SYMANITRON

Инновационные
промышленные сети

SWMGR-812GSFP
промышленный коммутатор L3

Руководство пользователя

Настройка и управление

Оглавление

Условные обозначения

1. Условные обозначения в тексте

Формат	Описание
< >	Скобки < > обозначают «кнопки». Например, нажмите кнопку <Set>
[ ]	Скобки [ ] обозначают имя окна или имя меню. Например, нажмите пункт меню [File]
→	Многоуровневое меню разделяется посредством знака «→». Например, [Start] → [All Programs] → [Accessories]. Нажмите меню [Start], войдите в подменю [All programs], затем войдите в подменю [Accessories]
/	Возможность выбора одной, двух или более опций обозначается при помощи символа «/». Например, «Add/Subtract» означает добавить или удалить

2. Условные символы

Символ	Описание
 **Предостережение**	Эти вопросы требуют внимания во время работы с устройством при настройке, а также дают дополнительную информацию
 **Заметка**	Необходимые пояснения к содержимому выполняемых операций с устройством
 **Внимание**	Вопросы, требующие особого внимания. Некорректная работа с устройством может привести к потере данных или повреждению

1. Приступая к работе

1.1 Основная информация о коммутаторе

SWMGR-812GSFP представляет собой управляемый Ethernet-коммутатор с 8 портами 10/100/1000Base-T(X) и 12 портами 100/1000Base-X SFP, оснащенный функциями сетевого резервирования. Устройство поддерживает маршрутизацию третьего уровня для повышения производительности в крупномасштабных локальных сетях. Аппаратная часть коммутатора оптимизирована для передачи данных с такой же скоростью, как у коммутаторов уровня 2. Благодаря поддержке протоколов резервирования и MSTP, совместимого с RSTP/STP, обеспечивается защита критически важных приложений от сетевых сбоев или временных неисправностей. Коммутатор может работать в широком диапазоне температур от -40 до +70°C и управляться через веб-интерфейс, Telnet и консоль (CLI). Таким образом, SWMGR-812GSFP является надежным компонентом управления сетями Ethernet, в том числе оптоволоконными.

1.2 Функциональные возможности ПО

- Поддерживает Sy-Ring (время восстановления < 30 мс на 250 единиц соединения) и MSTP (совместимый с RSTP/STP) для резервирования Ethernet
- Поддерживает All-Ring для взаимодействия с кольцевой технологией других поставщиков в открытой архитектуре
- Поддерживает Sy-Union, позволяющий использовать несколько резервных сетевых колец.
- Поддерживает стандартную функцию IEC 62439-2 MRP (протокол резервирования среды передачи данных)
- Поддерживает синхронизацию часов IEEE 1588v2
- Поддерживает новую версию интернет-протокола IPv6
- Поддерживает протокол Modbus TCP
- Поддерживает энергоэффективную технологию Ethernet IEEE 802.3az
- Предоставляет протоколы HTTPS/SSH для повышения безопасности сети
- Поддерживает SMTP-клиент
- Поддерживает управление полосой пропускания на основе IP
- Поддерживает управление QoS на основе приложений
- Поддерживает функцию безопасной привязки устройств
- Поддерживает автоматическое предотвращение атак DoS/DDoS
- Поддерживает IGMP v2/v3 (IGMP Snooping) для фильтрации многоадресного трафика
- Поддерживает SNMP v1/v2c/v3, RMON и управление VLAN 802.1Q

- Поддерживает ACL, TACACS+ и аутентификацию пользователей 802.1x
- Поддерживает Jumbo-фрейм размером 9,6 Кбайт
- Поддерживает различные виды уведомлений об инцидентах
- Поддерживает управление через веб-интерфейс, Telnet, консоль (CLI)
- Поддерживает протокол LLDP

1.3 Аппаратные характеристики

- 8 портов 10/100/1000Base-T(X)
- 12 портов SFP 100/1000Base-X
- 1 консольный порт
- Резервированные входы питания DC
- Поддерживается монтаж на DIN-рейку и на стену
- Рабочая температура: от -40 до +70°C
- Температура хранения: от -40 до +85°C
- Рабочая влажность: от 5 до 95%, без конденсации
- Корпус: IP30
- Размеры в мм: 96,4 (Ш) x 145,5 (Г) x 154 (В)

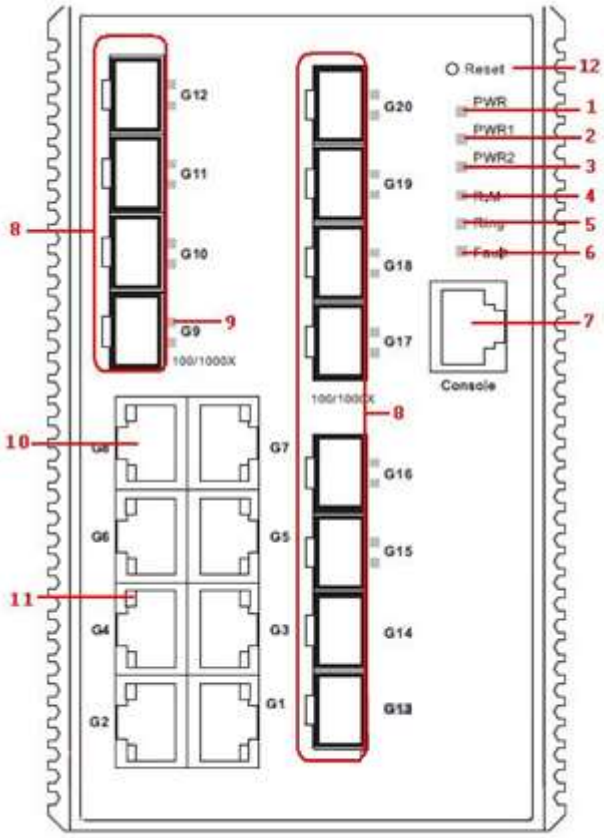
2. Описание оборудования

2.1 Передняя панель

2.1.1 Порты и коннекторы

Коммутатор имеет следующие порты на передней панели:

Порт	Количество, описание
Порт SFP	12 x 100 /1000Base-X
Порт Ethernet	8 x 10/100/1000Base-T(X); RJ-45
Консольный порт	1 консольный порт; RJ-45



1. Индикатор состояния питания
2. Индикатор активности источника питания 1
3. Индикатор активности источника питания 2
4. Индикатор мастера кольца
5. Индикатор состояния кольца
6. Индикатор неисправности
7. Консольный порт
8. Порты SFP
9. Индикатор состояния соединения портов SFP
10. Порты Ethernet (LAN)
11. Индикатор соединения/работы/скорости LAN-портов
12. Кнопка сброса

Рисунок 1 – Передняя панель

2.1.2 Светодиодные индикаторы

Таблица 1 – Светодиодные индикаторы

Индикатор	Цвет	Состояние	Описание
PWR	Зеленый	Горит	Питание постоянного тока включено
PWR1	Зеленый	Горит	Активирован модуль питания 1
PWR2	Зеленый	Горит	Активирован модуль питания 2
R.M	Зеленый	Горит	Устройство является главным в кольцевой топологии
Ring	Зеленый	Горит	Кольцо включено
		Мигает	Кольцо разомкнуто
Fault	Желтый	Горит	Индикатор неисправности (сбой питания или неисправность порта)

Порты Ethernet 10/100/1000Base-T(X)			
Link/ACT	Зеленый	Горит	Порт подключен
		Не горит	Порт не подключен
		Мигает	Идет передача данных
Speed	Зеленый	Горит	Порт работает на скорости 1000 Мбит/с
	Желтый	Горит	Порт работает на скорости 100 Мбит/с
	Выключен	Не горит	Порт работает на скорости 10 Мбит/с
SFP			
LNK/ACT	Зеленый	Горит	Порт подключен
		Мигает	Идет передача данных

2.2 Верхняя панель

Ниже приведены компоненты верхней панели SWMGR-812GSFP:

1. Клеммная колодка: PWR1, PWR2 (12-48 В постоянного тока), релейный выход.

2. Шина заземления. Для получения дополнительной информации о том, как заземлить коммутатор, см. раздел 3.3.1 «Заземление».

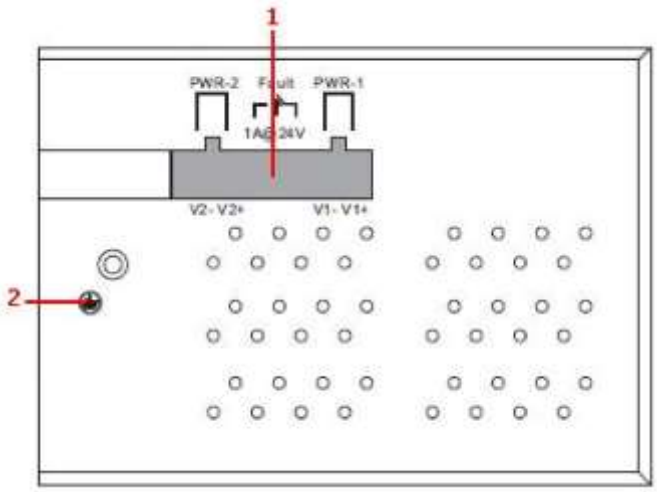
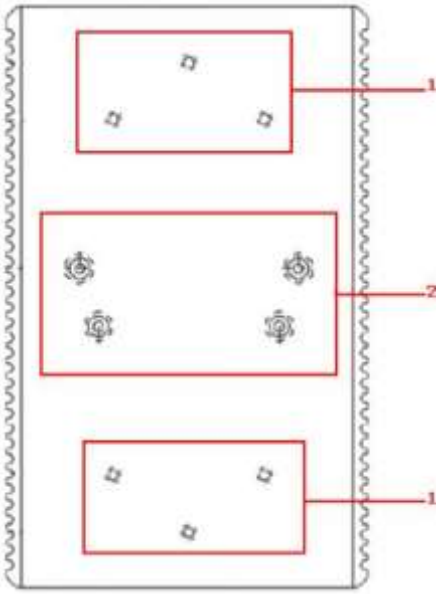


Рисунок 2 – Верхняя панель

2.3 Задняя панель

На задней панели коммутатора находятся три набора отверстий для винтов. Два набора, расположенные по форме треугольника на обоих концах задней панели, используются для настенного монтажа, а набор из четырех отверстий в середине используется для установки на Din-рейку. Для получения дополнительной информации об установке см. раздел 3.1 «Установка на Din-рейку».



1. Отверстия для крепления на стену
2. Отверстия для крепления на DIN-рейку

Рисунок 3 – Задняя панель

3. Монтаж оборудования

3.1 Установка на DIN-рейку

Каждый коммутатор поставляется с установочным комплектом для DIN-рейки, позволяющим закрепить на ней коммутатор.

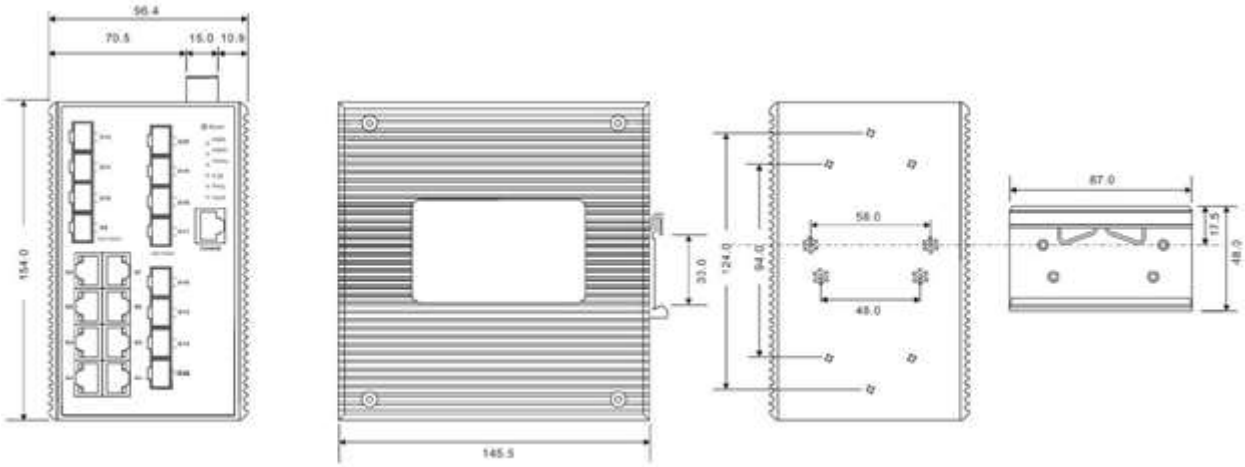


Рисунок 4 – Размеры установочного комплекта DIN-рейки (единица измерения – мм)

Для установки коммутатора на DIN-рейку сначала прикрутите монтажную площадку к задней части коммутатора, прямо посередине задней панели. Затем вставьте коммутатор в направляющие DIN-рейки и убедитесь, что коммутатор надежно защелкнулся на ней.

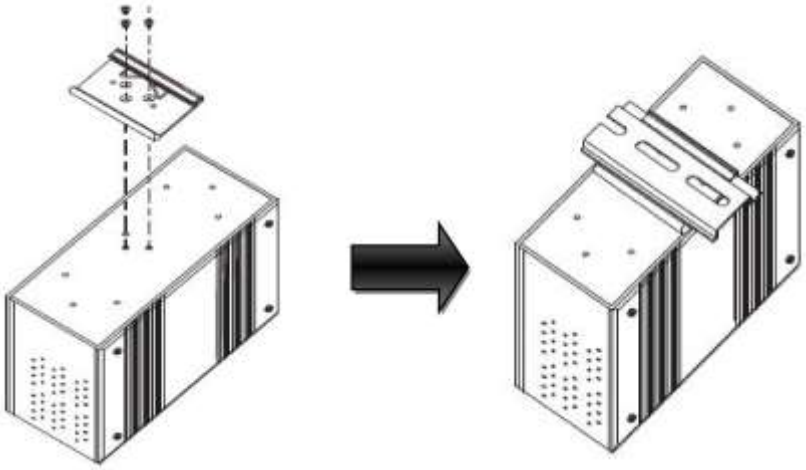


Рисунок 5 – Установка на DIN-рейку

3.2 Настенный монтаж

Помимо DIN-рейки, коммутатор можно закрепить на стене с помощью комплекта для настенного монтажа.

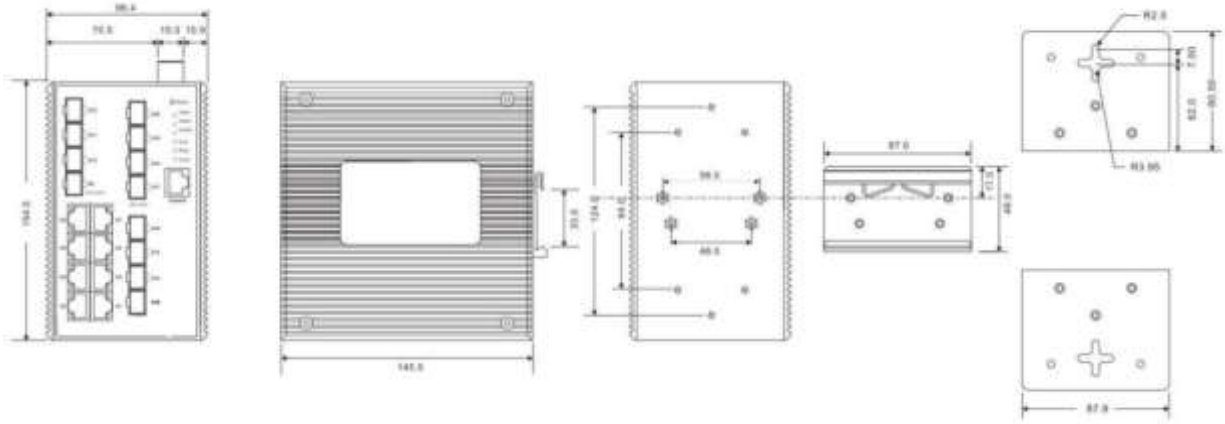


Рисунок 6 – Размеры комплекта для настенного монтажа (единица измерения – мм)

Чтобы закрепить коммутатор на стене, выполните следующие действия:

1. Прикрутите две части комплекта для настенного монтажа к обоим концам задней панели коммутатора. Всего потребуется шесть винтов, как показано ниже.

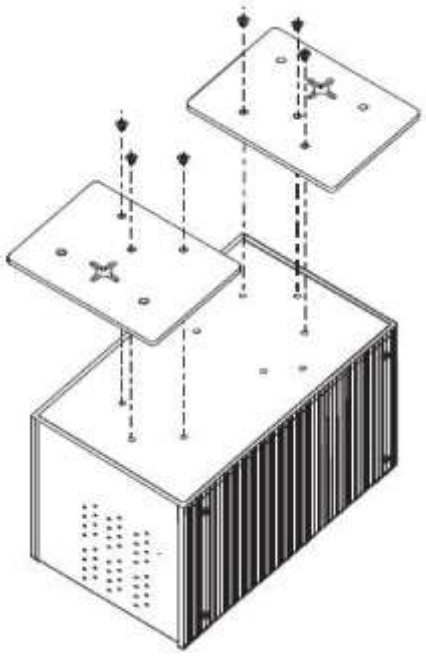


Рисунок 7 – Установка комплекта для настенного монтажа

2. Используйте коммутатор с прикрепленными монтажными пластинами в качестве ориентира, чтобы отметить правильное расположение четырех винтов на стене.

3. Сначала вкрутите четыре винта в стену так, чтобы между стеной и шляпкой винта оставалось немного пространства. Это нужно для того, чтобы шляпки винтов могли свободно входить в большие части отверстий в форме замочной скважины на корпусе коммутатора.

4. Поднимите коммутатор и совместите большие части отверстий на его задней панели с головками винтов.

5. Аккуратно сдвиньте коммутатор вниз, чтобы шляпки винтов переместились в узкую часть отверстий в форме замочной скважины. Это обеспечит первичную фиксацию коммутатора на стене.

6. После того как коммутатор окажется на своем месте, окончательно затяните все четыре винта, чтобы зафиксировать устройство на стене и придать ему дополнительную устойчивость.

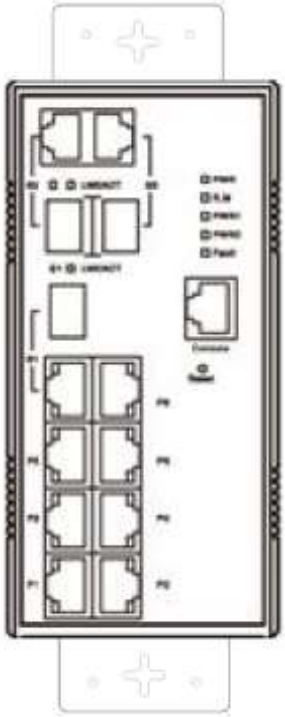


Рисунок 8 – Коммутатор с монтажными пластинами

3.3 Электропроводка

Не отсоединяйте модули и провода, если питание не отключено или зона не является безопасной. Устройства можно подключать только к напряжению питания, указанному на заводской табличке.

- Обязательно отсоедините шнур питания перед установкой и/или подключением коммутаторов.
- Рассчитайте максимально возможный ток в каждом проводе питания и общем проводе. Соблюдайте все электротехнические правила, определяющие максимально допустимый ток для каждого размера провода.
- Если ток превышает максимальные значения, проводка может перегреться, что приведет к серьезному повреждению вашего оборудования.
- Прокладывайте провода питания и провода устройств по отдельным маршрутам, чтобы они не пересекались и не шли рядом. Если они вынуждены пересекаться, убедитесь, что провода перпендикулярны в точке пересечения.
- Не прокладывайте сигнальные или коммуникационные провода и провода питания через один и тот же кабельный канал. Чтобы избежать помех, провода с разными характеристиками сигнала следует прокладывать отдельно.
- Вы можете использовать информацию о типе сигнала, передаваемого по проводу, чтобы определить, какие провода следует прокладывать отдельно.

Эмпирическое правило заключается в том, что провода с похожими электрическими характеристиками можно объединять вместе.

- Следует отделять друг от друга входную и выходную проводку.
- Рекомендуется маркировать провода, идущие ко всем устройствам в системе.

3.3.1 Заземление

Заземление и правильная прокладка проводов помогают ограничить влияние шума, вызванного электромагнитными помехами (ЭМП). Перед подключением устройств проложите заземляющее соединение от винта заземления к заземляющей поверхности.

3.3.2 Реле неисправности

Два контакта 6-контактного разъема клеммной колодки относятся к реле, используемому для оповещения о событиях, настроенных пользователем. Два провода, подключенные к этим контактам, образуют разомкнутую цепь в момент срабатывания настроенного пользователем события. Если настроенное пользователем событие не происходит, цепь сигнализации неисправности остается замкнутой.

3.3.3 Резервируемые входы питания

Коммутатор имеет две контактные группы для подключения питания, PWR1 и PWR2. Два верхних и два нижних контакта 6-контактного разъема клеммной колодки на верхней панели коммутатора используются для подачи цифрового питания, как показано на рисунке 9. Чтобы подключить резервируемые входы питания выполните следующие действия:

1. Вставьте отрицательный/положительный провода постоянного тока в клеммы V-/V+ соответственно.

2. Во избежание самопроизвольного отсоединения проводов постоянного тока затяните винты зажима проводов на передней части разъема клеммной колодки при помощи небольшой плоской отвертки.

3. Вставьте пластиковые штыри разъема в гнездо клеммной колодки на верхней панели коммутатора.

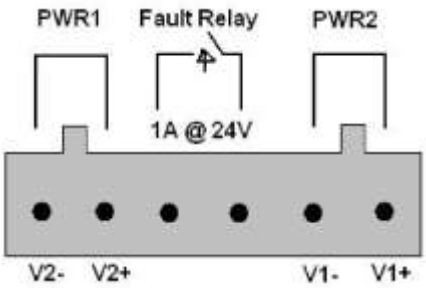


Рисунок 9 – 6-контактный разъем клеммной колодки

3.4 Подключение

3.4.1 Кабели

➢ Назначение контактов 10/100/1000BASE-T(X)

Устройство имеет стандартные порты Ethernet. В зависимости от типа соединения коммутатор использует кабели CAT 3, 4, 5,5e UTP для подключения к любым другим сетевым устройствам (ПК, серверам, коммутаторам, маршрутизаторам или концентраторам). Технические характеристики кабелей см. в следующей таблице.

Таблица 2 – Типы и характеристики кабелей

Кабель	Тип	Макс. длина	Коннектор
10BASE-T	Cat. 3, 4, 5; 100 Ом	UTP 100 м	RJ-45
100BASE-TX	Cat. 5; 100 Ом UTP	UTP 100 м	RJ-45
1000BASE-TX	Cat. 5/Cat. 5e; 100 Ом UTP	UTP 100 м	RJ-45

В кабелях 10/100/1000Base-T(X) контакты 1 и 2 используются для передачи данных, а контакты 3 и 6 – для приема.

Таблица 3 – Назначение контактов 10/100Base-T(X) RJ-45

Номер контакта	Назначение
1	TD+
2	TD-
3	RD+
4	Не используется
5	Не используется
6	RD-
7	Не используется
8	Не используется

Таблица 4 – Назначение контактов 1000Base-T(X) RJ-45

Номер контакта	Назначение
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD

- Режим MDI/MDI-X

Устройство также поддерживает работу в автоматическом режиме MDI/MDI-X. Вы можете использовать кабель для подключения коммутатора к ПК. В таблицах ниже показаны выводы портов MDI и MDI-X.

Таблица 5 – Назначение контактов 10/100Base-T(X) MDI/MDI-X

Номер контакта	Порт MDI	Порт MDI-X
1	TD+(передача)	RD+(прием)
2	TD-(передача)	RD-(прием)
3	RD+(прием)	TD+(передача)
4	Не используется	Не используется
5	Не используется	Не используется
6	RD-(прием)	TD-(передача)
7	Не используется	Не используется
8	Не используется	Не используется

Назначение контактов 1000Base-T(X) MDI/MDI-X

Номер контакта	Порт MDI	Порт MDI-X

1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC

Знаки «+» и «-» обозначают полярность проводов, составляющих каждую витую пару.

3.4.2 Подключение консольного порта RS-232

Коммутатор может управляться через консольный порт с помощью кабеля RS-232 из комплекта поставки. Вы можете подключить порт к ПК через кабель RS-232 с гнездовым разъемом DB-9. Разъем DB-9 (female) кабеля RS-232 должен быть подключен к ПК, а другой конец кабеля (разъем RJ-45) подключается к консольному порту коммутатора.

Таблица 6 – Назначение контактов RS-232

Назначение выводов ПК (штекер)	RS-232 с гнездовым разъемом DB9	DB9 к RJ 45
Контакт № 2 RD	Контакт № 2 TD	Контакт № 2
Контакт № 3 TD	Контакт № 3 RD	Контакт № 3
Контакт № 5 GD	Контакт № 5 GD	Контакт № 5

На рисунке 10 показано назначение всех контактов интерфейса RS232 и направление передачи сигнала. Только 3 контакта из 9 имеют строго определенное назначение: передача, прием и земля.

DCD (Carrier Detect) – наличие несущей

RxD (Received Data) – принимаемые данные

TxD (Transmitted Data) – передаваемые данные

DTR (Data Terminal Ready) – готовность терминала ООД

GND (Signal Ground) – «земля» сигналов (общий)

DSR (Data Set Ready) – готовность устройства АПД

RTS (Request to Send) – запрос на передачу

CTS (Clear to Send) – готовность передачи

RI (Ring Indicator) – сигнал вызова

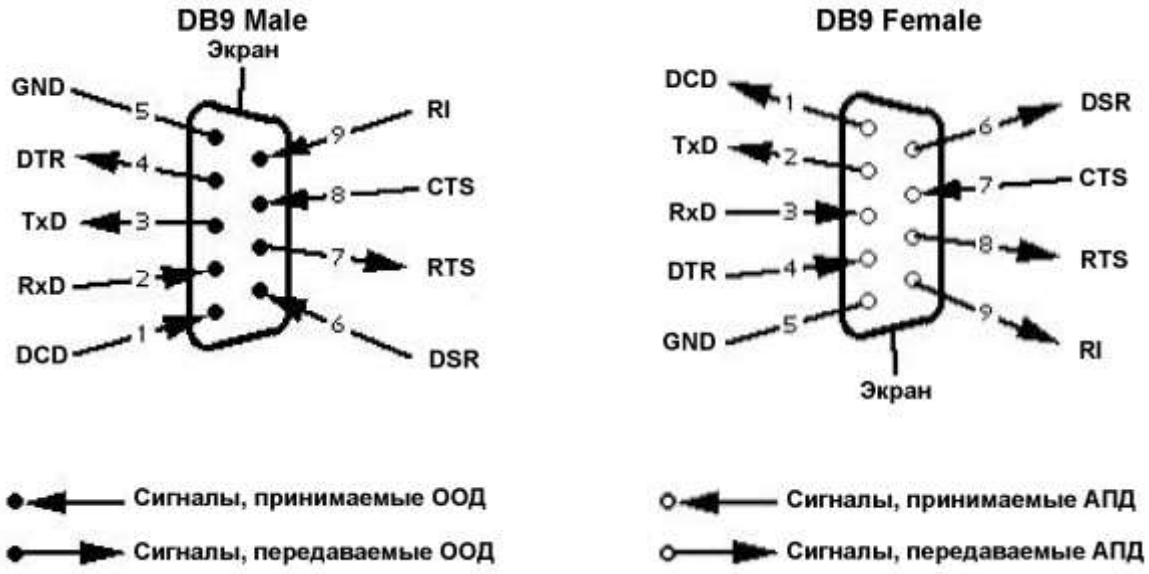


Рисунок 10 – Порядок расположения выводов интерфейса RS232

3.4.3 SFP

Коммутатор оснащен оптическими портами, которые используют разъемы SFP. Оптоволоконные трансиверы бывают многомодовыми (от 0 до 550 м, 850 Нм с волокном 50/125 мкм, 62,5/125 мкм) и одномодовыми с разъемами LC. Обратите внимание, что порт TX коммутатора A должен быть подключен к порту RX коммутатора B.

Рисунок 11 – SFP-модули и оптоволоконный кабель

3.4.4 Sy-Ring/Sy-Union

➢ Sy-Ring

Чтобы сформировать кольцевую топологию и получить возможности резервирования сети, вы можете подключить три коммутатора или более, выполнив следующие действия:

1. Подключите каждый коммутатор, чтобы сформировать последовательную цепь, с помощью кабеля Ethernet.

2. Настройте один из подключенных коммутаторов в качестве главного (мастера) и убедитесь, что настройка портов каждого подключенного коммутатора на странице управления соответствует подключенным физическим портам. Информацию о настройке портов см. в разделе 4.1.2 «Конфигурации».

3. Подключите последний коммутатор к первому, чтобы сформировать кольцевую топологию.

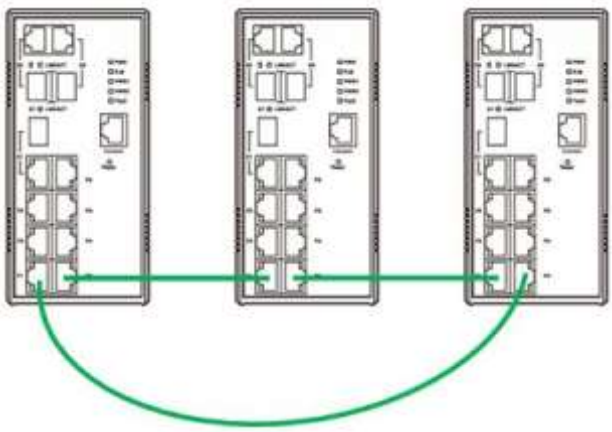


Рисунок 12 – Топология Sy-Ring

➢ Объединенное кольцо

Если у вас уже есть две топологии Sy-Ring, и вы хотите соединить кольца, можно сформировать из них одно объединенное кольцо. Все, что нужно сделать, это выбрать два коммутатора из каждого кольца для соединения, например, коммутаторы A и B из кольца

1 и коммутаторы C и D из кольца 2. Решите, какой порт на каждом коммутаторе будет использоваться в качестве объединяющего порта, а затем соедините их, например, порт 1 коммутатора A с портом 2 коммутатора C и порт 1 коммутатора B с портом 2 коммутатора D. Перейдите на страницу управления и включите опцию «Coupling Ring», установив галочку в соответствующем поле. Затем выберите соединенные порты, чтобы указать, что они теперь являются частью объединенного кольца. Для получения дополнительной информации о настройке портов см. раздел 4.1.2 «Конфигурации». После завершения настройки одно из соединений будет действовать как основной путь, а другое – как резервный.

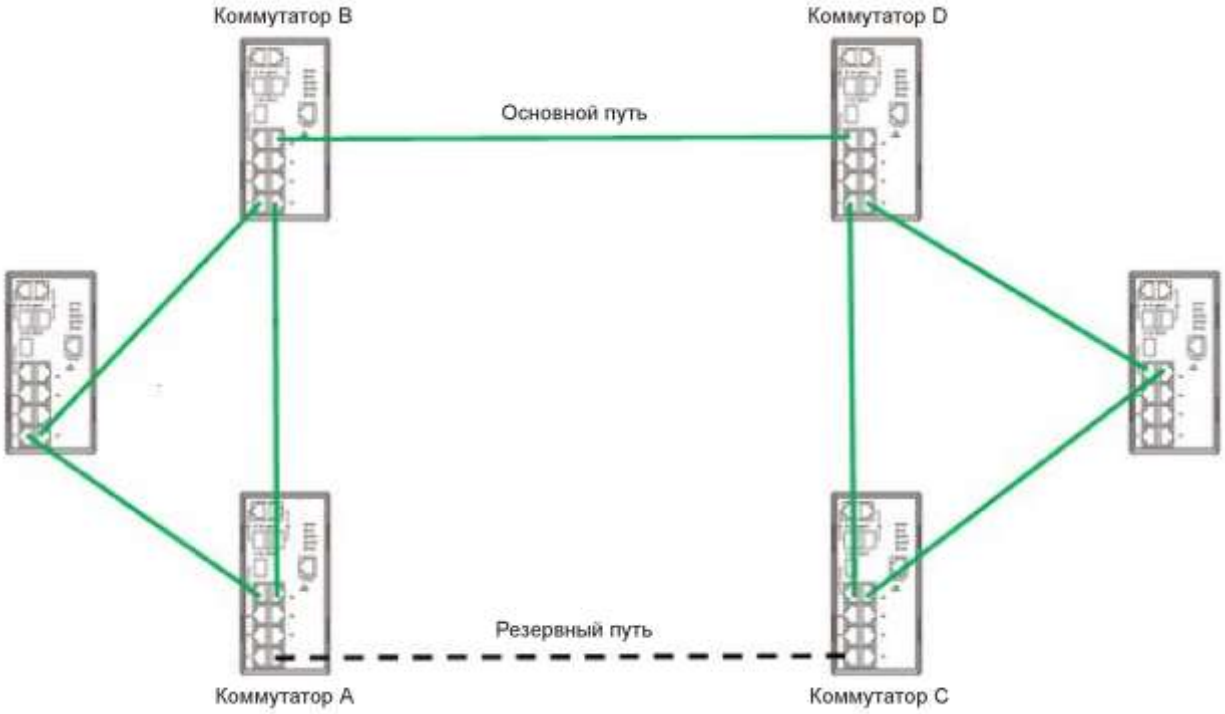


Рисунок 13 – Топология объединенного кольца

- Двойное подключение

Если необходимо подключить кольцевую топологию к сетевой среде RSTP, вы можете использовать двойное подключение Dual Homing. Выберите два коммутатора (коммутаторы A и B) из кольца для подключения к коммутаторам в сети RSTP (основные коммутаторы). Путь одного из коммутаторов (коммутатор A или B) будет действовать как основной, а путь другого коммутатора – как резервный, который активируется при сбое подключения по основному пути.

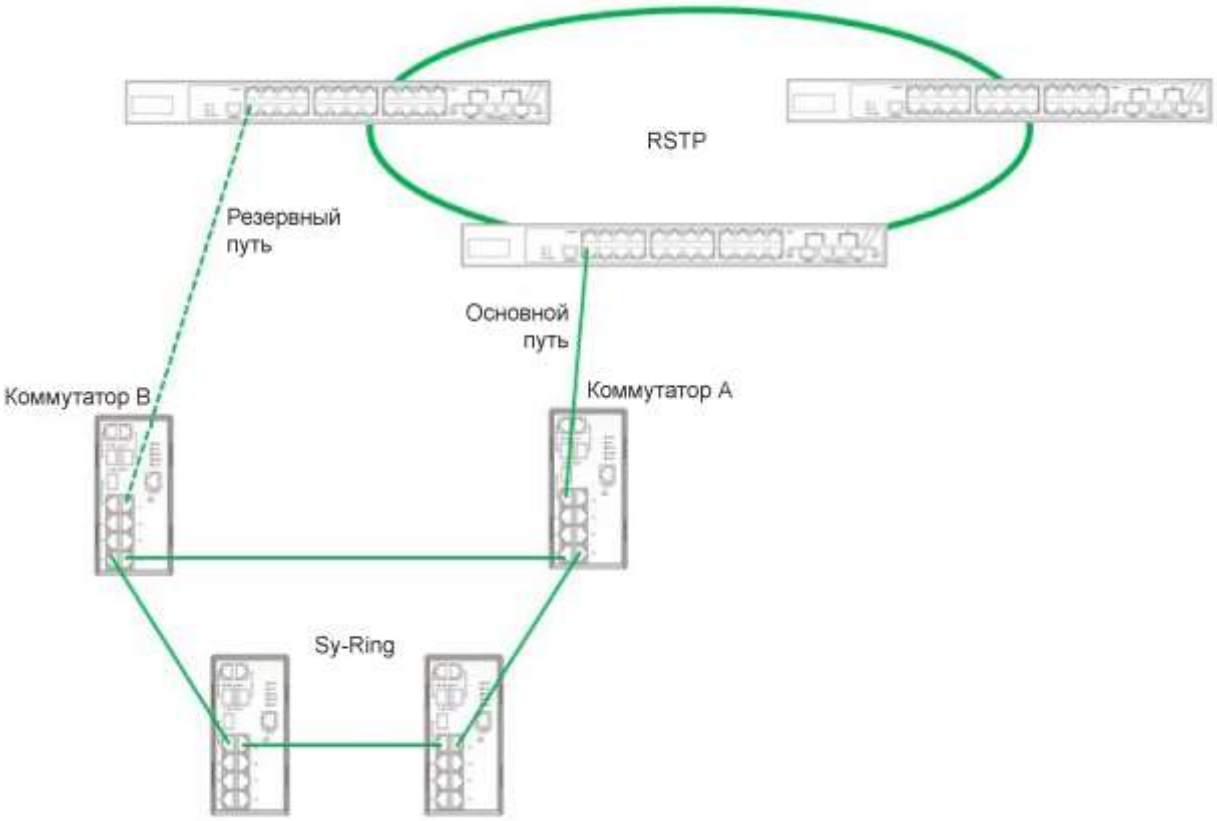


Рисунок 14 – Топология Dual Homing

- Sy-Union

В случае, если при имеющихся кольцах Sy-Ring необходимо расширение, вы можете создать топологию Sy-Union, выполнив следующие действия:

1. Выберите два коммутатора из цепочки (коммутаторы A и B), которые вы хотите подключить к Sy-Ring, и подключите их к коммутаторам в кольце (коммутаторы C и D).

2. Перейдите на страницу управления и настройте граничный порт для обоих выбранных коммутаторов из цепочки в соответствии с портом, подключенным к кольцу, установив галочку в соответствующем поле (см. раздел 4.2.2 «Настройка»).

3. После завершения настройки одно из подключений будет действовать как основной путь, а другое – как резервный.

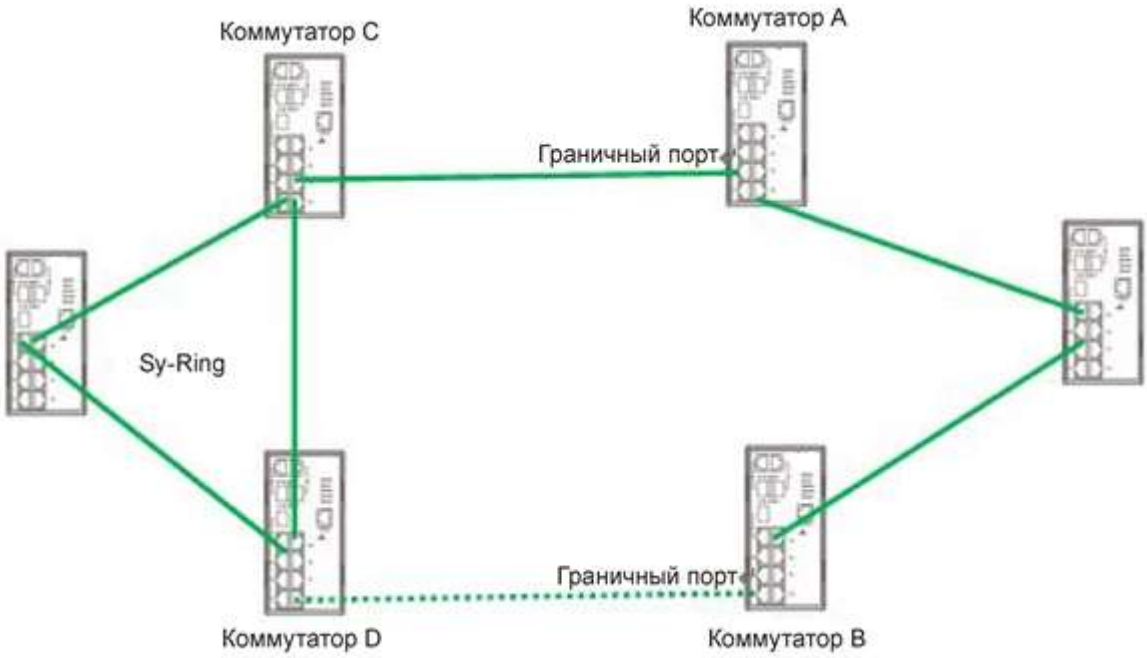


Рисунок 15 – Топология Sy-Union

4. Резервирование

Резервирование с целью минимизации времени простоя системы является одной из наиболее важных проблем для промышленных сетевых устройств. Поэтому компания Symanitron разработала собственные технологии резервирования, включая Sy-Ring и All-Ring, обеспечивающие более быстрое время восстановления, чем существующие технологии, широко используемые в коммерческих приложениях, такие как STP, RSTP и MSTP. Технологии резервирования Symanitron не только поддерживают различные сетевые топологии, но также обеспечивают надежность сети.

4.1 Sy-Ring

4.1.1 Введение

Sy-Ring – это фирменная технология кольцевого резервирования со временем восстановления менее 30 миллисекунд, допускающая включение 250 узлов гигабитных серий. Кольцевые протоколы идентифицируют один коммутатор как главный в сети, а затем автоматически блокируют прохождение пакетов через любые избыточные пути. В случае, если одна ветвь кольца отключается от остальной части сети, протокол автоматически перенастраивает кольцо так, чтобы данные перенаправлялись по резервному пути, а часть сети, которая была отключена, могла восстановить связь с остальной сетью. Технология кольцевого резервирования Sy-Ring может защитить критически важные приложения от сетевых сбоев или временных неисправностей благодаря своим возможностям быстрого восстановления.

Рисунок 16 – Технология кольцевого резервирования

4.1.2 Конфигурации

Sy-Ring поддерживает две кольцевые топологии: объединенное кольцо (Coupling Ring) и двойное подключение (Dual Homing). При помощи интерфейса управления можно настроить нужные параметры, как показано на рисунке 17.

Рисунок 17 – Окно настройки Sy-Ring

Параметр	Описание
Sy-Ring	Установите флажок, чтобы включить топологию Sy-Ring
Ring Master	В кольце допускается только один главный узел (мастер). Однако, если данная функция включена на нескольких коммутаторах, коммутатор с наименьшим MAC-адресом станет активным мастером кольца, а остальные будут выполнять роль резервных мастеров

1st Ring Port	Основной порт, когда коммутатор является мастером кольца
2nd Ring Port	Резервный порт, когда коммутатор является мастером кольца
Coupling Ring	Установите флажок, чтобы разрешить объединенное кольцо. Функция «Coupling Ring» может разделить большое кольцо на два меньших, чтобы избежать изменений топологии сети, влияющих на все коммутаторы. Также это хороший метод для объединения двух колец
Coupling Port	Порты для соединения нескольких колец. Для создания активного и резервного канала связи кольцу требуется четыре коммутатора. Каналы связи, образованные данными портами, будут работать в активном/резервном режиме
Dual Homing	Установите флажок, чтобы включить Dual Homing. Когда функция включена, кольцо будет подключено к обычным коммутаторам через два канала RSTP (например, магистральный коммутатор). Два канала работают в активном/резервном режиме и подключают каждое кольцо к обычным коммутаторам в режиме RSTP
Apply	Нажмите, чтобы применить настройки

Чтобы избежать чрезмерной нагрузки, не рекомендуется одновременно включать на одном коммутаторе функции «Ring Master» и «Coupling Ring».

4.2 Sy-Union

4.2.1 Введение

Sy-Union – это технология резервирования сети Symanitron, которая повышает надежность любых магистральных сетей, обеспечивая простоту использования и максимальную скорость восстановления после сбоев, а также гибкость, совместимость и экономическую эффективность при взаимодействии различных резервируемых топологий. Технология самовосстановления Ethernet, разработанная для распределенных и сложных промышленных сетей, позволяет сети масштаба до 250 коммутаторов восстанавливаться менее чем за 10 мс, если в какой-либо момент сегмент цепи выходит из строя.

Sy-Union позволяет нескольким резервным кольцам на основе различных протоколов резервирования объединяться и функционировать вместе как большая и надежная сетевая топология. Sy-Union может создавать несколько резервных сетей без учета ограничений текущих технологий кольцевого резервирования.

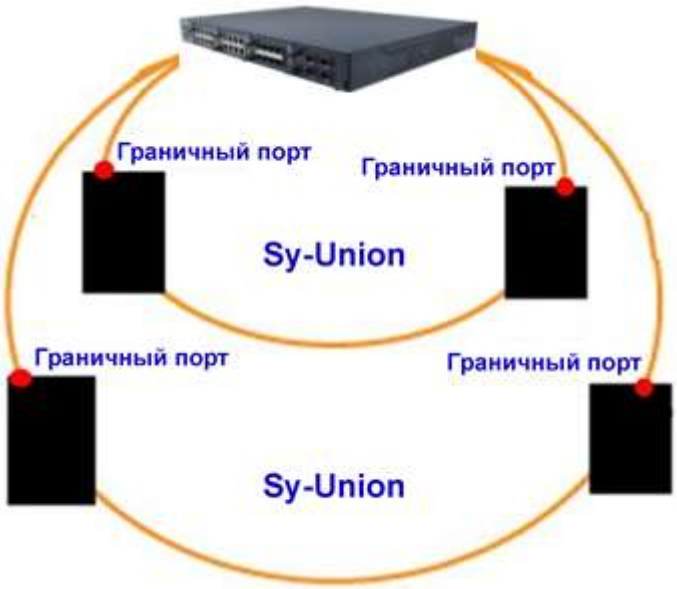


Рисунок 18 – Sy-Union

4.2.2 Настройка

Sy-Union очень прост в настройке и управлении. Необходимо определить только один граничный порт граничного коммутатора. Для других коммутаторов достаточно включить функцию Sy-Union.

Рисунок 19 – Окно настройки Sy-Union

Параметр	Описание
Enable	Установите флажок, чтобы включить функцию Sy-Union
1st	Первый порт, подключающийся к кольцу
2nd	Второй порт, подключающийся к кольцу

Edge Port	Для топологии Sy-Union сначала необходимо указать граничные порты. Порты с меньшим MAC-адресом коммутатора будут служить резервным каналом; загорится светодиод R.M
Apply	Нажмите, чтобы применить настройки

4.3 MRP

4.3.1 Введение

MRP (Media Redundancy Protocol) – промышленный стандарт для сетей Ethernet высокой доступности. MRP позволяет коммутаторам Ethernet в кольцевой конфигурации быстро восстанавливаться после сбоя, обеспечивая бесперебойную передачу данных. Кольцо MRP (IEC 62439) может поддерживать до 50 устройств и обеспечивает резервное соединение за 80 мс (регулируется до макс. 200 мс/500 мс).

4.3.2 Настройка

Рисунок 20 – Окно настройки MRP

Параметр	Описание
Enable	Установите флажок, чтобы включить функцию MRP
Manager	Каждой топологии MRP нужен главный узел, так называемый менеджер MRP. Одна топология MRP может иметь только один такой узел. Если два или более коммутаторов настроены на роль менеджера, топология MRP выйдет из строя
React on Link Change (расширенный режим)	Более быстрый режим. Включение этой функции приведет к ускорению схождения топологии MRP. Эту функцию можно настроить только на коммутаторе, выполняющем роль менеджера

1st Ring Port	Первый порт, подключающийся к кольцу MRP
2nd Ring Port	Второй порт, подключающийся к кольцу MRP
Apply	Нажмите, чтобы применить настройки

4.4 STP/RSTP/MSTP

4.4.1 STP/RSTP

Протокол связующего дерева STP (Spanning Tree Protocol), а также его усовершенствованные версии RSTP (Rapid Spanning Tree Protocol) и MSTP (Multiple Spanning Tree Protocol) предназначены для предотвращения сетевых петель и обеспечения резервирования сети. В больших сетях часто возникают сетевые петли, поскольку, когда несколько путей ведут к одному и тому же месту назначения, широковещательные пакеты могут попасть в бесконечный цикл и таким образом спровоцировать перегрузку. STP может определить лучший путь к месту назначения и заблокировать все остальные пути. Заблокированные каналы связи останутся подключенными, но неактивными. Когда лучший путь выходит из строя, заблокированные каналы связи активируются. По сравнению с STP, который восстанавливает канал за 30–50 секунд, RSTP может сократить время до 5–6 секунд.

➢ **Состояние мостов STP**

На этой странице отображается состояние всех экземпляров моста STP.

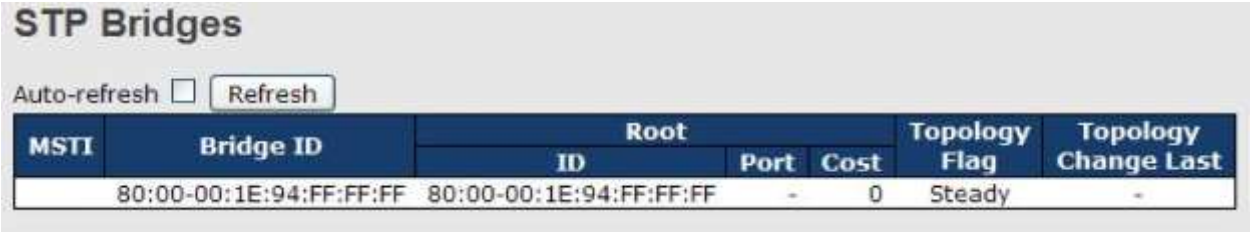


Рисунок 21 – Мосты STP

Параметр	Описание
MSTI	Экземпляр моста. Вы также можете перейти к подробному описанию состояния моста STP
Bridge ID	Идентификатор моста данного экземпляра
Root ID	Идентификатор выбранного в настоящий момент корневого моста

Root Port	Порт коммутатора, которому в данный момент назначена роль корневого порта
Root Cost	Стоимость корневого пути. Для корневого моста это ноль. Для других мостов это сумма стоимостей портов на наименее затратном пути к корневому мосту
Topology Flag	Текущее состояние флага изменения топологии для экземпляра моста
Topology Change Last	Время с момента последнего изменения топологии
Refresh	Нажмите, чтобы немедленно обновить страницу
Auto-refresh	Установите этот флажок, чтобы включить автоматическое обновление страницы через регулярные промежутки времени

- **Состояние портов STP**

На этой странице отображается состояние STP-портов выбранного коммутатора.

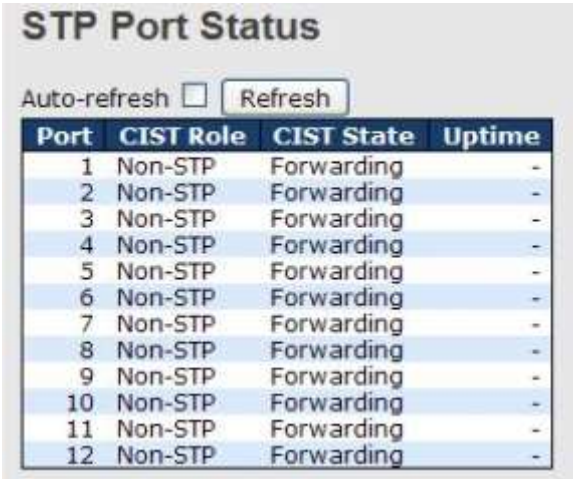


Рисунок 22 – Состояние портов STP

Параметр	Описание
Port	Номер порта коммутатора, к которому будут применены следующие настройки
CIST Role	Роль STP-порта в CIST. Включает следующие значения: **AlternatePort** – альтернативный порт;

	BackupPort – резервный порт; **RootPort** – корневой порт; **DesignatedPort** – назначенный порт
State	Текущее состояние STP-порта в CIST. Включает следующие значения: **Blocking** – блокировка; **Learning** – обучение; **Forwarding** – пересылка
Uptime	Время с момента последней инициализации порта моста
Refresh	Нажмите, чтобы немедленно обновить страницу
Auto-refresh	Установите этот флажок, чтобы включить автоматическое обновление страницы через регулярные промежутки времени

- **Статистика STP**

На этой странице отображается статистика порта STP выбранного коммутатора.

