Руководство по эксплуатации
Промышленные коммутаторы

GL-SW-G205-4PSG(BT)
GL-SW-G205-8PSG(BT)
GL-SW-G206-8PSG(BT)

2024

Оглавление

1. Описание функций

1.1 Функции L2		
1.2	Port Management	Включение/выключение порта
		Настройка скорости, дюплекса и MTU порта
		Настройка flow control на порту
		Проверка информации на порту
1.3	Mirroring	Поддержка ingress and egress зеркалирования портов
1.4	Rate Limit	Ограничение скорости порта на чипе
1.5	Storm Policing	Подавление broadcast/multicast/unicast/unknown шторма
1.6	Link Aggregation	Поддержка статической агрегации в ручном режиме
		Динамическая агрегация в режиме LACP
1.7	VLAN	Access
		Trunk
		Hybrid
1.8	MAC	Добавление/удаление статического MAC-адреса
		Ограничение прослушиваемых MAC-адресов
		Динамическое выставление aging-time
1.9	Spanning Tree	802.1d (STP), ERPS
		802.1w (RSTP)
		802.1s (MSTP)
1.10	IGMP Snooping	Добавление/удаление статического адреса
		Поддержка динамического мультикаста v1/2/3
2. Функции L3		
2.1	Interface Configuration	Поддержка VLAN интерфейса
2.2	ARP	Проверка ARP
2.3	Routing	Статическая маршрутизация
3. Расширенные функции		
3.1	ACL	Фильтр портов основанный на Source/Destination MAC, типе протокола, источник/Destination IP и L4
		Настройка ограничения по времени
3.2	QoS	Классификация по 802.1p (CoS)
		Классификация по DSCP
		Классификация по Source/Destination IP и порта

		Поддержка SP, WRR и DRR алгоритмов
		Поддержка CAR
3.3	LLDP	Поддержка LLDP
3.4	User Configuragion	Добавление/удаление пользователя с правами настройки
3.5	Log	Сбор логов по входу, операциям, статусам и событиям
3.6	Attack Resistance	Защита от DOS
		Защита CPU и ограничение трафика на ответные сообщения
		Назначение ARP (IP, MAC, Port)
3.7	Network Diagnostics	Поддержка PING, Telnet, Traceroute
3.8	System Management	Сброс устройства, сохранение/восстановление конфигурации, обновление прошивки, установка времени итд.
4. Функции управления		
4.1	CLI	Управление через Console-порт устройства
4.2	Telnet	Удаленное управление по Telnet
4.3	Web	Поддержка конфигурации уровня 2 (L2)
5. Прочие функции		
5.1	Поддержка DHCP Snooping	
5.2	Поддержка Ring Protection (ERPS)	
5.3	Поддержка SNMP v1/v2c/v3	

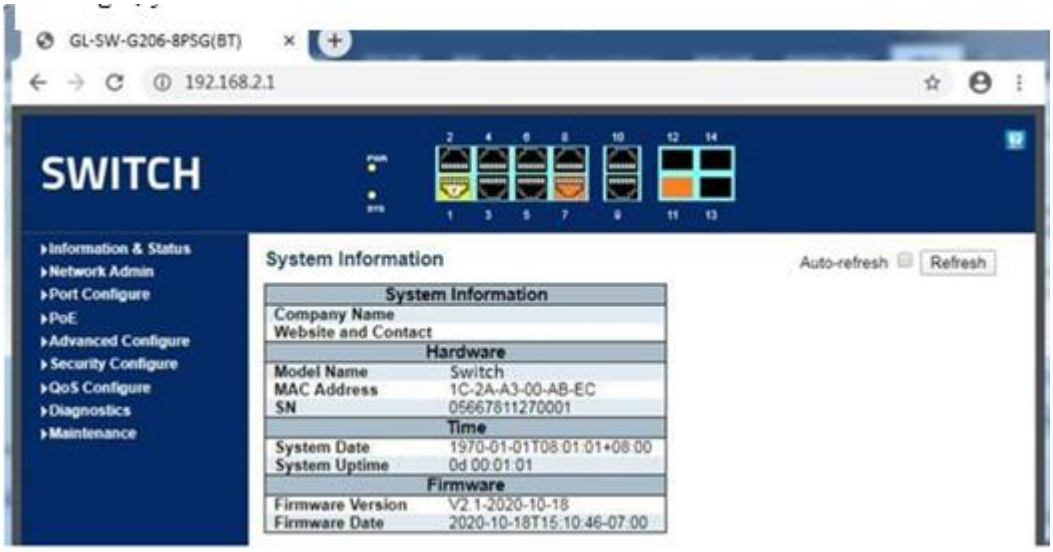
2. Веб конфигурация

2.1 Подключение к коммутатору через веб-интерфейс

По умолчанию веб-интерфейс коммутатора находится по адресу: http://192.168.2.1
Для доступа к нему на ПК необходимо сконфигурировать сетевой адаптер на ip-адрес из диапазона 192.168.2.x (где x – будет отличным от 1) и подсеть (шлюз) 255.255.255.0

Логин и пароль для доступа по умолчанию “**admin**”

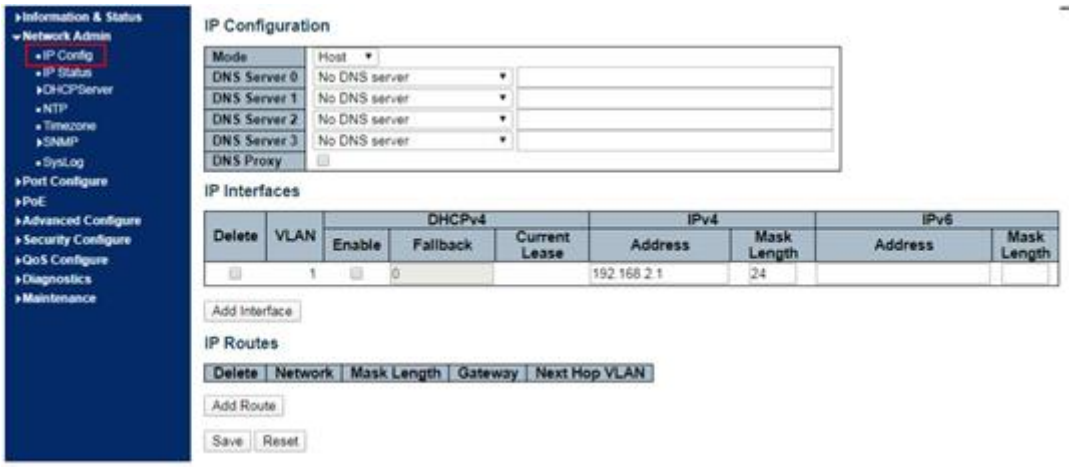
После успешного входа вы увидите веб-интерфейс коммутатора:



3. Network Admin

3.1 IP Config

Нажмите “**Network Admin-IP Config**” для входа в меню настройки ip-адреса



Описание пунктов меню IP Config:

Пункт меню	Описание
Mode	Выберите режим работы (Host mode/Router mode)
DNS Server	Выберите режим работы DNS-сервера (No DNS Server, Configurable IPv4, IPv4, From any DHCPv4 interface и from this DHCPv4 interface)
DNS Proxy	Адрес прокси-сервера DNS (DNS Proxy)
Interface Name	Имя интерфейса
VLAN	Применения VLAN для доступа и управления коммутатором
IPv4 DHCP	• Enabled означает, что интерфейс VLAN динамически получает IPv4-адрес коммутатора через DHCP-клиент IPv4. В противном случае будет происходить статическая настройка IP-адреса. • Время ожидания (единица измерения: секунда) означает период, в течение которого коммутатор пытается получить динамический IP-адрес через DHCP. В случае установки 0 секунд время ожидания никогда не закончится. • Текущий IP-адрес получен через DHCP.
IPv4	• IP-адрес: статический IPv4-адрес, введенный пользователем. • IP-маска: статическая маска подсети IPv4, введенная пользователем.
IPv6	• IP-адрес: статический IPv6-адрес, введенный пользователем.

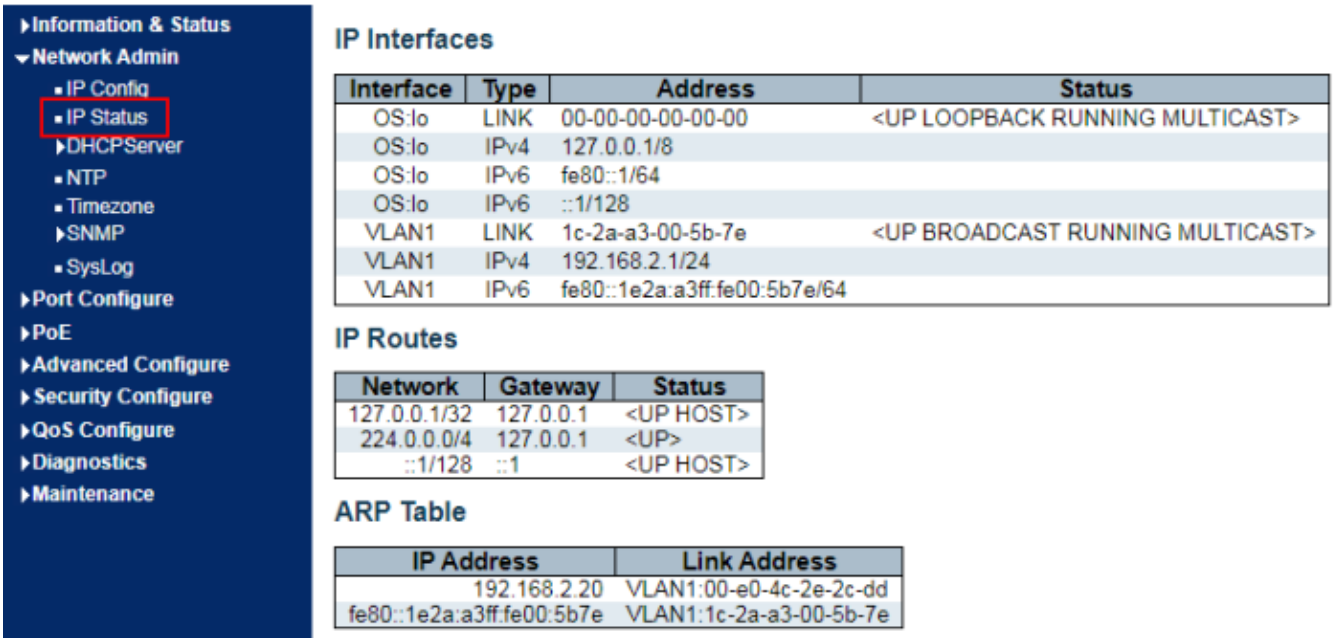
	• IP-маска: статическая маска подсети IPv6, введенная пользователем.
IP Routes	• Сегмент назначения: IPv4-адрес, введенный пользователем. • IP-маска: статическая маска подсети IPv4, введенная пользователем. • Адрес следующего хопа: следующий IPv4-адрес, введенный пользователем.

Нажмите “**Add**” для создания нового VLAN управления и IP-адреса, и “**Save**” для сохранения изменений.

Пояснение:
Управления коммутатором осуществляется в VLAN1 по-умолчанию. Пользователи, которым необходимо использовать другие коммутаторы для управления должны сначала добавить VLAN и соответствующие порты в модуль VLAN, чтобы реализовать связь уровня 3 между VLAN.

3.2 IP Status

Нажмите “**Network Admin-IP Status**” для просмотра информации о IP-адресах



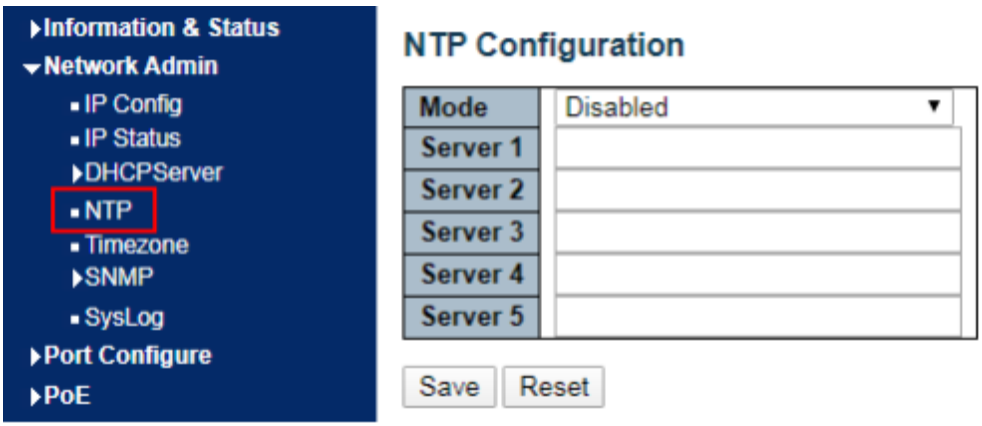
Описание таблиц пункта IP Status:

Параметр	Описание
IP Interfaces	Таблица IP Port адресов известных устройству
IP Routes	Таблица IP Routing (маршрутов) известных устройству
ARP Table	Таблица ARP соответствий известных устройству

3.3 NTP

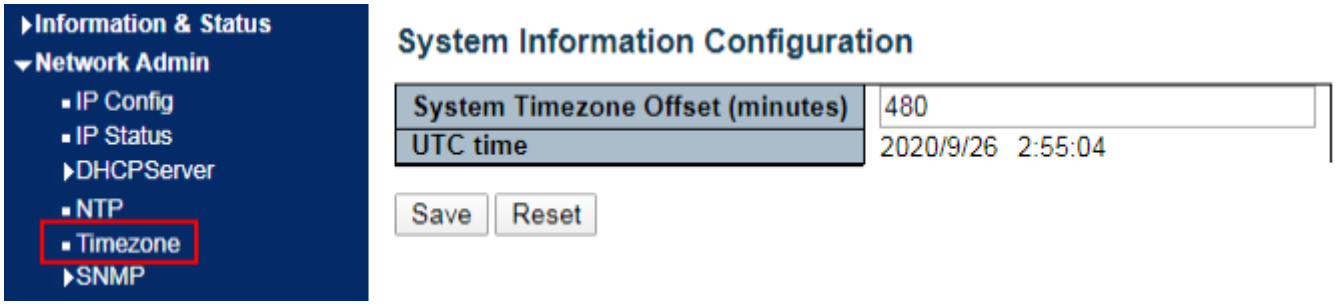
Применяемый для синхронизации часов между распределенными серверами времени и клиентами, протокол NTP (Network Time Protocol) находится на прикладном уровне семейства протоколов TCP/IP, который реализован на базе IP и UDP. Сообщение NTP передается через UDP с портом № 123. Синхронизация часов во всех сетевых устройствах будет играть решающую роль в условиях все более усложняющийся сетевой топологии. Поэтому NTP появился, так как ручная модификация системных часов администраторами приводит к огромной нагрузке и расхождениях во времени.

Для настройки работы сервера выберите пункт “**Network Admin**-**NTP**”



Параметр	Описание
Mode	Выберите режим вкл/выкл для NTP из выпадающего списка
NTP Server	Задайте IP адрес сервера NTP

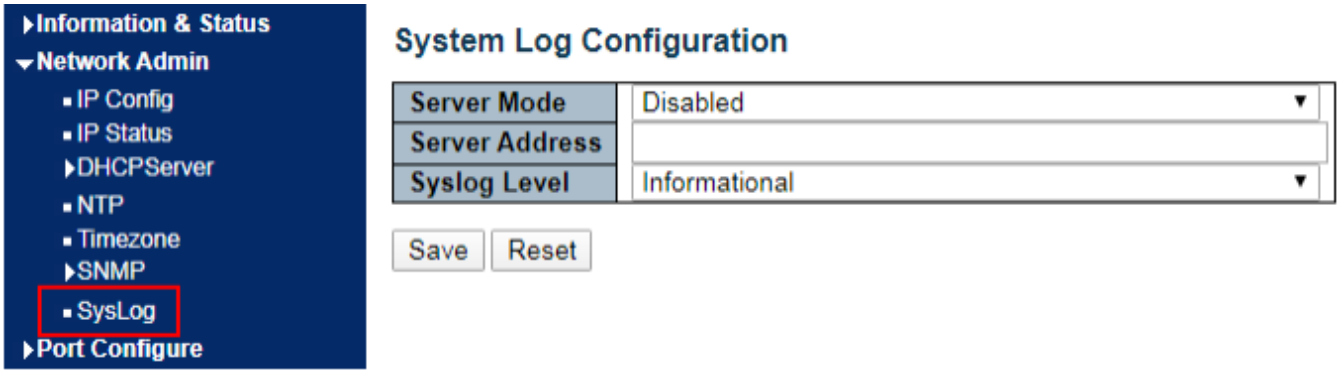
Для настройки временной зоны выберите в списке “**Network Admin**-**Timezone**”



Параметр	Описание
System Time-zone Offset (minutes)	Установка смещения времени в минутах от UTC
UTC Time	Всемирное координированное время

3.4 Syslog

У пользователя имеется возможность выгружать логи коммутатора на TFTP сервер. Выберите в меню “**Network Admin-SysLog**” для настройки:

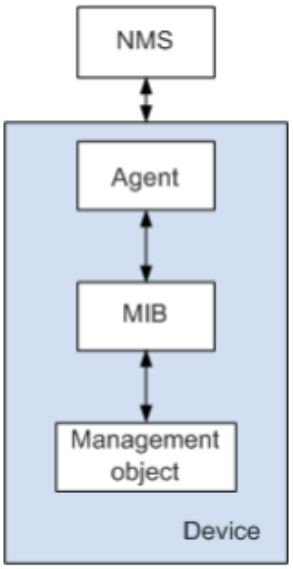


Параметр	Описание
Mode	Включение/выключение функции Syslog. Коммутатор будет отправлять логи на сервер если указан определенный адрес
Server IP Address	IP адрес сервера для сбора логов
Log Levels	По уровню захвата логи могут включать: **Info**: Информация, предупреждения, ошибки **Warning**: Предупреждения и ошибки **Error**: Ошибки

3.5 SNMP

Протокол SNMP (Simple Network Management Protocol) широко используется в сетях TCP/IP. Он управляет устройствами с помощью центрального компьютера, на котором установлено программное обеспечение для управления сетью (т.е. рабочей станцией управления сетью).
SNMP – это основанный на опросе, имеет фундаментальный набор функций, который применим для небольших сред с высокой скоростью и низкой стоимостью. Кроме того, SNMP, работающий по протоколу UDP, совместим с большинством устройств. SNMP нацелен на обеспечить передачу управляющей информации между двумя узлами, чтобы администраторы могли легко получать, изменять и устранять неисправности.
Существует 3 распространенные версии, а именно SNMPv1, v2c и v3. SNMP содержит: NMS (Система управления сетью), агент, объект управления и MIB (база управленческой информации). NMS, как центр управления, будет управлять всеми устройствами. Каждое

управляемое устройство включает в себя резидентный агент, MIB и объекты управления. NMS взаимодействует с агентом, запущенным на объекте управления, который будет работать с MIB для выполнения приказов NMS.



Модель управления SNMP

NMS

Как администратор сети, NMS управляет/наблюдает за сетевыми устройствами с помощью SNMP на своем сервере. Она может обратиться к Агенту, чтобы запросить или изменить значение(я) элемента конфигурации. NMS может получать активные ловушки (traps), отправляемые агентом, для обновления информации о состоянии управляемых устройств.

Агент

Как агентский процесс управляемых устройств, он поддерживает данные устройства и отвечает на запросы NMS, сообщая данные управления. Агент выполняет соответствующие заказы через таблицу MIB и отправляет результаты обратно в NMS после получения запроса. Устройства сами проявляют инициативу по отправке информации о текущем состоянии устройств в NMS
через агента, как только произойдет сбой или другое событие.

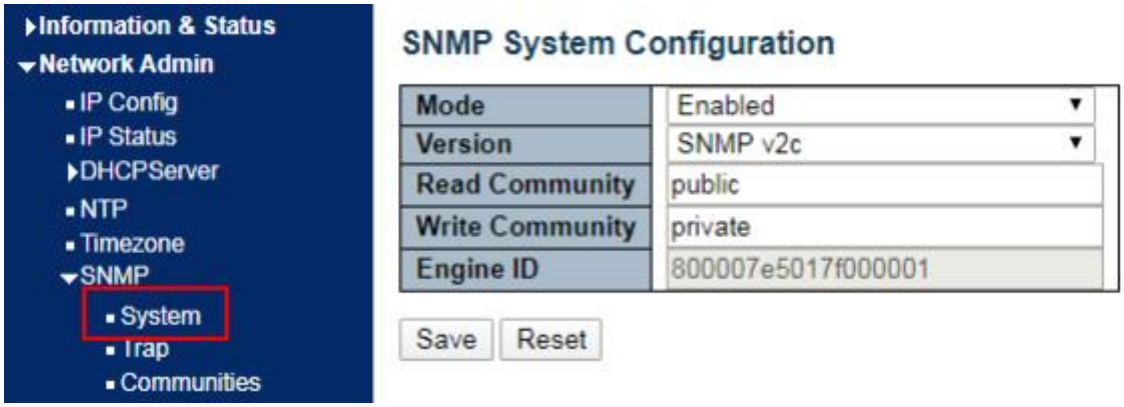
Объект управления

Относится к управляемому объекту. Каждое устройство может иметь более одного объекта, включая часть аппаратного обеспечения (например, интерфейсная плата), часть аппаратного и программного обеспечения (например, протокол маршрутизации), а также другие наборы конфигурационных элементов.

MIB

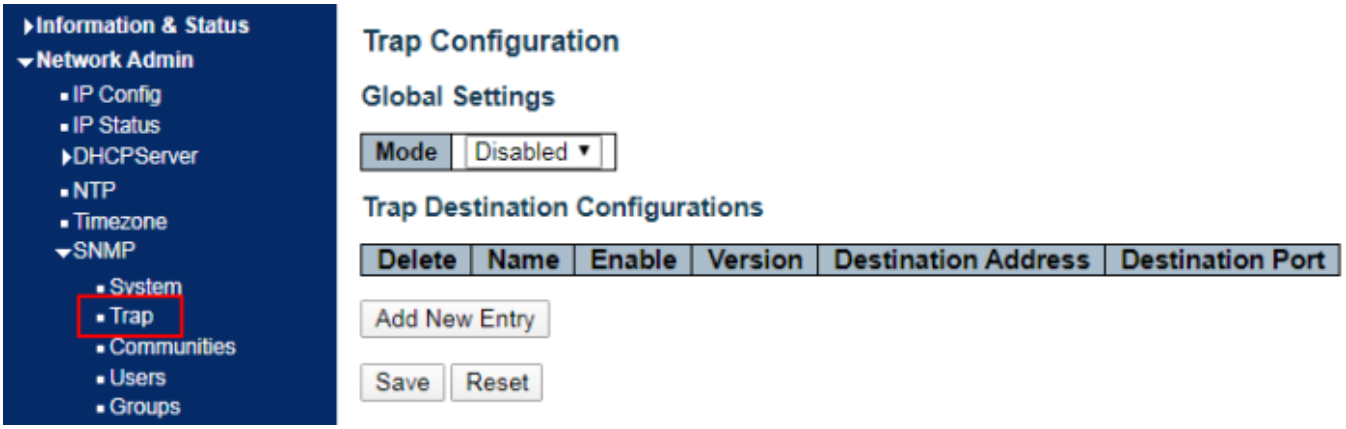
MIB - это база данных, определяющая переменные, поддерживаемые объектом управления (т.е. информация, которая может быть запрошена и устанавливаться агентом). MIB определяет атрибуты объекта управления, включая имя, статус, право доступа и тип данных. С помощью MIB могут быть реализованы следующие функции: агент получает мгновенную информацию об устройстве путем запросив MIB, и устанавливает элементы конфигурации состояния, изменяя MIB.

Для настройки выберите и разверните дерево в пункте “**Network Admin**-**SNMP**”:



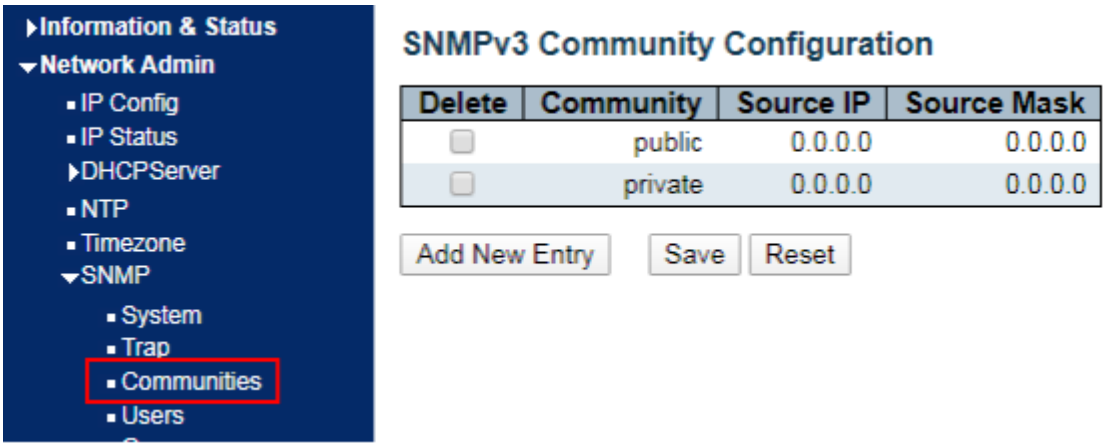
Параметр	Описание
Mode	Включение/отключение функции SNMP
Version	Выбор версии SNMP из списка v1, v2c, v3
Read Community	Авторизационное значение для возможности чтения MIB-объекта, по умолчанию “public”
Write Community	Авторизационное значения для возможности чтения/записи MIB-объекта, по умолчанию “private”

Для настройки SNMP Trap выберете пункт “**Network Admin**-**SNMP-Trap**”



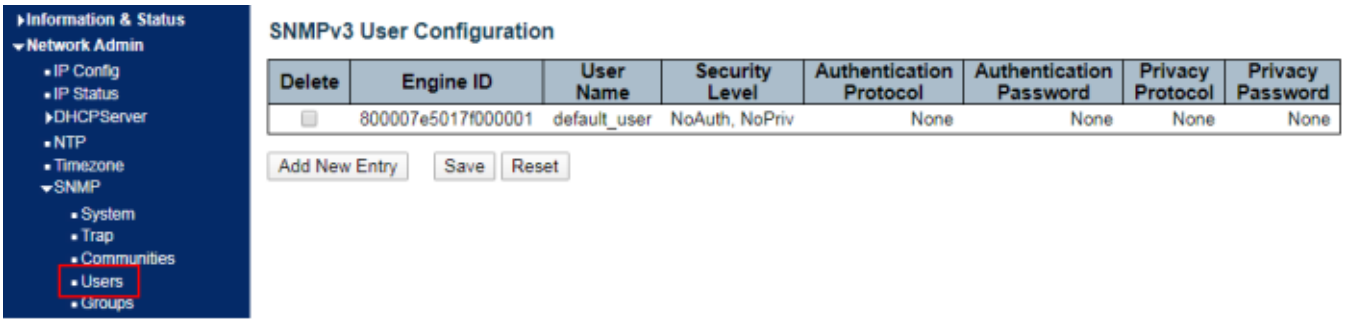
Параметр	Описание
Trap Name	Привязка имени SNMP Trap
Trap Mode	Вкл/Выкл функции SNMP Trap
Trap Version	Версия SNMPv1, v2c и v3
Trap Community	Имя группы заданное для SNMP Trap
Trap Destination IP Address	IP-адрес заданный для SNMP Trap
Trap Destination UDP Port	Номер UDP-порта используемый SNMP Trap
Trap Inform/Response Mode	Вкл/Выкл опроса
Trap Inform/Response Timeout (seconds)	Период опроса в секундах
Trap Inform/Response Retry Times	Количество повторных попыток опроса

Для переименования “**Community**” выберите пункт “**Network Admin-SNMP-Communities**”:



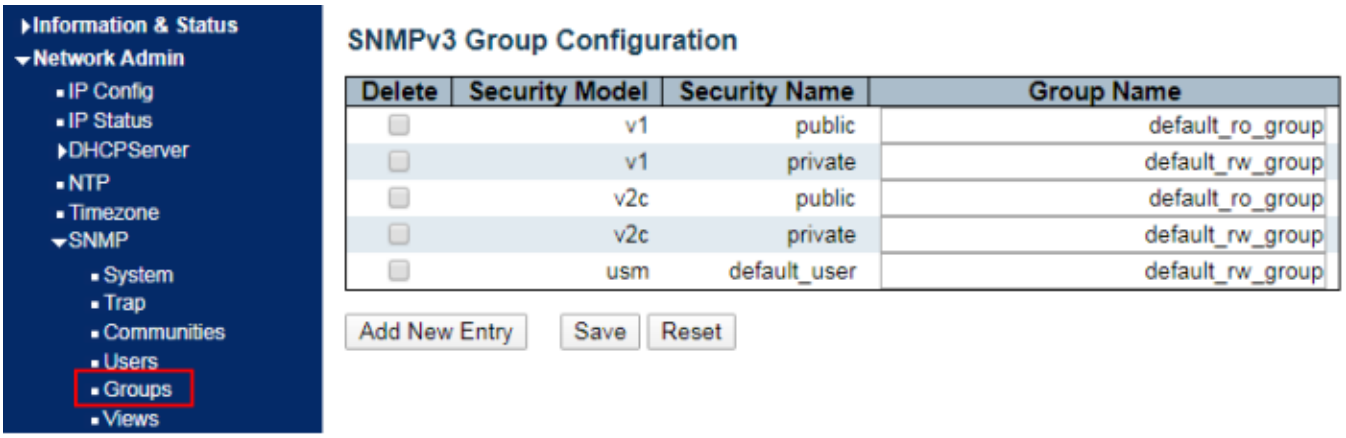
Параметр	Описание
Community	Задайте новое имя Community
Source IP	Задайте IPv4 адрес источника
Source Mask	Задайте IPv4 маску источника

Для создания пользователя SNMPv3 и выбора настроек приватности выберите пункт “**Network Admin-SNMP-Users**”:



Параметр	Описание
Group Name	Задайте имя группы
Security Model	Выберите из списка v1, v2c или usm
Security Level	Выберите метод шифрования noAuthnoPriv, authNoPriv, authPriv из списка
Read View Name	Выберете отображаемое имя из списка
Write View Name	Выберете отображаемое имя из списка

Для создания пользователей и настроек доступа в новой группе выберите “**Network Admin-SNMP-Groups**”:

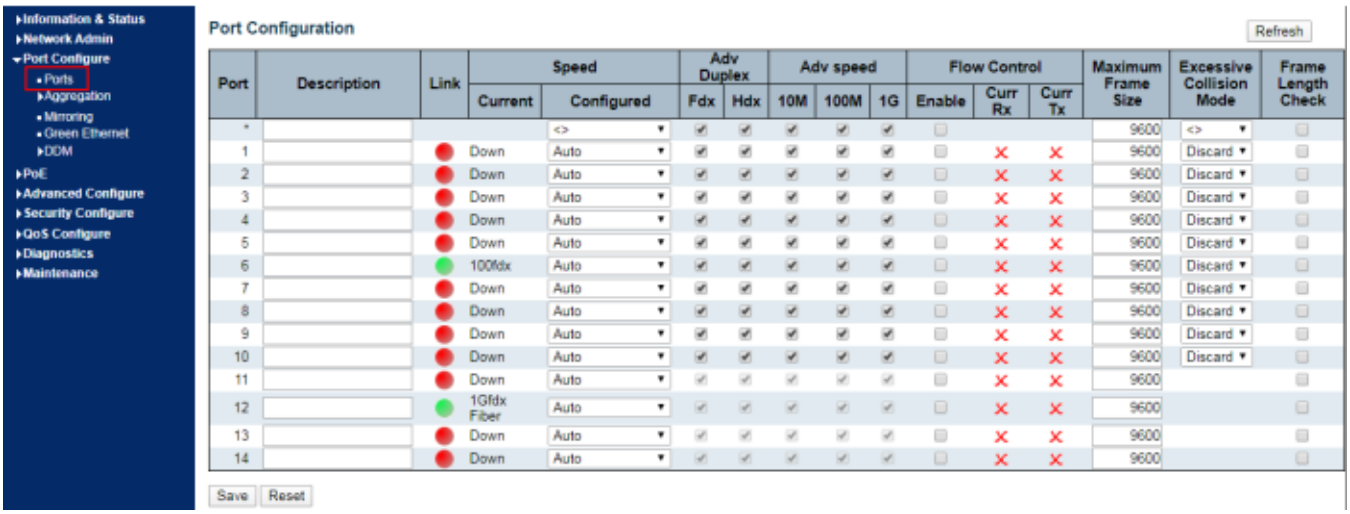


Параметр	Описание
Security Model	Выберите v1, v2c или usm из списка
Security Name	Задайте созданное имя, имя группы (для v1/v2c) и имя (для usm)
Group Name	Задайте имя права для группы

4. Port Configure

4.1 Ports

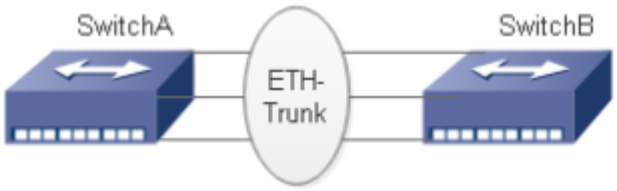
Интерфейсы должны быть определены таким образом, чтобы пользователи могли запрашивать и настраивать интерфейсы Ethernet по мере необходимости.
Выберите пункт “**Port Configure**-**Ports**” для настройки Description (описания порта), Autonegotiation (автосогласования/ручного выбора скорости порта), Flow Control (управление потоком вкл/выкл), Maximum Frame Size (установки максимального размера MTU):



Параметр	Описание
Autonegotiation	Настраиваемое автосогласование с обязательными состояниями 10 Мб, 100 Мб и 1 000 Мб. Скорости интерфейса, включая 10 Мбит/с, 100 Мбит/с и 1 000 Мбит/с, доступны для электрических интерфейсов Ethernet
Flow Control	После включения этой функции на устройствах локальной и противоположной стороны, локальное устройство будет уведомлять другое устройство о необходимости прекратить отправку сообщений при наличии перегрузки сети. Противоположное устройство временно выполнит команду, чтобы исключить потерю сообщений. Disable - отключает прием и передачу кадра PAUSE; Rx (RX Pause) - получение кадра PAUSE; Both (Rx/Tx Pause) - Прием и передача кадра PAUSE; Tx (Tx Pause) - передача кадра PAUSE.
Maximum Frame Size	Максимальный размер MTU (9600)
Enabled	Включение портов
Port Description	Отображаемое описание порта

4.2 Aggregation

Агрегация каналов увеличивает пропускную способность и надежность, объединяя группу физических интерфейсов в один логический интерфейс.
Link Aggregation Group (LAG) — это логический канал, объединенный несколькими каналами Ethernet (Eth-Trunk). Постоянно увеличивающийся размер сети повышает требования к пропускной способности и надежности каналов.
Механизм резервирования при использовании агрегации не только повышает надежность, но и распределяет нагрузку потока на разные физические каналы.
Как показано ниже, коммутатор A связан с коммутатором B тремя каналами Ethernet, которые объединены в логический канал Eth-Trunk. Его пропускная способность равна пропускной способности всех трех каналов, что позволяет расширить полосу пропускания. Между тем, эти три канала взаимно резервируют друг друга для большей надежности.



