



# Зелакс ZES

Руководство по настройке  
ZES-22xx

© 1998 — 2021 Zelax. Все права защищены.

Редакция 02 от 01.09.2021 г.  
ПО 1.118

Россия, 124681 Москва, г. Зеленоград, ул. Заводская, дом 1Б, строение 2  
Телефон: +7 (495) 748-71-78 (многоканальный) • <http://www.zelax.ru>  
Отдел технической поддержки: [tech@zelax.ru](mailto:tech@zelax.ru) • Отдел продаж: [sales@zelax.ru](mailto:sales@zelax.ru)



# Оглавление

1	Управление коммутатором.....	5
1.1	Варианты управления.....	5
1.1.1	Внеполосное управление.....	5
1.1.2	Внутриполосное управление.....	6
1.2	Интерфейс командной строки (CLI).....	8
1.2.1	Режимы конфигурирования.....	8
1.2.2	«Горячие» клавиши.....	10
1.2.3	Контекстная справка.....	10
1.2.4	Проверка вводимых команд.....	11
1.2.5	Поддержка доопределения команд.....	11
2	Основная настройка коммутатора.....	12
2.1	Начало сессии (регистрация).....	12
2.1.1	Состояние порта.....	12
2.1.2	Обновление экрана.....	12
2.1.3	Система справки.....	12
2.1.4	Завершение сессии.....	13
2.2	Меню System.....	13
2.2.1	System Configuration (системные настройки).....	13
2.2.2	System Information (системная информация).....	14
2.2.3	System IP (Настройки IP).....	14
2.2.4	System IP Status (Состояние IP-интерфейсов и маршрутов).....	16
2.2.5	System NTP (Протокол системного времени).....	17
2.2.6	System Time (Системное время).....	18
2.2.7	Настройка вывода журнала системных сообщений.....	19
2.2.8	CLI Logger Configuration (Логирование вводимых команд).....	19
2.2.9	System Log Information (Журнал системных сообщений).....	21
2.2.10	System Detailed Log (Детальный журнал).....	21
2.2.11	System CPU Load (Загрузка CPU).....	22
2.2.12	System SMTP (Отправка системных сообщений по электронной почте).....	22
2.3	Меню Green Ethernet («Зеленый Ethernet»).....	24
2.3.1	Функции энергосбережения для светодиодных индикаторов.....	24
2.3.2	Настройка Green Ethernet.....	25
2.3.3	Состояние Green Ethernet.....	27
2.4	Ports (Порты).....	28
2.4.1	Ports Configuration (Настройка портов).....	28
2.4.2	Ports State (Состояние портов).....	29
2.4.3	Ports Traffic Overview (Обзор трафика портов).....	30
2.4.4	Ports QoS Statistics (Статистика QoS для портов).....	31
2.4.5	Ports QCL Status (Состояние QCL).....	31
2.4.6	Ports Detailed Statistics (Детальная статистика портов).....	32
2.4.7	Ports VeriPHY™ (Диагностика подключения кабелей к портам).....	34
2.4.8	Ports SFP (Состояние SFP портов).....	35
2.5	Security (Безопасность).....	36
2.5.1	Switch (Коммутатор).....	36
2.5.2	Access Management (Управление доступом).....	41
2.5.3	SNMP.....	43
2.5.4	RMON.....	50
2.6	Network (Сеть).....	55
2.6.1	Port Security (Безопасность порта).....	55
2.6.2	NAS.....	60
2.6.3	ACL (Списки доступа).....	65
2.6.4	DHCP.....	72
2.6.5	IP Source Guard (Защита IP-адреса источника).....	75
2.6.6	ARP inspection (Инспекция ARP).....	77
2.7	RADIUS.....	79
2.7.2	TACACS+.....	84
2.8	Aggregation (Агрегирование).....	85
2.8.1	Static (Статическое агрегирование).....	85
2.8.2	LACP.....	86
2.9	Redundancy (Резервирование).....	89

2.9.1	Технология Z-Ring .....	89
2.9.2	Loop Protection (Защита от петель) .....	93
2.9.3	Spanning Tree.....	94
2.9.4	MEP (Maintenance Entity Point) .....	104
2.9.5	ERPS.....	112
2.10	IPMC Profile (Профиль IPMC) .....	114
2.11	MVR.....	116
2.12	IPMC.....	119
2.12.1	IGMP Snooping.....	119
2.12.2	MLD Snooping .....	124
2.13	LLDP.....	129
2.14	PoE (только для коммутаторов с поддержкой PoE) .....	136
2.15	MAC Table (Таблица MAC-адресов).....	141
2.16	VLAN Translation (Трансляция VLAN) .....	143
2.17	VLANs .....	144
2.18	Private VLANs (Частные VLAN).....	149
2.19	GVRP .....	150
2.20	VCL.....	151
2.20.1	MAC-based (На основе MAC-адресов) .....	151
2.20.2	Protocol-based VLAN (VLAN на основе протокола) .....	152
2.21	QoS (Качество обслуживания) .....	154
2.21.2	Storm Control (Управление широковещательным штормом) .....	169
2.22	Mirroring (Зеркалирование) .....	169
2.23	UPnP .....	170
2.24	PTP (IEEE1588) .....	171
2.25	Diagnostics (Диагностика).....	174
2.26	Maintenance (Обслуживание) .....	175
2.26.2	Software (Программное обеспечение).....	176
2.26.3	Configuration (Настройка).....	177

# 1 Управление коммутатором

## 1.1 Варианты управления

Для управления необходимо настроить коммутатор. Коммутатор обеспечивает два варианта управления: внеполосное (out-of-band) или внутрисполосное (in-band).

Для доступа к устройству с настройками по-умолчанию используются:

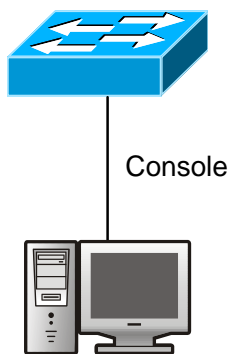
- Имя пользователя – admin;
- Пароль – admin.

### 1.1.1 Внеполосное управление

Внеполосное управление — это управление через консольный интерфейс. Внеполосное управление, в основном используется для начального конфигурирования коммутатора, либо когда внутрисполосное управление недоступно. Например, пользователь может через консольный порт присвоить коммутатору IP-адрес для доступа по Telnet.

Процедура управления коммутатором через консольный порт описана ниже:

Шаг 1: Подключить персональный компьютер к консольному порту коммутатора (Рис. 1):



**Рис. 1. Подключение ПК к консольному порту коммутатора**

Подключитесь к порту RS-232 коммутатора, используя консольный кабель, входящий в комплект поставки.

Персональный компьютер должен иметь порт RS-232 и иметь установленную терминальную программу, например, HyperTerminal, являющуюся стандартной программой операционных систем Windows 9x/NT/2000/XP.

Шаг 2: Загрузка программы HyperTerminal.

1. Загрузите программу HyperTerminal.
2. Установите соединения с параметрами:
  - скорость – 115200 бит/с;
  - данные – 8 бит;
  - четность – нет;
  - стоповые биты – 1;
  - управление потоком – нет.

Шаг 3: Вызов командного интерфейса (CLI) коммутатора.

Включите напряжение питания коммутатора. В окне HyperTerminal появится информация о вызове режима CLI-конфигурирования.

```
Boot> fi lo -d managed
Image loaded from 0x80040000-0x80ac4e4c
Boot> go

Press ENTER to get started

Username:
```

Теперь можно вводить команды управления коммутатором.

## 1.1.2 Внутриполосное управление

Внутриполосное управление сетью осуществляется путем доступа к коммутатору по Telnet, SSH или HTTP либо с помощью ПО управления по протоколу SNMP. В тех случаях, когда внутриполосное управление из-за изменений, сделанных в конфигурации коммутатора работает со сбоями, для управления и конфигурирования коммутатора можно использовать внеполосное управление.

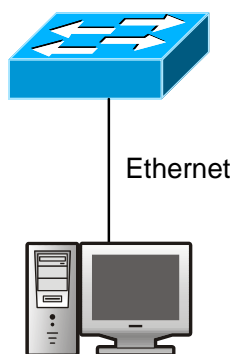


Рис. 2. Подключение ПК к коммутатору

### 1.1.2.1 Управление по Telnet и SSH

Для управления коммутатором по Telnet или SSH необходимо подключиться к коммутатору Рис. 2 и должны выполняться следующие условия:

1. Настроен IP-адрес коммутатора для управления;
2. IP-адреса хоста (клиента Telnet) и интерфейса VLAN коммутатора должны находиться в одном и том же сегменте IP-сети;
3. Если условие 2 не выполнено, клиент Telnet может быть подключен к IP-адресу коммутатора через другие устройства, например, через маршрутизатор.

### 1.1.2.2 Управление через Web-интерфейс

Для управления коммутатором через Web-интерфейс должны выполняться следующие условия:

1. Настроен IP-адрес коммутатора для управления;
2. IP-адреса хоста (клиента HTTP) и интерфейса VLAN коммутатора должны находиться в одном и том же сегменте сети;
3. Если условие 2 не выполнено, пользователя (клиента HTTP) можно подключить к IP-адресу коммутатора через другие устройства, например, через маршрутизатор.

Подобно управлению по Telnet, как только с хоста будет успешно проходить команда ping до IP-адреса коммутатора, введя правильное имя и пароль можно получить доступ к Web-интерфейсу коммутатора.

Зарегистрируйтесь в Web-интерфейсе конфигурирования. Для доступа к Web-интерфейсу коммутатора необходимо ввести имя пользователя и пароль, в противном случае в доступе будет отказано. Это сделано для защиты коммутатора от попыток несанкционированного доступа.

Окно для входа в Web-интерфейс коммутатора ZES показано на Рис. 3:

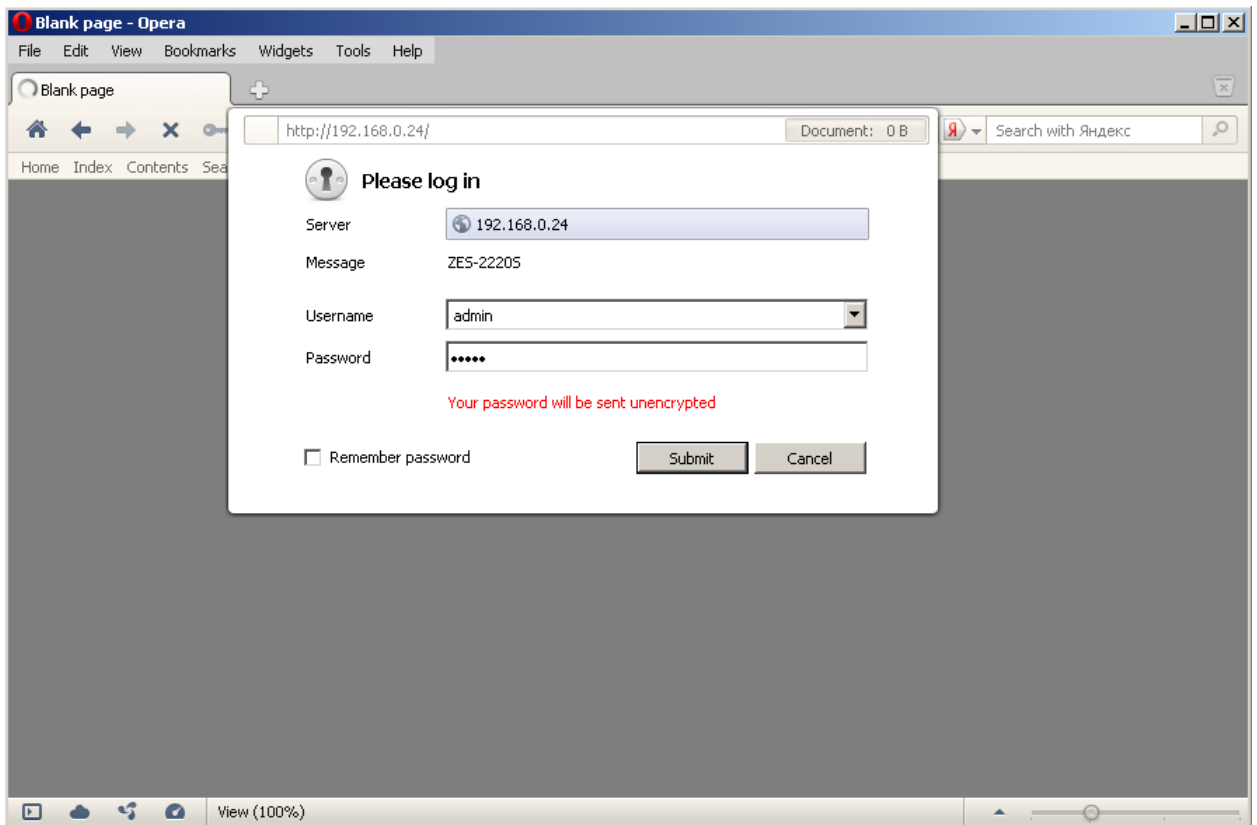


Рис. 3. Окно для входа в Web-интерфейс

Окно входа в Web-интерфейс. Введите имя и пароль, откроется окно Web-интерфейса для настройки коммутатора (см. Рис. 4).

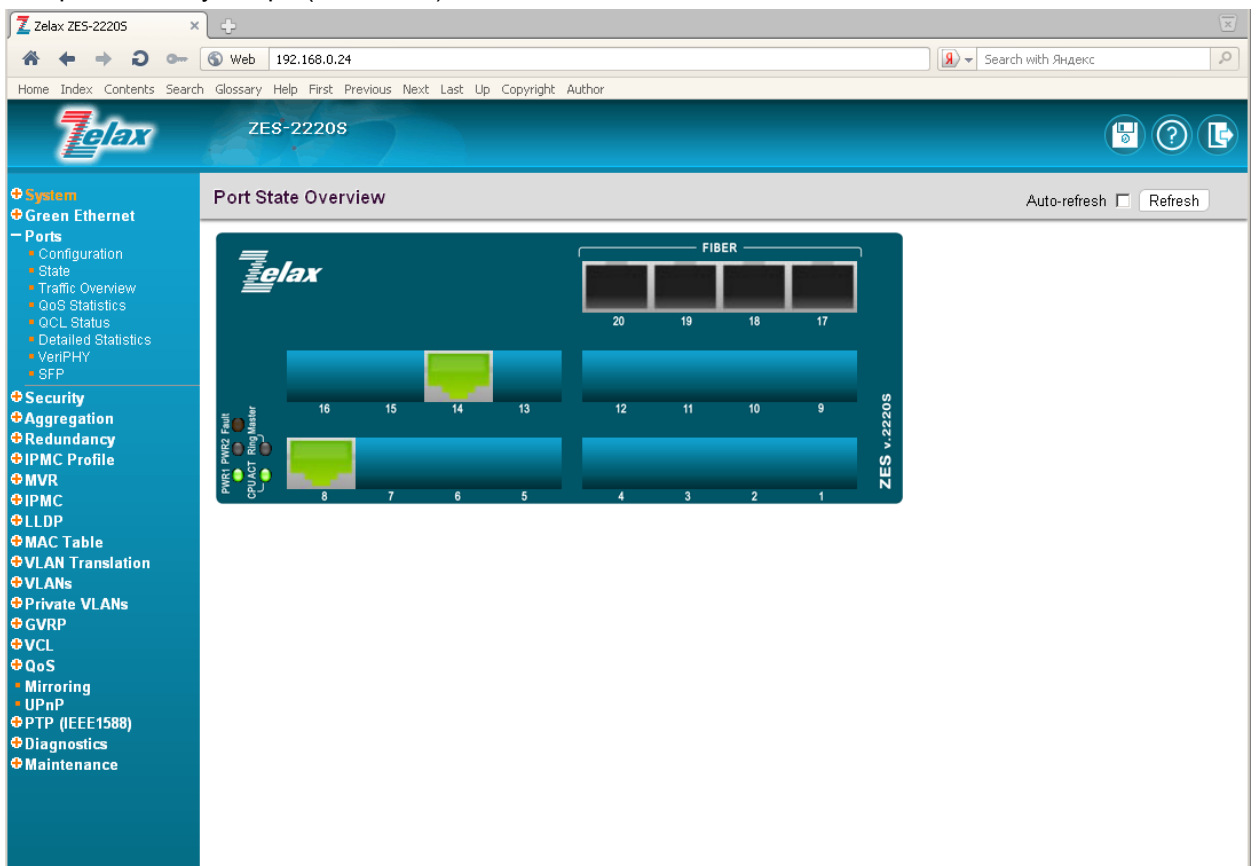


Рис. 4. Главное окно Web-интерфейса настройки коммутатора

### 1.1.2.3 Управление коммутатором по протоколу SNMP

Для управления коммутатором по протоколу SNMP должны выполняться следующие условия:

1. Настроен IP-адреса коммутатора;
2. IP-адреса хоста (с SNMP-менеджером) и интерфейса VLAN коммутатора должны находиться в одном и том же сегменте сети;
3. Если условие 2 не выполнено, клиент можно подключить к IP-адресу коммутатора через другие устройства, например, через маршрутизатор;
4. Должен быть включен протокол SNMP (настройка протокола описана в разделе 2.5.3).

## 1.2 Интерфейс командной строки (CLI)

Интерфейс CLI уже знаком большинству пользователей. Как отмечалось выше, внеполосное управление и управление коммутатором по Telnet и SSH выполняется посредством CLI.

Для управления коммутатором с помощью CLI имеется набор команд. Для управления и настройки коммутатора эти команды объединены в категории в соответствии с выполняемыми функциями. Каждой категории соответствует свой режим конфигурирования. Ниже рассмотрены команды для коммутатора:

- Режимы конфигурирования
- Синтаксис команд
- «Горячие» клавиши
- Контекстная справка
- Проверка вводимых команд
- Поддержка доопределения команд

### 1.2.1 Режимы конфигурирования

На Рис. 5 приведены режимы конфигурации коммутатора.

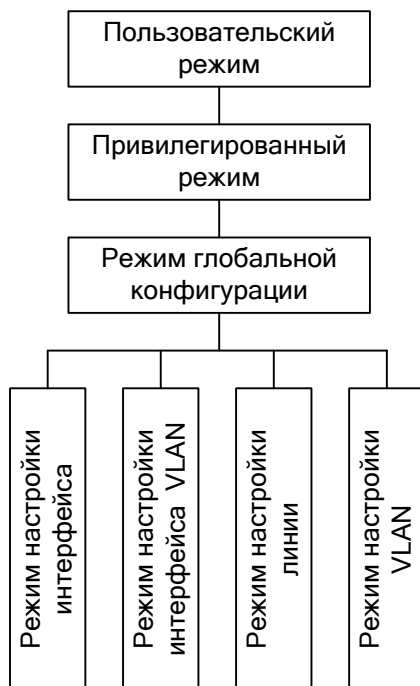


Рис. 5. Режимы конфигурирования коммутатора

#### 1.2.1.1 Пользовательский режим

При вызове интерфейса CLI сначала вызывается система регистрации пользователя. По умолчанию включен пользовательский режим. На экране появляется приглашение "Switch>", символ ">" указывает, что включен пользовательский режим. Если в привилегированном режиме ввести команду **exit** (выход), то выход произойдет также в пользовательский режим.

В пользовательском режиме конфигурирование коммутатора запрещено.



## 1.2.1.2 Привилегированный режим

Приглашение в привилегированном режиме имеет вид “Switch#”. В привилегированный режим можно войти из пользовательского режима, введя команду **enable**, а затем — имя и пароль администратора. Если в глобальном режиме конфигурирования (Global Mode) ввести команду **exit** (выход), то выход произойдет также в привилегированный режим. Для коммутатора также работает клавиатурная команда “Ctrl+z” — она выполняет выход из любого режима (кроме пользовательского) в привилегированный режим.

В привилегированном режиме пользователь может запрашивать информацию о конфигурировании коммутатора, статусе соединения и статистике трафика для всех портов; находясь в привилегированном режиме, пользователь может входить в глобальный режим конфигурирования и изменять всё конфигурирование коммутатора. По этой причине для входа в привилегированный режим должен быть установлен пароль, предотвращающий несанкционированный доступ.

## 1.2.1.3 Глобальный режим конфигурирования

При вводе в привилегированном режиме команды `config terminal` произойдет переключение в глобальный режим конфигурирования, появится приглашение “Switch(Config)#” при использовании команды **exit** в других режимах конфигурирования (интерфейсный режим, режим VLAN), произойдет возврат в глобальный режим конфигурирования.

В глобальном режиме конфигурирования пользователь может вводить настройки, например, задавать таблицу MAC-адресов, зеркалирование портов, создавать VLAN, включать GVRP, STP и т. п.

Затем пользователь может, например, включить режим настройки интерфейсов.

## 1.2.1.4 Режим настройки интерфейсов

Для входа в режим настройки интерфейсов в глобальном режиме конфигурирования введите команду `interface`. Коммутатор поддерживает три типа интерфейса:

1. Интерфейс VLAN;
2. Интерфейс FastEthernet;
3. Интерфейс GigabitEthernet.

Соответственно имеются три режима конфигурирования интерфейсов.

Тип интерфейса	Вводимая команда	Выполняемые операции	Выход
VLAN	В глобальном режиме конфигурирования введите команду <b>interface vlan</b> <vlan_list>	Настройка IP-адресов коммутатора и т. д.	Для возврата в глобальный режим конфигурирования введите команду <b>exit</b>
FastEthernet	В глобальном режиме конфигурирования введите команду <b>interface fastethernet</b> <port_type_list>	Настройка поддержки режима дуплекса, скорости Ethernet-порта и т. д.	Для возврата в глобальный режим конфигурирования введите команду <b>exit</b>
GigabitEthernet	В глобальном режиме конфигурирования введите команду <b>interface gigabitethernet</b> <port_type_list>	Настройка поддержки режима дуплекса, скорости Ethernet-порта и т. д.	Для возврата в глобальный режим конфигурирования введите команду <b>exit</b>

## 1.2.1.5 Режим настройки линии

Для входа в режим настройки линии в глобальном режиме конфигурирования введите команду `line`. В данном режиме могут быть настроены параметры подключения и по консоли и терминальным линиям.

## 1.2.1.6 Синтаксис команд

Коммутатор поддерживает различные команды конфигурирования. Хотя все команды разные, все они поддерживают синтаксис команд конфигурирования коммутатора. Общий формат команд коммутатора приведен ниже:

**cmdtxt** <variable> {enum1 | ... | enumN } [option1 | ... | optionN]

**cmdtxt** — строго заданная последовательность символов, определяющая дальнейшие параметры.

**<variable>** — обозначает переменный параметр;

**{enum1 | ... | enumN}** —обозначает штатный параметр, значения которого лежат в пределах **enum1** — **enumN**;

квадратные скобки ([ ]) в **[option]** обозначают опцию — дополнительный параметр. В командной строке могут присутствовать и комбинации этих обозначений, например “<>”, “{ }” и “[ ]”. Пример комбинации [**<variable>**], **{enum1 <variable>| enum2}**, **[option1 [option2]]**, и т. п.

Ниже приведены примеры некоторых актуальных команд конфигурирования:

**show version**, параметры не требуются. Эта команда состоит из одного ключевого слова и не имеет параметров. Для ее выполнения просто введите ее.

**vlan <vlan-id>**, после ключевого слова должны быть заданы значения параметра.

**hostname <string>**, позволяет задать имя коммутатора.

**snmp-server community {v2c | v3} <string> {ro | rw}**, возможны следующие варианты команды:

snmp-server community v2c <string>ro или snmp-server community v3 <string> rw

## 1.2.2 «Горячие» клавиши

Для обслуживания операций конфигурирования, выполняемых пользователем, коммутатор поддерживает несколько «горячих» клавиш (например, команды назначены на клавиши перемещения курсора (вверх, вниз, влево, вправо) и пробел. Если терминал не распознает клавиши Up (вверх) и Down (вниз), вместо них можно использовать сочетания клавиш ctrl+p и ctrl+n.

Клавиши	Функция	
Пробел	К перемещается назад на одну позицию	
Up “↑”	Отображает предыдущую введенную команду. Может быть показано до 10 последних введенных команд	
Down “↓”	Отображает следующую введенную команду. Если клавиша Up уже использовалась для отображения ранее введенных команд, можно использовать клавишу Down для просмотра следующей команды	
Left “←”	Курсор перемещается на один символ влево	Клавиши Left и Right можно использовать для редактирования команды на экране
Right “→”	Курсор перемещается на один символ вправо	
Ctrl+p	Выполняет те же функции, что и клавиша Up “↑”	
Ctrl+n	Выполняет те же функции, что и клавиша Down “↓”	
Ctrl+b	Выполняет те же функции, что и клавиша Left “←”	
Ctrl+f	Выполняет те же функции, что и клавиша Right “→”	
Ctrl+z	Выход в привилегированный режим из других режимов конфигурирования (за исключением пользовательского)	
Ctrl+c	Прерывание процесса выполнения команды, например, прерывание ping или другой команды	
Ctrl+a	Перевод курсора в начало строки	
Клавиша табуляции (Tab)	Если введена строка команды или ее ключевого слова, клавишу Tab можно использовать для дополнения этой команды или ее ключевого слова до полной формы (если это не приводит к конфликту имен)	

## 1.2.3 Контекстная справка

Пользователь может получить доступ к справочной информации по командам коммутатора двумя способами: введя команду “help” или нажав клавишу “?”.

Доступ к справке	Использование и способ ввода
Команда Help	В любом месте командной строки введите “help” и нажмите Enter. Коммутатор выведет краткое описание команды
“?”	1. В любом месте командной строки введите “?”. Будет выведен список команд текущего режима и краткое их описание. 2. Введите “?” после ключевого слова команды (через пробел). Если в этой позиции должен быть параметр, будет выведено описание типа параметра, области его применения и т. п. Если в этой позиции должно быть ключевое слово,



## 2 Основная настройка коммутатора

Для настройки коммутатора может быть использован любой из вышеперечисленных способов. В данном руководстве приводится описание настройки через web-интерфейс с указанием команд CLI для настройки описываемого функционала.

Управление по web-интерфейсу является интуитивно-понятным и простым в использовании; благодаря графическому интерфейсу, пользователи могут легко и быстро настроить устройство. Управление на основе web-интерфейса поддерживает различные web-браузеры, в том числе Internet Explorer (рекомендуется версия 9.0 или более поздняя), Firefox и Google Chrome. Для доступа к web-интерфейсу управления в начальный период использования устройства или после возврата к заводским настройкам, введите IP-адрес устройства используемый по умолчанию, в адресной строке браузера. Ниже это описано более подробно.

### 2.1 Начало сессии (регистрация)

Чтобы войти в web-интерфейс управления устройством в первый раз, либо после возврата к заводским настройкам, введите IP-адрес 192.168.0.24 используемый по умолчанию, в адресную строку web-браузера. После этого появится стандартное приглашение, зависящее от типа используемого браузера. В примере ниже приведен вид окна браузера Firefox.

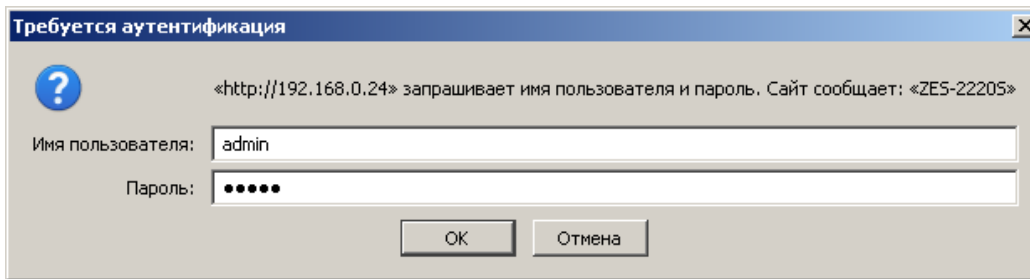


Рис. 6. Окно регистрации через web-интерфейс

Введите имя пользователя, заданное на заводе-изготовителе, по умолчанию "admin" и пароль "admin". После успешного завершения регистрации, откроется страница Port State (Состояние портов).

#### 2.1.1 Состояние порта

На главной странице, отображаемой сразу после завершения регистрации, показано состояние портов (электрических и оптических). Зеленый цвет порта указывает, что соединение порта LAN работает на скорости 100Мбит/с. Оранжевый цвет порта означает соединение на скорости 1000Мбит/с.

На страницу с отображением состояния портов можно попасть с помощью меню в левой части окна **Ports>State (Порты>Состояние)**.

#### 2.1.2 Обновление экрана

Чтобы обновить экран щелкните кнопку "Refresh" (Обновить экран). Чтобы экран обновлялся автоматически, установите флаг в поле "Auto-refresh" (Обновлять автоматически). Экран будет автоматически обновляться через каждые 3 секунды.

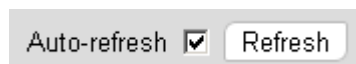


Рис. 7. Область параметров обновления экрана

Тем не менее, при прямом подключении к локальному порту LAN, рекомендуется не использовать функцию автоматического обновления, так как она увеличивает трафик.

#### 2.1.3 Система справки

Устройство оснащено системой справки, работающей в режиме «онлайн» и позволяющей инженеру настроить устройство. Каждая страница настройки функций дополняется специальной

страницей справки, посвященной данной функции. Пользователь может в любой момент открыть всплывающее окно справки на экране, нажав на кнопку "help" (Справка).



Рис. 8. Кнопка строенной справки

## 2.1.4 Завершение сессии

По окончании настройки, рекомендуется завершить работу в web-интерфейсе. Для этого нажмите на кнопку завершения сессии.



Рис. 9. Кнопка завершения сессии

После нажатия на кнопке завершения сессии, откроется окно с запросом подтверждения операции. Нажмите "OK", чтобы завершить сессию либо "Cancel" (Отмена), чтобы вернуться в web-интерфейс устройства.

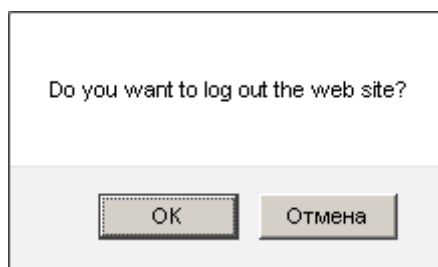


Рис. 10. Окно завершения сессии

В последующих подразделах этой главы описаны разделы системы меню в том порядке, в котором они перечислены в окне меню (сверху вниз), начиная с меню "System".

## 2.2 Меню System

Параметры, находящиеся в меню "System" определяют системные настройки, такие как IP-адрес, сервер времени и т.п.

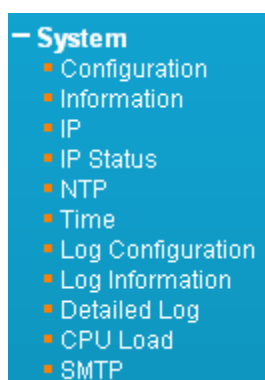


Рис. 11. Вид меню System

### 2.2.1 System Configuration (системные настройки)

Настройки, введенные в этом разделе меню, определяют содержимое полей 'sysContact' (OID 1.3.6.1.2.1.1.4), 'sysName' (OID 1.3.6.1.2.1.1.5) и 'sysLocation' (OID 1.3.6.1.2.1.1.6) в MIB2 стандартного протокола SNMP. После ввода настроек не забудьте нажать кнопку "Save" (Сохранить).

System Information Configuration	
System Contact	tech@zelax.ru
System Name	ZES-2220S
System Location	Russia, 124681, Moscow, Zelenograd
<input type="button" value="Save"/> <input type="button" value="Reset"/>	

Рис. 12. Вид пункта меню System - Configuration (системные настройки)

Поле **System Contact** (Контактная информация): В этом поле можно указать контактную информацию. Это может быть имя и фамилия лица, ответственного за систему, адрес электронной почты (email) или другие сведения. Допустимая длина строки 0~255 символов ASCII с номерами в диапазоне 32~126.

Поле **System Name** (Имя системы): Имя хоста для данного устройства. Можно использовать буквы алфавита (A-Z; a-z), цифры (0-9) и знак минус (-). Однако, применение символов «пробел» недопустимо. Первый символ должен быть буквой (прописной или строчной). Первый и последний символы не должны быть знаком минус. Допустимая длина строки 0~255.

Поле **System Location** (Местонахождение системы): В этом поле можно задать местонахождение для данного устройства. Допустимая длина строки 0~255.

Пример использования через CLI:

```
snmp-server contact tech@zelax.ru
hostname ZES-2220S
snmp-server location Russia, 124681, Moscow, Zelenograd, Zavodskaya st., 1B, bldg 2
```

## 2.2.2 System Information (системная информация)

На странице информации о системе отображается информация о настройках, аппаратная версия, MAC-адрес, системное время, время работы устройства с момента старта, версия ПО и дата компиляции.

System Information	
System	
Contact	tech@zelax.ru
Name	ZES-2220S
Location	Russia, 124681, Moscow, Zelenograd, Zavodskaya st., 1B, bldg 2
Hardware	
MAC Address	00-1a-81-00-c0-a9
Hardware Version	1.1
Time	
System Date	2013-01-02T03:29:42+00:00
System Uptime	1d 03:29:54
Software	
Software Version	"1.100"
Software Date	2015-01-20T10:28:26+08:00

Рис. 13. Вид пункта меню System - Information (системная информация)

## 2.2.3 System IP (Настройки IP)

В полях этой страницы можно задать настройки IP-адресов для интерфейса и маршрутов.

**IP Configuration**

**Mode** Host  
**DNS Server** No DNS server  
**DNS Proxy**

**IP Interfaces**

Delete	VLAN	IPv4 DHCP			IPv4		IPv6	
		Enable	Fallback	Current Lease	Address	Mask Length	Address	Mask Length
<input type="checkbox"/>	1	<input type="checkbox"/>	<input type="checkbox"/>		192.168.0.24	24		

Add Interface

**IP Routes**

Delete	Network	Mask Length	Gateway	Next Hop VLAN
<input type="checkbox"/>	0.0.0.0	0	192.168.0.254	0

Add Route

Save Reset

Рис. 14. Вид пункта меню System - IP (Настройки IP)

### Раздел меню IP Configuration (Настройки IP).

**Mode** (Режим работы): 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 Host выбран по умолчанию.

**DNS Server** (DNS-сервер): Данная настройка позволяет задать сервер доменных имен (DNS) для разрешения имен, которое выполняет коммутатор. Поддерживаются следующие режимы работы:

- From any DHCP interfaces (Из любых интерфейсов DHCP): Будет использован IP-адрес первого DNS-сервера, полученный от DHCP, при включенной поддержке 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 прокси-сервер DNS, система будет отправлять запросы DNS на текущий настроенный DNS-сервер, при этом ответы будут отправляться, как DNS-разрешения клиентским устройствам сети.

### Область IP Interface (IP –интерфейс)

Чтобы ввести новый интерфейс, нажмите кнопку "Add Interface" (Добавить интерфейс). Поддерживается не более 8 интерфейсов.

**VLAN** (Номер 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.

**DHCP**: Когда в этом поле установлен флаг, система будет получать IPv4-адрес и маску интерфейса с использованием протокола DHCP. DHCP-клиент будет анонсировать заданное имя системы как имя хоста для поиска DNS.

**IPv4 Address** (IPv4-адрес): IPv4-адрес должен быть введен в десятичном формате с точкой. Если активен протокол DHCP, это поле не используется. Если работа с IPv4 на интерфейсе нежелательна, это поле можно также оставить пустым.

**IPv4 Mask** (Маска IPv4): Маска IPv4 для сети вводится в виде некоторого числа битов (длина префикса). Для IPv4-адресов правильны значения длиной от 0 до 30 битов. Если активен протокол DHCP, это поле не используется. Если работа с IPv4 на интерфейсе нежелательна, это поле можно оставить пустым.

**IPv4 Current Lease** (Аренда текущего IPv4-адреса): Для DHCP с активированной арендой IP-адресов, в данном столбце может быть указан текущий адрес интерфейса, предоставленный DHCP –сервером.

**IPv6 Address** (IPv6-адрес): IPv6-адрес представляет собой 128-битную запись, состоящую из восьми полей, разделенных двоеточиями (:). В каждом поле может содержаться не более четырех шестнадцатиричных цифр. Например, fe80::215:c5ff:fe03:4dc7. Символ :: является специальным синтаксическим выражением, которое может использоваться для сокращенной записи множества 16-битных групп, содержащих одни нули. Выражение может применяться только один раз. Оно также может соответствовать формально правильному IPv4-адресу. Например, ::192.1.2.34. Если работа с IPv6 на интерфейсе нежелательна, это поле можно также оставить пустым.

**IPv6 Mask** (Маска IPv6): Маска IPv6 для сети вводится в виде некоторого числа битов (длина префикса). Для IPv6-адресов правильны значения длиной от 1 до 128 битов. Если работа с IPv6 на интерфейсе нежелательна, это поле можно оставить пустым.

### Область IP Routes (IP-адреса маршрутов)

**Network** (адрес сети назначения): IP-адрес сети назначения – это IP-адрес сети назначения или IP-адрес хоста этого маршрута. Правильными форматами при вводе являются формат с десятичной точкой или правильная нотация адресов IPv6. Маршрут, выбираемый по умолчанию может иметь адрес 0.0.0.0 либо при IPv6 можно использовать нотацию ::

**Mask Length** (Маска сети назначения): Маска сети назначения – это маска IP-адреса сети назначения или маска хоста, заданная некоторым числом битов (длина префикса). Маска маршрута определяет, сколько битов должно совпасть, чтобы данный маршрут можно было квалифицировать. Для IPv4-масок маршрутов правильны значения от 0 до 32 битов; для IPv6-масок маршрутов правильны значения от 0 до 128 битов. Только маршрут, выбираемый по умолчанию, имеет маску длины 0 (так как он будет совпадать с любым маршрутом).

**Gateway** (Шлюз): В этом поле можно ввести IP-адрес шлюза. Правильными форматами при вводе является указание IP-адреса в десятичном формате или правильная нотация адресов IPv6. Адреса шлюза и сети должны быть одного и того же типа.

Пример использования через CLI:

```
vlan 1
!
interface vlan 1
 ip address 192.168.0.24 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.0.254
```

## 2.2.4 System IP Status (Состояние IP-интерфейсов и маршрутов)

На этой странице отображается состояние IP-интерфейсов и маршрутов.



IP Interfaces			
Interface	Type	Address	Status
OS:lo	LINK	00-00-00-00-00-00	<UP LOOPBACK RUNNING MULTICAST>
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	fe80::1/64	
OS:lo	IPv6	::1/128	
VLAN1	LINK	00-1a-81-00-c0-a9	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.0.24/24	
VLAN1	IPv6	fe80::21a:81ff:fe00:c0a9/64	

IP Routes		
Network	Gateway	Status
0.0.0.0/0	192.168.0.254	<UP GATEWAY HW_RT>
127.0.0.1/32	127.0.0.1	<UP HOST>
192.168.0.0/24	VLAN1	<UP HW_RT>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

Neighbour cache	
IP Address	Link Address
192.168.0.105	VLAN1:00-1b-21-21-9f-fb
fe80::21a:81ff:fe00:c0a9	VLAN1:00-1a-81-00-c0-a9

Рис. 15. Вид пункта меню System - IP Status (Состояние IP-интерфейсов и маршрутов)

Для настройки интерфейсов и маршрутов используйте страницу "System IP". Данную страницу можно использовать только для информационных целей.

### 2.2.5 System NTP (Протокол системного времени)

Настройка протокола NTP выполняется, чтобы синхронизировать часы устройства с временем сети.

NTP Configuration	
Mode	Enabled
Server 1	192.168.0.105
Server 2	
Server 3	
Server 4	
Server 5	

Save Reset

Рис. 16. Вид пункта меню System - NTP (Протокол системного времени)

**Mode** (Режим работы): Позволяет настроить режим работы NTP. Возможны следующие режимы:

- Enabled (Активирован): включить NTP-клиент.
- Disabled (Деактивирован): выключить NTP-клиент.

**Server #**: Введите в это поле IPv4- или IPv6-адрес NTP-сервера.

NTP-сервера будут упорядочены по возрастанию номеров. Если 'Server 1' недоступен, NTP-клиент попытается установить контакт с 'Server 2'.

Пример использования через CLI:

```
ntp  
ntp server 1 ip-address 192.168.0.105
```

## 2.2.6 System Time (Системное время)

Установка времени устройства.

The screenshot displays the 'System Time' configuration page. It is divided into two main sections: 'Time Zone Configuration' and 'Daylight Saving Time Configuration'.  
**Time Zone Configuration:** A table with two rows. The first row is 'Time Zone' with a dropdown menu showing '(GMT+03:00) Moscow, St. Petersburg, Volgograd'. The second row is 'Acronym' with a text input field containing 'MSK' and a note '( 0 - 16 characters )'.  
**Daylight Saving Time Configuration:** A table with one row: 'Daylight Saving Time' with a dropdown menu set to 'Disabled'.  
Below these are three sub-sections for 'Start Time settings', 'End Time settings', and 'Offset settings'. Each has five rows for 'Month', 'Date', 'Year', 'Hours', and 'Minutes', all with dropdown menus. The 'Offset settings' section has one row: 'Offset' with a text input field containing '1' and a note '( 1 - 1440) Minutes'.  
At the bottom left are two buttons: 'Save' and 'Reset'.

Рис. 17. Вид пункта меню System - Time (Системное время)

### Time Zone Configuration (Настройка часового пояса)

**Time Zone (Часовой пояс):** В раскрывающемся списке приведены часовые пояса для всего мира. Выберите соответствующий часовой пояс из списка и нажмите кнопку Save (Сохранить), чтобы сохранить его.

**Acronym (Сокращенное наименование):** Позволяет задать сокращенное наименование часового пояса.

### Daylight Saving Time Configuration (Настройка перехода на летнее/зимнее время)

**Daylight Saving Time (Переход на летнее/зимнее время):** Используется для перевода часов вперед или назад в соответствии с настройками, заданными ниже для определенной продолжительности времени дня. Чтобы отменить переход на летнее/зимнее время выберите "Disable" (выключить). Если требуется, чтобы сделанные настройки повторялись каждый год, выберите из списка "Recurring" (Повторять каждый год). Если настройки следует выполнить только один раз, выберите "NonRecurring" (Не повторять). По умолчанию выбрано "Disable" (выключить).

Настройки, повторяемые каждый год, либо выполняемые только один раз:

**Start time settings** (Настройки времени начала): Выберите неделю, день, месяц, год, час и минуту, в которую произойдет переход с зимнего на летнее время.

**End time settings** (Настройки времени окончания): Выберите неделю, день, месяц, год, час и минуту, в которую произойдет переход с летнего на зимнее время.

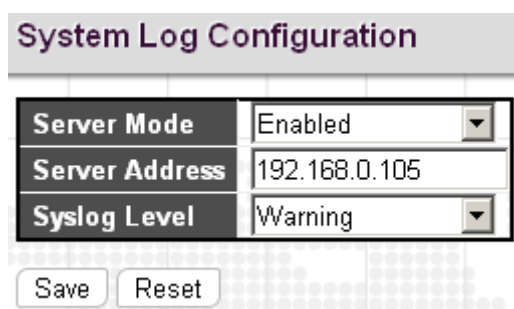
**Offset settings** (Настройки сдвига времени): Введите число минут, которое добавляется при переходе с летнего времени на зимнее время. Диапазон допустимых значений: от 1 до 1440.

Пример использования через CLI:

```
clock timezone MSK 3
```

## 2.2.7 Настройка вывода журнала системных сообщений

На этой странице можно настроить вывод журнала системных сообщений.



System Log Configuration	
Server Mode	Enabled
Server Address	192.168.0.105
Syslog Level	Warning

Save Reset

Рис. 18. Вид пункта меню System - Log Configuration

**Server Mode** (Режим работы сервера): Опции в этом списке определяют режим работы сервера. Когда включен этот режим работы, сообщения будут отправляться на Syslog-сервер (по IP-адресу сервера). Протокол системных сообщений основан на связи по протоколу UDP и принимается портом UDP с номером 514. Когда работа в этом режиме деактивирована, пакеты системных сообщений не посылаются.

**Server Address** (Адрес сервера): В этом поле можно задать IPv4-адрес syslog-сервера. Если коммутатор обеспечивает функцию DNS-сервера, то можно также указать его имя в качестве имени хоста.

**Syslog Level** (Уровень системных сообщений): Определяет, какие сообщения будут посылаться на сервер системных сообщений. Возможны следующие уровни:

- Info (Информация): Будут посылаться информационные сообщения, предупреждения и сообщения об ошибках.
- Warning (Предупреждение): Будут посылаться предупреждения и сообщения об ошибках.
- Error (Ошибка): Будут посылаться только сообщения об ошибках.

Пример использования через CLI:

```
logging on
logging host 192.168.0.105
logging level warning
```

## 2.2.8 CLI Logger Configuration (Логирование вводимых команд)

В данном раздел можно настроить логирование вводимых команд.

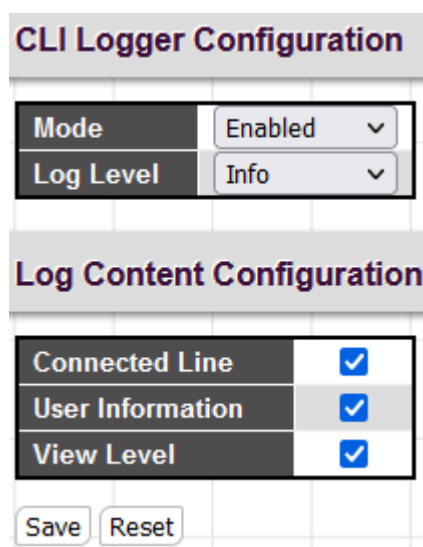


Рис. 19. Вид пункта меню System – CLI Logger

**Mode** (Режим работы): Включение/отключение логирования вводимых команд. В случае включения данной функции, выполнение команд будет записываться в журнал системных сообщений, а при настройке System Log Configuration, сообщения будут отправляться на Syslog-сервер.

Возможны следующие режимы работы:

- **Enabled** (Включен): Ведётся логирование вводимых команд.
- **Disabled** (Выключен): Не ведётся логирование вводимых команд. По умолчанию, режим работы - выключен.

**Log Level** (Уровень отправляемых сообщений): В открывающемся окне можно выбрать с каким уровнем сообщения произойдёт запись в журнал логирования.

Возможен выбор одного из следующего уровня отправляемых сообщений:

- **Info** (информация): Выполнение команд будет записываться в журнал системных сообщений с уровнем Info. По умолчанию, уровень отправляемых сообщений - Info.
- **Warning** (предупреждение): Выполнение команд будет записываться в журнал системных сообщений с уровнем Warning.
- **Error** (ошибка): Выполнение команд будет записываться в журнал системных сообщений с уровнем Error.

**Log Content Configuration** (информация сообщения): Настройка отображения дополнительной информации о выполненной команде. После ввода команды, в журнал системных сообщений заносится запись. В поле Message, после ключа "CMD=", отображается какая именно команда была применена. Для вывода дополнительных сведений о выполненной команде, необходимо активировать функции Log Content Configuration.

Возможна активация вывода следующих параметров:

- **Connected Line** (подключённая линия): В сообщении отображается информация о типе подключения пользователя, который выполнил команду с использованием telnet, ssh или с помощью консоли. Информация выводится после ключа "LINE=".
- **User Information** (информация о пользователе): В сообщении отображается информация о пользователе, который применил команду. Информация выводится после ключа "USER=".
- **View Level** (уровень просмотра): В сообщении отображается информация, в каком режиме была выполнена команда: в режиме глобальной конфигурации или конфигурирования интерфейса. Информация выводится после ключа "VIEW=".

По умолчанию данные функции не активированы.

Пример использования через CLI:

```
cli logger
cli logger level info
cli logger content all
```

## 2.2.9 System Log Information (Журнал системных сообщений)

Отображается информация, собранная в системном журнале.

ID	Level	Time	Message
1	Info	2013-01-01T02:59:59+03:00	Switch just made a cool boot.
2	Info	2013-01-01T03:00:01+03:00	Link up on port 3

Рис. 20. Вид пункта меню System - Log Information

**Level (Уровень):** В этом раскрывающемся списке можно выбрать: All (отображение всех сообщений), либо только сообщений с информацией определенного типа, а также предупреждений или сообщений об ошибках.

**Clear Level (Очистка уровня):** Используйте этот пункт для очистки сообщений выбранного типа в журнале.

**Browsing buttons (Кнопки перехода):** Эти кнопки можно использовать для быстрого перехода в начало или конец журнала, либо по страницам журнала.

Пример использования через CLI:

```
ZES-2220S# show logging
Switch logging host mode is enabled
Switch logging host address is 192.168.0.105
Switch logging level is warning

Number of entries on Switch 1:
Info : 28
Warning: 0
Error : 0
All : 28

ID      Level   Time                               Message
----
1      Info    2013-01-01T02:59:59+03:00         Switch just made a cool boot.
2      Info    2013-01-01T03:00:01+03:00         Link up on port 3
```

## 2.2.10 System Detailed Log (Детальный журнал)

Отображаются отдельные записи журнала.

Level	Info
Time	2013-01-01T02:59:59+03:00
Message	Switch just made a cool boot.

Рис. 21. Вид пункта меню System - Detailed Log (Детальный журнал)

Каждое сообщение можно просмотреть, введя его номер.

### 2.2.11 System CPU Load (Загрузка CPU)

На этой странице отображается загрузка центрального процессора (CPU) в виде графика SVG.



Рис. 22. Вид пункта меню System - CPU Load (Загрузка CPU)

Загрузка процессора измеряется как средняя на последнем интервале 100 мс, 1 секунда или 10 секунд. На график выводятся последние 120 выборок, отображаются как последние числа, так и текст. Чтобы график SVG отображался, используемый браузер должен поддерживать формат SVG. Экран автоматически обновляется через каждые 3 секунды.

### 2.2.12 System SMTP (Отправка системных сообщений по электронной почте)

Настройка оповещений о работе системы по электронной почте.

SMTP Configuration	
SMTP Mode	Enabled
SMTP Server	192.168.0.1
SMTP Port	25
Server requires authentication	<input type="checkbox"/>
Username:	
Password:	
Recipient mail address 1	test@zelay.ru
Recipient mail address 2	
Recipient mail address 3	
Recipient mail address 4	

SMTP Mail Event	
System	<input type="checkbox"/> + <input checked="" type="checkbox"/> Warm Start <input checked="" type="checkbox"/> Cold Start
Power	<input type="checkbox"/> + <input checked="" type="checkbox"/> Power1 Status <input checked="" type="checkbox"/> Power2 Status
Interface	<input type="checkbox"/> + <input checked="" type="checkbox"/> Port Link Up <input checked="" type="checkbox"/> Port Link Down

Save    Reset

Рис. 23. Вид пункта меню System - SMTP

### SMTP Configuration (Настройка SMTP)

**SMTP Mode** (Режим работы SMTP): Установка режима работы SMTP. Возможны следующие режимы:

- Enabled (Включен): SMTP-клиент включен.
- Disabled (Выключен): SMTP-клиент выключен.