Рисунок 23 – Статистика STP

Параметр	Описание
Port	Номер порта коммутатора, к которому будут применены следующие настройки
MSTP	Количество BPDU с конфигурацией MSTP, полученных/переданных на порту
RSTP	Количество BPDU с конфигурацией RSTP, полученных/переданных на порту
STP	Количество BPDU с конфигурацией STP, полученных/переданных на порту

TCN	Количество BPDU-уведомлений об изменении топологии, полученных/переданных на порту
Discarded Unknown	Количество неизвестных BPDU связующего дерева, полученных (и отклоненных) на порту
Discarded Illegal	Количество незаконных BPDU связующего дерева, полученных (и отклоненных) на порту
Refresh	Нажмите, чтобы немедленно обновить страницу
Auto-refresh	Установите этот флажок, чтобы включить автоматическое обновление страницы через регулярные промежутки времени
Clear	Нажмите, чтобы очистить статистику

- **Настройка моста STP**

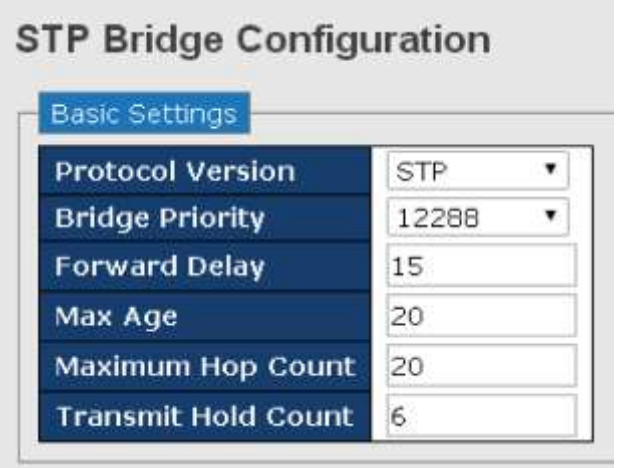


Рисунок 24 – Настройка моста STP

Параметр	Описание
Protocol Version	Версия протокола STP. Допустимые значения включают STP, RSTP и MSTP
Bridge Priority	Каждому коммутатору, участвующему в сети STP, назначается числовое значение, называемое значением приоритета моста. Значение приоритета моста определяет, какой коммутатор может стать корневым мостом. Вы можете уменьшить значение, чтобы повысить вероятность выбора коммутатора в качестве корневого
Forward Delay	Параметр, определяющий задержку, которую используют мосты STP для перехода корневых и назначенных портов в состояние передачи

	данных, когда они работают в режиме совместимости с STP. Диапазон допустимых значений – от 4 до 30 секунд
Max Age	Максимальное время, в течение которого информация, переданная корневым мостом, считается действительной. Диапазон допустимых значений составляет от 6 до 40 секунд, а Max Age должен быть <= (FwdDelay-1)*2
Maximum Hop Count	Это определяет начальное значение оставшихся переходов для BPDU-информации MSTI, сгенерированной на границе региона MSTI. Это определяет, на сколько мостов корневой мост может распространять свою информацию BPDU. Диапазон допустимых значений составляет от 1 до 40. BPDU со значением «Maximum Hop Count» равным нулю будет отброшено
Transmit Hold Count	Количество BPDU, которые порт моста может отправить за одну секунду. При превышении этого значения передача следующего BPDU будет отложена. Диапазон допустимых значений – от 1 до 10 BPDU в секунду
Save	Нажмите, чтобы сохранить изменения
Reset	Нажмите, чтобы отменить любые изменения, внесенные локально, и вернуться к ранее сохраненным значениям

Рисунок 25 – Расширенные настройки

Параметр	Описание
Edge Port BPDU Filtering	Указывает, будет ли порт, явно настроенный в качестве граничного, передавать и получать BPDU
Edge Port BPDU Guard	Указывает, будет ли порт, явно настроенный в качестве граничного, отключаться при получении BPDU. Отключенные порты переходят в состояние «error-disabled» и удаляются из активной топологии

Port Error Recovery	Указывает, будет ли порт в состоянии «error-disabled» автоматически включен по истечении времени восстановления после ошибки. Если функция отключена, порты необходимо сначала отключить вручную, а затем включить повторно для нормальной работы STP. Состояние «error-disabled» также очищается перезагрузкой системы
Port Error Recovery Timeout	Настройка времени, которое должно пройти, прежде чем порт в состоянии «error-disabled» будет автоматически включен снова. Допустимые значения находятся в диапазоне от 30 до 86400 секунд (24 часа)

4.4.2 MSTP

Поскольку время восстановления STP и RSTP занимает секунды, что неприемлемо в некоторых промышленных приложениях, был разработан протокол MSTP. Технология поддерживает несколько связующих деревьев в сети путем группировки и сопоставления нескольких VLAN в различные экземпляры связующего дерева, известные как MSTI, для формирования отдельных регионов MST. Каждый коммутатор назначается региону MST. Таким образом, каждый регион MST состоит из одного или нескольких коммутаторов MSTP с одинаковыми VLAN, по крайней мере одним экземпляром MST и одинаковым именем региона MST. Поэтому коммутаторы могут использовать разные пути в сети для эффективной балансировки нагрузки.

- **Настройка портов**

Эта страница позволяет вам проверять и изменять конфигурации текущих портов MSTI. Порт MSTI – это виртуальный порт, который создается отдельно для каждого активного порта CIST (физического) каждого экземпляра MSTI, настроенного и применимого для порта. Экземпляр MSTI должен быть выбран до отображения параметров конфигурации порта MSTI.

Эта страница содержит настройки порта MSTI для физических и агрегированных портов. Настройки агрегации являются глобальными для стека.

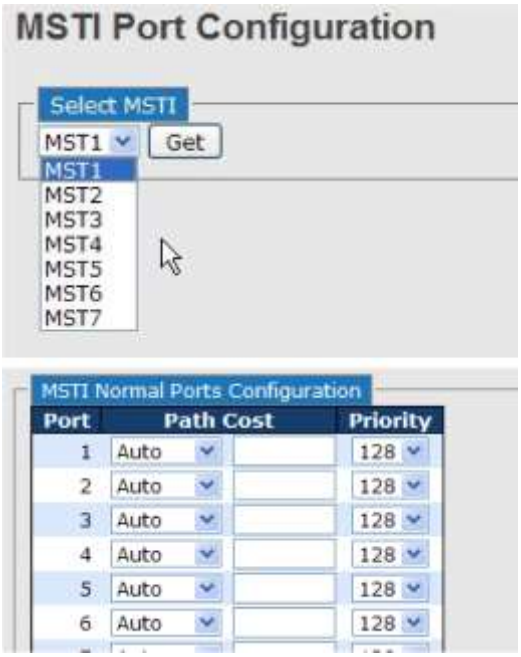


Рисунок 26 – Настройка портов MSTI

Параметр	Описание
Port	Номер порта коммутатора, соответствующего порту CIST STP и MSTI
Path Cost	Настраивает стоимость пути, ассоциируемую с портом. Режим «Auto» устанавливает стоимость пути в соответствии со скоростью физического соединения с использованием значений, рекомендуемых стандартом 802.1D. Чем выше пропускная способность интерфейса, тем ниже стоимость. Ручной режим позволяет ввести значение, определяемое пользователем. Стоимость пути учитывается при становлении активной топологии сети. Порты с более низкой стоимостью выбираются в качестве портов пересылки вместо портов с более высокой стоимостью. Диапазон допустимых значений – от 1 до 200000000
Priority	Настраивает приоритет для портов с одинаковой стоимостью пути (см. выше)
Save	Нажмите, чтобы сохранить изменения
Reset	Нажмите, чтобы отменить любые изменения, внесенные локально, и вернуться к ранее сохраненным значениям

- **Сопоставление**

Эта страница позволяет проверять и изменять конфигурацию текущего экземпляра STP-моста MSTI.

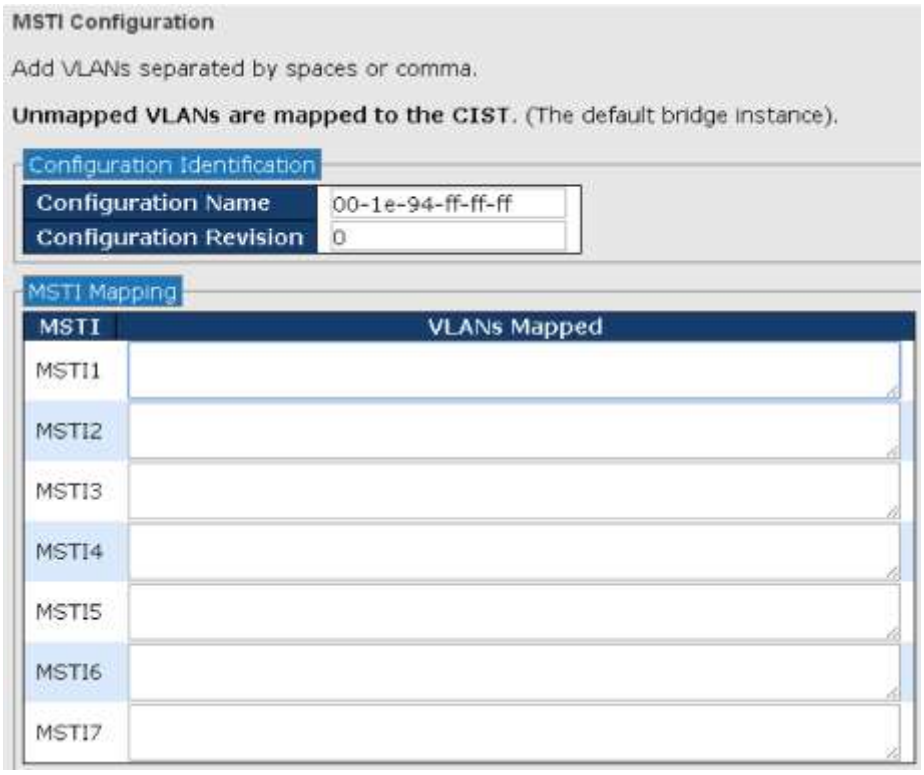


Рисунок 27 – Сопоставление VLAN с MSTI

Параметр	Описание
Configuration Name	Имя, которое идентифицирует сопоставление VLAN с MSTI. Мосты должны иметь общее имя и ревизию (см. ниже), а также конфигурации сопоставления VLAN-MSTI для совместного использования связующих деревьев для MSTI (внутри региона). Имя не должно превышать 32 символа
Configuration Revision	Ревизия конфигурации MSTI, указанной выше. Это должно быть целое число от 0 до 65535
MSTI	Экземпляр моста. CIST недоступен для явного сопоставления, так как он будет получать все VLAN, которые не были явно сопоставлены
VLANs Mapped	Список VLAN, сопоставленных с MSTI. VLAN должны быть разделены запятыми и/или пробелами. VLAN может быть сопоставлена только с одним MSTI. Поле неиспользуемого MSTI останется пустым, без сопоставленных VLAN
Save	Нажмите, чтобы сохранить изменения
Reset	Нажмите, чтобы отменить любые изменения, внесенные локально, и вернуться к ранее сохраненным значениям

➢ **Приоритет**

Эта страница позволяет проверять и изменять настройки приоритета текущего экземпляра STP-моста MSTI.

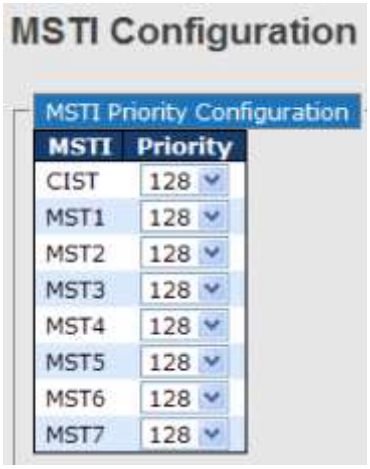


Рисунок 28 – Настройка приоритета

Параметр	Описание
MSTI	Экземпляр моста. CIST – это экземпляр по умолчанию, который всегда активен
Priority	Указывает приоритет моста. Чем ниже значение, тем выше приоритет. Приоритет моста, номер экземпляра MSTI и 6-байтовый MAC-адрес коммутатора формируют идентификатор моста
Save	Нажмите, чтобы сохранить изменения
Reset	Нажмите, чтобы отменить любые изменения, внесенные локально, и вернуться к ранее сохраненным значениям

4.4.3 CIST

Благодаря возможности пересекать региональные границы, CIST используется MSTP для связи с другими регионами и с любыми односоставными связующими деревьями RSTP и STP в сети. Любой граничный порт, то есть, подключенный к другому региону, будет автоматически принадлежать исключительно CIST, даже если он назначен MSTI. Все VLAN, которые не являются членами определенных MSTI, являются членами CIST.

➢ **Настройка портов**

Рисунок 29 – Настройка портов CIST

Параметр	Описание
Port	Номер порта коммутатора, к которому будут применены следующие настройки
STP Enabled	Установите флажок, чтобы включить STP для порта
Path Cost	Настраивает стоимость пути, ассоциируемую с портом. Режим «Auto» устанавливает стоимость пути в соответствии со скоростью физического соединения с использованием значений, рекомендуемых стандартом 802.1D. Чем выше пропускная способность интерфейса, тем ниже стоимость. Ручной режим позволяет ввести значение, определяемое пользователем. Стоимость пути учитывается при становлении активной топологии сети. Порты с более низкой стоимостью выбираются в качестве портов пересылки вместо портов с более высокой стоимостью. Диапазон допустимых значений – от 1 до 200000000
Priority	Настраивает приоритет для портов с одинаковой стоимостью пути (см. выше)
operEdge	Операционный флаг, который указывает, подключен ли порт напрямую к конечному устройству (без подключения мостов). Порты, подключенные к конечным устройствам (operEdge установлен в true), быстрее переходят в состояние пересылки, чем другие порты
AdminEdge	Параметр, который задаёт начальное состояние флага operEdge при инициализации порта. Позволяет определить, будет ли порт

	изначально рассматриваться как краевой (operEdge установлен) или нет (operEdge сброшен)
AutoEdge	Параметр, позволяющий коммутатору автоматически определять, какие порты подключены к конечным устройствам, а какие – к другим коммутаторам, на основе наличия или отсутствия BPDU
Restricted Role	Включение этого параметра не позволяет порту стать корневым для CIST или любого MSTI, даже если у него лучший вектор приоритета связующего дерева. После выбора корневого порта такой порт будет выбран в качестве альтернативного. Если параметр «Restricted Role» установлен, это может привести к потере связности в Spanning Tree, так как этот порт не будет участвовать в выборе корневого порта. Настройка может быть использована администратором сети, чтобы ограничить влияние мостов вне основной области сети, не находящихся под полным контролем администратора, на топологию связующего дерева. Эта функция также известна как Root Guard
Restricted TCN	Настройка, которая предотвращает распространение уведомлений о изменении топологии (TCN), полученных от других устройств, а также собственных TCN через этот порт. Это может привести к временной потере соединения после изменения топологии активного связующего дерева из-за того, что информация о местоположении станций может быть неправильно обновлена и не распространена по всей сети. Настройка используется администратором сети, чтобы предотвратить влияние мостов, находящихся вне основной области сети, на сброс адресов в основной области. Это полезно в тех случаях, когда мосты вне основной области сети не находятся под полным контролем администратора или когда физическое состояние связи часто изменяется (например, частые переключения состояния подключенных сетей)
BPDU Guard	BPDU Guard обычно применяется для портов, которые настроены как порты доступа и которые подключены к конечным устройствам, а не к другим коммутаторам. Когда BPDU Guard активирован на порту и этот порт получает BPDU, он автоматически блокируется. Это предотвращает возможность изменения топологии STP через этот порт, так как устройства, подключенные к порту, не должны посылать BPDU
Point2Point	Указывает, что порт подключается к локальной сети точка-точка, а не к общей среде. Можно настроить автоматическое определение или вручную установить значение true или false. Переход в состояние пересылки для локальных сетей точка-точка происходит быстрее, чем для общей среды
Save	Нажмите, чтобы сохранить изменения

Reset	Нажмите, чтобы отменить любые изменения, внесенные локально, и вернуться к ранее сохраненным значениям

4.5 Fast Recovery

Режим быстрого восстановления (Fast Recovery) можно настроить для подключения нескольких портов к одному или нескольким коммутаторам. В этом режиме устройство обеспечивает избыточные соединения. Режим Fast Recovery поддерживает 20 приоритетов. Порт с первым приоритетом станет активным, а остальные порты с другими приоритетами будут резервными.

Рисунок 30 – Настройка Fast Recovery

Параметр	Описание
Active	Установите флажок, чтобы активировать режим Fast Recovery
Port	Портам можно задать 20 приоритетов. Только порт с наивысшим приоритетом будет активным. 1-й приоритет – наивысший
Apply	Нажмите, чтобы применить настройки

5. Управление

Коммутатором можно управлять через встроенный веб-сервер, который поддерживает Internet Explorer, начиная с версии 5.0, и другие веб-браузеры, такие как Chrome. Через веб-браузер также можно обновлять прошивку. Функция веб-управления не требовательна к пропускной способности сети, повышает скорость доступа и обеспечивает удобный экран просмотра.

По умолчанию, современные браузеры не разрешают Java-апплетам или другим скриптам открывать сетевые сокеты без явного разрешения пользователя. Чтобы разрешить работу с сетевыми портами, необходимо изменить настройки безопасности браузера.

Для управления коммутатором через веб-браузер выполните следующие действия.

Вход в систему:

1. Запустите веб-браузер.
2. Введите http:// и IP-адрес коммутатора. Нажмите Enter.

Рисунок 31 – Ввод IP-адреса коммутатора

3. Появится экран входа в систему.
4. Введите имя пользователя и пароль. Имя пользователя и пароль по умолчанию – **admin**.
5. Нажмите кнопку <Enter> или <OK>, и появится основной интерфейс страницы управления.

Рисунок 32 – Экран входа в систему

Вы можете использовать следующие значения по умолчанию:

IP-адрес: 192.168.10.1

Маска подсети: 255.255.255.0

Шлюз по умолчанию: 192.168.10.254

Имя пользователя: admin

Пароль: admin

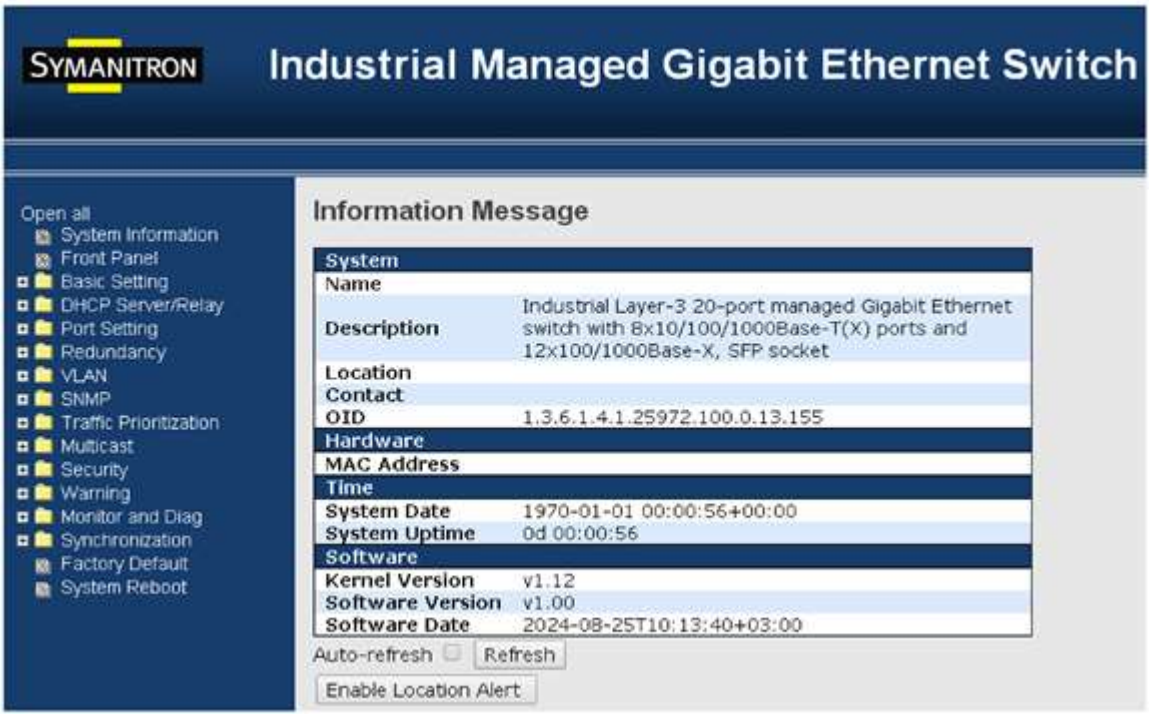


Рисунок 33 – Домашняя страница интерфейса управления

С левой стороны интерфейса управления показаны ссылки на различные настройки. Нажатие на ссылки приведет вас к отдельным страницам конфигурации.

5.1 Информация о системе

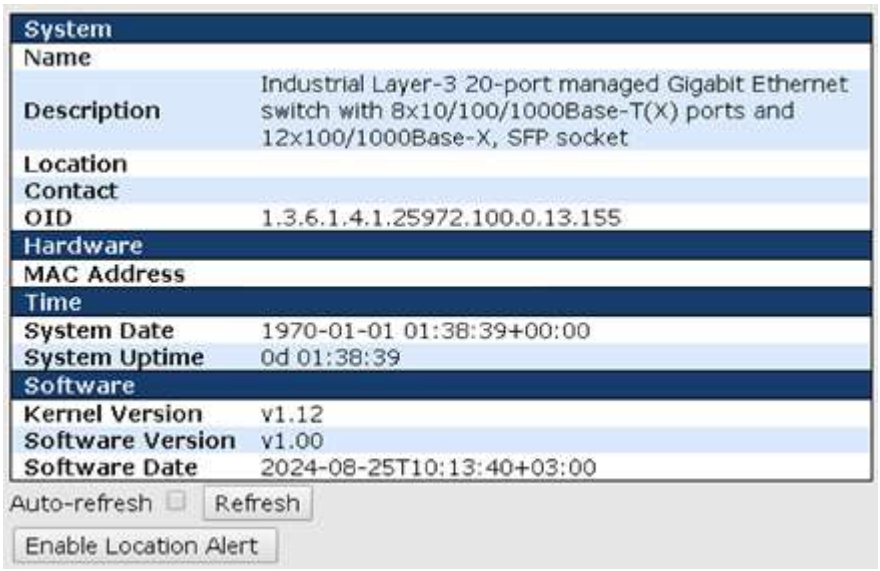


Рисунок 34 – Информация о системе

Нажмите [System Information] на левой панели, чтобы отобразить подробную информацию о системе, такую как имя устройства, описание, MAC-адрес и версия прошивки.

5.2 Передняя панель

Нажав на пункт меню [Front Panel], вы увидите изображение передней панели устройства в правой части окна. Используемый порт подсвечен зеленым. Нажмите на изображение порта, чтобы открыть окно с подробной информацией о нем.

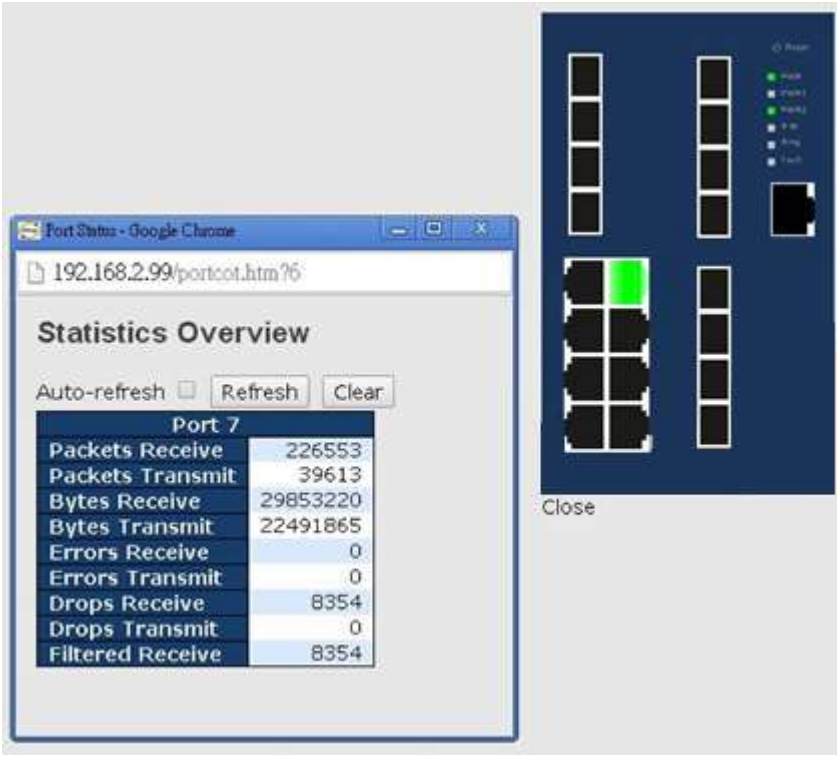


Рисунок 35 – Передняя панель

5.3 Основные настройки

Страница [Basic Settings] позволяет настраивать основные функции коммутатора.

5.3.1 Настройка системной информации

На странице [System Information Configuration] отображается общая информация о коммутаторе.

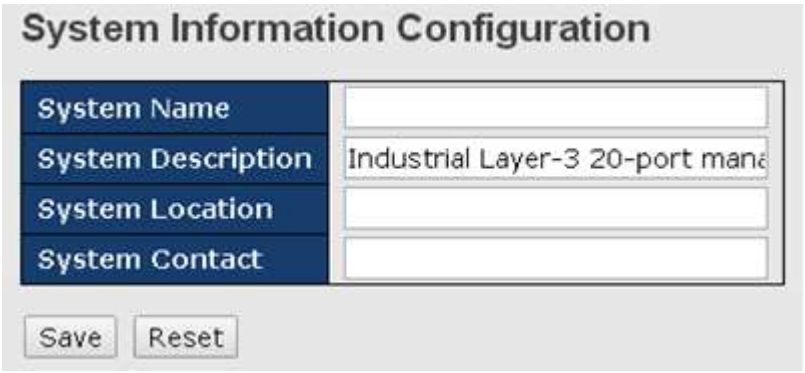


Рисунок 36 – Настройка информации о системе

Параметр	Описание
System Name	Административно назначенное имя для управляемого узла. По соглашению это должно быть полное доменное имя узла. Доменное имя представляет собой текстовую строку, состоящую из букв латинского алфавита (A-Z, a-z), цифр (0-9) и знака минус (-). Пробел не может быть частью имени. Первый символ должен быть буквой. Ни первый, ни последний символ не должен быть знаком минус. Допустимая длина строки составляет от 0 до 255
System Description	Описание устройства
System Location	Физическое местоположение узла (например, телефонный шкаф, 3-й этаж). Допустимая длина строки от 0 до 255, разрешены только символы ASCII от 32 до 126
System Contact	Текстовая идентификация контактного лица для этого управляемого узла вместе с информацией о том, как связаться с этим лицом. Допустимая длина строки от 0 до 255, разрешены только символы ASCII от 32 до 126
Save	Нажмите, чтобы сохранить изменения
Reset	Нажмите, чтобы отменить любые изменения и вернуться к ранее сохраненным значениям

5.3.2 Пароль администратора

Страница [System Password] позволяет настроить системный пароль, необходимый для доступа к веб-интерфейсу или входа в систему через CLI.

Рисунок 37 – Настройка системного пароля

Параметр	Описание
Old Password	Существующий пароль. Если он неверный, вы не сможете установить новый пароль
New Password	Новый системный пароль. Допустимая длина строки от 0 до 31, разрешены только символы ASCII от 32 до 126
Confirm New Password	Повторите новый пароль
Save	Нажмите, чтобы сохранить изменения

5.3.3 Метод аутентификации

Страница [Authentication Method Configuration] позволяет настроить способ аутентификации пользователя при входе в коммутатор через один из интерфейсов управления.

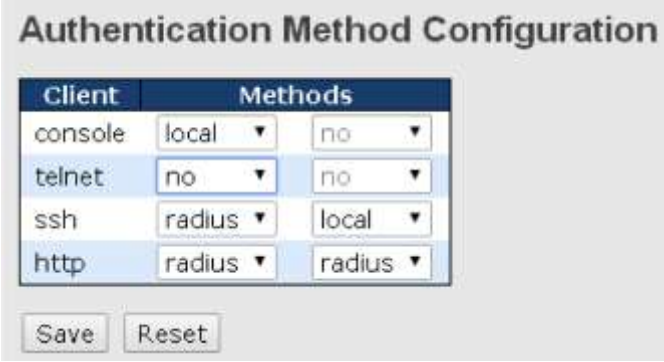


Рисунок 38 – Методы аутентификации

Параметр	Описание
Client	Клиент управления, для которого применяется приведенная ниже конфигурация
Methods	Метод аутентификации может быть настроен на одно из следующих значений: **None**: аутентификация отключена и вход невозможен **Local**: для аутентификации используется локальная база данных пользователей на коммутаторе **Radius**: для аутентификации используется удаленный сервер RADIUS
Save	Нажмите, чтобы сохранить изменения
Reset	Нажмите, чтобы отменить любые изменения, внесенные локально, и вернуться к ранее сохраненным значениям

5.3.4 Настройки IP

Эта страница позволяет настроить информацию для протокола IP коммутатора. Можно настроить параметры устройства, работающего в режиме хоста или маршрутизатора.

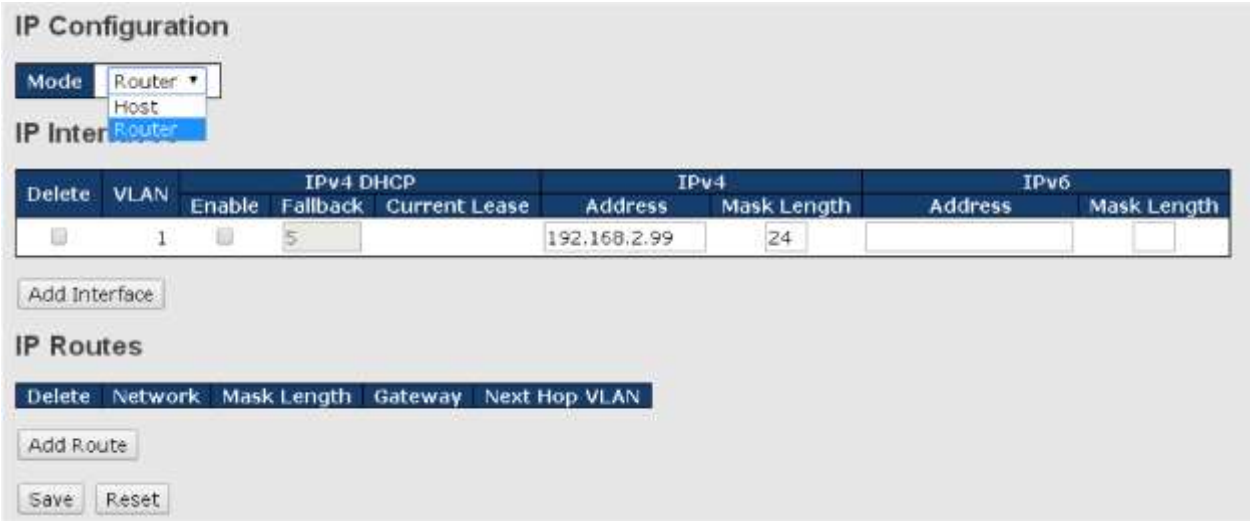


Рисунок 39 – Настройки IP

Параметр	Описание
Mode	Настройте, должен ли стек IP действовать как хост или маршрутизатор. В режиме хоста трафик IP между интерфейсами не будет

	маршрутизироваться. В режиме маршрутизатора трафик маршрутизируется между всеми интерфейсами
IP Interface	В этом разделе можно настроить параметры IPv4 и IPv6. Настройки IPv4 DHCP включают: **Enable**: установите флажок, чтобы включить функцию IPv4 DHCP. **Fallback**: указывает количество секунд для попытки получить аренду через DHCP. **Current Lease**: для интерфейсов DHCP с активной арендой в столбце отображается текущий адрес интерфейса, предоставленный сервером DHCP. Настройки IPv4 включают: **Address**: показывает IPv4-адрес интерфейса в десятичном формате с точками. Если включен DHCP, это поле не используется. Поле также можно оставить пустым, если работа IPv4 на интерфейсе нежелательна. **Mask Length**: количество бит сетевой маски IPv4 (длина префикса). Допустимые значения от 0 до 32 бит для адреса IPv4. Если включен DHCP, это поле не используется. Поле также можно оставить пустым, если работа IPv4 на интерфейсе нежелательна. Настройки IPv6 включают: **Address**: показывает адрес интерфейса. Адреса IPv6 – это 128-битные записи, представленные в виде восьми полей, содержащих до четырех шестнадцатеричных цифр, с двоеточием, разделяющим каждое поле (:). Например, fe80::21:cff:fe03:4dc7. Символ :: – это специальный синтаксис, который можно использовать в качестве сокращенного способа представления нескольких 16-битных групп смежных нулей; но он может появляться только один раз. Он также может представлять действительный адрес IPv4. Например, 192.1.2.34. Поле можно оставить пустым, если работа IPv6 на интерфейсе нежелательна. **Mask Length**: количество бит сетевой маски IPv6 (длина префикса). Допустимые значения от 1 до 128 бит для адреса IPv6. Поле можно оставить пустым, если работа IPv6 на интерфейсе нежелательна
IP Routes	**Delete**: выберите этот параметр, чтобы удалить существующий IP-маршрут. **Network**: IP-сеть назначения или адрес хоста этого маршрута. Допустимый формат – десятичная нотация с точками или нотация IPv6. Маршрут по умолчанию может использовать значение 0.0.0.0 или нотацию IPv6 (::). **Mask Length**: IP-сеть назначения или маска хоста в количестве бит (длина префикса). Она определяет, какая часть сетевого адреса должна совпадать, чтобы соответствовать этому маршруту. Допустимые

	значения находятся в диапазоне от 0 до 32 бит (соответственно 128 для маршрутов IPv6). Только маршрут по умолчанию будет иметь длину маски 0, так как он должен соответствовать любой конфигурации. **Gateway**: IP-адрес шлюза. Допустимый формат – десятичная запись с точками или запись IPv6. «Gateway» и «Network» должны быть одного типа. **Next Hop VLAN**: идентификатор VLAN (VID) определенного интерфейса IPv6, связанного со шлюзом. Указанный VID находится в диапазоне от 1 до 4094 и будет действовать только в том случае, если соответствующий интерфейс IPv6 является допустимым. Если адрес шлюза IPv6 является локальным для канала, он должен указывать VLAN следующего перехода для шлюза. Если адрес шлюза IPv6 не является локальным для канала, система игнорирует параметр «Next Hop VLAN»
Save	Нажмите, чтобы сохранить изменения
Reset	Нажмите, чтобы отменить любые изменения, внесенные локально, и вернуться к ранее сохраненным значениям

5.3.5 Состояние IP

На странице [IP Status] будут отображены сведения об IP-адресе устройства на основе конфигурации, настроенной в разделе [IP Setting].

Рисунок 40 – Состояние IP

5.3.6 SNTP

SNTP (Simple Network Time Protocol) – это протокол, способный синхронизировать время вашей системы с часами в Интернете. Он синхронизирует системное время вашего устройства с сервером, который уже был синхронизирован надежным источником, таким как радио, спутниковый приемник или модем.

Рисунок 41 – Настройка SNTP

Параметр	Описание
Mode	Включение (Enable) или отключение (Disable) использования SNTP-сервера
Server Address	Введите IP-адрес SNTP-сервера, если он включен
Save	Нажмите, чтобы сохранить изменения
Reset	Нажмите, чтобы отменить любые изменения, внесенные локально, и вернуться к ранее сохраненным значениям

5.3.7 Летнее время

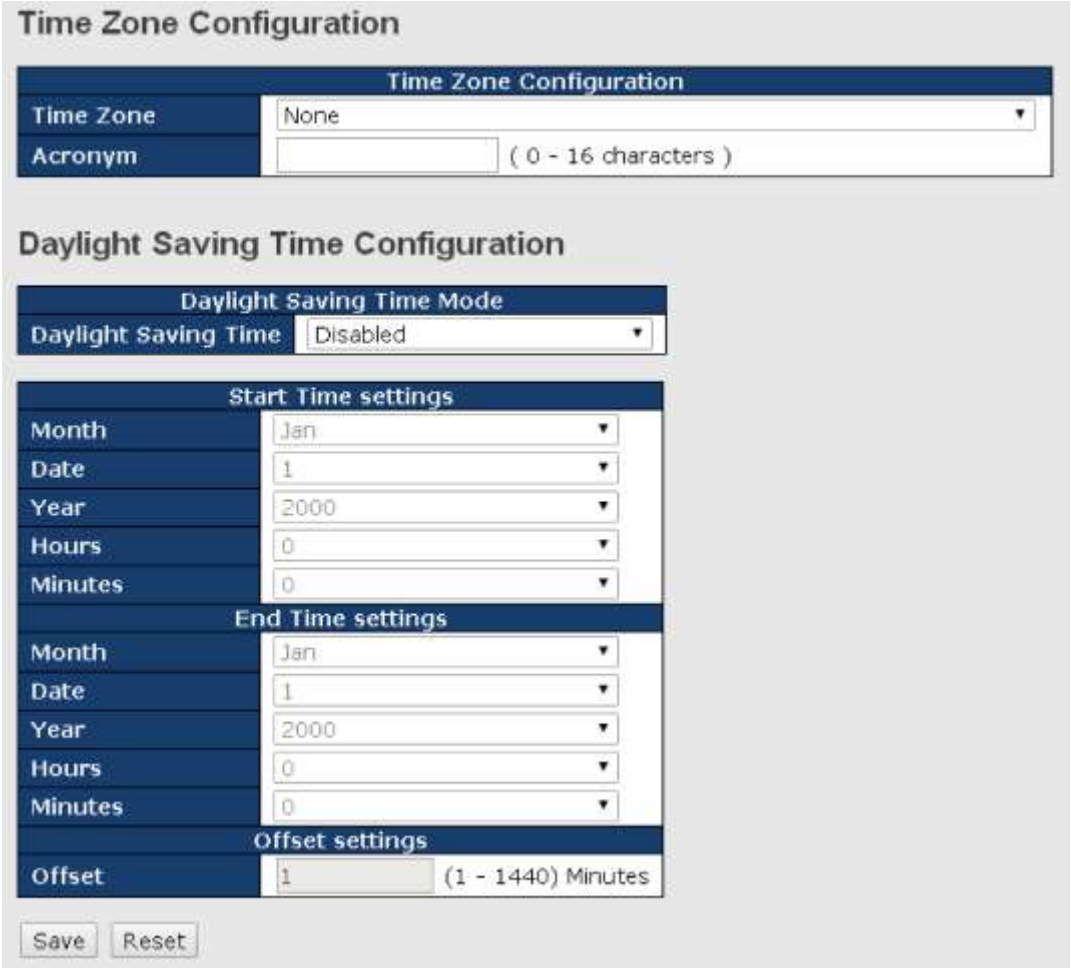


Рисунок 42 – Настройка параметров системного времени

Параметр	Описание
Time Zone Configuration	**Time Zone**: установите часовой пояс местоположения коммутатора. **Acronym**: пользователь может установить акроним часового пояса. Это настраиваемая пользователем аббревиатура для идентификации часового пояса. Диапазон: до 16 буквенно-цифровых символов. Может содержать символы «-», «_» или «.»
Daylight Saving Time Configuration	**Daylight Saving Time Mode**: включение или отключение функции летнего времени. Используется для перевода часов вперед или назад в соответствии с настройками, установленными ниже, для определенной продолжительности периода действия летнего времени. Выберите «Disable», чтобы отключить конфигурацию летнего времени. Выберите «Recurring» и настройте продолжительность летнего времени для ежегодного повторения

	перехода. Выберите «Non-Recurring» и настройте продолжительность летнего времени для единовременного перехода. По умолчанию включен параметр «Disable». **Start Time Settings**: установка времени начала периода летнего времени. **End Time Settings**: установка времени окончания периода летнего времени. **Offset Settings**: настройка времени смещения
Save	Нажмите, чтобы сохранить изменения
Reset	Нажмите, чтобы отменить любые изменения, внесенные локально, и вернуться к ранее сохраненным значениям

5.3.8 RIP

RIP (Routing Information Protocol) – один из протоколов, который может использоваться маршрутизаторами для обмена информацией о топологии сети. Он характеризуется как «внутренний» протокол шлюза и обычно используется в сетях малого и среднего размера. Маршрутизатор, работающий по протоколу RIP, отправляет содержимое своей таблицы маршрутизации каждому из своих соседних маршрутизаторов с периодичностью 30 секунд. Когда маршрут удаляется из таблицы маршрутизации, он помечается принимающими маршрутизаторами как непригодный для использования через 180 секунд и удаляется из их таблиц еще через 120 секунд. Вы можете включить или отключить RIP на странице [RIP Configuration].

Рисунок 43 – Включение/отключение RIP

5.3.9 VRRP

VRRP (Virtual Router Redundancy Protocol) – это сетевой протокол, предназначенный для обеспечения высокой доступности маршрутизаторов. Его цель – устранить точку отказа в сети, автоматически назначая доступные узлы, участвующие в группе, на роль IP-маршрутизатора.

VRRP использует виртуальный идентификатор маршрутизатора (VRID) и виртуальный IP-адрес маршрутизатора (VRIP) для представления группы маршрутизаторов как одного виртуального маршрутизатора. В эту группу входит два или более физических

маршрутизатора, среди которых выделяется главный маршрутизатор и один или несколько резервных. Все маршрутизаторы в группе имеют одинаковые VRID и VRIP.

Главный маршрутизатор выполняет основную маршрутизацию трафика. Резервные маршрутизаторы следят за состоянием главного и при его отказе автоматически принимают на себя его функции, обеспечивая непрерывность маршрутизации.

Рисунок 44 – Настройка VRRP

Параметр	Описание
VRRP Group	VRRP объединяет группу маршрутизаторов (включая главный и несколько резервных) в локальной сети в виртуальный маршрутизатор, называемый группой VRRP. **Delete**: нажмите кнопку, если хотите удалить запись из таблицы. **VRID**: введите уникальный идентификационный номер для этого виртуального маршрутизатора. Диапазон допустимых значений – от 1 до 255. **Priority**: VRRP определяет роль (главный или резервный) каждого маршрутизатора в группе VRRP согласно приоритету. Маршрутизатор с более высоким приоритетом с большей вероятностью станет главным. Приоритет VRRP находится в диапазоне от 0 до 255, и чем больше число, тем выше приоритет. Приоритеты от 1 до 254 настраиваются. Приоритет 0 зарезервирован для специального использования, а приоритет 255 – для владельца IP-адреса. Маршрутизатор, выступающий в качестве владельца IP-адреса в группе VRRP, всегда имеет текущий приоритет 255 и действует в качестве главного, пока он работает правильно. **AuthCode**: введите код авторизации для группы VRRP **Add Group**: нажмите кнопку, если хотите добавить новую запись

VRRP Member	Показывает информацию об участниках VRRP, включая VLAN ID устройства, статус в группе, VRID, VRIP и IP-адрес по умолчанию
Save	Нажмите, чтобы сохранить изменения

5.3.10 HTTPS

На этой странице можно настроить режим HTTPS.

Рисунок 45 – Настройка режима HTTPS

Параметр	Описание
Mode	Указывает выбранный режим HTTPS. Если текущее соединение – HTTPS, отключение функции автоматически перенаправит веб-браузер на соединение HTTP. Доступны режимы: **Enabled**: включить HTTPS **Disabled**: отключить HTTPS
Save	Нажмите, чтобы сохранить изменения
Reset	Нажмите, чтобы отменить любые изменения, внесенные локально, и вернуться к ранее сохраненным значениям

5.3.11 SSH

SSH (Secure Shell) – криптографический сетевой протокол, предназначенный для безопасной передачи данных и удаленного доступа путем создания защищенного канала между двумя сетевыми ПК. Настроить режим SSH можно на следующей странице.

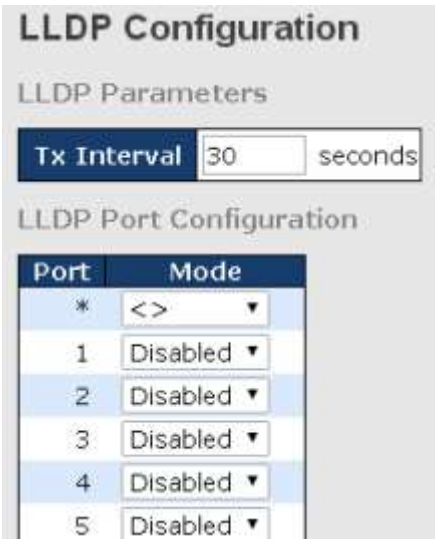
Рисунок 46 – Настройка режима SSH

Параметр	Описание
Mode	Указывает выбранный режим SSH. Доступны режимы: **Enabled**: включить SSH **Disabled**: отключить SSH
Save	Нажмите, чтобы сохранить изменения
Reset	Нажмите, чтобы отменить любые изменения, внесенные локально, и вернуться к ранее сохраненным значениям

5.3.12 LLDP

➢ **Настройки**

LLDP (Link Layer Discovery Protocol) предоставляет для сетевых устройств метод на канальном уровне получать и/или передавать свою информацию другим подключенным устройствам, использующим данный протокол, а также хранить полученную информацию о других устройствах. Эта страница позволяет проверять и настраивать текущие параметры порта LLDP.



Настройка LLDP

Параметр	Описание
Tx Interval	Устанавливает интервал между регулярными передачами объявлений LLDP
Port	Номер порта коммутатора, к которому будут применены следующие настройки
Mode	Указывает выбранный режим LLDP. **Rx only**: коммутатор не будет отправлять свою информацию LLDP, но будет анализироваться информация LLDP от соседей **Tx only**: коммутатор отбросит информацию LLDP, полученную от соседей, но будет отправлять свою информацию LLDP **Disabled**: коммутатор не будет отправлять свою информацию LLDP и будет отбрасывать информацию LLDP, полученную от соседей **Enabled**: коммутатор будет отправлять свою информацию LLDP и будет анализировать информацию LLDP, полученную от соседей

- **Информация о соседних устройствах**

Рисунок 47 – Список соседних устройств

Эта страница предоставляет обзор состояния всех соседних LLDP-устройств. Таблица содержит информацию для каждого порта, на котором обнаружен сосед, использующий протокол LLDP. Столбцы включают следующую информацию:

Параметр	Описание
Local Port	Порт, который использует локальное устройство для передачи и получения кадров LLDP
Chassis ID	Идентификационный номер соседа, отправляющего кадры LLDP
Port ID	Идентификатор порта соседа

Port Description	Описание порта, объявленного соседом
System Name	Имя, объявленное соседом
System Capabilities	Описание возможностей соседа. Значения включают: 1. Other (другое) 2. Repeater (повторитель) 3. Bridge (мост) 4. WLAN Access Point (точка доступа WLAN) 5. Router (маршрутизатор) 6. Telephone (телефон) 7. DOCSIS Cable Device (кабельное устройство DOCSIS) 8. Station Only (только станция) 9. Reserved (зарезервировано) Когда возможность включена, отображается (+). Если возможность отключена, отображается (-)
Management Address	Адрес соседа, который может быть использован для управления сетью. Может содержать IP-адрес соседнего устройства
Refresh	Нажмите, чтобы немедленно обновить страницу
Auto-refresh	Установите этот флажок, чтобы включить автоматическое обновление страницы через регулярные промежутки времени

- **Статистика**

Эта страница содержит обзор всего трафика LLDP. Показаны два типа счетчиков. Глобальные счетчики будут применять настройки ко всему стеку коммутаторов, а локальные – только к указанным коммутаторам.

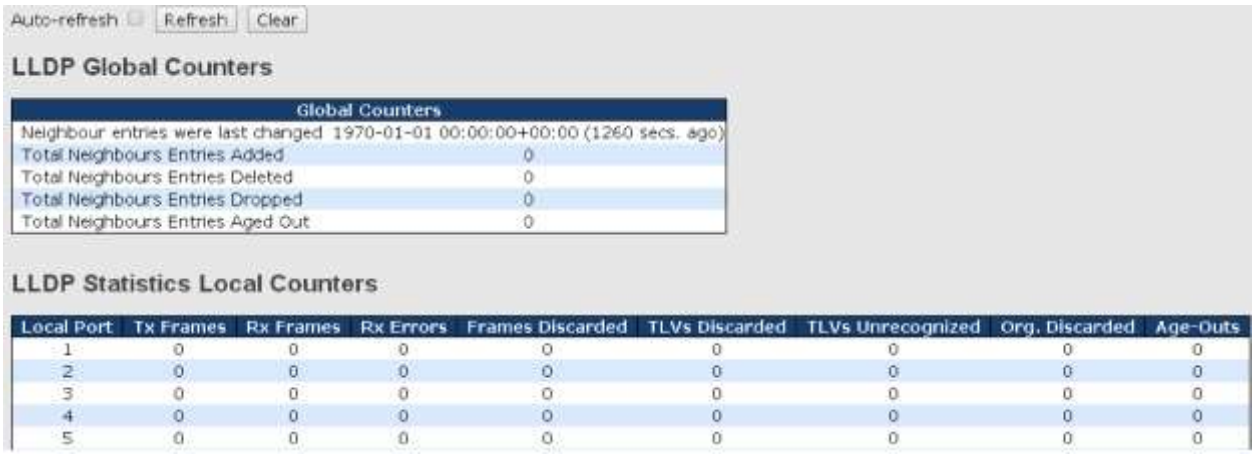


Рисунок 48 – Счетчики статистики LLDP

Глобальные счетчики

Параметр	Описание
Neighbor entries were last changed at	Показывает время, когда была удалена или добавлена последняя запись
Total Neighbors Entries Added	Показывает количество новых записей, добавленных с момента перезагрузки коммутатора
Total Neighbors Entries Deleted	Показывает количество новых записей, удаленных с момента перезагрузки коммутатора
Total Neighbors Entries Dropped	Показывает количество кадров LLDP, потерянных из-за переполнения таблицы записей
Total Neighbors Entries Aged Out	Показывает количество записей, удаленных из-за истечения срока жизни

Локальные счетчики

Параметр	Описание
Local Port	Порт, который принимает или передает кадры LLDP
Tx Frames	Количество кадров LLDP, переданных портом
Rx Frames	Количество кадров LLDP, полученных портом
Rx Errors	Количество полученных кадров LLDP, содержащих ошибки
Frames Discarded	Если порт получает кадр LLDP, а внутренняя таблица коммутатора заполнена, кадр будет подсчитан и отброшен. Такая ситуация в стандарте LLDP известна как «слишком много соседей». Кадры LLDP требуют новой записи в таблице, если «Chassis ID» или «Remote Port ID» не включены в таблицу. Записи удаляются из таблицы, когда определенный порт отключается, получен кадр закрытия LLDP, а также когда запись устаревает
TLVs Discarded	Каждый кадр LLDP может содержать несколько фрагментов информации, известных как TLV (Type Length Value). Если TLV имеет неправильный формат, кадр будет учтен и отброшен

TLVs Unrecognized	Количество правильно сформированных TLV, но с неизвестным значением типа
Org. Discarded	Количество TLV, отброшенных устройством из-за их организационной уникальности. В LLDP существуют организационно-уникальные TLV (OUI TLV), которые могут быть использованы производителями для передачи проприетарной информации
Age-Outs	Каждый кадр LLDP содержит сведения о том, как долго информация LLDP действительна (время устаревания). Если в течение времени устаревания не получен новый кадр LLDP, информация будет удалена, а значение счетчика устаревания будет увеличено
Refresh	Нажмите, чтобы немедленно обновить страницу
Clear	Нажмите, чтобы очистить локальные счетчики. Все счетчики (включая глобальные) очищаются при перезагрузке
Auto-refresh	Установите этот флажок, чтобы включить автоматическое обновление страницы через регулярные промежутки времени

5.3.13 Modbus TCP

Modbus TCP использует TCP/IP и Ethernet для передачи данных структуры сообщения Modbus между совместимыми устройствами. Протокол обычно используется в системах SCADA для связи между интерфейсом человек-машина (HMI) и программируемыми логическими контроллерами. Эта страница позволяет включать и отключать поддержку Modbus TCP коммутатора.

