ICON INDUSTRIAL ENGINEERING

Icon Industrial Engineering
ООО «Айкон»
ОГРН 1167746579000
ИНН 9701043400

Руководство по настройке индустриальных Layer 2 коммутаторов серии QBIT4000

Версия 2.2

105005, г. Москва, ул. Радио, д. 24, кор. 2, этаж 8, офис 101
+7 (495) 666-29-11
info@iie.ai
www.iie.ai

Отказ от ответственности:

ICON Industrial Engineering (IIE) старается, чтобы содержание данного руководства было как можно более точным и актуальным. Этот документ тем не менее может содержать неточности и ошибки, и мы оставляем за собой право вносить изменения в него без предварительного уведомления.

Все права защищены

Никакая часть этой документации не может быть скопирована, воспроизведена, переведена, распространена публично в любой форме или любым способом без предварительного письменного разрешения ICON Industrial Engineering (IIE).

© 2019-2021 ICON Industrial Engineering (IIE)

ICON Industrial Engineering

Телефон: +7 (495) 666-29-11

Email: support@iie.ai

Сайт: http://www.iie.ai

Оглавление

НАЧАЛО РАБОТЫ 9

Веб-интерфейс 9

Глобальные функции 10

Работа с настраиваемыми таблицами 12

СИСТЕМНЫЕ НАСТРОЙКИ 14

Общая информация о системе 14

Настройки IPv4 (VLAN IP) 15

Настройки IPv6 (VLAN IP) 16

Системное время 17

PRECISION TIME PROTOCOL (PTP) 20

Общие понятия 20

Базовые настройки PTP– Ordinary Clock (OC) 20

Расширенные настройки PTP - Advanced Settings 21

Статус PTP – Master 23

Статус PTP – Slave 24

Базовые настройки PTP - Transparent Clock 25

ПРОТОКОЛЫ СЕМЕЙСТВА SPANNING TREE (RSTP/MSTP) 27

Общие понятия 27

Базовые настройки RSTP/CIST 27

Настройка RSTP портов 29

Статус состояния протокола RSTP 30

Настройки протокола MSTP, параметров MSTI 33

Настройка MSTI портов 34

РЕЗЕРВИРОВАНИЕ ERPS 36

Общие понятия 36

Настройка ERPS резервирования 38

Статус работы ERPS 40

РЕЗЕРВИРОВАНИЕ MRP 43

Общие понятия 43

Настройка параметров MRP 44

Статус работы протокола MRP 46

SNMP-УПРАВЛЕНИЕ **49**

Общие понятия 49

Настройка параметров сервера SNMP 50

Настройка SNMP Trap 52

DHCP **54**

Общие понятия 54

DHCP клиент/сервер *54*

Привязка DHCP адресов *54*

DHCP ретрансляция/Option82 ..... *54*

Настройка DHCP клиента 55

Настройка DHCP сервера 56

Таблица арендованных DHCP адресов 57

Привязка DHCP адресов 57

Настройка DHCP ретрансляции 58

POE (ТОЛЬКО ДЛЯ МОДЕЛЕЙ С ПОДДЕРЖКОЙ POE) **60**

Общие понятия 60

Защита от перегрева *60*

Отладочные коды PoE *60*

Настройка PoE 61

Настройка PoE Keep Alive 62

Настройка расписания работы PoE 63

Настройка приоритета PoE на портах 64

УПРАВЛЕНИЕ ПОРТАМИ **66**

Настройка параметров портов 66

Информация о SFP DDM 68

Подробная информация о порте 70

Информация о состоянии EEE 72

Информация о состоянии портов 73

МУЛЬТИКАСТ, IGMP SNOOPING **75**

Настройка IGMP Snooping 75

Настройка IGMP Snooping Querier 76

Настройка обработки Unknown Multicast 78

Просмотр таблицы IGMP Snooping 79

НАСТРОЙКА VLAN (802.1Q) 80

Общие понятия 80

802.1Q VLAN 80

VLAN Q-in-Q 80

Настройка 802.1Q VLAN 80

Таблица существующих VLAN 81

Настройка режима работы портов VLAN и PVID 82

Настройка VLAN Q-in-Q 83

УПРАВЛЕНИЕ КАЧЕСТВОМ ОБСЛУЖИВАНИЯ (QOS) 85

Базовые настройки QoS 85

Настройка типа классификации трафика и CoS 86

Настройка очередей для поля PRI 87

Настройка очередей для поля DSCP 88

ТРАНКОВЫЕ ПОРТЫ 89

Базовые настройки транков 89

Статус транков 90

УПРАВЛЕНИЕ ТРАФИКОМ (STORM CONTROL) 92

Настройка управления трафиком 92

НАСТРОЙКА ДОСТУПА ПО 802.1X 93

Базовые настройки 802.1X 93

Настройка портов для 802.1X 94

Настройка локальных пользователей 95

Настройка параметров RADIUS сервера 96

МЕТОДЫ УПРАВЛЕНИЯ КОММУТАТОРОМ 97

Настройка методов управления 97

СПИСКИ ДОСТУПА (ACL) 99

Настройка списков доступа 99

Пример использования 100

УПРАВЛЕНИЕ КОММУТАТОРОМ ПО SSH 102

Резервная копия ключа 102

Восстановление ключа 103

Информация о ключе 103

ДИАГНОСТИКА 105

Зеркалирование портов 105

Функция Ping 106

Диагностика кабеля 108

LLDP 109

Настройка LLDP 109

Таблица LLDP соседей 110

Системные события 111

Настройка Syslog 111

Просмотр системных событий 112

Настройка SMTP 113

Настройка фильтра системных событий 115

Настройка фильтра событий на портах 116

Настройка фильтра событий SFP DDM 117

СБОР ДАННЫХ НА КОММУТАТОРЕ 117

Порядок настройки сбора данных 118

Сброс собранных данных 119

Диаграмма состояния PoE 120

Диаграмма трафика на интерфейсах 122

НАСТРОЙКА ТАБЛИЦЫ MAC АДРЕСОВ 124

Настойка статических MAC адресов 124

Просмотр таблицы MAC адресов 125

АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ ЛОКАЛЬНАЯ/TACACS/RADIUS 127

Настройка режима аутентификации 127

Настройка параметров RADIUS сервера 128

Настройка параметров TACACS+ сервера 129

ОБНОВЛЕНИЕ ВСТРОЕННОГО ПО 131

Обновление путем загрузки ПО с ПК 131

Обновление путем загрузки ПО с USB 133

РЕЗЕРВНОЕ КОПИРОВАНИЕ КОНФИГУРАЦИИ 136

Сохранение резервной копии 136

Восстановление конфигурации 137

Автозагрузка и автоматическое резервирование по USB 138

Доступ к файлам по SFTP 139
Сохранение конфигурации по SFTP 139

ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ (CLI) 140

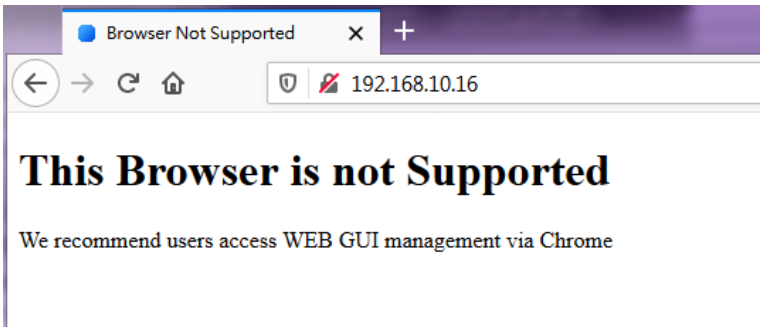
Подключение с помощью консольного порта 140
Подключение по Telnet 141
Различные режимы CLI 141
Обновление ПО через CLI 142
С помощью TFTP 142
С помощью Wget 144
С помощью USB 146
Группы команд CLI 147
Команды аутентификации 147
Команды SSH 148
Системные команды 148
Команды контроля сервисов 149
Команды IPv4 149
Команды IPv6 150
Команды настройки даты/времени 150
Команды PTP 151
Команды STP 152
Команды ERPS 153
Команды MRP 154
Команды SNMP 155
Команды DHCP 157
Команды индустриальных протоколов 158
Команды UPnP 158
Команды настройки портов 158
Команды PoE 159
Команды IGMP Snooping 160
Команды VLAN 161
Команды QoS 161
Команды настройки транков 162
Команды управления трафиком 162
Команды статической маршрутизации 163
Команды OSPFv2 163
Команды OSPFv3 164

Команды RIPv1/v2 ..... *165*
Команды RIPng *166*
Команды VRRP *166*
Команды 802.1X *167*
Команды зеркалирования *168*
Команды LLDP *168*
Команды Syslog *168*
Команды SMTP *169*
Команды управления отчетами *170*
Команды таблицы MAC адресов *172*
Команды операций с USB *172*
Команды управления файлами *173*

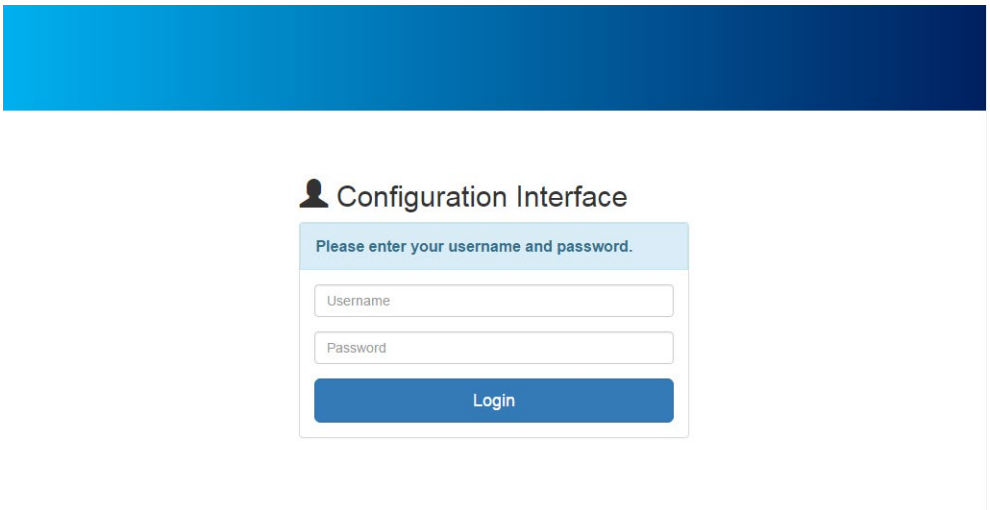
Начало работы

Веб-интерфейс

Запустите веб-браузер. Мы рекомендуем браузер Google Chrome. Если используемая вами версия веб-браузера не поддерживается, будет показано предупреждение.



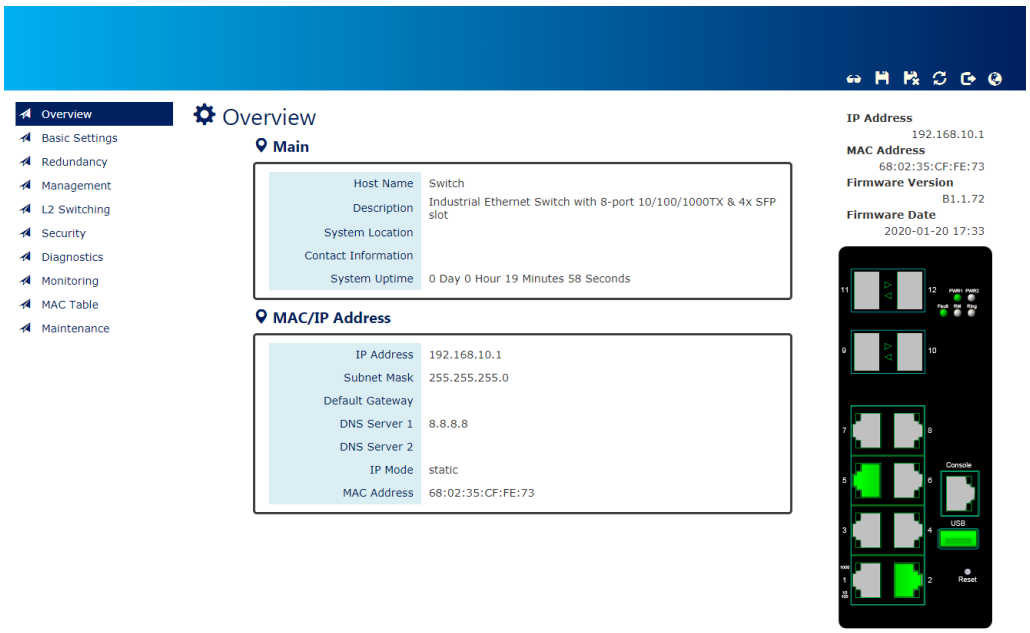
В адресной строке введите IP-адрес коммутатора к которому будете подключаться. По умолчанию IP адрес коммутаторов QBIT - **192.168.10.1**. Если адрес введен правильно, появится окно входа в веб-интерфейс управления.



Введите имя пользователя и пароль и нажмите кнопку "Login" для входа в систему. После входа в систему открывается страница Overview с общей информацией о коммутаторе.

Примечание: по умолчанию имя пользователя и пароль: **admin / admin**.

Ниже показан общий вид интерфейса пользователя и дано общее описание его структуры и базовых глобальных функций.

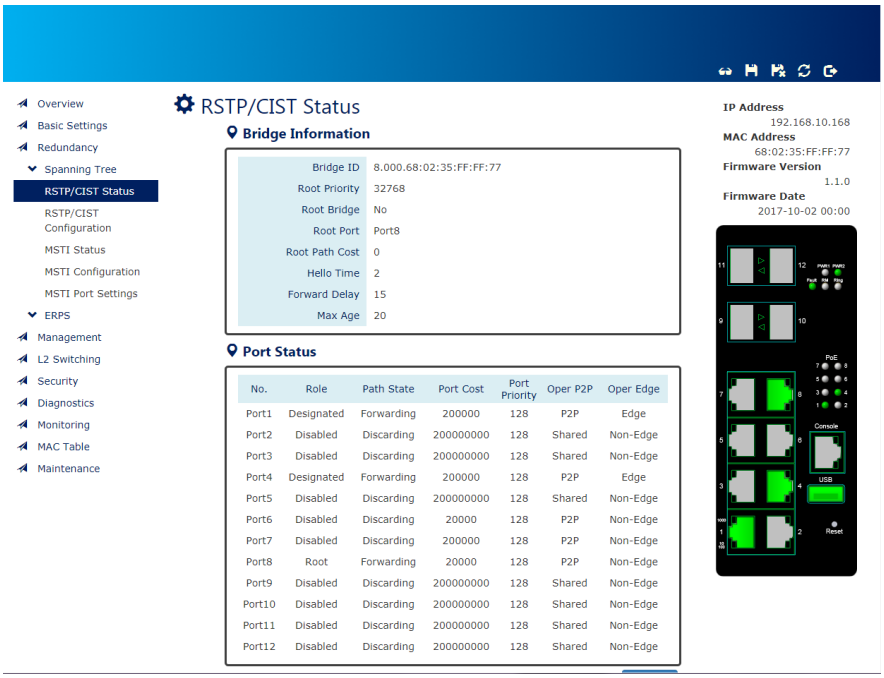


Глобальные функции

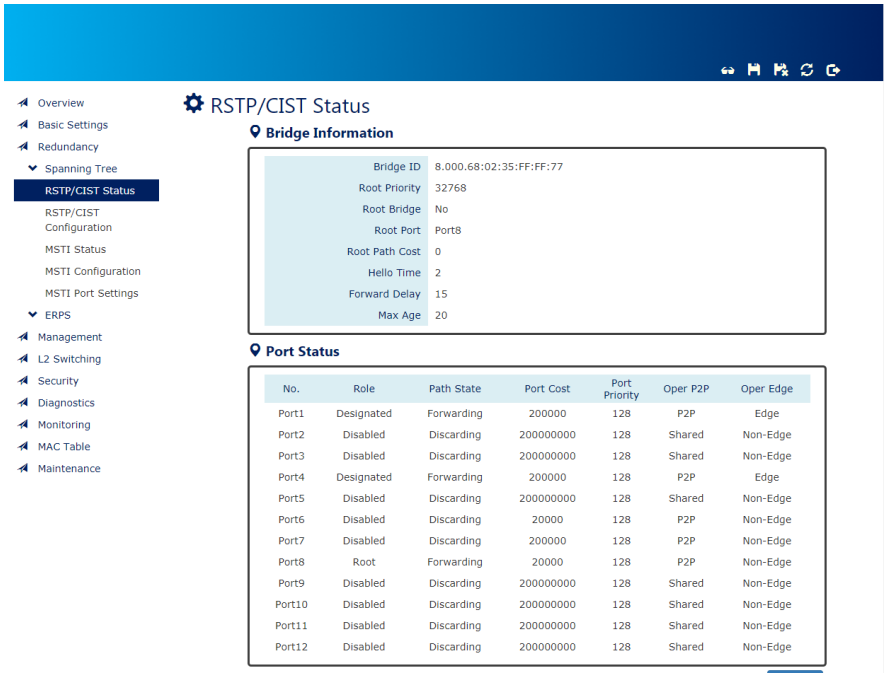
Пять глобальных функций представлены на панели инструментов в верхней части пользовательского веб-интерфейса в виде пяти иконок. Ниже дано краткое описание их назначение

- **- Отобразить/скрыть информацию о коммутаторе.**
  Для удобства работы можно скрывать панель с информацией о коммутаторе в правой части рабочего окна. Панель показывает информацию о модели коммутатора, MAC-адресе, версии ПО и состояние портов.

Вид при включенной информации:



Вид при выключенной информации:



- **Сохранение конфигурации**

  После окончания настройки коммутатора нажмите на эту иконку для того, чтобы сохранить текущую конфигурацию в файл startup-config. Сохраненная конфигурация сохраняется на коммутаторе вплоть до сброса на заводские настройки.

- **Сброс на заводские настройки**

  Удаление конфигурации, сохраненной в системе. После восстановления заводских настроек, все параметры будут сброшены на значения по умолчанию.

- **Перезагрузка**

  Перезагрузка устройства.

- **Выход из веб-интерфейса**

  После выхода из веб-интерфейса потребуется повторный ввод имени пользователя и пароля для получения доступа к управлению устройством.

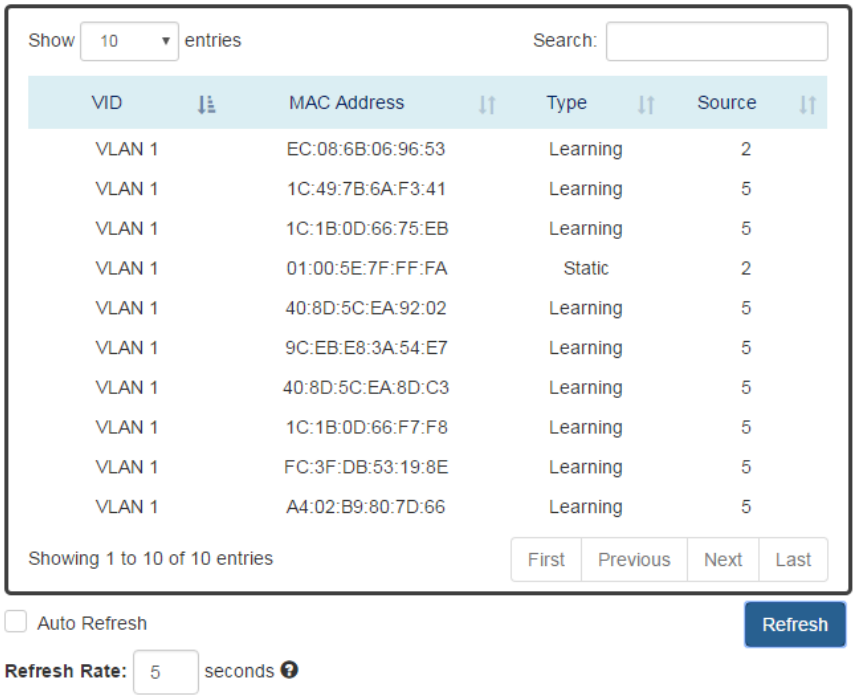
  Так же система автоматически выйдет из интерфейса веб-управления по истечении установленного таймаута. Таймаут устанавливается в CLI с использованием команды exec-timeout. Максимальное значение таймаута для веб-интерфейса составляет 30 минут.

- **Смена языка интерфейса**

  Мы поддерживаем различные языки в веб-интерфейсе. По умолчанию установлен английский язык.

Работа с настраиваемыми таблицами

Настраиваемые таблицы используются в разделах IPv6 Neighbor, IGMP Snooping, VLAN, LLDP Neighbor, MAC Address и других. В данном разделе описывается, как использовать функционал настраиваемых таблиц для удобной обработки информации. Ниже показана настраиваемая таблица на примере таблицы MAC Address.



- Show 10 entries

  Пользователи могут выбирать количество показываемых на одной странице записей. Следующие значения могут быть выбраны: 10, 25, 50, и 100 записей. По умолчанию установлено значение 10.

- Search:

  Поле Search позволяет осуществлять поиск в табличных данных по ключевым словам. Поиск будет проведен по всем столбцам и отображены строки в которых присутствует это ключевое слово.

- Showing 1 to 10 of 31 entries

  В данной строке показываются номера отображенных на странице записей и общее число записей.

- и

  Кнопки сортировки устанавливают сортировку столбца в восходящем или нисходящем порядке.

- First Previous Next Last

  Набор кнопок позволяет переходить на первую страницу - “First”, предыдущую - “Previous”, следующую - “Next”; или последнюю - “Last” страницы.

В дополнение к вышеупомянутым функциям, функции обновления и авто-обновления доступны для всех страниц состояния, включая «Таблица соседей IPv6», «Статус порта RSTP», «Таблица выделенных адресов DHCP», «Статус порта», «Таблица отслеживания IGMP», «Таблица VLAN», «Статус транков», «Таблица соседей LLDP» и «Таблица MAC-адресов».

- Auto Refresh

  Установка этого флажка включает, а снятие флажка отключает функцию автоматического обновления страницы.

- **Refresh Rate:** 5 seconds

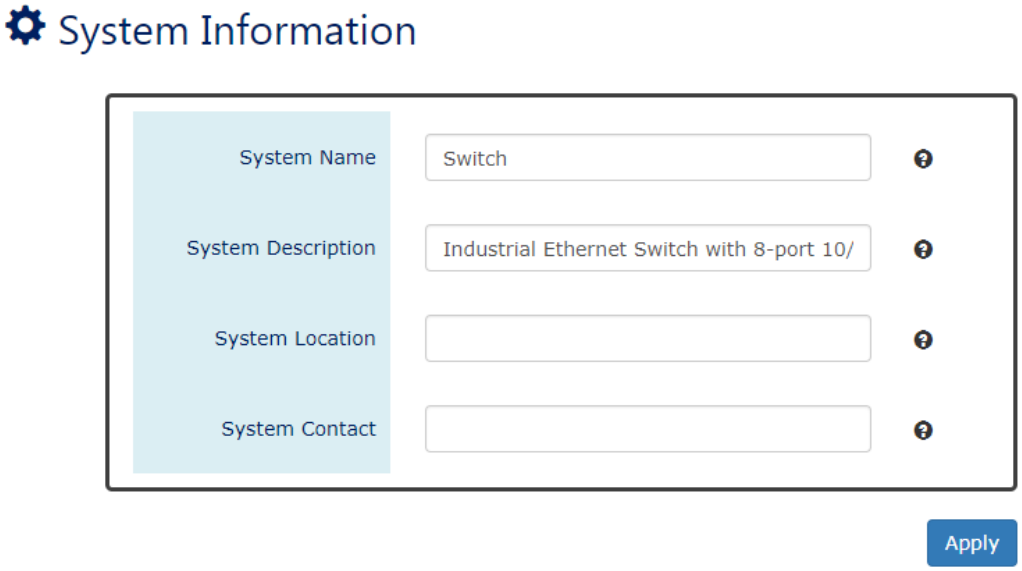
  Параметр частота обновления - это глобальная настраиваемая переменная. Когда опция автоматического обновления включена, статус будет обновляться автоматически в зависимости от интервала частоты обновления. Диапазон частоты обновления составляет от 5 до 300 секунд. По умолчанию частота обновления составляет 5 секунд.

- Refresh (Обновить)

  Вы можете нажать кнопку Refresh, чтобы обновить статус вручную.

Системные настройки

Общая информация о системе



Для более подробной информации наведите курсор мыши на иконку ?.

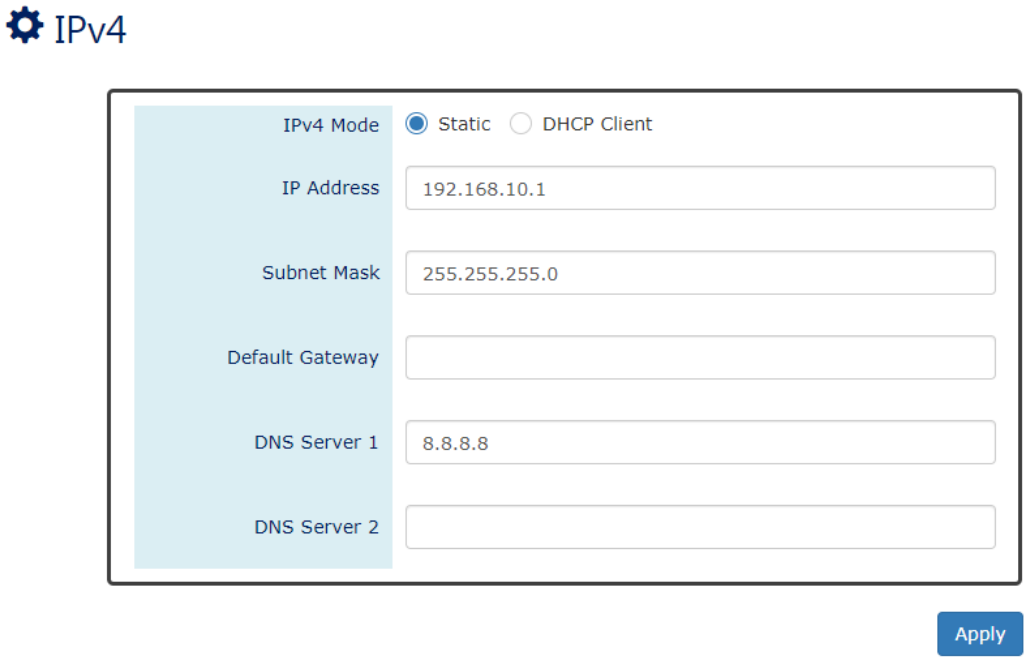
- **System Name.**
  Имя системы. Полезно менять наименование коммутатора что бы отличать один от другого. Максимальная для на поля 32 символа. Примечание: #, \, ', ", ? не разрешены в этом поле.
- **System Description**
  Описание системы. По умолчанию в описании дана информация о количестве и типе портов. Максимальная длина поля 68 символов. Примечание: #, \, ', ", ? не разрешены в этом поле.
- **Switch Location**
  Расположение коммутатора. Информация о местонахождении данного коммутатора. Максимальная длина поля 68 символов. Примечание: #, \, ', ", ? не разрешены в этом поле.
- **Contact Information**
  Контактная информация. Данные о Records the information of the person responsible for this device and also the contact details. Примечание: #, \, ', ", ? не разрешены в этом поле.

Apply (Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Настройки IPv4 (VLAN IP)

Интернет-протокол версии 4 (IPv4) - четвертая версия Интернет-протокола. Он используется в сетях с коммутацией пакетов и при связи без установления соединения. IPv4 имеет четырехбайтовый (32-битный) адрес, а адресное пространство ограничено 4 294 967 296 (232) уникальными адресами. В локальной сети (LAN) обычно используется диапазон для частных сетей. Он начинается с 192.168.0.0, а адресное пространство содержит 65 025 (2^{16}) IP-адресов. IP-адрес коммутатора по умолчанию - 192.168.10.1. Когда пользователи хотят подключиться к веб-консоли коммутатора, их компьютеру в этом случае должен быть назначен IP-адрес от «192.168.10.2» до «192.168.10.254».



- **IPv4 Mode (Режим IPv4)**

  Существует два способа настройки IPv4-адреса: один - настроить статический IP-адрес вручную, а другой - получить IP-адрес по DHCP. Если режим IPv4 - «DHCP Client», информационные поля IPv4 будут установлены на «Disabled».
- **IP Address**

  Уникальный IP адрес для интерфейса связанного с VLAN ID. IP адрес по умолчанию для VLAN 1 равен 192.168.10.1.
- **Subnet Mask**

  Маска сети для интерфейса связанного с VLAN ID. По умолчанию для VLAN 1 равна 255.255.255.0.
- **Default Gateway**

  Шлюз по умолчанию
- **DNS Server №1 / №2**

  Задает IP-адрес DNS-сервера, чтобы пользователи могли подключаться к другому

устройству на основе URL-адреса, а не IP-адреса. DNS-сервер №1 по умолчанию - «8.8.8.8». Предоставляется Google. DNS-сервер №2 по умолчанию не задан.

(Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Настройки IPv6 (VLAN IP)

Интернет-протокол версии 6 (IPv6) - это решение проблемы ограничения адресного пространства IPv4. Он предназначен для замены IPv4. IPv6 - это протокол уровня 3 (Интернет-уровень), который используется в сетях с коммутацией пакетов и при обмене данными без установления соединения. Для адреса IPv6 имеется 16 байтов (128 бит), а адресное пространство может содержать до 2^{128} уникальных адресов. Адрес IPv6 обычно представлен шестнадцатеричными цифрами, 8 группами по 4 цифры, и каждая группа разделена знаком «:» (двоеточие). Например, адрес DNS-сервера в IPv6 - «2001: 4860: 4860: 0000: 0000: 0000: 0000: 8888».

- **IPv6 Mode**

  «Enable» - включить или «Disable» - отключить IPv6. Когда режим IPv6 включен, другие устройства могут подключаться к этому устройству по IPv6. Режим IPv6 по умолчанию - «Включить».

- **Default Address**

  Это IPv6-адрес по умолчанию для этого устройства. Это локальный link-local адрес, который автоматически генерируется из MAC-адреса устройства.

- **Default Gateway**
  Это шлюз IPv6 по умолчанию для этого устройства. IPv6-адрес маршрутизатора, используемый для подключения LAN к WAN, когда устройства используют IPv6 для связи.
- **IPv6 Addresses**
  Позволяет пользователям определять другие адреса IPv6 для этого устройства. Адрес IPv6 содержит 2 раздела - адрес IPv6 и префикс. Префикс по умолчанию - 64-битный.

- ✚: Нажмите на иконку для добавления IPv6 адреса.
- ✖: Нажмите на иконку для удаления IPv6 адреса.

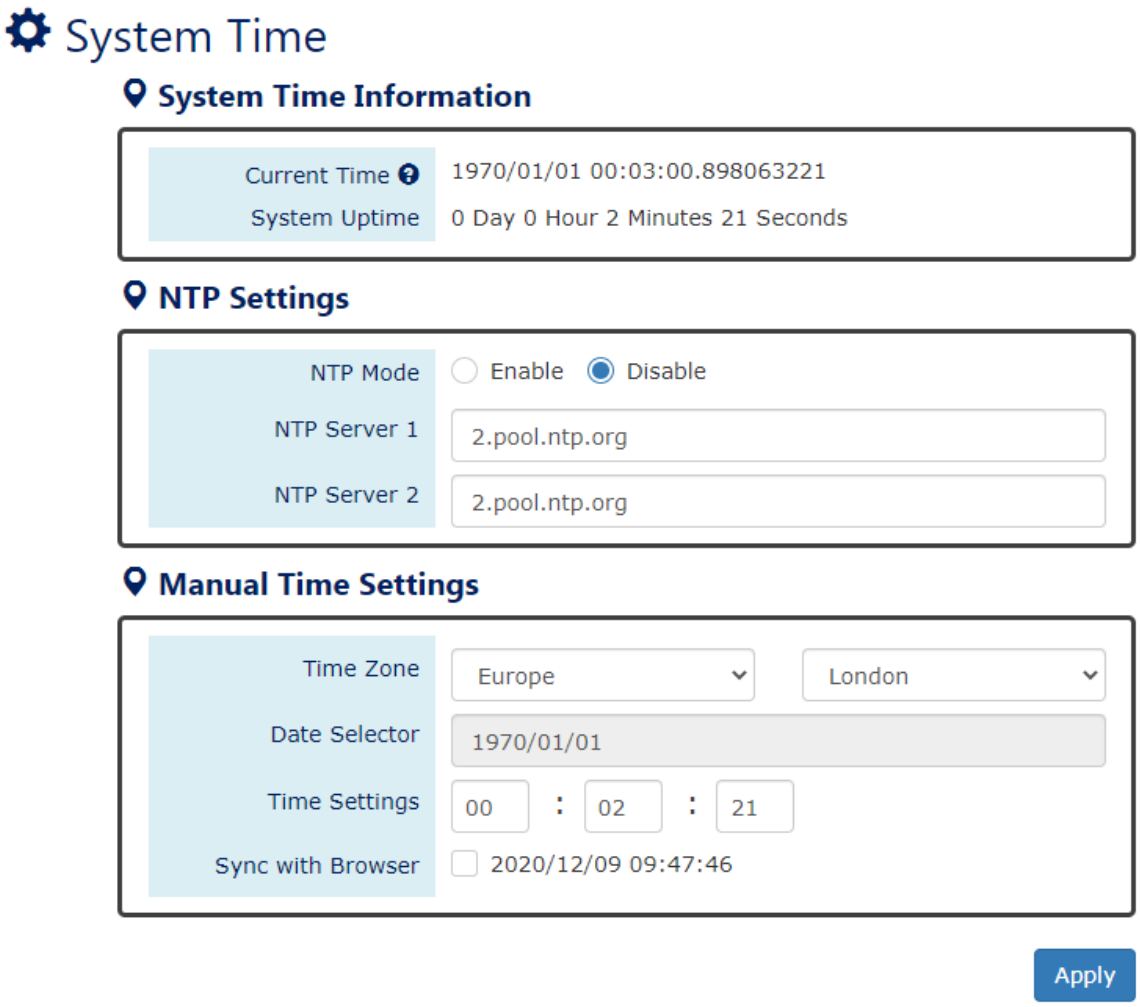
Apply (Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Системное время

Раздел **System time** представляет настройки даты и времени на коммутаторе. Время безотказной работы системы (**System uptime**) определяет время, прошедшее после загрузки системы. В коммутаторе нет батареи, поэтому системное время не может быть сохранено не может быть сохранено на оборудовании при потере питания. Пользователи могут настроить часовой пояс и системное время вручную, синхронизируя время с браузером. Или включив службу NTP для получения времени с NTP сервера.

Network time protocol (NTP) - это протокол синхронизации часов, который используется для синхронизации системного времени с сервером NTP. NTP - один из старейших Интернет-протоколов, используемых с 1985 года по настоящее время. Он работает на основе модели клиент-сервер, но также может использоваться в одноранговых отношениях. Приложение NTP на коммутаторе следует модели клиент-сервер, и коммутатор играет роль клиента NTP.



System Time Information – настройка даты и времени

- **Current Time:**
  Текущие дата и время системы. Примечание: формат даты и времени Год/месяц/день часы:минуты:секунды.наносекунды
- **System Uptime:**
  Продолжительность работы системы после последней загрузки.

Настройки NTP

- **NTP Mode**
  Включение работы NTP протокола. Включение – Enable, выключение - Disable. Если режим NTP включен, система будет синхронизировать время с NTP сервером каждый час.
- **NTP Server 1 & 2**
  Поля URL адресов внешних NTP серверов. Система поддерживает до двух NTP серверов.

Manual Time Settings – ручная настройка даты и времени

- Time Zone
  Выбор временной зоны времени коммутатора.
- Date Selector
  Ручной выбор даты. Формат ввода "год/месяц/день".
- Time Setting
  Ручной выбор времени. Формат ввода "часы:минуты:секунды".
- Sync with Browser
  Установите этот флажок для автоматической синхронизации текущей времени и даты с вашим браузером.

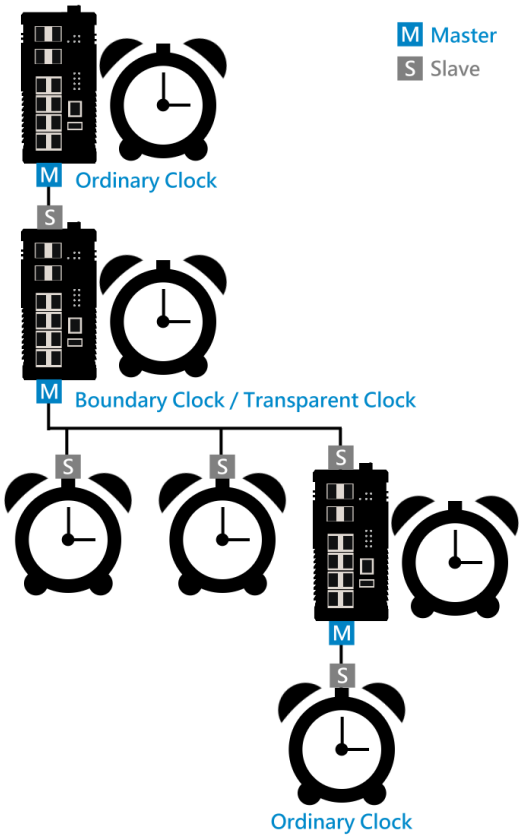
(Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Precision Time Protocol (PTP)

Общие понятия

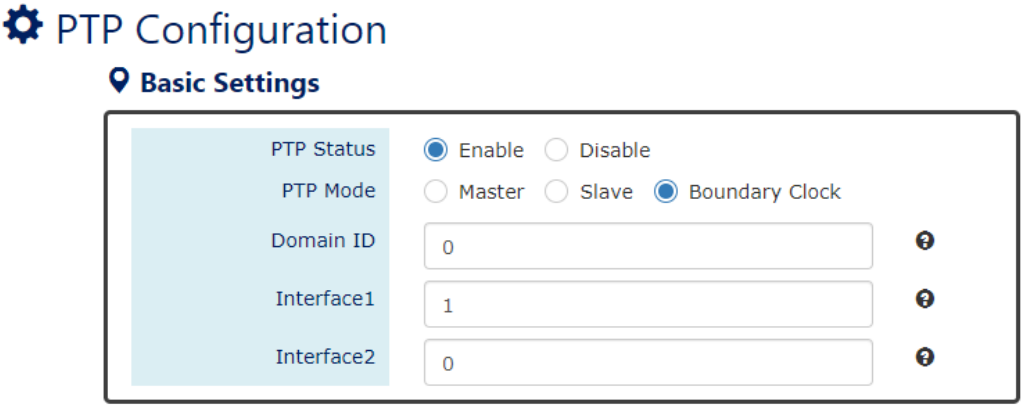
Протокол точного времени (PTP) используется для синхронизации часов, и он более точен, чем NTP. PTP в основном используется для синхронизации сетевых устройств, требующих точной синхронизации процессов. Синхронизация и управление сетью PTP осуществляется путем обмена сообщениями между коммутаторами.



PTP работает по структуре Master и Slave. Существует три типа часов PTP - обычные часы (Ordinary Clock, OC), граничные часы (Boundary Clock, BC) и прозрачные часы (Transparent Clock, TC). В настоящее время мы поддерживаем OC и TC на коммутаторах L2 и L3, а также BC на коммутаторах L3. Если коммутатор является OC, он может быть настроен как ведущий или ведомый (master и slave). Для BC и TC устройства могут быть одновременно и ведущим, и ведомым, чтобы синхронизироваться с вышестоящим master'ом.

Базовые настройки PTP– Ordinary Clock (OC)

Раздел PTP Configuration – Basic Settings



Для более подробной информации наведите курсор мыши на иконку ?.

- **PTP Status**

  Включение работы PTP протокола. Включение – Enable, выключение - Disable. Примечание: Режим PTP Slave несовместим с NTP клиентом на устройстве. Если вы хотите включить PTP роль Slave, пожалуйста убедитесь, что NTP клиент выключен.

- **PTP Mode**

  Режим работы PTP. На коммутаторе поддерживается три роли PTP – Master, Slave, и Boundary Clock (BC). Расширенные настройки для этих режимов различаются и приведены в соответствующих разделах далее.

- **Domain ID**

  Идентификатор домена определяет PTP сеть. Только узлы с одинаковым Domain ID синхронизируются между собой. Значение Domain ID по умолчанию - 0. Диапазон: от 0 до 127

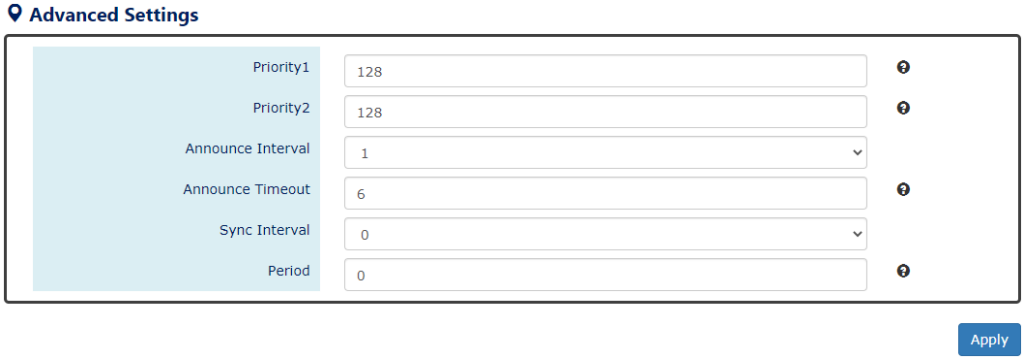
- **Interface1**

  Это поле предназначено для назначения интерфейса для функции PTP. Это Master интерфейс, когда PTP работает в режиме Boundary Clock. Значение Interface1 по умолчанию - 1. Диапазон Interface1 от 1 до 4094.

- **Interface2**

  Поле Interface2 поддерживается только в режиме Boundary Clock. Это интерфейс Slave для Boundary Clock. Значение Interface2 по умолчанию - 0. Диапазон Interface2 от 1 до 4094.

Расширенные настройки PTP - Advanced Settings



Для более подробной информации наведите курсор мыши на иконку ?.

- **Priority 1**

  Приоритет используется для определения лучшего мастера, когда в сети PTP есть несколько мастер-узлов. Если есть 2 или более мастера с одинаковым приоритетом Priority1, система будет использовать значение Priority2. Значение Priority1 по умолчанию - 128. Диапазон Priority1 составляет от 0 до 248. Примечание: чем ниже значение, тем выше приоритет.

- **Priority 2**

  Приоритет используется для определения лучшего мастера, когда в сети PTP есть несколько мастер-узлов. Если есть 2 или более мастера с одинаковым приоритетом Priority1, система будет использовать значение Priority2. Значение Priority2 по умолчанию - 128. Диапазон Priority1 составляет от 0 до 248. Примечание: чем ниже значение, тем выше приоритет.
- **Announce Interval**

  Интервал времени между отправками Announce Message. Значение интервала от -1 до 7.
- **Announce Timeout**

  Таймаут ожидания сообщения Announce Message. Значение по умолчанию 6. Диапазон значений: от 2 до 255
- **Sync Interval**

  Период отправки Sync Message. Диапазон значений: от -7 до 7.

Трансляция значений Announce Interval и Sync Interval в секунды дана в таблице ниже:

Интервал	0	1	2	3	4	5	6	7
Секунды	1с	2с	4с	8с	16с	32с	64с	128с
Интервал		-1	-2	-3	-4	-5	-6	-7
Секунды		512мсек	256мсек	128мсек	64мсек	32мсек	16мсек	8мсек

- **Period**

  Период ожидания синхросигнала. Ведомый узел будет ожидать N временных интервалов Announce Timeout, где N – это Period, до сброса попытки синхронизации. Значение по умолчанию- 0. Диапазон значений: от 0 до 20.

Apply (Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Статус PTP – Master

PTP Status

PTP device type	MasterOnly Clock
Clock Domain	0
Clock ID	680235fffef1c441
Best master ID	680235fffef1c441
Priority1	128
Priority2	128
Class	13

- **PTP Device Type**

  В этом поле указывается тип / роль коммутатора в сети PTP. В настоящее время коммутатор может быть «Master Only» или «Slave Only», потому что сейчас мы поддерживаем только обычные часы (OC).
- **Clock Domain**

  Поле показывает установленный Domain ID системы.
- **Clock ID**

  Это поле является идентификатором коммутатора в сети PTP. Clock ID по умолчанию настроен на MAC-адрес коммутатора.
- **Best Master ID**

  Clock ID лучшего PTP ведущего Master в сети PTP. Если на сети находится несколько PTP ведущих коммутаторов, это поле позволяет понять, кто из них активен в настоящий момент.
- **Priority 1**

  Настроенное значение Priority 1.
- **Priority 2**

  Настроенное значение Priority 2.
- **Class**

  Класс текущего уровня синхронизации. Значения классов PTP синхронизации базируются на традиционных значениях синхронизации SSM/ESMC.

Статус PTP – Slave

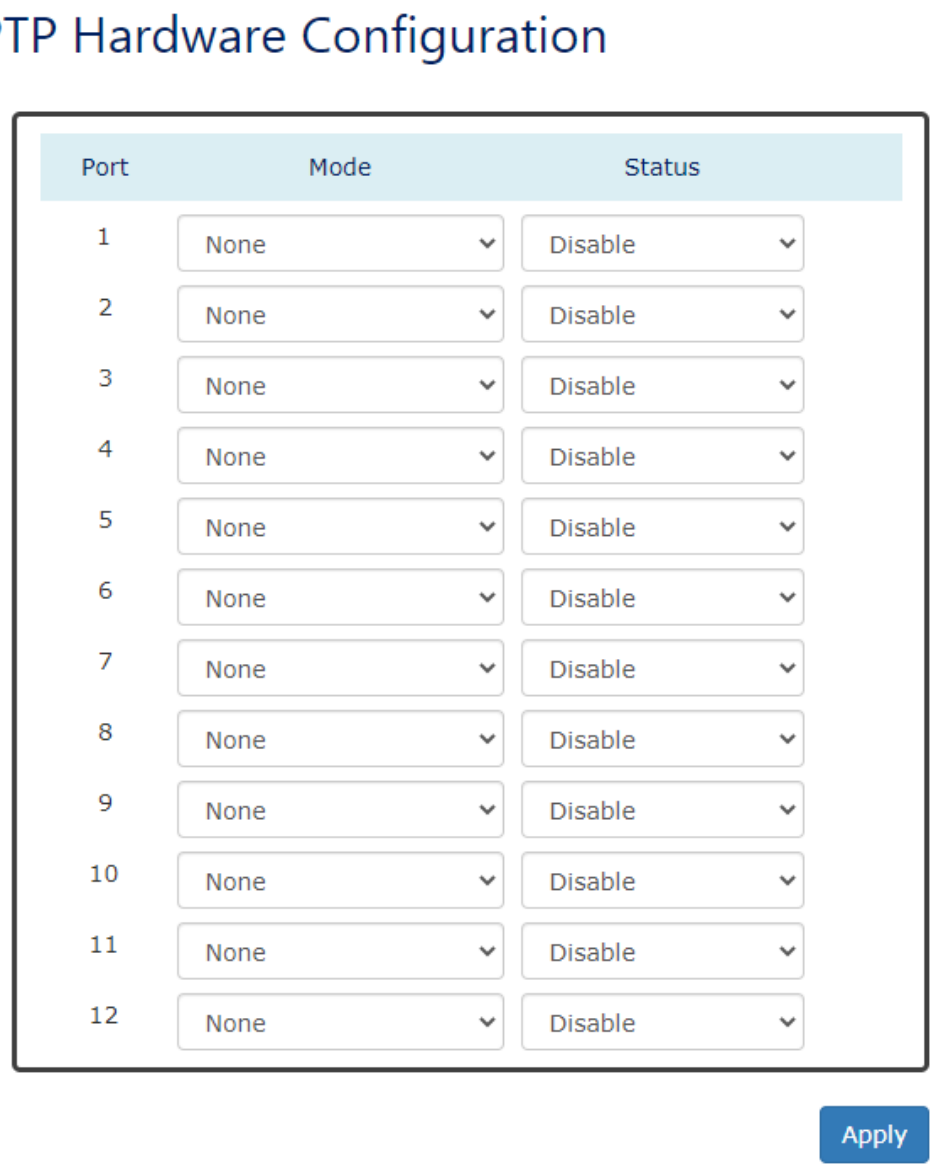
- **PTP Device Type**

  В этом поле указывается тип / роль коммутатора в сети PTP. В настоящее время коммутатор может быть «Master Only» или «Slave Only», потому что сейчас мы поддерживаем только обычные часы (OC).
- **Clock Domain**

  Поле показывает установленный Domain ID системы.
- **Clock ID**

  Это поле является идентификатором коммутатора в сети PTP. Clock ID по умолчанию настроен на MAC-адрес коммутатора.