**SMTP Server** (SMTP-сервер): Установка IP-адреса SMTP-сервера (этот сервер будет передавать сообщение email).

**SMTP Port** (Порт SMTP): Установка номера порта SMTP. По умолчанию для порта SMTP задано 25.

**Server requires authentication** (Сервер требует аутентификации): Установите в этом поле флаг, если сервер требует аутентификации. В большинстве случаев это требуется и необходимо заполнить поля, перечисленные ниже:

- Username (Имя пользователя): Введите правильное имя пользователя для аутентификации на SMTP-сервере.
- Password (Пароль): Введите пароль для аутентификации пользователя с именем username на SMTP-сервере.

**Recipient mail address** (Адрес получателя почты): Можно задать адреса не более чем четырех получателей, которым будут посылаться оповещения по электронной почте.

### SMTP Mail Event (События SMTP-почты)

Флаги, установленные в полях этой области, определяют, какие сообщения email будут генерироваться и посылаться.

**System** (Система): Включает/выключает оповещения о системных событиях. Возможны следующие события:

- Warm Start (Теплый пуск): Включает/выключает оповещения о событии "warm restart".

- Cold Start (Холодный пуск): Включает/выключает оповещения о событии "cold restart".

**Power** (Электропитание): Включает/выключает оповещения о событиях группы «Электропитание». Возможны следующие события:

- Power 1 Status (Состояние блока питания 1): Включает/выключает оповещения о состоянии блока питания 1.
- Power 2 Status (Состояние блока питания 2): Включает/выключает оповещения о состоянии блока питания 2.

**Interface** (Интерфейс): Включает/выключает оповещения о событиях на интерфейсах. Возможны следующие события:

- Port Link Up (Связь на порту установлена): Включает/выключает оповещения об установлении связи на порту.
- Port Link Down (Связь на порту потеряна): Включает/выключает оповещения о потере связи на порту.

Пример использования через CLI:

```
smtp
smtp server ip-address 192.168.0.1
smtp recipient 1 ip-address test@zelax.ru
smtp event system warmstart coldstart
smtp event system warmstart coldstart power power1 power2
smtp event system warmstart coldstart power power1 power2 interface linkup linkdown
```

## 2.3 Меню Green Ethernet («Зеленый Ethernet»)

В меню "Green Ethernet" («Зеленый Ethernet») включено несколько разделов для способов энергосбережения.



Рис. 24. Вид меню Green Ethernet («Зеленый Ethernet»)

### 2.3.1 Функции энергосбережения для светодиодных индикаторов

В полях, показанных ниже можно настроить интенсивность свечения светодиодных индикаторов, чтобы уменьшить энергопотребление.



### LED Power Reduction Configuration

#### LED Intensity Timers

Delete	Start Time	End Time	Intensity	
<input type="checkbox"/>	09:00 ▾	18:00 ▾	50 ▾	%
<input type="checkbox"/>	18:00 ▾	09:00 ▾	10 ▾	%

#### Maintenance

On time at link change	On at errors
<input style="width: 40px;" type="text" value="10"/> Sec.	<input checked="" type="checkbox"/>

**Рис. 25. Вид меню Green Ethernet - LED**

Интенсивность свечения светодиодных индикаторов можно задать в процентах от интенсивности – для каждого запрограммированного периода времени отдельно. В настройках, приведенных в примере выше, интенсивность свечения светодиодных индикаторов была задана 50% от полной интенсивности - в дневное время, и всего только 10% от полной интенсивности – в ночное время.

В поле с флагом maintenance (обслуживание), интенсивность свечения светодиодных индикаторов будет установлена 100% через 10 секунд после возникновения любой ошибки (например, события “link down”).

Пример использования через CLI:

```
green-ethernet led on-event error
green-ethernet led interval 9-18 intensity 50
green-ethernet led interval 18-9 intensity 10
```

### 2.3.2 Настройка Green Ethernet

На этой странице можно настроить функцию повышения энергетической эффективности Ethernet (EEE) и функции энергосбережения Ethernet.

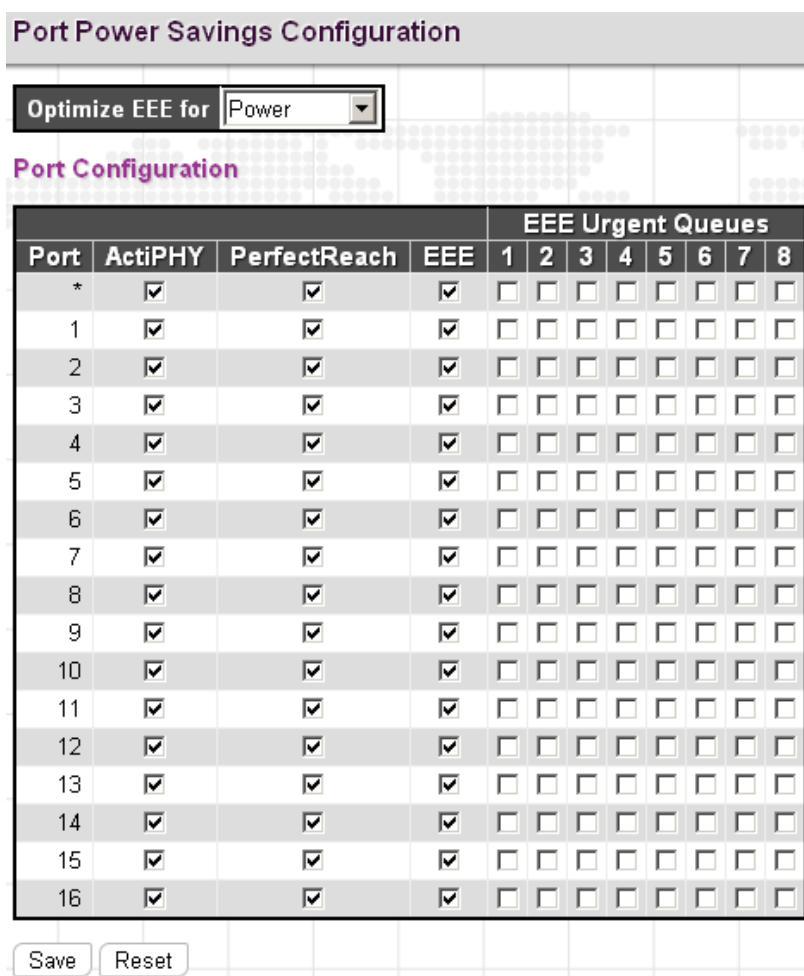


Рис. 26. Вид меню Green Ethernet - Configuration

**Port Power Savings Configuration** (Настройка энергосбережения портов)

Optimize EEE for (Оптимизировать EEE для): Включить/выключить функцию EEE для данного коммутатора. Можно выбрать одну из двух опций:

- Power (Электропитание): Функция EEE включена. Устройство оптимизировано с целью наибольшего сохранения электроэнергии.
- Latency (Работа в традиционном режиме): Функция EEE включена. Устройство оптимизировано с целью наименьшей задержки трафика. Это значение задано по умолчанию.

**Область Port Configuration** (Настройка портов)

**ActiPHY™:** Технология ActiPHY™ снижает электропитание порта, когда подключение отсутствует. На порт на короткое время подается электропитание, чтобы определить, вставлен ли штекер кабеля Ethernet в гнездо разъема порта. Для портов, к которым не подключены кабели, PHY оставит электропитание выключенным, чтобы сберечь энергию.

**PerfectReach™** (Технология PerfectReach™): Технология PerfectReach™ является другим способом энергосбережения. При котором определяется длина кабеля и понижается мощность передатчиков на портах с короткими кабелями.

**EEE** (Энергетически эффективный Ethernet): EEE реализует способ энергосбережения, при котором энергопотребление снижается, когда трафик отсутствует либо он мал. Протокол EEE был разработан в рамках IEEE802.3az и инициирован Институтом инженеров по радиоэлектронике и электротехнике (IEEE). Протокол EEE отключает электропитание схем, когда отсутствует трафик. Когда порт получает данные, подлежащие передаче, на все схемы подается электропитание. Время, требуемое для подачи питания на схемы, называется временем пробуждения. По умолчанию, время пробуждения составляет 17 мкс для линий, работающих на скорости 1 Гбит/с и 30 мкс для остальных линий. Устройства EEE должны согласовать значение времени пробуждения, чтобы гарантировать, что во время передачи трафика электропитание будет подано на все схемы и приемного и передающего устройства. Устройства могут обмениваться

информацией о времени пробуждения по протоколу LLDP (Link Layer Discovery Protocol – протокол обнаружения сетевых устройств на канальном уровне). EEE для портов работает в режиме автосогласования параметров, при этом порт согласует использование скорости либо 1 Гбит/с либо 100 Мбит/с в режиме полного дуплекса. Для портов, не поддерживающих EEE, соответствующие поля с флагами неработоспособны и окрашены в серый цвет.

Когда электропитание порта отключается для энергосбережения, исходящий трафик записывается в буфер до тех пор, пока на порт снова не будет подано электропитание. Вследствие того, что для включения/выключения электропитания порта требуется передать некоторый объем служебной информации, больше энергии удастся сэкономить, если трафик будет буферизоваться до получения большого кадра трафика, который затем будет передан. Буферизация трафика создаст некоторую задержку трафика. Для трафика, который не должен задерживаться, можно назначить срочные очереди, снижающие задержку, однако это ухудшит общее энергосбережение.

**EEE Urgent Queues** (Срочные очереди EEE): Для специальных кадров можно свести задержку к минимуму, распределив эти кадры в особую очередь (при помощи QOS), а затем пометить эту очередь как срочную. Когда срочная очередь получит данные, которые должны быть переданы, на схемы немедленно будет подано электропитание и задержка будет уменьшена до времени пробуждения.

Установленные очереди будут активировать передачу кадров, как только станут доступны данные. В противном случае очередь отложит передачу до тех пор, пока не станет возможной передача пачки кадров.

Пример использования через CLI:

```
green-ethernet eee optimize-for-power
!
interface FastEthernet 1/1
green-ethernet eee
green-ethernet energy-detect
green-ethernet short-reach
```

### 2.3.3 Состояние Green Ethernet

Отображается состояние энергосбережения для всех портов.

Port Power Savings Status								Auto-refresh <input type="checkbox"/>
Port	Link	EEE Cap	EEE Ena	LP EEE Cap	EEE In power save	ActiPhy Savings	PerfectReach Savings	
1	●	✓	✓	✗	✗	✓	✗	
2	●	✓	✓	✗	✗	✓	✗	
3	●	✓	✓	✗	✗	✓	✗	
4	●	✓	✓	✗	✗	✓	✗	
5	●	✓	✓	✗	✗	✓	✗	
6	●	✓	✓	✗	✗	✓	✗	
7	●	✓	✓	✗	✗	✓	✗	
8	●	✓	✓	✗	✗	✗	✗	
9	●	✓	✓	✗	✗	✓	✗	
10	●	✓	✓	✗	✗	✓	✗	
11	●	✓	✓	✗	✗	✓	✗	
12	●	✓	✓	✗	✗	✓	✗	
13	●	✓	✓	✗	✗	✓	✗	
14	●	✓	✓	✗	✗	✗	✗	
15	●	✓	✓	✗	✗	✓	✗	
16	●	✓	✓	✗	✗	✓	✗	

Рис. 27. Вид меню Green Ethernet - Status

На рисунке выше показано текущее состояние функций Green Ethernet на портах устройства. Следует заметить, что энергосберегающий протокол Ethernet не применяется к оптическим портам, а применяется только к электрическим портам LAN.

## 2.4 Ports (Порты)

В разделах меню Ports (Порты) содержатся параметры, определяющие настройку оптических и электрических портов.

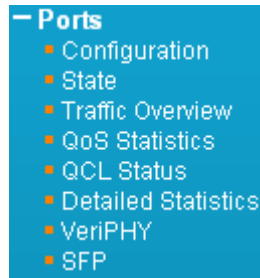


Рис. 28. Вид меню Ports

### 2.4.1 Ports Configuration (Настройка портов)

На этой странице отображаются текущие настройки портов, некоторые из которых можно изменить.

Port Configuration								
Port	Link	Speed		Flow Control			Maximum Frame Size	Excessive Collision Mode
		Current	Configured	Current Rx	Current Tx	Configured		
*			<>			<input type="checkbox"/>	9600	<>
1	Down	Auto		✗	✗	<input type="checkbox"/>	9600	Discard
2	Down	Auto		✗	✗	<input type="checkbox"/>	9600	Discard
3	Down	Auto		✗	✗	<input type="checkbox"/>	9600	Discard
4	Down	Auto		✗	✗	<input type="checkbox"/>	9600	Discard
5	Down	Auto		✗	✗	<input type="checkbox"/>	9600	Discard
6	Down	Auto		✗	✗	<input type="checkbox"/>	9600	Discard
7	Down	Auto		✗	✗	<input type="checkbox"/>	9600	Discard
8	100fdx	Auto		✗	✗	<input type="checkbox"/>	9600	Discard
9	Down	Auto		✗	✗	<input type="checkbox"/>	9600	Discard
10	Down	Auto		✗	✗	<input type="checkbox"/>	9600	Discard
11	Down	Auto		✗	✗	<input type="checkbox"/>	9600	Discard
12	Down	Auto		✗	✗	<input type="checkbox"/>	9600	Discard
13	Down	Auto		✗	✗	<input type="checkbox"/>	9600	Discard
14	100fdx	Auto		✗	✗	<input type="checkbox"/>	9600	Discard
15	Down	Auto		✗	✗	<input type="checkbox"/>	9600	Discard
16	Down	Auto		✗	✗	<input type="checkbox"/>	9600	Discard
17	Down	Auto		✗	✗	<input type="checkbox"/>	9600	
18	Down	Auto		✗	✗	<input type="checkbox"/>	9600	
19	Down	Auto		✗	✗	<input type="checkbox"/>	9600	
20	Down	1Gbps FDX		✓	✓	<input checked="" type="checkbox"/>	9600	

Save Reset

Рис. 29. Вид меню Ports - Configuration

**Port (Порт):** Данное устройство представляет собой промышленный коммутатор с 16 электрическими портами LAN с номерами 1~16 и 4 оптическими портами (для SFP-модулей) с номерами 17~20. Каждому пронумерованному логическому порту отводится одна строка. Порт, отмеченный знаком "\*" будет выполнять операции на всех портах.

**Link (Состояние подключения):** В этом столбце отображается текущее состояние подключения для каждого порта. Зеленый цвет означает, что подключение активно, красный – неактивно.

**Current Speed (Текущая скорость):** В этом столбце приведена текущая скорость подключения (10 Мбит/с, 100 Мбит/с, 1 Гбит/с) и тип дуплекса (fdx=полный дуплекс, hdx=полудуплекс).

**Configured Speed (Настроенная скорость):** В этом раскрывающемся списке можно выбрать любую скорость, доступную для данного порта коммутатора. Показаны только те скорости, которые поддерживаются данным портом.

Возможные настройки для медных портов:

- Disabled (Выключен): Порт коммутатора выключен.
- Auto (Автоматически): Выполняется согласование скорости с устройством на другом конце линии, при этом выбирается скорость, которая поддерживается этим устройством, согласуется также тип дуплекса.
- 10Mbps HDX: для порта принудительно устанавливается скорость 10 Мбит/с, полудуплекс.
- 10Mbps FDX: для порта принудительно устанавливается скорость 10 Мбит/с, полный дуплекс.
- 100Mbps HDX: для порта принудительно устанавливается скорость 100 Мбит/с, полудуплекс.
- 100Mbps FDX: для порта принудительно устанавливается скорость 100 Мбит/с, полный дуплекс.

Возможные настройки для оптических портов следующие:

- Disabled (Выключен): Порт коммутатора выключен.
- Auto (Автоматически): Выполняется согласование скорости с устройством на другом конце линии, при этом выбирается наибольшая скорость, поддерживаемая этим устройством, согласуется также тип дуплекса.
- 100Mbps FDX: для порта принудительно устанавливается скорость 100 Мбит/с, полный дуплекс.
- 1Gbps FDX: для порта принудительно устанавливается скорость 1 Гбит/с, полный дуплекс.

**Flow Control** (Управление потоком): В столбце Current Rx указано, 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 (см. выше).

**Maximum Frame Size** (Максимальный размер кадра): Здесь можно ввести максимальный размер кадра, допустимый для порта коммутатора, включая FCS. Данный коммутатор поддерживает пакеты длиной не более 9600 байт.

**Excessive Collision Mode** (Режим работы при слишком большом числе столкновений пакетов): Данная настройка конфигурирует порт на установку режима передачи при столкновениях пакетов: либо "Discard" (отбрасывание кадра после 16 столкновений – выбрано по умолчанию), либо "Restart" (перезапуск алгоритма смещения (backoff algorithm) после 16 столкновений).

Пример использования через CLI:

```
interface GigabitEthernet 1/4
speed 1000
flowcontrol on
duplex full
```

## 2.4.2 Ports State (Состояние портов)

Отображается графическое изображение коммутатора.

## Port State Overview

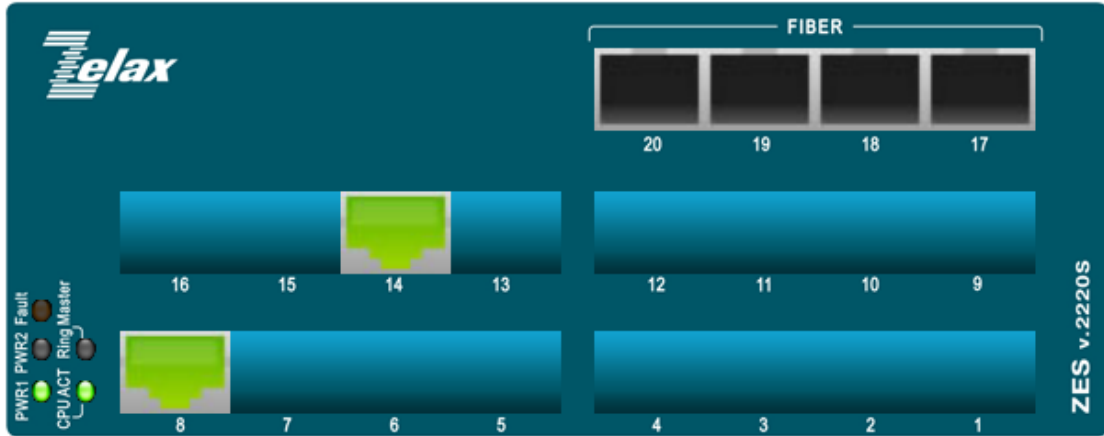


Рис. 30. Вид меню Ports - State

Оно точно такое же, как и изображение, отображаемое при первом входе в коммутатор для управления. "Зеленые" порты означают, что порт подключен при скорости передачи в линии 100 Мбит/с. "Оранжевые" порты означают подключение к линии на скорости 1 Гбит/с. "Серые" порты не подключены к линии. Окно состояния подключений можно обновить, нажав на кнопку "Refresh" (Обновить). Когда в поле "Auto-refresh" (Обновлять автоматически) установлен флаг, дисплей будет обновляться автоматически через каждые 3 секунды.

### 2.4.3 Ports Traffic Overview (Обзор трафика портов)

Отображается сводная информация по трафику на всех портах.

Port Statistics Overview										
Port	Packets		Bytes		Errors		Drops		Filtered	
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	
1	9	10	616	760	0	0	0	0	0	1
2	0	0	0	0	0	0	0	0	0	0
3	1432	1179	319718	570832	0	0	0	0	0	64
4	0	0	0	0	0	0	0	0	0	0
5	18556	17791	1660965	1938476	0	0	0	0	0	343
6	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0
8	6408	1331	410714	150511	0	0	0	0	0	3
9	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0
14	68363	68374	7320692	6441492	1	0	0	0	0	56
15	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0

Рис. 31. Вид меню Ports - Traffic Overview

**Port** (Порт): Номер логического порта (1~20), к которому относятся данные, приведенные в этой строке.

**Packets** (Пакеты): Число принятых и переданных через порт пакетов.

**Bytes** (Байты): Число принятых и переданных через порт байтов.

**Errors** (Ошибки): Число кадров, принятых с ошибками и число неполных кадров, переданных через порт.

**Drops** (Отброшено): Число кадров, отброшенных вследствие перегрузки на линиях входящего и исходящего потоков.

**Filtered** (Отфильтровано): Число принятых кадров, отфильтрованных в процессе последующей передачи (форвардинга).

Данное окно можно обновить, нажав на кнопку "Refresh" (Обновить). Когда в поле "Auto-refresh" (Обновлять автоматически) установлен флаг, окно будет обновляться автоматически через каждые 3 секунды. Чтобы очистить все счетчики и начать отсчет снова, нажмите кнопку "Clear" (Очистить).

## 2.4.4 Ports QoS Statistics (Статистика QoS для портов)

На этой странице приведена статистика различных очередей для всех портов коммутатора.

Queuing Counters																
Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	10
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	1432	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1179
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	18556	0	0	0	0	0	0	0	0	0	0	0	0	0	0	17791
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	6506	1309	0	0	0	0	0	0	0	0	0	0	0	0	0	33
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	68484	3246	0	0	0	0	0	0	0	0	0	0	0	0	0	65288
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Рис. 32. Вид меню Ports - QoS Statistics

**Port** (Порт): Номер логического порта, к которому относятся данные, приведенные в соответствующей ему строке.

**Qn** (Приоритет): На каждом порту имеется 8 очередей QoS. Q0 – очередь с наименьшим приоритетом.

**Rx/Tx**: Число принятых и переданных через каждую очередь пакетов.

## 2.4.5 Ports QCL Status (Состояние QCL)

На этой странице представлено состояние QCL (QoS Control List) для различных пользователей QCL.

QoS Control List Status							
User	QCE	Port	Frame Type	Action			Conflict
				CoS	DPL	DSCP	
No entries							

Рис. 33. Вид меню Ports - QCL Status

В каждой строке описан QCE (QoS Control Entry), который был определен. Если конкретный QCE не применим к аппаратным средствам из-за ограничений аппаратуры, то возникает конфликт. Для каждого коммутатора общее число QCE составляет 256.

**User** (Пользователь): Указывает пользователя QCL.

**QCE#:** Указывает индекс QCE.

**Frame Type** (Тип кадра): Указывает тип кадра, используемый при просмотре входящих кадров. Возможны следующие типы кадров:

- Any (Любой): QCE будет соответствовать всем типам кадров.
- Ethernet: 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.

**Port** (Порт): Указывает список портов, сконфигурированных с QCE.

**Action** (Операция): Указывает операцию классификации, выполняемую с входящим кадром, если настройки параметров согласуются с содержимым кадра. Имеется три поля операции: Class (Класс), DPL и DSCP.

- Class (Класс): Классифицированный класс QoS; если кадр соответствует QCE, он будет помещен в очередь.
- DPL: Уровень снижения приоритета (Drop Precedence Level); если кадр соответствует QCE, то уровень DP будет задан равным значению, отображенному в столбце DPL.
- DSCP: Если кадр соответствует QCE, то DSCP будет классифицировано со значением, отображенным в столбце DSCP.

**Conflict** (Конфликт): Отображается состояние конфликтов для элементов QCL. Так как аппаратные ресурсы совместно используются многими приложениями, может случиться так, что ресурсов, требующихся для добавления QCE, может оказаться недостаточно. В этом случае отображается состояние конфликта 'Yes' (Да), в противном случае всегда отображается 'No' (Нет). Пожалуйста, имейте в виду, что конфликт можно разрешить, освободив аппаратные ресурсы; чтобы добавить элемент QCL, нажмите кнопку 'Resolve Conflict' (Разрешить конфликт).

## 2.4.6 Ports Detailed Statistics (Детальная статистика портов)

На этой странице приведены детальная статистика трафика для конкретного порта коммутатора. Отображаются следующие счетчики: общие значения (передача и прием); счетчики по размерам кадров (передача и прием); счетчики ошибок (передача и прием). Для выбора порта, для которого будет отображена детальная статистика, используйте раскрывающийся список port select (выбор порта).



Detailed Port Statistics Port 1				Port 1	Auto-refresh	Refresh
Receive Total		Transmit Total				
Rx Packets	9	Tx Packets	10			
Rx Octets	616	Tx Octets	760			
Rx Unicast	7	Tx Unicast	3			
Rx Multicast	0	Tx Multicast	6			
Rx Broadcast	2	Tx Broadcast	1			
Rx Pause	0	Tx Pause	0			
Receive Size Counters		Transmit Size Counters				
Rx 64 Bytes	5	Tx 64 Bytes	2			
Rx 65-127 Bytes	4	Tx 65-127 Bytes	8			
Rx 128-255 Bytes	0	Tx 128-255 Bytes	0			
Rx 256-511 Bytes	0	Tx 256-511 Bytes	0			
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0			
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0			
Rx 1527- Bytes	0	Tx 1527- Bytes	0			
Receive Queue Counters		Transmit Queue Counters				
Rx Q0	9	Tx Q0	0			
Rx Q1	0	Tx Q1	0			
Rx Q2	0	Tx Q2	0			
Rx Q3	0	Tx Q3	0			
Rx Q4	0	Tx Q4	0			
Rx Q5	0	Tx Q5	0			
Rx Q6	0	Tx Q6	0			
Rx Q7	0	Tx Q7	10			
Receive Error Counters		Transmit Error Counters				
Rx Drops	0	Tx Drops	0			
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0			
Rx Undersize	0					
Rx Oversize	0					
Rx Fragments	0					
Rx Jabber	0					
Rx Filtered	1					

Рис. 34. Вид меню Ports - Detailed Statistics

Поля **Receive Total** (Всего принято) и **Transmit Total** (Всего передано):

- Rx и Tx Packets: Число принятых и переданных (хороших и плохих) пакетов.
- Rx и Tx Octets: Число принятых и переданных (хороших и плохих) пакетов. Включает FCS, за исключением служебных разрядов кадра.
- Rx и Tx Unicast: Число принятых и переданных (хороших и плохих) одноадресных пакетов.
- Rx и Tx Multicast: Число принятых и переданных (хороших и плохих) многоадресных пакетов.
- Rx и Tx Broadcast: Число принятых и переданных (хороших и плохих) широковещательных пакетов.
- Rx и Tx Pause: Число кадров MAC-управления, принятых или переданных этим портом, которые имеют код операции, соответствующий паузе.

Счетчики **Receive и Transmit Size**: Отображается число принятых и переданных (хороших и плохих) пакетов, отсортированных по категориям на основе длин кадров.

Счетчики **Receive и Transmit Queue**: Отображается число принятых и переданных пакетов по каждой входной и выходной очереди.

Счетчики **Receive Error** (Ошибки на приеме):

- Rx Drops (Сброс): Число отброшенных кадров, обусловленных нехваткой буферов на приеме или перегрузкой выходных линий.
- Rx CRC/Alignment: Число кадров, принятых с ошибками в контрольных суммах и ошибками в длине.
- Rx Undersize: Число коротких<sup>1</sup> кадров, принятых с правильной контрольной суммой.
- Rx Oversize: Число длинных<sup>2</sup> кадров, принятых с правильной контрольной суммой.
- Rx Fragments: Число коротких<sup>1</sup> кадров, принятых с неправильной контрольной суммой.
- Rx Jabber: Число длинных<sup>2</sup> кадров, принятых с неправильной контрольной суммой.
- Rx Filtered: Число принятых кадров, отфильтрованных в процессе последующей передачи (форвардинга).

<sup>1</sup> Короткие кадры – это кадры длиной менее 64 байта.

<sup>2</sup> Длинные кадры – это кадры, имеющие длину, превышающие максимальную длину кадра, заданную для данного порта.

Счетчики **Transmit Error** (Ошибки на передаче):

- Tx Drops: Число кадров, отброшенных вследствие переполнения выходного буфера.
- Tx Late/Exc. Coll.: Число кадров, отброшенных вследствие слишком большого числа столкновений или поздних столкновений.

## 2.4.7 Ports VeriPHY™ (Диагностика подключения кабелей к портам)

Эта страница используется для запуска утилиты диагностики кабелей VeriPHY™ для медных портов, работающих на скорости 10 Мбит/с, 100 Мбит/с и 1 Гбит/с. Из раскрывающегося списка выберите какие порты будут проверяться либо выберите All (все порты). Нажмите кнопку “Start” (Пуск).

Cable Status								
Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	--	--	--	--	--	--	--	--
2	--	--	--	--	--	--	--	--
3	--	--	--	--	--	--	--	--
4	--	--	--	--	--	--	--	--
5	--	--	--	--	--	--	--	--
6	--	--	--	--	--	--	--	--
7	--	--	--	--	--	--	--	--
8	OK	3	OK	3	OK	3	Open	0
9	--	--	--	--	--	--	--	--
10	--	--	--	--	--	--	--	--
11	--	--	--	--	--	--	--	--
12	--	--	--	--	--	--	--	--
13	--	--	--	--	--	--	--	--
14	--	--	--	--	--	--	--	--
15	--	--	--	--	--	--	--	--
16	--	--	--	--	--	--	--	--

Рис. 35. Вид меню Ports - VeriPHY™

Диагностика одного порта длится приблизительно 5 секунд. Если выбраны все порты, диагностика может занять около 15 секунд. По завершении диагностики, страница будет обновлена автоматически. Результаты диагностики будут представлены в таблице состояния кабелей. Имейте в виду, что утилита VeriPHY™ работает точно только для кабелей длиной 7 – 140 м.

Во время работы VeriPHY™ порты, работающие на скоростях 10 Мбит/с и 100 Мбит/с будут выключены. Поэтому, выполнение VeriPHY на порту управления, работающем на скорости 10 Мбит/с или 100 Мбит/с, приведет к тому, что коммутатор перестанет отвечать на команды до тех пор, пока VeriPHY не завершится.

**Port** (Порт): Номер порта.

**Pair** (Пара): Состояние кабеля пары:

- OK: К паре правильно подключена нагрузка.
- Open (Разомкнуто): Пара разомкнута на конце.
- Short (Замкнуто): Пара замкнута накоротко.
- Short A: Кросс-пара замкнута на пару A.
- Short B: Кросс-пара замкнута на пару B.
- Short C: Кросс-пара замкнута на пару C.
- Short D: Кросс-пара замкнута на пару D.
- Cross A: Анормальное соединение кросс-пары с парой A
- Cross B: Анормальное соединение кросс-пары с парой B
- Cross C: Анормальное соединение кросс-пары с парой C
- Cross D: Анормальное соединение кросс-пары с парой D

**Length** (Длина): Длина пары проводников в метрах. Точность  $\pm 3$  метра.

Пример использования через CLI:

```
ZES-2220S# show interface FastEthernet 1/8 veriphy
Starting VeriPHY - Please wait
Interface          Pair A  Length  Pair B, Length  Pair C  Length  Pair D  Length
-----
FastEthernet 1/8  OK     3       OK     3       OK     3       Open   0
```

## 2.4.8 Ports SFP (Состояние SFP портов)

На этой странице отображается текущее состояние SFP для всех оптических портов.

SFP and D/D Information	
<b>Port 17</b>	
Vendor Name	Zelax
Vendor Part Number	SFP-G-S1310/20-D
Fiber Type	Single
Wave Length	1310 nm
Link Length	20 km
TX Power	-6 dBm
RX Power	-40 dBm
RX Sensitivity	0 dBm
Temperature	37°C
<b>Port 18</b>	
None	
<b>Port 19</b>	
None	
<b>Port 20</b>	
None	

Рис. 36. Вид меню Ports - SFP

**Vendor Name** (Наименование изготовителя): Наименование изготовителя SFP.

**Vendor Part** (Номер изделия по каталогу изготовителя): Номер изделия по каталогу изготовителя (предоставляется изготовителем SFP).

**Fiber Type** (Тип оптоволоконного кабеля): Тип оптоволоконного кабеля – одномодовый или многомодовый.

**Wave Length** (Длина волны): Длина волны лазера на передачу (Tx).

**Wave Length 2** (Длина волны 2): Длина волны лазера на прием (Rx). (не все SFP поддерживают считывание этого параметра).

**Link Length** (Длина линии): Длина линии. (Берется из спецификации SFP модуля, не является реально измеренной.)

**TX Power** (Мощность на выходе передатчика): Мощность передатчика на лазерном диоде; сообщается модулем SFP, поддерживающим DDMI (цифровой интерфейс диагностики и мониторинга).

**RX Power** (Мощность на входе приемника): Принятая оптическая мощность, сообщенная модулем SFP, поддерживающим DDMI.

**RX Sensitivity** (Чувствительность приемника): Чувствительность приемника, сообщенная модулем SFP, поддерживающим DDMI.

**Temperature** (Температура): Внутренняя температура, сообщенная модулем SFP, поддерживающим DDMI.

Пример использования через CLI:

```
ZES-2220S# show sfp
17
-----
Vendor Name       : Zelax
Vendor Part Number: SFP-G-S1310/20-D
Fiber Type        : Single
Wave Length       : 1310 nm
Link Length       : 20 km
TX Power          : -6 dBm
RX Power          : -40 dBm
RX Sensitivity    : 0 dBm
Temperature       : 59 degree C
```

## 2.5 Security (Безопасность)

В меню Security (Безопасность) имеется три основных раздела switch (коммутатор), network (сеть) и RADIUS.

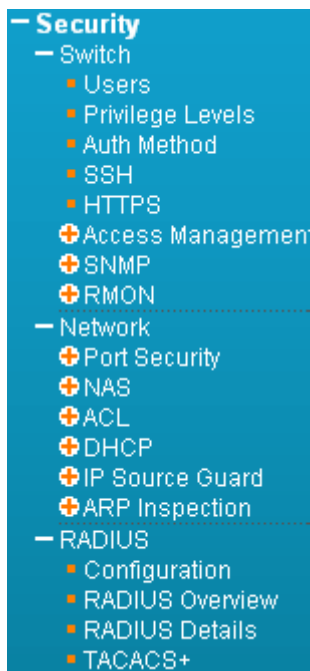


Рис. 37. Вид меню Security

### 2.5.1 Switch (Коммутатор)

## 2.5.1.1 Users (Пользователи)

На этой странице перечислены текущие пользователи. В настоящее время есть только один способ входа на web-сервер под именем другого пользователя – закрыть и снова открыть браузер.



Рис. 38. Вид меню Security – Switch - Users

По умолчанию существует только один пользователь 'admin', которому присвоен наивысший уровень привилегий (15).

Чтобы отредактировать существующего пользователя – нажмите мышью соответствующий элемент списка в столбце **User Name** (Имя пользователя) либо нажмите кнопку "Add New User" (Добавить нового пользователя), чтобы добавить нового пользователя.

### Add User (Добавить пользователя)

Add User

User Settings	
User Name	zelax
Password	*****
Password (again)	*****
Privilege Level	10

Save Reset Cancel

Рис. 39. Вид меню Security – Switch – Users (Add User)

**User Name** (Имя пользователя): Введите имя нового пользователя.

**Password** (Пароль): Введите пароль для учетной записи этого пользователя.

**Password (again)** (Пароль еще раз): Еще раз введите пароль для учетной записи этого пользователя.

**Privilege Level** (Уровень привилегий): Выберите соответствующий уровень привилегий для учетной записи этого пользователя. Диапазон допустимых значений: от 1 до 15.

Если значение уровня привилегий равно 15, пользователь имеет доступ ко всем группам, то есть имеет полный контроль над устройством. Для доступа только к определенным группам необходимо использовать другие значения уровня привилегий. Для доступа к группе пользователь должен иметь уровень привилегий не меньше того, который требуется для этой группы. По умолчанию, для доступа к большинству групп только по чтению достаточно уровня привилегий 5; уровень привилегий 10 обеспечивает доступ к большинству групп по чтению/записи. Для обслуживания системы (обновление ПО, установка заводских настроек и т. д.) необходим уровень привилегий пользователя, равный 15.

В целом, уровень привилегий 15 можно использовать для учетной записи администратора; уровень привилегий 10 – для стандартной пользовательской учетной записи; уровень привилегий 5 – для гостевой учетной записи.

Пример использования через CLI:

```
username zelax privilege 10 password unencrypted <password>
```

## 2.5.1.2 Уровни привилегий

На этой странице приведена сводная информация по уровням привилегий.

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
DHCP	5	10	5	10
Dhcp_Client	5	10	5	10
Diagnostics	5	10	5	10
EEE	5	10	5	10
ERPS	5	10	5	10
Green_Ethernet	5	10	5	10
IP2	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
Maintenance	15	15	15	15
Mirroring	5	10	5	10
MVR	5	10	5	10
NTP	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
RPC	5	10	5	10
Security	5	10	5	10
SMTP	5	10	5	10
Spanning_Tree	5	10	5	10
System	5	10	1	10
Timer	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
XXRP	5	10	5	10
Z-Ring	1	15	5	10

Save Reset

Рис. 40. Вид меню Security – Switch – Privilege Levels

**Group Name** (Имя группы): Имя, идентифицирующее группу привилегий. В большинстве случаев группа уровней привилегий содержит один модуль (например, LACP, RSTP или QoS), однако некоторые группы могут содержать более одного модуля. Ниже группы привилегий описаны более детально.

**System** (Система): Contact (Контактное лицо), Name (Имя), Location (Местонахождение), Timezone (Часовой пояс), Daylight Saving Time (Переход на летнее время), Log (Системный журнал).

**Security** (Безопасность): Authentication (Аутентификация), System Access Management (Управление доступом к системе), Port (Порт) (содержит разделы Dot1x port (Порт Dot1x), MAC based (На основе MAC-адресов), MAC Address Limit (ограничение MAC-адресов), ACL, HTTPS, SSH, ARP Inspection (Инспекция ARP), IP source guard (Защита IP-адреса источника).

**IP**: Все привилегии, за исключением команды 'ping'.

**Port** (Порт): Все привилегии, за исключением команды 'VeriPHY'.

**Diagnostics** (Диагностика): команды 'ping' и 'VeriPHY'.

**Maintenance** (Обслуживание): CLI System Reboot (Перезагрузка системы из командной строки), System Restore Default (Восстановление системных параметров по умолчанию), System Password (Пароль системы), Configuration Save (Сохранение конфигурации), Configuration Load (Загрузка конфигурации), Firmware Load (Загрузка ПО). Web Users (Пользователи Web-интерфейса), Privilege Levels (Уровни привилегий) и все остальное доступно в группе Maintenance.

**Debug** (Отладка): Присутствует только в CLI.

**Privilege Levels** (Уровни привилегий): Каждая группа имеет уровень привилегий авторизации для следующих подгрупп:

- configuration read-only (конфигурация, только на чтение)
- configuration/execute read-write (конфигурирование/выполнение, чтение-запись)
- status/statistics read-only (состояние/статистики, только на чтение)
- status/statistics read-write (e.g. for clearing of statistics) (состояние/статистики, чтение-запись – например, для очистки статистик).

Для получения доступа к группе привилегий, пользователь должен иметь такой же или больший уровень привилегий.

Пример использования через CLI:

```
web privilege group Z-Ring level cro 1 crw 15 sro 5 srw 10
```

### 2.5.1.3 Auth Method (Метод авторизации)

На этой странице можно задать как пользователи будут аутентифицироваться при регистрации на коммутаторе с помощью одного из клиентских интерфейсов управления.

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

Рис. 41. Вид меню Security – Switch – Auth Method

**Client** (Клиент): Способ управления для которого применяются настройки, перечисленные ниже.

**Methods** (Методы): В поле методов может быть указано одно из следующих значений:

- no (нет): Аутентификация выключена, регистрация невозможна.

- local (локально): Для аутентификации на коммутаторе используется локальная база данных пользователей.
- radius: Для идентификации используются удаленные RADIUS-сервера.
- tacacs+: Для идентификации используются удаленные TACACS+-сервера.

**Key Match Mode** (режим соответствия ключей): Изменение алгоритма при работе с сервером TACACS+. Данная функция предназначена, если в поле Methods выбрана первичная аутентификация с помощью сервера tacacs и вторичная local. Если сервер TACACS+ недоступен, коммутатор предоставляет возможность пользователю пройти вторичную аутентификацию по локальной учётной записи. В тот момент, когда сервер TACACS+ доступен, но ключ сервера и коммутатора не совпадает, пользователь не сможет пройти аутентификацию по локальной учётной записи, так как для коммутатора сервер доступен и несовпадение ключей не является причиной отказа от сервера, соответственно коммутатор не разрешает пройти аутентификацию по локальной учётной записи. Функция Key Match Mode позволяет предоставить возможность аутентификации пользователя по локальной учётной записи в случае несовпадения ключей на коммутаторе и сервере TACACS+.

Возможны следующие режимы работы:

- Enabled (Включен): Включение режима Key Match Mode позволит пользователю пройти аутентификацию по локальной учётной записи в случае, если по каким-то причинам ключ на коммутаторе и сервере TACACS+ не совпадает.
- Disabled (Выключен): При выключенном режиме Key Match Mode, коммутатор не даст пользователю пройти аутентификацию по локальной учётной записи, если ключ на коммутаторе и сервере TACACS+ не совпадает. По умолчанию данный режим выключен.

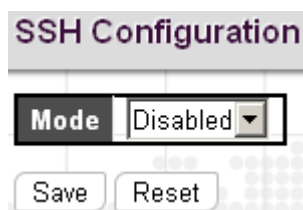
**ПРИМЕЧАНИЕ:** Методы, в которых участвуют удаленные серверы, имеют время ожидания, так как удаленные серверы могут быть отключены. В этом случае осуществляется попытка аутентификации со следующим методом. Предпринимаются попытки для всех методов, в том порядке, в котором они перечислены слева направо, до тех пор, пока не будет найден метод, аутентифицировавший или отвергнувший пользователя. Если удаленный сервер используется для первичной аутентификации, рекомендуется для вторичной аутентификации задать опцию 'local' (локально). Это позволит клиенту управления зарегистрироваться через локальную базу данных пользователей, если ни один из сконфигурированных серверов аутентификации не работает.

Пример использования через CLI:

```
aaa authentication login telnet radius tacacs local
aaa authentication login key-match
```

### 2.5.1.4 SSH

На этой странице можно настроить SSH.



**Рис. 42. Вид меню Security – Switch – SSH**

**Mode** (Режим работы): режим работы SSH. Возможны следующие режимы работы:

- Enabled (Включен): SSH включен. По умолчанию, режим работы - включен.
- Disabled (Выключен): SSH выключен.

**ПРИМЕЧАНИЕ:** SSH, используемый в данном устройстве, реализует версию 2 протокола SSH.

Пример использования через CLI:

```
no ip ssh
```



## 2.5.1.5 HTTPS

На этой странице можно настроить HTTPS.

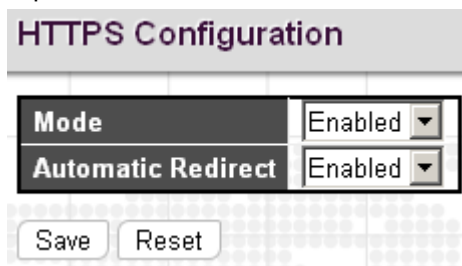


Рис. 43. Вид меню Security – Switch – HTTPS

**Mode** (Режим работы): режим работы HTTPS. Когда текущее соединение является соединением HTTPS, но HTTPS выключен, web-браузер будет автоматически перенаправляться на соединение HTTP. Возможны следующие режимы работы:

- Enabled (Включен): HTTPS включен.
- Disabled (Выключен): HTTPS выключен.

**Automatic Redirect** (Автоматическое перенаправление): режим работы автоматического перенаправления HTTPS. Применяется только, если для режима работы HTTPS выбрано "Enabled" (Включен). Автоматически перенаправляет HTTP web-браузера на соединение HTTPS, когда включены оба режима работы – HTTPS и Automatic Redirect. Возможны следующие режимы работы:

- Enabled (Включен): перенаправление HTTPS включено.
- Disabled (Выключен): перенаправление HTTPS выключено.

Пример использования через CLI:

```
ip http secure-server
ip http secure-redirect
```

## 2.5.2 Access Management (Управление доступом)

### 2.5.2.1 Access Management Configuration (Настройка управления доступом)

На этой странице можно настроить таблицу управления доступом. Максимальное число элементов списка 16. Если тип приложения совпадает с одним из типов, имеющимся в списке управления доступом, то доступ к коммутатору будет разрешен.

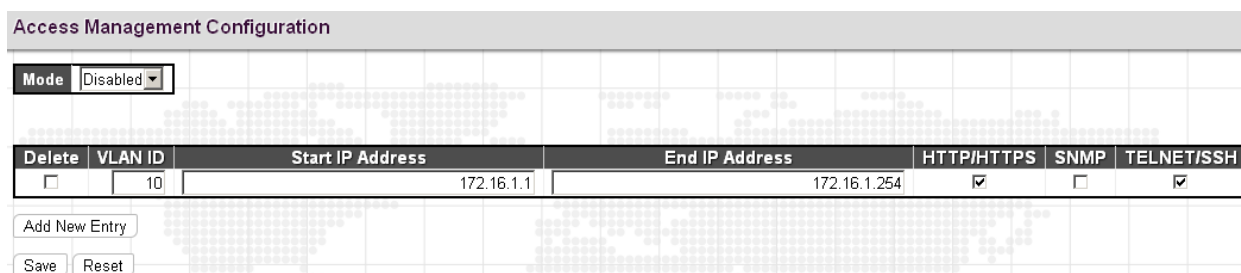


Рис. 44. Вид меню Security – Switch – Access Management - Configuration

**Mode** (Режим работы): режим работы управления доступом. Возможны следующие режимы работы:

- Enabled (Включен): Режим управления доступом включен.
- Disabled (Выключен): Режим управления доступом выключен.

**VLAN ID**: номер VLAN для элемента управления доступом.

**Start IP address** (Начальный IP-адрес): начальный IP-адрес для элемента управления доступом.

**End IP address** (Конечный IP-адрес): конечный IP-адрес для элемента управления доступом.

**HTTP/HTTPS**: если в этом поле установлен флаг, это указывает, что хосту с IP-адресом из указанного диапазона может быть предоставлен доступ к коммутатору по HTTP/HTTPS.

**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 .

Чтобы ввести новый элемент в список, нажмите кнопку “Add New Entry” (Добавить новый элемент). Чтобы удалить введенный элемент из списка нажмите кнопку “Delete” (Удалить) либо установите флаг в строке, чтобы ранее сохраненный элемент был удален при следующем сохранении.

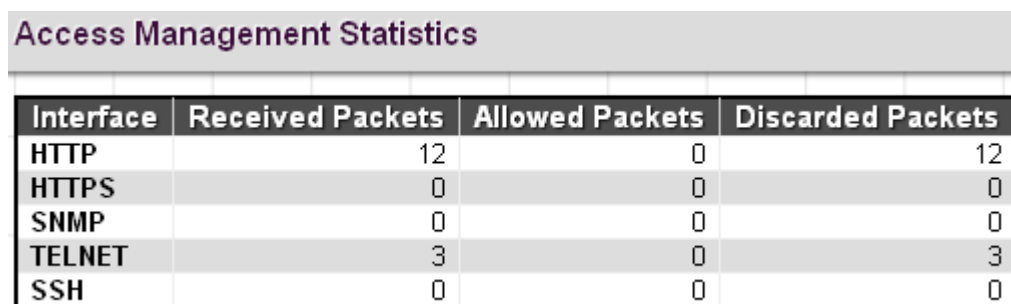
Нажмите кнопку “Save” (Сохранить), чтобы сохранить настройки или изменения. Нажмите кнопку “Reset” (Переустановить), чтобы восстановить настройки, используемые по умолчанию.

Пример использования через CLI:

```
access management 1 10 172.16.1.1 to 172.16.1.254 web telnet
```

## 2.5.2.2 Access Management Statistics (Статистики управления доступом)

На этой странице приведена статистика управления доступом.



Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	12	0	12
HTTPS	0	0	0
SNMP	0	0	0
TELNET	3	0	3
SSH	0	0	0

Рис. 45. Вид меню Security – Switch – Access Management - Statistics

**Interface** (Интерфейс): Тип интерфейса, посредством которого любой удаленный хост может получить доступ к коммутатору.

**Received Packets** (Принято пакетов): Число принятых пакетов для указанного типа доступа, когда включен режим управления доступом.

**Allowed Packets** (Разрешено пакетов): Число разрешенных пакетов для указанного типа доступа, когда включен режим управления доступом.

**Discarded Packets** (Отброшено пакетов): Число отброшенных пакетов, для указанного типа доступа, когда включен режим управления доступом.

Пример использования через CLI:

```
ZES-2220S# show access management statistics
Access Management Statistics:
-----
HTTP   Receive:      12   Allow:         0   Discard:       12
HTTPS  Receive:       0   Allow:         0   Discard:       0
SNMP   Receive:       0   Allow:         0   Discard:       0
TELNET Receive:       3   Allow:         0   Discard:       3
SSH    Receive:       0   Allow:         0   Discard:       0
```

## 2.5.3 SNMP

### SNMP System Configuration (Настройка SNMP системы)

На этой странице можно настроить SNMP.

Mode	Enabled
Version	SNMP v2c
Read Community	zelay_public
Write Community	zelay_private
Engine ID	800007e5017f000001

Save Reset

Рис. 46. Вид меню Security – Switch – SNMP - System Configuration

**Mode** (Режим работы): режим работы SNMP. Возможны следующие режимы работы:

- Enabled (Включен): SNMP включен.
- Disabled (Выключен): SNMP выключен.

**Version** (Версия): поддерживаемая версия SNMP. Возможны следующие версии:

- SNMP v1: включена поддержка версии 1 SNMP.
- SNMP v2c: включена поддержка версии 2c SNMP.
- SNMP v3: включена поддержка версии 3 SNMP.

**Read Community** (строка Community по чтению): строка community, доступная по чтению, разрешающая доступ к SNMP-агенту. Допустимая длина строки 0~255 символов ASCII с номерами в диапазоне от 0x21 до 0x7E.

**Write Community** (строка Community по записи): строка community, доступная по записи, разрешающая доступ к SNMP-агенту. Допустимая длина строки 0~255 символов ASCII с номерами в диапазоне от 0x21 до 0x7E. Эти два поля применимы только для SNMP версии v1 или v2c. При SNMP версии v3, строка community будет ассоциирована с таблицей community SNMPv3. SNMPv3 обеспечивает более гибкую настройку безопасного имени, чем при SNMPv1 или SNMPv2c. В дополнение к строке community, для ограничения доступа к подсети источника можно использовать определенный диапазон адресов источника.

**Engine ID**: идентификатор engine ID для SNMPv3. Строка должна содержать четное число (в шестнадцатиричном формате), число цифр от 10 до 64; комбинации цифр, состоящие из одних нулей и из одних «F» недопустимы. При изменении идентификатора Engine ID будут очищены все оригинальные локальные пользователи.

Пример использования через CLI:

```
snmp-server community v2c zelay_public RO
snmp-server community v2c zelay_private RW
```

### 2.5.3.1 Alarm Configuration (Настройка сигнализации)

На этой странице можно настроить SNMP trap.