Рисунок 49 – Modbus TCP

Параметр	Описание
Mode	Показывает текущее состояние функции Modbus TCP
Save	Нажмите, чтобы сохранить изменения

Reset	Нажмите, чтобы отменить любые изменения, внесенные локально, и вернуться к ранее сохраненным значениям

5.3.14 Резервное копирование/восстановление конфигурации

Вы можете сохранить настройки коммутатора в виде файла или загрузить ранее сохраненный файл конфигурации на устройство для восстановления старых настроек. Конфигурация находится файле формата XML. Вы можете нажать <Save configuration>, чтобы сохранить существующие настройки в виде файла и отправить их на локальный ПК.

Рисунок 50 – Сохранение конфигурации

Выберите файл конфигурации на диске и нажмите <Upload>. Файл будет загружен на устройство.

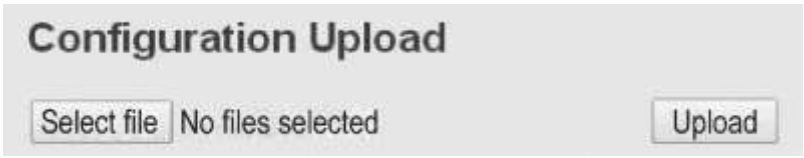


Рисунок 51 – Загрузка файла конфигурации на коммутатор

5.3.15 Обновление прошивки

Эта страница позволяет обновить прошивку коммутатора. Выберите файл прошивки, который вы хотите использовать, и нажмите <Upload>. Файл будет загружен на устройство.

Рисунок 52 – Загрузка файла прошивки на коммутатор

5.4 DHCP-сервер

Коммутатор обеспечивает функции DHCP-сервера. При включении DHCP коммутатор станет DHCP-сервером и будет динамически назначать IP-адреса и связанную с ними информацию протокола IP сетевым клиентам.

5.4.1 Настройки

Раздел [DHCP Server/Relay] позволяет настроить параметры DHCP для коммутатора. На странице настроек установите флажок «Enabled», чтобы активировать функцию. После этого вы сможете вводить информацию в каждый столбец.

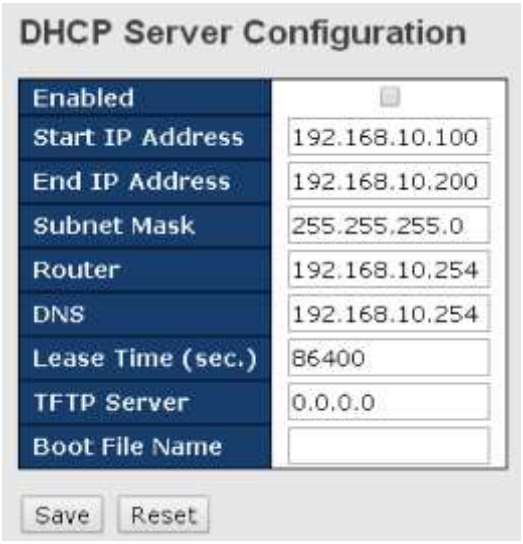


Рисунок 53 – Настройка параметров DHCP-сервера

Параметр	Описание
Enabled	Отметьте, чтобы включить функцию DHCP-сервера. Если включено, коммутатор будет DHCP-сервером в вашей локальной сети
Start IP Address	Начало диапазона динамических IP-адресов. Наименьший IP-адрес в диапазоне считается начальным. Например, если диапазон от 192.168.1.100 до 192.168.1.200, то начальным IP-адресом будет 192.168.1.100
End IP Address	Конец диапазона динамических IP-адресов. Наибольший IP-адрес в диапазоне считается конечным. Например, если диапазон от 192.168.1.100 до 192.168.1.200, то конечным IP-адресом будет 192.168.1.200
Subnet Mask	Маска подсети для диапазона динамически назначаемых IP-адресов
Router	Шлюз вашей сети
DNS	DNS вашей сети

Lease Time (sec.)	Продолжительность времени, в течение которого клиент может использовать назначенный ему IP-адрес. Время измеряется в секундах
TFTP Server	IP-адрес TFTP, на котором вы размещаете файл конфигурации или на котором вы хотите восстановить предыдущие настройки коммутатора
Boot File Name	Имя загрузочного файла используется клиентами для идентификации загрузочного образа. Укажите имя загрузочного файла, предоставленное администратором сети или указанное в документации вашей системы
Save	Нажмите, чтобы сохранить изменения
Reset	Нажмите, чтобы отменить любые изменения, внесенные локально, и вернуться к ранее сохраненным значениям

5.4.2 Список динамических клиентов

Когда функции DHCP-сервера активированы, коммутатор будет собирать информацию о клиентах DHCP и отображать ее в следующей таблице. Вы можете указать определенному порту всегда выделять определенный IP-адрес, который находится в назначенном диапазоне динамических IP-адресов. Когда какое-либо устройство подключается к этому порту и запрашивает динамический IP-адрес, система выделит именно тот адрес, который вы ранее указали.

Рисунок 54 – Список динамических клиентов

Параметр	Описание
MAC Address	Отображает MAC-адрес указанного хоста
IP Address	Отображает IP-адрес, который клиент получает от DHCP-сервера
Surplus Lease	Оставшееся время аренды соответствующего IP-адреса

5.4.3 Список статических клиентов

Вы можете вручную добавлять на свой DHCP-сервер клиентов, которые будут получать один и тот же IP-адрес при каждом запуске. Для добавления статического клиента необходимо ввести его MAC- и IP-адрес на странице настройки.

Рисунок 55 – Список статических клиентов

5.4.4 DHCP Relay

Ретранслятор DHCP используется для пересылки и передачи сообщений DHCP между клиентами и сервером, когда они не находятся в одном домене подсети. Вы можете настроить данную функцию на этой странице.

Рисунок 56 – Настройка DHCP-ретранслятора

Параметр	Описание
Relay Mode	Указывает существующий режим DHCP-ретрансляции. Включает следующие режимы: **Enabled**: активировать DHCP-ретрансляцию. Когда DHCP-ретрансляция включена, агент пересылает и передает DHCP-сообщения между клиентами и сервером, когда они не находятся в одном домене подсети, чтобы предотвратить

	лавинную рассылку широковещательных сообщений DHCP по соображениям безопасности **Disabled**: отключить DHCP-ретрансляцию
Relay Server	Указывает IP-адрес сервера DHCP-ретрансляции. Агент DHCP-ретрансляции используется для пересылки и передачи сообщений DHCP между клиентами и сервером, когда они не находятся в одном домене подсети
Relay Information Mode	Указывает существующий режим информации DHCP-ретрансляции. Формат Circuit ID Option 82 – «[vlan_id][module_id][port_no]». Первые четыре символа представляют идентификатор VLAN, а пятый и шестой символы – идентификатор модуля. В автономных устройствах идентификатор модуля всегда равен 0; в стековых устройствах он означает идентификатор коммутатора. Последние два символа – номер порта. Например, «00030108» означает, что сообщение DHCP получено от VLAN 3, коммутатора 1 и порта № 8. Значение Remote ID Option 82 равно MAC-адресу коммутатора. Включает следующие режимы: **Enabled**: активировать информацию DHCP-ретрансляции. Когда информация DHCP-ретрансляции включена, агент добавляет определенную информацию (Option 82) в сообщение DHCP при пересылке на DHCP-сервер и удаляет ее из сообщения DHCP при передаче DHCP-клиенту. Работает только при включенном режиме ретрансляции DHCP. **Disabled**: отключить информацию DHCP-ретрансляции
Relay Information Policy	Определяет политику, которая будет применяться при получении информации от DHCP-ретранслятора. Если режим обработки информации от ретранслятора включен, и агент получает DHCP-сообщение, которое уже содержит информацию от relay-агента, то данная политика будет применена. Опция «Replace» становится недоступной, если режим обработки информации от DHCP-ретранслятора отключен. Включает следующие политики: **Replace**: заменить исходную информацию DHCP Relay при получении содержащего ее DHCP-сообщения. **Keep**: сохранить исходную информацию DHCP Relay при получении содержащего ее DHCP-сообщения. **Drop**: удалить пакет при получении сообщения DHCP, содержащего информацию DHCP Relay
Save	Нажмите, чтобы сохранить изменения

Reset	Нажмите, чтобы отменить любые изменения, внесенные локально, и вернуться к ранее сохраненным значениям

Статистика DHCP Relay показывает информацию о ретранслированных пакетах коммутатора.

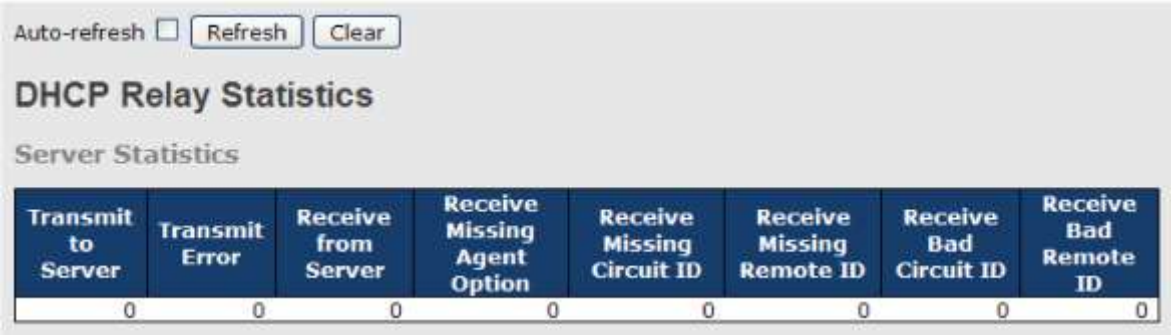
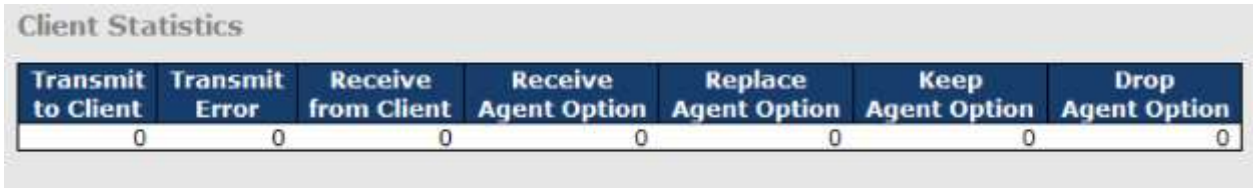


Рисунок 57 – Статистика сервера ретрансляции DHCP

Параметр	Описание
Transmit to Server	Количество пакетов, переданных от клиента на сервер
Transmit Error	Количество пакетов с ошибками при отправке клиентам
Receive from Server	Количество пакетов, полученных с сервера
Receive Missing Agent Option	Количество пакетов, полученных без информации агента
Receive Missing Circuit ID	Количество пакетов, полученных с Circuit ID
Receive Missing Remote ID	Количество пакетов, полученных с отсутствующей опцией Remote ID
Receive Bad Circuit ID	Количество пакетов, Circuit ID которых не совпадает с известным Circuit ID
Receive Bad Remote ID	Количество пакетов, Remote ID которых не совпадает с известным Remote ID


Client Statistics

Transmit to Client	Transmit Error	Receive from Client	Receive Agent Option	Replace Agent Option	Keep Agent Option	Drop Agent Option
0	0	0	0	0	0	0

Рисунок 58 – Статистика клиента ретрансляции DHCP

Параметр	Описание
Transmit to Client	Количество пакетов, переданных с сервера клиенту
Transmit Error	Количество пакетов с ошибками при отправке на серверы
Receive from Client	Количество пакетов, полученных с сервера
Receive Agent Option	Количество полученных пакетов, содержащих информацию агента ретрансляции
Replace Agent Option	Количество замененных пакетов, если полученные сообщения содержат информацию агента ретрансляции
Keep Agent Option	Количество пакетов, информация агента ретрансляции которых сохранена
Drop Agent Option	Количество пакетов, отброшенных из-за наличия в них информации агента ретрансляции

5.5 Настройка портов

В разделе [Port Setting] можно управлять отдельными портами коммутатора, включая настройки прохождения трафика, режимы питания и агрегацию.

5.5.1 Управление портами

Страница [Port Configuration] показывает текущие конфигурации портов. Также здесь можно настроить порты.

Рисунок 59 – Конфигурация портов

Параметр	Описание
Port	Номер порта коммутатора, к которому будут применены следующие настройки
Link	Текущее состояние соединения отображается разными цветами. Зеленый цвет означает, что соединение работает, а красный – что соединения в настоящий момент нет
Current Speed	Указывает текущую скорость соединения порта
Configured Speed	В раскрывающемся списке представлены доступные варианты настройки скорости соединения для данного порта коммутатора: **Auto** выбирает самую высокую скорость, поддерживаемую партнером по соединению **Disabled** отключает настройку порта коммутатора **<>** настраивает все порты
Flow Control	Если для настройки скорости выбрано значение «Auto», управление потоком будет согласовываться с пропускной способностью, объявленной партнером по соединению. Если выбрана настройка фиксированной скорости, то она и используется. **Current Rx** указывает, соблюдаются ли кадры паузы на порту, а **Current Tx** указывает, передаются ли кадры паузы на порту. Настройки Rx и Tx определяются результатом последнего автосогласования. Вы можете проверить столбец «Configured», чтобы использовать управление потоком. Эта настройка связана с настройкой «Configured Speed»
Maximum Frame Size	Вы можете ввести максимальный размер кадра, разрешенный для порта коммутатора в этом столбце, включая FCS. Допустимый диапазон составляет от 1518 байт до 9600 байт
Excessive Collision Mode	Настраивает поведение порта в случае коллизий при передаче. **Discard**: отбросить кадр после определенного количества коллизий (по умолчанию). **Restart**: перезапустить алгоритм отсрочки после определенного количества коллизий
Save	Нажмите, чтобы сохранить изменения

Reset	Нажмите, чтобы отменить любые изменения, внесенные локально, и вернуться к ранее сохраненным значениям
Refresh	Нажмите, чтобы обновить страницу. Любые изменения, внесенные локально, будут отменены

5.5.2 Агрегирование портов

Port Trunk – это группа агрегации портов, которые были сгруппированы вместе для работы в качестве одного логического пути. Этот метод обеспечивает экономичный способ увеличения пропускной способности между коммутатором и другим сетевым устройством. Кроме того, он полезен, когда одного физического соединения между устройствами недостаточно для обработки трафика. Эта страница позволяет настроить режим вычисления хеш-кода и группу агрегации.

➢ **Конфигурации**

Параметры «Hash Code Contributors» определяют, какие поля пакетов данных будут использоваться для вычисления хеш-кода, который затем определяет, по какому физическому порту будет отправлен пакет.

Рисунок 60 – Настройка режима вычисления хеш-кода

Параметр	Описание
Source MAC Address	Выбор этого параметра означает, что хеш-код будет вычисляться с использованием MAC-адреса источника кадра. Это полезно для равномерного распределения трафика от разных источников по различным портам. По умолчанию этот параметр включен
Destination MAC Address	Выбор этого параметра означает, что хеш-код будет вычисляться с использованием MAC-адреса назначения кадра. Это может быть полезно для распределения трафика к различным получателям через различные порты. По умолчанию этот параметр отключен

IP Address	Выбор этого параметра означает, что хеш-код будет вычисляться с использованием IP-адресов источника и назначения кадра. Это позволяет распределять трафик на основе логических сетевых адресов, что может улучшить балансировку нагрузки в сетях с большим количеством IP-трафика. По умолчанию этот параметр включен
TCP/UDP Port Number	Выбор этого параметра означает, что хеш-код будет вычисляться с использованием номеров портов TCP или UDP источника и назначения. Это полезно для распределения трафика между различными сеансами связи, такими как веб-запросы или передача данных по разным приложениям. По умолчанию этот параметр включен

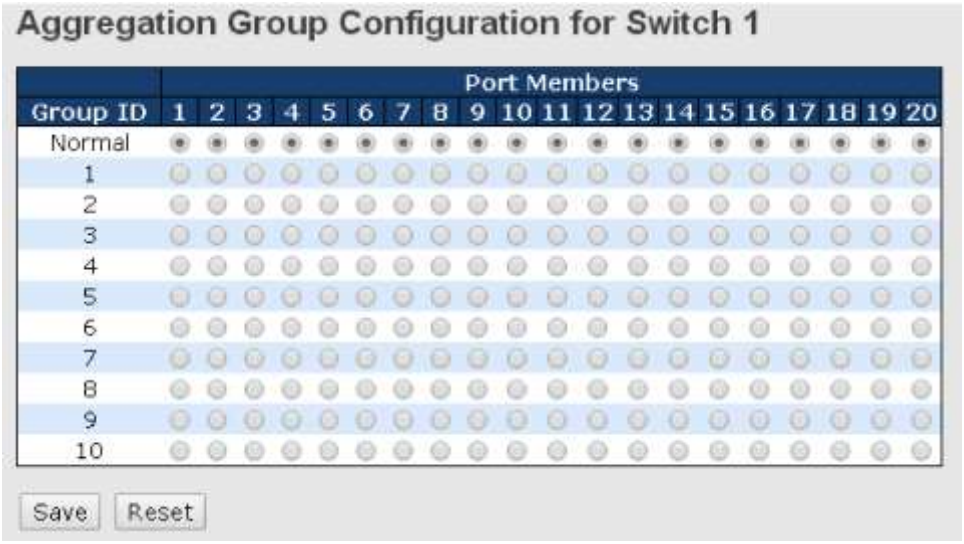


Рисунок 61 – Настройка группы агрегации

Параметр	Описание
Group ID	Указывает идентификатор каждой группы агрегации. «Normal» означает отсутствие агрегации. Для каждого порта действителен только один идентификатор группы
Port Members	Перечисляет каждый порт коммутатора для каждого идентификатора группы. Включение порта в группу агрегации и исключение порта из группы производится нажатием соответствующей кнопки в окне интерфейса. По умолчанию ни один порт не принадлежит ни к одной группе. К агрегации могут присоединиться только полнодуплексные порты. Также порты в каждой группе должны иметь одинаковую скорость

Save	Нажмите, чтобы сохранить изменения
Reset	Нажмите, чтобы отменить любые изменения, внесенные локально, и вернуться к ранее сохраненным значениям

- **LACP**

Агрегации LACP (Link Aggregation Control Protocol) похожи на статические портовые агрегации, но они более гибкие, поскольку протокол LACP соответствует стандарту IEEE 802.3ad. Следовательно, он совместим с оборудованием других поставщиков, которые также соответствуют стандарту. Эта страница позволяет включить функции LACP для группировки портов вместе и формирования отдельных виртуальных каналов, а также изменения связанных настроек, тем самым увеличивая пропускную способность между коммутатором и другими LACP-совместимыми устройствами.

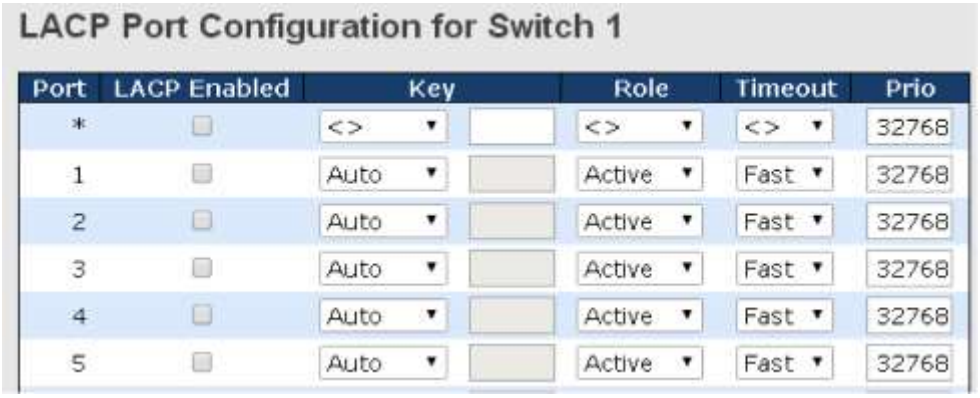


Рисунок 62 – Настройка LACP на портах

Параметр	Описание
Port	Номер порта
LACP Enabled	Установите флажок, чтобы включить LACP для порта
Key	Значение ключа зависит от порта и может находиться в диапазоне от 1 до 65535. **Auto** устанавливает значение ключа в соответствии со скоростью физического соединения (10 Мбит = 1, 100 Мбит = 2, 1 Гбит = 3). **Specific** позволяет ввести пользовательское значение. Порты с одинаковым значением ключа могут входить в одну и ту же группу агрегации, а порты с разными значениями – нет
Role	Указывает состояние активности LACP.

	Active передает пакеты LACP каждую секунду. **Passive** передает свои пакеты только получив пакет LACP от партнера
Timeout	Вы можете изменить длительность тайм-аута LACP, выбрав «Fast» или «Slow»
Prio	Установите приоритет порта. Чем выше значение, тем ниже приоритет
Save	Нажмите, чтобы сохранить изменения
Reset	Нажмите, чтобы отменить любые изменения, внесенные локально, и вернуться к ранее сохраненным значениям

- **Состояние системы LACP**

На этой странице представлен обзор состояния всех экземпляров LACP.

Рисунок 63 – Статус LACP

Параметр	Описание
Aggr ID	Идентификатор экземпляра агрегации. Для LLAG идентификатор отображается как «isid:aggr-id», а для GLAG как «aggr-id»
Partner System ID	Системный идентификатор (MAC-адрес) партнера по агрегации
Partner Key	Если ваш коммутатор подключается к устройству от другого производителя через LACP, может возникнуть необходимость в ручной настройке параметра «Partner Key». Это ключ, который определяет, как коммутатор партнера идентифицирует и управляет агрегированным каналом на своей стороне
Partner Prio	Настраивает приоритет партнера
Last Changed	Время, прошедшее с момента изменения этого агрегирования
Local Ports	Указывает, какие порты относятся к агрегации коммутатора/стека. Формат: «Switch ID:Port»

Refresh	Нажмите, чтобы немедленно обновить страницу
Auto-refresh	Установите этот флажок, чтобы включить автоматическое обновление страницы через регулярные промежутки времени

- **Состояние портов LACP**

На этой странице представлен обзор состояния LACP для всех портов.

Рисунок 64 – Состояние LACP на портах

Параметр	Описание
Port	Номер порта коммутатора
LACP	**Yes** означает, что LACP включен и порт в состоянии «Link-up» **No** означает, что LACP не включен или порт в состоянии «Link-down» **Backup** означает, что порт не может присоединиться к группе агрегации, если не удалить другие порты. LACP отключен
Key	Ключ, назначенный порту. Объединены могут быть только порты с одинаковым ключом
Aggr ID	Идентификатор, назначенный группе агрегации
Partner System ID	Системный идентификатор (MAC-адрес) партнера
Partner Port	Номер порта партнера, связанного с локальным портом
Partner Prio	Отображает приоритет партнера
Refresh	Нажмите, чтобы немедленно обновить страницу

Auto-refresh	Установите этот флажок, чтобы включить автоматическое обновление страницы через регулярные промежутки времени

➢ **Статистика портов LACP**

На этой странице представлен обзор статистики LACP для всех портов.

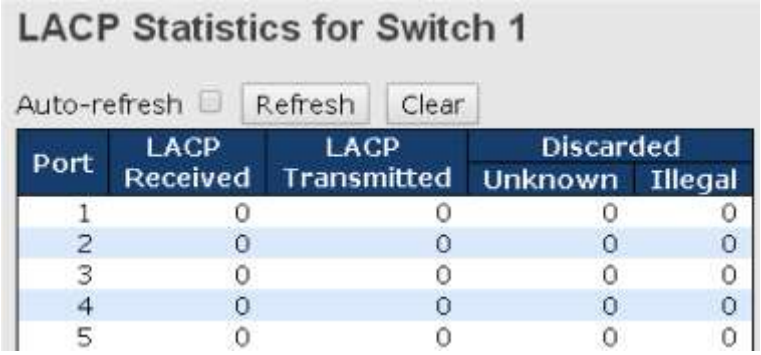


Рисунок 65 – Статистика LACP

Параметр	Описание
Port	Номер порта коммутатора
LACP Transmitted	Количество кадров LACP, отправленных с каждого порта
LACP Received	Количество кадров LACP, полученных на каждом порту
Discarded	Количество неизвестных (Unknown) или недопустимых(Illegal) кадров LACP, отброшенных на каждом порту
Refresh	Нажмите, чтобы немедленно обновить страницу
Auto-refresh	Установите этот флажок, чтобы включить автоматическое обновление страницы через регулярные промежутки времени
Clear	Нажмите, чтобы очистить счетчики для всех портов

5.5.3 Предотвращение возникновения петель

Функция Loop Protection предотвращает возникновение сетевых петель. Если на порт поступают пакеты, свидетельствующие о наличии петли, порт будет автоматически отключён. Это защищает другие устройства в сети от возможных проблем, вызванных сетевым циклом.

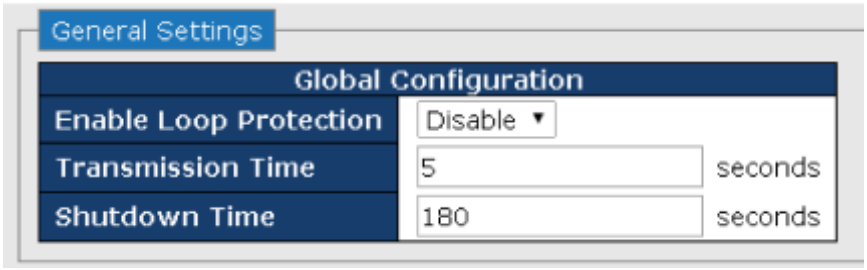


Рисунок 66 – Глобальная настройка Loop Protection

Параметр	Описание
Enable Loop Protection	Активация функции защиты от петель (глобально)
Transmission Time	Интервал между каждым PDU Loop Protection, отправляемым на каждый порт. Допустимое значение от 1 до 10 секунд
Shutdown Time	Период (в секундах), в течение которого порт будет оставаться отключенным при обнаружении петли. Допустимое значение от 0 до 604800 секунд (7 дней). Значение, равное нулю, будет держать порт отключенным постоянно, до перезапуска устройства

Рисунок 67 – Настройка Loop Protection на портах

Параметр	Описание
Port	Номер порта коммутатора
Enable	Активация функции защиты от петель

Action	Настраивает действие, которое следует предпринять при обнаружении петель. Имеет следующие значения: **Shutdown Port**: выключить порт **Shutdown Port and Log**: выключить порт и внести запись в журнал **Log Only**: внести запись в журнал
Tx Mode	Управляет тем, будет ли порт активно генерировать PDU Loop Protection или только пассивно ожидать PDU от других участников

➢ **Состояние защиты от петель**

На странице <Loop Protection Status> отображается информация о конфигурации функции, которая была создана на странице настроек.

Рисунок 68 – Состояние Loop Protection

Параметр	Описание
Port	Номер порта коммутатора
Action	Показывает действие, которое должно произойти на основе ваших настроек
Transmit	Показывает режим передачи на основе ваших настроек
Loops	Количество петель, обнаруженных на этом интерфейсе с момента последней загрузки системы или с момента очистки статистики
Status	Текущее состояние Loop Protection порта
Loop	Обнаружена ли в данный момент петля на порту
Time of Last Loop	Время последнего события, связанного с обнаружением петли
Refresh	Нажмите, чтобы немедленно обновить страницу
Auto-refresh	Установите этот флажок, чтобы включить автоматическое обновление страницы через регулярные промежутки времени

5.6 VLAN

5.6.1 Участие в VLAN

VLAN (виртуальная локальная сеть) – это логическая локальная сеть, основанная на физической локальной сети и ее связях, но не состоящая из физического (проводного или беспроводного) соединения между двумя вычислительными устройствами, а реализованная с использованием методов виртуализации. VLAN можно создать путем разделения физической локальной сети на несколько логических локальных сетей с использованием идентификатора VLAN. На странице <VLAN Membership> можно назначать порты коммутатора для VLAN и добавлять новые VLAN.

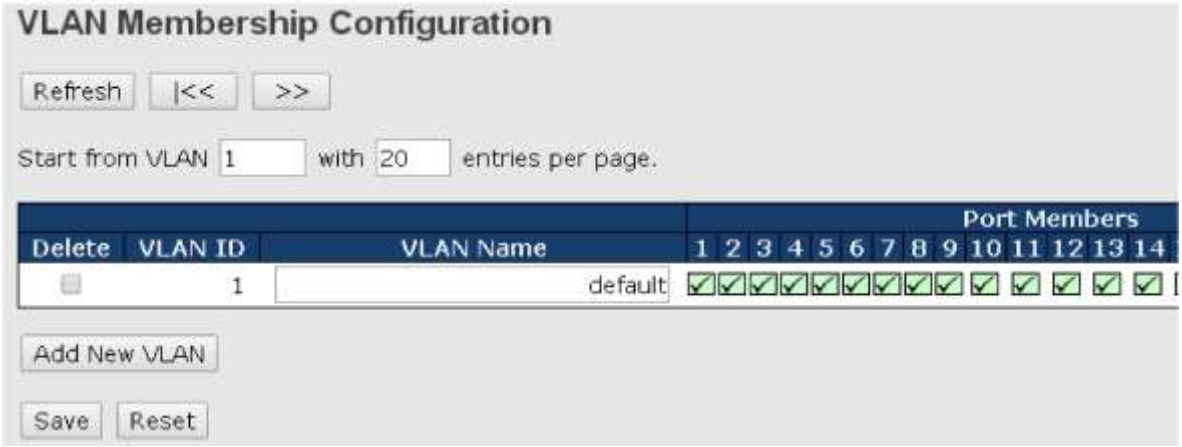


Рисунок 69 – Создание и настройка VLAN

Параметр	Описание
Delete	Установите флажок, чтобы удалить запись VLAN. Она будет удалена при следующем сохранении
VLAN ID	Идентификатор VLAN
VLAN Name	Имя VLAN
Port Members	Флажки указывают, какие порты являются участниками VLAN. Установите или снимите флажок, чтобы изменить запись
Add New VLAN	Нажмите, чтобы добавить новую VLAN. В таблицу добавляется пустая строка, и VLAN можно настроить по мере необходимости. Допустимые значения для идентификатора VLAN: от 1 до 4095. После нажатия кнопки <Save> новая VLAN будет включена в выбранном стеке, но не будет содержать портов-участников.

	При сохранении настроек VLAN без портов-участников в любом стеке будет удалена
Save	Нажмите, чтобы сохранить изменения
Reset	Нажмите, чтобы отменить любые изменения, внесенные локально, и вернуться к ранее сохраненным значениям

5.6.2 Настройка портов

Страница [VLAN Port Configurations] позволяет вам настраивать порты VLAN по отдельности.

Рисунок 70 – Настройка портов VLAN

Параметр	Описание
Ethertype for custom S-Ports	Этот параметр определяет значение поля **EtherType** для пользовательских S-портов. Данное значение будет применяться ко всем пользовательским S-портам в сети. Использование настраиваемого EtherType позволяет изменить стандартное значение поля на порту для поддержки сетевых устройств, которые не используют стандартное значение 0x8100 для 802.1Q- или 802.1p-тегированных кадров. Когда тип порта установлен как **S-custom-port**, значение **EtherType** (также известного как TPID) всех кадров, полученных на этом порту, будет изменено на указанное значение. По умолчанию, значение EtherType установлено на 0x88a8 (соответствующее стандарту IEEE 802.1ad)
Port	Номер порта коммутатора, к которому будут применены следующие настройки
Port type	Порт может быть одного из следующих типов: неосведомленный о VLAN (Unaware), клиентский (C-port), сервисный (S port), пользовательский сервисный (S-custom-port).

	C-port: каждый кадр назначается VLAN, указанной в теге VLAN, а тег удаляется. **S-port**: EtherType всех полученных кадров изменяется на 0x88a8, чтобы указать, что через коммутатор пересылаются кадры с двойным тегом. Коммутатор передаст эти кадры в VLAN, указанную во внешнем теге. Он не будет удалять внешний тег и не будет изменять какие-либо компоненты тега, кроме поля EtherType. **S-custom-port**: EtherType всех полученных кадров изменяется на значение, установленное в поле «Ethertype for Custom S-ports», чтобы указать, что через коммутатор пересылаются кадры с двойным тегом. Коммутатор передаст эти кадры в VLAN, указанную во внешнем теге. Он не будет удалять внешний тег и не будет изменять какие-либо компоненты тега, кроме поля EtherType. **Unaware**: все кадры классифицируются по PVID, а теги не удаляются
Ingress Filtering	Включите фильтрацию входящего трафика на порту, установив флажок. Этот параметр влияет на обработку входящего трафика VLAN. Если функция включена, а входящий порт не является членом классифицированной VLAN кадра, кадр будет отброшен. По умолчанию фильтрация входящего трафика отключена (флажок отсутствует)
Frame Type	Определяет, принимает ли порт все кадры или только тегированные/нетегированные кадры. Этот параметр влияет на обработку входящего трафика VLAN. Если порт принимает только тегированные кадры, то нетегированные кадры, полученные на порту, будут отбрасываться. По умолчанию значение установлено на «All» (принимаются все типы кадров)
Port VLAN Mode	Допустимые значения: **None** или **Specific**. Этот параметр влияет на обработку входящего и исходящего трафика VLAN. Если выбрано **None**, тег VLAN с классифицированным VLAN ID добавляется в кадры, передаваемые через порт. Этот режим обычно используется для портов, подключенных к коммутаторам с поддержкой проверки тегов VLAN. При использовании этого режима параметр «Tx Tag» должен быть установлен на «Untag_pvid». Если выбрано **Specific** (значение по умолчанию), можно настроить **Port VLAN ID** (PVID). Нетегированные кадры, полученные на порту, классифицируются по PVID. Если проверка тегов VLAN отключена, все кадры, полученные на порту, классифицируются по PVID. Если классифицированный VLAN ID кадра, переданного на порт,

	отличается от PVID, в кадр будет добавлен тег VLAN с классифицированным VLAN ID
Port VLAN ID	Настраивает идентификатор VLAN по умолчанию для порта (PVID). Допустимый диапазон значений – от 1 до 4095. Значение по умолчанию – 1. Примечание: порт должен быть членом VLAN, идентификатор которой совпадает с PVID
Tx Tag	Определяет выходную маркировку порта. **Untag_pvid**: все VLAN, кроме настроенного PVID, будут тегированы; **Tag_all**: все VLAN будут тегированы; **Untag_all**: все VLAN не тегируются
Save	Нажмите, чтобы сохранить изменения
Reset	Нажмите, чтобы отменить любые изменения, внесенные локально, и вернуться к ранее сохраненным значениям

- **Типы портов**

Ниже приведено подробное описание каждого типа порта, включая Unaware, C-port, S-port и S-custom-port.

Таблица 7 – Функции портов Unaware, C, S и S-custom

Тип порта	Действие на входе	Действие на выходе
Unaware Функция Unaware может использоваться для 802.1QinQ (двойной тег)	Когда порт получает нетегированные кадры, он добавляет в них тег на основе PVID и пересылает. Когда порт получает тегированные кадры: 1. Если тегированный кадр содержит TPID 0x8100, он станет кадром с двойным тегом и будет отправлен 2. Если TPID тегированного кадра не равен 0x8100 (например, 0x88A8), кадр будет отброшен	TPID кадра, переданного портом Unaware, будет установлен на 0x8100. Окончательный статус кадра после выхода также будет зависеть от настроенного на выходе правила

C-port	Когда порт получает нетегированные кадры, он добавляет в них тег на основе PVID и пересылает. Когда порт получает тегированные кадры: 1. Если тегированный кадр содержит TPID 0x8100, он будет отправлен 2. Если TPID тегированного кадра не равен 0x8100 (например, 0x88A8), кадр будет отброшен	TPID кадра, переданного С-портом, будет установлен на 0x8100
S-port	Когда порт получает нетегированные кадры, он добавляет в них тег на основе PVID и пересылает. Когда порт получает тегированные кадры: 1. Если тегированный кадр содержит TPID 0x88A8, он будет отправлен 2. Если TPID тегированного кадра не равен 0x88A8 (например, 0x8100), кадр будет отброшен	TPID кадра, переданного через S-порт, будет установлен на 0x88A8
S-custom-port	Когда порт получает нетегированные кадры, он добавляет в них тег на основе PVID и пересылает. Когда порт получает тегированные кадры: 1. Если тегированный кадр содержит TPID 0x88A8, он будет отправлен 2. Если TPID тегированного кадра не равен 0x88A8 (например, 0x8100), кадр будет отброшен	TPID кадра, переданного S-custom-портом, будет установлен на значение, которое ранее было настроено пользователем в поле **Ethertype for custom S-Ports**

Ниже приведены иллюстрации действий различных типов портов:

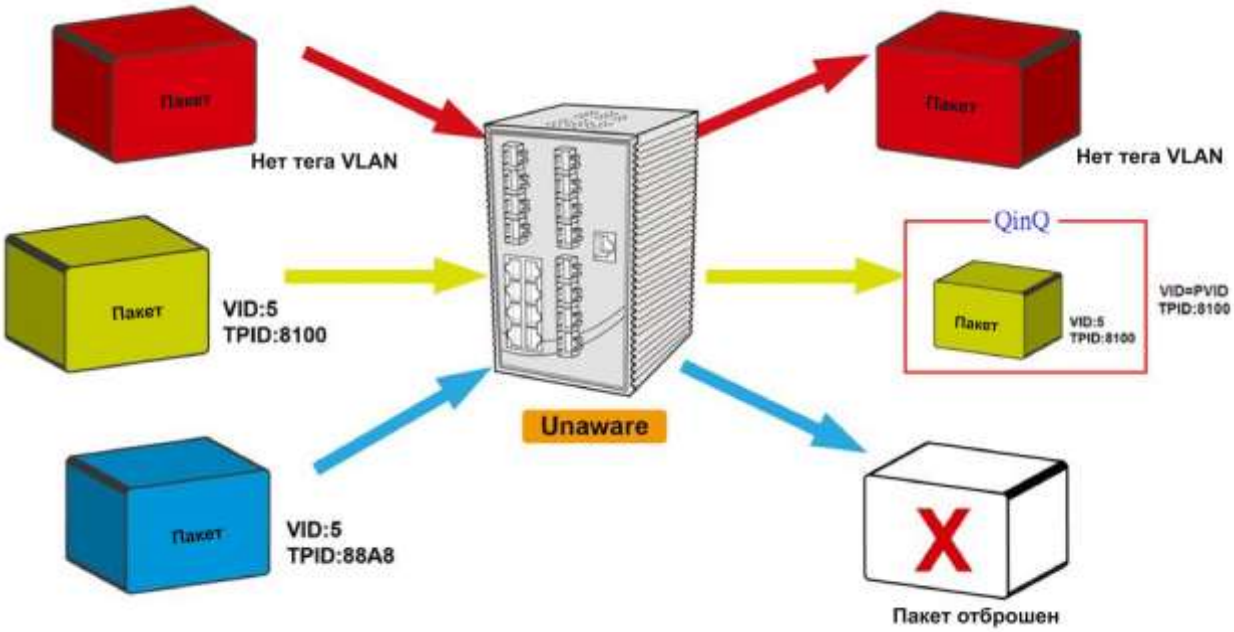


Рисунок 71 – Порт Unaware

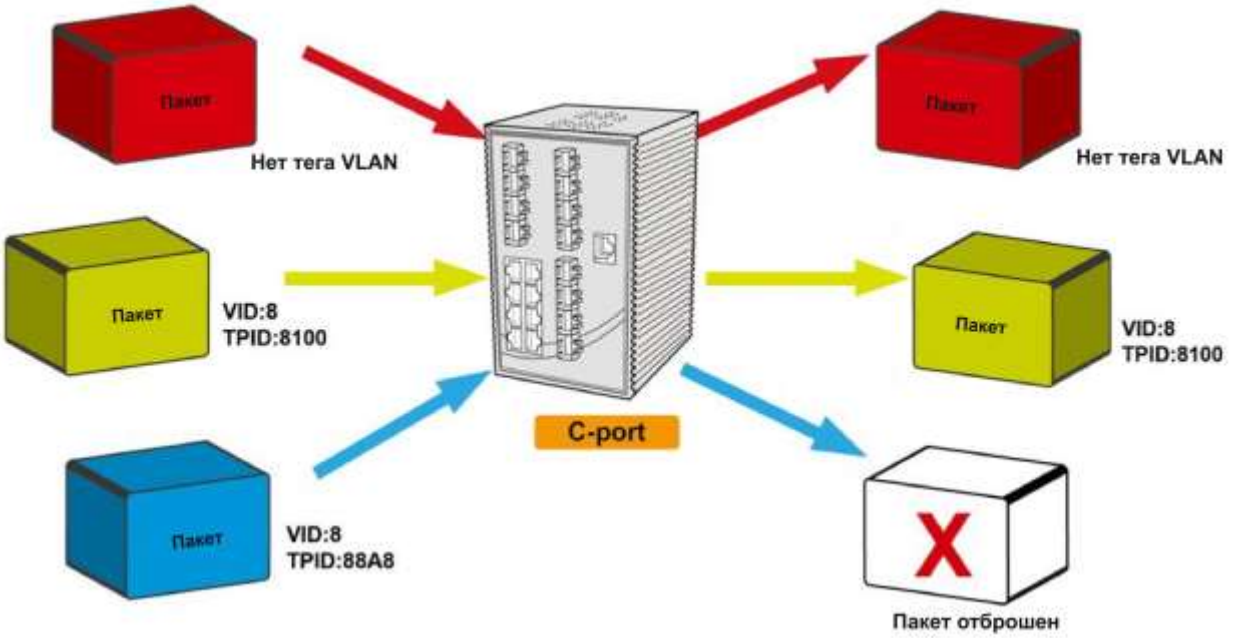


Рисунок 72 – С-порт

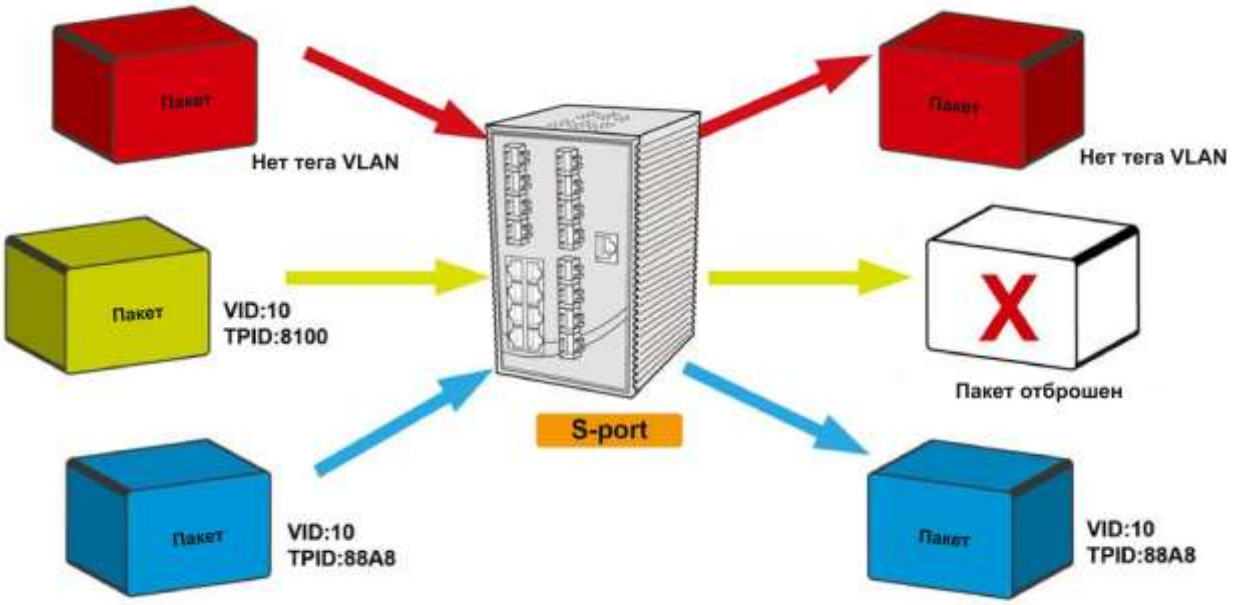


Рисунок 73 – S-порт

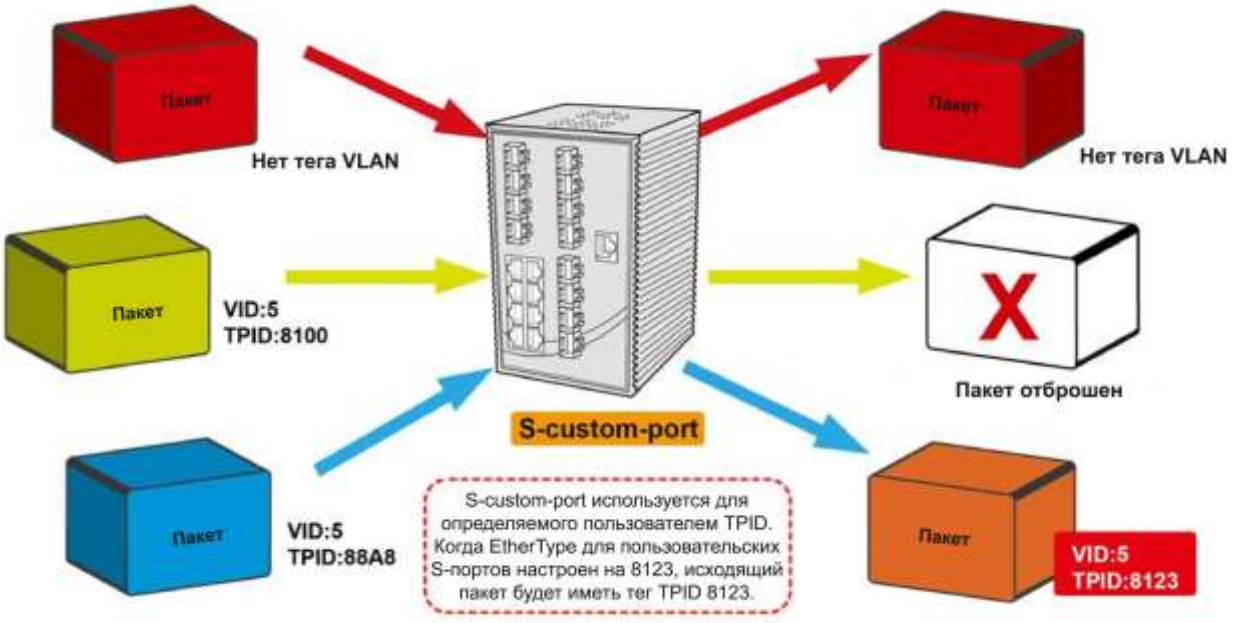


Рисунок 74 – S-custom-порт

5.6.2.1 Примеры настроек

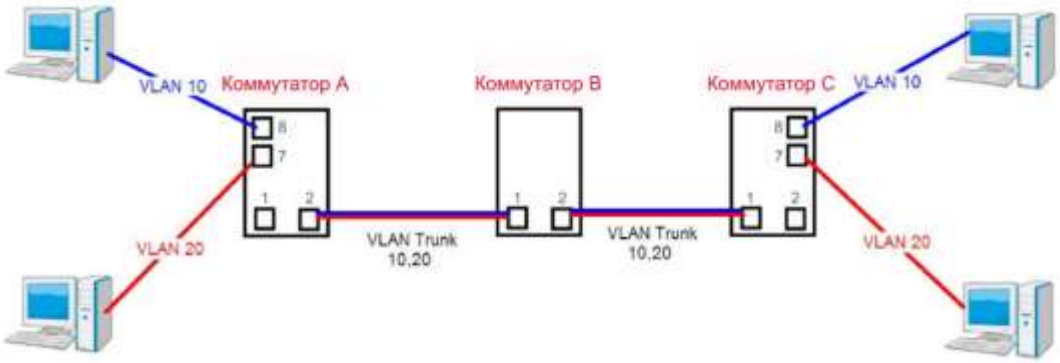


Рисунок 75 – Типовая топология

➢ **Режим доступа (VLAN Access)**

Коммутатор A:

Порт 7 – режим Access = VLAN 20 без тегов

Порт 8 – режим Access = VLAN 10 без тегов

Ниже приведены настройки коммутатора.

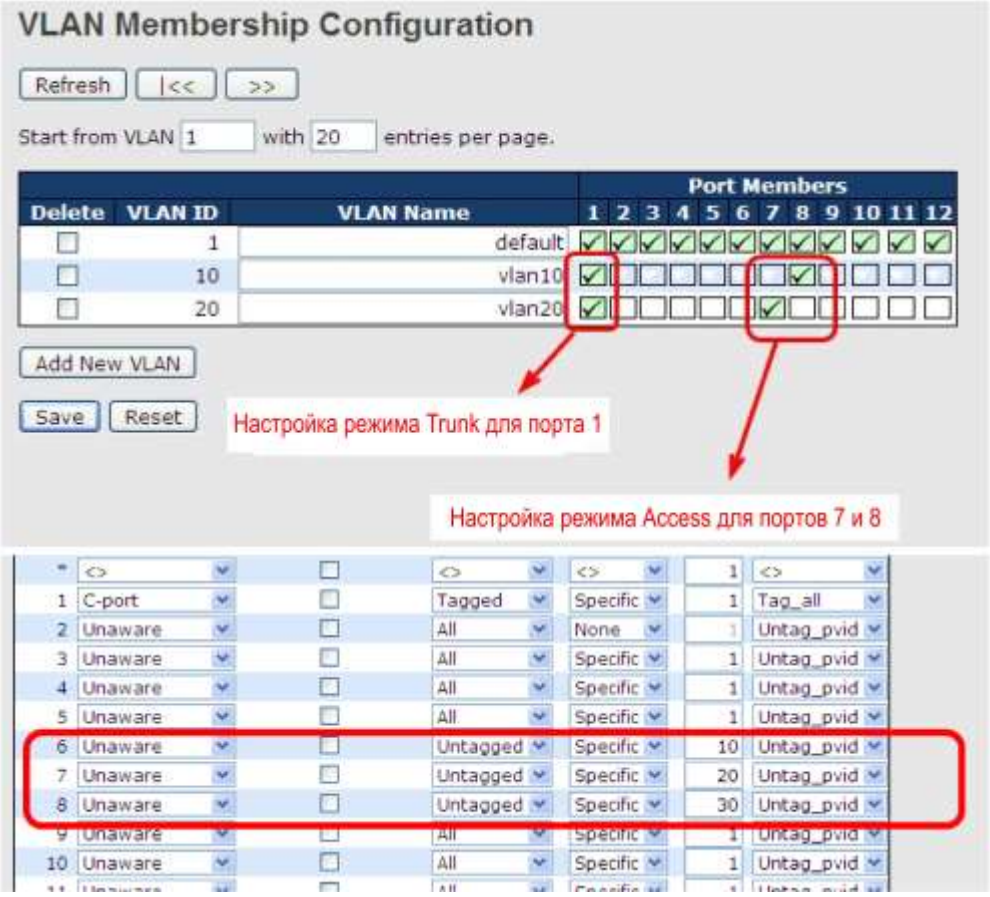


Рисунок 76 – Настройки VLAN на портах доступа

➢ **Магистральный режим (VLAN Trunk)**

Коммутатор B:

Порт 1 = режим Trunk = VLAN 10, 20 с тегами

Порт 2 = режим Trunk 1Qtrunk = VLAN 10, 20 с тегами

Ниже приведены настройки коммутатора.

