Инструкция по управлению коммутатором через

WEB-интерфейс

Оглавление

1. Подготовка перед управлением коммутатором через WEB-интерфейс... 6

2. Подготовка перед управлением коммутатором через порт CONSOLE 7

3. Подготовка перед управлением коммутатором через Telnet/SSH..... 9

4. Управление через WEB-интерфейс, основные элементы 12

4.1 Структура дерева навигации по группам 12

4.2 Описание кнопок WEB интерфейса 13

4.3 Сообщения об ошибке.....13

4.4 Поля для ввода информации или значений 14

4.5 Поля со значениями текущего статуса.....15

5. Описание разделов меню WEB-интерфейса коммутатора 15

5.1 Главная страница WEB интерфейса 15

5.2 Мониторинг датчиков (Industrial Switch Monitoring) 16

5.3 System Configuration (Конфигурация системы) 20

5.3.1 Basic Information (Общая информация) 20

5.3.2 Serial information (Информация о RS 232/485 порте для управления коммутатором) 21

5.3.3 User Management (Информация о пользователях).....22

5.3.4 Safe Management (управление безопасностью).....23

5.3.5 SNTP Configuration (Настройка протокола синхронизации времени) 23

5.3.6 Jumbo Frame Configuration (Выбор размера Jumbo пакетов).....25

5.3.7 Current Configuration File (Просмотр текущей конфигурации).....26

5.3.8 Configuration file (Стартовая конфигурация, сохранение файла с настройками) 27

5.3.9 File upload (Загрузка файла с настройками) 28

5.3.10 System Reset (Перезагрузка коммутатора) 29

5.4 Port configuration (Конфигурирование портов).....30

5.4.1 Common Configuration (Базовая конфигурация портов).....30

5.4.2 Port statistics (Статистика работы портов) 31

5.4.3 Flow Control (управление потоком для портов) 32
5.4.4 Broadcast storm control (управление защитой от Broadcast storm) 33
5.4.5 Port rate limit (Ограничение пропускной способности на портах) 34
5.4.6 Protected Port (Защита портов) 35
5.4.7 Learn Limit (Ограничение максимального количества MAC для работы) 36
5.4.8 Port Trunk Configuration (Конфигурирование trunk'ов) 37
5.4.9 Port mirror configuration (Зеркалирование портов) 38
5.4.10 DDM information (Информация о подключённых SFP модулях) 39
5.5 MAC binding (привязка MAC адреса) 40
5.5.1 MAC binding configuration (Настройка привязки MAC адресов) 40
5.5.2 MAC Auto Bind (Автоматическая привязка MAC адресов) 41
5.6 MAC Filter (Фильтр MAC адресов) 42
5.6.1 MAC Filter Configuration (Настройка фильтра MAC адресов) 42
5.6.2 MAC Auto Filter (Автоматический фильтр MAC адресов) 43
5.7 VLAN Configuration (Настройка VLAN) 44
5.7.1 VLAN information (Информация о VLAN) 44
5.7.2 Static VLAN Configuration (Настройка VLAN) 45
5.7.3 VLAN Port Configuration (Конфигурация портов VLAN) 46
5.8 SNMP Configuration (Настройка SNMP протокола управления) 47
5.8.1 SNMP Community Configuration (Общие настройки для SNMP) 47
5.8.2 TRAP Target Configuration (Настройка TRAP уведомлений) 47
5.9 ACL Configuration (Настройка Access Control List) 48
5.9.1 ACL Standard IP Configuration (Настройка ACL для IP) 48
5.9.2 ACL Extended IP (Расширенная настройка ACL правил для IP) 49
5.9.3 ACL Configuration (Настройка ACL правил с помощью MAC) 49
5.9.4 ACL MAC ARP Configure (Настройка ACL правил для ARP с помощью MAC адресов) 50
5.9.5 ACL information (Набор действующих ACL правил) 51
5.9.6 ACL reference configuration (Настройка ACL правил) 52

5.10 QoS Configuration (Настройка предоставления трафика с разным приоритетом)53
5.10.1 QoS Apply (Настройка приоритетов трафика для портов) 53
5.10.2 QoS Schedule Configuration (Настройка расписания применения QoS) 54
5.11 IP Basic Configuration (Базовая настройка IP).....55
5.11.1 IP Address Configuration (Настройка IP адреса коммутатора).....55
5.11.2 ARP configuration and Display (Настройка протокола ARP и отображение таблицы ARP) 56
5.11.3 Host Static Route Configuration (Настройка таблицы Static маршрутизации) 57
5.12 AAA Configuration (настройка системы аутентификации авторизации и учета событий).....58
5.12.1 Tacacs+ configuration (настройка протокола Tacacs+) 58
5.12.2 Radius Configuration (настройка Radius системы AAA) 59
5.12.3 802.1x Configuration (Настройка параметров системы авторизации и аутентификации по стандарту 802.1x) 60
5.12.4 802.1x Port Configuration (Настройка портов для системы авторизации и аутентификации по стандарту 802.1x) 62
5.12.5 802.1x User Authentication Information (Информация о всех процессах аутентификации по стандарту 802.1x) 63
5.13 MSTP Configuration (Настройка работы протокола STP) 64
5.13.1 MSTP Configuration (Основные настройки MSTP).....64
5.13.2 Port configuration (настройка MSTP на портах).....65
5.13.3 Port information (Общая информация о конфигурации MSTP) 67
5.14 IGMP Snooping configuration (Настройка отслеживания IGMP трафика).....68
5.14.1 IGMP Snooping configuration (Настройки функции IGMP snooping) 68
5.14.2 Multicast Group Information (Общая информация о IGMP) 69
5.15 GMRP Configuration (Настройка работы протокола GMRP).....69
5.15.1 GMRP Global Configuration (Глобальные настройки GMRP) 69
5.15.2 GMRP ports configuration (Настройка GMRP на портах).....70
5.15.3 GMRP State machine (Общая информация о GMRP) 71
5.16 EAPS Configuration (Настройка работы протокола EAPS).....72

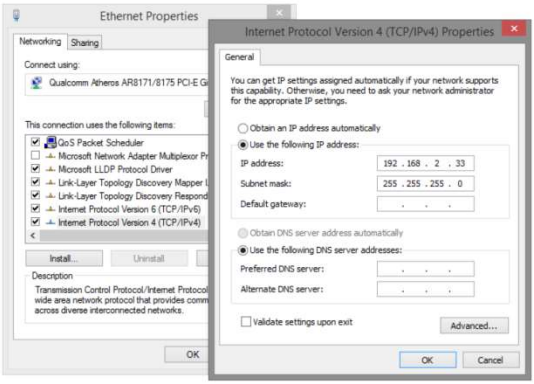
5.16.1 EAPS Configuration (Основные настройки работы протокола EAPS) 72
5.16.2 EAPS information (Сводная информация о работе протокола EAPS).....73
5.17 RMON Configuration (Настройка работы протокола RMON).....74
5.17.1 RMON statistics (Настройка групп статистики для RMON) 74
5.17.2 History Configuration (Настройка групп предыстории для RMON) 75
5.17.3 Alarm Configuration (Настройка групп аварийных сигналов).....76
5.17.4 Event Configuration (Настройка групп событий для RMON).....77
5.18 Cluster configuration (Настройка кластера) 78
5.18.1 NDP configuration (Настройка протокола NDP).....78
5.18.2 NTDP Configuration (Настройка протокола NTDP) 79
5.18.3 Cluster Configuration (Настройка кластера).....80
11.19 ERPS Configuration (Настройка ERPS).....82
5.19.1 ERPS Configuration (Настройка протокола ERPS).....82
5.19.2 ERPS Information (Информация о работе ERPS) 83
5.20 Log management (Управление записью логов).....83
5.21 POE Power Control (Управление параметрами PoE).....84
5.21.1 POE Port Configuration (Настройка параметров PoE).....84
5.21.2 POE Policy Configuration (Настройка расписания PoE) 85
5.21.3 PD Query Configuration (Функция антизависания PoE устройств) 86

1. Подготовка перед управлением коммутатором через WEB-интерфейс

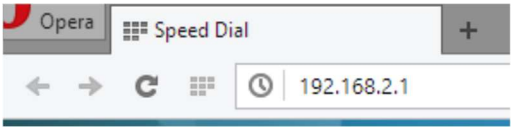
WEB-интерфейс позволяет гибко настраивать и отслеживать состояние коммутатора, используя браузер (Google Chrome, Opera, IE и тд) из любой точки в сети.

Прежде, чем приступить к настройке коммутатора через Web-интерфейс, необходимо убедиться, что ваш ПК и коммутатор находятся в одной сети. Чтобы правильно сконфигурировать ваш ПК используйте следующую пошаговую инструкцию:

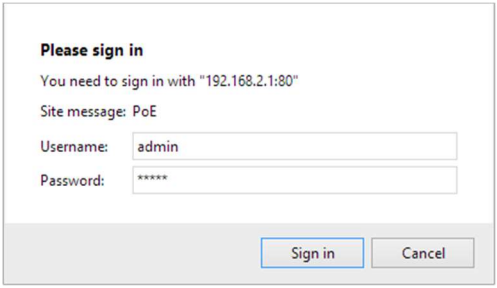
1. Убедитесь, что сетевая карта в вашем ПК установлена, работает и поддерживает TCP/IP протокол.
2. Подключите между собой коммутатор и ваш ПК, используя патч-корд RJ-45
3. По умолчанию IP-адрес коммутатора: **192.168.0.1** Коммутатор и ваш ПК должны находиться в одной подсети. Измените IP адрес вашего ПК на 192.168.0.X, где X-число от 2 до 254. Пожалуйста, убедитесь, что IP-адрес, который вы назначаете вашему ПК, не совпадал с IP-адресом коммутатора.



4. Запустите Web-браузер (IE, Firefox, Chrome) на вашем ПК
5. Введите в адресную строку **192.168.0.1** (IP-адрес коммутатора) и нажмите Enter на клавиатуре.



6. Появится форма аутентификации. По умолчанию Логин: **admin.** Пароль: **admin**



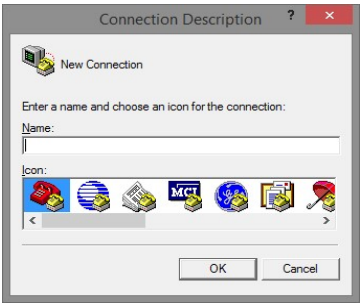
В дальнейшем пароль и логин можно поменять через WEB интерфейс коммутатора.

2. Подготовка перед управлением коммутатором через порт CONSOLE

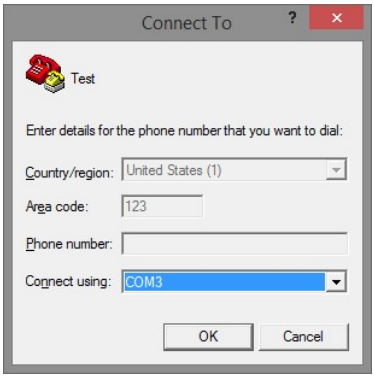
Управление коммутатором через COM-порт (RS-232) может потребоваться, если по каким-либо причинам управление через WEB-недоступно.

Скачайте и установите на ПК, с которого будет проводиться конфигурирование коммутатора программу-эмулятор HyperTerminal или PuTTY. После установки необходимого ПО используйте следующую пошаговую инструкцию:

1. Соедините порт Console коммутатора с COM-портом компьютера с помощью кабеля.
2. Запустите HyperTerminal на ПК.
3. Задайте имя для нового консольного подключения.

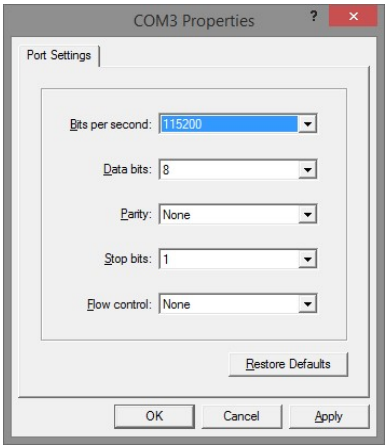


4. Выберите COM-порт, к которому подключен коммутатор.

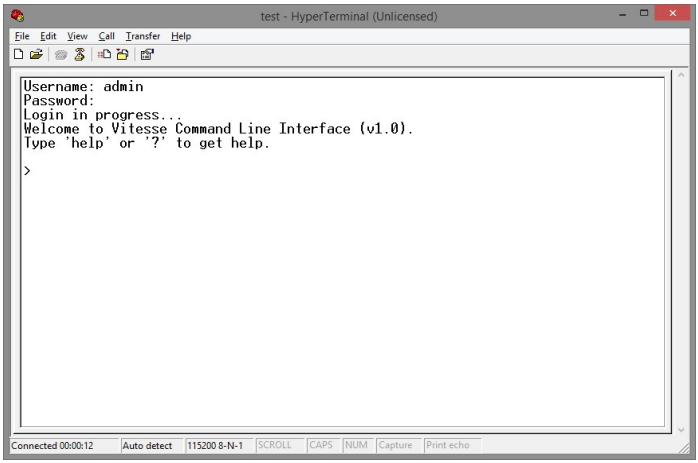


5. Настройте COM-порт следующим образом:

- Скорость передачи данных (Baud Rate) – 115200;
- Биты данных (Data bits) – 8;
- Четность (Parity) – нет;
- Стоп биты (Stop bits) – 1;
- Управление потоком (flow control) – нет.



6. Система предложит войти Вам в интерфейс CLI (управление через командную строку). По умолчанию имя пользователя/пароль – admin/admin.



3. Подготовка перед управлением коммутатором через Telnet/SSH

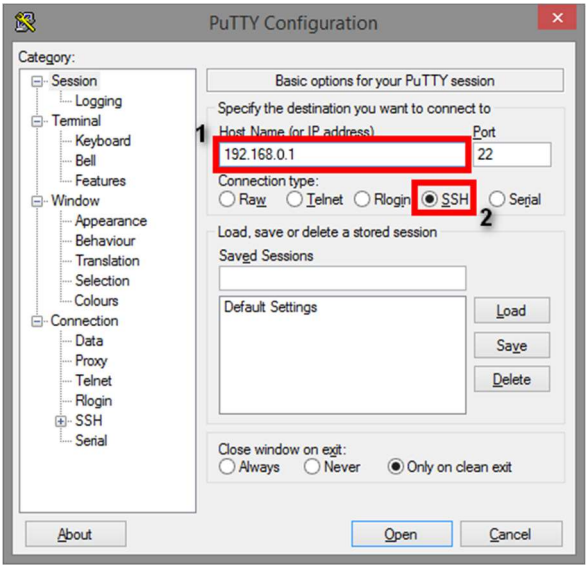
Протоколы Telnet и SSH предоставляют пользователю текстовый интерфейс командной строки для управления коммутатором (CLI). Но только SSH обеспечивает создание безопасного канала с полным

шифрованием передаваемых данных. Чтобы получить доступ к CLI коммутатора через Telnet/SSH, ваш ПК и коммутатор должны находиться в одной сети. Подробнее, как это сделать рассматривалось в разделе инструкции «Подготовка перед управлением коммутатором через WEB-интерфейс».

Telnet интерфейс встроен в командную строку CMD семейства операционных систем Microsoft Windows. SSH интерфейс доступен только с помощью программы эмулятора SSH терминала. Ниже показано, как получить доступ к CLI коммутатора через SSH с помощью программы PuTTY.

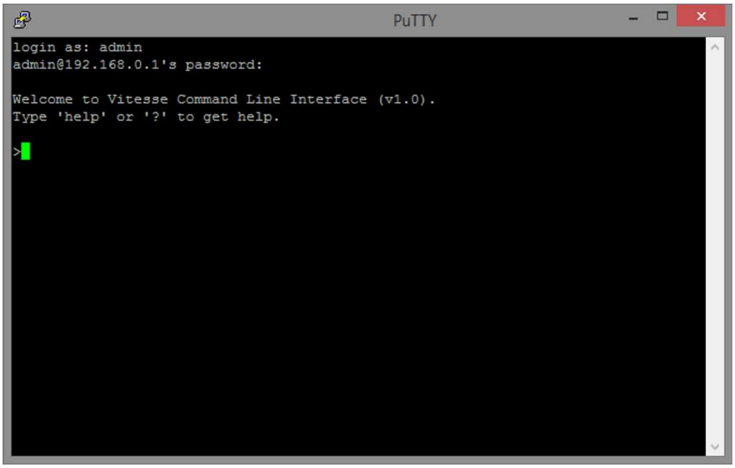
1. Зайдите в меню PuTTY Configuration. Введите IP адрес коммутатора в поле Имя хоста (Host Name) (или IP адрес). По умолчанию IP адрес коммутатора **192.168.0.1**

2. Выберите тип подключения (Connection type) – SSH.



3. Если вы подключаетесь к коммутатору через SSH впервые, вы увидите окно PuTTY Security Alert. Нажмите Yes (Да) для продолжения.

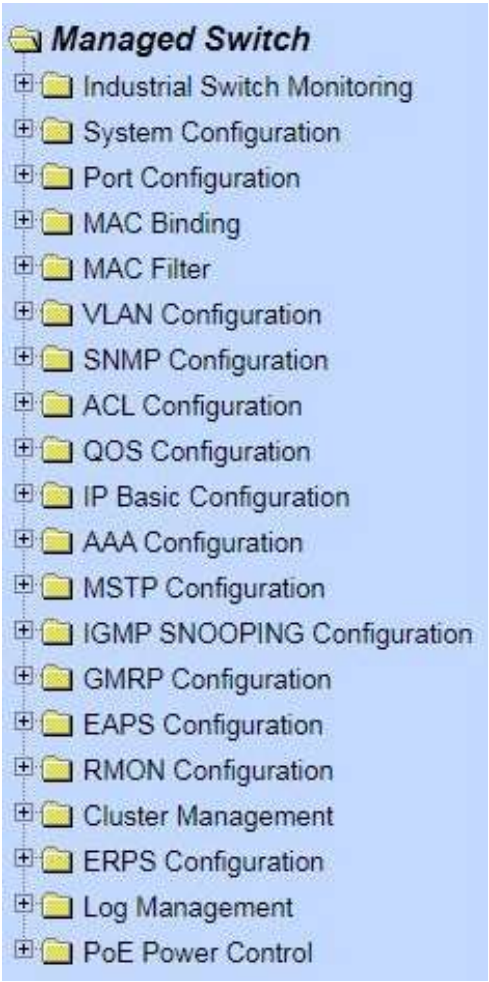
4. PuTTY обеспечит вам доступ к управлению коммутатором после того как Telnet/SSH подключение будет установлено. По умолчанию имя пользователя/пароль: **admin/admin.**



4. Управление через WEB-интерфейс, основные элементы

4.1 Структура дерева навигации по группам

Меню web-интерфейс состоит из 19 разделов:



4.2 Описание кнопок WEB интерфейса

Большинство кнопок для изменения настроек коммутатора через WEB-интерфейс чаще всего выполняют одну и ту же роль. В таблице приведены описания функций, которые кнопки выполняют.

