НПО “Телеком”
Разработка, производство и внедрение
цифрофых систем передачи данных

Руководство по настройке

Программное обеспечение коммутаторов Ethernet серии NTS

тел. +7 (3412) 573-040
https://npotelecom.ru
тех. поддержка:
+7 (3412) 57-30-32
help@npotelecom.ru

Версия 1.3

Целевая аудитория

Данное руководство по эксплуатации предназначено для технического персонала, выполняющего настройку и мониторинг устройства посредством WEB/CLI конфигуратора, а также процедуры по его установке и обслуживанию. Квалификация технического персонала предполагает знание работы протоколов и принципов построения Ethernet сетей, а также правила электробезопасности.

Данное руководство распространяется на модели: Данное руководство распространяется на модели: NTS-1024, NTS-1024P, NTS-1080, NTS-1080P, NTS NTS-15040P, NTS-15080P, NTS-15050P, NTS-15090P, NTS-15040, NTS-15080, NTS-15050, NTS-15090, NTS-2024, NTS-2024P, NTS-4G2S-PoE-B, NTS-4G2S-PoE+-B, NTS-8G2S-PoE+-B, NTS-25240P, NTS-25240, NTS-25480P, NTS-25480.

№	**Номер версии руководства и дата изм.**	**Внесенные изменения**
1	1.0 от 22.06.2021	Некоторые описанные функции могут находиться в стадии тестирования
2	1.1 от 20.07.2021	Добавлен раздел «Расширенные настройки», описание конфигурации через CLI и Web-интерфейс
3	1.2 от 24.04.2023	Добавлены новые модификации оборудования
4	1.3 от 04.05.2023	Добавлена глава «Конфигурация PPPoE Intermediate Agent». Добавлена информация по настройке IP DHCP Snooping option 82

Оглавление

1 Подключение к коммутатору

Настройка параметров и управление коммутатором осуществляется: через порт Console при подключении к нему внешнего терминала, в качестве которого может использоваться персональный компьютер; через порт Ethernet, управление осуществляется посредством SNMP, Telnet, SSH или Web-интерфейса.

1.1 Подключение через Console (RS-232)

Для установления соединения между консольным портом коммутатора и ПК, необходимо выполнить действия:

- соединить Serial-порт ПК с портом Console коммутатора консольным кабелем.
- запустить на ПК программу (Putty, HyperTerminal), установить настройки:
  - выбрать соответствующий Serial порт компьютера.
  - установить скорость передачи данных 115200.
  - задать формат данных: 8 бит данных, 1 стоповый бит, без контроля четности.
  - включить питание коммутатора.

Если вы выполнили действия правильно, в окне терминала появится лог загрузки коммутатора:

```
DDR3 initializing, ECC mode=4, clk_div=06, 2T=on init_by_pub=0
<>DDR3 up
CIict

U-Boot 2019.10 (Apr 06 2020 - 11:30:43 +0200)fireant

CPU:   ARM A53
Model: FireAnt PCB135/eMMC Reference Board
DRAM:  2 GiB
MMC:   sdhci@600800000: 0
Loading Environment from SPI Flash... SF: Detected mx66l1g45g with page size
256 Bytes, erase size 4 KiB, total 128 MiB
OK
In:    serial@600100000
Out:   serial@600100000
Err:   serial@600100000
Net:   eth0: switch@0
Hit any key to stop autoboot:  0
SF: Detected mx66l1g45g with page size 256 Bytes, erase size 4 KiB, total 128
MiB
Reading 20971520 byte(s) at offset 0x00000000
```

После окончания загрузки необходимо ввести имя пользователя (Username) и пароль (Password) (по умолчанию Username – “admin” Password – отсутствует (поле оставить пустым, нажав клавишу «Enter»). В окне терминала появится приглашение к вводу команд в виде символа «#»:

```
Username: admin
Password:
#
```

По умолчанию учетная запись admin наделена 15 уровнем (наивысший) привилегий системного администратора.

1.1 Подключение через Telnet, SSH

Для подключения к коммутатору, используя протокол Telnet или SSH. Необходимо чтобы на коммутаторе был сконфигурирован ipv4 или ipv6 адрес и хост с Telnet клиентом был доступен с коммутатора (находился в одной сети с ним или был доступен через маршрутизатор).

В текущем примере коммутатор имеет ip-адрес 192.168.0.186, маска 255.255.255.0. Сначала необходимо настроить IP-адрес на ПК, с которого будет осуществляться управление. Настроим адрес 192.168.0.176, маска 255.255.255.0. Соединим ПК и коммутатор патч кордом Ethernet. Выполним команду: `telnet 192.168.0.186 в командной строке ОС или подключимся через Putty.` Затем введем Username и Password (по умолчанию Username – “admin” Password - отсутствует).

```
Username: admin
Password:
#
```

1.2 Подключение через Web-интерфейс

Для доступа к коммутатору через WEB-интерфейс откройте WEB-браузер и введите в адресной строке http://ip-коммутатора. По умолчанию на коммутаторе получение ip-адреса настроено через DHCP, если получить ip-адрес не удалось, устанавливается ip-адрес 192.168.1.1 и маской подсети 255.255.255.0.

В данном примере ip-адрес коммутатора 192.168.0.186. В открывшейся странице введите имя пользователя и пароль (по умолчанию Имя пользователя – “admin” Пароль - отсутствует).

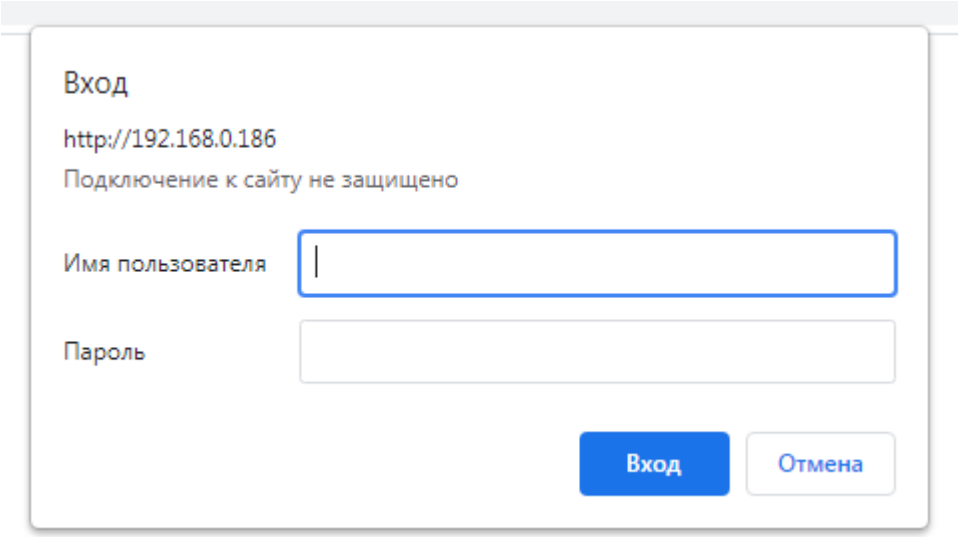


Рисунок 1.1 Страница авторизации

При верном вводе имени пользователя и пароля откроется основной WEB-интерфейс.

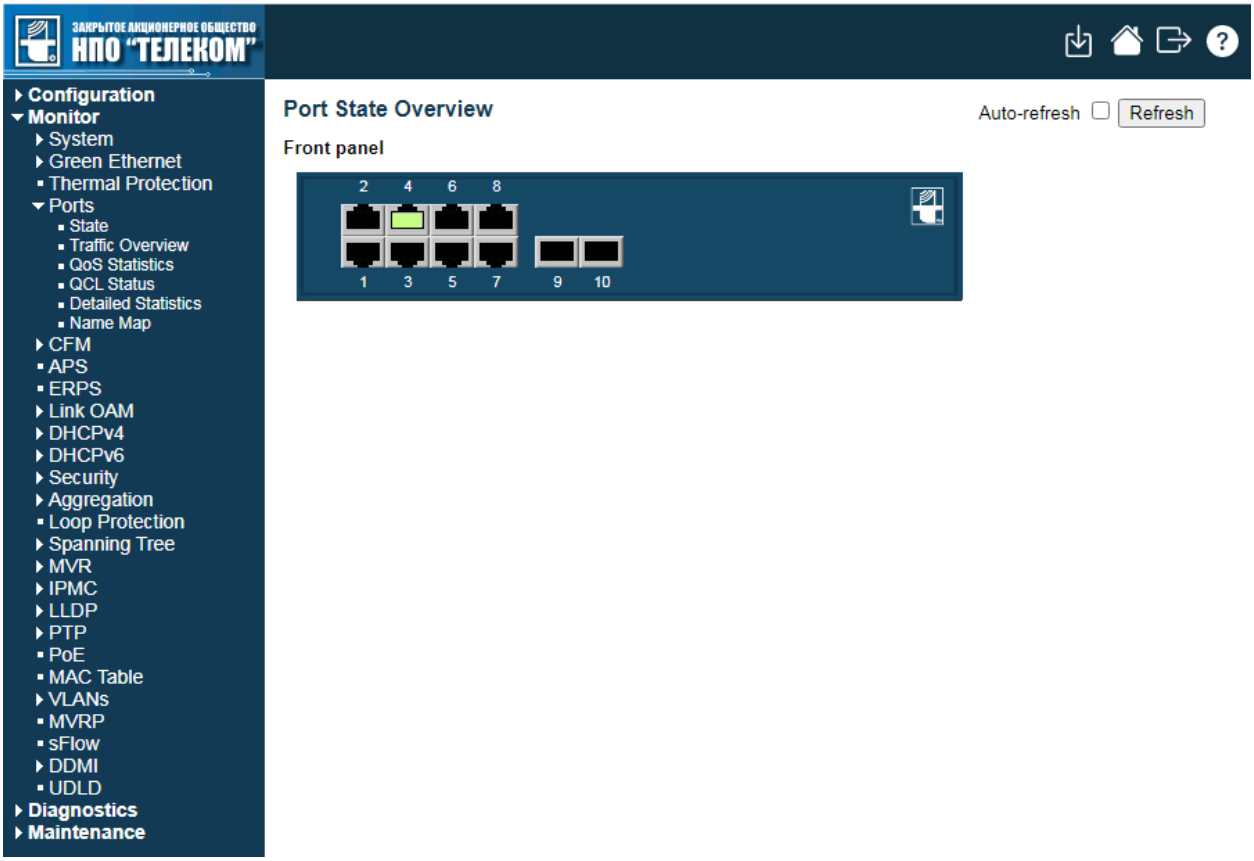


Рисунок 1.1 Основное меню WEB-интерфейса

2 CLI интерфейс

Для настройки, управления и мониторинга через CLI интерфейс, подключитесь к устройству через порт Console (смотри п.1.1), через telnet, SHH (смотри п.1.2).

2.1 Базовые настройки

Данный раздел содержит описание и рекомендации по базовым настройке коммутатора.

2.1.1 Режимы конфигурирования

В интерфейсе командной строки доступно три базовых режима:
- Пользовательский режим
- Привилегированный режим
- Режим глобальной конфигурации (для перехода требуется 15 уровень привилегий и ввод команды “configure terminal”, для выхода из режима требуется ввести команду “exit”)

2.1.2 Работа в командной строке

Интерфейс CLI коммутатора выполнен по промышленным стандартам и обладает типовым наборам команд. Доступны следующие клавиши для редактирования:

Клавиша	Функция
Back Space	Удаляет символ после курсора, позицию курсора не сдвигает.
Вверх	История введенных команд. Выводит предыдущую введенную команду. Многократное нажатие выводит ранее введенные команды по порядку.
Вниз	История введенных команд. Выводит следующую введенную команду.
Влево	Сдвиг курсора на один символ влево
Вправо	Сдвиг курсора на один символ вправо
Ctrl + P	То же что и клавиша «Вверх»
Ctrl + N	То же что и клавиша «Вниз»
Ctrl + Z	Возврат в Admin режим из любого конфигурационного режима
Ctrl + C	Остановка запущенной команды, например ping
Tab	При частичном вводе команды, при нажатии клавиши Tab, выводятся все допустимые варианты продолжения команды.

Для вызова справки в CLI предусмотрены команды:

“`help`” – доступна в любом режиме, выводит краткую информацию по использованию функции справки.

“?” – доступна в любом режиме, выводит список всех допустимых команд с их описанием.

В случае некорректного ввода команды возвращается информация об ошибке:

`% Incomplete command.` – команда введена не полностью либо отсутствует обязательный параметр.

`% Invalid word detected at '^' marker.` – неправильный ввод команды. Маркер '^' указывает на место неправильного ввода.

`% Ambiguous word detected at '^' marker.` – Введенная команда имеет два и более варианта интерпретации. Маркер '^' указывает на место неправильного ввода.

CLI поддерживает сокращенный ввод команд, если введенная строка может быть однозначно дополнена до полной команды и интерпретирована в случае единственно возможного варианта интерпретации. В ином случае вернется ошибка вида: "`% Ambiguous word detected at '^' marker.`"

2.1.3 Создание учетной записи

Пример создания учетной записи через интерфейс командной строки:

```
# configure terminal
(config)# username operator privilege 15 password unencrypted operator
(config)#
```

Разберем введённые команды:

`configure terminal` – переход в режим глобальной конфигурации.

`username operator privilege 15 password unencrypted operator`- создание пользователя с именем **operator**, наивысшим уровнем привилегий (15) и паролем **operator**

2.1.4 Сохранение конфигурации, перезагрузка и возврат к заводским настройкам

Для сохранения внесенных изменений в конфигурацию коммутатора требуется выйти из режима глобальной конфигурации и ввести команду "`copy running-config startup-config`", либо в режиме глобальной конфигурации ввести команду "`do copy running-config startup-config`".

Пример сохранения конфигурации в энергонезависимую память:

```
(config)# do copy running-config startup-config
Building configuration...
% Saving 1631 bytes to flash: startup-config
```

Для перезагрузки устройства воспользуйтесь командой `reload cold` в привилегированном режиме.

Пример ввода в терминале:

```
# reload cold
% Cold reload in progress, please stand by.
Rebooting system...
```

Для возврата к заводским установкам выполните команду `reload defaults.` В данном случае коммутатор не будет перезагружен.

Пример ввода в терминале:

```
# reload defaults
% Reloading defaults. Please stand by.
```

2.1.5 Настройка имени устройства

Пример создания учетной записи через интерфейс командной строки:

```
# configure terminal
(config)# hostname switch
switch(config)#
```

Задание имени хоста выполняется вводом команды `hostname <имя устройства>`. Ввод команды доступен из режима глобальной конфигурации. После выполнения команды, в терминале, перед символом “#” будет отображаться имя вашего устройства. Для отмены команды введите “`no hostname`”

2.1.6 Конфигурация интерфейсов

Для перехода в режим конфигурации интерфейсов необходимо в режиме глобальной конфигурации ввести команду `interface <name>.` Всего поддерживается три вида интерфейсов, соответственно возможны команды:

-`interface GigabitEthernet <port_type_list>` (Настройка параметров физических интерфейсов)

-`interface llag <1-5>` (Настройка параметров llag интерфейсов)

-`interface vlan <vlan_list>` (Настройка L3 интерфейсов коммутатора)

2.1.7 Настройка параметров физических интерфейсов

Как описано в п. 2.1.6., для настройки параметров физических интерфейсов, необходимо перейти в режим глобальной конфигурации и ввести команду `interface GigabitEthernet <port_type_list>` (где `<port_type_list>` -это номер или диапазон интерфейс(а)(ов), допустимы несколько вариантов ввода:

```
(config)# interface GigabitEthernet 1/1
```

```
(config-if)#
```

```
(config)# interface GigabitEthernet 1/1-4
(config-if)#
```

```
(config)# interface GigabitEthernet 1/1,4
(config-if)#
```

Команда	Описание
shutdown no shutdown	Выключение интерфейса Включение интерфейса
speed {10|100|1000|auto}	Настройка скорости физического порта: 10 – 10mb/s 100-100mb/s 1000-1000mb/s auto – автоматическое согласование скорости (есть возможность дополнительно указать какие скорости разрешить при автосогласовании)
duplex {auto|full|half}	Настройка режима дуплекса auto – автоматическое со гласование дуплекса full - полный дуплекс half - полудуплекс
description <описание> no description	назначение описания интерфейса удаление описания интерфейса

2.1.8 Настройка L3 интерфейсов коммутатора

По умолчанию на коммутаторе создан L3 интерфейс “vlan 1” с ip-адресом 192.168.1.1 и маской подсети 255.255.255.0.

Для настройки параметров L3 интерфейсов необходимо перейти в режим глобальной конфигурации и ввести команду interface vlan <vlan_list> (где <vlan_list> - это номер или диапазон интерфейс(а)(ов), если такого номера интерфейса еще нет на коммутаторе, то он будет создан автоматически), допустимы несколько вариантов ввода:

```
(config)# interface vlan 1
(config-if-vlan)#
```

```
(config)# interface interface vlan 1-4
(config-if-vlan)#
```

```
(config)# interface interface vlan 1,4
(config-if-vlan)#
```

Команда	Описание
ip address <ipv4_addr>	Назначение интерфейсу статического ipv4-

<ipv4_subnet> no ip address <ipv4_addr> <ipv4_subnet> ip address dhcp	адреса, где <ipv4_addr> - ip-адрес, а <ipv4_subnet>– маска подсети Удаление статического ip-адреса с интерфейса Получение ipv4-адреса автоматически от сервера dhcp
add ip address <ipv4_addr> <ipv4_subnet> del ip address	Назначение интерфейсу дополнительного статического ipv4-адреса, где <ipv4_addr> - ip-адрес, а <ipv4_subnet>– маска подсети Удаление дополнительного статического ip-адреса с интерфейса
ipv6 address <ipv6_subnet> no ip address <ipv6_subnet> ipv6 address dhcp	Назначение интерфейсу статического ipv6-адреса, где <ipv6_subnet> - ip-адрес_ маска подсети Удаление статического ip-адреса с интерфейса Получение ipv6-адреса автоматически от сервера dhcp
ip cos <0-7> no ip cos	Настройка маркировки исходящего трафика с интерфейса управления. Отмена команды.

Для удаления L3 интерфейса в режиме глобальной конфигурации введите команду:
no interface vlan <vlan_list> (где <vlan_list> - это номер или диапазон интерфейс(а)(ов)).

2.1.9 Настройка маршрутов

Для создания статического маршрута используется команда ip route <ipv4_addr> <ipv4_subnet> <ipv4_ucast>, где <ipv4_addr> – целевой адрес для удаленной сети, <ipv4_subnet> – маска подсети для удаленной сети, <ipv4_ucast> – ip-адрес следующего перехода для пересылки пакетов в удаленную сеть. Доступна в режиме глобальной конфигурации.

Пример настройки статического маршрута:

```
(config)# ip route 192.168.10.0 255.255.255.0 192.168.10.1
```

Для удаления маршрута применяется команда no ip route

```
(config)# no ip route 192.168.10.0 255.255.255.0 192.168.10.1
```

2.1.10 Настройка времени

2.1.11 Настройка NTP

Команда	Описание
ntp no ntp	Включение функции ntp Выключение функции ntp
ntp server <1-5> <domain name> < ipv4_ucast> <ipv6_ucast> no ntp server <1-5>	Позволяет указать адрес или доменное имя NTP-сервера. Возможно настроить до 5 адресов. Выключает указанный NTP-сервер.

2.1.11.1 Конфигурация часового пояса

Команда	Описание
clock timezone <word16> <-23-23>	<word16> - акроним для определения часового пояса <-23-23> - соответствующий часовой пояс
clock summer-time <word16> date <start time> <end time> <offset>	Конфигурация перехода на летнее время <word16> - акроним для определения часового пояса <start time> – время начала действия в формате (MM DD YYYY HH:MM) <end time> – время окончания действия в формате (MM DD YYYY HH:MM) <offset> – количество минут для добавления в летнее время

2.1.12 Конфигурация журнала системных сообщений

System log (системный журнал) — стандарт отправки и регистрации сообщений о происходящих в системе событиях (то есть создания логов), использующийся в компьютерных сетях, работающих по протоколу IP. Настройка доступна из режима глобальной конфигурации.

Команда	Описание
logging on no logging on logging flash no logging flash	Режим работы: включен. Режим работы: выключен. сохранение лога в энергонезависимую память отмена команды

debug logging flash debug logging erase platform debug allow	просмотр журнала в энергонезависимой памяти удаление записей журнала из энергонезависимой памяти переход в режим debug
logging host {<domain_name> | <ipv4_ucast>}	Настройка адреса syslog-сервера где <domain_name> - имя сервера <ipv4_ucast> - ipv4-адрес сервера
logging level {error | informational | notice | warning}	Выбор типа отправляемых сообщений. Error – отправлять только ошибки Informational – отправлять информ. сообщения, уведомления, предупреждения и ошибки. Notice – отправлять уведомления, предупреждения и ошибки. Warning – отправлять предупреждения и ошибки.

Пример настройки в терминале (включение ведения журнала событий, установка адреса syslog-сервера с адресом 192.168.0.176, выбор типа сообщений для записи в журнале – все):

```
(config)# logging on
(config)# logging host 192.168.0.176
(config)# logging level informational
```

2.1.13 VLAN

Использование виртуальных локальных сетей VLAN (Virtual Local Area Network) является популярным и недорогим способом сегментирования развернутой сети по логически сгруппированным устройствам безотносительно к их физическим соединениям. Сети VLAN также сегментируют сеть на различные 104 широковещательные домены таким образом, что пакеты передаются на порты внутри VLAN, которой они принадлежат.

Сети VLAN повышают безопасность. Устройства, которые часто связываются друг с другом группируются в одну и ту же VLAN. Если устройства данной VLAN желают связаться с устройствами в другой VLAN, трафик должен пройти через устройство маршрутизации или коммутатор 3-го уровня.

Сети VLAN упрощают управление трафиком. В обычных сетях, не сегментированных на VLAN, легко возникает перегрузка, обусловленная широковещательным трафиком, адресованного всем устройствам. Сводя к минимуму распространение широковещательного трафика по всей сети, сети VLAN облегчают работу устройствам группы, часто связывающимся с другими устройствами в той же VLAN за счет деления всей сети на несколько доменов вещания.

Для доступа к настройкам необходимо перейти в режим глобальной конфигурации, а также настроить необходимые порты.

Команда	Описание
Глобальные настройки	

`vlan <vlan_list>`
 	
`no vlan <vlan_list>`
	Создание vlan и переход в режим конфигурации vlan
	
	Удаление vlan

`name <vword32>`
 	
`no name <vword32>`
	Настройка имени vlan
	
	Удаление имени

`vlan ethertype s-custom-port`	Настройка типа ethertype/TPID, используемого для специализированных s-портов
Настройка портов	
`interface GigabitEthernet <port_type_list>`	Выбор портов для настройки параметров
`switchport mode {access | hybrid | trunk}`	Настройка режима работы порта `access` (Доступ): Порты доступа, как правило, используется для подключения к конечным станциям. Динамические функции, такие как Voice VLAN могут добавить порт к большему количеству VLAN. Порты доступа имеют следующие характеристики: - Принадлежит ровно к одной VLAN (port VLAN). - Принимает нетегированные и тегированные кадры. - Удаляет все кадры, которые не классифицируются как access VLAN. - На выходе все кадры, классифицированные как Access VLAN, передаются без тегов. Другие (динамически добавленные VLAN) передаются с тегами. `trunk` (Магистральные): Магистральные порты могут передавать трафик на несколько виртуальных локальных сетей одновременно и, как правило, используется для подключения к другим коммутаторам. Магистральные порты имеют следующие характеристики: - По умолчанию, trunk-порт является членом всех VLAN (1-4095). - VLAN, членом которых является магистральный порт, может быть ограничено путем использования Allowed

	VLAN. - Кадры, классифицированные с VLAN, членом которых порт не является, 106 отбрасываются. - По умолчанию, все кадры, кроме кадров, классифицированных как port VLAN, передаются тегированными. Кадры, классифицированные в port VLAN, не получают С-тегами на выходе - Можно настроить устройство тегировать на выходе все кадры, в этом случае только тегированные кадры будут приниматься на входе. `hybrid` (Гибридные): Гибридные порты схожи с портами типа Trunk во многих отношениях, но имеют дополнительные функции. В дополнение к характеристикам, описанным для trunk-портов, гибридные порты имеют следующие возможности: -Могут быть сконфигурирован как VLAN unaware, C-tag, S-tag или Scustom tag. - С возможностью фильтрации на входе. - Обработка входящих кадров и конфигурацию выходного тегирования можно настроить независимо.

`switchport access vlan vlan_id>`
 	
`switchport trunk allowed vlan <vlan_list>`
 	
`switchport hybrid allowed vlan <vlan_list>`
	Настройка VLAN ID для порта. Допустимый диапазон значений: от 1 до 4095. По умолчанию задано. Команды приведены в зависимости от режима работы порта.
	
	Порты в режимах Trunk и Hybrid могут контролировать членами каких VLAN они могут становиться. Порты в режиме Access может быть членом только одной VLAN, access VLAN. Поле может быть оставлено пустым. В таком случае, порт не будет членом ни одной VLAN.

`switchport forbidden vlan add <vlan_list>`	Настройка порта для того чтобы никогда не становиться членом определенных VLAN. Это может быть полезно при использовании динамических протоколов, работающих с VLAN, например, GVRP. По умолчанию, поле оставлено пустым и ограничений не накладывается.
`switchport hybrid ingress-filtering`	Настройка фильтрации входящих кадров. Если фильтрация входящих кадров включена и входящий кадр не принадлежит VLAN, указанному на

	данном порту, такой кадр отбрасывается. Если фильтрация входящих кадров выключена и входящий кадр не принадлежит VLAN такой кадр принимается и передается в коммутатор. По умолчанию фильтрация входящих кадров включена для портов в режимах access и trunk.
`switchport hybrid acceptable-frame-type {all | tagged | untagged}`	Настройка режима обработки входящих кадров (доступно только для Hybrid портов) `All` – Тегированные и нетегированные кадры принимаются. `Tagged` – Только тегированные кадры принимаются. Нетегированные - отбрасываются `Untagged` – Только не тегированные кадры принимаются. Тегированные - отбрасываются.
`switchport hybrid egress-tag { all | none}`	Настройка тегирования на выходе для hybrid портов. All - Все кадры передаются с метками. None - Все кадры передаются без меток. По умолчанию - кадры с меткой VLAN совпадающей с port VLAN передаются не тегированными. Остальные кадры передаются со своими метками.
`switchport trunk vlan tag native`	Настройка тегирования на выходе для trunk портов. При такой команде все кадры передаются с метками.
`switchport {trunk | hybrid} native vlan <vlan_id>`	Настройка Port VLAN
`switchport hybrid port-type {c-port | s-custom-port | s-port | unaware}`	Конфигурация гибридных портов. `c-port` – если во входящем тегированном кадре TPID=0x8100, он передается. Если кадр нетегированный или приоритетно тегированный в него добавляется тег port VLAN. Исходящие кадры тегируются меткой C-tag. `s-custom-port` – если во входящем тегированном кадре TIPID=0x8100 или Ethertype for Custom Sports он передается. Если кадр нетегированный или приоритетно тегированный в него добавляется тег port VLAN. Исходящие кадры тегируются меткой Custom S-tag. `s-port` – если во входящем

	тегированном кадре TIPID=0x8100 или 0x88A8, он передается. Если кадр нетегированный или приоритетно тегированный в него добавляется тег port VLAN. Исходящие кадры тегируются меткой S-tag. `unaware` – все входящие кадры, вне зависимости от того есть ли у них тег или нет, тегируются меткой port VLAN (PVID). Разрешенные VLAN не удаляются на выходе

Пример создания vlan:

```
(config)# vlan 90
(config-vlan)# name office
```

Пример настройки vlan на физическом интерфейсе:

```
(config)# interface GigabitEthernet 1/7-8
(config-if)# switchport mode trunk
(config-if)# switchport trunk allowed vlan 90
```

Разберем команды:

- Выбор необходимых интерфейсов для настройки (порт 7 и 8)
- Перевод интерфейсов в режим trunk
- Добавление vlan 90 (tagged)

2.2 Расширенные настройки

2.2.1 DHCP

2.2.1.1 DHCPv4

DHCP (протокол динамической настройки узла) — сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации, клиент на этапе конфигурации сетевого устройства обращается к так называемому серверу DHCP и получает от него нужные параметры.

Команда	Описание
Глобальные настройки	

`ip dhcp server`
 	
`no ip dhcp server`
	Включить DHCP сервер
	
	Выключить DHCP сервер

ip dhcp excluded-address <ipv4_addr> <ipv4_addr> no ip dhcp excluded-address <ipv4_addr> <ipv4_addr>	Добавить диапазон-группу исключаемых IP адресов. Обычно адреса шлюзов, так как DHCP сервер не должен раздавать адреса шлюзов клиентам Удалить диапазон-группу исключаемых IP адресов.
Настройка пула адресов	
ip dhcp pool <word32>	Создать пула ip-адресов, назначить имя
no ip dhcp pool <word32>	Удалить пул ip-адресов
{host | network} <ipv4_ucast> <ipv4_netmask>	Выбор типа пула задание ip-адреса и маски подсети пула
lease <0-365>	Время аренды адреса. По умолчанию время аренды равно 24 часам. Можно выставить свое время аренды.
DHCP Snooping	
ip dhcp snooping vlan <vlan_list>	Включить функцию DHCP snooping в отдельном vlan
ip dhcp snooping max-client <1-2048>	Задание максимального числа клиентов (по умолчанию 2048)
ip dhcp snooping option82	Включение опции 82
ip dhcp snooping circuit-id <word> remote-id <word> format ascii	Задание формата опции 82
DHCP Relay	
ip dhcp relay no ip dhcp relay	Включение функции DHCP Relay Выключение функции DHCP Relay
ip dhcp relay information option no ip dhcp relay information option	Включение режима информации DHCP-ретранслятора. Когда включен режим передачи информации DHCP, агент вставляет определенную информацию (параметр 82) в сообщение DHCP при пересылке на сервер DHCP и удаляет ее из сообщения DHCP при передаче на клиент DHCP. Работает только при включенном режиме работы DHCP-ретранслятора. Отключить режим добавления информации (параметр 82) DHCP-ретранслятора.
ip dhcp relay information policy { drop | keep | replace}	Настройка правила для параметра информации о ретрансляции DHCP. Возможные правила: replace: Заменить исходную информацию keep: Сохранить исходную информацию. drop: Отбросить пакет
Настройка портов	

interface GigabitEthernet <port_type_list>	Выбор портов для настройки параметров
ip dhcp snooping no ip dhcp snooping	Включение функции DHCP snooping Выключение функции DHCP snooping
ip dhcp snooping trust no ip dhcp snooping trust	Настройка режима для порта: Доверенный (Trusted) — порт коммутатора, к которому подключен другой коммутатор или DHCPсервер. DHCP-пакеты, полученные с доверенного порта, не отбрасываются. Ненадёжный (Untrusted) — порт, к которому подключен клиент. DHCP-ответы, приходящие с этого порта, отбрасываются коммутатором. Для ненадёжных портов выполняется ряд проверок сообщений DHCP и создаётся база данных привязки DHCP (DHCP snooping binding database).

2.2.1.2 DHCPv6

Команда	Описание
Глобальные настройки	
ipv6 dhcp snooping no ipv6 dhcp snooping	Включить режим DHCPv6 snooping. Когда включен режим DHCPv6 snooping, сообщения запроса клиента DHCPv6 будут пересылаться на доверенные порты и разрешать ответные пакеты только от доверенных портов. Выключить режим DHCPv6 snooping
ipv6 dhcp snooping nh-unknown {allow | drop}	Выбор обработки неизвестных значений заголовка IPv6. Коммутатор должен анализировать все пакеты IPv6 для клиента DHCPv6, чтобы определить, действительно ли это сообщение DHCPv6 Возможные варианты: drop- Отбрасывать пакеты с неизвестными заголовками расширения IPv6. Это наиболее безопасный вариант, но он может привести к перебоям в трафике. allow- Разрешить пакеты с неизвестными заголовками расширения IPv6. Это менее безопасный вариант, но он предотвращает перебои в трафике.
Dhcp6_Relay для определенного vlan.	
interface vlan <vlan_list>	Создание интерфейса Vlan

ipv6 dhcp relay interface vlan <vlan_id>	Указание идентификатора интерфейса, используемого для ретрансляции.
ipv6 dhcp relay destination <ipv6_ucast>	Указание адреса IPv6. IPv6-адрес сервера DHCPv6, на который должны быть ретранслированы запросы. Значение по умолчанию «ff05 :: 1: 3» означает «любой DHCP-сервер».
Настройка портов	
interface GigabitEthernet <port_type_list>	Выбор портов для настройки параметров
ipv6 dhcp snooping trust no ipv6 dhcp snooping trust	Настройка режима работы порта как надежный источник сообщений DHCPv6. Отмена команды и установка режима работы как ненадежный источник сообщений DHCPv6.

2.2.2 Уровни привилегий. Privilege Levels

Команда	Описание
Глобальные настройки	
web privilege group { APS | Aggregation | Alarm | CFM | DDMI | DHCP | DHCPv6_Client | Debug | Diagnostics | ERPS | ETH_LINK_OAM | Firmware | Green_Ethernet | IP | IPMC_Snooping | LACP | LLDP | Loop_Protect | MAC_Table | MRP | MVR | Miscellaneous | NTP | POE | PTP | Ports | Private_VLANs | QoS | RMirror | Security(access) | Security(network)| Spanning_Tree | System | UDLD | UPnP | VCL | VLAN_Translation | VLANs | Voice_VLAN | XXRP | sFlow | uFDMA_AIL | uFDMA_CIL} level {configRoPriv | configRwPriv | statusRoPriv | statusRwPriv} <0-15>	Выбор группы и настройка уровня привелегий для одного или нескольких модулей: -System: Contact, Name, Location, Timezone, Daylight Saving Time, Log; -Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard; -IP: все, кроме ping; -Ports: все, кроме VeriPHY; -Diagnostics: ping и VeriPHY; - Maintenance: CLI - System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web - Users, Privilege Levels и все в Maintenance; -Debug configRoPriv – Конфигурация: только чтение configRwPriv – Конфигурация:

	чтение и запись `statusRoPriv` - Статус/статистика: только чтение `statusRwPriv` - Статус/статистика: чтение и запись Уровень привилегий группы от 0 до 15. Привилегия пользователя должна быть такой же или больше, чем уровень этой группы, чтобы иметь доступ к этой группе.

`ip dhcp excluded-address <ipv4_addr> <ipv4_addr>`
 	
`no ip dhcp excluded-address <ipv4_addr> <ipv4_addr>`
	Добавить диапазон-группу исключаемых IP адресов. Обычно адреса шлюзов, так как DHCP сервер не должен раздавать адреса шлюзов клиентам
	
	Удалить диапазон-группу исключаемых IP адресов.

2.2.3 Конфигурация аутентификации, авторизации и учета. Authentication, Authorization, Accounting

Authentication (аутентификация) — сопоставление запроса существующей учётной записи в системе безопасности.

Authorization (авторизация, проверка уровня доступа) — сопоставление учётной записи в системе (прошедшей аутентификацию) и определённых полномочий.

Accounting (учёт) — слежение за потреблением ресурсов пользователем.

Команда	Описание
Глобальные настройки	

`aaa authentication login {console | http | ssh | telnet} {local | radius | tacacs}`
 	
`no aaa authentication login {console | http | ssh | telnet}`
	`Local` - использовать локальную базу данных на коммутаторе для проверки подлинности;
	`Radius` - использовать удаленные серверы RADIUS для аутентификации; - `Tacacs` - использовать удаленные серверы TACACS для аутентификации;
	
	Отключение аутентификации, и вход в систему невозможен;

`aaa authorization { console | ssh | telnet } tacacs`	`Tacacs` - для авторизации команд используется один или несколько удаленных серверов TACACS+. Если все удаленные серверы находятся в автономном режиме, пользователю предоставляется доступ к командам CLI в

`no aaa authorization { console | ssh | telnet }`	соответствии с его уровнем привилегий. Отключение авторизации. Пользователь получает доступ к командам CLI в соответствии со своим уровнем привилегий

`aaa accounting { console | ssh | telnet } tacacs {commands | exec}`
 	
`No aaa accounting { console | ssh | telnet }`
	`Commands` - Включает учет всех команд с уровнем привилегий выше или равным этому уровню. Допустимые значения находятся в диапазоне от 0 до 15. Оставьте поле пустым, чтобы отключить учет команд.
	`Exec` - Режим учета EXEC
	
	Отключение учета

2.2.4 Конфигурация SSH, HTTPS

Команда	Описание
Глобальные настройки	

`ip ssh`
 	
`no ip ssh`
	Включить ssh
	
	Выключить ssh

`ip http secure-server`
 	
`no ip http secure-server`
	Включение режима HTTPS.
	
	Выключение режима HTTPS

`ip http secure-certificate {delete | generate | upload}`
 	
`No ip http secure-certificate`
	Настройка обслуживания сертификации. Возможные действия:
	`Delete` - удалить сертификат
	`Upload` - загрузка сертификата, можно выбрать два метода загрузки. Необходимо ввести ссылку на сертификат.
	`Generate` - создание сертификата.
	
	Отключение сертификации

`ip http secure-redirect`
 	
`No ip http secure-redirect`
	Включение режима автоматического перенаправления HTTPS. Применяется только, если для режима работы HTTPS включен. Автоматически направляет HTTP web-браузера на соединение HTTPS, когда включены оба режима работы – HTTPS и Automatic Redirect
	
	выключение режима автоматического перенаправления HTTPS

2.2.5 Конфигурация управления доступом. Access Management Configuration

Команда	Описание
`access management` `no access management`	Режим работы: включен. Режим работы: выключен.
`access management <1-16> <1-4095> {<ipv4_ucast> | <ipv6_ucast>} to <ipv4_ucast>} {telnet | web | snmp}`	Пример настройки доступа `<1-16>` – указывает на порядковый номер правила (всего возможно настроить 16 правил) `<1-4095>` – номер vlan для элемента управления доступом. `{<ipv4_ucast> | <ipv6_ucast>} to <ipv4_ucast>}` – диапазон ip-адресов для управления доступом. Допускается запись только одного ip-адреса. `telnet web snmp` – сервисы к которым будет предоставлен доступ.
`no access management <1-16>`	Отключение указанного номера записи в списке управления доступом.

2.2.6 SNMP

Команда	Описание
Глобальные настройки	
`snmp-server` `no snmp-server`	Включить `snmp-server` Выключить `snmp-server`
Trap Configuration	
`snmp-server host <word32>` `no snmp-server host <word32>`	Создание snmp-ловушки Удаление snmp-ловушки
`no shutdown` `shutdown`	Включение отправки SNMP trap Выключение отправки SNMP trap
`Version {v1 | v2 | v3} <word63>`	Выбор версии протокола snmp `<word63>` - trap community
`Host {<domain_name> | <ipv4_ucast> | <ipv6_ucast>} {informs | traps} <1-65535>`	Настройка ip-адреса сервера для отправки SNMP trap. Корректный IP-адрес в десятичном формате с точкой. Допустимо также указать корректное имя хоста. Выбор режима работы snmp (informs или

	trap) и указание UDP порта, по умолчанию порт 162.
informs retries <0-255> timeout <0-2147>	Установка таймера попыток повторения сообщений SNMP trap inform. Диапазон допустимых значений: от 0 до 255. Установка таймера сообщений SNMP trap inform. Диапазон допустимых значений: от 0 до 2147.
SNMPv3 community	
snmp-server community <word32> <word32> ip-range <ipv4_addr> <ipv4_netmask> no snmp-server community <word32>	Создание имени и пароля snmp community. Указание ip-адреса и маски источника при доступе по SNMP Удаление указанной записи.
snmp-server engine-id local <word10-64>	Настройка идентификатора engine ID для SNMPv3. Строка должна содержать четное число (в 16-ном формате), число 39 цифр от 10 до 64; комбинации цифр, состоящие из одних нулей и из одних «F» недопустимы.
SNMPv3 User Configuration	
snmp-server user <word32> engine-id <word10-64> { md5 | sha} <word8- 32 | 40> priv { aes | des} <word8-32>	Создание записи user <word32> - имя пользователя, которому принадлежит данный параметр. Допустимая длина строки 1~32 символов ASCII с 43 номерами в диапазоне от 0x21 до 0x7E. engine-id <word10-64> - индентификатор. В архитектуре SNMPv3 используется модель безопасности на основе пользователя USM (User based Security Model) для обеспечения безопасности сообщений и модель управления доступом на основе вида VACM (View-based Access Control Model) при управлении доступом. Для входа USM ключами входов являются usmUserEngineID и usmUserName. В простом агенте usmUserEngineID всегда совпадает с собственным значением snmpEngineID агента. В качестве значения также может использоваться значение snmpEngineID удаленного устройства (SNMP engine), с которым может связываться данный пользователь. Другими словами, если engine ID

	пользователя равен engine ID системы, то он является локальным пользователем, в противном случае пользователь является удаленным. `md5, sha` – протоколы аутентификации, если не указывать конкретный протокол - значит протокол отсутствует. При выборе протокола требуется ввести пароль для аутентификации. `Aes, des` – протоколы конфиденциальности, если протокол не выбран – значит протокол отсутствует. При выборе протокола требуется ввести пароль конфиденциальности.
SNMPv3 Group Configuration	

`snmp-server security-to-group model {v1 | v2c | v3} name <word32>`
`group <word32>`
 	
`no snmp-server security-to-group model v1 name <word32>`
	Настройка групп SNMP
	`v1 | v2c | v3` – выбор модели безопасности, каждая зарезервирована в соответствии с версией SNMP
	`name <word32>` - назначение имени безопасности
	`group <word32>` - назначение имени группы.
	
	Удаление соответствующей группы

SNMPv3 View Configuration	

`snmp-server view <word32> <word255> {exclude | include}`
 	
`No snmp-server view <word32> <word255>`
	`<word32>` - указание имени
	`<word255>` - указание OID
	`exclude include` – выбор типа included (поддерево включено): дополнительный флаг, указывающий, что в вид должно быть включено поддерево. • excluded (поддерево исключено): дополнительный флаг, указывающий, что из вида должно быть исключено поддерево. В целом, если для типа вида задано ' excluded ' (поддерево исключено), должен существовать другой вид с типом ' included ' (поддерево включено) и его поддерево OID должно перекрывать поддерево вида с типом ' excluded ' (поддерево исключено).
	
	Удаление соответствующей записи

SNMPv3 Access Configuration	
`snmp-server access <word32>`	Настройка доступа SNMPv3

model {any | v1 | v2c | v3} level { auth | noauth | priv}{read | write} <word32>	<word32> - имя группы any | v1 | v2c | v3 – выбор модели безопасности level {auth | noauth | priv} – выбор уровня безопасности auth - Выполняется аутентификация, конфиденциальность отсутствует. Noauth - Аутентификация и конфиденциальность отсутствуют. Priv - Выполняется аутентификация, обеспечивается конфиденциальность read | write <word32> - имя вида MIB, определяющего объекты MIB. Read – используется для чтения текущих значений Write - используется для установки новых значений

2.2.7 RMON

Команда	Описание
Alarm	
rmon alarm <1-65535> {ifInDiscards | ifInErrors | ifInNUcastPkts |ifInOctets | ifInUcastPkts | ifInUnknownProtos | ifOutDiscards | ifOutErrors | ifOutNUcastPkts | ifOutOctets | ifOutQLen | ifOutUcastPkts} <uint> <1-2147483647> {absolute | delta} rising-threshold <-2147483648-2147483647> <0-65535> falling-threshold <-2147483648-2147483647> <0-65535> {both | falling | rising}	Настройка аварийных сигналов <1-65535> - Индекс {ifInDiscards | ifInErrors | ifInNUcastPkts |ifInOctets | ifInUcastPkts | ifInUnknownProtos | ifOutDiscards | ifOutErrors | ifOutNUcastPkts | ifOutOctets | ifOutQLen | ifOutUcastPkts} - выбор переменной <uint> - номер интерфейса <1-2147483647>- интервал опроса при выборке и сравнении с нижним или верхним пороговым значением. absolute | delta –выбор типа. Для указанной переменной тест может быть выполнен для абсолютных значений или их относительного изменения. rising-threshold <-2147483648-2147483647> - Включает сигнализацию, когда значение первый раз превысит пороговое значение подъема либо станет меньше, чем пороговое значение спада <0-65535> - Индекс подъема для

	события. `falling-threshold <-2147483648-2147483647> -` Пороговое значение спада. Если текущее значение станет меньше порогового значения спада и, при этом, последнее значение выборки больше этого порогового значения, то выдается сигнализация. После генерации события спада, другое такое событие не будет сгенерировано до тех пор, пока значение выборки не станет больше порогового 49 значения спада, достигнет порогового значения подъема и снова вернется к пороговому значению спада. `<0-65535> -` Индекс спада для события `{both | falling | rising} -` Выбор метода, который будет использоваться для выборки выбранной переменной и вычисления значения, которое сравнивается с пороговыми значениями.
Event	
`rmon event <1-65535> {log | trap} description <line127>`	Настройка событий. `<1-65535>` - Индекс `{log | trap}` – выбор типа `log`: Когда генерируется событие, генерируется и запись журнала RMON. `trap`: посылает сообщение trap всем установленным менеджерам сообщений trap. `Log trap`: О событии создается запись в журнале, посылается сообщение trap. `description <line127>` - описание

2.2.8 Port Security

Функция управлением безопасностью порта (Port Security Limit Control) может ограничить число пользователей, которым разрешен доступ к коммутатору на основе MAC- адресов и VLAN ID (выполняется для каждого порта). Как только число пользователей, желающих получить доступ к коммутатору, превысит заданное число, будет немедленно выполнена выбранная операция.

Команда	Описание
Глобальные настройки	

port-security aging no port-security aging	Включить функцию устаревания. Если функция включена, то оценивается «возраст» безопасных MAC-адресов в том смысле, в котором он учитывается параметром Aging Period (Срок устаревания). Когда устаревание включено, с того момента, как конечный хост станет безопасным, запускается таймер. По истечении таймера, коммутатор начинает искать кадры конечного хоста и, если таких кадров не появляется в течение следующего срока устаревания (Aging Period), то предполагается, что конечный хост отключился и на коммутаторе освобождаются соответствующие ресурсы Выключить функцию устаревания.
port-security aging time <10-10000000>	Установка срока устаревания. По умолчанию установлен срок устаревания 3600 секунд.
port-security hold time <10-10000000>	Настройка времени удержания, используется для определения того, как долго MAC-адрес хранится в таблице MAC-адресов, если было обнаружено, что он нарушает ограничение. Допустимый диапазон составляет от 10 до 10 000 000 секунд, по умолчанию - 300 секунд.
Настройка портов	
interface GigabitEthernet <port_type_list>	Выбор портов для настройки параметров
port-security no port-security	Включение управления ограничением количества хостов порта. Чтобы сделать данную функцию работоспособной, необходимо включить ее как глобально, так и для порта. Выключение управления ограничением количества хостов порта
port-security maximum <0-1023>	Установка максимального числа MAC-адресов, которые могут оставаться безопасными на этом порту. Это число не может превышать 1024.
port-security violation {protect | restrict | shutdown }	Выбор режима при превышении предела MAC-адресов на порту Protect – ничего не предпринимать

	Restrict - Если предел достигнут, последующие MAC-адреса порта будут подсчитаны и отмечены как нарушающие. Такие адреса MAC удаляются из таблицы MAC-адресов по истечении времени удержания. В лучшем случае нарушения предельных значений MAC - адрес может быть помечен как нарушение в любой момент времени. Shutdown- Если предел достигнут, то это приведет к отключению порта. Это означает, что все защищенные MAC-адреса будут удалены из порта и новые адреса не будут изучены.
port-security maximum-violation <1-1023>	Настройка максимального количества MAC-адресов, которые могут быть помечены как нарушающие этот порт. Это число не может превышать 1023. По умолчанию - 4. Он используется только тогда , когда установлен режим restrict
port-security mac-address sticky	Включение прикрепления MAC-адресов к порту. Когда порт находится в режиме sticky, все MAC-адреса, которые в противном случае были бы изучены как динамические, узнаются как закрепленные. Прикрепленные MAC-адреса являются частью рабочей конфигурации и поэтому могут быть сохранены в startup-config. Прикрепленные MAC-адреса сохраняются при изменении ссылок (в отличие от динамических, которые придется запоминать заново). Они также выдерживают перезагрузку, если рабочая конфигурация сохранена в startup-config.
port-security mac-address <mac_ucast> vlan <vlan_id> sticky	добавление статического или закрепленного MAC-адреса, управляемого Port Security. Для добавления статического MAC-адреса ввод sticky опускается.

2.2.9 NAS (Network Access Server)

Конфигурирование сервера доступа в сеть (Network Access Server) полезно в сетевой среде, в которой желательно аутентифицировать клиентов (supplicants) до того, как они получат доступ к ресурсам защищенной сети. Для эффективного управления доступом для неизвестных клиентов, IEEE разработал стандарт 802.1X, обеспечивающий процедуру аутентификации на порту, предотвращающую несанкционированный доступ к сети по запросам пользователей, впервые предоставляющих учетные данные для целей

аутентификации. Коммутатор, соединяющий клиентов и radius-сервер, обычно работает как аутентификатор. Для обмена сообщениями аутентификации между клиентами и удаленным RADIUS-сервером, проверяющим аутентичность пользователя и его права доступа, используется EAPOL (расширенный протокол аутентификации по локальным сетям). На данной странице можно настроить конфигурацию аутентификатора либо глобально, либо для каждого порта отдельно.

Команда	Описание
Глобальные настройки	

`dot1x system-auth-control`
 	
`no dot1x system-auth-control`
	Включение на коммутаторе глобально 802.1X и аутентификацию на основе MAC-адресов.
	
	Выключение на коммутаторе глобально 802.1X и аутентификацию на основе MAC-адресов. Если глобально эти протоколы выключены, передача кадров будет разрешена на всех портах.

`dot1x re-authentication`
 	
`no dot1x re-authentication`
	Включить повторную аутентификацию по истечении интервала времени, заданного в поле "Reauthentication Period" (Интервал повторной аутентификации). Повторную аутентификацию можно использовать для определения того, подключено ли к порту коммутатора новое устройство.

`dot1x authentication timer re-authenticate <1-3600>`	Установка интервала времени, по истечении которого подключенное устройство может быть аутентифицировано повторно. По умолчанию установлен интервал повторной аутентификации 3600 секунд. Допустимый диапазон значений от 1 до 3600 секунд.
`dot1x timeout tx-period <1-65535>`	Установка интервала времени, в течение которого коммутатор будет ожидать ответ от подавшего запрос на доступ к сети устройства в течение сессии аутентификации перед тем, как передать пакет Request Identify (Запрос идентификации) EAPOL. По умолчанию задано 30 секунд. Допустимый диапазон значений от 1 до 65535 секунд.
`dot1x authentication timer inactivity <10-1000000>`	Установка интервала времени, определяющего допустимое время доступа клиента к коммутатору для аутентификации по 802.1X и MAC- адресу.

	По умолчанию составляет 300 секунд. Допустимый диапазон значений от 10 до 1 000 000 секунд.
dot1x timeout quiet-period <10-1000000>	Установка времени, по истечении которого индицируется отказ EAP, либо превышение интервала ожидания RADIUS, из-за чего клиент не получил доступ. Эта настройка применяется к портам, работающим при аутентификации Single 802.1X, Multi 802.1X или на основе MAC - адресов. По умолчанию время удерживания составляет 10 секунд. Допустимый диапазон значений от 10 до 1 000 000 секунд.
dot1x feature radius-qos	Включение QoS, назначенного RADIUS.
dot1x feature radius-vlan	Включение VLAN, назначенного RADIUS.
dot1x feature guest-vlan	Включение гостевого VLAN является специальной VLAN, типичным назначением которой является предоставление ограниченного доступа к сети. Когда функция включена, дубликаты настроек индивидуального порта определяют, может ли порт быть перемещен в гостевую VLAN. Когда функция выключена, возможность перемещения порта в гостевую VLAN отключена на всех портах.
dot1x guest-vlan <1-4095>	Установка номера гостевого vlan, работает только в том случае, когда гостевая VLAN включена. VLAN ID представляет собой значение, присваиваемое порту, если порт перемещается в гостевую VLAN. Диапазон значений: от 1 до 4095.
dot1x max-reauth-req <1-255>	Установка максимального числа повторных аутентификаций. Максимальное число передач коммутатором кадра запроса идентификации EAPOL, остающихся без ответа перед тем, как порт будет добавлен в гостевую VLAN. Значение может быть изменено только в том случае, если гостевая VLAN включена глобально. Диапазон 1~255.
dot1x guest-vlan supplicant	Разрешение гостевого VLAN, если виден EAPOL. Коммутатор помнит, был ли принят кадр EAPOL в течение времени жизни порта. Когда коммутатор принимает решение о входе в гостевую VLAN, он сначала проверяет, включена или выключена эта опция. Если она выключена (флаг в поле снят – значение по

	умолчанию), коммутатор войдет в гостевую VLAN только в том случае, если кадр EAPOL не был принят на порту в течение времени жизни порта. Если опция включена (флаг в поле установлен), коммутатор войдет в гостевую VLAN, даже если кадр EAPOL был принят на порту в течение времени жизни порта. Значение может быть изменено только в том случае, если гостевая VLAN включена глобально.
Настройка портов	
`interface GigabitEthernet <port_type_list>`	Выбор портов для настройки параметров
`dot1x port-control {auto | force-authorized | force-unauthorized | mac-based | multi | single}`	Выбирает режим аутентификации порта. Данная настройка работает только в том случае, когда глобально включен NAS. Режимы работы: `Auto` – В этом режиме работы требуется, чтобы сервером аутентификации был авторизован dot1x-совместимый клиент. Клиентам, не обладающим dot1x-совместимостью, доступ будет запрещен. `force-authorized` – В этом режиме работы коммутатор отправит один кадр успешной (аутентификации) EAPOL, если осуществляется подключение к порту, при этом любому клиенту на порту будет разрешен доступ к сети без аутентификации `force-unauthorized` – В этом режиме работы коммутатор отправит один кадр отказа (аутентификации) EAPOL, если будет осуществляется подключение к порту, при этом любому клиенту на порту будет запрещен доступ к сети. `mac-based` – авторизация на основе MAC – адресов. Не принимаются и не передаются кадры EAPOL. При аутентификации на основе MAC - адресов, для половины клиентов коммутатор работает, как клиентское устройство, пославшее запрос на доступ к ресурсам сети. Начальный кадр (любого типа), отправленный клиентом, анализируется коммутатором, который, в свою очередь, использует MAC - адрес клиента в качестве имени пользователя и пароля в последующем обмене данными с RADIUS-сервером по EAP. 6-байтный MAC - адрес

	преобразуется в строку вида "xx-xx-xx-xx-xx-xx", где тире (-) используется в качестве символа-разделителя между шестнадцатиричными цифрами (записанными символами нижнего регистра). `Multi` – В режиме работы Multi 802.1X, одно или более клиентских устройств могут быть аутентифицированы на одном и том же порту в одно и то же время. Каждое клиентское устройство аутентифицируется индивидуально; его безопасность в таблице MAC - адресов обеспечивает модуль “Port Security” (Безопасность порта). `Single` – В режиме работы Single 802.1X, аутенцифицироваться на порту будет преимущественно одно клиентское устройство, отправившее запрос на доступ к ресурсам сети. Для связи между клиентским устройством и коммутатором используются нормальные кадры EAPOL. Если к порту подключено более одного клиентского устройства, первым из них будет считаться то, которое появилось раньше всех остальных в тот период, когда порт был включен. Если такое клиентское устройство не отправило правильной учетной информации в течение заданного времени, шанс получит другое клиентское устройство. Как только клиентское устройство будет успешно аутентифицировано, только ему будет разрешен доступ. Этот режим работы является наиболее безопасным из всех поддерживаемых режимов. В этом режиме для обеспечения безопасности MAC - адреса клиентского устройства используется модуль “Port Security” (Безопасность порта) (после того, как устройство будет успешно аутентифицировано).
`dot1x radius-qos`	включение RADIUS-Assigned QoS на порту
`dot1x radius-vlan`	включение RADIUS-Assigned VLAN на порту
`dot1x guest-vlan`	включение гостевого VLAN на порту
`dot1x re-authenticate`	Рестарт процесса аутентификации

2.2.10 ACL. Списки доступа

ACL является последовательным списком, используемым для разрешения или запрета доступа пользователей к информации или к выполнению задач по сети. В данном коммутаторе пользователи могут задать правила, применяемые к номерам портов для разрешения или запрета операций, или ограничения предельной скорости.

