



Комплексные решения для построения сетей

MES1024

MES1124

MES2124

Руководство по эксплуатации, Часть 1
версия ПО 1.1.12

Управляемые коммутаторы L2 Fast Ethernet и
Gigabit Ethernet

Версия документа	Дата выпуска	Содержание изменений
Версия 2.3	05.07.2013	Добавлены разделы: - 6.27 Конфигурирование защиты от DoS-атак Изменения в разделах: - Приложение А Примеры применения и конфигурирования устройства
Версия 2.2	18.06.2013	Добавлены разделы: - 5.14.9 Настройка протокола OAM - 5.14.10 Настройка протокола CFM Изменения в разделах: - 4.1 Настройка терминала - 5.9 Контроль широковещательного «шторма» - 5.17.1 Механизм AAA - 5.17.7.1 Telnet, SSH, HTTP и FTP - 5.17.7.2 Команды конфигурирования терминала
Версия 2.1	28.05.2013	Добавлены разделы: - 5.6.3 Команды для резервирования конфигурации - 5.15.7 Настройка протокола G.8032v2 (ERPS) Изменения в разделах: - 5.18.2 Протокол RADIUS - 5.18.3 Протокол TACACS+ - 5.18.4 Протокол управления сетью (SNMP) - 5.21.2 Диагностика оптического трансивера
Версия 2.0	03.04.2013	Добавлено описание устройства MES1124
Версия 1.6	20.03.2013	Добавлены разделы: - Функции ограничения multicast-трафика Изменения в разделах: - Функция посредника протокола IGMP (IGMP Snooping) - Механизм AAA - Настройка доступа - Контроль протокола DHCP и опция 82 - Конфигурирование PPPoE Intermediate Agent
Версия 1.5	06.03.2013	Изменения в разделах: - 5.4 Команды управления системой; - 5.9 Selective Q-in-Q; - 5.17.2 Функция посредника протокола IGMP (IGMP Snooping) Добавлено: - Приложение Б Типовые схемы построения сетей на базе протокола EAPS
Версия 1.4	28.12.2012	Изменения в разделах: - 5.4 Команды управления системой: добавлено описание конфигурирования функций мониторинга и защиты CPU; - 5.8.1. Добавлено описание конфигурирования функций мониторинга нагрузки на интерфейсах. - 5.8.2. Добавлено описание конфигурирования MAC-based vlan, EtherType для исходящих пакетов. - 5.17.1. Добавлено описание конфигурирования изучения MAC-адресов во VLAN. - 5.18.4. Добавлено описание конфигурирования snmp trap сообщений на портах. - 5.20. Добавлено описание конфигурирования удаленного зеркалирования. - 5.23.3. Добавлено описание конфигурирования формата DHCP опции 82. Удален раздел 5.28 Работа в режиме маршрутизатора. Добавлен раздел 5.23.6 "Настройка функции MAC Address Notification".
Версия 1.3	10.09.2012	Изменения в разделе 5.22 Функции диагностики физического уровня
Версия 1.2	21.08.2012	Добавлено описание конфигурирования протокола EAPS.
Версия 1.1	12.05.2012	Добавлен раздел: - Настройка PPPoE Intermediate Agent
Версия 1.0	21.12.2011	Первая публикация.
Версия программного обеспечения	1.1.12	

СОДЕРЖАНИЕ

1	ВВЕДЕНИЕ	7
2	ОПИСАНИЕ ИЗДЕЛИЯ	8
2.1	Назначение.....	8
2.2	Функции MES1024/MES1124/MES2124	8
2.2.1	Основные функции	8
2.2.2	Функции при работе с MAC – адресами	9
2.2.3	Функции второго уровня сетевой модели OSI	10
2.2.4	Функции третьего уровня сетевой модели OSI	12
2.2.5	Функции QoS.....	12
2.2.6	Функции обеспечения безопасности	12
2.2.7	Функции управления коммутатором	13
2.2.8	Дополнительные функции	15
2.3	Основные технические характеристики	16
2.4	Конструктивное исполнение	18
2.4.1	Передняя панель устройства	18
2.4.2	Боковые панели устройства	19
2.4.3	Световая индикация	20
2.5	Комплект поставки	21
3	УСТАНОВКА И ПОДКЛЮЧЕНИЕ.....	22
3.1	Крепление кронштейнов	22
3.2	Установка устройства в стойку.....	22
3.3	Установка и удаление SFP-трансиверов	24
3.4	Подключение питающей сети	25
4	ВКЛЮЧЕНИЕ УСТРОЙСТВА, НАЧАЛЬНОЕ КОНФИГУРИРОВАНИЕ.....	26
4.1	Настройка терминала.....	26
4.2	Включение устройства	26
4.3	Порядок конфигурирования.....	28
4.3.1	Начальное конфигурирование.....	28
4.3.2	Настройка параметров системы безопасности.....	31
5	УПРАВЛЕНИЕ УСТРОЙСТВОМ. ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ	35
5.1	Правила работы с командной строкой.....	36
5.2	Базовые команды	36
5.3	Настройка макрокоманд.....	38
5.4	Команды управления системой	39
5.5	Команды для настройки параметров для задания паролей	43
5.6	Работа с файлами	44
5.6.1	Описание аргументов команд	44
5.6.2	Команды для работы с файлами.....	45
5.6.3	Команды для резервирования конфигурации	47
5.6.4	Команды для автоматического обновления и конфигурирования.....	48
	Команды доступные в режиме глобального конфигурирования:	48
	Команды режима privileged EXEC.....	49
5.7	Настройка системного времени	49
5.8	Конфигурирование интерфейсов	53
5.8.1	Параметры Ethernet-интерфейсов и интерфейсов Port-Channel	53
5.8.2	Настройка интерфейса VLAN.....	61
5.9	Selective Q-in-Q.....	67
5.10	Контроль широковещательного «шторма».....	68
5.11	Группы агрегации каналов – Link Agregation Group (LAG).....	69
5.11.1	Статические группы агрегации каналов.....	70
5.11.2	Протокол агрегации каналов LACP	70
5.12	Настройка IPv4-адресации	72
5.13	Настройка Green Ethernet	74

5.14	Настройка IPv6-адресации	76
5.14.1	Протокол IPv6	76
5.14.2	Туннелирование протокола IPv6 (ISATAP).....	79
5.15	Настройка протоколов.....	81
5.15.1	Настройка протокола DNS – системы доменных имен.....	81
5.15.2	Настройка протокола ARP.....	82
5.15.3	Настройка протокола GVRP	84
5.15.4	Механизм обнаружения петель (loopback-detection).....	86
5.15.5	Семейство протоколов STP (STP, RSTP, MSTP).....	87
5.15.6	Протокол EAPS.....	93
5.15.7	Настройка протокола G.8032v2 (ERPS)	94
5.15.8	Настройка протокола LLDP	96
5.15.9	Настройка протокола OAM.....	102
5.15.10	Настройка протокола CFM.....	104
5.16	Voice VLAN	107
5.17	Групповая адресация.....	109
5.17.1	Правила групповой адресации (multicast addressing).....	109
5.17.2	Функция посредника протокола IGMP (IGMP Snooping).....	115
5.17.3	MLD snooping – протокол контроля многоадресного трафика в IPv6	119
5.17.4	Функции ограничения multicast-трафика.....	121
5.18	Функции управления	123
5.18.1	Механизм AAA.....	123
5.18.2	Протокол RADIUS.....	127
5.18.3	Протокол TACACS+.....	129
5.18.4	Протокол управления сетью (SNMP)	131
5.18.5	Протокол удалённого мониторинга сети (RMON).....	135
5.18.6	Списки доступа ACL для управления устройством	142
5.18.7	Настройка доступа	143
5.19	Журнал аварий, протокол SYSLOG	147
5.20	Зеркалирование (мониторинг) портов	149
5.21	Функция SFlow.....	151
5.22	Функции диагностики физического уровня.....	153
5.22.1	Диагностика медного кабеля.....	153
5.22.2	Диагностика оптического трансивера	155
5.23	Функции обеспечения безопасности	157
5.23.1	Функции обеспечения защиты портов.....	157
5.23.2	Проверка подлинности клиента на основе порта (стандарт 802.1x).....	159
5.23.3	Контроль протокола DHCP и опция 82	166
5.23.4	Защита IP-адреса клиента (IP-source Guard)	170
5.23.5	Контроль протокола ARP (ARP Inspection).....	172
5.23.6	Настройка функции MAC Address Notification	174
5.24	Функции DHCP Relay посредника	176
5.25	Конфигурирование PPPoE Intermediate Agent.....	178
5.26	Конфигурирование ACL (списки контроля доступа).....	180
5.26.1	Конфигурирование ACL на базе IPv4	182
5.26.2	Конфигурирование ACL на базе IPv6	186
5.26.3	Конфигурирование ACL на базе MAC	188
5.26.4	Настройка временных интервалов «time-range» для списков доступа	190
5.27	Конфигурирование защиты от DoS-атак	191
5.28	Качество обслуживания - QoS	192
5.28.1	Настройка QoS.....	192
5.28.2	Статистика QoS	199
6	СЕРВИСНОЕ МЕНЮ, СМЕНА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ.....	201
6.1	Меню Startup.....	201

6.2	Обновление программного обеспечения с сервера TFTP	203
6.2.1	Обновление системного программного обеспечения	203
6.2.2	Обновление загрузочного файла устройства (начального загрузчика)	204
ПРИЛОЖЕНИЕ А ПРИМЕРЫ ПРИМЕНЕНИЯ И КОНФИГУРИРОВАНИЯ УСТРОЙСТВА		206
Настройка протокола множества связующих деревьев (MSTP)		206
Настройка selective-qinq		208
Настройка multicast-TV VLAN.....		209
ПРИЛОЖЕНИЕ Б ТИПОВЫЕ СХЕМЫ ПОСТРОЕНИЯ СЕТЕЙ НА БАЗЕ ПРОТОКОЛА EAPS.....		212
ПРИЛОЖЕНИЕ В ОПИСАНИЕ ПРОЦЕССОВ КОММУТАТОРА.....		214

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

Обозначение	Описание
[]	В квадратных скобках в командной строке указываются необязательные параметры, но их ввод предоставляет определенные дополнительные опции.
{ }	В фигурных скобках в командной строке указываются обязательные параметры.
«,» «-»	Данные знаки в описании команды используются для указания диапазонов.
« »	Данный знак в описании команды обозначает «или».
«/»	Данный знак при указании значений переменных разделяет возможные значения и значения по умолчанию.
<i>Курсив Calibri</i>	Курсивом Calibri указываются переменные или параметры, которые необходимо заменить соответствующим словом или строкой.
Полужирный курсив	Полужирным курсивом выделены примечания и предупреждения.
<Полужирный курсив>	Полужирным курсивом в угловых скобках указываются названия клавиш на клавиатуре.
Courier New	Полужирным Шрифтом Courier New записаны примеры ввода команд.
<code>Courier New</code>	Шрифтом Courier New в рамке с тенью указаны результаты выполнения команд.

Примечания и предупреждения



Примечания содержат важную информацию, советы или рекомендации по использованию и настройке устройства.



Предупреждения информируют пользователя о ситуациях, которые могут нанести вред устройству или человеку, привести к некорректной работе устройства или потере данных.

1 ВВЕДЕНИЕ

В последние годы наблюдается тенденция к осуществлению масштабных проектов по построению сетей связи в соответствии с концепцией NGN. Одной из основных задач при реализации крупных мультисервисных сетей является создание надежных и высокопроизводительных транспортных сетей, которые являются опорными в многослойной архитектуре сетей следующего поколения.

Для достижения высоких скоростей широко применяются технологии передачи информации Gigabit Ethernet (GE). Передача информации на высоких скоростях, особенно в сетях крупного масштаба, подразумевает выбор такой топологии сети, которая позволяет гибко осуществлять распределение высокоскоростных потоков.

Коммутаторы MES1024, MES1124, MES2124 могут использоваться на сетях крупных предприятий и предприятий малого и среднего бизнеса (SMB), в операторских сетях. Они обеспечивают высокую производительность, гибкость, безопасность и многоуровневое качество обслуживания (QoS).

В настоящем руководстве изложены назначение, технические характеристики, рекомендации по начальной настройке, синтаксис команд для конфигурирования, мониторинга и обновления программного обеспечения коммутатора.

2 ОПИСАНИЕ ИЗДЕЛИЯ

2.1 Назначение

Устройства MES1024/MES1124/MES2124 являются управляемыми стекируемыми коммутаторами, выполняющими свои коммутационные функции на канальном и сетевом уровнях модели OSI.

Сетевые коммутаторы MES1024 имеют в своём составе 24 порта Fast Ethernet с электрическими интерфейсами и 2 порта Gigabit Ethernet, совмещенные со слотами для установки SFP-трансиверов (combo-порты).

Сетевые коммутаторы MES1124 имеют в своём составе 24 порта Fast Ethernet с электрическими интерфейсами и 4 порта Gigabit Ethernet, совмещенные со слотами для установки SFP-трансиверов (combo-порты).

Сетевые коммутаторы MES2124 имеют в своём составе 24 порта Gigabit Ethernet с электрическими интерфейсами и 4 порта Gigabit Ethernet, совмещенные со слотами для установки SFP-трансиверов (combo-порты).



В комбинированных портах может быть активным только один из интерфейсов, но не оба одновременно.

2.2 Функции MES1024/MES1124/MES2124

2.2.1 Основные функции

В таблице 2.1 приведен список основных функций устройств MES1024/MES1124/MES2124.

Таблица 2.1 – Основные функции устройства

<p><i>Защита от блокировки очереди (NOL)</i></p>	<p>Блокировка возникает в случаях перегрузки выходных портов устройства трафиком от нескольких высокоактивных источников. Это может привести к потере трафика от других источников с низкой активностью. Для предотвращения таких ситуаций используются методы резервирования ресурсов коммутатора.</p>
<p><i>Поддержка обратного давления (Back pressure)</i></p>	<p>Метод обратного давления используется на полудуплексных соединениях для регулирования потока данных от встречного устройства путем создания коллизий. Метод позволяет избежать переполнения буферной памяти устройства и потери данных.</p>
<p><i>Поддержка MDI/MDIX</i></p>	<p>Автоматическое определение типа кабеля - перекрестный кабель или кабель прямого подключения.</p> <ul style="list-style-type: none"> – MDI (Media-Dependent Interface – прямой) – стандарт кабелей для подключения оконечных устройств; – MDIX (Media-Dependent Interface with Crossover – перекрестный) - стандарт кабелей для подключения концентраторов и коммутаторов.
<p><i>Поддержка сверхдлинных кадров (Jumbo frames)</i></p>	<p>Сетевой коммутатор моделей MES1024, MES1124, MES2124 способен поддерживать передачу сверхдлинных кадров, что позволяет передавать данные меньшим числом пакетов. Это снижает объем служебной информации, время обработки и перерывы. Поддерживаются пакеты размером до 10 К.</p>

<p><i>Управление потоком (IEEE 802.3X)</i></p>	<p>Управление потоком позволяет соединять низкоскоростное устройство с высокоскоростным. Для предотвращения переполнения буфера низкоскоростное устройство имеет возможность отправлять пакет PAUSE, тем самым информируя высокоскоростное устройство о необходимости сделать паузу при передаче пакетов.</p>
<p><i>Работа в стеке устройств¹</i></p>	<p>Коммутатор поддерживает объединение до 4 устройств в стек, в этом случае коммутаторы рассматриваются как единое устройство с общими настройками. Возможны две топологии построения стека – кольцо и цепочка. При этом параметры портов всех устройств, включенных в стек можно задать с коммутатора, работающего в режиме «мастер». Стекирование устройств позволяет снизить трудоемкость управления сетью.</p>

2.2.2 Функции при работе с MAC – адресами

В таблице 2.2 приведены функции устройств MES1024/MES1124/MES2124 при работе с MAC-адресами.

Таблица 2.2 – Функции работы с MAC-адресами

<p><i>Таблица MAC-адресов</i></p>	<p>Коммутатор составляет в памяти таблицу, в которой устанавливается соответствие между MAC-адресами и интерфейсами коммутатора. MES1024/MES1124/MES2124 поддерживает таблицу размером до 16K MAC-адресов и резервирует определенные MAC-адреса для использования системой.</p>
<p><i>Режим обучения</i></p>	<p>В отсутствие обучения, данные, поступающие на какой-либо порт, передаются на все остальные порты коммутатора. В режиме обучения коммутатор анализирует кадры и, определив MAC-адрес отправителя, заносит его в таблицу маршрутизации. Впоследствии, поступивший кадр, предназначенный для хоста, MAC-адрес которого уже есть в таблице, передается только через указанный порт в таблице.</p>
<p><i>Поддержка передачи на несколько MAC-адресов (MAC Multicast Support)</i></p>	<p>Данная функция позволяет устанавливать соединения «один ко многим» и «многие ко многим». Таким образом, кадр, адресованный многоадресной группе, передается на каждый порт, входящий в группу.</p>
<p><i>Автоматическое время хранения MAC- адресов (Automatic Aging for MAC Addresses)</i></p>	<p>Если от устройства с определенным MAC-адресом за определенный период времени не поступают пакеты, то запись в таблице маршрутизации для данного адреса устаревает и удаляется. Это позволяет поддерживать таблицу в актуальном состоянии.</p>
<p><i>Статические записи MAC (Static MAC Entries)</i></p>	<p>Сетевой коммутатор позволяет пользователю определить статические записи соответствий MAC-адресов интерфейсам, которые сохраняются в таблице маршрутизации.</p>

¹ В данной версии ПО не поддерживается

2.2.3 Функции второго уровня сетевой модели OSI

В таблице 2.3 приведены функции и особенности *второго уровня (уровень 2 OSI)*

Таблица 2.3 – Описание функций второго уровня (уровень 2 OSI)

Поддержка VLAN	Сетевой коммутатор MES1024/MES1124/MES2124 поддерживает работу виртуальных сетей VLAN.
Функция IGMP Snooping	Реализация протокола IGMP позволяет MES1024/MES1124/MES2124 на основе информации, полученной при анализе содержимого IGMP пакетов, определить, какие устройства в сети участвуют в группах многоадресной рассылки, и адресовать трафик на соответствующие порты.
Функция MLD Snooping	Реализация функции MLD Snooping позволяет устройству минимизировать многоадресный IPv6 трафик.
Функция Multicast-TV VLAN	Функция, позволяющая перенаправлять многоадресный трафик из заданной VLAN (multicast VLAN) в порт пользователя на основании IGMP-сообщений, что позволяет уменьшить нагрузку на uplink-порт коммутатора. Функция применяется в решениях III-play.
Защита от широковещательного «шторма» (Broadcast Storm Control)	Широковещательный шторм – это размножение широковещательных сообщений в каждом узле, которое приводит к лавинообразному росту их числа и парализует работу сети. Устройство MES1024/MES1124/MES2124 имеет функцию, позволяющую ограничить скорость передачи многоадресных и широковещательных кадров, принятых и переданных коммутатором.
Зеркалирование портов (Port Mirroring)	Зеркалирование портов позволяет дублировать трафик наблюдаемых портов, пересылая входящие и/или исходящие пакеты на контролирующий порт. У пользователя MES1024/MES1124/MES2124 есть возможность задать контролирующий и контролируемые порты и выбрать тип трафика (входящий и/или исходящий), который будет передан на контролирующий порт.
Изоляция портов (Protected ports)	Данная функция позволяет назначить порту его uplink-порт, на который безусловно будет перенаправляться весь трафик, обеспечивая тем самым изоляцию с другими портами (в пределах одного коммутатора).
Private VLAN Edge	Данная функция позволяет изолировать группу портов (в пределах одного коммутатора), находящихся в одном широковещательном домене между собой, позволяя при этом обмен трафиком с другими портами, находящимися в этом же широковещательном домене, но не принадлежащими к этой группе.
Private VLAN	Обеспечивает изоляцию между устройствами, находящимися в одном широковещательном домене, в пределах всей L2-сети. Реализованы только два режима работы порта Promiscuous и Isolated (Isolated-порты не могут обмениваться друг с другом).
Поддержка протокола STP (Spanning Tree Protocol)	Spanning Tree Protocol — сетевой протокол, основной задачей которого является приведение сети Ethernet с избыточными соединениями к древовидной топологии, исключающей петли. Коммутаторы обмениваются конфигурационными сообщениями, используя кадры специального формата, и выборочно включают и отключают порты устройства.
Поддержка протокола RSTP (IEEE 802.1w Rapid spanning tree protocol)	Rapid (быстрый) STP (RSTP) – является усовершенствованием протокола STP, характеризуется меньшим временем приведения сети к древовидной топологии и имеет более высокую устойчивость.
Протокол EAPS	EAPS (Ethernet Automatic Protection Switching) – протокол, обеспечивающий исключение зацикливания трафика в сетях с кольцевой топологией, а также предназначенный для быстрого восстановления прохождения трафика в

	случае аварии на отдельном участке сети. EAPS обеспечивает время восстановления существенно меньше, чем протоколы spanning tree.
<i>Протокол ERPS (Ethernet Ring Protection Switching)</i>	Протокол предназначен для повышения устойчивости и надежности сети передачи данных, имеющей кольцевую топологию, за счет снижения времени восстановления сети в случае аварии. Время восстановления не превышает 1 секунды, что существенно меньше времени перестройки сети при использовании протоколов семейства spanning tree.
<i>Поддержка GVRP (GARP VLAN)</i>	Протокол регистрации GARP VLAN обеспечивает динамическое добавление/удаление групп VLAN на портах MES1024/MES1124/MES2124. Если включен протокол GVRP, коммутатор определяет, а затем распространяет данные о принадлежности к VLAN на все порты, являющиеся частью активной топологии.
<i>Поддержка VLAN на базе портов (Port-Based VLAN)</i>	Распределение по группам VLAN выполняется по входящим портам. Данное решение позволяет использовать на каждом порту только одну группу VLAN.
<i>Поддержка 802.1Q</i>	IEEE 802.1Q — открытый стандарт, который описывает процедуру тегирования трафика для передачи информации о принадлежности к VLAN. Позволяет использовать несколько групп VLAN на одном порту.
<i>Агрегация каналов (группы каналов LAG)</i>	<p>В устройстве MES1024/MES1124/MES2124 поддерживается функция создания групп каналов. Агрегация каналов (Link aggregation, trunking) или IEEE 802.3ad — технология объединения нескольких физических каналов в один логический. Это способствует не только увеличению пропускной способности магистральных каналов коммутатор—коммутатор или коммутатор—сервер, но и повышению их надежности. Возможны три типа балансировки нагрузки между каналами: на основании MAC-адресов, на основании IP адресов и на основании порта назначения.</p> <p>Сетевой коммутатор позволяет определить до восьми объединенных каналов, каждый из которых может содержать до восьми портов. Группа LAG состоит из портов с одинаковой скоростью, работающих в дуплексном режиме.</p>
<i>Динамические группы каналов (протокол LACP)</i>	<p>Протокол LACP обеспечивает автоматическое объединение отдельных каналов между двумя устройствами (коммутатор—коммутатор или коммутатор—сервер) в единый канал передачи данных.</p> <p>В протоколе постоянно определяется возможность объединения каналов, и в случае отказа соединения, входящего в объединенный канал, его трафик автоматически перераспределяется по неотказавшим компонентам объединенного канала.</p>
<i>Поддержка Auto Voice VLAN</i>	Предоставляет возможность идентифицировать голосовой трафик на основании OUI (Organizationally Unique Identifier – первые 24 бита MAC-адреса). Если в MAC-таблице коммутатора присутствует MAC-адрес с OUI голосового шлюза или же IP-телефона, то данный порт автоматически добавляется в voice vlan (идентификация по протоколу SIP или же по MAC-адресу получателя не поддерживается)
<i>Selective Q-in-Q</i>	Позволяет выполнять действия с внешним идентификатором VLAN SPVLAN (Service Provider's VLAN) на основе сконфигурированных правил фильтрации по внутреннему идентификатору VLAN (Customer VLAN), по MAC-адресу или IP-адресу источника данных, по типу Ethernet-трафика (EtherType). Применение Selective Q-in-Q позволяет разобрать трафик абонента на несколько VLAN, добавить или изменить метку SPVLAN у пакета на отдельном участке сети

2.2.4 Функции третьего уровня сетевой модели OSI

В таблице 2.4 приведены функции третьего уровня (уровень 3 OSI)

Таблица 2.4 – Описание функций третьего уровня (Layer 3)

<i>Клиенты BOOTP и DHCP (Dynamic Host Configuration Protocol)</i>	Устройство MES1024/MES1124/MES2124 способно автоматически получать IP-адрес по протоколу BOOTP/DHCP.
<i>Протокол ARP (Address Resolution Protocol)</i>	ARP – протокол сопоставления IP-адреса и физического адреса устройства. Соответствие устанавливается на основе анализа ответа от узла сети, адрес узла запрашивается в широковещательном пакете.

2.2.5 Функции QoS

В таблице 2.5 приведены основные функции качества обслуживания (Quality of Service)

Таблица 2.5 – Основные функции качества обслуживания

<i>Поддержка приоритетных очередей</i>	Устройство поддерживает 4 выходных очередей с разными приоритетами для каждого порта. Распределение пакетов по очередям может производиться в результате классификации пакетов по различным полям в заголовках пакетов.
<i>Поддержка класса обслуживания 802.1p</i>	Стандарт 802.1p специфицирует метод указания приоритета кадра и алгоритм использования приоритета в целях своевременной доставки чувствительного к временным задержкам трафика. Стандарт 802.1p определяет восемь уровней приоритетов. MES1024/MES1124/MES2124 может использовать значение приоритета 802.1p для распределения кадров по приоритетным очередям.

2.2.6 Функции обеспечения безопасности

Таблица 2.6 – Функции обеспечения безопасности

<i>DHCP snooping</i>	Функция коммутатора, предназначенная для защиты от атак с использованием протокола DHCP. Обеспечивает фильтрацию DHCP сообщений, поступивших с ненадежных портов путем построения и поддержания базы данных привязки DHCP (DHCP snooping binding database). DHCP snooping выполняет действия брандмауэра между ненадежными портами и серверами DHCP.
<i>Опция 82 протокола DHCP</i>	Опция, которая позволяет проинформировать DHCP – сервер о том, с какого DHCP-ретранслятора и через какой порт пришел запрос. По умолчанию коммутатор, использующий функцию DHCP snooping, обнаруживает и отбрасывает любой DHCP-запрос содержащий опцию 82, который он получил через ненадежный (untrusted) порт.
<i>UDP relay</i>	Перенаправление широковещательного UDP-трафика на указанный IP-адрес
<i>IP Source address guard</i>	Функция коммутатора, которая ограничивает IP-трафик, фильтруя его на основании таблицы соответствий базы данных привязки DHCP – DHCP snooping и статически сконфигурированных IP-адресов. Функция используется для борьбы с подменой IP-адресов.
<i>Dynamic ARP Inspection (Protection)</i>	Функция коммутатора, предназначенная для защиты от атак с использованием протокола ARP. Сообщение, которое поступает с

	<p>ненадежного порта, подвергается проверке – соответствует ли IP-адрес в теле принятого ARP-пакета IP-адресу отправителя.</p> <p>Если адреса не совпадают, то коммутатор отбрасывает пакет.</p>
<i>L2 – L3 – L4 ACL (Access Control List)</i>	<p>На основе информации, содержащейся в заголовках уровней 2, 3 и 4, у администратора есть возможность настроить правила, согласно которым пакет будет обработан, либо отброшен.</p>
<i>Time-Based ACL</i>	<p>Позволяет сконфигурировать временные рамки, в течение которых данный ACL будет действовать</p>
<i>Поддержка блокировки портов</i>	<p>Основная функция блокировки – повысить безопасность сети, предоставляя доступ к порту коммутатора только для устройств имеющих MAC – адреса, закрепленные за этим портом.</p>
<i>Проверка подлинности на основе порта (802.1x)</i>	<p>Проверка подлинности IEEE 802.1x представляет собой механизм контроля доступа к ресурсам через внешний сервер. Прошедшие проверку подлинности пользователи получают доступ к ресурсам выбранной сети.</p>
<i>PPPoE IA</i>	<p>Функция позволяет дополнять пакеты PPPoE Discovery информацией, характеризующей интерфейс доступа. Это необходимо для идентификации пользовательского интерфейса на сервере доступа (BRAS, Broadband Remote Access Server).</p>

2.2.7 Функции управления коммутатором

Таблица 2.7 – Основные функции управления коммутаторов MES1024/MES1124/MES2124

<i>Загрузка и выгрузка файла настройки</i>	<p>Параметры устройств MES1024/MES1124/MES2124 сохраняются в файле настройки, который содержит данные конфигурации как всей системы в целом, так и определенного порта устройства.</p>
<i>Протокол TFTP (Trivial File Transfer Protocol)</i>	<p>Протокол TFTP используется для операций записи и чтения файлов. Протокол основан на транспортном протоколе UDP.</p> <p>Устройства MES1024/MES1124/MES2124 поддерживают загрузку и передачу по данному протоколу файлов настройки и образов программного обеспечения.</p>
<i>Удаленный мониторинг (RMON)</i>	<p>Удаленный мониторинг (RMON) - средство мониторинга компьютерных сетей, расширение SNMP. Совместимые устройства позволяют собирать диагностические данные с помощью станции управления сетью. RMON - это стандартная база MIB, в которой определены текущая и предыдущая статистика уровня MAC и объекты управления, предоставляющие данные в реальном времени.</p>
<i>Протокол SNMP</i>	<p>Протокол SNMP используется для мониторинга и управления сетевым устройством. Для управления доступом к системе определяется список записей сообщества, каждая из которых содержит привилегии доступа.</p>
<i>Интерфейс командной строки (CLI)</i>	<p>Управление устройствами MES1024/MES1124/MES2124 посредством CLI осуществляется локально через последовательный порт RS-232, либо удаленно через telnet, ssh. Интерфейс командной строки консоли (CLI) является промышленным стандартом. Интерпретатор CLI предоставляет список команд и ключевых слов для помощи пользователю и сокращению объема вводимых данных.</p>

<i>Syslog</i>	<i>Syslog</i> – протокол, обеспечивающий передачу сообщений о происходящих в системе событиях, а также уведомлений об ошибках удаленным серверам.
<i>SNTP (Simple Network Time Protocol)</i>	Протокол <i>SNTP</i> - протокол синхронизации времени сети, гарантирует точность синхронизации времени сетевого устройства с сервером до миллисекунды.
<i>Traceroute</i>	<i>Traceroute</i> – служебная функция, предназначенная для определения маршрутов передачи данных в IP-сетях.
<i>Управление контролируемым доступом – уровни привилегий</i>	Администратор может определить уровни привилегий доступа для пользователей устройства и характеристики для каждого уровня привилегий (только для чтения – 1 уровень, полный доступ – 15 уровень)
<i>Блокировка интерфейса управления</i>	Коммутатор способен устанавливать запрет доступа к каждому интерфейсу управления (SNMP, Telnet, SSH). Запрет может быть установлен отдельно для каждого типа доступа: Telnet(CLI over Telnet Session) Secure Shell (CLI over SSH) SNMP
<i>Локальная аутентификация</i>	Для локальной аутентификации поддерживается хранение паролей в базе данных коммутатора.
<i>Фильтрация IP адресов для SNMP</i>	Доступ по SNMP разрешается для определенных IP-адресов, являющихся членами SNMP-сообщества.
<i>Клиент RADIUS</i>	Протокол RADIUS используется для аутентификации, авторизации и учета. Сервер RADIUS использует базу данных пользователей, которая содержит данные проверки подлинности для каждого пользователя. Коммутаторы MES1024/MES1124/MES2124 поддерживают клиентскую часть протокола RADIUS.
<i>TACACS+ (Terminal Access Controller Access Control System)</i>	Устройство предоставляет поддержку проверки подлинности клиентов посредством протокола TACACS+. Протокол TACACS+ обеспечивает централизованную систему безопасности для проверки пользователей, получающих доступ к устройству, а так же централизованную систему управления при соблюдении совместимости с RADIUS и другими процессами проверки подлинности.
<i>Сервер SSH</i>	Функция сервера SSH позволяет клиенту SSH установить с устройством защищенное соединение для управления им.
<i>Поддержка макрокоманд</i>	Данная функция предоставляет возможность создавать макрокоманды, представляющие собой набор команд, и применять их для оперативного управления устройством.

2.2.8 Дополнительные функции

В таблице приведены дополнительные функции устройства.

Таблица 2.8 – Дополнительные функции устройства

<p><i>Виртуальный кабельный тестер (VCT)</i></p>	<p>Сетевые коммутаторы MES1024/MES1124/MES2124 имеют в своём составе программные и аппаратные средства, позволяющие выполнять функции тестирования кабеля – VCT:</p> <ul style="list-style-type: none"> – определение проблем связи при использовании медных кабелей (обрыв, замыкание проводов); – отчет по результатам тестирования.
<p><i>Диагностика оптического трансивера</i></p>	<p>Устройство позволяет тестировать оптический трансивер. При тестировании отслеживаются такие параметры, как ток и напряжение питания, температура трансивера, мощность сигнала на приёме и передаче. Диагностика доступна только для трансиверов, поддерживающих функцию Digital Diagnostics Monitoring (DDM).</p>
<p><i>Green Ethernet</i></p>	<p>Данный механизм позволяет коммутатору снизить энергопотребление за счет перевода неактивных электрических портов в экономичный режим.</p>

2.3 Основные технические характеристики

Основные технические параметры коммутаторов приведены в таблице 2.9

Таблица 2.9 – Основные технические характеристики

Общие параметры	
Пакетный процессор	Marvell 98DX1035 / 98DX3035
Интерфейсы	MES1024 24x 10/100Base-T 2x (10/100/1000Base-T / 1000Base-X)
	MES1124 24x 10/100Base-T 4x (10/100/1000Base-T / 1000Base-X)
	MES2124 24x 10/100/1000Base-T 4x (10/100/1000Base-T / 1000Base-X)
Оптические трансиверы	SFP
Дуплексный/Полудуплексный режим	Дуплексный/ полудуплексный режим для электрических портов, дуплексный режим для оптических портов
Производительность коммутатора	MES1024 8,8 Гбит/с
	MES1124 12,8 Гбит/с
	MES2124 56 Гбит/с
Объем буферной памяти	8 Mb
Скорость передачи данных	Электрические интерфейсы 10/100/1000 Мбит/с Оптические интерфейсы 1Гбит/с
Таблица MAC-адресов	16К записей
Поддержка VLAN	согласно 802.1Q до 4К
Качество обслуживания QoS	Приоритезация трафика, 4 уровня. 4 выходных очереди с разными приоритетами для каждого порта.
Multicast	До 1000 статических multicast-групп
Соответствие стандартам	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-T Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z Fiber Gigabit Ethernet ANSI/IEEE 802.3 автоопределение скорости IEEE 802.3x контроль потоков данных IEEE 802.3ad объединение каналов LACP IEEE 802.1p приоритезация трафика IEEE 802.1q виртуальные локальные сети VLAN IEEE 802.1v IEEE 802.3 ac IEEE 802.1d связующее дерево STP IEEE 802.1w быстрое связующее дерево RSTP IEEE 802.1s множество связующих деревьев MSTP IEEE 802.1x аутентификация пользователей

Управление	
Локальное управление	Консоль RS-232
Удаленное управление	telnet, ssh, SNMP
Физические характеристики и условия окружающей среды	
Напряжение питания	сеть переменного тока: 220В, 50 Гц
Потребляемая мощность	MES1024: не более 25Вт MES1124: не более 25Вт MES2124: не более 30Вт
Масса	не более 2 кг
Габаритные размеры	430x44x138 мм
Интервал рабочих температур	от -10 до +45 °С
Интервал температуры хранения	от -40 до +70 °С
Относительная влажность при эксплуатации (без образования конденсата)	не более 80%
Относительная влажность при хранении (без образования конденсата)	от 10% до 95%
Средний срок службы	20 лет

2.4 Конструктивное исполнение

В данном разделе описано конструктивное исполнение устройств. Представлены изображения передней и боковых панелей устройства, описаны разъемы, светодиодные индикаторы и органы управления.

Ethernet-коммутаторы MES1024/MES1124/MES2124 выполнены в металлическом корпусе с возможностью установки в 19” каркас типоразмера 1U.

2.4.1 Передняя панель устройства

Внешний вид передней панели MES1024, MES1124, MES2124 показан на рисунках 1-3.

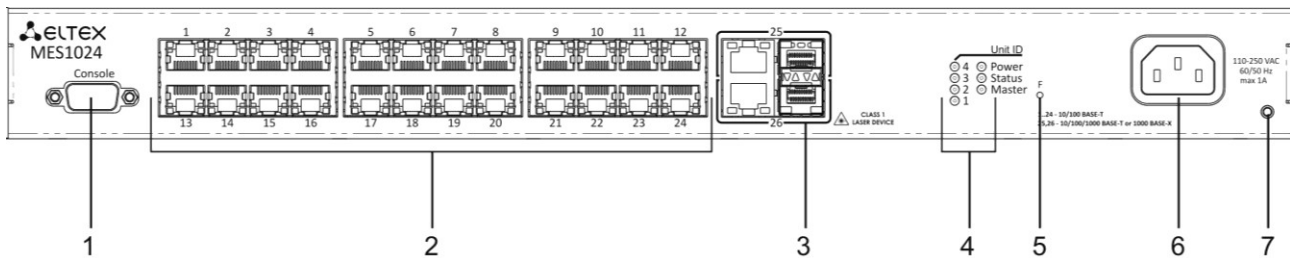


Рисунок 1 – MES1024, передняя панель

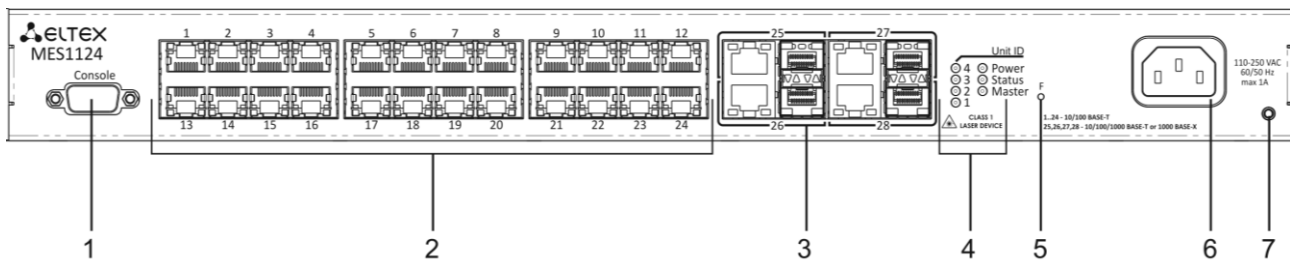


Рисунок 2 – MES1124, передняя панель

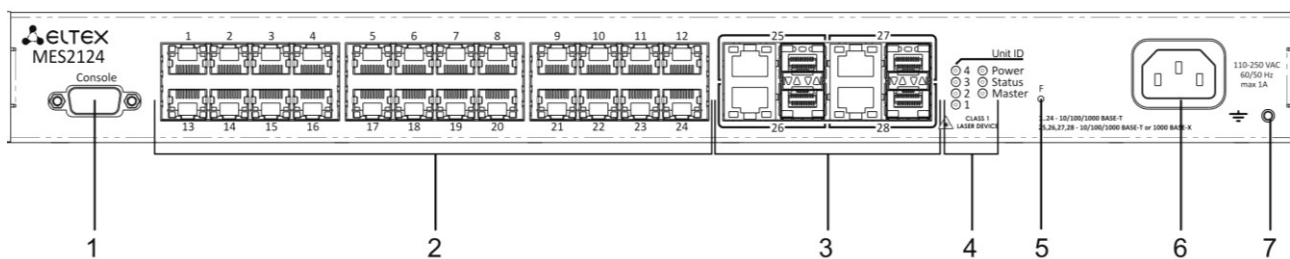


Рисунок 3 – MES2124, передняя панель

В таблице 2.10 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели коммутатора.

Таблица 2.10 – Описание разъемов, индикаторов и органов управления передней панели

№	Элемент панели		Описание
1	Console		Консольный порт RS-232 для локального управления устройством
2	[1 .. 24]	MES1024 MES1124	24 порта 10/100 Base-T (RJ-45)
		MES2124	24 порта 10/100/1000 Base-T (RJ-45)
3	25,26	MES1024	комбо-порты: порты 10/100/1000 Base-T (RJ45) и слоты для установки трансиверов 1000Base-X (SFP)
	25,26,27,28	MES1124 MES2124	
4	Unit ID (1-4)		Индикаторы номера устройства в стеке
	Power		Индикатор питания устройства
	Status		Индикатор состояния устройства
	Master		Индикатор режима работы устройства в стеке - ведущий или ведомый
5	F		Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: - при нажатии на кнопку длительностью менее 10 с происходит перезагрузка устройства. - при нажатии на кнопку длительностью более 10 с. происходит сброс настроек устройства до заводской конфигурации.
6	~150-250VAC, 60/50Hz		Разъем для подключения к источнику электропитания
7			Болт для заземления устройства.



Порты 25, 26, 27, 28 являются комбинированными. В комбинированных портах может быть активным только один из интерфейсов, но не оба одновременно.

2.4.2 Боковые панели устройства

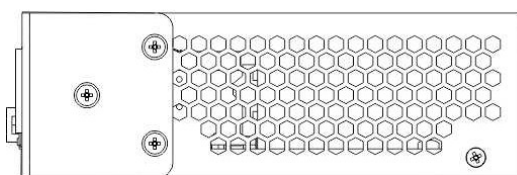


Рисунок 4 – Правая боковая панель Ethernet-коммутатора MES1024/MES1124/MES2124

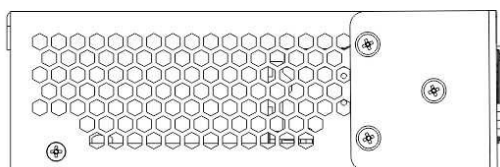


Рисунок 5 – Левая боковая панель Ethernet-коммутатора MES1024/MES1124/MES2124

На боковых панелях устройства расположены вентиляционные решетки, которые служат для отвода тепла. Не закрывайте вентиляционные отверстия посторонними предметами. Это может привести к перегреву компонентов устройства и вызвать нарушения в его работе. Рекомендации по установке устройства расположены в разделе «Установка и подключение».

2.4.3 Световая индикация

Состояние интерфейсов Ethernet индицируется двумя светодиодными индикаторами, SPEED янтарного цвета и LINK/ACT зеленого цвета, расположенными возле каждого интерфейсного разъема. Расположение светодиодов показано на рисунках 5, 6.

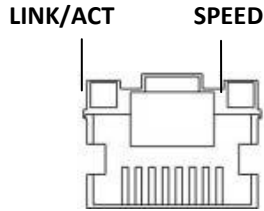


Рисунок 6– Внешний вид разъема RJ-45

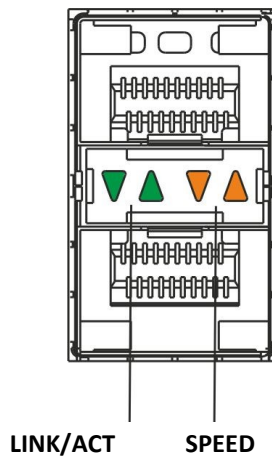


Рисунок 7– Внешний вид разъема с SFP-трансиверами

Таблица 2.11 – Световая индикация состояния электрических и оптических интерфейсов Ethernet

Свечение индикатора LINK/ACT	Свечение индикатора SPEED	Состояние интерфейса Ethernet
Выключен	Выключен	Порт выключен или соединение не установлено
Горит постоянно	Выключен	Установлено соединение на скорости 10 или 100Мбит/с
Горит постоянно	Горит постоянно	Установлено соединение на скорости 1000Мбит/с
Мигание	X	Идет передача данных

Индикаторы *Unit ID* (1-4) служат для обозначения номера устройства в стеке.

Системные индикаторы (Power, Status, Master) служат для определения состояния работы узлов коммутатора MES1024/MES1124/MES2124.

Таблица 2.12 – Световая индикация системных индикаторов

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
<i>Power</i>	Состояние источников питания	Выключен	Питание выключено
		Зеленый, горит постоянно	Питание включено, нормальная работа устройства
		Красный	Авария как минимум одного из вторичных источников питания.
<i>Status</i>	Состояние устройства	Зеленый, горит постоянно	Нормальная работа устройства
		Красный, горит постоянно	Отказ управляющей или коммутирующей части устройства
<i>Master</i>	Признак ведущего устройства при работе в стеке	Зеленый, горит постоянно	Устройство является «мастером» стека
		Выключен	Устройство не является «мастером» в стеке или не задан режим стекирования



В том случае, когда коммутатор работает в автономном режиме без стекирования, индикаторы *Master* и *Unit ID* выключены.

2.5 Комплект поставки

В базовый комплект поставки входят:

- Ethernet-коммутатор MES1024/MES1124/MES2124;
- шнур питания;
- комплект крепежа в стойку;
- документация.



По заказу покупателя в комплект поставки могут быть включены SFP -трансиверы.

3 УСТАНОВКА И ПОДКЛЮЧЕНИЕ

В данном разделе описаны процедуры установки оборудования в стойку и подключения к питающей сети.

3.1 Крепление кронштейнов

В комплект поставки устройства входят кронштейны для установки в стойку и винты для крепления кронштейнов к корпусу устройства. Для установки кронштейнов:

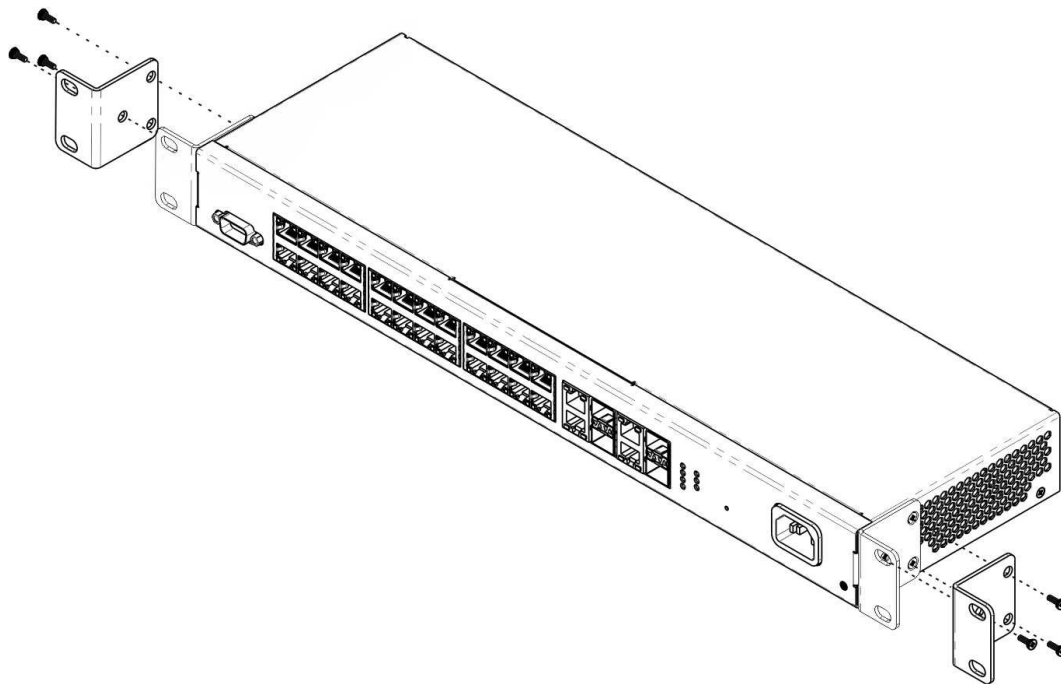


Рисунок 8– Крепление кронштейнов

1. Совместите три отверстия для винтов на кронштейне с такими же отверстиями на боковой панели устройства.
2. С помощью отвертки прикрепите кронштейн винтами к корпусу.
3. Повторите действия 1,2 для второго кронштейна.

3.2 Установка устройства в стойку

Для установки устройства в стойку:

1. Приложите устройство к вертикальным направляющим стойки.
2. Совместите отверстия кронштейнов с отверстиями на направляющих стойки. Используйте отверстия в направляющих на одном уровне с обеих сторон стойки, для того чтобы устройство располагалось горизонтально.
3. С помощью отвертки прикрепите коммутатор к стойке винтами.

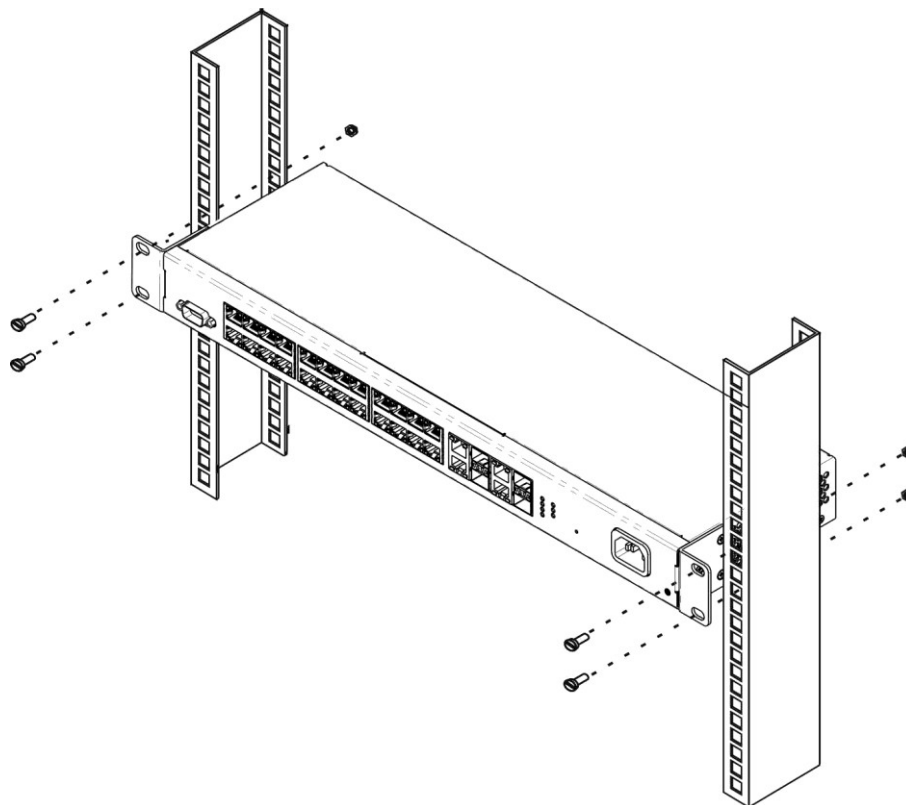


Рисунок 9 – Установка устройства в стойку

На рисунке 8 приведен пример размещения коммутаторов MES1024/MES1124/MES2124 в стойке.

○	MES1024/MES1124/MES2124 N1	○
○	Кабельный органайзер	○
○	MES1024/MES1124/MES2124 N2	○
○	Кабельный органайзер	○
○	MES1024/MES1124/MES2124 N3	○
○	Кабельный органайзер	○
○	MES1024/MES1124/MES2124 N4	○
○	Кабельный органайзер	○
○	MES1024/MES1124/MES2124 N5	○
○	Кабельный органайзер	○

Рисунок 10 – Размещение коммутаторов MES1024/MES1124/MES2124 в стойке

Минимальное расстояние между коммутаторами по высоте – не менее 1U.

При установке коммутаторов вблизи приборов с повышенным тепловыделением расстояние необходимо увеличить.

3.3 Установка и удаление SFP-трансиверов.



Установка оптических модулей может производиться как при выключенном, так и при включенном устройстве.

1. Вставьте верхний SFP-модуль в слот открытой частью разъема вниз, а нижний SFP-модуль открытой частью разъема вверх.

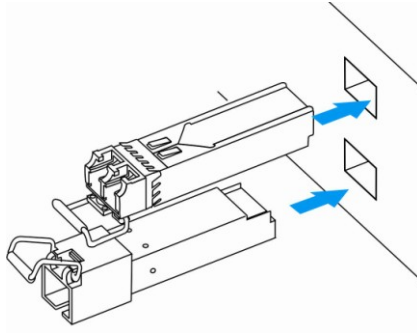


Рисунок 11 – Установка SFP-трансиверов

2. Надавите на модуль. Когда он встанет на место, вы услышите характерный щелчок.

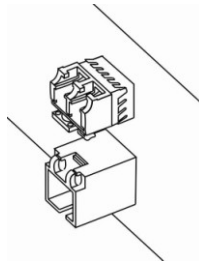


Рисунок 12 – Установленные SFP-трансиверы

Для удаления трансивера:

1. Откройте защелку модуля.

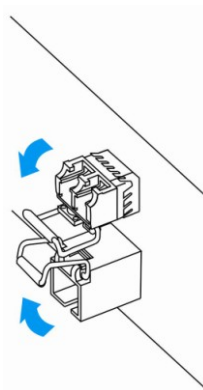


Рисунок 13 – Открытие защелки SFP-трансиверов

2. Извлеките модуль из слота.

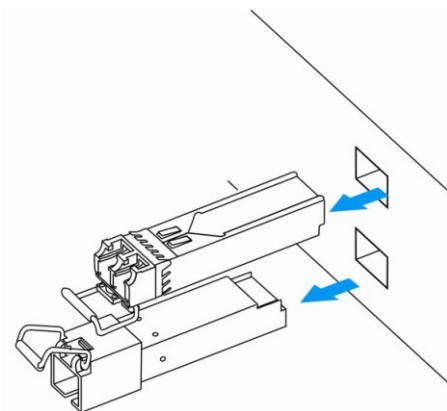


Рисунок 14 – Извлечение SFP-трансиверов

3.4 Подключение питающей сети

Порядок установки устройства:

1. Смонтировать устройство. В случае установки устройства в 19" конструктив, необходимо прикрепить к нему кронштейны, входящие в комплект устройства (см. п/п 3.1).
2. Заземлить корпус устройства. Это необходимо выполнить прежде, чем к устройству будет подключена питающая сеть. Заземление необходимо выполнять изолированным многожильным проводом. Устройство заземления и сечение заземляющего провода должны соответствовать требованиями ПУЭ.
3. Если предполагается подключение компьютера или иного оборудования к консольному порту коммутатора, это оборудование также должно быть надежно заземлено.
4. Подключить к устройству кабель питания. Питание устройства должно осуществляться от розетки с заземляющим контактом. Источник питания - сеть переменного тока 220В 50/60 Гц. Следует использовать кабель, входящий в комплект устройства.
5. Включить питание устройства и убедиться в отсутствии аварий по состоянию индикаторов на передней панели.

4 ВКЛЮЧЕНИЕ УСТРОЙСТВА, НАЧАЛЬНОЕ КОНФИГУРИРОВАНИЕ.

Коммутатор оснащен консольным портом, который предоставляет доступ к диагностике, управлению и мониторингу устройства. В этом разделе описаны возможности консольного порта устройства и процедуры начального конфигурирования.

4.1 Настройка терминала

Для связи с коммутатором через консольный порт на компьютере необходимо запустить программу эмуляции терминала (HyperTerminal, TeraTerm) и произвести следующие настройки:

1. Выбрать соответствующий последовательный порт компьютера.
2. Установить скорость передачи данных – 9600 бод.
3. Задать формат данных: 8бит данных, 1 стоповый бит, без контроля четности.
4. Отключить аппаратное и программное управление потоком данных.
5. Задать режим эмуляции терминала VT100 (многие терминальные программы используют данный режим эмуляции терминала в качестве режима по умолчанию).

4.2 Включение устройства

Подготовить оборудование к работе в соответствии с требованиями раздела 3.

Установить соединение консоли коммутатора (порт «console») с разъемом последовательного интерфейса компьютера, на котором установлено программное обеспечение эмуляции терминала.

Включить коммутатор. При каждом включении запускается процедура «тестирования системы при включении» (POST), которая позволяет определить работоспособность устройства перед загрузкой основной программы.

Отображение хода выполнения процедуры POST на коммутаторе:

```
Boot1 Checksum Test.....PASS
Boot2 Checksum Test.....PASS
Flash Image Validation Test.....PASS

BOOT Software Version 0.0.0.3 Built 23-Feb-2011 17:40:14

Networking device with CPU based on arm926ejs core. 128 MByte SDRAM.
I-Cache 16 KB. D-Cache 16 KB. L2 Cache 256 KB. Cache Enabled.

MAC Address : 02:11:12:13:14:27.

Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom.
```

Спустя две секунды после завершения процедуры POST начинается автозагрузка программного обеспечения коммутатора. Для выполнения специальных процедур используется сервисное меню, войти в которое можно прервав загрузку нажатием клавиши <Esc> или <Enter> в течение этого времени. Описание возможностей управления устройством средствами сервисного меню представлено в разделе 6.

Пример дальнейшей загрузки устройства.

```

Preparing to decompress...
 100%
Decompressing SW from image-2
 100%

OK
Running from RAM...

*****
*** Running SW Ver. 1.0.18 Date 23-Nov-2011 Time 18:14:56 ***
*****

HW version is V00
Base Mac address is: 02:11:12:13:14:27
Dram size is : 128M bytes
Dram first block size is : 98304K bytes
Dram first PTR is : 0x1C00000
Dram second block size is : 4096K bytes
Dram second PTR is : 0x7C00000
Flash size is: 16M
23-Nov-2011 18:15:04 %CDB-I-LOADCONFIG: Loading running configuration.
23-Nov-2011 18:15:04 %CDB-I-LOADCONFIG: Loading startup configuration.
The monitor is activated with Trace Enabled.
It will be automatic enabled after system reset also.
Device configuration:
Slot 1 - Eltex MES-2124
Device 0: GT_98DX1035 (AlleyCat)

-----
-- Unit Standalone --
-----

23-Nov-2011 18:15:16 %Entity-I-SEND-ENT-CONF-CHANGE-TRAP: entity configuration
change trap.
Tapi Version: v1.9.5
Core Version: v1.9.5
23-Nov-2011 18:15:29 %INIT-I-InitCompleted: Initialization task is completed

23-Nov-2011 18:15:41 %SNMP-I-CDBITEMSNUM: Number of running configuration items
loaded: 12

23-Nov-2011 18:15:41 %SNMP-I-CDBITEMSNUM: Number of startup configuration items
loaded: 12

console>
23-Nov-2011 18:15:43 %LINK-W-Down: fa1/0/1
23-Nov-2011 18:15:43 %LINK-W-Down: fa1/0/2
23-Nov-2011 18:15:43 %LINK-W-Down: fa1/0/3
23-Nov-2011 18:15:43 %LINK-W-Down: fa1/0/4
23-Nov-2011 18:15:43 %LINK-W-Down: fa1/0/5
23-Nov-2011 18:15:43 %LINK-W-Down: fa1/0/6
23-Nov-2011 18:15:44 %LINK-W-Down: fa1/0/7
23-Nov-2011 18:15:44 %LINK-W-Down: fa1/0/8
23-Nov-2011 18:15:44 %LINK-W-Down: fa1/0/9
23-Nov-2011 18:15:44 %LINK-W-Down: fa1/0/10
23-Nov-2011 18:15:44 %LINK-W-Down: fa1/0/11
23-Nov-2011 18:15:44 %LINK-W-Down: fa1/0/12
23-Nov-2011 18:15:44 %LINK-W-Down: fa1/0/13
23-Nov-2011 18:15:44 %LINK-W-Down: fa1/0/14
23-Nov-2011 18:15:44 %LINK-W-Down: fa1/0/15
23-Nov-2011 18:15:45 %LINK-W-Down: fa1/0/16
23-Nov-2011 18:16:31 %SYSLOG-N-LOGGING: Logging started.
23-Nov-2011 18:17:51 %INIT-I-Startup: Warm Startup

```

После успешной загрузки коммутатора необходимо ввести имя пользователя и пароль.



Устройство поставляется производителем с параметрами конфигурации, установленными в начальное состояние.

При этом имя пользователя и пароль не заданы и не запрашиваются системой.

После регистрации на устройстве в консоли появится системное приглашение интерфейса командной строки CLI .

```
console>
```



Для быстрого вызова справки о доступных командах используйте комбинацию клавиш «SHIFT» и «?».

4.3 Порядок конфигурирования

Прежде, чем приступить к конфигурированию, необходимо иметь следующую минимальную информацию:

- IP-адрес, который будет использоваться для доступа к управлению коммутатором;
- Маршрут по умолчанию;
- Значение маски подсети.

В первую очередь должно быть выполнено **начальное конфигурирование** коммутатора, в ходе которого должны быть подготовлены интерфейсы управления устройством и настроен необходимый уровень безопасности.

Следующим шагом конфигурирования может быть детальная **настройка системы безопасности**, включающая настройку процедур авторизации и аутентификации при управлении устройством.



После внесения любых изменений в конфигурацию устройства необходимо делать сохранение конфигурации в энергонезависимой памяти до перезагрузки устройства. Для сохранения конфигурации используйте команду:

```
console# copy running-config startup-config
```

4.3.1 Начальное конфигурирование

Начальное конфигурирование выполняется через консольный порт устройства. В результате выполнения начального конфигурирования могут быть настроены различные способы доступа к управлению - может быть изменен режим консольного порта или разрешен удаленный доступ через доступные интерфейсы и протоколы управления.

Приведенные далее примеры начального конфигурирования включают следующие настройки:

1. Создание учетной записи администратора с именем «admin», паролем «pass» и максимальным уровнем приоритета - 15.
2. Конфигурирование статического IP-адреса и адреса шлюза сети для управления коммутатором.

3. Настройка параметров управления по протоколу SNMP.
4. Настройка получения IP-адреса от сервера DHCP.
5. Настройка параметров протокола SNMP.



Параметры, необходимые для конфигурирования, могут быть получены у администратора сети.



При описании процедур конфигурирования предполагается, что коммутатор не был сконфигурирован ранее.

4.3.1.1 Создание учетной записи администратора



Для обеспечения защищенного входа в систему всем привилегированным пользователям должны быть назначены пароли доступа.

Имя пользователя и пароль вводится при входе в систему во время сеансов администрирования устройства. Для создания нового пользователя системы или настройки любого из параметров – имени пользователя, пароля, уровня привилегий, используются команды:

```
console(config)# username name password password privilege {1-15}
```



Уровень привилегий 1 разрешает доступ к устройству, но запрещает настройку. Уровень привилегий 15 разрешает как доступ, так и настройку устройства.

Пример команд для задания пользователю «admin» пароля «eltex» и создания пользователя «operator» с паролем «pass» и уровнем привилегий 1:

```
console> enable
console# configure
console(config)# username admin password eltex
console(config)# username operator password pass privilege 1
console (config) # exit
console#
```

4.3.1.2 Конфигурирование статических сетевых параметров управления.

Для возможности управления коммутатором из сети необходимо назначить устройству IP-адрес, маску подсети и, в случае управления из другой сети, адрес шлюза.

IP-адрес можно назначить любому интерфейсу – VLAN, физическому порту, группе портов. IP-адрес шлюза должен принадлежать к той же подсети, что и один из IP-интерфейсов устройства.



По умолчанию назначен IP-адрес 192.168.1.239, маска 255.255.255.0 на интерфейсе VLAN 1.



В случае если IP-адрес настраивается для интерфейса физического порта или группы портов, этот интерфейс удаляется из группы VLAN, которой он принадлежал.

- Пример команд настройки IP-адреса для интерфейса VLAN 1.