Рис. 47. Вид меню Security – Switch – SNMP - Alarm Configuration

### Global Settings (Глобальные настройки)

**Mode** (Режим работы): Включает или выключает функцию отправки SNMP trap в глобальном режиме.

Чтобы добавить SNMP trap, нажмите кнопку “Add New Entry” (Добавить новый элемент списка).

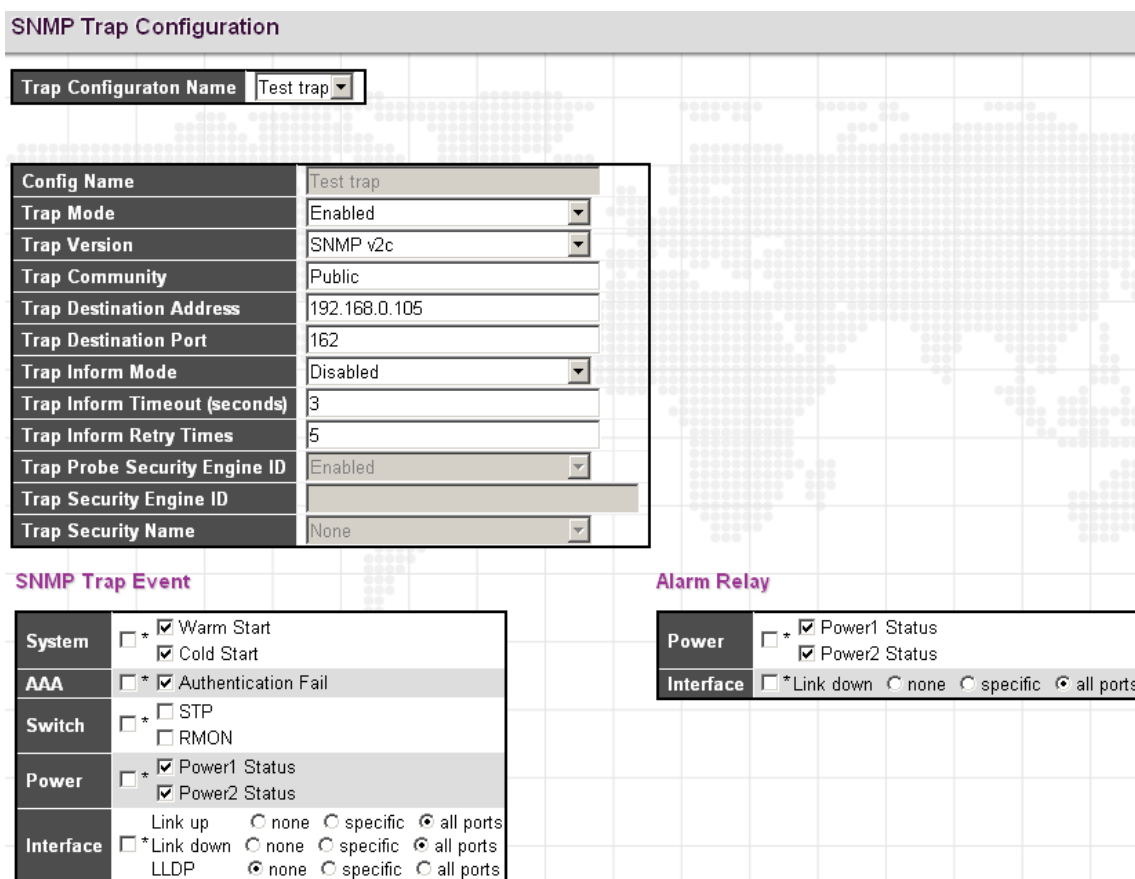


Рис. 48. Вид меню Security – Switch – SNMP - Trap Configuration

### SNMP Trap Configuration (Настройка SNMP Trap)

**Config Name** (Имя конфигурации): содержательное имя для данного элемента списка SNMP trap.

**Trap Mode** (Режим работы Trap): режим работы SNMP trap.

- Enabled (Включен): отправка SNMP trap включена.
- Disabled (Выключен): отправка SNMP trap выключена.

**Trap Version** (Версия Trap): поддерживаемая версия SNMP trap. Возможны следующие версии:

- SNMP v1: включена поддержка версии 1 SNMP trap.
- SNMP v2c: включена поддержка версии 2c SNMP trap.
- SNMP v3: включена поддержка версии 3 SNMP trap.

**Trap Community** (строка Community для отправка SNMP trap): строка доступа community для отправки пакета SNMP trap. Допустимая длина строки 0~255 символов ASCII с номерами в диапазоне от 0x21 до 0x7E.

**Trap Destination Address** (IP-адрес назначения Trap): IP-адрес сервера для отправки SNMP trap. Корректный IP-адрес в десятичном формате с точкой ('x.y.z.w'). Допустимо также указать корректное имя хоста. Корректное имя хоста – строка из алфавитно-цифровых символов (допустимо использовать буквы A-Z; a-z, цифры 0-9, точку (.) и тире (-)). Использовать пробелы запрещается. Первый символ должен быть буквой; первый и последний символы не должны быть точкой или подчеркиванием.

**Trap Destination port** (Порт назначения Trap): 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** (Режим работы Trap Inform): режим работы SNMP trap inform. Возможны следующие режимы работы:

- Enabled (Включен): режим работы SNMP trap inform включен.
- Disabled (Выключен): режим работы SNMP trap inform выключен.

**Trap Inform Timeout** (seconds) (Таймер сообщений Trap Inform (секунд): таймер сообщений SNMP trap inform. Диапазон допустимых значений: от 0 до 2147.

**Trap Inform Retry Times** (Таймер попыток повторения сообщений Trap Inform): таймер попыток повторения сообщений SNMP trap inform. Диапазон допустимых значений: от 0 до 255.

**Trap Probe Security Engine ID**: режим работы SNMP trap probe security engine ID. Возможны следующие значения:

- Enabled (Включен): режим работы SNMP trap probe security engine ID включен.
- Disabled (Выключен): режим работы SNMP trap probe security engine ID выключен.

**Trap Security Engine ID**: режим работы SNMP trap security engine ID.

Протокол SNMPv3 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 шестнадцатиричном 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 SNMPv3 используют USM для аутентификации и обеспечения конфиденциальности. Когда включен режим отправки trap и inform, необходимо задать уникальное имя для обеспечения безопасности.

### **SNMP Trap Event** (События SNMP Trap)

**System** (Системные): Сообщения о системных событиях (system trap events) содержат следующую информацию:

- Warm Start (Рестарт): Коммутатор будет перезагружен из состояния, когда на него подано питание.
- Cold Start (Холодный пуск): Коммутатор будет загружен из состояния с выключенным питанием либо после восстановления подачи питания (после сбоя электросети).

**AAA**: протокол аутентификации, авторизации и проверки учетных записей. Сообщение trap будет создано при любом сбое аутентификации.

**Switch** (Коммутатор): указывает группу сообщений traps коммутатора. Возможны следующие сообщения traps:

- STP: установите флаг в этом поле, чтобы включить режим отправки сообщений STP trap. Снимите флаг, чтобы выключить режим отправки сообщений STP trap.

- RMON: установите флаг в этом поле, чтобы включить режим отправки сообщений RMON trap. Снимите флаг, чтобы выключить режим отправки сообщений RMON trap.

**Power** (Питание): указывает группу сообщений traps, связанных с электропитанием.

Возможны следующие сообщения trap о событиях:

- Power 1 Status (Состояние блока питания 1): установите флаг в этом поле, чтобы включить режим отправки сообщений trap о состоянии блока питания 1. Снимите флаг в этом поле, чтобы выключить режим отправки сообщений trap о состоянии блока питания 1.
- Power 2 Status (Состояние блока питания 2): установите флаг в этом поле, чтобы включить режим отправки сообщений trap о состоянии блока питания 2. Снимите флаг в этом поле, чтобы выключить режим отправки сообщений trap о состоянии блока питания 2.

**Interface** (Интерфейс): указывает группу сообщений traps, связанных с интерфейсами.

Возможны следующие сообщения traps:

- Link Up (Линия включена): none (нет)/specific (для конкретного порта)/all ports (все порты).
- Link Down (Линия выключена): none (нет)/specific (для конкретного порта)/all ports (все порты).
- LLDP: none (нет)/specific (для конкретного порта)/all ports (все порты).

**PoE**: none (нет)/specific (для конкретного порта)/all ports (все порты). Эта опция имеется только на коммутаторах с PoE.

Когда выбрано значение "specific" (конкретный порт), открывается окно с полями флагов, позволяющими выбрать конкретные порты. По завершении настройки всех портов нажмите кнопку "Save" (Сохранить).

### **Alarm Relay** (Аварийное Реле)

**Power** (Питание): указывает группу аварийного реле, связанную с электропитанием.

Возможны следующие опции:

- Power 1 Status (Состояние блока питания 1): Установите флаг в этом поле, чтобы включить функцию сигнализации аварийного реле о состоянии блока питания 1. При отказе блока питания 1 контакты аварийного реле разомкнутся, начнет светиться оранжевый светодиодный индикатор отказа. Снимите флаг в этом поле, чтобы выключить реле сигнализации о состоянии блока питания 1.
- Power 2 Status (Состояние блока питания 2): Установите флаг в этом поле, чтобы включить функцию сигнализации аварийного реле о состоянии блока питания 2. При отказе блока питания 2 контакты аварийного реле разомкнутся, начнет светиться оранжевый светодиодный индикатор отказа. Снимите флаг в этом поле, чтобы выключить реле сигнализации о состоянии блока питания 2.

**Interface** (Интерфейс): указывает группу реле сигнализации, связанную с интерфейсами.

Возможны следующие опции:

- Link Down (Линия выключена): none (нет)/specific (для конкретного порта)/all ports (все порты). При отказе пропадания подключения на выбранных интерфейсах, контакты реле разомкнутся, начнет светиться оранжевый светодиодный индикатор отказа. Чтобы выключить функцию реле сигнализации, снимите флаг в этом поле.

**PoE**: none (нет)/specific (для конкретного порта)/all ports (все порты). Эта опция имеется только на коммутаторах с PoE. При отказе функции PoE на выбранных интерфейсах, контакты реле разомкнутся, начнет светиться оранжевый светодиодный индикатор отказа. Чтобы выключить функцию реле сигнализации, снимите флаг в этом поле.

Когда выбрано значение "specific" (конкретный порт), открывается окно с полями флагов, позволяющими выбрать конкретные порты.

Пример использования через CLI:

```

snmp-server host Test trap
no shutdown
host 192.168.0.105 162 traps
traps system warmstart coldstart
traps system warmstart coldstart aaa authentication
traps system warmstart coldstart aaa authentication power power1 power2
alarm power power1 power2
!
snmp-server trap
!
interface FastEthernet 1/1
snmp-server host Test trap traps linkup linkdown
snmp-server host Test trap alarm linkdown

```

### 2.5.3.2 SNMPv3 Community Configuration (Настройка SNMPv3 Community)

На этой странице можно настроить таблицу SNMPv3 community.

Delete	Community	Source IP	Source Mask
<input type="checkbox"/>	public	192.168.0.0	255.255.255.0
<input type="checkbox"/>	private	0.0.0.0	0.0.0.0

Рис. 49. Вид меню Security – Switch – SNMP - Communities

**Delete** (Удалить): Установите флаг в этом поле, чтобы удалить строку списка, в которой установлен флаг. Строка будет удалена при следующем сохранении.

**Community**: строка доступа community, разрешающая доступ к SNMP-агенту. Допустимая длина строки 1~32 символов ASCII с номерами в диапазоне от 0x21 до 0x7E. Строка community будет трактоваться, как безопасное имя и отображаться в строку community SNMPv1 или SNMPv2c. В строке различаются прописные и строчные буквы.

**Source IP** (IP-адрес источника): IP-адрес источника при доступе по SNMP.

**Source Mask** (Маска источника): Маска IP-адресов источника при доступе по SNMP.

Пример использования через CLI:

```
snmp-server community v3 public 192.168.0.0 255.255.255.0
```

### 2.5.3.3 SNMPv3 User Configuration (Пользовательская настройка SNMPv3)

На этой странице можно настроить пользовательскую таблицу SNMPv3. Ключами списка являются идентификатор Engine ID и User Name (Имя пользователя).

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
<input type="checkbox"/>	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None

**Рис. 50. Вид меню Security – Switch – SNMP - SNMPv3 User**

**Engine ID:** строка октета, идентифицирующая engine ID, которому принадлежит этот элемент списка. Строка должна содержать четное число (в шестнадцатиричном 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** (Имя пользователя): строка, идентифицирующая имя пользователя, которому принадлежит данный параметр. Допустимая длина строки 1~32 символов ASCII с номерами в диапазоне от 0x21 до 0x7E.

**Security Level** (Уровень безопасности): 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): протокол аутентификации, которому принадлежит данный параметр. Возможны следующие протоколы аутентификации:

- None (Нет): протокол аутентификации отсутствует.
- 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** (Пароль аутентификации): 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): протокол конфиденциальности, которому принадлежит данный вход. Возможны следующие протоколы конфиденциальности:

- None (Нет): Протокол конфиденциальности отсутствует.
- DES: дополнительный флаг, указывающий, что пользователь использует протокол аутентификации DES.
- AES: дополнительный флаг, указывающий, что пользователь использует протокол аутентификации AES.

**Privacy Password** (Пароль конфиденциальности): строка, идентифицирующая фразу пароля конфиденциальности. Допустимая длина строки 8~32 символов ASCII с номерами в диапазоне от 0x21 до 0x7E.

Чтобы ввести новый элемент в список, нажмите кнопку “Add New Entry” (Добавить новый элемент). Чтобы удалить введенный элемент из списка, нажмите кнопку “Delete” (Удалить), либо установите флаг около нее, чтобы ранее сохраненный элемент был удален при следующем сохранении.

Нажмите кнопку “Save” (Сохранить), чтобы сохранить настройки или изменения.

Нажмите кнопку “Reset” (Переустановить), чтобы восстановить настройки, используемые по умолчанию.



### 2.5.3.4 SNMPv3 Group Configuration (Настройки группы SNMPv3)

На этой странице можно настроить таблицу группы SNMPv3. Ключами списка входов являются идентификатор Security Model (Модель безопасности) и Security Name (Безопасное имя).

Delete	Security Model	Security Name	Group Name
<input type="checkbox"/>	v1	public	default_ro_group
<input type="checkbox"/>	v1	private	default_rw_group
<input type="checkbox"/>	v2c	public	default_ro_group
<input type="checkbox"/>	v2c	private	default_rw_group
<input type="checkbox"/>	usm	default_user	default_rw_group

Add New Entry Save Reset

Рис. 51. Вид меню Security – Switch – SNMP - SNMPv3 Group

**Security Model** (Модель безопасности): 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** (Безопасное имя): 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** (Имя группы): строка, идентифицирующая имя группы, которому принадлежит данный параметр. Допустимая длина строки 1~32 символов ASCII с номерами в диапазоне от 0x21 до 0x7E.

### 2.5.3.5 SNMPv3 View Configuration (Настройка вида SNMPv3)

На этой странице можно настроить таблицу вида SNMPv3. Ключами списка являются идентификатор View Name (Имя вида) и OID Subtree (Поддерево OID).

Delete	View Name	View Type	OID Subtree
<input type="checkbox"/>	default_view	included	.1

Add New Entry Save Reset

Рис. 52. Вид меню Security – Switch – SNMP - SNMPv3 View

**View Name** (Имя вида): 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): 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** (Поддерево OID): 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 (\*).

### 2.5.3.6 SNMPv3 Access Configuration (Настройка доступа SNMPv3)

На этой странице можно настроить таблицу доступа SNMPv3. Ключами списка входов являются: Group Name (Имя группы), идентификатор Security Model (Модель безопасности) и Security Level (Уровень безопасности).

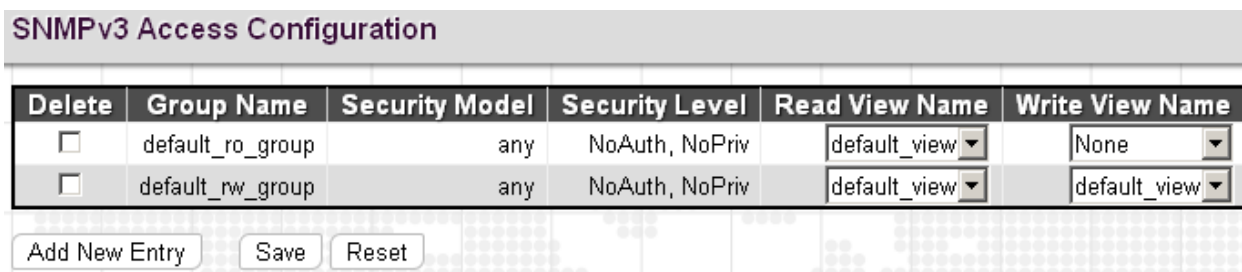


Рис. 53. Вид меню Security – Switch – SNMP - SNMPv3 Access

**Delete** (Удалить): Установите флаг в этом поле, чтобы удалить строку списка, в которой установлен флаг. Строка будет удалена при следующем сохранении.

**Group Name** (Имя группы): 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): 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): 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.

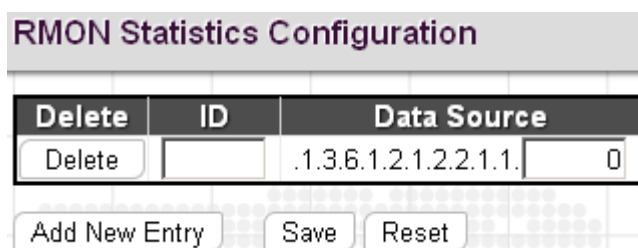
**Read View Name** (Имя вида при чтении): имя вида MIB, определяющего объекты MIB, для которых данный запрос может быть запросом текущих значений. Допустимая длина строки 1~32 символов ASCII с номерами в диапазоне от 0x21 до 0x7E.

**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.

## 2.5.4 RMON

### 2.5.4.1 RMON Statistics Configuration (Настройка статистик RMON)

На этой странице можно настроить таблицу статистик RMON. Ключ индекса входа – ID.



**Рис. 54. Вид меню Security – Switch – RMON - Statistics Configuration**

**Delete** (Удалить): Установите флаг в этом поле, чтобы удалить строку списка, в которой установлен флаг. Строка будет удалена при следующем сохранении.

**ID**: индекс входа. Допустимые значения — от 1 до 65535.

**Data Source** (Источник данных): ID порта, мониторинг которого требуется осуществлять.

### 2.5.4.2 RMON History Configuration (Настройка журнала RMON)

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.

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
Delete		.1.3.6.1.2.1.2.2.1.1.	0	1800	50

Buttons: Add New Entry, Save, Reset

**Рис. 55. Вид меню Security – Switch – RMON - History Configuration**

**ID**: индекс входа. Допустимые значения — от 1 до 65535.

**Data Source** (Источник данных): ID порта, мониторинг которого требуется осуществлять.

**Interval** (Интервал): интервал опроса. По умолчанию 1800 секунд. Диапазон допустимых значений: от 1 до 3600 секунд.

**Buckets** (Число сегментов): Число сегментов, требуемых для этого параметра. По умолчанию 50. Диапазон допустимых значений: от 1 до 3600.

**Buckets Granted** (Предполагаемое число сегментов): предполагаемое число сегментов.

Чтобы ввести новый элемент в список, нажмите кнопку “Add New Entry” (Добавить новый элемент). Чтобы удалить введенный элемент из списка, нажмите кнопку “Delete” (Удалить), либо установите флаг около нее, чтобы ранее сохраненный элемент был удален при следующем сохранении.

Нажмите кнопку “Save” (Сохранить), чтобы сохранить настройки или изменения. Нажмите кнопку “Reset” (Переустановить), чтобы восстановить настройки, используемые по умолчанию.

### 2.5.4.3 RMON Alarm Configuration (Настройка сигнализаций RMON)

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.

Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
Delete		30	.1.3.6.1.2.1.2.2.1.0.0	Delta	0	RisingOrFalling	0	0	0	0

Buttons: Add New Entry, Save, Reset

**Рис. 56. Вид меню Security – Switch – RMON - Alarm Configuration**

**ID**: индекс входа. Допустимые значения — от 1 до 65535.

**Interval** (Интервал): Интервал опроса при выборке и сравнении с нижним или верхним пороговым значением. Диапазон от 1 до 2^31 секунд.

**Variable** (Переменная): 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.

**Absolute** (Абсолютное значение): Переменная сравнивается с пороговыми значениями в конце периода выборки.

**Delta** (Изменение): Последняя выборка вычитается из текущего значения и разность сравнивается с пороговыми значениями.

**Value** (Значение): Статистическое значение в течение последнего периода выборки.

**Startup Alarm** (Сигнализация при пуске): Выбирает метод, который будет использоваться для выборки выбранной переменной и вычисления значения, которое сравнивается с пороговыми значениями.

**Rising or Falling** (Подъем или спад): Включает сигнализацию, когда значение первый раз превысит пороговое значение подъема либо станет меньше, чем пороговое значение спада.

**Rising** (Подъем): Включает сигнализацию, когда значение первый раз превысит пороговое значение подъема.

**Falling** (Спад): Включает сигнализацию, когда значение первый раз станет меньше, чем пороговое значение спада.

**Rising Threshold** (Пороговое значение подъема): Если текущее значение превышает пороговое значение подъема и, при этом, последнее значение выборки меньше этого порогового значения, то выдается сигнализация. После генерации события подъема, другое такое событие не будет сгенерировано до тех пор, пока значение выборки не станет меньше порогового значения подъема, достигнет порогового значения спада и снова вернется к пороговому значению подъема. Диапазон пороговых значений: от -2147483647 до 2147483647.

**Rising Index** (Индекс подъема): 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): индекс спада для события. Диапазон 1~65535.

Чтобы ввести новый элемент в список, нажмите кнопку “Add New Entry” (Добавить новый элемент). Чтобы удалить введенный элемент из списка, нажмите кнопку “Delete” (Удалить), либо установите флаг около нее, чтобы ранее сохраненный элемент был удален при следующем сохранении.

Нажмите кнопку “Save” (Сохранить), чтобы сохранить настройки или изменения. Нажмите кнопку “Reset” (Переустановить), чтобы восстановить настройки, используемые по умолчанию.

#### 2.5.4.4 RMON Event Configuration (Настройка событий RMON)

На странице RMON Event Configuration (Настройка событий RMON) можно задать операцию, которая выполняется при выдаче сигнализации.

Delete	ID	Desc	Type	Community	Event Last Time
<input type="checkbox"/>			none	public	0

Buttons: Add New Entry, Save, Reset

Рис. 57. Вид меню Security – Switch – RMON - Event Configuration

**Delete** (Удалить): Установите флаг в этом поле, чтобы удалить строку списка, в которой установлен флаг. Строка будет удалена при следующем сохранении.

**ID**: индекс ID. Диапазон 1~65535.

**Desc**: введите в это поле описание для данного входа.

**Type** (Тип): 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.

**Community:** Вместе с сообщением trap посылается строка community, подобная паролю. Хотя строку community можно задать и на этой странице, рекомендуется задать ее на странице SNMP trap configuration (Настройка сообщений SNMP trap) до ввода настроек на этой странице. Допускается использование символов 0~127.

**Event Last Time** (Время последнего события): Значение sysUpTime, когда событие для этого входа было сгенерировано последний раз.

## 2.5.4.5 RMON Statistics Overview (Обзор статистик RMON)

На странице RMON statistics overview отображается статистика интерфейса. Все отображаемые значения являются аккумулярованными за время, прошедшее с момента последней перезагрузки системы. Отображение значений выполняется в виде числа соответствующих событий в секунду. По умолчанию, система обновляет экран каждые 60 секунд.

ID	Data Source (ifindex)	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1588
No more entries																		

Рис. 58. Вид меню Security – Switch – RMON - Statistics Overview

**ID:** индекс ID.

**Data Source** (Источник данных): ID контролируемого порта.

**Drop** (Отброшенные пакеты): Общее число отброшенных пакетов из-за недостатка ресурсов.

**Octets** (Октеты): Общее число принятых октетов данных.

**Pkts**: Общее число принятых пакетов (включая плохие пакеты, широковещательные пакеты).

**Broadcast** (Широковещательные пакеты): Общее число хороших пакетов, которые были направлены на широковещательный адрес.

**Multicast** (Многоадресные пакеты): Общее число хороших пакетов, которые были направлены на многоадресный адрес.

**CRC Errors** (Пакеты с ошибками в контрольных суммах): Общее число принятых пакетов длиной от 64 до 1518 октетов (исключая служебные биты кадров, но включая октеты FCS).

**Undersize** (Пакеты недостаточной длины): Общее число принятых пакетов с длиной менее 64 октетов.

**Oversize** (Пакеты слишком большой длины): Общее число принятых пакетов с длиной более 1518 октетов.

**Frag.:** Число кадров размером менее 64 октетов, принятых с неправильной контрольной суммой CRC.

**Jabb.:** Число кадров размером более 64 октетов, принятых с неправильной контрольной суммой CRC.

**Coll.:** Наилучшая оценка общего числа столкновений на данном сегменте Ethernet.

**64 Bytes** (Пакеты длиной 64 байта): Общее число принятых пакетов длиной 64 байта (включая и плохие пакеты).

**X~Y** (65~127, 128~255, 256~511, 512~1023, 1024~1588): Общее число пакетов с длиной, находящейся в пределах от X до Y октетов.

## 2.5.4.6 History Overview (Обзор истории)

RMON History Overview														Auto-refresh <input type="checkbox"/>	Refre	
Start from Control Index <input type="text" value="0"/> and Sample Index <input type="text" value="0"/> with <input type="text" value="20"/> entries per page.																
History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization		
No more entries																

Рис. 59. Вид меню Security – Switch – RMON - History Overview

**History Index** (Индекс истории): Отображается индекс записи управления из истории.

**Sample Index** (Индекс выборки): Отображается индекс данных, ассоциированных с записью управления.

**Sample Start** (Начало выборки): Время, в которое была начата выборка (в секундах, прошедших с момента загрузки коммутатора).

**Drop** (Отброшенные пакеты): Общее число отброшенных пакетов из-за недостатка ресурсов.

**Octets** (Октеты): Общее число принятых октетов данных.

**Pkts**: Общее число принятых пакетов (включая плохие пакеты, широковещательные пакеты).

**Broadcast** (Широковещательные пакеты): Общее число хороших пакетов, которые были направлены на широковещательный адрес.

**Multicast** (Многоадресные пакеты): Общее число хороших пакетов, которые были направлены на многоадресный адрес.

**CRC Errors** (Пакеты с ошибками в контрольных суммах): Общее число принятых пакетов длиной от 64 до 1518 октетов (исключая служебные биты кадров, но включая октеты FCS).

**Undersize** (Пакеты недостаточной длины): Общее число принятых пакетов с длиной менее 64 октетов.

**Over-size** (Пакеты слишком большой длины): Общее число принятых пакетов с длиной более 1518 октетов.

**Frag.**: Число кадров размером менее 64 октетов, принятых с неправильной контрольной суммой CRC.

**Jabb.**: Число кадров размером более 64 октетов, принятых с неправильной контрольной суммой CRC.

**Coll.**: Наилучшая оценка общего числа столкновений на данном сегменте Ethernet.

**Utilization** (Использование): Наилучшая оценка использования средств физического уровня сети на данном интерфейсе в течение интервала выборки, измеренная до сотых долей процента.

## 2.5.4.7 Alarm Overview (Обзор сигнализаций)

RMON Alarm Overview									
Start from Control Index <input type="text" value="0"/> with <input type="text" value="20"/> entries per page.									
ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
No more entries									

Рис. 60. Вид меню Security – Switch – RMON - Alarm Overview

**ID**: индекс управления сигнализацией.

**Interval** (Интервал): Интервал опроса при выборке (в секундах) и сравнение с пороговыми значениями подъема и спада.

**Variable** (Переменная): Объект MIB, который используется для выборки.

**Sample Type** (Тип выборки): Метод выборки выбранной переменной и вычисления значения, сравниваемого с пороговыми значениями.

**Value** (Значение): Статистическое значение в течение последнего периода выборки.

**Startup Alarm** (Сигнализация при пуске): Сигнализация, которая может быть выдана, если этот вход вначале установлен, как правильный.

**Rising Threshold** (Пороговое значение подъема): Если текущее значение станет больше порогового значения подъема и, при этом, последнее значение выборки было меньше этого порогового значения, то будет выдана сигнализация.

**Rising Index** (Индекс подъема): Индекс события, используемого, когда выдана сигнализация вследствие того, что значение переменной превысило пороговое значение подъема.

**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.

**Falling Index** (Индекс спада): Индекс события, используемого, когда выдана сигнализация вследствие того, что значение переменной стало меньше порогового значения спада.

## 2.5.4.8 Event Overview (Обзор события)

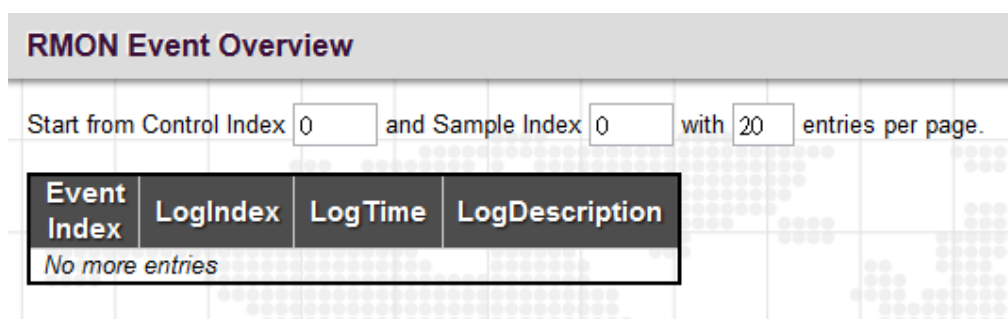


Рис. 61. Вид меню Security – Switch – RMON - Event Overview

**Event Index** (Индекс события): Отображается индекс записи события.

**Log Index** (Индекс журнала): Отображается индекс записи в журнале.

**Log Time** (Время регистрации в журнале): Отображается время регистрации события в журнале.

**Log Description** (Описание в журнале): Отображается описание события.

## 2.6 Network (Сеть)

### 2.6.1 Port Security (Безопасность 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.

## 2.6.1.1 Limit Control (Управление безопасности порта)

**System Configuration**

Mode	Enabled
Aging Enabled	<input checked="" type="checkbox"/>
Aging Period	600 seconds

**Port Configuration**

Port	Mode	Limit	Action	State	Re-open
*	<>	2	<>		
1	Enabled	2	Trap & Shutdown	Ready	Reopen
2	Disabled	4	None	Disabled	Reopen
3	Disabled	4	None	Disabled	Reopen
4	Disabled	4	None	Disabled	Reopen
5	Disabled	4	None	Disabled	Reopen
6	Disabled	4	None	Disabled	Reopen
7	Disabled	4	None	Disabled	Reopen
8	Disabled	4	None	Disabled	Reopen
9	Disabled	4	None	Disabled	Reopen
10	Disabled	4	None	Disabled	Reopen
11	Disabled	4	None	Disabled	Reopen
12	Disabled	4	None	Disabled	Reopen
13	Disabled	4	None	Disabled	Reopen
14	Disabled	4	None	Disabled	Reopen
15	Disabled	4	None	Disabled	Reopen
16	Disabled	4	None	Disabled	Reopen
17	Disabled	4	None	Disabled	Reopen
18	Disabled	4	None	Disabled	Reopen
19	Disabled	4	None	Disabled	Reopen
20	Disabled	4	None	Disabled	Reopen

Рис. 62. Вид меню Security – Network - Port Security - Limit Control

### System Configuration (Настройка системы)

**Mode** (Режим работы): Включает или отключает (глобально) управление ограничением устройств, находящихся за одним портом. Если управление выключено (глобально), то другие модули могут продолжать использовать доступный им функционал, но проверка ограничения и соответствующие операции отключены.

**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** (Срок устаревания): 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.

### Port Configuration (Настройка порта)

**Port** (Порт): Отображается номер порта. Правила "Port \*" означают применение ко всем портам.

**Mode** (Режим работы): 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** (Предел): Максимальное число MAC-адресов, которые могут оставаться безопасными на этом порту. Это число не может превышать 1024. Если этот предел превышен, выполняется соответствующая операция.



**Action** (Операция): Если предел превышен, выполняется выбранная операция:

- None (Нет): Доступ к порту может получить только количество MAC-адресов, не превышающее установленного предела. Никаких операций не выполняется.
- Trap (Сообщение): Если число появившихся на порту MAC-адресов превысит указанный предел, то будет отправлено сообщение SNMP trap. Если устаревание (Aging) выключено, то будет отправлено только одно сообщение SNMP trap. Если устаревание включено, то новые сообщения SNMP trap будут отправляться всякий раз, когда будет превышать установленный предел.
- Shutdown (Отключение порта): Если число появившихся на порту MAC-адресов превысит предел, то порт будет выключен. Это приведет к тому, что все безопасные MAC-адреса будут удалены с порта, а новые MAC-адреса не будут получены обучением. Порт будет оставаться отключенным даже в том случае, если линия будет физически отсоединена от порта, а затем присоединена к нему снова (путем отсоединения / присоединения кабеля). Существует три способа переоткрыть порт:
  - Перезагрузить коммутатор;
  - Выключить и снова включить функцию Limit Control (Управление пределом безопасности) на порту или на коммутаторе;
  - Нажать кнопку "Reopen" (Переоткрыть).
- Trap & Shutdown (Сообщение и отключение): Если число появившихся на порту MAC-адресов превысит предел, то будут выполнены обе операции - "Trap" (Сообщение) и "Shutdown" (Отключение порта), рассмотренные выше.

**State** (Состояние): Отображается текущее состояние порта с точки зрения управления ограничением количества хостов порта. Отображаемое сообщение может быть одним из следующих:

- Disabled (Выключен): Предел выключен (либо глобально, либо на порту).
- Ready (Готов): Предел не достигнут.
- Limit Reached (Предел достигнут): На порту достигнут предел. Это состояние может появиться только в том случае, если для Action (Операция) задано значение None (Нет) или Trap (сообщение).
- Shutdown (Отключение порта): Порт отключен модулем управления пределом безопасности. Это состояние может появиться только в том случае, если для Action (Операция) задано значение Shutdown (Отключение) или Trap & Shutdown (Сообщение и отключение).

**Re-open Button** (Кнопка переоткрытия порта): Если порт отключен данным модулем, можно переоткрыть его, нажав на эту кнопку, которая будет работоспособной только тогда, когда переоткрыть порт возможно. О других способах см. Shutdown (Отключение порта) в разделе Action (Операция). Имейте в виду, что при нажатии на кнопку Reopen (переоткрыть порт), страница будет обновлена, так что все не подтвержденные изменения будут потеряны.

Пример использования через CLI:

```
port-security aging
port-security aging time 600
port-security
!
interface FastEthernet 1/1
port-security
port-security maximum 2
port-security violation trap-shutdown
```

## 2.6.1.2 Switch Status (Состояние коммутатора)

Port Security Switch Status				
User Module Legend				
User Module Name	Abbr			
Limit Control	L			
802.1X	8			
Port Status				
Port	Users	State	MAC Count	
			Current	Limit
1	L-	Ready	0	2
2	--	Disabled	-	-
3	--	Disabled	-	-
4	--	Disabled	-	-
5	--	Disabled	-	-
6	--	Disabled	-	-
7	--	Disabled	-	-
8	--	Disabled	-	-
9	--	Disabled	-	-
10	--	Disabled	-	-
11	--	Disabled	-	-
12	--	Disabled	-	-
13	--	Disabled	-	-
14	--	Disabled	-	-
15	--	Disabled	-	-
16	--	Disabled	-	-
17	--	Disabled	-	-
18	--	Disabled	-	-
19	--	Disabled	-	-
20	--	Disabled	-	-

Рис. 63. Вид меню Security – Network - Port Security - Switch Status

**User Module Legend** (Условные обозначения пользовательского модуля)

**User Module Name** (Имя модуля пользователя): Полное имя модуля, которое может быть запрошено службами безопасности порта.

**Abbr**: В данном столбце приведено сокращенное имя модуля пользователя, которое используется в столбце “Users” (Пользователи) таблицы “Port Status” (Состояние порта).

**Port Status** (Состояние порта)

**Port** (Порт): Номер порта. Чтобы просмотреть состояние порта нажмите мышью на его номер в таблице.

**Users** (Пользователи): Каждому модулю пользователя отведен свой столбец, показывающий, включена ли служба безопасности порта в этом модуле или нет. Знак '-' означает, что соответствующий модуль не включен. Буква в этом поле означает, что в модуле, сокращенное имя которого является этой буквой, включена служба безопасности порта.

**State** (Состояние): Отображается текущее состояние порта. Оно может быть одним из следующих состояний:

- Disabled (Выключен): Модули пользователя, в настоящее время использующие службу безопасности порта, отсутствуют.
- Ready (Готов): Служба безопасности порта используется по крайней мере одним модулем; ожидается получение кадров с неизвестных MAC-адресов.
- Limit Reached (Предел достигнут): Служба безопасности порта включена, по крайней мере, в одном модуле; для этого модуля индицируется, что предел безопасности достигнут и больше MAC-адреса набираться не будут.

- Shutdown (Отключение порта): Служба безопасности порта включена, если присутствует хотя бы один пользовательский модуль управления пределом безопасности и этот модуль указывает, что предел превышен. Порт невозможно будет обучить MAC-адресам до тех пор, пока он не будет переоткрыт администратором на странице настройки предела безопасности.

**MAC Count (Current/Limit)** (Счетчик MAC-адресов (Текущее значение//Предел безопасности)): В двух столбцах указано число MAC-адресов, которым обучен порт (адресов, по которым производится передача данных и заблокированных) и максимальное число MAC-адресов, которым может быть обучен порт. Если на порту нет включенных модулей пользователя, в текущем столбце будет отображено тире (-). Если на порту нет включенных модулей пользователя, в столбце Limit (Предел безопасности) будет отображено тире (-).

Пример использования через CLI:

```
ZES-2220S# show port-security switch
Users:
L = Limit Control
8 = 802.1X
Interface          Users  State          MAC Cnt
-----
FastEthernet 1/1      L-    Ready          0
FastEthernet 1/2      --    No users       0
FastEthernet 1/3      --    No users       0
FastEthernet 1/4      --    No users       0
FastEthernet 1/5      --    No users       0
FastEthernet 1/6      --    No users       0
FastEthernet 1/7      --    No users       0
FastEthernet 1/8      --    No users       0
FastEthernet 1/9      --    No users       0
FastEthernet 1/10     --    No users       0
FastEthernet 1/11     --    No users       0
FastEthernet 1/12     --    No users       0
FastEthernet 1/13     --    No users       0
FastEthernet 1/14     --    No users       0
FastEthernet 1/15     --    No users       0
FastEthernet 1/16     --    No users       0
GigabitEthernet 1/1  --    No users       0
GigabitEthernet 1/2  --    No users       0
GigabitEthernet 1/3  --    No users       0
GigabitEthernet 1/4  --    No users       0
```

### 2.6.1.3 Port Statistics (Статистика порта)

На этой странице отображаются MAC-адреса, полученные обучением на данном порту.

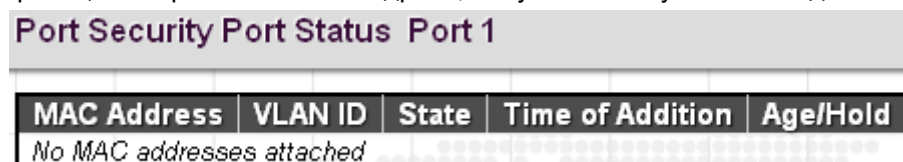


Рис. 64. Вид меню Security – Network - Port Security - Port Statistics

**MAC Address** (MAC-адрес): Когда функция “Port Security Limit Control” включена глобально и на порту, здесь отображаются MAC-адреса, полученные обучением на данном порту.

**VLAN ID**: Отображается номер VLAN ID, который виден на данном порту.

**State** (Состояние): В этом столбце отображается, осуществляется передача данных по этому MAC-адресу или он заблокирован. В заблокированном состоянии прием и передача трафика на MAC-адрес невозможны.

**Time of Addition** (Время дополнения): Отображается дата и время, в которые данный MAC-адрес был виден на порту.

**Age/Hold** (Возраст/срок удерживания): Если хотя бы один модуль пользователя решит заблокировать данный MAC-адрес, то этот MAC-адрес будет оставаться в заблокированном состоянии до истечения времени удерживания (измеряемого в секундах). Если все модули пользователей решат разрешить передачу данных на этот MAC-адрес и включено устаревание адресов, модуль безопасности порта будет периодически проверять, передается ли трафик на этот MAC-адрес. Если срок устаревания (измеряемый в секундах) истек и кадров больше не наблюдается, MAC-адрес будет удален из таблицы MAC-адресов. В противном случае, начнется новый срок устаревания. Если устаревание выключено либо модуль пользователя решил удерживать MAC-адрес неограниченное время, то в столбце будет отображено тире (-).

## 2.6.2 NAS

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 для глобально либо для каждого порта отдельно. Чтобы сконфигурировать сервер базы данных, пожалуйста, перейдите на страницу настройки RADIUS.

### 2.6.2.1 Configuration (Настройка)

Network Access Server Configuration

System Configuration

Mode	Enabled
Reauthentication Enabled	<input checked="" type="checkbox"/>
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds
RADIUS-Assigned QoS Enabled	<input type="checkbox"/>
RADIUS-Assigned VLAN Enabled	<input type="checkbox"/>
Guest VLAN Enabled	<input type="checkbox"/>
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	<input type="checkbox"/>

Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart
*	<>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
1	Port-based 802.1X	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate Reinitialize
2	MAC-based Auth.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate Reinitialize
3	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate Reinitialize
4	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate Reinitialize
5	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Authorized	Reauthenticate Reinitialize
6	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate Reinitialize
7	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate Reinitialize
8	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate Reinitialize

Рис. 65. Вид меню Security – Network – NAS - Configuration

#### System Configuration (Настройка системы)

**Mode** (Режим работы): 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** (Включить повторную аутентификацию): 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 повторной аутентификации): 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** (Таймер EAPOL): 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** (Срок устаревания): 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 удерживания): 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** (Включить QoS, назначаемый Radius): Установите флаг в этом поле, чтобы глобально включить QoS, назначаемый RADIUS.

**Radius-Assigned VLAN Enabled** (Включить VLAN, назначаемый Radius): 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 "Radius-Assigned 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** (Включить гостевую VLAN): 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 гостевой VLAN): 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** (Порт): Номер порта. Правила "Port \*" означают применение ко всем портам.

**Admin State** (Административное состояние): Выбирает режим аутентификации порта. Данная настройка работает только в том случае, когда глобально включен NAS. Поддерживаются следующие режимы работы:

- **Force Authorized** (Принудительная авторизация): 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** (Принудительная неавторизация): В этом режиме работы коммутатор отправит один кадр отказа (аутентификации) EAPOL, если 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, аутентифицироваться 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 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 шестнадцатичными цифрами (записанными символами нижнего регистра).

Коммутатор поддерживает только метод аутентификации MD5-Challenge, поэтому RADIUS-сервер должен быть соответствующим образом сконфигурирован.

**Radius-Assigned QoS Enabled** (Включение QoS, назначаемый Radius): Установите флаг в этом поле, чтобы включить RADIUS-Assigned QoS на порту.

**Radius-Assigned VLAN Enabled** (Включение VLAN, назначаемый Radius): Установите флаг в этом поле, чтобы включить RADIUS-Assigned VLAN на порту.

**Guest VLAN Enabled** (Включить гостевую VLAN): Установите флаг в этом поле, чтобы включить гостевую VLAN на порту.

**Port State** (Состояние порта): 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 unsuccessful.
- 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** (Перезапуск): 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): Расписание повторной аутентификации 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 неавторизованы.

**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.

Пример использования через CLI:

```
dot1x re-authentication
dot1x system-auth-control
!
interface FastEthernet 1/1
  dot1x port-control auto
!
interface FastEthernet 1/2
  dot1x port-control mac-based
```

### 2.6.2.2 Switch Status (Состояние коммутатора)

Network Access Server Switch Status						
Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Port-based 802.1X	Link Down			-	
2	MAC-based Auth.	Link Down			-	
3	Force Authorized	Link Down			-	
4	Force Authorized	Link Down			-	
5	Force Authorized	Authorized			-	
6	Force Authorized	Link Down			-	
7	Force Authorized	Link Down			-	
8	Force Authorized	Link Down			-	
9	Force Authorized	Link Down			-	
10	Force Authorized	Link Down			-	
11	Force Authorized	Link Down			-	
12	Force Authorized	Link Down			-	
13	Force Authorized	Link Down			-	
14	Force Authorized	Link Down			-	
15	Force Authorized	Link Down			-	
16	Force Authorized	Link Down			-	
17	Force Authorized	Link Down			-	
18	Force Authorized	Link Down			-	
19	Force Authorized	Link Down			-	
20	Force Authorized	Link Down			-	

Рис. 66. Вид меню Security – Network – NAS - Switch Status

**Port** (Порт): Номер порта. Для просмотра детальной статистики NAS нажмите мышью на номер порта.

**Admin State** (Административное состояние): Отображается административное состояние порта.

**Port Status** (Состояние порта): Отображается состояние порта.

**Last Source** (Последний источник): источник MAC-адресов, содержащийся в самом последнем принятом кадре EAPOL при аутентификации на основе EAPOL.

**Last ID** (Последний ID клиентского устройства): имя пользователя (идентификатор клиентского устройства), содержащийся в самом последнем принятом кадре EAPOL при аутентификации на основе EAPOL.

**QoS Class** (Класс QoS): Отображается класс QoS, который NAS присвоил порту. Если QoS не установлено сервером NAS, то это поле будет пустым.

**Port VLAN ID** (VLAN-ID порта): Номер VLAN ID порта, присвоенный сервером NAS. Если VLAN ID не установлен сервером NAS, то это поле будет пустым.

Пример использования через CLI:

```
ZES-2220S# show dot1x status brief
```

Inf	Admin	Port	State	Last Src	Last ID	QoS	VLAN	Guest
Fa 1/1	Port	Down	-	-	-	-	-	-
Fa 1/2	MAC	Down	-	-	-	-	-	-
Fa 1/3	Auth	Down	-	-	-	-	-	-
Fa 1/4	Auth	Down	-	-	-	-	-	-
Fa 1/5	Auth	Auth	-	-	-	-	-	-
Fa 1/6	Auth	Down	-	-	-	-	-	-
Fa 1/7	Auth	Down	-	-	-	-	-	-
Fa 1/8	Auth	Down	-	-	-	-	-	-
Gi 1/1	Auth	Down	-	-	-	-	-	-
Gi 1/2	Auth	Down	-	-	-	-	-	-
Gi 1/3	Auth	Down	-	-	-	-	-	-
Gi 1/4	Auth	Down	-	-	-	-	-	-

### 2.6.2.3 Port Statistics (Статистика порта)

**NAS Statistics Port 5** Port 5

**Port State**

<b>Admin State</b>	Force Authorized
<b>Port State</b>	Authorized

**Port Counters**

Receive EAPOL Counters		Transmit EAPOL Counters	
Total	0	Total	1
Response ID	0	Request ID	0
Responses	0	Requests	0
Start	0		
Logoff	0		
Invalid Type	0		
Invalid Length	0		

Рис. 67. Вид меню Security – Network – NAS - Port Statistics

**Port State** (Состояние порта)



**Admin State** (Административное состояние): Отображается текущее административное состояние порта.

**Port Status** (Состояние порта): Отображается состояние порта.

#### Receive EAPOL Counters (Счетчики принятых кадров EAPOL)

**Total** (Всего кадров): Число правильных кадров EAPOL любого типа, которые были приняты коммутатором.

**Response ID** (Ответные кадры идентификации): Число правильных кадров EAPOL с ответами идентификации, которые были приняты коммутатором.

**Responses** (Ответные кадры): Число правильных ответных кадров EAPOL (отличающихся от кадров с ответами идентификации), которые были приняты коммутатором.

**Start** (Старт): Число стартовых кадров EAPOL, которые были приняты коммутатором.

**Logoff** (Отключение): Число правильных кадров отключения EAPOL, которые были приняты коммутатором.

**Invalid Type** (Неправильного типа): Число кадров EAPOL, которые были приняты коммутатором, в которых тип кадра не распознан.

**Invalid Length** (Неправильная длина): Число кадров EAPOL, которые были приняты коммутатором, в которых неправильно поле Packet Body Length (Длина тела пакета).

#### Transmit EAPOL Counters (Счетчики переданных кадров EAPOL)

**Total** (Всего): Число кадров EAPOL любого типа, которые были переданы коммутатором.

**Request ID** (ID запроса): Число правильных кадров EAPOL с запросами идентификации, которые были приняты коммутатором.

**Requests** (Запросы): Число правильных запросных кадров EAPOL (отличающихся от кадров с запросами идентификации), которые были приняты коммутатором.

## 2.6.3 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.

### 2.6.3.1 Ports (Порты)

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	0
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

Рис. 68. Вид меню Security – Network – ACL – Ports

**Port** (Порт): Номер порта.

**Policy ID** (Идентификатор правила): 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** (Операция): Разрешает или запрещает кадр на основе того, согласуется ли он с правилом из присвоенной группы правил.

**Rate Limiter ID** (Идентификатор ограничителя скорости): Выбирает идентификатор ограничителя скорости, применяемого к порту. Правило ограничителя скорости может быть задано на странице настройки "Rate Limiters" (Ограничители скорости).

**Port Redirect** (Перенаправление порта): Выбор порта, на который перенаправляются согласующиеся кадры.

**Mirror** (Зеркало): 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** (Регистрация в системном журнале): 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** (Отключение порта): Это поле позволяет задать, следует ли отключать порт, когда согласующиеся кадры появляются на порту.

**State** (Состояние): Выбор состояния порта^

- Enabled (Включить): позволяет переоткрыть порт.
- Disabled (Выключить): позволяет закрыть порт.

**Counters** (Счетчики): Число кадров, которые согласуются с правилами, определенными в выбранной группе правил.

### 2.6.3.2 Rate Limiters (Ограничители скорости)

ACL Rate Limiter Configuration		
Rate Limiter ID	Rate	Unit
*	1000	<>
1	1000	kbps
2	500	kbps
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. 69. Вид меню Security – Network – ACL – Rate Limiters

**Rate Limiter ID** (Идентификатор ограничителя скорости): Отображается идентификатор каждого ограничителя скорости.

**Rate** (Скорость): 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** (Единицы измерения): выбор единиц измерения скорости.