Команда	Описание
Глобальные настройки	
`access-list rate-limiter <1-16> { 100kbps | 100pps | pps}`	Настройка ограничения скорости: <1-16> - идентификатор правила {100kbps | 100pps | pps} – выбор единиц измерения, после ввода единиц измерения требуется ввести пороговое значение, при превышении которого пакеты будут отбрасываться.

`access-list ace <1-128>`
 	
`no access-list ace <1-128>`
	Создание правила фильтрации для политики доступа – для определенного порта или для всех портов
	
	Удаление правила

`access-list ace <1-128> ingress {any | interface}`	Выбор входящего порта.
`access-list ace <1-128> policy <0-63>`	Выбор фильтра политики, чтобы отфильтровать конкретную политику по данному ACE. По умолчанию установлен фильтр не присвоен.
`access-list ace <1-128> frame-type {any | arp | etype | ipv4 | ipv4-icmp | ipv4-tcp | ipv4-udp | ipv6 | ipv6-icmp | ipv6-tcp | ipv6-udp}`	Выбор типа кадра. По умолчанию можно использовать любой тип кадра.
`access-list ace <1-128> action {deny | filter | permit}`	Выбор операции с кадром, который попадает в этот ACE `Deny` - кадр, попавший в этот ACE, отбрасывается. `Permit` – кадру, который попадает в этот ACE, предоставляется разрешение на операцию ACE. `Filter` - кадры, соответствующие ACE, фильтруются.

`access-list ace <1-128> rate-limiter <1-16>`
 	
`access-list ace <1-128> rate-limiter disable`
	Включение ограничения скорости.
	
	Выключение ограничения скорости.

access-list ace <1-128> mirror access-list ace <1-128> mirror disable	Включение функции зеркала Выключение функции зеркала
access-list ace <1-128> logging access-list ace <1-128> logging disable	Включение регистрации в системном журнале. Выключение регистрации в системном журнале.
access-list ace <1-128> shutdown access-list ace <1-128> shutdown disable	Включить функцию отключения порта Выключить функцию отключения порта
access-list ace <1-128> tag {any | tagged | untagged}	Выбор кадров в соответствии с тегами 802.1Q. Any - допускается любое значение Tagged- Только кадр с тегами. Untagged - Только кадры без тегов. Значение по умолчанию - Any
access-list ace 1 vid {<1-4095> | any}	Выбор vlan id для данного ACE Any - фильтр не задан
access-list ace 1 tag-priority { 0-1 | 0-3 | 2-3 | 4-5 | 4-7 | 6-7 | <0-7> | any}	Выбор значения User Priority (Приоритет пользователя), найденного в теге VLAN
Настройка портов	
interface GigabitEthernet <port_type_list>	Выбор портов для настройки параметров
access-list policy <0-63>	Установка идентификатора правил списка доступа определенному порту. Порт может использовать только один идентификатор правил списка доступа, однако, идентификатор правил списка доступа может быть применен ко многим портам. По умолчанию идентификатор имеет значение 0.
access-list action {deny | permit}	Разрешает или запрещает кадр на основе того, согласуется ли он с правилом из присвоенной группы правил.
access-list rate-limiter <1-16>	Установка идентификатора ограничителя скорости, применяемого к порту. Правило ограничения скорости может быть задано в режиме глобальной конфигурации, командой access-list rate-limiter <1-16> {100kbps | 100pps | pps}
access-list redirect interface GigabitEthernet <port_type_list>	Выбор порта, на который перенаправляются согласующиеся кадры.

access-list mirror No access-list mirror	Включение функции зеркалирования. Когда функция зеркалирования включена, копии согласованных кадров будут зеркалироваться в порт назначения. Этим параметром задается зеркалирование порта на основе ACL, а порт зеркалирования задается на общей странице настройки зеркала, реализованной независимо. Выключение функции зеркалирования
access-list logging no access-list logging	Включение регистрации согласующихся кадров в системном журнале. Выключение регистрации
access-list shutdown no access-list shutdown	Выключение порта, когда согласующиеся кадры появляются на порту. Отмена команды
access-list port-state no access-list port-state	Изменение состояния порта. Повторное включение порта, который был выключен правилом acl Изменение состояния порта. Выключение

2.2.11 IP Source Guard. Защита IP-адреса источника

Функция IP Source Guard в Ethernet-коммутаторах предназначена для обеспечения дополнительной защиты от несанкционированных действий пользователей.

2.2.11.1 IP Source Guard

Команда	Описание
Глобальные настройки	
ip verify source no ip verify source	Включение защиты IP-адреса источника Выключение защиты IP-адреса источника
ip verify source translate no ip verify source translate	преобразование динамических записей в статические. Отмена команды
ip source binding interface GigabitEthernet <port_type_id> <vlan_id> <ipv4_ucast>	Настройка статических правил. Установка соответствий между IP-адресом, номером порта, MAC-адресом и VLAN ID.

<mac_ucast>	
Настройка портов	
interface GigabitEthernet <port_type_list>	Выбор портов для настройки параметров
ip verify source no ip verify source	Включение защиты IP-адреса источника на порту. Для того, чтобы защита IP-адресов источника работала, функция должна быть включена в глобальном режиме и на порту. Выключение защиты IP-адреса источника на порту.
ip verify source limit <0-2>	Выбор максимального числа динамических клиентов на порту. Возможны следующие варианты: 0, 1, 2 Если включен режим работы порта и максимальное число клиентов равно 0, коммутатор будет только передавать IP-пакеты, которые согласуются со статическими элементами списка (IP-адресами) для данного порта. По умолчанию значение unlimited (неограниченное количество)

2.2.11.2 IPv6 Source Guard

Команда	Описание
Глобальные настройки	
ipv6 verify source no ipv6 verify source	Включение защиты IP-адреса источника Выключение защиты IP-адреса источника
ipv6 verify source translate no ipv6 verify source translate	преобразование динамических записей в статические. Отмена команды
ipv6 source binding interface GigabitEthernet <port_type_id> { <ipv6_ucast> | vlan}	Настройка статических правил. Установка соответствий между IP-адресом, номером порта, MAC-адресом и VLAN ID.
Настройка портов	
interface GigabitEthernet <port_type_list>	Выбор портов для настройки параметров
ipv6 verify source No ipv6 verify source	Включение защиты IP-адреса источника на порту. Для того, чтобы защита IP-адресов источника работала, функция должна быть включена в глобальном режиме и на порту. Выключение защиты IP-адреса источника на порту.
ipv6 verify source limit <0-2>	Выбор максимального числа динамических клиентов на порту.

	Возможны следующие варианты: 0, 1, 2 Если включен режим работы порта и максимальное число клиентов равно 0, коммутатор будет только передавать IP-пакеты, которые согласуются со статическими элементами списка (IP-адресами) для данного порта. По умолчанию значение unlimited (неограниченное количество)

2.2.12 ARP inspection. Инспекция ARP

Инспекция ARP-пакетов используется для отфильтровывания несанкционированных пакетов ARP. Это позволяет предотвратить многие виды атак класса «man-in-the-middle» (атака «человек посередине»). При обнаружении коммутатором несанкционированного ARP-пакета им автоматически создается фильтр MAC-адресов, блокирующий трафик от MAC-адреса и сети VLAN, от которых поступил несанкционированный ARP-пакет. Период активности фильтра MAC-адресов на коммутаторе можно настраивать.

Команда	Описание
Глобальные настройки	

`ip arp inspection`
 	
`no ip arp inspection`
	Включение функции инспекции ARP-пакетов
	
	Выключение функции инспекции ARP-пакетов

`ip arp inspection vlan <vlan_list> logging {all | deny | permit}`	Выбор VLAN на которых будет включена функция инспекции ARP-пакетов. А также настройка типа записей передаваемых в журнал.
`ip arp inspection entry interface GigabitEthernet <port_type_id> <vlan_id> <mac_ucast> <ipv4_ucast>`	Настройка статической записи `<port_type_id>` - номер порта `<vlan_id>` - номер vlan `<vlan_id>` - mac-адрес `<ipv4_ucast>` - ip-адрес
Настройка портов	
`interface GigabitEthernet <port_type_list>`	Выбор портов для настройки параметров

`no ip arp inspection trust`
 	
`ip arp inspection trust`
	Включение функции инспекции ARP-пакетов на порту.
	
	Выключение функции инспекции ARP-пакетов на порту.

`ip arp inspection check-vlan`
 	
`no ip arp inspection check-vlan`
	Включение проверки VLAN.
	
	Выключение проверки VLAN.

ip arp inspection logging {all | deny | permit}	deny - В журнал помещаются запрещенные записи. permit - В журнал помещаются разрешенные записи. All – В журнал помещаются все записи
no ip arp inspection logging	В журнал ничего не записывается.

2.2.13 Настройка Radius.

Команда	Описание
Глобальные настройки	
radius-server timeout <1-1000>	Настройка времени ожидания ответа от сервера аутентификации перед тем, как повторить запрос.
radius-server retransmit <1-1000>	Настройка числа повторной передачи запросов на сервер аутентификации.
radius-server deadtime <1-1440>	Настройка времени отсутствия сервера (время в течении которого коммутатор не будет посылать новые запросы на сервер, который не ответил на предыдущий запрос)
radius-server key (unencrypted | encrypted) <line1-63>	Ввод ключа длиной не более 64 символов.
radius-server attribute 4 <ipv4_ucast>	Настройка ipv4-адреса, в качестве атрибута 4 в пакетах запроса достуа RADIUS. По умолчанию используется ip-адрес исходящего интерфейса.
radius-server attribute 95 <ipv6_ucast>	Настройка ipv6-адреса, в качестве атрибута 4 в пакетах запроса достуа RADIUS. По умолчанию используется ip-адрес исходящего интерфейса.
radius-server attribute 32 <line1-253>	Идентификатор длиной не более 256 символов, используемый в качестве атрибута 32 в пакетах запроса доступа RADIUS.
Настройка сервера	
radius-server host <word1-255>	Настройка имени хоста RADIUS сервера или его ip-адрес
radius-server host <имя или ip-адрес> auth-port <0-65535>	Настройка порта UDP, используемого для аутентификации на RADIUS-сервере.
radius-server host <имя или ip-адрес> acct-port <0-65535>	Настройка порта UDP, используемого для аккаутинга.
radius-server host <имя или ip-адрес> timeout <1-1000>	Настройка время ожидания, оно будет использовано вместо глобального времени ожидания. Если желательно использовать

	глобальное значение, команду вводить не нужно.
radius-server host <имя или ip-адрес> retransmit <1-1000>	Настройка времени повторной передачи, оно будет использовано вместо глобального значения времени повторной передачи. Если желательно использовать глобальное значение, команду вводить не нужно.
radius-server host <имя или ip-адрес> key (unencrypted | encrypted) <line1-63>	Настройка ключа, оно будет использовано вместо глобального значения секретного ключа. Если желательно использовать глобальное значение, команду вводить не нужно.

Примечание: передать все параметры сервера можно одной строкой, указывая значения параметров последовательно. Сервер, указанный раньше в конфигурации считается основным.

2.2.14 Настройка TACACS+

Команда	Описание
Глобальные настройки	
tacacs-server timeout <1-1000>	Настройка времени ожидания ответа от сервера аутентификации перед тем, как повторить запрос.
tacacs-server deadtime <1-1440>	Настройка времени отсутствия сервера (время в течении которого коммутатор не будет посылать новые запросы на сервер, который не ответил на предыдущий запрос)
tacacs-server key (unencrypted | encrypted) <line1-63>	Ввод ключа длиной не более 64 символов.
Настройка сервера	
tacacs-server host <word1-255>	Настройка имени хоста TACACS+ сервера или его ip-адрес
tacacs-server host <имя или ip-адрес> port <0-65535>	Настройка порта TCP, используемого для аутентификации на сервере TACACS+.
tacacs -server host <имя или ip-адрес> timeout <1-1000>	Настройка время ожидания, оно будет использовано вместо глобального времени ожидания. Если желательно использовать глобальное значение, команду вводить не нужно.
tacacs-server host <имя или ip-адрес> key (unencrypted | encrypted) <line1-63>	Настройка ключа, оно будет использовано вместо глобального значения секретного ключа. Если желательно использовать глобальное значение, команду вводить не нужно.

Примечание: передать все параметры сервера можно одной строкой, указывая значения параметров последовательно. Сервер, указанный раньше в конфигурации считается основным.

2.2.15 static aggregation (Статическое агрегирование)

Команда	Описание

`aggregation mode (smac | dmac | ip | port)`
 	
`no aggregation mode (smac | dmac | ip | port)`
	Настройка режима работы для расчета линейного порта, через который будет передаваться кадр.
	`smac` – используется MAC-адрес источника
	`dmac` – используется MAC-адрес назначения
	`ip` – используется ip-адрес
	`port` – используются порты TCP/UDP назначения и источника.
	Возможно включение нескольких режимов работы.
	
	Отключение соответствующего режима работы.

Настройка группы агрегирования	
`interface GigabitEthernet <port_type_list>`	Выбор порты для объединения в группу
`aggregation group <1-5> mode {active | on | passive}`	Выбор id группы и включение режима статической агрегации `On` – статическая агрегация `Active` – режим активной агрегации LACP `Passive`– режим пассивной агрегации LACP

2.2.16 LACP

Команда	Описание
Глобальные настройки	
`lacp system-priority <1-65535>`	Настройка значения `system-priority`. По умолчанию - 32768
Настройки портов	
`interface GigabitEthernet <port_type_list>`	Выбор портов для настройки параметров

lacp port-priority <1-65535>	Чем меньше это целое число, тем больше приоритет. Это значение приоритета определяет, какой порт будет активен, а какой – будет играть роль резервного.
lacp timeout (fast | slow)	Параметр Timeout (Время ожидания) определяет период времени между передачами BPDU. Когда параметр имеет значение Fast (Быстро), пакеты LACP будут передаваться каждую секунду; когда параметр имеет значение Slow (Медленно), перед отправкой пакета LACP будет выдержан интервал 30 секунд.

2.2.17 Loop protection

Вследствие неправильного выполнения соединений, проблем с аппаратурой, неправильной настройки протоколов, в сетях иногда возникают петли. В коммутируемых сетях петли потребляют ресурсы коммутатора, в результате чего падает его производительность. Функция Loop Protection (Защита от петель), реализованная в данном коммутаторе, может быть включена глобально либо индивидуально на каждом порту. Использование функции защиты от петель дает возможность коммутатору автоматически обнаруживать петли в сети. При обнаружении петель, порты, принявшие от коммутатора пакет защиты от петель, 74 могут быть отключены либо соответствующие события могут быть зарегистрированы в журнале.

Команда	Описание
Глобальные настройки	
loop-protect no loop-protect	Включение функции защиты от петель Выключение функции защиты от петель
loop-protect shutdown-time <0-604800>	Период времени, на который порт будет выключен. Допустимые значения: от 0 до 604800 секунд. 0 означает, что порт будет оставаться выключенным до тех пор, пока устройство не будет перезагружено.
loop-protect transmit-time <1-10>	Интервал между отправкой пакетов защиты от петель PDU на каждом порту. Допустимые значения: от 1 до 10 секунд.
Настройки портов	
interface GigabitEthernet <port_type_list>	Выбор портов для настройки параметров
loop-protect no loop-protect	Включение функции защиты от петель на выбранных портах Выключение функции защиты от петель на выбранных портах
loop-protect action (log | log shutdown | shutdown)	Настройка операции при обнаружении петли на порту: Log – События регистрируются в журнале, но порт остается включенным. Log shutdown – Порт, на котором обнаружена петля, отключается на период времени, заданный в глобальных настройках и события регистрируются в журнале.

	Shutdown – Порт, на котором обнаружена петля, отключается на период времени, заданный в глобальных настройках.
loop-protect tx-mode no loop-protect tx-mode	Включение генерации пакетов защиты от петель PDU либо осуществляется пассивный поиск PDU, переданных по петле. Выключение генерации пакетов защиты от петель PDU либо осуществляется пассивный поиск PDU, переданных по петле.

2.2.18 IPMC Profile

PMC профили используются для обеспечения контроля доступа к IP мультикаст потокам. Существует возможность создать 64 профиля с 128 правилами в каждом.

Команда	Описание
Глобальные настройки	
ipmc profile no ipmc profile	Включение функции ipmc profile Выключение функции ipmc profile
ipmc profile <word16> no ipmc profile <word16>	Назначение имени профиля, при вводе команды осуществляется переход в режим конфигурации профиля. Удаление соответствующего профиля.
Ipmc range <word16> (<ipv4_mcast> | <ipv6_mcast>)	Создание и назначение имени диапазону ip-адресов а также указание диапазона ipv4 или ipv6 мультикастовых адресов для многоадресной рассылки.
Настройка профиля IPMC	
Description <line64>	Настройка описания профиля
range <word16> (deny | permit)	Команда разрешает или запрещает правило для профиля.

2.2.19 MVR

Протокол MVR - регистрация многоадресных VLAN (Multicast VLAN Registration) позволяет медиасерверу передавать многоадресный поток по одной многоадресной VLAN, при этом клиенты, принимающие поток многоадресной VLAN, могут оставаться в различных сетях VLAN. Клиенты различных VLAN, намеревающиеся вступить в многоадресную группу или выйти из нее, отправляют в порт приемника сообщение IGMP

Join (Вступить в группу) либо IGMP Leave (Покинуть группу). Порт приемника, принадлежащий одной из многоадресных групп, может принимать многоадресный поток от медиасервера. Далее, MVR изолирует пользователей, не намеревающихся принимать многоадресный трафик и, следовательно, обеспечивать безопасность данных за счет сегрегации VLAN, допускающей только многоадресный трафик в другие сети VLAN, к одной из которых принадлежит абонент. Несмотря на то, что общий многоадресный трафик проходит от MVR VLAN в VLAN различных групп, пользователи различных VLAN IEEE 802.1Q или частных VLAN не могут обмениваться какой-либо информацией (за исключением услуг маршрутизации верхнего уровня).

Команда	Описание
Глобальные настройки	
`mvr` `no mvr`	Включение функции mvr Выключение функции mvr
`mvr vlan <vlan_list>`	Указание идентификатора многоадресной VLAN
`mvr name <word16>`	назначение имени многоадресной VLAN
`mvr vlan <vlan_list> igmp-address`	Назначение IPv4-адреса в качестве адреса источника, используемого в заголовке IP кадров управления IGMP
`mvr vlan <vlan_list> mode (compatible | dynamic)`	Выбор режима работы MVR Dynamic (Динамический): MVR разрешает динамически отправлять сообщения о членстве на порты источника. Этот режим работы задан по умолчанию. Compatible (Совместимый): Отправка на порты источника сообщений MVR о членстве запрещена.
`mvr vlan <vlan_list> frame priority <0-7>`	Настройка приоритета передачи кадров управления IGMP/MLD. По умолчанию, приоритет равен 0. Допустимые значения приоритета: 0 -7
`mvr vlan <vlan_list> frame tagged`	Настройка тегирования кадров управления IGMP/MLD.
`mvr vlan <vlan_list> channel <word16>`	Выбор профиля IPMC (настройка профиля описана в п. 1.2.14)
`mvr vlan <vlan_list> last-member-query-interval <0-31744>`	Настройки максимального времени ожидания сообщения о членстве IGMP/MLD на порту приемника до удаления порта из многоадресной группы. По умолчанию LLQI равно 0,5 секунды. Диапазон допустимых значений: 0-31744 десятых долей секунды
Настройка порта	
`interface GigabitEthernet <port_type_list>`	Выбор портов для настройки параметров
`mvr immediate-leave`	Включение функции немедленного выхода из группы
`mvr vlan 131 type(receiver | source)`	Назначение роли порта `Source-` Порт (входящего трафика) является портом источника. Порты источников будут принимать и посылать многоадресные данные. Абоненты не могут быть напрямую подключены к портам источника. `Receiver -` Порт установлен как порт приемника. Клиентские или абонентские порты сконфигурированы,

	как порты приемников, так что они могут использовать сообщения IGMP/MLD для приема многоадресных данных

2.2.20 IPMC

2.2.20.1 IGMP Snooping

Протокол управления группами интернета IGMP (Internet Group Management Protocol) обеспечивает управление участием в многоадресных IP-группах. IGMP используется IP-хостами и соседними многоадресными маршрутизаторами для установления принадлежности к многоадресной группе. Он может использоваться наиболее эффективно при поддержке таких услуг, как потоковое онлайн-видео и игры. IGMP Snooping – это процесс слушания трафика IGMP. Как следует из названия, IGMP snooping представляет собой функцию, позволяющую коммутатору «прослушивать» обмен данными между хостами и маршрутизаторами, обрабатывая пакеты 3-го уровня (пакеты IGMP, посылаемые по многоадресной сети). Когда на коммутаторе включен IGMP snooping, он анализирует все пакеты, передаваемые между хостами, подключенными к коммутатору и многоадресными маршрутизаторами в сети. Когда коммутатор принимает отчет IGMP для данной многоадресной группы от хоста, коммутатор добавляет номер порта хоста к многоадресному списку для этой группы. Когда коммутатор обнаруживает сообщение IGMP Leave (Покинуть группу IGMP), он удаляет порт хоста из ячейки таблицы. IGMP snooping позволяет эффективно снижать многоадресный трафик при стриминге и других экстенсивно расходующих полосу пропускания IP приложениях. Коммутатор, использующий IGMP snooping, в этом трафике будет передавать хостам только многоадресный трафик. Снижение многоадресного трафика уменьшает число пакетов, обрабатываемых коммутатором (однако при этом требуется увеличение оперативной памяти для обработки многоадресных таблиц) и снижает нагрузку на оконечные хосты, так как их сетевые карты (или операционные системы) не будут принимать и фильтровать весь многоадресный трафик, генерируемый сетью.

Команда	Описание
Глобальные настройки	
`ip igmp snooping` `no ip igmp snooping`	Включение функции `igmp snooping` Выключение функции `igmp snooping`

`ip igmp unknown-flooding`
 	
`no ip igmp unknown-flooding`
	включение режима передачи незарегистрированного (не принадлежащего группам) многоадресного IP-трафика.
	
	выключение режима передачи незарегистрированного (не принадлежащего группам) многоадресного IP-трафика.

`ip igmp ssm-range <ipv4_mcast>`	Назначение диапазона многоадресных адресов для конкретного источника SSM (Source-Specific Multicast), позволяет поддерживающим SSM хостам и маршрутизаторам выполнять модель услуг SSM для групп в заданном диапазоне адресов.
`ip igmp host-proxy leave-proxy`	Подавляет сообщения о выходе из группы, отличающиеся от принятых, от последнего порта

	участника группы. Прокси-сервер сообщений о выходе из группы подавляет все не являющиеся необходимыми сообщения IGMP о выходе из группы таким образом, что коммутатор, не являющийся querier, передает пакет выхода из группы только тогда, когда последний динамический порт-участник покидает многоадресную группу

`ip igmp host-proxy`
 	
`no ip igmp host-proxy`
	Включение прокси-сервера
	
	Выключение прокси-сервера

Настройка порта	
`interface GigabitEthernet <port_type_list>`	Выбор портов для настройки параметров
`ip igmp snooping mrouter`	Назначение порта портом маршрутизатора
`ip igmp snooping immediate-leave`	Включение функции быстрого выхода из группы. Когда принят пакет выхода из группы, коммутатор немедленно удаляет порт из многоадресной услуги, не посылая специфичный для группы запрос IGMP GS на этот интерфейс.
`ip igmp snooping max-groups`	Назначение максимального числа многоадресных групп, в которые порт может вступить одновременно. Когда для порта будет достигнуто максимальное число групп, новые сообщения с отчетами IGMP о вступлении в группу будут отбрасываться. По умолчанию выбрано неограниченное число групп (unlimited). Допустимый диапазон значений от 1 до 10.
`ip igmp snooping filter <word16>`	Настройка фильтра на порту для многоадресных групп. Когда определенная многоадресная группа выбрана на порту, сообщения IGMP join reports (отчеты о вступлении в группу) на порту отбрасываются.

2.2.20.2 MLD Snooping

MLD - Multicast Listener Discovery Protocol - протокол определения получателей многоадресных потоков, использующийся в IPv6. Аналогичную роль в IPv4 выполняет протокол IGMP.

Команда	Описание
Глобальные настройки	
`ipv6 mld snooping` `no ipv6 mld snooping`	Включение функции `mld snooping`, включено по умолчанию Выключение функции `mld snooping`

`ipv6 mld unknown-flooding`
 	
`no ipv6 mld unknown-flooding`
	Включение функции рассылки незарегистрированного трафика
	
	Отключение функции рассылки незарегистрированного трафика. Управление лавинной рассылкой вступает в силу только тогда, когда включена функция `mld`

	snooping. Когда MLD Snooping отключен, незарегистрированный трафик IPMCv6 всегда активен, несмотря на этот параметр.
ipv6 mld ssm-range <ipv6_mcast>	Настройка диапазона SSM (многоадресная рассылка с учетом источника) позволяет узлам и маршрутизаторам, поддерживающим SSM, запускать модель службы SSM для групп в диапазоне адресов.
ipv6 mld host-proxy no ipv6 mld host-proxy	Включение прокси-сервера. Эту функцию можно использовать, чтобы избежать пересылки ненужных сообщений о присоединении и оставить сообщения на стороне маршрутизатора. Отключение прокси-сервера
ipv6 mld host-proxy leave-proxy no ipv6 mld host-proxy leave-proxy	Включение MLD Leave Proxy. Эту функцию можно использовать, чтобы избежать пересылки ненужных сообщений о выходе на сторону маршрутизатора. Выключение MLD Leave Proxy.
ipv6 mld snooping vlan <vlan_list>	
MLD Snooping VLAN Configuration	
interface vlan <vlan_list>	Создание интерфейса
ipv6 mld snooping no ipv6 mld snooping	Включение функции mld snooping для VLAN Выключение функции mld snooping для VLAN
ipv6 mld snooping querier election no ipv6 mld snooping querier election	Включение выбора MLD Querier в VLAN Выключение выбора MLD Querier в VLAN
ipv6 mld snooping compatibility {auto | v1 | v2}	Настройка совместимости. Значение совместимости по умолчанию - MLD-Auto.
ipv6 mld snooping priority <0-7>	Приоритет интерфейса. Он указывает уровень приоритета управляющего кадра MLD, сгенерированный системой. Эти значения можно использовать для определения приоритетов различных классов трафика. Значение приоритета интерфейса по умолчанию - 0.
ipv6 mld snooping robustness-variable <1-255>	Настройка переменной устойчивости. Переменная устойчивости позволяет настроить ожидаемую потерю пакетов в канале.

	Допустимый диапазон 1 к 255, значение переменной устойчивости по умолчанию - 2.
ipv6 mld snooping query-interval <1-31744>	Настройка интервала запроса. Интервал запроса - это интервал между общими запросами, отправляемыми запросчиком. Допустимый диапазон <1-31744> секунд, интервал запроса по умолчанию составляет 125 секунд.
ipv6 mld snooping query-max-response-time <0-31744>	Настройка интервала ответа на запрос. Максимальная задержка ответа, используемая для расчета максимального кода ответа, вставляемого в периодические общие запросы. Допустимый диапазон <0-31744> Интервал ответа на запрос по умолчанию составляет 100 в десятых долях секунды (10 секунд).
ipv6 mld snooping last-member-query-interval <0-31744>	Настройка максимальной задержки ответа, Допустимый диапазон <0-31744> в десятых долях секунды, интервал по умолчанию составляет 10 в десятых долей секунды (1 секунда).
ipv6 mld snooping unsolicited-report-interval <0-31744>	Настройка интервала незапрашиваемого отчета - это время между повторениями первоначального отчета узла, представляющего интерес, в многоадресном адресе. Допустимый диапазон <0-31744> в десятых долях секунды, интервал по умолчанию - 1 секунда
Настройка портов	
interface GigabitEthernet <port_type_list>	Выбор портов для настройки параметров
ipv6 mld snooping mrouter no ipv6 mld snooping mrouter	Настройка порта в качестве порта маршрутизатора Отмена команды
ipv6 mld snooping immediate-leave No ipv6 mld snooping immediate-leave	Включение функции немедленного отключения. Система удалит запись группы и прекратит пересылку данных после получения сообщения о выходе из MLDv1, не отправляя сообщения запроса последнего участника. Выключение функции немедленного отключения.
ipv6 mld snooping max-groups <1-10>	Ограничение количества групп многоадресной рассылки, к которым

	может принадлежать порт коммутатора.
`ipv6 mld snooping filter <word16>`	Настройка контроля доступа при регистрации групп многоадресной рассылки <word16> - профиль IPMC в качестве условия фильтрации для конкретного порта

2.2.21 LLDP

Протокол LLDP (Link Layer Discovery Protocol) является протоколом канального уровня, на котором сетевые устройства обмениваются информацией о себе с другими устройствами, напрямую соединенными через сеть. Используя LLDP, два устройства, на которых функционируют сетевые протоколы разных уровней, могут обучаться информации друг друга. Для обнаружения соседних устройств используется набор атрибутов, ссылающийся на TLV. Устройство может передавать и принимать такую детальную информацию, как описание порта, описание системы и ее возможностей, адрес управления.

Команда	Описание
Глобальные настройки	
`lldp timer <5-32768>`	Настройка интервала между кадрами LLDP, отправляемыми соседям данного устройства для обновления информации о данном устройстве. Допустимые значения: от 5 до 32768 секунд. По умолчанию задано 30 секунд.
`lldp holdtime <2-10>`	Данная настройка определяет, как долго кадры LLDP будут считаться правильными и используется для вычисления TTL. Диапазон допустимых значений: 2~10 раз. По умолчанию задано 4.
`lldp transmission-delay <1-8192>`	Настройка задержки между кадрами LLDP, содержащими изменения конфигурации. Допустимые значения: от 1 до 8192 секунд.
`lldp reinit <1-10>`	Настройка задержки между кадром отключения и новой инициализацией LLDP. Допустимые значения: от 1 до 10 секунд
Настройка порта	
`interface GigabitEthernet <port_type_list>`	Выбор портов для настройки параметров
`lldp transmit`	Режим работы: только передача. Коммутатор будет посылать информацию

`no lldp transmit`	LLDP, но будет отбрасывать информацию LLDP, принятую от соседних устройств. Выключат режим

`lldp receive`
 	
`no lldp receive`
	Режим работы: только прием. Коммутатор будет анализировать информацию LLDP, принятую от соседних устройств.
	
	Выключат режим

`lldp cdp-aware`	Операция CDP aware (Распознавание CDP) используется для декодирования входящих кадров CDP (Cisco Discovery Protocol). Если эта опция включена, CDP TLVs, которые могут быть отображены в соответствующее поле таблицы соседних устройств LLDP будут декодированы, в противном случае эти кадры будут отброшены. CDP TLVs отображаются в поле таблицы соседних устройств LLDP

`lldp tlv-select (management-address vid| port-description | system-capabilities | system-description | system-name)`
 	
`no lldp tlv-select (management-address vid| port-description | system-capabilities | system-description | system-name)`
	Настройка атрибутов для обнаружения соседних устройств. Эти атрибуты содержат описания типа, длины и значений и ссылаются на TLVs. Данное устройство может передавать такую детальную информацию, как описание порта, имя и описание системы и ее возможностей, адрес управления.
	
	Отключение соответствующего атрибута. Соседние устройства не будут получать соответствующую информацию об устройстве.

2.2.21.1 LLDP MED

Протокол LLDP для конечных медиа-устройств LLDP-MED (LLDP for Media Endpoint Devices) является расширением LLDP и работает между конечными устройствами, такими как IP-телефоны и сетевыми устройствами (например, коммутаторами). Протокол LLDP-MED обеспечивает поддержку приложений передачи голоса по IP (VoIP) и дополнительные TLVs для обнаружения, обеспечения политики сети, функции Power over Ethernet, управления реестром и информации о местоположении.

Команда	Описание
Глобальные настройки	
`lldp med fast <1-10>`	Настройка параметра Fast start repeat count (Число повторов быстрого старта) позволяет задать, сколько раз будет

	повторен быстрый старт передачи. Рекомендуемое значение (4 раза) означает, что с интервалом 1 секунда будут переданы 4 кадра LLDP, если принят кадр LLDP с новой информацией. Следует отметить, что LLDP-MED и механизм LLDP-MED Fast Start 100 предназначены только для работы на линиях между устройствами соединения по сети, поддерживающими LLDP-MED и конечными устройствами и неприменимы к линиям между элементами инфраструктуры LAN, включая и устройства соединения по сети или линии другого типа.
`lldp holdtime <2-10>`	Данная настройка определяет, как долго кадры LLDP будут считаться правильными и используется для вычисления TTL. Диапазон допустимых значений: 2~10 раз. По умолчанию задано 4.
`lldp transmission-delay <1-8192>`	Настройка задержки между кадрами LLDP, содержащими изменения конфигурации. Допустимые значения: от 1 до 8192 секунд.
`lldp reinit <1-10>`	Настройка задержки между кадром отключения и новой инициализацией LLDP. Допустимые значения: от 1 до 10 секунд
Настройки местоположения	
`lldp med location-tlv latitude (north  south) <word8>`	Задание широты. Широта должна быть приведена в диапазоне 0-90 градусов и содержать не более 4 цифр. Можно задать экваториальное положение либо на север от экватора (North) либо на юг (South) от экватора.
`lldp med location-tlv longitude (east  west) <word9>`	Задание долготы. Долгота должна быть приведена в диапазоне 0-180 градусов и содержать не более 4 цифр. Можно указать направление – либо на восток от нулевого меридиана (East) либо на запад от нулевого меридиана (West).
`lldp med location-tlv (floors meters) <word11>`	Задание высоты. Высота должна быть приведена в диапазоне от - 32767 до 32767 и содержать не более 4 цифр. Можно выбрать единицы измерения высоты – либо в метрах, либо в этажах.
`lldp med datum (nad83-mllw nad83-navd88  wgs84)`	Выбор системы координат: • WGS84: (Географические, трехмерные) – Всемирная геодезическая система 1984, CRS Code 4327, нулевой меридиан: гринвичский.

	• NAD83/NAVD88: Североамериканская система координат 1983, CRS Code 4269,нулевой меридиан: гринвичский; связанная с этой система координат по вертикали - North American Vertical Datum of 1988 (NAVD88). Эта пара систем координат используется для указания местоположения на земле, на водных пространствах, подверженных приливам и отливам (для которых можно использовать систему координат NAD83/MLLW). • NAD83/MLLW: Североамериканская система координат 1983, CRS Code 4269, нулевой меридиан: гринвичский; связанная с этой система координат по вертикали - Mean Lower Low Water (MLLW). Эта пара связанных систем координат используется при указании местоположения в океане, на морях и на 101 других водных пространствах.опция включена, CDP TLVs, которые могут быть отображены в соответствующее поле таблицы соседних устройств LLDP будут декодированы, в противном случае эти кадры будут отброшены. CDP TLVs отображаются в поле таблицы соседних устройств LLDP
`lldp med location-tlv civic-addr (additional-code | additional-info | apartment | block | building | city | country | county | district | floor | house-no | house-no-suffix | landmark | leading-street-direction | name | p-o-box | place-type | postal-community-name | room-number | state | street | street-suffix | trailing-street-suffix | zip-code)`	Указание адреса `additional-code` - Добавочный код `additional-info` - Дополнительная информация о местоположении. `Apartment` - Апартамент, номер. `Block` - Квартал, блок. `Building` - Строение. `City` - Город, поселок. `Country` - Код страны по стандарту ISO 3166, состоящий из двух прописных букв ASCII. `County` - Округ. `District` - Район города, округ города, административный район города. `Floor` - Этаж `house-no` - Номер дома `house-no-suffix` - Суффикс номера дома. `Landmark` - Адрес какого-либо заметного объекта на местности. `leading-street-direction` - Направление главной улицы. `Name` - ФИО резидента или лица,

	арендующего офис. `p-o-box` - Номер абонентского ящика `place-type` - Тип площади `postal-community-name` - ФИО почтового адресата `room-number` - Номер комнаты `state` - Единица административно-территориального деления (штат, кантон, регион, провинция, префектура). `Street` - Улица. `street-suffix` - Суффикс улицы `trailing-street-suffix` - Навигационный суффикс улицы `zip-code` - Почтовый код
Создание правил	
`lldp med media-vlan-policy <0-31> (guest-voice guest-voice-signaling softphone-voice streaming-video video-conferencing video-signaling voice voice-signaling) (tagged untagged) <vlan_id> (dscp l2-priority)`	Типы приложений, в том числе: “Voice” (Голосовой вызов), “Voice Signalling” (Сигнализация голосового вызова), “Guest Voice” (Гостевой голосовой вызов), “Guest Voice Signalling” (Сигнализация гостевого голосового вызова), “Softphone Voice” (Голосовой вызов по софтофону), “Video Conferencing” (Видеоконференция), “Streaming” (Потоковая передача), “Video Signalling” (Сигнализация видеопотока). `l2-priority` – выбор одного из восьми уровней приоритета `dscp` – одно из значений 64-точечного кода

2.2.22 Таблица mac –адресов

Таблица MAC-адресов - это таблица соответствий между MAC-адресами устройств назначения и портами коммутатора. MAC-адреса могут быть статические и динамические. Статические MAC-адреса настраиваются пользователем вручную, имеют наивысший приоритет, хранятся постоянно и не могут быть перезаписаны динамическими MAC-адресами. MAC-адреса - это записи, полученные коммутатором в пересылке кадров данных, и хранятся в течение ограниченного периода времени. Когда коммутатор получает кадр данных для дальнейшей передачи, он сохраняет MAC-адрес кадра данных вместе с соответствующим ему портом назначения. Когда MAC-таблица опрашивается для поиска MAC-адреса назначения, при нахождении нужного адреса кадр данных отправляется на соответствующий порт, иначе коммутатор отправляет кадр на широковещательный домен. Если динамический MAC-адрес не встречается в принятых

кадрах данных длительное время, запись о нем будет удалена из MAC-таблицы коммутатора.

Команда	Описание
`mac address-table aging-time <0,10-1000000>`	Настройка срока устаревания для MAC - адресов, полученных обучением, которые будут присутствовать в таблице MAC - адресов. Диапазон допустимых значений: от 10 до 1000000 секунд
`mac address-table learning vlan <vlan_list>`	Включение изучения MAC-адресов в заданном vlan
`mac address-table static <mac_addr> vlan <vlan_id> interface GigabitEthernet <port_type_list>`	Настройка статических MAC-адресов

2.2.23 Private vlan

Частные VLAN основаны на маске порта источника и не соединяются с обычными VLAN. Это означает, что номера VLAN ID обычных VLAN и номера VLAN ID частных VLAN могут быть одинаковыми. Чтобы была возможна передача пакетов, порт должен принадлежать и обычной, и частной VLAN. По умолчанию, все порты не поддерживают VLAN и являются членами VLAN 1, и Private VLAN 1.

Порт, не поддерживающий VLAN, может быть членом только одной VLAN, но может быть членом нескольких частных VLAN.

Частные VLAN используются для группировки портов с целью предотвращения связи внутри PVLAN. Изоляция порта используется для предотвращения связи между портами клиентов в одной и той же VLAN или частной VLAN. Порт, который изолирован от остальных портов не может передавать какой-либо одноадресный, многоадресный или широковещательный трафик в любые другие порты той же самой VLAN или PVLAN.

Команда	Описание
Настройка портов	
`interface GigabitEthernet <port_type_list>`	Выбор портов для настройки параметров

`pvlan <range_list>`
 	
`no pvlan <range_list>`
	Создание Private VLAN
	
	Удаление Private VLAN

`pvlan isolation`
 	
`no pvlan isolation`
	Команда выполнение которой приведет к изоляции выбранных портов от остальных.
	
	Отмена команды

2.2.24 VCL

MAC-based VLAN -назначение номера VLAN в соответствии с мак-адресом хоста.

Команда	Описание
Настройка портов	
`interface GigabitEthernet <port_type_list>`	Выбор портов для настройки параметров

`switchport vlan mac <mac_ucast> vlan <vlan_id>`
 	
`no switchport vlan mac <mac_ucast> vlan <vlan_id>`
	Настройка привязки mac-адреса к vlan
	
	Удаление привязки.

Protocol-based VLAN – назначение номера VLAN в зависимости от используемого протокола.

Команда	Описание
Глобальные настройки	

`vlan protocol eth2 <0x600-0xffff> group <word16>`
 	
`vlan protocol snap 0x00E02B 0x0001 group <word16>`
 	
`vlan protocol llc 0xff 0xff group <word16>`
	Выбор соответствующего протокола
	
	0x00E02B – OUL (0x000000 - 0XFFFFFF)
	0x0001 – PID(0x0 - 0xFFFF)
	
	0xff – DSAP(0x00 - 0xFF)
	0xff - SSAP(0x00 - 0xFF)

Настройка группы	
`interface GigabitEthernet <port_type_list>`	Выбор портов для объединения в группу

`switchport vlan protocol group <word16> vlan <vlan_id>`
 	
`no switchport vlan protocol group <word16>`
	Команда выполнение которой приведет к объединению портов в одну группу и назначение ей VLAN.
	
	Удаление соответствующей группы

IP Subnet-based VLAN - назначение номера VLAN в зависимости от ip-адреса

Команда	Описание
Настройка портов	
`interface GigabitEthernet`	Выбор портов для настройки параметров

<port_type_list>	
switchport vlan ip-subnet <ipv4_subnet> <vlan_id> no switchport vlan ip-subnet <ipv4_subnet> <vlan_id>	Настройка привязки ip-адресов к vlan Удаление привязки.

2.2.25 Voice VLAN

Функция голосовой VLAN позволяет пересылать голосовой трафик в голосовой VLAN, после чего коммутатор может классифицировать и планировать сетевой трафик. Рекомендуется, чтобы на порту было две сети VLAN - одна для голоса, другая для данных.

Команда	Описание
Глобальные настройки	
voice vlan no voice vlan	Включение функции voice vlan Прежде чем включить голосовой VLAN, отключите MSTP, чтобы избежать конфликта. Выключение функции voice vlan
voice vlan vid	Назначение номера vlan
voice vlan aging-time <10-10000000>	Настройка времени безопасного обучения. Допустимый диапазон составляет от 10 до 10000000 секунд. По умолчанию – 86400сек.
voice vlan class <0-7>	Указывает класс трафика. Весь трафик в Voice VLAN будет иметь этот класс. По умолчанию установлен 7 класс.
voice vlan oui <oui> description <line32> no vlan oui <oui>	Создание записи в таблице OUI Oui – это глобальный уникальный идентификатор, присвоенный IEEE. Он должен состоять из 6 символов, формат ввода - «xx-xx-xx» (x - шестнадцатеричная цифра). Description – Описание адреса OUI Удаление соответствующей записи.
Настройка портов	
interface GigabitEthernet <port_type_list>	Выбор портов
switchport voice vlan mode	Настройка режима

{auto | disable | force}	Auto – автоматическое определение Disable - отключен Force - принудительное включен
switchport voice vlan security no switchport voice vlan security	Включение режима безопасности. Когда эта функция включена, все нетелефонные MAC-адреса в VLAN будут заблокированы на 10 секунд. Выключение режима безопасности. Когда эта функция включена, все нетелефонные MAC-адреса в VLAN будут заблокированы на 10 секунд.
switchport voice vlan discovery-protocol { both | lldp | oui}	Настройка протокола обнаружения порта. Работает только при режиме «Auto». Возможные протоколы обнаружения: Both- OUI и LLDP Lldp- обнаружение телефонного устройства по LLDP Oui- обнаружение телефонного устройства по адресу OUI

2.2.26 QoS (Качество обслуживания)

Сетевой трафик всегда непредсказуем, поэтому основным фактором обеспечения качества является предоставление наилучшего способа доставки. Для преодоления этой проблемы используется понятие качества обслуживания (Quality of Service (QoS)) применяемое ко всей сети. Гарантируется, что сетевой трафик будет приоритезирован в соответствии с заданным критерием, и прием будет производиться с использованием обработки по приоритетам. 115 QoS позволяет назначить различные классы сетевых услуг различным типам трафика, например, мультимедийному, видео, трафику конкретного протокола, критичному по времени трафику, трафику резервного копирования файлов. Чтобы задать приоритеты пакетов на данном коммутаторе, перейдите на страницу “Port Classification” (Классификация порта).

Команда	Описание
Глобальные настройки	
DSCP-Based QoS Ingress Classification	
qos map dscp-cos <0-63> cos <0-7> dpl <0-1>	настройка основных QoS DSCP на основе параметров QoS Ingress классификации. dscp-cos <0-63> - Значение DSCP входящего пакета. <0-7> - значение cos dpl <0-1> – Выбор приоритета отбрасывания DPL для соответствующего значения DSCP для обработки входящих кадров. По умолчанию задано 0. Значение “1” дает более высокий приоритет отбрасывания.
DSCP Translation	
qos map dscp-ingress-translation <0-63> <0-63>	Преобразование DSCP на входящей стороне в любое из <0-63> значений DSCP.
qos map dscp-classify <0-63>	Включение классификации на входящей стороне, как определено в таблице настройки DSCP QoS на порту
qos map dscp-egress-translation <0-63> <0-1> to <0-63>	Настройки для исходящей стороны. Заново отображает значение DP в выбранное значение DSCP. <0-1> 0- Управляет перераспределением кадров с уровнем DP 0. 1- Управляет перераспределением кадров с DP уровня 1. В любом случае после выбора требуется ввести значение, на которое будет переназначен DSCP
DSCP Classification	
qos map cos-dscp <0~7> dpl <0~1> dscp {<0-63> | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af3 | af33 | af41 | af42 | af43 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va }	Настройка сопоставления CoS и DPL со значением DSCP <0~7> - класс обслуживания <0~1> - уровни приоритета отбрасывания для которого необходимо выбрать значение dscp
QoS Control List Configuration	
qos qce <1-256>	Создание записи QCE
qos qce <1-256> interface GigabitEthernet <port_type_list>	Выбор портов, настроенных с помощью этого QCE
qos qce <1-256> dmac {<mac_addr> | any | broadcast | multicast | unicast}	Настройка MAC-адреса назначения. Возможны следующие значения: any (Любой), broadcast (Широковещательный), multicast

	(Многоадресный), unicast (Одноадресный).
qos qce <1-256> smac {<mac_addr> | any}	Настройка MAC-адреса источника. Возможно указать конкретный MAC или выбрать любой.
qos qce <1-256> tag type {any | c-tagged | s-tagged | tagged | untagged}	Указание тип тега. Возможные значения: any: Сопоставление кадров с тегами и без тегов. untagged: Соответствие немаркированным кадрам. tagged: Сопоставление кадров с тегами. c-tagged: Соответствие фреймов с C-тегами. s-tagged: Соответствие фреймов с S-тегами. Значение по умолчанию - «Любой».
qos qce <1-256> tag vid {<vcap_vr> | any}	Указание диапазона VLAN или любой VLAN
qos qce <1-256> tag pcp { <pcp> | any}	Указание значения PCP, возможно указать конкретное значение, диапазон или выбрать вариант “любой”. Допустимые значения 0-7.
qos qce <1-256> tag dei { <0-1> | any}	Указание значения DEI. Может быть “0”, “1” или “любое”
qos qce <1-256> inner-tag type {any | c-tagged | s-tagged | tagged | untagged}	Указание типа внутреннего тега.
qos qce <1-256> inner-tag vid {<vcap_vr> | any}	
qos qce <1-256> inner-tag pcp {<pcp> | any}	
qos qce <1-256> inner-tag dei {<0-1> | any}	
qos qce <1-256> frame-type {any | etype |ipv4 | ipv6 | llc | snap}	Указание типа кадра, используемого при просмотре входящих кадров. Возможны следующие типы кадров: Any - QCE будет соответствовать всем типам кадров. Etype – Будут разрешены только кадры Ethernet (с типом EtherType 0x600-0xFFFF) llc – Будут разрешены только кадры LLC. snap -Будут разрешены только кадры SNAP. ipv4–QCE будет соответствовать только кадрам IPV4. ipv6–QCE будет соответствовать только кадрам IPV6.
qos qce <1-256> action { cos | dpl | dscp | pcp-dei | policy	Настройка операции, выполняемой на входящих кадрах, когда настройки

`| vid}`	параметров согласуются с содержимым кадра. `Cos` – значения (0-7) или «По умолчанию» `Dpl` – значения (0- 1) или «По умолчанию». `Dscp` - (0-63, BE, CS1-CS7, EF или AF11-AF43) или «По умолчанию». `pcp-dei` – значения pcp (0-7) или «По умолчанию», dei - (0-1) или «По умолчанию» `policy` – номер acl политики или «По умолчанию» `vid -` значение vlan «По умолчанию» означает, что классифицированное значение по умолчанию не изменяется этим QCE.
Global Storm Policer Configuration	
`qos storm {broadcast | multicast | unicast} <1-1024000> {fps | kfps}`	Настройка управления широковещательным штормом `broadcast | multicast | unicast - выбор типа пакетов` `<1-1024000> -` пороговое значение в пакетах в секунду. Принятые пакеты, при которых превышено выбранное значение, будут отброшены. `fps | kfps-` единицы измерения
Weighted Random Early Detection Configuration	
`qos wred queue <0~7> min-fl <1-100> max <1-100> fill-level`	Настройка управления переполнением очередей `<0~7>` - номер очереди `min-fl <1-100>` - нижний пороговый уровень заполнения. Если уровень заполнения очереди ниже этого порога, вероятность отбрасывания равна нулю. Значение 0–100%. `max <1-100>` - Управляет верхней вероятностью отбрасывания или пороговым значением уровня заполнения для кадров, помеченных как уровень приоритета отбрасывания > 0. Значение 1–100%. `fill-level -max` управляет уровнем заполнения, при котором вероятность выпадения достигает 100%. Эта конфигурация позволяет зарезервировать часть очереди исключительно для кадров, отмеченных уровнем приоритета отбрасывания 0 (зеленые

	кадры). Зарезервированная часть рассчитывается как (100 - Макс) %. По умолчанию - `max` управляет вероятностью выпадения, когда уровень заполнения чуть ниже 100%.
Настройка порта	
`interface GigabitEthernet <port_type_list>`	Выбор портов
QoS Port DSCP Configuration	
`qos dscp-translate`	включение трансляцию значений DSCP на основе установленного метода классификации

`qos dscp-classify {any | selected | zero}`
 	
`No qos dscp-classify`
	Выбор метода классификации
	`Zero` – Классификация выполняется, если DSCP входящих кадров равен 0.
	`Selected` - классифицируются только DSCP, для которых включена классификация в таблице трансляции DSCP.
	`any` – классифицируются все поля DSCP.
	
	Классификация DSCP входящих кадров не выполняется

`qos dscp-remark {remap | remap-dp | rewrite}`
 	
`No qos dscp-remark`
	Настройка перезаписи значений DSCP исходящих кадров.
	`rewrite` - Перезапись значений DSCP исходящих кадров включена, но отображение после перезаписи не выполняется.
	`remap` - Кадр с DSCP, поступивший от анализатора, снова отображается и помечается новым значением DSCP. В зависимости от уровня DP кадра, новое значение DSCP берется из таблицы трансляции DSCP из поля Egress Remap DP0 или DP1.
	`remap-dp` – Кадр с DSCP, поступивший от анализатора снова отображается и помечается новым значением DSCP. Новое значение DSCP всегда берется из таблицы трансляции DSCP из поля Egress Remap DP0
	
	Перезапись значений DSCP исходящего трафика выключена

QoS Egress Port Tag Remarking	

qos tag-remark {mapped | pcp <0-7> dei <0-1>}	Выбор режима изменения тегов на порту Mapped – Используется отображение значений классов QoS и уровней DP в значения PCP/DEI. pcp <0-7> dei <0-1> – Используются значения PCP/DEI. По умолчанию - PCP:0; DEI:0.
QoS Egress Port Shapers	
qos wrr <1-100>	Установка режима работы с очередями – взвешенный, должен быть задан вес в каждой очереди. По умолчанию режим работы с очередями - строгий. В этом режиме кадры из выходных очередей с более высокими приоритетами будут передаваться первыми (по сравнению с кадрами, находящимися в очередях с низкими приоритетами).
No qos wrr	Bsключение взвешенного режима работы с очередями
Ingress Queue Policers	
qos queue-policer queue <0~7> <1-3276700> {kbps | mbps}	Настройка скорости в очередях <0~7> – номер очереди <1-3276700> – Скорость, до которой будет ограничена скорость в очереди. По умолчанию задано 500 кбит/с. Допустимый диапазон значений для kbps (кбит/с): от 100 до 1000000. Допустимый диапазон значений для Mbps (Мбит/с): от 1 до 3300 Мбит/с. { kbps | mbps} – Единицы измерения ограничения скорости очереди входящих кадров.
Ingress Port Policers	
qos policer <1-3276700> {fps | kbps | kfps | mbps} flowcontrol	Настройка и включение функции ограничения скорости на порту <1-3276700>– скорость, до которой будет ограничена скорость на порту. По умолчанию задано 500 кбит/с. Допустимый диапазон для kbps (кбит/с) и fps (кадров/с): от 100 до 1000000. Допустимый диапазон для Mbps (Мбит/с) и kfps (кадров/с): от 1 до 3300 Мбит/с. {fps | kbps | kfps | mbps} – Единицы измерения ограничения скорости Flowcontrol – включение функции управления потоком. Если управление потоком включено и порт работает в режиме управления потоком, то будут

	отправляться кадры pause, вместо отбрасывания входящих кадров.
Port Classification	
`qos cos <0-7>`	Настройка класса QoS, выбираемый по умолчанию. Класс QoS с номером 0 имеет наименьший приоритет. По умолчанию задано 0.
`qos dpl <0-1>`	Настройка приоритета отбрасывания: 0: Подтвержденные кадры. 1: Кадры, которые могут быть отброшены
`qos pcp <0-7>`	Настройка значения пользовательского приоритета (Priority Code Point) для нетегированных кадров.
`qos dei <0-1>`	Настройка значения индикатора отбрасывания по критерию (Drop Eligible Indicator) для нетегированных кадров.