Базовые настройки PTP - Transparent Clock



Существующие ограничения. Transparent Clock (TC) поддерживается только при следующих условиях:

- Нетегированный режим VLAN;
- L2 коммутаторы;
- Порты 1Гбит/с;
- Режим One-step;
- Задержка End-to-End

Пункты настройки в таблице:

- **Port**

  Номер порта коммутатора от 1 до N, где N определяется общим количеством портов модели коммутатора.

- **Mode**

  Режим работы порта - Transparent Mode (TC) или Normal Mode (OC).

- **Status**

  Включение выбранного режима работы. Включение – Enable, выключение - Disable.

Apply (Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Протоколы семейства Spanning Tree (RSTP/MSTP)

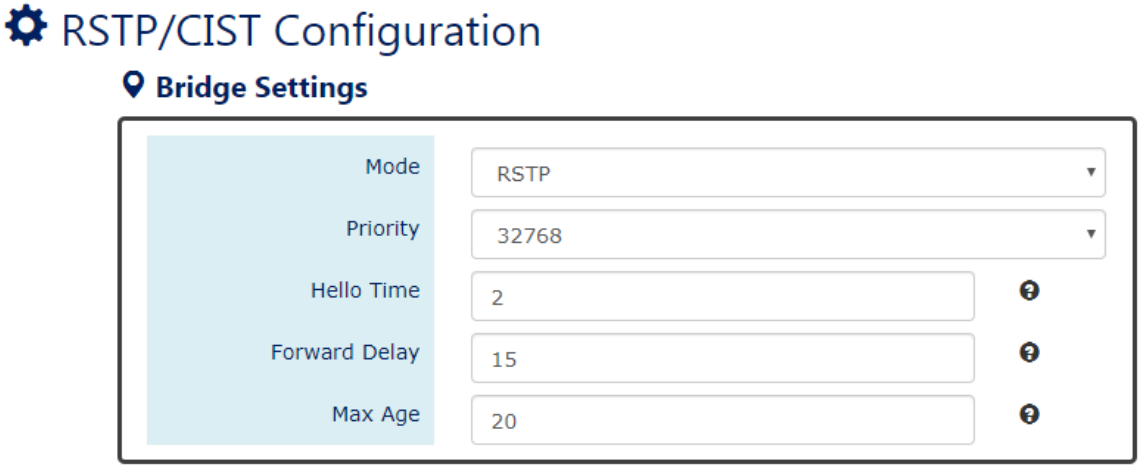
Общие понятия

Протокол связующего дерева (STP) - это стандартный протокол, определенный в IEEE 802.1D. Он используется для построения логической топологии без петель для сетей Layer 2. Основная функция протокола - предотвращение зацикливания и штормов широковещательной рассылки на коммутаторах. STP позволяет резервным каналам в структуре сети обеспечивать резервные пути при выходе из строя активного канала и требует времени сходимости 30–50 секунд для восстановления топологии при ее изменении. Это побудило использовать протокол Rapid Spanning-Tree Protocol, поскольку он обеспечивает более быструю сходимость при изменении топологии.

RSTP был представлен IEEE как 802.1w. Он может ответить в пределах интервала 3 x Hello Time при изменении топологии. Hello Time - это настраиваемое значение, которое очень важно для RSTP. Значение по умолчанию составляет 2 секунды, и обычно время сходимости для RSTP составляет менее 6 секунд. RSTP намного быстрее, чем STP. Вместо STP следует использовать RSTP.

Протокол множественного связующего дерева (MSTP), определенный в IEEE 802.1s, является расширением RSTP для виртуальных локальных сетей (VLAN). MSTP обеспечивает лучший альтернативный путь, чем STP/RSTP для разных VLAN. Это может сделать управление трафиком группы VLAN более систематизированной в сложной топологии.

Базовые настройки RSTP/CIST



Для более подробной информации наведите курсор мыши на иконку ?.

- **Mode**

  Выбор режима работы STP. Возможные варианты: RSTP, MSTP или Disable – отключить использование STP. В этом случае необходимо использовать другие протоколы или настройки для того что бы избежать закольцовывания трафика.

- **Root Priority**

  Корневой приоритет используется для определения «корневого моста». Мост с самым низким корневым приоритетом - это «корневой мост» (root bridge). Если для всех мостов установлено одинаковое значение приоритета, система выберет root bridge на основе MAC-адресов. Диапазон корневого приоритета составляет от 0 до 61440 (кратно 4096). Приоритет по умолчанию - 32768.
- **Hello Time**

  Интервал Hello очень важен и используется для определения интервала отправки BPDU (кадра управления) для проверки топологии и статуса RSTP. Диапазон времени рассылки Hello составляет от 1 до 10 секунд. По умолчанию составляет 2 секунды.
- **Forward Delay**

  Задержка пересылки. Таймер определяет задержку между переходом порта из состояния ожидания Learning/Listening в состояние пересылки кадров Forwarding. Диапазон значений: от 4 до 30 секунд. Значение по умолчанию: 15 секунд.
- **Maximum Age**

  Таймер, который используется для ожидания Hello BPDU от корневого моста. Если этот коммутатор получит BPDU до истечения таймера, таймер будет сброшен. В противном случае коммутатор отправит BPDU с уведомлением об изменении топологии другим коммутаторам. Диапазон значений составляет от 6 до 40 секунд. По умолчанию составляет 20 секунд.

Соотношение между "Hello Time", "Forward Delay" и"Maximum Age" таково:
2 x (Forward Delay - 1 секунда) >= Max Age >= 2 x (Hello Time + 1 секунда)

Настройка RSTP портов

Port Settings

Port	Port Cost	Port Priority	Admin P2P	Edge	Admin STP
1	0	128	Shared	Auto	Enable
2	0	128	Shared	Auto	Enable
3	0	128	Shared	Auto	Enable
4	0	128	Shared	Auto	Enable
5	0	128	Shared	Auto	Enable
6	0	128	Shared	Auto	Enable
7	0	128	Shared	Auto	Enable
8	0	128	Shared	Auto	Enable
9	0	128	Shared	Auto	Enable
10	0	128	Shared	Auto	Enable
11	0	128	Shared	Auto	Enable
12	0	128	Shared	Auto	Enable

Apply

Для более подробной информации наведите курсор мыши на иконку ?.

- **Port**

  Номер порта коммутатора от 1 до N, где N определяется общим количеством портов модели коммутатора.

- **Path Cost**

  Стоимость пути на линии от порта текущего узла до порта другого устройства. Диапазон стоимости пути составляет от 0 до 200000000. Стоимость пути по умолчанию равна 0. Обычно стоимость пути определяется системой.

- **Port Priority**

  Приоритет порта. Используется для принятия решения о блокировании порта в кольцевой топологии. Диапазон приоритета составляет от 0 до 240 и кратен 16. По умолчанию корневой приоритет равен 128.

- **Admin P2P**

  Определяет тип линии на порту. P2P – полнодуплексная линия точка-точка. Shared: полудуплексный канал.

- **Edge**

  Порт который не участвует в расчете топологии STP называется Edge-портом. Пользователь может установить тип порта вручную.

  Auto: система сама определяет, является порт Edge или нет.

  Edge: порт принудительно должен быть Edge-портом. Edge-порт будет напрямую переведен в состояние «Forwarding», и ему не нужно ждать «Forward Delay». Если порт напрямую подключен к устройству, не поддерживающему STP, пользователи могут вручную установить для него значение «Edge» и разрешить ему более быструю передачу.

  Non-Edge: Порт принудительно будет не-Edge портом. Это подразумевает что порт принудительно будет проходить через состояние Learning/Listening к Forwarding вне зависимости от того подключен он к оконечному устройству или нет.

- **Admin STP**

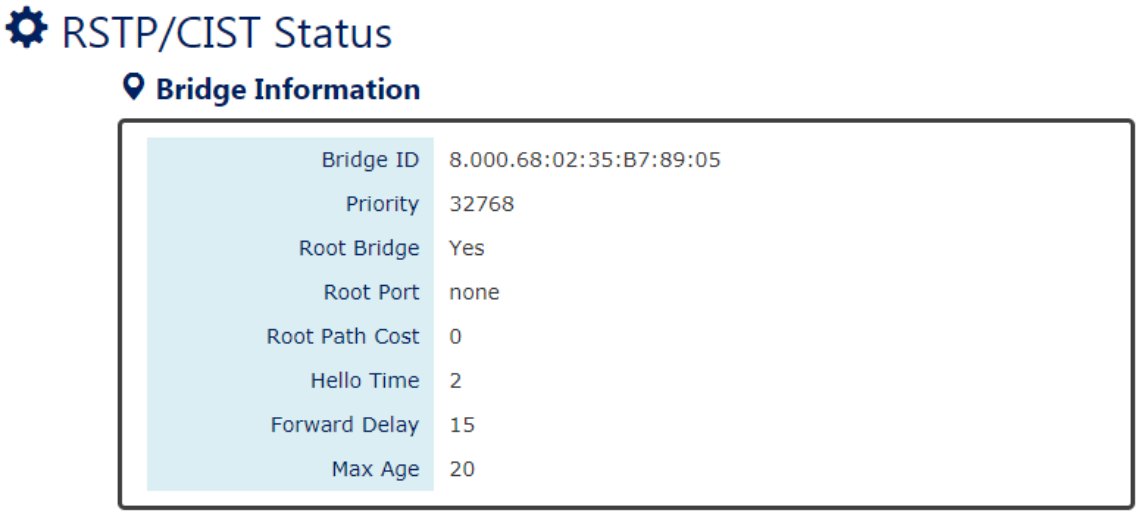
  Включение режима STP на порту. Включение – Enable, выключение - Disable.

(Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Статус состояния протокола RSTP

Общее состояние RSTP на устройстве – Bridge Information



- **Bridge ID**

  В этом поле отображается уникальный идентификатор этого узла, когда он является частью сети STP. Он содержит 8 байтов - первые 2 байта предназначены для значения приоритета моста (настраиваемого), а оставшиеся 6 байтов - для MAC-адреса (уникального).

- **Priority**

  Корневой приоритет коммутатора в RSTP.
- **Root Bridge**

  Является ли данный коммутатор корневым мостом в топологии RSTP, да/нет.
- **Root Port**

  Порт, который подключен к корневому мосту с наименьшей стоимостью пути. Если порт показывает «none», это означает, что этот узел сам является корневым мостом.
- **Root Path Cost**

  Стоимость пути до корневого моста.
- **Hello Time**

  Текущий интервал отправки Hello BPDU.
- **Forward Delay**

  Текущая задержка пересылки.
- **Max Age**

  Текущий таймаут ожидания BPDU.

Состояние портов участвующих в RSTP топологии – Port Status

Port Status

Port	Role	Port Status	Port Cost	Port Priority	Oper P2P	Oper Edge
1	Disabled	Discarding	200000000	128	Shared	Non-Edge
2	Designated	Forwarding	20000	128	P2P	Non-Edge
3	Disabled	Discarding	200000000	128	Shared	Non-Edge
4	Disabled	Discarding	200000000	128	Shared	Non-Edge
5	Disabled	Discarding	200000000	128	Shared	Non-Edge
6	Disabled	Discarding	200000000	128	Shared	Non-Edge
7	Disabled	Discarding	200000000	128	Shared	Non-Edge
8	Disabled	Discarding	200000000	128	Shared	Non-Edge
9	Disabled	Discarding	200000000	128	Shared	Non-Edge
10	Disabled	Discarding	200000000	128	Shared	Non-Edge
11	Disabled	Discarding	200000000	128	Shared	Non-Edge
12	Disabled	Discarding	200000000	128	Shared	Non-Edge

Auto Refresh Refresh

- **Port**

  Номер порта коммутатора от 1 до N, где N определяется общим количеством портов модели коммутатора.
- **Role**

  Поле показывает текущую роль STP порта.

Root: это корневой порт, который с наименьшими затратами подключается к корневому мосту.

Designated: это назначенный порт, который может отправлять лучшие BPDU в сегменте на другие подключенные узлы.

Alternate: альтернативный порт, который заблокирован. Этот порт все еще может получать полезные BPDU от другого моста. Когда он получает полезный BPDU, он помогает пересылать его по сегменту.

Backup: это резервный порт, который заблокирован. Это соответствует роли Alternate. Этот порт также принимает полезные BPDU, но BPDU исходит от того же моста. Когда он получает полезный BPDU, он помогает пересылать его по сегменту.

- **Port Status**

  Поле показывает текущее состояние STP линии.

  Discarding: входящие кадры отбрасываются, а изучение MAC-адресов прекращается.

  Learning: порт изучает MAC-адреса, но входящие кадры отбрасываются.

  Forwarding: порт в состоянии пересылки, пересылает входящие кадры на основе таблицы MAC-адресов.

- **Port Cost**

  Это стоимость от порта до корневого моста. Протокол связующего дерева предполагает, что стоимость пути определяется скоростью доступа каналов. Стоимость пути RSTP по умолчанию показана в следующей таблице:

Скорость	RSTP Стоимость пути	Скорость	RSTP Стоимость пути
4 Мбит	5,000,000	1000 Мбит (1 Гбит)	20,000
10 Мбит	2,000,000	2000 Мбит (2 Гбит)	10,000
16 Мбит	1,250,000	10000 Мбит (10 Гбит)	2,000
100 Мбит	200,000		

- **Port Priority**

  Приоритет порта используется для определения корневого порта некорневого моста. Порт с наименьшим значением приоритета порта получает более высокий приоритет.

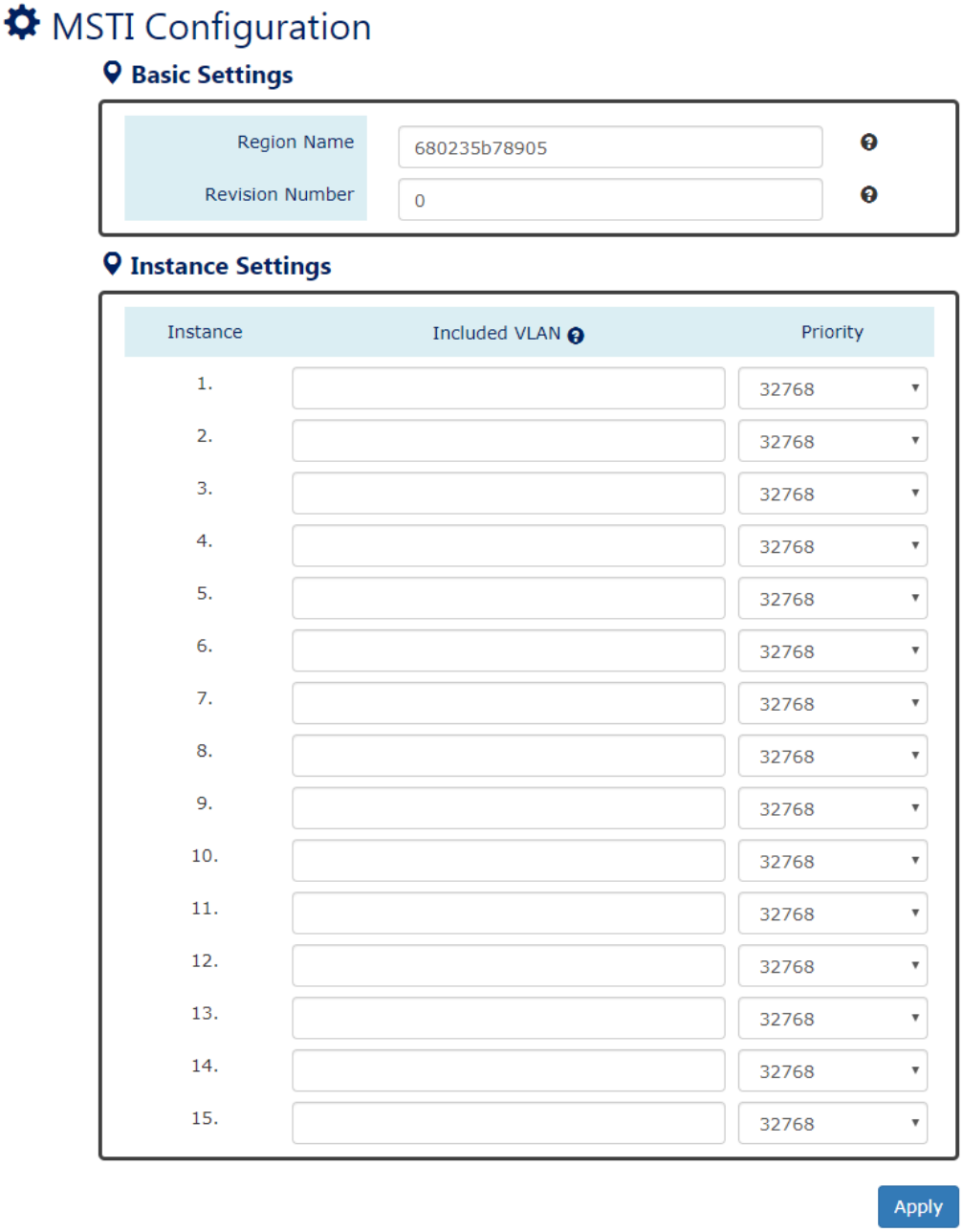
- **Oper. P2P**

  В этом поле отображается тип линии связи порта STP. P2P означает «точка-точка», а Shared означает «точка-многоточка».

- **Oper. Edge**

  Это поле показывает, является ли STP порт – Edge-портом.

Настройки протокола MSTP, параметров MSTI



Для более подробной информации наведите курсор мыши на иконку ?.

Базовые настройки - Basic Settings

- **Region Name**

  Название региона MST. Коммутаторы в общей топологии MSTP должны быть настроены на одно и то же название региона. Максимальная длина названия региона составляет 32 символа. Примечание: #, \, ‘, «, ? не разрешены в этом поле.

- **Revision Number**

  Номер редакции MSTP - параметр аналогичный названию региона. Коммутаторы в одном регионе MST должны быть установлены на один и тот же номер редакции. Диапазон номера редакции от 0 до 65535. Номер редакции по умолчанию - 0.

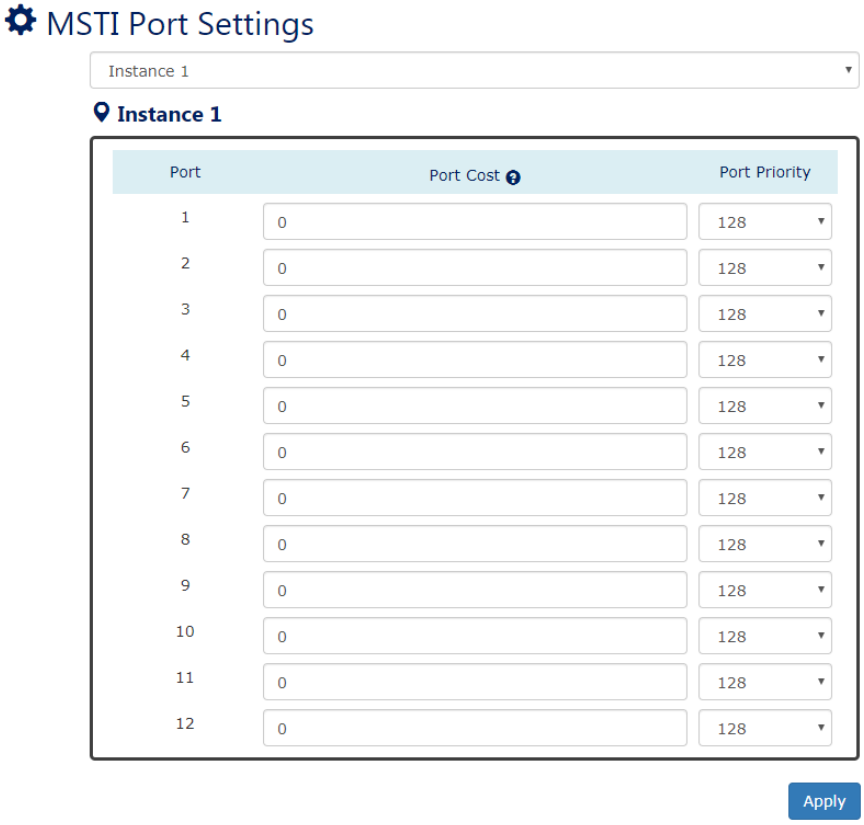
Настройки экземпляров MSTI - Instance Settings

- **Instance**
  Номер экземпляра MSTP, от 1 to 15.
- **Included VLAN**
  Список VLAN ассоциированных с данным экземпляром MSTI. Формат VLAN ID в виде списка разделенного запятыми: 10, 20, 30.
- **Priority**
  Приоритет используется для определения «корневого моста», который используется для связи с другим регионом MSTI. Диапазон корневого приоритета составляет от 0 до 61440 (кратно 4096). Приоритет корня по умолчанию - 32768.

Apply (Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Настройка MSTI портов



Для более подробной информации наведите курсор мыши на иконку ?.

- **Выпадающий список экземпляров MSTI**
  Для выбора интересующего экземпляра MSTI, от 1 до 15.

- **Port**

  Номер порта коммутатора от 1 до N, где N определяется общим количеством портов модели коммутатора.

- **Path Cost**

  Стоимость пути на линии от порта текущего узла до порта другого устройства. Диапазон стоимости пути составляет от 0 до 200000000. Стоимость пути по умолчанию равна 0. Обычно стоимость пути определяется системой.

- **Port Priority**

  Приоритет порта. Используется для принятия решения о блокировании порта в кольцевой топологии. Диапазон приоритета составляет от 0 до 240 и кратен 16. По умолчанию корневой приоритет равен 128.

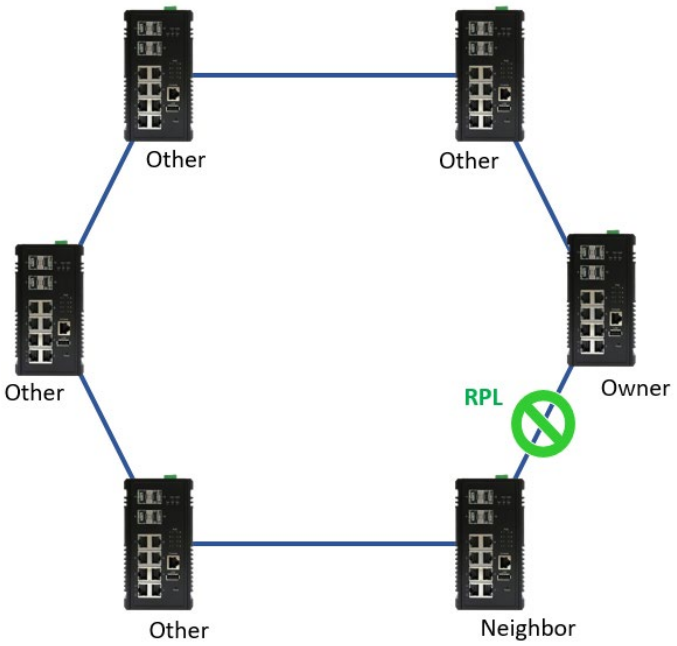
(Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Резервирование ERPS

Общие понятия

Ethernet Ring Protection Switching (ERPS) применяет механизм защитного переключения для трафика Ethernet в кольцевой топологии. Этот механизм определен в ITU-T G8032. Дает возможность резервирования путей передачи трафика, избегая возможных петель в сети. Это делается путем блокирования потока трафика на специально выделенном канале Ring Protection Link (RPL).



Когда ERPS реализован в кольцевой топологии, только один коммутатор назначается владельцем RPL (RPL owner). Этот коммутатор отвечает за блокировку трафика по RPL, чтобы избежать петель. Коммутатор, расположенный рядом с владельцем RPL, называется RPL Neighbor, и он отвечает за блокировку своего конца RPL в нормальных условиях. Участвующие в кольце коммутаторы, которые находятся рядом с владельцем или соседом RPL в кольце, называются участниками кольца. Основная функция этих коммутаторов - пересылать полученный трафик.

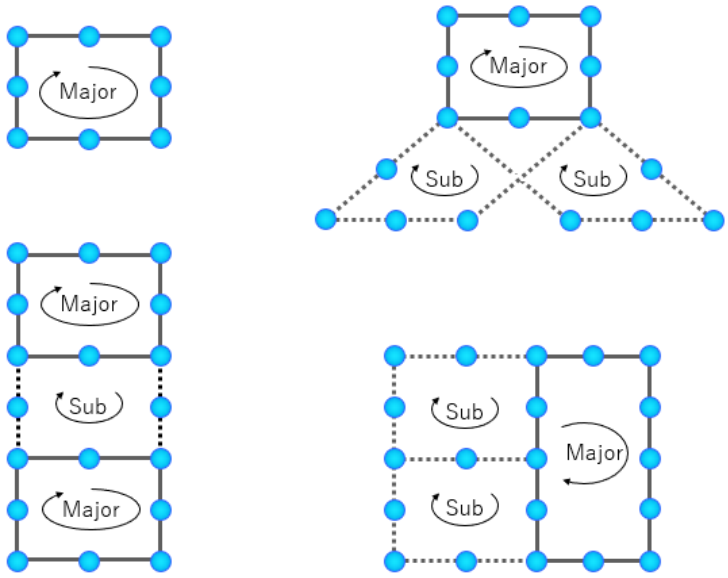
Преимущества архитектуры коммутации с защитой кольца ERPS:

- Защитное переключение на уровне Ethernet
- Предотвращение петли с помощью механизма блокировки RPL
- Защита на основе VLAN
- Защитное переключение менее 50 мсек
- Поддержка OAM
- Протестированы топологии до 250 коммутаторов в едином кольце

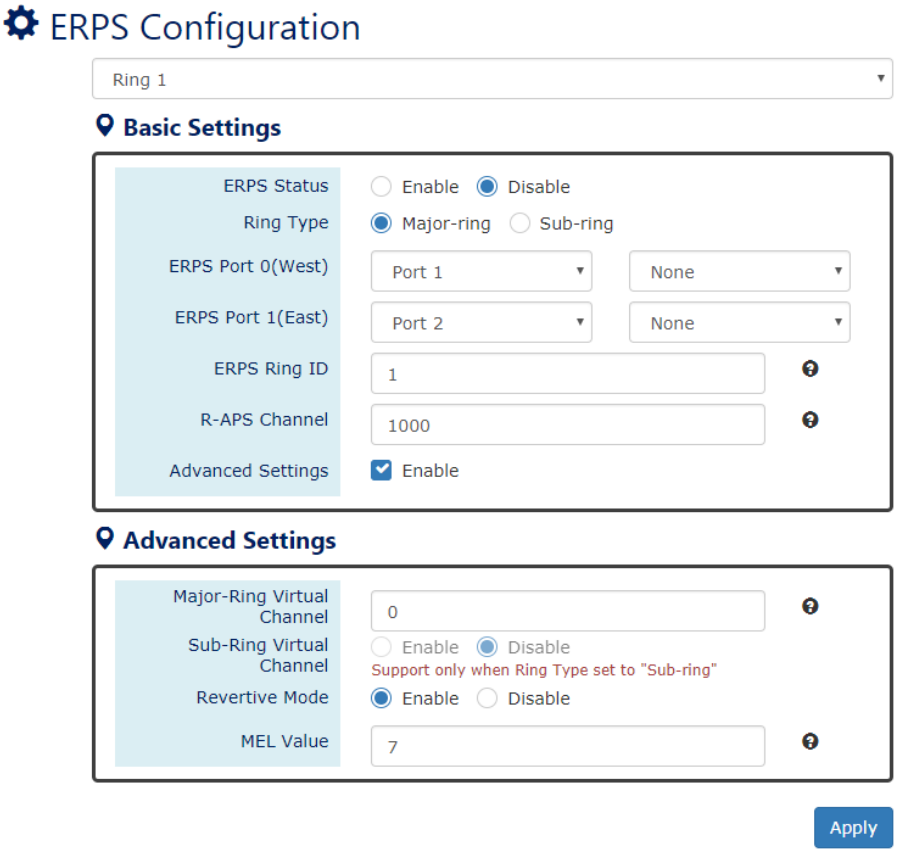
Чтобы убедиться, что кольцо установлено и не имеет петель, узлами в кольце регулярно отправляется сообщение Ring Automatic Protection Switching (R-APS). В случае обрыва канала связи R-APS инициируют процесс переключения на резерв и RPL owner разблокирует канал защиты кольца (RPL) и пропускает защищенный трафик VLAN.

ERPS, аналогично STP, обеспечивает сеть без петель, используя пакеты опроса для обнаружения ошибок. В случае сбоя ERPS восстанавливает передачу данных, отправляя трафик по защищенному обратному пути, а не вычисляя новую топологию пересылки. Механизм обнаружения сбоев в ERPS позволяет ERPS переключиться менее чем за 50 миллисекунд и быстро восстанавливается для пересылки трафика. В реальном тестовом случае время защитного переключения составляет 15 мс для 250 устройств с однокольцевой топологией.

В новой версии ERPS, G.8032 v2, протокол поддерживает множественную кольцевую топологию. Кольца могут соединяться между собой на одном или нескольких узлах. Главное кольцо представляет собой полное физическое кольцо. Починенные кольца формируются в виде полуколе,ц заведенных на главное кольцо в точках подключения.



Настройка ERPS резервирования



Для более подробной информации наведите курсор мыши на иконку ❓.

- **Выпадающий список колец ERPS**

  Коммутатор поддерживает три кольца ERPS. Используя раскрывающийся список, выберите, то, которое планируете настраивать.

Базовые настройки - Basic Settings

- **ERPS Status**

  Включение работы ERPS протокола. Включение – Enable, выключение - Disable. Примечание: по умолчанию протокол ERPS выключен

- **Ring Type**

  Тип кольца. Major-ring: основное физическое кольце. Sub-ring: Полукольцо связанное с основным кольцом.

- **ERPS Port 0**

  Так же обозначается как порт направления Запад (West). Выберите один из портов коммутатора как West и определите его роль в схеме ERPS.

- **ERPS Port 1**

  Так же обозначается как порт направления Восток (East). Выберите один из портов коммутатора как East и определите его роль в схеме ERPS.

Примечание: только один из портов коммутатора может быть назначен как ERPS West или East.

Роль	Описание
Owner	В кольцевой топологии ERPS есть только один Owner (владелец). Владелец RPL несет ответственность за блокировку трафика в RPL и защищает одну сторону RPL.
Neighbor	В кольцевой топологии ERPS есть только один Neighbor (сосед). Сосед владельца RPL защищает вторую сторону RPL.
Interconnection	Порт, соединяющий подкольцо с основным кольцом. Только один порт может быть в этой роли одновременно
None	Порт не имеет специальных ролей в кольце

- **ERPS Ring ID**
  Идентификатор кольца. Участники кольца должны иметь один и тот же идентификатор кольца ERPS. Диапазон идентификатора кольца ERPS составляет от 1 до 239. По умолчанию равен 1.
- **R-APS Channel**
  Сообщения R-APS используется для пересылки информации ERPS и сопоставляется с меткой служебного VLAN – каналом R-APS. Этот служебный VLAN не может использоваться для передачи трафика. Участники кольца должны быть настроены на один и тот же канал R-APS. Диапазон канала R-APS составляет от 1 до 4094. Канал R-APS по умолчанию - 1000.

Расширенные настройки - Advanced Settings

Расширенные настройки доступны только когда включен флажок “Advanced Settings” в основных настройках.

- **Major-Ring Virtual Channel**
  Это поле используется для настройки номера виртуального канала для передачи пакетов управления подкольца через основное кольцо.
- **Sub-Ring Virtual Channel**
  Включает или выключает использование виртуального канала для подкольца. Когда опция Sub-Ring Virtual Channel включена, ERPS протокол будет передавать данные управление подкольцом по назначенному виртуальному каналу.
- **Revertive Mode**
  Включить или Отключить реверсивный режим ERPS. Если включен реверсивный режим, назначенная RPL будет заблокирована после восстановления неисправной

линии. Если нет – заблокированной линией останется та, что была неисправна. По умолчанию включен реверсивный режим ERPS.

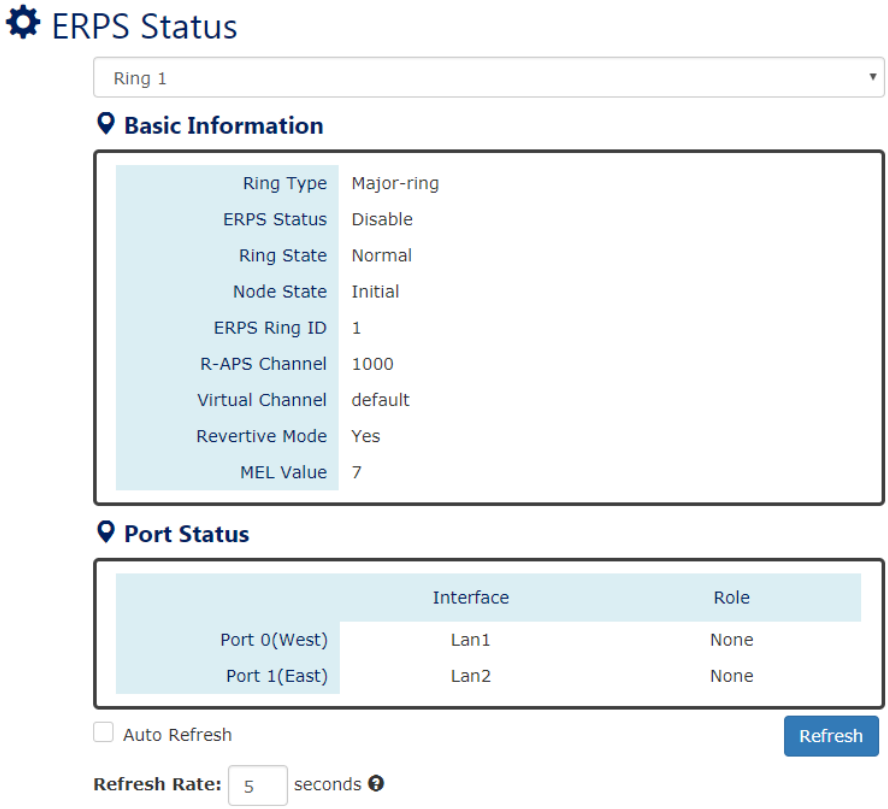
- **MEL Value**

  Поле MEL предназначено для совместимости с другими устройствами, на которых работает протокол OAM ITU-T G.8031 от сторонних производителей. MEL подразумевает уровень MEG. Это поле в PDU R-APS. Большее значение MEL подразумевает большее количество устройств, расположенных на более низких уровнях. Например, уровень 7 содержит уровни от 0 до 6. Диапазон значений MEL от 0 до 7. Значение MEL по умолчанию равно 7.

Apply (Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Статус работы ERPS



- **Выпадающий список колец ERPS**

  Коммутатор поддерживает три кольца ERPS. Используя раскрывающийся список, выберите, то, которое планируете настраивать.

Основная информация - Basic Information

- **Ring Type**

  Тип выбранного кольца ERPS, может быть одни из: “Major-ring”, “Sub-ring with virtual channel” или “Sub-ring without virtual channel”.
- **ERPS Status**

  Статус ERPS кольца может быть включено - “Enable” или выключено - “Disable”.
- **Ring State**

  Состояние кольца ERPS: нормальное - Normal или аномальное - Abnormal.
- **Node State**

  Состояние ERPS на данном коммутаторе: Initial, Idle, Pending или Protection. Ниже в таблице дана расшифровка состояний:

Состояние	Описание
Initial	Протокол ERPS отключен в выбранном кольце.
Idle	Протокол ERPS включен в выбранном кольце, и кольцо ERPS находится под контролем RPL Owner.
Pending	Протокол ERPS включен в выбранном кольце. Кольцо ERPS выходит из состояния переключения на резервное направление и ожидает истечения таймера wtr.
Protection	Протокол ERPS включен в выбранном кольце, но одна из линий в кольце разорвана. RPL включил пересылку кадров, чтобы кольцо продолжало работать.

- **ERPS Ring ID**

  Идентификатор выбранного кольца ERPS.
- **R-APS Channel**

  VLAN ID настроенного канала R-APS.
- **Virtual Channel**

  Поле показывает настроенный виртуальный канал для подкольца. Значение“default” подразумевает что виртуальный канал не имеет отдельной настройки, следует настройке канала R-APS.
- **Revertive Mode**

  Статус реверсивного режима в кольце ERPS – включен/выключен.
- **MEL Value**

  Настроенное значение MEL кольца.

Состояние портов - Port Status

Для портов – участников данного кольца показывается их текущий статус

- **Interface**

- Назначенный порт для ERPS west/east.
- **Role**
- Назначенная роль порта.

Резервирование MRP

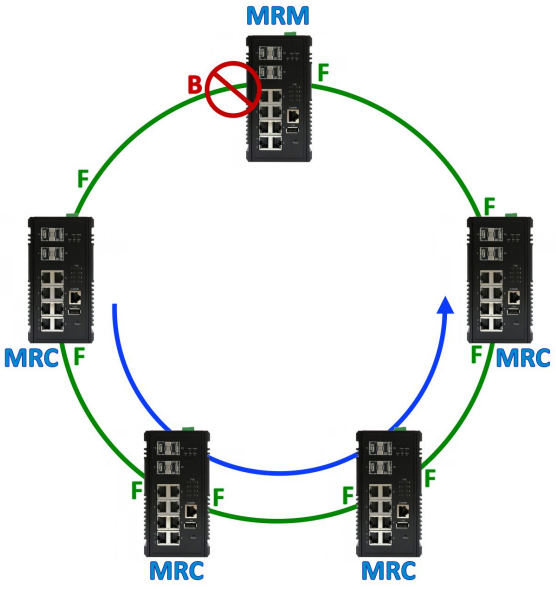
Общие понятия

Внимание: функция MRP поддерживается в коммутаторах QBIT4000-2XG8G, QBIT4000-4XG8G, QBIT4000S-2XG8G, QBIT4000S-4XG8G, QBIT4000S-2XG8G-T, QBIT4000S-4XG8G-T, QBIT4000X-2X8G, QBIT4000X-4X8G, QBIT4000XS-2X8G, QBIT4000XS-4X8G, QBIT4000XS-4X8G-T.

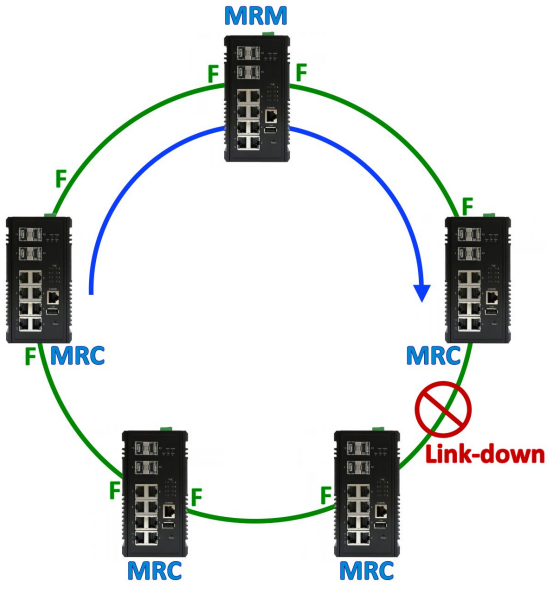
Media Redundancy Protocol (MRP) - это стандартный протокол МЭК для предотвращения образования петель в кольцевой топологии, он определен в МЭК 62439-2. Время восстановления MRP намного быстрее, чем у STP и даже чем у RSTP, поэтому он подходит для большинства приложений Industrial Ethernet.

В кольцевой топологии с MRP менеджер называется Media Redundancy Manager (MRM), а клиенты называются Media Redundancy Clients (MRC). MRM периодически отправляет тестовые пакеты с обоих своих кольцевых портов, чтобы подтвердить работоспособность кольцевой топологии.

Есть три состояния для кольцевых портов MRP – отключен (Disabled), заблокировано (Blocked) и пересылка (Forwarding). Когда кольцо MRP находится в нормальном режиме работы, сеть работает в состоянии замкнутого кольца. В закрытом состоянии один из портов кольца MRM заблокирован, а другой выполняет пересылку кадров в нормальном режиме, в то время как в MRC оба порта кольца выполняют пересылку кадров. Из-за заблокированного порта топология представляет собой разомкнутое логическое кольцо, и петли избегаются. Если один из каналов пересылки кадров выходит из строя, кольцевая топология переходит в открытое состояние, а заблокированный порт MRM переходит в состояние пересылки, чтобы обеспечить передачу в кольце.



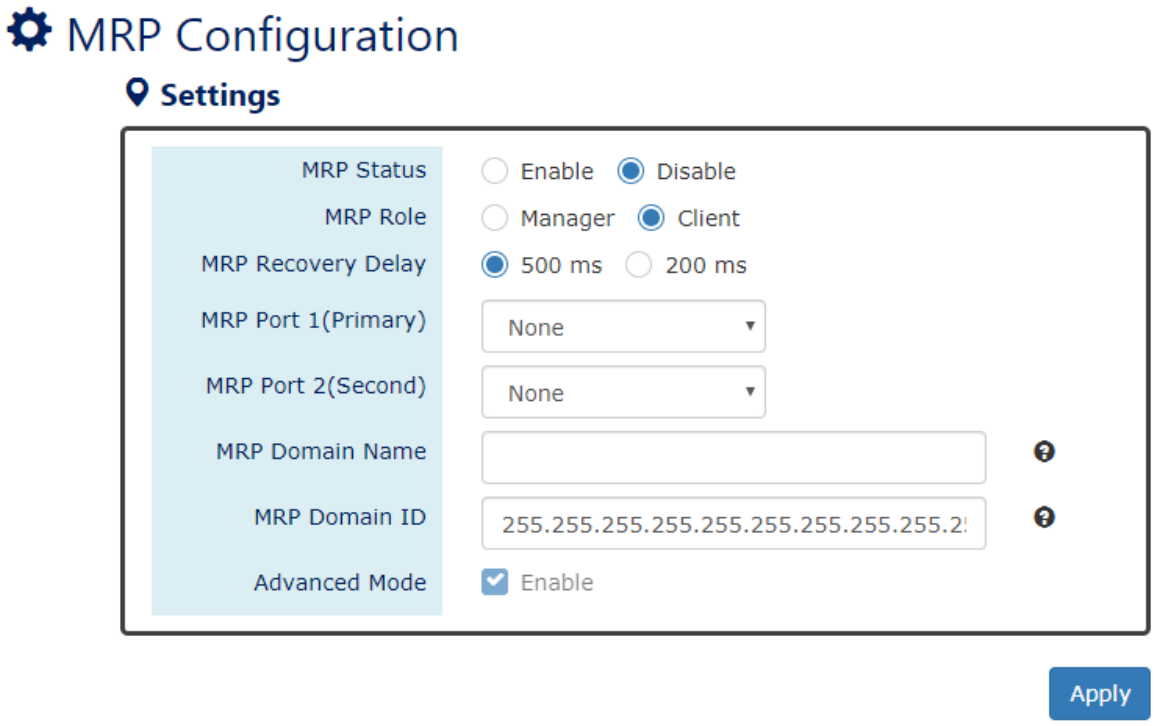
Кольцевая топология открыта



Кольцевая топология закрыта

Стандарт MRP дает гарантированное время восстановления в своих спецификациях. Время восстановления составляет 500 мсек, 200 мсек, 30 мсек с максимум 50 коммутаторами и 10 мсек с максимум 14 коммутаторами в кольце. В настоящее время мы поддерживаем время восстановления 500 мсек и 200 мсек.

Настройка параметров MRP



Для более подробной информации наведите курсор мыши на иконку ?.

- **MRP Status**

  Включение работы MRP протокола. Включение – Enable, выключение - Disable. Примечание: по умолчанию протокол MRP выключен
- **MRP Role**

  Роль коммутатора при запуске протокола MRP. Тип «Manager» подразумевает MRM, а тип «Клиент» - MRC.
- **MRP Recovery Delay**

  Задержка восстановления. МЭК 62439-2 определяет 4 варианта гарантированной задержки: 500 мсек, 200 мсек, 30 мсек, and 10 мсек. В настоящее время мы поддерживаем только 500 мсек, 200 мсек.
- **MRP Port 1 (Primary)**

  Выберите один из портов коммутатора в качестве первичного порта MRP. Первичный порт по умолчанию настроен на пересылку при закрытом кольце.
- **MRP Port 2 (Second)**

  Выберите один из портов коммутатора в качестве вторичного порта MRP. Вторичный порт по умолчанию заблокирован при закрытом кольце.
- **MRP Domain Name**

  Уникальное имя MRP домена.
- **MRP Domain ID**

  Идентификатор домена MRP является ключевым атрибутом для определения членов одного кольца MRP. Идентификатор домена MRP по умолчанию: 255.255.255.255.255.255.255.255.255.255.255.255.255.255.255.255.
- **Advanced Mode**

  Расширенный режим. Поддерживается, только если для роли MRP задано значение «Manager». В расширенном режиме, когда MRM получает сигнал об отключении канала, MRM немедленно активирует резервный порт, а не ожидает потери достаточного количества служебных кадров.

Статус работы протокола MRP

MRP Status

Basic Information

Instance ID	1
Domain ID	255.255.255.255.255.255.255.255.255.255.255.255.255.255.255.255

Configure Information

Advanced Mode(react on link change)	Enabled
Role of Switch (administrative setting)	Manager
Role of Switch (real operating state)	Manager
Domain Name	
Recovery delay	500 (msec)
Port Number, Secondary	3, State: Blocked
Port Number, Primary	4, State: Blocked
Operation	Enabled

Основная информация - Basic Information

- **Instance ID**

  Идентификатор кольца. В настоящее время мы поддерживаем только одно кольцо, так что идентификатор всегда равен 1.
- **Domain ID**

  Идентификатор домена текущего MRP кольца. Только коммутаторы с одинаковым идентификатором домена могут быть участниками одного и того де кольца MRP.

Настройки кольца MRP - Configure Information

- **Advanced Mode**

  Поле показывает состояние статуса расширенного режима MRP. Расширенный режим включается только на коммутаторе, который настроен как MRM (Manager).
- **Role of Switch**

  Существует 2 роли коммутатора в MRP – Manager и Client.

  Administrative Setting: пользовательская настройка роли коммутатора в кольце.

  Real Operating State: фактическая текущая роль коммутатора в кольце.
- **Domain Name**

  Настроенное имя MRP домена.
- **Recovery Delay**

  Поле показывает текущую настройку задержки восстановления передачи. Может быть равно 500 или 200 мсек.
- **Port Number, Secondary**

  Port Number, Primary

Эти поля отображают два элемента информации: первый – это номер порта, который настроен как Primary/Secondary порт на коммутаторе, второй – состояние этого порта. Существует 3 состояние MRP порта: Forwarding, Blocked или Disabled. Если MRP отключен, состояние порта показывается как “N/A”.

- **Operation**

  Текущее состояние операции– Enabled или Disabled.