Агрегация каналов позволяет удовлетворить следующие потребности:

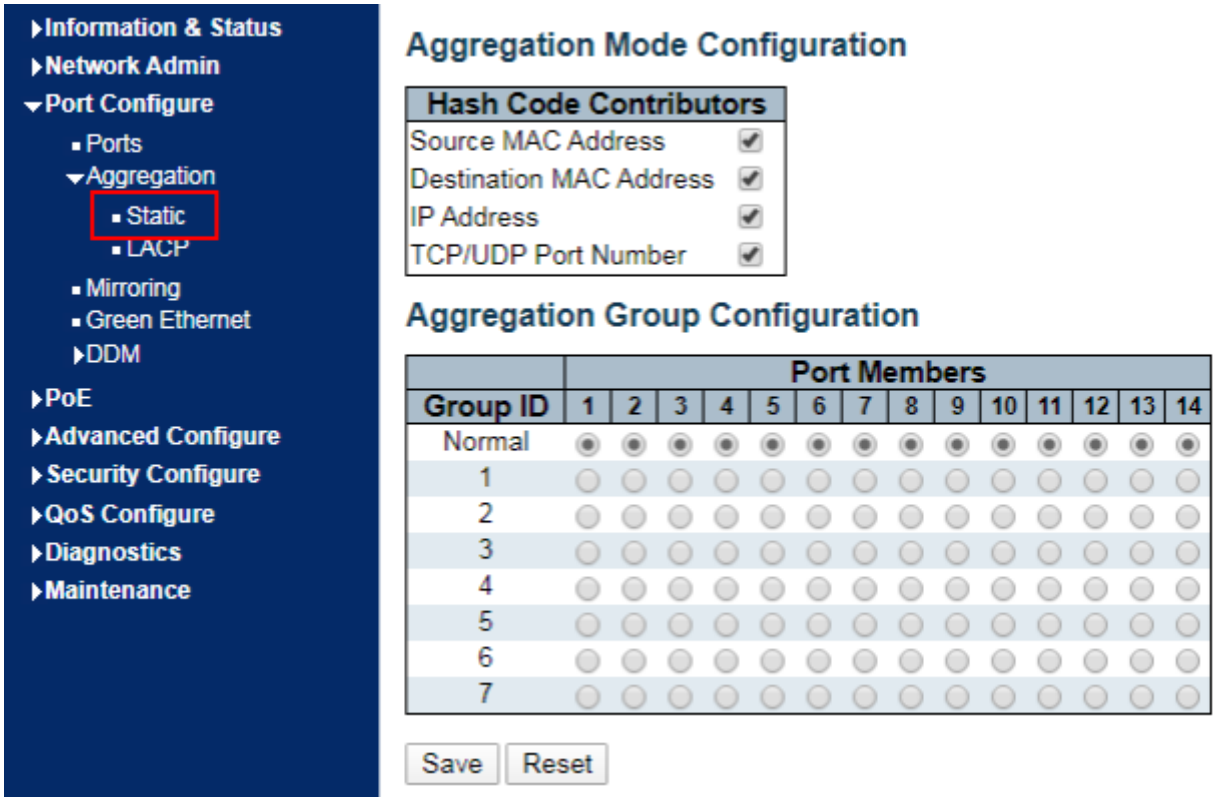
- Недостаточная пропускная способность двух коммутаторов, соединенных одним каналом.
- Недостаточная надежность двух коммутаторов, соединенных одним каналом.

Агрегация каналов может быть разделена на ручной режим и режим LACP в соответствии со статусом Link Aggregation Control (LACP).
В первом режиме, при создании Eth-магистрали, доступ к интерфейсам-участникам должен быть добавлен вручную без LACP. Он также называется режимом распределения нагрузки, поскольку все каналы участвуют в пересылке данных и распределении нагрузки. В случае отказа одного из активных каналов LAG будет распределять нагрузку между оставшимися.
Этот режим предпочтителен в том случае, если двум напрямую подключенным устройствам требуется большая пропускная способность канала, но у них нет доступа к LACP.

4.2.1 Static

Инструкция по добавлению Static Link Aggregation (т.е. в ручном режиме):

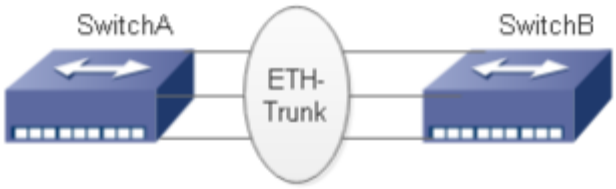
Выберите пункт “**Port Configure**-**Aggregation**-**Static**” и нажмите “**Add a static link aggregation**”, далее выберите Group ID (1-16), load-sharing метод (Src MAC, Dst MAC, IP Address, TCP/UDP Port Number) и порт для агрегации, нажмите “**Add**” для продолжения настройки:



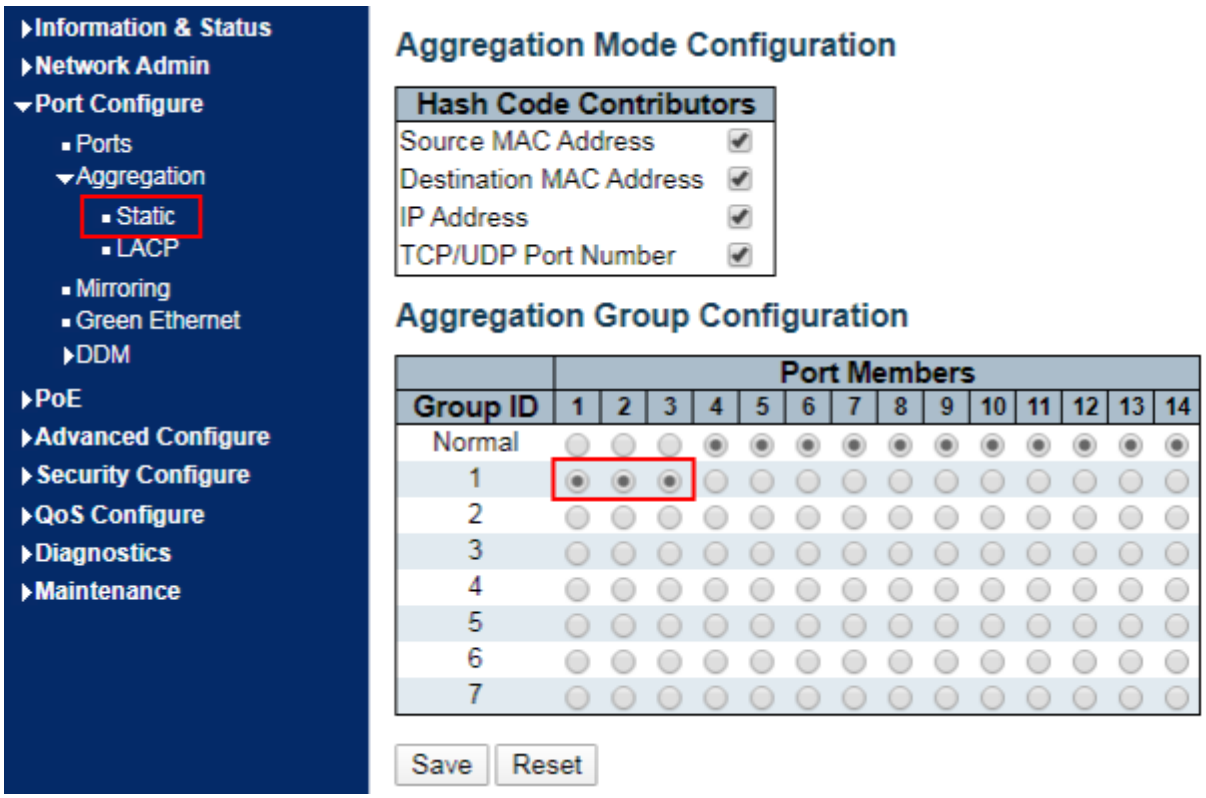
Параметр	Описание
Group ID	Доступно до 16 групп, LAG ID может быть от 1 до 16
Load-sharing Method	Src MAC, Dst MAC, IP Address, TCP/UDP номер порта
Port List	Доступно объединение до 8 портов

Пример настройки

Коммутатор A включен в агрегацию с коммутатором B интерфейсами GE1-GE3, значит он будет распределять нагрузку на каждый порт.



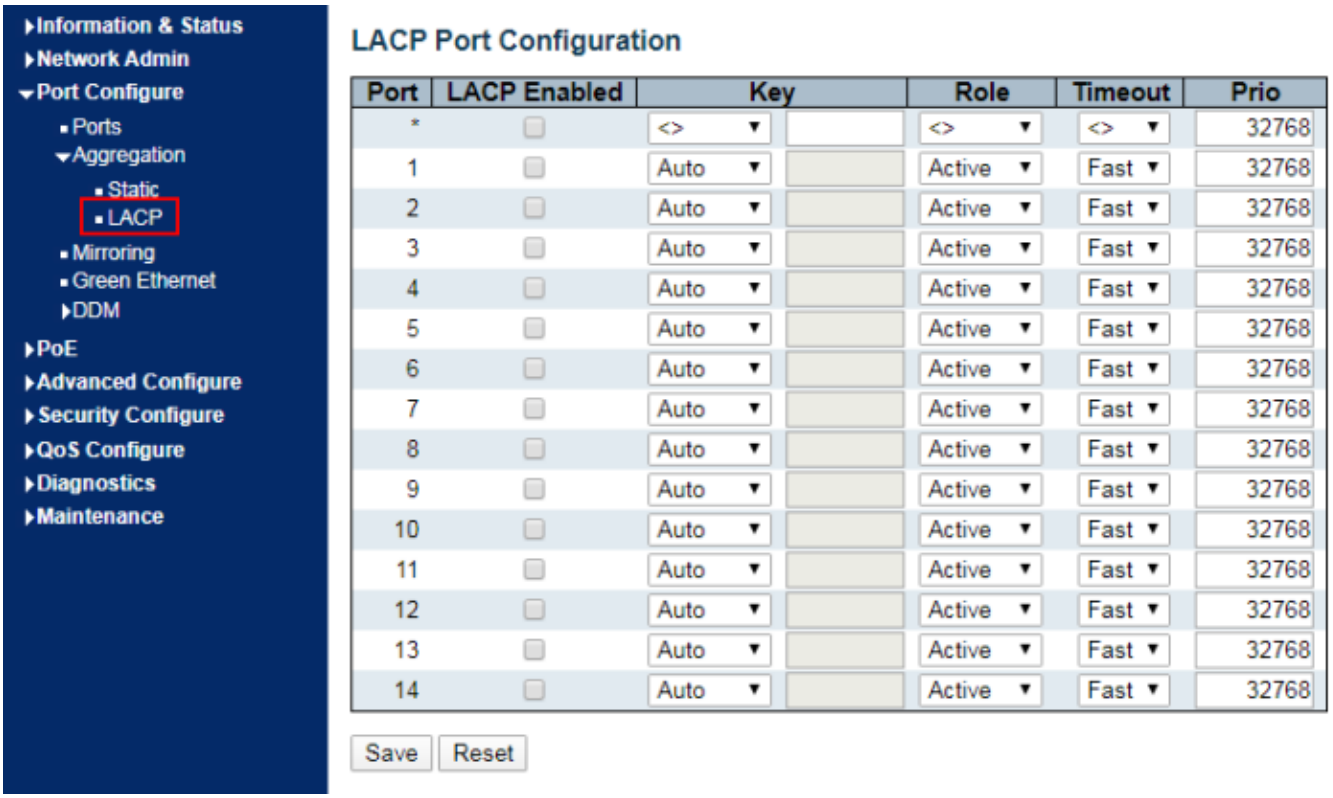
Аналогично шагу настройки коммутатора B, коммутатор A создает интерфейс Eth-Trunk и получает доступ к интерфейсам-членам, участвующим в соединении, чтобы расширить пропускную способность канала. Нажмите кнопку "**Port Configure**-**Aggregation-Static**" и нажмите "**Add a static link aggregation**", чтобы выбрать идентификатор группы "**1**", выберите режим распределения нагрузки (Src Mac, Dst Mac, IP Address) и порт для агрегации (GE1-1, GE1-2 и GE1-3) следующим образом.



4.2.2 LACP

Динамическая агрегация каналов
Протокол LACP (Link Aggregation Control Protocol), основанный на стандарте IEEE 802.3ad, динамически агрегирует и дезагрегирует каналы связи.
LACP обменивается информацией с противоположным сетевым устройством через LACPDU (Link Aggregation Control Protocol Data Unit).
После того как порт использует LACP, он сообщает противоположному сетевому устройству системный приоритет, системный MAC, приоритет и номер, а также ключ операции путем отправки LACPDU. Противоположное устройство сравнивает эту информацию с информацией, сохраненной другими портами после ее получения, тем самым достигая соглашения об участии порта в динамической агрегации или выходе из нее.
Динамическая агрегация LACP автоматически создается или удаляется системой, то есть внутренние порты могут быть добавлены или удалены самостоятельно. Только порты, подключенные к одному устройству с одинаковой скоростью, дуплексом и базовой конфигурацией, могут быть агрегированными.

Инструкция по настройке динамической агрегации:
Выберите в списке пункт “**Port Configure**-**Aggregation**-**LACP**”, укажите порт, включите LACP Enabled, укажите роль (Active/Passive), и приоритет (в диапазоне 0-65535 со значением 32768 по умолчанию)



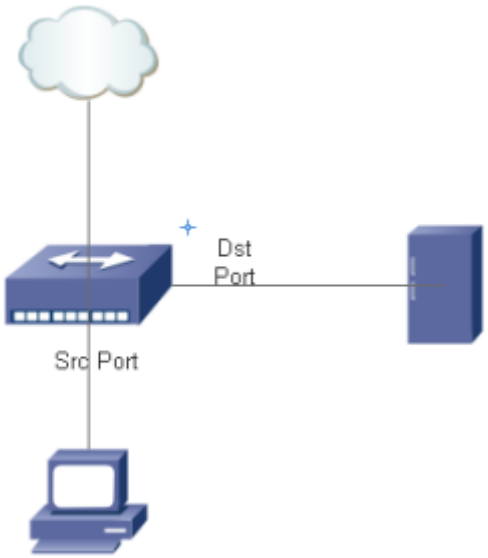
Описание пунктов интерфейса:

Параметр	Описание
LACP Enabled	Включен/выключен
Mode	**Active:** Порт автоматически отправляет пакет данных LACP. Каналы с одним или двумя активными портами LACP могут быть динамически агрегированы. Однако, этого не произойдет с двумя подключенными пассивными портами LACP, поскольку оба они ожидают пакета, с другой стороны. **Passive:** Порт отправляет пакеты LACP вручную и отвечает на пакеты, отправленные только противоположным сетевое устройство.
Port Priority	LACP будет определять члена группы динамической агрегации на основе приоритета идентификатора порта. Среди них ID устройства состоит из 2-байтового системного приоритета и 6-байтового системного MAC. Другими словами, идентификатор устройства состоит из системного приоритета и MAC. Сравните сначала системный приоритет, а затем системный MAC-адрес, если они одинаковы. Предпочтительнее будет тот, у которого будет наименьшее значение. Диапазон: 0 - 65535, по умолчанию 32768.
Key	Автоматический/ручной режим

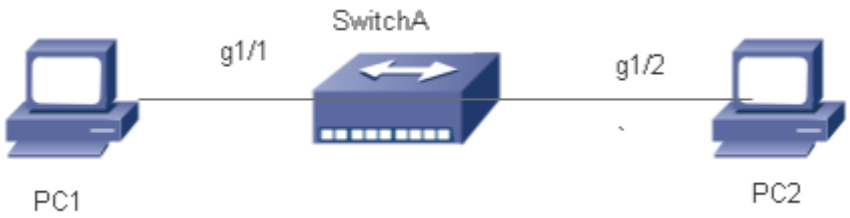
Пояснение
Перед изменением схемы работы убедитесь, что к Eth-Trunk нет доступа через интерфейс участника, иначе она не будет изменена.
Схема работы устройств локальной и противоположной сети должны быть одинаковыми.

4.3 Mirroring

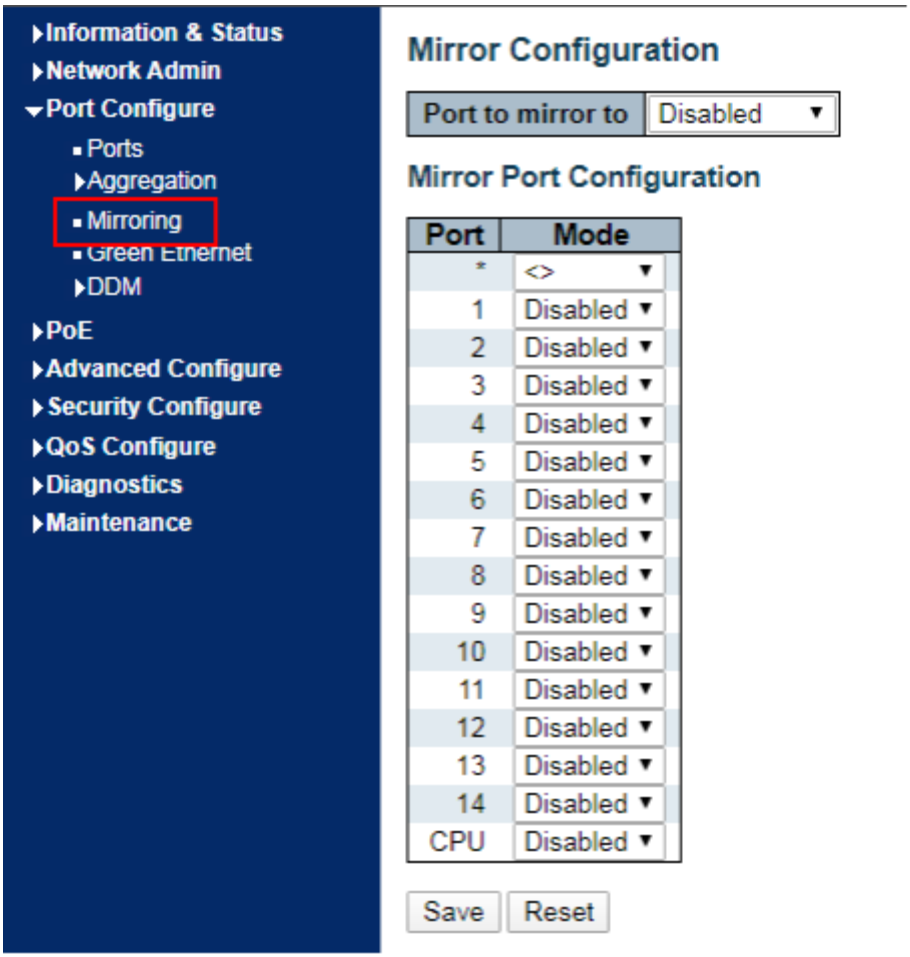
Port Mirroring копирует сообщение указанного порта коммутатора на порт назначения. Копируемый порт — это порт источника, а порт копирования - порт назначения. Порт назначения будет использовать устройства проверки данных, чтобы пользователи могли анализировать полученные сообщения для мониторинга и устранения неполадок в сети следующим образом:



Пример конфигурации:
ПК1 получает доступ к коммутатору A через интерфейс GE1-1, а ПК2 напрямую подключен к интерфейсу GE1-2.
Пользователи намерены отслеживать сообщения, отправляемые соответствующими устройствами с ПК2 на ПК1.



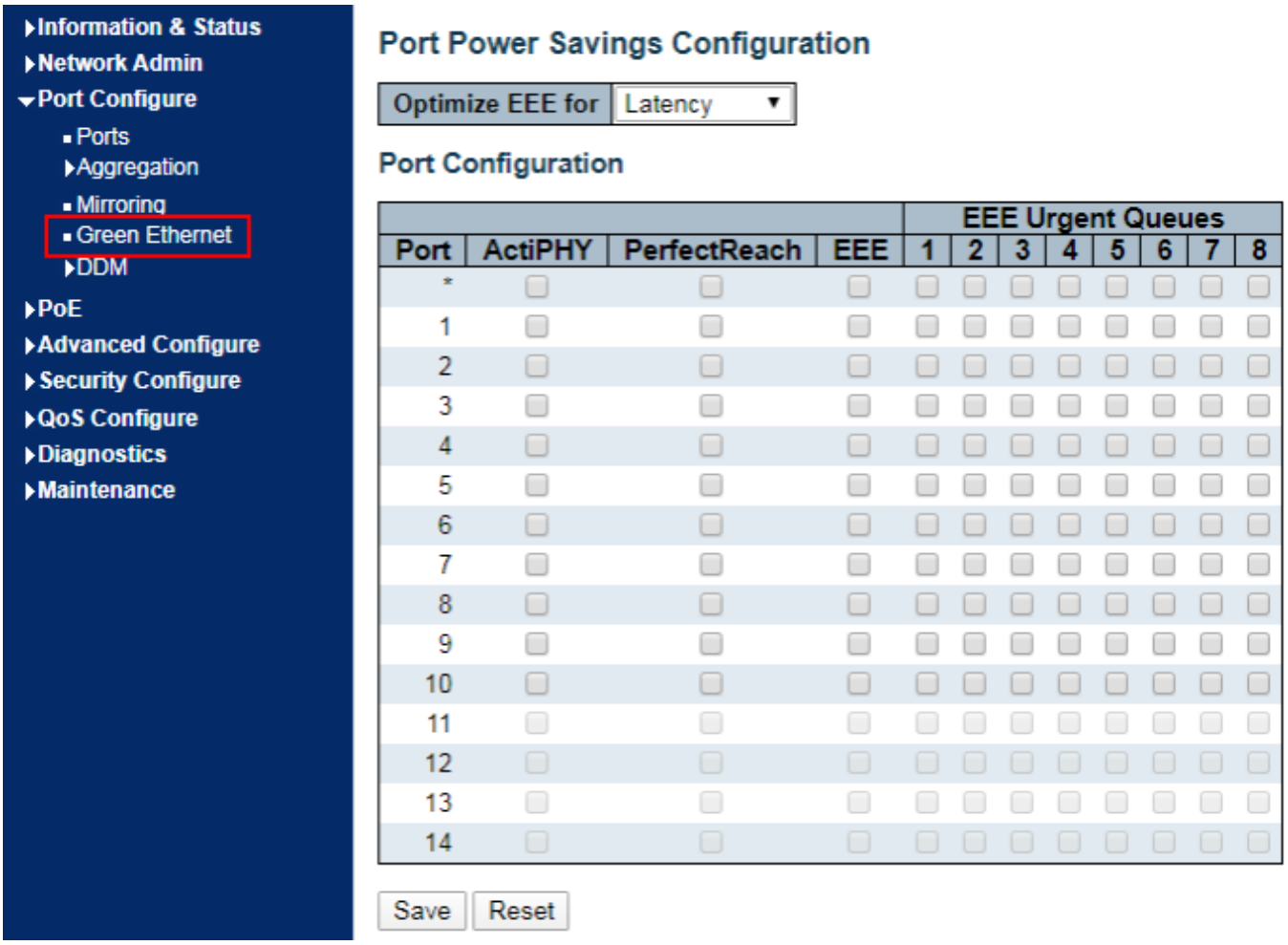
1. Нажмите "**Port Configure**-**Mirroring**" на панели навигации, чтобы выбрать session ID (идентификатор сеанса).
2. Отметьте порт источника GE1-2, выберите порт назначения GE1-1 и режим "**Enabled**" и добавьте их следующим образом.



Параметр	Описание
Source Port	Возможен выбор нескольких портов
Destination Port	Можно выбрать только один порт, исключая порт, использующий соединение и порт источника.
Direction	Tx "Mirroring Ingress Port": любое полученное сообщение будет зеркально отображено на порт назначения. Rx "Mirroring Egress Port": любое отправленное сообщение будет зеркально отображаться на порту назначения. Включить "Mirror Ingress/Egress Port" зеркалирует все отправленные и полученные сообщения на порт назначения.

4.4 Green Ethernet

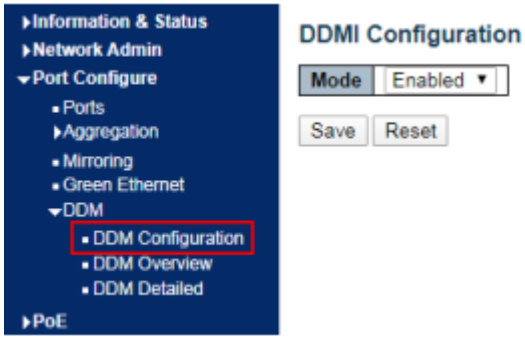
Питание порта будет отключено в случае отсутствия трафика.
Нажмите кнопку "**Port Configure**-**Green Ethernet**" следующим образом:



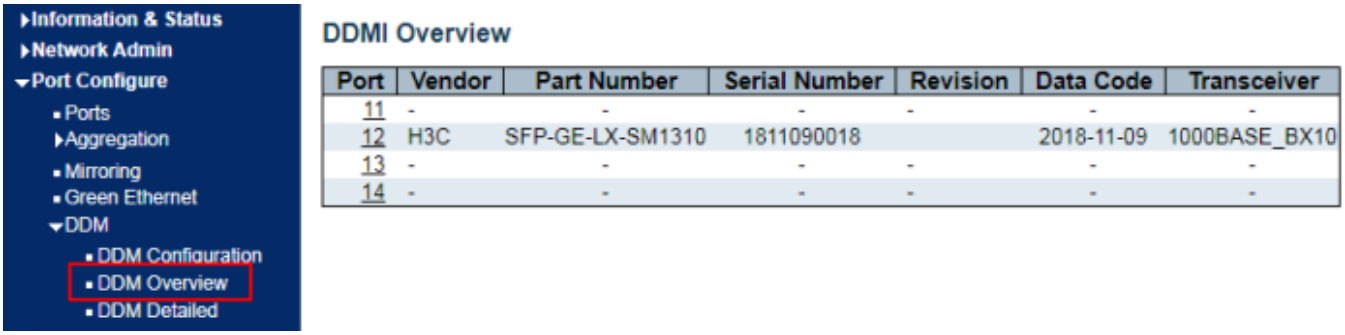
Параметр	Описание
Optimize EEE for	Выберите оптимизацию по мощности или задержке
Port Configuration	Выберите из: ActiPHY, PerfectReach, EEE, EEE Urgent Queues

4.5 DDM

DDM позволяет просматривать информацию по оптическим модулям
Выберите “**Port Configure-DDM-DDMI Configuration**” для включения этой функции:



Выберите “**Port Configure-DDM-DDMI Overview**” для просмотра общей информации о модулях:



Port	Vendor	Part Number	Serial Number	Revision	Data Code	Transceiver
11	-	-	-	-	-	-
12	H3C	SFP-GE-LX-SM1310	1811090018		2018-11-09	1000BASE_BX10
13	-	-	-	-	-	-
14	-	-	-	-	-	-

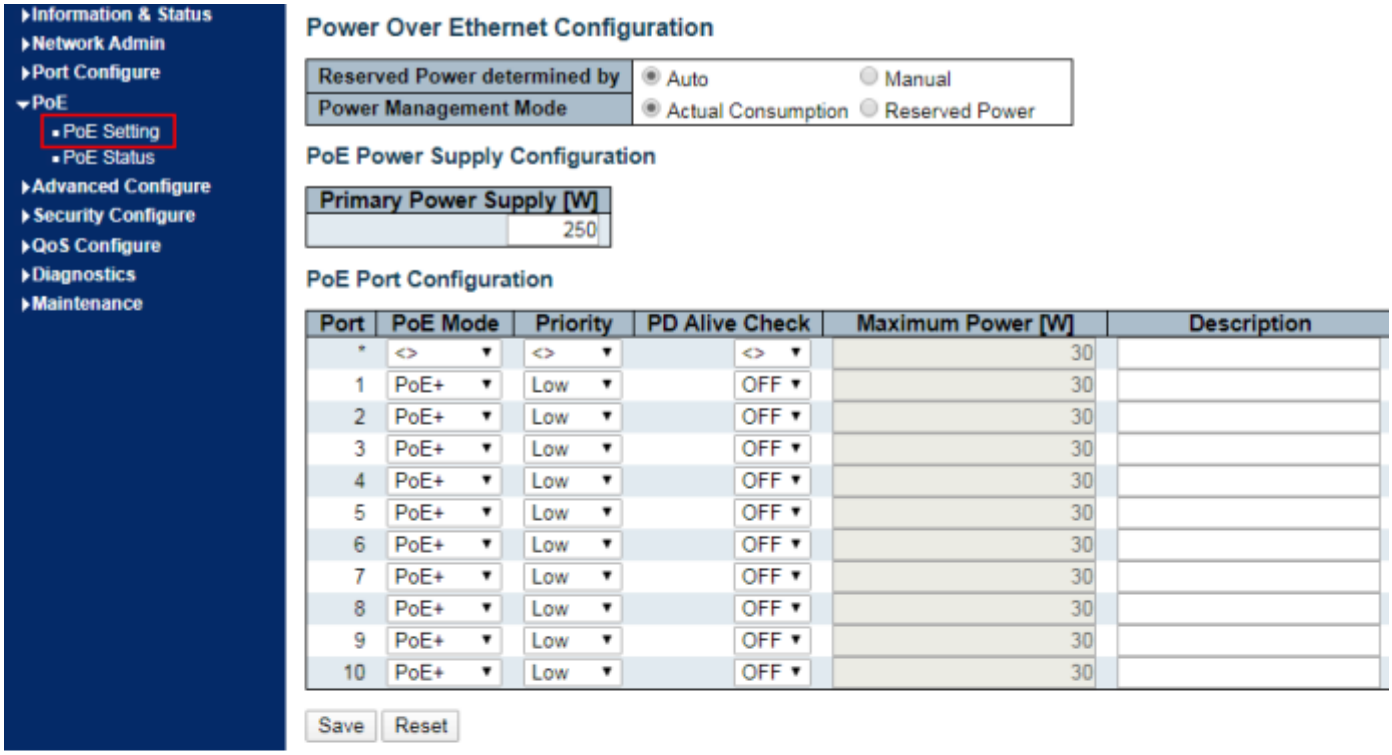
Выберите “**Port Configure-DDM-DDM Detailed**” для просмотра детализированной информации о модулях:

Type	Current	High Alarm Threshold	High Warn Threshold	Low Warn Threshold	Low Alarm Threshold
Temperature(C)	46.250	90.000	85.000	-5.000	-10.000
Voltage(V)	3.2876	3.5999	3.5000	3.0999	3.0000
Tx Bias(mA)	16.714	65.000	55.000	3.000	1.000
Tx Power(dBm)	-5.47	1.00	-3.00	-9.00	-12.01
Rx Power(dBm)	-4.31	1.00	-3.00	-25.09	-28.24

5. PoE

5.1 PoE Setting

Выберите “**PoE**-**PoE Setting**” для настройки:



Power Over Ethernet Configuration

Reserved Power determined by	Auto	Manual
Power Management Mode	Actual Consumption	Reserved Power

PoE Power Supply Configuration

Primary Power Supply [W]
250

PoE Port Configuration

Port	PoE Mode	Priority	PD Alive Check	Maximum Power [W]	Description
*	<>	<>	<>	30	
1	PoE+	Low	OFF	30	
2	PoE+	Low	OFF	30	
3	PoE+	Low	OFF	30	
4	PoE+	Low	OFF	30	
5	PoE+	Low	OFF	30	
6	PoE+	Low	OFF	30	
7	PoE+	Low	OFF	30	
8	PoE+	Low	OFF	30	
9	PoE+	Low	OFF	30	
10	PoE+	Low	OFF	30	

Save Reset

Power Over Ethernet Configuration

Reserved Power determined by	Auto	Manual
Power Management Mode	Actual Consumption	Reserved Power

PoE Power Supply Configuration

Primary Power Supply [W]
250

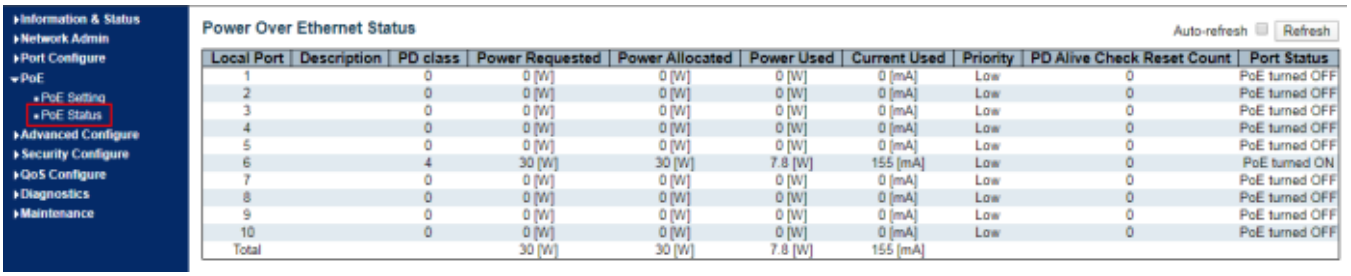
PoE Port Configuration

Port	PoE Mode	Priority	PD Alive Check	Maximum Power [W]	Description
*	<>	<>	<>	30	
1	PoE+	Low	OFF	30	
2	PoE+	Low	OFF	30	
3	PoE+	Low	OFF	30	
4	PoE+	Low	OFF	30	
5	PoE+	Low	OFF	30	
6	PoE+	Low	OFF	30	
7	PoE+	Low	OFF	30	
8	PoE+	Low	OFF	30	
9	PoE++	Low	OFF	90	
10	PoE++	Low	OFF	90	

Параметр	Описание
Power Reserve Mode	Доступны два режима резервирования мощности: • **Auto**: Порт коммутатора автоматически распределяет максимальную мощность в соответствии с определенным классом PD. Определения стандартов 802.3af/802.3at см. в соответствующей таблице мощностей. • **Manual**: Максимальная резервная мощность будет определяться пользователями.
Power Management Mode	Доступны два режиме управления мощностью: • **Actual Consumption**: При этой схеме работы порт с наименьшим приоритетом будет отключатся, если фактическая потребляемая мощность превышает номинальную мощность коммутатора. Порт с наивысшим приоритетом будет отключен, если все приоритеты находятся на одном уровне. • **Reserved Power**: При этой схеме работы порт с новым PD-устройством будет отключен, когда максимальная резервная мощность всех портов превысит номинальную мощность.
Max (Rated) Power Supply	Выбор максимальной мощность PoE на коммутаторе
PoE Mode	Выбор режима работы порта 802.3af (**PoE**)/802.3at (**PoE+**). 802.3at (PoE+) по-умолчанию.
Priority	Выбор приоритета PoE на порту (**Low**, **High**, **Critical**)
Maximum Power (W)	Режим "**Manual Allocation**" резервирует максимальную мощность на порту.

5.2 PoE Status

Выберите "**PoE**-**PoE Status**" для отображения информации о текущем статусе PoE:

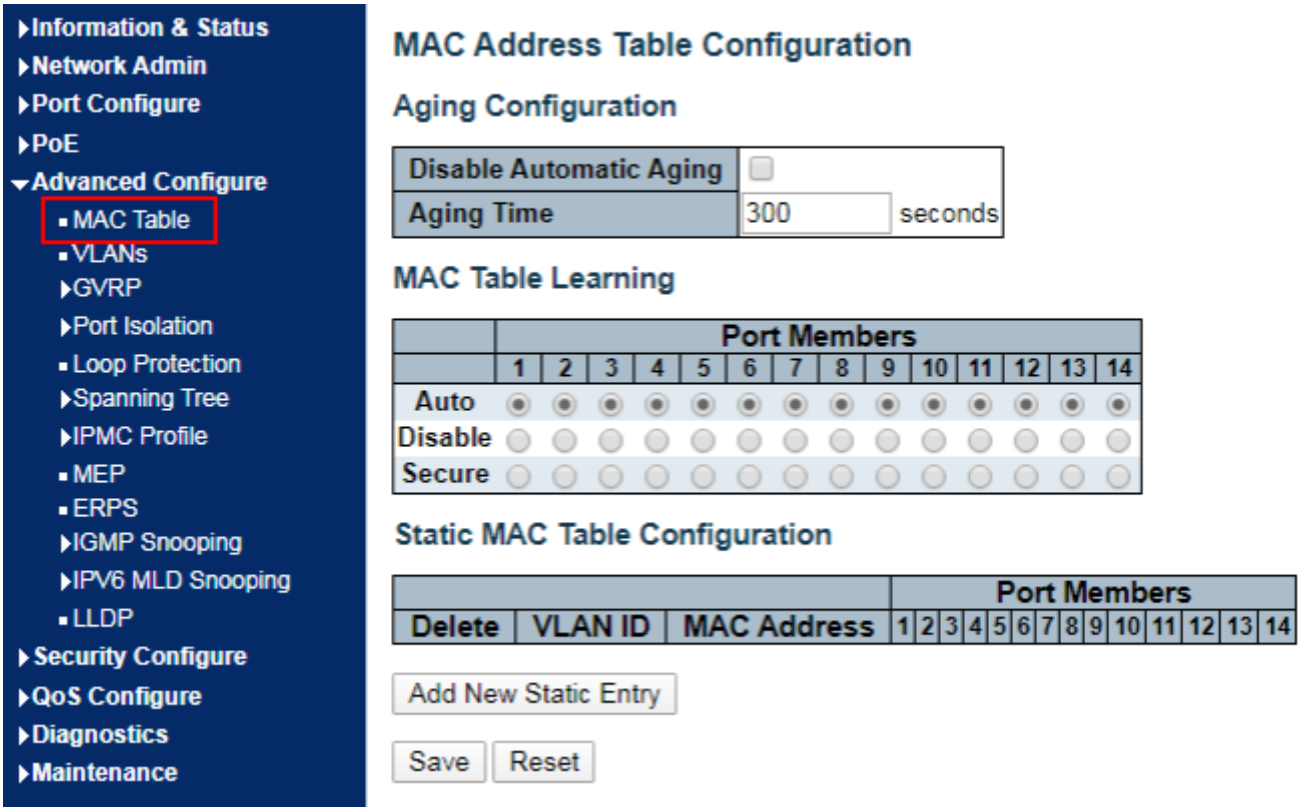


Страница отображает информацию о: Local Port, Description, PD Class, Power Requested, Power Allocated, Power Used, Current Used, Priority, Port Status.

