ООО "НАГТЕХ"

Руководство администратора по работе с ПО для коммутаторов серии s5xxx, s6xxx

RU.13725199.01.01.00001-18 34 01

Редакция 18

г. Екатеринбург

2024 г.

Редакция	Дата выпуска	Содержание изменений
18	18.11.2024	Версия ПО 1.12.0 Изменены разделы: • ACL; • Dying Gasp; • Настройка IGMP Snooping Authentication.
17	20.09.2024	Версия ПО 1.11.0 Добавлены разделы: • MAC-VLAN. Изменены разделы: • Policy-map; • ACL; • Конфигурация AAA; • Конфигурация system log.
15	27.06.2024	Версия ПО 1.9.0 Изменены разделы: • ZTP (Auto Provisioning); • DHCP Relay share-vlan;
14	22.04.2024	Версия ПО 1.8.2 Добавлены разделы: • DHCPv6 Snooping с Option 37/38; • SAVI. Изменены разделы: • Базовые настройки коммутатора; • Настройка DHCP snooping.
13	01.03.2024	Версия ПО 1.8.0 Добавлены разделы: • Лицензирование; • ULDP; • Настройка приоритета 802.1p для control-plane пакетов; Изменены разделы: • Изоляция портов (Port Isolation); • Настройка Policy-map; • Настройка Q-in-Q; • Конфигурация AAA; • Конфигурация system log.
12	29.12.2023	Версия ПО 1.7.0 Добавлены разделы: • Dynamic Arp Inspection;

Редакция	Дата выпуска	Содержание изменений
		• VLAN-translation; • Режим отладки; • ZTP (Auto Provisioning); Изменены разделы: • Конфигурация Port-based VLAN; • Зеркалирование трафика RSPAN; • Dying Gasp; • Настройка switchport flood-control.
11	29.09.2023	Версия ПО 1.6.0 Добавлены разделы: • BPDU-Tunnel. Изменены разделы: • Конфигурация LLDP; • Конфигурация Port-based VLAN; • Конфигурация таблицы MAC-адресов; • Обновление ПО коммутатора через eNOS; • Настройка параметров Ethernet интерфейсов.
10	31.05.2023	Версия ПО 1.5.0 Добавлены разделы: • Packet-capture; • Switchport flood-control; • Dying Gasp. Изменены разделы: • PoE.
09	31.03.2023	Версия ПО 1.4.0 Добавлены разделы: • MAB (MAC Authentication Bypass); • Отложенная перезагрузка; • Управление вентиляторами. Изменены разделы: • Multicast VLAN; • Настройка ACL; • Управление системой, мониторинг и отладка. Изменен формат имени SVI с vlan0.X на vlanX.
08	29.12.2022	Версия ПО 1.3.0 Добавлены разделы: • Policy-map; • MSTP; • PoE.

Редакция	Дата выпуска	Содержание изменений
		Изменены разделы: • IGMP Snooping; • Настройка DHCP snooping; • Конфигурация LLDP; • Конфигурация QoS; • ACL.
07	28.09.2022	Версия ПО 1.2.0 Добавлены разделы: • IGMP Snooping Authentication; • Настройка уведомлений об изменениях в MAC-таблице. Изменен раздел: • Настройка IGMP Snooping.
06	01.07.2022	Версия ПО 1.1.0 Добавлены разделы: • Errdisable; • Port-security; • Зеркалирование трафика RSPAN; • PPPoE Intermediate Agent; • AM; • iPerf3 клиент; • Ограничение доступа к управлению по Telnet и SSH. Изменены разделы: • Настройка storm-control; • Настройка интерфейса уровня 3; • Конфигурация Port-based VLAN.
05	21.03.2022	Версия ПО 1.0.0 Добавлены разделы: • Загрузочное меню; • DHCP Relay; • DHCP Snooping Binding; • Multicast Destination Control; • Фильтрация IGMP пакетов по типам query/report; • Ограничение количества IGMP подписок на порте. Изменены разделы: • Мониторинг и отладка; • Настройка интерфейсов; • Настройка DHCP snooping; • Обновление загрузчика и ПО коммутатора.
04	01.11.2021	Добавлен раздел: • Ограничение трафика в CPU.

Редакция	Дата выпуска	Содержание изменений
03	01.10.2021	Добавлены разделы: • TACACS+; • Обновление загрузчика и ПО коммутатора.
02	01.09.2021	Добавлены разделы: • Сохранение конфигурации на удаленный сервер по расписанию; • Voice VLAN; • Protocol-VLAN; • Q-in-Q (Double VLAN); • AAA; • Конфигурация SNTP. Изменен раздел: • Настройка SNMP.
01	01.03.2021	Начальная версия

Содержание

1. Введение

1.1 Назначение программы

Программное обеспечение предназначено для управления пакетным процессором коммутаторов серий S5xxx, 6xxxx на основании настроек пользователей, состояний интерфейсов, полученных протокольных пакетов и состояния регистров пакетного процессора.

1.2 Возможности программы

ПО обеспечивает следующий функционал:

- Поддержка интерфейса командной строки для управления коммутатором через консольный порт и удаленно, с использованием протоколов Telnet, SSH и SNMP;
- Поддержка командной строки с возможностью разграничения прав доступа;
- Поддержка протоколов STP (IEEE 802.1d, 802.1s);
- Поддержка списков контроля доступа (ACL) на основании входящего порта, L2 и L3 заголовков пакета;
- Поддержка статической агрегации каналов с использованием протокола LACP 8021.ax;
- Поддержка управления PoE (Power over Ethernet);
- Поддержка управления качеством обслуживания (QoS), управление аппаратными очередями, bandwidth control;
- Управление вентиляторами;
- Управление коммутацией пакетов с метками VLAN на основе стандарта IEEE 802.1Q, Protocol-based VLAN и Voice-VLAN;
- Управление настройками изоляции портов;
- Управление потоком: 802.3x flow-control;
- Диагностические функций - виртуальное тестирование кабеля, диагностика оптического трансивера;
- Зеркалирование трафика RSPAN;
- Ограничение доступа к управлению по Telnet и SSH;
- Ограничение Broadcast, Multicast и Unicast трафика на Ethernet интерфейсе (storm-control, flood-control).
- Определение петель (Loopback-detection);
- Отложенная перезагрузка;
- Поддержка AAA по протоколу RADIUS и локальных учетных данных;
- Поддержка IGMP Snooping v1/v2/v3, Multicast VLAN registration (MVR);
- Поддержка L3 интерфейсов на коммутаторе;
- L3 функционал: статическая маршрутизация, DHCP-Server;
- Диагностические утилиты: Ping, Traceroute, iPerf3;

- Access Management (AM);
- BPDU-Tunnel;
- Broadcast, multicast, unicast storm-control;
- DHCP-Snooping, DHCP Snooping Option 82;
- OAM Dying Gasp;
- Dynamic Arp Inspection;
- Errdisable;
- LLDP, ULDP;
- MAC Authentication Bypass;
- MAC-VLAN;
- MSTP;
- NTP и SNTP клиент;
- Packet-capture;
- Policy-map;
- Port-security;
- Port Isolation и Port Isolation в VLAN;
- PPPoE Intermediate Agent;
- Selective Q-in-Q;
- Switchport flood-control;
- VLAN-translation;
- ZTP (Auto Provisioning).

1.3 Технические характеристики

Аппаратной платформой для работы программы должны быть коммутаторы серии S5xxx, S6xxxx, выполненные на основе пакетного процессора серии RTL93XX фирмы Realtek.

2. Основные настройки управления

2.1 Виды управления коммутатором

После приобретения коммутатора необходима его настройка для корректной работы. Поддерживается два вида управления: In-band и Out-of-band.

2.1.1 Out-of-band управление

Out-of-Band управление осуществляется через консольный порт коммутатора для его первоначальной настройки или когда In-band управление недоступно. Например, вы можете назначить IP-адрес коммутатору через консоль для того, чтобы иметь возможность управлять коммутатором по протоколу Telnet. Для связи с коммутатором через консольный порт на ПК, необходимо выполнить следующие действия:

- Соединить Serial-порт ПК с портом Console коммутатора консольным кабелем идущим в комплекте с коммутатором.
- Запустить программу эмуляции терминала (Putty, Minicom, Hyper Terminal) и произвести следующие настройки:
  - Выбрать соответствующий Serial порт компьютера;
  - Установить скорость передачи данных 115200;
  - Задать формат данных: 8 бит данных, 1 стоповый бит, без контроля чётности;
  - Отключить аппаратное и программное управление потоком данных;
  - Включить питание коммутатора.

При правильном выполнении вышеперечисленных пунктов в эмуляторе терминала появится лог загрузки коммутатора:

```
## Booting kernel from Legacy Image at 81000000 ...
Image Name: eNOS
Created: 2021-04-28 12:45:29 UTC
Image Type: MIPS Linux Kernel Image (lzma compressed)
Data Size: 15333633 Bytes = 14.6 MB
Load Address: 80000000
Entry Point: 802a64a0
Verifying Checksum ... OK
Uncompressing Kernel Image ... OK
```

После окончания загрузки коммутатора необходимо ввести имя пользователя (login) и пароль (password). По умолчанию используется admin/admin. После чего открывается доступ к конфигурированию коммутатора:

```
Welcome to SNR-S5210G-24TX
SNR-S5210G-24TX login:
```

2.1.2 In-band управление

In-band управление предполагает управление коммутаторам используя протоколы Telnet, SSH или SNMP с устройств подключенных к коммутатору. Если In-Band управление недоступно используйте Out-of-Band управление для настройки коммутатора.

Настройка коммутатора при помощи Telnet

Для управления коммутатором, используя протокол Telnet необходимо, чтобы на коммутаторе был сконфигурирован IPv4 или IPv6 адрес и хост с Telnet-клиентом был доступен с коммутатора (находился в одной сети с ним или был доступен через маршрутизатор). Коммутатор по умолчанию имеет IP-адрес 192.168.1.1 в Vlan 1.

Коммутатор может иметь несколько IP-адресов для управления, в том числе в различных Vlan. Более подробное описание настройки приведено в соответствующем разделе данного руководства.

Пример подключения к коммутатору с конфигурацией по умолчанию, используя протокол Telnet.

В примере коммутатор имеет IP-адрес по умолчанию 192.168.1.1, маска 255.255.255.0. Сначала необходимо настроить IP-адрес на ПК с которого будет осуществляться управление. Затем настроить адрес 192.168.1.2, маску 255.255.255.0. Соединить ПК и коммутатор патч-кордом Ethernet. Выполнить команду: Telnet 192.168.1.1, затем ввести логин и пароль (по умолчанию admin / admin).

```
telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
SNR-S5210G-24TX login: admin
Password:*****
SNR-S5210G-24TX>
```

Управление коммутатором по SNMP

Для управления коммутатором по SNMP необходимо чтобы на коммутаторе был сконфигурирован IPv4 или IPv6 адрес и хост с SNMP клиентом был доступен с коммутатора (находился в одной сети с ним или был доступен через маршрутизатор). Коммутатор по умолчанию имеет IP-адрес 192.168.1.1 в VLAN1.

Коммутатор может иметь несколько IP-адресов для управления, в том числе в различных VLAN.

Более подробное описание настройки приведено в соответствующем разделе данного Руководства.

2.2 Интерфейс командной строки (CLI)

Коммутатор поддерживает 2 типа интерфейса для конфигурирования: **CLI (Command Line Interface)** и **SNMP**. CLI интерфейс знаком большинству пользователей и как уже описывалось выше Out-of-Band управление и Telnet используют CLI интерфейс для настройки коммутатора.

В основе CLI интерфейса лежит оболочка, состоящая из набора команд. Команды разделены по категориям в соответствии со своими функциями по настройке и управлению коммутатором. Каждая категория определяется различными конфигурационными режимами.

CLI интерфейс определяется:

- Режимами конфигурирования;
- Синтаксисом команд;
- Короткими сочетаниями клавиш;
- Функцией справки;
- Проверкой корректности ввода;
- Сокращенным вводом команд.

2.2.1 Режимы конфигурирования

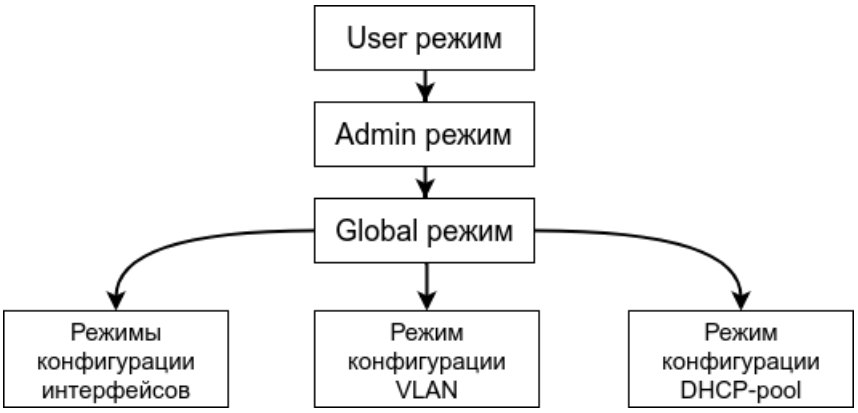

Рис. 1: Режимы конфигурирования CLI

User режим

При входе в CLI интерфейс пользователь попадает в режим User. В User режиме приглашение выглядит как <hostname>. Символ ”>” означает, что пользователь находится в User режиме. При выходе из Admin режима пользователь также попадает в User режим.

В User режиме недоступна настройка коммутатора, разрешены только команды show.

Admin режим

В Admin режим попадают пользователи после ввода команды "enable"и пароля, если задан пароль для enable. В admin режиме приглашение CLI выглядит как hostname#. Символ "#"означает, что пользователь находится в Admin режиме.

В Admin режиме пользователь может запрашивать вывод полной конфигурации и статуса коммутатора, а также может переходить в режим глобального конфигурирования (Global режим) для настройки любых параметров коммутатора. В связи с этим рекомендуется задавать пароль для перехода в Admin режим, для предотвращения несанкционированного доступа и изменений настроек коммутатора.

Global режим (Режим глобальной конфигурации)

При вводе команды "**configure terminal**"из Admin режима пользователь попадает в режим глобальной конфигурации. Для возврата в Global режим из вышестоящих режимов конфигурации, таких как Vlan, Порт и.т.д. предназначена команда **exit**.

В Global режиме доступна конфигурация глобальных параметров коммутатора, таких как таблица MAC-адресов, настройка SNMP, пользователей и.т.п., а так же возможен переход в режимы конфигурации интерфейсов, Vlan и.т.п.

Режим конфигурации интерфейсов

Для перехода в режим конфигурирования интерфейсов используйте команду **interface <name>**. Для возврата в глобальный режим конфигурации используйте команду **exit**.

Поддерживаются три вида интерфейсов: Vlan, Ethernet порт и Port-channel.

Тип интерфейса	Команда	Описание
Vlan интерфейс	interface vlan<vlan-id> *! В режиме глобальной конфигурации*	Настройка L3 интерфейсов коммутатора
Ethernet порт	interface <interface-list> *! В режиме глобальной конфигурации*	Настройка параметров физических интерфейсов (скорость, режим и.т.п)
Port-channel	interface po <port-channel-number> *! В режиме глобальной конфигурации*	Настройка параметров Port-Channel интерфейсов (режим, vlan и.т.п.)

Режим конфигурации VLAN

Для перехода в режим конфигурации Vlan используйте команду **interface vlan <vlan-id>** в режиме глобальной конфигурации. В этом режиме настраиваются параметры Vlan, такие как имя Vlan, remote-span, Multicast Vlan.

2.2.2 Синтаксис

Коммутатор поддерживает большое количество команд, тем не менее все они имеют общий синтаксис: **cmdtxt** <variable> {enum1 | . . . | enumN } [option1 | . . . | optionN].

Условные обозначения:

- **cmdtxt** жирным шрифтом обозначает название ключевое слово команды;
- **<variable>** обозначает обязательный параметр;
- **{enum1 | . . . | enumN }** обозначает обязательный параметр, который должен быть указан из ряда значений enum1~enumN;

• квадратные скобки ([ ]) в [option1 | . . . | optionN] обозначают необязательные параметры.

В CLI поддерживаются различные комбинации “< >“, “{ }” и “[ ]” такие, как [<variable>], {enum1 <variable>| enum2}, [option1 [option2]], и т.д. Ниже приведены примеры команд в конфигурационном режиме:

- **show version**, Эта команда не требует параметров, просто введите команду и нажмите Enter для её выполнения.

- **vlan <vlan-id>**, требуется ввести параметр - номер vlan для выполнения команды.

- **firewall** {enable | disable}, при вводе команды после ключевого слова firewall необходимо указать enable или disable. - **snmp-server community** {ro | rw <string>, допустимы следующие варианты: snmp-server community ro <string>.

- **snmp-server community** rw < string >.

2.2.3 Горячие клавиши

CLI поддерживает ряд коротких сочетаний клавиш для упрощения работы. Если терминальный клиент не распознает клавиши Вверх и Вниз, можно использовать сочетания “***Ctrl+P***” и “***Ctrl+N***” вместо них.

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

2.2.4 Справка

CLI поддерживает две команды для вызова справки: команда “**help**” и “**?**”

Команда	Описание
help	В любом режиме команда help выводит краткую информацию по использованию функции справки
“?”	В любом режиме ввод “?” выводит список всех допустимых для данного режима команд с описанием;Ввод “?” через пробел после ключевого слова выводит список допустимых параметров/ключевых слов с коротким описанием. Вывод “<cr>“ означает что команда введена полностью введена и необходимо нажать Enter для её выполнения;Ввод “?” сразу после строки. В этом случае выводятся все допустимые команды, начинающиеся с введенной строки.

2.2.5 Проверка ввода

Все введенные команды проверяются на правильность. При некорректном вводе возвращается информация об ошибке.

Информация об ошибке	Описание
% Incomplete command.	Команда введена не полностью либо отсутствует обязательный параметр.
% Invalid input detected at ’^’ marker.	Неправильный ввод команды. Маркер ‘^’ указывает на место неправильного ввода.
% Ambiguous command.	Введенная команда имеет два и более варианта интерпретации.

2.2.6 Сокращенный ввод команд

CLI поддерживает сокращенный ввод команд, если введенная строка может быть однозначно дополнена до полной команды и интерпретирована.

Пример:

1. Для команды **show interface ge1 counters** допустим сокращенный ввод **sh int ge1 coun**
2. Для команды **show running-config** сокращенный ввод **show r** вернет ошибку “**% Ambiguous command:**“ так как существует несколько команд начинающихся с sh r: show radius-server, show running-config. В то же время команда **show ru** будет выполнена, так как существует единственный вариант интерпретации.

3. Базовые настройки коммутатора

Базовые настройки коммутатора включают в себя команды для входа/выхода из **admin** режима, конфигурации и просмотра времени, вывода базовой информации о коммутаторе.

Команда	Описание
Режимы User и Admin	
enable	Переход из режима User в Admin режим.
disable	Выход из режима Admin.
show privilege	Вывод текущего уровня привилегий пользователя.
Все режимы	
exit	Выход из текущего режима конфигурирования в нижестоящий режим. Например, из глобального режима в Admin.
Все режимы за исключением User и Admin	
end	Выход из текущего режима конфигурирования и возврат в Admin режим.
Глобальный режим	
banner motd {<text> | default}	Настройка многострочного баннера, отображающегося при входе пользователя на коммутатор. Для переноса текста на новую строку необходимо использовать символы: \n.
hostname	Установка имени хоста коммутатора.
multi config access	Включение режима одновременного конфигурирования несколькими пользователями.
Admin режим	
configure terminal	Переход в режим глобального конфигурирования из режима Admin.
terminal length <0-511>	Установка количества строк терминала постраничного вывода. При установке значения 0 постраничный вывод отключается.
terminal width <24-511>	Установка ширины терминала в символах.
clock set <HH:MM:SS> [DD][month][year]	Установка системной даты и времени.
show version	Вывод информации о коммутаторе.
write	Сохранение текущей конфигурации коммутатора на Flash память.
delete startup-config	Удаление текущей загрузочной конфигурации.
reload	Перезагрузка коммутатора.
show system resources	Вывод информации о текущей загрузке CPU и ОЗУ коммутатора, свободных ресурсах ОЗУ.
show system uptime	Вывод информации о времени, прошедшем с момента запуска системы, числе подключенных пользователей и средней загрузке системы.

3.1 Управление локальными пользователями и паролями

Для доступа к интерфейсу управления коммутатором используется авторизация по имени пользователя и паролю. В конфигурации **по умолчанию** существует пользователь "**admin**"с паролем "**admin** в целях безопасности рекомендуется сменить пароль по умолчанию при первоначальной настройке коммутатора.

Поддерживается 3 типа привилегий пользователей:

- **network-user** - доступны только команды ”show”. Переход в конфигурационный режим запрещен;
- **network-operator** - доступны все команды, кроме команд ”copy ...”, ”write”, ”mv”, ”rm”, ”delete startup-config”;
- **network-admin** - доступны все команды.

1. Настройка пользователей:

Команда	Описание
username <user-name> [role {network-admin | network-operator | network-user }] [password { <password>| encrypted <encrypted>}]	Настроить имя пользователя и пароль для доступа на коммутатор. **<user-name>** - имя пользователя; **role** - указать уровень привилегий (по умолчанию network-user); **password <password>** - задать пароль в открытом виде или <encrypted> в зашифрованном виде.
no username <username> *! В режиме глобальной конфигурации*	Удалить пользователя.
enable password {<password>| encrypted <password>} **no enable password** *! В режиме глобальной конфигурации*	Задать пароль для перехода в Admin режим. Удалить пароль для перехода в Admin режим (будет установлен пустой пароль).

3.2 Telnet

Telnet - это простой протокол для доступа к удаленному терминалу. Используя Telnet пользователь может удаленно зайти на оборудование зная его IP-адрес или доменное имя. Telnet может отправлять введенную пользователем информацию на удаленный хост и выводить ответы хоста на терминал пользователя аналогично тому, что пользователь подключен напрямую к оборудованию.

Telnet работает по Клиент-Серверной технологии, на локальной системе работает Telnet клиент, а на удаленном хосте Telnet server. Коммутатор может работать как в роли Telnet-сервера, так и в роли Telnet-клиента. При работе коммутатора в роли Telnet+сервера, пользователи могут удаленно заходить на него используя Telnet-клиент, как было описано ранее в разделе In-band управления.

Используя коммутатор в качестве Telnet клиента пользователь может удаленно заходить на другие хосты.

1. Настройка Telnet-сервера на коммутаторе

Команда	Описание
feature telnet	Включить telnet сервер на коммутаторе.
no feature telnet	Отключить telnet сервер на коммутаторе.
! В режиме глобальной конфигурации	

2. Использование Telnet-клиента на коммутаторе

Команда	Описание
telnet {<ip-addr> | <hostname>} [<port>]	Подключение к удаленному терминалу по протоколу Telnet. **<ip-addr>** - ipv4 адрес удаленного терминала; **<hostname>** - доменное имя удаленного терминала; **<port>** - TCP порт (1-65535) для подключения. По умолчанию используется порт 23.
! В User или Admin режиме	

3.3 SSH

SSH — сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений. Схож по функциональности с протоколами Telnet и rlogin, но, в отличие от них, шифрует весь трафик, включая и передаваемые пароли. SSH допускает выбор различных алгоритмов шифрования. SSH-клиенты и SSH-серверы доступны для большинства сетевых операционных систем. SSH позволяет безопасно передавать в незащищенной среде практически любой другой сетевой протокол.

1. Настройка SSH-сервера на коммутаторе:

Команда	Описание
feature ssh **no feature ssh** *! В режиме глобальной конфигурации*	Включение SSH сервера на коммутаторе (при первом включении ssh сервера производится генерация ключа, что может занять несколько минут). Отключение SSH сервера на коммутаторе.
ssh server port <1024-65535> **no ssh server port** *! В режиме глобальной конфигурации*	Настройка порта, используемого SSH-сервером. Использовать порт по умолчанию (порт 22).
ssh login-attempts <authentication-retires> **no ssh login-attempts** *! В режиме глобальной конфигурации*	Настройка ограничения количества попыток аутентификации при подключении к SSH. Сброс ограничения количества попыток аутентификации к значению по умолчанию (3 попытки).
ssh key rsa [lenght <768-2048>] [force] *! В режиме глобальной конфигурации*	Сгеренировать ключ RSA.
ssh key dsa [force] *! В режиме глобальной конфигурации*	Сгеренировать ключ DSA.

2. Использование SSH-клиента на коммутаторе:

Команда	Описание
ssh {<user>@<ip-addr> | hostname} [<port>] *! В User или Admin режиме*	Подключение к удаленному терминалу по протоколу SSH. **<user>** - имя пользователя удаленного терминала; **<ip-addr>** - IPv4 адрес удаленного терминала; **<hostname>** - доменное имя удаленного терминала; **<port>** - TCP порт (1-65535) для подключения. По умолчанию используется порт 22.

3.4 Настройка IP-адреса коммутатора

1. Создание VLAN интерфейса на коммутаторе.

Команда	Описание
interface vlan<vlan-id>	Создание L3 интерфейса в Vlan <vlan-id>.
no interface vlan<vlan-id>	Удаление L3 интерфейса в Vlan <vlan-id>.
! В режиме глобальной конфигурации	

2. Статическая настройка IP-адреса на Vlan интерфейсе.

Команда	Описание
ip address [<ip_address> <mask> | <ip_address>/<mask>] [secondary]	**<ip_address>** - статический адрес формата IPv4; **<mask>** - маска сети; **[secondary]** - IP-адрес будет добавлен на интерфейс как дополнительный.
no ip address [<ip_address> <mask>| <ip_address>/<mask>] [secondary]	Удаление статического IP-адреса с интерфейса.
! В режиме конфигурации Interface VLAN	

3.5 SNMP

SNMP (Simple Network Management Protocol) — стандартный протокол, который широко используется для управления сетевыми устройствами. SNMP протокол работает по технологии клиент-сервер. В роли сервера выступает SNMP Агент, который работает на управляемых устройствах, например коммутаторах. В роли клиента *NMS* (Network Management Station) — станция управления сетью. На коммутаторах SNR поддерживается только функции SNMP-агента.

Обмен информацией между NMS и SNMP-агентом осуществляется путем отправки стандартизированных сообщений. В SNMP определены 7 типов сообщений:

- Get-Request
- Get-Response
- Get-Next-Request
- Get-Bulk-Request
- Set-Request
- Trap
- Inform-Request

NMS может посылать следующие сообщения Агенту: **Get-Request**, **Get-Next-Request**, **Get-Bulk-Request** и **Set-Request**. Агент отвечает сообщением Get-Response. Также Агент может отсылать **Trap сообщения** на NMS для информирования о событиях, например UP/DOWN порта и.т.п. Сообщение Inform-Request используется для обмена информацией между NMS.

3.5.1 Описание MIB

Формат сообщений которыми обмениваются NMS и SNMP-агент описан в Management Information Base (MIB). Информация в MIB организована в виде иерархической древовидной структуры. Каждая запись содержит OID (Object IDentifier) и короткое описание. OID состоит из набора чисел разделенных точками. Он определяет объект и его положение в дереве MIB как показано на рисунке 2.

Как показано на рисунке, OID объекта A - 1.2.1.1. NMS зная этот OID может получить значения данного объекта. Таким образом в MIB определяется набор стандартных объектов для управляемых устройств. Для просмотра базы MIB можно использовать специализированное ПО называемое MIB Browser.

MIB разделяются на публичные (public) и частные (private). Public MIB определяются RFC и являются общими для всех поддерживающих их Агентов, например MIB для управления интерфейсами - IF-MIB определенный в RFC 2863. Private MIB создаются производителями оборудования и соответственно поддерживаются только на оборудовании данного производителя.

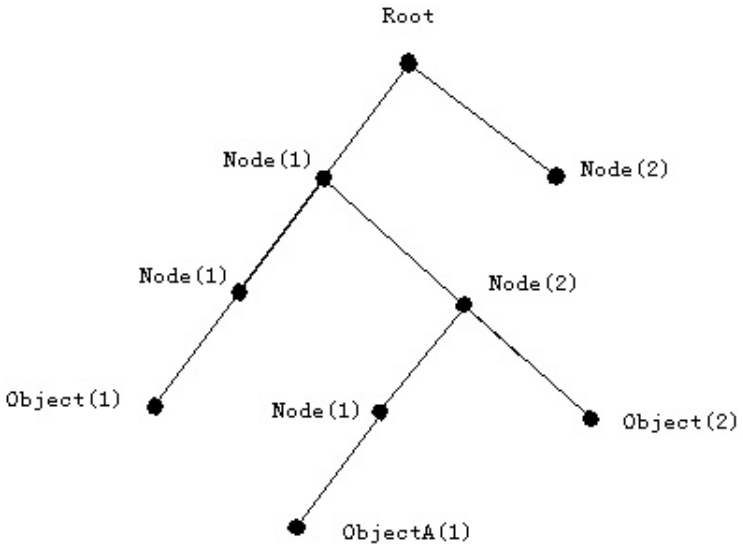

Рис. 2: Древовидная структура MIB

SNMP-агент на коммутаторах SNR поддерживает основные публичные MIB такие, как MIB-II, IF-MIB, BRIDGE-MIB и др., а также Private SNR MIB.

3.5.2 Настройка SNMP

SNMP-агент - программное обеспечение, запускаемое на управляемом устройстве, которое собирает данные и передает их на SNMP manager.

1. Включение/отключение SNMP-агента:

Команда	Описание
snmp-server enable snmp	Включение SNMP-агента на коммутаторе.
no snmp-server enable snmp	Отключение SNMP-агента на коммутаторе.
! В режиме глобальной конфигурации	

2. Настройка SNMP community:

SNMP community - ключевое слово (имя сообщества) для взаимодействия по протоколу SNMP 1 или 2 версии. Сообщество состоит из одного или нескольких агентов и менеджеров. Один хост с установленным на нем агентом может одновременно принадлежать к нескольким сообществам, при этом агент будет принимать запросы только от устройств управления, принадлежащих к этим группам. Безопасность обмена сообщениями между агентами и менеджером в этом случае обеспечивается при помощи передачи в теле сообщения в открытом виде имени сообщества или community-string.

Команда	Описание
snmp-server community <string> [{ro | rw} | group <group-name> | view <view-name> version {v1 | v2c} {ro | rw}]	Настроить SNMP community: **ro** - только чтение; **rw** - чтение и запись; **<string>** - SNMP community; **<group-name>** - network-admin или network-operator; **<view-name>** - имя SNMP View.
no snmp-server community <string>	Удалить SNMP community.
! В режиме глобальной конфигурации	

3. Настройка sysContact и Location.

SysContact используется в качестве значения настоящего имени ответственного за устранение неполадок на коммутаторе.

Location используется в качестве значения физического местоположения коммутатора.

Команда	Описание
snmp-server contact <syscont-string> **no snmp-server contact** *! В режиме глобальной конфигурации*	Настроить SysContact SNMP-сервера. Восстановить SysContact по умолчанию.
snmp-server location <location-string> **no snmp-server location** *! В режиме глобальной конфигурации*	Настроить Location SNMP-сервера. Восстановить Location по умолчанию.

4. Создание пользователя SNMP v3:

Команда	Описание
snmp-server user <user-string> [[network-operator | network-admin] [auth {md5 | sha} [encrypt] <auth-pass>] [priv {des | aes} [encrypt] <priv-pass>] **no snmp-server user** <user-string> *! В режиме глобальной конфигурации*	**<user-string>** - имя пользователя; **priv** - выбрать шифрование данных aes или des с указанием пароля <priv-pass>; **auth** {md5 | sha} - выбрать аутентификацию md5 или sha с указанием пароля <auth-pass>. При указании **encrypt** пароли <priv-pass> и <auth-pass> задаются в шифрованном виде. Удаление SNMP пользователя.

5. Настройка представлений (**SNMP View**) создаваемые для ограничения доступа к объектам дерева MIB. Для создания и настройки представления используется команда конфигурационного режима snmp-server view.

Команда	Описание
snmp-server view <view-string> <oid-string> {include | exclude} **no snmp-server view** <view-string> [<oid-string>] *! В режиме глобальной конфигурации*	**<view-string>** - имя SNMP View; **<oid-string>** - OID; **include** - добавить OID в View; **exclude** - исключить OID из View. Удаление SNMP View <view-string> либо отмена настройки <oid-string> для данного SNMP View.

6. Настройка SNMP TRAP:

SNMP TRAP - особый сигнал отправляемый устройством для оповещения администратора сети о наступлении критического события.

Команда	Описание
snmp-server enable traps **no snmp-server enable traps** *! В режиме глобальной конфигурации*	Глобальное включение SNMP Trap. Отключение SNMP Trap.
snmp-server host {<host-ipv4-address>} [traps version | informs version | version] {1 | 2c | 3 {auth | noauth | priv}} <string> **no snmp-server host** <host-ipv4-address> *! В режиме глобальной конфигурации*	**<host-ipv4-address>** - IPv4 адрес на который будут отсылаться Trap/inform сообщения. **1 | 2c | 3** - Версия SNMP Trap; **noauthnopriv | authnopriv | authpriv** - настройки шифрования (только для SNMPv3); **<string>** - community (для SNMPv1/v2c) или имя пользователя для SNMPv3. Удаление IPv4 адреса для отправки Trap сообщения с community <string>.
snmp trap link-status **no snmp trap link-status** *! В режиме конфигурации порта*	Включение отсылки трапов при изменении статуса порта UP/Down. По умолчанию включено. Отключение отсылки трапов при изменении статуса порта UP/Down.

7. Настройка ограничения доступа к SNMP.

Функция **snmp-server securityip** разрешает доступ к SNMP-агенту только с указанных IP-адресов и запрещает со всех остальных.

Команда	Описание
snmp-server securityip enable **no snmp-server securityip enable** *! В режиме глобальной конфигурации*	Включение функции ограничения доступа. По умолчанию отключено. Отключение функции.

Команда	Описание
snmp-server securityip {X.X.X.X | X.X.X.X/Y}	Добавление IP-адреса или сети в список разрешенных. Допускаются множественные команды, для прописывания нескольких адресов или сетей.
no snmp-server securityip {X.X.X.X | X.X.X.X/Y}	Удаление адреса или сети из списка разрешенных.
! В режиме глобальной конфигурации	

3.5.3 Примеры настройки SNMP

Во всех примерах IP-адрес NMS - 1.1.1.5, IP-адрес SNMP-агента - 1.1.1.9.

Сценарий 1: NMS используется для получения данных через SNMP с коммутатора.

```
Switch(config)#snmp-server enable snmp
Switch(config)#snmp-server community private rw
Switch(config)#snmp-server community public ro
```

NMS использует SNMP community public с правами только на чтение, community private имеет права на чтение и запись.

Сценарий 2: NMS используется для получения SNMP Trap с коммутатора с community usertrap.

```
Switch(config)#snmp-server enable snmp
Switch(config)#snmp-server host 1.1.1.5 traps version 1 usertrap
Switch(config)#snmp-server enable traps
```

3.5.4 SNMP Troubleshooting

При возникновении проблем с получением или отправкой данных с SNMP сервера на коммутатор проверьте следующие пункты:

- Соединение между SNMP сервером и коммутатором утилитой ping;
- SNMP Community для SNMPv1/v2 или аутентификация для SNMPv3 правильно сконфигурирована и совпадает с конфигурацией на NMS;
- Используя команду sh snmp проверьте что коммутатор получает и отправляет пакеты.

3.6 Таблица MAC-адресов

Таблица MAC - это таблица соответствий между MAC-адресами устройств назначения и портами коммутатора. MAC-адреса могут быть статические и динамические. Статические MAC-

адреса настраиваются пользователем вручную, имеют наивысший приоритет, хранятся постоянно и не могут быть перезаписаны динамическими MAC-адресами.

MAC-адреса - это записи, полученные коммутатором в пересылке кадров данных, и хранятся в течение ограниченного периода времени. Когда коммутатор получает кадр данных для дальнейшей передачи, он сохраняет MAC-адрес кадра данных вместе с соответствующим ему портом назначения. Когда MAC-таблица опрашивается для поиска MAC-адреса назначения, при нахождении нужного адреса кадр данных отправляется на соответствующий порт, иначе коммутатор отправляет кадр на широковещательный домен. Если динамический MAC-адрес не встречается в принятых кадрах данных длительное время, запись о нем будет удалена из MAC-таблицы коммутатора.

Коммутатором могут пересылаться 3 типа кадров:

1. **Широковещательные.** Коммутатор может определять коллизии в домене, но не в широковещательном. Если VLAN не определена, все устройства, подключенные к коммутатору, находятся в одном широковещательном домене. Когда коммутатор получает широковещательный кадр, он передает кадр во все порты. Если на коммутаторе настроены VLAN, таблица MAC-адресов соответствующим образом адаптирована для добавления информации о VLAN и широковещательные кадры будут пересылаться только в те порты, в которых настроена данная VLAN.

2. **Многоадресные.** Если многоадресный домен неизвестен, коммутатор пересылает многоадресный кадр как широковещательный. Если на коммутаторе включен **IGMP-snooping** и сконфигурирована многоадресная группа, коммутатор будет пересылать многоадресный кадр только портам этой группы.

3. **Одноадресные.** Если на коммутаторе не настроена VLAN, коммутатор ищет MAC-адрес назначения в таблице MAC-адресов и отправляет кадр на соответствующий порт. Если соответствие MAC-адреса и порта не найдено в таблице MAC-адресов, коммутатор пересылает одноадресный кадр как широковещательный. Если на коммутаторе настроен VLAN, коммутатор пересылает кадр только в этом VLAN. Если в таблице MAC-адресов найдено соответствие для VLAN, отличного от того в котором был принят кадр, коммутатор пересылает кадр широковещательно в том VLAN, в котором кадр был принят.

3.6.1 Формирование таблицы MAC-адресов

Таблица MAC-адресов может быть создана динамически или статически. Статическая конфигурация заключается в ручной настройке соответствия между MAC-адресами и портами. Динамическое обучение - это процесс, в котором коммутатор изучает соответствие между MAC-адресами и портами и регулярно обновляет таблицу MAC.

3.6.2 Конфигурация таблицы MAC-адресов

1. Управление обучением таблицы MAC-адресов:

Команда	Описание
mac-address-table learning {**interface** <if-name> | **vlan** <vlan-id>} **no mac-address-table learning** {**interface** <if-name> | **vlan** <vlan-id>} *! В режиме глобальной конфигурации*	Включить обучение таблицы MAC-адресов на порте или vlan. Включено по умолчанию. Выключить обучение таблицы MAC-адресов на порте или vlan.
mac-address-table aging-time <0-1000000> **no mac-address-table aging-time** *! В режиме глобальной конфигурации*	Задать время (в секундах) жизни для динамических MAC-адресов. Вернуть значение по умолчанию - 300 секунд.
mac-address-table limit maximum <1-32768> **no mac-address-table limit maximum** *! В режиме конфигурации порта*	Задать максимальное число MAC-адресов <1-32768> которое может быть изучено на интерфейсе. Выключить лимит таблицы MAC-адресов для интерфейса. Используется по умолчанию.

2. Настройка статической пересылки и фильтрации:

Команда	Описание
mac-address-table static <mac-address> {forward | discard} <ifname> **vlan** <1-4094> **no mac-address-table static** <mac-address> {forward | discard} <ifname> **vlan** <1-4094> *! В режиме глобальной конфигурации*	Задать статическую запись. Удалить статическую запись.

3. Просмотр информации о состоянии таблицы MAC-адресов:

Команда	Описание
show mac-address-table {learning | limit} *! В Admin режиме*	Просмотр информации о настроенных лимитах и состоянии обучения таблицы MAC.

Команда	Описание
show mac address-table [count] [dynamic | multicast | static] [address <mac-address>] [interface <ifname>] [vlan <1-4094>] *! В Admin режиме*	Просмотр информации о записях в таблице MAC.
show mac-address-table aging-time *! В Admin режиме*	Вывести установленное значение aging-time.

4. Очистка таблицы MAC-адресов:

Команда	Описание
clear mac address-table {dynamic | static} [address <MAC-address>] [vlan <1-4094>] [interface <ifname>] *! В Admin режиме*	Очистка таблицы MAC-адресов.

3.6.3 Настройка уведомлений об изменениях в MAC-таблице (MAC-notification)

MAC-notification - функция используемая для мониторинга MAC-адресов, изучаемых коммутатором. Она позволяет уведомлять администратора об изменениях в таблице MAC-адресов с помощью SNMP trap. Уведомления отправляются только при добавлении и/или удалении MAC-адресов на тех портах коммутатора, на которых настроена функция MAC-notification.

