuration

Элемент		Описание
Port Configuration	Name	Имя физического интерфейса
	Port Control	Режим управления портом
	Protocol Version	Версия протокола EAPOL, по умолчанию - 2 секунды
	Quiet Period(s)	Количество секунд, в течение которых коммутатор остается в режиме ожидания после неудачного обмена аутентификацией с клиентом.

		Диапазон: от 0 до 65 535 секунд; по умолчанию - 60 секунд. Если коммутатор не может аутентифицировать клиента, он остается бездействующим в течение заданного периода, а затем пытается снова. Время простоя определяется значением Quiet Period(s)
	Tx Period(s)	Количество секунд, в течение которых коммутатор ожидает ответа на EAP-запрос/фрейм идентификации от клиента перед повторным запросом. Диапазон: от 1 до 65 535 секунд; по умолчанию - 30 секунд
	ReAuth Enabled	Включает повторную аутентификацию клиента
	ReAuth Period(s)	Количество секунд между попытками повторной аутентификации или тайм-аут сеанса RADIUS. Диапазон от 1 до 65 535; по умолчанию - 3600 секунд
	Supp Timeout(s)	Количество секунд, в течение которых коммутатор ожидает ответа на кадр EAP-Request/MD5 Challenge от клиента перед повторным запросом. Диапазон: от 1 до 65 535 секунд; по умолчанию - 30 секунд
	Server Timeout(s)	Количество секунд, в течение которых коммутатор ожидает ответа на пакет Access-Request от RADIUS. Диапазон: от 1 до 65 535 секунд; по умолчанию - 30 секунд

3.6.4. MAC Authentication

Выберите «Configuration» - «Security» - «MAC Authentication» в дереве навигации для перехода на страницу MAC Authentication, как показано на Рисунке 70.

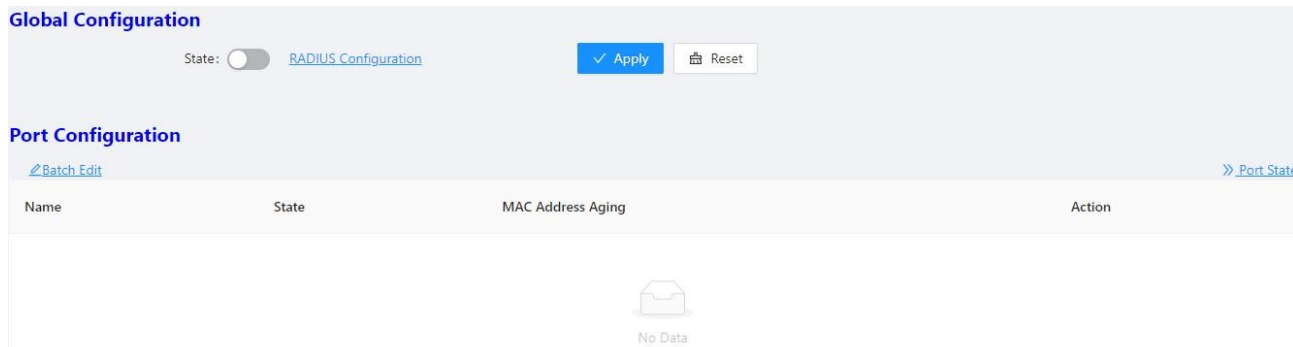


Рисунок 70 – Страница MAC Authentication

Элемент		Описание
Global Configuration	State	Включает функцию 802.1X
	RADIUS Configuration	Переход к интерфейсу настройки RADIUS
Port Configuration	Name	Имя физического интерфейса
	State	Состояние MAC-аутентификации
	MAC Address Aging	Состояние времени жизни MAC-адреса
	Action	Изменение правила

Конфигурация MAC Authentication:

1. Включение MAC Auth.

Выберите «Configuration» - «Security» - «MAC Authentication» в дереве навигации. Нажмите кнопку «State» на странице Global Configuration, затем нажмите кнопку «Apply», чтобы включить функцию MAC-auth.

2. Конфигурация порта.

Нажмите кнопку «Batch Edit» под «Port Configuration», чтобы перейти на страницу конфигурации порта, как показано на Рисунке 71. Нажмите кнопку «State», выберите порт на панели портов для настройки, нажмите кнопку «ОК».

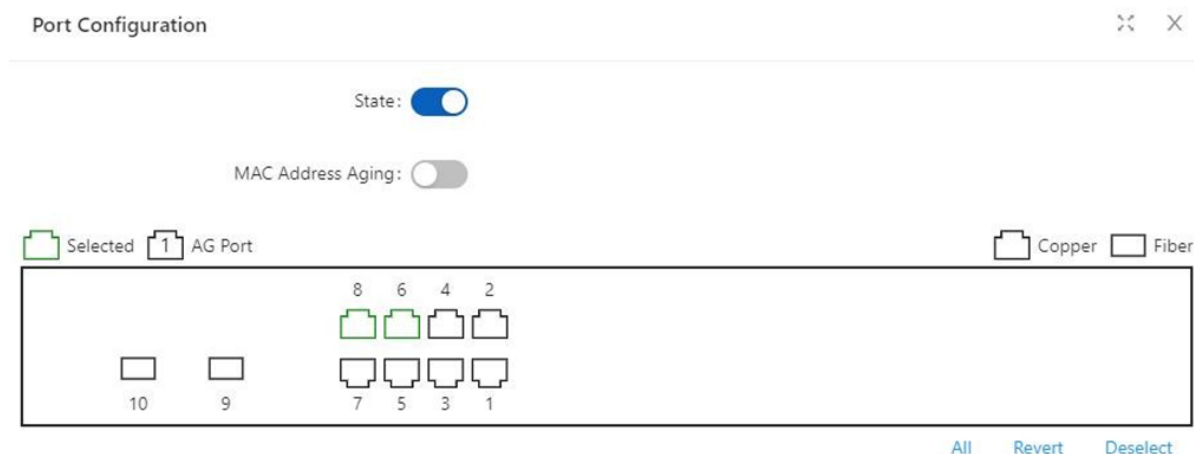


Рисунок 71 – Страница MAC Authentication Port Configuration

3.6.5. RADIUS

3.6.5.1. Введение

RADIUS - это один из сетевых клиент-серверных протоколов, используемый для централизованного управления авторизацией, аутентификацией и учетов при запросе доступа пользователей к различным сетевым службам. Клиент RADIUS обычно используется на

сетевом устройстве для реализации AAA совместно с протоколом 802.1x. Сервер RADIUS хранит базу данных для AAA и связывается с клиентом RADIUS через протокол RADIUS, который является наиболее распространенным протоколом в рамках AAA.

Модель клиент/сервер:

- Клиент: Клиент RADIUS работает на NAS, расположенных по всей сети. Он передает информацию о пользователе на назначенные серверы RADIUS и обрабатывает ответы (например, отклоняет или принимает запросы на доступ пользователей).
- Сервер: Сервер RADIUS работает на компьютере или рабочей станции и хранит информацию, связанную с аутентификацией пользователей и доступом к сетевым службам. Он прослушивает запросы на подключение, аутентифицирует пользователей и возвращает результаты обработки (например, отклонение или принятие запроса на доступ пользователя) клиентам.

Сервер RADIUS поддерживает три базы данных: «Users», «Clients» и «Dictionary», как показано на Рисунке 72.

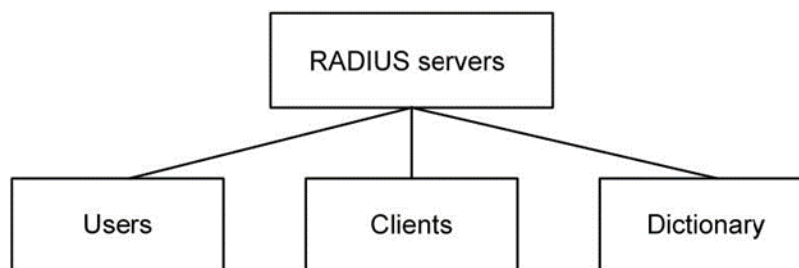


Рисунок 72 – Компоненты RADIUS Server

- Users: хранит информацию о пользователях, такую как имена пользователей, пароли, применяемые протоколы и IP-адреса.
- Clients: хранит информацию о клиентах RADIUS, такую как общие ключи и IP-адреса.
- Dictionary: хранит информацию о значениях атрибутов протокола RADIUS и их значениях.

Взаимодействие хоста, RADIUS клиента и RADIUS сервера представлено на рисунке 73.

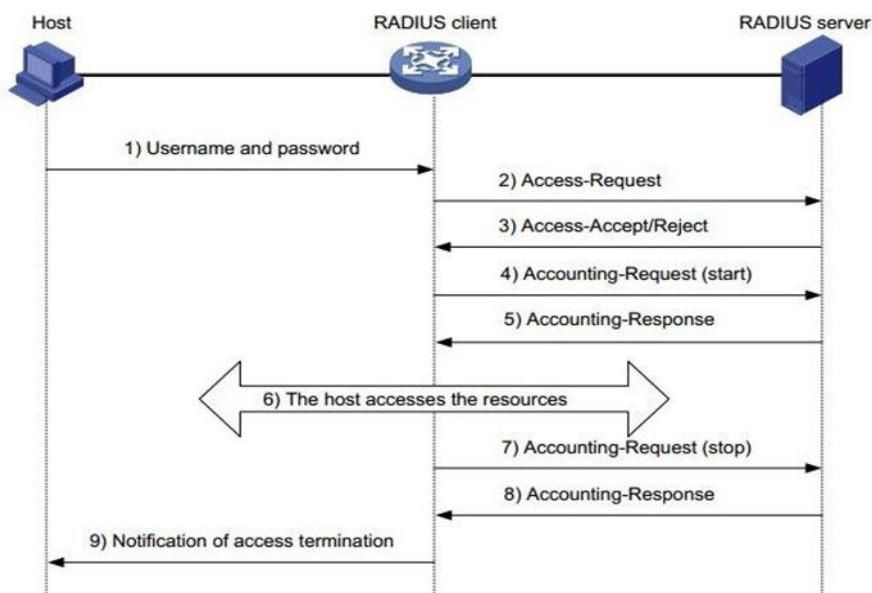


Рисунок 73 – Процесс обмена сообщениями RADIUS

3.6.5.2. Конфигурация RADIUS

Глобальная конфигурация RADIUS:

Выберите «Configuration» - «Security» - «RADIUS» в дереве навигации для перехода на страницу RADIUS Global Configuration, как показано на Рисунке 74.

RADIUS

Global Configuration

Key:

* Dead Time(min.):

* Timeout(s):

* Retransmission:

✓ Apply

Reset

Рисунок 74 – Страница RADIUS Global Configuration

Элемент		Описание
Global Configuration	Key	Глобальный ключ RADIUS-сервера
	Timeout(s)	Время ожидания ответа от сервера перед повторной отправкой пакета. По умолчанию - 5 секунд
	Retransmission	Число попыток повторной отправки пакетов на RADIUS-сервер. По умолчанию - 3 попытки
	Dead Time(min)	Время восстановления статуса RADIUS-сервера после того, как коммутатор обнаружил его недоступность, в минутах. По умолчанию - 0 минут, что указывает на то, что сервер будет восстановлен сразу после обнаружения недоступности

Конфигурация RADIUS Server:

Нажмите кнопку «+Add» под «Server Configuration» на текущей странице, чтобы перейти на страницу конфигурации, как показано на Рисунке 75.

Элемент	Описание
IP	IP-адрес сервера
Auth Port	Номер порта аутентификации сервера; по умолчанию 1812
Key	Ключ сервера
Timeout(s)	Время ожидания ответа от сервера перед повторной отправкой пакета. По умолчанию - 5 секунд
Retransmission	Число попыток повторной отправки пакетов на RADIUS-сервер. По умолчанию - 3 попытки

Server Configuration

* IP:

Key:

Advanced Setting

* Auth Port:

* Timeout(s):

* Retransmission:

Рисунок 75 – Страница RADIUS Server Configuration

3.7. Control

3.7.1. Serial Servers

3.7.1.1. Введение

Сервер последовательных устройств используется для подключения последовательных устройств к Ethernet. Сервер последовательных устройств может работать как в режиме tcp-клиента, так и tcp-сервера, как показано на Рисунке 76, 77.