Параметры интерфейса:

IP-адрес, назначаемый для интерфейса VLAN 1 – 192.168.16.144

Маска подсети – 255.255.255.0

IP-адрес шлюза по умолчанию - 192.168.16.1

```
console# configure
console(config)# interface vlan 1
console (config-if) # ip address 192.168.16.144 /24
console (config-if) # exit
console (config) # ip default-gateway 192.168.16.1
console (config) # exit
console#
```

Для того чтобы убедиться, что адрес был назначен интерфейсу, введите команду:

```
console# show ip interface vlan 1
```

IP Address	Type	Directed Broadcast	Precedence	Status
192.168.25.67/24	Static	disable	No	Valid

4.3.1.3 Настройка параметров протокола SNMP для доступа к устройству

Протокол SNMP (Simple Network Management Protocol) предоставляет средства для управления сетевыми устройствами. Устройства, поддерживающие протокол SNMP, содержат в составе своего программного обеспечения код, выполняющий функцию агента управления. Агент SNMP взаимодействует с набором параметров устройства. Эти параметры описаны в Информационной базе управления (MIB, Management Information Base).

Права доступа к Агенту SNMP управляются путем задания имени SNMP сообщества и указанием разрешенного типа доступа.

Коммутаторы MES1024/MES1124/MES2124 допускают управление с помощью протокола SNMP, содержат встроенного агента SNMP и поддерживают версии протокола v1/v2c/v3. Агент SNMP поддерживает набор стандартных и расширенных переменных MIB.



В целях обеспечения интеграции коммутаторов в системы мониторинга и управления или для разработки таких систем может быть предоставлено полное описание MIB.

С помощью протокола SNMP могут быть изменены любые параметры устройства за исключением IP-адреса управления, имени SNMP сообщества и уровня привилегий пользователей.



Устройства поставляются без определенных настроек SNMP сообществ.

Для возможности администрирования устройства посредством протокола SNMP, необходимо создать хотя бы одну строку сообщества. Коммутаторы MES1024/MES1124/MES2124 поддерживают три типа сообществ:

- Read Only (ro) – определяет, что члены сообщества имеют доступ только на чтение (просмотр конфигурации), но не могут менять какие-либо параметры;
- Read/Write (rw) - определяет, что члены сообщества имеют доступ на чтение и изменение параметров конфигурации;
- Super (su) - определяет, что члены сообщества имеют уровень привилегий администратора.

Наиболее распространено использование строк сообщества *public* – с доступом только для чтения объектов MIB (ro) и *private* – с доступом на чтение и изменение объектов MIB (rw). Для каждого сообщества можно задать IP-адрес станции управления.

Пример создания сообщества *private* с доступом на чтение и запись и IP-адресом станции управления 192.168.16.44:

```
console> enable
console# configure
console(config)# snmp-server server
console(config)# snmp-server community private rw 192.168.16.44
console (config)# exit
console#
```

Для просмотра созданных строк сообщества и настроек SNMP используется команда:

```
console# show snmp

SNMP is enabled.

Community-String      Community-Access      View name      IP address
-----
private              read write           Default        192.168.16.44

Community-String      Group name            IP address      Type
-----
Traps are enabled.
Authentication-failure trap is enabled.

Version 1,2 notifications
Target Address      Type      Community      Version      Udp      Filter      To      Retries
Port              name              Sec
-----
Version 3 notifications
Target Address      Type      Username      Security      Udp      Filter      To      Retries
Level              Port              name              Sec
-----

System Contact:
System Location:
```

4.3.2 Настройка параметров системы безопасности

В этом разделе приведена информация о настройке динамического назначения IP-адреса и настройке защищенного управления устройством на основании механизмов аутентификации, авторизации и учета.

- *Authentication* (аутентификация) — сопоставление запроса существующей учётной записи в системе безопасности.
- *Authorization* (авторизация, проверка уровня доступа) — сопоставление учётной записи в системе (прошедшей аутентификацию) и определённых полномочий.
- *Accounting* (учёт) — слежение за потреблением ресурсов пользователем.

4.3.2.1 Получение IP-адреса от сервера DHCP

Для получения IP-адреса может использоваться протокол DHCP, для этого в сети должен присутствовать DHCP-сервер. Устройство выступает в роли DHCP-клиента. IP-адрес от сервера DHCP можно получать через любой интерфейс – VLAN, физический порт, группу портов.

Полученный с помощью протокола DHCP адрес не сохраняется в конфигурации устройства.

Пример настройки получения динамического IP-адреса от DHCP-сервера на интерфейсе VLAN 1:

```
console> enable
console# configure
console(config)# interface vlan 1
console(config-if)# ip address dhcp
console(config-if)# exit
console#
```

Для того чтобы убедиться, что адрес был назначен интерфейсу введите команду:

```
console# show ip interface vlan 1
```

IP Address	Type	Directed Broadcast	Precedence	Status
----- 192.168.25.67/24	DHCP	disable	No	Valid

4.3.2.2 Безопасность управления и конфигурирование паролей

Для обеспечения безопасности системы используется механизм аутентификации, авторизации и учета (AAA, Authentication, Authorization, Accounting), который управляет правами доступа пользователей, уровнями привилегий и методами управления. Механизм AAA может использовать либо локальную, либо удаленную базу пользователей.

Для обеспечения безопасности управления может использоваться шифрование данных управления с помощью протокола SSH.

Устройство поставляется с неназначенным паролем доступа. Назначение паролей доступа является ответственностью администратора.

В том случае, если пароль доступа к устройству утерян, может быть использована процедура восстановления пароля. Эта процедура однократно разрешает доступ к управлению устройством без пароля с локального терминала (консольного порта). Восстановление пароля может быть инициировано только через консольный порт.

Пароли доступа к устройству могут быть установлены для следующих интерфейсов доступа:

- Локальный терминал (подключение через консольный порт);
- Telnet;
- SSH;
- HTTP.



При создании пользователя назначается уровень привилегий 1, что дает возможность выборочного просмотра параметров устройства, но не дает возможности управлять устройством. Возможность конфигурирования имеют пользователи с уровнем привилегии 15.



Возможно, но не рекомендуется не назначать пароль пользователям с уровнем привилегии 15.



В том случае, если привилегированному пользователю не назначен пароль, такой пользователь может получить доступ к Web интерфейсу устройства с любым паролем.

Установка пароля для консоли

```
console(config)# aaa authentication login default line
console(config)# aaa authentication enable default line
console(config)# line console
console(config-line)# login authentication default
console(config-line)# enable authentication default
console(config-line)# password passwd1
```

В ответ на приглашение ввести пароль во время регистрации в устройстве через сеанс консоли введите пароль **-passwd1**.

Кроме того, ввод пароля может потребоваться при переходе в привилегированный режим с помощью команды **enable**.

Установка пароля для Telnet

```
console(config)# aaa authentication login default line
console(config)# aaa authentication enable default line
console(config)# ip telnet server
console(config)# line telnet
console(config-line)# login authentication default
console(config-line)# enable authentication default
console(config-line)# password passwd2
```

В ответ на приглашение ввести пароль во время регистрации в устройстве через сеанс Telnet введите пароль **-passwd2**.

Установка пароля для SSH

```
console(config)# aaa authentication login default line
console(config)# aaa authentication enable default line
console(config)# ip ssh server
console(config)# line ssh
console(config-line)# login authentication default
console(config-line)# enable authentication default
console(config-line)# password passwd3
```

В ответ на приглашение ввести пароль во время регистрации в устройстве через сеанс SSH введите пароль **-passwd3**.

Установка пароля для HTTP

Для конфигурирования пароля доступа по протоколу HTTP следует ввести команды:

```
console(config)# ip http authentication local  
console(config)# username admin password passwd4 level 15
```

При инициализации HTTP сессии следует использовать имя пользователя **admin** и пароль **passwd4**.

Восстановление пароля доступа к устройству.

При использовании настроек устройства по умолчанию имя пользователя – **admin**, пароль не задан. Пароль назначается пользователем.

В случае если пароль утрачен, можно перезагрузить устройство и через консольный порт прервать загрузку, нажав клавишу **<Esc>** или **<Enter>** в течение первых двух секунд после появления сообщения автозагрузки. Откроется меню **Startup**, в котором нужно запустить процедуру восстановления пароля ([3] Password Recovery Procedure).

5 УПРАВЛЕНИЕ УСТРОЙСТВОМ. ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ

Для конфигурирования настроек коммутатора используется четыре основных режима. В каждом режиме доступен определенный список команд. Ввод символа «?» служит для просмотра набора команд, доступных в каждом из режимов.

Для перехода из одного режима в другой используются специальные команды. Перечень существующих режимов и команд входа в режим:

Командный режим (EXEC), данный режим доступен сразу после успешной загрузки коммутатора и ввода имени пользователя. Приглашение системы в этом режиме состоит из имени устройства (host name) и символа “>”.

```
console>
```

Если имя устройства не назначено, то вместо него используется слово “console”.

Привилегированный командный режим (privileged EXEC), этот режим доступен при входе привилегированного пользователя. Вход в режим должен быть обязательно защищен паролем. Только в привилегированном режиме доступны команды изменения системных параметров коммутатора. В привилегированном режиме в строке приглашения системы используется символ «#». Для перехода из режима EXEC в привилегированный режим может быть использована команда enable.

```
console> enable
enter password:
console#
```

Режим глобального конфигурирования (global configuration), данный режим предназначен для задания общих настроек коммутатора. Команды режима глобальной конфигурации доступны из любого подрежима конфигурации. Вход в режим осуществляется командой **configure**.

```
console# configure
console(config)#
```

Режим конфигурирования интерфейса (interface configuration), данный режим предназначен для конфигурирования интерфейсов (порт, группа портов, интерфейс VLAN) коммутатора. Вход в режим осуществляется из режима глобального конфигурирования, для каждого интерфейса своей командой (в примере ниже команда для входа в режим конфигурирования интерфейса VLAN с VID=1).

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

Режим конфигурирования терминала (line configuration), данный режим предназначен для конфигурирования, связанного с работой терминала. Вход в режим осуществляется из режима глобального конфигурирования.

```
console(config)# line {console | telnet | ssh}
console(config-line)#
```

5.1 Правила работы с командной строкой



При перезагрузке устройства все несохраненные данные будут утеряны. Для сохранения любых внесенных изменений в настройку коммутатора используется следующая команда:

```
console# copy running-config startup-config
```



Для ускорения ввода команд можно воспользоваться функцией автоматического дополнения, которая активируется при неполно набранной команде и при нажатии клавиши <Tab>.

5.2 Базовые команды

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 5.1 – Базовые команды доступные в режиме EXEC

Команда	Значение/ значение по умолчанию	Действие
enable [priv]	priv: {1..15}/15	Переключиться в привилегированный режим (если значение не указано – то уровень привилегий 15).
login	-	Завершение текущей сессии и смена пользователя.
exit	-	Закрыть активную терминальную сессию.
help		Запрос справочной информации о работе интерфейса командной строки
show history	-	Показать историю команд, введенных в текущей терминальной сессии.
show privilege	-	Показать уровень привилегий текущего пользователя.
terminal history	-/ функция включена	Включить функцию сохранения истории введенных команд для текущей терминальной сессии.
no terminal history		Выключить функцию сохранения истории введенных команд для текущей терминальной сессии.
terminal history size {size}	Size: {10..216}/10	Изменить размер буфера истории введенных команд для текущей терминальной сессии.
no terminal history size		Установить значение по умолчанию.
terminal datadump	-/ вывод команд разделяется по страницам	Отобразить вывод команд без разделения на страницы (разделение вывода справки по страницам осуществляется строкой: More: <space>, Quit: q, One line: <return>)..
no terminal datadump		Установить значение по умолчанию.
show banner [motd login exec]	-	Отображает конфигурацию баннеров.

Команды режима privileged EXEC

Таблица 5.2 – Базовые команды, доступные в режиме privileged EXEC

Команда	Значение/ значение по умолчанию	Действие
disable [priv]	priv: {1..15}/1	Вернуться в нормальный режим из привилегированного (если значение не указано – то уровень привилегий 1).
configure[terminal]	-	Перейти в режим конфигурирования.

debug-mode	-	Перейти в режим отладки (команда доступна только для привилегированного пользователя).
-------------------	---	--

Команды, доступные во всех режимах конфигурирования

Запрос командной строки имеет один из следующих видов:

```
console#
console(config)#
console(config-line)#
...
```

Таблица 5.3 – Базовые команды, доступные во всех режимах конфигурирования

Команда	Значение	Действие
exit	-	Выйти из любого режима конфигурирования на уровень выше в иерархии команд CLI.
end	-	Выйти из любого режима конфигурирования в командный режим (Privileged EXEC).
do	-	Выполнить команду командного уровня (EXEC) из любого режима конфигурирования.
help	-	Выводит справку по используемым командам.

Команды, доступные в глобальном режиме конфигурирования

Запрос командной строки имеет следующий вид:

```
console#
console(config)#
```

Таблица 5.4 – Базовые команды доступные в режиме конфигурирования

Команда	Значение	Действие
banner motd d message-text d no banner motd	-	Задать текст сообщения motd (сообщения текущего дня), и включить вывод на экран. d - разделитель; message-text – текст сообщения (в строке до 510 символов, общее 2000 символов).
banner exec d message-text d no banner exec	-	Задать текст сообщения exec (пример: пользователь успешно вошел в систему), и включить вывод на экран. d - разделитель; message-text – текст сообщения (в строке до 510 символов, общее 2000 символов).
banner login d message-text d no banner login	-	Задать текст сообщения login (информационное сообщение, которое отображается перед вводом имени пользователя и пароля), и включить вывод на экран. d - разделитель; message-text – текст сообщения (в строке до 510 символов, общее 2000 символов).

Команды, доступные в режиме конфигурирования терминала

Запрос командной строки в режиме конфигурирования терминала имеет следующий вид:

```
console(config-line)#
```

Таблица 5.5 – Базовые команды доступные в режиме конфигурирования терминала

<i>Команда</i>	<i>Значение/ Значение по умолчанию</i>	<i>Действие</i>
history	-/ функция включена	Включить функцию сохранения истории введенных команд.
no history		Выключить функцию сохранения истории введенных команд.
history size {size}	{0..216}/10	Изменить размер буфера истории введенных команд.
no history sie		Установить значение по умолчанию.
motd-banner	-/включен	Включить вывод приветственных сообщений типа «motd» (сообщения текущего дня).
no motd-banner		Выключить вывод информационных сообщений типа «motd».
login-banner	-/ включен	Включить вывод приветственных сообщений login.
no login-banner		Выключить вывод приветственных сообщений login.
exec-banner	-/ включен	Включить вывод приветственных сообщений exec.
no exec-banner		Выключить вывод приветственных сообщений exec.

5.3 Настройка макрокоманд

Данная функция позволяет создавать унифицированные наборы команд - макросы, которые можно впоследствии применять в процессе конфигурации.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console (config) #
```

Таблица 5.6 – Команды режима глобального конфигурирования

<i>Команда</i>	<i>Значение/Значение по умолчанию</i>	<i>Действие</i>
macro name [word]	1..32 символов	Создает новый набор команд, если набор с таким именем существует – перезаписывает его. Набор команд вводится построчно. Закончить макрос можно с помощью символа “@”. Максимальная длина макроса – 510 символов.
no macro name word		Удаляет указанный макрос.
macro global apply word	1..32 символов	Применяет указанный макрос.
macro global trace word	1..32 символов	Проверяет указанный макрос на валидность.
macro global description word	1..160 символов	Создает строку-дескриптор глобального макроса.
no macro global description		Удаляет строку-дескриптор.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Таблица 5.7 – Команды режима EXEC

Команда	Действие	
macro apply word	1..32 символов	Применяет указанный макрос
macro trace word		Проверяет указанный макрос на валидность
show parser macro [description [interface {gigabitethernet gi_port fastethernet fa_port port-channel group}] name macro-name]	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}; macro-name: 1..32 символов	Отображает параметры настроенных макросов на устройстве.

Команды режима конфигурации интерфейса

Вид запроса командной строки режима конфигурации интерфейса:

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

Таблица 5.8 – Команды режима конфигурации интерфейса






Команда	Действие	
macro apply word	1..32 символов	Применяет указанный макрос.
macro trace word	1..32 символов	Проверяет указанный макрос на валидность.
macro description word	1..160 символов	Устанавливает строку-дескриптор макроса
no macro description		Удаляет строку-дескриптор

5.4 Команды управления системой

Команды режима EXEC

Таблица 5.9 – Команды управления системой в режиме EXEC

Команда	Значение/ Значение по умолчанию	Действие
ping [ip] {A.B.C.D host} [size size] [count count] [timeout timeout]	host {1..158} символов; size [64..1518]/64 Байт; count [0..65535]/4; timeout [50..65535] /2000 мс	Команда служит для передачи запросов (ICMP Echo-Request) протокола ICMP указанному узлу сети, а так же для контроля поступающих ответов (ICMP Echo-Reply). - A.B.C.D - IPv4-адрес узла сети; - host – доменное имя узла сети; - size – размер пакета для отправки, количество байт в пакете; - count – количество пакетов для передачи; - timeout – время ожидания ответа на запрос.
ping ipv6 {A.B.C.D.E.F host} [size size] [count count] [timeout timeout]	host {1..158} символов; size [64..1518]/68 Байт; count [0..65535]/4; timeout [50..65535] /2000 мс	Команда служит для передачи запросов (ICMP Echo-Request) протокола ICMP указанному узлу сети, а так же, для контроля поступающих ответов (ICMP Echo-Reply). - A.B.C.D.E.F - IPv6-адрес узла сети; - host – доменное имя узла сети; - size – размер пакета для отправки, количество байт в пакете; - count – количество пакетов для передачи; - timeout – время ожидания ответа на запрос.
traceroute ip {A.B.C.D host} [size size] [ttl ttl] [count count] [timeout timeout] [source ip-address] [tos tos]	host {1..158} символов; size [64..1518]/64 Байт; ttl [1..255]/30; count [1..10]/3; timeout [1..60] /3 с; tos [0..255]/0	Определение маршрута трафика до узла назначения. - A.B.C.D - IPv4-адрес узла сети. - host – доменное имя узла сети; - size – размер пакета для отправки, количество байт в пакете; - ttl – максимальное количество участков в маршруте; - count – количество попыток передачи пакета на каждом


		<p>участке;</p> <ul style="list-style-type: none"> - timeout – время ожидания ответа на запрос; - source – IP-адрес интерфейса коммутатора MES1024/MES1124/MES2124 используемый для передачи пакетов; - tos – тип сервиса, передаваемый в заголовке протокола IP. <p> Описание ошибок при выполнении команд и результатов приведено в таблицах 5.11, 5.12</p>
<p>traceroute ipv6 {A.B.C.D.E.F/host} [size size] [ttl ttl] [count count] [timeout timeout] [source ip-address] [tos tos]</p>	<p>host {1..158} символов; size [66..1518]/66 Байт; ttl [1..255]/30; count [1..10]/3; timeout [1..60] /3 с; tos [0..255]/0</p>	<p>Определение маршрута трафика до узла назначения. - A.B.C.D.E.F - IPv6-адрес узла сети.</p> <ul style="list-style-type: none"> - host – доменное имя узла сети; - size – размер пакета для отправки, количество байт в пакете; - ttl – максимальное количество участков в маршруте; - count – количество попыток передачи пакета на каждом участке; - timeout – время ожидания ответа на запрос; - source – IP-адрес интерфейса коммутатора MES2124, используемый для передачи пакетов; - tos – тип сервиса, передаваемый в заголовке протокола IP. <p> Описание ошибок при выполнении команд и результатов приведено в таблицах 5.11, 5.12</p>
<p>telnet {A.B.C.D host} [port] [keyword1...]</p>	<p>host {1..158} символов; port [1..65535]/23</p>	<p>Открытие TELNET-сессии для узла сети.</p> <ul style="list-style-type: none"> - A.B.C.D - IPv4-адрес узла сети; - host – доменное имя узла сети; - port – TCP-порт, по которому работает служба Telnet; - keyword – ключевое слово. <p> Описание специальных команд Telnet и ключевых слов приведено в таблицах 5.13 , 5.14</p>
<p>resume [connection]</p>	<p>[1..4]/последняя установленная сессия</p>	<p>Переключение на другую установленную TELNET-сессию.</p> <ul style="list-style-type: none"> - connection – номер установленной telnet-сессии.
<p>show switch [number]</p>	<p>number: {1 .. 4}</p>	<p>Отображает информацию о состоянии стека. Number – номер стека.</p>
<p>show cpu counters</p>	-	<p>Просмотр счетчиков пакетов центрального процессора.</p>
<p>show users</p>	-	<p>Отображение информации о пользователях, использующих ресурсы устройства.</p>
<p>show sessions</p>	-	<p>Отображение информации об открытых TELNET-сессиях к удаленным устройствам.</p>
<p>show system [unit unit]</p>	<p>[1..4]/-</p>	<p>Отображение системной информации коммутатора.</p> <ul style="list-style-type: none"> - unit – номер устройства в стеке (для коммутатора, работающего в автономном режиме, параметр не используется). <p> Параметр [unit unit] при выполнении команды доступен только в режиме стекирования.</p>
<p>show version</p>	-	<p>Отображение текущей версии системного программного обеспечения, работающего на устройстве.</p>
<p>show system tcam utilization [unit unit]</p>	<p>[1..4]/-</p>	<p>Отображение загрузки ресурсов памяти TCAM (трехмерная адресуемая память).</p> <ul style="list-style-type: none"> - unit – номер устройства в стеке (для коммутатора, работающего в автономном режиме, параметр не используется). <p> Параметр [unit unit] при выполнении команды доступен только в режиме стекирования.</p>

Команды режима privileged EXEC

Запрос командной строки в режиме privileged EXEC имеет следующий вид:

```
console#
```

Таблица 5.10 – Команды управления системой в режиме privileged EXEC

Команда	Значение/ Значение по умолчанию	Действие
reload [slot stack--number]	stack-number: {1..4}	Команда служит для перезапуска устройства. stack-number – номер устройства в стеке.
show cpu utilization	-	Отображение статистики по уровню загрузки ресурсов центрального процессора.
show cpu input-rate	-	Отображение статистики по скорости входящих фреймов обрабатываемых процессором
show cpu input-rate detailed	-	Отображение статистики по скорости входящих фреймов обрабатываемых процессором по типу трафика
show cpu rate-limits	-	Отображение ограничений по скорости для входящих фреймов обрабатываемых процессором
show tasks utilization	-	Отображение статистики по уровню загрузки ресурсов центрального процессора для каждого процесса
clear cpu counters	-	Обнуление счетчиков пакетов центрального процессора.
show system id [unit unit]	[1..4]/-	Отображение информации системной идентификации устройства. - unit – номер устройства в стеке (для коммутатора, работающего в автономном режиме, параметр не используется).  Параметр [unit unit] при выполнении команды доступен только в режиме стекирования.
show system defaults [{management ipv6 802.1x port fdb multicast port-mirroring spanning-tree vlan voice-vlan network-security dos-attacks ip-addressing qos-acl }]	-	Отображение заводских настроек устройства
show system tcam utilization	-	Отображает использование TCAM (Ternary Content Addressable Memory)

- Пример использования команды **traceroute**:

```
console# traceroute eltex.com
```

```
Type Esc to abort.
Tracing the route to eltex.com (148.21.11.69)
 1 gateway.eltex (192.168.1.101)  0 msec 0 msec 0 msec
 2 eltexsrv (192.168.0.1) 0 msec 0 msec 0 msec
 3 * * *
```

Таблица 5.11 – Описание результатов выполнения команды **traceroute**

Поле	Описание
1	Порядковый номер маршрутизатора в пути к указанному узлу сети.
gateway.eltex	Сетевое имя этого маршрутизатора.
192.168.1.101	IP-адрес этого маршрутизатора.
0 msec 0 msec 0 msec	Время, за которое пакет был передан и вернулся от маршрутизатора. Указывается для каждой попытки передачи пакета.

При выполнении команды **traceroute** могут произойти ошибки, описание ошибок приведено в таблице

Таблица 5.12 – Ошибки при выполнении команды traceroute

Символ ошибки	Описание
*	Таймаут при попытке передачи пакета.
?	Неизвестный тип пакета.
A	Административно недоступен. Обычно происходит при блокировании исходящего трафика по правилам в таблице доступа ACL.
F	Требуется фрагментация и установка битов DF.
H	Узел сети недоступен.
N	Сеть недоступна.
P	Протокол недоступен.
Q	Источник подавлен.
R	Истекло время повторной сборки фрагмента.
S	Ошибка исходящего маршрута.
U	Порт недоступен.

Программное обеспечение Telnet коммутатора MES1024/MES1124/MES2124 поддерживает специальные команды – функции контроля терминала. Для входа в режим специальных команд во время активной Telnet-сессии используется комбинация клавиш Ctrl-shift-6.

Таблица 5.13 – Специальные команды Telnet

Специальная команда	Назначение
^^ b	Передать по telnet разрыв соединения.
^^ c	Передать по telnet прерывание процесса (IP).
^^ h	Передать по telnet удаление символа (EC).
^^ o	Передать по telnet прекращение вывода (AO).
^^ t	Передать по telnet сообщение «Are You There?» (AYT) для контроля подключения.
^^ u	Передать по telnet стирание строки (EL).
^^ x	Возврат в режим командной строки.

Также возможно использование дополнительных опций при открытии Telnet-сессии:

Таблица 5.14 – Ключевые слова, используемые при открытии Telnet-сессии

Опция	Описание
/echo	Локально включает функцию <i>echo</i> (подавление вывода на консоль).
/quiet	Не допускает вывод всех сообщений программного обеспечения Telnet.
/source-interface	Определяет интерфейс-источник.
/stream	Включает обработку потока, который разрешает незащищенное TCP-соединение без контроля последовательностей Telnet. Поточное соединение не обрабатывает Telnet-опции и может использоваться для подключения к портам, на которых запущены программы копирования UNIX-to-UNIX (UUCP) либо другие протоколы, не являющиеся Telnet-протоколами.

Команды доступные в режиме глобального конфигурирования:

Запрос командной строки в режиме глобального конфигурирования имеет следующий вид:

```
console (config) #
```

Таблица 5.15 – Команды управления системой в режиме глобального конфигурирования

<i>Команда</i>	<i>Значение/ Значение по умолчанию</i>	<i>Действие</i>
hostname <i>name</i>	1..160 символов/-	Команда служит для задания сетевого имени устройства.
no hostname		Вернуть сетевое имя устройства в значение по умолчанию.
service cpu-utilization	-/enabled	Разрешить устройству программно измерять уровень загрузки ресурсов центрального процессора коммутатора.
no service cpu-utilization		Запретить устройству программно измерять уровень загрузки ресурсов центрального процессора коммутатора.
service cpu-input-rate	-/disabled	Разрешить устройству программно измерять скорость входящих фреймов обрабатываемых центральным процессором коммутатора.
no service cpu-input-rate		Запретить устройству программно измерять скорость входящих фреймов обрабатываемых центральным процессором коммутатора.
service cpu-rate-limits <i>traffic limit pps</i>	traffic: http, telnet, shh, snmp, ip, link-local, arp-switch-mode, arp-inspection, stp-bpdu, other-bpdu, dhcp-snooping, web-auth, igmp-snooping, mld-snooping, sflow, log-denya-ces, ptp, other pps: 8..1024	Установка ограничений скорости входящих фреймов для определенного типа трафика. - Pps - пакетов в секунду.
service tasks-utilization	-/disabled	Разрешить устройству программно измерять уровень загрузки ресурсов центрального процессора коммутатора для каждого системного процесса
no service tasks-utilization		Запретить устройству программно измерять уровень загрузки ресурсов центрального процессора коммутатора для каждого системного процесса

5.5 Команды для настройки параметров для задания паролей

Данный комплекс команд предназначен для того задания минимальной сложности пароля, а также для задания времени действия пароля.

Команды доступные в режиме глобального конфигурирования:

Запрос командной строки в режиме глобального конфигурирования имеет следующий вид:

```
console (config) #
```

Таблица 5.16 – Команды управления системой в режиме глобального конфигурирования

<i>Команда</i>	<i>Значение/ Значение по умолчанию</i>	<i>Действие</i>
passwords aging <i>age</i>	age: {0 .. 365}/0 дней	Задаёт время жизни паролей. По истечению заданного срока будет предложено сменить пароль. Значение 0 говорит о том, что время жизни паролей не задано
no password aging		Восстанавливает значение по умолчанию
passwords complexity enable	-/disabled	Включает ограничение на формат пароля
passwords complexity min-classes <i>value</i>	Value: {0..4}/3	Включает ограничение, задающее минимальное количество классов символов (строчные буквы, заглавные буквы, цифры, символы)

no passwords complexity min-classes		Восстанавливает значение по умолчанию
passwords complexity min-length <i>value</i>	Value: {0..64}/8	Включает ограничение на минимальную длину пароля.
no passwords complexity min-length		Восстанавливает значение по умолчанию
passwords complexity no-repeat <i>number</i>	Number: {0 ..16}/3	Включает ограничение, задающее максимальное количество последовательно повторяющихся символов в новом пароле.
no password complexity no-repeat		Восстанавливает значение по умолчанию
passwords complexity not-current	-/enabled	Запрещает при смене пароля использовать в качестве нового старый
no passwords complexity not-current		Разрешает использовать старый пароль при смене
passwords complexity not-username	-/enabled	Запрещает использовать в качестве пароля имя пользователя
no passwords complexity not-username		Разрешает использовать в качестве пароля имя пользователя

Таблица 5.17 – Команды управления системой в режиме Privileged EXEC

<i>Команда</i>	<i>Действие</i>
show passwords configuration	Отображает информацию об ограничениях на пароли

5.6 Работа с файлами

5.6.1 Описание аргументов команд

При осуществлении операций над файлами, в качестве аргументов команд выступают адреса URL – определители местонахождения ресурса. Описание ключевых слов, используемых в операциях, приведено в таблице 5.12.

Таблица 5.18 – Список ключевых слов и их описание

<i>Ключевое слово</i>	<i>Описание</i>
flash://	Исходный адрес или адрес места назначения для энергонезависимой памяти. Энергонезависимая память используется по умолчанию, если адрес URL определен без префикса (префиксами являются: flash:, tftp:, scp:...).
running-config	Файл текущей конфигурации.
startup-config	Файл первоначальной конфигурации.
image	Если исходный файл – данный образ активный. Если удаленный файл – данный образ не активный.
boot	Загрузочный файл.
tftp://	Исходный адрес или адрес места назначения для TFTP-сервера. Синтаксис: tftp://host/[directory] /filename. host – может быть IPv4-адресом, IPv6-адресом или сетевым именем устройства, directory – каталог, папка, filename – имя файла.
xmodem:	Исходный адрес файла при использовании протокола X-modem по последовательному соединению.
unit://member/ startup-config	Конфигурационный файл, используемый при запуске устройства. <i>member</i> – может быть IP-адресом или сетевым именем устройства в стеке.

unit://member/ image	Файл системного ПО на устройстве или на одном из устройств стека. Для копирования с ведущего устройства на все остальные модули можно в элементе <i>member</i> использовать «*». <i>member</i> – может быть IP-адресом или сетевым именем устройства в стеке.
unit://member/ boot	Загрузочный файл на устройстве или на одном из устройств стека. Для копирования с ведущего устройства на все остальные модули можно в элементе <i>member</i> использовать «*». <i>member</i> – может быть IP-адресом или сетевым именем устройства в стеке.
null:	Пустое место назначения для копий или файлов. Можно копировать удаленный файл к пустому указателю, чтобы определить его размер.
logging	Файл с историей команд.
unit://member/ backup-config	Резервный файл конфигурации на устройстве или на одном из устройств стека. <i>member</i> – может быть IP-адресом или сетевым именем устройства в стеке.

5.6.2 Команды для работы с файлами

Команды для работы с файлами доступны только привилегированному пользователю.

Запрос командной строки в режиме Privileged EXEC имеет следующий вид:

```
console#
```

Таблица 5.19 – Команды для работы с файлами в режиме Privileged EXEC

Команда	Значение	Действие
copy source-url destination-url [snmp]		Копирование файла из местоположения источника в местоположение назначения. - snmp – используется только когда копирование осуществляется из/в startup-config. Специфицирует использование исходного адреса или адреса места назначения в формате SNMP; - source-url – местоположение копируемого файла; - destination-url – адрес места назначения, куда файл будет скопирован.
copy source-url image	source-url: 1..160 символов;	Копирование файла системного ПО с сервера в энергонезависимую память.
copy source-url boot	destination-url: 1..160 символов;	Копирование загрузочного файла с сервера в энергонезависимую память.
copy source-url running-config		Копирование файла конфигурации с сервера в текущую конфигурацию.
copy source-url startup-config		Копирование файла конфигурации с сервера в первоначальную конфигурацию.
copy running-config destination-url		Сохранение текущей конфигурации на сервере.
copy startup-config destination-url		Сохранение первоначальной конфигурации на сервере.
copy running-config startup-config	-	Сохранение текущей конфигурации в первоначальную конфигурацию.
copy running-config file	-	Сохранение текущей конфигурации в заданный резервный файл конфигурации.
copy startup-config file	-	Сохранение первоначальной конфигурации в заданный резервный файл конфигурации.
copy running-config backup-config	-	Сохранение текущей конфигурации в резервный файл конфигурации.
copy startup-config backup-config	-	Сохранение первоначальной конфигурации в резервный файл конфигурации.
dir	-	Отображает список файлов во флэш-памяти

more {flash://<file> startup-config running-config mirror-config <file>}	<file> - 1..160 символов	<p>Отображает содержимое файла.</p> <ul style="list-style-type: none"> - startup-config – отображает содержимое файла первоначальной конфигурации; - running-config – отображает содержимое файла текущей конфигурации; - flash:// – отображает файлы с USB flash-накопителей; - mirror-config – отображает содержимое файла текущей конфигурации с зеркала; - file – имя файла. <p>! Файлы отображаются в формате ASCII, за исключением image, которые отображаются в шестнадцатеричном формате. *.prv файлы не отображаются.</p>
delete url	-	Удаление файла с флэш-памяти устройства. Файлы *.prv, image-1 и image-2 не могут быть удалены.
delete startup-config	-	Удаления файла первоначальной конфигурации.
boot system [unit unit] {image-1 image-2}	unit [1..4]	<p>Определяет файл системного ПО, который будет загружен при запуске.</p> <ul style="list-style-type: none"> - unit – номер устройства в стеке (для коммутатора, работающего в автономном режиме, параметр не используется).
show running-config	-	Отображает содержимое файла текущей конфигурации.
show startup-config	-	Отображает содержимое файла первоначальной конфигурации.
show bootvar [unit unit]	unit [1..4]	<p>Показывает активный файл системного ПО, который устройство загружает при запуске.</p> <ul style="list-style-type: none"> - unit – номер устройства в стеке (для коммутатора, работающего в автономном режиме, параметр не используется). <p>! Параметр [unit unit] при выполнении команды доступен только в режиме стекирования</p>
write [memory terminal]		Сохранение текущей конфигурации в файл первоначальной конфигурации.
rename url new-url	url: {1 .. 160}	Изменение имени файла. url – текущее имя файла; new-url – новое имя файла.



Существуют некоторые недопустимые комбинации местоположения и места назначения. Нельзя копировать в следующих случаях:

- если исходный файл и файл назначения – один и тот же файл;
- xmodem не может быть адресом назначения. По X-modem с адреса источника файл может быть скопирован только в файл системного ПО, в загрузочный файл или в pull;
- сервер TFTP не может быть адресом источником и адресом назначения для одной команды копирования;
- *.prv файлы не могут быть скопированы;
- копирование к/от устройств стека, работающих в ведомом режиме, возможно только для файла системного ПО и загрузочного файла.

Таблица 5.20 - Описание признаков копирования

Признак	Описание
!	Восклицательный знак означает, что процесс копирования идет успешно. Каждый восклицательный знак указывает на успешную передачу десяти пакетов (512 байтов каждый).

	Точка означает, что процесс копирования прерван. Несколько точек подряд означает, что в процессе копирования возникла ошибка.
--	---

Примеры использования команд.

Удалить файл *test* из энергонезависимой памяти:

```
console# delete flash: test
Delete flash:test? [confirm]
```

Результат выполнения команды: после подтверждения файл будет удален.

5.6.3 Команды для резервирования конфигурации

В данном разделе описаны команды настройки резервирования конфигурации по таймеру или при сохранении текущей конфигурации на flash-накопитель.

Команды доступные в режиме глобального конфигурирования:

Запрос командной строки в режиме глобального конфигурирования имеет следующий вид:

```
console(config) #
```

Таблица 5.21 – Команды управления системой в режиме глобального конфигурирования

<i>Команда</i>	<i>Значение/ Значение по умолчанию</i>	<i>Действие</i>
backup server <i>server</i>	server: 1..22 символов	Указание tftp-сервера, на который будет производиться резервирование конфигурации. Строка в формате «tftp://XXX.XXX.XXX.XXX».
no backup server		Удаление сервера для резервирования.
backup path <i>path</i>	path: 1..128 символов	Указание пути расположения файла на сервере и префикса файла. При сохранении к префиксу будет добавляться текущая дата и время в формате ггггммддччммсс.
no backup path		Удаление пути для резервирования.
backup time-period <i>timer</i>	timer: 1..35791394 мин/720 мин	Указание промежутка времени, по истечении которого будет осуществляться автоматическое резервирование конфигурации.
no backup time-period		Восстанавливает значение по умолчанию
backup auto	/disabled	Включение автоматического резервирования конфигурации.
no backup auto		Установка значения по умолчанию.
backup write-memory	/disabled	Включение резервирования конфигурации при сохранении пользователем конфигурации на flash.
no backup write-memory		Установка значения по умолчанию.

Таблица 5.22 – Команды управления системой в режиме Privileged EXEC

<i>Команда</i>	<i>Действие</i>
show backup	Отображает информацию о настройках резервирования конфигурации

5.6.4 Команды для автоматического обновления и конфигурирования

Процесс автоматического обновления

Коммутатор запускает процесс автоматического обновления базирующийся на DHCP (до процесса автоматической конфигурации), если он включен и имя текстового файла (DHCP-опция 125), содержащего имя образа ПО, было предоставлено сервером DHCP.

Процесс автоматического обновления состоит из следующих шагов:

1. Коммутатор загружает текстовый файл и читает из него имя файла образа ПО на TFTP-сервере;
2. Коммутатор скачивает первый блок (512 байт) образа ПО с TFTP-сервера, в котором содержится версия ПО;
3. Коммутатор сравнивает версию файла образа ПО, полученного с TFTP-сервера, с версией активного образа ПО коммутатора. Если они отличаются, коммутатор загружает образ ПО с TFTP-сервера вместо неактивного образа ПО коммутатора и делает данный образ активным;
4. Если образ ПО был загружен, то коммутатор перезагружается.

Процесс автоматического конфигурирования

Коммутатор запускает процесс автоматического конфигурирования, базирующийся на DHCP. Если он включен и IP-адреса TFTP-сервера (DHCP-опция 66) с именем файла конфигурации (DHCP-опция 67) были предоставлены DHCP-сервером. Полученный файл конфигурации добавляется к текущей (running) конфигурации. Если пользователь включил автоматическое сохранение (команда `boot host auto-save`), то текущая (running) конфигурация будет скопирована в первоначальную конфигурацию (startup). Коммутатор делает попытку загрузить конфигурацию, если выполняется одно из условий:

1. Коммутатор имеет конфигурацию по умолчанию;
2. До перезагрузки коммутатора пользователем была введена команда `boot host dhcp`, которая форсирует получение конфигурации при загрузке.

Команды доступные в режиме глобального конфигурирования:

Запрос командной строки в режиме глобального конфигурирования имеет следующий вид:

```
console(config)#
```

Таблица 5.23 – Команды управления системой в режиме глобального конфигурирования

Команда	Значение/ Значение по умолчанию	Действие
<code>boot host auto-config</code>	-/включено	Включение автоматического конфигурирования базирующегося на DHCP.
<code>no boot host auto-config</code>		Установка значения по умолчанию.
<code>boot host auto-save</code>	-/выключено	Включение автоматического сохранения текущей конфигурации в первоначальную после получения ее по TFTP.
<code>no boot host auto-save</code>		Установка значения по умолчанию.
<code>boot host auto-update</code>	-/включено	Включение автоматического конфигурирования базирующегося на DHCP.
<code>no boot host auto-update</code>		Установка значения по умолчанию.
<code>boot host dhcp</code>	-/выключено	Включение принудительной загрузки конфигурации при

		следующем включении коммутатора.
<code>no boot host dhcp</code>		Установка значения по умолчанию.

Команды режима *privileged EXEC*

Запрос командной строки в режиме *privileged EXEC* имеет следующий вид:

```
console#
```

Таблица 5.24 – Команды управления системой в режиме *privileged EXEC*

<i>Команда</i>	<i>Значение/ Значение по умолчанию</i>	<i>Действие</i>
<code>show boot</code>	-	Просмотр настроек автоматического обновления и конфигурирования.

- Пример конфигурации ISC DHCP Server:

```
option image-filename code 125 = {
unsigned integer 32, #enterprise-number. Идентификатор производителя, всегда равен
35265 (Eltex)
unsigned integer 8, #data-len. Длина всех данных опции. Равна длине строки sub-
option-data + 2.
unsigned integer 8, #sub-option-code. Код подопции, всегда равен 1
unsigned integer 8, #sub-option-len. Длина строки sub-option-data
text #sub-option-data. Имя текстового файла, содержащего имя
образа ПО
};

host mes2124-test {
hardware ethernet a8:f9:4b:85:a2:00; #mac-адрес коммутатора
filename "mes2124-test.cfg"; #имя конфигурации коммутатора
option image-filename 35265 15 1 13 "mes2000-image"; #имя текстового
файла, содержащего имя образа ПО
next-server 192.168.1.3; #IP-адрес TFTP сервера
fixed-address 192.168.1.36; #IP-адрес коммутатора
}
```

5.7 Настройка системного времени



Автоматический переход на летнее время осуществляется в соответствии со стандартами США и Европы, также возможно переключение на летнее время для указанного периода.

Команды режима *Privileged EXEC*

Запрос командной строки в режиме *Privileged EXEC* имеет следующий вид:

```
console#
```

Таблица 5.25 - Команды настройки системного времени в режиме Privileged EXEC

<i>Команда</i>	<i>Значение</i>	<i>Действие</i>
clock set hh:mm:ss day month year	hh 0..23, mm 0..59, ss 0..59, day 1..31; month Jan..Dec; year 2000 – 2037	Ручная установка системного времени (команда доступна только для привилегированного пользователя). - hh – часы, mm – минуты, ss – секунды; - day – день; - month – месяц; - year – год.
clock set hh:mm:ss month day year		
show sntp configuration	-	Показывает конфигурацию протокола SNTP.
show sntp status	-	Показывает статус протокола SNTP.

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 5.26 - Команды настройки системного времени в режиме «EXEC»

<i>Команда</i>	<i>Значение</i>	<i>Действие</i>
show clock		Показывает системное время и дату.
show clock detail	-	Дополнительно отображает параметры часового пояса и перехода на летнее время.

Команды доступные в режиме глобального конфигурирования

Запрос командной строки в режиме глобального конфигурирования имеет следующий вид:

```
console(config)#
```

Таблица 5.27 – Список команд для настройки системного времени в режиме глобального конфигурирования

<i>Команда</i>	<i>Значение/Значение по умолчанию</i>	<i>Действие</i>
clock source {sntp}		Использование внешнего источника для установки системного времени.
no clock source	-/внешний источник не используется	Запрещает использование внешнего источника для установки системного времени.
clock timezone zone hours-offset [minutes minutes-offset]	zone описание до 4 символов/ нет описания зоны hours-offset -12..+13/0; minutes-offset [0..59]/0;	Устанавливает значение часового пояса. - zone – слово, сформированное из первых букв словосочетания, которое оно заменяет (описание зоны); - hours-offset – часовое смещение относительно нулевого меридиана UTC; - minutes-offset – минутное смещение относительно нулевого меридиана UTC.
no clock timezone		Устанавливает значение по умолчанию.
clock summer-time zone date date month year hh:mm [offset]	zone [1..4] символа/ нет описания зоны week 1..4, first, last; day mon..sun; date 1..31; month Jan..Dec; year 2000 – 2097; hh 0..23, mm 0..59; offset [1..1440]/60 мин;	Задает дату и время для автоматического перехода на летнее время и возврата обратно (для определенного года). Первым в команде указывается описание зоны, вторым время для перехода на летнее время и третьим время для возврата. - zone – слово, сформированное из первых букв словосочетания, которое оно заменяет (описание зоны); - date – число; - month – месяц; - year – год;
clock summer-time zone date month date year hh:mm [offset]		

	По умолчанию переход на летнее время выключен	- hh – часы, mm – минуты; - offset – количество минут, добавляемых при переходе на летнее время.
clock summer-time <i>zone recurring {usa eu {week day month hh:mm week day month hh:mm}} [offset]</i>		Задаёт дату и время для автоматического перехода на летнее время и возврата обратно в режиме ежегодно. - zone – слово, сформированное из первых букв словосочетания, которое оно заменяет (описание зоны); - usa – установить правила перехода на летнее время, используемые в США (переход во второе воскресенье марта, обратно в первое воскресенье ноября, в 2 часа утра по местному времени); - eu – установить правила перехода на летнее время, используемые Евросоюзом (переход в последнее воскресенье марта, обратно в последнее воскресенье октября, в 1 час утра по Гринвичу); - hh – часы, mm – минуты; - week – неделя месяца (может принимать значения: 1-4, первая, последняя); - day – день недели; - month – месяц; - offset – количество добавляемых минут при переходе на летнее время.
no clock summer-time		Отключает автоматический переход на летнее время.
sntp authentication-key <i>number md5 value</i>	number 1..4294967295; value 1..8 символов;	Устанавливает ключ проверки подлинности для протокола SNMP. - number – номер ключа; - value – значение ключа.
no sntp authentication-key <i>number</i>	По умолчанию проверка подлинности отключена	Удаляет ключ проверки подлинности для протокола SNMP.
sntp authenticate	-/проверка подлинности не требуется	Требует проверку подлинности для получения информации от NTP-серверов.
no sntp authenticate		Устанавливает значение по умолчанию.
sntp trusted-key <i>key-number</i>	key-number 1..4294967295;	Осуществляет проверку подлинности системы, от которой синхронизируется с помощью SNMP по заданному ключу. - key-number – номер ключа.
no sntp trusted-key <i>key-number</i>	По умолчанию проверка подлинности отключена	Устанавливает значение по умолчанию.
sntp client poll timer <i>seconds</i>	seconds 60 .. 86400/1024	Устанавливает время опроса для SNMP-клиента.
no sntp client poll timer		Устанавливает значение по умолчанию.
sntp broadcast client enable		Разрешает работу широковещательных SNMP-клиентов.
no sntp broadcast client enable	-/запрещено	Устанавливает значение по умолчанию.
sntp anycast client enable		Разрешает работу SNMP-клиентам, поддерживающим метод рассылки пакетов, позволяющий посылать данные ближайшему устройству из группы получателей
no sntp anycast client enable	-/запрещено	Устанавливает значение по умолчанию.
sntp client enable <i>{ gigabitethernet gi_port fastethernet fa_port port-channel group vlan vlanID}</i>	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}; vlanID {1..4094}	Разрешает работу SNMP-клиентам, поддерживающим метод рассылки пакетов, позволяющий посылать данные ближайшему устройству из группы получателей, а также широковещательным SNMP-клиентам для выбранного интерфейса. - подробное описание интерфейсов изложено в разделе «Конфигурирование интерфейсов».
no sntp client enable <i>{ gigabitethernet gi_port fastethernet fa_port port-channel group vlan vlanID}</i>	/запрещено	Устанавливает значение по умолчанию.
sntp unicast client enable		Разрешает работу одноадресных SNMP-клиентов.
no sntp unicast client enable	-/запрещено	Устанавливает значение по умолчанию.
sntp unicast client poll	-/запрещено	Разрешает последовательный опрос заданных одноадресных SNMP-серверов.

no snntp unicast client poll		Устанавливает значение по умолчанию.
snntp server {ipv4-address ipv6-address { ipv6-link-local-address } % {vlan {integer} ch {integer} isatap {integer} {physical- port-name}} hostname} [poll] [key keyid]	hostname 1..158 символов; keyid 1..4294967295	Задаёт адрес SNTP-сервера. - ipv4-address - IPv4-адрес узла сети; - ipv6-address - IPv6-адрес узла сети; - ipv6z-address - IPv6z-адрес узла сети для ping. Формат адреса {ipv6-link-local-address}%{interface-name}; ipv6-link-local-address – локальный IPv6 адрес канала; interface-name – имя исходящего интерфейса задается в следующем формате: vlan {integer} ch {integer} isatap {integer} {physical- port-name} - hostname – доменное имя узла сети; - poll – включает опрос; - keyid – идентификатор ключа.
no snntp server {ipv4-address ipv6-address { ipv6-link-local-address}% {vlan {integer} ch {integer} isatap {integer} {physical- port-name}} hostname}		Удаление сервера из списка NTP-серверов.
snntp port port-number port-number	port-number 1..65535/ 123	Определяет UDP-порт SNTP сервера.
no snntp port		Устанавливает значение по умолчанию.
clock dhcp timezone	-/запрещено	Разрешает получение таких данных как часовой пояс и летнее время от DHCP-сервера.
no clock dhcp timezone		Запрещает получения таких данных как часовой пояс и летнее время от DHCP-сервера.

Команды режима конфигурирования интерфейса

Запрос командной строки в режиме конфигурирования интерфейса имеет следующий вид:

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

Таблица 5.28 – Список команд для настройки системного времени в режиме конфигурирования интерфейса

Команда	Значение/Значение по умолчанию	Действие
snntp client enable	-/запрещено	Разрешает работу SNTP-клиенту, который поддерживает метод рассылки пакетов, позволяющий посылать данные устройству ближайшему из группы получателей, а также широковещательному SNTP-клиенту на настраиваемом интерфейсе (ethernet, port-channel, VLAN).
no snntp client enable		Устанавливает значение по умолчанию.

Примеры выполнения команд

- Отобразить системное время, дату и данные по часовой зоне:

```
console# show clock detail
15:29:08 PDT(UTC-7) Jun 17 2009
Time source is SNTP

Time zone:
Acronym is PST
Offset is UTC-8

Summertime:
Acronym is PDT
```

Recurring every year.
Begins at first Sunday of April at 2:00.

- Задать дату и время на системных часах: 7 марта 2009 года, 13:32

```
console# clock set 13:32:00 7 Mar 2009
```

- Отобразить статус протокола SNTP:

```
console# show sntp status
```

```
Clock is synchronized, stratum 0, reference is 192.168.16.1, unicast
Reference time is cec866d5.8a20cccb 05:47:01.0 UTC Dec 8 2009
```

```
Unicast servers:
```

Server	Status	Last Response	Offset [mSec]	Delay [mSec]
192.168.16.1	up	05:47:01.0 UTC Dec 8 2009	7230	-1000

```
Anycast server:
```

Server	Interface	Status	Last Response	Offset [mSec]	Delay [mSec]

```
Broadcast:
```

Interface	IP address	Last Response

В примере выше системное время синхронизировано от сервера 192.168.16.1, последний ответ получен в 05:47:01, несовпадение системного времени с временем на сервере составило 7.23 с.

5.8 Конфигурирование интерфейсов



В зависимости от того в каком режиме работает коммутатор – автономно или в составе стека, изменяется вид записи для интерфейса Ethernet. При автономной работе запись для интерфейса имеет вид: 1/0/N, где N – номер интерфейса; при работе в составе стека запись для интерфейса имеет вид: K/0/N, где K – номер устройства в стеке, N – номер интерфейса. Выбор режима работы коммутатора описан в пункте 4 Меню Startup.



Значение маски может быть записано либо в формате X.X.X.X, либо в формате /N, где N – количество единиц в двоичном представлении маски.

5.8.1 Параметры Ethernet-интерфейсов и интерфейсов Port-Channel

Команды режима конфигурирования интерфейса (диапазона интерфейсов)

```
console# configure
console(config)# interface { gigabitethernet gi_port | fastethernet
fa_port|port-channel group|range {...}}
console(config-if)#
```

Данный режим доступен из режима конфигурирования и предназначен для задания параметров конфигурации интерфейса (порта коммутатора или группы портов, работающих в режиме разделения нагрузки), либо диапазона интерфейсов.

Выбор интерфейса осуществляется при помощи команд:

для MES1024

interface fastethernet *fa_port* – для настройки интерфейсов Fast Ethernet 1-24;
interface gigabitethernet *gi_port* – для настройки интерфейсов Gigabit Ethernet 25-26;
interface port-channel *group* – для настройки группы каналов,

где

- *group* – порядковый номер группы каналов принимает значения (1..8);
- *fa_port* – порядковый номер интерфейса Fast Ethernet задается в виде: 1..8/0/1..24;
- *gi_port* – порядковый номер интерфейса Gigabit Ethernet задается в виде: 1..8/0/25..26.

для MES1124

interface fastethernet *fa_port* – для настройки интерфейсов Fast Ethernet 1-24;
interface gigabitethernet *gi_port* – для настройки интерфейсов Gigabit Ethernet 25-28;
interface port-channel *group* – для настройки группы каналов,

где

- *group* – порядковый номер группы каналов принимает значения (1..8);
- *fa_port* – порядковый номер интерфейса Fast Ethernet задается в виде: 1..8/0/1..24;
- *gi_port* – порядковый номер интерфейса Gigabit Ethernet задается в виде: 1..8/0/25..28.

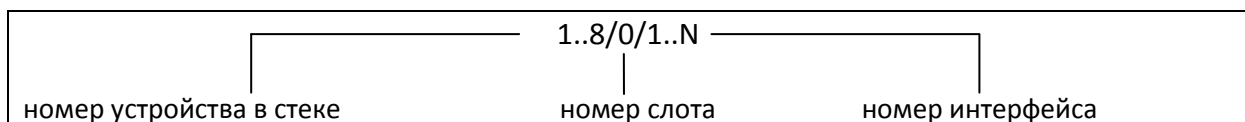
для MES2124

interface gigabitethernet *gi_port* – для настройки интерфейсов Gigabit Ethernet 1-28;
interface port-channel *group* – для настройки группы каналов,

где

- *group* – порядковый номер группы каналов принимает значения (1..8);
- *gi_port* – порядковый номер интерфейса Gigabit Ethernet задается в виде: 1..8/0/1..28.

Запись интерфейса



Команды, введенные в режиме конфигурирования интерфейса, применяются к выбранному интерфейсу.

Ниже приведены команды для входа в режим настройки десятого ethernet-интерфейса первого устройства в стеке и входа в режим настройки группы каналов 1.

```
console# configure
console(config)# interface gigabitethernet 1/0/10
console(config-if)#
console# configure
console(config)# interface port-channel 1
console(config-if)#
```

Выбор диапазона интерфейсов осуществляется при помощи команд:

interface range gigabitethernet *portlist* – для настройки диапазона интерфейсов;
interface range port-channel *groupelist* – для настройки всех групп портов.

Команды, введенные в данном режиме, применяются к выбранному диапазону интерфейсов.

Ниже приведены команды для входа в режим настройки диапазона ethernet интерфейсов с 1 по 10 и для входа в режим настройки всех групп портов.

