NetVICE

Руководство по установке и настройке

Управляемые коммутаторы серии NetVICE

Фундамент вашей системы безопасности

Настройка безопасности сети

Отказоустойчивость сети

Автоматический поиск камер

Удалённая настройка

Содержание

1 Установка и подключение коммутатора Netvice

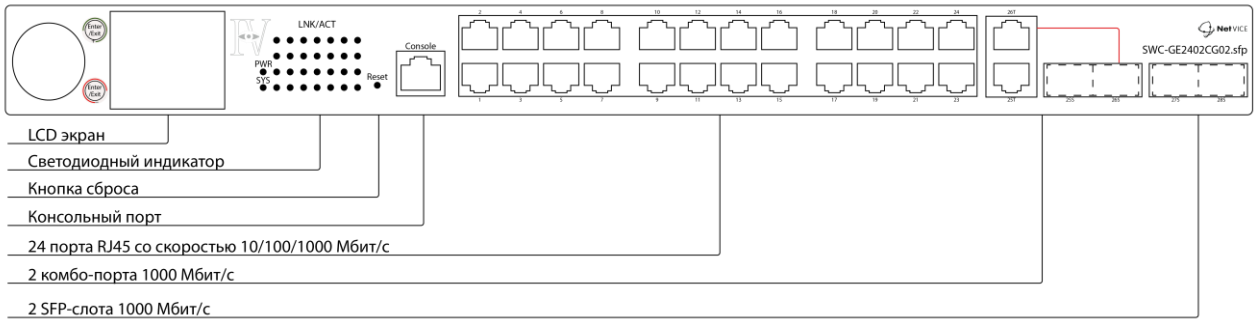
1.1 Передняя панель сетевого коммутатора

Коммутатор представляет собой многофункциональное сетевое устройство с различным количеством портов (16 / 24 / 48), предназначенное для построения корпоративных и операторских сетей.

Устройство оснащено:

- **16 (24 или 48) портами 10/100/1000 Мбит/с** — для подключения пользовательских устройств (ПК, IP-телефоны, точки доступа и др.);
- **2 комбинированными (Combo) портами 1000 Мбит/с** — позволяют использовать либо медный Ethernet-порт, либо оптический интерфейс;
- **2 портами SFP 1000 Мбит/с** — для подключения оптических линий связи и организации аплинков;
- **консольным портом** — для локального управления и первичной настройки устройства;
- **кнопкой сброса (Reset)** — для восстановления заводских настроек;
- **светодиодными индикаторами** — для отображения состояния портов, питания и активности устройства.
- **поворотной кнопкой управления (энкодером) —** для навигации по встроенному меню (в зависимости от модели) коммутатора и позволяет выполнять базовые операции без использования консоли или удаленного доступа: поворот влево/вправо — перемещение по пунктам меню, нажатие — выбор или подтверждение действия.

Такая конфигурация обеспечивает гибкость подключения, возможность масштабирования сети и удобство администрирования.



Значения светодиодных индикаторов:

Индикатор	Цвет	Описание
PWD	Зеленый	Индикатор не работает: коммутатор не включен Индикатор работает: коммутатор включен
System	Зеленый	Индикатор моргает: система работает Индикатор не работает: система загружается/коммутатор выключен
LNK/ACT	Зеленый	Индикатор не работает: отсутствует подключение сетевого устройства Индикатор работает: устройство подключено Индикатор моргает: подключенное устройство обменивается информацией
PoE	Оранжевый	Для коммутаторов со встроенным PoE. Индикатор не работает: устройство не использует PoE Индикатор работает: устройство использует POE

Данный коммутатор является универсальным решением для построения сетевой инфраструктуры различного масштаба, обеспечивая высокую скорость передачи данных, поддержку оптических соединений и удобные средства управления.

1.2 Задняя панель

Для подключения коммутатора к питающей сети используйте адаптер питания из комплекта поставки. Подключите сперва один конец адаптера питания к разъему питания на задней панели коммутатора, потом другой конец адаптера питания к розетке питающей сети.

Устройство предназначено для использования в местах с эквипотенциальным соединением, таких как центры телекоммуникаций, выделенные серверные комнаты или зоны с ограниченным доступом и др.

Коммутатор оснащен разъемом питания переменного тока (диапазон входного напряжения 100–240 В, 50/60 Гц) и отверстием для винта заземления:

Внимание! Устройство требует обязательного подключения к отдельной клемме защитного заземления. Монтаж должен предусматривать постоянное соединение с контуром заземления здания, выполняемое квалифицированным специалистом.

Клемма заземления. Коммутатор уже оснащен механизмом грозозащиты. Вы также можете заземлить коммутатор через жилу защитного заземления (PE) шнура питания переменного тока или с помощью отдельного кабеля заземления.

Разъем питания. Подключите гнездовой разъем шнура питания сюда, а штекер – к розетке переменного тока (AC). Пожалуйста, убедитесь, что напряжение источника питания соответствует требованиям входного напряжения.

1.3 Предупреждения и меры предосторожности

Во избежание повреждения оборудования и получения травм, вызванных неправильным использованием, соблюдайте следующие меры предосторожности:

- ✓ Перед очисткой коммутатора необходимо вытащить вилку шнура питания;
- ✓ Не используйте влажную ткань и жидкие средства для чистки коммутатора;
- ✓ Не включайте устройство в местах с повышенной влажностью и не допускайте попадания воды или влаги внутрь корпуса;
- ✓ Не размещайте коммутатор на неустойчивых поверхностях или столах – падение может привести к серьезным повреждениям устройства;
- ✓ Обеспечьте хорошую вентиляцию в помещении и следите за тем, чтобы вентиляционные отверстия коммутатора оставались открытыми;
- ✓ Для корректной работы подавайте на коммутатор надлежащее напряжение. Убедитесь, что рабочее напряжение сети соответствует указанному на устройстве;

✓ Во избежание поражения электрическим током не вскрывайте корпус самостоятельно; в случае возникновения неисправности обратитесь к квалифицированному обслуживающему персоналу.

Внимание! В случае возникновения неисправности обратитесь к квалифицированному обслуживающему персоналу!

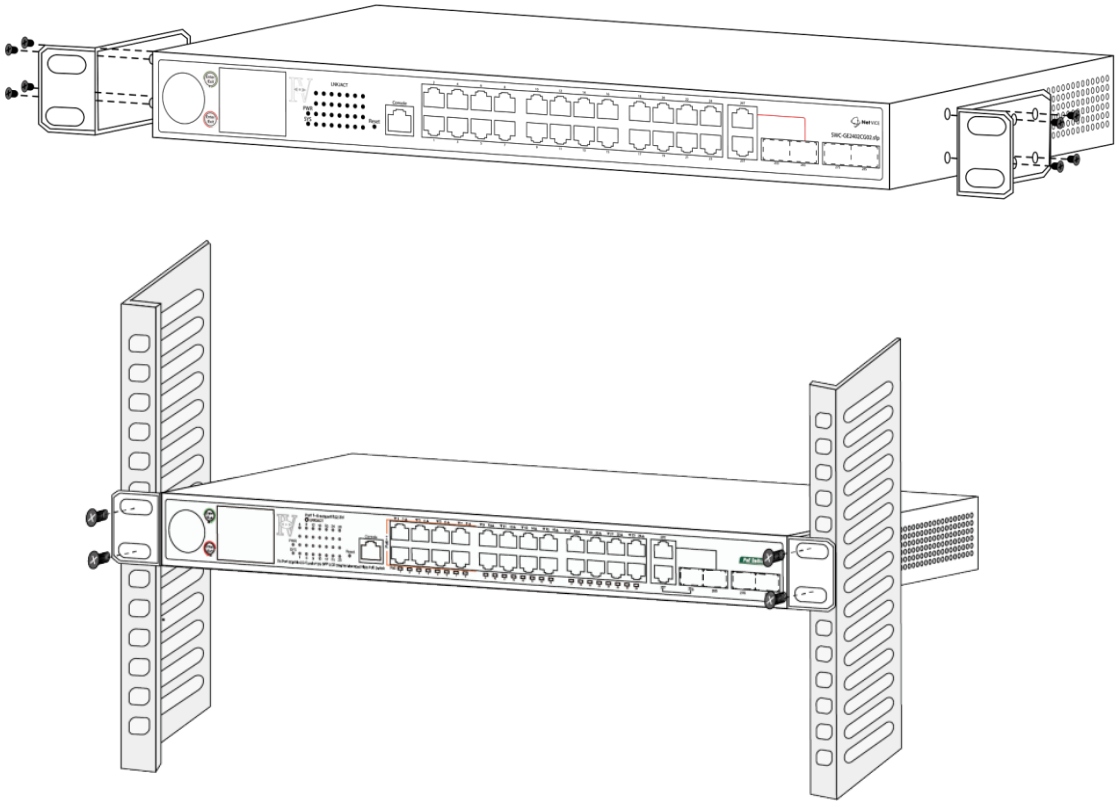
1.4 Установка коммутатора

- **На рабочую поверхность:**

✓ Поместите нижнюю часть коммутатора на достаточно большой и устойчивый стол;
✓ Снимите защитный слой с клейких ножек, идущих в комплекте, и приклейте их в пазы на дне корпуса для защиты от внешних вибраций;
✓ Аккуратно установите коммутатор на рабочую поверхность;

- **В шкаф 19”:**

✓ Проверьте заземление и устойчивость 19-дюймового шкафа EIA;
✓ Винтами закрепите монтажные «ушки» по бокам передней панели коммутатора;
✓ Установите коммутатор на кронштейны в шкафу и сдвиньте по направляющим в нужное положение;
✓ Затем винтами закрепите «ушки» на стойках шкафа, обеспечив надежную фиксацию устройства.



2 Базовые команды для настройки коммутатора

В данной инструкции рассмотрен только базовый функционал коммутатора, достаточные для развертывания и базовой эксплуатации сети, однако не включает полный перечень всех поддерживаемых функций устройства. Дополнительные возможности устройства могут отличаться в зависимости от модели и версии программного обеспечения и требуют отдельного рассмотрения.

Внимание! Монтажные кронштейны служат только для фиксации, а основной вес устройства должен приходиться на опорные полки или уголки шкафа.

2.1 Строка аутентификации (authentication line)

Команда позволяет настраивать методы аутентификации для консоли (Console), удаленного доступа (VTY) и веб-интерфейса (Web) по отдельности. Методом аутентификации может быть любой из перечисленных или их комбинация: Local (локально), RADIUS и TACACS.
При комбинированной настройке приоритет отдается методам слева направо. Если пользователь успешно прошел проверку одним методом, методы с более низким приоритетом (расположенные правее) игнорируются. Для входа в систему пользователю достаточно пройти проверку любым из настроенных методов.
Перед использованием RADIUS-аутентификации необходимо настроить функции AAA и сам RADIUS-сервер. Если настроена локальная аутентификация, но локальный пользователь не создан, пользователь все равно сможет войти в систему через консольное подключение.

Все типы подключений поддерживают следующие методы:
- Local: использование локальной базы данных учетных записей пользователей - для проверки.
- Tacacs: аутентификация через удаленный сервер TACACS.
- Radius: аутентификация через удаленный сервер RADIUS.

Команда с приставкой «**no**» сбрасывает настройки аутентификации к значениям по умолчанию. Параметры и примеры использования описаны в таблице:

Команда	**authentication line {console | vty | web} login {local | radius | tacacs} no authentication line {console | vty | web} login**	
Параметр	**console**	Вход в систему коммутатора через консольный порт
	vty	Вход в систему коммутатора через SSH или Telnet
	web	Вход в систему коммутатора через веб-интерфейс
Настройка по умолчанию	Для входа через консольный порт метод аутентификации не настроен. Для входа через VTY (удаленный доступ, например SSH/Telnet) и через веб-интерфейс по умолчанию включена локальная аутентификация	
Режим	Глобальный режим	
Пример использования	Настройка методов входа по Telnet и SSH на использование локальной (Local) и RADIUS аутентификации: **Switch(config)# authentication line vty login local radius lists**	

2.2 Сообщение после успешной аутентификации (banner motd)

Команда используется для настройки информации (сообщения), которая отображается при успешной аутентификации пользователя Telnet или консоли.
Команда с приставкой «**no**» сбрасывает настройки аутентификации к значениям по умолчанию. Параметры и примеры использования описаны в таблице:

Команда	**banner motd<LINE> no banner motd**	
Параметр	**<LINE>**	Информация, которая выводится при успешном прохождении аутентификации; ограничение по длине от 1 до 100 символов
Настройка по умолчанию	Не показывать информацию (сообщение) при успешном прохождении аутентификации	
Режим	Глобальный режим	
Пример использования	Вывести сообщение: «**Welcome**», после успешной аутентификации: **Switch(config)# banner motd Welcome**	

2.3 Выбор файла прошивки (boot img)

Команда используется для настройки первого и второго файлов образа (img), которые будут использоваться коммутатором при следующей загрузке. В качестве первого и второго образов можно использовать только файлы с расширением .img, хранящиеся в памяти коммутатора.

Команда	**boot img <img-file-url> {primary | backup}**	
Параметр	**<img-file-url>**	Информация, которая выводится при успешном прохождении аутентификации; ограничение по длине от 1 до 100 символов
	primary	Первая запись (путь) для файла образа
	backup	Вторая запись (путь) для файла образа
По умолчанию	Заводская конфигурация по умолчанию определяет только первый загрузочный файл (IMG) – это файл nos.img, находящийся во флеш-памяти (FLASH). Второй загрузочный файл при этом не назначен	
Режим	Глобальный режим	
Пример использования	Установите файл flash:/nos.img в качестве второго загрузочного образа (IMG), который будет использоваться при следующей загрузке коммутатора: **Switch# boot img flash:/nos.img backup**	

2.4 Загрузочный файл конфигурации (boot startup-config)

Команда используется для настройки файла конфигурации (CFG), который будет использоваться при следующей загрузке коммутатора. Для настройки загрузки могут быть использованы только те файлы с расширением .cfg, которые уже хранятся в памяти коммутатора.

Команда	**boot startup-config {NULL | <file-url>}**	
Параметр	**NULL**	Использовать заводскую конфигурацию по умолчанию в качестве загрузочной конфигурации при следующей перезагрузке
	<file-url>	Полный путь к файлу конфигурации (.cfg), который будет использоваться при следующей загрузке
По умолчанию	Отсутствует	
Режим	Режим администратора	
Пример использования	Установка flash:/startup.cfg в качестве конфигурационного файла (CFG): **Switch# boot startup-config flash:/ startup.cfg**	

2.5 Настройка времени (clock set)

Команда используется для настройки системного времени и даты коммутатора. Коммутатор не может продолжать отсчет времени при выключении питания, поэтому в условиях, где требуется точное время, дату и время необходимо устанавливать заново после каждого включения.

Команда	**clock set <HH:MM:SS> <YYYY.MM.DD>**

Параметр	**<HH:MM:SS>**	Время: допустимый диапазон для часов (HH) — от 0 до 23, для минут (MM) и секунд (SS) — от 0 до 59
	<YYYY.MM.DD>	Год, месяц и дата: допустимый диапазон для года (YYYY) — с 1970 по 2038, для месяца (MON) — с 1 до 12, для числа (DD) — с 1 по 31
По умолчанию	По умолчанию при первом запуске установлено время: 1 января 2006 года, 00:00:00	
Режим	Режим администратора	
Пример использования	Установить текущую дату и время коммутатора на 1 августа 2002 года, 23:00:00: **Switch# clock set 23:0:0 2002.8.1**	

2.6 Режим настройки (config)

Команда используется для перехода из режима административного управления в режим глобальной конфигурации.

Команда	**config [terminal]**	
Параметр	**[terminal]**	Указывает на конфигурацию терминала
По умолчанию	Отсутствует	
Режим	Режим администратора	
Пример использования	Перевести коммутатор в режим глобальной настройки: **Switch# config**	

2.7 Выход из режима администратора (disable)

Команда используется для выхода из режима администратора обратно в режим обычного пользователя.

Команда	**disable**
Параметр	**Отсутствует**
По умолчанию	Отсутствует
Режим	Режим администратора
Пример использования	Выход из режима администратора в режим пользователя: **Switch# disable** **Switch#**

2.8 Вход в режим администратора (enable)

Команда используется для перехода из режима пользователя в режим администратора или для изменения уровня привилегий пользователей.
Чтобы предотвратить несанкционированный доступ лиц, не являющихся администраторами, при переходе из пользовательского режима в режим администратора требуется аутентификация, т. е. необходимо ввести пароль администратора.
Если введен верный пароль администратора, предоставляется доступ к режиму администратора. Если пароль введен неправильно 3 раза подряд, устройство остается в пользовательском режиме.
При повышении уровня привилегий пользователя с низкого на высокий требуется подтверждение паролем соответствующего уровня, в противном случае аутентификация не будет пройдена.

Команда	**enable**
Параметр	**Отсутствует**
По умолчанию	Отсутствует
Режим	Режим администратора
Пример использования	Войти в режим управления из пользовательского режима: **Switch# enable** **Switch#**

2.9 Возврат к режиму администратора (end)

Команда используется для выхода из различных режимов настройки.

Команда	**end**
Параметр	**Отсутствует**
По умолчанию	Отсутствует
Режим	Режим администратора/пользователя
Пример использования	Выход с режима настройки VLAN на режим администратора **Switch(config-vlan1)# end** **Switch#**

2.10 Время активного сеанса администратора (exec-timeout)

Команда используется для настройки времени ожидания (тайм-аута) выхода из режима администратора.
По истечении времени ожидания происходит выход из режима управления. Для повторного входа потребуется снова ввести команду управления и пароль.
Если установить значение тайм-аута на 0, таймер ожидания будет отключен (автоматический выход не произойдет).

Команда	**exec-timeout <minutes> [<seconds>]** **no exec-timeout**	
Параметр	**<minutes>**	Значение времени указывается в минутах и находится в диапазоне от 0 до 35 791
	[<seconds>]	Значение времени указывается в секундах и находится в диапазоне от 0 до 59
По умолчанию	По умолчанию значение 10 минут	
Режим	Глобальный режим	
Пример использования	Установка значения тайм-аута режима администратора на 5 минут 30 секунд: **Switch(config)# exec-timeout 5 30**	

2.11 Выход из текущего режима и возврат в предыдущий режим настройки (exit)

Команда используется для выхода из текущего режима и возврата в предыдущий режим.

Команда	**exit**
Параметр	Отсутствует
По умолчанию	Отсутствует
Режим	Все режимы
Пример использования	Выйти из глобального режима в предыдущий режим: **Switch(config-vlan1)# end** **Switch#**

2.12 Справочная информация (help)

Мгновенная оперативная помощь (справка), предоставляемая коммутатором. Команда «**help**» отображает информацию по всей справочной системе, включая как полную, так и частичную справку.

Команда	**help**
Параметр	Отсутствует
По умолчанию	Отсутствует
Режим	Все режимы
Пример использования	Получить справочную информацию в глобальном режиме: **Switch(config)# help**

*Интерфейс командной строки (CLI) поддерживает расширенную систему контекстной справки. Для получения помощи введите символ «**?**» в любой момент набора команды. Если совпадения отсутствуют, список справки будет пуст. В этом случае следует удалить часть введённой команды до появления доступных вариантов при вводе «**?**».*

2.13 Имя хоста (hostname)

Команда изменяет название узла (хоста).

Команда	**hostname**
Параметр	Отсутствует
По умолчанию	Отсутствует
Режим	Глобальный режим
Пример использования	Установить имя узла «Test»: **Switch(config)# hostname Test** **Test(config)#**

2.14 Статическая привязка узла к IP-адресу (ip host)

С помощью этой команды вы можете установить связь (маппинг) между именем хоста и IP-адресом.

Команда	**ip host <hostname> <ip_addr>** **no ip host {<hostname>|all}**	
Параметр	**<hostname>**	Строка для названия устройства, допускается до 64 символов
	<ip_addr>	Соответствующий IP-адрес для имени хоста указывается в формате десятичных чисел, разделенных точками
	all	Весь список имен узлов
По умолчанию	Отсутствует	
Режим	Глобальный режим	
Пример использования	Установить IP-адрес 200.121.1.1 для узла с именем (hostname) «Irkutsk»: **Switch(config)# ip host Irkutsk 200.121.1.1**	

2.15 Статическая привязка узла к IPv6-адресу (ipv6 host)

Команда позволяет настроить сопоставление (маппинг) имени хоста с IPv6-адресом. Созданная ассоциация может быть использована в других командах, например, «**ping <имя_хоста>**».

Команда	**ipv6 host <hostname> <ipv6_addr>** **no ipv6 host {<hostname> | all}**	
Параметр	**<hostname>**	Строка для названия устройства, допускается до 64 символов
	<ip_addr>	Соответствующий IPv6-адрес для имени хоста; указывается в формате десятичных чисел, разделенных точками
	all	Весь список имен узлов
По умолчанию	Отсутствует	
Режим	Глобальный режим	
Пример использования	Установить IPv6-адрес 2001:1:2:3::1 для узла с именем (hostname) «Irkutsk»: **Switch(config)# ipv6 host Irkutsk 2001:1:2:3::1**	

2.16 Включение функции веб-сервера (ip http server)

Используйте эту команду для включения веб-конфигурации (управления через браузер). Команда «**no ip http server**» отключает возможность настройки через веб-интерфейс.