1. Включить уведомления об изменениях в MAC-таблице глобально:

Команда	Описание
mac-address-table notification **no mac-address-table notification** *! В режиме глобальной конфигурации*	Включить глобально отправку уведомлений об изменении в таблице MAC-адресов. Выключить глобально отправку уведомлений об изменении в таблице MAC-адресов.

2. Настройка интервала отправки уведомлений об изменениях в MAC-таблице:

Команда	Описание
mac-address-table notification interval <1-30>	Установить интервал отправки SNMP trap от 1 до 30 секунд.

Команда	Описание
no mac-address-table notification interval *! В режиме глобальной конфигурации*	Вернуть значение по умолчанию - 5 секунд.

3. Настройка размера истории таблицы:

Команда	Описание
mac-address-table notification history-size <1-100> **no mac-address-table notification history-size** *! В режиме глобальной конфигурации*	Установить максимальное количество MAC-адресов отправляемых в одном SNMP trap. Вернуть значение по умолчанию - 10 записей.

4. Настройка типа события для отправки SNMP-trap:

Команда	Описание
mac-notification {added | both | removed} **no mac-notification** *! В режиме конфигурации порта*	Установить на порте событие по которому будет отправляться SNMP trap: **added** - изучен новый MAC-адрес; **removed** - MAC-адрес удален из таблицы; **both** - изучен или удален MAC-адрес из таблицы. Выключить событие для отправки SNMP trap.

3.6.4 Пример настройки уведомлений об изменениях в MAC-таблице

Сценарий: Необходимо получать уведомления при изучении новых MAC-адресов на порте ge1.

Конфигурация будет выглядеть следующим образом:

```
Switch(config)#snmp-server community private group network-operator
Switch(config)#snmp-server host 10.10.10.10 traps version 2c private udp-port 162
Switch(config)#snmp-server enable snmp
Switch(config)#snmp-server enable traps snmp authentication
Switch(config)#mac-address-table notification
Switch(config)#interface ge1
Switch(config-if)#mac-notification added
```

4. Загрузочное меню

Загрузчик - это специальное ПО хранящееся в отдельном разделе flash-памяти, предназначенное для запуска основного ПО коммутатора (eNOS).

С помощью загрузочного меню можно восстановить ПО коммутатора, выбрать образ ПО для загрузки, очистить конфигурационный файл перед загрузкой ПО, отформатировать пользовательский раздел flash-памяти. Для входа в загрузочное меню необходимо нажать клавишу "Esc"сразу после включения питания.

Загрузочное меню имеет следующую структуру:

```
  *** S5xxx Boot Menu ***
1. Display switch info

     Switch info:
     Bootrom version: <bootversion>
     CPU MAC: <cpumac>
     Vlan MAC: <vlanmac>
     SN: <sn>
     id: <deviceid>
     Switch IP: <ipaddr>
     TFTP server IP: <serverip>
     Frimware filename: <filename>

2. Set bootrom network parameters
     1. Set switch IP address
     2. Set server IP address
     0. Back to main menu
3. Upgrade bootrom via TFTP
4. Run firmware from TFTP
5. Set boot option to default config
6. Set boot firmware filename
     1. Set boot firmware filename
     2. Reset boot firmware filename to the default value
     0. Back to main menu
7. Run firmware from flash
8. Format flash
0. Reboot switch
```

Пункт **1. Display switch info** - отобразить основную информацию коммутатора, такую как: версия загрузчика, CPU MAC, VLAN MAC, серийный номер устройства, IP-адрес коммутатора, имя загрузочного файла, скорость консольного порта.

Пункт **2. Set bootrom network parameters** используется для настройки сетевых параметров TFTP-соединения.

Пункт **2.1. Set switch IP address** - задать IP-адрес коммутатора.

Пункт **2.2. Set server IP address** - задать IP-адрес TFTP-сервера.

Пункт **2.0. Back to main menu** - вернуться в главное меню.

Пункт **3. Upgrade bootrom via TFTP** - обновление загрузчика через TFTP.
Для обновления необходимо задать имя файла загрузчика, который должен находиться в корне TFTP-сервера и иметь расширение ".rom". По умолчанию используется имя "boot.rom".

Пункт **4. Run firmware from TFTP** - загрузка образа ПО с TFTP-сервера.
Для обновления необходимо задать имя образа ПО, который должен находиться в корне TFTP-сервера и иметь расширение ".bix". По умолчанию используется имя "vmlinux.bix".

Пункт **5. Set boot option to default config** - загрузка ПО с конфигурационным файлом используемым по умолчанию.

Пункт **6. Set boot firmware filename** - используется для изменения имени файла загружаемого образа ПО.

Пункт **6.1. Set boot firmware filename** - задать имя файла, загружаемого образа ПО, хранящегося на flash-памяти коммутатора.

Пункт **6.2. Reset boot firmware filename to the default value** - задать имя файла по умолчанию - vmlinux.bix.

Пункт **6.0. Back to main menu** - вернуться в главное меню.

Пункт **7. Run firmware from flash** - запуск ПО с flash-памяти.

Пункт **8. Format flash** - форматирование пользовательского раздела flash-памяти, где хранятся образы ПО и файлы конфигурации.

Пункт **0. Reboot switch** - перезагрузить коммутатор.

5. Обновление загрузчика и ПО коммутатора

Обновление загрузчика и ПО коммутатора осуществляется через eNOS по протоколам FTP, SFTP, SCP, TFTP или через загрузочное меню по протоколу TFTP.

Формат URL при использовании в eNOS сервера:

TFTP: `tftp:[//server[:port]][/path/filename]`

SFTP: `sftp:[//[username:pw@]server][/path/filename]`

FTP: `ftp:[//[username:pw@]server][/path/filename]`

SCP: `scp:[//[username:pw@]server][/path/filename]`

5.1 Обновление загрузчика через eNOS

Для обновления загрузчика необходимо принять файл через один из протоколов передачи данных с именем **boot.rom**.

Команда	Описание
copy { tftp | ftp | scp | sftp } <url> **bootrom** *! В Admin режиме*	Принять файл с расширением ***.rom** через протоколы передачи данных TFTP/FTP/SFTP/SCP. **<url>** - URL-адрес файла (формат URL см. в разделе 5).

5.1.1 Пример обновления загрузчика через eNOS по протоколу TFTP

В корневом каталоге TFTP сервера с адресом 192.168.10.2 расположен файл образа загрузчика “**boot.rom**”.

```
Switch#copy tftp tftp://192.168.10.2/boot.rom bootrom
Warning: Don't power off device during bootrom updating!
Are you sure to start update ?(y/n): y
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  771k  100  771k    0     0   123k      0  0:00:06  0:00:06 --:--:-- 100k
100  771k  100  771k    0     0   123k      0  0:00:06  0:00:06 --:--:-- 123k
Read image from file..
Check image CRC..
Erase a flash partition..
Write image to flash..
Read and check data CRC from flash..
Copy Success
```

5.2 Обновление ПО коммутатора через eNOS

Для работы коммутатора необходим образ ПО с расширением **".bix"**, который хранится во Flash памяти коммутатора, обычно с именем **vmlinux.bix**.

Принять файлы на коммутатор через протоколы передачи данных:

Команда	Описание
copy { tftp | ftp | scp | sftp } <url> **file** <file-name> [force] *! В Admin режиме*	Принять файл через протоколы передачи данных. **<url>** - URL-адрес файла на TFTP / FTP / SFTP / SCP сервере (см. раздел 4); **<file-name>** - имя файла в памяти коммутатора; **force** - загрузка файла без проверки версии.

5.2.1 Downgrade ПО коммутатора через eNOS

При downgrade ПО с версии 1.6.0 и выше до версии 1.4.0 и выше, необходимо использовать промежуточную прошивку версии 1.5.5, с обязательным сохранением конфигурационного файла.

При downgrade ПО с версии 1.6.0 и выше до версии ниже 1.4.0, необходимо использовать две промежуточные прошивки версии 1.5.5 и 1.4.0, с обязательным сохранением конфигурационного файла на каждой из них.

При обновлении ПО на предыдущую версию будет выведено предупреждение с требованием подтвердить действие. Для выполнения действия без предупреждения можно использовать ключ force.

5.2.2 Пример обновления ПО по протоколам FTP и TFTP

Коммутатор используется в качестве FTP и TFTP клиента. FTP / TFTP-сервер с адресом 10.1.1.1 подключен к одному из портов коммутатора. Интерфейс управления коммутатором имеет IP-адрес 10.1.1.2. Необходимо обновить ПО коммутатора, загрузив файл образа новой версии “vmlinux.bix”.

Использование **FTP.**

В корневом каталоге пользователя “admin” FTP сервера расположен файл образа последней версии ПО коммутатора “vmlinux.bix”. Пароль пользователя **admin - “switch”**.

```
copy ftp ftp://admin:switch@10.1.1.1/vmlinux.bix file vmlinux.bix
```

Использование **TFTP.**

В корневом каталоге TFTP сервера расположен файл образа последней версии ПО коммутатора “vmlinux.bix”.

```
copy tftp tftp://10.1.1.1/vmlinux.bix file vmlinux.bix
```

5.2.3 Решение проблем с FTP и TFTP

Ниже показан лог коммутатора при передаче файла по FTP/SFTP/SCP/TFTP с помощью команды copy. Если лог на вашем коммутаторе отличается, проверьте IP связность и конфигурацию FTP сервера и попробуйте выполнить копирование снова.

```
% Total % Received % Xferd Average Speed Time  Time  Time Current
                           Dload  Upload Total Spent Left Speed
      100  14.7M   0 0 0   14.7M 0 854k -:-:- 0:00:17 -:-:- 933k
      100  14.7M   0 0 0   14.7M 0 854k -:-:- 0:00:17 -:-:- 854k
Copy Success
```

Если на коммутаторе происходит обновление системных файлов, не перезагружайте коммутатор до тех пор, пока не появится сообщение “**Copy Success**” или “**Copy Failed**” иначе коммутатор может не загрузиться. Если это все же произошло и коммутатор не загружается, попробуйте зайти в загрузочное меню и запустить образ ПО из него.

5.3 Обновление загрузчика через загрузочное меню

Для обновления загрузчика, ПК должен поддерживать функцию TFTP-сервера. Его необходимо подключить одновременно к консольному порту и одному из Ethernet портов коммутатора (см. рис. 3 в разделе 5.4).

Во время загрузки, сразу после включении коммутатора в сеть, нажмите клавишу **"Esc"**, после чего появится загрузочное меню. В случае отсутствия образа ПО на flash-памяти коммутатор перейдет в загрузочное меню автоматически.

```
  *** S5xxx Boot Menu ***
1. Display switch info
2. Set bootrom network parameters
3. Upgrade bootrom via TFTP
4. Run firmware from TFTP
5. Set boot option to default config
6. Set boot firmware filename
7. Run firmware from flash
8. Format flash
0. Reboot switch
```

Перед обновлением загрузчика необходимо настроить сетевые параметры для TFTP - соединения. Для этого в загрузочном меню выбрать пункт `"2. Set bootrom network parameters"`, нажав соответствующую клавишу, затем `"1. Set switch IP address"` и ввести IP-адрес коммутатора:

```
Set bootrom network parameters
1. Set switch IP address
2. Set server IP address
0. Back to main menu

Please Input new one /or Ctrl-C to discard
Input device IP (192.168.1.1): 192.168.1.1
```

В пункте 2.2. `"Set server IP address"` указать IP-адрес TFTP-сервера:

```
Set bootrom network parameters
1. Set switch IP address
2. Set server IP address
0. Back to main menu

Please Input new one /or Ctrl-C to discard
Input device IP (192.168.1.2): 192.168.1.2
```

Затем выбрать пункт меню "3. Upgrade bootrom via TFTP" и ввести имя файла с расширением ".rom". По умолчанию используется "boot.rom".

```
Upgrade bootrom via TFTP
Please Input new one /or Ctrl-C to discard
Input loader filename (boot.rom): boot.rom
Warning: Don't power off device during bootrom updating!
Are you sure to start update ? (y/n): y
Upgrade loader image [boot.rom]......
Enable network
Please wait for PHY init-time ...

Using rtl9300#0 device
TFTP from server 192.168.1.2; our IP address is 192.168.1.1
Filename 'boot.rom'.
Load address: 0x81000000
Loading: ############################################################
done
Bytes transferred = 832148 (cb294 hex)
Loader Chip: 93000000
Loader CRC: e61d138e
Loader Size: cb27c
Loader Tail CRC: e45e7ec4
Comparing file ......
Total of 917504 bytes were the same
Upgrade loader image [boot.rom] success
```

После успешного обновления выбрать пункт "0. Reboot switch" для перезагрузки коммутатора.

5.4 Восстановление ПО через загрузочное меню

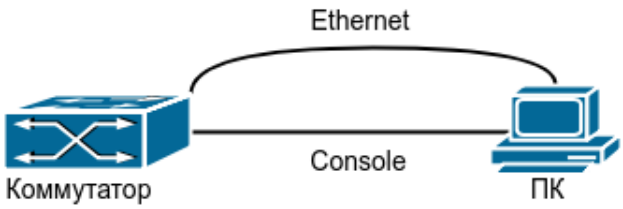

Рис. 3: Обновление через загрузочное меню

! Данный способ рекомендуется использовать только в случае невозможности загрузить образ с flash памяти.

Один из способов восстановления ПО - через загрузочное меню. Образ ПО может быть загружен в оперативную память по протоколу TFTP, после чего потребуется загрузить файл на flash-память как указано в п 5.2.

Шаг 1. Как показано на рисунке 5.1, ПК необходимо подключить одновременно к консольному порту, а также к одному из Ethernet портов коммутатора. ПК должен поддерживать функцию TFTP-сервера.

Шаг 2. Во время загрузки, сразу после включении коммутатора в сеть нажмите клавишу **"Esc"**, после чего появится загрузочное меню. В случае отсутствия образа ПО на flash-памяти коммутатор перейдет в загрузочное меню автоматически.

```
  *** S5xxx Boot Menu ***
1. Display switch info
2. Set bootrom network parameters
3. Upgrade bootrom via TFTP
4. Run firmware from TFTP
5. Set boot option to default config
6. Set boot firmware filename
7. Run firmware from flash
8. Set console speed
9. Format flash
0. Reboot switch
```

Шаг 3. После перехода в загрузочное меню необходимо выбрать пункт "2. Set bootrom network parameters"и затем "1. Set switch IP address для указания IP-адреса коммутатора:

```
Set bootrom network parameters
1. Set switch IP address
2. Set server IP address
0. Back to main menu

Please Input new one /or Ctrl-C to discard
Input device IP (192.168.1.1): 192.168.1.1
```

В пункте "2. "Set server IP address" указать IP-адрес TFTP-сервера:

```
Set bootrom network parameters
1. Set switch IP address
2. Set server IP address
0. Back to main menu

Please Input new one /or Ctrl-C to discard
Input device IP (192.168.1.2): 192.168.1.2
```

Шаг 4. После настройки сетевых параметров можно перейти к загрузке образа ПО с TFTP-сервера выбрав пункт меню "4. Run firmware from TFTP". Далее будет предложено ввести имя образа с расширением ".bix". По умолчанию используется имя "vmlinux.bix". Файл с образом ПО должен находиться в корне TFTP-сервера.

```
Run firmware from TFTP
Please Input new one /or Ctrl-C to discard
Input firmware filename (vmlinux.bix): vmlinux.bix
Start firmware boot and run ? (y/n): y
Please wait for PHY init-time ...

Using rtl9300#0 device
TFTP from server 192.168.1.2; our IP address is 192.168.1.1
Filename 'vmlinux.bix'.
Load address: 0x81000000
Loading:
#################################################################
#################################################################
#################################################################
#################################################################
#################################################################
#################################################################
#################################################################
#################################################################
#################################################################
#################################################################
#########################################
done
```

Шаг 5. После успешной загрузки образа в оперативную память, перейдите к загрузке файла (описанной в п. 5.2) на flash-память.

5.5 Выбор загрузочного файла в eNOS

При загрузке образа ПО с именем отличного от "vmlinux новое имя необходимо задать с помощью команды **boot img**.

Выбор загрузочного файла ПО:

Команда	Описание
boot img <filename> *! В Admin режиме*	Выбрать загрузочный файл образа ПО коммутатора. **<filename>** - имя образа ПО для загрузки. Например: "newimage.bix"

Просмотр информации об используемых загрузочных файлах:

Команда	Описание
show boot-files *! В Admin режиме*	Просмотр информации о загрузочном образе ПО и файле конфигурации.

5.6 Выбор загрузочного файла в загрузочном меню

Сменить образ ПО для загрузки можно в загрузочном меню выбрав пункт `"6. Set boot firmware filename"`, затем `"1. Set boot firmware filename"`, указав новое имя образа с расширением ".bix".

Пункт `"2. Reset boot firmware filename to the default value"` устанавливает имя загрузочного файла в значение по умолчанию - vmlinux.bix.

```
Set boot firmware filename
1. Set boot firmware filename
2. Reset boot firmware filename to the default value
0. Back to main menu

Please Input new one /or Ctrl-C to discard
Input boot firmware filename (vmlinux.bix): vmlinux.bix
```

5.7 ZTP (Auto Provisioning)

ZTP (**Zero-Touch Provisioning**) — это способ автоматической удалённой настройки сетевых устройств, который позволяет конечным пользователям настраивать новые устройства без посторонней помощи.

Начиная с версии ПО 1.7.0 коммутаторы SNR поддерживают возможность автоматической конфигурации и обновления ПО средствами DHCP.

Если на коммутаторе отсутствует стартовая конфигурация (файл startup.conf), то после загрузки eNOS будет активирован DHCP-клиент, ожидающий от DHCP-сервера помимо сетевых реквизитов указания следующих параметров: next-server, server-name, filename (вариант 1) либо опции 66, 67, 125 (вариант 2). Опция 125 поддерживается на версиях ПО 1.9.0 и выше.

Алгоритм работы ZTP

Вариант 1. Указание параметров next-server, server-name и filename.

Next-server должен содержать корректный IPv4 адрес, **server-name** может принимать значения: ”tftp://”, ”sftp://<user>:<password>”, ”ftp://<user>:<password>” или ”scp://<user>: <password>”, а поле **filename** должно обязательно содержать значение вида ”xxxx.conf” (startup-config) и может содержать ”yyyy.rom” (bootrom) и ”zzzz.bix” (прошивка). Значения параметра filename разделяются

символом ":" и могут быть установлены в строке в произвольном порядке (см. пример конфигурации isc-dhcp-server).

Порядок загрузки файлов следующий: startup.conf, boot.rom, vmlinux.bix.

В случае получения необходимой информации коммутатор попытается загрузить указанные файлы с файлового сервера, применить их и при успешном завершении процесса перезагрузиться.

Если коммутатору не удалось получить настройки по DHCP или DHCP-сервер не доступен, то через каждые 10 минут будет происходить повторный запуск ZTP.

Вариант 2. Наличие опции 66, 67 и 125 в пакете ACK полученном от DHCP-сервера.

Опция 66 (tftp-server-name) должна содержать следующий формат: {server-type}[<user>[:<password>]@]<ip>, где server-type может принимать значения: "tftp://", "ftp://", "scp://", "sftp://".

Опция 67 (boot-filename) должна обязательно содержать значение вида "zzzz.conf" (startup-config) и может содержать "xxxx.rom" (bootrom) и "yyyy.bix"(прошивка). Указанные значения должны разделяться символом ":" и могут быть установлены в строке в произвольном порядке (см. пример конфигурации isc-dhcp-server с опциями 66, 67 и 125).

Опция 125 (Vendor-Identifying Vendor Class Specific Information) - это строка в hex формате следующего вида: **00:00:df:76:03:01:01:01** (00:00:9d:e2:03:01:01:01), где

00:00:df:76 - Enterprise ID Nagtech (57206) или 00:00:9d:e2 - Enterprise ID NAG (40418);

03 - длина подопции;

01 - код подопции;

01 - длина значения подопции;

01 - значение подопции. Значение 0x01 в подопции 0x01 требует от коммутатора выполнить на интерфейсе vlan1 команду "no ip address", а затем "ip address dhcp".

В случае получения необходимой информации коммутатор попытается загрузить указанные файлы с файлового сервера, применить их и при успешном завершении процесса перезагрузиться.

Если ZTP остановлен вручную, то дальнейший его перезапуск не выполняется.

На версиях ПО 1.9.0 и выше, если коммутатор получил настройки по DHCP с опцией 125, в которой значение Enterprise равно 0xdf76 или 0x9de2, значение подопции 0x01 равно 0x01 и при этом обновление завершилось неуспешно (кроме остановки ZTP вручную), то на интерфейсе vlan1 удаляется статический IP-адрес и запускается DHCP-клиент, после чего работа ZTP завершается. В любом ином случае неуспешного завершения ZTP, через 10 минут будет произведён повторный запуск.

Работа ZTP может быть остановлена в следующих случаях:

- Выполнение команды "ztp stop"в Admin режиме;
- Выполнение команды "write"в Admin режиме;
- Выполнение команды "copy running-config startup-config"в Admin режиме;
- Переход в конфигурационный режим ("configure terminal").

Пример конфигурации isc-dhcp-server

```
subnet 192.168.12.0 netmask 255.255.255.0 {
       range 192.168.12.100 192.168.12.200;
       option subnet-mask 255.255.255.0;
       option routers 192.168.12.1;
       next-server 192.168.12.20;
       server-name "sftp://userf:userf";
       filename = "/home/userf/boot.rom:/home/userf/vm.bix:/home/userf/start.conf";
}
```

Пример конфигурации isc-dhcp-server с опциями 66, 67 и 125:

```
option tftp-server code 66 = string;
option bootfile-name code 67 = string;
option op125 code 125 = string;

shared-network one {
    subnet 192.168.20.0 netmask 255.255.255.0 {
         range 192.168.20.100 192.168.20.200;
         option subnet-mask 255.255.255.0;
         option broadcast-address 192.168.20.255;
         option routers 192.168.20.1;
         option tftp-server-name "tftp://192.168.20.20";
         option bootfile-name "startup.conf:boot.rom:vmlinux.bix";
         option op125 00:00:df:76:03:01:01:01;
    }
}
```

6. Операции с файловой системой

В качестве устройства для хранения файлов используется встроенная **flash память**. Обычно она используется для хранения файлов - образов ПО коммутатора (.bix файл) и файлов конфигурации (.cfg файл). Flash может копировать, удалять файлы в режиме работы ОС.

6.1 Операции с файловой системой

1. Удаление файла:

Команда	Описание
rm <file-name> *! В Admin режиме*	Удалить файл. **<file-name>** - имя удаляемого файла.

2. Переименование файла:

Команда	Описание
mv <file-name> <new-file-name> *! В Admin режиме*	Переименовать файл. **<file-name>** - имя переименуемого файла; **<new-file-name>** - новое имя файла.

3. Копирование файла:

Команда	Описание
cp <file-name> <new-file-name> *! В Admin режиме*	Скопировать файл расположенный во flash памяти. **<file-name>** - имя копируемого файла; **<new-file-name>** - новое имя файла.
copy file <file-name> **{ tftp | ftp | scp | sftp }** <url> *! В Admin режиме*	Скопировать файл из коммутатора на сервер с использованием сетевых протоколов передачи данных. **<file-name>** - имя копируемого файла; **<url>** - URL-адрес файла на TFTP / FTP / SFTP / SCP сервере (см. раздел 4).

Команда	Описание
copy { tftp | ftp | scp | sftp } <url> **file** <file-name> *! В Admin режиме*	Скопировать файл с сервера с использованием сетевых протоколов передачи данных во flash память. **<url>** - URL-адрес файла на TFTP / FTP / SFTP / SCP сервере (см. раздел 4). **<file-name>** - имя файла при сохранении в памяти коммутатора.

4. Просмотр списка файлов на flash:

Команда	Описание
dir *! В Admin режиме*	Просмотреть список файлов во flash памяти.

6.2 Сохранение конфигурации на удаленный сервер по расписанию

Коммутатор поддерживает функционал периодического сохранения текущей конфигурации (running-config) на удаленный сервер по протоколам SFTP, FTP, TFTP, SCP.

При сохранении производится ротация файлов с настраиваемой глубиной.

Команда	Описание
archive running-config location <url> [maximum <num>] [period <h>]	Включить периодическое сохранение конфигурации коммутатора. **<url>** - URL-адрес файла на TFTP / FTP / SFTP / SCP сервере (см. раздел 4). **maximum <num>** - количество файлов для ротации; **period <h>** - период сохранения конфигурации в часах;
no archive running-config *! В режиме глобальной конфигурации*	Отключить периодическое сохранение конфигурации.
archive running-config force *! В режиме глобальной конфигурации*	Принудительно запустить сохранение конфигурации на сервер.

Команда	Описание
show archive running-config *! В Admin режиме*	Вывести настройки и статус периодического сохранения конфигурации.

6.3 Пример операций с файловой системой

Сценарий 1:

Для бекапа образа ПО на flash скопировать файл vmlinux.bix с сервера под именем vmlinux_backup.bix. После копирования необходимо проверить содержимое flash.

```
Switch#copy sftp://admin:switch@10.0.0.253/vmlinux.bix file vmlinux_backup.bix
Switch#dir
-rw-r--- 1 15510154 Jan 1 05:00 vmlinux.bix
-rw-r--- 1 15510154 Jan 1 11:45 vmlinux_backup.bix
-rw-r--- 1 1101 Jan 1 06:18 startup.conf
```

Сценарий 2:

Включить периодическое сохранение конфигурации на сервер по протоколу sftp с глубиной ротации - 5 файлов и периодом сохранения 1 час.

```
Switch#conf
Switch(config)#archive running-config location sftp://sftptest:sftptest@10.10.10.1/
home/sftptest/runnin-config maximum 5 period 1
```

7. Настройка интерфейсов

Для настройки физического Ethernet интерфейса необходимо зайти в режим конфигурации интерфейса из режима глобального конфигурирования при помощи команды **Interface** <interface-list>, где в <interface-list> должны быть указаны один или несколько номеров Ethernet интерфейсов. Специальные символы "," и "**-**" служат для задания нескольких номеров интерфейсов. символ "," предназначен для разделения отдельных номеров, "-" для задания диапазона интерфейсов.

Например, командой interface ge1-5 осуществляется переход в режим конфигурирования интерфейсов из диапазона ge1-ge5. Команда interface ge1,ge5 переводит в режим конфигурирования интерфейсов ge1 и ge5.

7.1 Настройка параметров Ethernet интерфейсов

1. Вход в режим конфигурации Ethernet интерфейса:

Команда	Описание
interface <interface-list> *! В режиме глобальной конфигурации*	Вход в режим конфигурирования Ethernet интерфейса.

2. Конфигурация Ethernet интерфейсов:

Команда	Описание
shutdown **no shutdown** *! В режиме конфигурации порта*	Административное включение Ethernet интерфейса. Административное отключение Ethernet интерфейса.
description <string> **no description** *! В режиме конфигурации порта*	Конфигурация имени интерфейса <string> Удаление имени интерфейса.
speed-duplex {auto [10 [100 [1000]] [auto | full | half] | force10m-half | force10m-full | force100m-half | force100m-full | force1g-full | force10g-full [high-leq | media {dac100cm | dac300cm | dac500cm | dac50cm| fiber}]]}}	Настройка параметров скорости/дуплекса Ethernet интерфейса. **auto** - автоматическое согласование скорости (можно указать определенные типы скоростей, которые будут разрешены при автосогласовании). **10** - 10 mb/s; **100** - 100 mb/s; **1000** - 1000 mb/s;

Команда	Описание
	auto - автоматическое согласование дуплекса; **full** - задать полный дуплекс; **half** - задать полудуплекс; **force10m-half** - принудительно перевести интерфейс в режим 10 mb/s half-duplex; **force10m-full** - принудительно перевести интерфейс в режим 10 mb/s full-duplex; **force100m-full** - принудительно перевести интерфейс в режим 100 mb/s full-duplex; **force100m-half** - принудительно перевести интерфейс в режим 100 mb/s half-duplex; **force1g-full** - принудительно перевести интерфейс в режим 1000 mb/s full-duplex; **force10g-full** - принудительно перевести интерфейс в режим 10 gb/s full-duplex; **high-leq** - повышение значения LEQ для интерфейса (необходимо для совместимости с сетевым оборудованием на чипсетах Centec. Например, OLT BDCOM GP3600); **media** - настройка типа 10G трансивера (опционально); **dac100cm** - DAC кабель длиной 100 см; **dac300cm** - DAC кабель длиной 300 см; **dac500cm** - DAC кабель длиной 500 см; **dac50cm** - DAC кабель длиной 50 см; **fiber** - оптический трансивер.
no speed-duplex *! В режиме конфигурации порта*	Вернуть настройки по умолчанию (auto).
bandwidth control <bandwidth> [both | receive | transmit]	Ограничения скорости трафика на интерфейсе. **<bandwidth>** - ограничение скорости в kbps; **both** - в обоих направлениях RX и TX; **receive** - только на RX; **transmit** - только на TX.

Команда	Описание
no bandwidth control [both | receive | transmit] *! В режиме конфигурации порта*	Отключить ограничение скорости трафика на порте.
flowcontrol **no flowcontrol** *! В режиме конфигурации порта*	Включить flowcontrol на порте. Отключить flowcontrol на порте (по умолчанию).
negotiation off **negotiation on** *! В режиме конфигурации порта*	Отключить автосогласование на порте для режима 1000BaseX. Включить автосогласование на порте для режима 1000BaseX (по умолчанию).

3. Смена режима combo-порта:

Команда	Описание
media-type {copper | fiber} *! В режиме конфигурации порта*	Настройка режима combo-порта. **Copper** - медный; **Fiber** - оптоволоконный.

7.1.1 Пример настройки Ethernet интерфейса

Перевод интерфейса в режим 100BaseT (100mb/s).

```
Switch#configure terminal
Switch(config)#interface ge2
Switch(config-if)#speed-duplex force100m-full
```

Настройка автоопределения скорости 10/100 mb/s, duplex auto на гигабитном интерфейсах ge2 и ge4.

```
Switch#config
Switch(config)#interface ge2,ge4
Switch(config-if)#speed-duplex auto 10 100 auto
```

Перевод SFP+ интерфейса в режим 1000 мб/с full-duplex.

```
Switch#conf
Switch(config)#interface xe1
Switch(config-if)#speed-duplex force1g-full
```

Возврат настроек интерфейса к значению по умолчанию (автоматическое согласование скорости/дуплекса).

```
Switch#config
Switch(config)#interface ge1
Switch(config-if)#no speed-duplex
```

7.2 Настройка ограничения Broadcast, Multicast и Unicast трафика на Ethernet интерфейсе

Storm-control - это механизм ограничения входящего трафика определенного типа (Broadcast, Multicast, Unicast). Он пропускает трафик до установленного лимита и отбрасывает все пакеты превышающие его.

Опционально можно включить логирование события о превышении лимита трафика на порте или перевод его в состояние errdisable (административное отключение порта).

7.2.1 Настройка storm-control

1. Включить ограничение входящего трафика на интерфейсе.

Команда	Описание
storm-control { broadcast | multicast | unicast} **level** <value> { kbps | pps}	Включение strom control на интерфейсе для определенного типа трафика с указанием порога ограничения. **broadcast** - широковещательный трафик; **multicast** - мультикаст трафик; **unicast** - unknown Unicast; **kbps** - значение задается в kbps; **pps** - значение задается в pps; **<value>** - порог ограничения <1-16777215>.
no storm-control {broadcast | multicast | unicast} **level** *! В режиме конфигурации порта*	Отмена ограничения для выбранного типа трафика.

2. Включить логирование сообщений при срабатывании storm-control.

Команда	Описание
storm-control action log	Включение записи сообщений storm-control в лог файл при срабатывании ограничения по трафику broadcast, multicast, unicast.
no storm-control action *! В режиме конфигурации порта*	Отключение логирования storm-control.

3. Административное выключение порта при срабатывании storm-control.

Команда	Описание
storm-control action errdisable	Включение перевода порта в состояние errdisable при срабатывании storm-control. По умолчанию порт выключается на 60 сек.
no storm-control action *! В режиме конфигурации порта*	Отключение перевода порта в состояние errdisable.

При срабатывании storm-control action log или storm-control action errdisable и настроенном snmp-агенте происходит отправка SNMP Trap.

7.2.2 Пример настройки storm-control

Настройка логирования и ограничения до 1024 kbps входящего broadcast и multicast трафика при помощи storm-control:

```
Switch#configure terminal
Switch(config)#interface ge1
Switch(config-if)#storm-control broadcast level 1024 kbps
Switch(config-if)#storm-control multicast level 1024 kbps
Switch(config-if)#storm-control action log
```

7.2.3 Настройка switchport flood-control

Flood-control - механизм запрещающий отправку broadcast и unknown multicast/unicast трафика в интерфейс.

Команда	Описание
switchport flood-control {bcast | mcast | ucast}	Включить flood-control на порте для: **bcast** - broadcast трафика;

Команда	Описание
	mcast - unknown multicast трафика; **ucast** - unknown unicast трафика.
no switchport flood-control {bcast | mcast | ucast} *! В режиме конфигурации порта*	Отменить flood-control на порте.

Функционал flood-control multicast применяется только к трафику в Vlan с отключенным igmp snooping.

7.2.4 Пример настройки flood-control

Запретить отправку broadcast, unknown multicast и unknown unicast трафика на порт:

```
Switch#configure terminal
Switch(config)#vlan 10
Switch(config)#interface vlan 10
Switch(config-if)#igmp snooping
Switch(config-if)#exit
Switch(config)#interface ge1
Switch(config-if)#switchport access vlan 10
Switch(config-if)#switchport flood-control bcast
Switch(config-if)#switchport flood-control mcast
Switch(config-if)#switchport flood-control ucast
Switch(config-if)#end
```

7.3 Диагностика медного кабеля

Коммутаторы SNR поддерживают диагностику медного кабеля. В процессе диагностики проверяется длина кабеля, а также целостность каждой пары.

Возвращаются следующие статусы:

Normal - кабель подключен верно;

Short - короткое замыкание между проводами одной пары;

Cross - короткое замыкание между парами;

Open - кабель не подключен или есть разрыв;

Hi impedanse - состояние высокого сопротивления, но не обрыва;

Mismath - невозможно интерпретировать результат;

Skip - пропущен опрос пары или провода.

7.3.1 Запуск диагностики медного кабеля

Команда	Описание
show cable-test <interface-list> *! В Admin режиме*	Запуск тестирование кабеля интерфейса. **<interface-list>** - интерфейс или список интерфейсов.

7.3.2 Пример диагностики медного кабеля

Диагностика кабеля, подключенного к порту ge1:

```
Switch#show cable-test ge1
Interface    type       Pair          Status           Lenght(M)
----------  ------     -------      ------------     -----------
ge1           GE        Pair1          Open            108
ge1           GE        Pair2          Open            112
ge1           GE        Pair3          Open            112
ge1           GE        Pair4          Open            112
```

8. Errdisable

Errdisable - функция осуществляющая административное выключение порта с последующим включением после истечения установленного времени.

Данная функция используется при превышении ограничений storm-control и port-security, обнаружении петель loopback detection и включенном на порте spanning-tree bpdu-guard.

1. Настройка функции errdisable timeout:

Команда	Описание
errdisable timeout enable **errdisable timeout disable** *! В режиме глобальной конфигурации*	Включить функцию автоматического выхода порта из режима errdisable по истечении заданного времени. Выключить функцию автоматического выхода порта из режима errdisable по истечении заданного времени. Если применена эта команда, вывести порт из состояния errdisable можно только с помощью команд shutdown и no shutdown.
errdisable timeout interval <10-1000000> *! В режиме глобальной конфигурации*	Установить время (в секундах), по истечении которого порт автоматически выйдет из состояния errdisable. Значение по умолчанию - 60 секунд.

2. Просмотр состояния функции errdisable timeout:

Команда	Описание
show errdisable details *! В Admin режиме*	Отображение состояния errdisable timeout и времени ожидания перед поднятием порта после его срабатывания.

3. Просмотр портов находящихся в состоянии errdisable:

Команда	Описание
show interface errdisable status *! В Admin режиме*	Отображение всех портов в находящихся в состоянии errdisable и события по которому порт был переведен в данное состояние.

9. Изоляция портов (Port Isolation)

Изоляция портов (Port Isolation) - это независимый функционал, который ограничивает как передачу пакетов между определенными портами, так и изоляцию трафика в рамках определенного VLAN.

Настройка функционала Port Isolation сводится к указанию двух списков интерфейсов, между которыми необходимо запретить передачу трафика, а при настройке функционала **изоляция портов в VLAN** достаточно указать список интерфейсов и VLAN.

9.1 Настройка изоляции портов

1. Настройка Port Isolation:

Команда	Описание
isolate-traffic from <interface-list1> **to** <interface-list2>	Запретить передачу трафика, полученного с портов списка **<interface-list1>** на порты списка **<interface-list2>**.
no isolate-traffic from <interface-list1> **to** <interface-list2>	Разрешить передачу трафика, полученного с портов списка **<interface-list1>** на порты списка **<interface-list2>**.
! В режиме глобальной конфигурации	

2. Настройка Port Isolation в Vlan:

Команда	Описание
isolate-traffic vlan <vid> <interface-list>	Запретить передачу трафика между портами **<interface-list>** в VLAN **<vid>**.
no isolate-traffic vlan <vid>	Разрешить передачу трафика для всех портов в VLAN **<vid>**.
! В режиме глобальной конфигурации	

3. Просмотр конфигурации изоляции портов:

Команда	Описание
show isolate-traffic	Просмотр конфигурации изоляции портов для port isolation и vlan isolation.
! В Admin режиме	

9.2 Примеры настройки изоляции портов

Настройка изоляции трафика полученного с порта ge4 в сторону портов ge5 и ge8:

```
Switch#configure terminal
Switch(config)#isolate-traffic from ge4 to ge5,ge8
```

Настройка изоляции трафика в VLAN 50 между портами ge10 и ge11:

```
Switch#configure terminal
Switch(config)#vlan 50
Switch(config)#int ge10-15
Switch(config-if)#switchport access vlan 50
Switch(config-if)#exit
Switch(config)#isolate-traffic vlan 50 ge10-11
```

10. Packet-capture

Функционал packet-capture предназначен для перехвата пакетов, приходящих на порт, с возможностью записи в файл. Реализуется с помощью правила policy-map, применяемого на интерфейсе.

После запуска packet-capture происходит захват первых 256 байт пакета с ограничением скорости в 50pps. Изменить это ограничение можно применив команду:

```
cpu-rx-ratelimit protocol packet-capture <1-1200>
```

Для отображения установленного ограничения используется команда:

```
show cpu-rx protocol packet-capture
```

! Рекомендуется убирать правило policy-map с packet-capture с порта после использования для избежания лишней нагрузки на CPU коммутатора.

10.1 Настройка Packet-capture

1. Установить действие packet-capture в policy-map и применить правило на порт с которого будет перехватываться трафик(см. раздел Настройка Policy-map).

! Не рекомендуется использование функционала packet-capture на портах со включенным MAB, так как это может привести к некорректной работе MAB.

2. Запуск и остановка packet-capture:

Команда	Описание
packet-capture start [file <filename> [count <1-10000>] [proto {icmp | igmp | tcp | udp | arp | ip | ip6}] | [ether]] | [verbose] [timestamp] [proto {icmp | igmp | tcp | udp | arp | ip | ip6}]	Запустить захват пакетов с порта. Допустимо применение следующих аргументов: **file** <filename> - имя файла, в который будет производиться запись. Файлы сохраняются во flash-памяти коммутатора. Если аргумент file не указан, то вывод будет осуществляться в консоль; **count <1-10000>** - количество пакетов для захвата; **verbose** - подробный вывод; **timestamp** - вывод с указанием времени; **ether** - отображать ethernet заголовки; **proto** {icmp | igmp | tcp | udp | arp | ip | ip6} - фильтровать пакеты по выбранному протоколу.
packet-capture stop	Остановить захват пакетов в режиме записи в файл.

Команда	Описание
Ctrl+C *! В Admin режиме*	Остановить захват пакетов в режиме вывода в консоль.

10.2 Пример настройки и запуска packet-capture

Сценарий 1: Перехват пакетов с определенного MAC-адреса с выводом в консоль.