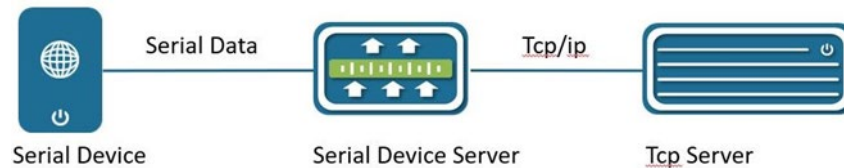


Рисунок 76 – Serial Device Server в режиме tcp-клиента

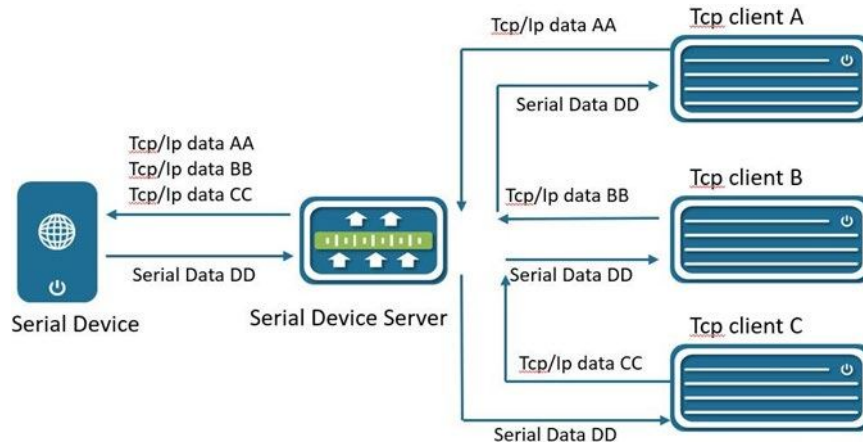


Рисунок 77 – Serial Device Server в режиме tcp-сервера

3.7.1.2. Конфигурация Serial Server

Выберите «Configuration» - «Control» - «Serial Server» в дереве навигации для перехода на страницу конфигурация Serial Server, как показано на Рисунке 78.

Configuration			» State
ID	Mode	Action	
1	none	Edit	Clear

Рисунок 78 – Страница Serial Server Configuration

Нажмите кнопку «Edit», чтобы перейти на страницу конфигурации Serial Server, как показано на Рисунке 79.

Configuration

Basic

ID: 1

Mode:

none

tcp-client

tcp-server

Serial

Baud Rate:

9600

19200

38400

57600

115200

Parity:

none

even

odd

mark

space

Data Bits:

7

8

Stop Bits:

1

2

Communication

* Buffer Size(packets):

64

* Interval(ms):

10

* Max Packet Length(bytes):

1460

* Alive Check Time(s):

30

Server

* Port:

* Max Connections:

1

Рисунок 79 – Страница Serial Server Configuration

Элемент		Описание
Basic	ID	Номер последовательного порта
	None	Выключение последовательного сервера
	tcp-client	Режим работы tcp-клиента
Serial	tcp-server	Режим работы на tcp-сервера
	Baud Rate	Скорость передачи последовательного порта: 9600, 19200, 38400, 57600 и 115200
	Data Bits	Биты данных последовательного порта: 7, 8
	Parity	Тип методов контрольной суммы: none, even, odd, mark, space
Communication	Stop Bits	Настройка стоп-бита: 1, 2
	Buffer size	Биты данных последовательного порта, диапазон <0-128>, по умолчанию - 64
	Max packet Length	Длина пакета данных последовательного порта, превышающая значение LEGGTH, диапазон <0-1460>, по умолчанию - 1460
	Interval	Если интервал между байтами данных превышает миллисекунды, данные постбайта распознаются как новый байт заголовка сообщения.

		Диапазон <1-1000>, по умолчанию - 10 мс
	Alive check time	Настройка последовательного порта для поддержания активности соединения, во время которого отсутствует передача данных
Client	Remote IP	IP-адрес удаленного подключения
	Remote port	Номер порта для удаленного подключения, диапазон от 1 до 65535
	Local port	Номер локального порт
Server	Port	Настройте номер порта tcp-сервера, диапазон от 1 до 65535
	Max connections	Максимальное количество подключений в режиме tcp-сервера, диапазон от 1 до 65535

3.7.2. IO Control

Модуль управления вводом-выводом разделен на две части DI и DO. В текущем программном обеспечении DO поддерживает только функцию ручного управления включения/выключения реле (DO), как показано на Рисунке 80. DI поддерживает только высокий и низкий уровень входного сигнала, как показано на Рисунке 81.

Input

» State

ID	Description	Status	Action
2		high	Apply

Рисунок 80 – Страница конфигурации DI

Output

» State

ID	Description	Status	Default Status	Action
1		low	low	Apply

Рисунок 81 – Страница конфигурации DO

4. Advance

4.1. LLDP

4.1.1. Введение

LLDP (Link Layer Discovery Protocol) — это протокол, используемый для обнаружения и обмена информацией между сетевыми устройствами на канальном уровне (Layer 2) модели OSI. Он позволяет устройствам в сети автоматически обмениваться информацией о своих возможностях и конфигурациях.

Основные функции LLDP:

- **Обмен информацией:** Устройства отправляют информацию о себе, включая идентификаторы, IP-адреса, возможности портов и другие параметры, в формате TLV (тип, длина, значение).
- **Обнаружение соседей:** LLDP позволяет устройствам обнаруживать друг друга и строить топологию сети, что упрощает управление и мониторинг.
- **Стандартизация:** LLDP является стандартом IEEE 802.1AB, что обеспечивает совместимость между устройствами разных производителей.
- **Управление сетью:** Протокол помогает системам управления сетью быстро реагировать на изменения в топологии, что улучшает управление и диагностику сети.

4.1.2. Конфигурация LLDP

Глобальная конфигурация LLDP:

Выберите «Advance» - «Layer2» - «LLDP Configuration» в дереве навигации для перехода на страницу глобальной конфигурации, как показано на Рисунке 82.

Рисунок 82 – Страница LLDP Global Configuration

Элемент	Описание
Status	Disabled: Отключение функции LLDP Enabled: Включение функции LLDP
System Name	Название конфигурации LLDP, может быть пустым
Description	Описание конфигурации LLDP, может быть пустым
Apply	Подтверждение введенных параметров

Конфигурация порта LLDP:

1. Страница настройки порта LLDP появляется после включения глобальной конфигурации LLDP, как показано на Рисунке 83.

Port Configuration

[Batch Edit](#) [» LLDP State](#)

Name	State	Description	Agent Circuit ID	Locally Assigned	Chassis Type	Port ID Type	Management Address Type	Action
gigabitEthernet0/1	TxRx				mac-address	if-name	ip-address	Edit
gigabitEthernet0/2	TxRx				mac-address	if-name	ip-address	Edit

Рисунок 83 – Страница состояния LLDP port configuration

2. Нажмите кнопку «Batch Edit» под «Port Configuration» или «Edit» соответствующую порту, чтобы перейти на страницу конфигурации портов, как показано на Рисунке 84.

Port Configuration ⌵ ✕

State:

Chassis Type:

Description:

Port ID Type:

Agent Circuit ID:

Management Address Type:

Locally Assigned:

Basic Tlvs: ☒ port-description ☒ system-description ☒ management-address ☒ system-name ☒ system-capabilities

802.1 Tlvs: ☒ port-vlanid ☒ ptcl-identity ☐ vid-digest ☒ vlan-name ☒ port-ptcl-vlanid ☒ link-agg ☐ mgmt-vid

802.3 Tlvs: ☒ mac-phy ☒ max-mtu-size

Tx Hold:

Tx Interval:

Reinit Delay:

Fast Tx:

Tx Fast Init:

Tx Credit Max:

☒ Selected ☐ AG Port

☐ Copper ☐ Fiber

Рисунок 84 – Страница состояния LLDP port

Элемент	Описание
Description	Описание текущего настраиваемого порта LLDP
Agent Circuit ID	Идентификатор порта. Может использоваться как значение для port-id-tlv.
Locally Assigned	Локальное назначение
Admin Status	Disabled: пакеты LLDP не отправляются/не принимаются на интерфейсе TxOnly: пакеты LLDP отправляются на интерфейсе RxOnly: пакеты LLDP принимаются на интерфейсе TxRx: пакеты LLDP отправляются/принимаются на интерфейсе
Chassis Subtype	Mac-address: MAC-адрес If-alias: alias интерфейса If-name: имя интерфейса Ip-address: IP-адрес Locally-assigned: локальная конфигурация
Port ID Subtype	Mac-address: MAC-адрес If-alias: alias интерфейса If-name: имя интерфейса Ip-address: IP-адрес Agt -circuit-id: agt-circuit-id Locally-assigned: значение локального назначения
Management Address Subtype	Mac-адрес: MAC-адрес устройства Ip-адрес: IP-адрес устройства
Basic Tlvs	port-description: описание порта system-description: системное описание management-address: адрес управления system-name: системное имя system-capabilities: поддерживаемые возможности системы соседних устройств
802.1 Tlvs	port-vlanid: vlanid порта

	ptcl -identity: id протокола vid-digest: vid digest vlan-name: имя vlan port-ptcl - vlanid: vlanid протокола порта link- agg mgmt -vid: vid управления агрегацией каналов
802.3 Tlvs	mac-phy: скорость и дуплексный статус поддерживаемые портом, поддерживает ли он автоматическое согласование скорости порта, включена ли функция автоматического согласования, а также текущая скорость и дуплексный статус max - mtu -size: максимальное значение mtu
Tx hold	Задержка передачи, значение по умолчанию txFastInit равно 4, используется для расчета TTL пакета; $TTL = msgTxInterval * msgTxHold + 1$
Tx interval	Интервалы передачи, по умолчанию 30 сек.; может быть изменено на любое значение от 5 до 300 сек.
Reinit delay	Величина задержки между моментом, когда adminStatus становится «disabled», и попыткой повторной инициализации. Значение reinitDelay по умолчанию - 2 сек.
Fast tx	Определяет временной интервал для интервала таймера между двумя передачами в течение периода быстрой передачи (если txFast не равен нулю). Значение по умолчанию для msgFastTx равно 1; может быть изменено на любое значение от 1 до 3600.
Tx fast init	Переменная используется как начальное значение переменной txFast. Это значение определяет количество LLDPDU, переданных в течение периода быстрой передачи.
Tx credit max	Максимальное значение txCredit. Значение по умолчанию - 5.; может быть изменено на любое значение от 1 до 10.

Просмотр состояния LLDP:

На текущей странице нажмите кнопку «State LLDP», чтобы перейти на страницу состояния LLDP, как показано на Рисунке 85.

Name	Tx	Aged	Rx	Rx Errors	Discards	Discard Tlvs	Unknown Tlvs	Action
gigabitEthernet0/1	29	0	1	0	0	0	0	Clear Neighbor

Рисунок 85 – Страница статистики LLDP port

Элемент	Описание
Name	Описание текущего настроенного LLDP порта
Tx	Количество пакетов, отправленных на интерфейс
Aged	Количество устаревших пакетов на интерфейсе
Rx	Количество пакетов, полученных на интерфейсе
Rx Errors	Количество пакетов с ошибками, полученных на интерфейсе
Discards	Количество пакетов, отброшенных на интерфейсе
Discard Tlvs	Количество пакетов tlv, отброшенных на интерфейсе
Unknown Tlvs	Количество неизвестных пакетов tlvs на интерфейсе
CLEAR	Очистить счетчики на текущем интерфейсе

Просмотр информации о соседях:

На странице текущего состояния LLDP порта нажмите кнопку «Neighbor», чтобы войти в интерфейс просмотра информации о соседях, как показано на Рисунке 86.

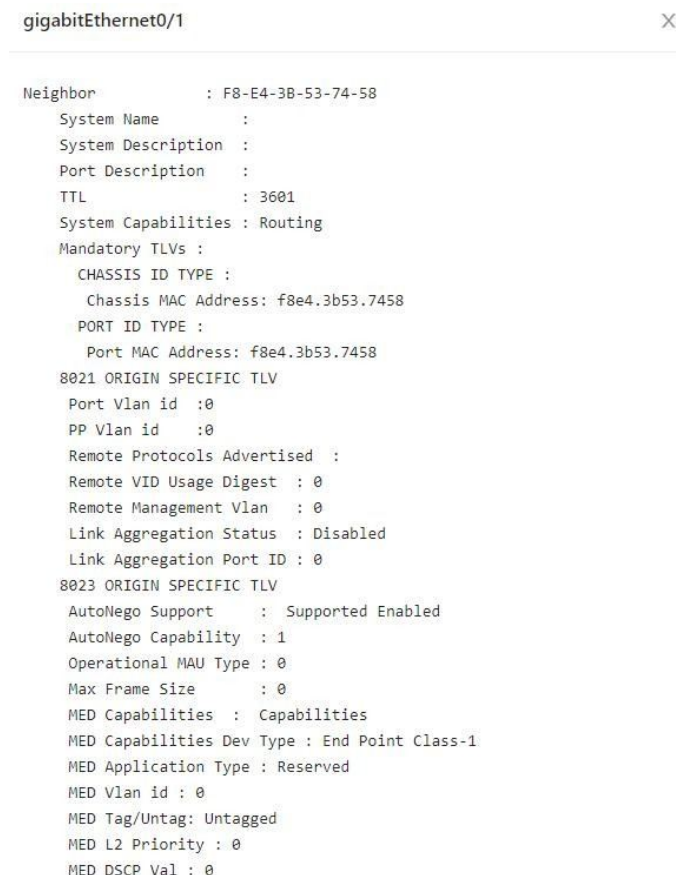


Рисунок 86 – Страница интерфейса просмотра информации о соседях

4.2. IGMP Snooping

IGMP snooping (Internet Group Management Protocol snooping) — это функция, используемая в коммутаторах для оптимизации передачи мультикаст-трафика в локальных сетях (LAN). Она позволяет коммутатору "подслушивать" (snoop) сообщения IGMP, которые отправляются хостами для управления членством в мультикаст-группах.