Кнопка	Назначение
Refresh (Обновить)	Обновляет значение всех текстовых полей и параметров на странице.
Apply (Принять/подтвердить)	Числовое значение будет обновлено в памяти. Введенные значения параметра вступают в силу только после нажатия этой кнопки. Если данные введены не корректно, появится сообщение об ошибке.
Delete (Удалить)	Удаляет текущее значение
Help (Помощь/справка)	Открывает страницу справки. Отдельная страница справки для каждого запроса.

4.3 Сообщения об ошибке

При возникновении ошибки при обработке запроса от пользователя к коммутатору (введены не корректные значения) появляется окно с описанием ошибки.

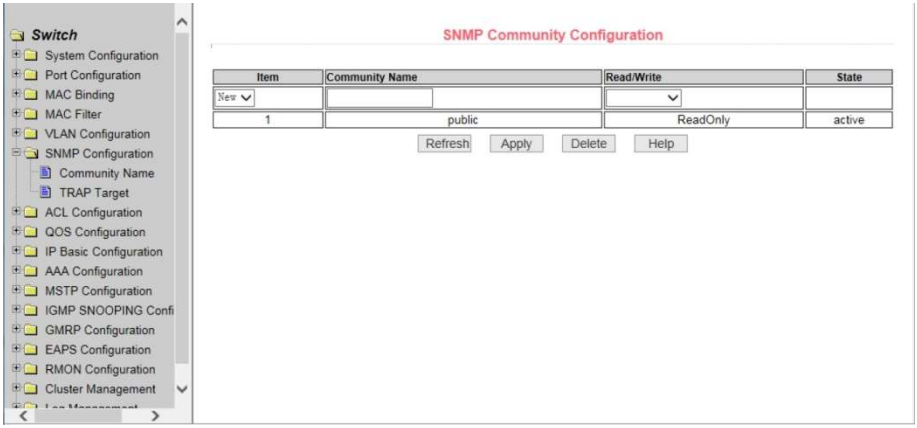
4.4 Поля для ввода информации или значений

Некоторые страницы WEB-интерфейса коммутатора содержат поля для ввода той или иной информации или значений. С помощью этих полей можно получить доступ к различным строкам в таблице (рис.).

Если понадобится добавить новую строку необходимо выбрать из выпадающего списка *NEW* (новая) и нажать для подтверждения кнопку *Apply* (принять).

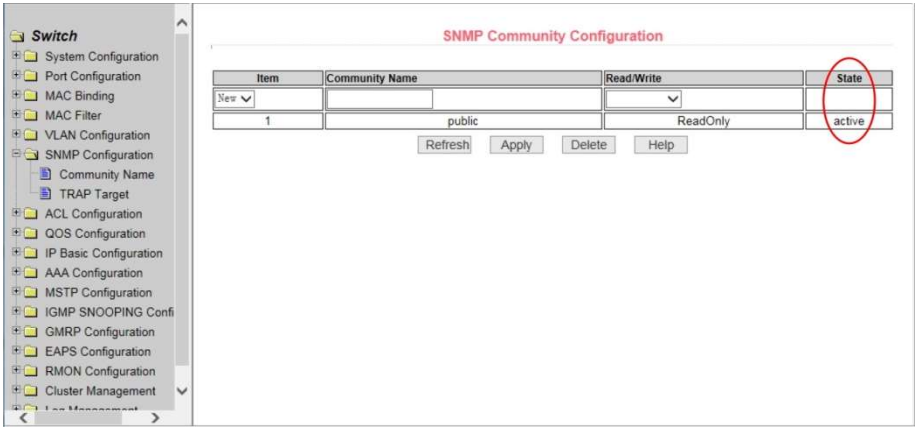
Если нужно изменить уже существующую строку, необходимо выбрать из выпадающего списка соответствующий номер строки, ввести нужные значения и нажать для подтверждения кнопку *Apply* (принять).

Для удаления строки из таблицы, выберите из выпадающего списка нужный номер строки и нажмите кнопку *Delete* (удалить).



4.5 Поля со значениями текущего статуса

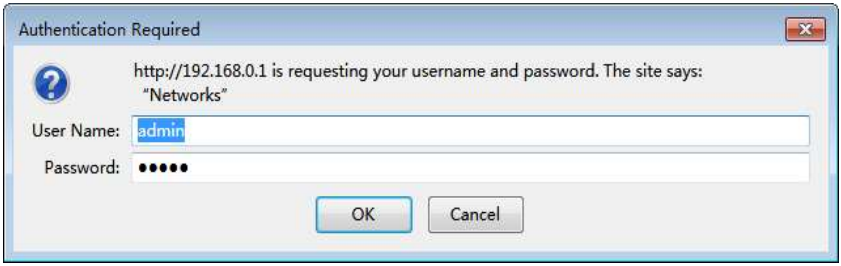
Некоторые страницы (или поля на страницах) WEB-интерфейса предназначены только для отображения данных о работе коммутатора. Отображаемые значения на этих страницах предназначены только для чтения и не могут быть изменены (например, поля колонки *State* на рисунке ниже).



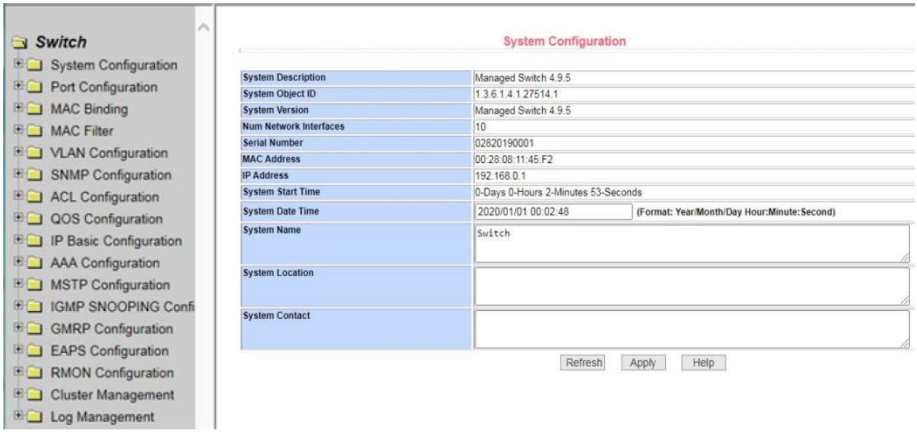
5. Описание разделов меню WEB-интерфейса коммутатора

5.1 Главная страница WEB интерфейса

После того, как были введены корректные данные для входа (по умолчанию имя пользователя: ***admin***, пароль: ***admin***),



коммутатор отобразит главную страницу WEB-интерфейса управления коммутатором (рис.):



5.2 Мониторинг датчиков (Industrial Switch Monitoring)

На данной странице WEB интерфейса коммутатора находятся данные с датчиков температуры, влажности и тд.

Кроме того, здесь также представлена возможность настройки сценариев реагирования портов коммутатора на различные события.

Ring Control – при активации (on) позволяет отслеживать обнаружение кольцевой топологии в сети.

System Temperature – поле отображает текущую температуру на центральном чипе коммутатора.

System Temperature Upper – значение температуры из диапазона на центральном чипе коммутатора, при превышении которого подается сигнал (если настроен) на выход ALARM коммутатора.

System Temperature Lower – отрицательное значение температуры из диапазона на центральном чипе коммутатора, при понижении которого подается сигнал (если настроен) на выход ALARM коммутатора.

Ambient Temperature – поле отображает текущую температуру на внешнем подключаемом к коммутатору датчике.

Ambient Temperature Upper – значение температуры из диапазона на внешнем подключаемом к коммутатору датчике, при превышении которого подается сигнал (если настроен) на выход ALARM коммутатора.

Ambient Temperature Lower – отрицательное значение температуры из диапазона на внешнем подключаемом к коммутатору датчике, при понижении которого подается сигнал (если настроен) на выход ALARM коммутатора.

Ambient Humidity – поле отображает текущую влажность на внешнем подключаемом к коммутатору датчике.

Ambient Humidity Upper – значение влажности из диапазона на внешнем подключаемом к коммутатору датчике, при превышении которого подается сигнал (если настроен) на выход ALARM коммутатора.

System Power Upper – значение мощности PoE из диапазона, при превышении которого подается сигнал (если настроен) на выход ALARM коммутатора.

Power Type – поле отображает тип питания.

Power In (Master V1, Slave V2*)* – поле отображает подключенные к коммутатору блоки питания. Основной – V1 и резервный – V2.

System Current (A) – поле отображает ток в Амперах, потребляемый коммутатором.

Master V1 Voltages (V) – поле отображает значение напряжения в Вольтах на основном блоке питания.

Slave V2 Voltages (V) – поле отображает значение напряжения в Вольтах на резервном блоке питания.

System Power (W) – поле отображает текущую потребляемую коммутатором мощность в Ваттах.

System 3.3V – поле отображает значение системного напряжения 3.3V на плате коммутатора.

System 1.5V – поле отображает значение системного напряжения 1.5V на плате коммутатора.

System 1.2V – поле отображает значение системного напряжения 1.2V на плате коммутатора.

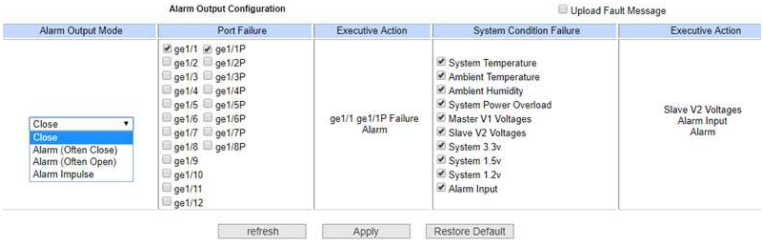
Раздел **Alarm Input Configuration** позволяет настраивать сценарий работы портов коммутатора при получении сигнала тревоги на входе *Alarm*.

Alarm detection method – выбор порога срабатывания

- ✓ *OFF* - вход Alarm отключен
- ✓ *Low level alarm* – срабатывание при низком уровне напряжения на входе Alarm (low level < 5V)
- ✓ *High level alarm* - срабатывание при высоком уровне напряжения на входе Alarm (57V >high level >5V)

Close port / Reboot port – выбор сценария работы портов при получении сигнала тревоги, выбранные порты могут быть отключены. При отключении сигнала тревоги выбранные порты могут быть автоматически включены или перезагружены.

Alarm Output Configuration - позволяет закрывать для трафика/перезагружать и отключать порты, подавать сигнал тревоги на тревожный выход коммутатора в случае превышения напряжений БП, температуры на основном чипе, на внешнем датчике и т.д.



Alarm Output Mode – Режим работы выхода Alarm (включение / отключение, другие режимы работы).

- ✓ *Close* - выход Alarm отключен
- ✓ *Normally closed* – при срабатывании «сухой контакт» замыкается
- ✓ *Normally open* – при срабатывании «сухой контакт» размыкается
- ✓ *Cycle alarm* - при срабатывании «сухой контакт» периодически замыкается

Port status monitoring – позволяет контролировать состояние портов (в т.ч. PoE) коммутатора. При возникновении сбоев в работе портов подается сигнал тревоги, при нормализации работы портов тревожный сигнал отключается.

System Condition Failure - позволяет контролировать такие ошибки состояния системы как температура коммутатора, внешняя температура и влажность, параметры питания.

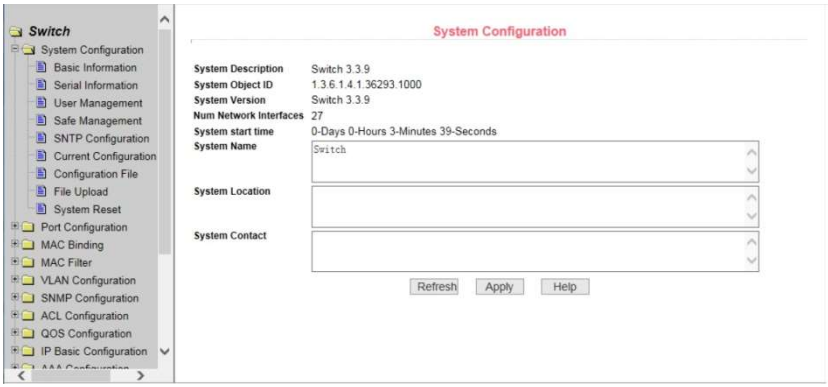
Для того чтобы обновить значения текущих параметров в используйте кнопку *Refresh*.

Для подтверждения прочих настроек – кнопку *Apply*.

Для возврата всех настроек на этой странице к исходным – кнопку *Restore Default*.

5.3 System Configuration (Конфигурация системы)

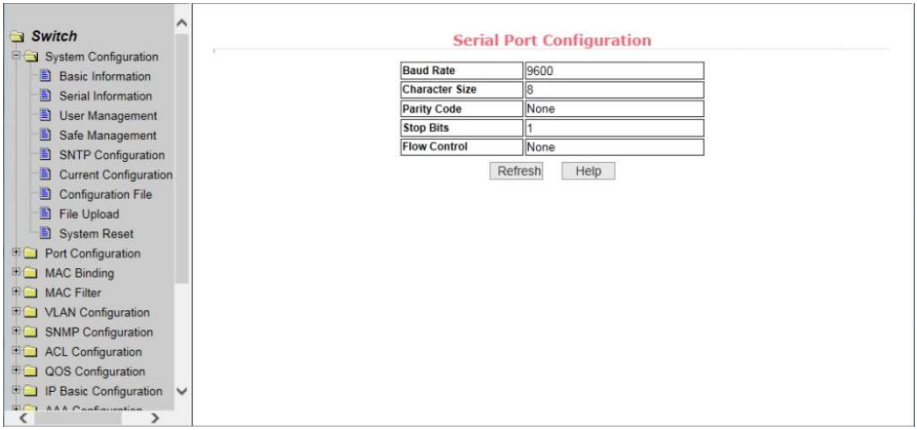
5.3.1 Basic Information (Общая информация)



- ✓ **System Description** (Описание системы) содержит общую информацию о системе;
- ✓ **System Object ID** (Идентификатор системы) отображает сетевой идентификатор системы;
- ✓ **System Version** (Версия прошивки) отображает текущую версию установленной на коммутатор прошивки;
- ✓ **Num network interfaces** (Количество портов в коммутаторе) отображает количество всех портов для соединения с сетью;
- ✓ **System start time** (Время запуска системы) отображает сколько времени прошло с момента включения;
- ✓ **System name** (Имя коммутатора) отображает имя коммутатора. Пользователь может переименовать коммутатор;

- ✓ **System location** (Местоположение коммутатора) отображает физическое местоположение коммутатора. Задается пользователем;
- ✓ **System Contact** (Контактные данные) отображает имя владельца и его контактные данные. Задается пользователем.

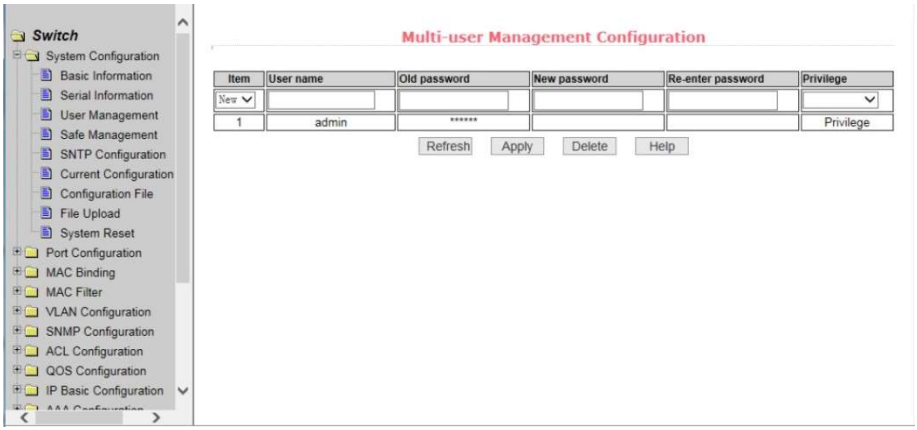
5.3.2 Serial information (Информация о RS 232/485 порте для управления коммутатором)



Данная страница WEB интерфейса содержит ряд параметров, которые необходимы для управления коммутатором через интерфейс RS232/485 используя порт CONSOLE. При управлении коммутатором через HyperTerminal убедитесь, что настройки соответствуют приведенным на этой странице значениям.

- ✓ **Baud rate** – скорость передачи данных
- ✓ **Character Size** – количество бит данных
- ✓ **Parity code –** четность
- ✓ **Stop bits –** стоповые биты
- ✓ **Flow control –** управление потоком

5.3.3 User Management (Информация о пользователях)



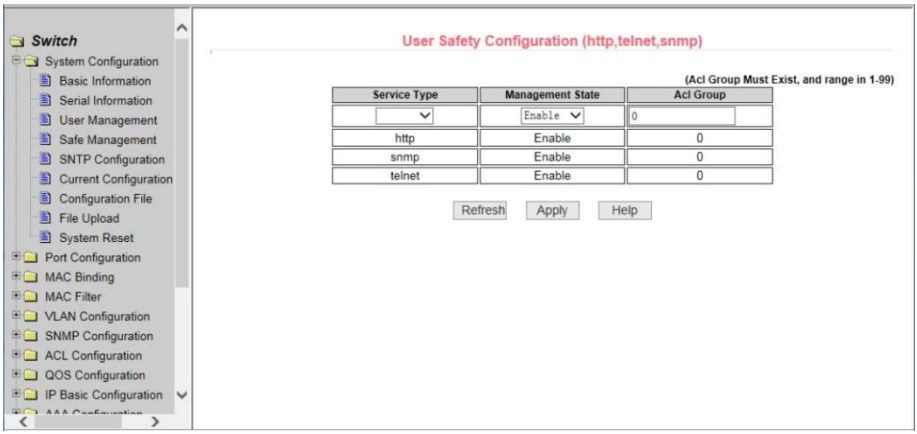
На этой странице можно изменить/задать новый пароль (*new password*) для текущего пользователя, изменить права доступа к управлению коммутатором (*privilege*) и др.