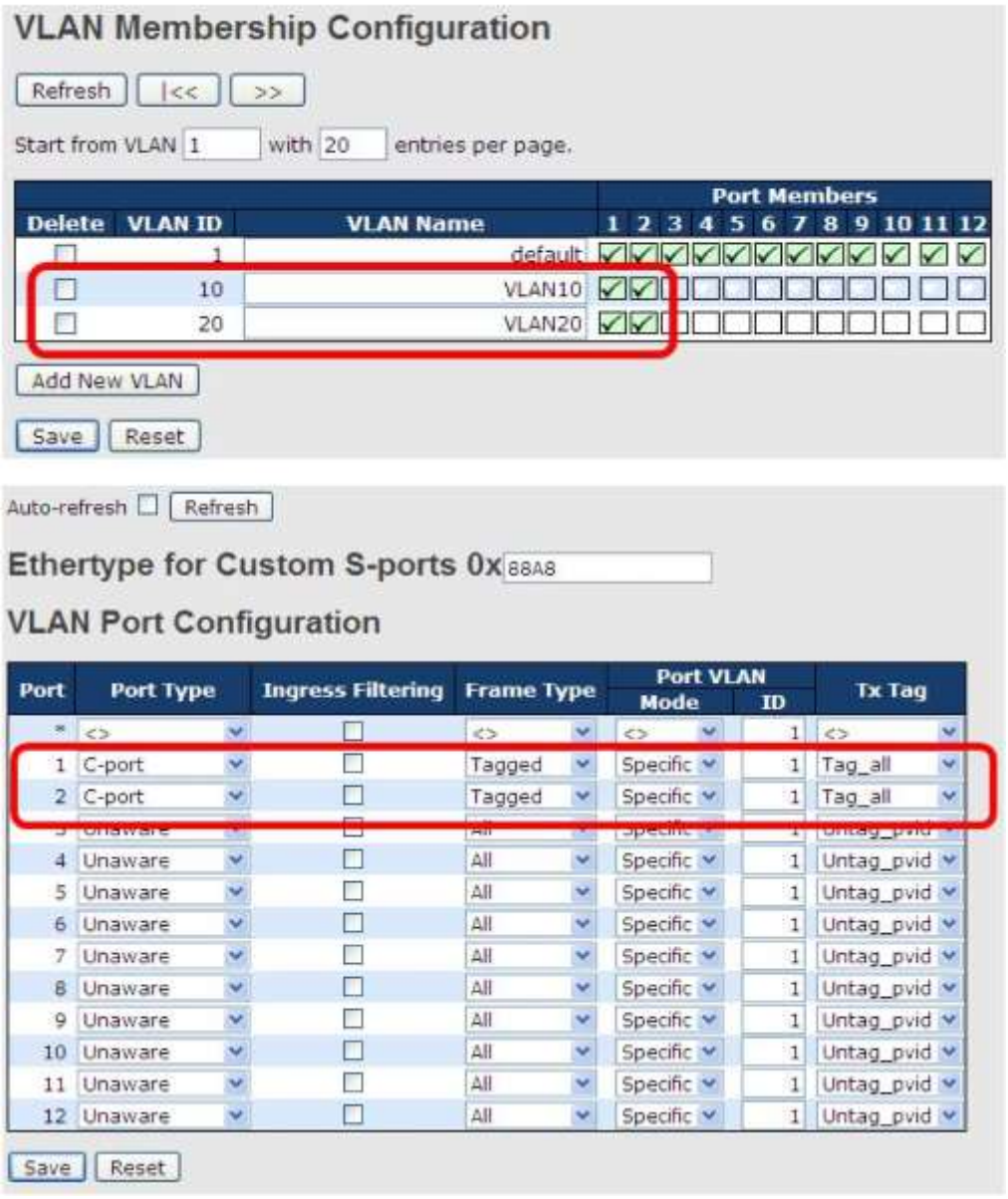


Рисунок 77 – Настройки VLAN на магистральных портах

➢ **Гибридный режим (VLAN Hybrid)**

Порт 1 режим Hybrid = VLAN 10 без тегов; VLAN 10, 20 с тегами

Ниже приведены настройки коммутатора.

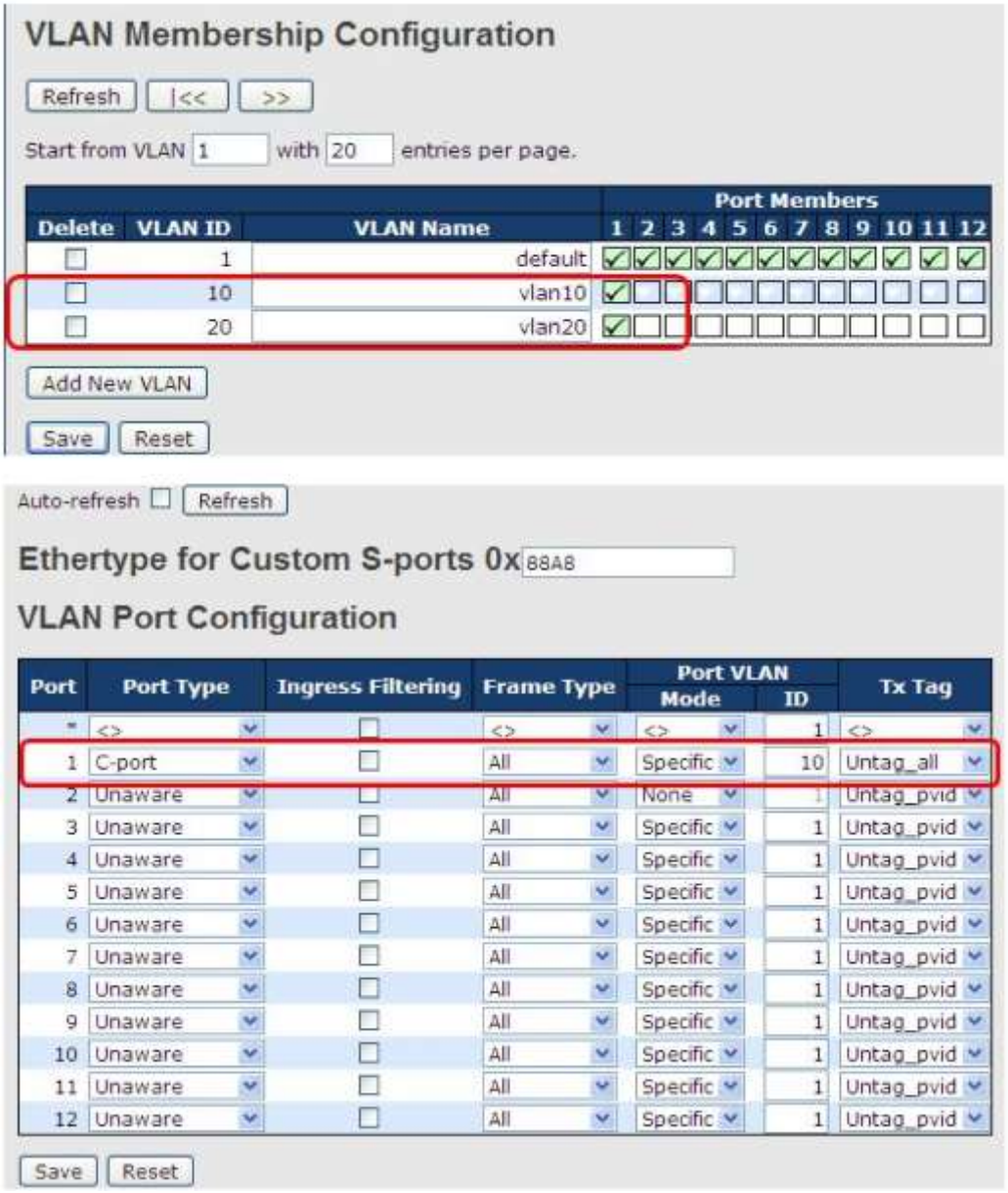


Рисунок 78 – Настройки VLAN на гибридном порту

- **Режим VLAN QinQ**

Режим VLAN QinQ обычно применяется, когда есть неизвестные VLAN, как показано на рисунке 79.

VLAN «X» = неизвестная VLAN

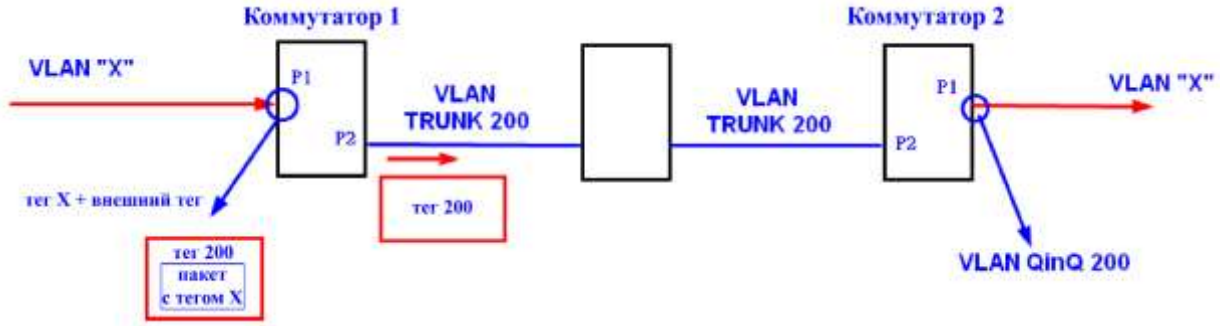


Рисунок 79 – QinQ

Ниже показаны настройки портов на коммутаторе.

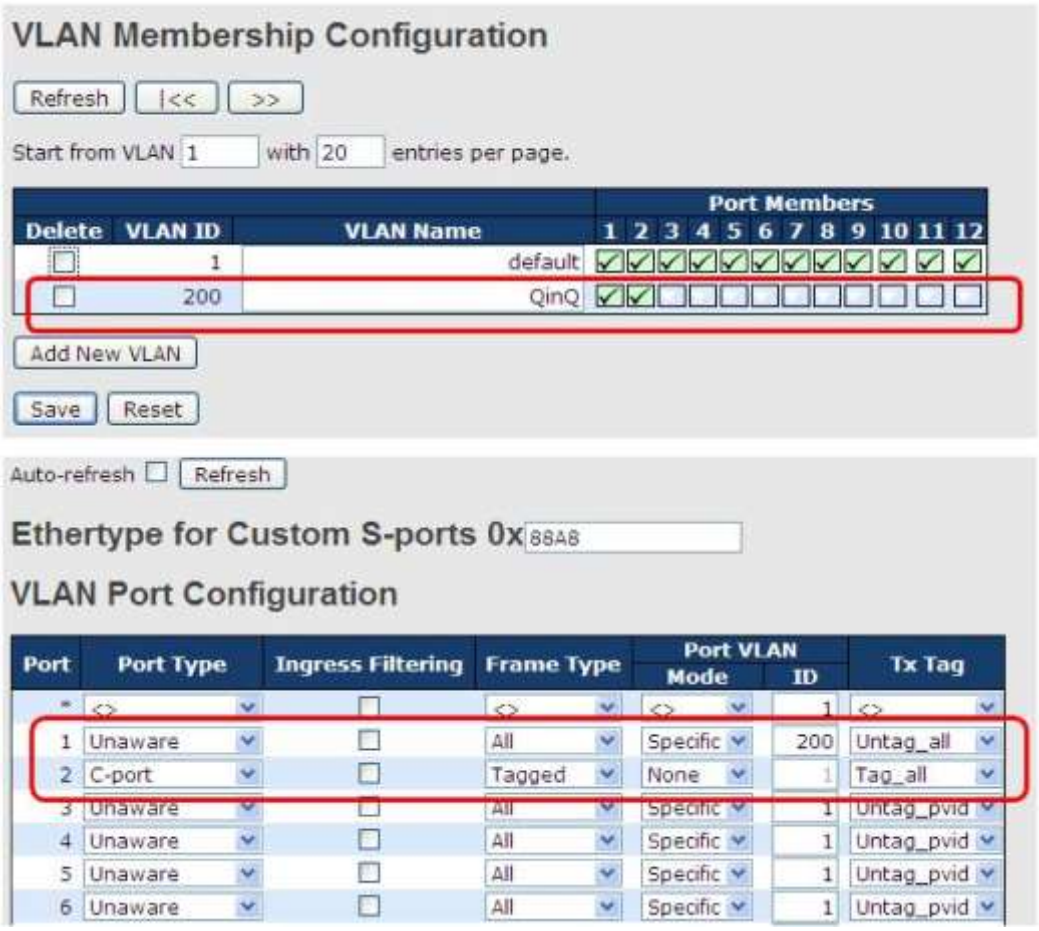


Рисунок 80 – Настройка режима QinQ

➢ **Настройка VLAN ID**

При настройке управляющей VLAN только порт с идентичным ей VLAN ID можно использовать для управления коммутатором.

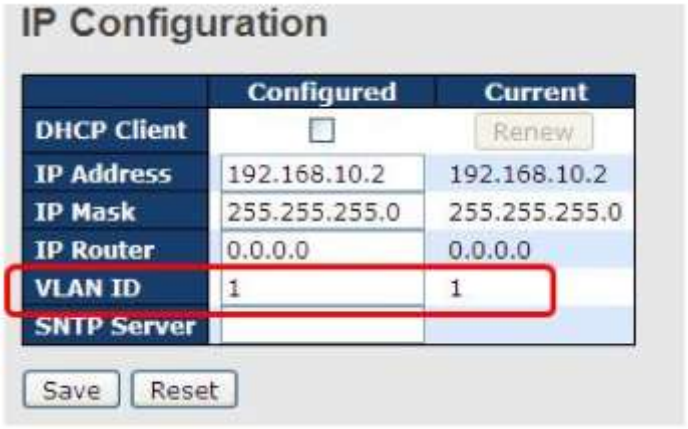


Рисунок 81 – Настройка VLAN ID на порту

5.6.3 Частная VLAN

Частная VLAN (PVLAN) включает порты коммутатора, которые могут взаимодействовать только с заданным «восходящим каналом». Ограниченные таким образом порты называются частными портами. Каждая частная VLAN обычно содержит много частных портов и один восходящий канал. Все полученные на частном порту кадры коммутатор пересылает через порт восходящего канала, независимо от VLAN ID или MAC-адреса назначения. Порт должен быть участником как публичной, так и частной VLAN, чтобы иметь возможность пересылать пакеты. Страница [Private VLAN Membership Configuration] позволяет настраивать для коммутатора членство в частной VLAN. По умолчанию все порты относятся к типу «Unaware» и являются членами VLAN 1 и частной VLAN 1.

- **Участие в PVLAN**

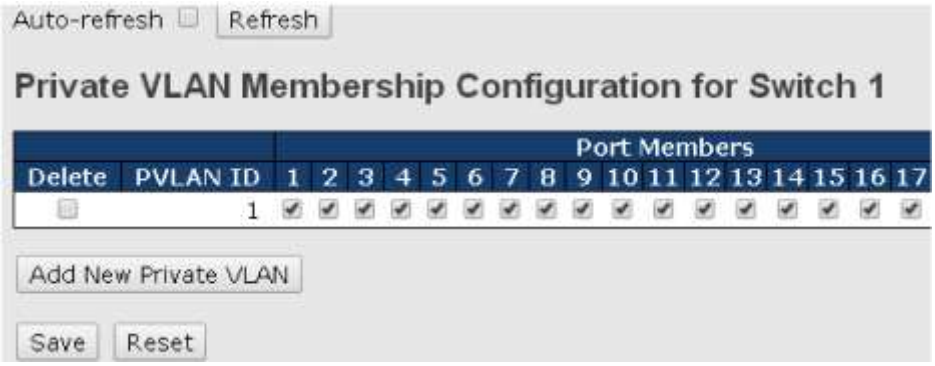


Рисунок 82 – Выбор портов PVLAN

Параметр	Описание
Delete	Отметьте, чтобы удалить запись. Она будет удалена при следующем сохранении

PVLAN ID	Указывает идентификатор выбранной частной VLAN
Port Members	Для каждого PVLAN ID отображается ряд флажков для каждого порта. Вы можете установить флажок, чтобы включить порт в выбранную частную VLAN. Чтобы исключить порт из частной VLAN, убедитесь, что флажок не установлен. По умолчанию ни один порт не является участником PVLAN и флажки не установлены
Save	Нажмите, чтобы сохранить изменения
Reset	Нажмите, чтобы отменить любые изменения, внесенные локально, и вернуться к ранее сохраненным значениям

- **Изоляция портов**

Частная VLAN определяется как сопряжение первичной и вторичной VLAN. Общий порт (promiscuous port) – это порт, который может взаимодействовать со всеми другими типами портов частной VLAN через первичную VLAN и любые связанные вторичные VLAN, тогда как изолированные порты могут взаимодействовать только с общим портом.

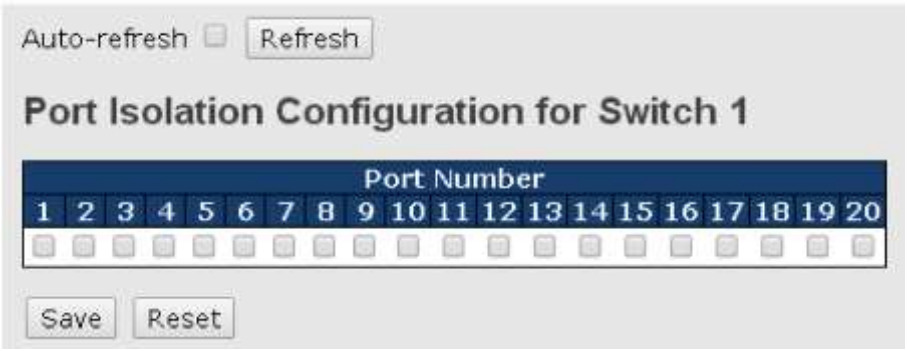


Рисунок 83 – Настройка изолированных портов

Параметр	Описание
Port Number	Для каждого порта частной VLAN предусмотрен флажок. Если флажок установлен, это означает, что функция изоляции для данного порта включена. Если флажок не установлен – изоляция отключена. По умолчанию функция изоляции отключена для всех портов
Save	Нажмите, чтобы сохранить изменения
Reset	Нажмите, чтобы отменить любые изменения, внесенные локально, и вернуться к ранее сохраненным значениям

5.7 SNMP

SNMP (Simple Network Management Protocol) – это протокол управления устройствами в IP-сетях. Он в основном используется системами управления для мониторинга рабочего состояния сетевых устройств. В случае возникновения определенных событий администраторам будут отправлены trap-сообщения и уведомления.

5.7.1 Системные настройки

Страница [SNMP System Configuration] позволяет проводить базовые настройки системы SNMP.

Рисунок 84 – Системные настройки SNMP

Параметр	Описание
Mode	Указывает текущий режим SNMP. Доступны режимы: **Enabled**: включить SNMP **Disabled**: отключить SNMP
Version	Указывает поддерживаемую версию SNMP. Доступны следующие версии: **SNMP v1**: поддерживает SNMP версии 1 **SNMP v2c**: поддерживает SNMP версии 2c **SNMP v3**: поддерживает SNMP версии 3
Read Community	Указывает на строку комьюнити с правами для чтения, чтобы разрешить доступ к агенту SNMP. Допустимая длина строки от 0 до 255, и разрешены только символы ASCII от 33 до 126. Поле актуально только для SNMPv1 и SNMPv2c. SNMPv3 для аутентификации и конфиденциальности использует USM, и каждый пользователь имеет свой собственный профиль безопасности, который определяет его права доступа к информации

Write Community	Указывает на строку комьюнити с правами для чтения и записи, чтобы разрешить доступ к агенту SNMP. Допустимая длина строки от 0 до 255, и разрешены только символы ASCII от 33 до 126. Поле актуально только для SNMPv1 и SNMPv2c. SNMPv3 для аутентификации и конфиденциальности использует USM, и каждый пользователь имеет свой собственный профиль безопасности, который определяет его права доступа к информации
Engine ID	Engine ID – это уникальный идентификатор, используемый в протоколе SNMPv3 для аутентификации и шифрования сообщений между коммутатором и системой управления сетью. Строка должна содержать четное число от 10 до 64 шестнадцатеричных цифр. Нельзя использовать строку, состоящую только из нулей (0000...) или только из символов «F» (FFFF…). Изменение Engine ID приведет к удалению всех локальных пользователей, созданных на коммутаторе

5.7.2 Настройка Trap

Страница [Trap Configuration] позволяет настроить параметры SNMP Trap.

Рисунок 85 – Включение функции и список конфигураций

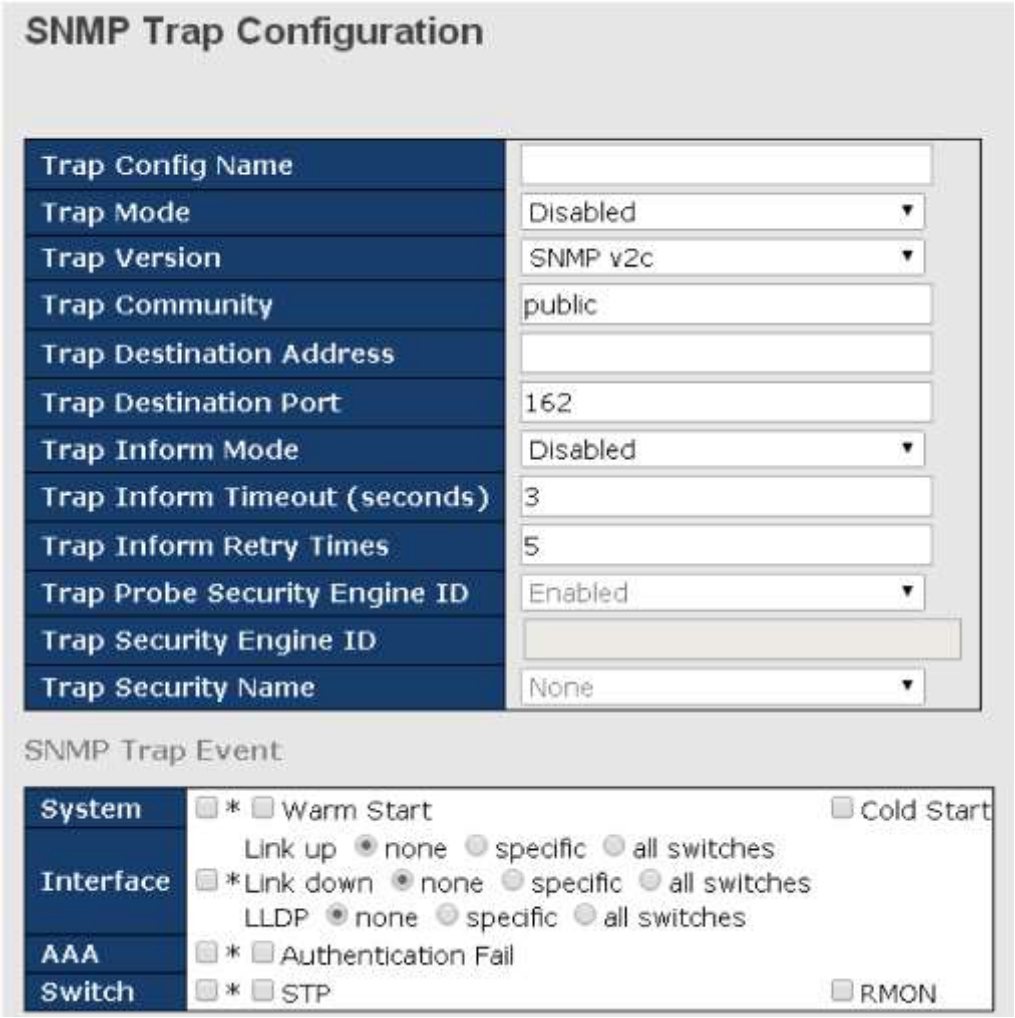


Рисунок 86 – Настройка SNMP-ловушки

Параметр	Описание
Trap Config Name	Имя конфигурации ловушки
Trap Mode	Указывает текущий режим SNMP Trap. Доступны режимы: **Enabled**: включить функцию Trap **Disabled**: отключить функцию Trap
Trap Version	Указывает поддерживаемую версию SNMP Trap. Доступны следующие версии: **SNMP v1**: поддерживает SNMP Trap версии 1 **SNMP v2c**: поддерживает SNMP Trap версии 2c **SNMP v3**: поддерживает SNMP Trap версии 3

Trap Community	Указывает строку доступа комьюнити при отправке пакетов SNMP-ловушек. Допустимая длина строки от 0 до 255, разрешены только символы ASCII от 33 до 126
Trap Destination Address	Указывает адрес назначения trap-сообщений
Trap Destination Port	Это порт назначения функции Trap, используемый для уведомления о событиях. При желании вы можете изменить порт IP, на который следует отправлять trap-сообщения. Это должен быть фактический порт, который прослушивает соответствующий SNMP-хост. Типичный, общеизвестный порт для SNMP-ловушек – 162 (по умолчанию)
Trap Inform Mode	Указывает режим информирования о событиях SNMP Trap. Доступны режимы: **Enabled**: включить режим информирования **Disabled**: отключить режим информирования
Trap Inform Timeout (seconds)	Настраивает тайм-аут информирования о событиях SNMP Trap. Допустимый диапазон от 0 до 2147 секунд
Trap Inform Retry Times	Настраивает количество повторных попыток информирования о событиях SNMP Trap. Допустимый диапазон от 0 до 255 раз
Trap Probe Security Engine ID	Эта функция позволяет коммутатору автоматически обнаруживать идентификатор объекта SNMP Trap или использовать заданный вручную идентификатор. **Enabled**: включить автоматическое обнаружение. Коммутатор сам обнаружит идентификатор безопасности и использует его. **Disabled**: отключить автоматическое обнаружение. Коммутатор будет использовать идентификатор безопасности, который вы указали в поле «Trap Security Engine ID»
Trap Security Engine ID	Указывает уникальный идентификатор, используемый в протоколе SNMPv3 для аутентификации и шифрования сообщений между коммутатором и системой управления сетью. SNMPv3 отправляет trap-сообщения и информацию используя USM, для чего требуется уникальный идентификатор объекта SNMP. Если включена функция «Trap Probe Security Engine ID», 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 нельзя использовать строку, состоящую только из нулей (0000...) или только из символов «F» (FFFF…)

Trap Security Name	Указывает уникальное имя, ассоциированное в модели безопасности с данным объектом SNMP trap. SNMPv3 отправляет trap-сообщения и информацию используя модель USM, для чего требуется уникальное имя
Save	Нажмите, чтобы сохранить изменения
Reset	Нажмите, чтобы отменить любые изменения, внесенные локально, и вернуться к ранее сохраненным значениям

5.7.3 Настройка SNMP-комьюнити

Вы можете определить доступ к данным SNMP на ваших устройствах, создав одно или несколько SNMP-комьюнити. Комьюнити – это группа, к которой принадлежат устройства и станции управления SNMP. Это помогает определить, куда отправляется информация. Устройство, или агент SNMP может принадлежать к нескольким комьюнити. Он не будет отвечать на запросы от станций управления, которые не принадлежат ни к одному из его комьюнити. Эта страница позволяет настроить таблицу комьюнити SNMPv3. Ключевая строка записи указывается в поле «Community».

Рисунок 87 – Настройка SNMP-комьюнити

Параметр	Описание
Delete	Отметьте, чтобы удалить запись. Она будет удалена при следующем сохранении
Community	Указывает ключевую строку комьюнити для разрешения доступа к агенту SNMPv3. Допустимая длина строки от 1 до 32 символов, разрешены только символы ASCII от 33 до 126
Source IP	Указывает адрес источника SNMP
Source Mask	Указывает маску адреса источника SNMP
Save	Нажмите, чтобы сохранить изменения

Reset	Нажмите, чтобы отменить любые изменения, внесенные локально, и вернуться к ранее сохраненным значениям

5.7.4 Настройка пользователя SNMP

Каждый пользователь SNMP имеет свое имя, группу, к которой он принадлежит, пароль аутентификации, протокол аутентификации, протокол конфиденциальности и пароль конфиденциальности. При создании пользователя необходимо связать его с группой SNMP, после чего пользователь наследует модель безопасности группы. Эта страница позволяет настроить таблицу пользователей SNMPv3. Ключами каждой записи являются «Engine ID» и «User Name».

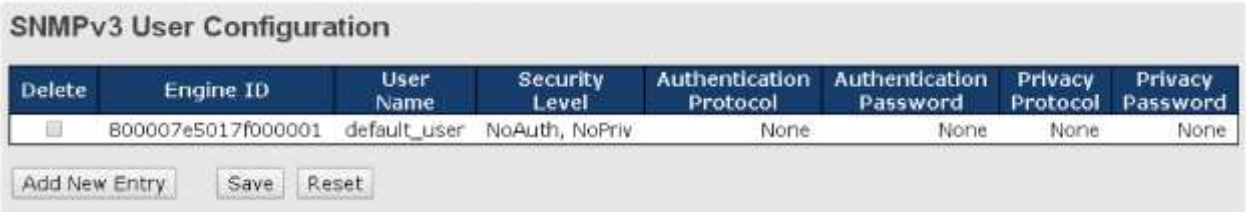


Рисунок 88 – Настройка пользователей

Параметр	Описание
Delete	Отметьте, чтобы удалить запись. Она будет удалена при следующем сохранении
Engine ID	Октетная строка уникального идентификатора объекта SNMP, которому должна принадлежать эта запись. Строка должна содержать четное число от 10 до 64 шестнадцатеричных цифр. Нельзя использовать строку, состоящую только из нулей (0000...) или только из символов «F» (FFFF…). Архитектура SNMPv3 использует модель безопасности на основе пользователя (USM) и модель контроля доступа на основе представлений (VACM). Для USM ключами записи являются **usmUserEngineID** и **usmUserName**. В простом агенте usmUserEngineID всегда является собственным значением snmpEngineID этого агента. Значение также может принимать значение snmpEngineID удаленного объекта SNMP, с которым этот пользователь может взаимодействовать. Другими словами, если Engine ID пользователя совпадает с Engine ID системы, то это локальный пользователь; если не совпадает, то пользователь удаленный
User Name	Строка, идентифицирующая имя пользователя, которому должна принадлежать эта запись. Допустимая длина строки от 1 до 32. Разрешены только символы ASCII от 33 до 126

Security Level	Указывает уровень безопасности, к которой должна относиться эта запись. Доступны следующие уровни безопасности: **NoAuth**, **NoPriv**: без аутентификации и шифрования **Auth**, **NoPriv**: аутентификация без шифрования **Auth**, **Priv**: аутентификация и шифрование Значение уровня безопасности не может быть изменено, если запись уже существует. Таким образом, необходимо сразу установить правильное значение во время создания записи
Authentication Protocol	Указывает протокол аутентификации, к которому должна относиться эта запись. Доступны следующие протоколы аутентификации: **None**: нет протокола аутентификации **MD5**: необязательный флаг, указывающий, что этот пользователь использует протокол MD5 **SHA**: необязательный флаг, указывающий, что этот пользователь использует протокол SHA Значение уровня безопасности не может быть изменено, если запись уже существует. Таким образом, необходимо сразу установить правильное значение во время создания записи
Authentication Password	Строка, идентифицирующая парольную фразу аутентификации. Для протокола аутентификации MD5 допустимая длина строки составляет от 8 до 32. Для протокола аутентификации SHA допустимая длина строки составляет от 8 до 40. Разрешены только символы ASCII от 33 до 126
Privacy Protocol	Указывает протокол шифрования, к которому должна относиться эта запись. Возможные значения включают: **None**: нет протокола шифрования **DES**: необязательный флаг, указывающий, что этот пользователь использует протокол DES
Privacy Password	Строка, идентифицирующая парольную фразу, используемую для шифрования данных. Допустимая длина строки от 8 до 32, разрешены только символы ASCII от 33 до 126
Add New Entry	Нажмите, чтобы добавить новую запись
Save	Нажмите, чтобы сохранить изменения
Reset	Нажмите, чтобы отменить любые изменения, внесенные локально, и вернуться к ранее сохраненным значениям

5.7.5 Настройка групп SNMP

Группа SNMP – это политика управления доступом, необходимая для добавления пользователей. Каждая группа настроена с моделью безопасности и связана с представлением SNMP. Пользователь в группе SNMP должен соответствовать модели безопасности группы. Эти параметры определяют, какой тип аутентификации и конфиденциальности использует пользователь. Каждая пара «имя группы – модель безопасности» должна быть уникальной. Страница [SNMPv3 Group Configuration] позволяет вам настроить таблицу групп SNMPv3. Ключами записей являются «Security Model» и «Security Name».

Рисунок 89 – Настройка групп SNMP

Параметр	Описание
Delete	Отметьте, чтобы удалить запись. Она будет удалена при следующем сохранении
Security Model	Указывает модель безопасности, к которой должна относиться эта запись. Доступны следующие модели безопасности: **v1**: зарезервировано для SNMPv1 **v2c**: зарезервировано для SNMPv2c **usm**: модель безопасности на основе пользователя (USM)
Security Name	Имя, связанное с пользователем SNMP в модели безопасности SNMPv3. Оно используется для идентификации пользователя и определения его прав доступа. Имя безопасности обычно совпадает с именем пользователя, но может быть и другим. Допустимая длина строки от 1 до 32. Разрешены только символы ASCII от 33 до 126

Group Name	Строка, идентифицирующая имя группы, которой должна принадлежать эта запись. Допустимая длина строки от 1 до 32. Разрешены только символы ASCII от 33 до 126
Add New Entry	Нажмите, чтобы добавить новую запись
Save	Нажмите, чтобы сохранить изменения
Reset	Нажмите, чтобы отменить любые изменения, внесенные локально, и вернуться к ранее сохраненным значениям

5.7.6 Настройка представлений SNMP

Таблица представлений SNMPv3 определяет требования доступа к объектам MIB для представлений с различными именами. Вы можете указать конкретные области MIB, к которым можно получить или запретить доступ на основе записей, или создать и удалить записи в таблице представлений на странице [SNMPv3 View Configurations]. Ключами для записей являются строки в полях «View Name» и «OID Subtree».

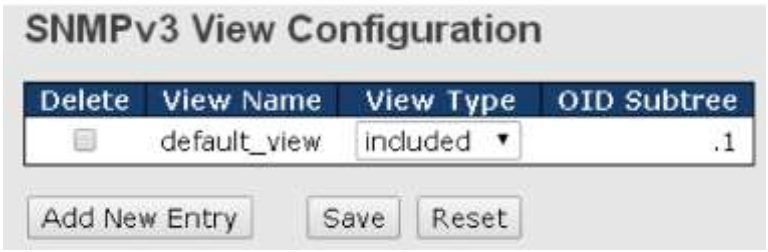


Рисунок 90 – Настройка представлений

Параметр	Описание
Delete	Отметьте, чтобы удалить запись. Она будет удалена при следующем сохранении
View Name	Строка, идентифицирующая имя представления, которому должна принадлежать эта запись. Допустимая длина строки от 1 до 32. Разрешены только символы ASCII от 33 до 126
View Type	Указывает тип представления, к которому относится эта запись. Доступны следующие типы представлений: **Included**: необязательный флаг, указывающий, что это поддерево представлений должно быть включено **Excluded**: необязательный флаг, указывающий, что это поддерево представлений должно быть исключено

	Как правило, если тип представления записи «Excluded», должна существовать другая запись, тип представления которой «Included», и ее поддерево OID выходит за пределы записи типа «Excluded»
OID Subtree	OID, определяющий корень поддерева для добавления к представлению с соответствующим именем. Допустимая длина OID от 1 до 128. Допустимое содержимое строки – цифровое число или звездочка (*)
Add New Entry	Нажмите, чтобы добавить новую запись
Save	Нажмите, чтобы сохранить изменения
Reset	Нажмите, чтобы отменить любые изменения, внесенные локально, и вернуться к ранее сохраненным значениям

5.7.7 Настройка доступа SNMP

Страница [SNMPv3 Access Configuration] позволяет вам настроить таблицу доступа SNMPv3. Ключами записи являются «Group Name», «Security Model», and «Security Level».

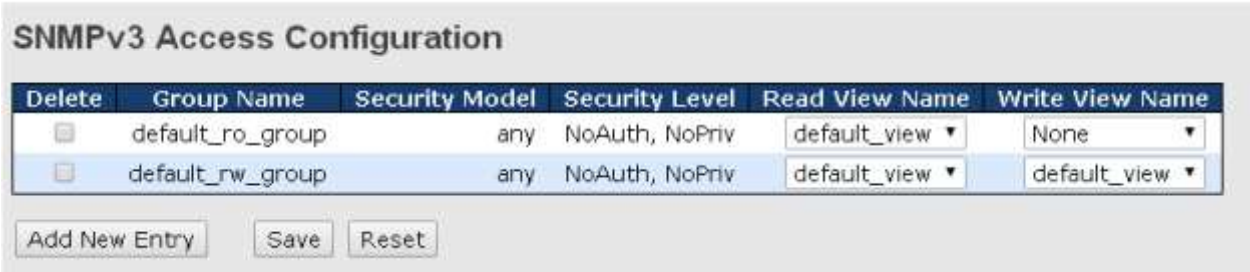


Рисунок 91 – Настройка доступа

Параметр	Описание
Delete	Отметьте, чтобы удалить запись. Она будет удалена при следующем сохранении
Group Name	Строка, идентифицирующая имя группы, которой должна принадлежать эта запись. Допустимая длина строки от 1 до 32. Разрешены только символы ASCII от 33 до 126
Security Model	Указывает модель безопасности, к которой должна относиться эта запись. Доступны следующие модели безопасности: **any**: принимаются любые модели безопасности (v1|v2c|usm) **v1**: зарезервировано для SNMPv1

	v2c: зарезервировано для SNMPv2c **usm**: модель безопасности на основе пользователя (USM)
Security Level	Указывает уровень безопасности, к которой должна относиться эта запись. Доступны следующие уровни безопасности: **NoAuth**, **NoPriv**: без аутентификации и шифрования **Auth**, **NoPriv**: аутентификация без шифрования **Auth**, **Priv**: аутентификация и шифрование
Read View Name	Имя представления, которое используется для чтения информации из базы данных MIB Допустимая длина строки составляет от 1 до 32. Разрешены только символы ASCII от 33 до 126
Write View Name	Имя представления, которое используется для записи информации в базу данных MIB. Допустимая длина строки составляет от 1 до 32. Разрешены только символы ASCII от 33 до 126
Add New Entry	Нажмите, чтобы добавить новую запись
Save	Нажмите, чтобы сохранить изменения
Reset	Нажмите, чтобы отменить любые изменения, внесенные локально, и вернуться к ранее сохраненным значениям

5.8 Настройка приоритета трафика

5.8.1 Контроль штормов

Сетевой шторм происходит, когда пакеты заполняют LAN, создавая избыточный трафик и ухудшая производительность сети. Ошибки в реализации стека протоколов, ошибки в конфигурации сети или пользователи, инициирующие атаку типа «отказ в обслуживании», могут вызвать шторм. Функция контроля скорости прохождения пакетов (Storm Control) предотвращает прерывание трафика в сети широковещательным, многоадресным или одноадресным штормом на порту. На этой странице вы можете указать скорость, с которой принимаются пакеты для одноадресного, многоадресного и широковещательного трафика. Единицей скорости может быть pps (пакетов в секунду) или kpps (килопакетов в секунду).

Скорость отправки кадров на ЦП коммутатора всегда ограничена приблизительно 4 kpps. Например, широковещательные рассылки в управляющей VLAN ограничены этой скоростью. Управляющая VLAN настраивается на странице настройки IP.

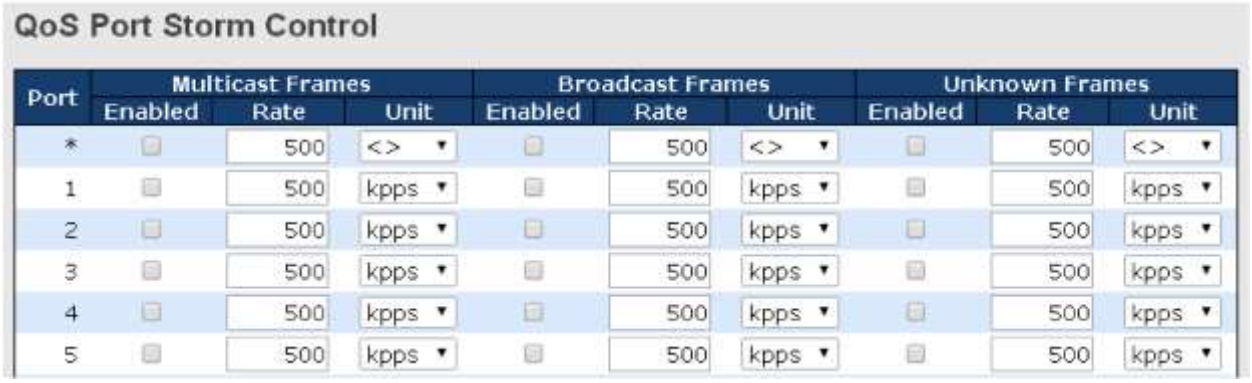


Рисунок 92 – Настройка контроля штормов

Параметр	Описание
Port	Номер порта коммутатора, к которому будут применены следующие настройки
Multicast / Broadcast / Unknown Frames	Типы кадров, поддерживаемые функцией Storm Control, включая многоадресные, широковещательные и неизвестные одноадресные пакеты
Enabled	Включает или отключает контроль выбранного типа кадров
Rate	Значение скорости прохождения кадров
Unit	Единица измерения: pps (пакетов в секунду), kpps (килопакетов в секунду) 1 kpps на самом деле равен 1002,1 pps

5.8.2 Классификация портов

QoS (качество обслуживания) – это метод достижения эффективного использования полосы пропускания между устройствами путем назначения приоритетов кадрам в соответствии с индивидуальными требованиями и передачи кадров на основе их важности. Кадры в очередях с более высоким приоритетом получают бóльшую часть полосы пропускания, чем кадры в очереди с более низким приоритетом.

Рисунок 93 – Классификация QoS для входящего трафика

Параметр	Описание
Port	Номер порта коммутатора, к которому будут применены следующие настройки
QoS Class	Управляет классом QoS по умолчанию Все кадры классифицируются по классу QoS. Существует соответствие один к одному между классом QoS, очередью и приоритетом. Класс QoS 0 (ноль) имеет самый низкий приоритет Если порт поддерживает VLAN и кадр маркирован, то кадр классифицируется по классу QoS, который основан на значении PCP в теге, как показано ниже. В противном случае кадр классифицируется согласно классу QoS по умолчанию PCP: 0 1 2 3 4 5 6 7 QoS: 1 0 2 3 4 5 6 7 Если порт поддерживает VLAN, кадр маркирован и включен Tag Class, то кадр классифицируется по классу QoS, который сопоставляется со значением PCP и DEI в теге. В противном случае кадр классифицируется согласно классу QoS по умолчанию Класс QoS, назначенный классификатором, может быть переопределен записью в таблице QCL (см. раздел 5.8.12). Обратите внимание: если класс QoS по умолчанию был изменен динамически, то фактический класс по умолчанию будет отображаться в скобках после изначально настроенного класса по умолчанию
DP level	Управляет уровнем приоритета сброса по умолчанию Все кадры классифицируются по уровню DP. Если порт поддерживает VLAN и кадр маркирован, то кадр классифицируется по уровню DP, который равен значению DEI в теге. В противном случае кадр классифицируется согласно уровню DP по умолчанию

	Уровень DP, назначенный классификатором, может быть переопределен записью в таблице QCL
PCP	Управляет значением PCP (приоритет кадра) по умолчанию Все кадры классифицируются по значению PCP. Если порт поддерживает VLAN и кадр маркирован, то кадр классифицируется по значению PCP в теге. В противном случае кадр классифицируется согласно значению PCP по умолчанию
DEI	Управляет значением DEI по умолчанию Все кадры классифицируются по значению DEI, которое указывает, может ли кадр быть отброшен в случае перегрузки сети. Если порт поддерживает VLAN и кадр маркирован, то кадр классифицируется по значению DEI в теге. В противном случае кадр классифицируется согласно значению DEI по умолчанию
Tag Class	Показывает режим классификации для тегированных кадров на этом порту **Disabled**: использовать для тегированных кадров класс QoS по умолчанию и уровень DP **Enabled**: использовать для тегированных кадров сопоставленные значения PCP и DEI Обратите внимание: этот параметр не действует, если порт не поддерживает VLAN. Маркированные кадры, полученные на портах, не поддерживающих VLAN, всегда классифицируются согласно классу QoS по умолчанию и уровню DP
DSCP Based	Нажмите, чтобы включить классификацию входных портов QoS на основе DSCP

5.8.3 Перемаркировка трафика

Вы можете установить исходящие очереди QoS на порту, например, классифицировать данные и маркировать их в соответствии с их приоритетом и политиками. Затем пакеты будут проходить по внутренним путям коммутатора, неся назначенные им маркеры тега QoS. На выходном порту эти маркеры считываются и используются для определения, в какую очередь пересылается каждый пакет данных. Если трафик не соответствует условиям, установленным командой **policer**, вы можете перемаркировать трафик.

Рисунок 94 – Перемаркировка трафика для выходных портов

Параметр	Описание
Port	Номер порта коммутатора, к которому будут применены следующие настройки. Нажмите на номер порта, чтобы настроить перемаркировку
Mode	Показывает режим перемаркировки тегов для этого порта: **Classified**: использовать классифицированные значения PCP/DEI **Default**: использовать значения PCP/DEI по умолчанию **Mapped**: использовать сопоставление класса QoS и уровня DP

5.8.4 DSCP порта QoS

DSCP (Differentiated Services Code Point) – это код в поле DS заголовка IP, который в пределах данного DS-домена характеризует конкретный класс сервиса, необходимый пакету и его приоритет отбрасывания. QoS может классифицировать пакеты данных, используя 6-битное поле DS, чтобы по-разному и эффективно управлять каждым классом трафика, тем самым достигая оптимизированного использования пропускной способности сети. Маршрутизаторы с поддержкой DSCP в сети будут считывать значение DSCP пакета данных и перед передачей помещать пакет в очереди с разным приоритетом и эффективностью передачи. Эта функция помогает обеспечить низкую задержку для критического трафика. Страница [QoS port DSCP Configuration] позволяет вам настраивать параметры DSCP для каждого порта.

Рисунок 95 – Настройка DSCP для портов

Параметр	Описание
Port	Показывает список портов, для которых можно настроить параметры DSCP входящего и исходящего трафика
Ingress	В настройках «Ingress» вы можете изменить настройки преобразования и классификации входящего трафика для отдельных портов Доступны следующие параметры конфигурации: **Translate**: отметьте, чтобы включить функцию преобразования меток DSCP **Classify**: включает четыре значения: **Disable**: нет классификации DSCP входящего трафика **DSCP=0**: классифицировать, если входящий (или преобразованный, когда «Translate» включен) DSCP равен 0 **Selected**: будут классифицироваться только те пакеты, для которых конкретные значения DSCP были настроены в окне преобразования DSCP **All**: классифицироваться будут все входящие пакеты, независимо от их DSCP
Egress	Функция перезаписи (**Rewrite**) на выходном порту может быть настроена с использованием следующих параметров: **Disable**: перезапись исходящего трафика отключена **Enable**: перезапись включена, но без изменения значений **Remap DP Unaware**: переназначение без учета уровня DP. DSCP из анализатора переназначается, и кадр перезаписывается новым значением DSCP. Значение DSCP всегда берется из таблицы [DSCP Translation] → [Egress Remap DP0] **Remap DP Aware**: переназначение с учетом уровня DP. DSCP из анализатора переназначается, и кадр перезаписывается новым значением DSCP. В зависимости от уровня DP кадра, значение DSCP берется либо из таблицы [DSCP Translation] → [Egress Remap DP0], либо из таблицы [DSCP Translation → [Egress Remap DP1]

5.8.5 Контроль скорости трафика (Port Policing)

Полисинг – это механизм регулирования трафика, ограничивающий его скорость для управления передачей или приемом данных на интерфейсе. Если скорость трафика

превышает настроенное максимальное значение, механизм контроля скорости либо отбрасывает избыточный трафик, либо изменяет его метки. На этой странице вы можете настроить полисеры (ограничители скорости трафика) для всех портов коммутатора

Рисунок 96 – Контроль скорости входящего трафика

Параметр	Описание
Port	Номер порта коммутатора, к которому будут применены следующие настройки.
Enabled	Установите флажок, чтобы включить ограничитель для отдельных портов коммутатора
Rate	Настраивает значение скорости для каждого полисера. Значение по умолчанию – 500. Диапазон от 100 до 1000000, когда единица измерения kbps и fps; или от 1 до 3300, когда единица измерения Mbps и kfps
Unit	Настраивает единицу измерения скорости для каждого полисера как kbps (кбит/с), Mbps (Мбит/с), fps (кадр/с) или kfps (килокадр/с). Значение по умолчанию – kbps

5.8.6 Управление очередями

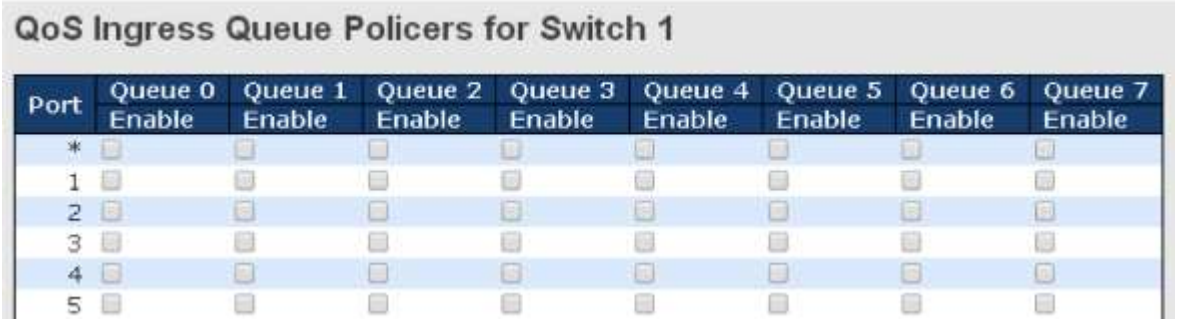
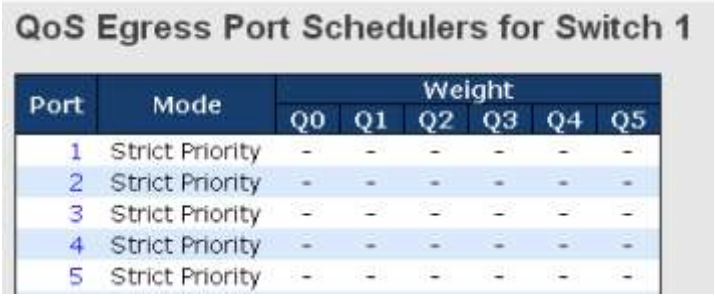


Рисунок 97 – Контроль скорости трафика входящих очередей

Параметр	Описание
Port	Номер порта коммутатора, к которому будут применены следующие настройки
Enabled	Установите флажок, чтобы включить ограничитель для отдельных входящих очередей
Rate	Настраивает значение скорости для каждого полисера. Значение по умолчанию – 500. Диапазон от 100 до 1000000, когда единица измерения kbps и от 1 до 3300, когда единица измерения Mbps. Это поле отображается только в том случае, если включен хотя бы один из ограничителей очереди
Unit	Настраивает единицу измерения скорости для каждого полисера как kbps или Mbps. Значение по умолчанию – kbps. Это поле отображается только в том случае, если включен хотя бы один из ограничителей очереди

5.8.7 Планировщик портов

Планирование на портах коммутатора может решить проблему снижения производительности во время перегрузок сети. Планировщики позволяют коммутаторам поддерживать отдельные очереди для пакетов из каждого источника и не допускать использования всей полосы пропускания определенным трафиком. Эта страница позволяет вам настраивать планировщик и шейперы для отдельных 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	-	-	-	-	-	-

Рисунок 98 – Планировщики выходных портов QoS

5.8.7.1 Планировщик и шейперы выходного порта QoS

- **Строгий приоритет**

Строгий приоритет (SP) использует очереди, основанные только на приоритете. Когда трафик поступает на устройство, данные из очереди с наивысшим приоритетом будут переданы первыми. За ними следуют данные с более низкими приоритетами. Если в очереди с наивысшим приоритетом постоянно есть какой-то контент, то другие пакеты в

остальных очередях не будут отправлены, пока очередь с наивысшим приоритетом не опустеет. Алгоритм SP предпочтителен, когда полученные пакеты содержат высокоприоритетные данные, такие как голос и видео.