6. Advanced Configure

6.1 MAC Table

Выберите “**Advanced Configure**-**MAC Table**” для отображения информации о MAC-адресах:



Параметр	Описание
Disable Automatic Aging	Динамический MAC-адрес, полученный коммутатором, не будет автоматически устаревать, если эта опция отмечена.
Aging Time	Динамический MAC-адрес, полученный коммутатором, автоматически устаревает через 300 с по умолчанию. Период варьируется от 10 с до 1000000 с.
Learn the MAC Address Table	Коммутатор совместим с 3 режимами работы с MAC-адресами: **Auto mode**: порты узнают MAC-адрес автоматически; **Disabled mode**: порты не будут узнавать MAC адреса; **Safe mode**: порты направляют поток данных по настроенным статическим MAC адресам.

6.2 VLANS

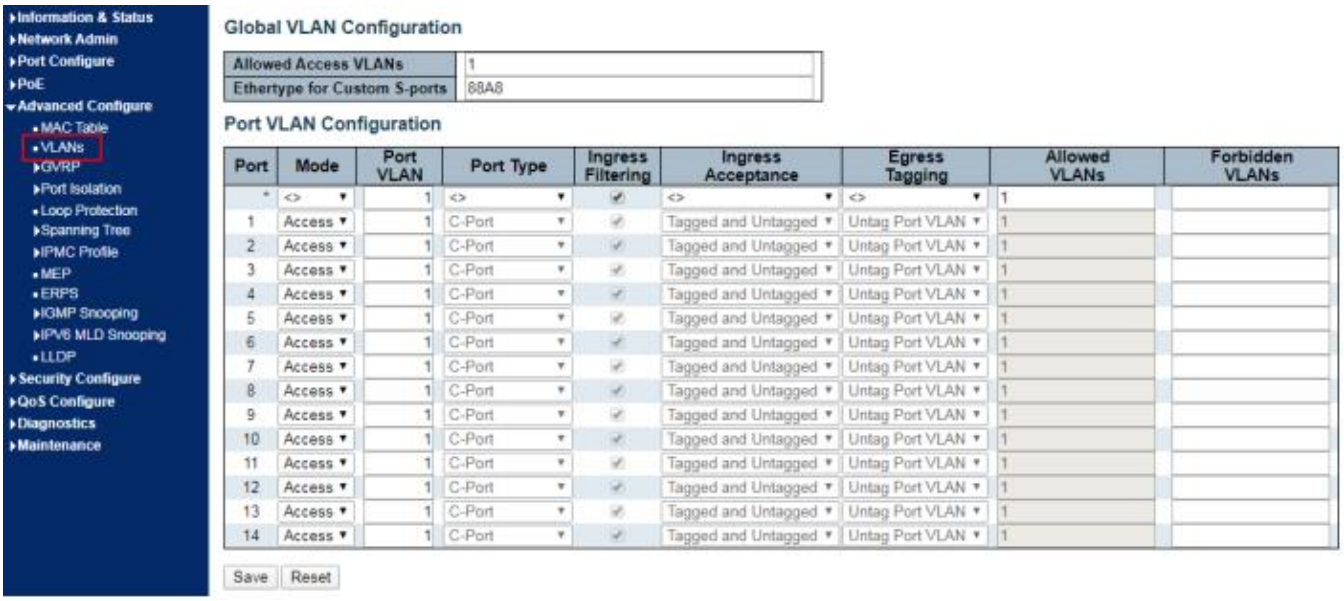
VLAN не имеет ограничений физического расположения, что означает, что хосты в одной VLAN могут быть размещены отдельно. Как показано ниже, каждая VLAN, являясь широковещательным доменом, делит физическую локальную сеть на несколько логических локальных сетей. Хосты могут обмениваться сообщениями традиционным способом. Для тех, кто находится в разных VLAN, необходимы такие устройства, как маршрутизаторы или коммутаторы уровня 3.

VLAN превосходит традиционный Ethernet по следующим параметрам:

- **Охват широковещательного домена**: широковещательные сообщения в локальной сети ограничены в VLAN для экономии полосы пропускания и более эффективной обработки проблем, связанные с сетью.
- **Безопасность локальной сети**: узлы VLAN не могут взаимодействовать друг с другом, поскольку сообщения разделены широковещательным доменом на уровне канала передачи данных. Для пересылки сообщений третьего уровня им требуется маршрутизатор или коммутатор третьего уровня.
- **Гибкость при создании виртуальной рабочей группы**: VLAN позволяет создать виртуальную рабочую группу, не зависящую от физической сети. Пользователи имеют доступ к сети без изменения конфигурации, если их физические местоположения перемещаются в пределах зоны действия сети.

Этот коммутатор поддерживает VLAN на основе IEEE 802.1Q, протоколов, MAC и портов. По умолчанию конфигурации принят режим 802.1Q VLAN.
VLAN на основе портов разделяется в зависимости от номера интерфейса коммутатора. Сетевой администратор присваивает каждому интерфейсу коммутатора другой PVID, а именно VLAN по умолчанию для порта. Если кадр данных без метки VLAN поступает на интерфейс коммутатора с PVID, он будет помечен тем же PVID, либо избавится от дополнительной метки несмотря на то, что интерфейс уже имеет PVID.
Решение для кадра VLAN зависит от типа интерфейса, что облегчает определение участника.

Выберите “**Advanced Configure**-**VLANs**” для настройки:

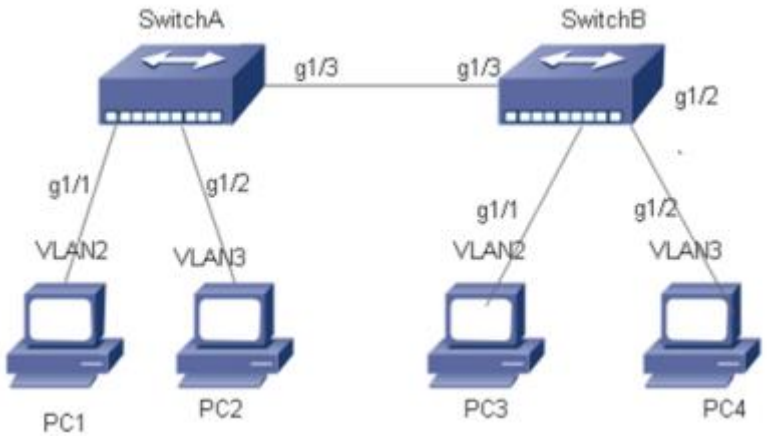


Параметр	Описание
Allowed Access VLANs	Отображение списка идентификаторов, разрешенных виртуальных локальных сетей доступа, с VLAN 1 по умолчанию. Добавьте идентификатор для нового разрешенного VLAN.
Ethertype for Custom S-ports	В этом поле задается Ethertype/TPID (указанный в шестнадцатеричном виде), используемый для пользовательских S-портов. Настройка действует для всех портов, тип порта которых установлен на S-Custom-Port.
Mode	Режим порта (по умолчанию - **Access**) определяет поведение порта. Порт может находиться в одном из трех режимов. При выборе определенного режима остальные поля в этой строке будут либо закрашены, либо изменены в зависимости от режима. Серые поля показывают значение, которое получит порт, когда будет применен данный режим применен. **Access**: Порты доступа обычно используются для подключения к конечным станциям. Режим работы **Access** имеет следующие характеристики: • Принадлежат только к одному VLAN - Port VLAN (он же Access VLAN), который по умолчанию равен 1 • Принимает не тегированные и C-тегированные кадры • Отбрасывает все кадры, не относящиеся к сети Access VLAN • На выходе все кадры, классифицированные для сети Access VLAN, передаются не тегированными. Другие (динамически добавляемые VLAN) передаются с тегами.

	Trunk: Магистральные порты могут передавать поток в нескольких VLAN одновременно и обычно используются для подключения к другим коммутаторам. Обычно эти порты используются для подключения к другим коммутаторам. Режим работы **Trunk** имеет следующие характеристики: • По умолчанию магистральный порт является членом всех VLAN (1-4094) • VLANs, к которым принадлежит магистральный порт, могут быть ограничены использованием разрешенных VLAN. • Кадры, отнесенные к VLAN, членом которой порт не является, отбрасываются • По умолчанию все кадры, кроме кадров, классифицированных в Port VLAN (Native VLAN), получают метку на выходе. Кадры, классифицированные в Port VLAN, не получают C-метки на выходе • Пометка на выходе может быть изменена **Hybrid**: Гибридные порты во многом похожи на **Trunk** порты, но в них добавлены дополнительные возможности настройки порта для применения **Access** режима. В дополнение к характеристикам, описанным для магистральных портов, гибридные порты обладают следующими возможностями: • Может быть настроен на работу без тегов VLAN или C-tag, S-tag или S-custom-tag • Можно управлять фильтрацией на входе • Прием кадров на входе и настройка тегов на выходе могут быть настроены независимо
Port VLAN	Определяет идентификатор VLAN порта (также известный как PVID). Разрешенные VLAN находятся в от 1 до 4094, по умолчанию - 1. При входе кадры классифицируются в VLAN порта, если порт настроен как VLAN unaware, кадр является не тегированным, или на порту включено понимание VLAN, но кадр имеет приоритетную метку (VLAN ID = 0). На выходе кадры, отнесенные к VLAN порта, не маркируются, если для настройки Egress Tagging configuration установлено значение untag Port VLAN. Порт VLAN называется "Access VLAN" для портов в режиме доступа и Native VLAN для портов в режиме Trunk или Hybrid.
Port Type	Порты в гибридном режиме позволяют изменять тип порта, то есть то, используется ли тег VLAN кадра для классификации кадра на входе в определенную VLAN, и то, используется ли тег VLAN для классификации кадра на входе в определенную VLAN. VLAN-тег используется для классификации кадра на входе в определенную VLAN, и если он совпадает, то на такой TPID он реагирует. Аналогичным образом, на выходе, тип порта

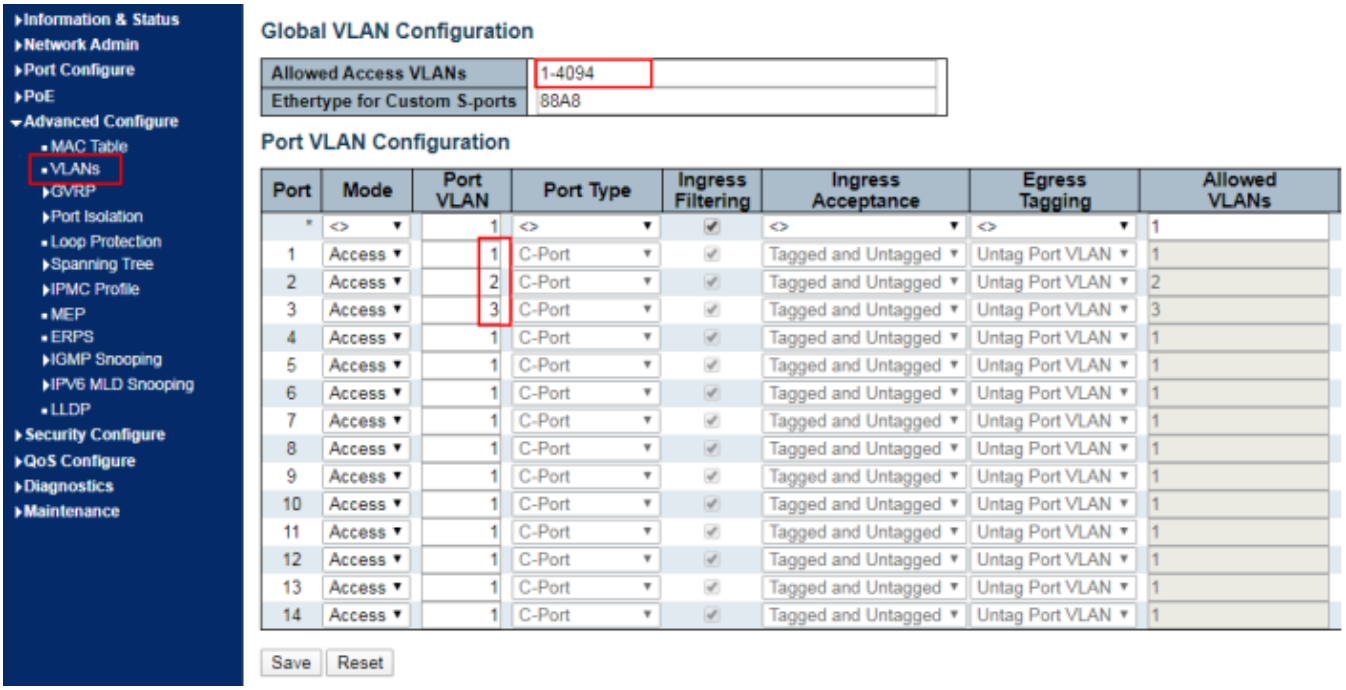
	определяет TPID метки, если такая метка требуется. **Unaware**: На входе все кадры, независимо от того, содержат они метку VLAN или нет, классифицируются в VLAN порта, и возможные теги не удаляются на выходе. **C-port**: На входе кадры с тегом VLAN с TPID = 0x8100 классифицируются по идентификатору VLAN, встроенному в тег. Если кадр не помечен или помечен приоритетом, он кадр классифицируется в VLAN порта. Если кадры должны быть помечены на выходе, они будут помечены C-тегом. **S-port**: На входе кадры с тегом VLAN с TPID = 0x8100 или 0x88A8 классифицируются по идентификатору VLAN, встроенному в тег. Если кадр является не тегированным или приоритетной меткой, кадр классифицируется в VLAN порта. Если кадры должны помечены на выходе, они будут помечены S-меткой. **S-Custom-Port**: На входе кадры с тегом VLAN с TPID = 0x8100 или равным Ethertype, настроенного для портов Custom-S, классифицируются по идентификатору VLAN встроенному в тег. Если кадр не тегирован или тегирован с приоритетом, он классифицируется в VLAN порта. Если кадры должны быть помечены на выходе, они будут помечены пользовательским S-тегом.
Ingress Filter	Гибридные порты позволяют изменять фильтрацию на входе. На порты access и trunk всегда включена фильтрация входящих сообщений. Если фильтрация на входе включена (флажок установлен), кадры, отнесенные к VLAN, членом которой порт не является, отбрасываются. Однако порт не будет никогда не будет передавать кадры, классифицированные для VLAN, членом которой он не является
Ingress Acceptance	**Hybrid** Гибридные порты позволяют изменять тип кадров, принимаемых на входе. **Tagged and Untagged** Принимаются как тегированные, так и не тегированные кадры. **Tagged Only** На входе принимаются только тегированные кадры. Не тегированные кадры отбрасываются. **Untagged Only** На входе принимаются только не тегированные кадры. Тегированные кадры отбрасываются.
Egress Tagging	Порты в режиме Trunk и Hybrid могут управлять маркировкой кадров на выходе. **Untag Port VLAN**

	Кадры, отнесенные к VLAN порта, передаются без тегов. Другие кадры передаются с соответствующей меткой **Tag All** Все кадры, независимо от того, отнесены они к VLAN порта или нет, передаются с тегом **Untag All** Все кадры, независимо от того, относятся они к виртуальной локальной сети порта или нет, передаются без метки Эта опция доступна только для портов в гибридном режиме.
Allowed VLANs	Порты в магистральном и гибридном режиме могут контролировать, какие VLAN могут быть разрешены. Порты доступа могут быть членами только одной VLAN - Access VLAN. Синтаксис поля идентичен синтаксису поля Enabled VLANs. По умолчанию магистральный или гибридный порт будет входить во все VLAN, поэтому для него установлено значение 1-4094. Поэтому для него установлено значение 1-4094. Поле можно оставить пустым, что означает, что порт не будет членом VLAN.
Forbidden VLANs	Порт может быть настроен на то, чтобы никогда не быть членом одной или нескольких VLAN. Это особенно полезно, когда динамические протоколы VLAN, такие как MVRP и GVRP включены и необходимо предотвратить динамическое добавление портов в VLAN. Особенность заключается в том, чтобы пометить такие VLAN как запрещенные на соответствующем порту. Синтаксис идентичен синтаксису, используемому в поле Enabled VLANs. По умолчанию поле оставлено пустым, что означает, что порт может стать членом любого из возможных VLAN.
Non-static port	Нажмите радиокнопку и укажите порт как нестатический. Нажмите кнопку "**Select All**", чтобы проверить все порты.



Пример настройки

1. Создайте VLAN 2 и 3 на коммутаторе A, добавьте VLAN к пользовательским интерфейсам и переведите GE1-3 в режим trunk. Сделайте тоже самое для коммутатора B, нажмите "**Advanced Configure-VLANs**" в дереве навигации, заполните соответствующие пункты и сохраните конфигурацию следующим образом.



2. Настройте тип интерфейса на коммутаторе A, подключенного к коммутатору B, а такой же передаваемый VLAN. Выполнив аналогичные действия для коммутатора B, щелкните "**Advanced Configure-VLANs**" в дереве навигации, заполните соответствующие пункты и сохраните конфигурацию следующим образом. Ниже показано, как добавить VLAN 2, что аналогично шагам добавления VLAN 3.

3. Проверьте результат конфигурации

Настройте параметры сетевого подключение у пользователей 1 и 2 в одном сегменте, например, 192.168.100.0/24 и настройте эти же параметры для пользователей 3 и 4 так же в одном сегменте, например, 192.168.200.0/24.

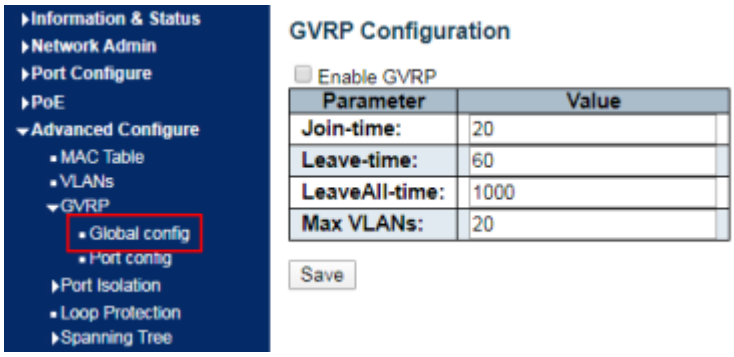
Пользователи 1 и 2 смогут видны друг для друга, но не смогут видеть пользователей 3 или 4, и наоборот.

6.3 GVRP

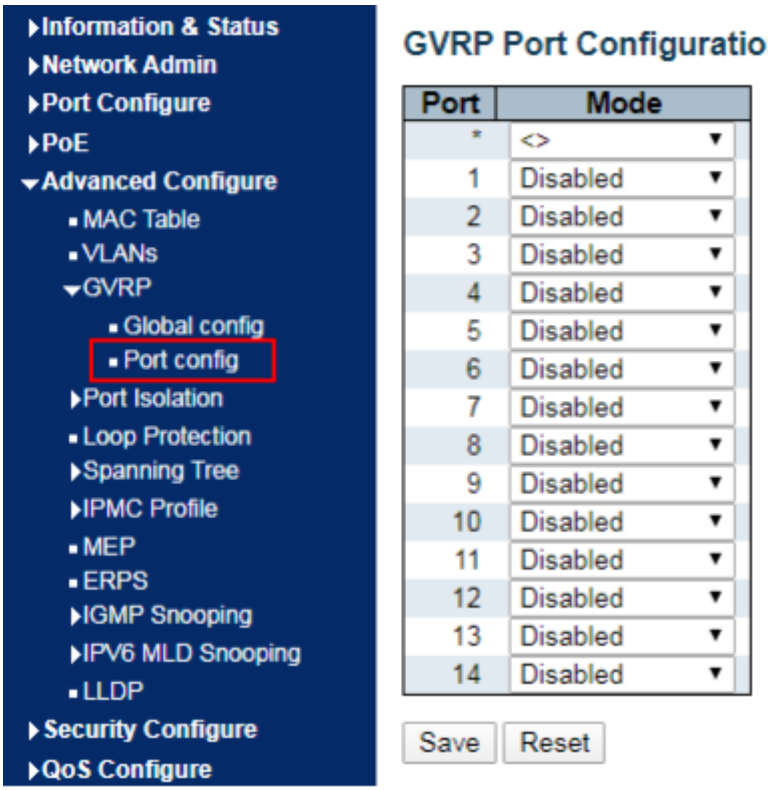
Протокол регистрации VLAN GVRP является приложением протокола регистрации общих атрибутов, который обеспечивает совместимую с 802.1Q функцию обрезки VLAN и динамическое создание VLAN на Trunk (магистральном) порту 802.1Q.
Коммутаторы, поддерживающие GVRP, могут обмениваться друг с другом информацией о конфигурации VLAN, отсекать ненужный широковещательный и неизвестный одноадресный трафик, а также динамически создавать и управлять VLAN на коммутаторах, подключенных через магистраль 802.1Q.

GID и GIP используются в GVRP, которые обеспечивают описание механизма общего состояния и механизм распространения информации для приложений на основе GARP для приложений, основанных на GARP, соответственно. GVRP работает только на магистральных каналах 802.1Q. GVRP отслеживает магистральный линк чтобы по магистральному линку передавался только активный VLAN. Прежде чем GVRP добавит VLAN в магистраль, он сначала получит информацию о присоединении от коммутатора. Информация об обновлении GVRP и таймер могут быть изменены. GVRP порты имеют различные режимы работы для управления тем, как они адаптируют VLAN. GVRP может динамически добавлять и управлять VLAN-ами из базы данных.
GVRP поддерживает распространение информации о VLAN между устройствами.
В GVRP информация VLAN коммутатора может быть настроена вручную, а все остальные коммутаторы в сети могут динамически понимать VLAN. Узел может получить доступ к любому коммутатору и подключиться к нужному VLAN. Для использования GVRP необходимо установить сетевую интерфейсную карту (NIC), совместимую с GVRP. Совместимая с GVRP сетевая карта может быть настроена на присоединение к требуемой VLAN, а затем и для доступа к коммутатору с поддержкой GVRP. Между сетевой картой и коммутатором устанавливается соединение, после чего будет реализовано соединение в VLAN.

Пример глобальной конфигурации:
Выберете пункт “**Advanced Configure-GVRP-Global config**” для включения функции и настройки её параметров



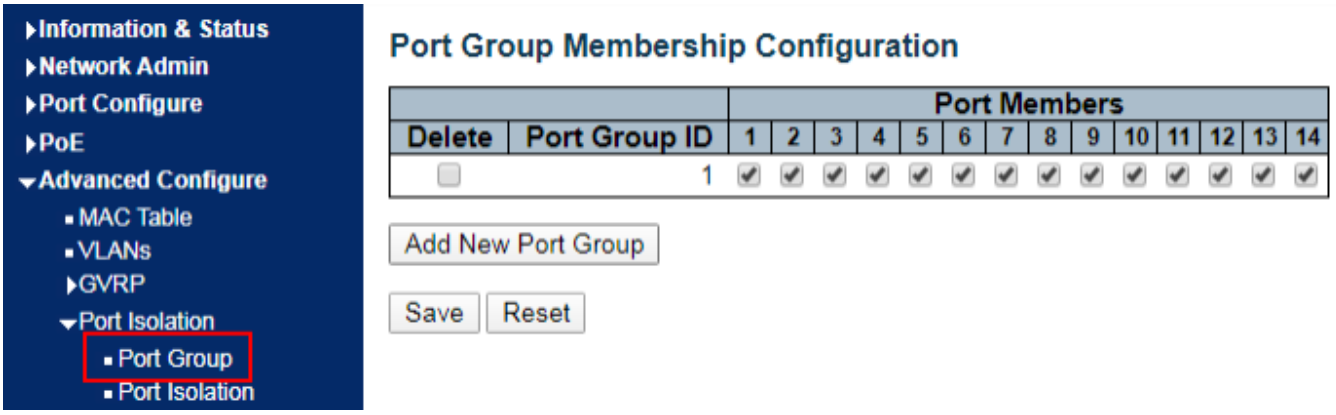
Пример конфигурации на порту:
Выберете пункт “**Advanced Configure**-**GVRP**-**Port config**” для включения функции на порту и настройки её параметров



6.4 Port Isolation

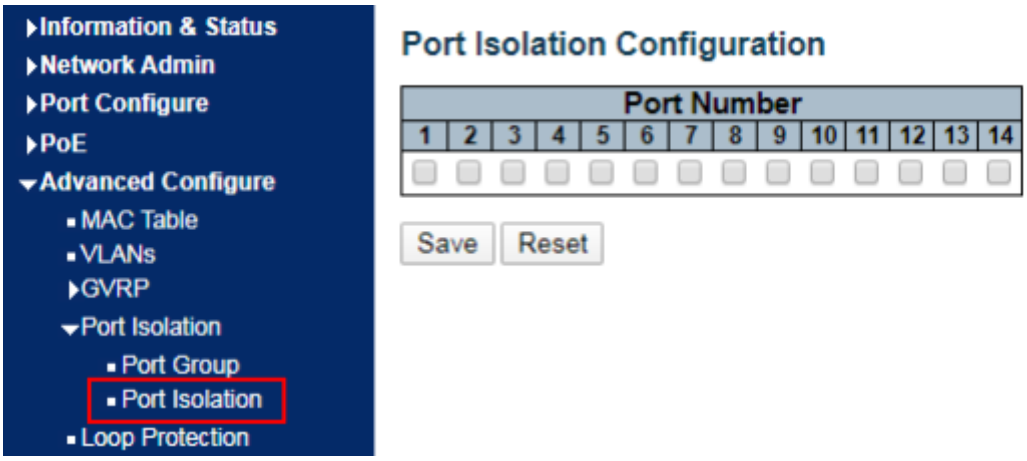
6.4.1 Port Group

Один порт может быть одновременно подчинен нескольким группам портов. Любые два порта могут пересылать поток данных, если они находятся в одной группе.
Выберите "**Advanced Configure-Port Isolation**", отметьте порт для создания группы изоляции и сохраните ее следующим образом



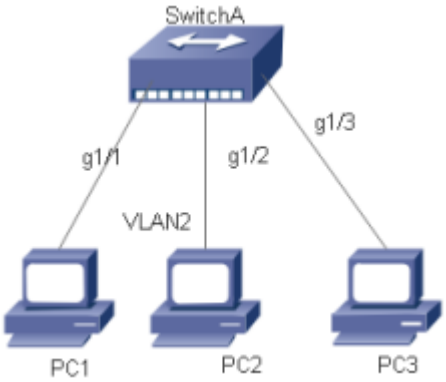
6.4.2 Port Isolation

Интерфейсы в одной группе будут изолированы друг от друга, чего не произойдет с интерфейсами в разных группах.
Выберите "**Advanced Configure-Port Isolation**", отметьте порт для создания группы изоляции и сохраните ее следующим образом

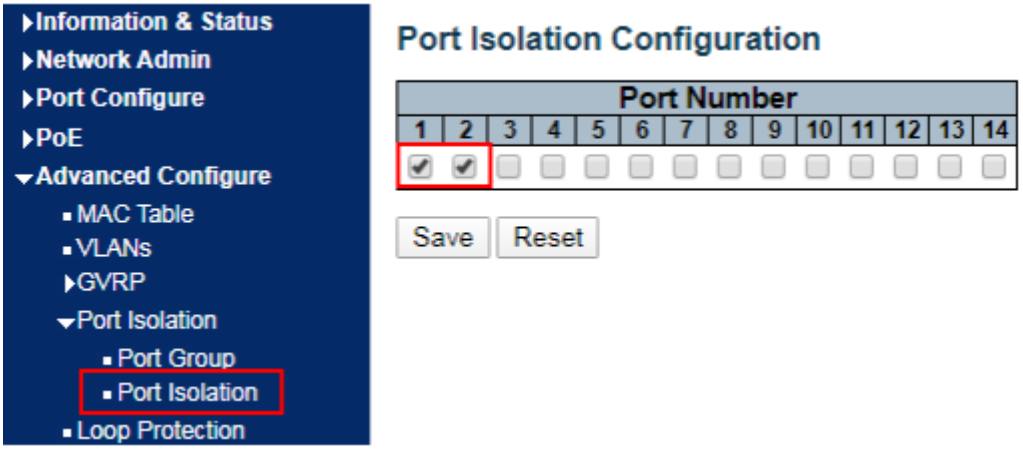


В следующем примере показано, что ПК1, 2 и 3 подчинены VLAN 1. Пользователи хотят заблокировать доступ между ПК1 и 2 в VLAN 1, но разрешить доступ между PC1 и 3, а также PC2 и 3.

Сетевая диаграмма примера конфигурации изоляции портов



Для настройки изоляции портов GE1-1 и GE1-2 нажмите кнопку "**Port Configure**-**Port Isolation**-**Port Isolation**", отметьте галочками порты GE1-1 и GE1-2, чтобы создать группу изоляции, и сохраните ее следующим образом.

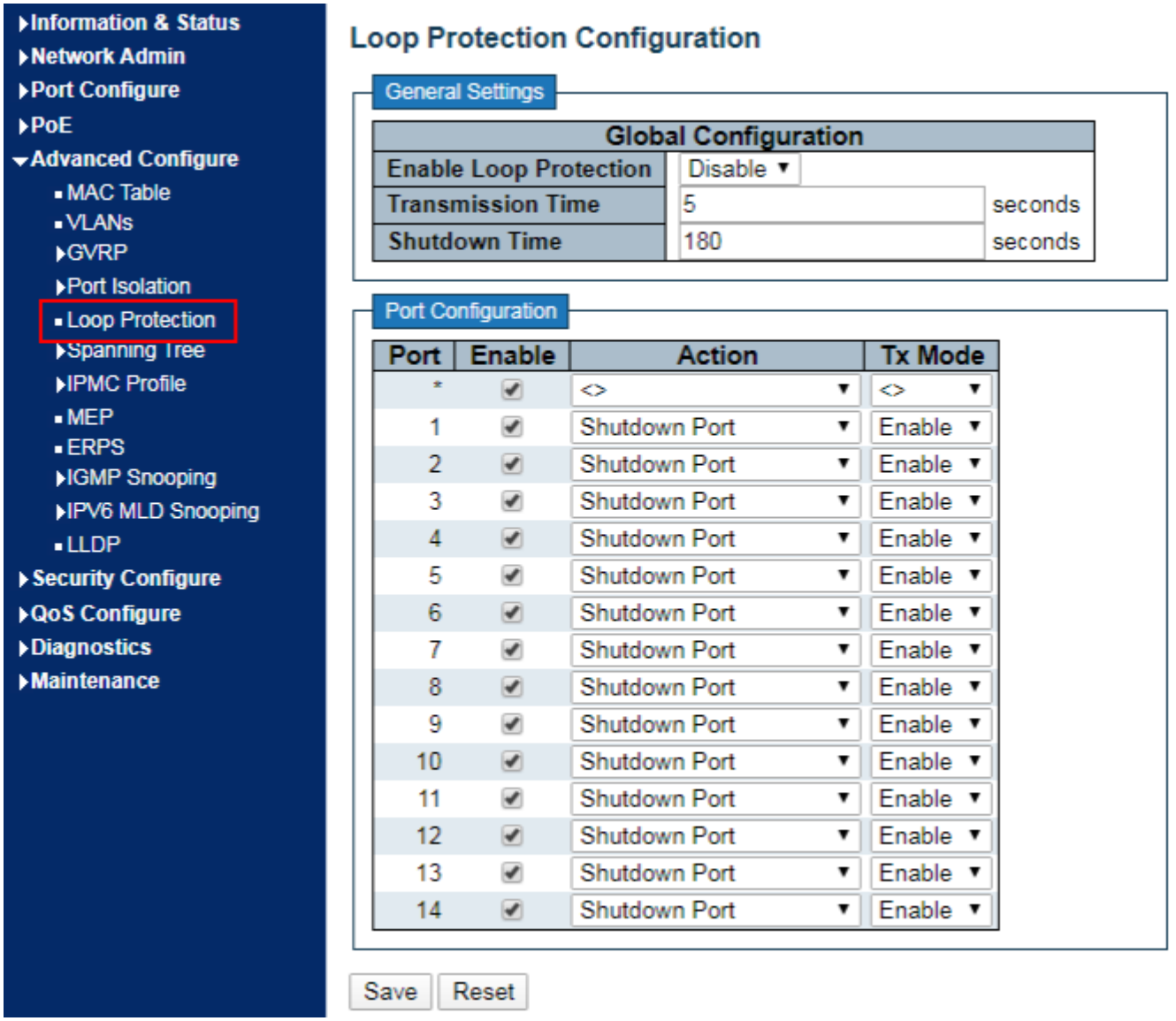


Проверьте результаты настройки:

- Ни PC1, ни PC2 не могут пинговать друг друга
- PC1 и PC3 могут пинговать друг друга
- PC2 и PC3 могут пинговать друг друга

6.5 Loop Protection

Защита от петель настраивается следующим образом: включается использование loop detection глобально и настраивается проверка портов коммутатора, чтобы пользователи могли изменять интервалы проверки и времени отключения портов. Существует 3 способа обработки обнаружения кольцевой сети портами: отключение портов, отключение портов с сохранением журналов и только сохранение журналов; Выберите пункт "**Advanced Configure**-**Loop Protection**" как показано ниже.



Параметр	Описание
General Settings	Настройте Enable Loop Protection, Transmission Time, and Shutdown Time
Port Configuration	Настройте Enable, Action and Tx Mode

6.6 Spanning Tree

Для резервирования каналов и повышения надежности сети Ethernet обычно используется резервирование каналов связи.
Однако такие каналы будут создавать петли в коммутируемой сети, что приведет к широковещательному шторму, нестабильному списку MAC-адресов и другие сбои, ухудшая качество связи пользователей или даже прерывая ее. Для решения этих проблем появился протокол STP (Spanning Tree Protocol).
Аналогично развиваются и другие протоколы, начиная с оригинального STP, определенного в IEEE 802.1D, и заканчивая RSTP (Rapid Spanning Tree Protocol), определенного в IEEE 802.1W, и MSTP (Multiple Spanning Tree Protocol),
В последнее время STP продолжает совершенствоваться.
MSTP совместим с RSTP и STP, в то время как RSTP совместим только с STP.

Различия между этими тремя протоколами заключаются в следующем:

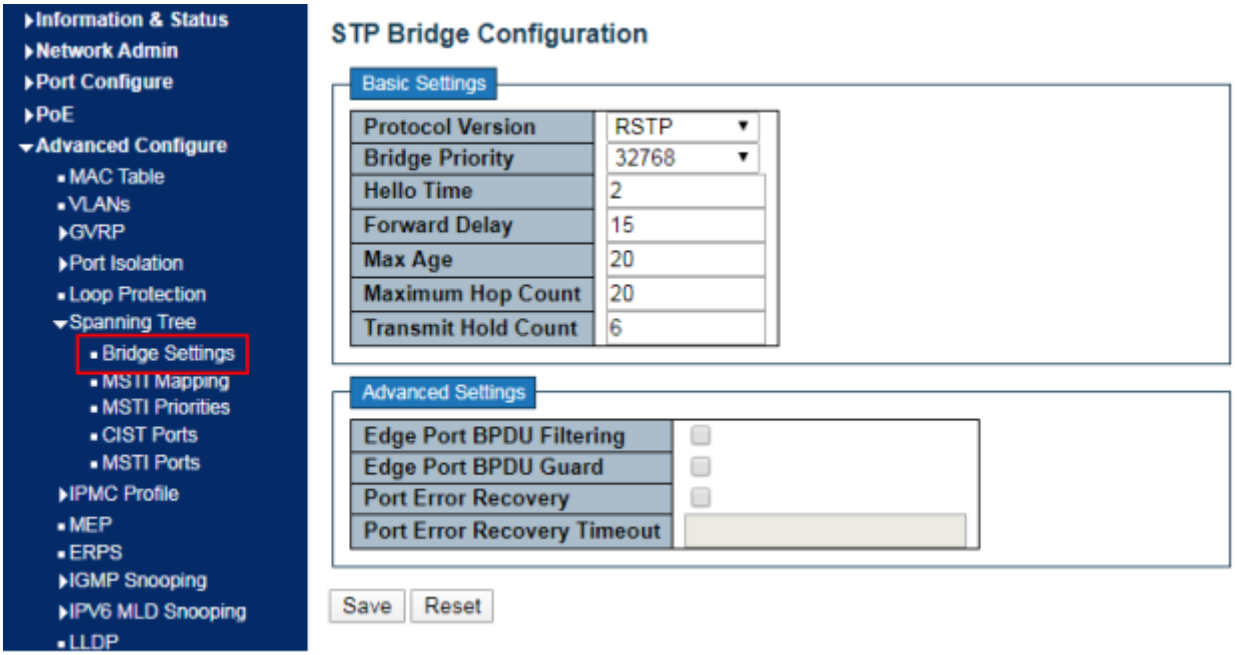
Протокол	Характеристики	Прикладной уровень
STP	Защищенная от петель топология используется в качестве решения проблемы широковещательного шторма и избыточного резервирования, работает медленно.	Все VLAN используют одно и то же Spanning tree без дискриминации по типу потока.
RSTP	Защищенная от петель топология формируется как решение проблемы широковещательного шторма и избыточного резервирования.	
MSTP	Защищенная от петель топология формируется как решение проблемы широковещательного шторма и избыточного резервирования. Дополнительно Spanning tree балансируют нагрузку в VLAN. Поток из разных VLAN будут пересылаться с учетом в зависимости от пути.	Поток данных следует различать для распределения нагрузки. Различные VLAN направляют поток через отдельные spanning tree.

