OSNOVO
cable transmission

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

Промышленные управляемые (L2+) PoE коммутаторы на 10 портов

SW-60822/ILR,
SW-80822/ILR

Прежде чем приступать к эксплуатации изделия, внимательно прочтите настоящее руководство

www.osnovo.ru

Оглавление

1. Назначение

Управляемые (L2+) PoE коммутаторы на 10 портов SW-60822/ILR и SW-80822/ILR предназначены для систем промышленного применения и для установки в уличные станции OSNOVO.

Коммутаторы оснащены 8 основными портами: Fast Ethernet (10/100Base-T) для SW-60822/ILR и Gigabit Ethernet (10/100/1000Base-T) для SW-80822/ILR. В этом заключается основное отличие моделей между собой. Каждый из 8ми портов соответствует стандартам PoE IEEE 802.3af/at и автоматически определяет подключаемые PoE-устройства. Максимальная мощность PoE на порт равна 30 Вт (общая выходная мощность до 240 Вт). Функция PoE может быть отключена или включена для каждого порта в отдельности через WEB интерфейс.

Присутствует функция PoE Alive, автоматически возобновляющая подачу PoE, если устройство зависло по каким-либо причинам, тем самым перезагружая его.

Кроме того, коммутаторы оснащены 2мя Gigabit Ethernet Combo Uplink портами: RJ45 (10/100/1000Base-T) + SFP (1000Base-X). В качестве SFP-модулей рекомендуется использовать промышленные модули с расширенным температурным диапазоном (скорость SFP-портов – 100 Мбит/с или 1 Гбит/с – можно настраивать через WEB-интерфейс коммутатора).

Коммутаторы настраиваются через WEB-интерфейс и имеет множество функций L2 и L2+ уровня, таких как:

- ✓ VLAN;
- ✓ IGMP snooping;
- ✓ STP;
- ✓ ERPS;
- ✓ QoS и др.

В моделях SW-60822/ILR и SW-80822/ILR предусмотрен порт RJ-45 (Console) для управления коммутаторами через интерфейс RS-232.

Кроме того, промышленные коммутаторы поддерживают автоматическое определение MDI/MDIX (Auto Negotiation) на всех портах. Коммутаторы распознают тип подключенного сетевого устройства и при необходимости меняют контакты передачи данных, что позволяет использовать кабели, обжатые любым способом (кроссовые и прямые).

Коммутаторы питаются от блоков питания напряжением DC 45-57V. Обладают возможностью подключения источника резервного питания и функцией оповещения при его отключении, а также при отсутствии соединения на портах (выставляется dip-переключателями).

Коммутаторы моделей SW-60822/ILR и SW-80822/ILR могут быть с успехом использованы в самых различных сферах применения и обладают температурным режимом -40…+70 ºС, что позволяет эксплуатировать их в промышленных условиях.

2. Комплектация*

SW-60822/ILR

1. Коммутатор SW-60822/ILR – 1шт.
2. Колодка 6-pin – 1шт.
3. Краткое руководство по эксплуатации –1шт.
4. Руководство по эксплуатации на CD – 1шт.
5. Упаковка – 1шт.

SW-80822/ILR

1. Коммутатор SW-80822/ILR – 1шт.
2. Колодка 6-pin – 1шт.
3. Руководство по эксплуатации –1шт.
4. CD с ПО – 1шт.
5. Упаковка – 1шт.

3. Особенности оборудования

- Диапазон рабочих температур -40…+70°С, IP30, разработаны для эксплуатации в промышленных условиях;
- Подходят для установки в уличные станции OSNOVO;
- 8 коммутируемых Fast Ethernet (10/100 Мбит/с) портов с PoE для модели SW-60822/ILR и 8 коммутируемых Gigabit Ethernet 10/100/1000 Мбит/с портов с PoE для модели SW-80822/ILR;

- 2 Gigabit Ethernet Combo Uplink порта – RJ45 (10/100/1000Base-T) + SFP (1000Base-X) – для передачи Ethernet по витой паре или оптике с помощью SFP-модулей (в комплект не входят);
- Соответствие стандартам PoE IEEE 802.3 af/at, автоматическое определение подключаемых PoE-устройств;
- Максимальная мощность PoE на порт – до 30 Вт;
- Общая выходная мощность PoE (8 портов) – до 240 Вт;
- PoE Alive – функция антизависания PoE устройств;
- Поддержка функций L2 уровня (VLAN, IGMP snooping, QoS и тд.);
- Высокая надежность сети (RSTP, MSTP, ERPS, LACP);
- Настройка и управление через WEB-интерфейс, RS-232 и Telnet/SSH;
- Автоматическое определение MDI/MDIX;
- Размер буфера пакетов: 4 МБ;
- Размер таблицы MAC-адресов: 8К;
- Поддержка Jumbo-фреймов: 9,6 КБ;
- Система тревожного оповещения типа «сухой контакт» при отключении источника резервного питания;
- Диапазон входного напряжения DC 45-57V (БП в комплект поставки не входит);
- Функция резервирования питания, защита от переполюсовки.

4. Внешний вид и описание элементов

4.1 Внешний вид

Рис.1 Коммутаторы SW-60822/ILR (SW-80822/ILR), внешний вид

4.2 Описание элементов коммутатора

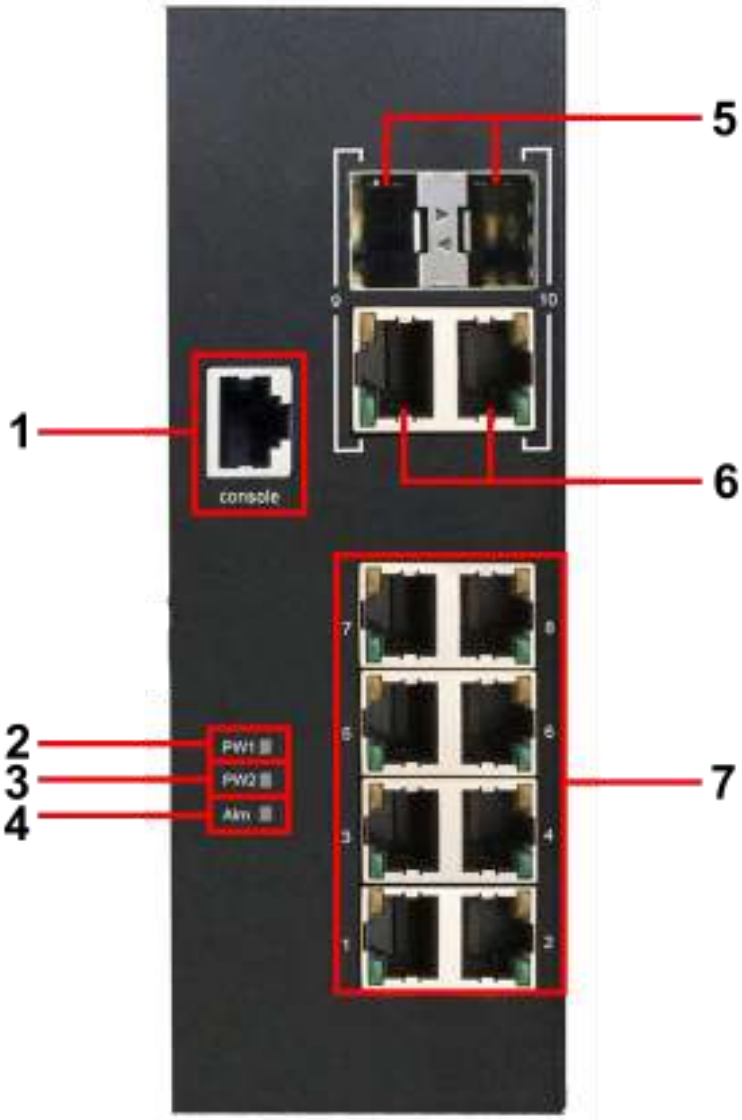


Рис. 2 Коммутаторы SW-60822/ILR (SW-80822/ILR), разъемы, кнопки и индикаторы передней панели

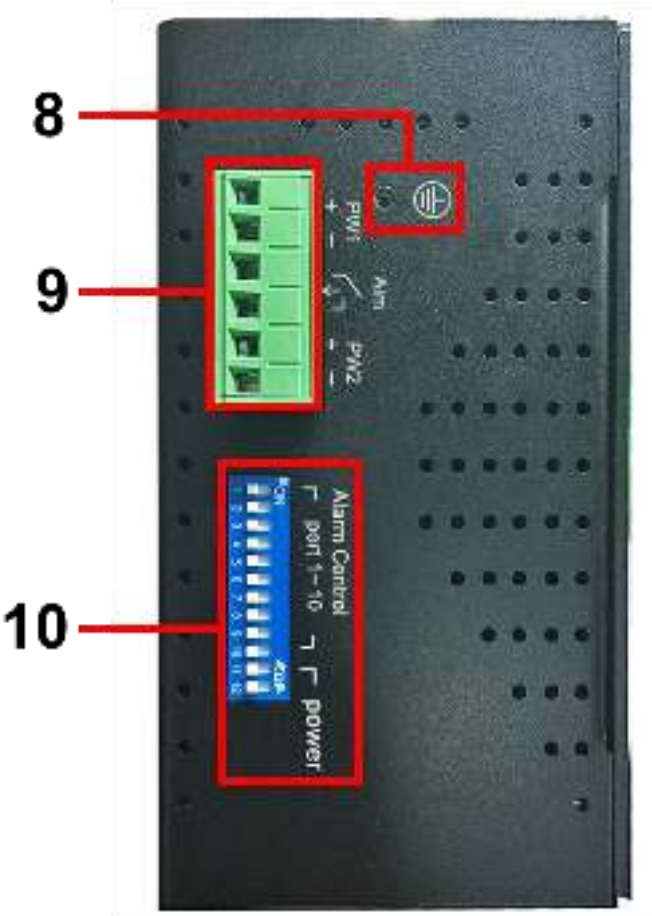


Рис. 3 Коммутаторы SW-60822/ILR (SW-80822/ILR), разъемы, кнопки и индикаторы вид сбоку

Таб.1 Назначение разъемов, кнопок и индикаторов коммутаторов SW-60822/ILR, SW-80822/ILR

№ п/п	Обозначение	Назначение	
		SW-60822/ILR	**SW-80822/ILR**
1	Console	Разъем RJ-45 для подключения коммутатора к COM порту ПК для управления им через интерфейс RS-232	

2	PW1	LED-индикатор подключения 1го блока питания DC 45-57V. Горит зеленым, если питание присутствует.	
3	PW2	LED-индикатор подключения 2го, резервного блока питания DC 45-57V. Горит зеленым, если питание присутствует.	
4	Alm	LED-индикатор неисправности. Горит красным, если не подключен один из блоков питания или произошел обрыв Ethernet - соединения	
5	9, 10	SFP-слоты в 9 и 10м Combo-портах. Используются для подключения коммутатора к оптическим линиям связи. SFP-модули в комплект поставки не входят.	
6	9, 10	Медные RJ-45 разъемы для подключения коммутатора к медным (витая пара) линиям связи.	
7	1 2 3 4 5 6 7 8	Разъемы RJ-45 для подключения сетевых устройств на скорости 10/100 Мбит/с с PoE. LED-индикаторы Ethernet.	Разъемы RJ-45 для подключения сетевых устройств на скорости 10/100/1000 Мбит/с с PoE. LED-индикаторы Ethernet.
8		Винтовая клемма для подключения коммутатора к контуру заземления.	
9	PW1 Alm PW2 + - + - 	Клеммная колодка для подключения основного и резервного БП DC 45-57V (PW1 PW2), а также выход реле типа «сухой контакт» (Alm).	

10	Alarm Control 	DIP-переключатель на 12 положений, используется для настройки тревожной сигнализации для разных портов. Используются 1 - 11. 12 DIP не используется.

5. Подключение

5.1 Схема подключения

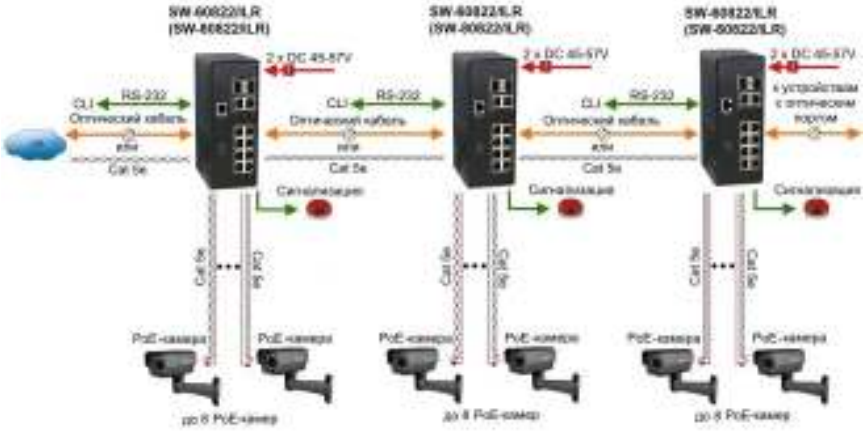
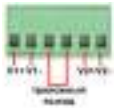


Рис.4 Типовая схема подключения коммутаторов SW-60822/ILR, SW-80822/ILR

5.2 Подключение блока питания

1. Подключается кабель от блока питания с учётом полярности.



2. Закручиваются винты с другой стороны клеммной колодки.

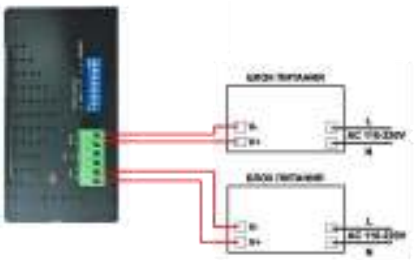


Рис.5 Схема подключения блоков питания к клеммной колодке коммутаторов SW-60822/ILR, SW-80822/ILR

5.3 Подключение системы оповещения

Коммутаторы SW-60822/ILR, SW-80822/ILR имеют релейный выход типа сухой контакт (NO) для включения системы оповещения при отключении одного из источников питания. Релейный выход поддерживает управление исполнительными устройствами (сирена, светодиодное табло и т.д.) с потребляемой мощностью не более 24 Вт.

Примечание:
Напряжение источника питания, подключенного к релейному выходу, должно быть не более DC 24 V, а ток, проходящий через реле, - не более 1 А (Рис.6).

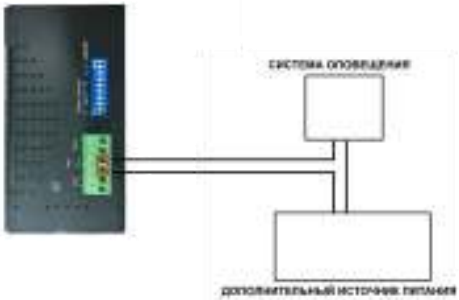


Рис.6 Схема подключения системы оповещения к коммутаторам SW-60822/ILR, SW-80822/ILR

5.4 Подключение цепи заземления

Рис.7 Заземление коммутаторов SW-60822/ILR, SW-80822/ILR

Во избежание электромагнитных наводок и помех коммутаторы SW-60822/ILR, SW-80822/ILR нужно заземлять (Рис.7).

6. Проверка работоспособности системы

После подключения кабелей к разъёмам и подачи питания на коммутатор SW-60822/ILR (или SW-80822/ILR) можно убедиться в его работоспособности.

Подключите коммутатор между двумя ПК с известными IP-адресами, располагающимися в одной подсети, например, 192.168.1.1 и 192.168.1.2.

На первом компьютере (192.168.1.2) запустите командную строку (выполните команду cmd) и в появившемся окне введите команду:

ping 192.168.1.1

Если все подключено правильно, на экране монитора отобразится ответ от второго компьютера (Рис.8). Это свидетельствует об исправности коммутатора.

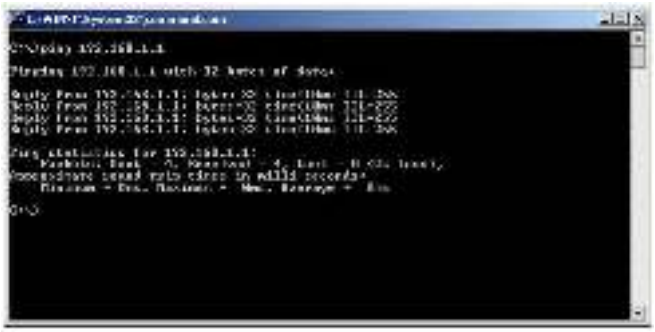


Рис.8 Данные, отображающиеся на экране монитора, после использования команды Ping.

Если ответ ping не получен («Время запроса истекло»), то следует проверить соединительный кабель и IP-адреса компьютеров.

Если не все пакеты были приняты, это может свидетельствовать:

- о низком качестве кабеля;
- о неисправности коммутатора;
- о помехах в линии.

Примечание:

Причины потери в оптической линии могут быть вызваны:

- неисправностью SFP-модулей
- изгибами кабеля
- большим количеством узлов сварки
- неисправностью или неоднородностью оптоволокна.

7. Подготовка перед управлением коммутатором через WEB-интерфейс**

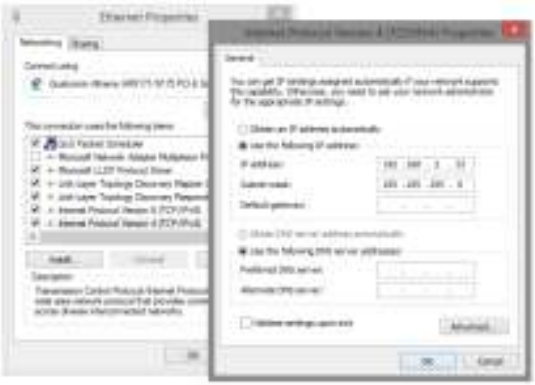
Web-интерфейс позволяет гибко настраивать и отслеживать состояние коммутатора, используя браузер (Google Chrome, Opera, IE и тд) из любой точки в сети.

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

1. Убедитесь, что сетевая карта в вашем ПК установлена, работает и поддерживает TCP/IP протокол.

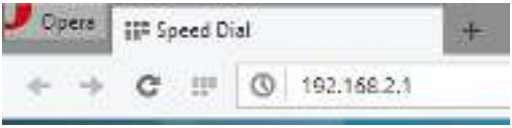
2. Подключите между собой коммутатор и ваш ПК, используя патч-корд RJ-45

3. По умолчанию IP-адрес коммутатора: **192.168.2.1.** Коммутатор и ваш ПК должны находиться в одной подсети. Измените IP адрес вашего ПК на 192.168.2.X, где X-число от 2 до 254. Пожалуйста, убедитесь, что IP-адрес, который вы назначаете вашему ПК, не совпадал с IP-адресом коммутатора.



4. Запустите Web-браузер (IE, Firefox, Chrome) на вашем ПК

5. Введите в адресную строку **192.168.2.1** (IP-адрес коммутатора) и нажмите Enter на клавиатуре.



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

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

8. Подготовка перед управлением коммутатором через порт CONSOLE

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

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

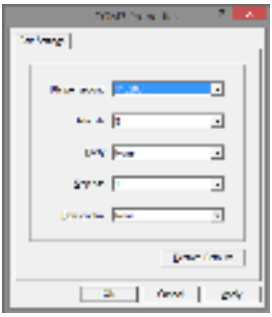
1. Соедините порт Console коммутатора с COM-портом компьютера с помощью кабеля.
2. Запустите HyperTerminal на ПК.
3. Задайте имя для нового консольного подключения.

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

5. Настройте COM-порт следующим образом:

- Скорость передачи данных (Baud Rate) – 115200;
- Биты данных (Data bits) – 8;

- Четность (Parity) – нет;
- Стоп биты (Stop bits) – 1;
- Управление потоком (flow control) – нет.



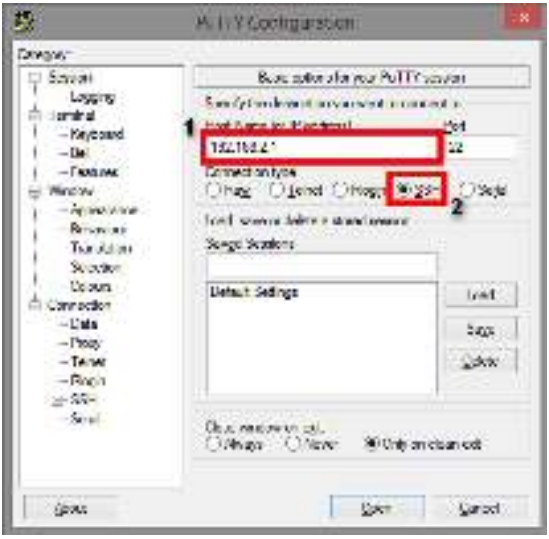
6. Система предложит войти Вам в интерфейс CLI (управление через командную строку). По умолчанию имя пользователя/пароль – admin/admin.

9. Подготовка перед управлением коммутатором через Telnet/SSH

Протоколы Telnet и SSH предоставляют пользователю текстовый интерфейс командной строки для управления коммутатором (CLI). Но только SSH обеспечивает создание безопасного канала с полным шифрованием передаваемых данных. Чтобы получить доступ к CLI коммутатора через Telnet/SSH, ваш ПК и коммутатор должны находиться в одной сети. Подробнее, как это сделать рассматривалось в разделе инструкции «Подготовка перед управлением коммутатором через WEB-интерфейс».

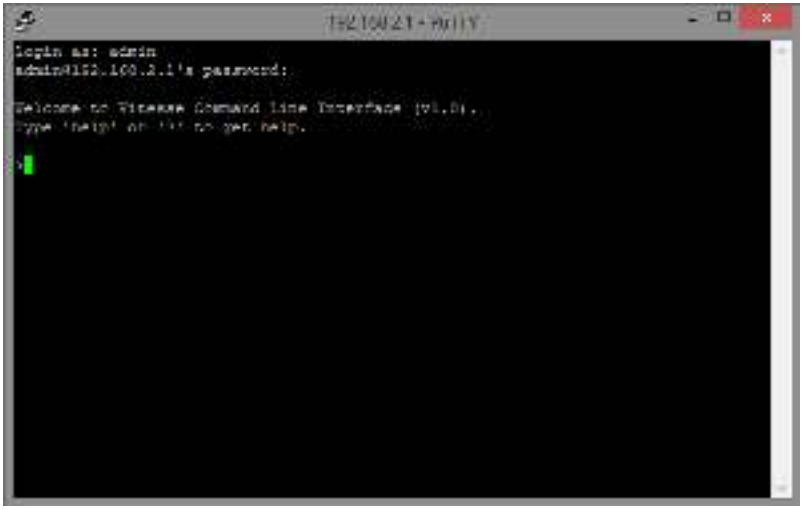
Telnet интерфейс встроен в командную строку CMD семейства операционных систем Microsoft Windows. SSH интерфейс доступен только с помощью программы эмулятора SSH терминала. Ниже показано, как получить доступ к CLI коммутатора через SSH с помощью программы PuTTY.

1. Зайдите в меню PuTTY Configuration. Введите IP адрес коммутатора в поле Имя хоста (Host Name) (или IP адрес). По умолчанию IP адрес коммутатора **192.168.2.1**
2. Выберите тип подключения (Connection type) – SSH.



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

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



10. Управление через WEB. Общая информация.

- ✓ System (Системная информация). В этом разделе представлены возможности конфигурирования основных системных настроек таких как: информация о системе, IP коммутатора, системное время и тд.
- ✓ Green Ethernet. В этом разделе представлены возможности включения/выключения функции EEE (Energy Efficient Ethernet) для каждого порта. EEE позволяет снизить мощность потребляемую коммутатором.
- ✓ Ports (Настройка портов). В этом разделе представлены возможности по просмотру статуса всех портов коммутатора. Например, скорости соединения, максимальную длину фрейма и тд.
- ✓ DHCP. В этом разделе представлены возможности по настройке DHCP сервера, который позволит коммутатору присваивать IP адреса подключенным устройствам.
- ✓ Security (Безопасность). В этом разделе представлены возможности по настройке опций безопасности, которые помогут защитить как сам коммутатор так и сеть, где он используется.
- ✓ Aggregation (Объединение портов). В этом разделе представлены возможности по объединению (агрегации) нескольких физических портов в один логический, пропускная способность которого будет больше чем у одного физического порта.
- ✓ Loop Protection (Защита от сетевых петель). В этом разделе представлены возможности по борьбе с «сетевыми петлями» (могут вызвать шторм (broadcast storm) и парализовать работу сети).
- ✓ Spanning Tree. В этом разделе представлены возможности по настройке протоколов связующего дерева STP, RSTP, MSTP. Использование данных протоколов при построении сети поможет избежать образование сетевых петель и повысит надежность сети.
- ✓ MVR (Multiple VLAN Registration). В этом разделе представлены возможности по настройке протокола MVR, который позволяет создать multicast VLAN и настраивать ее динамически при необходимости.

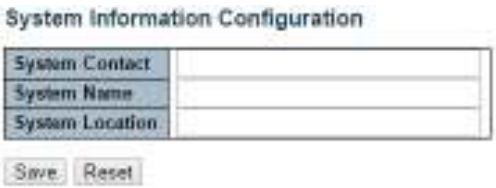
- ✓ IPMC. В этом разделе представлены возможности по настройке протоколов IGMP Snooping (для IPv4) или MLD (для IPv6). Эти протоколы позволяют снизить загрузку сети при передаче мультимедийного трафика.
- ✓ LLDP. В этом разделе представлены возможности по настройке протокола LLDP – протокола оповещения «соседей». Данный протокол позволяет узнать устройства по близости в сети и оценить их возможности.
- ✓ PoE (Передача питания по сетевому кабелю). В этом разделе представлены возможности по управлению PoE для каждого порта в отдельности (вкл/выкл, ограничение мощности и тд.)
- ✓ SyncE. SyncE это аббревиатура от Synchronous Ethernet. В этом разделе представлены возможности по модификации изначально асинхронной сети Ethernet в синхронную.
- ✓ MEP. В этом разделе представлены возможности по настройке MEP
- ✓ ERPS. В этом разделе представлены возможности по настройке ERPS – протокола, который обеспечивает повышенную надежность сети при использовании кольцевой топологии.
- ✓ MAC Table (Таблица MAC адресов). В этом разделе представлены возможности по просмотру и настройке таблицы MAC адресов коммутатора.
- ✓ VLAN (Логические «виртуальные» локальные сети). В этом разделе представлены возможности по созданию VLAN сетей. В таких сетях порты коммутатора можно назначать в различные VLAN группы, которые будут работать как отдельные сети.
- ✓ Private VLAN (Частные VLAN). Функция VLAN также известная как изоляция портов (port isolation).
- ✓ VCL. В этом разделе представлены возможности по настройке VLAN на основе MAC адресов, VLAN на основе протоколов, VLAN на основе IP адреса подсети.
- ✓ Voice VLAN (Голосовые VLAN). В этом разделе представлены возможности по настройке особых VLAN, предназначенных для голосовой коммуникации (например, VoIP телефония). Голосовой трафик в такой сети имеет повышенный приоритет.
- ✓ Mirroring (Зеркалирование портов). В этом разделе представлены возможности по настройке зеркалирования

входящего исходящего трафика с выбранного порта на отдельный порт. Это может помочь диагностировать неисправности в сети.

- ✓ UPnP. В этом разделе представлены возможности по настройке протокола UPnP, который позволяет всем устройствам в сети обнаруживать друг друга и устанавливать соединение.
- ✓ PTP. В этом разделе представлены возможности по настройке протокола PTP, который используется для синхронизации времени в локальных сетях.
- ✓ GVRP. В этом разделе представлены возможности по настройке протокола GARP VLAN Registration Protocol.
- ✓ sFlow. sFlow – это стандартная отраслевая технология для мониторинга коммутируемых сетей посредством случайной выборки пакетов на портах коммутатора и выборки счетчиков портов на основе времени. Отобранные пакеты будут отправлены назначенному приемнику (хосту) sFlow системного администратора для анализа.
- ✓ UDLD. В этом разделе представлены возможности по настройке UDLD – протокола, позволяющего на канальном уровне сети обнаруживать однонаправленные линии связи, которые могут в дальнейшем приводить к образованию сетевых петель.

10.1 Configuration – System (Системные настройки)

10.1.1 System (Системная информация)



System Contact (Контактная информация). Содержит информацию о лице, ответственном за это устройство, а также его контактные данные. Допустимая длина строки - от 0 до 255, а допустимое содержимое - символы ASCII от 32 до 126.

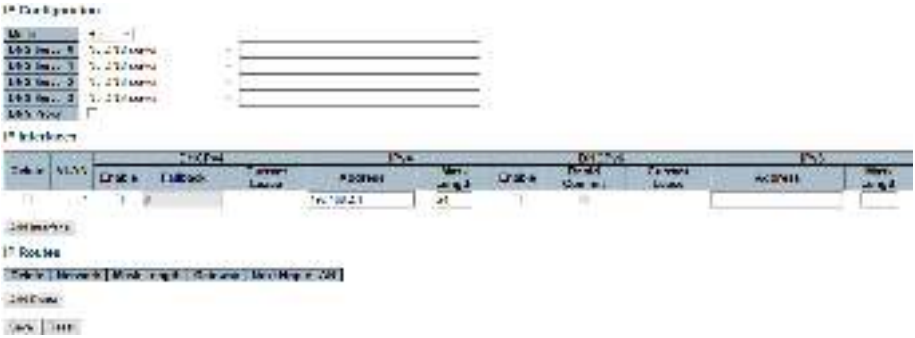
System Name (Идентификационное имя коммутатора). Здесь можно задать имя для коммутатора. По умолчанию – это полное доменное имя коммутатора. Доменное имя - это текстовая строка, составленная из алфавита (A-Z и a-z), цифр (0-9), знака минус (-). Запрещается использование пробелов в качестве части имени. Первый символ должен быть заглавным. Первый или последний символ не должен быть знаком –(). Допустимая длина строки - от 0 до 255.

System Location (Местоположение коммутатора). Физическое месторасположение коммутатора. Например, «3 этаж. Телекоммуникационный шкаф». Допустимая длина строки - от 0 до 255, а допустимое содержимое - символы ASCII от 32 до 126.

Кнопки

Save (Сохранить). Нажмите, чтобы сохранить изменения.
Reset (Сбросить). Нажмите, чтобы отменить изменения и вернуть их к предыдущим сохраненным значениям.

10.1.2 System – IP (Конфигурация IP интерфейсов)



Настройка IP адресов, мониторинг IP маршрутов и интерфейсов. Максимальное поддерживаемое количество интерфейсов – 8, максимальное количество маршрутов – 32.

Базовые настройки.

Mode (Режим работы). Выберите режима работы для устройства host или router (хост или маршрутизатор). В режиме хоста IP трафик между интерфейсами не будет маршрутизироваться. В режиме маршрутизатора трафик будет перенаправляться между всеми интерфейсами.

DNS Server (Сервер DNS имен). Настройки позволяют контролировать расшифровку DNS имен, выполняемую коммутатором. Для конфигурации доступно 4 сервера. Индекс сервера связан с приоритетом. Чем меньше индекс, тем выше приоритет при выполнении расшифровки DNS имен. Система поочередно выбирает активный DNS-сервер из конфигурации, если предпочтительный сервер не отвечает в течение пяти попыток.

Поддерживаются следующие режимы:

- ✓ Из любых DHCPv4 интерфейсов: будет использоваться первый DNS-сервер, предлагаемый от аренды DHCPv4 до интерфейса с поддержкой DHCPv4.
- ✓ Без DNS сервера: DNS сервер не используется.
- ✓ Настроенный IPv4: укажите вручную действительный IPv4 адрес DNS сервера в десятичном виде, разделенный точками. Убедитесь, что настроенный DNS сервер доступен (например, с помощью команды PING).
- ✓ Из этого DHCPv4 интерфейса: укажите, из какого интерфейса с поддержкой DHCPv4 предпочтительный DNS-сервер должен быть выбран.
- ✓ Настроенный IPv6: укажите вручную действительный IPv6 адрес DNS сервера. (кроме linklocal). Убедитесь, что настроенный DNS сервер доступен (например, с помощью команды PING).
- ✓ Из этого DHCPv6 интерфейса: укажите, из какого интерфейса с поддержкой DHCPv6 предпочтительный DNS-сервер должен быть выбран.
- ✓ Из любых DHCPv6 интерфейсов: будет использоваться первый DNS-сервер, предлагаемый от аренды DHCPv6 до интерфейса с поддержкой DHCPv6.

DNS Proxy (DNS прокси-сервер). Когда DNS сервер активен, система будет передавать DNS запросы на текущий настроенный DNS-сервер и отвечать в качестве расшифровщика DNS на клиентские устройства в сети.

IP интерфейсы

Delete (Удалить). Выбор этой опции отвечает за удаление существующего IP интерфейса.

VLAN (Виртуальные локальные сети). Сеть VLAN связанная с IP интерфейсом. Только порты из этой VLAN будут иметь доступ к IP интерфейсу. Это поле доступно только для ввода при создании нового интерфейса.

IPv4 DHCP Enabled (DHCP сервер). Если эта опция включена, система настроит IPv4-адрес и маску интерфейса, используя протокол DHCP. Клиент DHCP объявит отобразит имя системы как имя хоста, чтобы обеспечить возможность поиска через DNS.

IPv4 DHCP Fallback Timeout (Таймаут отката DHCP). Количество секунд для получения аренды DHCP. По истечении этого периода настроенный адрес IPv4 будет использоваться в качестве адреса интерфейса IPv4. Нулевое значение отключает резервный механизм, так что DHCP будет повторять попытки до получения действительной аренды. Допустимые значения: от 0 до 4294967295 секунд.

IPv4 DHCP Current Lease (текущий адрес интерфейса от DHCP). Для интерфейсов DHCP с активной арендой этот столбец показывает текущий адрес интерфейса, предоставленный сервером DHCP.

IPv4 Address (IPv4 Адрес). IPv4-адрес интерфейса в десятичном виде с разделительными точками. Если DHCP включен, в этом поле задается резервный адрес. Поле может быть оставлено пустым, если операции с IPv4 на интерфейсе нежелательны или не требуется резервный адрес DHCP.

IPv4 Mask (Маска для IPv4). Маска сети IPv4, в количестве бит (длина префикса). Допустимые значения находятся в диапазоне от 0 до 30 бит для адреса IPv4. Если DHCP включен, это поле настраивает маску сети с резервным адресом. Поле может быть оставлено пустым, если операции с IPv4 на интерфейсе нежелательны или не требуется резервный адрес DHCP.

IPv6 Address (IPv6 Адрес). IPv6-адрес интерфейса. Адрес IPv6 задается в 128-битными значениями, представленными в виде восьми полей длиной до четырех шестнадцатеричных цифр с двоеточием, разделяющим каждое поле (:). Например, fe80 :: 215: c5ff: fe03: 4dc7. Символ :: - это специальный синтаксис, который можно использовать как краткий способ представления нескольких 16-битных групп непрерывных нулей; но он может быть использован только один раз.
Система принимает только действительный IPv6-адрес, за исключением IPv4-совместимого адреса и IPv4-сопоставленного адреса. Поле можно оставить пустым, если операции с IPv6 на интерфейсе нежелательны.

IPv6 Mask (Маска для IPv6). Маска сети IPv6 в количестве бит (длина префикса). Допустимые значения составляют от 1 до 128 бит для адреса IPv6. Поле можно оставить пустым, если операции с IPv6 на интерфейсе нежелательны.

IP маршруты

Delete (Удалить). Выбор этой опции отвечает за удаление существующего IP маршрута.

Network. IP-сеть назначения или адрес хоста этого маршрута. Допустимый формат - десятичная запись с точками или действительная запись IPv6. Маршрут по умолчанию может использовать значение 0.0.0.0 или :: для IPv6.

Mask Length. Маска сети назначения или хотста в количестве бит (длина префикса). Он определяет, какой сетевой адрес должен совпадать, чтобы претендовать на этот маршрут. Допустимые значения от 0 до 32 битов соответственно 128 для маршрутов IPv6. Только

маршрут по умолчанию будет иметь длину маски 0 (так как он будет соответствовать чему угодно).

Gateway (Шлюз). IP адрес шлюза. Допустимый формат - десятичная запись с точками или действительный IPv6. Шлюз и Сеть должны быть одного типа.

Next Hop VLAN. Идентификатор VLAN (VID) конкретного интерфейса IPv6, связанного со шлюзом. Заданный VID находится в диапазоне от 1 до 4094 и будет действовать только в том случае, если действителен соответствующий интерфейс IPv6. Если адрес шлюза IPv6 является linklocal, он должен указать VLAN следующего перехода (hop'a) для шлюза.
Если адрес шлюза IPv6 не является linklocal, система игнорирует VLAN следующего перехода (hop'a) для шлюза.

Кнопки

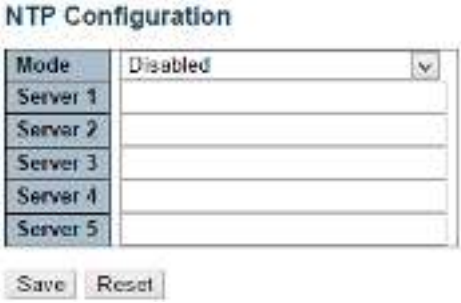
Add Interface (Добавить интерфейс). Нажмите, чтобы добавить новый IP интерфейс. Поддерживается максимум 128 интерфейсов.

Add Route (Добавить маршрут). Нажмите, чтобы добавить новый IP маршрут. Поддерживается максимум 32 маршрута.

Save (Сохранить). Нажмите для сохранения изменений

Reset (Сбросить). Нажмите, чтобы отменить изменения и вернуть их к предыдущим сохраненным значениям.

10.1.3 System – NTP (Настройка протокола NTP)



NTP (или сетевой протокол времени) обеспечивает подстройку текущего времени с помощью синхронизации с NTP сервером.

Mode (Режимы).

- ✓ Enabled (включено) – включен режим NTP клиента;
- ✓ Disabled (выключено) – выключен режим NTP клиента.

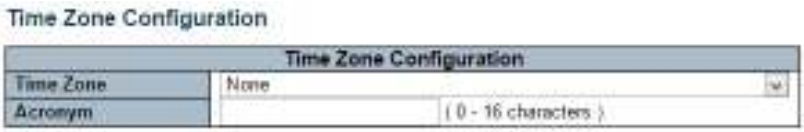
Server 1~5 (Выбор NTP сервера). Укажите IPv4 или IPv6 адрес NTP сервера. Адрес IPv6 должен быть в виде 8 полей. Также можно указать URL адрес NTP сервера.

Кнопки

Save (Сохранить). Нажмите для сохранения изменений

Reset (Сбросить). Нажмите, чтобы отменить изменения и вернуть их к предыдущим сохраненным значениям.

10.1.4 System – Time (Настройка системного времени)



На данной странице WEB интерфейса можно задать часовой пояс и сконфигурировать летнее время.

Time Zone Configuration (Настройка часового пояса)

- ✓ Time Zone (Часовой пояс). Выпадающий список часовых поясов по всему миру. Выберите подходящий и нажмите сохранить (Save).
- ✓ Acronym (Акроним). Пользователь может самостоятельно установить сокращение-аббревиатуру для обозначения выбранного часового пояса. Можно использовать до 16 буквенно-числовых символов и знаков препинания.

Daylight Saving Time Configuration (Настройка летнего времени). При активации данной функции коммутатор будет переводить часы вперед или назад в соответствии с настройками, указанными ниже, для определенной продолжительности перехода на летнее время.

Disable (Отключить). Отключить настройку перехода на летнее время. По умолчанию.

Reccuring (Повторять). Настройки перехода на летнее время будут применяться каждый год.

Non-Reccuring (Не повторять). Настройки перехода на летнее время будут применены единожды.

10.1.5 System-Log (Журнал системных событий)

На этой странице WEB интерфейса представлены настройки журнала системных событий.

Server Mode (Режим сервера). Когда режим включен (enabled) сообщение журнала системных событий будет отправлено на сервер, который задается в поле ниже (Server Address). Протокол журнала основан на UDP и использует порт 514.

Server Address (IPv4 адрес сервера журнала системных событий). Если активна функция DNS, здесь можно указать имя хоста.

System log Level (Тип событий отправляемых на сервер). Предусмотрено 3 типа событий:

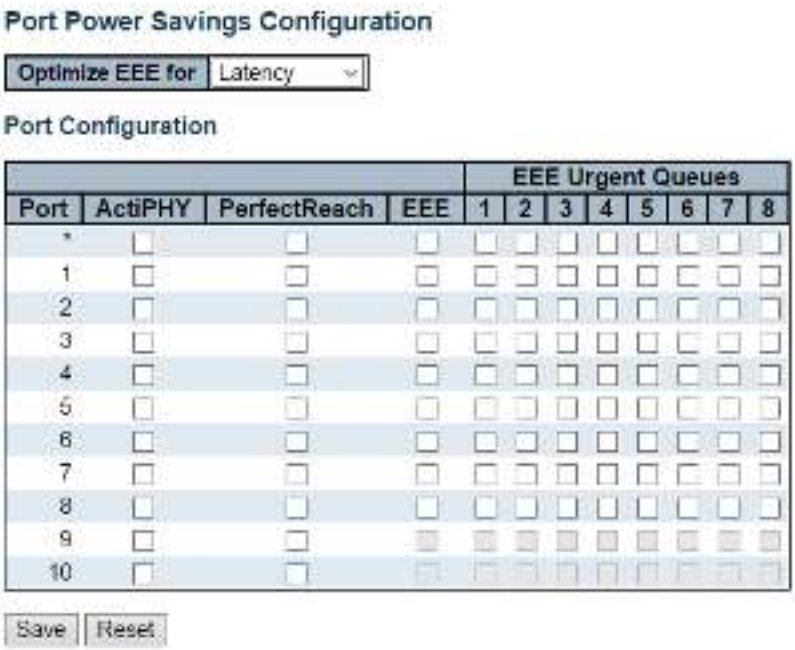
- ✓ Info – информация, предупреждения и ошибки;
- ✓ Warning – предупреждения и ошибки;
- ✓ Error – только ошибки.

Кнопки

Save (Сохранить). Нажмите для сохранения изменений

Reset (Сбросить). Нажмите, чтобы отменить изменения и вернуть их к предыдущим сохраненным значениям.

10.2 Configuration - Green Ethernet (Настройки - Green Ethernet)



Технология EEE (или Green Ethernet) используется для снижения потребляемой мощности коммутатором в момент, когда обрабатывается незначительное количество сетевого трафика.

Optimize EEE for (Оптимизировать EEE для)
На выбор предоставляется 2 варианта:

- ✓ Latency (Задержки) – при выборе этого режима коммутатор старается снижать задержки и отклик в сети;
- ✓ Power (Мощность) – при выборе этого режима коммутатор в первую очередь снижает потребляемую мощность при работе в моменты простоя или при низкой загрузке сети.

Port Configuration (Настройка для портов)

Port (Выбор порта)
Номер порта.

ActiPHY При выборе этой функции коммутатор снижает потребление энергии, если к этому порту ничего не подключено.

Perfect Reach (Идеальная длина) При выборе этой функции коммутатор автоматически определяет длину кабеля и снижает потребление энергии на портах подключенных короткими кабелями.

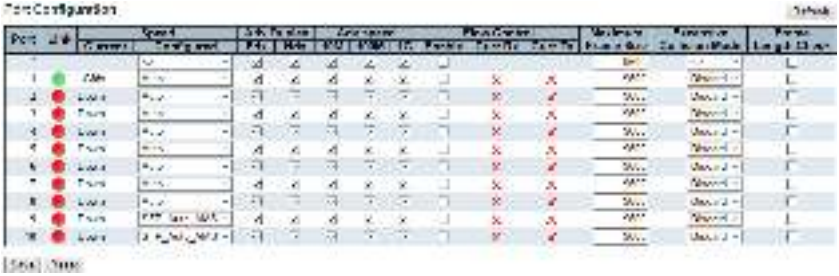
EEE Включает/отключает EEE функцию на порте при выставлении/снятии галки.

Кнопки

Save (Сохранить). Нажмите для сохранения изменений

Reset (Сбросить). Нажмите, чтобы отменить изменения и вернуть их к предыдущим сохраненным значениям.

10.3 Configuration-Ports (Конфигурирование портов коммутатора)



На этой странице WEB интерфейса отображается информация о текущей конфигурации портов коммутатора. Порты также могут быть настроены отсюда.

Port
Номер порта

Link
Текущее состояние порта. Зеленый – порт задействован. Красный – к порт не активен.

Current Link Speed

Текущая скорость на которой выполняется обмен данными на выбранном порте.

Configured Link Speed

Настройка скорости для выбранного порта. Предусмотрены следующие режимы:

- ✓ Disabled – порт отключен;
- ✓ Auto – автосогласование скорости;
- ✓ 10Mbps HDX – скорость 10 Мбит/с полудуплекс;
- ✓ 10Mbps FDX – скорость 10 Мбит/с полный дуплекс;
- ✓ 100Mbps HDX – скорость 100 Мбит/с полудуплекс;
- ✓ 100Mbps FDX – скорость 100 Мбит/с полный дуплекс;
- ✓ 1Gbps FDX – скорость 1 Гбит/с полный дуплекс;
- ✓ SFP Auto AMS – автоматическое определение скорости используемых SFP модулей. Это нестандартизированный способ определения скорости, поэтому некоторые модули могут быть не определены SFP Auto AMS. Медный порт в комбопорте автоматически определяет скорость;
- ✓ 100-FX – скорость SFP порта соответствует 100FX (модули 155 Мбит/с). Медный порт в комбопорте не активен;
- ✓ 1000-FX – скорость SFP порта соответствует 1000FX (модули 1,25 Гбит/с). Медный порт в комбопорте не активен;

Advertise Duplex

Когда режим дуплекс/полудплекс выставлен на Авто, порт будет использовать режим передачи данных на основании возможностей подключенного устройства.

Advertise Speed

Когда скорость определяется автоматически (выбран режим Авто), порт работает на скорости, основанной на возможностях подключенного сетевого устройства.

Flow Control

Когда включено автосогласование скорости на выбранном порте, порт обьявляет подключенному устройству о возможности управления потоком (flow control). Столбец Current Rx указывает, выполняются ли

фреймы паузы на порту, а столбец Current Tx указывает, переданы ли фреймы паузы на порт. Настройки Rx и Tx определяются результатом последнего автосогласования.

PFC

PFC (802.1Qbb Приоритезация управление потоком)
Включение/выключение для выбранного порта. PFC и Flow Control не могут быть одновременно выбраны для порта.

Maximum Frame Size

Максимальный размер фрейма, который сможет обработать порт.

Excessive Collision Mode

Поведение порта при образовании коллизии

- ✓ Discard – Отбрасывание пакетов после 16 коллизий;
- ✓ Restart – Перезапуск алгоритма после 16 коллизий;

Frame Length Check

Конфигурация проверки длины кадра.

Кнопки

Save (Сохранить). Нажмите для сохранения изменений

Reset (Сбросить). Нажмите, чтобы отменить изменения и вернуть их к предыдущим сохраненным значениям.

Refresh (Обновить)

10.4 Configuration – DHCP (Настройка DHCP)

10.4.1 DHCP – Server – Mode (Сервер DHCP – режимы)

На этой странице WEB интерфейса представлены глобальные настройки DHCP сервера для системы и для VLAN.

Mode (Режимы)

- ✓ Enabled – Включить DHCP сервер для системы;
- ✓ Disabled – Выключить DHCP сервер для системы.

VLAN Range

Укажите диапазон VLAN'ов в котором DHCP будет включен или отключен. Первый VLAN ID должен быть меньше или равен второму VLAN ID. Но, если диапазон VLAN содержит только 1 VLAN ID, вы можете просто объединить его в один из первого и второго VLAN ID или в оба. С другой стороны, если вы хотите отключить существующий диапазон VLAN, вы можете выполнить следующие действия:

1. Нажмите «Добавить диапазон VLAN», чтобы добавить новый диапазон VLAN.
2. Введите диапазон VLAN, который вы хотите отключить.
3. Выберите Mode для отключения.
4. Нажмите «Сохранить», чтобы применить изменения.

Затем вы увидите, что отключенный диапазон VLAN удаляется со страницы конфигурации режима DHCP-сервера.

Mode (Режимы)

- ✓ Enabled – Включить DHCP сервер для VLAN;
- ✓ Disabled – Выключить DHCP сервер для VLAN.

Кнопки

Save (Сохранить). Нажмите для сохранения изменений

Reset (Сбросить). Нажмите, чтобы отменить изменения и вернуть их к предыдущим сохраненным значениям.

10.4.2 DHCP - Server - Excluded IP (Сервер DHCP – исключенные IP)

На этой странице WEB интерфейса настраиваются исключенные IP-адреса. DHCP-сервер не будет назначать эти исключенные IP-адреса DHCP-клиенту.

IP Range (диапазон IP адресов)

Определите диапазон IP-адресов для исключения. Первый исключенный IP-адрес должен быть меньше или равен второму исключенному IP-адресу.

Кнопки

Save (Сохранить). Нажмите для сохранения изменений

Reset (Сбросить). Нажмите, чтобы отменить изменения и вернуть их к предыдущим сохраненным значениям.

10.4.3 DHCP-Server-Pool (Пул адресов для DHCP сервера)

Эта страница управляет пулами адресов DHCP. В соответствии с пулом DHCP, сервер DHCP будет выделять IP-адрес и передавать параметры конфигурации клиенту DHCP.