Команда	**ip http server** **no ip http server**
Параметр	Отсутствует
По умолчанию	Включена
Режим	Глобальный режим
Пример использования	Включить функцию веб-сервера и разрешить конфигурацию через веб-интерфейс: **Switch(config)# ip http server**

2.17 Аутентификация пользователя коммутатора (login)

При использовании этой команды пользователи должны будут вводить пароль, установленный командой «**password**», чтобы войти в обычный пользовательский режим через консоль. Подробнее в разделе *2.18 Установка пароля коммутатора (password)*. Команда «**no login**» отменяет это ограничение.

Команда	**login** **no login**
Параметр	Отсутствует
По умолчанию	Без пароля
Режим	Глобальный режим
Пример использования	Включить пароль: **Switch(config)# login**

2.18 Установка пароля коммутатора (password)

С помощью этой команды установите пароль, используемый для входа в обычный пользовательский режим через консоль. Команда «**no password**» удаляет этот пароль.

Команда	**password [0 | 7] <password>** **no password**	
Параметр	**[0 | 7]**	При выборе параметра 0 пароль сохраняется без шифрования; при выборе параметра 7 пароль сохраняется в зашифрованном виде
	<password>	Пароль пользователя
По умолчанию	Пароль пустой	
Режим	Глобальный режим	
Пример использования	Настройте пароль без шифрования «test» для входа в обычный пользовательский режим: **Switch(config)# password 0 test**	

2.19 Права доступа (privilege)

Используйте эту команду для настройки уровня привилегий (прав доступа) для указанной команды. Данная функция не изменяет саму команду.
Параметр «**LINE**» должен содержать полную форму команды. Сокращенная форма допускается только в том случае, если она однозначно распознается системой.
Можно настроить уровень привилегий для команды с приставкой «**no**», однако, это не влияет на результат выполнения команды. При использовании отрицательной формы (добавление

«**no**» перед основной командой) параметр «**LINE**» должен точно соответствовать уже настроенной командной строке.
Если командная строка содержит параметры, они должны полностью совпадать с параметрами ранее настроенной команды.
Команда «**no**» (в начале строки конфигурации) восстанавливает исходный уровень привилегий команды.

Команда	**privilege mode level <1-15> LINE** **no privilege mode level <1-15> LINE**	
Параметр	**mode**	Режим регистрации команды. Для просмотра всех доступных режимов используйте клавишу «**Tab**» или символа «**?**»
	<1-15>	Уровень (приоритета/права доступа) может быть задан в диапазоне от 1 до 15
	LINE	Указывает команду для конфигурации. Система поддерживаетт польз использование сокращенных форм (аббревиатур) команд
По умолчанию	Отсутствует	
Режим	Глобальный режим	
Пример использования	Измените уровень команды show ip route на уровень 5: **Switch(config)# privilege exec level 5 show ip route** Восстановите исходный уровень команды show ip route: **Switch(config)# no privilege exec level 5 show ip route**	

2.20 Перезагрузка (reload)

Пользователь может использовать эту команду для перезагрузки коммутатора.

Команда	**reload**
Параметр	Отсутствует
По умолчанию	Отсутствует
Режим	Режим администратора
Пример использования	Горячая перезагрузка коммутатора: **Switch(config)# reload**

2.21 Шифрование паролей (service password-encryption)

Команда обеспечивает шифрование всех текущих незашифрованных паролей и любых новых паролей, заданных через команды «**password**», «**enable password**», «**ip ftp password**» и «**username**». Команда «**no service password-encryption**» отключает шифрование паролей, при этом уже все зашифрованные пароли сохраняются в зашифрованном виде.

Команда	**service password-encryption** **no service password-encryption**
Параметр	Отсутствует
По умолчанию	Шифрование паролей отключено
Режим	Глобальный режим
Пример использования	Шифрование системных паролей: **Switch(config)# service password-encryption**

2.22 Количество отображаемых столбцов (service terminal-length)

Команда позволяет настроить количество столбцов (символов), отображаемых на каждом экране терминала. Количество отображаемых символов (столбцов) для клиентов Telnet/SSH и консоли будет соответствовать данной конфигурации. Команда «**no service terminal-length**» отключает разбиение вывода на страницы (прокрутку экранов).

Команда	**service terminal-length <0-512>** **no service terminal-length**	
Параметр	**<0-512>**	Количество столбцов (символов), отображаемых на каждом экране VTY; значение задается в диапазоне от 0 до 512
По умолчанию	Отсутствует	
Режим	Глобальный режим	
Пример использования	Установить количество потоков (сессий) VTY равным 20: **Switch(config)# service terminal-length 20**	

2.23 Контактные данные производителя (sysContact)

С помощью этой команды пользователь может установить контактные данные производителя для конкретного устройства. Команда «**no sysContact**» возвращает настройки контактной информации к заводским значениям.

Команда	**sysContact <LINE>** **no sysContact**	
Параметр	**<LINE>**	Строка, используемая в качестве приглашения или текста, содержащая от 0 до 255 символов
По умолчанию	Заводские настройки	
Режим	Глобальный режим	
Пример использования	Установить контактные данные производителя в режим «test»: **Switch(config)# sysLocation test**	

2.24 Сброс на заводские настройки (set default)

Команда выполняет сброс конфигурации коммутатора к заводским настройкам. В результате все параметры, настроенные пользователем, будут удалены. После перезагрузки коммутатора приглашение командной строки будет соответствовать состоянию устройства при первом включении.

Команда	**Set default**
Параметр	Отсутствует
По умолчанию	Отсутствует
Режим	Режим администратора
Пример использования	Вернуть коммутатор к заводским настройкам: **Switch# set default** *Are you sure? [Y/N] = y* **Switch# write Switch#reload**

*После ввода данной команды следует выполнить команду «**write**», для сохранения конфигурации. Восстановление заводских настроек произойдёт после перезагрузки устройства.*

2.25 Загрузочный пароль (set boot password)

В режиме IMG (режим работы с образом) данная команда используется для настройки пароля входа в режим BootROM при следующей загрузке устройства.
В глобальном режиме после ввода команды необходимо задать пароль в соответствии с запросом системы и подтвердить его для завершения настройки. Длина пароля должна составлять от 3 до 32 символов. Команда с приставкой «**no**» удаляет установленный пароль.

Команда	**set boot password** **no set boot password**
Параметр	Отсутствует
По умолчанию	Отсутствует
Режим	Глобальный режим
Пример использования	Устанавливает пароль для входа в режим загрузки (boot mode): **Switch(config)# set boot password** New password :***** Confirm password :***** Set password success

2.26 Быстрая настройка (setup)

Коммутатор поддерживает режим быстрой настройки (Setup Mode), предназначенный для конфигурирования IP-адреса и основных параметров устройства.

Команда	**setup**
Параметр	Отсутствует
По умолчанию	Отсутствует
Режим	Режим администратора
Пример использования	Войти в режим быстрой настройки: **Switch# setup**

2.27 Демонстрация системного времени (show clock)

Показывает текущее системное время.

Команда	**show clock**
Параметр	Отсутствует
По умолчанию	Отсутствует
Режим	Режим администратора
Пример использования	Показать текущее системное время: **Switch# show clock**

2.28 Загрузка процессора (show cpu usage)

Команда отображает текущую загрузку центрального процессора (CPU), а также средние значения за последние 5 секунд, 30 секунд и 5 минут.
Параметр «**slotno**» используется только на шассийных коммутаторах для отображения загрузки CPU модуля, установленного в указанном слоте. Если параметр не указан, по умолчанию отображаются данные для текущего модуля.

Команда	**show cpu usage [<slotno>]**	
Параметр	**[<slotno>]**	Выбор слотов

По умолчанию	Отсутствует
Режим	Глобальный и режим администратора
Пример использования	Показать текущий уровень загрузки центрального процессора (ЦП): **Switch# show cpu usage** *Last 5 second CPU IDLE: 87%* *Last 30 second CPU IDLE: 89%* *Last 5 minute CPU IDLE: 89%* *From running CPU IDLE: 89%*

2.29 Коэффициент утилизации процессора (show cpu utilization)

Команда используется для отображения коэффициента утилизации центрального процессора (CPU) за последние 5 секунд, 30 секунд и 5 минут.

Команда	**show cpu utilization**
Параметр	Отсутствует
По умолчанию	Отсутствует
Режим	Режим администратора
Пример использования	Отображает коэффициент утилизации центрального процессора: **Switch# show cpu utilization** *Last 5 second CPU USAGE: 9%* *Last 30 second CPU USAGE: 11%*

2.30 Использование памяти (show memory usage)

Команда отображает текущий уровень использования памяти устройства.
Параметр «**slotno**» применяется только на шассийных коммутаторах и предназначен для вывода информации об использовании памяти модуля, установленного в указанном слоте. Если параметр не указан, по умолчанию отображаются данные для текущего модуля.

Команда	**show memory usage [<slotno>]**	
Параметр	**[<slotno>]**	Выбор слотов
По умолчанию	Отсутствует	
Режим	Режим администратора	
Пример использования	Показать текущий уровень загрузки памяти: **Switch# show memory usage** *The memory total 128 MB, free 58914872 bytes, usage is 56.10%*	

2.31 Просмотр уровня привилегий пользователя (show privilege)

Показывает права доступа для текущего пользователя.

Команда	**show privilege**
Параметр	Отсутствует
По умолчанию	Отсутствует
Режим	Глобальный режим
Пример использования	Показать права текущего пользователя: **Switch(config)# show privilege** *Current privilege level is 15*

2.32 Просмотр уровня привилегий команды (show privilege mode LINE)

Команда отображает уровень прав доступа (привилегий) для указанной команды.
Параметр «**LINE**» должен содержать полную форму команды. Сокращённая форма допускается только в том случае, если она однозначно распознаётся системой.
Для незавершённых (неполностью введённых) команд, команд сохранения (записи), а также команд, сокращённая форма которых не может быть однозначно интерпретирована, отображение уровня привилегий невозможно.

Команда	**privilege mode level <1-15> LINE** **no privilege mode level <1-15> LINE**	
Параметр	**mode**	Режим регистрации команды; для отображения всех доступных режимов используйте клавишу «**Tab**» или символ «**?**»
	LINE	Указывает команду, для которой выполняется настройка
По умолчанию	Отсутствует	
Режим	Глобальный и режим администратора	
Пример использования	Показать уровень прав доступа для указанной команды: **Switch(config)# show privilege exec show ip route** **The command: show ip route** *Privilege is: 15*	

2.33 Информация для технической поддержки (show tech support)

Команда используется для сбора диагностической информации при возникновении сбоев в работе коммутатора.
Она отображает текущие рабочие параметры и состояние задач устройства.

Команда применяется техническими специалистами для анализа и проверки корректности функционирования коммутатора.

Команда	**show tech-support [no-more]**	
Параметр	**[no-more]**	Команда отображает рабочую информацию и состояние задач коммутатора напрямую, без прерывания вывода подсказкой «**more**»
По умолчанию	Отсутствует	
Режим	Глобальный и режим администратора	
Пример Использования	Отображает рабочую информацию и статус задач коммутатора: **Switch# show tech-support**	

2.34 Версия устройства (show version)

Команда используется для отображения информации о версии коммутатора, включая версию аппаратного обеспечения и версию программного обеспечения.

Команда	**show version**
Параметр	Отсутствие
По умолчанию	Отсутствие
Режим	Глобальный и режим администратора
Пример использования	Показать информацию о версии коммутатора: **Switch# show version**

2.35 Добавление пользователя (username)

Команда предназначена для настройки имени пользователя, пароля для локального входа и уровня его привилегий.
На устройстве может быть настроено не более 16 локальных пользователей. Максимальная длина пароля — до 32 символов.
После завершения настройки пользователь может войти в систему с указанным именем и соответствующим уровнем привилегий. Перед вводом команды «**authentication line console login local**» необходимо убедиться, что настроен как минимум один пользователь с уровнем привилегий 15. Это требуется для обеспечения возможности входа в систему и внесения изменений в конфигурацию в привилегированном и глобальном режимах.
Если пользователи с уровнем привилегий 15 не настроены, но для входа через консоль выбрана локальная аутентификация (Local), доступ к коммутатору будет предоставляться без проверки подлинности (без запроса пароля). При использовании HTTP-доступа вход в систему разрешён только пользователям с уровнем привилегий 15. Пользователям с другими уровнями будет отказано в доступе.
Команда с приставкой «**no**» удаляет указанного пользователя.

Команда	**username <username> [privilege <privilege>] [password [0 | 7] <password>]** **no username <username>**	
Параметр	**<username>**	Имя пользователя. Длина не должна превышать 32 символа
	<privelege>	Максимальный уровень привилегий команд, которые пользователь может выполнять. Диапазон значений — от 1 до 15; значение по умолчанию — 1
	[0 | 7]	Режим хранения пароля. [**0**] – пароль сохраняется без шифрования, [**7**] – пароль сохраняется в зашифрованном виде
	<password>	Пароль для пользователя
По умолчанию	Отсутствует	
Режим	Глобальный режим	
Пример использования	Настройте учетную запись администратора с именем admin и уровнем привилегий 15: **Switch(config)# username admin privilege 15 password 0 admin** Настройте две обычные учетные записи с уровнем привилегий 1. После этого включите метод локальной аутентификации: **Switch(config)# username user1 privilege 1 password 74a7d1ed414474e4033ac29ccb8653d9b** **Switch(config)# username user2 password 0 user2** **Switch(config)# authentication line console login local**	

2.36 Настройка доступа к веб-интерфейсу (web-auth privilege)

Команда предназначена для настройки уровня привилегий, необходимого для входа в коммутатор через веб-интерфейс. После установки требуемого уровня веб-доступа вход через браузер будет разрешён только пользователям, чей уровень привилегий равен указанному значению или превышает его.

Команда	**web-auth privilege <1-15>** **no web-auth privilege**	
Параметр	**<1-15>**	Задаёт уровень привилегий для входа в коммутатор через веб-интерфейс. Допустимый диапазон значений — от 1 до 15
По умолчанию	Уровень 15	
Режим	Глобальный режим	
Пример использования	Настройка уровня доступа 10 для веб-интерфейса: **Switch(config)# web-auth privilege 10**	

2.37 Сохранение конфигурации (write)

Команда используется для сохранения текущей конфигурации устройства в энергонезависимую память (Flash-память) память, что позволяет системе автоматически восстановить настройки в случае перезагрузки, случайного выключения или сбоя электропитания. Команду следует выполнить после завершения настройки всех необходимых функций.
При выполнении команды действующая сохранённая конфигурация перезаписывается. После выполнения команды текущие настройки будут сохранены и применены при следующей перезагрузке коммутатора.

Команда	**write**
Параметр	Отсутствие
По умолчанию	Отсутствие
Режим	Режим администратора
Пример использования	Сохранение текущих настроек во Flash-память: **Switch# write**

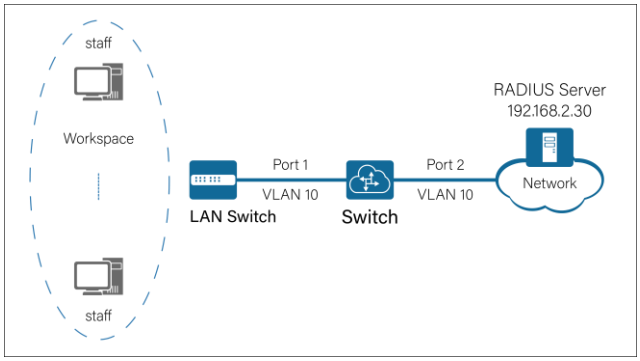
2.38 Сохранение текущей конфигурации (write running-config)

Команда предназначена для сохранения текущей рабочей конфигурации (running-config) во Flash-память в виде файла с расширением .cfg. Путь к файлу состоит из двух частей: префикса устройства, используемого в качестве корневого каталога (например, flash:/), и имени файла. Пробелы внутри каждой части пути и между ними не допускаются.
Все имена файлов должны иметь расширение .cfg. Длина полного пути к файлу не должна превышать 128 символов, при этом длина имени файла — не более 80 символов.

Команда	**write running-config [<startup-config-file-name>]**	
Параметр	**[<startup-config-file-name>]**	Полный путь к файлу конфигурации (.cfg)
По умолчанию	Отсутствует	
Режим	Режим администратора	
Пример использования	Сохранить текущую рабочую конфигурацию как файл конфигурации с именем 123.cfg: **Switch# write running-config 123.cfg**	

3 Функции коммутатора

3.1 Контроль доступа по стандарту IEEE 802.1X



Терминал в офисном помещении компании подключается к внутренней сети через коммутатор. В случае несанкционированного или незаконного доступа существует риск нарушения работы корпоративной бизнес-системы и утечки ключевых информационных активов. Для повышения безопасности внутренней сети администратор рассчитывает на использование коммутатора для контроля прав доступа пользователей. Протокол IEEE 802.1X позволяет реализовать аутентификацию пользователей на уровне порта, что обеспечивает безопасный доступ к сети только авторизованным устройствам и пользователям.

План конфигурации IEEE 802.1X на коммутаторе

В данном примере рассматривается настройка **главного коммутатора** для аутентификации пользователей через RADIUS-сервер с использованием протокола 802.1X. Конфигурация LAN-коммутатора и самого RADIUS-сервера здесь не описывается.

Задачи:

- Создание и настройка группы RADIUS-серверов.
- Настройка схемы AAA и домена аутентификации.
- Установка метода аутентификации dot1x в домене аутентификации для аутентификации пользователей через RADIUS-сервер.

Этапы работы:

Шаг 1. Создание VLAN и настройка интерфейсов. Создайте VLAN 10 и настройте интерфейсы ethernet 1/0/1-2 как access-порты в VLAN 10:

```
Switch(config)# vlan 10
Switch(config)# interface ethernet 1/0/1-2
Switch(config-if-port-range)# switchport access vlan 10
Switch(config-if-port-range)# exit
```

Шаг 2. Настройка RADIUS-сервера и AAA. Создайте и настройте RADIUS-сервер и схему аутентификации AAA:

```
Switch(config)# radius-server key 0 abc
Switch(config)# radius-server authentication host 192.168.2.30
Switch(config)# aaa enable
```

Шаг 3. Настройка аутентификации 802.1X. Включите 802.1X глобально и на интерфейсе ethernet 1/0/1:

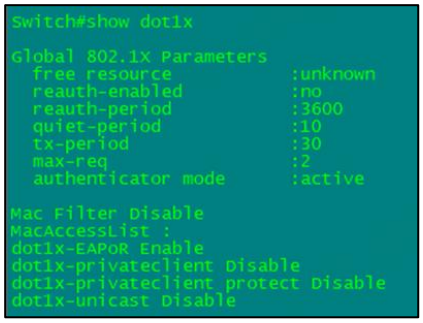
```
Switch(config)# dot1x enable
Switch(config)# interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# dot1x enable
Switch(config-if-ethernet1/0/1)# dot1x port-method portbased
Switch(config-if-ethernet1/0/1)# exit
```

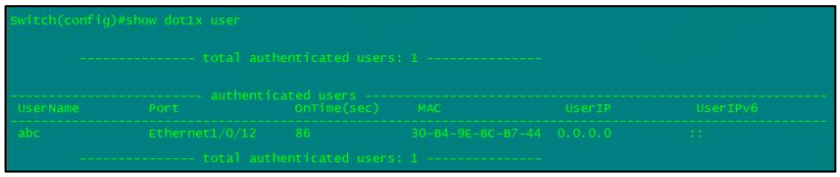
Шаг 4. Настройка IP-адреса управления. Коммутатор должен находиться в том же сетевом сегменте, что и RADIUS-сервер:

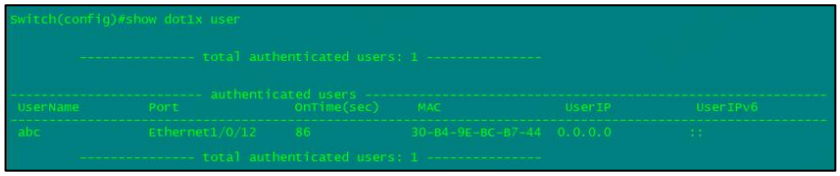
```
Switch(config)# interface vlan 10
Switch(config-if-vlan10)# ip address 192.168.2.1 255.255.255.0
Switch(config-if-vlan10)# exit
```

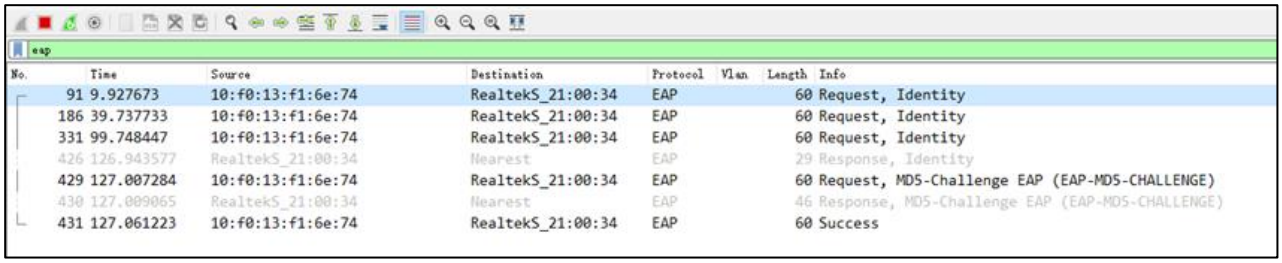
Шаг 5. Проверка конфигурации:

- Выполните команды «**show dot1x**» и «**show dot1x port-control**».
- Пользователь запускает клиент 802.1X, вводит учетные данные и начинает аутентификацию.
- При успешной проверке учетных данных пользователь получает доступ к сети.
- Администратор может использовать команду «**show dot1x user**» для просмотра информации об онлайн-пользователях:









После завершения настройки 802.1X на коммутаторе пользователи будут аутентифицироваться через RADIUS-сервер, и только авторизованные устройства получат доступ к сети.