`qos trust tag`
 	
`No qos trust tag`
	режим классификации для тегированных кадров на данном порту:
	• Enabled (Включен): Для тегированных кадров используется значение PCP и DEI из таблицы (PCP, DEI) to (QoS class, DP level) Mapping.
	
	• Disabled (Выключен): Для тегированных кадров используется класс QoS и уровень DP по умолчанию.

`qos trust dscp`	включение QoS на основе DSCP (входящий порт).
`qos qce key {double-tag | ip-addr | mac-ip-addr | normal}`	Выбор типа определяющего ключа, сгенерированный для кадров, полученных через порт. Допустимые значения: `Normal` – соответствует внешнему тегу, SMAC/DMAC, IP-протоколу, DSCP, SIP/DIP, SPORT и DPORT. `double-tag` – четверть ключа, соответствует внутреннму и внешнему тегу. `ip-addr` - половина ключа, совпадение внутреннего и внешнего тега, SIP и DIP. Для кадров, не относящихся к IP, используйте только внешний тег. `mac-ip-addr` – Полный ключ, совпадающий внутренний и внешний тег, SMAC, DMAC, SIP и DIP.
`qos qce addr {destination | source}`	Выбор режима IP/MAC-адреса, определяющего, должна ли классификация QCL основываться на адресах источника (SMAC/SIP) или назначения (DMAC/DIP) на этом порту. Этот параметр используется только в том случае, если тип ключа

	Normal . Допустимыми значениями являются: `source` – Позволяет сопоставлять SMAC/SIP. `Destination` – Позволяет сопоставлять DMAC/DIP.

2.2.27 Mirroring (Зеркалирование)

Зеркалирование портов— технология дублирования пакетов одного порта сетевого коммутатора (или отдельной VLAN) на другом.

Зеркалирование портов используется на сетевом коммутаторе для отправки копии сетевых пакетов, видимых на указанных портах (исходный порт), на другие указанные порты (порт назначения). При включенном зеркалировании портов пакеты можно отслеживать и анализировать. Зеркалирование портов применяется широко, например, сетевые инженеры могут использовать зеркалирование портов для анализа и отладки данных или диагностики ошибок в своих сетях, без влияния на возможности обработки пакетов сетевых устройств.

Команда	Описание
Глобальные настройки	

`monitor session <1-5>`
 	
`no monitor session <1-5>`
	Включение функции зеркального отображения (всего возможно создать до пяти сеансов)
	
	Выключение функции зеркального отображения или дистанционного зеркалирования

`monitor session <1-5> source interface` <port_type_list> { both | rx | tx}	Выбор порта источника и типа трафика Both - На зеркальный порт будут переданы кадры, принятые и переданные данным портом Rx - На зеркальный порт будут направлены только кадры, принятые данным портом. Tx - На зеркальный порт будут направлены только кадры, переданные данным портом.
`monitor session <1-5> destination interface` <port_type_list>	Выбор порта назначения, который получает копию трафика из исходного порта.
`monitor session <1-5> source remote vlan <vlan_id>`	Включение режима RMirror Source и назначение vlan куда будет скопирован пакет. Коммутатор является исходным узлом для

	отслеживания потока. Порт источника расположены на этом коммутаторе.
monitor session <1-5> destination remote vlan <vlan_id>	Включение режима RMirror Destination и назначение vlan куда будет скопирован пакет. Коммутатор является конечным узлом для отслеживания потока. Порт назначения расположен на этом коммутаторе.
monitor session <1-5> source vlan <vlan_list>	Настройка функции зеркалирования на основе VLAN. Если вы хотите контролировать некоторые VLAN на коммутаторе, вы можете установить выбранные VLAN. Сеанс зеркалирования должен иметь в качестве источников либо порты, либо сети VLAN, но не то и другое вместе.

2.2.28 UPnP

Команда	Описание
Глобальные настройки	
Upnp No Upnp	Включение функции UPnP. При включении автоматически создается два правила списка доступа (ACE) для перенаправления соответствующих UPnP пакетов к процессору. Выключает функцию UPnP. При выключении правила автоматически удаляются.
upnp advertising-duration <100-86400>	Настройка параметра продолжительности. Этот параметр определяет, насколько часто могут посылаться уведомления UPnP. Длительность переносится пакетами протокола SSDP (Simple 129 Service Discover Protocol), которые информируют пункт управления о том, насколько часто следует принимать сообщения с уведомлениями SSDP от коммутатора. По умолчанию установлена длительность уведомления 100 секунд. Однако, вследствие ненадежности протокола UDP рекомендуется уменьшать длительность, так как чем она меньше, тем быстрее обновляется состояние UPnP.
upnp ip-addressing-mode {dynamic | static}	Режим ip-адресации dynamic - режим по умолчанию. Модуль UPnP помогает пользователям выбрать IP-адрес коммутатора. Он находит первый доступный системный IP-адрес.

	static - Пользователь указывает IP-интерфейс VLAN для выбора IP-адреса коммутирующего устройства.
upnp static interface vlan <vlan_id>	Настройка Vlan id для режима статической ip адресации.

2.2.29 PTP

Протокол точного времени (PTP - Precision Time Protocol), также известный как IEEE1588, является стандартом, определённым Институтом инженеров по электротехнике и электронике (IEEE) и используемым для точной синхронизации часов сетевых устройств. На коммутаторе применяется протокол синхронизации времени IEEE 1588v2, обеспечивающий высокую точность синхронизации между устройствами и позволяющий распределённой системе на основе Ethernet поддерживать точную синхронизацию времени между всеми сетевыми узлами.

Команда	Описание
Глобальные настройки	
ptp ext {auto | ltc} {input | output}	Настройка режима 1PPS Auto – автоматический выбор управления часами на основе профиля PTP и доступных ресурсов HW. Ltc – выбор управления частотой счетчика местного времени (LTC). Input – включает вход тактовой частоты 1 pps. output – включает выход тактовой частоты 1 pps.
ptp ext ext <1-25000000> no ptp ext ext <1-25000000>	Настройка тактовой частоты. Возможный диапазон значений: 1 - 25000000 (1 - 25 МГц). Отмена команды
ptp <0-3>	Создание экземпляра часов
ptp <0-3> domain	указывает на HW-тактовый домен, используемый часами.
ptp <0-3> mode{ boundary | e2etransparent | master | p2ptransparent | slave} profile { 802.1as | g8265.1 | g8275.1 | ieee1588}	выбор типа часов и профиля, используемого часами Boundary – обычные часы с ограничением e2etransparent- сквозные прозрачные часы master- только мастер p2ptransparent- одноранговые прозрачные часы slave- только ведомое устройство

2.2.30 GVRP

GVRP (Genecic VLAN Registration Protocol) является одним из приложений GARP (Generic Attribute Registration Protocol, Протокол регистрации общих аттрибутов). GARP используется в сетевых мостах, сетевых коммутаторах, или других аналогичных устройствах с возможностью регистрации и перерегистрации специальных атрибутов, таких как идентификаторы VLAN и членство в мультикастовых группах в больших локальных сетях. GVRP - приложение GARP, которое отвечает за обмен информацией о VLAN и позволяет коммутаторам регистрировать VLAN динамически.

Команда	Описание
Глобальные настройки	
`gvrp`	Включение протокола GVRP глобально

`gvrp time join-time <1-20>`
 	
`gvrp time leave-time <60-300>`
 	
`gvrp time leave-all-time <1000-5000>`
	Настройка таймеров. Таймеры на обоих концах сети должны быть одинаковы, иначе GVRP не сможет работать нормально.

`gvrp max-vlans <1-4094>`	Настройка максимального количества VLAN, которыми GVRP может управлять.
Настройка порта	
`interface GigabitEthernet <port_type_list>`	Выбор портов
`gvrp`	Включение функции gvrp Рекомендуется избегать использования функций GVRP и RSTP одновременно на коммутаторе. Если необходимо включить GVRP, сначала необходимо отключить функцию RSTP для портов

2.2.31 sFlow

sFlow - это технология системы измерения сетевого трафика общего назначения. sFlow предназначен для встраивания в любое сетевое устройство и обеспечения непрерывной статистики по любому протоколу (L2, L3, L4 и вплоть до L7), так что весь трафик в сети может быть точно охарактеризован и отслежен. Эти статистические данные важны для контроля перегрузки, устранения неполадок, наблюдения за безопасностью, планирования сети и т. Д. Они также могут использоваться для целей учета IP.

Команда	Описание
Глобальные настройки	
sflow agent-ip {ipv4 | ipv6} {<ipv4_addr> | <ipv6_addr>}	Настройка IP-адреса, используемого в качестве IP-адреса агента в sFlow. Он служит уникальным ключом, который будет идентифицировать агента в течение длительных периодов времени. Поддерживаются адреса IPv4 и IPv6
sflow collector-address {<domain_name> | <ipv4_addr> | <ipv6_ucast>}	Настройка IP-адреса или имя хоста приемника sFlow
sflow collector-port <1-65535>	Настройка просматриваемого UDP порта
sflow max-datagram-size <200-1468>	Настройка максимального количество байтов данных, которое может быть отправлено в одной тестовой датаграмме
sflow timeout <0-2147483647>	Настройка таймаута
Настройка портов	
interface GigabitEthernet <port_type_list>	Выбор портов
sflow	Включает функцию sflow на порту.
sflow sampling-rate <1-4096>	Настройка статической частоты дискретизации.
sflow max-sampling-size <14-200>	Максимальное количество байтов, которое должно быть скопировано из пакета, выбранного для выборки, в дейтаграмму sFlow.
sflow counter-poll-interval <1-3600>	Интервал опроса. Допустимый диапазон: от 1 до 3600 секунд

2.2.32 UDLD

Обнаружение однонаправленного соединения (UDLD) это уровень канала передачи данных протокол для контроля физической конфигурации кабелей и обнаружения однонаправленных каналов. UDLD дополняет протокол связующего дерева, который используется для устранения петли переключения.

Чтобы обнаружить однонаправленные каналы до создания петли пересылки, UDLD работает путем обмена пакетами протокола между соседними устройствами.

Для работы UDLD оба коммутирующих устройства в канале должны поддерживать UDLD и иметь его включенным на соответствующих портах.

Команда	Описание
Глобальные настройки	
Udld enable	Включение UDLD на всех

	оптоволоконных портах.
`Udld aggressive`	Включение UDLD в агрессивном режиме на всех оптоволоконных портах.
`udld message time-interval <7-90>`	Настройка интервал сообщений `<7-90>`
`udld unblocking`	Ручное включение заблокированных портов.

2.2.33 DDMI (интерфейс цифрового диагностического мониторинга)

Усовершенствованный цифровой интерфейс позволяет установить связь в реальном времени между коммутатором и трансивером SFP. Это позволяет коммутатору получать доступ к рабочим параметрам в оптоволоконном канале.

DDMI контролирует:

• температуру

• напряжение питания

• передаваемый ток смещения.

• Передаваемая мощность

• Полученная мощность

Команда	Описание
Глобальные настройки	

`ddmi`
 	
`no ddmi`
	Включение функции DDMI. Функция DDMI включена по умолчанию.
	
	Выключение функции DDMI

2.2.34 MRP и MVRP

Multiple Registration Protocol (MRP) - это общая структура, рекомендованная IEEE для использования в сетевых мостах, сетевых коммутаторах, или других аналогичных устройствах с возможностью регистрации и перерегистрации специальных атрибутов, таких как идентификаторы VLAN и членство в мультикастовых группах в больших локальных сетях LAN.

Протокол множественных регистраций **VLAN** Multiple VLAN Registration Protocol (MVRP) является сетевым протоколом второго уровня для автоматической конфигурации информации **VLAN** в коммутаторах. Он был определён приложением **802.1ak** к рекомендациям **IEEE 802.1Q**-2005.

В пределах второго уровня сетевой модели **OSI** MVRP обеспечивает динамический обмен информации о **VLAN** и конфигурацию необходимых **VLAN**. Например, поставлена задача добавить определённый порт коммутатора в **VLAN**, или сетевое устройство, поддерживающее VLAN и подключённое в порт коммутатора требует переконфигурации, и все необходимые транки динамически созданы на других коммутаторах,

поддерживающих MVRP. Для выполнения этой задачи без возможностей MVRP потребуется ручная конфигурация VLAN или какой-либо проприетарный метод производителя. Если же выполнять эту задачу средствами MVRP, который использует динамические значения VLAN в фильтруемой базе данных. Если коротко — MVRP помогает динамически поддерживать конфигурации VLAN в статических конфигурациях сетей.

802.1Q даёт возможность:

- Динамически конфигурировать и распределять информацию о принадлежности VLAN через механизмы MVRP.
- Статически конфигурировать информацию о принадлежности VLAN посредством механизмов менеджмента, которые позволяют управлять регистрационными данными о статических записях регистраций VLAN.
- Поддерживать комбинированные статические и динамические конфигурации, при которых некоторые VLAN конфигурируются посредством механизмов менеджмента, а для других VLAN сохраняется возможность динамической конфигурации средствами MVRP.

Команда	Описание
Глобальные настройки	

`mvrp`
 	
`no mvrp`
	Включение функции MVPR.
	
	Выключение функции MVRP

`mvrp managed vlan {<vlan_list> | add | all | except | none | remove}`	Настройка списка VLAN, управляемых MVRP `<vlan_list>` - создание нового списка `Add` – добавить VLAN к существующему списку `All` – все VLAN `Except` – Добавить все VLAN, кроме следующих `None` – пустой список `Remove` – удалить VLAN из текущего списка
Настройка портов	
`interface GigabitEthernet <port_type_list>`	Выбор портов
`Mvrp` `No mvrp`	Включение функции MVRP на порту Выключение функции MVRP на порту.

`mrp periodic`
 	
`no mrp periodic`
	Включение функции PeriodicTransmission для всех приложений MRP на порту
	
	Выключение функции PeriodicTransmission на порту

`mrp timers {default | join-`	Настройка таймеров

time | leave-all-time | leave-time}	Default - Установка всех таймеров MRP по умолчанию join-time – таймер присоединения. Значения от 1-20сс. По умолчанию значение 20сс. leave-all-time – таймер отключения от всех мультикастовых групп. Значения 1000-5000сс. По умолчанию – 1000сс leave-time – таймер отключения. Значения от 60-300сс. По умолчанию значение 60сс

2.2.35 Link OAM

Команда	Описание
Настройка портов	
interface GigabitEthernet <port_type_list>	Выбор портов
link-oam no link-oam	Включение Link OAM на порту коммутатора. Включение Link OAM дает операторам сети возможность отслеживать состояние сети и быстро определять местоположение неисправных каналов или неисправных состояний. Выключение Link OAM на порту
link-oam mode {active |} passive}	Настройка режима OAM как активный или пассивный. По умолчанию установлен пассивный режим. active - DTE, настроенные в активном режиме, инициируют обмен информационными OAMPDU, как определено в процессе обнаружения. После завершения процесса обнаружения активным DTE разрешается отправлять любые OAMPDU при подключении к удаленному одноранговому объекту OAM в активном режиме. Активные DTE работают в ограниченном отношении, если удаленный объект OAM работает в пассивном режиме. Активные устройства не должны отвечать на команды удаленной обратной связи OAM и запросы переменных от пассивного однорангового узла. passive - DTE, настроенные в пассивном режиме, не инициируют процесс обнаружения. Пассивные DTE реагируют на инициирование процесса обнаружения удаленным DTE. Это исключает

	возможность перехода от пассивных к пассивным ссылкам. Пассивные DTE не должны отправлять запросы переменных или OAMPDU управления шлейфом.

`link-oam remote-loopback supported`
 	
`no link-oam remote-loopback supported`
	Включение функции удаленной петли. Может использоваться для локализации неисправностей и тестирования производительности связи.
	
	Выключение функции удаленной петли.

`link-oam link-monitor supported`
 	
`no link-oam link-monitor supported`
	Включение функции мониторинга на порту.
	
	Выключение функции мониторинга на порту.

`link-oam mib-retrieval supported`
 	
`no link-oam mib-retrieval supported`
	Включение поддержки MIB на порту коммутатора
	
	Выключение поддержки MIB на порту коммутатора

Настройка событий	
`link-oam link-monitor frame {threshold | window}`	Событие "Ошибочный кадр" подсчитывает количество ошибочных кадров, обнаруженных в течение указанного периода. Период задается временным интервалом (`window`). Это событие генерируется, если количество ошибочных кадров равно или превышает заданный порог для этого периода (`threshold`). `Window` – окно ошибки должно иметь целое значение от 1 до 60, а его значение по умолчанию равно "1". `Threshold` – порог ошибки должен находиться в диапазоне 0-4294967295, а его значение по умолчанию равно "1".
`link-oam link-monitor symbol-period {threshold | window}`	Событие подсчитывает количество ошибок символа, произошедших в течение указанного периода. Период определяется количеством символов, которые могут быть получены за определенный промежуток времени на базовом физическом уровне. Это событие генерируется, если количество ошибок символа равно или превышает заданный порог для этого периода. `window` - окно ошибки должно иметь целое значение от 1 до 60, а его значение по умолчанию равно "1". `threshold` - порог ошибки должен

	находиться в диапазоне 0-4294967295, а его значение по умолчанию равно "1".
link-oam link-monitor frame-seconds {threshold | window}	Событие подсчитывает количество секунд с ошибками, произошедших в течение указанного периода. Период определяется временным интервалом. Это событие генерируется, если количество секунд с ошибками в кадре равно или превышает заданный порог для этого периода. Window – окно ошибки должно иметь целое значение в диапазоне от 10 до 900, а его значение по умолчанию равно "60". threshold - порог ошибки должен находиться в диапазоне 0-65535, а его значение по умолчанию равно "1".

2.2.36 CFM

CFM (Connectivity Fault Management), IEEE 802.1 ag – предоставляет функции наблюдения, поиска и устранения неисправностей в сетях Ethernet, позволяя контролировать соединение, изолировать проблемные участки сети и идентифицировать клиентов, к которым применялись ограничения в сети.

Команда	Описание
Глобальные настройки	
cfm sender-id-tlv {chassis | chassis-management | disable | management}	Выбор идентификатора tlv Chassis – идентификатор шасси(MAC-адрес) chassis-management - идентификатор шасси(MAC-адрес) и адрес управления (IPv4-адрес) management - адрес управления (IPv4-адрес) disable – исключить идентификатор tlv
cfm port-status-tlv {disable enable}	Включение или выключение tlv для статуса порта
cfm interface-status-tlv {disable enable}	Включение или выключение tlv для статуса интерфейса
cfm organization-specific-tlv disable	Исключить TLV для конкретной организации
cfm organization-specific-tlv enable oui <oui> subtype <0-255> value <string63>	Включить TLV для конкретной организации <oui> - Это трехбайтовый OUI, передаваемый с TLV, зависящим от организации. <0-255> - Это подтип, передаваемый с

	TLV для конкретной организации. Может быть любым значением в диапазоне [0; 255] `<string63>` - Это значение, передаваемое в TLV для конкретной организации. Значение представляет собой печатаемую строку символов длиной 0-63.
CFM Domain Configuration	
`cfm domain <kword1-15>`	Создание имени домена
`Format {none | string}`	Выбор формата имени MD. Чтобы имитировать идентификаторы MEG Y.1731, используйте тип None.
`Level <0-7>`	Уровень MD / MEG этого домена. Допустимые значения ограничены до 0–7.
`sender-id-tlv {chassis | chassis-management | defer | disable | management }`	Выбор идентификатора tlv `Chassis` – идентификатор шасси(MAC-адрес) `chassis-management` - идентификатор шасси(MAC-адрес) и адрес управления (IPv4-адрес) `management` - адрес управления (IPv4-адрес) `disable` – исключить идентификатор tlv `defer` – применяются настройки глобальной конфигурации
`port-status-tlv {defer | disable | enable}`	Включение или выключение tlv для статуса порта `Defer` – применяются настройки глобальной конфигурации
`interface-status-tlv {defer | disable | enable}`	Включение или выключение tlv для статуса интерфейса `Defer` – применяются настройки глобальной конфигурации
`organization-specific-tlv {defer | disable}`	`disable` - исключить TLV для конкретной организации `Defer` – применяются настройки глобальной конфигурации
`Service <kword1-15>`	Переход в режим конфигурации CFM Service
CFM Service Configuration	
`Format { integer primary-vid string }`	Выбор формата имени службы. Это решает, как будет интерпретироваться значение параметра Name. Возможные значения: `integer`

	primary-vid string
type {port | vlan <1-4095>}	Выбор MEP в сервисе Основной VID MA. VLAN, равный 0, означает, что все MEP, созданные в этом MA, будут созданы как MEP порта (интерфейсные MEP). На каждом интерфейсе может быть только одна портовая MEP. MEP данного порта может быть создана с тегами, если VLAN этой MEP не равна нулю.
continuity-check interval {100ms | 10ms | 1s | 3.3ms}	Настройка скорости CCM всех MEP, привязанных к этой услуге
sender-id-tlv {chassis | chassis-management | defer | disable | management}	Выбор идентификатора tlv Chassis – идентификатор шасси(MAC-адрес) chassis-management - идентификатор шасси(MAC-адрес) и адрес управления (IPv4-адрес) management - адрес управления (IPv4-адрес) disable – исключить идентификатор tlv defer – применяются настройки глобальной конфигурации
port-status-tlv {defer | disable | enable}	Включение или выключение tlv для статуса порта Defer – применяются настройки глобальной конфигурации
interface-status-tlv {defer | disable | enable}	Включение или выключение tlv для статуса интерфейса Defer – применяются настройки глобальной конфигурации
organization-specific-tlv {defer | disable}	disable - исключить TLV для конкретной организации Defer – применяются настройки глобальной конфигурации
Mep <1-8191>	Переход в режим конфигурации CFM Mep
CFM Mep Configuration	
interface GigabitEthernet <port_type_id>	Указание порта на котором находится эта MEP
Vlan {1-4095 | inherit}	Указание идентификатора VLAN. inherit - используется для обозначения нетегированного трафика (подразумевается MEP порта).
Pcp <0-7>	Выбор значения PCP в теге VLAN PDU. Не используется без тегов.

Smac <mac_ucast>	Настройка MAC-адреса источника, который будет использоваться в блоках PDU CCM, исходящих от этой MEP. Адрес должен быть одноадресным. Формат: XX: XX: XX: XX: XX: XX. Если все нули, вместо него будет использоваться MAC-адрес порта коммутатора.
alarm-level <1-6>	Установка уровня сигнализации. Если обнаружен дефект с приоритетом выше этого уровня, будет сгенерировано уведомление о неисправности. Допустимый диапазон: [1; 6], где 1 указывает, что любой дефект вызывает аварийный сигнал, а 6 означает, что никакой дефект не может вызвать аварийный сигнал.
alarm-time-present <2500-10000>	Установка времени в миллисекундах, в течение которого должны присутствовать дефекты, прежде чем будет выдано уведомление о неисправности. По умолчанию 2500 мс.
alarm-time-absent <2500-10000>	Установка времени в миллисекундах, в течение которого дефекты должны отсутствовать до сброса уведомления о неисправности. По умолчанию 10000 мс.
continuity-check no continuity-check	включение генерации сообщений проверки целостности (CCM) отключение генерации сообщений проверки целостности
admin-state {disable | enable}	включить или отключить эту MEP. Когда эта MEP включена, она проверяет полученные / отсутствующие CCM и может вызывать дефекты.
remote mep <1-8191>	Установка удаленной MEP, от которой эта MEP, как ожидается, будет получать PDU CCM.

2.2.37 APS

APS сетевой протокол канального уровня, предназначен для поддержки топологии, исключающей зацикливание трафика, и её перестроение в случае нарушений в кольцевых сетях Ethernet на первом-втором уровне сетевой модели OSI.

Команда	Описание
Глобальные настройки	
Aps <1-10>	Создание экземпляра APS
working interface GigabitEthernet <port_type_id>	Назначение интерфейса в качестве рабочего порта
working sf-trigger link	Выбор триггера для сигнала ошибки

	В качестве триггера используется состояние порта
working sf-trigger mep domain <kword1-15> service <kword1-15> mep-id <1-8191>	В качестве триггера используется mep. Требуется ввод domain service mep-id, относящиеся к экземпляру MEP, который должен представлять рабочий поток. Выбранный экземпляр MEP может не существовать при настройке этого APS.
protect interface GigabitEthernet <port_type_id>	Назначение интерфейса в качестве защищенного порта
protect sf-trigger link	Выбор триггера для сигнала ошибки В качестве триггера используется состояние порта
protect sf-trigger mep domain <kword1-15> service <kword1-15> mep-id <1-8191>	В качестве триггера используется mep. Требуется ввод domain service mep-id, относящиеся к к экземпляру MEP, который должен представлять рабочий поток. Выбранный экземпляр MEP может не существовать при настройке этого APS.
Mode {1-for-1 | bidirectional-1-plus-1 | unidirectional-1-plus-1}	1-for-1 - В линейной архитектуре защитной коммутации 1: 1 защитный транспортный объект выделен рабочему транспортному объекту. Однако нормальный трафик транспортируется либо на рабочем транспортном объекте, либо на защитном транспортном объекте, используя мост селектора в источнике защищенного домена. Селектор в приемнике защищенного домена выбирает объект, который несет нормальный трафик bidirectional-1-plus-1 - В линейной архитектуре защитной коммутации 1 + 1 для каждого рабочего транспортного объекта выделен защитный транспортный объект. Обычный трафик копируется и направляется как рабочим, так и защитным транспортным объектам с постоянным мостом в источнике защищенного домена. Трафик на рабочих и защитных транспортных объектах передается одновременно в приемник защищенного домена, где выбор между рабочим и защитным транспортными объектами осуществляется на основе некоторых заранее определенных критериев, таких как индикация неисправности сервера. unidirectional-1-plus-1 – однонаправленный APS.

	Команда `mode unidirectional-1-plus-1 tx-aps` включает передачу блоков APS PDUs. PS даже в однонаправленном режиме 1+1. Прием APS PDU в этом режиме используются только в информационных целях.
`Level <0-7>`	Установка уровня MD / MEG, используемый в L-APS PDU. По умолчанию 0.
`Vlan <vlan_id>`	Установка идентификатора VLAN, используемого в L-APS PDU. Команда `vlan untagged` – не вставлять тег VLAN в PDU LAPS
`vlan <vlan_id> pcp <0-7>`	Настройка PCP (приоритет) (по умолчанию 7). Значение PCP, используемое в теге VLAN, если L-APS PDU не является немаркированным. Должно быть значение в диапазоне 0–7.
`Smac <mac_ucast>`	Установка MAC-адреса источника, используемый в PDU L-APS. Адрес должен быть одноадресным. Если все нули, будет использоваться MAC-адрес порта коммутатора.

`Revertive`
 	
`no revertive`
	Включение реверсивного режима, то есть трафик переключается обратно на рабочий порт после устранения условий, вызывающих переключение. В случае сброса команды (например, принудительное переключение) это происходит немедленно. В случае устранения дефекта это обычно происходит по истечении таймера WTR (ожидания восстановления).
	
	Режим восстановления порта не является реверсивным, и трафику разрешается оставаться на защищенном порте после устранения причины переключения.

`wait-to-restore <1-720>`	Настройка ожидания перед восстановлением рабочего порта после устранения неисправности. Допустимый диапазон 1–720
`hold-off-time <0-10000>`	Установка таймера задержки. Когда возникает новый (или более серьезный) дефект, запускается таймер задержки, и о событии будет сообщено после истечения таймера. Время удержания измеряется в миллисекундах, а допустимые значения находятся в диапазоне от 0 до 10000 . По умолчанию 0, что означает немедленное

	сообщение о дефекте.
admin-state { disable | enable}	Изменение состояния экземпляра APS (выключено/включено)

2.2.38 ERPS

ERPS - сетевой протокол, использующийся для исключения образования колец в топологии. Может быть заменой семейству протоколов **STP**.

Команда	Описание
Глобальные настройки	
Erps <1-64>	Создание экземпляра ERPS
rpl {neighbor | owner} {port0 | port1}	Выбор режима кольцевой защиты и кольцевого порта
Version {v1 | v2}	Выбор версии протокола ERPS
ring-type {interconnected-sub-ring | major | sub-ring}	Выбор типа кольца.
ring-type sub-ring	Выбор режима подкольцо При вводе дополнительной команды virtual-channel – включает виртуальный канал R-APS, то есть PDU R-APS не пересылаются между кольцевым портом, если один конец заблокирован
ring-type interconnected-sub-ring connected-ring <1-64>	Выбор режима взаимосвязанного подкольца, которое имеет только один кольцевой порт (порт 0), но подключается к главному кольцу. <1-64> - Номер экземпляра ERPS подключенного кольца Дополнительная команда propagate-topology-change - Управляет тем, должно ли кольцо, на которое ссылается экземпляр Interconnect, распространять R-APS для PDU всякий раз, когда изменяется топология этого под-кольца. При вводе команды virtual-channel - PDU R-APS передаются по подключенному кольцу, к которому подключается это под-кольцо
{port0 | port1} interface GigabitEthernet <port_type_id>	Назначение интерфейса кольцевому порту 0
{port0 | port1} sf-trigger link	Установка в качестве триггера сбоя сигнала состояние соединения
{port0 | port1} sf-trigger mep domain <kword1-15> service <kword1-15> mep-id <1-8191>	В качестве триггера используется mep. Требуется ввод domain service mep-id, относящиеся к экземпляру MEP, который должен представлять рабочий поток. Выбранный экземпляр MEP может не существовать при настройке этого APS.

ring-id <1-239>	Настройка идентификатора кольца. Идентификатор кольца используется - вместе с управляющей VLAN - для идентификации блоков PDU R-APS как принадлежащих определенному кольцу.
node-id <mac_ucast>	Настройка идентификатора узла. Идентификатор узла используется внутри конкретного PDU R-APS для уникальной идентификации этого узла (коммутатора) в кольце.
Level <0-7>	Установка уровня MD / MEG
control-vlan <vlan_id>	Установка VLAN, по которой блоки PDU R-APS передаются и принимаются на кольцевых портах.
control-vlan <vlan_id> pcp <0-7>	Установка значения PCP, используемое в теге VLAN PDU R-APS.
revertive	Включение режима возврата. Восстановление значений по умолчанию после истечения таймера ожидания восстановления.
guard-time <0-2000>	Установка таймера защиты.
wait-to-restore <1-720>	Установка времени ожидания восстановления в секундах. Допустимый диапазон 1–720 сек. Используется только в реверсивном режиме
hold-off-time <0-10000>	Установка таймера задержки. Когда возникает новый (или более серьезный) дефект, запускается таймер задержки, и о событии будет сообщено после истечения таймера. Время удержания измеряется в миллисекундах, а допустимые значения находятся в диапазоне от 0 до 10000. По умолчанию 0, что означает немедленное сообщение о дефекте.
admin-state { disable | enable}	Изменение состояния экземпляра ERPS (выключено/включено)
protected-vlans <vlan_list>	Указание VLAN, защищенные этим экземпляром кольца. По крайней мере, одна VLAN должна быть защищена.
rpl {neighbor | owner} { port0 | port1}	Настройка режима rpl Neighbor - этот коммутатор является соседом RPL Owner - этот коммутатор является владельцем RPL В обоих режимах требуется указать кольцевой порт.

2.2.39 Spanning Tree

При некоторых услугах, предоставляемых по сети необходимо, чтобы соединения были всегда включены – это гарантирует конечным пользователям выполнение требующихся им операций в режиме «онлайн», которые не должны прерываться неожиданными разрывами соединений. В таких обстоятельствах, для предотвращения разрывов соединений устанавливается множество активных маршрутов между узлами сети. Однако, наличие множества соединяющихся друг с другом маршрутов увеличивает вероятность образования петель (мостов), которые делают сеть нестабильной, а в наихудшем случае – неработоспособной. Например, таблица MAC-адресов, используемая коммутатором или мостом, может отказать вследствие того, что одни и те же MAC-адреса (и следовательно – одни и те же хосты сети) видны на множестве портов. Во-вторых, может произойти широковещательный шторм. Он обусловлен передачей широковещательных пакетов между коммутаторами по бесконечной петле. Широковещательный шторм может захватить все доступные ресурсы CPU и всю полосу пропускания. Для решения проблем, связанных с мостами, протокол STP допускает сети, включающие резервные линии, которые обеспечивают автоматические резервные маршруты в том случае, если отказывает активная линия, при этом не возникает опасности образования петель и не требуется вручную включать или отключать резервные линии. Протокол STP (Spanning Tree Protocol) определен в стандарте IEEE Standard 802.1s. Он позволяет создать топологию в смешанной сети с подключенными мостами 2-го уровня (в типичном случае - Ethernet-коммутаторами) и отключать линии, не являющиеся частью дерева, оставляя один активный маршрут между двумя любыми узлами сети. Для обеспечения быстрой сходимости после изменения топологии сети, введен протокол, являющийся развитием IEEE Standard 802.1s - RSTP (Rapid Spanning Tree Protocol (IEEE 802.1w)). Протокол RSTP – это улучшенный STP, поэтому эти протоколы имеют сходные основные характеристики. Важно, что создается эффект каскадного соединения – начиная с корневого моста, от которого каждый назначенный (некорневой) мост предлагает своим соседям определить – возможен ли быстрый переход. Это является одним из основных элементов, которые обеспечивают ускоренную сходимость RSTP по сравнению с STP. Другим расширением RSTP является IEEE 802.1s – MSTP (Multiple Spanning Tree protocol), который позволяет различным сетям VLAN использовать отдельные копии протокола. В отличие от STP и RSTP, MSTP устраняет необходимость иметь различные STP для каждой VLAN. Поэтому в больших сетевых средах, в которых эксплуатируется множество VLAN, MSTP может оказаться полезнее, чем традиционно используемый STP.

Команда	Описание
Глобальные настройки	
`spanning-tree mode {mstp | rstp | stp}`	Выбор версии протокола
`spanning-tree mst forward-time <4-30>`	Установка времени, проведенное в каждом из состояний – Listening (Прослушивание) и Learning (Обучение) до перехода в состояние Forwarding (Передача пакетов). Данная задержка возникает, когда в сеть включается новый мост. Допустимые

	значения: от 4 до 30 секунд
spanning-tree mst max-age <6-40>	Настройка времени ожидания. Если другой коммутатор не пошлет конфигурационный пакет в течение заданного периода времени, он считается отключенным. Допустимый диапазон значений: от 6 до 40 секунд, значение Max Age должно быть меньше или равно (Forward Delay-1)*2.
spanning-tree mst max-hops <6-40>	Настройка максимального числа участков между коммутаторами, после прохождения которых, пакет BPDU будет отброшен. При прохождении каждого моста пакетом BPDU, значение счетчика уменьшается на единицу. Когда счетчик участков маршрута станет равным нулю, пакет BPDU будет отброшен. По умолчанию число участков равно 20. Диапазон допустимых значений 6 – 40.
spanning-tree transmit hold-count <1-10>	Установка числа пакетов BPDU, посылаемых портом моста в секунду. Когда это значение превышено, передача следующего пакета BPDU будет задержана. По умолчанию задано 6 секунд. Допустимый диапазон значений: от 1 до 10. Пожалуйста, имейте в виду, что при увеличении этого значения может значительно возрасти загрузка CPU; при уменьшении значения замедляется сходимость алгоритма. 78 Рекомендуется оставить для Transmit Hold Count значение, заданное по умолчанию.
spanning-tree edge bpdu-filter	Включение фильтрации BPDU на граничном порту. Целью фильтрации пакетов BPDU на порту является предотвращение отправки с коммутатора кадров BPDU на порты, которые подключены к конечным устройствам.
spanning-tree edge bpdu-guard	Включение защиты BPDU на граничном порту. Граничные порты обычно напрямую подключены к ПК, файл-серверам или принтерам. Поэтому граничные порты сконфигурированы таким образом, чтобы обеспечивалось быстрое изменение состояния. В нормальных ситуациях, граничные порты не должны принимать конфигурационные BPDU. Однако, если они принимают их, то вероятно, вследствие атак злоумышленников или неправильных

	настроек. Когда граничные порты принимают конфигурационные BPDU, они будут автоматически переключены в состояние неграничных портов и запустится процесс вычисления новой топологии STP. В связи с этим, для защиты устройства от атак злоумышленников применяется BPDU guard. Если граничные порты приняли конфигурационные BPDU, когда эта функция включена, то STP отключит те из них, которые приняли конфигурационные BPDU. По истечении периода времени восстановления эти выключенные порты вновь будут включены.
`spanning-tree recovery interval <30-86400>`	Включение восстановления порта после ошибки. И установка времени, которое должно пройти до того момента, когда порт, выключенный из-за ошибки, будет включен вновь. Допустимый диапазон значений от 30 до 86400 секунд.
MSTI	
`spanning-tree mst name <word32> revision <0-65535>`	Настройка имени и номера версии для MSTI. По умолчанию используется MAC-адрес коммутатора. Максимальная длина 32 символа. Для того, чтобы совместно использовать STP для MSTI, мосты должны иметь одинаковые имена конфигураций и номера версий конфигураций.
`spanning-tree mst <0-31> vlan <vlan_list>`	Указание номера сетей VLAN, которые будут привязаны к MSTI. Можно ввести как одну VLAN, так и диапазон номеров VLAN. Номера VLAN можно отделять запятыми и использовать тире для указания диапазона VLAN. (Пример: 2,5,20-40). Для неиспользуемых MSTI оставьте поле пустым.
`spanning-tree mst <0-31> priority <0-61440>`	Установка приоритета. Приоритет моста используется при выборе корневого устройства, корневого порта и назначенного порта. Устройство с наивысшим приоритетом становится корневым устройством. Однако, если все устройства имеют одинаковый приоритет, корневым устройством станет устройство с наименьшим MAC-адресом. Имейте в виду, что чем меньше численное значение, тем выше приоритет. Идентификатор моста формируется конкатенацией следующего: приоритет моста плюс номер

	копии MSTI, конкатенированный с 6-байтным MAC-адресом коммутатора.
Настройка портов	
`interface GigabitEthernet <port_type_list>`	Выбор портов

`spanning-tree`
 	
`no spanning-tree`
	Включает функцию STP
	
	Выключает функцию STP

`spanning-tree mst <0-31> cost { <1-200000000> | auto}`	Установка стоимости маршрута, используется для определения наилучшего маршрута между устройствами. Если выбран режим работы “Auto” (Автоматически), при определении стоимости маршрута система автоматически определяет скорость и режим дуплекса. Возможно ввести значение. Допустимые значения: от 1 до 200000000. Пожалуйста, имейте в виду, что стоимость маршрута имеет более высокий приоритет, чем приоритет порта.
`spanning-tree mst <0-31> port-priority <0-240>`	Установка приоритета порта

`spanning-tree edge`
 	
`no spanning-tree edge`
	Установка границ администрирования. Если интерфейс подключен к оконечным узлам, то на интерфейсе можно указать “Edge” (Граница).
	
	Отмена команды

`spanning-tree auto-edge`
 	
`no spanning-tree auto-edge`
	Включение автоматического определения границы сети. Когда функция включена, порт автоматически определяет границу сети при приеме BPDU.
	
	Выключение автоматического определения границы сети.

`spanning-tree restricted-role`	Включение ограниченной роли. Если включено, порт не будет выбран в качестве корневого для CIST или любого MSTI даже тогда, когда он имеет наилучший приоритет STP.
`spanning-tree restricted-tcn`	Включение ограниченного TCN. Если включено, порт не будет распространять принятые уведомления об изменении топологии и сами изменения топологии на другие порты.
`spanning-tree bpdu-guard`	Включение функции защиты портов от приема BPDU. Позволяет предотвратить петли путем выключения порта при приеме BPDU вместо помещения его в состояние discarding. Если включено, порт

No spanning-tree bpdu-guard	выключится до тех пор, пока не примет правильный BPDU. Выключение функции защиты портов от приема BPDU
spanning-tree link-type {auto | point-to-point | shared}	Выбор типа линии, подключенной к интерфейсу: auto - Коммутатор автоматически определит, какой интерфейс подключен - либо линия точка-точка либо разделяемая среда. point-to-point - Установка соединения точка-точка. shared - Установка соединения разделяемой среды.

2.2.40 POE

Power over Ethernet (PoE) — технология, позволяющая передавать удалённому устройству электрическую энергию вместе с данными через стандартную **витую пару** в сети **Ethernet**. Данная технология предназначается для **IP-телефонии**, точек доступа беспроводных сетей, **IP-камер**, сетевых концентраторов и других устройств, к которым нежелательно или невозможно проводить отдельный электрический кабель.

Команда	Описание
Глобальные настройки	
poe supply <0-460>	Настройка максимальной мощности, которую может обеспечить источник питания.
poe capacitor-detect no poe capacitor-detect	Включение функции capacitor-detect Выключение функции capacitor-detect
Настройка портов	
interface GigabitEthernet <port_type_list>	Выбор портов
poe mode {plus | standard}	Выбор режима poe для порта Plus - включает PoE PoE IEEE 802.3at с поддержкой IEEE 802.3af Standard - включает режим соответствия PoE IEEE 802.3af
poe priority {critical | high | low}	Установка приоритета. Существует три уровня приоритета мощности: низкий, высокий и критический. Приоритет используется в том случае,

	когда удаленным устройствам требуется больше энергии, чем может обеспечить источник питания. В этом случае порт с самым низким приоритетом будет отключен, начиная с порта с самым высоким номером порта.

`poe lldp`
 	
`no poe lldp`
	Включение обработки параметров PoE, полученных через LLDP.
	
	Отключение обработки
	
	протокол LLDP настраивается отдельно, а передачу информации PoE через LLDP можно настроить командой `lldp med transmit-tlv poe`.

2.2.41 SyncE

Команда	Описание
Глобальные настройки	
`network-clock clk-source <1-2> nominate ptp <0-3>`	Выбор источника синхронизации `<1-2>` – экземпляр источника `ptp <0-3>` - выбор порта для источника синхронизации.
`network-clock clk-source <1-2> priority <0-1>`	Назначение приоритета для источника синхронизации. Наименьшее число (0) - самый высокий приоритет. Если два источника синхронизации имеют одинаковый приоритет, наименьший номер источника синхронизации получает наивысший приоритет в процессе выбора часов.
`network-clock clk-source <1-2> ssm-overwrite {dnu | eec1 | prc | ssua | ssub}`	Выбираемый уровень качества источника синхронизации (QL) для перезаписи любого QL, полученного в SSM . Если QL не получен в SSM (SSM не включен на этом порту), QL перезаписи SSM используется, как если бы он был получен. Для SSM Overwrite может быть установлено значение QL_NONE, что указывает на то, что источник синхронизации не имеет какого-либо известного качества (самое низкое по сравнению с источником синхронизации с известным качеством)

2.2.42 Selective QinQ

Selective QinQ - функции, позволяющая тегировать пакеты разным внешним тэгом VLAN в зависимости от разного внутреннего тэга VLAN в соответствии с требованиями пользователя.

Команда	Описание
Глобальные настройки	
`evc vce add vce-id <int> port-no <int> vid <int> new-vid <int>`	Создание записи, где: `vce-id <int>` - номер записи `port-no <int>` - порядковый номер порта (начиная с 0) `vid <int>` - значение outer tag VID во фрейме приходящем на UNI порт (порт, к которому подключается пользовательское оборудование.), для которого будет активна эта VCE запись `new-vid <int>` - новое значение VID для фрейма, которое будет добавлено при отсылке через NNI порт (порт в направлении ядра сети)
`evc vce del vce-id <int>`	Удаление соответствующей записи
Настройка портов	
`interface GigabitEthernet <port_type_list>`	Выбор портов для настройки
`switchport mode {access | hybrid | trunk}`	В зависимости от ваших требований настройте режим работы порта.

`switchport trunk allowed vlan <vlan_id>`
или
`switchport hybrid native vlan <vlan_id>`
	В соответствии с режимом порта, добавьте необходимые VLAN в соответствии с записями VCE.

2.2.43 Обновление ПО и автоматическая конфигурация.

Коммутатор имеет возможность автоматической конфигурации и обновления ПО через DHCP (66,67 опции)

Коммутатор загрузит конфигурацию или образ ПО только в том случае если startup и running config будут равны default config.

Важно, в 67опции передается имя файла конфигурации или имя файла прошивки. Имена файлов конфигурации и прошивки в обязательном порядке должны начинаться с config_ и image_ соответственно. Имя файла прошивки необходимо указывать с расширением, например «image_istax.itb».

Пример настройки DHCP-сервера:

subnet 192.168.102.0 netmask 255.255.255.0 {

range 192.168.102.10 192.168.102.20;

default-lease-time 60;

max-lease-time 120;

option routers 192.168.102.1;

}

#option 66

option tftp-server-name "192.168.102.1";

#option 67

option bootfile-name "config_nts25";

2.2.44 Конфигурация PPPoE Intermediate Agent.

Команда	Описание
Глобальные настройки	
`pppoe intermediate-agent`	Включить фунцию PPPoE Intermediate Agent
`no pppoe intermediate-agent`	Отключить фунцию PPPoE Intermediate Agent
`pppoe intermediate-agent delimiter <word5>`	Задать разделитель
`pppoe intermediate-agent type self-defined circuit-id <line64>`	Задать собственный формат circuit-id
`pppoe intermediate-agent type self-defined remote-id <line64> / raw-mac`	Задать собственный формат remote-id или передавать mac
`pppoe intermediate-agent type tr-101 circuit-id identifier-`	Настроить добавляемые поля circuit-id формата tr-101. pv - порт и vlan, sp - слот и

`string <word32> option (pv sp spv sv) delimiter <word5>`	порт, spv - слот порт и vlan, sv - слот и vlan. Задать разделитель
Настройка портов	

`pppoe intermediate-agent`
 	
`no pppoe intermediate-agent`
	Включить фунцию PPPoE Intermediate Agent
	
	Отключить фунцию PPPoE Intermediate Agent,

`pppoe intermediate-agent trust`
 	
`no pppoe intermediate-agent trust`
	Назначить порт в качестве доверенного
	
	Назначить порт в качестве недоверенного

`pppoe intermediate-agent vendor-tag strip`
 	
`no pppoe intermediate-agent vendor-tag strip`
	Включить функцию снятия тега вендора на порту
	
	Отключить функцию снятия тега вендора на порту

`pppoe intermediate-agent circuit-id <line64>`	Задать строку circuit-id, для добавления на порту
`pppoe intermediate-agent remote-id <line64> raw-mac`	Задать строку или mac remote-id, для добавления на порту

3 Web-интерфейс

Рис. 3.1 – Web-интерфейс

Для удобства навигации все команды разделены на четыре основные группы:

• configuration – конфигурация;

• monitor – мониторинг;

• diagnostics – диагностика;

• maintenance – обслуживание.

3.1 Основные команды управления настройками

Auto-refresh ☐ - Включить/выключить автоматическое обновление параметров;

Refresh - Обновить параметры;

Save - Сохранить введенные значения;

Reset - Сбросить введенные значения;

 - Update – Обновление прошивки коммутатора;

 - Home – Отображает стартовую страницу мониторинга;

 - Logout – Смена пользователя;

 - Show Help – Показать справку.

3.2 Конфигурация.

Вкладка конфигурации (Configuration) сгруппирована по названиям протоколов и используемым настройкам (Рис. 3.2).

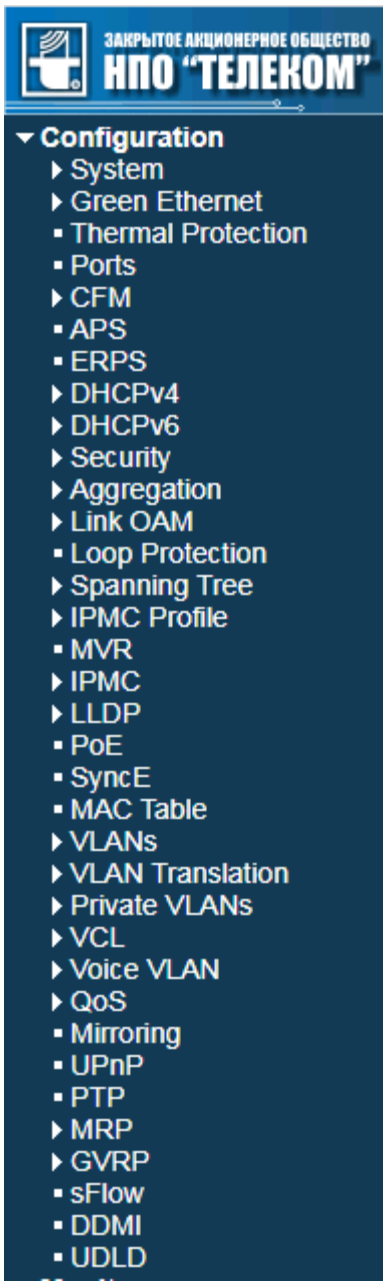


Рис. 3.2 – Вкладка Configuration

3.2.1 System. Системные настройки

Конфигурация системной информации (System Information Configuration) (Рис. 3.3) (Табл. 3.1). Позволяет задать информацию о коммутаторе в соответствии с предпочтениями пользователя.

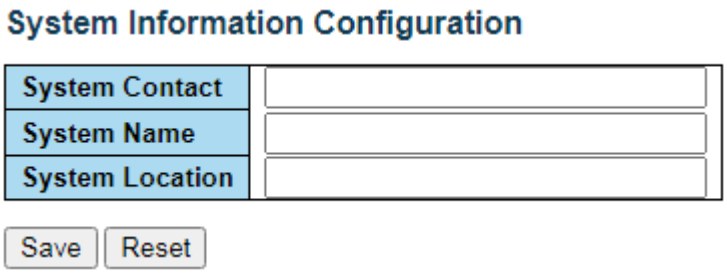


Рис. 3.3 – Вкладка System Information Configuration

Таблица 3.1 - Вкладка System Information Configuration

System Contact	Контактная информация. В этом поле можно указать контактную информацию. Имя, фамилия лица, ответственного за систему, адрес электронной почты или другие сведения.
System Name	Имя системы. Имя хоста для данного устройства. Можно использовать (A-Z), (a-z), (0-9), (-). Применение символа «пробел» недопустимо. Первый символ должен быть буквой (прописной или строчной). Первый и последний символы не должны быть знаком минус. Допустимая длина строки 0~255.
System Location	Расположение системы, физическое расположение этого устройства (например: garderob, etazh3 и т.п.). Допустимая длина строки от 0 до 255.

Конфигурация IP (IP Configuration) (Рис. 3.4) (Табл. 3.2).

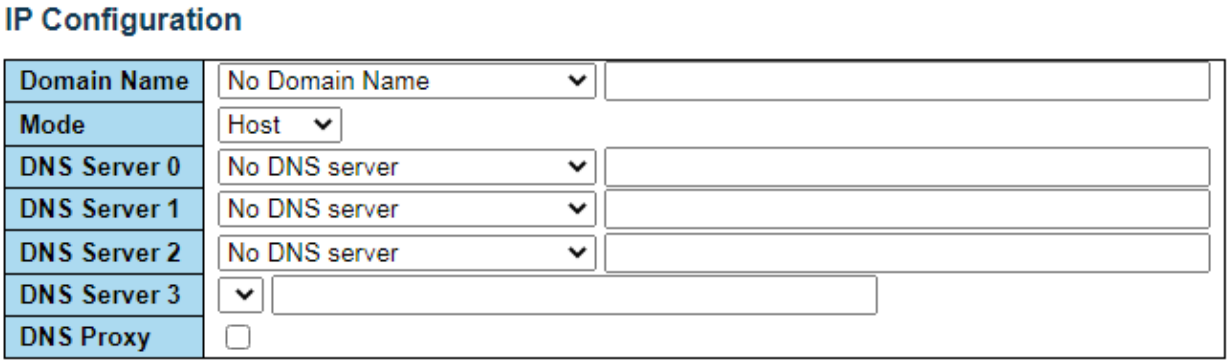


Рис. 3.4 – IP Configuration

Таблица 3.2 - IP Configuration

Domain Name	Строка имени локального домена, в котором находится устройство. Большинство запросов для имен в этом домене могут использовать короткие имена относительно локального домена. Затем система добавляет доменное имя в качестве суффикса к неквалифицированным именам. Например, если доменное имя задано как «example.com» и вы укажете пункт назначения PING по неквалифицированному имени как «test», тогда система определит имя как «test.example.com». Поддерживаются следующие режимы: No Domain Name - Доменное имя использоваться не

	будет. `Configured Domain Name` –Явно укажите имя локального домена. Убедитесь, что настроенное доменное имя соответствует домену вашей организации. `From any DHCPv6 interfaces` – Будет использоваться первое доменное имя, предложенное при аренде DHCPv6 интерфейсу с поддержкой DHCPv6. `From this DHCPv6 interface` – Укажите, из какого интерфейса с поддержкой DHCPv6 следует отдавать предпочтение предоставленному доменному имени.
Mode	В списке можно выбрать, как будет функционировать стек протоколов IP – как хост или как маршрутизатор. В режиме Host (Хост) IP–трафик между интерфейсами не может быть маршрутизирован. В режиме Router (Маршрутизатор), трафик может маршрутизироваться между всеми интерфейсами. При настройке данного устройства для множества VLAN, следует выбрать режим Router. Режим 21 Host выбран по умолчанию.
DNS Server 0..3	Данная настройка позволяет задать сервер доменных имен (DNS). Режим работы: • From any DHCP interfaces (Из любых интерфейсов DHCP): Будет использован IP-адрес первого DNSсервера, полученный от DHCP, при включенной поддержки DHCP на интерфейсе. • No DNS server (Без DNS-сервера): DNS-сервер использоваться не будет. • Configured (Заданный IP-адрес): Будет использован IP-адрес DNS-сервера, введенный в десятичном формате с точкой. • From this DHCP interface (Из данного интерфейса DHCP): Можно указать из какого интерфейса с активированным DHCP-протоколом предпочтительно выбрать DNS-сервер.
DNS Proxy	Прокси-сервер доменных имен. Когда активирован проксисервер DNS, система будет отправлять запросы DNS на текущий настроенный DNS-сервер, при этом ответы будут отправляться, как DNS-разрешения клиентским устройствам сети.

IP Интерфейсы (IP Interfaces) (Рис. 3.5) (Табл. 3.3).

Рис. 3.5 – IP Interfaces

Таблица 3.3 - IP Configuration

Delete			Выберите, чтобы удалить текущий IP-интерфейс.
VLAN			В этом поле указан номер VLAN, ассоциированный с IP-интерфейсом. Доступ к IP-интерфейсу будут иметь только порты с данным номером VLAN. Это поле доступно для ввода только при создании нового интерфейса
DHCPv4	Enable		Включить клиент DHCP. Если этот параметр включен, система настроит адрес IPv4 и маску интерфейса с использованием протокола DHCP. Клиент DHCP объявит сконфигурированное имя системы как имя хоста (hostname), чтобы обеспечить поиск DNS.
	Hostname		Имя хоста DHCP-клиента. Если клиент DHCPv4 включен, настроенное имя хоста будет использоваться в поле DHCP option 12. Если это значение представляет собой пустую строку, в поле используется настроенное имя системы плюс последние три байта системных MAC-адресов в качестве имени хоста.
	Fallback		Опция IPv4 DHCP Fallback определяет как долго (в 22 секундах) коммутатор будет ожидать ответа от DHCPсервера, прежде чем он начнет использовать настроенный статический IP-адрес. Допустимые значения: от 0 до 4294967295 секунд. Нулевое значение отключает механизм резервных действий, таким образом, что коммутатор будет ожидать ответа до тех пор, пока не получит
	Current Lease		Показывает текущий адрес интерфейса, предоставленный сервером DHCP.
	Client ID	Type	Тип идентификатора клиента DHCP IPv4. Выберите, какой из трех типов ниже, то есть IfMac, ASCII или HEX, должен использоваться для идентификатора клиента
		IfMac	Идентификатор клиента DHCP IPv4 IfMac. Когда клиент DHCPv4 включен и тип идентификатора клиента - ifmac, аппаратный MAC-адрес настроенного интерфейса будет использоваться в поле DHCP option 61.
		ASCII	Идентификатор клиента DHCP IPv4 ASCII. Когда клиент DHCPv4 включен и тип идентификатора клиента - ascii, строка ASCII будет использоваться в поле DHCP option 61.
		HEX	Идентификатор клиента DHCP IPv4 HEX. Когда клиент DHCPv4 включен и тип идентификатора клиента «HEX», шестнадцатеричное значение будет использоваться в поле DHCP option 61.
IPv4	Address		IP v4-адрес интерфейса. Если DHCP включен, то это поле не используется. Поле может оставаться пустым, если не требуется IP v4.