Operating States

Ring State	Open
Topology Change Interval	20.0 (msec)
Topology Change Repeat Count	3
Short Test Interval	30.0 (msec)
Default Test Interval	50.0 (msec)
Test Monitoring Count	5
Nonblocking Client Supported	Enabled
Test Monitoring Extended Count	15
Check Media Redundancy	Enabled

Состояние работы MRP для менеджера (MRM)

- **Ring State**

  Отображает текущее состояние кольца MRP

  Open: кольцо открыто – какой то из линков в кольце MRP разорван или отказ MRC.

  Closed: кольцо закрыто и работает в нормальном режиме.

- **Topology Change Interval**

  Интервал отправки кадров MRP_TopologyChange.

- **Topology Change Repeat Count**

  Количество повтором отправки кадров MRP_TopologyChange.

- **Short Test Interval**

  Таймер отправки MRP_Test кадров после изменения топологии.

- **Default Test Interval**

  Интервал отправки кадров MRP_Test.

- **Test Monitoring Count**

  Количество интервалов для мониторинга приема кадров MRP_Test.

- **Non-blocking Client Supported**

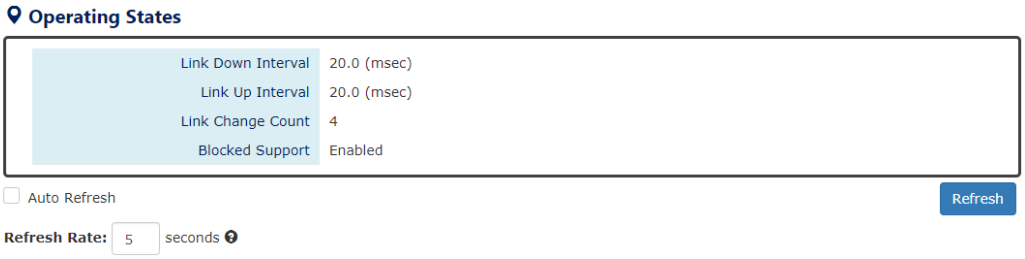
  В этом поле отображается способность MRM поддерживать MRC без поддержки состояния BLOCKED порта в кольце.

- **Test Monitoring Extended Count**

  Это поле является необязательным параметром. Это расширенный счетчик интервалов для мониторинга приема кадров MRP_Test.

- **Check Media Redundancy**

  Проверка текущего состояния MRM. Состояние может быть “Enabled” или “Disabled”.



Состояние работы MRP для клиента (MRC)

- **Link Down Interval**

  Интервал показывает период, в течение которого кадры MRP Link-down отправляются на кольцевой порт. Значение Link-down Interval по умолчанию составляет 20 мсек.
- **Link Up Interval**

  Интервал показывает период, в течение которого кадры MRP Link-up отправляются на кольцевой порт. Значение Link-up Interval по умолчанию составляет 20 мсек.
- **Link Change Count**

  Количество повторов отправки MRP Link-Change кадров. По умолчанию - 4 раза.
- **Blocked Support**

  Поддержка состояния Blocked. По умолчанию включено

SNMP-управление

Общие понятия

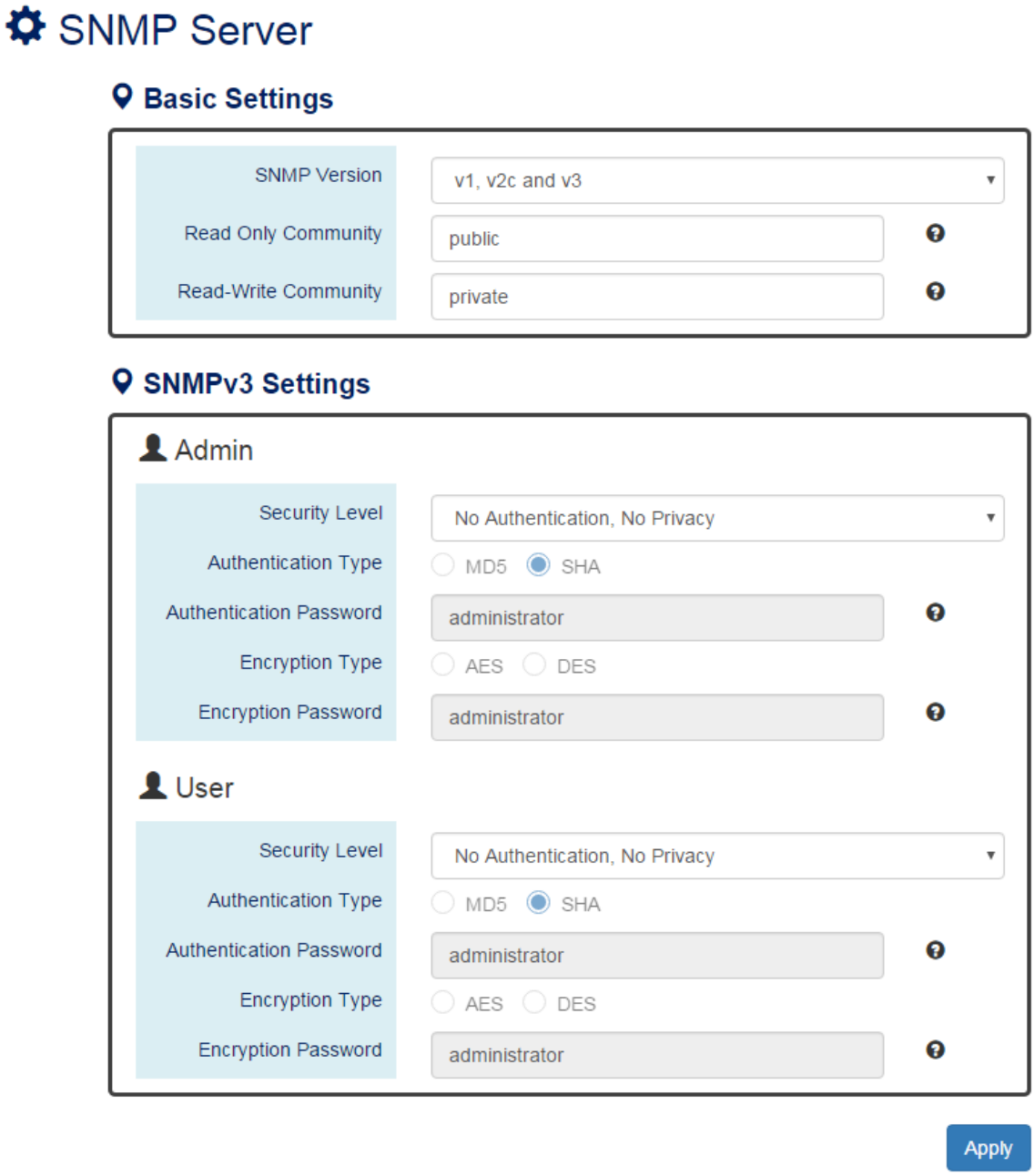
Simple Network Management Protocol (SNMP) Simple Network Management Protocol (SNMP) is a standard for collecting and structuring information on the managed devices of the IP network. It can also modify some of the information to change the behavior of the devices. SNMP is usually used in monitoring the network. The users can remotely query the information provided by the devices running SNMP.

Коммутаторы поддерживают SNMP v1, v2c и v3. SNMP v1 и v2c аутентифицируется с помощью строки сообщества (community) для разрешения «только чтение» или «чтение-запись». Аутентификация SNMP v3 требует выбора уровня аутентификации (MD5 или SHA), а также поддерживает шифрование данных, чтобы сделать работу с коммутатором более защищенной.

Информацию о взаимосвязи между версией SNMP и методом аутентификации см. в таблице ниже:

Версия	Настройка	Аутентификация	Шифрован.	Доступ
v1 & v2c	Read Only Community	Имя Community	Нет	Совпадение имени Community для аутентификации
	Read-Write Community	Имя Community	Нет	Совпадение имени Community для аутентификации
v3	Настройки безопасности: No Authentication, No Privacy	No	Нет	Доступ по имени пользователя
	Настройки безопасности: Authentication, No Privacy	MD5 / SHA	Нет	Доступ по имени пользователя и паролю больше 8 символов, на основе MD5 или SHA
	Настройки безопасности: Authentication, Privacy	MD5 / SHA	Да AES / DES	Доступ по имени пользователя и паролю больше 8 символов, на основе MD5 или SHA. Шифрование на основе AES или DES и ключ от 8 до 32 символов.

Настройка параметров сервера SNMP



Для более подробной информации наведите курсор мыши на иконку ?.

Базовые настройки - Basic Settings

- **SNMP Version**

  По умолчанию система включает использование SNMP v1, v2c и v3. Пользователи могут включить сервер SNMP только на «v1 и v2c» или «v3». «None» означает отключение сервера SNMP.

- **Read Only Community**

  Сообщество только для чтения. Макс. длина для сообщества только для чтения составляет 32 символа. Примечание: #, \, ‘, «, ? не разрешены в этом поле.

- **Read-Write Community**

  Сообщество для чтения-записи. Макс. длина для сообщества для чтения-записи составляет 32 символа. Примечание: #, \, ‘, «, ? не разрешены в этом поле.
- **SNMPv3 Settings**

  Этот раздел отображается только в том случае, если для версии SNMP установлено значение «v3» или «v1, v2c и v3». Предусмотрены две учетные записи - Admin и User для доступа к агенту SNMP. Пользователи могут установить разные уровни для двух учетных записей.
- **Security Level**

  No Authentication, No Privacy: доступ по имени пользователя без пароля.

  Authentication, No Privacy: доступ по имени пользователя с паролем.

  Authentication, Privacy: доступ по имени пользователя с паролем и шифрованием.
- **Authentication Type**

  Предусмотрено два алгоритма - MD5 и SHA для пароля аутентификации.
- **Authentication Password**

  Строка/ключ используется для аутентификации на сервере SNMP и получения разрешения на доступ. Перед аутентификацией пароль будет хеширован с помощью MD5 или SHA. Его мин. длина для сообщества чтения и записи составляет 8 символов. Макс. длина для сообщества чтения-записи составляет 32 символа. Примечание: разрешено использовать только цифры, буквы и подчеркивание.
- **Encryption Type**

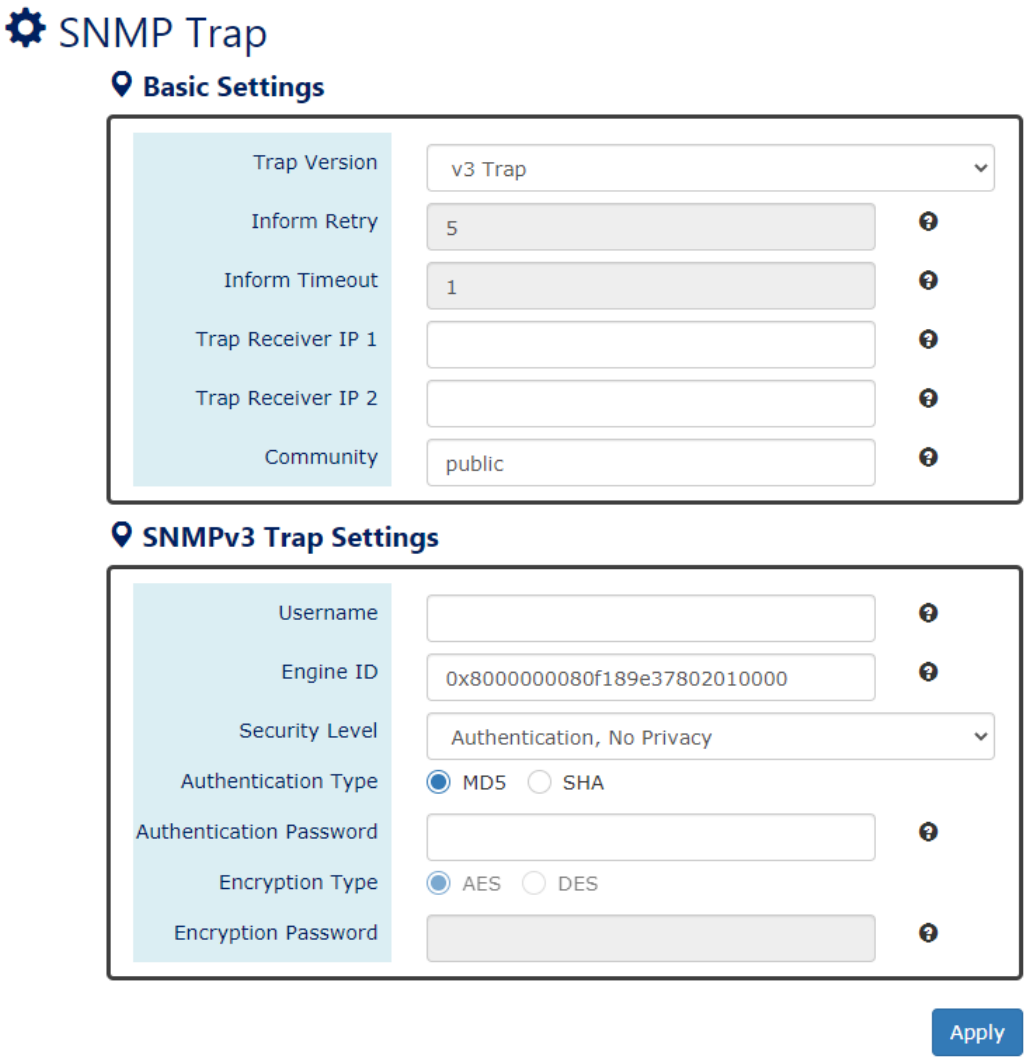
  Предусмотрено два алгоритма - AES и DES для шифрования данных.
- **Encryption Password**

  Строка/ключ используется для шифрования данных SNMP. Его мин. длина для сообщества чтения и записи составляет 8 символов. Макс. длина для сообщества чтения-записи составляет 32 символа. Примечание: разрешено использовать только цифры, буквы и подчеркивание.

(Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Настройка SNMP Trap



Для более подробной информации наведите курсор мыши на иконку ❓.

Базовые настройки - Basic Settings

- **Trap Mode**

  Режим SNMP ловушек. По умолчанию система включает использование trap v1, v2c и v3. Пользователи могут включить trap только на «v1 и v2c» или «v3». «None» означает отключение отправки trap-сообщений.

- **Inform Retry**

  Количество попыток отправки trap-уведомлений для режимов “v2 Inform” или“v3 Inform”. Диапазон значений от 1 до 100. Значение по умолчанию - 5.

- **Inform Timeout**

  Таймаут ожидания отправки trap-уведомлений для режимов “v2 Inform” or “v3 Inform”. Диапазон значений от 1 до 100. Значение по умолчанию - 5.

- **Trap Receiver IP 1 & 2**

  IP-адрес сервера SNMP для получения информации о trap-уведомлениях. Система

поддерживает адреса IPv4 и IPv6 для получателя. Поддерживаются 2 IP-адреса получателя ловушек.

- **Community**

  Сообщество для trap-уведомлений. Максимальная длина – 32 символа. Примечание: #, \, ‘, «, ? не разрешены в этом поле.

Дополнительный настройки v3 - SNMPv3 Trap/Inform Settings

Этот раздел отображается только в том случае, если для параметра Trap Mode установлено значение «v3 Trap» или «v3 Inform».

- **Username**

  Имя пользователя для авторизации на SNMP trap server.
- **Engine ID**

  The Engine ID идентификатор SNMP приложения.
- **Security Level**

  No Authentication, No Privacy: доступ по имени пользователя без пароля.

  Authentication, No Privacy: доступ по имени пользователя с паролем.

  Authentication, Privacy: доступ по имени пользователя с паролем и шифрованием.
- **Authentication Type**

  Предусмотрено два алгоритма - MD5 и SHA для пароля аутентификации.
- **Authentication Password**

  Строка/ключ используется для аутентификации на сервере SNMP и получения разрешения на доступ. Перед аутентификацией пароль будет хеширован с помощью MD5 или SHA. Его мин. длина для сообщества чтения и записи составляет 8 символов. Макс. длина для сообщества чтения-записи составляет 32 символа. Примечание: разрешено использовать только цифры, буквы и подчеркивание.
- **Encryption Type**

  Предусмотрено два алгоритма - AES и DES для шифрования данных.
- **Encryption Password**

  Строка/ключ используется для шифрования данных SNMP. Его мин. длина для сообщества чтения и записи составляет 8 символов. Макс. длина для сообщества чтения-записи составляет 32 символа. Примечание: разрешено использовать только цифры, буквы и подчеркивание.

(Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

DHCP

Общие понятия

DHCP клиент/сервер

DHCP, протокол динамической конфигурации хоста, представляет собой стандартизованный протокол, используемый в IP-сетях. DHCP-сервер содержит пул IP-адресов, и когда DHCP-клиент запрашивает IP-адрес, DHCP-сервер выбирает IP-адрес из пула и назначает его клиенту. DHCP-сервер также управляет другой IP-информацией, такой как шлюз по умолчанию и DNS-сервер. DHCP очень полезен для настройки IP-информации для ряда устройств. Администратору нужно лишь включить DHCP-клиент для каждого устройства и настроить сам DHCP-сервер. Затем клиенты получат уникальный IP-адрес и другие параметры IP для подключения к сети.

Привязка DHCP адресов

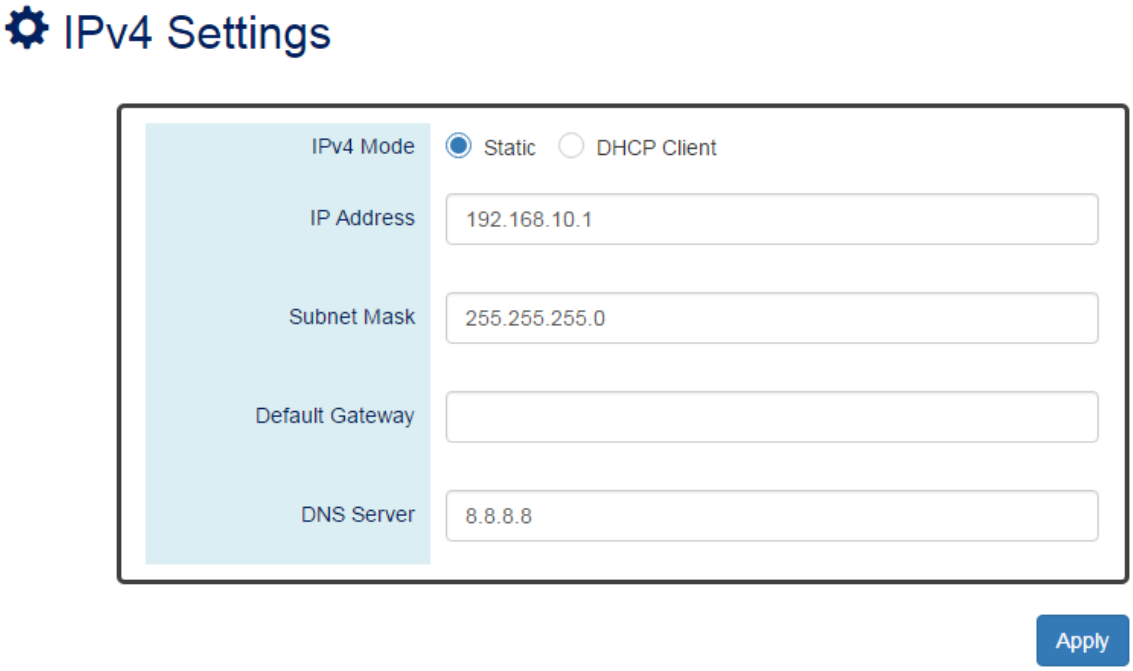
Помимо динамического назначения IP-адреса DHCP-клиенту, DHCP-сервер также предоставляет функцию ручного назначения статического IP-адреса устройству с конкретным MAC-адресом. Это называется привязкой к серверу DHCP (DHCP binding).

DHCP ретрансляция/Option82

В большой сети может существовать несколько подсетей, и DHCP-сервер не может обслуживать DHCP-клиентов напрямую. В этом случае нам нужен агент ретрансляции, который поможет передать кадры запроса на DHCP-серверы. Когда агент ретрансляции получает кадр широковещательного запроса от DHCP-клиента, он передает этот кадр на DHCP-серверы, которые находятся в той же подсети, по одноадресной передаче.

Option 82 - это информационная опция для идентификации клиентов по идентификатору цепи Circuit ID и удаленному идентификатору Remote ID. Circuit ID - это идентификатор, содержащий имя интерфейса и / или информацию о VLAN, а Remote ID используется для идентификации удаленного хоста (агента ретрансляции). DHCP-сервер может передавать IP-адрес DHCP-клиенту в соответствии с информацией указанной в Option 82 и делать выдачу IP-адресов более управляемой.

Настройка DHCP клиента



IPv4 Mode

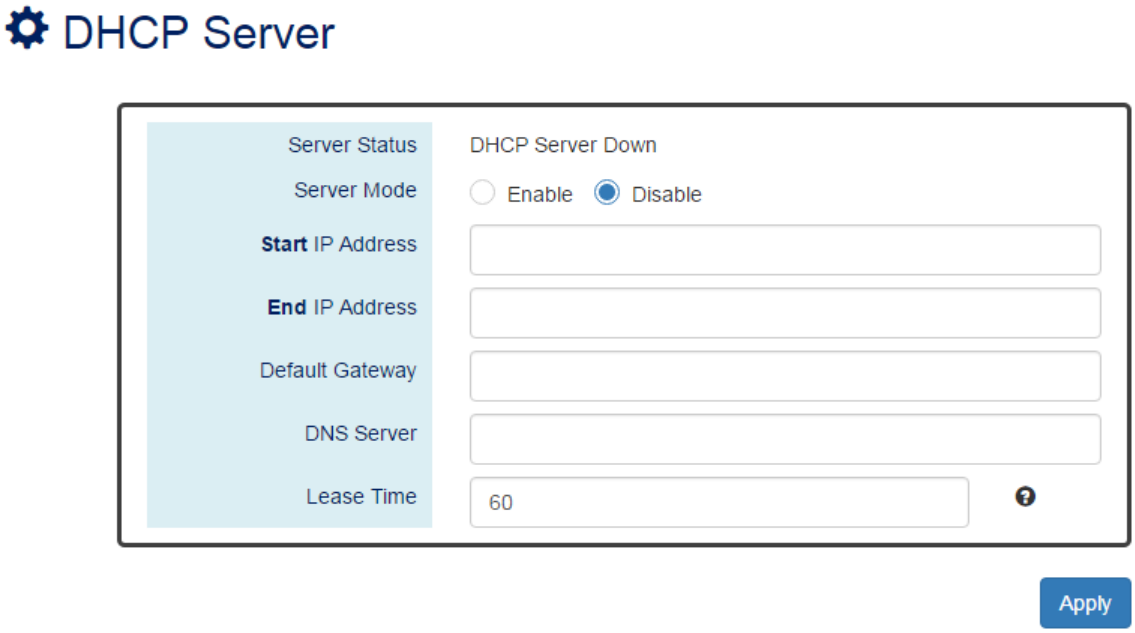
Установите для режима IPv4 значение «DHCP-клиент», чтобы включить DHCP-клиент. Система отправляет в сеть кадр обнаружения и пытается получить IP-адрес от DHCP-сервера.

После включения DHCP-клиента пользователям необходимо подключиться к консольному порту, чтобы получить IP-адрес коммутатора, используя команду «show ip address» в интерфейсе командной строки.

(Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Настройка DHCP сервера



Для более подробной информации наведите курсор мыши на иконку ?.

- **Server Status**

  Показывает состояние DHCP-сервера: включен – Up, выключен - Down
- **Server Mode**

  Включение сервера DHCP на коммутаторе
- **Start IP Address**

  Начальный IP-адрес пула IP-адресов DHCP сервера. Начальный IP адрес должен находится в той же подсети что и коммутатор.
- **End IP Address**

  Конечный IP-адрес пула IP-адресов DHCP сервера. Конечный IP адрес должен находится в той же подсети что и коммутатор.
- **Default Gateway**

  Шлюз по умолчанию для пула адресов. Должен находится в той же подсети что и коммутатор
- **DNS Server**

  IP-адрес DNS сервера выдаваемого DHCP клиентам.
- **Lease Time**

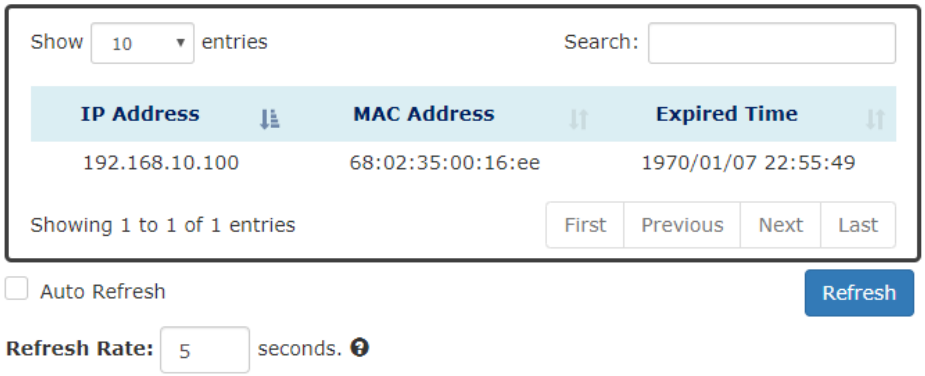
  Время аренды. DHCP-сервер предоставляет устройству в аренду IP-адрес на определенный период времени. По истечении срока аренды DHCP-сервер может назначить устройству другой IP-адрес в пуле.

Apply (Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Таблица арендованных DHCP адресов

DHCP Leased Table



- **IP Address**

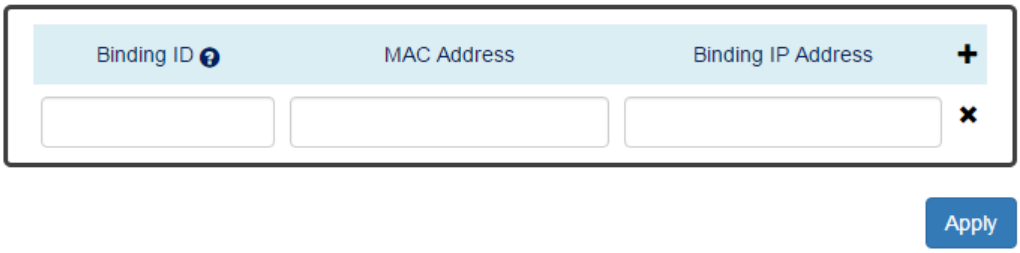
  IP адрес выданный DHCP сервером из пула конечному устройству.
- **MAC Address**

  MAC адрес конечного устройства которому сопоставлен IP адрес
- **Expired Time**

  Время окончания аренды. После окончания аренды клиент должен вновь получить IP адрес от DHCP сервера

Привязка DHCP адресов

DHCP Server Binding



Для более подробной информации наведите курсор мыши на иконку ?.

- **Binding ID**

  Порядковый номер привязки, от 1 до 32.
- **MAC Address**

  MAC адрес устройства , к которому будет привязан IP адрес.

- **Binding IP Address**

  A static IP Address will be assigned to the specified MAC Address.

✚: Нажмите на иконку для добавления новой записи DHCP Binding.

✖: Нажмите на иконку для удаления существующей записи DHCP Binding.

Apply (Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Настройка DHCP ретрансляции

DHCP Relay

Basic Settings

Relay Mode	Enable Disable
Relay Option82	Enable Disable
Helper Address 1	
Helper Address 2	
Helper Address 3	
Helper Address 4	

Relay Untrust

Port	Untrust Status
1	Enable Disable
2	Enable Disable
3	Enable Disable
4	Enable Disable
5	Enable Disable
6	Enable Disable
7	Enable Disable
8	Enable Disable
9	Enable Disable
10	Enable Disable
11	Enable Disable
12	Enable Disable

Apply

Для более подробной информации наведите курсор мыши на иконку ❓.

Базовые настройки ретрансляции - Relay Basic Settings

- **Relay Mode**
  Включение/выключение Enable/Disable функции DHCP ретрансляции.
- **Relay Option82**
  Включение/выключение Enable/Disable функции DHCP Option82 ретрансляции.
- **Helper Address 1 – 4**
  Список IP-адресов DHCP серверов обеспечивающих резервированную раздачу IP адресов клиентам.

Доверие к ретрансляции - Relay Untrust

- **Port**
  Номер порта коммутатора от 1 до N, где N определяется общим количеством портов модели коммутатора.
- **Untrust Status**
  Недоверие к данному порту. Если выбрано Enable – порт не является доверенным для управления DHCP адресами. Управляющие кадры DHCP на этом порту будут игнорироваться.

(Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

PoE (только для моделей с поддержкой PoE)

Общие понятия

PoE, или Power over Ethernet, позволяет коммутаторам подавать электроэнергию вместе с данными по кабелям Ethernet с витой парой. Технология Power over Ethernet, определенная в IEEE 802.3af, обеспечивает мощность до 15,4 Вт, а IEEE 802.3at - до 25,5 Вт. Для поддержки высоких уровней мощности требуются кабели категории 5 или выше. PoE полезен, когда питание переменного тока недоступно или доступно по высокой цене. Обычно он используется в IP-камерах наблюдения, датчиках ввода-вывода, точках беспроводного доступа и IP-телефонах.

Защита от перегрева

Из-за того, что блок питания для некоторых моделей коммутаторов сделан встроенным, доступный бюджет мощности PoE зависит от рабочей температуры. Чтобы обеспечить функциональность PoE, мы выполняем программную защиту в фоновом режиме и корректируем бюджет при повышении температуры. Пожалуйста, обратитесь к Руководству по монтажу вашего коммутатора для получения подробной информации о соотношении бюджета мощности и температуры.

Отладочные коды PoE

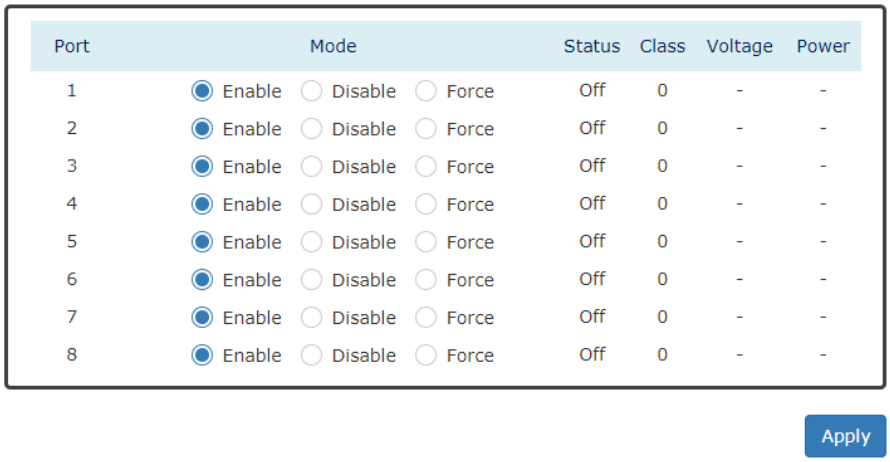
Мы предоставляем команды отладки PoE в CLI для устранения неполадок. Когда пользователи обнаруживают, что функции PoE работают ненормально, пользователи могут использовать команду для получения кода ошибки. Коды ошибок соответствуют различным ситуациям, пользователи могут понять коды ошибок из следующей таблицы:

Код	Описание
0x00	
0x01	
0x02	PoE порт включен
0x03	
0x04	
0x06	PoE порт отключен. Напряжение выше допустимого.
0x07	PoE порт отключен. Напряжение ниже допустимого.
0x11	PoE не определен.
0x20	PoE порт отключен из-за превышения ограничений по энергопотреблению.
0x1F	PoE порт отключен из-заперегрузки согласно 802.3AF/AT.
0x43	PoE порт отключен из-за ошибки класса
0x81	802.3BT–совместимый PD был обнаружен на BT порту (30Вт)

0x85	802.3BT - SSPD was detected using BT Port (60w/95w) and operates as BT Port (30w) if requested class =< 4.
0x86	802.3BT - SSPD was detected using BT Port (60w|95w) and operates as BT Port (60w/95w) if requested class > 4.
0x90	BT Port (30w) and delivers power due to force power command.
0x91	BT Port (60w/95w) and delivers power due to force power command.
0x1B	PoE порт отключен потому что идет процесс обнаружения.
0xA8	PoE порт не подключен.
Другое	Свяжитесь с системным администратором

Настройка PoE

PoE Configuration



Port	Mode	Status	Class	Voltage	Power
1	Enable Disable Force	Off	0	-	-
2	Enable Disable Force	Off	0	-	-
3	Enable Disable Force	Off	0	-	-
4	Enable Disable Force	Off	0	-	-
5	Enable Disable Force	Off	0	-	-
6	Enable Disable Force	Off	0	-	-
7	Enable Disable Force	Off	0	-	-
8	Enable Disable Force	Off	0	-	-

Apply

- **Port**

  Номер порта коммутатора от 1 до N, где N определяется общим количеством портов модели коммутатора.

- **Mode**

  Режим работы PoE на порту. Enable - включен, Disable – выключен, Force – включен принудительно, даже в отсутствие подключенного устройства.

- **Status**

  Поле показывает текущий статус PoE на конкретном порту.

  On: PoE включен на порту и PoE устройство запитано от порта.

  Off: PoE включен на порту, но PoE устройство не подключено.

  Disabled: PoE отключено на порту.

- **Class**

  Поле показывает класс подключенного PD. Приемлемые уровни энергопотребления классов описаны в IEEE 802.3af/at.

- **Voltage**

  Выходное напряжение на порту.

- **Power**

  Показывает энергопотребление на порту. Коммутатор может выдавать до 30 Ватт и PD получать до 25.5 Ватт.

Apply (Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Настройка PoE Keep Alive

PoE Keep Alive

Port	Detect	IP Address	Ping Interval	Hold Time
1	Enable		30	60
2	Enable		30	60
3	Enable		30	60
4	Enable		30	60
5	Enable		30	60
6	Enable		30	60
7	Enable		30	60
8	Enable		30	60

Apply

Для более подробной информации наведите курсор мыши на иконку ?.

- **Port**

  Номер порта коммутатора от 1 до N, где N определяется общим количеством портов модели коммутатора.

- **Detect**

  Детектирование Powered Device (PD) на данном порту. Когда обнаружение включено, система проверяет настроенный IP-адрес через каждый интервал проверки связи.

- **IP Address**

  IP адрес подключенного Powered Device (PD).

- **Ping Interval**

  Интервал опроса с помощью ping для подключенного Powered Device (PD). Диапазон от 1 to 65535 секунд. Значение по умолчанию - 30 секунд.

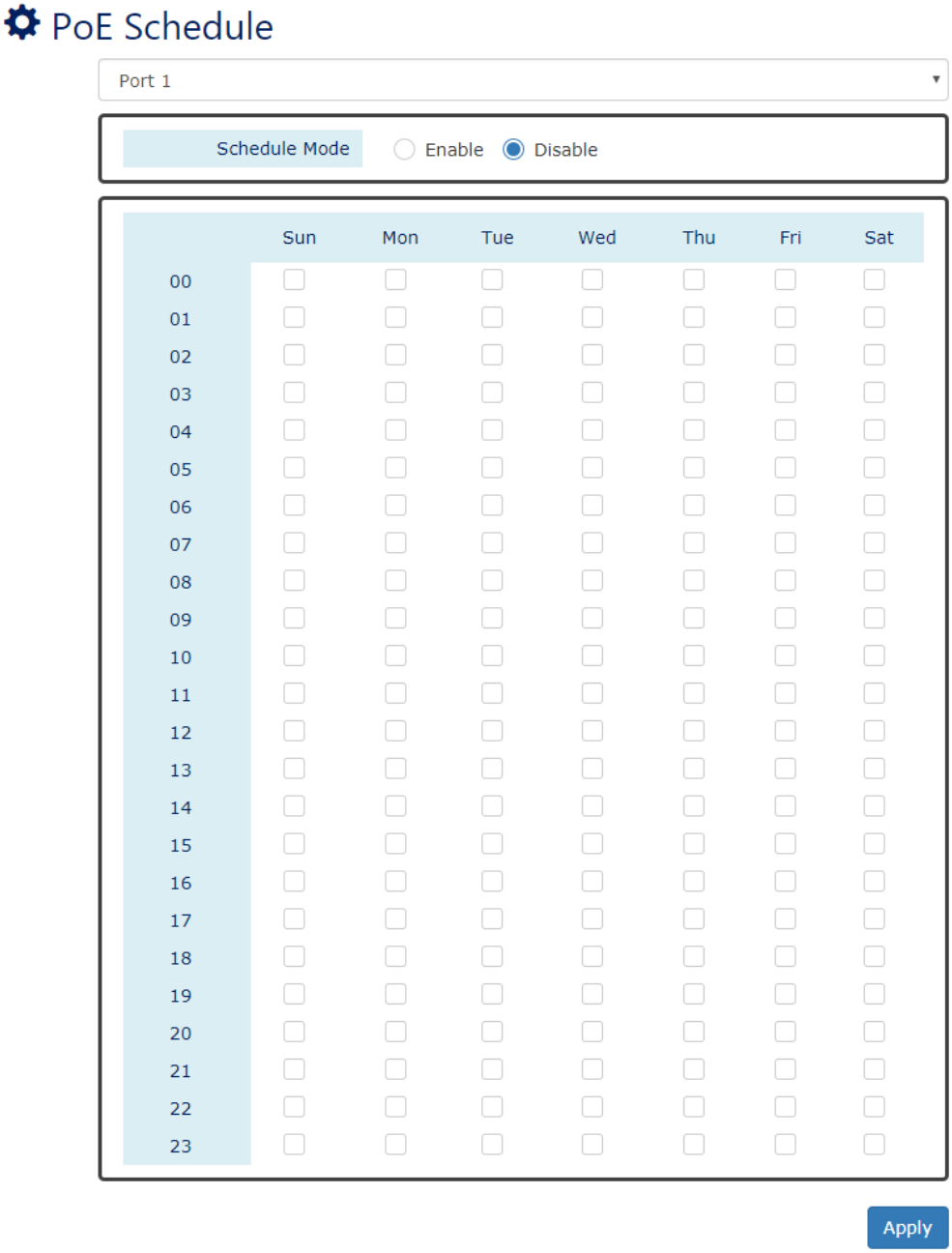
- **Hold Time**

  Время удержания. Если ping не проходит, система ждет окончания времени удержания и затем пробует связаться с PD снова. Диапазон от 1 to 65535 секунд. Значение по умолчанию - 60 секунд.

Apply (Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Настройка расписания работы PoE



- **Выпадающий список выбора порта**
  Выберите порт для настройки его расписания PoE. Номер порта коммутатора от 1 до N, где N определяется общим количеством портов модели коммутатора.
- **Schedule Mode**
  Включение или выключение применения расписания для данного порта.

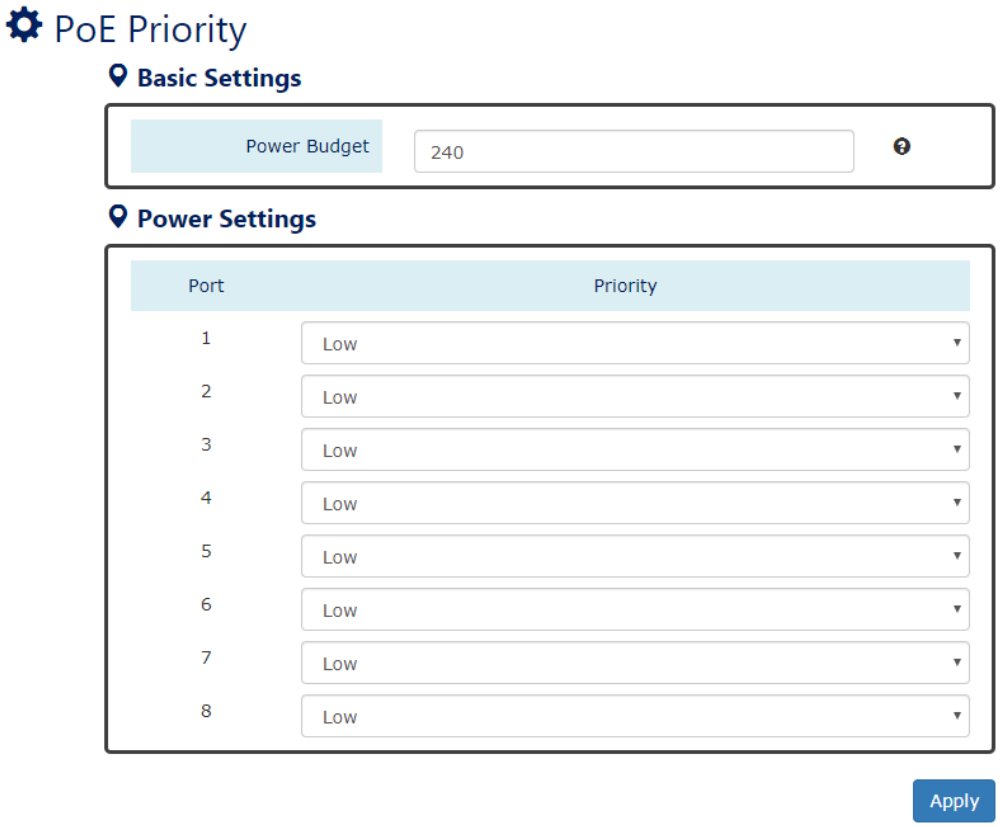
Каждый столбец в таблице – день недели, с воскресения до субботы. каждая строка – час суток, с 0 часов до 23 часов. Соответственно ставя флажки можно настроить: в какие часы каких дней недели должно подаваться PoE питание

Например, если пользователь хочет, чтобы PoE было включено только в понедельник с 6:00 до 7:00 и в среду с 13:00 до 15:00, необходимо установить следующие флажки - «Mon-06», «Mon-07», «Wed-13», «Mon-14», «Mon-15».

Apply (Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Настройка приоритета PoE на портах



Для более подробной информации наведите курсор мыши на иконку ?.

Базовые настройки - Basic Setting

- **Power Budget**

  Ограничение энергопотребления – максимальное энергопотребление всех PD. Диапазон значени от 1 до 240 Ватт. По умолчанию равен 240 Ватт.

Настройки питания - Power Settings

- **Port**

  Номер порта коммутатора от 1 до N, где N определяется общим количеством портов модели коммутатора.
- **Priority**

  Приоритет подачи PoE питания на порты: высокий high, средний -medium, низкий - low

Apply (Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Управление портами

Управление портами расположено в разделе меню «L2 Switching»

Настройка параметров портов

Port Settings

Port	Description	Link Status	Admin Status	Speed	Flow Control
1		Down	Enable	Auto	Off
2		Up	Enable	Auto	Off
3		Down	Enable	Auto	Off
4		Down	Enable	Auto	Off
5		Down	Enable	Auto	Off
6		Down	Enable	Auto	Off
7		Down	Enable	Auto	Off
8		Down	Enable	Auto	Off
9		Down	Enable	Auto	Off
10		Down	Enable	Auto	Off
11		Down	Enable	Auto	Off
12		Down	Enable	Auto	Off

Apply

Для более подробной информации наведите курсор мыши на иконку ?.

- **Port**

  Номер порта коммутатора от 1 до N, где N определяется общим количеством портов модели коммутатора.

- **Description**

  Описание порта. Помогает администратору определить разницу между портами. Максимальная длина описания составляет 32 символа. Примечание: #, \, ‘, «, ? не разрешены в этом поле.

- **Link Status**

  Поле показывает «Up», «Down» или «Disable», чтобы отразить состояние канала связи порта.

- **Admin Status**

  Административное состояние порта – Enable или Disable, чтобы ограничить передачу через порт. Примечание: администратор может отключить неиспользуемый порт, чтобы защитить сеть от неожиданного устройства.

- **Speed**

  Пользователи могут вручную установить скорость и дуплекс или автоматически запустить автосогласование, чтобы определить скорость и дуплекс для медных портов.

  - Auto: порт следует протоколу IEEE 802.3 для автоматического согласования с подключенным устройством.
  - 100M-Full: порт передает кадры со скоростью 100 Мбит / с в полнодуплексном режиме.
  - 100M-Half: порт передает кадры со скоростью 100 Мбит / с в полудуплексном режиме.
  - 10M-Full: порт передает кадры со скоростью 10 Мбит / с в полнодуплексном режиме.
  - 10M-Half: порт передает кадры со скоростью 10 Мбит / с в полудуплексном режиме.

Пользователи могут вручную настроить порты SFP, чтобы установить скорость и дуплекс. По умолчанию установлена максимальная скорость для слота SFP.

- Auto: порт следует протоколу IEEE 802.3 для автоматического согласования с подключенным устройством.
- 10G-Full (поддерживается только в моделях 10G) Порт передает кадры со скоростью 10 Гбит / с и в полнодуплексном режиме.
- 1G-Full: порт передает кадры со скоростью 1 Гбит / с в полнодуплексном режиме.
- 100 MB (поддерживается только на двухскоростных портах SFP) Порт передает кадры со скоростью 100 Мбит / с в полнодуплексном режиме.
- Copper-Full: выберите этот режим при использовании медного модуля SFP.

Примечание: настройте скорость порта на «1G-Full», если пользователям требуется поддержка VDSL2 SFP. Установите для скорости порта значение «Авто», если подключенное устройство является неуправляемым.

Для медного модуля SFP руководствуйтесь следующими правилами, чтобы настроить правильную скорость:

Тип медного SFP	Настройка порта	Примечание
SGMII (10/100/1000M)	Copper-Full	Поддерживает только передачу на 1000M
Multi-Speed (1G/10G)	10G-Full	Зависит от скорости соединения
10G	10G-Full	
1G / VDSL2	1G-Full	

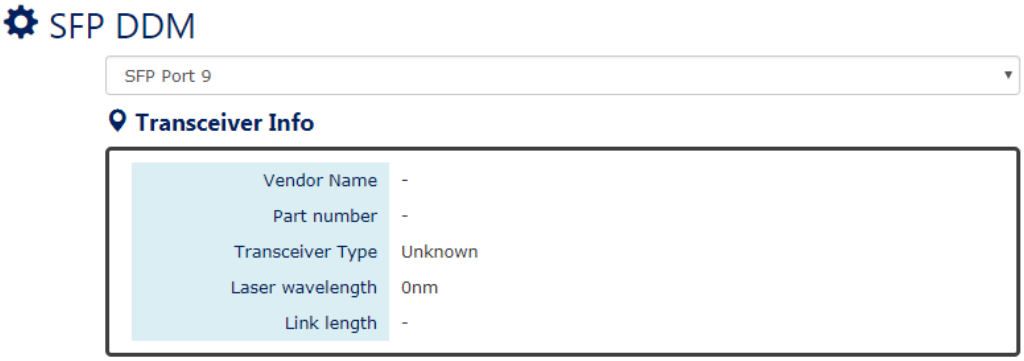
- **Flow Control**

  “Enable” или “Disable”. Включение Flow Control предотвращает потерю данных при большой нагрузке на порт.

(Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Информация о SFP DDM



- **Выпадающий список выбора SFP порта**

  Выберите поддерживающий SFP порт для просмотра информации о трансивере.

Информация о трансивере - Transceiver Info

Если модуль SFP не вставлен или информация не читается, в поле отображается «-».

- **Vendor Name**

  В этом поле отображается марка или название поставщика модуля SFP.
- **Part Number**

  В этом поле отображается название модели (код производителя) модуля SFP.
- **Transceiver Type**

  В этом поле отображается тип приемопередатчика модуля SFP, включая скорость передачи и тип волокна. Если модуль SFP не вставлен или тип трансивера не может быть прочитан, в поле будет отображаться «Unknown».

- **Laser Wavelength**

  В этом поле отображается рабочая длина волны лазера модуля SFP.
- **Link Length**

  В этом поле отображается максимальная протяженность линии для модуля SFP.