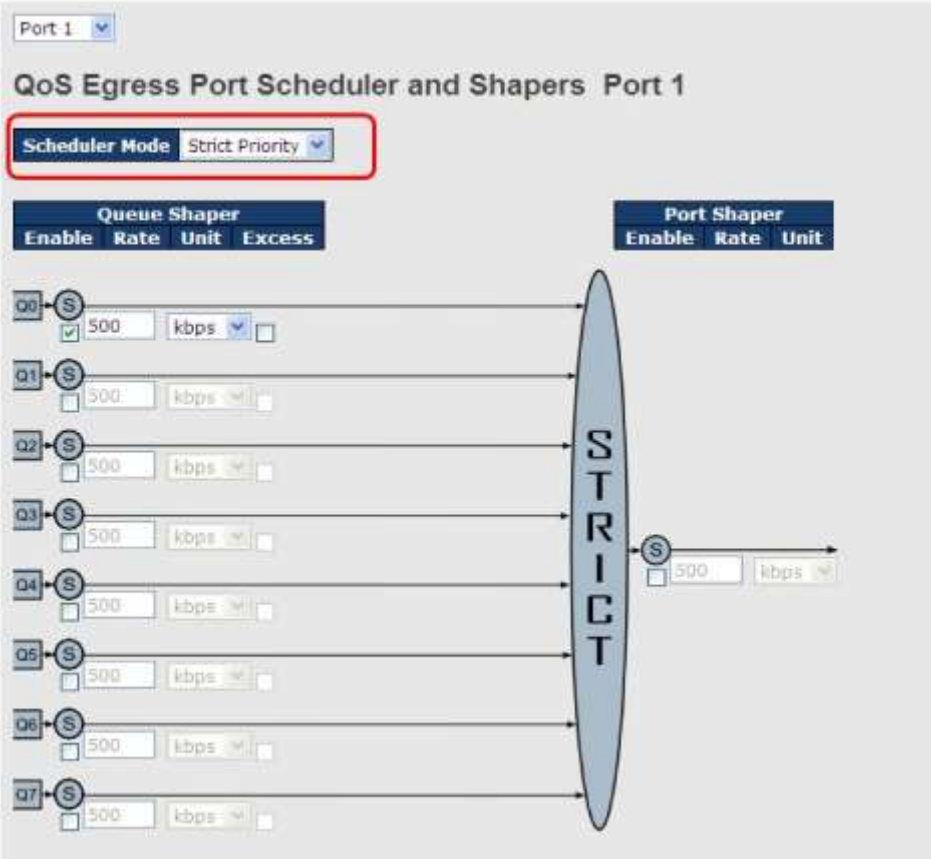


Рисунок 99 – Режим строгого приоритета

Параметр	Описание
Scheduler Mode	Режим планирования. Доступны два режима: **Strict Priority** (строгий приоритет) или **Weighted** (взвешенный)
Queue Shaper Enable	Установите флажок, чтобы включить шейпер для отдельных очередей
Queue Shaper Rate	Настраивает значение скорости для каждого шейпера очереди. Значение по умолчанию – 500. Диапазон от 100 до 1000000, когда единица измерения kbps и от 1 до 3300, когда единица измерения Mbps
Queue Shaper Unit	Настраивает единицу измерения скорости для каждого шейпера очереди как kbps или Mbps. Значение по умолчанию – kbps

Queue Shaper Excess	Позволяет очереди использовать избыточную пропускную способность
Port Shaper Enable	Установите флажок, чтобы включить шейпер для выбранного порта коммутатора
Port Shaper Rate	Настраивает значение скорости для шейпера порта. Значение по умолчанию – 500. Диапазон от 100 до 1000000, когда единица измерения kbps и от 1 до 3300, когда единица измерения Mbps
Port Shaper Unit	Настраивает единицу измерения скорости для шейпера порта как kbps или Mbps. Значение по умолчанию – kbps

- **Взвешенный режим**

Взвешенное планирование будет доставлять трафик на основе ротации. При перегрузке трафика такой режим позволяет гарантировать минимальную полосу пропускания каждой очереди на основе ее настроенного веса. Этот режим активируется только тогда, когда порт получает больше трафика, чем он способен обработать. Очереди предоставляется объем пропускной способности независимо от остального входящего трафика на этом порту. Очередь с бóльшим весом будет иметь более широкую гарантированную полосу пропускания, чем другие очереди с меньшим весом.

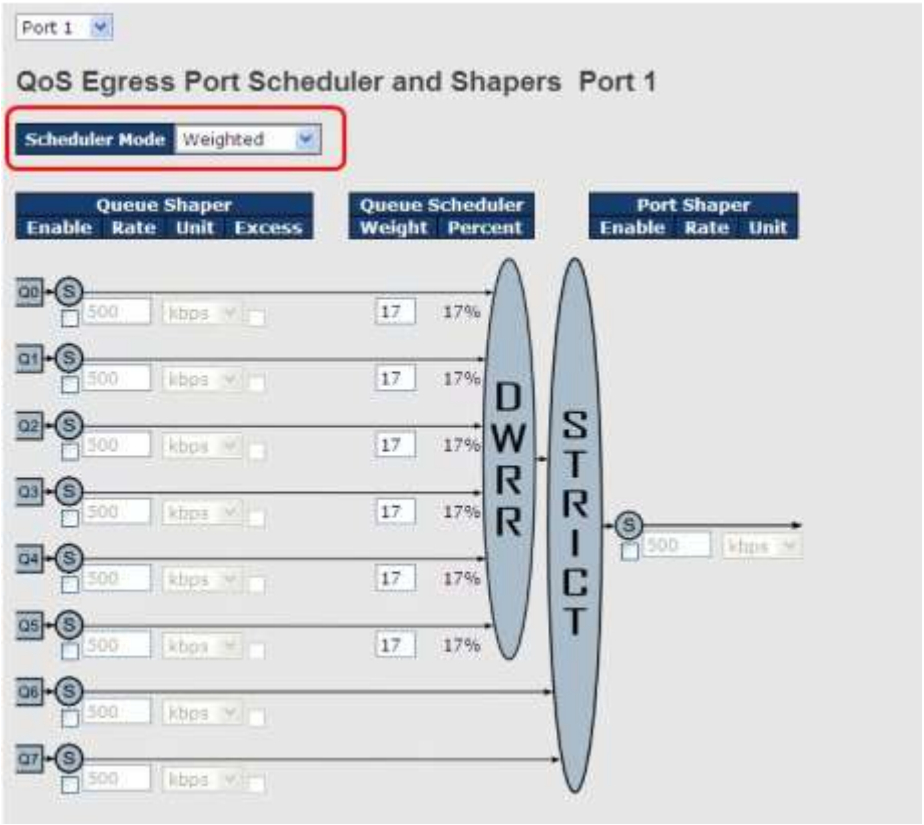


Рисунок 100 – Взвешенный режим

Параметр	Описание
Scheduler Mode	Режим планирования. Доступны два режима: **Strict Priority** (строгий приоритет) или **Weighted** (взвешенный)
Queue Shaper Enable	Установите флажок, чтобы включить шейпер для отдельных очередей
Queue Shaper Rate	Настраивает значение скорости для каждого шейпера очереди. Значение по умолчанию – 500. Диапазон от 100 до 1000000, когда единица измерения kbps и от 1 до 3300, когда единица измерения Mbps
Queue Shaper Unit	Настраивает единицу измерения скорости для каждого шейпера очереди как kbps или Mbps. Значение по умолчанию – kbps
Queue Shaper Excess	Позволяет очереди использовать избыточную пропускную способность
Queue Scheduler Weight	Настраивает вес каждой очереди. Значение по умолчанию – 17. Допустимый диапазон от 1 до 100. Этот параметр отображается только в том случае, если для «Scheduler Mode» выбрано значение «Weighted»
Queue Scheduler Percent	Показывает вес очереди в процентах. Этот параметр отображается только в том случае, если для «Scheduler Mode» выбрано значение «Weighted»
Port Shaper Enable	Установите флажок, чтобы включить шейпер для выбранного порта коммутатора
Port Shaper Rate	Настраивает значение скорости для шейпера порта. Значение по умолчанию – 500. Диапазон от 100 до 1000000, когда единица измерения kbps и от 1 до 3300, когда единица измерения Mbps
Port Shaper Unit	Настраивает единицу измерения скорости для шейпера порта как kbps или Mbps. Значение по умолчанию – kbps

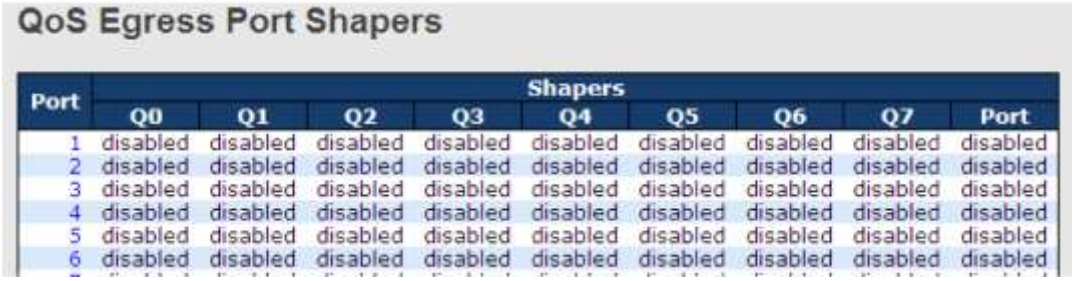
5.8.8 Контроль скорости трафика (Port Shaping)

Ограничение трафика на порту при помощи шейпинга (Port Shaping) позволяет управлять объемом трафика, проходящего через порт, путем установки максимальной скорости передачи данных, которая ниже пропускной способности интерфейса. С помощью

шейпинга можно сформировать общий трафик через интерфейс до заданной скорости, что позволяет избежать перегрузок и потерь данных.

При настройке шейперов (ограничителей) вы указываете максимальное допустимое количество трафика для данного интерфейса. Эта величина должна быть меньше, чем максимальная пропускная способность настраиваемого интерфейса.

В отличие от полисинга (см. раздел 5.8.5), когда избыточный трафик, превышающий установленный лимит, либо отбрасывается, либо его метки изменяются, шейпинг буферизует избыточный трафик и отправляет его позже, что позволяет смягчить кратковременные пики нагрузки.



Параметр	Описание
Port	Номер порта коммутатора, к которому будут применены следующие настройки. Нажмите номер порта, чтобы настроить шейперы
Q0 – Q7	Номер очереди. Показывает «disabled», если шейпер отключен или отображает заданное ограничение максимальной скорости очереди, например «800 Mbps»

5.8.9 QoS на основе DSCP

Страница [DSCP-based QoS] позволяет настроить параметры классификации QoS входящего трафика на основе DSCP для всех портов.

Рисунок 101 – Глобальная настройка классификации QoS на основе DSCP

Параметр	Описание
DSCP	Максимальное количество поддерживаемых значений DSCP – 64. Допустимые значения находятся в диапазоне от 0 до 63
Trust	Установите флажок, чтобы доверять определенному значению DSCP. Только кадры с доверенными значениями DSCP сопоставляются с определенным классом QoS и уровнем DP. Кадры с недоверенными значениями DSCP рассматриваются как не являющиеся кадрами IP
QoS Class	Значение класса QoS. Может быть любым числом от 0 до 7
DPL	Уровень приоритета сброса (0–1)

5.8.10 Преобразование DSCP

Страница [DSCP Translation] позволяет вам настроить основные параметры преобразования DSCP для всех портов коммутатора. Преобразование может применяться к входящему и исходящему трафику.

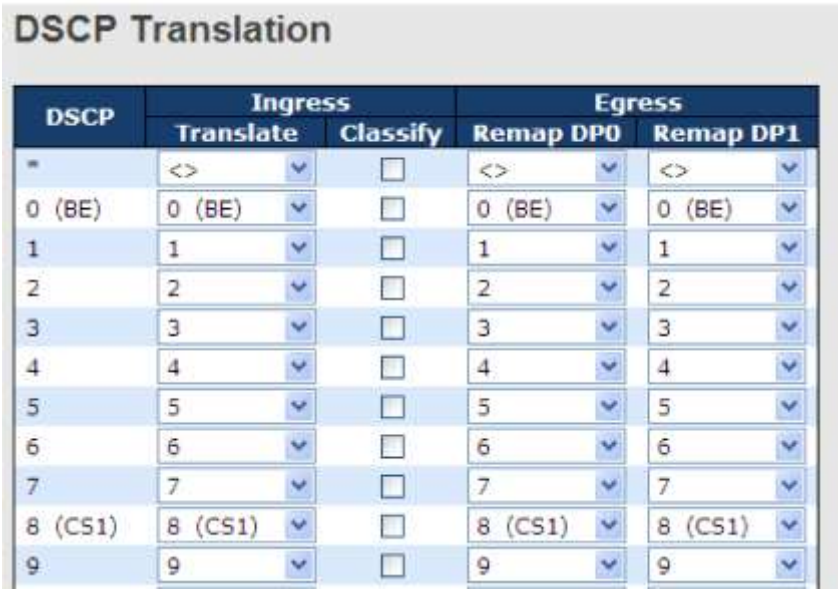


Рисунок 102 – Глобальная настройка преобразования DSCP

Параметр	Описание
DSCP	Максимальное количество поддерживаемых значений DSCP – 64. Допустимые значения находятся в диапазоне от 0 до 63

Ingress	Когда пакеты данных поступают в сеть через коммутатор, их значение DSCP может быть сначала преобразовано в новое значение. Новое значение затем используется для определения класса обслуживания (QoS Class) и уровня приоритета сброса (DPL) этих данных. Для преобразования DSCP есть два параметра конфигурации: 1. **Translate**: включает преобразование значений DSCP входящего трафика на основе указанного метода классификации. DSCP может быть преобразован в любое из допустимых значений (0–63) 2. **Classify**: включает классификацию на входной стороне при помощи метода, определенного в таблице конфигурации QoS порта
Egress	Настраиваемые параметры на выходе включают: **Remap DP0**: повторно сопоставляет поле DP0 с выбранным значением DSCP. DP0 указывает низкий приоритет сброса. Вы можете выбрать из всплывающего меню значение, на которое хотите переназначить DSCP. Значение DSCP находится в диапазоне от 0 до 63 **Remap DP1**: повторно сопоставляет поле DP1 с выбранным значением DSCP. DP1 указывает высокий приоритет сброса. Вы можете выбрать из всплывающего меню значение, на которое хотите переназначить DSCP. Значение DSCP находится в диапазоне от 0 до 63

5.8.11 Классификация DSCP

Страница [DSCP Classification] позволяет настроить сопоставление класса QoS и уровня приоритета сброса со значением DSCP.

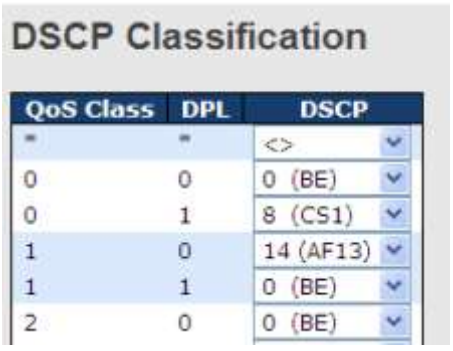


Рисунок 103 – Классификация DSCP

Параметр	Описание
QoS Class	Фактический класс QoS
DPL	Фактический уровень приоритета сброса

DSCP	Выберите классифицированное значение DSCP (0-63)

5.8.12 Список управления QoS (QCL)

Страница [QoS Control List Configuration] показывает все QCE (записи правил QoS) таблицы QCL. Вы можете редактировать имеющиеся записи или добавлять новые. QCE состоит из нескольких параметров. Эти параметры различаются в зависимости от выбранного вами типа кадра.

Рисунок 104 – Записи QCL

Нажмите на «+» в правой части таблицы, чтобы открыть еще одну страницу с подробными конфигурациями, как показано ниже.

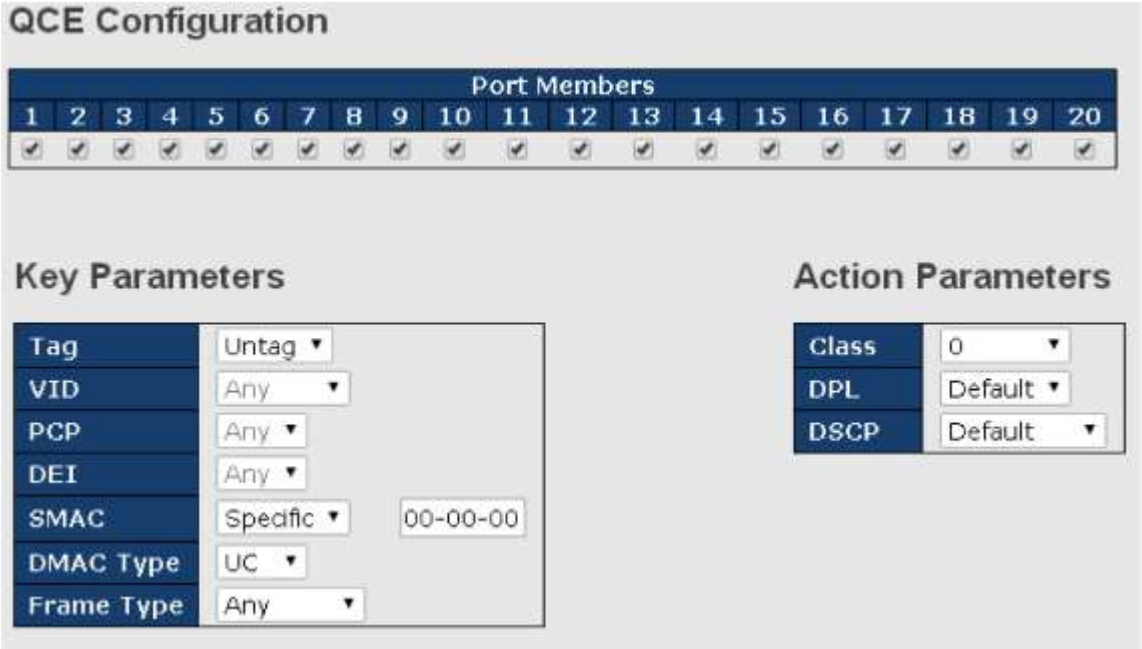


Рисунок 105 – Настройка параметров записи QCL

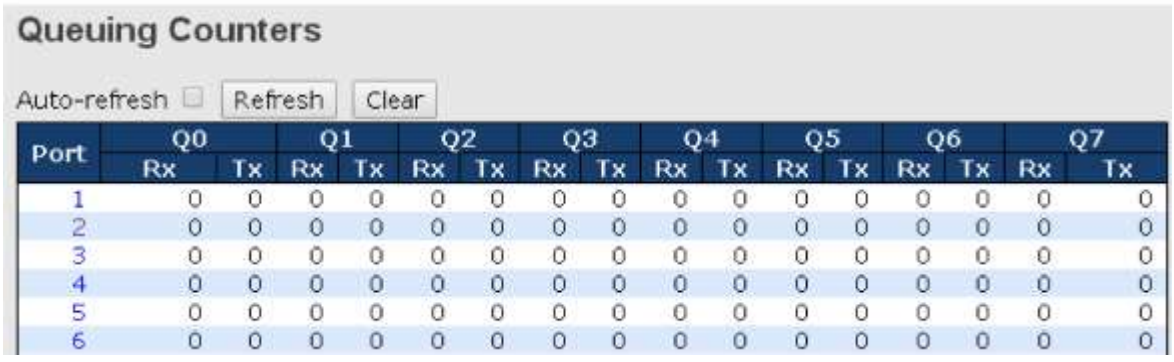
Параметр	Описание
Port Members	Отметьте, чтобы включить порт в запись QCL. По умолчанию включены все порты

Key Parameters	Ключевые параметры конфигурации следующие: **Tag**: тегирование, может быть любым (**Any**), без тега (**Untag**) или с тегом (**Tag**) **VID**: допустимое значение VLAN ID от 1 до 4095. **Any** включает все значения и диапазоны VID **PCP**: код приоритета, может быть определенным числом (0, 1, 2, 3, 4, 5, 6, 7), диапазоном (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) или Any **DEI**: индикатор возможности сброса кадра. Может иметь значение 0, 1 или Any **SMAC**: MAC-адрес источника. 24 старших бита (OUI) или Any **DMAC Type**: тип MAC-адреса назначения. Может быть одноадресным (UC), многоадресным (MC), широковещательным (BC) или любым (Any) **Frame Type**: тип кадра. Может иметь следующие значения: Any, Ethernet, LLC, SNAP, IPv4 и IPv6 Все типы кадров описаны ниже
Any	Разрешить все типы кадров
Ethernet	Допустимые значения Ethernet могут быть в диапазоне от 0x600 до 0xFFFF или Any, но исключая 0x800(IPv4) и 0x86DD(IPv6). Значение по умолчанию – Any
LLC	**SSAP Address**: допустимые значения SSAP (точка доступа к сервису источника) могут находиться в диапазоне от 0x00 до 0xFF или Any. Значение по умолчанию – Any **DSAP Address**: допустимые значения DSAP (точка доступа к сервису получателя) могут находиться в диапазоне от 0x00 до 0xFF или Any. Значение по умолчанию – Any **Control Valid Control**: допустимые значения могут находиться в диапазоне от 0x00 до 0xFF или Any. Значение по умолчанию – Any
SNAP	**PID**: допустимые значения PID (т.е. тип Ethernet) могут быть в диапазоне от 0x00 до 0xFFFF или Any. Значение по умолчанию – Any
IPv4	**Protocol**: (0–255, TCP или UDP) или Any **Source IP**: определенный исходный IP-адрес в формате значение/маска или Any. IP и маска имеют формат x.y.z.w, где x, y, z и w – десятичные числа от 0 до 255. Когда маска преобразуется в 32-битную двоичную строку и считывается слева направо, все биты после первого нуля также должны быть равны нулю

	DSCP: может быть определенным значением, диапазоном или Any. Значения DSCP находятся в диапазоне 0–63, включая BE, CS1–CS7, EF или AF11–AF43 **IP Fragment**: параметры фрагментации кадра Ipv4. Включают «yes», «no» и «any» **Sport**: TCP/UDP-порт источника. 0–65535 или Any; определенное значение или диапазон портов, применимый для IP-протокола UDP/TCP **Dport**: TCP/UDP-порт назначения. 0–65535 или Any; определенное значение или диапазон портов, применимый для IP-протокола UDP/TCP
IPv6	**Protocol**: (0–255, TCP или UDP) или Any **Source IP**: (a.b.c.d) или Any; 32 младших бита **DSCP**: может быть определенным значением, диапазоном или Any. Значения DSCP находятся в диапазоне 0–63, включая BE, CS1-CS7, EF или AF11-AF43 **Sport**: TCP/UDP-порт источника. 0–65535 или Any; определенное значение или диапазон портов, применимый для IP-протокола UDP/TCP **Dport**: TCP/UDP-порт назначения. 0–65535 или Any; определенное значение или диапазон портов, применимый для IP-протокола UDP/TCP
Action Parameters	**Class**: Класс QoS. Значение от 0 до 7 или **Default** **DPL**: допустимое значение уровня приоритета сброса может быть 0, 1 или **Default** **DSCP**: допустимое значение DSCP может быть 0–63, BE, CS1-CS7, EF или AF11–AF43, или **Default** **Default** означает, что классифицированное значение по умолчанию не изменяется этим правилами QCE

5.8.13 Счетчики QoS

На этой странице отображается информация о количестве отправленных и полученных пакетов каждой очереди.



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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Рисунок 106 – Счетчики QoS

Параметр	Описание
Port	Номер порта коммутатора
Q1 – Q7	На каждый порт приходится по 8 очередей QoS. Q0 имеет самый низкий приоритет
Rx / Tx	Количество полученных и переданных пакетов на очередь

Рисунок 107 – Подробная статистика порта QoS

5.8.14 Статус QCL

На этой странице отображается статус QCL для разных пользователей. Каждая строка описывает определенную запись с набором правил (QCE). Если QCE невозможно применить из-за ограничений оборудования, возникнет конфликт. Максимальное количество QCE – 256.

Рисунок 108 – Статус QCL

Параметр	Описание
User	Указывает пользователя QCL
QCE#	Указывает порядковый номер QCE
Frame Type	Указывает, какой тип входящих кадров следует искать. Возможные типы кадров: **Any**: будут учитываться все типы кадров **Ethernet**: будут учитываться только Ethernet-кадры с Ether Type от 0x600 до 0xFFFF **LLC**: будут учитываться только кадры уровня управления логическими каналами (LLC) **SNAP**: будут учитываться только кадры типа SNAP **IPv4**: будут учитываться только кадры IPv4 **IPv6**: будут учитываться только кадры IPv6
Port	Указывает список портов, настроенных с помощью QCE
Action	Указывает, какое действие по классификации будет выполнено для входящего кадра, если его содержимое соответствует настроенным параметрам Существует три поля для действий: **Class**: указывает класс QoS. Если кадр соответствует условиям, указанным в QCE, он будет помещен в соответствующую очередь **DPL**: если кадр соответствует условиям QCE, уровень DP будет установлен в значение, указанное в столбце DPL. Этот уровень определяет приоритет кадра при возможных сбросах **DSCP**: если кадр соответствует условиям QCE, ему будет присвоено значение DSCP, указанное в соответствующем столбце. DSCP определяет приоритет кадра для маршрутизации в сети
Conflict	Показывает, есть ли конфликт среди записей QCL. Поскольку аппаратные ресурсы используются несколькими приложениями, необходимых ресурсов для добавления QCE может не хватать. В таком случае статус конфликта будет отображаться как «Yes». В противном случае будет отображаться «No» Обратите внимание, что конфликт можно устранить, освободив ресурсы, необходимые для добавления записи QCL, с помощью кнопки <Resolve Conflict>

5.9 Многоадресная передача

5.9.1 IGMP Snooping

➢ **Базовая конфигурация**

IGMP Snooping отслеживает трафик IGMP между хостами и маршрутизаторами многоадресной рассылки. Коммутатор использует информацию, изучаемую при помощи IGMP Snooping, для пересылки многоадресного трафика на интерфейсы, подключенные к заинтересованным получателям. Это экономит полосу пропускания, позволяя коммутатору отправлять многоадресный трафик только на те интерфейсы, которые подключены к хостам, желающим его получать, вместо того, чтобы передавать данные широковещательно на все интерфейсы в VLAN. Эта страница позволяет настроить параметры IGMP Snooping.

Рисунок 109 – Основные настройки IGMP Snooping

Параметр	Описание
Snooping Enabled	Установите флажок, чтобы включить IGMP Snooping в глобальном режиме
Unregistered IPMCv4 Flooding enabled	Установите флажок, чтобы разрешить передачу незарегистрированного (не принадлежащего группам) многоадресного IP-трафика
Router Port	Указывает, какие порты выполняют роль портов маршрутизатора. Порт маршрутизатора, или маршрутизирующий порт – это порт на Ethernet-коммутаторе,

	который соединяется с устройством, работающим на сетевом уровне (Layer 3), или с IGMP-запросчиком (устройством, управляющим групповыми запросами в сети) Если один из портов, входящих в агрегацию (группу портов), выбран в качестве маршрутизирующего, вся группа портов будет выполнять функцию порта маршрутизатора
Fast Leave	Установите флажок, чтобы включить на порту функцию быстрого выхода

- **Настройки VLAN**

Если для VLAN не включена функция IGMP Snooping, то многоадресные данные и управляющие пакеты отправляются на все порты этой VLAN, что создает избыточный трафик. Когда функция IGMP Snooping включена, пакеты IGMP перенаправляются на процессор коммутатора для обработки. Многоадресные данные также сначала отправляются на процессор, а затем рассылка продолжается на все порты VLAN. Процессор устанавливает правила в аппаратной части коммутатора, чтобы последующие многоадресные данные отправлялись только на нужные порты, минуя процессор. Таким образом, включение IGMP Snooping позволяет коммутатору более эффективно управлять многоадресным трафиком, отправляя его только на те порты, где это необходимо.

На каждой странице отображается до 99 записей из таблицы VLAN в зависимости от значения в поле «entries per page». По умолчанию на странице отображаются первые 20 записей с начала таблицы. Первой будет отображена запись с наименьшим VLAN ID, найденным в таблице VLAN.

Поле «VLAN» позволяет пользователю выбрать начальную точку в таблице VLAN. После нажатия кнопки «Refresh» таблица отобразится, начиная с указанной VLAN или ближайшего к ней совпадения. Кнопка «>>» перемещает отображение на следующую страницу таблицы, начиная с последней VLAN на текущей странице. Если достигнут конец таблицы, появится сообщение «No more entries». Чтобы вернуться к началу таблицы, нажмите кнопку «|<<».

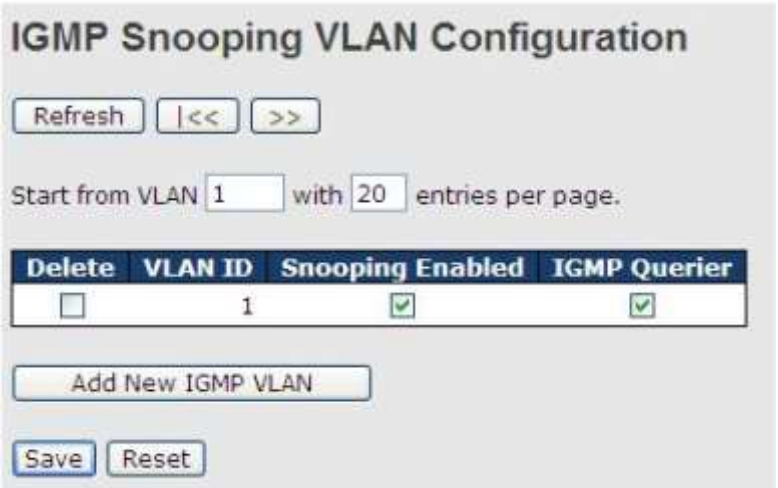


Рисунок 110 – Настройка VLAN

Параметр	Описание
Delete	Установите флажок, чтобы удалить запись. Назначенная запись будет удалена при следующем сохранении
VLAN ID	Идентификатор VLAN записи
IGMP Snooping Enable	Установите флажок, чтобы включить IGMP Snooping для отдельной VLAN. Можно выбрать до 32 VLAN
IGMP Querier	Установите флажок, чтобы включить запросчик IGMP в VLAN

➢ **Статус**

Эта страница отображает состояние IGMP Snooping.

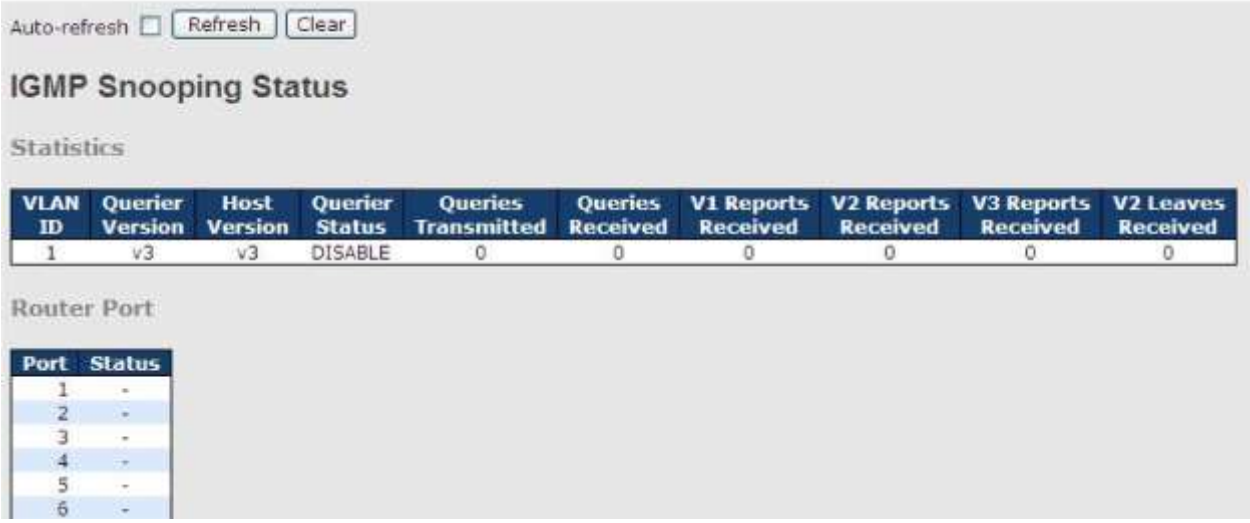


Рисунок 111 – Состояние IGMP Snooping

Параметр	Описание
VLAN ID	Идентификатор VLAN записи
Querier Version	Версия активного запросчика
Host Version	Версия активного хоста
Querier Status	Показывает состояние запросчика как «ACTIVE» или «IDLE»
Querier Receive	Количество запросов

V1 Reports Receive	Количество полученных отчетов V1
V2 Reports Receive	Количество полученных отчетов V2
V3 Reports Receive	Количество полученных отчетов V3
V2 Leave Receive	Количество полученных пакетов leave V2
Refresh	Нажмите, чтобы немедленно обновить страницу
Clear	Очистить все счетчики статистики
Auto-refresh	Отметьте, чтобы включить автоматическое обновление страницы через регулярные интервалы
Port	Номер порта коммутатора
Status	Указывает, является ли определенный порт портом маршрутизатора или нет

- **Информация о группах IGMP Snooping**

На этой странице показана информация о записях в таблице IGMP-групп. Таблица сортируется сначала по идентификатору VLAN, а затем по группе.

Рисунок 112 – Информация о группах IGMP Snooping

Параметр	Описание
VLAN ID	Идентификатор VLAN группы
Groups	Адрес группы
Port Members	Порты в этой группе

5.10 Безопасность

5.10.1 Безопасность удаленного управления

На странице [Remote Control Security] можно ограничить удаленный доступ к интерфейсу управления. При включении данной функции запросы клиента, не входящего в разрешенный список, будут отклоняться.

Рисунок 113 – Контроль удаленного управления

Параметр	Описание
Port	Номер порта удаленного клиента
IP Address	IP-адрес удаленного клиента. 0.0.0.0 означает «любой IP»
Web	Отметьте, чтобы включить управление через веб-интерфейс
Telnet	Отметьте, чтобы включить управление через интерфейс Telnet
SNMP	Отметьте, чтобы включить управление через интерфейс SNMP
Delete	Отметьте, чтобы удалить записи

5.10.2 Привязка устройств

Привязка устройств (Device Binding) – это технология, которая привязывает IP/MAC устройства к указанному порту Ethernet. Если IP/MAC устройства, подключенного к порту Ethernet, не соответствует требованиям привязки, устройство будет заблокировано по соображениям безопасности. Привязка устройств также обеспечивает функции безопасности посредством проверки активности, проверки потоковой передачи и предотвращения атак DoS/DDoS.

Рисунок 114 – Привязка устройств

Параметр	Описание
Mode	Указывает операцию привязки устройства для каждого порта. Возможные режимы: ---: отключает любые проверки **Scan**: автоматически сканирует IP/MAC, но без функции привязки **Binding**: включает привязку. В этом режиме любой IP/MAC, который не соответствует записи, не будет допущен к сети **Shutdown**: выключает порт (нет связи)
Alive Check Active	Установите флажок, чтобы включить проверку активности. Если включено, коммутатор будет постоянно пинговать устройство
Alive Check Status	Указывает состояние проверки активности. Возможные статусы: ---: отключено **Got Reply**: от устройства получен ответ на ping, что означает, что оно все еще активно **Lost Reply**: от устройства не получен ответ на ping, что означает, что оно могло быть неактивным
Stream Check Active	Установите флажок, чтобы включить проверку потока. Если включено, коммутатор обнаружит снижение трафика, идущего от устройства
Stream Check Status	Указывает состояние проверки потока. Возможные статусы: ---: отключено **Normal**: поток в норме **Low**: интенсивность потока снижается

DdoS Prevention Action	Установите флажок, чтобы включить предотвращение DDoS. Если включено, коммутатор будет контролировать устройство на предмет DDoS-атак
DdoS Prevention Status	Указывает состояние предотвращения DDoS. Возможные статусы: ---: отключено **Analyzing**: анализирует занимаемую пакетами полосу пропускания для инициализации **Running**: анализ завершен, готов к следующему шагу **Attacked**: происходят DDOS-атаки
Device IP Address	Указывает IP-адрес устройства
Device MAC Address	Указывает MAC-адрес устройства

5.10.2.1 Дополнительные IP-адреса

Для назначения вторичного IP-адреса создается псевдоним (alias) сетевого интерфейса. На странице [Alias IP Address] можно настроить дополнительные IP-адреса для устройства.

Рисунок 115 – Дополнительные IP-адреса

Параметр	Описание
Port	Номер порта коммутатора
Alias IP Address	Указывает вторичный IP-адрес. Если в таком адресе нет необходимости, оставьте значение 0.0.0.0 без изменений

5.10.2.2 Проверка активности

Функция Alive Check отслеживает состояние устройства, подключенного к порту, в режиме реального времени. Пакеты проверки активности будут отправлены на устройство, чтобы удостовериться, работает ли оно. Если коммутатор не получает ответа от устройства, будут предприняты действия в соответствии с вашими настройками.

Рисунок 116 – Настройка проверки активности

Параметр	Описание
Link Change	Отключает и включает порт
Only log it	Только регистрирует событие на сервере журналирования
Shut Down the Port	Отключает порт
Reboot Device	Отключает и включает питание PoE

5.10.2.3 Предотвращение DDoS-атак

Коммутатор может отслеживать входящие пакеты и выполнять определенные действия при возникновении DDoS-атаки на указанном порту. Когда сетевой трафик с удаленного устройства значительно увеличивается за короткий промежуток времени, коммутатор блокирует IP-адрес этого устройства, чтобы защитить сеть от атак. На странице [DDoS Prevention] можно настроить предотвращение DDoS-атак, чтобы добиться максимальной защиты.

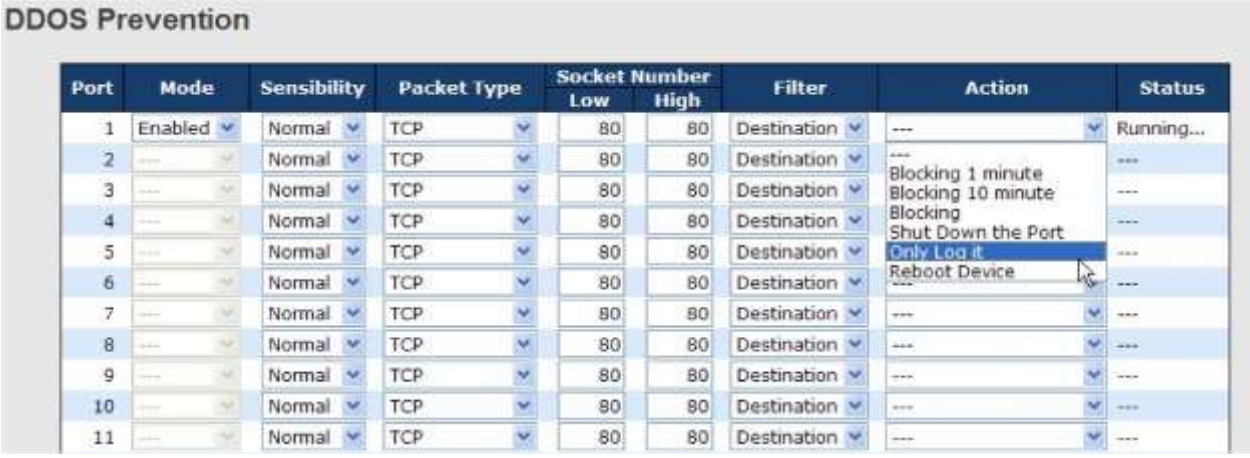


Рисунок 117 – Предотвращение DDoS-атак

Параметр	Описание
Mode	Включает или отключает защиту порта от DDoS-атак
Sensibility	Указывает уровень обнаружения DDoS. Возможны следующие уровни: **Low**: низкая чувствительность **Normal**: нормальная чувствительность **Medium**: средняя чувствительность **High**: высокая чувствительность
Packet Type	Указывает типы пакетов DDoS-атак, которые необходимо отслеживать. Возможны следующие типы: **RX Total**: все входящие пакеты **RX Unicast**: входящие пакеты одноадресной рассылки **RX Multicast**: входящие пакеты многоадресной рассылки **RX Broadcast**: входящие пакеты широковещательной рассылки **TCP**: входящие пакеты TCP **UDP**: входящие пакеты UDP
Socket Number	Если тип пакета – UDP или TCP, необходимо указать номер сокета (то есть номер порта), который будет фильтроваться. Параметр может быть задан как диапазон от низкого до высокого значения. Если нужно указать только один номер порта, то его следует записать в оба поля – как в «low», так и в «high»

Filter	Если тип пакета – UDP (или TCP), выберите, будет ли трафик фильтроваться на основании номера порта назначения или источника (**Destination**/**Source**)
Action	Указывает действие, которое необходимо выполнить при возникновении DDOS-атак. Возможные действия: **---**: никаких действий **Blocking 1 minute**: блокирует пересылку на 1 минуту и регистрирует событие **Blocking 10 minute**: блокирует пересылку на 10 минут и регистрирует событие **Blocking**: блокирует и регистрирует событие **Shut Down the Port**: отключает порт (нет связи) и регистрирует событие **Only Log it**: просто регистрирует событие **Reboot Device**: если поддерживается PoE, удаленное устройство можно перезагрузить. Событие будет регистрироваться
Status	Указывает состояние защиты от DDoS-атак. Возможные статусы: **---**: отключено **Analyzing**: анализирует занимаемую пакетами пропускную способность для инициализации **Running**: анализ завершен и готов к следующему шагу **Attacked**: происходят DDoS-атаки

5.10.2.4 Описание устройств

На странице [Device Description] можно выполнить описание подключенного устройства.

Рисунок 118 – Описание устройства

Параметр	Описание
Port	Номер порта коммутатора
Device Type	Указывает тип устройства. Доступны следующие типы: **---**: тип не указан **IP Camera**: IP-камера **IP Phone**: IP-телефон **Access Point**: точка доступа **PC**: персональный компьютер **PLC**: программируемый логический контроллер **Network Video Recorder**: сетевой видеорегистратор
Location Address	Указывает информацию о местоположении устройства. Информацию можно использовать для позиционирования на карте
Description	Описание устройства

5.10.2.5 Проверка потоковой передачи

Функция Stream Check отслеживает в реальном времени согласованность сетевого трафика от устройства, связанного с портом. При резком изменении трафика будет выдано оповещение. Эта страница позволяет вам настроить параметры проверки потока.

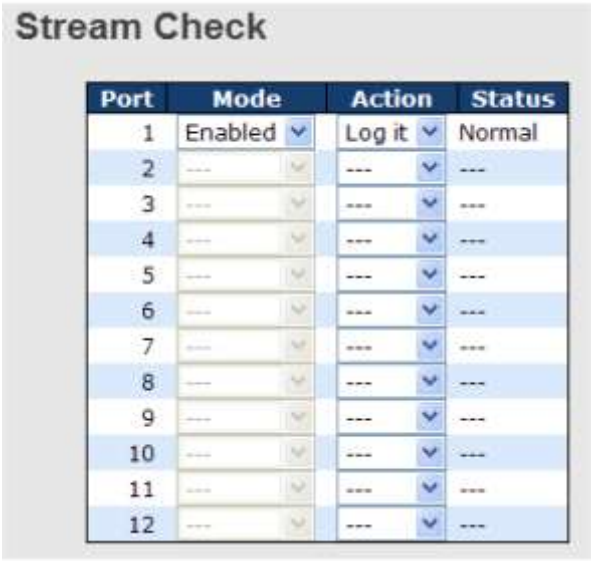


Рисунок 119 – Проверка потока

Параметр	Описание
Port	Номер порта коммутатора
Mode	Включает или отключает мониторинг потока на порту
Action	Указывает действие, которое следует предпринять, когда интенсивность потока снижается. Возможные действия: ---: никаких действий **Log it**: регистрация события
Status	Указывает состояние проверки потока. Возможные статусы: ---: отключено **Normal**: поток в норме **Low**: интенсивность потока снижается

5.10.3 ACL

ACL (список управления доступом) – это список разрешений, прикрепленных к объекту. ACL определяет, какие пользователи или системные процессы имеют право доступа к объектам и какие операции разрешены для данных объектов.

5.10.3.1 Настройка портов

Рисунок 120 – Настройка портов

Параметр	Описание
Port	Номер порта коммутатора, к которому будут применены следующие настройки
Policy ID	Выберите, чтобы применить политику к порту. Допустимые значения: от 1 до 8. Значение по умолчанию: 1
Action	Выберите **Permit**, чтобы разрешить, или **Deny**, чтобы запретить пересылку. Значение по умолчанию: **Permit**
Rate Limiter ID	Выберите ограничитель скорости для порта. Допустимые значения: **Disabled** (отключено) или числа от 1 до 15. Значение по умолчанию: **Disabled**
Port Copy	Выберите, на какой порт копируются кадры. Допустимые значения: **Disabled** (отключено) или определенный номер порта. Значение по умолчанию: **Disabled**
Logging	Задает режим ведения журнала порта. Допустимые значения: **Enabled**: кадры, полученные на порту, сохраняются в системном журнале **Disabled**: кадры, полученные на порту, не регистрируются Значение по умолчанию – **Disabled**. Обратите внимание, что объем памяти системного журнала и скорость ведения журнала ограничены
Shutdown	Указывает условия выключения этого порта. Допустимые значения: **Enabled**: если на порт получен кадр, порт будет отключен

	Disabled: выключение порта не предусмотрено Значение по умолчанию – **Disabled**
Counter	Подсчитывает количество кадров, соответствующих этому элементу списка управления доступом

5.10.3.2 Ограничители скорости

Страница [ACL Rate Limiter Configuration] позволяет вам определить ограничения скорости для ACL.

Рисунок 121 – Настройка ограничения скорости

Параметр	Описание
Rate Limiter ID	Идентификатор ограничителя скорости для настроек, содержащихся в той же строке
Rate	Единицей скорости является пакет в секунду (pps), который можно настроить как 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K или 1024K 1 kpps на самом деле равен 1002,1 pps

5.10.3.3 ACE

ACE (Access Control Entry) – это элемент списка управления доступом (ACL). ACL может иметь ноль или более ACE. Каждый ACE контролирует или отслеживает доступ к объекту на основе пользовательских конфигураций. Каждый ACE состоит из нескольких параметров, которые различаются в зависимости от выбранного вами типа кадра.

Рисунок 122 – Конфигурация ACL

Нажмите на «+» в правой части таблицы, чтобы открыть страницу с подробными настройками параметров (как показано ниже).