Пароли нужно вводить с учетом регистра. Они могут содержать до 16 символов. Для ввода пароля необходимо дважды ввести новый пароль в поле *New Password* и в *Re-enter Password*. Для того, чтобы изменения вступили в силу, необходимо нажать кнопку *Apply* (Принять). После этого пользователю потребуется заново войти в WEB интерфейс, используя новый пароль.

С помощью настроек на этой странице пользователь может задать многопользовательский режим управления коммутатором (*multi-user).*

Для управления через Telnet и WEB для пользователя должен быть выбран многопользовательский режим.

5.3.4 Safe Management (управление безопасностью)



На данной странице находятся настройки, позволяющие администратору гибко управлять доступом к управлению коммутатором (*WEB, TELNET* или *SNMP*) на основе *ACL* (лист управления доступом)

Есть возможность полностью отключить управление коммутатором для конкретного метода управления (*WEB, TELNET* или *SNMP*). По умолчанию управление с помощью каждого метода разрешено и ACL фильтрация не применяется.

Администратор может частично запретить управление коммутатором с помощью одного или нескольких методов, используя ACL фильтрацию.

При применении ACL фильтрации для каждого метода управления необходимо указать этот метод в списке *service type*, а затем выбрать ACL от 1 до 99. Главное условие – выбранный ACL должен быть создан заранее.

Обратите внимание, если администратор закроет возможность управлять коммутатором по WEB, эта страница с настройками перестанет быть доступна. Тогда можно воспользоваться другим методом управления, например через Telnet или SNMP.

5.3.5 SNTP Configuration (Настройка протокола синхронизации времени)

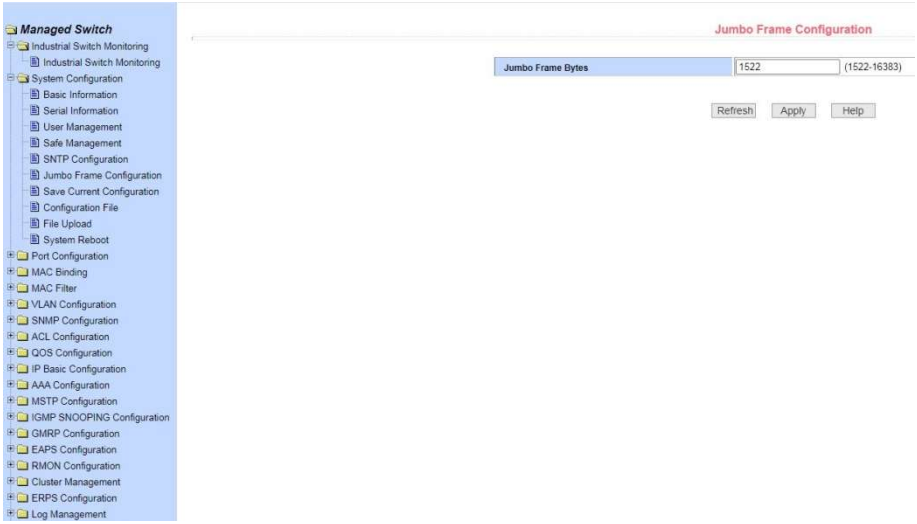
На данной странице WEB интерфейса представлены настройки для синхронизации времени коммутатора с одним из серверов с использованием протокола SNTP.

- ✓ **Server IP Address 1, Server IP Address 1, Server IP Address 1 –** поля для указания IP адресов серверов, с которыми будет проводится синхронизация.
- ✓ **Time Interval** – интервал синхронизации в сек. По умолчанию значение – 1800 сек.
- ✓ **Time Zone** – выбор часового пояса.

Refresh – обновить значения для обновляемых полей

Apply – принять настройки.

5.3.6 Jumbo Frame Configuration (Выбор размера Jumbo пакетов)



На данной странице WEB интерфейса находится поле для указания размера обрабатываемых пакетов.

При работе с multicast трафиком (например, HDMI по Ethernet) рекомендуется выставлять значение не менее 10240 Байт.

- ✓ **Jumbo Frame Bytes** – поле в котором задается размер обрабатываемых пакетов. Доступные значение в диапазоне от 1522 до 16383 Байт. Значение по умолчанию – 1522.

Refresh – обновить значения для обновляемых полей

Apply – принять настройки.

5.3.7 Current Configuration File (Просмотр текущей конфигурации)

На этой странице можно просмотреть текущую конфигурацию коммутатора в виде текстовой информации. Кнопка Save (сохранить) позволит сохранить текущую конфигурацию коммутатора в память коммутатора.

Поскольку запись файла требует удаления/записи на FLASH память коммутатора, операция может занять определенное время.

5.3.8 Configuration file (Стартовая конфигурация, сохранение файла с настройками)

Стартовая конфигурация представляет собой файл, записанный во FLASH памяти коммутатора. Когда коммутатор запускается и не находит записанный ранее файл конфигурации во FLASH памяти, устройство использует файл с настройками по умолчанию (*default*).

Кнопка *Delete* (удалить) позволяет вызвать диалоговое окно, где будет предложено удалить текущий файл конфигурации из FLASH памяти. Если вы передумали это делать, нажмите кнопку *Cancel* (отмена).

Кнопка *Download* (скачивание) используется для скачивания конфигурационного файла на ПК из памяти коммутатора. В диалоговом окне выберите SAVE (сохранить), а затем путь к каталогу с файлами конфигурации. По умолчанию имя файла switch.cfg

5.3.9 File upload (Загрузка файла с настройками)

На этой странице представлена возможность для загрузки ранее созданных файлов конфигурации в память коммутатора.

Нажмите кнопку Path (путь), чтобы выбрать нужный файл с конфигурацией на ПК. Далее, после выбора необходимого файла нажмите кнопку Upload (загрузить). Файл должен иметь расширение **.cfg**

Если у вас есть образ диска с настройками, то вы можете загрузить его также. Образ должен иметь расширение файла **.img**

⚠ Во время загрузки файла конфигурации в память коммутатора не переходите на другие страницы WEB интерфейса, не перезагружайте и не отключайте коммутатор, иначе настройки будут записаны с ошибками, что может повлечь за собой сбои в работе коммутатора.

5.3.10 System Reset (Перезагрузка коммутатора)

На данной странице WEB интерфейса предоставляется возможность перезагрузить коммутатор. Для этого нажмите кнопку *Reset* (перезагрузка). В появившемся диалоговом окне подтвердите свое действие кнопкой *OK* или отмените его с помощью кнопки *Cancel* (отмена).

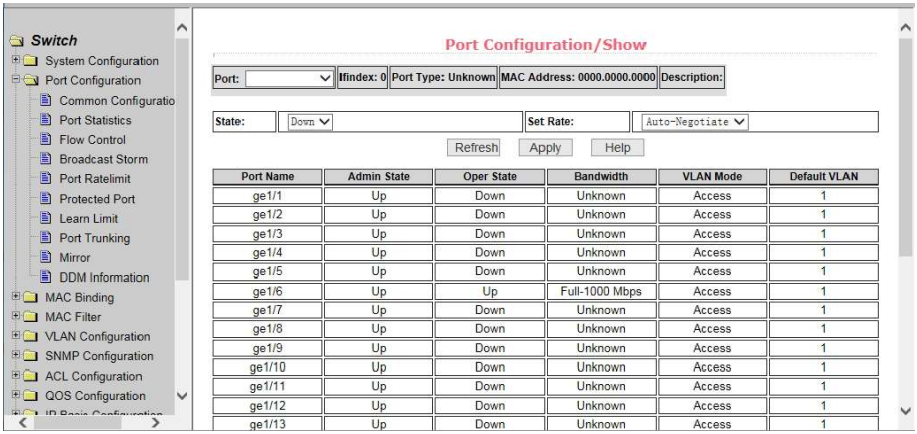
5.4 Port configuration (Конфигурирование портов)

5.4.1 Common Configuration (Базовая конфигурация портов)

На этой страницы представлена информация по каждому из портов коммутатора. Пользователь может менять скорость, включать или отключать тот или иной порт, просматривать базовую информацию.

Для настройки конкретного порта необходимо выбрать его название из выпадающего списка. По умолчанию все порты включены (UP), чтобы выключить порт необходимо выбрать пункт DOWN (выключить) и применить изменения кнопкой Apply (принять). Таким же образом выбирается и значения скорости для выбранного порта.

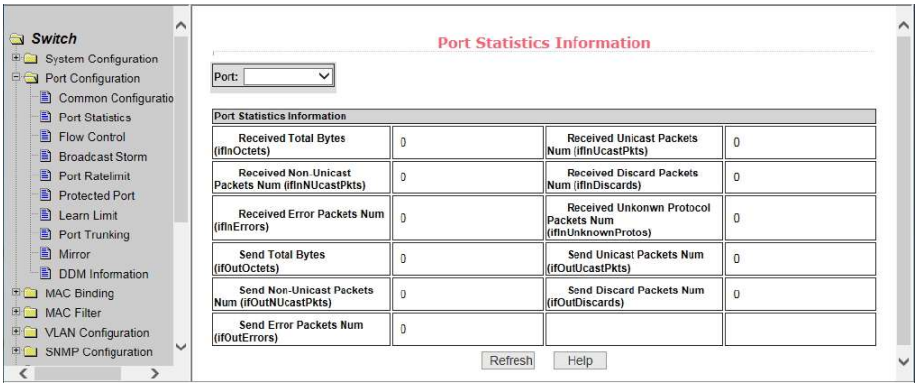
Если для какого-либо порта выбрать *Full-10 (Скорость передачи 10 Мбит/с, дуплекс),* то порт переключится в режим увеличения дальности передачи сигналов до 250м. Также порты матрицы способны автоматически переходить в этот режим при подключении к линии длиной 100-250м, обмен данными поддерживается только с Uplink портами.



Apply (принять) – сохранить изменения в настройках.

Refresh (обновить) - обновит значения настроек для портов.

5.4.2 Port statistics (Статистика работы портов)



На этой странице представлена сводная информация по работе портов. Для выбора конкретного порта воспользуйтесь выпадающем меню Port (порт). В таблице ниже отобразится вся доступная информация:

- Received Total Bytes (количество принятых байт);
- Received Non-Unicast Packets Num (количество принятых «не Unicast» пакетов);
- Received Error Packets Num (количество принятых пакетов с ошибкой);
- Send Total Bytes (количество отправленных байт);
- Send Non-Unicast Packets Num (количество отправленных «не Unicast» пакетов);
- Send Error Packets Num (количество отправленных с ошибкой пакетов);
- Received Unicast Packets Num (количество полученных Unicast пакетов);
- Received Discard Packets Num (количество «дропнутых» пакетов при получении);

- Received Unknown Protocol Packets Num (количество полученных пакетов с неизвестным протоколом передачи);
- Send Unicast Packets Num (количество отправленных Unicast пакетов);
- Send Discard Packets Num (количество отбрасываемых пакетов при отправке).

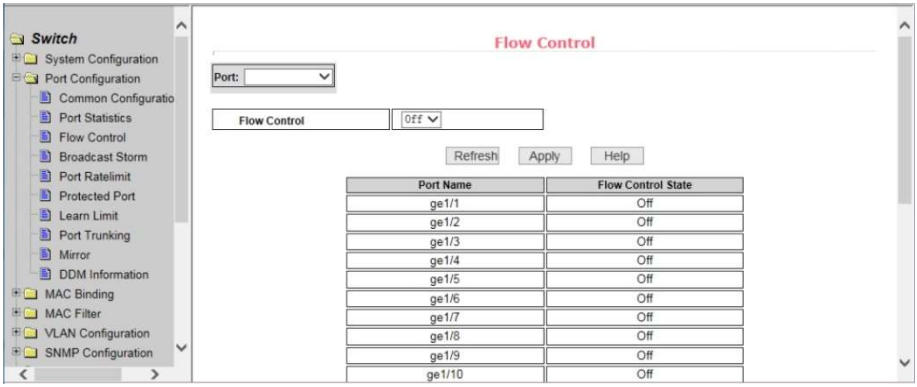
5.4.3 Flow Control (управление потоком для портов)

Данная страница позволяет настраивать функцию Flow Control (управление потоком) для конкретного порта.

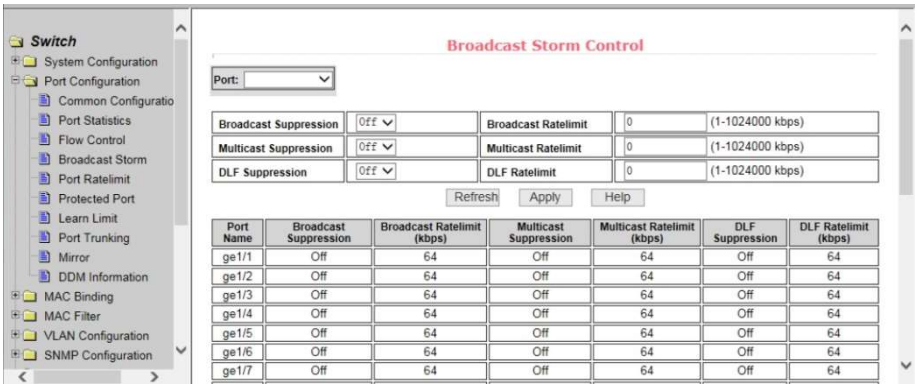
Чтобы включить или отключить Flow Control выберите конкретный порт из выпадающего меню, а затем состояние ON (вкл) или OFF (выкл.)

Данная настройка может выполняться для отправки и для получения пакетов.

Все изменения подтверждаются кнопкой Apply (принять).



5.4.4 Broadcast storm control (управление защитой от Broadcast storm)



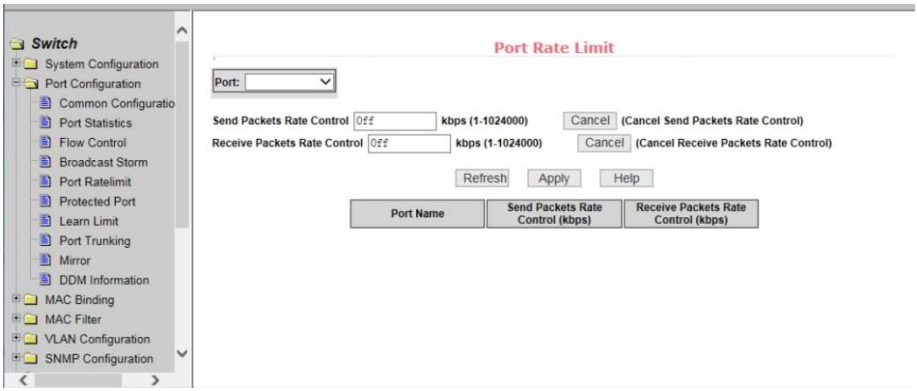
На данной странице находятся настройки, позволяющие включить или выключить защиту от влияния широковещательных (Multicast) пакетов и DLF пакетов на передаваемый/получаемый трафик.

В выпадающем списке PORT (порт) выберите необходимый порт, включите или выключите (ON или OFF) защиту для конкретного вида пакетов Broadcast, Multicast или DLF. Также можно задать скорость в Кбит/с для конкретного вида пакетов. DLF и Multicast скорости должны быть одинаковыми.

Refresh – обновить значения для обновляемых полей

Apply – принять настройки.

5.4.5 Port rate limit (Ограничение пропускной способности на портах)



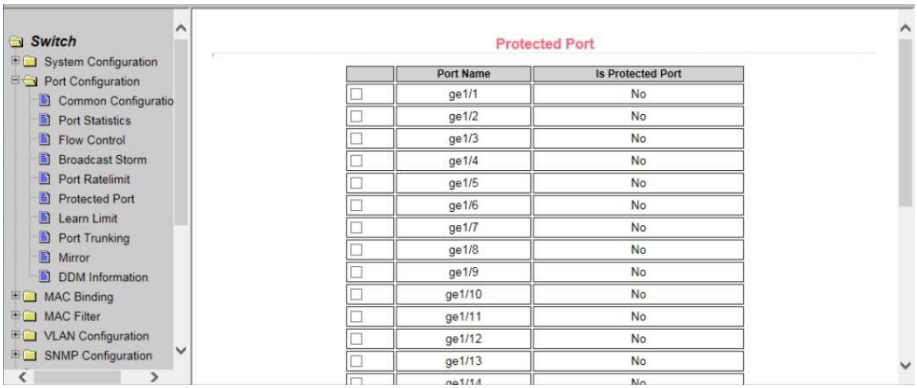
На данной странице можно гибко ограничивать скорость приема/передачи пакетов на выбранном порте. Для этого выберите порт в выпадающем списке PORT, а затем укажите значение в Кбит/с для скорости передачи данных (Send Packets Rate Control) и для скорости приема данных (Receive Packets Rate Control).

Для применения настроек нажмите кнопку Apply (принять).

Для отмены ограничения пропускной способности нажмите кнопку Cancel (отмена).

Refresh – обновить значения для обновляемых полей

5.4.6 Protected Port (Защита портов)



На данной странице можно выбрать порт, который будет изолирован от других.

Изолированный порт не может обмениваться данными с другими изолированными портами.

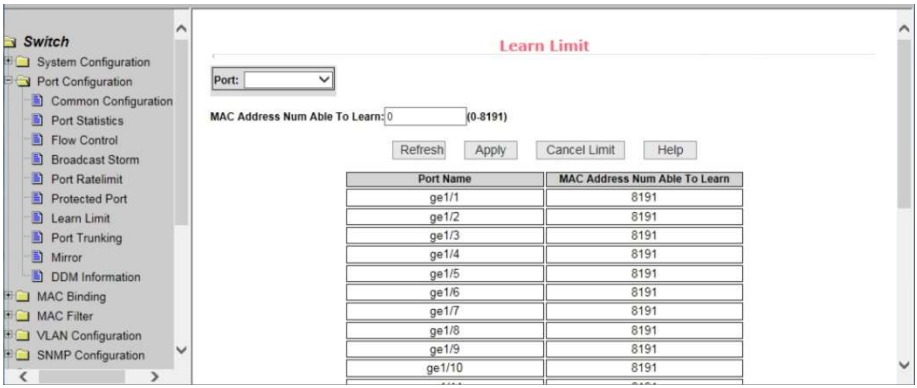
Изолированный порт может обмениваться данными только с неизолированным портом/портами.