	Mask Length	Маска сети IP v4. Если протокол DHCP активирован, это поле не используется. Поле можно оставить пустым.
	Pri/Sec	Основной/Дополнительный ip адрес
IPv6	Address	IPv6-адрес интерфейса. Поле можно оставить пустым
	Mask Length	Маска сети IP v6. Поле можно оставить пустым.
DHCP v6	Enable	Включить клиент DHCP. Если этот параметр включен, система настроит адрес IP v6 и маску интерфейса с использованием протокола DHCP.
	Rapid Commit	Позволяет серверу быстро фиксировать контейнер или глобальную группу. По умолчанию эта опция не задана и считается отключенной.
	Current Lease	Показывает текущий адрес интерфейса, предоставленный сервером DHCP.
CoS		Позволяет задать маркировку 802.1p исходящего трафика с интерфейса управления.

IP-маршруты (IP Routers) (Рис. 3.6) (Табл. 3.4).

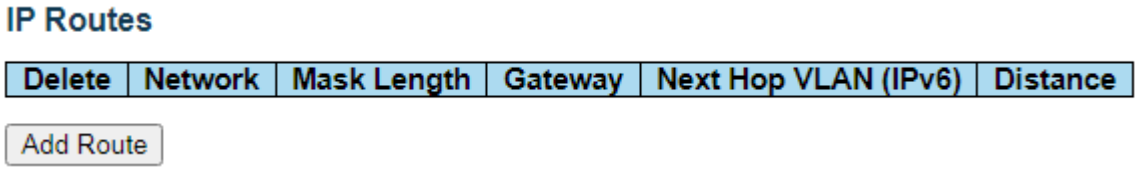


Рис. 3.6 – IP Route

Таблица 3.4 - IP Route

Delete	Удаление текущего маршрута
Network	Адрес сети назначения. Это IP-адрес сети назначения или IP-адрес хоста этого маршрута.
Mask Length	Маска сети. Это маска IP-адреса сети назначения или маска хоста.
Gateway	IP-адрес шлюза. Шлюз и сеть должны быть одного типа.
Next Hop VLAN	Идентификатор VLAN (VID) конкретного интерфейса IPv6, связанного со шлюзом. Данный VID находится в диапазоне от 1 до 4094 и будет работать только тогда, когда соответствующий интерфейс IPv6 действителен. Если IP-адрес шлюза IPv6 локальный, он должен указать VLAN следующего перехода для шлюза. Если IP-адрес шлюза IPv6 не локальный, система игнорирует VLAN

	следующего перехода для шлюза.
Distance	Значение расстояния в записи маршрута используется для предоставления маршрутизаторам информации о приоритете протоколов маршрутизации. Когда задействованы два или более разных протокола маршрутизации и имеют один и тот же пункт назначения, значение расстояния может использоваться для выбора наилучшего пути.

Кнопка Add Route предназначена для добавления новых маршрутов.

Конфигурация NTP (NTP Configuration) (Рис. 3.7) (Табл. 3.5)

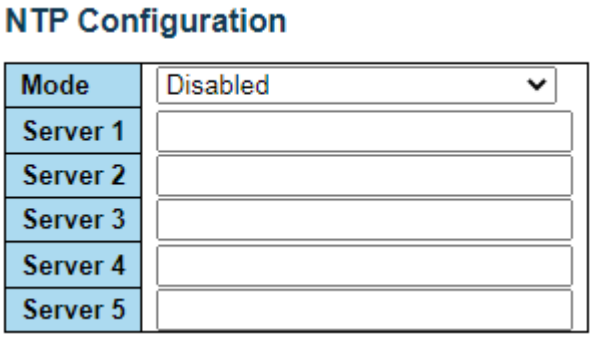


Рис. 3.7 – NTP

Таблица 3.5 - NTP

Mode	Режим работы NTP: включен/выключен
Server 1..5	IPv4 или IPv6-адрес NTP-сервера

Конфигурация часового пояса (Time Zone Configuration) (Рис. 3.8) (Табл. 3.6).

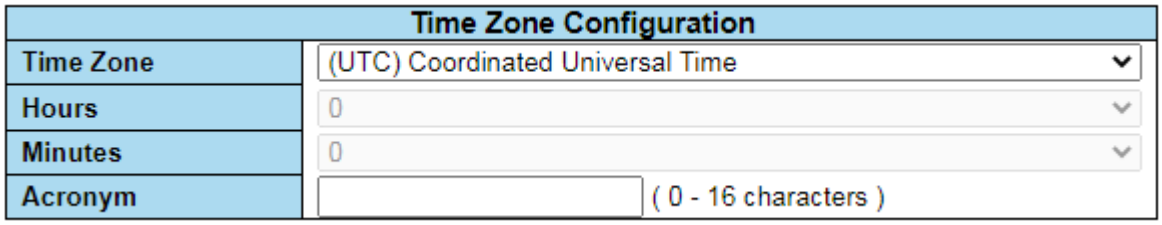


Рис. 3.8 – Конфигурация часового пояса

Таблица 4.6 - Конфигурация часового пояса

Time Zone	Выберите соответствующий часовой пояс из раскрывающегося списка

Acronym	Настраиваемый пользователем акроним для определения часового пояса (до 16 символов).

Конфигурация перехода на летнее время (Daylight Saving Time Configuration) (Рис. 3.9) (Табл. 3.7).

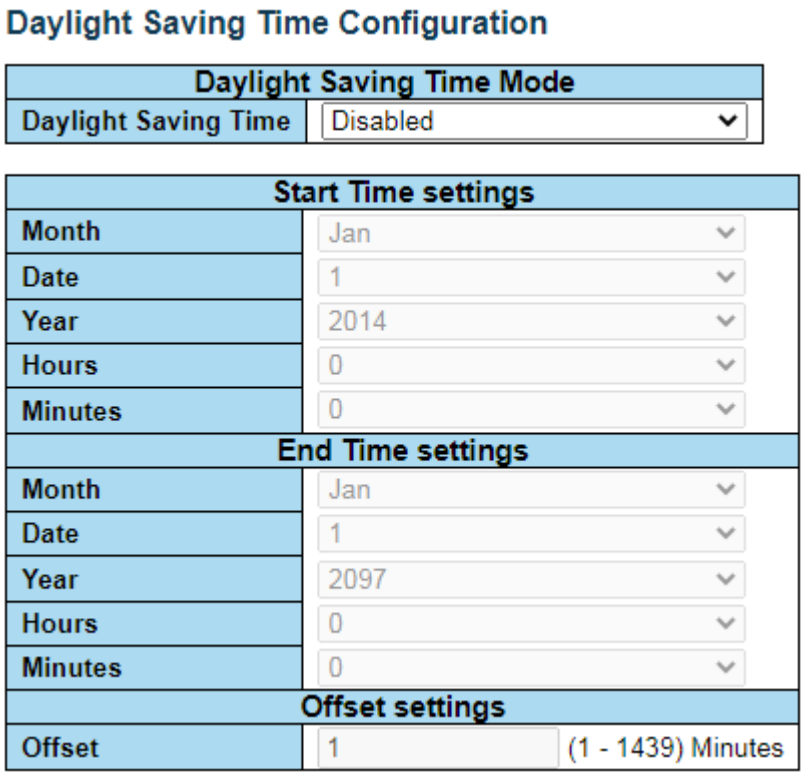


Рис. 3.9 – Конфигурация перехода на летнее время

Таблица 4.7 - Конфигурация часового пояса

Daylight Saving Time		Disabled (Отключено) – переход на летнее время отключен; Recurring (Повторяющийся) – повторять переход на летнее время каждый год; Non-Recurring (Единовременный) - переход на летнее время один раз
Start Time settings (Время начала действия)	Month	Месяц начала
	Date	Дата начала
	Year	Год начала
	Hours	Час начала
	Minutes	Минуты начала
End Time settings (Время окончания действия)	Month	Месяц конца
	Date	Дата конца
	Year	Год конца
	Hours	Час конца
	Minutes	Минуты конца
Offset settings		Введите количество минут для добавления в летнее время. (Диапазон: 1-1440)

Конфигурация журнала системных сообщений (System Log) (Рис. 3.10) (Табл. 3.8).

Syslog (системный журнал) — стандарт отправки и регистрации сообщений о происходящих в системе событиях (то есть создания логов), использующийся в компьютерных сетях, работающих по протоколу IP.

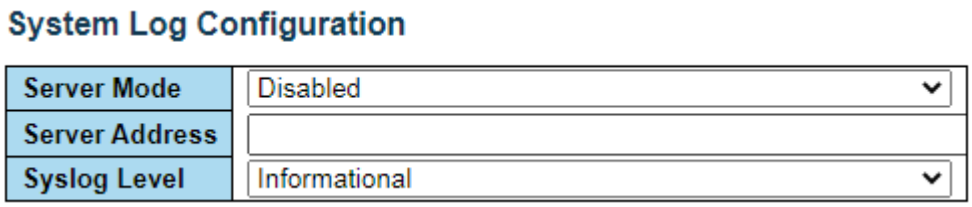


Рис. 3.10 – System Log

Таблица 3.8 - System Log

Server Mode	Режим работы сервера: Включен (Enabled)/Выключен (Disabled);
Server Address	IP v4 – адрес syslog-сервера, также можно указать host name;
Syslog Level	Укажите тип отправляемых сообщений. Возможные режимы: • Error (Ошибка) –отправлять только ошибки; • Warning (Предупреждение) – отправлять предупреждения и ошибки; • Notice (Уведомление) – отправлять уведомления, предупреждения и ошибки; • Informational (Информация) – отправлять информационные сообщения, уведомления, предупреждения и ошибки;

3.2.2 Green Ethernet. Настройка энергосбережения.

Настройка энергосбережения.

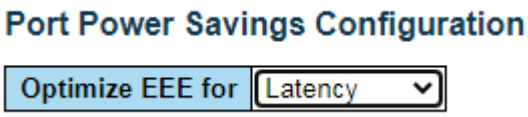


Рис. 3.11 – Port Power Savings Configuration

Таблица 3.9 - Port Power Savings Configuration

Optimize EEE for	Коммутатор может быть настроен на оптимизацию EEE для наилучшего энергосбережения (Power) или минимальной задержки трафика(Latency).

Конфигурация портов.

Port Configuration

				EEE Urgent Queues							
Port	ActiPHY	PerfectReach	EEE	1	2	3	4	5	6	7	8
*	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
3	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
4	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
5	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
9	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
10	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Рис. 3.12 – Port Configuration

Таблица 3.10 - Port Configuration

ActiPHY	Включение/выключение функции ActiPHY. ActiPHY снижает мощность порта при отсутствии связи. Порт включается на короткое время, чтобы определить, вставлен ли кабель.
PerfectReach	Включение/выключение функции PerfectReach. PerfectReach работает, определяя длину кабеля и снижая мощность для портов с короткими кабелями.
EEE	Включение/выключение EEE для порта коммутатора. Для максимальной экономии энергии схема не запускается сразу после того, как данные для передачи готовы для порта, а вместо этого ставится в очередь до тех пор, пока пакет данных не будет готов к передаче. Это приведет к некоторой задержке трафика.
EEE Urgent Queues	Настройка очередей. Установленные очереди активируют передачу кадров, как только данные станут доступны. В противном случае очередь отложит передачу до тех пор, пока не будет передана пачка кадров.

3.2.3 Thermal Protection Configuration. Настройка защиты от перегрева.

Эта страница позволяет пользователю проверить и настроить текущую настройку защиты от перегрева.

Когда температура превышает настроенную температуру тепловой защиты, порты отключаются, чтобы снизить энергопотребление. Можно распределить порты по разным группам(Рис 3.14). Каждой группе может быть задана температура (Рис 3.13), при которой соответствующие порты должны быть выключены.

Temperature settings for groups

Group	Temperature	
0	255	°C
1	255	°C
2	255	°C
3	255	°C

Рис. 3.13 – Настройка температуры

Port groups

Port	Group
*	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled

Рис. 3.14 – Группы портов

3.2.4 Конфигурация портов. Ports

Рис. 3.15 – Port Configuration

Таблица 3.11 - Port Configuration

Port		Номер порта
Description		
Link		Текущее состояние (Link): - наличие; - отсутствие;
Speed	Current	Отображает текущую скорость соединения;
	Configured	Установка скорости соединения. Отображаются только поддерживаемые скорости. Возможные варианты: • Disabled - отключить порт коммутатора; • Auto – автоматический режим, выбирается максимальная скорость, которая возможна при текущем соединении; • SFP_Auto_AMS – автоматический режим определения скорости SFP; • Скорости: 10Mbps HDX/10Mbps FDX/100Mbps HDX/100Mbps FDX/1Gbps FDX/ 2.5Gbps FDX/10Gbps FDX/100-FX/100-FX_AMS/1000- X/1000-X_AMS;
Adv Duplex	Fdx	При установленном режиме автоматического Hdx определения FDX/HDX, порт будет предлагать указанные режимы (FDX дуплекс) и (HDX полудуплекс) в качестве предпочтительных для порта, связанного по этому каналу устройства (если на нем также установлен автоматический режим);
	Hdx	
Adv speed	10M	При установленном режиме автоматического определения скорости, порт будет предлагать указанные скорости в качестве предпочтительных для порта, связанного по этому каналу устройства (если на нем также установлен автоматический режим);
	100M	
	1G	
	2.5G	
	5G	
	10G	
Flow	Enable	Управление потоком. В столбце Current Rx указано,

Control	Curr Rx Curr Tx	поддерживает ли порт паузы при приеме кадров. В столбце Current Tx указано, поддерживает ли порт паузы при передаче кадров. Настройки Rx и Tx определяются результатами последнего автосогласования параметров. Перед тем, как использовать управление потоком проверьте настройки в этих столбцах. Данная настройка связана также с выбранной скоростью Configured Speed.
PFC	Enable Priority	Установить приоритет (0-7) потока управления;
Maximum Frame Size		Максимальный размер фрейма для порта коммутатора, включая FCS;
Excessive Collision Mode		Режим работы при слишком большом числе столкновений пакетов: Данная настройка конфигурирует порт на установку режима передачи при столкновениях пакетов "Discard" (отбрасывание кадра после 16 столкновений – выбрано по умолчанию),
Frame Length Check		Включение/выключение проверки длины кадра. Если включена «проверка длины кадра», кадры с размером полезной нагрузки менее 1536 байтов отбрасываются, если поле EtherType / Length не соответствует фактической длине полезной нагрузки. Если «проверка длины кадра» отключена, кадры не отбрасываются из-за несоответствия длины кадра. Примечание. Счетчики отбрасывания не подсчитывают количество потерянных кадров из-за несоответствия длины кадра.

3.2.5 CFM Global Configuration

CFM Global Configuration

Sender Id TLV	None
Port Status TLV	Enable
Interface Status TLV	Disable
Organisation Specific TLV	Disable
Organisation Specific TLV OUI	000000
Organisation Specific TLV Subtype	0
Organisation Specific TLV Value	

Рис. 3.16 – CFM Global Configuration

Таблица 3.12 - Port Configuration

Sender Id TLV	Выбор идентификатора tlv: Chassis – идентификатор шасси(MAC-адрес) chassis-management - идентификатор шасси(MAC-адрес) и адрес управления (IPv4-адрес) management - адрес управления (IPv4-адрес) disable – исключить идентификатор tlv

Port Status TLV	Включение или выключение tlv для статуса порта
Interface Status TLV	Включение или выключение tlv для статуса интерфейса
Organisation Specific TLV	Включение или выключение TLV для конкретной организации
Organisation Specific TLV OUI	трехбайтовый OUI, передаваемый с TLV, зависящим от организации.
Organisation Specific TLV Subtype	подтип, передаваемый с TLV для конкретной организации. Может быть любым значением в диапазоне [0; 255]
Organisation Specific TLV Value	значение, передаваемое в TLV для конкретной организации. Значение представляет собой печатаемую строку символов длиной 0-63.

настройка домена CFM

CFM Domain Configuration

Delete	Domain	Format	Name	Level	TLV option select			
					Sender Id	Port Status	Interface Status	Org. Specific
*								
No entry exists								

Add New Entry

Рис. 3.17 – настройка домена CFM

Таблица 3.13 - настройка домена CFM

Delete		Кнопка удаления записи. Запись будет удалена при следующем сохранении.
Domain		Имя домена. Значение - это отдельное слово, начинающееся с буквенной буквы AZ или az длиной от 1 до 15.
Format		Выбор формата имени: None `String`
Name		Содержимое этого параметра зависит от значения параметра формата. Если формат None: Имя не используется, но за кадром будет установлены все нули. Этот формат обычно используется блоками PDU типа Y.1731. Если формат `String`: Имя должно содержать строку от 1 до 43 символов.
Level		Уровень этого домена. Допустимые значения ограничены 0–7.
TLV option select	Sender Id	Выбор идентификатора tlv Chassis – идентификатор шасси(MAC-адрес) chassismanage - идентификатор шасси(MAC-адрес) и адрес управления (IPv4-адрес)

		management - адрес управления (IPv4-адрес) none – исключить идентификатор tlv defer – применяются настройки глобальной конфигурации
	Port Status	Включение или выключение tlv для статуса порта Defer – применяются настройки глобальной конфигурации
	Interface Status	Включение или выключение tlv для статуса интерфейса Defer – применяются настройки глобальной конфигурации
	Org. Specific	disable - исключить TLV для конкретной организации Defer – применяются настройки глобальной конфигурации

CFM Service Configuration

CFM Service Configuration

Delete	Domain	Service	Format	Name	VLAN	CCM Interval	TLV option select			
							Sender Id	Port Status	Interface Status	Org. Specific
*										
No entry exists										

Add New Entry

Рис. 3.18 – CFM Service Configuration

Таблица 3.14 - CFM Service Configuration

Delete	Кнопка удаления записи. Запись будет удалена при следующем сохранении.
Domain	Имя домена, под которым находится эта Служба.
Service	Название службы. Значение - это отдельное слово, начинающееся с буквенной буквы AZ или az длиной от 1 до 15.
Format	Выбор формата имени службы. Это решает, как будет интерпретироваться значение параметра Name. Возможные значения: String Two Octets Y1731 ICC Y1731 ICC CC
Name	Содержимое этого параметра зависит от значения элемента Format. Помимо ограничений объяснить для каждого из них, применяется следующее в целом: Если формат домена none, размер не может превышать 45 байт. Если формат домена не none, размер не может превышать 44 байта. Если формат String, применяется следующее: длина должна быть в диапазоне [1; 44]. Содержание должно быть в диапазоне [32; 126] Если формат Two Octets , применяется следующее: Имя [0] и Имя [1] будут интерпретироваться как 8-разрядные целые числа без знака (допустим диапазон [0; 255]). Имя [0] будет помещено

		в PDU перед именем [1]. Оставшиеся доступные байты в имени использоваться не будут. Если формат Y1731 ICC, применяется следующее: длина должна быть 13. Содержимое должно быть в диапазоне [az, AZ, 0-9]. Y.1731 указывает, что это конкатенация ICC (кода оператора связи ITU) и UMC (уникального кода идентификатора MEG): ICC: 1-6 байтов UMC: 7-12 байтов В принципе UMC может принимать любое значение в диапазоне [1; 127], но этот API не позволяет указывать длину ICC, поэтому базовый код не знает, где заканчивается ICC и начинается UMC. Формат домена должен быть none. Если формат Y1731 ICC CC, применяется следующее: длина должна быть 15. Первые 2 символа (CC): должны быть среди [AZ] Следующие 1-6 символов (ICC): должны быть среди [az, AZ, 0-9] Следующие 7-12 символов (UMC): должно быть среди [az, AZ, 0-9]. В имени [3-7] может присутствовать ОДИН (косая черта). Формат домена должен быть none.
VLAN		Выбор MEP в сервисе Основной VID MA. VLAN, равный 0, означает, что все MEP, созданные в этом MA, будут созданы как MEP порта (интерфейсные MEP). На каждом интерфейсе может быть только одна портовая MEP. MEP данного порта может быть создана с тегами, если VLAN этой MEP не равна нулю.
CCM Interval		Настройка скорости CCM всех MEP, привязанных к этой услуге
TLV option select	Sender Id	Выбор идентификатора tlv Chassis – идентификатор шасси(MAC-адрес) chassismanage - идентификатор шасси(MAC-адрес) и адрес управления (IPv4-адрес) management - адрес управления (IPv4-адрес) none – исключить идентификатор tlv defer – применяются настройки глобальной конфигурации
	Port Status	Включение или выключение tlv для статуса порта Defer – применяются настройки глобальной конфигурации
	Interface Status	Включение или выключение tlv для статуса интерфейса Defer – применяются настройки глобальной конфигурации
	Org. Specific	disable - исключить TLV для конкретной организации Defer – применяются настройки глобальной конфигурации

CFM Mep Configuration

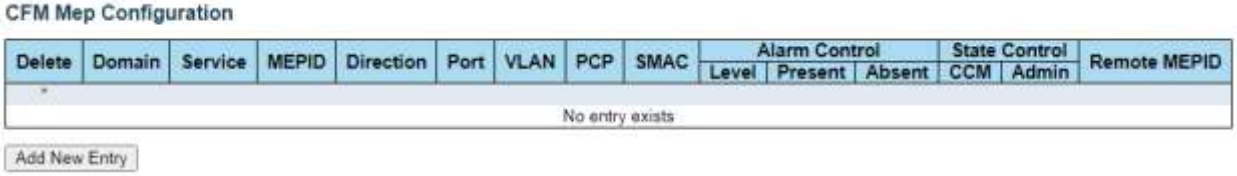


Рис. 3.19 – CFM Mep Configuration

Таблица 3.15 - CFM Mep Configuration

Delete		Кнопка удаления записи. Запись будет удалена при следующем сохранении.
Domain		Имя домена, в котором находится эта MEP.
Service		Имя сервиса, под которым находится данный MEP.
MEPID		Идентификатор этого MEP. Должно быть целым числом [1..8091]
Direction		Установите, является ли эта MEP восходящей или нисходящей.
Port		Порт, на котором находится эта MEP.
VLAN		Идентификатор VLAN. Используйте значение 0 для обозначения нетегированного трафика (подразумевается MEP порта).
PCP		Выберите значение PCP в теге VLAN PDU. Не используется без тегов.
SMAC		Установите MAC-адрес источника, который будет использоваться в блоках PDU CCM, исходящих от этой MEP. Адрес должен быть одноадресным. Формат: XX: XX: XX: XX: XX: XX. Если все нули, вместо него будет использоваться MAC-адрес порта коммутатора.
Alarm Control	Level	Установка уровня сигнализации. Если обнаружен дефект с приоритетом выше этого уровня, будет сгенерировано уведомление о неисправности. Допустимый диапазон: [1; 6], где 1 указывает, что любой дефект вызывает аварийный сигнал, а 6 означает, что никакой дефект не может вызвать аварийный сигнал.
	Present	Установка времени в миллисекундах, в течение которого должны присутствовать дефекты, прежде чем будет выдано уведомление о неисправности. По умолчанию 2500 мс.
	Absent	Установка времени в миллисекундах, в течение которого дефекты должны отсутствовать до сброса уведомления о неисправности. По умолчанию 10000 мс
State Control	CCM	Включение или отключение генерации сообщений проверки целостности (CCM)
	Admin	включить или отключить эту MEP. Когда эта MEP включена, она проверяет полученные / отсутствующие CCM и может вызывать дефекты.
Remote MEPID		Укажите удаленную MEP, от которой эта MEP, как ожидается, будет получать PDU CCM. Должно быть целым числом [0..8091], где 0 означает неопределенное. Значение Remote MEPID должно отличаться от значения MEPID.

3.2.6 автоматическое защитное переключение (APS)

APS - сетевой протокол канального уровня, предназначен для поддержки топологии, исключающей зацикливание трафика, и её перестроение в случае нарушений в кольцевых сетях Ethernet на первом-втором уровне сетевой модели OSI.

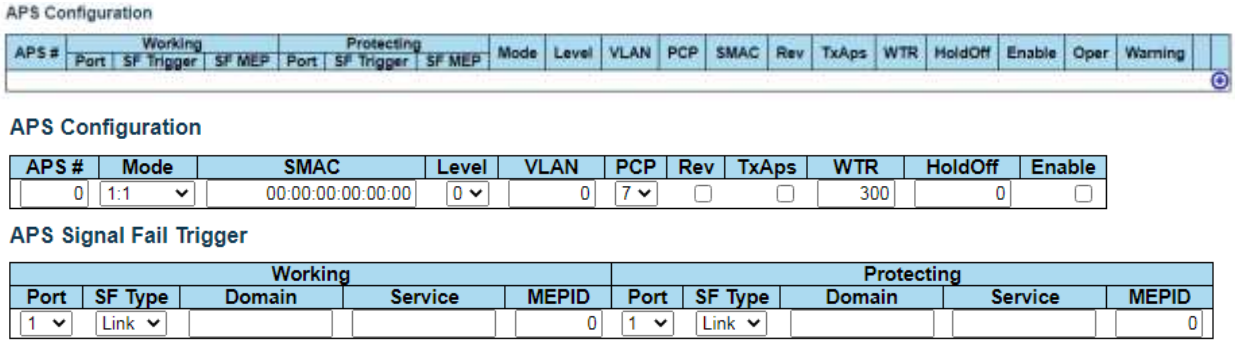


Рис. 3.20 – настройка автоматического защитного переключения

Таблица 3.16 - настройка автоматического защитного переключения

APS	Идентификатор APS. Максимальное количество создаваемых экземпляров APS - 10 . Щелкните ссылку, чтобы перейти на страницу экземпляра APS, вы можете сбрасывать счетчики и выдавать команды.
Mode	**1: 1 -** В линейной архитектуре защитной коммутации 1: 1 защитный транспортный объект выделен рабочему транспортному объекту. Однако нормальный трафик транспортируется либо на рабочем транспортном объекте, либо на защитном транспортном объекте, используя мост селектора в источнике защищенного домена. Селектор в приемнике защищенного домена выбирает объект, который несет нормальный трафик **1 + 1 Bi–** В линейной архитектуре защитной коммутации 1 + 1 для каждого рабочего транспортного объекта выделен защитный транспортный объект. Обычный трафик копируется и направляется как рабочим, так и защитным транспортным объектам с постоянным мостом в источнике защищенного домена. Трафик на рабочих и защитных транспортных объектах передается одновременно в приемник защищенного домена, где выбор между рабочим и защитным транспортными объектами осуществляется на основе некоторых заранее определенных критериев, таких как индикация неисправности сервера. **1 + 1 Uni**– однонаправленный APS.
SMAC	MAC-адрес источника, используемый в PDU L-APS. Адрес должен быть одноадресным. Если все нули, будет использоваться MAC-адрес порта коммутатора.
Level	Установка уровня MD / MEG, используемый в L-APS PDU. По

		умолчанию 0.
VLAN		Установка идентификатора VLAN, используемого в L-APS PDU. При VLAN 0 – не вставлять тег VLAN в PDU LAPS
PCP		Выбор значения PCP в теге VLAN PDU. Не используется без тегов.
Rev		Включение/выключение реверсивного режима, то есть трафик переключается обратно на рабочий порт после устранения условий, вызывающих переключение. В случае сброса команды (например, принудительное переключение) это происходит немедленно. В случае устранения дефекта это обычно происходит по истечении таймера WTR (ожидания восстановления).
TxAps		Выберите, будет ли этот конец передавать блоки PDU APS. Используется только для режима **1 + 1 Uni**– однонаправленный APS
WTR		Настройка ожидания перед восстановлением рабочего порта после устранения неисправности. Допустимый диапазон 1–720
HoldOff		Установка таймера задержки. Когда возникает новый (или более серьезный) дефект, запускается таймер задержки, и о событии будет сообщено после истечения таймера. Время удержания измеряется в миллисекундах, а допустимые значения находятся в диапазоне от 0 до 10000 . По умолчанию 0, что означает немедленное сообщение о дефекте.
Enable		Изменение состояния экземпляра APS (включено /выключено)
Working	Port	Выбор интерфейса в качестве рабочего порта
	SF Type Domain Service MEPID	Выбор триггера для сигнала ошибки LINK - В качестве триггера используется состояние порта MEP - В качестве триггера используется mep. Требуется ввод domain, service, mep-id, относящиеся к экземпляру MEP, который должен представлять рабочий поток. Выбранный экземпляр MEP может не существовать при настройке этого APS.
Protecting	Port	Назначение интерфейса в качестве защищенного порта
	SF Type Domain Service MEPID	Выбор триггера для сигнала ошибки LINK - В качестве триггера используется состояние порта MEP - В качестве триггера используется mep. Требуется ввод domain, service, mep-id, относящиеся к экземпляру MEP, который должен представлять рабочий поток. Выбранный экземпляр MEP может не существовать при настройке этого APS.

3.2.7 ERPS

ERPS - сетевой протокол, использующийся для исключения образования колец в топологии. Может быть заменой семейству протоколов **STP**.

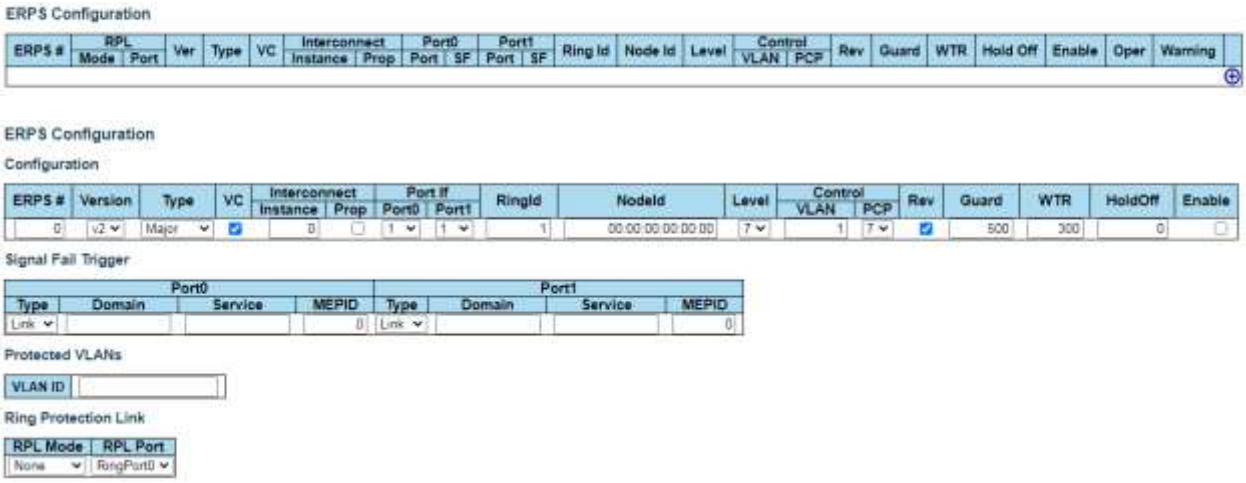


Рис. 3.21 – конфигурация ERPS

Таблица 3.17 - конфигурация ERPS

ERPS		Идентификатор ERPS. Допустимое значение от 1 до 64 .
Version		Версия протокола ERPS. Поддерживаются версии v1 и v2 .
Type		Тип кольца. Возможные значения: Major: основное кольцо ERPS Sub: Подкольцо ERPS InterSub: подкольцо ERPS на соединительном узле
VC		Включение/выключение виртуального канала R-APS, то есть PDU R-APS не пересылаются между кольцевым портом, если один конец заблокирован
Interconnect	Instance	идентификатор экземпляра кольца, к которому это подкольцо подключено.
	Prop	Определяет, должно ли кольцо, на которое ссылается Interconnect Instance, распространять PDU очистки R-APS всякий раз, когда изменяется топология этого подкольца.
Port If	Port0	Указание интерфейса используемого в качестве порта 0
	Port1	Указание интерфейса используемого в качестве порта 1
RingId		Идентификатор кольца. Используется - вместе с управляющей VLAN - для идентификации блоков PDU R-APS как принадлежащих определенному кольцу.
NodeId		ID узла. Используется внутри конкретного PDU R-APS для уникальной идентификации этого узла (коммутатора) в кольце.
Level		Установка уровня MD / MEG
Control	VLAN	VLAN, по которой блоки PDU R-APS передаются и принимаются на кольцевых портах.
	PCP	Значение PCP, используемое в теге VLAN PDU R-APS
Rev		Включение/выключение режима возврата. Восстановление значений по умолчанию после истечения таймера ожидания восстановления.

Guard		Время защиты в мс. Допустимый диапазон: 10 - 2000 мс.
WTR		Время ожидания восстановления в секундах. Допустимый диапазон 1 - 720 сек.
HoldOff		Время задержки в мс. Значение округляется до точности 100 мс. Допустимый диапазон 0 - 10000 мс.
Enable		Изменение состояния экземпляра ERPS (выключено/включено)
Port0	Type	Настройка триггера сигнализации для порта0. Тип: LINK - В качестве триггера используется состояние порта MEP - В качестве триггера используется mep. Требуется ввод domain, service, mep-id, относящиеся к экземпляру MEP.
	Domain	
	Service	
	MEPID	
Port1	Type	Настройка триггера сигнализации для порта1. Тип: LINK - В качестве триггера используется состояние порта MEP - В качестве триггера используется mep. Требуется ввод domain, service, mep-id, относящиеся к экземпляру MEP.
	Domain	
	Service	
	MEPID	
VLAN ID		Сети VLAN, защищенные этим экземпляром кольца. По крайней мере, одна VLAN должна быть защищена. Укажите в виде списка номеров vlan или диапазонов vlan, разделенных запятыми. Например: 1,4,7,30-70
RPL Mode		Режим соединения с кольцевой защитой. None: у этого коммутатора нет порта RPL в кольце. Owner: этот коммутатор является владельцем RPL для кольца Neighbor: этот коммутатор является соседом RPL для кольца
RPL Port		Указывает, является ли это портом 0 или 1 каналом защиты кольца. Не используется, если для параметра RPL Mode установлено значение None .

3.2.8 Конфигурирование DHCPv4 сервера

DHCP (протокол динамической настройки узла) — сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации, клиент на этапе конфигурации сетевого устройства обращается к так называемому серверу DHCP и получает от него нужные параметры. Можно задать диапазон адресов, 28 распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок.

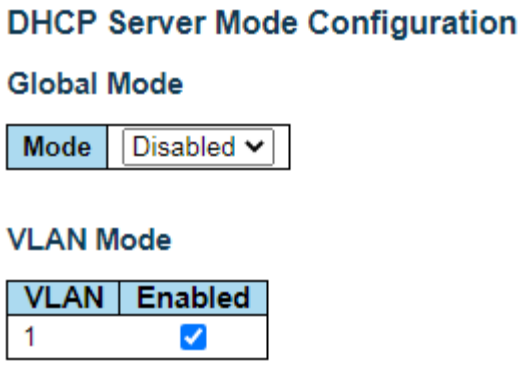


Рис. 3.22 – DHCP Сервер

Таблица 3.19 - DHCP Сервер

Mode	Включить/выключить DHCPv4
VLAN	Номер VLAN
Enabled	Включения / отключение DHCP-сервера для соответствующего VLAN.

Исключение групп IP адресов (Рис. 2.23) (Табл. 3.20).

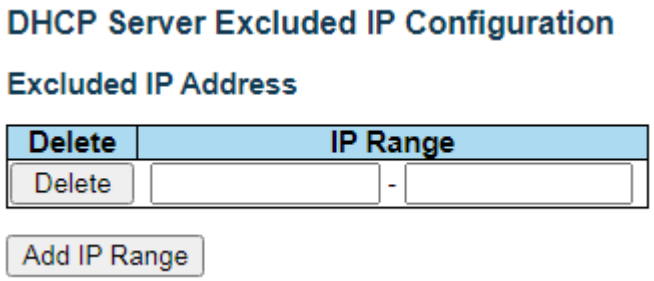


Рис. 3.23 – Исключение групп IP адресов

Таблица 3.20 - Исключение групп IP адресов

Delete	Удалить текущий диапазон IP адресов
IP Range	Задать диапазон-группу исключаемых IP адресов. Обычно адреса шлюзов, так как DHCP сервер не должен раздавать адреса шлюзов клиентам
Add IP Range	Добавить диапазон IP адресов

Создание адресных пулов DHCP (Рис. 3.24) (Табл. 3.21). При этом методе, DHCP сервер будет выделять IP адрес из пула адресов (иногда называемым диапазоном или областью) на период времени (в аренду), который настраивается.

Pool Setting

Delete	Name	Type	IP	Subnet Mask	Reserved only	Lease Time
Delete		-	-	-	-	1 days 0 hours 0 minutes

Add New Pool

Рис. 3.24 – Адресные пулы DHCP

Таблица 3.21 - Адресные пулы DHCP

Delete	Удалить текущий адресный пул
Name	Имя пула
Type	Тип узла для клиента NetBIOS Node Type. Здесь могут быть следующие значения: b – broadcast, p - peer-to-peer, m – mixed, h – hybrid От этого зависит порядок преобразования имени в IP для клиентов сети Microsoft.
IP	IP адрес, диапазон
Subnet Mask	Маска подсети
Reserved only	Только зарезервированные адреса. Если этот параметр включен, IP-адреса, которые можно выбрать из пула, ограничиваются теми, которые введены в таблицу зарезервированных записей.
Lease Time	Время аренды адреса. По умолчанию время аренды равно 24 часам. Можно выставить свое время аренды.

DHCP snooping (Рис. 3.25) (Табл. 3.22). DHCP snooping (Отслеживание DHCP) – защитная функция, позволяющая предотвратить несанкционированное подключение к сети стороннего DHCP сервера с целью перехвата клиентских DHCP запросов. Сущность DHCP snooping заключается в том, чтобы закрыть возможность обработки DHCP запросов на недоверенных портах. Администратор сети должен вручную настроить доверенные порты, - порты за которыми находится настоящий DHCP сервер.

DHCP Snooping Configuration

Snooping Mode	Disabled
Max Count Client	2048
Vlan	1
Option 82	Enabled
Circuit ID	circuit_id
Remote ID	remote_id
Format	HEX

Port Mode Configuration

Port	Mode	Max Count
*	<>	2048
1	Trusted	2048
2	Trusted	2048
3	Trusted	2048
4	Trusted	2048
5	Trusted	2048
6	Trusted	2048
7	Trusted	2048
8	Trusted	2048
9	Trusted	2048
10	Trusted	2048

Рис. 3.25 – DHCP snooping

Таблица 3.22 - DHCP snooping

Snooping mode	Включение/выключение функции DHCP snooping
Max Count Client	Максимальное количество клиентов
Vlan	Номер vlan
Option 82	Включение/выключение опции 82
Circuit ID	Идентификатор порта коммутатора
Remote ID	Идентификатор коммутатора
Format	Формат опции 82 HEX/ascii
Port	Номер порта
Mode	Режим для порта: • Ненадёжный (Untrusted) — порт, к которому подключен

	клиент. DHCP-ответы, приходящие с этого порта, отбрасываются коммутатором. Для ненадёжных портов выполняется ряд проверок сообщений DHCP и создаётся база данных привязки DHCP (DHCP snooping binding database). • Доверенный (Trusted) — порт коммутатора, к которому подключен другой коммутатор или DHCPсервер. DHCP-пакеты, полученные с доверенного порта, не отбрасываются.
Max Count	Максимальное количество клиентов

DHCP Relay (Рис. 3.26) (Табл. 3.23). Настройка DHCP Relay позволяет коммутатору переадресовывать запросы от DHCP-клиента к другому DHCPсерверу (например, старшему в иерархии сети).

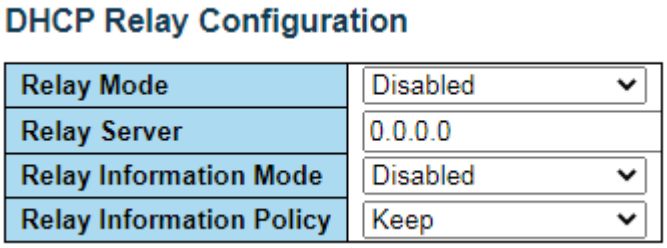


Рис. 3.26 – DHCP Relay

Таблица 3.23 - DHCP Relay

Relay Mode	Включение/выключение функции DHCP Relay
Relay Server	Адрес DHCP сервера
Relay Information Mode	Включение/выключение режима выбора действия, которое необходимо выполнить, если пересылаемое сообщение уже содержит информацию о переадресации
Relay Information Policy	Действие: Keep – информация не меняется; Replace – информация перезаписывается. Drop – отбросить пакет.

3.2.9 DHCPv6

Switch Configuration

Snooping Mode	Disabled
Unknown IPv6 Next-Headers	Drop

Port Configuration

Port	Trust Mode
*	<>
Gi 1/1	Untrusted
Gi 1/2	Untrusted
Gi 1/3	Untrusted
Gi 1/4	Untrusted
Gi 1/5	Untrusted
Gi 1/6	Untrusted
Gi 1/7	Untrusted
Gi 1/8	Untrusted
Gi 1/9	Untrusted
Gi 1/10	Untrusted

Рис. 3.27 – DHCPv6

Таблица 3.24 - DHCPv6

Snooping Mode	Включение/выключение функции DHCPv6 snooping
Unknown IPv6 Next-Headers	Выбор обработки неизвестных значений заголовка IPv6. Коммутатор должен анализировать все пакеты IPv6 для клиента DHCPv6, чтобы определить, действительно ли это сообщение DHCPv6 Возможные варианты: drop- Отбрасывать пакеты с неизвестными заголовками расширения IPv6. Это наиболее безопасный вариант, но он может привести к перебоям в трафике. allow- Разрешить пакеты с неизвестными заголовками расширения IPv6. Это менее безопасный вариант, но он предотвращает перебои в трафике.
Port	Номер порта
Trust Mode	Режим для порта: • Ненадёжный (Untrusted) — порт, к которому подключен клиент. DHCP-ответы, приходящие с этого порта, отбрасываются коммутатором. Для ненадёжных портов выполняется ряд проверок сообщений DHCP и создаётся база данных привязки DHCP (DHCP snooping binding database). • Доверенный (Trusted) — порт коммутатора, к которому подключен другой коммутатор или DHCPсервер. DHCP-пакеты, полученные с доверенного порта, не отбрасываются.

DHCPv6 Relay (Рис. 3.28) (Табл. 3.25). Настройка DHCPv6 Relay для vlan

DHCPv6 Relay Configuration

Delete	Interface	Relay Interface	Relay Destination
Delete	VLAN 1	VLAN 1	ff05::1:3

Add New Entry

Рис. 3.28 – DHCPv6 Relay

Таблица 3.25 – DHCPv6 Relay

Delete	Удалить текущую запись
Interface	Номер интерфейса
Relay Interface	Номер интерфейса, используемый для ретрансляции.
Relay Destination	Адрес IPv6, представленный в виде удобочитаемого теста, как указано в RFC5952. IPv6-адрес сервера DHCPv6, на который должны быть ретранслированы запросы. Значение по умолчанию «ff05 :: 1: 3» означает «любой DHCP-сервер».

3.2.10 Конфигурация пользователей. Users Configuration.

Для управления учетными записями пользователей необходимо перейти по вкладке Configuration→Security→Switch→Users. На этой странице представлен обзор текущих пользователей (Рис. 4.17) (Табл. 4.15).

Users Configuration

User Name	Privilege Level
admin	15

Add New User

Рис. 3.29 – Конфигурация пользователей

Таблица 3.26 – Конфигурация пользователей

User Name	Имя пользователя
Privilege Level	Уровень привилегий пользователя. Допустимый диапазон: от 0 до 15. Как правило, уровень привилегий 15 используется

	для учетной записи администратора, уровень привилегий 10 для стандартной учетной записи пользователя и уровень привилегий 5 для учетной записи наблюдателя.

Кнопка Add New User предназначена для добавления новых пользователей (Рис. 3.20) (Табл. 3.27).

Add User

User Settings	
User Name	
Password	
Password (again)	
Privilege Level	0

Рис. 3.30 – Добавление пользователей

Таблица 3.27 – Добавление пользователей

User Name	Имя пользователя
Password	Пароль
Password (again)	Повтор пароля
Privilege Level	Уровень привилегий пользователя от 0 до 15.

3.2.11 Уровни привилегий. Privilege Levels

Для доступа к настройкам уровней привилегий необходимо перейти по вкладке Configuration→Security→Switch→ Privilege Levels. На этой странице представлен обзор текущих уровней привилегий (Рис. 3.31) (Табл. 3.28).

Privilege Level Configuration

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
Alarm	5	10	5	10
APS	5	10	5	10
CFM	5	10	5	10
DDMI	5	10	5	10
Debug	15	15	15	15
DHCP	5	10	5	10
DHCPv6_Client	5	10	5	10
Diagnostics	5	10	5	10
ERPS	5	10	5	10
ETH_LINK_OAM	5	10	5	10
Firmware	5	10	5	10
Green_Ethernet	5	10	5	10
IP	5	10	5	10
IPMC_Snooping	5	10	5	10
LACP	5	10	5	10
LLDP	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
Miscellaneous	15	15	15	15
MRP	5	10	5	10
MVR	5	10	5	10
NTP	5	10	5	10
POE	5	10	5	10
Ports	5	10	1	10
Private_VLANs	5	10	5	10
PTP	5	10	5	10
QoS	5	10	5	10
RMirror	5	10	5	10
Security(access)	10	10	5	10
Security(network)	5	10	5	10
sFlow	5	10	5	10
Spanning_Tree	5	10	5	10
System	5	10	1	10
UDLD	5	10	5	10
uFDMA_AIL	5	10	5	10
uFDMA_CIL	5	10	5	10
UPnP	5	10	5	10
VCL	5	10	5	10
VLAN_Translation	5	10	5	10
VLANs	5	10	5	10
Voice_VLAN	5	10	5	10
XXRP	5	10	5	10

Рис. 3.30 – *Уровни привилегий*

Таблица 3.28 – Уровни привилегий

<table>
<tr><td colspan="2">Group Name</td><td colspan="2">Имя, идентифицирующее группу привилегий. В большинстве случаев группа состоит из одного модуля (например, LACP, RSTP или QoS), но некоторые содержат более одного. Группы в деталях: -System: Contact, Name, Location, Timezone, Daylight Saving Time, Log; -Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard; -IP: все, кроме ping; -Ports: все, кроме VeriPHY; - Diagnostics: ping и VeriPHY; - Maintenance: CLI - System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web - Users, Privilege Levels и все в Maintenance; -Debug: присутствует только в CLI.</td></tr>
<tr><td rowspan="4">Privilege Levels</td><td>Configuration Read-only</td><td>Конфигурация: только чтение</td><td rowspan="4">Уровень привилегий группы от 0 до 15. Привилегия пользователя должна быть такой же или больше, чем уровень этой группы, чтобы иметь доступ к этой группе.</td></tr>
<tr><td>Configuration/Execute Read/write</td><td>Конфигурация: чтение и запись</td></tr>
<tr><td>Status/Statistics Read-only</td><td>Статус/статистика: только чтение</td></tr>
<tr><td>Status/Statistics Read/write</td><td>Статус/статистика: чтение и запись</td></tr>
</table>

3.2.12 Конфигурация аутентификации, авторизации и учета. Authentication, Authorization, Accounting

Для доступа к настройкам аутентификации, авторизации и учета необходимо перейти по вкладке Configuration→Security→Switch→Auth Method. Authentication (аутентификация) — сопоставление запроса существующей учётной записи в системе безопасности. Authorization (авторизация, проверка уровня доступа) — сопоставление учётной записи в системе (прошедшей аутентификацию) и определённых полномочий. Accounting (учёт) — слежение за потреблением ресурсов пользователем. На этой странице представлен обзор текущих параметров аутентификации, авторизации и учета (Рис. 3.31) (Табл. 3.29).

Authentication Method Configuration

Client	Methods		
console	local	no	no
telnet	local	no	no
ssh	local	no	no
http	local	no	no

Command Authorization Method Configuration

Client	Method	Cmd Lvl	Cfg Cmd
console	no	0	☐
telnet	no	0	☐
ssh	no	0	☐

Accounting Method Configuration

Client	Method	Cmd Lvl	Exec
console	no		☐
telnet	no		☐
ssh	no		☐

Рис. 3.31 – *Конфигурация аутентификации, авторизации и учета*

Таблица 3.29 – Конфигурация аутентификации, авторизации и учета

Authentication Method Configuration	Client	Клиент: console, telnet, SSH, http
	Methods	- no: аутентификация отключена, и вход в систему невозможен; 35 - local: использовать локальную базу данных на коммутаторе для проверки подлинности; - radius: использовать удаленные серверы RADIUS для аутентификации; - tacacs: использовать удаленные серверы TACACS для аутентификации; Доступность метода проверяется слева направо.
Command Authorization Method Configuration	Client	Клиент: console, telnet, ssh
	Method	- no: авторизация команд отключена. Пользователь получает доступ к командам CLI в соответствии со своим уровнем привилегий. - tacacs: для авторизации команд используется один или несколько удаленных серверов TACACS+. Если все удаленные серверы находятся в автономном режиме, пользователю предоставляется доступ к командам CLI в соответствии с его уровнем привилегий.
	Cmd Lvl	Авторизовать все команды с уровнем привилегий выше или равным этому уровню. Допустимые значения находятся в диапазоне от 0 до 15.
	Cfg Cmd	Авторизовать команды конфигурации
Accounting Method Configuration	Client	Клиент: console, telnet, ssh
	Methods	- no: учет отключен; - tacacs: для учета используется один или несколько удаленных серверов TACACS+

	Cmd Lvl	Включает учет всех команд с уровнем привилегий выше или равным этому уровню. Допустимые значения находятся в диапазоне от 0 до 15. Оставьте поле пустым, чтобы отключить учет команд.
	Exec	Режим учета EXEC

3.2.13 Конфигурация SSH

Для доступа к настройкам SSH необходимо перейти по вкладке Configuration→Security→Switch→ SSH. На этой странице представлен обзор текущих параметров SSH. Параметр Mode указывает режим работы SSH.

3.2.14 Конфигурация HTTPS

Для доступа к настройкам HTTPS необходимо перейти по вкладке Configuration→Security→Switch→HTTPS. На этой странице представлен обзор текущих параметров HTTPS (Рис. 3.32) (Табл. 3.30).

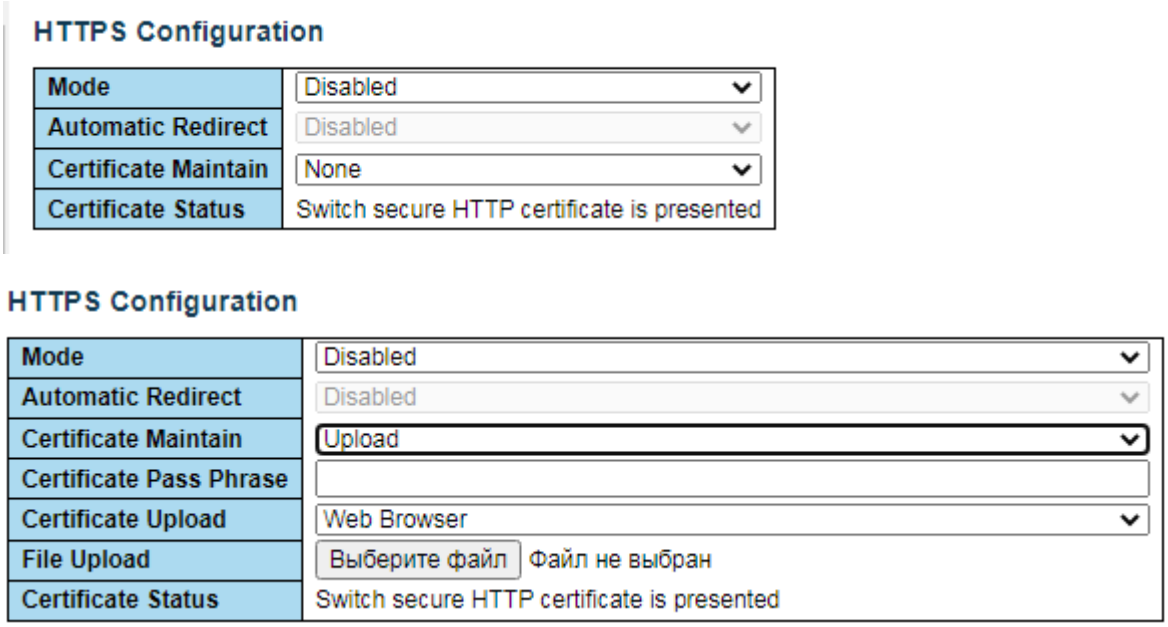


Рис. 3.32 – *Конфигурация HTTPS*

Таблица 3.30 – Конфигурация HTTPS

Mode	Режим работы HTTPS. Когда текущее соединение HTTPS, но HTTPS выключен, web-браузер будет автоматически перенаправляться на соединение HTTP.
Automatic Redirect	Режим работы автоматического перенаправления HTTPS. Применяется только, если для режима работы HTTPS выбрано "Enabled" (Включен). Автоматически направляет HTTP web-браузера на соединение HTTPS, когда

	включены оба режима работы – HTTPS и Automatic Redirect
Certificate Maintain	Это поле может быть настроено только при отключенном HTTPS. Оно используется для обслуживания сертификации. Возможные действия: - None: никаких действий сертификации; - Delete: удалить сертификат; - Upload: загрузка сертификата, можно выбрать два метода загрузки; - Generate: создание сертификата.
Certificate Algorithm	Алгоритм сертификации. Возможные типы: DSA, RSA.
Certificate Status	Статус сертификации. Возможный статус: 37 - Выдается защищенный сертификат HTTP. Сертификат хранится в базе данных HTTPS; - Сертификат безопасного переключения SSL не представлен: сертификат не хранится в базе данных HTTPS. - Выдача защищенного сертификата HTTP. Генерируется сертификат
Pass Phrase	Шаблон для шифровки сертификата
Certificate Upload	Загрузка сертификата. Возможные режимы: - Web Browserr: загрузка сертификата через веб - браузер; - URL: для загрузки сертификата через URL
File Upload	Файл для загрузки

3.2.15 Конфигурация управления доступом. Access Management Configuration

Для доступа к конфигурации управления доступом необходимо перейти по вкладке Configuration→Security→Switch→ Access Management. На этой странице можно настроить таблицу управления доступом (Рис. 3.33) (Табл. 3.31). Максимальное число элементов списка 16. Если тип приложения совпадает с одним из типов, имеющимся в списке управления доступом, то доступ к коммутатору будет разрешен.