Pool Setting (Настройка пула адресов)
Добавить или удалить пулы адресов.
Добавление пула и присвоение имени - это создание нового пула адресов с конфигурацией «по умолчанию». Если вы хотите настроить все параметры, включая тип, маску IP-подсети и время аренды, вы можете щелкнуть имя пула адресов, чтобы перейти на страницу конфигурации.

Name (Имя)
Задайте имя пула адресов (исключая пробелы).

Type (Тип)
Поле отображает тип пула адресов:

- ✓ Network – пул определяет пул IP адресов для обслуживания более чем 1 DHCP клиента;
- ✓ Host – пул обслуживает особого DHCP клиента, определяемого по аппаратному адресу или идентификатору клиента;

IP
Поле отображает количество пулов адресов для DHCP

Subnet Mask (Маска подсети)
Поле отображает маску подсети для пула адресов DHCP

Lease Time (Время аренды)
Поле отображает время аренды для выбранного пула адресов.

Кнопки

Save (Сохранить). Нажмите для сохранения изменений

Reset (Сбросить). Нажмите, чтобы отменить изменения и вернуть их к предыдущим сохраненным значениям.

10.4.4 DHCP - Snooping

На данной странице представлены настройки DHCP Snooping.

Snooping Mode

- ✓ Enabled – Когда режим DHCP Snooping включен, сообщения запроса DHCP будут пересылаться на доверенные порты и разрешать только ответные пакеты от доверенных портов.
- ✓ Disabled – режим DHCP Snooping отключен.

Port Mode Configuration
Отображает статус работы DHCP Snooping для портов.

Trusted – настройка порта в качестве доверенного источника сообщений DHCP;

Untrusted – настройка порта в качестве ненадежного источника сообщений DHCP.

Кнопки

Save (Сохранить). Нажмите для сохранения изменений

Reset (Сбросить). Нажмите, чтобы отменить изменения и вернуть их к предыдущим сохраненным значениям.

10.4.5 DHCP Relay (Настройка DHCP Relay)

Агент ретрансляции DHCP (DHCP Relay Agent) используется для пересылки и передачи сообщений DHCP между клиентами и сервером, когда они не находятся в одной подсети. Он хранит IP-адрес входящего интерфейса в поле GIADDR пакета DHCP. Сервер DHCP может использовать значение поля GIADDR для определения назначенной подсети. Убедитесь, что конфигурация VLAN IP и PVID заданы корректно.

Relay Mode (Режимы ретрансляции)

- ✓ Enabled – Включить режим ретрансляции DHCP;
- ✓ Disabled – Отключить режим ретрансляции DHCP.

Relay Server (Сервер ретрансляции)
Поле отображает IP адресс сервера ретрансляции DHCP

Relay Information Mode (Режимы ретрансляции информации)

- ✓ Enabled – Включить режим Relay Information. DHCP Relay Agent вставляет конкретную информацию (опция 82) в сообщение

DHCP при пересылке на сервер DHCP и удаляет ее из сообщения DHCP при передаче клиенту DHCP.

- ✓ Disabled – Отключить режим Relay Information.

Relay Information Policy

Поле содержит настройки конкретных политик ретрансляции DHCP. Когда включен режим Relay Information Mode и агент DHCP ретрансляции получает сообщение DHCP, которое уже содержит информацию об агенте DHCP ретрансляции, он будет применять политику. Политика «Replace» (Заменять) недействительна, когда Relay Information Mode отключен.

- ✓ Replace (Заменять) – замена оригинальной информации при ретрансляции, если исходное сообщение DHCP уже получено;
- ✓ Keep (Сохранять) – сохранение исходной информации ретрансляции DHCP;
- ✓ Drop (Отбрасывать) – удаление пакета DHCP, когда полученное сообщение DHCP уже содержить информацию о ретрансляции.

Кнопки

Save (Сохранить). Нажмите для сохранения изменений

Reset (Сбросить). Нажмите, чтобы отменить изменения и вернуть их к предыдущим сохраненным значениям.

10.5 Configuration – Security (Настройки безопасности)

В этом разделе WEB интерфейса представлены настройки относящиеся к функциям безопасности коммутатора. Настройки, представленные здесь, можно разделить на 3 категории:

Switch

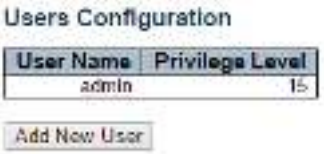
Настройки безопасности, относящиеся к самому коммутатору

Network

Настройки безопасности, относящиеся к локальной сети

AAA
Настройки Безопасности, относящиеся к аутентификации (RADIUS, TACACS+)

10.5.1 Security – Switch – Users (Безопасность – коммутатор - Пользователи)



На данной странице WEB интерфейса представлен список текущих пользователей. Единственный способ войти в систему в качестве другого пользователя на веб-сервере - закрыть и снова открыть браузер.

User Name (Имя пользователя)
Имя пользователя. При щелчке по нему доступно меню с настройками пользователя.

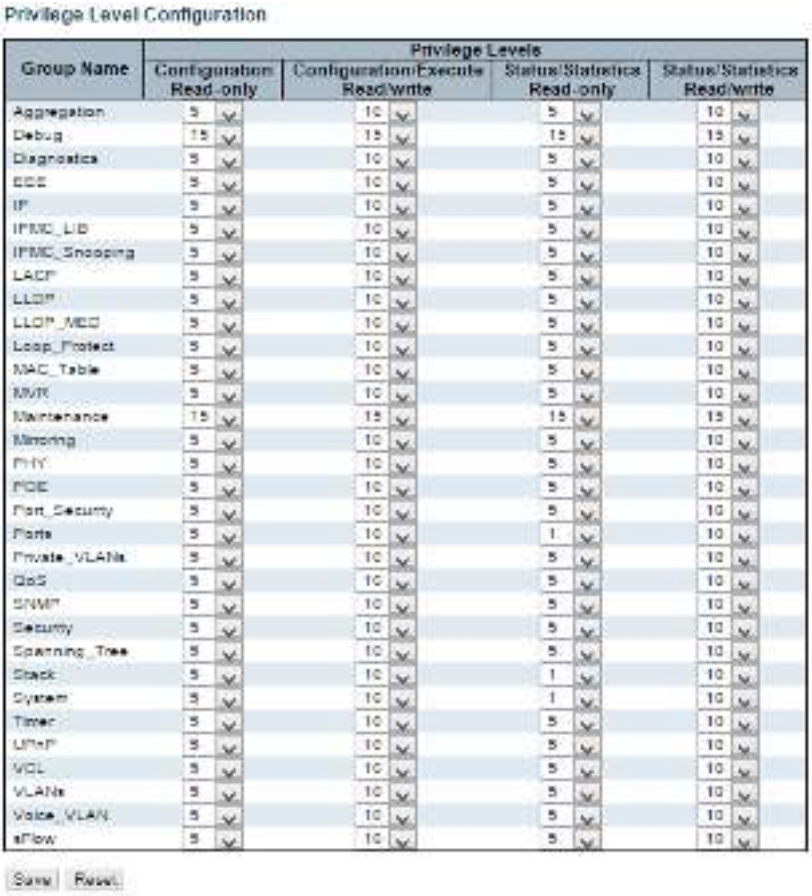
Privelege Level (Уровень привилегий)
Уровень привилегий пользователя. Допустимый диапазон - от 1 до 15.

Если значение уровня привилегий - 15, он может получить доступ ко всем группам, т.е. ему предоставлен полный контроль над устройством (статус администратора).

Значения от 1 до 14 ссылаются на каждый уровень привилегий группы. Уровень привилегии пользователя должен быть такой же или больше, чем уровень привилегий группы, чтобы иметь доступ к этой группе. По умолчанию для большинства групп уровень привилегий равен 5 (доступ только для чтения), уровень привилегий 10 – (доступ для чтения и записи).

Для обслуживания системы (загрузка программного обеспечения, заводские настройки по умолчанию и т.д.) необходим уровень привилегий 15. Уровень привилегий 15 соответствует учетной записи администратора, уровень привилегий 10 соответствует стандартной учетной записи пользователя, уровень привилегий 5 соответствует гостевой учетной записи.

10.5.2 Security – Switch – Privilege Level (Безопасность – Коммутатор – Уровень привилегий)



На этой странице WEB интерфейса представлены настройки уровней привилегий пользователей.

Group Name (Имя группы привилегий)
В большинстве случаев, группа уровня привилегий состоит из одного раздела (например, LACP, RSTP или QoS), но некоторые из них содержат более одного.

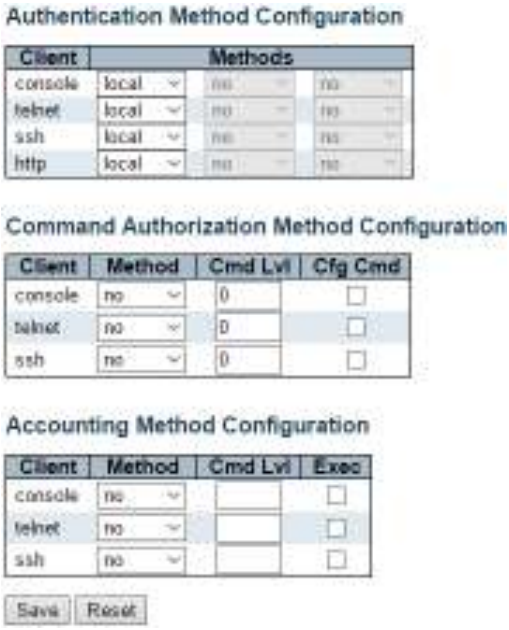
Privilege Levels (Уровни привилегий)
Каждая группа имеет уровень привилегий авторизации для следующих подгрупп: только для чтения, выполнение чтения-записи, статус / статистика только для чтения, статус / статистика для чтения-записи (например, для очистки статистики). Привилегия пользователя должна быть такой же или большей, чем уровень привилегий авторизации, чтобы иметь доступ к этой группе.

Кнопки

Save (Сохранить). Нажмите для сохранения изменений

Reset (Сбросить). Нажмите, чтобы отменить изменения и вернуть их к предыдущим сохраненным значениям.

10.5.3 Security – Switch – Authentication Method (Безопасность – Коммутатор – Аутентификация)



На этой странице представлены возможности по настройке методов аутентификации пользователей.

Client (Клиент управления)
Клиент управления для которого применяются остальные настройки

Method (Метод аутентификации)
Метод аутентификации может быть установлен в одно из следующих значений:

- ✓ No – аутентификация отключена и вход невозможен.
- ✓ Local – использовать локальную базу данных пользователей на коммутаторе для аутентификации.
- ✓ Radius – использовать удаленные серверы RADIUS для аутентификации.
- ✓ Tacacs – использовать удаленные серверы TACACS + для аутентификации.

Методы, в которых задействованы удаленные серверы, блокируются по времени, если удаленные серверы отключены. В этом случае используется следующий метод.

Каждый метод пробуется слева направо до тех пор, пока метод не одобрит или не отклонит пользователя.

Если для первичной аутентификации используется удаленный сервер, рекомендуется настроить вторичную аутентификацию как «локальную».

Это позволит клиенту управления войти в систему через локальную базу данных пользователей, если ни один из настроенных серверов аутентификации не работает в данный момент.

Command Authorization Method Configuration Help

Авторизация через команды позволяет ограничить команды CLI, доступные для пользователя.
Таблица имеет одну строку для каждого типа клиента и количество столбцов:

Client
Клиент управления для которого применяются остальные настройки

Method

- ✓ No – Авторизация через команды отключена. Пользователю предоставляется доступ к командам CLI в соответствии с его уровнем привилегий.
- ✓ Tacacs – Используются удаленные серверы TACACS + для авторизации через команды. Если все удаленные серверы отключены, пользователю предоставляется доступ к командам CLI в соответствии с его уровнем привилегий.

CMD Lvl
Установка приоритета с уровнем привилегий выше или равным этому уровню. Допустимые значения находятся в диапазоне от 0 до 15.

CFG CMD
Установка приоритета для команд конфигурации (CFG).

Accounting Method Configuration Help

Раздел учета позволяет вам настроить учет на основе команд и exec (логин) учет по логину/паролю.

Таблица имеет одну строку для каждого типа клиента и количество столбцов:

Client
Клиент управления для которого применяются остальные настройки

Method

- ✓ No – Авторизация через учет пользователей отключена. Пользователю предоставляется доступ к командам CLI в соответствии с его уровнем привилегий.
- ✓ Tacacs – Используются удаленные серверы TACACS +

CMD Lvl
Активация учета с уровнем привилегий выше или равным этому уровню. Допустимые значения находятся в диапазоне от 0 до 15.

Exec
Активация учета по логину/паролю

Кнопки

Save (Сохранить). Нажмите для сохранения изменений

Reset (Сбросить). Нажмите, чтобы отменить изменения и вернуть их к предыдущим сохраненным значениям.

10.5.4 Security – Switch – SSH (Безопасность – Коммутатор – SSH)

Mode (Режим работы)
- ✓ Enabled – Активация операций через SSH;
- ✓ Disabled – Отключение операций через SSH

Кнопки

Save (Сохранить). Нажмите для сохранения изменений

Reset (Сбросить). Нажмите, чтобы отменить изменения и вернуть их к предыдущим сохраненным значениям.

10.5.5 Security – Switch – HTTPS (Безопасность – Коммутатор – HTTPS)

Mode (Режим работы)
Указывает на работу в режиме HTTPS. Если текущим соединением является HTTPS, для применения режима «disabled HTTPS» сеанс автоматически будет перенаправлен на соединение HTTP.
Возможные режимы:

- ✓ Enabled – Активация использования HTTPS;
- ✓ Disabled – Запрет на использование HTTPS.

Automatic Redirect (Автоматическое перенаправление)
Укажите режим перенаправления HTTPS. Это имеет значение только в том случае, если выбран «HTTPS Mode – Enabled». Когда режим перенаправления включен, HTTP-соединение будет перенаправлено на HTTPS-соединение автоматически.

Внимание! Браузер может не разрешить операцию перенаправления из-за соображений безопасности, если сертификат коммутатора не является доверенным для браузера. В этом случае необходимо инициализировать HTTPS-соединение вручную.

- ✓ Enabled – Включить перенаправление HTTPS;
- ✓ Disabled – Выключить перенаправление HTTPS

Certificate Maintain (Поддержка сертификата)

- ✓ None – не использовать сертификаты;
- ✓ Delete – Удалить текущий сертификат;
- ✓ Upload – Загрузить файл сертификата с разрешением PEM;
- ✓ Generate – Сгенерировать RSA сертификат.

Certificate Pass Phrase
Фраза пароль, если сертификат защищен подобным образом.

Certificate Upload (Загрузка сертификата)
Загрузка сертификата с расширением PEM в коммутатор. Файл должен содержать сертификат и секретный ключ. Если у вас несколько файлов отдельно, то используйте команду в Linux cat my.cert my.key > my.pem
Доступна загрузка через WEB браузер или через ссылку URL.

Certificate Status (Статус сертификата)
Поле отображает текущий статус сертификата. Возможные статусы:

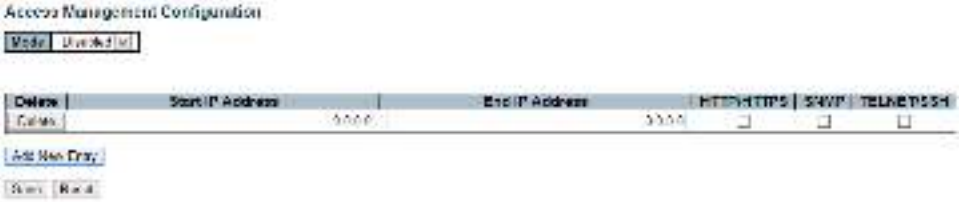
- ✓ Switch secure HTTP certificate is presented – HTTP сертификат присутствует;
- ✓ Switch secure HTTP certificate is not presented – HTTP сертификат не найден;
- ✓ Switch secure HTTP certificate is generating – HTTP сертификат подготавливается…

Кнопки

Save (Сохранить). Нажмите для сохранения изменений

Reset (Сбросить). Нажмите, чтобы отменить изменения и вернуть их к предыдущим сохраненным значениям.

10.5.6 Security – Switch – Access Management (Безопасность – Коммутатор – Управление доступом)



Настройте таблицу управления доступом на этой странице. Максимальное количество записей - 16. Если тип приложения соответствует какой-либо из записей управления доступом, он получит доступ к коммутатору.

Mode (режим работы)

- ✓ Enabled – Включить управление доступом;
- ✓ Disabled – Выключить управление доступом.

Delete (Удалить)
Отметьте, чтобы удалить запись. Запись будет удалена при следующем сохранении.

Start IP Address (Начальный IP адрес)
Отображает стартовый стартовый IP адрес

End IP Address (Конечный IP адрес)
Отображает конечный стартовый IP адрес

HTTP/HTTPS (Доступ через HTTP/HTTPS)
Отображает возможность хоста получить доступ через HTTP/HTTPS

SNMP (Доступ через SNMP)
Отображает возможность хоста получить доступ к коммутатору через SNMP

TELNET/SSH (Доступ через TELNET/SSH)
Отображает возможность хоста получить доступ к коммутатору через TELNET/SSH

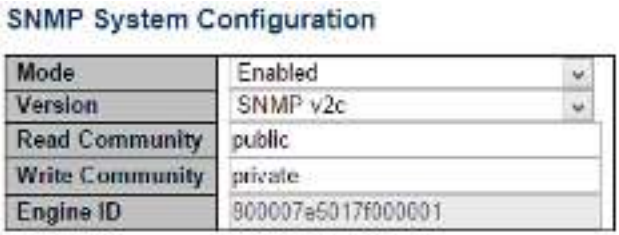
Кнопки

Save (Сохранить). Нажмите для сохранения изменений

Reset (Сбросить). Нажмите, чтобы отменить изменения и вернуть их к предыдущим сохраненным значениям.

10.5.7 Security – Switch – SNMP (Безопасность – Коммутатор – SNMP)

10.5.7.1 SNMP-System (SNMP-Основные настройки)



На данной странице WEB интерфейса представлены основные настройки SNMP (протокол сетевого управления) в системе. Чаще всего, SNMP используется для получения какой либо диагностической информации из коммутатора.

Mode (Режимы работы)

- ✓ Enabled – поддержка SNMP включена;
- ✓ Disabled – поддержка SNMP отключена.

Version (Используемая версия SNMP). Протокол SNMP v3 требует аутентификацию на основе хеширования (md5 или SHA). Это делает использование SNMP v3 более безопасным.

- ✓ SNMP v1;
- ✓ SNMP v2c;
- ✓ SNMP v3.

Read Community (Строка для группы пользователей с правами на чтение).

Допустимая длина 0 – 255 символов. Поле применимо только если используется SNMPv1 или SNMPv2c. В случае, если выбран протокол SNMPv3, строка Read Community будет связана с таблицей SNMPv3. В дополнение к Read Community для ограничения подсети истоника можно использовать определенный диапазон адресов.

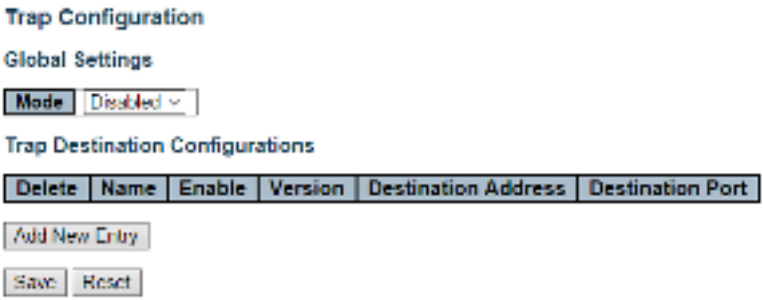
Write Community (Строка для группы пользователей с правами на запись).

Допустимая длина 0 – 255 символов. Поле применимо только если используется SNMPv1 или SNMPv2c. В случае, если выбран протокол SNMPv3, строка Write Community будет связана с таблицей SNMPv3. В дополнение к Write Community для ограничения подсети истоника можно использовать определенный диапазон адресов.

Engine ID

Указывает ID SNMPv3. Строка должна содержать четное число (в шестнадцатеричном формате) с количеством цифр от 10 до 64, но все нули и все -F не допускаются к использованию. Изменение Engine ID приведет к очистке списка локальных пользователей.

10.5.7.2 SNMP-TRAP



На данной странице WEB интерфейса представлены настройки SNMP Trap.

Глобальные настройки:
Mode (Режим работы с SNMP Trap)

- ✓ Enabled – включены операции с SNMP Trap;
- ✓ Disabled – отключены операции с SNMP Trap.

Настройки
Name Отображает имя назначения SNMP Trap.

Enabled (Режим работы с SNMP Trap). Включено (Enabled) / Выключено (Disabled).

Version (Версия SNMP Trap). Доступные версии:

- ✓ SNMPv1;
- ✓ SNMPv2c;
- ✓ SNMPv3.

Destination Address (Адрес назначения SNMP Trap).
Здесь отображается действительный IP адрес в десятичном виде с точками (x.y.z.w) или действительное имя хоста (строка из алфавита A-Za-z), цифр 0-9, точки(.) и тире (-)). Для IPv6 адрес указан в 128-битном виде (8 полей длиной до четырех шестнадцатеричных цифр с двоеточием, разделяющим каждое поле (:). Например, 'fe80 :: 215: c5ff: fe03: 4dc7').

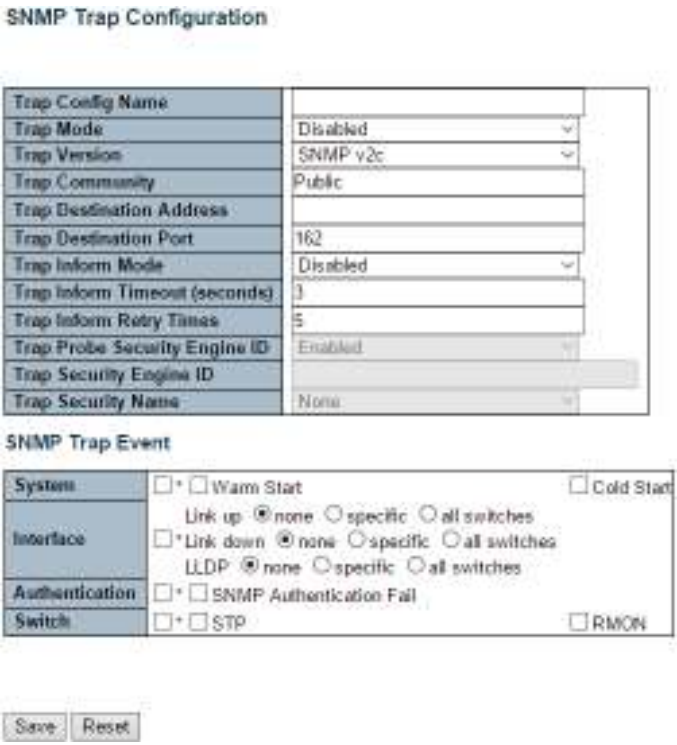
Destination Port (порт назначения SNMP Trap).
Поле отображает порт назначения SNMP Trap. SNMP Agent отправляет SNMP сообщение через этот порт. Допустимый диапазон выбранных портов 1-65535.

Кнопки

Add New Entry (Добавить новую запись). Нажмите, чтобы добавить новую запись.

Save (Сохранить). Нажмите для сохранения изменений

Reset (Сбросить). Нажмите, чтобы отменить изменения и вернуть их к предыдущим сохраненным значениям.



Детальная настройка SNMP Trap.

Trap Config Name (Имя конфигурации SNMP Trap).
Поле, в котором задается имя для настраиваемой конфигурации SNMP Trap. Допустимое имя 1 – 32 символа ASCII.

Trap Mode (режим работы SNMP Trap)

- ✓ Enabled – включено;
- ✓ Disabled – выключено.

Trap Version (Версия SNMP Trap). Доступные версии:

- ✓ SNMPv1;
- ✓ SNMPv2c;
- ✓ SNMPv3.

Trap Community (Строка доступа при отправке SNMP Trap)
Допустимая длина 0 – 255 символов ASCII.

Trap Destination Address (Адрес назначения SNMP Trap)
Здесь может быть указан действительный IP адрес в десятичном виде с точками (x.y.z.w) или действительное имя хоста (строка из алфавита A-Za-z), цифр 0-9, точки(.) и тире (-)). Для IPv6 адрес должен быть указан в 128-битном виде (8 полей длиной до четырех шестнадцатеричных цифр с двоеточием, разделяющим каждое поле (:). Например, 'fe80 :: 215: c5ff: fe03: 4dc7').

Destination Port (порт назначения SNMP Trap).
Поле задает порт назначения SNMP Trap. SNMP Agent отправляет SNMP сообщение через этот порт. Допустимый диапазон выбранных портов 1-65535.

Trap Inform Mode (Режим работы SNMP Trap Inform)

- ✓ Enabled – включено;
- ✓ Disabled – выключено.

Trap Inform Timeout(seconds)
Поле, в котором задается временной интервал для SNMP Trap Inform. Доступные значения 0 – 2147 (сек).

Trap Inform Retry Times (Количество повторений SNMP Trap Inform)
Поле, в котором задается количество повторных отправлений SNMP Trap Inform. Доступные значения 0 – 255.

Trap Probe Security Engine ID (Идентификатор подсистемы безопасности SNMP Trap, режим работы)

- ✓ Enabled – включено;
- ✓ Disabled – выключено.

Trap Security Engine ID (Идентификатор подсистемы безопасности SNMP Trap)
SNMPv3 отправляет SNMP Trap и SNMP Informs пакеты используя USM для аутентификации и соблюдения конфиденциальности. Для таких SNMP Trap используется уникальный Engine ID. Если «Trap Probe Security Engine ID» включен, идентификатор будет проверяться автоматически. В противном случае используется идентификатор, указанный в этом поле. Строка должна содержать четное число (в шестнадцатеричном формате) с количеством цифр от 10 до 64, но все нули и все -F не допускаются.

Trap Security Name (Имя безопасности SNMP Trap)
Поле содержит SNMP trap security name. SNMPv3 использует USM для аутентификации и соблюдения конфиденциальности. Уникальное имя необходимо для SNMP Trap и SNMP Inform, если они включены.

System (Основные настройки интерфейсных групп SNMP Trap)
Warm Start – включает/отключает «теплый» старт для SNMP Trap;
Cold Start – включает/отключает «холодный» старт для SNMP Trap.

Interface (Интерфейс). Поле содержит настройки, позволяющие SNMP генерировать SNMP Trap при ошибках в аутентификации. Доступные режимы:

- ✓ Link Up – Включить/выключить Link Up Trap;
- ✓ Link Down – Включить/выключить Link down Trap;
- ✓ LLDP – Включить/выключить LLDP trap.

Authentication (Аутентификация)
Поле активирует генерацию SNMP Trap при процессах аутентификации.

Switch

Поле активирует генерацию SNMP Trap при активном STP и RMON

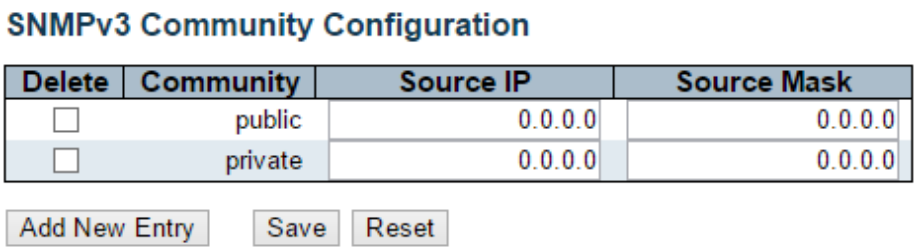
- ✓ STP – Включает/выключает генерацию SNMP Trap при активном STP;
- ✓ RMON – Включает/выключает генерацию SNMP Trap при активном RMON.

Кнопки

Save (Сохранить). Нажмите для сохранения изменений

Reset (Сбросить). Нажмите, чтобы отменить изменения и вернуть их к предыдущим сохраненным значениям.

10.5.7.3 SNMP-Community (Таблица строк состояний доступа SNMP)



На данной странице WEB интерфейса представлены настройки таблицы Community для SNMPv3 (если активно).

Delete (Удалить).
Необходимо отметить галкой, если планируется удалить запись из таблицы при следующем сохранении.

Community (Строка состояния доступа).
Отображает строку состояния доступа. Допустимая длина строки 1- 32 символа ASCII. Данная строка будет считаться Security Name и отображать SNMPv1 / SNMPv2c строку.

Source IP (IP адрес источника)
Отображает IP адрес источника доступа SNMP. Определенный диапазон адресов источника может использоваться для ограничения подсети источника в сочетании с маской источника.

Source Mask (Маска подсети источника)
Отображает маску подсети источника доступа SNMP.

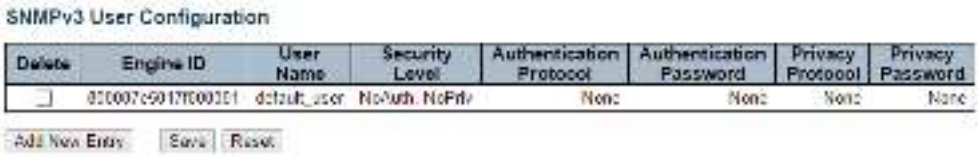
Кнопки

Add New Entry (Добавить новую запись). Нажмите, чтобы добавить новую запись.

Save (Сохранить). Нажмите для сохранения изменений

Reset (Сбросить). Нажмите, чтобы отменить изменения и вернуть их к предыдущим сохраненным значениям.

10.5.7.4 SNMP-User (Настройка пользователя SNMP)



На данной странице WEB интерфейса представлена возможность гибко настроить пользователей для SNMPv3. Ключами записи будут являться Engine ID и User Name.

Delete (Удалить).
Необходимо отметить галкой, если планируется удалить запись из таблицы при следующем сохранении.

Engine ID

Строка должна содержать четное число (в шестнадцатеричном формате) с количеством цифр от 10 до 64, но все нули и все -F не допускаются.

Архитектура SNMPv3 предполагает использование модели безопасности на основе разделения прав доступа пользователей (USM) для защиты сообщений и модель управления доступом на основе представлений (VACM) для контроля доступа.

Для записи USM usmUserEngineID и usmUserName являются ключами записи. В простом агенте usmUserEngineID всегда является собственным значением snmpEngineID этого агента.

Это значение также может принимать значение snmpEngineID удаленного механизма SNMP, с которым этот пользователь может общаться. Другими словами, если Engine ID пользователя равен идентификатору System ID, то это локальный пользователь; в противном случае это удаленный пользователь.

User Name (Имя пользователя)

Строка, идентифицирующая имя пользователя. Допустимая длина строки 1 – 32 символа ASCII.

Security Level (Уровень безопасности)

Поле содержит модели безопасности, к которой должна принадлежать запись.

- ✓ NoAuth, NoPriv – нет аутентификации / нет конфиденциальности;
- ✓ Auth, NoPriv – аутентификация / нет конфиденциальности;
- ✓ Auth, Priv – аутентификация / конфиденциальность.

Значения уровня безопасности нельзя изменить, если запись уже существует. Это означает, что необходимо убедиться, что значение установлено правильно.

Authentication Protocol (Протокол аутентификации)

Поле содержит протокол аутентификации, который использует конфигурируемая запись. Доступны следующие протоколы:

- ✓ None – протокол аутентификации не используется;
- ✓ MD5 – используется протокол MD5 для аутентификации;
- ✓ SHA – используется протокол SHA для аутентификации.

Authentication Password (Пароль для аутентификации)
Для аутентификации с использованием протокола MD5 длина пароля составляет от 8 до 32 символов. Для аутентификации с использованием протокола SHA длина пароля составляет от 8 до 40 символов ASCII.

Privacy Protocol (Протокол конфиденциальности)

- ✓ None – протокол конфиденциальности не используется;
- ✓ DES – используется протокол конфиденциальности DES.

Privacy Password (Пароль конфиденциальности)
Допустимая длина 8 – 32 символа ASCII.

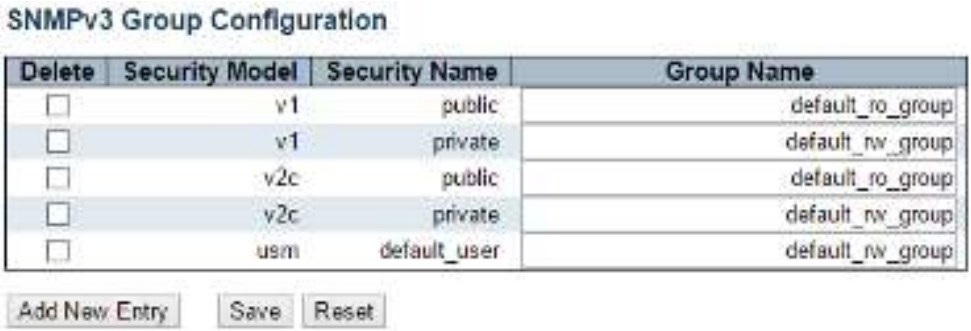
Кнопки

Add New Entry (Добавить новую запись). Нажмите, чтобы добавить новую запись.

Save (Сохранить). Нажмите для сохранения изменений

Reset (Сбросить). Нажмите, чтобы отменить изменения и вернуть их к предыдущим сохраненным значениям.

10.5.7.5 SNMP-Groups (SNMP-Группы)



На данной странице WEB интерфейса представлены возможности по настройке таблицы групп SNMPv3.

Delete (Удалить).
Необходимо отметить галкой, если планируется удалить запись из таблицы при следующем сохранении.

Security Model (Модель безопасности)

- ✓ v1 – зарезервировано для SNMPv1;
- ✓ v2c – зарезервировано для SNMPv2c;
- ✓ USM – модель безопасности на основе пользователей.

Security Name (Строка имени)
Строка отображает имя, которому принадлежит эта запись. Допустимая длина 1-32 символа ASCII.

Group Name (Имя группы)
Строка, идентифицирующая имя группы, к которой должна принадлежать эта запись. Допустимая длина 1-32 символа ASCII.

Кнопки

Add New Entry (Добавить новую запись). Нажмите, чтобы добавить новую запись.

Save (Сохранить). Нажмите для сохранения изменений

Reset (Сбросить). Нажмите, чтобы отменить изменения и вернуть их к предыдущим сохраненным значениям.

10.5.7.6 SNMP–Views

На данной странице WEB интерфейса представлены настройки таблицы представления.

Delete (Удалить).
Необходимо отметить галкой, если планируется удалить запись из таблицы при следующем сохранении.

View Name (Имя представления)
Строка, отображающая имя представления, которому должна принадлежать запись. Допустимая длина 1-32 символа ASCII.

View Type (Тип представления)
- ✓ Included – включенные в дерево записи;
- ✓ Excluded – исключенные из дерева записи.

OID Subtree (OID субдерево)
Допустимая длина OID 1-128. Допустимым содержимым является цифровой номер или звездочка.

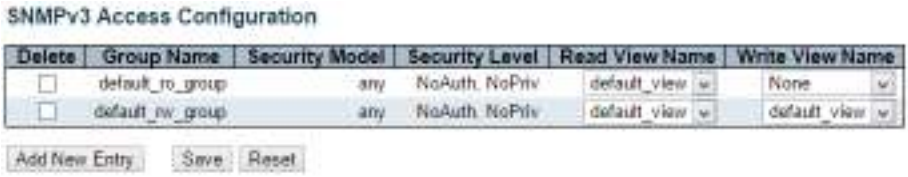
Кнопки

Add New Entry (Добавить новую запись). Нажмите, чтобы добавить новую запись.

Save (Сохранить). Нажмите для сохранения изменений

Reset (Сбросить). Нажмите, чтобы отменить изменения и вернуть их к предыдущим сохраненным значениям.

10.5.7.7 SNMP-Access (SNMP-Доступ)



На данной странице WEB интерфейса представлены настройки доступа для SNMPv3.

Delete (Удалить).
Необходимо отметить галкой, если планируется удалить запись из таблицы при следующем сохранении.

Group name (Групповое Имя)
Строка, содержащая групповое имя, которому принадлежит запись. Допустимая длина 1-32 символа ASCII.

Security Model (Модель безопасности)

- ✓ Any – любая модель будет принята (v1/v2c/usm)
- ✓ v1 – зарезервировано для SNMPv1;
- ✓ v2c – зарезервировано для SNMPv2c;
- ✓ USM – модель безопасности на основе пользователей.

Security Level (Уровень безопасности)
Поле содержит модели безопасности, к которой должна принадлежать запись.

- ✓ NoAuth, NoPriv – нет аутентификации / нет конфиденциальности;
- ✓ Auth, NoPriv – аутентификация / нет конфиденциальности;
- ✓ Auth, Priv – аутентификация / конфиденциальность.

Read View Name (Имя представления на чтение)
Имя представления MIB, определяющее объекты MIB, для которых этот запрос может запрашивать текущие значения. Допустимая длина строки - от 1 до 32, символы ASCII от 33 до 126.

Write View Name (Имя представления на запись)
Имя представления MIB, определяющее объекты MIB, для которых этот запрос может запрашивать текущие значения. Допустимая длина строки - от 1 до 32, символы ASCII от 33 до 126.

Кнопки

Add New Entry (Добавить новую запись). Нажмите, чтобы добавить новую запись.

Save (Сохранить). Нажмите для сохранения изменений

Reset (Сбросить). Нажмите, чтобы отменить изменения и вернуть их к предыдущим сохраненным значениям.

10.5.8 Security - Switch – RMON (Протокол дистанционного мониторинга RMON)

10.5.8.1 RMON – Statistics (RMON – Таблица статистики)

На данной странице WEB интерфейса представлены настройки протокола дистанционного сетевого мониторинга RMON.

Delete (Удалить).
Необходимо отметить галкой, если планируется удалить запись из таблицы при следующем сохранении.

ID (Идентификатор)
Поле содержит идентификатор входа в диапазоне от 1 до 65535.

Data Source (Источник данных)
Поле отображает ID порта, за которым будет вестись мониторинг. Если коммутатор находится в стеке, то к значению необходимо добавить 1000*(ID коммутатора-1), например, если порт 5 коммутатора № 3, то значение будет 2005

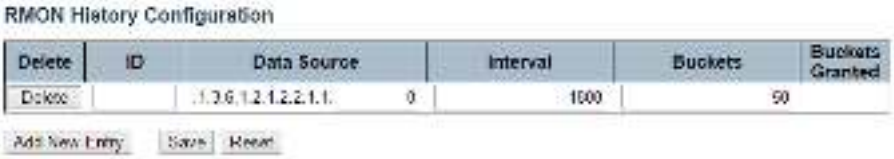
Кнопки

Add New Entry (Добавить новую запись). Нажмите, чтобы добавить новую запись.

Save (Сохранить). Нажмите для сохранения изменений

Reset (Сбросить). Нажмите, чтобы отменить изменения и вернуть их к предыдущим сохраненным значениям.

10.5.8.2 RMON – History (RMON – Таблица с историей работы RMON)



На данной странице WEB интерфейса представлены инструменты доступа к таблице с историей работы RMON.

Delete (Удалить).
Необходимо отметить галкой, если планируется удалить запись из таблицы при следующем сохранении.

ID (Идентификатор)
Поле содержит идентификатор входа в диапазоне от 1 до 65535.

Data Source (Источник данных)
Поле отображает ID порта, за которым будет вестись мониторинг. Если коммутатор находится в стеке, то к значению необходимо добавить 1000*(ID коммутатора-1), например, если порт 5 коммутатора № 3, то значение будет 2005

Interval (Временной интервал)
Поле содержит временной интервал в секундах для выборки данных из истории работы RMON. Доступные значения 1 – 3600 сек. Значение по умолчанию – 1800 сек.

Buckets
Поле содержит максимальное количество записей данных, связанных с этой записью управления историей, сохраненной в RMON. Диапазон составляет от 1 до 3600, значение по умолчанию - 50.

Buckets Granted
Количество данных, которое должно быть сохранено в RMON

Кнопки

Add New Entry (Добавить новую запись). Нажмите, чтобы добавить новую запись.

Save (Сохранить). Нажмите для сохранения изменений

Reset (Сбросить). Нажмите, чтобы отменить изменения и вернуть их к предыдущим сохраненным значениям.

10.5.8.3 RMON-Alarm (RMON-Тревога)

На данной странице WEB интерфейса представлены инструменты для работы с тревожными событиями RMON.

Delete (Удалить).
Необходимо отметить галкой, если планируется удалить запись из таблицы при следующем сохранении.

ID (Идентификатор)
Поле содержит идентификатор входа в диапазоне от 1 до 65535.

Interval (Временной интервал)
Указывает интервал в секундах для выборки и сравнения порога нарастания и спада. Диапазон составляет от 1 до 2 ^ 31-1.

Variable (Переменные)
Указывает конкретную переменную для выборки, возможные переменные:

- ✓ InOctets – Общее количество октетов, полученных на интерфейсе, включая символы кадрирования;
- ✓ InUcastPkts – Количество одноадресных пакетов, доставленных по протоколу более высокого уровня;
- ✓ InNUcastPkts – Количество многоадресных и многоадресных пакетов, доставленных по протоколу более высокого уровня;
- ✓ InDiscards – Количество входящих пакетов, которые отбрасываются, даже если они нормальные;
- ✓ InErrors – Количество входящих пакетов, которые содержали ошибки, препятствующие их доставке в протокол более высокого уровня;
- ✓ InUnknownProtos – количество входящих пакетов, которые были отброшены из-за неизвестного или неподдерживаемого протокола;
- ✓ OutOctets – Количество октетов, передаваемых вне интерфейса, включая символы кадрирования;
- ✓ OutUcastPkts – Количество одноадресных пакетов, которые запрашивают передачу;
- ✓ OutNUcastPkts – Количество многоадресных и многоадресных пакетов, которые запрашивают передачу;
- ✓ OutDiscards – Количество исходящих пакетов, которые отбрасываются, если пакеты нормальные;
- ✓ OutErrors – Количество исходящих пакетов, которые не удалось передать из-за ошибок;
- ✓ OutQLen – Длина очереди исходящих пакетов (в пакетах).

Sample Type (Тип выборки)
Метод выборки выбранной переменной и вычисления значения для сравнения с пороговыми значениями, возможные типы выборки:

- ✓ Absolute – напрямую;
- ✓ Delta – рассчитать разницу между образцами (по умолчанию).

Value (Значение)
Значение статистики за последний период выборки.

Startup Alarm (Тревожное сообщение при запуске)

Метод выборки выбранной переменной и вычисления значения для сравнения с пороговыми значениями, возможные типы выборки:

- ✓ RisingTrigger – тревожное сообщение, когда первое значение больше, чем порог нарастания;
- ✓ FallingTrigger – тревожное сообщение FallingTrigger, когда первое значение меньше порога падения;
- ✓ RisingOrFallingTrigger – тревожное сообщение, когда первое значение больше, чем порог нарастания или меньше, чем порог спада (по умолчанию).

Rising Threshold (Повышение порога)
Повышение порогового значения (-2147483648-2147483647).

Rising Index (Индекс роста)
Доступные значения 1 – 65535

Falling Threshold (Порог падения)
Значение порога падения (-2147483648-2147483647)

Falling Index (Индекс падения)
Доступные значения 1 – 65535

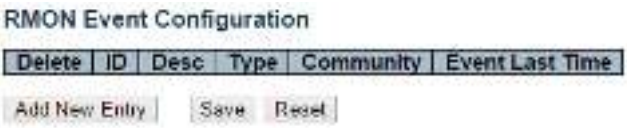
Кнопки

Add New Entry (Добавить новую запись). Нажмите, чтобы добавить новую запись.

Save (Сохранить). Нажмите для сохранения изменений

Reset (Сбросить). Нажмите, чтобы отменить изменения и вернуть их к предыдущим сохраненным значениям.

10.5.8.4 RMON – Event (RMON - События)



На данной странице WEB интерфейса представлены инструменты для работы с журналом событий. Индекс входа является ID.

Delete (Удалить).
Необходимо отметить галкой, если планируется удалить запись из таблицы при следующем сохранении.

ID (Идентификатор)
Поле содержит идентификатор входа в диапазоне от 1 до 65535.

Desc
Длина строки от 0 до 127, по умолчанию это пустая строка.

Type (Тип)

- ✓ None – общее количество октетов, полученных на интерфейсе, включая символы кадрирования;
- ✓ Log – количество одноадресных пакетов, доставленных по протоколу более высокого уровня;
- ✓ Snmptrap – количество пакетов с широковещательной (broadcast) и многоадресной передачей (multicast), доставленных по протоколу более высокого уровня;
- ✓ Logandtrap – количество входящих пакетов, которые отбрасываются, даже если пакеты нормальные.

Community
Укажите значение Community при отправке SNMP Trap, длина строки от 0 до 127, по умолчанию "public".

Event Last Time (Событие в последний момент)
Указывает значение sysUpTime в момент, когда эта запись события в последний раз генерировала событие.

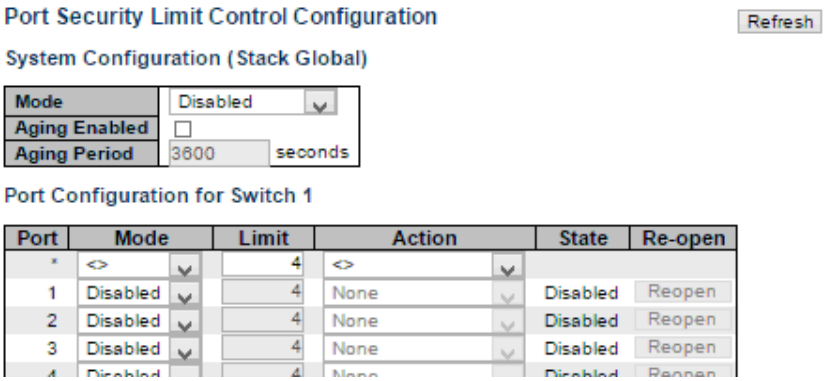
Кнопки

Add New Entry (Добавить новую запись). Нажмите, чтобы добавить новую запись.

Save (Сохранить). Нажмите для сохранения изменений

Reset (Сбросить). Нажмите, чтобы отменить изменения и вернуть их к предыдущим сохраненным значениям.

10.5.9 Security – Network – Limit Control (Безопасность – Сеть – Контроль ограничений)



На данной странице WEB интерфейса представлены настройки контроля ограничений безопасности портов.

Ограничение контроля позволяет ограничить количество пользователей на данный порт.

Пользователь идентифицируется по MAC-адресу и идентификатору VLAN.

Если для порта включено ограничение контроля, ограничение определяет максимальное количество пользователей на порте. Если

это число превышено, выполняется действие. Действие может быть одним из четырех различных действий, как описано ниже.

Модуль контроля ограничений (Limit Control) использует модуль нижнего уровня, модуль безопасности порта, который управляет MAC-адресами, запомненными на порте.

Конфигурация Limit Control состоит из двух разделов:

- ✓ Для системы в целом
- ✓ Для портов

Системные настройки

Mode (Режим работы)

Отображает текущее состояние функции Limit Control. Включена ли глобально или выключена.

Если отключено глобально, то другие модули могут все еще использовать базовую функциональность, но проверка ограничений и соответствующие действия отключены.

Aging Enabled (Устаревание включено)

Если активно, то защищаемые MAC адреса подвержены устареванию, подробнее описано в разделе «Период старения»

Aging Period (Период старения)

Если установлен флаг «Aging Enabled», период старения контролируется этим параметром.

Если другие модули используют базовый порт безопасности для защиты MAC-адресов, они могут иметь другие требования к периоду старения. Базовая защита порта будет использовать более короткий запрошенный период устаревания всех модулей, которые используют этот параметр. Период старения может быть установлен в диапазоне от 10 до 10 000 000 секунд.

Настройка портов.

Port (Порт)

Номер порта, к которому будут применены настройки ниже.

Mode (Режим работы)
Управляет включением Limit Control на этом порту. Для этого, и для общего режима должно быть установлено значение «Включено» (Enabled), чтобы функция Limit Control имела эффект.
Другие модули могут по-прежнему использовать базовые функции безопасности порта без включения Limit Control для данного порта.

Limit (Ограничение)
Максимальное количество MAC-адресов, которые могут быть защищены на этом порту. Это число не может превышать 1024. Если лимит превышен, выполняется соответствующее действие (action).
Стек создается с общим количеством MAC-адресов, с которых все порты получают адрес каждый раз, когда новый MAC-адрес виден на порте с включенной функцией Limit Control.
Поскольку все порты берутся из одного пула, может случиться так, что сконфигурированный максимум не может быть предоставлен, если оставшиеся порты уже использовали все доступные MAC-адреса.

Action (Действие)
Если значение ограничение (Limit) достигнуто (1024/порт), коммутатор может применить одно из следующих действий:

- ✓ None – Не разрешать дальнейшее ограничение MAC адресов на порте, но не предпринимать никаких действий;
- ✓ Trap – Если на порту достигнут предел +1 MAC адрес, будет отправлен пакет SNMP Trap. Если устаревание отключено, будет отправлен один пакет SNMP Trap. Если устаревание включено, пакеты SNMP Trap будут отправляться каждый раз, когда достигнут предел MAC адресов.
- ✓ Shutdown – Если на порту достигнут предел +1 MAC адрес, порт будет отключен. Имеется ввиду, что все защищенные MAC адреса будут удалены из таблицы для этого порта, а новые MAC адреса не смогут быть запомнены. Даже если порт физически отсоединен/соединен кабелем, порт останется отключенным. Предусмотрено 3 способа сделать порт снова активным:
    - Перезагрузить стэк;
    - Выключить/включить заново Limit Control для порта или стэка;

- Нажать кнопку – «Reopen» (открыть заново).