Создать MAC-ACL, задав необходимый MAC-адрес. В режиме конфигурации карты классов настроить критерий соответсвия данных карте классов на основе созданного MAC-ACL. Создать карту политик, задать действие packet-capture для class-map в policy-map, Назначить данное правило на порт и запустить packet-capture с указанием протокола arp и аргументом verbose.

Конфигурация коммутатора:

```
Switch#configure terminal
Switch(config)#access-list 100 permit mac host 0027.19B0.71FF any
Switch(config)#class-map 100
Switch(config-cmap)#match access-group 100
Switch(config-cmap)#exit
Switch(config)#policy-map p100
Switch(config-pmap)#class 100
Switch(config-pmap-c)#packet-capture
Switch(config-pmap-c)#exit
Switch(config-pmap)#exit
Switch(config)#interface ge1
Switch(config-if)#service-policy input p100
Switch(config-if)#end
Switch#packet-capture start
```

Сценарий 2: Захват и запись в файл 500 пакетов.

Для записи перехваченных пакетов в файл, необходимо в режиме конфигурации карты классов настроить критерий соответствия vlan, применить действие packet-capture для class-map в policy-map, назначить данное правило на порт и запустить packet-capture с указанием имени файла - dump.pcap и количеством пакетов для записи - 500.

Конфигурация коммутатора:

```
Switch#configure terminal
Switch(config)#vlan 10
Switch(config)#class-map c1
Switch(config-cmap)#match vlan 10
Switch(config-cmap)#exit
Switch(config)#policy-map p1
```

```
Switch(config-pmap)#class c1
Switch(config-pmap-c)#packet-capture
Switch(config-pmap-c)#exit
Switch(config-pmap)#exit
Switch(config)#interface ge1
Switch(config-if)#service-policy input p1
Switch(config-if)#end
Switch#packet-capture start file dump.pcap count 500
```

11. LLDP

LLDP (Link Layer Discovery Protocol, 802.1ab) - протокол канального уровня, позволяющий коммутатору оповещать оборудование, работающее в локальной сети, о своем существовании и передавать ему свои характеристики, а также получать от него аналогичные сведения. Каждое устройство **LLDP** может отправлять информацию о себе соседям независимо от того, отправляет ли сосед информацию о себе. Устройство хранит информацию о соседях, но не перенаправляет её. Коммутатор может передавать и принимать такую информацию, как: имя порта (**Port name**), идентификатор порта (**PortID**), аппаратный адрес (**ChassisID**), адрес управления (**Management address**), описание порта (**PortDesc**), описание устройства (**SysDesc**).

Полученная информация может быть запрошена с помощью стандартных **SNMP MIB** и использоваться в **NMS** для сбора информации и построения топологии сети.

11.1 Конфигурация LLDP

1. Включить функцию LLDP и настроить статус порта:

Команда	Описание
set lldp enable {rxonly | txonly | txrx}	Включить LLDP на порте и настроить статус. **rxonly** - разрешает только прием LLDP сообщений; **txonly** - разрешает только отправку LLDP сообщений; **txrx** - разрешает прием и отправку одновременно.
set lldp disable *! В режиме конфигурации порта*	Выключить LLDP на порте.

2. Настроить таймеры:

Команда	Описание
set lldp timer msg-tx-interval <5-32768> *! В режиме конфигурации порта*	Настроить интервал отправки LLDP сообщений в секундах. Конфигурация по умолчанию - 30 секунд.
set lldp timer reinitDelay <value> *! В режиме конфигурации порта*	Задать минимальный интервал времени, в течение которого порт LLDP ожидает перед повторной инициализацией передачи LLDP. **<value>** - Значение от 1 до 10. Конфигурация по умолчанию - 2 секунды.

Команда	Описание
set lldp timer tx-delay <seconds> *! В режиме конфигурации порта*	Задать время в течении которого коммутатор не будет принимать новые LLDP сообщения на порте после получения последнего. **<seconds>** - Значение от 1 до 8192. Конфигурация по умолчанию - 2 секунды.
set lldp msg-tx-hold <seconds> *! В режиме конфигурации порта*	Настроить количество интервалов tx-interval - время жизни информации о соседе LLDP с момента последнего обновления. **<seconds>** - Значение от 2 до 10. Конфигурация по умолчанию - 4.

3.Настроить передаваемые TLV:

Команда	Описание
set lldp system-name <name> **unset lldp system-name** *! В режиме глобальной конфигурации*	Задать имя системы, которое будет передаваться в LLDP TLV в качестве system-name. Вернуть значение по умолчанию - hostname.
set lldp system-description <text> **unset lldp system-description** *! В режиме глобальной конфигурации*	Задать описание системы, которое будет передаваться в LLDP TLV в качестве system-description. Вернуть значение по умолчанию.
lldp tlv [chassis-id] [ieee-8021-org-specific] [ieee-8023-org-specific] [management-address] [port-description] [port-id] [system-capabilities] [system-description] [system-name] [ttl]	Задать LLDP TLV отправляемые опционально. **chassis-id** - идентификатор шасси; **ieee-8021-org-specific** - IEEE 802.1 Organizationally Specific TLV; **ieee-8023-org-specific** - IEEE 802.3 Organizationally Specific TLV; **management-address** - управляющий адрес; **port-description** - описание порта; **port-id** - идентификатор порта;

Команда	Описание
	system-capabilities - возможности устройства; **system-description** - описание коммутатора; **system-name** - имя коммутатора (hostname); **ttl** - предписанное время жизни.
lldp tlv unset [ieee-8021-org-specific] [ieee-8023-org-specific] [system-name] [management-address] [port-description] [system-capabilities][system-description] *! В режиме конфигурации порта*	Отключить опциональные tlv.
set lldp management-address-tlv {ip-address | mac-address} *! В режиме конфигурации порта*	Выбрать тип адреса (**ip** или **mac**), передаваемого в management-address TLV. По умолчанию используется тип адреса IP.
set lldp locally-assigned <name> **unset lldp locally-assigned** *! В режиме конфигурации порта*	Установить локальное имя для интерфейса. Удалить имя интерфейса.
lldp port-id-tlv {if-name | ip-address | local | mac-address} *! В режиме конфигурации порта*	Выбрать данные для передачи в качестве port-id-tlv.
lldp chassis-id-tlv {if-name | ip-address | local | mac-address} *! В режиме конфигурации порта*	Выбрать данные для передачи в качестве chassis-id-tlv.

4. Настроить таблицу соседей:

Команда	Описание
set lldp too-many-neighbors limit <1-65535> discard {exiting-info <mac-address> | received-info} timer <1-65535>	Задать действие при получении информации от нового соседа при превышении максимального числа <1-65535> соседей. **discard exiting-info** - MAC-адрес соседа для отмены ограничения; **discard received-info** - не записывать информацию о новом соседе (по умолчанию).

Команда	Описание
set lldp too-many-neighbors limit disable *! В режиме конфигурации порта*	Отменить установленное действие.

5. Вывод информации и отладка:

Команда	Описание
show lldp port <ifname> *! В Admin режиме*	Вывести суммарную информацию о конфигурации LLDP на порте и его соседях. **<ifname>** - имя интерфейса.
show lldp neighbors brief *! В Admin режиме*	Вывести краткую информацию по всем портам, где есть LLDP-соседи.

11.2 Пример конфигурации LLDP

Два коммутатора соединены друг с другом одним линком. Порт коммутатора **Switch B** настроен только для получения **LLDP** сообщений. Порт коммутатора **Switch A** должен передавать информацию об описании порта и возможностях системы.

Конфигурация коммутаторов будет выглядеть следующим образом:

Конфигурация коммутатора **Switch A**:

```
SwitchA(config)#interface ge4
SwitchA(config)#set lldp enable txrx
SwitchA(config-if)#lldp tlv system-capabilities port-description
SwitchA(config-if)#end
```

Конфигурация коммутатора **Switch B**:

```
SwitchB(config)#interface ge1
SwitchB(config-if)#set lldp enable rxonly
SwitchB(config-if)#end
```

12. ULDP

ULDP (Unidirectional Link Detection Protocol) - протокол уровня 2 (L2), который работает с механизмами уровня 1 (L1) для определения физического состояния канала. На уровне 1 автосогласование обеспечивает физическую передачу сигналов и обнаружение неисправностей. ULDP выполняет задачи, которые не может выполнить автоматическое согласование, например, отключение неправильно подключенных портов.

ULDP использует систему собственных сообщений и работает посредством обмена этими сообщениями между соседними устройствами. Для работы ULDP устройства в соединении должны поддерживать данный функционал, который необходимо применить на соответствующих портах.

Каждый порт коммутатора, настроенный для ULDP, отправляет пакеты протокола, которые содержат MAC-адрес порта и его Port Index. Соседние порты видят свои собственные идентификаторы устройства/порта (эхо) в пакетах, полученных с другой стороны. Если порт не видит свой собственный идентификатор устройства/порта во входящих пакетах ULDP в течение определенного периода времени, канал считается однонаправленным (**Unidirectional**).

Этот эхо-алгоритм позволяет обнаруживать следующие проблемы:

- Соединение установлено с обеих сторон, но пакеты принимает только одна сторона.
- Ошибки подключения провода, когда волокна приема и передачи не подключены к одному и тому же порту на удаленной стороне.

ULDP может работать в двух режимах: обычном (normal mode) и агрессивном (aggressive mode):

В обычном режиме (**normal mode**), если состояние порта было определено как двунаправленное и в течении 3 интервалов Hello не получен корректный пакет ULDP Hello, то выводится сообщение о необходимости отключить порт. Порт не выключается и состояние порта для ULDP изменяется на неопределенное.

В агрессивном режиме (**aggressive mode**), если состояние порта определено как двунаправленное и в течении 3 интервалов Hello не получен корректный пакет ULDP Hello и затем в течение 7 секунд не установлено новое соседство по ULDP, то порт переводится в состояние errdisable.

Если порт переходит в состояние Unidirectional (однонаправленный), то независимо от выбранного режима normal или aggressive порт переходит в состояние errdisable.

Состояние порта останется отключенным до тех пор, пока оно не будет включено вручную или пока не истечет время ожидания отключения по ошибке (если оно настроено).

12.1 Конфигурация ULDP

1. Включить функцию ULDP:

Команда	Описание
uldp enable **no uldp enable** *! В режиме конфигурации порта*	Включить ULDP на порте. Выключить ULDP на порте.

2. Настроить режим работы:

Команда	Описание
uldp aggressive-mode **no uldp aggressive-mode** *! В режиме конфигурации порта*	Установить режим Aggressive. Вернуть режим Normal.

3. Настроить интервал и таймер:

Команда	Описание
uldp hello-interval <5-100> **no uldp hello-interval** *! В режиме глобальной конфигурации*	Задать интервал отправки сообщений ULDP в секундах. Вернуть значение по умолчанию - 10 секунд.
uldp recovery-time <30-86400> **no uldp recovery-time** *! В режиме глобальной конфигурации*	Задать время (в секундах) восстановления порта после отключения протоколом ULDP. Вернуть значение по умолчанию - 0 секунд (порт не будет восстановлен автоматически).

4. Вывести информацию о конфигурации:

Команда	Описание
show uldp [interface <if-name>] *! В Admin режиме*	Отобразить конфигурацию и состояние ULDP на всех портах или детальную информацию на определённом порте interface <if-name>.

12.2 Пример конфигурации ULDP

Как показано на рисунке 4, коммутаторы соединены между собой двумя отдельными линиями. При организации связи волокна, предназначенные для передачи трафика от коммутатора Switch B коммутатору Switch A, в результате ошибки оказались перепутаны местами. Физический уровень при этом работает, но на канальном уровне будут возникать проблемы. ULDP обнаружит эту проблему и переведет порты в статус ошибки.

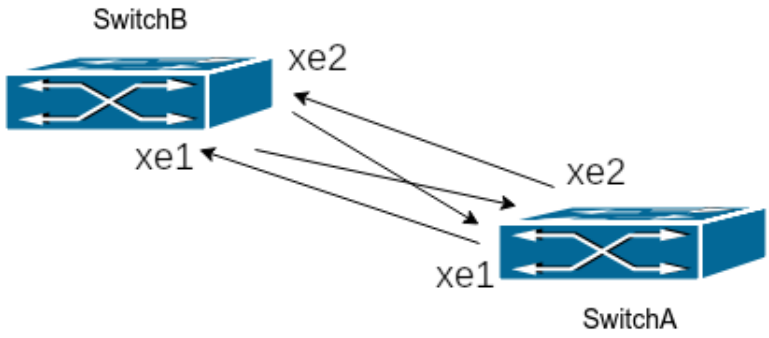

Рис. 4: ULDP

Конфигурация коммутатора **Switch A**:

```
SwitchA#configure terminal
SwitchA(config)#interface xe1-2
SwitchA(config-if)#uldp enable
SwitchA(config-if)#end
```

Конфигурация коммутатора **Switch B**:

```
SwitchB#configure terminal
SwitchB(config)#interface xe1-2
SwitchB(config-if)#uldp enable
SwitchB(config-if)#end
```

При обнаружении проблем ULDP выведет следующие сообщения:

```
2024 Jan 20 16:50:15 NSM-4: Unidirectional port xe1 was shutted down by ULDP
2024 Jan 20 16:50:15 NSM-4: Interface xe1 changed state to admin down
2024 Jan 20 16:50:15 NSM-4: Unidirectional port xe2 was shutted down by ULDP
2024 Jan 20 16:50:15 NSM-4: Interface xe2 changed state to admin down
```

12.3 Решение проблем с конфигурацией ULDP

• Для обнаружения некорректного соединения порты должны работать в дуплексном режиме и иметь одинаковую скорость;

• Интервал отправки сообщений Hello может быть изменен (в интервале от 5 до 100 секунд, по умолчанию - 10 секунд) для увеличения скорости реакции на ошибки. Но рекомендуется, чтобы этот интервал был менее 1/3 от времени сходимости STP, так как большее время может повлечь создание петли коммутации раньше, чем ULDP обнаружит проблему;

• LACP прозрачен для ULDP, он работает на каждом линке как на независимом;

• Таймер восстановления порта отключен по умолчанию и будет включен только после его настройки.

13. Loopback detection

Петля коммутации (loopback) - состояние в сети, при котором коммутатор принимает кадры, отправленные им же. При получении кадра впервые, коммутатор добавляет MAC-адреса источника в таблицу, создавая соответствие с тем портом, на котором был получен кадр. Следующий кадр с данным MAC-адресом получателя будет отправлен на порт в соответствии с таблицей. Когда MAC-адрес источника уже изучен коммутатором, но кадр тем же MAC-адресом получен через другой порт, коммутатор меняет соответствие для MAC-адреса в таблице. В результате, если на порте существует петля, из-за наличия широковещательных и многоадресных кадров может произойти не только лавинный рост количества таких кадров - все MAC-адреса в пределах второго уровня(L2) сегмента сети будут изучены на порте с петлей, что вызовет потерю работоспособности сети. Избежать возникновения петель коммутации поможет функция **Loopback detection**. С её помощью порт с петлей будет автоматически заблокирован - переведен в статус errdisable, а коммутатор может послать уведомление в Syslog для своевременного обнаружения петли администратором.

13.1 Конфигурация Loopback detection

1. Настроить loopback-detection:

Команда	Описание
loopback-detection interval-time <1-300> *! В режиме глобальной конфигурации*	Задать интервал отправки BPDU, в секундах.

2. Включить функцию Loopback detection:

Команда	Описание
loopback-detection enable **no loopback-detection enable** *! В режиме конфигурации порта*	Включить функцию loopback-detection на интерфейсе. Выключить функцию loopback-detection на интерфейсе.

3. Отобразить информацию о конфигурации и отладочную информацию:

Команда	Описание
show loopback-detection *! В Admin режиме*	Просмотр информации о конфигурации и счетчика обнаружения петли.

4. Очиста счетчика:

Команда	Описание
loopback-detection reset-counters *! В режиме глобальной конфигурации*	Очистка счетчика обнаружения петли.

13.2 Пример конфигурации Loopback detection

Чтобы защитить сеть от последствий возникновения петли коммутации из-за ошибки пользователя, неисправности линии или оборудования, подключенных к порту ge1 коммутатора, необходимо настроить функцию **loopback-detection**.

Конфигурация коммутатора будет выглядеть следующим образом:

```
switch#configure
switch(config)#loopback-detection interval-time 10
switch(config)#errdisable timeout interval 600
switch(config)#interface ge1
switch(config-if)#loopback-detection enable
```

13.3 Решение проблем с конфигурацией Loopback detection

• Убедитесь, что оборудование, подключенное к интерфейсу с loopback detection, прозрачно пропускает Loopback-detection BPDU, иначе функция не будет работать;

• Рекомендуется использовать Loopback-detection только на портах в сторону неконтролируемого участка сети (порты доступа, сегменты с неуправляемыми коммутаторами);

• Не рекомендуется использовать loopback-detection на одном порте с протоколами STP, так как это может повлечь за собой некорректную работу STP или Loopback-detection.

14. LACP и агрегация портов

Агрегирование портов - это процесс объединения нескольких портов с одинаковой конфигурацией для использования их логически в качестве одного физического порта **Port-Channel** (см. рис. 5 LACP), что позволяет суммировать полосу пропускания в одном логическом линке и использовать резервирование. Для агрегации портов на коммутаторах SNR используется **Port-Group**, который должен быть создан и добавлен на порты для работы их как часть одного Port-Channel.

Для создания и корректной работы, физические порты интерфейса Port-Channel должны работать в дуплексном режиме (full-duplex) и иметь одинаковую конфигурацию.

После объединения физические порты могут конфигурироваться одновременно как один логический интерфейс Port-channel. Система автоматически установит порт с наименьшим номером в качестве Master port. Если на коммутаторе включен функционал spanning tree protocol (STP), то STP будет рассматривать Port-Channel как логический порт и отправлять кадры BPDU через Master port.

Коммутатор позволяет объединять физические порты любых двух коммутаторов, существует ограничение на максимальное число групп - 14, и максимальное число портов в каждой группе - 8.

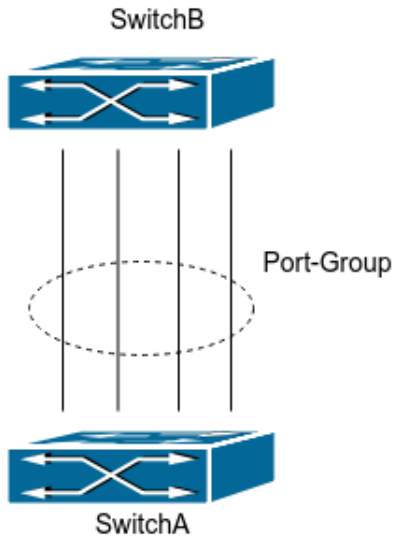

Рис. 5: LACP

14.1 Статическое агрегирование

Статическое агрегирование производится путем ручного конфигурирования пользователем и не требует использования протокола LACP. При конфигурировании статического агрегирования используется режим “static-channel-group” для добавления порта в Channel-Group.

14.2 Динамическое агрегирование LACP

LACP (Link Aggregation Control Protocol) - протокол агрегирования каналов, описанный в стандарте IEEE 802.3ad. LACP использует LACPDU сообщения для обмена информацией с соседней стороной.

После включения LACP порт посылает LACPDU, уведомляя ответную сторону о приоритете и MAC-адресе системы, приоритете и адресе порта и ключе операции. Когда ответный порт получает эту информацию, он сравнивает её с информацией о своих портах, настроенных на агрегацию. Таким образом обе стороны достигают соглашения о включении или исключении порта из динамической группы агрегации.

В динамической группе агрегации порты имеют 2 статуса - выбранный (selected) и в ожидании (standby). Порты могут посылать и принимать LACPDU находясь в любом статусе, но в статусе standby порт не может передавать данные.

Поскольку существует ограничение на количество портов в группе, если текущее число членов агрегации превышает это ограничение, коммутатор согласовывает статус порта с другой стороной на основании port ID. Согласование происходит следующим образом:

1. Сравнение ID устройств (приоритет системы + MAC-адрес системы). Если приоритет устройств одинаков - сравниваются MAC-адреса устройств. Наименьший номер будет иметь наивысший приоритет;

2. Сравнение ID портов (приоритет порта + идентификатор порта). Для каждого порта на стороне устройства с наивысшим приоритетом системы сравниваются приоритеты портов. Если приоритеты одинаковые - сравниваются ID портов. Порт с наименьшим идентификатором порта становится выбранным (selected), а остальные - в режим ожидания (standby).

3. В данной Port-Group порт с наименьшим идентификатором и статусом standby становится мастер-портом. Другие порты со статусом selected становятся членами группы.

14.3 Конфигурация агрегации портов

1. Добавить порт в Port-Group для агрегации, выбрать режим:

Команда	Описание
channel-group <port-group-number> **mode** {**active** | **passive**}	Добавить данный порт в Port-Group и выбрать режим агрегации. **active** - порт будет посылать сообщения LACPDU независимо от второй стороны; **passive** - порт будет ожидать получения LACPDU от ответной стороны.

Команда	Описание
no channel-group *! В режиме конфигурации порта*	Удалить порт из Port-Group.
static-channel-group <port-group-number> **no static-channel-group** *! В режиме конфигурации порта*	Добавить данный порт в Port-Group с режимом статической агрегации. Удалить порт из Port-Group.

2. Войти в режим конфигурации Port-Channel:

Команда	Описание
interface po <port-channel-number> *! В режиме глобальной конфигурации*	Войти в режим конфигурации Port-Channel. **<port-channel-number>** - соответствует **<port-group-number>** созданной Port-Group.

3. Войти в режим конфигурации Static-Port-Channel:

Команда	Описание
interface sa <port-channel-number> *! В режиме глобальной конфигурации*	Войти в режим конфигурации Static-Port-Channel. **<port-channel-number>** - соответствует **<port-group-number>** созданной Port-Group.

4. Выбрать метод балансировки трафика:

Команда	Описание
port-channel load-balance {dst-ip | dst-mac | dst-port | src-dst-ip | src-dst-mac | src-dst-port | src-ip | src-mac | src-port} **no port-channel load-balance** *! В режиме глобальной конфигурации*	Выбрать метод балансировки трафика для всех Port-Channel. Вернуть метод по умолчанию - src-dst-mac.

5. Задать приоритет системы для LACP:

Команда	Описание
lacp system-priority <system-priority> **no lacp system-priority** *! В режиме глобальной конфигурации*	Задать приоритет системы для LACP. Вернуть приоритет по умолчанию - 32768.

6. Задать приоритет порта для LACP:

Команда	Описание
lacp port-priority <port-priority> **no lacp port-priority** *! В режиме конфигурации порта*	Задать приоритет порта для LACP. Вернуть приоритет по умолчанию - 32768.

7. Задать режим тайм-аута для LACP:

Команда	Описание
lacp timeout {short | long} **no lacp timeout** *! В режиме конфигурации порта*	Выбрать режим таймаута порта для LACP. Вернуть режим по умолчанию - long.

8. Просмотр информации:

Команда	Описание
show etherchannel <channel-group-num> *! В Admin режиме*	Просмотр информации о заданной channel-group.
show etherchannel detail [<channel-group-num>] *! В Admin режиме*	Просмотр детальной информации о состоянии и конфигурации всех channel-group на коммутаторе или на конкретном channel-group.
show etherchannel summary *! В Admin режиме*	Просмотр суммарной информации о состоянии channel-group на коммутаторе.

Команда	Описание
show etherchannel load-balance *! В Admin режиме*	Просмотр информации о конфигурации load-balance.
show lacp sys-id *! В Admin режиме*	Просмотр LACP sys-id.
show lacp-counter <channel-group-num> *! В Admin режиме*	Просмотр счетчиков LACP.

14.4 Пример конфигурации агрегации портов

Сценарий 1: LACP.

Коммутаторы Switch A и Switch B соединены между собой с помощью 4-х линий: порты ge1-ge4 коммутатора Switch A добавлены в channel-group 1 в режиме active, порты ge7-ge10 коммутатора Switch B добавлены в channel-group 2 в режиме passive. В результате конфигурации и согласований LACP порты ge1-ge4 коммутатора Switch A будут объединены в интерфейс “Port-Channel1”, а порты ge7-ge10 коммутатора Switch B будут объединены в интерфейс “Port-Channel2”.

Конфигурация будет выглядеть следующим образом:

Switch A

```
SwitchA#configure terminal
SwitchA(config)#interface ge1-4
SwitchA(config-if)#channel-group 1 mode active
```

Switch B

```
SwitchB#configure terminal
SwitchB(config)#interface ge7-10
SwitchB(config-if)#channel-group 2 mode passive
```

Сценарий 2: Ручное агрегирование портов.

Коммутаторы Switch A и Switch B соединены между собой с помощью 4-х линий: порты ge1 - ge4 коммутатора Switch A добавлены в static-channel-group 1, порты ge1 - ge4 коммутатора Switch B добавлены в static-channel-group 2.

Switch A

```
SwitchA#configure terminal
SwitchA(config)#interface ge1-4
SwitchA(config-if)#static-channel-group 1
```

Switch B

```
SwitchB#configure terminal
SwitchB(config)#interface ge7-10
SwitchB(config-if)#static-channel-group 2
```

В результате выполнения конфигурации описанной выше, порты добавляются в Port-Channel сразу, как только выполняется команда. Обмен LACPDU не требуется.

14.5 Решение проблем при конфигурации агрегации портов

Убедитесь, что все порты в группе имеют одинаковую конфигурацию, используются в режиме полного дуплекса и имеют одинаковую скорость.

15. Настройка MTU

MTU (Maximal Transmition Unit) означает максимальный размер кадра данных, который может быть передан без фрагментации. По умолчанию MTU на физических интерфейсах 12270 байт, а на vlan интерфейсах - 1500 байт. Существует возможность разрешения работы с кадрами данных 1501-12270 байт для каждого интерфейса.

15.1 Конфигурация MTU

Команда	Описание
mtu [<value>] **no mtu** *! В режиме конфигурации порта*	Задать максимальный размер MTU пакетов в диапазоне 1500-12270 байт, принимаемых/ отправляемых коммутатором. Команда no восстанавливает значение по умолчанию.

16. VLAN

VLAN (Virtual Local Area Network) - это технология, позволяющая объединять устройства в сети в сегменты на основе функций, приложений или требований управления. Виртуальные сегменты могут формироваться в независимости от физического расположения устройств. VLAN имеют те же свойства, что и физические LAN, за исключением того, что VLAN представляет собой логическое объединение, а не физическое. Поэтому во VLAN можно объединять устройства, независимо от того, где они находятся физически, а широковещательный, многоадресный и одноадресный трафик в одном VLAN отделен от других VLAN.

Стандарт IEEE 802.1Q определяет процедуру передачи трафика VLAN.

Основная идея технологии VLAN заключается в том, что большая локальная сеть может быть динамически разделена на отдельные широковещательные области, удовлетворяющие различным требованиям, каждый VLAN представляет собой отдельный широковещательный домен.

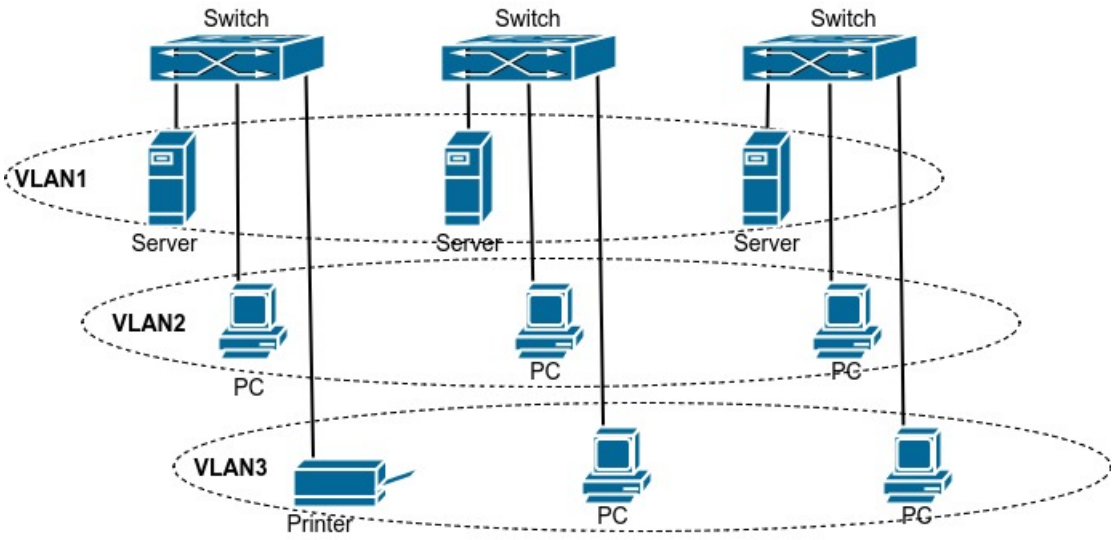

Рис. 6: Логическое разделение сети на VLAN

Благодаря этим функциям технология VLAN предоставляет следующие возможности:

- Повышение производительности сети;
- Сохранение сетевых ресурсов;
- Оптимизация сетевого управления;
- Снижение стоимости сети;
- Повышение безопасности сети.

16.1 Port-based VLAN

Ethernet-порт коммутатора может работать в трех режимах: Access, Trunk и Hybrid, каждый режим имеет различный метод обработки при передаче кадров с тегом или без.

Порт в режиме **Access** относится только к одному VLAN, обычно используется для подключения конечных устройств, таких как персональный компьютер или WI-FI маршрутизатор в квартире или офисе.

Порт в режиме **Trunk** относится к нескольким VLAN и может принимать и отправлять кадры одновременно в нескольких VLAN. Обычно используется для соединения коммутаторов.

Порт в режиме **Hybrid**, так же как и Trunk, относится к нескольким VLAN и может принимать и отправлять кадры одновременно в нескольких VLAN. Может использоваться как для подключения персональных компьютеров, так и для соединения коммутаторов.

Ethernet-порты в режимах Hybrid и Trunk могут принимать данные одним, но отправляют разными способами: Hybrid порт может отправлять пакеты в нескольких VLAN в нетегированном виде, в то время как Trunk может отправлять трафик в нескольких VLAN только с тегом, за исключением native VLAN.

16.1.1 Конфигурация Port-based VLAN

1. Создание и удаление VLAN:

Команда	Описание
vlan <vlan-range> **no vlan** <vlan-range> *! В режиме глобальной конфигурации*	Создание одного или группы VLAN. Удаление одного или группы VLAN.

2. Конфигурация VLAN:

Команда	Описание
vlan database *! В режиме глобальной конфигурации*	Вход в режим конфигурации vlan database.
vlan <vlan-id> **no vlan** <vlan-id> *! В режиме конфигурации vlan database*	Создание VLAN с номером <vlan-id>. Удаление VLAN с номером <vlan-id>.
vlan <vlan-id> **name** <vlan-name> *! В режиме конфигурации vlan database*	Назначение имени VLAN.

3. Выбор типа порта коммутатора:

Команда	Описание
switchport mode {trunk [allow-null] | access | hybrid} *! В режиме конфигурации порта*	Установка текущего порта в режим Trunk, Access или Hybrid. **trunk*** - перевести порт в режим Trunk и разрешить все VLAN на порте, если список разрешенных VLAN не указан; **trunk allow-null** - установить запрет всех VLAN на порте, кроме native VLAN; **access** - перевести порт в режим access с установкой default VLAN (vlan 1). **hybrid** - перевести порт в режим hybrid с установкой запрета всех VLAN, кроме native VLAN. **** В версии ниже 1.7.0 команда switchport mode trunk запрещает все VLAN на порте**, если список разрешенных VLAN не указан.*

4. Настройка порта в режиме Trunk:

Команда	Описание
switchport trunk allowed vlan {**<vlan>** | **all** | **add** <vlan_list> | **except** <vlan_list> | **remove** <vlan_list> | **none** } **no switchport trunk** *! В режиме конфигурации порта*	Настройка списка разрешенных VLAN на порте. **<vlan>** - задать список разрешенных VLAN; **all** - разрешить все VLAN на порте; **add** - добавить указанные VLAN к списку разрешенных; **except** - запретить указанные VLAN на порте; **remove** - удалить указанные VLAN из списка разрешенных; **none** - запретить все VLAN на порте. Вернуть значение по умолчанию на Access.
switchport trunk native vlan <vlan-id> **no switchport trunk native vlan** *! В режиме конфигурации порта*	Установить VLAN для нетегированных пакетов (PVID) для интерфейса. Вернуть значение по умолчанию (VLAN 1).

5. Настройка порта в режиме Access:

Команда	Описание
switchport access vlan <vlan-id> *! В режиме конфигурации порта*	Добавить текущий порт в VLAN <vlan-id>

6. Настройка порта в режиме Hybrid:

Команда	Описание
switchport hybrid allowed vlan {**<vlan>** {**tag** | **untag**} | **add** <vlan_list> {**tag** | **untag**} | **except** <vlan_list> | **remove** <vlan_list> | **none** }	Настройка списка разрешенных VLAN на порте в Hybrid режиме. **<vlan>** - задать список разрешенных VLAN; **add** - добавить указанные VLAN к списку разрешенных; **except** - запретить указанные VLAN на порте; **remove** - удалить указанные VLAN из списка разрешенных; **none** - запретить все VLAN на порте; **tag** - отправлять пакеты с тегом VLAN; **untag** - снимать тег VLAN при отправке пакета.
no switchport hybrid *! В режиме конфигурации порта*	Вернуть значение по умолчанию на Access.
switchport hybrid native vlan <vlan-id> *! В режиме конфигурации порта*	Установка PVID для интерфейса.

7. Запрет приема нетегированного трафика на портах в режиме Trunk и Hybrid:

Команда	Описание
switchport discard packet untag	Разрешить прием только тегированных пакетов.
no switchport discard packet untag *! В режиме конфигурации порта*	Разрешить прием всех пакетов.

16.1.2 Пример конфигурации VLAN

Представленная, на рисунке 7, сеть разделена на 3 VLAN (VLAN2, VLAN100, VLAN200) по используемым приложениям, а также по соображениям безопасности. Эти VLAN расположены

в разных локациях: A и B. Каждый из двух коммутаторов размещен в своей локации. Устройства в разных локациях могут быть объединены виртуальную локальную сеть, если трафик будет передаваться между коммутаторами A и B.

Соедините порты в режиме trunk на коммутаторах A и B друг с другом, подключите остальные сетевые устройства к соответствующим портам.

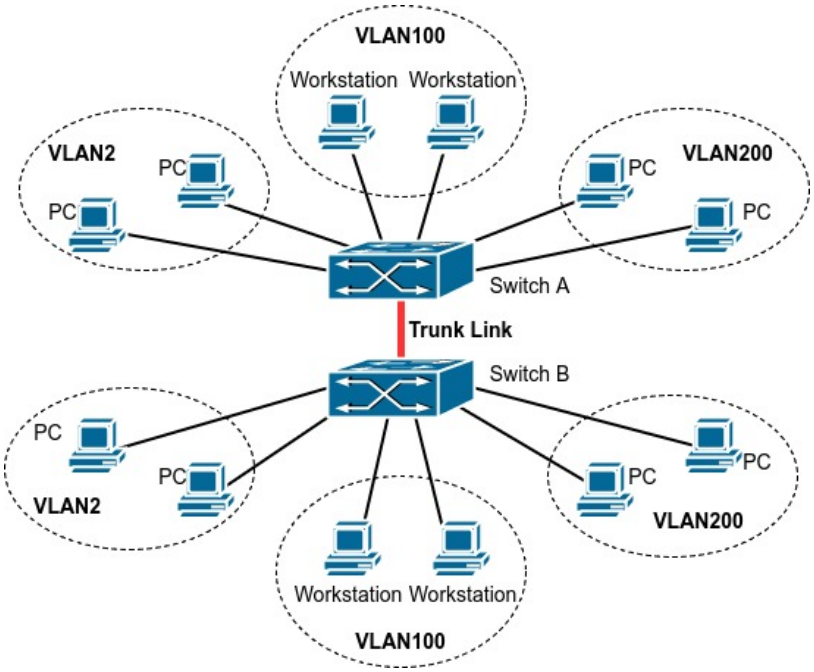

Рис. 7: Топология для примера настройки VLAN

Switch A:

```
Switch(config)#vlan 2,100,200
Switch(config)#interface ge2-4
Switch(config-if)#switchport access vlan 2
Switch(config-if)#interface ge5-7
Switch(config-if)#switchport access vlan 100
Switch(config-if)#interface ge8-10
Switch(config-if)#switchport access vlan 200
Switch(config-if)#interface ge11
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 2,100,200
```

Switch B:

```
Switch(config)#vlan 2,100,200
Switch(config)#interface ge2-4
Switch(config-if)#switchport access vlan 2
Switch(config-if)#interface ge5-7
Switch(config-if)#switchport access vlan 100
Switch(config-if)#interface ge8-10
```

```
Switch(config-if)#switchport access vlan 200
Switch(config-if)#interface ge11
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 2,100,200
```

16.2 Voice VLAN

Voice VLAN (Голосовой VLAN) предназначен для выделения трафика VOIP в отдельный VLAN. Настроив Voice VLAN пользователь сможет настроить QoS (качество сервиса) для голосовых данных и повысить приоритет передачи трафика голосовых данных для обеспечения качества.

После настройки соответствия Voice VLAN - MAC-адрес и включения Voice VLAN на интерфейсе, коммутатор будет отслеживать MAC-адрес голосового устройства в трафике данных, входящем в порт и передавать его Voice VLAN. Благодаря этому оборудование может всегда относиться к определенной Voice VLAN даже если голосовое устройство будет перемещено физически без модификации конфигурации коммутатора.

Для корректной работы функционала порт, на котором настроен Voice VLAN, должен быть настроен в режиме Hybrid, и Voice VLAN разрешен в нетегированном режиме.

16.2.1 Конфигурация Voice VLAN

1. Выбор VLAN как Voice VLAN:

Команда	Описание
voice-vlan vlan <vlan-id>	Выбрать VLAN в качестве Voice VLAN.
no voice-vlan	Отменить выбор VLAN в качестве Voice VLAN.
! В режиме глобальной конфигурации	

2. Добавление голосового оборудования в Voice VLAN:

Команда	Описание
voice-vlan mac <mac-address> <mac-mask> **priority** <priority-id> [**name** <voice-name>]	Выбрать MAC-адрес голосового оборудования для добавления в Voice VLAN.
no voice-vlan {**mac** <mac-address> **mask** <mac-mask> | **name** <voice-name> | **all**}	Удалить MAC-адрес голосового оборудования из Voice VLAN.
! В режиме глобальной конфигурации	

3. Включение Voice VLAN на портах:

Команда	Описание
switchport voice-vlan enable	Включить функцию Voice VLAN на порте.
no switchport voice-vlan enable	Выключить функцию Voice VLAN на порте.
! В режиме конфигурации порта	

16.2.2 Пример конфигурации Voice VLAN

Сценарий:

Для IP-телефонов используется VLAN 100, для компьютера подключенного через телефон - vlan 199. Устройство IP-phone1" имеет MAC-адрес 00-03-0f-11-22-33 и подключен к порту ge1 коммутатора, "IP-phone2" имеет MAC-адрес 00-03-0f-11-22-55 и подключен к порту ge2 коммутатора.

Конфигурация будет выглядеть следующим образом:

```
switch(config)#vlan 100,199
switch(config)#voice-vlan vlan 100
switch(config)#voice-vlan mac 00-03-0f-11-22-33 ff-ff-ff-ff-ff-00 priority 5 name
IP-phone1
switch(config)#voice-vlan mac 00-03-0f-11-22-55 ff-ff-ff-ff-ff-00 priority 5 name
IP-phone2
switch(config)#int ge1-2
switch(config-if)#switchport mode hybrid
switch(config-if)#switchport hybrid native vlan 199
switch(config-if)#switchport hybrid allowed vlan 100 untag
switch(config-if)#switchport voice-vlan enable
```

16.2.3 Решение проблем с Voice VLAN

Убедитесь, что Voice VLAN настроен на порте в hybrid untag режиме.

Убедитесь, что MAC-адрес VOIP устройства входит в настроенный диапазон для Voice VLAN.

16.3 MAC-VLAN

Функционал MAC-VLAN предназначен для возможности назначения тега VLAN пакету, на основе MAC-адреса источника.