Рисунок 123 – Настройки ACE

Параметр	Описание
Ingress Port	Указывает входной порт, к которому будет применяться ACE **Any**: ACE применяется к любому порту **Port n**: ACE применяется к порту n коммутатора **Policy n**: ACE применяется к номеру политики n, где n может находиться в диапазоне от 1 до 8
Policy Filter	Указывает фильтр номера политики для этого ACE **Any**: фильтр политики не указан. Статус фильтра политики – «не имеет значения» **Specific**: если вы хотите отфильтровать определенную политику с помощью этого ACE, выберите это значение. Появятся два поля для ввода значения политики и битовой маски **Policy Value**: Если для фильтра политики выбрано **Specific**, вы можете ввести определенное значение политики. Допустимый диапазон – от 0 до 255

	Policy Bitmask: Если для фильтра политики выбрано **Specific**, вы можете ввести определенную битовую маску политики. Допустимый диапазон – от 0x0 до 0xff
Frame Type	Указывает тип кадра для применения ACE. Эти типы кадров являются взаимоисключающими. **Any**: любой кадр может соответствовать ACE **Ethernet Type**: только кадры типа Ethernet могут соответствовать этому ACE **ARP**: только кадры ARP могут соответствовать ACE. Обратите внимание, что кадры ARP не будут соответствовать ACE с типом Ethernet **IPv4**: только кадры IPv4 могут соответствовать ACE. Обратите внимание, что кадры IPv4 не будут соответствовать ACE с типом Ethernet
Action	Указывает действие, которое следует предпринять, если кадр соответствует ACE **Permit**: выполнить действие, если кадр соответствует ACE **Deny**: отбросить кадр, соответствующий ACE
Rate Limiter	Указывает ограничитель скорости в количестве базовых единиц. Допустимый диапазон – от 1 до 15. **Disabled** означает, что функция ограничителя скорости отключена
Port Copy	Кадры, соответствующие ACE, копируются на указанный здесь номер порта. Допустимый диапазон совпадает с диапазоном номеров портов коммутатора. **Disabled** означает, что операция копирования не разрешена
Logging	Задает операцию регистрации событий, относящихся к ACE. Допустимые значения: **Enabled**: кадры, соответствующие ACE, сохраняются в системном журнале **Disabled**: кадры, соответствующие ACE, не регистрируются Обратите внимание, что объем памяти системного журнала и скорость регистрации ограничены
Shutdown	Указывает условия выключения порта согласно ACE. Допустимые значения: **Enabled**: если кадр соответствует ACE, входной порт будет отключен **Disabled**: для данного ACE не предусмотрено выключение порта
Counter	Подсчитывает количество кадров, сопоставленных с данным ACE

5.10.3.4 Тип кадра – Ethernet

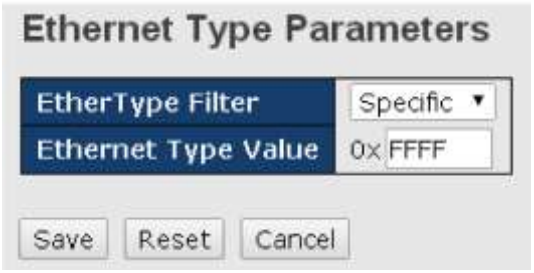


Рисунок 124 – Параметры кадра Ethernet

Параметр	Описание
EtherType Filter	Укажите фильтр кадров типа Ethernet для этого ACE, включая: **Any**: фильтр EtherType не указан. Статус фильтра EtherType – «не имеет значения» **Specific**: если вы хотите применить ACE к определенным Ethernet-кадрам, выберете **Specific** и введите нужное значение EtherType в появившемся поле
Ethernet Type Value	Если для фильтра EtherType выбрана опция **Specific**, можно ввести определенное значение EtherType. Допустимый диапазон – от 0x600 до 0xFFFF. ACE будет применяться к кадрам, имеющим выбранное значение

5.10.3.5 Тип кадра – ARP

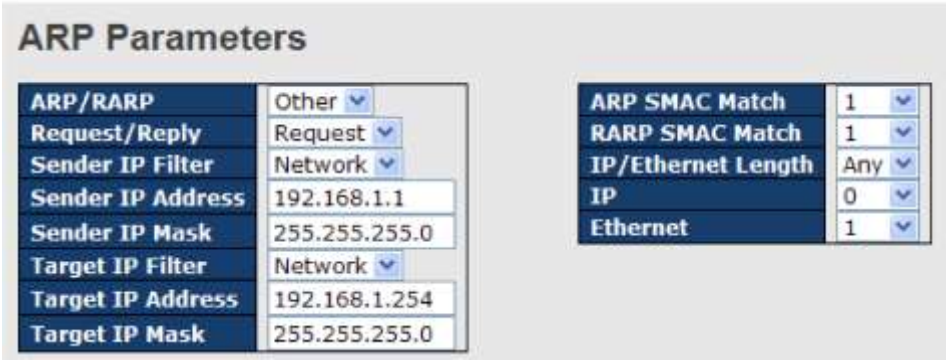


Рисунок 125 – Параметры кадра ARP

Параметр	Описание
ARP/RARP	Позволяет фильтровать ARP/RARP-трафик, к которому применяется ACE, на основе кода операции (OP). В этой настройке можно указать, какой именно тип ARP/RARP сообщений нужно учитывать: **Any**: неважно, какой код операции (игнорировать флаг OP) **ARP**: фильтрация применяется только к кадрам, содержащим код операции ARP **RARP**: фильтрация применяется только к кадрам с кодом операции RARP **Other**: фильтрация применяется к кадрам с неизвестным или нестандартным кодом операции ARP/RARP
Request/Reply	Указывает доступный флаг OP ARP/RARP для ACE

	Any: неважно, какой код операции (игнорировать флаг OP) **Request**: кадр должен иметь флаг OP запроса ARP или запроса RARP **Reply**: кадр должен иметь флаг OP ответа ARP или ответа RARP
Sender IP Filter	Указывает фильтр на основе IP-адреса отправителя для ACE **Any**: фильтр IP отправителя не указан. Статус фильтра «не имеет значения» **Host**: фильтр IP отправителя на основе хоста. Укажите IP-адрес отправителя в появившемся поле «SIP Address» **Network**: фильтр IP отправителя на основе подсети. Укажите IP-адрес и маску подсети отправителя в появившихся полях «SIP Address» и «SIP Mask»
Sender IP Address	Если для фильтра IP-адресов отправителя выбрано значение **Host** или **Network**, можно ввести конкретный IP-адрес отправителя в десятичном формате с разделительными точками
Sender IP Mask	Если для фильтра IP-адресов отправителя выбрано значение **Network**, можно ввести маску подсети отправителя в десятичном формате с разделительными точками
Target IP Filter	Указывает фильтр на основе IP-адреса получателя для ACE **Any**: фильтр IP получателя не указан. Статус фильтра «не имеет значения» **Host**: фильтр IP получателя на основе хоста. Укажите IP-адрес получателя в появившемся поле «Target IP Address» **Network**: фильтр IP получателя на основе подсети. Укажите IP-адрес и маску подсети получателя в появившихся полях «Target IP Address» и «Target IP Mask»
Target IP Address	Если для фильтра IP-адресов получателя выбрано значение **Host** или **Network**, можно ввести конкретный IP-адрес получателя в десятичном формате с разделительными точками
Target IP Mask	Если для фильтра IP-адресов получателя выбрано значение **Network**, можно ввести маску подсети получателя в десятичном формате с разделительными точками
ARP SMAC Match	Позволяет управлять обработкой ARP-кадров в зависимости от совпадения их MAC-адреса отправителя (SHA) с исходным MAC-адресом (SMAC): **0**: применяется к ARP-кадрам, где SHA и SMAC совпадают **1**: применяется к ARP-кадрам, где SHA и SMAC не совпадают

	Any: правило действует для всех ARP-кадров, независимо от совпадения адресов (игнорировать соответствие)
RARP SMAC Match	Позволяет управлять обработкой ARP-кадров в зависимости от совпадения их MAC-адреса получателя (THA) с исходным MAC-адресом (SMAC): **0**: применяется к ARP-кадрам, где THA и SMAC совпадают **1**: применяется к ARP-кадрам, где THA и SMAC не совпадают **Any**: правило действует для всех ARP-кадров, независимо от совпадения адресов (игнорировать соответствие)
IP/Ethernet Length	Позволяет управлять обработкой ARP/RARP-кадров в зависимости от их длины аппаратного адреса (HLN) и длины протокольного адреса (PLN): **0**: ARP/RARP-кадры, где длина HLN равна Ethernet (0x06), а длина PLN равна IPv4 (0x04), не должны соответствовать этому правилу **1**: ARP/RARP-кадры, где длина HLN равна Ethernet (0x06), а длина PLN равна IPv4 (0x04), должны соответствовать этому правилу **Any**: правило действует для всех ARP/RARP-кадров, независимо от значений HLN и PLN (игнорировать соответствие)
IP	Позволяет управлять обработкой ARP/RARP-кадров в зависимости от их типа протокольного адреса (PRO): **0**: ARP/RARP-кадры, где PRO равен IP (0x800), не должны соответствовать этому правилу **1**: ARP/RARP-кадры, где PRO равен IP (0x800), должны соответствовать этому правилу **Any**: правило действует для всех ARP/RARP-кадров, независимо от типа протокольного адреса (игнорировать соответствие)
Ethernet	Позволяет управлять обработкой ARP/RARP-кадров в зависимости от их типа аппаратного адреса (HRD): **0**: ARP/RARP-кадры, где HRD равен Ethernet (значение 1), не должны соответствовать этому правилу. **1**: ARP/RARP-кадры, где HRD равен Ethernet (значение 1), должны соответствовать этому правилу. **Any**: правило действует для всех ARP/RARP-кадров, независимо от типа аппаратного адреса (игнорировать соответствие)

5.10.3.6 Тип кадра – IPv4

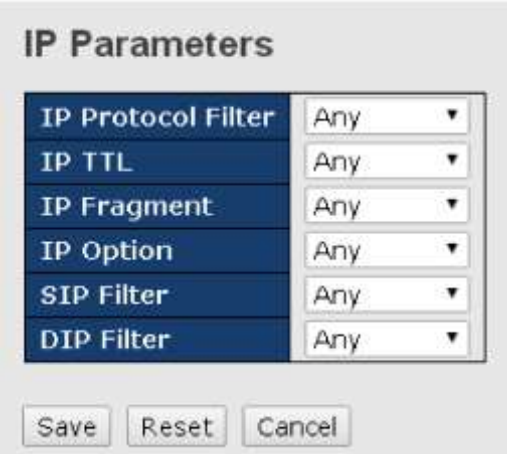


Рисунок 126 – Параметры кадра IP

Параметр	Описание
IP Protocol Filter	Указывает фильтр протокола IP для ACE **Any**: фильтр протокола IP не указан. Статус «не имеет значения» **Specific**: если вы хотите отфильтровать определенный параметр протокола IP с помощью ACE, выберите нужное значение. Появится поле для ввода значений **ICMP**: выбор фильтрации кадров ICMP протокола IPv4. Появятся дополнительные поля для определения параметров ICMP **UDP**: выбор фильтрации кадров UDP протокола IPv4. Появятся дополнительные поля для определения параметров ICMP **TCP**: выбор фильтрации кадров ICMP протокола IPv4. Появятся дополнительные поля для определения параметров ICMP
IP TTL	Позволяет управлять обработкой кадров IPv4 в зависимости от их параметра «time-to-live»: **Zero**: кадры IPv4 со значением поля TTL больше нуля не должны соответствовать этой записи **Non-zero**: кадры IPv4 со значением поля TTL больше нуля должны соответствовать этой записи **Any**: правило действует для кадров IPv4, независимо от значения TTL (игнорировать соответствие)
IP Fragment	Определяет, как будут обрабатываться IPv4-пакеты в зависимости от их фрагментации, а именно состояния бита More Fragments (MF) и значения поля Fragment Offset (FRAG OFFSET):

	No: IPv4-пакеты, у которых установлен бит MF или значение поля FRAG OFFSET больше нуля, не должны соответствовать этому правилу **Yes**: IPv4-пакеты, у которых установлен бит MF или значение поля FRAG OFFSET больше нуля, должны соответствовать этому правилу **Any**: правило применяется ко всем IPv4-пакетам, независимо от состояния бита MF и значения поля FRAG OFFSET (игнорировать соответствие)
IP Option	Позволяет фильтровать IPv4-пакеты в зависимости от наличия дополнительных опций в заголовке. **No**: IPv4-пакеты, имеющие флаг в поле «IP Options», не должны соответствовать этому правилу **Yes**: IPv4-пакеты, имеющие флаг в поле «IP Options», должны соответствовать этому правилу **Any**: правило применяется ко всем IPv4-пакетам, независимо от того, настроены ли опции (игнорировать соответствие)
SIP Filter	Указывает фильтр на основе IP-адреса источника для ACE **Any**: фильтр IP источника не указан. Статус фильтра «не имеет значения» **Host**: фильтр IP источника на основе хоста. Укажите IP-адрес источника в появившемся поле «SIP Address» **Network**: фильтр IP источника на основе подсети. Укажите IP-адрес и маску подсети источника в появившихся полях «SIP Address» и «SIP Mask»
DIP Filter	Указывает фильтр на основе IP-адреса назначения для ACE **Any**: фильтр IP назначения не указан. Статус фильтра «не имеет значения» **Host**: фильтр IP назначения на основе хоста. Укажите IP-адрес назначения в появившемся поле «DIP Address» **Network**: фильтр IP назначения на основе подсети. Укажите IP-адрес и маску подсети назначения в появившихся полях «DIP Address» и «DIP Mask»

5.10.3.7 Настройка на основе MAC-адреса

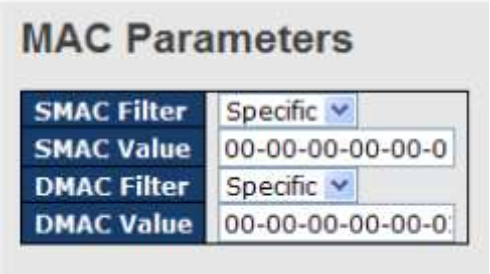


Рисунок 127 – Параметры MAC

Параметр	Описание
SMAC Filter	Отображается только в том случае, если тип кадра – Ethernet или ARP. Определяет, как будут обрабатываться пакеты на основании их MAC-адреса источника **Any**: фильтр SMAC не указан. Статус фильтра «не имеет значения» **Specific**: выберите это значение, если хотите применить правило ACE к определенному исходному MAC-адресу. Появится поле ввода
SMAC Value	Если для фильтра SMAC выбрано значение **Specific**, в этом поле вводится конкретный исходный MAC-адрес. Допустимый формат – «xx-xx-xx-xx-xx-xx». Кадры будут обрабатываться при помощи ACE на основании этого значения SMAC
DMAC Filter	Определяет, как будут обрабатываться пакеты на основании их MAC-адреса назначения **Any**: фильтр DMAC не указан. Статус фильтра «не имеет значения»; **MC**: кадр должен быть многоадресным **BC**: кадр должен быть широковещательным **UC**: кадр должен быть одноадресным **Specific**: выберите это значение, если хотите применить правило ACE к определенному MAC-адресу назначения. Появится поле ввода
DMAC Value	Если для фильтра SMAC выбрано значение **Specific**, в этом поле вводится конкретный MAC-адрес назначения. Допустимый формат – «xx-xx-xx-xx-xx-xx». Кадры будут обрабатываться при помощи ACE на основании этого значения DMAC

5.10.3.8 Настройка на основе VLAN

Рисунок 128 – Параметры VLAN

Параметр	Описание
VLAN ID Filter	Определяет, как будут обрабатываться пакеты на основании их VLAN ID **Any**: правило применяется к пакетам всех VLAN, независимо от их идентификатора (игнорировать соответствие) **Specific**: выберите это значение, если хотите применить правило ACE к кадрам определенной VLAN. Появится поле ввода
VLAN ID	Если для фильтра выбрано значение **Specific**, вы можете ввести конкретный номер VLAN ID. Допустимый диапазон – от 1 до 4095. Кадры будут обрабатываться при помощи ACE на основании этого значения VLAN ID
Tag Priority	Указывает приоритет тега VLAN для ACE. Кадр с соответствующим приоритетом будет соответствовать данному ACE Допустимый диапазон чисел – от 0 до 7 **Any**: означает, что приоритет тега не указан Статус «не имеет значения»

5.10.3.9 Настройка на основе ICMP

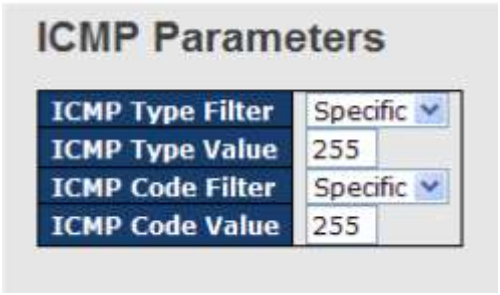


Рисунок 129 – Параметры ICMP

Параметр	Описание
ICMP Type Filter	Определяет, как будут обрабатываться кадры ICMP на основании их типа **Any**: правило применяется к любым кадрам ICMP, независимо от их типа (игнорировать соответствие) **Specific**: выберите это значение, если хотите применить правило ACE к кадрам ICMP определенного типа. Появится поле ввода значения ICMP Type
ICMP Type Value	Если для фильтра выбрано значение **Specific**, вы можете ввести конкретное значение ICMP Type. Допустимый диапазон – от 0 до 255. Кадры ICMP будут обрабатываться при помощи ACE на основании их типа
ICMP Code Filter	Определяет, как будут обрабатываться кадры ICMP на основании их кода **Any**: правило применяется к любым кадрам ICMP, независимо от их кода (игнорировать соответствие) **Specific**: выберите это значение, если хотите применить правило ACE к кадрам ICMP с определенным кодом. Появится поле ввода значения ICMP Type
ICMP Code Value	Если для фильтра выбрано значение **Specific**, вы можете ввести конкретное значение ICMP Code. Допустимый диапазон – от 0 до 255. Кадры ICMP будут обрабатываться при помощи ACE на основании их кода

5.10.3.10 Настройка на основе TCP/UDP

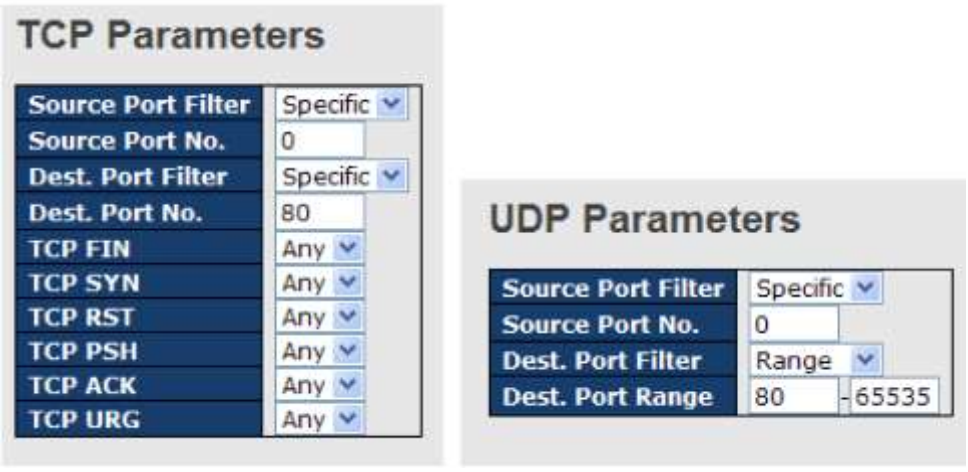


Рисунок 130 – Параметры TCP/UDP

Параметр	Описание
TCP/UDP Source Port Filter	Указывает фильтр портов источника TCP/UDP для ACE **Any**: правило применяется к любым кадрам TCP/UDP, независимо от их исходного порта (игнорировать соответствие) **Specific**: выберите это значение, если хотите применить ACE к кадрам TCP/UDP определенного исходного порта. Появится поле ввода **Range**: выберите это значение, если хотите применить ACE к кадрам TCP/UDP определенного диапазона исходных портов. Появится поле ввода
TCP/UDP Source Port No.	Если для фильтра выбрано значение **Specific**, вы можете ввести конкретный номер порта источника TCP/UDP. Допустимый диапазон – от 0 до 65535. Кадры TCP/UDP будут обрабатываться при помощи ACE на основании номера их исходного порта
TCP/UDP Source Port Range	Если для фильтра выбрано значение **Specific**, вы можете ввести диапазон исходных портов TCP/UDP. Допустимые значения – от 0 до 65535. Кадры TCP/UDP будут обрабатываться при помощи ACE на основании указанного диапазона их исходных портов
TCP/UDP Dest. Port Filter	Указывает фильтр портов назначения TCP/UDP для ACE **Any**: правило применяется к любым кадрам TCP/UDP, независимо от их порта назначения (игнорировать соответствие) **Specific**: выберите это значение, если хотите применить ACE к кадрам TCP/UDP с определенным портом назначения. Появится поле ввода **Range**: выберите это значение, если хотите применить ACE к кадрам TCP/UDP с определенным диапазоном портов назначения. Появится поле ввода
TCP/UDP Dest. Port No.	Если для фильтра выбрано значение **Specific**, вы можете ввести конкретный номер порта назначения TCP/UDP. Допустимый диапазон – от 0 до 65535. Кадры TCP/UDP будут обрабатываться при помощи ACE на основании номера их порта назначения
TCP/UDP Des. Port Range	Если для фильтра выбрано значение **Specific**, вы можете ввести диапазон портов назначения TCP/UDP. Допустимые значения – от 0 до 65535. Кадры TCP/UDP будут обрабатываться при помощи ACE на основании указанного диапазона их портов назначения
TCP FIN	Указывает для ACE значение поля TCP FIN (больше нет данных от отправителя)

	0: TCP-кадры, в которых установлен флаг FIN, не должны соответствовать этой записи **1**: TCP-кадры, в которых установлен флаг FIN, должны соответствовать этой записи. **Any**: разрешено любое значение (флаг FIN игнорируется)
TCP SYN	Указывает для ACE значение поля TCP SYN (синхронизировать начальный номер последовательности для нового соединения). **0**: TCP-кадры, в которых установлен флаг SYN, не должны соответствовать этой записи **1**: TCP-кадры, в которых установлен флаг SYN, должны соответствовать этой записи **Any**: разрешено любое значение (флаг SYN игнорируется)
TCP RST	Указывает для ACE значение поля TCP RST (сигнал закрытия соединения) **0**: TCP-кадры, в которых установлен флаг RST, не должны соответствовать этой записи **1**: TCP-кадры, в которых установлен флаг RST, должны соответствовать этой записи **Any**: разрешено любое значение (флаг RST игнорируется)
TCP PSH	Указывает для ACE значение поля TCP PSH (передача без буферизации) **0**: TCP-кадры, в которых установлен флаг PSH, не должны соответствовать этой записи **1**: TCP-кадры, в которых установлен флаг PSH, должны соответствовать этой записи **Any**: разрешено любое значение (флаг PSH игнорируется)
TCP ACK	Указывает для ACE значение поля TCP ACK (подтверждение получения данных) **0**: TCP-кадры, в которых установлен флаг ACK, не должны соответствовать этой записи **1**: TCP-кадры, в которых установлен флаг ACK, должны соответствовать этой записи **Any**: разрешено любое значение (флаг ACK игнорируется)
TCP URG	Указывает для ACE значение поля TCP URG (требуется срочная передача вне очереди) **0**: TCP-кадры, в которых установлен флаг URG, не должны соответствовать этой записи

	1: TCP-кадры, в которых установлен флаг URG, должны соответствовать этой записи **Any**: разрешено любое значение (флаг URG игнорируется)

5.10.3.11 Состояние ACL

Страница [ACL Status] отображает текущее состояние списка управления доступом.

Рисунок 131 – Статус ACL

5.10.4 AAA (аутентификация, авторизация и учет)

Сервер AAA – это приложение, которое предоставляет услуги аутентификации, авторизации и учета для безопасного доступа к сети. Приложение может находиться на выделенном компьютере, коммутаторе Ethernet, точке доступа или сервере сетевого доступа (NAS). Текущим стандартом, по которому устройства или приложения взаимодействуют с сервером AAA, является RADIUS (служба удаленной аутентификации пользователей по коммутируемым линиям). RADIUS – это протокол, используемый между коммутатором и сервером аутентификации. На этой странице можно настроить общие параметры для сервера.

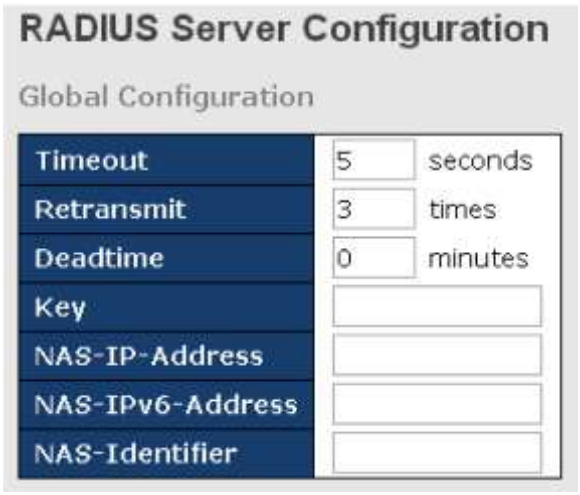


Рисунок 132 – Общая настройка RADIUS

Параметр	Описание

Timeout	Тайм-аут, который можно установить в диапазоне от 3 до 3600 секунд, – это максимальное время ожидания ответа от сервера Если сервер не отвечает в течение этого периода времени, система будет считать его неработоспособным и будет пытаться связаться со следующим включенным сервером (если таковой имеется) Серверы RADIUS используют протокол UDP, который по своей сути ненадежен. Чтобы справиться с потерянными кадрами, суммарная продолжительность тайм-аута делится на 3 интервала равной длины. Если ответ не получен в течение интервала, запрос передается снова. Этот алгоритм опрашивает сервер RADIUS до 3 раз, прежде чем он будет считаться неработоспособным
Retransmit	Количество попыток коммутатора подключиться к серверу RADIUS
Dead Time	Время простоя, которое можно задать в диапазоне от 0 до 3600 секунд, – это период, в течение которого коммутатор не будет отправлять новые запросы на сервер, не ответивший на предыдущий запрос. Это остановит постоянные попытки коммутатора связаться с сервером, который он уже определил как неработающий. Установка времени простоя на значение больше 0 (нуля) включит эту функцию, но только если настроено более одного сервера
NAS-IP-Address	Указывает идентификационный IP-адрес сервера сетевого доступа, который запрашивает аутентификацию пользователя. Адрес должен быть уникальным для NAS в пределах области действия сервера RADIUS
NAS-ID	Идентификатор сервера сетевого доступа (NAS-ID) для интерфейса. NAS-ID отправляется на сервер RADIUS контроллером (как клиент RADIUS) с помощью запроса аутентификации, который используется для классификации пользователей по разным группам. Можно ввести до 32 буквенно-цифровых символов

Когда пользователь запрашивает сетевое соединение, клиент RADIUS, который получает запрос, выполнит начальное согласование доступа с пользователем для получения информации об идентификаторе/пароле. Затем клиент передает информацию на сервер RADIUS как часть запроса аутентификации/авторизации.

Сервер RADIUS сопоставляет данные из запроса аутентификации или авторизации с информацией в доверенной базе данных. Если совпадение найдено и учетные данные пользователя верны, сервер отправляет клиенту сообщение о принятии, что позволяет предоставить доступ. Если совпадения нет или учетные данные неверны, сервер возвращает сообщение об отклонении, отказывая в доступе. После этого устройство сетевого доступа (NAD) устанавливает или разрывает соединение пользователя. Кроме того, NAD может передать учетную информацию на сервер RADIUS для документирования

транзакции. Сервер RADIUS может хранить эту информацию или пересылать ее по мере необходимости для поддержки выставления счетов за предоставленные услуги.

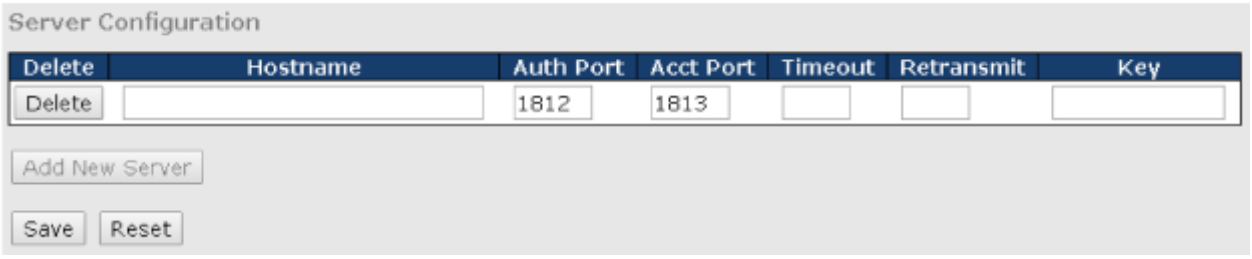


Рисунок 133 – Настройка параметров связи с RADIUS-сервером

Параметр	Описание
Delete	Нажмите, чтобы удалить запись из таблицы
Hostname	Указывает имя хоста сервера RADIUS. Максимальная поддерживаемая длина имени хоста AAA RADIUS составляет 40 символов
Auth Port	Указывает порт UDP, используемый при подключении к серверу RADIUS для аутентификации. Значение по умолчанию – 1812
Acct Port	Указывает порт UDP, используемый при подключении к серверу RADIUS для учета и регистрации действий пользователей. Если порт установлен на 0 (ноль), устройство будет использовать стандартный порт по умолчанию 1813
Key	Общий секретный ключ между коммутатором и сервером RADIUS
Timeout	Время ожидания ответа сервера RADIUS
Retransmit	Количество попыток коммутатора подключиться к серверу RADIUS

- **Обзор серверов RADIUS**

На этой странице представлена информация о состоянии серверов RADIUS, которые были настроены на странице [Server Configuration].

Рисунок 134 – Список серверов аутентификации RADIUS

Параметр	Описание
#	Номер сервера RADIUS. Нажмите, чтобы перейти к подробной статистике сервера
IP Address	IP-адрес и номер UDP-порта сервера в формате <IP-адрес>:<UDP-порт>
Status	Текущее состояние сервера. Это поле может иметь одно из следующих значений: **Disabled**: сервер отключен **Not Ready**: сервер включен, но IP-связь еще не запущена **Ready**: сервер включен, IP-связь настроена, и модуль RADIUS готов принимать попытки доступа **Dead (X seconds left)**: к этому серверу предпринимаются попытки доступа, но он не отвечает в течение настроенного времени ожидания. Сервер временно отключен, но будет снова включен, когда истечет время простоя. Количество секунд, оставшихся до включения, отображается в скобках. Это состояние доступно только при наличии более одного активного сервера

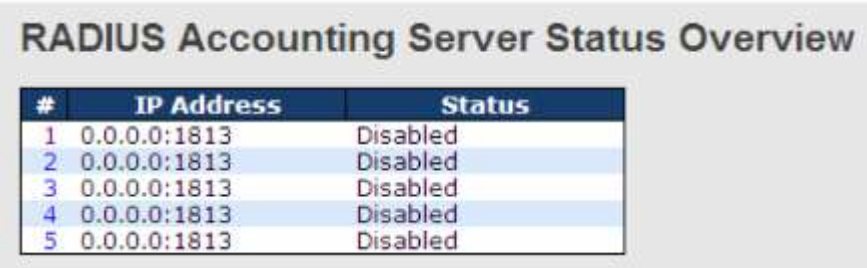


Рисунок 135 – Список серверов учета RADIUS

Параметр	Описание
#	Номер сервера RADIUS. Нажмите, чтобы перейти к подробной статистике сервера
IP Address	IP-адрес и номер UDP-порта сервера в формате <IP-адрес>:<UDP-порт>
Status	Текущее состояние сервера. Это поле может иметь одно из следующих значений: **Disabled**: сервер отключен

	Not Ready: сервер включен, но IP-связь еще не запущена **Ready**: сервер включен, IP-связь настроена, и модуль RADIUS готов принимать попытки доступа **Dead (X seconds left)**: к этому серверу предпринимаются попытки доступа, но он не отвечает в течение настроенного времени ожидания. Сервер временно отключен, но будет снова включен, когда истечет время простоя. Количество секунд, оставшихся до включения, отображается в скобках. Это состояние достижимо только при наличии более одного активного сервера

➢ **Подробные сведения о RADIUS**

На этой странице отображается статистика доступа к серверам аутентификации и учета. Используйте раскрывающийся список серверов для переключения между серверами и отображения соответствующих сведений.

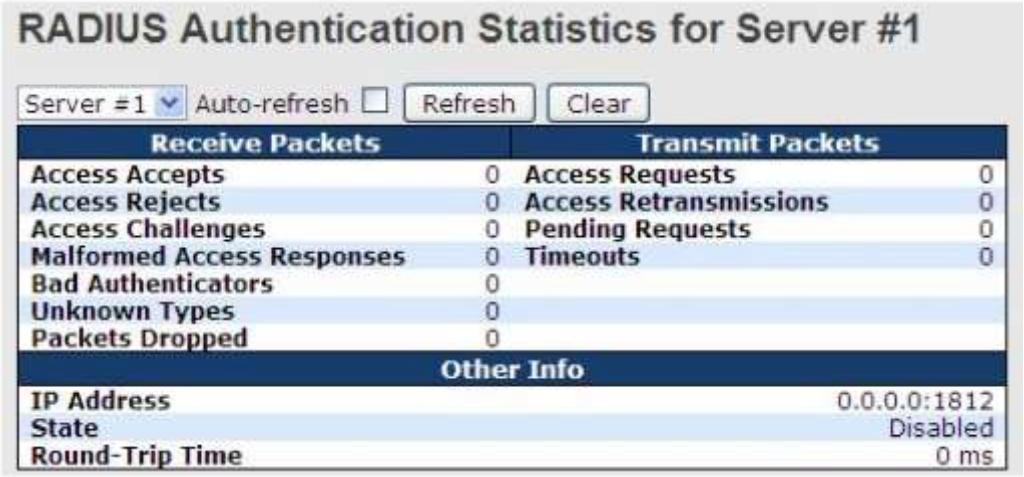


Рисунок 136 – Статистика аутентификаций сервера RADIUS

Параметр	Описание
Receive Packets	Отображает статистику полученных пакетов, включая: **Access Accepts**: количество пакетов разрешения доступа Access-Accept (действительных или недействительных), полученных от сервера **Access Rejects**: количество пакетов отказа в доступе Access-Reject (действительных или недействительных), полученных от сервера **Access Challenges**: количество пакетов запроса на ввод дополнительной информации Access-Challenge (действительных или недействительных), полученных от сервера

	Malformed Access Responses: количество неправильно сформированных пакетов ответа на запрос доступа Access-Response, полученных от сервера. К ним относятся пакеты с недопустимой длиной. Неверные аутентификаторы, атрибуты аутентификатора сообщения или неизвестные типы не включаются в этот подсчет **Bad Authenticators**: количество пакетов Access-Response, содержащих недопустимые аутентификаторы или атрибуты аутентификатора сообщения, полученных от сервера **Unknown Types**: количество пакетов неизвестного типа, полученных от сервера **Packets Dropped**: количество пакетов, полученных от сервера на порту аутентификации и отброшенных по какой-либо причине
Transmit Packets	Отображает статистику переданных пакетов, включая: **Access Requests**: количество пакетов запроса доступа Access-Request, отправленных на сервер. Подсчет не включает повторные передачи **Access Retransmissions**: количество пакетов Access-Request, повторно переданных на сервер аутентификации RADIUS **Pending Requests**: количество пакетов Access-Request, предназначенных для сервера, для которых еще не истекло время ожидания или не получен ответ. Эта переменная увеличивается, когда отправляется очередной пакет Access-Request, и уменьшается при получении пакетов Access-Accept, Access-Reject, Access-Challenge, а также из-за тайм-аута или повторной передачи **Timeouts**: количество таймаутов аутентификации на сервере. По истечении времени ожидания клиент может повторить попытку обращения к тому же серверу, отправить запрос на другой сервер или отказаться от дальнейших запросов. Повторная попытка обращения к тому же серверу считается как повторной передачей, так и тайм-аутом. Отправка на другой сервер считается как запросом, так и тайм-аутом
Other Info	В этом разделе содержится информация о состоянии сервера и длительности задержки коммуникации между сервером и клиентом **IP-Address**: IP-адрес и номер порта UDP (в формате <IP-адрес>:<UDP-порт>) сервера **State**: показывает состояние сервера. Может принимать одно из следующих значений **Disabled**: сервер отключен **Not Ready**: сервер включен, но IP-связь еще не запущена **Ready**: сервер включен, IP-связь настроена, и модуль RADIUS готов принимать попытки доступа

	Dead (X seconds left): к этому серверу предпринимаются попытки доступа, но он не отвечает в течение настроенного времени ожидания. Сервер временно отключен, но будет снова включен, когда истечет время простоя. Количество секунд, оставшихся до включения, отображается в скобках. Это состояние достижимо только при наличии более одного активного сервера **Round-Trip Time**: интервал времени (измеряется в миллисекундах), которое прошло с момента получения ответа или запроса от сервера RADIUS до следующего запроса от клиента, который соответствует полученному ответу или запросу. Измерение имеет разрешение в 100 миллисекунд. Значение 0 миллисекунд указывает на то, что пока не было совершено двустороннего обмена сообщениями с сервером

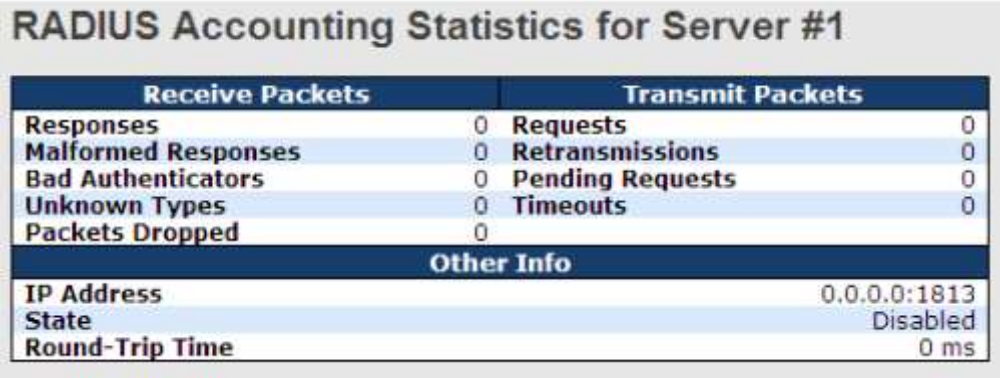


Рисунок 137 – Статистика учета сервера RADIUS

Параметр	Описание
Receive Packets	Отображает статистику полученных пакетов, включая: **Responses**: количество пакетов RADIUS (действительных или недействительных), полученных от сервера **Malformed Responses**: количество неправильно сформированных пакетов RADIUS, полученных от сервера. К ним относятся пакеты с недопустимой длиной. Пакеты с неверными аутентификаторами и пакеты неизвестных типов не включаются в этот подсчет **Bad Authenticators**: количество пакетов RADIUS, содержащих недопустимые аутентификаторы, полученных от сервера **Unknown Types**: количество пакетов неизвестного типа, полученных от сервера на порту учета **Packets Dropped**: количество пакетов, полученных от сервера на порту учета и отброшенных по какой-либо причине

Transmit Packets	Отображает статистику переданных пакетов, включая: **Requests**: количество пакетов RADIUS, отправленных на сервер. Подсчет не включает повторные передачи **Retransmissions**: количество пакетов RADIUS, повторно переданных на сервер учета RADIUS **Pending Requests**: количество пакетов RADIUS, предназначенных для сервера, для которых еще не истекло время ожидания или не получен ответ. Эта переменная увеличивается, когда отправляется очередной пакет Request, и уменьшается при получении пакетов Response, а также из-за тайм-аута или повторной передачи **Timeouts**: количество таймаутов учета на сервере. По истечении времени ожидания клиент может повторить попытку обращения к тому же серверу, отправить запрос на другой сервер или отказаться от дальнейших запросов. Повторная попытка обращения к тому же серверу считается как повторной передачей, так и тайм-аутом. Отправка на другой сервер считается как запросом, так и тайм-аутом
Other Info	В этом разделе содержится информация о состоянии сервера и длительности задержки коммуникации между сервером и клиентом **IP-Address**: IP-адрес и номер порта UDP (в формате <IP-адрес>:<UDP-порт>) сервера **State**: показывает состояние сервера. Может принимать одно из следующих значений: **Disabled**: сервер отключен **Not Ready**: сервер включен, но IP-связь еще не запущена **Ready**: сервер включен, IP-связь настроена, и модуль RADIUS готов принимать данные от клиента **Dead (X seconds left)**: попытки передачи данных на сервер предпринимаются, но он не отвечает в течение настроенного времени ожидания. Сервер временно отключен, но будет снова включен, когда истечет время простоя. Количество секунд, оставшихся до включения, отображается в скобках. Это состояние достижимо только при наличии более одного активного сервера **Round-Trip Time**: интервал времени (измеряется в миллисекундах), необходимый для завершения полного обмена соответствующими сообщениями с сервером учёта RADIUS. Измерение имеет разрешение в 100 миллисекунд. Значение 0 миллисекунд указывает на то, что пока не было совершено двустороннего обмена сообщениями с сервером

5.10.5 NAS (802.1x)

NAS (Network Access Server) – это шлюз доступа между внешней сетью связи и внутренней сетью. Например, когда пользователь посылает запрос интернет-провайдеру, ему будет предоставлен доступ в Интернет после авторизации сервером доступа. Аутентификация между клиентом и сервером может быть на основе IEEE 802.1X и MAC-адреса.

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 внутренних серверов (RADIUS) определяют, разрешен ли пользователю доступ к сети.

Аутентификация на основе MAC-адресов позволяет аутентифицировать более одного пользователя на одном порту и не требует от пользователей установки специального программного обеспечения 802.1X в их системе. Для аутентификации на внутреннем сервере коммутатор использует MAC-адреса пользователей. Поскольку злоумышленники могут создавать поддельные MAC-адреса, такая аутентификация менее безопасна, чем аутентификация 802.1X.

5.10.5.1 Обзор аутентификации 802.1X (на основе портов)

В сетевой среде 802.1X пользователь является соискателем, или запрашивающим. Коммутатор – аутентификатором, а сервер RADIUS – сервером аутентификации. Коммутатор действует как посредник, пересылая запросы и ответы между запрашивающим устройством и сервером аутентификации. Кадры, отправляемые между запрашивающим и коммутатором, являются специальными кадрами 802.1X, известными как кадры EAPOL (EAP Over LAN), которые инкапсулируют EAP PDU (RFC3748). Кадры, отправляемые между коммутатором и сервером RADIUS, являются пакетами RADIUS. Пакеты RADIUS также инкапсулируют EAP PDU вместе с другими атрибутами, такими как IP-адрес коммутатора, имя и номер порта соискателя на коммутаторе. EAP очень гибок, поскольку допускает различные методы аутентификации, такие как MD5-Challenge, PEAP и TLS. Важно то, что аутентификатору (коммутатору) не нужно знать, какой метод аутентификации используют запрашивающее устройство и сервер аутентификации, или сколько кадров обмена информацией необходимо для конкретного метода. Коммутатор просто инкапсулирует часть EAP кадра в соответствующий тип (EAPOL или RADIUS) и пересылает его.

После завершения аутентификации сервер RADIUS отправляет специальный пакет, содержащий указание на успех или неудачу. Помимо пересылки результата запрашивающему устройству, коммутатор использует его для открытия или блокировки трафика на порту коммутатора, подключенном к запрашивающему устройству.

После завершения аутентификации сервер RADIUS отправляет специальный пакет, содержащий указание на успех или неудачу. Помимо пересылки результата запрашивающему устройству, коммутатор использует его для открытия или блокировки трафика на порту коммутатора, подключенном к запрашивающему устройству.

В среде с двумя активными серверами бэкенда, где время ожидания сервера настроено на X секунд, и первый сервер в списке временно недоступен (но не считается полностью

неработоспособным), если запрашивающий будет отправлять кадры EAPOL Start быстрее, чем каждые X секунд, он никогда не сможет пройти аутентификацию.

Это происходит потому, что коммутатор отменяет текущие запросы к серверу аутентификации, как только получает новый EAPOL Start фрейм от запрашивающего устройства. Поскольку сервер не считается неработоспособным (потому что X секунд еще не истекло), коммутатор снова попытается связаться с тем же сервером при следующем запросе аутентификации.

Таким образом, возникает бесконечный цикл. Чтобы избежать этой ситуации, время ожидания сервера должно быть меньше, чем скорость, с которой запрашивающий отправляет пакеты EAPOL Start.

5.10.5.2 Обзор аутентификации на основе MAC-адресов

В отличие от 802.1X, аутентификация на основе MAC-адресов не является стандартом, а всего лишь передовым методом, принятым в отрасли. При аутентификации на основе MAC-адресов пользователи называются клиентами, а коммутатор действует как запрашивающий от имени клиентов. Начальный кадр (любой тип кадра), отправленный клиентом, отслеживается коммутатором, который, в свою очередь, использует MAC-адрес клиента как имя пользователя и пароль 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 в качестве разделителя между шестнадцатеричными цифрами в нижнем регистре используется дефис (-). Коммутатор поддерживает только метод аутентификации MD5-Challenge, поэтому сервер RADIUS должен быть настроен соответствующим образом.

После завершения аутентификации сервер RADIUS отправляет сообщение об успехе или неудаче, которое, в свою очередь, заставляет коммутатор открыть или заблокировать трафик для этого конкретного клиента, используя статические записи в таблице MAC-адресов. Только после этого кадры от клиента будут пересылаться на коммутатор. В этой аутентификации нет кадров EAPOL, и поэтому аутентификация на основе MAC-адресов не имеет ничего общего со стандартом 802.1X.

Преимущество аутентификации на основе MAC по сравнению с 802.1X заключается в том, что несколько клиентов могут быть подключены к одному и тому же порту (например, через сторонний коммутатор или концентратор) и по-прежнему требовать индивидуальной аутентификации, а также что клиентам не требуется для нее специальное программное обеспечение. Недостатком является то, что MAC-адреса могут быть подделаны злонамеренными пользователями. Кроме того, оборудование, MAC-адрес которого является допустимым пользователем RADIUS, может использоваться кем угодно, и поддерживается только метод MD5-Challenge.

Аутентификация 802.1X и аутентификация на основе MAC-адресов имеют конфигурации, которые делятся на системные и портовые настройки.

5.10.5.3 Настройки

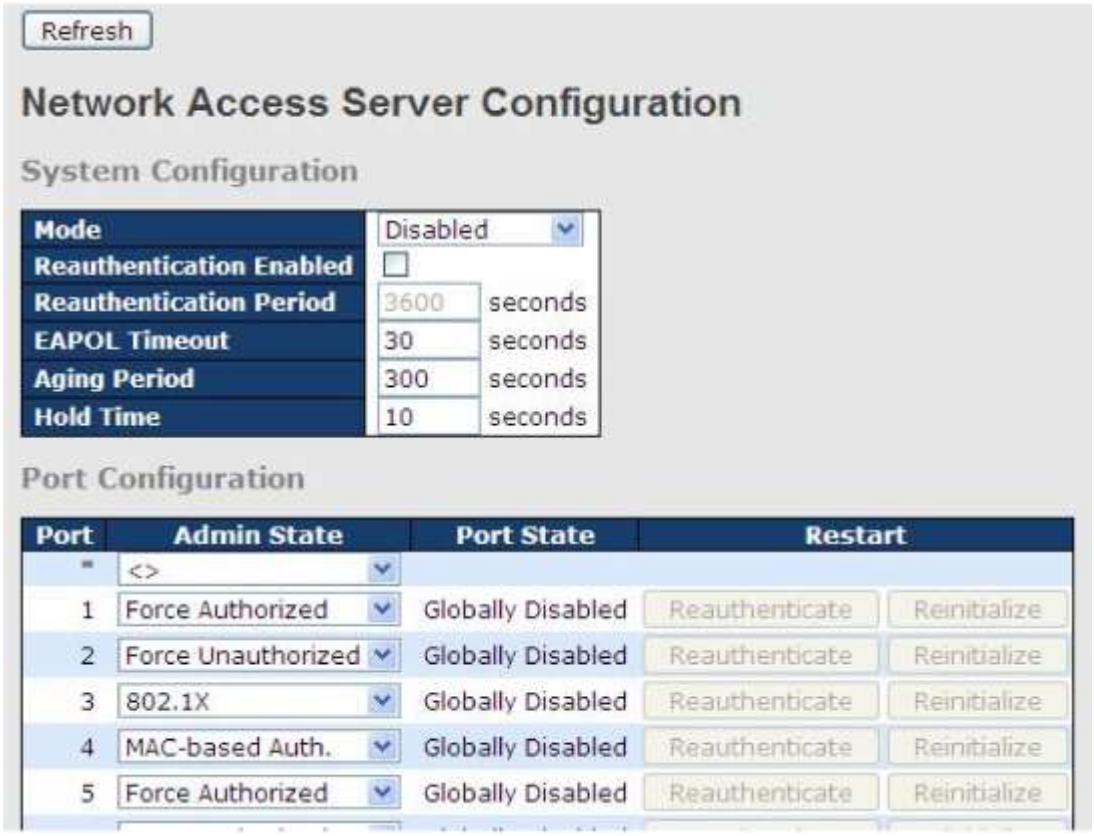


Рисунок 138 – Конфигурация NAS

Параметр	Описание
Mode	Указывает, включена или отключена глобально аутентификация 802.1X и MAC на коммутаторе. Если отключено глобально (**Disabled**), всем портам разрешено пересылать кадры
Reauthentication Enabled	Если этот флажок установлен, клиенты повторно аутентифицируются после интервала, указанного в поле **Reauthentication Period**. Повторная аутентификация для портов с поддержкой 802.1X может использоваться для обнаружения того, подключено ли новое устройство к порту коммутатора. Для портов с аутентификацией на основе MAC эта функция полезна только в случае изменения конфигурации сервера RADIUS. Она не подразумевает связь между коммутатором и клиентом и, следовательно, не подразумевает, что клиент все еще присутствует на порту (см. **Aging Period** ниже)
Reauthentication Period	Определяет период в секундах, после которого подключенный клиент должен пройти повторную аутентификацию. Настройка активна только если установлен флажок **Reauthentication Enabled**. Допустимый диапазон значений – от 1 до 3600 секунд

EAPOL Timeout	Определяет интервал для повторной передачи кадров EAPOL с запросом идентификации Допустимый диапазон значений – от 1 до 65535 секунд. Это не влияет на порты с аутентификацией на основе MAC
Aging Period	Период устаревания. Применяется к режимам, использующим функциональность Port Security для защиты MAC-адресов: **MAC-Based Auth.** Когда модуль NAS использует модуль Port Security для защиты MAC-адресов, модулю Port Security необходимо проверять активность на соответствующем MAC-адресе через регулярные интервалы и освобождать ресурсы, если в течение заданного периода времени не наблюдается никакой активности. Параметр **Aging Period** управляет именно этим периодом и может быть установлен в диапазоне от 10 до 1000000 секунд Для портов в режиме **MAC-based Auth.** повторная аутентификация не вызывает прямых соединений между NAS и клиентом, поэтому он не будет определять, подключен ли клиент или нет, и единственный способ освободить какие-либо ресурсы – это объявить запись устаревшей
Hold Time	Время удержания. Применяется к режимам, использующим функциональность Port Security для защиты MAC-адресов: **MAC-Based Auth.** Если клиенту отказано в доступе – либо потому, что ему отказывает сервер RADIUS, либо потому, что время для запроса сервера RADIUS истекло в соответствии с тайм-аутом, указанным на странице [Configuration] → [Security] → [AAA] – клиент временно переводится в состояние «не авторизован». Таймер удержания не учитывается во время текущей аутентификации Коммутатор будет игнорировать новые кадры, поступающие от клиента в период времени удержания Время удержания может быть установлено в диапазоне от 10 до 1000000 секунд
Port	Номер порта, к которому применяется приведенная ниже конфигурация
Admin State	Если NAS включен глобально, эта настройка управляет режимом аутентификации каждого отдельного порта. Доступны следующие режимы: **Force Authorized**

	В этом режиме коммутатор отправит один кадр EAPOL Success, как только соединение порта будет установлено. Таким образом, любому клиенту на порту разрешается доступ к сети без аутентификации **Force Unauthorized** В этом режиме коммутатор отправит один кадр EAPOL Failure, как только соединение порта будет установлено. Таким образом, любому клиенту на порту запрещается доступ к сети **Port-based 802.1X** Аутентификации 802.1X на основе портов. Подробное описание см. в разделе 5.10.5.1 **a) Single 802.1X** В режиме **Port-based 802.1X** после успешной аутентификации запрашивающего устройства на порту весь порт открывается для сетевого трафика. Это позволяет другим клиентам, соединенным с портом (например, через концентратор), подключаться к успешно аутентифицированному клиенту и получать сетевой доступ, даже если они не аутентифицированы по отдельности. Чтобы преодолеть эту брешь в безопасности, используйте вариант Single 802.1X Single 802.1X пока не является стандартом IEEE, но обладает многими из тех же характеристик, что и 802.1X на основе портов. В Single 802.1X одновременно на порту может быть аутентифицировано не более одного запрашивающего устройства. В коммуникациях между запрашивающим устройством и коммутатором используются обычные кадры EAPOL. Если к порту подключено более одного запрашивающего устройства, то первым будет рассматриваться то, которое придет первым при подключении канала связи. Если этот запрашивающее устройство не предоставит действительные учетные данные в течение определенного времени, шанс будет предоставлен другому запрашивающему устройству. После успешной аутентификации запрашивающего устройства доступ будет разрешен только ему. Это самый безопасный из всех поддерживаемых режимов. В этом режиме для защиты MAC-адреса клиента после успешной аутентификации используется модуль Port Security **б) Multi 802.1X** В этом режиме на одном и том же порту может быть аутентифицировано одновременно одно или несколько запрашивающих устройств. Каждый запрашивающий аутентифицируется индивидуально и защищен в таблице MAC с помощью модуля Port Security В конфигурации Multi 802.1X нельзя использовать мультикастовый MAC-адрес BPDU в качестве целевого MAC-адреса для EAPOL-фреймов, отправляемых коммутатором к запрашивающим

	устройствам. Если использовать мультикастовый MAC-адрес, все клиенты, подключенные к порту, будут отвечать на запросы от коммутатора. Вместо этого коммутатор использует MAC-адрес конкретного клиента, который был получен из первого кадра EAPOL Start или EAPOL Response Identity, отправленного клиентом Исключение составляет случай, когда на порту нет подключенных устройств. В этом случае коммутатор отправляет запросы EAPOL Request Identity с использованием мультикастового MAC-адреса BPDU, чтобы активировать любые потенциальные клиенты на порту Максимальное количество запрашивающих клиентов, которые могут быть подключены к порту, можно ограничить с помощью функции Port Security Limit Control **MAC-based Auth.** Аутентификация на основе MAC-адресов. Подробное описание см. в разделе 5.10.5.2. Максимальное количество запрашивающих клиентов, которые могут быть подключены к порту, можно ограничить с помощью функции Port Security Limit Control
Port State	Текущее состояние порта. Может принимать одно из следующих значений: **Globally Disabled**: NAS глобально отключен **Link Down**: NAS глобально включен, но на порту нет соединения **Authorized**: порт находится в режиме **Force Authorized** или в режиме поддержки одного запрашивающего устройства, и запрашивающее устройство авторизовано **Unauthorized**: порт находится в режиме **Force Unauthorized** или в режиме поддержки одного запрашивающего устройства, и запрашивающее устройство не было успешно авторизовано сервером RADIUS **X Auth/Y Unauth**: порт находится в режиме поддержки нескольких запрашивающих устройств. В настоящее время X клиентов авторизованы, а Y не авторизованы
Restart	Для каждой строки доступны две кнопки. Кнопки активируются только при включенной глобальной аутентификации на основе EAPOL или MAC. Нажатие этих кнопок не приведет к вступлению в силу настроек, измененных на странице **Reauthenticate**: планирует повторную аутентификацию всякий раз, когда заканчивается период молчания порта (аутентификация на основе EAPOL). Для режима на основе MAC повторная аутентификация будет предпринята немедленно

	Кнопка действует только на успешно аутентифицированных клиентов на порту и не приведет к временной потере авторизации клиентов **Reinitialize**: принудительно и немедленно выполняет повторную инициализацию клиентов на порту и, следовательно, повторную аутентификацию. Пока она выполняется клиенты перейдут в неавторизованное состояние

5.10.5.4 Состояние коммутации NAS

На этой странице отображается информация о текущем состоянии портов NAS.