Настройка экземпляра гостевого VLAN (Guest VLAN)

Функция гостевого VLAN используется для предоставления неаутентифицированным пользователям ограниченного доступа к определённым ресурсам сети. До прохождения аутентификации 802.1X порт пользователя автоматически принадлежит гостевому VLAN, где доступ к другим сетевым ресурсам ограничен. После успешной аутентификации порт покидает гостевой VLAN, и пользователь получает полный доступ к сети.

Этапы настройки:

Шаг 1. Создание VLAN:

```
Switch(config)# vlan 4
```

Шаг 2. Настройка порта и функции гостевого VLAN:

```
Switch(config)# dot1x enable
Switch(config)# interface ethernet 1/0/3
Switch(config-if-ethernet1/0/3)# dot1x port-method portbased
Switch(config-if-ethernet1/0/3)# dot1x guest-vlan 4
```

Шаг 3. Проверка конфигурации порта. Просмотрите текущую информацию о VLAN и статус порта:

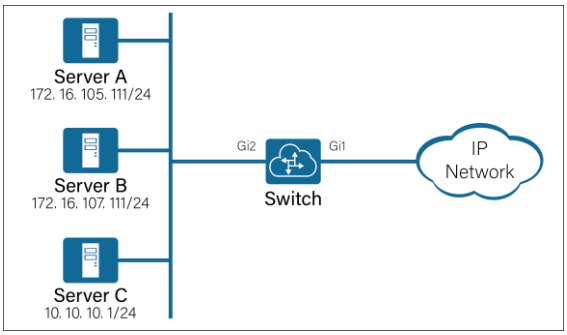
```
Switch(config-if-ethernet1/0/3)# show vlan id 4
```

После настройки гостевого VLAN пользователи, не прошедшие аутентификацию 802.1X, будут изолированы в гостевом VLAN с ограниченным доступом. После успешной аутентификации порт автоматически покидает гостевой VLAN, предоставляя пользователю полный доступ к сети.

3.2 Экземпляр конфигурации AAA (AAA Configuration instance)

3.2.1 Настройка стандартного списка контроля доступа (ACL)

Коммутатор (Switch) выполняет функции сервера доступа к целевой сети. Для доступа к коммутатору через Telnet пользователю необходимо пройти удалённую аутентификацию на сервере. Режим удалённой аутентификации на коммутаторе настроен, как показано на рисунке справа.



Этапы настройки:

Шаг 1. Создание стандартного ACL. Настройте правило стандартного ACL с номером в качестве идентификатора:

```
Switch(config)# access-list 1 deny 172.16.105.111 255.255.255.0
Switch(config)# access-list 1 deny 172.16.107.111 255.255.255.0
Switch(config)# access-list 1 permit any
```

Шаг 2. Применение ACL к интерфейсу. Примените правило в направлении входящего трафика на интерфейсе ethernet 1/0/2:

```
Switch(config)# interface ethernet 1/0/2
Switch(config-if-ethernet 1/0/2)# ip access-group 1 in
Switch(config-if-ethernet 1/0/2)# exit
```

Шаг 3. Проверка конфигурации.

Просмотрите статистику стандартного ACL и количество обработанных пакетов:

```
Switch# show access-list
```

Просмотрите интерфейс, к которому применён ACL:

```
Switch# show access-group
```

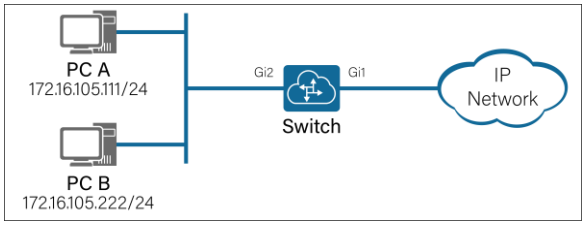
Пример конфигурации:

```
vlan 1
access-list 1 deny 172.16.105.0 0.0.0.255
access-list 1 deny 172.16.107.0 0.0.0.255
access-list 1 permit any-source
!
interface Ethernet1/0/1
!
interface Ethernet1/0/2
ip access-group 1 in
```

После настройки стандартного ACL доступ к коммутатору через указанный интерфейс будет разрешён только для авторизованных источников, а трафик с запрещённых адресов будет блокирован.

3.2.2 Настройка расширенного списка контроля доступа (ACL)

Коммутатор, выступая в роли шлюза, требует настройки расширенного ACL для запрета прохождения UDP-пакетов с исходным IP-адресом 172.16.105.111 к целевым IP-адресам 172.16.105.8, 172.16.105.10, 172.16.105.12 и 172.16.105.14. При этом все остальные UDP-пакеты должны быть разрешены.



Этапы настройки:

Шаг 1. Настройка временного диапазона действия правила:

```
Switch(config)# time-range test
Switch(config-time-range test)# periodic weekdays 9:00:00 to 17:00:00
Switch(config-time-range test)# exit
```

Шаг 2. Настройка расширенного ACL:

```
Switch(config)# access-list 100 deny udp host-source 172.16.105.111 172.16.105.8 0.0.0.0 time-range test
Switch(config)# access-list 100 deny udp host-source 172.16.105.111 172.16.105.10 0.0.0.0 time-range test
Switch(config)# access-list 100 deny udp host-source 172.16.105.111 172.16.105.12 0.0.0.0 time-range test
Switch(config)# access-list 100 deny udp host-source 172.16.105.111 172.16.105.14 0.0.0.0 time-range test
Switch(config)# access-list 100 permit udp any-source any-destination
```

Шаг 3. Применение ACL к интерфейсу. Примените правило во входящем направлении на интерфейсе ethernet 1/0/2:

```
Switch(config)# interface ethernet 1/0/2
Switch(config-if-ethernet 1/0/2)# ip access-group 100 in
Switch(config-if-ethernet 1/0/2)# exit
```

Шаг 4. Проверка конфигурации. Используйте команду «**show time range**», чтобы проверить состояние временного диапазона:

```
Switch(config)#show time-range
time-range test (inactive, used 1 times)
periodic weekdays 09:00:00 to 17:00:00
```

Используйте команду «**show access-list**», чтобы просмотреть конфигурацию стандартного ACL и статистику пакетов:

```
Switch(config)#show access-lists
access-list 100(used 0 time(s)) 4 rule(s)
rule ID 1: deny udp host-source 172.16.105.111 host-destination 172.16.105.8 time-range test (inactive)
rule ID 2: deny udp host-source 172.16.105.111 host-destination 172.16.105.10 time-range test (inactive)
```

rule ID 3: deny udp host-source 172.16.105.111 host-destination 172.16.105.12 time-range test (inactive)
rule ID 4: deny udp host-source 172.16.105.111 host-destination 172.16.105.14 time-range test (inactive)

Используйте команду «**show access-group**», чтобы просмотреть порты, к которым был применен ACL:

Switch(config)# show access-group
interface name:Ethernet1/0/2
IP Ingress access-list used is 100, traffic-statistics Disable

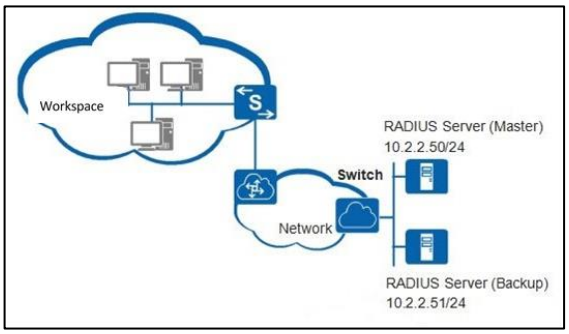
После завершения настройки UDP-трафик от указанного источника к заданным адресам будет блокироваться в пределах настроенного временного диапазона, тогда как остальной UDP-трафик будет разрешён.

3.3 Настройка AAA

Коммутатор выполняет роль сервера доступа к целевой сети. Для подключения к коммутатору по протоколу Telnet пользователю необходимо пройти удалённую аутентификацию на сервере.

3.3.1 Аутентификация через RADIUS

Аутентификация через RADIUS позволяет централизованно управлять доступом пользователей к коммутатору. RADIUS-сервер и коммутатор должны находиться в одном широковещательном домене или иметь корректно настроенную маршрутизацию.



Этапы настройки:

Шаг 1. Настройка RADIUS-сервера.

Настройка IP-адреса, порта и ключа основного сервера аутентификации и учета RADIUS:
Switch(config)# radius-server key 0 abc
Switch(config)# radius-server authentication host 10.2.2.50 port 1812 key 1234 primary

Настройка IP-адреса, порта и ключа резервного сервера аутентификации и учета RADIUS:
Switch(config)# radius-server authentication host 10.2.2.51 port 1812 key 1234

Шаг 2. Включение AAA:

Switch(config)# aaa enable

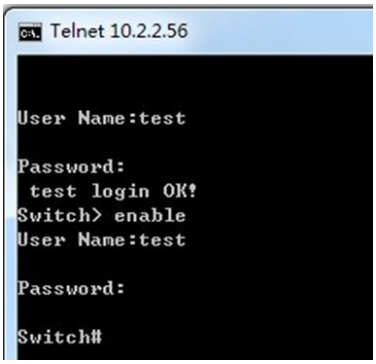
Шаг 3. Настройка IP-интерфейса VLAN:

Switch(config)# interface vlan 1
Switch(config-if-vlan1)# ip address 10.2.2.56 255.255.255.0
Switch(config-if-vlan1)# exit

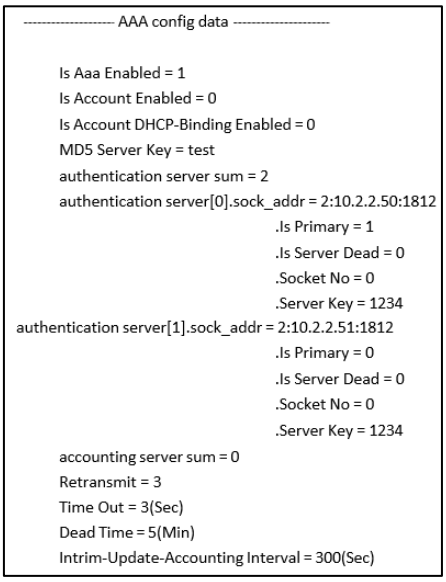
Шаг 4. Настройка пользователя на RADIUS-сервере. Создайте учётную запись на RADIUS-сервере.

Шаг 5. Проверка конфигурации:

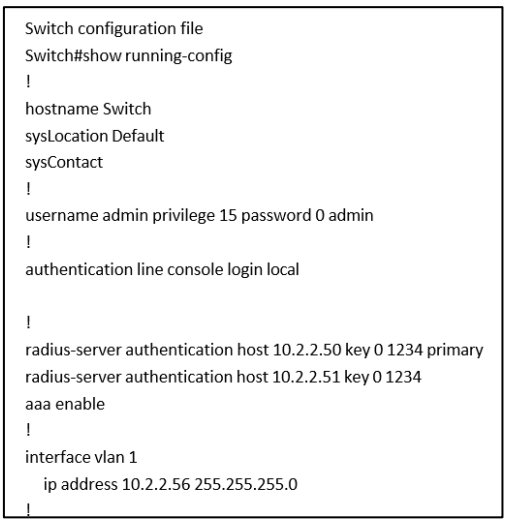
Используйте командную строку в Windows, чтобы подключиться к коммутатору по протоколу Telnet, и пройдите аутентификацию, используя учетные данные пользователя, созданного на RADIUS-сервере:



Проверьте настройки AAA с помощью команды «**show aaa config**» на коммутаторе:
Switch(config)# show aaa config



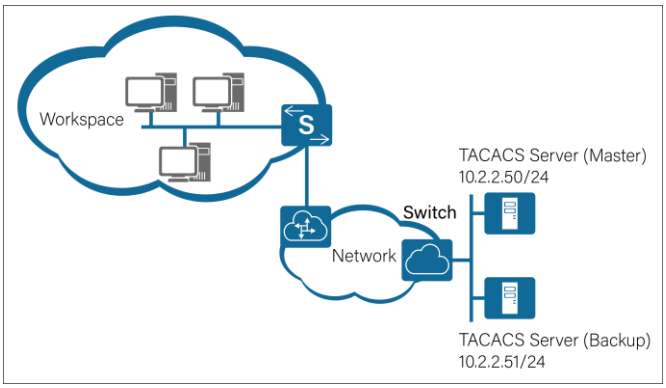
Конфигурация коммутатора показана на рисунке ниже:



После завершения настройки доступ к коммутатору через Telnet будет предоставляться только пользователям, успешно прошедшим аутентификацию на RADIUS-сервере.

3.3.2 Аутентификация через TACACS+

Коммутатор выполняет роль сервера доступа к целевой сети. Для подключения к коммутатору по протоколу Telnet пользователю необходимо пройти удаленную аутентификацию на сервере.
Сервер TACACS+ настраивается отдельно.



Этапы настройки:

Шаг 1. Конфигурация сервера TACACS+ на коммутаторе.

Настройка IP-адреса, порта и ключа основного сервера аутентификации и учета TACACS:
Switch(config)# tacacs-server key 0 abc
Switch(config)# tacacs-server authentication host 10.2.2.50 port 49 key 0 1234
Switch(config)# tacacs-server timeout 10

Настройка IP-адреса, порта и ключа резервного сервера аутентификации и учета TACACS:
Switch(config)# tacacs-server authentication host 10.2.2.51 port 49 key 0 1234
Switch(config)# tacacs-server timeout 10

Шаг 2. Настройка VLAN-интерфейса:

Switch(config)# interface vlan 1
Switch(config-if-vlan1)# ip address 10.2.2.56 255.255.255.0
Switch(config-if-vlan1)# exit

Шаг 3. Настройка пользователя и пароля для сервера TACACS+. Создайте учётную запись на сервере TACACS+

Шаг 4. Настройка метода аутентификации:

Switch(config)# authentication line vty login tacacs local

Шаг 5. Проверка конфигурации:

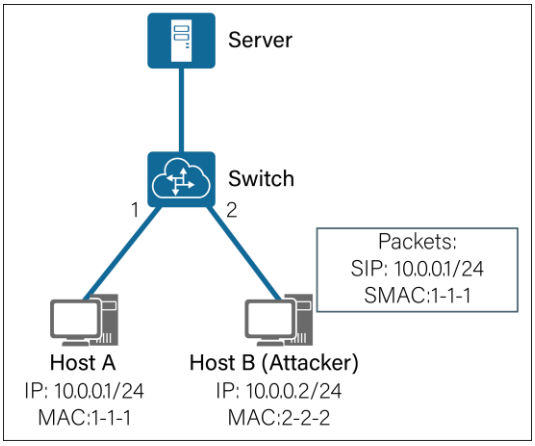
Используйте командную строку в Windows, чтобы подключиться к коммутатору по протоколу Telnet, и пройдите аутентификацию, используя учетные данные пользователя, созданного на RADIUS-сервере.

Выполните проверку настроек с помощью команды «**show aaa config**» на коммутаторе:
Switch(config)# show aaa config

После настройки аутентификация пользователей при подключении по Telnet будет выполняться через сервер TACACS+. В случае недоступности сервера может использоваться локальная база пользователей (если настроено local).

3.4 Настройка экземпляра конфигурации AM

Как показано на рисунке справа, узлы HostA и HostB подключены к интерфейсам коммутатора (Switch) 10ge1/0/1 и 10ge1/0/2 соответственно. Требуется исключить возможность подмены (имперсонации) IP- и MAC-адресов узла HostA узлом HostB с целью несанкционированного доступа к серверу, а также обеспечить корректную передачу IP-пакетов от HostA.



Этапы настройки:

Шаг 1. Включение управления доступом (AM):

Switch# config Switch(config)# am enable
Switch(config)# interface ethernet 1/0/1-2 Switch(config-if- port-range)#am port

*Команда «**am enable**» включает глобальный механизм Access Management (AM), а команда «**am port**» активирует контроль доступа на указанных интерфейсах.*

Шаг 2. Настройка статической привязки MAC- и IP-адресов.

Настройка привязки для HostA:
Switch(config)# interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# am mac-ip-pool 00-01-00-01-00-01 10.0.0.1

Настройка привязки для HostB:
Switch(config)# interface ethernet 1/0/2
Switch(config-if-ethernet1/0/2)# am mac-ip-pool 00-02-00-02-00-02 10.0.0.2

Статическая привязка гарантирует, что передача трафика через порт будет разрешена только при совпадении заданных MAC- и IP-адресов.

Шаг 3. Проверка результатов настройки:

Switch(config)#show am
Пример вывода:

AM is enabled

Interface Ethernet1/0/1
am port
am mac-ip-pool 00-01-00-01-00-01 10.0.0.1

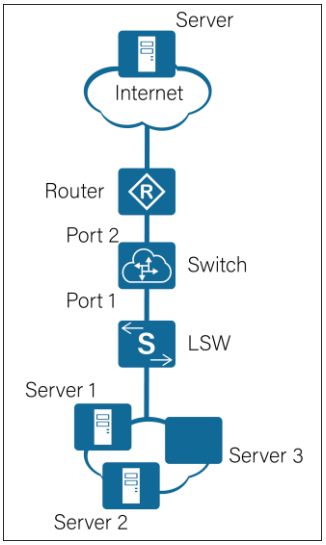
Interface Ethernet1/0/2
am port
am mac-ip-pool 00-02-00-02-00-02 10.0.0.2

Согласно выводу команды, для HostA и HostB настроены записи статической привязки MAC- и IP-адресов.

После завершения настройки механизм AM обеспечивает контроль соответствия MAC- и IP-адресов на указанных интерфейсах. Попытки подмены адресов будут блокироваться коммутатором, что повышает уровень безопасности сети и предотвращает несанкционированный доступ к сетевым ресурсам

3.5 Настройка ARP

3.5.1 Настройка стандартного ARP



Как показано на рисунке справа, порт 10GE1/0/1 коммутатора подключен к Server1, Server2 и Server3 через коммутатор локальной сети (LSW). Порт 10GE1/0/2 подключен к маршрутизатору (Router) и обеспечивает дальнейшую передачу трафика во внешние сети.
Для корректной адаптации к изменениям в сети используется динамический ARP, который автоматически формирует таблицу соответствия IP- и MAC-адресов. Однако, для повышения безопасности и предотвращения атак с использованием подмены ARP (ARP spoofing), необходимо настроить статическую ARP-запись для маршрутизатора.
IP-адрес маршрутизатора – 10.2.2.3, соответствующий ему MAC-адрес — 00e0-fc01-0000.

Этапы настройки:

Шаг 1. Создание VLAN и добавление интерфейсов:

```
Switch(config)# vlan 2
Switch(config-vlan2)# exit
Switch(config)# interface ethernet 1/0/1-2
Switch(config-if-port-range)# switchport access vlan 2
Switch(config-if-port-range)# exit
```

Шаг 2. Настройка статической ARP-записи:

```
Switch(config)# interface Vlan2
Switch(config-if-vlan2)# arp 10.2.2.3 00-e0-fc-01-00-00 interface Ethernet1/0/2
```

Данная команда создаёт статическую привязку IP-адреса маршрутизатора к его MAC-адресу на указанном интерфейсе. Это предотвращает изменение записи динамическими ARP-пакетами.

Шаг 3. Проверка результатов настройки.

Для проверки статической ARP-записи используйте команду:

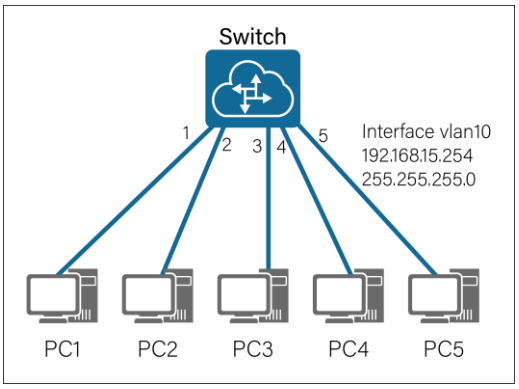
```
Switch# show arp type static
```

В выводе команды должна отображаться настроенная статическая запись для IP-адреса 10.2.2.3:

```
ARP Unicast Items: 1, Valid: 1, Matched: 1, Verifying: 0, Incomplete: 0, Failed: 0, None: 0
Address          Hardware Addr     Interface        Port                Flag
Age-time(sec)
10.2.2.3         00-e0-fc-01-00-00 Vlan2            Ethernet1/0/2       Static
```

После выполнения настройки коммутатор использует статическую ARP-запись для связи с маршрутизатором. Это предотвращает возможность подмены ARP-записей злоумышленниками, повышает надёжность передачи данных и обеспечивает безопасное взаимодействие серверов с внешними сетями.