DDM Module

Real-Time Value

Temperature	57.000deg
Voltage	0.0mV
Current	0.000mA
Tx Power	0.0000mW
Rx Power	0.0000mW

Alarm Warning

	HI ALARM	HI WARNNING	LOW WARNNING	LOW ALARM
TEMP	57.000deg	0.000deg	0.000deg	0.000deg
VOLT	1459.2mV	0.0mV	0.0mV	0.0mV
CURR	29.184mA	0.000mA	0.000mA	0.000mA
TX PW	1.4592mW	0.0000mW	0.0000mW	0.0000mW
RX PW	1.4592mW	0.0000mW	0.0000mW	0.0000mW

Секция DDM Module

Этот раздел отображается только в том случае, если SFP DDM поддерживается на вставленном модуле SFP.

- **Real Time Value – текущие значения**

  Текущая рабочая информация, включая температуру, напряжение, ток, мощность Tx и мощность Rx.
- **Alarm Warning – аварии и предупреждения**

  Пороговое значение, настроенное по умолчанию для срабатывания сигнализации и системного предупреждения. Существует 5 типов информации (температура, напряжение, ток, мощность Tx и мощность Rx) и 4 уровня аварийных сигналов и предупреждений (аварийный сигнал / предупреждение о высоком уровне сигнала, аварийный сигнал / предупреждение о низком уровне).

Подробная информация о порте

Есть два метода получения подробной информации о порте. Один - из меню, второй – с изображения передней панели коммутатора. Пользователи могут напрямую щелкнуть порт на передней панели, и будут перенаправлены на страницу с подробной информацией о статусе конкретного порта. RMON - это набор данных на основе SNMP, который полезен для мониторинга и управления входящим и исходящим трафиком.

Detailed Port Status

Port 1

Received Packets

Rx Octets	210214768
Rx Unicast	0
Rx Multicast	431649
Rx Broadcast	1391
Rx Pause	0

Received Size Counter

Rx 64 Bytes	512514
Rx 65-127 Bytes	9572
Rx 128-255 Bytes	35690
Rx 256-511 Bytes	433090
Rx 512-1023 Bytes	19
Rx 1024-1518 Bytes	57136

Received Error Counter

Rx Collision	0
Rx CRC/Alignment	0
Rx Drop	0
Rx Fragment	0
Rx Jabber	0
Rx Oversize	0
Rx Undersize	0

Transmitted Packets

Tx Octets	108301443
Tx Unicast	17
Tx Multicast	531719
Tx Broadcast	83245
Tx Pause	0

Transmitted Error Counter

Tx Discard	0
Tx Error	0

- **Выпадающий список выбора порта**

  Выберите порт для просмотра его статистики. Номер порта коммутатора от 1 до N, где N определяется общим количеством портов модели коммутатора.

- **Received Packets**

  Rx Octets: общий полученный трафик в байтах.

  Rx Unicast: количество полученных одноадресных пакетов

  Rx Multicast: количество полученных многоадресных пакетов.

  Rx Broadcast: количество полученных широковещательных пакетов

  Rx Pause: количество пакетов управления MAC, полученных на конкретном интерфейсе с кодом операции, указывающим на операцию PAUSE.

- **Received Size Counter**

  Rx 64 Bytes: количество полученных пакетов размером 64 байта.

  Rx 65-127 Bytes: количество полученных пакетов размером от 65 до 127 байтов.

  Rx 128-255 Bytes: количество полученных пакетов размером от 128 до 255 байтов.

  Rx 256-511 Bytes: количество полученных пакетов размером от 256 до 511 байтов.

  Rx 512-1023 Bytes: количество полученных пакетов размером от 512 до 1023 байтов.

  Rx 1024-1518 Bytes: количество полученных пакетов размером от 1024 до 1518 байтов.

- **Received Error Counter**

  Rx Collision: общее количество конфликтов в сегменте Ethernet.

  Rx CRC/Alignment: общее количество принятых пакетов, которые имеют либо ошибку FCS с целым числом октетов (ошибка FCS), либо ошибку FCS с нецелым числом октетов (ошибка выравнивания).

  Rx Drop: общее количество пакетов, отброшенных из-за нехватки ресурсов.

  Rx Fragment: общее количество принятых пакетов, размер которых меньше 64 октетов и которые имели либо ошибку FCS.

  Rx Jabber: общее количество принятых пакетов, длина которых превышает 1518 октетов и которые имели ошибки FCS.

  Rx Oversize: общее количество полученных пакетов, длина которых превышает 1518 октетов.

  Rx Undersize: общее количество полученных пакетов размером менее 64 октетов.

- **Transmitted Packets**

  Tx Octets: общий переданный трафик в байтах.

  Tx Unicast: количество переданных одноадресных пакетов.

  Tx Multicast: количество переданных многоадресных пакетов.

  Tx Broadcast: количество переданных широковещательных пакетов.

  Tx Pause: количество пакетов управления MAC, переданных через определенный интерфейс с кодом операции, указывающим на операцию PAUSE.

- **Transmitted Error Counter**

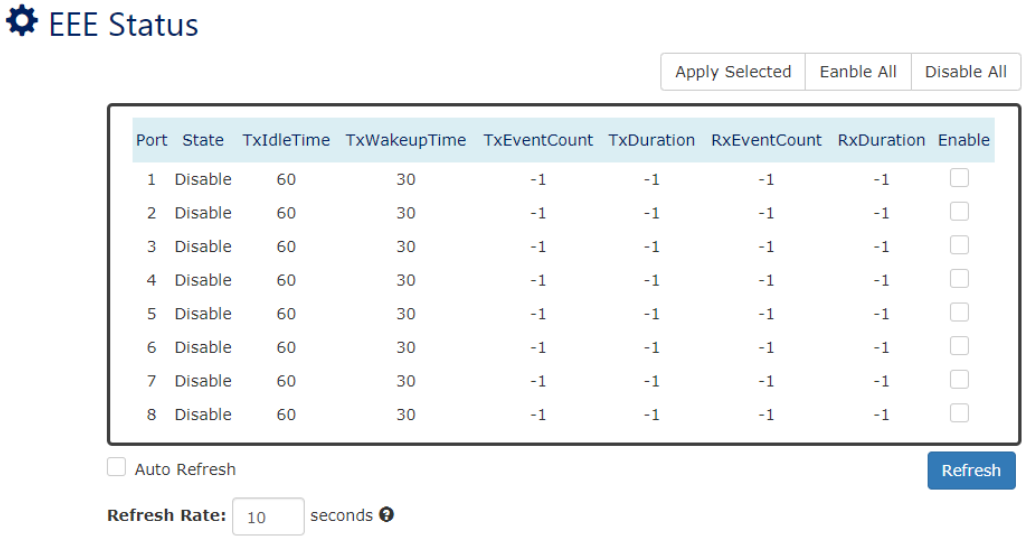
  Tx Discard: количество исходящих пакетов, которые выбраны для отбрасывания, даже

если ошибок не было обнаружено. Одна из возможных причин для отбрасывания такого пакета может заключаться в освобождении буферного пространства.

Tx Error: количество исходящих пакетов, которые не удалось передать из-за ошибок.

Информация о состоянии EEE

Energy-Efficient Ethernet (EEE) - это функция экономии электроэнергии, когда канал неактивен, когда порт подключен, но по каналу нет трафика. Функцию EEE можно включить или отключить в зависимости от порта.



Port	State	TxIdleTime	TxWakeupTime	TxEventCount	TxDuration	RxEventCount	RxDuration	Enable
1	Disable	60	30	-1	-1	-1	-1	
2	Disable	60	30	-1	-1	-1	-1	
3	Disable	60	30	-1	-1	-1	-1	
4	Disable	60	30	-1	-1	-1	-1	
5	Disable	60	30	-1	-1	-1	-1	
6	Disable	60	30	-1	-1	-1	-1	
7	Disable	60	30	-1	-1	-1	-1	
8	Disable	60	30	-1	-1	-1	-1	

- **Port**

  Номер порта коммутатора от 1 до N, где N определяется общим количеством портов модели коммутатора.
- **State**

  Состояние функцииEEE на порту. Enable – включена, Disable - выключена.
- **TxIdleTime**

  Время простоя перед входом в режим энергосбережения.
- **TxWakeupTime**

  Минимальное время до выхода из режима энергосбережения.
- **TxEventCount**

  TxEventCount - это счетчик событий EEE Low Power Idle (LPI) для передачи. Этот счетчик показывает, сколько раз режим LPI был принудительно активирован функцией EEE на передающей стороне.
- **TxDuration**

  TxDuration - это продолжительность событий LPI на передаче, которая обновляется, если порт находится в режиме EEE LPI.

- **RxEventCount**

  RxEventCount - это счетчик событий EEE Low Power Idle (LPI) для приема. Этот счетчик показывает, сколько раз режим LPI был принудительно активирован функцией EEE на принимающей стороне.

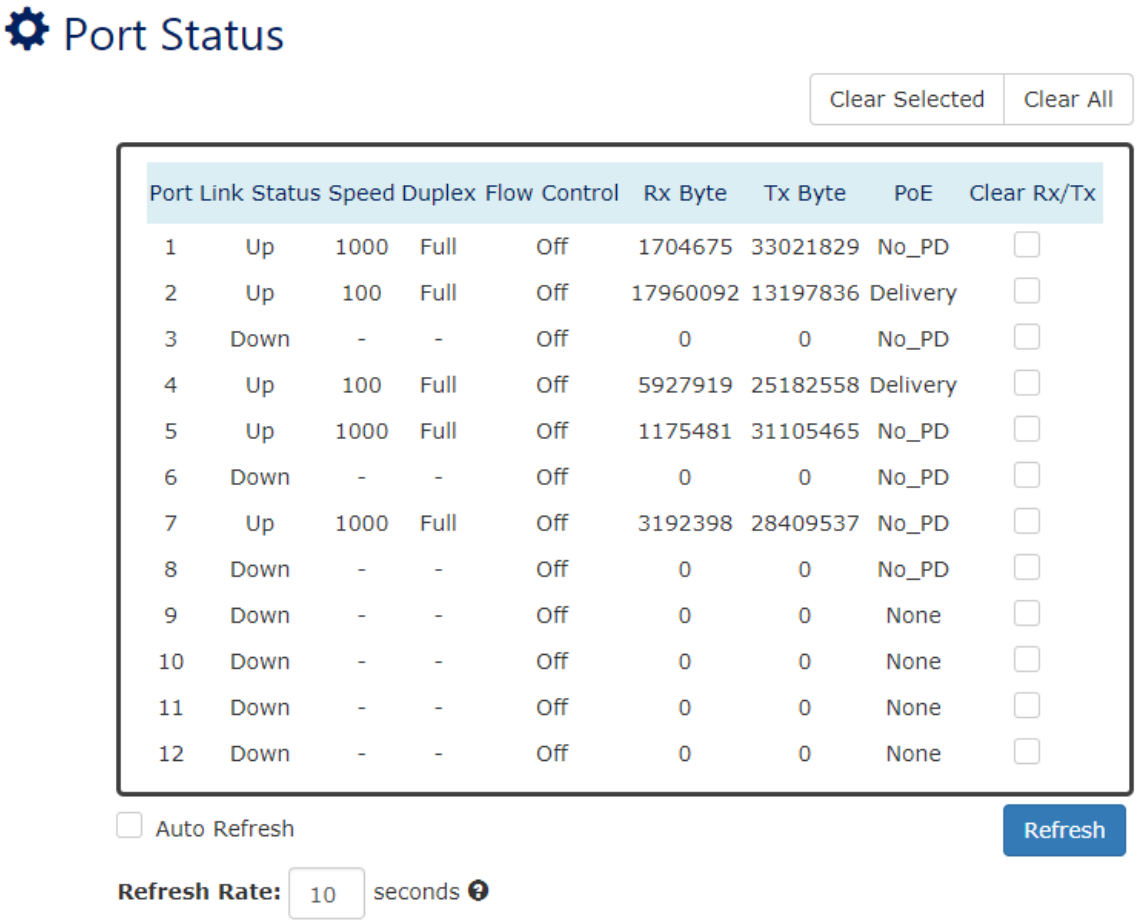
- **RxDuration**

  RxDuration - это продолжительность событий LPI на приеме, которая обновляется, если порт находится в режиме EEE LPI.

- **Enable**

  Выберите определенные порты или отмените выбор выбранных портов, а затем нажмите кнопку «Apply selected», чтобы включить или отключить функцию EEE. Нажмите «Enable all», чтобы включить функцию EEE на всех портах, или «Disable all», чтобы отключить функцию EEE на всех портах.

Информация о состоянии портов



Port	Link Status	Speed	Duplex	Flow Control	Rx Byte	Tx Byte	PoE	Clear Rx/Tx
1	Up	1000	Full	Off	1704675	33021829	No_PD	
2	Up	100	Full	Off	17960092	13197836	Delivery	
3	Down	-	-	Off	0	0	No_PD	
4	Up	100	Full	Off	5927919	25182558	Delivery	
5	Up	1000	Full	Off	1175481	31105465	No_PD	
6	Down	-	-	Off	0	0	No_PD	
7	Up	1000	Full	Off	3192398	28409537	No_PD	
8	Down	-	-	Off	0	0	No_PD	
9	Down	-	-	Off	0	0	None	
10	Down	-	-	Off	0	0	None	
11	Down	-	-	Off	0	0	None	
12	Down	-	-	Off	0	0	None	

- **Port**

  Номер порта коммутатора от 1 до N, где N определяется общим количеством портов модели коммутатора.

- **Link Status**

  Отображает состояние канала на порте («Up» или «Down») of the port. Если порт принудительно отключен показывается статус “Disabled”.
- **Speed**

  Отображает скорость на порту в битах в секунду. Если на порту нет канала связи, отображается «-».
- **Duplex**

  отображает тип канала (полнодуплексный или полудуплексный) порта. Если канала связи нет, отображается «-».
- **Flow Control**

  Состояние (вкл/выкл) Flow Control.
- **Rx Byte**

  Общее количество принятых на порту байтов.
- **Tx Byte**

  Общее количество переданных на порту байтов.
- **PoE**

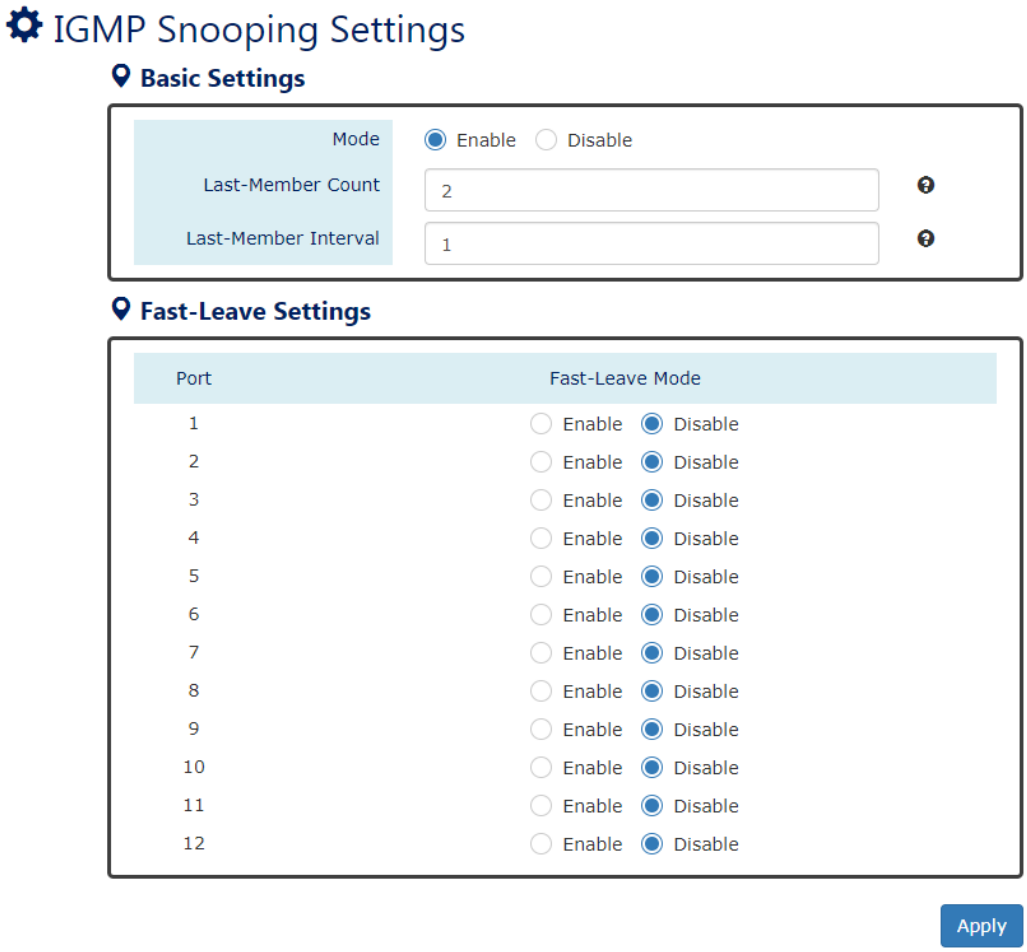
  Отображает состояние PoE (Delivery, No PD, Disabled, None) порта. Если порт не поддерживает функцию PoE, отображается «Нет». Примечание. Эта информация отображается в системе, которая поддерживает функцию PoE.
- **Clear Rx/Tx**

  Выберите определенные порты и нажмите кнопку «Clear Selected», чтобы очистить статистику приема-передачи для этих портов, или нажмите кнопку «Click All», чтобы очистить статистику всех портов.

Мультикаст, IGMP Snooping

Internet Group Management Protocol (IGMP) используется для связи между хостами и установления членства в группах многоадресной рассылки в сетях IPv4 (уровень 3). IGMP предоставляет возможность ограничивать многоадресный трафик только для тех, кому он нужен, и сокращать объем трафика в сети. Однако коммутаторы работают на уровне MAC (уровень 2) и не могут получать информацию IGMP. IGMP Snooping позволяет коммутатору прослушивать обмен данными IGMP между хостами и маршрутизаторами, а также поддерживает таблицу IP-адресов многоадресной рассылки и членов группы. IGMP Snooping может препятствовать тому, чтобы узлы в локальной сети получали трафик от не присоединившейся группы многоадресной рассылки, и экономить полосу пропускания сети..

Настройка IGMP Snooping



Для более подробной информации наведите курсор мыши на иконку ?.

Базовые настройки - Basic Setting

- **Mode**

  Включение работы IGMP Snooping. Включение – Enable, выключение - Disable.

- **Last-Member Count**
  Счетчик количества раз, когда маршрутизатор отправляет сообщения запроса IGMP для получения сообщения Leave-message. Диапазон составляет от 2 до 10. По умолчанию равен 2.
- **Last-Member Interval**
  Интервал отправки запроса IGMP query. Диапазон составляет от 1 до 25 секунд. По умолчанию равен 1 секунде.

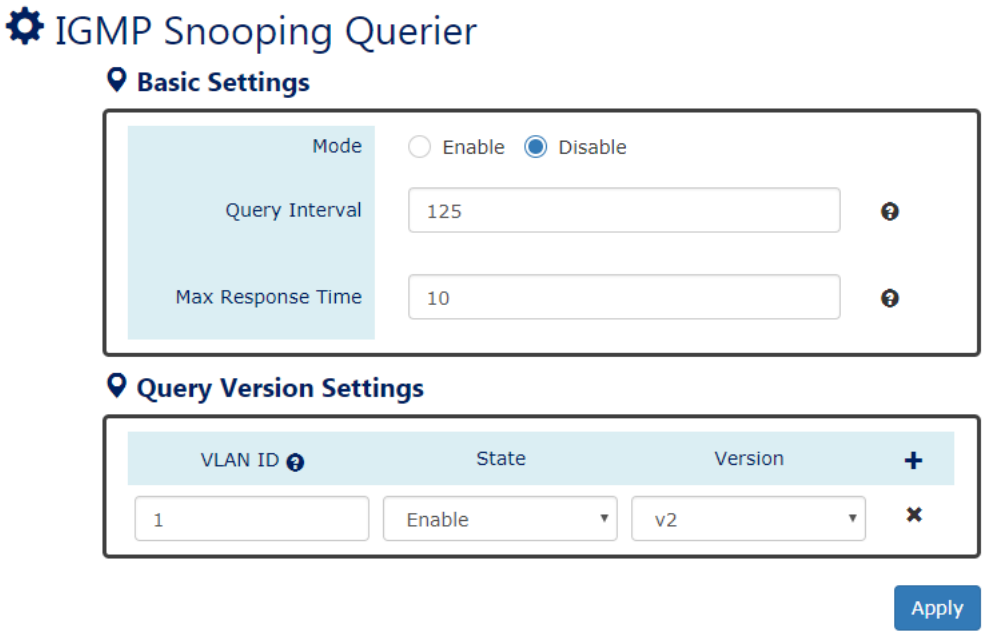
Настройки Fast-Leave Setting

- **Port**
  Номер порта коммутатора от 1 до N, где N определяется общим количеством портов модели коммутатора.
- **Fast-Leave Mode**
  Включите или отключите функцию быстрого выхода (fast-leave) на конкретном порту. Если на порту включен режим быстрого выхода, коммутатор закроет многоадресный поток при получении сообщения о выходе на этот порт без дальнейших действий.

Apply (Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Настройка IGMP Snooping Querier



Для более подробной информации наведите курсор мыши на иконку ?.

Базовые настройки - Basic Settings

- **Mode**

  Включение работы IGMP Snooping. Включение – Enable, выключение - Disable. При включении, системы рассылает запросы IGMP snooping версий 1 и 2.
- **Querier Interval**

  Интервал времени рассылки запросов IGMP snooping. Диапазон значений от 1 до 3600 секунд. Значение по умолчанию 125 секунд.
- **Query Max Response Time**

  Это таймер для ожидания ответа участников групп IGMP. Он используется для удаления информации о группах IGMP, если ни один из участников не отвечает на запрос.

Query Version Settings

Параметры версии запроса настраиваются отдельно для запросов в каждом VLAN

- **VLAN ID**

  Это поле предназначено для заполнения идентификатора VLAN для настройки версии запроса IGMP Snooping.
- **State**

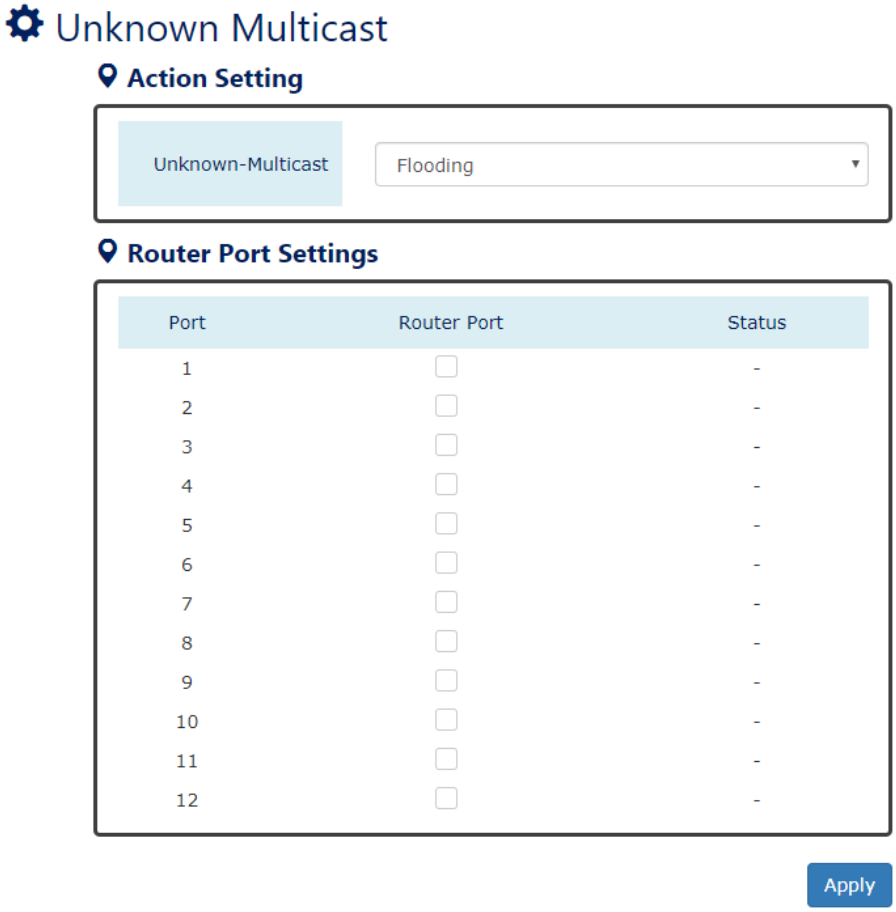
  Включить или отключить запрос IGMP Snooping для настроенного идентификатора VLAN.
- **Version**

  Установите версию IGMP Snooping (v1, v2c, v3) для конкретного VLAN.

(Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Настройка обработки Unknown Multicast



Настройка действия - Action Settings

- **Unknown-Multicast**

  Настройте действие при получении системой неизвестного многоадресного пакета.

  Flooding: лавинная рассылка неизвестного многоадресного пакета на все другие порты.

  Discarding: отбросить неизвестный многоадресный пакет.

  Router: пересылать неизвестный многоадресный пакет на порт маршрутизатора.

Router Port Settings

- **Port**

  Номер порта коммутатора от 1 до N, где N определяется общим количеством портов модели коммутатора.

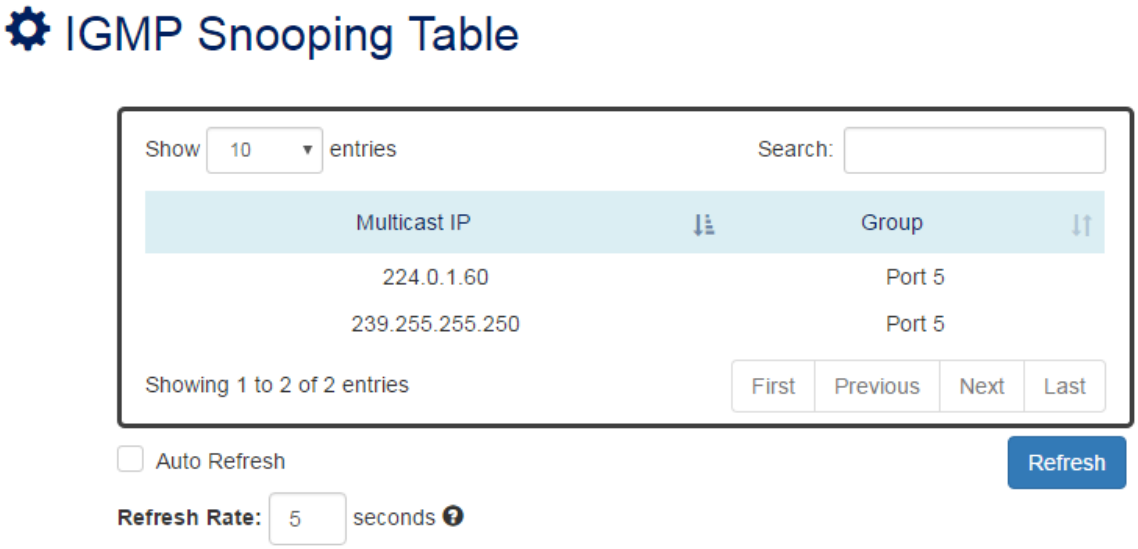
- **Router Port**

  Назначить данный порт маршрутизатором.

- **Status**

  В поле статуса отображается статус порта, где «-» означает, что это не порт маршрутизатора, а «статический» означает установленный порт маршрутизатора.

Просмотр таблицы IGMP Snooping



- **Multicast IP**

  IP-адрес группы многоадресной рассылки.

- **Group**

  В группе отображается номер порта, который вошел в группу.

Настройка VLAN (802.1Q)

Общие понятия

802.1Q VLAN

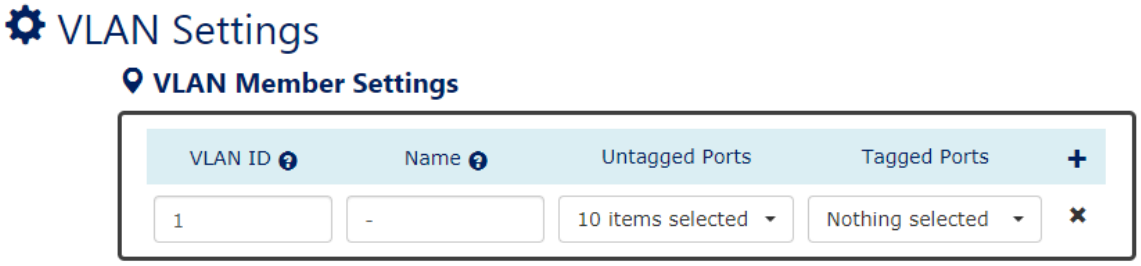
Виртуальная локальная сеть (VLAN) - это структура, которая может упростить планирование сети. Устройства в VLAN могут быть расположены где угодно без ограничения физических подключений, но работают так, как будто они находятся в одном физическом сегменте.

IEEE 802.1Q определяет концепцию маркировки VLAN для кадров Ethernet. Маркировка VLAN поддерживает кадры в различных группах VLAN, передаваемых по групповому каналу (так называемый транк VLAN). Максимальное количество VLAN в сети Ethernet - 4096. VLAN 0 и VLAN 4095 предназначены для конкретного использования, и, следовательно, максимальный используемый номер VLAN - 4094.

VLAN Q-in-Q

VLAN Q-in-Q, также называемая Stacked VLAN, является расширением 802.1Q VLAN. Он поддерживает максимум 4096 * 4096 групп VLAN. VLAN Q-in-Q может применяться на порту к трафику провайдера, заказчика или создавать туннель для различных приложений. Заголовок составного кадра VLAN содержит два заголовка 802.1Q с разными типами Ethertype (TPID). TPID «0x88A8» является внешним тегом по умолчанию, а TPID «0x8100» является внутренним тегом для 802.1Q VLAN. Индивидуальный Ethertype так же поддерживается, если для одного или нескольких портов установлено значение «Specific Provider»

Настройка 802.1Q VLAN



Для более подробной информации наведите курсор мыши на иконку ?.

VLAN Member Settings

- **VLAN ID**

  Назначает уникальный идентификатор VLAN этой группе VLAN. Диапазон идентификаторов VLAN от 1 до 4094.

- **Name**

  Назначает имя этой группе VLAN для идентификации различных VLAN. Макс. длина имени составляет 32 символа. Примечание: #, \, ‘, «, ? не разрешены в этом поле.

- **Untagged Ports**

  Устанавливает нетегированные порты для этой группы VLAN. Система удаляет тег VLAN перед передачей кадра с порта, для которого установлено значение «untagged». Обычно этот порт подключен к конечному устройству, которое принадлежит этой VLAN.

- **Tagged Ports**

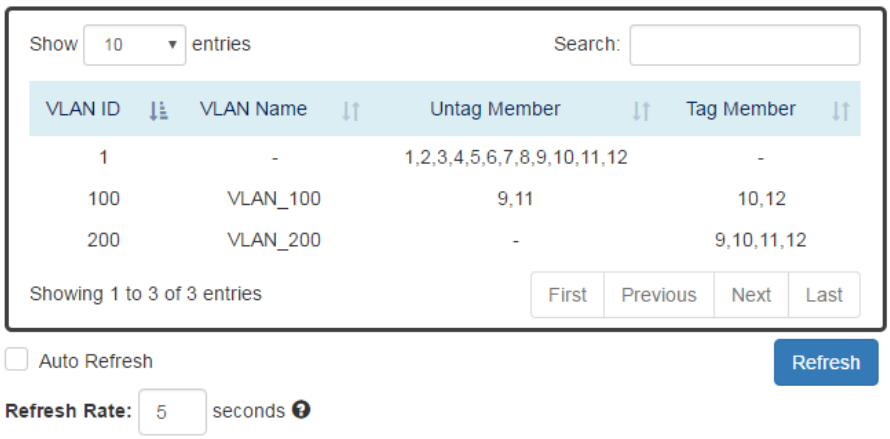
  Устанавливает тегированные порты для этой группы VLAN. Система сохраняет тег VLAN при передаче с порта, для которого установлено значение «tagged». Обычно этот порт подключен к другому коммутатору и использует тег VLAN для передачи информации о VLAN.

✚: Щелкните значок плюса, чтобы добавить строку участника VLAN.

✖: Щелкните значок удаления, чтобы удалить строку участника VLAN.

Таблица существующих VLAN

VLAN Table



- **VLAN ID**

  Это назначенный уникальный идентификатор VLAN для данной группы VLAN.

- **VLAN Name**

  Это назначенное имя VLAN для данной группы VLAN.

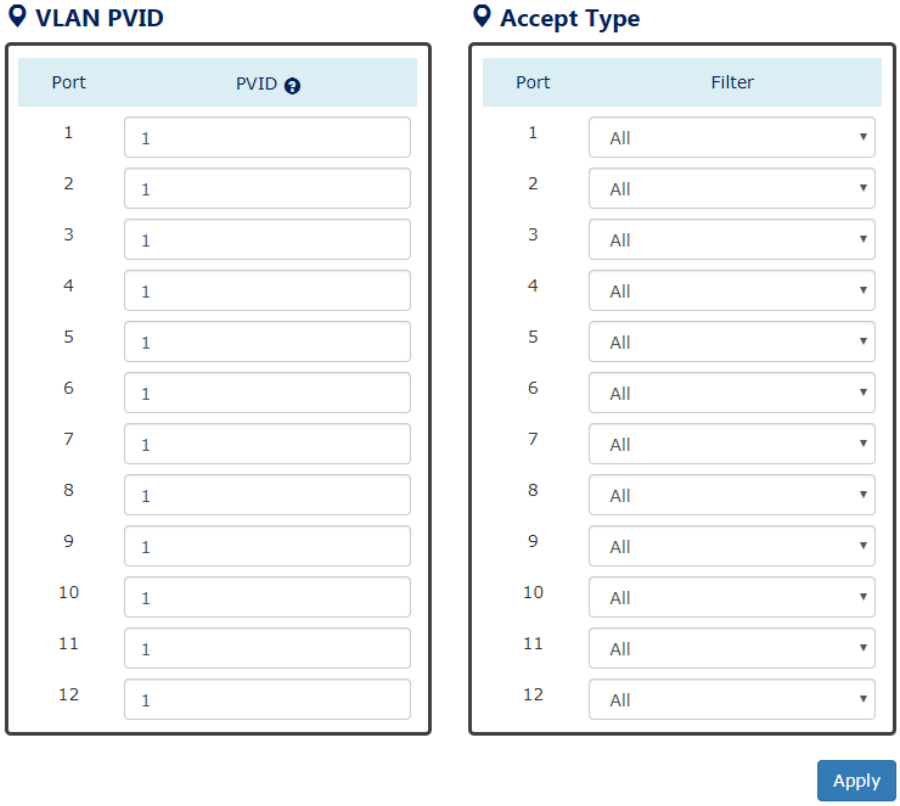
- **Untag Member**

  Эти порты назначаются как нетегированные порты VLAN.

- **Tag Member**

  Эти порты назначаются как тегированные порты VLAN.

Настройка режима работы портов VLAN и PVID



Для более подробной информации наведите курсор мыши на иконку ?.

VLAN PVID

- **Port**

  Номер порта коммутатора от 1 до N, где N определяется общим количеством портов коммутатора.
- **PVID**

  Назначьте идентификатор VLAN кадрам без тега VLAN, которые поступают на порт.

Accept Type

- **Port**

  Номер порта коммутатора от 1 до N, где N определяется общим количеством портов модели коммутатора.
- **Filter**

  Есть три типа фильтров: All, Tagged Only, Untagged Only.

  All: Прием как тегированных, так и не тегированных кадров приходящих на порт

  Tagged Only: Прием только тегированных кадров приходящих на порт.

  Untagged Only: Прием только не тегированных кадров приходящих на порт.

Apply (Применить)

После настройки данных нажмите кнопку Apply что бы изменения были активированы.

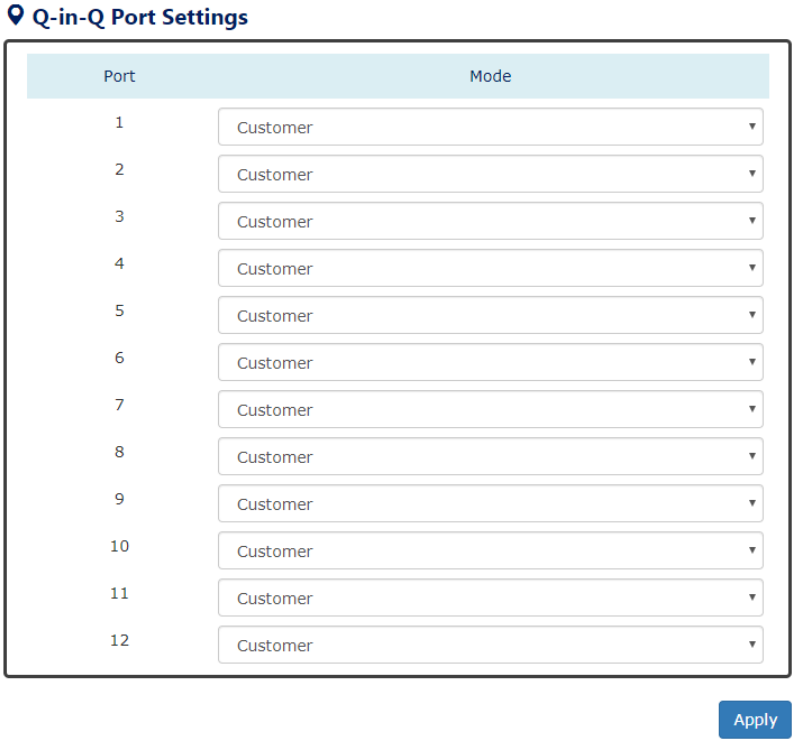
Настройка VLAN Q-in-Q

Для более подробной информации наведите курсор мыши на иконку ?.

Specific Provider Ethertype

Это глобальная настройка, и Ethertype назначается для всех портов, которые настроены как «Specific Provider». Это поле заблокировано (отключено) до тех пор, пока хотя бы один порт не будет настроен как «Specific Provider» в разделе «Настройки порта Q-in-Q».

Диапазон Ethertype провайдера составляет от 0x0000 до 0xFFFF, но 0x8100 недействителен. Значение по умолчанию - 0x88A8.



Настройка портов Q-in-Q - Q-in-Q Port Settings

- **Port**

  Номер порта коммутатора от 1 до N, где N определяется общим количеством портов коммутатора.

- **Mode**

  Установите порт в один из режимов Q-in-Q. Тип передачи зависит от подключенного устройства, поэтому действие при передаче (Eggress action) пропускается.

Режим	Действие на приеме (Ingress action)
Q-in-Q Tunnel	Не тегированные кадры: добавить тег TPID:0x88A8 и переслать. Тегированные кадры: — TPID:0x8100: добавить тег TPID:0x88A8 и переслать. — TPID:0x88A8: переслать кадры.
Customer	Порт установленный в “Customer” – обычный 802.1Q VLAN. Не тегированные кадры: добавить тег TPID:0x8100 и переслать. Тегированные кадры: — TPID:0x8100: ○ Тот же VLAN ID: переслать кадры. ○ Другой VLAN ID: отбросить кадры. — TPID:0x88A8: отбросить кадры.
Provider	Не тегированные кадры: добавить тег TPID:0x88A8 и переслать. Тегированные кадры: — TPID:0x8100: отбросить кадры. — TPID:0x88A8: ○ Тот же VLAN ID: переслать кадры. ○ Другой VLAN ID: отбросить кадры.
Specific Provider	Использует настроенный Ethertype. Не тегированные кадры: добавить пользовательский тег TPID и переслать. Тегированные кадры: — TPID:0x8100: отбросить кадры. — TPID:0x88A8: отбросить кадры. — TPID: [пользовательский]: ○ Тот же VLAN ID: переслать кадры. ○ Другой VLAN ID: отбросить кадры.

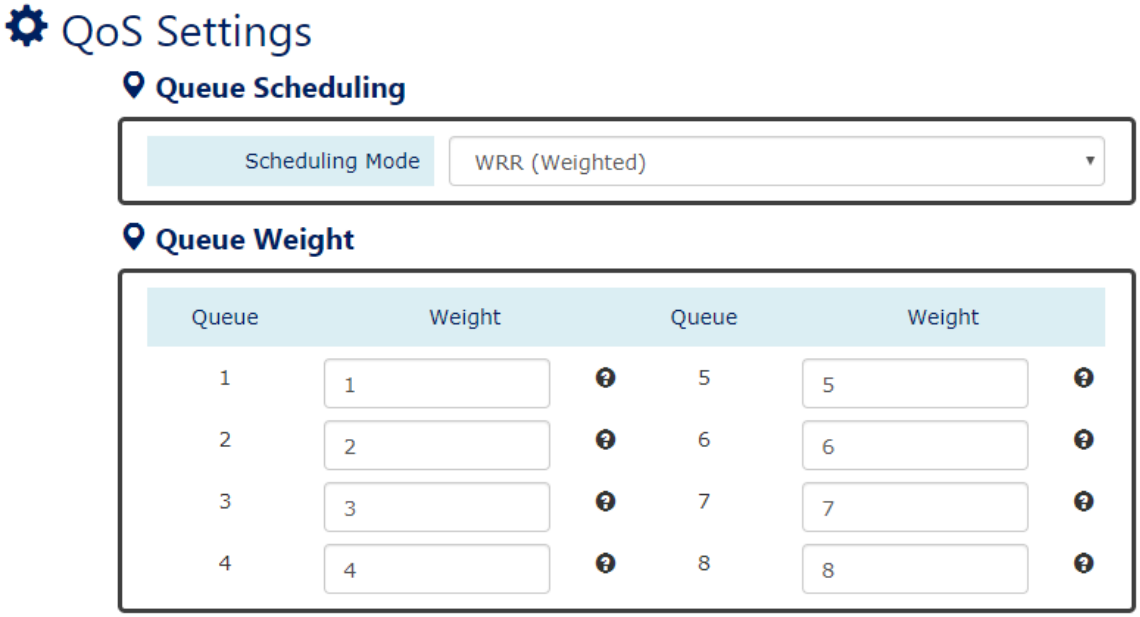
Apply (Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Управление качеством обслуживания (QoS)

Качество обслуживания, известное как QoS, обеспечивает стабильную и предсказуемую услугу передачи. Дает возможность более эффективно управлять полосой пропускания в зависимости от требований приложений. Пользователи могут устанавливать разные приоритеты для разных потоков, чтобы удовлетворить потребности служб, которым требуется фиксированная полоса пропускания и которые более чувствительны к задержкам. Качество обслуживания может также оптимизировать ресурс ограничения полосы пропускания и контролировать сетевой трафик коммутаторов.

Базовые настройки QoS



Для более подробной информации наведите курсор мыши на иконку ?.

Управление очередями - Queue Scheduling

- **Scheduling Mode**

  Выберите режим работы QoS.

  WRR: Weighted Round Robin. WRR гарантирует, что каждая очередь передает трафик пропорционально своему установленному весу.

  Strict: очередь со строгим приоритетом. Трафик передается в зависимости от приоритета, от наивысшего к низшему.

Веса очередей - Queue Weight

- **Queue**

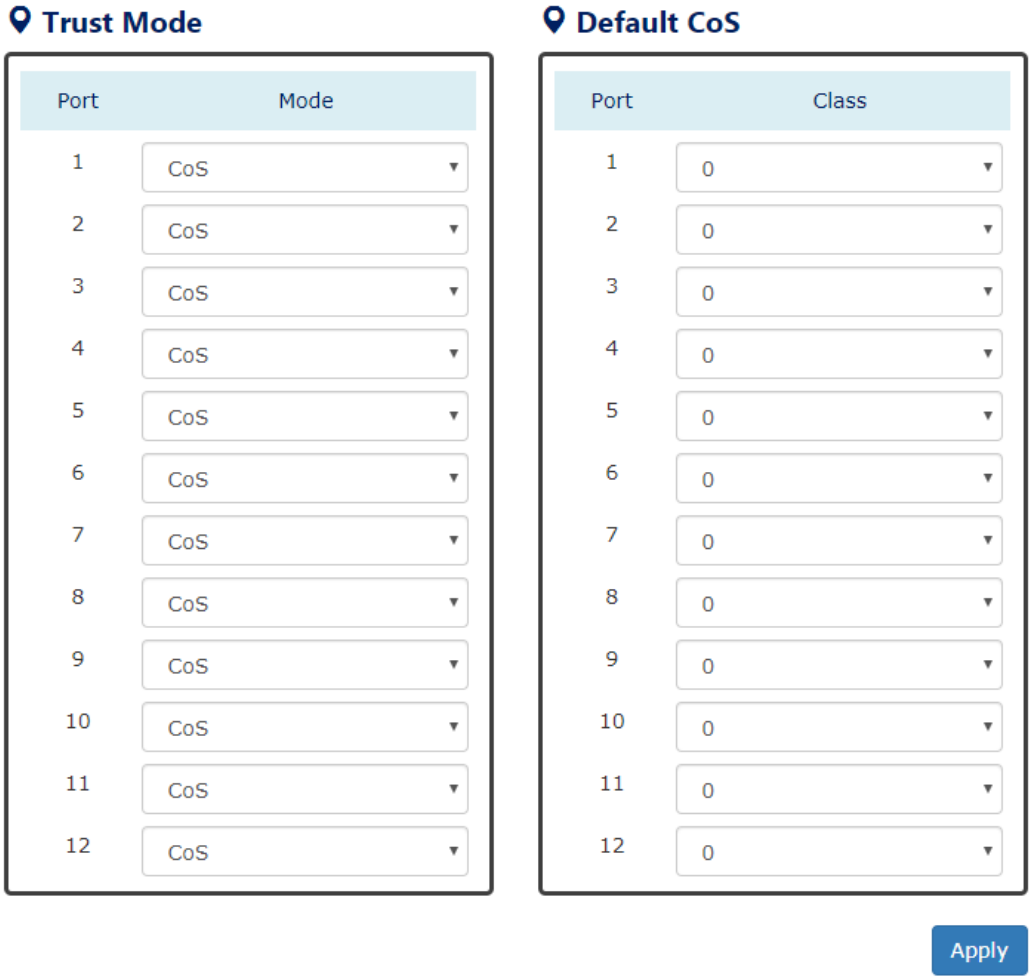
  Номер очереди. Поддерживаются восемь очередей от очереди 0 до очереди 7.

- **Weight**

  Позволяет вам настроить определенный вес для порта. Диапазон веса от 1 до 100. Нет необходимости суммировать все очереди до 100. Вес по умолчанию для каждой очереди отображается в таблице:

Номер очереди	0	1	2	3	4	5	6	7
Вес	1	2	3	4	5	6	7	8

Настройка типа классификации трафика и CoS



Режим доверия к параметрам QoS - Trust Mode

- **Port**

  Номер порта коммутатора от 1 до N, где N определяется общим количеством портов модели коммутатора.

- **Mode**

  CoS: Class of Service. Использовать 3 бита поля “PRI” в теге VLAN. Дает возможность назначать до 8 различных классов сервиса от 0 до 7.

DSCP: использовать 6 битное поле DSCP в поле Type of Service (ToS). Дает возможность назначать до 64 различных типов сервиса от 0 до 63.