Пример использования через CLI:

```
access-list rate-limiter 1 100kbps 10
access-list rate-limiter 2 100kbps 5
```

### 2.6.3.3 Access Control List (Список доступа)

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									Auto-refresh <input type="checkbox"/>	Refresh
ACE	Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter		
1	2	Any	Any	Permit	1	Disabled	Disabled	0	⊕ ⊖ ⊗ ⊘ ⊙	

Рис. 70. Вид меню Security – Network – ACL – Configuration

**Ingress Port** (Входящий порт): Входящий порт элемента списка доступа. Выберите “All” (Все), чтобы применить (список доступа) ко всем портам либо выбрать определенный порт.

**Policy Bitmask** (Маска битов политики): Номер политики и маска битов ACE.

**Frame Type** (Тип кадра): Тип кадра, согласующегося с этим правилом.

**Action** (Операция): Отображается тип операции - permit (разрешить) либо deny (запретить).

**Rate Limiter** (Ограничитель скорости): Отображается, включен или выключен ограничитель скорости, когда найдены согласующиеся кадры.

**Port Redirect** (Перенаправление порта): в этом поле отображается, включено или выключено перенаправление порта.

**Mirror** (Зеркало): в этом поле отображается, включена или выключена функция зеркала.

**Counter** (Счетчик): 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 плюса.

The screenshot shows the 'ACE Configuration' interface. It is divided into several sections:

- ACE Configuration:** Contains dropdown menus for 'Ingress Port' (set to 'Port 2'), 'Policy Filter' (set to 'Any'), and 'Frame Type' (set to 'Ethernet Type'). To the right, a table of actions is shown: 'Action' (Permit), 'Rate Limiter' (1), 'Mirror' (Disabled), 'Logging' (Enabled), 'Shutdown' (Disabled), and 'Counter' (0).
- MAC Parameters:** Contains dropdown menus for 'SMAC Filter' and 'DMAC Filter', both set to 'Any'.
- VLAN Parameters:** Contains dropdown menus for '802.1Q Tagged' (Any), 'VLAN ID Filter' (Specific), 'VLAN ID' (10), and 'Tag Priority' (Any).
- Ethernet Type Parameters:** Contains a dropdown menu for 'EtherType Filter' set to 'Any'.

At the bottom, there are 'Save', 'Reset', and 'Cancel' buttons.

Рис. 71. Вид меню Security – Network – ACL – ACE

### ACE Configuration (Настройка ACE)

**Ingress Port** (Входящий порт): Выберите входящий порт для элемента списка доступа. Выберите "All" (Все), чтобы применить правило список доступа ко всем портам либо выбрать определенный порт.

**Policy Filter** (Политики): выбор типа фильтра политики. "Any" (Любой) означает, что этому правилу не присвоено фильтра политики. Выберите "Specific" (Специальный), чтобы отфильтровать конкретную политику по данному ACE.

**Frame Type** (Тип кадра): Выберите согласующийся тип кадра. Доступны следующие типы кадров: Any (Любой), Ethernet, ARP, IPv4. По умолчанию можно использовать любой тип кадра.

**Action** (Операция): Выберите тип операции - permit (разрешить) либо deny (запретить).

**Rate Limiter** (Ограничитель скорости): позволяет включить или выключить ограничитель скорости, когда найдены согласующиеся кадры.

**Mirror** (Зеркало): позволяет включить или выключить функцию зеркала.

**Logging** (Регистрация в системном журнале): позволяет включить или выключить регистрацию в системном журнале для согласующихся кадров.

**Shutdown** (Отключение порта): позволяет включить или выключить отключение порта для согласующихся кадров.

**Counter** (Счетчик): в этом поле отображается число кадров, согласующихся с какими-либо правилами, определенными для этого списка доступа.

### VLAN Parameters (Параметры VLAN)

**802.1Q Tagged** (802.1Q с тегированием): позволяет выбрать, должны ли кадры содержать теги (то есть быть тегируемыми).

**VLAN ID Filter** (Фильтр VLAN ID): 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** (Приоритет тега): позволяет выбрать значение User Priority (Приоритет пользователя), найденного в теге VLAN для согласования с данным правилом.

**MAC Parameter** (MAC-параметр)

**SMAC Filter** (Фильтр SMAC): MAC-адрес источника. Выберите "Any" (Любой), чтобы разрешить любые MAC-адреса источника либо выберите "Specific" (Специальные), чтобы определить MAC-адрес источника. (Это поле присутствует только для типов кадров Any (Любой) и Ethernet.

**DMAC Filter** (Фильтр DMAC): MAC-адрес назначения.

- Any (Любой): разрешает все MAC-адреса назначения.
- MC: многоадресный MAC-адрес.
- BC: широковещательный MAC-адрес.
- UC: одноадресный MAC-адрес.
- Specific (Специальный): используйте эту опцию, чтобы задать MAC-адреса по своему усмотрению. (Это поле присутствует только для типа кадров Ethernet.)

**Ethernet Type Parameter** (Параметр типа Ethernet )

**EtherType Filter** (Фильтр типа Ether): Данная опция может использоваться только для фильтрации пакетов формата Ethernet II. Для определения значения EtherType (Тип Ether) выберите "Specific" (Специальный).

**ARP Parameter** (Параметр ARP)

**ARP/RARP**: тип пакета ARP.

- Any (Любой): флаг кода операции ARP/RARP не задан.
- ARP: код операции ARP/RARP для кадра должен быть установлен на ARP.
- RARP: код операции ARP/RARP для кадра должен быть установлен на RARP.
- Other (Другие): кадр имеет флаг неизвестного кода операции ARP/RARP.

**Request/Reply** (Запрос/Ответ): задает, является пакет запросом ARP, ответом ARP или любого типа.

- Any (Любой): флаг кода операции ARP/RARP не задан.
- Request (запрос): кадр должен иметь установленный флаг кода операции ARP Request (запрос ARP) или RARP Request (Запрос RARP).
- Reply (Ответ): Кадр должен иметь установленный флаг кода операции ARP Reply (Ответ ARP) или RARP Request (Ответ RARP).

**Sender IP Filter** (Фильтр IP-адреса отправителя): здесь можно задать IP-адрес отправителя.

- Any (Любой): фильтр IP-адреса отправителя не задан.
- Host (Хост): здесь можно задать IP-адрес отправителя.
- Network (Сеть): здесь можно задать IP-адрес отправителя и IP-маску отправителя.

**Target IP Filter** (Фильтр целевого IP-адреса): здесь можно задать IP-адрес назначения.

- Any (Любой): фильтр целевого IP-адреса не задан.
- Host (Хост): здесь можно задать целевой IP-адрес.
- Network (Сеть): здесь можно задать целевой IP-адрес и IP-маску целевых адресов.

**ARP Sender SMAC Match** (Согласование SMAC-адреса отправителя с ARP): Выберите 0, чтобы указать, что содержимое поля SHA (Sender Hardware Address – аппаратный адрес отправителя) в кадре ARP/RARP не равно MAC-адресу источника. Выберите 1, чтобы указать, что содержимое поля SHA в кадре ARP/RARP равно MAC-адресу источника. Выберите "Any" (Любой), чтобы указать любой из вышеописанных случаев.

### **RARP Target MAC Match** (Согласование MAC-адреса с целевым адресом RARP):

Выберите 0, чтобы указать, что содержимое поля THA (Target Hardware Address – аппаратный целевой адрес) в кадре ARP/RARP не равно MAC-адресу источника. Выберите 1, чтобы указать, что содержимое поля THA в кадре ARP/RARP равно MAC-адресу источника. Выберите “Any” (Любой), чтобы указать любой из вышеописанных случаев.

**IP/Ethernet Length** (Длина IP-адресов/Ethernet): Выберите 0, чтобы указать, что содержимое поля HLN (Hardware Address Length – длина аппаратного адреса) в кадре ARP/RARP не равно Ethernet (0x6) и содержимое поля Protocol Address Length (Длина адреса протокола) не равно IPv4 (0x4). Выберите 1, чтобы указать, что содержимое поля HLN в кадре ARP/RARP равно Ethernet (0x6) и содержимое поля Protocol Address Length (Длина адреса протокола) равно IPv4 (0x4). Выберите “Any” (Любой), чтобы указать любой из вышеописанных случаев.

**IP:** Выберите 0, чтобы указать, что содержимое поля Protocol Address Space (Пространство адресов протокола) в кадре ARP/RARP не равно IP (0x800). Выберите 1, чтобы указать, что содержимое поля Protocol Address Space (Пространство адресов протокола) равно IP (0x800). Выберите “Any” (Любой), чтобы указать любой из вышеописанных случаев.

**Ethernet:** Выберите 0, чтобы указать, что содержимое поля Hardware Address Space (Пространство аппаратных адресов протокола) в кадре ARP/RARP не равно Ethernet (1). Выберите 1, чтобы указать, что содержимое поля Hardware Address Space (Пространство адресов протокола) равно Ethernet (1). Выберите “Any” (Любой), чтобы указать любой из вышеописанных случаев.

### **IP Parameters** (Параметры протокола IP)

**IP Protocol Filter** (Фильтр протокола IP): Для выбора фильтрации протокола IP из раскрывающегося меню выберите протокол, возможные варианты: “Any” (Любой), “ICMP”, “UDP”, “TCP” или “Other” (Другой).

**IP TTL:** Выберите “Zero” (Ноль), чтобы указать, что поле TTL в заголовке IPv4 равно 0. Если значение в поле TTL не равно 0, укажите “Non-Zero” (не ноль). Если значение поля не важно, выберите “any” (любое значение).

**IP Fragment** (Фрагмент IP): Чтобы разрешить любые значения, выберите “Any” (Любые значения). “Yes” (Да) означает, что имеются кадры IPv4, в которых установлен бит MF, либо поле FRAG OFFSET больше 0 и должно совпадать с этим элементом. “No” (Нет) означает, что имеются кадры IPv4, в которых установлен бит MF, либо поле FRAG OFFSET больше 0 и должно не совпадать с этим элементом.

**IP Option** (Опция протокола IP): Задайте флаг опций для данного правила.

Чтобы разрешить любые значения, выберите “Any” (Любые значения). “Yes” (Да) означает, что имеются кадры IPv4 с установленным флагом опций, который должен совпадать с этим элементом списка. “No” (Нет) означает, что имеются кадры IPv4 с установленным флагом опций, который должен не совпадать с этим элементом списка.

**SIP Filter** (Фильтр SIP): Выберите один из вариантов фильтрации IP-адресов источника: “Any” (Любой), “Host” (Хост) или “Network” (Сеть). Если выбран вариант “Host” (Хост), необходимо указать IP-адрес конкретного хоста. Если выбран вариант “Network” (Сеть), необходимо указать и сетевой адрес, и маску подсети.

**SIP Address** (Адрес SIP): Задайте IP-адрес источника.

**SIP Mask** (Маска SIP): Задайте маску подсети источника.

**DIP Filter** (Фильтр DIP): Выберите один из вариантов фильтрации IP-адресов назначения: “Any” (Любой), “Host” (Хост) или “Network” (Сеть). Если выбран вариант “Host” (Хост), необходимо указать IP-адрес конкретного хоста. Если выбран вариант “Network” (Сеть), необходимо указать и сетевой адрес, и маску подсети.

**DIP Address** (Адрес DIP): Задайте IP-адрес назначения.

**DIP Mask** (Маска DIP): Задайте маску подсети назначения.

### **IPv6 Parameters** (Параметры IPv6)

**Next Header Filter** (Фильтр следующего заголовка): Выберите вариант фильтра следующего заголовка. Доступны следующие варианты: ICMP, UDP, TCP, Other (Другой протокол).

**SIP Filter** (Фильтр SIP): Выберите фильтр IP-адресов источника. “Any” (Любой) означает, что допустим любой SIP-фильтр. Выберите “Specific” (Специальный), чтобы задать фильтр SIP по своему усмотрению.

**Hop Limit** (Макс. число хопов между маршрутизаторами): Чтобы разрешить любые значения, выберите "Any" (Любые значения). Выберите 0, если любые кадры IPv6, у которых поле hop limit больше нуля не должны согласовываться с этим элементом списка. Выберите 1, если любые кадры IPv6, у которых поле hop limit больше нуля должны согласовываться с этим элементом списка.

Пример использования через CLI:

```
access-list ace 1 ingress interface FastEthernet 1/2 vid 10 rate-limiter 1 logging
```

### 2.6.3.4 ACL Status (Состояние списка доступа)

ACL Status								
User	ACE	Frame Type	Action	Rate Limiter	Mirror	CPU	Counter	Conflict
Static	1	Any	Permit	1	Disabled	No	0	No

Рис. 72. Вид меню Security – Network – ACL – Status

На этой странице представлено состояние ACL для различных пользователей ACL. В каждой строке описан ACE, который был определен. Если конкретный ACE неприменим к аппаратным средствам из-за ограничений аппаратуры, то возникает конфликт. Для каждого коммутатора общее число ACE составляет 256.

**User** (Пользователь/Модуль): Выводит на дисплей информацию о модуле ACL.

**Ingress Port** (Входящий порт): Отображается входящий порт ACE. В этом поле могут быть указаны все порты, конкретный порт или диапазон портов.

**Frame Type** (Тип кадра): Отображается тип кадра ACE. Возможны следующие значения:

- Any (Любой): ACE будет совпадать со всеми типами кадров.
- EType: ACE будет совпадать с кадрами типа Ethernet. Имейте в виду, что тип Ethernet на основе ACE не будет согласовываться с кадрами IP и ARP.
- ARP: ACE будет совпадать с кадрами типа ARP/RARP.
- IPv4: ACE будет совпадать со всеми кадрами IPv4.
- IPv4/ICMP: ACE будет совпадать с кадрами IPv4 с протоколом ICMP.
- IPv4/UDP: ACE будет совпадать с кадрами IPv4 с протоколом UDP.
- IPv4/TCP: ACE будет совпадать с кадрами IPv4 с протоколом TCP.
- IPv4/Other (Другие протоколы IPv4): ACE будет совпадать с кадрами IPv4, которые не являются кадрами с протоколами ICMP/UDP/TCP.
- IPv6: ACE будет совпадать со всеми стандартными кадрами IPv6.

**Action** (Операция): Отображается операция передачи (форвардинга) ACE.

**Permit** (Разрешить): Кадры, согласующиеся с ACE, могут участвовать в обучении и передаваться.

**Deny** (Запретить): Кадры, согласующиеся с ACE, отбрасываются.

**Filtered** (Отфильтрованные): Кадры, согласующиеся с ACE отфильтрованы.

**Rate Limiter** (Ограничитель скорости): В этом поле указан номер ограничителя скорости ACE. Диапазон допустимых значений: от 1 до 16. Когда в этом поле отображается Disabled (Выключен), операция ограничения скорости выключена.

**Port Redirect** (Перенаправление порта): Указывает операцию перенаправления порта ACE.

Кадры, согласующиеся с ACE перенаправляются в порт с указанным номером. Допустимые значения: Disabled (Выключено), либо номер порта. Когда в этом поле отображается Disabled (Выключено), операция ограничения скорости выключена.

**Mirror** (Зеркалирование): В этом поле указана операция зеркалирования данного порта. Допустимы следующие значения:

- Enabled (Включено): Кадры, принятые портом, зеркалируются.
- Disabled (Выключено): Кадры, принятые портом, не зеркалируются. По умолчанию установлено "Disabled" (Выключено).

**CPU:** Передача пакета, согласующегося с конкретным ACE в CPU.

**CPU Once** (Передача первого пакета в CPU): Передача первого пакета, согласующегося с конкретным ACE в CPU.

**Counter** (Счетчик): В поле счетчика указано число использований ACE кадром.

**Conflict** (Конфликт): Указано аппаратное состояние конкретного ACE. Конкретный ACE не применен к аппаратуре вследствие ограничений аппаратуры.

Пример использования через CLI:

```
ZES-2220S# show access-list ace-status
User
----
S   : Static
IPSG: IP Source Guard
IPMC: IPMC
MEP  : MEP
ARPI: ARP Inspection
UPnP: UPnP
PTP  : PTP
DHCP: DHCP
LOOP: Loop Protect
?   : Z-Ring

User ID   Frame   Action Rate L.   Mirror   CPU   Counter Conflict
-----
S    1    Any    Permit 1         Disabled No           0 No
Switch 1 access-list ace number: 1
```

## 2.6.4 DHCP

DHCP Snooping позволяет коммутатору защитить сеть от атак другими устройствами или поддельными серверами DHCP. Когда DHCP Snooping включен на коммутаторе, он может фильтровать IP-трафик на небезопасных (ненадежных) портах, адреса источников которых не могут быть идентифицированы DHCP Snooping. Адреса, присвоенные подключенным клиентам на ненадежных портах, могут тщательно контролироваться, либо с помощью динамического связывания, зарегистрированного в DHCP Snooping, либо при помощи статического связывания, сконфигурированного в IP Source Guard.

### 2.6.4.1 Snooping Configuration (Настройка DHCP Snooping)



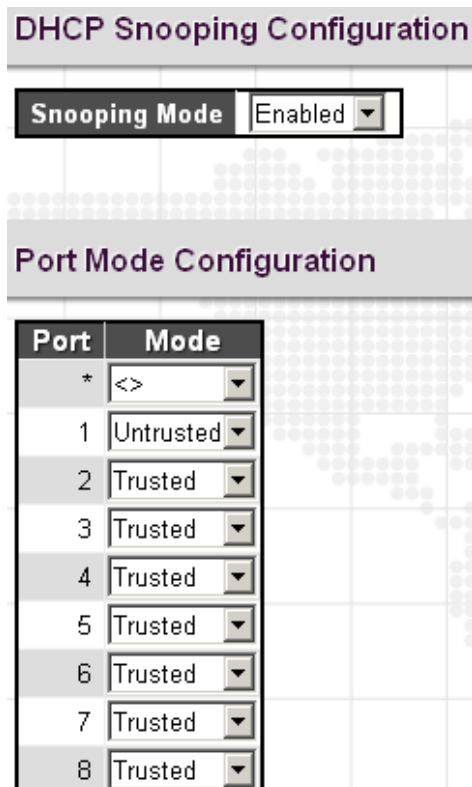


Рис. 73. Вид меню Security – DHCP – Snooping Configuration

#### DHCP Snooping Configuration (Настройка DHCP Snooping)

**Snooping Mode** (Режим работы Snooping): Включает или выключает функцию DHCP Snooping глобально. Когда включен режим работы DHCP snooping, сообщения с запросами DHCP будут передаваться в безопасные порты, ответные пакеты также могут поступать только от безопасных портов.

#### Port Mode Configuration (Настройка режима работы порта)

**Port** (Порт): Номер порта. Правила "Port \*" означают применение ко всем портам.

**Mode** (Режим работы): выберите режим работы порта DHCP Snooping. Порты могут быть либо "Trusted" (Безопасные) либо "Untrusted" (Небезопасные).

Пример использования через CLI:

```
ip dhcp snooping
!
interface FastEthernet 1/1
no ip dhcp snooping trust
```

### 2.6.4.2 Настройка функции DHCP Relay

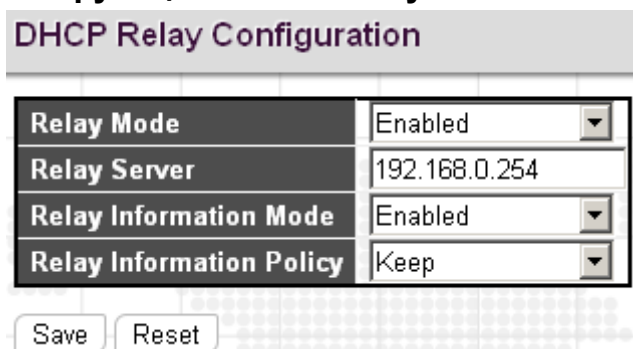


Рис. 74. Вид меню Security – DHCP – Relay configuration

**Relay Mode** (Режим работы DHCP Relay): Включает или выключает функцию DHCP relay.

**Relay Server** (Сервер DHCP Relay): Введите IP-адрес DHCP-сервера, используемого агентом DHCP relay коммутатора.

**Relay Mode** (Информационный режим работы DHCP Relay): Включает или выключает функцию DHCP Relay option 82. Пожалуйста, имейте в виду, что для того, чтобы эта функция работала, необходимо сначала для параметра "Relay Mode" выбрать значение "Enabled" (Включен).

**Relay Information Policy** (Политика информационного режима работы DHCP Relay): Выберите политику информационного режима работы DHCP Relay для DHCP-клиента, включающую информацию option 82.

- **Replace** (Заменять): Замена информации DHCP-клиента информацией DHCP Relay с коммутатора. Это значение задано по умолчанию.
- **Keep** (Поддерживать): Сохранение информации DHCP-клиента.
- **Drop** (Отбрасывать): Отбрасывать пакет, когда принято сообщение DHCP, которое уже содержит информацию DHCP Relay.

Пример использования через CLI:

```
ip dhcp relay
ip helper-address 192.168.0.254
ip dhcp relay information option
```

### 2.6.4.3 Relay Statistics (Статистики DHCP Relay)

DHCP Relay Statistics								Auto-refresh <input type="checkbox"/>
<b>Server Statistics</b>								
Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive Missing Circuit ID	Receive Missing Remote ID	Receive Bad Circuit ID	Receive Bad Remote ID	
0	0	0	0	0	0	0	0	
<b>Client Statistics</b>								
Transmit to Client	Transmit Error	Receive from Client	Receive Agent Option	Replace Agent Option	Keep Agent Option	Drop Agent Option		
0	0	0	0	0	0	0		

Рис. 75. Вид меню Security – DHCP – Relay Statistics

#### DHCP Relay Statistics (Статистики DHCP Relay)

**Transmit to Server** (Передано на сервер): Число пакетов, которые ретранслированы от клиента на сервер.

**Transmit Error** (Передано с ошибками): Число пакетов, которые стали содержать ошибки во время пересылки клиентам.

**Receive from Client** (принято от клиента): Число пакетов, принятых от сервера.

**Receive Missing Agent Option** (Принято без опции агента): Число пакетов, принятых без опций информации агента.

**Receive Missing Circuit ID** (Принято без идентификатора канала): Число пакетов, принятых без опции Circuit ID (Идентификатор канала).

**Receive Missing Remote ID** (Принято без идентификатора удаленного хоста): Число пакетов, принятых без опции Remote ID (Идентификатор хоста).

**Receive Bad Circuit ID** (Принято с плохим идентификатором канала): Число пакетов, у которых опция Circuit ID (Идентификатор канала) не совпадает ни с одним из известных circuit ID.

**Receive Bad Remote ID** (Принято с плохим идентификатором удаленного хоста): Число пакетов, у которых опция Remote ID (Идентификатор удаленного хоста) не совпадает ни с одним из известных Remote ID.

#### Client Statistics (Статистики клиента)

**Transmit to Client** (Передано клиенту): Число пакетов ретранслированных клиенту с сервера.

**Transmit Error** (Передано с ошибками): Число пакетов, которые стали содержать ошибки во время пересылки на серверы.

**Receive from Client** (Принято от клиента): Число пакетов, принятых от сервера.

**Receive Missing Agent Option** (Принято без опции агента): Число пакетов, принятых без опции информации агента ретрансляции.

**Replace Agent Option** (Заменены опцией агента): Число пакетов, которые были заменены опцией информации агента ретрансляции.

**Keep Agent Option** (Ретранслированы с поддержкой опции агента): Число пакетов, в которых была сохранена информация агента ретрансляции.

**Drop Agent Option** (Отброшено без опции агента): Число пакетов, которые были отброшены, но которые были приняты с информацией агента ретрансляции.

## 2.6.5 IP Source Guard (Защита IP-адреса источника)

### 2.6.5.1 Configuration (Настройка)

Port	Mode	Max Dynamic Clients
*	<>	<>
1	Disabled	Unlimited
2	Enabled	1
3	Disabled	Unlimited
4	Disabled	Unlimited
5	Disabled	Unlimited
6	Disabled	Unlimited

Рис. 76. Вид меню Security – IP Source Guard – Configuration

**IP Source Guard Configuration** (Настройка защиты IP-адреса источника)

**Mode** (Режим работы): Включение или выключение защиты IP-адреса источника (глобальное).

**Translate dynamic to static** (Преобразование динамических записей в статические): Нажмите на эту кнопку, чтобы преобразовать динамические записи в статические.

**Port Mode Configuration** (Настройка режима работы порта)

**Port** (Порт): Номер порта. Правила "Port \*" означают применение ко всем портам.

**Mode** (Режим работы): 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** (Макс. число динамических клиентов): 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 с статическими элементами списка (IP-адресами) для данного порта.

Пример использования через CLI:

```
ip verify source
!
interface FastEthernet 1/2
 ip verify source
 ip verify source limit 1
```

### 2.6.5.2 Static Table (Таблица статических записей)

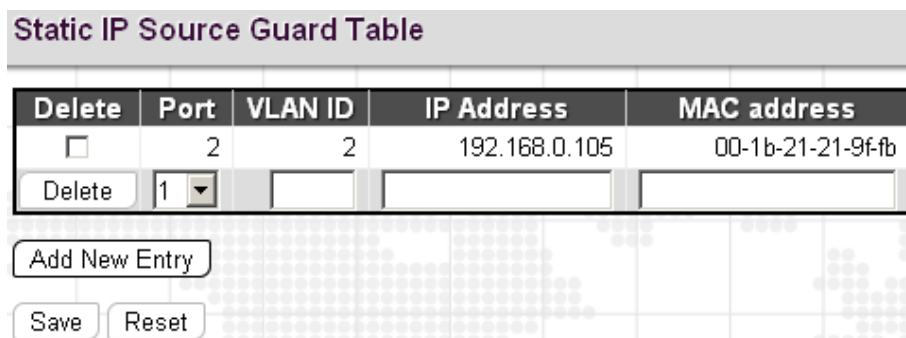


Рис. 77. Вид меню Security – IP Source Guard – Static Table

**Port** (Порт): Порт для которого создается статическая запись.

**VLAN ID**: Введите ранее сконфигурированный номер VLAN ID.

**IP Address** (IP-адрес): Введите корректный IP-адрес.

**MAC Address** (MAC-адрес): Введите корректный MAC-адрес.

Чтобы ввести новый элемент в таблицу, нажмите кнопку “Add New Entry” (Добавить новый элемент). Установите флаг в поле “Delete” (Удалить), чтобы удалить элемент во время следующего сохранения.

Нажмите кнопку “Save” (Сохранить), чтобы сохранить настройки или изменения. Нажмите кнопку “Reset” (Переустановка), чтобы восстановить настройки, заданные по умолчанию, либо ранее сделанные настройки.

Пример использования через CLI:

```
ip source binding interface FastEthernet 1/2 2 192.168.0.105 00-1b-21-21-9f-fb
```

### 2.6.5.3 Dynamic Table (Таблица динамических адресов)

В таблице защиты динамических IP-адресов источника отображаются ее элементы, отсортированные по портам, VLAN ID, IP-адресам и MAC-адресам. По умолчанию, на каждой странице отображается 20 элементов таблицы. Однако на одной странице может отображаться до 999 элементов; число элементов, которое требуется отображать на странице необходимо указать в поле ввода “entries per page” (число элементов на странице).

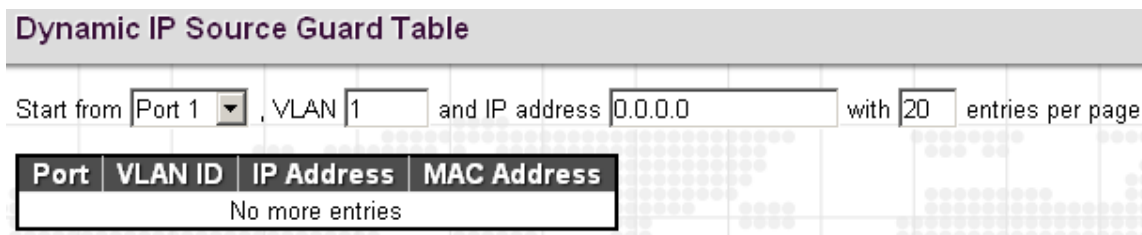


Рис. 78. Вид меню Security – IP Source Guard – Dynamic Table

## 2.6.6 ARP inspection (Инспекция ARP)

### 2.6.6.1 Port Configuration (Настройка порта)

The screenshot shows two configuration sections. The top section, 'ARP Inspection Configuration', has a 'Mode' dropdown set to 'Enabled' and a button labeled 'Translate dynamic to static'. The bottom section, 'Port Mode Configuration', is a table with four columns: 'Port', 'Mode', 'Check VLAN', and 'Log Type'. The table contains seven rows, including a wildcard row for all ports.

Port	Mode	Check VLAN	Log Type
*	<>	<>	<>
1	Disabled	Disabled	None
2	Enabled	Enabled	All
3	Disabled	Disabled	None
4	Disabled	Disabled	None
5	Disabled	Disabled	None
6	Disabled	Disabled	None

Рис. 79. Вид меню Security – ARP inspection – Port Configuration

#### ARP Inspection Configuration (Настройка инспекции ARP)

**Mode** (Режим работы): Включает или выключает функцию инспекции ARP глобально.

#### Port Mode Configuration (Настройка режима работы порта)

**Port** (Порт): Номер порта. Правила "Port \*" означают применение ко всем портам.

**Mode** (Режим работы): 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** (Проверка VLAN): Включает (Enable) или выключает (disable) проверку VLAN.

**Log Type** (Тип журнала): 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.

Пример использования через CLI:

```
ip arp inspection
!
interface FastEthernet 1/2
no ip arp inspection trust
ip arp inspection check-vlan
ip arp inspection logging all
```

### 2.6.6.2 VLAN Configuration (Настройка VLAN)

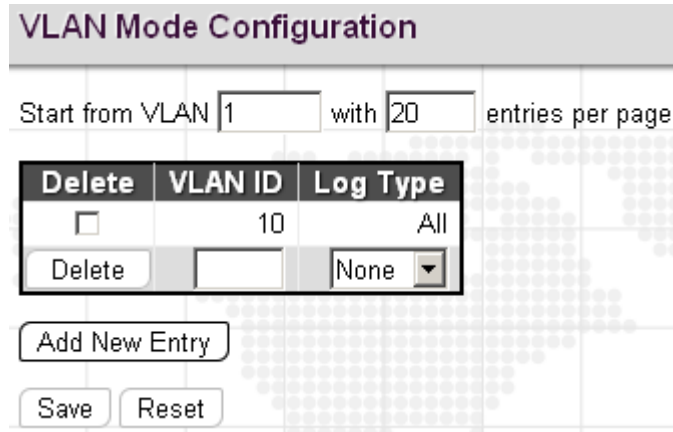


Рис. 80. Вид меню Security – ARP inspection – VLAN Configuration

**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** (Тип журнала): 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.

Чтобы ввести новый элемент в таблицу, нажмите кнопку “Add New Entry” (Добавить новый элемент). Установите флаг в поле “Delete” (Удалить), чтобы удалить элемент во время следующего сохранения.

Нажмите кнопку “Save” (Сохранить), чтобы сохранить новые настройки или их изменения. Нажмите кнопку “Reset” (Переустановка), чтобы восстановить настройки, заданные по умолчанию, либо ранее сделанные настройки.

Пример использования через CLI:

```
ip arp inspection vlan 10
ip arp inspection vlan 10 logging all
```

### 2.6.6.3 Static Table (Таблица статических адресов)

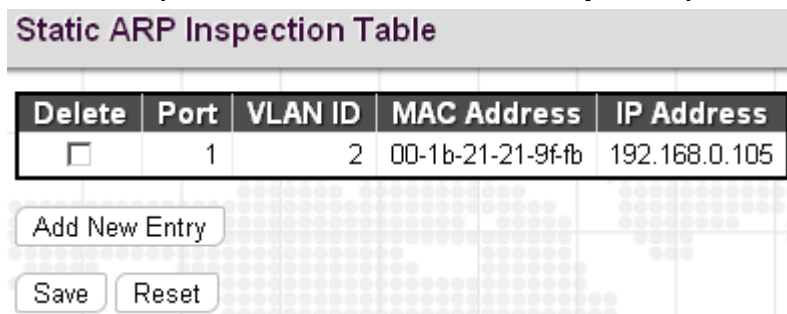


Рис. 81. Вид меню Security – ARP inspection – Static Table

**Port** (Порт): Порт для которого создается статическая запись.

**VLAN ID:** Позволяет задать номер VLAN ID.

**MAC Address** (MAC-адрес): Укажите допустимый MAC-адрес источника в пакетах запросов ARP.

**IP Address** (IP-адрес): Укажите допустимый IP-адрес источника в пакетах запросов ARP.

Чтобы ввести новый элемент в таблицу, нажмите кнопку “Add New Entry” (Добавить новый элемент). Установите флаг в поле “Delete” (Удалить), чтобы удалить элемент во время следующего сохранения.

Нажмите кнопку “Save” (Сохранить), чтобы сохранить новые настройки или их изменения. Нажмите кнопку “Reset” (Переустановка), чтобы восстановить настройки, заданные по умолчанию, либо ранее сделанные настройки.

Пример использования через CLI:

```
ip arp inspection entry interface FastEthernet 1/1 2 00-1b-21-21-9f-fb 192.168.0.105
```

## 2.6.6.4 Dynamic Table Status (Состояние динамической таблицы)

Port	VLAN ID	MAC Address	IP Address
No more entries			

Рис. 82. Вид меню Security – ARP inspection – Dynamic Table Status

**Port** (Порт): Номер порта для данного элемента таблицы.

**VLAN ID**: Номер сети VLAN ID, в которой разрешен трафик ARP.

**MAC Address** (MAC-адрес): Пользовательский MAC-адрес данного элемента таблицы.

**IP Address** (IP-адрес): Пользовательский IP-адрес данного элемента таблицы.

## 2.7 RADIUS

### 2.7.1.1 Configuration (Настройка)

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
<input type="checkbox"/>	192.168.0.105	1812	1813			

Рис. 83. Вид меню Security – Radius – Configuration

#### Global Configuration (Глобальные настройки)

**Timeout** (Время ожидания ответа сервера): Время, которое коммутатор ожидает ответа от сервера аутентификации перед тем, как повторить запрос.

**Retransmit** (Повторная передача): 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** (Время отсутствия сервера): 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.

**Key** (Ключ): 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 Identifier** (Идентификатор NAS): 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): Имя хоста RADIUS-сервера или его IP-адрес.

**Auth Port** (Порт аутентификации): Порт UDP, используемый на RADIUS-сервере для аутентификации.

**Acct Port** (Порт аккаунтинга): Порт UDP, используемый на RADIUS-сервере для аккаунтинга.

**Timeout** (Время ожидания): Если в этом поле указано время ожидания, оно будет использовано вместо глобального времени ожидания. Если желательно использовать глобальное значение, оставьте это поле пустым.

**Retransmit** (Повторная передача): 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.

**Key** (Ключ): 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.

Пример использования через CLI:

```
radius-server host 192.168.0.105
```

## 2.7.1.2 RADIUS Overview (Обзор RADIUS)

RADIUS Authentication Server Status Overview		
#	IP Address	Status
1	192.168.0.105:1812	Ready
2	0.0.0.0:0	Disabled
3	0.0.0.0:0	Disabled
4	0.0.0.0:0	Disabled
5	0.0.0.0:0	Disabled

RADIUS Accounting Server Status Overview		
#	IP Address	Status
1	192.168.0.105:1813	Ready
2	0.0.0.0:0	Disabled
3	0.0.0.0:0	Disabled
4	0.0.0.0:0	Disabled
5	0.0.0.0:0	Disabled

Рис. 84. Вид меню Security – Radius – Overview



#: Число серверов Radius. Поддерживается не более пяти серверов. Для просмотра подробной информации по каждому серверу, нажмите соответствующий номер в столбце #.

**IP Address** (IP-адрес): Настроенный IP-адрес и номер порта UPD.

**Status** (Состояние): Текущее состояние сервера аутентификации RADIUS. Отображаются состояния, в том числе, следующие:

- Disabled (Выключен): Сервер выключен.
- Not Ready (Не готов): Сервер готов, но связь по IP еще не установлена и не работает.
- Ready (Готов): Сервер готов, но связь по IP еще не включена и не работает. RADIUS-сервер готов принимать запросы на доступ.

### 2.7.1.3 RADIUS Details (Подробная информация RADIUS)

RADIUS Authentication Statistics for Server #1			
Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
IP Address		192.168.0.105:1812	
State			Ready
Round-Trip Time			0 ms

RADIUS Accounting Statistics for Server #1			
Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
IP Address		192.168.0.105:1813	
State			Ready
Round-Trip Time			0 ms

Рис. 85. Вид меню Security – Radius – Details

**RADIUS Authentication Statistics for Server** (Статистика аутентификации RADIUS для сервера)

**Access Accepts** (Доступ предоставлен): Число пакетов RADIUS Access-Accept (Доступ предоставлен) корректных и некорректных, принятых от сервера.

**Access Rejects** (Доступ отклонен): Число пакетов RADIUS Access-Reject (Доступ отклонен) корректных и некорректных, принятых от сервера.

**Access Challenges** (Доступ с проблемами): Число пакетов RADIUS Access-Challenge (Доступ с проблемами) корректных и некорректных, принятых от сервера.

**Malformed Access Responses** (Некорректно сформированные ответные пакеты): Число некорректно сформированных пакетов RADIUS Access-Response (Ответные пакеты доступа), принятых от сервера. Среди некорректно сформированных пакетов содержатся и пакеты неправильной длины. Пакеты с атрибутами Bad authenticators (Плохие аутентификаторы) и Message Authenticator (Аутентификатор сообщения), а также пакеты неизвестных типов не относятся к плохо сформированным ответным пакетам доступа.

**Bad Authenticators** (Плохие аутентификаторы): Число ответных пакетов доступа RADIUS, принятых от сервера и содержащих неправильные аутентификаторы или атрибут Message Authenticator (Аутентификатор сообщения).

**Unknown Types** (Неизвестных типов): Число пакетов RADIUS, которые были приняты от сервера с неизвестными типами и отброшены на порту аутентификации.

**Packets Dropped** (Отброшено пакетов): Число пакетов RADIUS, которые были приняты от сервера на порту аутентификации и отброшены по некоторым другим причинам.

**Access Requests** (Запросы доступа): Число пакетов RADIUS Access-Request (Запрос доступа), посланных на сервер. В это число пакетов не входят повторно переданные пакеты.

**Access Retransmissions** (Повторно переданные пакеты запроса доступа): Число пакетов RADIUS Access-Request (Запрос доступа), повторно переданных на RADIUS-сервер аутентификации.

**Pending Requests** (Ожидающие запросы): Число пакетов RADIUS Access-Request (Запрос доступа), назначенных серверу, для которых еще не истек таймер ожидания, либо принят ответ. Данная переменная увеличивается при отправке пакета Access-Request (Запрос доступа) и уменьшается при приеме пакетов Access-Accept (Доступ предоставлен), Access-Reject (Доступ отклонен), Access-Challenge (Доступ с проблемами), а также при ожидании и повторной передаче.

**Timeouts** (Число ожиданий): Число ожиданий аутентификации на сервере. По истечении времени ожидания, клиент может попытаться использовать тот же сервер, послать пакеты на другой сервер или отказаться от отправки пакетов. Попытки с тем же сервером считаются как повторные передачи (то же самое относится и к числу ожиданий). Отправки пакетов на другой сервер считаются как запросы (то же самое относится и к числу ожиданий).

**IP Address** (IP-адрес): IP-адрес и порт UDP для рассматриваемого сервера аутентификации.

**State** (Состояние): Отображается состояние сервера. Возможны следующие значения состояния:

- Disabled (Выключен): Выбранный сервер выключен.
- Not Ready (Не готов): Сервер включен, но связь по IP еще не включена и не работает.
- Ready (Готов): Сервер включен, связь по IP включена и работает; модуль RADIUS готов предоставлять доступ в ответ на запросы.
- Dead (X seconds left) (До принятия решения о том, что сервер вновь присутствует осталось X секунд): К данному серверу были сделаны попытки доступа, однако он не отвечает в течение заданного времени ожидания. Сервер считается временно выключенным (отсутствующим), но по истечении времени отсутствия он вновь будет считаться включенным. В круглых скобках отображается число секунд, оставшееся до того, как это произойдет. Данное состояние может возникнуть только в том случае, если включено более одного сервера.

**Round-Trip Time** (Время на передачу и подтверждение): Интервал времени (измеренный в миллисекундах) между последним обменом пакетами Access-Reply/Access-Challenge и Access-Request с RADIUS-сервером аутентификации. Дискретность (гранулярность) измерения этого интервала времени составляет 100 мс. Значение 0 мс указывает, что двухсторонний обмен сообщениями с сервером еще не установлен.

**RADIUS Accounting Statistics for Server** (Статистика аккаунтинга RADIUS для сервера)

**Responses** (Ответные пакеты): Число пакетов RADIUS (корректных и некорректных), принятых от сервера.

**Malformed Responses** (Плохо сформированные ответные пакеты): Число некорректно сформированных пакетов RADIUS, принятых от сервера. Среди некорректно сформированных пакетов содержатся и пакеты неправильной длины. Пакеты с некорректными аутентификаторами или пакеты неизвестных типов не относятся к некорректным ответным пакетам доступа.

**Bad Authenticators** (Плохие аутентификаторы): Число пакетов RADIUS, содержащих неправильные аутентификаторы, принятые от сервера.

**Unknown Types** (Неизвестных типов): Число пакетов RADIUS неизвестного типа, которые были приняты от сервера на порту аккаунтинга.

**Packets Dropped** (Отброшено пакетов): Число пакетов RADIUS, которые были приняты от сервера на порту аккаунтинга и отброшены по некоторым другим причинам.

**Requests** (Запросы): Число пакетов RADIUS, посланных на сервер. В это число пакетов не входят повторно переданные пакеты.

**Retransmissions** (Повторные передачи): Число пакетов RADIUS, повторно переданных на сервер аккаунтинга RADIUS.

**Pending Requests** (Ожидающие запросы): Число пакетов RADIUS, назначенных серверу, для которых еще не истек таймер ожидания, либо принят ответ. Данная переменная увеличивается, когда отправляется запрос и уменьшается, когда принимается ответ; она уменьшается также во время ожидания или повторной передачи пакетов.

**Timeouts** (Число ожиданий): Число ожиданий аккаунтинга на сервере. По истечении времени ожидания, клиент может попытаться использовать тот же сервер, послать пакеты на другой сервер или отказаться от отправки пакетов. Попытки с тем же сервером считаются как повторные передачи (то же самое относится и к числу ожиданий). Отправки пакетов на другой сервер считаются как запросы (то же самое относится и к числу ожиданий).

**IP Address** (IP-адрес): IP-адрес и порт UDP для рассматриваемого сервера аккаунтинга.

**State** (Состояние): Отображается состояние сервера. Возможны следующие значения состояния:

- **Disabled** (Выключен): Выбранный сервер выключен.
- **Not Ready** (Не готов): Сервер включен, но связь по IP еще не включена и не работает.
- **Ready** (Готов): Сервер включен, связь по IP включена и работает; модуль RADIUS готов принимать попытки регистрации учетных записей.
- **Dead (X seconds left)** (До принятия решения о том, что сервер вновь присутствует осталось X секунд): На данном сервере были предприняты попытки регистрации, однако он не отвечает в течение заданного времени ожидания. Сервер считается временно выключенным (отсутствующим), но по истечении времени отсутствия он вновь будет считаться включенным. В круглых скобках отображается число секунд, оставшееся до того, как это произойдет. Данное состояние может возникнуть только в том случае, если включено более одного сервера.

**Round-Trip Time** (Время на передачу и подтверждение): Интервал времени (измеренный в миллисекундах) между самым последним ответным пакетом и запросным пакетом для него для RADIUS-сервера аккаунтинга. Дискретность измерения указанного интервала составляет 100 мс. Значение 0 мс указывает, что двухсторонний обмен сообщениями с сервером еще не установлен.

Пример использования через CLI:

```
ZES-2220S# show radius-server statistics
Global RADIUS Server Timeout      : 5 seconds
Global RADIUS Server Retransmit   : 3 times
Global RADIUS Server Deadttime    : 0 minutes
Global RADIUS Server Key          :
Global RADIUS Server Attribute 4  :
Global RADIUS Server Attribute 95 :
Global RADIUS Server Attribute 32 :
RADIUS Server #1:
  Host name   : 192.168.0.105
  Auth port  : 1812
  Acct port  : 1813
  Timeout    :
  Retransmit :
  Key        :

RADIUS Server #1 (192.168.0.105:1812) Authentication Statistics:
Rx Access Accepts:          0   Tx Access Requests:          0
Rx Access Rejects:         0   Tx Access Retransmissions:    0
Rx Access Challenges:      0   Tx Pending Requests:         0
Rx Malformed Acc. Responses: 0   Tx Timeouts:                  0
Rx Bad Authenticators:     0
Rx Unknown Types:         0
```

```

Rx Packets Dropped:          0
State:                       Ready
Round-Trip Time:             0 ms

RADIUS Server #1 (192.168.0.105:1813) Accounting Statistics:
Rx Responses:                0    Tx Requests:                0
Rx Malformed Responses:     0    Tx Retransmissions:       0
Rx Bad Authenticators:      0    Tx Pending Requests:     0
Rx Unknown Types:           0    Tx Timeouts:              0
Rx Packets Dropped:         0
State:                       Ready
Round-Trip Time:             0 ms

```

## 2.7.2 TACACS+

Данная страница позволяет настроить Tacacs+ сервер.

**TACACS+ Server Configuration**

**Global Configuration**

<b>Timeout</b>	5	seconds
<b>Deadtime</b>	0	minutes
<b>Key</b>	123456	

**Server Configuration**

Delete	Hostname	Port	Timeout	Key
<input type="checkbox"/>	192.168.0.110	49	20	

Рис. 86. Вид меню Security – Tacacs+

### Global Configuration (Глобальные настройки)

**Timeout** (Время ожидания): Время, которое коммутатор ожидает ответа от сервера TACACS+ перед тем, как повторно передать запрос.

**Deadtime** (Время отсутствия сервера): 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.

**Key** (Ключ): Укажите секретный ключ длиной не более 63 символов. Он будет доступен серверу TACACS+ и коммутатору.

### Server Configuration (Настройка сервера)

**Hostname** (Имя хоста): Имя хоста сервера TACACS+ или его IP-адрес.

**Port** (Порт): Номер порта TCP, используемого на сервере TACACS+ для аутентификации.

**Timeout** (Время ожидания): Если в этом поле указано время ожидания, оно будет использовано вместо глобального времени ожидания. Если желательно использовать глобальное значение, оставьте это поле пустым.

**Key** (Ключ): 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.

Пример использования через CLI:

```

tacacs-server key 123456
tacacs-server host 192.168.0.110 timeout 20

```

## 2.8 Aggregation (Агрегирование)

В сравнении с увеличением стоимости, обусловленным монтажом дополнительных кабелей для повышения скорости передачи на линии и ее резервирования, агрегирование линии является относительно недорогим способом организации высокоскоростной магистральной сети, по которой передается гораздо больше данных, чем может обеспечить один порт или одно устройство. При агрегировании линии используется параллельная работа множества портов, в результате чего скорость обмена данными по линии увеличивается. Используется два типа агрегирования: статическое и LACP.

В меню Aggregation (Агрегирование) имеется два основных раздела static (Статическое агрегирование) и LACP.

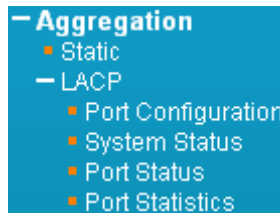


Рис. 87. Вид меню Aggregation

### 2.8.1 Static (Статическое агрегирование)

The screenshot shows the "Aggregation Mode Configuration" section with a "Hash Code Contributors" table and the "Aggregation Group Configuration" section with a "Port Members" table.

Hash Code Contributors			
Source MAC Address	<input checked="" type="checkbox"/>		
Destination MAC Address	<input type="checkbox"/>		
IP Address	<input checked="" type="checkbox"/>		
TCP/UDP Port Number	<input checked="" type="checkbox"/>		

Group ID	Port Members																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Normal	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Рис. 88. Вид меню Aggregation – Static

**Aggregation Mode Configuration** (настройка режима работы агрегирования)

**Source MAC Address** (MAC-адрес источника): MAC-адрес источника используется для расчета линейного порта, через который будет передаваться кадр.

**Destination MAC Address** (MAC-адрес назначения): MAC-адресом назначения используется для расчета линейного порта, через который будет передаваться кадр.

**IP Address** (IP-адрес): IP-адрес используется для расчета линейного порта, через который будет передаваться кадр.

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

**Aggregation Group Configuration** (Настройка группы агрегирования)

**Group ID** (Идентификатор группы): 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** (Порты-члены группы): Выберите порты, принадлежащие некоторой магистрали.

Пример использования через CLI:

```
interface FastEthernet 1/1
 aggregation group 1
!
interface FastEthernet 1/2
 aggregation group 1
```

## 2.8.2 LACP

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.

### 2.8.2.1 Port Configuration (Настройка порта)

Настройка LACP.

LACP Port Configuration						
Port	LACP Enabled	Key		Role	Timeout	Prio
*	<input type="checkbox"/>	<>		<>	<>	32768
1	<input type="checkbox"/>	Auto		Active	Fast	32768
2	<input type="checkbox"/>	Auto		Active	Fast	32768
3	<input type="checkbox"/>	Auto		Active	Fast	32768
4	<input type="checkbox"/>	Auto		Active	Fast	32768
5	<input type="checkbox"/>	Auto		Active	Fast	32768
6	<input type="checkbox"/>	Auto		Active	Fast	32768
7	<input type="checkbox"/>	Auto		Active	Fast	32768
8	<input type="checkbox"/>	Auto		Active	Fast	32768
9	<input type="checkbox"/>	Auto		Active	Fast	32768
10	<input checked="" type="checkbox"/>	Auto		Active	Fast	32768
11	<input checked="" type="checkbox"/>	Auto		Active	Fast	32768

Рис. 89. Вид меню Aggregation – LACP

**Port** (Порт): Номер порта. Правила “Port \*\*” означают применение ко всем портам.

**LACP Enabled** (Включить LACP): Позволяет включить LACP на порту коммутатора.

**Key** (Ключ): Настройка “Auto” (Автоматически) означает, что ключ соответствует физической скорости линии. Если требуется ввести значение ключа, выбранное пользователем, выберите “Specific” (Специальный). Допустимый диапазон ключей: от 1 до 65535. Порты в группе агрегированной линии должны иметь одинаковые ключи LACP порта. Чтобы разрешить участие

порта в группе агрегирования, ключ порта должен иметь то же самое значение (что и у остальных портов группы).

**Role** (Роль): Пользователь может выбрать либо “Active” (Активная роль), либо “Passive” (Пассивная роль), в зависимости от возможностей устройства по согласованию и отправке пакетов управления LACP. Порты, которые были обозначены, как “Active” способны обрабатывать и отправлять кадры управления LACP. В свою очередь, это позволяет LACP-совместимым устройствам согласовывать агрегирование таким образом, что группа может динамически изменяться, если это требуется. Чтобы добавить порты в группу или удалить их из нее, хотя бы один из ее портов-участников должен быть активным портом.