Protected Port – изолировать порт

Unprotected Port – снять изоляцию порта

Refresh – обновить значения для обновляемых полей

5.4.7 Learn Limit (Ограничение максимального количества MAC для работы)



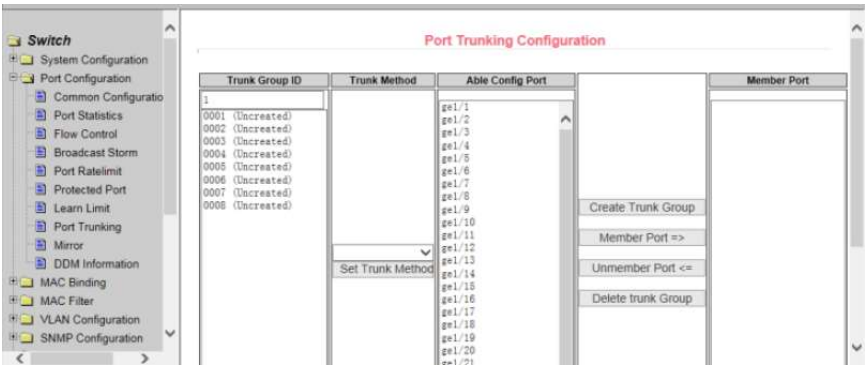
На данной странице WEB интерфейса представлена возможность управления максимальным количеством MAC адресов, с которыми способен работать порт. По умолчанию это значение равно 8191.

Для изменения этого значения выберите порт в выпадающем меню Port (порт), а затем в строке MAC Address Num Able to Learn (макс. количество MAC адресов) укажите свое значение.

Для применения настроек используйте кнопку Apply (принять),

Для отмены – Cancel Limit (отменить лимит).

5.4.8 Port Trunk Configuration (Конфигурирование trunk'ов)



На данной странице представлены настройки для конфигурации Trunk портов. Вы можете объединять их в группы (агрегирование), назначать ID для порта, менять способ выбора Trunk и тд.

Чтобы создать trunk для порта или изменить существующий необходимо выбрать ID от 1 до 3. Чтобы создать trunk группу выберите соответствующий идентификатор и нажмите кнопку Trunk ID Settings (настройка ID для trunk). Для настройки метода транкинга портов выберите из выпадающего списка необходимый и нажмите на кнопку Polymerization Settings.

Для удаления существующей группы trunk используйте кнопку Delete trunk group (удалить trunk группу).

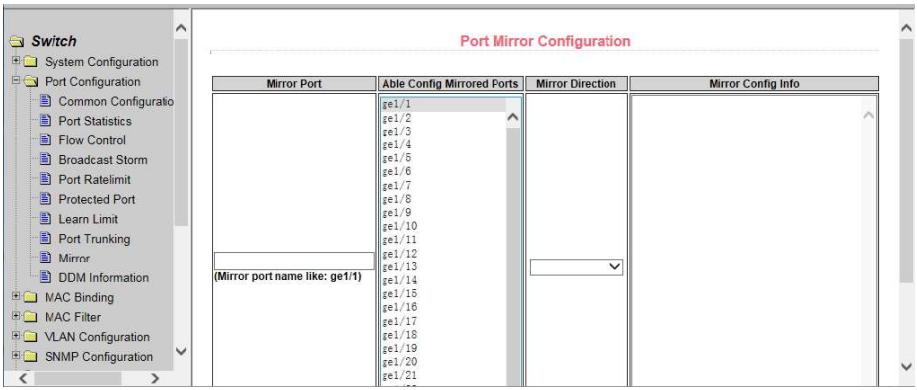
В процессе настройки, по крайней мере один trunk должен быть установлен, чтобы Polymerization Settings вступили в силу. Выбранные методы создания Trunk'ов применяются ко всем группам.

Коммутатор позволяет использовать три метода создания trunk'ов:

- Метод, основанный на исходном MAC адресе;
- Метод, основанный на MAC адресе назначения;
- Метод, основанный как на исходном MAC, так и на MAC адресе назначения.

Коммутатор поддерживает максимум 3 группы trunk'ов. Trunk1 и Trunk2 не могут создавать trunk из гигабитных портов. Trunk3 может объединять максимум 2 гигабитных порта. Метод агрегирования общий для всех trunk'ов.

5.4.9 Port mirror configuration (Зеркалирование портов)

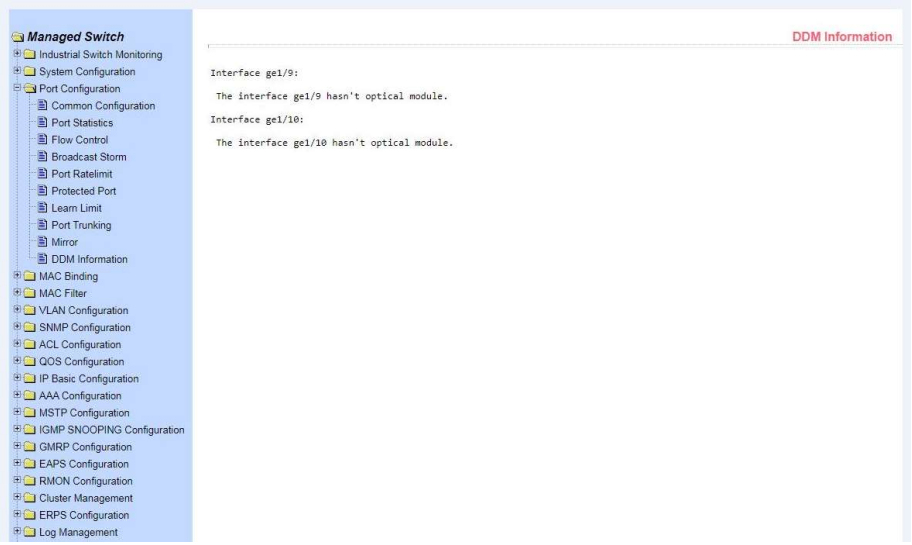


На данной странице представлены возможности для зеркалирования (mirroring) портов. Выбирается один порт (Mirror Port) который будет дублировать трафик других портов, указанных в настройках зеркалирования.

Выберите порт (порт-зеркало), который будет дублировать трафик других портов;

- Выберите порты, трафик которых будет дублироваться на порт-зеркало;
- Выберите, какие именно пакеты будут дублироваться на порт-зеркало в выпадающем меню Mirror Direction (RECEIVE – получаемые пакеты, TRANSMIT – отправляемые пакеты, BOTH – получаемые и отправляемые пакеты, NOT_RECEIVE – отменяет дублирование получаемых пакетов на порт-зеркало, NOT_TRANSMIT – отменяет дублирование отправляемых пакетов на порт-зеркало, NEITHER – отменяет дублирование каких либо пакетов на порт-зеркало);
- Результаты будут отображены в поле Mirror Config Info

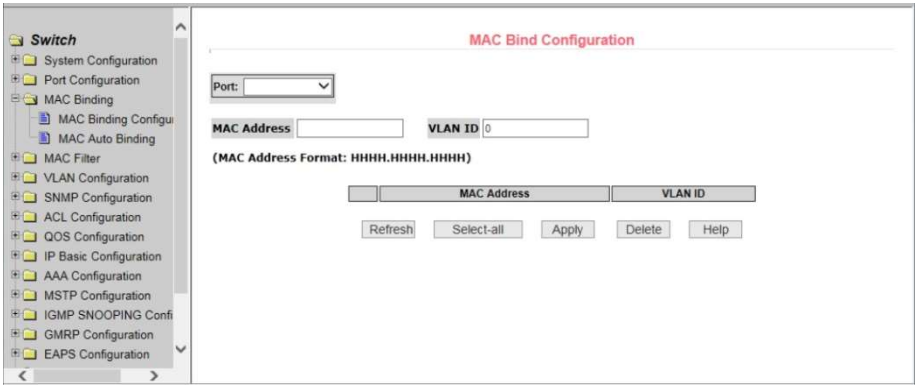
5.4.10 DDM information (Информация о подключённых SFP модулях)



На этой странице представлена информация о таких параметрах работы SFP модулей как напряжение питания, температура модуля, ток смещения и мощность лазера, уровень принимаемого сигнала. Данные параметры позволяют определить состояние линии в целом. (*Используемые SFP модули должны поддерживать эту функцию.*)

5.5 MAC binding (привязка MAC адреса)

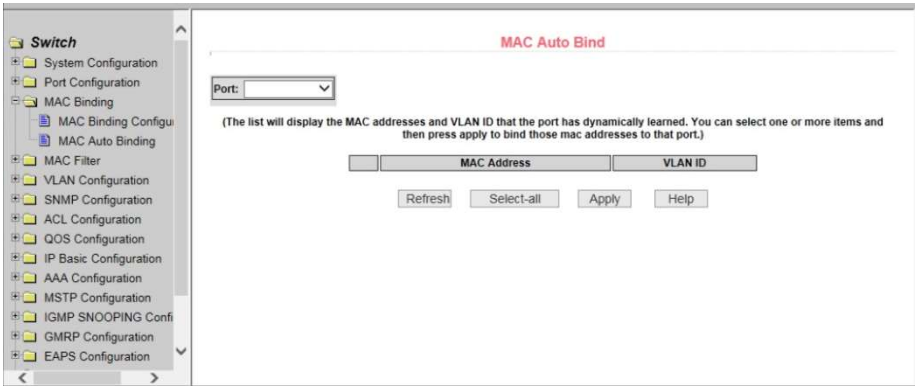
5.5.1 MAC binding configuration (Настройка привязки MAC адресов)



Данная страница предоставляет возможность привязки MAC адреса к порту (MAC Adress) или к VLAN (VLAN ID).

Все изменения на странице подтверждаются кнопкой Apply (Принять), если привязку необходимо удалить используйте кнопку Delete (Удалить), кнопка Select all (выбрать все) позволит удалить сразу все привязки, настроенные ранее.

5.5.2 MAC Auto Bind (Автоматическая привязка MAC адресов)

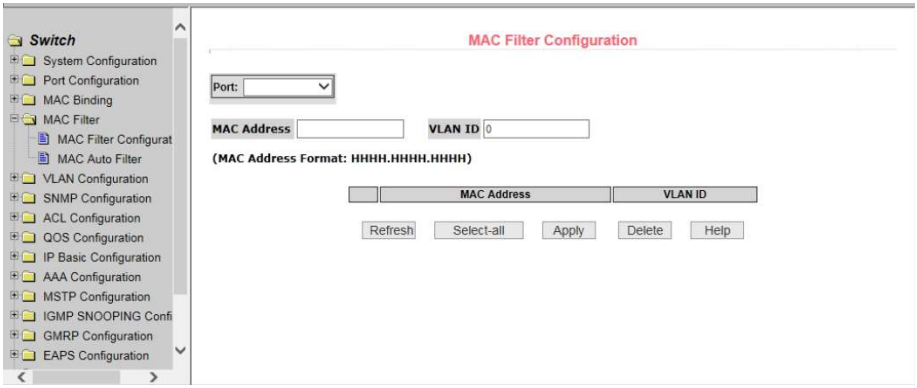


На данной странице находятся данные об автоматической привязке MAC адресов к портам. Показана динамическая привязка MAC адресов к портам (MAC которые были занесены в таблицу MAC адресов коммутатора), а также к VLAN относящимся к этим портам. Вы можете выбрать одну из динамических привязок и конвертировать ее в постоянную привязку (static binding).

Все настройки на данной странице подтверждаются кнопкой Apply (принять), если запись необходимо удалить используйте кнопку Delete (Удалить), кнопка Select all (выбрать все) позволит удалить сразу все записи.

5.6 MAC Filter (Фильтр MAC адресов)

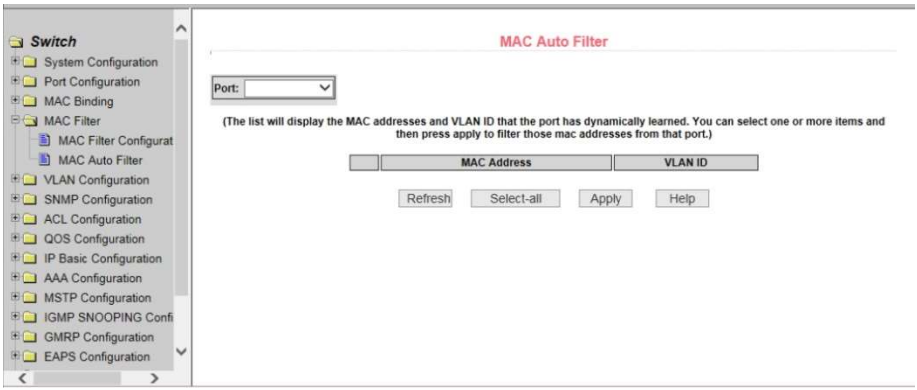
5.6.1 MAC Filter Configuration (Настройка фильтра MAC адресов)



Настройки на этой странице позволяют фильтрацию MAC адресов для портов. Записи с MAC адресами на этой странице используются для входа в фильтр MAC адресов, а VLAN ID используется для фильтрации MAC адреса соответствующей VLAN.

Все настройки на данной странице подтверждаются кнопкой Apply (принять), если запись необходимо удалить используйте кнопку Delete (Удалить), кнопка Select all (выбрать все) позволит удалить сразу все записи.

5.6.2 MAC Auto Filter (Автоматический фильтр MAC адресов)



Здесь представлены данные об автоматической конверсии MAC адресов.

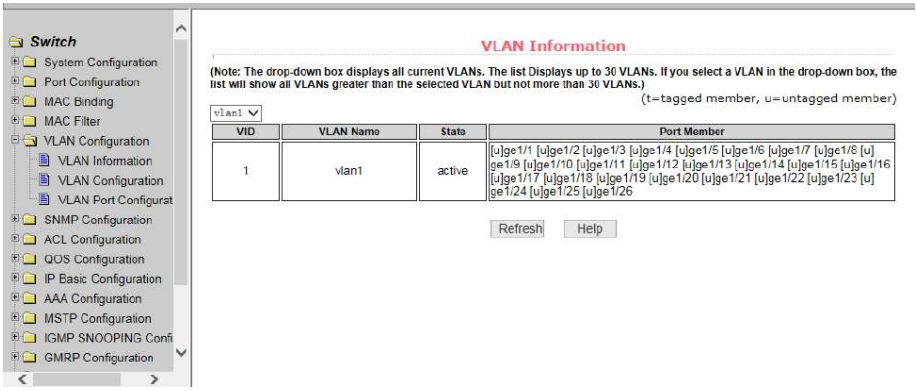
Показана динамическая привязка MAC адресов к портам (MAC которые были занесены в таблицу MAC адресов коммутатора), а также к VLAN относящимся к этим портам.

Вы можете выбрать одну и привязок и конвертировать ее в постоянную привязку (static binding) для фильтра MAC адресов.

Все настройки на данной странице подтверждаются кнопкой Apply (принять), если запись необходимо удалить используйте кнопку Delete (Удалить), кнопка Select all (выбрать все) позволит удалить сразу все записи.

5.7 VLAN Configuration (Настройка VLAN)

5.7.1 VLAN information (Информация о VLAN)

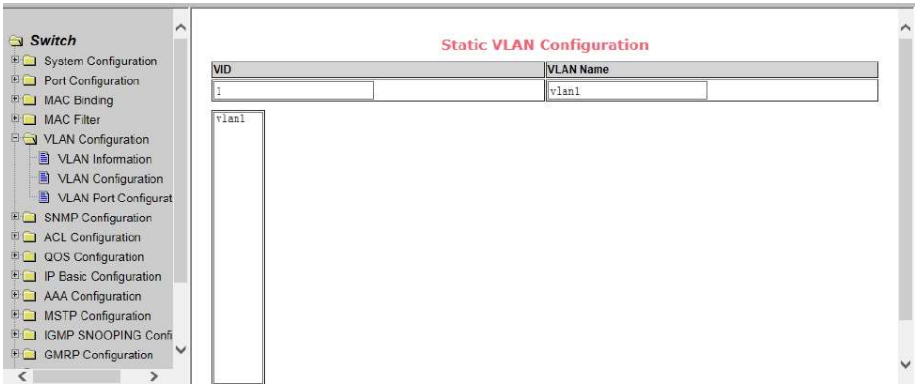


На этой странице представлена информация о существующих VLAN. Данные предоставлены только для чтения и не могут быть изменены.

Информация о текущей конфигурации VLAN выбирается в выпадающем меню в левом верхнем углу и включает в себя:

- ✓ VID (VLAN ID);
- ✓ VLAN Name (Имя VLAN);
- ✓ State (состояние активное или неактивное);
- ✓ Port member (порты – участники VLAN, могут включать в себя как тегированные порты (t) и нетегированные (u)).

5.7.2 Static VLAN Configuration (Настройка VLAN)



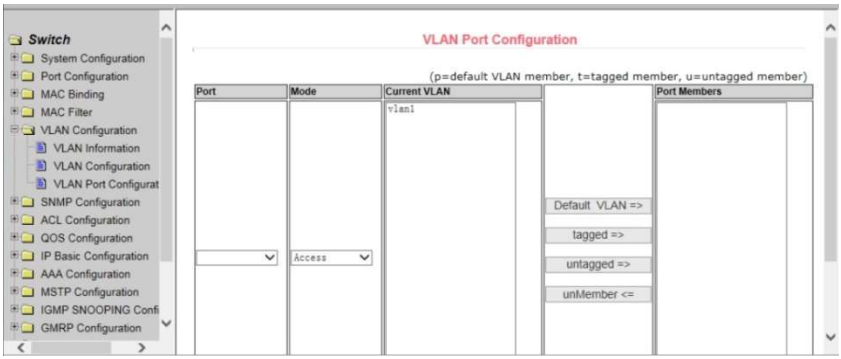
На этой странице вы можете создать VLAN. Для этого задайте VLAN ID в строке VID (от 2 до 4094, значение 1 зарезервировано системой).

Имя в строке VLAN Name задается автоматически и зависит от VLAN ID. Для подтверждения создания VLAN нажмите кнопку Apply (Принять).