16.3.1 Конфигурация MAC-VLAN

1. Создание MAC-VLAN:

Команда	Описание
mac-vlan vlan <1-4094>	Задать VLAN в качестве MAC-VLAN.
no mac-vlan vlan <1-4094>	Удалить MAC-VLAN.
! В режиме глобальной конфигурации	

2. Создание диапазона MAC-адресов:

Команда	Описание
mac-vlan mac <mac-addr> <mac-mask> **vlan** <1-4094> [priority <0-7>] **name** <word>	Задать диапазон MAC-адресов для VLAN.
no mac-vlan { **all** | **mac** <mac-addr> <mac-mask> **vlan** <1-4094> | **name** <word> }	Удалить: **all** - все MAC-VLAN записи; **mac** <mac-addr> <mac-mask> **vlan** <1-4094> - определённую запись MAC-VLAN; **name** <word> - запись MAC-VLAN по имени.
! В режиме глобальной конфигурации	

3. Включение MAC-VLAN на портах:

Команда	Описание
switchport mac-vlan enable	Включить MAC-VLAN на порте.
no switchport mac-vlan enable	Выключить MAC-VLAN на порте.
! В режиме конфигурации порта	

16.3.2 Пример конфигурации MAC-VLAN

Сценарий: Требуется создать привязку диапазона MAC-адресов с 12:34:56:AA:00:00 по 12:34:56:AA:FF:FF к VLAN 10, а трафик с MAC-адресом источника AB:CD:EF:99:99:99 следует направлять в VLAN 9. После чего включить MAC-VLAN на портах ge9 и ge10.

Конфигурация будет выглядеть следующим образом:

```
switch#configure terminal
switch(config)#vlan 9,10
switch(config)#mac-vlan vlan 9
switch(config)#mac-vlan vlan 10
switch(config)#mac-vlan mac AB:CD:EF:99:99:99 FF:FF:FF:FF:FF:FF vlan 9 name N1
switch(config)#mac-vlan mac 12:34:56:AA:00:00 FF:FF:FF:FF:00:00 vlan 10 name GR1
switch(config)#interface ge9-10
switch(config-if)#switchport mode trunk
switch(config-if)#switchport mac-vlan enable
switch(config-if)#end
```

16.4 Protocol-VLAN

Функционал Protocol-VLAN позволяет назначать VLAN тег на приходящие на порт кадры на основании типа кадра и поля Ethertype. Таким образом можно помещать трафик определенных протоколов (IPv4, IPv6, PPPoE) в отдельный VLAN.

Настройка Protocol-vlan производится путем создания группы, где указывается тип пакета и ethertype. Затем на физическом интерфейсе настраивается соответствие группы и номера VLAN.

Коммутатор поддерживает 8 групп Protocol-VLAN.

16.4.1 Конфигурация Protocol-VLAN

1. Создание группы Protocol-VLAN:

Команда	Описание
protocol-vlan group <N> **mode** {ethernet | llc | snap} **etype** <ethertype>	Создать группу protocol-VLAN: **<N>** - номер группы от 1 до 8; **ethernet | llc | snap** - тип пакета (Ethernet2, LLC или SNAP); **<ethertype>** - номер ethertype в HEX формате.
no protocol-vlan group N	Удалить группу protocol-VLAN.
! В режиме глобальной конфигурации	

2. Настройка Protocol-VLAN на порте:

Команда	Описание
switchport protocol-vlan group N vlan X [priority 0-7]	Включить привязку VLAN X к группе protocol-VLAN N. **[priority 0-7]** - установить приоритет COS пакетов для VLAN X.
no switchport protocol-vlan group N *! В режиме конфигурации порта*	Удалить привязку VLAN X к группе protocol-VLAN N.

3. Просмотр информации о Protocol-VLAN:

Команда	Описание
show protocol-vlan *! В Admin режиме*	Вывод информации о protocol-VLAN

16.4.2 Пример конфигурации Protocol-VLAN

Сценарий:

Требуется все PPPoE пакеты (Ethertype 0x8863 и 0x8864) приходящие на порт ge1 помещать в VLAN 100, остальные пакеты назначать в VLAN 200.

Конфигурация будет выглядеть следующим образом:

```
switch#configure terminal
switch(config)#vlan 100,200
switch(config)#protocol-vlan group 1 mode ethernet etype 0x8863
switch(config)#protocol-vlan group 1 mode ethernet etype 0x8863
switch(config)#int ge1
switch(config-if)#switchport protocol-vlan group 1 vlan 100
switch(config-if)#switchport protocol-vlan group 2 vlan 100
switch(config-if)#switchport mode hybrid
switch(config-if)#switchport hybrid allowed vlan 100 untag
switch(config-if)#switchport hybrid native vlan 200
switch(config-if)#end
```

17. BPDU-Tunnel

BPDU-Tunnel - это функционал, позволяющий передавать служебный трафик протоколов канального уровня без изменений. Функционал может быть полезен, например, при подключении географически распределенной корпоративной сети через L2-каналы оператора. В этом случае трафик служебных протоколов, таких как STP, может помешать нормальной работе коммутаторов оператора и наоборот. BPDU-Tunnel позволяет передавать такие кадры прозрачно для коммутатора оператора.

Для этого, на портах со включенным BPDU-Tunnel, у пакетов определенных протоколов заменяется DST-MAC на специальный multicast-mac и отправляется во все порты в Vlan. И наоборот, при получении коммутатором пакета со специальным multicast-mac, он заменяется на DST-MAC протокола.

Например, при получении STP BPDU со стандартным MAC 01:80:C2:00:00:00 на порт с включенным BPDU-Tunnel, mac заменяется на 01-00-0c-cd-00-02 и пакет отправляется во все порты, и наоборот, при получении пакета с DST-MAC 01-00-0c-cd-00-02 на любом порту, MAC меняется на 01:80:C2:00:00:00 и отправляется в порт со включенным BPDU-Tunnel.

17.1 Конфигурация BPDU-Tunnel

1. Настройка BPDU-Tunnel:

Команда	Описание
bpdu-tunnel-protocol {stp | gvrp | dot1x | user-defined-protocol <name> protocol-mac <mac> } {group-mac <mac> | default-group-mac}	Включить BPDU-Tunnel для протоколов STP, GVRP, Dot1x или протокола задаваемого пользователем. Команда позволяет выбрать MAC-адрес группы на который будет заменен оригинальный MAC-адрес. **protocol-mac** <mac> - оригинальный MAC-адрес протокола; **default-group-mac** - MAC-адрес по умолчанию (01-00-0c-cd-00-02); **group-mac <mac>** - назначить MAC-адрес группы вручную (любой мультикаст MAC-адрес).
no bpdu-tunnel-protocol {stp | gvrp | dot1x | user-defined-protocol <name> } *! В режиме глобальной конфигурации*	Выключить BPDU-Tunnel для протоколов STP, GVRP, Dot1x или протокола, задаваемого пользователем.

2. Включение BPDU-Tunnel на порте:

Команда	Описание
bpdu-tunnel-protocol {stp | gvrp | dot1x | user-defined-protocol <name> }	Включить на порте BPDU-Tunnel для протоколов STP, GVRP, Dot1x или протокола, задаваемого пользователем.
no bpdu-tunnel-protocol { stp | gvrp | dot1x | user-defined-protocol <name> }	Выключить на порте BPDU-Tunnel для протоколов STP, GVRP, Dot1x или протокола, задаваемого пользователем.
! В режиме конфигурации порта	

17.2 Пример конфигурации BPDU-Tunnel

Как показано на рисунке 8, оператор предоставляет клиенту L2 VLAN для соединения географически удаленных филиалов через коммутаторы PE1 и PE2. В свою очередь, клиент использует коммутаторы CE1 и CE2 для подключения к сети оператора. В своей сети клиент использует для резервирования протокол STP и LLDP. Необходимо настроить BPDU-tunnel для корректной передачи BPDU STP и LLDP из сети клиента по сети оператора.

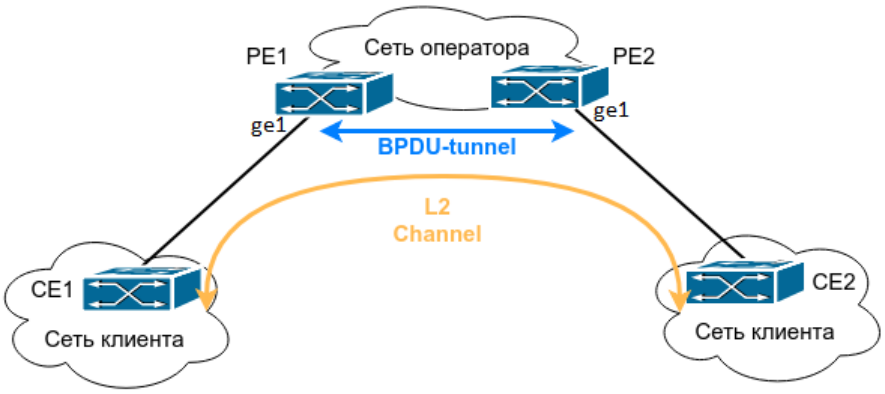

Рис. 8: BPDU-Tunnel

Конфигурация коммутатора PE1:

```
switch(config)#bpdu-tunnel-protocol stp default-group-mac
switch(config)#bpdu-tunnel-protocol user-defined-protocol LLDP protocol-mac
01-80-c2-00-00-0e group-mac 11-11-11-11-11-11
switch(config)#interface ge1
switch(config-if)#bpdu-tunnel-protocol stp
switch(config-if)#bpdu-tunnel-protocol user-defined-protocol LLDP
switch(config-if)#end
```

Конфигурация коммутатора PE2:

```
switch(config)#bpdu-tunnel-protocol stp default-group-mac
switch(config)#bpdu-tunnel-protocol user-defined-protocol LLDP protocol-mac
01-80-c2-00-00-0e group-mac 11-11-11-11-11-11
switch(config)#interface ge1
switch(config-if)#bpdu-tunnel-protocol stp
switch(config-if)#bpdu-tunnel-protocol user-defined-protocol LLDP
switch(config-if)#end
```

После применения данной конфигурации будет происходить следующее:

1. При получении кадра протокола канального уровня коммутатор инкапсулирует пакет, а именно заменяет MAC-адрес назначения на конкретный multicast MAC-адрес (по умолчанию 01-00-0c-cd-00-02) и отправляет дальше по сети;

2. На другом конце сети кадр деинкапсулируется, MAC-адрес назначения 01-00-0c-cd-00-02 меняется на оригинальный.

18. Q-in-Q (Double VLAN)

Функция Q-in-Q, также известная как Double VLAN, соответствует стандарту IEEE 802.1ad, который является расширением стандарта IEEE 802.1Q. Она позволяет добавлять в маркированные кадры Ethernet второй тег IEEE 802.1Q.

Внешний тег VLAN называется Service VID или SVID, внутренний VLAN - Customer VID или CVID.

Для корректной работы QinQ, порт коммутатора со включенным dot1q-tunnel selective должен быть в режиме hybrid. SVID vlan должны быть разрешены в режиме untag.

18.1 Настройка Q-in-Q

Selective QinQ - это функционал, позволяющий тегировать пакеты внешним тегом VLAN (SVID) в зависимости от внутреннего тега VLAN (CVID) в соответствии с требованиями пользователя. Это позволяет выбирать каналы передачи для разных типов трафика с разным тегом VLAN.

1. Включение функции selective QinQ

Команда	Описание
dot1q-tunnel selective enable	Включить на интерфейсе функцию Selective QinQ.
no dot1q-tunnel selective enable	Выключить на интерфейсе функцию Selective QinQ.
! В режиме конфигурации порта	

2. Настройка правил сопоставления внешнего тэга внутреннему

Команда	Описание
dot1q-tunnel selective s-vlan <SVID> **c-vlan** <CVID-LIST>	Создать правило для QinQ. **<SVID>** - внешний тэг Vlan; **<CVID-LIST>** - список CVID, к которым будет добавляться <SVID>.
no dot1q-tunnel selective s-vlan <SVID>	Удалить правило QinQ для <SVID>.
! В режиме конфигурации порта	

3. Настройка использования для s-vlan дополнительного TPID:

Команда	Описание
dot1q-tunnel tpid {0x8100 | 0x9100 | 0x88a8}	Установить TPID 0x8100, 0x88A8 или 0x9100 для пакетов с двумя тегами.
no dot1q-tunnel tpid	Вернуть значение по умолчанию - 0x8100.
! В режиме глобальной конфигурации	

4. Просмотр правил для QinQ на интерфейсах.

Команда	Описание
show dot1q-tunnel	Вывод информации о созданных правилах для QinQ на интерфейсах.
! В Admin режиме	

18.2 Пример конфигурации Q-in-Q

Сценарий 1: Реализовать port-based QinQ. На все пакеты приходящие в порт ge3 должен добавляться SVID 10.

Конфигурация будет выглядеть следующим образом:

```
switch(config)#int ge3
switch(config-if)#dot1q-tunnel selective enable
switch(config-if)#dot1q-tunnel selective s-vlan 10 c-vlan 1-4094
switch(config-if)#switchport mode hybrid
switch(config-if)#switchport hybrid allowed vlan add 10 untag
switch(config-if)#end
```

Сценарий 2: Для пакетов приходящих в порт ge3 с Vlan 15, 35 - 40 должен добавляться SVID 10, а для диапазона Vlan 100 - 150 добавляться SVID 15. На пакеты с Vlan 1000 и Vlan 1001 внешний тэг добавляться не должен.

Конфигурация будет выглядеть следующим образом:

```
switch(config)#int ge3
switch(config-if)#dot1q-tunnel selective enable
switch(config-if)#dot1q-tunnel selective s-vlan 10 c-vlan 15, 35-40
switch(config-if)#dot1q-tunnel selective s-vlan 15 c-vlan 100-150
switch(config-if)#switchport mode hybrid
switch(config-if)#switchport hybrid allowed vlan add 1000,1001 tag
switch(config-if)#switchport hybrid allowed vlan add 10,15 untag
switch(config-if)#end
```

19. VLAN-translation

VLAN-translation - это функция, которая позволяет преобразовать тег VLAN пакета в новый, в соответствии с требованиями. Это позволяет обмениваться данными в разных VLAN. VLAN-translation может быть использован на обоих направлениях трафика.

19.1 Настройка VLAN-translation

1. Включение функции VLAN-translation на порте:

Команда	Описание
vlan-translation enable **no vlan-translation enable** *! В режиме конфигурации порта*	Включить трансляцию VLAN на порте. Выключить трансляцию VLAN на порте.

2. Создание соответствий VLAN-translation на порте:

Команда	Описание
vlan-translation <old-vlan-id> **to** <new-vlan-id> {**in** | **out**} **no vlan-translation** <old-vlan-id> {**in** | **out**} *! В режиме конфигурации порта*	Включить на порте преобразование тега **<old-vlan-id>** в новый **<new-vlan-id>**. **in** - для входящих на порт пакетов (для корректной работы на порте должен быть разрешен <new-vlan-id>); **out** - исходящих с порта пакетов (для корректной работы на порте должен быть разрешен <old-vlan-id>). Выключить трансляцию VLAN на порте.

3. Отображение настроек VLAN-translation:

Команда	Описание
show vlan-translation *! В Admin режиме*	Просмотр сконфигурированных соответствий трансляции VLAN.

19.2 Пример конфигурации VLAN-translation

Сценарий: На рисунке 9 изображена топология с применением VLAN-translation. Пограничные коммутаторы PE1 и PE2 Интернет-провайдера поддерживают VLAN 20 для передачи трафика между CE1 и CE2 из клиентской сети через собственный Vlan 3. Порт ge1 PE1 подключен к CE1 в VLAN 20, порт ge10 подключен к публичной сети в VLAN 3, порт ge1 PE2 подключен к CE2 в VLAN 20, порт ge10 подключен к публичной сети в VLAN 3.

Конфигурация коммутаторов PE1 и PE2 будет выглядеть следующим образом:

```
switch(config)#vlan 3,20
switch(config)#interface ge1
switch(config-if)#switchport mode trunk
switch(config-if)#vlan-translation enable
switch(config-if)#vlan-translation 20 to 3 in
switch(config-if)#vlan-translation 3 to 20 out
switch(config-if)#exit
switch(config)#interface ge10
switch(config-if)#switchport mode trunk
switch(config-if)#end
```

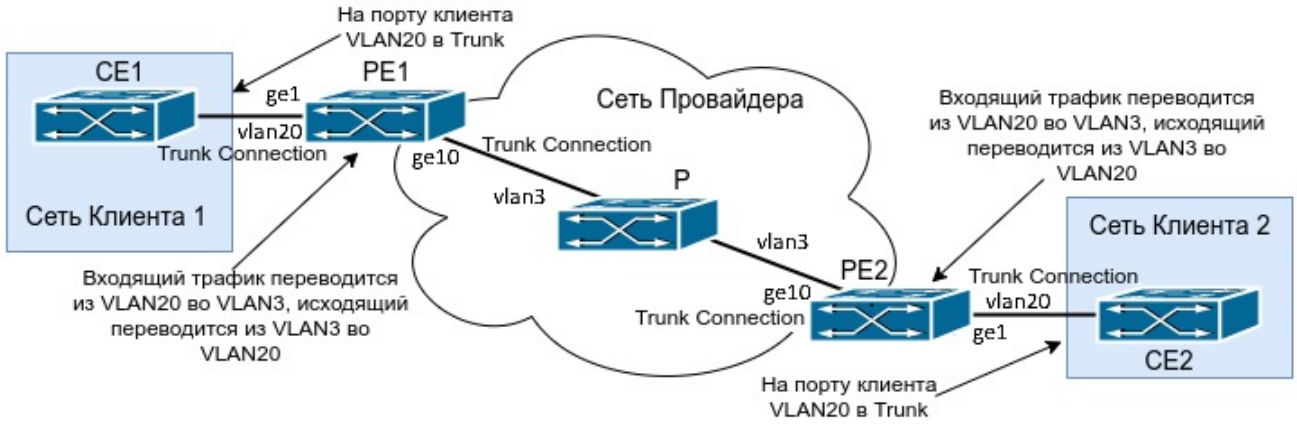

Рис. 9: Топология с применением VLAN-translation

20. STP, RSTP, MSTP

20.1 Общие сведения о STP, RSTP и MSTP

STP - Spanning Tree Protocol (протокол покрывающего дерева) - протокол канального уровня, разработанный в 1985 году и описан в стандарте IEEE 802.1D. Основной его задачей является защита от петель в топологии сети Ethernet, в которой присутствует одно или несколько избыточных соединений. Наличие таких соединений в сети с коммутатором без использования протоколов защиты, приводит к тому, что широковещательные и многоадресные кадры в большинстве случаев передаются бесконечно повторяясь, в результате чего пропускная способность сети оказывается практически полностью занята бесполезными повторами.

STP автоматически блокирует те соединения, которые в данный момент являются избыточными для полной связности коммутаторов в сети, тем самым предотвращая возникновение циклических маршрутов передачи кадров.

Принцип работы STP:

1. Один из коммутаторов выбирается в роли Root (корневого).
2. Каждый коммутатор просчитывает кратчайший путь к Root. Тот порт, путь через который является кратчайшим к корневому коммутатору, называется Root port.
3. Для каждого сегмента сети просчитывается кратчайший путь к корневому коммутатору. Мост, через который проходит этот путь, становится назначенным для этой сети (Designated Bridge). Непосредственно подключенный к сети порт моста — назначенным портом.
4. На всех мостах блокируются все порты, не являющиеся корневыми и назначенным.

RSTP (**Rapid Spanning Tree Protocol**) - улучшение STP, разработан в 2001 году и описан в стандарте 802.1w. Принцип работы в целом остается тем же, но ряд внедренных доработок, упрощений, уменьшение времени ожидания событий или отказ от таймеров, позволяет снизить время сходимости топологии с 30-50 секунд (для STP) до 1-6 секунд.

MSTP (Multiple Spanning Tree Protocol) - протокол множественного связующего дерева, в котором создаются независимые экземпляры покрывающего дерева. В один экземпляр MSTP могут входить несколько виртуальных сетей при условии, что их топология одинакова. Минимальное количество экземпляров MSTP соответствует количеству топологически уникальных групп VLAN в домене второго уровня. MSTP налагает важное ограничение: все коммутаторы, участвующие в MSTP, должны иметь одинаково сконфигурированные группы VLAN (**MSTI - Multiple Spanning Tree Instance**), что ограничивает гибкость при изменении конфигурации сети. Соответствия VLAN-MSTI задаются администратором вручную. Формат MSTP BPDU аналогичен RSTP BPDU. Для снижения нагрузки на коммутаторы, все BPDU различных MSTI коммутатора объединяются в один BPDU.

Регионы MSTP

Новая концепция вызывала сложности в эксплуатации, так как было необходимо идентично конфигурировать соответствие VLAN-MSTI на всех коммутаторах. Для упрощения и поддержания обратной совместимости с STP и RSTP была разработана концепция регионов. Регион MSTP может быть образован из нескольких смежных коммутаторов с одинаковыми MSID (MST Configuration Identification), состоящими из:

- Имя региона MSTP;
- Ревизия конфигурации;
- Дайджест соответствий VLAN-MSTI.

MSID добавляется к MSTP BPDU так, что сохраняется совместимость с STP и RSTP. При этом MSTP BPDU, отправленные разными коммутаторами одного региона, воспринимаются смежными STP/RSTP-коммутаторами как RSTP BPDU одного коммутатора (рис. 10). Таким образом кольцевая топология на разных коммутаторах по-прежнему поддерживается и в регионе MSTP сохраняется гибкость управления трафиком.

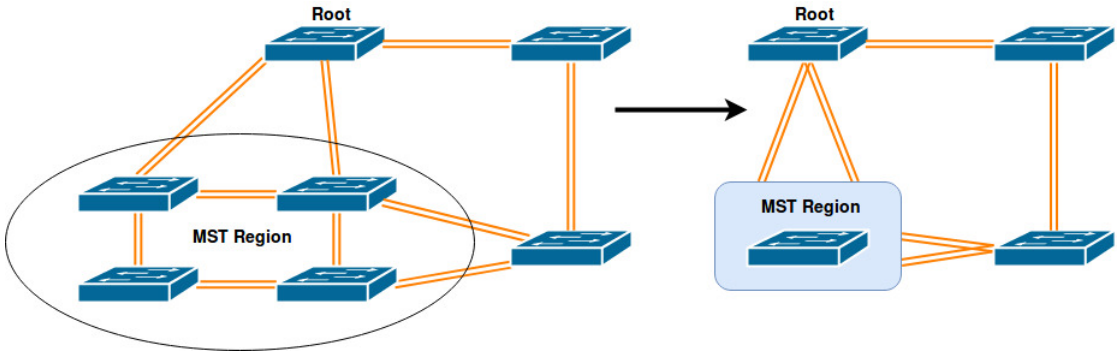

Рис. 10: Регион MST в сети

MSTP внутри региона

Для каждого региона выбирается региональный корневой коммутатор, относительно которого строится внутреннее покрывающее дерево (IST - Internal Spanning Tree), объединяющее все коммутаторы региона. Региональный корневой коммутатор выбирается по наименьшему приоритету коммутатора, а при равных по минимальной стоимости пути до корневого коммутатора всей сети (либо региона, в котором находится корневой коммутатор). Если таких коммутаторов несколько, то среди них выбирается один с наименьшим ID.

MSTP между регионами

Для защиты топологий соединения различных регионов и отдельных коммутаторов строится общее покрывающее дерево (CST - Common Spanning Tree). В качестве корневой коммутатора в CST выбирается коммутатор с наименьшим приоритетом, а при равных с наименьшим ID. Каждый регион MSTP представляется для CST как отдельный виртуальный коммутатор. CST совместно с IST всех регионов формируют полное покрывающее дерево сети (CIST - Common and Internal Spanning Tree).

Балансировка трафика в MSTP

Параметры коммутатора и его портов могут быть изменены для каждого MSTI в отдельности, таким образом трафик разных групп VLAN может быть отправлен по разным путям, распределяя нагрузку по всей сети.

20.2 Конфигурация STP, RSTP и MSTP

1. Выбрать режим Spanning tree:

Команда	Описание
spanning-tree mode {stp | rstp | mstp} *! В режиме глобальной конфигурации*	Выбрать режим spanning-tree. Значение по умолчанию - rstp.

2. Включение или отключение spanning-tree глобально или на порте:

При отключении STP на порте, порт блокирует входящие на него BPDU пакеты. При глобальном отключении STP, BPDU пропускаются коммутатором прозрачно, за исключением портов с отключенным STP.

Команда	Описание
spanning-tree shutdown **no spanning-tree shutdown** *! В режиме глобальной конфигурации*	Отключить глобально функцию spanning-tree. Включить глобально функцию spanning-tree.
spanning-tree disable **spanning-tree enable** *! В режиме конфигурации порта*	Отключить режим spanning-tree на порте. Включить режим spanning-tree на порте.

3. Настройка режимов STP и RSTP.

3.1. Настроить приоритет коммутатора:

Команда	Описание
spanning-tree priority <bridge-priority> **no spanning-tree priority** *! В режиме глобальной конфигурации*	Установить приоритет spanning-tree коммутатора. Установить приоритет по умолчанию.

3.2. Настроить параметры порта:

Команда	Описание
spanning-tree path-cost <cost> **no spanning-tree path-cost** *! В режиме конфигурации порта*	Установить стоимость пути через порт spanning-tree. Отменить установку стоимости пути через порт spanning-tree.
spanning-tree guard root **no spanning-tree guard root** *! В режиме конфигурации порта*	Включить функционал rootguard для порта spanning-tree. Порт с включенным rootguard не может стать root port. Выключить функционал rootguard для порта spanning-tree

3.3. Настроить таймеры:

Команда	Описание
spanning-tree forward-time <time> **no spanning-tree forward-time** *! В режиме глобальной конфигурации*	Установить значение таймера Bridge_Forward_Delay для коммутатора. **Bridge_Forward_Delay** - таймер перехода порта из статуса blocking в forwarding. Отменить установку таймера Bridge_Forward_Delay.
spanning-tree hello-time <time> **no spanning-tree hello-time** *! В режиме глобальной конфигурации*	Установить значение таймера Bridge_Hello_Time для коммутатора. **Bridge_Hello_Time** - таймер отправки spanning-tree BPDU. Отменить установку таймера Bridge_Hello_Time.
spanning-tree max-age <time>	Установить значение таймера Bridge_Max_Age для коммутатора. **Bridge_Max_Age** - таймер времени жизни лучшего полученного spanning-tree BPDU.

Команда	Описание
no spanning-tree max-age *! В режиме глобальной конфигурации*	Отменить установку таймера Bridge_Max_Age.
spanning-tree max-hops <hop-count> **no spanning-tree max-hops** *! В режиме глобальной конфигурации*	Установить значение счетчика Max_Hop, который определяет какое количество коммутаторов может пройти BPDU, до того как будет отброшен. Отменить установку счетчика Max_Hop.

3.4. Включить механизмы ускорения сходимости:

Команда	Описание
spanning-tree link-type {auto | point-to-point | shared} **no spanning-tree link-type** *! В режиме конфигурации порта*	Выбор механизма определения типа подключенной к порту сети. **auto** - автоматическое определение типа соединения; **point-to-point** - всегда point-to-point; **shared**- всегда shared. Восстановить значение по умолчанию (auto).
spanning-tree portfast **no spanning-tree portfast** *! В режиме конфигурации порта*	Включение механизма portfast определяющего порт spanning-tree как граничный. Выключение механизма portfast определяющего порт spanning-tree как граничный.

3.5. Включить механизмы защиты топологии:

Команда	Описание
spanning-tree {bpdu-filter | bpdu-guard} {enable | disable }	Включить механизм защиты от нежелательных BPDU. **bpdu-filter** - отбрасывает поступающие на порт BPDU; **bpdu-guard** - отключает порт при получении BPDU.

Команда	Описание
no spanning-tree {bpdu-filter | bpdu-guard} *! В режиме конфигурации порта*	Отключить механизм защиты от нежелательных BPDU.
spanning-tree restricted-tcn **no spanning-tree restricted-tcn** *! В режиме конфигурации порта*	Игнорировать флаг TC из BPDU, полученного с этого порта, а также запретить его добавление в BPDU транслируемый дальше. Отменить установленную функцию.
spanning-tree restricted-role **no spanning-tree resticted-role** *! В режиме конфигурации порта*	Запретить порту становиться root портом. Отменить установленную функцию.

4. Настройка режима MSTP.

4.1. Конфигурация MSTI:

Команда	Описание
spanning-tree mst configuration *! В режиме глобальной конфигурации*	Войти в режим конфигурирования MST.
region <name> **no region** *! В режиме конфигурирования MST*	Задать имя региона. Удалить имя региона.
revision <0-65535> *! В режиме конфигурирования MST*	Установить уровень ревизии для региона. Значение по умолчанию - 0.
instance <1-63> **vlan** <vlan-id> **no instance** <1-63> vlan [<vlan-id>] *! В режиме конфигурирования MST*	Установить соответствие VLAN-MSTI. Удалить instance целиком или Vlan.

4.2. Настройка приоритета instance глобально:

Команда	Описание
spanning-tree instance <1-63> **priority** <0-61440>	**priority** <0-61440> - установить приоритета instance с шагом 4096 (чем меньше значение, тем выше приоритет).
no spanning-tree instance <1-63> **priority**	Отменить установку приоритета.
! В режиме глобальной конфигурации	

4.3. Настрока instance на порте:

Команда	Описание
spanning-tree instance <1-63> {path-cost <1-20000000> | priority <0-240> | restricted-role}	**path-cost** <1-20000000> - задать стоимость пути; **priority** <0-240> - установить приоритет порта spanning-tree в указанном MSTI; **restricted-role** - включить ограничение роли порта, (порт не может стать корневым).
no spanning-tree instance <1-63> {path-cost | restricted-role}	Отменить установленные действия.
! В режиме конфигурации порта	

5. Просмотр настроек spanning-tree:

Команда	Описание
show spanning-tree [brief | interface <ifname> | mst [config | detail [interface <ifname>] | instance <1-63> [interface <ifname>] | interface <ifname> | statistics [interface <ifname> [instance <1-63>]]]	Отобразить информацию о состоянии протокола.
! В Admin режиме	

20.3 Пример конфигурации MSTP

На всех коммутаторах в сети (рисунок 11) включен spanning-tree в режиме MSTP. Все праметры spanning-tree установлены по умолчанию и равны.

По умолчанию MSTP формирует древовидную топологию, растущую из SW1, блокируя избыточные соединения. Порты с пометкой X переведены в состояние blocking, остальные в состоянии forwarding.

Имя коммутатора	SW1	SW2	SW3	SW4
MAC-адрес коммутатора	...00-00-01	...00-00-02	...00-00-03	...00-00-04
Приоритет коммутатора	32768	32768	32768	32768
Приоритет порта 1	128	128	128	
Приоритет порта 2	128	128	128	
Приоритет порта 3		128	128	
Приоритет порта 4		128		128
Приоритет порта 5		128		128
Приоритет порта 6			128	128
Приоритет порта 7			128	128
Стоимость пути 1	200000	200000	200000	
Стоимость пути 2	200000	200000	200000	
Стоимость пути 3		200000	200000	
Стоимость пути 4		200000		200000
Стоимость пути 5		200000		200000
Стоимость пути 6			200000	200000
Стоимость пути 7			200000	200000

Ниже представлена конфигурация коммутаторов по умолчанию.

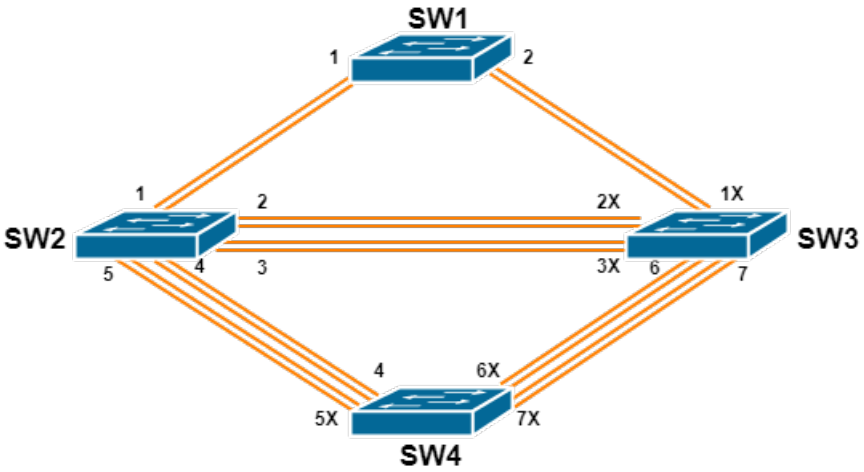

Рис. 11: Пример сети с кольцевой топологией

Сконфигурировать сеть:

1. Сконфигурировать VLAN:
   - Создать VLAN 20, 30, 40, 50 на коммутаторах SW2, SW3 и SW4;

- Перевести порты 1-7 коммутаторов SW2, SW3 и SW4 в режим trunk.

2. Сконфигурировать MSTP:
   - Определить коммутаторы SW2, SW3 и SW4 в регион MSTP;
   - Установить соответствие VLAN 20 и 30 - MSTI 3;
   - Установить соответствие VLAN 40 и 50 - MSTI 4.
3. Распределить нагрузку, определив корневые коммутаторы для каждого MSTI:
   - Установить приоритет коммутатора SW3 равным 0 в MSTI 3;
   - Установить приоритет коммутатора SW4 равным 0 в MSTI 4.

Конфигурация SW2:

```
SW2(config)#vlan 20,30,40,50
SW2(config)#spanning-tree mst configuration
SW2(config-mst)#region sw2-sw3-sw4
SW2(config-mst)#instance 3 vlan 20,30
SW2(config-mst)#instance 4 vlan 40,50
SW2(config-mst)#exit
SW2(config)#interface ge1-7
SW2(config-if)#switchport mode trunk
```

Конфигурация SW3:

```
SW3(config)#vlan 20,30,40,50
SW3(config)#spanning-tree mst configuration
SW3(config-mst)#region sw2-sw3-sw4
SW3(config-mst)#instance 3 vlan 20,30
SW3(config-mst)#instance 4 vlan 40,50
SW3(config-mst)#exit
SW3(config)#interface ge1-7
SW3(config-if)#switchport mode trunk
SW3(config-if)#exit
SW3(config)#spanning-tree instance 3 priority 0
```

Конфигурация SW4:

```
SW4(config)#vlan 20,30,40,50
SW4(config)#spanning-tree mst configuration
SW4(config-mst)#region sw2-sw3-sw4
SW4(config-mst)#instance 3 vlan 20,30
SW4(config-mst)#instance 4 vlan 40,50
SW4(config-mst)#exit
SW4(config)#interface ge1-7
SW4(config-if)#switchport mode trunk
SW4(config-if)#exit
SW4(config)#spanning-tree instance 4 priority 0
```

После применения описанной конфигурации коммутатор SW1 остается корневым для MST 0 всей сети. В регионе sw2-sw3-sw4 коммутатор SW2 становится региональным корневым для MSTI 0, SW3 - для MSTI 3, SW4 - для MSTI 4.

MSTP генерирует топологии для MSTI 0, MSTI 3, и MSTI 4 (см. рис. 12, 13, 14). Порты с пометкой X переведены в состояние blocking, остальные в состоянии forwarding.

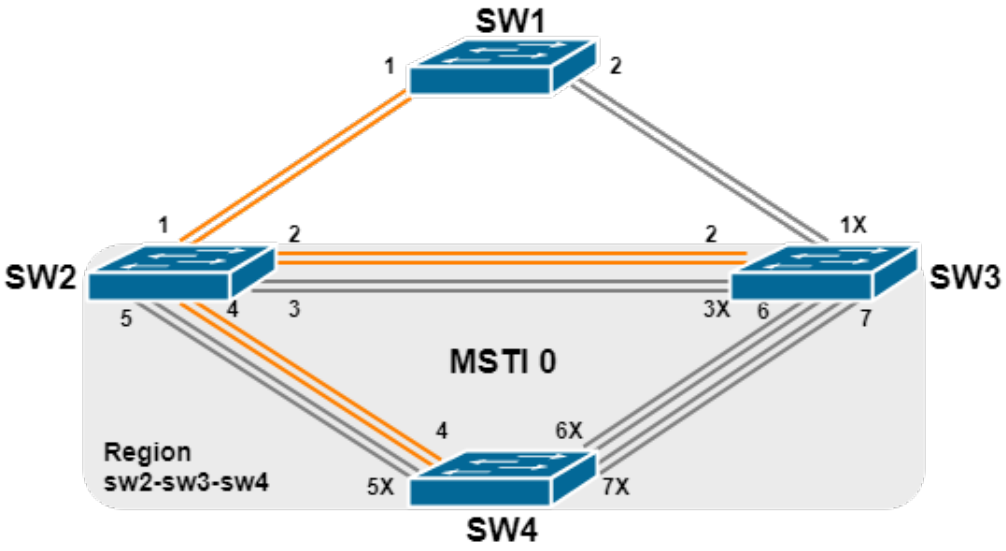

Рис. 12: Топология MSTI 0

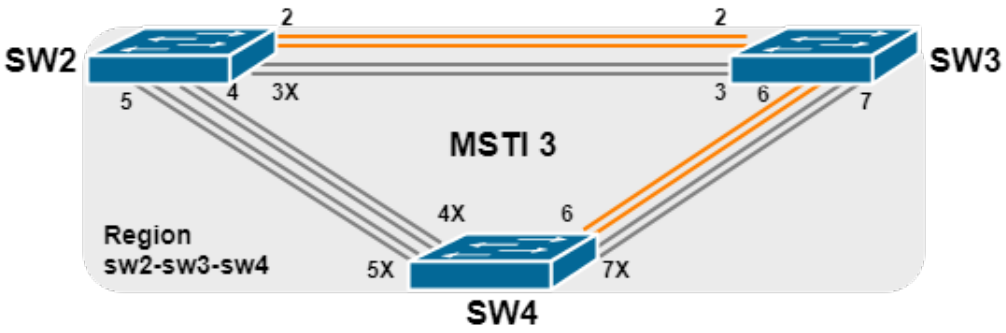

Рис. 13: Топология MSTI 3

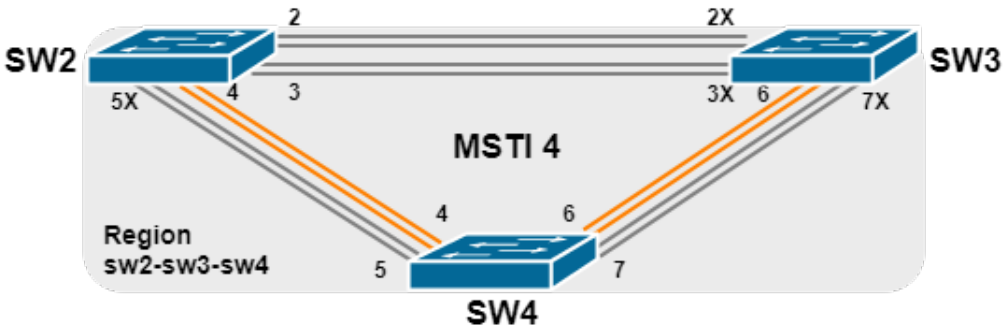

Рис. 14: Топология MSTI 4

20.4 Решение проблем при конфигурации RSTP/MSTP

Для включения RSTP/MSTP на порту, RSTP/MSTP должен быть включен глобально.

Параметры RSTP/MSTP взаимосвязаны и следует соблюдать следующие соответствия, иначе RSTP/MSTP может работать некорректно:

```
2 x (Bridge_Forward_Delay - 1 sec) >= Bridge_Max_Age
Bridge_Max_Age >= 2 x (Bridge_Hello_Time + 1 sec)
```

Нужно всегда помнить, что изменение параметров RSTP/MSTP может вызвать изменение топологии.

21. Качество сервиса (QoS)

QoS (Quality of Service) - это набор возможностей, которые позволяют логически разделять проходящий по сети трафик на основании критериев и управлять качеством каждого типа трафика, обеспечивая лучший сервис для выбранного трафика. QoS обеспечивает гарантию предсказуемого сервиса передачи данных для выполнения требований программ. QoS не генерирует дополнительную полосу, но обеспечивает более эффективное управление существующей пропускной способностью в соответствии с требованиями приложений и политикой управления сетью.

21.1 Термины QoS

QoS: Quality of Service, качество сервиса, обеспечивает гарантию предсказуемого сервиса передачи данных для выполнения требований программ.

Домен QoS: сетевая топология, сформированная устройствами, поддерживающими QoS для обеспечения качества сервиса.

CoS: Class of Service, информация о классификации, передаваемая на 2 уровне модели OSI в **подзаголовке** 802.1Q заголовка Ethernet-кадра. CoS занимает 3 бита, поэтому может принимать значения от 0 до 7.