4.2.1. Принцип IGMP Snooping

В локальной сети многоадресные пакеты должны проходить через коммутаторы уровня 2 между маршрутизатором и пользователями многоадресной рассылки. Однако многоадресные пакеты могут транслироваться всем хостам в широковещательном домене, включая не входящих членов группы без многоадресной рассылки, так как коммутатор уровня 2 не может узнать многоадресные MAC-адреса. Это приводит к потере пропускной способности сети и угрожает информационной безопасности сети.

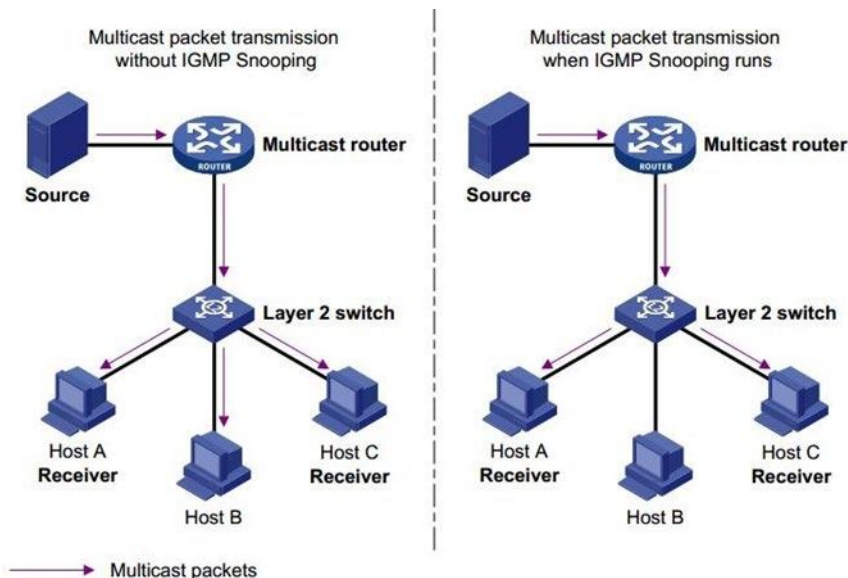


Рисунок 87 – Многоадресная передача пакетов до и после IGMP Snooping.

4.2.2. Конфигурация IGMP Snooping

4.2.2.1. Глобальная конфигурация

Выберите «Advance» - «Layer2» - «IGMP Snooping Configuration» в дереве навигации для перехода на страницу глобальной конфигурации, как показано на Рисунке 88.

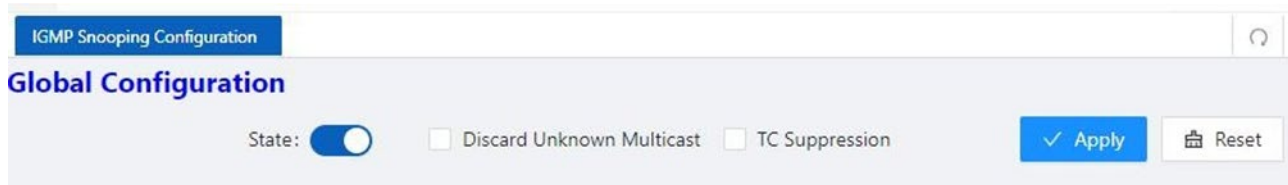


Рисунок 88 – Страница IGMP Snooping Global Configuration

Элемент		Описание
Global Configuration	State	Disabled: Отключение функции IGMP Snooping Enabled: Включение функции IGMP Snooping
	Discard Unknown Multicast	Если эта опция включена, неизвестный многоадресный трафик будет отброшен коммутатором
	TC Suppression	Если эта опция включена, событие изменения топологии будет проигнорировано коммутатором

4.2.2.2. Конфигурация IGMP M-router Interface

1. Выберите «Advance» - «Layer2» - «IGMP Snooping Configuration» в дереве навигации для перехода на страницу IGMP M-router Interface, как показано на Рисунке 89.

IGMP Snooping Configuration

Global Configuration

State: ☒ Discard Unknown Multicast ☐ TC Suppression

Apply Reset

Рисунок 89 – Страница IGMP M-router Interface Configuration

Элемент		Описание
IGMP M-router Interface	VID	VLAN ID
	Interface	Имя интерфейса
	Delete	Удалить запись

- Нажмите кнопку «+Add» чтобы перейти к настройке IGMP M-router Interface, введите значения в поля «Vid», «Interface», нажмите кнопку «ОК», как показано на Рисунке 90.

M-router Interface

* VID:

* Interface:

Рисунок 90 – Страница создания IGMP M-router Interface

4.2.2.3. Конфигурация IGMP Static Group

- Выберите «Advance» - «Layer2» - «IGMP Snooping Configuration» в дереве навигации для перехода на страницу IGMP Static Group, как показано на Рисунке 91.

Static Group

+Add

IGMP Snooping State

VID	Group Address	Source Address	Interface	Action
No Data				

Рисунок 91 – Страница IGMP Static Group Configuration

Элемент		Описание
IGMP Static Group	VID	VLAN ID
	Group Address	IP-адрес группы
	Source Address	IP-адрес источника

	Interface	Имя интерфейса
	Delete	Удалить запись

2. Нажмите кнопку «+Add» чтобы перейти к настройке IGMP Static Group, введите значения в поля «Vid», «Group Address», «Source Address», «Interface», нажмите кнопку «ОК», как показано на Рисунке 92.

Рисунок 92 – Страница создания IGMP Static Group

4.3. Управление MAC-адресами

4.3.1. Введение

Таблица MAC - это таблица соответствий между MAC-адресами устройств назначения и портами коммутатора. MAC-адреса могут быть статические и динамические. Статические MAC-адреса настраиваются пользователем вручную, имеют наивысший приоритет, хранятся постоянно и не могут быть перезаписаны динамическими MAC-адресами. MAC-адреса - это записи, полученные коммутатором в пересылке кадров данных, и хранятся в течение ограниченного периода времени. Когда коммутатор получает кадр данных для дальнейшей передачи, он сохраняет MAC-адрес кадра данных вместе с соответствующим ему портом назначения. Когда MAC-таблица опрашивается для поиска MAC-адреса назначения, при нахождении нужного адреса кадр данных отправляется на соответствующий порт, иначе коммутатор отправляет кадр на широковещательный домен. Если динамический MAC-адрес не встречается в принятых кадрах данных длительное время, запись о нем будет удалена из MAC-таблицы коммутатора.

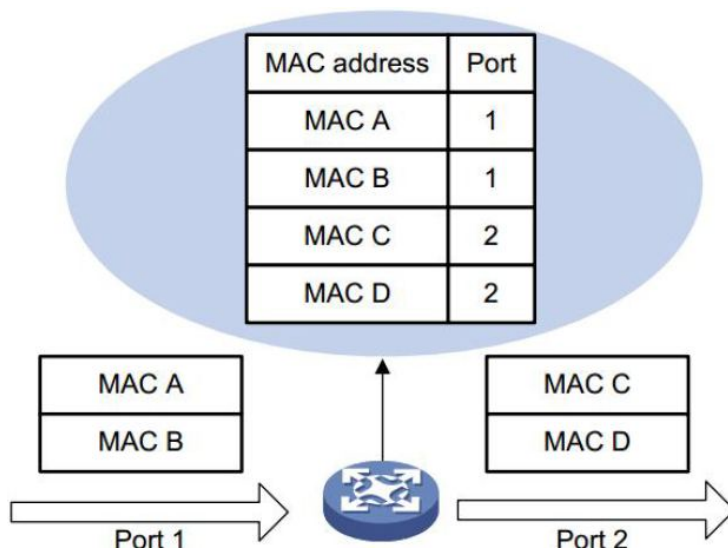


Рисунок 93 – Таблица MAC-адресов устройства

4.3.2. Конфигурация MAC-адресов

Конфигурация MAC-адресов включает в себя настройку и отображение статического «MAC address», «Filter MAC Address», и установку времени устаревания записи «MAC address».

Глобальная конфигурация MAC-адресов:

Выберите «Advance» - «Layer2» - «MAC Configuration» в дереве навигации для перехода на страницу глобальной конфигурации MAC, как показано на Рисунке 94.

Рисунок 94 – Страница MAC Global Configuration

Элемент		Описание
Global configuration	Aging time	Время старения для MAC-адреса, значение по умолчанию -300 сек.
	Apply	Подтверждение введенных параметров

Конфигурация статического MAC-адреса:

1. Выберите «Advance» - «Layer2» - «MAC Configuration» в дереве навигации для перехода на страницу конфигурации Static MAC Address, как показано на Рисунке 95.

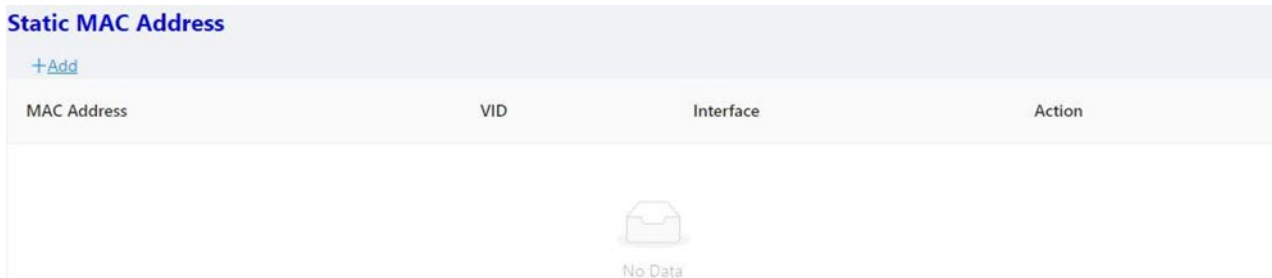


Рисунок 95 – Страница Static MAC Address Configuration

2. Нажмите кнопку «+Add» чтобы перейти к настройке Static MAC Address, введите значение в поле «MAC address», выберите в выпадающих списках «VID» и «Interface» необходимые значения, нажмите кнопку «ОК» как показано на Рисунке 96.

Рисунок 96 – Страница создания Static MAC Address

Элемент		Описание
Static Mac Address	MAC Address	MAC-адрес
	VID	Идентификатор VLAN, к которой принадлежит MAC-адрес.
	Interface	Порт, к которому принадлежит MAC-адрес.

Конфигурация фильтрации MAC-адреса:

1. Выберите «Advance» - «Layer2» - «MAC Configuration» в дереве навигации, система автоматически отобразит страницу Filter MAC Address, как показано на Рисунке 97.

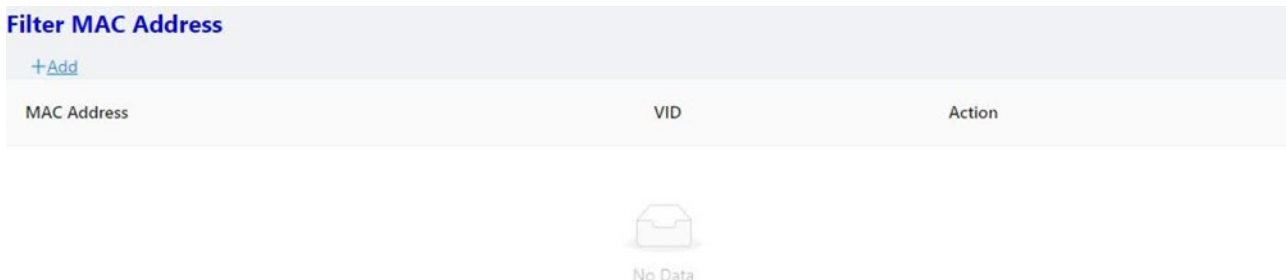


Рисунок 97 – Страница Filter MAC Address Configuration

2. Нажмите кнопку «+Add» чтобы перейти к настройке Filter MAC Address, введите значение в поле «MAC address», выберите в выпадающем списке «VID» необходимое значение, нажмите кнопку «OK» как показано на Рисунке 98.