- ✓ Trap & Shutdown – Если на порту достигнут предел +1 MAC адрес, будут выполнены оба действия, описанные выше «Trap» и «Shutdown».

State (Состояние)
В этом столбце отображается текущее состояние порта с включенной функцией Limit Control. Состояние может принимать одно из 4 значений:

- ✓ Disabled – функция Limit Control отключена для этого порта или отключена в глобальных настройках;
- ✓ Ready – функция Limit Control активна, предел MAC адресов не достигнут;
- ✓ Limit Reached – лимит MAC адресов достигнут;
- ✓ Shutdown – порт отключен для дальнейшего запоминания MAC адресов.

Re-Open Button (Кнопка «Открыть заново»)
Если порт выключен в следствие достигнутого предела MAC адресов, вы можете открыть его заново, нажав данную кнопку.

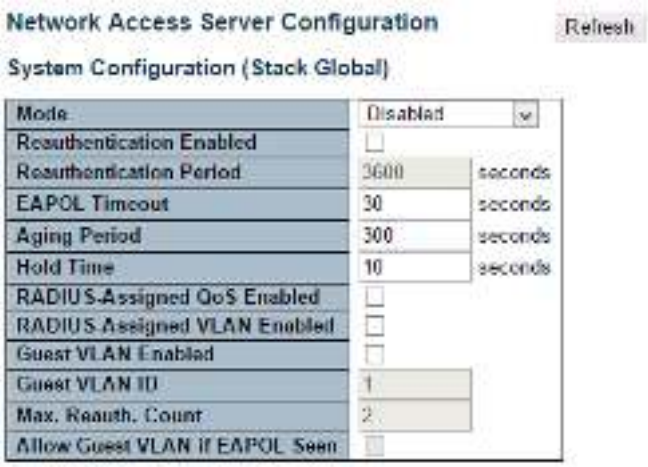
Кнопки

Add New Entry (Добавить новую запись). Нажмите, чтобы добавить новую запись.

Save (Сохранить). Нажмите для сохранения изменений

Reset (Сбросить). Нажмите, чтобы отменить изменения и вернуть их к предыдущим сохраненным значениям.

10.5.10 Security – Network – NAS (Network Access Server)



На данной странице WEB интерфейса представлены настройки IEEE 802.1X и системы аутентификации на базе MAC адресов.

Стандарт IEEE 802.1X определяет процедуру контроля доступа на основе портов, которая предотвращает несанкционированный доступ к сети, требуя от пользователей сначала предоставить учетные данные для аутентификации.

Один или несколько центральных серверов, дополнительные серверы, определяют, разрешен ли пользователю доступ к сети. Эти внутренние серверы (RADIUS) настраиваются на странице «Configuration→Security→AAA»

Аутентификация на базе MAC-адресов позволяет аутентифицировать более одного пользователя на одном и том же порту и не требует, чтобы у пользователя было установлено специальное программное обеспечение как при использовании 802.1X в системе.

Коммутатор использует MAC-адрес пользователя для аутентификации на внутреннем сервере. Злоумышленники могут подменять MAC-адреса, что делает проверку подлинности на основе MAC менее безопасной, чем проверка подлинности 802.1X.

Mode (Режим работы)
Enabled – NAS глобально включен;
Disabled – NAS глобально выключен (всем портам разрешена пересылка фреймов).

Re-authentication Enabled (Включить повторную аутентификацию)
Если этот флаг установлен, устройства, прошедшие успешную аутентификацию, проходят повторную аутентификацию после интервала, указанного в поле «Re-authentication Period». Повторную аутентификацию для портов с поддержкой 802.1X можно использовать для определения, подключено ли новое устройство к порту коммутатора.

Re-authentication Period (Период повторной аутентификации)
Данное поле определяет период в секундах после которого клиент должен пройти повторную аутентификацию. Поле активно, если установлен флаг «Re-authentication Enabled». Допустимые значения 1 – 3600 сек.

EAPOL Timeout
Определяет время для повторной передачи фреймов EAPOL идентификатора запроса.
Допустимые значения находятся в диапазоне от 1 до 65535 сек. Это не влияет на порты на основе MAC адресов.

Aging Period (Период устаревания)
Этот параметр применяется к следующим режимам работы NAS:

- ✓ Single 802.1X
- ✓ Multi 802.1X
- ✓ MAC-Based Auth.

Когда модуль NAS использует модуль защиты портов (Port Security) для защиты MAC адресов, Port Security требует проверку рассматриваемого MAC адреса и освобождает ресурсы, если не наблюдается никакой активности за определенный период. Этот период и есть период устаревания. Он может быть установлен в диапазоне от 10 до 1000000 сек.

Если повторная аутентификация включена и порт находится в режиме на основе 802.1X, это не так критично, так как устройства-соискатели, которые больше не подключены к порту, будут удалены при следующей повторной аутентификации, что приведет к сбою. Но если повторная аутентификация не включена, единственный способ освободить ресурсы коммутатора – использование устаревания записей.

Для портов на основе MAC адресной аутентификации повторная аутентификация не вызывает прямой связи между коммутатором и клиентом, поэтому она не определяет, подключен ли клиент по-прежнему или нет, и единственный способ освободить какие-либо ресурсы - использование устаревания записей.

HOLD Time (Время удержания)

Этот параметр применяется к следующим режимам работы NAS:

- ✓ Single 802.1X
- ✓ Multi 802.1X
- ✓ MAC-Based Auth.

Если клиенту отказано в доступе - либо из-за того, что сервер RADIUS отказывает в доступе к клиенту, либо из-за истечения времени ожидания запроса к серверу RADIUS (в соответствии с таймаутом, указанным на странице «Configuration→Security→AAA»), - клиент переходит в состояние «Unauthorized». Таймер удержания не учитывается во время текущей аутентификации.

Для портов на основе MAC адресной аутентификации – в этом режиме коммутатор будет игнорировать новые фреймы, поступающие от клиента во время удержания.

Время удержания может быть установлено в диапазоне от 10 до 1000000 сек.

RADIUS-Assigned QoS Enabled

RADIUS-Assigned QoS представляет собой инструмент для управления трафиком. Сервер RADIUS должен быть настроен на передачу специальных атрибутов RADIUS, чтобы воспользоваться преимуществами этой функции.

Флаг «RADIUS-Assigned QoS Enabled» предоставляет быстрый способ глобально включить / отключить RADIUS-Assigned QoS. Если этот флаг установлен, то настройки отдельных портов контролируют,

включен ли RADIUS-Assigned QoS для этого порта. Если этот флаг не установлен, RADIUS-Assigned QoS отключен на всех портах.

RADIUS-Assigned VLAN Enabled

RADIUS-Assigned VLAN представляет собой инструмент для централизованного управления VLAN, в которой закреплен клиент, успешно завершивший процесс аутентификации.

Сервер RADIUS должен быть настроен на передачу специальных атрибутов RADIUS, чтобы воспользоваться преимуществами этой функции.

Флаг «RADIUS-Assigned VLAN Enabled» предоставляет быстрый способ глобально включить / отключить RADIUS-Assigned VLAN. Если этот флаг установлен, то настройки отдельных портов контролируют, включен ли RADIUS-Assigned VLAN для этого порта. Если этот флаг не установлен, RADIUS-Assigned VLAN отключен на всех портах.

Guest VLAN Enabled

Guest VLAN – это специальная VLAN, обычно с ограниченным доступом к сети, в которой размещаются клиенты не прошедшие аутентификацию 802.1x. Коммутатор соблюдает ряд правил для того чтобы работать с гостевой VLAN.

Флаг « Guest VLAN Enabled » предоставляет быстрый способ глобально включить / отключить Guest VLAN. Если этот флаг установлен, то настройки отдельных портов контролируют, включена ли Guest VLAN для этого порта. Если этот флаг не установлен, Guest VLAN отключена на всех портах.

Guest VLAN ID

Это значение является идентификатором VLAN порта, который был перемещен в гостевую VLAN. Допустимые значения 1 – 4096.

Max. Reauth. Count (Счетчик повторных процессов аутентификации)

Количество раз, когда коммутатор передает фрейм с идентификатором запроса EAPOL без ответа, прежде чем перекинуть порт в гостевую VLAN, регулируется этим параметром. Диапазон возможных значений 1 - 255

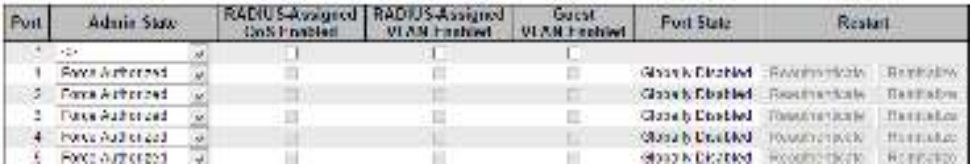
Allow Guest VLAN if EAPOL Seen

Коммутатор запоминает, был ли принят фрейм EAPOL на порт в течение срока жизни порта. Как только коммутатор решит, помещать ли порт в гостевую VLAN, он сначала проверит, включена или отключена эта опция.

Если этот параметр отключен (не отмечен; по умолчанию), коммутатор будет помещать порт в гостевую VLAN, только если фрейм EAPOL не был получен на порте в течение срока жизни порта.

Если этот параметр включен (отмечен флажком), коммутатор будет рассматривать возможность входа в гостевую VLAN, даже если на порт получен фрейм EAPOL в течение срока жизни порта.

Значение может быть изменено только в том случае, если опция Guest VLAN включена глобально.



Настройка портов.

Port (Порт)

Номер порта, к которому будут применены настройки.

Admin State

Если NAS включен глобльно, этот параметр управляет режимом аутентификации порта. Доступны следующие режимы:

- ✓ Force Authorized – В этом режиме коммутатор отправит один фрейм EAPOL Success, когда будет установлена связь с портом, и любому клиенту на порте будет разрешен доступ к сети без аутентификации.
- ✓ Force Unauthorized – В этом режиме коммутатор отправит один фрейм EAPOL Failure, когда появится соединение с портом, и любому клиенту на порту будет запрещен доступ к сети.
- ✓ Port-based 802.1X – В этом режиме аутентификация проводится с помощью серверов проверки подлинности RADIUS. Фреймы,

передаваемые между соискателем и коммутатором, представляют собой специальные фреймы 802.1X, известные как фреймы EAPOL (EAP Over LANs). Фреймы EAPOL инкапсулируют блоки EAP PDU (RFC3748). Фреймы, передаваемые между коммутатором и сервером RADIUS, являются пакетами RADIUS. Пакеты RADIUS также инкапсулируют блоки EAP PDU вместе с другими атрибутами, такими как IP-адрес коммутатора, имя и номер порта соискателя на коммутаторе. EAP очень гибок в том, что он допускает различные методы аутентификации, такие как MD5-Challenge, PEAP и TLS. Когда аутентификация завершена, сервер RADIUS отправляет специальный пакет, содержащий указание об успешном или неудачном завершении.

- ✓ Single 802.1X – В аутентификации 802.1X на базе портов, после того, как клиент-соискатель успешно аутентифицирован на порту, весь порт открывается для сетевого трафика. Это позволяет другим клиентам, подключенным к порту (например, через концентратор), подключиться к успешно аутентифицированному клиенту и получить доступ к сети, даже если они действительно не аутентифицированы. Чтобы преодолеть это нарушение безопасности, используйте режим Single 802.1X.
- ✓ Multi 802.1X – В Multi 802.1X один или несколько клиентов - соискателей могут проходить аутентификацию на одном и том же порту одновременно. Каждый клиент-соискатель аутентифицируется индивидуально и попадает в таблицу MAC адресов с использованием модуля безопасности порта. В Multi 802.1X невозможно использовать MAC-адрес BPDU multicast рассылки в качестве MAC-адреса назначения для фреймов EAPOL, отправляемых от коммутатора к клиенту-соискателю, так как это приведет к тому, что все клиенты-соискатели, подключенные к порту, будут отвечать на запросы, отправленные от коммутатора. Вместо этого коммутатор использует MAC-адрес запрашивающей стороны, который получен из первого фреймов EAPOL Start или EAPOL Response Identity, отправленного запрашивающей стороной.
- ✓ MAC-based Auth – аутентификация на базе MAC адресов не является стандартом в отличие от 802.1x. Данный режим

является отличной альтернативой. При аутентификации на основе MAC-адреса пользователи называются клиентами, а коммутатор выступает в качестве соискателя от имени клиентов. Начальный фрейм (любой тип фрейма), отправленный клиентом, отслеживается коммутатором, который, в свою очередь, использует MAC-адрес клиента в качестве имени пользователя и пароля в последующем обмене EAP с сервером RADIUS. 6-байтовый MAC-адрес преобразуется в строку в следующей форме «xx-xx-xx-xx-xx-xx», то есть тире (-) используется в качестве разделителя между шестнадцатеричными цифрами в нижнем регистре. Коммутатор поддерживает только метод аутентификации MD5-Challenge, поэтому сервер RADIUS должен быть настроен соответствующим образом. Преимущество аутентификации на основе MAC-адресов по сравнению с аутентификацией на основе 802.1X заключается в том, что клиентам не требуется специальное программное обеспечение для проверки подлинности. Недостатком является то, что MAC-адреса могут быть подменены злоумышленниками.

RADIUS-Assigned QoS Enabled

RADIUS-Assigned QoS представляет собой инструмент для управления трафиком. Сервер RADIUS должен быть настроен на передачу специальных атрибутов RADIUS, чтобы воспользоваться преимуществами этой функции.

RADIUS-Assigned VLAN Enabled

RADIUS-Assigned VLAN представляет собой инструмент для централизованного управления VLAN, в которой закреплен клиент, успешно завершивший процесс аутентификации.

Сервер RADIUS должен быть настроен на передачу специальных атрибутов RADIUS, чтобы воспользоваться преимуществами этой функции.

Guest VLAN Enabled

Guest VLAN – это специальная VLAN, обычно с ограниченным доступом к сети, в которой размещаются клиенты не прошедшие аутентификацию

802.1x. Коммутатор соблюдает ряд правил для того чтобы работать с гостевой VLAN.

Port State

Текущее состояние порта. Может принимать одно из следующих значений:

- ✓ Globally Disabled – NAS полностью отключен;
- ✓ Link Down – NAS включен, но нет соединения на порте;
- ✓ Authorized – Порт прошел авторизацию;
- ✓ Unauthorized – Порт не авторизован;
- ✓ X Auth / Y Unauth – Порт работает в режиме мульти-авторизации, где X – количество авторизованных клиентов, а Y – количество неавторизованных клиентов.

Restart

- ✓ Re-authenticate – нажатие кнопки приведет к повторной аутентификации (на основе EAPOL). На основе MAC адреса повторная аутентификация будет принята немедленно.
- ✓ Reinitialize – нажатие кнопки приведет к повторной инициализации клиентов на порте и, следовательно, немедленную повторную аутентификацию. Клиенты перейдут в неавторизованное состояние во время повторной аутентификации.

Кнопки

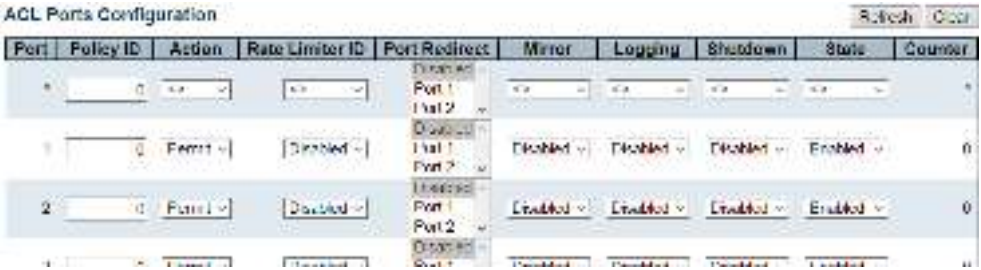
Add New Entry (Добавить новую запись). Нажмите, чтобы добавить новую запись.

Save (Сохранить). Нажмите для сохранения изменений

Reset (Сбросить). Нажмите, чтобы отменить изменения и вернуть их к предыдущим сохраненным значениям.

10.5.11 Security–Network–ACL (Безопасность–Сеть–ACL)

10.5.11.1 ACL–Ports (ACL – Порты)



На данной странице WEB интерфейса представлены настройки Access Control List (список разрешенных/запрещенных действий) для каждого порта.

Port (Порт)
Настройки будут применены для этого порта

Policy ID (идентификатор выбранной политики)
Выберите идентификатор политики ACL, которая будет применена к порту. Допустимые значения 0 – 255. Значение по умолчанию 0.

Action (действие)
Выбор действия – разрешена ли пересылка («Permit») или запрещена («Deny»). Значением по умолчанию является «Permit».

Rate Limiter ID (идентификатор ограничителя скорости)
Выбор ограничителя скорости. Доступные значения 1 – 16. Доступные значения 1 – 16. Значение по умолчанию – отключено (disabled).

Port Redirect (Перенаправление портов)
Выбор порта, пакеты на который будут перенаправлены. Значение по умолчанию – отключено (disabled).

Mirror (зеркалирование)
Зеркалирование трафика порта на выбранный порт. Доступные значения:

- ✓ Enabled – пакеты полученные на порт зеркалируются;
- ✓ Disabled – пакеты полученные на порт не зеркалируются.

Значение по умолчанию – зеркалирование отключено (disabled).

Logging (учет в журнале)
Настройка отвечает за учет принятых пакетов в системном журнале. Доступные значения:

- ✓ Enabled – пакеты полученные на порт учитываются в системном журнале;
- ✓ Disabled – пакеты полученные на порт не учитываются в системном журнале.

Значение по умолчанию – учет в журнале отключен (disabled).

Shutdown (Отключение порта)
Настройка отвечает за полное отключение порта при приеме пакета на порт. Доступны значения:

- ✓ Enabled – пакеты полученные на порт отключают порт;
- ✓ Disabled – функция отключения порта при получении пакета отключена.

Значение по умолчанию – функция отключения порта при получении пакета отключена (disabled).

State (состояние порта)
Настройка отвечает за изменение состояния порта при получении пакета. Доступные значения:

- ✓ Enabled – включено повторное открытие портов при изменении настройки модуля ACL;
- ✓ Disabled – закрытие портов при изменении настройки модуля ACL.

Значение по умолчанию – включено повторное открытие портов при изменении настройки модуля ACL (enabled).

Counter (счетчик)
Счетчик количества пакетов, совпадающих с описанными в списке ACL.

Кнопки:
Save – сохранить изменения.

Reset – отменить изменения, вернуть к первоначальным параметрам.

Refresh – обновить страницу. Изменения автоматически отменяются.

Clear – очистить все счетчики.

10.5.11.2 ACL–Rate Limiter (ACL – Ограничитель скорости)

На данной странице WEB интерфейса представлены настройки ограничителя скорости портов (rate limiter).

Rate Limiter ID (идентификатор ограничителя скорости)
Идентификатор ограничителя скорости, настройки которого находятся в той же строке.

Rate (Скорость передачи данных)
Доступные значения 0 – 131071 пакетов/сек.

Unit (единицы измерения)
- ✓ pps – пакетов/сек;
- ✓ kbps – килобит/сек.

Кнопки:
Save – сохранить изменения.

Reset – отменить изменения, вернуть к первоначальным параметрам.

10.5.11.3 ACL–Access Control List

На данной странице WEB интерфейса представлен список контроля доступа (ACL), который состоит из ACE, определенных для данного коммутатора.

Ingress Port (Входной порт)
Настройки входящего порта ACE. Допустимые значения:
- ✓ All – ACE будет соответствовать всем входным портам;
- ✓ Port – ACE будет соответствовать только особым входным портам.

Policy / Bitmask (Политика / битовая маска)

Поле отображает, номер политики и битовую маску ACE. Доступные значения:
- ✓ Any – ACE будет соответствовать любым типам пакетов;
- ✓ Etype – ACE будет соответствовать Ethernert типу пакетов;
- ✓ ARP – ACE будет соответствовать ARP/RARP пакетам;
- ✓ IPv4 – ACE будет соответствовать IPv4 пакетам;

- ✓ IPv4/ICMP – ACE будет соответствовать IPv4 пакетам с ICMP протоколом;
- ✓ IPv4/UDP – ACE будет соответствовать IPv4 пакетам с UDP протоколом
- ✓ IPv4/TCP – ACE будет соответствовать IPv4 пакетам с TCP протоколом
- ✓ IPv4/Other – ACE будет соответствовать IPv4 пакетам, не использующим ICMP/UDP/TCP протоколы;
- ✓ IPv6 – ACE будет соответствовать IPv6 стандартным пакетам.

Action (Действие)
Поле определяет действие – пакеты соответствующие ACE будут запомнены и переадресованы («Permit») или пакеты соответствующие ACE будут отброшены («Deny»).

Rate Limiter (Ограничитель скорости)
Доступные значения 1 – 16. Когда отображается «Отключено» (Disabled), операции по ограничению скорости отключены.

Port Redirect (Перенаправление на порт)
Поле отображает операции по перенаправлению пакетов на порт. Пакеты, соответствующие ACE перенаправляются на выбранный порт. Доступные значения – отключено (disabled) или номер выбранного порта.

Counter (счетчик)
Счетчик отображает количество соответствующих ACE пакетов принятых коммутатором.

Кнопки для управления:
Помещает новый ACE перед текущей строкой;
Редактирование текущей ACE строки;
Помещает ACE наверх списка;
Помещает ACE вниз списка;
Удаление ACE;
Добавление новой записи ACE в нижней части списка.

Кнопки:

Auto Refresh – автоматическое обновление списка каждые 3 секунды;

Refresh – обновление страницы. Любые изменения сделанные локально не будут сохранены;

Clear – очистить все счетчики;

Remove all – Удалить все ACE из списка.

На данной страниц WEB интерфейса представлены настройки ACE (записи в таблице контроля доступа ACL).

ACE состоит из нескольких параметров. Эти параметры зависят от выбранных типа пакетов. Первый выбор – выбор входящего порта. Второй определяет тип пакетов.

Ingress Port (Входящий порт)
Выбор входящего порта, к которому будет применена ACE.

- ✓ ALL – ACE применяется ко всем портам;
- ✓ Port # – номер порта к которому будет применена ACE.

Policy Filter (Фильтр политик)

- ✓ Any – фильтр особых политик для ACE не применяется;
- ✓ Specific – Если есть необходимость отфильтровать определенную политику с этим ACE, выберите это значение. Появятся два поля для ввода значения политики и битовой маски.

Policy Value (Значение политики)
Когда для фильтра политики выбрано «Specific», вы можете ввести определенное значение политики. Допустимый диапазон от 0 до 255.

Policy Bitmask (Битовая маска политики)
Когда для фильтра политики выбрано «Specific», вы можете ввести определенное значение битовой маски политики. Допустимый диапазон 0x0 – 0xff

Switch (Выбор коммутатора)
Выбор коммутатора к которому будет применена ACE.
Any – ACE применяется к любому порту;
Switch in – ACE применяется к указанному коммутатору.

Frame Type (Тип пакетов)
Выбор типа пакетов для данной ACE.

- ✓ Any – Любой пакет может соответствовать ACE;
- ✓ Ethernet Type – только пакеты, определенные стандартом IEEE 802.3 могут соответствовать ACE;
- ✓ ARP – только пакеты ARP могут соответствовать ACE;
- ✓ IPv4 – только пакеты IPv4 могут соответствовать ACE;
- ✓ IPv6 – только пакеты IPv6 могут соответствовать ACE.

Action (Действие)

- ✓ Permit – пакет, соответствующий ACE будет обработан согласно ACE операции, прописанной также в этой записи;
- ✓ Deny – пакет соответствующий ACE будет отброшен.

Rate Limiter (Ограничитель скорости)
Ограничитель скорости, основанный на выбранных единицах измерения (пакетов/сек, кбит/сек). Доступные значения 1 – 16.

Port redirect (Перенаправление пакетов на порт)
Поле отображает операции по перенаправлению пакетов на порт. Пакеты, соответствующие ACE перенаправляются на выбранный порт. Доступные значения – отключено (disabled) или номер выбранного порта.

Logging (учет в журнале)
Настройка отвечает за учет принятых пакетов в системном журнале. Доступные значения:

- ✓ Enabled – пакеты полученные на порт учитываются в системном журнале;
- ✓ Disabled – пакеты полученные на порт не учитываются в системном журнале.

Значение по умолчанию – учет в журнале отключен (disabled).

Shutdown (Отключение порта)
Настройка отвечает за полное отключение порта при приеме пакета на порт. Доступны значения:

- ✓ Enabled – пакеты полученные на порт отключают порт;
- ✓ Disabled – функция отключения порта при получении пакета отключена.

Значение по умолчанию – функция отключения порта при получении пакета отключена (disabled).

Counter (счетчик)
Счетчик отображает количество соответствующих ACE пакетов принятых коммутатором.

MAC Parameters

SMAC Filter	Specific
SMAC Value	00-00-00-00-00-01
DMAC Filter	Specific
DMAC Value	00-00-00-00-00-02

Параметры MAC адреса

SMAC Filter (Фильтр MAC адресов источника)
Отображается только, если выбран тип пакетов Ethernet Type или ARP
Укажите исходный фильтр MAC адресов для этого ACE.

- ✓ Any – Особый MAC фильтр для ACE не используется.
- ✓ Specific – если вы хотите создать особый MAC фильтр для ACE, выберите это значение. Появятся дополнительные SMAC поля.

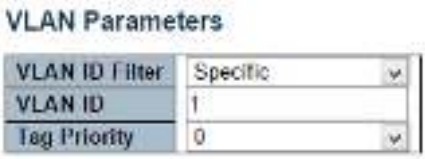
SMAC Value (значение SMAC)
Если выбран особый SMAC фильтр, то вы можете указать особый MAC адрес.

DMAC (Целевой Фильтр MAC адресов)

- ✓ Any – Особый Целевой MAC фильтр для ACE не используется;
- ✓ MC – пакеты должны быть типа multicast;
- ✓ BC – пакеты должны быть типа broadcast;
- ✓ UC – пакеты должны быть типа unicast;
- ✓ Specific – если вы хотите создать особый Целевой MAC фильтр для ACE, выберите это значение. Появятся дополнительные DMAC поля

DMAC Value (значение DMAC)

Если выбран особый Целевой DMAC фильтр, то вы можете указать особый MAC адрес.



Параметры VLAN

VLAN ID Filter (Фильтр VLAN ID)

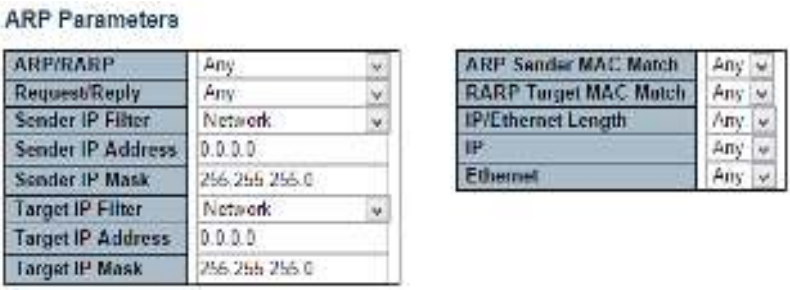
- ✓ Any – к ACE не применяется особый фильтр;
- ✓ Specific – если вы хотите создать особый фильтр VLAN ID для ACE укажите этот параметр.

VLAN ID

Если в поле VLAN ID Filter выбрано значение Specific, то это поле становится доступным. Диапазон значений 1 – 4095.

Tag Priority

Укажите приоритет тэга для этой ACE. Пакет, который попадет в эту ACE, соответствует приоритет этого тэга. Допустимый диапазон значений 0 – 7. Any означает, что приоритет не требуется.



ARP параметры.

ARP/RARP

Укажите доступный ARP/RARP код операции для выбранной ACE:

- ✓ ANY – особый код операции не указан;
- ✓ ARP – пакет должен содержать код операции ARP;
- ✓ RARP – пакет должен содержать код операции RARP;
- ✓ Other – пакет содержит неизвестный код операции ARP/RARP.

Request / Reply (Повторный запрос / повтор)

Укажите доступный код операции повторного запроса / повтора для ACE.

- ✓ Any – особый код операции повторного запроса / повтора не указан;
- ✓ Request – пакет должен содержать код операции ARP/RARP повторного запроса;
- ✓ Reply – пакет должен содержать код операции ARP/RARP повтора.

Sender IP Filter (Фильтр IP адреса отправителя)

- ✓ Any – фильтр IP адреса отправителя не указан;
- ✓ Host – фильтр IP адреса отправителя настроен как Host;
- ✓ Network – фильтр IP адреса отправителя настроен как Network.

Sender IP адрес (IP адрес отправителя)

Когда в поле Sender IP Filter выбрано значение Host или Network, это поле становится активным для редактирования. Укажите IP адрес через «.»

Sender IP Mask (маска IP адреса отправителя)
Когда в поле Sender IP Filter выбрано значение Host или Network, это поле становится активным для редактирования. Укажите маску IP адреса через «.»

Target IP Filter (Фильтр IP адреса получателя)
- ✓ Any – фильтр IP адреса получателя не указан;
- ✓ Host – фильтр IP адреса получателя настроен как Host;
- ✓ Network – фильтр IP адреса получателя настроен как Network.

Target IP адрес (IP адрес получателя)
Когда в поле Target IP Filter выбрано значение Host или Network, это поле становится активным для редактирования. Укажите IP адрес через «.»

Target IP Mask (маска IP адреса получателя)
Когда в поле Target IP Filter выбрано значение Host или Network, это поле становится активным для редактирования. Укажите маску IP адреса через «.»

ARP Sender MAC Match (Соответствие ARP отправителя с MAC адресом)
Укажите, могут ли фреймы выполнять действие в соответствии с настройками из поля MAC адреса отправителя (SHA):
- ✓ 0 – ARP фреймы, где SHA не совпадает с адресом SMAC;
- ✓ 1 – ARP фреймы, где SHA совпадает с SMAC адресом;
- ✓ Any – все значения разрешены.

IP/Ethernet Length (Параметры длины IP/Ethernet)
Укажите, могут ли фреймы выполнять действие в соответствии с настройками длины (HLN) ARP/RARP адреса и длины адреса протокола (PLN).
- ✓ 0 – ARP/RARP фреймы, где HLN не равен Ethernet (0x06) или PLN не равен IPv4 (0x04);
- ✓ 1 – ARP/RARP фреймы, где HLN равен Ethernet (0x06) или PLN равен IPv4 (0x04);
- ✓ Any – все значения разрешены.

IP (IP параметры)
Укажите, могут ли фреймы выполнять действие в соответствии с их настройками аппаратного адресного пространства (HRD) ARP/RARP

- ✓ 0 – ARP/RARP фреймы, где HRD не равен Ethernet (1);
- ✓ 1 – ARP/RARP фреймы, где HRD равен Ethernet (1);
- ✓ Any – все значения разрешены.

Ethernet (Ethernet параметры)
Укажите, могут ли фреймы выполнять действие в соответствии с их настройками адресного пространства протокола (PRO) ARP/RARP

- ✓ 0 – ARP/RARP фреймы, где PRO не равен IP (0x800);
- ✓ 1 – ARP/RARP фреймы, где PRO равен IP (0x800);
- ✓ Any – все значения разрешены.

IP Parameters

IP Protocol Filter	Other
IP Protocol Value	255
IP TTL	Any
IP Fragment	Any
IP Option	Any
SIP Filter	Network
SIP Address	0.0.0.0
SIP Mask	255.255.255.0
DIP Filter	Network
DIP Address	0.0.0.0
DIP Mask	255.255.255.0

IP параметры

Параметры IP можно настроить, если выбран тип кадра «IPv4»

IP Protocol Filter (Фильтр для IP протокола)
Укажите параметры фильтра IP протокола для ACE.

- ✓ Any – параметры для фильтра IP протокола не указаны;
- ✓ Specific – если вы хотите отфильтровать определенный фильтр протокола IP с этим ACE, выберите это значение. Появится поле для ввода фильтра протокола IP;

- ✓ ICMP – Выберите ICMP для фильтрации кадров протокола IPv4 ICMP. Появятся дополнительные поля для определения параметров ICMP;
- ✓ UDP – Выберите UDP для фильтрации кадров протокола IPv4 UDP. Появятся дополнительные поля для определения параметров UDP;
- ✓ TCP – Выберите TCP для фильтрации кадров протокола IPv4 TCP. Появятся дополнительные поля для определения параметров TCP.

IP Protocol Value (Значение IP протокола)
Если в качестве значения протокола IP выбрано «Specific», вы можете ввести определенное значение. Допустимый диапазон от 0 до 255. Фрейм, который попадает в этот ACE, соответствует этому значению протокола IP.

IP TTL (Параметры TTL для IP)
Укажите особые параметры TTL для ACE:
- ✓ Zero – IPv4 фреймы с TTL > 0 не должны соответствовать этой записи;
- ✓ Non-zero – IPv4 фреймы с TTL > 0 должны соответствовать этой записи;
- ✓ Any – все значения разрешены.

IP Fragment (Параметры фрагментов IP протокола)
Укажите настройки смещения фрагмента для этого ACE. Параметр включает в себя настройки для бита «More Fragments» (MF) и поля «Fragment offset» (FRAG OFFSET) для фрейма IPv4.
Кадры IPv4, в которых установлен бит MF или поле FRAG OFFSET больше нуля, не должны соответствовать этой записи.
- ✓ Yes – фреймы IPv4, в которых установлен бит MF или поле FRAG OFFSET больше нуля, должны соответствовать этой записи;
- ✓ Any – любые значения разрешены.

IP Option (Опциональные параметры IP протокола)
Укажите опциональные параметры для ACE.

- ✓ No – IPv4 фреймы, где флаг с дополнительными параметрами настроен, не должны соответствовать этой записи;
- ✓ Yes – IPv4 фреймы, где флаг с дополнительными параметрами настроен, должны соответствовать этой записи
- ✓ Any – любые значения разрешены.

SIP Filter (Параметры SIP фильтра)
Укажите исходный IP фильтр для ACE.

- ✓ Any – параметры фильтра не указаны;
- ✓ Host – Исходный IP фильтр настроен как Host. Укажите исходный IP-адрес в появившемся поле SIP-адрес.
- ✓ Network – Исходный IP фильтр настроен как Network. Укажите исходный IP-адрес и маску в появившемся поле SIP-адрес и SIP-маска.

SIP Address (SIP адрес)
Поле активно, если в SIP Filter выбрано значение Host или Network. Укажите SIP адрес с разделением через «.»

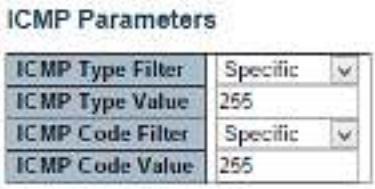
SIP Mask (SIP Маска)
Поле активно, если в SIP Filter выбрано значение Network. Укажите SIP маску с разделением через «.»

DIP Filter (Параметры DIP фильтра)
Укажите DIP фильтр для ACE.

- ✓ Any – параметры фильтра не указаны;
- ✓ Host – DIP фильтр настроен как Host. Укажите DIP-адрес в появившемся поле DIP-адрес.
- ✓ Network – DIP фильтр настроен как Network. Укажите DIP-адрес и маску в появившемся поле DIP-адрес и DIP-маска.

DIP Address (DIP Адрес)
Поле активно, если в DIP Filter выбрано значение Host или Network. Укажите DIP адрес с разделением через «.»

DIP Mask (DIP Маска)
Поле активно, если в DIP Filter выбрано значение Network. Укажите DIP маску с разделением через «.»



ICMP параметры

ICMP Type Filter (Тип фильтра ICMP)
Укажите тип ICMP фильтра для ACE.

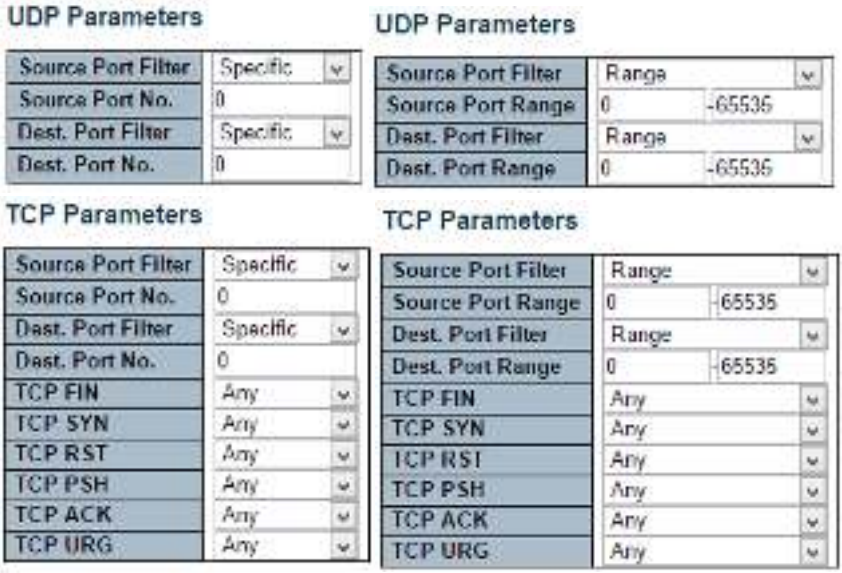
- ✓ Any – тип фильтра ICMP не задан;
- ✓ Specific – если вы хотите указать особый фильтр ICMP для ACE вы можете заполнить поле «ICMP Type Value». Поле станет активным, только если выбрано значение «Specific».

ICMP Type Value (Значение типа фильтра ICMP)
Если в поле «ICMP Type Filter» выбрано значение «Specific», то станет доступно для ввода данное поле. Допустимые значение 0 – 255. Фрейм, который попадает в ACE соответствует этому значению ICMP.

ICMP Code Filter (Фильтр кода ICMP)
Укажите Фильтр кода ICMP.

- ✓ Any – фильтр кода ICMP не задан;
- ✓ Specific – если вы хотите указать особый тип кода ICMP для ACE вы можете заполнить поле «ICMP Code Value». Поле станет активным, только если выбрано значение «Specific».

ICMP Code Value (Значение фильтра кода ICMP)
Если в поле «ICMP Code Filter» выбрано значение «Specific», то станет доступно для ввода данное поле. Допустимые значение 0 – 255. Фрейм, который попадает в ACE соответствует этому значению ICMP.



TCP/UDP параметры

TCP/UDP Source Filter (фильтр источника TCP/UDP)
Укажите TCP/UDP фильтр источник для этой ACE.

- ✓ Any – TCP/UDP фильтр источника не указан;
- ✓ Specific – если вы хотите отфильтровать определенный фильтр источника TCP/UDP с помощью этой ACE, вы можете ввести определенное значение источника TCP/UDP. Появится поле для ввода значения источника TCP/UDP;
- ✓ Range – если вы хотите отфильтровать определенный фильтр диапазона источника TCP/UDP с помощью этой ACE, вы можете ввести определенное значение диапазона источника TCP/UDP. Появится поле для ввода значения диапазона источника TCP/UDP.

TCP/UDP Source No.
Если для фильтра источника TCP/UDP выбран параметр «Specific», вы можете ввести конкретное значение источника TCP/UDP. Допустимый диапазон от 0 до 65535. Фрейм, который попадает в эту ACE, соответствует этому исходному значению TCP/UDP.

TCP/UDP Source Range

Если для фильтра источника TCP/UDP выбран «Range», вы можете ввести конкретное значение диапазона источника TCP/UDP. Допустимый диапазон от 0 до 65535. Кадр, который попадает в этот ACE, соответствует этому исходному значению TCP/UDP.

TCP/UDP Destination Filter (фильтр назначения TCP/UDP)

Укажите TCP/UDP фильтр назначения для этой ACE.

- ✓ Any – TCP/UDP фильтр назначения не указан;
- ✓ Specific – если вы хотите отфильтровать определенный фильтр назначения TCP/UDP с помощью этой ACE, вы можете ввести определенное значение назначения TCP/UDP. Появится поле для ввода значения TCP/UDP назначения;
- ✓ Range – если вы хотите отфильтровать определенный фильтр диапазона назначения TCP/UDP с помощью этой ACE, вы можете ввести определенное значение диапазона TCP/UDP назначения. Появится поле для ввода значения диапазона TCP/UDP назначения.

TCP/UDP Destination Number

Если для фильтра назначения TCP/UDP выбрано «Specific», вы можете ввести конкретное значение назначения TCP/UDP. Допустимый диапазон от 0 до 65535. Кадр, который попадает в этот ACE, соответствует этому значению TCP/UDP назначения.

TCP/UDP Destination Range

Если для фильтра назначения TCP/UDP выбран «Range», вы можете ввести конкретное значение диапазона назначения TCP/UDP. Допустимый диапазон от 0 до 65535. Кадр, который попадает в этот ACE, соответствует этому значению TCP/UDP назначения.

TCP FIN

Укажите для TCP Значение «Больше нет данных от отправителя» FIN для этой ACE.

- ✓ 0 – фреймы TCP, где значение FIN установлено, не должны соответствовать этой записи;
- ✓ 1 – фреймы TCP, где значение FIN установлено, должны соответствовать этой записи;

- ✓ Any – любые значения разрешены.

TCP SYN

Укажите для TCP Значение «Синхронизировать порядковые номера» SYN для этой ACE.

- ✓ 0 – фреймы TCP, где значение SYN установлено, не должны соответствовать этой записи;
- ✓ 1 – фреймы TCP, где значение SYN установлено, должны соответствовать этой записи;
- ✓ Any – любые значения разрешены.

TCP RST

Укажите для TCP Значение «Сбросить соединение» RST для этой ACE.

- ✓ 0 – фреймы TCP, где значение RST установлено, не должны соответствовать этой записи;
- ✓ 1 – фреймы TCP, где значение RST установлено, должны соответствовать этой записи;
- ✓ Any – любые значения разрешены.

TCP PSH

Укажите для TCP Значение «Функция PUSH» PSH для этой ACE.

- ✓ 0 – фреймы TCP, где значение PSH установлено, не должны соответствовать этой записи;
- ✓ 1 – фреймы TCP, где значение PSH установлено, должны соответствовать этой записи;
- ✓ Any – любые значения разрешены.

TCP ACK

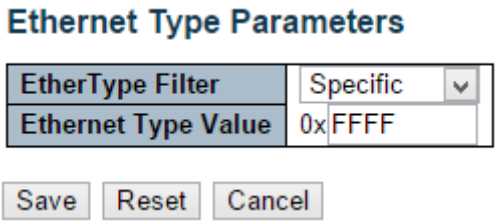
Укажите для TCP Значение «Значимое поле подтверждения» ACK для этой ACE.

- ✓ 0 – фреймы TCP, где значение ACK установлено, не должны соответствовать этой записи;
- ✓ 1 – фреймы TCP, где значение ACK установлено, должны соответствовать этой записи;
- ✓ Any – любые значения разрешены.

TCP URG

Укажите для TCP Значение URG для этой ACE.

- ✓ 0 – фреймы TCP, где значение URG установлено, не должны соответствовать этой записи;
- ✓ 1 – фреймы TCP, где значение URG установлено, должны соответствовать этой записи;
- ✓ Any – любые значения разрешены.



Ethernet Type параметры

Параметры Ethernet можно настроить, если выбран тип фрейма «Type Ethernet»

Ethernet Type Filter (Фильтр Ethernet)

Укажите фильтр Ethernet для этой ACE.

- ✓ Any – не указан фильтр для Ethernet;
- ✓ Specific – если вы хотите отфильтровать особое значение «Ethernet Type Filter» для этой ACE, укажите особое значение в поле «Ethernet Type Value».

Ethernet Type Value

Когда для фильтра Ethernet выбрано «Specific», вы можете ввести конкретное значение. Допустимый диапазон от 0x600 до 0xFFFF, исключая 0x800 (IPv4), 0x806 (ARP) и 0x86DD (IPv6). Фрейм, который попадает в эту ACE, соответствует этому значению Ethernet.

Кнопки:

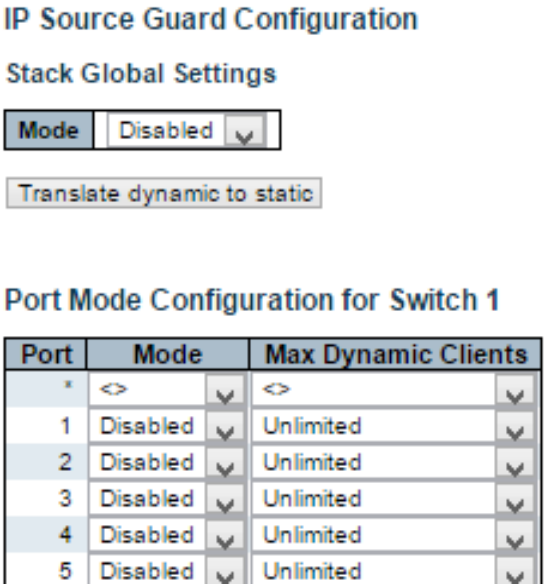
Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения и вернуть их к первоначальным значениям;

Cancel – Вернуться на предыдущую страницу.

10.5.12 Security – Network – IP Source Guard (Безопасность – Сеть – IP Source Guard)

10.5.12.1 IP Source Guard – Configuration (IP Source Guard – Настройки)



Настройки на этой странице WEB интерфейса позволяют настроить функцию IP Source Guard.

Mode of IP Source Guard Configuration (Выбор режима работы функции IP Source Guard)
Включите (enable) или выключите (disable) глобально функцию IP Source Guard. Все настроенные ACE будут утеряны при активации функции.

Port Mode Configuration (Настройка режима работы портов)
Укажите порты, для которых будет настроена функция IP Source Guard. Только при условии, что IP Source Guard включен глобально, а также выбран для конкретного порта, функция будет активирована.

Max Dynamic Clients (Максимальное количество динамических клиентов)
Укажите максимальное количество динамических клиентов, которые могут быть изучены (learned) на данном порту. Это значение может быть 0, 1, 2 или неограниченным. Если режим порта включен, а значение **Max Dynamic Clients** равно 0, это означает, что разрешена только пересылка IP-пакетов, которые совпадают в статических записях на конкретном порте.

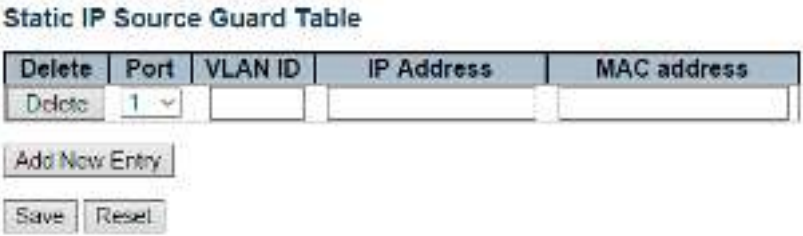
Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения и вернуть их к первоначальным значениям;

Translate Dynamic to Static – нажмите, чтобы перевести все динамические записи в статические.

10.5.12.2 IP Source Guard – Static Table (IP Source Guard – Таблица статичных записей функции IP Source Guard)



Delete (Удалить)
Отметьте, чтобы удалить запись. Запись будет удалена при следующем сохранении (кнопка save).

Port (Номер порта)
Выберите порт, чтобы применить к нему дальнейшие настройки.

VLAN ID
Идентификатор VLAN для настроек.

IP Address (IP адрес)
Разрешенный IP адрес источника.

MAC Address (MAC адрес)
Разрешенный MAC адрес источника.

Кнопки:

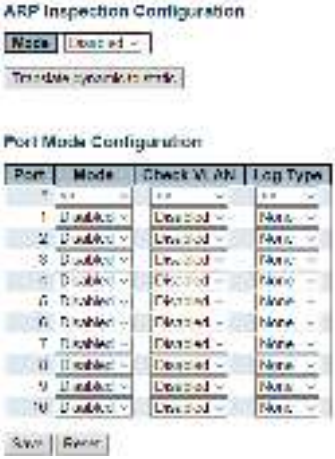
Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения и вернуть их к первоначальным значениям;

Add New Entry – нажмите, чтобы добавить новую запись в таблицу функции IP Source Guard

10.5.13 Security – Network – ARP Inspection (Безопасность – Сеть – ARP Inspection)

10.5.13.1 ARP Inspection – Port Configuration (ARP Inspection – Настройка портов)



На данной странице WEB интерфейса представлены настройки функции ARP Inspection (Проверка ARP).

Mode (Режим работы)
Включите (enable) или выключите (disable) глобально функцию ARP Inspection.

Port Mode Configuration (Настройка режима работы портов)
Укажите, на каких портах включена функция ARP Inspection. Только когда функция ARP Inspection включена глобально, а также для выбранного порта, ARP Inspection включается на этом порте. Возможные режимы:

- ✓ Enabled – включены операции по проверке ARP;
- ✓ Disabled – функция ARP Inspection отключена на выбранном порте.

Если вы хотите включить ARP Inspection для VLAN, вам нужно включить настройку «Check VLAN». Настройка по умолчанию «Check VLAN» отключена.

Когда настройка «Check VLAN» отключена, тип журнала ARP Inspection будет ссылаться на настройку порта.