В текстовом поле появится созданная VLAN (VLAN ID+ VLAN Name). VLAN1 нельзя изменить или удалить, данное имя зарезервировано системой.

Для удаления созданной ранее VLAN потребуется выбрать нужную запись из списка и далее нажать кнопку REMOVE (удалить). Запись из списка также будет удалена.

5.7.3 VLAN Port Configuration (Конфигурация портов VLAN)



На этой странице представлены возможности по конфигурированию портов для VLAN, а также просмотру результатов.

Эта страница с настройками состоит из 8 частей:

- Port (Выбор порта);
- Mode (Режим, в котором порт будет работать в VLAN. Режим Access подразумевает, что порт будет помечен, как untagged (нетегированный) и являться членом VLAN1, Режим Hybrid подразумевает, что порт будет являться членом VLAN1 и будет помечен, как untagged (нетегированный). Режим TRUNK подразумевает, что порт будет являться членом VLAN1 и будет помечен, как tagged (тегированный));
- Current VLAN (имя VLAN. Позволяет выбрать одну или несколько VLAN, к которым будет относится выбранный порт);
- Port Members (порты – участники VLAN);
- Кнопки Default VLAN (добавить запись в VLAN по умолчанию), tagged => (добавить порт как тегированный), untagged => (добавить порт как нетегированный), unMember <= (удалить порт из поля Port Members)

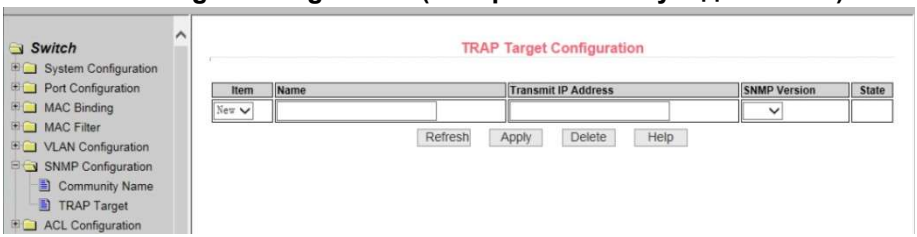
5.8 SNMP Configuration (Настройка SNMP протокола управления)

5.8.1 SNMP Community Configuration (Общие настройки для SNMP)

На этой странице представлены общие настройки для управления коммутатором через SNMP. По умолчанию в коммутаторе создана одна запись Public с правами только на чтение (ReadOnly).

Всего может быть создано 8 записей. Если предполагается управлять коммутатором через SNMP следует создать запись с правами на Чтение/Запись (Read/Write).

5.8.2 TRAP Target Configuration (Настройка TRAP уведомлений)



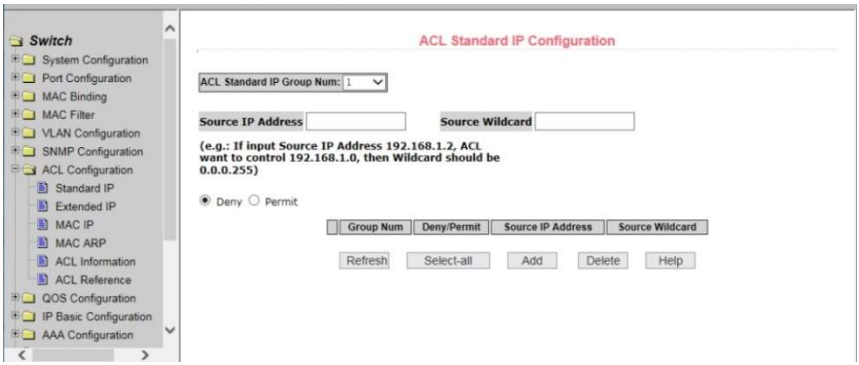
Настройки на данной странице позволяют сконфигурировать получение TRAP сообщений. Для этого необходимо:

- ✓ Выбрать в поле Name имя для получения TRAP сообщений;
- ✓ Выбрать IP адрес (Transmit IP Address), который будет использовать TRAP протокол;
- ✓ Выбрать версию SNMP (SNMP Version);

Когда все настройки будут произведены успешно в строке состояния (State) появится Active. Теперь коммутатор сможет пересылать TRAP сообщения на указанный IP адрес.

5.9 ACL Configuration (Настройка Access Control List)

5.9.1 ACL Standard IP Configuration (Настройка ACL для IP)



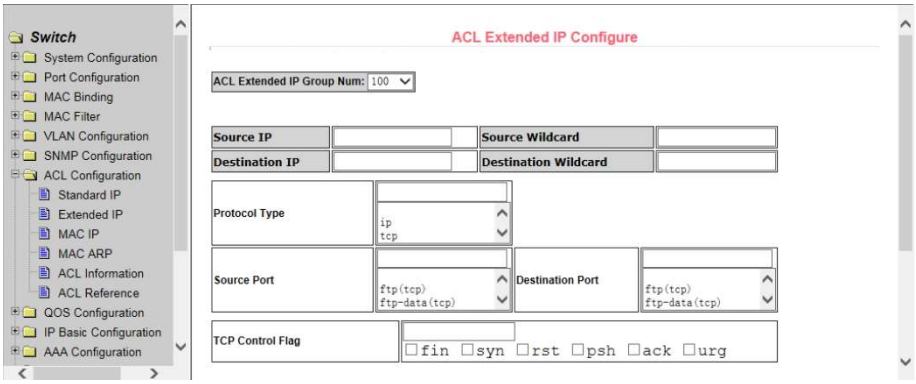
Здесь представлены настройки ACL для IP протокола. Пользователь может задать самостоятельно ACL базу с правилами для IP адресов. Стандартные правила контролируют перенаправление исходных IP пакетов.

Пользователь может настраивать правила, исходный IP адрес должен быть указан с маской, правило может совпадать с набором IP адресов. Каждое правило должно содержать параметр фильтрации: запретить (deny) или разрешить (allow).

Пользователь может создавать правило в группе, имя для правила автоматически задается. При удалении одного правила остальные правила не изменяются.

Для удаления всех правил сразу используйте кнопку Select all (выбрать все), а затем кнопку Delete (удалить).

5.9.2 ACL Extended IP (Расширенная настройка ACL правил для IP)

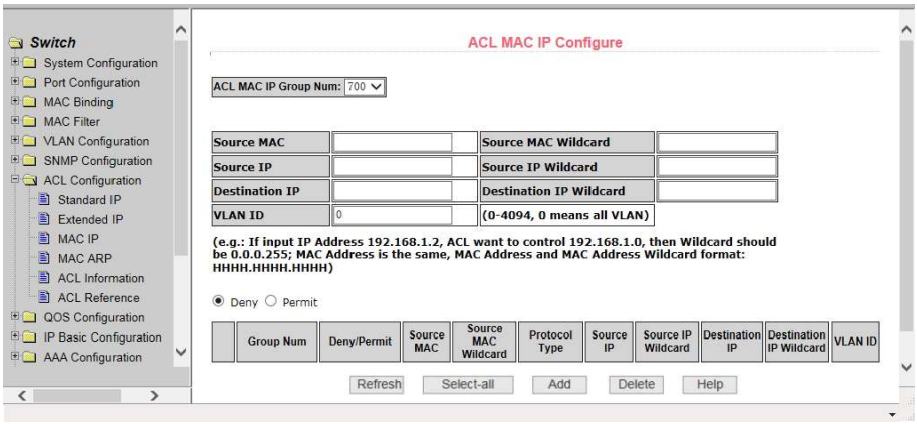


Здесь представлена возможность для создания ACL правил с расширенными настройками IP адресов. Контроль пересылки пакетов через исходный IP адрес, адрес назначения, тип протокола, служебный порт.

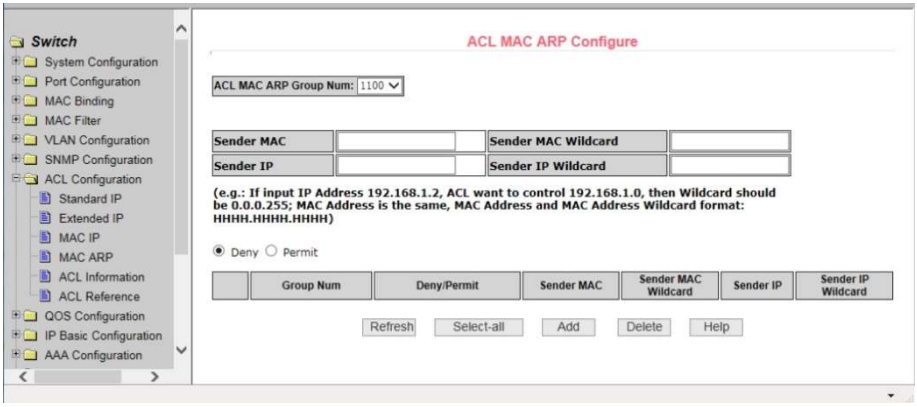
5.9.3 ACL Configuration (Настройка ACL правил с помощью MAC)

Здесь представлены настройки ACL правил для группы IP адресов, связанными с MAC адресами. Правила могут быть созданы на основе исходного IP адреса, исходного MAC адреса, а также IP адреса назначения.

Все настройки на данной странице подтверждаются кнопкой *Apply* (принять), если запись необходимо удалить используйте кнопку *Delete* (Удалить), кнопка *Select all* (выбрать все) позволит удалить сразу все записи.



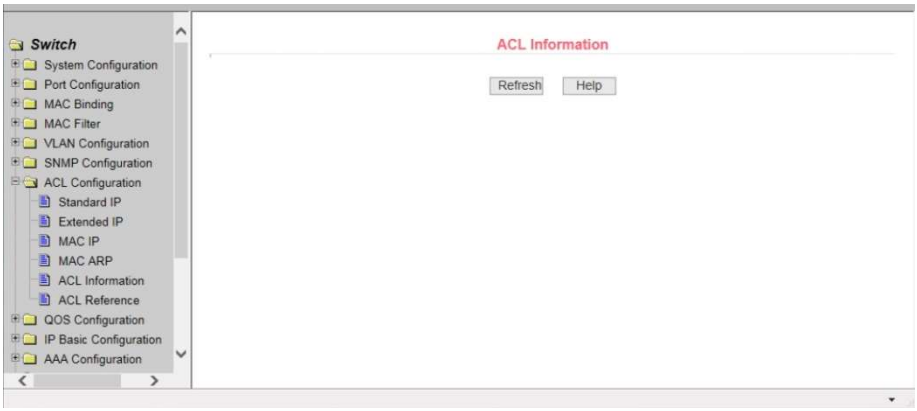
5.9.4 ACL MAC ARP Configure (Настройка ACL правил для ARP с помощью MAC адресов)



На этой странице представлены настройки ACL правил для ARP пакетов с помощью MAC адресов. Правила могут быть созданы на основе IP адреса отправителя, MAC адреса отправителя.

Все настройки на данной странице подтверждаются кнопкой Apply (принять), если запись необходимо удалить используйте кнопку Delete (Удалить), кнопка Select all (выбрать все) позволит удалить сразу все записи.

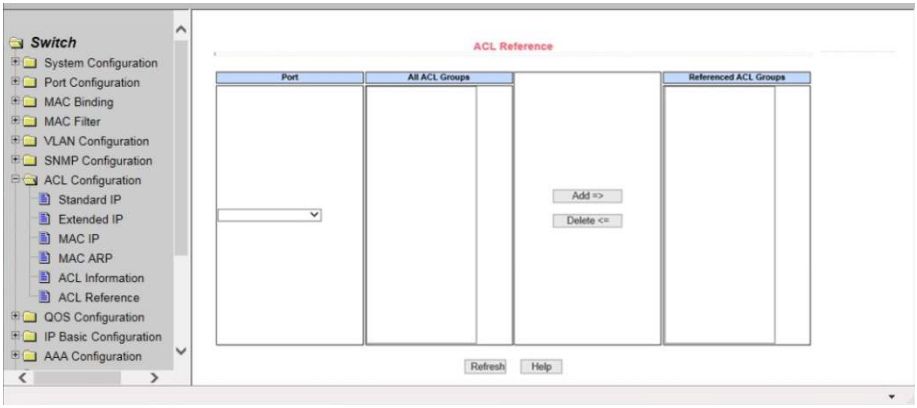
5.9.5 ACL information (Набор действующих ACL правил)



На данной странице отображены действующие в текущий момент ACL правила.

Информация представлена только для чтения и может быть обновлена кнопкой Refresh (обновить).

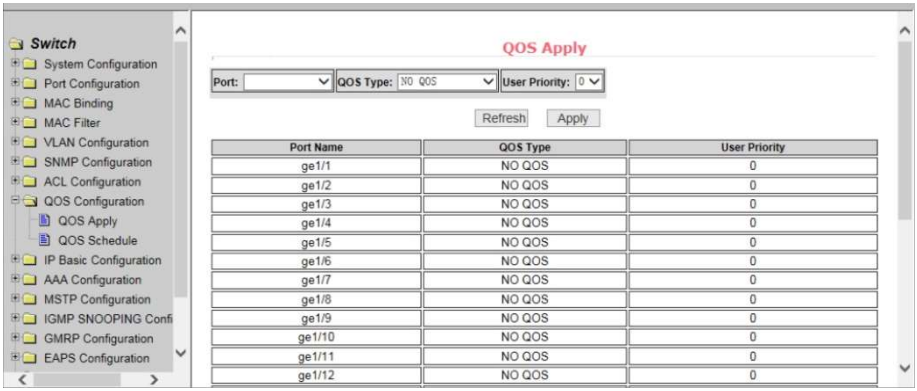
5.9.6 ACL reference configuration (Настройка ACL правил)



На этой странице представлены настройки ACL правил для фильтрации пакетов, получаемых портами. Выберите порт, выберите ALC группу из списка и нажмите *Add*=>. Для удаления выберите ALC группу из списка добавленных и нажмите *Delete*<=.

5.10 QoS Configuration (Настройка предоставления трафика с разным приоритетом)

5.10.1 QoS Apply (Настройка приоритетов трафика для портов)



На этой странице находятся основные настройки QoS. Вы можете выбрать порт в выпадающем меню PORT, затем QoS режим (QOS Type) для него (вкл/выкл) и приоритет трафика (User Priority).

По умолчанию QoS отключен на всех портах а приоритет трафика нулевой.

Все настройки на данной странице подтверждаются кнопкой Apply (принять).

Чтобы обновить значения полей нажмите кнопку Refresh.

5.10.2 QoS Schedule Configuration (Настройка расписания применения QoS)

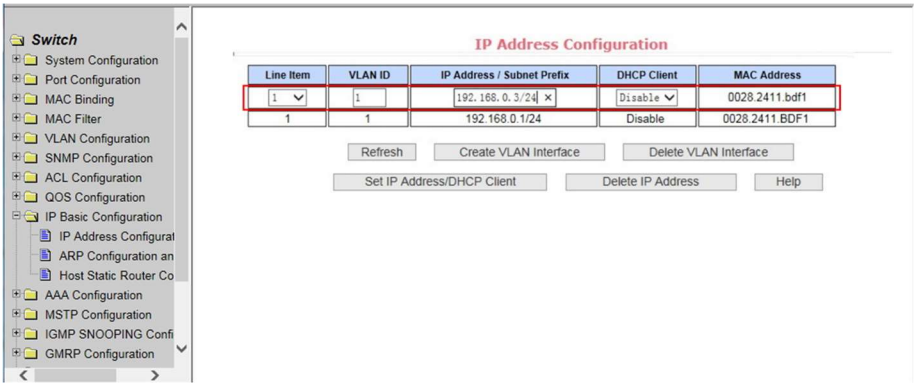
На этой странице WEB интерфейса представлены настройки позволяющие применять QoS приоритезацию трафика по расписанию.

Все настройки на данной странице подтверждаются кнопкой Apply (принять).

Чтобы обновить значения полей нажмите кнопку Refresh.

5.11 IP Basic Configuration (Базовая настройка IP)

5.11.1 IP Address Configuration (Настройка IP адреса коммутатора)



Для изменения IP адреса:

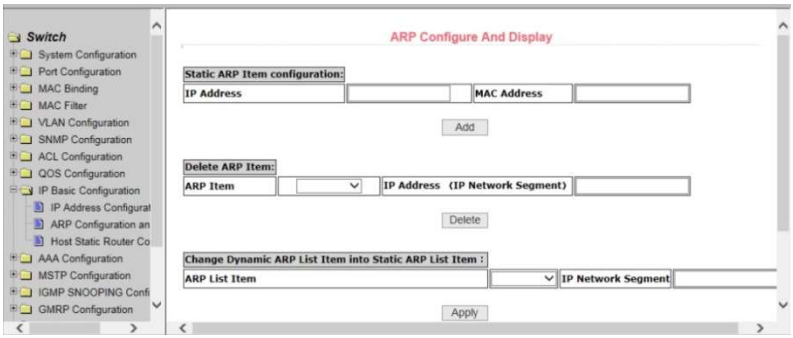
- установите *Line Item* «1», *DHCP Client* «Disable»;
- введите новый адрес в поле *IP Address/Subnet Prefix* (адрес должен быть уникальным и не должен повторяться);
- нажмите *Set IP Address/DHCP Client* (установить адрес), ***старый IP адрес автоматически перестанет действовать;***
- ***Выполните повторный вход в WEB интерфейс, используя новый IP адрес.***

Для сохранения нового IP адреса в энергонезависимой памяти коммутатора в разделе **11.3.7** Current Configuration (Просмотр текущей конфигурации) сохраните настройки, в противном случае при перезагрузке коммутатора будет установлен предыдущий IP адрес.

Также на этой странице находятся настройки VLAN интерфейса. Вы можете создать VLAN интерфейс, удалить его, изменить. Существующие VLAN интерфейсы могут быть настроены только если заданы остальные параметры такие как IP адрес, маска, и MAC адрес.

Коммутатор по умолчанию имеет VLAN1 интерфейс, который не может быть удален.

5.11.2 ARP configuration and Display (Настройка протокола ARP и отображение таблицы ARP)



Страница настроек ARP предоставляет возможность отображать всю таблицу ARP коммутатора, менять Static ARP, удалять ARP, менять Dynamic ARP на Static ARP.

При настройке static ARP необходимо указать IP адрес и MAC адрес. MAC адрес должен быть типа unicast. После этого нажмите кнопку Add (добавить).