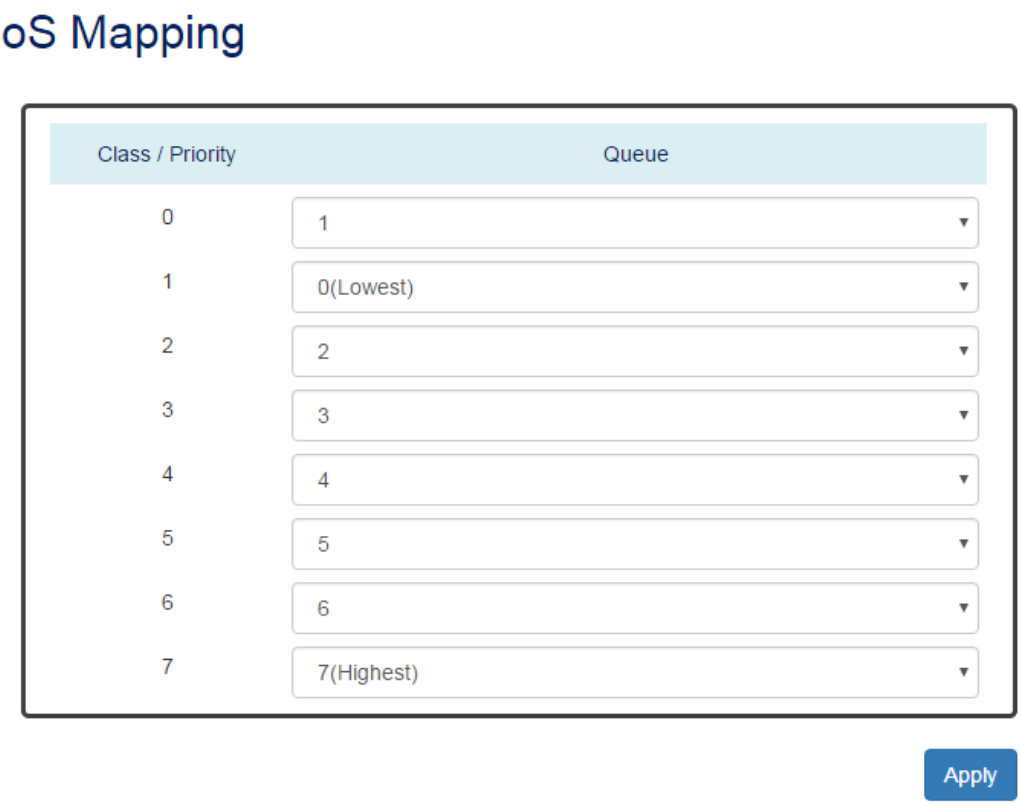
Класс сервиса по умолчанию - Default CoS

- **Port**
  Номер порта от 1 до N, где N определяется общим количеством портов коммутатора.
- **Class**
  Вы можете назначить порту класс по умолчанию. Система следует назначенным классам CoS для передачи кадров, если в заголовке кадра нет тега VLAN. Класс по умолчанию для порта - 0.

Apply (Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Настройка очередей для поля PRI



Сопоставление номера очереди со значением приоритета в поле PRI

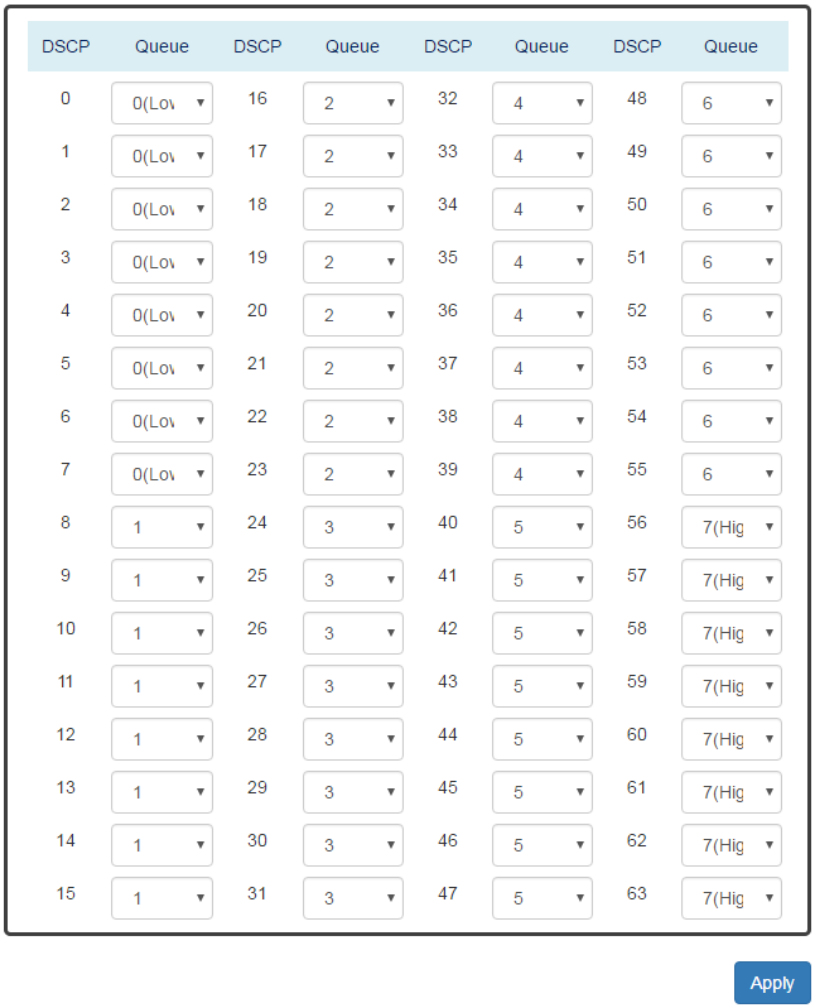
- **Class / Priority**
  В теге VLAN есть 3 бита PRI для определения класса обслуживания, и есть 8 классов от 0 до 7

- **Queue**

  Чипсет поддерживает 8 очередей от очереди 0 до очереди 7. Очередь 0 — это очередь с самым низким приоритетом, а очередь 7 - с самым высоким приоритетом. Очередь по умолчанию для каждого класса отображается в таблице:

Класс	0	1	2	3	4	5	6	7
Очередь	1	0	2	3	4	5	6	7

Настройка очередей для поля DSCP



- **DSCP**

  Поле DSCP(ToS) имеет длину 6 бит, и поэтому есть 64 типов сервиса от 0 до 63.

- **Queue**

  Чипсет поддерживает 8 очередей от очереди 0 до очереди 7. Очередь 0 — это очередь с самым низким приоритетом, а очередь 7 - с самым высоким приоритетом. Очередь по умолчанию для каждого класса отображается в таблице:

Тип	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63

Очерель	0	1	2	3	4	5	6	7

Apply (Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Транковые порты

Протокол транковых (магистральных) портов, также известный как агрегация каналов, представляет собой протокол формирования групповых каналов связи. Всего предусмотрено 8 транков. Это хороший метод для балансировки нагрузки и резервирования линий связи. Например, если порты с 1 по 4 объединены с транком 1, а все порты поддерживают FastEthernet и настроены на полнодуплексный режим, пропускная способность магистрали будет 800 Мбит/с. Трафик, передаваемый по магистрали, распределяется по одному из каналов на основе MAC-адреса источника для балансировки нагрузки. Когда режим транка установлен на LACP и когда один из каналов разрывается, трафик будет передаваться по другому каналу в группе.

Базовые настройки транков

Trunking Settings

Group	Trunking Mode	Member Ports
Trunk 1	LACP	Nothing selected
Trunk 2	LACP	Nothing selected
Trunk 3	LACP	Nothing selected
Trunk 4	LACP	Nothing selected
Trunk 5	LACP	Nothing selected
Trunk 6	LACP	Nothing selected
Trunk 7	LACP	Nothing selected
Trunk 8	LACP	Nothing selected

Apply

- **Group**

  Поддерживаются 8 транковых групп от Trunk 1 до Trunk 8.

- **Trunking Mode**

  Два режима транка доступны: «LACP» и «Static».

  Static: трафик передается по одной из линий связи в группе. Линия связи определяется MAC-адресом в заголовке кадра. Если линия разорвана, трафик не может передаваться по другим линиям в группе.

  LACP: он также известен как «динамический» транкинг. Если текущий канал передачи разорван, трафик может быть передан по другому каналу в группе.

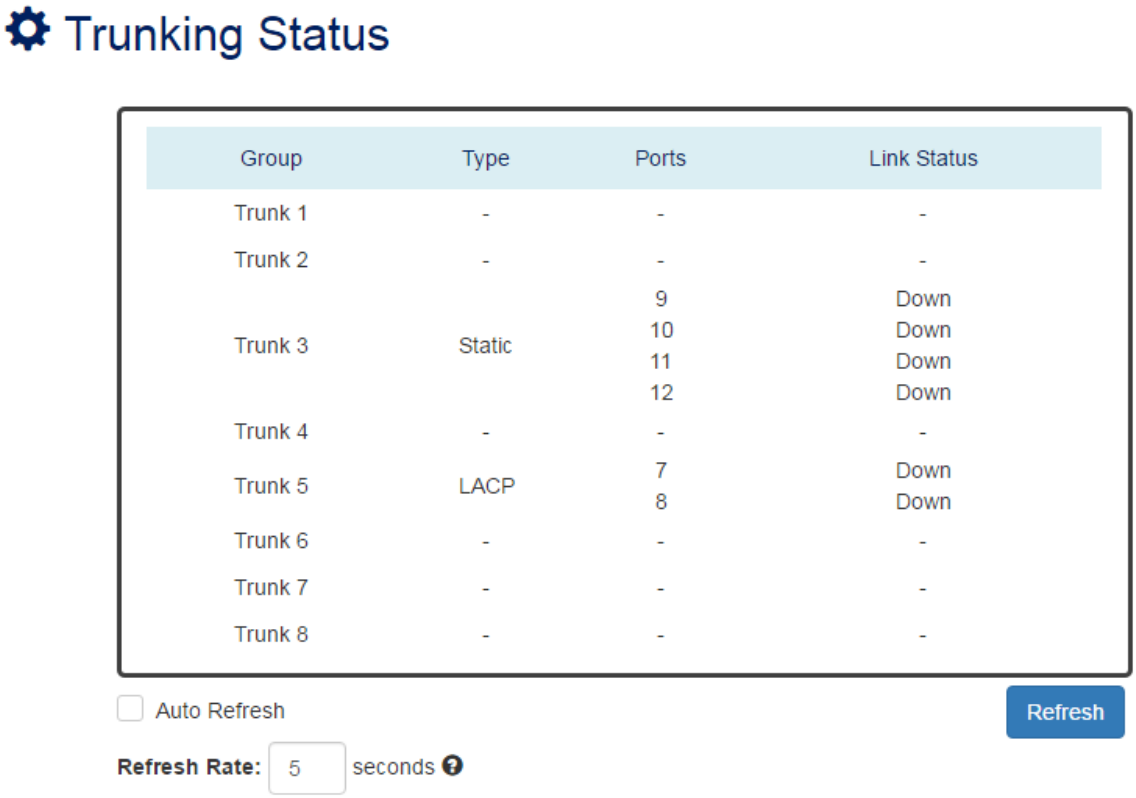
- **Member Ports**

  Выберите порты-участники, которые будут присоединены к указанной группе. Порт может быть только в одной из транковых групп. Каждая группа поддерживает максимум 8 участников.

(Применить)

После настройки данных нажмите кнопку Apply, что бы изменения были активированы.

Статус транков



- **Group**

  Поддерживаются 8 транковых групп от Trunk 1 до Trunk 8.

- **Type**

  Два режима транка доступны: «LACP» и «Static». В поле стоит“-“ когда у группы нет членов.

- **Ports**

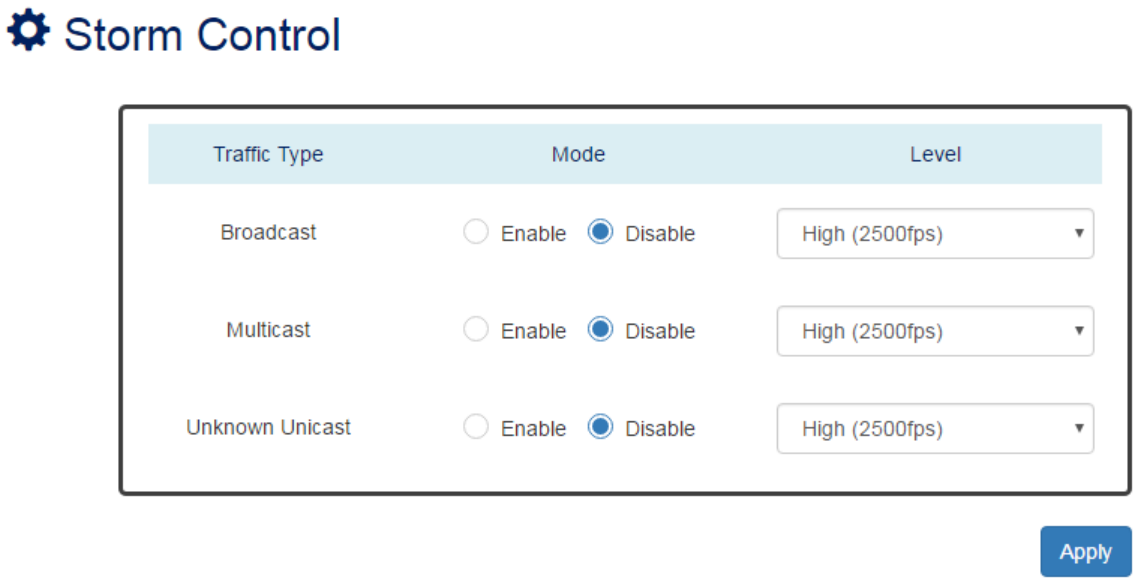
  Порты входящие в данную группу
- **Link Status**

  Состояние транка – up/down

Управление трафиком (storm control)

Пакетный шторм возникает, когда в локальную сеть поступает слишком много пакетов, что снижает производительность. Функция Storm Control используется для предотвращения выхода системы из строя из-за шторма широковещательного, многоадресного или неизвестного unicast трафика. Когда Storm Control включен для определенного типа трафика, система будет отслеживать входящий трафик. Если трафик превышает настроенный уровень, он будет отключен, чтобы избежать шторма.

Настройка управления трафиком



Traffic Type

В Storm Control поддерживаются три типа трафика: broadcast, multicast и unknown unicast.

- **Mode**

  Включение/выключение storm control для определенного вида трафика.
- **Level**

  Доступны три уровня количества кадров: высокий, средний и низкий. Если количество кадров определенного типа трафика превышает установленный уровень, система отбрасывает этот тип кадров, чтобы предотвратить отказ системы.

  High: высокий, более 2500 кадров в секунду.

  Mid: средний, более 1000 кадров в секунду.

  Low: низкий, более 500 кадров в секунду.

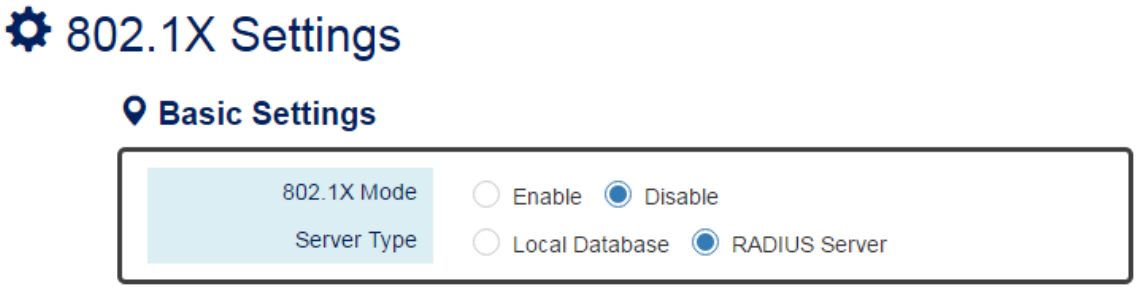
(Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Настройка доступа по 802.1X

802.1X — это стандарт IEEE для управления доступом к сети на порту коммутатора. Он обеспечивает безопасный механизм аутентификации для устройств, которые хотят подключиться к LAN или WAN. Протокол управления доступом к сети на основе портов является удобным методом для пользователей, поскольку аутентификация выполняется для каждого порта, и после того, как порт проходит аутентификацию, не требуется повторная аутентификация при переходе на другое устройство. В силу этого, для улучшения защищенности, обеспечивается так же метод управления доступом на основе MAC адресов. Это более безопасный, но менее удобный метод аутентификации. В сети можно добавить только устройство с MAC-адресом, прошедшее аутентификацию. Эти два метода не являются обязательными для каждого порта, и пользователи могут выбрать один из них на разных портах независимо от других.

Базовые настройки 802.1X



Для более подробной информации наведите курсор мыши на иконку ?.

Базовые настройки - Basic Settings

- **802.1X Mode**

  Включение работы 802.1X на коммутаторе. Включение – Enable, выключение - Disable.

- **Server Type**

  Выберите тип источника данных для аутентификации 802.1X: «Local Database» или «RADIUS Server».

  Local Database - локальная база данных хранится в таблице, хранящейся в коммутаторе. Клиент должен отправить имя пользователя и пароль для аутентификации в базе данных коммутатора.

  RADIUS Server - сервер RADIUS, база данных поддерживается на другом устройстве, на котором запущена служба RADIUS. Аутентификация следует протоколу RADIUS, включая связь и шифрование.

Настройка портов для 802.1X

Port Settings

Port	Enable	Mode	Re-Auth	Re-Auth Period
1	No	MAC-based	Yes	3600
2	No	MAC-based	Yes	3600
3	No	MAC-based	Yes	3600
4	No	MAC-based	Yes	3600
5	No	MAC-based	Yes	3600
6	No	MAC-based	Yes	3600
7	No	MAC-based	Yes	3600
8	No	MAC-based	Yes	3600
9	No	MAC-based	Yes	3600
10	No	MAC-based	Yes	3600
11	No	MAC-based	Yes	3600
12	No	MAC-based	Yes	3600

Для более подробной информации наведите курсор мыши на иконку ?.

Настройки портов - Port Settings

- **Port**

  Номер порта коммутатора от 1 до N, где N определяется общим количеством портов модели коммутатора.

- **Enable**

  Включать ли функцию 802.1X на порту. “Yes” означает, что 802.1X включена на порту и порт заблокирован до прохождения аутентификации подключенным на порт устройством.

- **Mode**

  Выбор режима работы 802.1X на порту: “Mac-based” или“Port-based”.

  Mac-based: Только MAC-адрес, прошедший аутентификацию, может подключаться к сетям.

  Port-based: Если порт прошел аутентификацию, каждое устройство, подключенное к порту, может подключаться к сетям.

- **Re-Auth**

  Включение повторной аутентификации на порту. “Yes” повторная аутентификация

включена и устройство должно проходить аутентификацию регулярно, сообразно настроенному периоду ре-аутентификации.

- **Re-Auth Period**

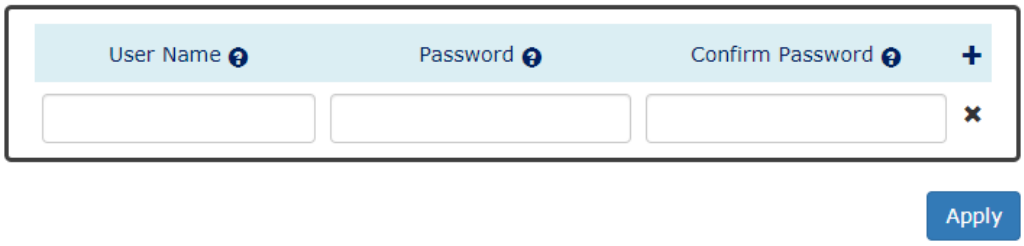
  Период ре-аутентификации в секундах.

Apply (Применить)

После настройки нажмите кнопку Apply, что бы изменения были активированы.

Настройка локальных пользователей

Local Database



Для более подробной информации наведите курсор мыши на иконку ?.

- **User Name**

  Имя пользователя, используемое для аутентификации. Максимальная длина 32 символа. Примечание: #, \, ‘, «, ? не разрешены в этом поле.

- **Password**

  Пароль пользователя, используемый для аутентификации. Максимальная длина 20 символов. Примечание: #, \, ‘, «, ? не разрешены в этом поле.

- **Confirm Password**

  Подтверждение пароля пользователя.

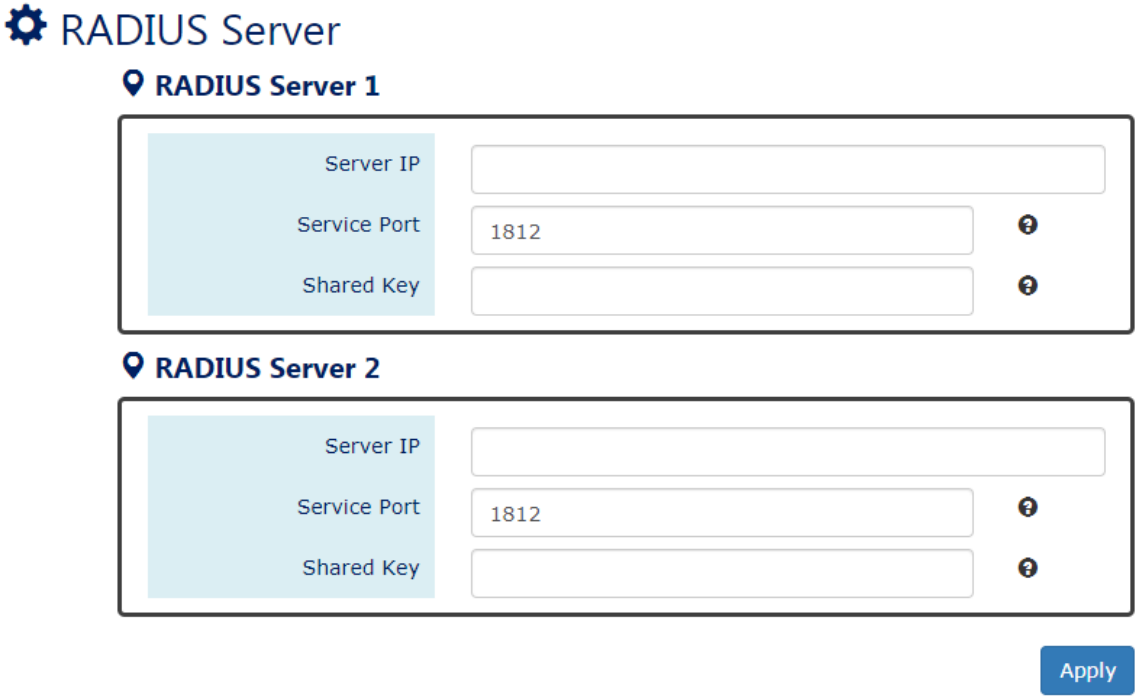
+: Щелкните значок плюса, чтобы добавить строку имени пользователя и пароля.

✖: Щелкните значок удаления, чтобы удалить строку имени пользователя / пароля.

Apply (Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Настройка параметров RADIUS сервера



Для более подробной информации наведите курсор мыши на иконку ?.

- **Server IP**

  IP адрес RADIUS сервера.

- **Service Port**

  Сервисный порт — это порт на сервере RADIUS.

- **Shared Key**

  Ключ используется для установления соединения между RADIUS сервером и аутентификатором перед началом аутентификации.

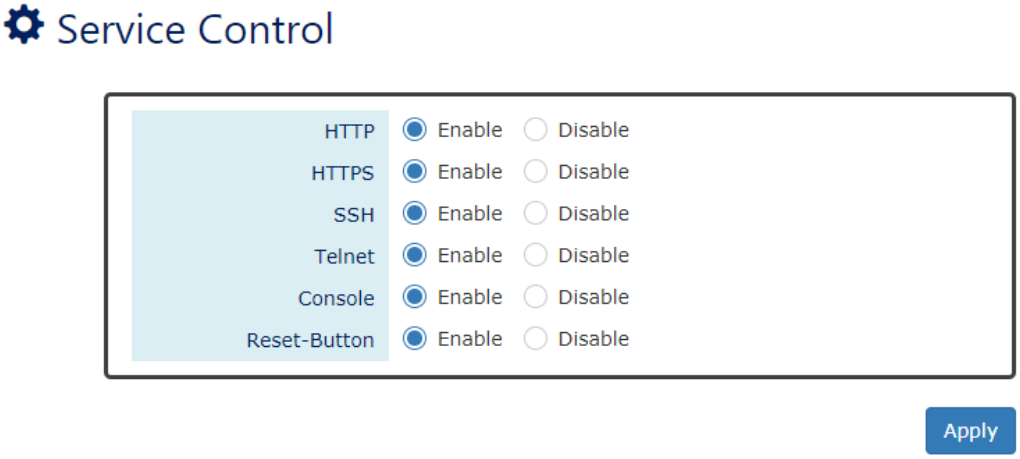
Apply (Применить)

После настройки нажмите кнопку Apply, что бы изменения были активированы.

Методы управления коммутатором

Мы предоставляем 5 типов доступа к управлению коммутатором: HTTP, HTTPS, SSH, Telnet и консольный порт. Пользователи могут настроить включение/отключение доступа к каждому типу управления. Кнопка Reset — это еще один способ перезагрузки или сброса настроек по умолчанию. Для нее также доступна возможность отключения доступа к ее функционалу. Все службы включены по умолчанию, и пользователи могут отключить неиспользуемые службы, чтобы сделать систему более безопасной.

Настройка методов управления



HTTP

Включите или отключите доступ к интерфейсу управления по протоколу HTTP, который является основой обмена данными во всемирной паутине (WWW).

HTTPS

Включите или отключите доступ к интерфейсу управления по протоколу HTTPS, который является адаптацией протокола HTTP для обеспечения безопасности. Связь будет зашифрована в HTTPS.

SSH

Включите или отключите доступ к интерфейсу управления по SSH, который является криптографическим сетевым протоколом. SSH обеспечивает безопасный канал через незащищенную сеть в архитектуре клиент-сервер. Коммутатор играет роль SSH-сервера, а хосты - SSH-клиента.

Telnet

Включите или отключите доступ к интерфейсу управления по Telnet, который представляет собой текстовое виртуальное терминальное соединение. Он менее безопасен, чем SSH, поскольку не шифрует данные, даже пароль, при передаче.

Console

Включите или отключите доступ к интерфейсу управления через последовательный консольный порт. Отключение консольного порта позволяет избежать неправильной настройки кем-либо, кто может получить доступ к устройству на месте.

Reset Button

Включите или отключите реакцию, когда пользователи нажимают кнопку Reset. Кнопка Reset обеспечивает различные функции, включая перезагрузку и восстановление заводских настроек по умолчанию. Отключение кнопки Reset - это защита от ошибочного или несанкционированного нажатия кнопки для перезагрузки системы или восстановления системы до состояния по умолчанию.

(Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Списки доступа (ACL)

Список управления доступом содержит правила для применения на всех сетевых портах. Входящий трафик проверяется относительно записей в таблице ACL. Каждая запись может быть записью MAC для адреса Layer 2 и записью IP для адреса Layer 3. Может проверяться как адрес источника, так и адрес назначения. Пользователь может настроить маску адреса, чтобы указать настройку группы адресов в одной записи. У записи есть два действия: разрешить или запретить передачу сетевых пакетов, соответствующих правилам ACL на другой порт.

Настройка списков доступа

```
Switch(config)# acl mac
Usage: acl mac [Index] [drop|permit] [SrcMac|DstMac] [Mac] [Mac_Mask]
<1-128> Index range
```

```
Switch(config)# acl ip
Usage: acl ip [Index] [drop|permit] [SrcIp|DstIp] [IP] [IP_Mask]
<1-128> Index range
```

Index

Номер записи в таблице ACL. Входящий пакет данных будет сравниваться со списками в порядке возрастания индексов. Диапазон индекса от 1 до 128.

Action

Действие

Drop: пакет должен быть отброшен, если соответствует правилу.

Permit: пакет должен быть передан, если соответствует правилу.

Address Type

Тип адреса

Src: Правило на основе адреса источника

Dst: Правило на основе адреса назначения

Address

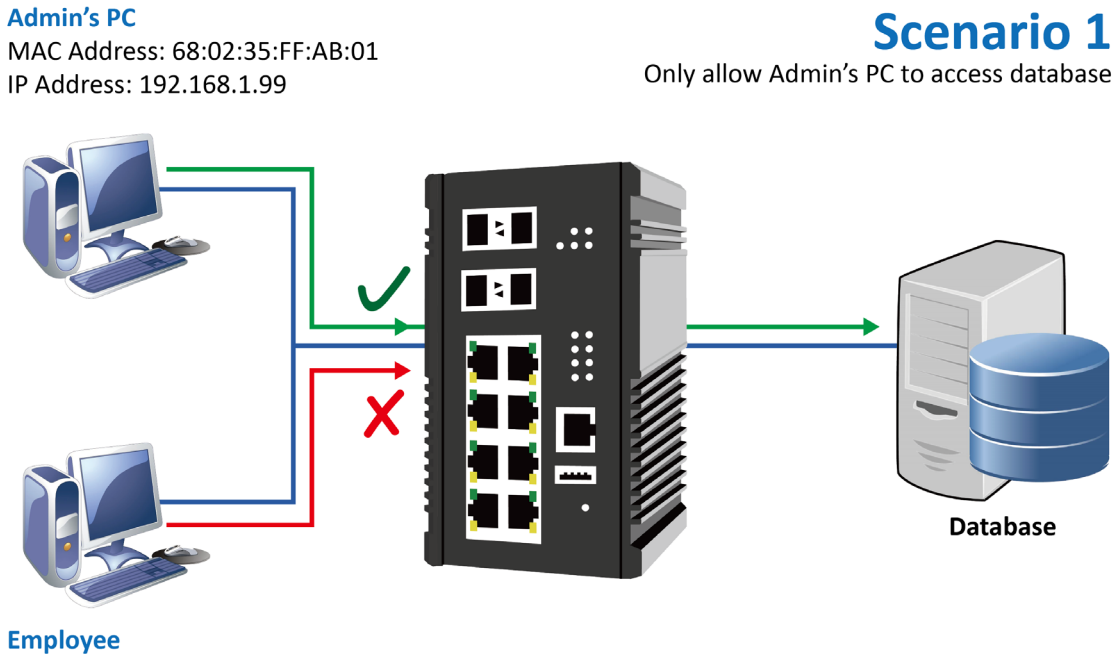
MAC адрес в формат с двоеточиями. Например: 00:80:C2:01:23:45

IP адрес в формате с точками. Например: 192.168.1.123

Address Mask

Битовая маска для MAC адреса с разделение байтов двоеточием. Сетевая маска IP адреса с разделителем точкой. Для битов маски равных 1, эта часть адреса включается в проверку соответствия правилу, для битов равных 0 - исключается.

Пример использования



Configure Permission by MAC Address

Login Command Line Interface (CLI) with username and password which are admin/admin by default.

Configure ACL rule for the MAC Address of Admin's PC by issuing:

acl mac 1 permit src 68:02:35:FF:AB:01 ff:ff:ff:ff:ff:ff

Note: the index ID is from 1 to 128

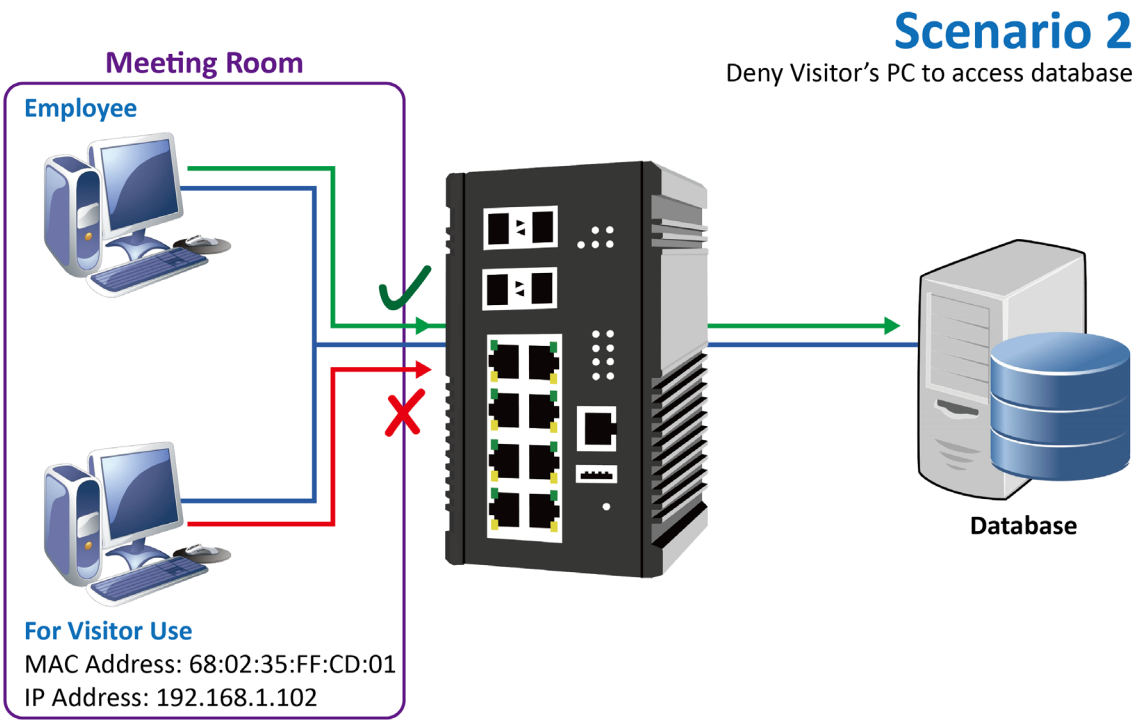
Configure Permission by IP Address

Login Command Line Interface (CLI) with username and password which are admin/admin by default.

Configure ACL rule for the IP Address of Admin's PC by issuing:

acl ip 1 permit src 192.168.1.99 255.255.255.0

Note: the index ID is from 1 to 128



Configure Deny by MAC Address

Login Command Line Interface (CLI) with username and password which are admin/admin by default.

Configure ACL rule for the MAC Address of Visitor's PC by issuing:

acl mac 1 drop src 68:02:35:FF:CD:01 ff:ff:ff:ff:ff:ff

Note: the index ID is from 1 to 128

Configure Deny by IP Address

Login Command Line Interface (CLI) with username and password which are admin/admin by default.

Configure ACL rule for the IP Address of Visitor's PC by issuing:

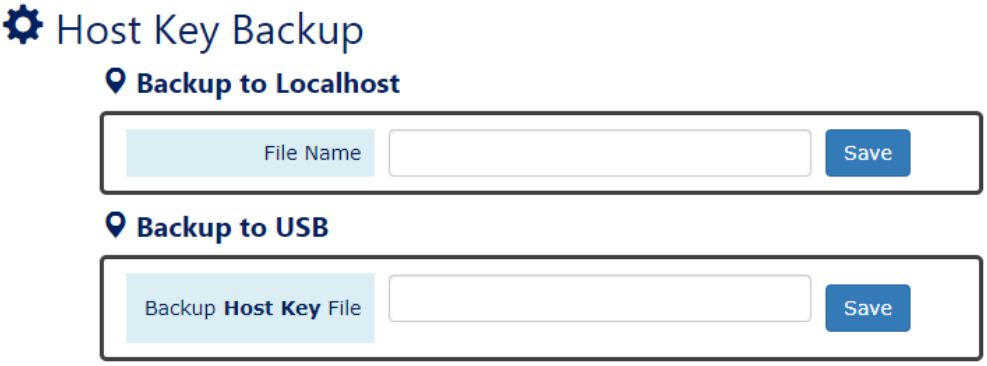
acl ip 1 drop src 192.168.1.102 255.255.255.0

Note: the index ID is from 1 to 128

Управление коммутатором по SSH

To reduce the steps for login the system via SSH connection, the public/private key pair is a good choice for users. The pair of keys is created on the local device and users have to provide the public key to the target device, for example, the Ethernet switch. When users connect to the target device, the system creates a safe connection by SSH. The localhost and target device authenticates each other with the public and private keys to make sure the security.

Резервная копия ключа



Backup to Localhost

File Name

Specify the File Name for the SSH Host Key file, which will be saved to the localhost.

Backup to USB

Ensure there is a USB stick inserted into the USB port.

Backup Host Key File

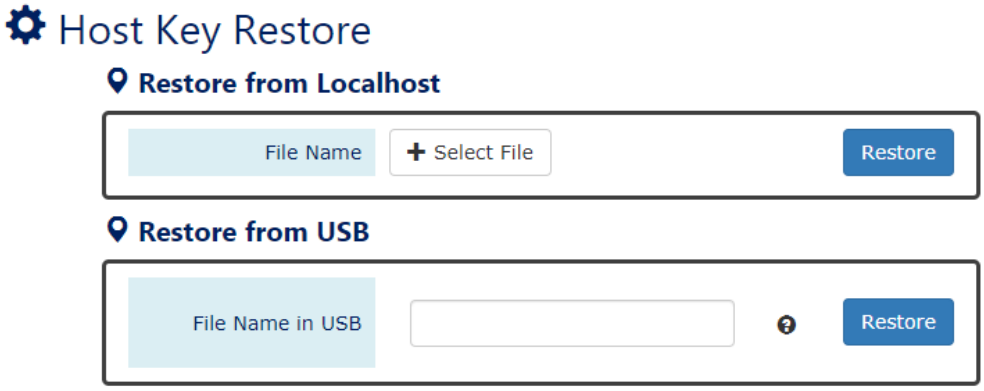
Specify the File Name for the saved SSH Host Key file, which will be saved to the USB.

Note: The file system of USB must be FAT32.

(Save Button)

Click the "Save" button to save the configuration file to the Localhost or USB.

Восстановление ключа



Restore from Localhost

File Name

Select the SSH Host Key file, which is saved in the Localhost.

Restore from USB

Please ensure there is a USB stick inserted into the USB port.

File Name in USB

The File Name of the saved SSH Host Key file, which is saved to the USB. If the configuration file is saved in the directory, please specify the full path.

Note: The file system of USB must be FAT32.

(Restore Button)

Click the "Restore" button to restore the SSH Host Key from the Localhost or USB.

Информация о ключе

The current SSH Host Key is displayed in the “SSH Host Key” page. The system only accept one SSH Host Key, once users restore another Host Key, the current Host Key will be replaced.

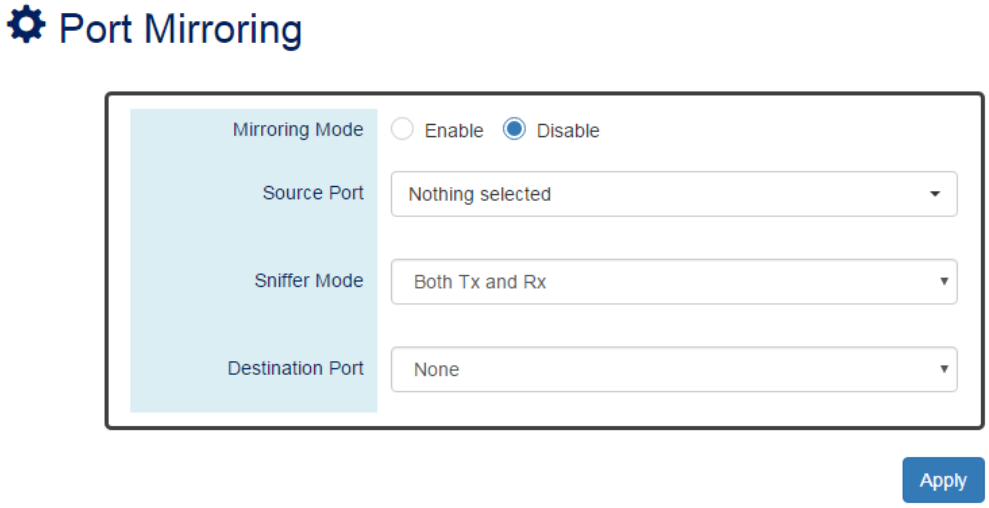
SSH Host Key

AAAAB3NzaC1yc2EAAAADAQABAAABAQCqlNLLQMBzd+BcavrgDWypnd3
1h5/lwimsRWAneEMFuLwdP3L0PIlK05HLnouprQjyWiJjYZmQ9wgucZ1dXUtpne
1yfgxTi8CQayACHMj3gTVzWAAPNhS8Ouq7LRMThucySBQouiQHKPlbi2KZm6+IX
DHAmAG1cOM9vnRuiymDkmWBI/xVk4i0Vx+q2rAUcUOKBNm2Ydr/rz4MxoAeQRCJ
UhjeH0ylBhCtM8+stM1/3k54Kn4Ivt9OqDCnLGjC3hwKxLDn1UxPDp46+oKbTls
8OLAca285mTTKMj8g9XTlGsRD259bsajaj65e7GAI6ovnlnWqew4f4jGOOOOVdh

Диагностика

Зеркалирование портов

Функция, которая копирует входящие или исходящие пакеты с одного или нескольких портов на другой порт назначения. Очень полезно отслеживать сетевой трафик и анализировать скопированный трафик. Зеркалирование портов помогает при управлении сетью внимательно следить за трафиком и отлаживать настройки при возникновении некоторых проблем.



- **Mirroring Mode**

  Включение или отключение функции зеркалирования портов. Если пользователь включает функцию зеркалирования портов, система будет передавать трафик в соответствии с выбранным Sniffer Mode с порта источника на порт назначения.
- **Source Port**

  Порт, трафик с которого должен зеркалироваться.
- **Sniffer Mode**

  Режим зеркалирования

  Both Tx and Rx: Зеркалировать принимаемый и передаваемый на порту трафик

  Tx Only: Зеркалировать только передаваемый на порту трафик.

  Rx Only: Зеркалировать только принимаемый на порту трафик.
- **Destination Port**

  Порт, на который должен зеркалироваться трафик. Обычно подключен к хосту с ПО для захвата пакетов для анализа

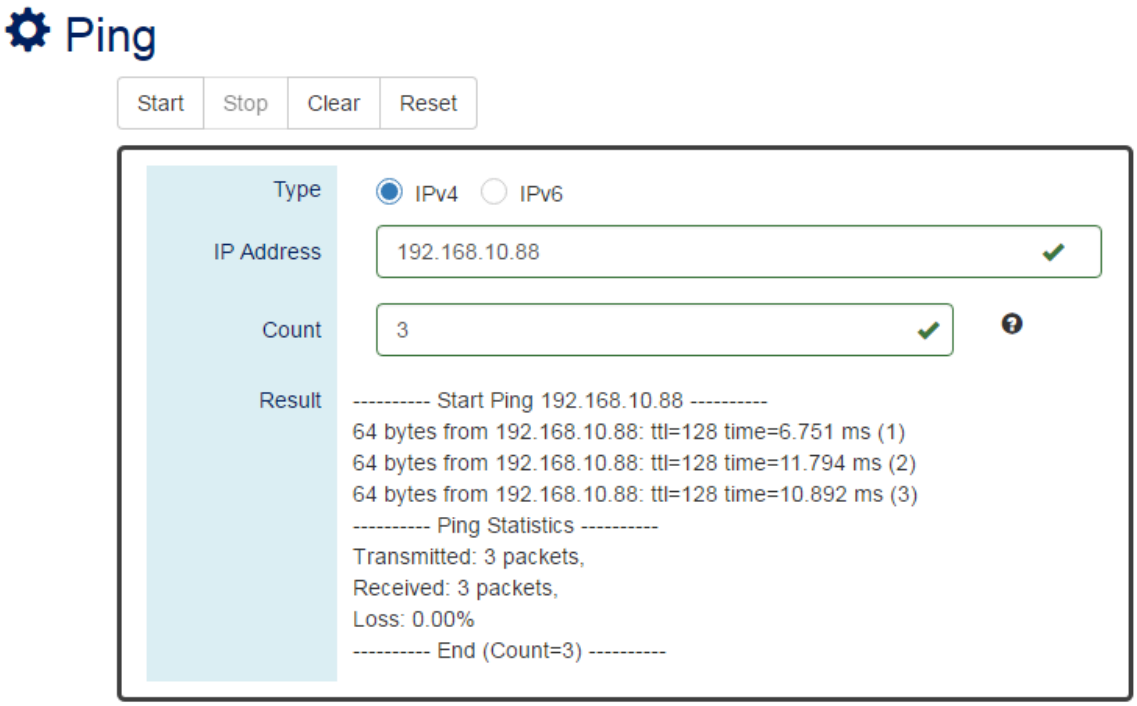
(Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Функция Ping

Ping - это инструмент, используемый для проверки доступности устройства в IP-сети. Ping включается путем отправки запроса протокола управляющих сообщений Интернета (ICMP) на целевое устройство и ожидания пакета ответа от целевого устройства для проверки соединения.

Ping другого устройства по IPv4/IPv6



Для более подробной информации наведите курсор мыши на иконку ?.

Type

Тип протокола для пинга: IPv4 или IPv6.

IP Address

IP адрес удаленного устройства, формат зависит от протокола – IPv4 или IPv6.

Count

Количество ICMP пакетов для отправки. Диапазон значений от 3 до 50. По умолчанию - 3.

Result

Результат проверки связи показывает ответ с определенного IP-адреса. Если конкретный IP-адрес не отвечает, отображается No Response.

Кнопка “Start”

Нажмите кнопку «Start», чтобы начать проверку связи с IP-адресом.

Кнопка “Stop”

Нажмите кнопку «Stop», чтобы остановить проверку до отправки всех ICMP пакетов.

Кнопка “Clear”

Нажмите кнопку “Clear” для очистки окна результатов.

Кнопка “Reset”

Нажмите кнопку “Reset” для очистки окна результатов и всех настроек в окне.

Диагностика кабеля

Эта команда может проверить состояние медных кабелей с помощью технологии рефлектометрии (TDR). Она может обнаружить неисправность кабеля, посылая сигнал обнаружения и считывая отраженный сигнал. С помощью этого теста можно выявить и локализовать проблему физического уровня.

Для отображения диагностики кабеля на порту:

```
Switch(config-lan3)# show cable-diagnostic
cable (4 pairs, length +/- 10 meters)
        pair A Ok, length 5 meters
        pair B Ok, length 5 meters
        pair C Ok, length 5 meters
        pair D Ok, length 5 meters
```

Зайдите в CLI в настройки интересующего вас порта и выполните команду

show cable-diagnostic

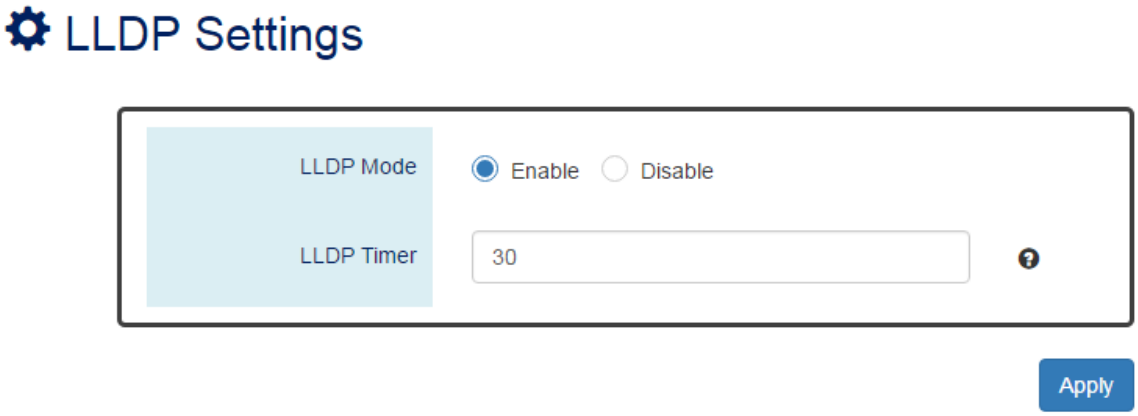
В текстовом выводе будет дана следующая информация:

- Состояние кабеля. Он содержит количество пар в кабеле и количество ошибок. Обычно в кабеле CAT-5E есть 4 пары для соединения Gigabit Ethernet.
- Статус каждой пары порта. Статус «OK» означает, что кабель подключен к другому узлу. Статус «Open» означает, что кабель не подключается ни к какому устройству.
- Длина каждой пары портов в метрах. Обратите внимание, что из-за технологии TDR погрешность составляет около 10 метров. Короткий кабель меньше, чем значение погрешности, может быть измерен неточно.