Если настройка «Check VLAN» включена, тип журнала проверки ARP будет ссылаться на настройку VLAN. Доступные настройки «Check VLAN»:

- ✓ Enabled – включена опция «Check VLAN»;
- ✓ Disabled – опция «Check VLAN» отключена.

На данном порту включены Mode (глобальное включение ARP Inspection) и Port Mode (включение ARP Inspection на выбранном порте), а параметр «Check VLAN» отключен.

Тип журнала проверки ARP будет соответствовать настройке порта. Есть четыре типа журнала:

- ✓ None – Журнал не ведется;
- ✓ Deny – Записывать только запрещающие записи;
- ✓ Permit – Записывать только разрешающие записи;
- ✓ ALL – Записывать все записи.

Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения и вернуть их к первоначальным значениям;

Translate Dynamic to Static – нажмите, чтобы перевести все динамические записи в статические.

10.5.13.2 ARP Inspection – VLAN Configuration (ARP Inspection – Настройка VLAN)

На этой странице WEB интерфейса представлены настройки функции ARP Inspection (Проверка ARP) для VLAN.

Navigating the VLAN Configuration (Навигация по настройкам VLAN)
На каждой странице отображается до 9999 записей из таблицы VLAN, по умолчанию 20, выбираемых через поле ввода «записей на страницу».

При первом посещении веб-страницы будут отображаться первые 20 записей в начале таблицы VLAN. Первым будет отображаться та запись, у которой найден самый низкий VLAN ID в таблице VLAN.

Поля ввода «VLAN» позволяют пользователю выбрать начальную точку в таблице VLAN. Нажатие кнопки «Refresh» (Обновить) обновит отображаемую таблицу, начиная с этого или ближайшего следующего соответствия таблицы VLAN.

Кнопка >> будет использовать следующую запись текущей отображаемой записи VLAN в качестве основы для следующего поиска.

Когда достигнут конец таблицы, предупреждающее сообщение отображается в отображаемой таблице. Используйте кнопку <<, чтобы начать просмотр настроек сначала.

VLAN Mode Configuration (Настройка режима работы VLAN)
Укажите, что проверка ARP (ARP Inspection) включена на выбранных VLAN.

Во-первых, вы должны включить настройку порта на веб-странице конфигурации режима порта. Только когда функция ARP Inspection включена глобально, а также для выбранного порта, ARP Inspection включается на этом порте.

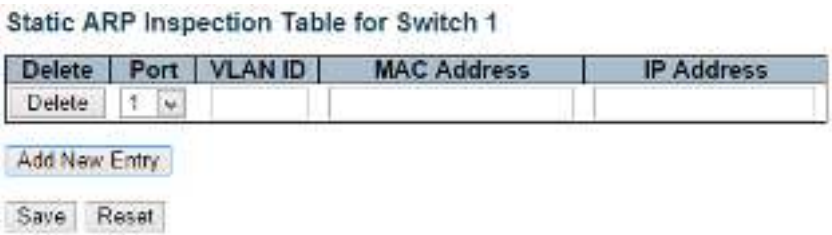
Во-вторых, вы можете указать, какая VLAN будет проверяться на веб-странице конфигурации режима VLAN. Тип журнала также может быть настроен для каждой настройки VLAN.

- ✓ None – Журнал не ведется;
- ✓ Deny – Записывать только запрещающие записи;
- ✓ Permit – Записывать только разрешающие записи;
- ✓ ALL – Записывать все записи.

Кнопки:

Save – нажмите, чтобы сохранить изменения;
Reset – нажмите, чтобы отменить изменения и вернуть их к первоначальным значениям;
Add New Entry – нажмите, чтобы перевести все динамические записи в статические.

10.5.13.3 ARP Inspection – Static Table (ARP Inspection – Таблица статичных записей функции ARP Inspection)



Delete (Удалить)
Отметьте, чтобы удалить запись. Запись будет удалена при следующем сохранении (кнопка save).

Port (Номер порта)
Выберите порт, чтобы применить к нему дальнейшие настройки.

VLAN ID
Идентификатор VLAN для настроек.

IP Address (IP адрес)
Разрешенный IP адрес источника.

MAC Address (MAC адрес)
Разрешенный MAC адрес источника.

Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения и вернуть их к первоначальным значениям;

Add New Entry – нажмите, чтобы добавить новую запись в таблицу функции IP Source Guard

10.5.13.4 ARP Inspection – Dynamic Table (ARP Inspection – Таблица динамических записей функции ARP Inspection)

Записи в динамической таблице проверки ARP (ARP Inspection) показаны на этой WEB странице. Динамическая таблица проверки ARP

содержит до 1024 записей и сортируется сначала по порту, затем по идентификатору VLAN, затем по MAC-адресу и затем по IP-адресу.

Navigating the ARP Inspection Table (Навигация по таблице ARP Inspection)
На каждой странице отображается до 99 записей из таблицы Dynamic ARP Inspection, по умолчанию 20, выбираемых через поле ввода «записей на страницу».

При первом посещении веб-страницы будут отображаться первые 20 записей с начала таблицы проверки динамического ARP.

Поля ввода «Start from port address», «VLAN», «MAC address» и «IP-address» позволяют пользователю выбрать начальную точку в динамической таблице проверки ARP.

Нажатие кнопки «Refresh» (Обновить) обновит отображаемую таблицу, начиная с этого или ближайшего следующего совпадения с динамической таблицей ARP Inspection.

Кроме того, два поля ввода - при нажатии кнопки «Auto - Refresh» - предполагают значение первой отображаемой записи, что позволяет осуществлять непрерывное обновление с одним и тем же начальным адресом.

Кнопка >> будет использовать последнюю запись отображаемой в данный момент таблицы в качестве основы для следующего поиска.

Когда достигнут конец, в отображаемой таблице появится текст «No more entries» (Больше нет записей).

Используйте кнопку <<, чтобы начать просмотр настроек сначала.

Столбцы и строки динамической таблицы ARP Inspection

Port (Порт)
Номер порта коммутатора для которого отображаются записи

VLAN ID (Идентификатор VLAN)
Идентификатор VLAN, в которой разрешен трафик ARP.

MAC Address (MAC Адрес)
MAC адрес пользователя записи.

IP Address (IP Адрес)
IP адрес пользователя записи.

Translate to static (Перевести в статические значения)
Отметьте этот чекбокс, если хотите перевести запись в статическую.

Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения и вернуть их к первоначальным значениям;

Auto-refresh – Установите этот чекбокс, чтобы обновлять страницу автоматически. Автоматическое обновление происходит каждые 3 секунды.

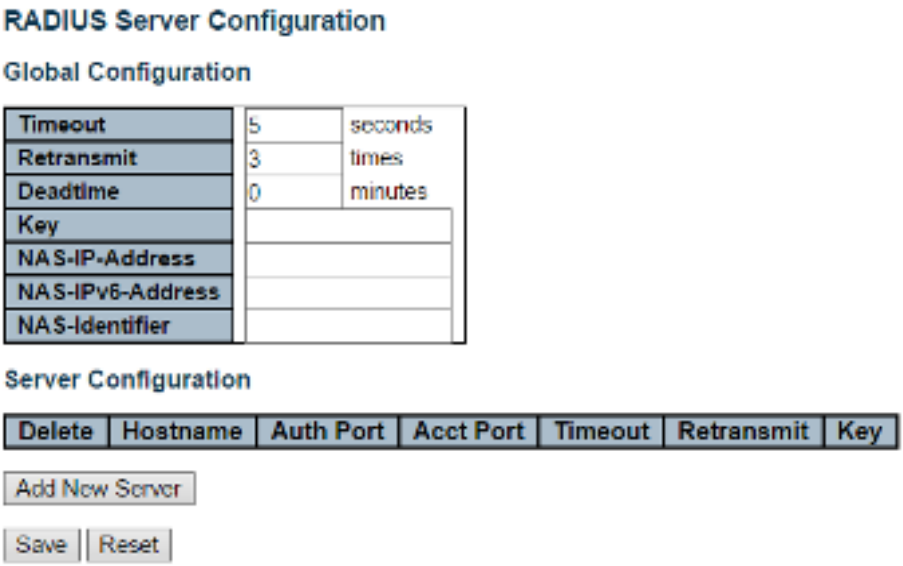
Refresh – Обновляет отображаемую таблицу, начиная с полей ввода.

<< – Обновляет таблицу, начиная с первой записи в таблице проверки динамического ARP.

>> – Обновляет таблицу, начиная с записи после последней отображаемой записи.

10.5.14 Security – AAA (Безопасность – AAA)

10.5.14.1 Security – AAA – RADIUS (Безопасность – AAA – Настройки RADIUS)



На данной странице WEB интерфейса представлены настройки RADIUS серверов.

Глобальные настройки

Timeout (Таймаут)
Тайм-аут - это количество секунд в диапазоне от 1 до 1000 для ожидания ответа от сервера RADIUS перед повторной передачей запроса.

Retransmit (Повторная передача)
Повторная передача - это количество раз, в диапазоне от 1 до 1000, запрос RADIUS повторно передается на сервер, который не отвечает. Если сервер не ответил после последней повторной передачи, он считается неактивным (dead).

Deadtime (Время простоя)
Время простоя, которое может быть установлено в диапазоне от 0 до 1440 минут, представляет собой период, в течение которого коммутатор не будет отправлять новые запросы на сервер, который не смог ответить на предыдущий запрос.

Это не позволит коммутатору постоянно пытаться связаться с сервером, который уже определен как неактивный (dead).

Установка для Deadtime значения больше 0 активирует эту функцию, но только если был настроены хотя бы 2 и более серверов.

Key (Ключ)
Секретный ключ длиной до 63 символов используется совместно между сервером RADIUS и коммутатором.

NAS-IP-Address (Attribute 4)
Адрес IPv4, который будет использоваться в качестве атрибута 4 в пакетах запроса доступа RADIUS. Если это поле оставить пустым, используется IP-адрес исходящего интерфейса.

NAS-IPv6-Address (Attribute 95)
Адрес IPv6, который будет использоваться в качестве атрибута 95 в пакетах запроса доступа RADIUS. Если это поле оставить пустым, используется IP-адрес исходящего интерфейса.

NAS-Identifier (Attribute 32)
Идентификатор - длиной до 253 символов - для использования в качестве атрибута 32 в пакетах запроса доступа RADIUS. Если это поле оставить пустым, идентификатор NAS не включается в пакет.

Настройки сервера

В таблице настроек есть одна строка для каждого сервера RADIUS и несколько столбцов:

Delete (Удалить)
Чтобы удалить запись сервера RADIUS, установите этот флаг. Запись будет удалена при следующем сохранении.

Hostname (Имя Хоста)
IP-адрес или имя хоста сервера RADIUS

Auth Port (Порт для аутентификации)
Порт UDP для использования на сервере RADIUS для аутентификации

Acct Port (Порт для учета)
Порт UDP для использования на сервере RADIUS для учета

Timeout (Таймаут)
Этот необязательный параметр переопределяет значение глобального тайм-аута. Если оставить это поле пустым, будет использоваться значение глобального тайм-аута.

Retransmit (Повторная передача)
Этот необязательный параметр переопределяет глобальное значение повторной передачи. Если оставить это поле пустым, будет использоваться глобальное значение повторной передачи.

Key (Ключ)
Этот необязательный параметр переопределяет глобальный ключ. Если оставить это поле пустым, будет использован глобальный ключ.

Добавление нового сервера

Нажмите кнопку «Добавить новый сервер» (Add new Server), чтобы добавить новый сервер RADIUS.

Пустая строка добавляется в таблицу, и сервер RADIUS может быть настроен по мере необходимости. Поддерживается до 5 серверов.

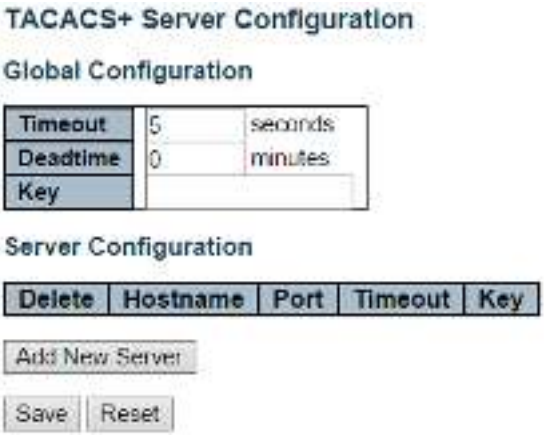
Кнопка «Удалить» (Delete) может использоваться для отмены добавления нового сервера.

Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения и вернуть их к первоначальным значениям;

10.5.14.2 Security – AAA – TACACS+ (Безопасность – AAA – Настройки TACACS+)



На данной странице WEB интерфейса представлены настройки TACACS+ серверов.

Глобальные настройки

Timeout (Тайм-аут)
Тайм-аут - это количество секунд в диапазоне от 1 до 1000 для ожидания ответа от сервера TACACS+ перед повторной передачей запроса.

Deadtime (Время простоя)
Время простоя, которое может быть установлено в диапазоне от 0 до 1440 минут, представляет собой период, в течение которого коммутатор не будет отправлять новые запросы на сервер, который не смог ответить на предыдущий запрос.

Это не позволит коммутатору постоянно пытаться связаться с сервером, который уже определен как неактивный (dead).

Установка для Deadtime значения больше 0 активирует эту функцию, но только если было настроено более одного сервера.

Key (Ключ)
Секретный ключ длиной до 63 символов используется совместно между сервером RADIUS и коммутатором.

Настройки сервера

Delete (Удалить)
Чтобы удалить запись сервера TACACS+, установите этот флаг. Запись будет удалена при следующем сохранении.

Hostname (Имя Хоста)
IP-адрес или имя хоста сервера TACACS+

Port (Порт для аутентификации)
Порт TCP для использования на сервере TACACS + для аутентификации.

Timeout (Таймаут)
Этот необязательный параметр переопределяет значение глобального тайм-аута. Если оставить это поле пустым, будет использоваться значение глобального тайм-аута.

Key (Ключ)
Этот необязательный параметр переопределяет глобальный ключ. Если оставить это поле пустым, будет использован глобальный ключ.

Добавление нового сервера

Нажмите кнопку «Добавить новый сервер» (Add new Server), чтобы добавить новый сервер TACACS+.

Пустая строка добавляется в таблицу, и сервер TACACS+ может быть настроен по мере необходимости. Поддерживается до 5 серверов.

Кнопка «Удалить» (Delete) может использоваться для отмены добавления нового сервера.

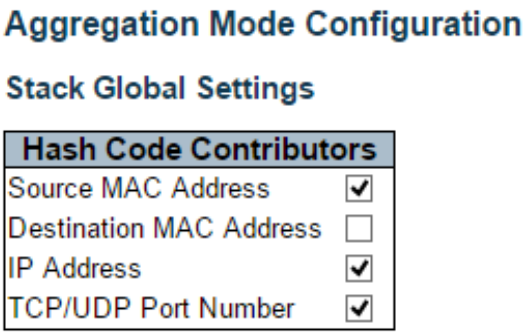
Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения и вернуть их к первоначальным значениям;

10.6 Configuration-Aggregation (Настройки - Агрегация)

10.6.1 Aggregation – Static



На данной странице WEB интерфейса представлены настройки Агрегации и групп агрегации.

Source MAC Address (Исходный MAC адрес)
Исходный MAC-адрес может использоваться для расчета порта назначения для фрейма. Установите флаг, чтобы включить использование исходного MAC-адреса, или снимите флаг, чтобы отключить. По умолчанию исходный MAC-адрес включен.

Destination MAC Address (MAC адрес назначения)
MAC-адрес назначения может использоваться для расчета порта назначения для фрейма. Установите флаг, чтобы включить использование MAC-адреса получателя, или снимите флаг, чтобы отключить его. По умолчанию MAC-адрес получателя отключен.

IP Address (IP Адрес)
IP-адрес может использоваться для расчета порта назначения для фрейма. Установите флаг, чтобы включить использование IP-адреса, или снимите флаг, чтобы отключить. По умолчанию IP-адрес включен.

TCP/UDP Port Number (Номер порта TCP/UDP)
Номер порта TCP/UDP можно использовать для расчета порта назначения для фрейма. Установите флаг, чтобы включить

использование номера порта TCP/UDP, или снимите флаг, чтобы отключить. По умолчанию номер порта TCP/UDP включен.

Настройка групп Агрегации

Locality (Местонахождение)
Настройка определяет тип группы агрегации. Это поле действительно только для стекируемых коммутаторов.

- ✓ Global – участники этой группы могут находиться в разных коммутаторах стека. Каждая global группа может состоять из 8 участников.
- ✓ Local – члены этой группы находятся в одном коммутаторе. Каждая local группа может состоять из 16 участников.

Group ID (Идентификатор Группы)
Определяет идентификатор группы для настроек, содержащихся в той же строке. Идентификатор группы «Normal» указывает на отсутствие агрегации. Только один идентификатор группы действителен для каждого порта.

Port Members (Порты участники)
Каждый порт коммутатора указан для каждого идентификатора группы. Отметьте точкой элемент, чтобы включить порт в агрегацию, или уберите точку, чтобы удалить порт из агрегации.

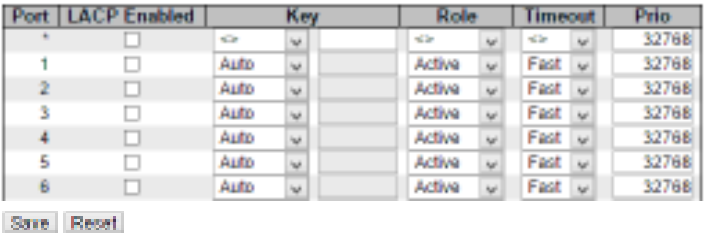
По умолчанию порты не принадлежат какой-либо группе агрегации. Только полнодуплексные порты могут участвовать в агрегации, кроме того, порты должны быть с одинаковой скоростью в каждой группе.

Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения и вернуть их к первоначальным значениям;

10.6.2 Aggregation – LACP (Агрегация – LACP)



На данной странице WEB интерфейса коммутатора представлены настройки для проверки конфигурации портов LACP. В случае необходимости конфигурацию можно изменить.

Настройки порта LACP относятся к выбранному в настоящий момент коммутатору в стеке, что отражено в заголовке страницы.

Port (Порт)
Номер порта коммутатора

LACP Enabled (LACP включен)
Элемент интерфейса управляет включением LACP на этом порту коммутатора. LACP будет производить агрегацию, когда 2 или более портов подключены к одному и тому же устройству. LACP может формировать максимум 12 LLAG на коммутатор и 2 GLAG на стек.

Key (Ключ)
Значение ключа, получаемое портом, находится в диапазоне 1-65535. Автоматическая настройка установит ключ в зависимости от скорости физической линии: 10 МБ = 1, 100 МБ = 2, 1 ГБ = 3.

Используя параметр «Specific», можно ввести значение, задаваемое пользователем. Порты с одинаковым значением ключа могут участвовать в одной группе агрегации, а порты с разными ключами - нет.

Role (Роль)
Роль показывает статус активности LACP. Active будет передавать пакеты LACP каждую секунду, в то время как Passive будет ожидать пакета LACP от устройства-партнера.

Timeout (Время ожидания)
Время ожидания контролирует период между передачами BPDU пакетов. Fast будет передавать пакеты LACP каждую секунду, а Slow будет ждать 30 секунд перед отправкой пакета LACP.

Prio (Приоритет)
Prio отвечает за приоритет порта.

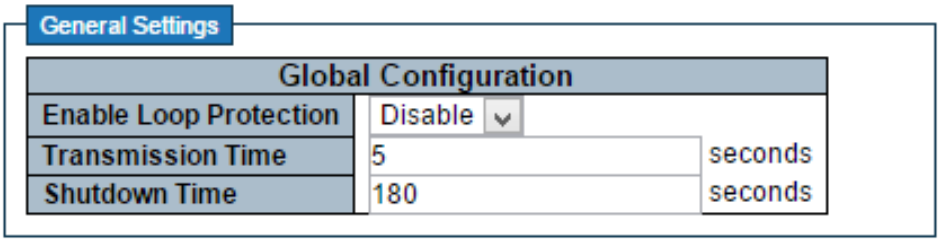
Если устройство-партнер LACP хочет сформировать большую группу, чем поддерживается этим устройством, то этот параметр будет определять, какие порты будут активными, а какие будут выполнять роль резервного копирования. Меньшее число означает больший приоритет.

Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения и вернуть их к первоначальным значениям;

10.7 Configuration–Loop Protection (Настройки – Защита от петель)



На данной странице WEB интерфейса представлены настройки защиты от сетевых петель (Loop Protection).

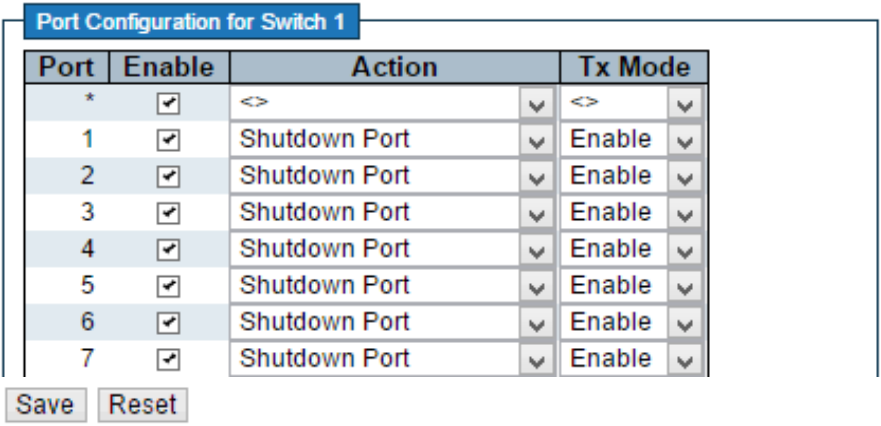
Основные настройки

Enable Loop Protection (Включить защиту от петель)
Элемент интерфейса отвечает за включение/выключение (enable/disable) функции защиты от петель.

Transmission Time (Время передачи)
Время передачи определяет интервал между отправками PDU защиты от петель на каждый порт. Допустимые значения от 1 до 10.

Shutdown Time (Время отключения)
Временной период (в секундах), в течение которого порт будет отключен в случае возникновения петли.

Допустимые значения: от 0 до 604800 секунд (7 дней). Нулевое значение будет удержать порт в неактивном состоянии (до следующей перезагрузки устройства).



Настройка портов

Port (Порт)
Номер порта коммутатора

Enable (Включение)
Элемент интерфейса контролирует включение/выключение функции Loop Protection для выбранного порта.

Action (Действие)
Элемент интерфейса определяет действие, выполняемое при обнаружении петли на порте. Допустимые значения:

- ✓ «Отключение порта» (Shutdown Port)
- ✓ «Отключение порта и запись в журнал» (Shutdown Port and Log)
- ✓ «Только Запись в журнал» (Log Only)

Tx Mode (Режим передачи)
Данная настройка контролирует, активно ли порт генерирует блоки Loop Protection PDU или ищет блоки PDU петли в пассивном режиме.

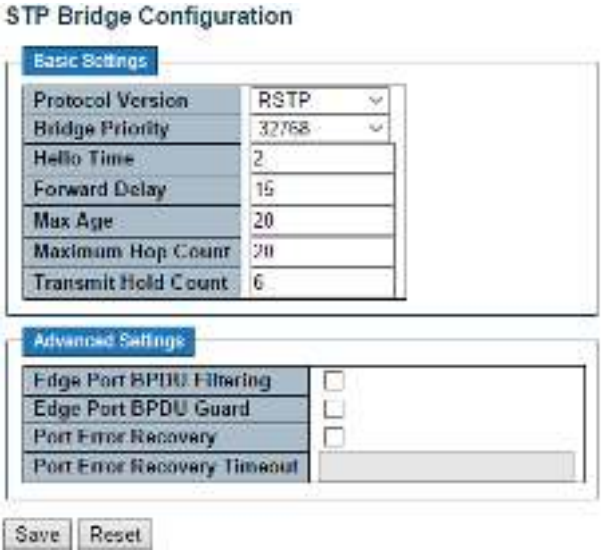
Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения и вернуть их к первоначальным значениям;

10.8 Configuration–Spanning Tree (Настройки – Протокол связующего дерева STP)

10.8.1 Spanning Tree–Bridge Settings (Протокол связующего дерева STP–Настройки корневого моста)



На данной странице WEB интерфейса представлены настройки протокола STP. Эти настройки используются всеми корневыми мостами (bridge) в стэке коммутаторов.

Базовые настройки.

Protocol Version (Версия протокола)
Выбор версии протокола связующего дерева (MSTP/RSTP/STP)

Bridge Priority (значение для определения корневого моста)
Определяет приоритет корневого устройства – моста (root bridge). Более низкие числовые значения имеют больший приоритет. Приоритет моста + MSTI, объединенный с 6-байтовым MAC-адресом коммутатора, образует идентификатор моста (Bridge ID).
Для операции с MSTP протоколом это приоритет CIST. В противном случае это приоритет моста STP/RSTP.

Hello Time (интервал отправки пакетов BPDU)
Интервал между отправкой STP BPDU. Допустимые значения находятся в диапазоне от 1 до 10 секунд, значение по умолчанию - 2 секунды.
Примечание. Изменение этого параметра по умолчанию не рекомендуется и может оказать неблагоприятное влияние на вашу сеть.

Forward Delay (задержка смены состояний)
Интервал, через который порт коммутатора меняет состояние с обучения/прослушивания на пересылку. Диапазон возможных значений 4-30сек. Значение по умолчанию – 15 сек.

Max Age (время хранения текущей конфигурации)
Таймер, определяющий ожидание BPDU пакетов от корневого моста. Если устройство получает пакеты BPDU до истечения времени таймера, значение таймера будет сброшено.

Кроме того, устройство отправит топологию с измененным BPDU для уведомления других устройств. Диапазон значений составляет от 6 – 40сек. Значение по умолчанию – 20 сек.

Maximum Hop Count (Максимальное количество хопов – переходов)
Это поле определяет начальное значение оставшихся переходов (хопов) для информации MSTI, сгенерированной на границе области MSTI.

Он определяет, на сколько мостов корневой мост (root bridge) может распространять свою информацию BPDU. Допустимые значения находятся в диапазоне от 6 до 40 переходов (хопов).

Transmit Hold Count (Максимальное количество пакетов BPDU для отправки)

Количество пакетов BPDU, которые может передать порт в секунду. При превышении этого значения передача следующего BPDU пакета будет отложена. Допустимые значения находятся в диапазоне от 1 до 10 BPDU в секунду.

Расширенные настройки

Edge Port BPDU Filtering (Фильтрация BPDU для крайнего порта)
Поле определяет, будет ли порт, помеченный как Edge (крайний), передавать и получать BPDU пакеты.

Edge Port BPDU Guard (Функция «Edge Port BPDU Guard»)
Поле определяет, будет ли порт, помеченный как Edge (крайний), отключаться при получении BPDU пакетов. Порт перейдет в состояние отключения по ошибке и будет удален из активной топологии.

Port Error Recovery (Восстановление порта после ошибки)
Поле определяет, будет ли порт, находящийся в состоянии отключения после ошибки, автоматически включен через определенное время.

Если Port Error Recovery не включено, порты должны быть вручную отключены и повторно включены для нормальной работы протокола STP.

Данное условие выполняется также после перезагрузки коммутатора.

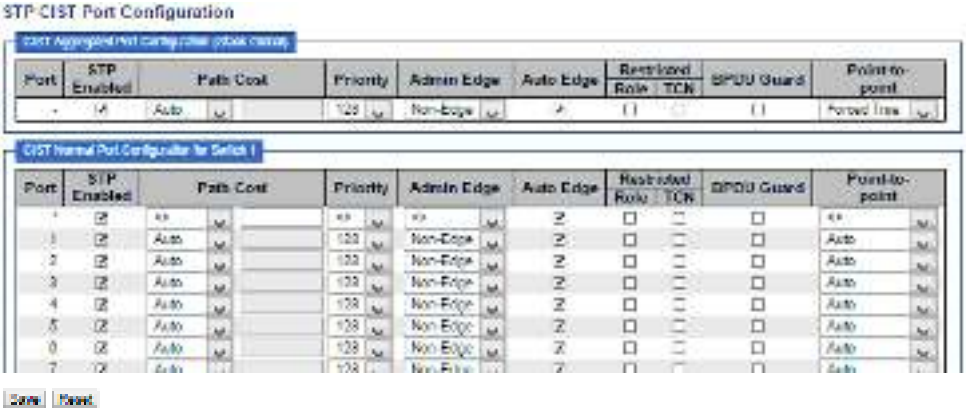
Port Error Recovery Timeout
Время до перевода порта в состоянии «отключения по ошибке» в рабочее состояние. Допустимые значения: от 30 до 86400 секунд (24 часа).

Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения и вернуть их к первоначальным значениям;

10.8.2 Spanning Tree–Bridge Ports (Протокол связующего дерева STP–Настройки портов)



Эта страница WEB интерфейса предоставляет возможность проверить текущие конфигурации порта STP/CIST и изменить их, если это необходимо.

Эта страница WEB интерфейса содержит настройки, как для физических так и для агрегированных портов.

Используются глобальные параметры агрегации.

Настройки порта STP относятся к текущему выбранному коммутатору из стека, что отражено в заголовке страницы.

Port (Порт)

Номер порта коммутатора – логического порта STP.

STP Enabled (Включение STP)

Поле отвечает за включение STP на этом порту коммутатора.

Path Cost (Стоимость пути)

Диапазон «стоимости пути». Диапазон возможных значений от 0 – 200000000. По умолчанию значение – 0. Это означает, что расчет стоимости пути определяется системой автоматически.

Priority (Приоритет)
Поле отвечает за приоритет порта. Настройка может использоваться для контроля приоритета портов, имеющих одинаковую стоимость порта. (PathCost).

operEdge (state flag)
Флаг, отвечающий за определения подключения порта напрямую к периферийным устройствам.

Переход к состоянию пересылки выполняется быстрее для крайних портов (имеющих значение operEdge true), чем для других портов.

Значение этого флага основано на полях AdminEdge и AutoEdge. Этот флаг отображается как Edge в Monitor-> Spanning Tree -> STP (Подробное описание состояния моста).

AdminEdge
Поле определяет, должен ли флаг operEdge быть установлен или снят. (Начальное состояние operEdge при инициализации порта).

AutoEdge
Поле определяет, должен ли мост активировать автоматическое определение состояния Edge на корневом порте. Это позволяет определить значение флага operEdge (установлен или снят) из того, получены ли BPDU пакеты на порт или нет.

Restricted Role
Если этот параметр включен, порт не будет выбран в качестве корневого порта для CIST или любого MSTI, даже если он имеет лучшее значение приоритета STP.

Такой порт будет выбран в качестве альтернативного порта после выбора корневого порта (Root Port). Если данная настройка активирована, это может привести к отсутствию связности топологии.

Он может быть установлен сетевым администратором так, чтобы мосты, внешние по отношению к основной области сети, не влияли на активную топологию связующего дерева, в следствие, что эти мосты не находятся под полным контролем администратора.

Эта функция также известна как Root Guard.

Restricted TCN

Если этот параметр включен, порт не будет пересылать полученные уведомления об изменении топологии и изменения топологии на другие порты.

Если активировано, то это может вызвать временную потерю соединения после изменений в активной топологии связующего дерева из-за постоянно неверной информации о местоположении изученного коммутатора (устройства).

Параметр устанавливается сетевым администратором для предотвращения возникновения внешних мостов по отношению к основному региону сети, что приведет к сбросу адресов в этом регионе.

BPDU Guard

Если функция включена, порт отключается при получении BPDU. В отличие от аналогичного параметра моста, статус пограничного порта (Edge) не влияет на этот параметр.

Порт, находящийся в отключенном из-за ошибки состоянии из-за этого параметра, также подчиняется настройке Port Error Recovery.

Point-to-Point

Функция управляет подключением порта к локальной сети типа «точка-точка», а не к распределенной сети.

Это может быть определено автоматически или вручную. Переход в состояние пересылки происходит быстрее для «точка-точка» локальных сетей, чем для распределенной сети.

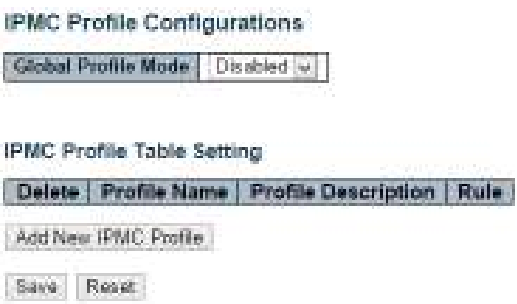
Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения и вернуть их к первоначальным значениям;

10.9 Configuration–IPMC Profile (Настройки – IPMC)

10.9.1 IPMC – Profile Table (IPMC – Таблица профиля)



На этой странице WEB интерфейса представлены настройки, связанные с профилем IPMC.

Профиль IPMC используется для развертывания управления доступом в Multicast IP потоках. Разрешается создавать не более 64 профилей и не более 128 соответствующих правил для каждого.

Global Profile Mode (Глобальный режим работы)
Включить/Выключить глобально профиль IPMC.
Система начинает выполнять фильтрацию на основе настроек профиля, только когда включен режим «Global Profile Mode».

Delete (Удалить)
Нажмите, чтобы удалить запись. Запись будет удалена при следующем сохранении (save).

Profile Name (Имя профиля)
Имя, использующееся для индексирования таблицы профиля.
Каждая запись обладает уникальным именем, которое состоит максимум из 16 символов алфавита и цифр. Как минимум один символ алфавит должен присутствовать в имени.

Profile Description (Описание профиля)
Дополнительное описание профиля, которое состоит максимум из 64 буквенных и цифровых символов.
Используйте «_» или «-», пробелы не допускаются.

Rule (Правила)
Когда профиль создан, нажмите кнопку редактирования, чтобы перейти на страницу настройки правил для указанного профиля.

Сводка о назначенном профиле будет отображаться нажатием кнопки просмотра.

Вы можете управлять или проверять правила назначенного профиля с помощью следующих кнопок:

- ✓ Navigate – список с правилами, связанными с данным профилем;
- ✓ Edit – настройка правил связанных с назначенным устройством.

Кнопки:

Add New IPMC Profile – нажмите, чтобы добавить новый IPMC профиль. Укажите имя и создайте новую запись. Нажмите сохранить (save)

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения и вернуть их к первоначальным значениям;

10.9.2 IPMC – Address Entry (IPMC – Ввод адреса)

Эта страница WEB интерфейса предоставляет возможность настроить диапазон адресов, используемых в IPMC.

Запись адреса используется для указания диапазона адресов, который будет связан с профилем IPMC. В системе разрешено создавать не более 128 адресных записей.

Delete (Удалить)
Отметьте этот элемент, чтобы удалить запись. Запись будет удалена при следующем сохранении.

Entry Name (Имя записи)
Имя, используемое для индексации таблицы адресов ввода.
Каждая запись имеет уникальное имя, которое состоит максимум из 16 букв и цифр. Должен присутствовать хотя бы один символ алфавита.

StartAddress (Начальный адрес)
Начальный адрес группы многоадресной рассылки IPv4/IPv6, который будет использоваться в качестве диапазона адресов.

EndAddress (Конечный адрес)
Конечный адрес группы многоадресной рассылки IPv4/IPv6, который будет использоваться в качестве диапазона адресов.

Кнопки:

Add New Address (Range) Entry – нажмите, чтобы добавить новый диапазон адресов. Укажите имя и настройте адреса. Нажмите сохранить (save)

Save – нажмите, чтобы сохранить изменения;

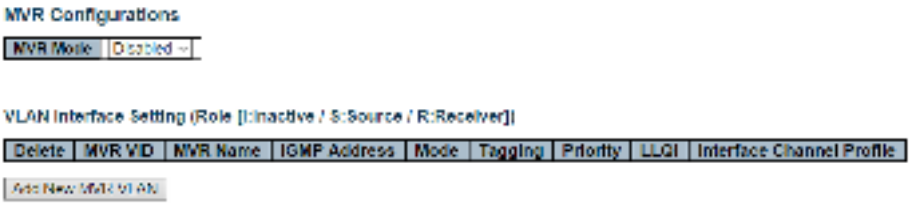
Reset – нажмите, чтобы отменить изменения и вернуть их к первоначальным значениям;

Refresh – нажмите, чтобы обновить отображающиеся в полях значения;

<< – Обновляет таблицу, начиная с первой записи в конфигурации адреса профиля IPMC

>> – Обновляет таблицу, начиная с записи после последней отображаемой записи.

10.10 Configuration – MVR (Настройки – MVR)



Данная страницы WEB интерфейса содержит инструменты для настройки MVR. Функция MVR обеспечивает переадресацию multicast трафика в multicast сетях VLAN.

Разрешается создавать максимум 8 VLAN MVR с соответствующими настройками канала для каждой multicast VLAN-сети. Всего может быть максимум 256 групповых адресов.

MVR Mode (Режим работы MVR)
Включить/Выключить (Enable/Disable) глобально MVR.

Delete (Удалить)
Отметьте этот элемент, чтобы удалить запись. Запись будет удалена при следующем сохранении.

MVR VID (идентификатор multicast VLAN)
Укажите идентификатор multicast VLAN.
Примечание: порты источника MVR не рекомендуется перекрывать портами управления VLAN.

MVR Name (Имя MVR)
Имя MVR является необязательным атрибутом для указания имени конкретной VLAN MVR.

Максимальная длина строки имени VLAN MVR - 32. Имя VLAN MVR может содержать только буквы или цифры. Когда указывается необязательное имя VLAN MVR, оно должно содержать хотя бы один символ алфавита.

Имя MVR VLAN может быть отредактировано для существующих записей MVR VLAN или может быть добавлено к новым записям.

Mode (Режим)
Укажите режим работы MVR.

В динамическом режиме «Dynamic» MVR допускает динамические отчеты о регистрации multicast VLAN на портах источника.

В режиме совместимости «Compatible» отчеты о регистрации multicast VLAN запрещены на портах источника. По умолчанию используется динамический режим.

Tagging (Тэгирование)
Укажите, будут ли контрольные пакеты IGMP/MLD отправляться без тега (untagged) или с тегом MVR VID (tagged).

LLQI
Поле определяет максимальное время ожидания членства в отчетах IGMP/MLD на порте получателя, прежде чем удалять порт из группы multicast рассылки.

Значение указывается в десятых долях секунды. Диапазон составляет от 0 до 31744.

Значение по умолчанию LLQI составляет 5 десятых или полсекунды.

Interface Channel Setting (Интерфейс настроек канала)
Когда MVR VLAN будет создана, нажмите «Edit», чтобы развернуть соответствующие настройки канала multicast для конкретной MVR VLAN.

Сводка о настройке интерфейсного канала (для MVR VLAN) будет показана помимо символа редактирования.

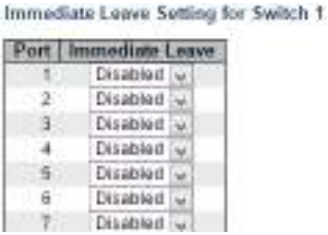
Port (Порт)
Логический порт для настроек.

Port Role (Роль порта)
Настройте порт MVR в соответствующей VLAN MVR присвоив одну из следующих ролей:

- ✓ Inactive (I) – назначенный порт не участвует в операциях MVR;
- ✓ Source (S) – настройте порты uplink, которые получают и отправляют данные ьгдешсфые рассылки в качестве исходных

портов. Абоненты не могут быть напрямую подключены к исходным портам.

- ✓ Receiver (R) – настройте порт, как порт получателя, если он должен принимать только данные multicast рассылки. Такой порт не получает данные, если не является членом группы multicast рассылки.



Immediate Leave (Немедленный выход)
Настройка разрешает быстрый выход на порте.

Кнопки:

Add New MVR VLAN – нажмите, чтобы добавить MVR VLAN. Укажите VID и настройте запись. Нажмите сохранить (save)

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения и вернуть их к первоначальным значениям;

Delete (Удалить)
Отметьте этот элемент, чтобы удалить запись. Запись будет удалена при следующем сохранении.

VLAN ID (Идентификатор VLAN)
Поле отображает особый идентификатор multicast VLAN. Поле не редактируемое.

VLAN Name (Имя записи)
Поле отображает особое имя multicast VLAN. Поле не редактируемое.

StartAddress (Начальный адрес)
Начальный адрес группы многоадресной рассылки IPv4/IPv6, который будет использоваться как канал для потока (streaming channel)

EndAddress (Конечный адрес)
Конечный адрес группы многоадресной рассылки IPv4/IPv6, который будет использоваться как канал для потока (streaming channel)

Channel Name (Имя канала)
Укажите название канала определенной multicast VLAN.

Максимальная длина строки имени канала - 32. Имя канала может содержать только буквы или цифры.

Название канала должно содержать хотя бы один символ алфавита.

Кнопки:

Add New MVR Channel – нажмите, чтобы добавить новый канал. Укажите адрес и настройте новую запись. Нажмите сохранить (save)

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения и вернуть их к первоначальным значениям;

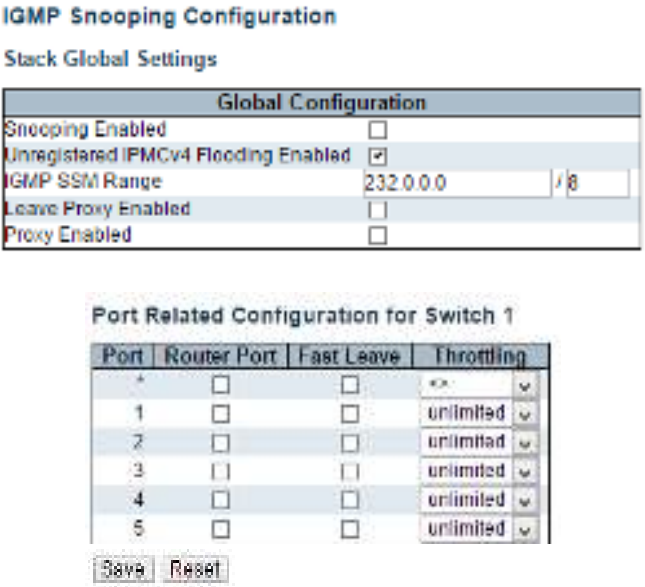
Refresh – нажмите, чтобы обновить отображающиеся в полях значения;

<< – Обновляет таблицу, начиная с первой записи в MVR Channel Configuration
>> – Обновляет таблицу, начиная с записи после последней отображаемой записи.

10.11 Configuration – IPMC (Настройки – IPMC)

10.11.1 IPMC – IGMP Snooping (Настройки – IGMP Snooping)

10.11.1.1 IGMP Snooping – Basic Configuration (IGMP Snooping – Базовые настройки)



На данной странице WEB интерфейса представлены основные настройки функции IGMP Snooping.

Snooping Enabled (Включение функции IGMP Snooping)
Включить глобально поддержку IGMP Snooping.

Unregistered IPMCv4 Flooding Enabled (Незарегистрированный флудинг IPMCv4 включен)
Включить / Выключить незарегистрированный поток трафика IPMCv4.

Контроль флудинга (копирования фрейма во все порты) вступает в силу только при включенном глобально IGMP Snooping.

Когда IGMP Snooping отключен, функция Unregistered IPMCv4 Flooding всегда активна, несмотря на значения этой настройки.

IGMP SSM Range (Диапазон SSM)
Диапазон SSM (Source-Specific Multicast) позволяет хостам и маршрутизаторам, поддерживающим SSM, запускать модель обслуживания SSM для групп в диапазоне адресов.

Leave Proxy Enabled
Включить/Выключить IGMP Leave Proxy. Эту функцию можно использовать, чтобы избежать пересылки ненужных сообщений маршрутизатору.

Proxy Enabled (Включить Proxy)
Включить / Выключить IGMP Proxy. Эту функцию можно использовать, чтобы избежать пересылки информации о ненужных подключениях и ненужных сообщений маршрутизатору.

Router Port (Порт маршрутизатора)
Укажите, какие порты действуют, как порты маршрутизатора. Порт маршрутизатора - это порт на коммутаторе Ethernet, который ведет к устройству multicast устройству Layer 3 или работает с IGMP запросами.

Fast Leave (Быстрый выход)
Включить/Выключить быстрый выход на порте

Throttling (Троттлинг)
Включите, чтобы ограничить количество Multicast групп, к которым может принадлежать порт коммутатора.

Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения и вернуть их к первоначальным значениям;

10.11.1.2 IGMP Snooping – VLAN Configuration (IGMP Snooping – Настройки VLAN)

Столбцы таблицы IGMP Snooping VLAN Configuration

Delete (Удалить)
Отметьте этот элемент, чтобы удалить запись. Запись будет удалена при следующем сохранении.

VLAN ID (Идентификатор VLAN)
Поле отображает особый идентификатор VLAN соответствующий записи.

IGMP Snooping Enabled (Состояние функции IGMP Snooping)
Включите отслеживание IGMP для каждой VLAN. Для отслеживания состояния IGMP можно выбрать до 32 VLAN.

Querier Election
Опция отвечает за выбор IGMP Querier в VLAN.

Querier Address
Задайте адрес IPv4 в качестве адреса источника, используемого в заголовке IP для выбора IGMP Querier в VLAN.

Если адрес не задан, система использует IPv4-адрес, связанный с этой VLAN.

Если адрес IPv4, связанный с VLAN, не задан, система использует первый доступный адрес IPv4 для управления.

Compatibility (Совместимость)
Совместимость должна быть между хостами и маршрутизаторами, выполняющими соответствующие действия в зависимости от версии IGMP протокола, использующегося на хостах и маршрутизаторах в сети. На выбор предусмотрено 4 варианта:

- ✓ IGMP-Auto;
- ✓ Forced IGMPv1;
- ✓ Forced IGMPv2;
- ✓ Forced IGMPv3.

PRI (Приоритет интерфейса)
Поле определяет уровень приоритета фрейма управления IGMP, сгенерированный системой.

Эти значения могут использоваться для определения приоритетов разных классов трафика.

Допустимый диапазон - от 0 до 7 (максимальное), значение приоритета интерфейса по умолчанию - 0.

RV
Переменная Robustness Variable (RV) позволяет настраивать предполагаемую потерю пакетов в сети.
Допустимый диапазон - от 1 до 255, значение RV по умолчанию - 2.

QI (Интервал запросов)
Это интервал между общими запросами, отправляемыми запрашивающим устройством.
Допустимый диапазон - от 1 до 31744 секунд, интервал запроса по умолчанию - 125 секунд.

QRI (Интервал ответов на запросы)
Допустимый диапазон: от 0 до 31744 за десятые секунды, QRI по умолчанию составляет 100 за десятые секунды (10 секунд).

LLQI (LMQI for IGMP)
Интервал между запросами последнего участника.
Допустимый диапазон от 0 до 31744 в десятых долях секунды, LLQI - 10 в десятых долях секунды (1 секунда).

URI
Допустимый диапазон - от 0 до 31744 секунд, URI по умолчанию - 1 секунда.

Кнопки:

Add New IGMP VLAN – нажмите, чтобы добавить новую IGMP VLAN. Укажите VID и настройте новую запись. Нажмите сохранить (save)

Save – нажмите, чтобы сохранить изменения;

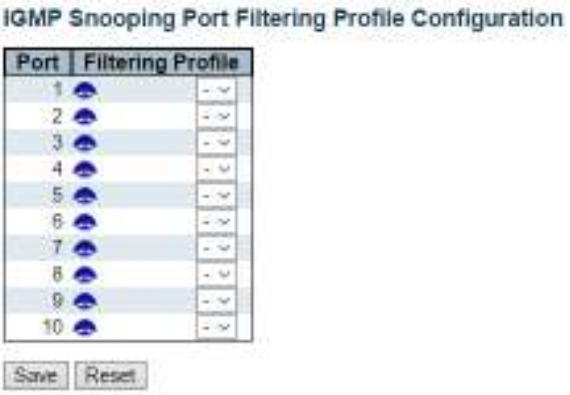
Reset – нажмите, чтобы отменить изменения и вернуть их к первоначальным значениям;

Refresh – нажмите, чтобы обновить отображающиеся в полях значения;

<< – Обновляет таблицу, начиная с первой записи;

>> – Обновляет таблицу, начиная с записи после последней отображаемой записи.

10.11.1.3 IGMP Snooping – Port Group Filtering (IGMP Snooping – Фильтрация для групп портов)



Port (Порт)
Логический порт для конфигурирования.

Filtering Profile (Профиль фильтрации)
Выбор профиля IPMC в качестве условия фильтрации для определенного порта.

Сведения о назначенном профиле будет отображаться нажатием кнопки просмотра.

Profile Management Button (Кнопки управления профилем)
Возможность проверки правил назначенного профиля с помощью следующей кнопки:

- ✓ Navigate – просмотр списка правил, связанных с данным профилем.