3.5.2 Типовые сценарии работы функции отправки самопроизвольных ARP-пакетов



В данном сценарии коммутатор обслуживает пять хостов (PC1–PC5), подключённых к VLAN 10. Для своевременного обновления ARP-таблиц устройств в сети и предотвращения конфликтов IP-адресов используется функция отправки самопроизвольных ARP-пакетов (Gratuitous ARP).

Этапы настройки:

Шаг 1. Создание VLAN и добавление интерфейсов:

Switch(config)# vlan 10 Switch(config-vlan)# exit
Switch(config)# interface ethernet 1/0/1-5
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# exit

Шаг 2. Настройка интерфейса VLAN 10.

Создание интерфейса VLAN на назначение IP-адреса:
Switch(config)# interface vlan 10
Switch(config-if-vlan10)# ip address 192.168.15.254 255.255.255.0
Switch(config-if-vlan10)# exit

Шаг 3. Включение функции отправки Gratuitous ARP:

Switch(config)# ip gratuitous-arp

После включения функции коммутатор периодически отправляет самопроизвольные ARP-пакеты от имени интерфейса VLAN.

Шаг 4. Проверка результата настройки

Switch(config)# show ip gratuitous-arp

Пример вывода:
Gratuitous ARP send is Global disabled
Gratuitous ARP send enabled interface vlan information:
Name Interval-Time(seconds)
Vlan10 300

После включения функции Gratuitous ARP коммутатор автоматически рассылает ARP-пакеты для обновления таблиц соответствия IP- и MAC-адресов у устройств в сети. Это позволяет:

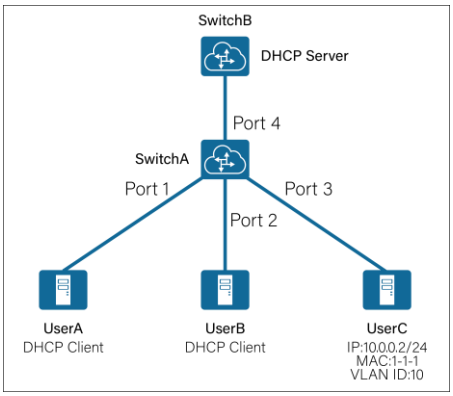
- ускорить обновление ARP-кэша;
- уменьшить вероятность конфликтов IP-адресов;

- повысить стабильность работы VLAN при изменении MAC-адресов или перезапуске оборудования.

Функция особенно полезна в динамичных сетевых средах и при использовании механизмов резервирования шлюза.

3.6 Настройка безопасности ARP

3.6.1 Предотвращение атак типа «человек посередине» (MITM) через ARP



Как показано на рисунке справа, пользователи в определенном отделе предприятия подключены к коммутатору SwitchA и находятся в VLAN 10. Часть устройств получает IP-адреса по DHCP, часть использует статическую адресацию. Все устройства и DHCP-сервер расположены в одном VLAN. При выполнении ARP-атаки типа «man-in-the-middle» злоумышленник может подменять ARP-ответы, что приводит к перехвату или модификации трафика. Для защиты сети на коммутаторе настраиваются механизмы DHCP Snooping и Dynamic ARP Inspection (DAI).

Этапы настройки:

Шаг 1. Настройка VLAN и интерфейсов:

Switch(config)# hostname SwitchA SwitchA(config)# vlan 10
SwitchA(config-vlan)# exit
SwitchA(config)# interface ethernet 1/0/1-4
SwitchA(config-if-port-range)# switchport access vlan 10

Шаг 2. Настройка DHCP Snooping. Включение функции DHCP Snooping и определение доверенного порта.

Включение DHCP Snooping глобально:
SwitchA(config)# ip dhcp snooping enable

Включение DHCP Snooping для VLAN 10:
SwitchA(config)# ip dhcp snooping vlan 10

Назначение доверенного интерфейса (подключён DHCP-сервер):
SwitchA(config)# interface ethernet 1/0/4
SwitchA(config-if-ethernet 1/0/4)# ip dhcp snooping trust

Шаг 3. Включение динамической проверки ARP Dynamic ARP Inspection (DAI) на портах 1–3.

Включение ARP Inspection для VLAN 10:
SwitchA(config)# ip arp inspection vlan 10

Назначение доверенного порта:
SwitchA(config)# interface ethernet 1/0/4
SwitchA(config-if-ethernet1/0/4)# ip arp inspection trust

Для устройств со статическими IP-адресами необходимо создать статические привязки:
SwitchA(config)# interface vlan 10
SwitchA(config-if-vlan10)# arp 10.0.0.2 00-01-00-01-00-01 interface ethernet 1/0/3

Шаг 4. Проверка результата настройки.

Проверка таблицы привязок DHCP Snooping:
SwitchA(config)# show ip dhcp snooping binding all

Пример вывода справа:

MAC	IP address	Interface	Vlan ID	Flag
2c:53:4a:03:31:40	192.168.1.3	Gi1	10	
2c:53:4a:03:31:42	192.168.1.2	Gi2	10	

Проверка ARP-таблицы и привязок:
SwitchA# show arp

Пример вывода справа:

```
ARP Unicast Items: 3, Valid: 3, Matched: 3, Verifying: 0, Incomplete: 0, Failed: 0, None: 0 Address
Hardware Addr   Interface       PortFlag
192.168.1.2  2c-53-4a-03-31-42    Vlan10  Ethernet1/0/2     Dynamic 192.168.1.32c-53-4a-03-31-
40  Vlan10   Ethernet1/0/1     Dynamic
10.0.0.2 00-01-00-01-00-01    Vlan10  Ethernet1/0/3     Static
```

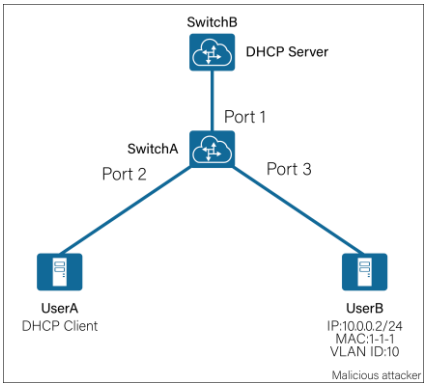
После настройки DHCP Snooping и Dynamic ARP Inspection коммутатор:

- формирует таблицу соответствия IP–MAC–порт на основе DHCP-ответов;
- проверяет корректность ARP-пакетов на недоверенных портах;
- блокирует поддельные ARP-сообщения;
- предотвращает атаки типа ARP MITM и ARP Spoofing.

Данная конфигурация значительно повышает уровень безопасности внутри VLAN и защищает пользователей от перехвата трафика и подмены сетевых параметров.

3.6.2 Настройка защиты от ARP-спуфинга

В данном сценарии пользователи подключены к коммутатору SwitchA и находятся в одном VLAN. Часть устройств получает IP-адреса по DHCP, часть использует статическую адресацию.
Если пользователь инициирует атаку ARP-спуфинга (подмену IP- и MAC-адреса в ARP-пакетах), это может привести к перехвату трафика, нарушению связи или компрометации данных. Для предотвращения подобных атак на коммутаторе настраиваются механизмы DHCP Snooping и функция Anti-ARP-Spoofing.



Этапы настройки:

Шаг 1. Настройка DHCP Snooping.

Включение DHCP Snooping глобально:
SwitchA(config)# ip dhcp snooping enable

Включение DHCP Snooping для VLAN 1:
SwitchA(config)# ip dhcp snooping vlan 1

Назначение доверенного интерфейса (порт подключения DHCP-сервера):

```
SwitchA(config)# interface ethernet 1/0/1
SwitchA(config-if-ethernet 1/0/1)# ip dhcp snooping trust
```

Шаг 2. Включение глобальной защиты от ARP-спуфинга:

```
SwitchA(config)# anti-spoofing enable
```

Шаг 3. Настройка доверенных портов. Порты, подключенные к легитимным устройствам или сетевому оборудованию, настраиваются как доверенные:

```
SwitchA(config)# interface ethernet 1/0/1-2
SwitchA(config-if-port-range)# anti-arpscan trust port
```

Шаг 4. Проверка результатов настройки. Проверка состояния функции защиты от ARP-спуфинга:

```
SwitchA(config)# show anti-arpscan
```

По результатам вывода можно убедиться, что функция включена, а доверенные порты настроены корректно:

Total port: 28

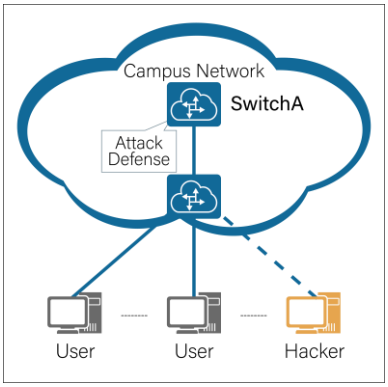
Name	Port-property	beShut	shutTime(seconds)
Ethernet1/0/1	trust	N	0
Ethernet1/0/2	trust	N	0
Ethernet1/0/3	untrust	N	0
Ethernet1/0/4	untrust	N	0
Ethernet1/0/5	untrust	N	0
Ethernet1/0/6	untrust	N	0
Ethernet1/0/7	untrust	N	0
Ethernet1/0/8	untrust	N	0
Ethernet1/0/9	untrust	N	0
Ethernet1/0/10	untrust	N	0

После включения DHCP Snooping и глобальной защиты Anti-ARP-Spoofing коммутатор:

- формирует таблицу соответствия IP–MAC–порт;
- проверяет корректность ARP-пакетов;
- блокирует попытки подмены IP- и MAC-адресов;
- предотвращает ARP-спуфинг и связанные с ним атаки.

Данная конфигурация повышает уровень безопасности внутри VLAN и обеспечивает защиту пользователей от сетевых атак, связанных с подменой ARP.

3.7 Настройка защиты от атак



В данном сценарии коммутатор SwitchA может подвергаться различным видам атак: отправке некорректно сформированных пакетов (malformed packets), атакам фрагментированными пакетами, а также flood-атакам (TCP SYN flood, ICMP flood и др.). Для предотвращения перегрузки оборудования и нарушения его работы на коммутаторе включаются встроенные механизмы защиты от DoS-атак.

Этапы настройки:

Шаг 1. Включение защиты от совпадения IP-адреса источника и назначения:

```
SwitchA(config)# dosattack-check srcip-equal-dstip enable
```

Шаг 2. Включение защиты от совпадения портов источника и назначения:

SwitchA(config)# dosattack-check srcport-equal-dstport enable

Шаг 3. Включение защиты от flood- и фрагментационных атак.

Включение защиты от TCP SYN-атак:
SwitchA(config)# dosattack-check tcp-flags enable

Включение защиты от ICMP-атак:
SwitchA(config)# dosattack-check icmp-attacking enable

Ограничение максимального размера ICMPv4-пакета (512 байт):
SwitchA(config)# dosattack-check icmpV4-size 512

Проверка корректности первого фрагмента IPv4-пакета:
SwitchA(config)# dosattack-check ipv4-first-fragment enable

Шаг 4. Проверка результатов настройки. Для просмотра текущей конфигурации защиты от атак используется команда:

SwitchA# show dosattack-check config

По результатам вывода можно убедиться, что необходимые механизмы защиты активированы:

```
Use the show dosattack-check config command on SwitchA to view the attack defense configuration.
Switch(config)# show dosattack-check config
Detect-type      Stats

icmp-attacking   enable
icmpV4-size      512
icmpV6-size      512
ipv4-first-fragment        enable
srcip-equal-dstipenable
srcport-equal-dstport      enable
tcp-flags        enable
tcp-fragment     disable
tcp-segment      20
```

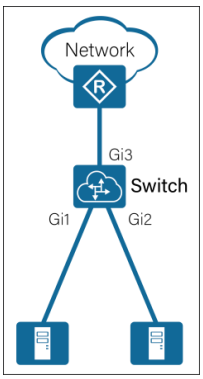
После включения механизмов защиты коммутатор:

- блокирует пакеты с одинаковыми IP-адресами источника и назначения;
- предотвращает атаки с совпадающими портами;
- защищает от TCP SYN flood и ICMP flood;
- контролирует корректность фрагментированных пакетов;
- ограничивает аномальные ICMP-пакеты.

Данная конфигурация значительно повышает устойчивость коммутатора к DoS-атакам и обеспечивает стабильную работу сетевой инфраструктуры.

3.8 Настройка управления CoS

3.8.1 Настройка стандартного CoS



В данном сценарии два арендатора используют разные серверы, взаимодействующие через маршрутизатор и внешнюю сеть ЦОД. Пакеты обоих арендаторов имеют значение 802.1p = 0, однако значения DSCP различаются: Арендатор 1 — **AF12** (DSCP 12) и Арендатор 2 — **AF22** (DSCP 20). Требуется обеспечить отправку трафика к маршрутизатору в соотношении **2:1**.

Этапы настройки:

Шаг 1. Настройка приоритета для порта Gi1:

Switch(config)# interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# mls qos cos 3

Switch(config-if-ethernet1/0/1)# exit

Шаг 2. Настройка доверительного значения DSCP на интерфейсе Gi2:

Switch(config)# interface ethernet 1/0/2
Switch(config-if-ethernet1/0/2)# mls qos trust dscp
Switch(config-if-ethernet1/0/2)# exit

Шаг 3. Настройка соответствия между DSCP и внутреннего приоритета:

Switch(config)# mls qos map dscp-intp 20 to 7

Шаг 4. Настройка соответствия приоритетов 802.1p аппаратным очередям:

Switch(config)# mls qos map cos-intp 7 6 5 4 3 2 1 0

Шаг 5. Настройка алгоритма планирования очередей. Используется алгоритм **WDRR (Weighted Deficit Round Robin)**:

Switch(config)# interface ethernet 1/0/1-2
Switch(config-if-port-range)# mls qos queue algorithm wdrr
Switch(config-if-port-range)# mls qos queue wdrr weight 10 40 20 10 20 20 40 80

Шаг 6. Проверка результатов настройки.

Проверка конфигурации QoS на интерфейсах:
Switch(config)# show mls qos interface ethernet 1/0/1-2 Ethernet1/0/1

Проверка сопоставления 802.1p и аппаратных очередей:
Switch(config)#show mls qos maps cos-intp

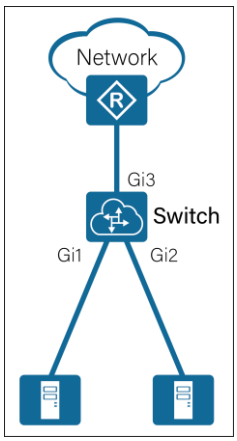
Проверка сопоставления DSCP и внутреннего приоритета:
Switch(config)# show mls qos maps dscp-intp

В результате настройки:

- коммутатор учитывает значения DSCP;
- выполняется сопоставление DSCP → внутренний приоритет → аппаратная очередь;
- используется алгоритм WDRR для распределения полосы пропускания;
- трафик арендаторов обслуживается с заданным соотношением 2:1.

Данная конфигурация позволяет гибко управлять качеством обслуживания (QoS) и гарантировать приоритетную обработку критичного трафика.

3.8.2 Настройка планировщика очередей SP (Strict Priority) для CoS



В данном сценарии требуется обеспечить приоритетную передачу трафика Арендатора 1 через выходной маршрутизатор. Трафик Арендатора 1 должен обслуживаться в очереди строгого приоритета (SP) и гарантированно получать не менее 500 Мбит/с пропускной способности.

Этапы настройки:

Шаг 1. Создание ACL для классификации трафика:

```
Switch(config)# access-list 1 permit host-source 172.168.253.10 dscp 46
Switch(config)# access-list 2 permit host-source 172.168.253.11 dscp 23
```

Шаг 2. Создание class-map для сопоставления трафика:

```
Switch(config)#class-map 1
Switch(config-classmap-1)#match access-group 1
Switch(config-classmap-1)#exit

Switch(config)#class-map 2
Switch(config-classmap-1)#match access-group 2
Switch(config-classmap-1)#exit
```

Шаг 3. Включение алгоритма Strict Priority:

```
Switch(config)# interface ethernet 1/0/1-2
Switch(config-if-port-range)# mls qos queue algorithm sp
```

Шаг 4. Применение политики обслуживания:

```
Switch(config-if-port-range)# service-policy input 1
```

Политика должна содержать настройку приоритетной очереди и гарантированной полосы пропускания.

Шаг 5. Проверка результатов настройки. Проверка конфигурации QoS:

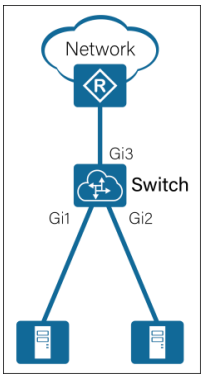
```
Switch(config)# show mls qos interface ethernet 1/0/1-2
```

```
Ethernet1/0/1:
Default COS: 0 Trust: COS
Attached Policy Map for Ingress: 1


Egress Internal-Priority-TO-Queue map:

INTP:  0  1  2  3  4  5  6  7
Queue: 0  1  2  3  4  5  6  7

Queue Algorithm: SP Queue weights:
Queue  1  2  3  4  5  6  7  8
WrrWeight  1  2  3  4  5  6  7  8
WdrrWeight 1  2  4  8  16 32 64 64

Bandwidth Guarantee Configuration:

Queue  1  2  3  4  5  6  7  8
MinBW(K) 0  0  0  0  0  0  0  0
MaxBW(K) 0  0  0  0  0  0  0  0
```

По результатам вывода на рисунке справа можно убедиться, что необходимые механизмы приоритета активированы.

После настройки алгоритма SP трафик Арендатора 1 обрабатывается в очереди строгого приоритета и передается первым, что обеспечивает минимальные задержки и гарантированную полосу пропускания.
Такой механизм рекомендуется использовать для критически важного трафика (например, голосового или управляющего), требующего высокой приоритетности обслуживания.

3.8.3 Настройка управления CoS с использованием алгоритма WRR



В данном примере два арендатора используют разные серверы, взаимодействующие с внешней сетью ЦОД через выходной маршрутизатор. Значение 802.1p для обоих потоков равно 0.
Значения DSCP: Арендатор 1 — AF12 и Арендатор 2 — AF22. Требуется обеспечить передачу трафика в соотношении 2:1.

Этапы настройки:

Шаг 1. Настройка приоритета для интерфейса Gi1:

```
Switch(config)# interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# mls qos cos 3
Switch(config-if-ethernet1/0/1)# exit
```

Шаг 2. Настройка доверия DSCP на интерфейсе Gi2:

```
Switch(config)# interface ethernet 1/0/2
Switch(config-if-ethernet1/0/2)# mls qos trust dscp
Switch(config-if-ethernet1/0/2)# exit
```

Шаг 3. Настройка сопоставления DSCP и внутреннего приоритета:

```
Switch(config)# mls qos map dscp-intp 20 to 7
```

Шаг 4. Привязка 802.1p к аппаратным очередям:

```
Switch(config)# mls qos map cos-intp 7 6 5 4 3 2 1 0
```

Шаг 5. Настройка алгоритма планирования WRR (Weighted Round Robin):

```
Switch(config)# interface ethernet 1/0/1-2
Switch(config-if-port-range)# mls qos queue algorithm wrr
Switch(config-if-port-range)# mls qos queue wrr weight 10 40 20 10 20 20 40 80
```

Шаг 6. Проверка результата настройки:

```
Switch(config)# show mls qos interface ethernet 1/0/2-11
```

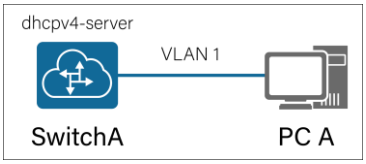
Результат работы команды показан на рисунке справа:

```
Ethernet1/0/1:
Default COS: 0 Trust: COS
Attached Policy Map for Ingress: 1


Egress Internal-Priority-TO-Queue map:

INTP:  0   1   2   3   4   5   6   7
Queue: 0   1   2   3   4   5   6   7

Queue Algorithm: SP Queue weights:
Queue  1   2   3   4   5   6   7   8
WrrWeight  1   2   3   4   5   6   7   8
WdrrWeight 1   2   4   8   16  32  64  64

Bandwidth Guarantee Configuration:

Queue  1   2   3   4   5   6   7   8
MinBW(K) 0   0   0   0   0   0   0   0
MaxBW(K) 0   0   0   0   0   0   0   0
```

После настройки алгоритма WRR трафик арендаторов распределяется между очередями пропорционально заданным весам. Благодаря сопоставлению DSCP → внутренний приоритет → аппаратная очередь обеспечивается передача пакетов в требуемом соотношении 2:1. Алгоритм WRR позволяет гарантировать справедливое распределение полосы пропускания без полной блокировки менее приоритетного трафика.

3.9 Настройка сервера DHCPv4

3.9.1 Настройка DHCPv4



В данном сценарии коммутатор SwitchA выступает в роли DHCPv4-сервера и назначает IP-адреса клиентам в локальной сети. ПК А подключается напрямую и получает параметры сети автоматически.