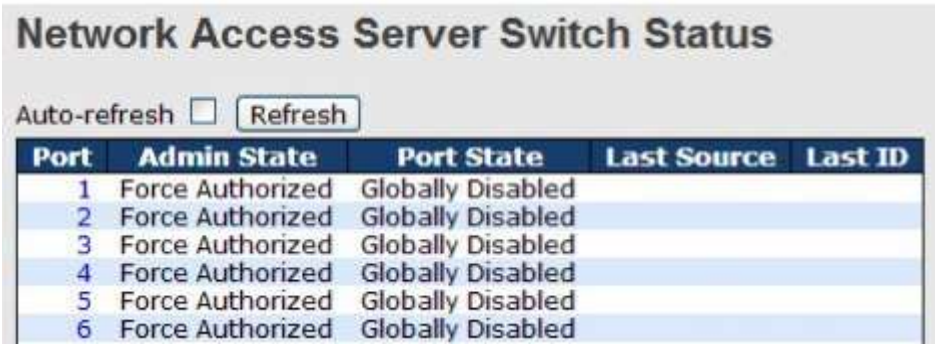


Рисунок 139 – Статус портов NAS

Параметр	Описание
Port	Номер порта коммутатора. Нажмите, чтобы перейти к подробной статистике 802.1X для каждого порта
Admin State	Текущее административное состояние порта. Подробнее о каждом значении см. выше в описании **Admin State** NAS
Port State	Текущее состояние порта. Подробнее о каждом значении см. выше в описании **Port State** NAS
Last Source	MAC-адрес источника, переданный в последнем полученном кадре EAPOL для аутентификации на основе EAPOL и последнем полученном кадре от нового клиента для аутентификации на основе MAC
Last ID	Имя пользователя (идентификатор запрашивающего), содержащееся в последнем полученном кадре EAPOL Response Identity для аутентификации на основе EAPOL, и исходный MAC-адрес из последнего полученного кадра от нового клиента для аутентификации на основе MAC

5.10.5.5 Статистика портов NAS

Эта страница содержит подробную статистику IEEE 802.1X для определенного порта коммутатора, применяющего аутентификацию на основе порта. Для портов с режимом на основе MAC будет показана только статистика выбранного бэкенд-сервера. Используйте раскрывающийся список, чтобы выбрать, какие сведения о порте следует отображать.

Рисунок 140 – Статистика порта NAS

Параметр	Описание
Admin State	Текущее административное состояние порта. Подробнее о каждом значении см. выше в описании **Admin State** NAS
Port State	Текущее состояние порта. Подробнее о каждом значении см. выше в описании **Port State** NAS
EAPOL Counters	Эти счетчики кадров запрашивающего устройства доступны для следующих административных состояний: • **Force Authorized** • **Force Unauthorized** • **802.1X** Входящие кадры: **Total**: количество допустимых кадров EAPOL любого типа, полученных коммутатором **Response ID**: количество допустимых кадров идентификации EAP Resp/ID, полученных коммутатором **Responses**: количество допустимых кадров ответа EAPOL (кроме кадров Resp/ID), полученных коммутатором **Start**: количество инициализирующих аутентификацию кадров EAPOL Start, полученных коммутатором **Logoff**: количество допустимых кадров выхода из системы EAPOL logoff, полученных коммутатором

	Invalid Type: количество кадров EAPOL, полученных коммутатором, в которых тип кадра не распознан **Invalid Length**: количество кадров EAPOL, полученных коммутатором, имеющих недопустимую длину Исходящие кадры: **Total**: количество кадров EAPOL любого типа, переданных коммутатором **Request ID**: количество кадров начального запроса EAP, переданных коммутатором **Requests**: количество допустимых кадров запроса EAP (кроме кадров начального запроса), переданных коммутатором
Backend Server Counters	Эти счетчики кадров серверной части (RADIUS) доступны для следующих административных состояний: • **802.1X** • **MAC-based Auth.** Входящие кадры: **Access Challenges**: для 802.1X отслеживает, сколько раз коммутатор получил первый запрос от сервера аутентификации после того, как клиентское устройство отправило свой первый ответ. Это показывает, что сервер аутентификации успешно установил связь с коммутатором и начал процесс аутентификации Для MAC-based Auth. подсчитывает все запросы на дополнительную проверку (Access Challenges), которые сервер аутентификации отправляет для данного порта (отображается в левой таблице) или для конкретного клиента (отображается в правой таблице) **Other Requests**: для 802.1X подсчитывает количество раз, когда коммутатор отправляет пакет запроса EAP, следующий за первым, запрашивающему устройству. Указывает, что сервер выбрал метод EAP Для MAC-based Auth. не применяется **Auth. Successes**: для 802.1X и MAC-based Auth. подсчитывает количество раз, когда коммутатор получает сообщение об успешном завершении. Указывает, что соискатель/клиент успешно аутентифицировался на сервере **Auth. Failures**: для 802.1X и MAC-based Auth. подсчитывает количество раз, когда коммутатор получает сообщение о неудаче. Это указывает на то, что соискатель/клиент не прошел аутентификацию на сервере Исходящие кадры:

	Responses: для 802.1X подсчитывает количество попыток коммутатора отправить первый ответный пакет соискателя на бэкенд-сервер. Указывает, что коммутатор пытался связаться с сервером. Возможные повторные передачи не учитываются Для MAC-based Auth. подсчитывает все пакеты сервера, перенаправленные коммутатором на сервер для заданного порта (крайняя левая таблица) или клиента (крайняя правая таблица). Возможные повторные передачи не учитываются
Last Supplicant/Client Info	Информация о последнем соискателе/клиенте, который пытается пройти аутентификацию. Эта информация доступна для следующих административных состояний: • **802.1X** • **MAC-based Auth.** **MAC Address**: MAC-адрес последнего запрашивающего устройства/клиента **VLAN ID**: идентификатор VLAN, на которой был получен последний кадр от последнего запрашивающего устройства/клиента **Version**: для 802.1X номер версии протокола, переданный в последнем полученном кадре EAPOL Для MAC-based Auth. не применяется **Identity**: для 802.1X имя пользователя (идентификация запрашивающего), содержащееся в последнем полученном кадре EAPOL Response Identity Для MAC-based Auth. не применяется

5.11 Предупреждения

5.11.1 Сигнал неисправности

При возникновении любого события, к которому привязаны настройки оповещения, загорается индикатор неисправности на панели коммутатора (см. рисунок 1) и одновременно с этим подается сигнал электрического реле. Следующие страницы позволяют настроить условия оповещения на основе ваших потребностей для отдельных портов коммутатора, включая действия, которые необходимо предпринять при отключении порта и проблемах питания.

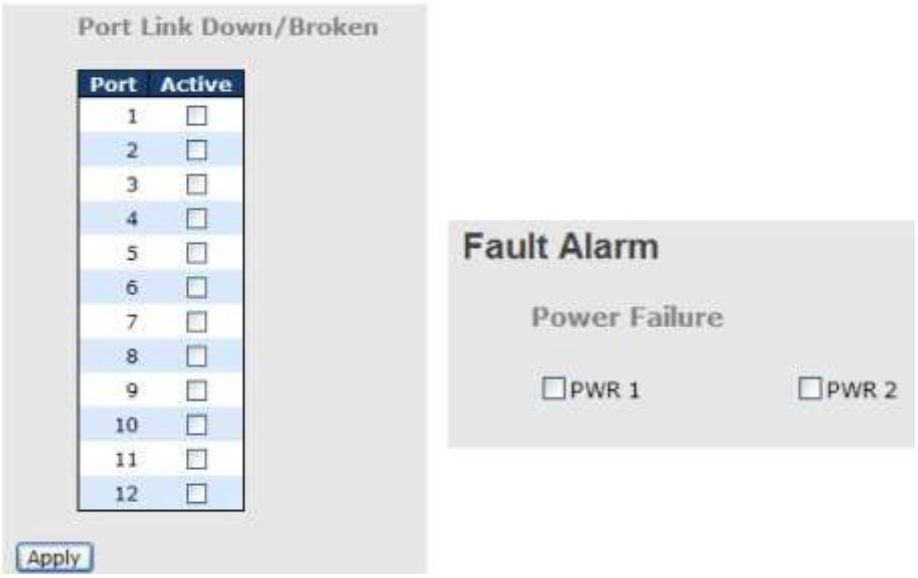


Рисунок 141 – Настройка оповещений о неисправности

5.11.2 Системные предупреждения

5.11.2.1 Настройка SYSLOG

SYSLOG – это протокол, который позволяет устройству отправлять сообщения об событиях через сеть IP на устройства, которые собирают и хранят эти сообщения. Он отделяет программное обеспечение, генерирующее сообщения, от системы, которая их хранит и обрабатывает. Сообщения SYSLOG передаются с помощью UDP, поэтому, если из-за разрыва сети пакет потеряется во время передачи, отправитель и получатель не узнают об этом, и пакет не будет отправлен повторно.

Рисунок 142 – Настройка SYSLOG

Параметр	Описание
Server Mode	Указывает на текущий режим сервера. В режиме **Enabled** сообщение syslog будет отправлено на Syslog-сервер. Протокол основан на UDP-коммуникациях и по умолчанию использует порт UDP 514. Сервер Syslog не будет отправлять подтверждения отправителю, поскольку UDP – это протокол без процедуры установления соединения, и он не

	предоставляет подтверждений. Пакет Syslog будет отправлен в любом случае, даже если сервера не существует. Возможные режимы: **Enabled**: включить сервер **Disabled**: отключить сервер
Server Address	Указывает IPv4-адрес хоста Syslog-сервера. Если коммутатор предоставляет функции DNS, это также может быть имя хоста

5.11.2.2 Настройка SMTP

SMTP (Simple Mail Transfer Protocol) – это протокол для передачи электронной почты через Интернет. При настройке оповещения SMTP устройство будет отправлять уведомление по электронной почте, когда происходит определенное пользователем событие.

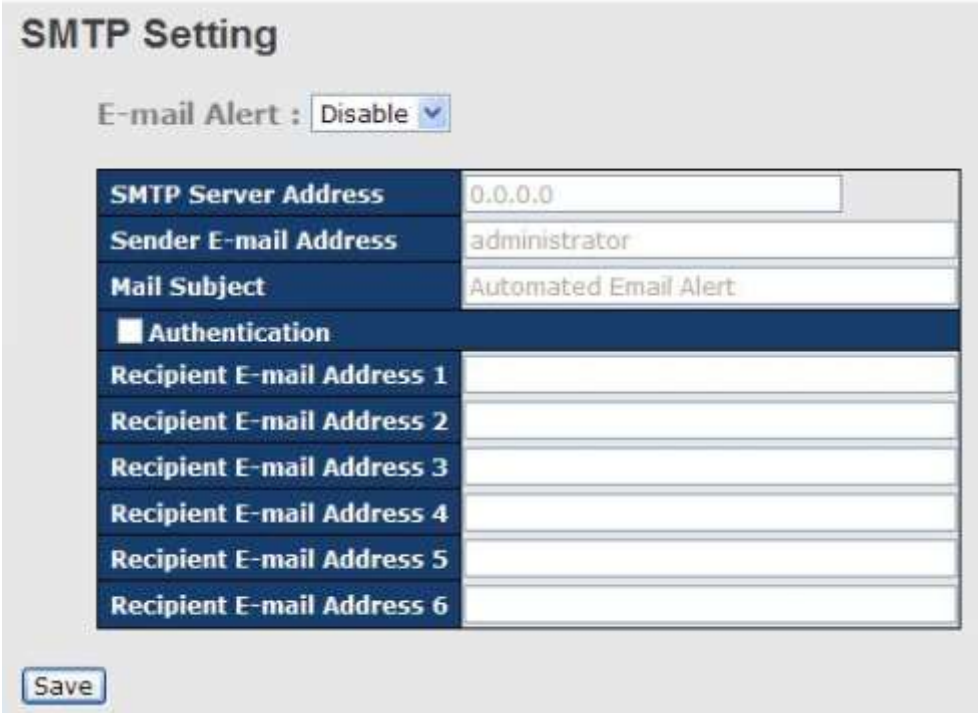


Рисунок 143 – Настройка оповещений по SMTP

Параметр	Описание
E-mail Alarm	Включает или отключает передачу системных предупреждений по электронной почте
Sender E-mail Address	IP-адрес SMTP-сервера
Mail Subject	Тема письма

Authentication	Аутентификация: **Username**: имя пользователя **Password**: пароль для аутентификации **Confirm Password**: введите пароль еще раз
Recipient E-mail Address	Адрес электронной почты получателя. Можно указать до 6 получателей
Apply	Нажмите, чтобы активировать настройки
Help	Показывает файл справки

5.11.2.3 Выбор событий

Устройство поддерживает оповещения SYSLOG и SMTP. Установите соответствующий флажок, чтобы включить нужный вам метод оповещения о системных событиях. Обратите внимание, что флажки будут неактивны, если SYSLOG или SMTP отключены.

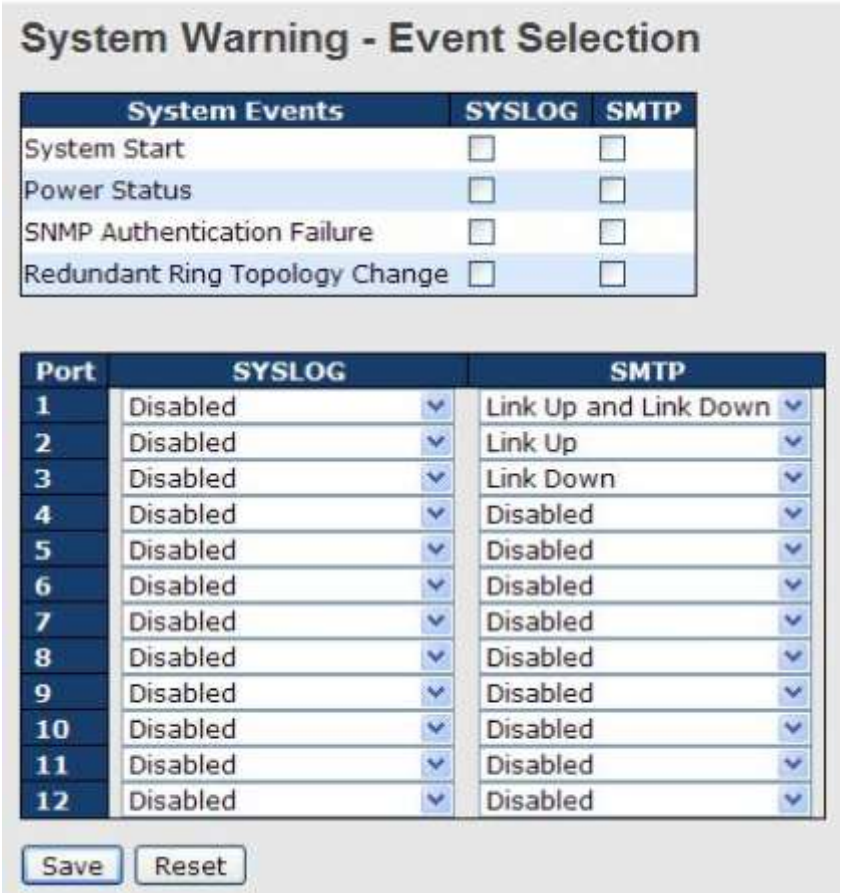


Рисунок 144 – Выбор событий для оповещения

Параметр	Описание
System Cold Start	Отправляет оповещения при перезапуске системы
Power Status	Отправляет оповещения при включении или выключении питания
SNMP Authentication Failure	Отправляет оповещения при сбое аутентификации SNMP
Redundant Ring Topology Change	Отправляет оповещения при изменении топологии Sy-Ring
Port	Номер порта коммутатора
SYSLOG	Событие для оповещения при помощи SYSLOG: **Disabled**: оповещения отключены **Link Up**: включение порта **Link Down**: выключение порта **Link Up & Link Down**: включение и выключение порта
SMTP	Событие для оповещения при помощи SMTP: **Disabled**: оповещения отключены **Link Up**: включение порта **Link Down**: выключение порта **Link Up & Link Down**: включение и выключение порта

5.12 Мониторинг и диагностика

5.12.1 Таблица MAC-адресов

Таблица MAC-адресов – это таблица в сетевом коммутаторе, которая сопоставляет MAC-адреса с портами. Коммутатор использует таблицу для определения того, на какой порт следует пересылать входящий пакет. Записи в таблице MAC-адресов делятся на два типа: динамические и статические. Записи в статической таблице MAC-адресов добавляются или удаляются вручную и не могут устареть сами по себе. Записи в динамической таблице MAC устаревают по истечении настроенного периода времени. Такие записи можно добавлять автоматически, путем обучения, или при помощи ручной настройки.

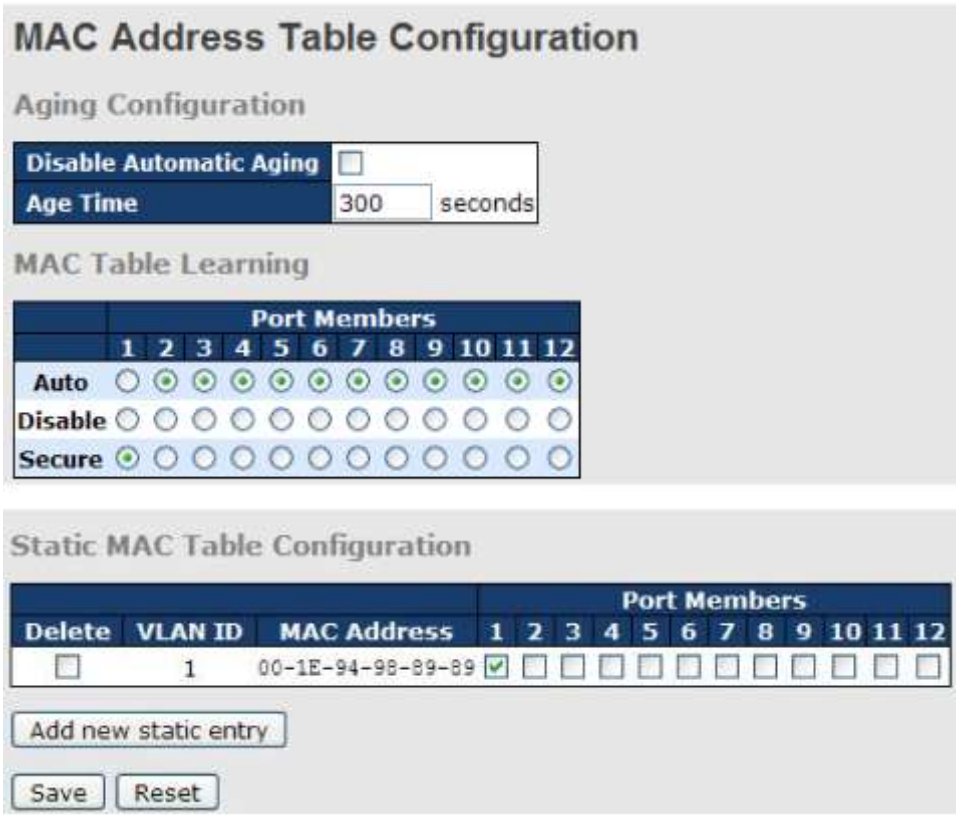


Рисунок 145 – Конфигурация таблицы MAC-адресов

➢ **Настройка времени устаревания**

Функция устаревания MAC-адресов позволяет коммутатору отслеживать только активные адреса в сети и удалять те, которые больше не используются, постоянно поддерживая актуальность таблицы. По умолчанию устаревшие записи удаляются через 300 секунд. Вы можете настроить время устаревания, введя значение в поле «Age Time» в секундах. Допустимый диапазон составляет от 10 до 1000000 секунд. Вы также можете отключить автоматическое устаревание динамических записей, установив флажок «Disable Automatic Aging».

➢ **Обучение таблицы MAC-адресов**

Если адреса не существует в таблице, коммутатор может добавить адрес и порт, на котором был получен пакет, в таблицу MAC-адресов, путем проверки исходного адреса каждого полученного пакета. Эта функция называется обучением. Она позволяет таблице MAC-адресов динамически расширяться. Если режим обучения для данного порта неактивен, это означает, что режимом управляет другой модуль, и, таким образом, пользователь не может изменить конфигурации. Примером такого модуля является аутентификация на основе MAC-адресов в соответствии с 802.1X.

Рисунок 146 – Настройка обучения

Параметр	Описание
Auto	Обучение выполняется автоматически, как только получен кадр с неизвестным MAC-адресом источника
Disable	Обучение не выполняется
Secure	Изучаются только статические записи MAC, все остальные кадры отбрасываются. Прежде чем переходить в безопасный режим обучения, необходимо убедиться, что связь, используемая для управления коммутатором, добавлена в статическую таблицу. В противном случае канал управления будет потерян и может быть восстановлен только с помощью другого незащищенного порта или путем подключения к коммутатору через последовательный интерфейс

- **Настройка статических MAC-адресов**

Эта страница показывает статические записи в таблице MAC-адресов, которая может содержать до 64 записей. Использование статических записей MAC-адресов может значительно сократить широковещательные пакеты и подходит для сетей, где сетевые устройства редко меняются. Вы можете управлять записями на этой странице. Таблица MAC-адресов сортируется сначала по идентификатору VLAN, а затем по MAC-адресу.

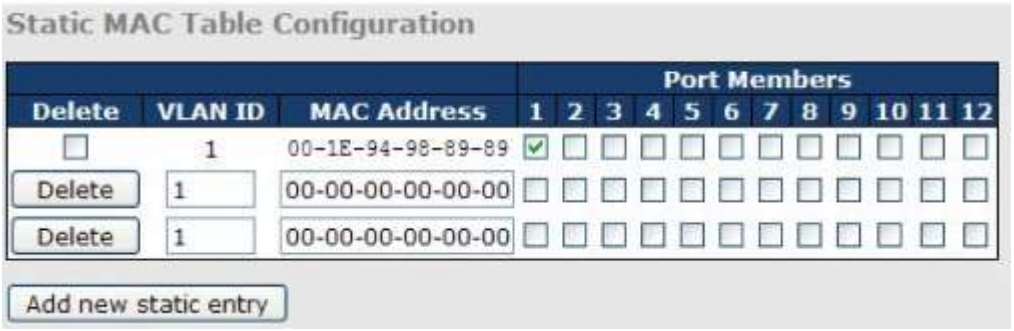


Рисунок 147 – Настройка записей статических MAC-адресов

Параметр	Описание
Delete	Отмеченная запись будет удалена при следующем сохранении
VLAN ID	Номер VLAN, которой соответствует запись
MAC Address	MAC-адрес
Port Members	Флажки указывают, на каких портах принимаются пакеты от указанного MAC-адреса. Отметьте или снимите отметку, чтобы изменить запись
Add new static entry	Нажмите, чтобы добавить новую запись в таблицу статических MAC-адресов. Вы можете указать VLAN ID, MAC-адрес и порты-участники для новой записи. Нажмите <Save>, чтобы сохранить изменения

- **Просмотр таблицы MAC-адресов**

На каждой странице отображается до 999 записей из таблицы MAC-адресов, при этом значение по умолчанию равно 20. Изменить его можно в поле ввода «entries per page». При первом посещении веб-страница покажет начальные 20 записей таблицы MAC-адресов. Первой будет отображена запись с наименьшим VLAN ID и наименьшим MAC-адресом, найденным в таблице.

Поля «Start from VLAN and MAC address» позволяют пользователю выбрать начальную точку в таблице. Нажатие кнопки <Refresh> обновит отображаемую таблицу, начиная с прежней записи или ближайшей следующей. Кроме того, два поля ввода после нажатия <Refresh> примут значение первой отображаемой записи, что позволяет выполнять непрерывное обновление с тем же начальным адресом. Кнопка >> будет использовать последнюю запись из отображаемых в данный момент пар VLAN/MAC в качестве основы для следующего поиска. Когда поиск подойдет к концу, в отображаемой таблице отобразится текст «no more entries» (больше записей нет). Используйте кнопку |<<, чтобы начать заново.

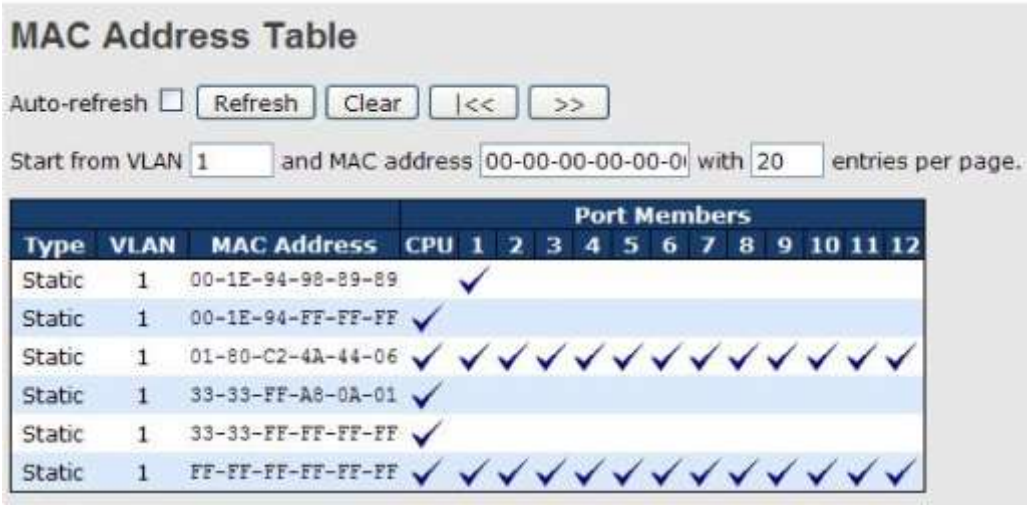


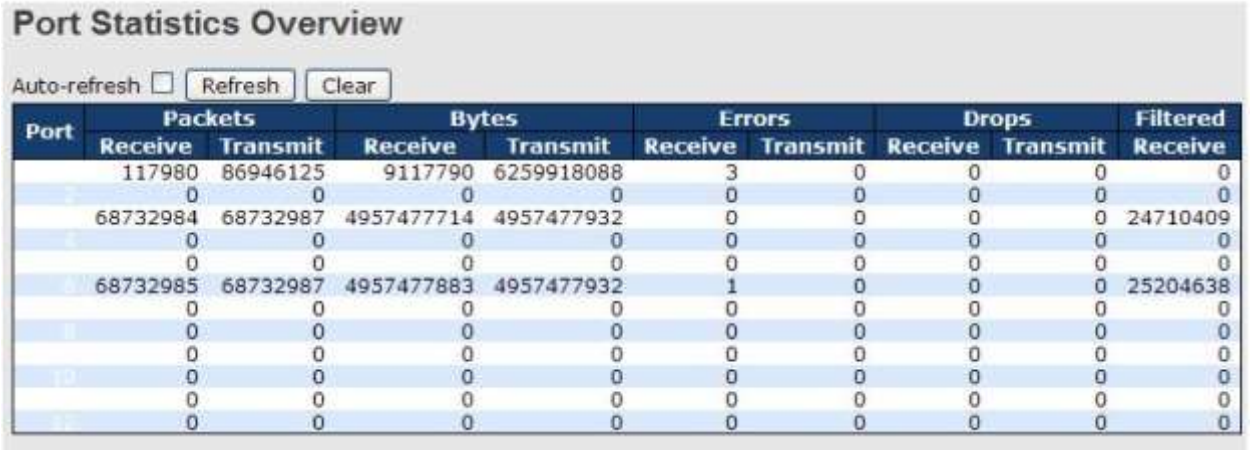
Рисунок 148 – Отображение таблицы MAC-адресов

Параметр	Описание
Type	Указывает, является ли запись статической или динамической
VLAN	VLAN ID записи
MAC Address	MAC-адрес записи
Port Members	Порты-участники данной записи

5.12.2 Статистика портов

➢ **Обзор трафика**

На этой странице представлен обзор общей статистики трафика для всех портов коммутатора.



Port	Packets		Bytes		Errors		Drops		Filtered
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive
	117980	86946125	9117790	6259918088	3	0	0	0	0
	0	0	0	0	0	0	0	0	0
	68732984	68732987	4957477714	4957477932	0	0	0	0	24710409
	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0
	68732985	68732987	4957477883	4957477932	1	0	0	0	25204638
	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0

Рисунок 149 – Общая статистика портов

Параметр	Описание
Port	Номер порта коммутатора
Packets	Количество полученных и переданных пакетов
Bytes	Количество полученных и переданных байтов
Errors	Количество кадров, полученных с ошибкой, и количество незавершенных передач
Drops	Количество кадров, отброшенных из-за перегрузки на входе или выходе

Filtered	Количество полученных кадров, отфильтрованных процессом пересылки
Auto-refresh	Установите флажок, чтобы включить автоматическое обновление страницы через регулярные интервалы
Refresh	Немедленно обновляет записи счетчиков, начиная с текущего идентификатора записи
Clear	Очищает все записи счетчиков

- **Подробная статистика**

Эта страница содержит подробную статистику трафика для определенного порта коммутатора. Используйте раскрывающийся список портов, чтобы решить, данные какого порта коммутатора следует отобразить.

Отображаемые поля включают количество принятых и переданных пакетов, их суммарный размер в байтах, а также ошибки приема и передачи.

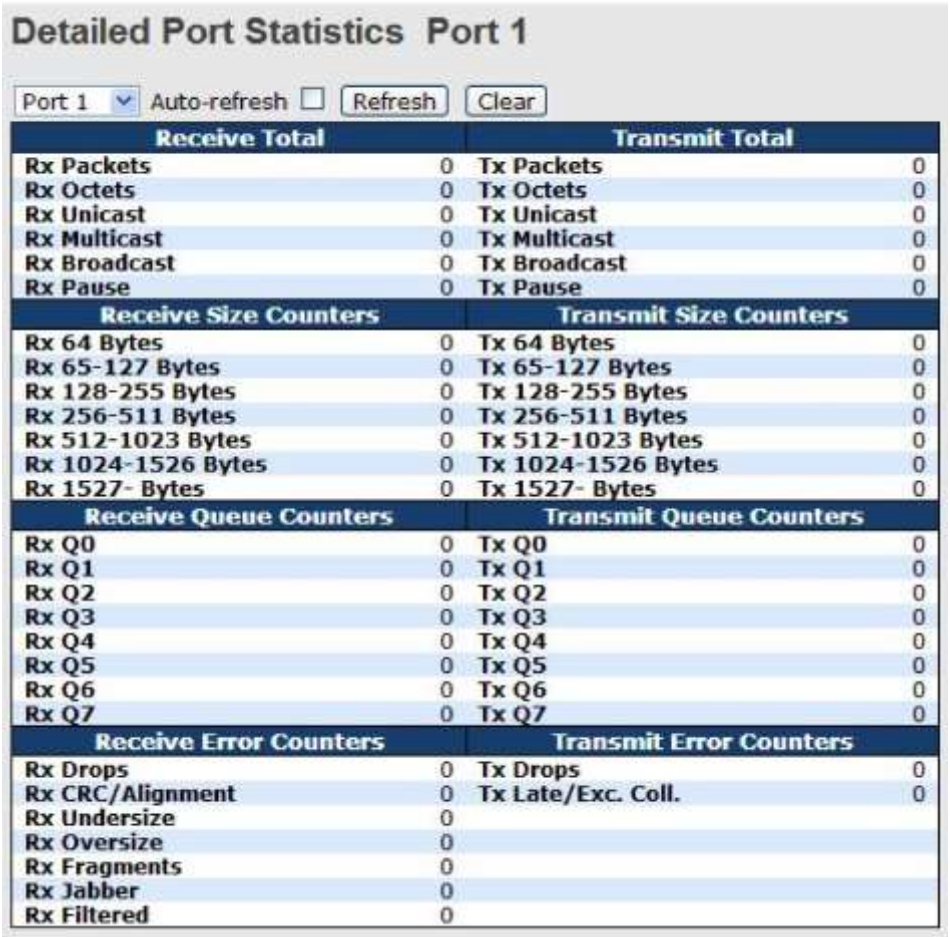


Рисунок 150 – Подробная статистика порта

Параметр	Описание
Rx and Tx Packets	Количество всех полученных и переданных пакетов
Rx and Tx Octets	Количество всех полученных и переданных байтов, включая FCS, за исключением кадрирующих битов
Rx and Tx Unicast	Количество всех полученных и переданных одноадресных пакетов
Rx and Tx Multicast	Количество всех полученных и переданных многоадресных пакетов
Rx and Tx Broadcast	Количество всех полученных и переданных широковещательных пакетов
Rx and Tx Pause	Количество кадров MAC Control, полученных или переданных через этот порт, которые имеют код, указывающий на операцию PAUSE
Rx Drops	Количество кадров, потерянных из-за недостаточного буфера приема или перегрузки на выходе
Rx CRC/Alignment	Количество кадров, полученных с ошибками CRC или выравнивания
Rx Undersize	Количество кадров short[1], полученных с допустимым CRC
Rx Oversize	Количество кадров long[2], полученных с допустимым CRC
Rx Fragments	Количество кадров short, полученных с недопустимым CRC
Rx Jabber	Количество кадров long, полученных с недопустимым CRC
Rx Filtered	Количество полученных кадров, отфильтрованных процессом пересылки
Tx Drops	Количество кадров, отброшенных из-за переполнения выходного буфера
Tx Late / Exc.Coll.	Количество кадров, которые были отправлены с опозданием или с ошибками коллизии

[1] короткие кадры размером менее 64 байт.

[2] длинные кадры, превышающие максимальную длину, настроенную для кадров этого порта.

5.12.3 Зеркалирование портов

Функция зеркалирования копирует трафик одного порта на другой порт того же коммутатора, чтобы сетевой анализатор, подключенный к зеркальному порту, мог отслеживать и анализировать пакеты. Функция полезна для устранения неполадок. Трафик, который нужно скопировать на зеркальный порт, может включать все полученные кадры (зеркалирование трафика источника, или входящее зеркалирование), или все кадры, переданные портом (зеркалирование целевого трафика, или исходящее зеркалирование). Порт, на который копируется отслеживаемый трафик, называется зеркальным портом.

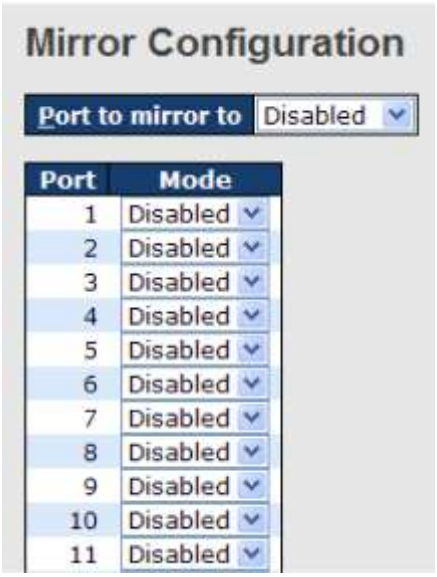


Рисунок 151 – Настройка зеркалирования

Параметр	Описание
Port to mirror to	Номер порта зеркалирования
Port	Номер порта коммутатора, к которому будут применены следующие настройки
Mode	Раскрывающийся список для выбора режима зеркалирования **Rx only**: только кадры, полученные на этом порту, зеркалируются на порт зеркалирования. Переданные кадры не зеркалируются **Tx only**: зеркалируются только кадры, переданные с этого порта. Полученные кадры не зеркалируются **Disabled**: ни переданные, ни полученные кадры не зеркалируются **Enabled**: зеркалируются как полученные, так и переданные кадры

5.12.4 Информация системного журнала

Страница [System Log Information] предоставляет информацию системного журнала коммутатора.

Рисунок 152 – Просмотр системного журнала

Параметр	Описание
Auto-refresh	Установите этот флажок, чтобы включить автоматическое обновление страницы через регулярные интервалы
Refresh	Обновляет записи системного журнала, начиная с текущего ID
Clear	Очищает все записи системного журнала
|<<	Обновляет записи системного журнала, начиная с первого доступного идентификатора записи
<<	Обновляет записи системного журнала, заканчивая последним ID
>>	Обновляет записи системного журнала, начиная с последней отображаемой в данный момент записи
>>|	Обновляет записи системного журнала, заканчивая последней доступной записью
ID	Идентификатор (>= 1) записи в системном журнале
Level	Уровень записи системного журнала. Поддерживаются следующие уровни: **Info**: предоставляет общую информацию **Warning**: предоставляет предупреждение о ненормальной работе **Error**: предоставляет сообщение об ошибке

	All: включает все уровни
Time	Время записи в системном журнале
Message	Информация о событии

5.12.5 Диагностика кабеля

Вы можете выполнить диагностику кабеля для всех или для выбранных портов, чтобы обнаружить любые неисправности кабеля (короткое замыкание, обрыв и т. д.) и определить расстояние до места повреждения. На странице [VeriPHY Cable Diagnostics] выберите порт из раскрывающегося списка и нажмите <Start>, чтобы запустить диагностику. Это займет около 5 секунд. Если выбраны все порты, может потребоваться около 15 секунд. После завершения страница автоматически обновится, и вы сможете просмотреть результаты проверки кабеля в таблице «Cable Status». Обратите внимание, что диагностика VeriPHY точна только для кабелей длиной от 7 до 140 метров. Порты 10 и 100 Мбит/с будут отключены во время выполнения диагностики. Поэтому запуск VeriPHY на порту управления 10 или 100 Мбит/с приведет к тому, что коммутатор перестанет отвечать, пока не будет завершена процедура диагностики.

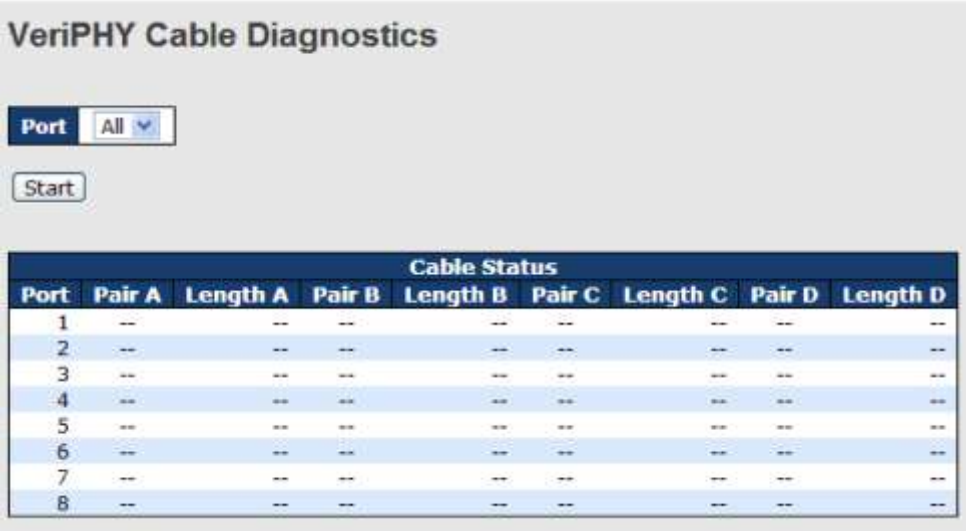


Рисунок 153 – Диагностика кабеля

Параметр	Описание
Port	Порт, для которого запрашивается диагностика кабеля VeriPHY
Cable Status	**Port**: номер порта **Pair**: состояние витой пары **Length**: длина кабеля (в метрах)

5.12.6 Мониторинг SFP

SFP-модули с функцией DDM (цифровой диагностический мониторинг) отслеживают свои рабочие параметры, тем самым позволяя контролировать состояние соединения. На странице [SFP Monitor] можно настроить значение температуры модуля, при достижении которой будет сгенерировано тревожное событие.

Рисунок 154 – SFP-мониторинг

5.12.7 Ping

Эта команда отправляет пакеты ICMP-запросов на другой узел сети. Используя команду **ping**, вы можете проверить, работает ли связь с удаленным узлом.

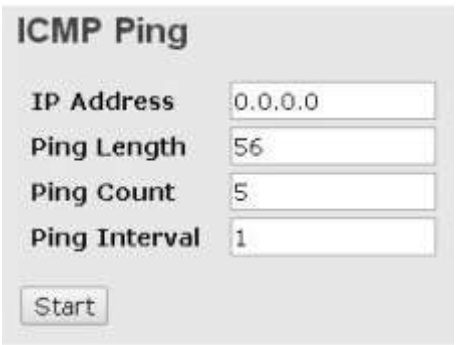


Рисунок 155 – Ping

Параметр	Описание
IP Address	IP-адрес назначения
Ping Length	Размер данных пакета ICMP. Диапазон значений от 8 до 1400 байт
Ping Count	Определяет количество пингов, которые будут отправлены. Введите целое число
Ping Interval	Указывает интервал между пингами, которые отправляются на адрес назначения

После нажатия кнопки <Start> будет передано пять пакетов ICMP. Порядковый номер и время приема-передачи будут отображены после получения ответа. Страница автоматически обновляется до тех пор, пока не будут получены ответы на все пакеты или пока не истечет время ожидания.

PING6 server ::10.10.132.20

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

5.12.8 ICMPv6 Ping

Эта страница позволяет выполнить пинг IPv6-адреса для проверки подключения локального устройства к устройству IPv6.

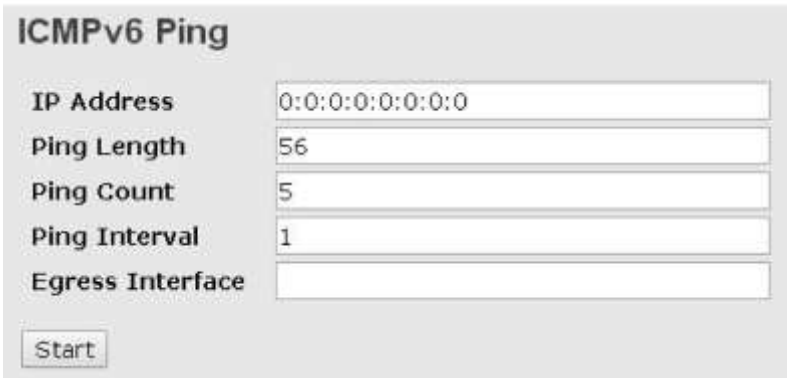


Рисунок 156 – IPv6 Ping

Параметр	Описание
IP Address	IP-адрес назначения. Укажите адрес в шестнадцатеричном формате, используя 16-битные значения между двоеточиями
Ping Length	Размер данных пакета ICMP. Диапазон значений от 8 до 1400 байт
Ping Count	Определяет количество пингов, которые будут отправлены. Введите целое число
Ping Interval	Указывает интервал между пингами, которые отправляются на адрес назначения
Egress Interface	Указывает физический интерфейс, через который можно проверить подключение. Если вы указываете физический интерфейс, например порт Ethernet, вы также должны указать номер порта. Если вы указываете виртуальный интерфейс, например VE, вы должны указать номер, связанный с VE

PING6 server ::192.168.10.1

sendto

sendto

sendto

sendto

sendto

Sent 5 packets, received 0 OK, 0 bad

5.12.9 Тип SFP

На странице [SFP Type] отображаются сведения о SFP-модулях. Для каждого порта в сводке отображается тип SFP, имя производителя и серийный номер.

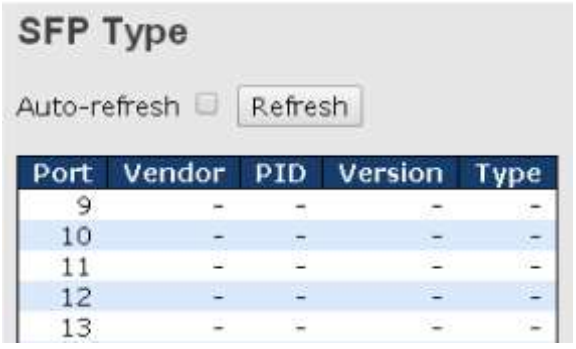


Рисунок 157 – Тип SFP

5.13 Синхронизация

5.13.1 PTP

PTP External Clock Mode – это протокол синхронизации часов по всей компьютерной сети. В локальной сети он достигает точности часов в диапазоне субмикросекунд, что делает его пригодным для систем измерения и управления.

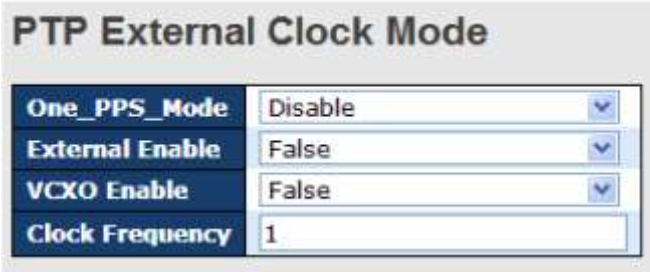


Рисунок 158 – Конфигурация PTP

Параметр	Описание
One_pps_mode	Определяет, как будет использоваться сигнал 1 PPS, который представляет собой импульс, возникающий каждый секунду: **Output**: аппаратное обеспечение будет генерировать и выводить сигнал 1 PPS **Input**: аппаратное обеспечение будет принимать сигнал 1 PPS от другого источника **Disable**: сигнал 1 PPS (и входящий, и исходящий) будет отключен
External Enable	Определяет, будет ли ваше устройство генерировать внешний сигнал синхронизации для других систем или устройств. Значения для этой настройки следующие: **True**: устройство будет генерировать внешний сигнал синхронизации **False**: устройство не будет генерировать внешний сигнал синхронизации
VCXO_Enable	Управляет возможностью внешней настройки частоты генератора времени. Значения для этой настройки следующие: **True**: устройство будет использовать внешние сигналы или команды для корректировки частоты VCXO **False**: устройство не будет использовать внешние сигналы или команды для корректировки частоты VCXO
Clock Frequency	Позволяет установить тактовую частоту. Диапазон значений: 1–25000000 (1–25 МГц)

Рисунок 159 – Настройка часов PTP

Параметр	Описание
Delete	Установите этот флажок и нажмите <Save>, чтобы удалить экземпляр часов
Clock Instance	Обозначает конкретный идентификатор или номер для различных экземпляров часов в системе PTP. Возможные значения находятся в диапазоне от 0 до 3
Device Type	Указывает тип экземпляра часов. Существует пять типов устройств: **Ord-Bound**: обычные/граничные часы **P2p Transp**: одноранговые прозрачные часы **E2e Transp**: сквозные прозрачные часы **Master Only**: только главный **Slave Only**: только подчиненный
Port List	Отметьте все порты, предназначенные для выбранного экземпляра часов
2 Step Flag	Используется для указания метода синхронизации времени, который применяется в системе. Этот флаг является статическим. Его значение фиксируется системой и не меняется динамически. Может иметь следующие значения: **True**: используются двухступенчатые события синхронизации (Sync) и ответы на запросы временных задержек (Pdelay_Resp). В двухступенчатой модели процесс синхронизации времени разбивается на два этапа: 1) периодический обмен событиями Sync между источником времени и клиентами, чтобы передать текущие временные метки

	2) ответы на запросы Pdelay_Req (запросы временных задержек) и их соответствующие ответы Pdelay_Resp, которые помогают корректировать задержки в сети и уточнять синхронизацию **False**: используется одноступенчатый метод синхронизации, при котором события синхронизации и ответы на запросы временных задержек объединены в одном сообщении
Clock Identity	Указывает уникальный идентификатор часов
One Way	Если выбрано значение **true**, используются односторонние измерения. Этот параметр применяется только к ведомому устройству. В одностороннем режиме измерения задержки не производятся, т.е. эта функция применима только в случае необходимости синхронизации частоты. Ведущее устройство всегда отвечает на запросы Pdelay_Req
Protocol	Транспортный протокол, используемый механизмом протокола PTP: **Ethernet**: PTP через Ethernet multicast **ip4multi**: PTP через IPv4 multicast **ip4uni**: PTP через IPv4 unicast Следует учитывать, что одноадресный протокол IPv4 работает только для часов в режимах **Master Only** и **Slave Only**. Также в одноадресных часах Slave Only необходимо настроить, с каких главных часов запрашивать сообщения Announce и Sync
VLAN Tag Enable	Включает или отключает добавление тегов VLAN к кадрам PTP. Важно учитывать, что кадры PTP будут тегироваться только в случае, если порт, через который они передаются, настроен для использования VLAN-тегов. Порт не должен быть настроен как «Unaware» по отношению к VLAN. Режим VLAN на порту не должен быть «None», а сам порт должен быть членом соответствующей VLAN
VID	Идентификаторы VLAN, используемые для маркировки кадров PTP
PCP	Значения точек кода приоритета, используемые для кадров PTP

Текущее состояние PTP

На странице [Status]отображается статус функции PTP на основе настроек, которые вы выполнили на странице конфигурации.

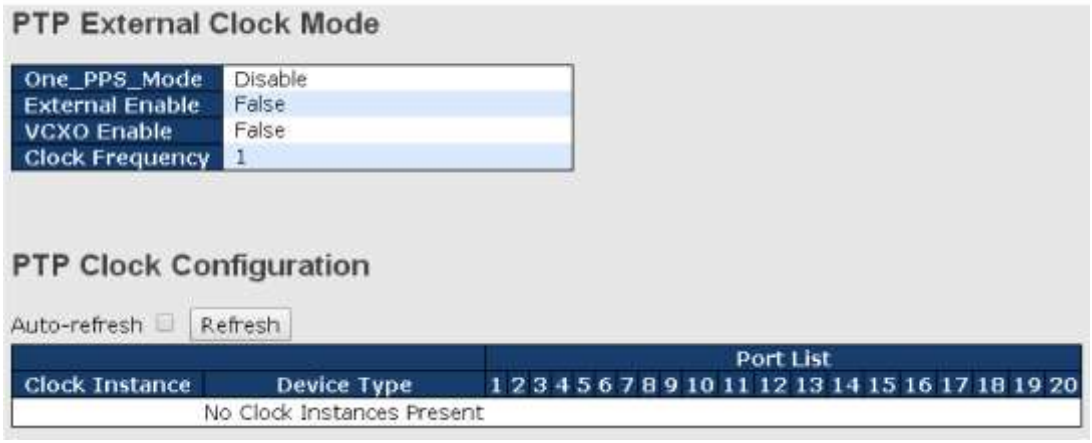


Рисунок 160 – Состояние PTP

5.14 PoE

5.14.1 Настройки

PoE (Power Over Ethernet) — это технология, которая передает электропитание удаленным устройствам по стандартным кабелям Ethernet. Она может обеспечивать питание для IP-телефонов, точек доступа беспроводной локальной сети и другого оборудования в местах, где подача питания затруднена или требует больших затрат. Коммутатор укомплектован портами SFP, которые поддерживают функции PoE. Таким образом, он может раздавать питание устройствам через витую пару.