После развертывания STP вычисление петель в сети используется с топологией, тем самым достигая цели при помощи:

- Loop elimination: устранение возможных петель связи в сети путем блокирования избыточных каналов.
- Link backups: активация резервных каналов для восстановления сетевого соединения в случае отказа основных путей передачи данных.

6.6.1 Bridge Configuration

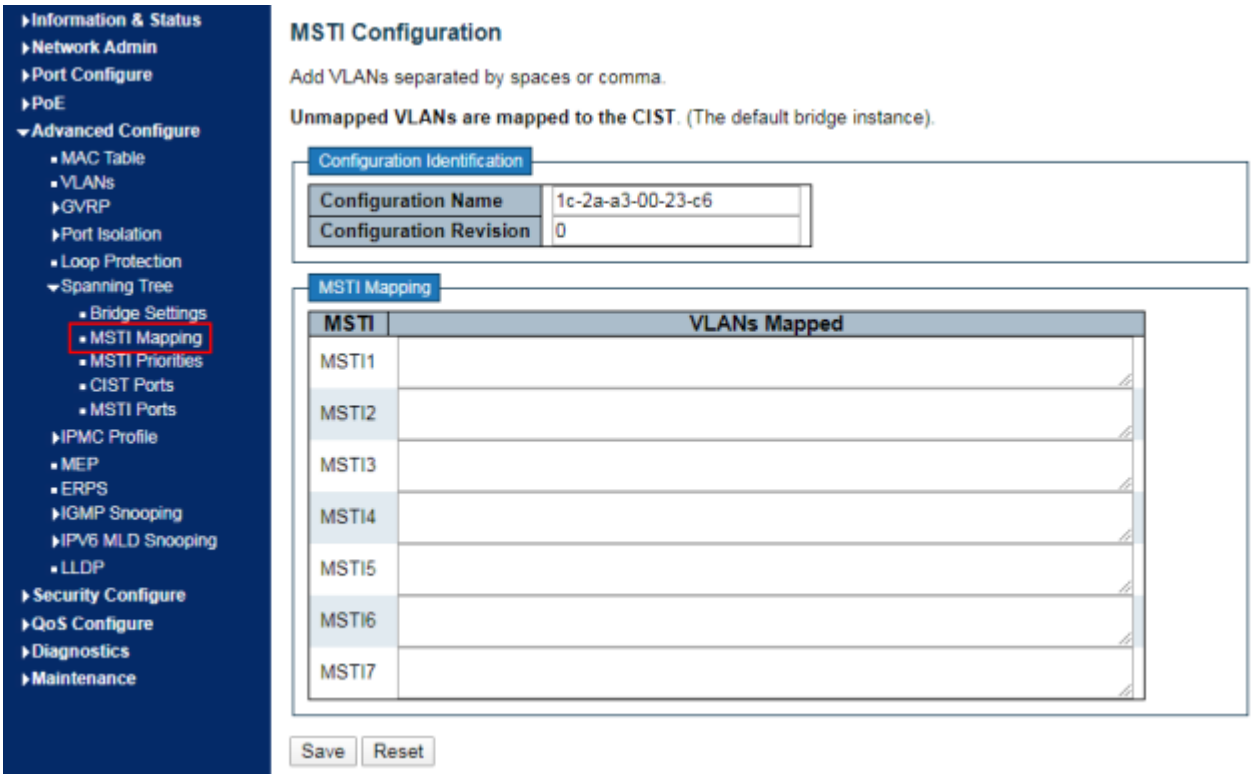
На этой странице пользователи могут настроить глобальные параметры моста STP. Щелкните "**Advanced Configure-Spanning Tree-Bridge Settings**" следующим образом:



Параметр	Описание
Protocol Ver	Выберите версию работы протокола STP для глобальной конфигурации: STP/RSTP/MSTP
Bridge Priority	Управление приоритетом моста. Меньшие числовые значения имеют больший приоритет. Номер экземпляра MSTI, объединенные с 6-байтовым MAC-адресом коммутатора, образуют идентификатор моста
Forward Delay (4-30s)	Диапазон задержки от 4 до 30 секунд. 15 секунд по умолчанию
Max Age (6-40s)	Диапазон времени, через которое информация устаревает и поступает новая. По умолчанию 20 секунд
Max hops (6-40)	Установка количества переходов между устройствами в области spanning tree до того, как BPDU (Bridge Protocol Data Unit), отправленный коммутатором, будет отброшен. Количество хопов будет уменьшаться на один каждый раз, когда пакет проходит через коммутатор. Пользователи могут установить количество хопов от 6 до 40, а по умолчанию - 20
Transmit Hold Count (1-10)	Максимальное количество пакетов “Hello” отсылаемых в интервал. В диапазоне от 1 до 10, 6 по умолчанию

6.6.2 MSTI Mapping

Выберите “**Advanced Configure-Spanning Tree-MSTI Mapping**”

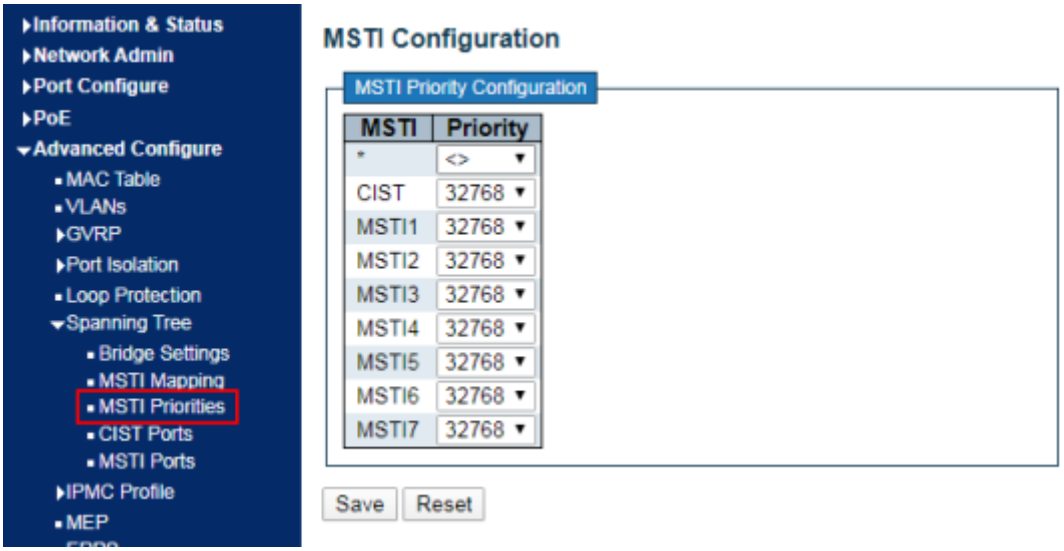


Параметр	Описание
Configuration Name	Настройка доменного имени MSTP
Configuration Revision	Выбор ревизии
MSTI Mapping	Введите VLAN-ы участвующие в группе

Примечание
Instance - это группа VLAN, которая снижает стоимость связи и скорость использования ресурсов. Каждый Instance, независимо от топологии, может балансировать нагрузку. VLAN с одинаковой топологией могут быть сгруппированы на один и тот же Instance, и они пересылаются в соответствии со статусом порта в соответствующих Instance MSTP. Проще говоря, один или несколько VLAN одновременно сопоставляются со Spanning Tree в Instanc-ax MSTP.

6.6.3 MSTI Priorities

Выберите “**Advanced Configure**-**Spanning Tree**-**MSTI Priorities**” для определения приоритетов MSTI:

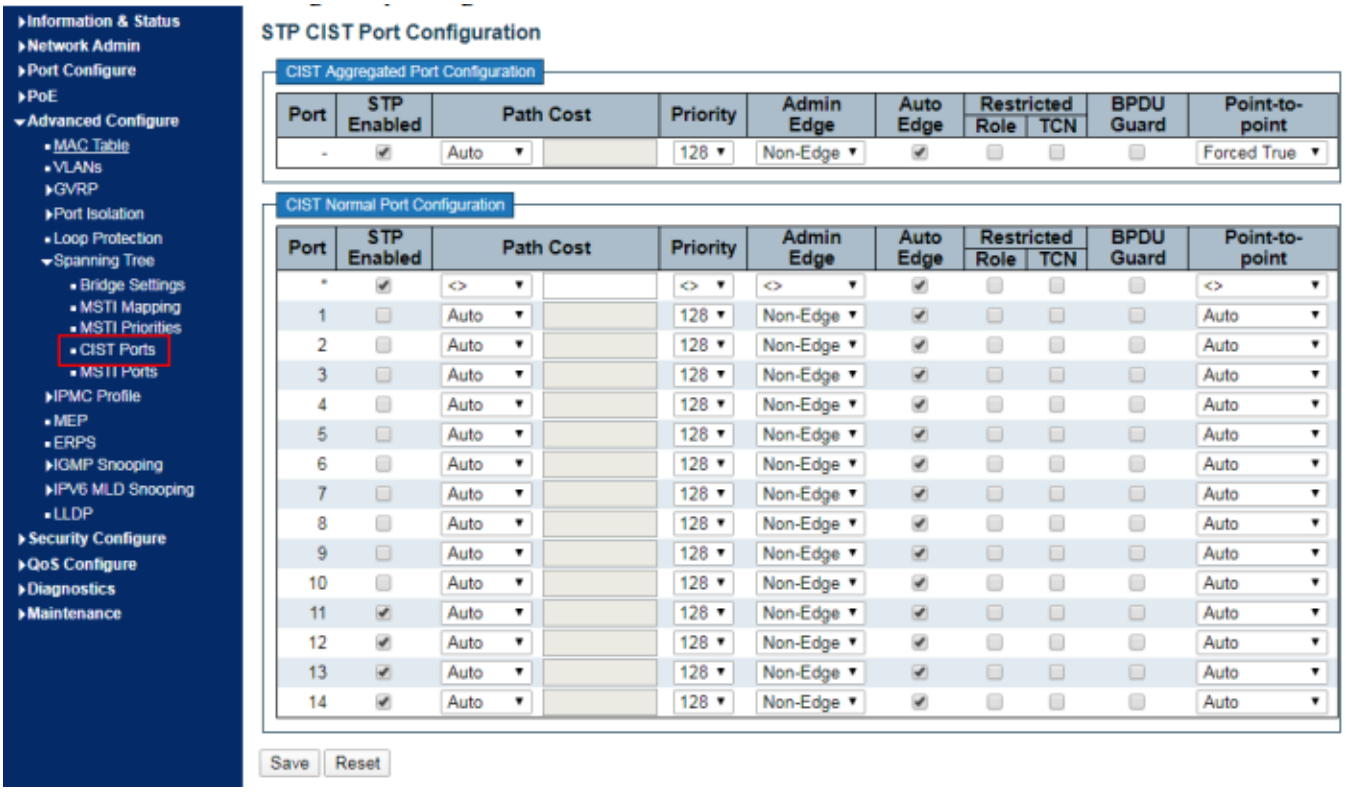


Приоритет может быть выставлен для каждого Instance MSTI в диапазоне от 0 до 61,440 с шагом 4,094.

www.giga-link.ru info@giga-link.ru +7 (499) 649-25-76

6.6.4 CIST Ports

Выберите “**Advanced Configure-Spanning Tree-CIST Ports**” для определения портов CIST:

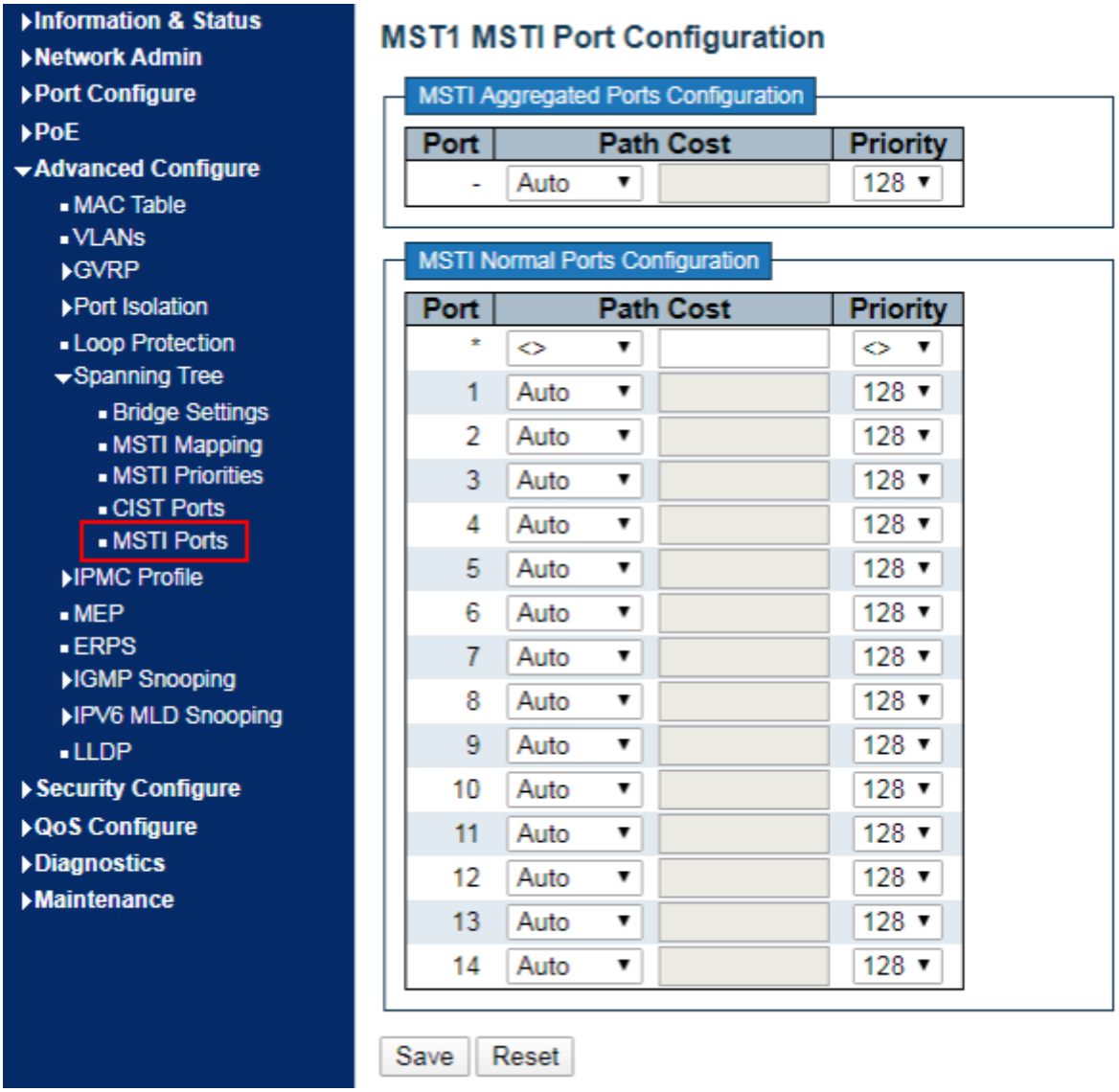


Параметр	Описание
Ring Network Enabled	Управляет включением STP на этом порту коммутатора.
Path Cost (0=Auto)	Управляет стоимостью пути, который несет порт. Параметр Авто установит стоимость пути в зависимости от скорости физического канала, используя рекомендованные значения 802.1D. Используя параметр Specific, можно ввести пользовательское значение. Стоимость пути используется при установлении активной топологии сети. Порты с более низкой стоимостью пути выбираются в качестве портов переадресации в пользу портов с более высокой стоимостью пути. Допустимые значения находятся в диапазоне от 1 до 200000000
Priority	Управляет приоритетом порта. Это может использоваться для контроля приоритета портов с одинаковым Path Cost.
AdminEdge	Определяет, должен ли флаг operEdge начинаться как установленный или очищенный. (Начальное состояние operEdge при инициализации порта)
Auto Edge	Управляет, должно ли активироваться автоматическое определение на порту

Restricted Role	Если этот параметр включен, порт не будет выбран в качестве корневого порта для CIST для любого MSTI, даже если он имеет лучший приоритет в spanning tree. Такой порт будет выбран в качестве альтернативного порта после выбора корневого порта. Если установлено, это может привести к отсутствию связности в spanning tree. Сетевой администратор может установить, чтобы мосты, внешние по отношению к основной области сети, не влияли на активную топологию spanning tree, возможно, потому что эти мосты не находятся под полным контролем администратора. Эта функция также известна как Root Guard.
Restricted TCN	Если этот параметр включен, порт не будет распространять полученные уведомления об изменении топологии и изменения топологии на другие порты. Если установлено, что это может вызвать временную потерю соединения после изменений в активной топологии spanning tree в результате постоянно неверной информации о местоположении изученной станции. Он устанавливается сетевым администратором для предотвращения внешних мостов по отношению к основной области сети, что приводит к сбросу адресов в этой области, возможно, из-за того, что эти мосты не находятся под полным контролем администратора или состояние физического канала подключенных локальных сетей часто изменяется
BPDU Protection	Если включено, порт отключается при получении действительных BPDU. В отличие от аналогичного параметра моста, статус пограничного порта не влияет на этот параметр. Порт, входящий в отключенное из-за ошибки состояние из-за этого параметра, также является объектом настройки восстановления порта моста
P2P	Управляет подключением порта к локальной сети «точка-точка», а не к общей среде. Это может быть определено автоматически или принудительно, либо истинно, либо ложно. Переход в состояние пересылки происходит быстрее для двухточечных локальных сетей, чем для совместно используемых сред

6.6.5 MSTI Ports

Выберите пункт “**Advanced Configure-Spanning Tree-MSTI Ports**” для настройки path cost и instance:

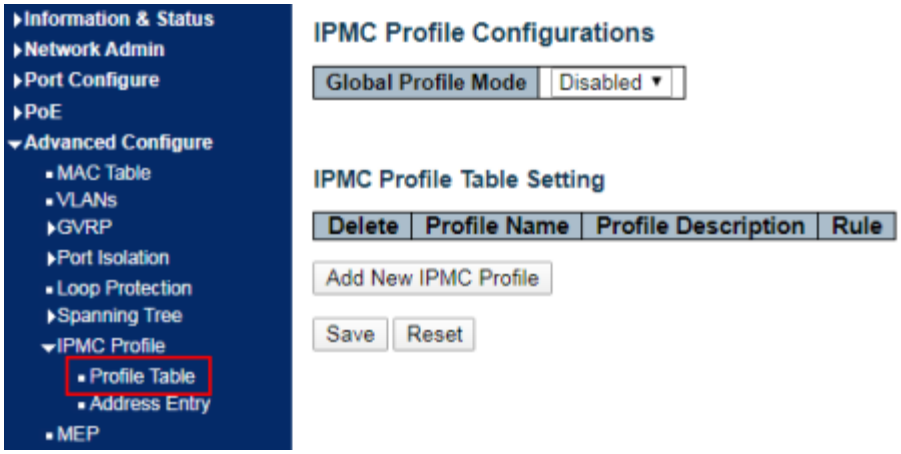


Параметр	Описание
Path Cost	Автоматическое определение Path cost, связанной с пересылкой пакетов в указанный список портов, по умолчанию 0 (авто). Чем меньше число, тем больше вероятность того, что коммутатор будет использовать этот порт для пересылки пакетов. Контролирует Path cost, используемого портом. Настройка Авто устанавливает стоимость пути в зависимости от в зависимости от скорости физического соединения, используя рекомендуемые значения 802.1D. С помощью параметра

	Specific можно ввести значение, определенное пользователем. Path cost используется при создании активной топологии сети. Порты с меньшей стоимостью пути выбираются в качестве портов пересылки в отличии от портов с более высокой Path cost. Допустимые значения находятся в диапазоне от 1 до 200 000 000.
Priority	Приоритет определяет состояние пересылки портов, когда Path cost одинаков

6.7 IPMC Profile

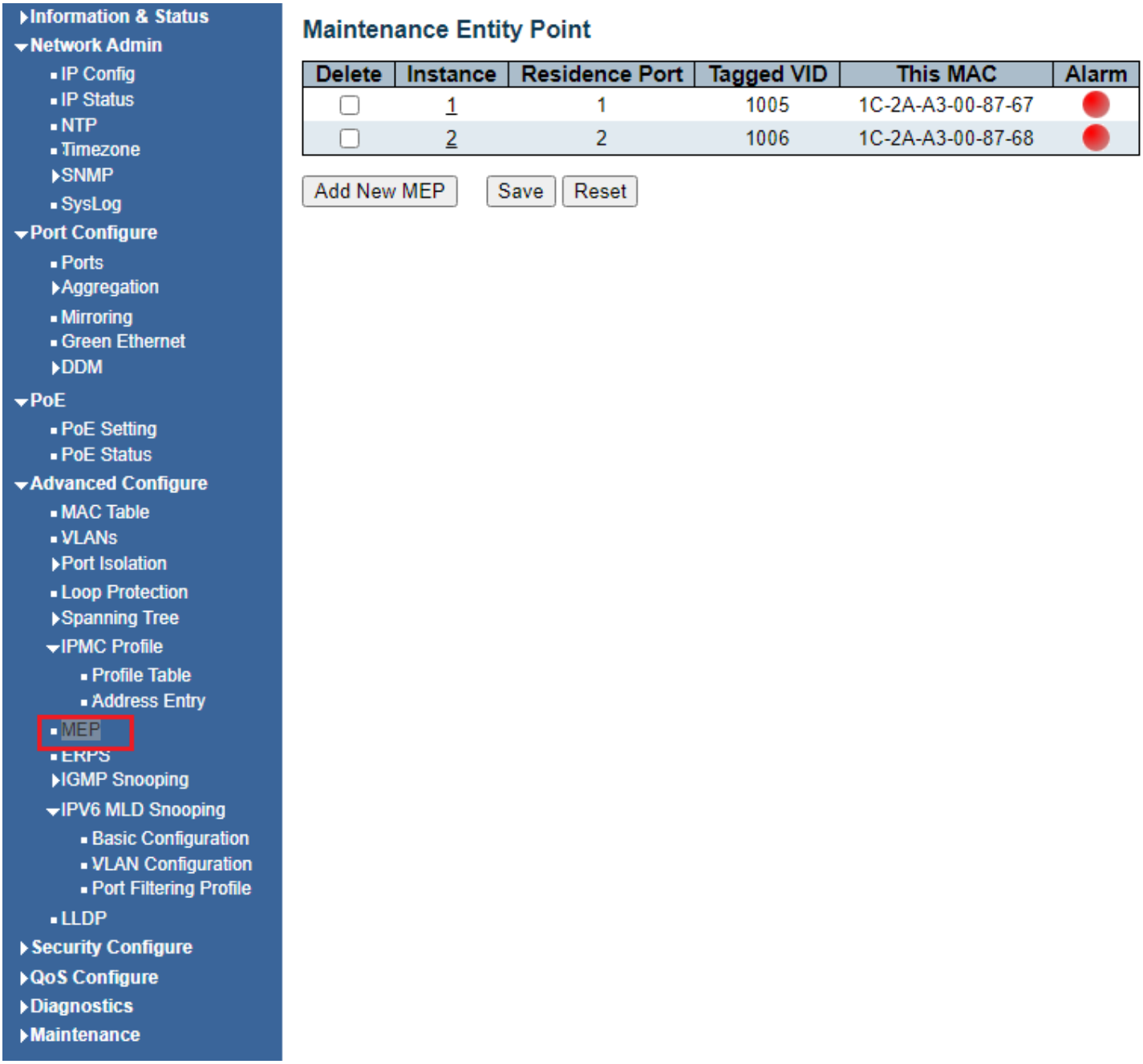
Выберите пункт “**Advanced Configure-IPMC Profile-Address Entry**” для настройки профиля IPMC (фильтр многоадресного списка):



Параметр	Описание
Entry Name	Введите имя группы фильтрации
Start Address	Введите начальный адрес группы
End Address	Введите конечный адрес группы

6.8 MEP

Maintenance Entity Point (Настройка точки обслуживания) — это демаркация точки на интерфейсе (порте), который участвует в CFM в пределах домена обслуживания. Точки обслуживания на портах устройств действуют как фильтры, которые ограничивают кадры CFM в пределах домена, отбрасывая кадры, не принадлежащие к нужному уровню.

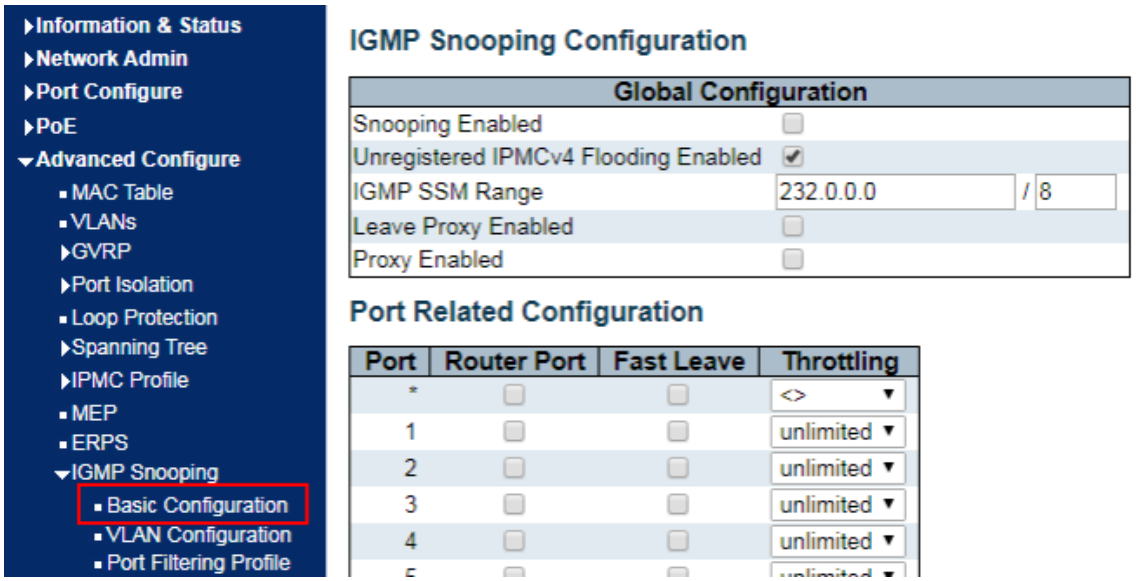


6.9 IGMP Snooping

IGMP Snooping (Internet Group Management Protocol Snooping) - это механизм управления и контроля многоадресной рассылки который работает на коммутаторе. Коммутатор сопоставляет свои интерфейсы с адресами многоадресных групп и соответствующим образом перенаправляет потоки многоадресных данных путем отслеживая IGMP-сообщений, полученных каждым интерфейсом, когда IGMP Snooping включен на этом интерфейсе.

6.9.1 Basic Configuration

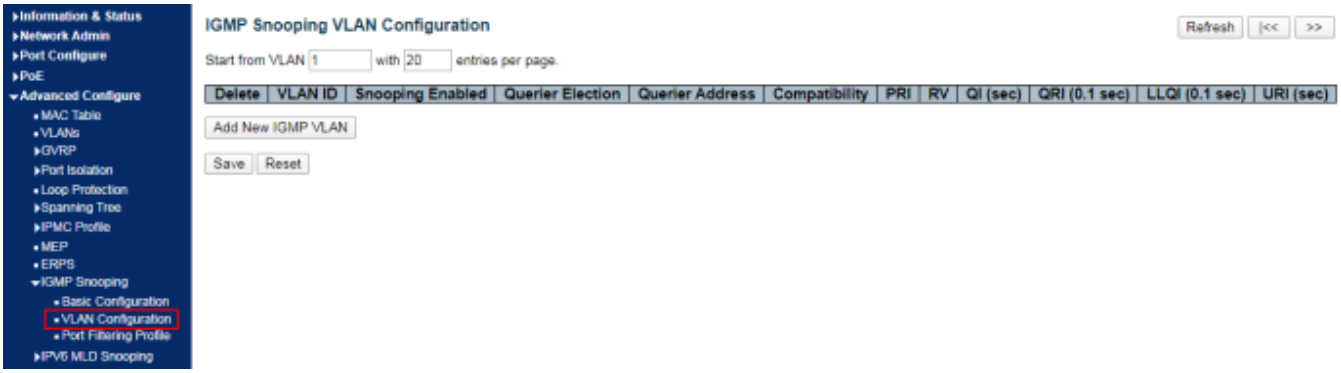
Выберите пункт "**Advanced Configure-IGMP Snooping-Basic Configuration**" для получения информации и конфигурации IGMP Snooping:



Параметр	Описание
Snooping Enabled	Включение/выключение IGMP Snooping
Unregistered IPMCv4 Flooding Enabled	Включение/выключение контроля флуда IPMCv4
Routing Port	Относится к порту, подключенному к маршрутизатору многоадресной рассылки уровня 3 или IGMP Querier. Укажите, какие порты выступают в качестве портов маршрутизатора. Порт маршрутизатора — это порт на коммутаторе Ethernet который ведет к устройству многоадресной рассылки 3-го уровня или IGMP Querier. Если порт члена агрегации выбран в качестве порта маршрутизатора, вся агрегация будет действовать как порт маршрутизатора
Fast Leave	Fast leave выполняет удаление записи MAC forward сразу после получения сообщения для отмены регистрации группы

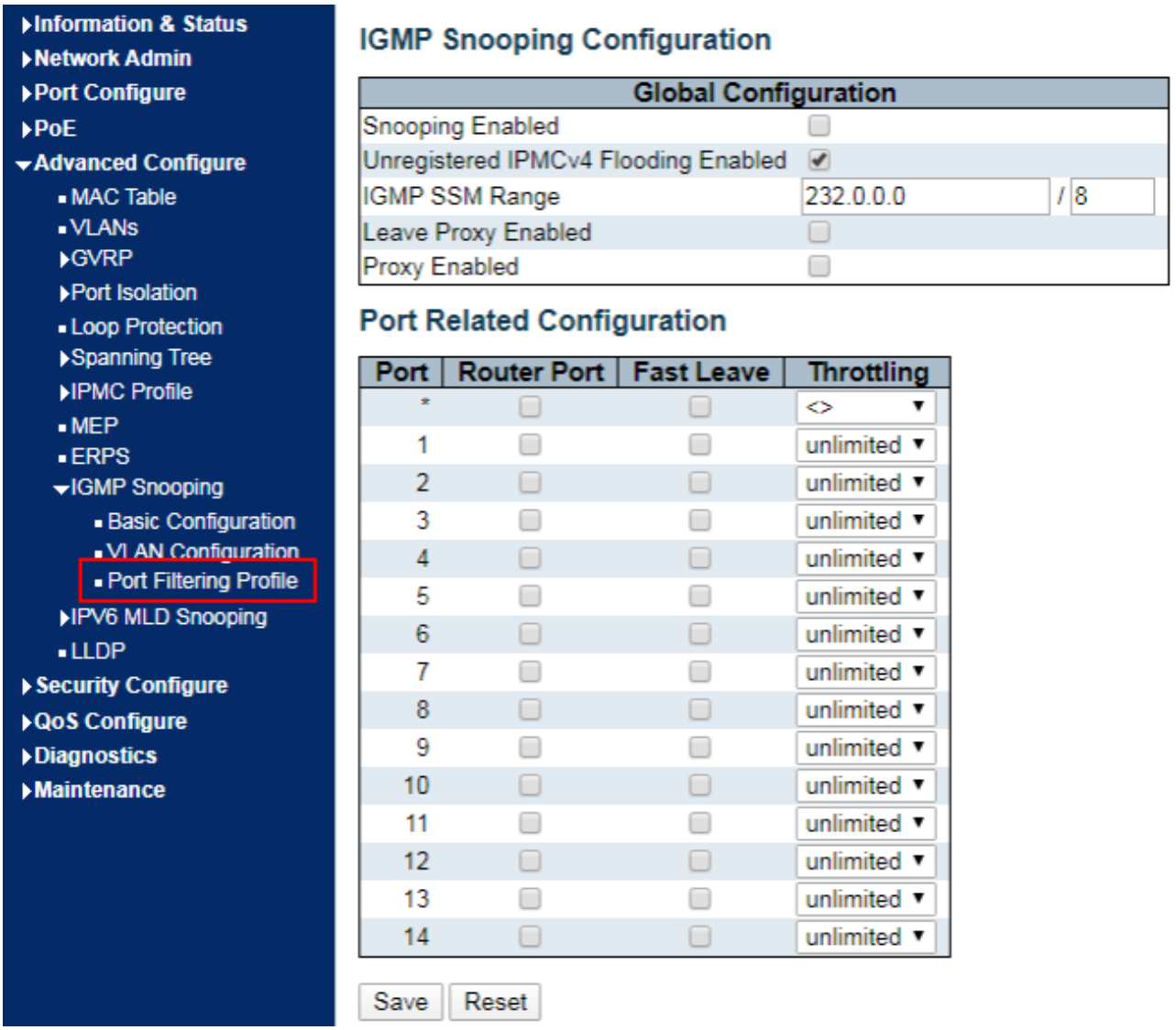
6.9.2 VLAN Configuration

Выберите “**Advanced Configure-IGMP Snooping-VLAN Configuration**” для настройки VLAN в IGMP Snooping:



6.9.3 Port Filtering Profile

Выберите “**Advanced Configure-IGMP Snooping-Port Filtering Profile**” для определения списка мультикаст трафика в IPMC профиле:



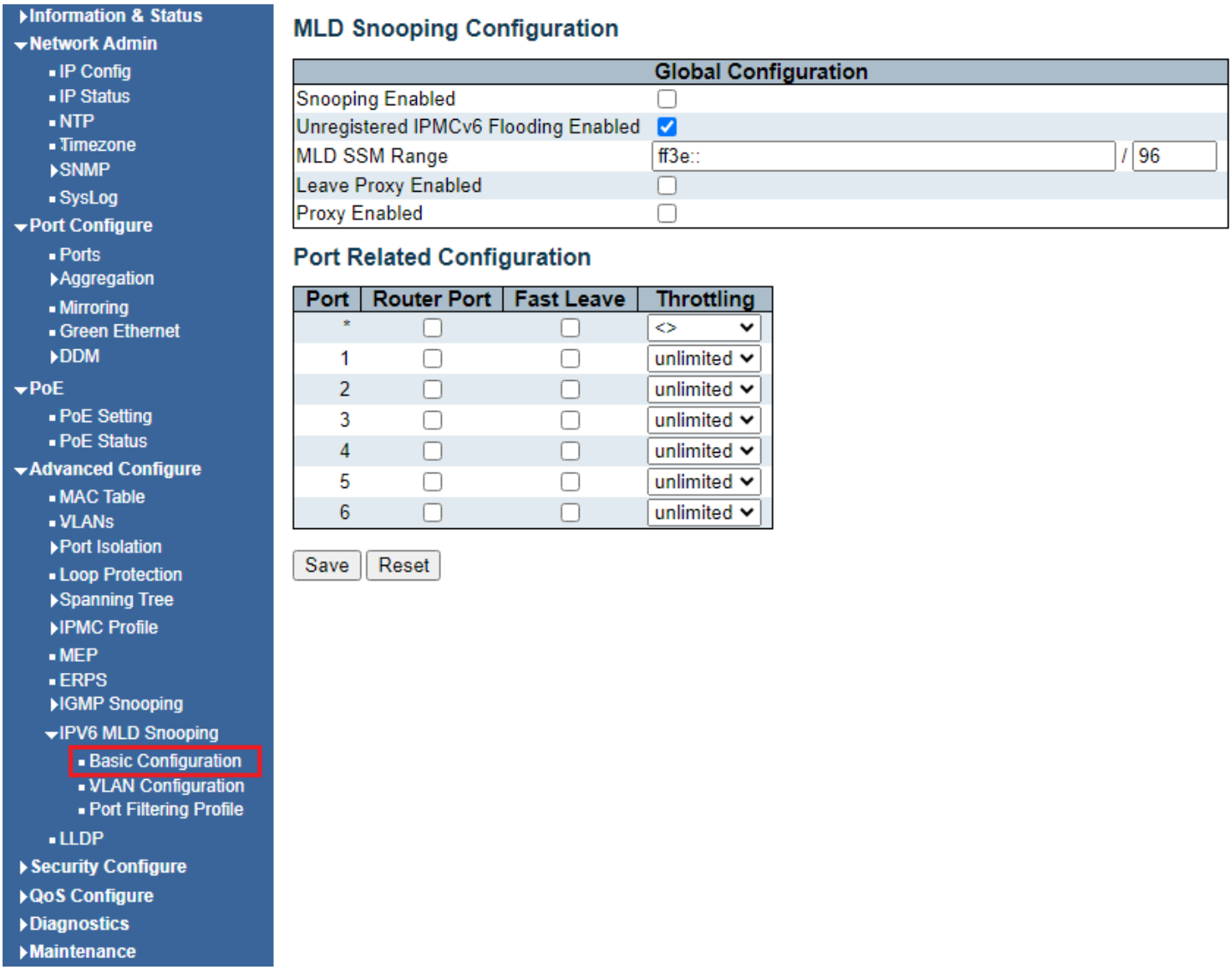
Параметр	Описание
VLAN ID	Используемый ID в диапазоне 1-4094
Snooping Enabled	Включите или отключите IGMP Snooping для каждого VLAN. Можно выбрать до 32 VLAN для IGMP Snooping
Querier Election	Включить или отключить выбор IGMP Querier. Включить, чтобы присоединиться к выбору IGMP Querier в VLAN. Отключить, чтобы действовать как IGMP NonQuerier.
Querier Address	Определение адреса IPv4 в качестве адреса источника, используемого в заголовке IP для выбора IGMP Querier. Если адрес Querier не задан, система использует IPv4-адрес управления IP-интерфейса, связанного с этим VLAN. Если адрес управления IPv4 не задан, система использует первый доступный адрес IPv4 как адрес управления. В противном случае система использует предварительно заданное значение. По умолчанию это значение будет 192.0.2.1

6.10 IPv6 MLD Snooping

IPv6 MLD Snooping — это механизм управления и контроля многоадресной рассылки, который работает на Ethernet-коммутаторе второго уровня.
Коммутатор сопоставляет свои интерфейсы с адресами многоадресных групп и соответствующим образом перенаправляет потоки многоадресных данных путем отслеживания сообщений IPv6 MLD, полученных каждым интерфейсом, когда функция IPv6 MLD Snooping включена.