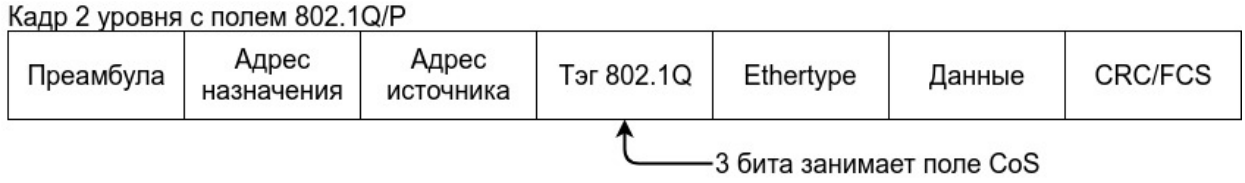

Рис. 15: Поле CoS

ToS: Type of Service, однобайтовое поле в составе заголовка пакета IPv4, используется для обозначения типа сервиса IP-пакетов. Может содержать DSCP и IP-precedence.

Рис. 16: Поле DSCP

IP precedence: информация о классификации, передаваемая в IPv4 заголовке 3 уровня (поле ToS). Занимает 3 бита, поэтому может принимать значения от 0 до 7.

DSCP: Differentiated Services Code Point**,** информация о классификации, передаваемая в IPv4 заголовке 3 уровня (поле ToS). Занимает 6 бит, поэтому может принимать значения от 0 до 63. Поле пересекается с IP Precedence, но совместимо с ним.

Classification (классификация): классификация отдельных пакетов в трафике в соответствии с информацией о классификации, передаваемой в заголовке пакета или на основании списков контроля доступа (ACL).

Policing (управление полосой пропускания): действие механизма QoS на входе, которое устанавливает политику для полосы трафика и управляет классифицированными пакетами.

Remark (перемаркировка): действие механизма QoS на входе, выполняющее перемаркировку пакета в соответствии с настроенной политикой.

Scheduling (управление очередями): действие механизма QoS на выходе, которое принимает решение о передаче или сбросе пакетов, в зависимости от настройки очереди в которую помещен пакет.

21.2 Реализация QoS

Спецификации передачи IP-пакетов охватывают адресацию и сервисы источника и получателя трафика, а также описывают механизм правильной передачи пакетов с использованием протоколов уровня 4 модели OSI (например TCP). В большинстве случаев IP использует максимально возможную пропускную способность вместо механизма защиты полосы пропускания. Это приемлемо для таких сервисов, как электронная почта или FTP, но для постоянно растущих объемов мультимедийных сервисов этот метод не может удовлетворить требования необходимой пропускной способности и низких задержек.

Используя различные методы, QoS определяет приоритет для каждого входящего пакета. Информация о классификации содержится в заголовке IP-пакета 3-го уровня или в заголовке кадра 802.1Q уровня 2. QoS обеспечивает одинаковый сервис для пакетов с одинаковым приоритетом, в то же время для пакетов с разным приоритетом сервис может обеспечиваться разный. Коммутатор или маршрутизатор с поддержкой QoS может обеспечивать различную пропускную способность в соответствии с информацией о классификации, помечать трафик в соответствии с настроенной политикой, а также сбрасывать некоторые пакеты с низким приоритетом в случае нехватки полосы пропускания. QoS может быть сконфигурирован гибко: степень сложности зависит от топологии сети и глубины анализа трафика.

21.3 Базовая модель QoS

Базовая модель QoS (рисунок 19.3) состоит из 4 частей: **Classification** (классификация) и **Policing** (управление полосой пропускания) - действия на входе, **Remark** (перемаркировка) и **Scheduling** (планирование) - действие на выходе. На схеме ниже изображена базовая модель QoS.

Classification (классификация). Классифицирует трафик в соответствии с классификационной информацией пакетов и определяет номер исходящей очереди в которую будет помещен пакет. В зависимости от типов пакетов и настроек коммутатора классификация обеспечивается различным образом. Схема ниже показывает процесс классификации (рисунок 18).

Рис. 17: Базовая модель QoS

Policing (управление полосой пропускания). Может выполняться на потоке данных с целью выделения полосы классифицированному трафику в соответствии с настроенной политикой.

Remark (перемаркировка). Позволяет заменить оригинальное значение DSCP и CoS кадра.

Scheduling (работа с очередями и планирование). Коммутатор принимает решение о передаче или сбросе пакета на основе настроек очередей и заполненности буфера.

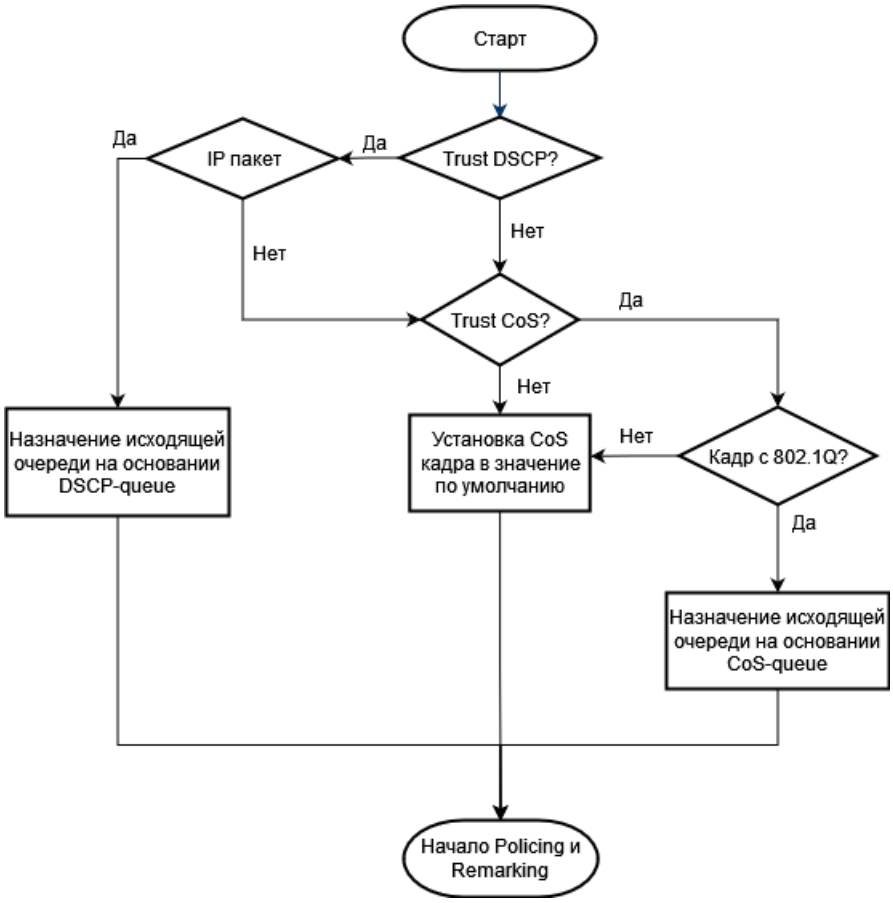

Рис. 18: Процесс классификации пакетов

21.4 Конфигурация QoS

1. Настройка глобальных параметров:

Команда	Описание
mls qos queue weight <w0> <w1> <w2> <w3> <w4> <w5> <w6> <w7>	Изменить веса очередей по умолчанию. **<w1> ... <w7>** - вес <0-127>. Вес 0 переключает очередь в режим Strict-priority.
no mls qos queue weight	Вернуть значения веса очередей по умолчанию - 1 2 3 4 5 6 7 8.
! В режиме глобальной конфигурации	

2. Настройка карты преобразований CoS:

Команда	Описание
mls qos map cos-queue <q0> <q1> <q2> <q3> <q4> <q5> <q6> <q7>	Задать соответствие номера очереди и значения CoS. **<q0>** - номер очереди <0-7> для CoS 0 **<q1>** - номер очереди <0-7> для CoS 1 ... **<q7>** - номер очереди <0-7> для CoS 7
no mls qos map cos-queue	Вернуть значения по умолчанию - 0 1 2 3 4 5 6 7.
! В режиме глобальной конфигурации	

3. Настройка карты преобразований DSCP:

Команда	Описание
mls qos map dscp-queue <DSCP1> [<DSCP2> [... [<DSCP8>]]] to <queue>	Задать соответствие номера очереди и значения DSCP. **<DSCP>** - значение DSCP <0-63>; **<queue>** - номер очереди <0-7>.
no mls qos map dscp-queue	Вернуть значения по умолчанию: <DSCP0-7> - 0, <DSCP8-15> - 1, <DSCP16-23> - 2, <DSCP24-31> - 3, <DSCP32-39> - 4, <DSCP40-47> - 5, <DSCP48-55> - 6, <DSCP56-63> - 7.
! В режиме глобальной конфигурации	

4. Настройка QoS на портах:

Команда	Описание
mls qos queue weight <w0> <w1> <w2> <w3> <w4> <w5> <w6> <w7> **no mls qos queue weight** *! В режиме конфигурации порта*	Установить вес очередей на физическом порте. **<w1> ... <w7>** - вес <0-127>. Вес 0 переключает очередь в режим Strict-priority. Вернуть значения веса очередей по умолчанию - 1 2 3 4 5 6 7 8.
mls qos trust cos **no mls qos trust cos** *! В режиме конфигурации порта*	Задать доверие метке cos для входящего трафика на интерфейсе. Отменить доверие метке cos для входящего трафика на интерфейсе.
mls qos trust dscp **no mls qos trust dscp** *! В режиме конфигурации порта*	Задать доверие метке cos для входящего трафика на интерфейсе. Отменить доверие метке cos для входящего трафика на интерфейсе.
mls qos default-cos <0-7> **no mls qos default-cos** *! В режиме конфигурации порта*	Задать значение COS для входящего в интерфейс трафика без метки. Удалить значение COS для входящего в интерфейс трафика без метки.

5. Просмотр карты CoS:

Команда	Описание
show mls qos maps cos-queue *! В Admin режиме*	Отобразить карту CoS - Очередь.

6. Просмотр карты DSCP:

Команда	Описание
show mls qos maps dscp-queue *! В Admin режиме*	Отобразить карту DSCP - Очередь.

7. Просмотр настроек QoS на интерфейсе:

Команда	Описание
show mls qos interface <ifname> *! В Admin режиме*	Отобразить настройки QoS и информацию о весе очередей на физическом интерфейсе.

21.4.1 Пример конфигурации QoS

Пример 1:

Необходимо приоритезировать мультикаст трафик, имеющий CoS 2 и повысить приоритет для трафика с CoS 3 (VOIP). За портом ge1 находится клиент с IPTV, за портом ge2 - клиент с VOIP, порт XE1 - uplink.

Конфигурация коммутатора будет выглядеть следующим образом:

```
Switch#configure terminal
Switch(config)#interface xe1
Switch(config-if)#mls qos trust cos
Switch(config-if)#mls qos queue weight 1 2 20 4 5 6 7 8
Switch(config-if)#exit
Switch(config)#interface ge1
Switch(config-if)#mls qos queue weight 1 0 3 4 5 6 7 8
Switch(config-if)#exit
Switch(config)#interface ge2
Switch(config-if)#mls qos queue weight 1 2 20 4 5 6 7 8
Switch(config-if)#mls qos default-cos 3
Switch(config-if)#end
```

21.4.2 Решение проблем при настройке QoS

При одновременном доверии меткам **CoS** и **DSCP**, приоритет **DSCP** выше.

21.5 Настройка приоритета 802.1p для control-plane пакетов

1. Установка приоритета 802.1p для всех пакетов, отправляемых с VLAN интерфейса:

Команда	Описание
cos <0-7>	Включить присвоение приоритета 802.1p пакетам VLAN интерфейса.
no cos	Отключить присвоение приоритета 802.1p пакетам VLAN интерфейса.
! В режиме конфигурации interface vlan	

2. Установка приоритета 802.1p для IGMP-пакетов в VLAN:

Команда	Описание
igmp snooping cos <0-7>	Включить присвоение приоритета 802.1p IGMP пакетам в VLAN со включенным IGMP Snooping.
no igmp snooping cos	Отменить присвоение приоритета 802.1p IGMP пакетам.
! В режиме глобальной конфигурации	

21.6 Policy-map

Policy-map (карта политик) - позволяет связать политики, такие как ограничение полосы, изменение меток CoS или DSCP, с картами классов, тем самым применив их к различным потокам данных.

Class-map (карта классов) используются для задания критериев, на основе которых сетевой трафик будет группироваться в классы. Критерии могут задаваться на основе ACL, меток CoS или VLAN ID для классификации потока данных.

После того как командой class-map заданы классы трафика и их критерии, командой policymap задается политика работы с классами, а команда **service-policy** привязывает политику к интерфейсу.

21.6.1 Настройка Policy-map

1. Настройка карты классов:

Команда	Описание
class-map <class-map-name>	Создать карту классов с именем <class-map-name> и войти в режим её конфигурирования.

Команда	Описание
no class-map <class-map-name> *! В режиме глобальной конфигурации*	Удалить карту классов с именем <class-map-name>.
match {access-group <acl-index> | cos <cos-list> | vlan <vlan- list>} **no match** {access-group | cos | vlan} *! В режиме конфигурации карты классов*	Настроить критерий соответствия данных карте классов на основе: **access-group** <acl-index> - 1-199, 1300-2699; **cos** <cos-list> - 0-7; **vlan** <vlan-list> - 1-4094. Удалить критерий соответствия.

2. Настройка карты политик:

Команда	Описание
policy-map <policy-map-name> **no policy-map** <policy-map-name> *! В режиме глобальной конфигурации*	Создать карту политик с именем <policy-map- name> и войти в режим её конфигурирования. Удалить карту политик с именем <policy-map-name>.
class <class-map-name> **no class** <class-map-name> *! В режиме конфигурации карты политик*	Задать для текущей карты политик ассоциацию с картой классов с именем <class-map-name>. Отменить ассоциацию.
set {cos <new-cos> | ip-dscp <new-dscp> | ip-precedence <new-precedence> | ip-tos <new-tos> | queue <new-queue> | s-vid <1-4094> [cos <0-7>]}	Присвоить классифицированному трафику новое значение: **cos** <new-cos> - 0-7; **ip-dscp** <new-dscp> - 0-63; **ip-precedence** <new-precedence> - 0-7; **ip-tos** <new-tos> - 0-255; **queue** <new-queue> - 0-7; **s-vid** <1-4094> [**cos** <0-7>] - VLAN тег и опционально CoS.

Команда	Описание
no set {cos | ip-dscp | ip-precedence | ip-tos | queue | s-vid} *! В режиме конфигурации карты классов в карте политик*	Отменить присвоение нового значения.
police <CIR> <CBS> **no police** <CIR> <CBS> *! В режиме конфигурации карты классов в карте политик*	Задать ограничение скорости. **<CIR>** - 1-10000000 Kbits/sec; **<CBS>** - 0-16000 Kbyte. CIR (Committed Information Rate) — гарантированная скорость передачи данных; CBS (Committed Burst Size) — размер burst. Отменить ограничение скорости.
packet-capture **no packet-capture** *! В режиме конфигурации действия для class-map в policy-map*	Установить действие packet-capture. Совместное использование packet-capture с другими action в policy-map не применимо. Отменить действие packet-capture.

3. Применение карты политик на порте:

Команда	Описание
service-policy input <policy-map-name> **no service-policy input** <policy-map-name> *! В режиме конфигурации порта*	Применить карту политик с именем <policy-map-name> для входящего трафика на порте. Удалить карту политик с именем <policy-map-name> для входящего трафика на порте.

21.6.2 Пример настройки карты политик

Сценарий 1

Установить ACL правило, фильтрующее по MAC и полю ethertype, и устанавливающее метку ip-dscp для трафика приходящего на порт ge1.

Конфигурация коммутатора будет выглядеть следующим образом:

```
Switch(config)#access-list 102 permit mac 0101.0202.0000 0000.0000.FFFF
0133.2222.1100 0000.0000.00FF 0x806
Switch(config)#class-map c1
Switch(config-cmap)#match access-group 102
Switch(config-cmap)#exit
Switch(config)#policy-map p1
Switch(config-pmap)#class c1
Switch(config-pmap-c)#set ip-dscp 32
Switch(config-pmap-c)#exit
Switch(config-pmap)#exit
Switch(config)#interface ge1
Switch(config-if)#service-policy input p1
Switch(config-if)#end
```

Сценарий 2

Изменение ip precedence в IP-заголовке трафика приходящего в vlan 10 порта ge1.

Конфигурация коммутатора будет выглядеть следующим образом:

```
Switch(config)#class-map c1
Switch(config-cmap)#match vlan 10
Switch(config-cmap)#exit
Switch(config)#policy-map p1
Switch(config-pmap)#class c1
Switch(config-pmap-c)#set ip-precedence 5
Switch(config-pmap-c)#exit
Switch(config-pmap)#exit
Switch(config)#interface ge1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan all
Switch(config-if)#service-policy input p1
Switch(config-if)#end
```

22. L3 интерфейс и маршрутизация

Коммутатор поддерживает не только L2-коммутацию, но и аппаратную L3-маршрутизацию. Коммутатор имеет возможность настройки L3 интерфейсов, а также статических маршрутов.

Интерфейс уровня 3 является не физическим, а логическим интерфейсом на основе VLAN и может содержать один или несколько L2 портов, принадлежащих к этой VLAN, или не содержать L2 портов. Чтобы интерфейс уровня 3 был в состоянии UP, необходимо, чтобы как минимум один порт уровня 2, принадлежащий к этому интерфейсу, был в состоянии UP, иначе интерфейс уровня 3 находится в состоянии DOWN. Коммутатор может использовать IP-адреса настроенные как статически, так и динамически на интерфейсе уровня 3 для связи с другими устройствами через IP-протокол.

Статический маршрут - это маршрут прохождения пакета в сторону подсети назначения через gateway, явно указанный при конфигурации. Статические маршруты обычно используются для указания маршрута по умолчанию или тогда, когда нужно временно указать маршрут до подсети в случае ухудшения качества основного маршрута, либо при отсутствии возможности использовать протокол динамической маршрутизации.

На коммутаторах SNR серии S5210G доступна аппаратная маршрутизация на скорости порта.

22.1 Настройка интерфейса уровня 3

1. Создать интерфейс управления уровня 3:

Команда	Описание
interface vlan<vlan-id>	Создать VLAN-интерфейс. **<vlan-id>** - номер vlan от 2 до 4094.
no interface vlan<vlan-id>	Удалить созданный VLAN-интерфейс.
! В режиме глобальной конфигурации	

2. Настроить описание интерфейса VLAN:

Команда	Описание
description <text>	Добавить описание **<text>** VLAN-интерфейсу.
no description	Удалить описание VLAN-интерфейса.
! В режиме конфигурирования interface vlan	

3. Установить статический IP-адрес интерфейсу управления уровня 3:

Команда	Описание
ip address {<ip-address/mask> | <ip-address> <mask>} [secondary] **no ip address**{<ip-address/mask> | <ip-address> <mask>} [secondary] *! В режиме конфигурирования interface vlan*	Назначить IP-адрес VLAN-интерфейсу. **<ip-address/mask>** - IP-адрес сети с указанием префикса маски; **<ip-address> <mask>** - IP-адрес сети с указанием маски; **secondary** - установить дополнительный IP -адрес на VLAN-интерфейс. Удалить статический IP-адрес с VLAN-интерфейса.

4. Динамическое получение IP-адреса на интерфейсе управления уровня 3:

Команда	Описание
ip address dhcp **no ip address dhcp** *! В режиме конфигурирования interface vlan*	Включить DHCP-клиент на VLAN-интерфейсе для получения IP-адреса от DHCP-сервера. Команда может применяться только на одном interface vlan. Выключить DHCP-клиент на VLAN-интерфейсе.
show ip dhcp-client *! В Admin режиме*	Отобразить полученный IP-адрес.

5. Настройка опции 60 на DHCP-клиенте:

При включенном DHCP-клиенте, на VLAN-интерфейсе, по умолчанию в опции 60 - Vendor class identifier клиент передает строку идентифицирующую производителя и модель коммутатора. Эту информацию можно изменить указав собственную:

Команда	Описание
ip dhcp client vendor-identifier <string>	Установить собственное значение **<string>** в передаваемой опции 60 - Vendor class identifier.

Команда	Описание
no ip dhcp client vendor-identifier *! В режиме глобальной конфигурации*	Передавать в опции 60 - Vendor class identifier значение используемое по умолчанию.

22.2 Настройка статической маршрутизации

Добавить статический маршрут:

Команда	Описание
ip route {<ip-address/mask> | <ip-address> <mask>} {<gateway-ip-address>} [description <name>]	Создать запись статического маршрута для сети, с указанием шлюза через который доступна эта сеть.
no ip route {<ip-address/mask> | <ip-address> <mask>} {<gateway-ip-address>} [description <name>] *! В режиме глобальной конфигурации*	Удалить созданный статический маршрут.

23. Dynamic Arp Inspection

Динамическая проверка ARP (**Dynamic ARP Inspection** или **DAI**) защищает локальную сеть от спуфинга ARP пакетов.

DAI использует информацию из базы данных DHCP для проверки пакетов ARP и защиты от подмены. Когда злоумышленник пытается использовать поддельный пакет ARP для подмены адреса, коммутатор сравнивает адрес с записями в таблице DHCP Binding. Если MAC-адрес или IP-адрес в пакете ARP не соответствует действующей записи в таблице, то пакет отбрасывается.

В DAI могут быть настроены доверенные порты, на которых входящие ARP пакеты не проверяются.

23.1 Настройка Dynamic Arp Inspection

1. Включить Dynamic Arp Inspection глобально:

Команда	Описание
ip arp inspection vlan <vlan-range>	Включить DAI на основе VLAN, глобально. (Максимальное количество Vlan со включенным DAI - 16).
no ip arp inspection vlan <vlan-range>	Выключить DAI глобально.
! В режиме глобальной конфигурации	

2. Настроить DAI на портах:

Команда	Описание
ip arp inspection trust	Назначить порт в качестве доверенного для DAI.
no ip arp inspection trust	Назначить порт как недоверенный для DAI (по умолчанию).
! В режиме конфигурации порта	

3. Настроить лимит ARP-сообщений:

Команда	Описание
ip arp inspection limit-rate <rate>	Настроить лимит ARP-сообщений в секунду для порта.
no ip arp inspection limit-rate <rate>	Удалить лимит ARP-сообщений (по умолчанию).
! В режиме конфигурации порта	

4. Настроить дополнительную проверку ARP-сообщений:

Команда	Описание
ip arp inspection validate	Включить дополнительную проверку ARP-сообщений на порте: - идентичность senderMac и srcMac; - корректность senderIP (не является all-zero, multicast или broadcast).
no ip arp inspection validate	Отключить дополнительную проверку ARP-сообщений на порте.
! В режиме конфигурации порта	

5. Отобразить состояние функционала DAI:

Команда	Описание
show ip arp inspection	Отобразить общее состояние функционала DAI на коммутаторе.
show ip arp inspection interface <if-name>	Отобразить состояние функционала DAI на порте.
! В Admin режиме	

23.2 Пример использования Dynamic ARP Inspection

DHCP-сервер и ПК пользователя принадлежат Vlan 10. DHCP-сервер подключен к интерфейсу ge1 коммутатора. ПК пользователя подключен к интерфейсу ge2 коммутатора и получает IP-адрес динамически через DHCP.

Конфигурация коммутатора выглядит следующим образом:

```
Switch(config)#vlan 10
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping binding
Switch(config)#ip dhcp snooping vlan 10
Switch(config)#ip arp inspection vlan 10
Switch(config)#interface ge1
Switch(config-if)#switchport access vlan 10
Switch(config-if)#ip arp inspection trust
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#exit
```

```
Switch(config)#interface ge2
Switch(config-if)#switchport access vlan 10
Switch(config-if)#ip arp inspection limit-rate 50
Switch(config-if)#end
```

В этом случае коммутатор будет перехватывать сообщения ARP только с порта ge2, с ограничением в 50 pps. Каждый раз при получении ARP-сообщения функционал DAI сравнит данные в сообщении с записью в базе, сформированной в процессе мониторинга DHCP. При обнаружении записи ARP-сообщение будет отправлено дальше. Если запись отсутствует в базе, то пакет будет отброшен.

24. DHCP snooping и Option 82

С помощью **DHCP snooping** коммутатор контролирует процесс получения DHCP-клиентом IP-адреса для предотвращения атак DHCP и появления нелегитимных DHCP-серверов в сети, устанавливая доверенные и недоверенные порты. Сообщения из доверенных портов передаются коммутатором без проверки. Обычно, доверенные порты используются для подключения DHCP-сервера или DHCP relay, а недоверенные - для подключения DHCP-клиентов. Коммутатор передает сообщения DHCP-запросов из недоверенных портов, но не передает DHCP-ответы. Кроме того, при получении DHCP-ответа из недоверенного порта, коммутатор заблокирует это сообщение.

Опция 82 протокола DHCP используется для того, чтобы проинформировать DHCP-сервер о том, от какого коммутатора и через какой его порт был получен запрос. DHCP-snooping добавляет опцию в DHCP-запросы от клиента и передает их серверу. DHCP-сервер, в свою очередь, предоставляет IP-адрес и другую конфигурационную информацию в соответствии с преднастроенными политиками на основании информации, полученной в заголовке опции 82. Применение опции 82 прозрачно для клиента. Сообщение DHCP может включать множество полей различных опций. Опция 82 - одна из них. Она должна располагаться после других опций, но до опции 255.

Заголовок опции 82 может содержать несколько саб-опций (рис.19). RFC3046 описывает 2 саб-опции Circuit-ID и Remote-ID.

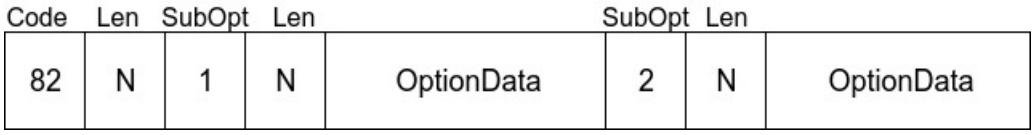

Рис. 19: Формат опции 82

24.1 Настройка DHCP snooping

1. Включить DHCP Snooping:

Команда	Описание
ip dhcp snooping **no ip dhcp snooping** *! В режиме глобальной конфигурации*	Включить функцию DHCP snooping. Выключить функцию DHCP snooping.
ip dhcp snooping vlan <vlan-range> **no ip dhcp snooping vlan** <vlan-range> *! В режиме глобальной конфигурации*	Включить функцию DHCP snooping на диапазоне VLAN. Выключить функцию DHCP snooping на диапазоне VLAN.

2. Настроить доверенные порты:

Команда	Описание
ip dhcp snooping trust **no ip dhcp snooping trust** *! В режиме конфигурации порта*	Назначить порт в качестве доверенного. Назначить порт в качестве недоверенного (по умолчанию).

3. Включить добавление опции 82 DHCP snooping:

Команда	Описание
ip dhcp snooping information option **no ip dhcp snooping information option** *! В режиме глобальной конфигурации*	Включить опцию 82 для добавления DHCP snooping. Выключить добавление опции 82 DHCP snooping.

4. Настроить атрибуты опции 82 глобально:

Команда	Описание
ip dhcp snooping information option self-defined remote-id <remote-id>	Задать контекст **<remote-id>** в двойных кавычках не длиннее 64 символов, передаваемый в качестве саб-опции Remote-ID, добавляемой в DHCP-запросы, полученные с интерфейса. Возможно указать следующие ключи: **%v** - номер vlan; **%M** - локальный MAC в верхнем регистре; **%m** - локальный MAC в нижнем регистре; **%R** - клиентский MAC в верхнем регистре; **%r** - клиентский MAC в нижнем регистре; **%p** - номер порта; **%s** - номер в стеке; **%h** - имя хоста.
no ip dhcp snooping information option self-defined remote-id *! В режиме глобальной конфигурации*	Восстановить конфигурацию по умолчанию (VLAN MAC коммутатора, формат ascii).

Команда	Описание
ip dhcp snooping information option self-defined subscriber-id <circuit-id> **no ip dhcp snooping information option self-defined subscriber-id** *! В режиме глобальной конфигурации*	Задать контекст **<circuit-id>** в двойных кавычках не длиннее 64 символов, передаваемый в качестве саб-опции Circuit-ID, добавляемой в DHCP-запросы, полученные с интерфейса. Возможно указать следующие ключи: **%v** - номер vlan; **%M** - локальный MAC в верхнем регистре; **%m** - локальный MAC в нижнем регистре; **%R** - клиентский MAC в верхнем регистре; **%r** - клиентский MAC в нижнем регистре; **%p** - номер порта; **%s** - номер в стеке; **%h** - имя хоста. Восстановить конфигурацию по умолчанию (VLAN ID номер порта, формат ascii).
ip dhcp snooping information option self-defined remote-id format {hex | acsii} **no ip dhcp snooping information option self-defined remote-id** *! В режиме глобальной конфигурации*	Задать формат опции 82, саб-опции Remote-ID, добавляемой DHCP-snooping. Для конфигурации атрибутов по умолчанию применяется формат ascii. Восстановить конфигурацию по умолчанию (VLAN MAC коммутатора, формат ascii).
ip dhcp snooping information option self-defined subscriber-id format {hex | acsii} **no ip dhcp snooping information option self-defined subscriber-id** *! В режиме глобальной конфигурации*	Задать формат опции 82, саб-опции Circuit-ID, добавляемой DHCP-snooping. Для конфигурации атрибутов по умолчанию применяется только hex формат. Восстановить конфигурацию по умолчанию (VLAN ID номер порта, формат ascii).

5. Настроить атрибуты опции 82 на порте:

Команда	Описание
ip dhcp snooping information option self-defined subscriber-id <remote-id> **no ip dhcp snooping information option self-defined subscriber-id** *! В режиме конфигурации порта*	Задать контекст <remote-id> в двойных кавычках не длиннее 64 символов, передаваемый в качестве саб-опции Remote-ID, добавляемой в DHCP-запросы, полученные с интерфейса. Возможно указать следующие ключи: **%v**: vlan-id; **%M**: local MAC в верхнем регистре; **%m**: local MAC в нижнем регистре; **%R**: client MAC в верхнем регистре; **%r**: client MAC в нижнем регистре; **%p**: portID - номер порта; При отсутствии настройки на порте, формат опции формируется в соответствии с глобальной настройкой. Отменить настройки на порте и применить значения установленные глобально.
ip dhcp snooping information option self-defined subscriber-id format {hex | acsii} *! В режиме конфигурации порта*	Задать формат ascii или hex для саб-опции Remote-ID опции 82, добавляемой DHCP-snooping. Для конфигурации атрибутов по умолчанию применяется формат ascii.

6. Настройка policy:

Команда	Описание
ip dhcp snooping information option policy { drop | keep | replace } **no ip dhcp snooping information option policy** *! В режиме глобальной конфигурации*	Настроить правило обработки входящих DHCP-Request пакетов с опцией 82 на untrust портах. **drop** - отбросить пакет, если в нем есть опция; **keep** - оставить существующую опцию 82 в пакете; **replace** (по умолчанию) - заменить опцию 82 в пакете. Команда выполняет установку значения по умолчанию (ip dhcp snooping information option policy replace).

7. Включить блокировку трафика для MAC-адресов, от которых были получены DHCP Offer или Ack пакеты на untrust портах:

Команда	Описание
ip dhcp snooping action blackhole recovery <10-3600>	Включить механизм блокировки трафика с нелегальных DHCP-серверов.
no ip dhcp snooping action	Выключить механизм блокировки трафика с нелегальных DHCP-серверов.
! В режиме конфигурации порта	

8. Просмотр настроек DHCP snooping:

Команда	Описание
show ip dhcp snooping	Отображение состояния dhcp snooping и конфигурации на интерфейсах.
! В Admin режиме	

9. Просмотр таблицы DHCP snooping Blackhole:

Команда	Описание
show ip dhcp snooping blackhole [interface <if-name>]	Отобразить таблицу Blackhole.
! В Admin режиме	

10. Очистка таблицы Blackhole:

Команда	Описание
clear ip dhcp snooping blackhole [interface <if-name>]	Очистить таблицу Blackhole.
! В Admin режиме	

24.2 Пример настройки DHCP snooping

Как показано на рисунке 20, ПК1 подключен к недоверенному порту ge1 коммутатора Switch1 и получает конфигурацию через DHCP, IP-адрес клиента 10.10.10.5. DHCP-сервер и шлюз подключены к портам коммутатора ge11 и ge12 соответственно, настроенным как доверенные. Злоумышленник ПК2, подключенный к недоверенному порту ge2 пытается подделать DHCP-сервер, посылая ложные DHCP ACK. Функция DHCP snooping эффективно обнаружит и заблокирует такой тип атаки.

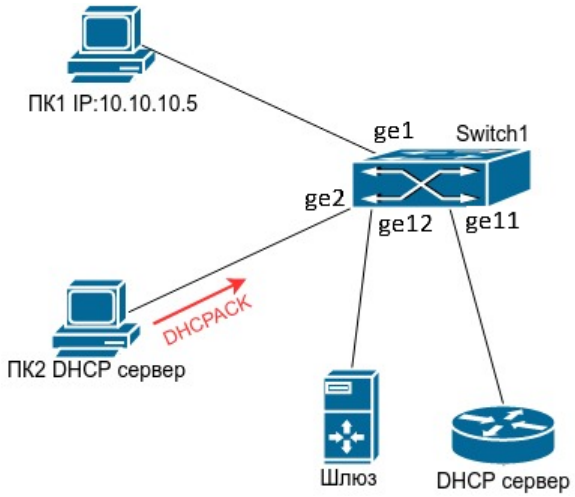

Рис. 20: Настройка DHCP snooping

Конфигурация коммутатора Switch1:

```
Switch1#configure terminal
Switch1(config)#ip dhcp snooping
Switch1(config)#ip dhcp snooping vlan 1
Switch1(config)#interface ge11-12
Switch1(config-if)#ip dhcp snooping trust
Switch1(config-if)#end
```

24.3 Пример конфигурации DHCP snooping с опцией 82

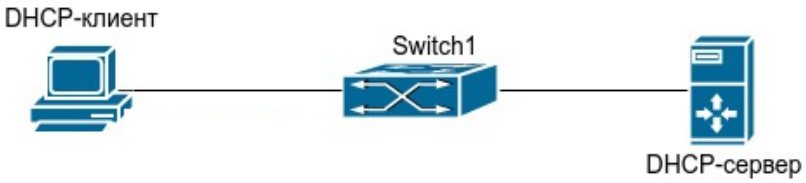

Рис. 21: Настройка опции 82 для DHCP snooping

Как показано на рисунке 21, коммутатор уровня 2 Switch1 с включенным DHCP-snooping передает DHCP-запросы серверу и ответы от DHCP-сервера клиенту. После того как на коммутаторе будет включена функция добавления опции 82 для DHCP snooping, Switch1 будет добавлять информацию о коммутаторе, интерфейсе и VLAN клиента в сообщения запроса.

Конфигурация коммутатора Switch1 (MAC address is f8:f0:82:75:33:01):

```
Switch1#configure terminal
Switch1(config)#ip dhcp snooping
Switch1(config)#ip dhcp snooping information option
Switch1(config)#ip dhcp snooping vlan 1
```

```
Switch1(config)#interface xe1
Switch1(config-if)#ip dhcp snooping trust
Switch1(config-if)#end
```

Пример конфигурации ISC DHCP Server для Linux:

```
ddns-update-style interim;
ignore client-updates;
class "Switch1Vlan1Customer1"{
match if option agent.circuit-id="Switch1ge1"and option agent.remote-id=f8f082753301;
}
subnet 192.168.102.0 netmask 255.255.255.0 {
option routers 192.168.102.2;
option subnet-mask 255.255.255.0;
option domain-name-servers 192.168.10.3;
authoritative;
pool {
range 192.168.102.51 192.168.102.80;
default-lease-time 43200; #12 Hours
max-lease-time 86400; #24 Hours
allow members of "Switch1Vlan1Customer1";
}}
```

После описанных выше настроек DHCP-сервер будет выделять адреса из диапазона 192.168.102.51-192.168.102.80 для устройств, подключенных к коммутатору Switch1.

24.4 Решение проблем с конфигурацией DHCP snooping

- Проверьте, включен ли DHCP-snooping;
- Если порт не реагирует на ложные DHCP сообщения, проверьте, настроен ли этот порт как недоверенный.

25. DHCP Snooping Binding

Функционал **DHCP Snooping Binding** позволяет реализовать контроль доступа пользователей, получающих IP-адреса по DHCP, на основании анализа DHCP пакетов проходящих через коммутатор.

При включении DHCP Snooping Binding, DHCP пакеты в Vlan, где включен DHCP Snooping, анализируются коммутатором. При успешном получении IP-адреса клиентом создается запись в binding таблице, которая связывает полученный IP-адрес с MAC-адресом, VLAN и номером порта, к которому подключен клиент.

На портах коммутатора можно включить контроль трафика на основании данной таблицы, при котором трафик будет пропускаться только в том случае, если IP-адрес, MAC-адрес источника, Vlan и порт на который пришел пакет, соответствуют записи в binding таблице. Таким образом трафик не легитимных клиентов (не получивших адрес по DHCP) будет заблокирован.

Дополнительно можно настроить ограничение по максимальному количеству клиентов, работающих за портом.

1. Включить функцию DHCP snooping binding:

Команда	Описание
ip dhcp snooping binding **no ip dhcp snooping binding** *! В режиме глобальной конфигурации*	Включить функцию отслеживания пакетов. Выключить функцию отслеживания пакетов.

2. Просмотр таблицы DHCP snooping binding:

Команда	Описание
show ip dhcp snooping binding *! В Admin режиме*	Отобразить записи в таблице DHCP snooping binding.

3. Очистка таблицы DHCP snooping binding:

Команда	Описание
clear ip dhcp snooping binding *! В Admin режиме*	Очистить таблицу DHCP snooping binding.

4. Включить функцию привязки DHCP Snooping Binding к пользователю:

Команда	Описание
ip dhcp snooping binding user-control	Включить контроль трафика на основании DHCP Snooping Binding на порте.
no ip dhcp snooping binding user-control *! В режиме конфигурации порта*	Выключить привязку DHCP Snooping Binding к пользователю.

5. Включить ограничение максимального количества клиентов в DHCP Snooping Binding:

Команда	Описание
ip dhcp snooping binding user-control max-user X	Задать ограничение количества привязок на порте. **X** - максимальное количество пользователей (от 1 до 254).
no no ip dhcp snooping binding user-control max-user *! В режиме конфигурации порта*	Отменить ограничение количества привязок на порте.

26. DHCP Relay

DHCP Relay - функционал, обеспечивающий ретрансляцию DHCP-пакетов от клиента к серверу. Поскольку протокол DHCP основан на широковещательной рассылке, DHCP пакеты не проходят через маршрутизаторы. Коммутатор, выступающий в роли DHCP Relay, перехватывает broadcast пакеты от DHCP-клиента и перенаправляет их на заданный адрес DHCP-сервера как unicast. Получив ответ от DHCP-сервера, коммутатор перенаправляет пакеты DHCP-клиенту которому они предназначались. В результате внедрения DHCP-Relay, один DHCP-сервер может использоваться для разных сегментов сети, что удобно в администрировании и позволяет уменьшить размер L2 сегментов в сети.

Коммутаторы SNR-S5210 поддерживают два вида DHCP Relay:

DHCP-Relay (L3) - стандартный вид, при котором в клиентском vlan должен быть настроен IP-адрес;

DHCP Relay share-vlan - позволяет пересылать DHCP пакеты без настройки IP-адреса в клиентском VLAN.

26.1 DHCP-Relay (L3)

Стандартный DHCP Relay используется в случаях, когда коммутатор является шлюзом для DHCP-клиентов. При помощи DHCP-Relay коммутатор ретранслирует DHCP пакеты от клиента к серверу и обратно, так как в этом случае L2 связность между ними отсутствует. Для настройки DHCP Relay необходимо глобально включить функционал DHCP-relay, указать адреса DHCP серверов и включить DHCP Relay на L3 интерфейсе в котором находятся клиенты.

26.1.1 Конфигурация DHCP-Relay (L3)

1. Глобальное включение DHCP-Relay:

Команда	Описание
ip dhcp relay enable	Глобальное включение функции DHCP-Relay.
no ip dhcp relay enable	Глобальное выключение функции DHCP-Relay.
! В режиме глобальной конфигурации	

2. Конфигурирование адреса DHCP-сервера:

Команда	Описание
ip dhcp relay address <ip-address>	Задать IP-адрес DHCP-сервера. Допускается конфигурирование до 8 IP-адресов.