Рисунок 98 – Страница создания Filter MAC Address

Элемент		Описание
Static Mac Address	MAC Address	MAC-адрес
	VID	Идентификатор VLAN, к которой принадлежит MAC-адрес.

4.4. DHCP Snooping

4.4.1. Введение

DHCP snooping - это функция безопасности, с помощью которой коммутатор контролирует процесс получения DHCP-клиентом IP-адреса для предотвращения атак DHCP и появления не легитимных DHCP-серверов в сети, устанавливая доверенные и недоверенные порты. Сообщения из доверенных портов передаются коммутатором без проверки. Обычно, доверенные порты используются для подключения DHCP-сервера или DHCP relay, а недоверенные - для подключения DHCP-клиентов. Коммутатор передает сообщения DHCP-запросов из недоверенных портов, но не передает DHCP-ответы. Кроме того, при получении DHCP-ответа из недоверенного порта, коммутатор может выполнить предварительно настроенное действие: shutdown или blackhole. Если включена функция DHCP Snooping Binding, то после каждого успешного получения IP адреса через DHCP коммутатор создаст запись в таблице, которая свяжет полученный IP-адрес с MAC-адресом DHCP-клиента, номером его VLAN и порта. С помощью этой информации можно реализовать контроль доступа пользователей.

4.4.2. Конфигурация DHCP Snooping

Глобальная конфигурация DHCP Snooping:

Выберите «Advance» - «Layer2» - «DHCP Snooping» в дереве навигации для перехода на страницу глобальной конфигурации DHCP Snooping, как показано на Рисунке 99.

DHCP Snooping Configuration

Global Configuration

Status: ☐

* VLAN list:

Verify mac-address: ☐

Option-82: ☐

DB write-delay(second):

✓ Apply

Reset

Рисунок 99 – Страница DHCP Snooping Global Configuration

Элемент	Описание
Status	Включить/выключить DHCP Snooping
Vlan	Включить/выключить DHCP Snooping для vlan
Verify mac-address	Проверка совпадения исходного MAC-адреса и адреса оборудования клиента в пакетах DHCP
option-82	Включить/выключить option-82
DB write-delay(s)	Интервал времени записи базы данных во флэш-память в секундах.

Конфигурация портов DHCP Snooping:

1. Выберите «Advance» - «Layer2» - «DHCP Snooping» в дереве навигации для перехода на страницу конфигурации портов DHCP Snooping, как показано на Рисунке 100.

Port Configuration

[Batch Edit](#)
[» DHCP Snooping State](#)

Name	Trust	Ratelimit(pps)	Action
gigabitEthernet0/1	Disable		Edit
gigabitEthernet0/2	Disable		Edit

Рисунок 100 – Страница DHCP Snooping Global Configuration

2. Нажмите кнопку «Batch Edit» под «Port Configuration» или «Edit» соответствующую порту, чтобы перейти на страницу конфигурации портов, как показано на Рисунке 101.

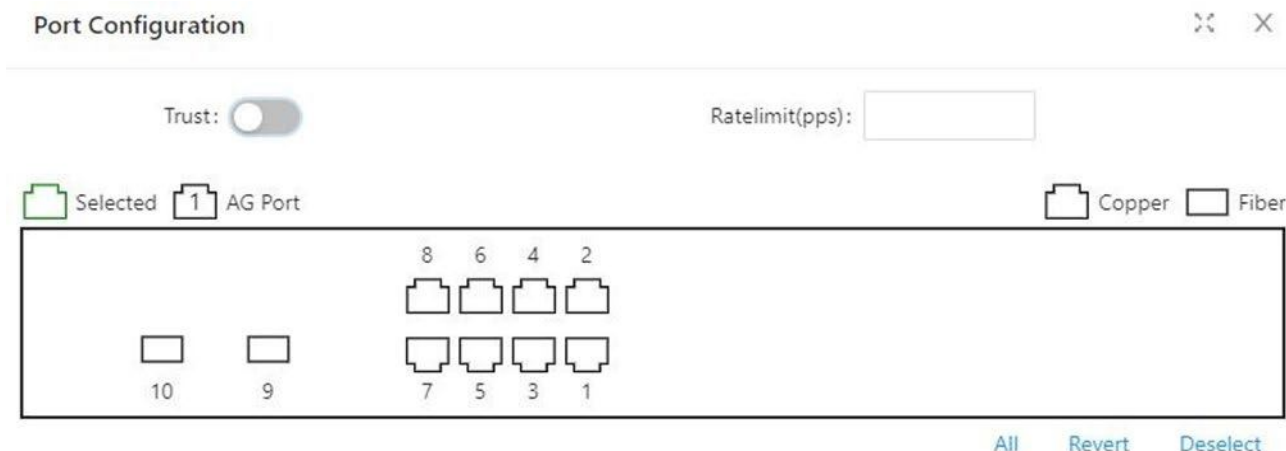


Рисунок 101 – Страница DHCP Snooping Global Configuration

Элемент	Описание
Trust	Определяет, являются ли источники трафика доверенными или нет
Ratelimit(pps)	Количество пакетов DHCP в секунду, которые может получить интерфейс

Просмотр состояния DHCP Snooping:

Нажмите кнопку «DHCP Snooping state» на текущей странице, чтобы перейти на страницу состояния DHCP Snooping, как показано на Рисунке 102.

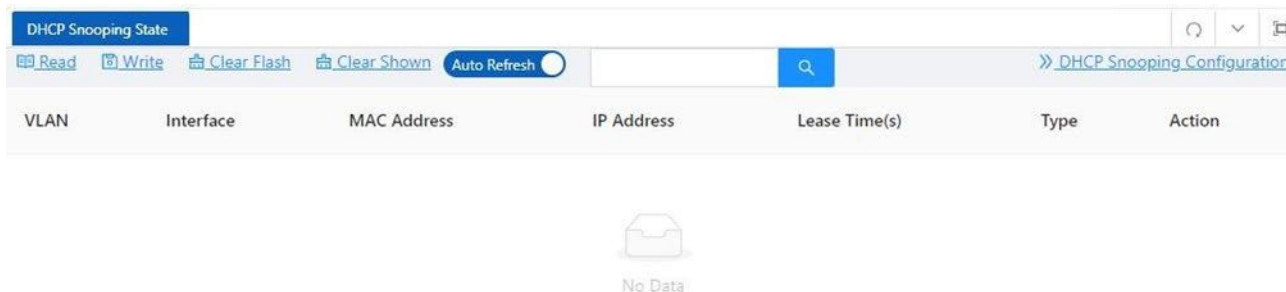


Рисунок 102 – Страница DHCP Snooping State

Элемент	Описание
Search	Поиск записей в базе данных
WRITE	Сохранить записи в базу данных
READ	Чтение записей из базы данных
CLEAR	Очистка записей базы данных

4.5. QinQ

4.5.1. Введение

QinQ (IEEE 802.1QinQ) - расширение к стандарту IEEE 802.1Q, описывающее как тегированный трафик может передаваться внутри уже тегированного по 802.1Q трафика. Поскольку в сетях растет число пользователей, которым требуется большое количество идентификаторов VLAN. Традиционная маркировка VLAN, использующая IEEE 802.1Q, не может идентифицировать и изолировать данные пользователей при расширении работы городской сети Ethernet. Поэтому QinQ используется для расширения номеров VLAN до 4096×4096 , что позволяет эффективно сохранять общедоступные идентификаторы VLAN.

Пакеты QinQ имеют фиксированный формат. Обычно тегированный пакет 802.11Q инкапсулируется в другой тег 802.1Q, от которого происходит название «QinQ». Во время передачи пакеты пересылаются на основе тега внешней VLAN в общедоступной сети. Внутренний тег VLAN используется как данные, которые также передаются в общедоступной сети. С этой формой двойного тега пакеты QinQ имеют на четыре байта больше, чем обычные пакеты с тегами 802.1Q VLAN.

Существует два типа реализаций QinQ - базовый QinQ и выборочный QinQ.

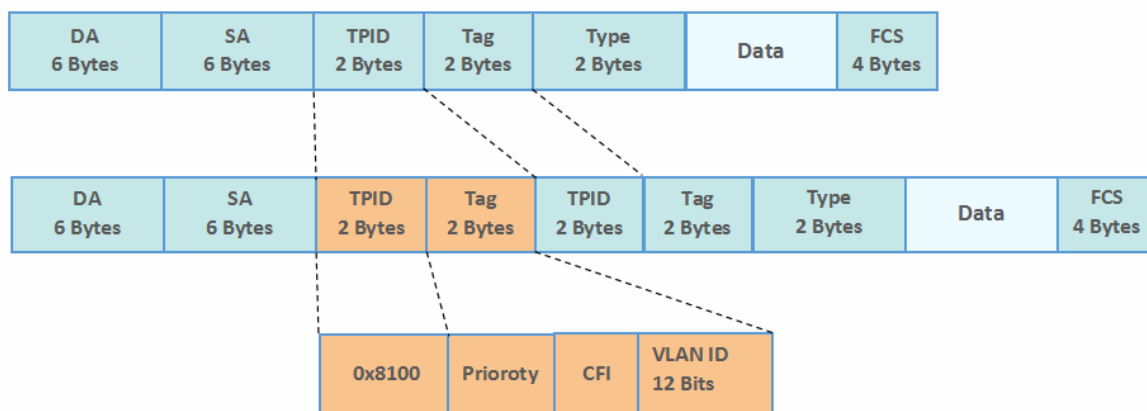


Рисунок 103 – QinQ и VLAN

Базовый QinQ - это способ тегирования на основе порта. Когда пакет прибывает на интерфейс, на котором включена VLAN VPN, коммутатор помечает пакет своим тегом VLAN по умолчанию. Не имеет значения, помечен входящий пакет или нет. Если он был помечен, то он будет иметь двойные теги VLAN; в противном случае у него будет один тег VLAN с портом коммутатора.

Селективный QinQ владеет функциями базового QinQ, но он более гибкий. Он может идентифицировать внутренний тег VLAN пакетов в соответствии с MAC-адресом, IP-протоколом, исходным IP-адресом и тегом VLAN, а затем определять, какой тег следует добавить.

4.5.2. Конфигурация QinQ

Конфигурация VPN:

1. Выберите «Advance» - «Layer2» - «QinQ configuration» в дереве навигации, система автоматически отобразит страницу VPN Configuration, как показано на Рисунке 104.

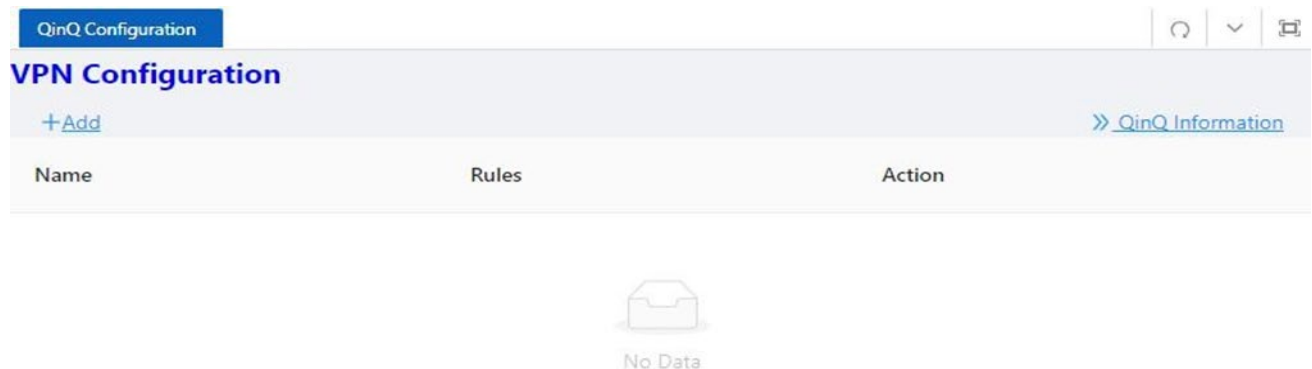


Рисунок 104 – Страница сводной информации QinQ VPN Configuration

2. Нажмите кнопку «+Add» под «VPN Configuration», чтобы перейти к настройке правил VPN, как показано на Рисунке 105.