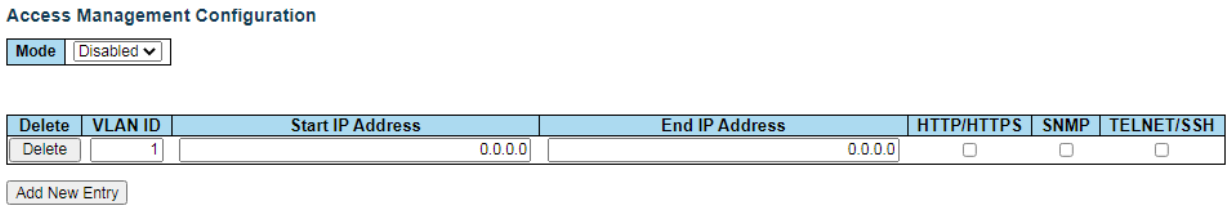


Рис. 3.33 – *Конфигурация управления доступом*

Таблица 3.31 – Конфигурация управления доступом

Mode	Включение/выключение
Delete	Удалить текущую запись
VLAN ID	Номер VLAN для элемента управления доступом
Start IP Address	Начальный IP-адрес для элемента управления доступом
End IP Address	Конечный IP-адрес для элемента управления доступом
SNMP	Если в этом поле установлен флаг, это указывает, что хосту с IP-адресом из указанного диапазона может быть предоставлен доступ к коммутатору по SNMP.

TELNET/SSH	Если в этом поле установлен флаг, это указывает, что хосту с IP-адресом из указанного диапазона может быть предоставлен доступ по TELNET/SSH

Кнопка Add New Entry служит для добавления новой записи.

3.2.16 SNMP

Для доступа к конфигурации SNMP необходимо перейти по вкладке Configuration→Security→Switch→ SNMP.

SNMP System Configuration (Системные настройки SNMP) (Рис. 3.34) (Табл. 3.32).

SNMP System Configuration

Mode	Enabled
Engine ID	800019cb03001232541243

Рис. 3.34 – *Системные настройки SNMP*

Таблица 3.32 – Системные настройки SNMP

Mode	Режим работы SNMP
Engine ID	Идентификатор engine ID для SNMPv3. Строка должна содержать четное число (в 16-ном формате), число 39 цифр от 10 до 64; комбинации цифр, состоящие из одних нулей и из одних «F» недопустимы.

Trap Configuration (Настройки сигнализации) (Рис. 3.35) (Табл. 3.33).

Trap Configuration

Trap Destination Configurations

Delete	Name	Enable	Version	Destination Address	Destination Port

Add New Entry

SNMP Trap Configuration

Trap Config Name	
Trap Mode	Disabled
Trap Version	SNMP v2c
Trap Community	public
Trap Destination Address	
Trap Destination Port	162
Trap Inform Mode	Disabled
Trap Inform Timeout (seconds)	3
Trap Inform Retry Times	5
Trap Security Engine ID	800019cb03001232541243
Trap Security Name	None

Рис. 3.35 – Настройки сигнализации

Таблица 3.33 – Настройки сигнализации

Mode	Включить/выключить отправку SNMP trap
Trap Config Name	Имя конфигурации
Trap Version	Поддерживаемая версия SNMP trap. (SNMP 1/ SNMP v2c/SNMP 3)
Trap Community	Строка доступа community для отправки пакета SNMP trap.
Trap Destination Address	IP-адрес сервера для отправки SNMP trap. Корректный IP-адрес в десятичном формате с точкой. Допустимо также указать корректное имя хоста.
Trap Destination port	Порт назначения SNMP trap. SNMP-агент будет посылать сообщения SNMP на этот порт; диапазон номеров портов 1~65535. По умолчанию порт для сообщений SNMP trap имеет номер 162.
Trap Inform Mode	Включить/выключить режим работы SNMP trap inform
Trap Inform Timeout	Таймер сообщений SNMP trap inform. Диапазон допустимых значений: от 0 до 2147.
Trap Inform Retry Times	Таймер попыток повторения сообщений SNMP trap inform. Диапазон допустимых значений: от 0 до 255
Trap Security Engine ID	Режим работы SNMP trap security engine ID. Протокол SNMP v3 посылает сообщения trap и inform, использующие USM для аутентификации и обеспечения конфиденциальности. Сообщениям назначается уникальный идентификатор engine ID и необходимая информация. Если включен режим "Trap Probe Security Engine ID", идентификатор (ID) будет генерироваться автоматически. В противном случае, будет использован ID, указанный в этом поле. Строка должна содержать четное число (в 16-ном формате), число цифр от 10 до 64; комбинации цифр, состоящие из одних нулей и из одних «F» недопустимы

Trap Security Name	Имя SNMP trap security name. Сообщения SNMP trap и inform SNMP v3 используют USM для аутентификации и обеспечения конфиденциальности. Когда включен режим отправки trap и inform, необходимо задать уникальное имя для обеспечения безопасности.

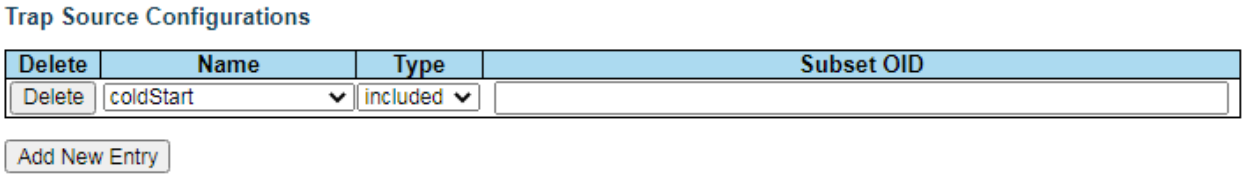


Рис. 3.36 – Trap Source Configurations

Таблица 3.34 – Trap Source Configurations

Delete	Удаление текущей записи.
Name	Указывает имя записи.
Type	Тип фильтра для записи (включить или исключить)
Subset OID	Подмножество OID для записи. Значение должно зависеть от того, какое имя указано в поле Name . Например, ifIdex - это OID подмножества для linkUp и linkDown. Допустимый OID подмножества - это одно или несколько цифровых чисел (0-4294967295) или звездочка (*), разделенных точками (.). Первый символ не должен начинаться со звездочки (*), а максимальное количество OID не должно превышать 128.

SNMPv3 Community Configuration (Настройка SNMPv3Community) (Рис. 3.37) (Табл. 3.35).

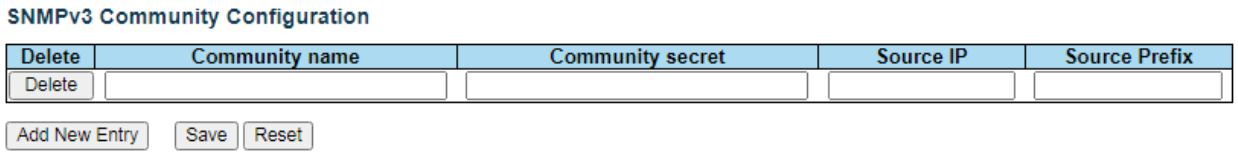


Рис. 3.37 – Настройка SNMP v3 Community

Таблица 3.35 – Настройка SNMP v3 Community

Delete	Удаление текущей записи.
Community name	Указывает имя безопасности для сопоставления сообщества с конфигурацией групп SNMP. Допустимая длина строки составляет от 1 до 32, а допустимое содержимое - символы ASCII от 33 до 126.
Community secret	Пароль сообщества (строку доступа) для разрешения доступа с использованием SNMPv1 и SNMPv2c к агенту SNMP. Допустимая длина строки составляет от 1 до 32, а

	допустимое содержимое - символы ASCII от 33 до 126.
Source IP	IP-адрес источника при доступе по SNMP
Source Prefix	префикс адреса источника.

Кнопка Add New Entry служит для добавления новой записи.

SNMP v3 User Configuration (Пользовательская настройка SNMP v3) (Рис. 3.38) (Табл. 3.36).

SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
Delete	800019cb03001232541243		Auth, Priv	MD5		DES	

Add New Entry Save Reset

Рис. 3.38 – Пользовательская настройка SNMP v3

Таблица 3.36 – Пользовательская настройка SNMP v3

Delete	Удаление текущей записи.
Engine ID	Строка, идентифицирующая engine ID, которому принадлежит этот элемент списка. Строка должна содержать четное число (в 16-чном формате), число цифр от 10 до 64; комбинации цифр, состоящие из одних нулей и из одних «F» недопустимы. В архитектуре SNMPv3 используется модель безопасности на основе пользователя USM (User based Security Model) для обеспечения безопасности сообщений и модель управления доступом на основе вида VACM (View-based Access Control Model) при управлении доступом. Для входа USM ключами входов являются usmUserEngineID и usmUserName. В простом агенте usmUserEngineID всегда совпадает с собственным значением snmpEngineID агента. В качестве значения также может использоваться значение snmpEngineID удаленного устройства (SNMP engine), с которым может связываться данный пользователь. Другими словами, если engine ID пользователя равен engine ID системы, то он является локальным пользователем, в противном случае пользователь является удаленным.
User Name	Строка, идентифицирующая имя пользователя, которому принадлежит данный параметр. Допустимая длина строки 1~32 символов ASCII с 43 номерами в диапазоне от 0x21 до 0x7E
Security Level	Модель безопасности, которой принадлежит данный параметр. Возможны следующие модели безопасности: • NoAuth, NoPriv: Аутентификация и конфиденциальность отсутствуют. • Auth, NoPriv: Выполняется аутентификация,

	конфиденциальность отсутствует. • Auth, Priv: Выполняется аутентификация, обеспечивается конфиденциальность. Если параметр уже существует, значение уровня безопасности изменить невозможно. Это означает, что сначала надо удостовериться, что значение установлено правильно.
Authentication Protocol	Протокол аутентификации, которому принадлежит данный параметр. Возможны следующие протоколы аутентификации: • MD5: дополнительный флаг, указывающий, что пользователь использует протокол аутентификации MD5. • SHA: дополнительный флаг, указывающий, что пользователь использует протокол аутентификации SHA. Если параметр уже существует, значение уровня безопасности изменить невозможно. Это означает, что сначала надо удостовериться, что значение установлено правильно.
Authentication Password	Строка, идентифицирующая фразу пароля аутентификации. Допустимая длина строки для протокола аутентификации MD5: от 8 до 32 символов. Допустимая длина строки для протокола аутентификации SHA: от 8 до 40 символов. При записи строки аутентификации могут использоваться символы ASCII с кодами в диапазоне от 0x21 до 0x7E.
Privacy Protocol	Протокол конфиденциальности, которому принадлежит данный вход. Возможны следующие протоколы конфиденциальности: • AES: дополнительный флаг, указывающий, что пользователь использует протокол аутентификации AES. • DES: дополнительный флаг, указывающий, что пользователь использует протокол аутентификации DES.
Privacy Password	Строка, идентифицирующая фразу пароля конфиденциальности. Допустимая длина строки 8~32 символов ASCII с номерами в диапазоне от 0x21 до 0x7E.

Кнопка Add New Entry служит для добавления новой записи.

SNMP v3 Group Configuration (Настройки группы SNMP v3) (Рис. 3.39) (Табл. 3.37).

SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
☐	v1	public	default_ro_group
☐	v1	private	default_rw_group
☐	v2c	public	default_ro_group
☐	v2c	private	default_rw_group

Add New Entry Save Reset

Рис. 3.39 – Настройки группы SNMP v3

Таблица 3.37 – Настройки группы SNMP v3

Delete	Удаление текущей записи.
Security Model	Модель безопасности, которой принадлежит данный параметр. Возможны следующие модели безопасности: • v1: зарезервировано для SNMPv1. • v2c: зарезервировано для SNMPv2c. • usm: модель безопасности на основе пользователя USM (User-based Security Model) для SNMPv3.
Security Name	Строка, идентифицирующая безопасное имя, которому принадлежит данный параметр. Допустимая длина строки 1~32 символов ASCII с номерами в диапазоне от 0x21 до 0x7E.
Group Name	Строка, идентифицирующая имя группы, которому принадлежит данный параметр. Допустимая длина строки 1~32 символов ASCII с номерами в диапазоне от 0x21 до 0x7E.

Кнопка Add New Entry служит для добавления новой записи.

SNMPv3 View Configuration (Настройка вида SNMP v3) (Рис. 3.40) (Табл. 3.38).

SNMPv3 View Configuration

Delete	View Name	View Type	OID Subtree
Delete		included	

Add New Entry Save Reset

Рис. 3.40 – Настройка вида SNMP v3

Таблица 3.38 – Настройка вида SNMP v3

Delete	Удаление текущей записи.
View Name	Строка, идентифицирующая имя вида, которому

	принадлежит данный параметр. Допустимая длина строки 1~32 символов ASCII с номерами в диапазоне от 0x21 до 0x7E.
View Type	Тип вида, которому принадлежит данный параметр. Возможны следующие типы видов: • included (поддерево включено): дополнительный флаг, указывающий, что в вид должно быть включено поддерево. • excluded (поддерево исключено): дополнительный флаг, указывающий, что из вида должно быть исключено поддерево. В целом, если для типа вида задано ' excluded ' (поддерево исключено), должен существовать другой вид с типом ' included ' (поддерево включено) и его поддерево OID должно перекрывать поддерево вида с типом ' excluded ' (поддерево исключено).
OID Subtree	OID определяет корень поддерева, добавляемый к именованному виду. Диапазон допустимых значений OID: от 1 до 128. В строке можно указать либо число, состоящее из цифр, либо звездочку(*).

Кнопка [Add New Entry] служит для добавления новой записи.

SNMPv3 Access Configuration (Настройка доступа SNMP v3) (Рис. 3.41) (Табл. 3.39).

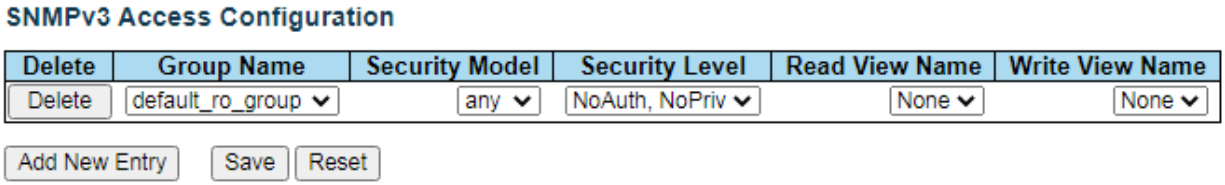


Рис. 3.41 – Настройка доступа SNMP v3

Таблица 3.39 – Настройка доступа SNMP v3

Delete	Удаление текущей записи.
Group Name	Строка, идентифицирующая имя группы, которой принадлежит данный параметр. Допустимая длина строки 1~32 символов ASCII с номерами в диапазоне от 0x21 до 0x7E.
Security Model	Модель безопасности, которой принадлежит данный параметр. Возможны следующие модели безопасности: • any (любая): будет принята любая модель безопасности (v1|v2c|usm). • v1: зарезервировано для SNMPv1. • v2c: зарезервировано для SNMPv2c. • usm: модель безопасности на основе пользователя USM (User-based Security Model) для SNMPv3.
Security Level	Уровень безопасности, которому принадлежит данный параметр. Возможны следующие модели безопасности: • NoAuth, NoPriv: Аутентификация и конфиденциальность

	отсутствуют. • Auth, NoPriv: Выполняется аутентификация, конфиденциальность отсутствует. • Auth, Priv: Выполняется аутентификация, обеспечивается конфиденциальность.
Read View Name	Имя вида при чтении, имя вида MIB, определяющего объекты MIB, для которых данный запрос может быть запросом текущих значений. Допустимая длина строки 1~32 символов ASCII с номерами в диапазоне от 0x21 до 0x7E.
Write View Name	Имя вида при записи, имя вида MIB, определяющего объекты MIB, для которых данный запрос потенциально может установить новые значения. Допустимая длина строки 1~32 символов ASCII с номерами в диапазоне от 0x21 до 0x7E.

Кнопка Add New Entry служит для добавления новой записи.

3.2.17 RMON

Для доступа к конфигурации RMON необходимо перейти по вкладке Configuration→Security→Switch→ RMON.

RMON Statistics Configuration (Настройка статистик RMON) (Рис. 3.42) (Табл. 3.40).

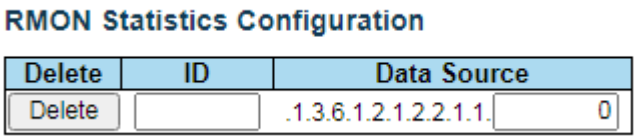


Рис. 3.42 – Настройка статистик RMON

Таблица 3.40 – Настройка статистик RMON

Delete	Удаление текущей записи.
ID	Индекс входа. Допустимые значения — от 1 до 65535.
Data Source	ID порта, мониторинг которого требуется осуществлять.

Кнопка Add New Entry служит для добавления новой записи.

RMON History Configuration (Настройка журнала RMON) (Рис. 3.43) (Табл. 3.41).

На странице RMON History Configuration можно настроить сбор статистики на физическом интерфейсе для мониторинга использования сети, типов пакетов и ошибок.

Записи журнала RMON можно использовать при мониторинге спорадически возникающих проблем.

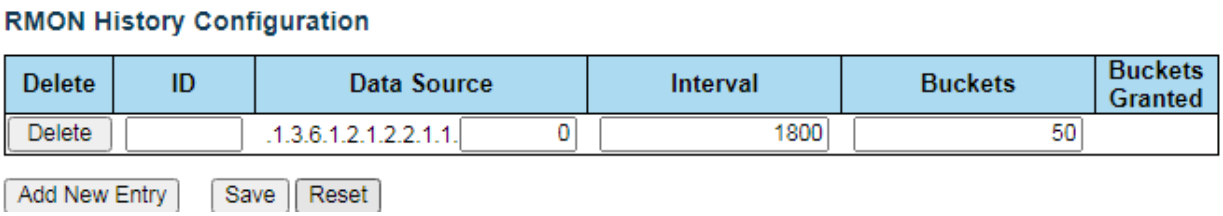


Рис. 3.43 – Настройка журнала RMON

Таблица 3.41 – Настройка журнала RMON

Delete	Удаление текущей записи.
ID	Индекс входа. Допустимые значения — от 1 до 65535.
Data Source	ID порта, мониторинг которого требуется осуществлять.
Interval	Интервал опроса. По умолчанию 1800 секунд. Диапазон допустимых значений: от 1 до 3600 секунд.
Buckets	Число сегментов, требуемых для этого параметра. По умолчанию 50. Диапазон допустимых значений: от 1 до 3600.
Buckets Granted	Предполагаемое число сегментов.

Кнопка Add New Entry служит для добавления новой записи.

RMON Alarm Configuration (Настройка сигнализаций RMON) (Рис.3.44) (Табл. 3.42).

На этой странице можно задать конкретный критерий, согласно которому будут генерироваться события. Он может быть установлен для данных теста, собранных за любой указанный интервал времени. Можно контролировать как абсолютные значения, так и их изменения. Можно также задать сигнализации, которые будут выдаваться при превышении пороговых значений либо при снижении ниже пороговых значений.

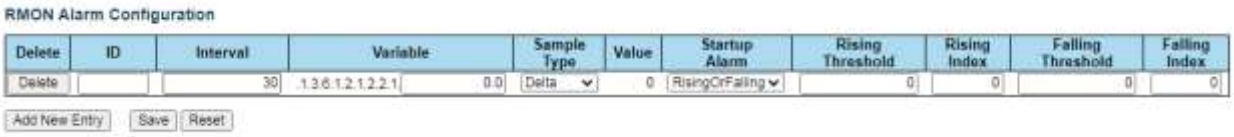


Рис. 3.44 – Настройка сигнализаций RMON

Таблица 3.42 – Настройка сигнализаций RMON

Delete	Удаление текущей записи.

ID	Индекс входа. Допустимые значения — от 1 до 65535.
Interval	Интервал опроса при выборке и сравнении с нижним или верхним пороговым значением. Диапазон от 1 до 2^31 секунд.
Variable	Номер объекта переменной MIB, из которой берутся выборки. Выборки могут браться только из переменной ifEntry.n.n . Возможны следующие переменные: InOctets, InUcastPkts, InNUcastPkts, InDiscards, InErrors, InUnknownProtos, OutOctets, OutUcastPkts, OutNUcastPkts, OutDiscards, OutErrors и OutQLen.
Sample type	Тип выборки. Для указанной переменной тест может быть выполнен для абсолютных значений или их относительного изменения.
Value	Статистическое значение в течение последнего периода выборки.
Startup Alarm	Выбирает метод, который будет использоваться для выборки выбранной переменной и вычисления значения, которое сравнивается с пороговыми значениями.
Rising Threshold	Включает сигнализацию, когда значение первый раз превысит пороговое значение подъема либо станет меньше, чем пороговое значение спада.
Rising Index	Индекс подъема для события. Диапазон 1~65535.
Falling Threshold	Пороговое значение спада. Если текущее значение станет меньше порогового значения спада и, при этом, последнее значение выборки больше этого порогового значения, то выдается сигнализация. После генерации события спада, другое такое событие не будет сгенерировано до тех пор, пока значение выборки не станет больше порогового значения спада, достигнет порогового значения подъема и снова вернется к пороговому значению спада. (Диапазон: от -2147483647 до 2147483647).
Falling Index	Индекс спада для события. Диапазон 1~65535.

Кнопка [Add New Entry] служит для добавления новой записи.

RMON Event Configuration (Настройка событий RMON) (Рис. 4.45) (Табл. 3.43).

На этой странице можно задать операцию, которая выполняется при выдаче сигнализации.

RMON Event Configuration

Delete	ID	Desc	Type	Event Last Time
Delete			none	0

Add New Entry Save Reset

Рис. 3.45 – Настройка событий RMON

Таблица 3.43 – Настройка событий RMON

Delete	Удаление текущей записи.
ID	Индекс ID. Диапазон 1~65535.
Desc	Введите в это поле описание для данного входа.
Type	Выберите тип события, которое будет выбираться при срабатывании сигнализации: • None (Нет): Событие сгенерировано не будет. • Log (Журнал): Когда генерируется событие, генерируется и запись журнала RMON. • snmptrap: посылает сообщение trap всем установленным менеджерам сообщений trap. • logandtrap: О событии создается запись в журнале, посылается сообщение trap.
Event Last Time	Время последнего события. Значение sysUpTime, когда событие для этого входа было сгенерировано последний раз.

Кнопка Add New Entry служит для добавления новой записи.

3.2.18 Network. Сеть

3.2.19 Port Security Limit Control Configuration. Управление безопасности порта

Функция управлением безопасностью порта (Port Security Limit Control) может ограничить число пользователей, которым разрешен доступ к коммутатору на основе MAC- адресов и VLAN ID (выполняется для каждого порта). Как только число пользователей, желающих получить доступ к коммутатору, превысит заданное число, будет немедленно выполнена выбранная операция.

Для доступа к настройкам необходимо перейти по вкладке Configuration→Security→Switch→Network→ Port Security→Configuration (Рис. 3.46) (Табл. 3.44).

Port Security Configuration

Global Configuration

Aging Enabled	☐
Aging Period	3600 seconds
Hold Time	300 seconds

Port Configuration

Port	Mode	Limit	Violation Mode	Violation Limit	Sticky	State
*	<>	4	<>	4	☐	
1	Disabled	4	Protect	4	☐	Disabled
2	Disabled	4	Protect	4	☐	Disabled
3	Disabled	4	Protect	4	☐	Disabled
4	Disabled	4	Protect	4	☐	Disabled
5	Disabled	4	Protect	4	☐	Disabled
6	Disabled	4	Protect	4	☐	Disabled
7	Disabled	4	Protect	4	☐	Disabled
8	Disabled	4	Protect	4	☐	Disabled
9	Disabled	4	Protect	4	☐	Disabled
10	Disabled	4	Protect	4	☐	Disabled

Рис. 3.46 – Управление безопасности порта

Таблица 3.44 – Управление безопасности порта

System Configuration (Настройка системы)	
Aging Enabled	Включить устаревание. Если в этом поле установлен флаг, то оценивается «возраст» безопасных MAC-адресов в том смысле, в котором он учитывается параметром Aging Period (Срок устаревания). Когда устаревание включено, с того момента, как конечный хост станет безопасным, запускается таймер. По истечении таймера, коммутатор начинает искать кадры конечного хоста и, если таких кадров не появляется в течение следующего срока устаревания (Aging Period), то предполагается, что конечный хост отключился и на коммутаторе освобождаются соответствующие ресурсы.
Aging Period	Если в поле Aging Enabled (Устаревание включено) установлен флаг, то становится возможно задать желаемое значение срока устаревания. По умолчанию установлен срок устаревания 3600 секунд. Допустимый диапазон значений от 10 до 10 000 000 секунд.
Hold Time	Время удержания, измеряемое в секундах, используется для определения того, как долго MAC-адрес хранится в таблице MAC-адресов, если было обнаружено, что он нарушает ограничение. Допустимый диапазон составляет от 10 до 10 000 000 секунд, по умолчанию - 300 секунд. Причина сохранения нарушающего MAC-адреса в таблице MAC-адресов заключается в первую очередь в

	том, чтобы гарантировать, что один и тот же MAC-адрес не вызывает непрерывных уведомлений (если включены уведомления о количестве нарушений).
Port Configuration (Настройка порта)	
Port	Отображается номер порта. “*” означают применение ко всем портам.
Mode	Включает или выключает управление ограничением количества хостов порта (по каждому порту отдельно). Чтобы сделать данную функцию работоспособной, необходимо включить ее как глобально, так и для порта.
Limit	Включает или выключает управление ограничением количества хостов порта (по каждому порту отдельно). Чтобы сделать данную функцию работоспособной, необходимо включить ее как глобально, так и для порта.
Violation Mode	Выбор режима при превышении предела MAC-адресов на порту Protect – ничего не предпринимать Restrict - Если предел достигнут, последующие MAC-адреса порта будут подсчитаны и отмечены как нарушающие. Такие адреса MAC удаляются из таблицы MAC-адресов по истечении времени удержания. В лучшем случае нарушения предельных значений MAC - адрес может быть помечен как нарушение в любой момент времени. Shutdown- Если предел достигнут, то это приведет к отключению порта. Это означает, что все защищенные MAC-адреса будут удалены из порта и новые адреса не будут изучены.
Violation Limit	Настройка максимального количества MAC-адресов, которые могут быть помечены как нарушающие этот порт. Это число не может превышать 1023. По умолчанию - 4. Он используется только тогда , когда установлен режим restrict
Sticky	Включение прикрепления MAC-адресов к порту. Когда порт находится в режиме sticky, все MAC-адреса, которые в противном случае были бы изучены как динамические, узнаются как закрепленные. Прикрепленные MAC-адреса являются частью рабочей конфигурации и поэтому могут быть сохранены в startup-config. Прикрепленные MAC-адреса сохраняются при изменении ссылок (в отличие от динамических, которые придется запоминать заново). Они также выдерживают перезагрузку, если рабочая конфигурация сохранена в startup-config.
State	Отображается текущее состояние порта с точки зрения управления ограничением количества хостов порта.

Port Security Static and Sticky MAC Addresses. Настройка статических и фиксированных MAC-адресов.

Для доступа к настройкам необходимо перейти по вкладке Configuration→Security→Switch→Network→ Port Security→MAC Addresses (Рис. 3.47) (Табл. 3.45).

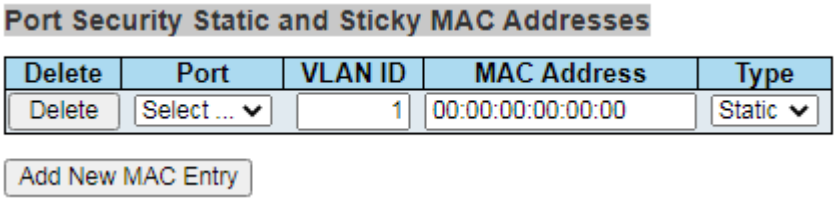


Рис. 3.47 – Настройка статических и фиксированных MAC-адресов

Таблица 3.45 – Настройка статических и фиксированных MAC-адресов

Delete	Удалить текущую запись
Port	Номер порта, к которому привязан MAC-адрес.
VLAN ID	Идентификатор VLAN
MAC Address	MAC-адрес
Type	Указывает тип записи и может быть статическим или фиксированным

Кнопка Add New MAC Entry служит для добавления новой записи.

3.2.19.1 NAS (Network Access Server)

Конфигурирование сервера доступа в сеть (Network Access Server) полезно в сетевой среде, в которой желательно аутентифицировать клиентов (supplicants) до того, как они получат доступ к ресурсам защищенной сети. Для эффективного управления доступом для неизвестных клиентов, IEEE разработал стандарт 802.1X, обеспечивающий процедуру аутентификации на порту, предотвращающую несанкционированный доступ к сети по запросам пользователей, впервые предоставляющих учетные данные для целей аутентификации. Коммутатор, соединяющий клиентов и radius-сервер, обычно работает как аутентификатор. Для обмена сообщениями аутентификации между клиентами и удаленным RADIUS-сервером, проверяющим аутентичность пользователя и его права доступа, используется EAPOL (расширенный протокол аутентификации по локальным сетям). На данной странице можно настроить конфигурацию аутентификатора либо глобально, либо для каждого порта отдельно.

Для доступа к настройкам необходимо перейти по вкладке Configuration→Security→Network→NAS (Рис. 3.48) (Табл. 3.46).

Network Access Server Configuration

System Configuration

Mode	Disabled
Reauthentication Enabled	☐
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds
RADIUS-Assigned QoS Enabled	☐
RADIUS-Assigned VLAN Enabled	☐
Guest VLAN Enabled	☐
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	☐

Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart	
*	<>	☐	☐	☐			
1	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
3	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
4	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
5	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
6	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
7	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
8	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
9	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
10	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize

Рис. 3.48 – Конфигурирование сервера доступа в сеть

Таблица 3.46 – Конфигурирование сервера доступа в сеть

System Configuration (Настройка системы)	
Mode	Включает на коммутаторе глобально 802.1X и аутентификацию на основе MAC- адресов. Если глобально эти протоколы выключены, передача кадров будет разрешена на всех портах.
Reauthentication Enabled	Установите флаг в этом поле, чтобы разрешить клиентам повторную аутентификацию по истечении интервала времени, заданного в поле "Reauthentication Period" (Интервал повторной аутентификации). Повторную аутентификацию можно использовать для определения того, подключено ли к порту коммутатора новое устройство.
Reauthentication Period	Интервал времени, по истечении которого подключенное устройство может быть аутентифицировано повторно. По умолчанию установлен интервал повторной аутентификации 3600 секунд. Допустимый диапазон значений от 1 до 3600 секунд.
EAPOL Timeout	Интервал времени, в течение которого коммутатор будет ожидать ответ от подавшего запрос на доступ к сети устройства в течение сессии аутентификации перед тем, как передать пакет Request Identify (Запрос идентификации) EAPOL. По умолчанию задано 30 секунд. Допустимый диапазон значений от 1 до 65535 секунд.
Aging Period	Интервал времени, определяющий допустимое время доступа клиента к коммутатору для аутентификации по 802.1X и MAC- адресу. По

	умолчанию составляет 300 секунд. Допустимый диапазон значений от 10 до 1 000 000 секунд
Hold Time	Время, по истечении которого индицируется отказ EAP, либо превышение интервала ожидания RADIUS, из-за чего клиент не получил доступ. Эта настройка применяется к портам, работающим при аутентификации Single 802.1X, Multi 802.1X или на основе MAC - адресов. По умолчанию время удерживания составляет 10 секунд. Допустимый диапазон значений от 10 до 1 000 000 секунд.
Radius - Assigned QoS Enabled	Установите флаг в этом поле, чтобы глобально включить QoS, назначаемый RADIUS.
Radius-Assigned VLAN Enabled	Номер VLAN, назначенный RADIUS, обеспечивает средства для централизованного управления VLAN, которому принадлежит успешно аутентифицированное устройство, подключенное к коммутатору. Для VLAN, присвоенному протоколом RADIUS, будет классифицироваться и коммутироваться входящий трафик. RADIUS-сервер должен быть настроен на передачу специальных атрибутов RADIUS для получения преимуществ от этой функции. Установка флага в поле "RADIUSAssigned VLAN Enabled" позволяет быстро (глобально) включить/выключить присвоение RADIUS-сервером меток VLAN. Когда флаг установлен, дубликаты настроек индивидуального порта определяют, включено ли на данном порту присваивание VLAN протоколом RADIUS. Когда флаг в поле снят, присваивание VLAN протоколом RADIUS отключено на всех портах.
Guest VLAN Enabled	Гостевая VLAN является специальной VLAN, типичным назначением которой является предоставление ограниченного доступа к сети. Когда флаг установлен, дубликаты настроек индивидуального порта определяют, может ли порт быть перемещен в гостевую VLAN. Когда флаг в поле снят, возможность перемещения порта в гостевую VLAN отключена на всех портах.
Guest VLAN ID	Номер VLAN ID работает только в том случае, когда гостевая VLAN включена. VLAN ID представляет собой значение, присваиваемое порту, если порт перемещается в гостевую VLAN. Диапазон значений: от 1 до 4095.
Max. Reauth. Count	Максимальное число повторных аутентификаций. Максимальное число передач коммутатором кадра запроса идентификации EAPOL, остающихся без ответа перед тем, как порт будет добавлен в гостевую VLAN. Значение может быть изменено только в том случае, если гостевая VLAN включена глобально. Диапазон 1~255.
Allow Guest VLAN if EAPOL Seen	Разрешать гостевую VLAN, если виден EAPOL. Коммутатор помнит, был ли принят кадр EAPOL в течение времени жизни порта. Когда коммутатор принимает решение о входе в гостевую VLAN, он сначала проверяет, включена или выключена эта опция. Если она выключена (флаг в поле снят – значение по умолчанию), коммутатор войдет в гостевую VLAN только в том случае, если кадр EAPOL не был принят на порту в течение времени жизни порта. Если опция включена (флаг в поле установлен), коммутатор войдет в гостевую VLAN, даже если кадр EAPOL был принят на порту в течение времени жизни порта. Значение может быть изменено только в том случае, если гостевая VLAN включена глобально.
Port Configuration (Настройка порта)	

Port	Номер порта. “*” означает применение ко всем портам.
Admin State	Выбирает режим аутентификации порта. Данная настройка работает только в том случае, когда глобально включен NAS. Режимы работы: • Force Authorized (Принудительная авторизация): В этом режиме работы 56 коммутатор отправит один кадр успешной (аутентификации) EAPOL, если осуществляется подключение к порту, при этом любому клиенту на порту будет разрешен доступ к сети без аутентификации. • Force Unauthorized (Принудительная не авторизация): В этом режиме работы коммутатор отправит один кадр отказа (аутентификации) EAPOL, если будет осуществляется подключение к порту, при этом любому клиенту на порту будет запрещен доступ к сети. • Port-Based 802.1X (802.1X на основе порта): В этом режиме работы требуется, чтобы сервером аутентификации был авторизован dot1x-совместимый клиент. Клиентам, не обладающим dot1x-совместимостью, доступ будет запрещен. • Single 802.1X (Аутентификация преимущественно одного устройства по 802.1X): В режиме работы Single 802.1X, аутенцифицироваться на порту будет преимущественно одно клиентское устройство, отправившее запрос на доступ к ресурсам сети. Для связи между клиентским устройством и коммутатором используются нормальные кадры EAPOL. Если к порту подключено более одного клиентского устройства, первым из них будет считаться то, которое появилось раньше всех остальных в тот период, когда порт был включен. Если такое клиентское устройство не отправило правильной учетной информации в течение заданного времени, шанс получит другое клиентское устройство. Как только клиентское устройство будет успешно аутентифицировано, только ему будет разрешен доступ. Этот режим работы является наиболее безопасным из всех поддерживаемых режимов. В этом режиме для обеспечения безопасности MAC - адреса клиентского устройства используется модуль “Port Security” (Безопасность порта) (после того, как устройство будет успешно аутентифицировано). • Multi Single 802.1X (Аутентификация многих 57 устройств по 802.1X): В режиме работы Multi 802.1X, одно или более клиентских устройств могут быть аутентифицированы на одном и том же порту в одно и то же время. Каждое клиентское устройство аутентифицируется индивидуально; его безопасность в таблице MAC - адресов обеспечивает модуль “Port Security” (Безопасность порта). • MAC-based Auth. (Авторизация на основе MAC - адресов): В отличие от аутентификации 802.1X, при аутентификации на основе MAC - адресов не принимаются и не передаются кадры EAPOL. При аутентификации на основе MAC - адресов, для половины клиентов коммутатор работает, как клиентское устройство, пославшее запрос на доступ к ресурсам сети. Начальный кадр (любого типа), отправленный клиентом, анализируется коммутатором, который, в свою очередь, использует MAC - адрес клиента в качестве имени пользователя и пароля в последующем обмене данными с RADIUS-сервером по EAP. 6-байтный MAC - адрес преобразуется в строку вида "xx-xx-xx-xx-xx-xx", где тире (-) используется в качестве символа-разделителя между шестнадцатиричными цифрами

	(записанными символами нижнего регистра). Коммутатор поддерживает только метод аутентификации MD5-Challenge, поэтому RADIUSсервер должен быть соответствующим образом сконфигурирован.
Radius-Assigned QoS Enabled	Установите флаг в этом поле, чтобы включить RADIUS-Assigned QoS на порту.
Radius-Assigned VLAN Enabled	Установите флаг в этом поле, чтобы включить RADIUS-Assigned VLAN на порту.
Guest VLAN Enabled	Установите флаг в этом поле, чтобы включить гостевую VLAN на порту.
Port State	Отображается текущее состояние порта (в смысле аутентификации 802.1X). Возможны следующие состояния: • Globally Disabled (Глобально выключен): Аутентификация по 802.1X и аутентификация по MAC-адресам глобально выключены. • Link Down (Порт выключен): Аутентификация по 802.1X и аутентификация по MAC-адресам включены, но к порту ничего не подключено. • Authorized (Авторизован): Порт принудительно переключен в авторизованный режим работы и клиентское устройство успешно авторизовано. • Unauthorized (Не авторизован): Порт принудительно переключен в не авторизованный режим работы, авторизация клиентского устройства RADIUS-сервером была неуспешной. • X Auth/Y Unauth (X авторизовано/Y не авторизовано): Порт работает в режиме с множеством клиентских устройств. X клиентских устройств авторизовано, а Y – не авторизовано.
Restart	При перезапуске аутентификации клиента используется один из методов, описанных ниже. Имейте в виду, что кнопки перезапуска работоспособны только в том случае, когда на коммутаторе глобально включен режим аутентификации (на странице System Configuration (Настройка системы), а Admin State (Административное состояние) порта имеет значение EAPOL-based (на основе EAPOL) или MAC-Based (на основе MAC-адресов). При нажатии кнопок настройки на странице изменены не будут. Reauthenticate (Повторная аутентификация): Повторная аутентификация в том случае, когда истекает период тишины на порту (аутентификация на основе EAPOL). При аутентификации на основе MAC-адресов, попытка повторной аутентификации будет предпринята немедленно. Кнопки будут работоспособны, если клиенты успешно аутентифицированы на порту, и не будут работоспособны, если клиенты временно не авторизованы. Reinitialize (Повторная инициализация): Выполняется принудительная повторная инициализация клиентов на порту, а затем – немедленная повторная аутентификация. Когда идет повторная аутентификация, клиенты будут переведены в неавторизованное состояние.

3.2.19.2 ACL. Списки доступа

ACL является последовательным списком, используемым для разрешения или запрета доступа пользователей к информации или к выполнению задач по сети. В данном коммутаторе пользователи могут задать правила, применяемые к номерам портов для разрешения или запрета операций или ограничения предельной скорости. Для доступа к настройкам необходимо перейти по вкладке Configuration→Security→Switch→Network→ACL.

ACL Ports Configuration (Конфигурирование ACL для портов) (Рис. 3.49) (Табл. 3.47).

ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	Disabled Port 1 Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	616455
3	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
8	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
9	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
10	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0

Рис. 3.49 – Конфигурирование ACL для портов

Таблица 3.47 – Конфигурирование ACL для портов

Port	Номер порта
Policy ID	Присваивает идентификатор правил списка доступа определенному порту. Порт может использовать только один идентификатор правил списка доступа, однако, идентификатор правил списка доступа может быть применен ко многим портам. По умолчанию идентификатор имеет значение 0. Допустимый диапазон значений 0~255.
Action	Разрешает или запрещает кадр на основе того, согласуется ли он с правилом из присвоенной группы правил
Rate Limiter ID	Выбирает идентификатор ограничителя скорости, применяемого к порту. Правило ограничителя скорости может быть задано на странице настройки “Rate Limiters” (Ограничители скорости).

Port Redirect	Выбор порта, на который перенаправляются согласующиеся кадры.
Mirror	Включает или выключает функцию зеркалирования. Когда функция зеркалирования включена, копии согласованных кадров будут зеркалироваться в порт назначения, заданный на странице настройки “Mirror” (Зеркало). Этим параметром задается зеркалирование порта на основе ACL, а порт зеркалирования задается на общей странице настройки зеркала, реализованной независимо. Для использования зеркалирования на основе ACL включите параметр Mirror (Зеркало) на странице ACL Ports Configuration (Настройка портов ACL). Затем откройте страницу Mirror Configuration (Настройка зеркала), в поле “Port to mirror on” (Порт, в который производится зеркалирование) задайте требуемый порт назначения, поле “Mode” (Режим работы) оставьте Disabled (Выключен).
Logging	Включает регистрацию согласующихся кадров в системном журнале. Для просмотра списка системных событий, войдите в меню System (Система), затем нажмите мышью опцию “System Log Information” (Информация системного журнала).
Shutdown	Это поле позволяет задать, следует ли отключать порт, когда согласующиеся кадры появляются на порту.
State	Выбор состояния порта: • Enabled (Включить): позволяет переоткрыть порт. • Disabled (Выключить): позволяет закрыть порт.
Counters	Число кадров, которые согласуются с правилами, определенными в выбранной группе правил.

Rate Limiters (Ограничители скорости) (Рис. 3.50) (Табл. 3.48).

ACL Rate Limiter Configuration

Rate Limiter ID	Rate	Unit
*	1	<>
1	1	pps
2	1	pps
3	1	pps
4	1	pps
5	1	pps
6	1	pps
7	1	pps
8	1	pps
9	1	pps
10	1	pps
11	1	pps
12	1	pps
13	1	pps
14	1	pps
15	1	pps
16	1	pps

Рис. 3.50 – Ограничители скорости

Таблица 3.48 – Ограничители скорости

Rate Limiter ID	Отображается идентификатор каждого ограничителя скорости
Rate	Указано пороговое значение, при превышении которого пакеты будут отбрасываться. Диапазон допустимых значений 0~3276700 pps (пакетов/сек.) или 1, 100, 200, 300…1000000 кбит/с.
Unit	Выбор единиц измерения скорости

Access Control List (Список доступа) (Рис. 3.51) (Табл. 3.49).

Список доступа задает правила фильтрации для политики доступа – для определенного порта или для всех портов. Правила, примененные к порту, начинают действовать немедленно.

Access Control List Configuration

ACE	Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter	
									⊕

Рис. 3.51 – Список доступа

Таблица 3.49 – Список доступа

Ingress Port	Входящий порт элемента списка доступа.
Policy Bitmask	Номер политики и маска битов ACE.
Frame Type	Тип кадра, согласующегося с этим правилом.

Action	Отображается тип операции - permit (разрешить) либо deny (запретить).
Rate Limiter	Отображается, включен или выключен ограничитель скорости, когда найдены согласующиеся кадры
Port Redirect	В этом поле отображается, включено или выключено перенаправление порта.
Mirror	В этом поле отображается, включена или выключена функция зеркала.
Counter	В этом поле отображается число кадров, согласующихся с какими-либо правилами, определенными для этого списка доступа.

Чтобы добавить новый элемент списка доступа нажмите мышью на знак плюс (Рис. 3.52) (Табл. 3.50).

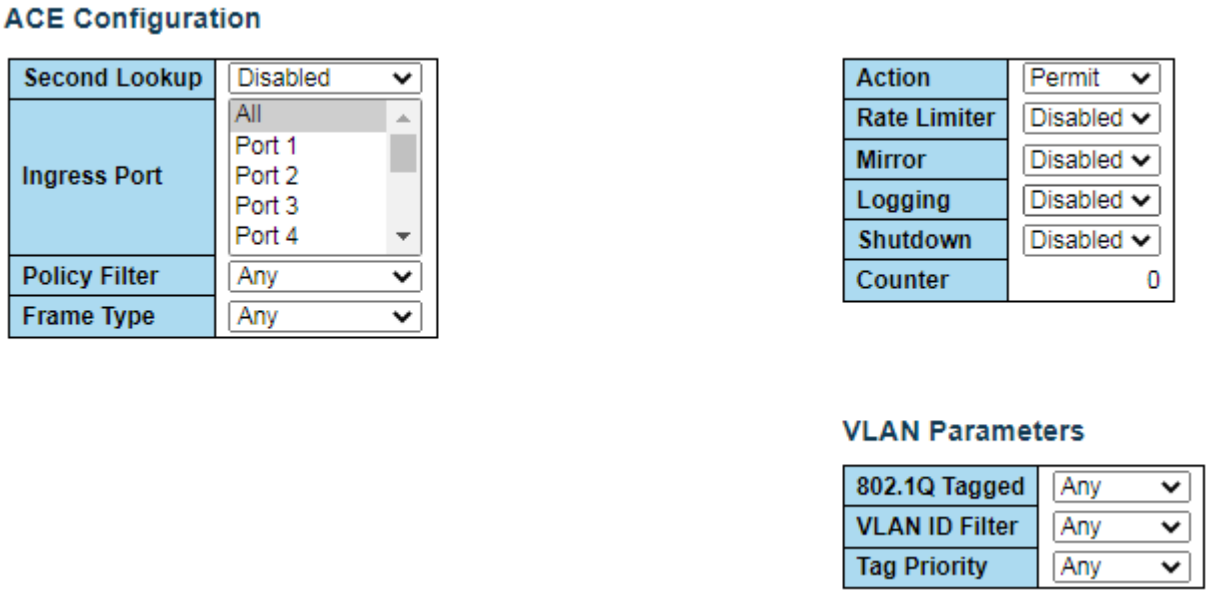


Рис. 3.52 – Новый элемент списка

Таблица 3.50 – Новый элемент списка

ACE Configuration (Настройка ACE)	
Ingress Port	Выберите входящий порт для элемента списка доступа. Выберите “All” (Все), чтобы применить правило список доступа ко всем портам либо выбрать определенный порт.
Policy Filter	Выбор типа фильтра политики. “Any” (Любой) означает, что этому правилу не присвоено фильтра политики. 63 Выберите “Specific” (Специальный), чтобы отфильтровать конкретную политику по данному ACE.
Frame Type	Выберите согласующийся тип кадра. Доступны следующие типы кадров: Any (Любой), Ethernet, ARP, IPv4. По умолчанию можно использовать любой тип кадра.
Action	Выберите тип операции - permit (разрешить) либо deny (запретить).
Rate Limiter	Позволяет включить или выключить ограничитель скорости, когда найдены согласующиеся кадры.

Mirror	Позволяет включить или выключить функцию зеркала.
Logging	Позволяет включить или выключить регистрацию в системном журнале для согласующихся кадров.
Shutdown	Позволяет включить или выключить отключение порта для согласующихся кадров.
Counter	В этом поле отображается число кадров, согласующихся с какими-либо правилами, определенными для этого списка доступа.
VLAN Parameters (Параметры VLAN)	
802.1Q Tagged	Позволяет выбрать, должны ли кадры содержать теги (то есть быть тегированными).
VLAN ID Filter	Позволяет выбрать фильтр VLAN ID для данного ACE. • Any (Любой): фильтр VLAN ID не задан. • Specific (Специальный): позволяет задать номер VLAN ID. Кадр с заданным номером VLAN ID, согласующийся с данным правилом ACE.
Tag Priority	Позволяет выбрать значение User Priority (Приоритет пользователя), найденного в теге VLAN для согласования с данным правилом.

3.2.19.3 IP Source Guard. Защита IP-адреса источника

Для доступа к настройкам необходимо перейти по вкладке Configuration→Security→Switch→Network→ IP Source Guard. Configuration (Настройка) (Рис. 3.53) (Табл. 3.51).

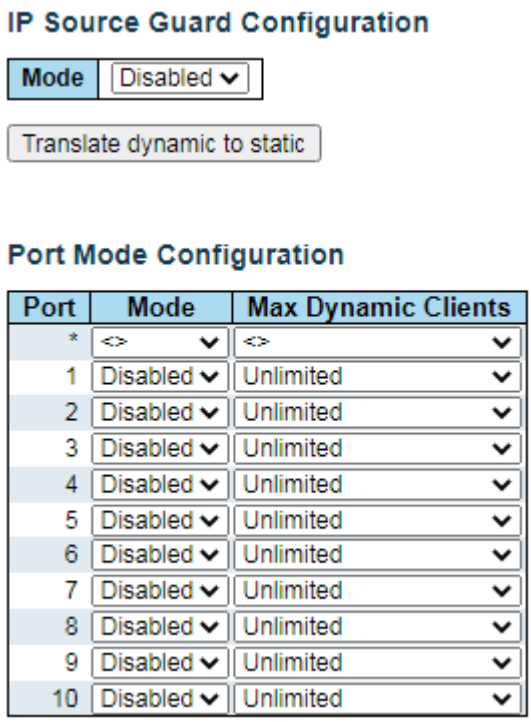


Рис. 3.53 – Настройка

Таблица 3.51 – Настройка

IP Source Guard Configuration (Настройка защиты IP-адреса источника)	
Mode	Включение или выключение защиты IP-адреса источника (глобальное)
Translate dynamic to static	Нажмите на эту кнопку, чтобы преобразовать динамические записи в статические.
Port Mode Configuration (Настройка режима работы порта)	
Port	Номер порта. “*” означает применение ко всем портам.
Mode	Включение или выключение защиты IP-адреса источника на порту. Пожалуйста, имейте в виду, для того, чтобы защита IP-адресов источника работала, должны быть включены и глобальный режим работы, и режим работы на порту.
Max Dynamic Clients	Выберите максимальное число динамических клиентов, которые могут быть обучены на порту. Возможны следующие варианты: 0, 1, 2, unlimited (неограниченное количество). Если включен режим работы порта и максимальное число клиентов равно 0, коммутатор будет только передавать IP-пакеты, которые согласуются со статическими элементами списка (IP-адресами) для данного порта.

Static Table (Таблица статических записей) (Рис. 3.54) (Табл. 3.52).

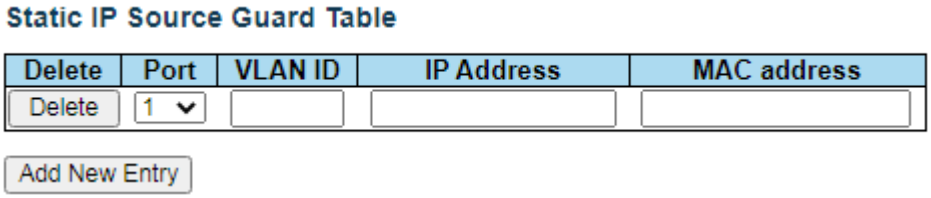


Рис. 3.54 – Таблица статических записей

Таблица 3.52 – Таблица статических записей

Delete	Удалить текущую запись
Port	Порт для которого создается статическая запись.
VLAN ID	Введите ранее сконфигурированный номер VLAN ID.
IP Address	Введите корректный IP-адрес.
MAC Address	Введите корректный MAC-адрес.

Кнопка Add New Entry служит для добавления новой записи.

3.2.19.4 IPv6 Source Guard. Защита IPv6-адреса источника

Для доступа к настройкам необходимо перейти по вкладке Configuration→Security→Switch→Network→ IPv6 Source Guard . Configuration (Настройка) (Рис. 3.55) (Табл. 3.53).

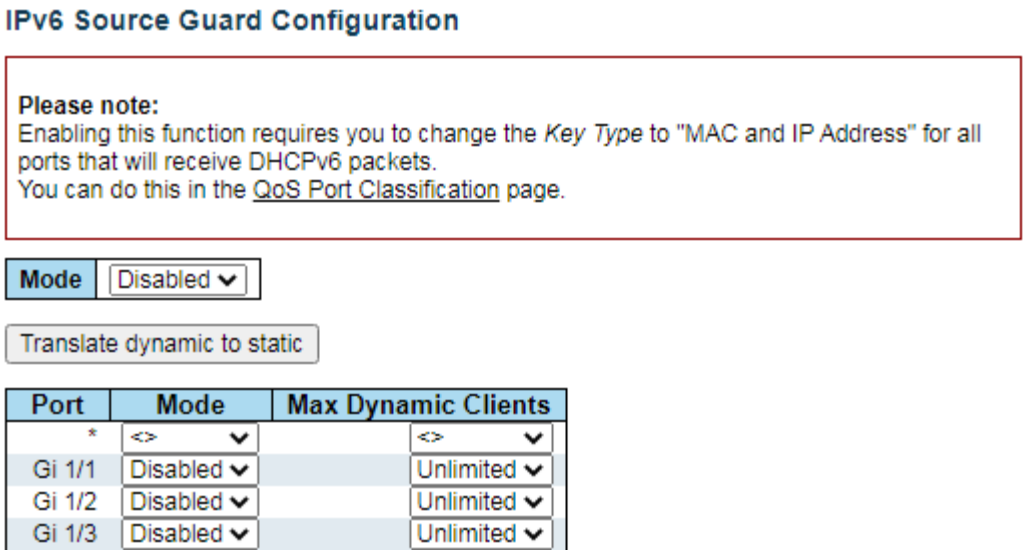


Рис. 3.55 – Настройка

Таблица 3.53 – Настройка

IPv6 Source Guard Configuration (Настройка защиты IPv6-адреса источника)	
Mode	Включение или выключение защиты IPv6-адреса источника (глобальное)
Translate dynamic to static	Нажмите на эту кнопку, чтобы преобразовать динамические записи в статические.
Port Mode Configuration (Настройка режима работы порта)	
Port	Номер порта. “*” означает применение ко всем портам.
Mode	IPv6 Source Guard может быть включен / отключен на отдельных портах. IPv6 Source Guard включен только в том случае, если на данном порте включены и глобальный режим, и режим порта.
Max Dynamic Clients	Укажите максимальное количество динамических клиентов, которые могут быть изучены на данном порту. Это значение может быть 0, 1, 2 или неограниченно. Если режим порта включен и значение max dynamic client равно 0, пересылаются только IPv6-пакеты, которые совпадают в статических записях на конкретном порту.

IPv6 Source Guard Static Table (Таблица статических записей ipv6) (Рис. 3.56) (Табл. 3.54).