LLDP

LLDP - это протокол обнаружения канального уровня, независимый от производителя протокол Layer 2, определенный IEEE 802.1AB. LLDP используется для обнаружения сетевых устройств, их возможностей и соседей в локальной сети. Информация от соседей позволяет коммутатору быстро идентифицировать устройства и взаимодействовать друг с другом более плавно и эффективно. Таблица соседей показывает информацию об устройстве, которое находится рядом с портом. LLDP может получать информацию только от близкого к нему устройства. Если пользователи хотят знать топологию локальной сети, они могут собрать всю информацию с устройства и проанализировать таблицу соседей.

Настройка LLDP



Для более подробной информации наведите курсор мыши на иконку ?.

- **LLDP Mode**
  Включение работы LLDP протокола. Включение – Enable, выключение - Disable.
- **LLDP Timer**
  Таймер LLDP — это временной интервал для отправки сообщений LLDP. Диапазон таймера LLDP составляет от 5 до 32767 секунд. Таймер LLDP по умолчанию составляет 30 секунд.

Apply (Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Таблица LLDP соседей

LLDP Neighbor

Show 10 entries Search:

Local Port	Remote System Name	Chassis ID	Remote Port	Port ID	Address
3	MT-0804G	00:AA:BB:CC:11:02	lan8	local 8	192.168.10.11
6	L2GigaBitEthern...	00:03:CE:11:22:33	Sid #2, Po...	local 1017	192.168.10.90

Showing 1 to 2 of 2 entries First Previous Next Last

Auto Refresh Refresh

Refresh Rate: 5 seconds

Local Port

Порт, подключенный к LLDP-соседу на локальном коммутаторе.

Remote System Name

Это системное имя соседа по LLDP. Это значение устанавливается и предоставляется удаленным устройством.

Chassis ID

Идентификатор шасси определяет MAC-адрес соседа по LLDP.

Remote Port

В этом поле отображается информация о порте, полученная от соседа LLDP.

Port ID

Идентификатор порта отображает идентификатор порта подключенного порта на соседнем узле LLDP.

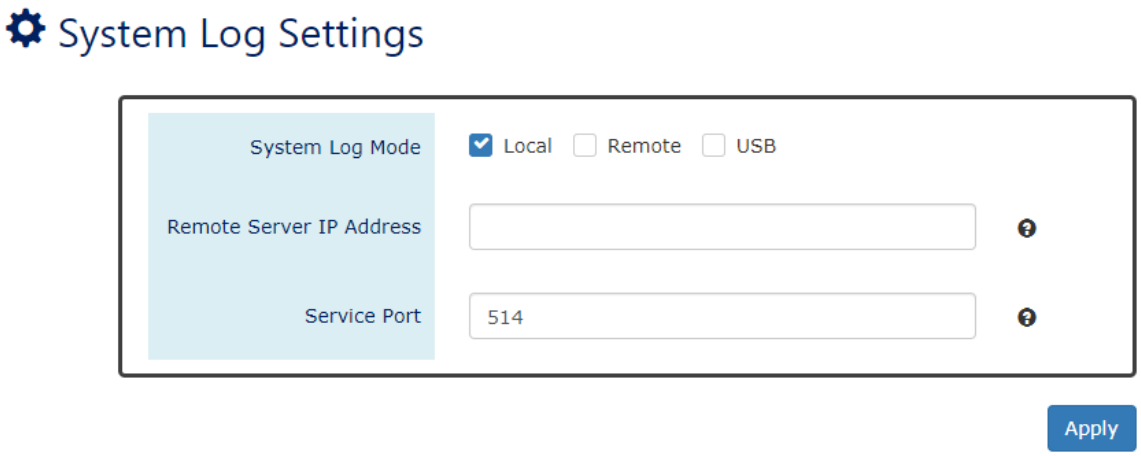
Address

Адрес отображает IP-адрес соседа по LLDP

Системные события

Работа с системными событиями сосредоточена в меню System Warning. В нем содержится настройки для различных видов журналирования и фильтрации системных событий. Эти журналы очень полезны для администратора при управлении и отладке системы. Когда система неожиданно выключена, или когда кто-то пытается войти в систему, или система перезагружается ненормально, или когда некоторые из интерфейсов заблокированы, система отправляет сообщения журнала, чтобы уведомить определенных пользователей и записать события на сервере или назначенной платформе. Пользователи также могут подключить зуммер аварийной сигнализации к контактам реле аварийной сигнализации. Когда срабатывают настроенные события «Тревога о неисправности», зуммер тревоги звонит, чтобы уведомить пользователей

Настройка Syslog



Для более подробной информации наведите курсор мыши на иконку ?.

System Log Mode

Установите флажок для отправки системного журнала: Local - на локальный коммутатор, Remote удаленный хост или USB для отправки на USB-накопитель.

Remote Server IP Address

Поле содержит IP-адрес удаленного сервера. Если включен «Remote» режим, пользователи должны назначить этот IP-адрес для получения системных журналов. Система поддерживает адреса IPv4 и IPv6 для удаленного сервера.

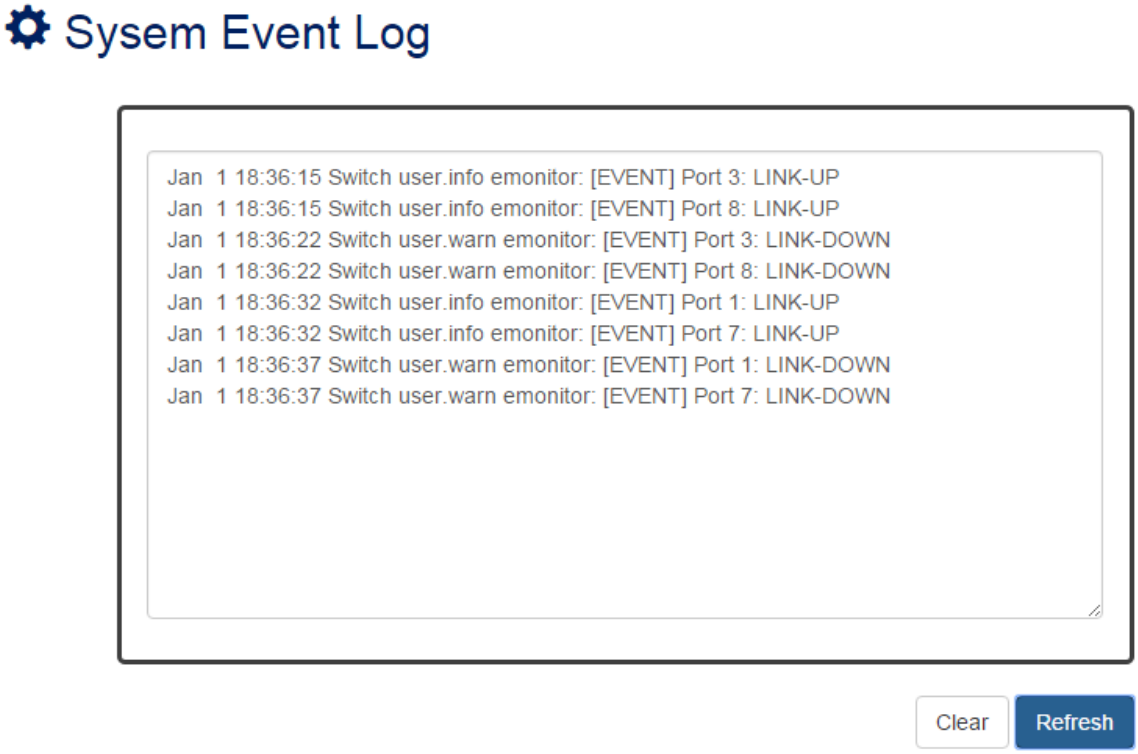
Service Port

Порт используемый для приема данных системного журнала на удаленном хосте. Диапазон служебного порта составляет от 1 до 65535. Служебный порт по умолчанию - 514.

Apply (Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Просмотр системных событий



- **Текстовая область журнала**

  Информация о системных событиях отображается, если включен режим системного журнала «Local» и включены уведомления о настроенных событиях.

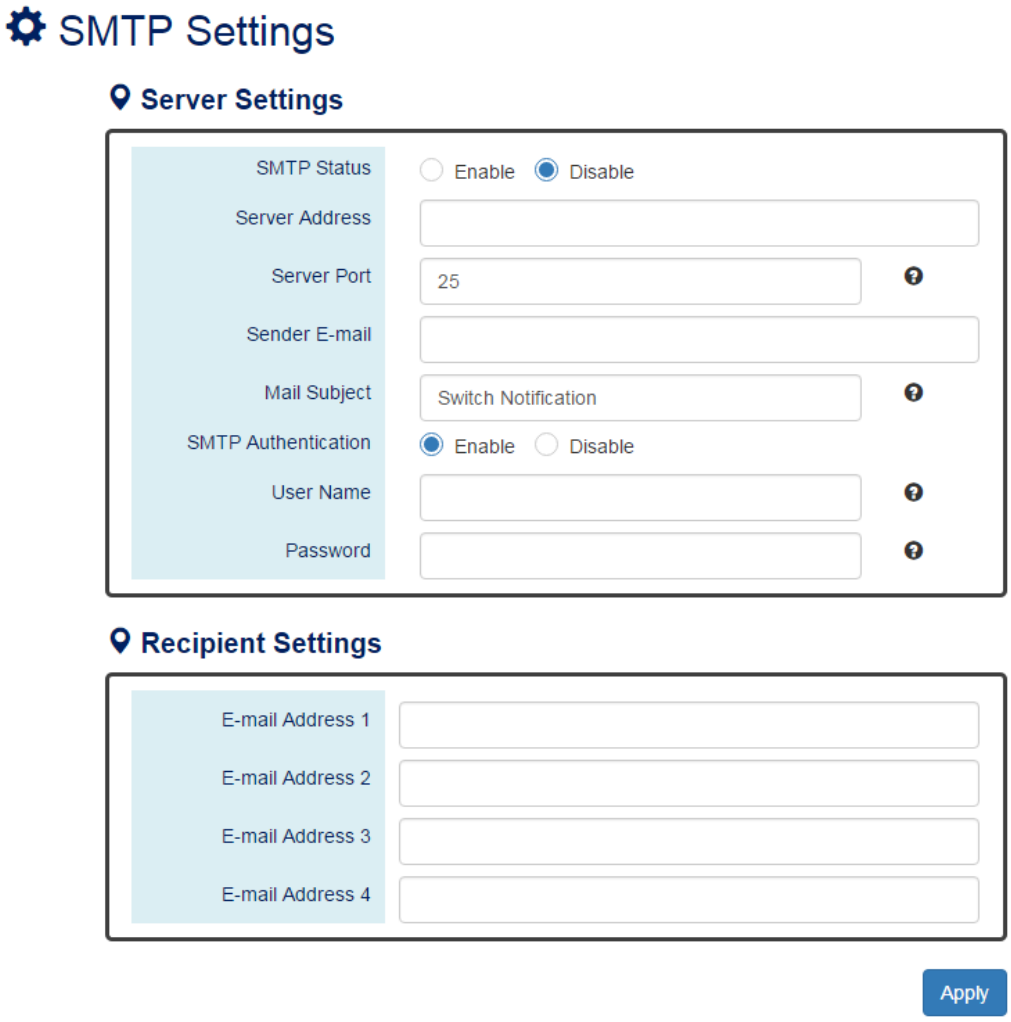
- Clear (Очистить)

  Нажмите кнопку «Очистить», чтобы очистить журнал системных событий в текстовой области.

- Refresh (Обновить)

  Нажмите кнопку «Обновить», чтобы обновить журнал системных событий в текстовой области.

Настройка SMTP



Для более подробной информации наведите курсор мыши на иконку ?.

Настройки сервера - Server Settings

- **SMTP Status**

  Включение работы SMTP протокола. Включение – Enable, выключение - Disable.

- **Server Address**

  Это IP-адрес или URL-адрес SMTP-сервера. Например, адрес SMTP-сервера, предоставляемого Google - smtp.gmail.com.

- **Server Port**

  Это поле – порт сервера, который принимает SMTP-запросы. В целях безопасности мы предлагаем пользователям настроить порт сервера на 465 для SSL или 587 для TLS. Диапазон служебного порта составляет от 1 до 65535. Служебный порт по умолчанию - 25. Порт 25 является портом по умолчанию для сервера электронной почты.

- **Sender E-mail**

  Электронная почта отправителя — это адрес электронной почты, используемый для отправки уведомлений получателям.
- **Mail Subject**

  Тема письма - это строка, которая отображается в заголовке электронного письма. Примечание: #, \, ‘, «, ? не разрешены в этом поле.
- **SMTP Authentication**

  Включение аутентификации на SMTP-сервере с настроенным именем пользователя и паролем.
- **User Name**

  Имя пользователя используется при аутентификации на SMTP-сервере. Макс. длина имени пользователя составляет 32 символа. Примечание: #, \, ‘, «, ? не разрешены в этом поле.
- **Password**

  Пароль используется при аутентификации на SMTP-сервере. Макс. длина пароля составляет 32 символа. Примечание: #, \, ‘, «, ? не разрешены в этом поле.

Настройки получателей - Recipient Settings

- **E-mail Address 1-4**

  На настроенные адреса электронной почты будут приходить уведомления, если SMTP включен и происходят события, настроенные для отправки на SMTP в фильтрах событий.

(Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Настройка фильтра системных событий

System Event Selections

Event	Fault Alarm	System Log	SMTP	SNMP
Authentication Failure	-	Disable	Disable	Disable
ERPS Change	-	Disable	Disable	Disable
Power 1	Disable	Disable	Disable	Disable
Power 2	Disable	Disable	Disable	Disable
Power 3	Disable	Disable	Disable	Disable
Power 4	Disable	Disable	Disable	Disable
Cold Start	-	Disable	Disable	Disable
Warm Start	-	Disable	Disable	Disable
Digital Input	Disable	Disable	Disable	Disable

Apply

Event

Существует пять основных типов событий в системе. Можно настроить каждый из типов для отображения в Fault Alarm, System Log, SNMP, SMTP

5 типов включают в себя:

- Ошибка аутентификации: Ошибка входа в веб-консоль или интерфейс командной строки. Это может быть вызвано неправильным именем пользователя или паролем.
- Изменение ERPS: функция ERPS работает и топология изменена.
- Питание 1–4: Питание 1–4 отключено.
- Холодный старт: система перезагружается из-за прерывания подачи питания.
- Теплый старт: система перезагружается, после ввода команды «reboot» в интерфейсе командной строки или нажатия на значок перезагрузки на веб-консоли.
- Цифровой вход (DI): сигнал с цифрового входа изменяется с высокого на низкий или с низкого на высокий.

Apply (Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Настройка фильтра событий на портах

Interface Event Selections

Event	Fault Alarm	System Log	SMTP	SNMP
All Ports Link	Down	Up Down	Up Down	Up Down
Port 1 Link	Down	Up Down	Up Down	Up Down
Port 2 Link	Down	Up Down	Up Down	Up Down
Port 3 Link	Down	Up Down	Up Down	Up Down
Port 4 Link	Down	Up Down	Up Down	Up Down
Port 5 Link	Down	Up Down	Up Down	Up Down
Port 6 Link	Down	Up Down	Up Down	Up Down
Port 7 Link	Down	Up Down	Up Down	Up Down
Port 8 Link	Down	Up Down	Up Down	Up Down
Port 9 Link	Down	Up Down	Up Down	Up Down
Port 10 Link	Down	Up Down	Up Down	Up Down
Port 11 Link	Down	Up Down	Up Down	Up Down
Port 12 Link	Down	Up Down	Up Down	Up Down

Apply

Event

События в фильтре события на портах отображают состояние линии на порту. Категория отчета Fault Alarm включает в себя только событие Link Down, для всех остальных категорий есть Link Down и Link Up события.

Fault Alarm

Светодиод Alarm загорится красным, и реле сухих контактов замкнется, если срабатывают настроенные события. По умолчанию светодиод неисправности горит зеленым светом, а в нормальных условиях реле выключено.

System Log

Когда настроенные события происходят, появляется запись в журнале “System Event Log”, на удаленном сервере syslog или на USB в файле с именем “message”. Это зависит от настроек “System Log Mode” на странице “System Log Settings”.

SMTP

Если SMTP включен и настроенные события происходят, система отправит уведомление по электронной почте на адреса электронной почты назначенного получателя, указанные на странице “SNMP Settings”.

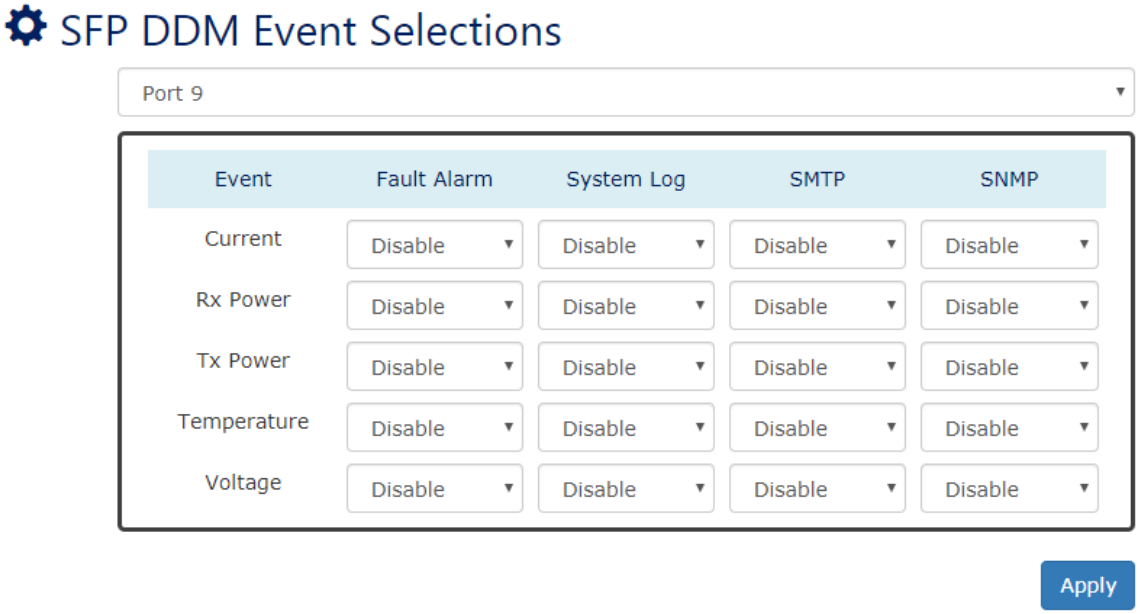
SNMP

Если настроенные события происходят, система отправляет trap-уведомление на настроенный адрес “Trap Receiver IP”, который задается на странице “SNMP Trap”.

Apply (Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Настройка фильтра событий SFP DDM



Event

Есть 5 видов событий: по току, по мощности приема, мощности передачи, температуре и напряжению. Включите или отключите сигнализацию о неисправности или системное предупреждение, если значение выше верхнего порога срабатывания сигнализации или значение ниже нижнего порога срабатывания сигнализации.

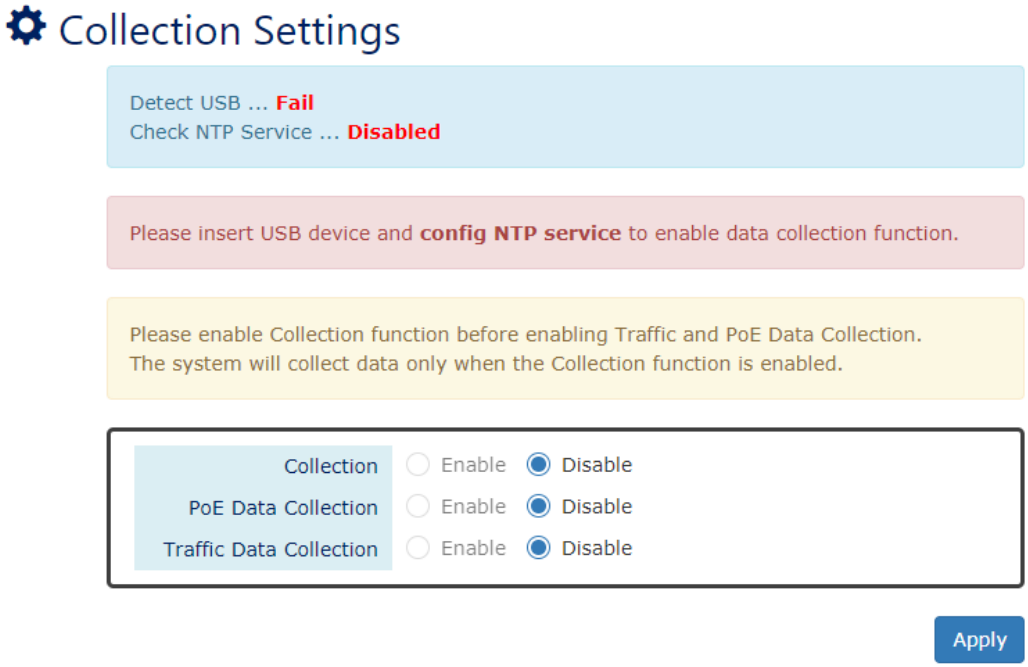
Сбор данных на коммутаторе

Здоровье коммутатора очень важно в реальных приложениях. Для большинства коммутаторов есть базовая информация в реальном времени о состоянии трафика и PoE, но пользователям нужны длительные записи для анализа и статистики системы. Для этого мы реализуем функцию сбора данных, чтобы периодически собирать данные о трафике и статусе PoE и сохранять собранные данные на USB-устройство. В дополнение к этому мы также предоставляем диаграммы для отображения собранных данных. Пользователи могут легко определить состояние коммутатора и найти необычные точки на графиках.

Чтобы обеспечить точность данных, службу NTP необходимо включить перед включением функции сбора данных, чтобы пользователи, обнаружив аномальную запись, могли отследить ее по времени записи. И не стоит беспокоиться о размере системного хранилища, потому что данные сохраняются на USB. Данные даже можно переместить на другие устройства для отображения, или пользователи могут использовать собранные необработанные данные в других приложениях.

Порядок настройки сбора данных

USB и NTP необходимы до того, как пользователи включат функции сбора данных. Пожалуйста, проверьте, вставлен ли USB-накопитель и включена ли служба NTP. Файловая система USB должна быть FAT32.



- **Collection**

  Включить или отключить функцию сбора данных на коммутаторе. Сбор данных о трафике и PoE можно включить, только если включен сбор данных.
- **PoE Data Collection (только для моделей с PoE)**

  Включить или отключить функцию сбора данных о PoE на коммутаторе.
- **Traffic Data Collection**

  Включить или отключить функцию сбора данных о трафике на коммутаторе.

Сброс собранных данных

Collected Data Reset

Port	Traffic	PoE
	Sel. All Desel. All	Sel. All Desel. All
1	☐	☐
2	☐	☐
3	☐	☐
4	☐	☐
5	☐	☐
6	☐	☐
7	☐	☐
8	☐	☐
9	☐	
10	☐	
11	☐	
12	☐	

Reset

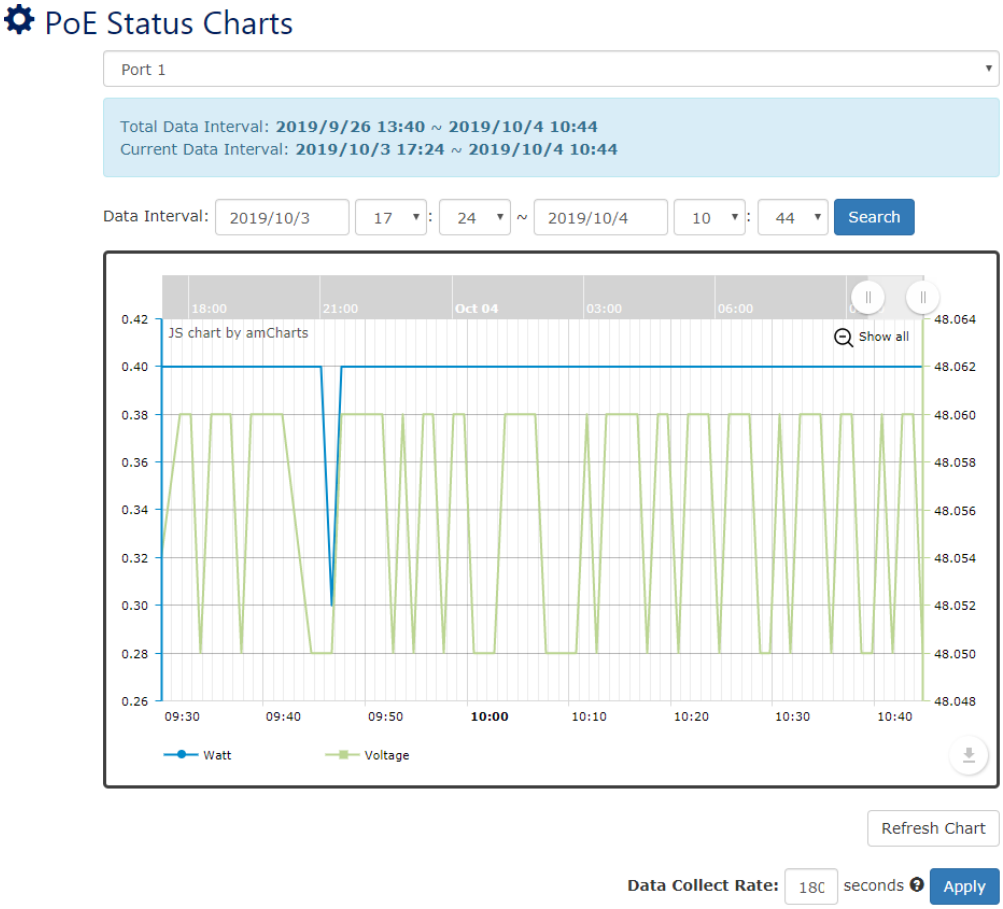
- **Port**

  Номер порта коммутатора от 1 до N, где N определяется общим количеством портов модели коммутатора.
- **Traffic**

  Флажок сброса данных соответствующего порта коммутатора. После сброса собранные данные будут удалены с USB. Примечание: это действие не может быть отменено, убедитесь, что вы хотите сбросить файл.
- **PoE (только для моделей с PoE)**

  Флажок сброса данных PoE соответствующего порта коммутатора.

Диаграмма состояния PoE



Для более подробной информации наведите курсор мыши на иконку ?.

- **Выпадающий список выбора порта**

  От Port1 до PortN, где N общее количество PoE портов в коммутаторе. График PoE показывается для выбранного порта.

- **Total Data Interval**

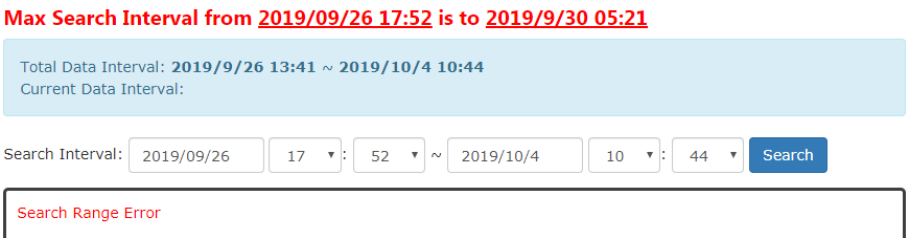
  Интервал времени между первыми и последними данными для порта собранными на USB.

- **Current Data Interval**

  Интервал времени показываемый на текущем графике.

- **Data Interval (выпадающий интерфейс выбора даты/времени)**

  Для выбора интервала времени для поиска данных. Возвращенные данные будут отображены на графике. Количество данных ограничено системой, если выбранный интервал превышает ограничение, система вернет приемлемый интервал (как показано на следующем снимке экрана).



Примечание. После настройки интервала данных нажмите кнопку «Search», чтобы получить данные в интервале.

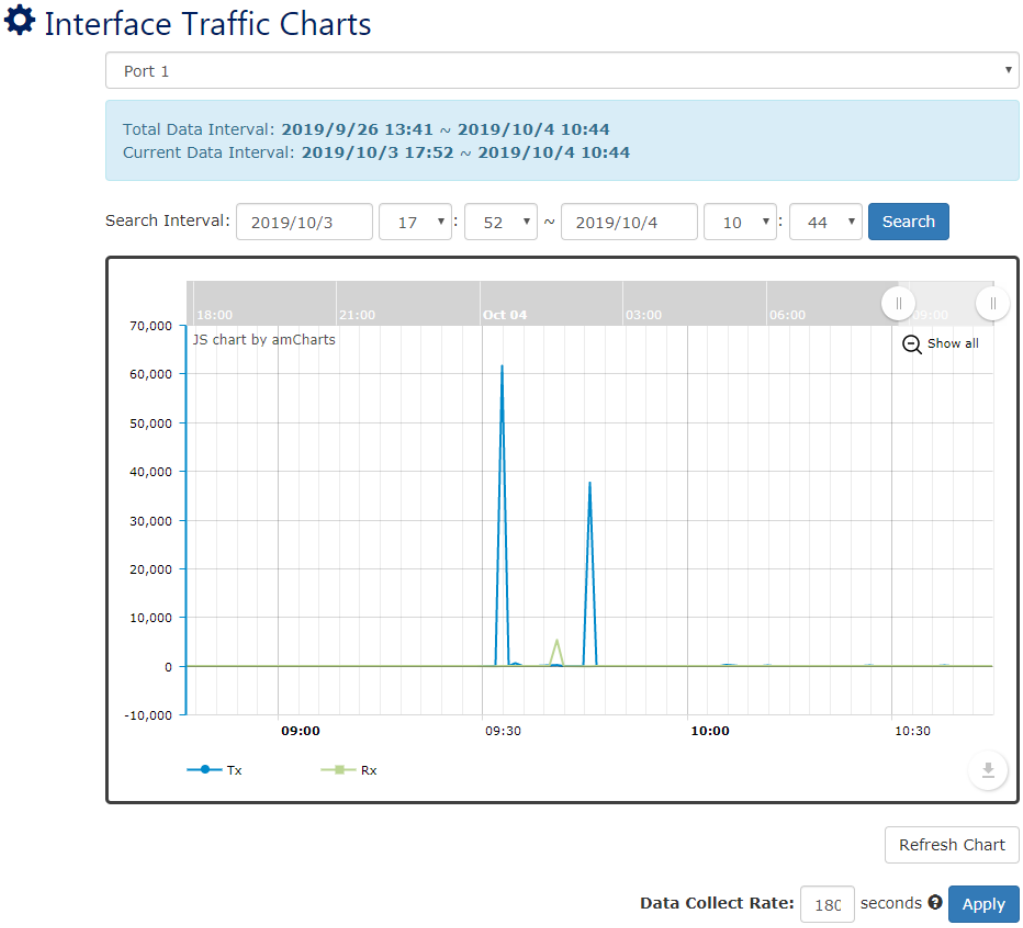
- **Chart**

  На диаграмме отображаются данные о ваттах (синяя линия) и напряжении (зеленая линия).
- **Refresh Chart (кнопка)**

  Нажмите для получения обновленных данных.
- **Data Collect Rate**

  Поле — это период для сбора данных. Система будет периодически получать данные в реальном времени в соответствии с настроенной скоростью сбора данных. Примечание. Диаграммы состояния PoE и диаграммы трафика интерфейса используются с одинаковой скоростью сбора данных. Диапазон скорости сбора данных составляет от 60 до 600 секунд. Скорость сбора данных по умолчанию составляет 180 секунд. Примечание. После настройки нажмите кнопку Apply, чтобы изменения вступили в силу.

Диаграмма трафика на интерфейсах



Для более подробной информации наведите курсор мыши на иконку ?.

- **Выпадающий список выбора порта**

  От Port1 до PortN, где N общее количество портов в коммутаторе. График трафика показывается для выбранного порта.

- **Total Data Interval**

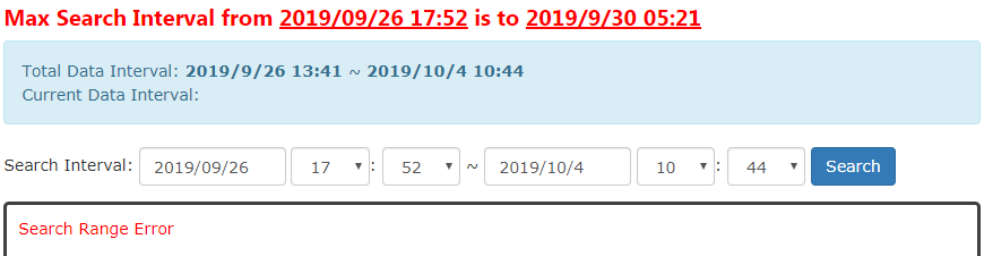
  Интервал времени между первыми и последними данными для порта собранными на USB.

- **Current Data Interval**

  Интервал времени показываемый на текущем графике.

- **Data Interval (выпадающий интерфейс выбора даты/времени)**

  Для выбора интервала времени для поиска данных. Возвращенные данные будут отображены на графике. Количество данных ограничено системой, если выбранный интервал превышает ограничение, система вернет приемлемый интервал (как показано на следующем снимке экрана).



Примечание. После настройки интервала данных нажмите кнопку «Search», чтобы получить данные в интервале.

- **Chart**

  На диаграмме отображаются данные о переданных (синяя линия) и принятых (зеленая линия) байтах.
- **Refresh Chart (кнопка)**

  Нажмите для получения обновленных данных.
- **Data Collect Rate**

  Поле — это период для сбора данных. Система будет периодически получать данные в реальном времени в соответствии с настроенной скоростью сбора данных. Примечание. Диаграммы состояния PoE и диаграммы трафика интерфейса используются с одинаковой скоростью сбора данных. Диапазон скорости сбора данных составляет от 60 до 600 секунд. Скорость сбора данных по умолчанию составляет 180 секунд. Примечание. После настройки нажмите кнопку Apply, чтобы изменения вступили в силу.

Настройка таблицы MAC адресов

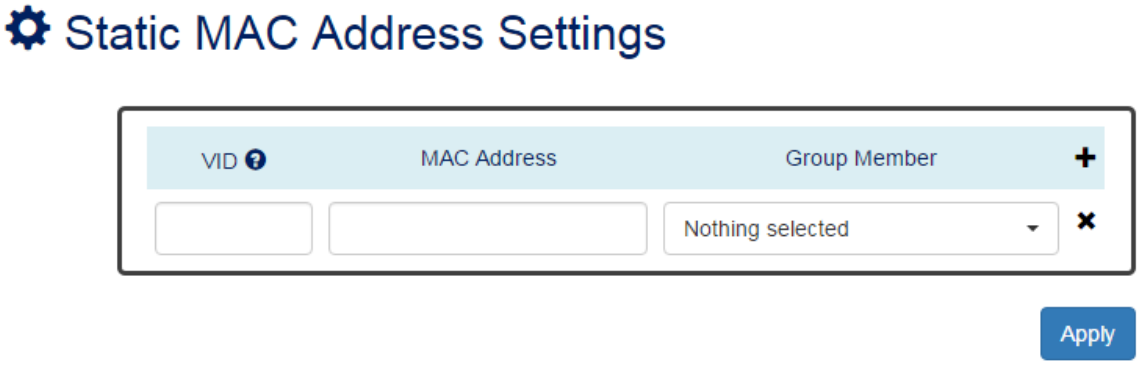
MAC-адрес - это адрес управления доступом к среде, который используется при коммутации уровня 2. Таблица MAC-адресов поддерживается коммутатором для более эффективной передачи кадров. Когда коммутатор получает кадр, система проверяет таблицу MAC и перенаправляет кадр на соответствующий порт. Таблица MAC-адресов создается динамически из полученных кадров, и когда система получает кадр с неизвестным MAC-адресом, она рассылает этот кадр всем портам LAN в той же VLAN. Когда устройство назначения отвечает, система идентифицирует MAC-адрес и целевой порт.

MAC-адрес коммутатора включает MAC адреса каждого порта, что означает, что каждый порт имеет свой собственный MAC-адрес. Это важно для протоколов, чувствительных к MAC, таких как протокол связующего дерева. Отображаемые MAC-адрес в правой части веб-интерфейса - это MAC-адрес для всей системы, а MAC-адреса для портов увеличиваются на 1 от первого порта до последнего.

Например, MAC-адрес системы 68: 02: 35: FF: FF: 05, а на коммутаторе 8 портов. MAC-адрес для каждого порта будет:

Порт	MAC адрес	Порт	MAC адрес
Port 1	68:02:35:FF:FF:06	Port 5	68:02:35:FF:FF:0A
Port 2	68:02:35:FF:FF:07	Port 6	68:02:35:FF:FF:0B
Port 3	68:02:35:FF:FF:08	Port 7	68:02:35:FF:FF:0C
Port 4	68:02:35:FF:FF:09	Port 8	68:02:35:FF:FF:0D

Настойка статических MAC адресов



Для более подробной информации наведите курсор мыши на иконку ?.

- **VID**
  Идентификатор VLAN, который содержит настраиваемый MAC-адрес. Диапазон VID от 1 до 4094.

- **MAC Address**

  Это поле представляет собой статический MAC-адрес настроенный для портов-участников в группе VLAN.

- **Group Member**

  Порты в группе VLAN, которой принадлежит настроенный MAC-адрес.

✚: Щелкните значок плюса, чтобы добавить строку статического MAC-адреса.

✖: Click the remove icon to delete the static MAC Address row.

Apply (Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Просмотр таблицы MAC адресов

MAC Address Table

Show 10 entries Search:

VID	MAC Address	Type	Source
VLAN 1	EC:08:6B:06:96:53	Learning	2
VLAN 1	1C:49:7B:6A:F3:41	Learning	5
VLAN 1	1C:1B:0D:66:75:EB	Learning	5
VLAN 1	01:00:5E:7F:FF:FA	Static	2
VLAN 1	40:8D:5C:EA:92:02	Learning	5
VLAN 1	9C:EB:E8:3A:54:E7	Learning	5
VLAN 1	40:8D:5C:EA:8D:C3	Learning	5
VLAN 1	1C:1B:0D:66:F7:F8	Learning	5
VLAN 1	FC:3F:DB:53:19:8E	Learning	5
VLAN 1	A4:02:B9:80:7D:66	Learning	5

Showing 1 to 10 of 10 entries First Previous Next Last

Auto Refresh Refresh

Refresh Rate: 5 seconds

- **VID**

  Идентификатор VLAN, который содержит MAC-адрес. Диапазон VID от 1 до 4094.

- **MAC Address**

  MAC адрес, изученный или настроенный вручную.

- **Type**

  Тип MAC адреса (Learning илиStatic).

  Learning: MAC изучен из передаваемых кадров.

  Static: MAC настроен вручную.

- **Source**

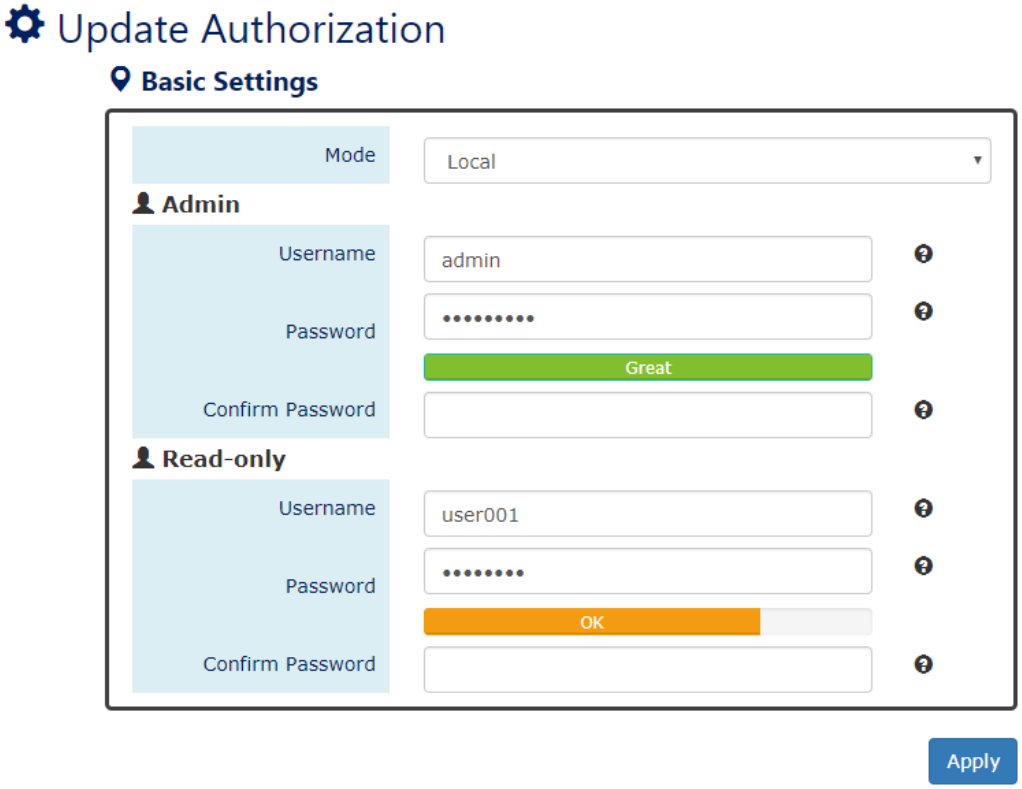
  Порт, которому принадлежит данный MAC адрес.

Аутентификация пользователей локальная/TACACS/RADIUS

Имя пользователя и пароль являются очень важной информацией как в интерфейсе командной строки, так и в веб-интерфейсе. Перед выполнением любой настройки пользователи должны войти в систему. Мы настоятельно рекомендуем пользователям изменить хотя бы пароль в целях безопасности, когда они собираются использовать это устройство.

Мы также обеспечиваем аутентификацию с сервером RADIUS/TACACS+, начиная с версии программного обеспечения 1.0.3. Пользователи могут хранить информацию для аутентификации в своей собственной базе данных RADIUS/TACACS+ и использовать несколько имен пользователей/паролей для входа в систему.

Настройка режима аутентификации



Для более подробной информации наведите курсор мыши на иконку ?.

Mode

Существует три режима аутентификации при входе.

Local: имя пользователя и пароль определяются в системе. В настоящее время мы поддерживаем два уровня пользователей - администратора и пользователя только для чтения. Администратор может получить доступ к любой странице и настроить систему, но пользователь только для чтения может получить доступ только к страницам состояния.

RADIUS: имя пользователя и пароль определяются на сервере RADIUS, и когда пользователи входят в систему, система аутентифицирует пользователя на сервере RADIUS, чтобы получить разрешение на вход. Пароль будет зашифрован во время передачи.

TACACS+: имя пользователя и пароль определяются на сервере TACACS+, и когда пользователи входят в систему, система аутентифицирует пользователя на сервере TACACS+, чтобы получить разрешение на вход. Вся полезная нагрузка и пароль будут зашифрованы во время передачи.

Username

Учетная запись, используемая для входа в систему. Максимальная длина имени пользователя - 32 символа. Разрешены только буквы (A-Z, a-z) и цифры (0-9). Имя пользователя по умолчанию - admin.

Password

Пароль, используемый для входа в систему. Мы предоставляем шкалу надежности пароля для справки. Есть 3 уровня – Слабый (Weak), Нормальный (Normal) и Отличный (Great). Мы настоятельно рекомендуем пользователям настроить пароль на уровень «Отличный» в целях безопасности. Максимальная длина пароля составляет 32 символа. Разрешены только буквы (A-Z, a-z), цифры (0-9) и символы (!, @,%, ^, *, (,)). Пароль по умолчанию - admin..

Confirm Password

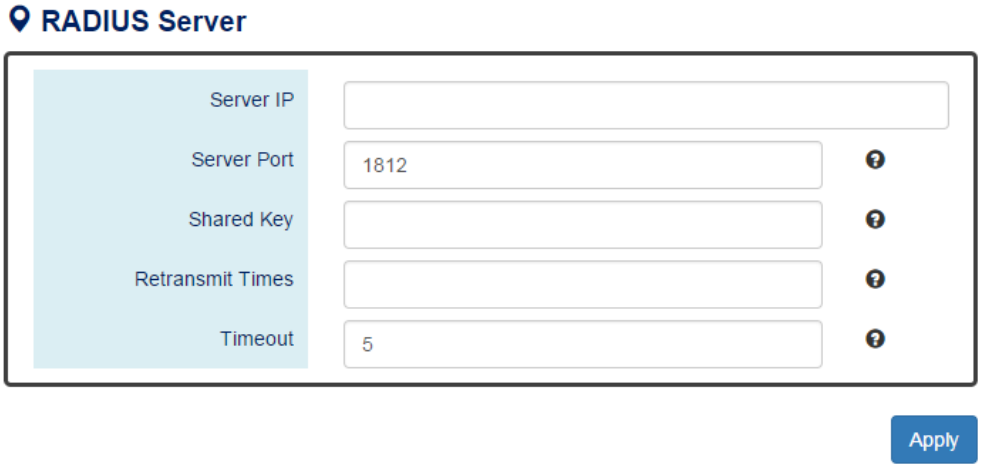
Поле используется для подтверждения значения, указанного пользователями в поле «Password». Значение поля должно быть таким же, как «Password».

(Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Настройка параметров RADIUS сервера

Этот раздел отображается только в том случае, если в основных настройках выбран режим «RADIUS».



Для более подробной информации наведите курсор мыши на иконку ?.

- **Server IP**

  IP адрес сервера RADIUS, должен быть из той же подсети что и адрес коммутатора.
- **Server Port**

  Порт сервиса RADIUS на сервере. Диапазон значений от 1 до 65535. Значение по умолчанию 1812.
- **Shared Key**

  Общий ключ — это строка, которая используется для установления соединения с сервером RADIUS. Он должен быть таким же, как строка/секрет, установленный на сервере RADIUS. Максимальная длина общего ключа составляет 32 символа.
- **Retransmit Times**

  Количество повторных попыток аутентификации. Диапазон значений от 1 до 1000.
- **Timeout**

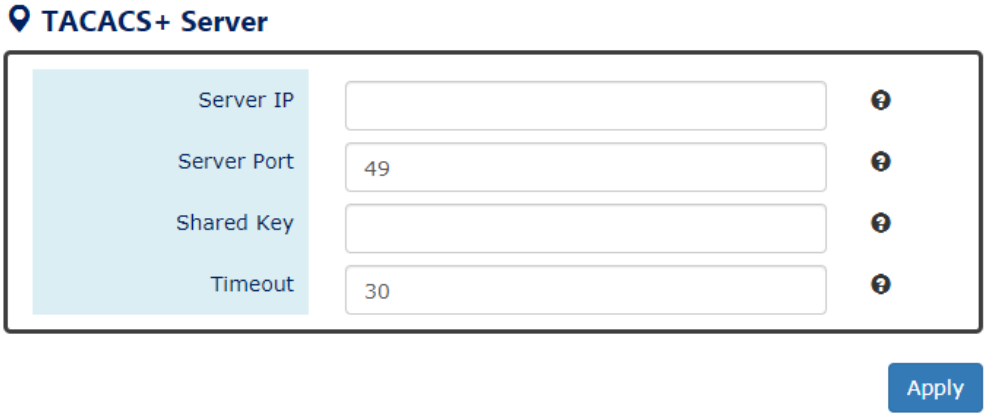
  Временной интервал ожидания ответа от сервера RADIUS. Диапазон тайм-аута составляет от 1 до 1000 секунд. По умолчанию время ожидания составляет 5 секунд.

Apply (Применить)

После настройки нажмите кнопку Apply что бы изменения были активированы.

Настройка параметров TACACS+ сервера

Этот раздел отображается только в том случае, если в основных настройках выбран режим «TACACS».



Для более подробной информации наведите курсор мыши на иконку ?.

- **Server IP**

  IP адрес сервера TACACS+, должен быть из той же подсети что и адрес коммутатора. Система поддерживает как IPv4 так и IPv6 адреса для TACACS сервера.

- **Server Port**

  Порт сервиса TACACS+ на сервере. Диапазон значений от 1 до 65535. Значение по умолчанию 49.