Команда	Описание
no ip dhcp relay address <ip-address> *! В режиме глобальной конфигурации*	Удалить адрес DHCP-сервера.

3. Включение DHCP-relay на клиентском L3 интерфейсе:

Команда	Описание
ip dhcp relay enable **no ip dhcp relay enable** *! В режиме конфигурации Interface VLAN*	Включить DHCP-Relay на интерфейсе. Отключить DHCP-Relay на интерфейсе.

4. Просмотр настроек DHCP-Relay:

Команда	Описание
show ip dhcp relay *! В Admin режиме*	Отображение информации о состоянии, настроенных интерфейсах и адресах DHCP-серверов.

26.1.2 Пример конфигурации DHCP-Relay (L3)

Сценарий: На коммутаторе включена глобально функция DHCP-Relay. DHCP-клиент подключен к интерфейсу vlan 200 с настроенным на нём адресом 20.20.20.1 и включенной функцией DHCP-Relay. DHCP-сервер подключен к интерфейсу vlan 100 с адресом 10.10.10.1. Адрес DHCP-сервера 10.10.10.10. На DHCP-сервере должен находиться конфигурационный файл с пулом IP-адресов из сети 20.20.20.0/24.

Конфигурация будет выглядеть следующим образом:

```
switch(config)#ip dhcp relay enable
switch(config)#ip dhcp relay address 10.10.10.10
switch(config)#vlan 100,200
switch(config)#interface vlan100
switch(config-if)#ip address 10.10.10.1/24
switch(config-if)#exit
switch(config)#interface vlan200
switch(config-if)#ip address 20.20.20.1/24
switch(config-if)#ip dhcp relay enable
switch(config-if)#exit
switch(config)#interface ge1
switch(config-if)#switchport mode access
```

```
switch(config-if)#switchport access vlan 100
switch(config-if)#exit
switch(config)#interface ge20
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 200
```

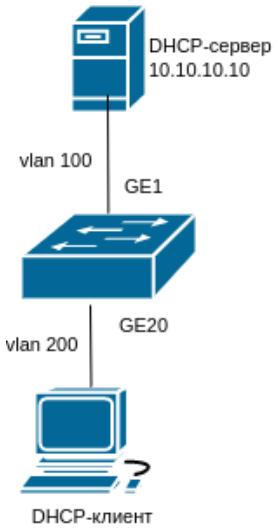

Рис. 22: Настройка DHCP-Relay

26.2 DHCP Relay share-vlan

DHCP-Relay share-vlan используется в случаях, когда на коммутаторе нежелательно иметь интерфейс с IP-адресом (в целях безопасности, экономии адресного пространства и.т.п.) и в тоже время есть необходимость пересылать DHCP пакеты на сервер. Для включения DHCP Relay share vlan необходимо глобально включить данный функционал, настроить uplink интерфейс (в который будут отправляться DHCP пакеты), настроить IP-адрес DHCP-сервера на uplink интерфейсе и настроить клиентский L3 интерфейс из которого будут пересылаться DHCP пакеты.

26.2.1 Конфигурация DHCP Relay share-vlan

1. Глобальное включение DHCP Relay share-vlan:

Команда	Описание
ip dhcp relay share-vlan enable	Глобальное включение функции DHCP Relay share-vlan.
no ip dhcp relay share-vlan enable	Глобальное отключение функции DHCP Relay share-vlan.
! В режиме глобальной конфигурации	

Команда	Описание
ip dhcp relay share-vlan relay-unicast	Включение перехвата и перенаправления DHCP Request unicast пакетов от клиента на DHCP-сервер.
no ip dhcp relay share-vlan relay-unicast	Отменить перенаправление DHCP Request unicast пакетов на DHCP-сервер.
! В режиме глобальной конфигурации	

2. Включение uplink-interface:

Команда	Описание
ip dhcp relay share-vlan uplink-interface	Задать uplink-interface для interface vlan. Команда может быть выполнена только на одном interface vlan.
no ip dhcp relay share-vlan uplink-interface	Удалить uplink-interface с interface vlan. Созданные IP-адреса share-vlan будут удалены.
! В режиме конфигурации Interface VLAN	

3. Задать IP-адрес DHCP-сервера:

Команда	Описание
ip dhcp relay share-vlan address <IP-address>	Задать IP-адрес сервера на uplink-interface.
no ip dhcp relay share-vlan address <IP-address>	Удалить IP-адрес сервера.
! В режиме конфигурации Interface VLAN	

4. Включение DHCP relay на клиентском L3 интерфейсе:

Команда	Описание
ip dhcp relay share-vlan customer-interface	Включить share-vlan на клиентском интерфейсе.
no ip dhcp relay share-vlan customer-interface	Отключить share-vlan на клиентском интерфейсе.
! В режиме конфигурации Interface VLAN	

5. Просмотр настроек DHCP-Relay share-vlan:

Команда	Описание
show ip dhcp relay share-vlan *! В Admin режиме*	Отображение информации о состоянии, статусе, настроенных интерфейсах и адресах DHCP-серверов.

26.2.2 Пример конфигурации DHCP Relay share-vlan

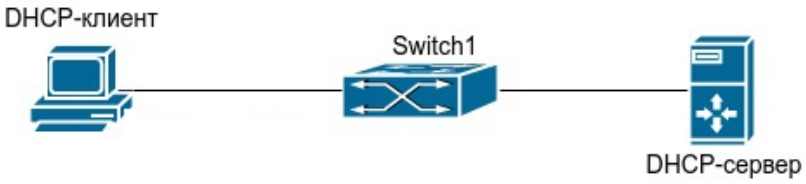

Рис. 23: Настройка DHCP-Relay share-vlan

Сценарий:

VLAN 12 предназначен для управления коммутатором, в VLAN 13 работает клиент подключенный в порт 10. Маршрутизация в VLAN 13 не производится. Необходимо пересылать DHCP запросы от клиента на сервер с адресом 1.1.1.1.

Для реализации сценария необходимо на коммутаторе включить глобально функцию ip dhcp relay share-vlan. Включить функцию uplink-interface на VLAN 12 и указать IP-адрес DHCP-сервера. На клиентском интерфейсе VLAN 13 включить функцию customer-interface.

Конфигурация будет выглядеть следующим образом:

```
switch#configure terminal
switch(config)#ip dhcp relay share-vlan enable
switch(config)#vlan 12,13
switch(config)#interface vlan12
switch(config-if)#ip address 192.168.2.9/24
switch(config-if)#ip dhcp relay share-vlan uplink-interface
switch(config-if)#ip dhcp relay share-vlan address 1.1.1.1
switch(config-if)#exit
switch(config)#interface ge24
switch(config-if)#switchport mode trunk
switch(config-if)#switchport trunk allowed vlan add 12,13
switch(config-if)#exit
switch(config)#interface vlan13
switch(config-if)#ip dhcp relay share-vlan customer-interface
switch(config-if)#exit
```

```
switch(config)#interface ge10
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 13
switch(config-if)#end
```

26.3 DHCP Relay broadcast suppress

DHCP Relay broadcast suppress - команда для подавления распространения Broadcast запросов от клиентов в Vlan, где включен DHCP-Relay (L3) или DHCP Relay share-vlan.

Команда	Описание
ip dhcp relay broadcast supress	Включить команду для подавления распространения Broadcast запросов.
no ip dhcp relay broadcast supress	Отключить команду для подавления распространения Broadcast запросов.
! В режиме глобальной конфигурации	

27. DHCP-сервер

DHCP (RFC2131) - сокращение от **Dynamic Host Configuration Protocol** (Протокол Динамической Конфигурации Узла). DHCP позволяет динамически назначить IP-адрес, а также передать хосту другие параметры сетевой конфигурации, такие как маршрут по умолчанию, DNS-сервер, местоположение файла образа прошивки и другие.

DHCP - имеет архитектуру “клиент-сервер”. DHCP-клиент запрашивает сетевой адрес и другие параметры у DHCP-сервера, сервер предоставляет сетевой адрес и параметры конфигурации клиентам. Если DHCP-сервер и DHCP-клиент находятся в разных подсетях, для перенаправления пакетов может быть настроен DHCP-relay.

В общем случае процесс предоставления адреса и других данных по DHCP выглядит следующим образом:

1. DHCP клиент отправляет широковещательный запрос DHCPDISCOVER;
2. При получении DHCPDISCOVER пакета DHCP сервер отправляет DHCP клиенту DHCPOFFER пакет, содержащий назначаемый IP-адрес и другие параметры;
3. DHCP клиент отправляет широковещательный DHCPREQUEST;
4. DHCP сервер отправляет пакет DHCPACK клиенту и клиент получает IP-адрес и другие параметры;

Вышеуказанные четыре этапа завершают процесс динамического назначения параметров. Однако, если DHCP сервер и DHCP клиент не находятся в одной сети, сервер не сможет получить широковещательные пакеты, отправленные DHCP клиентом. Для пересылки таких пакетов используется DHCP-relay, который перенаправит широковещательные пакеты от DHCP-клиента серверу как unicast.

Коммутаторы SNR могут быть настроены в качестве DHCP сервера.

27.1 Конфигурация DHCP-сервера

1. Включить DHCP server:

Команда	Описание
ip dhcp-server enable	Включить функцию DHCP-сервер.
no ip dhcp-server enable	Выключить функцию DHCP-сервер.
! В режиме глобальной конфигурации	

2. Настроить пул DHCP-адресов:

Команда	Описание
ip dhcp pool <name>	Создать пул адресов для DHCP-сервера и войти в режим его конфигурирования.

Команда	Описание
no ip dhcp pool <name> *! В режиме глобальной конфигурации*	Удалить пул адресов для DHCP-сервера.

2.1. Настроить передаваемые параметры:

Команда	Описание
network-address {<IP-address> | <IP-network>/<mask>} {<IP-address-start-range>}{<IP-address-stop-range>} **no network-address** *! В режиме конфигурации DHCP pool*	Добавить область адресов в текущий DHCP pool, а также начальный и конечный адрес используемого диапазона в этой области. Удалить область адресов из текущего DHCP pool.
default-route {<address1> | <hostname>} **no default-route** *! В режиме конфигурации DHCP pool*	Задать шлюз по умолчанию. Удалить адрес шлюза по умолчанию.
dns-server{<address1> | <hostname>} **no dns-server** *! В режиме конфигурации DHCP pool*	Задать адрес DNS-сервера. Удалить адрес DNS-сервера.
option-121 hex <hex-string> **no option-121** *! В режиме конфигурации DHCP pool*	Задать значение опции 121 в hex формате (длина префикса, адрес префикса, шлюз) Отключить передачу опции 121.
max-lease-time <seconds> **no max-lease-time** *! В режиме конфигурации DHCP pool*	Задать максимальное время аренды адреса в секундах. Вернуть значение по умолчанию - 7200 секунд.

Команда	Описание
default-lease-time <seconds>	Задать время аренды адреса в секундах, используемое в случае, если клиент самостоятельно не указал время использования адреса.
no default-lease-time	Вернуть значение по умолчанию - 600 секунд.
! В режиме конфигурации DHCP pool	

3. Настроить постоянно выделяемый адрес для хоста:

Команда	Описание
ip dhcp-server hardware-address {<name>} {<hw-addess>} {<ip-addess>}	Задать MAC-адрес для фиксированного назначения адреса.
no ip dhcp-server hardware-address <ip-addess>	Удалить MAC-адрес для фиксированного назначения адреса.
! В режиме глобальной конфигурации	

4. Просмотр информации и диагностика:

Команда	Описание
show ip dhcp-server	Просмотр статуса DHCP-сервера.
show ip dhcp binding	Просмотр выделенных IP-адресов.
! В Admin режиме	

27.2 Пример конфигурации DHCP-сервера

В примере указана настройка DHCP-сервера для выделения IP-адресов в Vlan 1 из диапазона 10.16.1.2 - 10.16.1.253. Дополнительно по DHCP выдается маршрут по умолчанию на 10.16.1.1, адрес DNS-сервера - 10.16.1.254 и статический маршрут на сеть 192.168.12.0/24 на шлюз 10.16.1.254.

IP-адрес 10.16.1.210 фиксированно задан для назначения устройству, имеющему MAC-адрес 0000.2223.ABCD.

```
Switch#configure terminal
Switch(config)#ip dhcp-server enable
Switch(config)#interface vlan1
Switch(config-if)#ip address 10.16.1.1 255.255.255.0
```

```
 Switch(config-if)#exit
Switch(config)#ip dhcp pool A
Switch(config-dhcp-pool)#network 10.16.1.0/24 10.16.1.2 10.16.1.253
Switch(config-dhcp-pool)#max-lease-time 3600
Switch(config-dhcp-pool)#default-route 10.16.1.1
Switch(config-dhcp-pool)#option 121 hex 18C0A80C0A1001FE
Switch(config-dhcp-pool)#dns-server 10.16.1.254
Switch(config-dhcp-pool)#end
```

27.3 Решение проблем при настройке DHCP-сервера

Если DHCP-клиент не может получить IP-адрес и другие сетевые параметры, после проверки кабеля и клиентского оборудования следует выполнить следующее:

- Проверьте, запущен ли DHCP-сервер;
- Если DHCP клиент и DHCP сервер находятся не в одной сети и не имеют прямой L2-связности, проверьте, настроена ли на коммутаторе, отвечающем за пересылку пакетов, функция DHCP-relay;
- Проверьте, имеет ли DHCP-сервер адресный пул в том же сегменте, что и адрес interface vlan коммутатора, перенаправляющего DHCP-пакеты.

28. DHCPv6 Snooping с Option 37/38

DHCPv6 Snooping с Option37/38 предназначен для блокирования DHCPv6 ответов от сервера на недоверенных портах, а также для вставки опций 37 и 38 в DHCPv6 пакеты от клиентов, аналогично функционалу DHCP Snooping с опцией 82.

DHCPv6 пакеты от клиента отправляются только в trust порты. DHCPv6 пакеты от сервера принимаются только на trust портах.

28.1 Настройка DHCPv6 Snooping

1. Включить DHCPv6 Snooping:

Команда	Описание
ipv6 dhcp snooping **no ipv6 dhcp snooping** *! В режиме глобальной конфигурации*	Включить функцию DHCPv6 Snooping глобально. Выключить функцию DHCPv6 Snooping глобально.
ipv6 dhcp snooping vlan <vlan-range> **no ipv6 dhcp snooping vlan** <vlan-range> *! В режиме глобальной конфигурации*	Включить функцию DHCPv6 Snooping на диапазоне VLAN. Выключить функцию DHCPv6 Snooping на диапазоне VLAN.

2. Настроить доверенные порты:

Команда	Описание
ipv6 dhcp snooping trust **no ipv6 dhcp snooping trust** *! В режиме конфигурации порта*	Назначить порт в качестве доверенного. Назначить порт в качестве недоверенного (по умолчанию).

3. Включить добавление опции 37/38:

Команда	Описание
ipv6 dhcp snooping {remote-id | subscriber-id} **option**	Включить добавление (замену) опции 37 - **remote-id** и/или 38 - **subscriber-id**.

Команда	Описание
no ipv6 dhcp snooping {remote-id | subscriber-id} **option** *! В режиме глобальной конфигурации*	Выключить добавление опций 37/38.

4. Задать значение опции 37/38:

Команда	Описание
ipv6 dhcp snooping information option self-defined {remote-id <remote-id> | subscriber-id <subscriber-id>}	Задать контекст опции 37 - **<remote-id>** и опции 38 - **<subscriber-id>** в двойных кавычках не длиннее 64 символов, передаваемый в качестве саб-опции, добавляемой в DHCPv6-запросы, полученные с интерфейса. Возможно указать следующие ключи: **%v**: vlan-id; **%M**: local MAC в верхнем регистре; **%m**: local MAC в нижнем регистре; **%R**: client MAC в верхнем регистре; **%r**: client MAC в нижнем регистре; **%p**: portID - номер порта.
no ipv6 dhcp snooping information option self-defined {remote-id | subscriber-id} *! В режиме глобальной конфигурации*	Отменить установленное значение опции 37/38.

5. Задать формат опции 37/38:

Команда	Описание
ipv6 dhcp snooping information option self-defined {remote-id | subscriber-id} **format** {ascii | hex} *! В режиме глобальной конфигурации*	Задать формат **ascii** или **hex** для опции 37/38. По умолчанию применяется формат ascii.

6. Просмотр состояния DHCPv6 Snooping:

Команда	Описание
show ipv6 dhcp snooping *! В Admin режиме*	Отображение состояния DHCPv6 Snooping и конфигурации на интерфейсах.

28.2 Пример настройки опций 37 и 38 для DHCPv6 Snooping

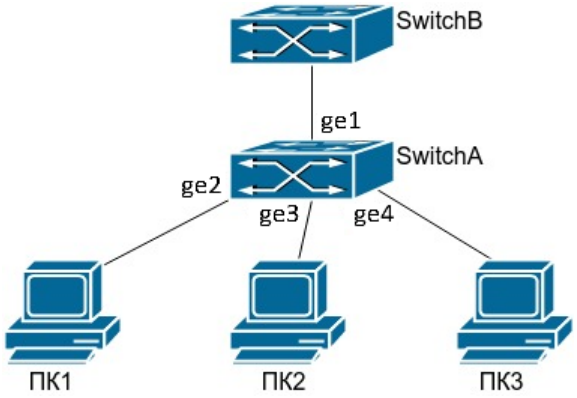

Рис. 24: Настройка DHCPv6 Snooping Option 37/38

Как показано на рисунке 24, ПК1, ПК2 и ПК3 подключены к недоверенным портам ge2, ge3 и ge4, и с помощью DHCPv6 получают IP-адреса. DHCPv6-сервер подключен к доверенному порту ge1. На коммутаторе Switch A включена функция DHCPv6 Snooping и настроены опции 37 и 38.

Конфигурация коммутатора Switch A будет выглядеть следующим образом:

```
SwitchA#configure terminal
SwitchA(config)#ipv6 dhcp snooping
SwitchA(config)#ipv6 dhcp snooping vlan 1
SwitchA(config)#ipv6 dhcp snooping remote-id option
SwitchA(config)#ipv6 dhcp snooping information option self-defined remote-id "Port
%p, Vlan %v"
SwitchA(config)#ipv6 dhcp snooping subscriber-id option
SwitchA(config)#ipv6 dhcp snooping information option self-defined subscriber-id
"local MAC: %M"
SwitchA(config)#interface ge1-4
SwitchA(config-if)#switchport access vlan 1
SwitchA(config-if)#exit
SwitchA(config)#interface ge1
SwitchA(config-if)#ipv6 dhcp snooping trust
SwitchA(config-if)#end
```

29. SAVI

Механизм **SAVI (Source Address Validation Improvement)** позволяет контролировать IPv6 трафик с помощью проверки соответствия IP и MAC-адресов источника с биндинг таблицей (Binding State Table, BST), а также защищаться от нелегитимных RA сообщений. Записи в BST создаются на основе DHCPv6 сообщений, перехватываемых функционалом DHCPv6 Snooping. При глобальном включении SAVI на портах без настройки 'ipv6 nd snooping trust' блокируются все RA сообщения. При включении SAVI на порту блокируются все IPv6 пакеты, у которых IP и MAC источника, а также VLAN не соответствуют BST (за исключением пакетов с link-local адресов и DHCPv6 пакетов).

29.1 Настройка SAVI

1. Включить функцию SAVI:

Команда	Описание
savi enable **no savi enable** *! В режиме глобальной конфигурации*	Включить функционал SAVI. Выключить функционал SAVI.

2. Задать метод обнаружения SAVI:

Команда	Описание
savi ipv6 dhcp-only enable **no savi ipv6 dhcp-only enable** *! В режиме глобальной конфигурации*	Включить заполнение таблицы BST на основе DHCPv6 сообщений. Выключить заполнение таблицы BST на основе DHCPv6 сообщений.

3. Включить валидацию IPv6 трафика согласно таблицы BST:

Команда	Описание
savi ipv6 check source ip-address mac-address **no savi ipv6 check source ip-address mac-address** *! В режиме конфигурации порта*	Включить контроль трафика на порте согласно таблицы BST. Выключить контроль трафика на порте согласно таблицы BST.

4. Включить ограничение на количество записей на порте:

Команда	Описание
savi ipv6 binding num <0-100>	Включить ограничение на количество создаваемых записей в BST для порта. При установке значения "0"записи на порте создаваться не будут.
no savi ipv6 binding num	Выключить ограничение на количество создаваемых записей в BST для порта.
! В режиме конфигурации порта	

5. Блокировка ND RA-пакетов на недоверенных портах:

Команда	Описание
ipv6 nd snooping trust	Сделать порт доверенным для ND RA-пакетов.
no ipv6 nd snooping trust	Сделать порт недоверенным для ND RA-пакетов.
! В режиме конфигурации порта	

6. Просмотр таблицы BST:

Команда	Описание
show savi ipv6 check source binding [interface <if-name>]	Отобразить всю таблицу BST или записи на определенном интерфейсе.
! В Admin режиме	

7. Очистка таблицы BST:

Команда	Описание
clear ipv6 dhcp snooping binding {**ipv6** <ipv6> | **mac** <mac> | **interface** <if-name> | **vlan** <vlan-id> | **all** }	Очистить записи в таблице BST с типом "dhcp". **ipv6** <ipv6> - удалить записи с указанным IPv6 адресом; **mac** <mac> - удалить записи с указанным MAC - адресом; **vlan** <vlan-id> - удалить записи с указанным VLAN; **interface** <if-name> - удалить записи с указанным интерфейсом; **all** - удалить все записи.
! В Admin режиме	

29.2 Пример конфигурации SAVI

Для осуществления проверки подлинности IPv6-адресов в пределах локальной сети и контроля их валидности необходимо включить функционал SAVI. Порт ge1 назначить доверенным для протоколов DHCPv6 и ND, так как за ним находится DHCPv6 сервер. На порте ge2, за которым находится DHCPv6 клиент, необходимо включить функцию контроля проверки подлинности пользователя для создания записей в таблице BST с ограничением в 5 записей.

Конфигурация будет выглядеть следующим образом:

```
Switch#configure terminal
Switch(config)#ipv6 dhcp snooping
Switch(config)#ipv6 dhcp snooping vlan 1
Switch(config)#savi enable
Switch(config)#savi ipv6 dhcp-only enable
Switch(config)#int ge1
Switch(config-if)#ipv6 dhcp snooping trust
Switch(config-if)#ipv6 nd snooping trust
Switch(config-if)#exit
Switch(config)#int ge2
Switch(config-if)#savi ipv6 binding num 5
Switch(config-if)#savi ipv6 check source ip-address mac-address
```

30. PPPoE Intermediate Agent

PPPoE (Point to Point Protocol over Ethernet) — это туннелирующий протокол, который позволяет инкапсулировать IP или другие протоколы через соединения Ethernet, устанавливая соединение «точка-точка», которое используется для транспортировки IP-пакетов. Такое соединение может быть установлено с BRAS, предоставляя пользователю широкополосный доступ и использующее аутентификацию.

PPPoE Intermediate Agent предоставляет возможность инкапсулировать в пакеты **PADI** (PPPoE Active Discovery Initiation), **PADR** (PPPoE Active Discovery Request) и **PADT** (PPPoE Active Discovery Termination) дополнительные данные, идентифицирующие местоположение пользователя, например MAC-адрес коммутатора, порт коммутатора, vlan пользователя, что обеспечивает дополнительные возможности для проверки подлинности. PPPoE Intermediate Agent также включает в себя функцию доверенного порта **pppoe intermediate-agent trust**, которая позволяет заблокировать прием нежелательных PADO и PADS-пакетов с недоверенных портов. Функция включается на порте, за которым находится сервер.

Для настройки вставки в пакет **vendor-specific TAG** необходимо:

1) Включить глобально опцию PPPoE Intermediate Agent;

2) Задать саб-опцию Circuit-ID - идентификатор подписчика (с какого порта приходит запрос) и/или Remote-ID - удаленный идентификатор (идентификатор самого ретранслятора).

Формат Circuit-ID и Remote-ID задается в виде шаблона, в котором можно указать произвольный текст с ключами, значения которых подставляются в момент формирования опции.

Пример шаблона опции PPPoE-пакета:

Шаблон	Пример в кодировке ascii	Пример в кодировке hex
interface %p	interface ge2	69 6e 74 65 72 66 61 63 65 20 00 02
vlan%v	vlan100	76 6c 61 6e 00 64
MAC - %R, PORT - %p	MAC - 00:D8:61:6F:E4:CC, PORT - ge7	4d 41 43 20 2d 20 00 d8 61 6f e4 cc 2c 20 50 4f 52 54 20 2d 20 00 07
%v%p	100ge2	00 64 00 02

3) Задать кодировку ascii или hex для текста в передаваемой саб-опции Circuit-ID и Remote-ID. Если кодировку не указывать, то по умолчанию будет использоваться ascii;

4)Включить опцию PPPoE Intermediate Agent на интерфейсе, в котором будет добавляться в пакет vendor-specific tag;

5) Порт, за которым находится PPPoE-сервер, назначить в качестве доверенного.

30.1 Конфигурация PPPoE Intermediate Agent

1. Включить глобально опцию PPPoE Intermediate Agent:

Команда	Описание
pppoe intermediate-agent	Включить опцию PPPoE Intermediate Agent глобально.
no pppoe intermediate-agent	Отключить опцию PPPoE Intermediate Agent глобально.
! В режиме глобальной конфигурации	

2. Задать саб-опцию, добавляемые поля и кодировку:

Команда	Описание
pppoe intermediate-agent self-defined {circuit-id | remote-id} {<string> | ascii | hex}	Задать саб-опцию **circuit-id** или **remote-id** и настроить добавляемые поля, указав контекст **<string>** в двойных кавычках не длиннее 64 символов, передаваемый в качестве саб-опции с кодировкой **ascii** или **hex**. В контексте можно указать следующие ключи: **%v** - номер vlan; **%M** - локальный MAC в верхнем регистре; **%m** - локальный MAC в нижнем регистре; **%R** - клиентский MAC в верхнем регистре; **%r** - клиентский MAC в нижнем регистре; **%p** - номер порта; **%s** - номер в стеке; **%h** - имя хоста.
no pppoe intermediate-agent self-defined {circuit-id | remote-id}	Удалить саб-опцию circuit-id или remote-id и вернуть кодировку по умолчанию в ascii.
! В режиме глобальной конфигурации	

3. Настроить PPPoE Intermediate Agent на интерфейсе:

Команда	Описание
pppoe intermediate-agent	Включить функцию PPPoE Intermediate Agent.
no pppoe intermediate-agent	Отключить функцию PPPoE Intermediate Agent.
! В режиме конфигурации порта	

Команда	Описание
pppoe intermediate-agent trust	Назначить порт в качестве доверенного.
no pppoe intermediate-agent trust	Назначить порт в качестве недоверенного.
! В режиме конфигурации порта	

30.2 Пример конфигурации PPPoE Intermediate Agent

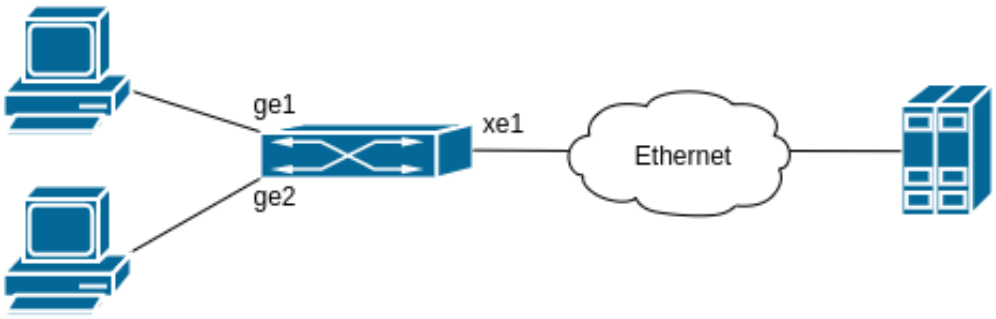

Рис. 25: Конфигурация PPPoE IA

Как показано на рисунке 25, PPPoE-клиенты и сервер подключены к одной L2 Ethernet сети. Клиенты подключены к портам ge1 и ge2, а сервер находится за портом xe1. На клиентских портах в PPPoE-пакеты требуется вставлять Vendor-specific-tag в формате ascii: circuit-id - ”interface <имя_порта>” и remote-id - ”mac-address <MAC-адрес коммутатора>”.

Конфигурация будет выглядеть следующим образом:

```
Switch#configure terminal
Switch(config)#pppoe intermediate-agent
Switch(config)#pppoe intermediate-agent self-defined circuit-id ascii
Switch(config)#pppoe intermediate-agent self-defined circuit-id "interface %p"
Switch(config)#pppoe intermediate-agent self-defined remote-id ascii
Switch(config)#pppoe intermediate-agent self-defined remote-id "mac-address %m"
Switch(config)#interface xe1
Switch(config-if)#pppoe intermediate-agent trust
Switch(config-if)#exit
Switch(config)#interface ge1
Switch(config-if)#pppoe intermediate-agent
Switch(config-if)#exit
Switch(config)#interface ge2
Switch(config-if)#pppoe intermediate-agent
Switch(config-if)#end
```

31. AAA

AAA - сокращение от **Authentication** (Аутентификация), **Authorization** (Авторизация) и **Accounting** (Учёт). Используется при предоставлении доступа в сеть, к управлению оборудованием и управления этим доступом. Наиболее распространёнными протоколами для централизованного управления AAA являются RADIUS и TACACS+.

31.1 RADIUS

RADIUS - это один из самых распространённых сетевых клиент-серверных протоколов, используемый для централизованного управления авторизацией, аутентификацией и учёта при запросе доступа пользователей к различным сетевым службам. Клиент RADIUS обычно используется на сетевом устройстве для реализации AAA. Сервер RADIUS хранит базу данных для AAA и связывается с клиентом через протокол RADIUS.

31.1.1 Конфигурация RADIUS

1. Настроить RADIUS-сервер и его параметры:

Команда	Описание
radius-server host {A.B.C.D | <hostname>} [key {0 | 7} <string>] [auth-port <port1>] [acct-port <port2>] [retransmit <n>] [timeout <sec>]	Настроить RADIUS-сервер с IP-адресом A.B.C.D или именем <hostname>. **key {0 | 7} <string>** - ключ RADIUS-сервера, **0** - в открытом виде, **7** - в шифрованном; **auth-port <port1>** - задать порт для аккаунтинга (по умолчанию - 1812); **acct-port <port2>** - задать порт RADIUS для аутентификации (по умолчанию - 1813); **retransmit <n>** - количество попыток повторной отправки пакетов на RADIUS-сервер (по умолчанию - 0); **timeout <sec>** - таймаут ожидания ответа от сервера (по умолчанию - 5 сек.).
no radius-server host {A.B.C.D | <hostname>} *! В режиме глобальной конфигурации*	Удалить RADIUS-сервер из конфигурации.

2. Создать группу серверов RADIUS (опционально):

Команда	Описание
aaa group server radius <name>	Создать группу серверов RADIUS.
no aaa group server radius <name>	Удалить группу серверов RADIUS.
! В режиме глобальной конфигурации	

3. Добавить сервер в группу серверов RADIUS (опционально):

Команда	Описание
server {A.B.C.D | <hostname>}	Добавить RADIUS-сервер в группу.
no server {A.B.C.D | <hostname>}	Удалить RADIUS-сервер из группы.
! В режиме конфигурации группы серверов RADIUS	

31.1.2 Передача уровня привилегий пользователя через RADIUS

Для передачи уровня привилегий необходимо, чтобы в ответе на запрос аутентификации RADIUS-сервер отправлял vendor-specific атрибут с кодом 240 и со значением уровня привилегий

Значение атрибута RADIUS-сервера	Уровень привилегий
1	network-user
10	network-operator
15	network-administrator

В этом случае пользователю автоматически назначаются права в соответствии с полученным уровнем привилегий. Если уровень привилегий не передается, то по умолчанию пользователь получает привилегии network-administrator.

Пример настройки передачи уровня привилегий для FreeRadius сервера.

В директории freeradius создаем файл (словарь) /usr/share/freeradius/dictionary.snr со следующим содержимым:

```
VENDOR SNR 40418
BEGIN-VENDOR SNR
ATTRIBUTE SNR-User-Priv 240 integer
END-VENDOR SNR
```

В конфигурационный файл /usr/share/freeradius/dictionary добавляем созданный нами словарь:

```
$INCLUDE /usr/share/freeradius/dictionary.snr
```

В файле /etc/freeradius/users создаем пользователя с необходимым уровнем привилегий (1,10 или 15):

```
user Cleartext-Password := "password"
SNR-User-Priv = 10
```

31.1.3 Проверка пароля enable через RADIUS

При включении проверки пароля enable через RADIUS, например командой “aaa authentication enable group radius”, коммутатор отправляет на RADIUS-сервер запрос авторизации с именем пользователя $enab15$. Соответственно на RADIUS-сервере должен быть заведен такой пользователь.

31.2 TACACS+

TACACS+ представляет собой похожий на RADIUS сеансовый протокол контроля доступа. Протокол TACACS+ использует три независимые функции: Аутентификация, Авторизация и Аккаунтинг (учёт). В отличие от RADIUS протокол TACACS+ использует TCP и шифрование передаваемых данных для обеспечения безопасности. TACACS+ может быть использован при авторизации и аутентификации пользователей для доступа к коммутатору по telnet, console или ssh.

31.2.1 Конфигурация TACACS+

1. Настроить сервер TACACS+ и его параметры:

Команда	Описание
feature tacacs+ **no feature tacacs+** *! В режиме глобальной конфигурации*	Включить протокол TACACS+. Отключить протокол TACACS+.
aaa authorization line vty exec tacacs+ **no aaa authorization line vty exec tacacs+** *! В режиме глобальной конфигурации*	Включить авторизацию через TACACS+. Отключить авторизацию через TACACS+.

Команда	Описание
tacacs-server host {A.B.C.D | <hostname>} key {0 | 7} <string>] [port <string>] [timeout <sec>]	Настроить TACACS+ сервер с IP-адресом **A.B.C.D** или именем **<hostname>**. **key {0 | 7} <string>** - ключ TACACS+ сервера, **0** - в открытом виде; **7** - в шифрованном; **port** - порт от 1 до 65535; **timeout <sec>** - таймаут ожидания ответа от сервера 1-60 сек. По умолчанию 5 сек.
no tacacs-server host {A.B.C.D | <hostname>} *! В режиме глобальной конфигурации*	Удалить TACACS+ сервер из конфигурации.

2. Создать группу серверов TACACS+ (опционально):

Команда	Описание
aaa group server tacacs+ <name>	Создать группу серверов TACACS+.
no aaa group server tacacs+ <name> *! В режиме глобальной конфигурации*	Удалить группу серверов TACACS+.

3. Добавить сервер в группу серверов TACACS+ (опционально):

Команда	Описание
server {A.B.C.D | <hostname>}	Добавить TACACS+ сервер в группу.
no server {A.B.C.D | <hostname>} *! В режиме конфигурации группы серверов TACACS+*	Удалить TACACS+ сервер из группы.

31.3 Конфигурация AAA

Настройка AAA заключается в выборе методов и их порядке для аутентификации и учёта пользователей, вводимых команд на коммутаторе, а также для проверки пароля перехода в привилегированный режим.

Доступные методы авторизации и учета:

- **group <имя группы>** - группа серверов RADIUS или TACACS+;

- **group radius** - зарезервированное имя группы, включающая все сервера RADIUS;
- **group tacacs+** - зарезервированное имя группы, включающая все сервера TACACS+;
- **local** - ааа с использованием локальной базы пользователей;
- **none** - отключение авторизации.

Порядок методов определяет порядок проверки учётных записей пользователей. Если метод авторизации по какой-то причине недоступен, например отсутствует связь с RADIUS сервером, то коммутатор переходит к следующему методу авторизации.

Существует два режима авторизации:

- **Стандартный** - роль пользователя назначается при авторизации на основе сконфигурированного уровня привилегий для локальных пользователей или переданного уровня привилегий через RADIUS/TACACS+ и не меняется при переходе в привилегированный режим;
- **Альтернативный** - изменяющий поведение коммутатора в процессах AAA:
  - Пользователи с уровнем привилегий 15 (network-admin) сразу попадают в привилегированный (enable) режим;
  - При переходе в привилегированный режим и успешной аутентификации роль пользователя повышается до network-admin;
  - Если при RADIUS или TACACS+ авторизации переданный уровень привилегий не соответствует network-admin, то пользователю назначается уровень 1 (network-user).

1. Использование альтернативного режима AAA:

Команда	Описание
aaa alternate-model	Включить альтернативный режим AAA.
no aaa alternate-model	Выключить альтернативный режим AAA.
! В режиме глобальной конфигурации	

2. Настройка параметров аутентификации пользователей:

Команда	Описание
aaa authentication login { console | remote } { group <name> | local } [none]	Включить аутентификацию для доступа к коммутатору через: **console** - консольный порт; **remote** - Telnet/SSH; используя метод: **group <name>** - группа серверов с именем <name>; **local** - локальная аутентификация (по умолчанию); **none** - без проверки. Группы с именами **radius** и **tacacs+**

Команда	Описание
	зарезервированы, и включают все настроенные сервера RADIUS или TACACS+ соответственно.
no aaa authentication login { console | remote } { group <name> | local } [none] *! В режиме глобальной конфигурации*	Выключить выбранный метод аутентификации.

3. Настройка параметров аутентификации для проверки enable:

Команда	Описание
aaa authentication enable {local | group radius [local] | group tacacs+ [local]}	Включить аутентификацию для перехода в привилегированный режим. **local** - локальная аутентификация (по умолчанию); **group radius** - аутентификация через сервера RADIUS; **group tacacs+** - аутентификация через сервера TACACS+; Группы с именами radius и tacacs+ зарезервированы и включают все настроенные сервера RADIUS или TACACS+ соответственно.
no aaa authentication enable group *! В режиме глобальной конфигурации*	Вернуть значение по умолчанию - локальная аутентификация.

4. Настройка авторизации вводимых команд по протоколу TACACS+:

Команда	Описание
aaa authorization line {vty | console} **command** [1 | 10 | 15] **tacacs** [local]	Включить авторизацию вводимых на коммутаторе команд с использованием протокола TACACS+ с доступом через консоль (**console**) и/или Telnet/SSH (**vty**) и уровнем привилегий 1, 10 или 15. **1** - авторизация всех команд; **10** - авторизация всех команд, кроме доступных для пользователя с правами network-user; **15** - авторизация только недоступных команд для пользователя с правами network-operator. **local** - выполнять вводимые команды в случае недоступности tacacs сервера.

Команда	Описание
no aaa authorization line {vty | console} *! В режиме глобальной конфигурации*	Выключить авторизацию вводимых на коммутаторе команд для определённого метода доступа.

5. Настройка аккаунтинга:

Команда	Описание
aaa accounting default {group <name> [local]}	Включить accounting авторизаций. **local** - локальный accounting; **group <name>** - accounting через группу серверов с именем <name>. Группы с именами **radius** и **tacacs+** зарезервированы и включают все настроенные сервера RADIUS или TACACS+ соответственно.
no aaa accounting default group <name> *! В режиме глобальной конфигурации*	Вернуть настройку по умолчанию - локальный accounting.
aaa accounting line {console | vty} **command** {1 | 10 | 15} **tacacs+**	Включить accounting для вводимых на коммутаторе команд с использованием протокола TACACS+ с доступом через консоль (**console**) и/или Telnet/SSH (**vty**) и уровнем привилегий 1, 10 или 15. **1** - accounting всех команд; **10** - accounting всех команд, кроме доступных для пользователя с правами network-user; **15** - accounting только недоступных команд для пользователя с правами network-operator.
no aaa accounting line {console | vty} *! В режиме глобальной конфигурации*	Выключить accounting вводимых команд для определённого метода доступа.

31.4 Ограничение доступа к управлению по Telnet и SSH

Для повышения безопасности при использовании протоколов Telnet и SSH можно установить access-list со списком разрешенных или запрещенных IP-адресов для удаленного подключения.

Команда	Описание
aaa authentication ip access-class <200-399> **in** (telnet | ssh) **no aaa authentication ip access-class** <200-399> **in** (telnet | ssh) *! В режиме глобальной конфигурации*	Ограничение доступа к управлению коммутатором по протоколам Telnet или SSH согласно ACL. Отменить ограничение доступа.