```

console# configure
console(config)# interface range gigabitethernet 1/0/1-10
console(config-if)#

console# configure
console(config)# interface range fastethernet 1/0/1-10
console(config-if)#

console# configure
console(config)# interface range port-channel 1-8
console(config-if)#

```

Таблица 5.29 – Команды режима конфигурирования интерфейса Ethernet и Port-Channel

Команда	Значение/значение по умолчанию	Действие
shutdown	-/выключен	Выключить конфигурируемый интерфейс (Ethernet, port-channel).
no shutdown		Включить конфигурируемый интерфейс.
description descr	1-64 символов/ нет описания	Добавить описание интерфейса (Ethernet, port-channel).
no description		Удалить описание интерфейса.
speed mode	10, 100, 1000	Задать скорость передачи данных (Ethernet, port-channel).
no speed		Установить значение по умолчанию.
duplex mode	{full, half}/full	Задать режим дуплекса интерфейса.
no duplex		Установить значение по умолчанию.
negotiation [cap1 [cap2... cap5]]	10f, 10h, 100f, 100h, 1000f	Включает автосогласование для скорости и дуплекса на настраиваемом интерфейсе. Можно указать определенные совместимости параметра автосогласования, если параметры не заданы, то поддерживаются все совместимости (Ethernet, port-channel).  Данная команда недоступна для портов xg(1-4)
no negotiation		Выключает автосогласование для скорости и дуплекса на настраиваемом интерфейсе.
flowcontrol mode	{on, off, auto}/off	Задать режим управления потоком flowcontrol (включить, отключить или автосогласование). Автосогласование flowcontrol работает только в случае, если режим автосогласования negotiation включен на настраиваемом интерфейсе (Ethernet, port-channel).
no flowcontrol		Отключить режим управления потоком.
mdix mode	{on, auto}/auto	Позволяет использование «перекрещенного» кабеля на настраиваемом интерфейсе (Ethernet).  Данная команда недоступна для портов xg(1-4)
no mdix		Запрещает использование «перекрещенного» кабеля на настраиваемом интерфейсе.
back-pressure	-/выключен	Включает функцию «обратного давления» на настраиваемом интерфейсе (Ethernet).
no back-pressure		Выключает функцию «обратного давления» на настраиваемом интерфейсе.
load-average period	period: {5..300}/15	Установить период, в течение которого собирается статистика о нагрузке на интерфейсе.
no load-average		Установить значение по умолчанию.

Команды режима глобального конфигурирования

Вид запроса командной строки в режиме конфигурирования интерфейса:

```
console# configure
console(config)#
```

Таблица 5.30 – Команды режима общих настроек интерфейса Ethernet и Port-Channel

Команда	Значение	Действие
port jumbo-frame	-/запрещено	<p>Разрешает коммутатору работать с фреймами большого размера.</p> <p><input checked="" type="checkbox"/> Значение maximum transmission unit (MTU) по умолчанию 1500 байт.</p> <p><input checked="" type="checkbox"/> Настройка вступит в силу только после перезагрузки устройства.</p>
no port jumbo-frame		Запрещает коммутатору работать с фреймами большого размера.
errdisable recovery cause { loopback-detection port-security dot1x-src-address acl-deny stp-bpdu-guard stp-loopback-guard }	-/запрещено	<p>Включить автоматическую активацию интерфейса после его отключения в следующих случаях:</p> <ul style="list-style-type: none"> - loopback-detection — обнаружение петель; - port-security — нарушение безопасности для port security; - dot1x-src-address — не прохождение аутентификации, основанной на MAC-адресах пользователей; - acl-deny — не соответствие спискам доступа (ACL); - stp-bpdu-guard — активация защиты BPDU Guard (передача несанкционированного пакета BPDU через интерфейс); - stp-loopback-guard — обнаружение петель.
no errdisable recovery cause { loopback-detection port-security dot1x-src-address acl-deny stp-bpdu-guard stp-loopback-guard }		Установить значение по умолчанию.
errdisable recovery interval seconds	seconds: {30..86400}/300 секунд	Установить временной интервал для автоматического повторного включения интерфейса.
no errdisable recovery interval		Установить значение по умолчанию.

Команды режима EXEC

Вид запроса командной строки в режиме EXEC:

```
console#
```

Таблица 5.31 – Команды режима EXEC

Команда	Значение	Действие
clear counters	-	Сброс статистики для всех интерфейсов.
clear counters { gigabitethernet gi_port fastethernet fa_port }	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24};	Сброс статистики для Ethernet-порта.
clear counters port-channel group	group: {1..8}	Сброс статистики для группы портов.
set interface active { gigabitethernet gi_port fastethernet fa_port }	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24};	Активирует порт, выключенный командой shutdown .
show interfaces configuration [gigabitethernet gi_port	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}	Показать конфигурацию интерфейсов.

<code>fastethernet fa_port port-channel group]</code>		
<code>set interface active port-channel group</code>	group: {1..8}	Активирует группу портов, выключенную командой shutdown .
<code>show interfaces status</code>	-	Показать состояние всех интерфейсов.
<code>show interfaces status { gigabitethernet gi_port fastethernet fa_port}</code>	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24};	Показать состояние Ethernet-порта.
<code>show interfaces status port-channel group</code>	group: {1..8}	Показать состояние группы портов.
<code>show interfaces advertise</code>	-	Показать параметры автосогласования, объявленные для всех интерфейсов.
<code>show interfaces advertise { gigabitethernet gi_port fastethernet fa_port}</code>	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24};	Показать параметры автосогласования, объявленные для Ethernet-порта.
<code>show interfaces advertise port-channel group</code>	group: {1..8}	Показать параметры автосогласования, объявленные для группы портов.
<code>show interfaces description</code>	-	Показать описания всех интерфейсов.
<code>show interfaces description { gigabitethernet gi_port fastethernet fa_port}</code>	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24};	Показать описание Ethernet-порта.
<code>show interfaces description port-channel group</code>	group: {1..8}	Показать описание группы портов.
<code>show interfaces counters</code>	-	Показать статистику для всех интерфейсов.
<code>show interfaces counters { gigabitethernet gi_port fastethernet fa_port}</code>	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24};	Показать статистику для Ethernet-порта.
<code>show interfaces counters port-channel group</code>	group: {1..8}	Показать статистику для группы портов.
<code>show interfaces utilization</code>	-	Показать статистику по нагрузке для всех интерфейсов.
<code>show interfaces utilization [gigabitethernet gi_port fastethernet fa_port port-channel group]</code>	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}	Показать статистику по нагрузке для Ethernet-интерфейса.
<code>show interfaces utilization port-channel group</code>	group: {1..8}	Показать статистику по нагрузке для группы портов.
<code>show ports jumbo-frame</code>	-	Показать настройку jumbo-frames в коммутаторе.
<code>show errdisable recovery</code>	-	Показать настройки для автоматической повторной активации интерфейса.
<code>show errdisable interfaces [gigabitethernet gi_port fastethernet fa_port port-channel group]</code>	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}	Показать причину отключения интерфейса/интерфейсов и состояние автоматической активации.

Примеры выполнения команд.

- Показать состояние интерфейсов:

```
console# show interfaces status
```

Port	Type	Duplex	Speed	Neg	Flow ctrl	Link State	Back Pressure	Mdix Mode
gi0/1	1G-Fiber	--	--	--	--	Down	--	--
gi0/2	1G-Fiber	--	--	--	--	Down	--	--
gi0/3	1G-Fiber	--	--	--	--	Down	--	--
gi0/4	1G-Fiber	--	--	--	--	Down	--	--
gi0/5	1G-Fiber	--	--	--	--	Down	--	--
gi0/6	1G-Fiber	--	--	--	--	Down	--	--
gi0/7	1G-Fiber	--	--	--	--	Down	--	--

gi0/8	1G-Fiber	--	--	--	--	Down	--	--
gi0/9	1G-Fiber	--	--	--	--	Down	--	--
gi0/10	1G-Fiber	--	--	--	--	Down	--	--
gi0/11	1G-Combo-C	--	--	--	--	Down	--	--
gi0/12	1G-Combo-C	--	--	--	--	Down	--	--
gi0/13	1G-Fiber	--	--	--	--	Down	--	--
gi0/14	1G-Fiber	--	--	--	--	Down	--	--
gi0/15	1G-Fiber	--	--	--	--	Down	--	--
gi0/16	1G-Fiber	--	--	--	--	Down	--	--
gi0/17	1G-Fiber	--	--	--	--	Down	--	--
gi0/18	1G-Fiber	--	--	--	--	Down	--	--
gi0/19	1G-Fiber	--	--	--	--	Down	--	--
gi0/20	1G-Fiber	--	--	--	--	Down	--	--
gi0/21	1G-Fiber	--	--	--	--	Down	--	--
gi0/22	1G-Fiber	--	--	--	--	Down	--	--
gi0/23	1G-Combo-C	--	--	--	--	Down	--	--
gi0/24	1G-Combo-C	Full	100	Enabled	Off	Up	Disabled	On
te0/1	10G-Fiber	--	--	--	--	Down	--	--
te0/2	10G-Fiber	--	--	--	--	Down	--	--
te0/3	10G-Fiber	--	--	--	--	Down	--	--
te0/4	10G-Fiber	--	--	--	--	Down	--	--

Ch	Type	Duplex	Speed	Neg	Flow control	Link State
Po1	--	--	--	--	--	Not Present
Po2	--	--	--	--	--	Not Present
Po3	--	--	--	--	--	Not Present
Po4	--	--	--	--	--	Not Present
Po5	--	--	--	--	--	Not Present
Po6	--	--	--	--	--	Not Present
Po7	--	--	--	--	--	Not Present
Po8	--	--	--	--	--	Not Present

- Показать параметры авто-согласования:

```
console# show interfaces advertise
```

Port	Type	Neg	Operational Link Advertisement
gi0/1	1G-Fiber	Disabled	--
gi0/2	1G-Fiber	Disabled	--
gi0/3	1G-Fiber	Disabled	--
gi0/4	1G-Fiber	Disabled	--
gi0/5	1G-Fiber	Disabled	--
gi0/6	1G-Fiber	Disabled	--
gi0/7	1G-Fiber	Disabled	--
gi0/8	1G-Fiber	Disabled	--
gi0/9	1G-Fiber	Disabled	--
gi0/10	1G-Fiber	Disabled	--
gi0/11	1G-Combo-C	Enabled	--
gi0/12	1G-Combo-C	Enabled	--
gi0/13	1G-Fiber	Disabled	--
gi0/14	1G-Fiber	Disabled	--
gi0/15	1G-Fiber	Disabled	--
gi0/16	1G-Fiber	Disabled	--
gi0/17	1G-Fiber	Disabled	--
gi0/18	1G-Fiber	Disabled	--
gi0/19	1G-Fiber	Disabled	--
gi0/20	1G-Fiber	Disabled	--
gi0/21	1G-Fiber	Disabled	--
gi0/22	1G-Fiber	Disabled	--
gi0/23	1G-Combo-C	Enabled	--
gi0/24	1G-Combo-C	Enabled	1000f, 100f, 100h, 10f, 10h
te0/1	10G-Fiber	Disabled	--
te0/2	10G-Fiber	Disabled	--
te0/3	10G-Fiber	Disabled	--
te0/4	10G-Fiber	Disabled	--

Ch	Type	Neg	Operational Link Advertisement
Po1	--	Enabled	--
Po2	--	Enabled	--
Po3	--	Enabled	--
Po4	--	Enabled	--
Po5	--	Enabled	--
Po6	--	Enabled	--
Po7	--	Enabled	--
Po8	--	Enabled	--

- Показать статистику по интерфейсам:

```
console# show interfaces counters
```

Port	InUcastPkts	InMcastPkts	InBcastPkts	InOctets
gi0/1	0	0	0	0
gi0/2	0	0	0	0
gi0/3	0	0	0	0
gi0/4	0	0	0	0
gi0/5	0	0	0	0
gi0/6	0	0	0	0
gi0/7	0	0	0	0
gi0/8	0	0	0	0
gi0/9	0	0	0	0
gi0/10	0	0	0	0
gi0/11	0	0	0	0
gi0/12	0	0	0	0
gi0/13	0	0	0	0
gi0/14	0	0	0	0
gi0/15	0	0	0	0
gi0/16	0	0	0	0
gi0/17	0	0	0	0
gi0/18	0	0	0	0
gi0/19	0	0	0	0
gi0/20	0	0	0	0

More: <space>, Quit: q, One line: <return>

- Показать статистику по группе каналов 1:

```
console# show interfaces counters port-channel 1
```

Ch	InUcastPkts	InMcastPkts	InBcastPkts	InOctets
Po1	111	0	0	9007

Ch	OutUcastPkts	OutMcastPkts	OutBcastPkts	OutOctets
Po1	0	6	3	912

Alignment Errors: 0
 FCS Errors: 0
 Single Collision Frames: 0
 Multiple Collision Frames: 0
 SQE Test Errors: 0
 Deferred Transmissions: 0
 Late Collisions: 0
 Excessive Collisions: 0
 Carrier Sense Errors: 0
 Oversize Packets: 0
 Internal MAC Rx Errors: 0
 Symbol Errors: 0
 Received Pause Frames: 0

Таблица 5.32 - Описание счетчиков

<i>Счетчик</i>	<i>Описание</i>
<i>InOctets</i>	Количество принятых байтов.
<i>InUcastPkts</i>	Количество принятых одноадресных пакетов.
<i>InMcastPkts</i>	Количество принятых многоадресных пакетов.
<i>InBcastPkts</i>	Количество принятых широковещательных пакетов.
<i>OutOctets</i>	Количество переданных байтов.
<i>OutUcastPkts</i>	Количество переданных одноадресных пакетов.
<i>OutMcastPkts</i>	Количество переданных многоадресных пакетов.
<i>OutBcastPkts</i>	Количество переданных широковещательных пакетов.
<i>Alignment Errors</i>	Количество принятых фреймов с нарушенной целостностью (с количеством байт не соответствующим длине) и не прошедших проверку контрольной суммы (FCS).
<i>FCS Errors</i>	Количество принятых фреймов с количеством байт, соответствующим длине, но не прошедших проверку контрольной суммы (FCS).
<i>Single Collision Frames</i>	Количество фреймов, вовлеченных в единичную коллизию, но впоследствии переданных успешно.
<i>Multiple Collision Frames</i>	Количество фреймов, вовлеченных более чем в одну коллизию, но впоследствии переданных успешно.
<i>Deferred Transmissions</i>	Количество фреймов, для которых первая попытка передачи отложена из-за занятости среды передачи.
<i>Late Collisions</i>	Количество случаев, когда коллизия зафиксирована после того, как в канал связи уже были переданы первые 64 байт (slotTime) пакета.
<i>Excessive Collisions</i>	Количество фреймов, которые не были переданы из-за избыточного количества коллизий.
<i>Carrier Sense Errors</i>	Количество случаев, когда состояние контроля несущей было потеряно, либо не утверждено при попытке передачи фрейма.
<i>Oversize Packets</i>	Количество принятых пакетов, размер которых превышает максимальный разрешенный размер фрейма.
<i>Internal MAC Rx Errors</i>	Количество фреймов, которые не были приняты успешно из-за внутренней ошибки приема на уровне MAC.
<i>Symbol Errors</i>	<p>Для интерфейса, работающего в режиме 100Мб/с – количество случаев, когда имелся недопустимый символ данных, в то время как правильная несущая была представлена.</p> <p>Для интерфейса, работающего в полудуплексном режиме 1000Мб/с – количество случаев, когда средства приема заняты в течение времени, равному или большему чем размер слота (slotTime), и в течение которого имелось хотя бы одно событие, которое заставляет PHY выдавать ошибку приема данных (Data reception error) или ошибку несущей (Carrier extend error) на GMII.</p> <p>Для интерфейса, работающего в полном дуплексном режиме 1000Мб/с – количество случаев, когда средства приема заняты в течение времени, равному или большему чем минимальный размер фрейма (minFrameSize), и в течение которого имелось хотя бы одно событие, которое заставляет PHY выдавать ошибку приема данных (Data reception error) на GMII.</p>
<i>Received Pause Frames</i>	Количество принятых управляющих MAC-фреймов с кодом операции PAUSE.
<i>Transmitted Pause</i>	Количество переданных управляющих MAC-фреймов с кодом операции PAUSE.

<i>Frames</i>	
---------------	--

- Показать настройку jumbo-frames в коммутаторе:

```
console# show ports jumbo-frame
```

```
Jumbo frames are disabled
Jumbo frames will be disabled after reset
```

5.8.2 Настройка интерфейса VLAN

Команды режима конфигурирования VLAN

Вид запроса командной строки в режиме конфигурирования VLAN:

```
console# configure
console(config)# vlan database
console(config-vlan)#
```

Данный режим доступен из режима глобального конфигурирования и предназначен для задания параметров конфигурации VLAN.

Таблица 5.33 – Команды режима конфигурирования VLAN

<i>Команда</i>	<i>Значение/значение по умолчанию</i>	<i>Действие</i>
vlan <i>vlan-range</i>	vlan_id: {2 .. 4094}	Добавить VLAN, или несколько VLAN.
no vlan <i>vlan-range</i>		Удалить VLAN, или несколько VLAN.
map protocol <i>protocol</i> [encaps] protocols-group <i>group</i>	protocol {ip, ipx, ipv6, arp, {0600-ffff (hex)}*}	Привязать протокол к группе протоколов ассоциированных вместе.
no map protocol <i>protocol</i> [encaps]	encaps {ethernet, rfc1042, llcOther} ethernet group {1.. 2147483647}	Удалить привязку. * - номер протокола (16 бит).
map mac <i>mac-address</i> { <i>host</i> <i>mask</i> } macs-group <i>group</i>	mask: {9..48}	Привязать MAC-адрес или группу по маске к группе MAC-адресов.
no map mac <i>mac-address</i> { <i>host</i> <i>mask</i> }		Удалить привязку.

Команды режима конфигурирования интерфейса (диапазона интерфейсов) VLAN

Вид запроса командной строки в режиме конфигурирования интерфейса VLAN:

```
console# configure
console(config)# interface {vlan {VLAN ID}|range vlan {VLANlist}}
```

Данный режим доступен из режима конфигурирования и предназначен для задания параметров конфигурации интерфейса VLAN, либо диапазона интерфейсов.

Выбор интерфейса осуществляется при помощи команды `interface vlan {VLAN ID}`.

Выбор диапазона интерфейсов осуществляется при помощи команды `interface range vlan {VLANlist}`.

Ниже приведены команды для входа в режим настройки интерфейса VLAN 1 и входа в режим настройки группы VLAN 1, 3, 7.

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

console# configure
console(config)# interface range vlan 1,3,7
console(config-if)#
```

Таблица 5.34 – Команды режима конфигурирования интерфейса VLAN

Команда	Значение/значение по умолчанию	Действие
<code>name name</code>	1-64 символов/ имя соответствует номеру VLAN	Добавить имя VLAN.
<code>no name</code>		Установить значение по умолчанию.

Команды режима конфигурирования интерфейса (диапазона интерфейсов) Ethernet, интерфейса группы портов

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet, интерфейса группы портов:

```
console# configure
console(config)# interface {fastethernet fa_port | gigabitethernet gi_port | port-channel group | range {...}}
console(config-if)#
```

Данный режим доступен из режима конфигурирования и предназначен для задания параметров конфигурации интерфейса (порта коммутатора или группы портов, работающих в режиме разделения нагрузки), либо диапазона интерфейсов.

Порт может работать в четырех режимах:

- *access* – интерфейс доступа – нетегированный интерфейс для одной VLAN;
- *trunk* – интерфейс, принимающий только тегированный трафик, за исключением одного VLAN, который может быть добавлен с помощью команды *switchport trunk native vlan*;
- *general* – интерфейс с полной поддержкой 802.1q, принимает как тегированный, так и нетегированный трафик;
- *customer* – 802.1 Q-in-Q интерфейс.

Таблица 5.35 – Команды режима конфигурирования интерфейса Ethernet

Команда	Значение/значение по умолчанию	Действие
<code>switchport mode mode</code>	access, trunk, general, customer/access	Задать режим работы порта в VLAN.
<code>no switchport mode</code>		Установить значение по умолчанию.
<code>switchport access vlan vlan_id</code>	vlan_id: {1..4094}/1	Добавить VLAN для интерфейса доступа.
<code>no switchport access vlan</code>		Установить значение по умолчанию.
<code>switchport trunk allowed vlan add VLANlist</code>	VLANlist: {2..4094, all}	Добавить список VLAN для интерфейса.
<code>switchport trunk allowed vlan remove VLANlist</code>		Удалить список VLAN для интерфейса.
<code>switchport trunk native</code>	vlan_id: {1..4095}/	Добавляет указанный VLAN в качестве Default VLAN для

vlan <i>vlan_id</i>	1 – если установлен VLAN по умолчанию, иначе 4095 – нетегированный трафик отбрасывается	данного интерфейса (port default VLAN ID – PVID), весь нетегированный трафик, поступающий на данный порт, определяется в данный VLAN.
no switchport trunk native vlan		Установить значение по умолчанию.
switchport general allowed vlan add <i>VLANlist</i> [tagged untagged]	<i>VLANlist</i> : {2..4094, all}	Добавить список VLAN для интерфейса. Порт будет передавать: Tagged - тегированные, untagged – нетегированные пакеты для VLAN.
switchport general allowed vlan remove <i>VLANlist</i>		Удалить список VLAN для интерфейса.
switchport general pvid <i>vlan_id</i>	<i>vlan_id</i> : {1..4094}/ 1 – если установлен VLAN по умолчанию, иначе 4095	Добавить идентификатор VLAN порта (PVID) для основного интерфейса.
no switchport general pvid		Установить значение по умолчанию.
switchport general ingress-filtering disable		Выключить для основного интерфейса фильтрацию входящих пакетов на основе присвоенного им значения VLAN ID.
no switchport general ingress-filtering disable	-/ фильтрация включена	Включить для основного интерфейса фильтрацию входящих пакетов на основе присвоенного им значения VLAN ID. Если фильтрация включена, и пакет не входит в группу VLAN с присвоенным пакету значением VLAN ID, то пакет отбрасывается.
switchport general acceptable-frame-type { tagged-only untagged-only all }	-/принимать все типы фреймов	Принимать на основном интерфейсе только фреймы определенного типа: - tagged-only – только тегированные; - untagged-only – только не тегированные; - all – все фреймы.
no switchport general acceptable-frame-type		Принимать на основном интерфейсе все типы фреймов.
switchport general map protocols-group <i>group</i> vlan <i>vlan_id</i>	<i>vlan_id</i> : {1..4094}	Установить правило классификации для основного интерфейса, основанное на привязке к протоколу.
no switchport general map protocols-group <i>group</i>	<i>group</i> : {1.. 2147483647}	Удалить правило классификации.
switchport general map macs-group <i>group</i> vlan <i>vlan_id</i>	<i>vlan_id</i> : {1..4094}	Установить правило классификации для основного интерфейса, основанное на привязке к MAC-адресу.
no switchport general map macs-group <i>group</i>	<i>group</i> : {1.. 2147483647}	Удалить правило классификации.
switchport dot1q ether-type egress stag <i>ether-type</i>	<i>ether-type</i> : 0xffff (hex)	Заменить EtherType в исходящих пакетах.
no switchport dot1q ether-type egress stag		Установить значение по умолчанию.
switchport customer vlan <i>vlan_id</i>	<i>vlan_id</i> : {1..4094}/1	Добавить VLAN для пользовательского интерфейса.
no switchport customer vlan		Установить значение по умолчанию.
switchport customer multicast-tv vlan <i>vlan_id</i>	<i>vlan_id</i> : {1..4094}	Разрешает принимать многоадресный трафик из указанной VLAN (не являющейся VLAN пользовательского интерфейса) на настраиваемом интерфейсе, совместно с пользователями других пользовательских портов, принимающих многоадресный трафик из данной VLAN.
no switchport customer multicast-tv vlan		Запрещает принимать многоадресный трафик на настраиваемом интерфейсе.
switchport forbidden vlan add <i>VLANlist</i>	<i>vlan_id</i> : {2..4094, all}/ все VLAN разрешены порту	Запретить добавление указанных VLAN порту.
no switchport forbidden vlan add <i>VLANlist</i>		Установить значение по умолчанию.
switchport forbidden vlan	<i>vlan_id</i> : {2..4094, all}/	Разрешить добавление указанных VLAN порту.

<code>remove VLANlist</code>	все VLAN разрешены порту	
<code>no switchport forbidden vlan remove VLANlist</code>		Установить значение по умолчанию.
<code>switchport forbidden default-vlan</code>	По умолчанию членство в дефолтной VLAN разрешено	Запретить добавление дефолтной VLAN порту.
<code>no switchport forbidden default-vlan</code>		Установить значение по умолчанию.
<code>switchport protected-port</code>	-	Переводит порт в режим Private VLAN Edge – изоляцию внутри группы портов.
<code>no switchport-protected-port</code>		Восстанавливает значение по умолчанию.
<code>switchport community community</code>	community: 1..30	Добавляет порт в private-vlan-edge-сообщество. Порты одного сообщества не могут обмениваться трафиком между собой.
<code>no switchport community</code>		Восстанавливает значение по умолчанию
<code>switchport protected {gigabitethernet gi_port fastethernet fa_port port-channel group}</code>	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8};	Отменяет маршрутизацию по базе данных изученных MAC-адресов (FDB) и направляет весь одноадресный, многоадресный и широковещательный трафик на uplink-порт.
<code>no switchport protected</code>	По умолчанию используется маршрутизация по базе данных изученных MAC-адресов (FDB)	Отключает отмену маршрутизации по базе данных изученных MAC-адресов (FDB).
<code>ip internal-usage-vlan vlan_id</code>	vlan_id: {1..4094}/ нет резерва	Зарезервировать VLAN для внутреннего использования на интерфейсе.
<code>no ip internal-usage-vlan</code>		Установить значение по умолчанию.
<code>switchport default-vlan tagged</code>	-	Установить порт как тегирующий в дефолтной VLAN.
<code>no switchport default-vlan tagged</code>		Установить значение по умолчанию.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console# configure
console(config)#
```

Таблица 5.36 – Команды режима глобального конфигурирования

<i>Команда</i>	<i>Значение</i>	<i>Действие</i>
<code>vlan database</code>	-	Вход в режим конфигурирования VLAN

Пример использования команды:

```
console# configure
console(config)# vlan database
console(config-vlan)#
```

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 5.37 – Команды режима Privileged EXEC

<i>Команда</i>	<i>Значение</i>	<i>Действие</i>
show vlan	-	Показать информацию по всем VLAN.
show vlan name name	1..32 символов	Показать информацию по VLAN, поиск по имени.
show vlan tag vlan_id	vlan_id: {1..4094}	Показать информацию по VLAN, поиск по идентификатору.
show vlan internal usage	-	Показать список VLAN для внутреннего использования коммутатором.
show default-vlan-membership [gigabitethernet gi_port fastethernet fa_port port-channel group]	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}	Показать состав группы дефолтной VLAN.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.38 – Команды режима EXEC

<i>Команда</i>	<i>Значение</i>	<i>Действие</i>
show vlan multicast-tv vlan vlan_id	vlan_id: {1..4094}	Показать порты-источники и приемники многоадресного трафика в данной VLAN. Порты источники могут, как передавать, так и принимать многоадресный трафик.
show vlan protocols-groups	-	Показать информацию о группах протоколов.
show vlan macs-groups	-	Показать информацию о группах MAC-адресов.
show interfaces switchport { gigabitethernet gi_port fastethernet fa_port port-channel group }	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}	Показать конфигурацию порта, группы портов.
show interfaces protected-ports [gigabitethernet gi_port fastethernet fa_port port-channel group]	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}	Показать состояние портов: в режиме Private VLAN Edge, в private-vlan-edge-сообществе.

Примеры выполнения команд

- Показать информацию о всех VLAN:

```
console# show vlan
```

Vlan	Name	Ports	Type	Authorization
1	1	1/g (1-48) , 2/g (1-48) , 3/g (1-48) , 4/g (1-48) , 5/g (1-48) , 6/g (1-48) , 7/g (1-4g (1-48) , ch (1-8)	other	Required
4	4		permanent	Required

- Показать порты источники и приемники многоадресного трафика в VLAN 4:

```
console# show vlan multicast-tv vlan 4
```

```
Source ports : 1/g1
Receiver ports: 1/g(2,4,8)
```

- Показать информацию о группах протоколов:

```
console# show vlan protocols-groups
```

Encapsulation	Protocol	Group Id
0x800 (IP)	Ethernet	1
0x806 (ARP)	Ethernet	1
0x86dd (IPv6)	Ethernet	3

- Показать информацию о группах подсетей:

```
console# show vlan subnets-groups
```

Ip Subnet Address	Mask	Group Id
192.168.16.44	255.255.255.0	1
192.168.16.44	255.255.255.0	2

- Показать список VLAN для внутреннего использования коммутатором:

```
console# show vlan internal usage
```

Usage	VLAN	Reserved	IP address
1/g22	9	Yes	Inactive

- Показать конфигурацию порта Ethernet 22:

```
console# show interfaces switchport gigabitethernet 1/0/22
```

```
Port : 1/g22
Port Mode: Access
Gvrp Status: disabled
Ingress Filtering: true
Acceptable Frame Type: admitAll
Ingress Untagged VLAN ( NATIVE ): 1
Protected: Disabled

Port is member in:

Vlan          Name          Egress rule Port Membership Type
-----
1             1             Untagged    System

Forbidden VLANS:
Vlan          Name
-----

Classification rules:

Protocol based VLANs:
Group ID Vlan ID
-----

Subnet based VLANs:
Group ID Vlan ID
```

5.9 Selective Q-in-Q

Данная функция позволяет на основе сконфигурированных правил фильтрации по номерам внутренних VLAN (Customer VLAN) производить добавление внешнего SPVLAN (Service Provider's VLAN), подменять Customer VLAN, а также запрещать прохождения трафика.

Для устройства создается список правил, на основании которого будет обрабатываться трафик.

Команды режима конфигурирования интерфейса (диапазона интерфейсов) Ethernet и Port-Channel

Вид запроса командной строки режима конфигурирования интерфейса конфигурирования:

```
console# configure
console(config)# interface { fastethernet fa_port | gigabitethernet gi_port
| port-channel group | range {...}}
console(config-if)#
```

Таблица 5.39 – Команды режима конфигурирования интерфейса (диапазона интерфейсов) Ethernet

Команда	Значение	Действие
selective-qinq list ingress add_vlan <i>vlan_id</i> [ingress_vlan Outer Vlan ID]	vlan_id: {1..4094} Outer Vlan ID: {1..4094}	Создает правило, на основании которого к внешней метке Outer Vlan ID входящего пакета будет добавляться VLAN ID. Если «ingress_vlan» не указывать – правило будет применяться ко всем входящим пакетам.
selective-qinq list ingress deny [ingress_vlan Outer Vlan ID]	Outer Vlan ID:{1..4094}	Создает запрещающее правило, на основании которого входящие пакеты с внешней меткой тега Outer Vlan ID будут отбрасываться. Если «ingress_vlan» не указывается – будут отбрасываться все входящие пакеты.
selective-qinq list ingress permit [ingress_vlan Outer Vlan ID]	Outer Vlan ID: {1..4094}	Создает разрешающее правило, на основании которого входящие пакеты с внешней меткой тега Outer Vlan ID будут передаваться без изменений. Если «ingress_vlan» не указывается – будут передаваться все входящие пакеты без изменений.
selective-qinq list ingress override_vlan <i>vlan_id</i> [ingress_vlan Outer Vlan ID]	VLAN ID: {1..4094} Outer Vlan ID:{1..4094}	Создает правило, на основании которого внешняя метка входящего пакета Outer Vlan ID будет заменяться на VLAN ID. Если Outer Vlan ID не указывать – правило будет применяться ко всем входящим пакетам.
selective-qinq list egress override_vlan <i>vlan_id</i> [ingress_vlan Outer Vlan ID]	VLAN ID: {1..4094} Outer Vlan ID: {1..4094}	Создает правило, на основании которого внешняя метка исходящего пакета Outer Vlan ID будет заменяться на VLAN ID. Если «ingress_vlan» не указывать – правило будет применяться ко всем исходящим пакетам.
no selective-qinq list ingress [ingress-vlan <i>vlan</i>]	vlan: {1-4094}	Удаляет указанное правило selective qinq для входящих пакетов. Команда без параметра «ingress vlan» удаляет правило по умолчанию.
no selective-qinq list egress ingress-vlan <i>vlan</i>	vlan: {1-4094}	Удаляет список правил selective qinq для исходящих пакетов.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.40 – Команды режима EXEC

<i>Команда</i>	<i>Значение</i>	<i>Действие</i>
<code>show selective-qinq</code>	-	Отображает список правил selective qinq.
<code>show selective-qinq interface {gigabitethernet gi_port tengigabitethernet te_port}</code>	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}	Отображает список правил selective qinq для указанного порта.

Примеры выполнения команд

- Создать правило, на основании которого внешняя метка входящего пакета 1198 будет заменяться на 100.

```
console# configure
console(config)# interface gigabitethernet 1/0/1
console(config-if)# selective-qinq list ingress override vlan 10 ingress-
vlan 11
console(config-if)# end
```

- Отобразить список созданных правил selective qinq:

Direction	Interface	Rule type	Vlan ID	Classification	by Parameter
ingress	gi0/1	override_vlan	10	ingress_vlan	11

5.10 Контроль широковещательного «шторма»

Широковещательный «шторм» возникает вследствие чрезмерного количества широковещательных сообщений, одновременно передаваемых по сети через один порт, что приводит к перегрузке ресурсов сети и появлению задержек. «Шторм» может возникнуть при наличии «закольцованных» сегментов в сети Ethernet. Коммутатор измеряет скорость принимаемого широковещательного, многоадресного и неизвестного одноадресного трафика для портов с включенным контролем широковещательного «шторма» и отбрасывает пакеты, если скорость превышает заданное максимальное значение.

Команды режима конфигурирования интерфейса Ethernet

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet, интерфейса группы портов:

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

Таблица 5.41 – Команды режима конфигурирования интерфейса Ethernet

<i>Команда</i>	<i>Значение</i>	<i>Действие</i>
<code>storm-control include-multicast</code>	По умолчанию функция включена	Добавляет контроль многоадресного трафика к контролю широковещательного.
<code>no storm-control include-multicast</code>		Выключает контроль многоадресного трафика.
<code>storm-control include-multicast unknown-unicast</code>	По умолчанию функция включена	Добавляет контроль неизвестного одноадресного трафика к контролю широковещательного.
<code>no storm-control include-multicast unknown-unicast</code>		Выключает контроль неизвестного одноадресного трафика.
<code>storm-control broadcast</code>	По умолчанию функция	Включает контроль широковещательного трафика.

enable	выключена	
no storm-control broadcast enable		Выключает контроль широковещательного трафика.
storm-control broadcast level kbps rate	64-1000000/ 3500 Кбит/с	Задаёт максимальную скорость для широковещательного, многоадресного и неизвестного одноадресного трафика.
no port storm-control broadcast level		Устанавливает значение по умолчанию.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.42 – Команды режима EXEC

<i>Команда</i>	<i>Значение</i>	<i>Действие</i>
show storm-control [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i>]	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}	Показывает конфигурацию функции контроля широковещательного «шторма» для указанного порта, либо всех портов.

Примеры выполнения команд

Включить контроль широковещательного, многоадресного и неизвестного одноадресного трафика на 15 интерфейсе Ethernet. Установить максимальную скорость для контролируемого трафика – 5000 Кб/с:

```
console# configure
console(config)# interface gigabitethernet 1/0/15
console(config-if)# storm-control broadcast enable
console(config-if)# storm-control include-multicast
console(config-if)# storm-control include-multicast unknown-unicast
console(config-if)# storm-control broadcast level kbps 5000
```

5.11 Группы агрегации каналов – Link Agregation Group (LAG)

Коммутатор MES1024/MES1124/MES2124 обеспечивает поддержку до восьми интерфейсов Ethernet в одной группе портов LAG и до восьми групп LAG на устройстве или стеке устройств. Каждая группа портов должна состоять из интерфейсов Ethernet с одинаковой скоростью, работающих в дуплексном режиме. Объединение портов в группу увеличивает пропускную способность канала между взаимодействующими устройствами и повышает отказоустойчивость. Группа портов является для коммутатора одним логическим портом.

Устройство поддерживает два режима работы группы портов – статическая группа и группа, работающая по протоколу LACP. Работа по протоколу LACP описана в соответствующем разделе конфигурации.



Если для интерфейса произведены настройки, то для добавления его в группу следует вернуть настройки по умолчанию.

Добавление интерфейсов в группу агрегации каналов доступно только в режиме конфигурирования интерфейса Ethernet.

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet:

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

Таблица 5.43 – Команды режима конфигурирования интерфейса Ethernet

Команда	Значение	Действие
channel-group {group} mode {mode}	group {1..8}	Добавить ethernet-интерфейс в группу портов (on – добавить порт в канал без lacp, auto – добавить порт в канал с lacp).
no channel-group	mode {on, auto}	Удалить Ethernet-интерфейс из группы портов.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console# configure
console(config)#
```

Таблица 5.44 – Команды режима глобального конфигурирования

Команда	Значение	Действие
port-channel load-balance {src-dst-mac-ip src-dst-mac src-dst-ip src-dst-mac-ip-port}	src-dst-mac	Задаёт механизм балансировки нагрузки для группы агрегированных портов. src-dst-mac-ip – Механизм балансировки основывается на MAC-адресе и IP-адресе; src-dst-mac – Механизм балансировки основывается на MAC-адресе; src-dst-ip – Механизм балансировки основывается на IP-адресе; src-dst-mac-ip-port – Механизм балансировки основывается на MAC-адресе, IP-адресе и порте назначения .

Вид запроса командной строки режима EXEC:

```
console>
```

Таблица 5.45 – Команды режима EXEC

Команда	Значение	Действие
show interfaces port-channel [group]	group [1..8]	Показывает информацию по группе каналов.

5.11.1 Статические группы агрегации каналов

Функцией статических групп LAG является объединение нескольких физических каналов в один, что позволяет увеличить пропускную способность канала и повысить его отказоустойчивость. Для статических групп приоритет использования каналов в объединенном пучке не задается.



Для включения работы интерфейса в составе статической группы используйте команду `channel-group {group} mode on` в режиме конфигурирования соответствующего интерфейса.

5.11.2 Протокол агрегации каналов LACP

Функцией протокола Link Aggregation Control Protocol (LACP) является объединение нескольких физических каналов в один. Агрегирование каналов используется для увеличения пропускной способности канала и повышения его отказоустойчивости. LACP позволяет передавать трафик по объединенным каналам в соответствии с заданными приоритетами.



Для включения работы интерфейса по протоколу LACP используйте команду `channel-group {group} mode auto` в режиме конфигурирования соответствующего интерфейса.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console (config) #
```

Таблица 5.46 – Команды режима глобального конфигурирования

<i>Команда</i>	<i>Значение/Значение по умолчанию</i>	<i>Действие</i>
<code>lACP system-priority value</code>	value: {1..65535/1}	Устанавливает приоритет системы.
<code>no lACP system-priority</code>		Устанавливает значение по умолчанию.

Команды режима конфигурирования интерфейса Ethernet

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet:

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

Таблица 5.47 – Команды режима конфигурирования интерфейса Ethernet

<i>Команда</i>	<i>Значение/Значение по умолчанию</i>	<i>Действие</i>
<code>lACP timeout {long short}</code>	По умолчанию используется значение long	Устанавливает административный таймаут протокола LACP: - long – длительное время таймаута; - short – малое время таймаута.
<code>no lACP timeout</code>		Устанавливает значение по умолчанию.
<code>lACP port-priority value</code>	value: {1..65535/1}	Устанавливает приоритет интерфейса Ethernet.
<code>no lACP port-priority</code>		Устанавливает значение по умолчанию.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.48 – Команды режима EXEC

<i>Команда</i>	<i>Значение/Значение по умолчанию</i>	<i>Действие</i>
<code>show lACP { gigabitEthernet gi_port fastEthernet fa_port } [parameters statistics protocol-state]</code>	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24};	Показывает информацию о протоколе LACP для интерфейса Ethernet. Если дополнительные параметры не используются, то будет показана вся информация. - parameters – показывает параметры настройки протокола; - statistics – показывает статистику работы протокола; - protocol-state – показывает состояние работы протокола.
<code>show lACP port-channel [group]</code>	group: [1..8]	Показывает информацию о протоколе LACP для группы портов.

Примеры выполнения команд

- Создать первую группу портов, работающую по протоколу LACP и включающую два интерфейса Ethernet – 3 и 4. Скорость работы группы – 1000 Мбит/с. Установить приоритет системы – 6, приоритеты 12 и 13 для портов 3 и 4 соответственно.

```

console# configure
console(config)# lacp system-priority 6
console(config)# interface port-channel 1
console(config-if)# speed 1000
console(config-if)# exit
console(config)# interface ethernet 1/0/3
console(config-if)# speed 1000
console(config-if)# channel-group 1 mode auto
console(config-if)# lacp port-priority 12
console(config-if)# exit
console(config)# interface ethernet 1/0/4
console(config-if)# speed 1000
console(config-if)# channel-group 1 mode auto
console(config-if)# lacp port-priority 13
console(config-if)# exit
console(config)#

```

5.12 Настройка IPv4-адресации

В данном разделе описаны команды для настройки статических параметров IP-адресации, таких как IP-адрес, маска подсети, шлюз по умолчанию. Настройка протоколов DNS и ARP описана в соответствующих разделах документации.

Команды режима конфигурирования интерфейса Ethernet, интерфейса группы портов, VLAN

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet, интерфейса группы портов, интерфейсов VLAN:

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

Таблица 5.49 – Команды режима конфигурирования интерфейса Ethernet

Команда	Значение	Действие
ip address <i>IP-addr mask [gateway]</i> prefix-length]	prefix-length:{8 .. 30}	Назначение физическому интерфейсу Ethernet IP-адреса, маски подсети, адреса шлюза по умолчанию
no ip address [<i>ip-address</i>]		Удаление IP-адреса на физическом интерфейсе Ethernet.
ip address dhcp	[1..20] символов	Получение IP-адреса для настраиваемого интерфейса от DHCP-сервера. Данная команда доступна только в режиме коммутатора (set system mode switch policy-based vlan active)
no ip address dhcp		Не получать для настраиваемого интерфейса IP-адрес от сервера DHCP.

Команды режима глобального конфигурирования

Вид запроса командной строки в режиме глобального конфигурирования:

```
console(config)#
```

Таблица 5.50 - Команды режима глобального конфигурирования

Команда	Значение	Действие
ip default-gateway <i>IP-address</i>	-/шлюз по умолчанию не задан	Задаёт для коммутатора шлюз по умолчанию. Данная команда доступна только в режиме коммутатора (set system mode switch policy-based vlan active)
no ip default-gateway		Удаляет для коммутатора шлюз по умолчанию.
ip helper-address [<i>ip-interface</i> <i>all</i>] <i>address</i> [<i>udp-port-list</i>]	-/disabled	Включить переадресацию UDP-пакетов широковещательной рассылки на определенный адрес. - ip-interface – IP-адрес; - all – все IP-интерфейсы; - address – IP-адрес назначения. Установленное значение 0.0.0.0 отключает переадресацию; - udp-port-list – номер порта UDP, на который направляются широковещательные пакеты.
no ip helper-address [<i>ip-interface</i> <i>all</i>] <i>address</i>		Устанавливает значение по умолчанию.

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 5.51 - Команды режима Privileged EXEC

Команда	Значение	Действие
clear host dhcp [<i>name</i> *]	{1..158} символов	Удаляет из памяти, полученные по протоколу DHCP записи соответствий имен интерфейсов и их IP-адресов (команда доступна только для привилегированного пользователя). * - удалить все соответствия. Данная команда доступна только в режиме коммутатора (set system mode switch policy-based vlan active)
renew dhcp [<i>gigabitethernet gi_port</i> <i>fastethernet fa_port</i> <i>port-channel group</i> <i>vlan vlanID</i>] [<i>force-autoconfig</i>]	<i>gi_port</i> : {1..8/0/1..28}; <i>fa_port</i> : {1..8/0/1..24}; <i>group</i> : {1..8}; <i>vlanID</i> {1..4094}	Отправляет запрос к DHCP-серверу на обновление IP-адреса. - force-autoconfig – при обновлении IP-адреса загружается конфигурация с TFTP-сервера. Данная команда доступна только в режиме коммутатора (set system mode switch policy-based vlan active)
show ip helper-address [<i>ip-interface</i>]	-	Отображает таблицу переадресации UDP-пакетов широковещательной рассылки.

Команды режима EXEC

Вид запроса командной строки в режиме Exec:

```
console>
```

Таблица 5.52 - Команды режима EXEC

Команда	Значение	Действие
show ip interface [<i>gigabitethernet gi_port</i> <i>fastethernet fa_port</i> <i>port-channel group</i> <i>vlan vlanID</i>]	<i>gi_port</i> : {1..8/0/1..28}; <i>fa_port</i> : {1..8/0/1..24}; <i>group</i> : {1..8}; <i>vlanID</i> {1..4094}	Показывает конфигурацию IP-адресации для указанного интерфейса.

Примеры выполнения команд

- Установить IP-адрес шлюза по умолчанию - 192.168.16.2:

```
console (config)# ip default-gateway 192.168.16.2
```

5.13 Настройка Green Ethernet

Green Ethernet – технология, позволяющая снизить энергопотребление устройства за счет отключения питания для неактивных электрических портов и изменения уровня передаваемого сигнала в зависимости от длины кабеля.

Команды режима глобального конфигурирования

Вид запроса командной строки в режиме глобального конфигурирования:

```
console (config) #
```

Таблица 5.53 - Команды режима глобального конфигурирования

<i>Команда</i>	<i>Значение</i>	<i>Действие</i>
green-ethernet energy-detect	-/Включен	Включает энергосберегающий режим для неактивных портов
no green-ethernet energy-detect		Отключает энергосберегающий режим для неактивных портов
green-ethernet short-reach	-/Включен	Включает энергосберегающий режим для портов, к которым подключаются устройства с длиной кабеля подключения меньше порогового значения, устанавливаемого с помощью команды green-ethernet short-reach threshold
no green-ethernet short-reach		Отключает энергосберегающий режим на основании длины кабеля
green-ethernet short-reach threshold value	value: {0..70/40} метров	Устанавливает пороговое значение для энергосберегающего режима short-reach.
no green-ethernet short-reach threshold		Возвращает настройки по умолчанию

Команды режима конфигурирования интерфейса

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet:

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

Таблица 5.54 – Команды режима конфигурирования интерфейса Ethernet

<i>Команда</i>	<i>Значение</i>	<i>Действие</i>
green-ethernet energy-detect	-/Включен	Включает энергосберегающий режим для интерфейса.
no green-ethernet energy-detect		Отключает энергосберегающий режим для интерфейса.
green-ethernet short-reach	-/Включен	Включает энергосберегающий режим на основании длины кабеля.
no green-ethernet short-reach		Отключает энергосберегающий режим на основании длины кабеля.
green-ethernet short-reach force	-/Отключен	Перманентно включает энергосберегающий режим для порта.

no green-ethernet short-reach force	Перманентно включает энергосберегающий режим для порта.
--	---

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 5.55 - Команды режима Privileged EXEC

Команда	Значение	Действие
show green-ethernet [gigabitethernet gi_port fastethernet fa_port]	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}	Отображает статистику green-ethernet.
green-ethernet power-meter reset	-	Сбрасывает счетчик измерителя мощности.

Примеры выполнения команд

- Отобразить статистику green-ethernet:

```
console# show green-ethernet
Energy-Detect mode: Enabled
Short-Reach mode: Enabled
Power Consumption: 83% (5.57W out of maximum 6.69W)
Cumulative Energy Saved: 0 [Watt*Hour]
Short-Reach cable length threshold: 10m
```

Port	Energy-Detect			Short-Reach			Reason	VCT Cable Length
	Admin	Oper	Reason	Admin	Force	Oper		
g1	on	off	LU	on	off	off	LL	< 50
g2	on	off	LU	on	off	off	LL	< 50
g3	on	off	LU	on	off	on		< 50
g4	on	on		on	off	off	LD	
g5	on	on		on	off	off	LD	
g6	on	on		on	off	off	LD	
g7	on	on		on	off	off	LD	
g8	on	on		on	off	off	LD	
g9	on	on		on	off	off	LD	
g10	on	off	LU	on	off	off	LL	50 - 80
g11	on	off	LU	on	off	on		< 50
g12	on	off	LU	on	off	on		< 50
g13	on	off	LU	on	off	on		< 50
g14	on	off	LU	on	off	on		< 50
g15	on	off	LU	on	off	off	LL	50 - 80
g16	on	on		on	off	off	LD	
g17	on	on		on	off	off	LD	
g18	on	on		on	off	off	LD	
g19	on	on		on	off	off	LD	
g20	on	on		on	off	off	LD	
g21	on	on		on	off	off	LD	
g22	on	off	LU	on	off	on		< 50
g23	on	off	LU	on	off	off	LL	50 - 80
g24	on	off	LU	on	off	off	LL	50 - 80
xg1	on	off	LT	on	off	off	LT	
xg2	on	off	LT	on	off	off	LT	
xg3	on	off	LT	on	off	off	LT	
xg4	on	off	LT	on	off	off	LT	

LU – интерфейс находится в состоянии UP.

LD – интерфейс находится в состоянии DOWN.

LL – длина кабеля, подключенного к интерфейсу превышает пороговое значение.

LT – интерфейс является оптическим

5.14 Настройка IPv6-адресации

5.14.1 Протокол IPv6

Коммутатор MES1024/MES1124/MES2124 поддерживает работу по протоколу IPv6. Поддержка IPv6 является важным достоинством, поскольку протокол IPv6 призван, в перспективе, полностью заменить адресацию протокола IPv4. По сравнению с IPv4 протокол IPv6 имеет расширенное адресное пространство – 128 бит вместо 32. Адрес IPv6 представляет собой 8 блоков, разделенных двоеточием, в каждом блоке 16 бит, записанных в виде четырех шестнадцатеричных чисел.

Помимо увеличения адресного пространства протокол IPv6 имеет иерархическую схему адресации, обеспечивает агрегацию маршрутов, упрощает таблицу маршрутизации, при этом эффективность работы маршрутизатора повышается за счет механизма обнаружения соседних узлов.

Локальные адреса IPv6 (IPv6Z) в коммутаторе назначаются интерфейсам, поэтому при использовании IPv6Z адресов в синтаксисе команд используется следующий формат:

```
<ipv6-link-local-address>%<interface-name>
```

где

interface-name – имя интерфейса:

interface-name = *vlan*<integer> | *ch*<integer> | <physical-port-name>

integer = <decimal-number> | <integer><decimal-number>

decimal-number = 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9

physical-port-name = **gigabitethernet** {1..8/0/1..24} | **fastethernet** {1..8/0/1..24}



Если значение группы или нескольких групп подряд в адресе протокола IPv6 равно нулю - 0000, то данные группы могут быть опущены. Например, адрес FE40:0000:0000:0000:0000:AD21:FE43 может быть сокращен до FE40::AD21:FE43. Сокращению не могут быть подвергнуты 2 разделенные нулевые группы из-за возникновения неоднозначности.



EUI-64 – это идентификатор, созданный на базе MAC-адреса интерфейса, являющийся 64 младшими битами IPv6-адреса. MAC-адрес разбивается на две части по 24 бита, между которыми добавляется константа FFFE.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.56 – Команды режима глобального конфигурирования

Команда	Значение	Действие
ipv6 default-gateway <i>ipv6-address</i>	-	Задаёт значение локального адреса IPv6-шлюза по умолчанию. Данная команда доступна только в режиме коммутатора (set system mode switch policy-based vlan active).
no ipv6 default-gateway		Удаляет настройки IPv6-шлюза по умолчанию

ipv6 host <i>name ipv6-address1 [ipv6-address2... ipv6-address4]</i>	name: 1..158 символов	Создает статическую запись, ставящую в соответствие сетевому имени устройства IPv6-адрес.
no ipv6 host <i>name</i>		Удаляет статическую запись соответствия IPv6-адреса и сетевого имени устройства.
ipv6 neighbor <i>ipv6_addr { gigabitethernet gi_port fastethernet fa_port port-channel group vlan vlanID } hw_addr</i>	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}; vlanID {1..4094}	Создает статическое соответствие между MAC-адресом соседнего устройства и его IPv6-адресом. <i>ipv6_addr</i> – IPv6-адрес; <i>hw_addr</i> – MAC-адрес;
no ipv6 neighbor		Удаляет статическое соответствие между MAC-адресом соседнего устройства и его IPv6-адресом.
ipv6 icmp error-interval <i>milliseconds [bucketsize]</i>	milliseconds: {0 .. 2147483647}/100 bucketsize: {1..200}/10	Задаёт ограничение скорости для ICMPv6 сообщений об ошибках.
no ipv6 icmp error-interval		Устанавливает значение по умолчанию.

Команды режима конфигурирования интерфейса (VLAN, Ethernet, Port-Channel)

Вид запроса командной строки режима конфигурирования интерфейса:

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

Таблица 5.57 – Команды режима конфигурирования интерфейса (Ethernet, VLAN, Port-channel)

Команда	Значение/Значение по умолчанию	Действие
ipv6 enable [no-autoconfig]	-	Включает поддержку IPv6 на интерфейсе.
no ipv6 enable		Отключает поддержку IPv6 на интерфейсе.
ipv6 address <i>ipv6-address/ prefix-length [eui-64] [anycast]</i>	prefix-length: 3..128 (64 если используется параметр eui-64)	Задаёт IPv6-адрес на интерфейсе. - <i>ipv6-address</i> – IPv6-сеть, назначенная интерфейсу (8 блоков разделенных двоеточием, в каждом блоке 16 бит, записанных в виде четырех шестнадцатеричных чисел); - <i>prefix-length</i> – длина префикса IPv6 – десятичное число – количество старших бит адреса составляющих префикс; - <i>eui-64</i> – идентификатор, созданный на базе MAC-адреса интерфейса, записывается в 64 младших бита IPv6 адреса; - <i>anycast</i> – указывает, что заданный адрес <i>anycast</i> -адрес.
no ipv6 address <i>[ipv6-address/ prefix-length] [eui-64]</i>		Удаляет IPv6-адрес с интерфейса.
ipv6 address autoconfig	По умолчанию автоматическая конфигурация включена, адреса не назначены.	Включение автоматической конфигурации IPv6-адресов на интерфейсе. Адреса настраиваются в зависимости от префиксов, которые получены в сообщениях «Router Advertisement».
no ipv6 address autoconfig		Устанавливает значение по умолчанию.
ipv6 address <i>ipv6-address/ prefix-length link-local</i>	По умолчанию значение локального адреса: FE80::EUI64	Задаёт локальный IPv6-адрес интерфейса. Старшие биты локальных IP-адресов в IPv6 – FE80::
no ipv6 address <i>[ipv6-address/prefix-length link-local]</i>		Удаляет локальный IPv6-адрес.
ipv6 nd dad attempts <i>attempts-number</i>	0..600/1	Задаёт количество сообщений-требований, передаваемых интерфейсом взаимодействующему устройству в случае обнаружения дубликации (коллизии) IPv6-адреса.
ipv6 unreachable	-	Включение ICMPv6 сообщений о недостижимости адресата при передаче пакетов на определенный интерфейс.
no ipv6 unreachable		Устанавливает значение по умолчанию.
ipv6 mld version {1 2}	{1,2}/2	Определение версии протокола MLD для интерфейса.
no ipv6 mld version		Устанавливает значение по умолчанию.

<code>ipv6 mld join-group group-address</code>	-	Задаёт MLD-сообщения для определенной группы. group-address – IPv6-адрес группы многоадресной рассылки.
<code>no ipv6 mld join-group group-address</code>	-	Отменяет отчетность и удаляет IP-адрес из группы многоадресной рассылки.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 5.58 – Команды режима Privileged EXEC

Команда	Значение/Значение по умолчанию	Действие
<code>ipv6 set mtu { gigabitethernet gi_port fastethernet fa_port port-channel group } { bytes default}</code>	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8} bytes: {1280 .. 65535} /1500	Задаёт значение MTU для IPv6 пакетов.
<code>show ipv6 neighbors {static dynamic} [ipv6-address ipv6-address] [mac-address mac-address] [gigabitethernet gi_port fastethernet fa_port port-channel group] [vlan vlanID]</code>	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}; vlanID {1..4094}	Показывает информацию о соседних IPv6 устройствах, содержащуюся в кэше. - static – показывает статические записи; - dynamic – показывает динамические записи.
<code>clear ipv6 neighbors</code>	-	Очищает кэш, содержащий информацию о соседних устройствах, работающих по протоколу IPv6. Информация о статических записях сохраняется.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.59 – Команды режима EXEC

Команда	Значение	Действие
<code>show ipv6 interface [gigabitethernet gi_port fastethernet fa_port port-channel group] [vlan vlanID]</code>	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}; vlanID {1..4094}	Показывает настройки протокола IPv6 для указанного интерфейса.
<code>show ipv6 route</code>	-	Показывает таблицу IPv6-маршрутов.
<code>show ipv6 icmp error-interval</code>	-	Показывает настройки ICMPv6 сообщений об ошибках.

Примеры выполнения команд

Показать динамические записи в таблице маршрутизации о соседних IPv6 устройствах.

```
console# show ipv6 neighbors dynamic
```

Interface	IPv6 address	HW address	State
VLAN 1	5629:78:13::6782:B588:1AB5	00:00:03:08:D8:98	REACH

Возможные состояния:

INCOMP (Incomplete) – Процедура разрешения адреса выполняется на входе. Это означает, что запрос о соседстве был отправлен на групповой адрес, но соответствующее подтверждение о соседстве еще не было получено.

REACH (Reachable) – Положительное подтверждение о том, что путь до соседнего устройства функционирует верно, было получено в течение периода «достижимости» (ReachableTime, мс). Пока соседнее устройство достижимо, и обмен пакетами идет нормально, никаких специальных действий не предпринимается.

STALE – Положительное подтверждение о том, что путь до соседнего устройства функционирует верно, было получено в течение времени большего, чем период «достижимости» (ReachableTime, мс). Пока соседнее устройство достижимо, и обмен пакетами идет нормально, никаких специальных действий не предпринимается.

DELAY – Положительное подтверждение о том, что путь до соседнего устройства функционирует верно, было получено в течение времени большего, чем период «достижимости» (ReachableTime, мс) и повторный запрос был передан в течение интервала времени отведенного на попытку (DELAY_FIRST_PROBE_TIME, сек). Если положительный ответ не придет в течение интервала времени, отведенного на попытку (DELAY_FIRST_PROBE_TIME, сек), то состояние пути до соседнего устройства изменится на PROBE.

PROBE – Запросы о соседстве периодически передаются с интервалом «ретрансляции» (RetransTimer, мс) до тех пор, пока не будет получено положительное подтверждение.

5.14.2 Туннелирование протокола IPv6 (ISATAP)

Функция туннелирования трафика IPv6 на базе протокола ISATAP (*Intra-Site Automatic Tunnel Addressing Protocol*) позволяет осуществлять передачу трафика IPv6 через сети с адресацией IPv4. Таким образом, узлы с адресацией IPv6, поддерживающие туннелирование ISATAP, могут сообщаться, инкапсулируя трафик в пакеты с заголовком IPv4.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console (config) #
```

Таблица 5.60 – Команды режима глобального конфигурирования

Команда	Значение/Значение по умолчанию	Действие
<code>interface tunnel number</code>	1	1. Создает интерфейс туннелирования. 2. Осуществляет вход в режим конфигурирования интерфейса туннелирования.
<code>tunnel isatap query-interval seconds</code>	10..3600/10 сек	Устанавливает период между DNS запросами, отправляемыми для автоматического определения IP-адреса маршрутизатора ISATAP.
<code>no tunnel isatap query-interval</code>		Устанавливает значение по умолчанию.
<code>tunnel isatap solicitation-interval seconds</code>	10..3600/10 сек	Устанавливает период передачи запросов, требующих подтверждения от маршрутизатора ISATAP (в случае отсутствия активного маршрутизатора).
<code>no tunnel isatap solicitation-interval</code>		Устанавливает значение по умолчанию
<code>tunnel isatap robustness number</code>	1..20/3	Задаёт количество DNS-query запросов и количество запросов, передаваемых маршрутизатору ISATAP в течение времени жизни установленного соединения. Периоды запросов определяется формулами:

		- для DNS: (время жизни принятое в ответе от сервера DNS)/(number+1); - для запросов к маршрутизатору ISATAP: (минимальное время жизни принятое в ответе от ISATAP маршрутизатора)/(number+1).
no tunnel isatap robustness		Устанавливает значение по умолчанию.

Команды режима туннелирования

Вид запроса командной строки режима туннелирования:

```
console# configure
console(config)# interface tunnel 1
console (config-tunnel)#
```

Таблица 5.61 – Команды режима туннелирования

Команда	Значение	Действие
tunnel mode ipv6ip isatap	По умолчанию туннелирование отключено	Включает поддержку туннелирования протокола IPv6 через IPv4 при помощи ISATAP. <input checked="" type="checkbox"/> Для одного и того же интерфейса (например Ethernet/VLAN) поддержка IPv6-адресации и туннелирования могут сосуществовать вместе. Выбор использования IPv6-адресации или туннелирования будет осуществлен на основании информации об IP-адресе назначения.
no tunnel mode ipv6ip isatap		Выключает поддержку туннелирования протокола IPv6.
tunnel isatap router <i>router_name</i>	По умолчанию, доменным именем является строка 'isatap'	Задаёт доменное имя для туннеля IPv6. Пользователи с адресацией IPv4 будут иметь возможность доступа к устройству (устройство туннелирования) при выполнении стандартной процедуры DNS.
no tunnel isatap router		Устанавливает значение по умолчанию
tunnel source { auto ip-address <i>ipv4-address</i> }	По умолчанию, IP-адрес не назначен.	Команда назначает локальный IP-адрес туннелю, который будет использоваться, в качестве адреса источника, при отправке пакетов. - auto – IP-адрес будет автоматически назначен системой.
no tunnel source		Удаляет локальный IP-адрес туннеля.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.62 – Команды режима EXEC

Команда	Действие
show ipv6 tunnel	Показывает информацию о настройках туннеля.

Примеры выполнения команд

Включить интерфейс туннелирования, назначить доменное имя туннеля – MES2124, установить локальный ip-адрес – 192.168.16.88.

```
console# configure
console(config)# interface tunnel 1
console(config-tunnel)# tunnel mode ipv6ip isatap
console(config-tunnel)# tunnel isatap router MES2124
console(config-tunnel)# tunnel source ip-address 192.168.16.88
```

5.15 Настройка протоколов

5.15.1 Настройка протокола DNS – системы доменных имен

Основной задачей протокола DNS является определение IP-адреса узла сети (хоста) по запросу, содержащему его доменное имя. База данных соответствий доменных имен узлов сети и соответствующих им IP-адресов ведется на DNS-серверах.

Команды режима глобального конфигурирования

Вид запроса командной строки в режиме глобального конфигурирования:

```
console(config)#
```

Таблица 5.63 - Команды режима глобального конфигурирования

Команда	Действие
ip domain lookup	Разрешает использование протокола DNS.
no ip domain lookup	Запрещает использование протокола DNS.
ip name-server {server1-ipv4-address server1-ipv6-address} [server-address2 ... server-address8]	Определяет IPv4/IPv6-адреса для доступных DNS-серверов. Можно определить IP-адреса для восьми серверов.
no ip name-server [server-address1 ... server-address8]	Удаляет IP-адрес DNS-сервера из списка доступных.
ip domain name name	Определяет доменное имя по умолчанию, которое будет использоваться программой, для дополнения неправильных доменных имен (доменных имен без точки). Для доменных имен без точки в конец имени будет добавляться точка и указанное в команде доменное имя. Имя должно содержать 1 до 158 символов.
no ip domain name	Удаляет доменное имя по умолчанию.
ip host name address1 [address2 ... address4]	Определяет статические соответствия имен узлов сети IP-адресам, добавляет установленное соответствие в кэш. Функция локального DNS. Имя должно содержать от 1 до 158 символов. Можно определить до четырех IP-адресов.
no ip host name	Удаляет статические соответствия имен узлов сети IP-адресам. Имя должно содержать от 1 до 158 символов.

Команды режима EXEC

Вид запроса командной строки в режиме EXEC:

```
console#
```

Таблица 5.64 - Команды режима EXEC

<i>Команда</i>	<i>Действие</i>
clear host {name *}	Удаляет запись соответствия имени узла сети IP-адресу кэша либо все записи (*). Имя должно содержать от 1 до 158 символов.
show hosts [name]	Отображает доменное имя по умолчанию, список DNS-серверов, статические и кэшированные соответствия имен узлов сети и IP-адресов. При использовании в команде имени узла сети, отображается соответствующий ему IP-адрес. Имя должно содержать от 1 до 158 символов.

Примеры использования команд

Использовать DNS-сервера по адресам 192.168.16.35 и 192.168.16.38, установить доменное имя по умолчанию - **mes**:

```
console# configure
console(config)# ip name-server 192.168.16.35 192.168.16.38
console(config)# ip domain-name eltex-sw-1
```

Установить статическое соответствие: узел сети с именем eltex.mes имеет IP-адрес 192.168.16.39:

```
console# configure
console(config)# ip host eltex.mes 192.168.16.39
```

5.15.2 Настройка протокола ARP

ARP (Address Resolution Protocol — протокол разрешения адресов) — протокол канального уровня, выполняющий функцию определения MAC-адреса, на основании содержащегося в запросе IP-адреса.

Команды режима глобального конфигурирования

Вид запроса командной строки в режиме глобального конфигурирования:

```
console(config)#
```

Таблица 5.65 - Команды режима глобального конфигурирования

<i>Команда</i>	<i>Значение/Значение по умолчанию</i>	<i>Действие</i>
arp <i>ip_addr hw_addr</i> [gigabitethernet gi_port fastethernet fa_port port-channel group vlan vlanID]	формат ip_addr: A.B.C.D; формат hw_addr: H.H.H H:H:H:H:H H-H-H-H-H-H; gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}; vlanID {1..4094}	Добавляет статическую запись соответствия IP и MAC-адресов в таблицу ARP для указанного в команде интерфейса. ip_addr – IP-адрес hw_addr – MAC-адрес
no arp <i>ip_addr [gigabitethernet gi_port fastethernet fa_port port-channel group vlan vlanID]</i>		Удаляет статическую запись соответствия IP и MAC-адресов из таблицы ARP для указанного в команде интерфейса.
arp timeout <i>sec</i>	1-40000000/ 60000 сек	Настраивает время жизни динамических записей в таблице ARP (сек).
no arp timeout		Устанавливает значение по умолчанию.

Команды режима privileged EXEC

Вид запроса командной строки в режиме privileged EXEC:

```
console#
```

Таблица 5.66 - Команды режима privileged EXEC

<i>Команда</i>	<i>Значение</i>	<i>Действие</i>
clear arp-cache	-	Удаляет все динамические записи из ARP таблицы. (Команда доступна только для привилегированного пользователя).
show arp [ip-address <i>ip-address</i> mac-address <i>mac-address</i> gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i>]	формат <i>ip-address</i> : A.B.C.D формат <i>mac-address</i> : H.H.H или H:H:H:H:H или H-H-H-H-H-H; gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}.	Показывает записи ARP-таблицы: все записи, фильтр по IP-адресу; фильтр по MAC-адресу; фильтр по интерфейсу. ip_address – IP-адрес; mac_address – MAC-адрес; gi_port – номер интерфейса Ethernet g1-g4; fa_port – номер интерфейса Ethernet XG1-XG4; group – группа каналов.
show arp configuration	-	Показывает глобальную конфигурацию ARP и конфигурацию ARP для интерфейсов.
ip arp proxy disable	-	Отключает режим проксирования ARP-запросов для коммутатора.
no ip arp proxy disable	-	Включает режим проксирования ARP-запросов для коммутатора.

Команды режима конфигурирование интерфейса

Вид запроса командной строки в режиме interface configuration:

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

Таблица 5.67 - Команды режима interface configuration

<i>Команда</i>	<i>Значение</i>	<i>Действие</i>
ip proxy-arp	-	Отключает режим проксирования ARP-запросов на настраиваемом интерфейсе.
no ip proxy-arp	-	Включает режим проксирования ARP-запросов на настраиваемом интерфейсе.
arp timeout sec	1-40000000	Настраивает время жизни динамических записей в таблице ARP (сек) для настраиваемого интерфейса.
no arp timeout	1-40000000	Устанавливает значение по умолчанию (устанавливается глобально).