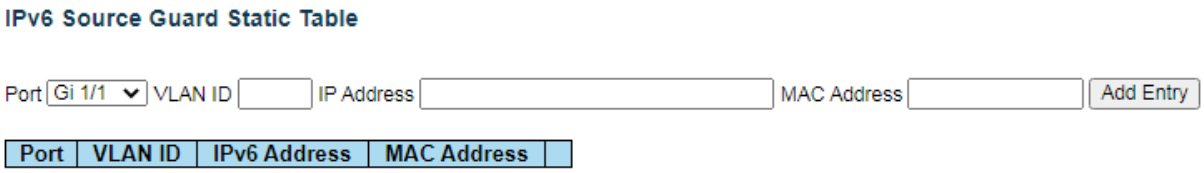


Рис. 3.56 – Таблица статических записей

Таблица 3.54 – Таблица статических записей

Port	порт, к которому привязана запись

VLAN ID	Идентификатор VLAN для записи. Если с записью не связан идентификатор VLAN, в этом поле отображается 0.
IPv6 Address	Разрешенный IPv6-адрес.
MAC Address	Разрешенный MAC-адрес.

Чтобы добавить запись нажмите кнопку Add Entry

3.2.19.5 ARP inspection. Инспекция ARP

Для доступа к настройкам необходимо перейти по вкладке Configuration→Security→Switch→Network→ ARP inspection.

Port Configuration (Настройка порта) (Рис. 3.57) (Табл. 3.55).

ARP Inspection Configuration

Mode	Disabled

Translate dynamic to static

Port Mode Configuration

Port	Mode	Check VLAN	Log Type
*	<>	<>	<>
1	Disabled	Disabled	None
2	Disabled	Disabled	None
3	Disabled	Disabled	None
4	Disabled	Disabled	None
5	Disabled	Disabled	None
6	Disabled	Disabled	None
7	Disabled	Disabled	None
8	Disabled	Disabled	None
9	Disabled	Disabled	None
10	Disabled	Disabled	None

Рис. 3.57 – Настройка порта

Таблица 3.55 – Настройка порта

ARP Inspection Configuration (Настройка инспекции ARP)	
Mode	Включает или выключает функцию инспекции ARP глобально.
Port Mode Configuration (Настройка режима работы порта)	
Port	Номер порта. “*” означает применение ко всем портам
Mode	Включает или выключает функцию инспекции ARP на порту. Пожалуйста, имейте в виду, для того, чтобы функция инспекции ARP работала, должны быть включены и глобальный режим работы, и режим работы на порту.
Check VLAN	Включает или выключает проверку VLAN.
Log Type	Доступно четыре типа журналов: • None (Нет): Журнала нет.

	• Deny (Запрещенные): В журнал помещаются запрещенные элементы списка. • Permit (Разрешенные): В журнал помещаются разрешенные элементы списка. • All (Все): В журнал помещаются все элементы списка.

VLAN Configuration (Настройка VLAN) (Рис. 3.58) (Табл. 3.56).

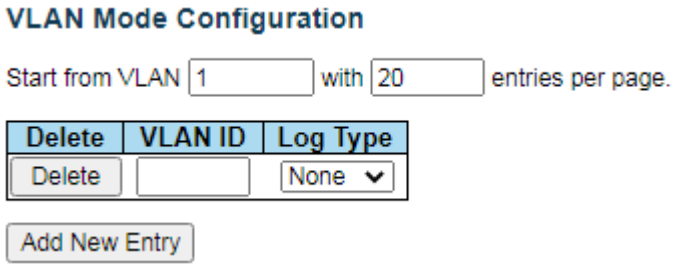


Рис. 3.58 – Настройка VLAN

Таблица 3.56 – Настройка VLAN

Delete	Удалить текущую запись
VLAN ID	Позволяет задать, на каких сетях VLAN включена функция инспекции ARP. Во-первых, необходимо включить настройки порта на web-странице Port mode configuration (Настройка режима работы порта). Только тогда, когда для данного порта включены и Global Mode (Глобальный режим работы) и Port Mode (Режим работы порта), функция ARP Inspection включена на данном порту. Во-вторых, на web-странице VLAN mode configuration (Настройка режима VLAN) можно задать, какие VLAN будут проинспектированы. Тип журнала также можно настроить отдельно для каждой VLAN.
Log Type	Доступно четыре типа журналов. • None (Нет): Журнала нет. • Deny (Запрещенные): В журнал помещаются запрещенные элементы. • Permit (Разрешенные): В журнал помещаются разрешенные элементы. • All (Все): В журнал помещаются все элементы.

Кнопка 

служит для добавления новой записи.

Static Table (Таблица статических адресов) (Рис. 3.59) (Табл. 3.57).

Static ARP Inspection Table

Delete	Port	VLAN ID	MAC Address	IP Address
Delete	1			

Add New Entry

Рис. 3.59 – Таблица статических адресов

Таблица 3.57 – Таблица статических адресов

Delete	Удалить текущую запись
Port	Порт, для которого создается статическая запись.
VLAN ID	Позволяет задать номер VLAN ID.
MAC Address	Укажите допустимый MAC - адрес источника.
IP Address	Укажите допустимый IP-адрес

Кнопка Add New Entry служит для добавления новой записи.

Dynamic Table Status (Состояние динамической таблицы) (Рис. 3.60) (Табл. 3.58).

Dynamic ARP Inspection Table

Start from Port 1 , VLAN 1 , MAC address 00-00-00-00-00-00 and IP address 0.0.0.0 with 20 entries per page.

Port	VLAN ID	MAC Address	IP Address	Translate to static
No more entries				

Рис. 3.60 – Состояние динамической таблицы

Таблица 3.58 – Состояние динамической таблицы

Port	Номер порта для данного элемента таблицы.
VLAN ID	Номер сети VLAN ID, в которой разрешен трафик ARP.
MAC Address	Пользовательский MAC - адрес данного элемента таблицы.
IP Address	Пользовательский IP-адрес данного элемента таблицы.

3.2.20 RADIUS

Для доступа к настройкам необходимо перейти по вкладке Configuration→Security→Switch→Network→AAA→Radius.

Configuration (Настройка) (Рис. 3.61) (Табл. 3.59).

RADIUS Server Configuration

Global Configuration

Timeout	5	seconds
Retransmit	3	times
Deadtime	0	minutes
Change Secret Key	No	
NAS-IP-Address		
NAS-IPv6-Address		
NAS-Identifier		

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Change Secret Key
Delete		1812	1813			

Add New Server

Рис. 3.61 – Настройка Radius

Таблица 3.59 – Настройка Radius

Global Configuration (Глобальные настройки)	
Timeout	Время, которое коммутатор ожидает ответа от сервера аутентификации перед тем, как повторить запрос.
Retrasmit	Укажите число раз повторной передачи запросных пакетов на сервер аутентификации, который не отвечает. Если сервер не ответил после последней повторной передачи, коммутатор считает, что сервер аутентификации отсутствует.
Deadtime	Deadtime (Время отсутствия сервера) – это время, в течение которого коммутатор не будет посылать новые запросы на сервер, который не ответил на предыдущий запрос. В результате, коммутатор не будет постоянно пытаться установить контакт с сервером, который уже квалифицирован, как отсутствующий. Если присвоить Deadtime значение, большее нуля (0), то эта функция будет включена, но только в том случае, если сконфигурировано более одного сервера. Допустимый диапазон Deadtime: от 0 до 1440 минут.
Change Secret Key	Выбор секретного ключа
Key	Укажите секретный ключ длиной не более 64 символов. Он будет доступен RADIUS-серверу и коммутатору.
NAS-IP- Address	Адрес IPv4, использованный в качестве атрибута 4 в пакетах запроса доступа RADIUS. Если это поле оставить пустым, будет использован IP-адрес исходящего интерфейса.
NAS-IPv6-Address	Адрес IPv6, использованный в качестве атрибута 95 в пакетах запроса доступа RADIUS. Если это поле оставить пустым, будет использован IP-адрес исходящего интерфейса.
NAS Identifer	Идентификатор длиной не более 256 символов, используемый в качестве атрибута 32 в пакетах запроса доступа RADIUS. Если это поле оставить пустым, идентификатор NAS не будет включен в пакет.
Server Configuration (Настройка сервера)	
Hostname	Имя хоста RADIUS-сервера или его IP-адрес.
Auth Port	Порт UDP, используемый на RADIUS-сервере для аутентификации.

Acct Port	Порт UDP, используемый на RADIUS-сервере для аккаунтинга.
Timeout	Если в этом поле указано время ожидания, оно будет использовано вместо глобального времени ожидания. Если желательно использовать глобальное значение, оставьте это поле пустым.
Retransmit	Если в этом поле указано значение времени повторной передачи, оно будет использовано вместо глобального значения времени повторной передачи. Если желательно использовать глобальное значение, оставьте это поле пустым.
Change Secret Key	Если в этом поле указано значение секретного ключа, оно будет использовано вместо глобального значения секретного ключа. Если желательно использовать глобальное значение, оставьте это поле пустым.

Кнопка [Add New Server] служит для добавления сервера.

Примечание. Сервер, указанный первым в списке, считается основным.

3.2.21 TACACS+

Для доступа к настройкам необходимо перейти по вкладке Configuration→Security→Switch→Network→AAA→TACACS+.

Configuration (Настройка) (Рис. 3.62) (Табл. 3.60)

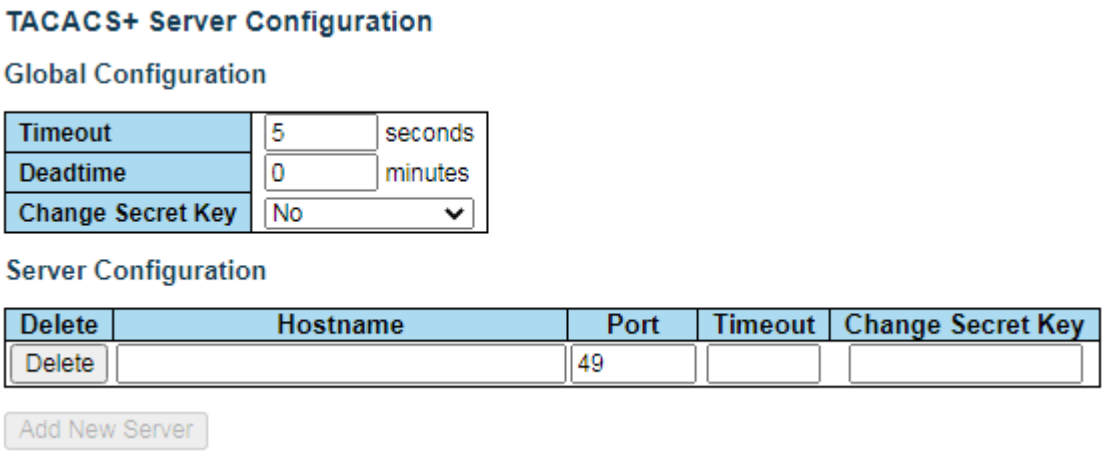


Рис. 3.62 – Настройка TACACS+

Таблица 3.60 – Настройка TACACS+

Global Configuration (Глобальные настройки)	
Timeout	Время, которое коммутатор ожидает ответа от сервера TACACS+ перед тем, как повторно передать запрос.
Deadtime	Deadtime (Время отсутствия сервера) – это время, в течение которого коммутатор не будет посылать новые запросы на сервер, который не ответил на предыдущий запрос. В результате, коммутатор не будет постоянно пытаться установить контакт с сервером, который уже квалифицирован, как отсутствующий. Если присвоить Deadtime значение, большее нуля (0), то эта функция

	будет включена, но только в том случае, если сконфигурировано более одного сервера. Допустимый диапазон Deadtime: от 0 до 1440 минут.
Change Secret Key	Выбор секресного ключа
Key	Укажите секретный ключ длиной не более 63 символов. Он будет доступен серверу TACACS+ и коммутатору
Server Configuration (Настройка сервера)	
Hostname	Имя хоста сервера TACACS+ или его IP-адрес.
Port	Номер порта TCP, используемого на сервере TACACS+ для аутентификации.
Timeout	Если в этом поле указано время ожидания, оно будет использовано вместо глобального времени ожидания. Если желательно использовать глобальное значение, оставьте это поле пустым.
Change Secret Key	Если в этом поле указано значение секретного ключа, оно будет использовано вместо глобального значения секретного ключа. Если желательно использовать глобальное значение, оставьте это поле пустым.

Кнопка Add New Server служит для добавления сервера.

Примечание. Сервер, указанный первым в списке, считается основным.

3.2.22 Aggregation. Агрегирование

При агрегировании линии используется параллельная работа множества портов, в результате чего скорость обмена данными по линии увеличивается. Используется два типа агрегирования: статический и LACP.

Для доступа к настройкам необходимо перейти по вкладке Configuration→ Aggregation. **Common Aggregation Configuration (Рис. 3.63) (Табл. 3.61).**

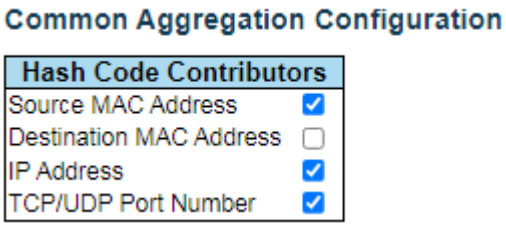


Рис. 3.63 – Настройка агрегирования

Таблица 3.61 – Настройка агрегирования

настройка режима работы агрегирования	
Source MAC Address	MAC-адрес источника используется для расчета линейного порта, через который будет передаваться кадр.
Destination MAC Address	MAC-адрес назначения используется для расчета линейного порта, через который будет передаваться кадр.
IP Address	IP-адрес используется для расчета линейного порта, через который

	будет передаваться кадр.
TCP/UDP Port Number	Порты TCP/UDP назначения и источника используются для расчета линейного порта, через который будет передаваться кадр.

Настройка группы агрегирования (Рис. 3.64) (Табл. 3.62).

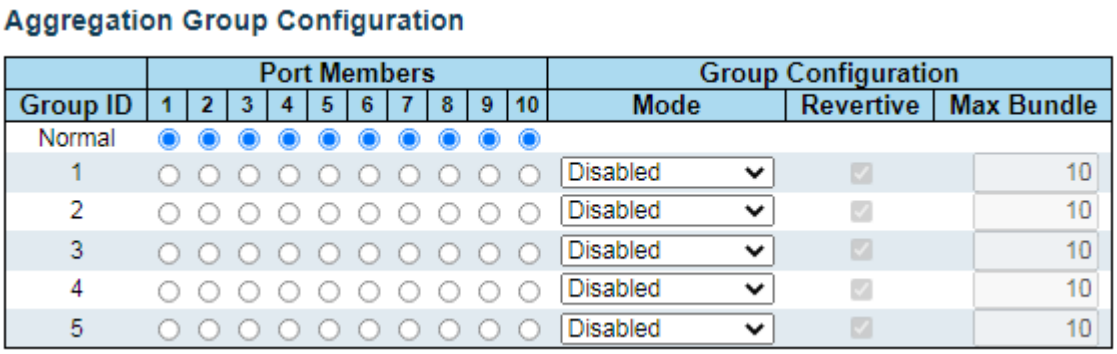


Рис. 3.64 – Настройка группы агрегирования

Таблица 3.62 – Настройка группы агрегирования

Настройка группы агрегирования	
Group ID	Номер, идентифицирующий магистраль. “Normal” (Обычный режим работы) означает, что агрегирование не используется. Каждая группа содержит не менее 2 и не более 10 линий (портов). Пожалуйста, имейте в виду, что в каждой группе каждый порт может использоваться только один раз.
Port Members	Выберите порты, принадлежащие магистрали
Mode	Выбор режима для группы агрегации • Disabled: группа отключена. • Static: группа работает в режиме статической агрегации. • LACP (Active): группа работает в режиме активной агрегации • LACP (Passive): группа работает в режиме пассивной агрегации
Revertive	Этот параметр применяется только к группам с включенным LACP. Он определяет, будет ли группа выполнять автоматический (повторный) расчет ссылок, когда становятся доступными ссылки с более высоким приоритетом.
Max Bundle	Этот параметр применяется только к группам с включенным LACP. Он определяет максимальное количество активных объединенных портов LACP, разрешенных в агрегации.

Коммутатор поддерживает протокол LACP (Link Aggregation Control Protocol – протокол управления агрегированием линии), который специфицирован в IEEE 802.3ad. Статические магистрали должны быть сконфигурированы вручную на обоих концах

линии. Другими словами, порты, на которых сконфигурирован LACP, могут автоматически согласовывать магистральную линию с портами других устройств, на которых также сконфигурирован LACP. На коммутаторе может быть сконфигурировано любое число портов LACP, однако они не должны при этом быть частью статической магистрали. Если порты на других устройствах также сконфигурированы, как LACP, коммутатор и другие устройства будут согласовывать свои параметры для работы по магистральной линии между ними.

LACP Configuration (Настройка LACP) (Рис. 3.65) (Табл. 3.63).

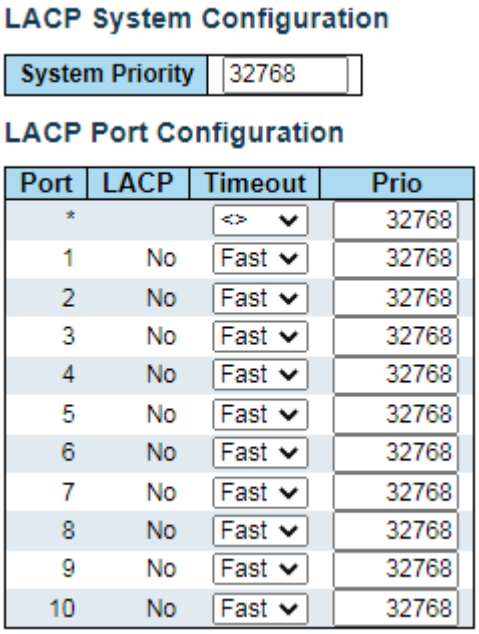


Рис. 3.65 – Настройка LACP

Таблица 3.63 – Настройка LACP

LACP System Configuration	
System Priority	Приоритет системы
LACP Port Configuration	
Port	Номер порта. “*” означает применение ко всем портам.
LACP	Показывает, включен ли LACP в данный момент на этом порту коммутатора.
Timeout	Параметр Timeout (Время ожидания) определяет период времени между передачами BPDU. Когда параметр имеет значение Fast (Быстро), пакеты LACP будут передаваться каждую секунду; когда параметр имеет значение Slow (Медленно), перед отправкой пакета LACP будет выдержан интервал 30 секунд.
Prio	Чем меньше это целое число, тем больше приоритет. Это значение приоритета определяет, какой порт будет активен, а какой – будет играть роль резервного.

3.2.23 Link OAM.

Link OAM дает операторам сети возможность отслеживать состояние сети и быстро определять местоположение неисправных каналов или неисправных состояний.

Для доступа к настройкам необходимо перейти по вкладке Configuration→ Link OAM.

Link OAM Port Configuration (Настройка портов) (Рис. 3.66) (Табл. 3.64).

Link OAM Port Configuration

Port	OAM Enabled	OAM Mode	Loopback Support	Link Monitor Support	MIB Retrieval Support	Loopback Operation
*	☑	<>	☑	☑	☑	☐
1	☑	Active	☑	☑	☑	☐
2	☑	Active	☑	☑	☑	☐
3	☑	Active	☑	☑	☑	☐
4	☑	Active	☑	☑	☑	☐
5	☑	Active	☑	☑	☑	☐
6	☑	Active	☑	☑	☑	☐
7	☑	Active	☑	☑	☑	☐
8	☑	Active	☑	☑	☑	☐
9	☐	Passive	☐	☑	☐	☐
10	☐	Passive	☐	☑	☐	☐

Рис. 3.66 – Настройка портов

Таблица 3.64 – Настройка портов

System Priority	Приоритет системы
Port	Номер порта. “*” означает применение ко всем портам.
OAM Enabled	Включение/выключение Link OAM на порту коммутатора.
OAM Mode	Выбор режима OAM как активный или пассивный. По умолчанию установлен пассивный режим. active - DTE, настроенные в активном режиме, инициируют обмен информационными OAMPDU, как определено в процессе обнаружения. После завершения процесса обнаружения активным DTE разрешается отправлять любые OAMPDU при подключении к удаленному одноранговому объекту OAM в активном режиме. Активные DTE работают в ограниченном отношении, если удаленный объект OAM работает в пассивном режиме. Активные устройства не должны отвечать на команды удаленной обратной связи OAM и запросы переменных от пассивного однорангового узла. passive - DTE, настроенные в пассивном режиме, не инициируют процесс обнаружения. Пассивные DTE реагируют на инициирование процесса обнаружения удаленным DTE. Это исключает возможность перехода от пассивных к пассивным ссылкам. Пассивные DTE не должны отправлять запросы переменных или OAMPDU управления шлейфом.
Loopback Support	Включение/выключение функции петли
Link Monitor Support	Включение/выключение функции мониторинга на порту.
MIB Retrieval	Включение/выключение поддержки MIB на порту коммутатора

Support	
Loopback Operation	Если поддержка обратной связи включена, включение этого поля запустит операцию обратной связи для порта.

Link Event Configuration for Port (настройка событий для порта) (Рис. 3.67) (Табл. 3.65).

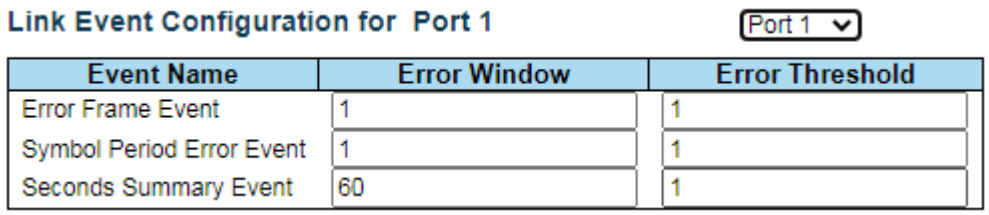


Рис. 3.67 – настройка событий

Таблица 3.65 – настройка событий

System Priority	Приоритет системы
Port	Номер порта коммутатора.
Event Name	Error Frame Event - Событие ошибочного кадра подсчитывает количество ошибочных кадров, обнаруженных в течение указанного периода. Symbol Period Error Event - Событие периода ошибочного символа подсчитывает количество ошибок символа, произошедших за указанный период. Seconds Summary Event - Событие подсчитывает количество секунд с ошибками, произошедших в течение указанного периода.
Error Window	Представляет период окна порядка 1 секунды для наблюдения за различными событиями связи.
Error Threshold	Представляет пороговое значение для периода окна для соответствующего события связи, чтобы уведомить одноранговый узел об этой ошибке.

3.2.24 Loop protection. Защита от петель

Вследствие неправильного выполнения соединений, проблем с аппаратурой, неправильной настройки протоколов, в сетях иногда возникают петли. В коммутируемых сетях петли потребляют ресурсы коммутатора, в результате чего падает его производительность. Функция Loop Protection (Защита от петель), реализованная в данном коммутаторе, может быть включена глобально либо индивидуально на каждом порту. Использование функции защиты от петель дает возможность коммутатору автоматически обнаруживать петли в сети. При обнаружении петель, порты, принявшие от коммутатора пакет защиты от петель, 74 могут быть отключены либо соответствующие события могут быть зарегистрированы в журнале.

Для доступа к настройкам необходимо перейти по вкладке Configuration→ Loop protection. (Рис. 3.68) (Табл. 3.66).

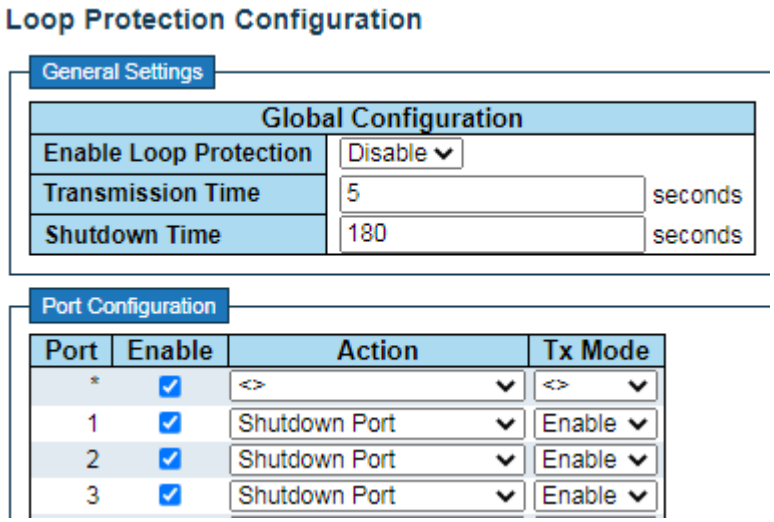


Рис. 3.68 – Защита от петель

Таблица 3.66 – Защита от петель

General Settings (Основные настройки)	
Enable Loop protection	Позволяет включить или выключить функцию защиты от петель.
Transmission Time	Интервал между отправкой пакетов защиты от петель PDU на каждом порту. Допустимые значения: от 1 до 10 секунд.
Shutdown Time	Период времени, на который порт будет выключен. Допустимые значения: от 0 до 604800 секунд. 0 означает, что порт будет оставаться выключенным до тех пор, пока устройство не будет перезагружено.
Port Configuration (Настройка порта)	
Port	Список номеров портов. “*” означает применение ко всем портам.
Enable	Позволяет включить или выключить функцию защиты от петель на выбранных портах.
Action	Когда на порту обнаружена петля, функция защиты от петель немедленно выполнит соответствующие операции. Операции могут быть следующими: • Shutdown Port (Отключить порт): Порт, на котором обнаружены петли, отключается на период времени, заданный в поле “Shutdown Time” (Период времени отключения). • Shutdown Port and Log (Выключить порт, но вести регистрацию в журнале): Порт, на котором обнаружены петли, отключается на период времени, заданный в поле “Shutdown Time” (Период времени отключения), но события регистрируются в журнале. • Log Only (Только регистрировать в журнале): События регистрируются в журнале, но порт остается включенным.
Tx Mode	Включает или выключает генерацию пакетов защиты от петель PDU либо осуществляется пассивный поиск PDU, переданных по петле.

3.2.25 Spanning Tree

При некоторых услугах, предоставляемых по сети необходимо, чтобы соединения были всегда включены – это гарантирует конечным пользователям выполнение требующихся им операций в режиме «онлайн», которые не должны прерываться неожиданными разрывами соединений. В таких обстоятельствах, для предотвращения разрывов соединений устанавливается множество активных маршрутов между узлами сети. Однако, наличие множества соединяющихся друг с другом маршрутов увеличивает вероятность образования петель (мостов), которые делают сеть нестабильной, а в наихудшем случае – неработоспособной. Например, таблица MAC-адресов, используемая коммутатором или мостом, может отказать вследствие того, что одни и те же MAC-адреса (и следовательно – одни и те же хосты сети) видны на множестве портов. Во-вторых, может произойти широковещательный шторм. Он обусловлен передачей широковещательных пакетов между коммутаторами по бесконечной петле. Широковещательный шторм может захватить все доступные ресурсы CPU и всю полосу пропускания.

Для решения проблем, связанных с мостами, протокол STP допускает сети, включающие резервные линии, которые обеспечивают автоматические резервные маршруты в том случае, если отказывает активная линия, при этом не возникает опасности образования петель и не требуется вручную включать или отключать резервные линии.

Протокол STP (Spanning Tree Protocol) определен в стандарте IEEE Standard 802.1s. Он позволяет создать топологию в смешанной сети с подключенными мостами 2-го уровня (в типичном случае - Ethernet-коммутаторами) и отключать линии, не являющиеся частью дерева, оставляя один активный маршрут между двумя любыми узлами сети.

Для обеспечения быстрой сходимости после изменения топологии сети, введен протокол, являющийся развитием IEEE Standard 802.1s - RSTP (Rapid Spanning Tree Protocol (IEEE 802.1w)). Протокол RSTP – это улучшенный STP, поэтому эти протоколы имеют сходные основные характеристики. Важно, что создается эффект каскадного соединения – начиная с корневого моста, от которого каждый назначенный (некорневой) мост предлагает своим соседям определить – возможен ли быстрый переход. Это является одним из основных элементов, которые обеспечивают ускоренную сходимость RSTP по сравнению с STP.

Другим расширением RSTP является IEEE 802.1s – MSTP (Multiple Spanning Tree protocol), который позволяет различным сетям VLAN использовать отдельные копии протокола. В отличие от STP и RSTP, MSTP устраняет необходимость иметь различные STP для каждой VLAN. Поэтому в больших сетевых средах, в которых эксплуатируется множество VLAN, MSTP может оказаться полезнее, чем традиционно используемый STP.

Для доступа к настройкам необходимо перейти по вкладке Configuration→ Spanning Tree.

Bridge Settings (Настройки моста) (Рис. 3.69) (Табл. 3.67).

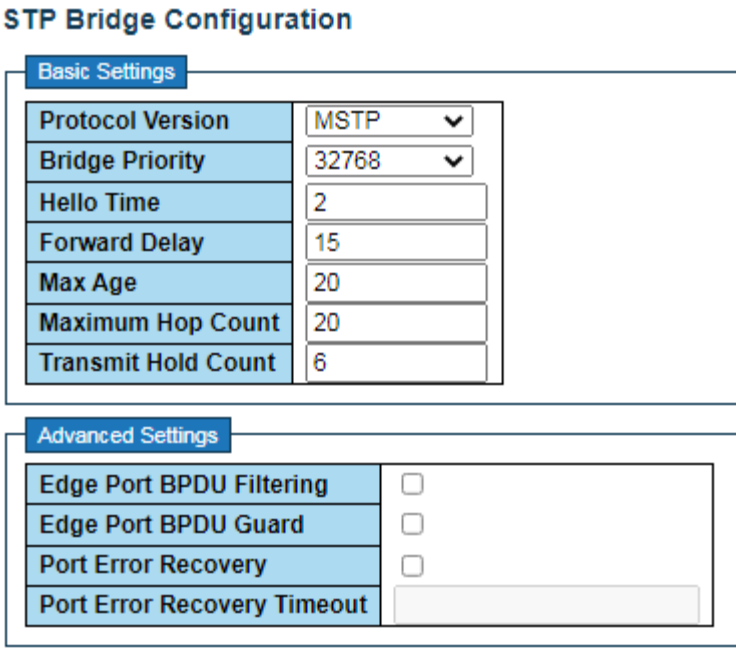


Рис. 3.69 – Настройки моста

Таблица 3.67 – Настройки моста

Basic Settings (Основные настройки)	
Protocol Version	Выберите соответствующий протокол. Версии протокола следующие: “STP”, “RSTP” и “MSTP”.
Bridge Priority	Каждый коммутатор имеет относительный приоритет и стоимость пути, которые используются для принятия решения о кратчайшем маршруте для передачи пакетов. Маршрут с наименьшей стоимостью (с наименьшим численным значением) имеет наивысший приоритет и используется всегда, пока не будет выключен. Если имеется множество мостов и интерфейсов, то для получения оптимальной производительности необходимо настроить их приоритеты. При MSTP – это приоритет CIST. В остальных случаях – это приоритет моста STP/RSTP.
Hello Time	Интервал между отправкой пакетов STP BPDU. Допустимые значения находятся в диапазоне от 1 до 10 секунд, по умолчанию - 2 секунды. Примечание. Изменение значения этого параметра по умолчанию не рекомендуется и может иметь неблагоприятные последствия для вашей сети.
Forward Delay	Для мостов STP, Forward Delay – это время, проведенное в каждом из состояний – Listening (Прослушивание) и Learning (Обучение) до перехода в состояние Forwarding (Передача пакетов). Данная задержка возникает, когда в сеть включается новый мост. Допустимые значения: от 4 до 30 секунд.
Max Age	Если другой коммутатор не пошлет конфигурационный пакет в течение заданного периода времени, он считается отключенным. Допустимый диапазон значений: от 6 до 40 секунд, значение Max Age должно быть меньше или равно (Forward Delay-1)*2.

Maximum Hop Count	Максимальное число участков между коммутаторами, после прохождения которых, пакет BPDU будет отброшен. При прохождении каждого моста пакетом BPDU, значение счетчика уменьшается на единицу. Когда счетчик участков маршрута станет равным нулю, пакет BPDU будет отброшен. По умолчанию число участков равно 20. Диапазон допустимых значений 6 – 40.
Transmit Hold Count	Число пакетов BPDU, посылаемых портом моста в секунду. Когда это значение превышено, передача следующего пакета BPDU будет задержана. По умолчанию задано 6 секунд. Допустимый диапазон значений: от 1 до 10. Пожалуйста, имейте в виду, что при увеличении этого значения может значительно возрасти загрузка CPU; при уменьшении значения замедляется сходимость алгоритма. Рекомендуется оставить для Transmit Hold Count значение, заданное по умолчанию.
Advanced Settings (Дополнительные настройки)	
Edge Port BPDU Filtering	Фильтрация BPDU на граничном порту. Целью фильтрации пакетов BPDU на порту является предотвращение отправки с коммутатора кадров BPDU на порты, которые подключены к конечным устройствам.
Edge Port BPDU Guard	Защита BPDU на граничном порту. Граничные порты обычно напрямую подключены к ПК, файл-серверам или принтерам. Поэтому граничные порты сконфигурированы таким образом, чтобы обеспечивалось быстрое изменение состояния. В нормальных ситуациях, граничные порты не должны принимать конфигурационные BPDU. Однако, если они принимают их, то вероятно, вследствие атак злоумышленников или неправильных настроек. Когда граничные порты принимают конфигурационные BPDU, они будут автоматически переключены в состояние неграничных портов и запустится процесс вычисления новой топологии STP. В связи с этим, для защиты устройства от атак злоумышленников применяется BPDU guard. Если граничные порты приняли конфигурационные BPDU, когда эта функция включена, то STP отключит те из них, которые приняли конфигурационные BPDU. По истечении периода времени восстановления эти выключенные порты вновь будут включены.
Port Error Recovery	Восстановление порта после ошибки. Порт, выключенный из-за ошибки, может быть автоматически включен по прошествии определенного времени.
Port Error Recovery Timeout	Время, которое должно пройти до того момента, когда порт, выключенный из-за ошибки, будет включен вновь. Допустимый диапазон значений от 30 до 86400 секунд.

MSTI Mapping (Отображение MSTI) (Рис. 3.70) (Табл. 3.68)

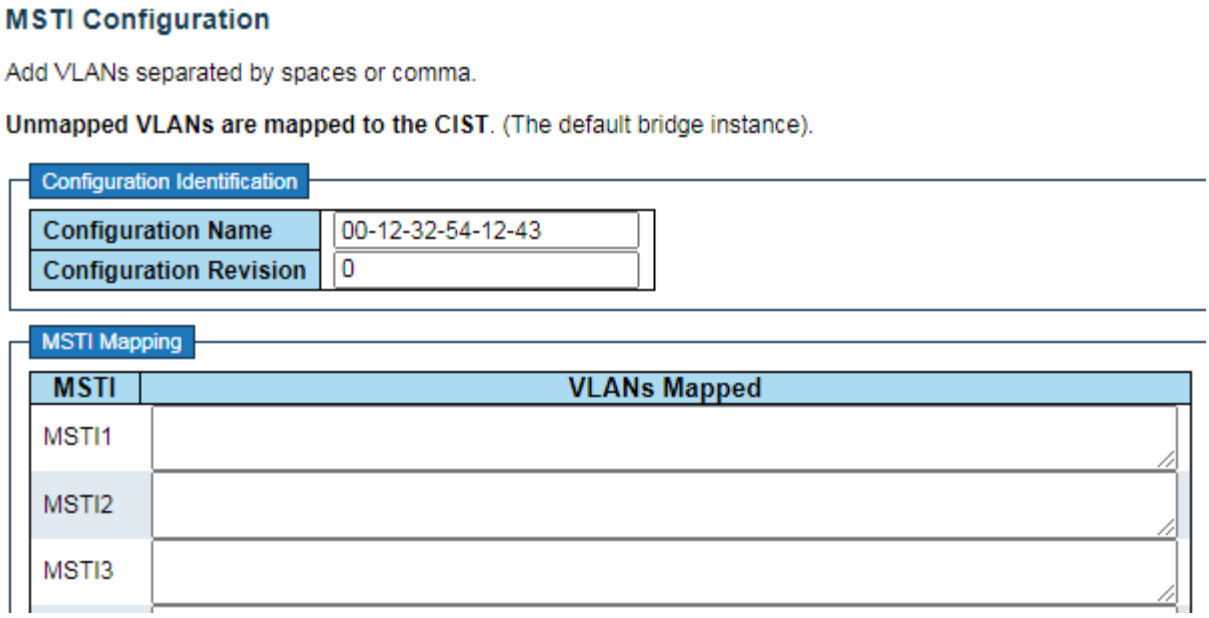


Рис. 3.70 – Отображение MSTI

Таблица 3.68 – Отображение MSTI

Configuration Identification (Идентификационные данные конфигурации)	
Configuration Name	Имя MSTI. По умолчанию используется MAC-адрес коммутатора. Максимальная длина 32 символа. Для того, чтобы совместно использовать STP для MSTI, мосты должны иметь одинаковые имена конфигураций и номера версий конфигураций.
Configuration Revision	Номер версии для MSTI. Допустимый диапазон значений: от 1 до 65535.
MSTI Mapping (Отображение MSTI)	
MSTI	Номер копии MSTI.
VLAN Mapped	Задайте номера сетей VLAN, которые будут привязаны к MSTI. Можно ввести как одну VLAN, так и диапазон номеров VLAN. Номера VLAN можно отделять запятыми и использовать тире для указания диапазона VLAN. (Пример: 2,5,20-40). Для неиспользуемых MSTI оставьте поле пустым.

MSTI Priorities (Приоритеты MSTI) (Рис. 3.71) (Табл. 3.69).

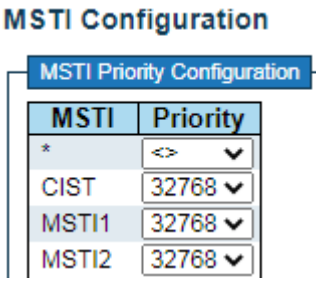


Рис. 3.71 – Приоритеты MSTI

Таблица 3.69 – Приоритеты MSTI

MSTI	Отображается номер копии MSTI. “*” – правило приоритета применяется ко всем портам.
Priority	Выберите соответствующий приоритет для каждой копии MSTI. Приоритет моста используется при выборе корневого устройства, корневого порта и назначенного порта. Устройство с наивысшим приоритетом становится корневым устройством. Однако, если все устройства имеют одинаковый приоритет, корневым устройством станет устройство с наименьшим MAC-адресом. Имейте в виду, что чем меньше численное значение, тем выше приоритет. Идентификатор моста формируется конкатенацией следующего: приоритет моста плюс номер копии MSTI, конкатенированный с 6- байтным MAC-адресом коммутатора.

CIST Ports (Порты CIST) (Рис. 3.72) (Табл. 3.70).

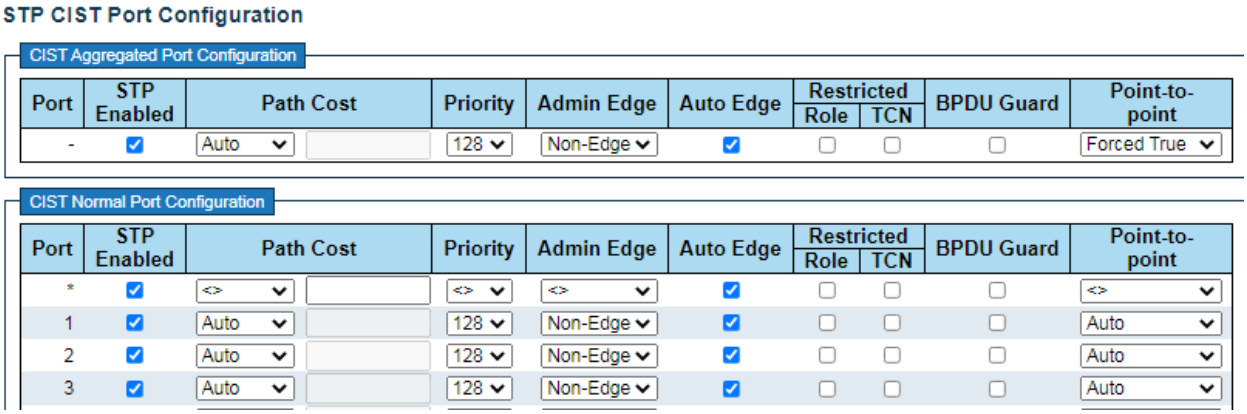


Рис. 3.72 – Порты CIST

Таблица 3.70 – Порты CIST

Port	Номер порта
STP Enabled	Включает функцию STP.
Path Cost	Стоимость маршрута используется для определения наилучшего маршрута между устройствами. Если выбран режим работы “Auto” (Автоматически), при определении стоимости маршрута система автоматически определяет скорость и режим дуплекса. Если требуется ввести значение, выбранное пользователем, выберите “Specific” (Специальный). Допустимые значения: от 1 до 200000000. Пожалуйста, имейте в виду, что стоимость маршрута имеет более высокий приоритет, чем приоритет порта.
Priority	Выберите приоритет порта
Admin Edge	Граница администрирования. Если интерфейс подключен к оконечным узлам, в этом поле можно задать “Edge” (Граница).
Auto Edge	Автоматическое определение границы сети. Установите флаг в этом поле, чтобы включить эту функцию. Когда функция

	включена, порт автоматически определяет границу сети при приеме BPDU.
Restricted Role	Ограниченная роль. Если включено, порт не будет выбран в качестве корневого для CIST или любого MSTI даже тогда, когда он имеет наилучший приоритет STP.
Restricted TCN	Ограниченный TCN. Если включено, порт не будет распространять принятые уведомления об изменении топологии и сами изменения топологии на другие порты.
BPDU Guard	Данная функция защищает порты от приема BPDU. Позволяет предотвратить петли путем выключения порта при приеме BPDU вместо помещения его в состояние discarding. Если включено, порт выключится до тех пор, пока не примет правильный BPDU.
Point-to-Point	Точка-точка. Выберите тип линии, подключенной к интерфейсу: • Auto (Автоматически): Коммутатор автоматически определит, какой интерфейс подключен - либо линия точка-точка, либо разделяемая среда. • Forced True (Принудительная установка соединения точка-точка): Установка соединения точка-точка. • Forced False (Принудительная установка соединения разделяемой среды): Установка соединения разделяемой среды.

MSTI Ports (Порты MSTI) (Рис. 3.73) (Табл. 3.71).

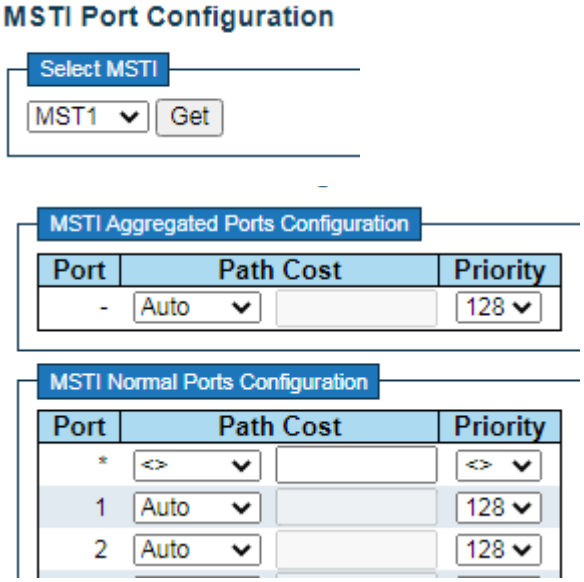


Рис. 3.73 – Порты MSTI

Выберите конкретный MSTI, который требуется настроить, затем нажмите кнопку “Get”.

Таблица 3.71 – Порты MSTI

Port	Номер порта

Path Cost	Стоимость маршрута используется для определения наилучшего маршрута между устройствами. Если выбран режим работы “Auto” (Автоматически), при определении стоимости маршрута система автоматически определяет скорость и режим дуплекса. Если требуется ввести значение, выбранное пользователем, выберите “Specific” (Специальный). Допустимые значения: от 1 до 200000000. Пожалуйста, имейте в виду, что стоимость маршрута имеет более высокий приоритет, чем приоритет порта.
Priority	Выберите приоритет порта.

3.2.26 IPMC Profile (Профиль IPMC)

IPMC профили используются для обеспечения контроля доступа к IPмультикаст потокам. Существует возможность создать 64 профиля с 128 правилами в каждом.

Для доступа к настройкам необходимо перейти по вкладке Configuration→IPMC Profile.

Profile Table (Таблица профиля) (Рис. 3.74) (Табл. 3.72).

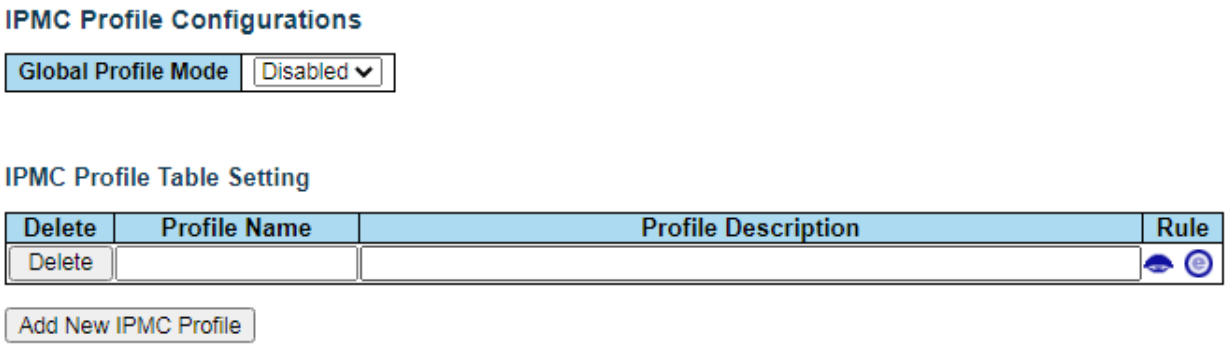


Рис. 3.74 – Таблица профиля

Таблица 3.72 – Таблица профиля

IPMC Profile Configuration (Настройка профиля IPMC)	
Global Profile Mode	Позволяет включить или выключить функцию IPMC Profile глобально.
IPMC Profile Table Setting (Настройка таблицы профиля IPMC)	
Profile Name	Введите имя для данного профиля.
Profile Description	Введите краткое описание для данного профиля

Кнопка Add New IPMC Profile позволяет добавить новый профиль.

Address entry (Диапазоны адресов) (Рис. 3.75) (Табл. 3.73).

IPMC Profile Address Configuration

Navigate Address Entry Setting in IPMC Profile by 20 entries per page.

Delete	Entry Name	Start Address	End Address
Delete			

Add New Address (Range) Entry

Рис. 3.75 – Диапазоны адресов

Таблица 3.73 – Диапазоны адресов

Delete	Удаление текущей записи
Entry Name	Введите имя, которое будет использоваться для индексации диапазона адресов.
Start Address	Введите в этом поле начальный адрес диапазона многоадресных адресов (IPv4 или IPv6).
End Add	Введите в этом поле конечный адрес диапазона многоадресных адресов (IPv4 или IPv6).

Кнопка Add New Address (Range) Entry позволяет добавить новый профиль.

3.2.27 MVR

Протокол MVR - регистрация многоадресных VLAN (Multicast VLAN Registration) позволяет медиасерверу передавать многоадресный поток по одной многоадресной VLAN, при этом клиенты, принимающие поток многоадресной VLAN, могут оставаться в различных сетях VLAN. Клиенты различных VLAN, намеревающиеся вступить в многоадресную группу или выйти из нее, отправляют в порт приемника сообщение IGMP Join (Вступить в группу) либо IGMP Leave (Покинуть группу). Порт приемника, принадлежащий одной из многоадресных групп, может принимать многоадресный поток от медиасервера.

Далее, MVR изолирует пользователей, не намеревающихся принимать многоадресный трафик и, следовательно, обеспечивать безопасность данных за счет сегрегации VLAN, допускающей только многоадресный трафик в другие сети VLAN, к одной из которых принадлежит абонент. Несмотря на то, что общий многоадресный трафик проходит от MVR VLAN в VLAN различных групп, пользователи различных VLAN IEEE 802.1Q или частных VLAN не могут обмениваться какой-либо информацией (за исключением услуг маршрутизации верхнего уровня).

Для доступа к настройкам необходимо перейти по вкладке Configuration→ MVR.

Configuration (Настройка) (Рис. 3.76) (Табл. 3.74).

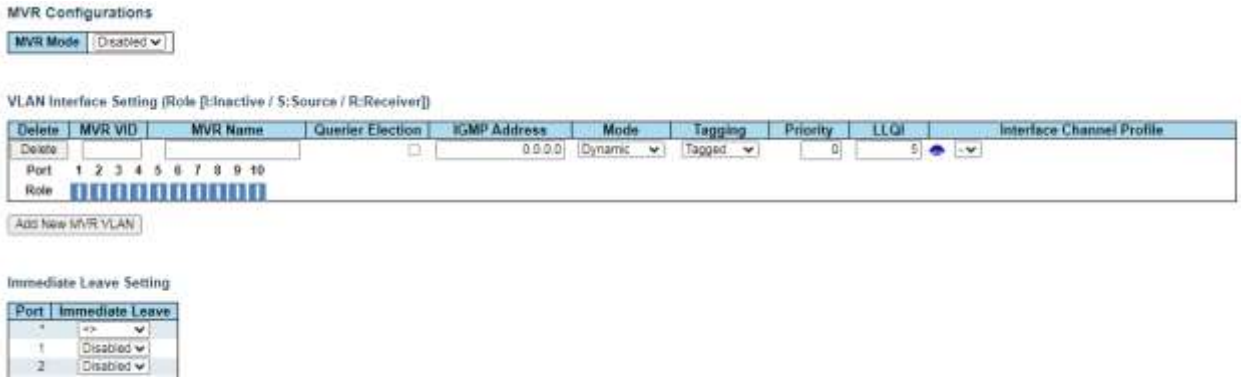


Рис. 3.76 – Настройка MVR

Таблица 3.74 – Настройка MVR

MVR Mode	Включение /выключение функции MVR.
VLAN Interface Setting (Настройка интерфейса VLAN)	
MVR VID	Задайте номер VLAN ID многоадресной VLAN. Пожалуйста, имейте в виду, что порты источника MVR не рекомендуется использовать как порты управления VLAN. Порты источника MVR должны быть сконфигурированы, как члены MVR VLAN, однако порты приемников MVR не следует вручную конфигурировать, как члены данной VLAN.
MVR Name	Дополнительно можно задать имя, определенное пользователем для данной многоадресной VLAN. Максимальная длина строки имени MVR равна 32. Разрешается использовать и буквы, и цифры.
Querier Election	Включите, чтобы присоединиться к выбору IGMP Querier в VLAN.
IGMP Address	Задайте одноадресный IPv4-адрес в качестве адреса источника, используемого в заголовке IP кадров управления IGMP.
Mode	Поддерживаются два режима работы MVR: • Dynamic (Динамический): MVR разрешает динамически отправлять сообщения о членстве на порты источника. Этот режим работы задан по умолчанию. • Compatible (Совместимый): Отправка на порты источника сообщений MVR о членстве запрещена.
Tagging	Задайте, следует ли при отправке помечать тегами MVR VID кадры управления IGMP/MLD либо их следует отправлять без тегов.
Priority	Задайте приоритет передачи кадров управления IGMP/MLD. По умолчанию, приоритет равен 0. Допустимые значения приоритета: 0 -7.
LLQI	LLQI – это сокращение для Last Listener Query Interval (Интервал запроса последнего слушания); LLQI применяется для настройки максимального времени ожидания сообщения о членстве IGMP/MLD на порту приемника до удаления порта из многоадресной группы. По умолчанию LLQI равно 0,5 секунды. Диапазон допустимых значений: 0-31744 десятых долей секунды.
Interface Channel	Выберите профиль IPMC из раскрывающегося меню.

Profile	
Port Role	Нажмите на значок роли порта, чтобы изменить состояние роли. • Inactive (I) (Неактивный): По умолчанию, все порты неактивны. Неактивные порты не 86 участвуют в работе MVR. • Source (S) (Источник): Порт (входящего трафика) является портом источника. Порты источников будут принимать и посылать многоадресные данные. Абоненты не могут быть напрямую подключены к портам источника. Имейте в виду, что порты источника не могут быть в то же время портами управления. • Receiver (R) (Приемник): Порт установлен как порт приемника. Клиентские или абонентские порты сконфигурированы, как порты приемников, так что они могут использовать сообщения IGMP/MLD для приема многоадресных данных.
Immediate Leave Setting (Настройка немедленного выхода (из группы))	
Port	Номер порта
Immediate Leave	Выбрав соответствующий раздел списка, можно включить (Enable) или выключить (disable) функцию немедленного выхода из группы. Когда функция включена, устройство немедленно удаляет порт из многоадресного потока, как только оно принимает сообщение leave (Покинуть группу) для этой группы. Данная опция применима только к интерфейсу, сконфигурированному, как приемники MVR.

Кнопка Add New MVR VLAN позволяет добавить новый MVR.

3.2.28 IPMC

3.2.28.1 IGMP Snooping

Протокол управления группами интернета IGMP (Internet Group Management Protocol) обеспечивает управление участием в многоадресных IP-группах. IGMP используется IP-хостами и соседними многоадресными маршрутизаторами для установления принадлежности к многоадресной группе. Он может использоваться наиболее эффективно при поддержке таких услуг, как потоковое онлайн-видео и игры.

IGMP Snooping – это процесс слушания трафика IGMP. Как следует из названия, IGMP snooping представляет собой функцию, позволяющую коммутатору «прослушивать» обмен данными между хостами и маршрутизаторами, обрабатывая пакеты 3-го уровня (пакеты IGMP, посылаемые по многоадресной сети).

Когда на коммутаторе включен IGMP snooping, он анализирует все пакеты, передаваемые между хостами, подключенными к коммутатору и многоадресными маршрутизаторами в сети. Когда коммутатор принимает отчет IGMP для данной многоадресной группы от хоста, коммутатор добавляет номер порта хоста к многоадресному списку для этой группы. Когда коммутатор обнаруживает сообщение IGMP Leave (Покинуть группу IGMP), он удаляет порт хоста из ячейки таблицы.

IGMP snooping позволяет эффективно снижать многоадресный трафик при стриминге и других экстенсивно расходующих полосу пропускания IPприложениях. Коммутатор, использующий IGMP snooping, в этом трафике будет передавать хостам только многоадресный трафик. Снижение многоадресного трафика уменьшает число пакетов,

обрабатываемых коммутатором (однако при этом требуется увеличение оперативной памяти для обработки многоадресных таблиц) и снижает нагрузку на оконечные хосты, так как их сетевые карты (или операционные системы) не будут принимать и фильтровать весь многоадресный трафик, генерируемый сетью.

Для доступа к настройкам необходимо перейти по вкладке Configuration→ IPMC→IGMP Snooping.

Basic Configuration (Основные настройки) (Рис. 3.77) (Табл. 3.75).