С другой стороны, порты LACP, сконфигурированные, как пассивные, не могут посылать кадры управления LACP. Для того, чтобы позволить поддерживающим LACP устройствам сформировать группу LACP, один конец соединения должен быть обозначен, как пассивные порты LACP.

**Timeout** (Время ожидания): 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** (Приоритет порта): Чем меньше это целое число, тем больше приоритет. Это значение приоритета определяет, какой порт будет активен, а какой – будет играть роль резервного.

Пример использования через CLI:

```
interface FastEthernet 1/10
  lacp
!
interface FastEthernet 1/11
  lacp
```

## 2.8.2.2 System Status (Состояние системы)

LACP System Status					
Aggr ID	Partner System ID	Partner Key	Partner Prio	Last Changed	Local Ports
No ports enabled or no existing partners					

Рис. 90. Вид меню Aggregation – System Status

**Aggr ID** (Идентификатор агрегирования): В этом поле отображается идентификатор агрегирования, ассоциированный с группой агрегирования линии LAG (Link Aggregation Group).

**Partner System ID** (Идентификатор партнерской системы): Идентификатор партнерской системы по группе LAG (MAC-адрес).

**Partner Key** (Ключ партнера): Ключ партнера, присвоенный данной LAG.

**Partner Prio** (Приоритет партнера): Значение приоритета партнера.

**Last Changed** (Последнее изменение): Время, прошедшее с момента изменения данной LAG.

**Local Ports** (локальные порты): Локальные порты, являющиеся портами данной LAG.

### 2.8.2.3 Port Status (Состояние порта)

LACP Status						
Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	No	-	-	-	-	-
2	No	-	-	-	-	-
3	No	-	-	-	-	-
4	No	-	-	-	-	-
5	No	-	-	-	-	-
6	No	-	-	-	-	-
7	No	-	-	-	-	-
8	No	-	-	-	-	-
9	No	-	-	-	-	-
10	No	-	-	-	-	-
11	No	-	-	-	-	-

Рис. 91. Вид меню Aggregation – Port Status

**Port** (Порт): Номер порта.

**LACP**: Отображается состояние LACP на порту.

- Yes (Да): LACP включен, линия порта включена.
- No (Нет): LACP не включен, либо выключена линия порта.
- Ваксир (Резервный порт): Порт играет роль резервного. Когда другие порты покинут группу LAG, данный порт вступит в LAG.

**Key** (Ключ): Значение ключа агрегирования на порту.

**Aggr ID** (Идентификатор агрегирования): Отображается идентификатор агрегирования, активный на порту.

**Partner System ID** (Идентификатор партнерской системы): Идентификатор LAG партнерской системы.

**Partner Port** (Партнерский порт): Партнерский порт, подключенный к данному локальному порту.

**Partner Prio** (Приоритет партнера): Значение приоритета партнера.

### 2.8.2.4 Port Statistics (Статистика порта)

LACP Statistics					
Port	LACP Received	LACP Transmitted	Discarded		
			Unknown	Illegal	
1	0	0	0	0	
2	0	0	0	0	
3	0	0	0	0	
4	0	0	0	0	
5	0	0	0	0	
6	0	0	0	0	
7	0	0	0	0	
8	0	0	0	0	
9	0	0	0	0	
10	0	0	0	0	
11	0	0	0	0	

Рис. 92. Вид меню Aggregation – Port Statistics



**Port** (Порт): Номер порта.

**LACP Received** (Принято пакетов LACP): Число пакетов LACP, принятых на порту.

**LACP Transmitted** (Число переданных пакетов LACP): Число пакетов LACP, переданных портом.

**Discarded** (Отброшено): Число неизвестных и неправильных пакетов, которые должны быть отброшены на порту.

## 2.9 Redundancy (Резервирование)

Разработка резервных маршрутов может защитить сети от неожиданных автоматических включений резервных комплектов оборудования. Это исключительно важно в сетях от которых требуется бесперебойное предоставление услуг и работоспособность которых критична для их применения. Однако, резервные маршруты могут приводить к образованию петель в сетях и при недостаточном обслуживании сетей - к их неработоспособности. На практике обычно реализуется несколько способов защиты от петель, гарантирующих, что сети будут функционировать нормально, без петель, и будут как можно скорее восстанавливаться после отказов. Наиболее популярными способами является использование STP (802.1d), RSTP (802.1w) и MSTP (802.1s). При промышленном применении настоятельно рекомендуется использовать нашу собственную разработку Z-Ring и ERPS (G.8032), которые обеспечивают значительно меньшее время восстановления, чем любой STP-протокол.

В данном разделе описаны функции, обеспечивающие резервирование. Функции, описанные в данном разделе находятся в меню "Redundancy" (резервирование).

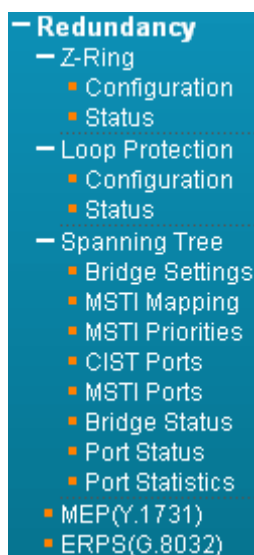


Рис. 93. Вид меню Redundancy

### 2.9.1 Технология Z-Ring

Технология Z-Ring является нашей собственной разработкой. Поддерживает 250 устройств, работающих при топологии «кольцо» и обеспечивает время переключения на резервный маршрут не более, чем через 10 мс после отказа линии. По сравнению с протоколом STP, Z-Ring обеспечивает меньшее время восстановления сети, является более гибкой и масштабируемой в архитектуре сети. Технология резервирования Z-Ring может автоматически идентифицировать ведущее устройство кольца (пользовательское ведущее устройство также поддерживается), а затем заблокировать порт, оставленный в ведущем устройстве для целей резервирования.

#### 2.9.1.1 Configuration (Настройка)

## Z-Ring Configuration

Delete	Instance	Type	Master	East		West	
				Port	Edge	Port	Edge
Delete	1	Z-Ring	<input type="checkbox"/>	1		2	

Add New Instance

Save Reset

Рис. 94. Вид меню Aggregation – Z-Ring – Configuration

Чтобы добавить новый элемент списка, нажмите кнопку “Add New Instance” (добавить новый объект).

**Instance** (Объект): Номер объекта. Общее число поддерживаемых объектов равно 5.

**Type** (Тип): Z-Ring поддерживает 3 типа кольца. Они описаны ниже.

- Z-Ring: Тип Z-Ring используется в технологии замкнутого кольца. Все устройства-участники должны поддерживать технологию резервирования Z-Ring.

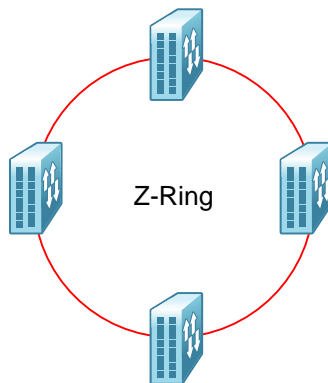


Рис. 95. Кольцо Z-Ring

- Z-Chain: Тип Z-Chain используется, когда устройства, поддерживающие Z-Ring соединяются через сеть либо через устройство, которое не поддерживает технологию Z-Ring.

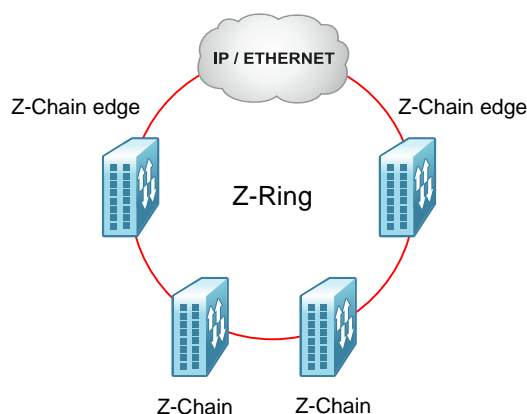
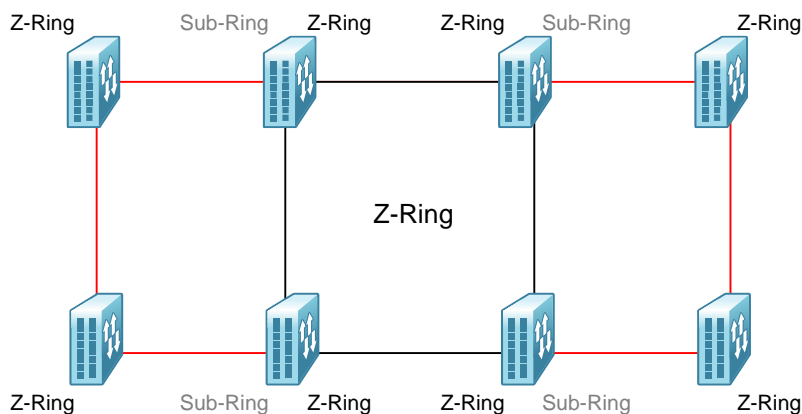


Рис. 96. Кольцо Z-Ring построенное через сеть

- Sub-Ring: Тип Sub-Ring используется при разомкнутом кольце и имеет только один узел. В топологии сети тип Sub-Ring должен использоваться вместе с типом Z-Ring или с типом Z-Chain. В кольце данного типа не используется сторонних устройств.



**Рис. 97. Кольцо Z-Ring с участками Sub-Ring**

**Master** (Ведущее устройство): Опция Master (Ведущее устройство) обычно используется, чтобы определить, какой сегмент будет использоваться в качестве резервного маршрута. Пользователь может вручную выбрать поле и установить в нем флаг, чтобы объявить определенное устройство в кольце, как ведущее (Master). Однако, если ни в одном из полей Master устройств флаг не будет установлен, то протокол Z-Ring объявит одно из устройств в кольце ведущим на основе его MAC-адреса. Процесс выбора описан ниже, в таблице «Определение ведущего устройства (Master) и блокирование порта».

**Port** (Порт): Выберите западный и восточный порт из раскрывающегося меню.

**Edge** (Граница): Это поле появляется, только когда выбран тип Z-Chain. Установите флаг в поле порта, чтобы настроить его, как граничный порт Z-Chain.

**Определение ведущего устройства (Master) и блокирование порта.**

	<b>Z-Ring</b>	<b>Z-Chain</b>	<b>Sub-Ring</b>
Шаг 1. Определение ведущего устройства	<ul style="list-style-type: none"> <li>• Вручную выбрать ведущее устройство кольца.</li> <li>• Если в качестве ведущих выбрано несколько устройств, протокол резервирования Z-Ring сам назначит ведущее устройство в зависимости от MAC-адреса устройства. Ведущим устройством кольца станет устройство с наибольшим MAC-адресом.</li> <li>• Если ведущее устройство кольца не выбрано, протокол резервирования Z-Ring сам назначит ведущее устройство в зависимости от MAC-адреса устройства. Ведущим устройством кольца станет устройство с наибольшим MAC-</li> </ul>	<ul style="list-style-type: none"> <li>• Вручную выбрать ведущее устройство кольца.</li> <li>• В качестве ведущего будет выбрано устройство с сконфигурированным граничным портом и наибольшим MAC-адресом.</li> <li>• Если в качестве ведущего ошибочно выбрано устройство, не имеющее границы, протокол резервирования Z-Ring проигнорирует эту неправильную настройку.</li> </ul> <p>ПРИМЕЧАНИЕ: Когда выбран тип Z-Chain, только устройство с граничным портом (или граничными портами) может быть выбрано в качестве ведущего.</p>	<ul style="list-style-type: none"> <li>• Вручную выбрать ведущее устройство кольца.</li> <li>• Если в качестве ведущих выбрано несколько устройств, протокол резервирования Z-Ring сам назначит ведущее устройство в зависимости от MAC-адреса устройства. Ведущим устройством кольца станет устройство с наибольшим MAC-адресом.</li> <li>• Если ведущее устройство кольца не выбрано, протокол резервирования Z-Ring сам назначит ведущее устройство в зависимости от MAC-адреса устройства. Ведущим устройством кольца станет устройство с наибольшим MAC-</li> </ul>

	адресом.		адресом.
Шаг 2. Блокирование порта	Будет блокирован порт с наибольшим номером в ведущем устройстве кольца.	<ul style="list-style-type: none"> <li>• Будет блокирован граничный порт в ведущем устройстве кольца.</li> <li>• Если ведущее устройство имеет два граничных порта, то будет блокирован порт с наибольшим номером.</li> </ul>	Будет блокирован порт с наибольшим номером в ведущем устройстве кольца.

Пример использования через CLI:

```
ring 1 ring east interface FastEthernet 1/1 west interface FastEthernet 1/2
```

### 2.9.1.2 Status (Состояние)


Z-Ring Status									
Instance	Type	Role	East			West			Healthy
			Port	State	Edge	Port	State	Edge	
1	Z-Ring	?	1	Down	---	2	Down	---	

Рис. 98. Вид меню Aggregation – Z-Ring – Status

**Instance** (Копия): Номер объекта.

**Type** (Тип): Отображается тип резервного кольца.

**Role** (Роль): В данном поле может быть указано либо Master (Ведущее устройство) либо Slave (Ведомое устройство). Порты в ведомом устройстве блокированы не будут.

**East & West Port Number** (Номер восточного (западного) порта): Номер порта, сконфигурированные в объекте.

**East & West Port State** (Состояние восточного (западного) порта): Текущее состояние сконфигурированного порта в кольце. Отображаемое состояние может быть одним из следующих:

- Forwarding (Передача): Порт обеспечивает нормальную передачу пакетов.
- Blocking (Блокирован): Порт блокирован и используется в качестве резервного.
- Down (Выключен): Физическое соединение отсутствует.

**East & West Port Edge** (Состояние восточного (западного) граничного порта): В данном поле указано, является ли сконфигурированный порт граничным или нет.

**Healthy** (Работоспособность кольца): В данном поле графически индицируется текущее состояние кольца.

«X»: Маршрут не входит в кольцо.

«O»: Выбрано ведущее устройство, резервный маршрут блокирован. Сеть с резервным маршрутом функционирует нормально.

«O»: Физическая линия или соединение кольца выключены. Состояние резервного маршрута изменилось с “blocked” (блокирован) на “forwarding” (передача), когда один из путей передачи пакетов стал недоступен.

Пример использования через CLI:

```
ZES-2220S#show ring 1
          |-----East-----| |-----West-----|
Inst Type  Role  Interface State Edge Interface State Edge Healthy
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
  1  Ring    -    Fa 1/1    Down  -    Fa 1/2    Down  -    -
```

## 2.9.2 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, могут быть отключены либо соответствующие события могут быть зарегистрированы в журнале.

### 2.9.2.1 Configuration (Настройка)

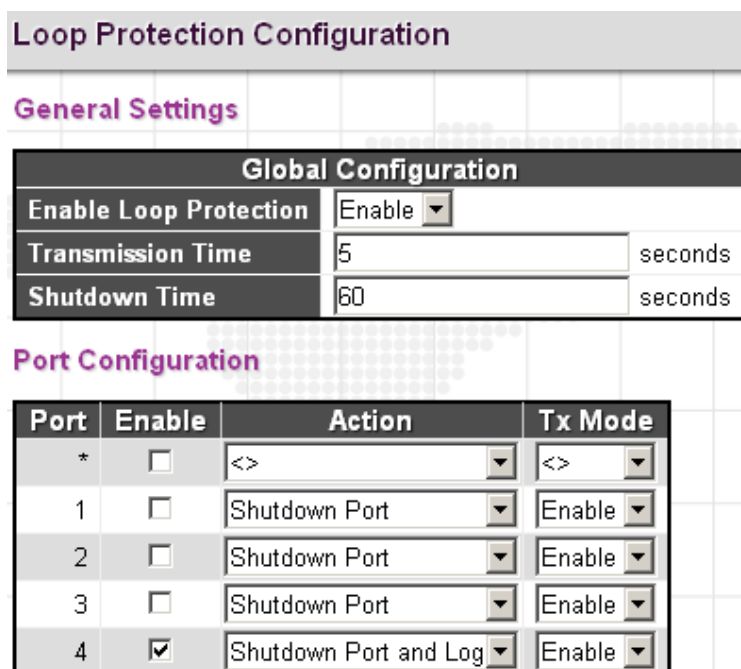


Рис. 99. Вид меню Loop Protection – Configuration

#### General Settings (Основные настройки)

**Enable Loop Protection** (Включить защиту от петель): Позволяет включить или выключить функцию защиты от петель.

**Transmission Time** (Время передачи): Интервал между отправкой пакетов защиты от петель PDU на каждом порту. Допустимые значения: от 1 до 10 секунд.

**Shutdown Time** (Время отключения): 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** (Порт): Список номеров портов. Правила “Port \*” означают применение ко всем портам.

**Enable** (Включить): Позволяет включить или выключить функцию защиты от петель на выбранных портах.

**Action** (Операция): Когда на порту обнаружена петля, функция защиты от петель немедленно выполнит соответствующие операции. Операции могут быть следующими: “Shutdown Port” (Выключить порт), “Shutdown Port and Log” (Выключить порт, но вести регистрацию в журнале) либо “Log Only” (Только регистрировать в журнале).

- **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** (Режим передачи): Включает или выключает генерацию пакетов защиты от петель PDU либо осуществляется пассивный поиск PDU, переданных по петле.

Пример использования через CLI:

```
loop-protect
loop-protect shutdown-time 60
!
interface FastEthernet 1/1
 no loop-protect
!
interface FastEthernet 1/4
 loop-protect action shutdown log
```

### 2.9.2.2 Status (Состояние)

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
4	Shutdown+Log	Enabled	0	Down	-	-

Рис. 100. Вид меню Loop Protection – Status

**Port** (Порт): Номер порта.

**Action** (Операция): Отображается операция, выполняемая при обнаружении петель коммутатором.

**Transmit** (Передача): Отображается установленный режим работы на передачу (Tx).

**Loops** (Петли): Число петель, обнаруженных на порту.

**Status** (Состояние): Текущее состояние петель, обнаруженных на порту.

**Loops** (Петля): Индицируется, обнаружена ли петля на порту или нет.

**Time of Last Loop** (Время последней петли): Время, в которое обнаружена последняя петля.

### 2.9.3 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.

### 2.9.3.1 Bridge Settings (Настройки моста)

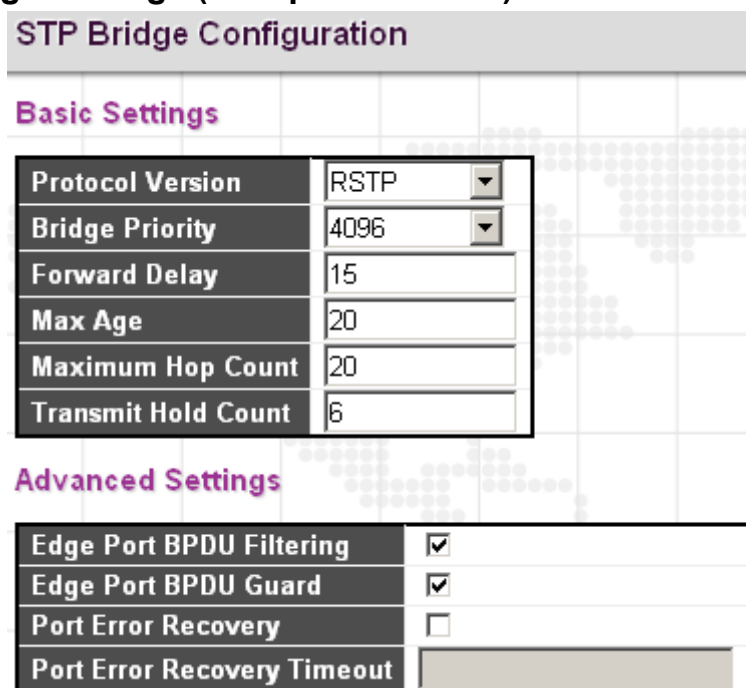


Рис. 101. Вид меню Spanning Tree – Bridge Settings

#### Basic Settings (Настройки моста)

**Protocol Version** (Версия протокола): Выберите соответствующий протокол. Версии протокола следующие: "STP", "RSTP" и "MSTP".

**Bridge Priority** (Приоритет коммутатора): 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.

**Forward Delay** (Задержка до передачи пакетов): 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** (Макс. период): Если другой коммутатор не пошлет конфигурационный пакет hello в течение заданного периода времени, он считается отключенным. Допустимый диапазон значений: от 6 до 40 секунд, значение Max Age должно быть меньше или равно  $(\text{Forward Delay} - 1) * 2$ .

**Maximum Hop Count** (Максимальное число участков между коммутаторами): 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 передаваемых пакетов BPDU в секунду): 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 оконечным 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): Когда включено, порт, выключенный из-за ошибки, может быть автоматически включен по прошествии определенного времени.

**Port Error Recovery Timeout** (Время восстановления порта после ошибки): Время, которое должно пройти до того момента, когда порт, выключенный из-за ошибки, будет включен вновь. Допустимый диапазон значений от 30 до 86400 секунд.

Пример использования через CLI:

```
spanning-tree mode rstp
spanning-tree edge bpdu-filter
spanning-tree edge bpdu-guard
spanning-tree mst 0 priority 4096
```



## 2.9.3.2 MSTI Mapping (Отображение MSTI)

### MSTI Configuration

Add VLANs separated by spaces or comma.

**Unmapped VLANs are mapped to the CIST.** (The default bridge instance).

### Configuration Identification

Configuration Name	00-1a-81-00-c0-a9
Configuration Revision	0

### MSTI Mapping

MSTI	VLANs Mapped
MST1	3-5
MST2	
MST3	
MST4	
MST5	
MST6	
MST7	
MST8	

Рис. 102. Вид меню Spanning Tree – MSTI Mapping

#### Configuration Identification (Идентификационные данные конфигурации)

**Configuration Name** (Имя конфигурации): Имя данной 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 конфигурации): Номер версии для данного MSTI. Допустимый диапазон значений: от 1 до 65535.

#### MSTI Mapping (Отображение MSTI)

**MSTI**: Номер копии MSTI.

**VLAN Mapped** (Отображение VLAN): Задайте номера сетей VLAN, которые будут привязаны к данной 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.

Пример использования через CLI:

```
spanning-tree mst name 00-1a-81-00-c0-a9 revision 0
spanning-tree mst 1 vlan 3-5
```

## 2.9.3.3 MSTI Priorities (Приоритеты MSTI)

## MSTI Configuration

### MSTI Priority Configuration

MSTI	Priority
*	<>
CIST	32768
MSTI1	32768
MSTI2	32768
MSTI3	32768
MSTI4	32768
MSTI5	32768
MSTI6	32768
MSTI7	32768
MSTI8	32768
MSTI9	32768
MSTI10	32768
MSTI11	32768
MSTI12	32768
MSTI13	32768
MSTI14	32768
MSTI15	32768

Рис. 103. Вид меню Spanning Tree – MSTI Priorities

**MSTI:** Отображается номер копии MSTI. “MSTI \*\*” – правило приоритета применяется ко всем портам.

**Priority (Приоритет):** 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.

Пример использования через CLI:

```
spanning-tree mst 1 priority 16384
```

## 2.9.3.4 CIST Ports (Порты CIST)

STP CIST Port Configuration										
CIST Aggregated Port Configuration										
Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
		Role	TCN							
-	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forced True
CIST Normal Port Configuration										
Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
		Role	TCN							
*	<input type="checkbox"/>	<>		<>	<>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<>
1	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
2	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
3	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
4	<input checked="" type="checkbox"/>	Auto		16	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Auto
5	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
6	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto

Рис. 104. Вид меню Spanning Tree – CIST Ports

### CIST Aggregated Port Configuration (Настройка агрегированного порта CIST)

**Port** (Порт): Номер порта.

**STP Enabled** (Включить STP): Включает функцию STP.

**Path Cost** (Стоимость пути): 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** (Приоритет): Выберите приоритет порта.

**Admin Edge** (Граница администрирования): Если интерфейс подключен к конечным 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** (Защита BPDU): 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.

Пример использования через CLI:

```
interface FastEthernet 1/4
 spanning-tree
 spanning-tree bpdu-guard
```

### 2.9.3.5 MSTI Ports (Порты MSTI)



Рис. 105. Вид меню Spanning Tree – MSTI Ports

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

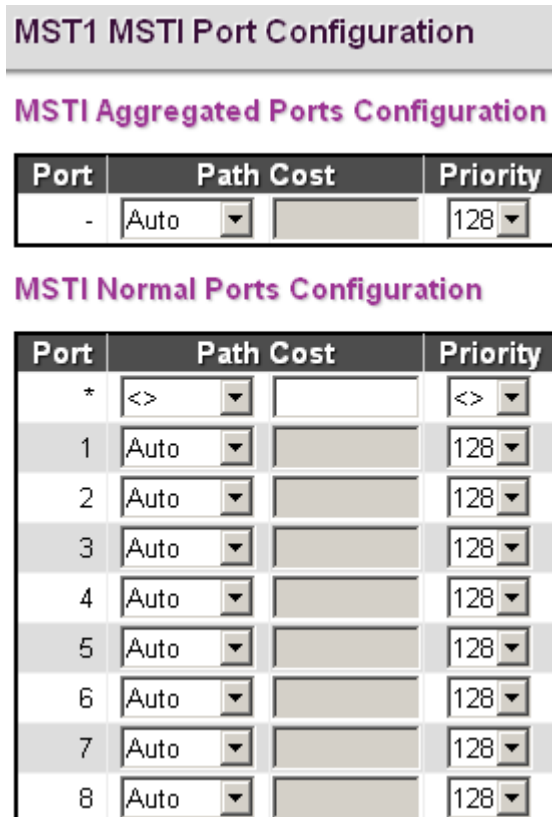


Рис. 106. Вид меню Spanning Tree – MSTI Port Configuration

**Port** (Порт): Номер порта.

**Path Cost** (Стоимость маршрута): 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** (Приоритет): Выберите приоритет порта.

### 2.9.3.6 Bridge Status (Состояние моста)

## STP Bridges

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
<a href="#">CIST</a>	32768.00-1A-81-00-C0-A9	32768.00-1A-81-00-C0-A9	-	0	Steady	-

Рис. 107. Вид меню Spanning Tree – Bridge Status

### STP Bridge (Мост STP)

**MSTI:** Копия моста. Для просмотра детальной информации о состоянии моста нажмите мышью на эту копию.

**Bridge ID** (Идентификатор моста): Уникальный идентификатор моста для данной копии, содержащий значение приоритета и MAC-адрес коммутатора.

**Root ID** (Идентификатор корневого устройства): Отображается значение приоритета корневого устройства и его MAC-адрес.

**Root Port** (Корневой порт): Номер порта на данном коммутаторе, который ближе всего к корневому коммутатору. Данный коммутатор связывается с корневым устройством через этот порт. Если корневой порт отсутствует, то этот коммутатор будет считаться корневым устройством.

**Root Cost** (Стоимость маршрута к корневому устройству): Стоимость маршрута от корневого порта коммутатора до корневого устройства. Для корневого моста равна нулю. Для всех других мостов является суммой стоимостей маршрутов между портами на маршруте с наименьшей стоимостью к корневому мосту.

**Topology Flag** (Флаг топологии): Текущее состояние флага уведомления об изменении топологии для данной копии моста.

**Topology Change Last** (Последнее изменение топологии): Время, прошедшее с момента последнего конфигурирования данного покрывающего дерева.

Для просмотра детальной информации о состоянии моста STP нажмите мышью на копию MSTI .

## STP Detailed Bridge Status

STP Bridge Status	
Bridge Instance	CIST
Bridge ID	32768.00-1A-81-00-C0-A9
Root ID	32768.00-1A-81-00-C0-A9
Root Cost	0
Root Port	-
Regional Root	32768.00-1A-81-00-C0-A9
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	0
Topology Change Last	-

### CIST Ports & Aggregations State

Port	Port ID	Role	State	Path Cost	Edge	Point-to-Point	Uptime
5	128:005	DesignatedPort	Forwarding	200000	Yes	Yes	0d 00:00:13
7	128:007	DesignatedPort	Forwarding	200000	Yes	Yes	0d 00:00:13

Рис. 108. Вид меню Spanning Tree – STP Detailed Bridge Status

### STP Detailed Bridge Status (Детальная информация о состоянии STP моста)

**Bridge Instance** (Копия моста): Копия моста.

**Bridge ID** (Идентификатор моста): Уникальный идентификатор моста для данной копии, содержащий значение приоритета и MAC-адрес коммутатора.

**Root ID** (Идентификатор корневого устройства): Отображается значение приоритета корневого устройства и его MAC-адрес.

**Root Cost** (Стоимость маршрута к корневому устройству): Стоимость маршрута от корневого порта коммутатора до корневого устройства. Для корневого моста равна нулю. Для всех других мостов является суммой стоимостей маршрутов между портами на маршруте с наименьшей стоимостью к корневому мосту.

**Root Port** (Корневой порт): Номер порта на данном коммутаторе, который ближе всего к корневому коммутатору. Данный коммутатор связывается с корневым устройством через этот порт. Если корневой порт отсутствует, то этот коммутатор будет считаться корневым устройством.

**Regional Root** (Региональное корневое устройство): Bridge ID (Идентификатор моста) текущего выбранного регионального корневого моста, внутри региона MSTP данного моста. (Этот параметр применим только к копии CIST.)

**Internal Root Cost** (Стоимость внутреннего маршрута): Стоимость маршрута к региональному корневому устройству. Для регионального корневого моста равна нулю. Для всех остальных копий CIST в том же регионе MSTP, является суммой стоимостей внутренних маршрутов между портами на маршруте с наименьшей стоимостью к корневому мосту. (Этот параметр применим только к копии CIST.)

**Topology Flag** (Флаг топологии): Текущее состояние флага уведомления об изменении топологии для данной копии моста.

**Topology Change Last** (Последнее изменение топологии): Время, прошедшее с момента последнего конфигурирования данного покрывающего дерева.

### **CIST Ports & Aggregations State** (Порты CIST и состояние агрегирования)

**Port** (Порт): Отображается номер порта.

**Port ID** (Идентификатор порта): Идентификатор порта, используемый для протокола RSTP. ID этого порта содержит номер порта и его приоритет.

**Role** (Роль): Роль, присвоенная алгоритмом STP. Роли могут быть следующими: “Designated Port” (Назначенный порт), “Backup Port” (резервный порт), “Root Port” (Корневой порт).

**State** (Состояние): Отображается текущее состояние порта.

- **Blocking** (Блокирован): Порт только принимает сообщения BPDU, но не передает их.
- **Learning** (Обучение): Порт передал конфигурационные сообщения за интервал, заданный параметром Forward Delay, но не принял противоречащей информации. Таблица адресов порта очищена, порт начал обучение адресам.
- **Forwarding** (Передача): Порты передают пакеты и продолжают обучаться адресам.

**Edge** (Граничный порт): Отображается, является ли данный порт граничным или нет.

**Point-to-Point** (Точка-точка): Отображается, участвует ли порт в соединении точка-точка или нет. Это может быть задано автоматически или вручную.

**Uptime** (Время после инициализации): Время, прошедшее с того момента, когда порт моста был инициализирован.

Пример использования через CLI:

```
ZES-2220S# show spanning-tree active
CIST Bridge STP Status
Bridge ID      : 32768.00-1A-81-00-C0-A9
Root ID       : 32768.00-1A-81-00-C0-A9
Root Port     : -
Root PathCost: 0
Regional Root: 32768.00-1A-81-00-C0-A9
Int. PathCost: 0
Max Hops      : 20
TC Flag       : Steady
TC Count      : 0
TC Last       : -
Port          Port Role      State      Pri  PathCost  Edge  P2P  Uptime
-----
Fa 1/5       DesignatedPort Forwarding 128   200000   Yes   Yes   0d 00:18:26
```

### 2.9.3.7 Port Status (Состояние порта)

STP Port Status			
Port	CIST Role	CIST State	Uptime
1	Disabled	Discarding	-
2	Disabled	Discarding	-
3	Disabled	Discarding	-
4	Disabled	Discarding	-
5	DesignatedPort	Forwarding	0d 00:19:58
6	Disabled	Discarding	-
7	DesignatedPort	Forwarding	0d 00:19:58
8	Disabled	Discarding	-
9	Disabled	Discarding	-
10	Disabled	Discarding	-
11	Disabled	Discarding	-
12	Disabled	Discarding	-
13	Disabled	Discarding	-
14	Disabled	Discarding	-
15	Disabled	Discarding	-
16	Disabled	Discarding	-
17	Disabled	Discarding	-
18	Disabled	Discarding	-
19	Disabled	Discarding	-
20	Disabled	Discarding	-

Рис. 109. Вид меню Spanning Tree – Port Status

**Port** (Порт): Номер порта.

**CIST Role** (Роль CIST): Роль, присвоенная алгоритмом STP. Роли могут быть следующими: “Designated Port” (Назначенный порт), “Backup Port” (резервный порт), “Root Port” (Корневой порт) или “Non-STP” (Порт, неохваченный STP).

**CIST State** (Состояние CIST): Отображается текущее состояние порта. Отображаемое состояние CIST может быть одним из следующих:

- Discarding (Отброшен): Порт только принимает сообщения BPDU, но не передает их.
- Learning (Обучен): Порт передал конфигурационные сообщения за интервал, заданный параметром Forward Delay, но не принял противоречащей информации. Таблица адресов порта очищена, порт начал обучение адресам.
- Forwarding (Передача): Порты передают пакеты и продолжают обучаться адресам.

**Uptime** (Время после инициализации): Время, прошедшее с того момента, когда порт моста был инициализирован.

### 2.9.3.8 Port Statistics (Статистика порта)

STP Statistics										
Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
5	0	659	0	0	0	0	0	0	0	0
7	0	659	0	0	0	0	0	0	0	0

Рис. 110. Вид меню Spanning Tree – Port Statistics

**Port** (Порт): Отображается номер порта.

**Transmitted & Received MSTP/RSTP/STP** (Передано (принято) BPDU): Число переданных (принятых) портом конфигурационных сообщений BPDU протокола MSTP/RSTP/STP.

**Transmitted & Received TCN** (Передано (принято) TCN): Число кадров TCN переданных (принятых) портом.

**Discarded Unknown/Illegal** (Отброшено неизвестных / неправильных): Число неизвестных и неправильных пакетов, которые отброшены на порту.

## 2.9.4 MEP (Maintenance Entity Point)

Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID	This MAC	Alarm
<input type="checkbox"/>	1	Port	Mep	Down	1	0	1	0	00-1A-81-00-C0-AA	

Рис. 111. Вид меню MEP (Maintenance Entity Point)

**Instance** (Копия): Задайте идентификатор копии MEP.

Сохраните введенные данные, затем нажмите мышью на номер копии и введите дополнительные конфигурационные данные этой копии MEP. Повторите эти действия для каждой копии MEP.

**Domain** (Домен)

**Port** (Порт): Это MEP в домене порта. 'Flow Instance' (Копия потока) – это порт. (В показанном примере порт доступен для использования.)

**MEP**: Это MEP в домене EVC. 'Flow Instance' (Копия потока) – это EVC. Должен быть создан EVC.

**Mode** (Режим работы): Выберите либо Mep (Maintenance Entity End Point – конечная точка обслуживания объекта) или Mip (Maintenance Entity Intermediate Point – промежуточная точка обслуживания объекта).

**Direction** (Направление): Выберите направление трафика – либо Down/Ingress (Входящий), либо Up/Egress (Исходящий) на резидентном порту.

**Residence Port** (Резидентный порт): Задайте порт, на котором осуществляется мониторинг.

**Level** (Уровень): Уровень MGP этого MEP.

**Flow Instance** (Копия потока): MEP, ассоциированный с данным потоком.

**Tagged VID** (Номер тегированной VLAN): Для VLAN с этим VID будет добавлен C-tag или S-tag (в зависимости от типа порта VLAN). Если добавление тега не требуется, введите 0.

**This MAC** (MAC-адрес данного MEP): MAC-адрес данного MEP (если выбрана одноадресная передача может быть использован другим MEP).

**Alarm** (Сигнализация): В MEP сработала сигнализация.

Нажмите мышью номер копии, чтобы ввести дополнительные настройки MEP.



MEP Configuration

Instance Data

Instance	Domain	Mode	Direction	Residence Port	Flow Instance	Tagged VID	EPS Instance	This MAC
1	Port	Mep	Down	1	1	0	0	00-1A-81-00-C0-AA

Instance Configuration

Level	Format	Domain Name	MEG id	MEP id	Tagged VID	cLevel	cMEG	cMEP	cAIS	cLCK	cSSF	aBLK	aTSF
0	ITU ICC		YOURSWmeg000	1	0	<span style="color: green;">●</span>	<span style="color: green;">●</span>	<span style="color: green;">●</span>	<span style="color: green;">●</span>	<span style="color: green;">●</span>	<span style="color: red;">●</span>	<span style="color: green;">●</span>	<span style="color: red;">●</span>

Peer MEP Configuration

Delete	Peer MEP ID	Unicast Peer MAC	cLOC	cRDI	cPeriod	cPriority
<input type="checkbox"/>	1	00-00-00-00-00-00	<span style="color: green;">●</span>	<span style="color: green;">●</span>	<span style="color: green;">●</span>	<span style="color: green;">●</span>

Add New Peer MEP

Functional Configuration

Continuity Check			APS Protocol				
Enable	Priority	Frame rate	Enable	Priority	Cast	Type	Last Octet
<input type="checkbox"/>	0	1 f/sec	<input type="checkbox"/>	0	Multi	L-APS	1

Fault Management Performance Monitoring

Рис. 112. Вид меню MEP Configuration

**Instance Data** (Данные копии) Подробная информация о текущей копии MEP.

**Instance Configuration** (Настройки копии)

**Level** (Уровень): Выберите уровень MEP. Допустимый диапазон значений: 0~7.

**Format** (Формат): Доступно два формата.

- ITU ICC: Определен ITU в стандарте Y.1731 раздел A3. Доменное имя не используется. Идентификатор MEG id должен иметь длину не более 13 символов.
- IEEE String (Строка IEEE): Определена IEEE в 802.1ag раздел 21.6.5. Можно ввести доменное имя и краткое имя длиной не более 16 символов. Длина идентификатора MEG id - не более 16 символов.
- ITU CC ICC: Определен ITU в стандарте Y.1731 раздел A5. Доменное имя не используется. Идентификатор MEG id должен иметь длину не более 15 символов.

**ICC/Domain Name** (Идентификатор ICC / Доменное имя): В зависимости от выбранного формата, введите идентификатор ITU ICC или доменное имя для обслуживания (IEEE Maintenance Domain Name).

**MEG id:** Либо ITU UMC (MEG ID значение [7-13]), либо краткое имя IEEE Short MA.

**MEP id:** В этом поле указано значение двух переданных байтов идентификатора CCM MEP ID.

**Tagged VID** (Номер тегированной VLAN): К OAM PDU будет добавлен тэг C-порта (применимо только к порту MEP).

**MEP STATE** (Состояние MEP)

**cLevel:** Индикация указывает, что принятое CCM имеет уровень меньше заданного для данного MEP.

**cMEG:** Индикация указывает, что принятое CCM имеет MEG ID, отличающийся от заданного для данного MEP.

**cMEP:** Индикация указывает, что принятое CCM имеет MEP ID, отличающийся от всех одноранговых идентификаторов 'Peer MEP ID', заданных для данного MEP.

**cAIS:** Индикация указывает, что принят AIS PDU.

**cLCK:** Индикация указывает, что принят LCK PDU.

**cSSF:** Индикация указывает, что на уровне сервера произошел отказ сигнала.

**aBLK:** Индикация указывает, что в этом потоке выполняется операция блокирования кадров обслуживания.

**aTSF:** Индикация прохождения сигнала из-за включенной защиты.

**Peer MEP Configuration** (Настройка одноранговых MEP)

Чтобы добавить новый элемент списка, нажмите кнопку “Add New Peer MEP” (Добавить новый одноранговый MEP). Чтобы удалить элемент списка из таблицы нажмите кнопку “Delete” (Удалить).

**Peer MEP ID:** Идентификатор однорангового MEP целевого MEP. Используется только, когда одноадресный MAC-адрес однорангового устройства состоит из одних нулей.

**Unicast Peer MAC** (MAC-адрес одноадресного однорангового устройства): Одноадресный MAC-адрес целевого коммутатора или устройства. Вы можете ввести одноадресный MAC-адрес в формате “xx-xx-xx-xx-xx-xx”, “xx.xx.xx.xx.xx.xx” или “xxxxxxxxxxxx”, где x – шестнадцатиричная цифра.

**ПРИМЕЧАНИЕ:** Когда задано содержимое поля “Peer MEP ID” (Идентификатор однорангового MEP), устройство может осуществлять автосогласование параметров с соседним устройством (по MAC-адресу). Поэтому, пользователь при начальном конфигурировании может задать в поле “Unicast Peer MAC” (одноадресный MAC-адрес однорангового устройства) одни нули, то есть “00-00-00-00-00-00”.

**cLOC:** Индикация указывает, что от этого однорангового узла MEP, кадр CCM принят не был (за 3,5 периода).

**cRDI:** Индикация указывает, что от этого однорангового узла MEP принят кадр CCM с индикацией дефекта удаленного узла ( Remote Defect Indication).

**cPeriod:** Индикация указывает, что от этого однорангового узла MEP принят кадр CCM с периодом, отличающимся от того, который задан для данного MEP .

**cPriority:** Индикация указывает, что от этого однорангового узла MEP принят кадр CCM с приоритетом, отличающимся от того, который задан для данного MEP.

## **Functional Configuration** (Настройка функционирования)

### **Continuity Check** (Проверка непрерывности)

**Enable** (Включить): Установите флаг в этом поле, чтобы включить проверку того, что кадры CCM PDU непрерывно передаются и принимаются. Кадры CCM PDU всегда передаются, как Multicast Class 1 (Многоадресные кадры класса 1).

**Priority** (Приоритет): В TAG (если присутствует) будет введен приоритет (как биты PCP).

**Frame rate** (Скорость передачи кадров): Выберите скорость передачи кадров CCM PDU.

### **Протокол APS**

**Enable** (Включить): Установите флаг в этом поле, чтобы включить протокол APS (Automatic Protection Switching – протокол автоматической защиты переключения).

**Priority** (Приоритет): В TAG (если присутствует) будет введен приоритет (как биты PCP).

**Cast** (Тип передачи): Выберите, как будут передаваться кадры APS PDU – как одноадресные или как многоадресные. Одноадресные MAC-адреса будут взяты из конфигурации “Unicast Peer MAC” (Одноадресные MAC-адреса одноранговых узлов). Одноадресная передача корректна только для кадров типа L-APS PDU. Кадры R-APS PDU всегда передаются с многоадресными MAC-адресами, как описано в G.8032.

**Type** (Тип): Может иметь следующие значения:

- R-APS: Кадры APS PDU, переданные как R-APS (для ERPS).
- L-APS: Кадры APS PDU, переданные как L-APS (для ELPS).

**Last Octet** (Последний октет): Последний переданный октет и ожидаемый RAPS многоадресный MAC-адрес. В G.8031 (03/2010) многоадресный RAPS MAC-адрес определен как 01-19-A7-00-00-XX. В текущем стандарте значение для этого последнего октета равно '01'; другие значения зарезервированы для использования в будущем.

Нажмите кнопку “**Fault Management**” (Управление обработкой отказов).

**Fault Management - Instance 1**

**Loop Back**

Enable	Dei	Priority	Cast	Peer MEP	Unicast MAC	To Send	Size	Interval
<input type="checkbox"/>	<input type="checkbox"/>	0	Multi	1	00-00-00-00-00-00	10	64	100

**Loop Back State**

Transaction ID	Transmitted	Reply MAC	Received	Out Of Order
1	0	00-00-00-00-00-00	0	0

**Link Trace**

Enable	Priority	Peer MEP	Unicast MAC	Time To Live
<input type="checkbox"/>	0	1	00-00-00-00-00-00	1

**Link Trace State**

Transaction ID	Time To Live	Mode	Direction	Forwarded	Relay	Last MAC	Next MAC
No Transactions							

**Test Signal**

Tx	Rx	Dei	Priority	Peer MEP	Rate	Size	Pattern	Sequence Number
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	1	1	64	All Zero	<input type="checkbox"/>

**Test Signal State**

TX frame count	RX frame count	RX rate	Test time	Clear
0	0	0	0	<input type="checkbox"/>

**Client Configuration**

Domain	Flow										
Evc	0	0	0	0	0	0	0	0	0	0	0
Level	0	0	0	0	0	0	0	0	0	0	0
AIS prio	0	0	0	0	0	0	0	0	0	0	0
LCK prio	0	0	0	0	0	0	0	0	0	0	0

**AIS**

Enable	Priority	Frame Rate	Protection
<input type="checkbox"/>	1 f/sec	<input type="checkbox"/>	

**LOCK**

Enable	Frame Rate
<input type="checkbox"/>	1 f/sec

Рис. 113. Вид меню MEP Fault Management

**Loop Back** (Тест по петле)

**Enable** (Включить): Установите флаг в этом поле, чтобы включить тест по петле (Loop Back) на основе передачи и приема LBM/LBR PDU. Тест по петле будет автоматически выключен, когда будут переданы все LBM PDU, число которых указано в столбце "To Send" (К отправке).

**Dei**: В TAG (если присутствует) будет введен DEI (как биты PCP).

**Priority** (Приоритет): В TAG (если присутствует) будет введен приоритет (как биты PCP).

**Cast** (Тип MAC-адреса): Выберите как будут передаваться кадры LBM PDU – как одноадресные или многоадресные. Одноадресные MAC-адреса будут сконфигурированы через

'Peer MEP' (Одноранговый MEP) или 'Unicast Peer MAC' (Одноранговый одноадресный MAC-адрес). Для MIP возможен только одноадресный тест по петле.

**Peer MEP** (Одноранговый MEP): Используется только в случае, если для the “Unicast MAC” (Одноадресный MAC-адрес) заданы одни нули. Одноадресные MAC-адреса LBM будут взяты из конфигурации “Unicast Peer MAC” (Одноадресные MAC-адреса одноранговых узлов) данного однорангового узла.

**Unicast MAC** (Одноадресный MAC-адрес): Используется только в том случае, если он не задан в виде одних нулей. Адрес будет использоваться как одноадресный MAC-адрес LBM PDU. Этот способ является единственным способом настройки теста по петле для MIP.

**To Send** (К отправке): Число кадров LBM PDU, отправляемых в рамках одного теста по петле. Если указано 0, то это означает бесконечную передачу (режим тестирования). Тест является аппаратным; он выполняется на основе LBM/LBR, критерием является требуемое VOE.

**Size** (Размер): Число байтов кадра LBM PDU Data Pattern TLV.

**Interval** (Интервал): Интервал между передачей кадров LBM PDU. Интервал равен 10 мс в случае, когда в поле 'To Send' (К отправке) указано значение, отличное от 0 (макс. 100 - '0' означает макс. быструю передачу). Интервал равен 1 мкс в случае, когда поле 'To Send' == 0 (макс. 10.000).

**Loop Back State** (Состояние теста по петле)

**Transaction ID** (Идентификатор транзакции): ID транзакции первого переданного кадра LBM. ID транзакции в PDU увеличивается при каждом переданном LBM.

**Transmitted** (Передано): Общее число переданных кадров LBM PDU.

**Reply MAC** (Ответный MAC-адрес): MAC-адрес отвечающего MEP/MIP. В случае многоадресных кадров LBM, ответы могут быть приняты от всех одноранговых MEP в группе. Если поле “To Send”= 0, этот MAC-адрес отображаться не будет.

**Received** (Принято): Общее число кадров LBR PDU, принятых от этого “Reply MAC” (Отвечающего MAC-адреса).

**Out of Order** (Некорректных кадров): Общее число кадров LBR PDU, принятых от этого “Reply MAC” (Отвечающего MAC-адреса) с некорректным “Transaction ID” (Идентификатор транзакции).

**Link Trace** (Трассировка линии)

**Enable** (Включить): Установите флаг в этом поле, чтобы включить трассировку линии (Link Trace) для передаваемых и принимаемых кадров LBM/LBR PDU. Трассировка линии будет автоматически отключена, когда все 5 транзакций будут выполнены с интервалами 5 секунд – 5 секунд ожидания для всех LTR в конце. Кадры LTM PDU всегда передаются, как Multicast Class 2 (Многоадресные кадры класса 2).

**Priority** (Приоритет): В TAG (если присутствует) будет введен приоритет (как биты PCP).

**Peer MEP** (Одноранговый MEP): Используется только в том случае, если для “Unicast MAC” (Одноадресный MAC-адрес) заданы одни нули. Целевые MAC-адреса трассировки линии будут взяты из конфигурации “Unicast Peer MAC” (Одноадресные MAC-адреса одноранговых узлов) данного однорангового узла.

**Unicast MAC** (Одноадресный MAC-адрес): Используется только в том случае, если он не задан в виде одних нулей. Адрес будет использоваться как одноадресный целевой MAC-адрес трассировки линии. Единственным способом конфигурирования MIP является использование целевого MAC-адреса.

**Time To Live** (Время жизни): Значение LTM PDU TTL, описанное в Y.1731. Всякий раз, когда MIP осуществляет передачу кадров (форвардинг), значение уменьшается. Когда значение TTL достигнет нуля, передача кадров PDU производиться не будет.

**Link Trace State** (Состояние трассировки линии)

**Transaction ID** (Идентификатор транзакции): Идентификатор транзакции уменьшается всякий раз, когда посылается LTM. Это значение введено в переданный LTM PDU, ожидается, что он будет принят в LTR PDU. Кадр LTR, принятый с неправильной транзакцией, игнорируется. При одной включенной трассировке линии осуществляется пять транзакций.

**Time To Live** (Время жизни): Значение TTL берется из кадра LTM, принятого MIP/MEP, пославшим данный кадр LTR – уменьшенное так, как если бы осуществлялась передача кадров.

**Mode** (Режим работы): В этом поле указано, существует ли MEP/MIP, пославший данный кадр LTR.

**Direction** (Направление): В этом поле указано, является ли MEP/MIP, пославший данный кадр LTR, входящим или исходящим.

**Relayed** (Ретранслировано): В этом поле указано, имеет ли MEP/MIP, пославший данный кадр LTR, ретранслированные или переданные LTM.

**Last MAC** (Последний MAC-адрес): Mac-адрес, идентифицирующий последнего отправителя LBM, приведшего к тому, что передан этот LTR (инициированный MEP или предыдущим MIP).

**Next MAC** (Следующий MAC-адрес): Mac-адрес, идентифицирующий следующего отправителя LBM, приведшего к тому, что передан этот LTR (передача MIP или терминирование MEP).

#### **Test Signal** (Тестовый сигнал)

**Tx/Rx**: Включает или выключает тестовый сигнал, отправку и прием кадров TST PDU.

**Dei**: В TAG (если присутствует) будет введен DEI (как биты PCP).

**Priority** (Приоритет): В TAG (если присутствует) будет введен приоритет (как биты PCP).

**Peer MEP** (Одноранговый MEP): MAC-адреса назначения кадра TST будут взяты из конфигурации "Unicast Peer MAC" (Одноадресные MAC-адреса одноранговых узлов) данного однорангового узла.