Примеры использования команд

Добавить статическую запись в ARP-таблицу: IP-адрес 192.168.16.32, MAC-адрес 0:0:C:40:F:BC, установить время жизни динамических записей в ARP-таблице – 12000 секунд:

```
console# configure
console(config)# arp 192.168.16.32 00-00-0c-40-0f-bc gigabitethernet 1/0/2
console(config)# exit
console# arp timeout 12000
```

- Показать содержимое ARP таблицы:

```
console# show arp
```

VLAN	Interface	IP address	HW address	status
vlan 1	gi0/12	192.168.25.1	02:00:2a:00:04:95	dynamic

5.15.3 Настройка протокола GVRP

GARP VLAN Registration Protocol (GVRP) – протокол VLAN-регистрации. Протокол позволяет распространить по сети идентификаторы VLAN. Основной функцией протокола GVRP является обнаружение информации об отсутствующих в базе данных коммутатора VLAN-сетях при получении сообщений GVRP. Получив информацию об отсутствующих VLAN, коммутатор добавляет ее в свою базу данных.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console (config) #
```

Таблица 5.68 – Команды режима глобального конфигурирования

Команда	Значение/Значение по умолчанию	Действие
gvrp enable	-/выключен	Включает использование протокола GVRP коммутатором.
no gvrp enable		Выключает использование протокола GVRP коммутатором.

Команды режима конфигурирования интерфейса (диапазона интерфейсов) Ethernet, интерфейса группы портов



Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet, интерфейса группы портов:

```
console# configure
console (config) # interface {gigabitethernet gi_port | fastethernet
fa_port | port-channel group}
console (config-if) #
```

Таблица 5.69 – Команды режима конфигурирования интерфейса Ethernet, группы интерфейсов

Команда	Значение/Значение по умолчанию	Действие
gvrp enable	-/выключен	Включает использование протокола GVRP на настраиваемом интерфейсе.
no gvrp enable		Выключает использование протокола GVRP на настраиваемом интерфейсе.
garp timer { join leave leaveall } <i>timer_value</i>	10-2147483640 мс Значения по умолчанию: join: 200 мс; leave: 600 мс; leaveall: 10000 мс	Устанавливает значения таймеров протокола GARP (описание таймеров приведено в таблице 5.70). <i>timer_value</i> – значение таймера (должно быть кратно 10).
no garp timer		Установить значения по умолчанию.
gvrp vlan-creation-forbid	-/разрешено	Запрещает динамическое изменение или создание VLAN для настраиваемого интерфейса.
no gvrp vlan-creation-forbid		Разрешает динамическое изменение или создание VLAN для настраиваемого интерфейса.
gvrp registration-forbid	По умолчанию создание и регистрация VLAN на интерфейсе разрешена	Выполняет снятие регистрации для всех VLAN и не допускает создания или регистрации новых VLAN на данном интерфейсе.
no gvrp registration-forbid		Устанавливает значение по умолчанию.

Таблица 5.70 – Описание таймеров GARP

<i>Таймер GARP</i>	<i>Значение</i>
Join Timer	Определяет интервал передачи запросов на присоединение в группу VLAN (диапазон значений от 10 до 2147483640 миллисекунд, значение по умолчанию – 200 миллисекунд).
Leave Timer	Определяет интервал, который интерфейс будет ожидать перед выходом из группы VLAN (диапазон значений от 10 до 2147483640 миллисекунд, значение по умолчанию – 600 миллисекунд).  Значение Leave таймера должно быть больше или равно трем значениям Join таймера.
LeaveAll Timer	Определяет интервал, который интерфейс будет ожидать перед отправкой запроса LeaveAll на полное отключение от группы VLAN (диапазон значений от 10 до 2147483640 миллисекунд, значение по умолчанию – 10000 миллисекунд).  Значение LeaveAll таймера должно быть намного больше значения Leave таймера.



Значения GARP таймеров должно быть одинаковым для всех взаимодействующих устройств. Если значения таймеров будут отличаться, то коммутатор может некорректно работать по протоколу GVRP.



Взаимодействие нетегированного порта с тегированным может быть административно определено путем установки значения PVID на нетегированном порту.



Интерфейс, настроенный в режиме порта доступа (Access port), не может работать по протоколу GVRP, поскольку он всегда является членом только одной группы VLAN.

Команды режима privileged EXEC

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 5.71 – Команды режима privileged EXEC

<i>Команда</i>	<i>Значение</i>	<i>Действие</i>
clear gvrp statistics [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port- channel <i>group</i>]	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}.	Очищает накопленную статистику протокола GVRP.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Таблица 5.72 – Команды режима EXEC

<i>Команда</i>	<i>Значение</i>	<i>Действие</i>
show gvrp configuration [<i>gigabitethernet gi_port</i> <i>fastethernet fa_port</i> port-channel group]		Показывает конфигурацию протокола GVRP для указанного интерфейса, либо для всех интерфейсов.
show gvrp statistics [<i>gigabitethernet gi_port</i> <i>fastethernet fa_port</i> port-channel group]	<i>gi_port</i> : {1..8/0/1..28}; <i>fa_port</i> : {1..8/0/1..24}; <i>group</i> : {1..8}.	Показывает накопленную статистику по протоколу GVRP для указанного интерфейса, либо для всех интерфейсов.
show gvrp error-statistics [<i>gigabitethernet gi_port</i> <i>fastethernet fa_port</i> port-channel group]		Показывает статистику по ошибкам при работе протокола GVRP для указанного интерфейса, либо для всех интерфейсов.

5.15.4 Механизм обнаружения петель (*loopback-detection*)

Данный механизм позволяет устройству отслеживать закольцованные порты. Петля на порту обнаруживается путём отсылки коммутатором фрейма с адресом назначения, совпадающим с одним из MAC-адресов устройства.

Команды режима глобального конфигурирования

Вид запроса командной строки в режиме глобального конфигурирования:

```
console(config)#
```

Таблица 5.73 - Команды режима глобального конфигурирования

<i>Команда</i>	<i>Значение/Значение по умолчанию</i>	<i>Действие</i>
loopback-detection enable		Включает механизм обнаружения петель для коммутатора.
no loopback-detection enable	-/disabled	Восстанавливает значение по умолчанию.
loopback-detection interval seconds		Устанавливает интервал между loopback-фреймами. <i>seconds</i> – интервал времени между LBD фреймами.
no loopback-detection interval	30-60/30 секунд	Восстанавливает значение по умолчанию
loopback-detection mode {src-mac-addr base-mac-addr}	-	Устанавливает режим обнаружения петель: <i>src-mac-addr</i> – определяет, что MAC-адрес назначения – MAC-адрес интерфейса; <i>base-mac-addr</i> – определяет, что MAC-адрес назначения – MAC-адрес устройства.

Команды режима конфигурирования интерфейса (диапазона интерфейсов) Ethernet, интерфейса группы портов

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet, интерфейса группы портов:

```
console# configure
console(config)# interface {gigabitethernet gi_port | fastethernet fa_port | port-channel group}
console(config-if)#
```

Таблица 5.74 – Команды режима конфигурирования интерфейса Ethernet, группы интерфейсов

<i>Команда</i>	<i>Значение/Значение по умолчанию</i>	<i>Действие</i>
loopback-detection enable	-/disabled	Включает механизм обнаружения петель на порту
no loopback-detection enable		Восстанавливает значение по умолчанию

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.75 – Команды режима EXEC

<i>Команда</i>	<i>Значение</i>	<i>Действие</i>
show loopback-detection [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i>]	<i>gi_port</i> : {1..8/0/1..28}; <i>fa_port</i> : {1..8/0/1..24}; <i>group</i> : {1..8}.	Отображает состояние механизма loopback-detection. <i>gi_port</i> – номер интерфейса Ethernet g1-g4; <i>fa_port</i> – номер интерфейса Ethernet XG1-XG4; <i>group</i> – группа каналов.

5.15.5 Семейство протоколов STP (STP, RSTP, MSTP)

Основной задачей протокола STP (Spanning Tree Protocol) является приведение сети Ethernet с множественными связями к древовидной топологии, исключающей циклы пакетов. Коммутаторы обмениваются конфигурационными сообщениями, используя кадры специального формата, и выборочно включают и отключают передачу на порты.

Rapid (быстрый) STP (RSTP) является усовершенствованием протокола STP, характеризуется меньшим временем приведения сети к древовидной топологии и имеет более высокую устойчивость.

Протокол Multiple STP (MSTP) является наиболее современной реализацией STP, поддерживающей использование VLAN. MSTP предполагает конфигурирование необходимого количества экземпляров связующего дерева (spanning tree) вне зависимости от числа групп VLAN на коммутаторе. Каждый экземпляр может содержать несколько групп VLAN. Недостатком протокола MSTP является то, что на всех коммутаторах, взаимодействующих по MSTP, должны быть одинаково сконфигурированы группы VLAN.

5.15.5.1 Настройка протокола STP, RSTP

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.76 – Команды режима глобального конфигурирования

<i>Команда</i>	<i>Значение/Значение по умолчанию</i>	<i>Действие</i>
spanning-tree	-	Разрешает использование коммутатором протокола STP.
no spanning-tree		Запрещает использование коммутатором протокола STP.
spanning-tree mode {stp rstp mstp}	-/RSTP	Устанавливает режим работы протокола STP: <i>stp</i> – IEEE 802.1D Spanning Tree Protocol; <i>rstp</i> – IEEE 802.1W Rapid Spanning Tree Protocol; <i>mstp</i> – IEEE 802.1S Multiple Spanning Tree Protocol.
no spanning-tree mode		Устанавливает значение по умолчанию.

spanning-tree forward-time <i>seconds</i>	4..30/15 сек	Устанавливает интервал времени, затрачиваемый на прослушивание и изучение состояний перед переключением в состояние передачи.
no spanning-tree forward-time		Устанавливает значение по умолчанию.
spanning-tree hello-time <i>seconds</i>	1..10/2 сек	Устанавливает интервал времени между передачами широковещательных сообщений «Hello» к взаимодействующим коммутаторам.
no spanning-tree hello-time		Устанавливает значение по умолчанию.
spanning-tree loopback-guard	-	Разрешает защиту, выключающую любой интерфейс при приеме пакетов BPDU.
no spanning-tree loopback-guard		Запрещает защиту, выключающую интерфейс при приеме пакетов BPDU.
spanning-tree max-age <i>seconds</i>	6..40/20 сек	Устанавливает время жизни связующего дерева STP.
no spanning-tree max-age		Устанавливает значение по умолчанию.
spanning-tree priority	0..61440/32768	Настраивает приоритет связующего дерева STP.
no spanning-tree priority		<input checked="" type="checkbox"/> Значение приоритета должно быть кратно 4096. Устанавливает значение по умолчанию.
spanning-tree pathcost method {long short}	-/short	Устанавливает метод определения ценности пути. - long – значение ценности в диапазоне 1..200000000; - short – значение ценности в диапазоне 1..65535.
no spanning-tree pathcost method		Устанавливает значение по умолчанию.
spanning-tree bpdu {filtering flooding}	-/flooding	Определяет режим обработки пакетов BPDU интерфейсом, на котором выключен протокол STP. - <i>filtering</i> – на интерфейсе с выключенным протоколом STP BPDU пакеты фильтруются; - <i>flooding</i> – на интерфейсе с выключенным протоколом STP нетегированные BPDU пакеты передаются, тегированные – фильтруются.
no spanning-tree bpdu		Устанавливает значение по умолчанию.



При задании таких параметров STP, как **forward-time**, **hello-time**, **max-age** необходимо учитывать следующее справедливое неравенство-формулу:
 $2*(Forward-Delay - 1) \geq Max-Age \geq 2*(Hello-Time + 1)$.

Команды режима конфигурирования интерфейса Ethernet, интерфейса группы портов

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet, интерфейса группы портов:

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

Таблица 5.77 – Команды режима конфигурирования интерфейса Ethernet, группы портов

Команда	Значение/Значение по умолчанию	Действие
spanning-tree disable	-/разрешено	Запрещает работу протокола STP на конфигурируемом интерфейсе.
no spanning-tree disable		Разрешает работу протокола STP на конфигурируемом интерфейсе.
spanning-tree cost <i>cost</i>	1..200000000/ см. таблицу 5.78	Устанавливает ценность пути через выбранный интерфейс.
no spanning-tree cost		Устанавливает значение, определяемое на основании скорости порта и метода определения ценности пути, таблица 5.78.

spanning-tree port-priority	0..240/128	Устанавливает приоритет интерфейса в связующем дереве STP. Значение приоритета должно быть кратно 16.
no spanning-tree port-priority		Устанавливает значение по умолчанию.
spanning-tree portfast [auto]	-	Включает режим, в котором порт при поднятии на нем линка сразу становится в состояние передачи, не дожидаясь истечения таймера. - auto – добавляет задержку 3 секунды перед переходом в состояние передачи.
no spanning-tree portfast		Выключает режим моментального перехода в состояние передачи по поднятию линка.
spanning-tree guard root	-/защита выключена	Включает защиту «корня» для всех связующих деревьев STP выбранного порта. Данная защита запрещает интерфейсу быть корневым портом коммутатора.
no spanning-tree guard root		Устанавливает значение по умолчанию.
spanning-tree bpduguard	-/защита выключена	Разрешает защиту, выключающую интерфейс при приеме пакетов BPDU.
no spanning-tree bpduguard		Запрещает защиту, выключающую интерфейс при приеме пакетов BPDU.
spanning-tree link-type {point-to-point shared}	Значение по умолчанию для дуплексного порта «точка-точка», для полудуплексного – «разветвленный»	Устанавливает протокол RSTP в передающее состояние и определяет тип связи для выбранного порта - «точка-точка», «разветвленный».
no spanning-tree link-type		Устанавливает значение по умолчанию.
spanning-tree bpdud {filtering flooding}	-	Определяет режим обработки пакетов BPDU интерфейсом, на котором выключен протокол STP. - <i>filtering</i> – на интерфейсе с выключенным протоколом STP BPDU пакеты фильтруются; - <i>flooding</i> – на интерфейсе с выключенным протоколом STP нетегированные BPDU-пакеты передаются, тегированные – фильтруются.
no spanning-tree bpdud		Устанавливает значение по умолчанию.

Таблица 5.78 – Ценность пути, установленная по умолчанию (spanning-tree cost)

Интерфейс	Метод определения ценности пути	
	Long	Short
Port-channel	20000	4
TenGigabit Ethernet (10000 Mbps)	2000	2
Gigabit Ethernet (1000 Mbps)	20000	4

Команды режима privileged EXEC

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 5.79 – Команды режима privileged EXEC

Команда	Значение	Действие
show spanning-tree [gigabitethernet gi_port fastethernet fa_port port-channel group]	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}.	Показывает конфигурацию протокола STP.
show spanning-tree [detail] [active blockedports]	-	Показывает подробную информацию о настройке протокола STP, информацию об активных или заблокированных портах.

clear spanning-tree detected-protocols [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i>]	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}.	Перезапускает процесс миграции протокола. Заново происходит расчёт дерева STP.
--	--	--

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.80 – Команды режима EXEC

<i>Команда</i>	<i>Значение</i>	<i>Действие</i>
show spanning-tree bpdud [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i>]	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}.	Показывает режим обработки пакетов BPDU на интерфейсах.

5.15.5.2 Настройка протокола MSTP

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.81 – Команды режима глобального конфигурирования

<i>Команда</i>	<i>Значение/Значение по умолчанию</i>	<i>Действие</i>
spanning-tree	-	Разрешает использование коммутатором протокола STP.
no spanning-tree		Запрещает использование коммутатором протокола STP.
spanning-tree mode {stp rstp mstp}	-/RSTP	Устанавливает режим работы протокола STP.
no spanning-tree mode		Устанавливает значение по умолчанию.
spanning-tree pathcost method {long short}	-/short	Устанавливает метод определения ценности пути.
no spanning-tree pathcost method		- long – значение ценности в диапазоне 1..200000000; - short – значение ценности в диапазоне 1..65535. Устанавливает значение по умолчанию.
spanning-tree mst instance-id priority priority	instance: 1..15; priority: 0..61440/32768	Устанавливает приоритет для данного коммутатора перед остальными, использующими общий экземпляр MSTP.
no spanning-tree mst instance-id priority		<input checked="" type="checkbox"/> Значение приоритета должно быть кратно 4096. Устанавливает значение по умолчанию.
spanning-tree mst max-hops hop-count	1..40/20	Устанавливает максимальное количество транзитных участков для пакета BPDU, необходимых для формирования дерева и удержания информации о его строении. Если пакет уже прошел максимальное количество транзитных участков, то на следующем участке он отбрасывается.
no spanning-tree mst max-hops		Устанавливает значение по умолчанию.
spanning-tree mst configuration	-	Вход в режим конфигурирования протокола MSTP.

Команды режима конфигурирования протокола MSTP

Вид запроса командной строки в режиме конфигурирования протокола MSTP:

```
console# configure
console (config)# spanning-tree mst configuration
console (config-mst)#
```

Таблица 5.82 – Команды режима конфигурирования протокола MSTP

Команда	Значение/Значение по умолчанию	Действие
instance <i>instance-id</i> vlan <i>vlan-range</i>	instance: 1..15;	Создает соответствие между экземпляром протокола MSTP и группами VLAN.
no instance <i>instance-id</i> vlan <i>vlan-range</i>	vlan-range: 1..4094	Удаляет соответствие между экземпляром протокола MSTP и группами VLAN.
name <i>string</i>	1..32 символа	Задает имя конфигурации MST.
no name		Удаляет имя конфигурации MST.
revision <i>value</i>	0..65535/0	Задает номер ревизии конфигурации MST.
no revision		Устанавливает значение по умолчанию.
show { <i>current</i> <i>pending</i> }	-	Показывает текущую (<i>current</i>), либо ожидающую (<i>pending</i>) конфигурацию MST.
exit	-	Выход из режима конфигурации протокола MSTP с сохранением конфигурации.
abort	-	Выход из режима конфигурации протокола MSTP без сохранения конфигурации.

Команды режима конфигурирования интерфейса Ethernet, интерфейса группы портов

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet, интерфейса группы портов:

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

Таблица 5.83 – Команды режима конфигурирования интерфейса Ethernet, группы портов

Команда	Значение/Значение по умолчанию	Действие
spanning-tree guard root	-/защита выключена	Включает защиту «корня» для всех связующих деревьев STP выбранного порта. Данная защита запрещает интерфейсу быть корневым портом коммутатора.
no spanning-tree guard root		Устанавливает значение по умолчанию.
spanning-tree mst <i>instance-id port-priority</i> <i>priority</i>	instance: 1..15;	Устанавливает приоритет интерфейса в экземпляре MSTP. <input checked="" type="checkbox"/> Значение приоритета должно быть кратно 16.
no spanning-tree mst <i>instance-id port-priority</i>	priority: 0..240/128	Устанавливает значение по умолчанию.
spanning-tree mst <i>instance-id</i> cost <i>cost</i>	instance: 1..15;	Устанавливает ценность пути через выбранный интерфейс, для определенного экземпляра протокола MSTP.
no spanning-tree mst <i>instance-id</i> cost	cost: 1..200000000	Устанавливает значение, определяемое на основании скорости порта и метода определения ценности пути, таблица 5.78.
spanning-tree port-priority	0..240/128	Устанавливает приоритет интерфейса в корневом связующем дереве MSTP. <input checked="" type="checkbox"/> Значение приоритета должно быть кратно 16.
no spanning-tree port-priority		Устанавливает значение по умолчанию.

Команды режима privileged EXEC

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 5.84 – Команды режима EXEC

<i>Команда</i>	<i>Значение</i>	<i>Действие</i>
show spanning-tree [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i>] [instance <i>instance-id</i>]	<i>gi_port</i> : {1..8/0/1..28}; <i>fa_port</i> : {1..8/0/1..24}; <i>group</i> : {1..8}. <i>instance</i> : {1..15}	Показывает конфигурацию протокола STP. - <i>instance-id</i> – идентификатор экземпляра протокола MSTP.
show spanning-tree [detail] [active blockedports] [instance <i>instance-id</i>]	<i>instance</i> : {1..15}	Показывает подробную информацию о настройке протокола STP, информацию об активных или заблокированных портах. - <i>instance-id</i> – идентификатор экземпляра протокола MSTP.
show spanning-tree mst-configuration	-	Показывает информацию о сконфигурированных экземплярах MSTP
clear spanning-tree detected-protocols [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i>]	<i>gi_port</i> : {1..8/0/1..28}; <i>fa_port</i> : {1..8/0/1..24}; <i>group</i> : {1..8}.	Перезапускает процесс миграции протокола. Заново происходит просчёт дерева STP.

Примеры выполнения команд

Включить поддержку протокола STP, установить значение приоритета связующего дерева RSTP – 12899, интервал *forward-time* – 20 секунд, интервал времени между передачами широковещательных сообщений «Hello» - 5 секунд, время жизни связующего дерева – 38 секунд. Показать конфигурацию протокола STP:

```
console(config)# spanning-tree
console(config)# spanning-tree mode rstp
console(config)# spanning-tree priority 12288
console(config)# spanning-tree forward-time 20
console(config)# spanning-tree hello-time 5
console(config)# spanning-tree max-age 38
console(config)# exit
```

```
console# show spanning-tree
```

```
Spanning tree enabled mode RSTP
Default port cost method: long

  Root ID    Priority    12288
           Address    02:10:11:12:13:00
           This switch is the root
           Hello Time 5 sec Max Age 38 sec Forward Delay 20 sec

Number of topology changes 2 last change occurred 01:41:53 ago
Times: hold 1, topology change 58, notification 5
       hello 5, max age 38, forward delay 20

Interfaces
Name    State    Prio.Nbr    Cost    Sts    Role    PortFast    Type
-----
1/g1    enabled  128.1       2000000  DSBL   Dsbl    No          -
1/g2    enabled  128.2       200000   FRW    Desg    No          P2p (RSTP)
1/g3    enabled  128.3       2000000  DSBL   Dsbl    No          -
```

5.15.6 Протокол EAPS

Протокол EAPS (Ethernet Automatic Protection Switching) предназначен для повышения устойчивости и надежности сети передачи данных, имеющей кольцевую топологию, за счет снижения времени восстановления сети в случае аварии. Время восстановления не превышает 1 секунды, что существенно меньше времени перестройки сети при использовании протоколов семейства spanning tree.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console (config) #
```

Таблица 5.85 – Команды режима глобального конфигурирования

Команда	Значение/Значение по умолчанию	Действие
eaps	-	Разрешает работу протокола EAPS.
no eaps	-	Запрещает работу протокола EAPS.
eaps fail-timer seconds	(1..10)/3 сек	Задает время отсутствия тестовых пакетов, по истечении которого будет зафиксирована авария кольца.
no eaps fail-timer		Устанавливает значение таймера по умолчанию.
eaps hello-timer seconds	(1..10)/1 сек	Таймер периодичности отправки hello-пакетов.
no eaps hello-timer		Устанавливает значение таймера по умолчанию.
eaps domain domain-id	0..63	Создание EAPS-региона с идентификатором <i>domain-id</i> и переход в режим конфигурирования региона.
no eaps domain domain-id		Удаление EAPS-региона с идентификатором <i>domain-id</i> .

Команды режима конфигурирования домена

Вид запроса командной строки в режиме конфигурирования домена:

```
console (config-eaps-domain) #
```

Таблица 5.86 – Команды режима конфигурирования EAPS домена

Команда	Значение/Значение по умолчанию	Действие
control-vlan vlan-id	1..4093	Идентификатор VLAN, используемой для управления EAPS. Кроме того, следующий по порядку идентификатор VLAN используется для управления вторичными кольцами. Управляющая VLAN EAPS не должна использоваться для передачи любого иного трафика.
no control-vlan		Отмена назначения VLAN
ring ring-id	0..15	Создание кольца с идентификатором <i>ring-id</i> и переход в режим конфигурирования кольца.
no ring ring-id		Удаление кольца с идентификатором <i>ring-id</i> .
set ring ring-id {enable disable}	0..15	Разрешение или запрет работы кольца с идентификатором <i>ring-id</i> .

Команды режима конфигурирования кольца

Вид запроса командной строки в режиме конфигурирования:

```
console (config-eaps-domain-ring) #
```

Таблица 5.87 – Команды режима конфигурирования EAPS кольца

Команда	Значение/Значение по умолчанию	Действие
primary-port {gigabitethernet gi_port tengigabitethernet te_port}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4).	Выбор первичного порта коммутатора, включенного в кольцо.
secondary-port {gigabitethernet gi_port tengigabitethernet te_port}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4).	Выбор вторичного порта коммутатора, включенного в кольцо.
role {master transit} level level-id	level-id: 0..1	Выбор роли коммутатора в конфигурируемом домене и кольце.
role {edge sub-edge}	-	Возможные роли: - master – устройство является ведущим узлом; - transit – устройство является транзитным узлом; - edge – смежный узел, принадлежащий основному и вторичному кольцам; - sub-edge – вспомогательный смежный узел, принадлежащий основному и вторичному кольцам.

Команды режима EХЕС

Вид запроса командной строки режима EХЕС:

```
console#
```

Таблица 5.88 – Команды режима EХЕС

Команда	Значение	Действие
show eaps [domain domain-id [ring ring-id]]	domain-id: 0..63; ring-id: 1..15.	Запрос информации о состоянии доменов и колец EAPS.

5.15.7 Настройка протокола G.8032v2 (ERPS)

Протокол ERPS (*Ethernet Ring Protection Switching*) предназначен для повышения устойчивости и надежности сети передачи данных, имеющей кольцевую топологию, за счет снижения времени восстановления сети в случае аварии. Время восстановления не превышает 1 секунды, что существенно меньше времени перестройки сети при использовании протоколов семейства spanning tree.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.89 – Команды режима глобального конфигурирования

Команда	Значение/Значение по умолчанию	Действие
erps	-	Разрешает работу протокола ERPS.
no erps		Запрещает работу протокола ERPS.
erps vlan vlan-id	1..4094	Создание ERPS-кольца с идентификатором R-APS VLAN, по которой будет передаваться служебная информация и переход в режим конфигурирования кольца.
no erps vlan vlan-id		Удаление ERPS-кольца с идентификатором vlan-id.

Команды режима конфигурирования кольца

Вид запроса командной строки в режиме конфигурирования кольца:

```
console(config-erps) #
```

Таблица 5.90 – Команды режима конфигурирования ERPS кольца

Команда	Значение/Значение по умолчанию	Действие
protected vlan add <i>vlan-range</i>	vlan-range:(2..4094, all)	Добавляет диапазон VLAN в список защищенных VLAN.
protected vlan remove <i>vlan-range</i>	vlan-range:(2..4094, all)	Удаляет диапазон VLAN из списка защищенных VLAN.
port {west east} {fastethernet <i>fa_port</i> gigabitethernet <i>gi_port</i> }	<i>fa_port</i> : (1..8/0/1..24); <i>gi_port</i> : (1..8/0/1..28).	Выбор west(east) порта коммутатора, включенного в кольцо.
no port {west east}	-	Удаление west(east) порта коммутатора, включенного в кольцо.
rpl {west east} {owner neighbor}	-/no rpl	Выбор RPL порта коммутатора и его роли.
no rpl		Удаление RPL порта коммутатора.
level <i>level</i>	level: (0..7)/1	Настройка уровня R-APS сообщений. Необходимо для прохождения сообщений через CFM MEP.
no level		Установка значения по умолчанию.
ring enable	-	Включение функционирования кольца.
no ring enable		Выключение функционирования кольца.
version <i>version</i>	version: (1..2)/2	Выбор режима совместимости с другими версиями протокола G.8032.
no version		Установка значения по умолчанию.
revertive	-/revertive	Выбор режима работы кольца.
no revertive		Установка значения по умолчанию.
sub-ring vlan <i>vlan-id</i>	vlan-id:(1..4094)	Указание подкольца для данного кольца.
no sub-ring vlan		Удаление подкольца.
timer guard <i>value</i>	value:(10-2000) мс, кратное 10/500 мс	Установка таймера блокирующего устаревшие R-APS сообщения.
no timer guard		Установка значения по умолчанию.
timer holdoff <i>value</i>	value:(0-10000) мс, кратное 100 с точностью 5 мс/0 мс	Установка таймера задержки реакции коммутатора на изменившееся состояние. Вместо реакции на событие включается таймер, по истечении которого коммутатор рапортует о своем состоянии. Предназначен для уменьшения флуда пакетов при флапинге портов.
no timer holdoff		Установка значения по умолчанию.
timer wtr <i>value</i>	value:(1-12) мин/5 мин	Установка таймера, который запускается на RPL Owner коммутаторе в revertive режиме. Используется для предотвращения частых защитных переключений из-за сигналов о неисправностях.
no timer wtr		Установка значения по умолчанию.
switch forced {west east}	-/no	Форсирует запуск защитного переключения кольца, при этом блокируется указанный порт.
no switch forced		Отмена форсирования переключения кольца.
switch manual {west east}	-/no	Ручное блокирование указанного west(east) порта и разблокирование east(west).
no switch manual		Отмена ручной блокировки.
abort	-	Откатить изменения внесенные с момента входа в режим конфигурации кольца

Команды режима EXEC

Вид запроса командной строки режима EXEC:

console#

Таблица 5.91 – Команды режима EXEC

Команда	Значение	Действие
<code>show erps [vlan vlan-id]</code>	vlan-id: 1..4094	Запрос информации об общем состоянии erps или состоянии указанного кольца.

5.15.8 Настройка протокола LLDP

Основной функцией протокола **Link Layer Discovery Protocol (LLDP)** является обмен между сетевыми устройствами о своем состоянии и характеристиках. Информация, собранная посредством протокола LLDP, накапливается в устройствах и может быть запрошена управляющим компьютером по протоколу SNMP. Таким образом, на основании собранной информации, на управляющем компьютере может быть смоделирована топология сети.

Коммутатор MES1024/MES1124/MES2124 поддерживает передачу, как стандартных параметров, так и опциональных, таких как:

- имя устройства и его описание;
- имя порта и его описание;
- информация о MAC/PHU;
- и т.д.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

console(config)#

Таблица 5.92 – Команды режима глобального конфигурирования

Команда	Значение/Значение по умолчанию	Действие
<code>lldp run</code>	enabled	Разрешает коммутатору использование протокола LLDP.
<code>no lldp run</code>		Запрещает коммутатору использование протокола LLDP.
<code>lldp timer seconds</code>	5..32768/30 сек	Определяет, как часто устройство будет отправлять обновление информации LLDP.
<code>no lldp timer</code>		Устанавливает значение по умолчанию.
<code>lldp hold-multiplier number</code>	2..10/4	Задаёт величину времени для принимающего устройства, в течение которого нужно удерживать принимаемые пакеты LLDP перед их сбросом. Данная величина передается на принимаемую сторону в LLDP update пакетах (пакетах обновления), является кратностью для таймера LLDP (lldp timer). Таким образом, время жизни LLDP пакетов рассчитывается по формуле $TTL = \min(65535, LLDP-Timer * LLDP-HoldMultiplier)$
<code>no lldp hold-multiplier</code>		Устанавливает значение по умолчанию.
<code>lldp reinit seconds</code>	1..10/2 сек	Минимальное время, которое LLDP-порт будет ожидать перед повторной инициализацией LLDP.
<code>no lldp reinit</code>		Устанавливает значение по умолчанию.
<code>lldp tx-delay seconds</code>	1..8192/2 сек	Устанавливает задержку между последующими передачами пакетов LLDP, инициированными изменениями значений или статуса в локальных базах данных MIB LLDP.
<code>no lldp tx-delay</code>		<input checked="" type="checkbox"/> Рекомендуется, чтобы данная задержка была меньше, чем значение $0.25 * LLDP-Timer$. Устанавливает значение по умолчанию.

lldp lldpdu {filtering flooding}	<i>filtering</i>	Определяет режим обработки пакетов LLDP, когда протокол LLDP выключен на коммутаторе: - <i>filtering</i> – указывает, что LLDP-пакеты фильтруются, если протокол LLDP выключен на коммутаторе; - <i>flooding</i> – указывает, что LLDP-пакеты передаются, если протокол LLDP выключен на коммутаторе.
no lldp lldpdu		Устанавливает значение по умолчанию.
lldp med fast-start repeat-count number	1..10/3	Устанавливает число повторений PDU LLDP для быстрого запуска, определяемого посредством LLDP-MED.
no lldp med fast-start repeat-count		Устанавливает значение по умолчанию.
lldp med network-policy number application [vlan id] [vlan-type {tagged untagged}] [up priority] [dscp value]	<i>number: 1..32; application: voice, voice-signaling, guest-voice, guest-voice-signaling, softphone-voice, video-conferencing, streaming-video, video-signaling; id: 0..4095; priority: 0..7; value: 0..63.</i>	Определяет правило для параметра network-policy (сетевая политика устройства). Данный параметр является опциональным для расширения протокола LLDP MED. - <i>number</i> – порядковый номер правила network policy; - <i>application</i> – главная функция, определенная для данного правила network policy. Используемые имена: voice, voice-signaling, guest-voice, guest-voice-signaling, softphone-voice, video-conferencing, streaming-video, video-signaling. - <i>vlan id</i> – идентификатор VLAN для данного правила; - <i>tagged/ untagged</i> – определяет тегированной или нетегированной будет VLAN, используемая данным правилом. - <i>priority</i> – приоритет данного правила (используется на втором уровне модели OSI); - <i>dscp value</i> – значение DSCP, используемое данным правилом.
no lldp med network-policy number		Удаляет созданное правило для параметра network-policy.
lldp notifications interval seconds	5..3600/5	Устанавливает максимальную скорость передачи уведомлений LLDP. <i>seconds</i> – период времени, в течение которого устройство может отправить не более одного уведомления.
no lldp notifications interval		Устанавливает значение по умолчанию.

Команды режима конфигурирования интерфейсов Ethernet

Вид запроса командной строки в режиме конфигурирования интерфейсов Ethernet:

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

Таблица 5.93 – Команды режима конфигурирования интерфейса Ethernet

Команда	Значение/Значение по умолчанию	Действие
lldp transmit	По умолчанию разрешено использование в обоих направлениях.	Разрешает передачу пакетов по протоколу LLDP на интерфейсе.
no lldp transmit		Запрещает передачу пакетов по протоколу LLDP на интерфейсе.
lldp receive		Разрешает прием пакетов по протоколу LLDP на интерфейсе.
no lldp receive		Запрещает прием пакетов по протоколу LLDP на интерфейсе.
lldp optional-tlv tlv1 [tlv2.. tlv5]	port-desc, sys-name, sys-desc, sys-cap, 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size По умолчанию опциональные TLV не включены в пакет.	Определяет, какие опциональные TLV-поля (Type, Length, Value) будут включены устройством в передаваемый LLDP-пакет. В команду можно включить от одного до пяти опциональных TLV: port-desc, sys-name, sys-desc, sys-cap, 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size.
no lldp optional-tlv		Устанавливает значение по умолчанию.

lldp optional-tlv 802.1 {pvid ppvid {add remove} pppvid vlan-name {add remove} vid}	Ppvid: {0-4094}; Vlan: {1-4094};	Определяет, какие опциональные TLV-поля будут включены устройством в передаваемый LLDP-пакет: - PVID – PVID интерфейса; - PPVID – добавить/удалить PPVID; - VLAN-NAME – добавить/удалить номер VLAN; - PROTOCOL – добавить/удалить определенный протокол.
lldp optional-tlv 802.1 protocol {add remove} {stp rstp mstp pause 802.1x lacp gvrp}	По умолчанию опциональные TLV не включены.	
no lldp optional-tlv 802.1 pvid		Устанавливает значение по умолчанию.
lldp management-address {ip-address none automatic [gigabitethernet gi_port fastethernet fa_port port- channel group vlan id] }	формат ip-address: A.B.C.D gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}; id: {1 .. 4094} По умолчанию управляющий адрес определяется автоматически.	Определяет управляющий адрес, объявленный на интерфейсе. - ip-address – задается статический IP-адрес; - none – указывает, что адрес не объявлен; - automatic – указывает, что система автоматически выбирает управляющий адрес из всех IP-адресов коммутатора; - automatic {gigabitethernet fastethernet port-channel vlan} – указывает, что система автоматически выбирает управляющий адрес, из сконфигурированных адресов заданного интерфейса. Если интерфейс ethernet или интерфейс группы портов принадлежит VLAN, то данный адрес VLAN не будет включен в список возможных управляющих адресов.  В случае если несколько IP-адресов, то система выбирает начальный IP-адрес из диапазона динамических IP-адресов. Если динамические адреса отсутствуют, то система выбирает начальный IP-адрес из диапазона возможных статических IP-адресов.
no lldp management-address		Удаляет управляющий IP-адрес.
lldp notification {enable disable}	По умолчанию отправка уведомлений LLDP запрещена.	Разрешает/запрещает отставку уведомлений LLDP на интерфейсе. - Enable – разрешает; - Disable – запрещает.
no lldp notifications		Устанавливает значение по умолчанию.
lldp med enable [tlv1 ... tlv4]	network-policy, location, poe-pse, inventory По умолчанию запрещено использование расширения протокола LLDP MED.	Разрешает использование расширения протокола LLDP MED. В команду можно включить специальные TLV: network-policy, location, poe-pse, inventory.
no lldp med enable		Устанавливает значение по умолчанию.
lldp med network-policy {add remove} number	number: {1-32}	Назначает правило network-policy данному интерфейсу. - add – назначает правило; - remove – удаляет правило; - number – номер правила.
no lldp med network-policy number		Удаляет правило network-policy с данного интерфейса.
lldp med location {coordinate coordinate civic-address civic-address- data ecs-elin ecs-elin- data}	coordinate: 16 байт; civic address: 6..160 байт; ecs-elin: 10 – 25 байт.	Задает местоположение устройства для протокола LLDP (значение параметра location протокола LLDP MED). - coordinate – адрес в системе координат; - civic-address – административный адрес устройства; - ecs-elin – адрес в формате, определенном ANSI/TIA 1057.
no lldp med location		Удаляет настройки параметра местоположения location.
lldp med notification topology-change {enable disable}	-	Разрешает/запрещает отставку уведомлений LLDP MED об изменении топологии. Enable – разрешает отставку уведомлений; Disable – запрещает отставку уведомлений.

no lldp med notifications topology-change	Устанавливает значение по умолчанию.
---	--------------------------------------



LLDP-данные, принятые через группу агрегации каналов, запоминаются индивидуально портами группы, принявшими сообщения. LLDP шлет разрозненные сообщения на каждый порт группы.



Работа протокола LLDP не зависит от состояния протокола STP на порту, пакеты LLDP отправляются и принимаются на заблокированных протоколом STP портах.

Если порт контролируется по 802.1X, то LLDP работает с портом только в случае, если он авторизован.

Команды режима privileged EXEC

Все команды доступны для привилегированного пользователя. Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 5.94 – Команды режима privileged EXEC

<i>Команда</i>	<i>Значение/Значение по умолчанию</i>	<i>Действие</i>
clear lldp table	-	Очищает таблицу адресов обнаруженных соседних устройств и начинает новый цикл обмена пакетами по протоколу LLDP MED.
show lldp configuration [gigabitethernet gi_port fastethernet fa_port]	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}.	Показывает LLDP конфигурации всех физических интерфейсов устройства, либо заданных интерфейсов.
show lldp med configuration [gigabitethernet gi_port fastethernet fa_port]	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}.	Показывает конфигурации расширения протокола LLDP - MED для всех физических интерфейсов, либо заданных интерфейсов.
show lldp local {gigabitethernet gi_port fastethernet fa_port}	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}.	Показывает LLDP-информацию, которую анонсирует данный порт.
show lldp local tlvs- overloading [gigabitethernet gi_port fastethernet fa_port]	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}.	Показывает статус перезагрузки TLVs LLDP.
show lldp neighbors [gigabitethernet gi_port fastethernet fa_port]	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}.	Показывает информацию о соседних устройствах, на которых работает протокол LLDP.
show lldp statistics [gigabitethernet gi_port fastethernet fa_port]	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}.	Показывает статистику LLDP.

Примеры выполнения команд

Установить для порта 1/g1 следующие tlv-поля: port-description, sytem-name, system-description.
Для данного интерфейса добавить управляющий адрес 192.168.17.55

```
console(config)# configure
console(config-if)# lldp optional-tlv port-desc sys-name sys-desc
console(config-if)# lldp management-address 192.168.17.55
```

Посмотреть конфигурацию lldp:

```
console# show lldp configuration
```

```
LLDP state: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
```

Port	State	Optional TLVs	Address
1/g1	Rx and Tx	PD, SN, SD	192.168.16.55
1/g2	Rx and Tx		
1/g3	Rx and Tx		
1/g4	Rx and Tx		
1/g5	Rx and Tx		
1/g6	Rx and Tx		
1/g7	Rx and Tx		
1/g8	Rx and Tx		
1/g9	Rx and Tx		
1/g10	Rx and Tx		
1/g11	Rx and Tx		
1/g12	Rx and Tx		
1/g13	Rx and Tx		
1/g14	Rx and Tx		
1/g15	Rx and Tx		
1/g16	Rx and Tx		
1/g17	Rx and Tx		
1/g18	Rx and Tx		
1/g19	Rx and Tx		
1/g20	Rx and Tx		
1/g21	Rx and Tx		
1/g22	Rx and Tx		

More: <space>, Quit: q, One line: <return>

Таблица 5.95 - Описание результатов

Поле	Описание
Timer	Определяет, как часто устройство шлет LLDP-обновления.
Hold multiplier	Определяет величину времени для принимающего устройства, в течение которого нужно удерживать принимаемые пакеты LLDP перед их сбросом.
Reinit delay	Определяет минимальное время, в течение которого порт будет ожидать перед посылкой следующего LLDP-сообщения.
Tx delay	Определяет задержку между последующими передачами LLDP-фреймов, инициированных изменениями значений либо статуса.
Port	Номер порта.
State	Режим работы порта для протокола LLDP.
Optional TLVs	TLV-опции, которые передаются Возможные значения: PD – Описание порта; SN – Системное имя; SD – Описание системы; SC – Возможности системы.
Address	Адрес устройства, который передается в LLDP-сообщениях.
Notifications	Указывает, разрешены или запрещены уведомления LLDP.

Показать информацию о соседних устройствах

```
console# show lldp neighbors
```

Port	Device ID	Port ID	System Name	Capabilities
-----	-----	-----	-----	-----

g1	0060.704C.73FE	1	ts-7800-2	B
g2	0060.704C.73FD	1	ts-7800-2	B
g3	0060.704C.73FC	9	ts-7900-1	B, R
g4	0060.704C.73FB	1	ts-7900-2	W

```
console# show lldp neighbors ethernet g1
```

<pre>Device ID: 02:10:11:12:13:00 Port ID: g23 Capabilities: B System Name: sandbox2 System description: 24-port 10/100/1000 Ethernet Switch Port description: Ethernet Interface 802.3 MAC/PHY Configuration/Status Auto-negotiation support: Supported Auto-negotiation status: Enabled Auto-negotiation Advertised Capabilities: 1000BASE-T full duplex, 100BASE-TX full duplex mode, 100BASE-TX half duplex mode, 10BASE-T full duplex mode, 10BASE-T half duplex mode Operational MAU type: Unknown</pre>

Таблица 5.96 - Описание результатов

<i>Поле</i>	<i>Описание</i>
Port	Номер порта.
Device ID	Имя или MAC-адрес соседнего устройства.
Port ID	Идентификатор порта соседнего устройства.
System name	Системное имя устройства.
Capabilities	Данное поле описывает тип устройства: B – Мост (Bridge); R – Маршрутизатор (Router); W – Точка доступа WI-FI (WLAN Access Point); T – Телефон (Telephone); D – DOCSIS-устройство (DOCSIS cable device); H – Сетевое устройство (Host); r – Повторитель (Repeater); O – Тип неизвестен (Other).
System description	Описание соседнего устройства.
Port description	Описание порта соседнего устройства.
Management address	Адрес управления устройством.
Auto-negotiation support	Определяет, поддерживается ли автоматическое определение режима порта.
Auto-negotiation status	Определяет, включена ли поддержка автоматического определения режима порта.
Auto-negotiation Advertised Capabilities	Определяет режимы, поддерживаемые функцией автоматического определения порта.
Operational MAU type	Рабочий MAU-тип устройства.

5.15.9 Настройка протокола OAM

Ethernet OAM (Operation, Administration, and Maintenance), IEEE 802.3 ah – функции уровня канала передачи данных представляют собой протокол мониторинга состояния канала. В этом протоколе для передачи информации о состоянии канала между непосредственно подключенными устройствами Ethernet используются блоки данных протокола OAM (OAMPDU). Оба устройства должны поддерживать стандарт IEEE 802.3ah.

Команды режима конфигурирования интерфейсов Ethernet

Вид запроса командной строки в режиме конфигурирования интерфейсов Ethernet:

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

Таблица 5.97 – Команды режима конфигурирования интерфейса Ethernet

Команда	Значение/Значение по умолчанию	Действие
ethernet oam	-/отключено	Включить поддержку Ethernet OAM на порту.
no ethernet oam		Отключить Ethernet OAM на конфигурируемом порту.
ethernet oam link-monitor frame threshold count	1..65535/1	Устанавливает порог количества ошибок за указанный период (период устанавливается командой ethernet oam link-monitor frame window).
no ethernet oam link-monitor frame threshold		Восстанавливает значение по умолчанию.
ethernet oam link-monitor frame window window	10..600/100 мс	Устанавливает временной промежуток для подсчета количества ошибок.
no ethernet oam link-monitor frame window		Восстанавливает значение по умолчанию.
ethernet oam link-monitor frame-period threshold count	1..65535/1	Устанавливает порог для события «frame-period» (период устанавливается командой ethernet oam link-monitor frame-period window).
no ethernet oam link-monitor frame-period threshold		Восстанавливает значение по умолчанию.
ethernet oam link-monitor frame-period window window	1..65535/10000	Устанавливает временной промежуток для события «frame-period» (в фреймах).
no ethernet oam link-monitor frame-period window		Восстанавливает значение по умолчанию.
ethernet oam link-monitor frame-seconds threshold count	1..900/1	Устанавливает порог для события «frame-period» (период устанавливается командой ethernet oam link-monitor frame-seconds window), в секундах.
no ethernet oam link-monitor frame-seconds threshold		Восстанавливает значение по умолчанию.
ethernet oam link-monitor frame-seconds window window	100..9000/100 мс	Устанавливает временной промежуток для события «frame-period».
no ethernet oam link-monitor frame-seconds window		Восстанавливает значение по умолчанию.
ethernet oam mode <active passive>	-/active	Устанавливает режим работы протокола OAM: - Active – коммутатор постоянно отправляет OAMPDU; - Passive – коммутатор начинает отправлять OAMPDU только при наличии OAMPDU со встречной стороны.
no ethernet oam mode		Восстанавливает значение по умолчанию.
ethernet-oam remote-failure	-/включено	Включает поддержку и обработку событий «remote-failure».
no ethernet oam remote-failure		Восстанавливает значение по умолчанию.

ethernet oam remote-loopback supported	-/отключено	Включает поддержку функции заворота трафика.
no ethernet oam remote-loopback supported		Восстанавливает значение по умолчанию.
ethernet oam uni-directional detection	-/отключено	Включает функцию обнаружения однонаправленных связей на базе протокола Ethernet OAM.
no ethernet oam uni-directional detection		Восстанавливает значение по умолчанию.
ethernet oam uni-directional detection action <log error-disable>	-/log	Определяет реакцию коммутатора на однонаправленную связь: - log – отправка SNMP trap и запись в журнал; - error-disable – перевод порта в состояние «error-disable», запись в журнал и отправка SNMP trap.
no ethernet oam uni-directional detection action		Восстанавливает значение по умолчанию.
ethernet oam uni-directional detection aggressive	-/отключено	Включает агрессивный режим определения однонаправленной связи. Если от соседнего устройства перестают приходить Ethernet OAM-сообщения – линк помечается как однонаправленный.
no ethernet oam uni-directional detection aggressive		Восстанавливает значение по умолчанию.
ethernet oam uni-directional detection discovery time time	5..300/5 сек	Устанавливает временной интервал для определения типа связи на порту.
no ethernet oam uni-directional detection discovery-time		Восстанавливает значение по умолчанию.

Команды режима privileged EXEC

Все команды доступны для привилегированного пользователя.

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 5.98 – Команды режима privileged EXEC

Команда	Значение/Значение по умолчанию	Действие
clear ethernet oam statistics [interface {gigabitethernet gi_port tengigabitethernet te_port}]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4).	Очищает статистику Ethernet OAM для указанного интерфейса.
show ethernet oam discovery [interface {gigabitethernet gi_port tengigabitethernet te_port}]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4).	Отображает состояние протокола Ethernet OAM для указанного интерфейса.
show ethernet oam statistics [interface {gigabitethernet gi_port tengigabitethernet te_port}]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4).	Отображает статистику обмена протокольными сообщениями для указанного интерфейса.
show ethernet oam status [interface {gigabitethernet gi_port tengigabitethernet te_port}]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4).	Отображает настройки Ethernet OAM для указанного интерфейса.
show ethernet oam uni-directional detection [interface {gigabitethernet	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4).	Отображает состояние механизма определения однонаправленных связей для указанного интерфейса.

<code>gi_port tengigabitethernet te_port}]</code>		
--	--	--

Примеры выполнения команд

Отобразить состояние протокола для порта gigabitethernet 1/0/3:

```
console#show ethernet oam discovery interface GigabitEthernet 0/3
gigabitethernet 1/0/3
Local client
-----
Administrative configurations:
Mode:                active
Unidirection:        not supported
Link monitor:         supported
Remote loopback:      supported
MIB retrieval:        not supported
Mtu size:             1500
Operational status:
Port status:          operational
Loopback status:      no loopback
PDU revision:         3

Remote client
-----
MAC address: a8:f9:4b:0c:00:03
Vendor(oui): a8 f9 4b
Administrative configurations:
PDU revision:         3
Mode:                active
Unidirection:        not supported
Link monitor:         supported
Remote loopback:      supported
MIB retrieval:        not supported
Mtu size:             1500
console#
```

5.15.10 Настройка протокола CFM

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

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.99 – Команды режима глобального конфигурирования

Команда	Значение/Значение по умолчанию	Действие
ethernet cfm domain name [level level]	name: (1..32) символов level: (0..7)/0	Создание (или смена уровня) CFM домена (MD) с именем «name» и переход в режим конфигурирования домена. - level – уровень CFM домена.
no ethernet cfm domain name		Удаление CFM домена (MD) с именем «name».

Команды режима конфигурирования домена

Вид запроса командной строки в режиме конфигурирования домена:

```
console(config-cfm-md) #
```

Таблица 5.100 – Команды режима конфигурирования CFM домена (MD)

Команда	Значение/Значение по умолчанию	Действие
<code>id { dns dns name name id mac mac-address number id null }</code>	name: (1..43) символов dns: (1..43) символов mac-address: Н.Н.Н или Н:Н:Н:Н:Н:Н или Н-Н-Н-Н-Н-Н number: (0-65535) По умолчанию: id name соответствует имени домена	Указание идентификатора CFM домена (MD). Именем домена может быть: <ul style="list-style-type: none"> – dns – dns-имя; – name – текстовая строка; – mac-address number – MAC-адрес и числовой идентификатор домена; – null – NULL идентификатор.
<code>no id</code>		Установка значения по умолчанию.
<code>service port { vlan-id vlan-id name name number number }</code>	vlan: (1..4094) vlan-id: (1..4094) name: (1..45) символов number: (0..65535)	Создание CFM-сервиса (MA) без привязки к VLAN и переход в режим конфигурирования сервиса.
<code>no service port</code>		Удаление CFM-сервиса (MA).
<code>service vlan vlan { vlan-id vlan-id name name number number }</code>		Создание CFM-сервиса (MA) привязанного к VLAN с номером «vlan» и переход в режим конфигурирования сервиса. Именем сервиса может быть: <ul style="list-style-type: none"> – vlan-id – номер VLAN; – name – текстовая строка; – number – числовой идентификатор.
<code>no service vlan vlan }</code>		Удаление CFM-сервиса (MA) привязанного к VLAN с номером «vlan».
<code>mip auto-create [lower-mer-only]</code>	-/автоматическое создание отключено	Включение автоматического создания промежуточных точек сервиса (MIP). Промежуточные точки сервиса (MIP) создаются на всех портах, на которых прописан VLAN сервиса. Необязательный параметр «lower-mer-only» исключает из списка порты, на которых уже создана конечная точка сервиса.
<code>no mip auto-create</code>		Устанавливает значение по умолчанию.

Команды режима конфигурирования сервиса

Вид запроса командной строки в режиме конфигурирования домена:

```
console(config-cfm-ma) #
```

Таблица 5.101 – Команды режима конфигурирования CFM сервиса (MA)

Команда	Значение/Значение по умолчанию	Действие
<code>continuity-check interval interval</code>	interval: (1, 10, 100, 600) секунд/1 секунда	Установка интервала отправки Continuity Check сообщений.
<code>no continuity-check interval</code>		Установка значения по умолчанию
<code>direction down</code>	-	Устанавливает направление конечной точки сервиса (MEP) в нисходящее.
<code>no direction down</code>		Устанавливает направление конечной точки сервиса (MEP) в восходящее.
<code>mer id</code>	id: (1..8191)	Добавление конечной точки сервиса (MEP) с идентификатором «id» к данному сервису. Данной командой осуществляется только привязка MEP к сервису. MEP создается в режиме конфигурирования интерфейса.
<code>no mer id</code>		Удаление конечной точки сервиса (MEP).

mip auto-create [{ lower-mep-only none }]	<p>-/По умолчанию используется режим, сконфигурированный для домена, в котором находится сервис</p>	<p>Включение автоматического создания промежуточных точек сервиса (MIP). Промежуточные точки сервиса (MIP) создаются на всех портах, на которых прописан VLAN сервиса. Необязательные параметры:</p> <ul style="list-style-type: none"> - lower-mep-only – исключает из списка порты, на которых уже создана конечная точка сервиса (MEP); - none – не создавать автоматически промежуточные точки сервиса (MIP).
no mip auto-create		<p>Установка значения по умолчанию.</p>

Команды режима конфигурирования интерфейса Ethernet

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet, интерфейса группы портов:

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

Таблица 5.102 – Команды режима конфигурирования интерфейса Ethernet

Команда	Значение/Значение по умолчанию	Действие
ethernet cfm mep id domain domain-name service { vlan-id vlan-id name name number number }	<p>id: (1..8191) domain-name: (0..32) символов vlan-id: (1..4094) name: (0..45) символов number: (0..65535)</p>	<p>Создание на интерфейсе конечной точки сервиса (MEP) с идентификатором «id» для указанного сервиса в указанном домене и переход в режим конфигурирования MEP.</p>
no ethernet cfm mep id domain domain-name service { vlan-id vlan-id name name number number }		<p>Удаление конечной точки сервиса (MEP) с интерфейса.</p>

Команды режима конфигурирования конечной точки сервиса

Вид запроса командной строки в режиме конфигурирования домена:

```
console(config-if-cfm-mep) #
```

Таблица 5.103 – Команды режима конфигурирования CFM конечной точки (MEP)

Команда	Значение/Значение по умолчанию	Действие
active	-/Выключена	Включение конечной точки сервиса (MEP).
no active		Установка значения по умолчанию.
continuity-check enable	-/Выключена	Включение отправки Continuity Check сообщений.
no continuity-check enable		Установка значения по умолчанию.
cos cos	cos: (0..7)/7	Установка значения приоритета CoS, с которым будут отправляться Continuity Check сообщения.
no cos		Установка значения по умолчанию.
alarm delay delay	delay: (2500..10000) мс/2500 мс	Указание интервала задержки, по истечении которого будет генерироваться авария.
no alarm delay		Установка значения по умолчанию.
alarm reset interval	interval: (2500..10000) мс/10000 мс	Указание промежутка времени, по истечении которого произойдет сброс аварии.
no alarm reset		Установка значения по умолчанию.
alarm notification { all error-xcon remote-error-xcon mac-remote-error-xcon xcon none }	-/mac-remote-error-xcon	<p>Включение уведомлений для определенных типов событий.</p> <p>Типы событий:</p> <ul style="list-style-type: none"> - all – все события DefRDI, DefMACStatus, DefRemote, DefError, DefXcon;

		- error-xcon – только события DefError и DefXcon; - remote-error-xcon – только события DefRemote, DefError и DefXcon; - mac-remote-error-xcon - только события DefMACStatus, DefRemote, DefError и DefXcon; - xcon – только событие DefXcon; - none – уведомления отключены.
no alarm notification		Установка значения по умолчанию.

Команды режима privileged EXEC

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 5.104 – Команды режима privileged EXEC

Команда	Значение/Значение по умолчанию	Действие
show ethernet cfm domain [name]	name: (1..32) символов	Отображает информацию об указанном домене или обо всех.
show ethernet cfm errors	-	Отображает информацию об ошибках Continuity Check протокола.
show ethernet cfm maintenance-points { local remote }	-	Отображает информацию о локальных или удаленных конечных точках сервиса (MEP).
show ethernet cfm mpdb [domain-id { dns name name name name mac mac-address number null}]	name: (1..43) символов mac-address: H.H.H или H:H:H:H:H:H или H-H-H-H-H-H number: (0-65535)	Отображает информацию о промежуточных точках сервиса (MIP) для указанного домена или для всех.
show ethernet cfm statistics	-	Отображает CFM-статистику для всех доменов.
show ethernet cfm statistics domain domain-name service { vlan-id vlan-id name name number number }	domain-name: (0..32) символов vlan-id: (1..4094) name: (0..45) символов number: (0..65535)	Отображает CFM-статистику для указанного домена.
show ethernet cfm statistics mpid id	id: (1..8191)	Отображает CFM-статистику для указанной конечной точки сервиса (MEP).

5.16 Voice VLAN

Voice VLAN используется для выделения VoIP-оборудования в отдельную VLAN. Для VoIP-фреймов могут быть назначены QoS-атрибуты для приоритезации трафика. Классификация фреймов, относящихся к фреймам VoIP-оборудования, базируется на OUI (Organizationally Unique Identifier – первые 24 бита MAC-адреса) отправителя. Назначение Voice VLAN для порта происходит автоматически - когда на порт поступает фрейм с OUI из таблицы Voice VLAN. Когда порт определяется, как принадлежащий Voice VLAN – данный порт добавляется во VLAN как tagged. Voice VLAN применим для следующих схем:

- VoIP-оборудование настраивается, чтобы рассылать тегируемые пакеты, с ID Voice VLAN, настроенным на MES2124.
- VoIP-оборудование рассылает нетегируемые DHCP-запросы. В ответе от DHCP-сервера присутствует опция 132 (VLAN ID) с ID Voice VLAN, с помощью которой устройство автоматически назначает себе VLAN для маркировки трафика.

Список OUI производителей VoIP-оборудования, доминирующих на рынке.