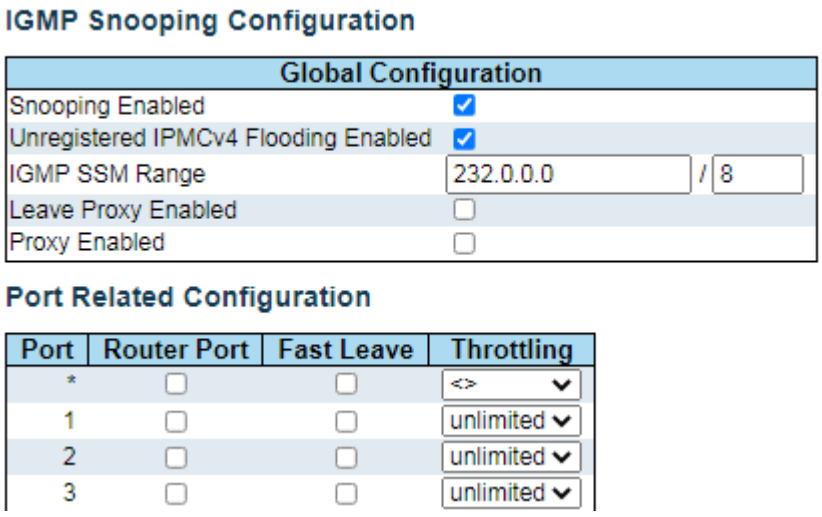


Рис. 3.77 – Основные настройки

Таблица 3.75 – Основные настройки

Global Configuration (Глобальные настройки)	
Snooping Enabled	Установите флаг, чтобы глобально включить функцию IGMP Snooping. Когда функция включена, данное устройство будет осуществлять мониторинг сетевого трафика и определять, какие хосты будут принимать многоадресный трафик. Коммутатор может пассивно контролировать или анализировать пакеты IGMP Query (Запросы IGMP) и IGMP Report (Отчеты IGMP), передаваемые между многоадресными IP-маршрутизаторами и подписчиками многоадресных IP-услуг для идентификации участников многоадресной группы. Коммутатор анализирует проходящие через него IGMP-пакеты, извлекает из них регистрационную информацию группы и соответствующим образом конфигурирует многоадресные фильтры.
Unregistered IPMCv4 Flooding Enabled	Если флаг в этом поле установлен, включен режим передачи незарегистрированного (не принадлежащего группам) многоадресного IP-трафика. Установите флаг в этом поле, чтобы включить рассылку пакетов всем узлам.
IGMP SSM Range	Диапазон многоадресных адресов для конкретного источника SSM (Source-Specific Multicast), позволяет поддерживающим SSM хостам и маршрутизаторам выполнять модель услуг SSM для групп в заданном диапазоне адресов.
Leave Proxy Enabled	Подавляет сообщения о выходе из группы, отличающиеся от принятых, от последнего портаучастника группы. Прокси-сервер

	сообщений о выходе из группы подавляет все не являющиеся необходимыми сообщения IGMP о выходе из группы таким образом, что коммутатор, не являющийся querier, передает пакет выхода из группы только тогда, когда последний динамический порт-участник покидает многоадресную группу.
Proxy Enabled	Прокси-сервер включен
Port Related Configuration (Настройки, связанные с портом)	
Port	Номер порта
Router Port	Установите флаг в поле данного порта, чтобы назначить его портом маршрутизатора. Если IGMP snooping не может определить местонахождение IGMP querier, Вы можете вручную назначить порт, который подключен к известному IGMP querier (например, к многоадресному маршрутизатору или коммутатору). Этот интерфейс затем вступит во все текущие многоадресные группы, поддерживаемые подключенным маршрутизатором/коммутатором, чтобы гарантировать, что многоадресный трафик прошел на все соответствующие интерфейсы коммутатора.
Fast Leave	Если флаг установлен, включена функция быстрого выхода из группы. Когда принят пакет выхода из группы, коммутатор немедленно удаляет порт из многоадресной услуги, не посылая специфичный для группы запрос IGMP GS на этот интерфейс.
Throttling	Это значение ограничивает максимальное число многоадресных групп, в которые порт может вступить одновременно. Когда для порта будет достигнуто максимальное число групп, новые сообщения с отчетами IGMP о вступлении в группу будут отбрасываться. По умолчанию выбрано неограниченное число групп (unlimited). Допустимый диапазон значений от 1 до 10.

VLAN Configuration (Настройка VLAN) (Рис. 3.78) (Табл. 3.76).

Рис. 3.78 – Настройка VLAN

Таблица 3.76 – Настройка VLAN

VLAN ID	Задайте номер VLAN, используемой для IGMP snooping.
Snooping Enabled	Установите флаг, чтобы включить функцию «прослушивания» на интерфейсе. Когда эта функция включена, коммутатор будет контролировать сетевой трафик на указанном интерфейсе, чтобы определить, какие хосты желают получать многоадресные услуги. Если IGMP snooping включен глобально и IGMP snooping включен на интерфейсе, то приоритетом будет пользоваться IGMP snooping на интерфейсе. Когда флаг в этом поле снят, «прослушивание» может оставаться сконфигурированным на интерфейсе. Однако настройки будут

	действовать только в том случае, если IGMP snooping включен глобально.
Querier Election	Установите флаг в этом поле, чтобы выбрать порт запросов в VLAN. Когда флаг в поле снят, порт будет использоваться как порт IGMP, не посылающий запросов.
Querier Address	Задайте одноадресный IPv4-адрес, используемый в 90 заголовке IP для выбора порта-источника запросов IGMP. Когда это поле не задано, коммутатор будет использовать первый доступный IPv4-адрес управления IP-интерфейса, ассоциированного с этой VLAN.
Compatibility	В этом поле задано, какие хосты и маршрутизаторы могут выполнять операции в сети (в зависимости от выбранной версии IGMP). Доступны следующие варианты: “IGMP-Auto” (Автоматический выбор версии IGMP), “Forced IGMPv1” (Принудительное использование IGMPv1), “Forced IGMPv2” (Принудительное использование IGMPv2), “Forced IGMPv3” (Принудительное использование IGMPv3). По умолчанию применяется “IGMP-Auto” (Автоматический выбор версии IGMP).
PRI	Выберите приоритет интерфейса. В этом поле указано уровень приоритета кадра управления IGMP, сгенерированный системой, которая использована для назначения приоритетов различным классам трафика. Диапазон допустимых значений: от 0 (наименьший приоритет) до 7 (наивысший приоритет). По умолчанию, приоритет интерфейса равен 0.
RV	Переменная надежности RV (robustness variable) позволяет настроить ожидаемые потери пакетов в подсети. Если есть подозрение, что в подсети теряются пакеты, это значение можно увеличить. Значение RV не должно быть нулем или 1. Значение должно быть 2 или более. По умолчанию задано 2.
QI	В поле Query Interval (Интервал между запросами) указан интервал времени между отправкой запросчиком сообщений с общими запросами IGMP (IGMP General Query). По умолчанию задан интервал 125 секунд.
QRI	Query Response Interval – максимальное время ожидания маршрутизатором IGMP приема ответа на сообщение с запросом IGMP General Query. QRI применяется, когда коммутатор функционирует, как запросчик и используется для информирования других устройств о максимальном времени, которое данная система ожидает ответа на общие запросы. По умолчанию задано значение 10 секунд. Диапазон допустимых значений: 0-31744 десятых долей секунды.
LLQI	Last Listener Query Interval – время ожидания ответа на запросное сообщение, специфичное для группы или на запросное сообщение, специфичное для группы и источника.
URI	Unsolicited Report Interval – время ожидания передачи входящим интерфейсом непредусмотренных отчетов IGMP, когда включено их подавление или фильтрация на прокси-сервере. По умолчанию для URI задано значение 1 секунда. Диапазон допустимых значений: от 0 до - 31744 секунд.

Port Filtering Profile (Профиль фильтрации порта) (Рис. 3.79) (Табл. 3.77).

На странице настройки фильтрации порта можно отфильтровать определенный многоадресный трафик по каждому порту отдельно. Перед тем, как выбирать профиль фильтрации, необходимо задать профили на странице IPMC Profile (Профиль IPMC).

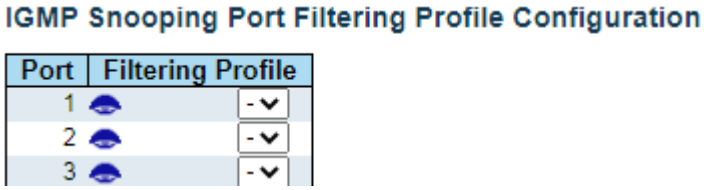


Рис. 3.79 – Профиль фильтрации порта

Таблица 3.77 – Профиль фильтрации порта

Port	Номер порта.
Filtering Profile	Выберите сконфигурированные многоадресные группы, которые запрещены на порту. Когда определенная многоадресная группа выбрана на порту, сообщения IGMP join reports (отчеты о вступлении в группу) на порту отбрасываются.

3.2.28.2 MLD Snooping

Протокол MLD (Multicast Listener Discovery snooping) подобен протоколу IGMP snooping для IPv4 и используется для многоадресного трафика IPv6. Другими словами, MLD snooping конфигурирует порты для ограничения многоадресного трафика IPv6 или управления им таким образом, чтобы он передавался на порты (или пользователям), которым он действительно требуется. В результате, MLD snooping снижает лавинообразную передачу многоадресных пакетов IPV6 по заданным VLAN. Пожалуйста, имейте в виду, что IGMP Snooping и MLD Snooping работают независимо друг от друга. Они могут быть включены одновременно.

Для доступа к настройкам необходимо перейти по вкладке Configuration→ IPMC→ MLD Snooping.

Basic Configuration (Основные настройки) (Рис. 3.80) (Табл. 3.78).

MLD Snooping Configuration

Global Configuration	
Snooping Enabled	☑
Unregistered IPMCv6 Flooding Enabled	☑
MLD SSM Range	ff3e:: / 96
Leave Proxy Enabled	☐
Proxy Enabled	☐

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	☐	☐	<>
1	☐	☐	unlimited
2	☐	☐	unlimited
3	☐	☐	unlimited

Рис. 3.80 – Основные настройки

Таблица 3.78 – Основные настройки

Global Configuration (Глобальные настройки)	
Snooping Enabled	Установите флаг, чтобы глобально включить функцию MLD Snooping . Когда функция включена, данное устройство будет осуществлять мониторинг сетевого трафика и определять, какие хосты будут принимать многоадресный трафик. Коммутатор может пассивно контролировать или анализировать пакеты MLD Listener Query (Запросы прослушивания MLD) и MLD Report (Отчеты MLD), передаваемые между многоадресными IPмаршрутизаторами и подписчиками многоадресных IPуслуг для идентификации участников многоадресной группы. Коммутатор анализирует проходящие через него IGMP-пакеты, извлекает из них регистрационную информацию группы и соответствующим образом конфигурирует многоадресные фильтры.
Unregistered IPMCv6 Flooding Enabled	Если флаг установлен, включен режим передачи незарегистрированного (не принадлежащего группам) многоадресного IP-трафика. Установите флаг, чтобы включить рассылку пакетов всем узлам.
MLD SSM Range	Диапазон многоадресных адресов для конкретного источника SSM (Source-Specific Multicast), позволяет поддерживающим SSM хостам и маршрутизаторам выполнять модель услуг SSM для групп в заданном диапазоне адресов.
Leave Proxy Enabled	Чтобы предотвратить перегрузку многоадресного маршрутизатора сообщениями о выходе из группы, MLD snooping подавляет их, пока не примет такое сообщение от последнего порта-участника группы. Когда коммутатор работает, как запросчик, функция проксисервера для сообщений о выходе из группы работать не будет.
Proxy Enabled	Когда прокси-сервер MLD включен, коммутатор обменивается сообщениями MLD с маршрутизатором своего восходящего интерфейса и выполняет задачи хоста MLD на восходящем интерфейсе: • Когда приходит запрос, он посылает отчет

	многоадресного прослушивания группе. • Когда хост вступает в многоадресную группу, в которой нет других хостов, он посылает этой группе непредусмотренные отчеты. • Когда определенную многоадресную группу покидает последний хост, коммутатор посылает непредусмотренный отчет по адресу, используемому всеми маршрутизаторами (FF02::2) при MLDv1.
Port Related Configuration (Настройки, связанные с портом)	
Port	Номер порта
Router Port	Установите флаг, чтобы назначить портом маршрутизатора. Если MLD snooping не может определить местонахождение MLD querier, Вы можете вручную назначить порт, который подключен к известному IGMP querier (например, к многоадресному маршрутизатору или коммутатору). Этот интерфейс затем вступит во все текущие многоадресные группы, поддерживаемые подключенным маршрутизатором /коммутатором, чтобы гарантировать, что многоадресный трафик прошел на все соответствующие интерфейсы коммутатора.
Fast Leave	Если флаг в поле установлен, включена функция быстрого выхода из группы. Когда принят пакет выхода из группы, коммутатор немедленно удаляет порт из многоадресной услуги, не посылая специфичный для группы запрос MLD GS на этот интерфейс.
Throttling	Это поле ограничивает максимальное число многоадресных групп, в которые порт может вступить одновременно. Когда для порта будет достигнуто максимальное число групп, новые сообщения с отчетами MLD о вступлении в группу будут отбрасываться. По умолчанию выбрано неограниченное число групп (unlimited). Допустимый диапазон значений от 1 до 10.

VLAN Configuration (Настройка VLAN) (Рис. 3.81) (Табл. 3.79).

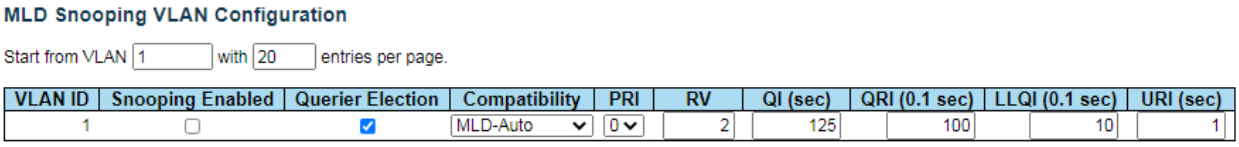


Рис. 3.81 – Настройка VLAN

Таблица 3.79 – Настройка VLAN

VLAN ID	Задайте номер VLAN, используемой для MLD snooping.
Snooping Enabled	Установите флаг в этом поле, чтобы включить функцию «прослушивания» на интерфейсе. Когда эта функция включена, коммутатор будет контролировать сетевой трафик на указанном интерфейсе, чтобы определить, какие хосты желают получать многоадресные услуги.
Querier Election	Установите флаг в этом поле, чтобы выбрать порт запросов в VLAN. Когда флаг в этом поле установлен, коммутатор может использоваться, как запросчик MLDv2, конкурируя с другими

	многоадресными маршрутизаторами или коммутаторами. Как только коммутатор станет запросчиком, он будет отвечать за отправку на хосты периодических запросов о том, желают ли они принимать многоадресный трафик. Когда флаг в поле снят, порт будет использоваться как порт IGMP, не посылающий запросов.
Compatibility	В этом поле задано, какие хосты и маршрутизаторы могут выполнять операции в сети (в зависимости от выбранной версии MLD). Доступны следующие варианты: “MLD-Auto” (Автоматический выбор версии MLD), “Forced MLDv1” (Принудительная установка версии MLDv1) и “Forced MLDv2” (Принудительная установка версии MLDv2). По умолчанию применяется “MLD-Auto” (Автоматический выбор версии MLD).
PRI	Выберите приоритет интерфейса. В этом поле указано уровень приоритета кадра управления MLD, сгенерированный системой, которая использована для назначения приоритетов различным классам трафика. Диапазон допустимых значений: от 0 (наименьший приоритет) до 7 (наивысший приоритет). По умолчанию, приоритет интерфейса равен 0.
RV	Переменная надежности RV (robustness variable) позволяет настроить ожидаемые потери пакетов в подсети. Если есть подозрение, что в подсети теряются пакеты, это значение можно увеличить. Значение RV не должно быть нулем или 1. Значение должно быть 2 или более. По умолчанию задано 2. Диапазон допустимых значений: 1~255.
QI	В поле Query Interval (Интервал между запросами) указан интервал времени между отправкой запросчиком сообщений с общими запросами IGMP (IGMP General Query). По умолчанию задан интервал 125 секунд. Допустимый диапазон значений от 1 до 31744 секунд.
QRI	Query Response Interval – максимальное время ожидания маршрутизатором IGMP приема ответа на сообщение с запросом IGMP General Query. QRI применяется, когда коммутатор функционирует, как запросчик и используется для информирования других устройств о максимальном времени, которое данная система ожидает ответа на общие запросы. По умолчанию для RQI задано значение 10 секунд. Диапазон допустимых значений: 0-31744 десятых долей секунды.
LLQI	Last Listener Query Interval – время ожидания ответа на запросное сообщение, специфичное для группы или на запросное сообщение, специфичное для группы и источника.
URI	Unsolicited Report Interval – время ожидания передачи входящим интерфейсом непредусмотренных отчетов IGMP, когда включено их подавление или фильтрация на прокси - сервере. По умолчанию для URI задано значение 1 секунда. Диапазон допустимых значений: от 0 до 31744 секунд.

Port Filtering Profile (Профиль фильтрации порта) (Рис. 3.82) (Табл. 3.80)

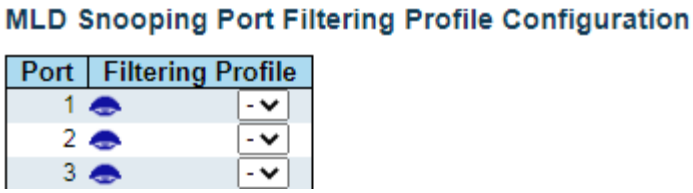


Рис. 3.82 – Профиль фильтрации порта

Таблица 3.80 – Профиль фильтрации порта

Port	Номер порта.
Filtering Profile	Выберите сконфигурированные многоадресные группы, которые запрещены на порту. Когда определенная многоадресная группа выбрана на порту, сообщения MLD join reports (отчеты о вступлении в группу) на порту отбрасываются.

3.2.29 LLDP

Протокол LLDP (Link Layer Discovery Protocol) является протоколом канального уровня, на котором сетевые устройства обмениваются информацией о себе с другими устройствами, напрямую соединенными через сеть. Используя LLDP, два устройства, на которых функционируют сетевые протоколы разных уровней, могут обучаться информации друг друга. Для обнаружения соседних устройств используется набор атрибутов, ссылающийся на TLV. Устройство может передавать и принимать такую детальную информацию, как описание порта, описание системы и ее возможностей, адрес управления.

Для доступа к настройкам необходимо перейти по вкладке Configuration→ LLDP.

Configuration (Настройка) (Рис. 3.83) (Табл. 3.81).

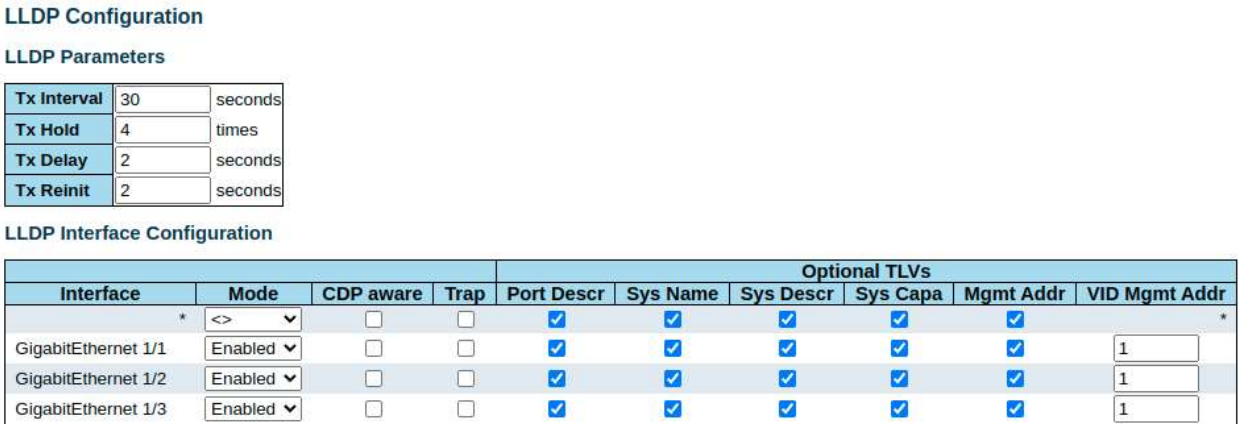


Рис. 3.83 – Настройка LLDP

Таблица 3.81 – Настройка LLDP

LLDP Parameters (Параметры LLDP)	
Tx Interval	Задайте интервал между кадрами LLDP, отправляемыми соседям данного устройства для обновления информации о данном устройстве. Допустимые значения: от 5 до 32768 секунд. По умолчанию задано 30 секунд.
Tx Hold	Данная настройка определяет, как долго кадры LLDP будут считаться правильными и используется для вычисления TTL. Диапазон допустимых значений: 2~10 раз. По умолчанию задано 4.
Tx Delay	Задайте задержку между кадрами LLDP, содержащими изменения конфигурации. Tx Delay не может превышать 1/4 от интервала Tx. Допустимые значения: от 1 до 8192 секунд.
Tx Reinit	Задайте задержку между кадром отключения и новой инициализацией LLDP. Допустимые значения: от 1 до 10 секунд.
LLDP Interface Configuration (Настройка интерфейса LLDP)	
Interface	Интерфейс
Mode	Выберите соответствующий режим работы LLDP: • Disabled (Выключен): Информация LLDP посылаться не будет, информация LLDP, принятая от соседних устройств будет отброшена. • Enabled (Включить): Информация LLDP будет посылаться, информация LLDP, принятая от соседних устройств будет проанализирована. • Rx Only (Только прием): Коммутатор будет анализировать информацию LLDP, принятую от соседних устройств. • Tx Only (Только передача): Коммутатор будет посылать информацию LLDP, но будет отбрасывать информацию LLDP, принятую от соседних устройств.
CDP Aware	Операция CDP aware (Распознавание CDP) используется для декодирования входящих кадров CDP (Cisco Discovery Protocol). Если эта опция включена, CDP TLVs, которые могут быть отображены в соответствующее поле таблицы соседних устройств LLDP будут декодированы, в противном случае эти кадры будут отброшены. CDP TLVs отображаются в поле таблицы соседних устройств LLDP.
Optional TLVs	Для обнаружения соседних устройств, LLDP использует несколько атрибутов. Эти атрибуты содержат описания типа, длины и значений и ссылаются на TLVs. Данное устройство может передавать такую детальную информацию, как описание порта, имя и описание системы и ее возможностей, адрес управления. Если нежелательно, чтобы соседние устройства обладали этой информацией, снимите флаг в этом поле.

LLDP-MED (Рис. 3.84) (Табл. 3.82).

Протокол LLDP для конечных медиа-устройств LLDP-MED (LLDP for Media Endpoint Devices) является расширением LLDP и работает между конечными устройствами, такими как IP-телефоны и сетевыми устройствами (например, коммутаторами). Протокол LLDP-MED обеспечивает поддержку приложений передачи голоса по IP (VoIP) и

дополнительные TLVs для обнаружения, обеспечения политики сети, функции Power over Ethernet, управления реестром и информации о местоположении.

LLDP-MED Configuration

Fast Start Repeat Count

Fast start repeat count	4

LLDP-MED Interface Configuration

	Transmit TLVs				
Interface	Capabilities	Policies	Location	PoE	Device Type
*	☑	☑	☑	☑	<>
GigabitEthernet 1/1	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/2	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/3	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/4	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/5	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/6	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/7	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/8	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/9	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/10	☑	☑	☑	☑	Connectivity

Coordinates Location

Latitude	0	°	North	Longitude	0	°	East	Altitude	0	Meters	Map Datum	WGS84

Civic Address Location

Country code		State		County	
City		City district		Block (Neighborhood)	
Street		Leading street direction		Trailing street suffix	
Street suffix		House no.		House no. suffix	
Landmark		Additional location info		Name	
Zip code		Building		Apartment	
Floor		Room no.		Place type	
Postal community name		P.O. Box		Additional code	

Emergency Call Service

Emergency Call Service	

Policies

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
No entries present						

Add New Policy

Рис. 3.84 – Настройка LLDP-MED

Таблица 3.82 – Настройка LLDP-MED

Fast Start Repeat Count	Быстрый старт и идентификация местоположения при аварийном вызове (Emergency Call Service Location Identification Discovery) для конечных устройств является важным аспектом VoIP-систем. Кроме того, лучше всего предоставлять только те части информации, которые действительно важны для конечного устройства данного типа (например, оповещать о правилах работы в голосовой сети следует только те устройства, которые могут работать с голосовым трафиком). Это необходимо также и для сохранения ограниченного пространства LLDPU и уменьшения проблем с безопасностью и целостностью системы, которые могут возникать изза того, что информация о правилах работы в сети будет попадать на не предназначенные для этой информации устройства. В связи с этим, в LLDPMED для достижения соответствующих свойств определен этап взаимодействия LLDP-MED Fast Start (Быстрый старт LLDP-MED) между протоколом и уровнем приложений на вершине протокола. Параметр Fast start

	repeat count (Число повторов быстрого старта) позволяет задать, сколько раз будет повторен быстрый старт передачи. Рекомендуемое значение (4 раза) означает, что с интервалом 1 секунда будут переданы 4 кадра LLDP, если принят кадр LLDP с новой информацией. Следует отметить, что LLDP-MED и механизм LLDP-MED Fast Start предназначены только для работы на линиях между устройствами соединения по сети, поддерживающими LLDP-MED и конечными устройствами и неприменимы к линиям между элементами инфраструктуры LAN, включая и устройства соединения по сети или линии другого типа.
LLDP-MED Interface Configuration	
Interface	интерфейс, к которому применяется конфигурация.
Transmit TLVs	При установленном флажке, соответствующие параметры коммутатора включаются в передаваемую информацию LLDP-MED .
Device Type	Тип устройства
Coordination Locations (Координаты местоположения)	
Latitude	Широта должна быть приведена в диапазоне 0-90 градусов и содержать не более 4 цифр. Можно задать экваториальное положение либо на север от экватора (North) либо на юг (South) от экватора.
Longitude	Долгота должна быть приведена в диапазоне 0-180 градусов и содержать не более 4 цифр. Можно указать направление – либо на восток от нулевого меридиана (East) либо на запад от нулевого меридиана (West).
Altitude	Высота должна быть приведена в диапазоне от - 32767 до 32767 и содержать не более 4 цифр. Можно выбрать единицы измерения высоты – либо в метрах, либо в этажах.
Meters	Метры высоты, отсчитываются от заданного датума (нулевого уровня) по вертикали.
Map Datum	Параметр Map Datum используется для выбора системы координат: • WGS84: (Географические, трехмерные) – Всемирная геодезическая система 1984, CRS Code 4327, нулевой меридиан: гринвичский. • NAD83/NAVD88: Североамериканская система координат 1983, CRS Code 4269, нулевой меридиан: гринвичский; связанная с этой система координат по вертикали - North American Vertical Datum of 1988 (NAVD88). Эта пара систем координат используется для указания местоположения на земле, на водных пространствах, подверженных приливам и отливам (для которых можно использовать систему координат NAD83/MLLW). • NAD83/MLLW: Североамериканская система координат 1983, CRS Code 4269, нулевой меридиан: гринвичский; связанная с этой система координат по вертикали - Mean Lower Low Water (MLLW). Эта пара связанных систем координат используется при указании местоположения в океане, на морях и на других водных пространствах.
Civic Address Location (Указание гражданского адреса) Стандартная форма гражданского адреса (IETF Geopriv Civic Address) базируется на конфигурационной информации местоположения (Location Configuration Information) и обозначается как	

Civic Address LCI.	
Country Cod	Код страны по стандарту ISO 3166, состоящий из двух прописных букв ASCII. Пример: DK, DE или US.
State	Единица административно-территориального деления (штат, кантон, регион, провинция, префектура).
Country	Округ.
City	Город, поселок.
City District	Район города, округ города, административный район города.
Block	Квартал, блок.
Street	Улица. Пример: ул. Ленина
Leading street direction	Направление главной улицы. Пример: N.
Trailing street suffix	Навигационный суффикс улицы. Пример: SW
Street suffix	Суффикс улицы. Пример: Проезд.
House no.	Номер дома
House no. suffix	Суффикс номера дома: Пример: B, 1/2.
Landmark	Адрес какого-либо заметного объекта на местности. Пример: Кремль.
Additional Location Info	Дополнительная информация о местоположении. Пример: Северное крыло.
Name	ФИО резидента или лица, арендующего офис.
Zip Code	Почтовый код
Building	Строение. Пример: Аквапарк.
Apartement	Апартамент, номер. Пример: Apt 34.
Floor	Этаж
Room no.	Номер комнаты
Place type	Тип площади
Postal community name	ФИО почтового адресата
P.O. Box	Номер абонентского ящика
Additional Code	Добавочный код
Emergency Call Service	Служба спасения
Policies (Правила)	
Policy Id	Задайте идентификатор ID для этой группы правил
Application Type	Типы приложений, в том числе: “Voice” (Голосовой вызов), “Voice Signalling” (Сигнализация голосового вызова), “Guest Voice” (Гостевой голосовой вызов), “Guest Voice Signalling” (Сигнализация гостевого голосового вызова), “Softphone Voice” (Голосовой вызов по софтофону), “Video Conferencing” (Видеоконференция), “Streaming” (Потоковая передача), “Video Signalling” (Сигнализация видеопотока).
Tag	Тег, указывающий, использует ли заданный тип приложения «тегированную» VLAN или «нетегированную» VLAN.
VLAN ID	Задайте VLAN ID для порта.
L2 Priority	Задайте один из восьми уровней приоритета (0-7), как определено в 802.1D-2004.
DSCP	Задайте одно из значений 64-точечного кода (0-63)

Кнопка Add New Policy предназначена для добавления нового правила.

3.2.30 POE.

Power over Ethernet (PoE) — технология, позволяющая передавать удалённому устройству электрическую энергию вместе с данными через стандартную **витую пару** в сети **Ethernet**. Данная технология предназначается для **IP-телефонии**, точек доступа беспроводных сетей, **IP-камер**, сетевых концентраторов и других устройств, к которым нежелательно или невозможно проводить отдельный электрический кабель.

Для доступа к настройкам необходимо перейти по вкладке Configuration→ PoE.

Power over Ethernet Configuration (Настройка PoE) (Рис. 3.85) (Табл. 3.83).

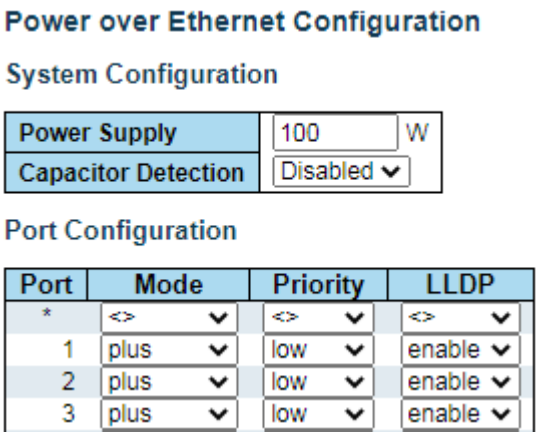


Рис. 3.85 – Настройка PoE

Таблица 3.83 – Настройка PoE

Глобальные настройки	
Power Supply	Настройка максимальной мощности, которую может обеспечить источник питания.
Capacitor Detection	Включение/выключение функции `capacitor-detect`
Настойка портов	
Port	Номер порта
Mode	Выбор режима poe для порта Plus - включает PoE IEEE 802.3bt с поддержкой устаревшей поддержки Standard - включает режим соответствия PoE IEEE 802.3bt Disable- PoE отключено для порта
Priority	Установка приоритета. Существует три уровня приоритета мощности: низкий, высокий и критический. Приоритет используется в том случае, когда удаленным устройствам требуется больше энергии, чем может обеспечить источник питания. В этом случае порт с самым низким приоритетом будет
LLDP	Включение/выключение обработки параметров PoE, полученных

	через LLDP.

3.2.31 SyncE

Для доступа к настройкам необходимо перейти по вкладке Configuration→ SyncE.

SyncE Configuration (Настройка SyncE) (Рис. 3.86) (Табл. 3.84).

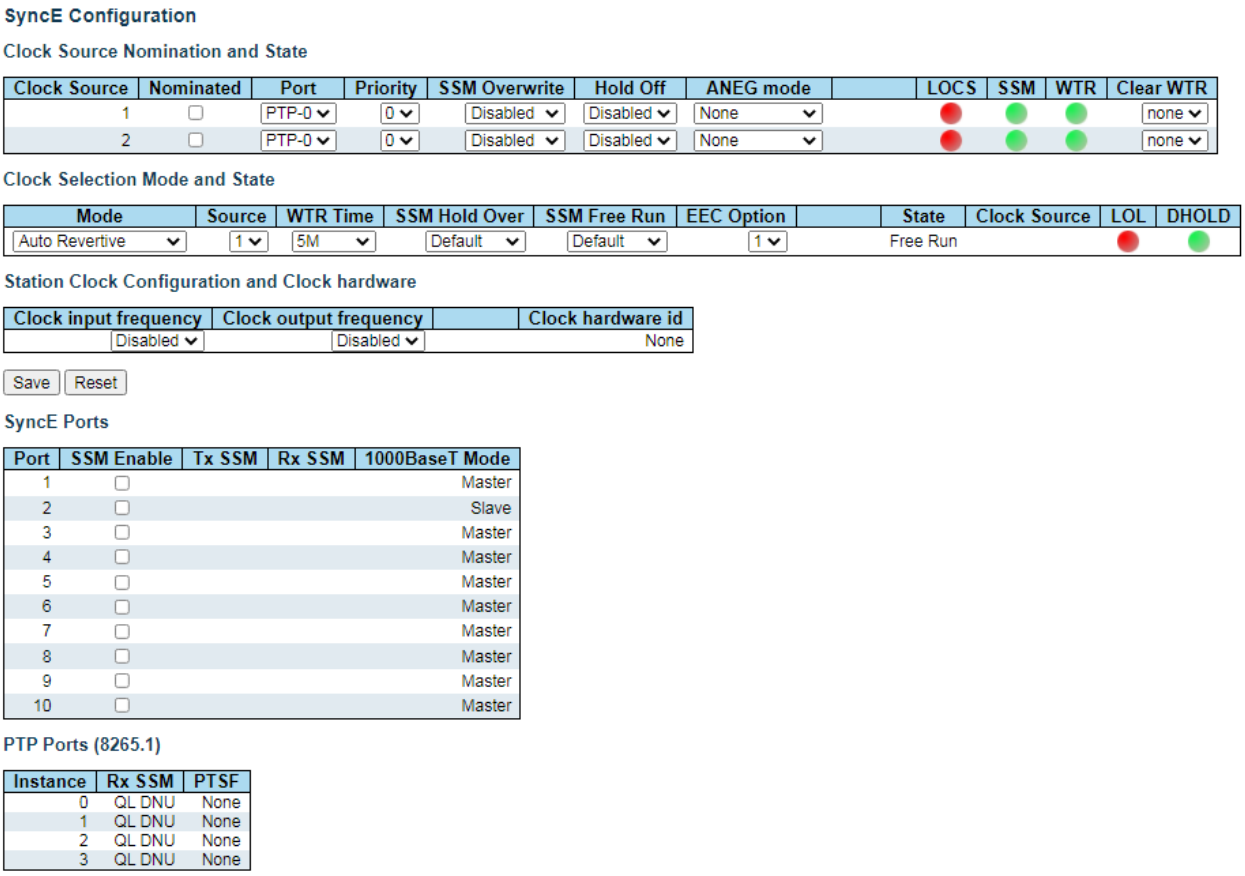


Рис. 3.86 – Настройка SyncE

Таблица 3.84 – Настройка SyncE

Clock Source Nomination and State	
Clock Source	источник синхронизации
Nominated	назначается источник тактовой частоты
Port	выбор порта для источника синхронизации.
Priority	Назначение приоритета для источника синхронизации. Наименьшее число (0) - самый высокий приоритет. Если два источника синхронизации имеют одинаковый приоритет, наименьший номер источника синхронизации получает наивысший приоритет в процессе выбора часов.
SSM Overwrite	Выбираемый уровень качества источника синхронизации (QL) для перезаписи любого QL, полученного в SSM . Если QL не получен в

	SSM (SSM не включен на этом порту), QL перезаписи SSM используется, как если бы он был получен. Для SSM Overwrite может быть установлено значение QL_NONE, что указывает на то, что источник синхронизации не имеет какого-либо известного качества (самое низкое по сравнению с источником синхронизации с известным качеством)
Hold Off	Значение таймера отключения. Активная потеря часов Источник будет отложен на выбранное количество времени. Селектор часов не изменит источник синхронизации, если состояние потери часов будет устранено в течение этого времени.
ANEG mode	Это актуально только для портов 1000BaseT. Чтобы восстановить часы из порта, он должен быть переведен в режим «Slave». Для распределения часов порт должен быть переведен в режим «Master». Эти различные режимы ANEG могут быть активированы на порте источника тактового сигнала: Prefer Slave: Порт будет переведен в режим «Slave», если это возможно. Prefer Master: Порт будет переведен в режим «Master», если это возможно. Forced Slave: порт будет принудительно переведен в режим «Slave». Выбранный порт в состоянии «заблокирован» всегда будет согласован как «ведомый», если это возможно.
LOCS	Сигнал на этом источнике тактовых импульсов потерян.
SSM	Если SSM включен и не получен должным образом. Тип сбоя SSM будет указан в поле «Rx SSM».
WTR	Таймер ожидания восстановления активен.
Clear WTR	Очищает таймер WTR и делает этот источник синхронизации доступным процессу выбора часов.
Clock Selection Mode and State	
Mode	Определение «лучшего» источника синхронизации - это, во-первых, тот, который имеет наивысший (QL), а во-вторых (источники с равным QL) наивысший приоритет. Селектор часов может быть в разных режимах: Manual: Селектор часов выберет источник синхронизации, указанный в поле «Источник» (см. Ниже). Если этот выбранный вручную источник тактовых импульсов выходит из строя, селектор тактовых импульсов переходит в состояние удержания. Manual To Selected: То же, что и ручной режим, где pt. выбранный источник синхронизации станет источником. Auto NonRevertive: выбор часов. Выбор наилучшего источника синхронизации выполняется только при выходе из строя выбранных часов. Auto Revertive: Clock Выбор лучшего источника синхронизации

	выполняется постоянно. Force Hold Over: Селектор часов принудительно удерживается в состоянии удержания. Force Free Run: Селектор часов принудительно переходит в состояние Free Run.
Source	Выбор источника. Актуально, только если выбран ручной режим (см. Выше)
WTR Time	значение таймера ожидания восстановления в минутах. Время WTR активируется на заднем фронте отказа источника синхронизации (в реверсивном режиме).
SSM Hold Over	Это передаваемое значение SSM QL, когда селектор тактовых импульсов находится в состоянии удержания.
SSM Free Run	Это передаваемое значение SSM QL, когда селектор часов находится в состоянии Free Run.
EEC Option	Модули синхронизации на базе ZL30xxx поддерживают как EEC1, так и EEC2. Разница: EEC1 => полоса пропускания DPLL = 3,5 Гц, EEC2 => полоса пропускания DPLL = 0,1 Гц.
State	Это указывает на состояние селектора часов. Возможные состояния: Free Run: нет внешних источников синхронизации для блокировки (разблокированное состояние). Селектор тактовых импульсов никогда не был привязан к источнику тактовых импульсов на достаточно долгое время, чтобы рассчитать смещение по частоте для гетеродина. Частота этого узла - частота гетеродина. Hold Over: нет внешних источников синхронизации, которые можно было бы заблокировать (разблокированное состояние). Селектор тактовых импульсов рассчитал смещение удерживаемой частоты по отношению к гетеродину. Частота этого узла удерживается на уровне частоты источника тактовых импульсов, на котором ранее была установлена привязка. Locked: селектор часов заблокирован для указанного источника синхронизации (см. Далее). Top: селектор часов заблокирован для времени по пакетам, например, PTP (см. Далее).
Clock Source	Источник синхронизации заблокирован, когда переключатель синхронизации находится в заблокированном состоянии.
LOL	Селектор часов поднял тревогу о потере блокировки.
DHOLD	Селектор тактовых импульсов еще не рассчитал смещение удерживаемой частоты по отношению к гетеродину. Становится активным примерно на 10 с. когда выбран новый источник часов
Station Clock Configuration and Clock hardware	
Clock input frequency	Тактовая частота на входе. Если это поддерживается Synce HW, входную частоту тактового сигнала станции можно настроить, возможные частоты: 1544 МГц, 2048 МГц или 10 МГц
Clock output	Тактовая частота на выходе. Если поддерживается Synce HW,

frequency	выходная частота тактового сигнала станции может быть настроена, возможные частоты: 1544 МГц, 2048 МГц или 10 МГц
SyncE Ports	
Port	Номер порта
SSM Enable	Включение и отключение функции SSM на этом порте.
Tx SSM	Мониторинг передаваемого SSM QL на этом порту.
Rx SSM	Мониторинг полученного SSM QL на этом порту.
1000BaseT Mode	Если порт находится в режиме 1000BaseT, то он контролирует режим, ведущий / ведомый. Чтобы принимать часы, он должен быть в ведомом режиме. Чтобы передавать часы, он должен быть в ведущем режиме.

3.2.32 MAC Table. Таблица MAC-адресов

Для доступа к настройкам необходимо перейти по вкладке Configuration→MAC Table.

MAC Address Table Configuration (Настройка таблицы MAC-адресов) (Рис. 3.87) (Табл. 3.85).

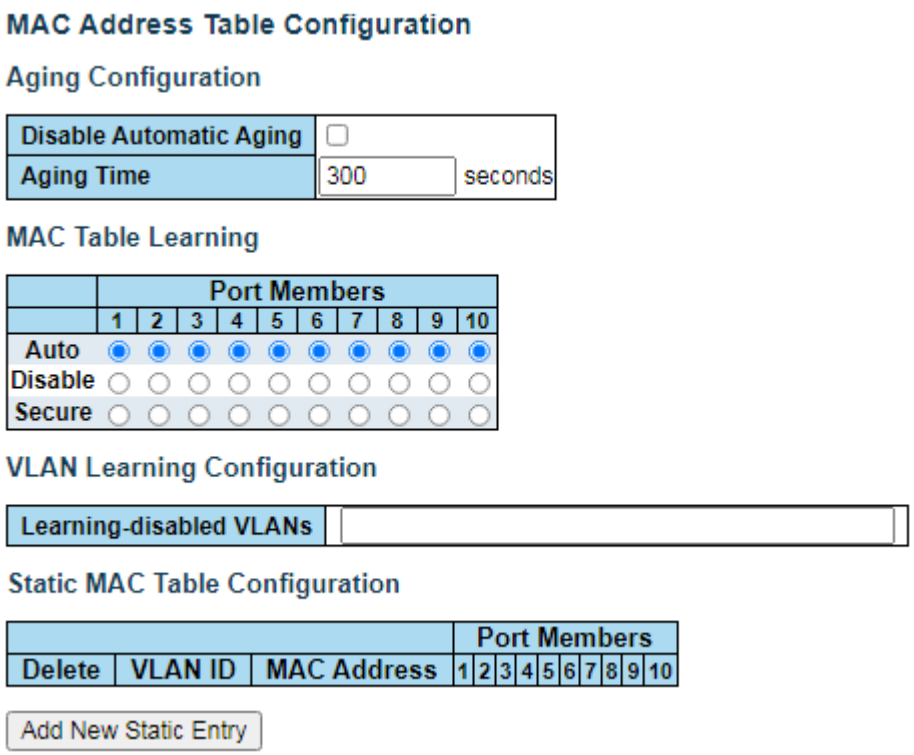


Рис. 3.87 – Настройка таблицы MAC – адресов

Таблица 3.85 – Настройка таблицы MAC - адресов

Disable Automatic Aging	Отключить автоматическое устаревание. MAC - адреса, полученные обучением будут присутствовать в таблице постоянно.

Aging Time	Задайте срок устаревания для MAC - адресов, полученных обучением, которые будут присутствовать в таблице MAC - адресов. Диапазон допустимых значений: от 10 до 1000000 секунд.
MAC Learning Table	На каждом порту можно включить одну из трех опций: • Auto (Автоматически): На данном порту обучение будет выполнено автоматически, как только будет принят неизвестный MACадрес. • Disable (Выключить): Функция обучения MAC-адресам выключена. • Secure (Только безопасные MAC-адреса): Обучение будет выполнено только для статических MAC-адресов, перечисленных в списке “Static MAC Table Configuration”. Другие MAC-адреса будут отброшены. Удостоверьтесь в том, что линия, используемая для управления коммутатором добавлена в таблицу статических MAC-адресов до включения режима обучения статическим адресам. В противном случае линия управления будет потеряна и ее можно будет восстановить только путем использования другого небезопасного порта либо при подключении коммутатора по последовательному интерфейсу.
Learning-disabled VLANs	В этом поле отображаются VLAN с отключенным обучением. Когда НОВЫЙ MAC-адрес поступает в виртуальную локальную сеть с отключенным обучением, MAC-адрес не будет изучен. По умолчанию поле пустое. Можно создать больше сетей VLAN, используя синтаксис списка, в котором отдельные элементы разделены запятыми. Диапазоны указываются с помощью тире, разделяющей нижнюю и верхнюю границы.
Static MAC Table Configuration (Настройка таблицы статических MAC - адресов): Эта таблица используется для установки статических MAC - адресов вручную. Общее число элементов таблицы, которые можно ввести, равно 64.	
Delete	Удаляет MAC - адрес из ячейки таблицы
VLAN ID	Задайте идентификатор VLAN ID для этого MAC - адреса.
Port Members	Установите (или снимите) флаги у соответствующих портов. Если входящий пакет имеет тот же MAC-адрес назначения, что и указанный в VID, он будет передан непосредственно в порт, отмеченный флагом.

Кнопка [Add New Static Entry] предназначена для добавления MAC – адреса.

3.2.33 VLANs

Использование виртуальных локальных сетей VLAN (Virtual Local Area Network) является популярным и недорогим способом сегментирования развернутой сети по логически сгруппированным устройствам безотносительно к их физическим соединениям. Сети VLAN также сегментируют сеть на различные широковещательные домены таким образом, что пакеты передаются на порты внутри VLAN, которой они принадлежат.

Сети VLAN повышают безопасность. Устройства, которые часто связываются друг с другом группируются в одну и ту же VLAN. Если устройства данной VLAN желают

связаться с устройствами в другой VLAN, трафик должен пройти через устройство маршрутизации или коммутатор 3-го уровня.

Сети VLAN упрощают управление трафиком. В обычных сетях, не сегментированных на VLAN, легко возникает перегрузка, обусловленная широковещательным трафиком, адресованного всем устройствам. Сводя к минимуму распространение широковещательного трафика по всей сети, сети VLAN облегчают работу устройствам группы, часто связывающимся с другими устройствами в той же VLAN за счет деления всей сети на несколько доменов вещания.

Сети VLAN упрощают замену устройств или их установку в другое место. В традиционных сетях, когда устройство требуется переместить в другое место (например, перенести со 2 этажа на 4 этаж), администратору сети потребуется изменить IP-адрес или даже подсеть сети либо заново протянуть кабели. Однако, при использовании сетей VLAN, исходные настройки можно сохранить, а прокладку кабелей – свести к минимуму.

Для доступа к настройкам необходимо перейти по вкладке Configuration→ VLANs.

VLAN Configuration (Настройка VLAN) (Рис. 3.88) (Табл. 3.86).

Рис. 3.88 – Настройка VLAN

Таблица 3.86 – Настройка VLAN

Global VLAN Configuration (Глобальная конфигурация VLAN)	
Allowed Access VLANs	Это поле показывает разрешенные Access VLAN, таким образом, эта настройка влияет только порты, настроенные в режиме access. Порты в других режимах являются членами всех VLAN, указанных в поле Allowed Access VLANs. По умолчанию, только VLAN 1 включено.
Ethertype for Custom Sports	Задайте тип ethertype/TPID, используемый для специализированных s-портов.
Port VLAN Configuration (Настройка VLAN на порту)	
Port	Номер порта. “*” означает применение ко всем портам.
Mode	Режим работы порта (по умолчанию access) определяет фундаментальное поведение порта. Порт может находиться в одном из трех режимов, как описано ниже: • Access (Доступ): Порты доступа, как правило, используется для подключения к конечным станциям. Динамические функции, такие как Voice VLAN могут добавить порт к большему количеству VLAN. Порты доступа имеют следующие характеристики: - Принадлежит ровно к одной VLAN (port VLAN). - Принимает нетегированные и Стегированные кадры. - Удаляет все кадры, которые не классифицируются как access

	VLAN. - На выходе все кадры, классифицированные как Access VLAN, передаются без тегов. Другие (динамически добавленные VLAN) передаются с тегами. • Trunk (Магистральные): Магистральные порты могут передавать трафик на несколько виртуальных локальных сетей одновременно и, как правило, используется для подключения к другим коммутаторам. Магистральные порты имеют следующие характеристики: - По умолчанию, trunk-порт является членом всех VLAN (1-4095). - VLAN, членом которых является магистральный порт, может быть ограничено путем использования Allowed VLAN. - Кадры, классифицированные с VLAN, членом которых порт не является, отбрасываются. - По умолчанию, все кадры, кроме кадров, классифицированных как port VLAN, передаются тегированными. Кадры, классифицированные в port VLAN не получают С-тегами на выходе - Можно настроить устройство тегировать на выходе все кадры, в этом случае только тегированные кадры будут приниматься на входе. • Hybrid (Гибридные): Гибридные порты схожи с портами типа Trunk во многих отношениях, но имеют дополнительные функции. В дополнение к характеристикам, описанным для trunk-портов, гибридные порты имеют следующие возможности: - Могут быть сконфигурирован как VLAN unaware, C-tag, S-tag или Scustom tag. - С возможностью фильтрации на входе. - Обработка входящих кадров и конфигурацию выходного тегирования можно настроить независимо.
Port VLAN	Задайте VLAN ID для порта. Допустимый диапазон значений: от 1 до 4095. По умолчанию задано 1.
Port Type	Выбор типа порта. Операция для входящего и исходящего трафика порта каждого типа описана в таблице 3.86a.
Ingress Filtering	Если фильтрация входящих кадров включена и входящий кадр не принадлежит VLAN, указанному на данном порту, такой кадр отбрасывается. Если фильтрация входящих кадров выключена и входящий кадр не принадлежит VLAN такой кадр принимается и передается в коммутатор. По умолчанию фильтрация входящих кадров включена для портов в режимах access и trunk.
Ingress Acceptance	Гибридные порты позволяют изменять режим обработки входящих кадров. • Tagged and Untagged: Тегированные и нетегированные кадры принимаются. • Tagged Only: Только тегированные кадры принимаются. Нетегированные - отбрасываются. • Untagged Only: Только нетегированные кадры принимаются. Тегированные - отбрасываются.
Egress Tagging	Порты в режимах Trunk и Hybrid могут контролировать тегирование кадров на выходе. • Untag Port VLAN: Кадры с меткой VLAN совпадающей с port VLAN передаются нетегированными. Остальные кадры передаются

	со своими метками. • Tag All: Все кадры передаются с метками. • Untag All: Все кадры передаются без меток. Эта опция доступна только в режиме Hybrid.
Allowed VLANs	Порты в режимах Trunk и Hybrid могут контролировать членами каких VLAN они могут становиться. Порты в режиме Access может быть членом только одной VLAN, access VLAN. Поле может быть оставлено пустым. В таком случае, порт не будет членом ни одной VLAN.
Forbidden VLANs	Порт может быть сконфигурирован так, чтобы никогда не становиться членом определенных VLAN. Это может быть полезно при использовании динамических протоколов, работающих с VLAN, например GVRP. По умолчанию, поле оставлено пустым и ограничений не накладывается.

Таблица 3.86а – Операция для входящего и исходящего трафика

Тип порта	Операция	
	Операция над входящим трафиком	Операция над исходящим трафиком
Unaware	Все входящие кадры, вне зависимости от того есть ли у них тег или нет, тегируются меткой port VLAN (PVID).	Разрешенные VLAN не удаляются на выходе
C-port	1. Если во входящем тегированном кадре TPID=0x8100, он передается. 2. Если кадр нетегированный или приоритетно тегированный в него добавляется тег port VLAN.	Исходящие кадры тегируются меткой C-tag.
S-port	Если во входящем тегированном кадре TIPID=0x8100 или 0x88A8, он передается. Если кадр Исходящие кадры тегируются меткой S-tag. 108 нетегированный или приоритетно тегированный в него добавляется тег port VLAN.	Исходящие кадры тегируются меткой S-tag.
S-Custom-port	1. Если во входящем тегированном кадре TIPID=0x8100 или Ethertype for Custom Sports он передается. 2. Если кадр нетегированный или приоритетно тегированный	Исходящие кадры тегируются меткой Custom S-tag.

	в него добавляется тег port VLAN.	

SVL (Рис. 3.89) (Табл. 3.87).

В SVL одна или несколько сетей VLAN сопоставляются с идентификатором фильтра (FID). По умолчанию существует взаимно-однозначное сопоставление от VLAN к FID, и в этом случае коммутатор действует как мост IVL, но с SVL несколько VLAN могут совместно использовать одни и те же записи в таблице MAC-адресов.

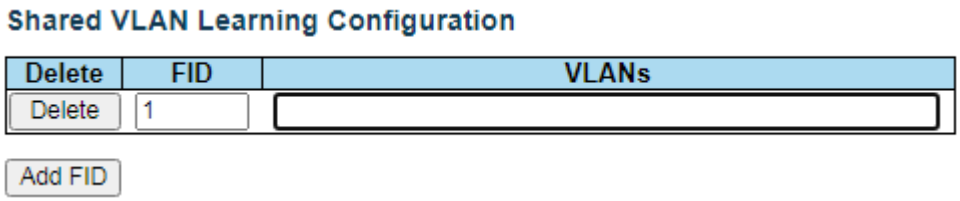


Рис. 3.89 – Настройка SVL

Таблица 3.87 – Настройка SVL

Delete	Удаление текущей записи
FID	Идентификатор фильтра (FID) - это идентификатор, который VLAN получает в таблице MAC-адресов, когда действует SVL. Никакие две строки в таблице не могут иметь одинаковый FID, и FID должен быть числом от 1 до 63 .
VLANs	Список сетей VLAN, отображаемых в FID. Синтаксис следующий: отдельные сети VLAN разделяются запятыми. Диапазоны указываются с помощью тире, разделяющей нижнюю и верхнюю границы. Одна и та же VLAN может быть членом только одного FID.

Кнопка Add FID предназначена для добавления новой строки в таблицу SVL. FID будет предварительно заполнен первым неиспользованным FID

3.2.34 VLAN Translation

Для доступа к настройкам необходимо перейти по вкладке Configuration→ VLAN Translation.

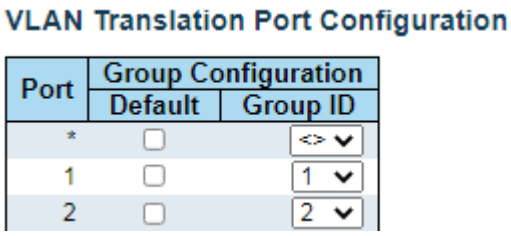


Рис. 3.90 – Настройка портов

Таблица 3.88 – Настройка портов

Port	Удаление текущей записи
Default	установите флаг, чтобы настроить порт коммутатора на использование группы трансляции VLAN по умолчанию.
Group ID	Номер группы. Порт можно настроить для использования любой из групп, но только одной.