**Rate** (Скорость): Скорость передачи кадра TST – в Мбит/с. Предельная скорость на Caracal: 400 Мбит/с. Предельная скорость на Serval: 1 Гбит/с.

**Size** (Размер): Размер кадра TST. Вводится, как желаемый размер (в байтах) нетегированного кадра, содержащего TST OAM PDU, в том числе и четыре байта контрольной суммы CRC.

**Pattern** (Шаблон): 'Пустой' кадр TST PDU имеет размер 12 байтов. Чтобы достичь заданного размера кадра, в шаблон будут добавлены кадры TLV.

- All Zero (Все нули): Шаблон имеет вид 00000000
- All One (Все единицы): Шаблон имеет вид 11111111
- 10101010: Шаблон имеет вид 10101010

**Sequence Number** (Числовая последовательность): Включает функцию числовой последовательности.

#### **Test Signal State** (Состояние тестового сигнала)

**TX frame count** (Передано кадров): Число переданных кадров TST с момента последней очистки.

**RX frame count** (Принято кадров): Число принятых кадров TST с момента последней очистки.

**RX rate** (Скорость приема): Скорость передачи принятого кадра TST, измеренная в 100 кбит/с. Вычисляется на интервалах длительностью 1 секунда, начиная с первого принятого кадра TST после очистки. В качестве размера кадра при этом вычислении используется размер первого кадра, принятого после очистки.

**Test time** (Время теста): Число секунд, прошедшее с момента первого приема кадра TST после последней очистки.

**Clear** (очистка): Очистка состояния тестового сигнала. Передача кадра TST будет начата снова. После того, как будет принят первый кадр, начнут вычисляться значения в полях 'Rx frame count' (Принято кадров), 'RX rate' (Скорость приема кадров) и 'Test time' (Время теста).

#### **Client Configuration** (Настройка клиента)

**Domain** (Домен): Домен слоя клиента. Он должен быть EVC.

**Level** (Уровень): Уровень клиентского слоя, означающий, что кадр PDU, переданный в клиентском слое, останется на этом уровне.

**Flow** (Поток): Номера копий потоков клиентского слоя. Они должны быть заданы только для порта MEP.

#### **AIS**

**Enable** (Включить): Включает или выключает ввод AIS-сигнала (передача AIS PDU) в потоки клиентского слоя.

**Priority** (Приоритет): На Caracal этот приоритет используется в исходящем направлении (клиентский слой). На Serval для каждого клиента EVC используется наивысший COS-ID (класс ECE).

**Frame rate** (Скорость передачи кадров): Выберите скорость передачи кадров AIS PDU. Скорость передачи обратно пропорциональна периоду (см. Y.1731).

**Protection** (Защита): Установите флаг в этом поле, чтобы включить защиту. Это означает, что первые 3 AIS PDU будут переданы как можно скорее – в случае использования этого средства для защиты в конечной точке.

### Lock

**Enable** (Включить): Включает или выключает ввод запирающего LOCK-сигнала (передача LCK PDU) в потоки клиентского слоя.

**Priority** (Приоритет): В направлении источника MEP вводится приоритет. На Caracal этот приоритет также используется в исходящем направлении (клиентский слой). На Serval для каждого клиента EVC используется наивысший COS-ID (класс ECE).

**Frame rate** (Скорость передачи кадров): Выберите скорость передачи кадров LCK PDU. Скорость передачи обратно пропорциональна периоду (см. Y.1731).

Нажмите кнопку **“Performance Monitoring”** (Мониторинг производительности).

Performance Monitoring Data Set

**Enable**

Loss Measurement

Enable	Priority	Frame rate	Cast	Ended	FLR Interval
<input type="checkbox"/>	0	1 f/sec	Multi	Single	5

Loss Measurement State

Tx	Rx	Near End Loss Count	Far End Loss Count	Near End Loss Ratio	Far End Loss Ratio	Available Time	Unavailable Time	Clear
0	0	0	0	0	0	0	0	<input type="checkbox"/>

Delay Measurement

Enable	Priority	Cast	Peer MEP	Way	Tx Mode	Calc	Gap	Count	Unit	D2forD1	Counter Overflow Action
<input type="checkbox"/>	0	Multi	1	Two-way	Standardize	Flow	10	10	us	<input type="checkbox"/>	Keep

Delay Measurement State

	Tx	Rx	Rx Timeout	Rx Error	Av Delay Tot	Av Delay last N	Delay Min.	Delay Max.	Av Delay-Var Tot	Av Delay-Var last N	Delay-Var Min.	Delay-Var Max.	Overflow	Clear
One-way														
F-to-N	0	0	0	0	0	0	0	0	0	0	0	0	0	
N-to-F	0	0	0	0	0	0	0	0	0	0	0	0	0	
Two-way	0	0	0	0	0	0	0	0	0	0	0	0	0	<input type="checkbox"/>

F-to-N :Far-end-to-near-end  
 N-to-F :Near-end-to-far-end

Рис. 114. Вид меню MEP Performance Monitoring

**Loss Measurement/Loss Measurement State** (Измерение потерь / Состояние измерения потерь)

**Enable** (Включить): Измерение потерь основано на передаче / приеме кадров CCM или LMM/LMR PDU, которое может быть включено (флаг установлен) или выключено (флаг снят) – см. также раздел 'Ended' (Тип измерения потерь – на одном конце или на двух концах). Все это правильно только тогда, когда сконфигурирован один одноранговый MEP.

**Priority** (Приоритет): В TAG (если присутствует) будет введен приоритет (как биты PCP). В случае, когда Continuity Check (Проверка непрерывности) и измерение потерь реализованы на программном CCM и включены, приоритет должен быть одинаковым на обеих сторонах.

**Frame rate** (Скорость передачи кадров): Выберите скорость передачи кадров CCM/LMM PDU. Скорость передачи обратно пропорциональна периоду (см. Y.1731). Выбор 300 кадров/с или 100 кадров/с является неправильным. В том случае, когда Continuity Check (Проверка непрерывности) и измерение потерь реализованы на программном CCM, скорость передачи кадров должна быть одной и той же на обеих сторонах.

**Cast** (Тип MAC-адреса): Выберите, как будут передаваться кадры CCM или LMM PDU – с одноадресными адресами или с многоадресными. Одноадресные MAC-адреса будут взяты из конфигурации “Unicast Peer MAC” (Одноадресные MAC-адреса одноранговых узлов). В том случае, когда Continuity Check (Проверка непрерывности) и измерение потерь на двух концах включены и реализованы на программном CCM, тип MAC-адреса на обеих сторонах должен быть одинаковым.

**Ended** (Тип измерения потерь – на одном конце или на двух концах):

- Single (На одном конце): Измерение потерь на одном конце, реализованное на LMM/LMR.
- Dual (На двух концах): Измерение потерь на двух концах реализовано на CCM с помощью программного обеспечения.

**FLR Interval** (Интервал FLR): Интервал в секундах, на котором вычисляется коэффициент потерь кадров (Frame Loss Ratio).

**Loss Measurement State** (Состояние измерения потерь)

**Near End Loss Count** (Акумулированное число кадров, потерянных на ближнем конце): Акумулированное значение счетчика кадров, потерянных на ближнем конце (с момента последней очистки).

**Far End Loss Count** (Акумулированное число кадров, потерянных на дальнем конце): Акумулированное значение счетчика кадров, потерянных на дальнем конце (с момента последней очистки).

**Near End Loss Ratio** (Коэффициент потерь для кадров, потерянных на ближнем конце): Коэффициент потерь кадров, потерянных на ближнем конце вычисляется по показанию аккумулируемого счетчика кадров, потерянных на ближнем конце и числу кадров, переданных на дальнем конце на последнем интервале FLR. Результат представлен в процентах.

**Far End Loss Ratio** (Коэффициент потерь для кадров, потерянных на дальнем конце): Коэффициент потерь кадров, потерянных на дальнем конце вычисляется по показанию аккумулируемого счетчика кадров, потерянных на дальнем конце и числу кадров, переданных на ближнем конце на последнем интервале FLR. Результат представлен в процентах.

**Clear** (очистка): После того, как в этом поле будет установлен флаг и выполнено сохранение, аккумулируемые счетчики будут очищены и вновь начнется вычисление коэффициента потерь.

**Delay Measurement** (Измерение задержки)

**Enable** (Включить): Установите флаг в этом поле, чтобы включить измерение задержки на основе передачи кадров 1DM/DMM PDU. Измерение задержки, основанное на приеме и обработке кадров 1DM/DMR PDU уже включено.

**Priority** (Приоритет): В TAG (если присутствует) будет введен приоритет (как биты PCP).

**Cast** (Тип MAC-адреса): Выберите, как будет передаваться кадр 1DM/DMM PDU – с одноадресными адресами или с многоадресными. Одноадресный MAC-адрес будет сконфигурирован с помощью 'Peer MEP' (Одноранговый MEP).

**Peer MEP** (Одноранговый MEP): Используется только тогда, когда 'Cast' (Тип адреса) имеет значение Uni. Одноадресные MAC-адреса кадра 1DM/DMR будут взяты из конфигурации “Unicast Peer MAC” (Одноадресные MAC-адреса одноранговых узлов) данного однорангового узла.

**Way** (Число сторон): Измерения задержки будут выполнены при односторонней передаче кадра 1 DM или DMM/DMR соответственно, либо при его двухсторонней передаче.

**Tx Mode** (Режим передачи):

- Standardize (Стандартный): Способ передачи 1 кадра DM/DMR по стандарту Y.1731.
- Proprietary (Фирменный): Наш собственный способ сборки пакетов для передачи 1 кадра DM/DMR.

**Calc**: Используется только тогда, когда 'Way' (Число сторон) имеет значение Two-way (Две стороны).

- Round trip (Задержка передачи туда и обратно): Задержка кадра, вычисленная по временным меткам инициаторов приема и передачи. Задержка кадра = RxTimeb-TxTimeStampf

- **Flow (Поток):** Задержка кадра, вычисленная по временным меткам инициаторов приема и передачи и удаленных узлов. Задержка кадра = (RxTimeb-TxTimeStamp)-(TxTimeStamp-RxTimeStamp)

**Gap (Промежуток):** Промежуток между передачей 1 кадра DM/DMM PDU составляет 10 мс. Диапазон значений: от 10 до 65535.

**Count (Счетчик):** Число последних записей, подлежащих вычислению. Диапазон значений: от 10 до 2000.

**Unit (Единицы измерения):** Разрешение по времени.

**D2forD1:** Позволяет использовать пакет DMM/DMR для вычисления односторонней задержки. Если в данном поле установлен флаг, будет выполнена следующая операция. Когда принят кадр DMR, вычисляется двухсторонняя задержка (туда и обратно, либо для потока), а также односторонние задержки near-end-to-far-end (от ближнего конца до дальнего конца) и far-end-to-near-end (от дальнего конца до ближнего конца). Когда принят кадр DMM или 1DM, вычисляется только односторонняя задержка far-end-to-near-end (от дальнего конца до ближнего конца).

**Counter Overflow Action (Операция при переполнении счетчика):** Операция, выполняемая со счетчиком при переполнении.

**Delay Measurement State (Состояние измерения задержки)**

**Tx:** Аккумулированный счетчик на стороне передачи (с момента последней очистки).

**Rx Timeout (Время ожидания приема):** Аккумулированный счетчик интервалов времени ожидания на стороне приема (с момента последней очистки).

**Rx:** Аккумулированный счетчик на стороне приема (с момента последней очистки).

**Rx Error (Ошибок на приеме):** Аккумулированное число ошибок на стороне приема (с момента последней очистки). Задержка кадра более 1 секунды (время ожидания).

**Average Total (Общее среднее значение):** Средняя задержка с момента последней очистки. Единицы измерения: микросекунды.

**Average last N (Среднее значение для последних N пакетов):** Средняя задержка для последних n пакетов – с момента последней очистки. Единицы измерения: микросекунды.

**AverageVariation Total (Общее отклонение от среднего значения):** Отклонение от средней задержки с момента последней очистки. Единицы измерения: микросекунды.

**Average Variation last N (Среднее отклонение для последних N пакетов):** Отклонение от средней задержки для последних n пакетов с момента последней очистки. Единицы измерения: микросекунды.

**Min.:** Минимальная задержка с момента последней очистки. Единицы измерения: микросекунды.

**Max.:** Максимальная задержка с момента последней очистки. Единицы измерения: микросекунды.

**Overflow (Переполнение):** Число переполнений счетчика с момента последней очистки.

**Clear (очистка):** Установите флаг в этом поле и сохраните настройку – все аккумулированные счетчики будут очищены.

## 2.9.5 ERPS

Протокол защиты коммутации в кольце Ethernet ERPS (Ethernet Ring Protection Switching), определенный в ITU-T G.8032, реализует механизм защиты коммутации Ethernet-трафика в сети с кольцевой топологией. Функция ERPS позволяет избежать потенциально возможных петель в сети за счет блокирования трафика на линии защиты кольца RPL (ring protection link).

В кольцевой топологии, в которой функционирует ERPS, один (и только один) коммутатор назначается владельцем RPL (RPL-owner), ответственным за блокирование трафика в ней, что позволяет избежать петель. Коммутатор, соседний с RPL-owner называется соседним RPL-узлом (neighbor) и в нормальных условиях работы отвечает за блокирование RPL со своего конца. Остальные коммутаторы, соседние с RPL-owner или соседние по кольцу являются членами кольца или узлами, соседними с соседним RPL-узлом и нормально передают принятый трафик.

Порты кольца периодически используют управляющие сообщения автоматической защиты коммутации кольца (Ring Automatic Protection Switching message), гарантирующие, что кольцо не содержит петель. Если RPL-owner не получает пакетов опроса или обучается пакетам обнаружения отказа, он регистрирует сигнал отказа SF (signal failure) в кольце (обрыв связи). При



обучении пакету отказа, RPL-owner разблокирует линию защиты кольца RPL, разрешая трафик по защищенному VLAN.

ERPS, подобно STP, обеспечивает отсутствие петель в сети, используя пакеты опроса для обнаружения отказов. Однако, когда происходит отказ, ERPS самовосстанавливается, посылая трафик по защищенному обратному маршруту вместо выполнения вычислений для обнаружения маршрута для передачи пакетов. Вследствие использования такого механизма обнаружения отказов, ERPS обеспечивает малое время сходимости (менее 50 мс) и быстрое восстановление передачи трафика.

Ethernet Ring Protection Switching													Refresh
Delete	ERPS ID	Port 0	Port 1	Port 0 APS MEP	Port 1 APS MEP	Port 0 SF MEP	Port 1 SF MEP	Ring Type	Interconnected Node	Virtual Channel	Major Ring ID	Alarm	
<input type="checkbox"/>	1	8	9	1	2	1	2	Major	No	No	1		

Рис. 115. Вид меню ERPS

**ERPS ID:** Задайте идентификатор ID для этой группы.

**Port 0** (Порт 0): Port 0 имеет и другое название - порт E (или Восточный порт). Это название используется некоторыми другими изготовителями аппаратуры. Задайте восточный порт коммутатора кольца.

**Port 1** (Порт 1): Port 1 имеет и другое название - порт W (или Западный порт). Это название используется некоторыми другими изготовителями аппаратуры. Когда данный порт соединен с другим суб-кольцом, "0" указанный в этом поле означает, что не существует западного порта, ассоциированного с данной копией протокола. Задайте западный порт коммутатора кольца.

**Port 0 APS MEP:** Задайте MEP, обрабатывающий кадры восточного порта (East APS PDU).

**Port 1 APS MEP:** Задайте MEP, обрабатывающий кадры западного порта (West APS PDU). Когда данный порт соединен с другим суб-кольцом, "0" указанный в этом поле означает, что не существует западного APS MEP, ассоциированного с данной копией протокола.

**Port 0 SF MEP:** Имеет и другое название: East Signal Fail APS MEP. Назначьте в этом поле MEP, посылающий кадры East Signal Fail (Отказ сигнала восточного порта).

**Port 1 SF MEP:** Имеет и другое название: West Signal Fail APS MEP. Когда данный порт соединен с другим суб-кольцом, "0" указанный в этом поле означает, что не существует западного SF MEP, ассоциированного с данной копией протокола. Назначьте в этом поле MEP, посылающий кадры West Signal Fail (Отказ сигнала западного порта).

**Ring Type** (Тип кольца): Выберите тип защитного кольца, которое может иметь тип "major" (основное), либо "sub" (суб-кольцо).

**Interconnected Node** (Узел межсоединения): Установите флаг в этом поле, чтобы указать, что для данной копии протокола этот узел работает в режиме interconnection node.

**Virtual Channel** (Виртуальный канал): На узле межсоединения (interconnected) суб-кольца могут иметь виртуальный канал либо не иметь его. Установите флаг в этом поле, если данная копия содержит узел межсоединения с виртуальным каналом. Если суб-кольцо не имеет виртуального канала, оставьте это поле пустым, без флага.

**Major Ring ID** (Идентификатор основного кольца): Это поле используется при межсоединительном суб-кольце для отправки обновлений изменений топологии на основное кольцо. Если выбрано основное кольцо, это значение совпадает с ID группы защиты данного кольца.

**Alarm** (Сигнализация): Когда настройка будет завершена, коммутатор выведет в окне браузера состояние сигнализации по ERPS.

Чтобы добавить новый элемент списка, нажмите кнопку "Add New Protection Group" (Добавить новую группу защиты). Чтобы удалить новый элемент списка из таблицы нажмите кнопку "Delete" (Удалить). Щелкните "Save" (Сохранить), чтобы сохранить изменения. Щелкните "Reset" (Переустановить), чтобы отменить любые изменения, сделанные локально и восстановить ранее сохраненные значения, которые будут назначаться по умолчанию.

Нажмите кнопку "Refresh" (Обновить), чтобы вручную обновить информацию ERPS.

## 2.10 IPMC Profile (Профиль IPMC)

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

"IPMC Profile" содержит два подчиненных меню, которые описаны ниже.



Рис. 116. Вид меню IPMC Profile

### 2.10.1.1 Profile Table (Таблица профиля)

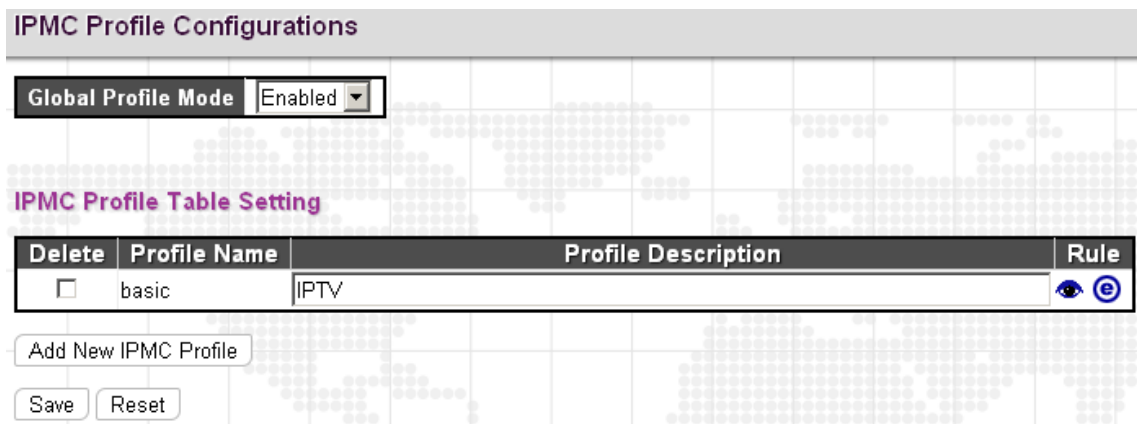


Рис. 117. Вид меню IPMC Profile – Profile Table

#### IPMC Profile Configuration (Настройка профиля IPMC)

**Global Profile Mode** (Глобальный режим работы профиля): Позволяет включить (Enable) или выключить (disable) функцию IPMC Profile глобально.

#### IPMC Profile Table Setting (Настройка таблицы профиля IPMC)

**Profile Name** (Имя профиля): Введите имя для данного профиля.

**Profile Description** (Описание профиля): Введите краткое описание для данного профиля.

Чтобы ввести новый элемент в таблицу, нажмите кнопку "Add New IPMC Profile" (Добавить новый профиль IPMC). Чтобы удалить элемент таблицы, установите флаг в поле "Delete" (Удалить). Чтобы отредактировать дополнительные настройки профиля, нажмите кнопку "e".

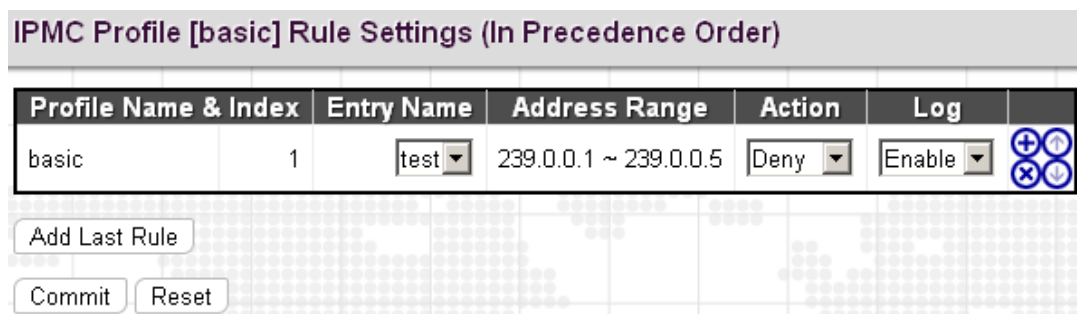


Рис. 118. Вид меню IPMC Profile – Rule Settings

**Profile Name & Index** (Имя и индекс профиля): Отображается имя и индекс профиля.

**Entry Name** (Имя элемента): Имя, используемое при указании диапазона адресов. В раскрывающемся меню можно выбрать только существующие адреса профилей.

**Address Range** (Диапазон адресов): Задайте диапазон многоадресных IP-адресов.  
Доступный диапазон IP-адресов: от 224.0.0.0 до 239.255.255.255

**Action** (Операция): Выберите операцию, которая выполняется при приеме кадра Join/Report (Вступить/Сообщить), который имеет групповой адрес, совпадающий с диапазоном адресов правила.

- Permit (Разрешить): Будет изучен групповой адрес, совпадающий с диапазоном адресов, заданным в правиле.
- Deny (Запретить): Будет отброшен групповой адрес, совпадающий с диапазоном адресов, заданным в правиле.

**Log** (Журнал): Выберите предпочтение регистрации в журнале принятого кадра Join/Report (Вступить / Сообщить), который имеет групповой адрес, совпадающий с диапазоном адресов правила.

- Enable (Включить): В журнале будет зарегистрирована соответствующая информация о групповом адресе, совпадающего с диапазоном адресов, указанным в правиле.
- Disable: В журнале не будет зарегистрирована соответствующая информация о групповом адресе, совпадающего с диапазоном адресов, указанным в правиле.

Управление правилами и порядком приоритетов может осуществляться при помощи следующих кнопок:

«+»: Ввод нового правила перед текущим правилом.

«x»: Удаление текущего правила.

«↑»: Перемещение текущего правила вверх по списку.

«↓»: Перемещение текущего правила вниз по списку.

Пример использования через CLI:

```
ipmc profile basic
description IPTV
range test deny log
!
ipmc profile
```

### 2.10.1.2 Address entry (Диапазоны адресов)

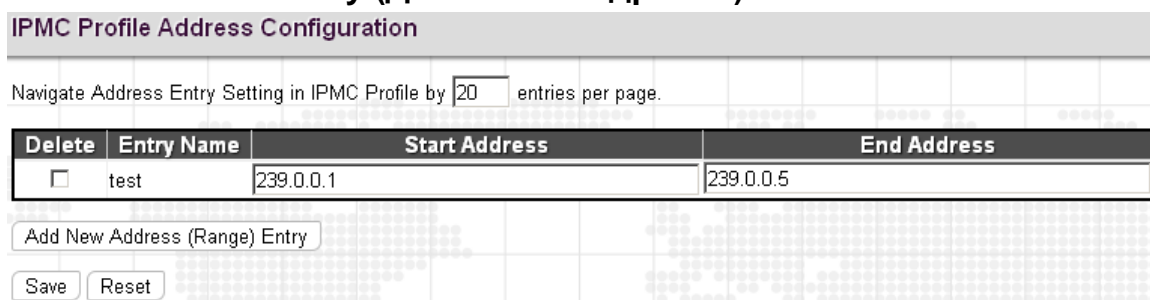


Рис. 119. Вид меню IPMC Profile – Address Entry

**Entry Name** (Имя элемента): Введите имя, которое будет использоваться для индексации диапазона адресов.

**Start Address** (Начальный адрес): Введите в этом поле начальный адрес диапазона многоадресных адресов (IPv4 или IPv6).

**End Address** (Конечный адрес): Введите в этом поле конечный адрес диапазона многоадресных адресов (IPv4 или IPv6).

Чтобы ввести новый элемент, нажмите кнопку "Add new Address (Range) Entry" (Добавить новый адрес входа (из диапазона адресов)). Установите флаг в поле "Delete" (Удалить), чтобы удалить элемент во время следующего сохранения.

Пример использования через CLI:

```
ipmc range test 239.0.0.1 239.0.0.5
```

## 2.11 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).

Меню “MVR” содержит подчиненные меню, которые описаны ниже.



Рис. 120. Вид меню MVR

### 2.11.1.1 Configuration (Настройка)

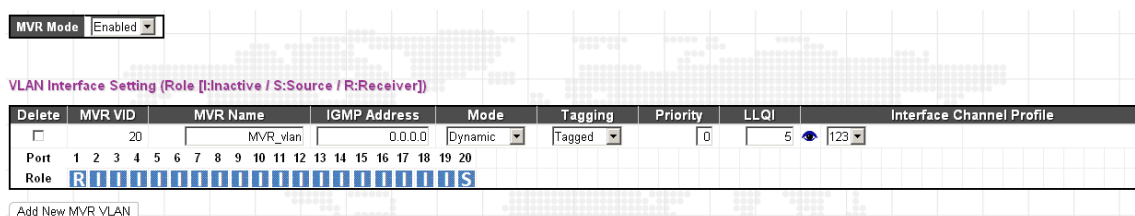


Рис. 121. Вид меню MVR – Configurations

#### MVR Configurations (Настройка MVR)

**MVR Mode** (Режим работы MVR): Позволяет включить (Enable) или выключить (disable) функцию MVR глобально на данном устройстве. Любые многоадресные данные от портов источника будут посылаются на ассоциированные с ними порты приемников, зарегистрированные в таблице. По умолчанию, функция MVR выключена.

#### VLAN Interface Setting (Настройка интерфейса VLAN)

**MVR ID:** 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** (Имя MVR): Дополнительно можно задать имя, определенное пользователем для данной многоадресной VLAN. Максимальная длина строки имени MVR равна 32. Разрешается использовать и буквы, и цифры.

**IGMP Address** (Адрес IGMP): Задайте одноадресный IPv4-адрес в качестве адреса источника, используемого в заголовке IP кадров управления IGMP.

**Mode** (Режим работы): 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** (Тегирование): Задайте, следует ли при отправке помечать тегами MVR VID кадры управления IGMP/MLD либо их следует отправлять без тегов.

**Priority** (Приоритет): 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 Profile** (Профиль канала интерфейса): Выберите профиль IPMC из раскрывающегося меню. Нажмите кнопку (\*), чтобы просмотреть сводную информацию о выбранных настройках профиля IPMC.

**Port Role** (Роль порта): Нажмите на значок роли порта, чтобы изменить состояние роли.

- **Inactive (I)** (Неактивный): По умолчанию, все порты неактивны. Неактивные порты не 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. Пожалуйста, 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** (Порт): Номер порта. Правило "Port \*" означает применение ко всем портам.

**Immediate Leave** (Немедленный выход из группы): 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.

Пример использования через CLI:

```
mvr
mvr vlan 20 name MVR_vlan
mvr name MVR_vlan channel 123
ip igmp snooping vlan 1
!
interface FastEthernet 1/1
  mvr immediate-leave
  mvr name MVR_vlan type receiver
!
interface GigabitEthernet 1/4
  mvr name MVR_vlan type source
```

### 2.11.1.2 MVR Statistics (Статистика MVR)

На этой странице отображается статистика MVR по очередям, сообщениям о вступлении и выходе из группы, сообщениям с отчетами.

MVR Statistics						
VLAN ID	IGMP/MLD Queries Received	IGMP/MLD Queries Transmitted	IGMPv1 Joins Received	IGMPv2/MLDv1 Reports Received	IGMPv3/MLDv2 Reports Received	IGMPv2/MLDv1 Leaves Received
20	0/0	0/0	0	0/0	0/0	0/0

Рис. 122. Вид меню MVR – Statistics

**VLAN ID:** Отображается номер VLAN, используемой для обработки многоадресного трафика.

**IGMP/MLD Queries Received** (Принято запросов IGMP/MLD): Число принятых запросов IGMP и MLD.

**IGMP/MLD Queries Transmitted** (Передано запросов IGMP/MLD): Число переданных запросов IGMP/MLD.

**IGMPv1 Joins Received** (Принято сообщений о вступлении IGMPv1) : Число принятых сообщений о вступлении в группу IGMPv1.

**IGMPv2/MLDv1 Reports Received** (Принято отчетов IGMPv2/MLDv1): Число принятых отчетов IGMPv2 и MLDv1.

**IGMPv3/MLDv2 Reports Received** (Принято отчетов IGMPv3/MLDv2) : Число принятых отчетов IGMPv3 и MLDv2.

**IGMPv2/MLDv1 Reports Received** (Принято отчетов IGMPv2/MLDv1): Число принятых сообщений о выходе из группы (IGMPv2 и MLDv1).

### 2.11.1.3 MVR Channel Groups (Группы канала MVR)

В таблице отображается информация каналов (групп) MVR, которые отсортированы по VLAN ID.

MVR Channels (Groups) Information																								
Start from VLAN		<input type="text" value="1"/>	and Group Address		<input type="text"/>															with		<input type="text" value="20"/>	entries per page.	
VLAN ID	Groups	Port Members																						
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20			
No more entries																								

Рис. 123. Вид меню MVR – Channel Groups

Start from VLAN (Начать с VLAN)\_\_\_\_ and Group Address (и адреса группы) \_\_\_\_\_ with 20 entries per page (выводить по 20 строк на странице).

**VLAN ID:** Номер VLAN группы.

**Groups** (Группы): Group ID (Идентификаторы групп).

**Port Members** (Порты-члены группы): Порты, которые принадлежат данной группе.

### 2.11.1.4 MVR SFM Information (Информация MVR SFM)

MVR SFM Information								
Start from VLAN		<input type="text" value="1"/>	and Group Address		<input type="text"/>		with	
VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch		
No more entries								

Рис. 124. Вид меню MVR – SFM Information

**VLAN ID:** Номер VLAN группы.

**Group** (Группа): Адрес группы.

**Port** (Порт): Номер порта коммутатора.

**Mode** (Режим работы): Указан режим фильтрации (VLAN ID, номер порта, адрес группы). Режим работы может иметь значение Include (Включить) либо Exclude (Исключить).

**Source Address** (Адрес источника): IP-адрес источника. В настоящее время система использует не более 128 IP-адресов источника при фильтрации.

**Type** (Тип): Указан тип. Он может иметь значение Allow (Разрешить) либо Deny (Запретить).

**Hardware Filter/Switch** (Аппаратный фильтр/коммутатор): Указано, может ли плоскость данных, назначенная конкретному адресу группы от IPv4/IPv6-адреса источника обрабатываться специализированной БИС или нет.

## 2.12 IPMC

Меню “IPMC” содержит подчиненные меню IGMP Snooping и MLD Snooping, описанные ниже. Чтобы выполнить детальную настройку выберите соответствующее меню.

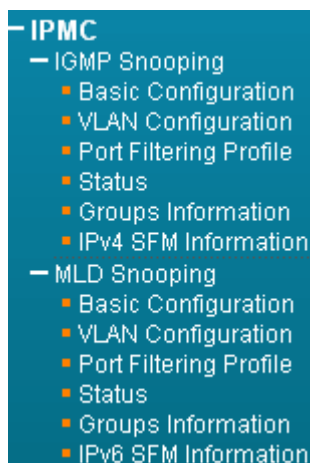


Рис. 125. Вид меню IPMC

### 2.12.1 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.

#### 2.12.1.1 Basic Configuration (Основные настройки)

**IGMP Snooping Configuration**

Global Configuration	
Snooping Enabled	<input checked="" type="checkbox"/>
Unregistered IPMCv4 Flooding Enabled	<input checked="" type="checkbox"/>
IGMP SSM Range	232.0.0.0 / 8
Leave Proxy Enabled	<input checked="" type="checkbox"/>
Proxy Enabled	<input type="checkbox"/>

**Port Related Configuration**

Port	Router Port	Fast Leave	Throttling
*	<input type="checkbox"/>	<input type="checkbox"/>	<>
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	5

Рис. 126. Вид меню IPMC - IGMP Snooping - Basic Configuration

### IGMP Snooping Configuration

#### Global Configuration (Настройки IGMP Snooping (Глобальные настройки))

**Snooping Enabled** («Прослушивание» включено): Установите флаг в этом поле, 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** (Включена передача незарегистрированного трафика IPMCv4): 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 адресов IGMP SSM): Диапазон многоадресных адресов для конкретного источника SSM (Source-Specific Multicast), позволяющий поддерживающим SSM хостам и маршрутизаторам выполнять модель услуг SSM для групп в заданном диапазоне адресов.

**Leave Proxy Enabled** (Включен прокси-сервер сообщений о выходе из группы): 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.

**Proxy Enabled** (Прокси-сервер включен): Когда прокси-сервер включен, коммутатор выполняет операцию, подобную рассмотренной в документе "IGMP Snooping with Proxy Reporting" (IGMP Snooping с прокси-сервером сообщений отчетов) - DSL Forum TR-101, April 2006 (DSL форум, TR-101, апрель 2006).

#### Port Related Configuration (Настройки, связанные с портом)

**Port (Порт):** Номер порта.



**Router Port** (Порт маршрутизатора): 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** (Быстрый выход из группы): 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 IGMP GS на этот интерфейс.

**Throttling** (Регулирование): 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 IGMP о вступлении в группу будут отбрасываться. По умолчанию выбрано неограниченное число групп (unlimited). Допустимый диапазон значений от 1 до 10.

Пример использования через CLI:

```
ip igmp host-proxy leave-proxy
ip igmp snooping
!
interface GigabitEthernet 1/2
 ip igmp snooping max-groups 5
 ip igmp snooping mrouter
 ip igmp snooping immediate-leave
```

## 2.12.1.2 VLAN Configuration (Настройка VLAN)

Эта страница используется для настройки IGMP Snooping интерфейса.

IGMP Snooping VLAN Configuration

Start from VLAN  with  entries per page.

Delete	VLAN ID	Snooping Enabled	Querier Election	Querier Address	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
<input type="checkbox"/>	20	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0.0.0.0	IGMP-Auto	0	2	125	100	10	1

Рис. 127. Вид меню IPMC - IGMP Snooping - VLAN Configuration

Чтобы добавить новый элемент списка, нажмите кнопку “Add New IGMP VLAN” (Добавить новую IGMP VLAN).

**VLAN ID:** Задайте номер VLAN, используемой для IGMP snooping.

**Snooping Enabled** («Прослушивание» включено): 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. 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** (Выбор порта запросов): 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** (Адрес querier): Задайте одноадресный IPv4-адрес, используемый в 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** (Совместимость): 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 указан уровень приоритета кадра управления IGMP, сгенерированный системой, которая используется 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 (sec):** В поле Query Interval (Интервал между запросами) указан интервал времени между отправкой запросом 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 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.

Пример использования через CLI:

```
interface vlan 20
  no ip address
  ip igmp snooping
  ip igmp snooping querier election
  ip igmp snooping compatibility auto
  ip igmp snooping priority 0
  ip igmp snooping robustness-variable 2
  ip igmp snooping query-max-response-time 100
  ip igmp snooping query-interval 125
  ip igmp snooping last-member-query-interval 10
  ip igmp snooping unsolicited-report-interval 1
```

### 2.12.1.3 Port Filtering Profile (Профиль фильтрации порта)

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

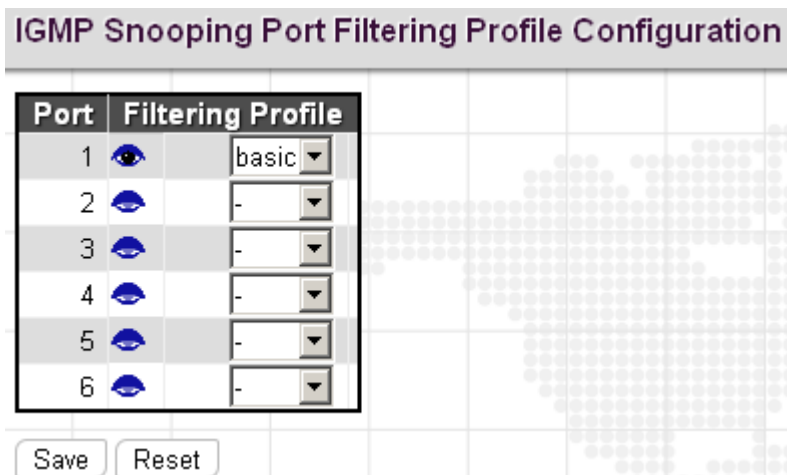


Рис. 128. Вид меню IPMC - IGMP Snooping - Port Filtering Profile

**Port** (Порт): Номер порта.

**Filtering Profile** (Профиль порта): 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.

Нажмите кнопку (\*), чтобы просмотреть подробную информацию о выбранных настройках профиля IPMC.

### 2.12.1.4 Status (Состояние)

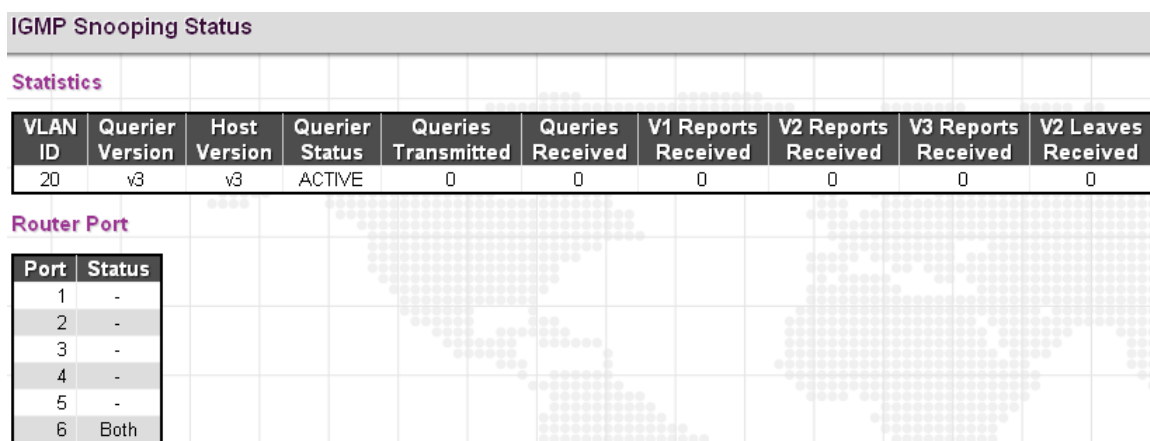


Рис. 129. Вид меню IPMC - IGMP Snooping - Status

**Statistics** (Статистика)

**VLAN ID**: Номер VLAN для данного элемента списка.

**Querier Version** (Версия запросчика): Текущая работающая версия запросчика.

**Host Version** (Версия хоста): Текущая версия хоста.

**Querier Status** (Состояние запросчика): Отображается состояние запросчика. Возможны следующие состояния: "ACTIVE" (активен) или "IDLE" (свободен). Состояние "DISABLE" (выключен) означает, что конкретный интерфейс выключен администратором сети.

**Queries Transmitted** (Передано запросов): Число переданных запросов.

**Queries Received** (Принято запросов): Число принятых запросов.

**V1 Reports Received** (Принято отчетов V1): Число принятых отчетов V1.

**V2 Reports Received** (Принято отчетов V2): Число принятых отчетов V2.

**V3 Reports Received** (Принято отчетов V3): Число принятых отчетов V3.

**V2 Leaves Received** (Принято выходов из группы V2): Число принятых сообщений выхода из группы для версии протокола V2.

**Router Port** (Порт маршрутизатора)

**Port** (Порт): Номер порта.

**Status** (Состояние): Указано, является ли конкретный порт портом маршрутизатора или нет.

### 2.12.1.5 Groups Information (Информация о группе)

IGMP Snooping Group Information

Start from VLAN  and group address

		Port Members					
VLAN ID	Groups	1	2	3	4	5	6
No more entries							

Рис. 130. Вид меню IPMC - IGMP Snooping - Groups Information

**VLAN ID:** Отображается номер VLAN группы.

**Groups** (Группы): Отображается адрес группы.

**Port Members** (Порты-участники группы): Порты, которые принадлежат данной группе.

ПРИМЕЧАНИЕ: Максимальное число групп IGMP Snooping, которые могут быть получены обучением, составляет 32.

### 2.12.1.6 IPv4 SFM Information (Информация IPv4 SFM)

IGMP SFM Information

Start from VLAN  and Group  with  entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

Рис. 131. Вид меню IPMC - IGMP Snooping - IPv4 SFM Information

**VLAN ID:** Отображается номер VLAN группы.

**Groups** (Группы): Отображается IP-адрес многоадресной группы.

**Port** (Порт): Номер порта коммутатора.

**Mode** (Режим работы): Указан режим фильтрации для каждого VLAN ID, номера порта и адреса группы.

**Source Address** (Адрес источника): IP-адрес источника, доступный для фильтрации.

**Type** (Тип): Отображается тип: Allow (Разрешить) или Deny (Запретить).

**Hardware Filter/Switch** (Аппаратный фильтр/коммутатор): Указано, может ли плоскость данных, назначенная конкретному адресу группы от IPv4-адреса источника обрабатываться специализированной БИС или нет.

### 2.12.2 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.

## 2.12.2.1 Basic Configuration (Основные настройки)

### IGMP Snooping Configuration

Global Configuration	
Snooping Enabled	<input checked="" type="checkbox"/>
Unregistered IPMCv4 Flooding Enabled	<input checked="" type="checkbox"/>
IGMP SSM Range	232.0.0.0 / 8
Leave Proxy Enabled	<input checked="" type="checkbox"/>
Proxy Enabled	<input type="checkbox"/>

### Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	<input type="checkbox"/>	<input type="checkbox"/>	<>
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	5

Рис. 132. Вид меню IPMC - MLD Snooping - IPv4 SFM Information

### MLD Snooping Configuration

#### Global Configuration (Настройки MLD Snooping (Глобальные настройки))

**Snooping Enabled** («Прослушивание» включено): Установите флаг в этом поле, 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 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 IPMCv6 Flooding Enabled** (Включена передача незарегистрированного трафика IPMCv6): 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.

**MLD SSM Range** (Диапазон адресов MLD SSM): 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** (Включен прокси-сервер сообщений о выходе из группы): 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 прокси-сервера для сообщений о выходе из группы работать не будет.

**Proxy Enabled** (Прокси-сервер включен): 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 (Порт):** Номер порта.

**Router Port (Порт маршрутизатора):** Установите флаг в поле данного порта, чтобы назначить его 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 вступает во все текущие многоадресные группы, поддерживаемые подключенным маршрутизатором/коммутатором, чтобы гарантировать, что многоадресный трафик прошел на все соответствующие интерфейсы коммутатора.

**Fast Leave (Быстрый выход из группы):** 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 (Регулирование):** 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.

## 2.12.2.2 VLAN Configuration (Настройка VLAN)

Эта страница используется для настройки MLD Snooping интерфейса.

Рис. 133. Вид меню IPMC - MLD Snooping - VLAN Configuration

**VLAN ID:** Задайте номер VLAN, используемой для MLD snooping.

**Snooping Enabled («Прослушивание» включено):** 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 (Выбор порта запросов):** 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 (Совместимость):** 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 (sec):** 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.

Чтобы добавить новый элемент списка, нажмите кнопку “Add New MLD VLAN” (Добавить новую MLD VLAN).

### 2.12.2.3 Port Filtering Profile (Профиль фильтрации порта)

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).

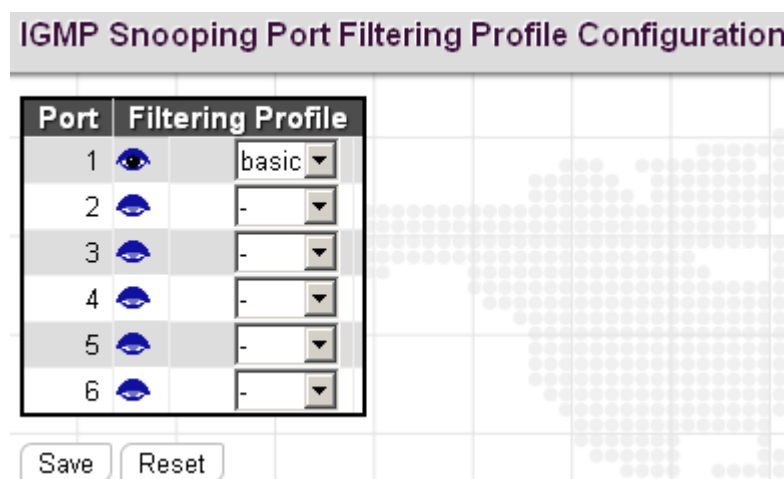


Рис. 134. Вид меню IPMC - MLD Snooping - Port Filtering Profile

**Port (Порт):** Номер порта.

**Filtering Profile (Профиль порта):** 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.

Нажмите кнопку (\*), чтобы просмотреть подробную информацию о выбранных настройках профиля IPMC.

### 2.12.2.4 Status (Состояние)

MLD Snooping Status									
Statistics									
VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V1 Leaves Received	
Router Port									
Port	Status								
1	-								
2	-								
3	-								
4	-								
5	-								
6	-								

Рис. 135. Вид меню IPMC - MLD Snooping - Status

#### Statistics (Статистика)

**VLAN ID:** Номер VLAN для данного элемента списка.

**Querier Version** (Версия запросчика): Текущая работающая версия запросчика.

**Host Version** (Версия хоста): Текущая версия хоста.

**Querier Status** (Состояние запросчика): Отображается состояние запросчика. Возможны следующие состояния: "ACTIVE" (активен) или "IDLE" (свободен). Состояние "DISABLE" (выключен) означает, что конкретный интерфейс выключен администратором сети.

**Queries Transmitted** (Передано запросов): Число переданных запросов.

**Queries Received** (Принято запросов): Число принятых запросов.

**V1 Reports Received** (Принято отчетов V1): Число принятых отчетов V1.

**V2 Reports Received** (Принято отчетов V2): Число принятых отчетов V2.

**V1 Leaves Received** (Принято выходов из группы V2): Число принятых сообщений выхода из группы для версии протокола V2.

#### Router Port (Порт маршрутизатора)

**Port** (Порт): Номер порта.

**Status** (Состояние): Указано, является ли конкретный порт портом маршрутизатора или нет.

### 2.12.2.5 Groups Information (Информация о группе)

MLD Snooping Group Information								
Start from VLAN		<input type="text" value="1"/>	and group address		<input type="text" value="ff00::"/>			
VLAN ID		Groups	Port Members					
			1	2	3	4	5	6
		No more entries						

Рис. 136. Вид меню IPMC - MLD Snooping - Groups Information

**VLAN ID:** Отображается номер VLAN группы.

**Groups** (Группы): Отображается адрес группы.

**Port Members** (Порты-участники группы): Порты, которые принадлежат данной группе.

ПРИМЕЧАНИЕ: Максимальное число групп MLD Snooping, которые могут быть получены обучением, составляет 32.



## 2.12.2.6 IPv6 SFM Information (Информация IPv6 SFM)

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

Рис. 137. Вид меню IPMC - MLD Snooping – Ipv6 SFM Information

**VLAN ID:** Отображается номер VLAN группы.

**Groups (Группы):** Отображается IP-адрес многоадресной группы.

**Port (Порт):** Номер порта коммутатора.

**Mode (Режим работы):** Указан режим фильтрации для каждого VLAN ID, номера порта и адреса группы.

**Source Address (Адрес источника):** IP-адрес источника, доступный для фильтрации.

**Type (Тип):** Отображается тип: Allow (Разрешить) или Deny (Запретить).

**Hardware Filter/Switch (Аппаратный фильтр/коммутатор):** Указано, может ли плоскость данных, назначенная конкретному адресу группы от IPv6-адреса источника обрабатываться специализированной БИС или нет.

## 2.13 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.

Меню “LLDP” содержит подчиненные меню, которые описаны ниже. Чтобы выполнить детальную настройку выберите соответствующее меню.



Рис. 138. Вид меню LLDP

## 2.13.1.1 Configuration (Настройка)

**LLDP Configuration**

**LLDP Parameters**

<b>Tx Interval</b>	30	seconds
<b>Tx Hold</b>	4	times
<b>Tx Delay</b>	2	seconds
<b>Tx Reinit</b>	2	seconds

**LLDP Port Configuration**

Port	Mode	CDP aware	Optional TLVs				
			Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Save Reset

Рис. 139. Вид меню LLDP - Configuration

### LLDP Parameters (Параметры LLDP)

**Tx Interval** (Интервал между передаваемыми кадрами): 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** (Время правильности передаваемого кадра): 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** (Задержка передачи): 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** (Задержка передачи кадра повторной инициализации): Задайте задержку между кадром отключения и новой инициализацией LLDP. Допустимые значения: от 1 до 10 секунд.

### LLDP Port Configuration (Настройка порта LLDP)

**Port** (Порт): Номер порта. Правила "Port \*" означают применение ко всем портам.

**Mode** (Режим работы): 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** (Распознавание CDP): 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 так, как показано ниже.

**Optional TLVs** (Дополнительные 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.

Пример использования через CLI:

```
interface FastEthernet 1/1
lldp receive
lldp transmit
```

### 2.13.1.2 LLDP-MED

Протокол LLDP для оконечных медиа-устройств LLDP-MED (LLDP for Media Endpoint Devices) является расширением LLDP и работает между оконечными 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

**Coordinates Location**

Latitude  ° North Longitude  ° East Altitude  Meters Map Datum WGS84

**Civic Address Location**

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

**Emergency Call Service**

Emergency Call Service

**Policies**

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
<input type="checkbox"/>	0	Voice	Tagged	1	6	0

**Policy Port Configuration**

Port	0
1	<input type="checkbox"/>
2	<input checked="" type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>

Рис. 140. Вид меню LLDP - LLDP-MED

**Fast Start Repeat Count** (Число повторов быстрого старта): Быстрый старт и идентификация местоположения при аварийном вызове (Emergency Call Service Location Identification Discovery) для оконечных устройств является важным аспектом VoIP-систем. Кроме того, лучше всего предоставлять только те части информации, которые действительно важны для оконечного 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 LLDPDU и уменьшения проблем с безопасностью и целостностью системы, которые могут возникнуть из-за того, что информация о правилах работы в сети будет попадать на не предназначенные для этой информации устройства.