OUI	Фирма-производитель
00:E0:BB	ЗСОМ
00:03:6B	Cisco
00:E0:75	Veritel
00:D0:1E	Pingtel
00:01:E3	Siemens
00:60:B9	NEC/ Philips
00:0F:E2	Huawei-ЗСОМ
00:09:6E	Avaya



Voice VLAN может быть активирован на портах, работающих в режиме trunk и general.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console (config) #
```

Таблица 5.105 – Команды режима глобального конфигурирования

Команда	Значение/Значение по умолчанию	Действие
voice vlan aging-timeout <i>timeout</i>	timeout: {1..43200/1440}	Устанавливает таймаут для порта, принадлежащего к voice-vlan. Если с порта в течение заданного времени не было фреймов с OUI VoIP-оборудования, то voice vlan удаляется с данного порта.
no voice vlan aging-timeout		Восстанавливает значение по умолчанию.
voice vlan cos <i>cos</i> [<i>remark</i>]	0-7/6	Устанавливает COS, которым маркируются фреймы, принадлежащие Voice VLAN.
no voice vlan cos		Восстанавливает значение по умолчанию.
voice vlan id <i>id</i>	Id: 2 .. 4094	Устанавливает идентификатор VLAN для Voice VLAN
no voice vlan id		Удаляет идентификатор VLAN для Voice VLAN Для удаления идентификатора VLAN требуется предварительно отключить функцию voice vlan на всех портах.
voice vlan oui-table { <i>add oui</i> <i>remove oui</i> } [<i>word</i>]	oui: первые 3 байта MAC-адреса word: 1..32 символов	Позволяет редактировать таблицу OUI. - word – описание oui.
no voice vlan oui-table		Удаляет все пользовательские изменения OUI-таблицы.

Команды режима конфигурирования интерфейса Ethernet

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet, интерфейса группы портов:

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

Таблица 5.106 – Команды режима конфигурирования интерфейса Ethernet

<i>Команда</i>	<i>Значение/Значение по умолчанию</i>	<i>Действие</i>
<code>voice vlan enable</code>	Отключена	Включает Voice VLAN для порта.
<code>no voice vlan enable</code>		Отключает Voice VLAN для порта.
<code>voice vlan cos mode {src all}</code>	-	Включает маркировку трафика для всех фреймов, либо только для источника.
<code>no voice vlan cos mode</code>		Восстанавливает значение по умолчанию.
<code>voice vlan secure</code>	Отключен	Включает безопасный режим для VLAN. Команда применяется только к портам, которые были добавлены к Voice VLAN автоматически.
<code>no voice vlan secure</code>		Восстанавливает значение по умолчанию.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.107 – Команды режима конфигурирования EXEC

<i>Команда</i>	<i>Значение/Значение по умолчанию</i>	<i>Действие</i>
<code>show voice vlan [gigabitethernet gi_port fastethernet fa_port port-channel group]</code>	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: { 1..8}	Отображает состояние Voice VLAN.

5.17 Групповая адресация

5.17.1 Правила групповой адресации (multicast addressing)

Данный класс команд предназначен для задания правил групповой адресации в сети на канальном и сетевом уровнях модели OSI.

Команды режима конфигурирования интерфейса VLAN

Вид запроса командной строки в режиме конфигурирования интерфейса VLAN:

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

Таблица 5.108 – Команды режима конфигурирования интерфейса VLAN

<i>Команда</i>	<i>Значение/Значение по умолчанию</i>	<i>Описание</i>
<code>bridge multicast mode {mac-group ipv4-group ipv4-src-group}</code>	-/mac-group	Задаёт режим групповой передачи данных. - mac-group – многоадресная передача, основанная на VLAN и MAC-адресах; - ipv4-group – многоадресная передача с типом фильтрации, основанной на VLAN и адресе приемника в формате IPv4; - ip-src-group – многоадресная передача с типом фильтрации, основанной на VLAN и адресе отправителя в формате IPv4.
<code>no bridge multicast mode</code>		Устанавливает значение по умолчанию.
<code>bridge multicast address</code>	gi_port: {1..8/0/1..28};	Добавляет групповой MAC-адрес в таблицу групповой

<p><i>mac-[multicast-address ip-multicast-address] [[add remove]</i> { gigabitethernet gi_port fastethernet fa_port port-channel group }</p>	<p>fa_port: {1..8/0/1..24}; group: {1..8}.</p>	<p>адресации и статически добавляет или удаляет интерфейсы из группы. - mac-multicast-address – групповой MAC-адрес; - ip-multicast-address – IP-адрес многоадресной рассылки; - add – добавляет статическую подписку к групповому MAC-адресу диапазон Ethernet-портов или групп портов. - remove – удаляет статическую подписку. Перечисление интерфейсов осуществляется через «–» и «,»</p>
<p>no bridge multicast address <i>[mac-multicast-address ip-multicast-address]</i></p>		<p>Удаляет групповой MAC-адрес из таблицы.</p>
<p>bridge multicast forbidden address <i>[mac-multicast-address ip-multicast-address]</i> {add remove} { gigabitethernet gi_port fastethernet fa_port port-channel group }</p>	<p>gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}.</p>	<p>Запрещает подключение настраиваемого порта/портов к групповому IPv6-адресу (MAC-адресу). - mac-multicast-address – групповой MAC-адрес; - ip-multicast-address – IP-адрес многоадресной рассылки; - add – добавление порта/портов в список запрещенных; - remove – удаление порта/портов из списка запрещенных. Перечисление интерфейсов осуществляется через «–» и «,».</p>
<p>no bridge multicast forbidden address <i>[mac-multicast-address ip-multicast-address]</i></p>		<p>Удаляет запрещающее правило для группового MAC-адреса.</p>
<p>bridge multicast forward-all {add remove} {gigabitethernet gi_port fastethernet fa_port port-channel group }</p>	<p>gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}.</p> <p>По умолчанию передача всех многоадресных пакетов запрещена.</p>	<p>Разрешает передачу всех многоадресных пакетов на порту. - mac-multicast-address – групповой MAC-адрес; - add – добавляет порты/объединённые порты в список портов, для которых разрешена передача всех групповых пакетов; - remove – убирает группу портов/объединённых портов из разрешающего правила. Перечисление интерфейсов осуществляется через «–» и «,»</p>
<p>no bridge multicast forward-all</p>		<p>Восстанавливает значение по умолчанию.</p>
<p>bridge multicast forbidden forward-all {add remove} {gigabitethernet gi_port fastethernet fa_port port-channel group }</p>	<p>gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}.</p> <p>По умолчанию портам не запрещено динамически присоединяться к многоадресной группе.</p>	<p>Запрещает порту динамически добавляться к многоадресной группе. - interface-list – список интерфейсов Ethernet; - port-channel-number-list – список групп портов; - add – добавляет порты/объединённых порты в список портов, для которых запрещена передача всех групповых пакетов; - remove – убирает группу портов/объединённых портов из запрещающего правила. Перечисление интерфейсов осуществляется через «–» и «,»</p>
<p>no bridge multicast forbidden forward-all</p>		<p>Восстанавливает значение по умолчанию.</p>
<p>bridge multicast ip-address <i>ip-multicast-address [[add remove]</i> {gigabitethernet gi_port fastethernet fa_port port-channel group }</p>	<p>gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}</p>	<p>Регистрирует IP-адрес в таблице групповой адресации, и статически добавляет/удаляет интерфейсы из группы. - ip-multicast-address – групповой IP-адрес; - add – добавляет порты к группе; - remove – удаляет порты из группы; Перечисление интерфейсов осуществляется через «–» и «,»</p>
<p>no bridge multicast ip-address <i>ip-multicast-address</i></p>		<p>Удаляет групповой IP-адрес из таблицы.</p>

bridge multicast forbidden ip-address { <i>ip-multicast-address</i> } { add remove } {gigabitethernet gi_port fastethernet fa_port port-channel group}	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}	Запрещает порту динамически добавляться к многоадресной группе.- ip-multicast-address – групповой IP-адрес; - add – добавление порта/портов к списку запрещенных; - remove – удаление порта/портов из списка запрещенных. Перечисление интерфейсов осуществляется через «–» и «,» <input checked="" type="checkbox"/> Прежде чем определить запрещенные порты, группы многоадресной рассылки должны быть зарегистрированы.
no bridge multicast forbidden ip-address { <i>ip-multicast-address</i> }		Восстанавливает значение по умолчанию.
bridge multicast source ip-address group ip-multicast-address [[add remove] {gigabitethernet gi_port fastethernet fa_port port-channel group}]	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}	Устанавливает соответствие между IP-адресом пользователя и групповым адресом в таблице групповой адресации и статически добавляет/удаляет интерфейсы из группы. - <i>ip-address</i> – исходный IP-адрес; - <i>ip-multicast-address</i> – групповой IP-адрес; - <i>add</i> – добавить порты в группу исходного IP-адреса; - <i>remove</i> - удалить порты из группы исходного IP-адреса.
no bridge multicast source ip-address group ip-multicast-address		Восстанавливает значение по умолчанию.
bridge multicast forbidden source ip-address group ip-multicast-address { add remove } {gigabitethernet gi_port fastethernet fa_port port-channel group}	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}	Устанавливает запрет на добавление/удаление соответствия между IP-адресом пользователя и групповым адресом в таблице групповой адресации для определенного порта. - <i>ip-address</i> – исходный IP-адрес; - <i>ip-multicast-address</i> – групповой IP-адрес; - <i>add</i> – запрет на добавление порта в группу исходного IP-адреса; - <i>remove</i> – запрет на удаление порта из группы исходного IP-адреса.
no bridge multicast forbidden source ip-address group ip-multicast-address		Восстанавливает значение по умолчанию.
bridge multicast ipv6 mode { mac-group ip-group ip-src-group }	-/ <i>mac-group</i>	Задает режим групповой передачи данных для IPv6-пакетов многоадресной рассылки. - <i>mac-group</i> – многоадресная передача, основанная на VLAN и MAC-адресах; - <i>ip-group</i> – многоадресная передача с типом фильтрации, основанном на VLAN и адресе приемника в формате IPv6; - <i>ip-src-group</i> – многоадресная передача с типом фильтрации, основанном на VLAN и адресе отправителя в формате IPv6.
no bridge multicast ipv6 mode		Устанавливает значение по умолчанию.
bridge multicast ipv6 ip-address ip-v6-multicast-address [[add remove] {gigabitethernet gi_port fastethernet fa_port port-channel group}]	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}	Регистрирует групповой IPv6-адрес в таблице групповой адресации и статически добавляет/удаляет интерфейсы из группы. - <i>ip-multicast-address</i> – групповой IP-адрес; - <i>add</i> – добавляет порты к группе; - <i>remove</i> – удаляет порты из группы; Перечисление интерфейсов осуществляется через «–» и «,»
no bridge multicast ipv6 ip-address ip-multicast-address		Удаляет групповой IP-адрес из таблицы.
bridge multicast ipv6 forbidden ip-address ip-v6-multicast-address	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}	Запрещает подключение настраиваемого порта/портов к групповому IPv6-адресу. - <i>ip-multicast-address</i> – групповой IP-адрес;

{add remove} { gigabitethernet gi_port fastethernet fa_port port-channel group}		- add –добавление порта/портов в список запрещенных; - remove –удаление порта/портов из списка запрещенных. Перечисление интерфейсов осуществляется через «-» и «,»
no bridge multicast ipv6 forbidden ip-address <i>ipv6-multicast-address</i>		Восстанавливает значение по умолчанию.
bridge multicast ipv6 source <i>ipv6-address group</i> <i>ipv6-multicast-address</i> [[add remove] { gigabitethernet gi_port fastethernet fa_port port-channel group}]	<i>gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}</i>	Устанавливает соответствие между IPv6-адресом пользователя и групповым адресом в таблице групповой адресации и статически добавляет/удаляет интерфейсы из группы. - <i>ipv6-address</i> – исходный IP-адрес; - <i>ip-multicast-address</i> – групповой IP-адрес; - <i>add</i> – добавить порты в группу исходного IP-адреса; - <i>remove</i> – удалить порты из группы исходного IP-адреса.
no bridge multicast ipv6 source <i>ipv6-address group</i> <i>ipv6-multicast-address</i>		Восстанавливает значение по умолчанию.
bridge multicast ipv6 forbidden source <i>ipv6-address group</i> <i>ipv6-multicast-address</i> {add remove} { gigabitethernet gi_port fastethernet fa_port port-channel group}	<i>gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}</i>	Устанавливает запрет на добавление/удаление соответствия между IPv6-адресом пользователя и групповым адресом в таблице групповой адресации для определенного порта. - <i>ip-address</i> – исходный IPv6-адрес; - <i>ip-multicast-address</i> – групповой IPv6-адрес; - <i>add</i> – запрет на добавление порта в группу исходного IPv6-адреса; - <i>remove</i> – запрет на удаление порта из группы исходного IPv6-адреса.
no bridge multicast ipv6 forbidden source <i>ipv6-address group</i> <i>ipv6-multicast-address</i>		Восстанавливает значение по умолчанию.

Команды режима конфигурирования интерфейса (диапазона интерфейсов) Ethernet, интерфейса группы портов

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet, интерфейса группы портов:

```
console# configure
console(config)# interface {ethernet port|port-channel group}
console(config-if)#
```

Таблица 5.109 – Команды режима конфигурирования интерфейса Ethernet, группы интерфейсов

Команда	Значение/Значение по умолчанию	Описание
bridge multicast unregistered { forwarding filtering }	<i>-/forwarding</i>	Устанавливает правило передачи пакетов с незарегистрированных групповых адресов. - <i>forwarding</i> – передавать незарегистрированные многоадресные пакеты; - <i>filtering</i> – фильтровать незарегистрированные многоадресные пакеты.
no bridge multicast unregistered		Устанавливает значение по умолчанию.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.110 – Команды режима глобального конфигурирования

Команда	Значение/Значение по умолчанию	Описание
bridge multicast filtering	-/отключено	Включает фильтрацию групповых адресов.
no bridge multicast filtering		Отключает фильтрацию групповых адресов.
mac address-table aging-time seconds	10..630/300 секунд	Задает время хранения MAC-адреса в таблице.
no mac address-table aging-time		Устанавливает значение по умолчанию.
mac address-table learning vlan vlan_id	vlan_id: {1..4094}/ включено	Включить изучение MAC-адресов в данном VLAN
no mac address-table learning vlan vlan_id		Отключить изучение MAC-адресов в данном VLAN
mac address-table static mac-address vlan vlan-id interface {gigabitethernet gi_port fastethernet fa_port port-channel group} [permanent delete-on-reset delete-on-timeout secure]	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}	Добавляет исходный MAC-адрес в таблицу групповой адресации. - mac-address – MAC-адрес; -vlan-id – номер VLAN; - permanent – данный MAC-адрес можно удалить только с помощью команды no bridge address ; - delete-on-reset – данный адрес удалится после перезагрузки устройства; - delete-on-timeout – данный адрес удалится по тайм-ауту; - secure – данный адрес удалится только с помощью команды no bridge address или после возвращения порта в режим обучения (no port security).
no mac address-table static [mac-address] vlan vlan-id		Удаляет MAC-адрес из таблицы групповой адресации.
bridge multicast reserved-address mac-multicast-address [ethernet-v2 ethtype llc sap llc-snap pid] {discard bridge}	Ethtype: { 0x0600 - 0xFFFF} Sap: { 0 - 0xFFFF} pid: { 0 - 0xFFFFFFFF}	Определяет действие для пакетов многоадресной рассылки с зарезервированного адреса. - mac-multicast-address – групповой MAC-адрес; - ethtype – тип пакета Ethernet v2; - sap – тип пакета LLC; - pid – тип пакета LLC-Snap; - discard - сброс пакетов; - bridge – пакеты передаются в режиме bridge.
no bridge multicast reserved-address mac-multicast-address [ethernet-v2 ethtype llc sap llc-snap pid]		Устанавливает значение по умолчанию.
mac address-table lookup-length <length>	length: (1..8)/3	Задание длины хеша в таблице MAC-адресов.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 5.111 – Команды режима Privileged EXEC

Команда	Значение	Описание
clear mac address-table {dynamic secure} [interface {gigabitethernet gi_port fastethernet fa_port port-channel group}]	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}	Удаляет статические/динамические записи из таблицы групповой адресации. - dynamic – удаление динамических записей; - secure – удаление статических записей.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Таблица 5.112 – Команды режима EXEC

Команда	Значение	Описание
show mac address-table [dynamic static] secure] [vlan vlan] [interface {gigabitethernet gi_port fastethernet fa_port port- channel group}] [address mac-address]	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}; VLAN ID: {1..4094}	Показывает таблицу MAC-адресов для указанного интерфейса, либо всех интерфейсов. - dynamic – просмотр только динамических записей; - static – просмотр только статических записей; - secure – просмотр только безопасных записей.
show mac address-table count [vlan vlan interface {gigabitethernet gi_port fastethernet fa_port port- channel group}]]	-	Показывает количество записей в таблице MAC-адресов для указанного интерфейса, либо для всех интерфейсов.
show bridge multicast address-table [vlan vlan-id] [address {mac-multicast- address ipv4-multicast- address ipv6-multicast- address}] [format {ip mac}] [source {ipv4-source- address ipv6-multicast- address}]	VLAN ID [1..4094]	Показывает таблицу групповых адресов для указанного интерфейса, либо всех интерфейсов VLAN (команда доступна только для привилегированного пользователя). - ip – показывать по IP-адресам; - mac – показывать по MAC-адресам.
show bridge multicast address-table static [vlan vlan-id] [address mac- multicast-address ipv4- multicast-address ipv6- multicast-address] [source ipv4-source-address ipv6-multicast-address] [all mac ip]	VLAN ID [1..4094]	Показывает таблицу статических групповых адресов для указанного интерфейса, либо всех интерфейсов VLAN.
show bridge multicast filtering vlan-id	VLAN ID [1..4094]	Показывает конфигурацию фильтра групповых адресов для указанного VLAN.
show bridge multicast unregistered [gigabitethernet gi_port fastethernet fa_port port- channel group]	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}	Показывает конфигурацию фильтра для незарегистрированных групповых адресов.
show bridge multicast mode [vlan vlan-id]	VLAN ID [1..4094]	Показывает режим групповой адресации для указанного интерфейса, либо всех интерфейсов VLAN.
show bridge multicast reserved-addresses	-	Отображает правила, установленные для групповых зарезервированных адресов.
show mac address-table mode	-	Просмотр текущей длины хеша в таблице MAC-адресов.

Примеры выполнения команд

Включить фильтрацию групповых адресов коммутатором. Задать время хранения MAC-адреса 450 секунд, разрешить передачу незарегистрированные многоадресных пакетов на 11 порту коммутатора.

```
console # configure
console(config) # bridge aging-time 450
console(config) # bridge multicast filtering
console(config) # interface gigabitethernet 1/0/11
console(config-if) # bridge multicast unregistered forwarding

console# show bridge multicast address-table format ip
```

Vlan	IP/MAC Address	type	Ports
1	224-239.130 2.2.3	dynamic	1/1, 2/2
19	224-239.130 2.2.8	static	1/1-8
19	224-239.130 2.2.8	dynamic	1/9-11

Forbidden ports for multicast addresses:

Vlan	IP/MAC Address	Ports
1	224-239.130 2.2.3	2/8
19	224-239.130 2.2.8	2/8

5.17.2 Функция посредника протокола IGMP (IGMP Snooping)

Функция IGMP Snooping используется в сетях групповой рассылки. Основной задачей IGMP Snooping является предоставление многоадресного трафика только для тех портов, которые запросили его.



IGMP Snooping может использоваться только в статической группе VLAN. Поддерживаются версии протокола IGMP – IGMPv1, IGMPv2, IGMPv3.



Чтобы IGMP Snooping был активным, функция групповой фильтрации “bridge multicast filtering” должна быть включена (см. раздел «Правила групповой адресации»).

Распознавание портов, к которым подключены многоадресные маршрутизаторы, основано на следующих событиях:

- IGMP-запросы приняты на порту;
- пакеты протокола Protocol Independent Multicast (PIM/PIMv2) приняты на порту;
- пакеты протокола многоадресной маршрутизации Distance Vector Multicast Routing Protocol (DVMRP) приняты на порту;
- пакеты протокола MRDISC приняты на порту;
- пакеты протокола Multicast Open Shortest Path First (MOSPF) приняты на порту.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config) #
```

Таблица 5.113 – Команды режима глобального конфигурирования

Команда	Значение	Действие
ip igmp snooping	По умолчанию функция выключена	Разрешает использование функции IGMP Snooping коммутатором.
no ip igmp snooping		Запрещает использование функции IGMP Snooping коммутатором.
ip igmp snooping vlan vlan-id	По умолчанию функция выключена	Разрешает использование функции IGMP Snooping коммутатором для данного интерфейса VLAN.
no ip igmp snooping vlan vlan-id		Запрещает использование функции IGMP Snooping коммутатором для данного интерфейса VLAN.
ip igmp snooping vlan vlan-id static ip-address [interface { gigabitethernet gi_port fastethernet fa_port port- channel group}]	Vlan_id: {1..4094}; gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}	Регистрирует групповой IP-адрес в таблице групповой адресации, и статически добавляет интерфейсы из группы для текущей VLAN. - ip-address – групповой IP-адрес; Перечисление интерфейсов осуществляется через «-» и «,»
no ip igmp snooping vlan vlan-id static ip-address [interface { gigabitethernet gi_port fastethernet fa_port port- channel group}]		Удаляет групповой IP-адрес из таблицы.
ip igmp snooping vlan vlan-id mrouter learn pim- dvmrp	Vlan_id: {1..4094}; По умолчанию – разрешено	Разрешает для данной группы VLAN автоматическое распознавание портов, к которым подключены многоадресные маршрутизаторы.
no ip igmp snooping vlan vlan-id mrouter learn pim- dvmrp		Запрещает для данной группы VLAN автоматическое распознавание портов, к которым подключены многоадресные маршрутизаторы.
ip igmp snooping vlan vlan-id mrouter interface { gigabitethernet gi_port fastethernet fa_port port- channel group}	Vlan_id: {1..4094}; gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}	Определяет порт, к которому подключен маршрутизатор многоадресной рассылки для заданной VLAN.
no ip igmp snooping vlan vlan-id mrouter interface { gigabitethernet gi_port fastethernet fa_port port- channel group}		Указывает, что к порту не подключен маршрутизатор многоадресной рассылки.
ip igmp snooping vlan vlan-id forbidden mrouter interface { gigabitethernet gi_port fastethernet fa_port port- channel group}	Vlan_id: {1..4094}; gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}	Устанавливает запрет на определение порта (статически, динамически) как порта, к которому подключен маршрутизатор многоадресной рассылки.
no ip igmp snooping vlan vlan-id forbidden mrouter interface { gigabitethernet gi_port fastethernet fa_port port- channel group}		Снимает запрет на определение порта как порта, к которому подключен маршрутизатор многоадресной рассылки.
ip igmp snooping vlan vlan-id multicast-tv ip_multicast_address [count count]	Vlan_id: {1..4094}; Count: {1..256}/1	Определяет групповой IP-адрес, который соответствует VLAN телевидения (multicast-tv-vlan). - count – параметр для настройки нескольких смежных IP-адресов.
no ip igmp snooping vlan vlan-id multicast-tv ip_multicast_address [count count]		Удаляет соответствие между групповым IP-адресом и VLAN телевидения
ip igmp snooping map cpe vlan vlan-id multicast-tv vlan vlan-id	Vlan_id: {1..4094}	Добавляет соответствие между VLAN пользователя (CPE-VLAN) и VLAN телевидения (multicast-tv-vlan). Если IGMP-сообщение приходит на порт с тегом CPE-vlan и

		существует соответствие CPE-vlan – multicast-tv-vlan, то IGMP-сообщение будет ассоциировано с VLAN для телевидения.
no ip igmp snooping map cpe vlan <i>vlan-id</i>		Удаляет соответствие между VLAN пользователя и VLAN телевидения
ip igmp snooping vlan <i>vlan_id querier</i>	Vlan_id: {1..4094}	Включает поддержку выдачи запросов igmp-query коммутатором в данной VLAN.
no ip igmp snooping vlan <i>vlan_id querier</i>	-/выдача запросов отключена	Отключает поддержку выдачи запросов igmp-query коммутатором в данной VLAN.
ip igmp snooping vlan <i>vlan_id querier version</i> {2 3}		Устанавливает версию IGMP-протокола, на основании которой будут формироваться IGMP-query запросы.
no ip igmp snooping vlan <i>vlan_id querier version</i>	-/IGMPv3	Устанавливает значение по умолчанию
ip igmp snooping vlan <i>vlan_id querier address ip_address</i>		Определяет исходный IP-адрес, который будет использоваться IGMP querier-ом. Querier – устройство, которое отправляет IGMP-запросы.
no ip igmp snooping vlan <i>vlan-id querier address</i>	Vlan_id: {1..4094}	Устанавливает значение по умолчанию. По умолчанию если IP-адрес настроен для VLAN, он используется в качестве адреса источника IGMP Snooping Querier.
ip igmp snooping vlan <i>vlan-id immediate-leave</i>		Включить процесс IGMP Snooping Immediate-Leave на текущей VLAN. Означает, что порт должен быть немедленно удален из группы IGMP после получения сообщения IGMP leave. При добавлении опции host-based – механизм fast-leave срабатывает только в том случае, когда все пользователи, подключенные к данному порту отписались от группы (счетчик пользователей ведется на основании src-MAC-адресов в заголовках IGMP-report'ов).
no ip igmp snooping vlan <i>vlan-id immediate-leave [host-based]</i>	Vlan_id: {1..4094}/disable	Отключить процесс IGMP Snooping Immediate-Leave на текущей VLAN.
ip igmp snooping vlan <i>vlan_id immediate-leave host-based</i>		Включить процесс IGMP Snooping Immediate-Leave на текущей VLAN. Означает, что порт должен быть немедленно удален из группы IGMP после получения сообщения IGMP leave, если больше нет клиентов, которым необходима данная группа.
no ip igmp snooping vlan <i>vlan_id immediate-leave</i>	vlan_id: {1..4094}/disable	Отключить процесс IGMP Snooping Immediate-Leave на текущей VLAN.

Команды режима конфигурирования интерфейса VLAN

Вид запроса командной строки режима конфигурирования VLAN:

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

Таблица 5.114 – Команды режима конфигурирования интерфейса VLAN

Команда	Значение/Значение по умолчанию	Действие
ip igmp robustness <i>count</i>	1-7/2	Устанавливает значение робастности для IGMP. Если на канале наблюдается потеря данных, значение робастности должно быть увеличено.
no ip igmp robustness		Устанавливает значение по умолчанию.
ip igmp query-interval <i>seconds</i>	30–18000/125 с	Устанавливает таймаут, по которому система отправляет основные запросы всем участникам группы многоадресной передачи для проверки их активности.
no ip igmp query-interval		Устанавливает значение по умолчанию.
ip igmp query-max-	5-20/10 с	Устанавливает максимальное время ответа на запрос.

response-time seconds		
no ip igmp query-max-response-time		Устанавливает значение по умолчанию.
ip igmp last-member-query-count count	1-7/значение переменной robustness	Устанавливает количество запросов, после рассылки которых, MES1024/MES1124/MES2124 определяет, что на данном порту нет желающих участвовать в многоадресной рассылке.
no ip igmp last-member-query-count		Устанавливает значение по умолчанию.
ip igmp last-member-query-interval milliseconds	100-25500/1000 мс	Устанавливает интервал запроса для последнего участника.
no ip igmp last-member-query-interval		Устанавливает значение по умолчанию.

Команды режима конфигурирования интерфейса (диапазона интерфейсов) Ethernet

Вид запроса командной строки режима конфигурирования интерфейса:

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

Таблица 5.115 – Команды режима конфигурирования интерфейса Ethernet

Команда	Значение/Значение по умолчанию	Действие
switchport access multicast-tv vlan vlan_id	vlan_id: (1-4094)	Включает перенаправление IGMP-запросов с клиентских Vlan в Multicast Vlan и мультикастового трафика в клиентские Vlan для интерфейса в режиме «access».
no switchport access multicast-tv vlan		Выключает перенаправление IGMP-запросов с клиентских Vlan в Multicast Vlan и мультикастового трафика в клиентские Vlan для интерфейса в режиме «access».
switchport trunk multicast-tv vlan vlan_id	vlan_id: (1-4094)	Включает перенаправление IGMP-запросов с клиентских Vlan в Multicast Vlan и мультикастового трафика в клиентские Vlan для интерфейса в режиме «trunk».
no switchport trunk multicast-tv vlan		Выключает перенаправление IGMP-запросов с клиентских Vlan в Multicast Vlan и мультикастового трафика в клиентские Vlan для интерфейса в режиме «trunk».

Команды режима EXEC

Все команды доступны только для привилегированного пользователя.

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.116 – Команды режима EXEC

Команда	Действие
show ip igmp snooping mrouter [interface vlan-id]	Показывает информацию об изученных многоадресных маршрутизаторах в указанной группе VLAN.
show ip igmp snooping interface vlan-id	Показывает информацию IGMP-snooping для данного интерфейса.
show ip igmp snooping groups [vlan vlan-id] [ip-multicast-address ip-multicast-address] [ip-address ip-address]	Показывает информацию об изученных многоадресных группах, участвующих в групповой рассылке.
show ip igmp snooping multicast-tv [vlan vlan-id]	Показывает IP-адреса, ассоциированные с VLAN для телевидения.

show ip igmp snooping cpe vlans [vlan <i>vlan-id</i>]	Показывает таблицу соответствий между VLAN оборудования, установленного у пользователя, и VLAN для телевидения.
--	---

Примеры выполнения команд

Включить функцию IGMP snooping на коммутаторе. Для VLAN 6 разрешить автоматическое распознавание портов, к которым подключены многоадресные маршрутизаторы. Установить интервал между IGMP-запросами – 100 сек. Увеличить значение робастности до 4. Установить максимальное время ответа на запрос – 15 сек.

```

console# configure
console (config)# ip igmp snooping
console (config-if)# ip igmp snooping vlan 6 mrouter learn pim-dvmrp
console (config)# interface vlan 6
console (config-if)# ip igmp snooping query-interval 100
console (config-if)# ip igmp robustness 4
console (config-if)# ip igmp query-max-response-time 15

```

5.17.3 MLD snooping – протокол контроля многоадресного трафика в IPv6

MLD snooping – механизм многоадресной рассылки сообщений, позволяющий минимизировать многоадресный трафик в IPv6-сетях.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console (config) #
```

Таблица 5.117 – Команды глобального режима конфигурирования

Команда	Значение	Действие
ipv6 mld snooping [vlan <i>vlan_id</i>]	Vlan_id: {1..4094}/ disable	Включает MLD snooping.
no ipv6 mld snooping [vlan <i>vlan_id</i>]		Отключает MLD snooping.
ipv6 mld snooping vlan <i>vlan-id</i> static <i>ipv6-address</i> [interface { <i>gigabitethernet gi_port</i> <i>fastethernet fa_port</i> <i>port-channel group</i>}]	Vlan_id: {1..4094}; gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}	Регистрирует групповой IPv6-адрес в таблице групповой адресации и статически добавляет/удаляет интерфейсы из группы для текущей VLAN. - <i>ipv6-address</i> – групповой IPv6-адрес; Перечисление интерфейсов осуществляется через «-» и «,»
no ipv6 mld snooping vlan <i>vlan-id</i> static <i>ipv6-address</i> [interface { <i>gigabitethernet gi_port</i> <i>fastethernet fa_port</i> <i>port-channel group</i>}]		Удаляет групповой IP-адрес из таблицы.
ipv6 mld snooping vlan <i>vlan_id</i> forbidden mrouter interface {<i>gigabitethernet gi_port</i> <i>fastethernet fa_port</i> <i>port-channel group</i>}	Vlan_id: {1..4094}; gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}	Добавляет правило, запрещающее регистрировать MLD-mrouter порты из списка.
no ipv6 mld snooping vlan <i>vlan_id</i> forbidden mrouter interface {<i>gigabitethernet gi_port</i> <i>fastethernet fa_port</i> <i>port-channel group</i>}		Удаляет правило, запрещающее регистрировать MLD-mrouter порты из списка.

<code>ipv6 mld snooping vlan vlan_id mrouter learn pim- dvmrp</code>	-/включено	Изучать порты, подключенные к mrouter'у по MLD-query-пакетам
<code>no ipv6 mld snooping vlan vlan_id mrouter learn pim- dvmrp</code>		Не изучать порты, подключенные к mrouter'у по MLD-query-пакетам
<code>ipv6 mld snooping vlan vlan_id mrouter interface { gigabitethernet gi_port fastethernet fa_port port- channel group}</code>	Vlan_id: {1..4094}; gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}	Добавляет список mrouter-портов.
<code>no ipv6 mld snooping vlan vlan_id mrouter interface { gigabitethernet gi_port fastethernet fa_port port- channel group}</code>		Удаляет mrouter-порты.
<code>Ipv6 mld snooping vlan vlan-id immediate-leave</code>	Vlan_id: {1..4094}/disable	Включить процесс MLD Snooping Immediate-Leave на текущей VLAN.
<code>no ipv6 mld snooping vlan vlan-id immediate-leave</code>		Отключить процесс MLD Snooping Immediate-Leave на текущей VLAN.

Команды режима конфигурирования интерфейса VLAN

Вид запроса командной строки режима глобального конфигурирования:

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

Таблица 5.118 – Команды режима конфигурирования интерфейса VLAN

Команда	Значение/Значение по умолчанию	Действие
<code>ipv6 mld join-group multicast_ipv6_address</code>	multicast_ipv6_address – Групповой адрес IPv6	Создает статическую группу многоадресной IPv6-рассылки
<code>no ipv6 mld join-group multicast_ipv6_address</code>		Удаляет статическую группу многоадресной IPv6-рассылки
<code>ipv6 mld last-member- query-count count</code>	count: {1..7}	Устанавливает количество MLD-запросов, после рассылки которых MES1024/MES1124/MES2124 определяет, что на данном порту нет желающих участвовать в многоадресной IPv6-рассылке
<code>no ipv6 mld last-member- query-count</code>		Восстанавливает значение по умолчанию
<code>ipv6 mld last-member- query-interval interval</code>	interval: {100..25500}/1000 миллисекунд	Задаёт максимальную задержку ответа последнего члена группы, которая используется для вычисления кода максимальной задержки ответа (Max Response Code)
<code>no ipv6 mld last-member- query-interval</code>		Восстанавливает значение по умолчанию
<code>ipv6 mld query-interval value</code>	value: {30..18000}/125 секунд	Задаёт интервал рассылки основных MLD-запросов.
<code>no ipv6 mld query-interval</code>		Восстанавливает значение по умолчанию
<code>ipv6 mld query-max- response-time value</code>	value: {5..20}/10 секунд	Задаёт максимальную задержку ответа, которая используется для вычисления кода максимальной задержки ответа
<code>no ipv6 mld query-max- response-time</code>		Восстанавливает значение по умолчанию
<code>ipv6 mld robustness value</code>	value: {1..7}	Устанавливает значение коэффициента отказоустойчивости. Если на канале наблюдается потеря данных, коэффициент отказоустойчивости должен быть увеличен.
<code>no ipv6 mld robustness</code>		Восстанавливает значение по умолчанию

Команды режима конфигурирования интерфейса (диапазона интерфейсов) Ethernet, интерфейса группы портов, интерфейса VLAN

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet, интерфейса группы портов и интерфейса VLAN:

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

Таблица 5.119 – Команды режима конфигурирования интерфейса Ethernet, группы интерфейсов

Команда	Значение/Значение по умолчанию	Описание
<code>ipv6 mld join-group ipv6_address</code>	-	Дает указание рассылать MLD-report сообщения на присоединение к <code>ipv6_address</code> группы с данного порта. <code>ipv6_address</code> – групповой адрес IPv6
<code>no ipv6 mld join-group ipv6_address</code>		Удаляет указание рассылать MLD-report сообщения на присоединение к <code>ipv6_address</code> группы с данного порта
<code>ipv6 mld version version</code>	Version: {1..2}/2	Устанавливает версию протокола, действующую на данном интерфейсе.
<code>no ipv6 mld version</code>		Восстанавливает значение по умолчанию

Таблица 5.120 – Команды режима EXEC

Команда	Значение	Действие
<code>show ipv6 mld snooping groups [vlan vlan_id] [address ipv6_multicast_address] [source ipv6_source_address]</code>	<code>vlan_id</code> – {1..4094} <code>ipv6_multicast_address</code> – групповой адрес IPv6 <code>ipv6_source_address</code> – IPv6-адрес	Отображает информацию о зарегистрированных группах в соответствии с заданными в команде параметрами фильтрации
<code>show ipv6 mld snooping interface vlan_id</code>	Vlan: {1..4094}	Отображает информацию о конфигурации MLD-snooping для данной VLAN.
<code>show ipv6 mld snooping mrouter [interface vlan_id]</code>	Vlan: {1..4094}	Отображает информацию о mrouter-портах


5.17.4 Функции ограничения multicast-трафика

Функции ограничения multicast-трафика используются для удобной настройки ограничения просмотра определенных групп многоадресной рассылки.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config) #
```

Команда	Значение	Действие
<code>multicast snooping profile name</code>		Переход в режим конфигурирования multicast-профиля
<code>no multicast snooping profile name</code>	<code>name</code> : 1..32 символов	Удалить указанный multicast-профиль  Multicast-профиль может быть удален только после того, как будет отвязан от всех портов коммутатора

Команды режима конфигурирования multicast-профиля

Вид запроса командной строки режима конфигурирования multicast-профиля:

```
console(config-mc-profile) #
```

Команда	Значение	Действие
match ip <i>low_ip</i> [<i>high_ip</i>]	<i>low_ip</i> : валидный multicast-адрес	Задаёт соответствие профиля указанному диапазону IPv4 multicast-адресов
no match ip <i>low_ip</i> [<i>high_ip</i>]	<i>high_ip</i> : валидный multicast-адрес	Удаляет соответствие профиля указанному диапазону IPv4 multicast-адресов
match ipv6 <i>low_ipv6</i> [<i>high_ipv6</i>]	<i>low_ipv6</i> : валидный IPv6 multicast-адрес <i>high_ipv6</i> : валидный IPv6 multicast-адрес	Задаёт соответствие профиля указанному диапазону IPv6 multicast-адресов
no match ipv6 <i>low_ipv6</i> [<i>high_ipv6</i>]		Удаляет соответствие профиля указанному диапазону IPv6 multicast-адресов
permit	-/no permit	В случае несоответствия одному из заданных диапазонов, IGMP-report будут пропускаться
no permit		В случае несоответствия одному из заданных диапазонов, IGMP-report будут отбрасываться

Команды режима конфигурирования интерфейса (диапазона интерфейсов) Ethernet

Вид запроса командной строки режима конфигурирования интерфейса:

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

Команда	Значение/Значение по умолчанию	Действие
multicast snooping max-groups <i>number</i>	1-1000/-	Ограничивает количество одновременно просматриваемых multicast-групп для порта
no multicast snooping max-groups		Снимает ограничение на количество одновременно просматриваемых групп для порта
multicast snooping profile <i>name</i>	<i>name</i> :1..32 символов	Привязывает указанный multicast-профиль к порту
no multicast snooping profile		Удаляет соответствие multicast-профиля с портом

Команды режима EXEC

Все команды доступны только для привилегированного пользователя.

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.121 – Команды режима EXEC

Команда	Действие
show multicast snooping groups count	Отображает информацию для всех портов о текущем количестве зарегистрированных групп, а также максимальное возможное количество
show multicast snooping profile [<i>name</i>]	Отображает информацию о сконфигурированных multicast-профилях

5.18 Функции управления

5.18.1 Механизм AAA

Для обеспечения безопасности системы используется механизм AAA (аутентификация, авторизация, учет).

- *Authentication* (аутентификация) — сопоставление запроса существующей учётной записи в системе безопасности.
- *Authorization* (авторизация, проверка уровня доступа) — сопоставление учётной записи в системе (прошедшей аутентификацию) и определённых полномочий.
- *Accounting* (учёт) — слежение за потреблением ресурсов пользователем.

Для шифрования данных используется механизм *SSH*.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console (config) #
```

Таблица 5.122 – Команды режима глобального конфигурирования

Команда	Значение/Значение по умолчанию	Действие
aaa authentication login {default list-name} method1 [method2...]	По умолчанию осуществляется проверка по локальной базе данных (aaa authentication login default local) list-name: 1..12 символов	Устанавливает способ аутентификации для входа в систему. - default – использовать для аутентификации описанные ниже методы; - list-name- имя списка аутентификационных методов, активирующегося, когда пользователь входит в систему. Описание методов (method1 [method2...]): - enable – использовать пароль для аутентификации; - line – использовать пароль терминала для аутентификации; - local – использовать локальную базу имен пользователей для аутентификации; - none – не использовать аутентификацию; - radius – использовать список RADIUS серверов для аутентификации; - tacacs – использовать список TACACS серверов для аутентификации. <input checked="" type="checkbox"/> Если метод аутентификации не определен, то доступ к консоли всегда успешный без аутентификационных проверок. <input checked="" type="checkbox"/> Создание списка осуществляется командой: aaa authentication login list-name method1 [method2...]. Использование списка: aaa authentication login list-name
no aaa authentication login {default list-name}		Устанавливает значение по умолчанию.
aaa authentication enable {default list-name} method1 [method2...]	По умолчанию осуществляется проверка пароля (aaa authentication enable default enable) list-name: 1..12 символов	Устанавливает способ аутентификации при повышении уровня привилегий для входа в систему. - default – использовать для аутентификации описанные ниже методы; - list-name- имя списка аутентификационных методов активирующийся, когда пользователь входит в систему. Описание методов (method1 [method2...]): - enable – использовать пароль для аутентификации; - line - использовать пароль терминала для

		<p>аутентификации;</p> <ul style="list-style-type: none"> - none – не использовать аутентификацию; - radius – использовать список RADIUS серверов для аутентификации; - tacacs – использовать список TACACS серверов для аутентификации. <p><input checked="" type="checkbox"/> Если для консоли пароль не определен, то доступ к консоли всегда успешный без пароля (<code>aaa authentication enable default enable none</code>).</p> <p><input checked="" type="checkbox"/> Создание списка осуществляется командой <code>aaa authentication enable list-name method1 [method2...]</code>. Использование списка: <code>aaa authentication enable list-name</code></p> <p><input checked="" type="checkbox"/> Все запросы, передаваемые к Radius и TACACS серверам, включают имя пользователя "\$enabx\$", где x – уровень привилегий.</p>
<code>no aaa authentication enable {default list-name}</code>		Устанавливает значение по умолчанию.
<code>enable password [level level] password [encrypted]</code>	<p>level: [1..15] password: [1..159] символов</p>	<p>Устанавливает пароль для контроля изменения привилегий доступа пользователей.</p> <ul style="list-style-type: none"> - level – уровень привилегий; - password – пароль; - encrypted – задать зашифрованный пароль (например, пароль в зашифрованном виде, скопированный с другого устройства).
<code>no enable password [level level]</code>		Удаляет пароль для соответствующего уровня привилегий.
<code>username name { nopassword password password password encrypted encrypted-password } [priviledged level]</code>	<p>level: [1..15] password: [1..159] символов name: 1..20 символов</p>	<p>Добавляет пользователя в локальную базу данных.</p> <ul style="list-style-type: none"> - level – уровень привилегий; - password – пароль; - name – имя пользователя; - encrypted – задать зашифрованный пароль (например, пароль в зашифрованном виде, скопированный с другого устройства).
<code>no username name</code>		Удаляет пользователя из локальной базы данных
<code>aaa accounting login start-stop group radius</code>	По умолчанию ведение учета запрещено	<p>Разрешает ведение учета (аккаунта) для сессий управления.</p> <p><input checked="" type="checkbox"/> Ведение учета разрешено только для пользователей, вошедших в систему по имени и паролю, для пользователей, вошедших по паролю терминала, ведение учета запрещено.</p> <p><input checked="" type="checkbox"/> Ведение учета активируется и прекращается, когда пользователь входит и отключается от системы, что соответствует значениям start и stop в сообщениях протокола RADIUS (параметры, содержащиеся в сообщениях протокола RADIUS, приведены в таблице 5.123).</p>
<code>no aaa accounting login start-stop group radius</code>		Устанавливает значение по умолчанию.
<code>aaa accounting dot1x start-stop group radius</code>	По умолчанию ведение учета запрещено	<p>Разрешает ведение учета (аккаунта) для сессий 802.1x.</p> <p><input checked="" type="checkbox"/> Ведение учета активируется и прекращается, когда пользователь входит и отключается от системы, что соответствует значениям start и stop в сообщениях протокола RADIUS (параметры, содержащиеся в сообщениях протокола RADIUS приведены в таблице 5.124).</p> <p><input checked="" type="checkbox"/> В режиме multiple sessions сообщения stat/stop посылаются для каждого пользователя, в режиме multiple hosts - только для пользователя, прошедшего аутентификацию (см. раздел по 802.1x).</p>
<code>no aaa accounting dot1x start-stop group radius</code>		Устанавливает значение по умолчанию.

ip http authentication aaa login-authentication method1 [method2...]	Method: local, none, tacacs, radius/local	Определяет метод аутентификации при доступе к HTTP-серверу. При установке списка методов, дополнительный метод будет применяться, только когда по основному методу аутентификации возвращена ошибка. - local – по имени из локальной базы данных; - none – не используется; - tacacs – использование списков всех серверов TACACS+; - radius – использование списков всех RADIUS-серверов.
no ip http authentication aaa login-authentication		Устанавливает значение по умолчанию.
ip ftp authentication aaa login-authentication method1 [method2...]	Method: local, none, tacacs, radius/local	Определяет метод аутентификации при доступе к FTP-серверу. При установке списка методов, дополнительный метод будет применяться, только когда по основному методу аутентификации возвращена ошибка. - local – по имени из локальной базы данных; - none – не используется; - tacacs – использование списков всех серверов TACACS+; - radius – использование списков всех RADIUS-серверов.
no ip ftp authentication aaa login-authentication		Устанавливает значение по умолчанию
aaa accounting commands stop-only default tacacs	По умолчанию ведение учета запрещено	Разрешает ведение учета (аккаунта) для введенных в CLI команд
no aaa accounting commands stop-only default tacacs		Устанавливает значение по умолчанию



Для того чтобы клиент получил доступ к устройству, даже если все методы аутентификации вернули ошибку, используйте значение последнего метода в команде – none.

Таблица 5.123 – Атрибуты сообщений ведения учета протокола RADIUS для сессий управления

Атрибут	Наличие атрибута в сообщении Start	Наличие атрибута в сообщении Stop	Описание
User-Name (1)	Есть	Есть	Идентификация пользователя.
NAS-IP-Address (4)	Есть	Есть	IP-адрес коммутатора, который используется для сессий с Radius-сервером.
Class (25)	Есть	Есть	Произвольное значение, включенное во все сообщения учета сессий.
Called-Station-ID (30)	Есть	Есть	IP-адрес коммутатора, используемый для сессий управления.
Calling-Station-ID (31)	Есть	Есть	IP-адрес пользователя.
Acct-Session-ID (44)	Есть	Есть	Уникальный идентификатор учета.
Acct-Authentic (45)	Есть	Есть	Указывает метод, по которому клиент должен быть аутентифицирован.
Acct-Session-Time (46)	Нет	Есть	Показывает, как долго пользователь был подключен к системе.
Acct-Terminate-Cause (49)	Нет	Есть	Причина закрытия сессии.

Таблица 5.124 – Атрибуты сообщений ведения учета протокола RADIUS для сессий 802.1x

<i>Атрибут</i>	<i>Наличие атрибута в сообщении Start</i>	<i>Наличие атрибута в сообщении Stop</i>	<i>Описание</i>
User-Name (1)	Есть	Есть	Идентификация пользователя.
NAS-IP-Address (4)	Есть	Есть	IP-адрес коммутатора, который используется для сессий с Radius-сервером.
NAS-Port (5)	Есть	Есть	Порт коммутатора, на котором подключился пользователь.
Class (25)	Есть	Есть	Произвольное значение, включенное во все сообщения учета сессий.
Called-Station-ID (30)	Есть	Есть	IP-адрес коммутатора.
Calling-Station-ID (31)	Есть	Есть	IP-адрес пользователя.
Acct-Session-ID (44)	Есть	Есть	Уникальный идентификатор учета.
Acct-Authentic (45)	Есть	Есть	Указывает метод, по которому клиент должен быть аутентифицирован.
Acct-Session-Time (46)	Нет	Есть	Показывает, как долго пользователь был подключен к системе.
Acct-Terminate-Cause (49)	Нет	Есть	Причина закрытия сессии.
Nas-Port-Type (61)	Есть	Есть	Показывает тип порта клиента.

Команды режима конфигурирования терминала

Вид запроса командной строки в режиме конфигурирования терминала:

```
console(config-line)#
```

Таблица 5.125 – Команды режима конфигурирования интерфейса Ethernet

<i>Команда</i>	<i>Значение/Значение по умолчанию</i>	<i>Действие</i>
login authentication {default list-name}	list-name: 1..12 символов	Задаёт метод аутентификации при входе для консоли, telnet, ssh. - default – использовать список «по умолчанию», созданный командой aaa authentication login default - list-name – использовать список, созданный командой aaa authentication login list-name.
no login authentication		Устанавливает значение по умолчанию.
enable authentication {default list-name}	list-name: 1..12 символов	Задаёт метод аутентификации пользователя при повышении уровня привилегий для консоли, telnet, ssh. - default – использовать список «по умолчанию», созданный командой aaa authentication login default - list-name – использовать список, созданный командой aaa authentication login list-name.
no enable authentication		Устанавливает значение по умолчанию.
password password [encrypted]	1..159 символов	Задаёт пароль для терминала. - encrypted – задать зашифрованный пароль (например, пароль в зашифрованном виде, скопированный с другого устройства).
no password		- Удаляет пароль для терминала.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 5.126 – Команды режима Privileged EXEC

Команда	Значение/Значение по умолчанию	Действие
show authentication methods	-	Показывает информацию об аутентификационных методах на коммутаторе.
show users accounts	-	Показывает локальную базу данных пользователей и их привилегий.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Все команды данного раздела доступны только для привилегированных пользователей.

Таблица 5.127 – Команды режима EXEC

Команда	Действие
show accounting	Показывает информацию о настроенных методах ведения учета (аккаунта).

5.18.2 Протокол RADIUS

Протокол RADIUS используется для аутентификации, авторизации и учета. Сервер RADIUS использует базу данных пользователей, которая содержит данные проверки подлинности для каждого пользователя. Таким образом, использование протокола RADIUS обеспечивает дополнительную защиту при доступе к ресурсам сети, а также при доступе к самому коммутатору.

Команды режима глобального конфигурирования

Вид запроса командной строки в режиме глобального конфигурирования:

```
console(config)#
```

Таблица 5.128 - Команды режима глобального конфигурирования

Команда	Значение/Значение по умолчанию	Действие
radius-server host <i>{ip-addr/hostname}</i> [auth-port auth_port] [acct-port acct-port] [timeout timeout] [retransmit retries] [deadtime time] [key secret_key] [encrypted key encrypted_key] [source source_ip-addr] [priority]	hostname: {1..158} символов; auth_port: [0..65535]/1812; acct_port: [0..65535]/1813; timeout: [1-30] сек; retries: [1-10]; time [0-2000] мин; secret_key: [0..128] символов; encrypted key:	Добавляет указанный сервер в список используемых RADIUS серверов. - ip-addr – IPv4 или IPv6-адрес RADIUS-сервера; - hostname – сетевое имя RADIUS-сервера; - auth_port – номер порта для передачи аутентификационных данных; - acct_port – номер порта для передачи данных учета; - timeout - интервал ожидания ответа от сервера; - retries - количество попыток поиска RADIUS-сервера; - time - время в минутах, в течение которого недоступные сервера не будут опрашиваться RADIUS-клиентом

<i>priority</i> [usage type]	[0..128] символов; priority: [0..65535]/0; type [login, 802.1x, all]/ all В случае отсутствия в команде параметров timeout, retries, time, secret_key, source_ip-addr для данного RADIUS-сервера используются значения настроенные с помощью команд указанных ниже (значения по умолчанию)	коммутатора; - secret_key – ключ для аутентификации и шифрования всего обмена данными RADIUS; - encrypted key – ключ для аутентификации и шифрования всего обмена данными RADIUS; - source ip-addr - IPv4 или IPv6-адрес, используемый в качестве адреса источника, передаваемого в сообщениях протокола RADIUS; - priority – приоритет использования RADIUS-сервера (чем ниже значение, тем приоритетнее сервер); - type – тип использования RADIUS-сервера.
no radius-server host <i>{ip-addr hostname}</i>		Удаляет указанный сервер из списка используемых RADIUS-серверов.
radius-server key <i>[key]</i>	[0..128] символов/ по умолчанию ключ - пустая строка	Устанавливает ключ, используемый по умолчанию, для аутентификации и шифрования всего обмена данными RADIUS между устройством и окружением RADIUS.
no radius-server key		Устанавливает значение по умолчанию.
radius-server timeout <i>timeout</i>	1-30/3 сек	Устанавливает интервал ожидания ответа от сервера, используемый по умолчанию.
no radius-server timeout		Устанавливает значение по умолчанию.
radius-server retransmit <i>retries</i>	1-10/3	Определяет количество попыток, используемое по умолчанию, поиска RADIUS-сервера из списка серверов. При отказе осуществляется поиск следующего по приоритету сервера из списка.
no radius-server retransmit		Устанавливает значение по умолчанию
radius-server deadtime <i>deadtime</i>	0-2000/0 мин.	Позволяет оптимизировать время опроса RADIUS-серверов, когда некоторые сервера недоступны. Устанавливает время в минутах, используемое по умолчанию, в течение которого недоступные сервера не будут опрашиваться RADIUS-клиентом коммутатора.
radius-server deadtime <i>deadtime</i>		Устанавливает значение по умолчанию.
radius-server source-ip <i>ip_addr</i>	-	Задаёт определенный IPv4-адрес, используемый по умолчанию в качестве адреса источника передаваемого в сообщениях протокола RADIUS.
no radius-server source-ip <i>[ip_addr]</i>		Удаляет определенный IPv4-адрес, используемый по умолчанию в качестве адреса источника передаваемого в сообщениях протокола RADIUS. Устанавливает IPv4-адрес интерфейса коммутатора в качестве адреса источника для использования в сообщениях протокола RADIUS.
radius-server source-ipv6 <i>ip_addr</i>	-	Задаёт определенный IPv6-адрес, используемый по умолчанию в качестве адреса источника передаваемого в сообщениях протокола RADIUS
no radius-server source-ipv6 <i>[ip_addr]</i>		Удаляет определенный IPv6-адрес, используемый по умолчанию в качестве адреса источника передаваемого в сообщениях протокола RADIUS. Устанавливает IPv6-адрес интерфейса коммутатора в качестве адреса источника для использования в сообщениях протокола RADIUS.

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 5.129 - Команды режима Privileged EXEC

Команда	Действие
show radius-servers	Отображает параметры настройки RADIUS серверов (Команда доступна только для

	привилегированных пользователей).
show radius statistics	Отображает статистику протокола Radius.

Примеры использования команд

- Установить глобальные значения для параметров: интервал ожидания ответа от сервера – 5 секунд, количество попыток поиска RADIUS сервера – 5, время, в течение которого недоступные сервера не будут опрашиваться RADIUS клиентом коммутатора – 10 минут, секретный ключ - secret. Добавить в список RADIUS сервер, расположенный на узле сети с IP адресом 192.168.16.3, порт сервера для аутентификации – 1645, количество попыток доступа к серверу – 2.

```
console# configure
console (config)# radius-server timeout 5
console (config)# radius-server retransmit 5
console (config)# radius-server deadtime 10
console (config)# radius-server key secret
console (config)# radius-server host 192.168.16.3 auth-port 1645 retransmit
2
```

- Показать параметры настройки RADIUS серверов

```
console# show radius-servers
```

```
start
```

IP address	Port Auth	port Acct	Tim Out	Ret- rans	Dead- Time	source IP	Prio.	Usage
192.168.16.3	1645	1813	Global	2	Global	Global	0	all
196.168.16.3	1645	1813	Global	2	Global	Global	0	all

```
Global values
-----
TimeOut : 5
Retransmit : 5
Deadtime : 10
Source IP : 0.0.0.0
Source IPv6 : ::
```

5.18.3 Протокол TACACS+

Протокол TACACS+ обеспечивает централизованную систему безопасности для проверки пользователей, получающих доступ к устройству, при этом поддерживая совместимость с RADIUS и другими процессами проверки подлинности. TACACS+ предоставляет следующие службы:

- Authentication (проверка подлинности). Обеспечивается во время входа в систему по именам пользователей и определенным пользователями паролям.
- Authorization (авторизация). Обеспечивается во время входа в систему. После завершения сеанса проверки подлинности запускается сеанс авторизации с использованием проверенного имени пользователя, также сервером проверяются привилегии пользователя.

Команды режима глобального конфигурирования

Вид запроса командной строки в режиме глобального конфигурирования:

```
console (config) #
```

Таблица 5.130 - Команды режима глобального конфигурирования

Команда	Значение/Значение по умолчанию	Действие
tacacs-server host <i>{ip-addr hostname}</i> [single-connection] [port port] [timeout timeout] [key secret_key] [encrypted key] [source encrypted_key] [priority priority]	hostname: {1..158} символов; port: [0..65535]/49; timeout: [1-30] сек; retries: [1-10]; time [0-2000] мин; key: [0..128] символов; encrypted_key: [0..128] символов; priority: [0..65535]/0; В случае отсутствия в команде параметров timeout, key, source_ip-addr для данного TACACS-сервера используются значения настроенные с помощью команд, указанных ниже (значения по умолчанию)	Добавляет указанный сервер в список используемых TACACS серверов. - ip-addr – IP адрес TACACS-сервера; - hostname – сетевое имя TACACS-сервера; - single connection – в каждый момент времени иметь не больше одного соединения для обмена данными с TACACS-сервером; - port – номер порта для обмена данными с TACACS-сервером; - timeout - интервал ожидания ответа от сервера; - key – ключ для аутентификации и шифрования всего обмена данными TACACS; - encrypted_key – ключ в зашифрованном виде для аутентификации и шифрования всего обмена данными TACACS;- source ip-addr – IP-адрес, используемый в качестве адреса источника, передаваемого в сообщениях протокола TACACS; - priority – приоритет использования TACACS-сервера (чем ниже значение, тем приоритетнее сервер).
no tacacs-server host <i>{ip-addr hostname}</i>		Удаляет указанный сервер из списка используемых TACACS-серверов.
tacacs-server key [<i>key</i>]	[0..128] символов/ по умолчанию ключ - пустая строка	Устанавливает ключ, используемый по умолчанию, для аутентификации и шифрования всего обмена данными TACACS между устройством и окружением TACACS.
no tacacs-server key		Устанавливает значение по умолчанию.
tacacs-server timeout <i>timeout</i>	1-30/5 сек	Устанавливает интервал ожидания ответа от сервера, используемый по умолчанию.
no tacacs-server timeout		Установить значение по умолчанию.
tacacs-server source-ip <i>source_ip-addr</i>		Задаёт IP-адрес коммутатора, используемый по умолчанию для обмена сообщениями с TACACS-сервером
no tacacs-server source-ip <i>source_ip-addr</i>	-	Устанавливает использование IP-адреса интерфейса коммутатора для обмена сообщениями с TACACS-сервером.

Команды режима EXEC

Вид запроса командной строки в режиме EXEC:

```
console#
```

Таблица 5.131 - Команды режима EXEC

Команда	Значение	Действие
show tacacs <i>[ip-addr]</i>	-	Отображает настройку и статистику для сервера TACACS+. Ip-addr – IP-адрес TACACS+ сервера, либо имя сервера.
show tacacs statistics	-	Отображает статистику протокола TACACS+.

Примеры использования команд

Добавить в список серверов TACACS-сервер, расположенный на узле сети с IP-адресом 192.168.16.34, таймаут ожидания ответа от сервера – 4 секунды, секретный ключ для обмена данными с сервером – secret, IP-адрес коммутатора, используемый для обмена с этим сервером – 192.168.16.38, приоритет сервера – 8.

```
console# configure
console(config)# tacacs-server host 192.168.16.34 timeout 4 key secret
source 192.168.16.38 priority 8
```

5.18.4 Протокол управления сетью (SNMP)

SNMP – технология, призванная обеспечить управление и контроль над устройствами и приложениями в сети связи путём обмена управляющей информацией между агентами, расположенными на сетевых устройствах, и менеджерами, находящимися на станциях управления. SNMP определяет сеть как совокупность сетевых управляющих станций и элементов сети (главные машины, шлюзы и маршрутизаторы, терминальные серверы), которые совместно обеспечивают административные связи между сетевыми управляющими станциями и сетевыми агентами.

Коммутатор MES1024/MES1124/MES2124 позволяет настроить работу протокола SNMP для удаленного мониторинга и управления устройством. Устройство поддерживает протоколы версий SNMPv1, SNMPv2, SNMPv3.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console (config) #
```

Таблица 5.132 – Команды режима глобального конфигурирования

Команда	Значение/Значение по умолчанию	Действие
snmp-server server	По умолчанию	Включить поддержку протокола SNMP.
no snmp-server server	поддержка протокола SNMP включена	Отключает поддержку протокола SNMP.
snmp-server community <i>community</i> [view <i>viewname</i>] [ro rw su] [<i>ipv4-addr</i> <i>ipv6-addr</i> <i>ipv6z-addr</i>] [<i>mask</i> <i>prefix-length</i>] [<i>use-acl ip-acl-name</i>]	community: 1..20 символов viewname: 1..30 символов groupname: 1..30 символов <i>mask по умолчанию</i> 255.255.255.255 prefix-length по умолчанию 32 ip-acl-name: 1..32 символов формат IPv4: A.B.C.D IPv6: X:X:X:X::X IPv6z: X:X:X:X::X%<ID>	Устанавливает значение строки сообщества для обмена данными по протоколу SNMP. - community – строка сообщества (пароль) для доступа по протоколу SNMP; - ro – доступ только для чтения; - rw – доступ для чтения и записи; - su – доступ администратора; - viewname – определяет имя для правила обозрения SNMP, которое должно быть предварительно определено с помощью команды snmp-server view . Определяет объекты, доступные сообществу; - ipv4-addr, ipv6-addr, ipv6z-addr – IP-адрес устройства; - mask – маска адреса IPv4, которая определяет, какие биты адреса источника пакета сравниваются с заданным IP-адресом; - prefix-length – число бит, которые составляют префикс IPv4-адреса; - ip-acl-name – имя существующего ACL-списка; - groupname – определяет имя группы, которое должно быть предварительно определено с помощью команды snmp-server group . Определяет объекты, доступные сообществу.
no snmp-server community <i>community</i> [<i>ipv4-addr</i> <i>ipv6-addr</i> <i>ipv6z-addr</i>]		Удаляет параметры для строки сообщества.
snmp-server view <i>view-name</i> <i>OID</i> {included excluded}	View-name: 1..30 символов	Создает или редактирует правило обозрения для SNMP – разрешающее правило, либо ограничивающее серверу-обозревателю доступ к OID. OID–идентификатор объекта MIB, представленный в виде дерева ASN.1 (строка вида 1.3.6.2.4, может включать в себя зарезервированные слова, например: system, dod). С помощью символа * можно обозначить семейство поддеревьев: 1.3.*.2); - include – OID включена в правило для обозревания;

		- exclude – OID исключена из правила для обозревания.
no snmp-server view <i>viewname [OID]</i>		Удаляет правило обозрения для SNMP.
snmp-server group <i>groupname {v1 v2 v3</i> <i>{noauth auth priv} [notify</i> <i>notifyview]}</i> <i>[read readview] [write</i> <i>writeview]</i>	groupname: 1..30 символов notifyview: 1..30 символов readview: 1..30 символов writeview: 1..30 символов	Создает SNMP-группу или таблицу соответствий SNMP-пользователей и правил обозрений SNMP. -v1,v2,v3 – SNMP v1, v2, v3 модель безопасности; - noauth,auth,priv – тип аутентификации, используемый протоколом SNMP v3 (noauth – без аутентификации, auth – аутентификация без шифрования, priv – аутентификация с шифрованием); - notifyview – имя правила обозрения, которому разрешено определять сообщения SNMP-агента – inform и trap; - readview – имя правила обозрения, которому разрешено только чтение содержимого SNMP-агента коммутатора; - writeview – имя правила обозрения, которому разрешено вводить данные и конфигурировать содержимое SNMP-агента коммутатора.
no snmp-server group <i>groupname</i> <i>{v1 v2 v3 [noauth </i> <i>auth priv]}</i>		Удаляет SNMP-группу
snmp-server user <i>username groupname</i> <i>{v1 v2c remote host v3</i> <i> v3 [encrypted] [auth</i> <i>{md5 sha}</i> <i>auth-password]}</i>	username: 1..20 символов groupname: 1..30 символов engineid-string: 5..32 символов password: 1..32 символа md5-des-keys: 16 или 32 байт sha-des-keys: 20 или 36 байт	Создает SNMPv3-пользователя. - username – имя пользователя; - groupname – имя группы; - engineid-string – идентификатор удаленного SNMP-устройства, которому пользователь принадлежит; - password – пароль для аутентификации и генерации ключа; - md5-des-keys – ключ md5; - sha-des-keys – ключ sha; - host – IP-адрес/ имя хоста.
no snmp-server user <i>username</i> <i>[remote engineid-string]</i>	формат IPv4: A.B.C.D IPv6: X:X:X:X::X IPv6z: X:X:X:X::X%<ID>	Удаляет SNMPv3-пользователя.
snmp-server filter <i>filter-</i> <i>name oid {included </i> <i>excluded}</i>	filter-name: 1..30 символов	Создает или редактирует правило SNMP-фильтра, которое позволяет фильтровать inform и trap-сообщения, передаваемые SNMP-серверу. - OID – идентификатор объекта MIB, представленный в виде дерева ASN.1 (строка вида 1.3.6.2.4, может включать в себя зарезервированные слова, например: system, dod. С помощью символа * можно обозначить семейство поддеревьев: 1.3.*.2); - include – OID включена в правило фильтрации; - exclude – OID исключена из правила фильтрации.
snmp-server filter <i>filter-</i> <i>name [oid]</i>		Удаляет правило SNMP-фильтра.
snmp-server host <i>{ipv4-</i> <i>address ipv6-address </i> <i>hostname} [traps informs]</i> <i>[version {1 2c 3 [auth </i> <i>noauth priv]}] community</i> <i>[udp-port port] [filter</i> <i>filtername] [timeout</i> <i>seconds] [retries retries]</i>	hostname: 1..158 символов community: 1..20 символов udp-port: 1..65535/162 filtername: 1..30 символов seconds: 1..300/15	Определяет настройки для передачи сообщений уведомления inform и trap SNMPv1/v2-серверу. - community – строка сообщества для передачи сообщений уведомления; - version – определяют тип сообщений trap – trap SNMPv1, trap SNMPv2, trap SNMPv3; - auto – указывает подлинность пакета без шифрования; - noauto – не указывает подлинность пакета; - priv – указывает подлинность пакета с шифрованием; - port – UDP порт SNMP-сервера; -seconds – период ожидания подтверждений перед повторной передачей сообщений inform;

	retries: 0..255/3	- retries – количество попыток передачи сообщений inform, при отсутствии их подтверждения.
no snmp-server host { <i>ipv4-address ipv6-address hostname</i> } [traps informs]		Удаляет настройки для передачи сообщений уведомления inform и trap SNMPv1/v2/v3-серверу.
snmp-server v3-host { <i>ipv4-address ipv6-address hostname</i> } <i>username</i> [traps informs] { noauth auth priv } [udp-port port] [filter filtername] [timeout seconds] [retries retries]	hostname: 1..158 символов username: 1..24 символов udp-port: 1..65535/162 filtername: 1..30 символов	Определяет настройки для передачи сообщений уведомления inform и trap SNMPv3-серверу. - noauth,auth,priv – тип аутентификации, используемый протоколом SNMP v3 (noauth – без аутентификации, auth – аутентификация без шифрования, priv – аутентификация с шифрованием); - port – UDP-порт SNMP-сервера; - seconds – период ожидания подтверждений перед повторной передачей сообщений inform; - retries – количество попыток передачи сообщений inform, при отсутствии их подтверждения.
no snmp-server v3-host { <i>ipv4-address ipv6-address hostname</i> } <i>username</i> [traps informs]	seconds: 1..300/15 retries: 0..255/3	Удаляет настройки для передачи сообщений уведомления inform и trap SNMPv3-серверу.
snmp-server engineID local { <i>engineid-string default</i> }	5..32 символов	Создает идентификатор локального SNMP устройства – engineID. - default – при использовании данной настройки engineID будет автоматически создан, на основе MAC-адреса устройства.
no snmp-server engineID local		Удаляет идентификатор локального SNMP устройства – engineID
snmp-server engineID remote { <i>ipv4-ip-address ipv6 address</i> } <i>engineid-string</i>	5..32 символов	Создает идентификатор удаленного SNMP устройства – engineID.
no snmp-server engineID remote { <i>ipv4-ip-address ipv6 address</i> }		Удаляет идентификатор удаленного SNMP устройства – engineID.
snmp-server enable traps		Включает поддержку SNMP trap сообщений.
no snmp-server enable traps	-	Отключает поддержку SNMP trap сообщений.
snmp-server enable traps link-status		Включает отправку SNMP trap сообщений при изменении состояния порта.
no snmp-server enable traps link-status	-/enabled	Отключает отправку SNMP trap сообщений при изменении состояния порта.
snmp-server trap authentication		Разрешает передавать сообщения trap серверу не прошедшему аутентификацию.
no snmp-server trap authentication	-	Запрещает передавать сообщения trap серверу не прошедшему аутентификацию.
snmp-server contact text	1..160 символов	Определяет контактную информацию устройства.
no snmp-server contact		Удаляет контактную информацию устройства.
snmp-server location text	1..160 символов	Определяет информацию о местоположении устройства.
no snmp-server location		Удаляет информацию о местоположении устройства.

snmp-server set variable-name <i>name1 value1</i> [<i>name2 value2 ...</i>]	variable-name, name, value должны задаваться в соответствии со спецификацией	Позволяет установить значения переменных в базе данных MIB коммутатора. - variable-name – имя переменной; - name, value – пары соответствий имя – значение.
--	--	---

Команды режима конфигурирования интерфейса (диапазона интерфейсов) Ethernet

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet:

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

Таблица 5.133 – Команды режима конфигурирования интерфейса Ethernet

Команда	Действие
snmp trap link-status	Включает отправку SNMP trap сообщений при изменении состояния настраиваемого порта.
no snmp trap link-status	Выключает отправку SNMP trap сообщений при изменении состояния настраиваемого порта.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 5.134 – Команды режима Privileged EXEC

Команда	Действие
show snmp	Показывает статус SNMP-соединений.
show snmp engineID	Показывает идентификатор локального SNMP-устройства – engineID.
show snmp views [<i>viewname</i>]	Показывает правила обозрения SNMP.
show snmp groups [<i>groupname</i>]	Показывает SNMP-группы.
show snmp filters [<i>filtername</i>]	Показывает SNMP-фильтры.
show snmp users [<i>username</i>]	Показывает SNMP-пользователей.

Примеры выполнения команд

Установить значения для параметров contact, location. Установить доступ на чтение для строки сообщества public. Установить доступ на чтение и запись SNMP-серверу с адресом 192.168.16.3 в сообществе private.

```
console# configure
console (config)# snmp-server enable
console (config)# snmp-server contact support@eltex.nsk.ru
console (config)# snmp-server location Objedineniya-street, 9
console (config)# snmp-server community-string public ro
console (config)# snmp-server community-string private rw 192.168.16.3
```

5.18.5 Протокол удалённого мониторинга сети (RMON)

Протокол мониторинга сети (RMON) является расширением протокола SNMP, позволяя предоставить более широкие возможности контроля сетевого трафика. Отличие RMON от SNMP состоит в характере собираемой информации – данные собираемые RMON в первую очередь характеризуют трафик между узлами сети. Информация, собранная агентом, передается в приложение управления сетью.


Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console (config) #
```

Таблица 5.135 – Команды режима глобального конфигурирования

Команда	Значение/Значение по умолчанию	Действие
rmon event <i>index type</i> [community text] [description text] [owner name]	index: 1..65535 community text: 0..127 символов description text: 0..127 символов owner name: строка	Настраивает события, используемые в системе удаленного мониторинга. - index – индекс события; - type – тип уведомления, генерируемого устройством по этому событию: none – не генерировать уведомления, log – генерировать запись в таблице, trap – отсылать SNMP trap, log-trap – генерировать запись в таблице и отсылать SNMP trap; - community - строка сообщества SNMP для пересылки trap; - description – описание события; - owner – имя создателя события.
no rmon event <i>index</i>		Удаляет событие, используемое в системе удаленного мониторинга.
rmon alarm <i>index mib_object_id interval rthreshold fthreshold revent fevent</i> [type type] [startup direction] [owner name]	index: 1..65535 mib_object_id: корректный OID; interval: 1..4294967295 сек rthreshold: 0..4294967295 fthreshold: 0..4294967295 revent: 0..65535 fevent: 0..65535 owner name: строка По умолчанию метод отбора переменных – absolute По умолчанию инструкция для генерации событий rising-falling	Настраивает условия выдачи аварийных сигналов. - index – индекс аварийного события; - mib_object_id – идентификатор переменной части объекта OID; - interval – интервал, в течение которого данные отбираются и сравниваются с восходящей и нисходящей границами; - rthreshold – восходящая граница; - fthreshold – нисходящая граница; - revent – индекс события, которое используется при пересечении восходящей границы; - fevent – индекс события, которое используется при пересечении нисходящей границы; - type – метод отбора указанных переменных и подсчета значения для сравнения с границами: Метод absolute – абсолютное значение выбранной переменной будет сравнено с границей на конце исследуемого интервала; Метод delta – значение выбранной переменной при последнем отборе будет вычтено из текущего значения и разница будет сравнена с границами (разница между значениями переменной в конце и в начале контрольного интервала); - startup – инструкция для генерации событий на первом контрольном интервале. Определяет правила генерации аварийных событий для первого контрольного интервала путем сравнения отобранной переменной с одной, либо обоими границами: - rising – генерировать единичное аварийное событие по восходящей границе, если значение отобранной переменной на первом контрольном интервале больше

		либо равно этой границе; - falling – генерировать единичное аварийное событие по нисходящей границе, если значение отобранной переменной на первом контрольном интервале меньше либо равно этой границе; - rising-falling – генерировать единичное аварийное событие по восходящей и/или нисходящей границе, если значение отобранной переменной на первом контрольном интервале больше либо равно восходящей границе, и/или меньше либо равно нисходящей границе; - owner – имя создателя аварийного события.
no rmon alarm index		Удаляет условие выдачи аварийных событий.
rmon table-size {history entries log entries}	history 20..32767/270 log 20..32767/100	Задает максимальный размер RMON-таблиц. - history – максимальное количество строк в таблице истории; - log – максимальное количество строк в таблице записей.  Значение вступит в силу только после перезагрузки устройства.
no rmon table-size {history log}		Устанавливает значение по умолчанию.

Команды режима конфигурирования интерфейса (диапазона интерфейсов) Ethernet, интерфейса группы портов

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet, интерфейса группы портов:

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

Таблица 5.136 – Команды режима конфигурирования интерфейса Ethernet, группы интерфейсов

Команда	Значение	Действие
rmon collection stats index [owner name buckets bucket_num] [interval interval]	index: 1..65535; name: корректная строка; bucket-num: 1..50/50; interval: 1..3600/1800 сек	Включает формирование истории по группам статистики для базы данных (MIB) удаленного мониторинга. - index – индекс требуемой группы статистики; - name – владелец группы статистики; - bucket_num – значение, ассоциируемое с количеством ячеек для сбора истории по группе статистики; - interval – период опроса для формирования истории.
no rmon collection stats index		Выключает формирование истории по группам статистики для базы данных (MIB) удаленного мониторинга.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Таблица 5.137 – Команды режима EXEC

Команда	Значение	Действие
show rmon statistics { gigabitethernet gi_port fastethernet fa_port port-channel group }	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}	Показывает статистику интерфейса Ethernet, либо группы портов, используемую для удаленного мониторинга.
show rmon collection stats [gigabitethernet gi_port 		Отображает информацию по запрашиваемым группам статистики.

fastethernet fa_port [port-channel group]		
show rmon history index {throughput errors other} [period period]	index: 1..65535 period: 1..2147483647 сек	Показывает историю Ethernet статистики RMON. - index – запрошенная группа статистики; - throughput - показывает счетчики производительности (пропускной способности); - errors - показывает счетчики ошибок; - other - показывает счетчики обрывов и коллизий; - period – показывает историю за запрошенный период времени.
show rmon alarm-table	-	Показывает сводную таблицу аварийных событий.
show rmon alarm number	1..65535	Показывает конфигурацию настройки аварийных событий. - number – индекс аварийного события.
show rmon events	-	Показывает таблицу событий удаленного мониторинга RMON.
show rmon log [event]	0..65535	Показывает таблицу записей удаленного мониторинга RMON. - Event - индекс события.

Примеры выполнения команд

- Показать статистику 10 интерфейса Ethernet первого устройства в стеке:

```
console# show rmon statistics gigabitethernet 1/0/10
```

<pre>Port 1/g10 Dropped: 8 Octets: 878128 Packets: 978 Broadcast: 7 Multicast: 1 CRC Align Errors: 0 Collisions: 0 Undersize Pkts: 0 Oversize Pkts: 0 Fragments: 0 Jabbers: 0 64 Octets: 98 65 to 127 Octets: 0 128 to 255 Octets: 0 256 to 511 Octets: 0 512 to 1023 Octets: 491 1024 to 1518 Octets: 389</pre>
--

Таблица 5.138 - Описание результатов

Параметр	Описание
Dropped	Количество задетектированных событий, когда пакеты были отброшены.
Octets	Количество байт данных (включая байты плохих пакетов), принятых из сети (исключая фреймовые биты, но включая биты контрольной суммы).
Packets	Количество принятых пакетов (включая плохие, широковещательные и многоадресные пакеты).
Broadcast	Количество принятых широковещательных пакетов (только корректные пакеты).
Multicast	Количество принятых многоадресных пакетов (только корректные пакеты).
CRC Align Errors	Количество принятых пакетов длиной от 64 до 1518 байт включительно, имеющих неверную контрольную сумму либо с целым числом байт (ошибки проверки контрольной суммы – FCS), либо с нецелым числом байт (ошибки выравнивания – Alignment).
Collisions	Оценка количества коллизий на данном Ethernet сегменте.
Undersize Pkts	Количество принятых пакетов длиной меньше 64 байт (исключая фреймовые биты, но включая биты контрольной суммы), но в остальном правильно сформированных.

Overize Pkts	Количество принятых пакетов длиной больше 1518 байт (исключая фреймовые биты, но включая биты контрольной суммы), но в остальном правильно сформированных.
Fragments	Количество принятых пакетов длиной меньше 64 байт (исключая фреймовые биты, но включая биты контрольной суммы), имеющих неверную контрольную сумму либо с целым числом байт (ошибки проверки контрольной суммы – FCS), либо с нецелым числом байт (ошибки выравнивания – Alignment).
Jabbers	Количество принятых пакетов длиной больше 1518 байт (исключая фреймовые биты, но включая биты контрольной суммы), имеющих неверную контрольную сумму либо с целым числом байт (ошибки проверки контрольной суммы – FCS), либо с нецелым числом байт (ошибки выравнивания – Alignment).
64 Octet	Количество принятых пакетов (включая плохие пакеты) длиной 64 байта (исключая фреймовые биты, но включая биты контрольной суммы).
65 to 127 Octets	Количество принятых пакетов (включая плохие пакеты) длиной от 65 до 127 байт включительно (исключая фреймовые биты, но включая биты контрольной суммы).
128 to 255 Octets	Количество принятых пакетов (включая плохие пакеты) длиной от 128 до 255 байт включительно (исключая фреймовые биты, но включая биты контрольной суммы).
256 to 511 Octets	Количество принятых пакетов (включая плохие пакеты) длиной от 256 до 511 байт включительно (исключая фреймовые биты, но включая биты контрольной суммы).
512 to 1023 Octets	Количество принятых пакетов (включая плохие пакеты) длиной от 512 до 1023 байт включительно (исключая фреймовые биты, но включая биты контрольной суммы).
1024 to 1518 Octets	Количество принятых пакетов (включая плохие пакеты) длиной от 1024 до 1518 байт включительно (исключая фреймовые биты, но включая биты контрольной суммы).

- Показать информацию по группам статистики для порта 8:

```
console# show rmon collection history gigabitethernet 1/0/8
```

Index	Interface	Interval	Requested Samples	Granted Samples	Owner
1	1/g8	300	50	50	Eltex

Таблица 5.139 - Описание результатов

Параметр	Описание
Index	Индекс, уникально идентифицирующий запись.
Interface	Ethernet-интерфейс, на котором запущен опрос.
Interval	Интервал в секундах между опросами.
Requested Samples	Запрошенное количество отсчетов, которое может быть сохранено.
Granted Samples	Разрешенное (оставшееся) количество отсчетов, которое может быть сохранено.
Owner	Владелец данной записи.

- Показать счетчики пропускной способности для группы статистики 1:

```
console# show rmon history 1 throughput
```

Sample set: 1	Owner: MES				
Interface: 1/g1	Interval: 1800				
Requested samples: 50	Granted samples: 50				
Maximum table size: 100					
Time	Octets	Packets	Broadcast	Multicast	%
Nov 10 2009 18:38:00	204595549	278562	2893	675218.67%	

Таблица 5.140 - Описание результатов

Параметр	Описание
Time	Дата и время создания записи.
Octets	Количество байт данных (включая байты плохих пакетов) принятых из сети (исключая фреймовые биты, но включая биты контрольной суммы).
Packets	Количество принятых пакетов (включая плохие пакеты) в течение периода формирования записи.
Broadcast	Количество принятых хороших пакетов в течение периода формирования записи направленных на широковещательные адреса.
Multicast	Количество принятых хороших пакетов в течение периода формирования записи направленных на многоадресные адреса.
Utilization	Оценка средней пропускной способности физического уровня на данном интерфейсе в течение периода формирования записи. Пропускная способность оценивается величиной до тысячной процента.
CRC Align	Количество принятых в течение периода формирования записи пакетов длиной от 64 до 1518 байт включительно, имеющих неверную контрольную сумму либо с целым числом байт (ошибки проверки контрольной суммы – FCS), либо с нецелым числом байт (ошибки выравнивания – Alignment).
Collisions	Оценка количества коллизий на данном Ethernet сегменте в течение периода формирования записи.
Undersize Pkts	Количество принятых в течение периода формирования записи пакетов длиной меньше 64 байт (исключая фреймовые биты, но включая биты контрольной суммы), но в остальном правильно сформированных.
Oversize Pkts	Количество принятых в течение периода формирования записи пакетов длиной больше 1518 байт (исключая фреймовые биты, но включая биты контрольной суммы), но в остальном правильно сформированных.
Fragments	Количество принятых в течение периода формирования записи пакетов длиной меньше 64 байт (исключая фреймовые биты, но включая биты контрольной суммы), имеющих неверную контрольную сумму либо с целым числом байт (ошибки проверки контрольной суммы – FCS), либо с нецелым числом байт (ошибки выравнивания – Alignment).
Jabbers	Количество принятых в течение периода формирования записи пакетов длиной больше 1518 байт (исключая фреймовые биты, но включая биты контрольной суммы), имеющих неверную контрольную сумму либо с целым числом байт (ошибки проверки контрольной суммы – FCS), либо с нецелым числом байт (ошибки выравнивания – Alignment).
Dropped	Количество задетектированных событий, когда пакеты были отброшены в течение периода формирования записи.

- Показать сводную таблицу сигналов тревоги:

```
console# show rmon alarm-table
```

Index	OID	Owner
1	1.3.6.1.2.1.2.2.1.10.1	CLI
2	1.3.6.1.2.1.2.2.1.10.1	Manager

Таблица 5.141 - Описание результатов

Параметр	Описание
Index	Индекс, уникально идентифицирующий запись
OID	OID контролируемой переменной
Owner	Пользователь, создавший запись.

```
console# show rmon alarm 1
```

Alarm 1 ----- OID: 1.3.6.1.2.1.2.2.1.10.1 Last sample Value: 878128 Interval: 30 Sample Type: delta Startup Alarm: rising Rising Threshold: 8700000 Falling Threshold: 78 Rising Event: 1 Falling Event: 1 Owner: CLI
--

Таблица 5.142 - Описание результатов

Параметр	Описание
OID	OID контролируемой переменной.
Last Sample Value	Значение переменной на последнем контрольном интервале. Если метод отбора переменных absolute – то это абсолютное значение переменной, если delta – то разница между значениями переменной в конце и в начале контрольного интервала.
Interval	Интервал в секундах, в течение которого данные отбираются и сравниваются с верхней и нижней границами.
Sample Type	Метод отбора указанных переменных и подсчета значения для сравнения с границами. Метод absolute – абсолютное значение выбранной переменной будет сравнено с границей на конце исследуемого интервала. Метод delta – значение выбранной переменной при последнем отборе будет вычтено из текущего значения, и разница будет сравнена с границами (разница между значениями переменной в конце и в начале контрольного интервала).
Startup Alarm	Инструкция для генерации событий на первом контрольном интервале. Определяет правила генерации аварийных событий для первого контрольного интервала путем сравнения отобранной переменной с одной, либо обеими границами. rising – генерировать единичное аварийное событие по восходящей границе, если значение отобранной переменной на первом контрольном интервале больше либо равно этой границе. falling – генерировать единичное аварийное событие по нисходящей границе,

	если значение отобранной переменной на первом контрольном интервале меньше либо равно этой границе. rising-falling – генерировать единичное аварийное событие по восходящей и/или нисходящей границе, если значение отобранной переменной на первом контрольном интервале больше либо равно восходящей границе, и/или меньше либо равно нисходящей границе.
Rising Threshold	Значение восходящей границы. Когда значение отобранной переменной на предыдущем контрольном интервале было меньше данной границы, а на текущем контрольном интервале больше либо равно значению границы, тогда единичное событие генерируется.
Falling Threshold	Значение нисходящей границы. Когда значение отобранной переменной на предыдущем контрольном интервале было больше данной границы, а на текущем контрольном интервале меньше либо равно значению границы, тогда единичное событие генерируется.
Rising Event	Индекс события используемого, когда восходящая граница пересечена.
Falling Event	Индекс события используемого, когда нисходящая граница пересечена.
Owner	Пользователь, создавший запись.

- Показать таблицу событий удаленного мониторинга RMON:

```
console# show rmon events
```

Index	Description	Type	Community	Owner	Last time sent
1	Errors	Log		CLINov 10	2009 18:47:17
2	High Broadcast	Log-Trap	router	Manager	Nov 10 2009 18:48:48

Таблица 5.143 – Описание результатов

<i>Параметр</i>	<i>Описание</i>
Index	Индекс, уникально идентифицирующий событие.
Description	Комментарий, описывающий событие.
Type	Тип уведомления, генерируемого устройством по этому событию: none – не генерировать уведомления, log – генерировать запись в таблице, trap – отсылать SNMP trap, log-trap – генерировать запись в таблице и отсылать SNMP trap.
Community	Строка сообщества SNMP для пересылки trap.
Owner	Пользователь, создавший событие.
Last time sent	Время и дата генерирования последнего события. Если не было сгенерировано событий, то это значение будет равно нулю.

- Показать таблицу записей удаленного мониторинга RMON:

```
console# show rmon log
```

Maximum table size: 100		
Event	Description	Time
1	Errors	Nov 10 2009 18:48:33

Таблица 5.144 – Описание результатов

<i>Параметр</i>	<i>Описание</i>
Index	Индекс, уникально идентифицирующий запись.
Description	Комментарий, описывающий событие.
Time	Время создания записи.

5.18.6 Списки доступа ACL для управления устройством

Программное обеспечение коммутатора MES1024/MES1124/MES2124 позволяет разрешить, либо ограничить доступ к управлению устройством через определенные порты или группы VLAN. Для этой цели создаются списки доступа (ACL) для управления.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console (config) #
```

Таблица 5.145 – Команды режима глобального конфигурирования

<i>Команда</i>	<i>Значение</i>	<i>Действие</i>
management access-list <i>name</i>	1..32 символа	Создает список доступа для управления. Вход в режим конфигурирования списка доступа для управления.
no management access-list <i>name</i>		Удаляет список доступа для управления.
management access-class { console-only <i>name</i> }	1..32 символа	Ограничивает управление устройством по определенному списку доступа (access list). Активирует указанный список доступа. - console-only – управление устройством доступно только с консоли.
no management access-class		Отменяет ограничение на управление устройством по определенному списку доступа (access list).

Команды режима конфигурирования списка доступа для управления

Вид запроса командной строки в режиме конфигурирования списка доступа для управления:

```
console (config) # management access-list eltex_manag  
console (config-macl) #
```

Таблица 5.146 – Команды режима конфигурирования списка доступа для управления

<i>Команда</i>	<i>Значение</i>	<i>Действие</i>
permit [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> vlan <i>vlanID</i>] [service <i>service</i>]	<i>gi_port</i> : {1..8/0/1..28}; <i>fa_port</i> : {1..8/0/1..24}; <i>group</i> : {1..8}; VLAN ID [1..4094]	Задаёт разрешающее условие для управляющего списка доступа. - <i>service</i> – тип доступа – Telnet, SSH, SNMP, HTTP, HTTPS.
permit ip-source { <i>ipv4-address</i> <i>ipv6-address/prefix-length</i> } [mask { <i>mask</i> <i>prefix-length</i> }] [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-		

<code>channel group vlan vlanID</code> <code>[service service]</code>		
deny <code>[gigabitethernet gi_port fastethernet fa_port port-channel group vlan vlanID]</code> <code>[service service]</code>	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}; VLAN ID [1..4094]	Задаёт запрещающее условие для управляющего списка доступа. - service – тип доступа – Telnet, SSH, SNMP, HTTP, HTTPS.
deny ip-source {ipv4-address ipv6-address/ prefix-length} [mask {mask prefix-length}] <code>[gigabitethernet gi_port fastethernet fa_port port-channel group vlan vlanID]</code> <code>[service service]</code>		

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 5.147 – Команды режима Privileged EXEC

Команда	Действие
<code>show management access-list</code> <code>[name]</code>	Показывает списки доступа (access list) для управления.
<code>show management access-class</code>	Показывает информацию об активных списках доступа (access list) для управления.

5.18.7 Настройка доступа

5.18.7.1 Telnet, SSH, HTTP и FTP

Данные команды предназначены для настройки серверов доступа для управления коммутатором. Поддержка серверов TELNET и SSH коммутатором позволяет удаленно подключиться к нему для мониторинга и конфигурирования.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console (config) #
```

Таблица 5.148 – Команды режима глобального конфигурирования

Команда	Значение/Значение по умолчанию	Действие
<code>ip telnet server</code>	По умолчанию Telnet сервер включен.	Разрешает удаленное конфигурирование устройства через Telnet.
<code>no ip telnet server</code>		Запрещает удаленное конфигурирование устройства через Telnet.
<code>ip ssh server</code>	По умолчанию SSH сервер включен.	Разрешает удаленное конфигурирование устройства через SSH. До тех пор, пока ключ для шифрования не сгенерирован, SSH-сервер будет находиться в

		резерве. После генерации ключа (используемые команды <code>crypto key generate rsa</code> и <code>crypto key generate dsa</code>) сервер перейдет в рабочее состояние.
<code>no ip ssh server</code>		Запрещает удаленное конфигурирование устройства через SSH.
<code>ip ssh port</code> <i>port-number</i>	(1..65535)/22	TCP-порт, используемый SSH-сервером.
<code>no ip ssh port</code>		Устанавливает значение по умолчанию.
<code>ip ssh pubkey-auth</code>	По умолчанию использование публичного ключа запрещено	Разрешает использование публичного ключа для входящих SSH-сессий.
<code>no ip ssh pubkey-auth</code>		Запрещает использование публичного ключа для входящих SSH-сессий.
<code>crypto key pubkey-chain ssh</code>	По умолчанию ключ не создан	Вход в режим конфигурации публичного ключа.
<code>crypto key generate dsa</code>		Генерирует пару ключей DSA – частный и публичный для SSH-сервиса. <input checked="" type="checkbox"/> Если хотя бы один из пары ключей уже создан, то система предложит перезаписать ключ.
<code>crypto key generate rsa</code>		Генерирует пару ключей RSA – частный и публичный для SSH-сервиса. <input checked="" type="checkbox"/> Если хотя бы один из пары ключей уже создан, то система предложит перезаписать ключ.
<code>ip ftp server</code>	По умолчанию FTP-сервер включен	Включает FTP-сервер
<code>no ip ftp server</code>		Отключает FTP-сервер
<code>ip http port</code> <i>port</i>	1..65535/80	Задает сокет HTTP-сервера
<code>no ip http port</code>		Восстанавливает значение по умолчанию
<code>ip http secure-port</code> <i>port</i>	1..65535/443	Задает сокет HTTPS-сервера
<code>no ip http secure-port</code>		Восстанавливает значение по умолчанию
<code>ip http secure-server</code>	По умолчанию HTTPS-сервер выключен	Включает HTTPS-сервер
<code>no ip http secure-server</code>		Выключает HTTPS-сервер
<code>ip http server</code>	По умолчанию HTTP-сервер включен	Включает HTTP-сервер
<code>no ip http server</code>		Выключает HTTP-сервер
<code>ip http timeout-policy</code> <i>seconds</i>	0..86400/600	Задает таймаут HTTP-сессии
<code>no ip http timeout-policy</code>		Восстанавливает значение по умолчанию
<code>ip https certificate {1 2}</code>	1	Определяет активный HTTPS-сертификат
<code>crypto certificate {1 2} generate</code>		Генерирует SSL-сертификат
<code>crypto certificate {1 2} import</code>		Импортирует SSL-сертификат, назначенный центром сертификации



Ключи, сгенерированные командами `crypto key generate rsa` и `crypto key generate dsa`, сохраняются в закрытом для пользователя файле конфигурации.

Команды режима конфигурирования публичного ключа

Вид запроса командной строки в режиме конфигурирования публичного ключа:

```
console# configure
console(config)# crypto key pubkey-chain ssh
console(config-pubkey-chain)#
```

Таблица 5.149 – Команды режима конфигурирования публичного ключа


Команда	Значение	Действие
<code>user-key {rsa dsa}</code> <i>username</i>	1..48 символов	Вход в режим создания индивидуального публичного ключа.

		- rsa – создать RSA-ключ; - dsa – создать DSA-ключ.
<code>no user-key username</code>		Удаляет публичный ключ для определенного пользователя.

Вид запроса командной строки в режиме создания индивидуального публичного ключа:

```
console# configure
console(config)# crypto key pubkey-chain ssh
console(config-pubkey-chain)# user-key eltex rsa
console(config-pubkey-key)#
```

Таблица 5.150 – Команды режима создания индивидуального публичного ключа

<i>Команда</i>	<i>Действие</i>
<code>key-string</code>	Создает публичный ключ для определенного пользователя.
<code>key-string row key-string</code>	Создает публичный ключ для определенного пользователя. Ввод ключа осуществляется построчно. - key-string – часть ключа.  Для того чтобы система поняла, что ключ введен полностью, необходимо ввести команду key-string row без символов.

Команды режима EXEC

Команды данного раздела доступны только для привилегированных пользователей.

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.151 – Команды режима EXEC

<i>Команда</i>	<i>Значение</i>	<i>Действие</i>
<code>show ip ssh</code>	-	Показывает конфигурацию SSH-сервера, а также активные входящие SSH-сессии.
<code>show crypto key pubkey-chain ssh [username username] [fingerprint {bubble-babble hex}]</code>	1..48 символов. По умолчанию отпечаток ключа в шестнадцатеричном формате.	Показывает публичные SSH-ключи, сохраненные на коммутаторе. - username – имя удаленного клиента; - bubble-babble – отпечаток ключа в коде Bubble Babble; - hex – отпечаток ключа в шестнадцатеричном коде.
<code>show crypto key mypubkey [rsa dsa]</code>	-	Показывает публичные ключи SSH-коммутатора.
<code>show crypto certificate mycertificate [1 2]</code>	-	Отображает SSL-сертификаты для HTTPS-сервера
<code>show ip http</code>	-	Отображает состояние HTTP-сервера
<code>show ip https</code>	-	Отображает состояние HTTPS-сервера

Примеры выполнения команд

Включить сервер SSH на коммутаторе. Разрешить использование публичных ключей. Создать RSA-ключ для пользователя **eltex**:

```
console# configure
console(config)# ip ssh server
console(config)# ip ssh pubkey-auth
```

```
console(config)# crypto key pubkey-chain ssh
console(config-pubkey-chain)# user-key eltex rsa
console(config-pubkey-key)# key-string AAAAB3NzaC1yc2EAAAADAQABAAQ=CvTnRw
Pw1A14kpqIw9GBRonZQZxjHKcQKL6rM1Q+ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+Vu4GR
fpSwoQUvV35LqJJk67IOU/zfwO11gkTwm175QR9gHujS6KwGN2QWXgh3ub8gDjTSqmuSn/Wd05i
DX2IExQWu08licglk02LYciz+Z4TrEU/9FJxwPivQOjC+KBXuR0juNg5nFYsY0ZCk0N/W9a/tnk
m1shRE7Di71+w3fNiOA6w9o44t6+AINEICBCCA4YcF6zMzaT1wefWwX6f+Rmt5nhhqAtN/4oJf
ce166DqVX1gWmNzNR4DYDvSzg01DnwCAC8Qh
```

Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9

5.18.7.2 Команды конфигурирования терминала

Команды конфигурирования терминала служат для настройки параметров локальной и удаленной консоли.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.152 – Команды режима глобального конфигурирования

<i>Команда</i>	<i>Действие</i>
line {console telnet ssh}	Вход в режим соответствующего терминала (локальная консоль, удаленная консоль – Telnet или удаленная защищенная консоль – SSH).

Команды режима конфигурирования терминала

Вид запроса командной строки в режиме конфигурирования терминала

```
console# configure
console(config)# line {console|telnet|ssh}
console(config-line)#
```

Таблица 5.153 – Команды режима конфигурирования терминала

<i>Команда</i>	<i>Значение</i>	<i>Действие</i>
speed <i>bps</i>	2400, 9600, 19200, 38400, 57600, 115200/9600 бод	Устанавливает скорость доступа по локальной консоли (команда доступна только в режиме конфигурирования локальной консоли).
no speed		Устанавливает значение по умолчанию.
autobaud	-	Включает автоматическое определение скорости доступа по локальной консоли (команда доступна только в режиме конфигурирования локальной консоли).
no autobaud		Выключает автоматическое определение скорости доступа по локальной консоли.
exec-timeout <i>minutes</i> [<i>seconds</i>]	<i>minutes</i> : 0..65535 мин <i>seconds</i> : 0..59 сек	Задаёт интервал, в течение которого система ожидает ввода пользователя. Если в течение данного интервала пользователь ничего не вводит, то консоль отключается.
no exec-timeout	По умолчанию 10 минут	Устанавливает значение по умолчанию.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.154 – Команды режима EXEC

<i>Команда</i>	<i>Действие</i>
show line [console telnet ssh]	Показывает параметры терминала.

5.19 Журнал аварий, протокол SYSLOG


Системные журналы позволяют вести историю событий, произошедших на устройстве, а также контролировать произошедшие события в реальном времени. В журнал заносятся события семи типов: чрезвычайные, сигналы тревоги, критические и не критические ошибки, предупреждения, уведомления, информационные и отладочные.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console (config) #
```

Таблица 5.155 - Команды режима глобальной конфигурации

<i>Команда</i>	<i>Значение/Значение по умолчанию</i>	<i>Действие</i>
logging on	-/ регистрация включена	Включает регистрацию отладочных сообщений и сообщений об ошибках.
no logging on		Выключает регистрацию отладочных сообщений и сообщений об ошибках.  При выключенной регистрации отладочные сообщения и сообщения об ошибках будут передаваться на консоль.
logging host {ipaddr host} [port port] [severity level] [facility facility] [description text]	host {1..158} символов; port [1..65535]/514; level [см. табл. 6.101]; facility [local0..7]/ local7; text [1..64] символа	Включает передачу аварийных и отладочных сообщений на удаленный SYSLOG сервер. - ipaddr – IPv4 или IPv6-адрес SYSLOG-сервера; - host – сетевое имя SYSLOG-сервера; - port – номер порта для передачи сообщений по протоколу SYSLOG; - level – уровень важности сообщений, передаваемых на SYSLOG-сервер; - facility – услуга, передаваемая в сообщениях; - text – описание SYSLOG-сервера.
no logging host {ipaddr host}		Удаляет выбранный сервер из списка используемых SYSLOG-серверов.
logging console level	level [см. табл. 5.156]	Включает передачу аварийных или отладочных сообщений выбранного уровня важности на консоль.
no logging console	Значение по умолчанию - informational	Выключает передачу аварийных или отладочных сообщений на консоль.
logging buffered [severity-level]	level [см. табл. 5.156]	Включает передачу аварийных или отладочных сообщений выбранного уровня важности во внутренний буфер.
no logging buffered	Значение по умолчанию - informational	Выключает передачу аварийных или отладочных сообщений во внутренний буфер.

logging buffered size size	20-400/200	Изменяет количество сообщений, запоминаемых во внутреннем буфере. Новое значение размера буфера применится после перезагрузки устройства.
no logging buffered size		Устанавливает значение по умолчанию.
logging file level	level [см. табл. 5.156]	Включает передачу аварийных или отладочных сообщений выбранного уровня важности в файл журнала.
no logging file	Значение по умолчанию - errors	Выключает передачу аварийных или отладочных сообщений в файл журнала.
aaa logging login	-/enable	Заносить в журналы события аутентификации, авторизации и учета (AAA).
no aaa logging login		Не заносить в журналы события аутентификации, авторизации и учета (AAA).
file-system logging {copy delete-rename}	По умолчанию регистрация включена	Включает регистрацию событий файловой системы. - copy – регистрация сообщений, связанных с операциями копирования файлов; - delete-rename – регистрация сообщений, связанных с удалением файлов и переименованием операций.
no file-system logging {copy delete-rename}		Выключает регистрацию событий файловой системы.
management logging deny	По умолчанию регистрация включена	Включает регистрацию событий доступа управления.
no management logging deny		Выключает регистрацию событий доступа управления.
logging aggregation on	-	Включает контроль агрегации syslog-сообщений.
no logging aggregation on		Отключает агрегацию syslog-сообщений.
logging aggregation aging-time sec	15–3600	Устанавливает время хранения сгруппированных syslog-сообщений.
no logging aggregation aging-time		Устанавливает значение по умолчанию.
logging cli-commands	По умолчанию ведение учета запрещено	Разрешает ведение учета (аккаунта) для введенных в CLI команд.
no logging cli-commands		Устанавливает значение по умолчанию.

Каждое сообщение имеет свой уровень важности, в таблице 6.101 приведены типы сообщений в порядке убывания их важности.

Таблица 5.156 – Типы важности сообщений

Тип важности сообщений	Описание
<i>Чрезвычайные (emergencies)</i>	В системе произошла критическая ошибка, система может работать неправильно.
<i>Сигналы тревоги (alerts)</i>	Необходимо немедленное вмешательство в систему.
<i>Критические (critical)</i>	В системе произошла критическая ошибка.
<i>Ошибочные (errors)</i>	В системе произошла ошибка.
<i>Предупреждения (warnings)</i>	Предупреждение, неаварийное сообщение.
<i>Уведомления (notifications)</i>	Уведомление системы, неаварийное сообщение.
<i>Информационные (informational)</i>	Информационные сообщения системы.
<i>Отладочные</i>	Отладочные сообщения, предоставляют пользователю информацию для

<i>(debugging)</i>	корректной настройки системы.
--------------------	-------------------------------

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 5.157 - Команда режима Privileged EXEC для просмотра файла журнала

<i>Команда</i>	<i>Действие</i>
<code>clear logging</code>	Удаляет все сообщения из внутреннего буфера.
<code>clear logging file</code>	Удаляет все сообщения из файла журнала.
<code>show logging file</code>	Отображает состояние журнала, аварийные и отладочные сообщения, записанные в файле журнала.
<code>show logging</code>	Отображает состояние журнала, аварийные и отладочные сообщения, записанные во внутреннем буфере.
<code>show syslog-servers</code>	Отображает настройки для удалённых syslog-серверов.

Примеры использования команд

- Включить регистрацию ошибочных сообщений на консоли:

```
console# configure
console (config)# logging on
console (config)# logging console errors
```

- Очистить файл журнала:

```
console# clear logging file
Clear Logging File [y/n]y
```

5.20 Зеркалирование (мониторинг) портов

Функция зеркалирования портов предназначена для контроля сетевого трафика путем пересылки копий входящих и/или исходящих пакетов с одного или нескольких контролируемых портов на один контролирующий порт.

К контролирующему порту применяются следующие ограничения:

- Порт не может быть контролирующим и контролируемым портом одновременно;
- Порт не может быть членом группы портов;
- IP-интерфейс не сконфигурирован для этого порта;
- Протокол GVRP должен быть выключен на этом порту.

К контролируемым портам применяются следующие ограничения:

- Порт не может быть контролирующим и контролируемым портом одновременно;
- Порт не может быть членом группы портов.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console (config) #
```

Таблица 5.158 - Команды режима глобальной конфигурации

Команда	Значение/Значение по умолчанию	Действие
<code>port monitor mode {monitor-only network}</code>	-/monitor-only	Задаёт режим работы порта monitor-only – фреймы, поступающие на порт, отбрасываются; network – позволяет вести обмен данными.
<code>port monitor remote vlan vlan_id [cos priority] [tx rx]</code>	vlan_id: 1..4094	Определение VLAN для удаленного мониторинга.
<code>port monitor remote vlan vlan_id</code>	cos: 0..7	Удаление VLAN для удаленного мониторинга.

Команды режима конфигурирования интерфейса Ethernet

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet:

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



Данные команды нельзя выполнять в режиме конфигурирования диапазона интерфейсов Ethernet.

Таблица 5.159 - Команды доступные в режиме конфигурирования интерфейса Ethernet

Команда	Значение/Значение по умолчанию	Действие
<code>port monitor {gigabitethernet gi_port fastethernet fa_port} [rx tx]</code>	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}	Включает функцию мониторинга на настраиваемом интерфейсе. Данный интерфейс будет контролирующим портом для указанного в команде контролируемого порта. - gi_port/fa_port – контролируемый порт; - rx – копировать пакеты принятые контролируемым портом; - tx – копировать пакеты, переданные контролируемым портом; При отсутствии параметра rx/tx с контролируемого порта копируются все пакеты.
<code>no port monitor { gigabitethernet gi_port fastethernet fa_port}</code>		Выключает функцию мониторинга на настраиваемом интерфейсе. Данный интерфейс больше не будет контролирующим портом для указанного в команде контролируемого порта.
<code>port monitor vlan {id}</code>	id: {1..4096}	Включает функцию мониторинга на настраиваемом интерфейсе. Данный интерфейс будет контролирующим портом для указанной VLAN.
<code>no port monitor vlan {id}</code>		<input checked="" type="checkbox"/> Порт мониторинга не должен принадлежать к настраиваемой VLAN Удаляет указанную VLAN из мониторинга.
<code>port monitor remote</code>		Включает функцию удаленного мониторинга на настраиваемом интерфейсе.
<code>no port monitor remote</code>		Выключает функцию удаленного мониторинга на настраиваемом интерфейсе.

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 5.160 – Команды, доступные в режиме EXEC

<i>Команда</i>	<i>Действие</i>
show ports monitor	Выводит информацию по контролирующим и контролируемым портам.

Примеры выполнения команд

- Установить 13 Ethernet интерфейс контролирующим для 18 интерфейса Ethernet. Весь трафик с 18 интерфейса передавать на 13.

```
console# configure
console(config)# interface gigabitethernet 1/0/13
console(config-if)# port monitor gigabitethernet 1/0/18
```

- Вывести информацию по контролирующим и контролируемым портам.

```
console# show ports monitor
```

Source Port	Destination Port	Type	Status
g18	g13	RX, TX	notReady

5.21 Функция SFlow

SFlow – технология, позволяющая мониторить трафик в пакетных сетях передачи данных путем частичной выборки трафика для последующей инкапсуляции в специальные сообщения, передаваемые на сервер сбора статистики.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 5.161 - Команды режима глобальной конфигурации

<i>Команда</i>	<i>Значение/Значение по умолчанию</i>	<i>Действие</i>
sflow receiver id {IPv4 IPv6 IPv6z url} [port port] [max-datagram-size byte]	Id: {1 .. 8} port: {1 .. 65535} / 6343 byte: положительное целое число /1400 формат IPv4: A.B.C.D IPv6: X:X:X:X:X IPv6z: X:X:X:X::X%<ID>	Задает адрес сервера сбора статистики sflow. - id – номер sflow-сервера; - IPv4, IPv6, IPv6z – IP-адрес; - url – доменное имя хоста; - port – номер порта; - byte – максимальное количество байт, которое может быть отправлено в один пакет данных.
no sflow receiver id		Удаляет адрес сервера сбора статистики sflow

Команды режима конфигурирования интерфейса Ethernet

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet:

```
console# configure
console(config)# interface {gigabitethernet gi_port| fastethernet fa_port}
console(config-if)#
```

Таблица 5.162 – Команды режима конфигурирования интерфейса Ethernet

Команда	Значение/Значение по умолчанию	Действие
sflow flow-sampling <i>rate id</i> [<i>max-header-size bytes</i>]	<i>rate</i> : {0, 1024..107374823} <i>id</i> : {0 .. 8} <i>bytes</i> : {20 .. 256} /128	Задаёт среднюю скорость выборки пакетов. Итоговая скорость выборки считается как 1/ <i>rate</i> * <i>current_spped</i> (<i>current_speed</i> – текущая средняя скорость). - <i>rate</i> – средняя скорость выборки пакетов; - <i>id</i> – номер sflow-сервера; - <i>bytes</i> – максимальное количество байт, которое будет скопировано из образца пакета.
no sflow flow-sampling		Отключает счетчики выборки на порту.
sflow counters-sampling <i>sec id</i>	<i>sec</i> : {0, 15 .. 86400} <i>id</i> : {0 .. 8}	Определяет максимальный интервал между успешными выборками пакетов. - <i>sec</i> - максимальный интервал между выборками, секунды. Значение «0» отключает выборку; - <i>id</i> - номер sflow-сервера (задается командой sflow receiver в глобальном режиме конфигурации).
no sflow counters-sampling		Отключает счетчики выборки на порту.

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 5.163 – Команды, доступные в режиме EXEC

Команда	Значение/Значение по умолчанию	Действие
show sflow configuration [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i>]		Выводит настройки sflow.
clear sflow statistics [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i>]	<i>gi_port</i> : {1..8/0/1..28}; <i>fa_port</i> : {1..8/0/1..24}.	Очищает статистику sFlow. Если интерфейс не указан, команда очищает все счетчики статистики sFlow.
show sflow statistics [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i>]		Отображает статистику sFlow

Примеры выполнения команд

- Установить IP-адрес 10.0.80.1 сервера 1 для сбора статистики sflow. Для ethernet-интерфейсов g1-g24 установить среднюю скорость выборки пакетов - 10240 кбит/с и максимальный интервал между успешными выборками пакетов – 240 с.

```
console# configure
console(config)# sflow receiver 1 10.0.80.1
console(config)# interface range gigabitethernet 1/0/1-24
console(config-if-range)# sflow flowing-sample 1 10240
console (config-if)# sflow counters-sampling 240 1
```

5.22 Функции диагностики физического уровня

Сетевой коммутатор MES1024/MES1124/MES2124 содержит аппаратные и программные средства для диагностики физических интерфейсов и линий связи. В перечень тестируемых параметров входят следующие:

Для электрических интерфейсов:

- длина кабеля;
- расстояние до места неисправности – обрыва или замыкания.

Для оптических интерфейсов:

- параметры питания – напряжение и ток;
- выходная оптическая мощность;
- оптическая мощность на приеме.

5.22.1 Диагностика медного кабеля



Оценка длины кабеля при использовании команды `'show cable-diagnostics cable-length'` выполняется по величине затухания сигнала. Функция `green-ethernet`, поддерживаемая коммутатором, уменьшает уровень передаваемого сигнала при отсутствии активности на линии и поэтому корректное измерение длины кабеля становится невозможным на устройстве, принимающем ослабленный сигнал. В связи с этим необходимо на время измерений длины кабеля отключать режим `green-ethernet` на удаленном устройстве.

По умолчанию на коммутаторах серии MES1024/MES1124/MES2124 режим `green-ethernet` включен. Допустимая погрешность измерения определяется разбросом параметров линии и составляет 6м

Команды режима `privileged EXEC`

Вид запроса командной строки режима `privileged EXEC`:

```
console#
```

Таблица 5.164 - Команды диагностики медного кабеля


Команда	Значение	Действие
<code>test cable-diagnostics tdr interface {gigabitethernet gi_port fastethernet fa_port}</code>	<code>gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}.</code>	Выполняет виртуальное тестирование кабеля для указанного интерфейса.

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 5.165 - Команды диагностики медного кабеля

Команда	Значение	Действие
show cable-diagnostics tdr [interface gigabitethernet gi_port interface fastethernet fa_port]	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}.	Отображает результаты последнего виртуального тестирования кабеля для указанного интерфейса (если номер порта не задан, то команда выполняется для всех портов).
show cable-diagnostics cable-length [interface gigabitethernet gi_port interface fastethernet fa_port]		Отображает предположительную длину кабеля, подключенного к указанному интерфейсу (если номер порта не задан, то команда выполняется для всех портов).  Интерфейс должен быть активным и работать в режиме 100Мбит/с или 1000Мбит/с.



Максимальная длина кабеля при тестировании не должна составлять более 120 метров.

Примеры выполнения команд

- Протестировать порт 11 первого устройства в стеке:

```
console# test cable-diagnostics tdr interface gigabitethernet 1/0/11
```

```
.console# test cable-diagnostics tdr interface gigabitethernet 1/0/11
.07-Feb-2011 16:22:16 %LINK-W-Down: gi0/11
07-Feb-2011 16:22:16 %LINK-W-Down: Vlan 1
.
Cable on port gi0/11 has short circuit at 2 m
console# 07-Feb-2011 16:22:17 %LINK-I-Up: gi0/11
07-Feb-2011 16:22:17 %LINK-I-Up: Vlan 1
```

- Показать результаты последнего тестирования:

```
console# show cable-diagnostics tdr
```

Port	Result	Length [meters]	Date
gi0/1	Fiber		
gi0/2	Fiber		
gi0/3	Fiber		
gi0/4	Fiber		
gi0/5	Fiber		
gi0/6	Fiber		
gi0/7	Fiber		
gi0/8	Fiber		
gi0/9	Fiber		
gi0/10	Fiber		
gi0/11	Short cable	2	07-Feb-2011 16:22:16
gi0/12	Not tested		
gi0/13	Fiber		
gi0/14	Fiber		
gi0/15	Fiber		
gi0/16	Fiber		
gi0/17	Fiber		
gi0/18	Fiber		
gi0/19	Fiber		
gi0/20	Fiber		
gi0/21	Fiber		

5.22.2 Диагностика оптического трансивера

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 5.166 - Команды режима глобальной конфигурации

Команда	Значение/Значение по умолчанию	Действие
optical-transceiver threshold notify-interval interval	interval: 30-3600 сек/600 сек	Установка промежутка времени до повторной генерации предупреждения/аварии по протоколу syslog/snmp.
no optical-transceiver threshold notify-interval		Установка значения по умолчанию.

Команды режима конфигурирования интерфейса Ethernet

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet:

```
console# configure
console(config)# interface {fastethernet fa_port| gigabitethernet gi_port}
console(config-if)#
```

Таблица 5.167 – Команды режима конфигурирования интерфейса Ethernet

Команда	Значение/Значение по умолчанию	Действие
optical-transceiver threshold action { parameter all }{ none syslog snmp-trap }	parameter: (current, input-power, output-power, temperature, voltage)	Назначаемое действие (не выполнять действий, генерация syslog-сообщения, генерация snmp-трапа), которое должно быть выполнено при превышении указанных порогов для заданного параметра: - current – сила тока; - input-power – мощность входящего сигнала; - output-power – мощность исходящего сигнала; - temperature – температура; - voltage – напряжение.
optical-transceiver threshold values parameter high-alarm high-warning low-warning low-alarm	parameter: (current, input-power, output-power, temperature, voltage) Значения values для: current: (0-131000) uA input-power: (-40000-8200) mdBm output-power: (-40000-8200) mdBm	Указание значений порогов, при превышении которых будет происходить генерация syslog/snmp-trap сообщения для указанного параметра: - current – сила тока; - input-power – мощность входящего сигнала; - output-power – мощность исходящего сигнала; - temperature – температура; - voltage – напряжение.
optical-transceiver threshold values parameter	temperature: (-127-127) °C voltage: (0-6550000) uV	Удаление заданных порогов для указанного параметра. Значения по умолчанию не установлены.

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 5.168 – Команда диагностики оптического трансивера

Команда	Значение	Действие
<code>show fiber-ports optical-transceiver [interface {gigabitethernet gi_port fastethernet fa_port}] [detailed]</code>	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}.	Отображает результаты диагностики оптического трансивера. - detailed – подробная диагностика, еергом-параметры трансивера.

Пример выполнения команды

`sw1#show fiber-ports optical-transceiver interface gi1/0/24 detailed`

Port	Temp [C]	Voltage [V]	Current [mA]	Output Power [mW / dBm]	Input Power [mW / dBm]	LOS	Transceiver Type
gi1/0/24	58	3.25	20.09	0.58 / -2.30	0.00 / -40.00	Yes	Fiber
Temp - Internally measured transceiver temperature Voltage - Internally measured supply voltage Current - Measured TX bias current Output Power - Measured TX output power in milliWatts Input Power - Measured RX received power in milliWatts LOS - Loss of signal N/A - Not Available, N/S - Not Supported, W - Warning, E - Error Transceiver information: Vendor name: OEM Serial number: SX31221300026 Connector type: LC Type: SFP/SFP+ Compliance code: 10GBASE-LR Laser wavelength: 1310 nm Transfer distance: 10000 m Diagnostic: supported							

Таблица 5.169 – Параметры диагностики оптического трансивера

Параметр	Значение
<i>Temp</i>	Температура трансивера.
<i>Voltage</i>	Напряжение питания трансивера.
<i>Current</i>	Отклонение тока на передаче.
<i>Output Power</i>	Выходная мощность на передаче (мВт).
<i>Input Power</i>	Входная мощность на приеме (мВт).
<i>LOS</i>	Потеря сигнала.

При подробной диагностике для параметров Temp, Voltage, Current, Power измеренные значения выводятся на дисплей. При обычной диагностике измеренные значения для этих параметров сравниваются с допустимыми, и на дисплей выводится результат сравнения (W, E, OK).

Значения результатов диагностики и сравнения параметров:

N/A - недоступно,

N/S - не поддерживается,

W - предупреждение,
E – ошибка,
OK – значение в порядке.

5.23 Функции обеспечения безопасности

5.23.1 Функции обеспечения защиты портов

С целью повышения безопасности в коммутаторе существует возможность настроить какой-либо порт так, чтобы доступ к коммутатору через этот порт предоставлялся только заданным устройствам. Функция защиты портов основана на определении MAC-адресов, которым разрешается доступ. MAC-адреса могут быть настроены вручную или изучены коммутатором. После изучения необходимых адресов порт следует заблокировать, защитив его от поступления пакетов с неизученными MAC-адресами. Таким образом, когда заблокированный порт получает пакет, и MAC-адрес источника пакета не связан с этим портом, активизируется механизм защиты, в зависимости от которого могут быть приняты следующие меры: несанкционированные пакеты, поступающие на заблокированный порт, пересылаются, отбрасываются, либо же порт, принявший пакет, отключается. Функция безопасности Locked Port позволяет сохранить список изученных MAC-адресов в файле конфигурации, таким образом, этот список можно восстановить после перезагрузки устройства.



Существует ограничение на количество MAC-адресов, которое может изучить порт использующий функцию защиты. Для коммутатора MES1024/MES1124/MES2124 это ограничение равно 128 адресам на порт.

Команды режима конфигурирования интерфейса (диапазона интерфейсов) Ethernet, интерфейса группы портов

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet, интерфейса группы портов:

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

Таблица 5.170 – Команды режима конфигурирования интерфейса Ethernet, группы интерфейсов

Команда	Значение/Значение по умолчанию	Действие
port security max num	1..128/1	Задаёт максимальное количество адресов, которое может изучить порт.
no port security max		Устанавливает значение по умолчанию.
port security routed secure-address MAC-addr	Формат MAC адреса: H.H.H, H:H:H:H:H:H, H-H-H-H-H-H	Устанавливает защищенный MAC-адрес.
no port security routed secure-address [MAC-addr]		Удаляет защищенный MAC-адрес.
port security	1..1000000 сек	Включает функцию защиты на интерфейсе. Блокирует функцию изучения новых адресов для интерфейса. Пакеты с неизученными MAC-адресами источника отбрасываются. Команда аналогична команде port security discard .
port security forward [trap trap]}		Включает функцию защиты на интерфейсе. Блокирует функцию изучения новых адресов для интерфейса. Пакеты с неизученными MAC-адресами источника пересылаются.

port security discard [trap trap]		Включает функцию защиты на интерфейсе. Блокирует функцию изучения новых адресов для интерфейса. Пакеты с неизученными MAC-адресами источника отбрасываются.
port security discard-shutdown [trap trap]		Включает функцию защиты на интерфейсе. Выключает порт при поступлении пакетов с неизученными MAC-адресами. Пакеты с неизученными MAC-адресами источника отбрасываются.
port security trap trap		Задаёт частоту генерируемых сообщений протокола SNMP trap при поступлении несанкционированных пакетов.
no port security		Выключает функцию защиты на интерфейсе.
port security mode {max-addresses lock}	-/lock	Задаёт режим ограничения изучения MAC-адресов для настраиваемого интерфейса. - max-addresses – удаляет текущие динамически изученные адреса, связанные с интерфейсом. Разрешено изучение максимального количества адресов на порту. Повторное изучение и старение разрешены. - lock – сохраняет в файл текущие динамически изученные адреса, связанные с интерфейсом и запрещает обучение новым адресам и старение уже изученных адресов.
no port security mode		Устанавливает значение по умолчанию.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Таблица 5.171 – Команды режима EXEC

Команда	Значение	Действие
show ports security {gigabitethernet gi_port fastethernet fa_port port- channel group}	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}	Показывает настройки функции безопасности на выбранном интерфейсе.
show ports security addresses {gigabitethernet gi_port fastethernet fa_port port- channel group}	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}	Показывает текущие динамические адреса для заблокированных портов.
set interface active {gigabitethernet gi_port fastethernet fa_port port- channel group}	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: {1..8}	Активизирует интерфейс, отключенный функцией защиты порта (команда доступна только для привилегированного пользователя).

Примеры выполнения команд

- Включить функцию защиты на 15 интерфейсе Ethernet. Установить ограничение на изучение портов – 1 порт. После изучения MAC-адреса заблокировать функцию изучения новых адресов для интерфейса с целью отбросить пакеты с неизученными MAC-адресами источника. Сохранить в файл изученный адрес.

```
console# configure
console(config)# interface gigabitethernet 1/0/15
console(config-if)# port security max 1
```

- Подключить клиента к порту и изучить MAC-адрес.

```
console(config-if) # port security discard
console(config-if) # port security mode lock
```

5.23.2 Проверка подлинности клиента на основе порта (стандарт 802.1x)

5.23.2.1 Базовая проверка подлинности

Аутентификация на основе стандарта 802.1x обеспечивает проверку подлинности пользователей коммутатора через внешний сервер на основе порта, к которому подключен клиент. Только аутентифицированные и авторизованные пользователи смогут передавать и принимать данные. Проверка подлинности пользователей портов выполняется сервером RADIUS посредством протокола EAP (Extensible Authentication Protocol).

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config) #
```

Таблица 5.172 – Команды режима глобального конфигурирования

Команда	Значение/ Значение по умолчанию	Действие
dot1x system-auth-control	-/ force-authorized	Включает режим аутентификации 802.1X на коммутаторе.
no dot1x system-auth-control		Выключает режим аутентификации 802.1X на коммутаторе.
aaa authentication dot1x default {none radius} [none radius]	-/radius	Задаёт один или два метода проверки подлинности, авторизации и учёта (AAA), для использования на интерфейсах IEEE 802.1X. - none – не выполнять аутентификацию; - radius – использовать список RADIUS-серверов для аутентификации пользователя. <input checked="" type="checkbox"/> Второй метод аутентификации используется только в случае, если по первому аутентификация была неуспешной.
no aaa authentication dot1x default		Устанавливает значение по умолчанию.

Команды режима конфигурирования интерфейса Ethernet

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet:

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



Протокол EAP (Extensible Authentication Protocol) выполняет задачи для аутентификации удаленного клиента, при этом определяя механизм аутентификации.

Таблица 5.173 – Команды режима конфигурирования интерфейса Ethernet

Команда	Значение/Значение по умолчанию	Действие
dot1x port-control {auto force-authorized	-/ force-authorized time: {1 .. 32}	Настраивает аутентификацию 802.1X на интерфейсе. Разрешает ручной контроль за состоянием авторизации

force-unauthorized [time-range <i>time</i>]		порта. - auto - использовать 802.1X для изменения состояния клиента между авторизованным и неавторизованным; - force-authorized – выключает аутентификацию 802.1X на интерфейсе. Порт переходит в авторизованное состояние без аутентификации; - force-unauthorized - переводит порт в неавторизованное состояние. Игнорируются все попытки аутентификации клиента, коммутатор не предоставляет сервис аутентификации для этого порта; time – интервал времени. Если данный параметр не определен, то порт не авторизован.
no dot1x port-control		Устанавливает значение по умолчанию.
dot1x reauthentication	-/ периодические повторные проверки подлинности выключены	Включает периодические повторные проверки подлинности (переаутентификацию) клиента.
no dot1x reauthentication		Выключает периодические повторные проверки подлинности (переаутентификацию) клиента.
dot1x timeout reauth-period <i>period</i>	30..4294967295/ 3600 сек	Устанавливает период между повторными проверками подлинности.
no dot1x timeout reauth-period		Устанавливает значение по умолчанию.
dot1x timeout quiet-period <i>period</i>	0..65535/60 сек	Устанавливает период, в течение которого коммутатор остается в состоянии молчания после неудачной проверки подлинности. В течение периода молчания коммутатор не принимает и не иницирует никаких аутентификационных сообщений.
no dot1x timeout quiet-period		Устанавливает значение по умолчанию
dot1x timeout tx-period <i>period</i>	30..65535/30 сек	Устанавливает период, в течение которого коммутатор ожидает ответ на запрос либо идентификацию по протоколу EAP от клиента, перед повторной отправкой запроса.
no dot1x timeout tx-period		Устанавливает значение по умолчанию.
dot1x max-req <i>count</i>	1..10/2	Устанавливает максимальное число попыток передачи запросов протокола EAP-клиенту перед новым запуском процесса проверки подлинности.
no dot1x max-req		Устанавливает значение по умолчанию.
dot1x timeout supp-timeout <i>period</i>	1..65535/30 секунд	Устанавливает период между повторными передачами запросов протокола EAP-клиенту.
no dot1x timeout supp-timeout		Устанавливает значение по умолчанию.
dot1x timeout server-timeout <i>period</i>	1..65535/30 секунд	Устанавливает период, в течение которого коммутатор ожидает ответа от сервера аутентификации.
no dot1x timeout server-timeout		Устанавливает значение по умолчанию.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 5.174 – Команды режима Privileged EXEC

Команда	Значение	Действие
dot1x re-authenticate [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i>]	<i>gi_port</i> : {1..8/0/1..28}; <i>fa_port</i> : {1..8/0/1..24}	Вручную осуществляет повторную проверку подлинности указанного порта в команде, либо всех портов, поддерживающих 802.1X.
show dot1x interface { gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> }	<i>gi_port</i> : {1..8/0/1..28}; <i>fa_port</i> : {1..8/0/1..24}	Показывает состояние 802.1X для коммутатора либо для указанного интерфейса.
show dot1x users	1..160 символов	Показывает активных аутентифицированных

[username username]		пользователей 802.1X коммутатора.
show dot1x statistics interface {gigabitethernet gi_port fastethernet fa_port}	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}	Показывает статистику по 802.1X для выбранного интерфейса.

Примеры выполнения команд

- Включить режим аутентификации 802.1X на коммутаторе. Использовать RADIUS-сервер для проверки подлинности клиентов на интерфейсах IEEE 802.1X. Для 18 интерфейса Ethernet использовать режим аутентификации 802.1x.

```
console# configure
console(config)# dot1x system-auth-control
console(config)# aaa authentication dot1x default radius
console(config)# interface gigabitethernet 1/0/18
console(config-if)# dot1x port-control auto
```

- Показать состояние 802.1X для коммутатора, для 12 интерфейса Ethernet.

```
console# show dot1x
```

```
802.1x is disabled
```

Port	Admin Mode	Oper Mode	Reauth Control	Reauth Period	Username
gi0/1	Force	Authorized	Authorized*	Disabled 3600	n/a
gi0/2	Force	Authorized	Authorized*	Disabled 3600	n/a
gi0/3	Force	Authorized	Authorized*	Disabled 3600	n/a
gi0/4	Force	Authorized	Authorized*	Enabled 3600	n/a
gi0/5	Force	Authorized	Authorized*	Disabled 3600	n/a
gi0/6	Force	Authorized	Authorized*	Disabled 3600	n/a
gi0/7	Force	Authorized	Authorized*	Disabled 3600	n/a
gi0/8	Force	Authorized	Authorized*	Disabled 3600	n/a
gi0/9	Force	Authorized	Authorized*	Disabled 3600	n/a
gi0/10	Force	Authorized	Authorized*	Disabled 3600	n/a
gi0/11	Force	Authorized	Authorized*	Disabled 3600	n/a
gi0/12	Force	Authorized	Authorized*	Disabled 3600	n/a
gi0/13	Force	Authorized	Authorized*	Disabled 3600	n/a
gi0/14	Force	Authorized	Authorized*	Disabled 3600	n/a
gi0/15	Force	Authorized	Authorized*	Disabled 3600	n/a
gi0/16	Force	Authorized	Authorized*	Disabled 3600	n/a

More: <space>, Quit: q, One line: <return>

```
console# show dot1x interface gigabitethernet 1/0/12
```

```
802.1x is disabled
```

Port	Admin Mode	Oper Mode	Reauth Control	Reauth Period	Username
gi0/12	Force	Authorized	Authorized*	Disabled 3600	n/a

* Port is down or not present

```
Quiet period:          60 Seconds
Tx period:             30 Seconds
Max req:               2
Supplicant timeout:   30 Seconds
Server timeout:       30 Seconds
Session Time (HH:MM:SS): 00:00:00
MAC Address:
Authentication Method: Remote
Termination Cause:    Port re-initialize
```

```

Authenticator State Machine
State:                INITIALIZE

Backend State Machine
State:                INITIALIZE
Authentication success: 0
Authentication fails: 0
    
```

Таблица 5.175 – Описание результатов выполнения команд

<i>Параметр</i>	<i>Описание</i>
<i>Port</i>	Номер порта.
<i>Admin mode</i>	Режим аутентификации 802.1X: Force-auth, Force-unauth, Auto.
<i>Oper mode</i>	Операционный режим порта: авторизованный, неавторизованный, либо выключенный (Authorized, Unauthorized, Down).
<i>Reauth Control</i>	Контроль переаутентификации.
<i>Reauth Period</i>	Период между повторными проверками подлинности.
<i>Username</i>	Имя пользователя при использовании 802.1X. Если порт авторизован, то отображается имя текущего пользователя. Если порт не авторизован, то отображается имя последнего успешно авторизованного пользователя на порту.
<i>Quiet period</i>	Период, в течение которого коммутатор остается в состоянии молчания после неудачной проверки подлинности.
<i>Tx period</i>	Период, в течение которого коммутатор ожидает ответ на запрос либо идентификацию по протоколу EAP от клиента, перед повторной отправкой запроса.
<i>Max req</i>	Максимальное число попыток передачи запросов протокола EAP клиенту перед новым запуском процесса проверки подлинности.
<i>Supplicant timeout</i>	Период между повторными передачами запросов протокола EAP клиенту.
<i>Server timeout</i>	Период, в течение которого коммутатор ожидает ответа от сервера аутентификации.
<i>Session Time</i>	Время подключения пользователя к устройству.
<i>Mac address</i>	MAC-адрес пользователя.
<i>Authentication Method</i>	Метод аутентификации установленной сессии.
<i>Termination Cause</i>	Причина закрытия сессии.
<i>State</i>	Текущее значение автомата состояний определителя подлинности и выходного автомата состояний.
<i>Authentication success</i>	Количество полученных сообщений об успешной аутентификации от сервера.
<i>Authentication fails</i>	Количество полученных сообщений о неуспешной аутентификации от сервера.
<i>VLAN</i>	Группа VLAN назначенная пользователю.
<i>Filter ID</i>	Идентификатор группы фильтрации.

- Показать статистику по 802.1X для интерфейса Ethernet 13.

```
console# show dot1x statistics interface gigabitethernet 1/0/13
```

```

EapolFramesRx: 12
EapolFramesTx: 8
EapolStartFramesRx: 1
EapolLogoffFramesRx: 1
EapolRespIdFramesRx: 4
EapolRespFramesRx: 6
EapolReqIdFramesTx: 3
EapolReqFramesTx: 5
InvalidEapolFramesRx: 0
    
```

```
EapLengthErrorFramesRx: 0
LastEapolFrameVersion: 1
LastEapolFrameSource: 00:00:02:56:54:38
```

Таблица 5.176 – Описание результатов выполнения команд

<i>Параметр</i>	<i>Описание</i>
<i>EapolFramesRx</i>	Количество корректных пакетов любого типа протокола EAPOL (Extensible Authentication Protocol over LAN), принятых данным определителем подлинности.
<i>EapolFramesTx</i>	Количество корректных пакетов любого типа протокола EAPOL, переданных данным определителем подлинности.
<i>EapolStartFramesRx</i>	Количество пакетов Start протокола EAPOL, принятых данным определителем подлинности.
<i>EapolLogoffFramesRx</i>	Количество пакетов Logoff протокола EAPOL, принятых данным определителем подлинности.
<i>EapolRespldFramesRx</i>	Количество пакетов Resp/Id протокола EAPOL, принятых данным определителем подлинности.
<i>EapolRespFramesRx</i>	Количество пакетов ответов (кроме Resp/Id) протокола EAPOL, принятых данным определителем подлинности.
<i>EapolReqldFramesTx</i>	Количество пакетов Resp/Id протокола EAPOL, переданных данным определителем подлинности.
<i>EapolReqFramesTx</i>	Количество пакетов запросов (кроме Resp/Id) протокола EAPOL, переданных данным определителем подлинности.
<i>InvalidEapolFramesRx</i>	Количество пакетов протокола EAPOL с нераспознанным типом, принятых данным определителем подлинности.
<i>EapLengthErrorFramesRx</i>	Количество пакетов протокола EAPOL с некорректной длиной, принятых данным определителем подлинности.
<i>LastEapolFrameVersion</i>	Версия протокола EAPOL, принятая в самом последнем на данный момент пакете.
<i>LastEapolFrameSource</i>	MAC-адрес источника, принятый в самом последнем на данный момент пакете.

5.23.2.2 Расширенная проверка подлинности.