6.10.1 Basic Configuration

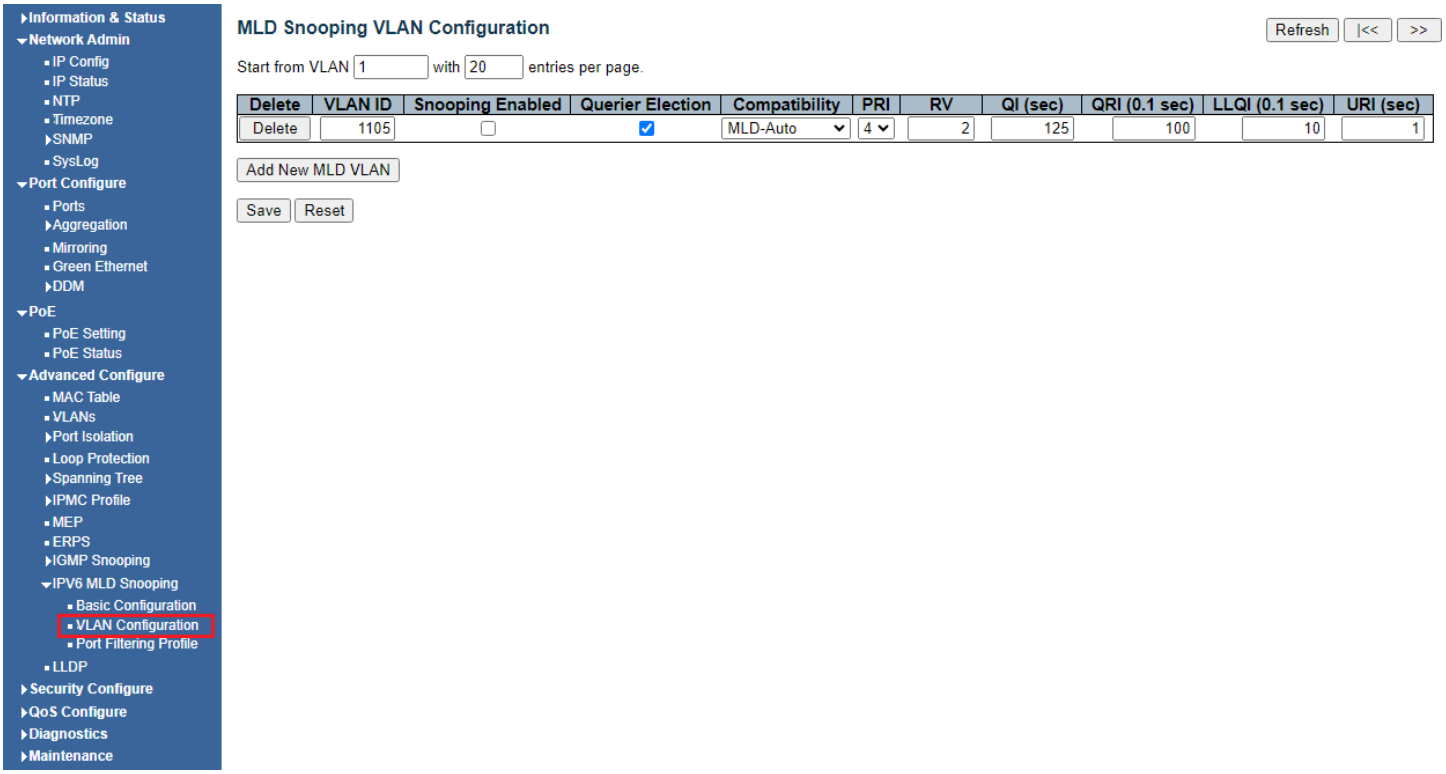
Выберите "**Advanced Configure-IPv6 MLD Snooping-Basic Configuration**"



Параметр	Описание
Enable Snooping	Включите или отключите IPv6 MLD Snooping
Unregistered IPMCv6 Flooding Enabled	Включить незарегистрированный поток трафика IPMCv6. Контроль флуда вступает в силу только тогда, когда MLD Snooping включен. Когда MLD Snooping отключен, незарегистрированный поток трафика IPMCv6 всегда активен, несмотря на этот параметр
MLD SSM Range	Диапазон SSM (Source-Specific Multicast) позволяет хостам и маршрутизаторам с поддержкой SSM запускать модель обслуживания SSM для групп в диапазоне адресов. В качестве префикса назначьте действительный адрес многоадресной рассылки IPv6 с длиной префикса (от 8 до 32) для диапазона
Leave Proxy Enabled	Включить MLD Leave Proxy. Эту функцию можно использовать, чтобы избежать пересылки ненужных сообщений о выходе на сторону маршрутизатора.
Proxy Enabled	Включить MLD Proxy. Эту функцию можно использовать, чтобы избежать пересылки ненужного соединения и оставлять сообщения на стороне маршрутизатора.
Routing port	Относится к порту, подключенному к маршрутизатору многоадресной рассылки уровня 3 или IGMP Querier. Укажите, какие порты выступают в качестве портов маршрутизатора. Порт маршрутизатора — это порт на коммутаторе Ethernet, который ведет к устройству многоадресной рассылки 3-го уровня или MLD querier. Если порт члена агрегации выбран в качестве порта маршрутизатора, вся агрегация будет действовать как порт маршрутизатора
Fast leave	Fast leave выполняет удаление записи MAC forward сразу после получения сообщение об отмене регистрации группы
Throttling	Включите, чтобы ограничить количество групп многоадресной рассылки, к которым может принадлежать порт коммутатора. Выбор из <>/1-10/Unlimited

6.10.2 VLAN Configuration

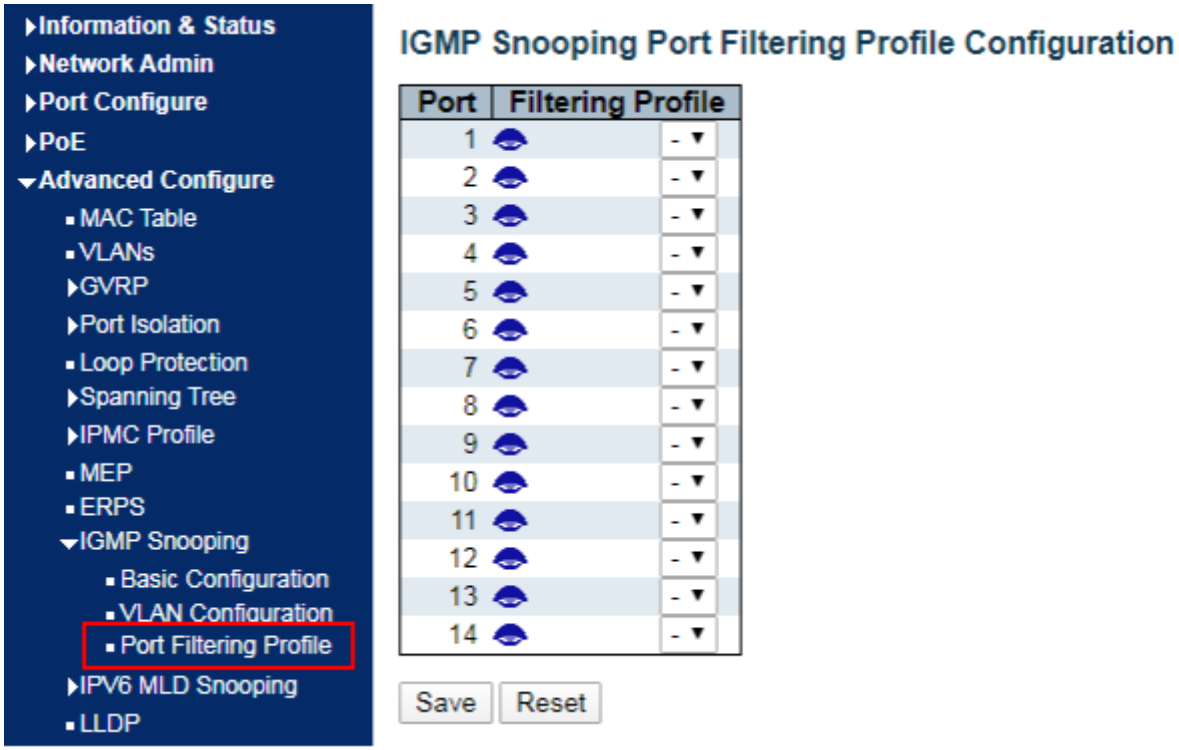
Выберите “**Advanced Configure-IPV6 MLD Snooping-VLAN Configuration**” для конфигурации MLD:



Параметр	Описание
VLAN ID	Используемый ID в диапазоне 1-4094
Snooping Enabled	Включите или отключите MLD Snooping для каждого VLAN. Можно выбрать до 32 VLAN для MLD Snooping
Querier Election	Включить или отключить выбор MLD Querier. Включите, чтобы присоединиться к выбору MLD Querier в VLAN. Отключить, чтобы действовать как MLD NonQuerier.
Compatibility	MLD-Auto/Forced MLDv1/Forced MLDv2
Querier Address	Определите IPv6-адрес в качестве адреса источника, используемого в IP-заголовке для выбора MLD Querier. Если адрес Querier не задан, система использует IPv6-адрес управления IP-интерфейса, связанного с данным VLAN интерфейса, связанным с этим VLAN. Если адрес управления IPv6 не задан, система использует первый доступный адрес IPv6 адрес управления. В противном случае система использует предварительно заданное значение

6.10.3 Port Filtering Profile

Выберите "**Advanced Configure-IPv6 MLD Snooping-VLAN Configuration**" для включения фильтрации в IPv6 MLD:

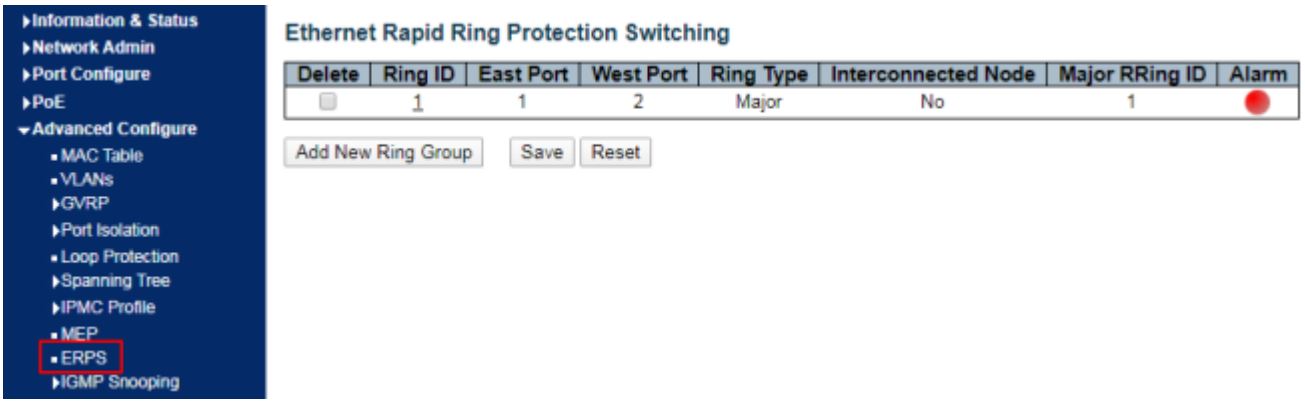


6.11 ERPS

ERPS (Ethernet Ring Protection Switching) является новейшим стандартом, ITU-TG.8032 ERPS и поддерживает многокольцевые и много доменные структуры, вбирает в себя преимущества EAPS, RPR, SDH, STP и т.д., и оптимизирует механизм проверки с точки зрения двусторонних неисправностей. Кроме того, поддерживается резервирование основного устройства, распределение нагрузки и другие методы работы при 50-мс переключении.

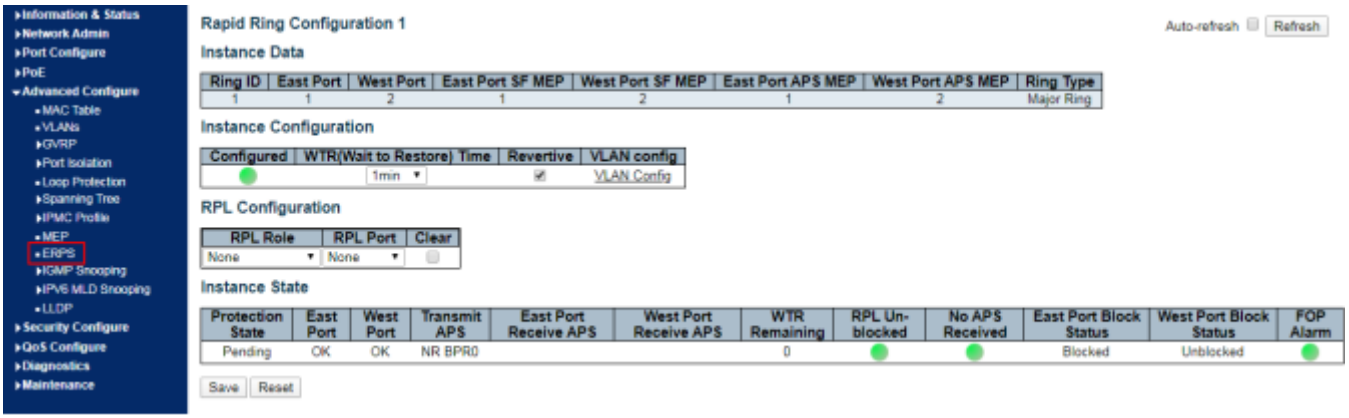
Примечание: перед включением ERPS отключите STP.

Выберите "**Advanced Configure-ERPS**":



Параметр	Описание
Ring ID	ID и ERPS идентификатор Instance
East Port	Выберите номер порта используемый в Ring Protection
West Port	Выберите номер другого порта используемый в Ring Protection
Ring Type	Выберите “Main Ring” и “Sub Ring” (Только в многокольцевых вариациях), с “Main Ring” по умолчанию
Interconnection Node	Он относится к узлу, соединяющему 2 или более колец в многокольцевом приложении одновременно
Main Ring ID	“Main Ring” раздает тот же ID что и в однокольцевой конфигурации, “Sub Ring” совпадает с “Main Ring” в многокольцевой конфигурации
R-APS VLAN (1- 4,094)	VLAN используемый в R-APS VLAN

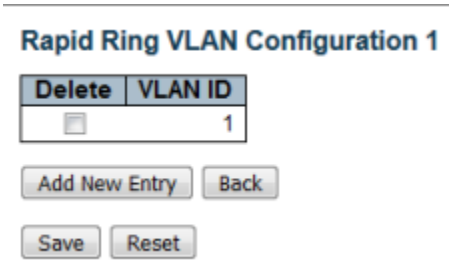
Нажмете “**Add New Ring Group**” для добавления Ring ID и настройки ERPS Ring:



Параметр	Описание
WTR Time (5-12s)	Включите этот пункт для установки WTR Time R-APS функции, по умолчанию 1 минута
Restore the Revertive Mode	Включите/выключите пункт для выбора режима из выпадающего списка для функции R-APS

VLAN Protection	Выберите пункт “VLAN Protection” для редактирования группы защищенного VLAN
RPL Role	Выберите из “None”, “RPL Owner”, “RPL Neighbor”
RPL Port	Выберите из “None”, “East Port”, “West Port”

Нажмите **“Save”** для сохранения
Выберите “**VLAN Protection**” для редактирования защиты VLAN

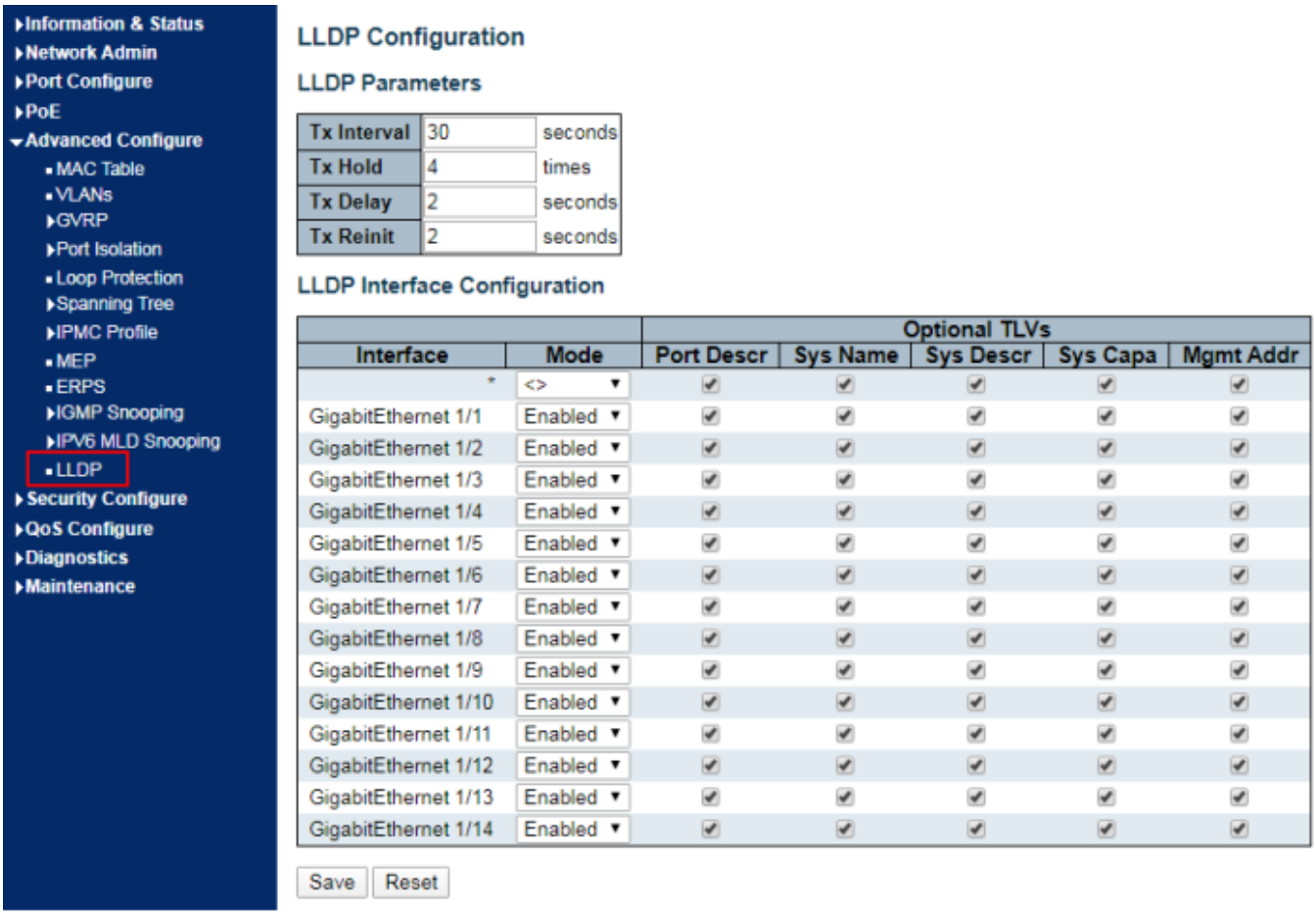


Примечание: имеется возможность добавить иной защищённый VLAN (ID 1 по умолчанию)

6.12 LLDP

Link Layer Discovery Protocol (LLDP) - это независимый от производителя протокол второго уровня, который позволяет сетевым устройствам уведомлять локальные подсети о своей идентификации и производительности.
В настоящее время диверсифицированные сетевые устройства со сложной конфигурацией нуждаются в стандартной платформе обмена информацией, чтобы производители могли обнаружить другие устройства и обменяться информацией о своих уникальных системах и конфигурации.
LLDP - это стандартный метод обнаружения канального уровня, который объединяет такую информацию, как основные возможности, адреса управления, идентификаторы устройств и интерфейсов оконечных устройств в TLV (Type/Length/Value), инкапсулирует его в LLDPDU (Link Layer Discovery Protocol Data Unit) и отправляет его непосредственно подключенным соседям. После получения информации они сохраняют ее в виде стандартной базы данных MIB (Management Information Base) для запросов NMS и для работы с соединениями Base для запросов NMS и оценки связи по каналу.

Нажмите кнопку "**Advanced Configure-LLDP**" следующим образом:

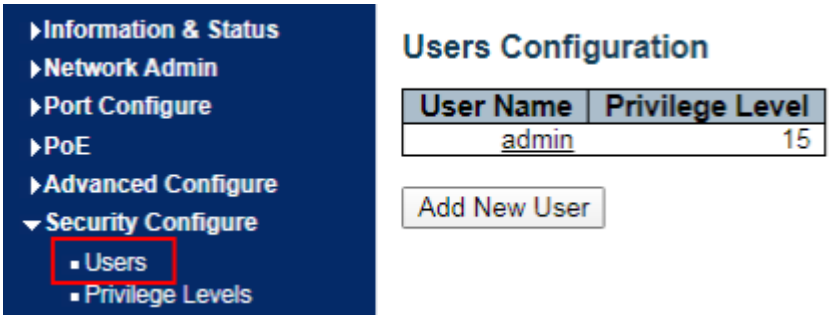


7. Security Configure

Настройки безопасности коммутатора

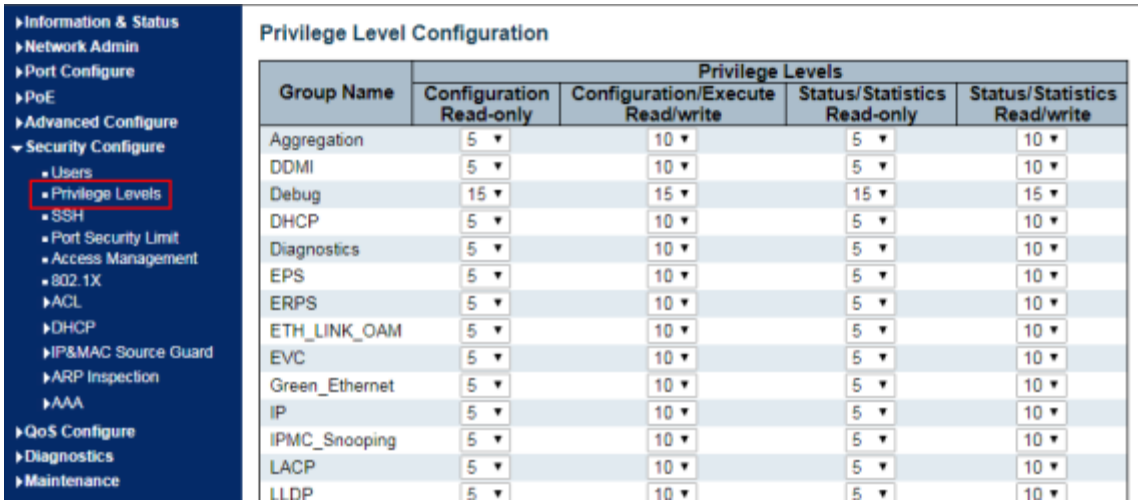
7.1 Users

В этом пункте возможно задать комбинацию пользователь/пароль
Выберите пункт для “**Security Configure-Users**” для изменения и нажмите “Save” для сохранения изменений:



7.2 Privilege Levels

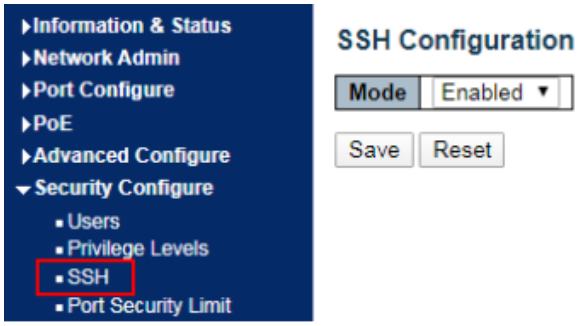
В этом пункте возможно задать приоритеты доступа для логина
Выберите “**Security Configure-Privilege Levels**” для настройки уровней доступа:



7.3 SSH

SSH (Secure Shell) - это протокол безопасности, основанный на прикладном уровне и разработанный рабочей группой по сетевым технологиям IETF.
SSH обеспечивает надежную работу сетевых служб, особенно службы Rlogin Session. Он может предотвратить раскрытие информации при удаленном управлении.

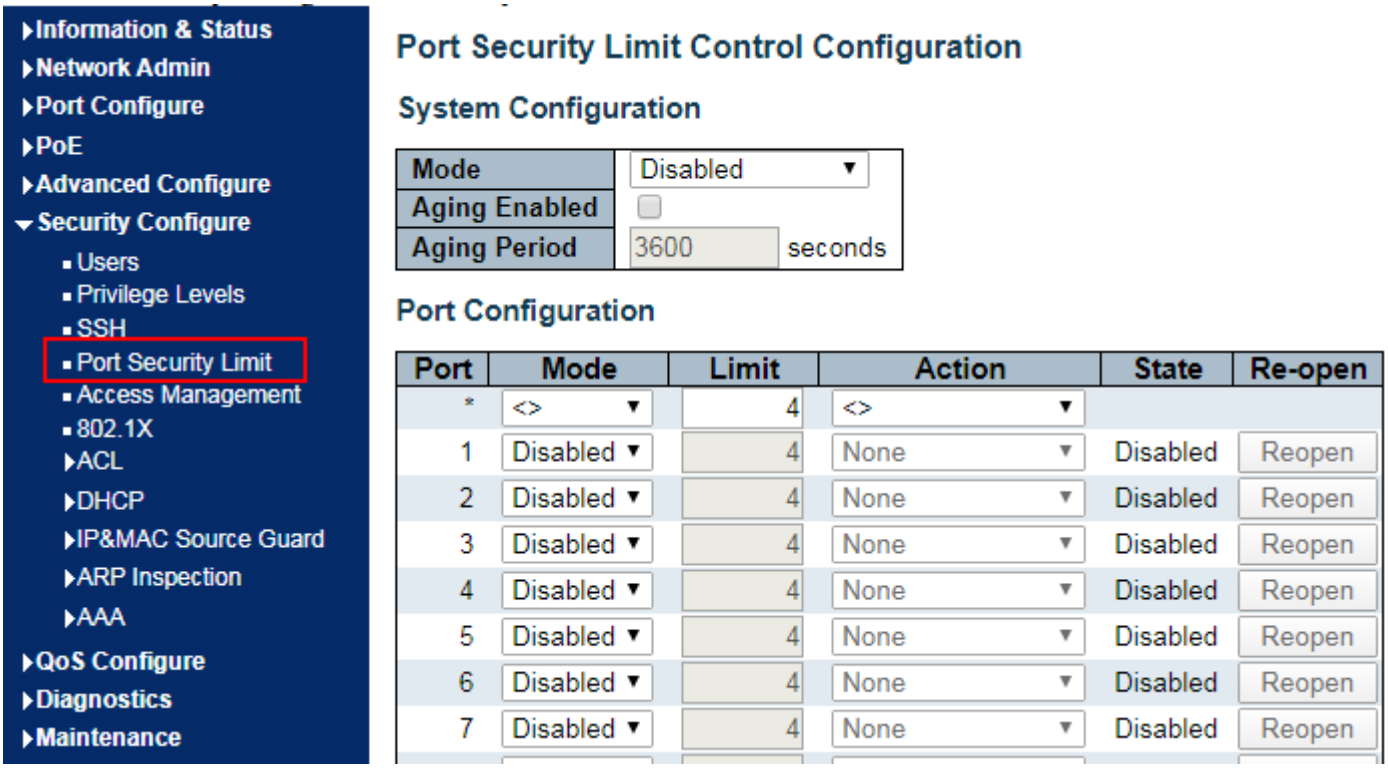
Выберите "**Security Configure**-**SSH**" для включения/выключения SSH:



7.4 Port Security Limit

Коммутатор поддерживает функцию Port Security и возможно задать разрешенное количество MAC-адресов на порту.

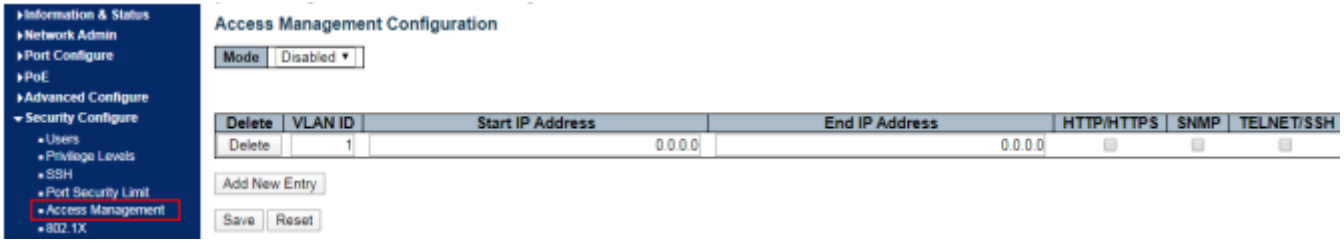
Выберите “**Security Configure**-**Port Security Limit**”:



7.5 Access Management

Веб-служба Access Management поможет вам получить безопасный доступ к ресурсам коммутатора. Коммутатор поддерживает разные уровни управления доступом.

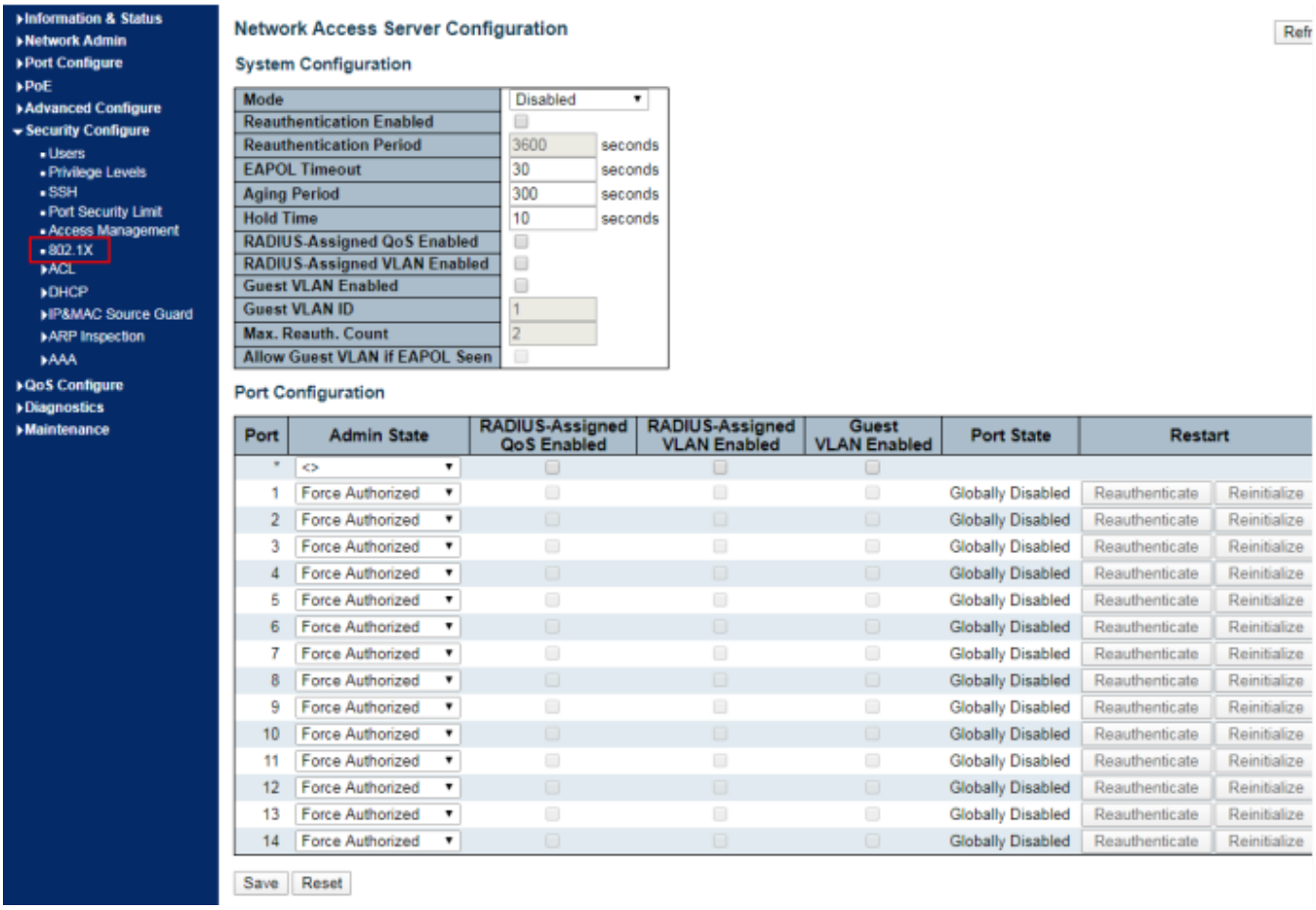
Выберите “**Security Configure-Access Management**”:



7.6 802.1X

802.1X — это протокол управления доступом и аутентификации на основе клиент-серверной технологии, который предотвращает доступ неавторизованных пользователей/устройств от доступа к LAN/WLAN через порт доступа. 802.1X проверяет подлинность пользователей/устройств, подключенных к порту перед получением услуг, предоставляемых коммутатором или локальной сетью.