В связи с этим, в LLDP-MED 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 оконечными устройствами и неприменимы к линиям между элементами инфраструктуры LAN, включая и устройства соединения по сети или линии другого типа.

**Coordinates Location** (Координаты местоположения)

**Latitude** (Широта): 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): 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): 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): Метры высоты, отсчитываются от заданного датума (нулевого уровня) по вертикали.

**Floors** (Этажи): Позволяют измерять высоту в единицах, наиболее подходящих для зданий, которые имеют различные межэтажные расстояния. Высота = 0.0 означает уровень земли (нулевая отметка) на данной широте и долготе. Внутри здания 0.0 соответствует уровню пола, привязанного к уровню земли на главном входе.

**Map Datum** (Система координат): 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 Code** (Код страны): Код страны по стандарту ISO 3166, состоящий из двух прописных букв ASCII. Пример: DK, DE или US.

**State** (Штат): Единица административно-территориального деления (штат, кантон, регион, провинция, префектура).

**County** (Округ): Округ.

**City** (Город): Город, поселок.

**City District** (Район города): Район города, округ города, административный район города.

**Block** (Neighbourhood) (Блок (квартал)): Квартал, блок.

**Street** (Улица): Улица. Пример: ул. Тверская

**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): Пример: 21.

**House no. suffix** (Суффикс номера дома): Пример: А, 1/2.

**Landmark** (Адрес объекта): Адрес какого-либо заметного объекта на местности. Пример: Кремль.

**Additional location info** (Дополнительная информация о местоположении): Пример: Южное крыло.

**Name** (Имя): Name (residence and office occupant) (ФИО резидента или лица, снимающего офис): Пример: Лев Толстой.

**Zip code** (Почтовый код): Почтовый код – Пример: 2791.

**Building** (Строение): Строение. Пример: Библиотека.

**Apartment** (Апартамент): Апартамент, номер. Пример: Apt 42.

**Floor** (Этаж): Пример: 4.

**Room no.** (Номер комнаты): Номер комнаты – Пример: 450F.

**Place type** (Тип площади): Пример: Офис.

**Postal community name** (ФИО почтового адресата): Пример: Леонид.

**P.O. Box** (Номер абонентского ящика): Пример: 123456.

**Additional code** (Добавочный код): Пример: 1320300003.

**Emergency Call Service** (Служба спасения)

**Emergency Call Service** (Служба спасения): Служба спасения (например, E911 и другие), в том смысле, как определено TIA или NENA.

**Policies** (Правила)

**Policy Id** (Идентификатор правил): Задайте идентификатор ID для этой группы правил.

**Application Type** (Тип приложения): 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** (Тэг): Тег, указывающий, использует ли заданный тип приложения «тегированную» VLAN или «нетегированную» VLAN.

**VLAN ID**: Задайте VLAN ID для порта.

**L2 Priority** (Приоритет L2 ): Задайте один из восьми уровней приоритета (0-7), как определено в 802.1D-2004.

**DSCP**: Задайте одно из значений 64-точечного кода (0-63), см. IETF RFC 2474.

Пример использования через CLI:

```
lldp med media-vlan-policy 0 voice tagged 1 l2-priority 6 dscp 0
!
interface FastEthernet 1/2
lldp med media-vlan policy-list 0
```

### 2.13.1.3 Neighbours (Соседние устройства)

LLDP Neighbor Information						
LLDP Remote Device Summary						
Local Port	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
Port 3	00-1A-81-00-C0-A9	10	Port #10	ZES-2220S	Bridge(+)	192.168.0.24 (IPv4)

Рис. 141. Вид меню LLDP - Neighbours

**Local Port** (Локальный порт): Локальный порт, к которому подключено удаленное устройство, поддерживающее LLDP.

**Chassis ID** (Идентификатор шасси): ID определенного шасси в системе.

**Port ID** (Идентификатор порта): ID удаленного порта, который будет передавать кадры LDPDU.

**Port Description** (Описание порта): Описание удаленного порта.

**System Name** (Имя системы): Имя системы, присвоенное удаленной системе.

**System Capabilities** (Возможности системы): В этом поле отображаются возможности соседнего устройства. Когда эти возможности включены, после соответствующей возможности указан знак плюс (+). Если возможность выключена, после нее указан знак (-).

**Management Address** (Адрес управления): IPv4-адрес удаленного устройства. Если адреса управления нет, адрес должен быть MAC-адресом CPU или адресом порта, отправившим данное уведомление. Если соседнее устройство поддерживает доступ для управления, мышью нажмите на объект в этом поле, чтобы открыть в web-браузере интерфейс управления соседним устройством.

Пример использования через CLI:

```
ZES-2206PS# show lldp neighbors
Local Interface      : FastEthernet 1/3
Chassis ID          : 00-1A-81-00-C0-A9
Port ID             : 10
Port Description     : Port #10
System Name         : ZES-2220S
System Description  : "1.100" 2015-01-20T10:28:26+08:00
System Capabilities : Bridge(+)
Management Address  : 192.168.0.24 (IPv4)
Power Over Ethernet :
```

### 2.13.1.4 LLDP-MED Neighbours (Соседние устройства, поддерживающие LLDP-MED)

На этой странице отображается информация о соседних устройствах LLDP-MED, обнаруженных в сети.



Рис. 142. Вид меню LLDP - LLDP-MED Neighbours

### 2.13.1.5 LLDP PoE

На этой странице отображается информация о соседних устройствах LLDP-MED, поддерживающих PoE.

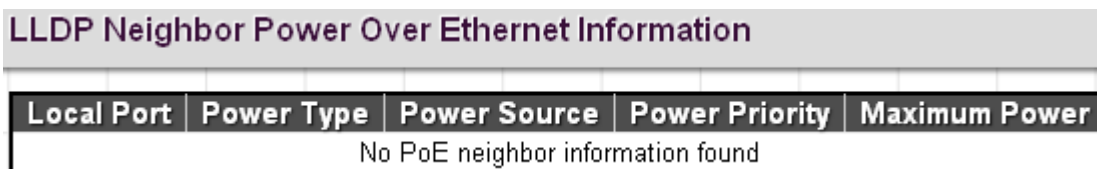


Рис. 143. Вид меню LLDP – LLDP PoE

**Local Port** (Локальный порт): Порт данного коммутатора, на котором принят кадр LLDP.

**Power Type** (Тип источника питания): В данном поле отображается тип устройства - PSE (Power Sourcing Entity – является источником питания) или PD (Powered Device - питание должно подаваться извне). Если тип источника питания неизвестен, отображается "Reserved" (Зарезервировано).

**Power Source** (Источник питания): В этом поле указан источник питания, используемый устройством PSE или PD.

**Power Priority** (Приоритет питания): В поле Power Priority указан приоритет устройства PD или порта устройства типа PSE, который является источником питания. Имеется три уровня приоритета питания - Critical (Критический), High (Высокий) и Low (Низкий). Если приоритет питания неизвестен, в данном поле указано "Unknown" (Неизвестен).

**Maximum Power** (Максимальная мощность): Указана максимальная мощность в Ваттах, требующаяся устройству PD от устройства PSE либо минимальная мощность устройства PSE, способного быть источником питания при максимальной длине кабеля (на основе текущей конфигурации устройства).

### 2.13.1.6 LLDP EEE

Энергосбережения (EEE) может быть достигнуто за счет задержки трафика. Эта задержка происходит в связи с тем, что отключаются некоторые элементы для экономии энергии и нужно время для включения перед отправкой трафика. Это время называется "Время пробуждения". Для достижения минимальной задержки, устройства могут использовать LLDP для обмена информацией о своих TX и RX "время пробуждения", с целью согласовать минимальное время пробуждения.

LLDP Neighbors EEE Information								
Local Port	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE in Sync
No LLDP EEE information found								

Рис. 144. Вид меню LLDP – LLDP EEE

**Local Port** (Локальный порт): Порт данного коммутатора, на котором принят кадр LLDP.

**Tx Tw**: Максимальное время партнерской линии, в течение которого на маршруте передачи могут быть задержаны отправленные данные после отмены подтверждения LPI.

**Rx Tw**: Время партнерской линии, на которое для приемника желательна задержка передачи передатчиком для того, чтобы приемник успел выйти из режима ожидания.

**Fallback Receive Tw** (Время возврата в исходный режим): Время возврата партнерской линии в исходный режим после приема Tw.

**Echo Tx Tw** (Значение эхо): Значение Echo Tx Tw партнерской линии. Должны быть определены соответствующие значения эхо – отражение для локальной партнерской линии от партнерской удаленной линии. Когда локальное партнерское устройство принимает значения эхо из линии удаленного партнерского устройства, оно может определить, приняло ли удаленное партнерское устройство последние значения (а также – зарегистрировало ли и обработало ли оно эти значения). Например, если локальное партнерское устройство принимает эхо параметров, которые не совпадают со значениями в его локальной MIB, оно делает вывод, что запрос удаленного партнерского устройства был обусловлен устаревшей информацией.

**Echo Rx Tw**: Значение Echo Rx Tw партнерской линии.

**Resolved Tx Tw** (Tx Tw, по которым принято решение): Tx Tw по которым для этой линии приняты решения.

**Resolved Rx Tw** (Rx Tw, по которым принято решение): Rx Tw по которым для этой линии приняты решения.

**EEE in Sync** (EEE синхронизирован): В этом поле отображается, согласовали ли коммутатор и партнерское устройство на этой линии время перехода из режима ожидания в активное состояние.

- Red (Красный индикатор): Коммутатор и партнер по линии не согласовали время перехода из режима ожидания в активное состояние.
- Green (Зеленый индикатор): Коммутатор и партнер по линии согласовали время перехода из режима ожидания в активное состояние.

### 2.13.1.7 Port Statistics (Статистика на портах)

Global Counters	
Neighbor entries were last changed 2015-01-02T00:21:15+00:00 (1889 secs. ago)	
Total Neighbors Entries Added	1
Total Neighbors Entries Deleted	1
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

LLDP Statistics Local Counters									
Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs	
1	0	0	0	0	0	0	0	0	
2	0	0	0	0	0	0	0	0	
3	193	33	0	0	0	0	0	0	
4	0	0	0	0	0	0	0	0	
5	0	0	0	0	0	0	0	0	
6	0	0	0	0	0	0	0	0	

Рис. 145. Вид меню LLDP – Port Statistics

#### Global Counters (Глобальные счетчики)

**Total Neighbours Entries Added** (Общее число добавленных соседних устройств): Отображается число новых устройств, добавленных с момента последней перезагрузки коммутатора и для которых удаленный TTL еще не истек.

**Total Neighbours Entries Deleted** (Общее число удаленных соседних устройств): Число соседних LLDP-устройств, которые были удалены из MIB удаленных LLDP-систем по любой причине.

**Total Neighbours Entries Dropped** (Общее число отброшенных соседних устройств): Число отбрасываний кадров LLDPDU удаленной базой данных вследствие переполнения таблицы входов.

**Total Neighbors Entries Aged Out** (Общее число устаревших соседних устройств): Число удалений информации о соседних устройствах из MIB удаленных LLDP-систем, обусловленных истечением таймера TTL удаленной системы.

#### LLDP Statistics Local Counters (Локальные счетчики статистики LLDP)

**Local Port** (Локальный порт): Номер порта.

**Tx Frames** (Передано кадров): Число переданных кадров LLDP PDU.

**Rx Frames** (Принято кадров): Число принятых кадров LLDP PDU.

**Rx Errors** (Ошибок на приеме): Число принятых кадров LLDP с ошибками некоторых типов.

**Frames Discarded** (отброшено кадров): Число кадров, отброшенных из-за несоответствия общим правилам правильности, а также специальным правилам, заданным для определенного значения длины типа TLV (Type Length Value).

**TLVs Discarded** (Отброшено по TLV): Каждый кадр LLDP может содержать множество частей информации, известных, как TLV. Если TLV сформирован неправильно, он подсчитывается и отбрасывается.

**TLVs Unrecognized** (Нераспознанные TLV): Число хорошо сформированных TLV, но с неизвестным значением типа.

**Org. Discarded** (Отброшено организационных TLV): Число отброшенных организационных TLV.

**Age-Outs** (Устаревших устройств): В каждом кадре LLDP содержится информация о том, насколько долго является правильной информация LLDP (срок старения). Если в течение срока старения новых кадров не принято, информация LLDP удаляется, а счетчик Age-Out (Устаревших устройств) увеличивается.

## 2.14 PoE (только для коммутаторов с поддержкой PoE)

На странице настройки функции Power over Ethernet (PoE) можно задать максимальную мощность PoE, обеспечиваемую портом, максимальную общую мощность, предоставляемую коммутатором (суммарная мощность, доступная на всех портах RJ-45), режим работы PoE на порту, приоритет выделения мощности, максимальную мощность, выделенную порту. Если мощность, требующаяся устройствам, присоединенным к коммутатору, превышает суммарную мощность, предоставляемую коммутатором, он использует настройки приоритетов мощностей портов для ограничения предоставляемой мощности.



Меню “PoE” содержит подчиненные меню, которые описаны ниже. Чтобы выполнить детальную настройку выберите соответствующее меню.

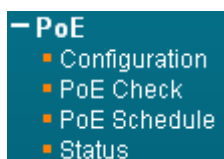


Рис. 146. Вид меню PoE

### 2.14.1.1 PoE Configuration (Настройка PoE)

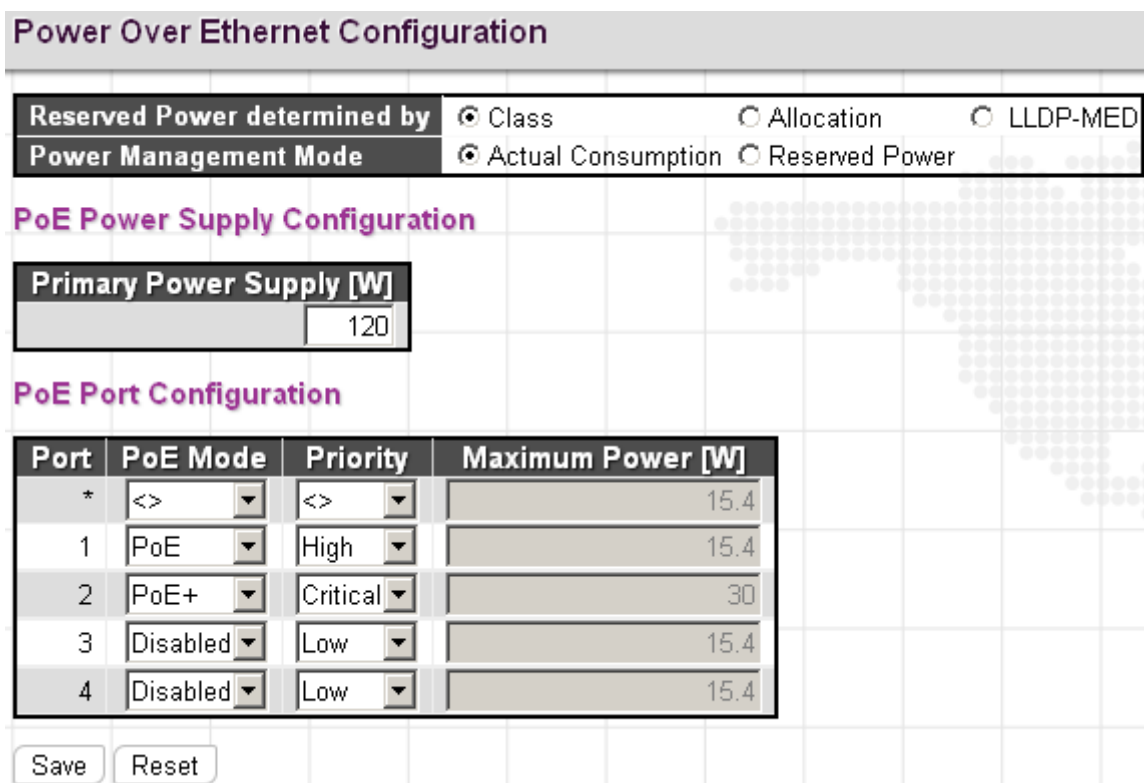


Рис. 147. Вид меню PoE - PoE Configuration

#### Power Over Ethernet Configuration (Настройка подачи питания по Ethernet-кабелям)

**Power Management Mode** (Режим управления электропитанием): Имеется два режима, определяющие последовательность отключения портов.

- **Actual Consumption** (По реальному потреблению): Когда выбран этот режим, порты отключаются при возникновении следующих ситуаций:
  1. Когда реальная потребляемая мощность на всех портах превысит мощность, которую может предоставить блок питания.
  2. Когда реальная потребляемая мощность превысит мощность, зарезервированную для данного порта.
 Порты отключаются в соответствии с приоритетами портов. Если два порта имеют одинаковые приоритеты, отключается порт с большим номером.
- **Reserved Power** (По зарезервированной мощности): Когда выбран этот режим, порты отключаются, когда общая зарезервированная мощность превысит мощность, которую может предоставить блок питания. В этом режиме, если устройство PD продолжает запрашивать больше мощности, чем доступно от источника питания, то питание порта не включается.

**Reserved Power determined by** (По зарезервированной мощности, определенной как): Доступно три режима для настройки того, как подключенное устройство PD может резервировать мощность:

- **Class (Класс):** Каждый порт автоматически определяет, сколько требуется зарезервировать мощности в соответствии с классом, к которому принадлежит подключенное устройство PD. Используется четыре различных класса порта: 4 Вт; 7 Вт; 15,4 Вт и 30 Вт.
- **Allocation (выделенная мощность):** Мощность, зарезервированная для каждого порта указана в поле “Maximum Power [W]” (Максимальная мощность, Вт).
- **LLDP-MED:** Этот режим подобен режиму class, за исключением того, что каждый порт определяет зарезервированную мощность, обмениваясь информацией о PoE по протоколу LLDP и резервирует мощность по результатам этого обмена. Если информация LLDP для порта отсутствует, порт будет резервировать мощность, используя режим class.

**ПРИМЕЧАНИЕ:** Если порты используют больше мощности, чем для них зарезервировано, то они будут выключены.

### **PoE Power Supply Configuration** (Настройка блока питания PoE)

**Primary Power Supply [W]** (Мощность первичного блока питания [Вт]): Бюджет мощности коммутатора. Если устройства PD требуют мощность, превышающую бюджет, для управления питанием используются настройки приоритетов портов.

### **PoE Port Configuration** (Настройка PoE порта)

**Port** (Порт): Номер порта. Правило “Port \*” означает применение ко всем портам.

**PoE Mode** (Режим работы PoE): Режимы работы PoE могут быть следующими:

- **Disabled (Выключен):** Функция PoE выключена (можно задать отдельно для каждого порта).
- **PoE:** Функция PoE включена, по стандарту IEEE 802.3af (устройства PD класса 4, мощность ограничена величиной 15,4 Вт).
- **PoE+:** Функция PoE включена, по стандарту IEEE 802.3at (устройства PD класса 4, мощность ограничена величиной 30 Вт).

**Priority** (Приоритет): Когда порты или подключенные устройства PD запрашивают больше мощности, чем может предоставить блок питания, порты отключаются на основе их уровней приоритета. Коммутатор будет отключать порты, начиная с порта, имеющего наименьший приоритет и наибольший номер.

**Maximum Power** (Максимальная мощность [Вт]): Максимальная мощность, предоставляемая портам.

Пример использования через CLI:

```
poe management mode allocation-consumption
!
interface FastEthernet 1/1
  poe mode standard
  poe priority high
!
interface FastEthernet 1/2
  poe mode plus
  poe priority critical
  poe power limit 30.0
```

### **2.14.1.2 PoE Check**

Функция PoE Check осуществляет проверку доступности подключенного к коммутатору устройства и выполняет указанное действие.

Power Over Ethernet Device Failure Check						
Port	PoE Check	Ping IP Address	No Response Timeout (Cycles 1 ~ 10)	Check Interval (10 ~ 300 Seconds)	No Response Action	Reboot Time (60 ~ 120)
*	<>	192.168.0.200	5	60	<>	60
1	Enabled	192.168.0.200	5	60	Reboot PD	60
2	Disabled		3	10	No Action	60
3	Disabled		3	10	No Action	60
4	Disabled		3	10	No Action	60

Save Reset

Рис. 148. Вид меню PoE - PoE Check

**Port** (Порт): Номер порта. Правило "Port \*" означает применение ко всем портам.

**PoE Check** (Проверка PoE): Включает (Enable) или выключает (Disable) функцию проверки отказов PoE. Этот коммутатор может осуществлять мониторинг работоспособности устройства PD, пингуя его IP-адрес. Если коммутатор не получает ответ от устройства PD) в течение заданного периода времени, делается заключение о том, что устройство PD отказало. После обнаружения отказа устройства PD, коммутатор (PSE) может выполнить соответствующую операцию, определенную в поле "No Response Action" (Операция, выполняемая при неполучении ответа).

**Ping IP Address** (Пингуемый IP-адрес): Задайте IP-адрес устройства PD для выдачи команды проверки связи с устройством (ping). Поддерживаются и IPv4- и IPv6-адреса.

**No Response Timeout** (Cycles 1~10) (Время ожидания ответа (Циклы 1~10)): Задайте общее число циклов проверки по IP-адресу.

**Check Interval** (10~300 Seconds) (Интервал проверки (от 10 до 300 секунд)): Задайте интервал между проверками связи.

**No Response Action** (Операция при неполучении ответа): Если устройство PD не отвечает на запросы ping, посылаемые коммутатором (PSE), то коммутатор (PSE) может выполнить одну из операций, перечисленных ниже:

- No Action (Операция не выполняется): Коммутатор (PSE) не будет выполнять никаких операций с устройством PD.
- Reboot PD (Перезагрузить устройство PD): Коммутатор (PSE) перезагрузит устройство PD после обнаружения его отказа в рамках проверки.
- Power Off PD (Выключить устройство PD): Коммутатор (PSE) выключит устройство PD после обнаружения его отказа в рамках проверки.

Пример использования через CLI:

```
interface FastEthernet 1/1
poe check
poe check ip-address 192.168.0.200
poe check timeout 5
poe check interval 60
poe check no-response-action reboot
```

### 2.14.1.3 PoE Schedule (Расписание PoE)

При некоторых условиях работы, устройства PD работают только ограниченное время. Поэтому для облегчения ограничений на мощность PSE можно использовать расписания PoE, позволяющие планировать PoE отдельно для каждого порта.

### Power Over Ethernet Device Schedule Configuration

Configure Port#

Schedule Mode

Weeks	Day Enable	Start Time	End Time
Sunday	<input type="checkbox"/>	00:00	23:00
Monday	<input checked="" type="checkbox"/>	08:00	18:00
Tuesday	<input type="checkbox"/>	00:00	23:00
Wednesday	<input type="checkbox"/>	00:00	23:00
Thursday	<input type="checkbox"/>	00:00	23:00
Friday	<input type="checkbox"/>	00:00	23:00
Saturday	<input type="checkbox"/>	00:00	23:00

Save    Reset

**Рис. 149. Вид меню PoE - PoE Schedule**

**Configure Port#** (Номер настраиваемого порта): Выберите настраиваемый порт, с которым будут связаны настройки расписания PoE.

**Schedule Mode** (Режим расписания): Позволяет включить (Enable) или выключить (Disable) режим работы PoE по расписанию).

**Weeks** (Дни недели): Список дней недели.

**Day Enable** (Включить день): Установите флаги в полях тех дней, в которые требуется, чтобы устройство PD получало питание от PSE.

**Start Time** (Время начала): Выберите время начала подачи питания от PSE на устройство PD.

**End Time** (Время окончания): Выберите время окончания подачи питания от PSE на устройство PD.

Пример использования через CLI:

```
interface FastEthernet 1/2
 poe schedule
 poe schedule monday
 poe schedule monday start-time 8
 poe schedule monday end-time 18
```

#### 2.14.1.4 Status (Состояние)

Power Over Ethernet Status							
Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	-	0 [W]	0 [W]	0 [W]	0 [mA]	High	No PD detected
2	-	0 [W]	0 [W]	0 [W]	0 [mA]	Critical	No PD detected
3	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
4	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
Total		0 [W]	0 [W]	0 [W]	0 [mA]		

**Рис. 150. Вид меню PoE - PoE Status**

**Local Port** (Локальный порт): Номер порта, на котором коммутатор обеспечивает функцию PoE.

**PD class** (Класс устройства PD): Каждое устройство PD классифицировано в соответствии с максимальной используемой мощностью. Имеются следующие классы устройств PD:

- Класс 0: Макс. мощность 15,4 Вт.

- Класс 1: Макс. мощность 4,0 Вт.
- Класс 2: Макс. мощность 7,0 Вт.
- Класс 3: Макс. мощность 15,4 Вт.
- Класс 4: Макс. мощность 30,0 Вт.

**Power Requested** (Запрашиваемая мощность): Мощность, которую желательно зарезервировать для данного устройства PD.

**Power Allocated** (Выделенная мощность): Мощность, которую коммутатор выделил данному устройству PD.

**Power Used** (Использованная мощность): Мощность, в данный момент используемая устройством PD.

**Current Used** (Используемый ток): Сила тока, в данный момент используемого устройством PD.

**Priority** (Приоритет): Заданный уровень приоритета порта.

**Port Status** (Состояние порта): Состояние услуг PoE для подключенного устройства.

Пример использования через CLI:

```
ZES-2206PS# show poe interface FastEthernet 1/2
Interface          PD Class  Port Status          Power Used [W]  Current Used [mA]
-----
FastEthernet 1/2  -          No PD detected          0.0             0
```

## 2.15 MAC Table (Таблица MAC-адресов)

Меню “MAC Table” (Таблица MAC-адресов) содержит подчиненные меню настройки и состояния. Чтобы выполнить детальную настройку выберите страницу настройки.



Рис. 151. Вид меню MAC Table

### 2.15.1.1 MAC Address Table Configuration (Настройка таблицы MAC-адресов)

**MAC Address Table Configuration**

**Aging Configuration**

Disable Automatic Aging

Aging Time  seconds

**MAC Table Learning**

	Port Members					
	1	2	3	4	5	6
Auto	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Disable	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Secure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

**Static MAC Table Configuration**

			Port Members					
Delete	VLAN ID	MAC Address	1	2	3	4	5	6
<input type="checkbox"/>	1	00-1B-21-21-9F-FB	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Рис. 152. Вид меню MAC Table - Configuration

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

**Aging Time** (Срок устаревания): 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** (Таблица MAC-адресов, полученных обучением): На каждом порту можно включить одну из трех опций:

- **Auto** (Автоматически): На данном порту обучение будет выполнено автоматически, как только будет принят неизвестный SMAC-адрес.
- **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.

**ПРИМЕЧАНИЕ:** 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.

**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** (Удалить): Удаляет MAC-адрес из ячейки таблицы.

**VLAN ID:** Задайте идентификатор VLAN ID для этого MAC-адреса.

**Port Members** (Порты-участники группы): 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.

Пример использования через CLI:

```
mac address-table static 00:1b:21:21:9f:fb vlan 1 interface FastEthernet 1/3
!
interface FastEthernet 1/2
  no mac address-table learning
!
interface FastEthernet 1/4
  mac address-table learning secure
```

### 2.15.1.2 MAC Address Table (Таблица MAC-адресов)

В таблице MAC-адресов отображены статические и динамические MAC-адреса, полученные обучением от CPU или портов коммутатора. Для просмотра требуемых элементов таблицы можно ввести начальный VLAN ID и MAC-адреса.

MAC Address Table									
Start from VLAN		1	and MAC address		00-00-00-00-00-00	with		20	entri
Type	VLAN	MAC Address	Port Members						
			CPU	1	2	3	4	5	6
Static	1	00-1A-81-00-B0-40	✓						
Dynamic	1	00-1B-21-21-9F-FB				✓			
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-00-00-00-02	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-00-B0-40	✓	✓	✓	✓	✓	✓	✓
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓

Рис. 153. Вид меню MAC Table - MAC Address Table

**Type** (Тип): В полях этого столбца отображается, являются ли MAC-адреса, полученными обучением, статическими или динамическими.

**VLAN**: Номер VLAN для данного элемента таблицы.

**MAC Address** (MAC-адрес): MAC-адрес, полученный обучением от CPU или некоторых портов.

**Port Members** (Порты-участники группы): Порты, связанные с данным элементом таблицы.

Пример использования через CLI:

```
ZES-2206PS# show mac address-table
Type    VID  MAC Address      Ports
Static  1    00:1a:81:00:b0:40 CPU
Dynamic 1    00:1b:21:21:9f:fb FastEthernet 1/3
Static  1    33:33:00:00:00:01 FastEthernet 1/1-4 GigabitEthernet 1/1-2 CPU
Static  1    33:33:00:00:00:02 FastEthernet 1/1-4 GigabitEthernet 1/1-2 CPU
Static  1    33:33:ff:00:b0:40 FastEthernet 1/1-4 GigabitEthernet 1/1-2 CPU
Static  1    ff:ff:ff:ff:ff:ff FastEthernet 1/1-4 GigabitEthernet 1/1-2 CPU
```

## 2.16 VLAN Translation (Трансляция VLAN)

Трансляция VLAN предназначена для пользователей, которым требуется преобразовать оригинальный VLAN ID в новый VLAN ID для обмена данными между разными сетями VLAN и улучшения масштабирования VLAN. При трансляции VLAN входящий тег C-VLAN будет заменен тегом S-VLAN (при этом нового тега добавлено не будет). При настройке трансляции VLAN замена соответствующих тегов должна быть возможна на обоих концах линии. Другими словами, на обоих концах линии должны быть введены настройки для замены тега C-VLAN на S-VLAN, а также для замены тега S-VLAN на C-VLAN. Имейте в виду, что трансляцию VLAN поддерживают только порты доступа. На магистральных портах конфигурировать трансляцию VLAN не рекомендуется.

Меню "VLAN Translation" (Трансляция VLAN) содержит подчиненные меню, которые описаны ниже. Для ввода или просмотра настроек выберите соответствующее меню.



Рис. 154. Вид меню VLAN Translation

### 2.16.1.1 Port to Group Mapping (Отображение порта в группу)

Port to Group mapping Table						
Group ID	Port Members					
	1	2	3	4	5	6
6	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
5	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
4	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
3	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
1	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Рис. 155. Вид меню VLAN Translation - Port to Group Mapping

**Group ID** (Идентификатор группы): Общее число групп трансляции VLAN, которые можно использовать, равно 11. При переходе на страницу “Port to Group Mapping” (Отображение порта в группу) эти 11 групп создаются автоматически. Порт может быть отображен в любую из этих групп. В одну группу с одним и тем же идентификатором может быть отображено множество портов.

ПРИМЕЧАНИЕ: По умолчанию, каждый порт отображается в группу с групповым ID, равным номеру порта. Например, порт 2 отображается в группу с ID, равным 2.

**Port Number** (Номер порта): Чтобы включить порт в группу, нажмите соответствующую радиокнопку.

### 2.16.1.2 Translation Mapping (Отображение при трансляции VID)

VLAN Translation Table			
Delete	Group ID	VLAN ID	Translated to VID
<input type="checkbox"/>	2	15	20

Add New Entry

Рис. 156. Вид меню VLAN Translation - Translation Mapping

**Group ID** (Идентификатор группы): Задайте Group ID, который используется для данного правила трансляции.

**VLAN ID:** Указан VLAN ID, который будет отображен в новый VID.

**Translated to VID** (Транслирован в VID): Укажите новый VID, на который будет заменен VID входящих кадров.

Чтобы добавить новый элемент списка трансляции VLAN, нажмите кнопку “Add New Entry” (Добавить новый элемент списка).

Пример использования через CLI:

```
switchport vlan mapping 2 15 20
```

## 2.17 VLANs

Использование виртуальных локальных сетей IEEE 802.1Q 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 широковебательные домены таким образом, что пакеты передаются на порты внутри VLAN, которой они принадлежат. К преимуществам использования VLAN можно отнести:

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 широковежательным трафиком, адресованного всем устройствам. Сводя к минимуму распространение широковежательного 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.

Меню “VLANs” содержит подчиненные меню, которые описаны ниже. Чтобы выполнить детальную настройку выберите соответствующее меню.

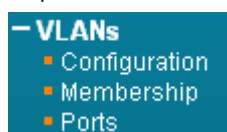


Рис. 157. Вид меню VLANs

### 2.17.1.1 Configuration (Настройка)

Данная страница позволяет работать с настройками VLAN на коммутаторе.

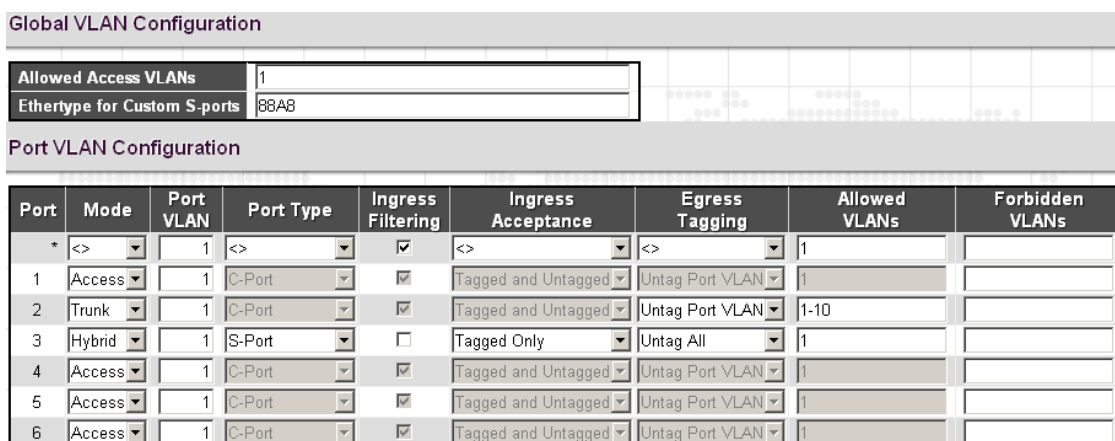


Рис. 158. Вид меню VLANs - Configuration

**Allowed Access VLANs** (Разрешенные Access VLAN): 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 S-ports** (Тип Ethertype для специализированных S-портов): Задайте тип ethertype/TPID, используемый для специализированных s-портов.

#### Port VLAN Configuration (Настройка порта VLAN)

**Port** (Порт): Список номеров портов. Правила “Port \*” означают применение ко всем портам.

**Mode** (Режим): 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 большому количеству VLAN. Порты доступа имеют следующие характеристики:
  - Принадлежит ровно к одной VLAN (port VLAN), по умолчанию 1.

- Принимает нетегированные и C-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 нескольких виртуальных локальных сетях 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 C-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 сконфигурированы как VLAN unaware, C-tag, S-tag или S-custom tag.
  - С возможностью фильтрации на входе.
  - Обработка входящих кадров и конфигурацию выходного тегирования можно настроить независимо.

**Port VLAN** (Порт VLAN): Задайте VLAN ID для порта. Допустимый диапазон значений: от 1 до 4095. По умолчанию задано 1.

**Port Type** (Тип порта): Доступно четыре типа портов. Операция для входящего и исходящего трафика порта каждого типа описана в таблице ниже.

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

**Ingress Filtering** (Фильтрация 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.

**Ingress Acceptance** (Действие на входе): 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** (Тегирование на выходе): 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** (Разрешенные VLAN): 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** (Запрещенные VLAN): 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.

Пример использования через CLI:

```
interface FastEthernet 1/2
  switchport trunk allowed vlan 1-10
  switchport mode trunk
!
interface FastEthernet 1/3
  switchport hybrid acceptable-frame-type tagged
  switchport hybrid egress-tag none
  switchport hybrid port-type s-port
  switchport mode hybrid
```

### 2.17.1.2 Membership (Настройка принадлежности к VLAN)

На данной странице можно настроить принадлежность к VLAN. По умолчанию на странице настройки показан список из 20 VLAN. Однако, можно изменить начальную VLAN списка и общее количество отображаемой информации о портах, входящих в VLAN. Изначально, все порты принадлежат к VLAN по умолчанию, с номером VLAN ID=1.

VLAN Membership Status						
Start from VLAN <input type="text" value="1"/> with <input type="text" value="20"/>						
VLAN ID	Port Members					
	1	2	3	4	5	6
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Рис. 159. Вид меню VLANs - Membership

**VLAN ID:** Номер VLAN для которого отображаются порты-участники.

**Port Members** (Порты-участники VLAN): Порты коммутатора.

### 2.17.1.3 Ports

На этой странице отображаются настройки текущей VLAN (для каждого порта), сохраненные в коммутаторе).

VLAN Port Status for Combined users								
							Combined	Auto-
Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts	
1	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No	
2	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No	
3	S-Port	<input type="checkbox"/>	Tagged	1	Untag All		No	
4	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No	
5	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No	
6	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No	

Рис. 160. Вид меню VLANs - Ports

**Port** (Порт): Номер порта.

**Port Type** (Тип порта): Отображается выбранный тип порта.

**Ingress Filtering** (Фильтрация входящих кадров): Отображается, включена (enabled) или выключена (disabled) фильтрация входящих кадров.

**Frame Type** (Тип кадра): Отображается допустимый для порта тип кадра.

**Port VLAN ID:** Номер VLAN ID, присвоенный порту.

**Tx Tag:** Отображается операция, выполняемая с исходящими кадрами порта.

**Untagged VLAN ID:** Отображается VLAN ID нетегированной VLAN. Untagged VLAN ID порта определяет режим обработки исходящего кадра.

**Conflicts** (Конфликты): В этом столбце отображается, имеются конфликты или нет. Когда модуль программного обеспечения запрашивает установку принадлежности к VLAN либо конфигурацию порта VLAN, могут произойти следующие конфликты:

- Конфликты между функциями (функциональные).
- Конфликты, обусловленные ограничениями аппаратуры.
- Прямые конфликты между модулями пользователей.

## 2.18 Private VLANs (Частные VLAN)

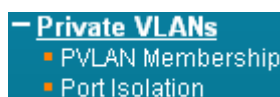


Рис. 161. Вид меню Private VLANs

Меню “Private VLANs” содержит подчиненные меню, которые описаны ниже. Чтобы выполнить детальную настройку выберите соответствующее меню.

### 2.18.1.1 PVLAN Membership (Принадлежность к Private VLAN)

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.

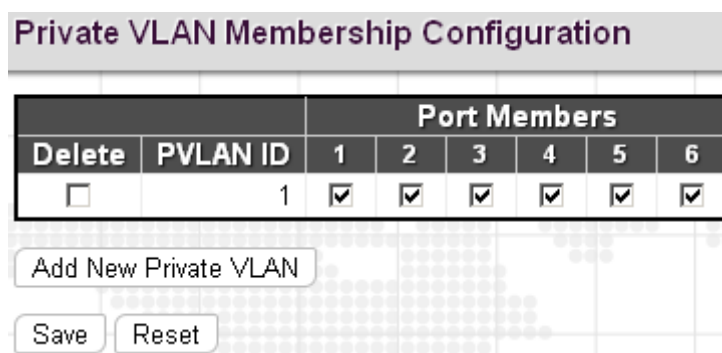


Рис. 162. Вид меню Private VLANs - PVLAN Membership

**PVLAN ID:** Задайте номер PVLAN ID. Допустимые значения: от 1 до 11.

**Port Members** (Порты-участники PVLAN): Установите флаг в поле, если требуется, чтобы порт принадлежал определенной частной VLAN. Чтобы удалить порт из частной VLAN, снимите флаг в соответствующем поле.

**Delete** (Удалить): Удаляет принадлежность к VLAN.

**Add New VLAN** (Добавить новую VLAN): Нажмите мышью на кнопку, чтобы добавить новую VLAN.

**Save** (Сохранить): После нажатия на кнопку “Save”, изменения в структуре VLAN будут сохранены и будут включены новые VLAN.

**Reset** (Переустановить): Нажмите на кнопку “Reset”, чтобы очистить все несохраненные настройки VLAN и их изменения.

### 2.18.1.2 Port Isolation (Изоляция порта)

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.

Port Isolation Configuration					
Port Number					
1	2	3	4	5	6
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Рис. 163. Вид меню Private VLANs - Port Isolation

**Port Number** (Номер порта): Установите флаг в этом поле, если желательно, чтобы порт или порты были изолированы от остальных портов.

Пример использования через CLI:

```
interface GigabitEthernet 1/1
 pvlan isolation
!
interface GigabitEthernet 1/2
 pvlan isolation
```

## 2.19 GVRP

Настройка протокола GVRP.

- GVRP	
<input checked="" type="checkbox"/>	Global Configuration
<input type="checkbox"/>	Port Configuration

Рис. 164. Вид меню GVRP

### 2.19.1.1 Global Configuration

GVRP Configuration	
<input checked="" type="checkbox"/>	Enable GVRP
Parameter	Value
Join-time:	20
Leave-time:	60
LeaveAll-time:	1000
Max VLANs:	20

Рис. 165. Вид меню GVRP - Global Configuration

**Enable GVRP** (Включение 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.

**LeaveAll-time:** Значение в диапазоне 1000-5000, указываемое в сентисекундах (сотых секунды). По умолчанию, значение равно 1000.

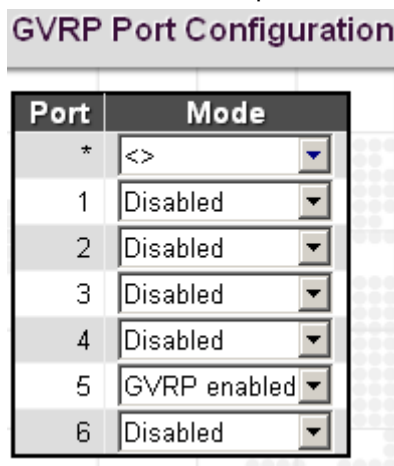
**Max VLANs:** Максимальное значение VLAN, поддерживаемое GVRP.

Пример использования через CLI:

```
gvrp max-vlans 20
gvrp time join-time 20 leave-time 60 leave-all-time 1000
```

## 2.19.1.2 Port Configuration

Данная страница позволяет включить GVRP на определенном порту.



Port	Mode
*	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	GVRP enabled
6	Disabled

Рис. 166. Вид меню GVRP - Port Configuration

**Port** (Порт): Номер порта.

**Mode** (Режим работы): Позволяет настроить режим работы GVRP на порту. Возможны следующие режимы:

- Enabled (Активирован): включить GVRP.
- Disabled (Деактивирован): выключить GVRP.

Пример использования через CLI:

```
interface GigabitEthernet 1/1
gvrp
```

## 2.20 VCL

Меню “VCL” содержит подчиненные меню, которые описаны ниже.

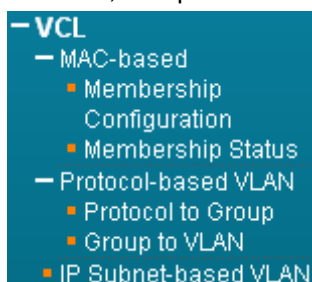


Рис. 167. Вид меню VCL

### 2.20.1 MAC-based (На основе MAC-адресов)

Страница конфигурирования VLAN на основе MAC-адресов предназначена для настройки VLAN по MAC-адресам источников. Когда порт принимает входящие нетегированные кадры, он обрабатывает MAC-адрес источника и принимает решение, какой VLAN принадлежат эти нетегированные кадры. Когда MAC-адреса источника не совпадают с созданными правилами, нетегированные кадры будут назначены VLAN с номером PVID, которой принадлежит принявший их порт.

#### 2.20.1.1 Membership Configuration (Настройка принадлежности к VLAN на основе MAC-адресов)

MAC-based VLAN Membership Configuration								
Delete	MAC Address	VLAN ID	Port Members					
			1	2	3	4	5	6
<input type="checkbox"/>	00-1b-21-21-9f-fb	2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Add New Entry

Рис. 168. Вид меню VCL - MAC-based - Membership Configuration

**MAC Address** (MAC-адрес): 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-участники): Порты, которые принадлежат данной VLAN.

Пример использования через CLI:

```
interface FastEthernet 1/1
switchport vlan mac 00-1b-21-21-9f-fb vlan 2
```

### 2.20.1.2 Membership Status (Состояние участия в VLAN)

На этой странице отображается состояние текущих правил VCL.

MAC-based VLAN Membership Status for User Static							
MAC Address	VLAN ID	Port Members					
		1	2	3	4	5	6
00-1b-21-21-9f-fb	2	✓					

Рис. 169. Вид меню VCL - MAC-based - Membership Status

**MAC Address** (MAC-адрес): Отображаются сконфигурированные MAC-адреса.

**VLAN ID:** Отображается номер VLAN ID для данного элемента списка участников.

**Port Members** (Порты-участники): Отображаются порты, которые приняли сконфигурированные MAC-адреса.

### 2.20.2 Protocol-based VLAN (VLAN на основе протокола)

Сетевые устройства, требуемые для поддержки множества протоколов не могут быть легко сгруппированы в обычной VLAN. Для пропуска трафика между различными VLAN, направленного всем устройствам, участвующим в протоколе, могут потребоваться нестандартные устройства. При таком конфигурировании пользователи лишаются основных преимуществ VLAN, в том числе безопасности и легкого доступа.

Во избежание этих проблем можно сконфигурировать этот коммутатор с сетями VLAN на основе протоколов, чтобы разделить физическую сеть на логические группы VLAN для каждого требуемого протокола. Когда порт принимает кадр, его принадлежность к VLAN может быть определена по типу протокола, используемого во входящих пакетах.

#### 2.20.2.1 Protocol to Group (Отображение протокола в группу)



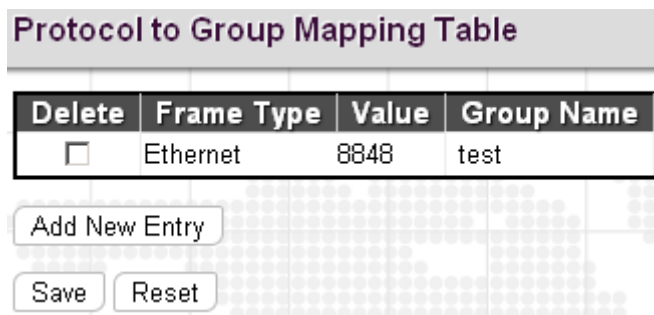


Рис. 170. Вид меню VCL - Protocol-based VLAN - Protocol to Group

**Frame Type** (Тип кадра): Можно выбрать один из трех типов кадров: “Ethernet”, “SNAP”, “LLC”. Поле значения (value) изменится соответствующим образом автоматически.

**Value** (Значение): В данном поле особым образом указан тип протокола. Содержимое данного поля зависит от выбранного типа кадра.

**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): Указано описательное имя для этой группы. Поле может содержать не более 16 алфавитно-цифровых символов (a-z; A-Z) или целых чисел (0-9).

Пример использования через CLI:

```
vlan protocol eth2 0x8848 group test
```

## 2.20.2.2 Group to VLAN (Отображение группы в VLAN)

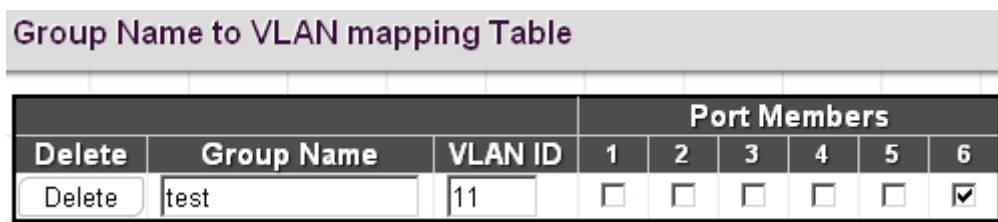


Рис. 171. Вид меню VCL - Protocol-based VLAN - Group to VLAN

**Group Name** (Имя группы): Указано описательное имя для этой группы. Поле может содержать не более 16 алфавитно-цифровых символов (a-z; A-Z) или целых чисел (0-9).

**VLAN ID:** Указан номер VLAN ID.

**Port Members** (Порты-участники): Порты, назначенные данному правилу.

Пример использования через CLI:

```
interface GigabitEthernet 1/2
switchport vlan protocol group test vlan 11
```

### 2.20.2.3 IP Subnet-based VLAN (VLAN на основе IP-подсети)

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	VCE ID	IP Address	Mask Length	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
<input type="checkbox"/>	1	192.168.0.0	24	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Рис. 172. Вид меню VCL - IP Subnet-based VLAN

**VCE ID:** Индекс ячейки таблицы. Допустимый диапазон значений 0-128.

**IP Address (IP-адрес):** Указан IP-адрес для данного правила.

**Mask Length (Длина маски):** Указана длина маски сети.

**VLAN ID:** Указан номер VLAN ID.

**Port Members (Порты-участники):** Порты, назначенные данному правилу.

Пример использования через CLI:

```
interface FastEthernet 1/1
switchport vlan ip-subnet id 1 192.168.0.0/255.255.255.0 vlan 1
```

### 2.21 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).

Меню "QoS" содержит подчиненные меню, которые описаны ниже.



Рис. 173. Вид меню QoS

## 2.21.1.1 Port Classification (Классификация на портах)

QoS Ingress Port Classification							
Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	Address Mode
*	<>	<>	<>	<>		<input type="checkbox"/>	<>
1	5	1	0	0	Disabled	<input type="checkbox"/>	Source
2	0	0	0	0	Disabled	<input type="checkbox"/>	Source
3	0	0	0	0	Disabled	<input type="checkbox"/>	Source
4	0	0	0	0	Disabled	<input type="checkbox"/>	Source
5	0	0	0	0	Disabled	<input type="checkbox"/>	Source
6	0	0	0	0	Disabled	<input type="checkbox"/>	Source
7	0	0	0	0	Disabled	<input type="checkbox"/>	Source
8	0	0	0	0	Disabled	<input type="checkbox"/>	Source
9	0	0	0	0	Disabled	<input type="checkbox"/>	Source
10	0	0	0	0	Disabled	<input type="checkbox"/>	Source
11	0	0	0	0	Disabled	<input type="checkbox"/>	Source
12	0	0	0	0	Disabled	<input type="checkbox"/>	Source
13	0	0	0	0	Disabled	<input type="checkbox"/>	Source
14	0	0	0	0	Disabled	<input type="checkbox"/>	Source
15	0	0	0	0	Disabled	<input type="checkbox"/>	Source
16	0	0	0	0	Disabled	<input type="checkbox"/>	Source
17	0	0	0	0	Disabled	<input type="checkbox"/>	Source
18	0	0	0	0	Disabled	<input type="checkbox"/>	Source
19	0	0	0	0	Disabled	<input type="checkbox"/>	Source
20	0	0	0	0	Disabled	<input type="checkbox"/>	Source

Рис. 174. Вид меню QoS - Port Classification

**Port** (Порт): Список номеров портов. Правила "Port \*" означают применение ко всем портам.

**CoS** (Класс обслуживания): Указан класс QoS, выбираемый по умолчанию. Класс QoS с номером 0 имеет наименьший приоритет. По умолчанию задано 0.