Этапы настройки:

Шаг 1. Создание пула адресов и настройка параметров. Настраиваются сеть выдачи адресов, шлюз по умолчанию, DNS-сервер, время аренды (lease):

```
Switch(config)# ip dhcp pool 1
Switch(dhcp-1-config)# network-address 192.168.2.0 255.255.255.0
Switch(dhcp-1-config)# default-router 192.168.2.1
Switch(dhcp-1-config)# dns-server 114.114.114.114
Switch(dhcp-1-config)# lease 5 10 30
Switch(dhcp-1-config)# exit
```

Шаг 2. Настройка IP-адреса интерфейса VLAN 1:

```
Switch(config)# interface vlan 1
Switch(config-if-vlan1)# ip address 192.168.2.1 255.255.255.0
Switch(config-if-vlan1)# exit
```

Шаг 3. Проверка результатов настройки:

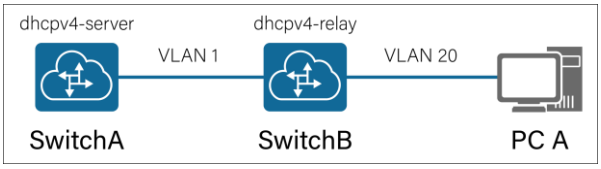
```
Switch(config)#show ip dhcp binding
```

По результатам вывода можно убедиться, что команда отображает список клиентов, получивших IP-адреса, и состояние аренды:

```
Total dhcp binding items: 2, the matched: 2
IP address      Hardware address    Lease expiration          Type 192.168.2.2
                00-E0-4C-21-00-34   Thu Jan 02 01:18:00 2020 Dynamic
192.168.2.3     F0-DE-F1-57-3B-C1   Thu Jan 02 01:24:00 2020 Dynamic
```

После выполнения настроек коммутатор функционирует как DHCPv4-сервер и автоматически выдает клиентам IP-адреса и сетевые параметры. Это упрощает администрирование сети и исключает необходимость ручной настройки адресов на каждом устройстве.

3.9.2 Настройка DHCPv4-ретранслятора



В данном сценарии сеть разделена на несколько VLAN, при этом DHCPv4-сервер физически расположен в одном сегменте сети, а клиентское устройство — в другом. Коммутатор **SwitchA** выполняет функции DHCPv4-сервера и отвечает за выдачу IP-адресов и других сетевых параметров (шлюз по умолчанию, DNS-сервер, время аренды). Коммутатор **SwitchB** работает как DHCPv4-ретранслятор (DHCP Relay Agent) и обеспечивает пересылку широковещательных DHCP-запросов от клиента к серверу. Поскольку широковещательные пакеты не проходят между различными VLAN, механизм ретрансляции

позволяет доставить запрос клиента к серверу и вернуть ответ обратно, обеспечивая корректное получение IP-адреса ПК А из удалённого сетевого сегмента.

Этапы настройки:

Шаг 1. Создание пула адресов на SwitchA:

```
SwitchA(config)# ip dhcp pool 1
SwitchA(dhcp-1-config)# network-address 192.168.2.0 255.255.255.0
SwitchA(dhcp-1-config)# default-router 192.168.2.1
SwitchA(dhcp-1-config)# dns-server 114.114.114.114
SwitchA(dhcp-1-config)# lease 5 10 30
Switch(dhcp-1-config)# exit
```

Шаг 2. Настройка IP-адреса интерфейса VLAN 1 на SwitchA:

```
SwitchA(config)# interface vlan 1
SwitchA(config-if-vlan1)# ip address 192.168.2.1 255.255.255.0
SwitchA(config-if-vlan1)# exit
```

Шаг 3. Включение службы DHCP:

```
Switch(config)# service dhcp
```

Шаг 4. Настройка DHCP-ретрансляции на SwitchB:

```
SwitchB(config)# ip forward-protocol udp bootps
SwitchB(config)# interface vlan 20
SwitchB(config)# ip helper-address 192.168.2.1
```

*Команда «**ip helper-address**» указывает IP-адрес DHCP-сервера, на который будут пересылаться широковещательные запросы клиентов.*

Шаг 5. Настройка статической маршрутизации на SwitchA:

```
SwitchA(config)# ip route 192.168.0.0/24 192.168.2.5
```

Шаг 6. Настройка порта для подключения ПК на SwitchB:

```
SwitchB(config)# interface ethernet 1/0/2
SwitchB(config-if-ethernet1/0/2)# switchport access vlan 20
```

Шаг 7. Проверка результатов настройки

#Проверка протоколов пересылки:

```
SwitchB# show ip forward-protocol
```

Проверка адреса DHCP-сервера для ретрансляции:

```
SwitchB# show ip helper-address
```

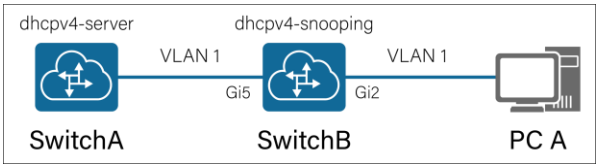
```
Switch(config)#show ip helper-address
Forward protocol    Interface                    Forward server
67(active)          Vlan1                        192.168.2.1
```

Проверка выданных адресов на DHCP-сервере:
SwitchB# show ip dhcp binding

```
Switch(config)#show ip dhcp binding
Total dhcp binding items: 1, the matched: 1
IP address          Hardware address        Lease expiration        Type    192.168.0.2
                    00-E0-4C-21-00-34       Sat Aug 19 03:22:00 2023 Dynamic
```

После выполнения настройки SwitchB пересылает DHCP-запросы клиентов из VLAN 20 на DHCP-сервер SwitchA. Это позволяет централизованно развернуть DHCP-сервер и обеспечивать автоматическую выдачу IP-адресов клиентам, находящимся в разных VLAN или сетевых сегментах.

3.9.3 Настройка отслеживания DHCPv4 (DHCP Snooping)



В этом сценарии коммутатор **SwitchA** выполняет функции DHCPv4-сервера, выдавая IP-адреса и сетевые параметры клиентам сети. Коммутатор **SwitchB** настроен с включенной функцией DHCPv4-Snooping, что позволяет контролировать легитимность DHCP-запросов, предотвращать использование поддельных DHCP-серверов и фиксировать привязку IP-адресов к портам для обеспечения безопасности сети. Клиентское устройство **PC A** получает IP-адрес через этот механизм, обеспечивая корректное управление распределением адресов.

Этапы настройки:

Шаг 1. Настройка IP-адреса на VLAN 1 коммутатора B:

SwitchB(config)# interface vlan 1
SwitchB(config-if-vlan1)# ip address 192.168.2.5 255.255.255.0
SwitchB(config-if-vlan1)# exit

Шаг 2. Включение и настройка функции отслеживания DHCPv4.

Включение DHCP Snooping:
SwitchB(config)# ip dhcp snooping enable

Включение отслеживания на VLAN 1:
SwitchB(config)# ip dhcp snooping vlan 1

Настройка доверенного порта:
SwitchB(config)# interface ethernet 1/0/5
SwitchB(config-if-ethernet 1/0/5)# ip dhcp snooping trust
SwitchB(config-if-ethernet 1/0/5)# exit

Шаг 3. Проверка результатов настройки:

Проверка конфигурации DHCP Snooping:
SwitchB(config)# show ip dhcp snooping

Результат работы команды показан на рисунке справа:

DHCP Snooping is enabled

DHCP Snooping maxnum of action info:10

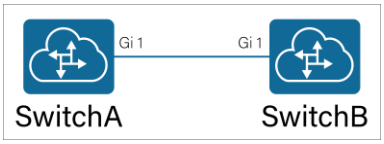
DHCP Snooping limit rate is 100 pps, switch ID 08-c6-b3-c9-1a-ac DHCP Snooping droped packets 0, discarded packets 0

DHCP Snooping alarm count 0, binding count 0, static binding count 0, from shell 0, from server 0 expired binding 0, request binding 0

interface	trust	action	recovery	alarm num	bind num
Ethernet1/0/1	untrust	none	0	0	0
Ethernet1/0/2	untrust	none	0	0	0
Ethernet1/0/3	untrust	none	0	0	0
Ethernet1/0/4	untrust	none	0	0	0
Ethernet1/0/5	trust	none	0	0	0
Ethernet1/0/6	untrust	none	0	0	0
Ethernet1/0/7	untrust	none	0	0	0
Ethernet1/0/8	untrust	none	0	0	0
Ethernet1/0/9	untrust	none	0	0	0
Ethernet1/0/10	untrust	none	0	0	0

После выполнения настроек коммутатор **SwitchB** отслеживает DHCP-запросы и привязки IP-адресов к портам, обеспечивая защиту сети от поддельных DHCP-серверов и некорректного распределения адресов. Пользователь **PC A** получает IP-адрес безопасным способом через механизм DHCPv4-Snooping.

3.10 Настройка EFM (Ethernet Fault Management)



В этом примере коммутаторы **A** и **B** соединены через интерфейсы **Gi1**. Для обеспечения надежности связи необходимо реализовать автоматическое обнаружение неисправностей канала и мониторинг качества соединения. Настройка функции **EFM** позволяет отслеживать количество ошибочных кадров, поступающих на коммутатор **A**, и своевременно выявлять проблемы в канале между коммутаторами.

Этапы настройки:

Шаг 1. Настройка на коммутаторе A:

```
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# ethernet-oam mode passive
Switch(config-if-ethernet1/0/1)# ethernet-oam
Switch(config-if-ethernet1/0/1)# ethernet-oam errored-frame window 20
Switch(config-if-ethernet1/0/1)# ethernet-oam errored-frame threshold high 10
Switch(config-if-ethernet1/0/1)# exit
```

Шаг 2. Настройка на коммутаторе B:

```
Switch(config)# interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# ethernet-oam mode active
Switch(config-if-ethernet1/0/1)# ethernet-oam
Switch(config-if-ethernet1/0/1)# ethernet-oam errored-frame window 20
Switch(config-if-ethernet1/0/1)# ethernet-oam errored-frame threshold high 10
Switch(config-if-ethernet1/0/1)# exit
```

Шаг 3. Проверка результатов настройки:

Просмотр сводной информации обо всех соединениях Ethernet OAM:
Switch(config)# show ethernet-oam

Результат работы программы показан на рисунке справа:

Capability codes: L - Link Monitor, R - Remote Loopback
U - Unidirection, V - Variable Retrieval

InterfaceLocal-Mode	Local-Capability	Remote-MAC-Addr	Remote-Mode Remote-Capability
1 passive	L	00-e0-4c-00-00-07 active	L

Просмотр конфигурации событий канала на порту 1
Switch(config)# show ethernet-oam link-events-configuration interface ethernet 1/0/1

Результат работы команды представлен на рисунке ниже:

```
Ethernet1/0/1 link-monitor configuration:
event high-threshold      low-threshold window(200ms
-------------------------------------------------------------------------------------------------------------
Err-symbol-period:        none          1          5
Err-frame-period:         none          1          5
Err-frame:                10            1          20
Err-frame-seconds-summary: none         1          300
-------------------------------------------------------------------------------------------------------------
```

После настройки функции EFM коммутаторы **A** и **B** способны автоматически отслеживать ошибки на линии и контролировать качество канала. Администратор может своевременно выявлять и устранять сбои соединения, что обеспечивает стабильность и надежность работы сети.

3.11 Настройка файлового сервера (FTP)

В этом примере коммутатор выполняет роль FTP-клиента, а удаленный сервер с IP-адресом **10.2.2.50/24** — роль FTP-сервера. Основные задачи включают: загрузку системного программного обеспечения с FTP-сервера на коммутатор, а также создание резервной копии текущей конфигурации на FTP-сервере. IP-адрес коммутатора: **10.2.2.56/24**, связь с сервером установлена.

Этапы настройки:

Шаг 1. Настройка FTP-сервера. Запустите FTP-сервер на удаленном устройстве и создайте учетную запись пользователя для доступа (например, имя пользователя **Switch**, пароль **superuser**).

Шаг 2. Передача файлов через FTP на коммутаторе.

Отправка конфигурации startup-config на FTP-сервер:
Switch# copy *ftp://Switch:superuser@10.2.2.50/startup.cfg startup.cfg*
Confirm to overwrite the existed destination file? [Y/N]: y

Загрузка текущей рабочей конфигурации на FTP-сервер:
Switch# copy running-config *ftp://Switch:superuser@10.2.2.50/running.cfg*
Confirm to copy file? [Y/N]: y

Загрузка файла обновления с FTP-сервера на коммутатор:
Switch# copy *ftp://Switch:superuser@10.2.2.50/nos.img nos.img*
Confirm to overwrite the existed destination file? [Y/N]: y

Шаг 3. Проверка результатов настройки.

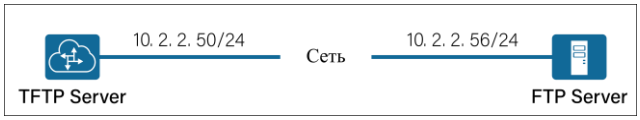
Просмотр содержимого флеш-памяти коммутатора:
Switch# show flash

Результат работы команды показан на рисунке справа:

```
total  22802K
-rw-  10817705    mantest.img
-rw-  12529295    nos.img
-rw-  1049    startup.cfg

Drive : flash:
Size:30.0M    Used:23.5M Available:6.5M  Use:78
```

После выполнения этих действий коммутатор может безопасно получать обновления программного обеспечения и сохранять резервные копии конфигурации на FTP-сервере. Это обеспечивает простое восстановление системы в случае сбоя и упрощает процессы обновления и резервного копирования.

3.12 Настройка файлового сервера (TFTP)



В этом примере коммутатор выполняет роль **TFTP-клиента**, а удаленный сервер с IP-адресом **10.2.2.50/24** — роль **TFTP-сервера**. Основные задачи включают: загрузку системного программного обеспечения с TFTP-сервера на коммутатор, а также создание резервной копии текущей конфигурации на TFTP-сервере. IP-адрес коммутатора: **10.2.2.56/24**, связь с сервером установлена.

Этапы настройки:

Шаг 1. Настройка TFTP-сервера. Запустите программное обеспечение TFTP на сервере и убедитесь, что создана папка для хранения файлов конфигурации и образов системы.

Шаг 2. Передача файлов через TFTP на коммутаторе.

Загрузка файла настроек с сервера на коммутатор:
Switch(config)# copy tftp://10.2.2.50/startup.cfg startup.cfg
Confirm to overwrite the existed destination file? [Y/N]: y

Загрузка текущей рабочей конфигурации коммутатора на TFTP-сервер:
Switch# copy running-config tftp: //10.2.2.50/running.cfg
Confirm to copy file? [Y/N]: y

Загрузка обновления коммутатора с TFTP-сервера:
Switch# copy tftp:/10.2.2.50/nos.img nos.img
Confirm to overwrite the existed destination file? [Y/N]: y

Шаг 3. Проверка результатов настройки.

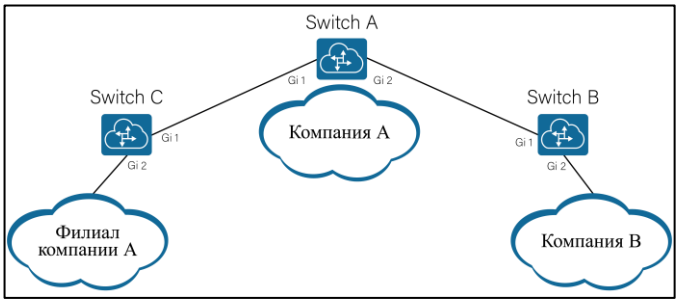
Просмотр содержимого флеш-памяти коммутатора:
Switch# show flash

Результат работы команды показан на рисунке справа:

```
total  22802K
-rw-  10817705    mantest.img
-rw-  12529295    nos.img
-rw-  1049    startup.cfg

Drive : flash:
Size:30.0M    Used:23.5M Available:6.5M  Use:78
```

После выполнения этих действий коммутатор может безопасно получать обновления системы и сохранять резервные копии конфигурации на TFTP-сервере. Это обеспечивает упрощённое восстановление настроек и обновление программного обеспечения без прерывания работы сети.

3.13 Настройка динамического VLAN (GVRP)



В данном примере коммутаторы обеспечивают автоматическую синхронизацию VLAN между филиалом компании «А» и отделом закупок компании «Б». Для этого используется протокол **GVRP (GARP VLAN Registration Protocol)**, который автоматически передаёт информацию о VLAN между коммутаторами, упрощая управление VLAN при расширении сети.

Этапы настройки:

Шаг 1. Включение функции GVRP на коммутаторе А:

SwitchA(config)# gvrp

Шаг 2. Создание VLAN на коммутаторе В:

SwitchB(config)# vlan 100,102-105

Шаг 3. Настройка trunk-портов и включение GVRP.

Коммутатор А:
SwitchA(config)# interface ethernet 1/0/1-2
SwitchA(config-if-port-range)# switchport mode trunk
SwitchA(config-if-port-range)# gvrp

Коммутатор С:
SwitchC(config)# interface ethernet 1/0/1-2
SwitchC(config-if-port-range)# switchport mode trunk
SwitchC(config-if-port-range)# gvrp

Коммутатор В:
SwitchB(config)# interface ethernet 1/0/1-2
SwitchB(config-if-port-range)# switchport mode trunk
SwitchB(config-if-port-range)# switchport trunk allowed vlan add 100,102-105
SwitchB(config-if-port-range)# gvrp

Дополнительно (пример настройки таймеров на коммутаторе А):

SwitchA(config)#garp timer join 210
SwitchA(config)#garp timer leave 700
SwitchA(config)#garp timer leaveall 20000
SwitchA(config)#show garp timer

Шаг 4: Проверка результата настройки.

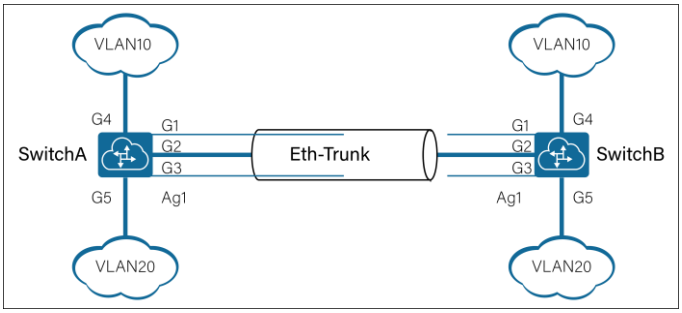
Проверка VLAN на коммутаторах:
SwitchA(config)# show vlan

Результат работы команды представлен на рисунке справа:

VLAN	Name	Type	Media	Ports	
1	default	Static	ENET	Ethernet1/0/1	Ethernet1/0/2
				Ethernet1/0/3	Ethernet1/0/4
				Ethernet1/0/5	Ethernet1/0/6
				Ethernet1/0/7	Ethernet1/0/8
				Ethernet1/0/9	Ethernet1/0/10
100	VLAN0100	Dynamic	ENET	Ethernet1/0/1(T)	
102	VLAN0102	Dynamic	ENET	Ethernet1/0/1(T)	
103	VLAN0103	Dynamic	ENET	Ethernet1/0/1(T)	
104	VLAN0104	Dynamic	ENET	Ethernet1/0/1(T)	
105	VLAN0105	Dynamic	ENET	Ethernet1/0/1(T)	

После настройки GVRP коммутаторы автоматически синхронизируют информацию о VLAN между собой. Это обеспечивает корректную маршрутизацию трафика между отделами компании «А» и «Б», упрощает управление VLAN при добавлении новых отделов или филиалов и снижает риск ошибок при ручной конфигурации.

3.14 Настройка агрегирования каналов (LACP)



В данном примере коммутаторы **A** и **B** соединены между собой несколькими физическими портами для передачи трафика VLAN 10 и VLAN 20. Для увеличения пропускной способности и обеспечения отказоустойчивости используется агрегирование каналов с помощью **LACP (Link Aggregation Control Protocol)**. Агрегация позволяет объединить несколько физических портов в один логический канал, обеспечивая балансировку трафика и резервирование при отказе одного из портов.

Этапы настройки:

Шаг 1. Создание порт-группы и добавление участников на коммутаторах A и B.

Коммутатор A:
SwitchA(config)# port-group 1
SwitchA(config)# interface ethernet 1/0/1-3
SwitchA(config-if-port-range)# port-group 1 mode on

Коммутатор B:
SwitchB(config)# port-group 1
SwitchB(config)# interface ethernet 1/0/1-3
SwitchB(config-if-port-range)# port-group 1 mode on

Шаг 2: Создание VLAN и настройка trunk-портов.

Коммутатор A:
SwitchA(config)# vlan 10,20
SwitchA(config)# interface ethernet 1/0/4
SwitchA(config-if-ethernet1/0/4)# switchport mode trunk
SwitchA(config-if-ethernet1/0/4)# switchport trunk allowed vlan add 10

SwitchA(config-if-ethernet1/0/4)# interface ethernet 1/0/5
SwitchA(config-if-ethernet1/0/5)# switchport mode trunk
SwitchA(config-if-ethernet1/0/5)# switchport trunk allowed vlan add 20

Настройка логического канала Eth-Trunk 1:

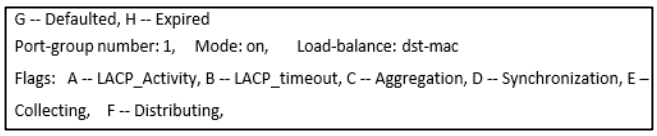
```
SwitchA(config)# interface port-channel 1
SwitchA(config-if-port-channel1)# switchport mode trunk
SwitchA(config-if-port-channel1)# switchport trunk allowed vlan add 10,20
```

Шаг 3. Настройка алгоритма балансировки трафика:

```
SwitchA(config)# load-balance dst-mac
```

Шаг 4. Проверка результата настройки. Проверка состояния агрегированного канала:

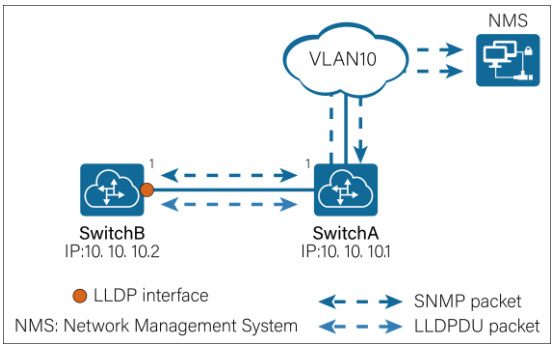
```
Switch(config)#show port-group 1 detail
```



Результат команды показан на рисунке справа:

После настройки LACP физические порты коммутаторов объединяются в один логический канал, что увеличивает пропускную способность между A и B, обеспечивает резервирование при отказе отдельных портов и равномерное распределение трафика по VLAN. Эта конфигурация повышает надежность и эффективность передачи данных в сети.