При удалении ARP вы можете выбрать, что именно удалить:

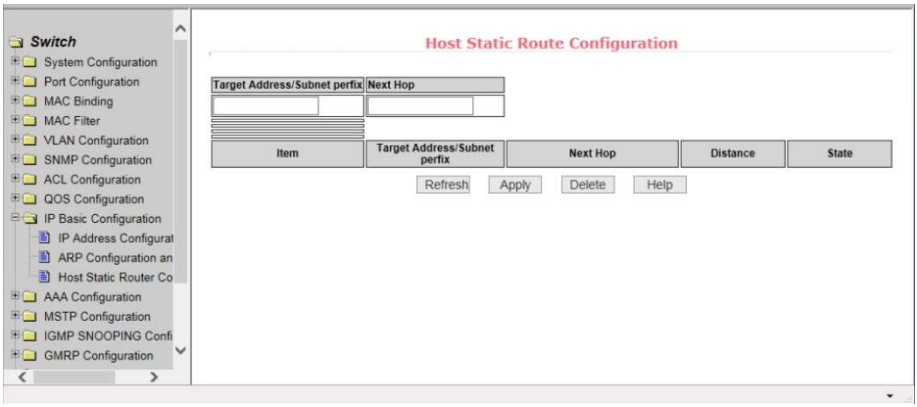
- ✓ Часть записи в ARP таблице коммутатора (для этого необходимо указать IP адрес или IP сегмента сети);
- ✓ Static ARP из таблицы;
- ✓ Dynamic ARP из таблицы.

Для подтверждения удаления используйте кнопку Delete (Удалить).

При переносе Dynamic ARP в Static ARP вы можете выбрать какой-либо сегмент сети или все Dynamic ARP записи в таблице. Для первого случая следует указать IP адрес сегмента сети.

Все настройки на данной странице подтверждаются кнопкой Apply (принять).

5.11.3 Host Static Route Configuration (Настройка таблицы Static маршрутизации)

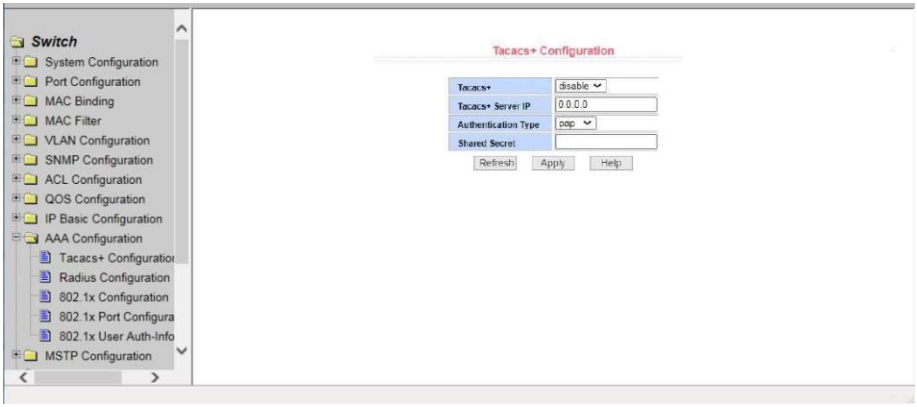


Вы можете добавлять и удалять записи в таблицу Static маршрутизации с помощью настроек на этой странице WEB-интерфейса. По умолчанию коммутатор не имеет каких-либо записей в таблице маршрутизации. Чтобы настроить маршрутизацию по умолчанию необходимо добавить 0.0.0.0 / 0 запись в таблицу.

Все настройки на данной странице подтверждаются кнопкой Apply (принять).

5.12 AAA Configuration (настройка системы аутентификации авторизации и учета событий)

5.12.1 Tacacs+ configuration (настройка протокола Tacacs+)



На этой странице WEB интерфейса представлены настройки TACACS + (Terminal Access Controller Access Control System plus) — сеансовый протокол, разработанного Cisco.

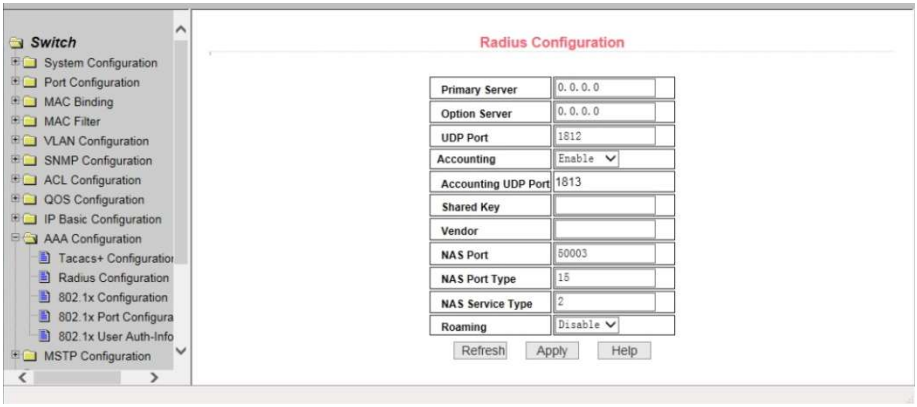
Улучшена безопасность протокола (шифрование), а также введено разделение функций аутентификации, авторизации и учёта, которые теперь можно использовать по отдельности.

- ✓ **Tacacs+** (disable/enable) – глобальное вкл/выкл протокола Tacacs+
- ✓ **Tacacs+ Server IP** – IP адрес сервера Tacacs+
- ✓ **Authentication Type** – типа аутентификации на сервере.
- ✓ **Shared Secret** – ключ для шифрования/дешифрования пакетов.

Refresh – обновить страницу.

Apply – сохранить настройки.

5.12.2 Radius Configuration (настройка Radius системы AAA)



На этой странице WEB интерфейса представлены настройки RADIUS (система использующая протокол для реализации аутентификации, авторизации и сбора сведений).

Для корректной работы системы RADIUS необходимо:

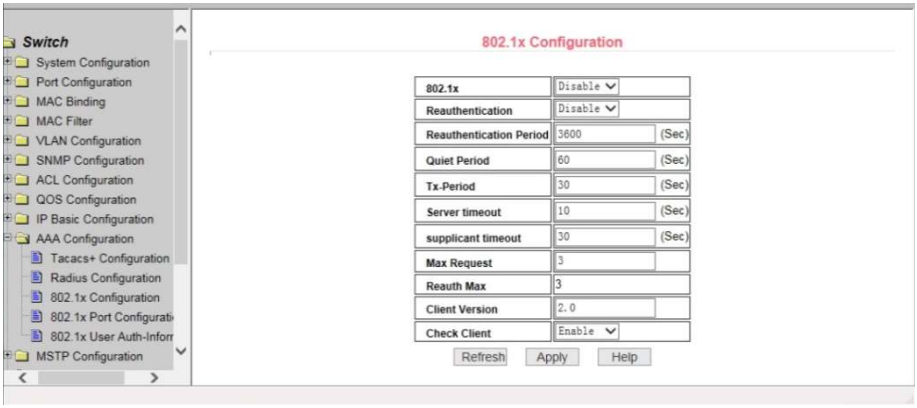
1) Быть уверенным, что IP адрес Radius сервера (Primary Server) задан прежде, чем выполнять аутентификацию и авторизацию;
2) Задать дополнительный IP адрес Radius сервера (Optional Server);
3) Указать UDP порт аутентификации (UDP Port). По умолчанию это значение равно 1812, обычно изменять это поле нет необходимости;
4) Указать следует ли выполнять аутентификацию и учет в целом в поле Accounting (значение Enable – вкл, Disable – откл.);
5) Указать порт выполнения учета (Accounting UDP Port). Значение по умолчанию 1813;
6) Ключ (Shared key) используется для установки общего пароля шифрования между коммутатором и Radius сервером.

Убедитесь, что настройки аутентификации и учета (Accounting) имеют те же значения, что и на сервере Radius;

7) Информация о поставщике (vendor). Обычно, это поле не стоит изменять;
8) NAS Port, NAS port type, NAS type of service. Эти значения не меняются;
9) Roaming отвечает за включение/отключение функции Roaming протокола Radius.

Все настройки на данной странице подтверждаются кнопкой Apply (принять).

5.12.3 802.1x Configuration (Настройка параметров системы авторизации и аутентификации по стандарту 802.1x)



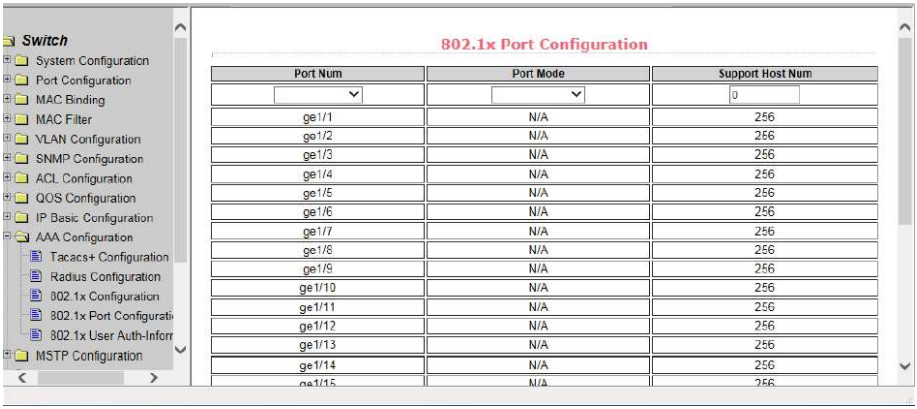
На этой странице WEB интерфейса представлены настройки системы аутентификации и авторизации на основе стандарта 802.1x:

1) 802.1x – включает/выключает (Disable/Enable) применение аутентификации и авторизации по стандарту 802.1x;

2) Reauthentication – включает/выключает (Disable/Enable) повторную аутентификацию. По умолчанию отключено. Включение данной функции сделает аутентификацию пользователей более надежной, но незначительно увеличит сетевой трафик;
3) Reauthentication period – задается время в секундах для повторной аутентификации. Активно только при включенной функции Reauthentication;
4) Quiet Period – время в секундах, не требует изменения;
5) Tx-Period – не требует изменения;
6) Server timeout – не требует изменения;
7) Supplicant timeout – не требует изменения;
8) Max request users – не требует изменения;
9) Reauth Max – отображает максимальное количество повторных аутентификаций;
10) Client Version – отображает текущую версию клиента для удаленной авторизации и аутентификации через 802.1x;
11) Check Client – вкл/выкл проверки прохождения сертификата от клиента.

Все настройки на данной странице подтверждаются кнопкой Apply (принять).

5.12.4 802.1x Port Configuration (Настройка портов для системы авторизации и аутентификации по стандарту 802.1x)



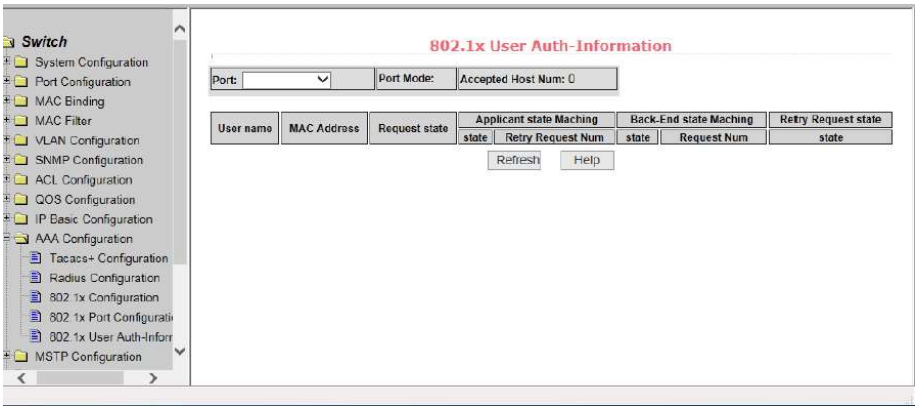
С помощью этой страницы WEB интерфейса пользователь может изменить режим работы порта для работы системы авторизации и аутентификации по стандарту 802.1x. Порт может работать в 4х режимах:

- ✓ N/A State (по умолчанию);
- ✓ Auto state (автоматически);
- ✓ Force-authorized (принудительная авторизация);
- ✓ Force-unauthorized (принудительный отказ от авторизации).

Если на порте требуется выполнять аутентификацию по стандарту 802.1x необходимо выставить режим Auto state. Если не требуется делать аутентификацию для доступа к сети следует выставить режим N/A. Остальные 2 режима редко используются в стандартных ситуациях.

Максимальное значение для пола Support Host Num – 100.

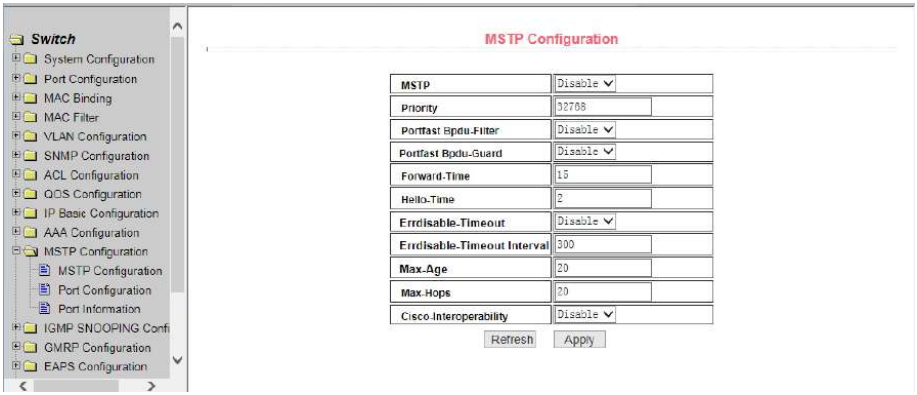
5.12.5 802.1x User Authentication Information (Информация о всех процессах аутентификации по стандарту 802.1x)



На этой странице представлены сведения обо всех процессах аутентификации на портах, настроенных для нее. Информация предоставлена только для чтения. Чтобы обновить информацию нажмите кнопку Refresh.

5.13 MSTP Configuration (Настройка работы протокола STP)

5.13.1 MSTP Configuration (Основные настройки MSTP)



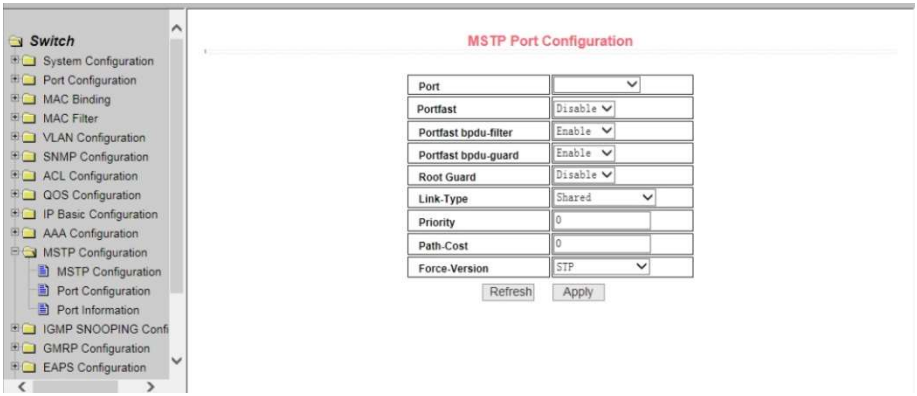
На данной странице WEB интерфейса представлены глобальные настройки протокола MSTP (Multiple Spanning Tree Protocol):

1) MSTP (Disable/Enable) – вкл/выкл поддержку протокола MSTP;
2) Priority – настройка приоритезации. Устройства с более низким приоритетом подходят больше для роли корневого моста(root bridge);
3) Portfast BPDU Filter (Disable/Enable) – вкл/выкл фильтрацию BPDU пакетов на порте;
4) Portfast BPDU Guard (Disable/Enable) – вкл/выкл функцию защиты BPDU пакетов;
5) Forward Time – настройка задержки пересылки пакетов;
6) Hello Time – настройка интервала отправки MSTP HELLO пакетов;
7) Errdisable Timeout (Enable/Disable) – вкл/выкл функции Errdisable. Если порт с включенным BPDU Guard получает пакеты BPDU запускается Errdisable таймер. По истечении заданного времени (Errdisable timeout) порт будет перезапущен;

8) Errdisable timeout – время после которого будет перезапущен порт получивший пакет BPDU;
9) Max Age – время в секундах в течение которого коммутатор ожидает информацию о конфигурации ST(spanning tree) прежде чем запустить процесс конфигурации заново;
10) Max Hops – количество переходов (хопов) до отбрасывания BPDU пакетов в домене;
11) CISCO Interoperability (Enable/Disable) – вкл/выкл совместимость с настройками STP CISCO.

Все настройки на данной странице подтверждаются кнопкой Apply (принять).

5.13.2 Port configuration (настройка MSTP на портах)



На данной странице WEB интерфейса представлены настройки MSTP (Multiple Spanning Tree Protocol) для портов.

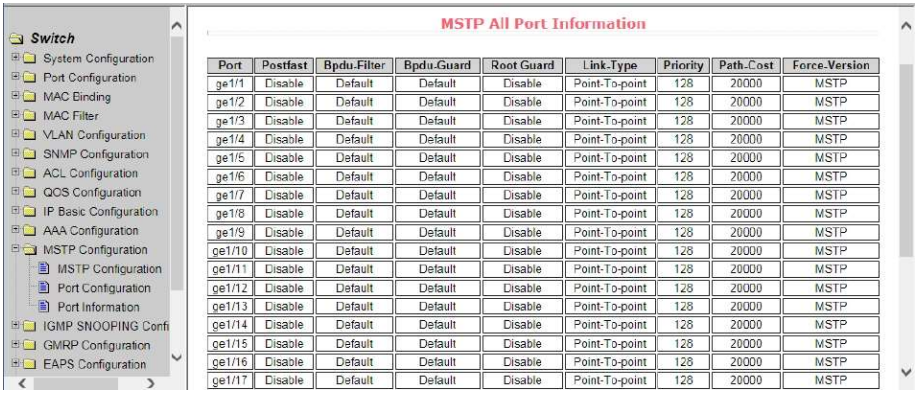
1) Port – выбор порта для настройки;
2) Portfast (Enable/Disable) – вкл/выкл состояния Portfast для выбранного ранее порта. В состоянии Portfast порт переходит из

состояния блокировки в состояние пересылки(forward) пакетов минуя состояние обучения(learning) и прослушивания (listening);

3) Portfast BPDU filter (Enable/Disable) – вкл/выкл фильтрацию BPDU пакетов на выбранном порте;
4) Portfast BPDU GUARD (Enable/Disable) – вкл/выкл функцию защиты BPDU пакетов на выбранном порте;
5) Root Guard (Enable/Disable) – вкл/выкл функции защиты корневого моста (root bridge) от приема BPDU пакетов от устройств с более высоким приоритетом, чем мост;
6) Link Type – настройка типа подключения. Point to Point (точка-точка) позволяет быстро менять состояние порта. Shared подключение не позволяет быстро менять состояние порта. Необходимо пройти 802.1D процедуры, чтобы определить статус порта;
7) Priority – настройка CIST приоритета, значение может быть только кратным 16 в диапазоне от 0-240. По умолчанию значение равно 128;
8) Path Cost – от 0 - 200000000. Более низкие значения обычно соответствуют root'ам;
9) Force Version – тип отправляемых пакетов.