**DP Level** (Уровень DP): 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** (Класс тега): 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** (На основе DSCP): Установите флаг в поле, чтобы включить QoS на основе DSCP (входящий порт).

**Address Mode** (Режим выбора адреса): Выбранный режим указывает должна ли выполняться классификация на основе адресов источника (SMAC/SIP) или на основе адресов назначения (DMAC/DIP):

- Source (Источник): Классификация на основе адресов источника (SMAC/SIP).
- Destination (Назначение): Классификация на основе адресов назначения (DMAC/DIP).

Пример использования через CLI:

```
interface FastEthernet 1/1
  qos cos 5
  qos dpl 1
```

### 2.21.1.2 Port Policing (Ограничение скорости на портах)

На этой странице можно задать полосу пропускания, выделяемую каждому порту.

QoS Ingress Port Policers				
Port	Enabled	Rate	Unit	Flow Control
*	<input checked="" type="checkbox"/>	1024	<>	<input checked="" type="checkbox"/>
1	<input checked="" type="checkbox"/>	1024	kbps	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
3	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
4	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
5	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
6	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
7	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
8	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
9	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
10	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
11	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
12	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
13	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
14	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
15	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
16	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
17	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
18	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
19	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
20	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>

Рис. 175. Вид меню QoS - Port Policing

**Port** (Порт): Номер порта. Правила "Port \*" означают применение ко всем портам.

**Enabled** (Включить): Установите флаг в этом поле, чтобы включить функцию ограничения скорости на порту.

**Rate** (Скорость): 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 (ккадров/с): от 1 до 3300 Мбит/с.

**Unit** (Единицы измерения): Выберите единицы измерения ограничения скорости.

**Flow Control** (Управление потоком): Если управление потоком включено и порт работает в режиме управления потоком, то будут отправляться кадры pause, вместо отбрасывания входящих кадров.

Пример использования через CLI:

```
interface FastEthernet 1/1
  qos policer 1024 flowcontrol
```

### 2.21.1.3 Queue Policing (Ограничение скорости в очередях)

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
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Рис. 176. Вид меню QoS - Queue Policing 1

**Port** (Порт): Номер порта. Правила "Port \*" означают применение ко всем портам.

**Queue 0~7 Enable** (Включить ограничение скорости в очередях 0~7): Установите флаг в соответствующем поле, чтобы включить функцию ограничения скорости в очередях на портах коммутатора.

После включения откроется следующее окно:

QoS Ingress Queue Policers										
Port	Queue 0			Queue 1	Queue 2	Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
	E	Rate	Unit	Enable	Enable	Enable	Enable	Enable	Enable	Enable
*	<input checked="" type="checkbox"/>	500	<>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Рис. 177. Вид меню QoS - Queue Policing 2

**Rate** (Скорость): Указана 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): Выберите единицы измерения ограничения скорости очереди входящих кадров.

**Save** (Сохранить): Нажмите на эту кнопку, чтобы сохранить текущие настройки в памяти.

**Reset** (Переустановить): Очистка всех выбранных настроек.

Пример использования через CLI:

```
interface FastEthernet 1/1
```

### 2.21.1.4 Port Scheduler

На этой странице можно настроить работу диспетчеров и формирователей трафика портов (индивидуально на каждом порту).

QoS Egress Port Schedulers							
Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Weighted	29%	14%	14%	14%	14%	14%
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-

Рис. 178. Вид меню QoS - Port Scheduler

**Port** (Порт): Нажмите мышью на порт, чтобы задать детали настройки диспетчера порта.

**Mode** (Режим работы): Отображается выбранный режим работы диспетчера.

**Weight** (Вес): Отображается вес в процентах, присвоенный очередям Q0~Q5.

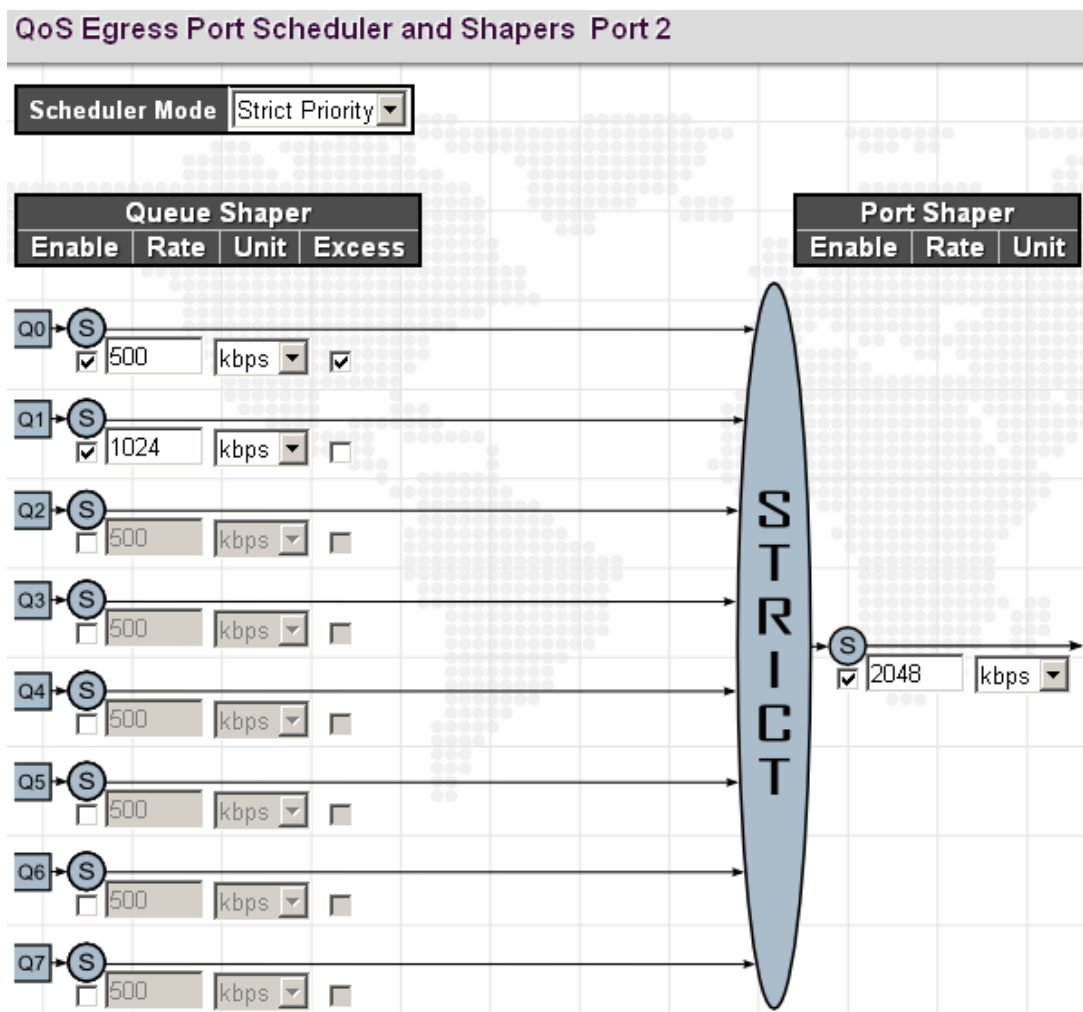


Рис. 179. Вид меню QoS - Port Scheduler (Strict priority)

## QoS Egress Port Scheduler and Shapers Port 3

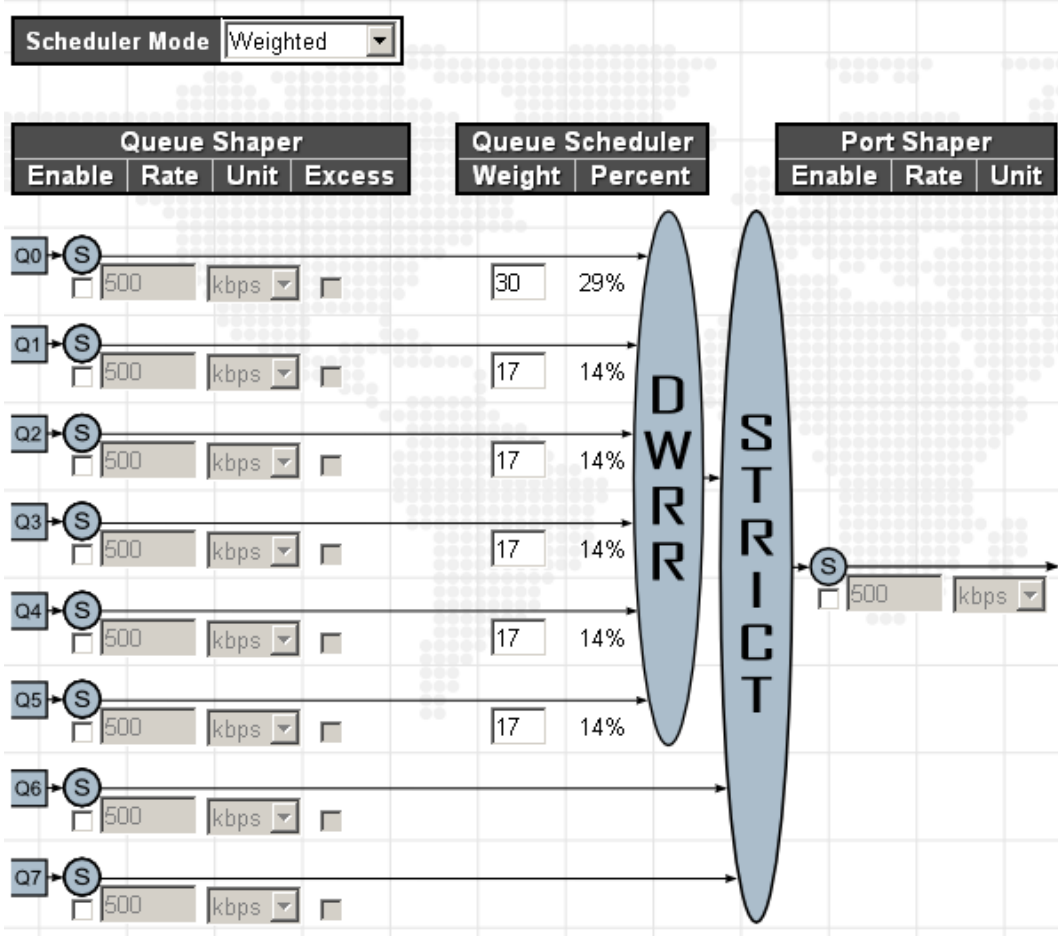


Рис. 180. Вид меню QoS - Port Scheduler (Weighted)

**Scheduler Mode** (Режим работы диспетчера): 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/Port Shaper/Queue Shaper** (Формирователи трафика порта и очередей)

**Enable** (Включить): Нажмите мышью это поле, чтобы включить формирователь для некоторой очереди на выбранном порту.

**Rate** (Скорость): 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** (Единицы измерения): Выберите единицы измерения скорости, которые будет использовать формирователь очереди при ограничении скорости.

**Excess** (Разрешить избыточную полосу пропускания): Установите флаг в этом поле, чтобы разрешить использование избыточной полосы пропускания.

### Queue Schedule (Диспетчер очереди)

**Queue Scheduler** (Диспетчер очереди): Если выбран режим работы диспетчера Weighted (с взвешиванием), пользователю необходимо задать вес для каждой очереди. При DWRR используется заранее определенный вес каждой очереди, который определяет процент времени обслуживания коммутатором каждой очереди до перехода к следующей очереди. В результате предотвращается блокировка очередей, которая может происходить при строгом обслуживании очередей в соответствии с их приоритетами.

**Weight** (Вес): Задайте вес для каждой очереди. Этот набор весов определяет частоту опроса каждой очереди для обслуживания и соответственно влияет на время отклика прикладного ПО, которому присвоено определенное значение приоритета.

**Percent** (Процент): Вес очереди, выраженный в процентах.

**Port Shaper** (Формирователь трафика порта): Задайте скорость, с которой трафик может покидать данную очередь.

**Enable** (Включить): Установите флаг в этом поле, чтобы включить формирователь трафика порта.

**Rate** (Скорость): 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** (Единицы измерения): Выберите единицы измерения скорости.

Пример использования через CLI:

```
interface FastEthernet 1/2
  qos shaper 2048
  qos queue-shaper queue 0 500 excess
  qos queue-shaper queue 1 1024
!
interface FastEthernet 1/3
  qos wrr 30 17 17 17 17 17
```

### 2.21.1.5 Port Shaping (Формирование трафика портов)

В этом окне отображаются формирователи очередей портов и скорость, которую они используют.

#### QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	500 kbps	1024 kbps	disabled	disabled	disabled	disabled	disabled	disabled	2048 kbps
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

Рис. 181. Вид меню QoS - Port Shaping

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

### 2.21.1.6 Port Tag Remarking (Изменение тегов на порту)

Данная страница предоставляет возможность просмотреть и внести изменения в правила перемаркировки исходящих кадров.



## QoS Egress Port Tag Remarking

Tag Remarking Mode

Рис. 182. Вид меню QoS - QoS Egress Port Tag Remarking (Classified)

**Tag Remarking Mode** (Режим изменения тегов на порту): 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.

## QoS Egress Port Tag Remarking

Tag Remarking Mode

### PCP/DEI Configuration

Default PCP

Default DEI

Рис. 183. Вид меню QoS - QoS Egress Port Tag Remarking (Default)

**PCP/DEI Configuration** (Конфигурация PCP/DEI): Настройка значений PCP/DEI для режима Default.

QoS Egress Port Tag Remarking Port 1

Tag Remarking Mode **Mapped**

(QoS class, DP level) to (PCP, DEI) Mapping

QoS class	DP level	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. 184. Вид меню QoS - QoS Egress Port Tag Remarking (Mapped)

**QoS class/DP level** (Класс QoS / Уровень DP): 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)

### 2.21.1.7 Port DSCP (Настройка трансляции DSCP на порту)

QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	<input checked="" type="checkbox"/>	<>	<>
1	<input checked="" type="checkbox"/>	DSCP=0	Enable
2	<input type="checkbox"/>	Disable	Disable
3	<input type="checkbox"/>	Disable	Disable
4	<input type="checkbox"/>	Disable	Disable
5	<input type="checkbox"/>	Disable	Disable
6	<input type="checkbox"/>	Disable	Disable

Рис. 185. Вид меню QoS - Port DSCP

**Port** (Порт): Номер порта. Правила "Port \*" означают применение ко всем портам.

**Ingress Translate** (Трансляция входящих кадров): Установите флаг в поле, чтобы включить трансляцию значений DSCP на основе выбранного метода классификации.

**Ingress Classify** (Классификация входящих пакетов): 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** (Переписывать исходящие значения): 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.
- Remark 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 Remark DP0 или DP1.
- Remark 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 Remark DP0.

Пример использования через CLI:

```
interface FastEthernet 1/1
  qos dscp-translate
  qos dscp-classify zero
  qos dscp-remark rewrite
```

## 2.21.1.8 DSCP-Based QoS (Настройка качества обслуживания по DSCP)

DSCP-Based QoS Ingress Classification			
DSCP	Trust	QoS Class	DPL
*	<input type="checkbox"/>	<>	<>
0 (BE)	<input type="checkbox"/>	0	0
1	<input type="checkbox"/>	0	0
2	<input type="checkbox"/>	0	0
3	<input type="checkbox"/>	0	0
4	<input type="checkbox"/>	0	0
5	<input type="checkbox"/>	0	0
6	<input type="checkbox"/>	0	0
7	<input type="checkbox"/>	0	0
8 (CS1)	<input type="checkbox"/>	0	0
9	<input type="checkbox"/>	0	0
10 (AF11)	<input type="checkbox"/>	0	0
11	<input type="checkbox"/>	0	0
12 (AF12)	<input type="checkbox"/>	0	0

Рис. 186. Вид меню QoS - DSCP-Based QoS

**DSCP:** Значение DSCP входящего пакета. Диапазон допустимых значений DSCP: от 0 до 63.

**Trust (Доверять):** 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.

**QoS Class (Класс QoS):** Выберите класс QoS для соответствующего значения DSCP для 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.

Пример использования через CLI:

```
qos map dscp-cos 63 cos 7 dpl 0
```

## 2.21.1.9 DSCP Translation (Трансляция DSCP)

DSCP Translation				
DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<>	<input type="checkbox"/>	<>	<>
0 (BE)	0 (BE)	<input type="checkbox"/>	0 (BE)	0 (BE)
1	1	<input type="checkbox"/>	1	1
2	2	<input type="checkbox"/>	2	2
3	3	<input type="checkbox"/>	3	3
4	4	<input type="checkbox"/>	4	4
5	5	<input type="checkbox"/>	5	5
6	6	<input type="checkbox"/>	6	6
7	7	<input type="checkbox"/>	7	7
8 (CS1)	8 (CS1)	<input type="checkbox"/>	8 (CS1)	8 (CS1)
9	9	<input type="checkbox"/>	9	9
10 (AF11)	10 (AF11)	<input type="checkbox"/>	10 (AF11)	10 (AF11)
11	11	<input type="checkbox"/>	11	11
12 (AF12)	12 (AF12)	<input type="checkbox"/>	12 (AF12)	12 (AF12)

Рис. 187. Вид меню QoS - DSCP Translation

**DSCP:** Значение DSCP входящего кадра. Диапазон допустимых значений DSCP: от 0 до 63.

**Ingress Translate** (Трансляция входящих кадров): Включает трансляцию значений DSCP входящих кадров на основе заданного метода классификации.

**Ingress Classify** (Классификация входящих кадров): Включает классификацию на входящей стороне, как определено в таблице настройки DSCP QoS на порту.

**Egress Remap DP0** (Отображение DP0 исходящих кадров заново): Заново отображает значение DP0 в выбранное значение DSCP. DP0 указывает приоритет отбрасывания с низким приоритетом.

**Egress Remap DP1** (Отображение DP1 исходящих кадров заново): Заново отображает значение DP1 в выбранное значение DSCP. DP1 указывает приоритет отбрасывания с высоким приоритетом.

## 2.21.1.10 DSCP Classification (Классификация DSCP)

Отображает значения DSCP в класс QoS и значение DPL.

DSCP Classification		
QoS Class	DPL	DSCP
*	*	<>
0	0	0 (BE)
0	1	0 (BE)
1	0	0 (BE)
1	1	0 (BE)
2	0	0 (BE)
2	1	0 (BE)
3	0	0 (BE)
3	1	0 (BE)
4	0	0 (BE)
4	1	0 (BE)
5	0	0 (BE)
5	1	0 (BE)
6	0	38 (AF43)
6	1	0 (BE)
7	0	0 (BE)
7	1	0 (BE)

Рис. 188. Вид меню QoS - DSCP Classification

**QoS Class** (Класс QoS): Список актуальных значений классов QoS.

**DPL**: Список актуальных значений DPL.

**DSCP**: Выберите значение DSCP для отображения в класс QoS и значение DPL. Значение DSCP, выбранное для "\*" будет отображено во все классы QoS и значения DPL.

Пример использования через CLI:

```
qos map cos-dscp 6 dpl 0 dscp 38
```

### 2.21.1.11 QoS Control List (Список управления QoS)

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.

QoS Control List Configuration												
QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action			
									CoS	DPL	DSCP	
1	All	Multicast	Any	Tagged	10	Any	Any	Any	6	Default	38 (AF43)	+ - e x +

Рис. 189. Вид меню QoS - QoS Control List

На этой странице отображаются правила, созданные только в списке управления QoS (QCL). Для этого устройства максимальное число QCL равно 256. Нажмите на «+», чтобы ввести в список новый QCL.

**QCE#:** Отображается номер элемента списка QCL.

**Port** (Порт): Отображается номер порта, использующего этот QCL

**Frame Type** (Тип кадра): Отображается тип кадра, поиск которого будет производиться во входящих кадрах. Возможны следующие типы кадров: Any (Любой), Ethernet, LLC SNAP, IPv4, IPv6.

**SMAC:** MAC-адрес источника.

**DMAC:** MAC-адрес назначения. Возможны следующие значения: Any (Любой), Broadcast (Широковещательный), Multicast (Многоадресный), Unicast (Одноадресный).

**VID:** Отображается VLAN ID (1-4095)

**PCP:** Отображается значение PCP.

**DEI:** Отображается значение DEI.

**Action** (Операция): Отображается операция классификации, выполняемая на входящих кадрах, когда настройки параметров согласуются с содержимым кадра. Если кадр согласуется с QCL, выполняются следующие операции:

- CoS: Если кадр согласуется с QCL, будет установлено заданное значение.
- DPL: Для уровня приоритета отбрасывания будет установлено заданное значение.
- DSCP: В качестве значения DSCP, будет установлено заданное значение.

Используя кнопки, перечисленные ниже, можно изменить каждый QCE (Элемент управления QoS) в таблице:

- «+»: Вставляет новую строку QCE перед текущей строкой.
- «e»: Редактирование элемента QCE.
- «↑»: Перемещает QCE вверх по списку.
- «↓»: Перемещает QCE вниз по списку.
- «x»: Удаляет QCE.

The screenshot shows the 'QCE Configuration' interface. At the top, there is a 'Port Members' section with a table of 20 ports, each with a checked checkbox. Below this are two main configuration panels: 'Key Parameters' and 'Action Parameters'. The 'Key Parameters' panel includes fields for DMAC (Multicast), SMAC (Any), Tag (Tagged), VID (Specific with Value: 10), PCP (Any), DEI (Any), and Frame Type (Any). The 'Action Parameters' panel includes fields for CoS (6), DPL (Default), and DSCP (38 (AF43)).

Рис. 190. Вид меню QoS - QoS Configuration

**QCE Configuration** (Настройка QCE)

**Port Members** (Порты-участники): Выберите порты, которые используют это правило.

**Key Parameters** (Ключевые параметры)

**SMAC:** Выберите тип MAC-адреса источника. По умолчанию используется any (любой). Выберите "Specific" (Конкретный), чтобы задать MAC-адрес источника (первые три байта MAC-адреса или OUI).

**DMAC** (Тип DMAC): Выберите тип MAC-адреса назначения. По умолчанию используется any (любой). Другие доступные варианты: “Unicast” для одноадресного трафика, “Multicast” для многоадресного трафика, “Broadcast” для широковещательного трафика.

**Tag** (Тэг): Выберите тип VLAN: Tagged (тегированная) или Untagged (Нетегированная). По умолчанию можно использовать любой тип.

**VID**: Выберите приоритет VID. По умолчанию используется любой VID (any). Если требуется назначить VID данному элементу QCL, выберите “Specific” (Специальный). Если требуется отобразить диапазон VID в данный элемент QCL, выберите “Range” (Диапазон).

**PCP**: Выберите значение PCP (либо конкретное значение, либо диапазон значений). По умолчанию используется any (любой).

**DEI**: Выберите значение DEI. По умолчанию используется any (любое).

**Frame Type** (Тип кадра): Типы кадров, которые могут быть выбраны, перечислены ниже.

**Any** (Любой): По умолчанию используется тип any (любой). Это означает, что будут разрешены кадры всех типов.

**Ethertype**: Данная опция может использоваться только для фильтрации пакетов формата Ethernet II. Доступные варианты: Any (Любой), Specific (Специальный) – 600-ffff (шестнадцатиричные значения); по умолчанию: ffff. Имейте в виду, что 800 (IPv4) и 86DD (IPv6) исключены. Подробный список типов протокола Ethernet см. в RFC 1060. Несколько часто используемых типов: 0800 (IP), 0806 (ARP), 8137 (IPX).

**LLC**: LLC является сокращением от Link Logical Control (Управление логической линией) и имеет три опции, описанные ниже.

- **SSAP**: SSAP – это сокращение от Source Service Access Point address – адрес точки доступа услуги источника. По умолчанию используется any (любой). Чтобы указать значение (0x00 - 0xFF), выберите specific (специальный).
- **DSAP**: DSAP – это сокращение от Destination Service Access Point address – адрес точки доступа услуги назначения. По умолчанию используется any (любой). Чтобы указать значение (от 0x00 до 0xFF), выберите specific (специальный).
- **Control** (Управление): Поле управления может содержать команду, ответ или информацию последовательности, в зависимости от того имеет кадр LLC тип Unnumbered (Ненумерованный), Supervisory (Супервизор) или Information (Информация). По умолчанию используется any (любой). Чтобы указать значение (от 0x00 до 0xFF), выберите specific (специальный).

**SNAP**: Протокол доступа в подсеть (SubNetwork Access Protocol) можно отличить по OUI и Protocol ID. (Доступные варианты для PID: Any (Любой), Specific (Специальный) (0x00-0xffff); по умолчанию задан: Any (Любой)). Если для OUI задано шестнадцатиричное значение 000000, то для protocol ID в поле значения типа Ethernet (тип Ether) 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.

**IPv4: Protocol** (Протокол): Для типа кадра IPv4 возможны варианты: Any (Любой), TCP, UDP, Other (Другой). Если выбрано “TCP” или “UDP”, можно определить значения Sport (Source port number – номер порта источника) и Dport (Destination port number – номер порта назначения).

**Source IP** (IP-адрес источника): Выберите IP-адрес источника. По умолчанию используется any (любой). Чтобы задать требующийся Вам IP-адрес источника, выберите “Specific” (Специальный) и формат маски.

**IP Fragment** (Фрагмент IP): По умолчанию используется any (любой). Датаграммы иногда могут быть фрагментированы, чтобы гарантировать, что они смогут пройти через сетевое устройство, использующее максимальные передаваемые блоки меньшей длины, чем длины оригинальных пакетов.

**DSCP**: По умолчанию используется any (любой). Чтобы задать значение DSCP, выберите “Specific” (Специальный). Чтобы задать диапазон значений DSCP, выберите “Range” (Диапазон).

**IPv6: Protocol** (Протокол): Для протокола IPv6 возможны варианты: Any (Любой), TCP, UDP, Other (Другой). Если выбрано “TCP” или “UDP”, можно далее определить значения Sport (Source port number – номер порта источника) и Dport (Destination port number – номер порта назначения).



**Source IP** (IP-адрес источника): Выберите IP-адрес источника. По умолчанию используется any (любой). Чтобы задать требующийся Вам IP-адрес источника, выберите "Specific" (Специальный) и формат маски.

**DSCP**: По умолчанию используется any (любой). Чтобы задать значение DSCP, выберите "Specific" (Специальный). Чтобы задать диапазон значений DSCP, выберите "Range" (Диапазон).

#### Action Parameters (Параметры операции)

Указывает действие, выполняемое с входящим кадром, если настройки параметров согласуются с содержимым кадра. Выполняемая операция имеет следующие параметры:

- **Class** (Класс): Если кадр согласуется с QCE, он будет помещен в очередь, соответствующую заданному классу QoS, либо помещен в очередь на основе базовых правил классификации.
- **DPL**: Если кадр согласуется с QCE, необходимо задать уровень приоритета отбрасывания (выбрать значение), либо оставить его без изменений.
- **DSCP**: Если кадр согласуется с QCE, необходимо выбрать значение DSCP.

Пример использования через CLI:

```
qos qce 1 interface FastEthernet 1/1-16 GigabitEthernet 1/1-2 tag type tagged vid 10
dmac multicast action cos 6 dscp 38
```

## 2.21.2 Storm Control (Управление широковещательным штормом)

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.

Frame Type	Enable	Rate (pps)
Unicast	<input type="checkbox"/>	1
Multicast	<input type="checkbox"/>	1
Broadcast	<input checked="" type="checkbox"/>	256K

Рис. 191. Вид меню QoS - Storm Control

**Enable** (Включить): Включает подавление шторма для пакетов типов Unicast (Одноадресный), Multicast (Многоадресный), Broadcast (Широковещательный).

**Rate** (pps): Выберите пороговое значение в пакетах в секунду. Принятые пакеты, при которых превышено выбранное значение, будут отброшены.

Возможные значения: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K и 1024K.

Пример использования через CLI:

```
qos storm broadcast 256 kfps
```

## 2.22 Mirroring (Зеркалирование)

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

Трафик, который должен быть скопирован на зеркальный порт, выбирается следующим образом:

- Все кадры, полученные на определенном порту (входящие);
- Все кадры, передаваемые на определенный порт (исходящие).

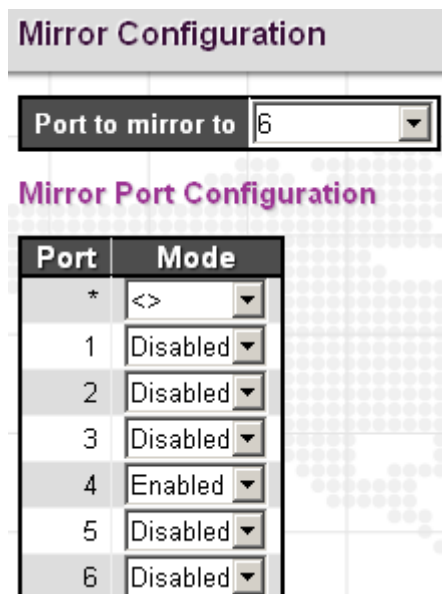


Рис. 192. Вид меню Mirroring

**Port to mirror** (Порт, на который будет зеркалирован трафик): Выберите порт, на который будет зеркалирован принимаемый или передаваемый трафик либо выключите функцию зеркалирования портов.

#### Mirror Port Configuration (Настройка зеркалирования портов)

**Mode** (Режим работы): 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.

Пример использования через CLI:

```
monitor destination interface FastEthernet 1/6  
monitor source interface FastEthernet 1/4 both
```

## 2.23 UPnP

Настройка UPnP.

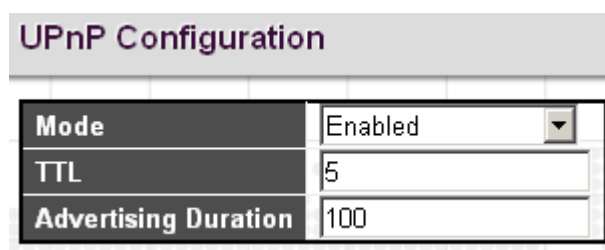


Рис. 193. Вид меню UPnP

**Mode** (Режим работы): 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** (Длительность уведомления): 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.

Пример использования через CLI:

```
upnp
upnp ttl 5
```

## 2.24 PTP (IEEE1588)

В меню “ PTP (IEEE1588)” имеются возможность настроить протокол PTP (IEEE1588) и просмотреть состояние его работы.



Рис. 194. Вид меню PTP (IEEE1588)

### 2.24.1.1 PTP Clock Configuration

Настройка PTP.

PTP Clock Configuration			Port List																				
Delete	Clock Instance	Device Type	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
	No Clock Instances Present																						
Delete	Clock Instance	Device Type	2 Step Flag	Clock Identity		One Way	Protocol	VLAN Tag Enable	VID	PCP													
Delete	0	Ord-Bound	True	00:1a:81:ff:fe:00:c0:a9		False	Ethernet	<input type="checkbox"/>	1	0													

Рис. 195. Вид меню PTP (IEEE1588) - Configuration

**Clock Instance** (Номер объекта): Номер объекта определенного Clock Instance. Номер может быть в диапазоне от 0 до 3.

**Device Type** (Тип устройства): Тип Clock Instance. Могут быть следующие типы:

- Ord-Bound: Тип Ordinary-Boundary Clock (граничные часы).
- P2p Transp: Тип Peer to Peer Transparent Clock (прозрачные часы Peer to).
- E2e Transp: Тип End to End Transparent Clock (прозрачные часы End to End).
- Master Only: Тип Master.
- Slave Only: Тип Slave.

**2 Step Flag** (Флаг 2 Step): Значение True, если используются события Sync и Pdelay\_Resp.

**Clock Identity** (Идентификатор часов): Отображает уникальный идентификатор часов.

**One Way** (Однонаправленный режим): Если установлено значение true, используются однонаправленные измерения. Этот параметр применим только к типу Slave. В однонаправленном режиме измерения задержки не выполняются, таким образом, этот режим применим только, если требуется синхронизация. Мастер всегда отвечает за запросы по задержке.

**Protocol** (Протокол): Выберите протокол, используемый PTP.

- Ethernet: Мультикастовый PTP через Ethernet.
- ip4multi: Мультикастовый PTP через IPv4.
- ip4uni: Одноадресный PTP через IPv4.

Примечание: IPv4 unicast работает только в режимах Master и Slave.

**VLAN Tag Enable** (Тегирование VLAN): Разрешает тегирование VLAN для кадров PTP.

**VID** (Идентификатор VLAN): Идентификатор VLAN используемый для тегирования кадров PTP.

**PCP**: Значение Priority Code Point используемое для кадров PTP.

PTP Clock's Configuration

**Local Clock Current Time**

PTP Time	Clock Adjustment method	Synchronize to System Clock	Ports Configuration
1970-01-02T00:04:25+00:00.923,317,340	Internal Timer	<input type="checkbox"/> Synchronize to System Clock	<a href="#">Ports Configuration</a>

**Clock Default DataSet**

ClockId	Device Type	2 Step Flag	Ports	Clock Identity	Dom	Clock Quality	Pri1	Pri2	Protocol	One-Way	VLAN Tag Enable	VID	PCP
0	Ord-Bound	True	20	00:1a:81:ff:fe:00:c0:a9	0	Cl:251 Ac:Unknwn Va:65535	128	128	Ethernet	False	False	1	0

**Clock Current DataSet**

stpRm	Offset From Master	Mean Path Delay
0	0.000,000,000	0.000,000,000

**Filter Parameters**

DelayFilter	period	dist
6	1	2

**Clock Parent DataSet**

Parent Port Identity	Port	PStat	Var	ChangeRate	Grand Master Identity	Grand Master Clock Quality	Pri1	Pri2
00:1a:81:ff:fe:00:c0:a9	0	False	0	0	00:1a:81:ff:fe:00:c0:a9	Cl:251 Ac:Unknwn Va:65535	128	128

**Clock Time Properties DataSet**

UtcOffset	Valid	leap59	leap61	Time Trac	Freq Trac	ptp Time Scale	Time Source
0	<input type="checkbox"/> False	<input type="checkbox"/> False	<input type="checkbox"/> False	<input type="checkbox"/> False	<input type="checkbox"/> False	<input type="checkbox"/> True	160

**Unicast Slave Configuration**

Index	Duration	ip_address	grant	CommState
0	100	0.0.0.0	0	IDLE
1	100	0.0.0.0	0	IDLE
2	100	0.0.0.0	0	IDLE
3	100	0.0.0.0	0	IDLE
4	100	0.0.0.0	0	IDLE

Рис. 196. Вид меню PTP (IEEE1588) – Clock's Configuration

**Local Clock Current Time** (Текущее локальное время): Отображает данные локальных часов.

**PTP Time** (Время PTP): Отображает актуальное PTP время с точностью до в наносекунд.

**Clock Adjustment Method** (Метод подстройки часов): Отображает актуальный метод подстройки часов.

**Synchronize to System Clock** (Синхронизация с системными часами): Нажмите эту кнопку чтобы синхронизировать системные часы с временем PTP.

**Ports Configuration** (Настройка портов): Нажмите для редактирования списка портов.

**Clock Default Dataset** (Набор параметров часов): Набор параметров часов, определенный стандартом IEEE 1588. Содержит три группы данных – статические параметры, определенные на этапе создания часов, динамические параметры, определенные системой и изменяемые параметры.

**ClockId** (Номер): Номер объекта (0~3).

**Device Type** (Тип часов): Отображает тип часов.

**2 Step Flag** (Флаг 2 step): Отображается True или False.

**Ports** (Порты): Количество портов.

**Clock Identity** (Идентификатор часов): Уникальный идентификатор часов.

**Dom** (Домен): Домен часов (0~127).

**Clock Quality** (Качество часов): Качество часов, определенное системой. Содержит три части – класс часов, точность часов и журнал сдвига.

**Pri1** (Приоритет1): Приоритет 1 часов, используемый алгоритмом выбора BMC master (0~255).

**Pri2** (Приоритет2): Приоритет 2 часов, используемый алгоритмом выбора BMC master (0~255).

**Protocol** (Протокол): Транспортный протокол, используемый PTP.

**One-Way** (Однонаправленный): Если установлено значение true, используются однонаправленные измерения. Этот параметр применим только к типу Slave. В однонаправленном режиме измерения задержки не выполняются, таким образом, этот режим применим только, если требуется синхронизация. Мастер всегда отвечает за запросы по задержке.

**VLAN Tag Enable** (Тегирование): Отображает состояние функции тегирования кадров PTP.

**VID** (Идентификатор VLAN): Идентификатор VLAN используемый для тегирования кадров PTP.

**PCP**: Значение Priority Code Point используемое для кадров PTP.

**Clock current Data Set** (Набор текущих параметров часов): Набор текущих параметров часов, определенный стандартом IEEE 1588.

**stpRm**: Это сокращение для словосочетания «Steps Removed». Отображает количество PTP устройств, пройденных от «grandmaster» до локальных часов.

**Offset from master** (Сдвиг относительно мастера): Разница во времени между часами Master и локальными часами Slave. Измеряется в наносекундах.

**Mean Path Delay** (Время распространения по линии связи): Время распространения по линии связи между часами Master и локальными часами Slave.

**Filter Parameters** (Параметры фильтра)

**DelayFilter, Period, Dist** (Фильтр Задержки, Период, Интервал): Фильтр задержки по умолчанию это фильтр с нижним значением и неизменным временем  $2 \cdot \text{DelayFilter} \cdot \text{DelayRequestRate}$ . Фильтр смещения по умолчанию использует метод фильтра минимальной задержки, т.о. минимальное измеренное смещение в интервале Period используется при вычислении. Интервал между двумя вычислениями указывается в Dist.

**Clock Parent Data Set** (Набор текущих параметров часов): Набор текущих родительских параметров часов, определенный стандартом IEEE 1588.

**Parent Port Identity** (Идентификатор родительского порта): Идентификатор родительских часов. Здесь будет отображаться идентификатор локальных часов, если режим часов отличается от Slave.

**Port** (Порт): Идентификатор порта master.

**PStat** (Состояние родителя): Состояние родителя. Всегда false.

**Var** (Изменение): Наблюдаемый сдвиг родительских часов.

**Change Rate** (Скорость изменения): Наблюдаемая скорость изменения фазы родительских часов.

**Grand Master Identity** (Идентификатор Grand Master): Идентификатор часов grand master. Здесь будет отображаться идентификатор локальных часов, если режим часов отличается от Slave.

**Grand Master Clock Quality** (Качество часов Grand Master): Качество часов Grand Master. Содержит три части – класс часов, точность часов и журнал сдвига анонсированные grand master.

**Pri1** (Приоритет1): Приоритет 1 часов, анонсированный grand master.

**Pri2** (Приоритет2): Приоритет 1 часов, анонсированный grand master.

**Clock Time Properties Data Set** (Набор параметров часов): Набор параметров часов, определенный стандартом IEEE 1588. Параметры могут быть как динамическими так и могут быть настроены для grandmaster.

**Unicast Slave Configuration** (Одноадресные настройки для режима Slave): В режиме IPv4 Unicast на устройстве может быть настроено до 5 IP-адресов Master-устройств. В таком случае, slave запрашивает сообщение Announce от всех настроенных Master-устройств.

**Duration** (Продолжительность): Количество секунд, в течении которых запрашивается с устройства Master запрашиваются сообщения Announce/Sync. Запросы отправляются с устройства Slave каждые Duration/4 секунды.

**ip\_address**: IPv4-адрес устройства Master.

**grant**: Предоставленный период повторения для сообщения sync.

**CommState**: Состояние связи с master. Возможные значения:

- IDLE: Не используется.
- INIT: Сообщение Announce отправлено устройству Master (ожидание ответа).
- CONN: Master ответил.
- SELL: Указанный Master выбран как текущий.
- SYNC: Master отправляет сообщения Sync.

### 2.24.1.2 Status (Состояние)

Просмотр состояния PTP.

PTP Clock Configuration		Port List																				
Clock Instance	Device Type	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
0	Ord-Bound																					
1	E2eTransp																					

Рис. 197. Вид меню PTP (IEEE1588) – Status

**Clock Instance** (Номер объекта): Номер объекта Clock Instance (0~3).

**Device Type** (Тип устройства): Отображает тип часов.

**Port List** (Список портов): Список портов, конфигурированных в данном устройстве.

## 2.25 Diagnostics (Диагностика)

В меню “Diagnostics” (Диагностика) имеются функции ping и traceroute для тестирования связности с указанным IP-адресом.

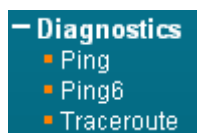


Рис. 198. Вид меню Diagnostics

### 2.25.1.1 Ping

Эта функция Ping предназначена для пакетов ICMPv4.

**ICMP Ping**

IP Address:

Ping Length:

Ping Count:

Ping Interval:

Рис. 199. Вид меню Diagnostics - Ping

**IP Address** (IP-адрес): Введите IP-адрес, связность с которым требуется проверить.

**Ping Length** (Длина Ping): Размер или длина эхо-пакетов.

**Ping Count** (Число эхо-пакетов): Число посылаемых командой ping эхо-пакетов.

**Ping Interval** (Интервал отправки пакетов): Задайте интервал между проверками связи.

### 2.25.1.2 Ping6

Эта функция Ping предназначена для пакетов ICMPv6.

ICMPv6 Ping	
IP Address	0:0:0:0:0:0:0
Ping Length	56
Ping Count	5
Ping Interval	1
Egress Interface	
<input type="button" value="Start"/>	

Рис. 200. Вид меню Diagnostics – Pingv6

**IP Address** (IP-адрес): Введите IPv6-адрес, связность с которым требуется проверить.

**Ping Length** (Длина Ping): Размер или длина эхо-пакетов.

**Ping Count** (Число эхо-пакетов): Число посылаемых командой ping эхо-пакетов.

**Ping Interval** (Интервал посылки пакетов): Задайте интервал между проверками связи.

**Egress Interface** (Исходящий интерфейс): Интерфейс с которого будут отправляться эхо-пакеты.

### 2.25.1.3 Traceroute

Функция traceroute предназначена для определения пути следования пакетов в сети до устройства с указанным IP-адресом.

TraceRoute	
IP Address	192.168.0.105
Max TTL	30
Wait Time	2
<input type="button" value="Start"/>	

Рис. 201. Вид меню Diagnostics - Traceroute

**IP Address** (IP-адрес): Введите IP-адрес, путь до которого требуется проверить.

**TTL**: Параметр TTL (Time to live – время жизни) используется для указания того, сколько шагов может пакет.

**Wait Time** (Время ожидания): Время ожидания ответа.

## 2.26 Maintenance (Обслуживание)

Меню “Maintenance” (Обслуживание) содержит подчиненные меню, которые описаны ниже. Выберите соответствующее подчиненное меню, чтобы перезагрузить устройство, восстановить его заводские настройки или обновить ПО.

- Maintenance
  - Reboot
  - Factory Defaults
  - Software
    - Upload
    - Image Select
  - Configuration
    - Save startup-config
    - Backup
    - Restore
    - Activate
    - Delete

Рис. 202. Вид меню Maintenance

### 2.26.1.1 Reboot (Перезагрузка)

Данный пункт меню позволяет выполнить перезагрузку коммутатора.

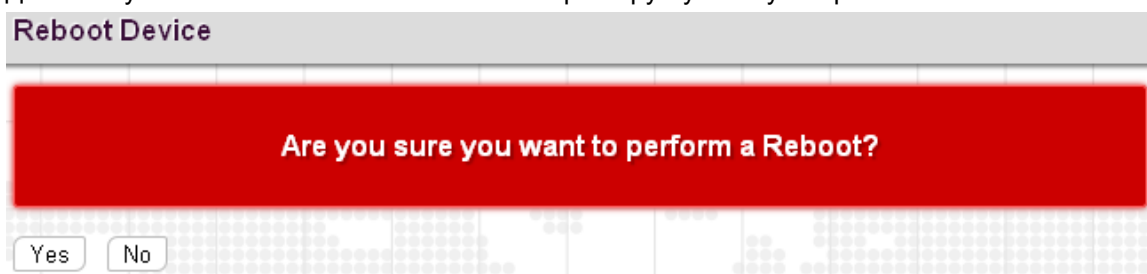


Рис. 203. Вид меню Maintenance - Reboot

Чтобы перезагрузить коммутатор, нажмите кнопку "Yes".

### 2.26.1.2 Factory Defaults (Восстановление заводских настроек)

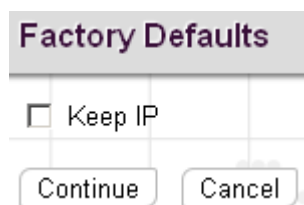


Рис. 204. Вид меню Maintenance - Factory Defaults

**Keep IP** (Сохранить IP-адрес): Установите флаг в поле "Keep IP" (Сохранить IP), если требуется использовать текущие настройки IP после восстановления заводских настроек.

Чтобы восстановить заводские настройки на устройстве, нажмите кнопку "Continue" (Продолжить). Имейте в виду, что все внесенные изменения настроек будут потеряны. Рекомендуется скопировать текущие настройки и сохранить их на локальном устройстве.

Пример использования через CLI:

```
reload defaults keep-ip
```

## 2.26.2 Software (Программное обеспечение)

### 2.26.2.1 Upload (Загрузка)

Обновление программного обеспечения.



Рис. 205. Вид меню Maintenance – Software - Upload

Выберите файл с ПО (этот файл должен иметь расширение ".dat" ) на локальном устройстве, затем нажмите кнопку "Upload" (Загрузить). Процесс загрузки занимает около 5 минут. После того, как файл с ПО будет успешно загружен в коммутатор, он будет использовать новый файл ПО. Перезагрузите коммутатор, чтобы изменения вступили в силу.

Пример использования через CLI:

```
firmware upgrade 192.168.0.131 ZES-2220_v1.100.dat
```



## 2.26.2.2 Image Select (Выбор образа)

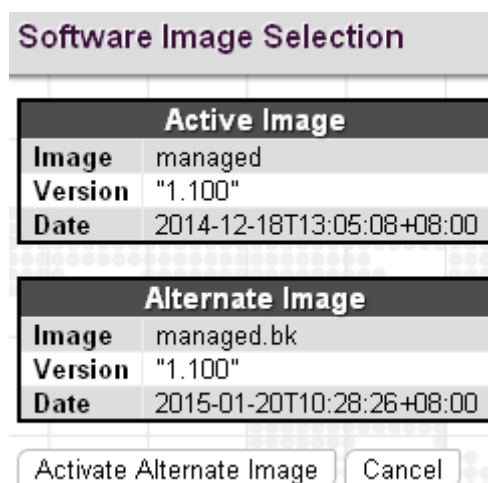


Рис. 206. Вид меню Maintenance – Software - Image Select

Выберите файл образа, используемый данным устройством.

Пример использования через CLI:

```
firmware swap
```

## 2.26.3 Configuration (Настройка)

### 2.26.3.1 Save startup-config (Сохранение текущих настроек)

Сохраните текущие настройки в энергонезависимую память устройства.



Рис. 207. Вид меню Maintenance – Configuration - Save startup-config

### 2.26.3.2 Backup (Резервное копирование конфигурации)

Сохраните копию настроек на локальном устройстве.

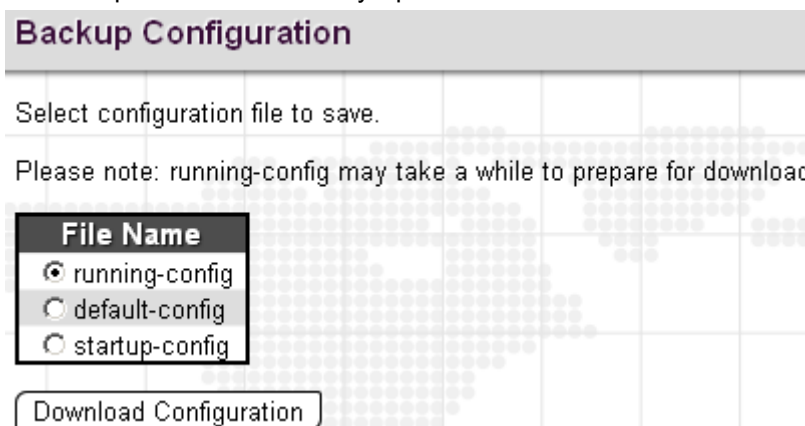


Рис. 208. Вид меню Maintenance – Configuration – Backup

**Running-config** (Текущие настройки): Сохранение текущих настроек.

**Default-config** (Заводские настройки): Сохранение заводских настроек.

**Startup-config** (Стартовые настройки): Сохранение настроек, сохраненных в энергонезависимой памяти устройства.

### 2.26.3.3 Restore (Восстановление конфигурации)

File Name	Parameters
<input type="radio"/> running-config	<input checked="" type="radio"/> Replace <input type="radio"/> Merge
<input type="radio"/> startup-config	
<input type="radio"/> Create new file	

Рис. 209. Вид меню Maintenance – Configuration – Restore

**File To Restore** (Файл с настройками): Выберите файл с настройками, которые необходимо восстановить.

**Replace running-config With IP** (Восстановление с настройками IP): Если требуется использовать настройки IP, сохраненные в файле Configuration (Конфигурация) и которые необходимо восстановить, установите флаг в поле “Restore With IP” (Восстановить с IP).

**Running-config** (Текущие настройки): Настройки из файла будут скопированы в текущие настройки.

**Startup-config** (Стартовые настройки): Настройки из файла будут скопированы в загрузочные настройки.

**Create new file** (Создать новый файл): Создать новый файл с настройками.

**Replace** (Заменить): При восстановлении, конечные настройки будут заменены загружаемыми.

**Merge** (Объединить): При восстановлении, конечные настройки будут объединены с загружаемыми.

### 2.26.3.4 Activate (Выбор загружаемой конфигурации)

Выберите файл настроек, который будет применен.

File Name
<input type="radio"/> default-config
<input type="radio"/> startup-config

Рис. 210. Вид меню Maintenance – Configuration – Activate

**Default-config** (Заводские настройки): Загрузка заводских настроек.

**Startup-config** (Стартовые настройки): Загрузка настроек, сохраненных в энергонезависимой памяти устройства.

### 2.26.3.5 Delete (Удаление файла конфигурации)

Выберите файл настроек, который будет удален.

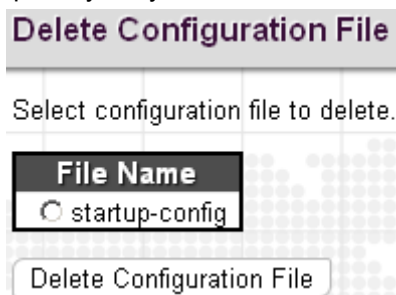


Рис. 211. Вид меню Maintenance – Configuration – Delete

**Startup-config** (Стартовые настройки): Удаление настроек, сохраненных в энергонезависимой памяти устройства.