Рисунок 105 – Страница QinQ VPN Configuration

Элемент	Описание
Name	Имя VLAN VPNRule
CVID	Идентификатор VLAN клиента
SVID	Идентификатор VLAN поставщика услуг

Конфигурация порта QinQ:

1. Выберите «Advance» - «Layer2» - «QinQ configuration» в дереве навигации, система автоматически отобразит страницу Port Configuration, как показано на Рисунке 106.

Port Configuration

Batch Edit	» QinQ Information			
Name	Basic	VLAN Stacking	VLAN Mapping	Action
gigabitEthernet0/1	Disable			Edit
gigabitEthernet0/2	Disable			Edit

Рисунок 106 – Страница сводной информации QinQ Port Configuration

- Нажмите кнопку «Batch Edit» под «Port Configuration» или «Edit» соответствующую порту, чтобы перейти на страницу конфигурации портов QinQ, как показано на Рисунке 107.

Port Configuration

Basic: ☐

VLAN Stacking:

VLAN Mapping:

Selected

1 AG Port

Copper ☐

Fiber ☐

8 6 4 2

10 9

7 5 3 1

All

Revert

Deselect

Рисунок 107 – Страница QinQ Port Configuration

Элемент	Описание
Basic	Включить режим VLAN mapping
VLAN Stacking	Многоуровневый режим тегов
VLAN Mapping	Режим замены тегов

4.6. ACL

ACL (Access Control List) - это механизм фильтрации IP-пакетов, позволяющий контролировать сетевой трафик, разрешая или запрещая прохождение пакетов на основе заданных признаков. Пользователь может самостоятельно задать критерии фильтрации ACL и применить фильтр на входящее по отношению к коммутатору направление трафика.

83

www.nikomax.ru

info@nikomax.ru

8 800 333-54-86

Производитель оставляет за собой право изменять внешний вид и характеристики товара, не снижая его потребительских свойств

4.6.1. Введение

4.6.2. Конфигурация ACL

Конфигурация правил для IP ACL:

1. Выберите «Advance» - «Security» - «ACL Configuration» в дереве навигации.
2. Нажмите кнопку «+Add ACL», чтобы перейти к настройке правил, выберите ACL тип «IP» для базового ACL, как показано на Рисунке 108.

Рисунок 108 – Страница ACL IP Configuration

Элемент		Описание
ACL Type	IP	ACL стандартного IP
Name		Номер правила, от 1 до 99 или от 1300 до 1999
Type	Permit	Позволяет передавать соответствующие пакеты
	Deny	Позволяет отбрасывать соответствующие пакеты
Source		IP-адрес источника
Source Mask		Маска IP-адреса меняется на противоположную. Если она совпадает с первыми 24 битами IP-адреса, маска будет 255.255.255.0, в таком случае необходимо указать значение маски 00.00.00.255.

3. Настройте правило для базового ACL и нажмите «OK».
4. Нажмите кнопку «Batch Edit» под «Port Configuration» или «Edit» соответствующую порту, чтобы перейти на страницу конфигурации ACL порта, как показано на Рисунке 109.

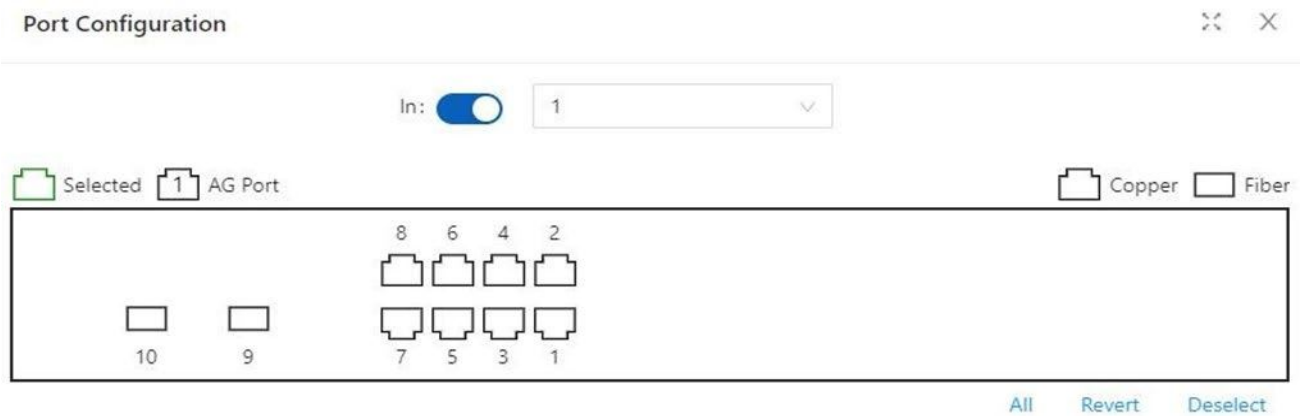


Рисунок 109 – Страница применения правил ACL к порту.

Конфигурация правил для IP-Extend ACL:

- 1. Выберите «Advance» - «Security» - «ACL Configuration» в дереве навигации.
- 2. Нажмите кнопку «+Add ACL», чтобы перейти к настройке правил, выберите ACL тип «IP-Extend» для базового ACL, как показано на Рисунке 110.

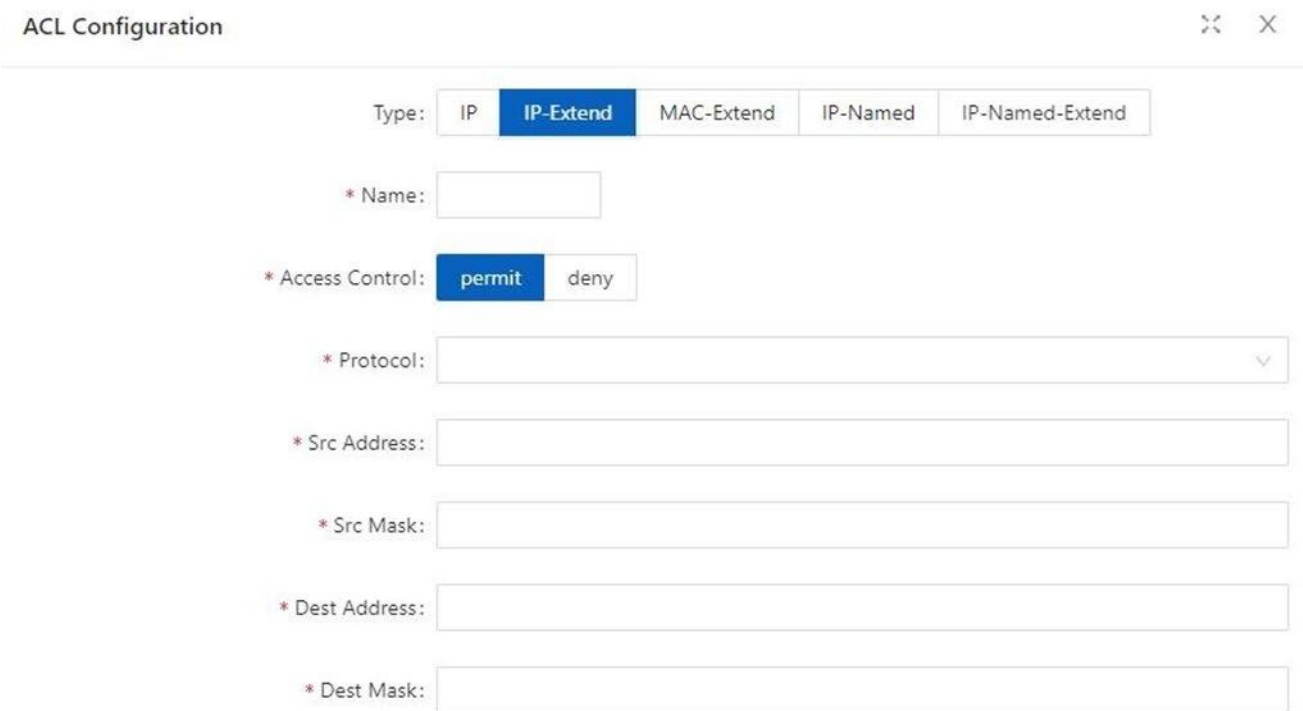


Рисунок 110 – Страница ACL IP-Extend Configuration

Элемент		Описание
ACL Type	IP-Extend	Extend ACL, сопоставление протокола, исходного IP-адреса и IP-адреса назначения пакетов IPv4
Name		Номер правила, от 1 до 99 или от 2000 до 2699

Type	Permit	Позволяет передавать соответствующие пакеты
	Deny	Позволяет отбрасывать соответствующие пакеты
Protocol		Поддержка общих параметров сообщений протокола, включая tcp, udp, vrrp, igmp, gre, ipcomp, ospf, pim, rsrp и т. д. Поддержка пакетов IPv4
Source		IP-адрес источника
Source Mask		Маска IP-адреса меняется на противоположную. Если она совпадает с первыми 24 битами IP-адреса, маска будет 255.255.255.0, в таком случае необходимо указать значение маски 00.00.00.255.
Destination		IP-адрес назначения
Destination Mask		Маска подсети для IP-адреса назначения. Маска IP-адреса обратная.

3. Настройте правило для базового ACL и нажмите «ОК».
4. Нажмите кнопку «Batch Edit» под «Port Configuration» или «Edit» соответствующую порту, чтобы перейти на страницу конфигурации ACL порта и нажмите «ОК».

Конфигурация правил для MAC-Extend ACL:

1. Выберите «Advance» - «Security» - «ACL Configuration» в дереве навигации.
2. Нажмите кнопку «+Add ACL», чтобы перейти к настройке правил, выберите ACL тип «MAC-Extend» для базового ACL, как показано на Рисунке 111.

ACL Configuration
✕ ✕

Type:
☐ IP
☐ IP-Extend
☒ MAC-Extend
☐ IP-Named
☐ IP-Named-Extend

* Name:

* Access Control:
☒ permit
☐ deny

* Src Address:

* Src Mask:

* Dest Address:

* Dest Mask:

Рисунок 111 – Страница ACL MAC-Extend Configuration

Элемент		Описание
ACL Type	MAC-Extend	Extended MAC ACL для сопоставления исходного MAC-адреса уровня 2 и MAC-адреса назначения
Name		Номер правила, от 200 до 699
Type	Permit	Позволяет передавать соответствующие пакеты
	Deny	Позволяет отбрасывать соответствующие пакеты
Source		IP-адрес источника
Source Mask		Маска IP-адреса меняется на противоположную. Если она совпадает с первыми 24 битами IP-адреса, маска будет 255.255.255.0, в таком случае необходимо указать значение маски 00.00.00.255.
Destination		IP-адрес назначения
Destination Mask		Маска подсети для IP-адреса назначения. Маска IP-адреса обратная.

3. Настройте правило для базового ACL и нажмите «ОК».
4. Нажмите кнопку «Batch Edit» под «Port Configuration» или «Edit» соответствующую порту, чтобы перейти на страницу конфигурации ACL порта и нажмите «ОК».

Конфигурация правил для IP-Named ACL:

1. Выберите «Advance» - «Security» - «ACL Configuration» в дереве навигации.
2. Нажмите кнопку «+Add ACL», чтобы перейти к настройке правил, выберите ACL тип «IP-Named» для базового ACL, как показано на Рисунке 112.

The screenshot shows the 'ACL Configuration' window. At the top, there are tabs for 'Type': IP, IP-Extend, MAC-Extend, **IP-Named** (selected), and IP-Named-Extend. Below the tabs, there are several fields with red asterisks indicating required fields:

- * Name: An empty text input field.
- * Access Control: Two buttons, 'permit' (selected) and 'deny'.
- * Src Address: An empty text input field.
- * Src Mask: An empty text input field.

Рисунок 112 – Страница ACL IP-Named Configuration

Элемент		Описание
ACL Type	IP-Named	Стандартный ACL, поддержка именования имен, первый символ должен быть буквой
Name		Строка, начинающаяся с буквы
Type	Permit	Позволяет передавать соответствующие пакеты
	Deny	Позволяет отбрасывать соответствующие пакеты
Source		IP-адрес источника
Source Mask		Маска IP-адреса меняется на противоположную. Если она совпадает с первыми 24 битами IP-адреса, маска будет 255.255.255.0, в таком случае необходимо указать значение маски 00.00.00.255.

3. Настройте правило для базового ACL и нажмите «ОК».
4. Нажмите кнопку «Batch Edit» под «Port Configuration» или «Edit» соответствующую порту, чтобы перейти на страницу конфигурации ACL порта и нажмите «ОК».