3.15 Настройка протокола обнаружения и сбора характеристик о соседях



В данном примере коммутаторы **A** и **B** соединены напрямую и управляются системой мониторинга сети (NMS) по протоколу SNMP. Для автоматического обнаружения соседних устройств, получения информации об их характеристиках, а также построения актуальной топологии сети используется протокол **LLDP (Link Layer Discovery Protocol)**.
LDP позволяет передавать сведения об устройстве (имя, модель, порт подключения, возможности) между соседними сетевыми устройствами канального уровня. Это упрощает администрирование сети, ускоряет выявление неисправностей и помогает обнаруживать ошибки конфигурации.

Этапы настройки:

Шаг 1. Настройка IP-адресов управления на VLAN 1:

```
SwitchA(config)# interface vlan 1
SwitchA(config-if-vlan1)# ip address 10.10.10.1 255.255.255.0
SwitchA(config-if-vlan1)# exit

SwitchB(config)# interface vlan 1
SwitchB(config-if-vlan1)# ip address 10.10.10.2 255.255.255.0
SwitchB(config-if-vlan1)# exit
```

Шаг 2. Включение LLDP на коммутаторах:

```
SwitchA(config)# lldp enable

SwitchB(config)# lldp enable
```

Шаг 3. Проверка результата настройки:

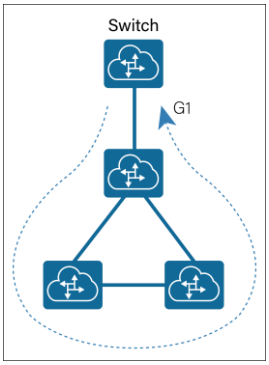
SwitchA(config)# show lldp neighbors brief

Команда отображает краткую информацию о соседних устройствах, обнаруженных через LLDP:

Local Interface	Chassis ID	CID subtype	Port ID	PID
subtype	Time Mark	System Name	-	
Ethernet1/0/1	00-e0-4c-00-00-00	4		gi4
Local	109			

После включения LLDP коммутаторы автоматически обмениваются информацией о своих характеристиках и состоянии соединения. Это позволяет системе управления сетью получать актуальные данные о топологии, отслеживать состояние каналов связи и оперативно выявлять возможные проблемы или конфигурационные несоответствия.

3.16 Настройка механизма обнаружения петель (LBD)



В данном сценарии интерфейс 10GE1/0/1 подключен к нижестоящей сети. При возникновении физической или логической петли в подключённом сегменте возможен широковещательный шторм, что приведёт к резкому росту нагрузки на процессор и каналы передачи данных коммутатора. Это может вызвать деградацию производительности сети или даже полную недоступность сервисов.
Для предотвращения подобных ситуаций используется механизм Loopback Detection (LBD). Данная функция позволяет обнаруживать закольцовывание трафика на порту и автоматически предпринимать защитные меры, например, переводить интерфейс в состояние shutdown. Это минимизирует влияние петли на остальные сегменты сети.

Этапы настройки:

Шаг 1. Настройка отключения интерфейса при обнаружении петли:

Switch(config)# interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# loopback-detection control shutdown

При обнаружении петли интерфейс будет автоматически отключён.

Шаг 2. Настройка VLAN для контроля петель:

Switch(config)# interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# switchport mode trunk
Switch(config-if-ethernet1/0/1)# switchport trunk allowed vlan all
Switch(config-if-ethernet1/0/1)# loopback-detection specified-vlan 1;3;5-20

Функция LBD будет отслеживать появление петель в указанных VLAN.

Шаг 3. Настройка параметров работы LBD.

Настройка интервала отправки и повторной проверки пакетов LBD:
Switch(config)# loopback-detection interval-time 35 15

Включение автоматического восстановления интерфейса:
Switch(config)# loopback-detection control-recovery timeout 30

- **interval-time 35 15** — задаёт параметры периодичности проверки.
- **control-recovery timeout 30** — включает автоматическое восстановление порта через 30 секунд после его отключения.

Шаг 4. Проверка результата настройки:

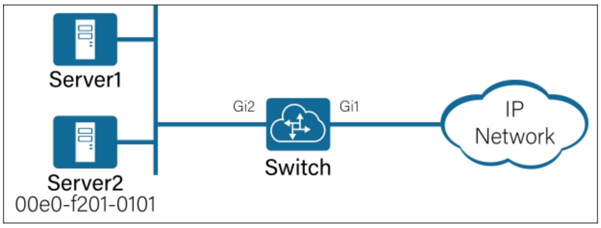
Switch(config)# show loopback-detection

```
Loopback Detection Global Information
Transmit Interval    : 35s(loopback mode), 15s(no loopback mode) Control Re-
cover Time : 30
Loopback Detection Port Information
PortName              Loopback  Detection              Control  Mode     Is  Controlled
Happen times
Ethernet1/0/1         Enable                                Shutdown              No
0
Ethernet1/0/2         Disable                          No                         No
0
Ethernet1/0/3         Disable                          No                         No
0
Ethernet1/0/4         Disable                          No                         No
0
Ethernet1/0/5         Disable                          No                         No
0
Ethernet1/0/6         Disable                          No                         No
0
Ethernet1/0/7         Disable                          No                         No
0
Ethernet1/0/8         Disable                          No                         No
0
Ethernet1/0/9         Disable                          No                         No
0
Ethernet1/0/10        Disable                          No                         No
0
```

Команда отображает текущий статус функции обнаружения петель и состояние интерфейсов:

После настройки LBD коммутатор способен автоматически выявлять петли во внешнем сегменте сети и оперативно блокировать проблемный порт. Это предотвращает широковещательные штормы, снижает риск перегрузки оборудования и обеспечивает стабильную работу всей сетевой инфраструктуры.

3.17 Настройка таблицы MAC-адресов



Глобальная настройка таблицы MAC-адресов позволяет управлять процессом обучения адресов, временем их хранения, ограничением количества записей, а также реализовывать механизмы фильтрации и статической привязки. Это повышает управляемость сети, предотвращает несанкционированный доступ и снижает риск перегрузки таблицы MAC-адресов.
В рамках данного примера выполняется настройка чёрного списка, статической и многоадресной привязки, а также параметров динамического обучения MAC-адресов.

Настройка фильтрации и статических записей

Этапы настройки:

Шаг 1. Добавление MAC-адреса в чёрный список:

Switch(config)# mac-address-table blackhole address 00-e0-f2-01-01-01 vlan 1

Данный MAC-адрес будет отфильтрован, а трафик от него — отброшен.

Проверка результата настройки:
Switch(config)# show mac address-table-blackhole

```
Read mac address table....
Vlan Mac Address                    Type     Creator    Ports
---- ---------------------------- ----- -----------------------------
1    00-e0-f2-01-01-01              STATIC   User       (blackhole)|(both)
```

Команда отображает MAC-адреса, добавленных в черный список:

Шаг 2. Настройка статической привязки MAC-адреса:

Switch(config)# mac-address-table static address 02-60-e2-07-00-02 vlan 1 interface ethernet 1/0/2

MAC-адрес будет жёстко привязан к указанному интерфейсу и VLAN.

Проверка результата настройки:
Switch(config)# show mac-address-table static

Результат работы команды показан справа:

```
View binding information
Switch(config)#show mac-address-table static vlan 1 interface ethernet 1/0/2
Read mac address table....
Vlan Mac Address                    Type      Creator    Ports
---- ------------------------------ ------ ------------------------------
1    02-60-e2-07-00-02              STATIC    User       Ethernet1/0/2
```

Шаг 3. Настройка статической многоадресной привязки:

Switch(config)# l2-address-table static-multicast address 01-e0-f2-01-01-01 vlan 1 interface ethernet 1/0/2

Настраивается обработка multicast-трафика для указанного VLAN и интерфейса.

Проверка результата настройки:
Switch(config)# show l2-address-table multicast

Результат работы команды показан справа:

```
View configuration binding information
Switch(config)#show l2-address-table multicast
Vlan Address                        Insert      Type      Creator    Ports
---- ------------------------------ ----------- ------ ------------------------------
1    01-e0-f2-01-01-01              Insert      STATIC    User       Ethernet1/0/2
```

Настройка параметров динамического обучения MAC-адресов

Этапы настройки:

Шаг 1. Настройка времени хранения записей (Aging Time):

Switch(config)# mac-address-table aging-time 60

Время хранения динамических MAC-адресов устанавливается равным 60 секундам.

Проверка результата настройки:
Switch(config)# show mac-address-table aging-time
Aging-time is: 60(s)

Шаг 2. Включение динамического обучения MAC-адресов на интерфейсе:

Switch(config)# mac-address-learning enable interface ethernet 1/0/2

Шаг 3. Ограничение максимального количества динамических MAC-адресов:

Switch(config)# mac-address dynamic maximum 1024

Устанавливается максимальное количество записей в таблице (диапазон 1–4096).

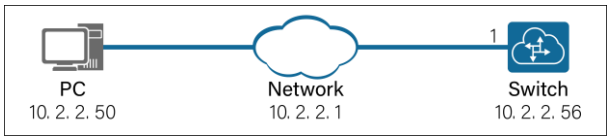
После выполнения настройки коммутатор:

- фильтрует трафик от MAC-адресов, внесённых в чёрный список;
- использует статические и multicast-привязки для контроля пересылки кадров;
- управляет временем хранения динамических записей;

- ограничивает максимальное количество изучаемых MAC-адресов.

Такая конфигурация повышает безопасность сети, предотвращает переполнение таблицы MAC-адресов и обеспечивает стабильную работу коммутатора.

3.18 Настройка интерфейса управления



В данном примере коммутатор подключён к хосту через выделенный VLAN управления (VLAN 4094). Для удалённого администрирования создаётся отдельный интерфейс VLAN с назначением IPv4- и IPv6-адресов. Это позволяет изолировать управляющий трафик от пользовательского и обеспечить безопасный доступ к устройству по сети.

Этапы настройки:

Шаг 1. Создание VLAN 4094 и добавление порта:

```
Switch(config)# vlan 4094
Switch(config-vlan4094)# exit

Switch(config)# interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# switchport access vlan 4094
```

Порт Ethernet 1/0/1 переводится в VLAN 4094 для подключения управляющего хоста.

Шаг 2. Настройка IP-адреса интерфейса управления:

```
Switch(config)# interface vlan 4094
Switch(config-if-vlan4094)# ip address 10.2.2.56 255.255.255.0
Switch(config-if-vlan4094)# ipv6 address 2001::1/64
Switch(config-if-vlan4094)# exit
```

Интерфейсу VLAN 4094 назначаются IPv4- и IPv6-адреса для обеспечения удалённого доступа по обоим протоколам.

Шаг 4. Проверка результата настройки:

```
Switch(config)#show ip interface brief
```

Команда позволяет убедиться, что интерфейс VLAN 4094 находится в состоянии **Up** и IP-адрес назначен корректно:

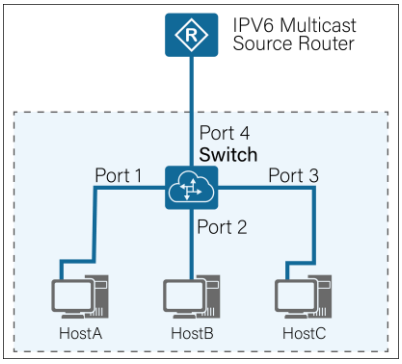
Index	Interface	IP-Address	Protocol
15094	Vlan4094	10.2.2.56	up
17500	Loopback	127.0.0.1	up

После выполнения настройки коммутатор получает выделенный интерфейс управления в VLAN 4094. Это обеспечивает:

- изоляцию управляющего трафика от пользовательских VLAN;
- возможность удалённого администрирования по IPv4 и IPv6;
- повышение безопасности и управляемости устройства.

Настройка интерфейса управления является обязательным этапом при вводе коммутатора в эксплуатацию.

3.19 Настройка оптимизации IPv6-мультикаста (MLD Snooping)



В данном примере хосты A, B и C подключены к разным VLAN (VLAN 2, VLAN 3 и VLAN 4 соответственно) и получают трафик IPv6-мультикаста из диапазона групп **FF02::0101 – FF02::0103**. Для предотвращения рассылки мультикаст-трафика на все порты VLAN используется механизм **MLD Snooping**, который анализирует MLD-сообщения и формирует таблицу подписчиков, обеспечивая передачу трафика только заинтересованным узлам.

Базовая настройка MLD Snooping

Этапы настройки:

Шаг 1. Создание VLAN и настройка портов:

```
Switch(config)# vlan 2-4

Switch(config)# interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# switchport mode access
Switch(config-if-ethernet1/0/1)# switchport access vlan 2
Switch(config-if-ethernet1/0/1)# exit

Switch(config)# interface ethernet1/0/ 2
Switch(config-if-ethernet1/0/2)# switchport mode access
Switch(config-if-ethernet1/0/2)# switchport access vlan 3
Switch(config-if-ethernet1/0/2)# exit

Switch(config)# interface ethernet 1/0/3
Switch(config-if-ethernet1/0/3)# switchport mode access
Switch(config-if-ethernet1/0/3)# switchport access vlan 4
Switch(config-if-ethernet1/0/3)# exit

Switch(config-if-ethernet1/0/3)# interface ethernet1/0/4
Switch(config-if-ethernet1/0/4)# switchport mode trunk
Switch(config-if-ethernet1/0/4)# switchport trunk allowed vlan add 2-4
```

Шаг 2. Включение MLD Snooping:

```
Switch(config)# ipv6 mld snooping
Switch(config)# ipv6 mld snooping vlan 2
Switch(config)# ipv6 mld snooping vlan 3
Switch(config)# ipv6 mld snooping vlan 4
```

Шаг 3. Проверка результата настройки:

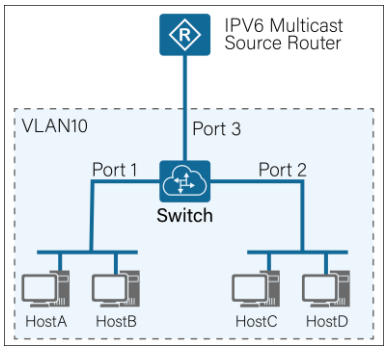
```
Switch(config)# show ipv6 mld snooping
```

Команда отображает состояние функции, активные VLAN и таблицу групп мультикаста:

```
Global mld snooping status: Enabled
L3 multicasting: running
Mld snooping is turned on for vlan 1
Mld snooping is turned on for vlan 2
Mld snooping is turned on for vlan 3
Mld snooping is turned on for vlan 4
```

После включения MLD Snooping коммутатор пересылает IPv6-мультикаст-трафик только на те порты, где есть подписчики соответствующих групп. Это снижает нагрузку на сеть и предотвращает ненужную рассылку трафика.

Статическая настройка портов для IPv6-мультикаста



В данном сценарии маршрутизатор передаёт данные в несколько фиксированных IPv6-мультикаст-групп. Динамический механизм управления группами отключён, поэтому требуется статическая привязка портов к определённым потокам. Устройства: A и B принимают группы 01–03, C и D принимают группы 04–05.

Этапы настройки:

Шаг 1. Создание VLAN и настройка портов:

```
Switch(config)# vlan 10
Switch(config)# interface ethernet 1/0/1-2
Switch(config-if-range)# switchport access vlan 10

Switch(config)# interface ethernet 1/0/3
Switch(config-if-ethernet 1/0/3)# switchport mode trunk
Switch(config-if-ethernet 1/0/3)# switchport trunk allowed vlan add 10
Switch(config-if-ethernet 1/0/3)# exit
```

Шаг 2. Включение MLD Snooping.

Глобальное включение функции:

```
Switch(config)# ipv6 mld snooping
```

Активация MLD Snooping для VLAN 10:

```
Switch(config)# ipv6 mld snooping vlan 10
```

Шаг 3. Настройка mrouter-порта:

```
Switch(config)# ipv6 mld snooping vlan 10 mrouter-port interface ethernet 1/0/3
```

Этот порт подключён к маршрутизатору и используется как источник мультикаст-трафика.

Шаг 4. Статическая привязка MAC-адресов мультикаста:

```
Switch(config)# mac-address-table static address 22-33-00-00-01-01 vlan 10 interface ethernet 1/0/1
Switch(config)# mac-address-table static address 22-33-00-00-01-02 vlan 10 interface ethernet 1/0/1
Switch(config)# mac-address-table static address 22-33-00-00-01-03 vlan 10 interface ethernet 1/0/1

Switch(config)# mac-address-table static address 22-33-00-00-01-04 vlan 10 interface ethernet 1/0/2
Switch(config)# mac-address-table static address 22-33-00-00-01-05 vlan 10 interface ethernet 1/0/2
```

Шаг 5. Проверка результата настройки:

Switch(config)# show ipv6 mld snooping

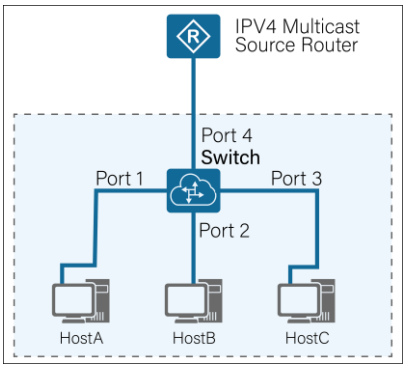
Статическая конфигурация MLD Snooping позволяет жёстко закрепить мультикаст-группы за конкретными портами. Такой подход применяется в сетях с фиксированной топологией и постоянным распределением потоков, обеспечивая предсказуемость передачи и минимизацию лишнего трафика.

Использование MLD Snooping:

- оптимизирует передачу IPv6-мультикаста;
- снижает нагрузку на каналы и оборудование;
- предотвращает широковещательные штормы;
- позволяет реализовать как динамическую, так и статическую модель распределения мультикаст-трафика.

Настройка является важной частью построения эффективной IPv6-инфраструктуры.

3.20 Настройка оптимизации IPv4-мультикаста (IGMP Snooping)



В данной топологии маршрутизатор подключён к пользовательской сети через коммутатор уровня L2. В сети присутствуют три получателя мультикаста: Узел A — VLAN 2, Узел B — VLAN 3, Узел C — VLAN 4.
Все устройства планируют получать IPv4-мультикаст-трафик в диапазоне групп 225.1.1.1 – 225.1.1.3. Для предотвращения рассылки мультикаст-трафика на все порты VLAN используется механизм IGMP Snooping, который анализирует IGMP-сообщения и пересылает трафик только на порты, где находятся подписчики соответствующих групп.

Этапы настройки:

Шаг 1. Настройка VLAN и интерфейсов.

Создание VLAN 2–4 и распределение портов:
Switch(config)# vlan 2-4

Switch(config)# interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# switchport access vlan 2
Set the port Ethernet1/0/1 access vlan 2 successfully

Switch(config-if-ethernet1/0/1)#interface ethernet 1/0/2
Switch(config-if-ethernet1/0/2)# switchport access vlan 3
Set the port Ethernet1/0/2 access vlan 3 successfully

Switch(config-if-ethernet1/0/2)#interface ethernet 1/0/3
Switch(config-if-ethernet1/0/3)# switchport access vlan 4
Set the port Ethernet1/0/3 access vlan 4 successfully

Switch(config-if-ethernet1/0/3)#interface ethernet 1/0/4
Switch(config-if-ethernet1/0/4)# switchport mode hybrid
Set the port Ethernet1/0/4 mode Hybrid successfully

Switch(config-if-ethernet1/0/4)# switchport hybrid allowed vlan 2-4 untag
set the Hybrid port Ethernet1/0/4 untag allowed vlan successfully
Switch(config-if-ethernet1/0/4)# exit

Порт 1/0/4 используется для подключения к маршрутизатору и обеспечивает прохождение трафика VLAN 2–4.

Шаг 2. Включение IGMP Snooping.

Глобальное включение функции:
Switch(config)# ip igmp snooping

#Активация IGMP Snooping для нужных VLAN:
Switch(config)# ip igmp snooping vlan 2
Switch(config)# ip igmp snooping vlan 3
Switch(config)# ip igmp snooping vlan 4

Шаг 3. Проверка результата настройки.