- **Shared Key**

  Общий ключ — это строка, которая используется для установления соединения с сервером TACACS. Он должен быть таким же, как строка/секрет, установленный на сервере TACACS. Максимальная длина общего ключа составляет 32 символа.

- **Retransmit Times**

  Количество повторных попыток аутентификации. Диапазон значений от 1 до 1000.

- **Timeout**

  Временной интервал ожидания ответа от сервера RADIUS. Диапазон тайм-аута составляет от 1 до 1000 секунд. По умолчанию время ожидания составляет 30 секунд.

Apply (Применить)

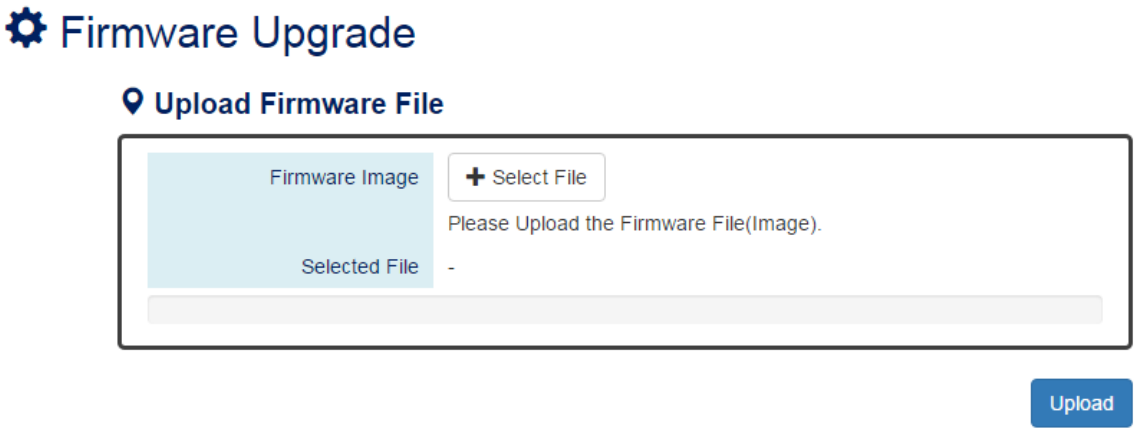
После настройки нажмите кнопку Apply что бы изменения были активированы.

Обновление встроенного ПО

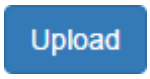
Для повышения производительности и более широкого промышленного применения мы постоянно разрабатываем новые функции и реагируем на запросы пользователей. Мы предлагаем пользователям обновлять систему до новейшей версии прошивки, чтобы улучшить работу с коммутаторами.

Мы предлагаем 2 способа обновления прошивки с помощью веб-консоли: один - это загрузка файла прошивки с USB-накопителя, а другой – загрузка файла прошивки с ПК. Если файл прошивки находится на ПК, пользователям нужно будет только выбрать файл и нажать кнопку «Применить», чтобы система обновила его автоматически.

Обновление путем загрузки ПО с ПК



- **Firmware Image**
  Нажмите "Select File" для выбора файла прошивки на диске.
- **Selected File**
  После выбора файла прошивки в этом поле показывается его имя.

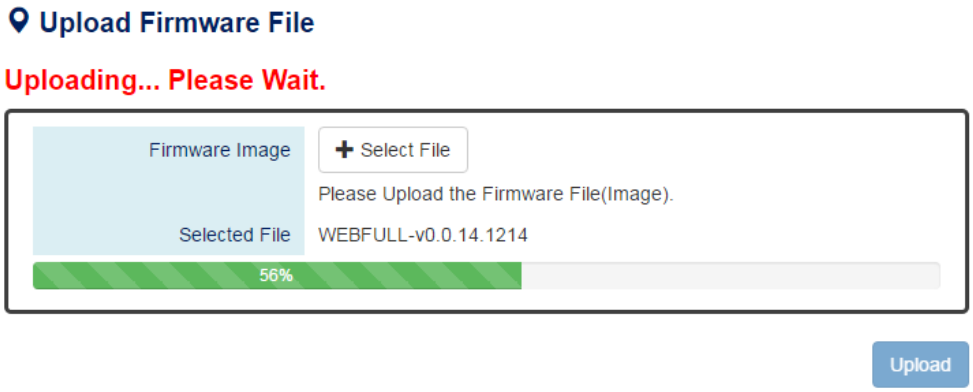


(кнопка Загрузить)

После выбора образа прошивки нажмите кнопку «Загрузить», чтобы загрузить его.

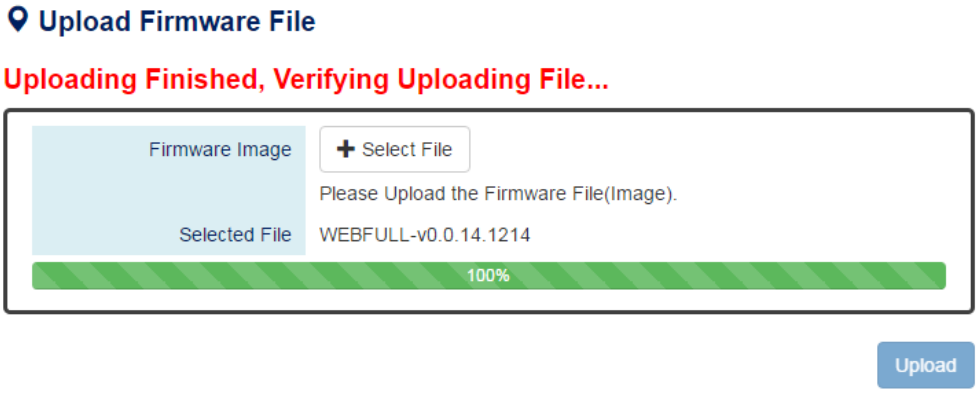
Далее происходит процесс обновления прошивки. Этапы процесса описаны ниже

1. **Загрузка прошивки на коммутатор**
   Индикатор выполнения отображает процент загрузки.



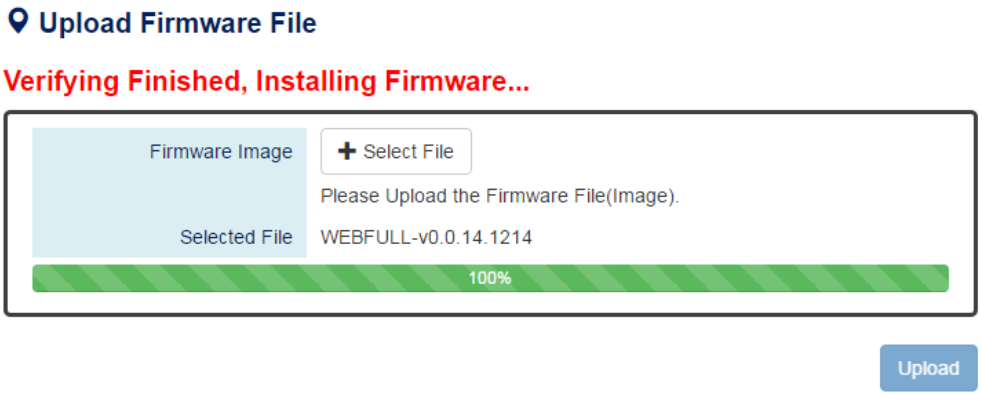
2. **Проверка загруженной прошивки**

   Когда файл загружен на 100%, система начинает проверять загруженный файл, чтобы убедиться, что он исправен. По умолчанию образ прошивки зашифрован, чтобы предотвратить хакерскую атаку на код. По желанию также предоставляется более сложная схема шифрования.



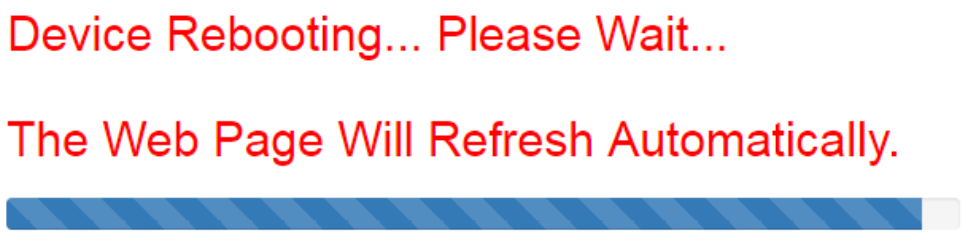
3. **Установка загруженной прошивки**

   Новая прошивка будет установлена после того, как система проверит ее.



4. **Перезагрузка системы**

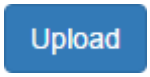
   Система автоматически перезагрузится, если прошивка обновится без каких-либо проблем. Индикатор выполнения отображает прогресс перезагрузки.



Обновление путем загрузки ПО с USB

- **Image File Name**

  Введите имя образа прошивки на USB. Система попытается идентифицировать файл с указанным именем, чтобы загрузить его в систему. Примечание: файловая система USB должна быть FAT32.



(кнопка Загрузки)

После ввода имени образа прошивки нажмите кнопку «Загрузить», чтобы скопировать его с USB-накопителя в систему.

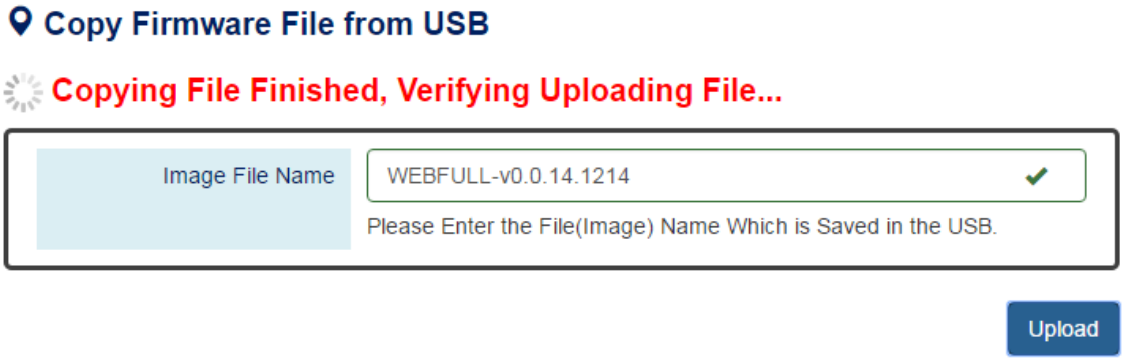
Далее происходит процесс обновления прошивки. Этапы процесса описаны ниже

1. **Копирование прошивки с USB**

   Копирование образа прошивки с USB на коммутатор. Система также проверит, вставлен ли USB-накопитель и существует ли файл.

2. **Проверка загруженного файла прошивки**

   Когда файл загружен на 100%, система начинает проверять загруженный файл, чтобы убедиться, что он исправен. По умолчанию образ прошивки зашифрован, чтобы предотвратить хакерскую атаку на код. По желанию также предоставляется более сложная схема шифрования.



3. **Установка загруженной прошивки**

   Новая прошивка будет установлена после того, как система проверит ее.

4. **Перезагрузка системы**

   Система автоматически перезагрузится, если прошивка обновится без каких-либо проблем. Индикатор выполнения отображает прогресс перезагрузки.

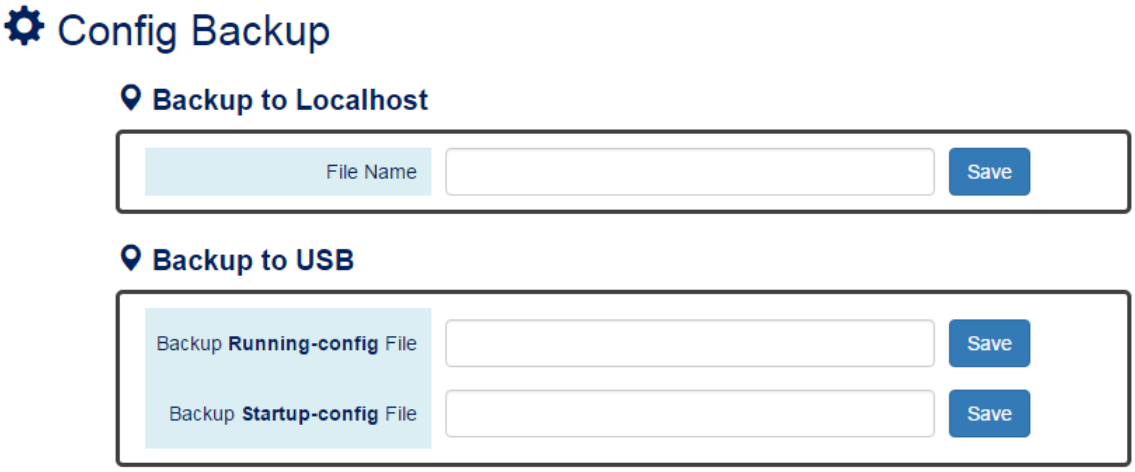
Device Rebooting... Please Wait...

The Web Page Will Refresh Automatically.

Резервное копирование конфигурации

В обычном случае в сети есть несколько коммутаторов, и они могут быть настроены на одни и те же функции. Для облегчения настройки, пользователи могут настроить один из коммутаторов и сохранить файл конфигурации на локальном хосте (например, на ПК пользователя) или на USB-накопителе, а затем восстановить конфигурацию на другом коммутаторе с помощью функции «Config Restore». Файл конфигурации на USB-накопителе также может быть использован для быстрого восстановления настроек в случае их потери.

Сохранение резервной копии



Backup to Localhost

- **File Name**
  Имя файла в который будет сохранен файл Startup-config на локальном хосте.

Backup to USB

Резервированая копия на USB карту памяти. Перед началом сохранения убедитесь, что карта памяти подключена в порт USB коммутатора.

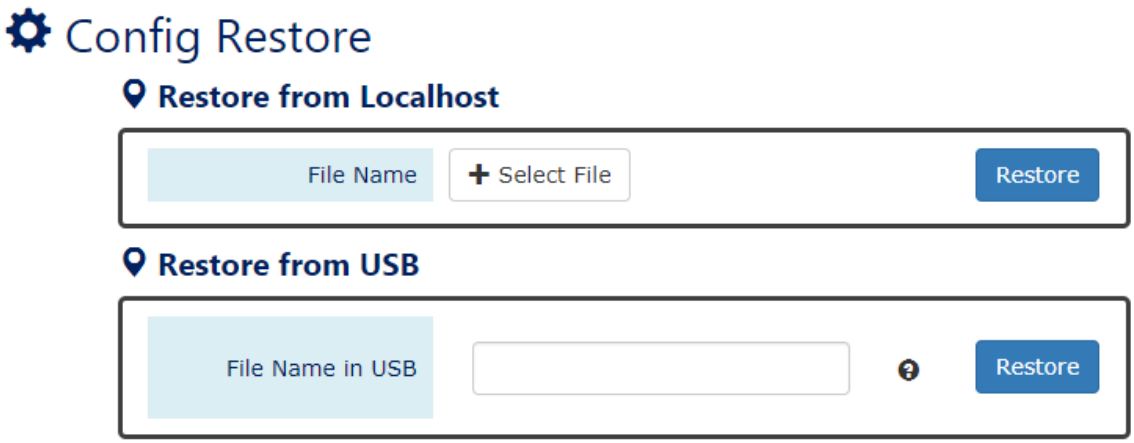
- **Backup Running-config File**
  Имя файла в который будет сохранен файл Running-config на USB карте памяти.
- **Backup Startup-config File**
  Имя файла в который будет сохранен файл Startup-config на USB карте памяти.

Примечание: файловая система USB должна быть FAT32. В имени файла нельзя использовать пробел. Save (кнопка Сохранить)

Нажмите кнопку «Сохранить», чтобы сохранить файл конфигурации на локальный хост или USB. Примечание: если поле имени файла пустое, система назначает имя по умолчанию: config- [datetime].cfg

Восстановление конфигурации

Мы предлагаем пользователям делать резервные копии конфигурации после ряда настроек. Если другому устройству требуются такие же настройки, пользователи могут использовать функцию восстановления конфигурации на этом устройстве.



Restore from Localhost

- **File Name**
  Выберите файл конфигурации, который сохранен на локальном компьютере.

Restore from USB

Убедитесь, что в порт USB вставлен USB-накопитель.

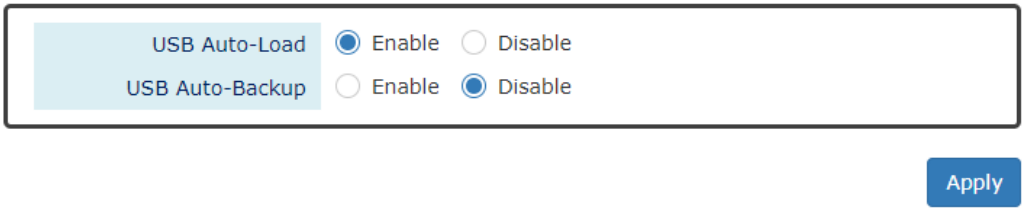
- **File Name in USB**
  Имя файла сохраненной конфигурации на USB. Если файл конфигурации сохранен в каталоге, укажите полный путь. Примечание: файловая система USB должна быть FAT32. В имени файла нельзя использовать пробел.

(кнопка Восстановить)

Нажмите кнопку «Восстановить», чтобы восстановить конфигурации с локального хоста или USB.

Автозагрузка и автоматическое резервирование по USB

Auto Load & Backup



- **USB Auto-Load**

  Автозагрузка по USB. Enable для включения, Disable – для выключения функции автоматической загрузки конфигурации с USB. Если «Автозагрузка по USB» включена, система будет искать файл конфигурации с именем «startup-config» на USB и загружать его при перезагрузке. Примечание: файловая система USB должна быть FAT32.

- **USB Auto-Backup**

  Функция автоматического резервного копирования USB. Если включено, система сохранит конфигурацию в файл с именем «running-config» на USB, когда пользователи изменят настройки коммутатора. Примечание: файловая система USB должна быть FAT32.

Apply (Применить)

После настройки нажмите кнопку Apply, что бы изменения были активированы.

Доступ к файлам по SFTP

Для загрузки конфигурации на SFTP сервер

```
Switch(config)# upload server sftp
  account                 Set uploading server account
  password                Set uploading server password

Switch(config)# upload sftp
Usage: upload sftp [<cr>]
```

Настроить IP-адрес SFTP-сервера

Switch(config)# upload server ip [SERVER_IP]

Настроить имя учетной записи для входа на SFTP-сервер

Switch(config)# upload sftp server account [SERVER_ACCOUNT]

Настроить пароль учетной записи для входа на SFTP-сервер

Switch(config)# upload sftp server password [SERVER_PASSWORD]

Действие для загрузки по SFTP

Switch(config)# upload sftp

Сохранение конфигурации по SFTP

```
Switch(config)# copy sftp
  account                 set sftp server account
  file                    Set uploading file
  ip                      set sftp server ip
  password                set sftp server password
  startup-config          Destination
  usb                     Destination
```

Настроить IP-адрес SFTP-сервера

Switch(config)# copy sftp ip [SERVER_IP]

Настроить имя учетной записи для входа на SFTP-сервер

Switch(config)# copy sftp account [SERVER_ACCOUNT]

Настроить пароль учетной записи для входа на SFTP-сервер

Switch(config)# copy sftp password [SERVER_PASSWORD]

Для загрузки startup-config по SFTP

Switch(config)# copy sftp startup-config

Примечание. После копирования загрузочной конфигурации система автоматически перезагрузится.

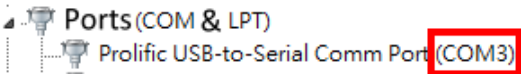
Интерфейс командной строки (CLI)

Интерфейс командной строки обычно называется CLI. Он позволяет пользователям настраивать, контролировать и обслуживать коммутатор путем непосредственного выполнения текстовых команд.

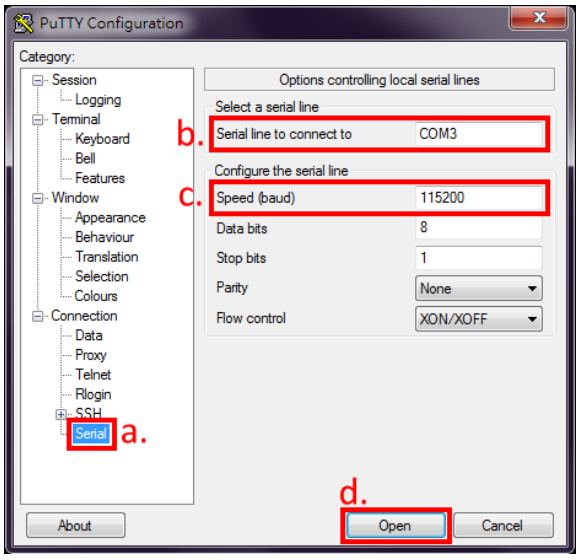
Подключение с помощью консольного порта

Перед началом подключения к консольному порту, убедитесь, что у вас есть соответствующая утилита (например, «Putty», «Tera Term», «HyperTerminal», «SecureCRT» и т.д.), чтобы сделать это. Следующий пример работает в Windows 7 с помощью Putty.

Подключите консольный порт к вашему ПК или ноутбуку и проверьте номер порта в «Диспетчере устройств» на ПК.



Сконфигурируйте порт, указав номер COM-порта и скорость (скорость передачи: 115200). По умолчанию биты данных и четность равны 8 и 1. Затем нажмите «Open», чтобы подключиться к интерфейсу командной строки.

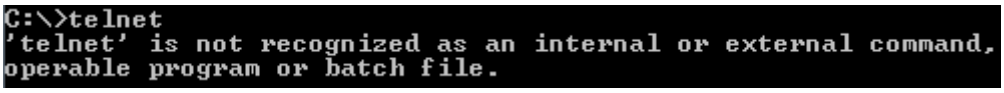


Введите имя пользователя и пароль. Имя пользователя и пароль по умолчанию - **admin/admin**.

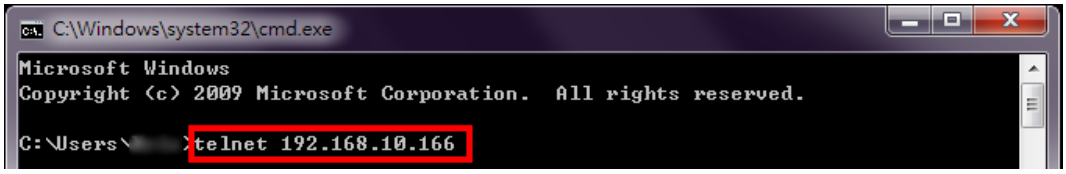
Когда вы видите приглашение вида “Switch>”, это означает что вы успешно зашли в CLI системы.

Подключение по Telnet

Следующий пример работает в Windows 7. Если система отображает информацию, как показано на рисунке ниже, пожалуйста, включите «Telnet Client» перед использованием функции telnet.



Нажмите кнопку Windows «Пуск» и введите «cmd» в поле поиска, чтобы открыть «Командную строку». Введите «telnet [IP_ADDRESS]» в окне CMD. Например, если IP-адрес коммутатора - 192.168.10.166, то введите «telnet 192.168.10.166» и нажмите клавишу «Ввод».



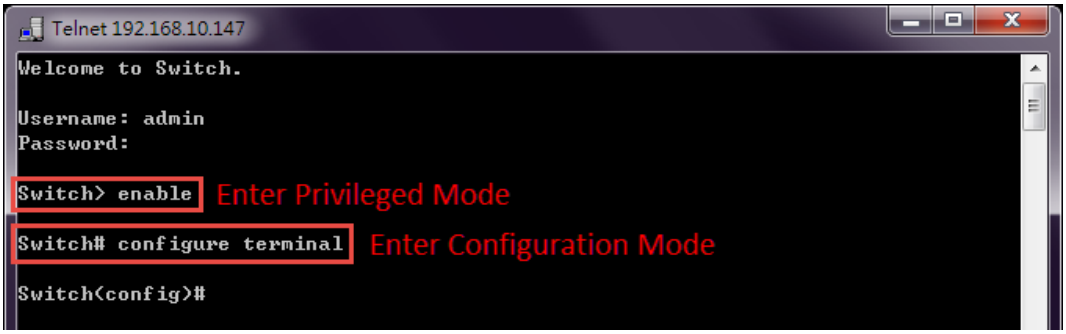
Введите имя пользователя и пароль. Имя пользователя и пароль по умолчанию - **admin/admin**.

Когда вы видите приглашение вида “Switch>”, это означает что вы успешно зашли в CLI системы.

Различные режимы CLI

После входа в интерфейс командной строки пользователи должны войти в привилегированный режим для команд «show». Если пользователи хотят настроить систему через интерфейс командной строки, они должны войти в режим конфигурирования.

Команда для входа в привилегированный режим - “enable”. После входа в привилегированный режим введите команду “configure terminal” для входа в режим конфигурирования. Когда появится приглашение вида“Switch(config)#” с символом # в конце, пользователи могут настраивать параметры коммутатора. В разделе групп команд данного руководства указаны режимы CLI в которых доступны те или иные команды.



В режиме конфигурации есть разные режимы, такие как режим интерфейса (Interface), режим VLAN, режим ERPS и режим MRP. Если команда, которую пользователи готовятся выполнить, находится в этих режимах, они должны сначала войти в назначенный режим. Пользователи могут ввести команду «exit», чтобы выйти из текущего режима. В следующей таблице даны образцы команд для входа в различные режимы.

Режим	Команда	Примечание
Interface	interface lanX	X подразумевает номер порта
VLAN	vlan X	X подразумевает VLAN ID
ERPS	ethernet redundancy erps-ring X	X подразумевает номер кольца от 1 до 3
MRP	ethernet redundancy mrp instance-mode 1	Поддерживается только одно кольцо

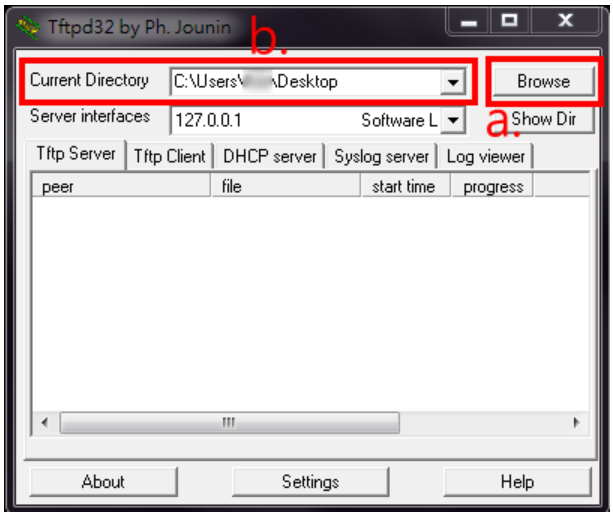
Обновление ПО через CLI

Пользователи могут обновить встроенное ПО с помощью новой прошивки как через веб-интерфейс, так и в режиме командной строки. Для обновления через веб интерфейс см. раздел «Обновление встроенного ПО». Для обновления в режиме CLI существует 3 метода: TFTP, wget (HTTP) и USB. В следующих разделах объясняется, как обновить прошивку этими тремя способами.

С помощью TFTP

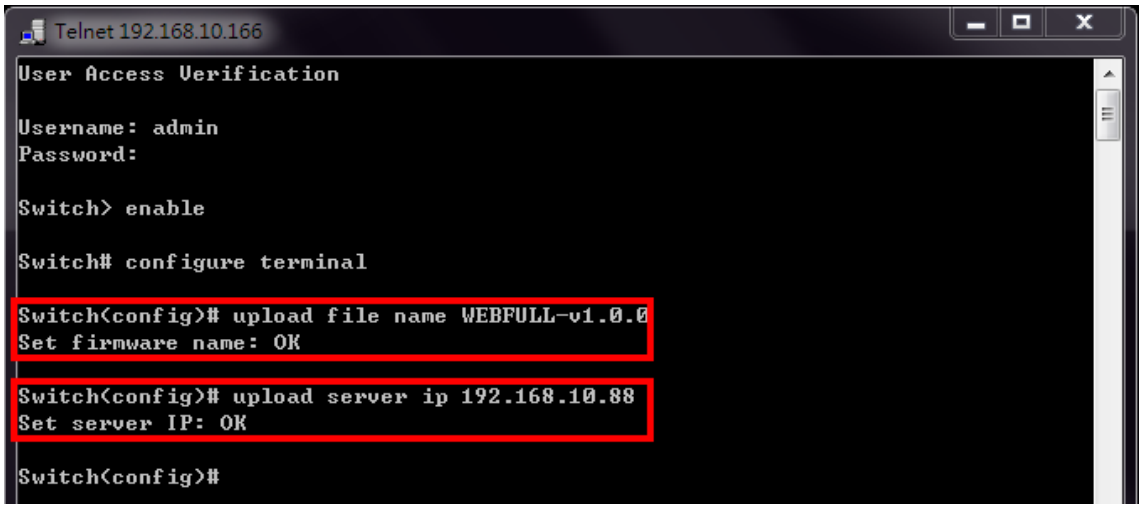
Если вы планируете обновить прошивку через режим CLI с использованием TFTP, перед обновлением необходим сервер TFTP. Вы можете скачать бесплатный TFTP-сервер с официального сайта tftpd.

Откройте сервер TFTP и укажите путь к каталогу файлов. Например, если файл прошивки сохранен на рабочем столе, путь к рабочему столу необходимо указать в поле «Current DIrectory».



Убедитесь, что соединение между коммутатором и хостом (ПК или портативным компьютером) подключено. Чтобы проверить это, запустите ping IP-адреса коммутатора с хоста.

В CLI укажите имя новой прошивки с помощью команды “upload file name [ИМЯ ФАЙЛА]“. Имя файла прошивки по умолчанию: WEBFULL с указанием версии.



Укажите адрес сервера TFTP Server командой “upload server ip [IP АДРЕС]”. IP адрес сервера – это адрес ПК, на котором запущен TFTP сервер.

Не забудьте перейти в режим настройки Configure командой“configure terminal”.

Начните процесс обновления командой “upload tftp”. Обновление займет несколько минут.

```
Telnet 192.168.10.166
User Access Verification

Username: admin
Password:

Switch> enable

Switch# configure terminal

Switch(config)# upload file name WEBFULL-v1.0.0
Set firmware name: OK

Switch(config)# upload server ip 192.168.10.88
Set server IP: OK

Switch(config)# upload tftp
CAUTION: DO NOT SHUTDOWN WHEN THE PROCEDURE IS NOT FINISHED
Uploading firmware via 'tftp'

firmware uploading ...
It may take few seconds or minutes to upload, please wait patiently.
```

После загрузки прошивки на коммутатор, система проверит загруженный файл. Если проверка пройдена успешно, новая прошивка будет установлена. Система перезагрузится автоматически после окончания установки.

```
Telnet 192.168.10.166
verifying firmware ...
It may take 5 - 6 seconds to complete, please wait patiently.
verified OK!

decompressing and extracting ...
It may take 10 - 20 seconds to complete, please wait patiently.
decompression OK!

Start Upgrading Kernel ...
Erasing blocks: 97/97 (100%)
Writing data: 6145k/0k (100%))
Verifying data: 6145k/0k (100%))

Start Upgrading Rootfs ...
libscan: scanning eraseblock 839 -- 100 % complete
ubiformat: 839 eraseblocks have valid erase counter, mean value is 58
ubiformat: 1 bad eraseblocks found, numbers: 170
ubiformat: flashing eraseblock 274 -- 100 % complete
9 -- 100 % complete   eraseblock 838 -- 99 % complete

finished!
System is going to reboot ...
```

Verify

Install

Finished and Reboot

С помощью Wget

Команда Wget использует протокол HTTP для передачи файла на коммутатор. Пользователь должен настроить HTTP сервер такой как, например, Apache и загрузить файл прошивки на этот HTTP сервер.

Предположим, что HTTP сервер настроен по адресу 192.168.1.9 и имя файла прошивки - WEBFULL-v1.0.0.

Далее порядок загрузки следующий:

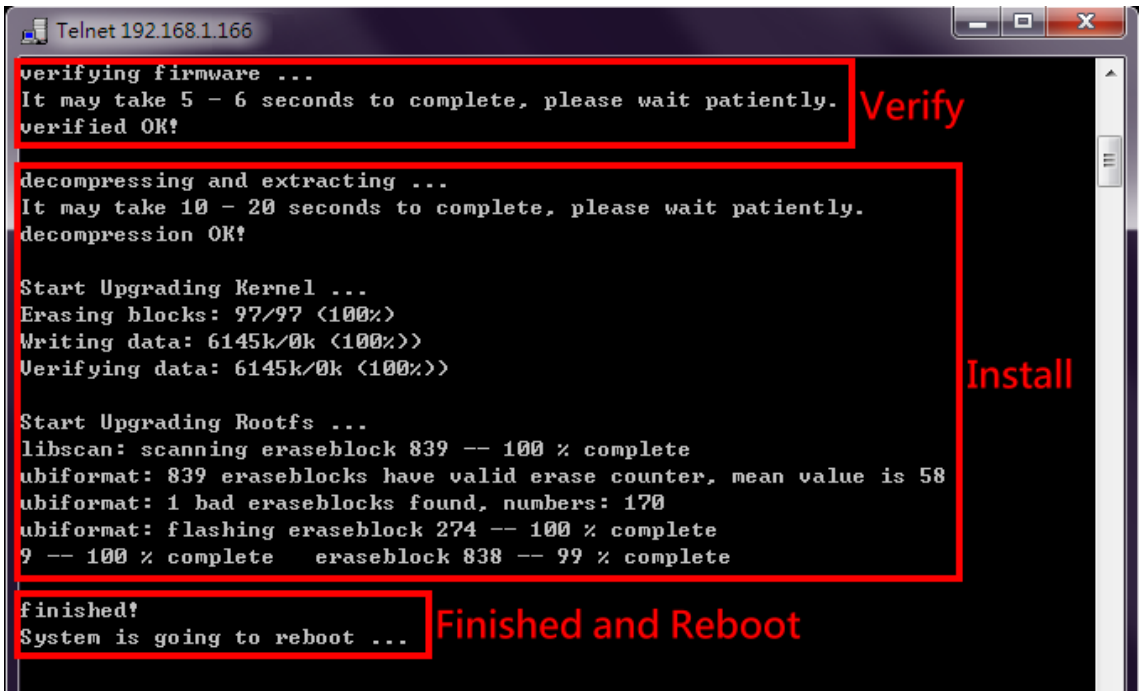
- Убедиться в наличии связи между коммутатором и HTTP-сервером, например командой “ip ping [IP_ADDRESS]”.
- Назначить имя файла для загрузки командой “upload file name WEBFULL-v1.0.0“.
- Назначить адрес сервера для wget командой “upload server ip 192.168.1.9”.
- Если настройки заданы корректно, система выдаст сообщение “OK”.

```
Telnet 192.168.1.166
User Access Verification

Username: admin
Password:

Switch> enable

Switch# configure terminal

Switch(config)# upload file name WEBFULL-v1.0.0
Set firmware name: OK

Switch(config)# upload server ip 192.168.1.9
Set server IP: OK

Switch(config)#
```

- Начать процесс обновления командой “upload wget”. Обновление может занять до нескольких минут.

```
Telnet 192.168.1.166
User Access Verification

Username: admin
Password:

Switch> enable

Switch# configure terminal

Switch(config)# upload wget
CAUTION: DO NOT SHUTDOWN WHEN THE PROCEDURE IS NOT FINISHED
Uploading firmware via 'wget'

firmware uploading ...
It may take few seconds or minutes to upload, please wait patiently.
Connecting to 192.168.1.9 (192.168.1.9:80)
WEBFULL-v1.0.0       100% |*******************************| 27940k  0:00:00 ETA
```

После завершения загрузки система проверит загруженный файл. Если проверка пройдет, будет установлен новый файл прошивки. Убедитесь, что система остается включенной, и система автоматически перезагрузится после полной установки новой прошивки.



С помощью USB

Перед обновлением убедитесь, что файл прошивки сохранен на USB, а USB-накопитель вставлен в USB-порт коммутатора. Используйте команду «copy usb firmware [FILE_NAME]» для обновления системы через USB.

После завершения установки система автоматически перезагрузится. Примечание: файловая система USB должна быть FAT32.

Группы команд CLI

Ниже приведены команды, которые пользователи могут использовать в режиме CLI. Пожалуйста, проверьте правильность выбора режима перед тем, как вводить команду.

Команды аутентификации

Команда	Назначение	Режим
login authentication [tacacs+ | radius]	Set login authentication method	Configure
logout	Disconnect	Configure
radius-server host [IP_ADDR]	Set IP address of RADIUS server	Configure
radius-server key [SHARED_KEY]	Set specific characters for authentication verification	Configure
radius-server port [1-65535]	Set communication port of RADIUS server	Configure
radius-server retransmit [1-1000]	Set the number of times a request re-sending to RADIUS server	Configure
radius-server timeout [1-1000]	Set the timeout period to wait for RADIUS server response	Configure
tacacs-server host [IP_ADDR]	Set IP address of TACASC+ server	Configure
tacacs-server key [SHARED_KEY]	Set specific characters for authentication verification	Configure
tacacs-server port [1-65535]	Set communication port of TACASC+ server	Configure
tacacs-server timeout [1-1000]	Set the timeout period to wait for TACASC+ server response	Configure
username [USER_ID] [PASSWORD]	Configure username and password	Configure
username-ro [USER_ID] [PASSWORD]	Configure read only username and password	Configure
show login authentication	Display login authentication method	Configure
show radius-server host	Display IP address of RADIUS server	Configure
show radius-server key	Display specific characters for authentication verification	Configure
show radius-server port	Display communication port of RADIUS server	Configure
show radius-server retransmit	Display the number of times a request is resent	Configure
show radius-server timeout	Display the timeout period to wait for RADIUS server response	Configure
show tacacs-server host	Display IP address of the server	Configure
show tacacs-server key	Display specific characters for authentication verification	Configure
show tacacs-server port	Display communication port of the server	Configure
show tacacs-server timeout	Display the timeout period to wait for the server response	Configure
show username	Display admin ID	Configure
show username-ro	Display read only user ID	Configure

no login authentication	Default Login authentication method	Configure
no radius-server host	Default IP address of the server	Configure
no radius-server key	Default specific characters for authentication verification	Configure
no radius-server port	Default communication port of the server	Configure
no radius-server retransmit	Default the number of times a request is resent	Configure
no radius-server timeout	Default the timeout period to wait for the server response	Configure
no tacacs-server host	Default IP address of TACACS+ server	Configure
no tacacs-server key	Default specific characters for authentication verification	Configure
no tacacs-server port	Default communication port of TACACS+ server	Configure
no tacacs-server timeout	Default the timeout period to wait for TACACS+ server response	Configure
no username	Default username and password	Configure
no username-ro	Default read only username and password	Configure

Команды SSH

Команда	Назначение	Режим
copy host-key-config usb [FILE_NAME]	Backup SSH host key to USB	Configure
copy usb host-key-config [file]	Upload SSH host key config from USB	Configure
download file name [FILE_NAME]	Set downloading file name, default name is host_key.cfg	Configure
download host-key-config	Download current SSH host key config	Configure
download server account [SERVER_ACCOUNT]	Set downloading server account	Configure
download server ip [SERVER_IP]	Set downloading server IP Address	Configure
download server password [SERVER_PASSWORD]	Set downloading server password	Configure
upload host-key-config wget [file]	Upload SSH host key config from Localhost	Configure
show ssh host-key	Display SSH host key	Configure

Системные команды

Команда	Назначение	Режим
erase startup-config	Reset to factory default and reboot	Configure
erase startup-config keep-ip	Reset to factory default except IP	Configure
erase startup-config keep-ip-user	Reset to factory default except IP and USER	Configure
erase startup-config keep-user	Reset to factory default except USER ID/PASS	Configure
exec-timeout [MINUTE] [SECOND]	Set idle timeout [MINUTE] [SECOND]	Configure
hostname [HOSTNAME]	Set Switch Host Name	Configure
reboot	Reboot the switch	Configure

system contact [CONTACT]	Set system contact	Configure
system description [SYS_DESCRIPTION]	Set device description	Configure
system location [LOCATION]	Set device location	Configure
show exec-timeout	Display idle timeout	Configure
show hostname	Display Switch Host Name	Configure
show environment power [1|2]	Display power 1/2 status	Configure
show event status relay	Display relay status	Configure
show system contact	Display system contact	Configure
show system description	Display system description	Configure
show system firmware-date	Display system release time	Configure
show system location	Display system location	Configure
show system mac	Display system MAC address	Configure
show system uptime	Display system uptime	Configure
show system version firmware	Display system version	Configure
show transceiver ddm	Display transceiver DDM information	Interface
show transceiver info	Display transceiver information	Interface
show transceiver raw	Display transceiver raw data	Interface
show username	Display admin ID	Configure
no exec-timeout	Default idle timeout	Configure
no hostname	Default Switch Host Name	Configure
no system contact	Clear system contact	Configure
no system description	Clear device description	Configure
no system location	Clear device location	Configure
no username	Default username and password	Configure

Команды контроля сервисов

Команда	Назначение	Режим
service [http | https | ssh | telnet | console | reset-button] enable	Enable service http, https, ssh, telnet, console port, or reset button	Configure
show service [http | https | ssh | telnet | console | reset-button]	Display service http, https, ssh, telnet, console port, or reset button state	Configure
no service [http | https | ssh | telnet | console | reset-button]	Disable service http, https, ssh, telnet, console port, or reset button	Configure

Команды IPv4

Команда	Назначение	Режим
ip address [IP_ADDR] [MASK]	Set IPv4 address and netmask	Configure
ip default-gateway [DEFAULT_GATEWAY_ADDR]	Set default gateway address	Configure
ip name-server [NAME_SERVER_IP]	Set Domain Name-Server	Configure

ip ping [IPV4_ADDR] [<size PKG_SIZ> | <repeat PKG_CNT>]	Issue an IPv4 ping command	Configure
show ip address	Display Host address of IPv4	Configure
show ip default-gateway	Display default gateway address	Configure
show ip mode	Display IP mode (Static or Dynamic)	Configure
show ip name-server	Display Domain Name-Server	Configure
no ip address	Delete IPv4 address	Configure
no ip default-gateway	Clear the default gateway address	Configure
no ip name-server	Clear the domain name-server	Configure

Команды IPv6

Команда	Назначение	Режим
ipv6 address add [IPV6_ADDR</PREFIX_LEN>]	Add an address and netmask of IPv6	Configure
ipv6 enable	Enable IPv6 protocol	Configure
ipv6 neighbor flush	Issue a neighbor flush command of IPv6	Configure
ipv6 ping [IPV6_ADDR] [<size PKG_SIZ> | <repeat PKG_CNT>]	Issue an IPv6 ping command	Configure
show ipv6	Display IPv6 protocol state	Configure
show ipv6 address	Display IPv6 addresses	Configure
show ipv6 default address	Display default IPv6 address	Configure
show ipv6 neighbor	Display neighbor cache of IPv6	Configure
no ipv6	Disable IPv6 protocol	Configure
no ipv6 address add [IPV6_ADDR/PREFIX_LEN]	Delete IPv6 address	Configure

Команды настройки даты/времени

Команда	Назначение	Режим
clock time [hh:mm:ss] [day] [month] [year]	Configure time	Configure
clock timezone [AREA] [CITY]	Configure time zone	Configure
ntp client sync [minute | hour | day | month | year] [NUMBER]	Configure NTP client sync	Configure
ntp client timeserver1 [SERVER_IP/URL]	Configure NTP client time server 1	Configure
ntp client timeserver2 [SERVER_IP/URL]	Configure NTP client time server 2	Configure
ntp time update	Configure NTP time update	Configure
show clock time	Show time	Configure
show clock timezone	Show timezone	Configure
show ntp client sync	Show sync time	Configure
show ntp client timeserver1	Show NTP server 1 configuration	Configure
show ntp client timeserver2	Show NTP server 2 configuration	Configure
no clock timezone	Remove timezone	Configure

no ntp client sync	Remove NTP sync time	Configure
no ntp client timeserver1	Remove NTP time server 1 configuration	Configure
no ntp client timeserver2	Remove NTP time server 2 configuration	Configure

Команды PTP

Команда	Назначение	Режим
ptp announce interval [-1 to 7]	Set PTP announce interval, the interval is expressed as log 2. i.e. -1 is 0.5s, 0 is 1s.	Configure
ptp announce timeout [2-255]	Set PTP announce timeout	Configure
ptp disable	Disable PTP	Configure
ptp domain [0-127]	Set PTP domain number	Configure
ptp enable	Enable PTP	Configure
ptp interface1	Set the interface to master of boundary clock mode	Configure
ptp interface2	Set the interface to slave of boundary clock mode	Configure
ptp mode [m(master) | s(slave) | b(boundary clock)]	Set PTP mode	
ptp period [0-20]	Set PTP timeout periods	Configure
ptp priority1 [0-248]	Set PTP priority1	Configure
ptp priority2 [0-248]	Set PTP priority2	Configure
ptp sync interval [-7 to 7]	Set PTP sync interval, the interval is expressed as log 2. i.e. -1 is 0.5s, 0 is 1s.	Configure
show ptp announce interval	Display PTP announce interval	Configure
show ptp announce timeout	Display PTP announce timeout	Configure
show ptp clock	Display PTP sync information	Configure
show ptp domain	Display PTP domain number	Configure
show ptp enable	Display PTP status	Configure
show ptp interface1	Display PTP interface1	Configure
show ptp interface2	Display PTP interface2	Configure
show ptp mode	Display PTP mode	Configure
show ptp period	Display PTP timeout periods	Configure
show ptp priority1	Display PTP priority1	Configure
show ptp priority2	Display PTP priority2	Configure
show ptp sync interval	Display PTP sync interval	Configure
no ptp announce interval	Default PTP announce interval	Configure
no ptp announce timeout	Default PTP announce timeout	Configure
no ptp domain	Default PTP domain number	Configure
no ptp interface1	Default PTP interface1	Configure

no ptp interface2	Default PTP interface2	Configure
no ptp mode	Default PTP mode	Configure
no ptp period	Default PTP timeout periods	Configure
no ptp priority1	Default PTP priority1	Configure
no ptp priority2	Default PTP priority2	Configure
no ptp sync interval	Default PTP sync interval	Configure

Команды STP

Команда	Назначение	Режим
spanning-tree forward-time [4-30]	Set STP forward time	Configure
spanning-tree hello-time [1-10]	Set STP hello time	Configure
spanning-tree max-age [6-40]	Set max age	Configure
spanning-tree mode [rstp]	Set STP mode as [RSTP]	Configure
spanning-tree mst instance [1-15] vlan [VLAN_LIST]	Set vlan group for specific MSTP instance	Configure
spanning-tree mst name [NAME]	Set MSTP name	Configure
spanning-tree mst revision [0-65535]	Set MSTP revision	Configure
spanning-tree mst [1-15] priority [0-61440]	Set priority for specific MSTP instance	Configure
spanning-tree priority [0-61440]	Set STP priority	Configure
spanning-tree cost [0-200000000]	Configure STP cost	Interface
spanning-tree edge [admin-edge|admin-non-edge]	Configure STP edge	Interface
spanning-tree link-type [point-to-multiple|point-to-point]	Configure STP link type on port	Interface
spanning-tree mst [1-15] cost [0- 200000000]	Configure port cost for specific MSTP instance	Interface
spanning-tree mst [1-15] port-priority [0-200000000]	Configure port priority for specific MSTP instance	Interface
spanning-tree port-priority [0-240]	Configure STP port priority	Interface
spanning-tree stp disable	Disable Spanning Tree Protocol (STP) on port	Interface
show spanning-tree forward-time	Show STP forward time	Configure
show spanning-tree hello-time	Show STP hello time	Configure
show spanning-tree max-age	Show STP max age	Configure
show spanning-tree mode	Show Spanning Tree mode (RSTP or disable)	Configure
show spanning-tree mst instance [1-15] vlan	Show vlan group for specific MSTP instance	Configure
show spanning-tree mst name	Show MSTP name	Configure
show spanning-tree mst revision	Show MSTP revision	Configure
show spanning-tree mst [1-15] priority	Show priority for specific MSTP instance	Configure
show spanning-tree mst [1-15] status	Show bridge status for specific MSTP instance	Configure
show spanning-tree priority	Show STP priority	Configure

show spanning-tree rstp-status	Show Spanning Tree rstp status	Configure
show spanning-tree cost	Show STP cost	Interface
show spanning-tree edge	Show STP auto edge	Interface
show spanning-tree link-type	Show STP link type	Interface
show spanning-tree mst [1-15] cost	Show port cost for specific MSTP instance	Interface
show spanning-tree mst [1-15] port-priority	Show port priority for specific MSTP instance	Interface
show spanning-tree port-priority	Show STP port priority	Interface
show spanning-tree stp	Show STP activated status on port	Interface
no spanning-tree forward-time	Remove STP forward time configuration	Configure
no spanning-tree hello-time	Remove STP hello time configuration	Configure
no spanning-tree max-age	Remove STP max age configuration	Configure
no spanning-tree mode	Disable STP configuration	Configure
no spanning-tree priority	Remove STP priority configuration	Configure
no spanning-tree cost	Remove STP cost configuration	Interface
no spanning-tree edge	Remove auto edge configuration	Interface
no spanning-tree link-type	Remove link type configuration	Interface
no spanning-tree mst [1-15] cost	Remove port cost for specific MSTP instance	Interface
no spanning-tree mst [1-15] port-priority	Remove port priority for specific MSTP instance	Interface
no spanning-tree port-priority	Remove STP port priority configuration	Interface
no spanning-tree stp	Enable STP on port	Interface