31.5 Примеры настройки AAA

Сценарий 1:

Необходимо настроить аутентификацию доступа к коммутатору для удалённых пользователей через протокол RADIUS. В случае недоступности RADIUS-сервера аутентификация не должна проходить. При доступе через консольный порт, сначала проверка должна выполняться через RADIUS-сервер, при его недоступности через локальную базу пользователей. Проверка пароля для привилегированного режима должна выполнятся через RADIUS, затем локально.

Для данного сценария настройка коммутатора будет выглядеть следующим образом:

```
Switch#configure terminal
Switch(config)#radius-server host 1.1.1.1 key 0 key123
Switch(config)#aaa authentication login remote group radius
Switch(config)#aaa authentication login console group radius local
Switch(config)#aaa authentication enable group radius local
```

Сценарий 2:

Необходимо настроить аутентификацию доступа к коммутатору для удалённых пользователей через 2 группы TACACS+. В случае недоступности серверов аутентификация проходить не должна. Проверка пароля для перехода в привилегированный режим должна выполнятся локально. При доступе через консольный порт, сначала проверка должна выполняться через все сервера TACACS+, при их недоступности через локальную базу пользователей.

Для данного сценария настройка коммутатора будет выглядеть следующим образом:

```
Switch#configure terminal
Switch(config)#feature tacacs+
Switch(config)#aaa authorization line vty exec tacacs+
Switch(config)#tacacs-server host 10.10.10.10 key 0 pasSw0rd
Switch(config)#tacacs-server host 10.10.10.11 key 0 pasSw0rd
Switch(config)#tacacs-server host 20.20.20.20 key 0 pasSw0rd
Switch(config)#tacacs-server host 20.20.20.21 key 0 pasSw0rd
Switch(config)#aaa group server tacacs+ gr1
```

```
Switch(config-tacacs)#server 10.10.10.10
Switch(config-tacacs)#server 10.10.10.11
Switch(config-tacacs)#exit
Switch(config)#aaa group server tacacs+ gr2
Switch(config-tacacs)#server 20.20.20.20
Switch(config-tacacs)#server 20.20.20.21
Switch(config-tacacs)#exit
Switch(config)#aaa authentication login remote group gr1 gr2
Switch(config)#aaa authentication login Console group tacacs+ local
Switch(config)#aaa authentication enable local
```

Сценарий 3:

Необходимо ограничить удалённое подключение к коммутатору по протоколу SSH разрешив соединение только с IP-адреса 10.10.10.50. В режиме глобальной конфигурации создаётся access-list с разрешённым IP-адресом, после чего данное правило применяется для аутентификации по протоколу SSH.

Для данного сценария настройка коммутатора будет выглядеть следующим образом:

```
Switch#configure terminal
Switch(config)#access-list 300 permit host 10.10.10.50
Switch(config)#aaa authentication ip access-class 300 in ssh
```

Сценарий 4:

Необходимо настроить авторизацию для всех вводимых команд на коммутаторе и вести их учёт с использованием протокола TACACS+ при подключении через Telnet/SSH.

Для данного сценария настройка коммутатора будет выглядеть следующим образом:

```
Switch#configure terminal
Switch(config)#feature tacacs+
Switch(config)#tacacs-server host 10.10.10.1 key 0 secret
Switch(config)#aaa authorization line vty command 1 tacacs
Switch(config)#aaa accounting line vty command 1 tacacs+
```

32. IGMP

IGMP (Internet Group Management Protocol) - протокол управления групповой (multicast) передачей данных в IP-сетях. IGMP используется маршрутизаторами и хостами для организации присоединения сетевых устройств к группам многоадресной рассылки (multicast). Маршрутизатор использует multicast-адрес 224.0.0.1 для отправки IGMP-сообщения запроса подтверждения членства в группах. Если хост присоединяется к какой-либо группе, он должен отправить IGMP-запрос на соответствующий адрес группы.

32.1 IGMP Snooping

IGMP Snooping используется для прослушивания IGMP-сообщений и контроля multicast трафика. На основе IGMP-сообщений коммутатор ведет таблицу переадресации multicast. Трафик отправляется только на порты, с которых поступил запрос на многоадресную группу.

Коммутатор поддерживает режим оптимизации IGMP сообщений **(report suppression**) для уменьшения количества IGMP пакетов в сети. В данном режиме коммутатор ретранслирует не все IGMP сообщения, а только те которые необходимы для добавления или удаления подписки. Так же в режиме report suppression возможно принудительное изменение версии IGMP пакетов и задание IP-адреса источника для IGMP пакетов. При включении функции igmp snooping, режим report suppression включается по умолчанию.

32.1.1 Настройка IGMP Snooping

1. Включить IGMP Snooping:

Команда	Описание
igmp snooping	Включить IGMP Snooping.
no igmp snooping	Выключить IGMP Snooping.
! В режиме конфигурации interface vlan	

2. Настроить IGMP Snooping:

Команда	Описание
igmp snooping report-suppression	Включить режим report suppression (по умолчанию).
no igmp snooping report-suppression	Выключить функцию report suppression.
! В режиме конфигурации interface vlan	

Команда	Описание
igmp snooping querier **no igmp snooping querier** *! В режиме конфигурации interface vlan*	Включить функционал General Querier. Выключить функционал General Querier.
igmp snooping mrouter interface <interface-name> **no igmp snooping mrouter interface** <interface-name> *! В режиме конфигурации interface vlan*	Задать mrouter порт <interface-name>. Удалить mrouter порт <interface-name>.
igmp snooping fast-leave **no igmp snooping fast-leave** *! В режиме конфигурации interface vlan*	Включить функцию быстрого удаления подписки на группу VLAN. Выключить функцию быстрого удаления подписки на группу для VLAN.
igmp snooping static-group <group-ip> **interface** <IFNAME> **no igmp snooping static-group** <group-ip> **interface** <IFNAME> *! В режиме конфигурации interface vlan*	Задать статическую подписку на группу <group-ip> на интерфейс <IFNAME> для VLAN. Удалить указанную статическую подписку на группу.
igmp snooping static-group <group-ip> **source** [ethernet | port-channel] <IFNAME> **no igmp snooping static-group** <group-ip> **source** [ethernet | port-channel] <IFNAME> *! В режиме конфигурации interface vlan*	Задать IP-адрес источника <source-ip> для статической подписки на группу <group-ip>. Удалить IP-адрес источника <source-ip> для статической подписки на группу <group-ip>.
igmp snooping report source-address <IP-address>	Задать IP-адрес источника для IGMP пакетов. Используется в режиме report-suppression.

Команда	Описание
no igmp snooping report source-address *! В режиме конфигурации interface vlan*	Отменить заданный IP-адрес источника для IGMP пакетов.
igmp snooping force-igmp-version 2 **no igmp snooping force-igmp-version 2** *! В режиме конфигурации interface vlan*	Установить принудительно версию 2 для всех отправляемых IGMP пакетов. Используется в режиме report-suppression. Вернуть значение по умолчанию. Использовать версию 3 для всех отправляемых IGMP пакетов.

3. Просмотр информации и диагностика:

Команда	Описание
show igmp snooping groups [<group-ip> | <int-vlan-id> | <detail>] *! В Admin режиме*	Просмотр информации о подписках.
show igmp snooping interface [<int-vlan-id>] *! В Admin режиме*	Просмотр информации о igmp snooping на vlan интерфейсе.
show igmp snooping mrouter vlan <vlan-id> *! В Admin режиме*	Просмотр информации о назначенном mrouter порте для VLAN.
show igmp snooping statistics interface <int-vlan-id> *! В Admin режиме*	Просмотр статистики igmp snooping для VLAN <int-vlan-id>.

4. Очистка таблицы подписок IGMP Snooping:

Команда	Описание
clear igmp snooping group * *! В Admin режиме*	Очистить таблицу подписок IGMP Snooping.

32.1.2 Пример настройки IGMP Snooping

Сценарий №1: IGMP Snooping

Как показано на рисунке 26, порты коммутатора 1, 2, 6, 10 и 12 добавлены во VLAN 100 на коммутаторе. Multicast маршрутизатор подключен к порту 1, а 4 хоста к остальным портам 2, 6, 10 и 12 соответственно. Поскольку IGMP Snooping по умолчанию глобально включен, но выключен для VLAN 100, он должен быть включен для VLAN 100. Кроме того, порт 1 должен быть выбран в качестве Mrouter порта для VLAN 100. Эти настройки можно осуществить следующим образом:

```
SwitchA#configure terminal
SwitchA(config)#interface vlan100
SwitchA(config-if)#igmp snooping
SwitchA(config-if)#igmp snooping mrouter interface ge1
```

Предположим, что сервер вещает 2 потока с использованием групповых адресов 239.255.0.1 и 239.255.0.2. Хосты из портов 2 и 3 подписались на группу 239.255.0.1, а хост из порта 6 - на группу 239.255.0.2.

Во время подписки, IGMP Snooping создаст таблицу, которая будет содержать соответствие портов 2 и 3 группе 239.255.0.1, а порт 6 - группе 239.255.0.2. В результате каждый порт получит трафик только тех групп, которые он запросил и не получит трафик других групп. Каждый порт сможет получить трафик любой их групп, запросив её.

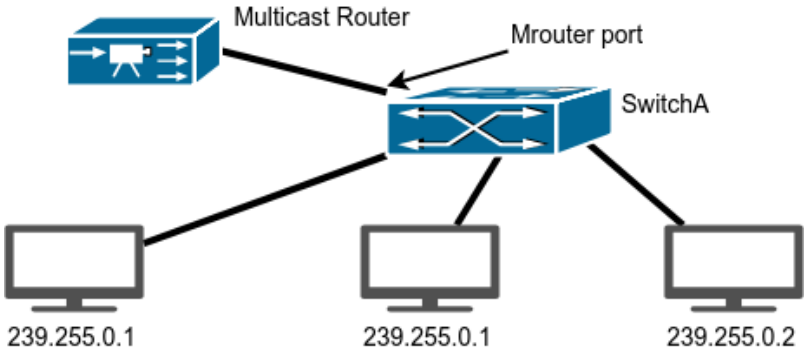

Рис. 26: IGMP Snooping

Сценарий №2: IGMP Querier

Схема, изображенная на рисунке 27, претерпела изменения: вместо Multicast маршрутизатора подключен источник мультикаст трафика, а между ним и Switch A подключен коммутатор Switch B, выполняющий роль IGMP Querier. Но подписчики, источник и порты между ними также принадлежат к VLAN 100.

Конфигурация **Switch A** такая же, как и в предыдущем примере. Конфигурация **Switch B** будет выглядеть следующим образом:

```
SwitchB#configure terminal
SwitchB(config)#interface vlan100
SwitchB(config-if)#igmp snooping
SwitchB(config-if)#igmp snooping querier
```

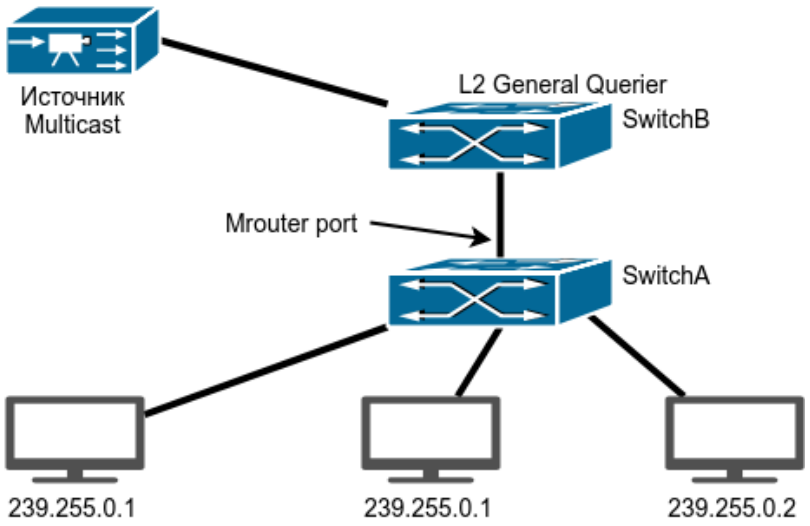

Рис. 27: IGMP Querier

32.1.3 Решение проблем с настройкой IGMP Snooping

При настройке и использовании IGMP Snooping могут возникнуть проблемы из-за физического соединения, а также некорректной настройки. Поэтому проверьте следующее:

- Убедитесь, что физическое соединение присутствует;
- Убедитесь, что IGMP Snooping включен как глобально, так и в нужном VLAN;
- Убедитесь, что mrouter порт присутствует;
- Используйте команды диагностики для проверки сконфигурированных параметров, а также записей в таблице IGMP Snooping.

32.2 Multicast Destination Control (Фильтрация IGMP подписок по адресам multicast групп)

Multicast Destination Control позволяет настроить список разрешенных и запрещенных multicast групп для подписчиков на порте.

Для работы Multicast Destination Control необходим IGMP Snooping, поэтому его нужно включить в тех VLAN, в которых планируется его использовать.

32.2.1 Настройка Multicast Destination Control

1. Конфигурирование ACL:

Команда	Описание
access-list <6000-7999> [<1-2147483645> | remark] [deny | permit] **ip any** [A.B.C.D/M | A.B.C.D A.B.C.D | host A.B.C.D | any]	Создать access-list **<6000-7999>** - диапазон ACL; **<1-2147483645>** - диапазон правил; **remark** - имя access list; **deny** - отбросить пакет; **permit** - пропустить пакет; **ip any** - адрес multicast-источника (поддерживается только any - любой); **A.B.C.D/M** - IP-адрес сети вида 239.255.1.0/24; **A.B.C.D A.B.C.D** - IP-адрес сети вида 239.255.1.0 0.0.0.255; **host A.B.C.D** - IP-адрес конкретной группы Например host 239.255.1.100; **any** - любой IP-адрес.
no access-list <6000-7999>	Полное удаление ACL.
no access-list <6000-7999> [<1-2147483645>] [(deny | permit) ip any (A.B.C.D/M | A.B.C.D A.B.C.D | host A.B.C.D | any)]	Удаление правила из ACL. Выполняется по номеру правила или по полному правилу.
no access-list <6000-7999> **remark**	Удаление имени ACL.
! В режиме глобальной конфигурации	

2. Применение ACL на порт:

Команда	Описание
ip multicast destination-control access-group <6000-7999>	Применить access-list на порт коммутатора.
no ip multicast destination-control access-group <6000-7999>	Удалить access-list с порта коммутатора.
! В режиме конфигурации порта	

32.2.2 Пример настройки Multicast Destination Control

Разрешить пользователю подписываться только на определенные multicast-группы. Для этого необходимо включить igmp snooping на interface vlan, задать mrouter port, создать access-list, в котором указать группы разрешенные для подписки и установить это правило на клиентский порт.

Конфигурация коммутатора будет следующая:

```
switch(config)#vlan 3
switch(config)#interface xe1,ge24
switch(config-if)#switchport access vlan 3
switch(config-if)#interface vlan3
switch(config-if)#igmp snooping
switch(config-if)#igmp snooping mrouter interface xe1
switch(config-if)#exit
switch(config)#access-list 6000 permit ip any host 239.255.3.153
switch(config)#access-list 6000 permit ip any host 239.255.2.21
switch(config)#access-list 6000 deny ip any any
switch(config)#interface ge24
switch(config-if)#ip multicast destination-control access-group 6000
```

32.3 Фильтрация IGMP пакетов по типам query/report

С помощью данной функции можно заблокировать все входящие IGMP пакеты с типом Report или Query.

32.3.1 Настройка фильтрации IGMP пакетов

1. Блокировка IGMP пакетов типа Query:

Команда	Описание
igmp snooping drop query	Включить блокировку IGMP пакетов типа Query.
no igmp snooping drop query	Отменить блокировку IGMP пакетов типа Query.
! В режиме конфигурации порта	

2. Блокировка IGMP пакетов типа Report:

Команда	Описание
igmp snooping drop report	Включить блокировку IGMP пакетов типа Report.
no igmp snooping drop report	Отменить блокировку IGMP пакетов типа Report.
! В режиме конфигурации порта	

32.3.2 Пример блокировки query и report пакетов на физических портах

На клиентском порте ge24 необходимо заблокировать прием Query пакетов, а на uplink порте xe1 заблокировать пакеты report.

Конфигурация коммутатора будет следующая:

```
switch(config)#vlan 5
switch(config)#interface xe1,ge24
switch(config-if)#switchport access vlan 5
switch(config-if)#exit
switch(config)#interface vlan5
switch(config-if)#igmp snooping
switch(config-if)#igmp snooping mrouter interface xe1
switch(config-if)#exit
switch(config)#interface ge24
switch(config-if)#igmp snooping drop query
switch(config-if)#exit
switch(config)#interface xe1
switch(config-if)#igmp snooping drop report
```

32.4 Ограничение количества IGMP подписок на порте

С помощью данной функции можно выставить ограничение на количество igmp подписок на клиентском порте.

32.4.1 Настройка ограничения количества подписок

1. Ограничение количества подписок на физическом порте:

Команда	Описание
igmp snooping limit group <1-1024>	Включить ограничение подписок на порте от 1 до 1024 групп.
no igmp snooping limit group	Отменить установленное ограничение.
! В режиме конфигурации порта	

32.4.2 Пример ограничения количества IGMP подписок

Установить на клиентском порте ограничение для igmp подписок на 10 групп.

Конфигурация коммутатора будет следующая:

```
switch(config)#vlan 5
switch(config)#interface xe1,ge24
switch(config-if)#switchport access vlan 5
switch(config-if)#exit
switch(config)#interface vlan5
switch(config-if)#igmp snooping
switch(config-if)#igmp snooping mrouter interface xe1
switch(config-if)#exit
switch(config)#interface ge24
switch(config-if)#igmp snooping limit group 10
```

32.5 IGMP Snooping Authentication

Для контроля доступа клиентов к различным multicast-группам используется функционал **IGMP Snooping Authentication**. IGMP Snooping Authentication работает следующим образом. Когда хост посылает сообщение о присоединении его к интересующей multicast-группе, коммутатор посылает запрос на RADIUS-сервер, в котором содержится MAC-адрес хоста, номер порта коммутатора и IP-адрес multicast-группы. Если на запрос RADIUS-сервер ответил Request-Accept, то осуществляется подписка на группу и multicast-трафик пропускается в клиентский порт. Если ответ Request-Reject - подписка отклоняется и multicast-трафик блокируется. Для уменьшения нагрузки на RADIUS-сервер, полученный ответ коммутатор записывает в кэш на 10 минут. В течение этого времени, при повторных подписках на multicast-группы, запросы на RADIUS-сервер отправляться не будут.

32.5.1 Настройка IGMP Snooping Authentication

1. Включить IGMP Snooping:

Команда	Описание
igmp snooping	Включить IGMP Snooping.
no igmp snooping	Выключить IGMP Snooping.
! В режиме конфигурации interface vlan	

2. Настроить аутентификацию для IGMP Snooping:

Команда	Описание
aaa authentication igmp group radius [none]	Включить аутентификацию IGMP групп через RADIUS-сервер. **none** - разрешить добавление подписки на группу, если RADIUS-сервер не отвечает.

Команда	Описание
no aaa authentication igmp group *! В режиме глобальной конфигурации*	Отключить аутентификацию IGMP через RADIUS-сервер.

3. Включить аутентификацию igmp snooping на клиентском порте:

Команда	Описание
igmp snooping authentication enable **no igmp snooping authentication enable** *! В режиме конфигурации порта*	Включить аутентификацию igmp snooping через RADIUS-сервер. Отключить аутентификацию igmp snooping через RADIUS-сервер.
igmp snooping authentication timeout <30-30000> **no igmp snooping authentication timeout** *! В режиме глобальной конфигурации*	Задать время жизни записи аутентификации в секундах. Восстановить значение по умолчанию (600 секунд).

32.5.2 Пример настройки IGMP Snooping Authentication

На коммутаторе настроен vlan 20 для порта ge2 с включенным IGMP Snopping, за которым находится пользователь и vlan 100 для порта ge24, за которым находится RADIUS-сервер. Для контроля многоадресных групп разрешенных пользователю в соответствии с политикой, требуется настроить аутентификацию для IGMP Snooping. RADIUS-сервер имеет адрес 10.10.10.10.

Конфигурация коммутатора следующая:

```
switch#configure terminal
switch(config)#radius-server host 10.10.10.10 key 0 secret
switch(config)#aaa authentication igmp group radius
switch(config)#vlan 20,100
switch(config)#interface vlan20
Switch(config-if)#igmp snooping
switch(config-if)#exit
switch(config)#interface vlan100
switch(config-if)#ip address 10.10.10.1/24
switch(config-if)#exit
```

```
switch(config)#interface ge24
switch(config-if)#switchport access vlan 100
switch(config-if)#exit
switch(config)#interface ge2
switch(config-if)#switchport access vlan 20
switch(config-if)#igmp snooping authentication enable
```

33. Multicast VLAN

В случае, если получатели Multicast трафика находятся в разных VLAN, в каждом VLAN создается своя копия одного и того же трафика, что может сказаться на свободной полосе пропускания каналов. Проблему решает **Multicast VLAN** - технология, которая позволяет серверу передавать мультикастовый поток в одном VLAN, в то время как конечные пользователи смогут получать его, находясь в различных VLAN, подключаясь к одному Multicast VLAN. Пользователи подключаются к мультикастовой рассылке и отсоединяются от нее, используя функционал IGMP snooping. Это позволяет не передавать multicast поток во все пользовательские VLAN и экономить ресурсы оборудования.

Multicast VLAN поддерживается на портах в режимах Access и Hybrid для нетегированного трафика. Для корректной работы в режиме Hybrid необходимо добавить multicast-vlan на порт в режиме untag.

33.1 Настройка Multicast VLAN

1. Настройка Multicast VLAN:

Команда	Описание
igmp snooping multicast-vlan <vlan_id> **no igmp snooping multicast-vlan** *! В режиме глобальной конфигурации*	Назначить Vlan <vlan_id> в качестве Multicast VLAN. Отменить установленную команду.
igmp snooping **no igmp snooping** *! В режиме конфигурации interface vlan*	Включить IGMP snooping для Multicast VLAN. Отменить установленную команду.
switchport association multicast-vlan <vlan_id> **no switchport association multicast-vlan** *! В режиме конфигурации порта*	Ассоциировать физический интерфейс коммутатора с multicast Vlan <vlan_id>. Отменить установленную команду.

33.2 Пример настройки Multicast VLAN

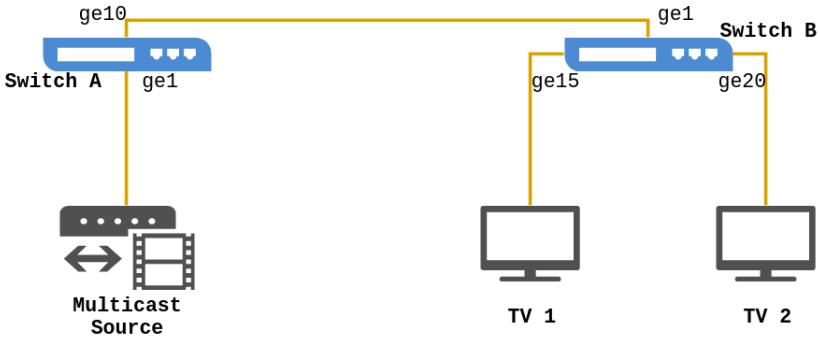

Рис. 28: Настройка Multicast Vlan

Как показано на рисунке 28, источник Mutlicast-трафика подключен к коммутатору Switch A через порт ge1 которому назначен Vlan 20. Switch A подключен к коммутатору уровня 2 Switch B через порт ge10, который настроен в режим trunk. К коммутатору Switch B подключены хосты пользователей TV1 и TV2. TV1 подключен к порту ge15, который принадлежит Vlan 100, а TV2 подключен к порту ge20, который принадлежит Vlan 101. Switch B подключен к Switch A через порт ge1. Vlan 20 настроен как Multicast Vlan.

Настройка Multicast VLAN в режиме Access

Конфигурация коммутатора A:

```
SwitchA#configure terminal
SwitchA(config)#vlan 20
SwitchA(config)#interface ge1,ge10
SwitchA(config-if)#switchport mode trunk
SwitchA(config-if)#switchport trunk allowed vlan add 20
SwitchA(config-if)#exit
SwitchA(config)#interface vlan20
SwitchA(config-if)#igmp snooping
SwitchA(config-if)#igmp snooping mrouter interface ge1
```

Конфигурация коммутатора B:

```
SwitchB#configure terminal
SwitchB(config)#vlan 20,100,101
SwitchB(config)#interface ge1
SwitchB(config-if)#switchport mode trunk
SwitchB(config-if)#switchport trunk allowed vlan add 20
SwitchB(config-if)#exit
SwitchB(config)#igmp snooping multicast-vlan 20
SwitchB(config)#interface vlan20
```

```
SwitchB(config-if)#igmp snooping
SwitchB(config-if)#igmp snooping mrouter interface ge1
SwitchB(config-if)#exit
SwitchB(config)#interface ge15
SwitchB(config-if)#switchport mode access
SwitchB(config-if)#switchport access vlan 100
SwitchB(config-if)#switchport association multicast-vlan 20
SwitchB(config-if)#exit
SwitchB(config)#interface ge20
SwitchB(config-if)#switchport mode access
SwitchB(config-if)#switchport access vlan 101
SwitchB(config-if)#switchport association multicast-vlan 20
```

Настройка Multicast VLAN в режиме Hybrid

Конфигурация коммутатора A:

```
SwitchA#configure terminal
SwitchA(config)#vlan 20
SwitchA(config)#interface ge1,ge10
SwitchA(config-if)#switchport mode trunk
SwitchA(config-if)#switchport trunk allowed vlan add 20
SwitchA(config-if)#exit
SwitchA(config)#interface vlan20
SwitchA(config-if)#igmp snooping
SwitchA(config-if)#igmp snooping mrouter interface ge1
```

Конфигурация коммутатора B:

```
SwitchB#configure terminal
SwitchB(config)#vlan 20,100,101
SwitchB(config)#interface ge10
SwitchB(config-if)#switchport mode trunk
SwitchB(config-if)#switchport trunk allowed vlan 20
SwitchB(config-if)#exit
SwitchB(config)#igmp snooping multicast-vlan 20
SwitchB(config)#interface vlan20
SwitchB(config-if)#igmp snooping
SwitchB(config-if)#igmp snooping mrouter interface ge1
SwitchB(config-if)#exit
SwitchB(config)#interface ge15
SwitchB(config-if)#switchport mode hybrid
SwitchB(config-if)#switchport hybrid allowed vlan 20 untag
SwitchB(config-if)#switchport hybrid native vlan 100
```

```
SwitchB(config-if)#switchport association multicast-vlan 20
SwitchB(config)#interface ge20
SwitchB(config-if)#switchport mode hybrid
SwitchB(config-if)#switchport hybrid allowed vlan 20 untag
SwitchB(config-if)#switchport hybrid native vlan 101
SwitchB(config-if)#switchport association multicast-vlan 20
```

34. ACL

Access Control List (список контроля доступа) - это механизм фильтрации IP-пакетов, позволяющий контролировать сетевой трафик, разрешая или запрещая прохождение пакетов на основе заданных признаков. Пользователь может самостоятельно задать критерии фильтрации ACL и применить фильтр на входящее по отношению к коммутатору направление трафика.

Access-list - последовательный набор правил. Каждое правило состоит из информации о фильтре и действии при обнаружении соответствия правилу. Информация, включенная в правило, представляет собой эффективную комбинацию таких условий, как исходный IP-адрес, IP-адрес получателя, номер протокола IP и порт TCP, порт UDP.

Списки доступа можно классифицировать по следующим критериям:

- Критерий на основе информации о фильтре:
  - IP ACL (фильтр на основе информации уровня 3 или выше);
  - MAC-IP ACL (уровень 2, 3 или выше).
  - MAC ACL (уровня 2);
- Критерий сложности конфигурации: стандартный (standard) и расширенный (extended).

Расширенный режим позволяет создавать более точные фильтры.

- Критерий на основе номенклатуры: нумерованный или именованный.

Описание ACL должно охватывать три вышеупомянутых аспекта.

Access-group - это описание привязки ACL к входящему направлению трафика на конкретном интерфейсе. Если группа доступа создана, все пакеты из входящего направления через интерфейс будут сравниваться с правилом ACL.

ACL может содержать два действия правила и действия по умолчанию: «разрешение» (permit) или «отказ» (deny). Access-list может состоять из нескольких правил. Фильтр сравнивает условия пакета с правилами, начиная с первого, до первого совпадения, остальные правила не будут обработаны. Глобальное действие по умолчанию применяется в случае, если для полученного пакета нет совпадений.

34.1 Настройка ACL

1. Настроить нумерованный standard IP access-list:

Команда	Описание
access-list {<1-99> | <1300-1999>} [<1-2147483645>] {deny | permit} {<source-ip-addr> | <source-ip-addr> <source-wildcard> | any }	Создать правило протокола **IP** нумерованного standard IP access-list с номером из диапазона <1-99> или <1300-1999>, с указанием адреса хоста - <source-ip-addr>, сети - <source-ip-addr> <source-wildcard> или любого адреса сети - any. **<1-2147483645>** - номер правила access-list; **deny** - отбросить пакет;

Команда	Описание
	permit - пропустить пакет. Если данный access-list не создан, то он будет создан после применения данной команды.
no access-list {<1-99> | <1300-1999>} [<1-2147483645> [{deny | permit} {<source-ip-addr> | <source-ip-addr> <source-wildcard> | any }]] *! В режиме глобальной конфигурации*	Удалить созданное правило (либо ACL полностью при указании только номера access-list).

2. Настроить нумерованный extended IP access-list:

Команда	Описание
access-list {<100-199> | <2000-2699>} [<1-2147483645>] {deny | permit} {**icmp | igmp**} {<src-ip-addr>/ <wildcard> | <src-ip-addr> <wildcard> | host <src-ip- addr> | any} (<dst-ip-addr> / <wildcard> | <dst-ip-addr> <wildcard> | host <dst-ip- addr> | any} [dscp {<0-63> | af11 | af12 | af13 | af21 | af22 | af23 |af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef} | precedence {<0-7> | critical | flash | flash-override | immediate | internet | network | priority | routine}] *! В режиме глобальной конфигурации*	Создать правило протокола **ICMP** или **IGMP** нумерованного extended IP access-list с номером из диапазона <100-199> или <2000-2699>. Если ACL не был создан ранее, он будет создан после применения данной команды. Команда **no** удаляет созданное правило (либо ACL полностью при указании только номера access-list).
access-list {<100-199> | <2000-2699>} [<1-2147483645>] {deny | permit} tcp {<src-ip-addr> / <wildcard> | <src-ip-addr> <wildcard> | host <src-ip-addr> | any} [eq <0-65535>] {<dst-ip-addr> / <wildcard> | <dst-ip-addr> <wildcard> | host <dst-ip-addr> | any}[eq {<0-65535> | ftp | ssh | telnet | www} | ack | psh | fin | rst | syn | urg | established]	Создать правило протокола **TCP** нумерованного extended IP access-list. Если ACL не был создан ранее, то он будет создан после применения данной команды.

Команда	Описание
[dscp {<0-63> | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef} | precedence {<0-7> | critical | flash | flash-override | immediate | internet | network | priority | routine}] [cos <0-7>] [vlan <1-4094> [vlan-mask <0-4095>]] *! В режиме глобальной конфигурации*	Команда **no** удаляет созданное правило (либо ACL полностью при указании только номера access-list).
access-list {<100-199> | <2000-2699>} [<1-2147483645>] {deny | permit} **udp** {<src-ip-addr> / <wildcard> | <src-ip-addr> <wildcard> | host <src-ip-addr> | any} [eq <0-65535>] {<dst-ip-addr> / <wildcard> | <dst-ip-addr> <wildcard> | host <dst-ip-addr> | any} [eq {<0-65535> | tftp | botp}] [dscp {<0-63> | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef} | precedence {<0-7> | critical | flash | flash-override | immediate | internet | network | priority | routine}] [cos <0-7>] [vlan <1-4094> [vlan-mask <0-4095>]] *! В режиме глобальной конфигурации*	Создать правило протокола **UDP** нумерованного extended IP access-list. Если ACL не был создан ранее, то он будет создан после применения данной команды. Команда **no** удаляет созданное правило (либо ACL полностью при указании только номера access-list).
access-list {<100-199> | <2000-2699>} [<1-2147483645>] {deny | permit} {**<0-255> | ip | gre** } {<src-ip-addr> / <wildcard> | <src-ip-addr> <wildcard> | host <src-ip-addr> | any} {<dst-ip-addr> / <wildcard> | <dst-ip-addr> <wildcard> | host<dst-ip-addr> | any} [dscp {<0-63> | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 |	Создать правило других протоколов, либо для всех IP протоколов нумерованного extended IP access-list. Если ACL не был создан ранее, то он будет создан после применения данной команды.

Команда	Описание
cs3 | cs4 | cs5 | cs6 | cs7 | default | ef} precedence {<0-7> | critical | flash | flash-override | immediate | internet | network | priority | routine}] [cos <0-7>] [vlan <1-4094> [vlan-mask <0-4095>]] *! В режиме глобальной конфигурации*	Команда **no** удаляет созданное правило (либо ACL полностью при указании только номера access-list).
access-list {<100-199> | <2000-2699>} [<1-2147483645>] {deny | permit} **igmp** {<src-ip-addr> / <wildcard> | <src-ip-addr> <wildcard> | host <src-ip-addr> | any }{<dst-ip-addr><wildcard> | <dst-ip-addr> <wildcard> | host <dst-ip-addr> | any} *! В режиме глобальной конфигурации*	Создать правило для фрагментированного трафика. Если ACL не был создан ранее, то он будет создан после применения данной команды. Команда **no** удаляет созданное правило (либо ACL полностью при указании только номера access-list).

3. Настроить нумерованный extended MAC access-list:

Команда	Описание
access-list {<100-199> | <2000-2699>} [<1-2147483645>] {deny | permit} **mac** {any | <src-mac-addr> <wildcard> | host <src-mac-addr>}{any | <dst-mac- addr> <wildcard> | host <dst-mac-addr>} [<ethertype>] [cos <0-7>] [vlan <1-4094> [vlan-mask <0-4095>]] *! В режиме глобальной конфигурации*	Создать правило нумерованного extended MAC access-list с номером из диапазона 100-199 или 2000-2699. Если ACL не был создан ранее, то он будет создан после применения данной команды. Команда **no** удаляет созданное правило (либо ACL полностью при указании только номера access-list).

4. Настроить нумерованный extended MAC-IP access-list:

Команда	Описание
access-list {<3100-3199>} [<1-2147483645>] {deny | permit} {host-mac <src-mac-addr> | <src-mac-addr> <wildcard> | any} {host-mac <dst-mac-addr> | <dst-mac-addr> <wildcard> | any} [ethertype <0x600-0xffff>] **ip | <0-255>**	Создать правило протокола **IP** или любого **протокола L4** нумерованного extended MAC-IP access-list с номером из диапазона 3100-3199. Если ACL не был создан ранее, то он будет создан после применения данной команды.

Команда	Описание
{<src-ip-addr>/<wildcard> | <src-ip-addr> <wildcard> | host-ip <src-ip-addr> | any} {<dst-ip-addr>/ <wildcard> | <dst-ip-addr> <wildcard> | host-ip <dst-ip-addr> | any } [dscp <0-63> | precedence <0-7>] [cos <0-7>] [vlan <1-4094> [vlan-mask <0-4095>]] *! В режиме глобальной конфигурации*	Команда **no** удаляет созданное правило (либо ACL полностью при указании только номера access-list).
access-list {<3100-3199>} [<1-2147483645>] {deny | permit} {host-mac <src-mac-addr> | <src-mac-addr> <wildcard> | any} {host-mac <dst-mac-addr> | <dst-mac-addr> <wildcard> | any} [ethertype <0x600-0xffff>] **udp** {<src-ip-addr>/<wildcard> | <src-ip-addr> <wildcard> | host-ip <src-ip-addr> | any } [eq <0-65535>] {<dst-ip-addr>/<wildcard> | <dst-ip-addr> <wildcard> | host-ip <dst-ip-addr> | any } [eq <0-65535>] [dscp <0-63> | precedence <0-7>] [cos <0-7>] [vlan <1-4094> [vlan-mask <0-4095>]] *! В режиме глобальной конфигурации*	Создать правило протокола **UDP** нумерованного MAC-IP access-list с номером из диапазона 3100-3199. Если ACL не был создан ранее, то он будет создан после применения данной команды. Команда **no** удаляет созданное правило (либо ACL полностью при указании только номера access-list).
access-list {<3100-3199>} [<1-2147483645>] {deny | permit} {host-mac <src-mac-addr> | <src-mac-addr> <wildcard> | any} {host-mac <dst-mac-addr> | <dst-mac-addr> <wildcard> | any} [ethertype <0x600-0xffff>] **tcp** {<src-ip-addr>/<wildcard> | <src-ip-addr> <wildcard> | host-ip <src-ip-addr> | any } [eq <0-65535>]	Создать правило протокола **TCP** нумерованного MAC-IP access-list с номером из диапазона 3100-3199. Если ACL не был создан ранее, то он будет создан после применения данной команды.

Команда	Описание
{<dst-ip-addr>/<wildcard> | <dst-ip-addr> <wildcard> | host-ip <dst-ip-addr> | any} [eq <0-65535>] [dscp <0-63> | precedence <0-7>] [cos <0-7>] [ack | fin | psh | rst | syn | urg] [vlan <1-4094> [vlan-mask <0-4095>]] *! В режиме глобальной конфигурации*	Команда **no** удаляет созданное правило (либо ACL полностью при указании только номера access-list).

5. Задать комментарий для access-list:

Команда	Описание
access-list {<1-399> | <1300-2699> | <3100-3199> | <6000-7999>} **remark** <LINE> **no access-list** {<1-399> | <1300-2699> | <3100-3199> | <6000-7999>} **remark** *! В режиме глобальной конфигурации*	Задать комментарий для access-list. Удалить комментарий для access-list.

6. Применить ACL на интерфейс:

Команда	Описание
{**ip** | **mac** | **mac-ip**} **access-group** <acl-name> **in** **no** {**ip** | **mac** | **mac-ip**} **access-group** <acl-name> **in** *! В режиме конфигурации порта*	Применить ACL <acl-name> на входящее направление трафика на интерфейсе. Удалить ACL <acl-name> с интерфейса.

7. Просмотр списка ACL:

Команда	Описание
show access-lists *! В Admin режиме*	Отобразить список всех ACL.

34.2 Пример настройки ACL

Сценарий 1: Порт ge10 относится к сегменту 10.0.0.0/24, протокол FTP не разрешен пользователю этого порта.

Конфигурация будет выглядеть следующим образом:

```
Switch(config)#access-list 2001 deny tcp 10.0.0.0 0.0.0.255 any eq 21
Switch(config)#interface ge10
Switch(config-if)#ip access-group 2001 in
```

Сценарий 2: Коммутатор должен отбрасывать ipv4 пакеты в интерфейсе ge10 с MAC-адресами источника из диапазона от 00-12-11-23-00-00 до 00-12-11-23-ff-ff.

Конфигурация будет выглядеть следующим образом:

```
Switch(config)#access-list 2200 deny mac 00-12-11-23-00-00 00-00-00-00-ff-ff any ip4
Switch(config)#interface ge10
Switch(config-if)#mac access-group 2200 in
```

Сценарий 3: Коммутатор должен отбрасывать на интерфейсе ge2 все TCP пакеты с MAC-адресом 0897.9890.8083 и IP-адресом 173.194.222.94 источника в VLAN 5.

Конфигурация будет выглядеть следующим образом:

```
Switch(config)#access-list 3110 deny host-mac 0897.9890.8083 any tcp host-ip
173.194.222.94 any vlan 5
Switch(config)#interface ge2
Switch(config-if)#mac-ip access-group 3110 in
```

34.3 Решение проблем с настройкой ACL

- Проверка правил ACL выполняется сверху вниз и заканчивается после первого совпадения;
- В одном ACL может быть не более 128 правил;
- Каждый порт может быть связан только с одним IP ACL, одним MAC-IP ACL и одним MAC ACL;
- При одновременном применении ACL разных типов на одном интерфейсе приоритет ACL будет следующим:
    1. IP ACL;
    2. MAC-IP ACL;
    3. MAC ACL.

35. AM (Access Management)

Функционал AM (Access Management) - управление доступом, заключается в ограничении трафика на порте с не разрешенных адресов. Разрешающие правила можно задавать как с указанием только IP-адреса или диапазона IP-адресов, так и связки MAC-адреса с IP-адресом.