Конфигурация правил для IP-Name-Extend ACL:

1. Выберите «Advance» - «Security» - «ACL Configuration» в дереве навигации.
2. Нажмите кнопку «+Add ACL», чтобы перейти к настройке правил, выберите ACL тип «IP-Name-Extend» для базового ACL, как показано на Рисунке 113.

The screenshot shows the 'ACL Configuration' window. At the top, there are tabs for 'Type': IP, IP-Extend, MAC-Extend, IP-Named, and IP-Named-Extend (which is selected). Below the tabs, there are several fields with red asterisks indicating required fields: 'Name' (text input), 'Access Control' (radio buttons for 'permit' and 'deny', with 'permit' selected), 'Protocol' (dropdown menu), 'Src Address' (text input), 'Src Mask' (text input), 'Dest Address' (text input), and 'Dest Mask' (text input).

Рисунок 113 – Страница ACL IP-Name-Extend Configuration

Элемент		Описание
ACL Type	IP-Name-Extend	Extended ACL, поддержка именования имен, первый символ должен быть буквой
Name		Строка, начинающаяся с буквы
Type	Permit	Позволяет передавать соответствующие пакеты
	Deny	Позволяет отбрасывать соответствующие пакеты
Protocol		Поддержка общих параметров сообщений протокола, включая tcp, udp, vrrp, igmp, gre, ipcomp, ospf, pim, rsvp и т. д. Поддержка пакетов IPv4
Source		IP-адрес источника
Source Mask		Маска IP-адреса меняется на противоположную. Если она совпадает с первыми 24 битами IP-адреса, маска будет 255.255.255.0, в таком случае необходимо указать значение маски 00.00.00.255.
Destination		IP-адрес назначения
Destination Mask		Маска подсети для IP-адреса назначения. Маска IP-адреса обратная.

3. Настройте правило для базового ACL и нажмите «ОК».
4. Нажмите кнопку «Batch Edit» под «Port Configuration» или «Edit» соответствующую порту, чтобы перейти на страницу конфигурации ACL порта и нажмите «ОК».

4.7. QoS

4.7.1. Введение

QoS (Quality of Service) - это набор возможностей, которые позволяют логически разделять проходящий по сети трафик на основании критериев и управлять качеством каждого типа трафика, обеспечивая лучший сервис для выбранного трафика. QoS обеспечивает гарантию предсказуемого сервиса передачи данных для выполнения требований программ. QoS не генерирует дополнительную полосу, но обеспечивает более эффективное управление существующей пропускной способностью в соответствии с требованиями приложений и политикой управления сетью.

4.7.2. Конфигурация QoS

Конфигурация QoS:

1. Выберите «Advance» - «Security» - «QoS Configuration» в дереве навигации, для перехода на страницу глобальной конфигурации QoS, как показано на Рисунке 114.

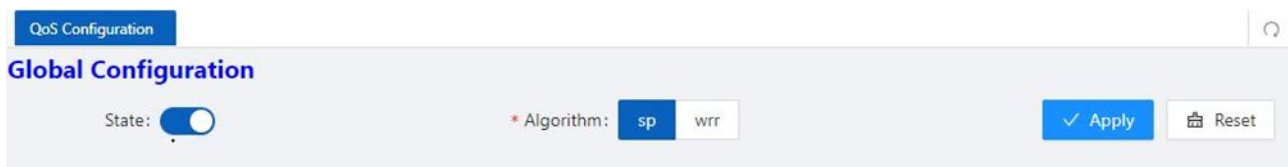


Рисунок 114 – Страница QoS Global Configuration

2. Нажмите кнопку «State», выберите «Algorithm» и нажмите «Apply», чтобы включить QoS.

Элемент			Описание
Qos Configuration	State		Включение функции QOS
	Algorithm	Sp	Строгий приоритет. Пока в более приоритетной очереди есть данные, которые необходимо передать, другие очереди не обрабатываются.
		Wrr	Для каждой очереди определяется вес. Из очередей по порядку берется кратное весу очереди число кадров.

Конфигурация QoS Mapping:

1. На текущей странице нажмите кнопку «Queue» под «Qos Mapping», чтобы перейти на страницу конфигурации QoS, как показано на Рисунке 115.

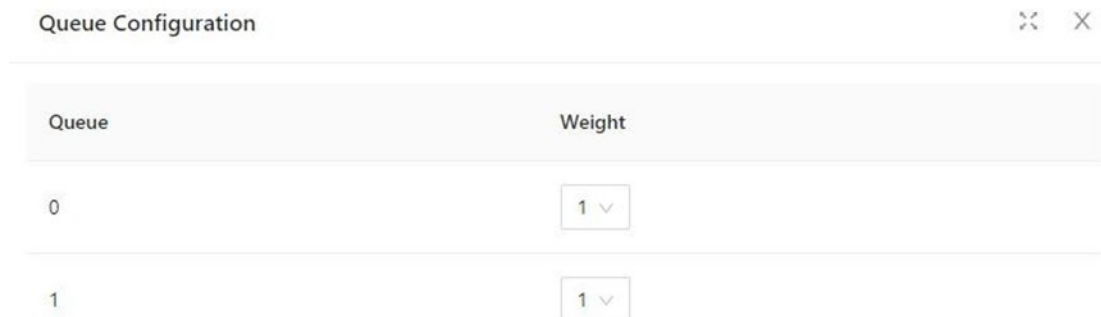


Рисунок 115 – Страница QoS Queue Configuration

Элемент		Описание
Queue weight	Queue	0 - 7
	Weight	0 - 32, чем больше значение, тем выше вес и вероятность преимущественной обработки пакетов в данной очереди в условиях загрузки канала, 0 означает бесконечность.

2. Нажмите кнопку «CoS» под «Qos Mapping», чтобы перейти на страницу конфигурации CoS, как показано на Рисунке 116.

CoS Configuration

CoS	Queue	DSCP
0	0	0
1	1	8

Рисунок 116 – Страница QoS Cos Configuration

Элемент		Описание
CoS Configuration	CoS	0 - 7
	Queue	0 – 7, Cos - отношение сопоставления очередей, на основе cos, указанного на порту, изменение очереди выхода пакетов вступает в силу, когда порт настроен как no trust, trust cos или trust dscp и non-ip packets.
	DSCP	Отношение сопоставления cos-dscp вступает в силу, когда порт настроен как no trust, trust cos или trust dscp и not ip packets. Измените значение packet dscp.

- Нажмите кнопку «DSCP» под «Qos Mapping», чтобы перейти на страницу конфигурации DSCP, как показано на Рисунке 117.

DSCP Configuration

[+Add](#)

DSCP	Queue	CoS	New DSCP	Action
 No Data				

Рисунок 117 – Страница QoS DSCP Configuration

Элемент		Описание
DSCP Map	DSCP	0 - 63
	Queue	0 – 7, отношение сопоставления dsp-queue, которое вступает в силу, когда порт настроен как trust dscp и ip packets, измените очередь экспорта пакетов

	CoS	0 – 7, отношение сопоставления dscp-cos, которое вступает в силу, когда порт настроен как trust dscp и ip packets, изменить поле cos пакета
	Nes DSCP	0 – 63, отношение сопоставления dscp-dscp, которое вступает в силу, когда порт настроен как trust dscp и ip packets, сначала выполните сопоставление dscp-dscp, а затем выполните сопоставление dscp-cos

Конфигурация Class:

На текущей странице нажмите кнопку «+Add» под «Class Setting», чтобы перейти на страницу Class Setting, как показано на Рисунке 118.

Class Setting

* Name:

* Match Type: acl etype dscp cos l4 vlan-range vlan

Рисунок 118 – Страница QoS Class Setting

Элемент		Описание
Class Setting	Name	Название категории
	Match	Тип соответствия, поддерживает связанный ACL; Поддержка соответствия пакетов etype, dscp, cos, l4port, полю vlan

Конфигурация Policy:

1. На текущей странице нажмите кнопку «+Add Policy» под «Policy Setting», чтобы перейти на страницу Policy Setting, как показано на Рисунке 119.

Policy Setting

* Name:

Рисунок 119 – Страница QoS Policy Setting

2. Нажмите кнопку «+Add Policy Ryle» под «Policy Setting», чтобы перейти на страницу Policy Setting, как показано на Рисунке 120.

Рисунок 120 – Страница QoS Rule Configuration

Элемент		Описание
Class Setting	Name	Название правила
	Class Name	Имя политики
	Modify	Политика, поддерживает изменение cos, dscp, vlan
	Ratelimit	Ограничение скорости
	CIR	Ограничение по скорости, кбит/с
	CBS	Размер всплеска, кбайт

Конфигурация Port:

На текущей странице нажмите кнопку «+Batch Edit» под «Port Configuration», чтобы перейти на страницу Port Configuration, как показано на Рисунке 121.

Рисунок 121 – Страница QoS Port Configuration

Элемент		Описание
Port Configuration	Default CoS	0 – 7, когда порт настроен как no trust или trust, но сообщение не соответствует условию доверия, для маркировки входящего сообщения используется cos порт по умолчанию
	Trust	Поддержка конфигурации untrust, trust cos, trust dscp. В режиме no trust этап входа изменяет поле cos и поле dscp сообщения в соответствии с cos по умолчанию порта; когда настроен trust cos, то же самое, что и режим no trust для немаркированных сообщений, а для тегированных сообщений выберите сообщение с собственным cos; При настройке trust dscp для ip packets выберите пакет с dscp, а для non-ip packets это то же самое, что и режим trust cos.
	Ingress Policy	Выберите политику входящего трафика

5. Maintenance

5.1. Конфигурация системы

Модуль System Configuration включает в себя настройки имени хоста, сервисов Telnet, SSH, HTTP, HTTPS, а также настройки IP-адреса управления.

5.1.1. Настройка имени хоста

Выберите «Maintenance» - «System Configuration» в дереве навигации, для перехода на страницу System Configuration, как показано на Рисунке 122.



Рисунок 122 – Страница System Configuration

5.1.2. Включение сервисов

Конфигурация сервисов:

1. Выберите «Maintenance» - «System Configuration» в дереве навигации, для перехода на страницу System Configuration, как показано на Рисунке 123.
2. Установите флажок напротив сервиса, нажмите кнопку «Apply», чтобы включить.
3. Если включен HTTPS Server, сертификат и ключ должны быть загружены. Если сертификат не указан, устройство будет использовать сертификат по умолчанию.

Service: ☐ Telnet ☐ SSH ☐ HTTP ☐ HTTPS

Рисунок 123 – Страница Service

5.1.3. IP-адрес управления

Выберите «Maintenance» - «System Configuration» в дереве навигации, для перехода на страницу System Configuration, как показано на Рисунке 124.

Рисунок 124 – Страница Management IP Information

Элемент	Описание
VID	VLAN ID управления, по умолчанию - 1
IPv4 Type	None: IP-адрес управления IPv4 не используется Static: Статический IP-адрес IPv4 DHCP: Получение IP-адреса IPv4 по DHCP
IPv4 Address	IP-адрес управления IPv4, по умолчанию - 192.168.56.166
IPv4 Mask	Маска IPv4, по умолчанию - 255.255.255.0
IPv4 Gateway	Шлюз управления IPv4, по умолчанию - 192.168.56.1
IPv6 Type	None: IP-адрес управления IPv6 не используется Static: Статический IP-адрес IPv6 DHCP: Получение IP-адреса IPv6 по DHCP

IPv6 Address	IP-адрес управления IPv6
IPv6 Prefix Length	Длина префикса IP-адреса IPv6
IPv6 Gateway	Шлюз управления IPv6

5.2. Управление файлами

Модуль File Management включает в себя функции базовой информации, управления программным обеспечением, конфигурацией и сертификатами.

5.2.1. Базовая информация

Выберите «Maintenance» - «File Management» - «Basic Information» в дереве навигации, для перехода на страницу Basic Information, как показано на Рисунке 125.



Рисунок 125 – Страница Basic Information

5.2.2. Управление программным обеспечением

Обновление программного обеспечения позволяет получить целевой файл с текущего хоста и установить этот файл в качестве основного загрузочного файла или резервного загрузочного файла для использования при следующей перезагрузке.

1. Выберите «Maintenance» - «File Management» - «Image Management» в дереве навигации, для перехода на страницу Image Management, как показано на Рисунке 126.