Команды ERPS

Команда	Назначение	Режим
ethernet redundancy erps-ring [1 | 2 | 3]	Ethernet Ring Protection Switching (ERPS) mode	Configure
aps-channel [1 - 4094]	Set APS channel	ERPS
disable	Disable ERPS function	ERPS
enable	Enable ERPS function	ERPS
erps-ring [1 | 2 | 3]	Change to Other ERPS Ring	ERPS
ext-command clear	Extended ERPS command - Clear	ERPS
ext-command fs	Extended ERPS command – Forced Switch	ERPS
ext-command ms	Extended ERPS command – Manual Switch	ERPS
id [1 - 239]	Set Ring ID	ERPS
mel [0 - 7]	ERPS mel	ERPS
revertive	Set as revertive mode	ERPS
ring-port 0 [1(lan1) - N(lanN)]	Mapping ERPS ring port0 to switch port	ERPS
ring-port 1 [1(lan1) - N(lanN)]	Mapping ERPS ring port1 to switch port	ERPS
role port0 [o(owner) | n(neigh) | i(interconn)]	Set role on ring port0	ERPS
role port1 [o(owner) | n(neigh) | i(interconn)]	Set role on ring port1	ERPS

timer guard [10 - 2000]	Set guard timer interval	ERPS
timer hold-off [0 - 10000]	Set hold-off timer interval	ERPS
timer wtr [1 - 12]	Set WTR timer interval	ERPS
type [m(major-ring) | s(sub-ring)]	Set type as Major-Ring or Sub-Ring	ERPS
virtual-channel major-ring channel-id [1-4094]	Set virtual channel for ERPS Ring	ERPS
virtual-channel sub-ring set	Set virtual channel for ERPS Sub-ring	ERPS
show config	Displays ERPS configuration	ERPS
show port status	Displays ERPS ring port status	ERPS
show status	Displays ERPS status	ERPS
no aps-channel	Default ERPS aps-channel	ERPS
no id	Default Ring ID as default	ERPS
no revertive	Default mode non-revertive	ERPS
no ring-port 0	Default ring port0 as lan1	ERPS
no ring-port 1	Default ring port1 as lan2	ERPS
no role port0	Default role of ring port0 as none	ERPS
no role port1	Default role of ring port1 as none	ERPS
no timer guard	Default guard timer	ERPS
no timer hold-off	Default hold-off timer	ERPS
no timer wtr	Default wtr timer	ERPS
no type	Default ring type as Major-Ring	ERPS
no virtual-channel major-ring channel-id	Default virtual channel as ERPS Major Ring's aps-channell	ERPS
no virtual-channel sub-ring set	Default virtual channel for ERPS Sub-ring as None	ERPS

Команды MRP

Команда	Назначение	Режим
ethernet redundancy mrp instance-mode [1]	Media Redundancy Protocol (MRP) mode	Configure
advanced-mode [enable | disable]	Enable/Disable MRP Advanced Mode	MRP
domain-id [DOMAIN_ID]	Set MRP Domain-id, the format is 16 bytes in decimal notaion	MRP
name [DOMAIN_NAME]	Set MRP Domain Name	MRP
operation [enable | disable]	Enable/Disable MRP Protocol	MRP
port 1 [1(lan1) - N(lanN)]	Set MRP ring-port 1 ID	MRP
port 2 [1(lan1) - N(lanN)]	Set MRP ring-port 2 ID	MRP
recovery-delay [500 | 200]	Set MRP Recovery Delay (unit: ms)	MRP
role [m(manager) | c(client)]	Set MRP Role to MRM(manager) or MRC(client)	MRP
show advanced-mode	Display MRP Advanced-mode	MRP

show config	Display MRP Domain Config	MRP
show domain-id	Display MRP Domain ID	MRP
show name	Display MRP Domain Name	MRP
show operation	Display MRP Operation Status	MRP
show port [1 | 2]	Display MRP ring-port [1 | 2] ID	MRP
show recovery-delay	Display MRP Recovery Delay	MRP
show role	Display MRP Domain Expected Role	MRP
show summary	Display MRP Domain Summary	MRP
no domain-id	Default MRP Domain ID	MRP
no name	Clear MRP Domain Name	MRP
no port [1 | 2]	Default MRP ring-port [1 | 2] ID	MRP
no recovery-delay	Default MRP Recovery Delay	MRP
no role	Default MRP Domain role	MRP

Команды SNMP

Команда	Назначение	Режим
snmp server community ro [COMMUNITY]	Set v1, v2c snmp server read-only community	Configure
snmp server community rw [COMMUNITY]	Set v1, v2c snmp server read-write community	Configure
snmp server enable	Enable snmp server	Configure
snmp server enable v1-v2c-only	Enable snmp v1 and v2c	Configure
snmp server enable v3-only	Enable snmp v3 command only	Configure
snmp server v3 auth admin [md5| sha] [PASSWORD]	Set SNMPv3 admin authentication type	Configure
snmp server v3 auth user [md5| sha] [PASSWORD]	Set SNMPv3 user authentication type	Configure
snmp server v3 encryption admin [des| aes] [PASSWORD]	Set SNMPv3 admin encryption type	Configure
snmp server v3 encryption user [des| aes] [PASSWORD]	Set SNMPv3 user encryption type	Configure
snmp server v3 level admin [auth| noauth| priv]	Set SNMPv3 admin security level	Configure
snmp server v3 level user [auth| noauth| priv]	Set SNMPv3 user security level	Configure
snmp trap community [COMMUNITY]	Set v1, v2c snmp trap community	Configure
snmp trap host1 [TRAP_HOST_IP]	Set snmp trap host 1 IP address	Configure
snmp trap host2 [TRAP_HOST_IP]	Set snmp trap host 2 IP address	Configure
snmp trap inform retry [1-100]	Set snmp inform retry times	Configure
snmp trap inform timeout [1-300]	Set snmp inform timeout	Configure
snmp trap v3 auth [sha| md5] [PASSWORD]	Set SNMPv3 authentication type: md5 or sha	Configure
snmp trap v3 encryption [des| aes] [PASSWORD]	Set SNMPv3 encryption type: des or aes	Configure
snmp trap v3 engine-ID [ENGINE_ID]	Set snmp trap engine ID	Configure
snmp trap v3 level [auth| noauth| priv]	Set SNMPv3 trap security level	Configure

snmp trap v3 user [USER_ID]	Set SNMPv3 trap user	Configure
snmp trap version [1| 2c trap| 2c inform| 3 trap| 3 inform]	Set snmp trap version and type	Configure
show snmp server	Display snmp server status	Configure
show snmp server community ro	Display snmp server read only community	Configure
show snmp server community rw	Display snmp server writable community	Configure
show snmp server v3 auth admin	Display SNMPv3 admin authentication type and passphrase	Configure
show snmp server v3 auth user	Display SNMPv3 user authentication type and passphrase	Configure
show snmp server v3 encryption admin	Display SNMPv3 admin encryption type and passphrase	Configure
show snmp server v3 encryption user	Display SNMPv3 user encryption type and passphrase	Configure
show snmp server v3 level admin	Display SNMPv3 admin security level	Configure
show snmp server v3 level user	Display SNMPv3 user security level	Configure
show snmp trap community	Display snmp trap community	Configure
show snmp trap host1	Display snmp trap host 1	Configure
show snmp trap host2	Display snmp trap host 2	Configure
show snmp trap inform retry	Display snmp inform retry times	Configure
show snmp trap inform timeout	Display snmp inform timeout	Configure
show snmp trap v3 auth	Display SNMPv3 authentication type and passphrase	Configure
show snmp trap v3 encryption	Display SNMPv3 encryption type and passphrase	Configure
show snmp trap v3 engine-ID	Display snmp trap engine ID	Configure
show snmp trap v3 level	Display SNMPv3 trap security level	Configure
show snmp trap v3 user	Display SNMPv3 trap user	Configure
show snmp trap version	Display snmp trap version and type	Configure
no snmp server	Disable snmp server	Configure
no snmp server community ro	Default ro-community name	Configure
no snmp server community rw	Default rw-community name	Configure
no snmp server v3 auth admin	Default SNMPv3 admin authentication type	Configure
no snmp server v3 auth user	Default SNMPv3 user authentication type	Configure
no snmp server v3 encryption admin	Default SNMPv3 admin encryption type	Configure
no snmp server v3 encryption user	Default SNMPv3 user encryption type	Configure
no snmp server v3 level admin	Default SNMPv3 admin security level	Configure
no snmp server v3 level user	Default SNMPv3 user security level	Configure

no snmp trap community	Default snmp trap community	Configure
no snmp trap host1	Default snmp trap host 1	Configure
no snmp trap host2	Default snmp trap host 2	Configure
no snmp trap inform retry	Default snmp inform retry times	Configure
no snmp trap inform timeout	Default snmp inform timeout	Configure
no snmp trap v3 auth	Default SNMPv3 authentication type and passphrase	Configure
no snmp trap v3 encryption	Default SNMPv3 encryption type and passphrase	Configure
no snmp trap v3 engine-ID	Default snmp trap engine ID	Configure
no snmp trap v3 level	Default SNMPv3 trap security level	Configure
no snmp trap v3 user	Default SNMPv3 trap user	Configure
no snmp trap version	Default snmp trap version	Configure

Команды DHCP

Команда	Назначение	Режим
boot host dhcp	Directs the system to get an IP address	Configure
dhcp relay information option	Set DHCP-relay option	Configure
dhcp relay server [server_number: 1-4] [server_IP]	Set DHCP-relay server [1-4] IP	Configure
dhcp relay untrust	Set DHCP-relay untrusted port	Interface
dhcp server binding [bind_ID: 1 - 32] [MAC] [IP_TO_BIND]	Set binding IP and MAC of DHCP	Configure
dhcp server default-gateway [IP_ADDR]	Set default-gateway IP for DHCP client	Configure
dhcp server included-address [START_OF_IP] [END_OF_IP]	Set IP range for its client	Configure
dhcp server lease-time [60-2592000]	Set DHCP server lease time	Configure
dhcp server name-server [IP_ADDR]	Set name-server address for DHCP client	Configure
dhcp service relay enable	Enable DHCP relay	Configure
dhcp service server enable	Enable DHCP server	Configure
show boot host dhcp	Display DHCP client state	Configure
show dhcp relay information option	Display DHCP relay option	Configure
show dhcp relay server [server_number: 1-4]	Display DHCP relay address	Configure
show dhcp relay untrust	Display DHCP untrusted port status	Interface
show dhcp server binding	Display all DHCP bounding entries	Configure
show dhcp server default-gateway	Display DHCP default-gateway IP	Configure
show dhcp server included-address	Display DHCP included IP range	Configure
show dhcp server lease	Display DHCP lease entries	Configure
show dhcp server lease-time	Display DHCP server lease time	Configure
show dhcp server name-server	Display DHCP name-server	Configure

show dhcp server status	Display DHCP server status	Configure
show dhcp service relay	Display DHCP relay agent status	Configure
show dhcp service server	Display DHCP server status	Configure
no boot host dhcp	Disable DHCP client	Configure
no dhcp relay information option	Disable DHCP relay option	Configure
no dhcp relay server [server_number: 1-4]	Remove DHCP relay server [1-4] IP	Configure
no dhcp relay untrust	Default port as trusted	Interface
no dhcp server binding [bind_ID: 1-32]	Remove DHCP bounding IP and MAC	Configure
no dhcp server default-gateway	Remove DHCP default-gateway IP	Configure
no dhcp server included-address	Remove DHCP included IP range	Configure
no dhcp server lease-time	Remove DHCP lease time	Configure
no dhcp server name-server	Remove DHCP name-server	Configure
no dhcp service relay	Disable DHCP relay	Configure
no dhcp service server	Disable DHCP server	Configure

Команды индустриальных протоколов

Команда	Назначение	Режим
ethernet-ip enable	Enable EtherNet/IP Protocol	Configure
modbus tcp enable	Enable Modbus/TCP Protocol	Configure
profinet enable	Enable PROFINET Protocol	Configure
show ethernet-ip	Show EtherNet/IP status	Configure
show modbus tcp	Show Modbus/TCP status	Configure
show profinet	Show PROFINET status	Configure
no ethernet-ip	Disable EtherNet/IP Protocol	Configure
no modbus tcp	Disable Modbus/TCP Protocol	Configure
no profinet	Disable PROFINET Protocol	Configure

Команды UPnP

Команда	Назначение	Режим
upnp advertisement interval [300-86400]	Set UPnP advertisement interval	Configure
upnp enable	Enable Universal Plug and Play (UPnP)	Configure
show upnp	Display Universal Plug and Play (UPnP) state	Configure
show upnp advertisement interval	Display UPnP advertisement interval	Configure
no upnp	Disable Universal Plug and Play (UPnP)	Configure
no upnp advertisement interval	Default UPnP advertisement interval	Configure

Команды настройки портов

Команда	Назначение	Режим
eee port-enable	802.3az (EEE) port enable	Interface
flowcontrol [on | off]	Configure port's flow-control to response a pause frame	Interface

name [PORT_NAME]	Set interface name	Interface
shutdown	Disable port	Interface
speed_duplex [10 | 100] [full | half]	Configure port's speed and duplex	Interface
show interface all link summary	To display interface link status globally	Configure
show administrate	To display port's admin state	Interface
show eee port-all	Display EEE port-all status	Configure
show eee-info	Display Port EEE statistic information	Interface
show flowcontrol	Display port's flow-control state	Interface
show link duplex	To display port's duplex	Interface
show link rx	To display port's Rx_Bytes	Interface
show link speed	To display port's speed	Interface
show link state	To display port's link state	Interface
show link summary	To display port's link summary	Interface
show link tx	To display port's Tx_Bytes	Interface
show name	To display port's name	Interface
show speed_duplex	To display port's speed and duplex	Interface
show transceiver	Transceiver information	Interface
no eee port-enable	802.3az (EEE) port disable	Interface
no flowcontrol	Default flow-control as Auto mode	Interface
no name	Remove port's name	Interface
no shutdown	Enable port	Interface
no speed_duplex	Default port speed-duplex as Auto mode	Interface

Команды PoE

Команда	Назначение	Режим
power inline budget [1-240]	Power PoE budget	Configure
power inline mode-config disable	Disable PoE on port	Interface
power inline mode-config enable	Enable PoE on port	Interface
power inline mode-config force	Force PoE powered on port	Interface
power inline priority [1-3]	Set PoE port priority on port; 1:high, 2:middle, 3:low	Interface
keepalive enable	Enable PoE keepalive	Interface
keepalive hold-time	Configure PoE keepalive power cycle hold-time	Interface
keepalive ip	Configure IP for PoE keepalive	Interface
keepalive time	Configure PoE keepalive cycle time	Interface
schedule enable	Enable one port PoE schedule	Interface
schedule [Sunday-Saturday] open-time [time]	Configure PoE schedule open time on one day	Interface
show power inline budget	Display PoE power budget	Configure

show power inline detail-code	Display PoE status code, refer to “Отладочные коды PoE” for more explanation	Interface
show power inline operation	Display All PoE ports operation status	Configure
show power inline status	Display All PoE ports detail status	Configure
show power inline status	Display PoE status for specific port	Interface
show power inline temperature	Display temperature of PoE controller	Configure
show keepalive table	Display All PoE keepalive info	Configure
show power inline status	Display PoE status	Interface
show keepalive	Show PoE keepalive status	Interface
show keepalive hold-time	Show PoE keepalive hold-time	Interface
show keepalive ip	Show IP for PoE keepalive	Interface
show keepalive time	Show PoE keepalive cycle time	Interface
show schedule	Disable Universal Plug and Play (UPnP)	Interface
show schedule [Sunday-Saturday] open-time	Show open time of POE schedule on one day	Interface
show schedule table	Show one port PoE schedule table	Interface
no power inline budget	Default PoE power budget	Configure
no power inline mode-config	Default PoE powered config on port	Interface
no power inline priority	Disable PoE port priority on port	Interface
no keepalive	Disable PoE keepalive	Interface
no keepalive hold-time	Default PoE keepalive power cycle hold-time	Interface
no keepalive ip	Remove IP for PoE keepalive	Interface
no keepalive time	Remove PoE keepalive cycle time	Interface
no schedule	Remove one port PoE schedule	Interface
no schedule [Sunday-Saturday] open-time	Remove PoE schedule on one day	Interface

Команды IGMP Snooping

Команда	Назначение	Режим
igmp snooping enable	Enable IGMP snooping	Configure
igmp snooping last-member count [2-10]	Set IGMP last-member-count	Configure
igmp snooping last-member interval [1-25]	Set IGMP last-member-interval	Configure
igmp snooping querier enable	Enable IGMP snooping querier	Configure
igmp snooping query interval [1-3600]	Set IGMP query interval	Configure
igmp snooping query max-respond-time [1-12]	Set IGMP max-query-respond time	Configure
igmp snooping query version [VLAN_ID] [STATE:0|1] [VERSION:1|2|3]	Add IGMP query version entry by VLAN ID. STATE 0: disable; STATE 1: enable	Configure
igmp snooping router-port [PORT_LIST]	Set router port list for multicast	Configure
igmp snooping unknown-multicast [f|d|r]	Set unknown-multicast action	Configure
show igmp snooping all	Display IGMP settings (summary)	Configure
show igmp snooping mdb	Display IGMP multicast database	Configure

show igmp snooping query-version	Display IGMP Query version by VLAN ID	Configure
show igmp snooping router-port	Display IGMP router port list	Configure
show igmp snooping unknown-multicast	Display unknown-multicast action	Configure
no igmp snooping	Disable IGMP snooping	Configure
no igmp snooping last-member count	Default IGMP Last-Member-Count	Configure
no igmp snooping last-member interval	Default IGMP Last-Member-Interval	Configure
no igmp snooping querier	Disable IGMP querier	Configure
no igmp snooping query interval	Default IGMP query interval	Configure
no igmp snooping query max-respond-time	Default IGMP max-respond-time	Configure
no igmp snooping router-port	Default IGMP router port	Configure
no igmp snooping unknown-multicast	Default unknown-multicast action	Configure

Команды VLAN

Команда	Назначение	Режим
provider ethertype [VALUE_IN_HEX (i.e., 0x88A8)]	Setup EtherType in S-TAG for provider port	Configure
member [untag PORT_LIST] [tag PORT_LIST]	Set VLAN member	VLAN
name [VLAN_NAME]	Set VLAN Name	VLAN
switchport accept [tagged | untagged]	Set VLAN acceptance of frame	Interface
switchport mode [d(dot1q-tunnel)| c(customer)| p(provider)| s(specific-provider)]	Configure port type as dot1q-tunnel, Customer, or Service Provider	Interface
switchport pvid [PVID: 1-4094]	Set port VLAN-Id	Interface
show provider ethertype	Display Service Provider EtherType	Configure
show vlan global	Display VLAN Global information	Configure
show member	Display port VLAN member	VLAN
show name	Displaty VLAN name	VLAN
show switchport accept	Display acceptance of VLAN frame	Interface
show switchport mode	Display VLAN interface port type	Interface
show switchport pvid	Display port VLAN-Id	Interface
no provider ethertype	Default EtherType as 0x88A8 in S-TAG for provider port	Configure
no member	Default VLAN member	VLAN
no name	Default VLAN name	VLAN
no switchport accept	Default acceptance of VLAN frame	Interface
no switchport mode	Default port type as Customer	Interface
no switchport pvid	Default port VLAN-Id	Interface

Команды QoS

Команда	Назначение	Режим

qos fair-queue weight [W0] [W1] [W2] [W3] [W4] [W5] [W6] [W7]	Set WRR Queue Weight	Configure
qos map cos [priority:0-7] to tx-queue [0-7]	Set Cos queue mapping of priority [0-7]	Configure
qos map dscp [0-63] to tx-queue [0-7]	Set DSCP mapping queue	Configure
qos queue-schedule [strict | wrr]	Set QoS scheduling type	Configure
qos default cos [0-7]	Set Default Class of Service (COS) value	Interface
qos trust [cos | dscp]	Set trust of cos or dscp	Interface
show qos fair-queue weight	Display WRR Queue Weight	Configure
show qos map cos	Display global QoS queue mapping status	Configure
show qos map cos [0-7]	Display QoS queue mapping status of Priority [0-7]	Configure
show qos map dscp	Display global DSCP queue mapping status	Configure
show qos map dscp [0-63]	Display DSCP queue mapping status of class [0-63]	Configure
show qos queue-schedule	Display queue scheduling type	Configure
show qos default cos	Display CoS default value	Interface
show qos trust	Display QoS trust	Interface
no qos fair-queue weight	Default WRR Queue Weight	Configure
no qos map cos [0-7]	Reset Cos queue mapping of priority [0-7]	Configure
no qos map dscp [0-63]	Reset DSCP mapping queue to default	Configure
no qos queue-schedule	Default scheduling type as WRR	Configure
no qos default cos	Reset default CoS to initial value	Interface
no qos trust	Default trust as CoS	Interface

Команды настройки транков

Команда	Назначение	Режим
trunk group [1-8] [static | lacp] INTERFACES_LIST	Configure port aggregation group	Configure
show trunk group	Show all trunk groups	Configure
show trunk group [1-8]	Show trunk group [1-8]	Configure
no trunk group [1-8]	Remove trunk group [1-8]	Configure

Команды управления трафиком

Команда	Назначение	Режим
storm-control broadcast enable	Enable the broadcast storm control	Configure
storm-control broadcast level [low | mid | high]	Set the broadcast storm control level	Configure
storm-control multicast enable	Enable the multicast storm control	Configure
storm-control multicast level [low | mid | high]	Set the multicast storm control level	Configure
storm-control unknown-unicast enable	Enable the unknown-unicast storm control	Configure
storm-control unknown-unicast level [low | mid | high]	Set the unknown-unicast storm control level	Configure
show storm-control broadcast	Display the broadcast storm control status	Configure

show storm-control broadcast level	Display the broadcast storm control level	Configure
show storm-control multicast	Display the multicast storm control status	Configure
show storm-control multicast level	Display the multicast storm control level	Configure
show storm-control unknown-unicast	Display the unknown-unicast storm control status	Configure
show storm-control unknown-unicast level	Display the unknown-unicast storm control level	Configure
no storm-control broadcast	Disable the broadcast storm control	Configure
no storm-control broadcast level	Default the broadcast storm control to level high	Configure
no storm-control multicast	Disable the multicast storm control	Configure
no storm-control multicast level	Default the multicast storm control to level high	Configure
no storm-control unknown-unicast	Disable the unknown-unicast storm control	Configure
no storm-control unknown-unicast level	Default the unknown-unicast storm control to level high	Configure

Команды статической маршрутизации

Команда	Назначение	Режим
ip route [IP_ADDR] [NETMASK:0-32] [NEXT_HOP]	Add static routing entry	Configure
ipv6 route [X:X::X:X/M] [X:X::X:X]	Set IPv6 Static Route	Configure
show ip route static	Display static routing entries	Configure
show ipv6 route	Display IPv6 Routing Table	Configure
show ipv6 route static	Display IPv6 Static Routing Table	Configure
no ip route [IP_ADDR] [NETMASK:0-32]	Delete an static routing entry	Configure
no ipv6 route [X:X::X:X/M] [X:X::X:X]	Remove an IPv6 Static Route entry	Configure

Команды OSPFv2

Команда	Назначение	Режим
ip ospf authentication	Enable OSPF Authentication on this VLAN	VLAN
ip ospf authentication message-digest	Enable OSPF Authentication with MD5 on this VLAN	VLAN
ip ospf authentication-key [AUTH_KEY]	Set OSPF Authentication Password (Key)	VLAN
ip ospf dead-interval [1-65535]	Set OSPF Dead Interval; The default OSPF Dead Interval is 4 times hello interval	VLAN
ip ospf hello-interval [1-65535]	Set OSPF Hello Interval	VLAN
ip ospf message-digest-key [1-8] md5 [AUTH_KEY]	Set OSPF MD5 Authentication Password for KEY ID [1-8]	VLAN
ip ospf metric [1-65535]	Set OSPF Metric	VLAN

router ospf authentication area [AREA_ID]	Enable OSPF Authentication	Configure
router ospf authentication message-digest area [AREA_ID]	Enable MD5 Authentication on specific OSPF Area	Configure
router ospf enable	Enable Global OSPF function	Configure
router ospf network [IP_ADDR] [NETMASK:0-32] [AREA_ID]	Set OSPF Network Interface and Area	Configure
router ospf router-id [ROUTER_ID]	Set OSPF Router-ID	Configure
show ip ospf authentication	Display OSPF Authentication on this VLAN	VLAN
show ip ospf authentication-key	Display OSPF Authentication Password (Key)	VLAN
show ip ospf dead-interval	Display OSPF Dead Interval	VLAN
show ip ospf hello-interval	Display OSPF Hello Interval	VLAN
show ip ospf message-digest-key	Display OSPF MD5 Authentication Password (Key)	VLAN
show ip ospf metric	Display OSPF Metric	VLAN
show router ospf	Display OSPF Routing Status	Configure
show router ospf authentication	Display OSPF Authentication Status	Configure
show router ospf mode	Display OSPF Enable/Disable	Configure
show router ospf neighbor	Display OSPF Routing Neighbor	Configure
show router ospf network	Display OSPF Network Interface and Area	Configure
show router ospf router-id	Display OSPF Router-ID	Configure
show router ospf vlan	Display OSPF Vlan Table	Configure
no ip ospf authentication	Disable OSPF Authentication on this VLAN	VLAN
no ip ospf authentication-key	Clear OSPF Authentication Password (Key)	VLAN
no ip ospf dead-interval	Clear OSPF Dead Interval	VLAN
no ip ospf hello-interval	Clear OSPF Hello Interval	VLAN
no ip ospf message-digest-key [1-8]	Remove OSPF MD5 Authentication Password for KEY ID [1-8]	VLAN
no ip ospf metric	Clear OSPF Metric	VLAN
no router ospf	Remove OSPF Routing Protocol Configuration	Configure
no router ospf authentication area [AREA_ID]	Disable OSPF Authentication on specific Area	Configure
no router ospf network [IP_ADDR] [NETMASK:0-32]	Clear OSPF Network Interface	Configure
no router ospf router-id	Clear OSPF Router-ID	Configure

Команды OSPFv3

Команда	Назначение	Режим
ipv6 ospf6 dead-interval [1-65535]	Set OSPFv3 Dead Interval; The default OSPF Dead Interval is 4 times hello interval	VLAN
ipv6 ospf6 hello-interval [1-65535]	Set OSPFv3 Hello Interval	VLAN

ipv6 ospf6 metric [1-65535]	Set OSPFv3 Metric	VLAN
ipv6 ospf6 network [broadcast | point-to-point]	Set OSPFv3 Network-type	VLAN
ipv6 ospf6 priority [0-255]	Set OSPFv3 Priority	VLAN
router ospf6 area [AREA_ID] [X:X::X:X/M]	Set OSPFv3 Area	Configure
router ospf6 enable	Global OSPFv3 On	Configure
router ospf6 router-id [ROUTER_ID]	Set OSPFv3 Router-ID; OSPFv3 router-id is in IP address format: A.B.C.D	Configure
router ospf6 vlan [VLAN_id] [AREA_ID]	Set OSPFv3 interface/Area	Configure
show ipv6 ospf6 interface	Display OSPFv3 Information	Configure
show ipv6 ospf6 dead-interval	Display OSPFv3 Dead Interval	VLAN
show ipv6 ospf6 hello-interval	Display OSPFv3 Hello Interval	VLAN
show ipv6 ospf6 metric	Display OSPFv3 Metric	VLAN
show router ospf6	Display OSPFv3 Routing Status	Configure
show router ospf6 mode	Display OSPFv3 Enable/Disable	Configure
show router ospf6 neighbor	Display OSPFv3 neighbor	Configure
show router ospf6 router-id	Display OSPFv3 Router-ID	Configure
show router ospf6 vlan	Display OSPFv3 VLAN Table	Configure
no router ospf6	Remove OSPFv3 Routing Protocol Configuration	Configure
no router ospf6 vlan [VLAN_id] [AREA_ID]	Remove OSPFv3 interface/area	Configure

Команды RIPv1/v2

Команда	Назначение	Режим
router rip enable	Enable Global RIP function	Configure
router rip neighbor [IP_ADDR]	Set RIP Neighbors	Configure
router rip network [IP_ADDR] [NETMASK:0-32]	Set RIP Network	Configure
router rip timers [Update] [Time-out] [Garbage]	Set Routing-Table Update, Time-Out, and Garbage Collection Timers Default timer - update timer: 30s, time-out: 180s , garbage: 120s	Configure
router rip version [1|2]	Set RIP Version	Configure
show router rip mode	Display RIP Enable/Disable	Configure
show router rip network	Show RIP Network Interface and Area	Configure
show router rip state	Show RIP Routing Table	Configure
show router rip status	Show RIP Status	Configure
no router rip	Remove RIP Configurations	Configure
no router rip neighbor	Clear RIP Router-ID	Configure
no router rip network [IP_ADDR] [NETMASK:0-32]	Remove RIP Network Interface and Area	Configure
no router rip timers	Clear RIP Timers	Configure

no router rip version	Reset RIP Version	Configure

Команды RIPng

Команда	Назначение	Режим
router ripng enable	Enable Global RIP function	Configure
router ripng timers [Update] [Time-out] [Garbage]	Set Routing-Table Update, Time-Out, and Garbage Collection Timers Default timer - update timer: 30s, time-out: 180s , garbage: 120s	Configure
Router ripng vlan	Set RIPng Network	Configure
show router ripng mode	Display RIPng Enable/Disable	Configure
show router ripng state	Show RIPng Routing Table	Configure
show router ripng status	Show RIPng Status	Configure
no router ripng	Remove RIPng Routing Protocol Configurations	Configure
no router ripng vlan	Remove RIPng network-interface	Configure

Команды VRRP

Команда	Назначение	Режим
vrrp adv-timer [1-60]	Set Advertise Interval Timer of VRRP	VLAN
vrrp enable	Enable VRRP	VLAN
vrrp group-id [1-255]	Set Virtual Group ID of VRRP	VLAN
vrrp ip-address [Virtual IP address]	Set Virtual Server IP of VRRP	VLAN
vrrp preempt	Enable Preemption Mode of VRRP	VLAN
vrrp priority [1-254]	Set Priority of VRRP	VLAN
show vrrp-config		Configure
show vrrp adv-timer	Display Advertise Interval Timer of VRRP	VLAN
show vrrp all	Display All VRRP Configuration	VLAN
show vrrp group-id	Display Virtual Group ID of VRRP	VLAN
show vrrp ip-address	Display Virtual IP of VRRP	VLAN
show vrrp preempt	Display Preemption Mode of VRRP	VLAN
show vrrp priority	Display Priority of VRRP	VLAN
show vrrp state	Display State of VRRP	VLAN
no vrrp adv-timer	Disable VRRP and Remove Advertise Interval Timer of VRRP	VLAN
no vrrp all	Disable VRRP and Remove All VRRP Configuration	VLAN
no vrrp group-id	Disable VRRP and Remove Virtual Group ID of VRRP	VLAN
no vrrp ip-address	Disable VRRP and Remove Virtual IP of VRRP	VLAN
no vrrp preempt	Disable Preemption Mode of VRRP	VLAN

no vrrp priority	Disable VRRP and Remove Priority of VRRP	VLAN
no vrrp state	Disable VRRP	VLAN

Команды 802.1X

Команда	Назначение	Режим
dot1x authentication server [1|2] ip [IP]	Set 802.1X authentication server 1 or 2 address	Configure
dot1x authentication server [1|2] port [PORT]	Set 802.1X authentication server 1 or 2 port	Configure
dot1x authentication server [1|2] share-key [KEY]	Set 802.1X authentication server 1 or 2 share-key	Configure
dot1x authentication server type [local|radius]	Set 802.1X authentication server type	Configure
dot1x enable	Enable 802.1X protocol	Configure
dot1x local-db [USER] [PASSWORD]	Set 802.1X local user database	Configure
dot1x authenticator enable	Set 802.1X authenticator	Interface
dot1x mode [mac-based | port-based]	Set 802.1X mode as 1. MAC-based, 2.Port-based	Interface
dot1x reauthentication enable	Set 802.1X reauthentication	Interface
dot1x reauthentication period [60-65535]	Set 802.1X reauthentication period	Interface
show dot1x	Display 802.1X protocol state	Configure
show dot1x authentication server [1|2] ip	Display 802.1X authentication server 1 or 2 address	Configure
show dot1x authentication server [1|2] port	Display 802.1X authentication server 1 or 2 port	Configure
show dot1x authentication server [1|2] share-key	Display 802.1X authentication server 1 or 2 key	Configure
show dot1x authentication server type	Display 802.1X authentication server type	Configure
show dot1x brief	Display 802.1X information	Configure
show dot1x local-db	Display 802.1X users and password in database	Configure
show dot1x server brief	Display 802.1X RADIUS server	Configure
show dot1x authenticator	Display 802.1X authenticator state	Interface
show dot1x mode	Display 802.1X mode config	Interface
show dot1x reauthentication	Display 802.1X reauthentication state	Interface
show dot1x reauthentication period	Display 802.1X reauthentication period (in sec.)	Interface
no dot1x	Disable 802.1X protocol	Configure
no dot1x authentication server [1|2] ip	Default 802.1X authentication server 1 or 2 address	Configure
no dot1x authentication server [1|2] port	Default 802.1X authentication server 1 or 2 port	Configure

no dot1x authentication server [1|2] share-key	Default 802.1X authentication server 1 or 2 share-key	Configure
no dot1x authentication server type	Default 802.1X authentication server type	Configure
no dot1x local-db [USER]	Remove an entry in 802.1X local database	Configure
no dot1x authenticator	Disable 802.1X authenticator	Interface
no dot1x mode	Default 802.1X mode as MAC-based	Interface
no dot1x reauthentication	Disable 802.1X reauthentication	Interface
no dot1x reauthentication period	Default 802.1X reauthentication period	Interface

Команды зеркалирования

Команда	Назначение	Режим
mirror destination [DEST_PORT]	Set mirror interface of destination	Configure
mirror enable	Enable port mirror	Configure
mirror source [rx | tx | both] [PORT_LIST]	Set mirror interface of source	Configure
show mirror	Show port mirror enable/disable state	Configure
show mirror destination	Show port mirror destination configuration	Configure
show mirror source	Show port mirror source configuration	Configure
no mirror	Disable port mirror	Configure
no mirror destination	Delete port mirror Destination configuration	Configure
no mirror source	Delete port mirror Source configuration	Configure

Команды LLDP

Команда	Назначение	Режим
lldp enable	Enable LLDP protocol	Configure
lldp timer [5-32767]	Set LLDP timer	Configure
show lldp neighbor	Display LLDP neighbor	Configure
show lldp neighbor detail	Display LLDP neighbors in detail	Configure
show lldp state	Display LLDP status	Configure
show lldp timer	Display LLDP timer	Configure
no lldp	Disable LLDP protocol	Configure
no lldp timer	Default LLDP timer	Configure

Команды Syslog

Команда	Назначение	Режим
syslog local enable	Enable logging to local	Configure
syslog log clear	Clear syslog log	Configure
syslog remote enable	Enable logging to remote	Configure
syslog remote port [PORT]	Set syslog remote server port	Configure

syslog remote server [ADDRESS]	Set syslog remote server address	Configure
syslog usb enable	Enable log to USB device	Configure
show syslog local	Display local logging state	Configure
show syslog log	Display syslog messages	Configure
show syslog remote	Display remote logging state	Configure
show syslog remote port	Display remote server port	Configure
show syslog remote server	Display remote server IP	Configure
show syslog usb	Display USB logging state	Configure
no syslog local	Disable logging to local	Configure
no syslog remote	Disable logging to remote	Configure
no syslog remote port	Default syslog remote server port	Configure
no syslog remote server	Clear syslog remote server address	Configure
no syslog usb	Disable logging to USB	Configure

Команды SMTP

Команда	Назначение	Режим
smtp authentication enable	Enable SMTP authentication	Configure
smtp authentication password [PASSWORD]	Set SMTP password	Configure
smtp authentication username [USER_NAME]	Set SMTP username	Configure
smtp enable	Enable SMTP	Configure
smtp receive [1-4] [RECEIVER_ADDRESS]	Set SMTP receiver [1-4] address	Configure
smtp sender [SMTP_SENDER_ADDRESS]	Set SMTP sender	Configure
smtp server address [SMTP_SERVER_ADDRESS]	Set SMTP server address	Configure
smtp server port [SMTP_SERVER_PORT]	Set SMTP server port	Configure
smtp subject [SUBJECT]	Set SMTP subject	Configure
show smtp authentication state	Display SMTP authentication status	Configure
show smtp authentication username	Display SMTP user name	Configure
show smtp receive [1-4]	Display SMTP receiver [1-4]	Configure
show smtp sender	Display SMTP sender	Configure
show smtp server address	Display SMTP server address	Configure
show smtp server port	Display SMTP server port	Configure
show smtp state	Display SMTP service	Configure
show smtp subject	Display SMTP subject	Configure
no smtp authentication	Disable SMTP authentication	Configure
no smtp authentication password	Clear SMTP password	Configure
no smtp authentication username	Clear SMTP user name	Configure
no smtp	Disable SMTP	Configure
no smtp receive [1-4]	Clear SMTP receiver [1-4]	Configure
no smtp sender	Clear SMTP sender	Configure

no smtp server address	Clear SMTP server	Configure
no smtp server port	Clear SMTP server port	Configure
no smtp subject	Clear SMTP subject	Configure

Команды управления отчетами

Команда	Назначение	Режим
event alarm ddm [lanX-lanY] [current | rx_power | temperature | tx_power | voltage]	Register a DDM event of current, Rx power, temperature, Tx power, or voltage	Configure
event alarm digital-input [high | low]	Register an event of digital-input	Configure
event alarm interface [lan1-lanN] down	Register an event of Interface DOWN	Configure
event alarm [power1|power2]	Register an event of power 1 or 2 failure	Configure
event smtp auth-failure	Register an event of authentication failure	Configure
event smtp cold-start	Register an event of cold-start	Configure
event smtp ddm [lanX-lanY] [current | rx_power | temperature | tx_power | voltage]	Register a DDM event of current, Rx power, temperature, Tx power, or voltage	Configure
event smtp digital-input [high | low]	Register an event of digital-input	Configure
event smtp interface [lan1-lanN] down	Register an event of Interface DOWN	Configure
event smtp interface [lan1-lanN] up	Register an event of Interface UP	Configure
event smtp [power1|power2]	Register an event of power 1 or 2 failure	Configure
event smtp warm-start	Register an event of warm-start	Configure
event snmptrap auth-failure	Register an event of authentication failure	Configure
event snmptrap cold-start	Register an event of cold-start	Configure
event snmptrap ddm [lanX-lanY] [current | rx_power | temperature | tx_power | voltage]	Register a DDM event of current, Rx power, temperature, Tx power, or voltage	Configure
event snmptrap digital-input [high | low]	Register an event of digital-input	Configure
event snmptrap interface [lan1-lanN] down	Register an event of Interface DOWN	Configure
event snmptrap interface [lan1-lanN] up	Register an event of Interface UP	Configure
event snmptrap [power1|power2]	Register an event of power 1 or 2 failure	Configure
event snmptrap warm-start	Register an event of warm-start	Configure
event syslog auth-failure	Register an event of authentication failure	Configure
event syslog cold-start	Register an event of cold-start	Configure
event syslog ddm [lanX-lanY] [current | rx_power | temperature | tx_power | voltage]	Register a DDM event of current, Rx power, temperature, Tx power, or voltage	Configure
event syslog digital-input [high | low]	Register an event of digital-input	Configure
event syslog interface [lan1-lanN] down	Register an event of Interface DOWN	Configure
event syslog interface [lan1-lanN] up	Register an event of Interface UP	Configure
event syslog [power1|power2]	Register an event of power 1 or 2 failure	Configure
event syslog warm-start	Register an event of warm-start	Configure

show event alarm ddm [lanX-lanY] [current | rx_power | temperature | tx_power | voltage]	Display current, Rx power, temperature, Tx power, or voltage event registration	Configure
show event alarm digital-input	Display digital-input event registration	Configure
show event alarm interface [lan1-lanN] down	Display interface DOWN event registration	Configure
show event alarm [power1|power2]	Display power 1 or 2 event registration	Configure
show event smtp auth-failure	Display authentication failure event registration	Configure
show event smtp cold-start	Display cold-start event registration	Configure
show event smtp ddm [lanX-lanY] [current | rx_power | temperature | tx_power | voltage]	Display current, Rx power, temperature, Tx power, or voltage event registration	Configure
show event smtp digital-input	Display digital-input event registration	Configure
show event smtp interface [lan1-lanN] down	Display interface DOWN event registration	Configure
show event smtp interface [lan1-lanN] up	Display interface UP event registration	Configure
show event smtp [power1|power2]	Display power 1 or 2 event registration	Configure
show event smtp warm-start	Display warm-start event registration	Configure
show event snmptrap auth-failure	Display authentication failure event registration	Configure
show event snmptrap cold-start	Display cold-start event registration	Configure
show event snmptrap ddm [lanX-lanY] [current | rx_power | temperature | tx_power | voltage]	Display current, Rx power, temperature, Tx power, or voltage event registration	Configure
show event snmptrap digital-input	Display digital-input event registration	Configure
show event snmptrap interface [lan1-lanN] down	Display interface DOWN event registration	Configure
show event snmptrap interface [lan1-lanN] up	Display interface UP event registration	Configure
show event snmptrap [power1|power2]	Display power 1 or 2 event registration	Configure
show event snmptrap warm-start	Display warm-start event registration	Configure
show event syslog auth-failure	Display authentication failure event registration	Configure
show event syslog cold-start	Display cold-start event registration	Configure
show event syslog ddm [lanX-lanY] [current | rx_power | temperature | tx_power | voltage]	Display current, Rx power, temperature, Tx power, or voltage event registration	Configure
show event syslog digital-input	Display digital-input event registration	Configure
show event syslog interface [lan1-lanN] down	Display interface DOWN event registration	Configure
show event syslog interface [lan1-lanN] up	Display interface UP event registration	Configure
show event syslog [power1|power2]	Display power 1 or 2 event registration	Configure
show event syslog warm-start	Display warm-start event registration	Configure
no event alarm ddm [lanX-lanY] [current | rx_power | temperature | tx_power | voltage]	Unregister a DDM event of current, Rx power, temperature, Tx power, or voltage	Configure
no event alarm digital-input	Unregister an event of digital-input	Configure

no event alarm interface [lan1-lanN] down	Unregister an event of Interface DOWN	Configure
no event alarm [power1|power2]	Unregister an event of power 1 or 2 failure	Configure
no event smtp auth-failure	Unregister an event of authentication failure	Configure
no event smtp cold-start	Unregister an event of cold-start	Configure
no event smtp ddm [lanX-lanY] [current | rx_power | temperature | tx_power | voltage]	Unregister a DDM event of current, Rx power, temperature, Tx power, or voltage	Configure
no event smtp digital-input	Unregister an event of digital-input	Configure
no event smtp interface [lan1-lanN] down	Unregister an event of Interface DOWN	Configure
no event smtp interface [lan1-lanN] up	Unregister an event of Interface UP	Configure
no event smtp [power1|power2]	Unregister an event of power 1 or 2 failure	Configure
no event smtp warm-start	Unregister an event of warm-start	Configure
no event snmptrap auth-failure	Unregister an event of authentication failure	Configure
no event snmptrap cold-start	Unregister an event of cold-start	Configure
no event snmptrap ddm [lanX-lanY] [current | rx_power | temperature | tx_power | voltage]	Unregister a DDM event of current, Rx power, temperature, Tx power, or voltage	Configure
no event snmptrap digital-input	Unregister an event of digital-input	Configure
no event snmptrap interface [lan1-lanN] down	Unregister an event of Interface DOWN	Configure
no event snmptrap interface [lan1-lanN] up	Unregister an event of Interface UP	Configure
no event snmptrap [power1|power2]	Unregister an event of power 1 or 2 failure	Configure
no event snmptrap warm-start	Unregister an event of warm-start	Configure
no event syslog auth-failure	Unregister an event of authentication failure	Configure
no event syslog cold-start	Unregister an event of cold-start	Configure
no event syslog ddm [lanX-lanY] [current | rx_power | temperature | tx_power | voltage]	Unregister a DDM event of current, Rx power, temperature, Tx power, or voltage	Configure
no event syslog digital-input	Unregister an event of digital-input	Configure
no event syslog interface [lan1-lanN] down	Unregister an event of Interface DOWN	Configure
no event syslog interface [lan1-lanN] up	Unregister an event of Interface UP	Configure
no event syslog [power1|power2]	Unregister an event of power 1 or 2 failure	Configure
no event syslog warm-start	Unregister an event of warm-start	Configure

Команды таблицы MAC адресов

Команда	Назначение	Режим
clear mac address-table dynamic	Flush dynamic MAC addresses in MAC table	Configure
mac address add [VID: 1-4094] [MAC_ADDR] [PORT]	Set a MAC address to MAC table	Configure
show mac address	Display MAC table	Configure
no mac address [VID: 1-4094] [MAC_ADDR]	Remove a MAC address from FDB	Configure

Команды операций с USB

Command	Explanation	Mode

usb auto-backup	Auto save to USB if running config is changed	Configure
usb auto-load	Auto load config from USB to switch	Configure
show usb auto-backup	Display USB auto backup activated status	Configure
show usb auto-load	Display USB auto load activated status	Configure
no usb auto-backup	Disable auto save	Configure
no usb auto-load	Disable auto load	Configure

Команды управления файлами

Команда	Назначение	Режим
copy running-config startup-config	Save running-config to startup-config	Configure
copy running-config usb [file]	Save running-config to USB	Configure
copy startup-config running-config	Restore from startup-config	Configure
copy usb firmware [file]	Upgrade firmware from USB	Configure
copy startup-config usb [file]	Save startup-config to USB	Configure
copy usb startup-config [file]	Restore startup-config from USB	Configure
upload file name [FILE_NAME]	Set uploading file name	Configure
upload server ip [SERVER_IP]	Set uploading server IP	Configure
upload tftp	Upload and update firmware via TFTP (slower)	Configure
upload wget	Upload and update firmware via HTTP (faster)	Configure
show upload file name	Display uploading file name	Configure
show upload server ip	Display uploading server IP	Configure
no upload file name	Default uploading file name	Configure
no upload server ip	Clear uploading server IP	Configure