Выберите “**Security Configure-802.1X**”:



Параметр	Описание
System Configuration	Выберите из: “Mode, Reauthentication Enabled, Reauthentication Period, 3,600 seconds, EAPOL Timeout, 30 seconds, Aging Period, 300 seconds, Hold Time, 10 seconds, RADIUS-Assigned QoS Enabled, RADIUS-Assigned VLAN Enabled, Guest VLAN Enabled, Guest VLAN ID 1, Max. Reauth Count 2, Allow Guest VLAN if EAPoL Seen”
Port Configuration	Выберите из: “Port, Admin State, RADIUS-Assigned QoS Enabled, RADIUS, Assigned VLAN Enabled, Guest VLAN Enabled, Port State, Restart”

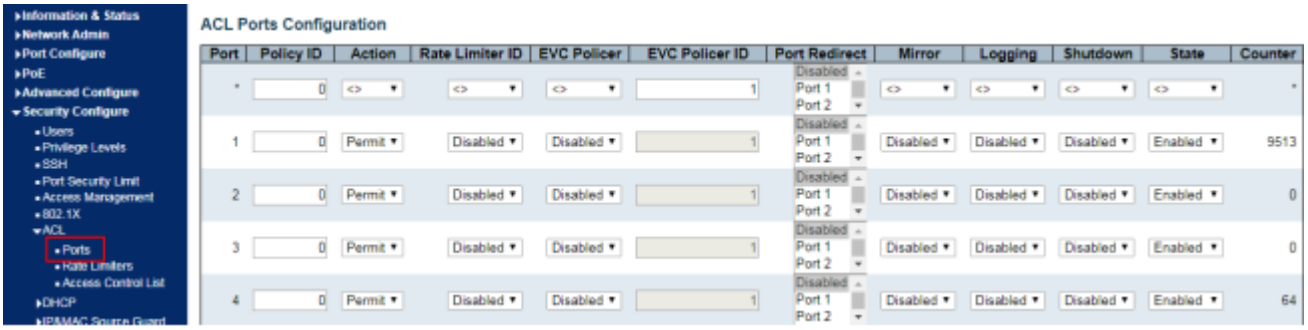
Нажмите “**Save**” для сохранения.

7.7 ACL

Список управления доступом (ACL) — это список инструкций для интерфейсов коммутатора, который используется для управления входом и выходом пакетов. Он применяется ко всем маршрутизируемым протоколам, таким как IP, IPX и AppleTalk. Связь между информационными точками и внутренними и внешними сетями - важнейшее требование бизнеса, предъявляемое к корпоративным сетям. корпоративных сетей. Для обеспечения безопасности Интранета права доступа можно контролировать путем разработки политик безопасности, гарантирующих, что неавторизованные пользователи могут использовать только определенные сетевые ресурсы. Вкратце, фильтрация потока ACL — это сетевая технология управления доступом. ACL настраивается для ограничения сетевого потока и авторизованных устройств, переадресации пакетов определенного порта и т. д. Например, внешняя публичная сеть находится за пределами досягаемости устройств в локальной сети, или доступна только служба FTP. ACL может быть настраиваться либо на маршрутизаторах, либо в программном обеспечении с функциями ACL. ACL, основанная на безопасности аппаратного уровня устройства, является важной технологией для обеспечения безопасности системы в IoT. Контролируя доступ к коммуникации между программными устройствами и задавая правила доступа, ACL отделяет нелегитимные устройства от нарушения безопасности системы и получения данных.

7.7.1 ACL Ports

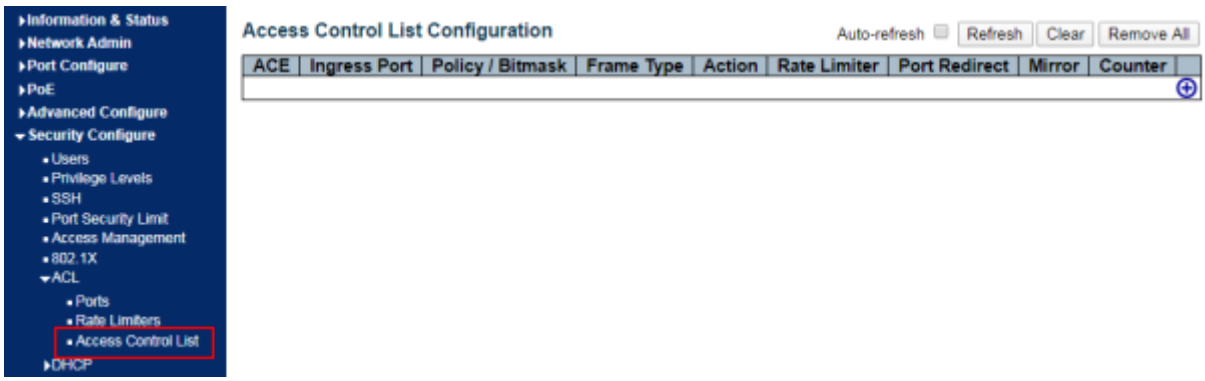
Выберите “**Security Configure**-**ACL**-**Ports**” для настройки ACL на портах:

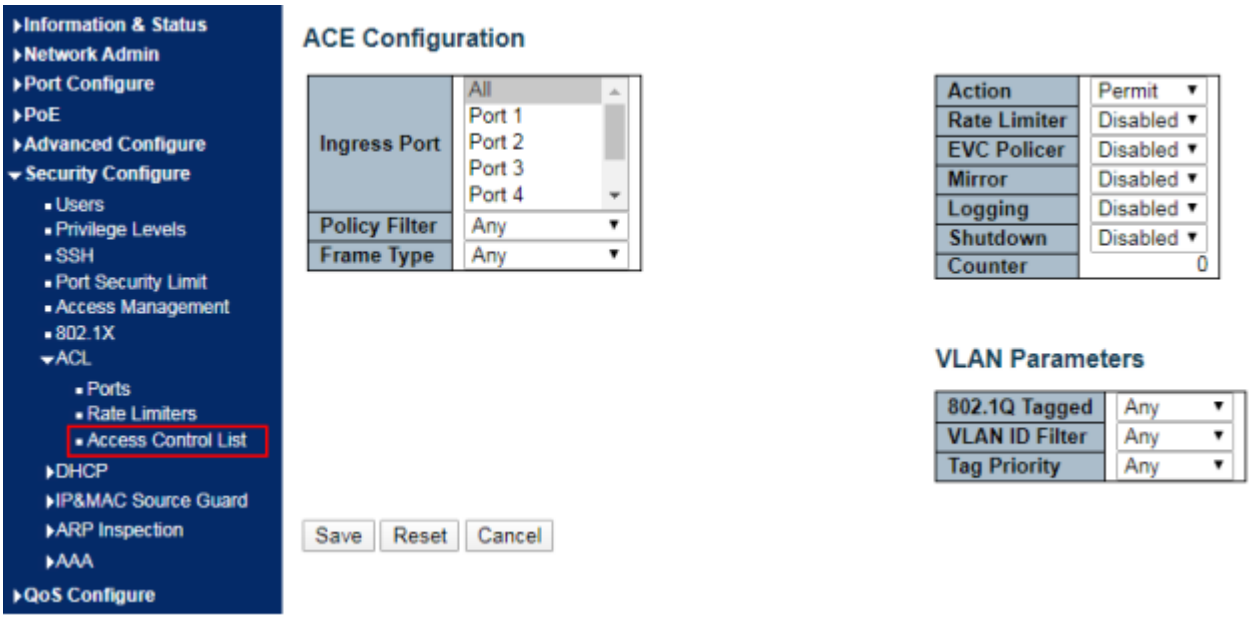


Параметр	Описание
Action	Разрешить: этот конкретный порт позволяет передавать данные. Запретить: этот конкретный порт запрещает прохождение данных
Rate Limiter ID	Фиксированный идентификатор ограничителя скорости порта. Для получения дополнительных сведений перейдите в раздел «Конфигурация ограничителя скорости»
Port Redirect	Выберите, на какой порт будет перенаправляться фрейм. Допустимые значения: Disabled или определенный номер порта, и его нельзя установить, если действие разрешено. Значение по умолчанию - «Отключено».
Mirror	Укажите операцию зеркалирования этого порта. Допустимые значения: Включено: кадры, полученные через порт, зеркалируются. Отключено: кадры, полученные через порт, не зеркалируются. Значение по умолчанию - «Отключено»
Logging	Ведение журнала включено или отключено
Shutdown	Завершение работы. Укажите операцию отключения порта для этого порта. Допустимые значения: Включено: если через порт получен кадр, порт будет отключен. Отключено: отключение порта отключено. Значение по умолчанию - «Отключено». Примечание. Функция выключения работает только при длине пакета менее 1518 (без тегов VLAN)
State	Укажите состояние порта для этого порта. Допустимые значения: Включено: повторное открытие портов путем изменения изменчивой конфигурации порта пользовательского модуля ACL. Отключено: закрытие портов путем изменения нестабильной конфигурации порта пользовательского модуля ACL. Значение по умолчанию - «Включено».
Counter	Подсчитывает количество кадров, соответствующих этому правилу

7.7.3 Access Control List

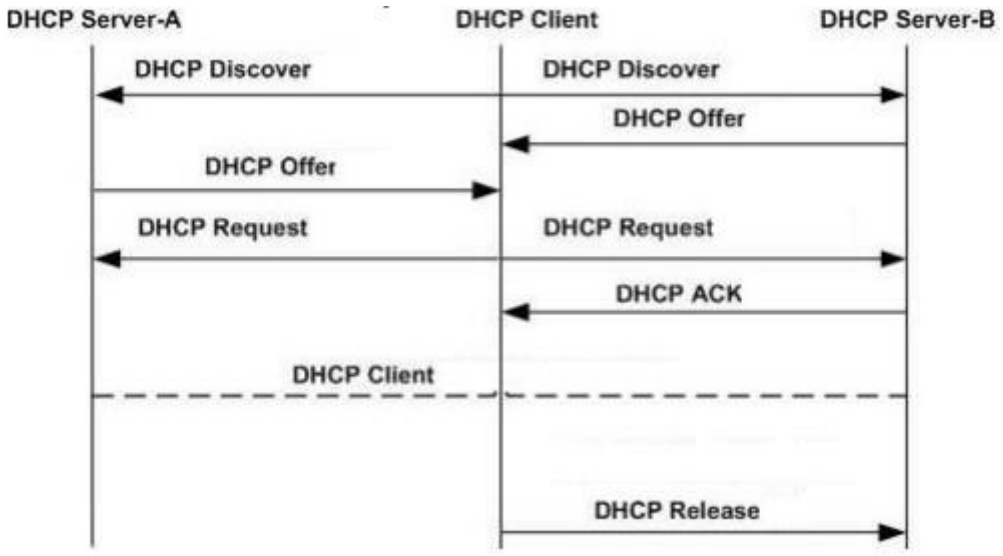
Выберите “**Security Configure**-**ACL**-**Access Control List**” и нажмите “+” для добавления правил





7.8 DHCP Snooping

В качестве протокола передачи данных DHCP использует UDP. Хост посылает запрос на 68-й порт DHCP-сервера, который отвечает на порт 67 хоста. Интерактивный процесс выглядит следующим образом:



1. DHCP-клиент передает сообщение DHCP Discover.

2. После получения сообщения все DHCP-серверы ответят DHCP-клиенту сообщением DHCP Offer. DHCP-сервер отправит клиенту DHCP поле "Ваш (клиентский) IP-адрес" в качестве IP-адреса в сообщении и поместит свой собственный IP-адрес в поле "Option" для различения. DHCP-сервер запишет назначенный IP-адрес после отправки сообщения.

3. Вообще говоря, DHCP-клиент может обработать только первое полученное сообщение DHCP Offer. Он передаст сообщение DHCP Request и добавит IP-адрес выбранного DHCP-сервера и требуемый IP-адрес в поле опции.

4. После получения сообщения DHCP Request сервер DHCP сравнивает IP-адреса со своим собственным адресом. DHCP-сервер только очистит соответствующие записи о выделении IP-адресов, если они отличаются; или ответит DHCP-клиенту сообщением DHCP-клиенту сообщением DHCP ACK и добавит срок аренды IP-адреса в поле опции.

5. DHCP-клиент проверит доступность IP-адреса, назначенного DHCP-сервером, в сообщении DHCP ACK8 сообщении. Клиент DHCP будет владеть IP-адресом и автоматически продлит срок аренды, если адрес действителен, или отправит сообщение DHCP Decline. отправит сообщение DHCP Decline, чтобы сообщить DHCP Server об отключении этого IP-адреса и подаче заявки на новый.

6. Клиент DHCP может освободить полученный IP-адрес, отправив сообщение DHCP Release в любое время, и DHCP-сервер восстановит и перераспределит соответствующий IP-адрес.

Принцип DHCP Snooping

Просматривая интерактивные сообщения DHCP между клиентом и сервером, функция DHCP Snooping отслеживает поведение пользователей и фильтрует сообщения DHCP. Ниже приведены толкования и функции DHCP Snooping:

1. DHCP Snooping Trust Port: Учитывая, что DHCP получает интерактивные сообщения IP путем широковещательной рассылки, существуют нелегальные серверы которые влияют на пользователей, чтобы получить нормальный IP, а некоторые из них даже обманывают пользователей и крадут информацию. В результате DHCP

Snooping классифицирует порты как доверительные и не доверенные. Устройства пересылают только сообщения DHCP Reply полученные с доверительных портов, и отклоняют сообщения с не доверенных портов, чтобы установить, что легальные порты, связанные с DHCP серверами в качестве доверительных портов, а другие - в качестве не доверенных, блокируя тем самым нелегальные серверы.

2. База данных привязки DHCP Snooping: Установка IP-адресов в частном порядке часто встречается в сети DHCP, что не только увеличивает сложность обслуживания сети, но и приводит к тому, что легальные пользователи не могут получить доступ к сети из-за конфликтов назначения адресов.
Путем прослушивания интерактивных сообщений между клиентом и сервером, IP, MAC, VID, PORT, аренда и другая информация, полученная пользователями, записывается в пользовательскую запись и формирует базу данных DHCP Snooping. При использовании функции проверки ARP, доступ пользователей будет контролироваться.
DHCP Snooping проверяет достоверность сообщений, проходящих через устройства, отбрасывает нелегальные, записывает информацию о пользователях и создает базу данных привязок для других функциональных запросов.

Вот некоторые типы нелегальных сообщений:

1. Сообщения DHCP Reply, полученные не доверенным портом, включая DHCP ACK, DHCP NACK, DHCP OFFER и т. д.
2. Сообщения DHCP Reply, полученные не доверенным портом с информацией об управлении сетью [giaddr].
3. Во время проверки MAC-адреса значения полей DHCP Client в сообщениях Source MAC и DHCP соответственно представляют собой разные пакеты.
4. При наличии информации о пользователе, сохраненной в базе данных привязки DHCP Snooping, сообщение DHCP Release имеет несоответствующую информацию о порте с информацией о порте, сохраненной в базе данных устройствами.

Параметры безопасности DHCP-Snooping

В сетевой среде DHCP администраторы часто сталкиваются с тем, что пользователи без разрешения изменяют и используют статические IP-адреса, а не динамические. Поэтому некоторые пользователи, использующие динамические IP-адреса, не могут получить доступ к сети что усложняет работу сетевых приложений и повышает сложность управления для администраторов.

Динамическое связывание DHCP — это безопасный процесс, в котором устройство получает информацию, записывая IP-адрес легального пользователя вовремя DHCP Snooping. Существует три типа управления. Первый - привязка адреса легального пользователя с помощью IP Source Guard. Второй - использование программного обеспечения DAI (Dynamic ARP Inspection) для проверки достоверности пользователя путем контролируя ARP. И последнее - привязка ARP-сообщения легального пользователя с помощью ARP Check.

Примечание: при использовании IP Source Guard для привязки адреса, количество пользователей DHCP, которое может поддерживать коммутатор, ограничено аппаратными записями.

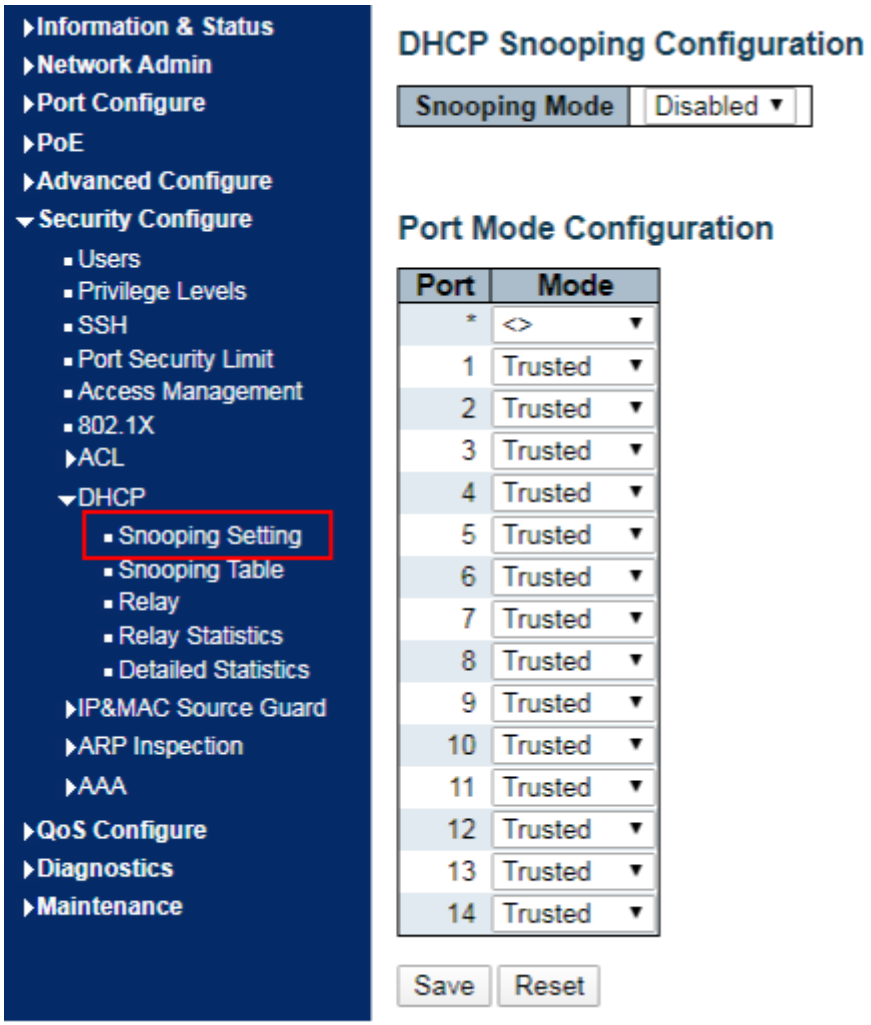
Легальные пользователи могут не добавлять аппаратные записи и не использовать сеть должным образом из-за слишком большого количества пользователей. Все ARP пересылаются и обрабатываются центральным процессором при использовании функции DAI, что серьезно влияет на производительность коммутатора.

Взаимосвязь привязки адресов между DHCP Snooping и IP Source Guard.
IP Source Guard поддерживает базу данных адресов IP-источников, устанавливая информацию о пользователях [IP, MAC] в базе данных на записи аппаратной фильтрации и ограничивая доступ пользователей к сети. Дополнительную информацию см. в разделе IP&MAC Source Guard.

DHCP Snooping предотвращает установку пользователями частных IP-адресов, отслеживая процесс DHCP, поддерживая базу данных пользовательских IP-адресов и отправляя данные в базу данных пользователей.
IP-базу данных и передавая данные в IP Source Guard для фильтрации, чтобы гарантировать, что только пользователи, получившие IP через DHCP, имеют доступ к сети.
Кроме того, пользователи, привязанные к DHCP, будут проверяться для повышения безопасности и предотвращения таких проблем, как ARP-спуфинг поскольку DHCP-привязка фильтрует только IP-сообщения. Для получения дополнительной информации обратитесь к разделу Конфигурация проверки ARP.

7.8.1 DHCP Snooping

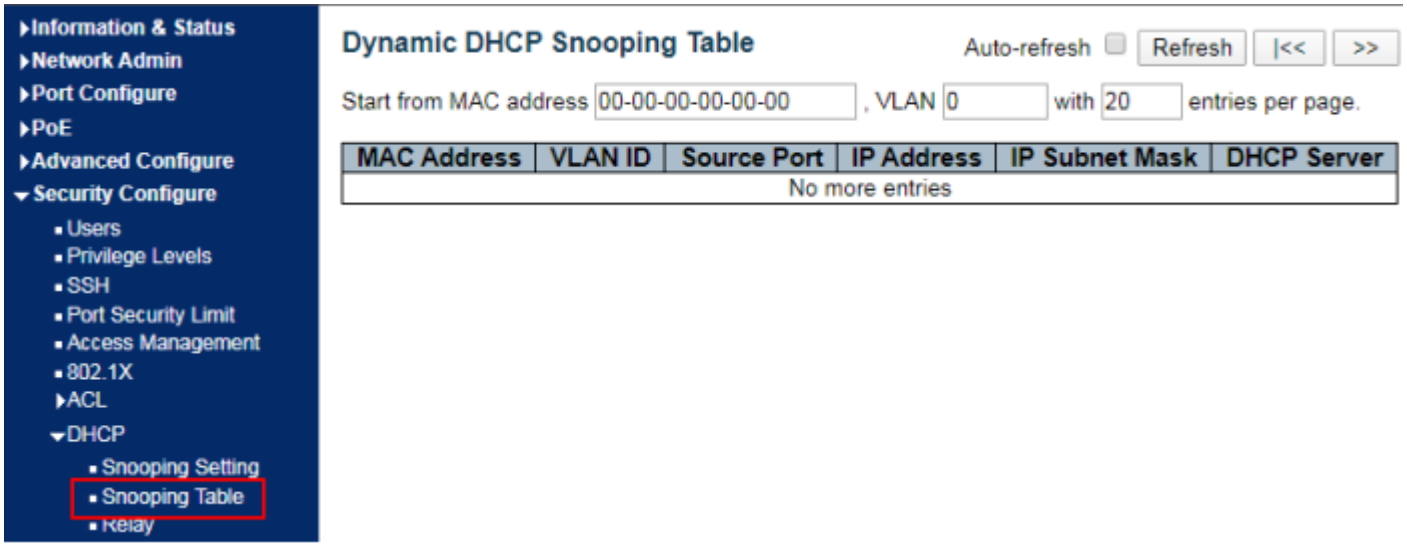
Для настройки выберите пункт “**Security Configure-DHCP-Snooping Setting**”



Параметр	Описание
DHCP Snooping Mode	Включение/отключение DHCP Snooping
Port Mode	Показывает режим работы DHCP Snooping на порту, варианты настройки: **Trusted**: Настраивает порт как доверенный источник DHCP-сообщений. **Untrusted**: Настройка порта как не доверенного источника DHCP-сообщений.

7.8.2 DHCP Snooping Table

Выберите “**Advanced Configure**-**DHCP**-**Snooping Table**” для проверки работы DHCP Snooping:

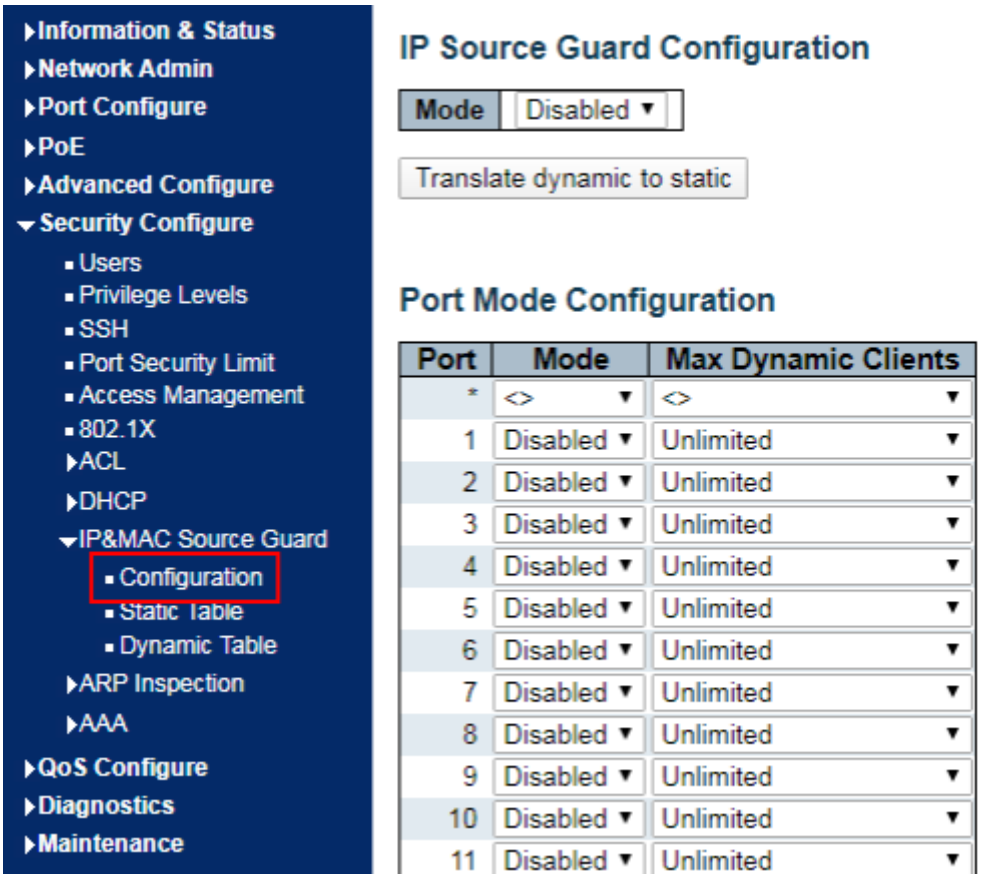


7.9 IP & MAC Source Guard

IP & MAC Source Guard поддерживает базу данных привязки Source IP & MAC для фильтрации сообщений хостов на основе Source IP & MAC на соответствующих портах, обеспечивая тем самым единственный доступ к сети.

7.9.1 Configuration

Выберите "**Security Configure-IP & MAC Source Guard-Configuration**" для настройки:



Параметр	Описание
Global Pattern	Включение/выключение IP & MAC Source Guard основано на глобальной конфигурации
Port Mode	Включение/выключение IP & MAC Source Guard основано на конфигурации порта
Max Dynamic Clients	Выберите максимальное количество поддерживаемых клиентов: Unlimited/0/1/2

7.9.2 Static Table

Для настройки статического присвоения соответствия значений IP & MAC Guard для портов выберите “**Security Configure-IP & MAC Source Guard-Static Table**”:

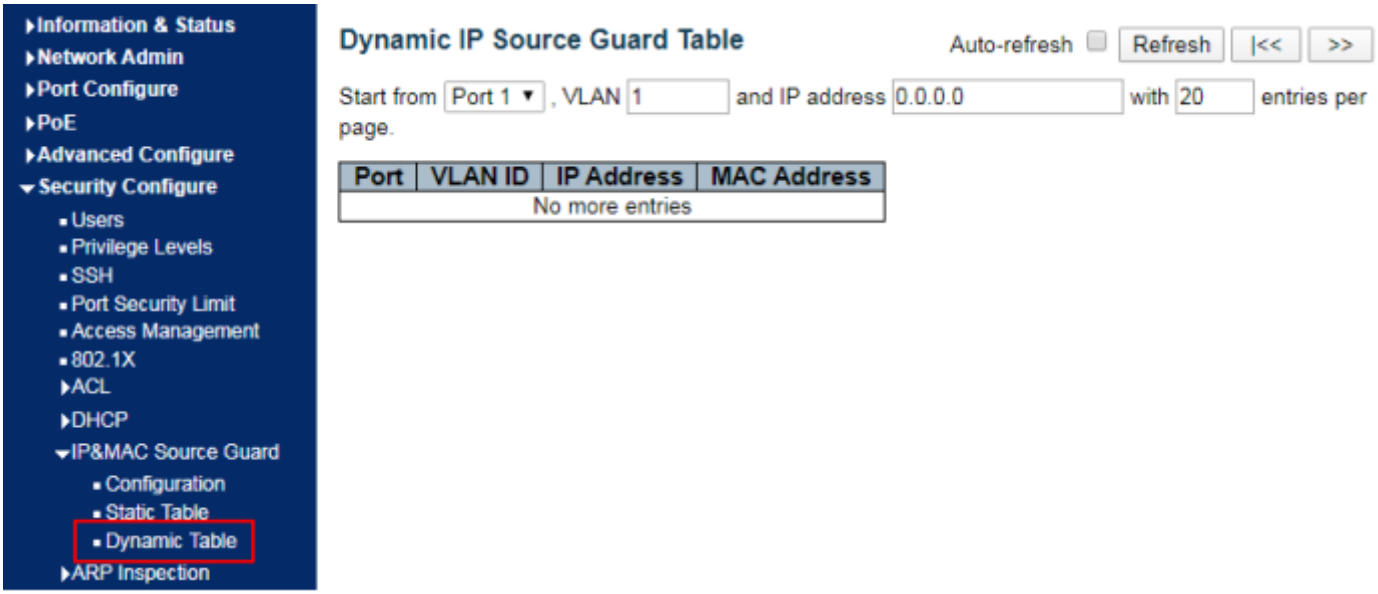
Выберите “**Add a New Entry**” для установки значений:

Параметр	Описание
Port	Введите значение Port ID
VLAN	Введите значение VLAN ID
IP Address	Введите значение IP Address
MAC Address	Введите значение MAC Address

Нажмите “**Save**” для сохранения параметров.

7.9.3 Dynamic Table

Для отображения информации о динамическом присвоении IP & MAC Guard выберите пункт “**Security Configure-IP & MAC Source Guard-Static Table**”:



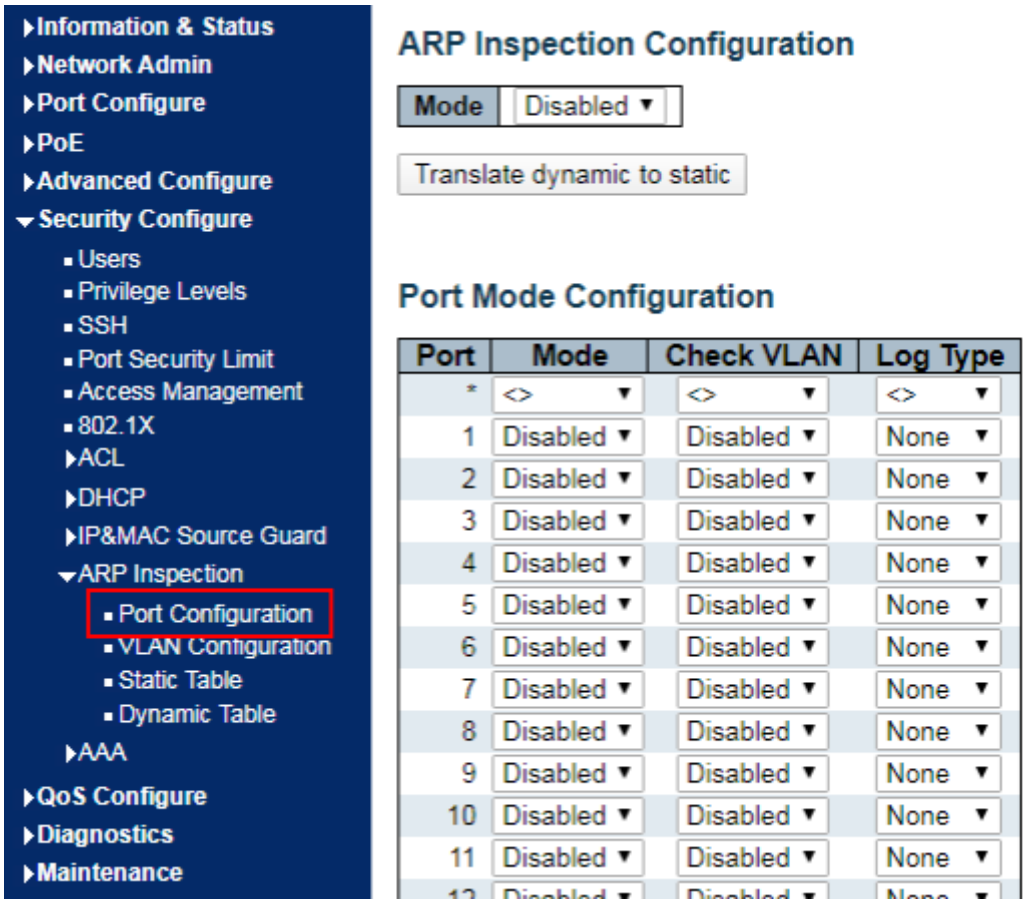
Параметр	Описание
Port	Отображение Port ID
VLAN	Отображает VLAN ID
IP Address	Отображает IP Address
MAC Address	Отображает MAC Address

7.10 ARP Inspection

IP & MAC Source Guard поддерживает базу данных привязки Source IP & MAC для фильтрации сообщений хостов на основе Source IP & MAC на соответствующих портах, обеспечивая тем самым единственный доступ к сети.
IP и MAC на соответствующих портах, обеспечивая тем самым единственный доступ к сети хостов, входящих в базу данных привязки Source IP & MAC.

7.10.1 Port Configuration

Для настройки работы протокола ARP на портах выберите “**Security Configure-ARP Inspection-Port Configuration**”:

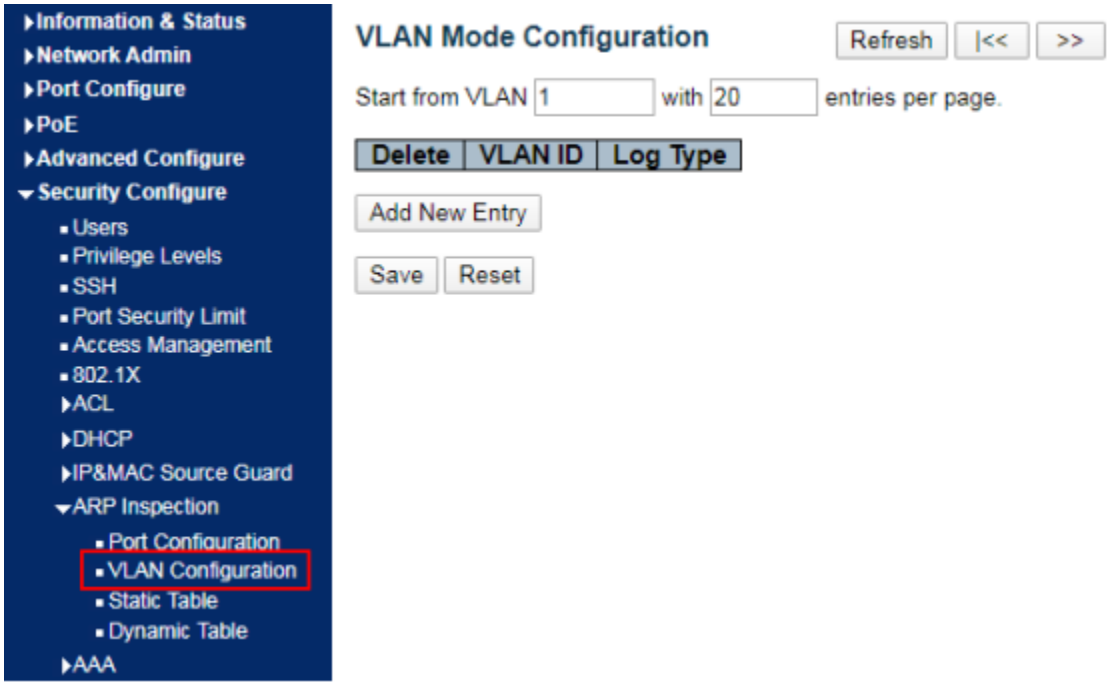


Параметр	Описание
Global Pattern	Включение/выключение ARP Inspection для глобальной конфигурации
Port Mode	Включение/выключение ARP Inspection для определенного порта
Check VLAN	Если вы хотите проверить конфигурацию VLAN, необходимо включить настройку "Check VLAN". По умолчанию параметр "Check VLAN" отключен. Когда настройка "Check VLAN" отключена, тип журнала ARP Inspection будет относиться к настройкам порта. А если настройка "Check VLAN" включена, тип журнала ARP Inspection будет относиться к настройке VLAN. Возможные настройки "Check VLAN" следующие: **Enabled**: Включить проверку VLAN. **Disabled**: Отключить проверку VLAN.
Log Type	Только при включенной проверке ARP в глобальный режиме и режим порта на и отключенной опции "Check VLAN" отключена, тип журнала ARP Inspection будет относиться к настройкам порта.