35.1 Настройка AM

1. Включение функции AM:

Команда	Описание
am enable **no am enable** *! В режиме глобальной конфигурации*	Глобальное включение функции. Глобальное выключение функции.
am port **no am port** *! В режиме конфигурации порта*	Включение функцию на порте. Выключение функцию на порте.

2. Настройка таблицы разрешенного доступа:

Команда	Описание
am ip-pool <ip-address> <count> **no am ip-pool** <ip-address> <count> *! В режиме конфигурации порта*	Создать разрешающее правило для IP-адреса или диапазона IP-адресов на порте. **<ip-address>** - начальный IP-адрес; **<count>** - количество разрешенных IP-адресов. Удалить разрешающее правило с порта.
am mac-ip-pool <mac-address> <ip-address> **no am mac-ip-pool** <mac-address> <ip-address> *! В режиме конфигурации порта*	Добавить разрешающее правило для связки MAC-адреса с IP-адресом на порт. Удалить правило с порта.

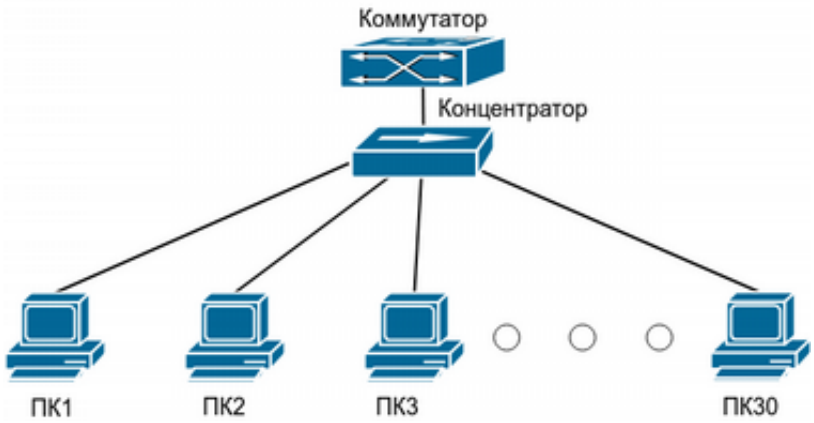

Рис. 29: Конфигурация AM

Как показано на рисунке 29, 30 ПК подключены через концентратор к коммутатору через интерфейс ge1. IP-адреса этих ПК находятся в диапазоне от 10.0.0.1 до 10.0.0.30. Согласно политике безопасности, администратор настраивает легальными только эти 30 адресов. Коммутатор будет пересылать только пакеты от этих IP-адресов, а пакеты от других адресов отбрасывать.

Конфигурация будет выглядеть следующим образом:

```
Switch#configure terminal
Switch(config)#am enable
Switch(config)#interface ge1
Switch(config-if)#am port
Switch(config-if)#am ip-pool 10.0.0.1 30
```

36. MAB (MAC Authentication Bypass)

Во многих сетях присутствуют устройства (такие, как сетевые принтеры, мобильные устройства и т.д), не имеющие возможности использовать проверку подлинности 802.1x. К таким устройствам может быть применена аутентификация **MAB (MAC Authentication Bypass)**, которая позволяет авторизовать пользователей по MAC-адресу через RADIUS сервер и назначать им номер VLAN. Пользователю не нужно устанавливать ПО клиента аутентификации или вводить логин и пароль в процессе. Для аутентификации коммутатору достаточно получить ARP-пакет от MAB-пользователя и после обнаружения соответствия аутентификационной информации на сервере, пользователю будет разрешен доступ. Используйте MAC-адрес пользователя в качестве логина и пароля в формате xx-xx-xx-xx-xx-xx, в нижнем регистре при настройке RADIUS-сервера. Для передачи номера Vlan в ответе от RADIUS сервера необходимо установить следующие атрибуты:

```
Tunnel-Type = 13,
Tunnel-Medium-Type = 6,
Tunnel-Private-Group-ID = "vlan-id"
```

36.1 Настройка MAB

1. Глобальные настойки MAB:

Команда	Описание
mac-authentication-bypass enable **no mac-authentication-bypass enable** *! В режиме глобальной конфигурации*	Включить функцию MAB глобально. Отключить функцию MAB глобально и удалить со всех интерфейсов настройки MAB.
aaa authentication mab group {radius [none] | none} **no aaa authentication mab group** *! В режиме глобальной конфигурации*	Задать метод аутентификации MAB. Отменить метод аутентификации MAB.
mac-authentication-bypass lease-time <1-3600> **no mac-authentication-bypass lease-time** *! В режиме глобальной конфигурации*	Задать время начала повторной аутентификации, после удачной аутентификации. Вернуть значение по умолчанию - 180 секунд.

Команда	Описание
mac-authentication-bypass timeout reauth-period <1-3600>	Задать время, в течение которого коммутатор не будет реагировать на запрос аутентификации от MAC-адреса, после его неудачной аутентификации.
no mac-authentication-bypass timeout reauth-period	Вернуть значение по умолчанию - 30 секунд.
! В режиме глобальной конфигурации	

2. Настройка MAB на портах:

Команда	Описание
mac-authentication-bypass enable	Включить функцию MAB на порте.
no mac-authentication-bypass enable	Отключить функцию MAB на порте и удалить все настройки MAB с порта.
! В режиме конфигурации порта	
mac-authentication-bypass guest-vlan <1-4094>	Задать гостевой VLAN.
no mac-authentication-bypass guest-vlan	Удалить гостевой VLAN.
! В режиме конфигурации порта	
mac-authentication-bypass binding-limit <1-100>	Задать максимальное количество записей MAB на порте.
no mac-authentication-bypass binding-limit	Вернуть значение по умолчанию - 3 записи.
! В режиме конфигурации порта	

3. Просмотр состояния MAB на интерфейсах

Команда	Описание
show mac-authentication-bypass brief	Отобразить состояние MAB на интерфейсах и количество авторизовавшихся MAC-адресов на них.
! В Admin режиме	

4. Просмотр записей в MAB-таблице:

Команда	Описание
show mac-authentication-bypass [interface <ifname>] [state {guest | authenticated | authenticating | reject}] [vlan <1-4094>] *! В Admin режиме*	Отобразить MAB-таблицу целиком, либо только записи по указанным параметрам. Допустимо указание нескольких параметров, например interface и state.

5. Очистка записей из MAB-таблицы:

Команда	Описание
clear mac-authentication-bypass binding { all } | { interface <ifname> | mac <mac-address> | vlan <1-4094> | state { authenticated | authenticating | guest | reject }} *! В Admin режиме*	Очистить записи в MAB-таблице. Допустимо указание нескольких параметров, например interface и state.

36.2 Пример конфигурации MAB

Как показано на рисунке 30, ПК пользователя подключен к порту GE1 коммутатора. В соответствии с политикой безопасности, доступ в офисную сеть через VLAN 9 предоставляется только после аутентификации на RADIUS-сервере, но для гостевых устройств предусмотрен гостевой VLAN 8. Сеть управления коммутатором, как и RADIUS-сервер, находится в VLAN 10.

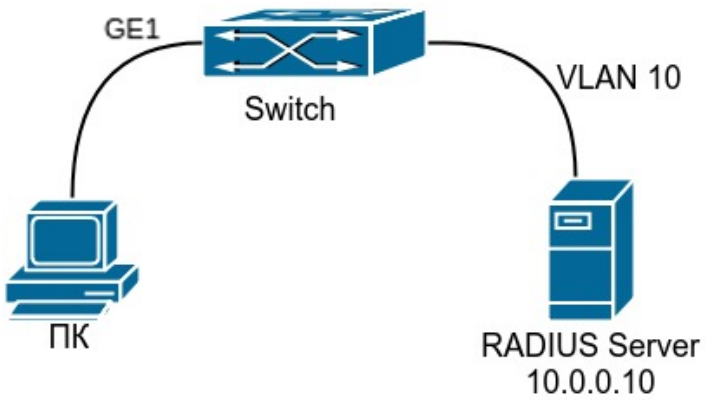

Рис. 30: MAB

Конфигурация коммутатора будет выглядеть следующим образом:

```
Switch(config)#vlan 8-10
Switch(config)#interface vlan 10
Switch(config-if)#ip address 10.0.0.9/24
Switch(config-if)#exit
Switch(config)#radius-server host 10.0.0.10 key 0 private
Switch(config)#mac-authentication-bypass enable
Switch(config)#aaa authentication mab group radius
Switch(config)#interface ge1
Switch(config-if)#switchport mode hybrid
Switch(config-if)#switchport hybrid native vlan 8
Switch(config-if)#switchport hybrid allowed vlan 8,9 untag
Switch(config-if)#mac-authentication-bypass enable
Switch(config-if)#mac-authentication-bypass guest-vlan 8
```

Пример добавления MAC-адреса пользователя на RADIUS-сервере для авторизации в VLAN 9.

В файл users ($/etc/freeradius/3.0/users$) добавить следующую запись:

```
54-af-97-2d-d6-c6 Cleartext-Password := "54-af-97-2d-d6-c6"
        Tunnel-Type = 13,
        Tunnel-Medium-Type = 6,
        Tunnel-Private-Group-ID = "9"
```

37. Port-security

Port-security - механизм обеспечения безопасности и контроля доступа, основанный на контроле изучаемых MAC-адресов. Port-security контролирует доступ неавторизованных устройств к сети проверяя MAC-адрес источника принятого кадра. Для настройки функции port-security необходимо задать максимальное количество изучаемых MAC-адресов на порте и правило поведения при превышении заданного ограничения. При получении кадра с неизученным MAC-адресом, коммутатор запускает заданное пользователем правило защиты порта и автоматически выполняет заданное действие.

37.1 Настройка Port-security

1. Включение функции port-security:

Команда	Описание
switchport port-security **no switchport port-security** *! В режиме конфигурации порта*	Включить port-security на порте. Выключить port-security на порте.

2. Установить максимальное количество изучаемых MAC-адресов:

Команда	Описание
switchport port-security maximum <count> **no switchport port-security maximum** *! В режиме конфигурации порта*	Установить максимальное количество изучаемых MAC-адресов на порте. **<count>** - значение от 0 до 4096. Вернуть значение по умолчанию (1 MAC-адрес).

3. Задать правило защиты:

Команда	Описание
switchport port-security violation {protect | restrict | errdisable}	Выбрать действие при превышении максимально допустимого количества изучения MAC-адресов на порте. **Protect** - не изучать новые MAC-адреса и отбросить пакеты;

Команда	Описание
! В режиме конфигурации порта	**Restrict** - не изучать новые MAC-адреса, отбросить пакеты, записать событие в syslog и отправить SNMP Trap; **Errdisable** - перевести порт в состояние errdisable, записать событие в syslog и отправить SNMP Trap.

4. Отображение информации о конфигурации Port-security:

Команда	Описание
show port-security *! В Admin режиме*	Вывод информации о конфигурации Port-security на портах в виде таблицы.

5. Очистка счетчиков срабатывания:

Команда	Описание
clear port-security counters *! В Admin режиме*	Очистка счетчиков количества срабатываний ограничения MAC-адресов.

37.2 Пример конфигурации Port-security

Для предотвращения подмены MAC-адреса одного пользователя другими, на портах коммутатора доступа используется port-security. Функционал будет разрешать доступ только авторизованным устройствам и отправлять SNMP Trap администратору при попытке изучения неизвестного MAC-адреса. Для этого необходимо настроить SNMP-сервер, на клиентском порте включить port-security и задать правило защиты restrict.

Конфигурация коммутатора будет выглядеть следующим образом:

```
Switch(config)#snmp-server enable snmp
Switch(config)#snmp-server enable traps snmp authentication
Switch(config)#snmp-server community private group network-operator
Switch(config)#snmp-server host 10.0.1.1 traps version 2c private udp-port 162
Switch(config)#interface ge10
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security violation restrict
```

38. NTP и SNTP

NTP (Network Time Protocol) - протокол сетевого времени, используемый с целью синхронизации времени среди распределенных серверов и клиентов. Благодаря используемым алгоритмам способен достичь точности до 10мс. События, состояния, функции передачи и действия определены в RFC-1305. Время на коммутаторе может быть синхронизировано с внешним сервером, также коммутатор может выполнять роль эталона времени в качестве NTP сервера.

SNTP (Simple Network Time Protocol) - простой протокол сетевого времени. Используется в системах и устройствах, не требующих высокой точности. SNTP протокол является упрощением NTP протокола, поэтому SNTP клиент может обращаться к любому NTP серверу, как к серверу SNTP.

38.1 Конфигурация NTP

1. Влючить NTP клиент:

Команда	Описание
ntp enable **no ntp enable** *! В режиме глобальной конфигурации*	Включить функцию NTP. Выключить функцию NTP.

2. Настроить NTP клиент:

Команда	Описание
ntp server {<ip-address>} [iburst] [key <key-id>] [maxpoll <4-16>] [minpoll <4-16>] [prefer]	Задать IP-адрес и ключ сервера. **iburst** - активирует упрощенный режим синхронизации; **key** - номер ключа аутентификации; **maxpoll** - максимальное время синхронизации; **minpoll** - минимальное время синхронизации; **prefer** - выбрать сервер предпочтительным.
no ntp server {<ip-address> } [key <key-id>] [maxpoll | minpoll] [prefer] *! В режиме глобальной конфигурации*	Удалить NTP сервер.

Команда	Описание
ntp peer {<ip-address>} [key <key-id>] [maxpoll <4-16>] [minpoll <4-16>] [prefer] **no ntp peer** {<ip-address>} [key <key-id>] [maxpoll <4-16> | minpoll <4-16>] [prefer] *! В режиме глобальной конфигурации*	Задать IP-адрес и ключ сервера NTP-партнёра. **key** - номер ключа аутентификации; **maxpoll** - максимальное время синхронизации; **minpoll** - минимальное время синхронизации; **prefer** - выбрать сервер предпочтительным. Удалить NTP-партнёра.
ntp authenticate **no ntp authenticate** *! В режиме глобальной конфигурации*	Включить функцию аутентификации NTP. Отключить функцию аутентификации NTP.
ntp authentication-key <key-id> md5 <value> **no ntp authentication-key** <key-id> *! В режиме глобальной конфигурации*	Задать ключ для аутентификации NTP. Удалить сконфигурированный ключ.
ntp trusted-key <key-id> **no ntp trusted-key** <key-id> *! В режиме глобальной конфигурации*	Задать идентификатор безопасного ключа. Удалить сконфигурированный идентификатор.
ntp sync-retry *! В Admin режиме*	Запустить синхронизацию времени принудительно.

3. Отобразить информацию о конфигурации и синхронизации NTP-серверов.

Команда	Описание
show ntp statistics **show ntp logging-status**	Вывод информации о статусе NTP в формате ntpq. Отобразить статус подключения.

Команда	Описание
show ntp peers	Вывести список NTP-серверов.
show ntp peer-status	Отобразить статус всех NTP-серверов.
show ntp authentication-keys	Отобразить ключ для аутентификации NTP.
show ntp authentication-status	Отобразить статус аутентификации.
show ntp trusted-keys	Отобразить идентификатор безопасного ключа.
! В Admin режиме	

4. Смещение часового пояса:

Команда	Описание
clock timezone <name> {add | substract} <0-23>	Задать смещение часового пояса относительно UTC. **substract** - отрицательное смещение, **add** - положительное смещение.
no clock timezone	Удалить настроенное смещение.
! В режиме глобальной конфигурации	

38.1.1 Пример конфигурации NTP

В сети расположены 2 сервера времени: один находится в активном режиме и используется, другой находится в режиме ожидания. На коммутаторе “**Switch A**” требуется синхронизировать локальное время.

Конфигурация коммутатора будет выглядеть следующим образом:

```
Switch(config)#ntp enable
Switch(config)#interface vlan1
Switch(config-if)#ip address 192.168.1.12/24
Switch(config)#interface vlan2
Switch(config-if)#ip address 192.168.2.12/24
Switch(config)#ntp server 192.168.1.11
Switch(config)#ntp server 192.168.2.11
```

38.2 Конфигурация SNTP

1. Включить SNTP клиент:

Команда	Описание
sntp enable **no sntp enable** *! В режиме глобальной конфигурации*	Включить функцию SNTP. Выключить функцию SNTP.

2. Настроить SNTP клиент:

Команда	Описание
sntp server {<ip-address>} [maxpoll <4-16>] [minpoll <4-16>] **no sntp server** {<ip-address>} [maxpoll | minpoll] *! В режиме глобальной конфигурации*	Задать IP-адрес SNTP-сервера. **maxpoll** - максимальное время синхронизации, по умолчанию 6; **minpoll** - минимальное время синхронизации, по умолчанию 4. Удалить SNTP-сервер.
sntp sync-retry *! В Admin режиме*	Запустить синхронизацию времени принудительно.

3. Отобразить информацию о конфигурации и синхронизации SNTP-серверов.:

Команда	Описание
show sntp statistics **show sntp logging-status** **show sntp peers** **show sntp peer-status** *! В Admin режиме*	Вывод информации о статусе SNTP в формате ntp. Отобразить статус подключения. Вывести список SNTP-серверов. Отобразить статус всех NTP-серверов.

4. Смещение часового пояса:

Команда	Описание
clock timezone <name> {add | substract} <0-23>	Задать смещение часового пояса относительно UTC. **substract** - отрицательное смещение, **add** - положительное смещение.
no clock timezone *! В режиме глобальной конфигурации*	Удалить настроенное смещение.

38.3 Пример конфигурации SNTP

На коммутаторе требуется синхронизировать локальное время с NTP сервером 192.168.1.11. Конфигурация коммутатора будет выглядеть следующим образом:

```
Switch#configure terminal
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.12/24
Switch(config-if)#exit
Switch(config)#sntp enable
Switch(config)#sntp server 192.168.1.11
```

39. Ограничение трафика в CPU

Для предотвращения высокой утилизации CPU коммутатора в следствии некорректного функционирования подключенного сетевого оборудования или атак типа DDOS, коммутатор поддерживает ограничение сетевого трафика, направляемого в CPU, по различным сетевым протоколам.

39.1 Отображение информации о трафике в CPU

Команда	Описание
show cpu-rx-ratelimit protocol <protocol-type> *! В Admin режиме*	Отобразить информацию о счетчиках и лимите для пакетов принимаемых в CPU. **<protocol-type>** - тип протокола: **all** - отображение всех протоколов; **arp** - протокол ARP; **bpdu** - STP BPDU; **bpdu-tunnel** - BPDU-Tunnel; **dai** - Dynamic ARP Inspection; **dhcp** - протокол DHCP; **igmp** - протокол IGMP; **l3-mtu-ttl** - пакеты с TTL=1 или размером больше L3 MTU; **l3-unrslvd** - пакеты с unresolved next-hop; **lacp** - протокол LACP; **lbd** - loopback detection; **lldp** - протокол LLDP; **local-ip** - трафик на локальные IP коммутатора; **mac-auth** - mac-authentication-bypass; **other** - все остальные пакеты; **pppoe** - протокол PPPoE; **packet-capture** - функционал packet-capture; **traffmon** - мониторинг трафика; **total** - суммарное количество пакетов отправленных в CPU. **uldp** - протокол ULDP;
clear cpu-rx protocol all *! В Admin режиме*	Очистить статистику всех пакетов принятых в CPU.

39.2 Настройка ограничений трафика в CPU

Команда	Описание
cpu-rx-ratelimit protocol <protocol-type> <packets>	Задать лимит пропускной способности. **<protocol-type>** - тип протокола; **<packets>** - пакетов в секунду.
no cpu-rx-ratelimit protocol <protocol-type>	Вернуть значение по умолчанию.
! В режиме глобальной конфигурации	

40. PoE (Power over Ethernet)

PoE (Power over Ethernet) - технология, позволяющая передавать удалённому устройству электрическую энергию вместе с данными через стандартную витую пару в сети Ethernet.

40.1 Настройка PoE

1. Глобальные настройки PoE:

Команда	Описание
power inline enable **no power inline enable** *! В режиме глобальной конфигурации*	Включить PoE глобально. На коммутаторах с PoE включено по умолчанию. Отключить PoE глобально.
power inline high-inrush enable **no power inline high-inrush enable** *! В режиме глобальной конфигурации*	Включить повышенный пусковой ток. Выключить повышенный пусковой ток. Установлено по умолчанию.
power inline max <W> **no power inline max** *! В режиме глобальной конфигурации*	Установить ограничение суммарной потребляемой энергии **<W>**. Вернуть значение по умолчанию.

2. Настройки PoE на портах:

Команда	Описание
power inline enable **no power inline enable** *! В режиме конфигурации порта*	Включить подачу питания на порте . На коммутаторах с PoE включено по умолчанию. Отключить на порте подачу питания.

Команда	Описание
power inline max <mW> **no power inline max** *! В режиме конфигурации порта*	Включить ограничение потребляемой энергии на отдельном порте. <mW> - значение в диапазоне 1-33000. Вернуть значение по умолчанию - 33000mW.
power inline priority { critical | high | low } *! В режиме конфигурации порта*	Установить приоритет питания для порта. В первую очередь питание подается на порты с уровнем Critical, затем на High, и, в последнюю очередь, на Low (по умолчанию все порты Low). При нехватке питания, PoE на портах с наименьшим приоритетом отключается. Если приоритеты равны, то отключается на порте со старшим номером.

3. Отображение состояния и настроек PoE:

Команда	Описание
show power inline [interface | interface <ifname>] *! В Admin режиме*	Отобразить настройки PoE, состояние всех интерфейсов **interface** или только выбранного интерфейса **interface <ifname>**.

4. Настройка и отображение состояния индикации PoE для коммутатора SNR-S5210G-24TX-POE:

Команда	Описание
poe-led-mode on **poe-led-mode off** *! В Admin режиме*	Включить индикацию PoE. В конфигурацию не сохраняется. Выключить индикацию PoE.
show poe-led-mode *! В Admin режиме*	Отобразить состояние индикации PoE.

41. Зеркалирование трафика RSPAN

Функция зеркалирования трафика **RSPAN (Remote Switch Port Analyzer)** позволяет дублировать отправляемый или принимаемый портом коммутатора трафик в контролирующий порт. К контролирующему порту может быть подключен анализатор трафика для диагностики проблем в сети. Функционал **RSPAN VLAN** позволяет зеркалировать трафик с различных портов в определенный VLAN.

1. Настройка порта для отправки зеркалируемого трафика:

Команда	Описание
monitor session <1-4> **destination interface** <if-name>	Задать интерфейс назначения **<if-name>** для сессии **1-4**. Допустимы только физические порты.
no monitor session <1-4> **destination interface** <if-name>	Удалить интерфейс назначения <if-name> для сессии 1-4.
! В режиме глобальной конфигурации	

2. Настройка портов с которых трафик будет зеркалироваться:

Команда	Описание
monitor session <1-4> **source interface** <if-list> {rx | tx | both}	Задать интерфейс(ы) **<if-list>** в качестве источника трафика зеркала для сессии **1-4** с указанием направления трафика: **rx** - входящий трафик; **tx** - исходящий трафик; **both** - оба направления. Допустимы только физические порты.
no monitor session <1-4> **source interface** <if-list>	Удалить источник трафика для сессии 1-4.
! В режиме глобальной конфигурации	

3. Настройка зеркалирования трафика в Vlan:

Команда	Описание
remote-span vlan <1-4094>	Назначить VLAN в качестве remote-span VLAN.
no remote-span vlan <1-4094>	Отменить установку VLAN в качестве remote-span VLAN.
! В режиме глобальной конфигурации	

Команда	Описание
monitor session <1-4> **remote vlan** <1-4094> **no monitor session** <1-4> **remote vlan** <1-4094> *! В режиме глобальной конфигурации*	Задать remote-span VLAN, в котором трафик будет зеркалироваться с source портов на destination порт. Отменить установку remote-span VLAN для зеркалируемого трафика.

4. Отображение настроек monitor session:

Команда	Описание
show monitor *! В Admin режиме*	Отобразить настройки зеркалирования трафика.

41.1 Пример конфигурации зеркала

Пример1: В порт ge1 необходимо дублировать исходящий трафик с порта ge9 и входящий на порт ge7.

Конфигурация коммутатора будет выглядеть следующим образом:

```
Switch(config)#monitor session 1 destination interface ge1
Switch(config)#monitor session 1 source interface ge9 tx
Switch(config)#monitor session 1 source interface ge7 rx
```

Пример2: В порт ge1 необходимо дублировать в Vlan 2 исходящий трафик с порта ge9 и входящий на порт ge7.

Конфигурация коммутатора будет выглядеть следующим образом:

```
Switch(config)#vlan 2
Switch(config)#remote-span vlan 2
Switch(config)#monitor session 1 destination interface ge1
Switch(config)#monitor session 1 source interface ge9 tx
Switch(config)#monitor session 1 source interface ge7 rx
Switch(config)#monitor session 1 remote vlan 2
```

42. Управление системой, мониторинг и отладка

42.1 Лицензирование

При загрузке коммутатора проверяется наличие на нём лицензионного ключа. В случае некорректного ключа либо его отсутствия после авторизации на коммутаторе в консоль будет выведено соответствующее предупреждение. Для ввода нового лицензионного ключа используется команда license в привилегированном режиме:

Команда	Описание
license	Ввод нового лицензионного ключа. После ввода команды необходимо вставить лицензионный ключ.
show license *! В Admin режиме*	Отобразить состояние лицензии на коммутаторе.

42.2 Show

Команды show могут быть применены для вывода информации о конфигурации, операциях и протоколах. В данной главе приведены команды show для общих функций коммутатора. Команды остальных функций приведены в соответствующих главах.

Следующие команды могут быть применены в Admin режиме, либо любом режиме конфигурации.

Команда	Описание
dir	Вывести информацию о содержимом flash-памяти.
show system resources	Вывести информацию об используемой памяти и ресурсах CPU.
show running-config [<parameters>]	Отобразить текущую конфигурацию коммутатора. В качестве **<parameters>** можно указать одну из доступных функций коммутатора для отображения её конфигурации.
show startup-config	Отобразить текущую загрузочную конфигурацию.
show interface <IFNAME>	Отобразить информацию о статусе интерфейса <IFNAME>.
show interface counter packet	Отобразить сводную статистику по количеству пройденных пакетов на интерфейсах.
show interface counter rate	Отобразить сводную статистику по скорости прохождения пакетов на интерфейсах.

Команда	Описание
show users	Отобразить информацию о пользователях, подключенных в данный момент.
show version	Отобразить информацию о коммутаторе.
show power	**Только для UPS и DC версии.** Отобразить информацию об используемом источнике питания, его состоянии, токе заряда/разряда и напряжении на АКБ.
show fan	Отобразить статус вентилятора (для моделей с вентилятором).
show temperature	Отобразить температуру.
show tech-support [page]	Вывести полную информацию о коммутаторе и его настройках.
show tcam usage	Вывести статистику TCAM.

42.3 DDM

DDM (Digital Diagnostic Monitor) реализует функцию диагностики по стандарту SFF-8472 MSA. **DDM** контролирует параметры сигнала и оцифровывает их на печатной плате оптического модуля. После чего информация может быть считана коммутаторов для мониторинга.

Обычно оптические модули поддерживают функцию DDM аппаратно, но её использование может быть ограничено программным обеспечением модуля. Устройства сетевого управления имеют возможность контролировать параметры (температура, напряжение, ток, мощности tx и rx) оптических модулей для получения их пороговых значений в режиме реального времени на оптическом модуле. Это помогает им обнаруживать неисправности в оптической линии, сокращать эксплуатационную нагрузку и повышать надежность сетевой системы в целом.

42.3.1 Просмотр информации DDM

Команда	Описание
show transceiver [<interface-list>] [detail] *! В Admin режиме*	Просмотр текущей информации о мониторинге состояния трансивера. При указании параметра **<interface-list>** информация будет отображена только для указанного интерфейса. **detail** - отобразить детальную информацию.

42.4 Управление вентиляторами

Изменить режим работы вентиляторов:

Команда	Описание
fanspeed auto *! В Admin режиме*	Включить автоматический режим работы вентиляторов.
fanspeed full *! В Admin режиме*	Включить режим работы вентиляторов на максимальной мощности.

42.5 System log

System log (системный журнал) представляет собой записи в текстовом формате о действиях и событиях в работе коммутатора. Все записи на данном коммутаторе подразделяются на четыре уровня срочности, в зависимости от которого может быть настроен вывод в определенный канал.

Коммутатор может выводить записи в следующие каналы:

- Консольный порт коммутатора - в этот порт происходит вывод записей всех уровней;
- В терминал telnet или ssh;
- В энергозависимую память RAM;
- В область журнала во FLASH-памяти;
- На удаленный хост.

Уровни срочности коммутатора соответствуют стандарту syslog UNIX систем.

Информация журнала делится на восемь уровней по степени срочности. Один уровень на одно значение и чем выше уровень записи журнала, тем меньше будет его значение. Правило, применяемое при фильтрации записей журнала по уровню срочности, заключается в следующем: выводятся только записи журнала с уровнем, равным или превышающим заданное значение. Поэтому фильтр уровня debugging включает все записи журнала.

42.5.1 Конфигурация system log

1. Настройка логирования:

Команда	Описание
logging logfile <0-7> **no logging logfile** *! В режиме глобальной конфигурации*	Задать уровень записываемых в файл на flash сообщений. Значение по умолчанию - 2 (critical). Выключить логирование сообщений в файл на flash.

Команда	Описание
logging buffer <0-7> **no logging buffer** *! В режиме глобальной конфигурации*	Задать уровень записываемых сообщений в RAM. Значение по умолчанию - 4 (warnings). Выключить логирование сообщений в RAM.
logging timestamp {microseconds | milliseconds | seconds} **no logging timestamp** *! В режиме глобальной конфигурации*	Задать точность записи времени сообщения. Вернуть значение по умолчанию (seconds).
logging console <0-7> **no logging console** *! В режиме глобальной конфигурации*	Задать уровень сообщений, выводимых в интерфейс консоли. Значение по умолчанию - 4 (warnings). Выключить логирование сообщений, выводимых в интерфейс консоли.
logging monitor <0-7> **no logging monitor** *! В режиме глобальной конфигурации*	Задать уровень сообщений, выводимых в интерфейс monitor. Значение по умолчанию - 4 (warnings). Выключить логирование сообщений, выводимых в интерфейс monitor.

2. Настройка логирования команд пользователя:

Команда	Описание
logging executed-commands [<0-7>] **no logging executed-commands** *! В режиме глобальной конфигурации*	Включить функцию логирования введенных пользователем команд и задать уровень <0-7>, с которым будут записаны эти сообщения. Если уровень в команде задан не будет, будет применен уровень по умолчанию - 2. Отключить функцию логирования введенных пользователем команд.

3. Просмотр и очистка лог-файла:

Команда	Описание
show logging logfile [**start-time** <date-time>] [**end-time** <date-time>] *! В Admin режиме*	Вывести все сообщения записанные в энергонезависимой памяти либо сообщения записанные в файл до даты указанной в **start-time** <date-time> и/или после даты указанной в **end-time** <date-time>. **<date-time>** - дата и время лог-файла в формате: <YYYY> <Month (Jan,Feb,Mar...)> <DD> <HH:MM:SS>.
show logging last <1-9999> *! В Admin режиме*	Просмотр последних <1-9999> сообщений записанных в файл.
clear logging logfile *! В режиме глобальной конфигурации*	Очистить лог-файл.

4. Просмотр сообщений в RAM:

Команда	Описание
show log [**start-time** <date-time>] [**end-time** <date-time>] *! В Admin режиме*	Вывести все сообщения записанные в RAM либо сообщения записанные в файл до даты указанной в **start-time** <date-time> и/или после даты указанной в **end-time** <date-time>. **<date-time>** - дата и время лог-файла в формате: <YYYY> <Month (Jan,Feb,Mar...)> <DD> <HH:MM:SS>.

5. Настроить сервер для отправки сообщений:

Команда	Описание
logging server {<ipv4-addr> | <hostname>} [level <0-7>] [facility {<local0 - local7> | user}] [transport udp port <1-65535>] **no logging** {<ipv4-addr> | <hostname>} *! В режиме глобальной конфигурации*	Настроить сервер для отправки логов: **<ipv4-addr> | <hostname>**) - задать IP-адрес сервера или имя хоста; **level** <0-7> - уровень логов; **facility** {<local0 - local7> | user} - источник сообщений; **transport udp port** <1-65535> - порт UDP. Удалить сервер для отправки логов.

6. Настройка формата времени в отправляемых syslog-сообщениях:

Команда	Описание
logging server time-format local	Задать передачу в syslog-сообщениях локального времени с установленным часовым поясом.
no logging server time-format local	Задать передачу в syslog-сообщениях времени в UTC.
! В режиме глобальной конфигурации	

7. Вывод информации о конфигурации:

Команда	Описание
show logging info	Просмотр общей информации о конфигурации логирования.
! В Admin режиме	
show logging console	Просмотр информации о конфигурации вывода сообщений в интерфейс консоли.
! В Admin режиме	
show logging monitor	Просмотр информации о конфигурации вывода сообщений в интерфейс terminal monitor.
! В Admin режиме	
show logging server	Просмотр информации о конфигурации отправки сообщений на сервер syslog.
! В Admin режиме	
clear logging buffer	Очистить сообщения хранимые в RAM.
! В режиме глобальной конфигурации	

42.6 Режим отладки

Для вывода отладочной информации необходимо включить соответствующий режим и вывод сообщений с уровнем 6 в требуемый тип лога. Например, logging console 6 для отображения debug сообщений в консоли (см. раздел "Конфигурация system log").

1. Настройка режима отладки для функционала **IGMP Snooping**:

Команда	Описание
debug igmp snooping brief	Включить отладочный режим IGMP Snooping.
no debug igmp snooping brief	Выключить отладочный режим IGMP Snooping.
! В Admin режиме	

2. Настройка режима отладки для функционала **DHCP Snooping**:

Команда	Описание
debug ip dhcp snooping {all | binding | event | packet | rx | tx}	Включить отладочный режим DHCP Snooping.
no debug ip dhcp snooping {all | binding | event | packet | rx | tx}	Выключить отладочный режим DHCP Snooping.
! В Admin режиме	

3. Настройка режима отладки для функционала **MAC Authentication Bypass**:

Команда	Описание
debug mab	Включить отладочный режим MAB.
no debug mab	Выключить отладочный режим MAB.
! В Admin режиме	

4. Настройка режима отладки при работе с **RADIUS-сервером**:

Команда	Описание
debug radius	Включить отладочный режим RADIUS.
no debug radius	Выключить отладочный режим RADIUS.
! В Admin режиме	

5. Настройка режима отладки при работе с ULDP:

Команда	Описание
debug uldp { all | event | rx | tx } [interface <if-name>]	Включить вывод отладочной информации на всех портах по типу сообщений: **all** - всех debug uldp сообщений; **event** - только debug uldp событий; **rx** - только входящих пакетов uldp; **tx** - только исходящих пакетов uldp. или на определённом **interface <if-name>**.
no debug uldp { all | event | rx | tx } [interface <if-name>]	Выключить вывод отладочной информации по типу сообщений на всех портах или на определённых.
! В Admin режиме	

6. Настройка режима отладки при работе с DHCPv6 Snooping:

Команда	Описание
debug ipv6 dhcp snooping	Включить отладочный режим DHCPv6 Snooping.
no debug ipv6 dhcp snooping	Выключить отладочный режим DHCPv6 Snooping.
! В Admin режиме	

7. Настройка режима отладки при работе с SAVI:

Команда	Описание
debug savi event	Включить отладочный режим SAVI.
no debug savi event	Выключить отладочный режим SAVI.
! В Admin режиме	

8. Вывод сообщений интерфейса monitor на терминал:

Команда	Описание
terminal monitor	Включить вывод сообщений интерфейса monitor на терминал.
terminal no monitor	Выключить вывод сообщений интерфейса monitor на терминал.
! В Admin режиме	

42.7 Dying Gasp

Функционал Dying Gasp предназначен для информирования администратора сети о внештатном прекращении подачи электропитания на коммутатор через отправку SNMP trap, Syslog-сообщений или ethernet OAM пакетов.

Для отправки пакетов **Dying Gasp** необходимо задать SNMP-сервер с отправкой SNMP trap и/или Syslog-сервер.

Пример настройки функционала Dying Gasp:

```
Switch(config)#snmp-server community private rw
Switch(config)#snmp-server enable traps
Switch(config)#snmp-server host 1.1.1.1 traps version 2c private
Switch(config)#logging server 2.2.2.2
```

Для отправки **OAMPDU Dying Gasp** пакетов необходимо применить на порте команду ethernet-oam.

Настройка отправки OAMPDU Dying Gasp:

Команда	Описание
ethernet-oam	Включить функцию OAM Dying Gasp на порте.
no ethernet-oam	Выключить функцию OAM Dying Gasp на порте.
! В режиме конфигурации порта	

Модели, поддерживающие функционал Dying Gasp:

- SNR-S5210G-24TX (hw version 1.2.0 и выше);
- SNR-S5210G-24TX-UPS (hw version 1.2.0 и выше);
- SNR-S5210G-24TX-POE;
- SNR-S5210G-24FX;
- SNR-S5210X-8F;
- SNR-S5210G-8TX;
- SNR-S5210G-8TX-POE;
- SNR-S5310G-48TX;
- SNR-S5310G-48TX-POE.

42.8 Отложенная перезагрузка

Перезагрузка коммутатора через заданное время может применяться для предотвращения потери управления коммутатором при ошибках конфигурации или для перезагрузки коммутатора в час наименьшей нагрузки для обновления ПО.

1. Настройка отложенной перезагрузки:

Команда	Описание
reload after [HH:MM:SS] [days <1-30>]	Настроить таймер, по истечению которого произойдет отложенная перезагрузка **HH:MM:SS** - задать время; **days <1-30>** - задать дни.
reload cancel *! В Admin режиме*	Отменить отложенную перезагрузку.

2. Просмотр настройки отложенной перезагрузки:

Команда	Описание
show reload *! В Admin режиме*	Отобразить настройку отложенной перезагрузки.

42.9 Диагностические утилиты

42.9.1 Ping

Ping — утилита для проверки целостности и качества соединений в сетях на основе TCP/IP.

Запуск утилиты ping:

Команда	Описание
ping <ip-address> [count <1-1000>] | [interval <100-10000>] | [size <1-65535>] *! В User или Admin режиме*	**ip-address** - IP-адрес удаленного хоста; **count** - количество эхо-запросов; **interval** - задержка перед отправкой следующего эхо-запроса в миллисекундах. **size** - количество байтов данных для отправки. По умолчанию, без указания дополнительных параметров, отправляется 5 эхо-запросов с интервалом в 1000мс.

42.9.2 Traceroute

Traceroute — команда предназначенная для определения маршрута следования данных.

Запуск утилиты traceroute:

Команда	Описание
traceroute {<dest-ip-addr> | <hostname>} [hops <1-255>] [source <sip-addr>] [timeout <100-10000>] *! В User или Admin режиме*	**dest-ip-addr** - IP-адрес назначения; **hostname** - имя хоста назначения; **hops** <1-255> - количество хопов; **source** <sip-addr> - альтернативный IP-адрес источника; **timeout** - время ожидания в миллисекундах.

42.9.3 iPerf3 клиент

iPerf3 - консольная клиент-серверная утилита, генерирующая TCP или UDP трафик для измерения пропускной способности сети.

Запуск утилиты iperf3:

Команда	Описание
iperf3 <A.B.C.D> | <hostname> [proto {udp | tcp}] [bandwidth <1-12>] [reverse] [time <10-600>] [length <1000-128000>] [tos <0-7>] *! В Admin режиме*	**<A.B.C.D>** - IP-адрес iperf3 сервера; **<hostname>** - доменное имя iperf3 сервера; **proto** {udp | tcp} - протокол UDP или TCP; **bandwidth** <1-12> - скорость трафика в Мбит/сек; **reverse** - реверсивный режим; **time** <10-600> - время теста в секундах; **length** <1000-128000> - длина буфера; **tos** <0-7> - тип обслуживания IP-пакетов.

По умолчанию, без указания дополнительных опций, команда будет запущена с протоколом TCP на 10 сек. и скоростью 10 Мбит/сек.

Для измерения пропускной способности со скоростью выше 10 Мбит/сек в обычном режиме или выше 5 Мбит/сек в reverse режиме необходимо увеличить значение `cpu-rx-ratelimit protocol local-ip`. Для обычного режима — 650, для режима reverse — 1200. После завершения работы с утилитой iperf3 необходимо вернуть значение по умолчанию командой:
`no cpu-rx-ratelimit protocol local-ip`.