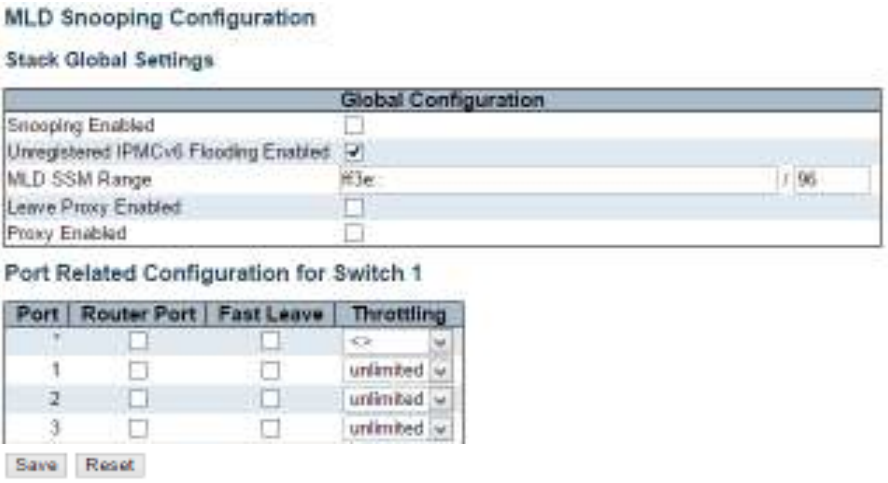
Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения и вернуть их к первоначальным значениям;

10.11.2 IPMC – MLD Snooping (IPMC – MLD Snooping)

10.11.2.1 MLD Snooping – Basic Configuration (IGMP Snooping – Базовые настройки)



Snooping Enabled (Включение функции MLD Snooping)
Включить глобально поддержку IGMP Snooping.

Unregistered IPMCv6 Flooding Enabled (Незарегистрированный флудинг IPMCv6 включен)
Включить / Выключить незарегистрированный поток трафика IPMCv6.
Контроль флудинга (копирования фрейма во все порты) вступает в силу только при включенном глобально MLD Snooping.
Когда MLD Snooping отключен, функция Unregistered IPMCv6 Flooding всегда активна, несмотря на значения этой настройки.

MLD SSM Range
Диапазон SSM (Source-Specific Multicast) позволяет хостам и маршрутизаторам, поддерживающим SSM, запускать модель обслуживания SSM для групп в диапазоне адресов.

Leave Proxy Enabled
Включить/Выключить MLD Leave Proxy. Эту функцию можно использовать, чтобы избежать пересылки ненужных сообщений маршрутизатору.

Proxy Enabled (Включить Proxy)
Включить / Выключить MLD Proxy. Эту функцию можно использовать, чтобы избежать пересылки информации о ненужных подключениях и ненужных сообщений маршрутизатору.

Router Port (Порт маршрутизатора)
Укажите, какие порты действуют, как порты маршрутизатора. Порт маршрутизатора - это порт на коммутаторе Ethernet, который ведет к устройству multicast устройству Layer 3 или работает с MLD запросами.

Fast Leave (Быстрый выход)
Включить/Выключить быстрый выход на порте

Throttling (Троттлинг)
Включите, чтобы ограничить количество Multicast групп, к которым может принадлежать порт коммутатора.

Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения и вернуть их к первоначальным значениям;

10.11.2.2 MLD Snooping – VLAN Configuration (MLD Snooping – Настройки VLAN)

Delete (Удалить)
Отметьте этот элемент, чтобы удалить запись. Запись будет удалена при следующем сохранении.

VLAN ID (Идентификатор VLAN)
Поле отображает особый идентификатор VLAN соответствующий записи.

MLD Snooping Enabled (Состояние функции MLD Snooping)
Включите отслеживание MLD для каждой VLAN. Для отслеживания состояния MLD можно выбрать до 32 VLAN.

Querier Election
Опция отвечает за выбор MLD Querier в VLAN.

Querier Address
Задайте адрес IPv4 в качестве адреса источника, используемого в заголовке IP для выбора MLD Querier в VLAN.

Если адрес не задан, система использует IPv4-адрес, связанный с этой VLAN.

Если адрес IPv4, связанный с VLAN, не задан, система использует первый доступный адрес IPv4 для управления.

Compatibility (Совместимость)
Совместимость должна быть между хостами и маршрутизаторами, выполняющими соответствующие действия в зависимости от версии MLD протокола, использующегося на хостах и маршрутизаторах в сети.
На выбор предусмотрено 4 варианта:

- ✓ MLD-Auto;
- ✓ Forced MLDv1;
- ✓ Forced MLDv2;
- ✓ Forced MLDv3.

PRI (Приоритет интерфейса)
Поле определяет уровень приоритета фрейма управления MLD, сгенерированный системой.

Эти значения могут использоваться для определения приоритетов разных классов трафика.

Допустимый диапазон - от 0 до 7 (максимальное), значение приоритета интерфейса по умолчанию - 0.

RV
Переменная Robustness Variable (RV) позволяет настраивать предполагаемую потерю пакетов в сети.
Допустимый диапазон - от 1 до 255, значение RV по умолчанию - 2.

QI (Интервал запросов)
Это интервал между общими запросами, отправляемыми запрашивающим устройством.
Допустимый диапазон - от 1 до 31744 секунд, интервал запроса по умолчанию - 125 секунд.

QRI (Интервал ответов на запросы)
Допустимый диапазон: от 0 до 31744 за десятые секунды, QRI по умолчанию составляет 100 за десятые секунды (10 секунд).

LLQI
Интервал между запросами последнего участника.
Допустимый диапазон от 0 до 31744 в десятых долях секунды, LLQI - 10 в десятых долях секунды (1 секунда).

URI
Допустимый диапазон - от 0 до 31744 секунд, URI по умолчанию - 1 секунда.

Кнопки:

Add New MLD VLAN – нажмите, чтобы добавить новую MLD VLAN. Укажите VID и настройте новую запись. Нажмите сохранить (save)

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения и вернуть их к первоначальным значениям;

Refresh – нажмите, чтобы обновить отображающиеся в полях значения;

<< – Обновляет таблицу, начиная с первой записи;

>> – Обновляет таблицу, начиная с записи после последней отображаемой записи.

10.11.2.3 MLD Snooping – Port Group Filtering (MLD Snooping – Фильтрация для групп портов)

Port (Порт)
Логический порт для конфигурирования.

Filtering Profile (Профиль фильтрации)
Выбор профиля IPMC в качестве условия фильтрации для определенного порта.

Сведения о назначенном профиле будет отображаться нажатием кнопки просмотра.

Profile Management Button (Кнопки управления профилем)
Возможность проверки правил назначенного профиля с помощью следующей кнопки:

- ✓ Navigate – просмотр списка правил, связанных с данным профилем.

Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения и вернуть их к первоначальным значениям;

10.12 Configuration – LLDP (Настройки – Протокол LLDP)

10.12.1 LLDP – LLDP Configuration (Протокол LLDP – Настройки протокола LLDP)

LLDP Configuration

LLDP Parameters

Tx Interval	30	seconds
Tx Hold	4	times
Tx Delay	2	seconds
Tx Reinit	2	seconds

LLDP Port Configuration for Switch 1

Port	Mode	CDP aware	Optional TLVs				
			Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	☐	☑	☑	☑	☑	☑
1	Enabled	☐	☑	☑	☑	☑	☑
2	Enabled	☐	☑	☑	☑	☑	☑
3	Enabled	☐	☑	☑	☑	☑	☑
4	Enabled	☐	☑	☑	☑	☑	☑
5	Enabled	☐	☑	☑	☑	☑	☑
6	Enabled	☐	☑	☑	☑	☑	☑
7	Enabled	☐	☑	☑	☑	☑	☑

LLDP (IEEE 802.1AB) протокол канального уровня, позволяющий сетевому оборудованию оповещать оборудование, работающие в локальной сети о своем существовании и передавать ему свои характеристики, а также получать от него аналогичные сведения.

Параметры LLDP

TX Intreval (Интервал отправки)
Коммутатор периодически передает фреймы LLDP своим устройствам-соседям для обеспечения актуальности discovery информации.

Интервал между передачей каждого фрейма LLDP определяется значением TX Intreval. Допустимые значения 5 - 32768 сек.

Tx Hold
Каждый фрейм LLDP содержит информацию о том, как долго информация внутри фрейма LLDP должна считаться действительной.

Период актуальности информации LLDP равен значению Tx Hold, умноженному на Tx Interval секунд.

Tx Delay (Задержка отправки)
Если конфигурация изменяется (например, IP-адрес), передается новый кадр LLDP, но время между кадрами LLDP всегда будет по меньшей мере равным значению Tx Delay. Tx Delay не может превышать 1/4 значения TX Intreval. Допустимые значения 1 - 8192 секундами.

TX Reinit ()
Когда порт отключен, LLDP отключен глобально или коммутатор перезагружен, фрейм отключения LLDP передается соседним устройствам, сигнализируя о том, что информация LLDP больше не действительна.

Tx Reinit определяется количеством секунд между кадром выключения и новой инициализацией LLDP. Допустимые значения ограничены 1 - 10 сек.

Настройка LLDP на портах

Port (Порт)
Номер порта коммутатора

Mode (Режим работы)
Выбор режима работы LLDP:

- ✓ Rx only – Коммутатор не будет отправлять информацию LLDP, но при этом, информация LLDP, полученная от соседних устройств, анализируется;
- ✓ Tx only – Коммутатор не будет самостоятельно обрабатывать информацию LLDP, полученную от устройств-соседей, но при этом, отправит информацию LLDP далее;
- ✓ Disabled – Коммутатор не будет отправлять информацию LLDP далее и не будет самостоятельно обрабатывать информацию LLDP, полученную от устройств – соседей;
- ✓ Enabled – Коммутатор будет отправлять информацию LLDP далее, а также самостоятельно анализировать информацию LLDP, полученную от устройств - соседей.

CDP Aware

- ✓ Функциональность CDP ограничена декодированием входящих фреймов CDP (коммутатор не передает фреймы CDP самостоятельно). Фреймы CDP декодируются, только если включен LLDP на порту.
- ✓ Декодируются только CDP TLV фреймы, которые могут быть сопоставлены с соответствующим полем в таблице устройств-соседей LLDP. Все остальные TLV не обрабатываются (нераспознанные CDP TLV и отброшенные кадры CDP не отображаются в статистике LLDP.).

Port Descr (Описание порта)
Необязательный TLV: если этот флаг установлен, «Port Descr» включается в передаваемую информацию LLDP.

Sys Name (Системное имя)
Необязательный TLV: если этот флаг установлен, «Sys Name» включается в передаваемую информацию LLDP.

Sys Descr (Описание системы)
Необязательный TLV: если этот флаг установлен, «Sys Descr» включается в передаваемую информацию LLDP.

Sys Capa (Совместимость системы)
Необязательный TLV: если этот флаг установлен, «Sys Capa» включается в передаваемую информацию LLDP.

Mgmt Addr (Адрес управления)
Необязательный TLV: если этот флаг установлен, «Mgmt Addr» включается в передаваемую информацию LLDP.

Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения

10.12.2 LLDP – LLDP MED (Протокол LLDP – LLDP MED)

На данной странице WEB интерфейса представлены настройки LLDP MED. Эта функция используются с VoIP устройствами, которые ее поддерживают.

Координаты местоположения

Latitude (Широта)
Широта должна быть в пределах 0-90 градусов с максимум 4 цифрами.
Можно указать направление к северу от экватора или к югу от экватора.

Longitude (Долгота)
Долгота должна быть в пределах 0-180 градусов с максимум 4 цифрами.
Можно указать направление к востоку от первичного меридиана или к западу от первичного меридиана.

Altitude (Высота)
Высота должна быть в пределах от -32767 до 32767 с максимум 4 цифрами.
Можно выбрать один из двух типов высоты (этажи или метры).

Map Datum (Опорная точка карты)
Опорная точка карты используется для координат, указанных в следующих параметрах:

- ✓ WGS84
- ✓ NAD83/NAVD88
- ✓ NAD83/MLLW

10.13 Configuration – PoE (Настройки – PoE)

Данная страница WEB интерфейса содержит инструменты по настройке текущей конфигурации PoE на портах.

Конфигурирование функции Power Over Ethernet

Зарезервированная мощность PoE определяется 3 различными режимами:

1) Allocated mode – распределенный режим. В этом режиме пользователь определяет мощность в Ваттах на каждый порт. Значение зарезервированной мощности указывается в поле Maximum Power.
2) Class mode – режим распределения мощности PoE в зависимости от класса устройства. В этом режиме каждый порт автоматически определяет, сколько энергии резервировать в соответствии с классом, к которому принадлежит подключенное POE устройство, и соответственно резервирует мощность. Существуют четыре различных класса и один на 4, 7, 15,4 или 30 Вт. В этом режиме поля Maximum Power не действуют.
3) LLDP-MED mode – этот режим аналогичен режиму Class mode, за исключением того, что каждый порт определяет объем мощности, который он резервирует, путем обмена информацией PoE с использованием протокола LLDP и резервирует мощность соответственно. Если информация о LLDP недоступна для порта, порт будет резервировать питание, используя Class mode. В этом режиме поля максимальной мощности не действуют

Примечание для всех режимов: если порт использует больше мощности, чем зарезервированная мощность для порта, порт отключается.

Конфигурирование источника питания

Primary and Backup Power Source (Основной и резервный источники питания)

Некоторые коммутаторы поддерживают наличие двух источников питания PoE. Один используется в качестве основного источника питания, а другой - в качестве резервного источника питания. Если коммутатор не поддерживает резервный источник питания, будут показаны только настройки основного источника питания.

В случае сбоя основного источника питания, начнет работать резервный источник питания. Чтобы иметь возможность определить количество энергии, которое может использовать PoE устройство, необходимо определить, какое количество энергии может предоставить основной и резервный источники питания в Ваттах.

Значения могут быть от 0 до 2000 Вт.

Настройка PoE для портов

Port (Порт)

Логический номер порта. Порты, которые не поддерживают PoE будут выделены серым цветом и недоступны для конфигурирования.

PoE Mode (режим работы PoE)

- ✓ Disabled – PoE отключено на выбранном порте;
- ✓ PoE – PoE включено и соответствует стандарту IEEE 802.3af (Class 4. Потребляемая мощность PoE устройств ограничена 15,4 Вт)
- ✓ PoE+ – PoE+ включено и соответствует стандарту IEEE 802.3at (Class 4. Потребляемая мощность PoE устройств ограничена 30 Вт)

Priority (Приоритет)

Предусмотрено три уровня приоритета PoE мощности: Низкий (Low), Высокий (High) и Критический (Critical).

Приоритет используется в случае, когда удаленным устройствам требуется больше энергии, чем может обеспечить источник питания.

В этом случае порт с самым низким приоритетом будет отключен, начиная с последнего порта.

Maximum Power (Максимальная мощность)
Поле содержит значение мощности PoE в Ваттах, которую можно передать на удаленное PoE устройство. Максимальное значение составляет 30 Вт.

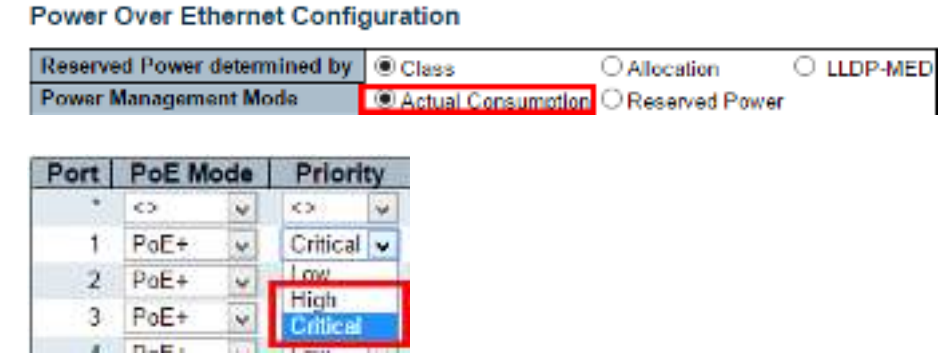
Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения

Внимание! Если PoE устройство подключено к коммутатору PoE и бюджет PoE не достаточен, чтобы запитать это устройство, светодиод PoE будет мигать, а порт не будет подавать питание на вновь подключенное PoE устройство.

Рекомендуется установить режим управления питанием PoE на фактическое потребление (actual Consumption), а порты, которые подключаются к важным PoE устройствам, настроить на высокий или критический приоритет, как показано на рисунках ниже.



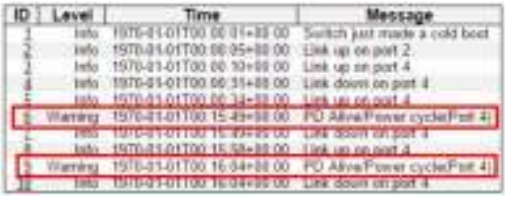
10.13.1 Configuration – PD Alive (Настройки – функция антизависания PoE устройств)

Функция PD Alive позволяет коммутатору автоматически определять зависшие PoE устройства на портах и перезагружать их путем переподачи питания.

Чтобы активировать функцию на порте необходимо:

1) выбрать порт/порты (Port);
2) в поле PD Alive Enable – выбрать Enable (включено);
3) в поле PD IP Address – указать IP адрес подключенного PoE устройства;
4) Задать интервал отправки запросов на устройство (Interval Time). По умолчанию каждые 5 сек;
5) Задать количество циклов повторений опрашивания (Retry Count). По умолчанию – 2;
6) Задать время, в течение которого коммутатор не будет опрашивать удаленное PoE устройство (PD Boot Time). Это время необходимо устройству для достижения рабочего состояния после перезагрузки. Значение по умолчанию – 10 сек.
7) Нажать кнопку Save (сохранить).

Результаты работы функции PD Alive можно посмотреть в журнале записей:



10.14. Configuration – SyncE (Настройки – SyncE)

Эта страница WEB интерфейса позволяет пользователю просматривать и настраивать текущие настройки SyncE для портов.

Источник синхронизации и текущее состояние

Источник синхронизации
Номер источника синхронизации.

Port (Порт)
В этом раскрывающемся списке представлены порты, которые можно выбрать для этого источника синхронизации.

Priority (Приоритет)
Приоритет для этого источника синхронизации.
Наименьшее число (0) является наивысшим приоритетом.

Если два источника синхронизации имеют одинаковый приоритет, наименьший номер источника синхронизации получает самый высокий приоритет в процессе выбора источника синхронизации.

SSM Overwrite
Выбираемый уровень качества источника синхронизации (QL) для перезаписи любого QL, полученного в SSM. Если QL не получен в SSM (SSM не включен на этом порту), SSL Overwrite QL используется так, как если бы он был получен.

Hold Off (Таймер удержания)
Значение таймера удержания. Активные потери в источнике синхронизации будут удержаны на указанное количество времени.

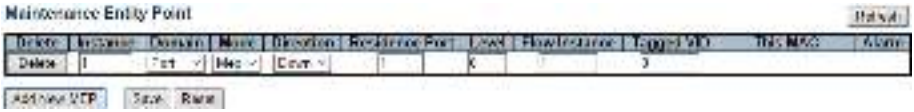
ANEG Mode
Это относится только к портам 1000BaseT. Чтобы восстановить синхронизацию на порте, порты должны быть переведены в режим «Slave». Чтобы распределить синхронизацию, порт должен быть переведен в режим «Master».

SSM
Если SSM включен и не получен должным образом.
Тип сбоя SSM будет указан в поле «Rx SSM».

WTR
Wait to Restore таймер включен.

CLEAR WTR
Очищает таймер WTR и делает источник синхронизации доступным для процесса выбора синхронизации.

10.15 Configuration – MEP (Настройки – MEP)



Delete (Удалить)
Удаление записи MEP при следующем сохранении.

Instance
Идентификатор MEP. Доступные значения 1 – 100.

Mode (режим работы)
- ✓ MEP (Maintenance Entity End Point)
- ✓ MIP (Maintenance Entity Intermediate Point)

Direction (Направление)

- ✓ Down
- ✓ UP

Residence Port

Порт, где MEP осуществляет мониторинг - см. «Direction». Для EVC MEP порт должен быть портом в EVC. Для VLAN MEP порт должен быть участником VLAN.

Level (Уровень)

MEG уровень MEP

This MAC (Этот MAC адрес)

MAC адрес этого MEP – может быть использован другим MEP, если выбран unicast.

Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения

10.16 Configuration – ERPS (Настройки – Протокол ERPS)

На данной странице WEB интерфейса представлены настройки протокола ERPS.

Delete (Удалить)

Удаление записи при следующем сохранении.

ERPS ID (Идентификатор ERPS)

Идентификатор созданной группы защиты. Это должно быть целочисленное значение от 1 до 64. Максимальное число групп защиты ERPS, которое можно создать, составляет 64. Нажмите на

идентификатор группы защиты, чтобы перейти на страницу конфигурации.

Port 0
Создает порт 0 для коммутатора в кольце.

Port 1
Эта настройка создаст «Port 1» для коммутатора в кольце. Поскольку у подключенного субкольца будет только один кольцевой порт, «Port 1» настроен как «0» для подключенного субкольца. «0» в этом поле означает, что «Порт 1» не связан.

Port 0 AF MP
Сообщение о сбое сигнала порта 0 MEP.

Port 1 SF MEP
Сообщение о сбое сигнала порта 1 MEP. Поскольку только один SF MEP связан с взаимосвязанным субкольцом без виртуального канала, он настроен как «0» для таких случаев вызова. «0» в этом поле указывает, что ни один порт 1 MEP SF не связан.

Port 0 APS MEP
Порт 0 APS PDU, обрабатывающий MEP.

Port 1 APS MEP
Порт 1 APS PDU, обрабатывающий MEP. Поскольку только один APS MEP связан с подключенным субкольцом без виртуального канала, он настроен как «0» для таких случаев вызова. «0» в этом поле указывает, что ни один APS MEP порта 1 не связан.

RING Type (Тип кольца)
Тип защитного кольца. Может быть основное кольцо (major ring) или субкольцо (sub-ring)

Interconnecting Node (Взаимосвязанный узел)
Взаимосвязанный узел указывает, что кольцо взаимосвязано. Установите флаг, чтобы настроить этот параметр.

- ✓ «Yes» означает, что для данного экземпляра это взаимосвязанный узел.
- ✓ «No» означает, что настроенный экземпляр не связан

Virtual Channel (Виртуальный канал)
Субкольца могут иметь свой виртуальный канал на взаимосвязанном узле (Interconnecting Node). Это опция настраивается с помощью флага «Virtual Channel».

- ✓ «YES» указывает, что это субкольцо с виртуальным каналом.
- ✓ «NO» означает, что субкольцо не имеет виртуального канала.

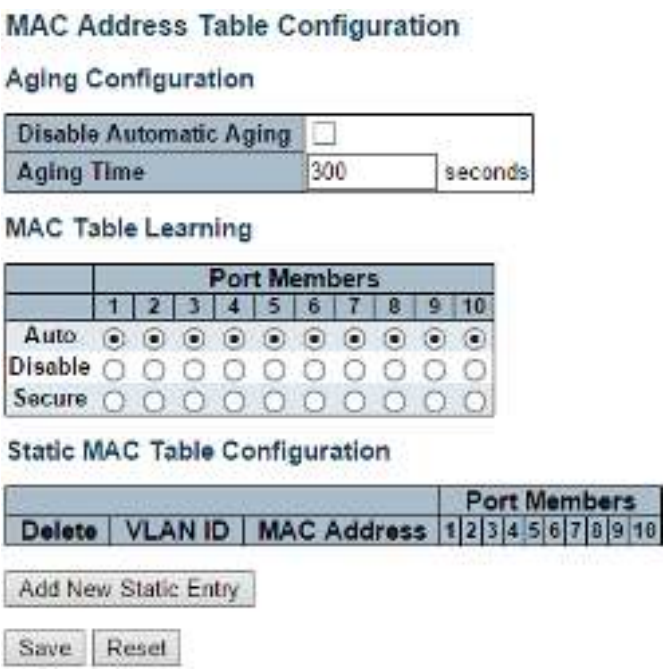
Major Ring ID (Идентификатор основного кольца)
Идентификатор основного кольца для взаимосвязанного субкольца.
Он используется для отправки обновлений об изменениях топологии по основному кольцу. Если кольцо является основным, это значение совпадает с идентификатором группы защиты этого кольца.

Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения

10.17 Configuration – MAC Table (Настройки – Таблица MAC адресов)



На данной странице WEB интерфейса настраивается таблица MAC адресов.

Настройка устаревания MAC адресов

По умолчанию динамические записи удаляются из таблицы MAC через 300 секунд. Это удаление также называется старением (aging).

Настройте время старения, введя значение здесь в секундах. Допустимый диапазон от 10 до 1000000 секунд.

Отключите автоматическое устаревание динамических записей, установив флаг «Disable automatic aging».

Запоминание MAC адресов (Learning)

Если режим learning для данного порта неактивен, другой модуль WEB интерфейса контролирует этот режим, поэтому пользователь не может его изменить.

Примером такого модуля является «MAC-Based Authentication under 802.1X».

Каждый порт может выполнять Learning на основе следующих режимов работы:

- ✓ Auto (Автоматически) – запоминание MAC адресов происходит автоматически, как только получен фрейм с неизвестным SMAC;
- ✓ Disable (Отключено) – запоминание MAC адресов отключено;
- ✓ Secure (Безопасный режим) – только записи из статической таблицы MAC адресов могут быть запомнены. Остальные пакеты будут дропнуты.

Настройка статической таблицы MAC адресов

Статическая таблица MAC может содержать 64 записи.
Предусмотрено максимум 64 записи для всего стека, а не для каждого коммутатора.
Таблица MAC сортируется сначала по идентификатору VLAN, а затем по MAC-адресу.

Delete (Удалить)
Удаление записи при следующем сохранении.

VLAN ID (Идентификатор VLAN)
Идентификатор VLAN соответствующий данной записи.

MAC Address (MAC Адрес)
Поле для ввода MAC адреса

Port Members (Порты участники)
Галочки указывают, какие порты являются участниками записи. Установите или снимите флаг, если необходимо изменить запись

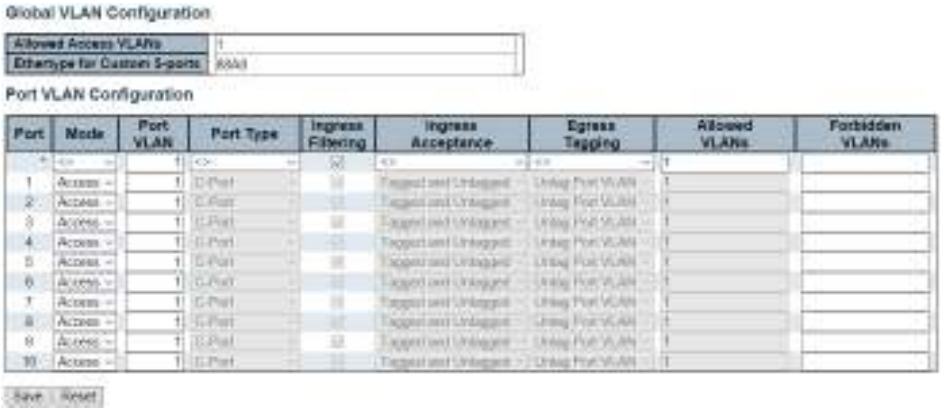
Кнопки:

Adding a New Static Entry – Нажмите, чтобы добавить новую запись в статическую таблицу MAC адресов. Укажите VLAN ID, MAC адрес, нажмите сохранить (Save)

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения

10.18 Configuration – VLANs (Настройки – Настройка VLAN'ов)



На данной странице WEB интерфейса находятся настройки, позволяющие создавать VLANы и гибко их настраивать.

Глобальные настройки VLAN

Allowed Access VLANs
Это поле содержит только разрешенные сети VLAN

Ethertype for Custom S-ports
В этом поле указывается ethertype/TPID (указанный в шестнадцатеричном формате), используемый для отдельно настроенных S-портов. Этот параметр действует для всех портов, для которых в качестве типа порта установлено значение S-Custom-Port.

Настройки VLAN для портов

Port (Порт)
Логический номер порта

Mode (Режим работы)
Режим порта (по умолчанию Access) определяет основное поведение рассматриваемого порта.

Порт может находиться в одном из трех режимов работы. Всякий раз, когда выбирается определенный режим работы, остальные поля в этой строке будут либо выделены серым цветом, либо изменены в зависимости от выбранного режима.

Неактивные (серые) поля содержат значения, которые порт получит, когда режим работы будет применен.

1) Access – access порты обычно используются для подключения к конечным станциям. Динамические функции, такие как Voice VLAN, могут добавить порт к большему количеству VLAN. Порты доступа имеют следующие характеристики:
   - ✓ Участник только одной VLAN, Порт VLAN (или Access VLAN), который по умолчанию равен 1;
   - ✓ Принимает нетегированные фреймы и фреймы с С тегом;
   - ✓ Отбрасывает все фреймы, которые не классифицированы в Access VLAN;
2) Trunk – trunk порты (они же магистральные) могут передавать трафик по нескольким сетям VLAN и обычно используются для подключения к другим коммутаторам. Магистральные порты имеют следующие характеристики:
   - ✓ По умолчанию транковый порт является членом всех VLAN (1-4095);
   - ✓ Сети VLAN, членом которых является trunk порт, могут быть ограничены использованием только Access VLAN;
   - ✓ Фреймы, классифицированные для VLAN, членом которой порт не является, отбрасываются;
   - ✓ По умолчанию все фреймы, кроме фреймов, классифицированных для VLAN порта (например, native VLAN), получают тег на выходе. Фреймы, относящиеся к VLAN-порту, не имеют С-тегов на выходе;

- ✓ Выходной тег можно изменить, чтобы пометить все фреймы, и в этом случае только входные тэги будут приниматься на входе.

3) Hybrid – Гибридные порты во многом напоминают магистральные порты, но обладают дополнительными функциями конфигурирования портов. В дополнение к характеристикам, описанным для магистральных портов, гибридные порты имеют следующие возможности:
   - ✓ Может быть настроен так, чтобы тег VLAN не распознавался, распознавал C-тег, распознавал S-тег или распознавал S-custom-тег
   - ✓ Входную фильтрацию тегов можно контролировать.

Port VLAN (Порт VLAN)

Поле определяет идентификатор VLAN порта (PVID). Допустимые VLAN находятся в диапазоне от 1 до 4095, по умолчанию 1.

Порт VLAN называется «Access VLAN» для портов в режиме «Access», и Native VLAN для портов в магистральном (trunk) или гибридном (hybrid) режиме.

Port Type (Тип порта)

Порты в гибридном режиме (Hybrid) позволяют изменять тип порта:

- ✓ Unaware – на входе все фреймы, независимо от того, несут ли они тег VLAN, классифицируются, как порт VLAN, и возможные теги не удаляются на выходе.
- ✓ C-Port – на входе фреймы с тегом VLAN с TPID = 0x8100 классифицируются по идентификатору VLAN, встроенному в тег. Если фрейм не имеет тег или тегирован как приоритетный, фрейм классифицируется как порт VLAN. Если фреймы должны быть тегированы на выходе, они будут тегированы C-меткой.
- ✓ S-Port – на входе фреймы с тегом VLAN с TPID = 0x8100 или 0x88A8 классифицируются по идентификатору VLAN, встроенному в тег. Если фрейм не имеет тег или тегирован как приоритетный, фрейм классифицируется как порт VLAN. Если фреймы должны быть тегированы на выходе, они будут тегированы S-меткой.
- ✓ S-Custom-Port – на входе фреймы с тегом VLAN с TPID = 0x8100 или равному Ethernet Type, настроенному для портов Custom –

S, классифицируются по идентификатору VLAN, встроенному в тег. Если фрейм не имеет тег или тегирован как приоритетный, фрейм классифицируется как порт VLAN. Если фреймы должны быть тегированы на выходе, они будут тегированы S-меткой.

Ingress Filtering (Входная фильтрация)

Гибридные порты позволяют менять входную фильтрацию. На портах доступа (access port) и магистральных Trunk портах всегда включена входная фильтрация.

Если входная фильтрация включена (флаг установлен), фреймы, классифицированные для VLAN, для которых порт не является участником VLAN, отбрасываются.

Если входная фильтрация отключена (флаг снят), фреймы, классифицированные для VLAN, для которых порт не является участником VLAN, принимаются и пересылаются в коммутационную матрицу. Однако порт никогда не будет передавать кадры, классифицированные для VLAN, членом которых он не является.

Ingress Acceptance

Гибридные порты позволяют изменять тип фреймов, которые принимаются на входе.

- ✓ Tagged and Untagged – фреймы с тэгом и без тэга будут приниматься;
- ✓ Tagged Only – только фреймы с тэгом будут приниматься;
- ✓ Untagged Only – только фреймы без тэга будут приниматься.

Egress Tagging (Тэгирование на выходе)

Порты в trunk и hybrid режимах могут управлять тэгированием фреймов на выходе.

- ✓ Untag Port VLAN – фреймы, относящиеся к Port VLAN, передаются без тегов. Другие фреймы передаются с соответствующим тегом;
- ✓ Tag All – все фреймы, относящиеся к Port VLAN или нет передаются с тегом;
- ✓ Untag All – все фреймы, относящиеся к Port VLAN или нет передаются без тега.

Allowed VLANs (Разрешенные сети VLAN)

Порты в trunk и hybrid режимах могут контролировать, в каких сетях VLAN им разрешено быть участниками. Порты access могут быть только членами одной VLAN – Access VLAN.

Синтаксис поля идентичен синтаксису, используемому в поле Enabled VLANs.

По умолчанию trunk или hybrid порт будет участником всех VLAN, поэтому для него установлено значение 1-4095.

Поле может быть оставлено пустым, что означает, что порт не станет членом каких-либо VLAN.

Forbidden VLANs (Запрещенные VLAN)

Порт может быть настроен так, чтобы никогда не быть участником одной или нескольких VLAN.

Синтаксис идентичен синтаксису, используемому в поле Enabled VLANs.

По умолчанию поле остается пустым, что означает, что порт может стать участником всех возможных сетей VLAN.

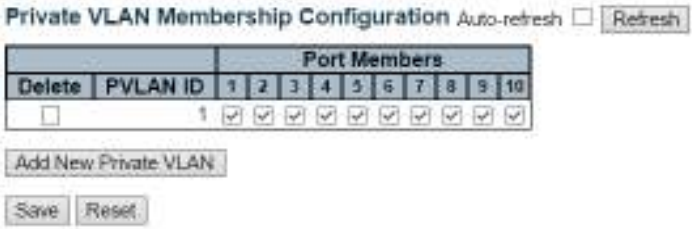
Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения

10.19 Configuration – Private VLANs (Настройки – Частные VLAN сети)

10.19.1 Private VLANs – Membership (Частные VLAN сети – порты участники)



Delete (Удалить)
Отметьте элемент интерфейса, если хотите удалить запись о частной VLAN;

Private VLAN ID (Идентификатор частной VLAN)
Поле определяет идентификатор настраиваемой частной VLAN сети

Port Members (Порты участники Private VLAN)
Перечень чекбоксов для каждого порта. Для того чтобы сделать порт участником частной VLAN необходимо отметить его. Чтобы убрать порт из частной VLAN, снимите выделение.

Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения

Auto Refresh – автоматическое обновление содержимого полей раз в 3 секунды;

Refresh – нажмите, чтобы обновить страницу немедленно.

10.19.2 Private VLANs – Port Isolation (Частные VLAN сети – Изоляция портов)

На данной странице WEB интерфейса представлены настройки функции изоляции портов в частной VLAN. Данная функция работает на весь стек.

Конфигурирование

Port Members (Порты участники)

Чек боксы выбора портов участников частной VLAN, на которых будет включена функция изоляции портов. По умолчанию изоляция портов выключена для всех портов.

Кнопки:

Save – нажмите, чтобы сохранить изменения;

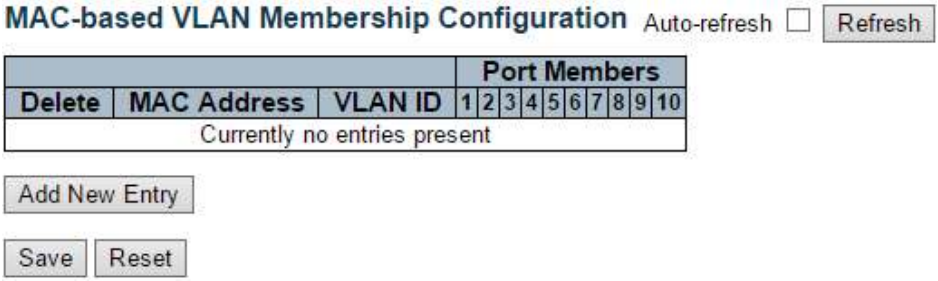
Reset – нажмите, чтобы отменить изменения

Auto Refresh – автоматическое обновление содержимого полей раз в 3 секунды;

Refresh – нажмите, чтобы обновить страницу немедленно.

10.20 Configuration – VCL (Настройки – VCL)

10.20.1 VCL – MAC Based VLAN (VCL – VLAN на базе MAC адреса)



На данной странице WEB интерфейса представлены настройки для записей VLAN на базе MAC адресов.

Delete (Удалить)
Отметьте элемент WEB интерфейса, чтобы удалить запись при следующем сохранении.

MAC Address (MAC Адрес)
Поле отображает MAC адрес.

VLAN ID (Идентификатор VLAN)
Поле отображает идентификатор VLAN (VLAN ID)

Port Members (Порты – участники)
Перечень чекбоксов для каждого порта отображается для каждой записи «VLAN на базе MAC адресов».

Чтобы добавить порт в VLAN на основе MAC адреса необходимо установить флаг в соответствующем чекбоксе.

По умолчанию ни один порт не является членом VLAN на базе MAC адресов.

Кнопки:

Adding a NEW MAC-based VLAN – добавить новую запись

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения

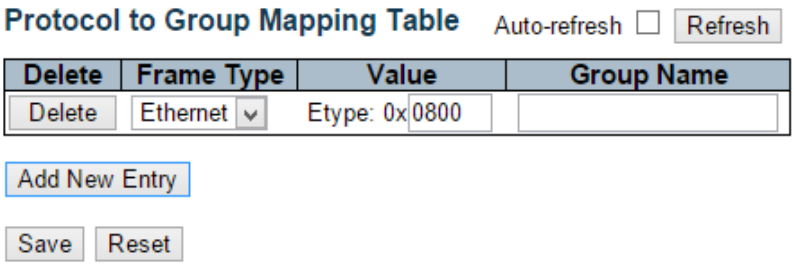
Auto Refresh – автоматическое обновление содержимого полей раз в 3 секунды;

Refresh – нажмите, чтобы обновить страницу немедленно;

<< – обновление таблицы, начиная с первой записи;

>> – обновление таблицы, начиная с записи после последней отображаемой записи.

10.20.2 VCL – Port Based VLAN (VCL – VLAN на базе портов)



На данной странице WEB интерфейса представлены настройки, позволяющие добавлять новые протоколы к записи сопоставления Группового Имени (Group Name), а также просматривать и удалять ранее сопоставленные записи для коммутатора в стеке.

Delete (Удалить)
Чтобы удалить запись при следующем сохранении, отметьте чекбокс.

Frame Type (Тип фрейма)
Тип фрема может принимать одно из следующих значений:

- ✓ Ethernet;
- ✓ LLC;
- ✓ SNAP.

Value (Допустимые значения)
Допустимое значение, которое можно ввести в это текстовое поле, зависит от параметра, выбранного в предыдущем меню выбора «Тип фрейма».

1) Если выбран тип фрейма Ethernet. Значения в текстовом поле, когда в качестве Типа фрейма выбран Ethernet, называются etype. Допустимые значения для etype составляют от 0x0600-0xffff
2) Если выбран тип фрейма LLC. Допустимое значение в этом случае состоит из двух разных значений:
    a. DSAP – строка длиной 1 байт (0x00-0xff);
    b. SSAP – строка длиной 1 байт (0x00-0xff).
3) Если выбран тип фрейма SNAP. Допустимое значение в этом случае состоит из двух разных значений:
    a. OUI – это значение в формате xx-xx-xx, где каждая пара (xx) в строке представляет собой шестнадцатеричное значение в диапазоне от 0x00-0xff.
    b. PID – если OUI имеет шестнадцатеричное значение 000000, идентификатор протокола – EtherType для протокола, работающего поверх SNAP.

Group Name (Групповое Имя)
Групповое имя это уникальная 16 символьная строка, которая может состоять из символов алфавита (a-z A-Z) и цифр (0-9). Специальные символы и нижнее подчеркивание (_) не поддерживаются.

Кнопки:

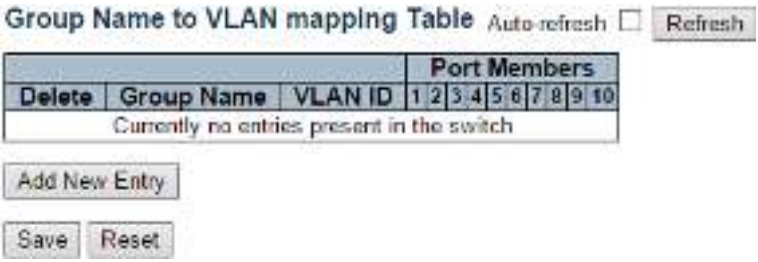
Adding a NEW entry – добавить новую запись

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения

Auto Refresh – автоматическое обновление содержимого полей раз в 3 секунды;

Refresh – нажмите, чтобы обновить страницу немедленно;



Delete (Удалить)
Чтобы удалить запись при следующем сохранении, отметьте чекбокс.

Group Name (Групповое Имя)
Групповое имя это уникальная 16 символьная строка, которая может состоять из символов алфавита (a-z A-Z) и цифр (0-9). Специальные символы и нижнее подчеркивание (_) не поддерживаются.

Независимо от того, какое имя группы вы пытаетесь сопоставить с VLAN, оно должно присутствовать в таблице сопоставления протокола и группы и не должно быть предварительно использовано любой другой существующей записью сопоставления на этой странице.

VLAN ID (Идентификатор VLAN)
Указывает идентификатор, которому будет сопоставлено имя группы. Допустимый идентификатор VLAN может быть от 1 до 4095.

Port Members (Порты – участники)
Выделите порты-участники сопоставления группового имени с идентификатором VLAN.

Чтобы удалить или исключить порт из сопоставления, убедитесь, что флаг снят. По умолчанию порты не являются участниками сопоставления группового имени и VLAN.

Кнопки:

Adding a NEW entry – добавить новую запись

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения

Auto Refresh – автоматическое обновление содержимого полей раз в 3 секунды;

Refresh – нажмите, чтобы обновить страницу немедленно;

На данной странице WEB интерфейса есть возможность настроить записи VLAN на основе IP-подсети.

Эта страница позволяет добавлять, обновлять и удалять записи VLAN на основе IP-подсети и назначать записи различным портам. Эта страница показывает только статические записи.

Delete (Удалить)
Чтобы удалить запись при следующем сохранении, отметьте чекбокс.

VCE ID
Поле отображает индекс записи. Значение может быть в пределах от 0-128

IP Address (IP Адрес)
Поле отображает IP адрес

Mask Length (Маска)
Поле отображает маску подсети

VLAN ID (Идентификатор VLAN)
Поле отображает идентификатор VLAN (VID). VID может быть изменен для существующей записи.

Port Members (Порты участники)
Перечень чекбоксов, позволяющих отметить порты-участники VLAN на базе IP адресов. По умолчанию флаги сняты со всех портов.

Кнопки:

Adding a NEW entry – добавить новую запись

Save – нажмите, чтобы сохранить изменения;

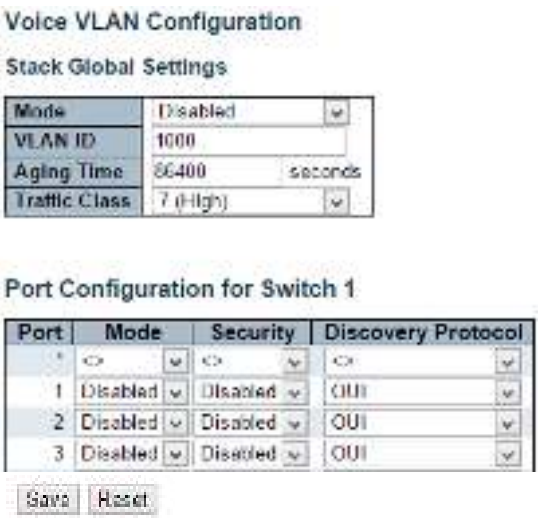
Reset – нажмите, чтобы отменить изменения

Auto Refresh – автоматическое обновление содержимого полей раз в 3 секунды;

Refresh – нажмите, чтобы обновить страницу немедленно;

10.21 Configuration – Voice VLAN (Настройки – Голосовые VLAN)

10.21.1 Voice VLAN – Configuration (Голосовые VLAN – Настройка)



На данной странице есть возможность сконфигурировать голосовую VLAN для передачи голосового трафика.

Mode (Режим работы)
Элемент контролирует работу в режиме Voice VLAN. Функция MSTP должна быть отключена, прежде чем будет включена функция Voice VLAN.

- ✓ Enabled – включение режима Voice VLAN;
- ✓ Disabled – выключение режима Voice VLAN.

VLAN ID (Идентификатор VLAN)
Поле отображает идентификатор голосовой сети VLAN (Voice VLAN).

Это должен быть уникальный идентификатор VLAN в системе, и он не может быть равен PVID порта.

Это конфликт конфигурации, если значение равно VID управления, MVR VID, PVID и т. Д. Допустимый диапазон от 1 до 4095.

Aging Time (Период Устаревания)
Поле отображает время устаревания Voice VLAN информации. Допустимый диапазон от 10 до 10000000 секунд.

Traffic Class (Класс трафика)
Поле отображает класс трафика для Voice VLAN. Весь трафик Voice VLAN будет классифицирован согласно этого класса.

Port Mode (Режим работы порта)
Поле отображает режим работы Voice VLAN для портов.
Возможные режимы:

- ✓ Disabled – отключить порт от Voice VLAN;
- ✓ Auto – включить режим автоопределения;
- ✓ Forced – Быстрое включение порта в Voice VLAN

Port Security (Безопасность порта)
Поле отображает режим безопасности порта Voice VLAN. Когда функция включена, все не телефонные MAC-адреса в Voice VLAN будут заблокированы на 10 секунд. Возможные режимы порта:

- ✓ Enabled – режим безопасности включен;
- ✓ Disabled – режим безопасности выключен.

Port Discovery Protocol (Протокол обнаружения портов)
Поле отображает протокол обнаружения порта голосовой VLAN.

Он будет работать только при включенном режиме автоопределения.

Функция LLDP должна быть включена перед настройкой протокола обнаружения на «LLDP» или «Both».

Изменение протокола обнаружения на «OUI» или «LLDP» перезапустит процесс автоопределения. Возможные протоколы обнаружения:

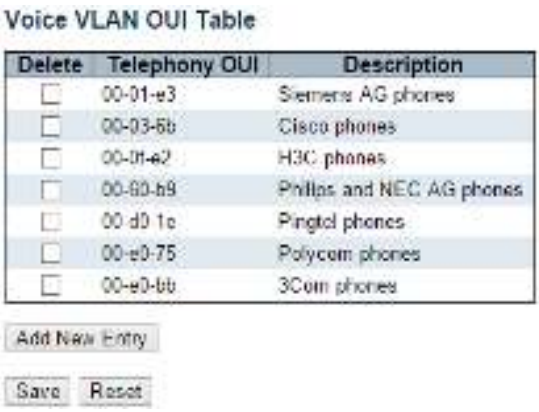
- ✓ OUI – определение телефонного устройства по OUI адресу;
- ✓ LLDP – определение телефонного устройства по LLDP протоколу;
- ✓ Both – определение телефонного устройства по OUI и LLDP вместе.

Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения

10.21.2 Voice VLAN – OUI (Голосовые VLAN – OUI)



На данной странице WEB интерфейса настраивается таблица Voice VLAN OUI. Максимальное количество записей – 16.

Delete (Удалить)
Удаление записи при следующем сохранении

Telephony OUI
Адрес OUI телефонии - это глобальный уникальный идентификатор, назначенный вендору IEEE. Длина должна быть 6 символов, а формат ввода - «xx-xx-xx» (x - шестнадцатеричная цифра).

Description (Описание)
Описание адреса OUI. Это поле содержит описание, к какому устройству телефонии вендора принадлежит адрес. Допустимая длина строки - от 0 до 32.

Кнопки:

Adding a NEW entry – добавить новую запись

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения

10.22 Configuration – QoS (Настройки – QoS)

10.22.1 QoS – Port Classification (QoS – Классификация портов)

На данной странице WEB интерфейса представлены настройки QoS классификации трафика для портов коммутатора.

Port (порт)
Номер порта, к которому будут применены дальнейшие настройки

CoS (Класс обслуживания)
Все фреймы классифицируются CoS. Предусмотрено однозначное соответствие между CoS, очередью (quenue), и приоритетом (priority). CoS 0 обладает самым низким приоритетом.

Если порт поддерживает VLAN, фрейм тегируется и Tag Class. активируется, затем фрейм классифицируется с помощью CoS, который получается из значения PCP и DEI в теге. В противном случае фрейм классифицируется, как CoS по умолчанию.
Классифицированный CoS может быть отменен записью QCL.

Примечание. Если CoS по умолчанию был динамически изменен, то фактический CoS по умолчанию отображается в скобках после настроенного CoS по умолчанию.

DPL
Опция управляет уровнем приоритета отбрасывания (drop precedence level) по умолчанию.
Все кадры классифицируются, как DPL

Если порт поддерживает VLAN, фрейм тегируется и Tag Class. активируется, затем фрейм классифицируется, как DPL, который получается из значения PCP и DEI в теге. В противном случае фрейма классифицируется на DPL по умолчанию.