Все настройки на данной странице подтверждаются кнопкой Apply (принять).

5.13.3 Port information (Общая информация о конфигурации MSTP)



Port	Postfast	Bpdu-Filter	Bpdu-Guard	Root Guard	Link-Type	Priority	Path-Cost	Force-Version
ge1/1	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/2	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/3	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/4	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/5	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/6	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/7	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/8	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/9	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/10	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/11	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/12	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/13	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/14	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/15	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/16	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/17	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP

На данной странице WEB интерфейса представлена сводная информация о конфигурации MSTP.

Информация предоставлена только для чтения.

5.14 IGMP Snooping configuration (Настройка отслеживания IGMP трафика)

5.14.1 IGMP Snooping configuration (Настройки функции IGMP snooping)

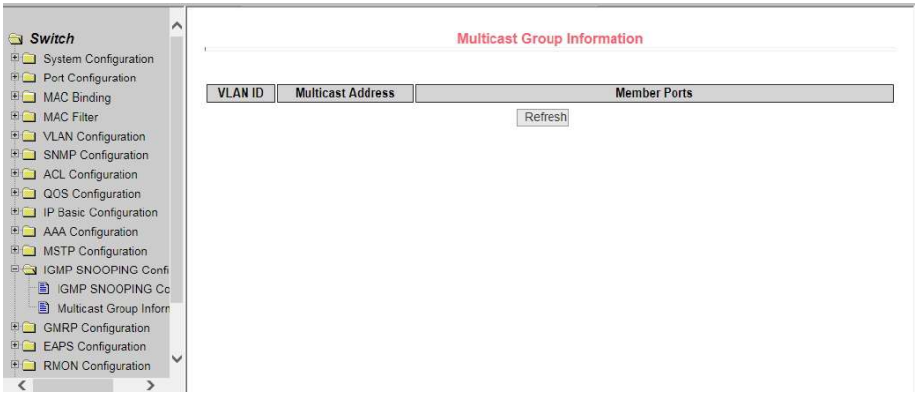
На данной странице WEB интерфейса вы можете глобально включить или выключить (Enable/Disable) функцию IGMP snooping (процесс отслеживания сетевого трафика IGMP, предотвращающий широковещательную (broadcast) ретрансляцию multicast трафика компьютерам-потребителям, которым не нужно его обрабатывать).

Включение данного протокола является обязательным при передаче трафика от большого количества передатчиков большому количеству приемников (HDMI по Ethernet). Рекомендуется также включить IGMP для VLAN

Все настройки на данной странице подтверждаются кнопкой Apply (принять).

С помощью кнопки Refresh можно обновить значения полей.

5.14.2 Multicast Group Information (Общая информация о IGMP)



На данной странице WEB интерфейса представлена общая информация о Multicast группах созданных в процессе работы протокола IGMP.

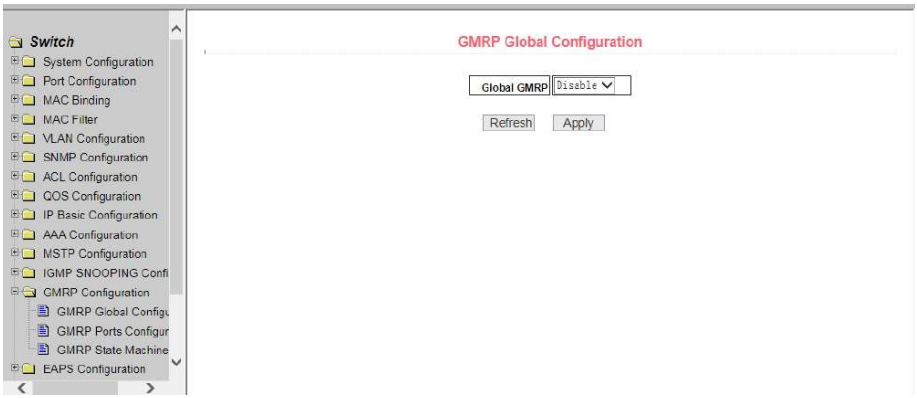
Информация предоставлена только для чтения и обновления (Refresh)

5.15 GMRP Configuration (Настройка работы протокола GMRP)

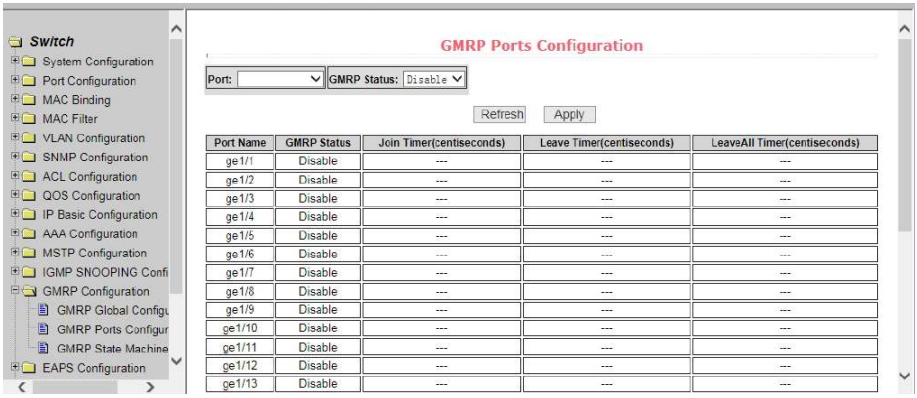
5.15.1 GMRP Global Configuration (Глобальные настройки GMRP)

На данной странице WEB интерфейса представлены глобальные настройки работы протокола GMRP (GARP Multicast Registration Protocol), предназначенного для упрощения распространения по сети информации о наличии определенной Multicast группы.

Включение/отключение поддержки GMRP осуществляется с помощью выбора Disable/Enable и последующего подтверждения кнопкой Apply (принять).



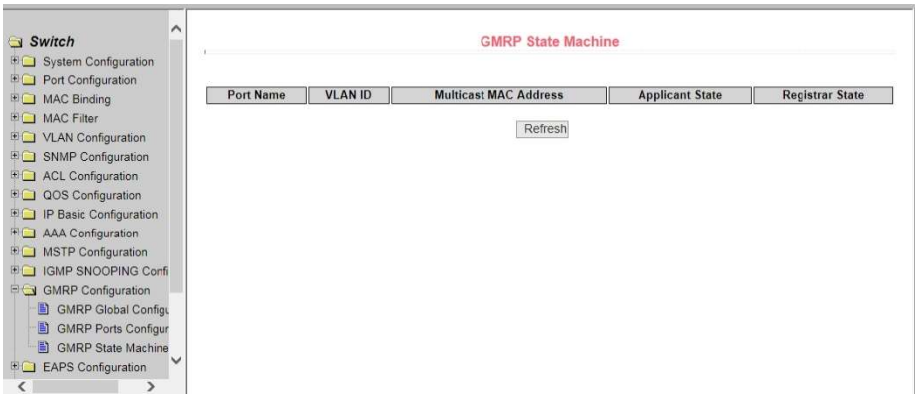
5.15.2 GMRP ports configuration (Настройка GMRP на портах)



На данной странице WEB интерфейса представлены настройки GMRP для отдельных портов. Порт выбирается в выпадающем меню Port, вкл/откл поддержки GMRP реализуется с помощью GMRP Status Disable/Enable.

Все настройки на данной странице подтверждаются кнопкой Apply (принять).

5.15.3 GMRP State machine (Общая информация о GMRP)



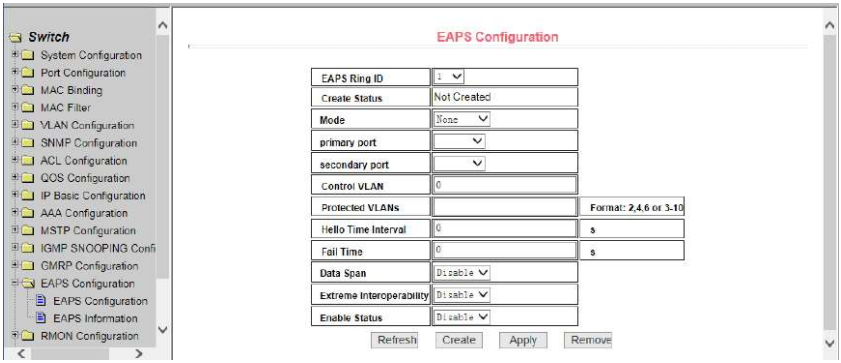
На данной странице WEB интерфейса находится сводная информация о работе протокола GMRP. Номер порта, VLAN ID, MAC адрес multicast группы и тд.

Информация предоставлена только для чтения.

Refresh – обновить содержание таблицы.

5.16 EAPS Configuration (Настройка работы протокола EAPS)

5.16.1 EAPS Configuration (Основные настройки работы протокола EAPS)

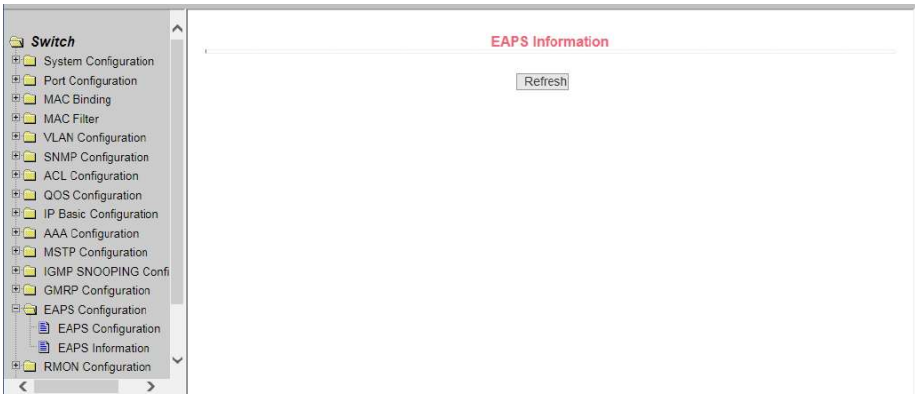


На данной странице WEB интерфейса представлены настройки протокола EAPS (Ethernet Automatic Protection Switching), предназначенного для защиты от петель в сети.

1) EAPS Ring ID – выбор ID для EAPS ring;
2) Mode – настройка режима работы рабочего узла для EAPS домена;
3) Primary Port – выбор ключевого порта для EAPS;
4) Secondary Port – выбор вторичного порта для EAPS;
5) Control VLAN – выбор VLAN ID для EAPS;
6) Protected VLANs – выбор одного или нескольких защищаемых VLAN в домене EAPS;
7) Hello Time Interval – настройка EAPS домена для периодической отправки пакетов HEALTH. Задаваемое значение в секундах должно быть меньше чем время до ошибки (fail time);
8) Fail Time – время до истечения срока действия в EAPS домене. Должно быть больше, чем Hello Time;
9) Extreme Interoperability (enable/disable) – вкл/выкл совместимость с extreme устройствами.

Все настройки на данной странице подтверждаются кнопкой Apply (принять).

5.16.2 EAPS information (Сводная информация о работе протокола EAPS)



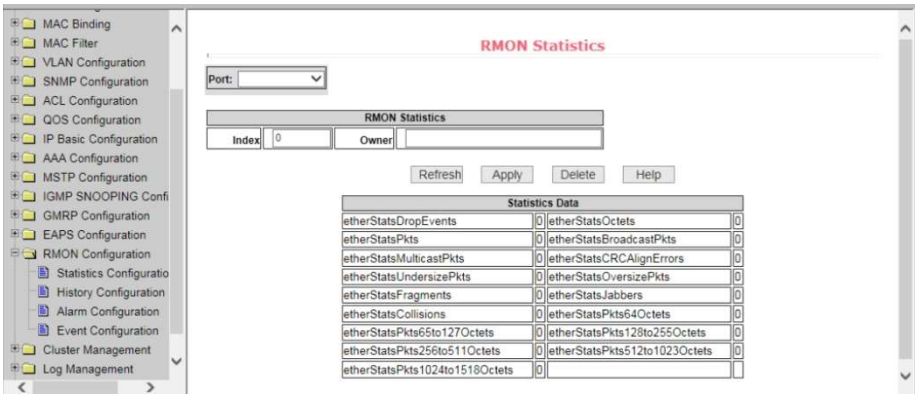
На данной странице WEB интерфейса представлены общие сведения о работе протокола EAPS.

Информация представлена только для чтения и не может быть изменена с этой страницы.

Refresh – обновить содержание страницы.

5.17 RMON Configuration (Настройка работы протокола RMON)

5.17.1 RMON statistics (Настройка групп статистики для RMON)

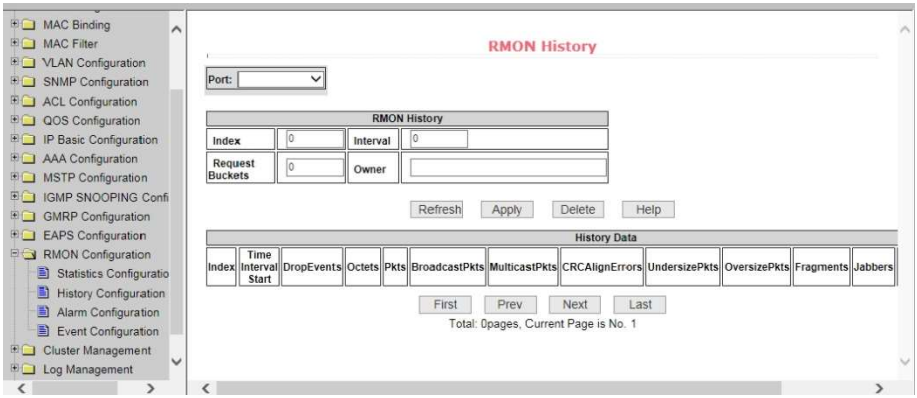


На данной странице WEB интерфейса представлены настройки групп статистики (Statistics) для работы RMON (дистанционный мониторинг сети).

Выберите порт из выпадающего списка Port, чтобы настроить группы данных статистики. Индекс 0 означает, что порт не сконфигурирован для RMON. Индекс может быть в пределах от 1-100. Заполнение поля Owner (владелец) не является обязательным.

Нажмите Apply для подтверждения. В таблице Statistics Data будет показана статистика работы порта.

5.17.2 History Configuration (Настройка групп предыстории для RMON)



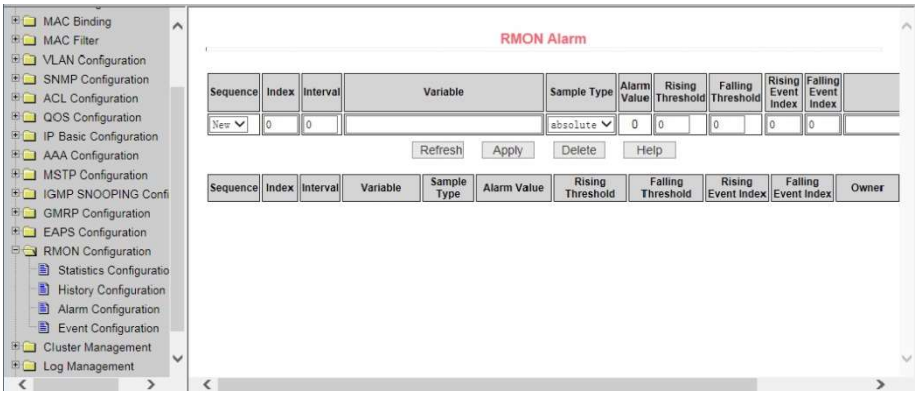
На данной странице WEB интерфейса представлены настройки групп предыстории (History) для работы RMON (дистанционный мониторинг сети).

Выберите порт из выпадающего списка для Port для настройки. Если порт не сконфигурирован для RMON, в поле INDEX отобразится 0. Значение Index может быть в пределах от 1 до 100. Поле владельца (Owner) не обязательно к заполнению.

В поле Interval устанавливается время от 1-3600 в течение которого собираются данные. Bucket – это выделенное хранилище для сбора записей. Значение может быть от 1 – 100.

Нажмите Apply для подтверждения. В таблице *History Data* будет показана история работы порта.

5.17.3 Alarm Configuration (Настройка групп аварийных сигналов)



На данной странице WEB интерфейса представлены настройки групп аварийных сигналов (Alarm) для работы RMON (дистанционный мониторинг сети).

Выберите существующую группу из выпадающего списка для просмотра событий или внесения изменений в настройки.

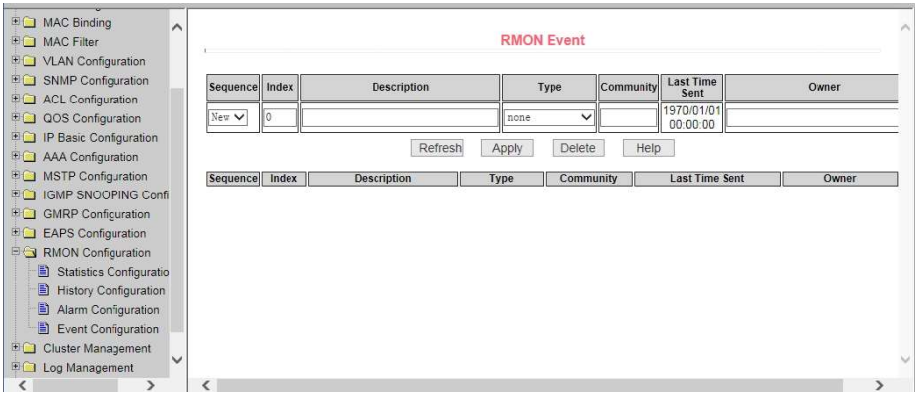
Для создания новой группы выберите New. Index должен находиться в пределах 1…60, Interval должен находиться в пределах 1…3600 (секунды).