Просмотр глобального состояния функции:
Switch(config)#show ip igmp snooping

Пример вывода:
Global igmp snooping status : Enabled
Igmp snooping is turned on for vlan 2
Igmp snooping is turned on for vlan 3
Igmp snooping is turned on for vlan 4

Для просмотра параметров конкретного VLAN:
Switch(config)# show ip igmp snooping vlan <1-4094>

Результат работы команды для VLAN 2:

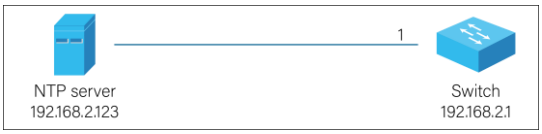
```
Igmp snooping information for vlan 2

Igmp snooping L2 general querier                :Yes(COULD_QUERY)
Igmp snooping query-interval                     :125(s)
Igmp snooping max response time                  :10(s)
Igmp snooping specific-query max response time   :1(s)
Igmp snooping robustness                         :2
Igmp snooping mrouter port keep-alive time       :65(s)
Igmp snooping query-suppression time             :65(s)
```

Принцип работы в данной топологии:

- Когда устройства A, B и C отправляют IGMP Report (сообщения о подписке), коммутатор формирует записи в таблице мультикаст-групп.
- Когда маршрутизатор отправляет IGMP Query, коммутатор определяет порт маршрутизатора (router port).
- При поступлении мультикаст-трафика для групп 225.1.1.1 – 225.1.1.3 коммутатор пересылает его только на порты, где находятся подписчики соответствующих групп.

После включения IGMP Snooping коммутатор предотвращает широковещательную рассылку мультикаст-трафика, направляет трафик только заинтересованным получателям, снижает нагрузку на сеть и оборудование, повышает эффективность использования полосы пропускания. Настройка IGMP Snooping является обязательным элементом оптимизации IPv4-мультикаст-трафика в сетях уровня L2.

3.21 Настройка протокола сетевого времени (NTP)



В данной топологии коммутатор должен синхронизировать системное время с внешним NTP-сервером. Корректная настройка времени необходима для ведения журналов событий (log), корректной работы механизмов безопасности (AAA, 802.1X, сертификаты), точной фиксации времени возникновения аварий и инцидентов, синхронизации с другими сетевыми устройствами. NTP-сервер доступен по сети, и коммутатор может установить с ним соединение для регулярной синхронизации.

Этапы настройки:

Шаг 1. Включение NTP:

```
Switch(config)# ntp enable
```

Шаг 2. Добавление адреса NTP-сервера:

```
Switch(config)# ntp server 192.168.2.123
```

Шаг 3. Настройка интерфейса VLAN:

```
Switch(config)# interface vlan 1
Switch(config-if-vlan1)# ip address 192.168.2.1 255.255.255.0
Switch(config-if-vlan1)# exit
```

Коммутатор должен находиться в одной сети с NTP-сервером либо иметь маршрут до него.

Шаг 4. Настройка часового пояса:

```
Switch(config)# clock timezone Krasnoyarsk add 7
```

Настройка часового пояса обеспечивает корректное отображение локального времени в журналах и системных событиях.

Шаг 5. Настройка интервала синхронизации:

```
Switch(config)# ntp syn-interval 100
```

Параметр определяет интервал отправки запросов к NTP-серверу для обновления времени.

Шаг 6. Проверка результатов настройки:

```
Switch(config)#show ntp status
ntp clock status: synchronized
Clock stratum:2

Reference clock server:192.168.2.123
Clock offset:-57600.854 s
Root delay:0.000 ms
Root dispersion:10148.699 ms
Reference time:Wed May    5 13:59:3.755 2021
Syn-interval:100s                          1          20
```

```
Switch(config)# show ntp status
```

По выводу команды можно определить установлен ли сеанс синхронизации, доступен ли сервер, синхронизировано ли системное время устройства:

После выполнения настройки коммутатор автоматически синхронизирует системное время с NTP-сервером, обеспечивает корректность журна-

лов и событий безопасности, поддерживает согласованное время во всей сетевой инфраструктуре. Использование NTP является обязательной практикой при эксплуатации корпоративных сетей.

3.22 Настройка ONVIF

Согласно спецификации протокола ONVIF, процесс обнаружения устройств основан на механизме WS-Discovery. Клиент отправляет широковещательное (multicast) сообщение **Probe** на адрес **239.255.255.250:3702 (UDP)** внутри локального сегмента сети. Устройства, поддерживающие ONVIF (IP-камеры, видеорегистраторы и др.), принимают этот запрос и отправляют ответ **ProbeMatch**, содержащий информацию о себе.
Для корректной работы механизмов обнаружения необходимо:

- поддержка мультикаст-трафика в сети;
- отсутствие блокировки UDP-порта 3702;
- корректная настройка VLAN и маршрутизации (если применимо).

В рассматриваемом сценарии коммутатор выполняет роль клиента обнаружения ONVIF-устройств (IP-камер), а также может работать как ONVIF-сервер.

Настройка обнаружения ONVIF-устройств

Подключите коммутатор к IP-камере и выполните следующие действия:

Шаг 1. Включение функции обнаружения ONVIF:

```
Switch(config)# onvif detect enable
```

После включения коммутатор начинает отправку Probe-сообщений в сеть.

Шаг 2. Просмотр базы обнаруженных устройств:

```
Switch(config)# show onvif detect database
```

Команда отображает IP-адрес обнаруженного устройства, тип устройства, идентификатор, дополнительную информацию о камере.

Настройка ONVIF-сервера на коммутаторе

Коммутатор также может функционировать как ONVIF-сервер, отвечая на запросы обнаружения от других клиентов.

Этапы настройки:

Шаг 1. Включение ONVIF-сервера:

```
Switch(config)# onvif server enable
```

Шаг 2. Проверка состояния ONVIF-сервера:

```
Switch(config)# show onvif server
```

Пример вывода:
Onvif server status: Enable

После выполнения настройки коммутатор способен автоматически обнаруживать ONVIF-устройства в локальном сегменте сети, формируется база подключённых IP-камер, при необходимости устройство может функционировать как ONVIF-сервер, обеспечивается упрощённая интеграция оборудования видеонаблюдения в сетевую инфраструктуру. Использование ONVIF значительно упрощает развертывание и администрирование систем видеонаблюдения.

3.23 Настройка PoE

Функция **PoE (Power over Ethernet)** позволяет коммутатору передавать электропитание подключённым устройствам (IP-камерам, точкам доступа, IP-телефонам и т.д.) по тому же кабелю Ethernet, по которому передаются данные.

Внимание! Функция PoE поддерживается только теми моделями коммутаторов, которые оснащены встроенными PoE-модулями!

Глобальная конфигурация PoE предназначена для управления общей доступной мощностью устройства и мониторинга состояния системы питания.
Коммутатор может обеспечивать питание в пределах своего максимального бюджета мощности. Например, если модель поддерживает до 140 Вт, администратор может ограничить этот бюджет до 120 Вт для контроля нагрузки или резервирования ресурса.

Глобальная настройка PoE

Этапы настройки:

Шаг 1. Изменение общего лимита мощности:

Switch(config)# power inline max 120

После выполнения команды общий доступный бюджет PoE будет ограничен 120 Вт.

Шаг 2. Проверка состояния PoE:

Switch(config)# show power inline

Команда отображает общий доступный бюджет мощности, текущую потребляемую мощность, состояние PoE по портам, наличие перегрузок или отключений:

PoE Work Status : online
PoE Port Max Number 24
PoE Support Type : 802.3at/802.3af PoE MCU Software Version : V1.1.2
PoE Power Available : 120 W
PoE Power Used : 0 W
PoE Power Remaining : 120 W
PoE Main Voltage : 54.1 V
PoE Min Voltage : 44 V
PoE Max Voltage : 57 V
PoE Police : Disable

Настройка PoE на уровне порта

В режиме конфигурации интерфейса можно управлять параметрами питания конкретного порта.

Этапы настройки:

Шаг 1. Включение или отключение PoE на порту:

```
Switch(config-if-ethernet1/0/1)# no power inline enable
Switch(config-if-ethernet1/0/1)# power inline enable
```

- **no power inline enable** — отключает питание на порту;
- **power inline enable** — включает питание.

Шаг 2. Настройка максимальной мощности порта:

```
Switch(config-if-ethernet1/0/1)# power inline max 25000
```

Значение указывается в милливаттах (например, 25000 мВт = 25 Вт).

Шаг 3. Настройка приоритета порта:

```
Switch(config-if-ethernet1/0/1)# power inline priority?
critical  Critical priority
high      High priority
low       Low priority
```

Приоритет используется в ситуации нехватки общего бюджета мощности:

- **critical** — питание сохраняется в первую очередь;
- **high** — высокий приоритет;
- **low** — питание может быть отключено первым.

Шаг 3. Проверка результата настройки:

```
Switch(config)# show power inline interface
```

Команда позволяет проверить состояние питания конкретного порта, выделенную и фактическую мощность, установленный приоритет:

Interface	Status	Oper	Power(mW)	Max(mW)	Current(mA)	Volt(V)	Priority	Class
Ethernet1/0/1	Enable	Off	0	25000	0	54	Critical	N/A
Ethernet1/0/2	Enable	Off	0	32000	0	54	Low	N/A
Ethernet1/0/3	Enable	Off	0	32000	0	54	Low	N/A
Ethernet1/0/4	Enable	Off	0	32000	0	54	Low	N/A
Ethernet1/0/5	Enable	Off	0	32000	0	54	Low	N/A
Ethernet1/0/6	Enable	Off	0	32000	0	54	Low	N/A
Ethernet1/0/7	Enable	Off	0	32000	0	54	Low	N/A
Ethernet1/0/8	Enable	Off	0	32000	0	54	Low	N/A

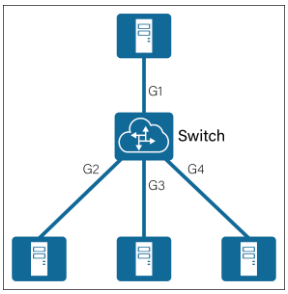
После выполнения настройки администратор получает возможность:

- управлять общим бюджетом PoE коммутатора;
- включать и отключать питание на отдельных портах;
- ограничивать максимальную мощность для подключённых устройств;
- задавать приоритеты питания при нехватке ресурсов.

Гибкая настройка PoE обеспечивает стабильную работу питаемых устройств и эффективное распределение энергоресурсов коммутатора.

3.24 Настройка портов

3.24.1 Настройка скорости и режима работы портов



Настройка скорости и режима дуплекса позволяет адаптировать параметры интерфейсов коммутатора под требования подключённых устройств. По умолчанию большинство портов работают в режиме автосогласования (auto), при котором автоматически определяется оптимальная скорость и тип дуплекса.

Этапы настройки:

Шаг 1. Настройка портов 1–4 в режиме auto. По умолчанию скорость и дуплекс установлены в режим автосогласования. При необходимости можно явно задать этот режим:

Switch(config)# interface ethernet 1/0/1-4
Switch(config-if-port-range)# speed-duplex auto

Switch(config)# show interface ethernet status

После настройки статус портов отображается следующим образом:

Codes: A-Down - administratively down, a - auto, f - force, G - Gigabit

Interface	Link/Protocol	Speed	Duplex	Vlan	Type
1/0/1	UP/UP	a-1G	a-FULL	1	G-TX
1/0/2	UP/UP	a-1G	a-FULL	1	G-TX
1/0/3	UP/UP	a-1G	a-FULL	1	G-TX
1/0/4	UP/UP	a-1G	a-FULL	1	G-TX
1/0/5	DOWN/DOWN	auto	auto	1	G-TX
1/0/6	DOWN/DOWN	auto	auto	1	G-TX
1/0/7	DOWN/DOWN	auto	auto	1	G-TX
1/0/8	DOWN/DOWN	auto	auto	1	G-TX
1/0/9	DOWN/DOWN	auto	auto	1	G-TX
1/0/10	DOWN/DOWN	auto	auto	1	G-TX

Обозначение **a-** указывает на работу в режиме автосогласования.

Шаг 2. Принудительная настройка скорости портов.

В данном примере: порт 1/0/2 — 1000 Мбит/с (1 Гбит/с), порт 1/0/3 — 100 Мбит/с, порт 1/0/4 — 10 Мбит/с:
Switch(config)# interface ethernet 1/0/2
Switch(config-if-ethernet1/0/2)# speed-duplex force1g-full

Switch(config-if-ethernet1/0/2)# interface ethernet 1/0/3
Switch(config-if-ethernet1/0/3)# speed-duplex force100-full

Switch(config-if-ethernet1/0/3)# interface ethernet 1/0/4
Switch(config-if-ethernet1/0/4)# speed-duplex force10-full

Switch(config)# show interface ethernet status

После настройки статус будет отображаться с префиксом **f-** (force):

Codes: A-Down - administratively down, a - auto, f - force, G - Gigabit

Interface	Link/Protocol	Speed	Duplex	Vlan	Type
1/0/1	UP/UP	a-1G	a-FULL	1	G-TX
1/0/2	UP/UP	f-1G	f-full	1	G-TX
1/0/3	UP/UP	f-100M	f-full	1	G-TX
1/0/4	UP/UP	f-10M	f-full	1	G-TX
1/0/5	DOWN/DOWN	auto	auto	1	G-TX
1/0/6	DOWN/DOWN	auto	auto	1	G-TX
1/0/7	DOWN/DOWN	auto	auto	1	G-TX
1/0/8	DOWN/DOWN	auto	auto	1	G-TX
1/0/9	DOWN/DOWN	auto	auto	1	G-TX
1/0/10	DOWN/DOWN	auto	auto	1	G-TX

Это означает, что параметры заданы вручную и автосогласование отключено.

Шаг 3. Настройка режима дуплекса.

В примере: порты 1–2 работают в режиме полного дуплекса (full-duplex), порты 3–4 — в режиме полудуплекса (half-duplex):
Switch(config)# interface ethernet 1/0/1-2
Switch(config-if-port-range)# speed-duplex force1g-full

Switch(config-if-port-range)# interface ethernet 1/0/3-4
Switch(config-if-port-range)# speed-duplex force100-half

Switch(config-if-port-range)# show interface ethernet status

Особенности работы half-duplex. *Если порт 3 передаёт данные со скоростью 70 Мбит/с, порт 4 сможет принять их со скоростью 70 Мбит/с. Однако, если оба порта (3 и 4) одновременно начнут передачу по 70 Мбит/с, фактическая скорость передачи и приёма будет ниже 70 Мбит/с. Это связано с тем, что в режиме* ***half-duplex*** *приём и передача не могут выполняться одновременно. Возникают коллизии, возможны повторные передачи кадров и снижение общей пропускной способности канала.*

Настройка скорости и режима дуплекса позволяет использовать автоматическое согласование параметров соединения, принудительно задавать скорость и тип дуплекса при необходимости, оптимизировать работу сети с устаревшими или специализированными устройствами, учитывать особенности режима half-duplex для предотвращения снижения производительности. Корректная настройка параметров портов обеспечивает стабильность соединения и эффективное использование пропускной способности сети.

3.24.2 Настройка статистики портов

Функция статистики портов позволяет отслеживать объём и тип передаваемого трафика, текущую скорость передачи данных, а также анализировать нагрузку на интерфейсы. Это необходимо для диагностики сетевых проблем, контроля пропускной способности и проверки корректности ограничений скорости.

Этапы настройки:

Шаг 1. Очистка статистики трафика. Перед началом тестирования рекомендуется обнулить счётчики интерфейсов:

Switch# clear counters

Команда очищает статистику по всем портам, что позволяет получить корректные результаты последующего измерения.

Шаг 2. Просмотр детальной статистики интерфейса. После отправки одноадресных (unicast) пакетов размером 128 байт с использованием тестового клиента (TC1) можно просмотреть статистику конкретного интерфейса:

Switch(config)# show interface ethernet 1/0/10 detail

В выводе отображаются: количество принятых и переданных пакетов, объём переданных данных (в байтах), число unicast, multicast и broadcast пакетов, ошибки передачи (при наличии):

```
Statistics:
5 minute input rate 109789 bits/sec, 104 packets/sec
5 minute output rate 237 bits/sec, 0 packets/sec
The last 5 second input rate 0 bits/sec, 0 packets/sec
The last 5 second output rate 0 bits/sec, 0 packets/sec
Input packets statistics:
  54924 input packets, 7725227 bytes, 0 no buffer
  53772 unicast packets, 130 multicast packets, 1022 broadcast packets
  0 input errors, 0 CRC, 0 frame alignment, 0 overrun, 0 ignored,
  0 abort, 0 length error, 0 undersize 0 jabber, 0 fragments, 0 pause frame
```

Сбор статистики для multicast и broadcast-трафика выполняется аналогично.

Шаг 3. Ограничение скорости порта. В данном примере ограничим пропускную способность порта 1/0/1 до 50 Мбит/с:

Switch(config)# interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# bandwidth control 50000 both

После этого отправляем трафик со скоростью 100 Мбит/с и проверяем фактическую скорость передачи:

Switch(config-if-ethernet1/0/1)# show interface ethernet counter rate

Команда позволяет увидеть текущую интенсивность трафика (в пакетах и битах в секунду) и убедиться, что скорость ограничена заданным значением:

Interface		IN(pkts/s)	IN(bits/s)	OUT(pkts/s)	OUT(bits/s)
1/0/1	5m	271	2,828,200	102	939,021
	5s	1,850	945,664	4,162	49,851,955
1/0/2	5m	104	944,420	272	2,811,718
	5s	4,156	49,928,119	1,868	1,020,517

Шаг 4. Просмотр средней скорости трафика. Для анализа средней нагрузки используются интервалы 5 секунд и 5 минут:

Switch# show interface ethernet counter rate

Interface		IN(pkts/s)	IN(bits/s)	OUT(pkts/s)	OUT(bits/s)
1/0/1	5m	268	137,777	3,368	39,932,115
	5s	585	297,723	7,279	85,507,661
1/0/2	5m	3,370	39,935,695	271	156,426
	5s	7,286	85,521,110	597	367,596

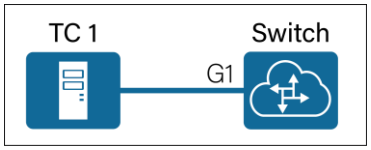
Где:

- **5s** — средняя скорость за последние 5 секунд;

- **5m** — средняя скорость за последние 5 минут;
- **IN** — входящий трафик;
- **OUT** — исходящий трафик.

Настройка и анализ статистики портов позволяют контролировать объём и тип передаваемого трафика, отслеживать текущую и среднюю нагрузку на интерфейсы, проверять корректность ограничения пропускной способности, выявлять возможные перегрузки или аномалии в работе сети. Регулярный мониторинг статистики помогает поддерживать стабильную и предсказуемую работу сетевой инфраструктуры.

3.24.3 Настройка описания портов



Назначение описания интерфейса позволяет упростить администрирование сети, облегчить идентификацию подключённых устройств и повысить наглядность конфигурации. Рекомендуется указывать в описании тип подключённого оборудования или назначение порта.

Этапы настройки:

Шаг 1. Настройка описания порта.

Пример настройки описания для порта Ethernet 1/0/1 (подключённого к TC1):

```
Switch(config)# interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# description abc
```

Для удаления описания и возврата к значению по умолчанию используется команда:

```
Switch(config-if-ethernet1/0/1)# no description
```

Шаг 2. Проверка результата настройки:

```
Switch(config)# show interface ethernet
```

В выводе команды отображается информация об интерфейсе, включая его текущее состояние и установленное описание:

Interface brief:
Ethernet1/0/1 is down, line protocol is down
Ethernet1/0/1 is layer 2 port, alias name is abcd, index 1
Hardware is Gigabit-TX, address is 08-c6-b3-c9—1a-ab

Настройка поддержки Jumbo-кадров

Jumbo-кадры позволяют передавать Ethernet-фреймы увеличенного размера, что может повысить эффективность передачи данных в сетях с высокой нагрузкой (например, в дата-центрах).

Этапы настройки:

Шаг 1. Настройка размера Jumbo-кадра. Установим максимальный размер кадра 3000 байт:

```
Switch(config)# mtu 3000
```

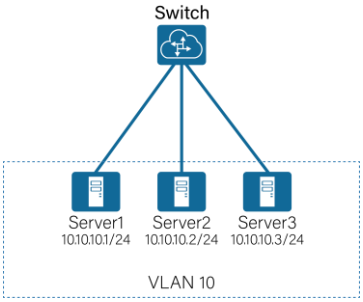
Шаг 2. Проверка результата:

- При отправке кадра размером 4000 байт он будет отброшен, так как превышает установленное значение MTU.
- При отправке кадра размером 2999 байт передача будет выполнена успешно.

Настройка описаний портов повышает удобство администрирования и упрощает сопровождение сети.
Настройка MTU и поддержка Jumbo-кадров позволяют оптимизировать передачу данных и адаптировать коммутатор к требованиям сетевой инфраструктуры.

3.25 Настройка изоляции портов

В пределах одного VLAN устройства по умолчанию могут свободно обмениваться трафиком. В некоторых сценариях требуется ограничить взаимодействие между определёнными узлами, сохранив при этом связь с другими устройствами (например, с сервером или шлюзом). В данном примере Server1, Server2 и Server3 находятся в VLAN 10. Требуется запретить обмен трафиком между Server1 и Server2, при этом сохранить их связь с Server3.