Расширенные настройки dot1x позволяют проводить проверку подлинности для нескольких клиентов, подключенных к порту. Существует два варианта аутентификации: первый, когда проверка подлинности на основе порта требует аутентификации только одного клиента, чтобы доступ к системе имели все клиенты (режим multiple hosts), второй, когда проверка подлинности требует аутентификации всех подключенных к порту клиентов (режим multiple sessions). Если порт в режиме multiple hosts не проходит аутентификацию, то всем подключенным хостам будет отказано в доступе к ресурсам сети. Также к расширенным настройкам относится администрирование гостевых VLAN, к которым имеют доступ не прошедшие аутентификацию пользователи.

Команды режима глобального конфигурирования

Вид запроса командной строки в режиме глобального конфигурирования:

```
console(config)#
```

Таблица 5.177 – Команды режима глобального конфигурирования

Команда	Значение/Значение по умолчанию	Действие
dot1x bpdu {filtering bridging}	-/filtering	<p>Задаёт обработку защиты портов 802.1x BPDU, когда 802.1x глобально выключен.</p> <ul style="list-style-type: none"> - filtering – фильтровать пакеты 802.1x BPDU; - bridging – передавать пакеты 802.1x BPDU как обычные пакеты данных. <p> Функция работает только когда режим аутентификации 802.1x на коммутаторе выключен. Для выключения аутентификации 802.1x используется команда: no dot1x system-auth-control.</p>
no dot1x bpdu		Устанавливает значение по умолчанию.
dot1x guest-vlan timeout	timeout: {30 .. 180} /	Устанавливает время задержки между включением режима аутентификации 802.1x (или включением порта) и добавлением порта в guest VLAN.
no dot1x guest-vlan timeout		Устанавливает значение по умолчанию.
dot1x traps mac-authentication success	-/ disable	Разрешает отправку trap-сообщений, когда клиент успешно проходит аутентификацию по MAC-адресу, основанную на стандарте 802.1x.
no dot1x traps mac-authentication success		Устанавливает значение по умолчанию.
dot1x traps mac-authentication failure	-/ disable	Разрешает отправку trap-сообщений, когда клиент не прошел аутентификацию по MAC-адресу, основанную на стандарте 802.1x.
no dot1x traps mac-authentication failure		Устанавливает значение по умолчанию.
dot1x radius-attributes errors filter-id resource {accept reject}	-/ reject	<p>Устанавливает обработку ошибок для атрибутов RADIUS:</p> <ul style="list-style-type: none"> - accept – пользователь принят, если фильтрация по ID не может быть произведена по причинам распределения ресурсов. Если фильтрация по ID не может быть произведена по другим причинам, пользователь будет отклонен; - reject – Если фильтрация по ID не может быть задана, то пользователь будет отклонен.
no dot1x radius-attributes errors filter-id resources		Устанавливает значение по умолчанию.

Команды режима конфигурирования интерфейса Ethernet

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet:

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

Таблица 5.178 – Команды режима конфигурирования интерфейса Ethernet

Команда	Значение/Значение по умолчанию	Действие
dot1x host-mode {multi-host single-host multi-sessions}	-/ multi-host	<p>Разрешает наличие одного/нескольких клиентов на авторизованном порту 802.1X.</p> <ul style="list-style-type: none"> multi-host – несколько клиентов; single-host – один клиент; multi-sessions – несколько сессий.
dot1x violation-mode {restrict protect shutdown }	-/protect	<p>Задаёт действие, которое необходимо выполнить, когда устройство, MAC-адрес которого отличается от MAC-адреса клиента, осуществляет попытку доступа к интерфейсу.</p> <ul style="list-style-type: none"> - restrict - пакеты с MAC-адресом, отличным от MAC-адреса клиента, пересылаются, при этом адрес источника не изучается; - protect – пакеты с MAC-адресом, отличным от MAC-адреса клиента, отбрасываются; - shutdown – порт выключается, пакеты с MAC-адресом, отличным от MAC-адреса клиента, отбрасываются;

		Частота генерируемых сообщений протокола SNMP trap при поступлении несанкционированных пакетов составляет 1 секунду. Команда игнорируется, когда multiple hosts используется. Команда значима для режима multiple sessions.
no dot1x single-host-violation		Устанавливает значение по умолчанию.
dot1x guest-vlan enable	-/доступ запрещен	Разрешает неавторизованным пользователям данного интерфейса доступ к гостевой VLAN. На устройстве должен быть авторизован хотя бы один гостевой VLAN (команда dot1x guest-vlan в настройках интерфейса VLAN).
no dot1x guest-vlan enable		Запрещает неавторизованным пользователям данного интерфейса доступ к гостевой VLAN.
dot1x mac-authentication {mac-only mac-and-802.1x}	-/выключена	Включает аутентификацию, основанную на MAC-адресах пользователей. - mac-only – включает аутентификацию, основанную только на MAC-адресах, пакеты 802.1x игнорируются; - mac-and-802.1x – включает аутентификацию, основанную на 802.1x и MAC-адресах. - Гостевая VLAN должна быть включена, когда используется аутентификация по MAC-адресу. - Статический MAC-адрес не должен быть прописан. - Функция переаутентификации должна быть включена.
no dot1x mac-authentication		Выключает аутентификацию, основанную на MAC-адресах пользователей.
dot1x radius-attributes filter-id	-/выключен	Включить проверку подлинности, основанную на ACL/назначить QoS-Policy.
no dot1x radius-attributes filter-id		Устанавливает значение по умолчанию.

Команды режима конфигурирования VLAN

Вид запроса командной строки в режиме конфигурирования интерфейса VLAN:

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



Порт доступа (Access) не может быть членом не аутентифицированной VLAN, родной VLAN транкового порта (Trunk) не может быть не аутентифицированным VLAN, но для главного (General) порта PVID может быть не аутентифицированным VLAN (но только тегированные пакеты могут быть приняты в неавторизованном состоянии).

Таблица 5.179 – Команды режима конфигурирования интерфейса VLAN

Команда	Значение	Действие
dot1x auth-not-req	По умолчанию доступ неавторизованным пользователям запрещен	Разрешает доступ к данной VLAN неавторизованным пользователям.
no dot1x auth-not-req		Запрещает доступ к данной VLAN неавторизованным пользователям.
dot1x guest-vlan	По умолчанию VLAN не определена как гостевая	Определяет гостевую VLAN. Открывает неавторизованным пользователям интерфейса доступ к гостевой VLAN. Если гостевая VLAN определена и разрешена, порт будет автоматически присоединяться к ней, когда не авторизован, и покидать, когда пройдет авторизацию. Чтобы использовать данный функционал, порт не должен быть статическим членом гостевой VLAN.
no dot1x guest-vlan		Устанавливает значение по умолчанию.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 5.180 – Команды режима Privileged EXEC

Команда	Значение	Действие
show dot1x advanced [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i>]	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}	Показывает дополнительные сведения о настройках протокола 802.1x (команда доступна только для привилегированного пользователя).

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.181 – Команды режима Privileged EXEC

Команда	Значение	Действие
show dot1x bpdud	-	Показывает обработку защиты портов 802.1x BPDU когда 802.1x глобально выключен.

5.23.3 Контроль протокола DHCP и опция 82

DHCP (Dynamic Host Configuration Protocol) – сетевой протокол, позволяющий клиенту по запросу получать IP-адрес и другие требуемые параметры, необходимые для работы в сети TCP/IP.

Протокол DHCP может использоваться злоумышленниками для совершения атак на устройство, как со стороны клиента, заставляя DHCP-сервер выдать все доступные адреса, так и со стороны сервера, путем его подмены. Программное обеспечение коммутатора позволяет обеспечить защиту устройства от атак с использованием протокола DHCP, для чего применяется функция контроля протокола DHCP – DHCP snooping.

Устройство способно отслеживать появление DHCP-серверов в сети, разрешая их использование только на «доверенных» интерфейсах, а также контролировать доступ клиентов к DHCP-серверам по таблице соответствий.

Опция 82 протокола DHCP (option 82) используется для того, чтобы проинформировать DHCP-сервер о том, от какого DHCP-ретранслятора (Relay Agent) и через какой его порт был получен запрос. Применяется для установления соответствий IP-адресов и портов коммутатора, а также для защиты от атак с использованием протокола DHCP. Опция 82 представляет собой дополнительную информацию (имя устройства, номер порта), добавляемую коммутатором, который работает в режиме DHCP Relay агента, в виде DHCP-запроса, принятого от клиента. На основании данной опции, DHCP-сервер выделяет IP-адрес (диапазон IP-адресов) и другие параметры порту коммутатора. Получив необходимые данные от сервера, DHCP Relay агент выделяет IP-адрес клиенту, а также передает ему другие необходимые параметры.

Таблица 5.182 - Формат полей опции 82

Поле	Передаваемая информация
Circuit ID	hostname устройства

	строка вида eth <stacked/slotid/interfaceid>:<vlan> Последний байт – номер порта, к которому подключено устройство, отправляющее dhcp-запрос.
Remote agent ID	Enterprise number – 0089c1 MAC-адрес устройства



Для использования опции 82 на устройстве должна быть включена функция DHCP relay агента. Для включения DHCP relay агента используется команда ip dhcp relay enable в режиме глобального конфигурирования (см. соответствующий раздел документации).



Для корректной работы функции DHCP Snooping все используемые DHCP-сервера должны быть подключены к «доверенным» портам коммутатора. Для добавления порта в список «доверенных» используется команда ip dhcp snooping trust в режиме конфигурации интерфейса. Для обеспечения безопасности все остальные порты коммутатора должны быть «недоверенными».

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

console (config) #

Таблица 5.183 – Команды режима глобального конфигурирования

Команда	Значение/Значение по умолчанию	Действие
ip dhcp snooping	По умолчанию контролирование протокола DHCP выключено	Разрешает коммутатору контролирование протокола DHCP.
no ip dhcp snooping		Запрещает коммутатору контролирование протокола DHCP.
ip dhcp snooping vlan <i>vlan-id</i>	vlan-id: 1..4094 По умолчанию контролирование протокола DHCP выключено	Разрешает контролирование протокола DHCP в пределах указанного VLAN.
no ip dhcp snooping vlan <i>vlan-id</i>		Запрещает контролирование протокола DHCP в пределах указанного VLAN.
ip dhcp snooping information option allowed-untrusted	По умолчанию прием DHCP-пакетов с опцией 82 от «ненадежных» портов запрещен	Разрешает принимать DHCP-пакеты с опцией 82 от «ненадежных» портов.
no ip dhcp snooping information option allowed-untrusted		Запрещает принимать DHCP-пакеты с опцией 82 от «ненадежных» портов.
ip dhcp snooping verify	По умолчанию верификация включена	Включает верификацию MAC-адреса клиента и MAC-адреса источника, принятого в DHCP-пакете на «недоверенных» портах.
no ip dhcp snooping verify		Выключает верификацию MAC-адреса клиента и MAC-адреса источника, принятого в DHCP-пакете на «недоверенных» портах.
ip dhcp snooping database	Резервный файл не используется	Разрешает использование резервного файла (базы) контроля протокола DHCP.
no ip dhcp snooping database		Запрещает использование резервного файла (базы) контроля протокола DHCP.
ip dhcp snooping database update-freq <i>seconds</i>	600 – 86400/1200	Задаёт частоту обновления файла (базы) контроля протокола DHCP.
no ip dhcp snooping database update-freq <i>seconds</i>		Устанавливает значение по умолчанию.

<code>ip dhcp information option</code>	По умолчанию добавление опции 82 разрешено	Разрешает устройству добавление опции 82 при работе протокола DHCP.
<code>no ip dhcp information option</code>		Запрещает устройству добавление опции 82 при работе протокола DHCP.
<code>ip dhcp information option format-type access-node-id string_id</code>	string_id: 1..32 символов	Установка идентификатора запрашивающего узла.
<code>no ip dhcp information option format-type access-node-id</code>		Установка значения по умолчанию.
<code>ip dhcp information option format-type option format [delimiter delimiter]</code>	format: sp, sv, pv, spv, bin delimiter: { . , ; # / space }	Настройка формата DHCP опции 82. Формат: - sp – номер слота и порта; - sv – номер слота и VLAN; - pv – номер порта и VLAN; - spv – номер слота, порта и VLAN; - bin – бинарный формат: VLAN, слот, порт.
<code>no ip dhcp information option format-type option</code>		Установка значения по умолчанию

Команды режима конфигурирования интерфейса (диапазона интерфейсов) Ethernet, интерфейса группы портов

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet, интерфейса группы портов:

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

Таблица 5.142 – Команды режима конфигурирования интерфейса Ethernet, группы интерфейсов

Команда	Значение по умолчанию	Действие
<code>ip dhcp snooping trust</code>	По умолчанию интерфейс не является доверенным	Добавляет интерфейс в список «доверенных» при использовании контроля протокола DHCP. DHCP-трафик «доверенного» интерфейса считается безопасным и не контролируется.
<code>no ip dhcp snooping trust</code>		Удаляет интерфейс из списка «доверенных» при использовании контроля протокола DHCP.
<code>ip dhcp information option format-type circuit-id circuit-id</code>	circuit-id: 1..63 символов	Устанавливает специфичный <i>Circuit-id</i> на интерфейсе.
<code>no ip dhcp information option format-type circuit-id</code>		Устанавливает значение по умолчанию.
<code>ip dhcp information option format-type remote-id remote-id</code>	remote -id: 1..63 символов	Устанавливает специфичный <i>Remote-id</i> на интерфейсе.
<code>no ip dhcp information option format-type remote-id</code>		Устанавливает значение по умолчанию.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 5.184 – Команды режима Privileged EXEC

<i>Команда</i>	<i>Значение</i>	<i>Действие</i>
ip dhcp snooping binding <i>mac-address</i> <i>vlan-id ip-address</i> { gigabitethernet gi_port fastethernet fa_port port-channel group } expiry { <i>seconds</i> <i>infinity</i> }	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; vlan-id: 1 .. 4094; group: 1 .. 8; period: 10..4294967295	Добавляет в файл (базу) контроля протокола DHCP соответствие MAC-адреса клиента, группе VLAN и IP-адресу для указанного интерфейса. Данная запись будет действительна в течение указанного в команде времени жизни записи, если клиент не отправит запрос на DHCP-сервер на обновление. Таймер обнуляется в случае получения от клиента запроса на обновление (команда доступна только для привилегированного пользователя). - seconds – время жизни записи; -infinity – время жизни записи не ограничено.
no ip dhcp snooping binding <i>mac-address</i> <i>vlan-id</i>		Удаляет из файла (базы) контроля протокола DHCP соответствие MAC-адреса клиента и группы VLAN.
clear ip dhcp snooping database	-	Очищает файл (базу) контроля протокола DHCP.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.185 – Команды режима EXEC

<i>Команда</i>	<i>Значение</i>	<i>Действие</i>
show ip dhcp information option	-	Показывает информацию об использовании опции 82 протокола DHCP.
show ip dhcp snooping { gigabitethernet gi_port fastethernet fa_port port-channel group }	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: 1 .. 8	Показывает конфигурацию функции контроля протокола DHCP.
show ip dhcp snooping binding [<i>mac-address</i> <i>mac-address</i>] [<i>ip-address</i> <i>ip-address</i>] [<i>vlan vlan</i>] { gigabitethernet gi_port fastethernet fa_port port-channel group }	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group: 1 .. 8 vlan-id: 1..4094	Показывает соответствия из файла (базы) контроля протокола DHCP.

Примеры выполнения команд

- Разрешить использование DHCP опции 82:

```
console# configure  
console(config)# ip dhcp relay enable  
console(config)# ip dhcp information option
```

- Показать все соответствия из файла (базы) контроля протокола DHCP:

```
console# show ip dhcp snooping
```

```
DHCP snooping is globally enabled  
DHCP snooping is configured on following VLANs: 2, 5
```

```
DHCP snooping database: enabled
Option 82 on untrusted port is allowed
Verification of hwaddr field is enabled
```

```
Interface           Trusted
-----
1/g17                yes
```

5.23.4 Защита IP-адреса клиента (IP-source Guard)

Функция защиты IP-адреса (IP Source Guard) предназначена для фильтрации трафика, принятого с интерфейса, на основании таблицы соответствий DHCP snooping и статических соответствий IP Source Guard. Таким образом, IP Source Guard позволяет бороться с подменой IP-адресов в пакетах.



Поскольку функция контроля защиты IP-адреса использует таблицы соответствий DHCP snooping, имеет смысл использовать данную функцию, предварительно настроив и включив DHCP snooping.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.186 – Команды режима глобального конфигурирования

Команда	Значение	Действие
ip source-guard	По умолчанию функция выключена	Включает функцию защиты IP-адреса клиента для всего коммутатора.
no ip source-guard		Выключает функцию защиты IP-адреса клиента для всего коммутатора.
ip source-guard binding <i>mac-address vlan-id ip-address</i> {gigabitethernet gi_port fastethernet fa_port port-channel group}	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; vlan-id 1..4094; group {1..8}	Создание статической записи в таблице соответствия между IP-адресом клиента, его MAC-адресом и группой VLAN для указанного в команде интерфейса.
no ip source-guard binding <i>mac-address vlan-id</i>		Удаление статической записи в таблице соответствия.
ip source-guard tcam retries-freq {seconds never}	{10-600, never}/60 сек	Задаёт частоту обращения устройства к внутренним ресурсам с целью записи в память неактивных защищённых IP-адресов. - never – запрещает запись в память неактивных защищённых IP-адресов.
no ip source-guard tcam retries-freq		Устанавливает значение по умолчанию.

Команды режима конфигурирования интерфейса (диапазона интерфейсов) Ethernet, интерфейса группы портов

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet, интерфейса группы портов:

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

Таблица 5.187 – Команды режима конфигурирования интерфейса Ethernet, группы интерфейсов

Команда	Значение	Действие
ip source-guard	По умолчанию функция выключена.	Включает функцию защиты IP-адреса клиента для настраиваемого интерфейса.
no ip source-guard		Выключает функцию защиты IP-адреса клиента для настраиваемого интерфейса.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 5.188 – Команды режима Privileged EXEC

Команда	Значение	Действие
ip source-guard tcam locate	-	Вручную запускает процесс обращения устройства к внутренним ресурсам с целью записи в память неактивных защищенных IP-адресов. Команда доступна только для привилегированного пользователя.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.189 – Команды режима EXEC

Команда	Значение	Действие
show ip source-guard configuration [gigabitethernet gi_port fastethernet fa_port port-channel group]	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group {1..8}	Команда отображает настройку функции защиты IP-адреса на заданном, либо на всех интерфейсах устройства.
show ip source-guard status [mac-address mac-address] [ip-address ip-address] [vlan vlan] [gigabitethernet gi_port fastethernet fa_port port-channel group]	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; vlan-id 1..4094; group {1..8}	Команда отображает статус функции защиты IP-адреса для указанного интерфейса, IP-адреса, MAC-адреса или группы VLAN.
show ip source-guard inactive	-	Команда отображает не активные IP-адреса отправителя.

Примеры выполнения команд

- Показать настройку функции защиты IP-адреса для всех интерфейсов:

```
console# show ip source-guard configuration
```

IP source guard is globally enabled.	
Interface	State
-----	-----
1/g4	Enabled

1/g21	Enabled
1/g22	Enabled

- Включить функцию защиты IP-адреса для фильтрации трафика на основании таблицы соответствий DHCP snooping и статических соответствий IP Source Guard. Создать статическую запись в таблице соответствия для интерфейса Ethernet 12 первого устройства в стеке: IP-адрес клиента – 192.168.16.14, его MAC-адрес – 00:60:70:4A:AB:AF. Интерфейс в 3-й группе VLAN:

```
console# configure
console(config)# ip dhcp snooping
console(config)# ip source-guard
console(config)# ip source-guard binding 0060.704A.ABAF 3 192.168.16.14
gigabitethernet 1/0/12
```

5.23.5 Контроль протокола ARP (ARP Inspection)

Функция контроля протокола **ARP (ARP Inspection)** предназначена для защиты от атак с использованием протокола ARP (например, ARP-spoofing – перехват ARP-трафика). Контроль протокола ARP осуществляется на основе статических соответствий IP- и MAC-адресов, заданных для группы VLAN.



Порт, сконфигурированный «недоверенным» для функции ARP Inspection, должен также быть «недоверенным» для функции DHCP snooping или соответствие MAC-адреса и IP-адреса для этого порта должно быть сконфигурировано статически. Иначе данный порт не будет отвечать на запросы ARP.



Для ненадёжных портов выполняются проверки соответствий IP- и MAC-адресов.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.190 – Команды режима глобального конфигурирования

<i>Команда</i>	<i>Значение/Значение по умолчанию</i>	<i>Действие</i>
ip arp inspection	По умолчанию функция выключена	Включает контроль протокола ARP (функцию ARP Inspection).
no ip arp inspection		Выключает контроль протокола ARP (функцию ARP Inspection).
ip arp inspection vlan <i>vlan-ID</i>	vlan-ID 1..4094	Разрешает проверку протокола ARP, основанную на базе соответствий DHCP snooping, в выбранной группе VLAN.
no ip arp inspection vlan <i>vlan-ID</i>	По умолчанию функция выключена	Запрещает проверку протокола ARP, основанную на базе соответствий DHCP snooping, в выбранной группе VLAN.
ip arp inspection validate		Предоставляет специфичные проверки для контроля протокола ARP. MAC-адрес источника: Для ARP-запросов и ответов проверяется соответствие MAC-адреса в заголовке Ethernet MAC-адресу источника в содержимом протокола ARP. MAC-адрес назначения: Для ARP-ответов проверяется соответствие MAC-адреса в заголовке Ethernet MAC-адресу назначения в содержимом протокола ARP. IP-адрес: Проверяется содержимое ARP-пакета на наличие некорректных IP-адресов.

no ip arp inspection validate		Запрещает специфичные проверки для контроля протокола ARP.
ip arp inspection list create name	Имя списка 1..32 символа	1. Создание списка статических ARP соответствий. 2. Вход в режим конфигурирования ARP-списков.
no ip arp inspection list create name		Удаление списка статических ARP соответствий.
ip arp inspection list assign vlan-id name	vlan-ID:{1 .. 4094}	Назначает список статических ARP соответствий для указанной VLAN.
no ip arp inspection list assign vlan-id		Отменяет назначение списка статических ARP соответствий для указанной VLAN.
ip arp inspection logging interval {seconds infinite}	{0..86400, infinite}/5 сек	Задаёт минимальный интервал между сообщениями, содержащими информацию протокола ARP, передаваемыми в журнал. - значение 0 указывает на то, что сообщения будут генерироваться незамедлительно; infinite – не генерировать сообщений в журнал.
no ip arp inspection logging interval		Устанавливает значение по умолчанию.

Команды режима конфигурирования интерфейса (диапазона интерфейсов) Ethernet, интерфейса группы портов

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet, интерфейса группы портов:

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

Таблица 5.191 – Команды режима конфигурирования интерфейса Ethernet, группы интерфейсов

Команда	Значение по умолчанию	Действие
ip arp inspection trust	По умолчанию интерфейс не является доверенным	Добавляет интерфейс в список «доверенных» при использовании контроля протокола ARP. ARP-трафик «доверенного» интерфейса считается безопасным и не контролируется.
no ip arp inspection trust		Удаляет интерфейс из списка «доверенных» при использовании контроля протокола ARP.

Команды режима конфигурирования ARP-списков

Вид запроса командной строки в режиме конфигурирования ARP-списков:

```
console# configure
console(config)# ip arp inspection list spisok
console(config-ARP-list)#
```

Таблица 5.192 – Команды режима конфигурирования ARP списков

Команда	Действие
ip ip-address mac mac-address	Добавляет статическое соответствие IP- и MAC-адресов.
no ip ip-address mac mac-address	Удаляет статическое соответствие IP- и MAC-адресов.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.193 – Команды режима EXEC

Команда	Значение	Действие
show ip arp inspection [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i>]	gi_port: {1..8/0/1..28}; fa_port: {1..8/0/1..24}; group {1..8}	Показывает конфигурацию функции контроля протокола ARP Inspection на выбранном интерфейсе/всех интерфейсах.
show ip arp inspection list	-	Показывает списки статических соответствий IP- и MAC-адресов (команда доступна только для привилегированного пользователя).
show ip arp inspection statistics [vlan <i>vlan-id</i>]	vlan-ID:{1 .. 4094}	Показывает статистику для следующих типов пакетов, которые были обработаны при помощи функции ARP: - переданные пакеты (forwarded); - потерянные пакеты (Dropped); - ошибки в IP/MAC (IP/MAC Failures).
clear ip arp inspection statistics [vlan <i>vlan-id</i>]	vlan-ID:{1 .. 4094}	Очищает статистику контроля протокола ARP Inspection.

Примеры выполнения команд

- Включить контроль протокола ARP и добавить в список *spisok* статическое соответствие: MAC-адрес: 00:60:70:AB:CC:CD, IP-адрес: 192.168.16.98. Назначить список *spisok* статических ARP соответствий для VLAN 11:

```
console# configure
console(config)# ip arp inspection list spisok
console(config-ARP-list)# ip 192.168.16.98 mac 0060.70AB.CCCD
console(config-ARP-list)# exit
console(config)# ip arp inspection list assign 11 spisok
```

- Показать списки статических соответствий IP- и MAC-адресов:

```
console# show ip arp inspection list
```

```
List name: servers
Assigned to VLANs: 11
IP          ARP
-----
192.168.16.98  0060.70AB.CCCD
```

5.23.6 Настройка функции MAC Address Notification

Функция MAC Address Notification позволяет отслеживать появление и исчезновение активного оборудования на сети, путем сохранения истории изучения MAC-адресов. При обнаружении изменений в составе изученных MAC-адресов коммутатор сохраняет информацию в таблице и извещает об этом с помощью сообщений протокола SNMP. Функция имеет настраиваемые параметры – глубина истории о событиях и минимальный интервал отправки сообщений. Сервис MAC Address Notification по умолчанию отключен и может быть настроен выборочно для отдельных портов коммутатора.

Команды режима глобального конфигурирования

Вид запроса командной строки в режиме глобального конфигурирования:

```
console (config) #
```

Таблица 5.194 - Команды режима глобального конфигурирования

Команда	Значение/ Значение по умолчанию	Действие
[no] mac address-table notification change	-/выключена	Команда предназначена для глобального управления функцией MAC notification. Команда разрешает регистрацию событий добавления и удаления MAC адресов в/из таблиц коммутатора и отправку уведомления о событиях. Отрицательная форма команды (с префиксом no) выключает функцию глобально и отменяет соответствующие настройки на всех интерфейсах. Для работы функции необходимо дополнительно разрешать генерацию уведомлений на интерфейсах (см. ниже).
mac address-table notification change interval {value}	[0..4294967295]/1	Максимальный промежуток времени между отправками SNMP-уведомлений. Если значение интервала времени равно 0, то генерация уведомлений и сохранение событий в историю будет осуществляться немедленно по мере возникновения событий об изменении состояния таблицы MAC-адресов. Если значение интервала времени больше 0, то устройство будет накапливать события об изменении состояния таблицы MAC-адресов в течение этого времени, а затем отправлять уведомления протокола SNMP и сохранять события в истории.
mac address-table notification change history {value}	[0..500]/1	Команда задает максимальное количество событий об изменении состояния таблицы MAC адресов, которое сохраняется в истории. Если установлен размер истории равный 0, то события не сохраняются. При переполнении буфера истории новое событие помещается на место самого старого.
[no] snmp-server enable traps mac-notification change	-/выключено	Команда предназначена для включения или отключения отправки SNMP-уведомлений об изменении состояния таблицы MAC-адресов. Для отключения используется отрицательная форма команды. Если отправка уведомлений включена, то устройство будет информировать о событиях сообщениями протокола SNMP и сохранять соответствующие события в истории. Если отправка SNMP-уведомлений выключена, то устройство будет только сохранять события в истории.

Команды режима конфигурирование интерфейса Ethernet

Вид запроса командной строки:

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

Таблица 5.195 - Команды режима конфигурирования интерфейса Ethernet

Команда	Значение по умолчанию	Действие
snmp trap mac-notification change [added removed]	выключена	Включение генерации уведомлений на каждом интерфейсе о событиях изменения состояния MAC-адресов. Отдельно можно разрешить генерацию уведомлений только об изучении MAC адресов либо только об их удалении.

Команды режима privileged EXEC

Вид запроса командной строки в режиме privileged EXEC:

```
console#
```

Таблица 5.196 - Команды режима privileged EXEC

<i>Команда</i>	<i>Значение</i>	<i>Действие</i>
show mac address-table notification change history [interfaces]	-	Отображение всех уведомлений об изменении состояния MAC-адресов, сохраненных в истории. Возможна фильтрация событий по портам, группам портов (LAG) и VLAN.
show mac address-table notification change statistics	-	Отображение статистики сервиса: общее количество событий об изучении MAC-адресов, общее количество событий об удалении MAC-адресов, общее количество отправленных SNMP-сообщений.

Примеры использования команд

- Пример показывает как настроить передачу сообщений SNMP MAC Notification на сервер с адресом 172.16.1.5. При настройке задается общее разрешение работы сервиса, настраивается минимальный интервал отправки сообщений, задается размер истории событий и настраивается сервис на заданном порту.

```
console (config)# snmp-server host 172.16.1.5 traps private
console (config)# snmp-server enable traps mac-notification change
console (config)# mac address-table notification change
console (config)# mac address-table notification change interval 60
console (config)# mac address-table notification change history 100
console (config)# interface gigabitethernet 0/7
console (config-if)# snmp trap mac-notification change
console (config-if)# exit
console (config)#
```

5.24 Функции DHCP Relay посредника

Коммутатор MES1024/MES1124/MES2124 поддерживает функции DHCP Relay агента. Задачей DHCP Relay агента является передача DHCP-пакетов от клиента к серверу и обратно, в случае если DHCP-сервер находится в одной сети, а клиент в другой. Другой функцией является добавление дополнительных опций в DHCP-запросы клиента (например, опции 82).

Принцип работы DHCP Relay агента на коммутаторе:

коммутатор принимает от клиента DHCP-запросы, передает эти запросы серверу от имени клиента (оставляя в запросе опции с требуемыми клиентом параметрами и, в зависимости от конфигурации, добавляя свои опции). Получив ответ от сервера, коммутатор передает его клиенту.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console (config)#
```

Таблица 5.197 – Команды режима глобального конфигурирования

<i>Команда</i>	<i>Значение</i>	<i>Действие</i>
ip dhcp relay enable	По умолчанию агент выключен	Включение функций DHCP Relay агента на коммутаторе.
no ip dhcp relay enable		Выключение функций DHCP Relay агента на коммутаторе.
ip dhcp relay address ip-addr	Может быть задано до 8-ми серверов	Задаёт IP-адрес доступного DHCP-сервера для DHCP Relay агента.
no ip dhcp relay address [ip-addr]		Удаляет IP-адрес из списка DHCP-серверов для DHCP Relay агента.

Команды режима конфигурирования интерфейса VLAN

Вид запроса командной строки в режиме конфигурирования интерфейса VLAN:

```
console# configure
console(config)# interface vlan {VLAN ID}
console(config-if)#
```

Таблица 5.198 – Команды режима конфигурирования интерфейса VLAN

<i>Команда</i>	<i>Значение</i>	<i>Действие</i>
ip dhcp relay enable	По умолчанию агент выключен	Включение функций DHCP Relay агента на настраиваемом интерфейсе.
no ip dhcp relay enable		Выключение функций DHCP Relay агента на настраиваемом интерфейсе.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.199 – Команды режима EXEC

<i>Команда</i>	<i>Действие</i>
show ip dhcp relay	Отображает конфигурацию настроенной функции DHCP Relay агента для коммутатора и отдельно для интерфейсов, а также список доступных серверов.

Примеры выполнения команд

- Показать состояние функции DHCP Relay агента:

```
console# show ip dhcp relay
```

```
DHCP relay is Enabled
DHCP relay is not configured on any vlan.
Servers: 192.168.16.38
Relay agent Information option is Enabled
```

5.25 Конфигурирование PPPoE Intermediate Agent

Функция PPPoE IA реализована в соответствии с требованиями документа DSL Forum TR-101 и предназначена для использования на коммутаторах, работающих на уровне доступа.

Функция позволяет дополнять пакеты PPPoE Discovery информацией, характеризующей интерфейс доступа. Это необходимо для идентификации пользовательского интерфейса на сервере доступа (BRAS, Broadband Remote Access Server). Управление перехватом и обработкой пакетов PPPoE Active Discovery осуществляется глобально для всего устройства и выборочно для каждого интерфейса.

Реализация функции PPPoE IA предоставляет дополнительные возможности контроля сообщений протокола путем назначения доверенных интерфейсов.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.200 – Команды режима глобального конфигурирования

<i>Команда</i>	<i>Значение/Значение по умолчанию</i>	<i>Действие</i>
[no] pppoe intermediate-agent	По умолчанию PPPoE IA отключен	Разрешение/запрет работы PPPoE Intermediate Agent.
[no] pppoe intermediate-agent format-type access-node-id word	<i>word</i> : строка от 1 до 32 символов По умолчанию идентификатор устройства не назначен.	Установка строки идентификации устройства доступа. Отрицательная форма команды (no) восстанавливает настройки по умолчанию.

<p>[no] pppoe intermediate-agent format-type generic-error-message <i>word</i></p>	<p><i>word</i>: строка до 128 символов</p> <p>По умолчанию назначено сообщение «PPPoE Discover packet is too large to process.».</p>	<p>Установка текста сообщения об ошибке превышения размера пакета (MTU), отправляемого PPPoE IA в PADO или PADS пакетах. Отрицательная форма команды восстанавливает значение параметра по умолчанию.</p> <p>Примечание: если сообщение содержит символы пробела, его необходимо заключить в кавычки.</p>
<p>[no] pppoe intermediate-agent format-type option [sp sv pv spv] delimiter <i>[,,:# /]</i></p>	<p><i>sp sv pv spv</i> <i>,,:#/</i></p> <p>По умолчанию установлен формат в соответствии с TR-101: slot / port : vlan</p>	<p>Настройка набора параметров и разделителя между ними, которые используются для формирования подопции circuit -id.</p> <p>В команде используются следующие условные обозначения:</p> <p>sp – slot + port sv – slot + vlan pv – port + vlan spv – slot + port + vlan</p>

Команды режима конфигурирования интерфейса

Вид запроса командной строки в режиме конфигурирования интерфейса:

console (config-if) #

Таблица 5.201 – Команды режима конфигурирования интерфейса Ethernet, группы портов

Команда	Значение/Значение по умолчанию	Действие
<p>[no] pppoe intermediate-agent</p>	<p>-</p>	<p>Разрешение/запрет работы PPPoE Intermediate Agent на интерфейсе.</p>
<p>[no] pppoe intermediate-agent format-type circuit-id <i>[word]</i></p>	<p><i>word</i>: строка от 1 до 63 символов</p>	<p>Назначение идентификатора circuit-id, добавляемого коммутатором. Идентификатор, заданный в команде, полностью переопределяет идентификатор, вычисляемый на основе глобальных параметров access-node-id и option/delimiter. Отрицательная форма команды восстанавливает настройку на основе глобальных параметров access-node-id и option/delimiter.</p>
<p>[no] pppoe intermediate-agent format-type remote-id <i>[word]</i></p>	<p><i>word</i>: строка от 1 до 63 символов.</p> <p>По умолчанию в качестве remote-id используется MAC-адрес коммутатора.</p>	<p>Назначение идентификатора remote-id, добавляемого коммутатором. Идентификатор должен быть сконфигурирован на всех интерфейсах коммутатора, где работает PPPoE IA. Отрицательная форма команды восстанавливает настройку по умолчанию.</p>
<p>[no] pppoe intermediate-agent trust</p>	<p>По умолчанию интерфейс не является доверенным.</p>	<p>Управление режимом доверия к интерфейсу. Команда добавляет или удаляет интерфейс из списка доверенных. Интерфейсы, к которым подключены PPPoE серверы, настраиваются как доверенные. Интерфейсы, к которым подключены пользователи, настраиваются как недоверенные. Отрицательная форма команды восстанавливает значение по умолчанию.</p>
<p>[no] pppoe intermediate-agent vendor-tag strip</p>	<p>По умолчанию режим удаления выключен.</p>	<p>Разрешение или запрет удаления vendor-speciifc опции из пакетов PADO, PADS, PADT перед отправкой их в сторону пользователя. Функция удаления может быть использована только на интерфейсе, на котором разрешена работа PPPoE IA и который является доверенным интерфейсом. Обычно функция удаления настраивается на интерфейсе, обращенном в сторону PPPoE сервера.</p> <p>Отрицательная форма команды выключает режим удаления.</p>

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.202 – Команды режима EXEC

Команда	Значение/Значение по умолчанию	Действие
<code>show pppoe intermediate-agent info [interface {gigabitethernet gi_port fastethernet fa_port port-channel po}]</code>	gi_port: (1..8/0/1..28); fa_port: (1..8/0/1..24); po: (1...8).	Отображение настроек PPPoE Intermediate Agent. Если в команде явно не задан интерфейс, то команда выполняется для всех интерфейсов, где разрешена работа PPPoE IA и всех доверенных портов.
<code>show pppoe intermediate-agent statistics [interface {gigabitethernet gi_port fastethernet fa_port port-channel po}]</code>	gi_port: (1..8/0/1..28); fa_port: (1..8/0/1..24); po: (1...8).	Отображение статистики работы PPPoE Intermediate Agent. Если в команде не задан явно интерфейс, то команда выполняется для всех интерфейсов с разрешенным PPPoE IA и всех доверенных портов.
<code>clear pppoe intermediate-agent statistics [interface {gigabitethernet gi_port fastethernet fa_port port-channel po}]</code>	gi_port: (1..8/0/1..28); fa_port: (1..8/0/1..24); po: (1...8).	Очистка статистики работы PPPoE Intermediate Agent. Если в команде не задан явно интерфейс, то команда выполняется для всех интерфейсов с разрешенным PPPoE IA и всех доверенных портов).
<code>show pppoe intermediate-agent sessions [interface {gigabitethernet gi_port fastethernet fa_port port-channel po}]</code>	gi_port: (1..8/0/1..28); fa_port: (1..8/0/1..24); po: (1...8).	Отображение всех зарегистрированных клиентских сессий. Если в команде не задан явно интерфейс, то отображаются все сессии с сортировкой по интерфейсам.

5.26 Конфигурирование ACL (списки контроля доступа)

ACL (Access Control List – список контроля доступа) – таблица, которая определяет правила фильтрации входящего и исходящего трафика на основании передаваемых в пакетах протоколов, TCP/UDP портов, IP-адресов или MAC-адресов.



ACL-списки на базе IPv6, IPv4 и MAC-адресов не должны иметь одинаковые названия.



IPv6 и IPv4-списки могут работать вместе на одном физическом интерфейсе. Список ACL на базе MAC-адресации не может совмещаться со списками для IPv4 или IPv6. Два списка одинакового типа не могут работать вместе на интерфейсе.

Команды для создания и редактирования списков ACL доступны в режиме глобального конфигурирования.

Команды режима глобального конфигурирования

Командная строка в режиме глобального конфигурирования имеет вид:

```
console (config)#
```

Таблица 5.203 – Команды для создания и конфигурирования списков ACL

Команда	Значение	Действие
ip access-list extended <i>access-list</i>	0..32 символа	Создание нового расширенного списка ACL для адресации IPv4 и вход в режим его конфигурирования (если список с данным именем еще не создан) либо вход в режим конфигурирования ранее созданного списка.
no ip access-list extended <i>access-list</i>		Удаление списка ACL для адресации IPv4.
ipv6 access-list <i>access-list</i>		Создание нового расширенного списка ACL для адресации IPv6 и вход в режим его конфигурирования (если список с данным именем еще не создан) либо вход в режим конфигурирования ранее созданного списка.
no ipv6 access-list <i>access-list</i>		Удаление списка ACL для адресации IPv6 ¹ .
mac access-list extended <i>access-list</i>		Создание нового списка ACL на базе MAC-адресации и вход в режим его конфигурирования (если список с данным именем еще не создан) либо вход в режим конфигурирования ранее созданного списка.
no mac access-list extended <i>access-list</i>	Удаление списка ACL на базе MAC-адресации.	
time-range <i>time-name</i>	0..32 символа	Вход в режим конфигурирования <i>time-range</i> и определение временных интервалов для списка доступа. - <i>time-name</i> - имя профиля настроек <i>time-range</i> .
no time-range <i>time-name</i>		Удаление заданной конфигурации <i>time-range</i> .

Для того чтобы активизировать список ACL, необходимо связать его с интерфейсом. Интерфейсом, использующим список, может быть либо интерфейс Ethernet, либо группа портов.

Команды режима конфигурирования интерфейса Ethernet, группы портов.

Командная строка в режиме конфигурирования интерфейса Ethernet, группы портов имеет вид:

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

Таблица 5.204 – Команда назначения списка ACL интерфейсу.

Команда	Значение	Действие
service-acl input <i>access-list</i>	0 .. 32 символа	В настройках определённого физического интерфейса команда привязывает указанный список к данному интерфейсу.
no service-acl input		Удаление списка с интерфейса.

Команды режима Privileged EXEC

Командная строка в режиме Privileged EXEC имеет вид:

```
console#
```

Таблица 5.205 – Команды для просмотра списков ACL

Команда	Значение	Действие
show access-lists [<i>access-list</i>]	0..32 символа	Показывает списки ACL, созданные на коммутаторе.
show access-lists time-range-active [<i>access-list</i>]		Показывает списки ACL, созданные на коммутаторе, которые в настоящее время являются активными.

¹ В текущей версии программного обеспечения не поддерживается

<code>show interfaces access-lists</code> <code>[gigabitethernet gi_port </code> <code>fastethernet fa_port </code> <code>port-channel group] vlan</code> <code>vlan_id]</code>	<code>gi_port: {1..8/0/1..28};</code> <code>fa_port: {1..8/0/1..24};</code> <code>vlan-id 1..4094;</code> <code>group {1..8}</code>	Показывает списки ACL назначенные интерфейсам.
<code>clear access-lists counters</code> <code>[gigabitethernet gi_port </code> <code>fastethernet fa_port </code> <code>port-channel group]</code>	<code>gi_port: {1..8/0/1..28};</code> <code>fa_port: {1..8/0/1..24};</code> <code>group {1..8}</code>	Обнулить все счетчики списков ACL, либо счетчики для списков ACL заданного интерфейса.
<code>show interfaces access-lists</code> <code>counters</code> <code>[gigabitethernet gi_port </code> <code>fastethernet fa_port </code> <code>port-channel group]</code>	<code>gi_port: {1..8/0/1..28};</code> <code>fa_port: {1..8/0/1..24};</code> <code>group {1..8}</code>	Показывает счетчики списков доступа.

Команды режима EXEC

Командная строка в режиме EXEC имеет вид:

```
console#
```

Таблица 5.206 – Команды для просмотра списков ACL

Команда	Значение	Действие
<code>show time-range time-name</code>	-	Показывает конфигурацию time-range

5.26.1 Конфигурирование ACL на базе IPv4

В данном разделе приведены значения и описания основных параметров, используемых в составе команд настройки списков ACL, основанных на адресации IPv4.

Создание и вход в режим редактирования списков ACL, основанных на адресации IPv4, осуществляется по команде: `ip access-list extended access-list`. Например, для создания списка ACL под названием EltexAL необходимо выполнить следующие команды:

```
console#
console# configure
console(config)# ip access-list extended EltexAL
console(config-ip-al)#
```

Таблица 5.207 – Основные параметры, используемые в командах

Параметр	Значение	Действие
permit	Действие 'разрешить'	Создает разрешающее правило фильтрации в списке ACL.
deny	Действие 'запретить'	Создает запрещающее правило фильтрации в списке ACL.
protocol	Протокол	Поле предназначено для указания протокола (или всех протоколов), на основе которого будет осуществляться фильтрация. При выборе протокола возможны следующие варианты: icmp, igmp, ip, tcp, egr, igr, udp, hmp, rdp, idpr, ipv6, ipv6:rout, ipv6:frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipinip, pim, l2tp, isis, ipip, либо числовое значение протокола, в диапазоне (0 – 255). Для соответствия любому протоколу используется значение ip .
source	Адрес источника	Определяет IP-адрес источника пакета.

source-wildcard	Маска адреса источника	Битовая маска, применяемая к IP-адресу источника пакета. Маска определяет биты IP-адреса, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы. Например, используя маску, можно определить для правила фильтрации IP-сеть. Чтобы добавить в правило фильтрации IP-сеть 195.165.0.0, необходимо задать значение маски 0.0.255.255, то есть согласно данной маске последние 16 бит IP-адреса будут игнорироваться.
destination	Адрес назначения	Определяет IP-адрес назначения пакета.
destination-wildcard	Маска адреса назначения	Битовая маска, применяемая к IP-адресу назначения пакета. Маска определяет биты IP-адреса, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы. Маска используется аналогично маске source-wildcard .
dscp	Поле DSCP в заголовке L3	Определяет значение DSCP-поля diffserv. Возможные коды сообщений поля dscp : (0 – 63).
precedence	Приоритет IP	Определяет приоритет IP-трафика: (0-7).
time-name	Имя профиля конфигурации time-range	Определяет конфигурацию временных интервалов.
icmp-type		Тип сообщений протокола ICMP, используемый для фильтрации ICMP-пакетов. Возможные типы сообщений поля icmp-type : <i>echo-reply, destination-unreachable, source-quench, redirect, alternate-host-address, echo-request, router-advertisement, router-solicitation, time-exceeded, parameter-problem, timestamp, timestamp-reply, information-request, information-reply, address-mask-request, address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, mobile-registration-request, mobile-registration-reply, domain-name-request, domain-name-reply, skip, photuris</i> , либо числовое значение типа сообщения, в диапазоне (0 – 255).
icmp-code	Код сообщения протокола ICMP	Код сообщений протокола ICMP, используемый для фильтрации ICMP-пакетов. Возможные коды сообщений поля icmp-code : (0 – 255).
igmp-type	Тип сообщения протокола IGMP	Тип сообщений протокола IGMP, используемый для фильтрации пакетов IGMP. Возможные типы сообщений поля igmp-type : <i>host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3</i> , либо числовое значение типа сообщения, в диапазоне (0 – 255).
destination-port	UDP/TCP-порт назначения	Возможные значения поля TCP-порта: <i>bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110), syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80)</i> ; для UDP-порта <i>biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), on500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177)</i> . Либо числовое значение (0 – 65535).
source-port	UDP/TCP-порт источника	
list-of-flags	Флаги протокола TCP	Если для условия фильтрации флаг должен быть установлен, то перед ним ставится знак «+», если не должен быть установлен, то «-». Возможные варианты флагов: +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn и -fin . При использовании нескольких флагов в условии фильтрации, флаги объединяются в одну строку без пробелов, например: +fin-ack .

disable-port	Отключение порта	Выключает порт, с которого был принят пакет, удовлетворяющий условиям любой из команд запрета deny , в составе которой, было описано поле.
log-input	Отправка сообщений	Включает отправку информационных сообщений в системный журнал при получении пакета, который соответствует записи.
offset-list	Наименование списка шаблонов пользователя	Задаёт использование списка шаблонов пользователя для распознавания пакетов. Для каждого списка ACL может быть определен свой список шаблонов.
Index	Индекс правила	Индекс задаёт положение правила в списке и его приоритет. Чем меньше индекс – тем приоритетнее правило. Диапазон допустимых значений 1-2147483647.



Для выбора всего диапазона параметров, кроме **dscp** и **ip-precedence** используется параметр **any**.



После того как хотя бы одна запись добавлена в список ACL, последней по умолчанию добавляется запись **deny any any any**, которая означает игнорирование всех пакетов, не удовлетворяющих условиям ACL.

Таблица 5.208 - Команды, используемые для настройки ACL списков на основе IP-адресации

Команда	Действие
permit protocol {any source source-wildcard} {any destination destination-wildcard} [dscp dscp precedence precedence] [time-range time-name] [index index] [offset-list name]	Добавляет разрешающую запись фильтрации для протокола. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
permit icmp {any source source-wildcard} {any destination destination-wildcard} {any icmp-type} {any icmp-code} [dscp dscp ip-precedence precedence] [time-range time-name] [index index] [offset-list name]	Добавляет разрешающую запись фильтрации для протокола ICMP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
permit igmp {any source source-wildcard} {any destination destination-wildcard} [igmp-type] [dscp dscp precedence precedence] [time-range time-name] [index index] [offset-list name]	Добавляет разрешающую запись фильтрации для протокола IGMP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
permit tcp {any source source-wildcard} {any source-port} {any destination destination-wildcard} {any destination-port} [dscp dscp precedence precedence] [match-all list-of-flags] [time-range time-name] [index index] [offset-list name]	Добавляет разрешающую запись фильтрации для протокола TCP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
permit udp {any source source-wildcard} {any source-port} {any destination destination-wildcard} {any destination-port} [dscp dscp precedence precedence] [time-range time-name] [index index] [offset-list name]	Добавляет разрешающую запись фильтрации для протокола UDP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.

<p>deny protocol {any source source-wildcard} {any destination destination-wildcard} [dscp dscp precedence precedence] [time-range time-name] [disable-port log-input]] [index index] [offset-list name]</p>	<p>Добавляет запрещающую запись фильтрации для протокола. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова <i>disable-port</i> физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова <i>log-input</i> будет отправлено сообщение в системный журнал.</p>
<p>deny icmp {any source source-wildcard} {any destination destination-wildcard} {any icmp-type} {any icmp-code} [dscp dscp precedence precedence] [time-range time-name] [disable-port log-input]] [index index] [offset-list name]</p>	<p>Добавляет запрещающую запись фильтрации для протокола ICMP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова <i>disable-port</i> физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова <i>log-input</i> будет отправлено сообщение в системный журнал.</p>
<p>deny igmp {any source source-wildcard} {any destination destination-wildcard} [igmp-type] [dscp dscp precedence precedence] [time-range time-name] [disable-port log-input] [index index] [offset-list name]</p>	<p>Добавляет запрещающую запись фильтрации для протокола IGMP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова <i>disable-port</i> физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова <i>log-input</i> будет отправлено сообщение в системный журнал.</p>
<p>deny tcp {any source source-wildcard} {any source-port} {any destination destination-wildcard} {any destination-port} [dscp dscp precedence precedence] [match-all list-of-flags] [time-range time-name] [disable-port log-input] [index index] [offset-list name]</p>	<p>Добавляет запрещающую запись фильтрации для протокола TCP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова <i>disable-port</i> физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова <i>log-input</i> будет отправлено сообщение в системный журнал.</p>
<p>deny udp {any source source-wildcard} {any source-port} {any destination destination-wildcard} {any destination-port} [dscp dscp precedence precedence] [time-range time-name] [disable-port log-input] [index index] [offset-list name]</p>	<p>Добавляет запрещающую запись фильтрации для протокола UDP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова <i>disable-port</i> физический интерфейс, принявший такой пакет, будет выключен.</p>
<p>offset-list name { offset_base offset mask value}</p>	<p>Создаёт список шаблонов пользователя с именем <i>name</i>. Имя может включать от 1 до 32 символов. В одной команде может содержаться до пяти шаблонов, состоящих из следующих параметров: <i>offset_base</i> – базовое смещение. Возможные значения: L3 – начало заголовка IPv4; L4 – конец заголовка IPv4; <i>offset</i> – смещение байта данных в пределах пакета. Базовое смещение принимается за начало отсчета; <i>mask</i> – маска. В анализе пакета принимают участие только те разряды байта, для которых в соответствующих разрядах маски задана ‘1’; <i>value</i> – искомое значение.</p>
<p>no offset-list name</p>	<p>Удаляет созданный ранее список.</p>

5.26.2 Конфигурирование ACL на базе IPv6

В данном разделе приведены значения и описания основных параметров, используемых в составе команд настройки списков ACL, основанных на адресации IPv6.

Создание и вход в режим редактирования списков ACL, основанных на адресации IPv6, осуществляется по команде: `ipv6 access-list access-list`. Например, для создания списка ACL под названием MESipv6 необходимо выполнить следующие команды:

```
console#
console# configure
console(config)# ipv6 access-list MESipv6
console(config-ipv6-a1)#
```

Таблица 5.209 – Основные параметры, используемые в командах

Параметр	Значение	Действие
permit	Действие разрешить	Создает разрешающее правило фильтрации в списке ACL.
deny	Действие запретить	Создает запрещающее правило фильтрации в списке ACL.
protocol	Протокол	Поле предназначено для указания протокола (или всех протоколов), на основе которого будет осуществляться фильтрация. При выборе протокола возможны следующие варианты: icmp , tcp , udp , либо числовое значение протокола – icmp (58), tcp (6), udp (17). Для соответствия любому протоколу используется значение ipv6 .
source-prefix/length	Адрес отправителя и его длина	Определяет IPv6-адрес и длину префикса сети (0-128) (количество старших бит адреса) источника пакета.
destination-prefix/length	Адрес назначения и его длина	Определяет IPv6-адрес и длину префикса сети (0-128) (количество старших бит адреса) назначения пакета.
dscp	Поле DSCP в заголовке L3	Определяет значение DSCP-поля diffserv. Возможные коды сообщений поля dscp : (0 – 63).
precedence	Приоритет IP	Определяет приоритет IP-трафика:(0-7).
time-name	Имя профиля конфигурации time-range	Определяет конфигурацию временных интервалов.
icmp-type	Тип сообщения протокола ICMP	Используется для фильтрации ICMP-пакетов. Возможные типы и числовые значения сообщений поля icmp-type : <i>destination-unreachable</i> (1), <i>packet-too-big</i> (2), <i>time-exceeded</i> (3), <i>parameter-problem</i> (4), <i>echo-request</i> (128), <i>echo-reply</i> (129), <i>mld-query</i> (130), <i>mld-report</i> (131), <i>mldv2-report</i> (143), <i>mld-done</i> (132), <i>router-solicitation</i> (133), <i>router-advertisement</i> (134), <i>nd-ns</i> (135), <i>nd-na</i> (136).
icmp-code	Код сообщений протокола ICMP	Используется для фильтрации ICMP-пакетов. Возможные значения поля 0 – 255.
destination-port	UDP/TCP-порт назначения	Возможные значения поля TCP-порта: <i>bgp</i> (179), <i>chargen</i> (19), <i>daytime</i> (13), <i>discard</i> (9), <i>domain</i> (53), <i>drip</i> (3949), <i>echo</i> (7), <i>finger</i> (79), <i>ftp</i> (21), <i>ftp-data</i> (20), <i>gopher</i> (70), <i>hostname</i> (42), <i>irc</i> (194), <i>klogin</i> (543), <i>kshell</i> (544), <i>lpd</i> (515), <i>nntp</i> (119), <i>pop2</i> (109), <i>pop3</i> (110), <i>smtp</i> (25), <i>sunrpc</i> (1110), <i>syslog</i> (514), <i>tacacs-ds</i> (49), <i>talk</i> (517), <i>telnet</i> (23), <i>time</i> (37), <i>uucp</i> (117), <i>whois</i> (43), <i>www</i> (80); для UDP-порта <i>biff</i> (512), <i>bootpc</i> (68), <i>bootps</i> (67), <i>discard</i> (9), <i>dnsix</i> (90), <i>domain</i> (53), <i>echo</i> (7), <i>mobile-ip</i> (434), <i>nameserver</i> (42), <i>netbios-dgm</i> (138), <i>netbios-ns</i> (137), <i>on500-isakmp</i> (4500), <i>ntp</i> (123), <i>rip</i> (520), <i>snmp</i> (161), <i>snmptrap</i> (162), <i>sunrpc</i> (111), <i>syslog</i> (514), <i>tacacs-ds</i> (49), <i>talk</i> (517), <i>tftp</i> (69), <i>time</i> (37), <i>who</i> (513), <i>xdmcp</i> (177). Либо числовое значение (0 – 65535).
source-port	UDP/TCP-порт источника	
list-of-flags	Флаги протокола TCP	Если для условия фильтрации флаг должен быть установлен, то перед ним ставится знак «+», если не

		должен быть установлен, то «-». Возможные варианты флагов: +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn и -fin .
disable-port	Отключение порта	Выключает порт, с которого был принят пакет, удовлетворяющий условиям любой из команд запрета deny , в составе которой, было описано поле.
log-input	Отправка сообщений	Включает отправку информационных сообщений в системный журнал при получении пакета, который соответствует записи.
offset-list	Имя списка битовых полей	Задаёт правило фильтрации по битовой маске, начиная с точки смещения. Правило смещения описывается командой offset-list
Index	Индекс правила	Индекс правила в таблице, чем меньше индекс – тем приоритетнее правило. Возможные значения поля 1-2147483647



Для выбора всего диапазона параметров, кроме **dscp** и **ip-precedence** используется параметр «**any**».



После того, как хотя бы одна запись добавлена в список ACL, последними в список добавляются записи:

permit-icmp any any nd-ns any

permit-icmp any any nd-na any

deny ipv6 any any

Две первые из них разрешают поиск соседних IPv6 устройств с помощью протокола ICMPv6, а последняя означает игнорирование всех пакетов, не удовлетворяющих условиям ACL.

Таблица 5.210 – Команды, используемые для настройки ACL списков на основе IPv6-адресации

Команда	Действие
permit protocol { any <i>source-prefix/length</i> } { any <i>destination-prefix/length</i> } [dscp <i>dscp</i> precedence <i>precedence</i>] [time-range <i>time-name</i>]	Добавляет разрешающую запись фильтрации для протокола. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
permit icmp { any <i>source-prefix/length</i> } { any <i>destination-prefix/length</i> } { any <i>icmp-type</i> } { any <i>icmp-code</i> } [dscp <i>dscp</i> precedence <i>precedence</i>] [time-range <i>time-name</i>]	Добавляет разрешающую запись фильтрации для протокола ICMP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
permit tcp { any <i>source-prefix/length</i> } { any <i>source-port</i> } { any <i>destination-prefix/length</i> } { any <i>destination-port</i> } [dscp <i>dscp</i> precedence <i>precedence</i>] [time-range <i>time-name</i>] [match-all <i>list-of-flags</i>]	Добавляет разрешающую запись фильтрации для протокола TCP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
permit udp { any <i>source-prefix/length</i> } { any <i>source-port</i> } { any <i>destination-prefix/length</i> } { any <i>destination-port</i> } [dscp <i>dscp</i> precedence <i>precedence</i>] [time-range <i>time-name</i>]	Добавляет разрешающую запись фильтрации для протокола UDP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.

<p>deny protocol {any source-prefix/length} { any destination-prefix/length} [dscp dscp precedence precedence] [time-range time-name] [disable-port log-input]</p>	<p>Добавляет запрещающую запись фильтрации для протокола. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова <code>disable-port</code> физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова <code>log-input</code> будет отправлено сообщение в системный журнал.</p>
<p>deny icmp {any source-prefix/length} { any destination-prefix/length} {any icmp-type} {any icmp-code} [dscp dscp precedence precedence] [time-range time-name] [disable-port log-input]</p>	<p>Добавляет запрещающую запись фильтрации для протокола ICMP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова <code>disable-port</code> физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова <code>log-input</code> будет отправлено сообщение в системный журнал.</p>
<p>deny tcp {any source-prefix/length} {any source-port} { any destination-prefix/length} {any destination-port} [dscp dscp precedence precedence] [match-all list-of-flags] [time-range time-name] [disable-port log-input]</p>	<p>Добавляет запрещающую запись фильтрации для протокола TCP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова <code>disable-port</code> физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова <code>log-input</code> будет отправлено сообщение в системный журнал.</p>
<p>deny udp {any source-prefix/length} {any source-port} { any destination-prefix/length} {any destination-port} [dscp dscp precedence precedence] [match-all list-of-flags] [time-range time-name] [disable-port log-input]</p>	<p>Добавляет запрещающую запись фильтрации для протокола UDP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова <code>disable-port</code> физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова <code>log-input</code> будет отправлено сообщение в системный журнал.</p>
<p>offset-list name { offset_base offset mask value} ...</p>	<p>Создаёт список шаблонов пользователя с именем <i>name</i>. Имя может включать от 1 до 32 символов. В одной команде может содержаться до пяти шаблонов, состоящих из следующих параметров: <i>offset_base</i> – базовое смещение. Возможные значения: L3 – начало заголовка IPv4; L4 – конец заголовка IPv4; <i>offset</i> – смещение байта данных в пределах пакета. Базовое смещение принимается за начало отсчета; <i>mask</i> – маска. В анализе пакета принимают участие только те разряды байта, для которых в соответствующих разрядах маски задана '1'; <i>value</i> – искомое значение.</p>
<p>no offset-list name</p>	<p>Удаляет созданный ранее список.</p>

5.26.3 Конфигурирование ACL на базе MAC

В данном разделе приведены значения и описания основных параметров, используемых в составе команд настройки списков ACL, основанных на MAC-адресации.

Создание и вход в режим редактирования списков ACL, основанных на MAC-адресации, осуществляется по команде: `mac access-list extended access-list`. Например, для создания списка ACL под названием `MESmac` необходимо выполнить следующие команды:

```
console#
console# configure
console(config)# mac access-list extended MESmac
```

```
console(config-mac-al) #
```

Таблица 5.211 - Основные параметры, используемые в командах.

Параметр	Значение	Действие
permit	Действие разрешить	Создает разрешающее правило фильтрации в списке ACL.
deny	Действие запретить	Создает запрещающее правило фильтрации в списке ACL.
source	Адрес отправителя	Определяет MAC-адрес источника пакета.
source-wildcard	Битовая маска, применяемая к MAC-адресу источника пакета	Маска определяет биты MAC-адреса, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы. Например, используя маску, можно определить для правила фильтрации диапазона MAC-адресов. Чтобы добавить в правило фильтрации все MAC-адреса начинающиеся на 00:00:02:AA.xx.xx, необходимо задать значение маски 0.0.0.0.FF.FF, то есть, согласно данной маске, последние 32 бита MAC-адреса будут не важны для анализа.
destination	Адрес назначения	Определяет MAC-адрес назначения пакета.
destination-wildcard	Битовая маска, применяемая к MAC-адресу назначения пакета	Маска определяет биты MAC-адреса, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы. Маска используется аналогично маске source-wildcard .
vlan-id	Диапазон значений 0 – 4095	Подсеть VLAN фильтруемых пакетов.
cos	Диапазон значений 0 – 7	Класс обслуживания (CoS) фильтруемых пакетов.
cos-wildcard	Битовая маска, применяемая к классу обслуживания (CoS) фильтруемых пакетов	Маска определяет биты CoS, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы. Например, чтобы использовать в правиле фильтрации CoS 6 и 7, необходимо в поле CoS указать значение 6, либо 7, а в поле маски значение 1 (7 в двоичном представлении – 111, 1 – 001, получается, что последний бит, будет игнорироваться, то есть CoS может быть либо 110 (6), либо 111 (7)).
eth-type	Диапазон значений 0 – 0xFFFF	Ethernet тип фильтруемых пакетов в шестнадцатеричной записи.
disable-port	-	Выключает порт, с которого был принят пакет, удовлетворяющий условиям команды запрета deny .
log-input	Отправка сообщений	Включает отправку информационных сообщений в системный журнал при получении пакета, который соответствует записи.
time-name	Имя профиля конфигурации time-range	Определяет конфигурацию временных интервалов.
offset-list	Побайтовое смещение от ключевой точки	Задаёт правило фильтрации по битовой маске, начиная с точки смещения. Правило смещения описывается командой offset-list
index	Индекс правила	Индекс правила в таблице, чем меньше индекс – тем приоритетнее правило. Возможные значения поля 1-2147483647



Для выбора всего диапазона параметров, кроме **dscp** и **ip-precedence** используется параметр «**any**».



После того как хотя бы одна запись добавлена в список ACL, последней по умолчанию добавляется запись **deny-any-any**, которая означает игнорирование всех пакетов не удовлетворяющих условиям ACL.

Таблица 5.212 – Команды, используемые для настройки ACL-списков на основе MAC-адресации

Команда	Действие
permit {any {source source-wildcard} {any destination destination-wildcard} [vlan vlan-id] [cos cos cos-wildcard] [eth-type] [time-range time-name] [index index] [offset-list name]	Добавляет разрешающую запись фильтрации. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
deny {any {source source-wildcard} {any { destination destination-wildcard}} [vlan vlan-id] [cos cos cos-wildcard] [eth-type] [time-range time-name] [disable-port log-input] [index index] [offset-list name]	Добавляет запрещающую запись фильтрации. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова <code>disable-port</code> , физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова <code>log-input</code> будет отправлено сообщение в системный журнал.
offset-list name { offset_base offset mask value} ...	Создает список шаблонов пользователя с именем <i>name</i> . Имя может включать от 1 до 32 символов. В одной команде может содержаться до пяти шаблонов, состоящих из следующих параметров: <i>offset_base</i> – базовое смещение. Возможные значения: L2 начало смещения от Ethertype; outer-tag начало смещения от STAG; inner-tag начало смещения от STAG; src-mac начало смещения с MAC-адреса источника; dst-mac начало смещения с MAC-адреса назначения ; <i>offset.offset</i> – смещение байта данных в пределах пакета. Базовое смещение принимается за начало отсчета; <i>mask</i> – маска. В анализе пакета принимают участие только те разряды байта, для которых в соответствующих разрядах маски задана '1'; <i>value</i> – искомое значение.
no offset-list name	Удаляет созданный ранее список.

5.26.4 Настройка временных интервалов «time-range» для списков доступа

В данном разделе приводятся команды настройки временных интервалов для списков ACL.

Создание и вход в режим редактирования профиля конфигурации «time-range», осуществляется по команде: `time-range time-name`. Например, для создания профиля временных интервалов под названием `http-allowed` необходимо выполнить следующие команды:

```

console#
console# configure
console(config)# time-range http-allowed
console(config-time-range)#
    
```

Таблица 5.213 – Команды режима конфигурирования временных интервалов

Параметр	Значение	Действие
absolute start <i>hh:mm day month year</i>	<i>hh:mm: (0..23):(0..5)</i> <i>day: 1..31</i> <i>month: Jan .. Dec</i> <i>year: 2000..2097</i>	Устанавливает абсолютные время и дату, когда список доступа вступает в силу.
no absolute start		Удаляет ограничение по времени
absolute end <i>hh:mm day month year</i>		Устанавливает абсолютные время и дату завершения действия списка доступа.
no absolute end		Удаляет ограничение по времени. Если время и дата завершения действия списка доступа не установлены, то список доступа будет действовать неопределенный срок.

periodic <i>day-of-the-week hh:mm to day-of-the-week hh:mm</i>	<i>day-of-the-week: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday</i> <i>hh:mm: (0..23):(0..5)</i>	Устанавливает время и день недели, когда список доступа будет активен.
periodic list <i>hh:mm to hh:mm day-of-the-week1 [day-of-the-week2... day-of-the-week7]</i>		Удаляет ограничение по времени.
periodic list <i>hh:mm to hh:mm all</i>		
no periodic <i>day-of-the-week hh:mm to day-of-the-week hh:mm</i>		
no periodic list <i>hh:mm to hh:mm day-of-the-week1 [day-of-the-week2... day-of-the-week7]</i>		
no periodic list all <i>hh:mm to hh:mm all</i>		

5.27 Конфигурирование защиты от DoS-атак

Данный класс команд позволяет блокировать некоторые распространенные классы DoS-атак.

Команды режима глобального конфигурирования

Командная строка в режиме глобального конфигурирования имеет вид:

```
console (config) #
```

Таблица 5.214 – Команды для настройки защиты от DoS-атак

<i>Параметр</i>	<i>Значение</i>	<i>Действие</i>
security-suite deny martian-addresses <reserved add <ip> remove <ip>>	<i><ip></i> - валидный IP-адрес	Запрещает прохождение фреймов с недопустимыми («марсианскими») IP-адресами источника (loopback, broadcast, multicast).
security-suite dos protect <add remove> <stacheldraht invasor- trojan back-orifice-trojan>		Запрещает/разрешает прохождение определенных типов трафика, характерных для вредоносных программ: - stacheldraht – отбрасывает TCP-пакеты с портом источника 16660; - invasor-trojan – отбрасывает TCP-пакеты с портом назначения 2140 и портом источника 2140; - back-orifice-trojan – отбрасывает UDP-пакеты с портом назначения 31337 и портом источника 1024.
security-suite enable		Включает класс команд security-suite.
no security-suite enable		Отключает класс команд security-suite

Команды режима конфигурирования интерфейса Ethernet, группы портов

Командная строка в режиме конфигурирования интерфейса Ethernet, группы портов имеет вид:

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

Таблица 5.215 – Команда конфигурирования защиты от DoS-атак для интерфейсов

<i>Команда</i>	<i>Значение</i>	<i>Действие</i>
security-suite deny <fragmented icmp syn>	<i><ip></i> - валидный IP-адрес <i><mask></i> – маска в формате	Создает/удаляет правило, запрещающее прохождение трафика, соответствующего критериям:

<code><add remove> <any <ip> [<mask>]></code>	IP-адреса или префикса	- fragmented – фрагментированные пакеты; - icmp – ICMP-трафик; - syn – syn-пакеты.
<code>no security-suite deny <fragmented icmp syn> <add remove> <any <ip> [<mask>]></code>		Восстанавливает значение по умолчанию.
<code>security-suite dos syn- attack <rate> <any <ip> [<mask>]></code>	<code><rate></code> – скорость (5..1000 пакетов в секунду) <code><ip></code> - валидный IP-адрес <code><mask></code> – маска в формате IP-адреса или префикса	Задаёт порог syn-запросов на определенный IP-адрес/сеть, при превышении которого лишние фреймы будут отбрасываться.
<code>no security-suite dos syn- attack <any <ip> [<mask>]></code>		Восстанавливает значение по умолчанию.

5.28 Качество обслуживания - QoS

По умолчанию на всех портах коммутатора используется организация очереди пакетов по методу FIFO: первый пришел – первый ушел (First In – First Out). Во время интенсивной передачи трафика при использовании данного метода могут возникнуть проблемы, поскольку устройством игнорируются все пакеты, не вошедшие в буфер очереди FIFO, и соответственно теряются безвозвратно. Решает данную проблему метод, организующий очереди по приоритету трафика. Механизм QoS (Quality of service – качество обслуживания), реализованный в коммутаторе MES2124, позволяет организовать четыре очереди приоритета пакетов в зависимости от типа передаваемых данных.


5.28.1 Настройка QoS

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.216 – Команды режима глобального конфигурирования

Команда	Значение/Значение по умолчанию	Действие
<code>qos [basic advanced]</code>	-/basic	Разрешает коммутатору использовать QoS. - basic – базовый режим QoS; - advanced – расширенный режим конфигурирования QoS, включающий полный перечень команд настройки QoS.
<code>no qos</code>		Установить механизм передачи данных FIFO.  Настройки QOS при этом будут удалены.

class-map <i>class-map-name</i> [match-all match-any]	1..32 символов По умолчанию используется опция match-all	1. Создает список критериев классификации трафика. 2. Входит в режим редактирования списка критериев классификации трафика. - match-all – все критерии данного списка должны быть выполнены; - match-any – один, любой критерий данного списка должен быть выполнен. <input checked="" type="checkbox"/> В списке критериев может быть одно или два правила. Если правила два, и оба они указывают на разные типы ACL (IP, MAC), то классификация будет осуществляться по первому в списке верному правилу. <input checked="" type="checkbox"/> Действует только для режима qos advanced
no class-map <i>class-map-name</i>		Удаляет список критериев классификации трафика.
policy-map <i>policy-map-name</i>	1..32 символов	1. Создает стратегию классификации трафика. 2. Входит в режим редактирования стратегии классификации трафика. <input checked="" type="checkbox"/> В одном направлении поддерживается только одна стратегия классификации трафика. По умолчанию policy-map устанавливает DSCP=0 для IP-пакетов и CoS=0 для тегированных пакетов. <input checked="" type="checkbox"/> Действует только для режима qos advanced.
no policy-map <i>policy-map-name</i>		Удаляет правило классификации трафика.
qos aggregate-policer <i>aggregate-policer-name</i> <i>committed-rate-kbps</i> <i>excess-burst-byte</i> [exceed-action { drop policed-dscp-transmit }]	aggregate-policer-name: 1..32 символа committed-rate-kbps: 3..57982058 committed-burst-byte: 3000..19173960	Определяет шаблон настроек, который позволяет ограничить полосу пропускания канала и в то же время гарантировать определенную скорость передачи данных. При работе с полосой пропускания используется алгоритм маркированной «корзины». Задачей алгоритма является принятие решения: передать пакет или отбросить. Параметрами алгоритма являются – скорость поступления (CIR) маркеров в «корзину» и объём (CBS) «корзины». - committed-rate-kbps – среднее значение скорости трафика, кбит/с. Данная скорость гарантируется при передаче информации; - committed-burst-byte – размер сдерживающего порога в байтах; - drop – пакет будет отброшен, когда «корзина» переполнится; - policed-dscp-transmit – при переполнении «корзины» значение DSCP будет переопределено. <input checked="" type="checkbox"/> Нельзя удалить шаблон настроек, если он используется в стратегии policy map, перед удалением следует удалить назначение шаблона стратегии: no police aggregate aggregate-policer-name <input checked="" type="checkbox"/> Действует только для режима qos advanced.
no qos aggregate-policer <i>aggregate-policer-name</i>		Удаляет шаблон настроек регулирования скорости канала.
wrr-queue cos-map <i>queue-id</i> <i>cos1...cos8</i>	queue-id: 1..4 cos1...cos8: 0..7 Значения CoS по умолчанию для очередей:	Определяет значения CoS для очередей исходящего трафика.
no wrr-queue cos-map [<i>queue-id</i>]	CoS = 1 – очередь 1 CoS = 2 – очередь 1 CoS = 0 – очередь 2 CoS = 3 – очередь 2 CoS = 4 – очередь 3 CoS = 5 – очередь 3 CoS = 6 – очередь 4 CoS = 7 – очередь 4	Устанавливает значения по умолчанию.
wrr-queue bandwidth	0..255/1	Присваивает вес исходящим очередям, используемый

<i>weight1 weight2 weight3 weight4</i>	По умолчанию вес каждой очереди равен 1	механизмом WRR (Weighted Round Robin – весовой механизм распределения нагрузки).
no wrr-queue bandwidth		Устанавливает значение по умолчанию.
priority-queue out num-of-queues number-of-queues	number-of-queues: 0..4 По умолчанию, все очереди обрабатываются по алгоритму «strict priority».	Задаёт количество приоритетных очередей. <input checked="" type="checkbox"/> Для приоритетной очереди вес WRR будет игнорироваться. Если задается отличное от «0» значение N, то старшие N очередей будут приоритетными (не будут участвовать в WRR). Пример: 0: все очереди равноправны; 1: семь младших очередей участвуют в WRR, 8-ая не участвует; 2: шесть младших очередей участвуют в WRR, 7,8 не участвуют.
no priority-queue out num-of-queues		Устанавливает значение по умолчанию.
qos wrr-queue threshold gigabitethernet <i>queue-id threshold-percentage</i>	queue-id: 1..4 threshold-percentage: 0..100 По умолчанию значение пороговых настроек для отбрасывания избыточного трафика равно 80%	Устанавливает пороговые значения для отбрасывания избыточного трафика очереди. <input checked="" type="checkbox"/> Объем трафика в зависимости от его приоритета сравнивается с соответствующим порогом. Если порог превышен, пакеты с соответствующим приоритетом сброса будут отбрасываться в течение всего времени, пока порог превышен. Действует только для режима qos advanced.
no qos wrr-queue threshold gigabitethernet <i>queue-id</i>		Устанавливает значения порогов по умолчанию
qos wrr-queue wrtd	По умолчанию WRD выключено	Включает WRD. <input checked="" type="checkbox"/> Изменения вступят в силу после перезагрузки устройства.
no qos wrr-queue wrtd		Выключает WRD.
qos map policed-dscp <i>dscp-list to dscp-mark-down</i>	dscp-list: 0..63 dscp-mark-down: 0..63 По умолчанию таблица повторной маркировки является пустой, то есть значения DSCP для всех входящих пакетов остаются неизменными.	Заполняет таблицу перемаркировки DSCP. Для входящих пакетов с указанными значениями DSCP задает новое значение DSCP. - dscp-list – определяет до 8 значений DSCP, значения разделяются знаком пробела. - dscp-mark-down – определяет новое значение dscp. <input checked="" type="checkbox"/> Действует только для режима qos advanced.
no qos map policed-dscp [<i>dscp-list</i>]		Устанавливает значение по умолчанию.
qos map dscp-queue <i>dscp-list to queue-id</i>	dscp-list: 0..63 queue-id: 1..4 Значения по умолчанию: DSCP: 0-15, очередь 1 DSCP: 15-31, очередь 2 DSCP: 32-47, очередь 3 DSCP: 48-53, очередь 4 DSCP: 54-63,	Устанавливает соответствие между значениями DSCP входящих пакетов и очередями. - dscp-list – определяет до 8 значений DSCP, значения разделяются знаком пробела. <input checked="" type="checkbox"/> Действует только для режима qos advanced.
no qos map dscp-queue [<i>dscp-list</i>]		Устанавливает значения по умолчанию
qos map dscp-dp <i>dscp-list to dp</i>	dscp-list: 0..63 dp: 0..2 По умолчанию все пакеты имеют приоритет сброса dp=0	Ставит в соответствие значению DSCP приоритет отброса (чем выше числовое значение приоритета, тем ниже вероятность того, что пакет будет отброшен; в первую очередь отбрасываются пакеты с приоритетом сброса 0, затем 1, затем 2) - dscp-list – определяет до 8 значений DSCP, значения разделяются знаком пробела. <input checked="" type="checkbox"/> Действует только для режима qos advanced.

no qos map dscp-dp [<i>dscp-list</i>]		Устанавливает значения по умолчанию.
qos trust { <i>cos</i> <i>dscp</i> }	-/cos	Устанавливает режим доверия коммутатора в базовом режиме QoS (CoS или DSCP). - cos – устанавливает классификацию входящих пакетов по значениям CoS. Для нетегированных пакетов используется значение CoS по умолчанию; - dscp – устанавливает классификацию входящих пакетов по значениям DSCP. <input checked="" type="checkbox"/> Действует только для режима qos basic.
no qos trust		Устанавливает значения по умолчанию.
qos dscp-mutation	-	Позволяет применить таблицу изменений dscp к совокупности dscp-доверенных портов. Использование таблицы изменений позволяет перезаписать значения dscp в IP-пакетах на новые значения. <input checked="" type="checkbox"/> Применить таблицу изменений DSCP возможно только для входящего трафика доверенных портов. <input checked="" type="checkbox"/> Действует только для режима qos basic.
no qos dscp-mutation		Отменяет использование карты изменений dscp.
qos map dscp-mutation <i>in-dscp to out-dscp</i>	in-dscp: 0..63, out-dscp: 0..63 По умолчанию карта изменений является пустой, то есть значения DSCP для всех входящих пакетов остаются неизменными	Заполняет таблицу перемаркировки DSCP. Для входящих пакетов с указанными значениями DSCP задает новые значения DSCP. - in-dscp – определяет до 8 значений DSCP, значения разделяются знаком пробела. - out-dscp – определяет до 8 новых значений DSCP, значения разделяются знаком пробела. <input checked="" type="checkbox"/> Действует только для режима qos basic.
no qos map dscp-mutation [<i>in-dscp</i>]	-	Устанавливает значения по умолчанию.
rate-limit <i>vlan_id rate burst</i>	vlan_id: 1 .. 4094; rate: 3 .. 57982058 кбит/с burst: 3000 .. 19173960 байт /128кбайт	Устанавливает ограничение скорости для входящего трафика для заданной VLAN. - <i>vlan_id</i> – номер VLAN; - <i>rate</i> – средняя скорость трафика (CIR), кбит/с; - <i>burst</i> – размер сдерживающего порога (ограничение скорости) в байтах.
no rate-limit		Снимает ограничение скорости входящего трафика.

Команды режима редактирования списка критериев классификации трафика

Вид запроса командной строки режима редактирования списка критериев классификации трафика:

```
console# configure
console(config)# class-map class-map-name [match-all|match-any]
console(config-cmap)#
```

Таблица 5.217 – Команды режима редактирования списка критериев классификации трафика

Команда	Значение	Действие
match <i>access-group acl-name</i>	1..32 символов	Добавляет критерий классификации трафика. Определяет правила фильтрации трафика по списку ACL для классификации. <input checked="" type="checkbox"/>

		Действует только для режима qos advanced.
<code>no match access-group acl-name</code>		Удаляет критерий классификации трафика.

Команды режима редактирования стратегии классификации трафика

Вид запроса командной строки режима редактирования стратегии классификации трафика:

```
console# configure
console(config)# policy-map policy-map-name
console(config-pmap)#
```

Таблица 5.218 – Команды режима редактирования стратегии классификации трафика

Команда	Значение	Действие
<code>class class-map-name</code> <code>[access-group acl-name]</code>	1..32 символов	<p>Определяет правило классификации трафика и входит в режим конфигурирования правила классификации – policy-map class.</p> <p>- access-group – определяет правила фильтрации трафика по списку ACL для классификации. При создании нового правила классификации, опциональный параметр access-group обязателен.</p> <p><input checked="" type="checkbox"/> Для того чтобы использовать настройки стратегии policy-map для интерфейса, используйте команду service-policy в режиме конфигурации интерфейса.</p> <p><input checked="" type="checkbox"/> Действует только для режима qos advanced.</p>
<code>no class class-map-name</code>		Удаляет правило классификации трафика class-map из стратегии policy-map.

Команды режима конфигурирования правила классификации

Вид запроса командной строки режима конфигурирования правила классификации:

```
console# configure
console(config)# policy-map policy-map-name
console(config-pmap)# class class-map-name [access-group acl-name]
console(config-pmap-c)#
```

Таблица 5.219 – Команды режима конфигурирования правила классификации

Команда	Значение	Действие
<code>trust [cos dscp cos-dscp]</code>	По умолчанию режим доверия не установлен	<p>Определяет режим доверия к определенному типу трафика. Данной командой выбирается значение, которое QoS будет использовать в качестве внутреннего DSCP.</p> <p>- cos – в качестве внутреннего DSCP используется CoS;</p> <p>- dscp – в качестве внутреннего DSCP используется DSCP входящих пакетов (значение по умолчанию);</p> <p>- cos-dscp – в качестве внутреннего DSCP используется DSCP входящих пакетов, если это IP-пакеты, иначе CoS.</p> <p><input checked="" type="checkbox"/> Действует только для режима qos advanced.</p>
<code>no trust</code>		Устанавливает значение по умолчанию.
<code>set</code>	new-dscp: 0..63	Устанавливает новые значения для IP-пакета.

<code>{dscp new-dscp queue queue-id cos new-cos}</code>	queue-id: 1..4 new-cos: 0..7	<input checked="" type="checkbox"/> Команда <code>set</code> является взаимоисключающей с командой <code>trust</code> для одной и той же стратегии <code>policy-map</code> . <input checked="" type="checkbox"/> Стратегии <code>policy-map</code> , использующие команды <code>set</code> , <code>trust</code> или имеющий классификацию ACL, назначаются только для исходящих интерфейсов. <input checked="" type="checkbox"/> Действует только для режима <code>qos advanced</code> .
<code>no set</code>		Удаляет новые значения для IP-пакета.
<code>police committed-rate-kbps committed-burst-byte [exceed-action {drop policed-dscp-transmit}]</code>	committed-rate: 3..12582912 кбит/с committed-burst: 3000..19173960 байт	<p>Позволяет ограничить полосу пропускания канала и в то же время гарантировать определенную скорость передачи данных.</p> <p>При работе с полосой пропускания используется алгоритм маркированной «корзины». Задачей алгоритма является принятие решения: передать пакет или отбросить. Параметрами алгоритма являются – скорость поступления (CIR) маркеров в «корзину» и объём (CBS) «корзины».</p> <ul style="list-style-type: none"> - committed-rate-kbps – среднее значение скорости трафика, кбит/с. Данная скорость гарантируется при передаче информации; - committed-burst-byte – размер сдерживающего порога в байтах; - drop – пакет будет отброшен, когда «корзина» переполнится; - policed-dscp-transmit – при переполнении «корзины», значение DSCP будет переопределено. <input checked="" type="checkbox"/> Действует только для режима <code>qos advanced</code> .
<code>no police</code>		Отключает регулирование скорости канала.
<code>police aggregate aggregate-policer-name</code>	1..32 символов	<p>Назначает правилу классификации трафика шаблон настроек, который позволяет ограничить полосу пропускания канала и в то же время гарантировать определенную скорость передачи данных.</p> <input checked="" type="checkbox"/> Действует только для режима <code>qos advanced</code> .
<code>no police aggregate aggregate-policer-name</code>		Удаляет шаблон настроек регулирования скорости канала из правила классификации трафика.

Команды режима конфигурирования интерфейса Ethernet, группы портов

Вид запроса командной строки режима конфигурирования интерфейса Ethernet, группы портов:

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

Таблица 5.220 – Команды режима конфигурирования интерфейса Ethernet, группы портов.

Команда	Значение	Действие
<code>service-policy input policy-map-name</code>	1..32 символов	<p>Назначает интерфейсу стратегию классификации трафика.</p> <input checked="" type="checkbox"/> В одном направлении интерфейсом поддерживается только одна стратегия классификации трафика. <input checked="" type="checkbox"/> Действует только для режима <code>qos advanced</code> .
<code>no service-policy input</code>		Удаляет стратегию классификации трафика с интерфейса.
<code>traffic-shape committed-rate [committed-burst]</code>	committed-rate: 64..1000000 кбит/с committed-burst:	<p>Устанавливает ограничение скорости для исходящего трафика через интерфейс.</p> <ul style="list-style-type: none"> - committed-rate – средняя скорость трафика, кбит/с; - committed-burst – размер сдерживающего порога

	4096..16769020 байт	(ограничение скорости) в байтах.
no traffic-shape		Снимает ограничение скорости исходящего трафика через интерфейс.
traffic-shape queue <i>queue-id committed-rate</i> [<i>committed-burst</i>]	committed-rate: 64..1000000 кбит/с committed-burst: 4096..16769020 байт	Устанавливает ограничение скорости трафика через интерфейс для исходящей очереди. - committed-rate – средняя скорость трафика, кбит/с; - committed-burst – размер сдерживающего порога (ограничение скорости) в байтах.
no traffic-shape queue <i>queue-id</i>	queue-id: 0-8	Снимает ограничение скорости трафика через интерфейс для исходящей очереди.
qos trust	-/включено	Включает базовый механизм qos для интерфейса. <input checked="" type="checkbox"/> Действует только для режима qos basic.
no qos trust		Выключает базовый механизм qos для интерфейса.
rate-limit rate [burst]	rate: 3 .. 10485760 кбит/с burst: 3000 .. 19173960 байт /128кбайт	Устанавливает ограничение скорости для входящего трафика. <input checked="" type="checkbox"/> Ограничение скорости для конкретного порта может быть применено, только если к нему не применена команда port storm-control broadcast enable. <input checked="" type="checkbox"/> Данная команда доступна только в режиме конфигурирования интерфейса Ethernet.
no rate-limit		Снимает ограничение скорости входящего трафика.
qos cos <i>default-cos</i>	0..7/0	Устанавливает значение CoS по умолчанию для порта (CoS, применяемый для всего нетегированного трафика, проходящего через интерфейс) <input checked="" type="checkbox"/> Данная команда доступна только в режиме конфигурирования интерфейса Ethernet.
no qos cos		Устанавливает значение по умолчанию.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

console#

Таблица 5.221 – Команды режима EXEC

Команда	Действие
show qos	Показывает режим QOS настроенный на устройстве. В базовом режиме показывает «доверенный» режим (trust mode).
show class-map [<i>class-map-name</i>]	Показывает списки критериев классификации трафика. <input checked="" type="checkbox"/> Действует только для режима qos advanced.
show policy-map [<i>policy-map-name</i>]	Показывает правила классификации трафика. <input checked="" type="checkbox"/> Действует только для режима qos advanced.
show qos aggregate-policer [<i>aggregate-policer-name</i>]	Показывает настройки средней скорости, и ограничения полосы пропускания для правил классификации трафика. <input checked="" type="checkbox"/> Действует только для режима qos advanced.
show qos interface [<i>buffers</i> <i>queueing</i> <i>policers</i> <i>shapers</i> <i>rate-limit</i>] [<i>gigabitethernet gi_port</i> <i>fastethernet fa_port</i> <i>port-channel group</i> <i>vlan vlan_id</i>]	Показывает QoS-параметры для интерфейса. - <i>vlan_id</i> – номер VLAN (1..4094); - <i>gi_port</i> – номер интерфейсов Ethernet g1-g24 (1..8/0/1..24); - <i>fa_port</i> – номер интерфейсов Ethernet XG1-XG4(1..8/0/1..24); - <i>group</i> – номер группы портов (1..8); - <i>buffers</i> – настройки буфера для очередей интерфейса; - <i>queueing</i> – алгоритм обработки очередей (WRR или EF), вес для WRR очередей, классы обслуживания для очередей и приоритет для EF; - <i>policers</i> – сконфигурированные стратегии классификации трафика для интерфейса; - <i>shapers</i> – ограничение скорости для исходящего трафика; - <i>rate-limit</i> – ограничение скорости для входящего трафика.
show qos map [<i>dscp-queue</i>]	Показывает информацию о замене полей в пакетах, используемых QOS. - <i>dscp-queue</i> – таблица соответствия DSCP и очередей;

dscp-dp policed-dscp dscp-mutation]	- dscp-dp – таблица соответствия меток DSCP и приоритета сброса (DP); - policed-dscp – таблица перемаркировки DSCP; - dscp-mutation – таблица изменения DSCP-to-DSCP.
--	---

Примеры выполнения команд.

- Включить режим QoS advanced. Распределить трафик по очередям, пакеты с DSCP 12 в первую очередь, пакеты с DSCP 16 во вторую. Восьмая очередь – приоритетная. Создать стратегию классификации трафика по списку ACL, разрешающему передачу TCP-пакетов с DSCP 12 и 16 и ограничивающую скорость – средняя скорость 1000 Кбит/с, порог ограничения 200000 байт. Использовать данную стратегию на интерфейсах Ethernet 14 и 16.

```

console#
console# configure
console(config)# ip access-list tcp_ena
console(config-ip-af)# permit tcp any any dscp 12
console(config-ip-af)# permit tcp any any dscp 16
console(config-ip-af)# exit
console(config)# qos advanced
console(config)# qos map dscp-queue 12 to 1
console(config)# qos map dscp-queue 16 to 2
console(config)# priority-queue out num-of-queues 1
console(config)# policy-map traffic
console(config-pmap)# class class1 access-group tcp_ena
console(config-pmap-c)# police 1000 200000 exceed-action drop
console(config-pmap-c)# exit
console(config-pmap)# exit
console(config)# interface gigabitethernet 1/0/14
console(config-if)# service-policy input
console(config-if)# exit
console(config)# interface gigabitethernet 1/0/16
console(config-if)# service-policy input
console(config-if)# exit
console(config)#

```

5.28.2 Статистика QoS

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.222 – Команды режима глобального конфигурирования.

Команда	Значение/Значение по умолчанию	Действие
qos statistics aggregate-policer <i>aggregate-policer-name</i>	1..32 символов	Включает QoS-статистику по ограничению полос пропускания.
no qos statistics aggregate-policer <i>aggregate-policer-name</i>	По умолчанию QoS-статистика отключена	Отключает QoS-статистику по ограничению полос пропускания.
qos statistics queues set { <i>queue</i> all }{ <i>dp</i> all } { gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> all }	set: 1..2 queue: 1..4 dp: {high, low} gi_port: {1..8/0/1..24} fa_port: {1..8/0/1..24}	Включает QoS -статистику для выходных очередей. - set – определяет набор счетчиков; - dp – определяет приоритет сброса.
no qos statistics queues set	Значение по умолчанию: Set 1: все приоритеты, все	Отключает QoS-статистику для выходных очередей.

	очереди, высокий приоритет сброса. Set 2: все приоритеты, все очереди, низкий приоритет сброса.	
--	--	--

Команды режима конфигурирования интерфейса Ethernet, группы портов

Вид запроса командной строки режима конфигурирования интерфейса Ethernet, группы портов:

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

Таблица 5.223 – Команды режима конфигурирования интерфейса Ethernet.

Команда	Значение	Действие
qos statistics policer <i>policy-map-name</i> <i>class-map-name</i>	policy-map-name: 1..32 символов class-map-name: 1..32 символов	Включает сбор QoS-статистики на интерфейсе. - policy-map-name – стратегия классификации трафика; - class-map-name – список критериев классификации трафика.
no qos statistics policer <i>policy-map-name</i> <i>class-map-name</i>	По умолчанию сбор QoS-статистики отключен	Отключает сбор QoS-статистики на интерфейсе.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.224 – Команды режима EXEC.

Команда	Действие
clear qos statistics	Очищает статистику QoS.
show qos statistics	Показывает статистику QoS.

6 СЕРВИСНОЕ МЕНЮ, СМЕНА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

6.1 Меню Startup

Меню **Startup** используется для выполнения специальных процедур, таких как: обновление программного обеспечения, удаление содержимого флэш-памяти, восстановление пароля, диагностика, задание скорости работы терминала, работа с параметрами стека устройства.

Для входа в меню **Startup** необходимо прервать загрузку нажатием клавиши **<Esc>** или **<Enter>** в течение первых двух секунд после появления сообщения автозагрузки (по окончании выполнения процедуры POST).

```
Startup Menu
```

```
[1] Download Software
[2] Erase Flash File
[3] Password Recovery Procedure
[4] Set Terminal Baud-Rate
[5] Stack menu
[6] Back
```

```
Enter your choice or press 'ESC' to exit:
```

Для выхода из меню и загрузки устройства нажмите клавишу **<6>**, либо **<esc>**.



Если в течение 15 секунд (значение по умолчанию) не выбран ни один из пунктов меню, то загрузка устройства продолжится. Время ожидания можно увеличить с помощью команд консоли.

Таблица 6.1 – Описание меню Startup

№	Название	Описание
<1>	Download Software Обновление программного обеспечения	<p>Для загрузки программного обеспечения используется протокол X-Modem. При нажатии клавиши <1> на консоль будет выведено следующее сообщение:</p> <p style="text-align: center;">Downloading code using XMODEM.</p> <p>Теперь, когда устройство готово к приему файла, необходимо передать его при помощи протокола X-Modem. После приема файла устройство перезагрузится автоматически.</p>
<2>	Erase Flash File Удаление содержимого флэш-памяти	<p>Данная процедура используется для удаления конфигурации устройства. Для удаления файла нажать клавишу <2>, появится предупреждение (подтвердите нажатием клавиши <y>):</p> <p style="text-align: center;">Warning! About to erase a Flash file. Are you sure (Y/N) ? y</p> <p>Ввести имя для нового файла конфигурации (в примере ниже, имя – config):</p> <p style="text-align: center;">Write Flash file name (Up to 8 characters, Enter for none.):config File config (if present) will be erased after system initialization.</p> <p>Для возврата в меню Startup нажать клавишу <enter>.</p> <p style="text-align: center;">==== Press Enter To Continue ====</p> <p><input checked="" type="checkbox"/> Для нового файла конфигурации имя должно быть отлично от имени конфигурации записанной на данный момент.</p>

<3>	Password Recovery Procedure Восстановление пароля	Данная процедура используется для восстановления утраченного пароля, она позволяет подключиться к устройству без пароля. Для восстановления пароля нажать клавишу <3> , при последующем подключении к устройству пароль будет проигнорирован. Current password will be ignored! Для возврата в меню Startup нажмите клавишу [enter] . ==== Press Enter To Continue ====
<4>	Set Terminal Baud-Rate Задание скорости работы терминала	Процедура используется для установки скорости работы терминала (по умолчанию 115200 Бод). Для задания новой скорости работы терминала нажать клавишу <5> и введите значение: Set new device Baud rate: 115200 Для возврата в меню Startup нажать клавишу <enter> . ==== Press Enter To Continue ====
<5>	Stack menu Работа с параметрами стека устройства	Для увеличения количества портов коммутатора, существует возможность объединения устройств в стек. В стек может быть объединено до 8 устройств, устройство с идентификатором 1 будет ведущим, остальные - ведомыми. Коммутатор MES1024/MES1124/MES2124 может работать как автономно, так и в составе стека. Для идентификации и установки режима работы устройства в стеке используется меню стека (Stack menu). Для входа в меню стека нажать клавишу <5> : Stack menu [1] Show unit stack id [2] Set unit stack id [3] Set unit working mode [4] Back Enter your choice or press 'ESC' to exit: Описание <i>Stack menu</i> указано в таблице 4.3
<6>	Back Выход из меню	Для выхода из меню и загрузки устройства нажмите клавишу <6> , либо <esc> .

Таблица 6.2 – Описание меню Stack menu, работа с параметрами стека устройства

№	Название меню	Описание
<1>	Show unit stack id Просмотр идентификатора устройства в стеке	Для просмотра идентификатора устройства в стеке нажмите клавишу <1> : Current working mode is stacking. Unit stack id set to 1.
<2>	Set unit stack id Назначение идентификатора устройства в стеке	Для назначения идентификатора устройства в стеке нажмите клавишу <2> : Enter unit stack id [0-8]: 1 Unit stack id updated to 1. где значение от «1» до «8» – номер устройства в стеке, значение «0» - автономный режим работы коммутатора. Для возврата в меню стека нажмите клавишу <enter> . ==== Press Enter To Continue ====
<3>	Set unit working mode Установка режима работы устройства	Для установки режима работы устройства нажмите клавишу <3> : Enter unit working mode [1- standalone, 2- stacking]:1 Unit working mode changed to standalone. где значение 1 – автономный режим, значение 2 – режим стекирования. Для возврата в меню стека нажмите клавишу <enter> . ==== Press Enter To Continue ====
<4>	Back Выход из меню	Для выхода из меню нажмите клавишу <4>

6.2 Обновление программного обеспечения с сервера TFTP



Сервер TFTP должен быть запущен и настроен на компьютере, с которого будет загружаться программное обеспечение. Файлы с загрузочным и/или системным программным обеспечением должны быть доступны серверу. Компьютер с запущенным TFTP-сервером доступен коммутатору MES1024/MES1124/MES2124 (можно проконтролировать, выполнив на коммутаторе команду `ping {A.B.C.D}`, где A.B.C.D – IP-адрес компьютера).



Обновление программного обеспечения может осуществляться только привилегированным пользователем.

6.2.1 Обновление системного программного обеспечения

Загрузка устройства осуществляется из файла системного программного обеспечения (ПО), который хранится во флэш-памяти. При обновлении, новый файл системного ПО сохраняется в специально выделенной области памяти. При загрузке устройство запускает активный файл системного ПО. Выбор активного файла задается командой:

```
boot system [unit unit] { image-1 | image-2 }
```

где *unit* – номер устройства в стеке (для устройства, работающего в автономном режиме, номер устройства не задается), *image-1*, *image-2* – файл системного ПО.



При работе в стеке, если номер устройства не задан, данная команда применяется к ведущему устройству.

Для просмотра текущей версии системного программного обеспечения, работающего на устройстве, введите команду `show version`:

```
console# show version
```

Unit	SW version	Boot version	HW version
1	3.0.0.0	3.0.0.0	01.00.00

Процедура обновления ПО:

1. Командой `copy` скопировать новый файл программного обеспечения на устройство в выделенную область памяти (*image2*). Формат команды `copy tftp://{tftp ip address}/{file name} image`.

Пример выполнения команды:

```
console# copy tftp://192.168.16.34/file1 image
```

```
Accessing file `file1' on 192.168.16.34
Loading file1 from 192.168.16.34:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Copy took 00:01:11 [hh:mm:ss]
```



Знак восклицания указывает на то, что идет процесс копирования. Каждый восклицательный знак соответствует успешной передаче 10 пакетов по 512 байт

информации каждый. Точка указывает на то, что в процессе копирования произошел таймаут ожидания пакетов от TFTP-сервера. Несколько точек в строке может означать, что возникла ошибка в процессе копирования.

2. Командой `boot` выберите активный файл системного ПО для последующей загрузки: `boot system [unit unit] { image-1 | image-2 }`.

```
console# boot system image-2
```



Если не выбран новый загруженный файл системного ПО активным, то устройство выполнит загрузку с использованием текущего активного образа.

3. Убедитесь, что правильно выбран активный файл системного ПО. Для просмотра данных о версиях программного обеспечения и их активности введите команду `show bootvar`:

```
console# show bootvar
```

Unit	Image	Filename	Version	Date	Status
1	1	image-1	3.0.0.0	17-Nov-2008 11:51:22	Active
1	2	image-2	3.0.0.0	28-Nov-2008 16:35:43	Not active*



Символом «*» отмечается файл программного обеспечения, который будет исполняться при последующей загрузке.

4. Перезагрузите коммутатор командой `reload`.

```
console# reload
```

```
This command will reset the whole system and disconnect your current session. Do you want to continue (y/n) [n]?
```

Подтвердите перезагрузку вводом 'y'.

6.2.2 Обновление загрузочного файла устройства (начального загрузчика)

Начальный загрузчик запускается сразу после включения питания устройства. Посредством загрузочного файла осуществляется процедура «тестирования системы при включении» (POST), распаковка и запуск файла системного ПО. При обновлении новый файл начального загрузчика сохраняется на flash на месте старого.

Для просмотра текущей версии загрузочного файла, работающего на устройстве, введите команду `show version`:

```
console# show version
```

Unit	SW version	Boot version	HW version
1	3.0.0.0	3.0.0.0	01.00.00

Процедура обновления ПО:

1. Командой `copy` скопировать новый загрузочный файл на устройство. Формат команды: `copy tftp://{tftp ip address}/{file name} boot`.

```
console# copy tftp://192.168.16.34/332448-10018.rfb boot
```

```
Erasing file..done.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Copy: 2739187 bytes copied in 00:01:18 [hh:mm:ss]
```



Знак восклицания указывает на то, что идет процесс копирования. Каждый восклицательный знак соответствует успешной передаче 10 пакетов по 512 байт информации каждый. Точка указывает на то, что в процессе копирования произошел таймаут ожидания пакетов от TFTP-сервера. Несколько точек в строке может означать, что возникла ошибка в процессе копирования.

2. Перезагрузите коммутатор командой `reload`.

```
console# reload
```

```
This command will reset the whole system and disconnect your current
session. Do you want to continue (y/n) [n]?
```

Подтвердите перезагрузку вводом 'y'.

ПРИЛОЖЕНИЕ А ПРИМЕРЫ ПРИМЕНЕНИЯ И КОНФИГУРИРОВАНИЯ УСТРОЙСТВА

Настройка протокола множества связующих деревьев (MSTP)

Протокол MSTP позволяет строить множество связующих деревьев для отдельных групп VLAN на коммутаторах локальной сети, что позволяет балансировать нагрузку. Для простоты рассмотрим случай с тремя коммутаторами, объединенными в кольцевую топологию.

Пусть vlan 10, 20, 30 объединяются в первом экземпляре MSTP, vlan 40, 50, 60 объединяются во втором экземпляре. Необходимо, чтобы трафик VLAN-ов 10, 20, 30 между первым и вторым коммутаторами передавался напрямую, а трафик VLAN-ов 40, 50, 60 передавался транзитом через коммутатор 3. Коммутатор 2 назначим корневым для внутреннего связующего дерева (IST – Internal Spanning Tree) в котором передается служебная информация. Коммутаторы объединяются в кольцо, используя порты g1 и g2. Ниже приведена схема, изображающая логическую топологию сети.



Рисунок 15- Настройка протокола множества связующих деревьев

Когда один из коммутаторов выходит из строя, либо обрывается канал, множество деревьев MSTP перестраивается, что позволяет минимизировать последствия аварии. Ниже приведен процесс конфигурации коммутаторов. Для более быстрой настройки создается общий конфигурационный шаблон, который загружается на TFTP-сервер и используется впоследствии для настройки всех коммутаторов.

1. Создание шаблона и конфигурация первого коммутатора

```
console# configure
console(config)# vlan database
console(config-vlan)# vlan 10,20,30,40,50,60
console(config-vlan)# exit
console(config)# interface vlan 1
console(config-if)# ip address 192.168.16.1 /24
console(config-if)# exit
console(config)# spanning-tree mode mstp
console(config)# interface range gigabitethernet 1/0/1-2
console(config-if)# switchport mode trunk
```

```

console(config-if)# switchport trunk allowed vlan add 10,20,30,40,50,60
console(config-if)# exit
console(config)# spanning-tree mst configuration
console(config-mst)# name sandbox
console(config-mst)# instance 1 add vlan 10,20,30
console(config-mst)# instance 2 add vlan 40,50,60
console(config-mst)# exit
console(config)# do copy running-config startup-config
01-Oct-2006 01:09:34 %COPY-I-FILECPY: Files Copy - source URL running-
config destination URL flash://startup-config
01-Oct-2006 01:09:44 %COPY-N-TRAP: The copy operation was completed
successfully
Copy succeeded
console(config)# do copy startup-config tftp://192.168.16.2/mstp.conf
01-Oct-2006 01:10:44 %COPY-I-FILECPY: Files Copy - source URL
flash://startup-config destination URL tftp://192.168.16.2/mstp.conf
01-Oct-2006 01:10:44 %COPY-N-TRAP: The copy operation was completed
successfully
!
Copy: 726 bytes copied in 00:00:01 [hh:mm:ss]
console(config)# spanning-tree mst 1 priority 0
console(config)# end

```

2. Конфигурация второго коммутатора

```

console# configure
console(config)# interface vlan 1
console(config-if)# ip address 192.168.16.1 /24
console(config-if)# do copy tftp://192.168.16.2/mstp.conf startup-config
01-Oct-2006 02:17:14 %COPY-I-FILECPY: Files Copy - source URL
tftp://192.168.16.2/mstp.conf destination URL flash://startup-config
.....01-Oct-2006 02:17:27 %COPY-N-TRAP: The copy operation was
completed successfully
!
726 bytes copied in 00:00:13 [hh:mm:ss]

console(config-if)# do reload
You haven't saved your changes. Are you sure you want to continue ?
(Y/N) [N] Y
This command will reset the whole system and disconnect your current
session. Do you want to continue ? (Y/N) [N] Y
Shutting down ...
console# configure
console(config)# interface vlan 1
console(config-if)# no ip address
console(config-if)# ip address 192.168.16.100 /24
console(config-if)# exit
console(config)# spanning-tree priority 0
console(config)# end

```

3. Конфигурация третьего коммутатора

```

console# configure
console(config)# interface vlan 1
console(config-if)# ip address 192.168.16.1 /24
console(config-if)# do copy tftp://192.168.16.2/mstp.conf startup-config
01-Oct-2006 02:17:14 %COPY-I-FILECPY: Files Copy - source URL
tftp://192.168.16.2/mstp.conf destination URL flash://startup-config
.....01-Oct-2006 02:17:27 %COPY-N-TRAP: The copy operation was
completed successfully
!
726 bytes copied in 00:00:13 [hh:mm:ss]

```

```
console(config-if)# do reload
You haven't saved your changes. Are you sure you want to continue ?
(Y/N) [N] Y
This command will reset the whole system and disconnect your current
session. Do you want to continue ? (Y/N) [N] Y
Shutting down ...
console# configure
console(config)# interface vlan 1
console(config-if)# no ip address
console(config-if)# ip address 192.168.16.101 /24
console(config-if)# exit
console(config)# spanning-tree mst 2 priority 0
console(config)# end
```

Настройка selective-qinq

Добавление SVLAN

Данный пример описывает, как добавлять метку SVLAN 20 ко всем VLAN за исключением VLAN 27.

```
console# show run
console(config)# vlan database
console(config-vlan)# vlan 20,27
console(config-vlan)# exit
console(config)# interface range gi0/1-24
console(config-if)# switchport mode general
console(config-if)# switchport general allowed vlan add 27 tagged
console(config-if)# exit
console(config)# interface range gi0/1-23
console(config-if)# switchport general allowed vlan add 20 untagged
console(config-if)# exit
console(config)# selective-qinq list ingress permit ingress_vlan 27 priority 1
console(config)# selective-qinq list ingress add_vlan 20 priority 2
```

Подмена CVLAN

В сетях передачи данных довольно часто возникают задачи, связанные с подменой VLAN (например, для коммутаторов уровня доступа существует типовая конфигурация, но пользовательский трафик, VOIP и трафик для управления требуется передавать в разных VLAN на различных направлениях). В этом случае было бы удобно воспользоваться функцией подмены CVLAN для замены типизированных VLAN на VLAN для требуемого направления. Рассмотрим конфигурацию коммутатора, в котором осуществляется подмена VLAN 100, 101 и 102 на 200,201 и 202:

```
console# configure
console(config)# vlan database
console(config-vlan)# vlan 100-102,200-202
console(config-vlan)# exit
console(config)# interface range gi0/1-24
console(config-if)# switchport mode trunk
console(config-if)# switchport trunk allowed vlan add 100-102,200-202
console(config-if)# exit
console(config)# selective-qinq list ingress override_vlan 200 ingress_vlan 100
priority 1
console(config)# selective-qinq list ingress override_vlan 201 ingress_vlan 101
priority 2
```

```
console(config)# selective-qinq list ingress override_vlan 202 ingress_vlan 102
priority 3
console(config)# selective-qinq list egress override_vlan 100 ingress_vlan 200
priority 1
console(config)# selective-qinq list egress override_vlan 101 ingress_vlan 201
priority 2
console(config)# selective-qinq list egress override_vlan 102 ingress_vlan 202
priority 3
```

Настройка multicast-TV VLAN.

Функция «*Multicast-TV VLAN*» дает возможность использовать для передачи многоадресного трафика одну VLAN в сети оператора и доставлять этот трафик пользователям даже в том случае, если они не являются членами этой VLAN. За счет функции «*Multicast-TV VLAN*» может быть сокращена нагрузка на сеть оператора за счет отсутствия дублирования многоадресных данных, например, при предоставлении услуги IPTV.

Схема применения функции предполагает, что порты пользователей работают в режиме «access» или «customer» и принадлежат к любой VLAN за исключением multicast-tv VLAN. Пользователи имеют возможность только получать многоадресный трафик из multicast-tv VLAN и не могут передавать данные в этой VLAN. Кроме того, в коммутаторе должен быть настроен порт-источник multicast-трафика, который должен быть участником multicast-tv VLAN.



Функция «*Multicast-tv VLAN*» работает только совместно с IGMP версий 1 и 2.

Пример настройки для порта в режиме работы access

1. Включить фильтрацию многоадресных данных

```
console(config)# bridge multicast filtering
```

2. Настроить VLAN пользователей (VID 100-124), multicast-tv VLAN (VID 1000), VLAN управления (VID 1200)

```
console(config)# vlan database
console(config-vlan)# vlan 100-124,1000,1200
console(config-vlan)# exit
```

3. Настроить порты пользователей.

```
console(config)# interface range fa1/0/1-24
console(config-if)# switchport mode access
console(config-if)# switchport access vlan 100
console(config-if)# switchport access multicast-tv vlan 1000
console(config-if)# bridge multicast unregistered filtering
console(config-if)# exit
```

4. Настроить uplink-порт, разрешив передачу многоадресного трафика, трафика пользователей и управление.

```
console(config)# interface gil/0/1
console(config-if)# switchport mode trunk
console(config-if)# switchport trunk allowed vlan add 100-124,1000,1200
console(config-if)# exit
```

5. Настроить igmp snooping глобально и на интерфейсах, добавить привязку групп.

```
console(config)# ip igmp snooping
console(config)# ip igmp snooping vlan 1000 multicast-tv 239.0.0.1
console(config)# ip igmp snooping vlan 1000 multicast-tv 239.5.0.1 count 10
console(config)# ip igmp snooping vlan 1000
console(config)# ip igmp snooping vlan 1000 querier
console(config)# ip igmp snooping vlan 100
console(config)# ip igmp snooping vlan 101
console(config)# ip igmp snooping vlan 102
console(config)# ip igmp snooping vlan 103
...
console(config)# ip igmp snooping vlan 124
```

6. Настроить интерфейс управления

```
console(config)# interface vlan 1200
console(config-if)# ip address 192.168.33.100 255.255.255.0
console(config-if)# exit
```

Пример настройки для порта в режиме «customer»

Данный тип подключения может быть использован для того, чтобы пометить пользовательские IGMP-report'ы определенных VLAN (CVLAN) отдельными внешними метками (SVLAN).

1. Включить фильтрацию многоадресных данных

```
console(config)# bridge multicast filtering
```

2. Настроить VLAN пользователей (VID 100), multicast-tv VLAN (VID 1000, 1001), VLAN управления (VID 1200)

```
console(config)# vlan database
console(config-vlan)# vlan 100,1000-1001,1200
console(config-vlan)# exit
```

3. Настроить порт пользователя

```
console(config)# interface fa1/0/1
console(config-if)# switchport mode customer
console(config-if)# switchport customer vlan 100
console(config-if)# switchport customer multicast-tv vlan add 1000,1001
console(config-if)# exit
```

4. Настроить uplink-порт, разрешив передачу многоадресного трафика, трафика пользователей и управление

```
console(config)# interface gil/0/1
console(config-if)# switchport mode trunk
console(config-if)# switchport trunk allowed vlan add 100,1000-1001,1200
console(config-if)# exit
```

5. Настроить igmp snooping глобально и на интерфейсах, добавить правила маркировки пользовательских IGMP-report'ов

```
console(config)# ip igmp snooping
console(config)# ip igmp snooping vlan 100
```

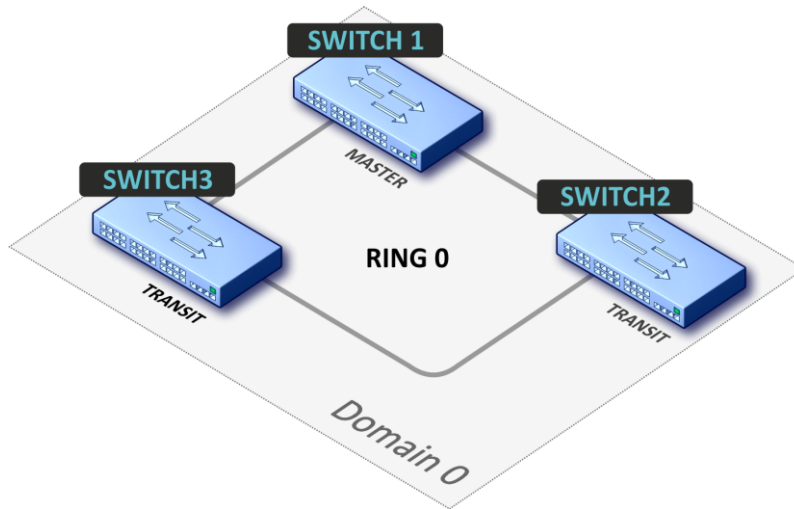
```
console(config)# ip igmp snooping map cpe vlan 5 multicast-tv vlan 1000
console(config)# ip igmp snooping map cpe vlan 6 multicast-tv vlan 1001
```

6. Настроить интерфейс управления

```
console(config)# interface vlan 1200
console(config-if)# ip address 192.168.33.100 255.255.255.0
console(config-if)# exit
```

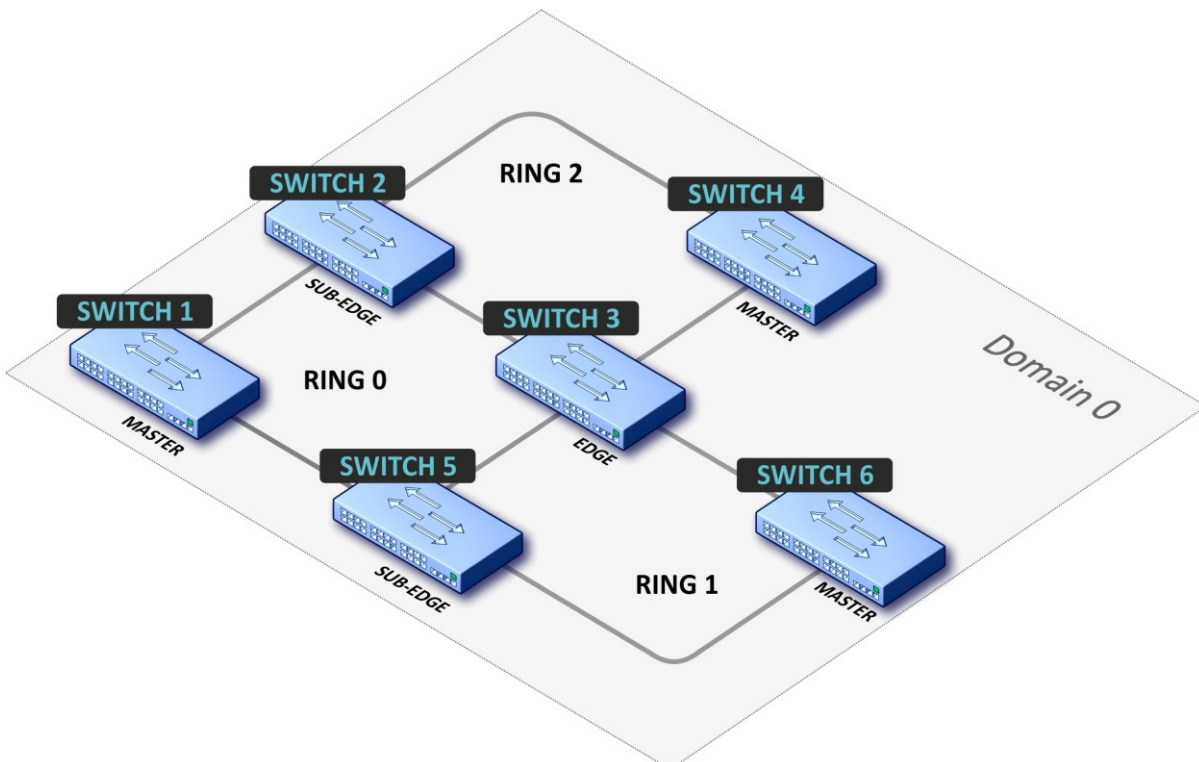
ПРИЛОЖЕНИЕ Б ТИПОВЫЕ СХЕМЫ ПОСТРОЕНИЯ СЕТЕЙ НА БАЗЕ ПРОТОКОЛА EAPS

1. Топология простое «кольцо»



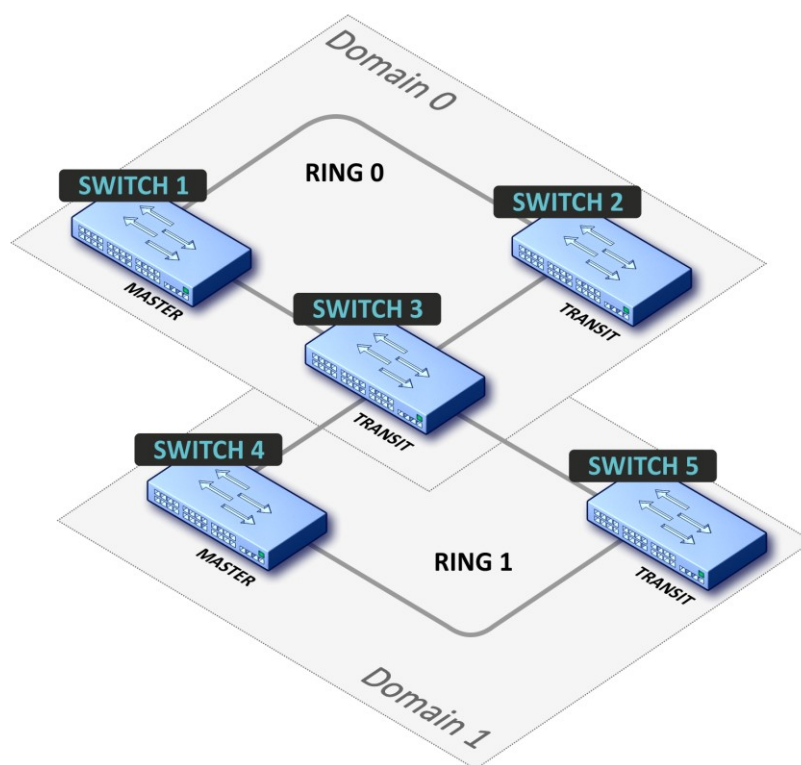
В топологии сети только одно кольцо. В этом случае необходимо определить для него только EAPS domain.

2. Топология один домен с несколькими «кольцами»



В топологии сети 3 кольца (может быть 2 и более) и 2 общих узла между ними. В этом случае необходимо определить EAPS-domain и установить одно кольцо в качестве основного, а другие как вторичные.

3. Топология несколько доменов со смежными «кольцами»



В топологии сети 2 кольца (может быть более двух) с одним общим узлом. В этом случае необходимо определить EAPS-domain для каждого кольца.

ПРИЛОЖЕНИЕ В ОПИСАНИЕ ПРОЦЕССОВ КОММУТАТОРА

Таблица - Описание процессов коммутатора

Имя процесса	Описание процесса
IDLE	Бездействие системы
SYLG	Вывод сообщений в syslog
CDB	Копирование конфигурационных файлов
SNMP	Реализация протокола SNMP
DDFG	Работа с файловой системой
CNLD	Загрузка/выгрузка конфигурации
IOTG	Управление терминалами ввода-вывода
IOUR	
IOTM	
HDEB	Сбор статистики работы задач системы
HOST	Основной host-поток, холостой ход
TBI_	Таблица временных промежутков для ACL
BRMN	Bridge Management: EAPS, STP, операции с FDB (добавление, удаление записей), зеркалирование, конфигурирование портов/вланов, GVRP, GARP, LLDP, IGMP snooping, IP multicast, OAM
TMNG	Управление приоритетами задач
COPY	Управление копированием файлов
MROR	Резервирование конфигурационного файла в энергонезависимой памяти
SFTR	Протокол Sflow
SFMG	
HCLT	Получение и обработка команд настройки устройства нижнего уровня
EVLC	Обработка событий о смене состояния порта, нижний уровень, передача выше
SELC	Получение событий о смене состояния порта, нижний уровень
EVAU	Обработка событий Address Update, нижний уровень, передача выше
SEAU	Получение событий Address Update, нижний уровень
PLCT	Обработка событий смены состояния портов
PLCR	Обработка событий смены состояния портов устройств стека
SWTR	Разрешение прохождения трафика через каскадные интерфейсы
DSPT	Диспетчеризация событий в стеке
OUIs	Обработка команды на восстановление OUI для Voice VLAN
BOXS	Обработка команд состояния стека: добавление мастера/слейва, изучение топологии, обновление версии ПО слейва
BSNC	Автомат синхронизации мастера и слейва в стеке
BOXM	Дополнительные действия в стеке (получение сведений о стеке, индикация, обмен сообщениями, смена unit id)

B_RS	Управление перезагрузкой устройств в стеке
TRMT	Управление юнитами в стеке с поддержкой транзакций
SW2M	Обработка событий Address update от FDB, блокировка порта при возникновении ошибок на порту
exRX	Обработка выхода пакетов с нижнего уровня 2
3SMA	Ageing для ip-multicast
3SWF	Передача пакетов между уровнем 2 и сетевым уровнем
3SWQ	Программная обработка ACL перехваченных пакетов
POLI	Policy Management
NTST	Добавление и удаление юнитов в стеке, сброс на дефолт состояния юнита, на сетевом уровне
NTPL	Периодическая генерация сигнала для опроса таблиц MAC, VLAN, портов, мультикаста, маршрутизации, приоритезации
L2HU	Передача пакетов на уровень 3
L2PS	Обработка событий смены состояния/настроек интерфейсов и передача сообщений зарегистрированным службам
LBDR	Настройка и приём пакетов Loopback Detection
LBDT	Отправка пакетов Loopback Detection
SFSM	Обработка sFlow
NSCT	Настройка ограничения скорости перехвата пакетов на CPU, ведение статистики по перехваченным пакетам
BRGS	Brige security - arp inspection, dhcp snooping, dhcp relay agent, ip source guard, pppoe intermediate agent
FFTT	Управление таблицей маршрутизации и маршрутизация пакетов
KEYM	Управление ключами аутентификации
IPAT	Управление базой данных ip-адресов
IP6C	Счётчики ipv4 и ipv6
IP6M	Маршрутизация ipv4 и ipv6
RPTS	Routing protocol
ARPG	Реализация протокола ARP
IPG	Обработка перехваченных фрагментированных IP-пакетов
ICMP	Реализация протокола ICMP
TFTP	Реализация протокола TFTP
IPRD	Вспомогательная задача для ARP, RIP, OSPF
DNSC	Клиент DNS
PNGA	Реализация ping
UDPR	UDP relay
TRCE	Реализация trace route
SSLP	Реализация SSL
WBSR	Управление и таймеры web-сервера

GOAH	Реализация web-сервера GoAhead
TNSR	Сервер telnet
TNSL	Клиент telnet
SSHP	Сервер ssh - настройка, обработка команд, таймер
SSHU	Сервер ssh - протокол
SNTP	Реализация протокола SNTP
IGMP	Реализация протокола IGMP (хостовой части)
TUNT	Реализация туннелей: конфигурирование, обработка пакетов
PTPT	Precise Time Protocol
FTPM	Управление ftp-сервером
FTPD	Реализация протокола FTP
SQIN	Настройка selective qinq
XMOD	Реализация протокола X-modem
SOCK	Управление работой сокетов
AAAT	Управление и обработка методов AAA
AATT	Симулятор AAA для проверки методов AAA
SCPT	Автообновление и автоконфигурирование
BTPC	Клиент BOOTP
SETX	Получение событий окончания отправки пакета из CPU в свич, нижний уровень
EVTX	Обработка событий окончания отправки пакета из CPU в свич, нижний уровень
SERX	Получение событий приёма пакета из свича в CPU, нижний уровень
EVRX	Обработка событий приёма пакета из свича в CPU, нижний уровень, передача пакета на уровень 2
HLTX	Отправка пакетов из CPU в свич
GRN_	Реализация Green Ethernet
TRIG	Запуск действия в FDB (ageing MAC-адресов)
MACT	Обработка события об окончании действия в FDB (ageing MAC-адресов)
TCPP	Реализация протокола TCP
DHCP	Сервер и Relay Agent DHCP
DHCp	DHCP-ping
IPMT	Управление ip multicast маршрутизацией и igmp проху
MSCm	Менеджер для работы с терминальными сессиями
STSA	CLI-сессия через COM-порт
STSB	CLI-сессия через VLAN
STSC	
STSD	
STSE	

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Для получения технической консультации по вопросам эксплуатации оборудования ООО «Предприятие «Элтекс» Вы можете обратиться в Сервисный центр компании:

Российская Федерация ,630020, г. Новосибирск, ул. Окружная, дом 29 в.

Телефон:

+7(383) 274-47-87

+7(383) 272-83-31

E-mail: techsupp@eltex.nsk.ru

На официальном сайте компании Вы можете найти техническую документацию и программное обеспечение для продукции ООО «Предприятие «Элтекс», обратиться к в базе знаний, оставить интерактивную заявку или проконсультироваться у инженеров Сервисного центра на техническом форуме:

<http://eltex.nsk.ru>

<http://eltex.nsk.ru/support/documentations>

<http://eltex.nsk.ru/forum>

<http://eltex.nsk.ru/interaktivnyi-zapros>

<http://eltex.nsk.ru/database>