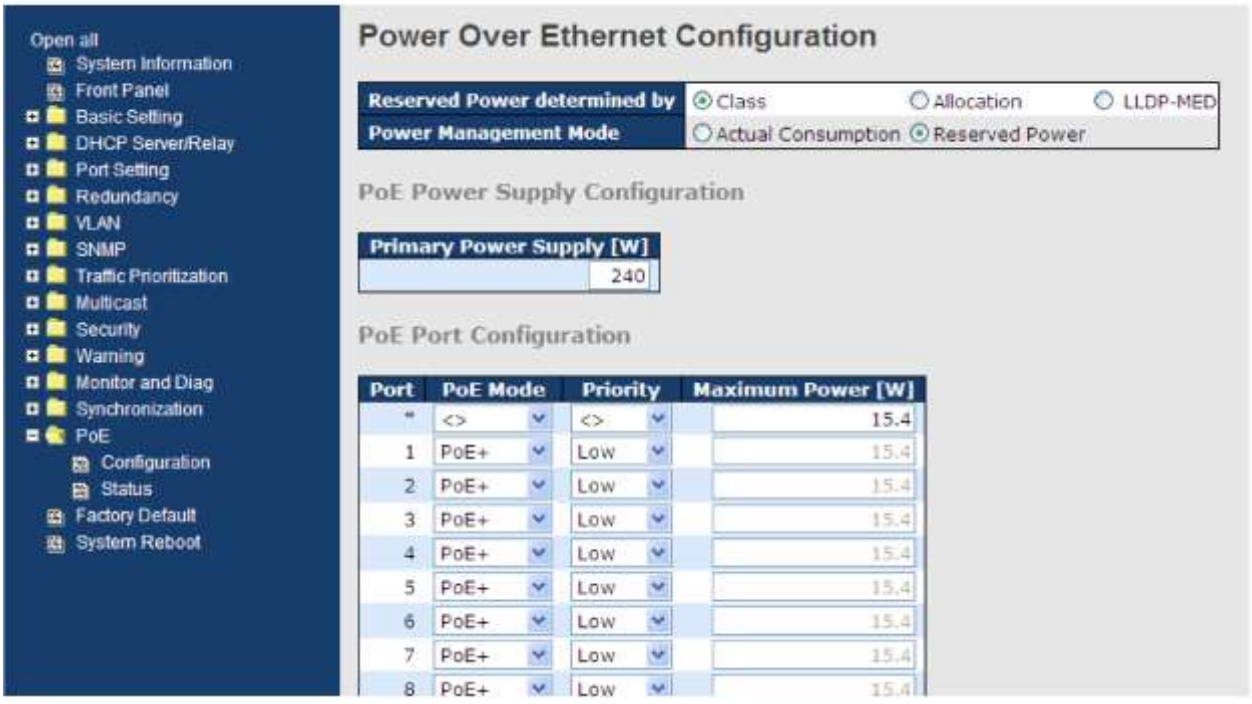


Рисунок 161 – Настройки PoE

Параметр	Описание
Reserved Power determined by	При настройке резервируемой мощности для каждого порта или питаемого устройства доступны три режима: **Allocation**: пользователи могут мощность, которую резервирует каждый порт. Распределенная / зарезервированная мощность для каждого порта / устройства указывается в поле «Maximum Power» **Class**: каждый порт автоматически определяет, сколько мощности необходимо зарезервировать в соответствии с классом, к которому относится подключенное питаемое устройство, а затем резервирует мощность соответствующим образом. Доступны четыре различных класса, включая 4, 7, 15,4 и 30 Вт. В этом режиме поле «Maximum Power» будет серым **LLDP-MED**: этот режим похож на режим **Class**, за исключением того, что каждый порт определяет величину мощности, которую он хочет зарезервировать, обмениваясь информацией PoE с использованием протокола LLDP. Если для порта нет доступной информации LLDP, он будет резервировать мощность с использованием режима **Class**. В этом режиме поля «Maximum Power» будут серыми Во всех вышеперечисленных режимах, если порт потребляет больше мощности, чем было для него зарезервировано, он отключится
Power Management Mode	При настройке условий отключения порта доступны два режима: **Actual Consumption**: порты отключаются, когда фактическое потребление мощности для всех портов превышает величину, которую может обеспечить блок питания, или если фактическое потребление мощности отдельного порта превышает зарезервированную для него мощность. Порты отключаются в соответствии с настройкой их приоритета. Если два порта имеют одинаковый приоритет, отключается порт с бóльшим номером **Reserved Power**: порты отключаются, когда общая зарезервированная мощность превышает величину мощности, которую может предоставить блок питания. Питание порта не будет включено, если питаемое устройство запрашивает больше мощности, чем доступно от блока питания
Primary and Backup Power Source	Для функции PoE может быть задействовано два источника питания. Один используется как основной, а другой как резервный. Если коммутатор не имеет резервного источника питания, будут показаны только настройки основного. Если основной источник питания выходит из строя, резервный возьмет на себя его функции. Чтобы определить количество мощности, разрешенное для питаемых устройств, необходимо настроить количество мощности, которое

	могут обеспечить основной и резервный источники питания. Допустимые значения находятся в диапазоне от 0 до 2000 Вт
Port	Указывает номер порта. Порты, не поддерживающие PoE, выделены серым цветом и, следовательно, не могут быть настроены
PoE Mode	Раскрывающийся список для выбора операций PoE. Режимы включают: **Disabled**: отключить PoE **PoE**: включить PoE IEEE 802.3af (питаемые устройства класса 4 ограничены мощностью 15,4 Вт) **PoE+**: включить PoE+ IEEE 802.3at (питаемые устройства класса 4 ограничены мощностью 30 Вт)
Priority	Указывает приоритет порта. Существует три уровня приоритета питания: низкий (**Low**), высокий (**High**) и критический (**Critical**) Приоритет используется, когда удаленным устройствам требуется больше мощности, чем может предоставить блок питания. Порт с самым низким приоритетом будет отключен
Maximum Power	Указывает максимальную мощность в ваттах, которая может быть передана удаленному устройству (максимально допустимое значение – 30 Вт)

5.14.2 Статус

Страница [Status] позволяет вам проверить текущее состояние всех портов PoE.

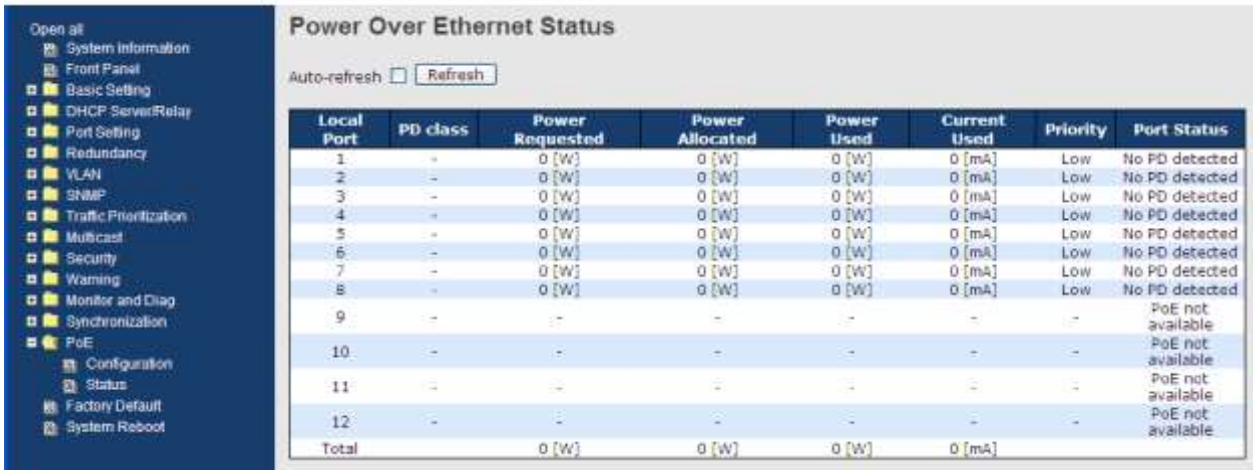


Рисунок 162 – Состояние портов PoE

Параметр	Описание
Local Port	Номер порта коммутатора, к которому будут применены следующие настройки
PD Class	Каждое питаемое устройство определяется в соответствии с классом, который ограничивает максимальную потребляемую мощность устройства Эта настройка включает пять 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 30,0 Вт
Power Requested	Отображает мощность, запрашиваемую питаемым устройством
Power Allocated	Отображает величину мощности, выделенной коммутатором для питаемого устройства
Power Used	Отображает потребляемую мощность питаемого устройства в настоящий момент
Current Used	Отображает потребляемый ток питаемого устройства в настоящий момент
Priority	Отображает приоритет порта, настроенный пользователем
Port Status	Показывает состояние порта. Оно может иметь одно из следующих значений: **PoE not available**: чип PoE не найден **PoE turned OFF**: а) PoE отключен пользователем; б) превышен бюджет мощности. Общая запрошенная или использованная мощность питаемых устройств превышает максимальную мощность, которую может обеспечить блок питания, и порты с самым низким приоритетом были отключены; в) питаемое устройство выключено **No PD detected**: на порту не обнаружено питаемых устройств **Invalid PD**: подключенное устройство обнаружено, но работает некорректно

5.15 Заводские настройки по умолчанию

Эта функция позволяет принудительно вернуть коммутатор к исходным заводским настройкам. Чтобы сбросить настройки коммутатора, выберите «Reset to Factory Defaults» в раскрывающемся списке стартовой страницы и нажмите <Yes>. Сохраняется только конфигурация IP.

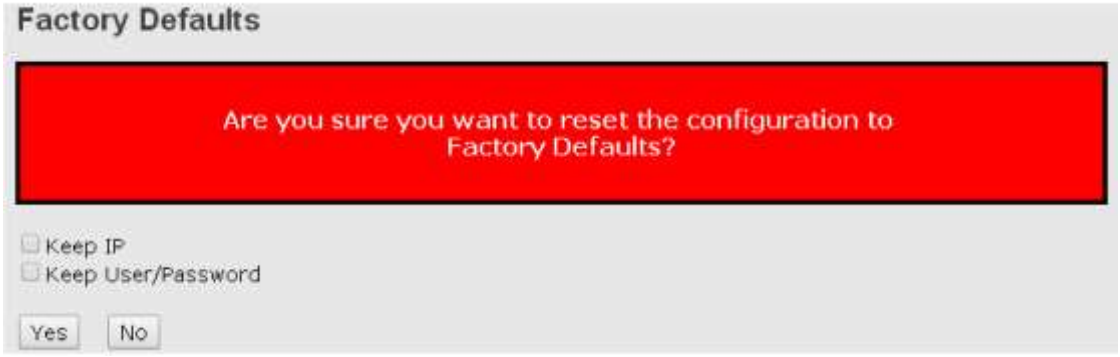


Рисунок 163 – Возвращение к заводским настройкам

Параметр	Описание
Yes	Нажмите, чтобы сбросить конфигурацию до заводских настроек по умолчанию
No	Нажмите, чтобы вернуться на домашнюю страницу без сброса конфигурации

5.16 Перезагрузка системы

Вы можете перезагрузить коммутатор стека на странице [System Reboot]. После перезапуска система загрузится в штатном режиме, как если бы вы включили устройства.

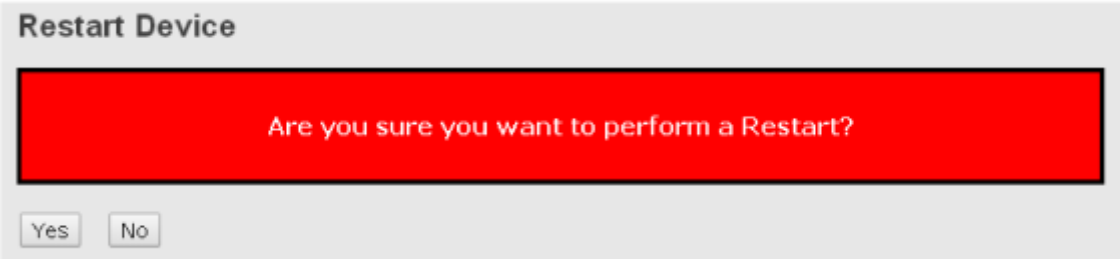


Рисунок 164 – Перезагрузка

Параметр	Описание
Yes	Нажмите, чтобы перезагрузить устройство
No	Нажмите, чтобы вернуться на домашнюю страницу без перезагрузки

6. Управление с помощью командной строки

Помимо управления через веб-интерфейс, коммутатор также поддерживает управление с помощью интерфейса командной строки. Вы можете использовать консоль или Telnet для управления коммутатором через CLI.

6.1 Подключение через консольный порт

Для управления устройством через командную строку необходимо подключить последовательный консольный порт устройства к COM-порту вашего компьютера. Используйте для этого кабель с адаптерами RJ45 на DB9-F. Настройки подключения должны быть следующими: скорость передачи данных 115200 бит/с, 8 бит данных, без четности, 1 стоп-бит и без управления потоком.

Ниже описано как получить доступ к консоли через последовательный кабель RS-232 на примере приложения Hyper Terminal.

1. Запустите Hyper Terminal и в открывшемся окне введите имя для нового соединения.

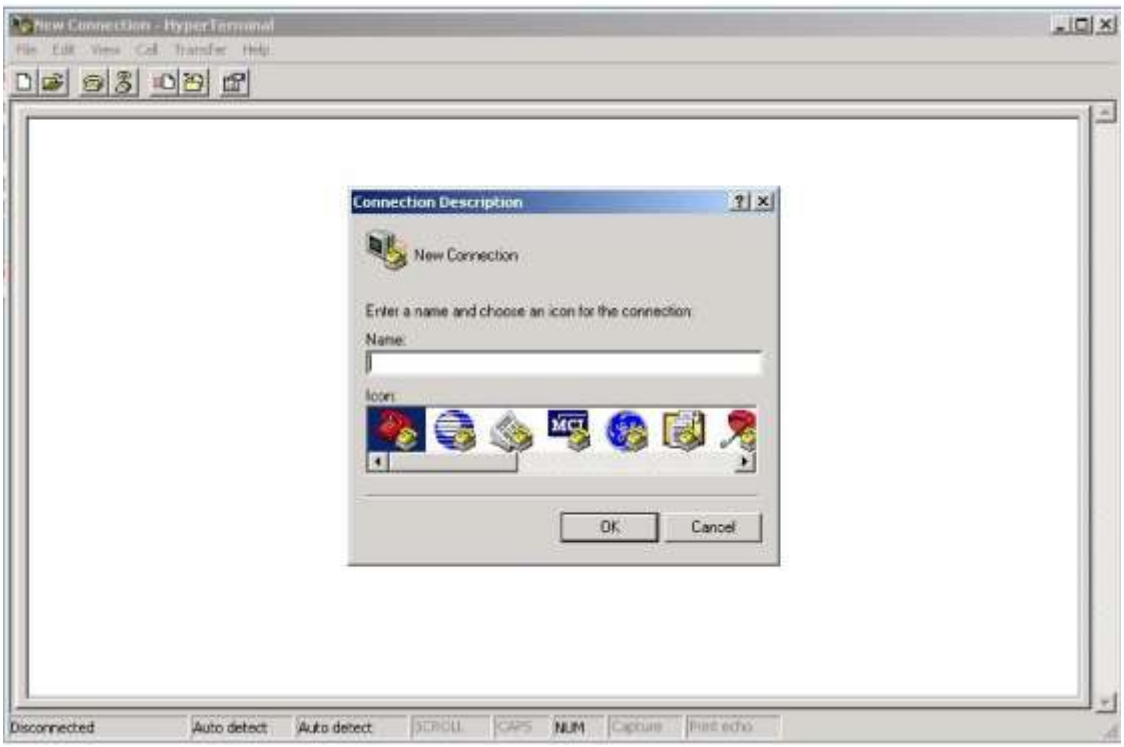


Рисунок 165 – Выбор имени и ярлыка для соединения

2. Выберите COM-порт в раскрывающемся списке.

Рисунок 166 – Выбор COM-порта

3. Появится всплывающее окно, в котором отображаются свойства COM-порта, включая биты в секунду, биты данных, четность, стоповые биты и управление потоком.

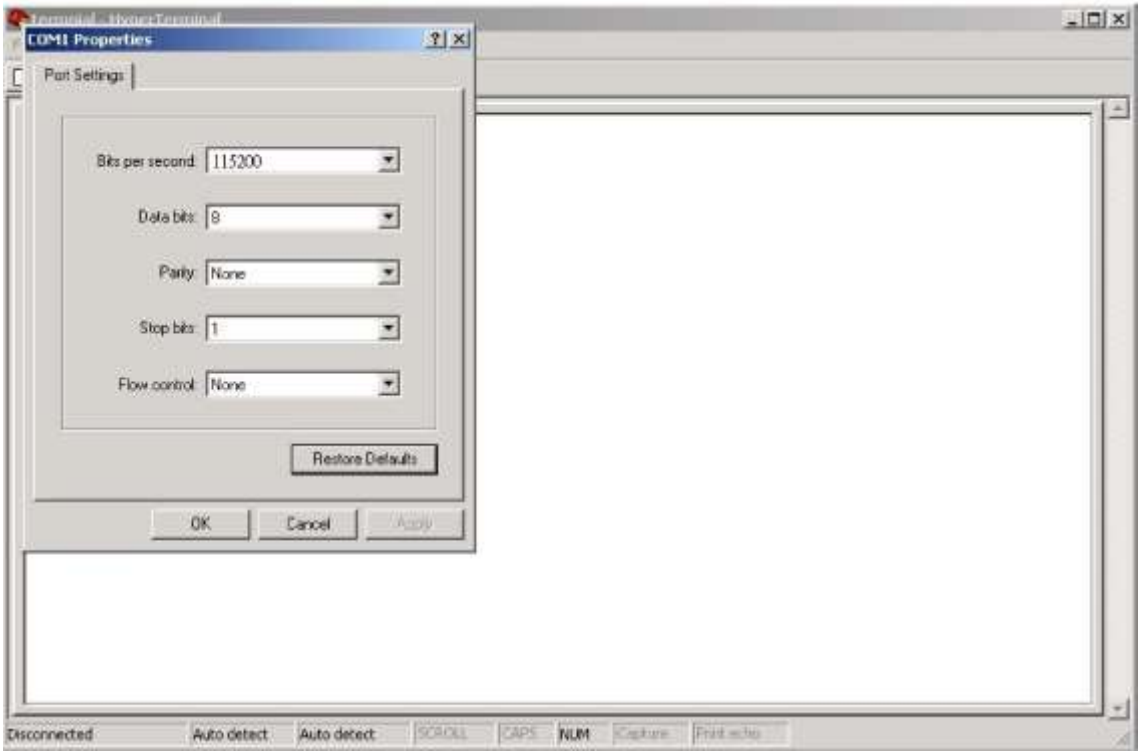


Рисунок 167 – Настройки COM-порта

4. Появится экран входа в консоль. Введите с клавиатуры имя пользователя и пароль (тот же, что и пароль для веб-браузеров), затем нажмите клавишу «Enter».

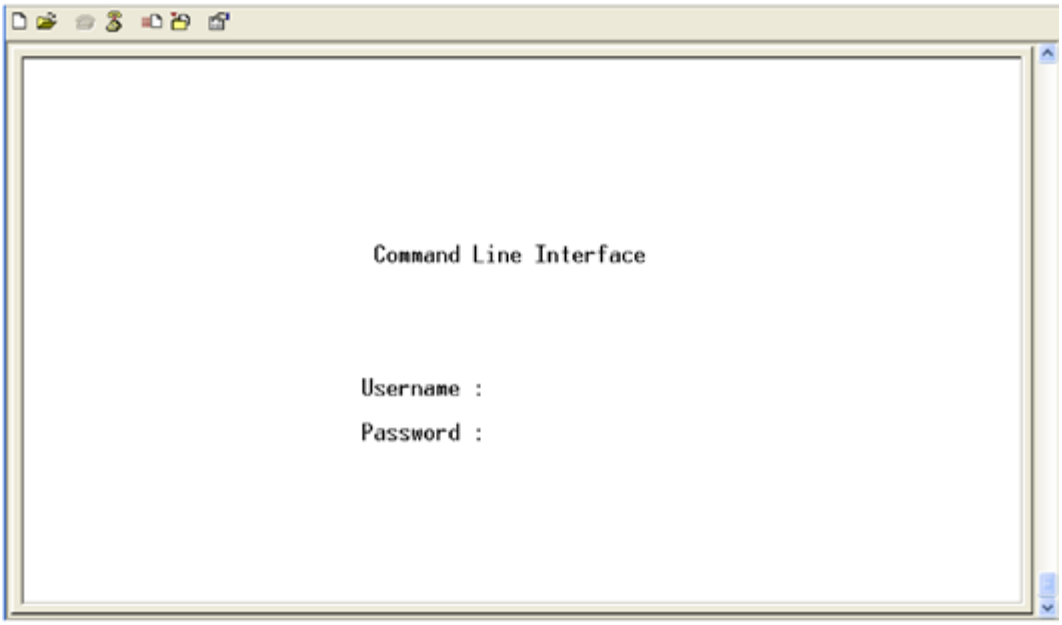


Рисунок 168 – Экран входа в систему

6.2 Подключение через Telnet

Для настройки коммутатора вы можете использовать Telnet. Значения по умолчанию:

IP-адрес: 192.168.10.1

Маска подсети: 255.255.255.0

Шлюз по умолчанию: 192.168.10.254

Имя пользователя: admin

Пароль: admin

Чтобы получить доступ к консоли через Telnet, выполните следующие действия.

1. Подключитесь по Telnet к IP-адресу коммутатора из командной строки MS-DOS или из окна «Выполнить» Windows, введя команды, как показано ниже.

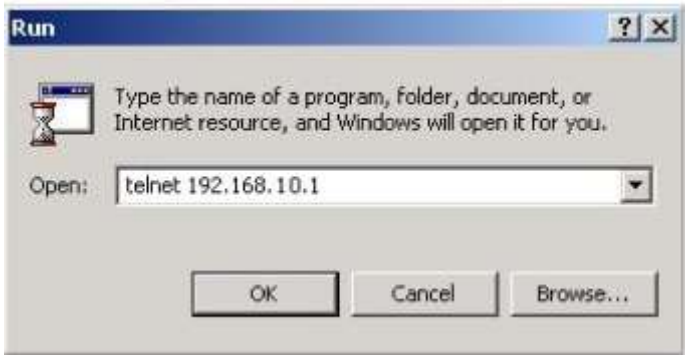


Рисунок 169 – Подключение через Telnet

2. Появится экран входа в систему. Введите с клавиатуры имя пользователя и пароль (тот же, что и для веб-браузера), а затем нажмите «Enter».

Рисунок 170 – Экран входа в систему

6.3 Основные команды CLI

Группы команд			Описание
System			Настройки системы и параметры сброса
IP			Настройка IP и Ping
Port			Управление портами
MAC			Таблица MAC-адресов
VLAN			Виртуальная локальная сеть
PVLAN			Частная виртуальная локальная сеть
Security	Switch	Auth	Аутентификация на коммутаторе
		SSH	Настройка SSH
		HTTPS	Настройка HTTPS
		RMON	Настройка удаленного мониторинга сети
	Network	Psec	Настройка функции Port Security
		NAS	Настройка сервера сетевого доступа (IEEE 802.1X)
		ACL	Настройка списка управления доступом
		DHCP	Настройка режима DHCP

	AAA	Настройка аутентификации, авторизации и учета
STP		Протокол связующего дерева
Aggr		Агрегирование каналов
LACP		Протокол управления агрегацией каналов
LLDP		Протокол обнаружения канального уровня
PoE		Электропитание через Ethernet
QoS		Качество обслуживания
Mirror		Зеркалирование портов
Config		Загрузка/сохранение конфигурации через TFTP
Firmware		Загрузка прошивки через TFTP
SNMP		Настройка сетевого управления устройствами
PTP		Протокол точного времени IEEE1588 и синхронизация
Loop Protect		Предотвращение петель
IPMC		Настройка многоадресной передачи (MLD/IGMP Snooping)
Fault		Настройка сигнализации о неисправностях
Event		Выбор событий
DHCPServer		Настройка сервера DHCP
Ring		Настройка Sy-Ring
Chain		Настройка Sy-Union
RCS		Безопасное удаленное управление
Fastrecovery		Настройка быстрого восстановления
SFP		Настройка SFP-мониторинга
DeviceBinding		Настройка привязки устройств
MRP		Настройка MRP
Modbus		Настройка Modbus TCP

System>

Configuration [all] [<port_list>]

Reboot

Restore Default [keep_ip]

Contact [<contact>]

Name [<name>]

Location [<location>]

Description [<description>]

Password <password>

Username [<username>]

Timezone [<offset>]

Log [<log_id>] [all|info|warning|error] [clear]

IP>

Configuration

DHCP [enable|disable]

Setup [<ip_addr>] [<ip_mask>] [<ip_router>] [<vid>]

Ping <ip_addr_string> [<ping_length>]

SNTP [<ip_addr_string>]

Port>

Configuration [<port_list>] [up|down]

Mode [<port_list>] [auto|10hdx|10fdx|100hdx|100fdx|1000fdx|sfp_auto_ams]

Flow Control [<port_list>] [enable|disable]

State [<port_list>] [enable|disable]

MaxFrame [<port_list>] [<max_frame>]

Power [<port_list>] [enable|disable|actiphy|dynamic]

Excessive [<port_list>] [discard|restart]

Statistics [<port_list>] [<command>] [up|down]

VeriPHY [<port_list>]

SFP [<port_list>]

MAC>

Configuration [<port_list>]

Add <mac_addr> <port_list> [<vid>]

Delete <mac_addr> [<vid>]

Lookup <mac_addr> [<vid>]

Agetime [<age_time>]

Learning [<port_list>] [auto|disable|secure]

Dump [<mac_max>] [<mac_addr>] [<vid>]

Statistics [<port_list>]

Flush

VLAN>

Configuration [<port_list>]

PVID [<port_list>] [<vid>|none]

FrameType [<port_list>] [all|tagged|untagged]

IngressFilter [<port_list>] [enable|disable]

tx_tag [<port_list>] [untag_pvid|untag_all|tag_all]

PortType [<port_list>] [unaware|c-port|s-port|s-custom-port]

EtypeCustomSport [<etype>]

Add <vid>|<name> [<ports_list>]

Forbidden Add <vid>|<name> [<port_list>]

Delete <vid>|<name>

Forbidden Delete <vid>|<name>

Forbidden Lookup [<vid>] [(name <name>)]

Lookup [<vid>] [(name <name>)] [combined|static|nas|all]

Name Add <name> <vid>

Name Delete <name>

Name Lookup [<name>]

Status [<port_list>] [combined|static|nas|mstp|all|conflicts]

PVLAN>

Configuration [<port_list>]

Add <pvlan_id> [<port_list>]

Delete <pvlan_id>

Lookup [<pvlan_id>]

Isolate [<port_list>] [enable|disable]

Security/switch/auth>

Configuration

Method [console|telnet|ssh|web] [none|local|radius]

[enable|disable]

Security/switch/ssh>

Configuration

Mode [enable|disable]

Security/switch/https>

Configuration

Mode [enable|disable]

Security/switch/rmon>

Statistics Add <stats_id> <data_source>

Statistics Delete <stats_id>

Statistics Lookup [<stats_id>]

History Add <history_id> <data_source> [<interval>] [<buckets>]

History Delete <history_id>

History Lookup [<history_id>]

Alarm Add <alarm_id> <interval> <alarm_variable> [absolute|delta] <rising_threshold> <rising_event_index> <falling_threshold> <falling_event_index> [rising|falling|both]

Alarm Delete <alarm_id>

Alarm Lookup [<alarm_id>]

Security/Network/Psec>

Switch [<port_list>]

Port [<port_list>]

Security/Network/NAS>

Configuration [<port_list>]

Mode [enable|disable]

State [<port_list>] [auto|authorized|unauthorized|macbased]

Reauthentication [enable|disable]

ReauthPeriod [<reauth_period>]

EapolTimeout [<eapol_timeout>]

Agetime [<age_time>]

Holdtime [<hold_time>]

Authenticate [<port_list>] [now]

Statistics [<port_list>] [clear|eapol|radius]

Security/Network/ACL>

Configuration [<port_list>]

Action [<port_list>] [permit|deny] [<rate_limiter>] [<port_redirect>] [<mirror>] [<logging>] [<shutdown>]

Policy [<port_list>] [<policy>]

Rate [<rate_limiter_list>] [<rate_unit>] [<rate>]

Add [<ace_id>] [<ace_id_next>] [(port <port_list>)] [(policy <policy> <policy_bitmask>)] [<tagged>] [<vid>] [<tag_prio>] [<dmac_type>] [(etype [<etype>] [<smac>] [<dmac>]) | (arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>]) | (ip [<sip>] [<dip>] [<protocol>] [<ip_flags>]) | (icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>]) | (udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>]) | (tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>])] [permit|deny] [<rate_limiter>] [<port_redirect>] [<mirror>] [<logging>] [<shutdown>]

Delete <ace_id>

Lookup [<ace_id>]

Clear

Status [combined|static|loop_protect|dhcp|ptp|ipmc|conflicts]

Port State [<port_list>] [enable|disable]

Security/Network/DHCP>

Configuration

Mode [enable|disable]

Server [<ip_addr>]

Information Mode [enable|disable]

Information Policy [replace|keep|drop]

Statistics [clear]

Security/Network/AAA>

Configuration

Timeout [<timeout>]

Deadtime [<dead_time>]

RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]

ACCT_RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]

Statistics [<server_index>]

STP>

Configuration

Version [<stp_version>]

Txhold [<holdcount>]

MaxAge [<max_age>]

FwdDelay [<delay>]

bpduFilter [enable|disable]

bpduGuard [enable|disable]

recovery [<timeout>]

CName [<config-name>] [<integer>]

Status [<msti>] [<port_list>]

Msti Priority [<msti>] [<priority>]

Msti Map [<msti>] [clear]

Msti Add <msti> <vid>

Port Configuration [<port_list>]

Port Mode [<port_list>] [enable|disable]

Port Edge [<port_list>] [enable|disable]

Port AutoEdge [<port_list>] [enable|disable]

Port P2P [<port_list>] [enable|disable|auto]

Port RestrictedRole [<port_list>] [enable|disable]

Port RestrictedTcn [<port_list>] [enable|disable]

Port bpduGuard [<port_list>] [enable|disable]

Port Statistics [<port_list>]

Port Mcheck [<port_list>]

Msti Port Configuration [<msti>] [<port_list>]

Msti Port Cost [<msti>] [<port_list>] [<path_cost>]

Msti Port Priority [<msti>] [<port_list>] [<priority>]

Aggr>

Configuration

Add <port_list> [<aggr_id>]

Delete <aggr_id>

Lookup [<aggr_id>]

Mode [smac|dmac|ip|port] [enable|disable]

LACP>

Configuration [<port_list>]

Mode [<port_list>] [enable|disable]

Key [<port_list>] [<key>]

Role [<port_list>] [active|passive]

Status [<port_list>]

Statistics [<port_list>] [clear]

LLDP>

Configuration [<port_list>]

Mode [<port_list>] [enable|disable]

Statistics [<port_list>] [clear]

Info [<port_list>]

PoE>

Configuration [<port_list>]

Mode [<port_list>] [disabled|poe|poe+]

Priority [<port_list>] [low|high|critical]

Mgmt_mode [class_con|class_res|al_con|al_res|lldp_res|lldp_con]

Maximum_Power [<port_list>] [<port_power>]

Status

Primary_Supply [<supply_power>]

QoS>

DSCP Map [<dscp_list>] [<class>] [<dpl>]

DSCP Translation [<dscp_list>] [<trans_dscp>]

DSCP Trust [<dscp_list>] [enable|disable]

DSCP Classification Mode [<dscp_list>] [enable|disable]

DSCP Classification Map [<class_list>] [<dpl_list>] [<dscp>]

DSCP EgressRemap [<dscp_list>] [<dpl_list>] [<dscp>]

Storm Unicast [enable|disable] [<packet_rate>]

Storm Multicast [enable|disable] [<packet_rate>]

Storm Broadcast [enable|disable] [<packet_rate>]

QCL Add [<qce_id>] [<qce_id_next>] [<port_list>] [<tag>] [<vid>] [<pcp>] [<dei>] [<smac>] [<dmac_type>] [(etype [<etype>]) | (LLC [<DSAP>] [<SSAP>] [<control>]) | (SNAP [<PID>]) | (ipv4 [<protocol>] [<sip>] [<dscp>] [<fragment>] [<sport>] [<dport>]) | (ipv6 [<protocol>] [<sip_v6>] [<dscp>] [<sport>] [<dport>])] [<class>] [<dp>] [<classified_dscp>]

QCL Delete <qce_id>

QCL Lookup [<qce_id>]

QCL Status [combined|static|conflicts]

QCL Refresh

Mirror>

Configuration [<port_list>]

Port [<port>|disable]

Mode [<port_list>] [enable|disable|rx|tx]

Dot1x>

Configuration [<port_list>]

Mode [enable|disable]

State [<port_list>] [macbased|auto|authorized|unauthorized]

Authenticate [<port_list>] [now]

Reauthentication [enable|disable]

Period [<reauth_period>]

Timeout [<eapol_timeout>]

Statistics [<port_list>] [clear|eapol|radius]

Clients [<port_list>] [all|<client_cnt>]

Agetime [<age_time>]

Holdtime [<hold_time>]

ACL>

Configuration [<port_list>]

Action [<port_list>] [permit|deny] [<rate_limiter>] [<port_copy>] [<logging>] [<shutdown>]

Policy [<port_list>] [<policy>]

Rate [<rate_limiter_list>] [<packet_rate>]

Add [<ace_id>] [<ace_id_next>] [switch | (port <port>) | (policy <policy>)] [<vid>] [<tag_prio>] [<dmac_type>] [(etype [<etype>] [<smac>] [<dmac>]) | (arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>]) | (ip [<sip>] [<dip>] [<protocol>] [<ip_flags>]) | (icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>]) | (udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>]) | (tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>])] [permit|deny] [<rate_limiter>] [<port_copy>] [<logging>] [<shutdown>]

Delete <ace_id>

Lookup [<ace_id>]

Clear

Config>

Save <ip_server> <file_name>

Load <ip_server> <file_name> [check]

Firmware>

Load <ip_addr_string> <file_name>

SNMP>

Trap Inform Retry Times [<retries>]

Trap Probe Security Engine ID [enable|disable]

Trap Security Engine ID [<engineid>]

Trap Security Name [<security_name>]

Engine ID [<engineid>]

Community Add <community> [<ip_addr>] [<ip_mask>]

Community Delete <index>

Community Lookup [<index>]

User Add <engineid> <user_name> [MD5|SHA] [<auth_password>] [DES] [<priv_password>]

User Delete <index>

User Changekey <engineid> <user_name> <auth_password> [<priv_password>]

User Lookup [<index>]

Group Add <security_model> <security_name> <group_name>

Group Delete <index>

Group Lookup [<index>]

View Add <view_name> [included|excluded] <oid_subtree>

View Delete <index>

View Lookup [<index>]

Access Add <group_name> <security_model> <security_level> [<read_view_name>] [<write_view_name>]

Access Delete <index>

Access Lookup [<index>]

PTP>

Configuration [<clockinst>]

PortState <clockinst> [<port_list>] [enable|disable|internal]

ClockCreate <clockinst> [<devtype>] [<twostep>] [<protocol>] [<oneway>] [<clockid>] [<tag_enable>] [<vid>] [<prio>]

ClockDelete <clockinst> [<devtype>]

DefaultDS <clockinst> [<priority1>] [<priority2>] [<domain>]

CurrentDS <clockinst>

ParentDS <clockinst>

Timingproperties <clockinst> [<utcoffset>] [<valid>] [<leap59>] [<leap61>] [<timetrac>] [<freqtrac>] [<ptptimescale>] [<timesource>]

PTP PortDataSet <clockinst> [<port_list>] [<announceintv>] [<announceto>] [<syncintv>] [<delaymech>] [<minpdelayreqintv>] [<delayasymmetry>] [<ingressLatency>]

LocalClock <clockinst> [update|show|ratio] [<clockratio>]

Filter <clockinst> [<def_delay_filt>] [<period>] [<dist>]

Servo <clockinst> [<displaystates>] [<ap_enable>] [<ai_enable>] [<ad_enable>] [<ap>] [<ai>] [<ad>]

SlaveTableUnicast <clockinst>

UniConfig <clockinst> [<index>] [<duration>] [<ip_addr>]

ForeignMasters <clockinst> [<port_list>]

EgressLatency [show|clear]

MasterTableUnicast <clockinst>

ExtClockMode [<one_pps_mode>] [<ext_enable>] [<clockfreq>] [<vcxo_enable>]

OnePpsAction [<one_pps_clear>]

DebugMode <clockinst> [<debug_mode>]

Wireless mode <clockinst> [<port_list>] [enable|disable]

Wireless pre notification <clockinst> <port_list>

Wireless delay <clockinst> [<port_list>] [<base_delay>] [<incr_delay>]

Loop Protect>

Configuration

Mode [enable|disable]

Transmit [<transmit-time>]

Shutdown [<shutdown-time>]

Port Configuration [<port_list>]

Port Mode [<port_list>] [enable|disable]

Port Action [<port_list>] [shutdown|shut_log|log]

Port Transmit [<port_list>] [enable|disable]

Status [<port_list>]

IPMC>

Configuration [igmp]

Mode [igmp] [enable|disable]

Flooding [igmp] [enable|disable]

VLAN Add [igmp] <vid>

VLAN Delete [igmp] <vid>

State [igmp] [<vid>] [enable|disable]

Querier [igmp] [<vid>] [enable|disable]

Fastleave [igmp] [<port_list>] [enable|disable]

Router [igmp] [<port_list>] [enable|disable]

Status [igmp] [<vid>]

Groups [igmp] [<vid>]

Version [igmp] [<vid>]

IGMP>

Configuration [<port_list>]

Mode [enable|disable]

State [<vid>] [enable|disable]

Querier [<vid>] [enable|disable]

Fastleave [<port_list>] [enable|disable]

Router [<port_list>] [enable|disable]

Flooding [enable|disable]

Groups [<vid>]

Status [<vid>]

Fault>

Alarm PortLinkDown [<port_list>] [enable|disable]

Alarm PowerFailure [pwr1|pwr2|pwr3] [enable|disable]

Event>

Configuration

Syslog SystemStart [enable|disable]

Syslog PowerStatus [enable|disable]

Syslog SnmpAuthenticationFailure [enable|disable]

Syslog RingTopologyChange [enable|disable]

Syslog Port [<port_list>] [disable|linkup|linkdown|both]

SMTP SystemStart [enable|disable]

SMTP PowerStatus [enable|disable]

SMTP SnmpAuthenticationFailure [enable|disable]

SMTP RingTopologyChange [enable|disable]

SMTP Port [<port_list>] [disable|linkup|linkdown|both]

DHCPServer>

Mode [enable|disable]

Setup [<ip_start>] [<ip_end>] [<ip_mask>] [<ip_router>] [<ip_dns>] [<ip_tftp>] [<lease>] [<bootfile>]

Ring>

Mode [enable|disable]

Master [enable|disable]

1stRingPort [<port>]

2ndRingPort [<port>]

Couple Mode [enable|disable]

Couple Port [<port>]

Dualhoming Mode [enable|disable]

Dualhoming Port [<port>]

Chain>

Configuration

Mode [enable|disable]

1stUplinkPort [<port>]

2ndUplinkPort [<port>]

EdgePort [1st|2nd|none]

RCS>

Configuration

Mode [enable|disable]

Add [<ip_addr>] [<port_list>] [web_on|web_off] [telnet_on|telnet_off] [snmp_on|snmp_off]

Del <index>

FastRecovery>

Mode [enable|disable]

Port [<port_list>] [<fr_priority>]

SFP>

syslog [enable|disable]

temp [<temperature>]

Info

DeviceBinding>

Mode [enable|disable]

Port Mode [<port_list>] [disable|scan|binding|shutdown]

Port DDOS Mode [<port_list>] [enable|disable]

Port DDOS Sensibility [<port_list>] [low|normal|medium|high]

Port DDOS Packet [<port_list>] [rx_total|rx_unicast|rx_multicast|rx_broadcast|tcp|udp]

Port DDOS Low [<port_list>] [<socket_number>]

Port DDOS High [<port_list>] [<socket_number>]

Port DDOS Filter [<port_list>] [source|destination]

Port DDOS Action [<port_list>] [do_nothing |block_1_min |block_10_mins |block |shutdown |only_log |reboot_device]

Port DDOS Status [<port_list>]

Port Alive Mode [<port_list>] [enable|disable]

Port Alive Action [<port_list>] [do_nothing|link_change|shutdown|only_log|reboot_device]

Port Alive Status [<port_list>]

Port Stream Mode [<port_list>] [enable|disable]

Port Stream Action [<port_list>] [do_nothing|only_log]

Port Stream Status [<port_list>]

Port Addr [<port_list>] [<ip_addr>] [<mac_addr>]

Port Alias [<port_list>] [<ip_addr>]

Port DeviceType [<port_list>] [unknown|ip_cam|ip_phone|ap|pc|plc|nvr]

Port Location [<port_list>] [<device_location>]

Port Description [<port_list>] [<device_description>]

MRP>

Configuration

Mode [enable|disable]

Manager [enable|disable]

React [enable|disable]

1stRingPort [<mrp_port>]

2ndRingPort [<mrp_port>]

Parameter MRP_TOPchgT [<value>]

Parameter MRP_TOPNRmax [<value>]

Parameter MRP_TSTshortT [<value>]

Parameter MRP_TSTdefaultT [<value>]

Parameter MRP_TSTNRmax [<value>]

Parameter MRP_LNKdownT [<value>]

Parameter MRP_LNKupT [<value>]

Parameter MRP_LNKNRmax [<value>]

Modbus>

Status

Mode [enable|disable]

Расшифровка аббревиатур

AAA	Authentication Authorization and Accounting	Система аутентификации авторизации и учета событий
ACE	Access Control Entry	Запись ACL – элемент списка управления доступом
ACL	Access Control List	Список управления доступом
ARP	Address Resolution Protocol	Протокол определения MAC-адреса другого узла по известному IP-адресу
BPDU	Bridge Protocol Data Unit	Блок данных протокола управления сетевыми мостами
CIST	Common and Internal Spanning Tree	Общее и внутреннее связующее дерево
CLI	Command Line Interface	Интерфейс командной строки
CoS	Class of Service	Класс сервиса
CRC	Cyclic Redundancy Check	Циклический избыточный код. Алгоритм нахождения контрольной суммы, предназначенный для проверки целостности данных
DCE	Data Communication Equipment	Аппаратура передачи данных (АПД)
DDM	Digital Diagnostics Monitoring	Функция цифрового контроля параметров производительности SFP-трансивера
DDoS	Distributed Denial of Service	Отказ в обслуживании (тип сетевой атаки)
DEI	Drop Eligible Indicator	Бит в теге VLAN, который указывает, может ли кадр быть отброшен в случае перегрузки сети
DHCP	Dynamic Host Configuration Protocol	Протокол динамической настройки узла
DNS	Domain Name System	Система доменных имен
DOS	Denial of Service	Отказ в обслуживании (тип сетевой атаки)
DP	Drop Precedence	Приоритет отбрасывания пакета (Class Selector поля DSCP)
DS Field	Definition of the Differentiated Services Field	Поле дифференцированных служб в IP-заголовке, использующееся для классификации пакетов (RFC 2474)
DSAP	Destination Service Access Point	Точка доступа к сервису системы получателя (LLC)
DSCP	Differentiated Services Code Point	Точка кода дифференцированных услуг. Использует 6-битное поле 8-битного IP-заголовка DS
DTE	Data Terminal Equipment	Оконечное оборудование данных (ООД)
EAPOL	Extensible Authentication Protocol over LAN	Протокол определяющий способ инкапсуляции, который позволяет передавать пакеты EAP между запрашивающим устройством и аутентификатором в локальных проводных сетях

EAP	Protected Extensible Authentication Protocol	Расширяемый протокол аутентификации
FCS	Frame Check Sequence	Часть кадра, содержащая контрольную сумму (CRC), используемую для проверки целостности данных внутри кадра
HTTP	Hyper Text Transfer Protocol	Протокол передачи гипертекста
HTTPS	Hypertext Transfer Protocol Secure	Безопасный протокол передачи гипертекста
ICMP	Internet Control Message Protocol	Протокол межсетевых управляющих сообщений
IGMP	Internet Group Management Protocol	Протокол управления многоадресной передачей данных в сетях, основанных на протоколе IP. Используется только в сетях IPv4. Аналогичную роль в стеке протоколов IPv6 выполняет протокол MLD
IGMP Snooping	Internet Group Management Protocol Snooping	Протокол отслеживания сетевого трафика IGMP
IP	Internet Protocol	Интернет-протокол
LACP	Link Aggregation Control Protocol	Протокол агрегирования каналов
LAN	Local Area Network	Локальная сеть
LLC	Logical Link Control	Подуровень канального уровня, отвечающий за управление логическими соединениями, кадрами и контроль ошибок, обеспечивая интерфейс между сетью и MAC-подуровнем
LLDP	Link Layer Discovery Protocol	Протокол обнаружения канального уровня
MIB	Management Information Base	Виртуальная база данных, используемая для управления объектами в сети связи
MRP	Media Redundancy Protocol	Протокол резервирования среды передачи данных IEC 62439-2
MST	Multiple Spanning Tree	Множественное связующее дерево
MSTI	Multiple Spanning Tree Instance	Экземпляр множественного связующего дерева
MSTP	Multiple Spanning Tree Protocol	Протокол множественного связующего дерева
NAD	Network Access Device	Устройство сетевого доступа
NAS	Network Access Server	Сервер сетевого доступа
OID	Object Identifier	Идентификатор объекта
PCP	Priority Code Point	Поле в теге VLAN, которое указывает приоритет кадра. Используется для определения уровня приоритета трафика и может принимать значения от 0 (низкий) до 7 (высокий)
PEAP	Extensible Authentication Protocol	Защищенный расширяемый протокол аутентификации

PID	Protocol Identifier	Идентификатор протокола (в кадре Ethernet версии 802.3)
PoE	Power over Ethernet	Технология подачи электропитания на клиентское устройство через витую пару стандарта Ethernet
PPS	Pulse per Second	Импульс, возникающий каждый секунду
PTP	Precision Time Protocol	Протокол точного времени
PVID	Port VLAN Identifier	Идентификатор VLAN по умолчанию для порта
PVLAN	Private VLAN	Частная виртуальная локальная сеть
QCE	QoS Control Entry	Запись списка управления QoS, содержащая правила классификации
QCL	QoS Control List	Список управления QoS
QinQ	802.1Q in 802.1Q	Технология, позволяющая добавлять в маркированные кадры Ethernet второй тег IEEE 802.1Q
QoS	Quality of Service	Качество обслуживания (технология предоставления различным классам трафика различных приоритетов в обслуживании)
RADIUS	Remote Authentication Dial-In User Service	Служба удаленной аутентификации пользователей по коммутируемым линиям
RARP	Reverse Address Resolution Protocol	Протокол определения IP-адреса другого узла по известному MAC-адресу
RIP	Routing Information Protocol	Протокол дистанционно-векторной маршрутизации
RMON	Remote Network Monitoring	Дистанционный мониторинг сети (расширение SNMP, разработанное IETF)
RSTP	Rapid Spanning Tree Protocol	Быстрый протокол связующего дерева (версия протокола STP с ускоренной реконфигурацией дерева)
SCADA	Supervisory Control And Data Acquisition	Диспетчерское управление и сбор данных
SFP	Small Form-factor Pluggable	Промышленный стандарт модульных компактных приемопередатчиков (трансиверов), используемых для передачи и приема данных в телекоммуникациях
SMTP	Simple Mail Transfer Protocol	Протокол для передачи электронной почты через Интернет
SNAP	Subnetwork Access Protocol	Поле заголовка LLC, указывающее протокол сетевого уровня, которому должен быть передан кадр
SNMP	Simple Network Management Protocol	Простой протокол сетевого управления (интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP)

SNTP	Simple Network Time Protocol	Простой протокол синхронизации времени (является упрощённой реализацией протокола NTP)
SSAP	Destination Service Access Point	Точка доступа к сервису системы источника (LLC)
SSH	Secure Shell	«Безопасная оболочка», сетевой протокол прикладного уровня
STP	Spanning Tree Protocol	Протокол связующего дерева
TACACS+	Terminal Access Controller Access Control System	Сеансовый протокол аутентификации, авторизации и учета доступа
TCN	Topology Change Notification	Сообщение об изменении топологии сети
TCP	Transmission Control Protocol	Протокол управления передачей
TFTP	Trivial File Transfer Protocol	Простой протокол передачи файлов
TLS	Transport Layer Security	Криптографический протокол защиты транспортного уровня на базе SSL, обеспечивающий безопасную передачу данных между узлами в сети
TLV	Type Length Value	Структура данных, используемая в протоколе LLDP для передачи информации о сетевых устройствах
ToS	Type of Service	Однооктетное поле в структуре IP-пакета, характеризует то, как должна обрабатываться дейтограмма
TPID	Tag Protocol Identifier	Идентификатор протокола тега – поле в теге VLAN, которое указывает тип протокола тега. Стандарт IEEE 802.1Q требует, чтобы значение этого поля было 0x8100
TTL	Time to Live	Предельный период времени или число итераций (переходов), которые пакет данных может осуществить (прожить) до своего исчезновения
UDP	User Datagram Protocol	Протокол пользовательских дейтаграмм
USM	User-Based Security Model	Модель безопасности на основе пользователей
VACM	View-based Access Control Model	Модель контроля доступа на основе представлений в SNMPv3
VCXO	Voltage-Controlled Crystal Oscillator	Кварцевый генератор, частота которого зависит от внешнего управляющего напряжения
VLAN	Virtual Local Area Network	Виртуальная локальная сеть
VRID	Virtual Router ID	Идентификатор виртуального маршрутизатора VRRP
VRIP	Virtual Router IP	IP-адрес виртуального маршрутизатора VRRP
VRRP	Virtual Router Redundancy Protocol	Протокол резервирования «Виртуальный маршрутизатор»

Техническая спецификация

Порты	
10/100/1000Base-T(X), RJ45, Auto MDI/MDIX	8
100/1000Base-X, SFP	12
Консольный порт	RS-232, RJ45, с консольным кабелем; 115200 бит/с, 8, N, 1
Производительность, технологии и функции ПО	
Стандарты Ethernet	IEEE 802.3 для 10Base-T IEEE 802.3u для 100Base-TX и 100Base-FX IEEE 802.3ab для 1000Base-T IEEE 802.z для 1000Base-X IEEE 802.3x для управления потоком IEEE 802.3ad для LACP (протокол управления агрегацией каналов) IEEE 802.1p для COS (класс обслуживания) IEEE 802.1Q для тегирования VLAN IEEE 802.1w для RSTP (протокол быстрого связующего дерева) IEEE 802.1s для MSTP (протокол множественного связующего дерева) IEEE 802.1x для аутентификации IEEE 802.1AB для LLDP (протокол обнаружения на уровне канала)
Количество MAC-адресов	8000
Приоритетные очереди	8
Режим коммутации	Store-forward
Возможности коммутации	Задержка коммутации: 7 мкс Пропускная способность: 40 Гбит/с Макс. количество доступных VLAN: 4095 Группы многоадресной рассылки IGMP: 128 для каждой VLAN Ограничение скорости порта: определяется пользователем
Jumbo frame	До 9,6 Кбайт
Функции безопасности	Функция привязки устройств Включение/отключение портов, Port Security на основе MAC-адресов Управление сетевым доступом на основе портов (802.1x) Single 802.1x и Multiple 802.1x Аутентификация на основе MAC-адресов QoS Гостевая VLAN Ограничение MAC-адресов TACACS+ VLAN (802.1Q) для разделения и защиты сетевого трафика Централизованное управление паролями Radius Шифрованная аутентификация и безопасный доступ SNMPv3 Аутентификация и авторизация WEB и CLI Авторизация (15 уровней) Защита от подделки IP-адресов HTTPS/SSH
Программные функции	Аппаратная маршрутизация, RIP и статическая маршрутизация Синхронизация часов IEEE 1588v2 Мост IEEE 802.1D, автоматическое изучение/устаревание MAC-адресов, статические MAC-адреса MRP (Multiple Registration Protocol 802.1Q) RSTP/MSTP (IEEE 802.1w/s) Кольцевое резервирование Sy-Ring со временем восстановления менее 30 мс для 250 устройств Поддержка TOS/Diffserv

	QoS (802.1p) для трафика в реальном времени VLAN (802.1Q) с тегированием Голосовая VLAN IGMP v2/v3 Snooping Управление полосой пропускания на основе IP Управление QoS на основе приложений Автоматическое предотвращение DOS/DDOS Управление портами (конфигурация, состояние, статистика, мониторинг, безопасность) DHCP Server/Client/snooping DHCP Relay Modbus TCP Прокси-клиент DNS Проверка ARP Клиент SMTP
Сетевое резервирование	Sy-Ring All-Ring Sy-Union MRP (протокол резервирования среды передачи данных IEC 62439-2) MSTP (RSTP/STP-совместимый)
Светодиодные индикаторы	
Индикатор питания (PWR)	Зеленый: светодиод питания x 2
Индикатор Ring Master (R.M.)	Зеленый: указывает, что система работает в качестве главного узла Sy-Ring
Индикатор Sy-Ring (Ring)	Зеленый: указывает, что система работает в режиме Sy-Ring Мигающий зеленый: указывает, что кольцо разорвано
Индикатор неисправности (Fault)	Желтый: указывает на непредвиденное событие
Индикатор порта 10/100/1000Base-T(X)	Зеленый для индикатора Link/Act 1000 Мбит/с Желтый для индикатора Link/Act 10/100 Мбит/с
Индикатор порта 100/1000Base-X	Зеленый для порта Link/Act
Контакт неисправности	
Реле	Релейный выход с допустимой нагрузкой 1 A при 24 В постоянного тока
Электропитание	
Резервируемые входы питания	Две контактные группы для подключения 12–48 В постоянного тока на 6-контактной клеммной колодке
Защита от перегрузки по току	Есть
Защита от обратной полярности	Есть
Физические характеристики	
Корпус	IP-30
Размеры (Ш x Г x В)	96,4 x 145,5 x 154 мм
Вес	1520 г
Условия окружающей среды	
Температура хранения	от -40 до +85°C
Рабочая температура	от -40 до +70°C
Рабочая влажность	от 5% до 95% без конденсации