Классифицированный DPL может быть отменен записью QCL.

PCP
Опция управляет значением PCP по умолчанию.
Все кадры классифицируются по значению PCP.

Если порт поддерживает VLAN и фрейм тегирован, то этот фрейм классифицируется по значению PCP в теге.

В противном случае фрейм классифицируется, как PCP value по умолчанию.

DEI

Управляет значением DEI по умолчанию.

Все кадры классифицируются по значению DEI.

Если порт поддерживает VLAN и фрейм помечен, то он классифицируется по значению DEI в теге.

В противном случае фрейм классифицируется на значение DEI по умолчанию.

Address Mode (Адресный режим)

Режим IP/MAC-адреса, определяющий, должна ли классификация QCL основываться на исходных адресах (SMAC/SIP) или адресах назначения (DMAC/DIP) на этом порту.

Допустимые значения:

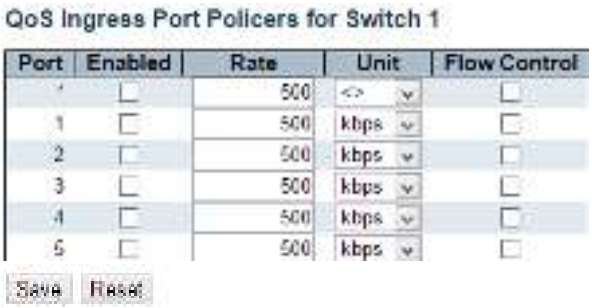
- ✓ Source – Включить сопоставление SMAC / SIP;
- ✓ Destination – Включить сопоставление DMAC / DIP

Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения

10.22.2 QoS – Port Policing (QoS – Классификация портов)



На данной странице WEB интерфейса представлены настройки функции Policer (ограничитель) для портов коммутатора.

Port (порт)
Номер порта, к которому будут применены дальнейшие настройки

Enabled (Включить)
Опция глобально управляет включением функции Policer на выбранном порте коммутатора.

Rate (Диапазон)
В данном поле задается скорость для функции Policer. По умолчанию – 500.

Это значение ограничено 100-1000000, если в качестве единиц измерения (Unit) выбраны «Кбит/с» или «FPS».

Если в качестве единицы измерения выбрано «Мбит/с» или «kfps», то значение Rate можно изменять в диапазоне от 1 – 13200.

Unit (Единицы измерения)
Из выпадающего списка есть возможность выбрать единицы измерения для поля Rate. Это могут быть «kbps», «Mbps», fps, kfps. Значение по умолчанию – «Кбит/с»

Flow Control (Управление потоком)
Если управление потоком включено и порт находится в этом режиме, то фреймы паузы отправляются вместо отбрасывания фреймов.

Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения

10.22.3 QoS – Port Scheduler (QoS – Планировщик портов)

QoS Egress Port Schedulers for Switch 1

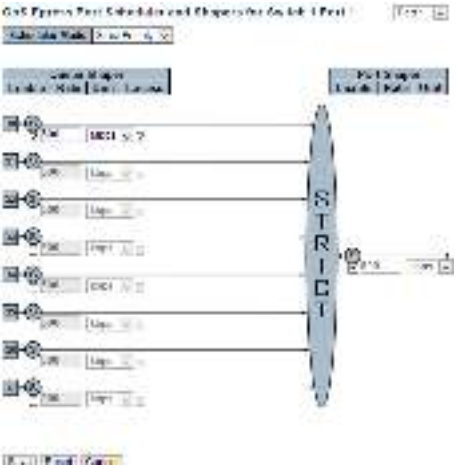
Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-

На данной странице WEB интерфейса находятся инструменты для управления планировщиками портов.

Port (Порт)
Номер порта, к которому будут применены дальнейшие настройки.

Mode (Режим работы)
Режим работы планировщика для выбранного порта.

Qn
Поле отображает «вес» для выбранной очереди и порта.



Sheduler Mode (Режим работы планировщика)
Инструмент управляет режимом работы планировщика:

- ✓ Strict Priority – строгий приоритет;
- ✓ Weighted – на основе «веса».

Queue Shaper Enable (Shaper Queue включить)
Инструмент управляет включением функции Shaper Queue для выбранной очереди на этом порте коммутатора.

Queue Shaper Rate (Диапазон скорости для Queue Shaper)
Инструмент управляет скоростью функции Queue Shaper
По умолчанию – 500.

Это значение ограничено 100-1000000, если в качестве единиц измерения (Unit) выбраны «Кбит/с».

Если в качестве единицы измерения выбрано «Мбит/с», то значение Queue Shaper Rate можно изменять в диапазоне от 1 – 13200.

Queue Shaper Unit (Единицы измерения для Queue Shaper Rate)
Из выпадающего списка есть возможность выбрать единицы измерения для поля Queue Shaper Rate. Это могут быть «kbps», «Mbps»
Значение по умолчанию – «Кбит/с»

Queue Shaper Excess
Инструмент управляет разрешением очереди использовать избыточную пропускную способность.

Queue Scheduler Weight
Инструмент управляет назначением «веса» для этой очереди. Значением по умолчанию является «17». Это значение ограничено 1-100.

Этот параметр отображается только в том случае, если «Scheduler Mode» установлен на «Weighted».

Queue Scheduler Percent
Поле отображает «вес» в процентах для этой очереди.

Этот параметр отображается только в том случае, если «Scheduler Mode» установлен на «Weighted».

Port Shaper Enable (Port Shaper включить)
Инструмент управляет включением функции Port Shaper для выбранного порта коммутатора.

Port Shaper Rate (Диапазон скорости для Port Shaper Rate)
Инструмент управляет скоростью функции Port Shaper Rate
По умолчанию – 500.

Это значение ограничено 100-1000000, если в качестве единиц измерения (Unit) выбраны «Кбит/с».

Если в качестве единицы измерения выбрано «Мбит/с», то значение Queue Shaper Rate можно изменять в диапазоне от 1 – 13200.

Port Shaper Unit (Единицы измерения для Port Shaper Rate)
Из выпадающего списка есть возможность выбрать единицы измерения для поля Port Shaper Rate. Это могут быть «kbps», «Mbps»
Значение по умолчанию – «Кбит/с»

Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения

Cancel – нажмите, чтобы отменить все изменения и вернуться на предыдущую страницу.

10.22.4 QoS – Port Shaping

QoS Egress Port Shapers for Switch 1

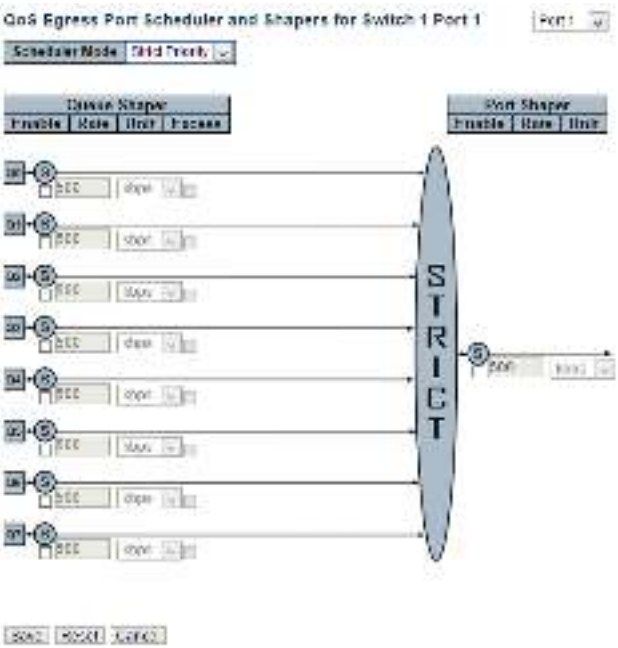
Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

На этой странице WEB интерфейса представлены инструменты для управления функцией Shaper для всех портов коммутатора.

Port (Порт)
Номер порта, к которому будут применены дальнейшие настройки.

Qn
Поле отображает «Disabled» (Отключено) или фактическую скорость функции Shaper для очереди, например «800 Mbps»

Port
Поле отображает «Disabled» (Отключено) или фактическую скорость функции Shaper для порта, например «800 Mbps»



На этой странице WEB интерфейса представлена возможность настроить планировщик и функцию Shaper для определенного порта. Настройки относятся к текущему выбранному стековому блоку

Sheduler Mode (Режим работы планировщика)
Инструмент управляет режимом работы планировщика для выбранного порта:

- ✓ Strict Priority – строгий приоритет;
- ✓ Weighted – на основе «веса».

Queue Shaper Enable (Shaper Queue включить)
Инструмент управляет включением функции Shaper Queue для выбранной очереди на этом порте коммутатора.

Queue Shaper Rate (Диапазон скорости для Queue Shaper)
Инструмент управляет скоростью функции Queue Shaper
По умолчанию – 500.

Это значение ограничено 100-1000000, если в качестве единиц измерения (Unit) выбраны «Кбит/с».

Если в качестве единицы измерения выбрано «Мбит/с», то значение Queue Shaper Rate можно изменять в диапазоне от 1 – 13200.

Queue Shaper Unit (Единицы измерения для Queue Shaper Rate)
Из выпадающего списка есть возможность выбрать единицы измерения для поля Queue Shaper Rate. Это могут быть «kbps», «Mbps»
Значение по умолчанию – «Кбит/с»

Queue Shaper Excess
Инструмент управляет разрешением очереди использовать избыточную пропускную способность.

Queue Scheduler Weight
Инструмент управляет назначением «веса» для этой очереди. Значением по умолчанию является «17». Это значение ограничено 1-100.

Этот параметр отображается только в том случае, если «Scheduler Mode» установлен на «Weighted».

Queue Scheduler Percent
Поле отображает «вес» в процентах для этой очереди.

Этот параметр отображается только в том случае, если «Scheduler Mode» установлен на «Weighted».

Port Shaper Enable (Port Shaper включить)
Инструмент управляет включением функции Port Shaper для выбранного порта коммутатора.

Port Shaper Rate (Диапазон скорости для Port Shaper Rate)
Инструмент управляет скоростью функции Port Shaper Rate
По умолчанию – 500.

Это значение ограничено 100-1000000, если в качестве единиц измерения (Unit) выбраны «Кбит/с».

Если в качестве единицы измерения выбрано «Мбит/с», то значение Queue Shaper Rate можно изменять в диапазоне от 1 – 13200.

Port Shaper Unit (Единицы измерения для Port Shaper Rate)
Из выпадающего списка есть возможность выбрать единицы измерения для поля Port Shaper Rate. Это могут быть «kbps», «Mbps»
Значение по умолчанию – «Кбит/с»

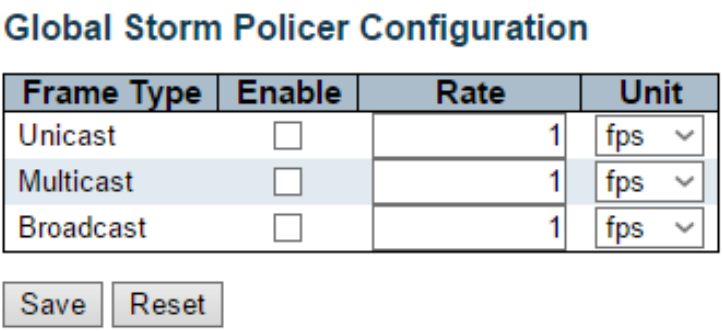
Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения

Cancel – нажмите, чтобы отменить все изменения и вернуться на предыдущую страницу.

10.22.5 QoS – Storm Policing



На данной странице WEB интерфейса представлены глобальные настройки функции Storm Policer.

Frame Type (Тип фреймов)
Тип фреймов, для которого применяются остальные настройки;

Enable (Включить)
Включение/Выключение функции Global Storm Policer для данного типа фреймов.

Rate (Диапазон)
Инструмент отвечает за скорость работы функции Global Storm Policer.

Значение 1-1024000, если в поле Unit выбраны единицы измерения «fps» (фреймов в сек) или 1-1024, если в поле Unit выбраны единицы измерения «kfps» (тысяч фреймов в сек).

Скорость округляется до ближайшего значения, поддерживаемого функцией Global Storm Policer.

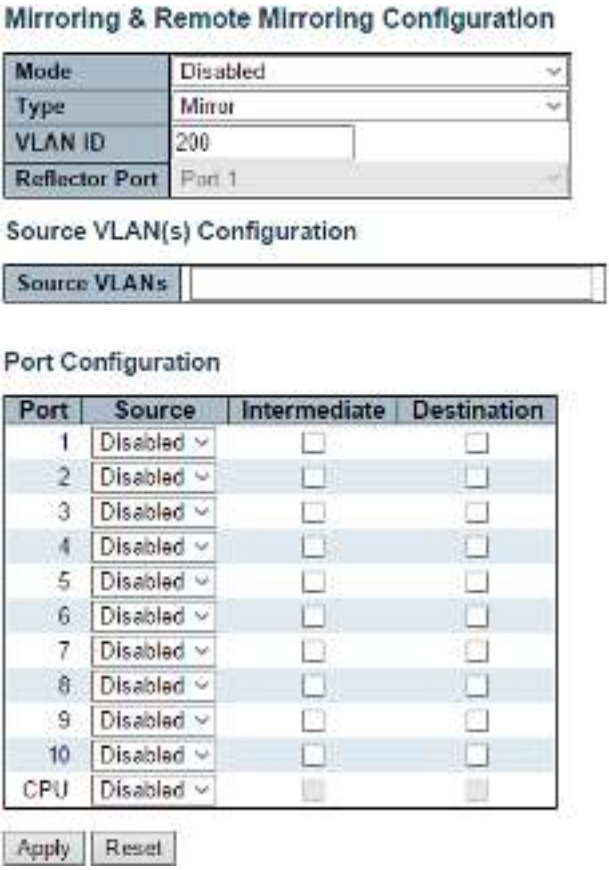
Unit (Единицы измерения)
Единицы измерения для диапазона скоростей функции Global Storm Policer. Возможные варианты «fps» (фреймов/с), «kfps» (тысяч фреймов в сек).

Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения

10.23 Configuration – Mirroring (Настройки – Зеркалирование портов)



Зеркалирование это полезный инструмент для анализа трафика на портах. Администратор сети может отлавливать ошибки с помощью зеркалирования трафика. Если есть необходимость тегировать зеркалированный трафик, вы можете настроить VLAN, как «Tag all» (тегировать все) на порте, куда будет отзеркален трафик.

Mirror (Зеркальный режим)
Настройка отвечает за работу коммутатора в режиме зеркала.
Исходный порт и порт назначения принадлежат этому коммутатору.

Source (Исходный порт)
Коммутатор является исходным узлом для трафика, подлежащего мониторингу.
Порт(ы) источника, порт отражателя и промежуточный порт(ы) принадлежат этому коммутатору.

Intermediate (Промежуточный узел)
Коммутатор является узлом пересылки для трафика, подлежащего мониторингу.

Цель промежуточного узла состоит в том, чтобы перенаправить трафик с исходного коммутатора на коммутатор назначения.

Destination (Порт назначения)

Коммутатор является конечным узлом для мониторинга трафика.

Порт(ы) назначения и порт(ы) промежуточного звена расположены на этом коммутаторе.

VLAN ID (Идентификатор VLAN)
Идентификатор сети VLAN отвечает за то, куда будет скопирован пакет трафика для мониторинга. ID VLAN по умолчанию - 200.

Reflector Port (Порт-отражатель)
Порт–отражатель используется для перенаправления трафика в удаленную зеркальную сеть VLAN.

Любое устройство, подключенное к порту, установленному в качестве порта - отражателя, теряет связь, пока удаленное зеркалирование не будет отключено.

- ✓ *Примечание 1*: Порт-отражатель необходимо выбирать только на коммутаторе – источнике.
- ✓ *Примечание 2*: Порт-отражатель должен быть настроен с отключенными функциями STP и MAC Table Learning.
- ✓ *Примечание 3*: Порт отражателя поддерживает только медные порты (оптическое подключение исключено)

Настройка VLANов источника.

Коммутатор может поддерживать зеркалирование на основе VLAN. Если вы хотите контролировать отдельные VLAN на коммутаторе, вы можете настроить выбранные VLAN в этом поле.

Настройка порта для дистанционного зеркалирования

Port (Порт)
Логический номер порта для дальнейшей настройки

Source (Источник)
Выбор режима зеркалирования.

- ✓ Disabled – принимаемые и передаваемые фреймы не зеркалируются;
- ✓ Both – зеркалируются как передаваемые, так и принимаемые кадры;
- ✓ Rx only – фреймы, принятые на этом порте зеркалируются (копируются) на промежуточном порте / порте назначения. Передаваемые фреймы не зеркалируются;
- ✓ Tx only – фреймы, передаваемые с этого порта зеркалируются (копируются) на промежуточном порте / порте назначения. Принимаемые фреймы не зеркалируются;

Intermediate (Промежуточный порт)
Выбор промежуточного порта.

Этот чекбокс предназначен специально для режима дистанционного зеркалирования.

Промежуточный порт является коммутируемым и предназначен для подключения к другому коммутатору.
На промежуточном порте необходимо отключить запоминание MAC адресов (MAC learning) в соответствующем разделе.

Destination (Порт назначения)
Выбор порта назначения.

Этот чекбокс предназначен специально для режима дистанционного зеркалирования.

Порт назначения – порт на который будет принят отзеркаленный (скопированный) трафик с порта источника (source).

На порте назначения необходимо отключить запоминание MAC адресов (MAC learning) в соответствующем разделе.

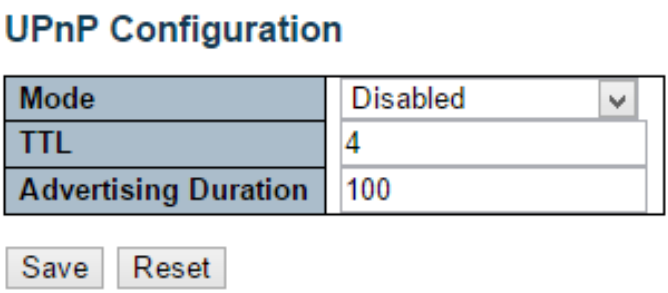
В режиме зеркалирования устройство поддерживает только один порт назначения.

Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения

10.24 Configuration – UPnP (Настройки – UPnP)



На данной странице WEB интерфейса представлены настройки для UPnP – Universal Plug and Play – набора сетевых протоколов для автоматической универсальной настройки сетевых устройств.

Mode (Режим работы)
Выбор режима поддержки UPnP

- ✓ Enabled – включена поддержка работы с UPnP;
- ✓ Disabled – отключена поддержка работы с UPnP

Когда выбран режим работы «Enabled», два ACE добавляются автоматически, чтобы перехватывать связанные с UPNP пакеты в CPU. ACE автоматически удаляются при отключении режима.

TTL (Время «жизни»)
Значение TTL используется UPnP для отправки advertising сообщений SSDP. Допустимые значения находятся в диапазоне от 1 до 255.

Advertising Duration (Длительность advertising)
Длительность, передаваемая в пакетах SSDP, используется для информирования контрольной точки или контрольных точек о том, как часто она или они должны получать advertising сообщение SSDP от этого коммутатора.

Если контрольная точка не получит ни одного сообщения в течение времени, она будет считать, что коммутатор больше не подключен.

Из-за использования UDP в стандарте рекомендуется, чтобы такое обновление advertising сообщений выполнялось менее чем на половине значения «Advertising Duration».

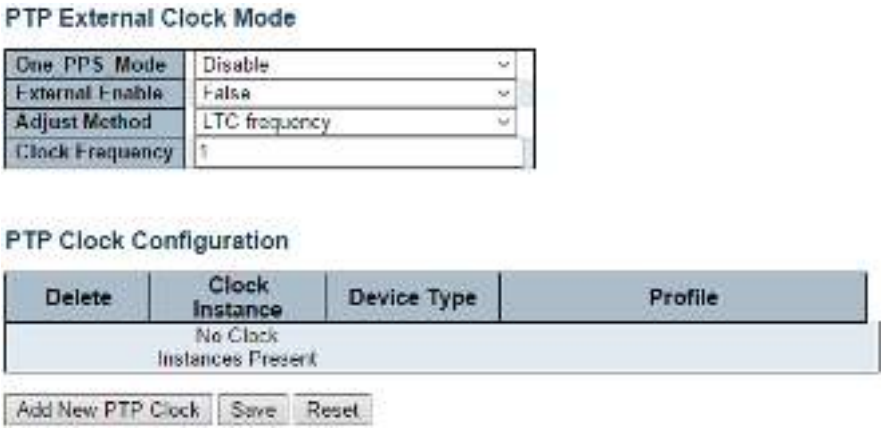
Допустимые значения находятся в диапазоне от 100 до 86400.

Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения

10.25 Configuration – PTP (Настройки – PTP)



На данной странице WEB интерфейса представлены настройки PTP – протокола точного времени.

Настройка внешних часов PTP

One_PPS_Mode
Поле отвечает за выбор окнфигурации One_pps_mode.

External Enable
Данное поле отвечает за настройку External Clock output

- ✓ True – External Clock output включен;
- ✓ False – External Clock output выключен

Adjust Method (Метод настройки)
Данное поле отвечает за настройку частоты (Frequency adjustment)

- ✓ LTC frequency – Выбор частоты локального счетчика времени (LTC).
- ✓ SyncE-DPLL – Выбор контроля частоты SyncE DPLL, если разрешено SyncE.
- ✓ Oscillator – Выбор генератора, независимого от SyncE для управления частотой, если поддерживается HW.
- ✓ LTC phase – Выбор управления фазой локального счетчика времени (LTC) (предполагается, что частота заблокирована с помощью SyncE)

Clock Frequency (Тактовая частота)
Допустимый диапазон значений 1 – 25000000 (1 – 25 МГц)

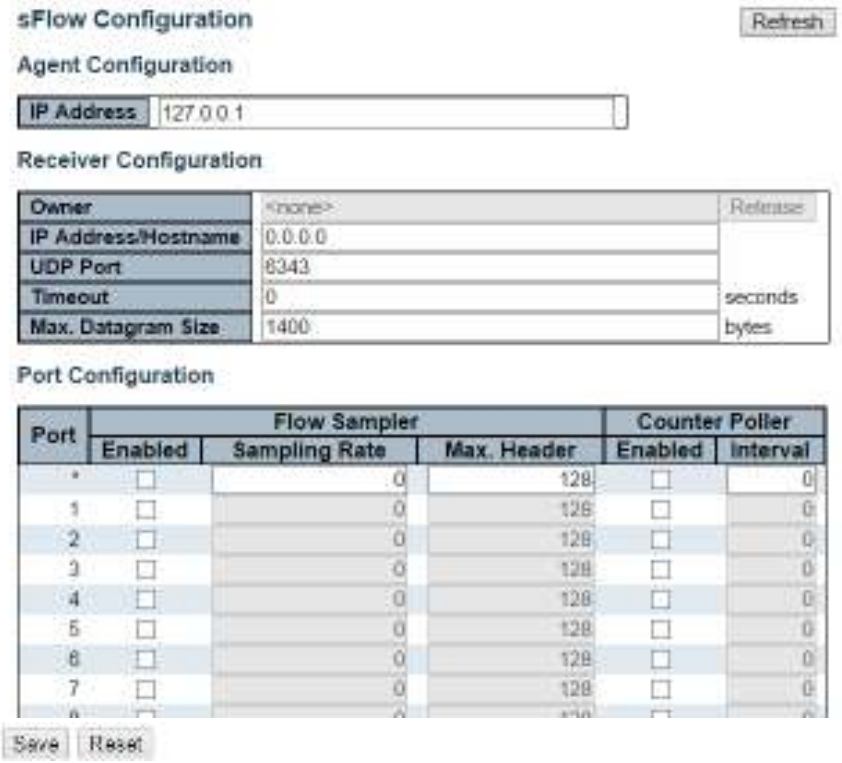
Кнопки:

Add New PTP Clock – добавить новые часы;

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения

10.26 Configuration – sFlow (Настройки – sFlow)



На данной странице WEB интерфейса представлены настройки функции sFlow – инструмент для мониторинга компьютерных сетей, беспроводных сетей и сетевых устройств.

Настройка агента

IP Address (IP адрес)
IP-адрес, используемый в качестве IP-адреса агента в дейтаграммах sFlow.

Он служит уникальным ключом, который будет идентифицировать этого агента в течение длительных периодов времени.
IPv4 и IPv6 адреса поддерживаются.

Настройка получателя

Owner (Владелец)
sFlow можно настроить двумя способами: через локальное управление через веб-интерфейс или интерфейс командной строки или через SNMP.

Это поле только для чтения показывает владельца текущей конфигурации sFlow и принимает значения следующим образом:

- ✓ Если sFlow в настоящее время не настроен / не востребован, поле владельца принимает значение <none>;
- ✓ Если sFlow настроен через WEB или CLI, поле владельца принимает значение <Configured through local management >;
- ✓ Если sFlow настроен через SNMP, поле владельца принимает значение, идентифицирующее получателя sFlow;

Если sFlow настроен через SNMP, все элементы управления - кроме кнопки Release - отключены, чтобы избежать случайной реконфигурации.

IP Address/Hostname (IP адрес / имя хоста)
IP адрес или имя хоста – получателя sFlow. Поддерживаются IPv4 и IPv6.

UDP Port (UDP порт)
Номер UDP порта, который прослушивается sFlow получателем. Если установлено значение «0», то используется порт по умолчанию (6343).

Timeout
Количество секунд, оставшееся до освобождения текущего владельца sFlow. Во время активности текущее оставшееся время может быть обновлено нажатием кнопки «Обновить».

При локальном управлении время ожидания может быть изменено на лету, не влияя на другие настройки.

Max. Datagram Size (Макс. размер дейтаграммы)
Максимальное количество байтов данных, которое может быть отправлено в одной дейтаграмме.

Допустимый диапазон от 200 до 1468 байт, по умолчанию 1400 байт.

Настройка портов

Port (Порт)
Номер порта, к которому будут применены дальнейшие настройки

Flow Sampler Enabled (Выборка потока)
Настройка включает/отключает выборку потока на этом порте

Flow Sampler Sampling Rate (Частота выборки)
Частота статистической выборки для пакетной выборки.

Установите значение N для выборки в среднем 1 / N-й пакетов, переданных / полученных по порту.

Не все частоты дискретизации достижимы. Если запрашивается неподдерживаемая частота дискретизации, коммутатор автоматически подстраивает ее до максимально возможного уровня.

Flow Sampler Max. Header (максимальный размер заголовка)
Максимальное количество байтов, которое должно быть скопировано из выборочного пакета в дейтаграмму sFlow.

Допустимый диапазон от 14 до 200 байт, по умолчанию 128 байт. Если максимальный размер дейтаграммы не учитывает максимальный размер заголовка, выборки могут быть отброшены.

Counter Poller Enabled (Счетчик опросов)
Включение/отключение счетчика опросов для выбранного порта

Counter Poller Interval (Интервал срабатывания счетчика опросов)
При включенном счетчике опроса (Counter Poller) указывается интервал (в секундах) между выборками счетчика.

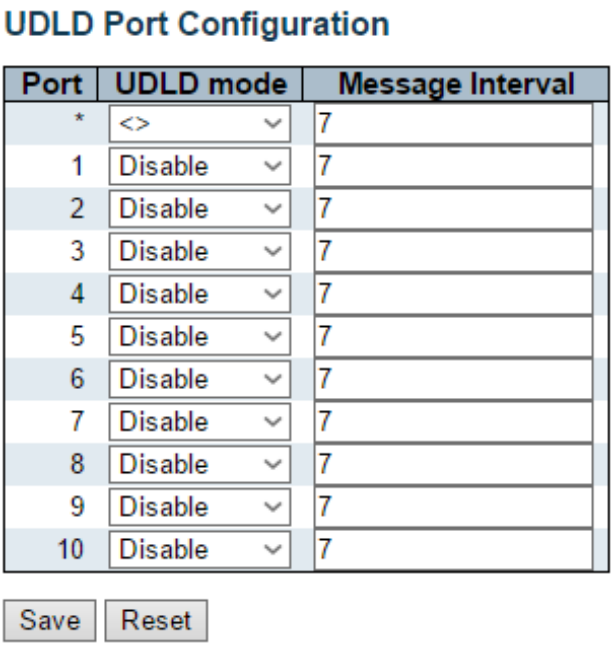
Кнопки:

Refresh – нажмите, чтобы обновить страницу. Несохраненные значения будут утеряны;

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения

10.27 Configuration – UDLD (Настройки – UDLD)



На данной странице WEB интерфейса представлены настройки для UDLD – протокола фирмы Cisco, необходимый для отслеживания состояния fiber портов, а также некорректной коммутации, когда Tx и Rx перепутаны.

Port (Порт)
Номер порта коммутатора

UDLD Mode (Режим работы UDLD)
Настройка UDLD на порте. Возможные значения:

- ✓ Disable – поддержка UDLD отключена на порте;
- ✓ Normal – в этом режиме, если состояние канала порта было определено как однонаправленное, это не повлияет на состояние порта.
- ✓ Aggressive – в этом режиме обнаруженные однонаправленные порты отключатся. Чтобы восстановить порты, необходимо отключить UDLD на этом порту.

Message Interval (Интервал отправки сообщений)
Поле отвечает за настройку периода между сообщениями UDLD на портах, которые находятся в фазе advertising и определяются как двунаправленные.

Диапазон составляет от 7 до 90 секунд (значение по умолчанию - 7 секунд).

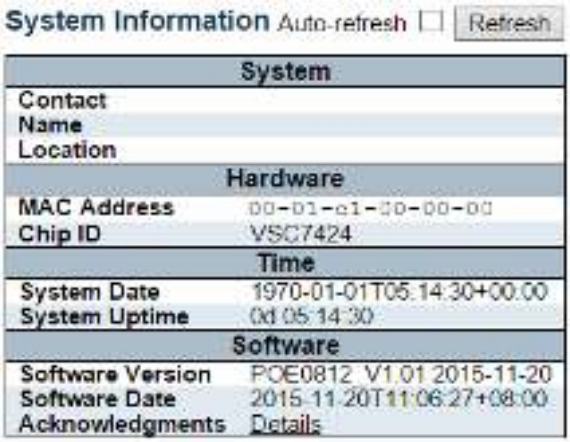
Кнопки:

Save – нажмите, чтобы сохранить изменения;

Reset – нажмите, чтобы отменить изменения

10.28 Monitor – System (Мониторинг – Система)

10.28.1 System – Information (Система – Общая информация)



На данной странице WEB интерфейса представлена общая сводная системная информация.

Contact (Контактная информация)
Контактная информация, настроенная в разделе Configuration | System | Information | System Contact

Name (Имя)
Системное имя, настроенное в разделе Configuration | System | Information | System Name

Location (Месторасположение)
Месторасположение системы, заданное в разделе Configuration | System | Information | System Location

MAC Address (MAC Адрес)
MAC адрес коммутатора

System Date (Системная дата и время)
Текущая системная дата и время (GMT). Значения для этого поля берутся с сервера синхронизации, запущенного на коммутаторе, если таковой настроен.

System Uptime (Время работы системы)
Время, в течение которого коммутатор не был выключен и продолжал работу.

Switch ID (Идентификатор коммутатора)
Идентификатор коммутатора

Chip ID (Идентификатор чипа)
Идентификатор главного чипа

Software Version (Версия прошивки)
Версия прошивки, установленной на коммутатор

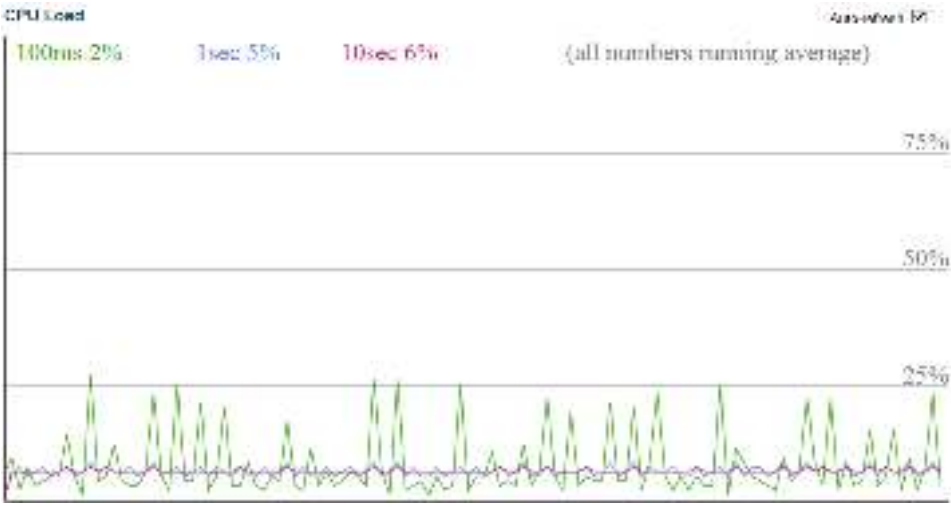
Software Date (Дата выхода прошивки)
Дата, когда прошивка была создана.

Кнопки:

Auto-refresh – нажмите, чтобы обновлять страницу автоматически раз в 3 сек;

Refresh – нажмите, чтобы обновить страницу

10.28.2 System – CPU Load (Система – Загрузка CPU)



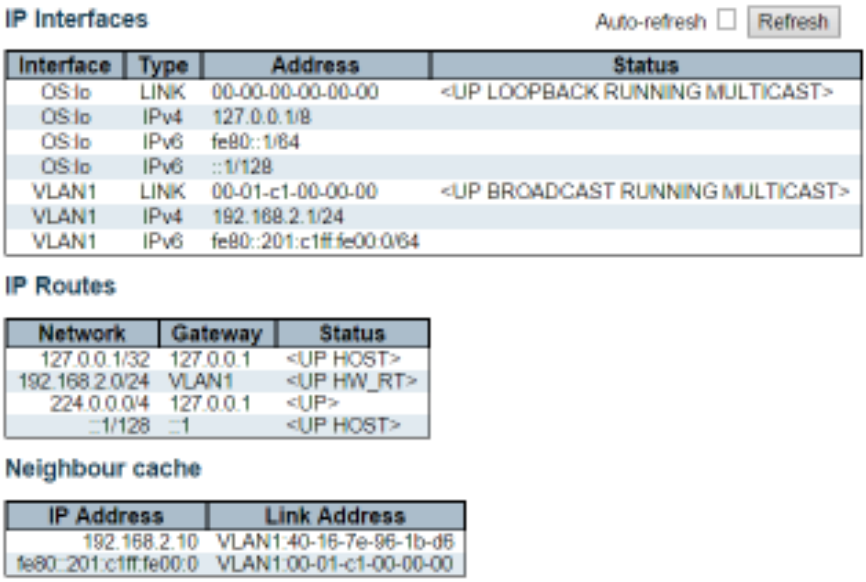
На данной странице WEB интерфейса представлены инструменты графического отображения загрузки процессора коммутатора.

Нагрузка измеряется как усредненная за последние 100 мс, 1 с и 10 с. Последние 120 сэмплов представлены графически, а последние цифры также отображаются в виде текста.

Для отображения графика SVG ваш браузер должен поддерживать формат SVG.

Auto-refresh – нажмите, чтобы обновлять страницу автоматически раз в 3 сек;

10.28.3 System – IP Status (Система – Состояние IP протокола на сетевом уровне)



IP Interfaces

Auto-refresh ☐ Refresh

Interface	Type	Address	Status
OS:lo	LINK	00-00-00-00-00-00	<UP LOOPBACK RUNNING MULTICAST>
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	fe80::1/64	
OS:lo	IPv6	::1/128	
VLAN1	LINK	00-01-c1-00-00-00	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.2.1/24	
VLAN1	IPv6	fe80::201:c1ff:fe00:0/64	

IP Routes

Network	Gateway	Status
127.0.0.1/32	127.0.0.1	<UP HOST>
192.168.2.0/24	VLAN1	<UP HW_RT>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

Neighbour cache

IP Address	Link Address
192.168.2.10	VLAN1 40-16-7e-96-1b-d6
fe80::201:c1ff:fe00:0	VLAN1 00-01-c1-00-00-00

Данная страница WEB интерфейса отображает состояние IP протокола на сетевом уровне. Состояние определяется IP-интерфейсами, IP-маршрутами и состоянием кэша (ARP-кэша) устройств-соседей.

IP интерфейсы

Interface (Интерфейсы)
Имя интерфейса

Type (Тип адреса записи)
Тип адреса записи. Может быть LINK или IPv4

Address (Адрес)
Текущий адрес интерфейса

Status (Состояние)
Флаги состояния интерфейса (и / или адреса)

IP маршруты

Network (Сеть)
IP адрес сети назначения или хоста на этом маршруте

Gateway (Шлюз)
Адрес шлюза на этом маршруте

Status (Статус)
Флаги состояния маршрута

Кэш устройств-соседей

IP Address (IP адрес)
IP адрес записи

Link Address (Адрес ссылки)
Адрес ссылки (MAC адрес), для которого настроена привязка с данному IP адресу

Кнопки:

Auto-refresh – нажмите, чтобы обновлять страницу автоматически раз в 3 сек;

Refresh – нажмите, чтобы обновить страницу

10.28.4 System – Log (Система – Журнал событий)

На данной странице WEB интерфейса представлен журнал системных событий.

ID
Идентификатор записи. Идентификатор >=1

Level (Уровень записи системных событий)
- ✓ Info – информационный уровень;
- ✓ Warning – уровень предупреждения;
- ✓ Error – уровень ошибок;
- ✓ All – все уровни сразу

Time
Время записи системного события

Message
Сообщение записи системного события

Кнопки:

Auto-refresh – нажмите, чтобы обновлять страницу автоматически раз в 3 сек;

Refresh – нажмите, чтобы отменить изменения;

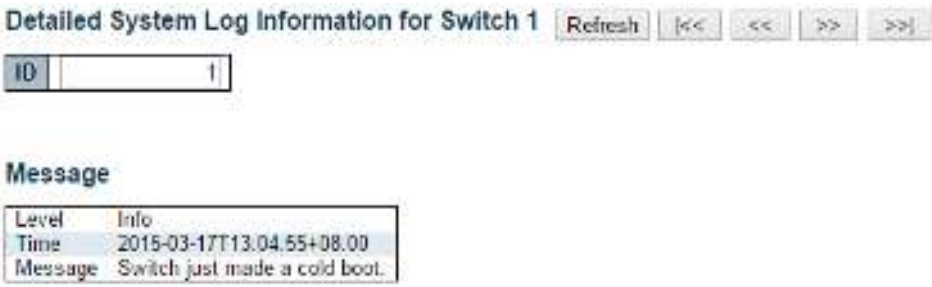
Clear – очистка всех выбранных записей событий;

|<< – обновление системного журнала, начиная с первого доступного идентификатора записи;
<< – обновление системного журнала, заканчивая последней отображаемой в данный момент записью;

>>| – обновление системного журнала, начиная с последней отображаемой записи;

>> – обновление системного журнала, заканчивая на последнем доступном идентификаторе записи.

10.28.5 System – Detailed Log (Система – Подробный журнал событий)



На данной странице WEB интерфейса представлен подробный журнал системных событий.

ID
Идентификатор записи. Идентификатор >=1

Message
Сообщение записи системного события

Кнопки:

Refresh – нажмите, чтобы обновить страницу;

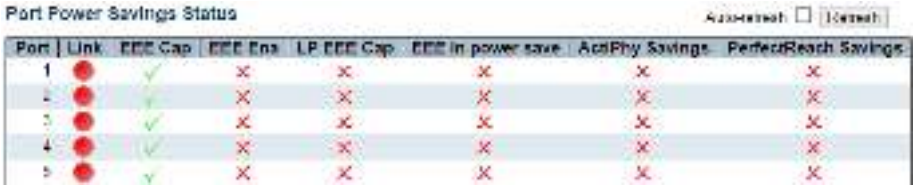
|<< – обновление системного журнала, начиная с первого доступного идентификатора записи;

<< – обновление системного журнала, заканчивая последней отображаемой в данный момент записью;

>>| – обновление системного журнала, начиная с последней отображаемой записи;

>> – обновление системного журнала, заканчивая на последнем доступном идентификаторе записи.

10.29 Monitor – Green Ethernet (Мониторинг – Green Ethernet)



На данной странице WEB интерфейса отображается текущий статус работы функции EEE (Green Ethernet)

Local Port (Локальный порт)
Логический номер порта

Link (Состояние соединения)
Поле отображает состояние соединения для порта. Красный – нет соединения, Зеленый – соединение есть.

EEE cap
Поле отображает поддержку EEE портом.

EEE Ena
Поле отображает включена ли функция EEE на выбранном порте

LP EEE cap
Поле отображает поддержку EEE подключенным к порту устройстовом.

EEE In power save (Режим экономии EEE)
Поле показывает, экономит ли система в настоящее время энергопотребление благодаря EEE. Когда EEE включен, система выключится, если ни один кадр не был получен или передан в течение 5 секунд.

Actiphy Savings
Поле отображает экономит ли система энергопотребление благодаря ActiPhy.

Perfect Reach Savings
Поле отображает экономит ли система энергопотребление благодаря Perfect Reach

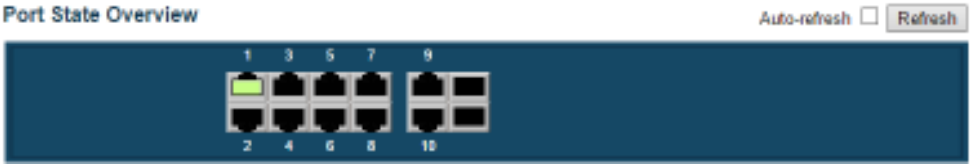
Кнопки:

Auto-refresh – нажмите, чтобы обновлять страницу автоматически раз в 3 сек;

Refresh – нажмите, чтобы отменить изменения;

10.30 Monitor – Ports (Мониторинг – Порты)

10.30.1 Ports – State (Порты – Состояние)



На данной странице WEB интерфейса отображается текущее состояние портов.

Порты могут принимать следующие состояния (рисунок ниже)

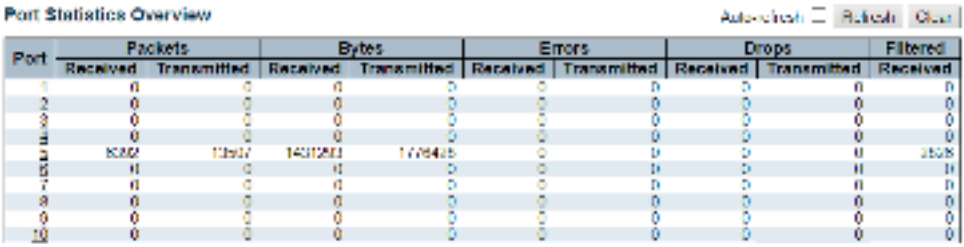
Состояние	Отключ.	Нет линка	Есть линк
RJ45 порты			
SFP порты			

Кнопки:

Auto-refresh – нажмите, чтобы обновлять страницу автоматически раз в 3 сек;

Refresh – нажмите, чтобы обновить страницу;

10.30.2 Ports – State (Порты – Состояние)



На данной странице WEB интерфейса представлена таблица со статистикой на весь трафик принятый/переданный через порты.

Port (Порт)
Логический номер порта

Packets (Пакеты)
Счетчик полученных и отправленных пакетов на каждом порте

Bytes (Байты)
Счетчик полученных и отправленных байтов на каждом порте

Errors (Ошибки)
Счетчик полученных и отправленных ошибок на каждом порте

Drops (Отброшенные пакеты)
Счетчик пакетов, отброшенных на каждом порте

Filtered (Отфильтрованные пакеты)
Счетчик пакетов, отфильтрованных на каждом порте в процессе пересылки

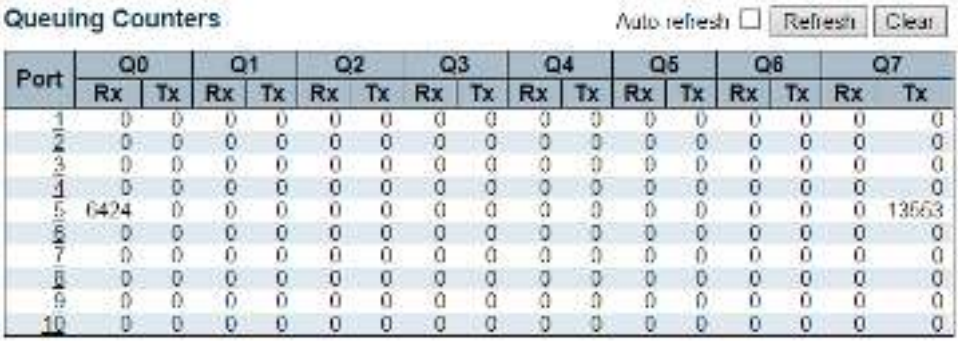
Кнопки:

Auto-refresh – нажмите, чтобы обновлять страницу автоматически раз в 3 сек;

Refresh – нажмите, чтобы обновить страницу;

Clear – нажмите, чтобы очистить все счетчики для портов.

10.30.3 Ports – QoS Statistics (Порты – Статистика QoS)


Queuing Counters

Auto-refresh ☐ Refresh Clear

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	6424	0	0	0	0	0	0	0	0	0	0	0	0	0	0	13663
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Port (Порт)
Логический номер порта

Qn (Номер очереди)
8 очередей на каждый порт. Q0 имеет самый низкий приоритет.

Rx/Tx
Количество принятых/переданных пакетов для каждой очереди

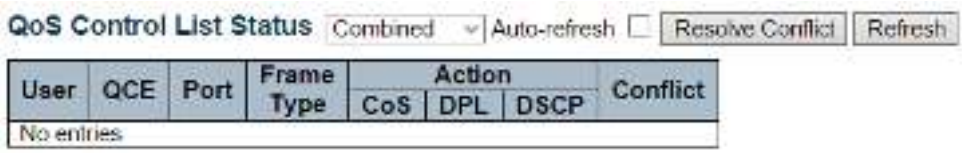
Кнопки:

Auto-refresh – нажмите, чтобы обновлять страницу автоматически раз в 3 сек;

Refresh – нажмите, чтобы обновить страницу;

Clear – нажмите, чтобы очистить все счетчики для портов.

10.30.4 Ports – QCL Status (Порты – Состояние QCL)



На данной странице отображается статус QCL для различных QCL пользователей.

User (Пользователь)
Поле отображает пользователя QCL

QCE
Поле отображает Идентификатор QCE

Port (Порт)
Поле отображает список портов, настроенных с QCE

Frame Type (Тип фрейма)
Поле отображает тип фрейма. Возможные значения:

- ✓ Any – соответствует любому типу фреймов;
- ✓ Ethernet – соответствует EtherType фремам;
- ✓ LLC – соответствует LLC фреймам;
- ✓ SNAP – соответствует SNAP фреймам;
- ✓ IPv4 – соответствует IPv4 фреймам;
- ✓ IPv6 – соответствует IPv6 фреймам.

Action (Действие)

- ✓ CoS – классификация с помощью CoS;
- ✓ DPL – классификация с помощью DPL;
- ✓ DSCP – классификация с помощью DSCP.

Conflict (Конфликт)

Поле отображает статус конфликта записей QCL.

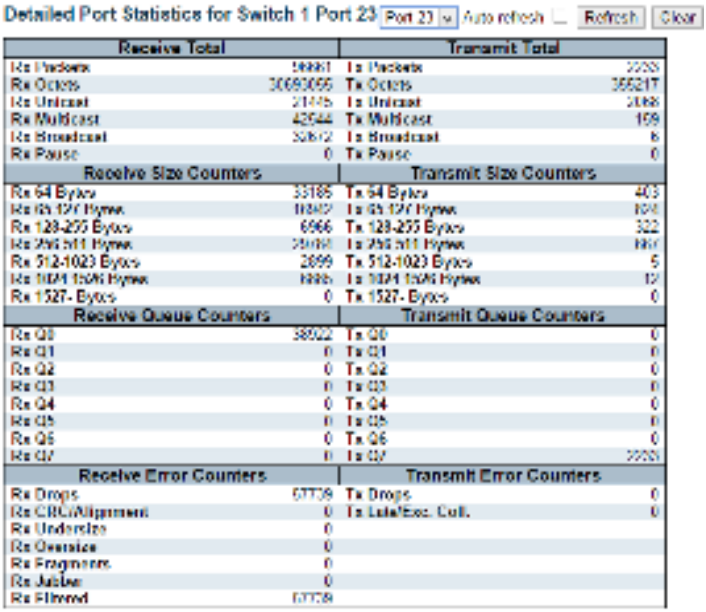
Конфликт может быть разрешен путем освобождения ресурсов H / W, необходимых для добавления записи QCL при нажатии кнопки «Разрешить конфликт» (Resolve Conflict)

Кнопки:

Auto-refresh – нажмите, чтобы обновлять страницу автоматически раз в 3 сек;

Refresh – нажмите, чтобы обновить страницу;

10.30.5 Ports – Detailed Statistics (Порты – Детальная статистика)



На данной странице WEB интерфейса представлены детальные сведения для выбранного порта коммутатора.