VLAN Translation Mapping Table

Group ID	Direction	VID	TVID	
				⊕

Рис. 3.91 – Настройка групп

Таблица 3.89 – Настройка групп

Group ID	Номер группы.
DIR	Указывает направление трансляции VLAN и относится к коммутатору. Направление может быть 'Ingress', когда трансляция происходит на идентификаторе VLAN фреймов, поступающих в порт коммутатора, 'Egress', где трансляция происходит на идентификаторе VLAN фреймов, покидающих порт коммутатора, или 'Both', где перевод осуществляется по обоим указанным выше направлениям.
VID	идентификатор VLAN
TVID	преобразованный идентификатор VLAN, в который будет преобразован идентификатор VLAN кадра.

3.2.35 Private VLANs (Частные VLAN)

Для доступа к настройкам необходимо перейти по вкладке Configuration→ Private VLANs.

Эта страница используется для конфигурирования частных VLAN. Здесь можно добавить новые частные VLAN и изменить существующие VLAN. Частные VLAN основаны на маске порта источника и не соединяются с обычными VLAN. Это означает, что номера VLAN ID обычных VLAN и номера VLAN ID частных VLAN могут быть одинаковыми. Чтобы была возможна передача пакетов, порт должен принадлежать и обычной, и частной VLAN. По умолчанию, все порты VLAN являются неподдерживаемыми и принадлежат как обычной VLAN 1, так и частной VLAN 1.

Неподдерживаемый порт VLAN может принадлежать только одной обычной VLAN, однако он может принадлежать множеству частных VLAN.

PVLAN Membership (Принадлежность к Private VLAN) (Рис. 3.92) (Табл. 3.90).

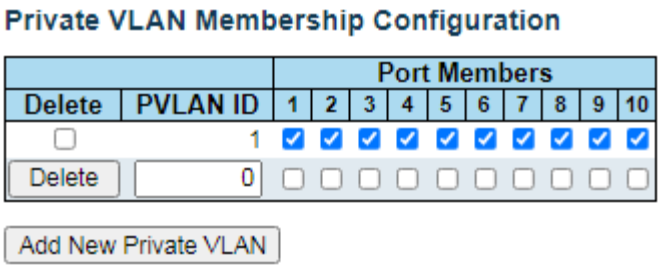


Рис. 3.92 – Принадлежность к Private VLAN

Таблица 3.90 – Принадлежность к Private VLAN

Delete	Удаляет текущую запись
PVLAN ID	Задайте номер PVLAN ID.
Port Members	Установите флаг в поле, если требуется, чтобы порт принадлежал определенной частной VLAN. Чтобы удалить порт из частной VLAN, снимите флаг в соответствующем поле.

Кнопка Add New Private VLAN предназначена для добавления новой принадлежности к VLAN.

Port Isolation (Изоляция порта) (Рис. 3.93) (Табл. 3.91).

Частные VLAN используются для группировки портов с целью предотвращения связи внутри PVLAN. Изоляция порта используется для предотвращения связи между портами клиентов в одной и той же VLAN или частной VLAN. Порт, который изолирован от остальных портов не может передавать какой-либо одноадресный, многоадресный или широковещательный трафик в любые другие порты той же самой VLAN или PVLAN.

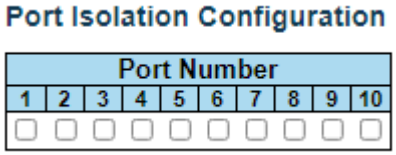


Рис. 3.93 – Изоляция порта

Таблица 3.91 – Изоляция порта

Port Number	Установите флаг, если желательно, чтобы порт или порты были изолированы от остальных портов.

3.2.36 VCL

Для доступа к настройкам необходимо перейти по вкладке Configuration→ VCL.

MAC-based (На основе MAC-адресов) (Рис. 3.94) (Табл. 3.92).

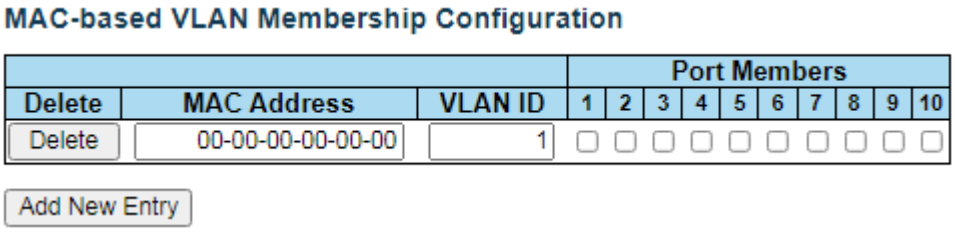


Рис. 3.94 – MAC-based

Таблица 3.92 – MAC-based

Delete	Удаляет текущую запись
MAC Address	Указан MAC - адрес источника. Имейте в виду, что MAC - адрес источника может отображаться только в один VLAN ID.
VLAN ID	Отображает данный MAC-адрес в связанный с ним VLAN ID.
Port Members	Порты, которые принадлежат данной VLAN.

Кнопка Add New Entry предназначена для добавления новой записи.

Protocol to Group (Рис. 3.95) (Табл. 3.93).

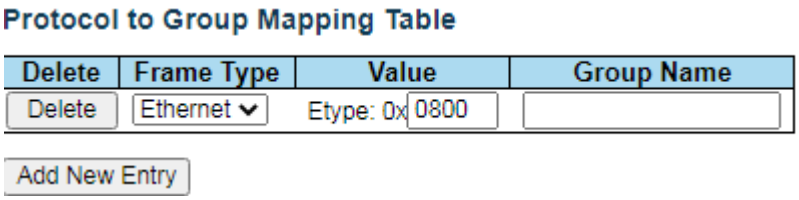


Рис. 3.95 – Protocol to Group

Таблица 3.93 – Protocol to Group

Delete	Удаляет текущую запись
Frame Type	Можно выбрать один из трех типов кадров. Поле значения (value) изменится соответствующим образом автоматически.
Value	• Ethernet: Значение типа Ether (Etype). По умолчанию задано 0x0800. Диапазон допустимых значений: от 0x0600 до 0xffff. • SNAP: Для типа кадра SNAP отображаются значения идентификатора OUI (Organizationally Unique Identifier – уникальный идентификатор организации) и идентификатора протокола PID (Protocol ID). • OUI: Значение в формате xx-xx-xx, где каждая пара (xx) в строке является шестнадцатиричным значением в диапазоне 0x00-0xff. • PID: Если для OUI задано шестнадцатиричное значение 000000, то для protocol ID в поле значения типа Ethernet указан протокол, работающий на вершине SNAP. Если OUI является

	идентификатором определенной организации, то protocol ID – это значение, назначенное этой организацией протоколу, работающему на вершине SNAP. Другими словами, если в поле OUI задано 00-00- 00, то значение PID будет etherType (0x0600-0xffff). Если значение OUI отличается от 00-00-00, то правильное значение PID будет любым значением в диапазоне от 0x0000 до 0xffff. • LLC (Логическое управление линией): Включает в себя значения DSAP (Destination Service Access Point – точка доступа назначения услуг) и SSAP (Source Service Access Point - точка доступа источника услуг). По умолчанию значение равно 0xff. Диапазон допустимых значений: от 0x00 до 0xff.
Group Name	Имя группы. Поле может содержать не более 16 алфавитно-цифровых символов (a-z; AZ) или целых чисел (0-9).

Кнопка Add New Entry предназначена для добавления новой записи.

Group to VLAN (Отображение группы в VLAN) (Рис. 3.96) (Табл. 3.94).

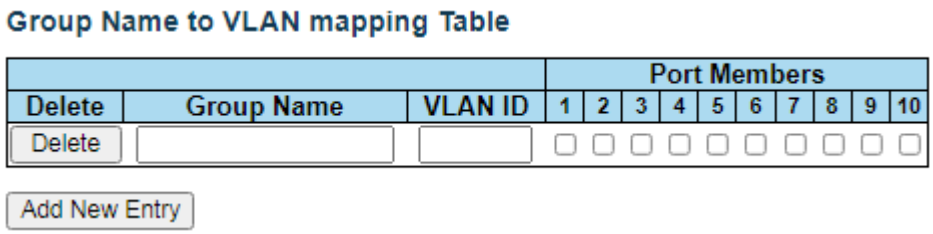


Рис. 3.96 – Group to VLAN

Таблица 3.94 – Group to VLAN

Delete	Удаляет текущую запись
Group Name	имя группы. Поле может содержать не более 16 алфавитно-цифровых символов (a-z; A-Z) или целых чисел (0-9).
VLAN ID	номер VLAN ID
Port Members	Назначенные порты

Кнопка Add New Entry предназначена для добавления новой записи.

IP Subnet-based VLAN (VLAN на основе IP-подсети) (Рис. 3.97) (Табл. 3.95).

На странице IP Subnet-based VLAN configuration можно задать отображение нетегированных входящих кадров в конкретную VLAN, если в таблице отображения IP-подсети в VLAN найден IP-адрес источника. Когда включена классификация VLAN на основе IP-подсети, адрес источника нетегированных входящих кадров проверяется по таблице отображения IP- подсети в VLAN. Если адрес источника для данной подсети

найден, то кадрам назначается VLAN, указанный в этой ячейке таблицы. Если согласующейся IP-подсети не обнаружено, нетегированные кадры классифицируются, как принадлежащие VLAN, которой принадлежит принявший их порт (с номером PVID).

IP Subnet-based VLAN Membership Configuration

				Port Members									
Delete	IP Address	Mask Length	VLAN ID	1	2	3	4	5	6	7	8	9	10
Delete	0.0.0.0	24	1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Add New Entry

Рис. 3.97 – VLAN на основе подсетей

Таблица 3.95 – VLAN на основе подсетей

Delete	Удаляет текущую запись
IP Address	IP-адрес для данного правила
Mask Length	Длина маски сети
VLAN ID	Номер VLAN ID
Port Members	Порты, назначенные данному правилу

Кнопка Add New Entry предназначена для добавления новой записи.

3.2.37 Voice VLAN. Голосовой VLAN

Для доступа к настройкам необходимо перейти по вкладке Configuration→ Voice VLAN.

Configuration (Настройка) (Рис. 3.98) (Табл. 3.96).

Voice VLAN Configuration

Mode	Disabled
VLAN ID	1000
Aging Time	86400 seconds
Traffic Class	7 (High)

Port Configuration

Port	Mode	Security	Discovery Protocol
*	<>	<>	<>
1	Disabled	Disabled	OUI
2	Disabled	Disabled	OUI
3	Disabled	Disabled	OUI

Рис. 3.98 – Настройка

Таблица 3.96 – Настройка

Voice VLAN Configuration (Настройка голосовой VLAN)	
Mode	Включить/выключить голосовой VLAN. Прежде чем включить голосовой VLAN, отключите MSTP, чтобы избежать конфликта.
VLAN ID	Идентификатор VLAN
Aging Time	Указывает время безопасного обучения. Допустимый диапазон составляет от 10 до 10000000 секунд.
Traffic Class	Указывает класс трафика. Весь трафик в Voice VLAN будет иметь этот класс.
Port Configuration (Настройка порта)	
Port	Номер порта
Mode	• Disabled – отключен; • Auto - включение режима автоматического определения; • Forced - принудительное подключение.
Security	Включить/выключить режим безопасности порта VLAN. Когда эта функция включена, все нетелефонные MACадреса в VLAN будут заблокированы на 10 секунд.
Discovery Protocol	Указывает протокол обнаружения порта. Работает только при режиме «Auto». Возможные протоколы обнаружения: • OUI: обнаружение телефонного устройства по адресу OUI. • LLDP: обнаружение телефонного устройства LLDP. • Both: OUI и LLDP. Мы должны включить функцию LLDP перед активацией протокола обнаружения на «LLDP» или «Both». Изменение протокола обнаружения на «OUI» или «LLDP» приведет к перезапуску процесса автоматического обнаружения.

OUI Table (Таблица OUI) (Рис. 3.99) (Табл. 3.97).

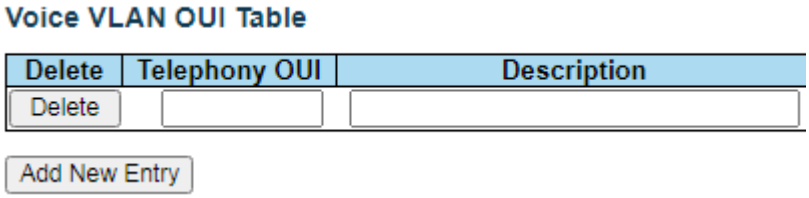


Рис. 3.99 – Таблица OUI

Таблица 3.97 – Таблица OUI

Delete	Удаляет текущую запись
Telephony OUI	Адрес OUI - это глобальный уникальный идентификатор, присвоенный IEEE. Он должен состоять из 6 символов, формат ввода - «xx-xx-xx» (x - шестнадцатеричная цифра).
Description	Описание адреса OUI. Допустимая длина строки от 0 до 32.

Кнопка Add New Entry предназначена для добавления новой записи.

3.2.38 QoS (Качество обслуживания)

Сетевой трафик всегда непредсказуем, поэтому основным фактором обеспечения качества является предоставление наилучшего способа доставки. Для преодоления этой проблемы используется понятие качества обслуживания (Quality of Service (QoS)) применяемое ко всей сети. Гарантируется, что сетевой трафик будет приоритезирован в соответствии с заданным критерием, и прием будет производиться с использованием обработки по приоритетам.

QoS позволяет назначить различные классы сетевых услуг различным типам трафика, например, мультимедийному, видео, трафику конкретного протокола, критичному по времени трафику, трафику резервного копирования файлов. Чтобы задать приоритеты пакетов на данном коммутаторе, перейдите на страницу “Port Classification” (Классификация порта).

Для доступа к настройкам необходимо перейти по вкладке Configuration→ QoS.

Port Classification (Классификация на портах) (Рис. 3.100) (Табл. 3.98).

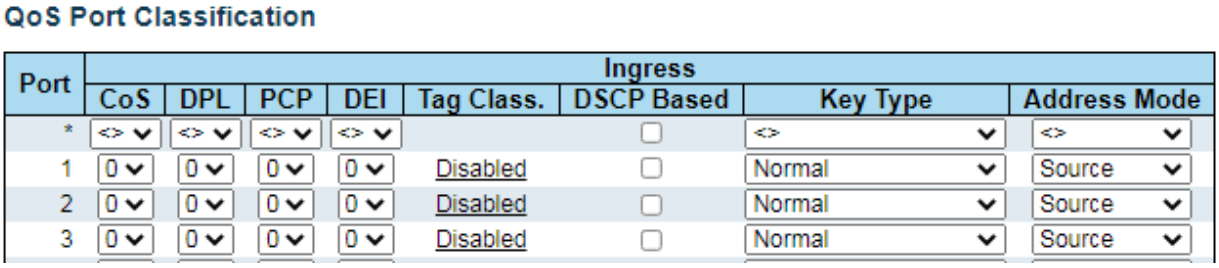


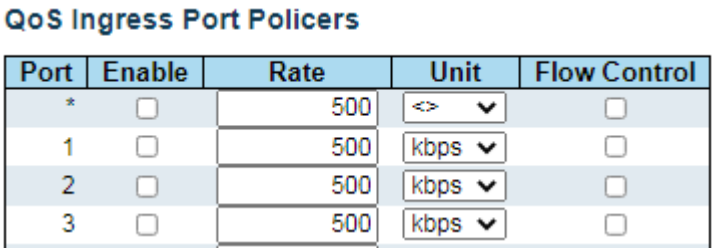
Рис. 3.100 – Классификация QoS на портах

Таблица 3.98 – Классификация QoS на портах

Port	Номер порта. “*” означает применение ко всем портам.
Cos	Класс CoS, выбираемый по умолчанию. Класс CoS с номером 0 имеет наименьший приоритет. По умолчанию задано 0.
DP Level	Выберите приоритет отбрасывания: 0: Подтвержденные кадры. 1: Кадры, которые могут быть отброшены.
PCP	Выберите соответствующее значение пользовательского приоритета (Priority Code Point) для нетегированных кадров.
DEI	Выберите соответствующее значение индикатора отбрасывания по критерию (Drop Eligible Indicator) для нетегированных кадров.
Tag Class	В этом поле отображен режим классификации для тегированных кадров на данном порту: • Disabled (Выключен): Для тегированных кадров используется класс QoS и уровень DP по умолчанию. • Enabled (Включен): Для тегированных кадров используется значение PCP и DEI из таблицы (PCP, DEI) to (QoS class, DP level) Mapping.
DSCP Based	Установите флаг в поле, чтобы включить QoS на основе DSCP (входящий порт).
Key Type	Тип определяющего ключа, сгенерированный для кадров, полученных через порт. Допустимые значения:

	Normal: соответствует внешнему тегу, SMAC/DMAC, IP-протоколу, DSCP, SIP/DIP, SPORT и DPORT. Double Tag: четверть ключа, соответствует внутреннму и внешнему тегу. IP Address: половина ключа, совпадение внутреннего и внешнего тега, SIP и DIP. Для кадров, не относящихся к IP, используйте только внешний тег. MAC and IP Address: Полный ключ, совпадающий внутренний и внешний тег, SMAC, DMAC, SIP и DIP.
Address Mode	режим IP/MAC-адреса, определяющий, должна ли классификация QCL основываться на адресах источника (SMAC/SIP) или назначения (DMAC/DIP) на этом порту. Этот параметр используется только в том случае, если тип ключа Normal . Допустимыми значениями являются: Source: Позволяет сопоставлять SMAC/SIP. Destination: Позволяет сопоставлять DMAC/DIP.

Port Policing (Ограничение скорости на портах) (Рис. 3.101) (Табл. 3.99).



QoS Ingress Port Policers

Port	Enable	Rate	Unit	Flow Control
*	☐	500	<>	☐
1	☐	500	kbps	☐
2	☐	500	kbps	☐
3	☐	500	kbps	☐

Рис. 3.101 – Ограничение скорости на портах

Таблица 3.99 – Ограничение скорости на портах

Port	Номер порта. “*” означает применение ко всем портам.
Enabled	Установите флаг в этом поле, чтобы включить функцию ограничения скорости на порту.
Rate	Задайте скорость, до которой будет ограничена скорость на порту. По умолчанию задано 500 кбит/с. Допустимый диапазон для kbps (кбит/с) и fps (кадров/с): от 100 до 1000000. Допустимый диапазон для Mbps (Мбит/с) и kfps (кадров/с): от 1 до 3300 Мбит/с.
Unit	Единицы измерения ограничения скорости
Flow Control	Если управление потоком включено и порт работает в режиме управления потоком, то будут отправляться кадры pause, вместо отбрасывания входящих кадров.

Queue Policing (Ограничение скорости в очередях) (Рис. 3.102) (Табл. 3.100).

QoS Ingress Queue Policers

Port	Queue 0	Queue 1	Queue 2	Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable
*	☐	☐	☐	☐	☐	☐	☐	☐
1	☐	☐	☐	☐	☐	☐	☐	☐
2	☐	☐	☐	☐	☐	☐	☐	☐
3	☐	☐	☐	☐	☐	☐	☐	☐

Рис. 3.102 – – Ограничение скорости в очередях

Таблица 3.100 – – Ограничение скорости в очередях

Port	Номер порта. “*” означает применение ко всем портам.
Queue 0~7 Enable	Установите флаг в соответствующем поле, чтобы включить функцию ограничения скорости в очередях на портах коммутатора
Rate	Скорость, до которой будет ограничена скорость в очереди. По умолчанию задано 500 кбит/с. Допустимый диапазон значений для kbps (кбит/с): от 100 до 1000000. Допустимый диапазон значений для Mbps (Мбит/с): от 1 до 3300 Мбит/с.
Unit	Единицы измерения ограничения скорости очереди входящих кадров.

Port Scheduler (Рис. 3.103) (Табл. 3.101).

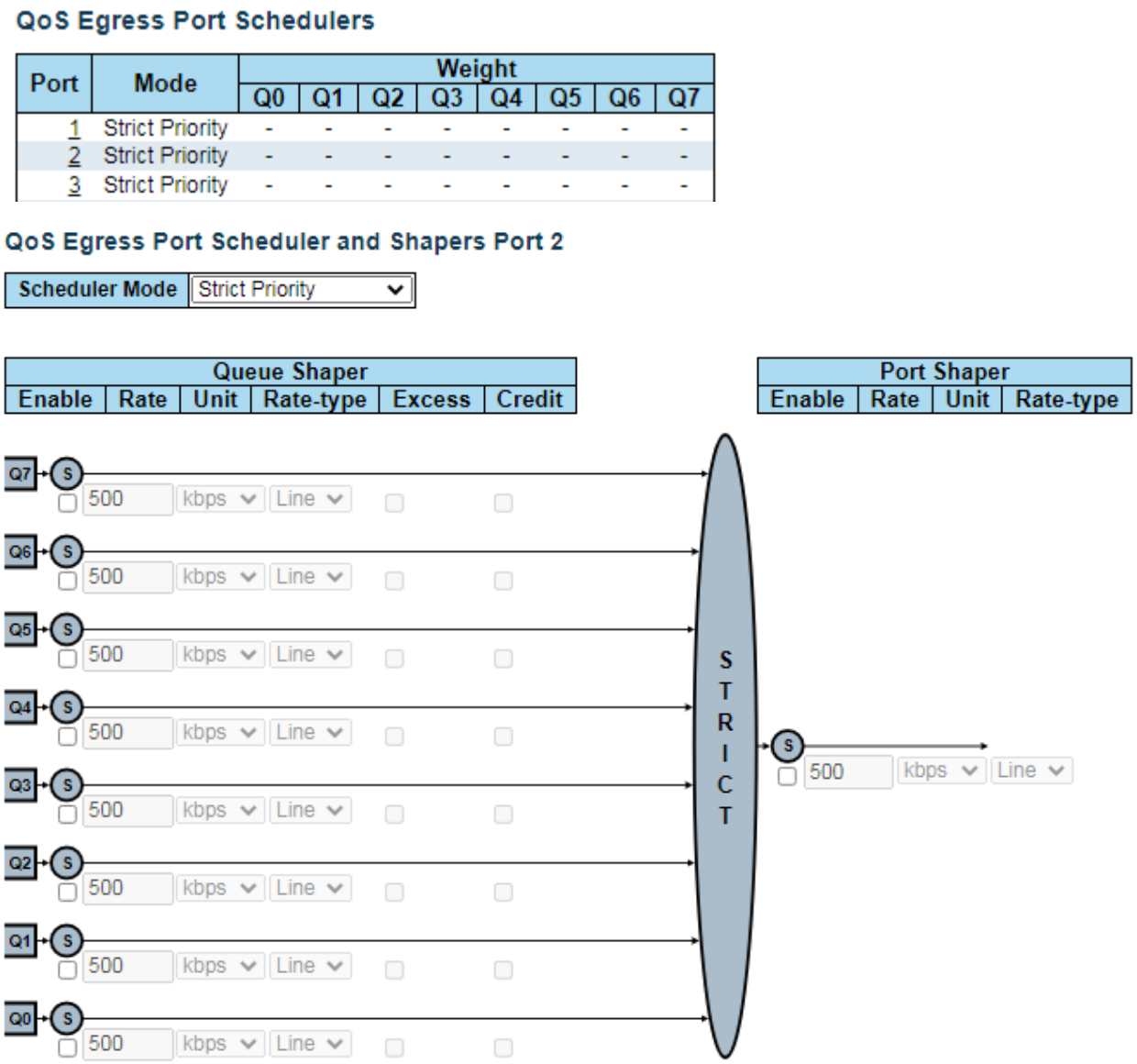


Рис. 3.103 – Port Scheduler

Таблица 3.101 – Port Scheduler

Port	Нажмите мышью на порт, чтобы задать детальные настройки диспетчера порта.
Mode	Отображается выбранный режим работы
Weight	Отображается вес в процентах, присвоенный очередям Q0~Q7.
Scheduler Mode	Устройство обеспечивает два режима работы с очередями. • Strict mode (Строгий режим работы): В этом режиме кадры из выходных очередей с более высокими приоритетами будут передаваться первыми (по сравнению с кадрами, находящимися в очередях с низкими приоритетами). • Weight mode (Режим работы с весами): Для очередей с взвешиванием DWRR (Deficit Weighted Round-Robin – циклическое взвешивание с учетом дефицита) должен быть задан вес в каждой очереди. Обслуживание очередей при DWRR во многом подобно WRR, однако следующая очередь обслуживается только тогда,

	когда ее счетчик дефицита (Deficit Counter) становится меньше размера переданного пакета.
Queue Shaper (Формирователь трафика очереди)	
Enable	Нажмите мышью это поле, чтобы включить формирователь для некоторой очереди на выбранном порту.
Rate	Задайте скорость, до которой формирователь очереди будет ограничивать скорость. По умолчанию задано 500 кбит/с. Допустимый диапазон значений для kbps (кбит/с): от 100 до 1000000. Допустимый диапазон значений для Mbps (Мбит/с): от 1 до 3300 Мбит/с.
Unit	Выберите единицы измерения скорости, которые будет использовать формирователь очереди при ограничении скорости.
Port Shaper (Формирователь трафика порта): Задайте скорость, с которой трафик может покидать данную очередь.	
Enable	Установите флаг в этом поле, чтобы включить формирователь трафика порта.
Rate	Задайте скорость, до которой будет ограничена скорость на выходе формирователя трафика порта. По умолчанию задано 500 кбит/с. Допустимый диапазон значений для kbps (кбит/с): от 100 до 1000000. Допустимый диапазон значений для Mbps (Мбит/с): от 1 до 3300 Мбит/с.
Unit	Выберите единицы измерения скорости.

Port Shaping (Формирование трафика портов) (Рис. 3.104).

Нажмите на номер порта, чтобы изменить или переустановить настройки формирователя трафика порта, в частности, ограничение скорости.

QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-

Рис. 3.104 – Port Shaping

Port Tag Remarking (Изменение тегов на порту) (Рис. 3.105) (Табл. 3.102).

QoS Egress Port Tag Remarking

Port	Mode
1	Classified
2	Classified
3	Classified

QoS Egress Port Tag Remarking Port 1

Tag Remarking Mode	Classified

QoS Egress Port Tag Remarking Port 1

Tag Remarking Mode	Default

PCP/DEI Configuration

Default PCP	0
Default DEI	0

QoS Egress Port Tag Remarking Port 1

Tag Remarking Mode	Mapped

(CoS, DPL) to (PCP, DEI) Mapping

CoS	DPL	PCP	DEI
*	*	<>	<>
0	0	1	0
0	1	1	1
1	0	0	0
1	1	0	1
2	0	2	0
2	1	2	1
3	0	3	0
3	1	3	1
4	0	4	0
4	1	4	1
5	0	5	0
5	1	5	1
6	0	6	0
6	1	6	1
7	0	7	0
7	1	7	1

Рис. 3.105 – Изменение тегов на порту

Таблица 3.102 – Изменение тегов на порту

Port	Нажмите мышью на порт, чтобы задать детальные настройки.
Tag Remarking Mode	Выберите соответствующий режим работы изменения тегов на этом порту. • Classified (Классифицированный): Используются классифицированные значения PCP/DEI. • Default (Значения по умолчанию): Используются значения PCP/DEI, заданные по умолчанию - PCP:0; DEI:0). • Mapped (Отображение): Используется отображение значений классов QoS и уровней DP в значения PCP/DEI.
PCP/DEI Configuration	Настройка значений PCP/DEI для режима Default.
QoS Class/DP level	Показаны опции отображения для значений классов QoS и уровней DP (приоритетов отбрасывания).
PCP	Изменение тегов согласующихся исходящих кадров в соответствии с указанным приоритетом Priority Code Point либо в соответствии с пользовательским приоритетом. (Диапазон: 0~7; По умолчанию

	задано: 0)
DEI	Изменение тегов согласующихся исходящих кадров в соответствии с заданным индикатором соответствия критерию отбрасывания (Drop Eligible Indicator). (Диапазон: 0~1; По умолчанию задано: 0)

Port DSCP (Настройка трансляции DSCP на порту) (Рис. 3.106) (Табл. 3.103).

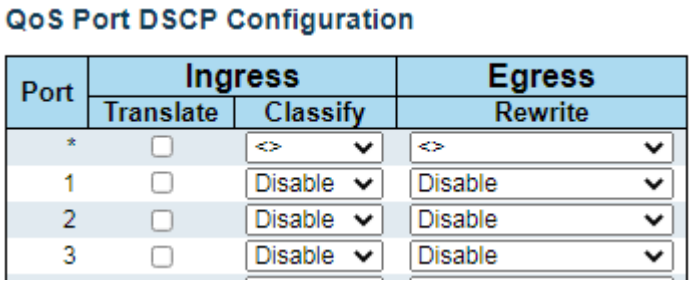


Рис. 3.106 – Настройка трансляции DSCP на порту

Таблица 3.103 – Настройка трансляции DSCP на порту

Port	Номер порта. “*” означает применение ко всем портам.
Ingress Translate	Установите флаг в поле, чтобы включить трансляцию значений DSCP на основе выбранного метода классификации
Ingress Classify	Выберите соответствующий метод классификации: • Disable (Выключить): Классификация DSCP входящих кадров не выполняется. • DSCP=0: Классификация выполняется, если DSCP входящих кадров равен 0. • Selected (Выбрано): Классифицируются только DSCP, для которых включена классификация в таблице трансляции DSCP. • All (Все): Классифицируются все поля DSCP.
Egress Rewrite	Значения DSCP исходящих кадров будут переписаны на порту. • Disable (Выключить): Перезапись значений DSCP исходящего трафика выключена. • Enable (Включить): Перезапись значений DSCP исходящих кадров включена, но отображение после перезаписи не выполняется. • Remap DP aware (Отображение поддерживаемых DP заново): Кадр с DSCP, поступивший от анализатора, снова отображается и помечается новым значением DSCP. В зависимости от уровня DP кадра, новое значение DSCP берется из таблицы трансляции DSCP из поля Egress Remap DP0 или DP1. • Remap DP aware (Отображение неподдерживаемых DP заново): Кадр с DSCP, поступивший от анализатора снова отображается и помечается новым значением DSCP. Новое значение DSCP всегда берется из таблицы трансляции DSCP из поля Egress Remap DP0.

DSCP-Based QoS (Настройка качества обслуживания по DSCP) (Рис. 3.107) (Табл. 3.104).

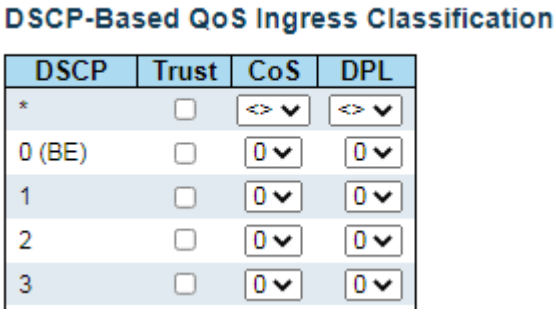


Рис. 3.107 – Настройка качества обслуживания по DSCP

Таблица 3.104 – Настройка качества обслуживания по DSCP

DSCP	Значение DSCP входящего пакета. Диапазон допустимых значений DSCP: от 0 до 63.
Trust	Установите флаг в этом поле, чтобы указать, что значение DSCP является надежным. Только надежные значения DSCP отображаются в соответствующий класс QoS и приоритет отбрасывания DPL (drop precedence level). Кадры с ненадежными значениями DSCP считаются не-IP кадрами.
CoS	Выберите класс QoS для соответствующего значения DSCP для 123 обработки входящих кадров. По умолчанию задано 0. Диапазон допустимых значений: от 0 до 7
DPL	Выберите приоритет отбрасывания DPL для соответствующего значения DSCP для обработки входящих кадров. По умолчанию задано 0. Значение “1” дает более высокий приоритет отбрасывания

DSCP Translation (Трансляция DSCP) (Рис. 3.108) (Табл. 3.105).

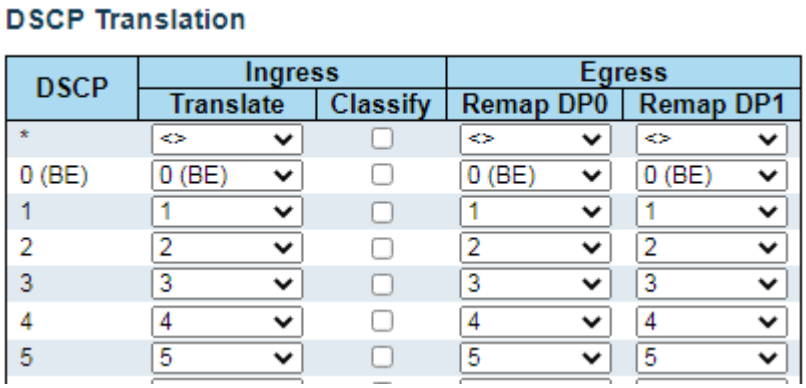


Рис. 3.108 – Трансляция DSCP

Таблица 3.105 – Трансляция DSCP

DSCP	Значение DSCP входящего кадра. Диапазон допустимых значений

	DSCP: от 0 до 63.
Ingress Translate	Включает трансляцию значений DSCP входящих кадров на основе заданного метода классификации.
Ingress Classify	Включает классификацию на входящей стороне, как определено в таблице настройки DSCP QoS на порту.
Egress Remap	Заново отображает значение DP в выбранное значение DSCP.

DSCP Classification (Классификация DSCP) (Рис. 3.109) (Табл. 3.106).

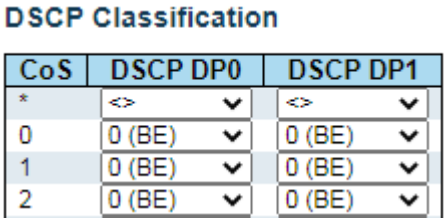


Рис. 3.109 – Классификация DSCP

Таблица 3.106 – Классификация DSCP

CoS	Список актуальных значений классов QoS
DSCP:	Выберите значение DSCP для отображения в класс QoS

QoS Control List Configuration (Список управления QoS) (Рис. 3.110) (Табл. 3.107).

Список управления качеством обслуживания используется для установки правил обработки входящих пакетов по типу кадра, MAC-адресу, значениям VID, PCP, DEI. Как только QCE привязан к порту, трафик согласуется с первым элементом списка управления QoS, которому назначен класс QoS, уровень приоритета отбрасывания и значение DSCP. Трафику, не согласующемуся ни с какими QCE, назначается класс QoS, используемый для порта по умолчанию.

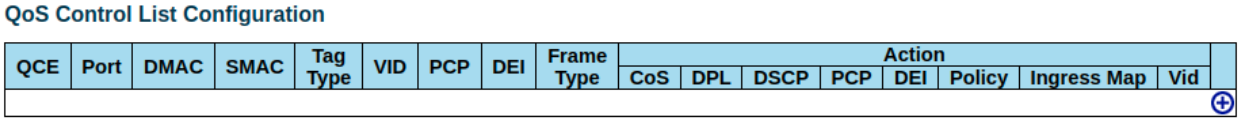


Рис. 3.110 – Список управления QoS

Таблица 3.107 – Список управления QoS

QCE	Отображается номер элемента списка QCL
Port	Отображается номер порта, использующего этот QCL
DMAC	MAC-адрес назначения. Возможны следующие значения: Any (Любой), Broadcast (Широковещательный), Multicast

	(Многоадресный), Unicast (Одноадресный).
SMAC	MAC - адрес источника
VID	Отображается VLAN ID (1-4095)
PCP	Отображается значение PCP.
DEI	Отображается значение DEI
Frame type	Отображается тип кадра, поиск которого будет производиться во входящих кадрах. Возможны следующие типы кадров: Any (Любой), Ethernet, LLC SNAP, IPv4, IPv6.
Action	Отображается операция классификации, выполняемая на входящих кадрах, когда настройки параметров согласуются с содержимым кадра.

Storm Control (Управление широковещательным штормом) (Рис. 3.111) (Табл. 3.108).

Управление широковещательным штормом используется для предотвращения ухудшения производительности сети или полного прекращения ее работы. Управление осуществляется путем установки пороговых значений для трафика, подобного широковещательному, одноадресному или многоадресному. Ухудшение производительности сети или полное прекращение ее работы могут быть обусловлены неполадками в работе сетевых устройств, плохой отладкой и неправильными настройками прикладного ПО. Защита сети от штормов может быть осуществлена путем установки пороговых значений для определенного трафика на устройстве. Любые указанные пакеты, при приеме которых превышено заданное пороговое значение, будут отброшены.

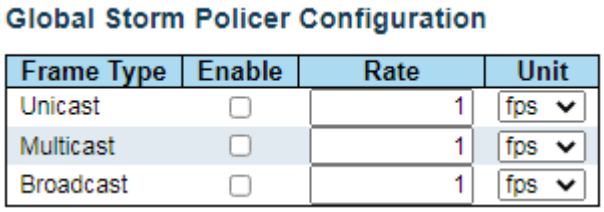


Рис. 3.111 – Управление широковещательным штормом

Таблица 3.108 – Управление широковещательным штормом

Enable	Включает подавление шторма для пакетов типов Unicast (Одноадресный), Multicast (Многоадресный), Broadcast (Широковещательный).
Rate	Выберите пороговое значение в пакетах в секунду. Принятые пакеты, при которых превышено выбранное значение, будут отброшены.
Unit	Единицы измерения

Weighted Random Early Detection (WRED) (Рис. 3.112) (Табл. 3.109).

Отслеживает длину очереди и отбрасывает некоторый процент пакетов в очереди для улучшения производительности сети.

Weighted Random Early Detection Configuration

Queue	Enable	Min	Max	Max Unit
0	☐	0	50	Drop Probability
1	☐	0	50	Drop Probability
2	☐	0	50	Drop Probability
3	☐	0	50	Drop Probability

Рис. 3.112 – WRED

Таблица 3.109 – WRED

Queue	Номер очереди (CoS)
Enable	Определяет, включен ли WRED для этой записи
Min	Нижний порог уровня заполнения.
Max	Верхний порог уровня заполнения.
Max Unit	Управляет вероятностью падения для кадров

3.2.39 Mirroring (Зеркалирование)

Для отладки сетевых проблем, исходящий трафик может быть скопирован на зеркальном порту, где может быть подключен анализатор.

Для доступа к настройкам необходимо перейти по вкладке Configuration→ Mirroring

Mirroring (Зеркалирование) (Рис. 3.113) (Табл. 3.110).

Mirror & RMirror Configuration Table

Session ID	Mode	Type	VLAN ID	Reflector Port
1	Disabled	Mirror	-	-
2	Disabled	Mirror	-	-
3	Disabled	Mirror	-	-

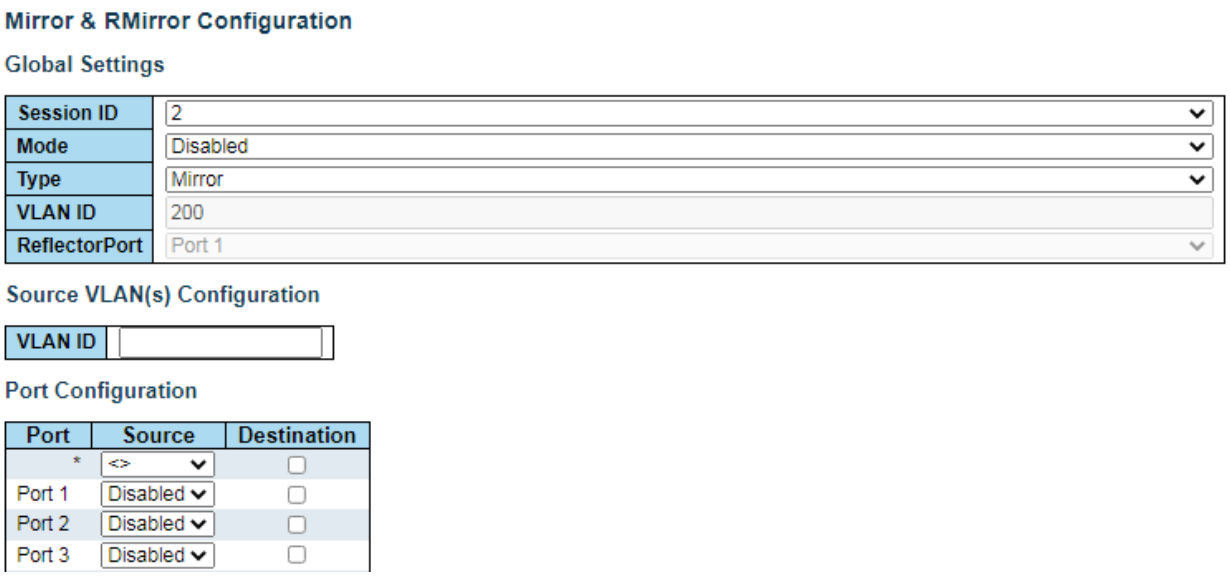


Рис. 3.113 – Зеркалирование

Таблица 3.110 – Зеркалирование

Session ID	Идентификатор сессиия. выберите идентификатор сеанса для настройки
Mode	Включение/выключение зеркального отображения или дистанционного зеркалирования.
Type	• Mirror – Зеркало; • Source – Источник; • Intermediate – Промежуточный; • Destination – Назначение;
VLAN ID	Идентификатор VLAN указывает, куда будет скопирован мониторный пакет. Идентификатор VLAN по умолчанию - 200.
Reflector Port	Порт с которого отправляется трафик
Source VLANs	Зеркалирование на основе VLAN
Port Configuration (Настройки порта)	
Port	Номер порта
Source	Имеется четыре режима, которые можно использовать на каждом порту индивидуально. • Disabled (Выключен): Функция зеркалирования на данном порту выключена. • Rx only (Только принимаемый трафик): На зеркальный порт будут направлены только кадры, принятые данным портом. • Tx only (Только передача): На зеркальный порт будут направлены только кадры, переданные данным портом. • Enable (Включить): На зеркальный порт будут переданы кадры, принятые и переданные данным портом.
Destination	Порт назначения, который получает копию трафика из исходного порта.

3.2.40 UPnP

Для доступа к настройкам необходимо перейти по вкладке Configuration→UPnP.

Настройка UPnP (Рис. 3.114) (Табл. 3.111)

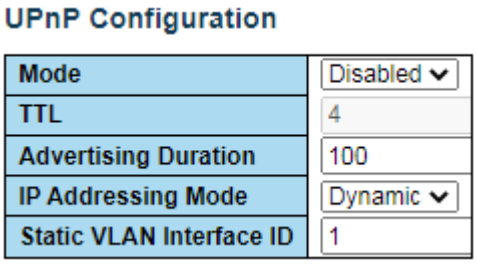


Рис. 3.114 – Настройка UPnP

Таблица 3.111 – Настройка UPnP

Mode	Включает или выключает функцию UPnP. При включении автоматически создается два правила списка доступа (ACE) для перенаправления соответствующих UPnP пакетов к процессору. При выключении правила автоматически удаляются.
TTL	Параметр TTL (Time to live – время жизни) используется для указания того, сколько шагов может сделать уведомление UPnP (SSDP) до своего исчезновения.
Advertising Duration	Этот параметр определяет, насколько часто могут посылаться уведомления UPnP. Длительность переносится пакетами протокола SSDP (Simple Service Discover Protocol), которые информируют пункт управления о том, насколько часто следует принимать сообщения с уведомлениями SSDP от коммутатора. По умолчанию установлена длительность уведомления 100 секунд. Однако, вследствие ненадежности протокола UDP рекомендуется уменьшать длительность, так как чем она меньше, тем быстрее обновляется состояние UPnP.
IP Addressing Mode	Режим IP-адресации предоставляет два способа определения назначения IP-адреса: **Динамический**: Выбор по умолчанию для UPnP. Модуль UPnP помогает пользователям выбрать IP-адрес коммутатора. Он находит первый доступный системный IP-адрес. **Статический**: Пользователь указывает IP-интерфейс VLAN для выбора IP-адреса коммутирующего устройства.
Static VLAN Interface ID	Индекс конкретного интерфейса IP VLAN. Он будет применяться только в статическом режиме IP-адресации. Допустимые настраиваемые значения находятся в диапазоне от 1 до 4095. Значение по умолчанию - 1.

3.2.41 PTP

Для доступа к настройкам необходимо перейти по вкладке Configuration→PTP.

PTP External Clock Mode

One_PPS_Mode	Disable
External Enable	False
Adjust Method	Auto
Clock Frequency	1

PTP Clock Configuration

Delete	Clock Instance	HW Domain	Device Type	Profile
Delete	0	0	Ord-Bound	No Profile

Add New PTP Clock | Save | Reset

Рис. 3.114 – Настройка PTP

Таблица 3.111 – Настройка PTP

One_PPS_Mode	Это поле выбора позволит вам выбрать конфигурацию One_pps_mode. Возможны следующие значения: Output: включает выход тактовой частоты 1 pps. Input: включает вход тактовой частоты 1 pps. Disable: отключает вход или выход тактовой частоты 1 pps.
External Enable	Настройка внешнего тактового выхода. Возможны следующие значения: True: Включает внешний тактовый выход. False: Отключает внешний тактовый выход.
Adjust Method	Настройка частоты: LTC: выбор управления частотой счетчика местного времени (LTC). Auto: автоматический выбор управления часами на основе профиля PTP и доступных ресурсов HW.
Clock Frequency	Тактовая частота. Возможный диапазон значений: 1 - 25000000 (1 - 25 МГц).
PTP Clock Configuration	
Delete	Удаляет текущую запись
Clock Instance	номер экземпляра часов
HW Domain	указывает на HW-тактовый домен, используемый часами.
Device Type	указывает тип экземпляра часов. Ord-Bound: обычные часы с ограничением. P2p Transp: одноранговые прозрачные часы E2e Transp: сквозные прозрачные часы, Master Only: только мастер. Slave Only: только ведомое устройство
Profile	профиль, используемый часами.

3.2.42 MRP и MVRP

Multiple Registration Protocol (MRP) - это общая структура, рекомендованная IEEE для использования в сетевых мостах, сетевых коммутаторах, или других аналогичных устройствах с возможностью регистрации и перерегистрации специальных атрибутов, таких как идентификаторы VLAN и членство в мультикастовых группах в больших локальных сетях LAN.

Протокол множественных регистраций **VLAN** Multiple VLAN Registration Protocol (MVRP) является сетевым протоколом второго уровня для автоматической конфигурации информации **VLAN** в коммутаторах. Он был определён приложением **802.1ak** к рекомендациям **IEEE 802.1Q**-2005.

В пределах второго уровня сетевой модели **OSI** MVRP обеспечивает динамический обмен информации о **VLAN** и конфигурацию необходимых **VLAN**. Например, поставлена задача добавить определённый порт коммутатора в **VLAN**, или сетевое устройство, поддерживающее VLAN и подключённое в порт коммутатора требует переконфигурации, и все необходимые транки динамически созданы на других коммутаторах, поддерживающих MVRP. Для выполнения этой задачи без возможностей MVRP потребуется ручная конфигурация VLAN или какой-либо проприетарный метод производителя. Если же выполнять эту задачу средствами MVRP, который использует динамические значения VLAN в фильтруемой базе данных. Если коротко — MVRP помогает динамически поддерживать конфигурации VLAN в статических конфигурациях сетей.

802.1Q даёт возможность:

- Динамически конфигурировать и распределять информацию о принадлежности VLAN через механизмы MVRP.
- Статически конфигурировать информацию о принадлежности VLAN посредством механизмов менеджмента, которые позволяют управлять регистрационными данными о статических записях регистраций VLAN.
- Поддерживать комбинированные статические и динамические конфигурации, при которых некоторые VLAN конфигурируются посредством механизмов менеджмента, а для других VLAN сохраняется возможность динамической конфигурации средствами MVRP.

Для доступа к настройкам необходимо перейти по вкладке Configuration→ MRP.

Настройка MRP (Рис. 3.115) (Табл. 3.112)

MVRP Global Configuration

Global State	Disabled
Managed VLANs	1-4094

MVRP Port Configuration

Port	Enabled
*	☐
1	☐
2	☐
3	☐

MRP Overall Port Configuration

Port	Join Timeout	Leave Timeout	LeaveAll Timeout	Periodic Transmission
*	20	60	1000	☐
1	20	60	1000	☐
2	20	60	1000	☐
3	20	60	1000	☐

Рис. 3.115 – Настройка MVRP

Таблица 3.112 – Настройка MVRP

Global State	Включение/выключение функции MVPR
Managed VLANs	Настройка списка VLAN, управляемых MVRP
Настройка портов	
Port	Номер порта
Enabled	Включение функции MVRP на порту
Join Timeout	таймер присоединения. Значения от 1-20сс. По умолчанию значение 20сс
Leave Timeout	таймер отключения. Значения от 60-300сс. По умолчанию значение 60сс
LeaveAll Timeout	таймер отключения от всех мультикастовых групп. Значения 1000-5000сс. По умолчанию – 1000сс
Periodic Transmission	Включение функции PeriodicTransmission для всех приложений MRP на порту

3.2.43 GVRP

Для доступа к настройкам необходимо перейти по вкладке Configuration→GVRP.

Global Configuration (Глобальные настройки) (Рис. 3.116) (Табл. 3.113).

GVRP Configuration

☐ Enable GVRP

Parameter	Value
Join-time:	20
Leave-time:	60
LeaveAll-time:	1000
Max VLANs:	20

Рис. 3.116 – Глобальные настройки

Таблица 3.113 – Глобальные настройки

Enable GVRP	Включение протокола GVRP глобально.
Join-time	Значение в диапазоне 1-20, указываемое в сентисекундах (сотых секунды). По умолчанию, значение равно 20.
Leave-time	Значение в диапазоне 60-300, указываемое в сентисекундах (сотых секунды). По умолчанию, значение равно 60.
Leave All-time	Значение в диапазоне 1000-5000, указываемое в сентисекундах (сотых секунды). По умолчанию, значение равно 1000.
Max VLANs	Максимальное значение VLAN, поддерживаемое GVRP.

Port Configuration (Настройки порта) (Рис. 3.117) (Табл. 3.114)

GVRP Port Configuration

Port	Mode
*	<>
1	Disabled
2	Disabled
3	Disabled

Рис. 3.116 – Настройки порта

Таблица 3.113 – Настройки порта

Port	Номер порта
Mode	Позволяет настроить режим работы GVRP на порту

3.2.44 sFlow

Для доступа к настройкам необходимо перейти по вкладке Configuration→sFlow

sFlow Configuration (Настройки sFlow) (Рис. 3.117) (Табл. 3.114).

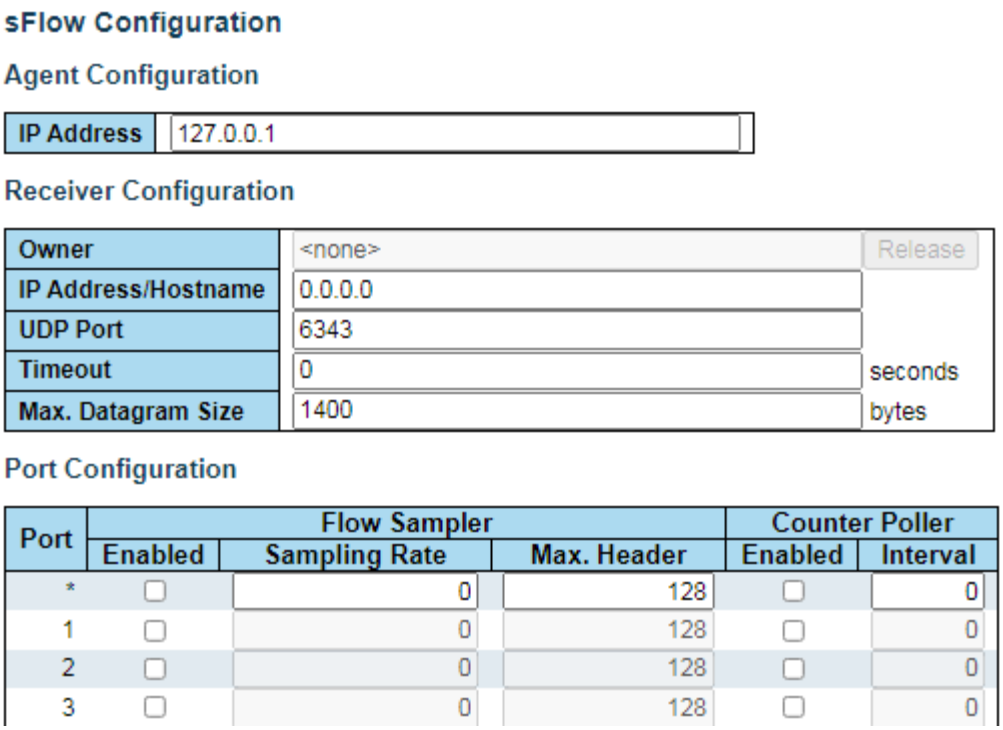


Рис. 3.117 – Настройки порта

Таблица 3.114 – Настройки порта

Agent Configuration (Настройки агента)	
IP Address	IP-адрес, используемый в качестве IP-адреса агента в sFlow. Он служит уникальным ключом, который будет идентифицировать агента в течение длительных периодов времени. Поддерживаются адреса IPv4 и IPv6.
Receiver Configuration (Конфигурация приемника)	
Owner	• None - не сконфигурирован / не востребован. • Configured through local management - сконфигурирован через Web или CLI; • Если sFlow в настоящий момент сконфигурирован через SNMP, содержит строку, идентифицирующую приемник sFlow.
IP Address/Hostname	IP-адрес или имя хоста приемника sFlow.
UDP Port	Просматриваемый порт UDP
Timeout	Таймаут
Max. Datagram Size	Максимальное количество байтов данных, которое может быть отправлено в одной тестовой датаграмме
Port Configuration (Настройки порта)	
Port	Номер порта
Flow Sampler Enabled	Включает или отключает выборку потока на порту.
Flow Sampler Sampling Rate	Статистическая частота дискретизации для выборки пакетов.
Flow Sampler Max. Header	Максимальное количество байтов, которое должно быть скопировано из пакета, выбранного для выборки, в дейтаграмму sFlow.
Counter Poller	Включает или отключает опрос счетчика на этом порту.

Enabled	
Counter Poller Interval	Интервал опроса. Допустимый диапазон: от 1 до 3600 секунд.

3.2.45 DDMI (интерфейс цифрового диагностического мониторинга)

Усовершенствованный цифровой интерфейс позволяет установить связь в реальном времени между коммутатором и трансивером SFP. Это позволяет коммутатору получать доступ к рабочим параметрам в оптоволоконном канале.

DDMI контролирует:

• температуру

• напряжение питания

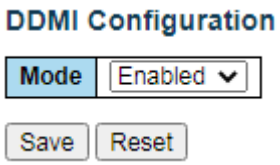
• передаваемый ток смещения.

• Передаваемая мощность

• Полученная мощность

Для доступа к настройкам необходимо перейти по вкладке Configuration→DDMI.

Настройка DDMI (Рис. 3.118) (Табл. 3.115)



•

Рис. 3.118 – Настройки порта

Таблица 3.115 – Настройки порта

Mode	Включение/выключение функции DDMI. Функция DDMI включена по умолчанию.

3.2.46 UDLD

Для доступа к настройкам необходимо перейти по вкладке Configuration→UDLD.

Протокол второго уровня, созданный для автоматического обнаружения потери двухсторонней коммуникации на линиях связи

Port Configuration (Настройки порта) (Рис. 3.119) (Табл. 3.116)

UDLD Port Configuration

Port	UDLD mode	Message Interval
*	<>	7
1	Disable	7
2	Disable	7
3	Disable	7

Рис. 3.119 – Настройки порта

Таблица 3.116 – Настройки порта

Port	Номер порта
UDLD mode	Включить/выключить UDLD на порту
Message Interval	Интервал сообщений