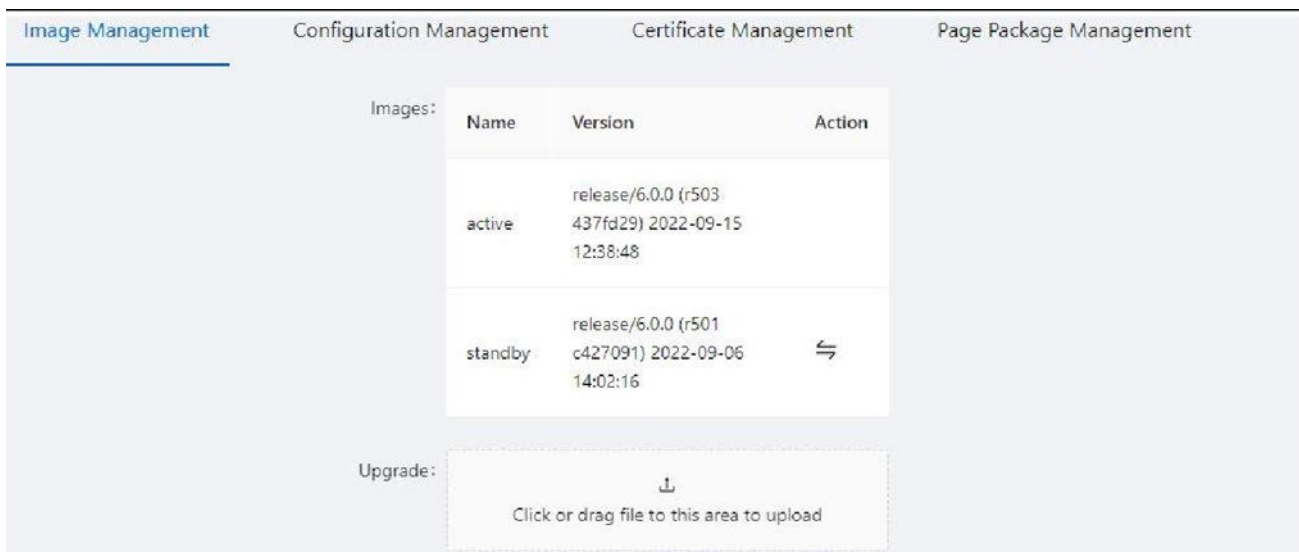


Рисунок 126 – Страница Image Management

2. Нажмите кнопку «Upgrade», в появившемся диалоговом окне выберите файл обновления, соответствующий устройству, файл обновления имеет формат *.bin. Процесс обновления показан на Рисунке 127, после завершения обновления устройство будет перезагружено.

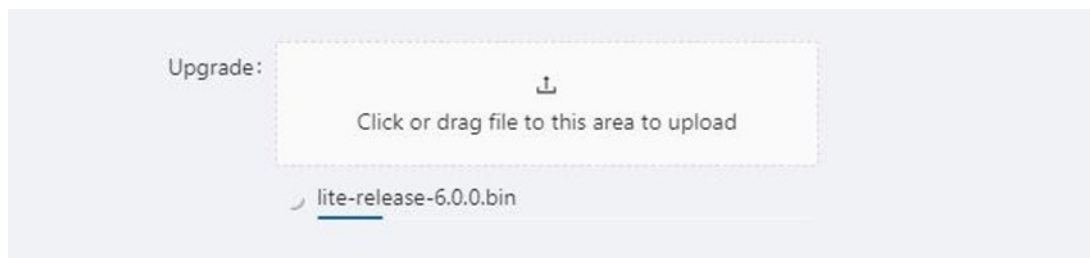


Рисунок 127 – Процесс обновления программного обеспечения

5.2.3. Управление конфигурацией

Выберите «Maintenance» - «File Management» - «Configuration Management» в дереве навигации, для перехода на страницу Configuration Management, как показано на Рисунке 128.

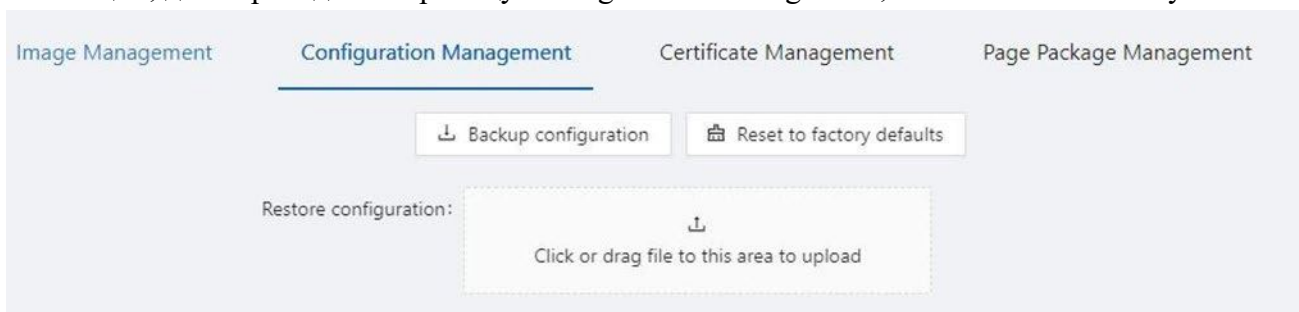


Рисунок 128 – Страница Configuration Management

Резервное копирование конфигурации:

Нажмите кнопку «Backup configuration» для сохранения файла конфигурации с устройства, вы можете сохранить файл локально.

Восстановление конфигурации:

Нажмите кнопку «Choose File» для загрузки файла конфигурации на устройство, выберите файл *.conf для загрузки, после чего устройство будет перезагружено.

Сброс к заводским настройкам:

Эта операция восстанавливает систему до заводских настроек, удаляет текущий файл конфигурации и перезагружает устройство.

Нажмите кнопку «Reset to Factory Defaults», чтобы применить эту операцию.

5.2.4. Управление сертификатами

При включении HTTPS вам необходимо загрузить сертификат и ключ, как показано на Рисунке 129. Если вы не укажете сертификат, устройство будет использовать сертификат по умолчанию.

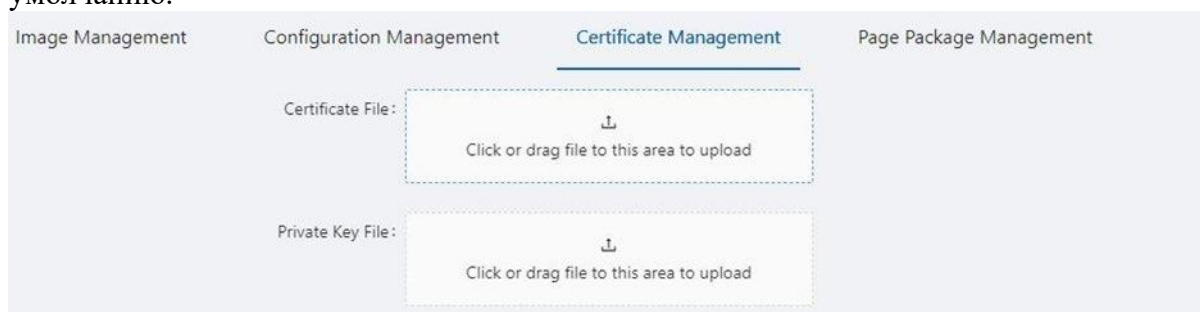


Рисунок 129 – Страница Certificate Management

5.2.5. Управление пакетами

Модуль Page Package Management предоставляет возможность получить целевой файл пакета страницы с локального хоста и применить файл в качестве файла пакета страницы устройства, как показано на Рисунке 130.

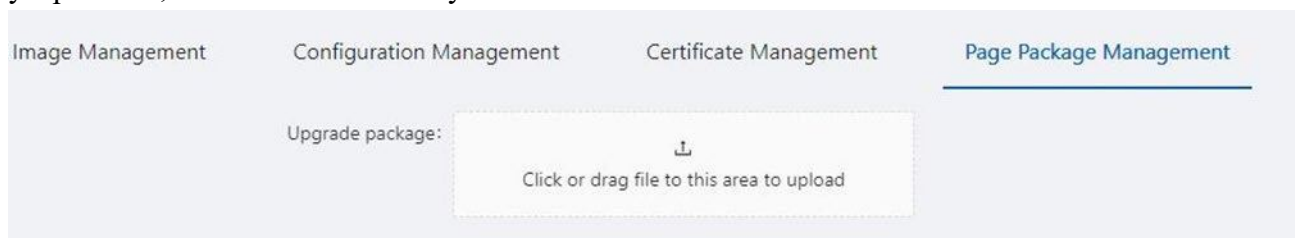


Рисунок 130 – Страница Page Package Management

5.3. Управление пользователями

Выберите «Maintenance» - «User Management» в дереве навигации, для перехода на страницу User Management, как показано на Рисунке 131.

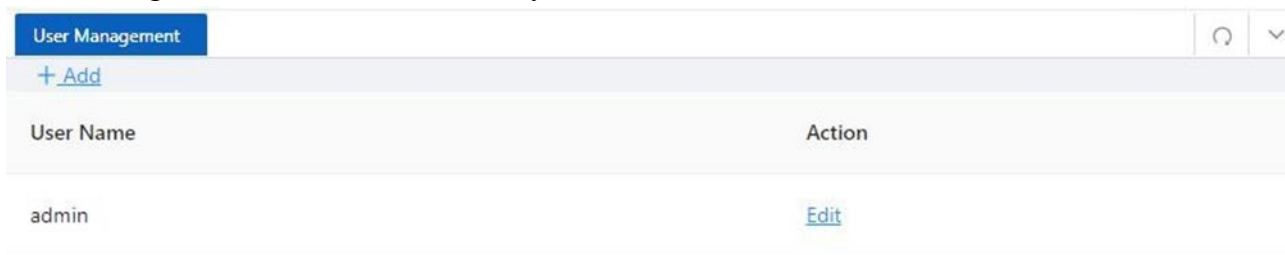


Рисунок 131 – Страница User Management

Элемент		Описание
Account	Name	Имя пользователя
	Edit	Редактировать пользователя
	Delete	Удалить пользователя
	+Add	Добавить пользователя

5.4. Управление системным временем

Модуль System Time позволяет отображать и устанавливать системное время устройства в веб-интерфейсе. Устройство поддерживает установку системного времени посредством ручной настройки и автоматической синхронизации времени сервера NTP.

5.4.1. Просмотр системного времени

Выберите «Maintenance» - «Time Management» в дереве навигации, для перехода на страницу Time Management, как показано на Рисунке 132.

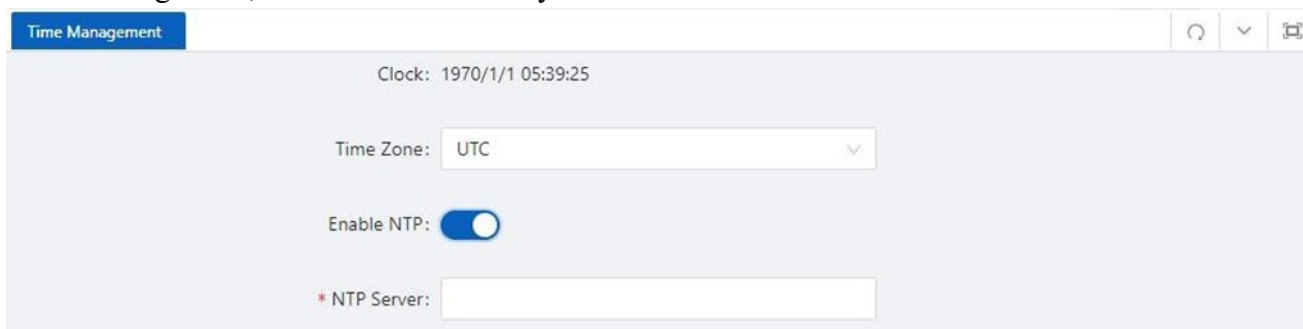


Рисунок 132 – Страница Time Management

Элемент	Описание
Clock	Системная дата и время
Time Zone	Часовой пояс
Enable NTP	Включить/Выключить NTP
NTP Server	IP-адрес NTP сервера

5.4.2. Конфигурация системного времени

1. Выберите «Maintenance» - «Time Management» в дереве навигации, для перехода на страницу Time Management.
2. Нажмите кнопку синхронизации позади часов, затем нажмите кнопку «Apply», как показано на Рисунке 133. Время ПК будет синхронизировано с коммутатором.
3. Нажмите «Save» во вспомогательной области.