Счетчик Получено/отправлено

RX and Tx Packets
Общее количество полученных и отправленных пакетов

Rx and Tx Octets
Общее количество полученных и отправленных байтов

Rx and Tx Unicast
Общее количество полученных и отправленных пакетов Unicast

Rx and Tx Multicast
Общее количество полученных и отправленных пакетов Multicast

Rx and Tx Broadcast
Общее количество полученных и отправленных пакетов Broadcast

Rx and Tx Pause
Количество пакетов MAC Control, указывающих на операцию «Пауза»

Счетчик ошибок при получении

Rx Drops
Количество фреймов отброшенных из за перегрузки выхода

Rx CRC/Alignment
Количество фреймов с CRC или ошибками выравнивания

Rx Undersize
Количество коротких фреймов полученных с действительной контрольной суммой CRC

Rx Oversize
Количество длинных фреймов полученных с действительной контрольной суммой CRC

Rx Fragments
Количество коротких фреймов полученных с недействительной контрольной суммой CRC

Rx Jabber
Количество длинных фреймов полученных с недействительной контрольной суммой CRC

Rx Filtered
Количество фреймов отфильтрованных при пересылке

Счетчик ошибок при пересылке

Rx Drops
Количество фреймов отброшенных из за перегрузки буфера

Tx Late/Exc. Coll
Количество фрейов отброшенных из за коллизий

Кнопки:

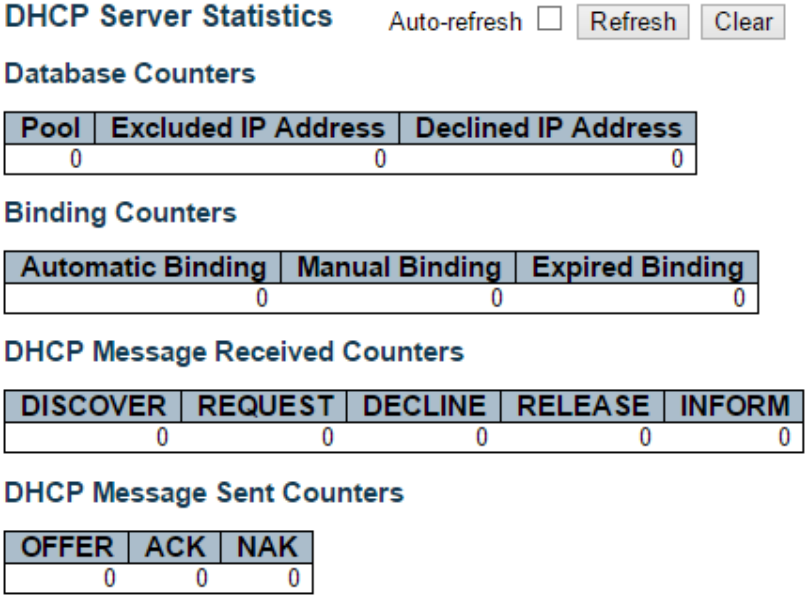
Auto-refresh – нажмите, чтобы обновлять страницу автоматически раз в 3 сек;

Refresh – нажмите, чтобы обновить страницу;

Clear – нажмите, чтобы очистить все счетчики для портов.

10.31 Monitor – DHCP (Мониторинг – DHCP)

10.31.1 DHCP – Server – Statistics (DHCP – Сервер – Статистика)



На данной странице WEB интерфейса находится счетчики базы данных и количества сообщений DHCP сообщений отправленных и полученных DHCP сервером.

Счетчики базы данных

Pool
Количество пулов адресов

Excluded IP Address
Количество исключенных диапазонов IP-адресов.

Declined IP Address
Количество отклоненных IP-адресов.

Счетчики привязок

Automatic Binding
Количество привязок с пулами сетевого типа.

Manual Binding
Количество привязок, которые администратор назначает клиенту по IP-адресу. То есть пул имеет тип хоста.

Expired Binding
Количество привязок, для которых истек срок их аренды.

Счетчики полученных DHCP сообщений

DISCOVER
Количество полученных сообщений DHCP DISCOVER

REQUEST
Количество полученных сообщений DHCP REQUEST

DECLINE
Количество полученных сообщений DHCP DECLINE

RELEASE
Количество полученных сообщений DHCP RELEASE

INFORM
Количество полученных сообщений DHCP INFORM

Счетчики отправленных DHCP сообщений

OFFER
Количество отправленных сообщений DHCP OFFER

ACK
Количество отправленных сообщений DHCP ACK

NAK
Количество отправленных сообщений DHCP NAK

Кнопки:

Auto-refresh – нажмите, чтобы обновлять страницу автоматически раз в 3 сек;

Refresh – нажмите, чтобы обновить страницу;

Clear – нажмите, чтобы очистить все счетчики для портов.

10.31.2 DHCP – Server – Binding (DHCP – Сервер – Привязка)

На данной странице WEB интерфейса отображаются привязки, генерируемые DHCP клиентами.

Привязка IP адреса

IP (IP адрес)
IP-адрес, выделенный для DHCP-клиента.

Type (Тип)
Тип привязки. Возможные типы:

- ✓ Automatic (автоматический);
- ✓ Manual (вручную);
- ✓ Expired (истекший).

State (Состояние)
Состояние привязки. Возможные состояния:

- ✓ Commited – выполненный;
- ✓ Allocated – выделенный;
- ✓ Expired – истекший.

Pool Name (Имя пула)
Пул, который генерирует привязку

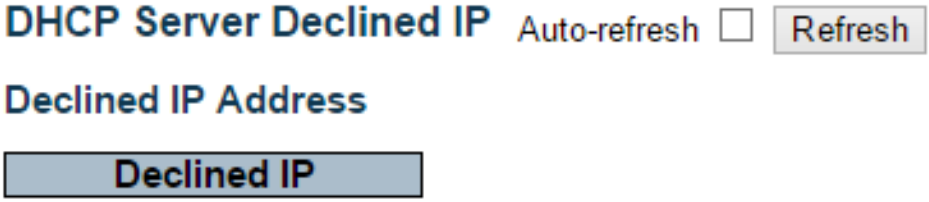
Server ID (Идентификатор сервера)
P-адрес сервера для обслуживания привязки.

Кнопки:

Auto-refresh – нажмите, чтобы обновлять страницу автоматически раз в 3 сек;

Refresh – нажмите, чтобы обновить страницу;

10.31.3 DHCP – Server – Declined IP (DHCP – Сервер – Отклоненные IP)



На данной странице WEB интерфейса находится список отклоненных IP адресов

Declined IP
Список IP отклоненных адресов

Кнопки:

Auto-refresh – нажмите, чтобы обновлять страницу автоматически раз в 3 сек;

Refresh – нажмите, чтобы обновить страницу;

10.31.4 DHCP – Snooping Table

На данной странице WEB интерфейса отображается информация о назначенном динамическом IP-адресе после отключения режима DHCP Snooping.

Все клиенты DHCP, получившие динамический IP-адрес от сервера DHCP, будут перечислены в этой таблице, за исключением IP-адресов локального интерфейса VLAN.

Столбцы таблицы DHCP Snooping

MAC Address (MAC адрес)
MAC адрес пользователя для этой записи

VLAN ID (Идентификатор VLAN)
Идентификатор VLAN в которой разрешен трафик DHCP.

Source Port (Порт источник)
Номер порта коммутатора, для которого отображаются записи.

IP Address (IP адрес)
IP адрес пользователя для этой записи

IP Subnet Mask (Маска подсети)
Маска подсети пользователя для этой записи

DHCP Server Address (Адрес DHCP сервера)
Адрес DHCP сервера для этой записи

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

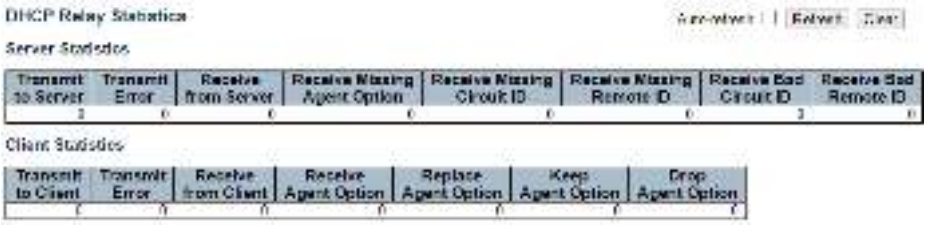
Refresh – нажмите, чтобы обновить страницу;

Clear – нажмите, чтобы очистить все динамические записи;

|<< – обновление таблицы, начиная с первой записи в таблице;

>>| – обновление таблицы, начиная с записи после последней отображаемой записи

10.31.5 DHCP – Relay Statistics (DHCP – Статистика ретрансляции DHCP)



На данной странице WEB интерфейса находится таблица статистики ретрансляции DHCP.

Статистика сервера

Transmit to Server
Количество пакетов, которые передаются от клиента к серверу.

Transmit Error
Количество пакетов, которые привели к ошибкам при отправке клиентам

Receive from Server
Количество пакетов, полученных с сервера.

Receive Missing Agent Option
Количество пакетов, полученных без информации об агентах.

Receive Missing Circuit ID
Количество пакетов, полученных с опцией Missing Circuit ID.

Receive Missing Remote ID
Количество пакетов, полученных с опцией Missing Remote ID.

Receive Bad Circuit ID
Количество пакетов, чья опция «Circuit ID» не соответствует известному Circuit ID.

Receive Bad Remote ID
Количество пакетов, чья опция «Missing Remote ID» не соответствует известному Missing Remote ID.

Статистика клиента

Transmit to Client
Количество ретранслируемых пакетов с сервера на клиент.

Transmit Error
Количество пакетов, которые привели к ошибке при отправке на сервер

Receive from Client
Количество полученных пакетов клиентом от сервера.

Receive Agent Option
Количество полученных пакетов с опцией информации агента ретрансляции.

Replace Agent Option
Количество пакетов, которые были заменены опцией информации агента ретрансляции.

Keep Agent Option
Количество пакетов, чья информация об агенте ретрансляции была сохранена.

Drop Agent Option
Количество отброшенных пакетов, полученных с информацией агента ретрансляции.

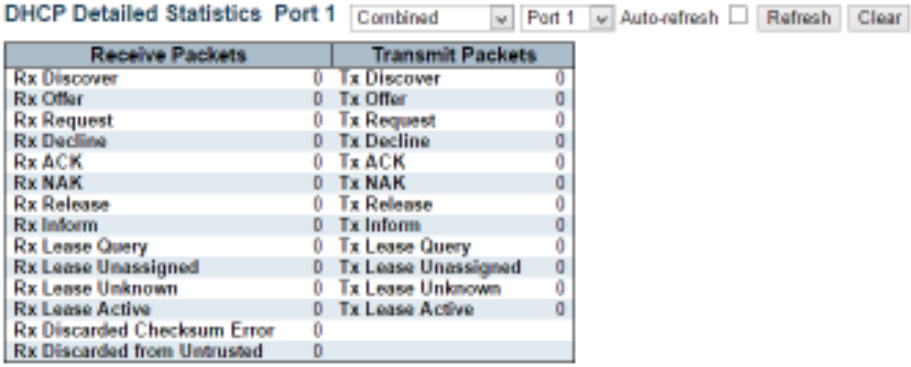
Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

Clear – нажмите, чтобы очистить всю статистику;

10.31.6 DHCP – Detailed Statistics (DHCP – Детальная Статистика)



На данной странице WEB интерфейса находится таблица детальной статистики DHCP Snooping

Полученные и отправленные пакеты

Rx and Tx Discover
Количество полученных и переданных пакетов Discover

Rx and Tx Offer
Количество полученных и переданных пакетов Offer

Rx and Tx Request
Количество полученных и переданных пакетов Request

Rx and Tx Decline
Количество полученных и переданных пакетов Decline

Rx and Tx ACK
Количество полученных и переданных пакетов ACK

Rx and Tx NAK
Количество полученных и переданных пакетов NAK

Rx and Tx Release
Количество полученных и переданных пакетов Release

Rx and Tx Inform
Количество полученных и переданных пакетов Inform

Rx and Tx Lease Query
Количество полученных и переданных пакетов lease query (запрос аренды)

Rx and Tx Lease Unassigned
Количество полученных и переданных пакетов Lease Unassigned (аренда не назначена)

Rx and Tx Lease Unknown
Количество полученных и переданных пакетов Lease Unknown (аренда неизвестна)

Rx and Tx Lease Active
Количество полученных и переданных пакетов Lease Active (аренда активна)

Rx Discarded checksum error
Количество полученных ошибок об отклонённых пакетах из за ошибки контрольной суммы

Rx Discarded from Untrusted
Количество отклоненных пакетов, поступающих с ненадежного порта.

Кнопки:

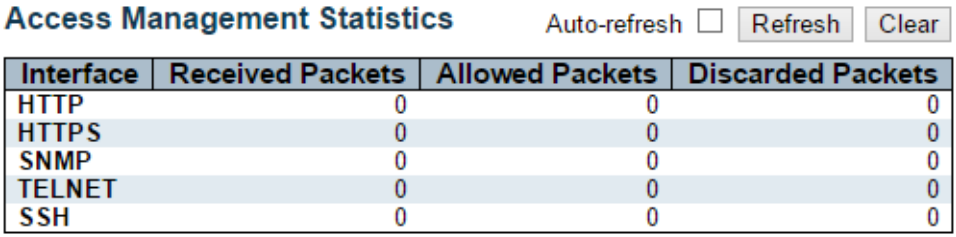
Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

Clear – нажмите, чтобы очистить всю статистику для выбранного порта;

10.32 Monitor – Security (Мониторинг – Безопасность)

10.32.1 Security – Access Management Statistics (Безопасность – Статистика управления доступом)


Access Management Statistics

Auto-refresh ☐ Refresh Clear

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

На данной странице WEB интерфейса представлена статистика управления доступом.

Interface (Интерфейс)
Тип интерфейса, через который удаленный хост может получить доступ к коммутатору.

Received Packets (Полученные пакеты)
Количество полученных пакетов от интерфейса, когда включен режим управления доступом.

Allowed Packets (Разрешенные пакеты)
Количество разрешенных пакетов от интерфейса, когда включен режим управления доступом

Discarded Packets (Отклоненные пакеты)
Количество отклоненных пакетов от интерфейса, когда включен режим управления доступом

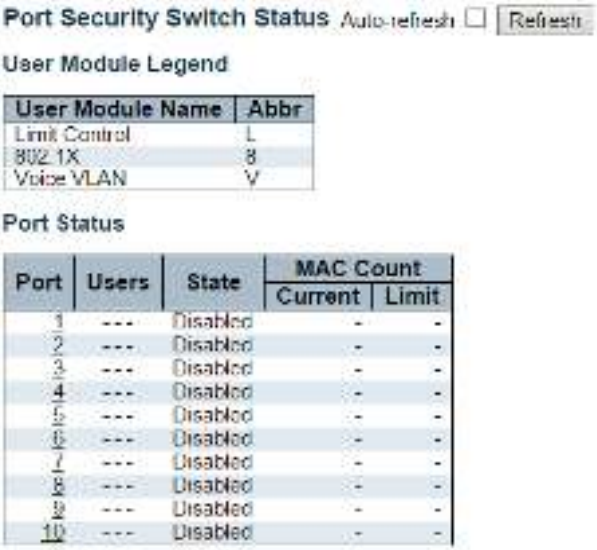
Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

Clear – нажмите, чтобы очистить всю статистику.

10.32.2 Security – Network – Port Security (Безопасность – Сеть – Безопасность портов)


Port Security Switch Status Auto-refresh Refresh

User Module Legend

User Module Name	Abbr
Limit Control	L
802.1X	8
Voice VLAN	V

Port Status

Port	Users	State	MAC Count	
			Current	Limit
1	---	Disabled	-	-
2	---	Disabled	-	-
3	---	Disabled	-	-
4	---	Disabled	-	-
5	---	Disabled	-	-
6	---	Disabled	-	-
7	---	Disabled	-	-
8	---	Disabled	-	-
9	---	Disabled	-	-
10	---	Disabled	-	-

На данной странице WEB интерфейса находится статистика безопасности портов. Безопасность портов (Port Security) это модуль

без прямой настройки. Конфигурация происходит косвенно от других пользовательских модулей.

Статус порта

Port (Порт)
Номер порта, к которому относится статус. Нажмите на номер порта, чтобы увидеть статус для этого конкретного порта.

Users (Пользователи)
У каждого из пользовательских модулей есть столбец, который показывает, включил ли этот модуль защиту портов или нет. «-» означает, что соответствующий пользовательский модуль не включен.

State (Состояние)
Поле отображает текущее состояние порта.

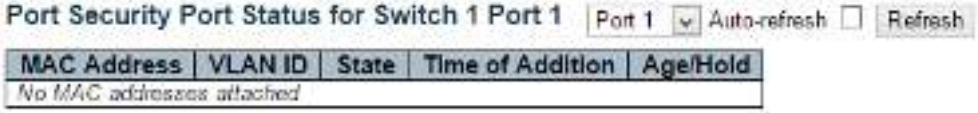
- ✓ Disabled – В настоящее время ни один пользовательский модуль не использует службу безопасности порта
- ✓ Ready – Port Security используется по крайней мере одним пользовательским модулем и ожидает поступления фреймов с неизвестных MAC-адресов
- ✓ Limit Reached – Port Security включена, по крайней мере, пользовательским модулем Limit Control, и этот модуль указал, что предел достигнут и больше MAC-адресов не должно приниматься.
- ✓ Shutdown – Port Security включена по крайней мере, пользовательским модулем Limit Control, и этот модуль указал, что предел превышен. Любые MAC-адреса не могут быть изучены для порта, пока он не будет повторно открыт администратором системы на веб-странице «Limit Control».

MAC Count (Количество MAC адресов)
В двух столбцах указано количество изученных в настоящий момент MAC-адресов (как переадресованных, так и заблокированных)

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;



На данной странице WEB интерфейса показаны MAC-адреса, защищенные модулем Port Security. Port Security - это модуль без прямой настройки. Конфигурация происходит косвенно от других пользовательских модулей.

MAC Address & VLAN ID (MAC адрес и идентификатор VLAN)
MAC-адрес и идентификатор VLAN, которые видны на этом порту. Если MAC-адреса не определены, отображается одна строка с надписью «No MAC addresses attached».

State (Состояние)
Поле указывает, заблокирован ли соответствующий MAC-адрес или выполняется переадресация. В заблокированном состоянии не будет разрешено передавать или получать трафик.

Time of Addition (Время обнаружения MAC)
Показывает дату и время, когда этот MAC-адрес впервые был обнаружен на порту.

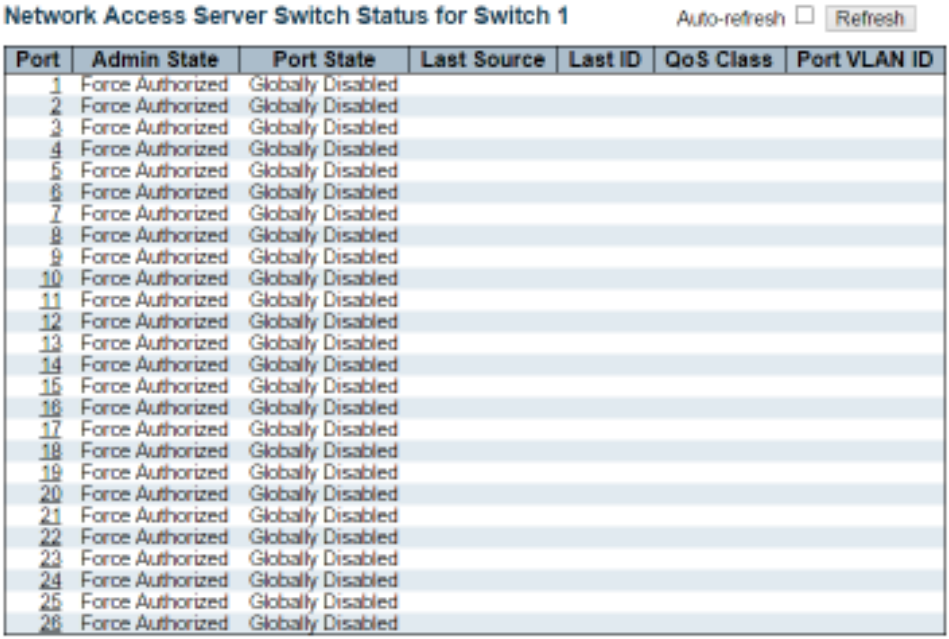
Age/Hold
Если хотя бы один пользовательский модуль решил заблокировать этот MAC-адрес, он будет оставаться в заблокированном состоянии до тех пор, пока не истечет время удержания Hold (измеренное в секундах).

Если все пользовательские модули решили разрешить пересылку этого MAC-адреса, а устаревание Age включено, модуль защиты порта будет периодически проверять, пересылает ли этот MAC-адрес трафик. Если период возраста (измеренный в секундах) истекает и кадры не были замечены, MAC-адрес будет удален из таблицы MAC.

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;



Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled				
2	Force Authorized	Globally Disabled				
3	Force Authorized	Globally Disabled				
4	Force Authorized	Globally Disabled				
5	Force Authorized	Globally Disabled				
6	Force Authorized	Globally Disabled				
7	Force Authorized	Globally Disabled				
8	Force Authorized	Globally Disabled				
9	Force Authorized	Globally Disabled				
10	Force Authorized	Globally Disabled				
11	Force Authorized	Globally Disabled				
12	Force Authorized	Globally Disabled				
13	Force Authorized	Globally Disabled				
14	Force Authorized	Globally Disabled				
15	Force Authorized	Globally Disabled				
16	Force Authorized	Globally Disabled				
17	Force Authorized	Globally Disabled				
18	Force Authorized	Globally Disabled				
19	Force Authorized	Globally Disabled				
20	Force Authorized	Globally Disabled				
21	Force Authorized	Globally Disabled				
22	Force Authorized	Globally Disabled				
23	Force Authorized	Globally Disabled				
24	Force Authorized	Globally Disabled				
25	Force Authorized	Globally Disabled				
26	Force Authorized	Globally Disabled				

На данной странице WEB интерфейса коммутатора находится сводная таблица текущих состояний порта NAS.

Port (Порт)
Номер порта коммутатора. Нажмите, чтобы перейти к подробной статистике NAS для этого порта

Admin State (Состояние Admin)
Текущее Admin состояние порта. Перейдите к NAS Admin State для описания возможных значений.

Port State (Состояние порта)
Текущее состояние порта. Перейдите к NAS Admin State для описания возможных значений.

Last Source (Последний принятый исходный MAC)
Исходный MAC-адрес передается в последнем принятом фрейме EAPOL для аутентификации на основе EAPOL и в последнем принятом кадре от нового клиента для аутентификации на основе MAC.

Last ID (Имя пользователя в последнем принятом фрейме)
Имя пользователя (идентификатор запрашивающей стороны) содержится в последнем принятом фрейме EAPOL идентификатора ответа для аутентификации на основе EAPOL и MAC-адресе источника из самого последнего принятого кадра от нового клиента для аутентификации на основе MAC.

QoS Class (Класс QoS)
Класс QoS, назначенный порту сервером RADIUS, если он включен

Port VLAN ID (Идентификатор VLAN для порта)
Идентификатор VLAN, в который NAS поместил порт. Поле пустое, если идентификатор VLAN порта не переопределен NAS.

Если идентификатор VLAN назначается сервером RADIUS, к идентификатору VLAN добавляется «(RADIUS-assigned)»

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

На данной странице WEB интерфейса содержится подробная статистика NAS для конкретного порта коммутатора, на котором выполняется аутентификация IEEE 802.1X на основе EAPOL.

Состояние порта

Admin State (Admin состояние)
Текущее Admin состояние порта. Перейдите к NAS Admin State для описания возможных значений.

Port State (Состояние порта)
Текущее состояние порта. Перейдите к NAS Admin State для описания возможных значений.

QoS Class (Класс QoS)
Класс QoS, назначенный порту сервером RADIUS, если он включен

Port VLAN ID (Идентификатор VLAN)
Идентификатор VLAN, в который NAS поместил порт. Поле пустое, если идентификатор VLAN порта не переопределен NAS.

Если идентификатор VLAN назначается сервером RADIUS, к идентификатору VLAN добавляется «(RADIUS-assigned)»

Счетчики EAPOL

Счетчики пакетов доступны для следующих состояний порта:

- ✓ Force Authorized
- ✓ Force Unauthorized
- ✓ Port-based 802.1X
- ✓ Single 802.1X
- ✓ Multi 802.1X

Счетчики для RADIUS сервера

Счетчики пакетов RADIUS доступны для следующих состояний порта:

- ✓ Port-based 802.1X
- ✓ Single 802.1X
- ✓ Multi 802.1X

10.32.3 Security - Network - ACL Status (Безопасность – Сеть – Состояние ACL)

На данной странице WEB интерфейса находится таблица состояния ACL для различных пользователей. Максимальное количество ACL – 512.

User (Пользователь)
Поле отображает пользователя ACE

ACE
Отображает идентификатор записи ACE

Frame Type (Тип фрейма)
Отображает тип фреймов для ACE. Возможные значения:

- ✓ Any
- ✓ EType
- ✓ ARP
- ✓ IPv4
- ✓ IPv4/ICMP
- ✓ IPv4/UDP
- ✓ IPv4/TCP
- ✓ IPv4/Other
- ✓ IPv6

Action (Действие)
Поле отображает состояние пересылки для ACE

- ✓ Permit – фреймы, соответствующие ACE, могут быть переданы и изучены (learning)
- ✓ Deny – – фреймы, соответствующие ACE будут отброшены.

Rate Limiter (Ограничитель скорости)
Доступные значения 1 – 16. Если в поле указано disabled – ограничитель скорости отключен.

CPU
Переслать пакет, который соответствует конкретному ACE для процессора

Counter (Счетчик)
Счетчик показывает количество раз, когда ACE совпал с типом кадра.

Conflict (Конфликт)
Поле показывает аппаратное состояние определенного ACE. Конкретный ACE не применяется к оборудованию из-за аппаратных ограничений.

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

10.32.4 Security - Network - ARP Inspection (Безопасность – Сеть – Проверка ARP)

Записи в динамической таблице проверки ARP показаны на этой странице WEB интерфейса.

Динамическая таблица проверки ARP содержит до 1024 записей и сортируется сначала по порту, затем по идентификатору VLAN, затем по MAC-адресу и затем по IP-адресу.

Столбцы навигации по таблице проверки ARP

Port (Порт)
Номер порта коммутатора для которого будут отображены записи.

VLAN ID (Идентификатор VLAN)
Идентификатор VLAN в которой разрешен ARP трафик

MAC Address (MAC Адрес)
MAC адрес пользователя этой записи

IP Address (IP адрес)
IP адрес пользователя этой записи

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

Clear – нажмите, чтобы обновить все динамические записи;

|<< – обновление таблицы, начиная с первой записи в таблице проверки динамического ARP

|>> – обновление таблицы, начиная с записи после последней отображаемой записи.

10.32.5 Security - Network – IP Source Guard (Безопасность – Сеть – Функция IP Source Guard)

Записи в таблице IP Source Guard динамического IP-адреса показаны на этой WEB странице.

Таблица IP Source Guard динамического IP-адреса сначала сортируется по порту, затем по идентификатору VLAN, затем по IP-адресу и затем по MAC-адресу.

Столбцы навигации по таблице IP Source Guard

Port (Порт)
Номер порта коммутатора для которого будут отображены записи.

VLAN ID (Идентификатор VLAN)
Идентификатор VLAN в которой разрешен IP трафик

IP Address (IP адрес)
IP адрес пользователя этой записи

MAC Address (MAC Адрес)
MAC адрес пользователя этой записи

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

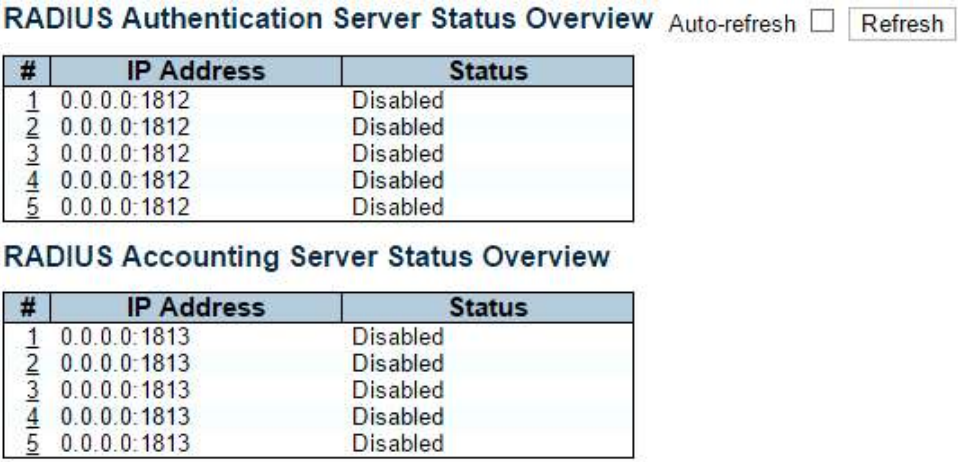
Refresh – нажмите, чтобы обновить страницу;

Clear – нажмите, чтобы обновить все динамические записи;

|<< – обновление таблицы, начиная с первой записи в таблице IP Source Guard

10.33 Security - AAA (Безопасность – AAA)

10.33.1 Security – AAA – RADIUS Overview (Безопасность – AAA – Аутентификация RADIUS)


RADIUS Authentication Server Status Overview Auto-refresh Refresh

#	IP Address	Status
1	0.0.0.0:1812	Disabled
2	0.0.0.0:1812	Disabled
3	0.0.0.0:1812	Disabled
4	0.0.0.0:1812	Disabled
5	0.0.0.0:1812	Disabled

RADIUS Accounting Server Status Overview

#	IP Address	Status
1	0.0.0.0:1813	Disabled
2	0.0.0.0:1813	Disabled
3	0.0.0.0:1813	Disabled
4	0.0.0.0:1813	Disabled
5	0.0.0.0:1813	Disabled

На данной странице WEB интерфейса находится сводная таблица состояния серверов RADIUS , настраиваемых на странице конфигурации аутентификации.

Сервера аутентификации RADIUS

#
Номер сервера RADIUS. Нажмите, чтобы получить подробную статистику

IP Address
IP адрес и номер UDP порта выбранного сервера.

Status
Текущее состояние сервера. Поле может принимать одно из следующих значений:

- ✓ Disabled – сервер отключен;
- ✓ Not Ready – сервер активен, но IP соединение еще не установлено;
- ✓ Ready – сервер активен, IP соединение установлено, RADIUS модуль готов выполнять свою функцию;
- ✓ Dead – были предприняты попытки доступа к выбранному серверу, но он не ответил в течение заданного времени.

Сервера учета RADIUS

#
Номер сервера RADIUS. Нажмите, чтобы получить подробную статистику

IP Address
IP адрес и номер UDP порта выбранного сервера.

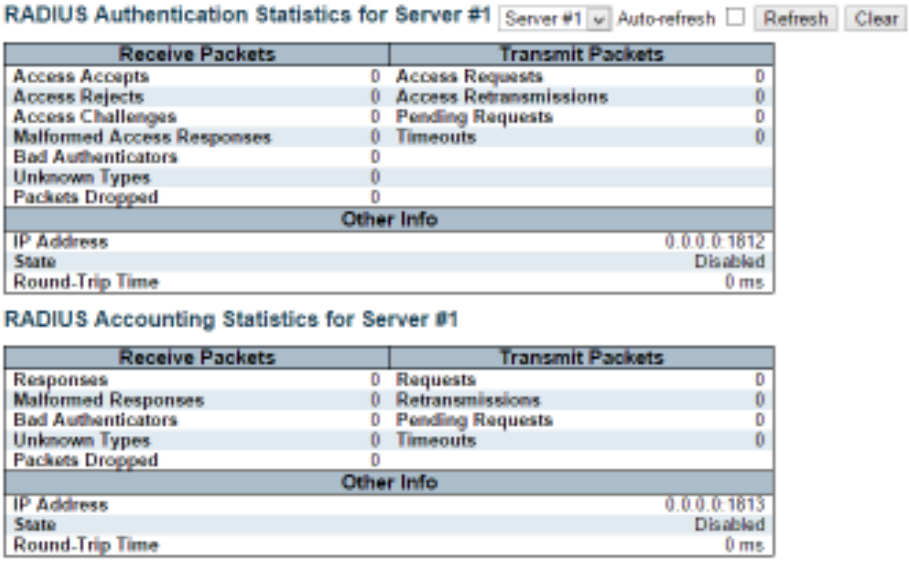
Status
- ✓ Disabled – сервер отключен;
- ✓ Not Ready – сервер активен, но IP соединение еще не установлено;
- ✓ Ready – сервер активен, IP соединение установлено, RADIUS модуль готов выполнять свою функцию;
- ✓ Dead – были предприняты попытки доступа к выбранному серверу, но он не ответил в течение заданного времени.

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

10.33.2 Security – AAA – RADIUS Details (Безопасность – AAA – Подробная статистика RADIUS)


RADIUS Authentication Statistics for Server #1 Server #1 Auto-refresh Refresh Clear

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
IP Address			0.0.0.0:1812
State			Disabled
Round-Trip Time			0 ms

RADIUS Accounting Statistics for Server #1

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
IP Address			0.0.0.0:1813
State			Disabled
Round-Trip Time			0 ms

На данной странице находится таблица с подробной статистикой работы выбранного RADIUS сервера.

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

Clear – нажмите, чтобы очистить счетчики для выбранного сервера.

10.34 Security – Switch – RMON (Безопасность – Коммутатор – Удаленный мониторинг)

10.34.1 Switch – RMON – Statistics (Коммутатор – Удаленный мониторинг – Статистика)

На данной странице WEB интерфейса представлена таблица статистики RMON (удаленный мониторинг). На каждой странице отображается до 99 записей из таблицы статистики

ID
Поле отображает индекс записи статистики

Data Source
Идентификатор порта, который необходимо отслеживать

Drop
Общее количество событий, в которых пакеты были отброшены из-за нехватки ресурсов.

Octets
Общее количество октетов данных (в том числе в пакетах «Bad»), полученных в сети

Pkts
Общее количество полученных пакетов (включая Error пакеты, Broadcast и Multicast пакеты)

Broad-cast
Общее количество принятых пакетов, которые были направлены на широковещательный адрес.

Multi-cast
Общее количество принятых пакетов, которые были направлены на multicast адрес.

CRC Errors
Общее количество полученных пакетов, которые имели длину (исключая кадрирующие биты, но включая октеты FCS) от 64 до 1518 октетов включительно, но имели либо неверную контрольную последовательность фрейма (FCS) с целым числом октетов (ошибка FCS) или неправильная FCS с нецелым числом октетов (ошибка выравнивания).

Under-size
Общее количество полученных пакетов, размером менее 64 октетов.

Over-size
Общее количество полученных пакетов, размером более 1518 октетов.

Frag.
Общее количество полученных пакетов, размером менее 64 октетов с ошибкой контрольной суммы CRC

Jabb.
Общее количество полученных пакетов, размером более 64 октетов с ошибкой контрольной суммы CRC

Coll.
Оценка общего количества коллизий в данном сегменте Ethernet.

64
Общее количество полученных пакетов (включая ошибочные) длиной 64 октета

65~127
Общее количество полученных пакетов (включая ошибочные) длиной 64 ~ 127 октетов

128~255
Общее количество полученных пакетов (включая ошибочные) длиной 128 ~ 255 октетов

256~511
Общее количество полученных пакетов (включая ошибочные) длиной 255 ~ 511 октетов

512~1023
Общее количество полученных пакетов (включая ошибочные) длиной 512 ~ 1023 октетов

1024~1588
Общее количество полученных пакетов (включая ошибочные) длиной 1024 ~ 1588 октетов

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

|<< – обновление таблицы, начиная с первой записи в таблице

|>> – обновление таблицы, начиная с записи после последней отображаемой записи.

10.34.2 Switch – RMON – History (Коммутатор – Удаленный мониторинг – История RMON)

На данной странице WEB интерфейса находится таблица истории записей RMON. На каждой странице отображается до 99 записей из таблицы.

History Index
Индекс элемента управления истории

Sample Index
Индекс записи данных, связанной с контрольной записью.

Drop
Общее количество событий, в которых пакеты были отброшены из-за нехватки ресурсов.

Octets
Общее количество октетов данных (в том числе в пакетах «Bad»), полученных в сети

Pkts
Общее количество полученных пакетов (включая Error пакеты, Broadcast и Multicast пакеты)

Broad-cast
Общее количество принятых пакетов, которые были направлены на широковещательный адрес.

Multi-cast
Общее количество принятых пакетов, которые были направлены на multicast адрес.

CRC Errors
Общее количество полученных пакетов, которые имели длину (исключая кадрирующие биты, но включая октеты FCS) от 64 до 1518 октетов включительно, но имели либо неверную контрольную последовательность фрейма (FCS) с целым числом октетов (ошибка FCS) или неправильная FCS с нецелым числом октетов (ошибка выравнивания).

Under-size
Общее количество полученных пакетов, размером менее 64 октетов.

Over-size
Общее количество полученных пакетов, размером более 1518 октетов.

Frag.
Общее количество полученных пакетов, размером менее 64 октетов с ошибкой контрольной суммы CRC

Jabb.
Общее количество полученных пакетов, размером более 64 октетов с ошибкой контрольной суммы CRC

Coll.
Оценка общего количества коллизий в данном сегменте Ethernet.

Utilization
Оценка использования сети физического уровня на этом интерфейсе в течение этого интервала выборки в сотых долях процента.

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

|<< – обновление таблицы, начиная с первой записи в таблице

|>> – обновление таблицы, начиная с записи после последней отображаемой записи.

10.34.3 Switch – RMON – Alarm (Коммутатор – Удаленный мониторинг – Тревожные сообщения)

На данной странице WEB интерфейса находится таблица тревожных сообщений RMON (удаленного мониторинга). На каждой странице отображается до 99 записей из таблицы.

ID
Поле отображает индекс записи тревожного сообщения

Interval
Поле определяет интервал в секундах для выборки и сравнения порога нарастания и спада.

Variable
Поле отображает конкретную переменную для выборки

Sample Type
Метод выборки выбранной переменной и вычисления значения для сравнения с пороговыми значениями.

Value
Значение статистики за последний период выборки.

Startup Alarm
Тревога, которая может быть отправлена, когда эта запись впервые установлена на значение Valid

Rising Threshold
Повышение порогового значения

Rising Index
Индекс события

Falling Threshold
Падение порогового значения

Falling Index
Индекс события

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

|<< – обновление таблицы, начиная с первой записи в таблице

|>> – обновление таблицы, начиная с записи после последней отображаемой записи.

10.34.4 Switch – RMON – Events (Коммутатор – Удаленный мониторинг – События)

На данной странице WEB интерфейса находится таблица событий RMON (удаленного мониторинга). На каждой странице отображается до 99 записей из таблицы.

Event Index
Поле отображает индекс записи события

Log Index
Поле отображает индекс записи журнала

Log Time
Поле отображает время события

Log Description
Поле отображает описание события

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

|<< – обновление таблицы, начиная с первой записи в таблице

|>> – обновление таблицы, начиная с записи после последней отображаемой записи.

10.35 Switch – LACP (Коммутатор – Удаленный мониторинг – События)

10.35.1 LACP – System Status (LACP – Состояние системы)

Aggr ID
Идентификатор агрегации

Partner System ID
Системный идентификатор (MAC-адрес) партнера по агрегации.

Partner Key
Ключ, который партнер назначил этому идентификатору агрегации.

Last changed
Поле указывающее на то, что время, прошедшее с момента агрегации, изменилось.

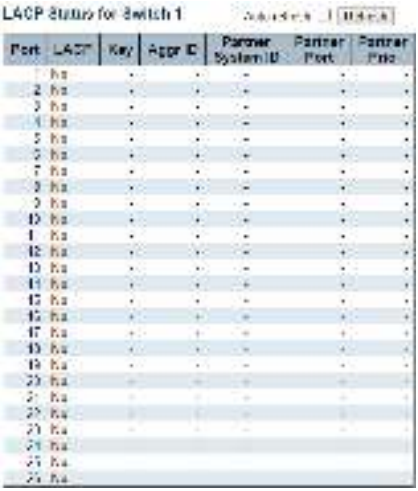
Local Ports
Поле отображает, какие порты являются частью данной агрегации / стэка.

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

10.35.2 LACP – Port Status (LACP – Состояние портов)



На данной странице WEB интерфейса представлена таблица состояния LACP для портов

Port
Номер порта коммутатора

LACP
- ✓ Yes – означает, что LACP включен, а связь с портом установлена.
- ✓ No – означает, что LACP выключен, или порт отключен.

Key
Ключ, назначенный этому порту. Только порты с одинаковым ключом могут быть агрегированы друг с другом

Aggr ID
Идентификатор агрегации, назначенный этой группе агрегации. Идентификаторы 1 и 2 являются GLAG, а идентификаторы 3-14 - LLAG.

Partner System ID
Системный идентификатор устройства * партнера (MAC-адрес).

Partner Port
Номер порта устройства – партнера, подключенного к этому порту коммутатора.

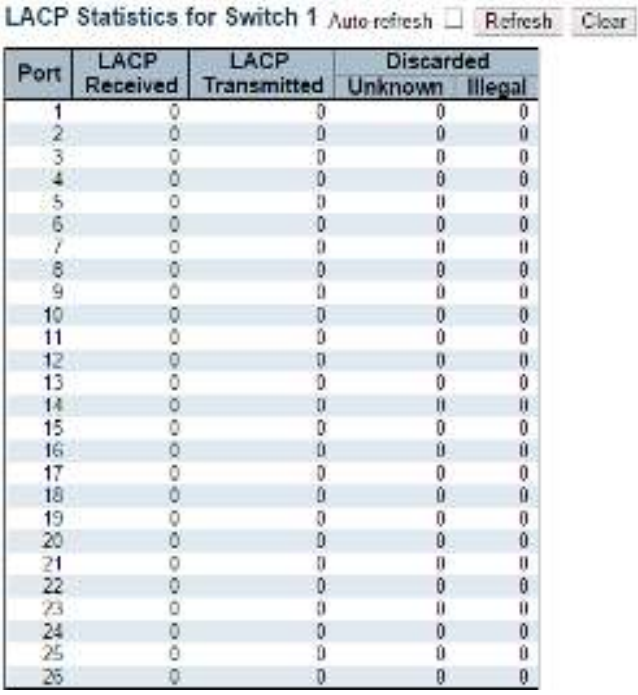
Partner Prio
Приоритет порта партнера.

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

10.35.3 LACP – Port Statistics (LACP – Статистика портов)


LACP Statistics for Switch 1 Auto-refresh Refresh Clear

Port	LACP Received	LACP Transmitted	Discarded Unknown	Discarded Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0
17	0	0	0	0
18	0	0	0	0
19	0	0	0	0
20	0	0	0	0
21	0	0	0	0
22	0	0	0	0
23	0	0	0	0
24	0	0	0	0
25	0	0	0	0
26	0	0	0	0

Port
Номер порта коммутатора

LACP Received
Поле отображает количество LACP фреймов полученных на каждый порт

LACP Transmitted
Поле отображает количество LACP фреймов переданных с каждого порта

Discarded
Поле отображает количество неизвестных или некорректных LACP фреймов, которые были отброшены каждым из портов

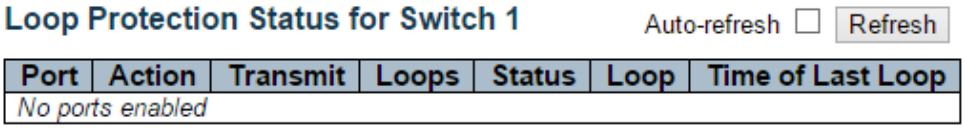
Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

Clear – очистка всех полей для всех портов

10.36 Monitor – Loop Protection (Мониторинг – Защита от сетевых петель)



На данной странице WEB находится таблица состояния защиты портов от сетевых петель.

Port
Номер порта коммутатора.

Action
Действие для порта

Transmit
Действие для порта в режиме передачи данных

Loops
Количество обнаруженных петель на порте

Status
Состояние защиты от петель для данного порта

Loop
Поле показывает, Обнаружена ли в данный момент петля на порте.

Time of Last Loop
Время обнаружения последней сетевой петли.

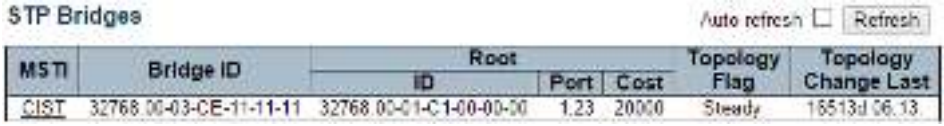
Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

10.37 Monitor – Spanning Tree (Мониторинг – Протокол связующего дерева)

10.37.1 Spanning Tree – Bridge Status (Протокол связующего дерева – Состояние моста)



На данной странице WEB интерфейса находится страница состояние Bridge устройств в STP топологии.

MSTI
Подробное описание статуса моста STP

Bridge ID
Идентификатор моста

Root ID
Идентификатор корневого моста

Root Port
Номер порта коммутатора, выполняющий роль корневого порта.

Root Cost
Стоимость пути. Для корневого моста этот показатель равен 0.

Topology Flag
Текущее состояние Topology Change Flag

Topology Change Last
Время с последнего изменения топологии.

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

10.37.2 Spanning Tree – Port Status (Протокол связующего дерева – Состояние портов)

STP Port Status Auto-refresh ☐ Refresh

Port	CIST Role	CIST State	Uptime
1	Disabled	Discarding	-
2	Disabled	Discarding	-
3	Disabled	Discarding	-
4	Disabled	Discarding	-
5	DesignatedPort	Forwarding	0d 05:30:16
6	Disabled	Discarding	-
7	Disabled	Discarding	-
8	Disabled	Discarding	-
9	Disabled	Discarding	-
10	Disabled	Discarding	-

На данной странице WEB интерфейса отображается состояние портов STP CIST.

Port
Номер порта коммутатора (логический STP порт)

CIST Role
Текущая роль порта STP в CIST. Данное поле может принимать одно из нескольких значений (подробно о ролях написано в соответствующем разделе документации):

- ✓ AlternatePort;
- ✓ BackupPort;
- ✓ RootPort;
- ✓ DesignatedPort;
- ✓ Disabled.

CIST State
Текущее состояние порта STP в CIST. Данное поле может принимать одно из нескольких значений (подробно о ролях написано в соответствующем разделе документации):

- ✓ Discarding – отбрасывание;
- ✓ Learning – запоминание;
- ✓ Forwarding – пересылка.

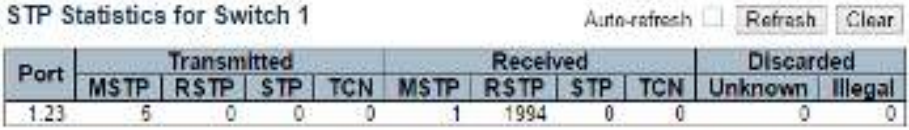
Uptime
Время с последнего момента инициализации порта устройства – моста.

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

10.37.3 Spanning Tree – Port Statistics (Протокол связующего дерева – Статистика портов)


STP Statistics for Switch 1

Auto-refresh | Refresh | Clear

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1.23	5	0	0	0	1	1994	0	0	0	0

На данной странице WEB интерфейса представлена таблицы статистики портов устройств-мостов.

Port
Номер порта коммутатора (логический STP порт)

MSTP
Количество MSTP BPDU, полученных / переданных через порт.

RSTP
Количество RSTP BPDU, полученных / переданных через порт.

STP
Количество устаревших BPDU STP конфигураций, полученных / переданных через порт

TCN
Количество устаревших уведомлений об изменении топологии, полученных / переданных через порт

Discarded Unknown
Количество неизвестных STP BPDU, полученных через порт и отброшенных в дальнейшем.

Discarded Illegal
Количество запрещенных STP BPDU, полученных через порт и отброшенных в дальнейшем.

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

Clear – нажмите, чтобы сбросить счетчики.

10.38 Monitor – MVR (Мониторинг – MVR)

10.38.1 MVR – Statistics (MVR – Статистика)

На данной странице представлена таблица статистики работы функции MVR (технология подключения пользовательских VLAN к одной Multicast VLAN, которая позволяет серверу передавать мультикастовый поток в одной VLAN, в то время как конечные пользователи смогут получать его, находясь в различных VLAN).

VLAN ID
Идентификатор Multicast VLAN ID

IGMP/MLD Queries Received
Количество полученных запросов для IGMP и MLD соответственно

IGMP/MLD Queries Transmitted
Количество отправленных запросов для IGMP и MLD соответственно

IGMPv1 Joins Received
Количество полученных разрешений IGMPv1 на вступление

IGMPv2/MLDv1 Report's Received
Количество полученных разрешений IGMPv2 на вступление и отчетов MLDv1 соответственно

IGMPv3/MLDv2 Report's Received
Количество полученных разрешений IGMPv3 на вступление и отчетов MLDv2 соответственно

IGMPv2/MLDv1 Leave's Received
Количество полученных пакетов IGMPv2 Leave и пакетов MLDv1 Done соответственно.

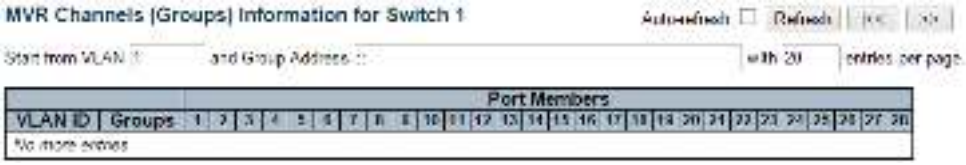
Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

Clear – нажмите, чтобы сбросить счетчики.