	Существует четыре типа ведения журналов, возможные типы: **None**: ничего не логируется **Deny**: логирует отклоненные значения **Permit**: логирует запрещённые значения **All**: логирует все значения

7.10.2 VLAN Configuration

Для настройки выберите “**Security Configure-ARP Inspection-VLAN Configuration**”:

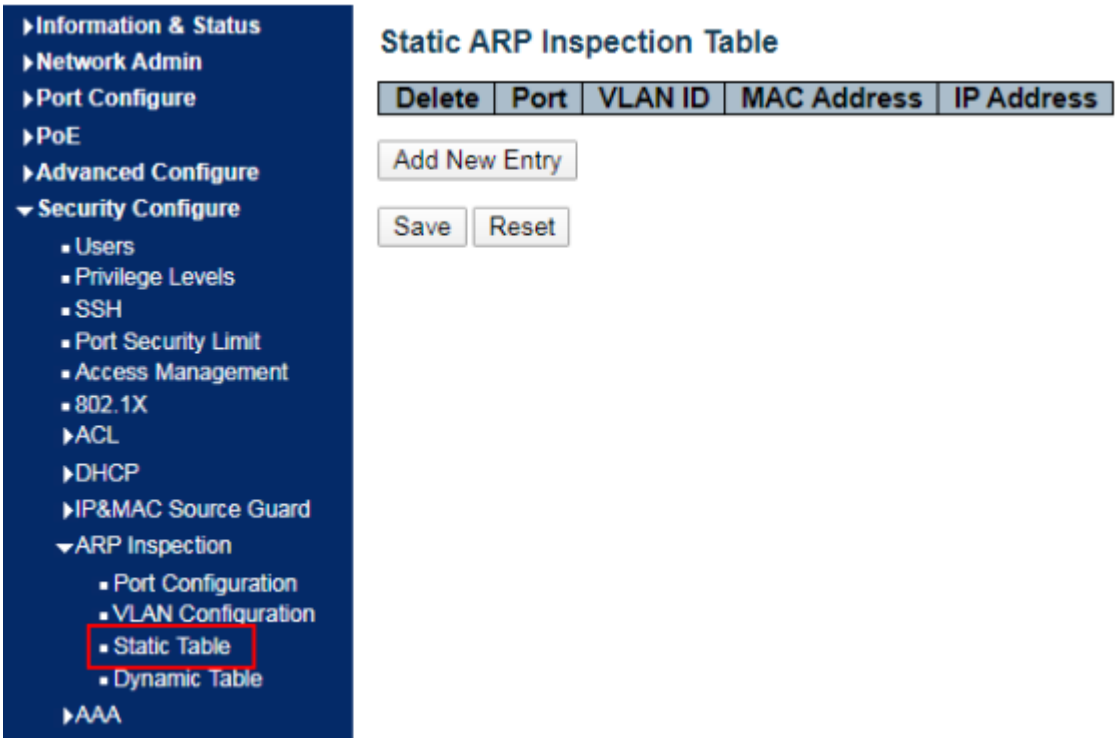


Параметр	Описание
VLAN ID	Конфигурация ARP Inspection основанного на VLAN
Log Type	Включение/отключение ARP Inspection основанного на портах
Check VLAN	Укажите, в каких VLAN ARP Inspection (проверка ARP). Сначала необходимо включить настройку порта на веб-странице конфигурации порта. Только если и глобальный режим, и режим по портам на данном порту включен, проверка ARP включена на данном порту. Во-вторых, вы можете указать, какая VLAN будет проверяться на веб-странице конфигурации режима VLAN. Тип логирования также может быть настроен для каждого VLAN. Возможными типами логирования являются: **None**: Логирование отключено **Deny**: Логирование запрещенных значений **Permit**: Логирование разрешенных значений **All**: Логирование всех значений

Для добавления новой конфигурации VLAN нажмите “**Add New Entry**”, для сохранения нажмите “**Save**”

7.10.3 Static Table

Для конфигурации **binding table** (таблицы соответствия) в **ARP Inspection** на портах выберите пункт “**Security Configure**-**ARP Inspection**-**Static Table**”:

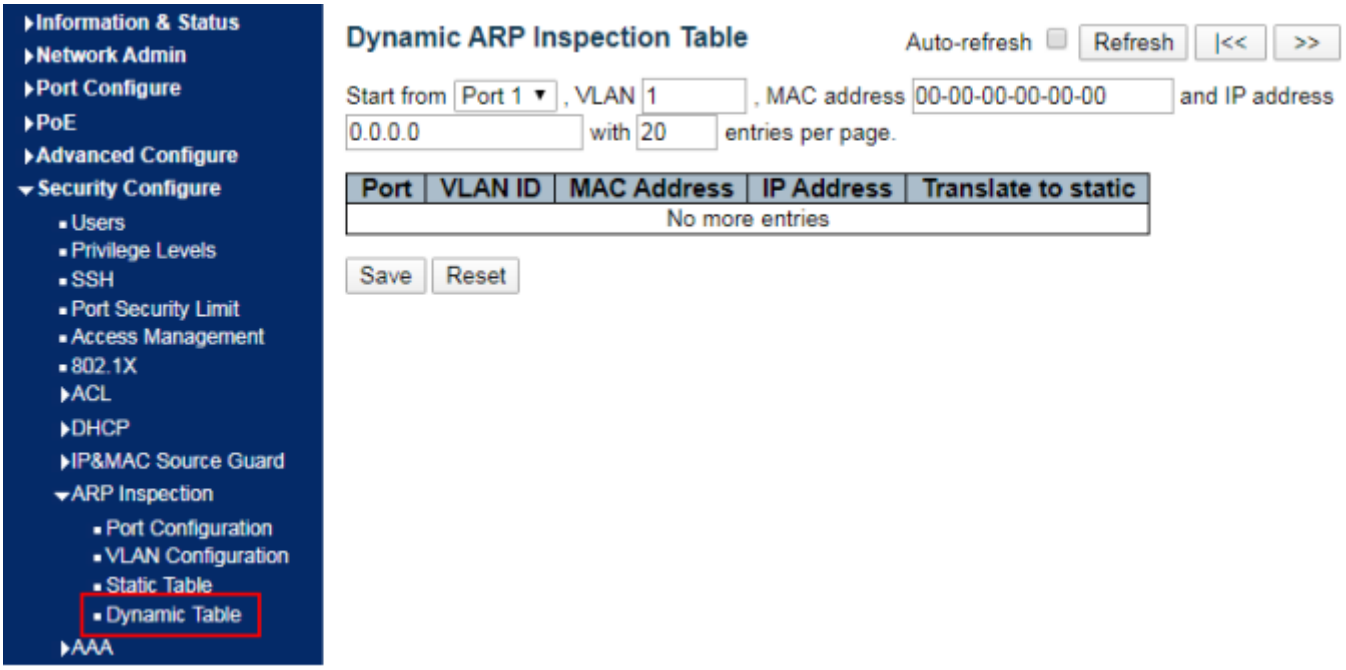


Параметр	Описание
Port	Задайте порт ID
VLAN	Задайте VLAN ID
IP Address	Задайте IP Address
MAC Address	Задайте MAC Address

Для введения информации выберите “**Add New Entry**”, для сохранения нажмите “**Save**”

7.10.4 Dynamic Table

Для просмотра динамической таблицы соответствия **IP & MAC Guard** выберите "**Security Configure-ARP Inspection-Dynamic Table**":



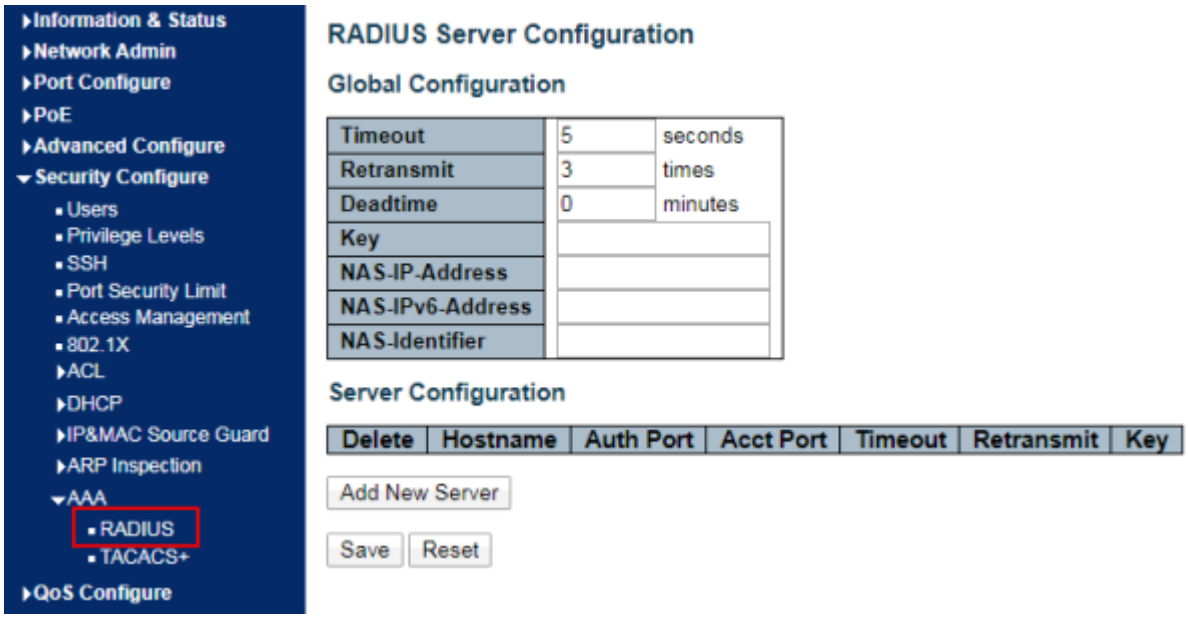
Параметр	Описание
Port	Отображение Port ID
VLAN	Отображение VLAN ID
IP Address	Отображение IP Address
MAC Address	Отображение MAC Address

7.11 AAA

AAA – это аббревиатура от Authentication, Authorization and Accounting. Это управление механизмами защиты доступа и управления коммутатором.

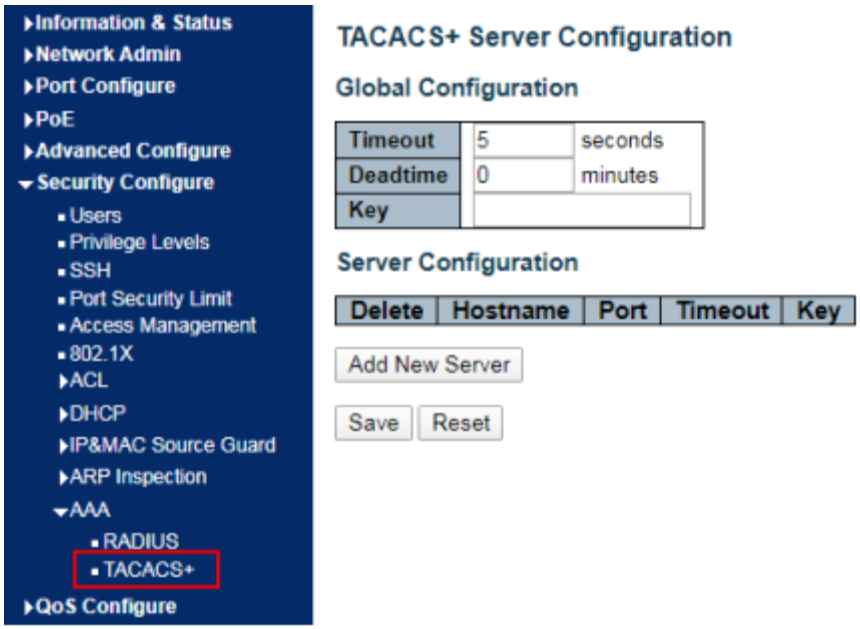
7.11.1 RADIUS

Для настройки функции RADIUS выберите “**Security Configure**-**AAA**-**RADIUS**”:



7.11.1 TACACS+

Для настройки функции TACACS+ выберите “**Security Configure**-**AAA**-**TACACS+**”:

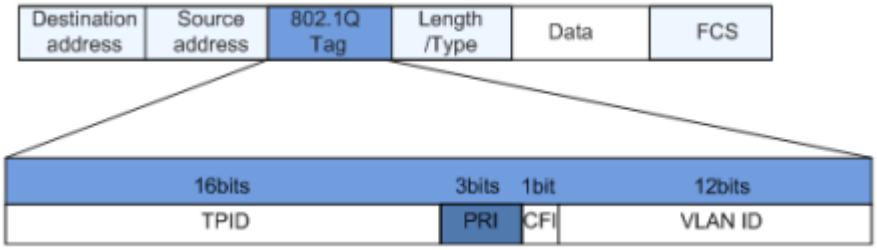


8. QoS

QoS (Quality of Service) - оценивает способность поставщиков услуг удовлетворять потребности клиентов и возможность отправки пакетов через Интернет. Диверсифицированные услуги могут оцениваться по различным аспектам. QoS обычно относится к оценке возможностей услуг, которые поддерживают основные требования, такие как пропускная способность, задержка, вариации задержки и уровень потери пакетов при доставке. Пропускная способность обозначает среднюю скорость потока за определенную единицу измерения - кбит/с. Задержка — это среднее время, необходимое для прохождения потока через сеть.
Для сетевого устройства ниже приведены общие уровни требований к задержке. Существует два уровня задержки, т. е. высокоприоритетный трафик может быть обслужен как можно быстрее благодаря методу планирования приоритетной очереди, а низкоприоритетный трафик получает обслуживание позже. Под изменением задержки понимается изменение времени прохождения трафика через сеть.
Коэффициент потери пакетов — это процент потерянного трафика во время передачи. Поскольку современные системы передачи данных очень надежны, информация часто теряется при перегрузке сети. Потеря пакетов из-за переполнения очереди является наиболее распространенной ситуацией.
Все сообщения в традиционной IP-сети обрабатываются одинаково. Каждое сетевое устройство обрабатывает сообщения по принципу FIFO и делает все возможное, чтобы отправить их по назначению, не гарантируя надежность, задержку передачи или другие характеристики.
Качество сетевых услуг постоянно улучшается, поскольку в быстро меняющейся IP-сети появляются новые приложения.
Например, VoIP, видео и другие сервисы, чувствительные к задержкам, установили более высокие стандарты на задержку передачи сообщений.
Передача сообщений за короткий промежуток времени стала общей тенденцией. Чтобы поддерживать услуги передачи голоса, видео и данных с различными требованиями, сеть должна определять типы трафика и предоставлять соответствующие услуги.
Способность различать типы трафика является предпосылкой для предоставления соответствующих услуг, поэтому традиционная услуга besteffort больше не отвечает потребностям приложений. Так появляется QoS. Он регулирует сетевой поток, чтобы избежать и справиться с перегрузкой сети и снизить уровень потери пакетов. При этом пользователи могут пользоваться выделенной полосой пропускания, а расстановка приоритетов может улучшить качество обслуживания, тем самым повышая пропускную способность сети.

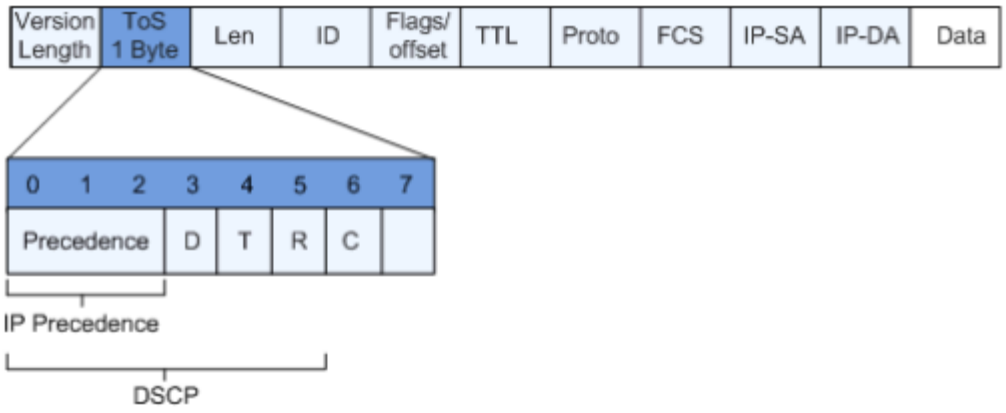
Приоритеты QoS зависят от типов сообщений. Например, сообщение VLAN использует 802.1p, также известный как поле CoS (Class of Service), а в IP-сообщениях - DSCP. Для поддержания приоритета эти поля должны быть сопоставлены на шлюзе соединенных с различными сетями, когда сообщения проходят через сеть. Приоритет 802.1p в заголовке кадра VLAN как правило, кадры VLAN взаимодействуют между устройствами второго уровня. Поле PRI (т. е. приоритет 802.1p), или поле CoS, в Поле PRI (т. е. приоритет 802.1p), или поле CoS, в заголовке кадра VLAN определяет требования к качеству обслуживания в соответствии с определениями, приведенными в стандарте IEEE 802.1Q.

Приоритет 802.1p в кадре VLAN



Заголовок 802.1Q содержит 3-битные поля PRI. Поле PRI определяет 8 CoS приоритетов в диапазоне от 7 до 0, от высокого до низкого.

Поле IP Precedence/DSCP
Согласно определению RFC791, домен ToS (Type of Service) в заголовке IP-сообщения состоит из 8 битов. Среди них 3-битное поле Precedence, как показано ниже, определяет приоритет IP-сообщения.



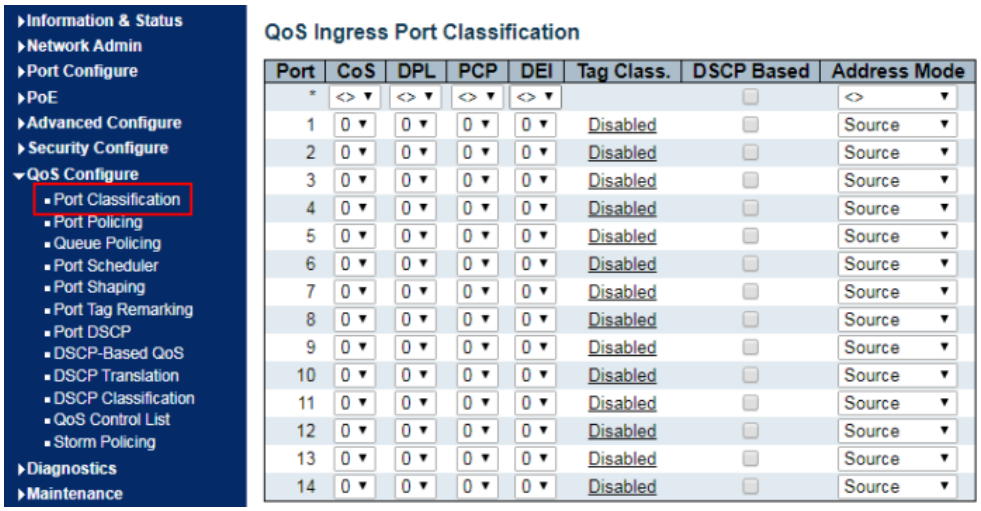
От 0 до 2 битов - это поля Precedence, представляющие 8 приоритетов передачи сообщений в диапазоне от 7 до 0 - от высокого до низкого, с уровнем 7 или 6 в качестве наивысшего приоритета, который обычно резервируется для маршрутизации или обновления управления сетью. Приложения пользовательского уровня имеют доступ только к уровням от 0 до 5.

Домен ToS, в дополнение к полям Precedence, также включает биты D, T и R:
D-бит представляет требование к задержке (0 для нормальной задержки и 1 для низкой задержки).
T-бит представляет пропускную способность (0 для нормальной пропускной способности и 1 для высокой пропускной способности).
R-бит представляет надежность (0 для нормальной надежности и 1 для высокой надежности).

Домен ToS резервирует 6 и 7 биты. RFC1349 переопределяет домен ToS, добавляя бит C для представления приоритета трафика. Затем группа IETF DiffServ переопределяет от 0 до 5 битов домена ToS в заголовке сообщения IPv4 как DSCP и переименовывает его в DS (Differentiated Service) байт, как показано на рисунке выше. Первые 6 бит (0-5 бит) поля DS обозначают DSCP (DS Code Point), а старшие 2 бита (6-7 бит) зарезервированы. Младшие 3 бита (0-2 бита) - это CSCP (Class Selector Code Point), причем одно и то же значение CSCP представляет DSCP одного и того же класса. Узлы DS выбирают соответствующие PHB (Per-Hop Behavior) в соответствии со значениями DSCP.

8.1 Port Classification

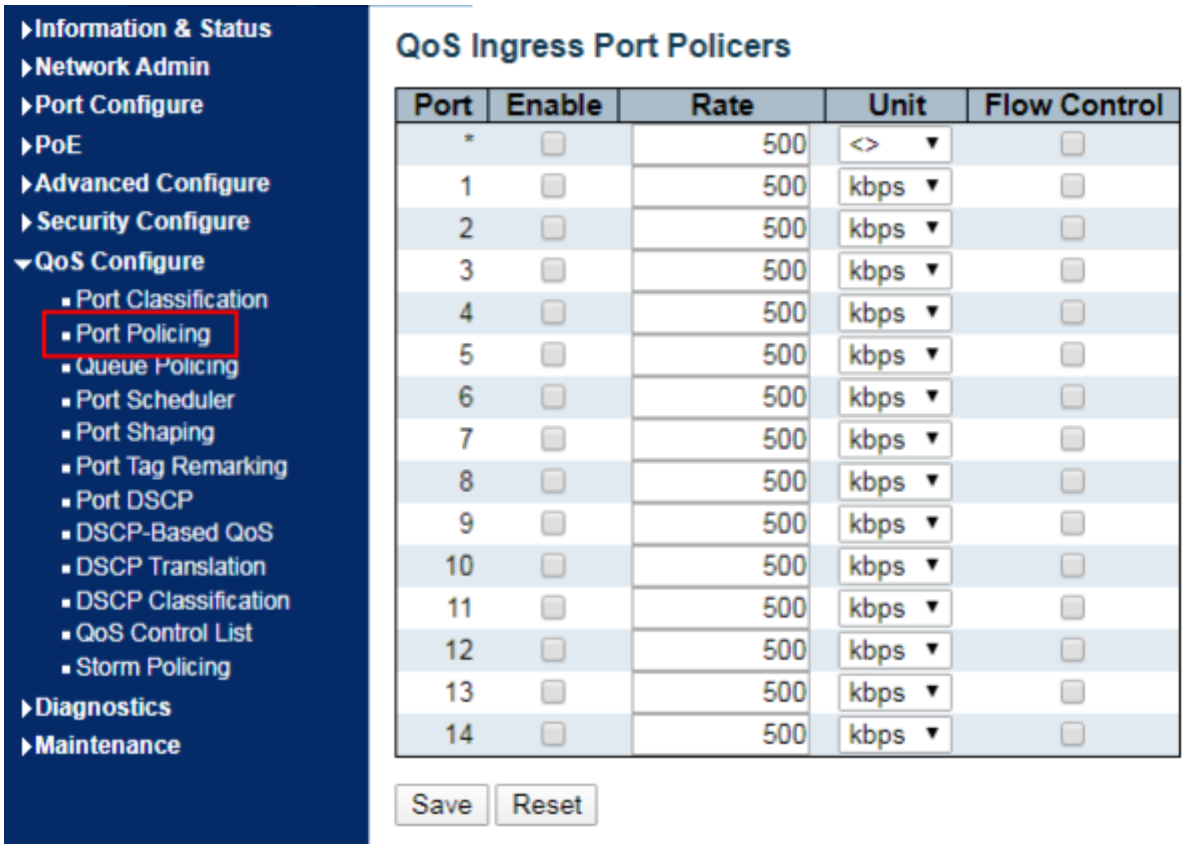
Коммутатор по умолчанию настраивает приоритет 802.1p и распределяет информацию, такую как DPL, PCP и DEI, по каждому порту. На сайте приоритет и действительный приоритет обозначаются как 0 (самый низкий) и 7 (самый высокий).
Для настройки выберите “**QoS Configure-Port Classification**”



Параметр	Описание
CoS	Управляет классом обслуживания по умолчанию. Все кадры классифицируются как CoS. Между CoS, очередью и приоритетом существует взаимно однозначное соответствие. CoS 0 (ноль) имеет самый низкий приоритет. Если порт поддерживает VLAN, кадр помечается тегами и классом тегов. Если параметр включен, то кадр классифицируется как CoS, который отображается из значений PCP и DEI в теге. В противном случае кадр классифицируется как CoS по умолчанию. **Примечание**: если CoS по умолчанию был динамически изменен, то фактический CoS по умолчанию показан в скобках после настроенного CoS по умолчанию.
DPL	Управляет значением «Отбросить уровень приоритета» по умолчанию. Все кадры классифицируются по уровню приоритета отбрасывания.
PCP	Управляет значением PCP по умолчанию. Все кадры классифицируются по значению PCP. Если порт поддерживает VLAN и фрейм помечен, тогда фрейм классифицируется по значению PCP в тэге. В противном случае кадр классифицируется по значению PCP по умолчанию.
DEI	Управляет значением DEI по умолчанию. Все кадры классифицируются по значению DEI. Если порт поддерживает VLAN и фрейм помечен, тогда фрейм классифицируется по значению DEI в тэге. В противном случае кадр классифицируется по значению DEI по умолчанию.
Tag Class	Показывает режим классификации для помеченных кадров на этом порту. **Disabled**: использовать CoS и DPL по умолчанию для помеченных кадров. **Enabled**: использовать сопоставленные версии PCP и DEI для кадров с тегами. Выберите чтобы настроить режим и/или отображение.
DSCP Based	Выберите, чтобы использовать классификацию входного порта QoS на основе DSCP
Address Mode	Режим IP/MAC-адреса, определяющий, должна ли классификация QCL основываться на адресах источника (SMAC/SIP) или назначения (DMAC/DIP) на этом порту. Допустимые значения: **Source**: включить сопоставление SMAC/SIP **Destination**: включить сопоставление DMAC/DIP

8.2 Port Policing

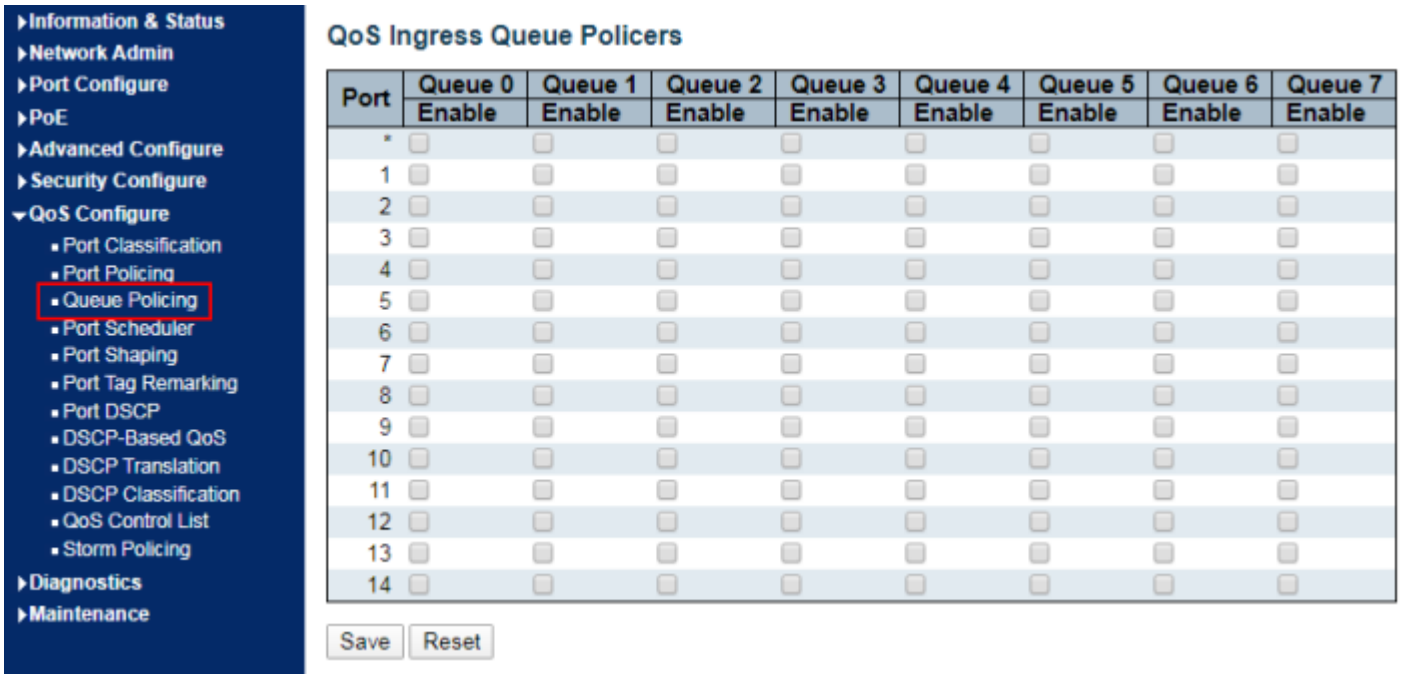
Для настройки ограничений на портах выберите “**QoS Configure-Port Policing**”:



Параметр	Описание
Enabled	Включите или отключите ограничитель очереди для этого порта коммутатора
Rate	Введите ограничение
Unit	Введите единицу измерения ограничения
Flow Control	Если контроль потока глобально включен и порт находится в режиме контроля потока, то вместо отбрасываемых кадров отправляются кадры паузы

8.3 Queue Policing

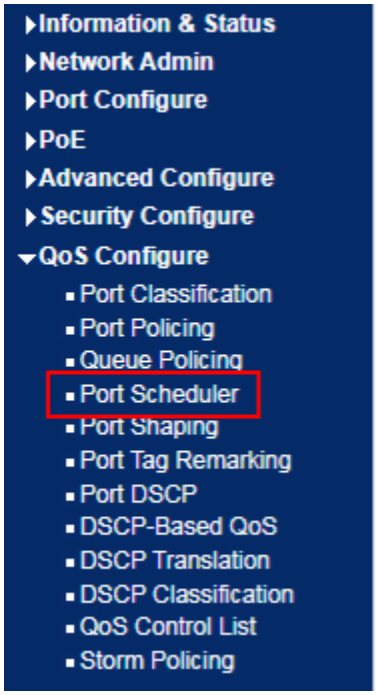
Для настройки очередей на портах выберите “**QoS Configure**-**Queue Policing**”:



Возможно задать приоритет очередей в диапазоне 0-7, нажать “**Save**” для сохранения изменений.

8.4 Port Scheduler

Для настройки расписания ограничений на портах выберите “**QoS Configure**-**Port Scheduler**” и щелкните по интересующими порту, например, “**1**”:



QoS Egress Port Schedulers

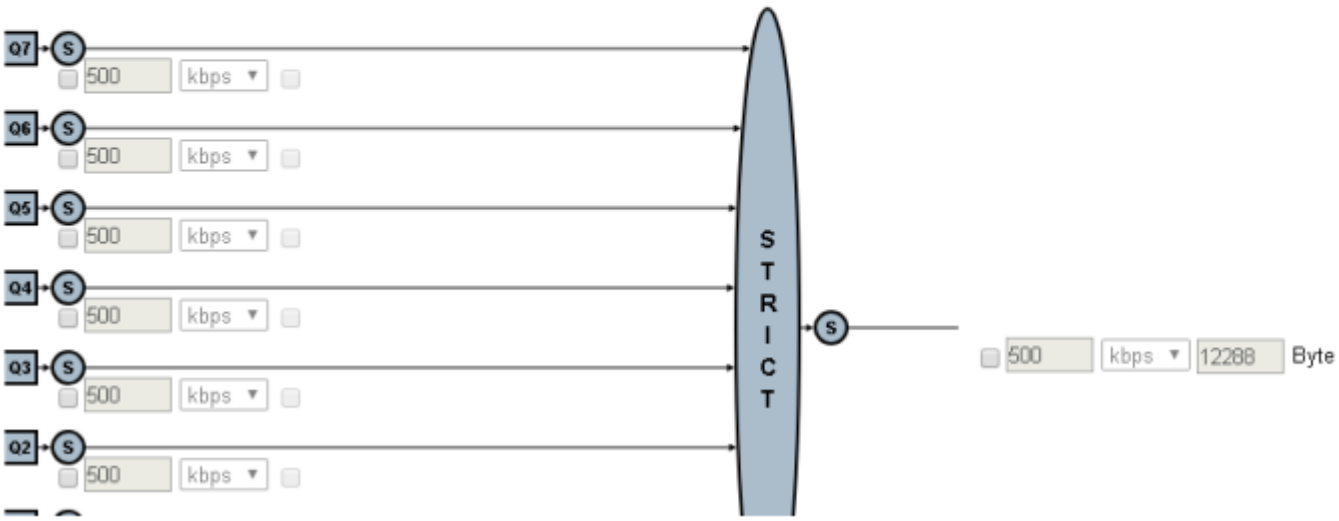
Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-
9	Strict Priority	-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

QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: Strict Priority

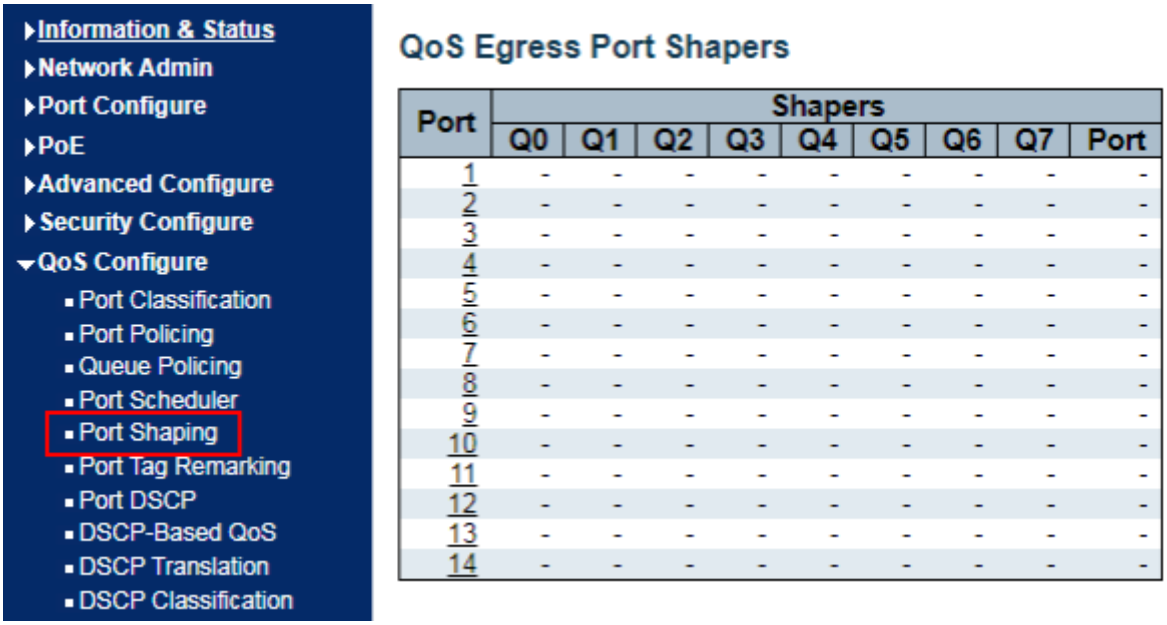
Queue Shaper			
Enable	Rate	Unit	Excess

Port Shaper				
Enable	Rate	Unit	Burst	Unit



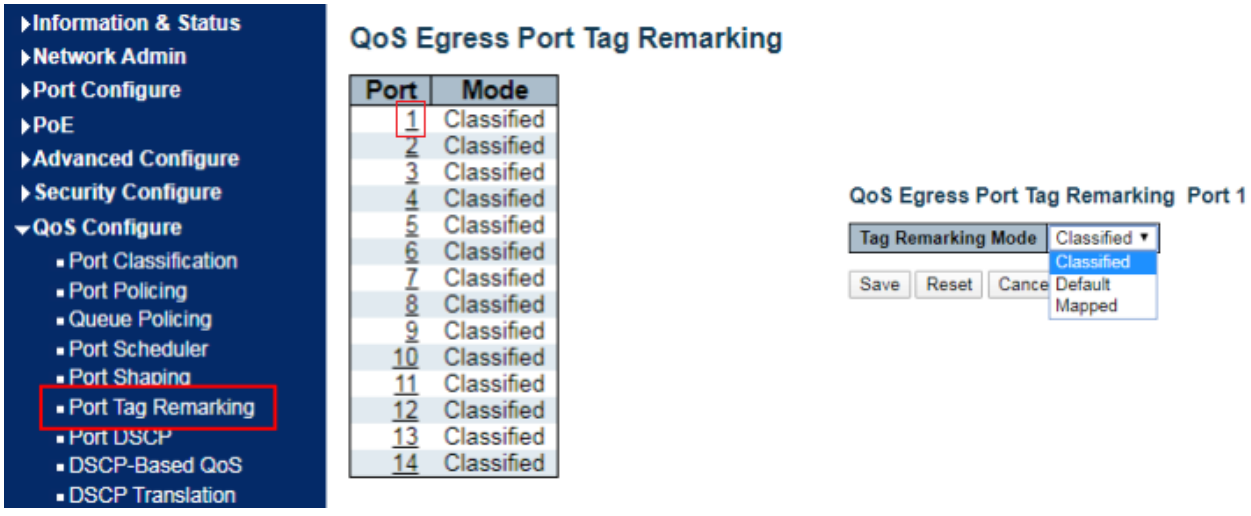
8.5 Port Shaping

Выберите **egress** порт для установки статического ограничения и использование WRR, для этого выберите пункт "**QoS Configure-Port Shaping**":