Refresh – обновить таблицу.

Apply – сохранить настройки.

Delete – удалить запись из таблицы.

5.17.4 Event Configuration (Настройка групп событий для RMON)



На данной странице WEB интерфейса представлены настройки групп событий (Event) для работы RMON (дистанционный мониторинг сети).

Из выпадающего списка выберите группу событий, чтобы просмотреть или настроить ее. Нажмите (NEW), если хотите создать новую группу.

Диапазон возможных значений в поле Index 1-60. В поле *Description* (описание) задается текстовое описание группы событий. Тип событий может быть none (не реагировать), log (сохранить запись), snmp-trap, log and trap. Поле владельца (owner) заполнять не обязательно.

Поле Last time sent (последнее время отправки) доступно только для чтения и показывает, когда в последний раз событие было отправлено.

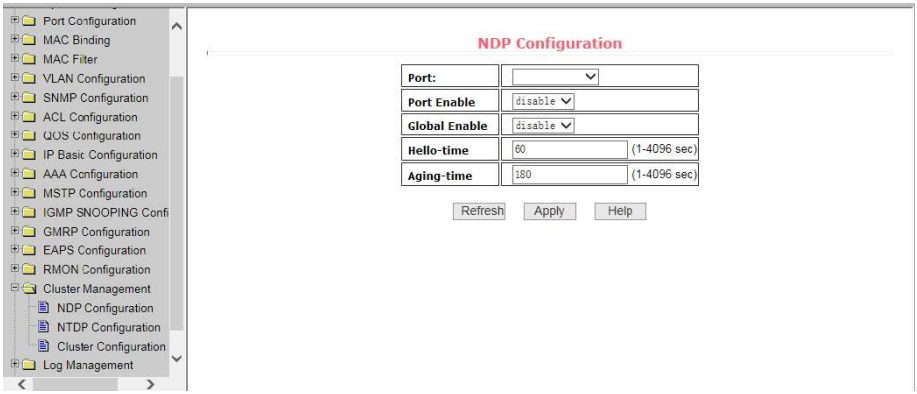
Refresh – обновить таблицу.

Apply – сохранить настройки.

Delete – удалить запись из таблицы.

5.18 Cluster configuration (Настройка кластера)

5.18.1 NDP configuration (Настройка протокола NDP)



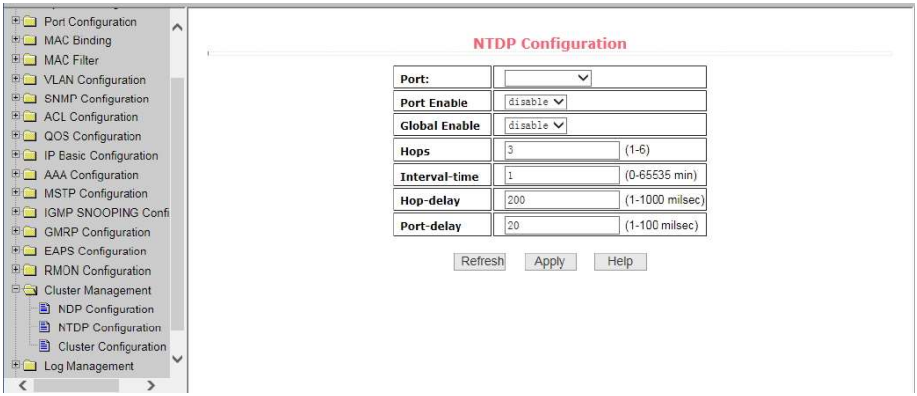
На данной странице WEB интерфейса представлены настройки NDP (Neighbor Discovery Protocol). Данный протокол используется совместно с IPv6 и ответственен за обнаружение конфликта адресов, других узлов в кластере, поиск доступных DNS серверов и т.д.

Доступны следующие настройки:

1) Port – выбор порта;
2) Port Enable (enable/disable) – вкл/выкл поддержки протокола NDP на выбранном порте;
3) Global Enable (enable/disable) – вкл/выкл глобальной поддержки протокола NDP;
4) Hello Time – интервал отправки NDP пакетов, 1-4096 сек, значение по умолчанию 60сек;
5) Aging time – интервал «старения» отправленных NDP пакетов не принятых удаленным устройством, 1-4096 сек, значение по умолчанию 180 сек.

Все настройки на данной странице подтверждаются кнопкой Apply (принять).

5.18.2 NTDP Configuration (Настройка протокола NTDP)



На данной странице WEB интерфейса представлены настройки протокола NTDP (Network Topology Discovery Protocol). Данный протокол используется для построения топологии в кластере.

Доступны следующие настройки:

1) Port – выбор порта;
2) Port Enable (enable/disable) – вкл/выкл поддержки протокола NTDP на выбранном порте;
3) Global Enable (enable/disable) – вкл/выкл глобальной поддержки протокола NTDP;
4) Hops – доступный диапазон топологии 1-6. По умолчанию значение равно 3. Количество переходов (хопов) от самого удаленного устройства до устройства, которое контролирует всю топологию;
5) Interval Time – время сбора топологии в минутах. Значение по умолчанию 1;
6) Hop delay – допустимый интервал задержки между переходами. Доступные значения 1-1000мс. Значение по умолчанию 200мс;

7) Port delay – допустимый интервал задержки перед пересылкой пакетов на первый порт. Доступные значения 1-100мс. Значение по умолчанию 20мс.

Все настройки на данной странице подтверждаются кнопкой Apply (принять).

5.18.3 Cluster Configuration (Настройка кластера)

На данной странице WEB интерфейса представлены настройки для кластера.

Вы можете просмотреть и отредактировать таблицу с участниками кластера.

Возможные настройки включают в себя:

- ✓ Cluster enable (enable/disable) – вкл/выкл кластера;

- ✓ Management VLAN – диапазон доступных VLAN'ов от 1-4094. Значение по умолчанию 1;
- ✓ IP pool – диапазон (пул) IP адресов участников кластера. Доступный диапазон от 0.0.0.0 до 255.255.255.255. Допустимая длина маски 0 до 32;
- ✓ Handshake time – интервал отправки handshake пакетов. Допустимый диапазон значений 1-255. Значение по умолчанию 10;
- ✓ Handshake hold time – время «удерживания». Допустимый диапазон значений 1-255. Значение по умолчанию 60.

Чтобы настроить кластер вам необходимо выбрать имя кластера и выбрать соединение с кластером. Существуют ручные и автоматические методы соединения с кластером.

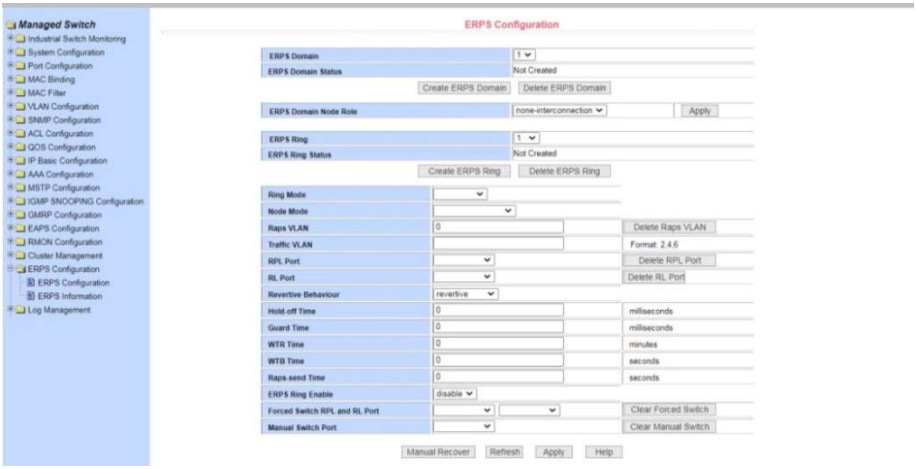
После подтверждения создания кластера вы можете автоматически переключится на ручной метод. Вы не можете в ручную переключится на автоматический метод. Ручной метод позволяет менять имя кластера.

После подтверждения создания кластера устройства – участники кластера и устройства-кандидаты могут быть просмотрены в таблице. Вы можете удалять участников кластера или добавлять устройства-кандидаты согласно списку ролей.

Все настройки на данной странице подтверждаются кнопкой Apply (принять).

11.19 ERPS Configuration (Настройка ERPS)

5.19.1 ERPS Configuration (Настройка протокола ERPS)



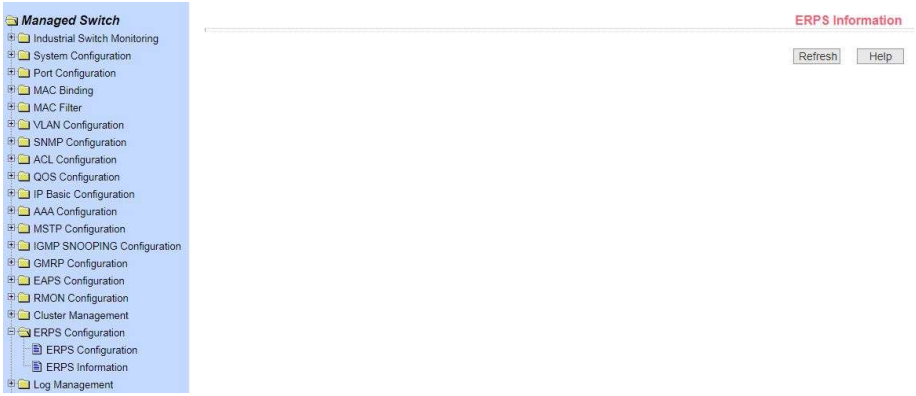
На данной странице WEB интерфейса находятся настройки протокола ERPS – высокоэффективной альтернативе протокола STP (время восстановления линка 50мс). Данный сетевой протокол используется для исключения образования коллизий, при использовании кольцевой топологии подключения.

- ✓ Raps VLAN – VLAN ID, в которой будет передаваться служебный трафик ERPS
- ✓ Traffic VLAN – VLAN ID, которые необходимо защищать от петель и коллизий

Refresh – обновить значения полей.

Apply – сохранить настройки.

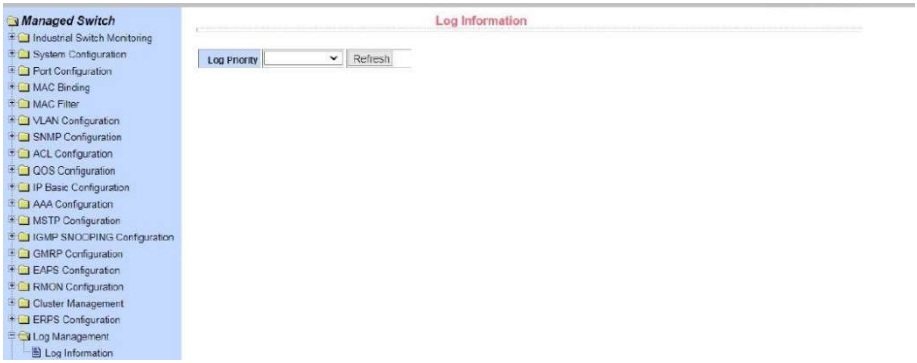
5.19.2 ERPS Information (Информация о работе ERPS)



На данной странице WEB интерфейса находятся сводные данные о результате работы протокола ERPS.

Вся информация доступна только для чтения, чтобы обновить информацию нажмите кнопку Refresh.

5.20 Log management (Управление записью логов)



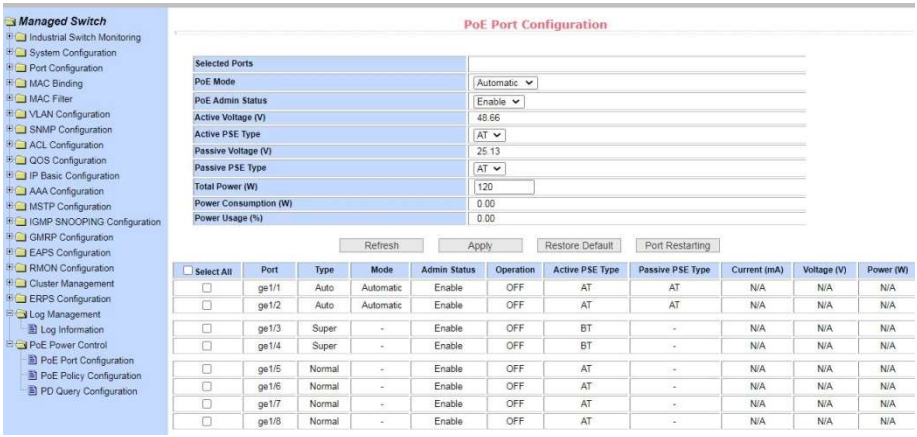
На данной странице WEB интерфейса представлены настройки фильтра вывода записанных логов. В поле Log Priority могут быть следующие значения:

- ✓ Critical – выводить информацию, относящуюся только к критическому уровню важности;
- ✓ Debugging – выводить информацию для отладки;
- ✓ Informational – выводить информацию для отладки и общую информацию в логах;
- ✓ ALL – выводить всю информацию.

Чтобы применить фильтр логов нажмите кнопку Refresh (обновить)

5.21 POE Power Control (Управление параметрами PoE)

5.21.1 POE Port Configuration (Настройка параметров PoE)

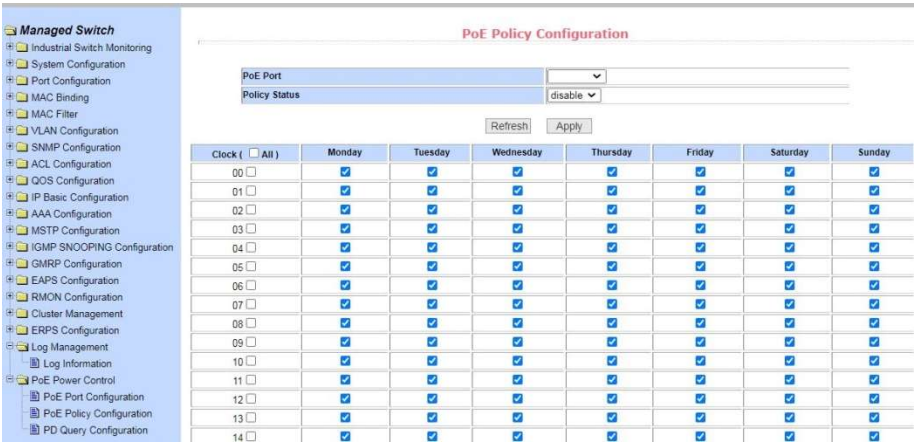


На данной странице WEB интерфейса представлена конфигурация настроек подачи питания к подключенному к коммутатору оборудованию по технологии PoE. Для настройки доступны следующие параметры:

- ✓ Total Power - суммарная мощность PoE. Поле для внесения информации о максимальной мощности используемого БП, информация необходима для автоматического расчета текущей нагрузки PoE коммутатором;
- ✓ PoE single port power - мощность PoE на одном порту;
- ✓ PoE on / off – включение / отключение подачи PoE;

Также на данной странице отражена информация о текущем состоянии PoE оборудования. Имеется возможность обновить (*Refresh*), подтвердить изменения (Apply), вернуться к заводским настройкам (Restore Default), перезапустить порты (Port Restarting).

5.21.2 POE Policy Configuration (Настройка расписания PoE)



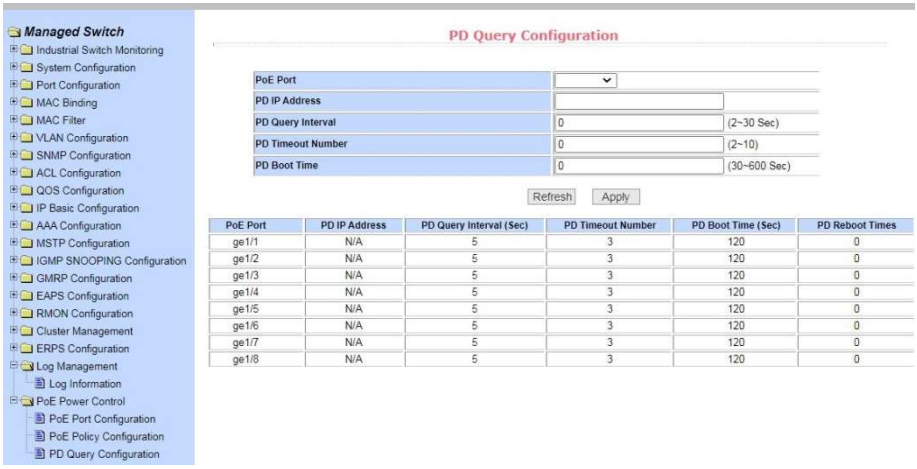
На данной странице WEB интерфейса представлена конфигурация настроек подачи питания PoE к подключенному оборудованию по расписанию. Для настройки расписания доступны следующие параметры:

- ✓ hour – часы;
- ✓ week – дни недели;

Для настройки расписания следует выбрать номер порта из выпадающего меню PoE port, активировать функцию Policy Status включения/отключения (*enable/disable)*; Выбрать время в колонке Clock и день недели Monday…Sunday в соответствующей колонке.

Нажмите Apply для подтверждения, чтобы обновить информацию нажмите кнопку Refresh.

5.21.3 PD Query Configuration (Функция антизависания PoE устройств)



На данной странице WEB интерфейса представлена конфигурация настроек контроля антизависания подключенному к коммутатору PoE оборудования. Для настройки доступны следующие параметры:

- ✓ PoE port – выбор номера порта (из выпадающего списка);
- ✓ PD IP address – IP адрес PoE подключенного оборудования;

- ✓ PD Query Interval – интервал отправки запросов к PoE оборудованию в пределах 2…30 сек (предустановленное время 5 сек);
- ✓ PD Timeout Number – количество запросов к PoE оборудованию, которое может оставаться без ответа в пределах 2…10 (предустановленное значение 3);
- ✓ PD Boot Time – максимальное время для перезагрузки PoE оборудования в пределах 30…600 сек (предустановленное время 120 сек).