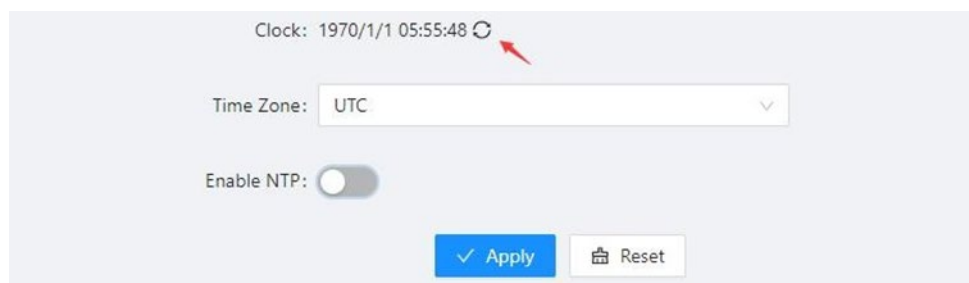


Рисунок 133 – Страница Time Management Configuration

5.4.3. Конфигурация NTP сервера

1. Выберите «Maintenance» - «Time Management» в дереве навигации, для перехода на страницу Time Management.
2. Включите NTP.
3. Введите адрес в поле IP-адрес NTP-сервера, как показано на Рисунке 134, нажмите кнопку «Apply».
4. Нажмите кнопку «Save» во вспомогательной области.

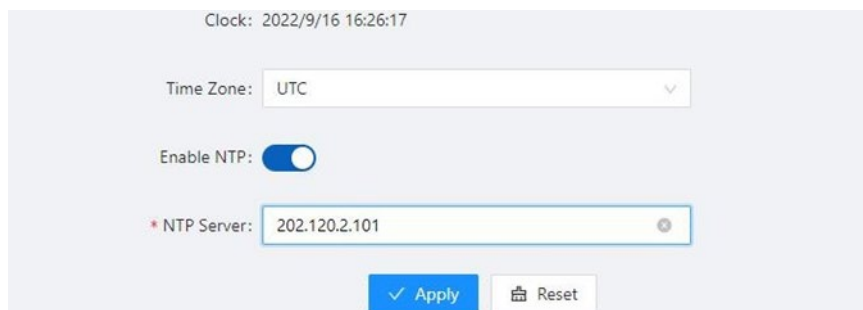


Рисунок 134 – Страница NTP Server Configuration

5.5. SNMP

5.5.1. Конфигурация SNMP

1. Выберите «Maintenance» - «SNMP» в дереве навигации, для перехода на страницу SNMP, как показано на Рисунке 135.
2. Выберите версию SNMP протокола, настройте пользователя, пароль шифрования аутентификации, укажите хост Trap и нажмите кнопку «Apply», чтобы завершить настройку.

Рисунок 135 – Страница SNMP

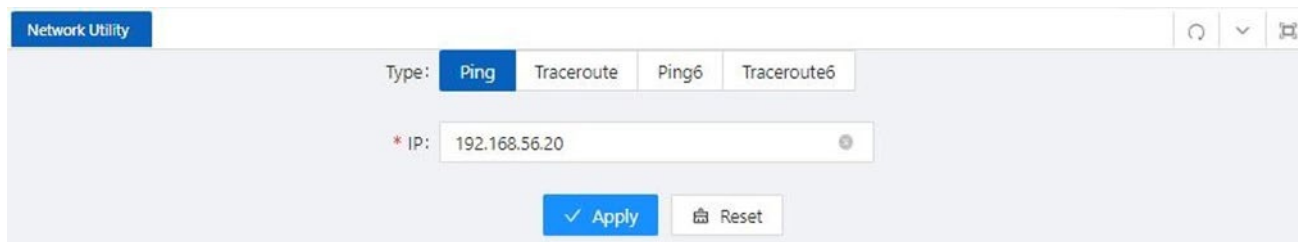
6. Diagnosis

6.1. Network Utilities

6.1.1. Инструменты диагностики

Инструмент Ping:

1. Выберите «Diagnosis» - «Network Utilities» в дереве навигации, для перехода на страницу Network Utilities.
2. Введите IP-адрес устройства назначения в поле IP, как показано на Рисунке 136.



The screenshot shows the 'Network Utility' window. At the top, there's a tab labeled 'Network Utility'. Below it, there's a 'Type' section with four buttons: 'Ping' (selected), 'Traceroute', 'Ping6', and 'Traceroute6'. Underneath, there's a field labeled '* IP:' with the value '192.168.56.20' entered. At the bottom, there are two buttons: 'Apply' (with a checkmark icon) and 'Reset' (with a trash can icon).

Рисунок 136 – Страница Network Utilities

3. Нажмите кнопку «Ping» и далее «Apply», чтобы выполнить команду Ping, после чего отобразится результат выполнения команды Ping в поле ниже, как показано на Рисунке 137.

```
Result: PING 192.168.56.20 (192.168.56.20) 56(84)
bytes of data.
64 bytes from 192.168.56.20: icmp_req=1
ttl=128 time=1.04 ms
64 bytes from 192.168.56.20: icmp_req=2
ttl=128 time=0.859 ms
64 bytes from 192.168.56.20: icmp_req=3
ttl=128 time=0.986 ms
64 bytes from 192.168.56.20: icmp_req=4
ttl=128 time=0.892 ms
64 bytes from 192.168.56.20: icmp_req=5
ttl=128 time=0.821 ms

--- 192.168.56.20 ping statistics ---
5 packets transmitted, 5 received, 0% packet
loss, time 4000ms
rtt min/avg/max/mdev =
0.821/0.920/1.046/0.091 ms
```

Рисунок 137 – Результат выполнения команды Ping

Инструмент Traceroute:

1. Выберите «Diagnosis» - «Network Utilities» в дереве навигации, для перехода на страницу Network Utilities.
2. Введите IP-адрес устройства назначения в поле IP.
3. Нажмите кнопку «Traceroute» и далее «Apply», чтобы выполнить команду Traceroute, после чего отобразится результат выполнения команды Traceroute в поле ниже, как показано на Рисунке 138.

```
Result: traceroute to 163.177.151.110
(163.177.151.110), 20 hops max, 60 byte
packets
 1 192.168.1.1 0.598 ms
 2 100.69.0.1 3.784 ms
 3 218.104.224.29 3.628 ms
 4 218.104.229.66 16.026 ms
 5 218.104.229.37 24.969 ms
 6 *
 7 120.83.0.86 20.729 ms
 8 120.80.137.202 21.808 ms
```

Рисунок 138 – Страница Traceroute

6.2. Optical Transceiver Information

6.2.1. Отображение информации оптического трансивера

Выберите «Diagnosis» - «Optical Transceiver Information» в дереве навигации, для перехода на страницу Transceiver Information, как показано на Рисунке 139.

Transceiver Information								
Name	State	Transceiver Status	Temperature(°C)	Voltage(V)	Current(mA)	RX Power(dBm)	TX Power(dBm)	Action
gigabitEthernet0/9	Down	OK	58(OK)	3.2104(OK)	18.07(OK)	-40(ALARM)	-5.5(OK)	Detail
gigabitEthernet0/10	Down	Transceiver absent	NA	NA	NA	NA	NA	Detail

Рисунок 139 – Страница Transceiver Information

Элемент	Описание
Name	Номер порт коммутатора в котором установлен оптический трансивер.
State	Состояние интерфейса
Transceiver State	Включить/Выключить NTP

Temperature(degree)	Температура трансивера
Voltage(V)	Напряжение питания трансивера
Current(mA)	Ток потребления трансивером.
Rx Power(dBm)	Уровень входящего сигнала
TX Power(dBm)	Уровень исходящего сигнала
Detail	Отображение детальной информации о трансивере

6.2.2. Отображение подробной информации

Нажмите кнопку «Detail» напротив соответствующего интерфейса, чтобы открыть страницу с подробной информацией о трансивере, как показано на Рисунке 140.

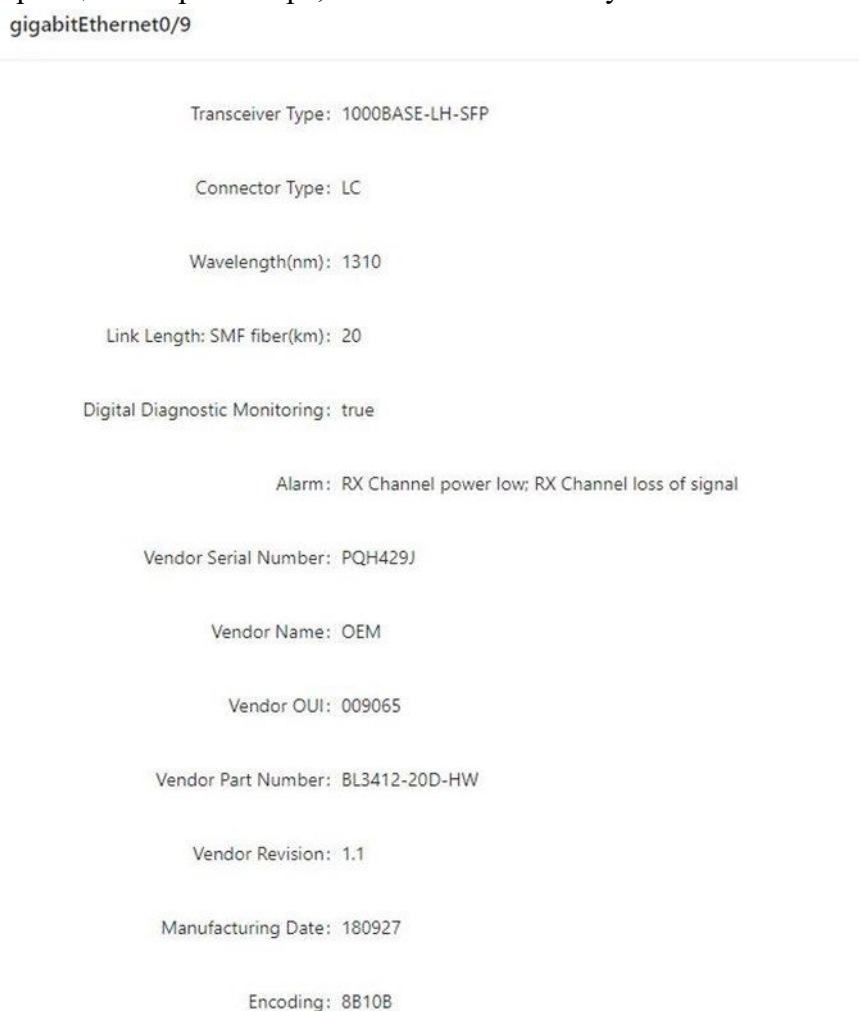


Рисунок 140 – Страница Transceiver Detail Information

6.3. One-click Collection

Каждый функциональный модуль сохраняет информацию о состоянии работы. Модуль диагностической информации позволяет сохранить статистику работы нескольких функциональных модулей в файл, а затем проанализировать их по отдельности.

1. Выберите «Diagnosis» - «One-click Collection» в области навигации, чтобы перейти на страницу One-click Collection, как показано на Рисунке 141.
2. Нажмите кнопку One-click Collection, система сгенерирует файл диагностической информации, после чего появится диалоговое окно загрузки файла.

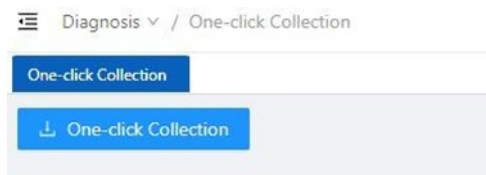


Рисунок 141 – Страница One-click Collection

6.4. Dying Gasp

6.4.1. Введение

Технология Dying Gasp позволяет мгновенно и гарантированно уведомить администратора о внештатном прерывании подачи электропитания на коммутатор. Сетевые устройства полагаются на временный резервный источник питания на конденсаторе, который рассчитан на 10-20 миллисекунд, что позволяет плавно завершить работу и создать сообщение Dying Gasp.

Элемент	Описание
Mib files	DOT3-OAM-MIB.mib
oid	1, 3, 6, 1, 2, 1, 158, 1, 6, 1, 4
value	dyingGaspEvent(257)

6.4.2. Конфигурация Dying Gasp

1. Выберите «Diagnosis» - «Dying Gasp» в области навигации, чтобы перейти на страницу конфигурации Dying Gasp, как показано на Рисунке 142.
2. Отметьте галочкой Dying Gasp и нажмите кнопку Apply, чтобы включить функцию Dying Gasp.

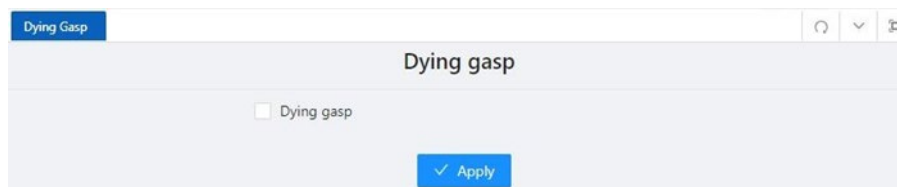


Рисунок 142 – Страница Dying Gasp Configuration