10.38.2 MVR – MVR Channel Groups (MVR – Группы каналов MVR)



На данной странице WEB интерфейса находится таблица каналов (групп) MVR. Сортировка происходит сначала по идентификатору VLAN, а затем по группам.

VLAN ID
Идентификатор VLAN ID для группы

Groups
Идентификатор группы для отображаемой в данный момент группы

Port Members
Порты – участники отображаемой группы

Кнопки:

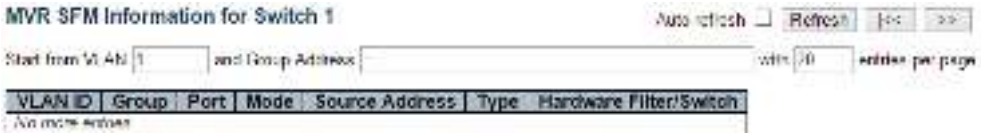
Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

|<< – обновление таблицы, начиная с первой записи в таблице

|>> – обновление таблицы, начиная с записи после последней отображаемой записи.

10.38.3 MVR – MVR SFM Information (MVR – Информация о MVR с SFM)



На данной странице WEB интерфейса содержится информация о MVR с SFM (Многоадресная рассылка с фильтрацией источников).

Сортировка происходит сначала по идентификатору VLAN, затем по группам, а далее по порту

VLAN ID
Идентификатор VLAN ID для группы

Group
Групповой адрес отображаемой группы

Port
Номер порта коммутатора

Mode

Поле отображает режим фильтрации функционирующий на основе (VLAN ID, номер порта, группового адреса)

Source Address

IP Адрес источника.

В настоящее время система ограничивает общее количество IP-адресов источника для фильтрации до 128.

Если адрес источника не указан, в поле «Source Address» отображается текст «None».

Type

Тип фильтрации:

- ✓ Allow – разрешено;
- ✓ Deny – запрещено.

Hardware Filter / Switch

Поле отображает информацию, может ли плоскость данных, предназначенная для определенного группового адреса из исходного адреса IPv4 / IPv6, обрабатываться сетевым чипом коммутатора или нет.

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

|<< – обновление таблицы, начиная с первой записи в таблице

|>> – обновление таблицы, начиная с записи после последней отображаемой записи.

10.39 Monitor – IPMC (Мониторинг – IPMC)

10.39.1 IPMC – IGMP Snooping (MVR – IGMP Snooping)

Состояние IGMP Snooping

На данной странице WEB интерфейса находится таблица состояния функции IGMP Snooping.

VLAN ID
Идентификатор VLAN ID для записи

Querier Version
Версия протокола на запрашивающем устройстве

Host Version
Версия протокола на хосте

Querier Status
Статус запрашивающего устройства

Queries Transmitted
Запросов отправлено

Queries Received
Запросов получено

V1 Reports Received
Получено отчетов версии v1

V2 Reports Received
Получено отчетов версии v2

V3 Reports Received
Получено отчетов версии v3

V2 Leaves Received
Получено пакетов Leave версии v2

Router Port
Поле отображает, какие порты коммутатора действуют, как порты маршрутизатора.
Порт маршрутизатора - это порт на коммутаторе Ethernet, который ведет к устройству многоадресной рассылки (multicast) уровня 3 или к устройству, запрашивающему IGMP.

- ✓ Static – означает, что определенный порт настроен, как порт маршрутизатора.
- ✓ Dynamic – обозначает, что определенный порт считается портом маршрутизатора.
- ✓ Both – что определенный порт настроен или изучен (learned), как порт маршрутизатора.

Port
Номер порта коммутатора

Status
Текущее состояние порта. Отображает, назначен ли порт, как порт маршрутизатора или нет.

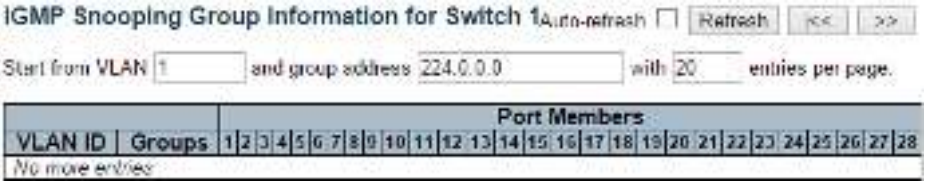
Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

Clear – нажмите, чтобы сбросить счетчики.

Информация о группах IGMP



На данной странице WEB интерфейса находится таблица групп IGMP.

VLAN ID
Идентификатор VLAN ID для группы.

Groups
Адреса групп в отображаемой группе.

Port Members
Порты – участники отображаемой группы.

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

|<< – обновление таблицы, начиная с первой записи в таблице

|>> – обновление таблицы, начиная с записи после последней отображаемой записи.

Информация IPv4 SFM IGMP Snooping

На данной странице WEB интерфейса находится таблица с информацией IGMP SFM (фильтрация источником)

VLAN ID
Идентификатор VLAN ID для группы

Group
Групповой адрес отображаемой группы

Port
Номер порта коммутатора

Mode
Поле отображает режим фильтрации функционирующий на основе (VLAN ID, номер порта, группового адреса)

Source Address
IP Адрес источника.

В настоящее время система ограничивает общее количество IP-адресов источника для фильтрации до 128.

Если адрес источника не указан, в поле «Source Address» отображается текст «None».

Type
Тип фильтрации:

- ✓ Allow – разрешено;
- ✓ Deny – запрещено.

Hardware Filter / Switch
Поле отображает информацию, может ли плоскость данных, предназначенная для определенного группового адреса из исходного адреса IPv4, обрабатываться сетевым чипом коммутатора или нет.

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

|<< – обновление таблицы, начиная с первой записи в таблице

|>> – обновление таблицы, начиная с записи после последней отображаемой записи.

10.39.2 IPMC – MLD Snooping (MVR – IGMP Snooping)

Состояние MLD Snooping

На данной странице WEB интерфейса находится таблица состояния функции IGMP Snooping.

VLAN ID
Идентификатор VLAN ID для записи

Querier Version
Версия протокола на запрашивающем устройстве

Host Version
Версия протокола на хосте

Querier Status
Статус запрашивающего устройства. Может быть:
- ✓ ACTIVE;
- ✓ IDLE;
- ✓ DISABLE.

Queries Transmitted
Запросов отправлено

Queries Received
Запросов получено

V1 Reports Received
Получено отчетов версии v1

V2 Reports Received
Получено отчетов версии v2

V1 Leaves Received
Получено пакетов Leave версии v1

Router Port
Поле отображает, какие порты коммутатора действуют, как порты маршрутизатора.
Порт маршрутизатора - это порт на коммутаторе Ethernet, который ведет к устройству многоадресной рассылки (multicast) уровня 3 или к устройству, запрашивающему IGMP.
- ✓ Static – означает, что определенный порт настроен, как порт маршрутизатора.
- ✓ Dynamic – обозначает, что определенный порт считается портом маршрутизатора.
- ✓ Both – что определенный порт настроен или изучен (learned), как порт маршрутизатора.

Port
Номер порта коммутатора

Status
Текущее состояние порта. Отображает, назначен ли порт, как порт маршрутизатора или нет.

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

Clear – нажмите, чтобы сбросить счетчики.

Информация о группах MLD Snooping

На данной странице WEB интерфейса находится таблица групп MLD Snooping.

VLAN ID
Идентификатор VLAN ID для группы.

Groups
Адреса групп в отображаемой группе.

Port Members
Порты – участники отображаемой группы.

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

|<< – обновление таблицы, начиная с первой записи в таблице

|>> – обновление таблицы, начиная с записи после последней отображаемой записи.

Информация IPv6 SFM MLD Snooping

На данной странице WEB интерфейса находится таблица с информацией MLD SFM (фильтрация источником)

VLAN ID
Идентификатор VLAN ID для группы

Group
Групповой адрес отображаемой группы

Port
Номер порта коммутатора

Mode
Поле отображает режим фильтрации функционирующий на основе (VLAN ID, номер порта, группового адреса)

Source Address
IP Адрес источника.

В настоящее время система ограничивает общее количество IP-адресов источника для фильтрации до 128.

Если адрес источника не указан, в поле «Source Address» отображается текст «None».

Type

Тип фильтрации:

- ✓ Allow – разрешено;
- ✓ Deny – запрещено.

Hardware Filter / Switch

Поле отображает информацию, может ли плоскость данных, предназначенная для определенного группового адреса из исходного адреса IPv6, обрабатываться сетевым чипом коммутатора или нет.

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

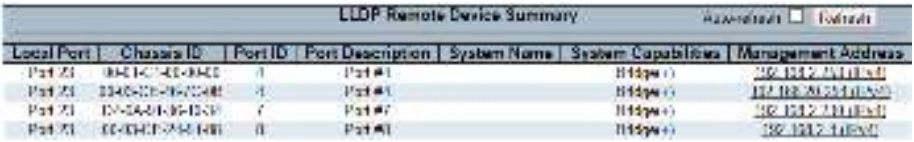
Refresh – нажмите, чтобы обновить страницу;

|<< – обновление таблицы, начиная с первой записи в таблице

|>> – обновление таблицы, начиная с записи после последней отображаемой записи.

10.40 Monitor – LLDP (Мониторинг – LLDP)

10.40.1 LLDP – Neighbours (LLDP – Устройства-соседи)



На данной странице WEB интерфейса находится таблица, в которой отображаются устройства - соседи поддерживающие протокол LLDP.

Local Port
Порт, которым были получены LLDP фреймы.

Chassis ID
Идентификатор фреймов LLDP устройства-соседа.

Port ID
Идентификатор порта устройства- соседа.

Port Description
Описание порта, объявленное устройством-соседом.

System Name
Системное имя, объявленное устройством-соседом.

System Capabilities
Системные возможности устройства-соседа.

1. Other –другое;
2. Repeater – повторитель;
3. Bridge – мост;
4. WLAN Access Point – точка доступа;
5. Router – маршрутизатор;
6. Telephone – телефонный аппарат;
7. DOCSIS cable device – кабельное устройство DOCSIS;
8. Station only – станция;
9. Reserved – зарезервировано.

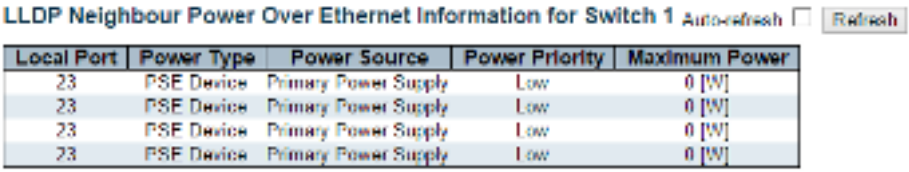
Management Address
Адрес управления - это адрес устройства-соседа, который используется для устройств более высокого уровня, чтобы помочь администратору сети.

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

10.40.2 LLDP – PoE (LLDP – PoE)


LLDP Neighbour Power Over Ethernet Information for Switch 1 Auto-refresh Refresh

Local Port	Power Type	Power Source	Power Priority	Maximum Power
23	PSE Device	Primary Power Supply	Low	0 [W]
23	PSE Device	Primary Power Supply	Low	0 [W]
23	PSE Device	Primary Power Supply	Low	0 [W]
23	PSE Device	Primary Power Supply	Low	0 [W]

На данной странице WEB интерфейса находится таблица устройств-соседей, поддерживающих PoE.

Local Port
Порт, которым были получены LLDP фреймы.

Power Type
Поле «Тип питания» отображает информацию, является ли устройство источником PoE (PSE) или устройством, пиющимся от PoE (PD). Если тип питания не известен, поле содержит запись «Reserved»

Power Source
Источник питания. Основной (Primary) или резервный (Backup)

Power Priority
Приоритет питания для питаемого устройства(PD), связанный с PSE устройством. Существует уровня приоритета:

- ✓ Critical – критический;

- ✓ High – высокий;
- ✓ Low – низкий.

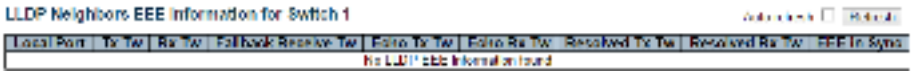
Maximum Power
Максимальное значение мощности в ваттах, требуемая устройством PD от устройства PSE или минимальную мощность, которую устройство PSE способно подавать через кабель максимальной длины в зависимости от его текущей конфигурации.

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

10.40.3 LLDP – EEE (LLDP – EEE)



На данной странице WEB интерфейса находится таблица EEE информации, которая используется протоколом LLDP при обмене.

Local Port
Порт, которым были получены LLDP фреймы.

Tx Tw
Максимальное время в течение которого канал передачи может продолжать отправку данных после сброса LPI.

Rx Tw
Максимальное время в течение которого канал передачи может продолжать прием данных после сброса LPI.

Echo Tx Tw
Поле содержит значение Echo Tx Tw для устройства-партнера по линку.

Echo Rx Tw
Поле содержит значение Echo Rx Tw для устройства-партнера по линку.

Resolved Tx Tw
Разрешенное значение Tx Tw для этого соединения. (не для устройства – партнера по линку)

Resolved Rx Tw
Разрешенное значение Rx Tw для этого соединения (не для устройства – партнера по линку)

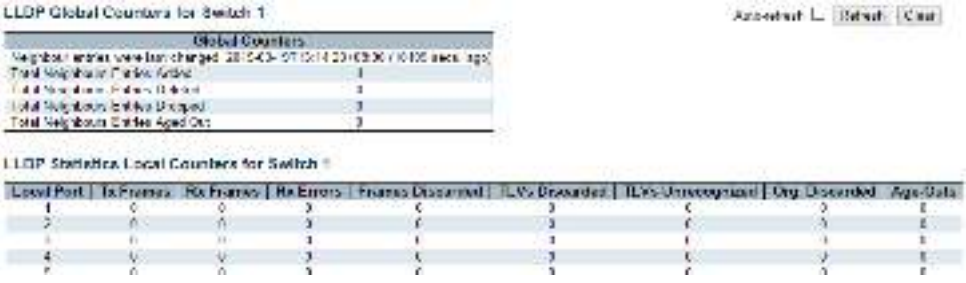
EEE in Sync
Поле отображает информацию о согласовании времени пробуждения коммутатором и устройством-партнером по линку.

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

10.40.4 LLDP – Port Statistics (LLDP – Статистика портов)



На данной странице WEB интерфейса представлена таблица статистики трафика LLDP для всех портов.

Глобальные столбцы

Neighbour entries were last changed
Поле отображает время удаления или добавления последней записи. Это поле также показывает время, прошедшее с момента обнаружения последнего изменения.

Total Neighbours Entries Added
Поле отображает количество новых записей, добавленных после перезагрузки коммутатора.

Total Neighbours Entries Deleted
Поле отображает количество новых записей, удаленных после перезагрузки коммутатора.

Total Neighbours Entries Dropped
Поле отображает количество фреймов LLDP, отброшенных из-за переполнения таблицы ввода.

Total Neighbours Entries Aged Out
Поле отображает количество записей, удаленных из-за истечения срока действия.

Локальные столбцы

Local Port
Порт, которым были получены или переданы LLDP фреймы.

Tx Frames
Количество LLDP фреймов, переданных этим портом

Rx Frames
Количество LLDP фреймов, полученных этим портом

Rx Errors
Количество LLDP фреймов, содержащих ошибки, полученных этим портом

Frames Discarded
Если на порт получен фрейм LLDP, а внутренняя таблица коммутатора заполнена, фрейм LLDP учитывается и отбрасывается. Эта ситуация известна как «Too many Neighbours» в стандарте LLDP.

TLVs Discarded
Каждый фрейм LLDP может содержать несколько фрагментов информации, известных как TLV (TLV - сокращение от «Type Length Value»). Если TLV искажен, он учитывается и отбрасывается.

TLVs Unrecognized
Количество корректных TLV, но неизвестного типа

Org. Discarded
Количество полученных TLV

Age-Outs
Каждый фрейм LLDP содержит информацию о том, как долго информация LLDP является действительной (Age Outs Time).

Если в течение времени ожидания не получен новый фрейм LLDP, информация LLDP удаляется, и Age Outs Time увеличивается.

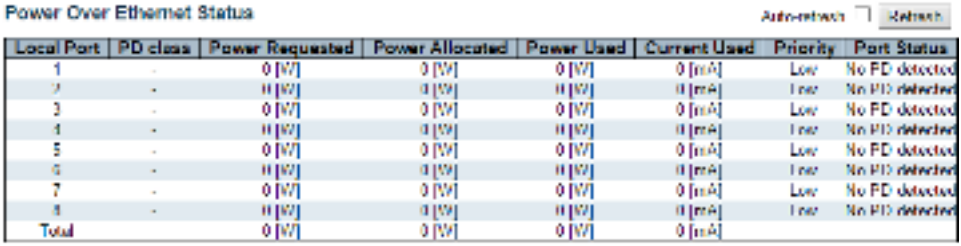
Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

Clear – нажмите, чтобы очистить все локальные счетчики.

10.41 Monitor – PoE (Мониторинг – PoE)


Power Over Ethernet Status

Auto-refresh Refresh

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
2	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
3	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
4	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
5	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
6	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
7	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
8	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
Total		0 [W]	0 [W]	0 [W]	0 [mA]		

На данной странице WEB интерфейса находится таблица состояния PoE на портах.

Local Port
Номер порта коммутатора

PD Class
Класс питаемого устройства (PD). Основан на максимальной мощности которую требует питаемое устройство (PD). Всего предусмотрено 5 классов:

- ✓ Class 0 – максимальная мощность 15,4 Вт;
- ✓ Class 1 – максимальная мощность 4,0 Вт;
- ✓ Class 2 – максимальная мощность 7,0 Вт;
- ✓ Class 3 – максимальная мощность 15,4 Вт;
- ✓ Class 4 – максимальная мощность 30 Вт.

Power Requested
Запрашиваемая мощность – поле, отображающее мощность в ваттах, которую PD хочет зарезервировать.

Power Allocated
Мощность, выделяемая коммутатором для PD

Current Used
Данное поле отображает текущее потребление тока в амперах для PD

Priority

Поле приоритета отображает приоритет порта, настроенный пользователем.

Port Status

Поле состояния порта может принимать следующие значения:

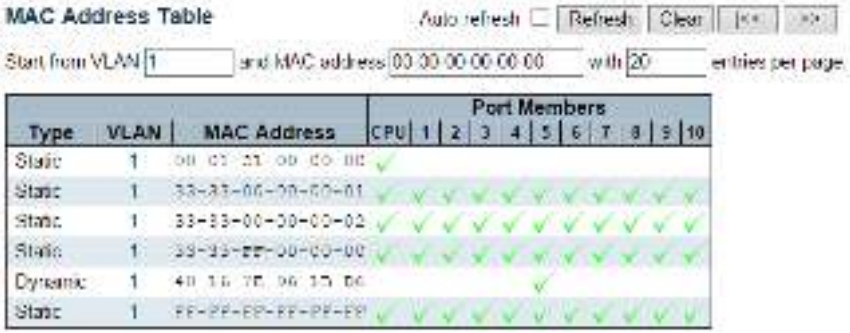
- ✓ PoE not available – PoE не поддерживается подключенным устройством, PoE чип не найден. PoE не поддерживается портом;
- ✓ PoE turned OFF – PoE отключено пользователем;
- ✓ PoE turned OFF – Общий бюджет PoE превышен;
- ✓ No PD detected – Не обнаружено PoE устройство при подключении;
- ✓ PoE turned OFF – PD в перегрузке, PD устройство запросило мощность больше, чем порт способен выдать.
- ✓ PoE turned OFF – подключенное PoE устройство выключено;
- ✓ Invalid PD – PD устройство обнаружено, но работает некорректно

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

10.42 Monitor – MAC Table (Мониторинг – Таблица MAC адресов)



На данной странице WEB интерфейса представлена таблица MAC адресов. Она может содержать 8192 записи. Сортировка происходит сначала по VLAN ID, а затем по MAC адресу.

Столбцы таблицы MAC адресов

Type
Тип записи – динамический или статический;

MAC address
MAC адрес, относящийся к записи

VLAN
VLAN ID, относящийся к записи

Port members
Порты-участники, относящиеся к записи

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

Clear –нажмите, чтобы очистить все динамические записи;

|<< – обновляет таблицу начиная с первой записи;

>> – обновляет таблицу начиная с последней записи.

10.43 Monitor – VLANs (Мониторинг – сети VLAN)

10.43.1 VLANs – VLAN Membership (сети VLAN – порты-участники VLAN)

На данной странице WEB интерфейса представлена таблица состояния пользователей VLAN.

VLAN User

Различные программные модули WEB интерфейса могут использовать службы VLAN для настройки VLAN на лету.

В раскрывающемся списке справа можно выбрать между отображением портов-участников VLAN в соответствии с настройками администратора (администратора) или в соответствии с настройками внутренних программных модулей.

Комбинированная запись отображает комбинацию администраторских настроек и настроек внутренних программных модулей.

VLAN ID

Идентификатор VLAN для которой отображаются порты-участники.

Port Members

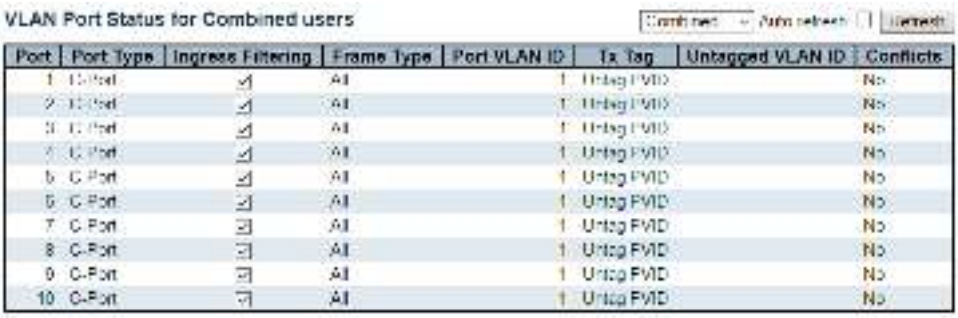
Строка чек-боксов для каждого порта для каждого VLAN ID

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

10.43.2 VLANs – VLAN Ports (сети VLAN – Состояние портов VLAN)


VLAN Port Status for Combined users

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	☑	All	1	Untag PVID		No
2	C-Port	☑	All	1	Untag PVID		No
3	C-Port	☑	All	1	Untag PVID		No
4	C-Port	☑	All	1	Untag PVID		No
5	C-Port	☑	All	1	Untag PVID		No
6	C-Port	☑	All	1	Untag PVID		No
7	C-Port	☑	All	1	Untag PVID		No
8	C-Port	☑	All	1	Untag PVID		No
9	C-Port	☑	All	1	Untag PVID		No
10	C-Port	☑	All	1	Untag PVID		No

На данной странице WEB интерфейса находится таблица состояния портов VLAN

VLAN User

Различные программные модули WEB интерфейса могут использовать службы VLAN для настройки VLAN на лету.

В раскрывающемся списке справа можно выбрать между отображением портов-участников VLAN в соответствии с настройками администратора (администратора) или в соответствии с настройками внутренних программных модулей.

Комбинированная запись отображает комбинацию администраторских настроек и настроек внутренних программных модулей.

Port

Логический номер порта, к которому относятся все настройки в той же строке.

Port Type

Поле отображает тип порта, который настраивается пользователем. Поле остается пустым, если оно не переопределено пользователем.

Ingress Filtering

Поле отображает наличие входной фильтрации. Поле остается пустым, если оно не переопределено пользователем.

Frame Type

Поле отображает допустимые типы фреймов (All, Taged, Untagged), которые данный пользователь хочет настроить на порту. Поле остается пустым, если оно не переопределено пользователем.

Port VLAN ID

Показывает идентификатор VLAN порта (PVID), который пользователь хочет закрепить за портом.

Поле остается пустым, если оно не переопределено пользователем.

TxTag

Поле отображает требования (Tag All, Tag PVID, Tag UVID, Untag All, Untag PVID, Untag UVID), которые пользователь настроил на порту.

Поле остается пустым, если оно не переопределено пользователем.

Untagged VLAND ID

Если Tx Tag переопределен выбранным пользователем и для него установлено значение Tag или Untag UVID, то в этом поле будет отображаться идентификатор VLAN, который пользователь хочет пометить тэгом или удалить из тега на выходе.

Поле остается пустым, если оно не переопределено пользователем.

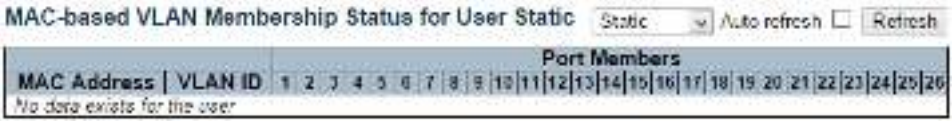
Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

10.44 Monitor – VCL (Мониторинг – VCL)

10.44.1 VCL – MAC based VLAN (VCL – VLAN на базе MAC адресов)



На данной странице WEB интерфейса представлена таблица записей VLANов на базе MAC адресов для различных VLAN пользователей

MAC Address
Поле отображает MAC адрес

VLAN ID
Поле отображает VLAN ID

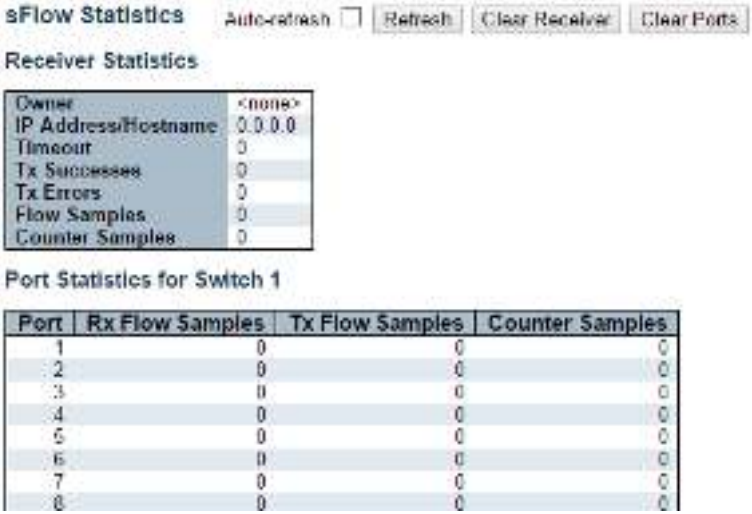
Port Members
Порты – участники VLAN на базе MAC адресов.

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

10.45 Monitor – sFlow (Мониторинг – sFlow)



На данной странице WEB интерфейсе представлена страница статистики sFlow.

Owner (Владелец)
В этом поле отображается текущий владелец конфигурации sFlow. Доступны следующие значения:

- ✓ Если sFlow в настоящее время не настроен / не востребован, поле owner содержит значение <none>.
- ✓ Если sFlow в настоящее время настроен с помощью WEB или CLI, поле owner содержит значение < Configured through local management >.
- ✓ Если sFlow в настоящее время настроен с помощью SNMP, поле owner содержит строку, идентифицирующую получателя sFlow.

IP Address/Hostname
IP-адрес или имя хоста sFlow.получателя.

Timeout
Количество секунд, оставшееся до остановки выборки и освобождения текущего владельца sFlow.

Tx Successes
Количество дейтаграмм UDP, успешно отправленных получателю sFlow.

Tx Errors
Количество дейтаграмм UDP, неотправленных получателю sFlow из за ошибок.

Наиболее распространенным источником ошибок является недопустимая конфигурация IP-адреса / имени хоста получателя sFlow.

Flow Samples
Общее количество выборок потока, отправленных получателю sFlow.

Counter Samples
Общее количество счетчиков выборок, отправленных получателю sFlow

Статистика портов

Port
Номер порта, к которому относится текущая статистика.

Rx and Tx Flow Samples
Количество выборок потока, отправленных получателю sFlow, исходящих с этого порта.

Выборки потока делятся на выборки потока Rx и Tx, где выборки потока Rx содержат количество пакетов, которые были отобраны при приеме (входе) в порт, а выборки потока Tx содержат количество пакетов, которые были отобраны при передаче (выход) на порте.

Counter Samples
Общее количество счетчиков выборок, отправленных получателю sFlow

Кнопки:

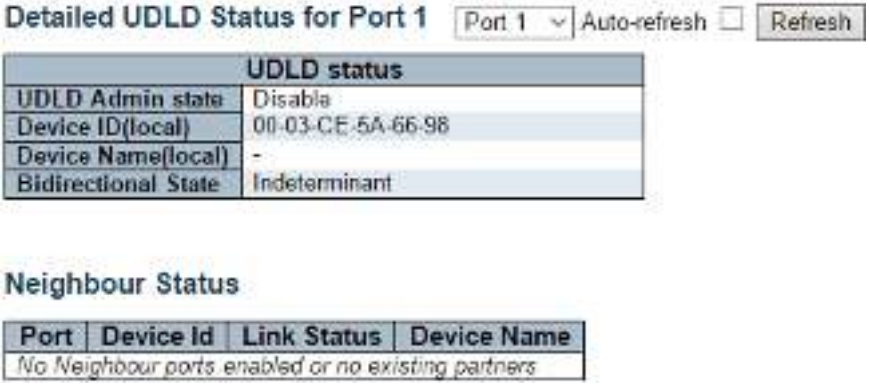
Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

Clear Receiver – нажмите, чтобы очистить счетчики получателя;

Clear Port – нажмите, чтобы очистить счетчики для портов.

10.46 Monitor – UDLD (Мониторинг – UDLD)



На данной странице WEB интерфейса находится таблица состояний UDLD для портов.

Состояние UDLD для портов

UDLD Admin State
Текущее состояние порта.

Device ID(local)
Идентификатор устройства

Device Name(local)
Имя устройства

Bidirectional State
Текущий режим работы порта (двунаправленный / однонаправленный)

Состояние устройства-соседа

Port
Текущий порт устройства-соседа

Device ID
Текущий идентификатор устройства-соседа

Link Status
Текущее состояние подключения к порту устройства-соседа

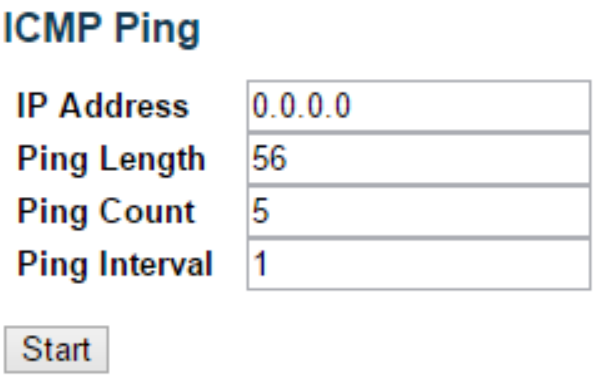
Device Name
Имя устройства-соседа

Кнопки:

Auto - Refresh – нажмите, чтобы обновить страницу автоматически раз в 3 сек.;

Refresh – нажмите, чтобы обновить страницу;

10.47 Diagnostics – Ping (Диагностика – команда Ping)



На данной странице WEB интерфейса находится инструмент диагностики Ping.

После нажатия кнопки «Start» начинают передаваться ICMP-пакеты, а порядковый номер и время прохождения сигнала отображаются при получении ответа.

Объем данных, полученных внутри IP-пакета типа ICMP ECHO_REPLY, всегда будет на 8 байт больше, чем запрашиваемое пространство данных (заголовок ICMP).

Страница обновляется автоматически до получения ответов на все пакеты или до истечения времени ожидания.

Например:

PING server 10.10.132.20, 56 bytes of data.
64 bytes from 10.10.132.20: icmp_seq=0, time=0ms
64 bytes from 10.10.132.20: icmp_seq=1, time=0ms
64 bytes from 10.10.132.20: icmp_seq=2, time=0ms
64 bytes from 10.10.132.20: icmp_seq=3, time=0ms
64 bytes from 10.10.132.20: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad

IP Address
IP адрес назначения (другое устройство и тд.)

Ping Length
Размер ICMP пакета. Может быть от 2 до 1452 байт.

Ping Count
Количество передаваемых пакетов. От 1 до 60.

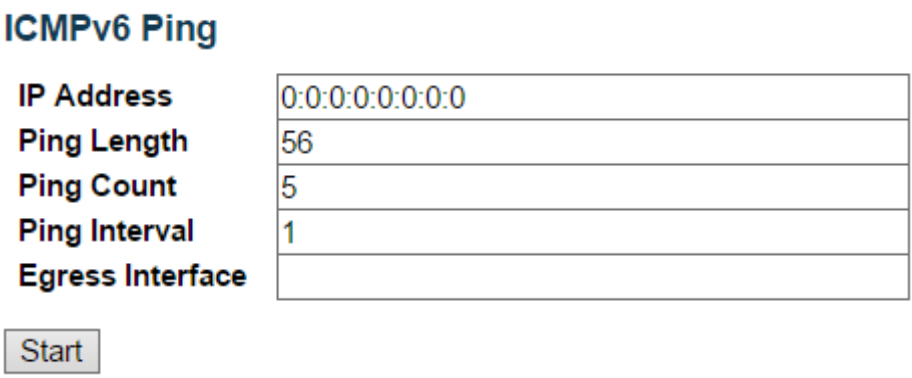
Ping Interval
Интервал передачи пакетов ICMP в секундах. От 0 до 30 сек.

Кнопки:

Start – нажмите, чтобы начать передавать ICMP пакеты

New Ping – нажмите, чтобы перезапустить диагностику с помощью Ping

10.48 Diagnostics – Ping6 (Диагностика – команда Ping6)



На данной странице WEB интерфейса находится инструмент диагностики Ping для проверки IPv6 соединений.

После нажатия кнопки «Start» начинают передаваться ICMPv6-пакеты, а порядковый номер и время прохождения сигнала отображаются при получении ответа.

Например:

PING6 server ::10.10.132.20, 56 bytes of data.
64 bytes from ::10.10.132.20: icmp_seq=0, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=1, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=2, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=3, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad

IP Address
IP адрес назначения (другое устройство и тд.)

Ping Length
Размер ICMP пакета. Может быть от 2 до 1452 байт.

Ping Count
Количество передаваемых пакетов. От 1 до 60.

Ping Interval

Интервал передачи пакетов ICMP в секундах. От 0 до 30 сек.

Egress Interface (Only for IPv6)

Идентификатор VLAN (VID) конкретного выходного интерфейса IPv6, по которому проходит пакет ICMP.

Заданный VID находится в диапазоне от 1 до 4094 и будет действовать только при действующем соответствующем интерфейсе IPv6.

Когда исходящий интерфейс не задан, PING6 находит интерфейс наилучшего соответствия для пункта назначения.

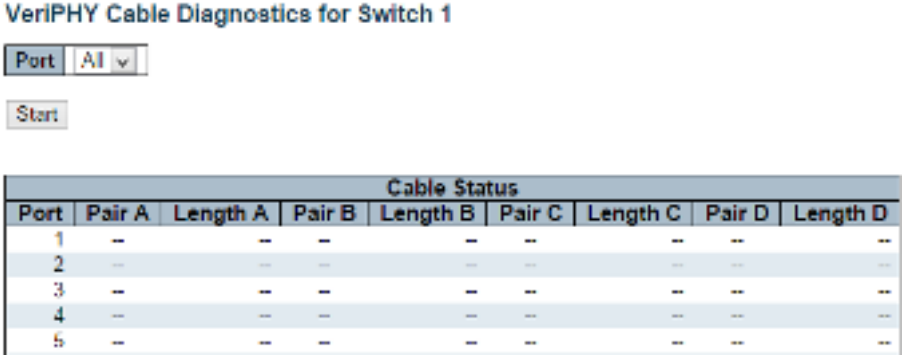
Не указывайте выходной интерфейс для адреса обратной связи. Укажите выходной интерфейс для локального или многоадресного (multicast) адреса.

Кнопки:

Start – нажмите, чтобы начать передавать ICMP пакеты

New Ping – нажмите, чтобы перезапустить диагностику с помощью Ping

10.49 Diagnostics – VeriPHY (Диагностика – инструмент VeriPHY)



На данной странице WEB интерфейса находится инструмент для диагностики кабельных соединений для 10/100 и 1G портов.

Нажмите «Start» чтобы начать диагностику. Приблизительное время диагностики 5 сек. Если выбраны все порты, время диагностики увеличивается до 15 сек.

Когда диагностика завершится, страница автоматически обновится, результаты диагностики отобразятся в полях таблицы.

Точность инструмента достигается при длине кабеля подключения от 7 – 140м.

Порты 10 и 100 Мбит/с отключаются при активной работе инструмента VeriPHY. Поэтому запуск VeriPHY на порте управления 10 или 100 Мбит / с приведет к тому, что коммутатор перестанет отвечать до завершения VeriPHY.

Port

Порт, для которого выполняется диагностика с помощью VeriPHY

Cable Status

Port:

- ✓ Номер порта

Pair:

- ✓ OK
- ✓ OPEN
- ✓ Short
- ✓ Short A
- ✓ Short B
- ✓ Short C
- ✓ Short D
- ✓ Cross A
- ✓ Cross B
- ✓ Cross C
- ✓ Cross D

Length

Длина (в метрах) кабельной пары.

10.50 Maintenance – Restart Device (Обслуживание – Перезагрузка устройства)

На данной странице WEB интерфейса находится инструмент для принудительной перезагрузки коммутатора.

Кнопки:

Yes – нажмите, чтобы перезагрузить коммутатор;

No – нажмите, чтобы вернуться к состоянию портов без перезагрузки.

10.51 Maintenance – Factory Defaults (Обслуживание – Возврат к заводским настройкам)

На данной странице WEB интерфейса находится инструмент, позволяющий вернуть коммутатор к заводским настройкам. Будет сохранена только IP конфигурация.

Новая конфигурация доступна сразу, что означает, что перезапуск не требуется

Кнопки:

Yes – нажмите, чтобы сбросить коммутатор к заводским настройкам;

No – нажмите, чтобы вернуться к состоянию портов без сброса настроек.

Примечание. Восстановление заводских настроек по умолчанию также можно выполнить, соединив физически 1 и 2 порты в течение первой минуты после перезагрузки коммутатора. В первую минуту после перезагрузки пакеты «loopback» будут передаваться через порт 1. Если пакет «loopback» получен через порт 2, коммутатор выполнит возврат к заводским настройкам.

10.52 Maintenance – Software (Обслуживание – Прошивка)

10.52.1 Software – Upload (Прошивка – Загрузка образа)

На данной странице WEB интерфейса находится инструмент для обновления прошивки коммутатора.

Кнопки:

Choose File – нажмите, чтобы выбрать файл-образ прошивки;

Update – нажмите, чтобы приступить к загрузке новой прошивки.

Система проинформирует вас, когда прошивка будет загружена в коммутатор. После установки новой прошивки, коммутатор будет перезагружен.

Внимание! Страница управления WEB будет недоступна в процессе установки новой прошивки. Не перезагружайте коммутатор самостоятельно в ходе установки прошивки и не отключайте питание!

10.52.2 Software – Image Select (Прошивка – Выбор основной и резервной прошивки)

На данной странице WEB интерфейса находится информация о текущей и резервной прошивках.

Примечание. Если текущий образ прошивки является и резервным образом, то отображается только таблица «Текущий образ прошивки».

В этом случае кнопка «Активировать резервный образ» также отключена.

Если резервный образ прошивки активен (из-за повреждения основного образа), при загрузке нового образа прошивки на устройство автоматически будет использоваться слот основной прошивки, он же будет активирован.

Информация о версии и дате прошивки может быть пустой для старых версий прошивки. Это не является ошибкой.

Информация об образе прошивки.

Image
Имя образа с прошивкой. Имя резервного образа прошивки содержит «.bk» в конце названия

Version
Версия образа с прошивкой.

Date
Дата, когда прошивка была создана.

Кнопки:

Activate – нажмите, чтобы выбрать резервный образ прошивки в качестве основного;

Cancel – нажмите, чтобы отменить активацию резервной прошивки.

10.53 Maintenance – Configuration (Обслуживание – Конфигурация)

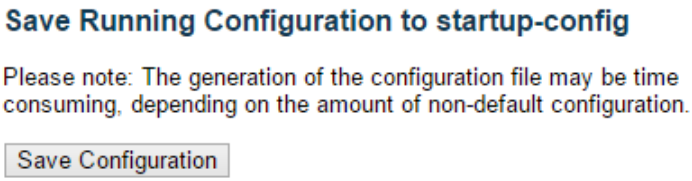
На данной странице WEB интерфейса находится инструмент для выбора конфигураций для коммутатора. Всего предусмотрено 3 типа конфигураций:

- ✓ Running config – файл, который содержит текущую конфигурацию коммутатора. Файл будет удален, если коммутатор будет перезагружен. Необходимо сохранить файл, как стартовую конфигурацию (startup), чтобы изменения были сохранены;

- ✓ Startup config – стартовая конфигурация коммутатора (при запуске). Будет прочитана при загрузке коммутатора.

- ✓ Default config – конфигурация только для чтения. Будет применена, когда система была возвращена к заводским настройкам.

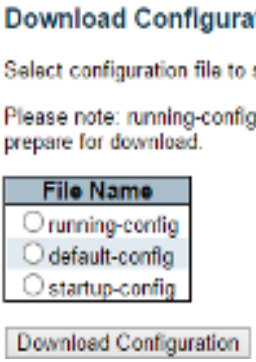
10.53.1 Configuration – Save Startup-config (Конфигурация – Сохранение стартовой конфигурации)



Кнопки:

Save Configuration – нажмите, чтобы сохранить текущую конфигурацию в виде стартовой.

10.53.2 Configuration – Download (Конфигурация – Загрузка)

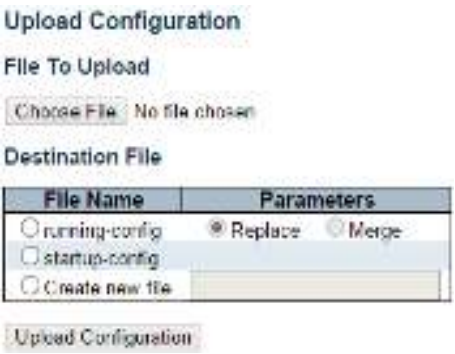


File Name
Выбор конфигурации, файл с которой необходимо загрузить на ПК.

Кнопки:

Download Configuration – нажмите, чтобы сохранить файл с конфигурацией на ПК.

10.53.3 Configuration – Upload (Конфигурация – Выгрузка)



File to Upload

Выбор конфигурации, файл с которой необходимо выгрузить с ПК на коммутатор (нажмите кнопку «choose file»).

Destination File

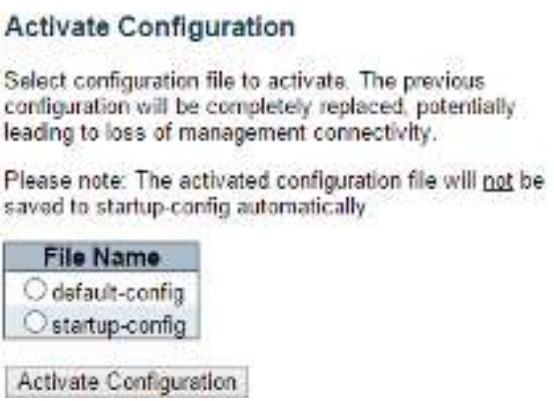
Выбор конфигурации, которая будет заменена файлом, выгруженным с ПК

- ✓ **Replace Mode** – текущая конфигурация будет полностью заменена выгруженным файлом с ПК
- ✓ **Merge Mode** – выгруженный файл будет совмещен с текущей конфигурацией коммутатора (running config)

Кнопки:

Upload Configuration – нажмите, чтобы выгрузить файл с конфигурацией с ПК на коммутатор.

10.53.4 Configuration – Activate (Конфигурация – Активация)

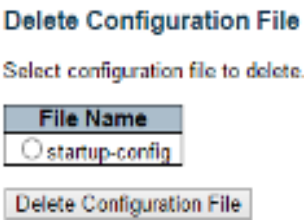


На данной странице WEB интерфейса есть возможность немедленно активировать выбранный файл с конфигурацией.

Кнопки:

Activate Configuration – нажмите, чтобы немедленно активировать файл с выбранной конфигурацией.

10.53.5 Configuration – Delete (Конфигурация – Удаление)



На данной странице WEB интерфейса есть возможность удалить файл с конфигурацией, сохраненный в коммутаторе.

Кнопки:

Delete Configuration File – нажмите, чтобы удалить файл с выбранной конфигурацией.

Внимание

- ✓ Для защиты оборудования от грозовых разрядов необходимо устанавливать устройства грозозащиты!
- ✓ Для того чтобы произвести **сброс** коммутатора к заводским настройкам необходимо соединить патчкордом UTP cat 5e 1й и 2й порты коммутатора. После получения 2м портом пакетов от первого – сброс к заводским настройкам будет осуществлен. Также операцию сброса настроек можно провести через WEB интерфейс.

8. Технические характеристики*

Модель	**SW-60822/ILR**	**SW-80822/ILR**
Общее кол-во портов	10	
Кол-во портов FE+PoE	8	-
Кол-во портов FE	-	-
Кол-во портов GE+PoE	-	8
Кол-во портов GE (не Combo порты)	-	
Кол-во портов Combo GE (RJ45+SFP)	2 GE	
Кол-во портов SFP (не Combo порты)	-	
Мощность PoE на один порт (макс.)	30 Вт	
Суммарная мощность PoE всех портов (макс.)	240 Вт	
Стандарты PoE	IEEE 802.3af IEEE 802.3at	
Метод подачи PoE	Метод А 1/2(+), 3/6(-)	
Встроенные оптические порты	-	
Топологии подключения	звезда каскад кольцо	
Буфер пакетов	4 МБ	
Таблицы MAC-адресов	8 К	

Пропускная способность коммутационной матрицы (Switching fabric)	5.6 Гбит/с	20 Гбит/с
Скорость обслуживания пакетов (Forwarding rate)	100 Мбит/с - 148,800 пакетов/с 10 Мбит/с- 14,880 пакетов/с	1000 Мбит/с – 1488,000 пакетов/с 100 Мбит/с - 148,800 пакетов/с 10 Мбит/с- 14,880 пакетов/с
Поддержка jumbo frame	9.6 КБ (только на медном порте Combo-порта)	9.6 КБ
Стандарты и протоколы	IEEE 802.3 10Base-T Ethernet IEEE 802.3u 100Base-TX IEEE 802.3ab 1000Base-T IEEE 802.3z 1000Base-X IEEE 802.3x Flow Control & Back Pressure IEEE 802.3 af/at Power over Ethernet IEEE 802.3az Energy Efficient Ethernet (EEE) IEEE 1588 Precision Time Protocol (PTP) IEEE G.8032 Ethernet Ring Protection IEEE 802.1D-2004 for Spanning Tree Protocol IEEE 802.1w for Rapid STP IEEE 802.1p for Class of Service IEEE 802.1X for Authentication IEEE 802.1Q for VLAN Tagging Протоколы: CSMA/CD, IGMP v1/v2, SNMP v1/v2c/v3, TFTP, SNTP, SMTP, RARP, RMON, Syslog, HTTP, Telnet, LLDP, HTTPS, SSH	
Функции уровня 2	802.1Q VLAN and 802.1ad Q-in-Q provider bridge IGMP/MLD Snooping IGMP/MLD query DHCP Client/Server/Relay with Option 82 Internet Protocol Version 6 (IPv6) Port Status, Statistics, Monitoring, Security, and Rate Limiting, SFP DDM Loop Detection, *PD Alive, Port Mirroring, uPnP, Modbus/TCP	
Качество обслуживания (QoS)	CoS ToS Diffserv mapping	

	SPQ/WRR queuing	
Безопасность	User Name / Password Protection User Privilege: up to 15 levels IEEE 802.1x: Port-based Access Control IP Source Guard MAC Based Authentication Web-based Authentication HTTPS SSHv2 RADIUS: Authentication/ Accounting TACACS+: Authentication ACL (Access control list)	
Управление	Web Telnet, Console, Cisco-like CLI, F/W upgrade	
Индикаторы	индикатор основного и резервного питания; индикатор ошибки; индикаторы Ethernet.	
Реле аварийной сигнализации	DC24V,1A(HO, H3)	
Питание**	DC 45-57V (с резервированием)	
Энергопотребление (без нагрузки PoE)	12 Вт	15 Вт
Встроенная грозозащита	6 кВ	
Охлаждение	Конвекционное (без вентилятора)	
Класс защиты	IP30	
Размеры (ШхВхГ) (мм)	75x175x125	
Способ монтажа	на DIN-рейку (вертикально)	
Рабочая температура	-40...+70 °C	
Дополнительно	DIP – переключатели для вкл/откл тревоги Console порт (RJ-45) для управления коммутатором через CLI по RS232 интерфейсу	

* Производитель имеет право изменять технические характеристики изделия и комплектацию без предварительного уведомления.
**Блоки питания в комплект поставки не входят.

9. Гарантия

Гарантия на все оборудование OSNOVO – 60 месяцев с даты продажи, за исключением аккумуляторных батарей, гарантийный срок - 12 месяцев.

В течение гарантийного срока выполняется бесплатный ремонт, включая запчасти, или замена изделий при невозможности их ремонта.

Подробная информация об условиях гарантийного обслуживания находится на сайте www.osnovo.ru

Составил: Елагин С.А.