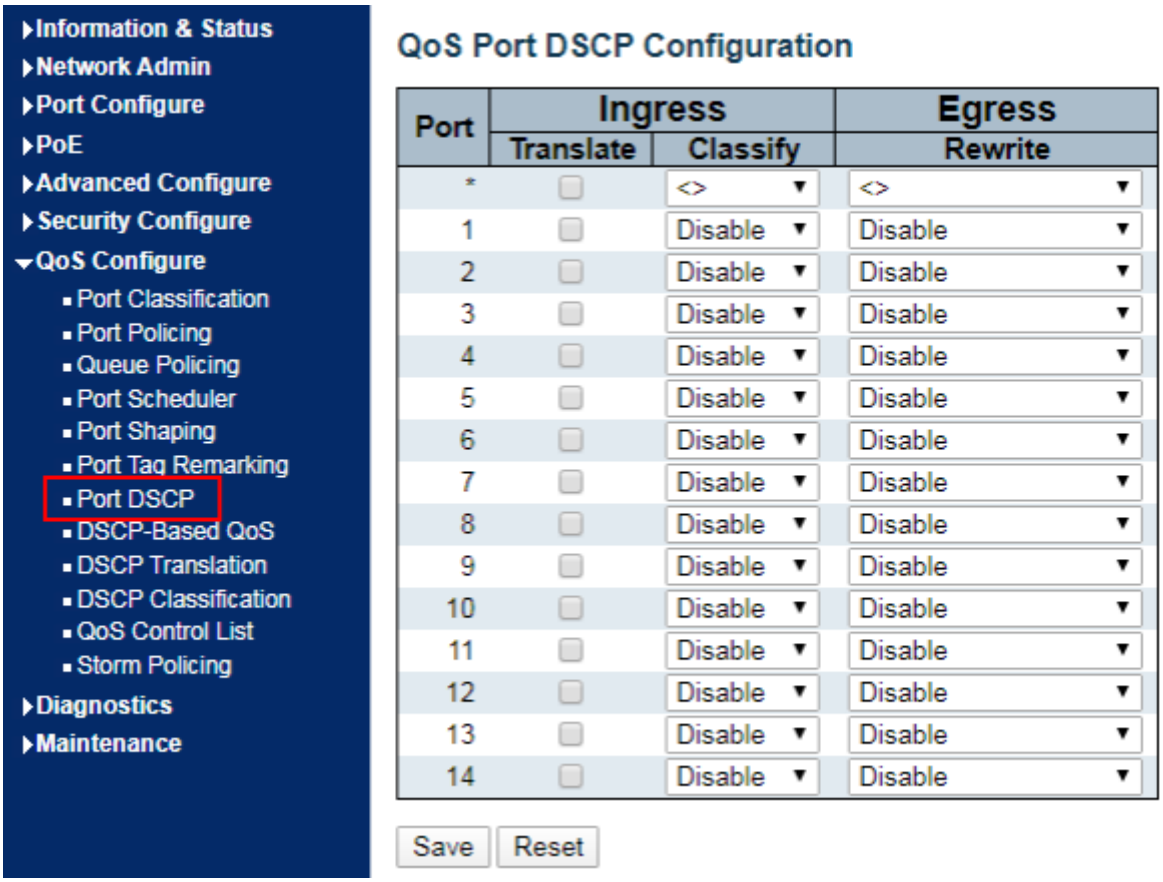
8.6 Port Tag Remarking

Для перемаркировки исходящего траффика выберите "**QoS Configure-Port Tag Remarking**" и порт, например, "**1**":



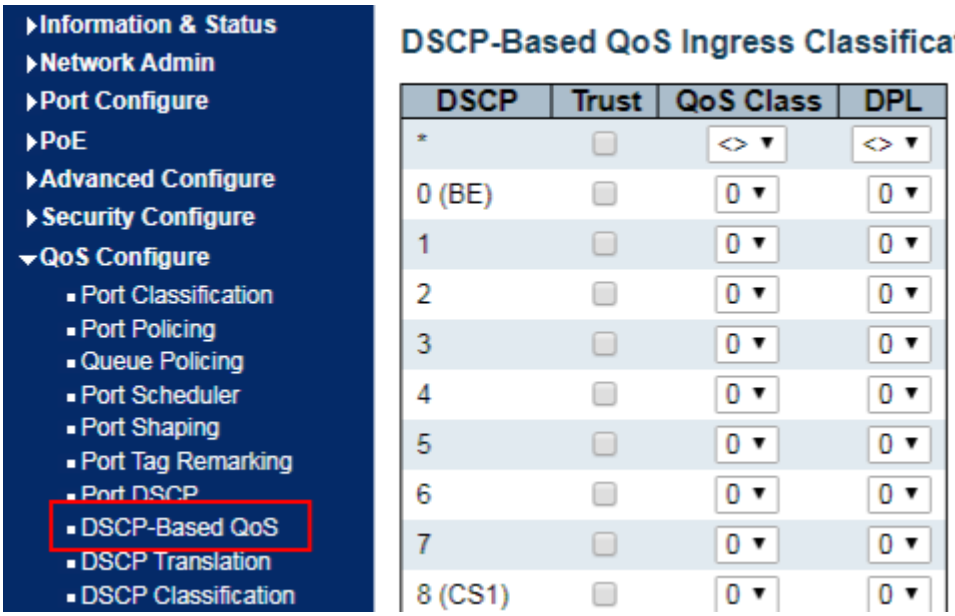
8.7 Port DSCP

Для настройки DSCP rewrite выберите “**QoS Configure-Port DSCP**”:



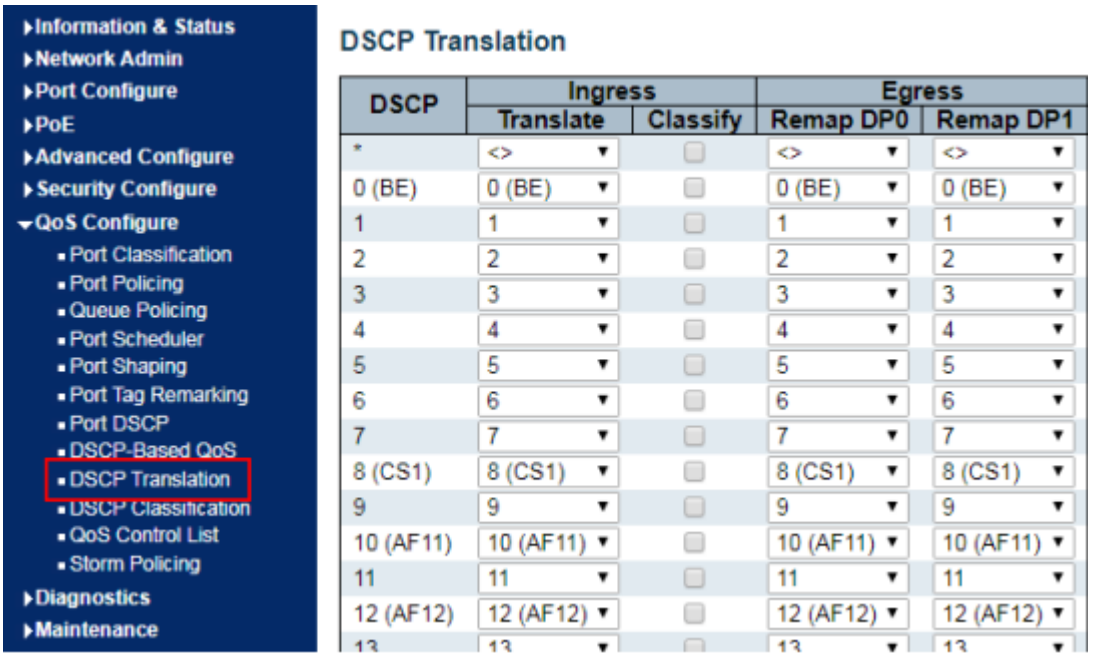
8.8 DSCP-Based QoS

Для настройки Trusted DSCP выберите "**QoS Configure**-**DSCP**-**Based QoS**":



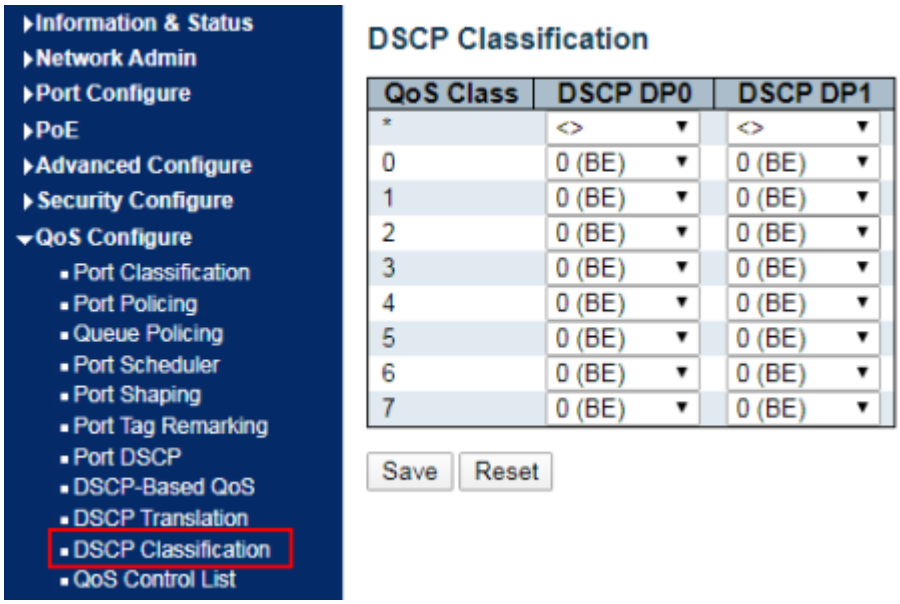
8.9 DSCP Translation

Для настройки трансляции DSCP выберите "**QoS Configure**-**DSCP Translation**":



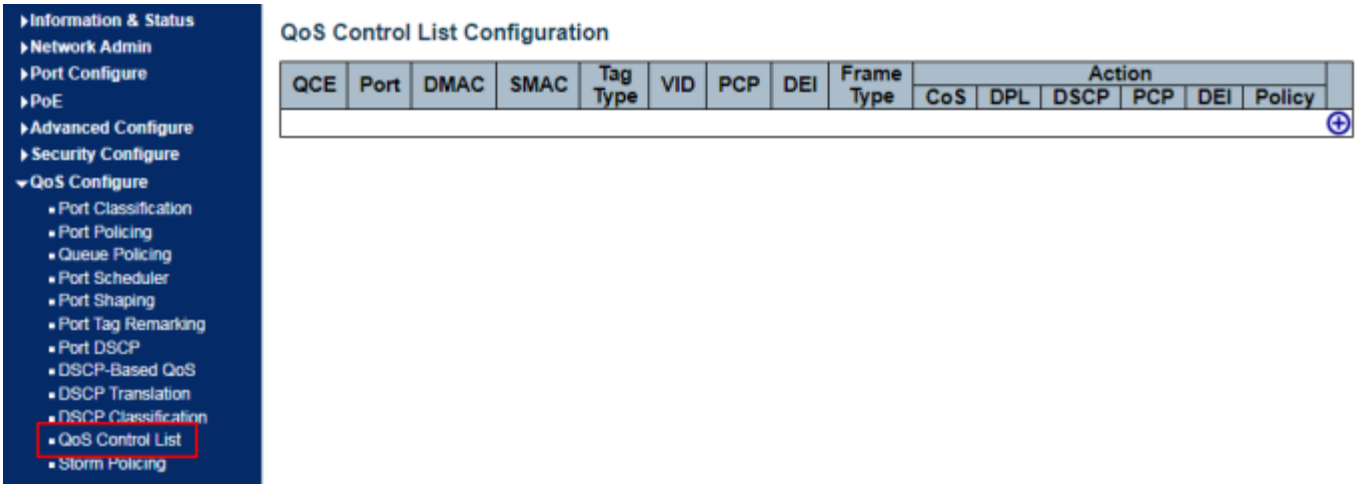
8.10 DSCP Classification

Для настройки классификации DSCP выберите “**QoS Configuration**-**DSCP Classification**”



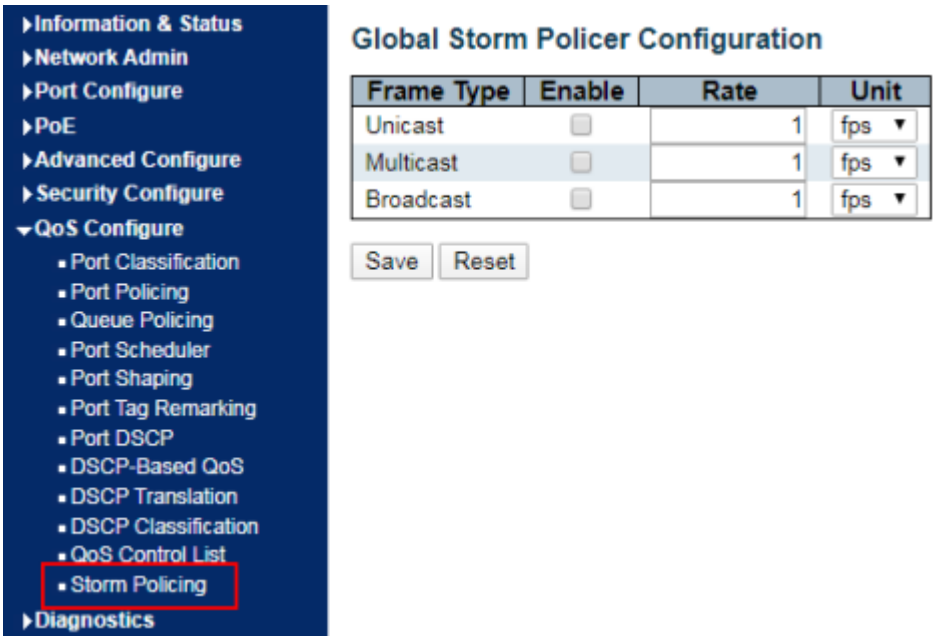
8.11 QoS Control List

Для настройки QoS ACL выберите “**QoS Configure**-**QoS Control List**”:



8.12 Storm Policing

Для настройки политик защиты от шторма выберите “**QoS Configure**-**Storm Policing**”:

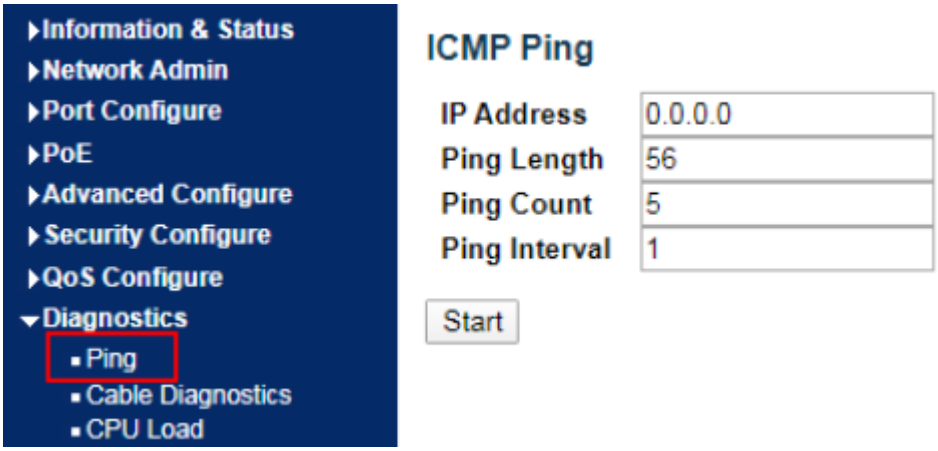


Параметр	Описание
Frame Type	Коммутатор поддерживает типы фреймов: Unknown Unicast, Unknown Multicast, Broadcast
Enable	Включение/отключение политики защиты от шторма
Rate	Ограничение в пакетах в секунду (pps): 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, 1,024K

9. Diagnostics

9.1 Ping

Для проверки ответа на пакеты ICMP Echo выберите “**Diagnostics**-**Ping**”:

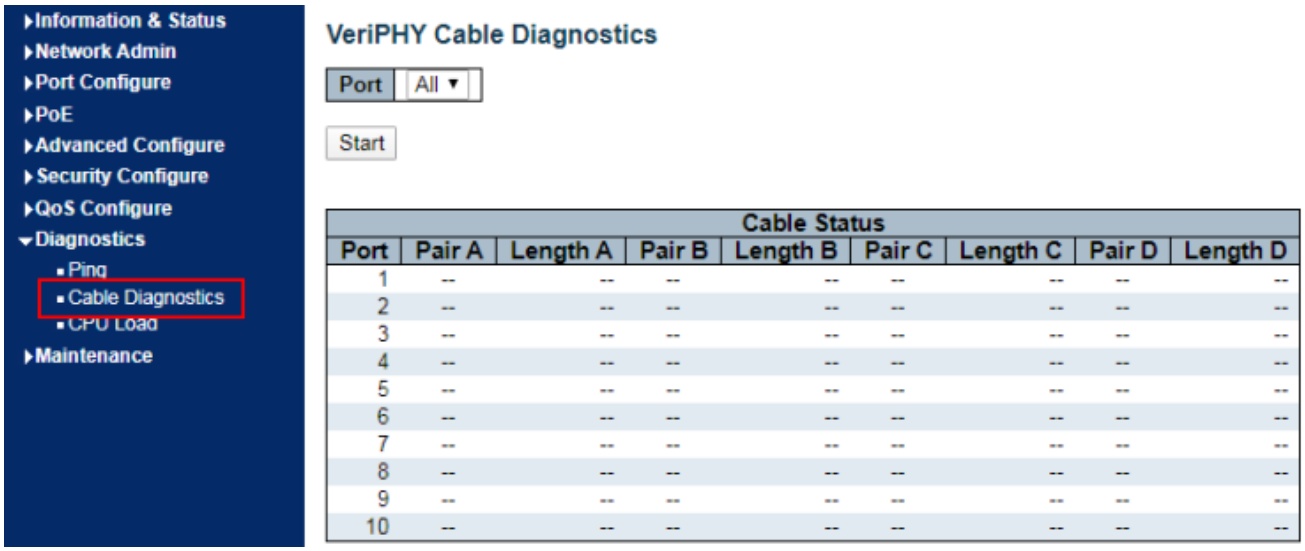


Параметр	Описание
IP Address	Введите адрес пинга
Ping Count	Введите количество отправляемых пакетов (От 1 до 60)
Ping Length	Введите размер пакета в битах в диапазоне от 1 до 1452, 56 по умолчанию
Ping Interval	Введите интервал пинга

Нажмите “**Start**” для запуска пинга.

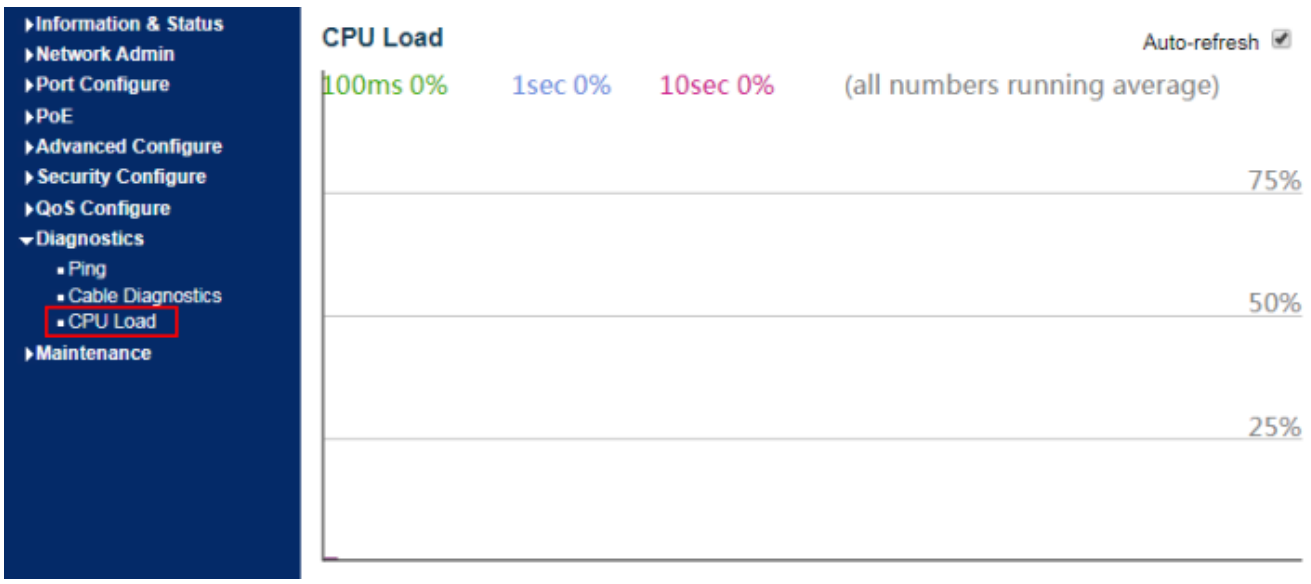
9.2 Cable Diagnostics

При использовании стандартов 10/100/1000 BASE-T на интерфейсах есть функция проверки открытых парт, петли и длины пар, для этого выберите “**Diagnostics-Cable Diagnostics**”:



9.3 CPU Load

Отображение нагрузки CPU в процентах и построение графика средней нагрузки на CPU в промежуток времени, для просмотра выберите “**Diagnostics-CPU Load**”:



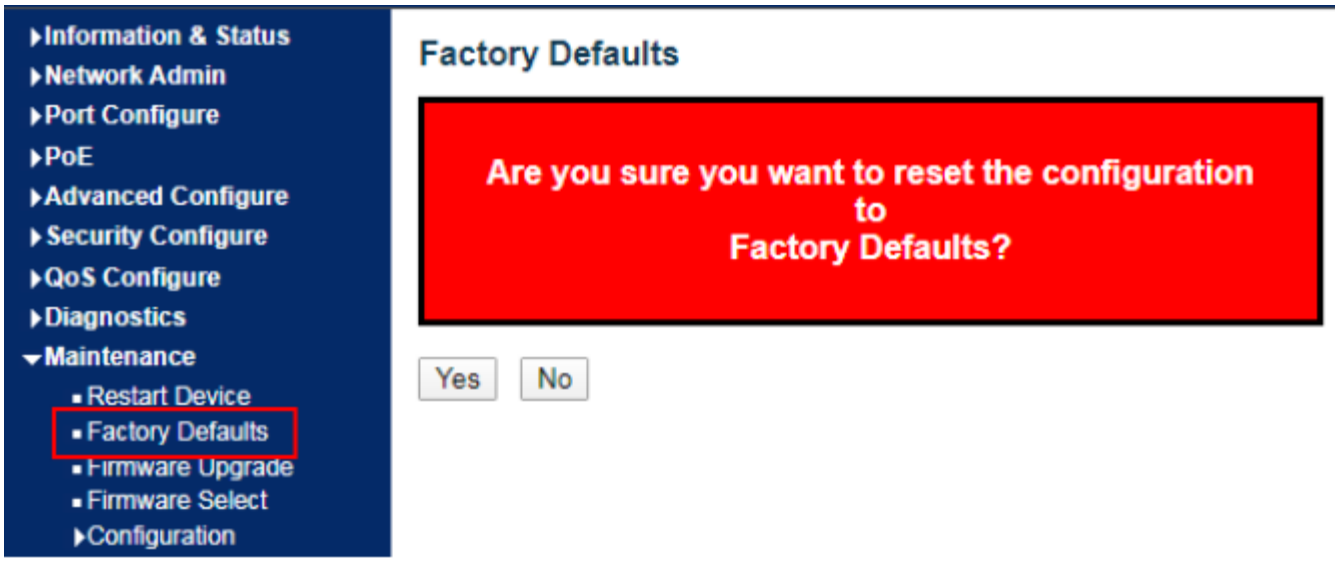
10. Maintenance

10.1 Restart Device

Выберите “**Maintenance**-**Restart Device**” и нажмите “**Yes**” для перезагрузки коммутатора:

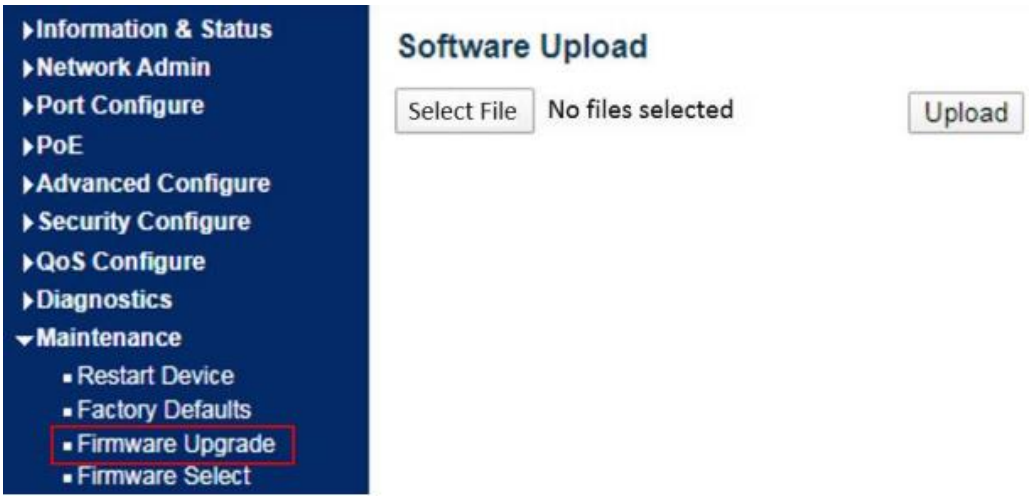
10.2 Factory Defaults

Выберите “**Maintenance**-**Factory Defaults**” и нажмите “**Yes**” для сброса конфигурации по умолчанию:



10.3 Firmware Upgrade

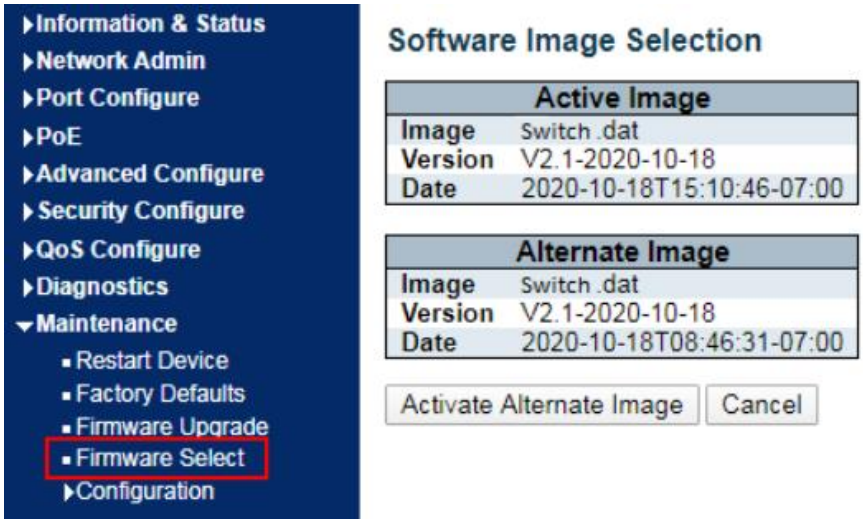
Выберите “**Maintenance-Firmware Upgrade**”



Нажмите “**Browse**” для выбора прошивки с ПК для её обновления
Нажмите “**Upload**” для обновления прошивки

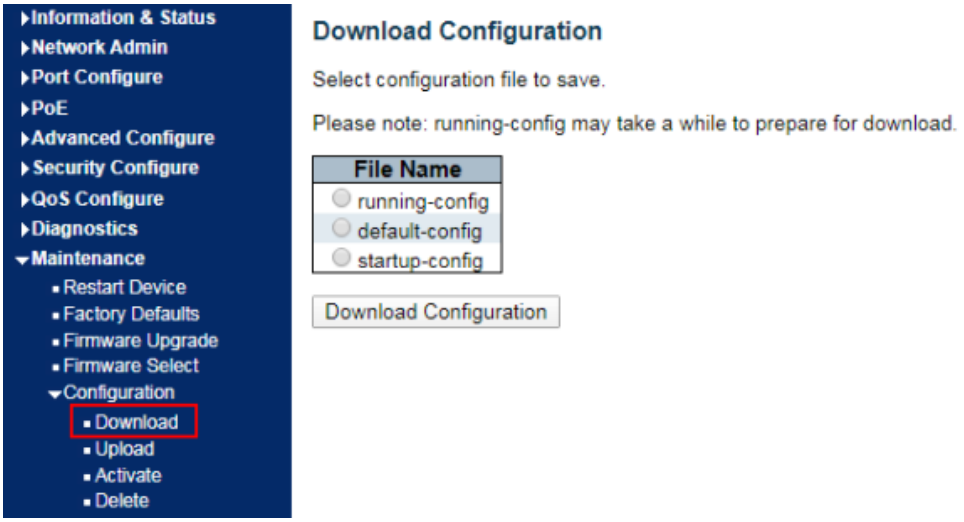
10.4 Firmware Select

На коммутаторе находятся 2 прошивки, основная и альтернативная, для смены прошивки на альтернативную выберите пункт “**Maintenance-Firmware Select**” и нажмите “**Activate Alternate Image**”:

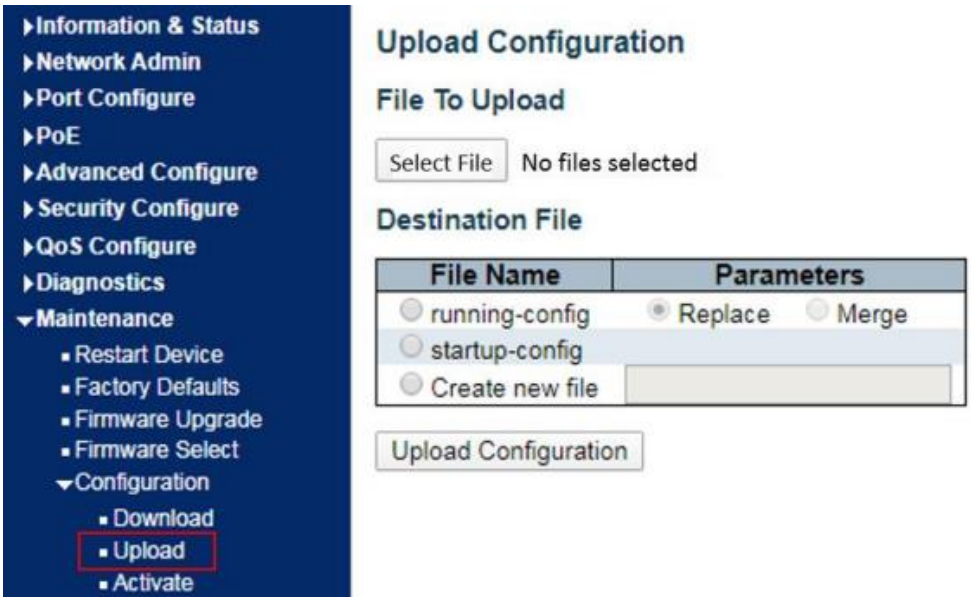


10.5 Configuration

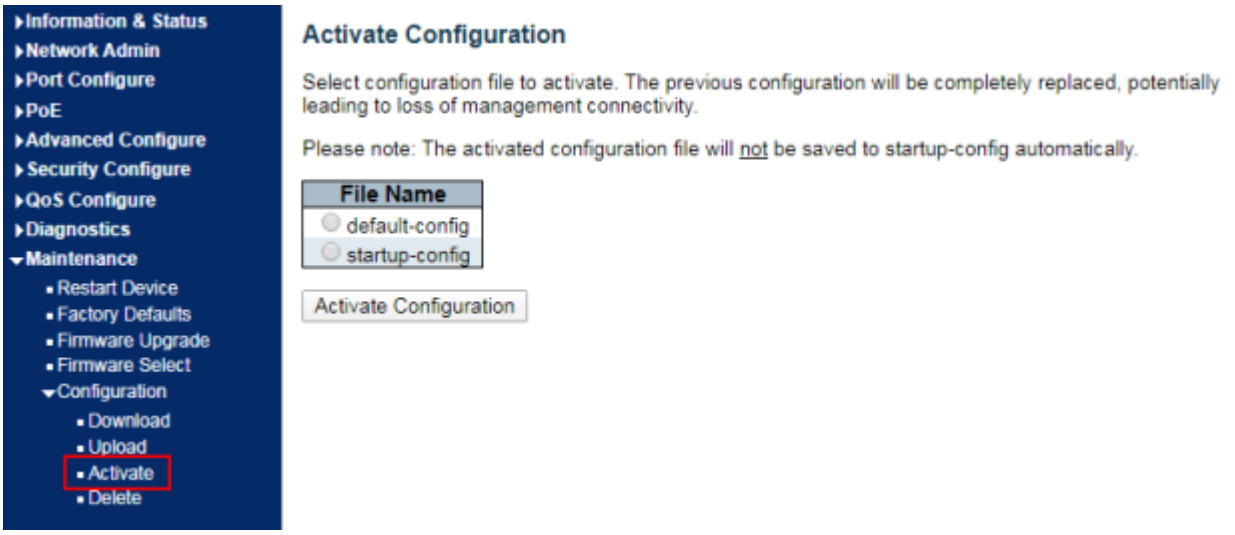
Для сохранения на ПК конфигурации выберите пункт “**Maintenance-Configuration-Download**” и нажмите “**Download Configuration**”:



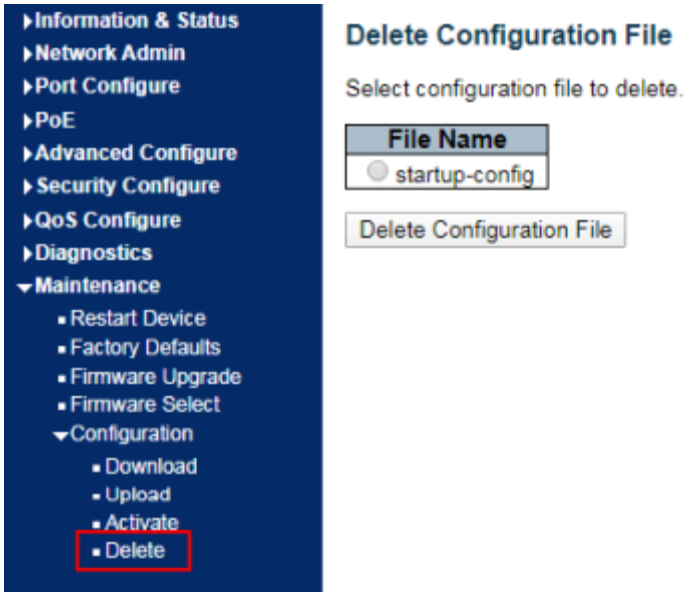
Для загрузки с ПК на коммутатор конфигурации выберите “**Maintenance-Configuration-Upload**” и нажмите “**Upload**”:



Для активации необходимой конфигурации при загрузке коммутатора выберите “**Maintenance-Configuration-Activate**” и нажмите “**Activate Configuration**”:



Для удаления конфигурации используйте пункт “**Maintenance – Configuration-Delete**” и нажмите “**Delete Configuration File”:**



11. Гарантийные обязательства

Производитель гарантирует отсутствие дефектов и неисправностей оборудования GIGALINK и несет ответственность по гарантийным обязательствам в соответствии с действующим законодательством Российской Федерации.

Гарантийный период исчисляется с момента приобретения Оборудования и составляет 12 (двенадцать) месяцев.

В течение гарантийного срока Производитель обязуется бесплатно устранить дефекты оборудования путем его ремонта или замены на аналогичное при условии, что дефект возник по вине Производителя. Устройство, предоставляемое для замены, может быть, как новым, так и восстановленным, но в любом случае Производитель гарантирует, что его характеристики будут не хуже, чем у заменяемого устройства.

Гарантийное обслуживание оборудования GIGALINK производится в авторизованных сервисных центрах более чем в 20 городах России.
Получить информацию о ближайшем сервисном центре можно по телефону +7 (499) 649-25-76.

Дополнительная информация о гарантии доступная на странице:

https://giga-link.ru/warranty/.

ООО «Тайле Рус»
Телефон 8 800 600-72-65
www.tayle.ru | office@tayle.ru
Юридический и фактический адрес: Россия,127410, г. Москва,
Алтуфьевское шоссе, д. 41
ТЕХНИЧЕСКАЯ ПОДДЕРЖКА
+7 (499) 649 25 76

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ ПО ПРОДУКТУ РАЗМЕЩЕНА НА ОФИЦИАЛЬНОМ САЙТЕ