Этапы настройки:

Шаг 1. Создание VLAN и добавление интерфейсов:

```
Switch(config)# vlan 10
Switch(config-vlan10)# exit
Switch(config)# interface ethernet 1/0/1-3
Switch(config-if-port-range)# switchport access vlan 10
```

Шаг 2. Настройка изоляции портов. Создадим группу изоляции и добавим в неё порты 1 и 2:

```
Switch(config)# isolate-port group Netvice
Switch(config)#vlan 10
Switch(config-vlan10)# isolate-port group Netvice switchport interface ethernet 1/0/1-2
```

После применения конфигурации:

- Порт 1 и порт 2 изолированы друг от друга.
- Порт 3 остаётся доступным для обмена данными с обоими портами.

Шаг 3. Проверка результатов настройки.

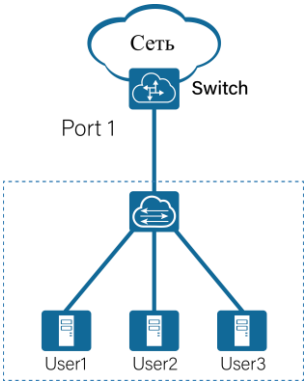
```
Switch(config)#show isolate-port group
```

Команда отображает созданные группы изоляции и назначенные им интерфейсы:

```
Isolate-port group Netvice
Vlan 10 :Isolate-port group Netvice
    The isolate-port Ethernet1/0/2
    The isolate-port Ethernet1/0/1
```

Изоляция портов позволяет ограничить взаимодействие между устройствами внутри одного VLAN без создания дополнительных VLAN.
Этот механизм повышает уровень безопасности сети и позволяет реализовать логическое разделение трафика при сохранении общей адресной структуры.

3.26 Настройка защиты портов (Port Security)



Для повышения уровня информационной безопасности на пользовательских интерфейсах коммутатора активируется функция защиты портов (Port Security). Она позволяет ограничить количество MAC-адресов, которые могут быть изучены на интерфейсе, и задать действия при попытке подключения неавторизованного устройства. Это предотвращает несанкционированный доступ к корпоративной сети через свободные порты.

Этапы настройки:

Шаг 1. Создание VLAN и настройка типа интерфейса:

```
Switch(config)# vlan 10
Switch(config-vlan)# exit
Switch(config)# interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# switchport mode trunk
Switch(config-if-ethernet1/0/1)# switchport trunk allowed vlan add 10
Switch(config-if-ethernet1/0/1)# exit
```

Шаг 2. Настройка функции Port Security.

Включение защиты порта и задание параметров безопасности:
```
Switch(config)# interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# switchport port-security
```

Настройка максимального количества MAC-адресов:
```
Switch(config-if-ethernet1/0/1)# switchport port-security maximum 4
```

Настройка действия при нарушении:
```
Switch(config-if- ethernet1/0/1)# switchport port-security violation protect
```

В данном примере предполагается подключение четырёх доверенных устройств, поэтому лимит установлен равным 4.

Шаг 3. Проверка результатов настройки:

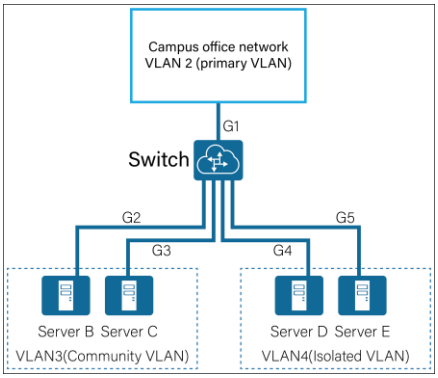
```
Switch(config-if-ethernet1/0/1)# show port-security interface ethernet 1/0/1
```

Команда отображает текущее состояние функции защиты, количество изученных MAC-адресов и информацию о нарушениях:

Violation mode : Protect
Maximum MAC Addresses : 4
Configured MAC Addresses : 0
Security Violation count : 0

Функция Port Security позволяет ограничить доступ к сети на уровне канального уровня, контролируя количество допустимых MAC-адресов и предотвращая подключение посторонних устройств. Это эффективный механизм базовой защиты пользовательских портов.

3.27 Настройка частных VLAN (Private VLAN, PVLAN)



В сетях дата-центров часто требуется разграничить взаимодействие серверов, сохранив при этом их доступ к общей инфраструктуре. Для решения этой задачи используется технология Private VLAN (PVLAN), которая позволяет логически разделить один VLAN на несколько типов:

- Primary VLAN — основной VLAN
- Community VLAN — групповой VLAN
- Isolated VLAN — изолированный VLAN

В рассматриваемом примере ServerB и ServerC должны взаимодействовать между собой, ServerD и ServerE должны быть изолированы, все серверы должны иметь доступ к внешней сети.

Этапы настройки:

Шаг 1. Создание и ассоциация VLAN:

```
Switch(config)# vlan 2
Switch(config-vlan)# private-vlan primary

Switch(config-vlan)# vlan 3
Switch(config-vlan)# private-vlan community

Switch(config-vlan)# vlan 4
Switch(config-vlan)# private-vlan isolated

Switch(config-vlan)# vlan 2
Switch(config-vlan)# private-vlan association 3-4
```

Шаг 2. Настройка портов

Настройка общего (promiscuous) порта для подключения к внешней сети:

```
Switch(config)# vlan 2
Switch(config-vlan2)# switchport interface ethernet 1/0/1
Set the port Ethernet1/0/1 access vlan 2 successfully
```

Настройка community-портов (ServerB и ServerC):

```
Switch(config)# vlan 3
Switch(config-vlan3)# switchport interface ethernet 1/0/2
Set the port Ethernet1/0/2 access vlan 3 successfully
Switch(config-vlan3)# switchport interface ethernet 1/0/3
Set the port Ethernet1/0/3 access vlan 3 successfully
```

Настройка isolated-портов (ServerD и ServerE):

```
Switch(config)# vlan 4
Switch(config-vlan4)# switchport interface ethernet 1/0/4
Set the port Ethernet1/0/4 access vlan 4 successfully
```

Switch(config-vlan4)# switchport interface ethernet 1/0/5
Set the port Ethernet1/0/5 access vlan 4 successfully

Дополнительная настройка MTU. Для поддержки технологии QinQ стандартного MTU 1500 байт может быть недостаточно. Рекомендуется увеличить значение:

Switch(config)# system mtu 1504

Для поддержки Jumbo-кадров:
Switch(config)# system mtu jumbo 9000

Шаг 3. Проверка результата настройки:

Switch(config)#show vlan private-vlan

Команда отображает типы VLAN, их ассоциации и назначенные интерфейсы:

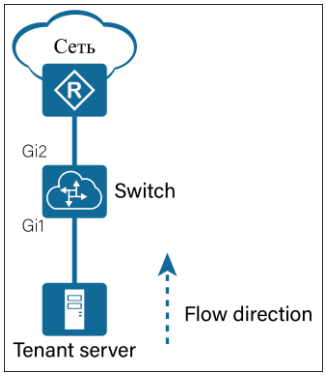
VLAN	Name	Type	Asso	VLAN	Ports	
2	VLAN0002	Primary	3	4	Ethernet1/0/1	
3	VLAN0003	Community	2		Ethernet1/0/2	Ethernet1/0/3
4	VLAN0004	Isolate	2		Ethernet1/0/4	Ethernet1/0/5

В результате все серверы имеют доступ к внешней сети через основной VLAN, ServerB и ServerC могут взаимодействовать друг с другом (community VLAN), ServerD и ServerE не могут взаимодействовать друг с другом (isolated VLAN). Взаимодействие между community и isolated VLAN отсутствует.

Технология Private VLAN позволяет гибко сегментировать трафик внутри одного VLAN, обеспечивая изоляцию устройств при сохранении доступа к общей инфраструктуре. Это особенно актуально для дата-центров и сетей с повышенными требованиями к безопасности и экономии VLAN-идентификаторов.

3.28 Настройка качества обслуживания и списков контроля доступа (QACL)

В данной схеме сервер арендатора передаёт трафик через коммутатор в сторону выходного маршрутизатора ЦОД. Требуется ограничить пропускную способность исходящего трафика сервера значением не более 100 Мбит/с. Для этого используется механизм QoS с привязкой к списку контроля доступа (ACL), который определяет источник трафика.



Этапы настройки:

Шаг 1. Создание стандартного ACL:

Switch(config)# access-list 1 permit host 192.85.1.11

Шаг 2. Создание класса трафика.

Создаём class-map и связываем его с ACL:
Switch(config)# class-map c1
Switch(config-classmap-c1)# match access-group 1
Switch(config-classmap-c1)# exit

Шаг 3: Создание политики ограничения скорости. Создаём policy-map и задаём ограничение CIR (Committed Information Rate):

Switch(config)# policy-map p1
Switch(config-policymap-p1)# class c1
Switch(config-policymap-p1-class-c1)# policy 100000
Switch(config-policymap-p1-class-c1)# exit
Switch(config-policymap-p1)# exit

Значение **100000** соответствует ограничению скорости до 100 Мбит/с.

Шаг 4. Применение политики к интерфейсу:

Switch(config)# interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# service-policy input p1
Switch(config-if-ethernet1/0/1)# exit

Шаг 5. Проверка результата настройки.

Просмотр ACL:
Switch(config)# show access-list

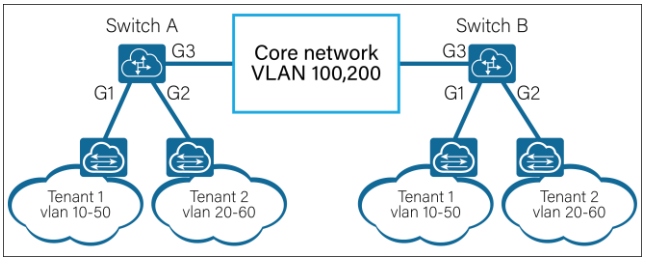
Пример вывода:
ip access-list standard 1
10 permit host 192.85.1.11

Просмотр политики QoS:
Switch(config)# show policy-map

Пример вывода:
Policy Map p1, used by 1 time(s)
Class Map name: c1
transmit
policy CIR: 100000 CBS: 0
conform-action: transmit
exceed-action: drop

Механизм QACL позволяет гибко управлять пропускной способностью трафика на основе заданных критериев (IP-адрес, подсеть и т.д.). В данном примере скорость передачи для сервера арендатора ограничена 100 Мбит/с, что обеспечивает контроль использования ресурсов сети.

3.29 Настройка Q-in-Q



Технология Q-in-Q (802.1ad) применяется для организации изолированной передачи трафика нескольких арендаторов через общую магистральную сеть. Каждый клиент может использовать собственные VLAN, при этом провайдер добавляет внешний тег (S-Tag), обеспечивая прозрачную транспортировку и изоляцию трафика. В рассматриваемом примере: Tenant 1 использует VLAN 100, Tenant 2 использует VLAN 200, магистральный канал передаёт трафик обоих арендаторов.

Этапы настройки:

Шаг 1. Создание VLAN:

SwitchA(config)# vlan 100,200

Шаг 2. Настройка клиентских портов и включение QinQ.

Порт 1 (Tenant 1):
SwitchA(config)# interface ethernet 1/0/1
SwitchA(config-if-ethernet1/0/1)# switchport access vlan 100
Set the port Ethernet1/0/1 access vlan 100 successfully
SwitchA(config-if-ethernet1/0/1)# dot1q-tunnel enable

Порт 2 (Tenant 2):
SwitchA(config-if-ethernet1/0/1)# interface ethernet 1/0/2
SwitchA(config-if-ethernet1/0/2)# switchport access vlan 200
Set the port Ethernet1/0/2 access vlan 200 successfully
SwitchA(config-if-ethernet1/0/2)# dot1q-tunnel enable

Шаг 3. Настройка магистрального порта:

SwitchA(config-if-ethernet1/0/2)# interface ethernet 1/0/3
SwitchA(config-if-ethernet1/0/3)# switchport mode hybrid
Set the port Ethernet1/0/3 mode Hybrid successfully
SwitchA(config-if-ethernet1/0/3)# switchport hybrid allowed vlan 100,200 tag
Set the Hybrid port Ethernet1/0/3 tag allowed vlan successfully

Инструкции по настройке протокола dot1q-tunnel (QinQ):
Switch# config
Switch(config)# interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# dot1q-tunnel ?
enable *Enable QinQ*
selective *Selective*
tpid *Tagged protocol id*

При необходимости можно изменить TPID:
Switch(config-if-ethernet1/0/1)# dot1q-tunnel tpid ?
0x8100 Установить значение TPID 0x8100 (Стандартное значение для vlan клиента)
0x9100 Установить значение TPID 0x9100 (Нестандартное значение для vlan провайдера qinq)
0x9200 Установить значение TPID 0x9200 (Нестандартное значение для vlan провайдера qinq)
<1-65535> Установить значение TPID вручную -65535 (Нестандартное значение для старых устройств qinq)

Switch(config-if)# dot1q-tunnel tpid 0x9100

Шаг 4. Проверка результатов настройки:

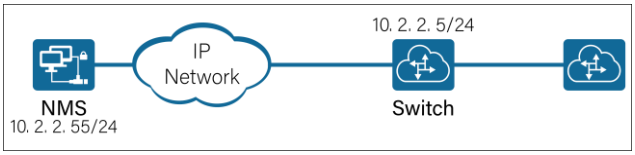
Switch(config)# show dot1q-tunnel

В результате Tenant 1 успешно взаимодействует внутри своей сети между удалёнными локациями, Tenant 2 успешно взаимодействует внутри своей сети, между Tenant 1 и Tenant 2 связь отсутствует:

```
Interface Ethernet1/0/1:
    dot1q-tunnel is enable
Interface Ethernet1/0/2:
dot1q-tunnel is enable
```

Q-in-Q обеспечивает прозрачную передачу VLAN арендаторов через общую транспортную сеть с сохранением полной изоляции клиентов. Это решение широко применяется в сетях провайдеров и дата-центрах.

3.30 Настройка дистанционного мониторинга (RMON)



RMON (Remote Monitoring) позволяет выполнять расширенный мониторинг состояния сети, сбор статистики трафика и автоматическую генерацию событий при превышении заданных порогов. В данном примере требуется вести историю статистики, регистрировать события, отслеживать широковещательный трафик, отправлять SNMP Trap-сообщения на NMS.

Этапы настройки:

Шаг 1. Настройка IP-интерфейса:

```
Switch(config)# interface vlan 1
Switch(config-if-vlan1)# ip address 10.2.2.5 255.255.255.0
```

Шаг 2. Настройка SNMP и Trap.

Включение SNMP:
```
Switch(config)# snmp-server enable
```

Настройка имен для чтения и записи:
```
Switch(config)# snmp-server community rw 0 public
```

Включение функции ловушек SNMP traps:
```
Switch(config)# snmp-server enable traps
```

Настройка отправки SNMP traps на NMS-сервер:
```
Switch(config)# snmp-server trap-source 10.2.2.5
```

Выключение функции ***securityip***:
```
Switch(config)# snmp-server securityip disable
```

Шаг 3. Настройка истории. Сбор статистики каждые 30 секунд, хранение 10 записей:

```
Switch(config)# rmon history 1 interface ethernet 1/0/1 buckets 10 interval 30 owner test
```

Шаг 4. Настройка событий:

```
Switch(config)# rmon event 1 log description test owner test
Switch(config)# rmon event 2 trap public description alarm owner test
```

Шаг 5. Настройка сигналов тревоги. Пример отслеживания broadcast-трафика:

```
Switch(config)# rmon alarm 1 interface ethernet 1/0/1 broadcast-pkts 30 absolute rising 500 2
falling 100 1 startup rising-falling owner test
```

Шаг 6. Проверка результатов настройки.

Просмотр сигналов тревоги:
Switch(config)# show rmon alarm

Пример вывода показан на рисунке справа:

```
Rmon Alarm Index                1
Rmon Alarm Sample Interval      30
Rmon Alarm Sample Interface  : Ethernet1/0/11
Rmon Alarm Sample Variable   : Broadcast-Pkts
Rmon Alarm Sample Type       : absolute
Rmon Alarm Type              : Rising or Falling
Rmon Alarm Rising Threshold     500
Rmon Alarm Rising Event         2
Rmon Alarm Falling Threshold : 100
Rmon Alarm Falling Event        1
Rmon Alarm Owner             : test
```

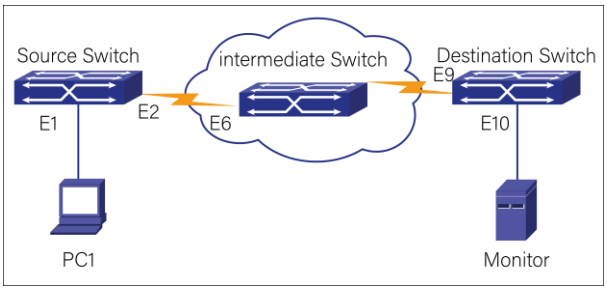
Просмотр журналов:
Switch(config)# show rmon event 2 log

Пример вывода:

```
Switch(config)#show rmon event 2 log
Index                1
Event Index          2
log Time             : (250400) 0 days, 00:41:44
log Description      :   : alarm rising event : value = 16939, RisingThreshold = 500

Index                2
Event Index          2
log Time             : (253400) 0 days, 00:42:14
log Description      :   : alarm rising event : value = 2064, RisingThreshold = 500
```

RMON обеспечивает детальный контроль состояния сети, позволяет автоматически выявлять перегрузки и аномалии трафика, а также оперативно уведомлять систему управления сетью о возникающих событиях. Это важный инструмент для поддержания стабильной и безопасной работы инфраструктуры.

3.31 Настройка отдельного VLAN для анализа трафика через всю сеть (RSPAN)



Технология RSPAN (Remote Switched Port Analyzer) предназначена для удалённого зеркалирования трафика между коммутаторами через выделенный VLAN. В отличие от обычного локального SPAN, при котором анализ возможен только на одном устройстве, RSPAN позволяет передавать зеркалируемый трафик через магистральную сеть на удалённый коммутатор, где подключено устройство анализа (например, сервер мониторинга или анализатор трафика).
До внедрения RSPAN сетевым администраторам приходилось физически подключаться к каждому коммутатору для диагностики, что усложняло обслуживание и увеличивало время устранения неисправностей. Использование RSPAN позволяет централизованно контролировать состояние сети из центра управления, при условии, что все задействованные коммутаторы поддерживают данную функцию.
Существует два варианта реализации: без отражающего порта (reflector-port) и с использованием отражающего порта.
Первый вариант предполагает жёсткую привязку порта для передачи зеркалируемого трафика к следующему коммутатору. Второй вариант более гибкий и позволяет использовать отражающий порт для передачи инкапсулированного трафика в RSPAN VLAN.

Настройка RSPAN без отражающего порта

Этапы настройки:

Шаг 1. Настройка исходного коммутатора.

Создание VLAN и назначение исходному коммутатору роли RSPAN:
Switch(config)# vlan 5
Switch(Config-Vlan5)#remote-span

Switch(Config-Vlan5)#exit

Настройка магистрального порта для передачи RSPAN VLAN:
Switch(config)# interface ethernet 1/2
Switch(Config-If-Ethernet1/2)# switchport mode trunk
Switch(Config-If-Ethernet1/2)# exit

Шаг 2. Настройка сессии мониторинга.

Отслеживание входящего трафика на интерфейсе 1/1:
Switch(config)# monitor session 1 source interface ethernet1/1 rx

Передача зеркалируемого трафика в сторону магистрали:
Switch(config)# monitor session 1 destination interface ethernet1/2
Switch(config)# monitor session 1 remote vlan 5

Шаг 3. Настройка промежуточного коммутатора.

Создание VLAN 5 и назначение роли remote-span:
Switch(config)# vlan 5
Switch(Config-Vlan5)# remote-span
Switch(Config-Vlan5)# exit

Настройка транковых портов:
Switch(config)# interface ethernet 1/6-7
Switch(Config-If-Port-Range)# switchport mode trunk

Шаг 4. Настройка конечного коммутатора.

Создание RSPAN VLAN:
Switch(config)# vlan 5
Switch(Config-Vlan5)# remote-span

Настройка магистрального порта:
Switch(config)# interface ethernet 1/9
Switch(Config-If-Ethernet1/9)# switchport mode trunk

Настройка порта для подключения анализатора:
Switch(config)# interface ethernet 1/10
Switch(Config-If-Ethernet1/10)# switchport access vlan 5

В результате зеркалируемый трафик будет доставляться на порт 1/10, к которому подключено устройство анализа.

Настройка RSPAN с использованием отражающего порта

Этапы настройки:

Шаг 1. Настройка исходного коммутатора.

Создание VLAN 5 с ролью remote-span:
Switch(config)# vlan 5
Switch(Config-Vlan5)# remote-span

Настройка отражающего порта:
Switch(config)# interface ethernet 1/3
Switch(Config-If-Ethernet1/3)# switchport mode trunk

Шаг 2. Создание сессии мониторинга:

Switch(config)# monitor session 1 source interface ethernet1/1 rx
Switch(config)# monitor session 1 reflector-port ethernet1/3
Switch(config)# monitor session 1 remotevlan 5

Шаг 3. Промежуточный коммутатор настраивается аналогично первому варианту.

Шаг 4. Настройка конечного коммутатора:

Switch(config)# interface Ethernet1/0/9
Switch(Config-If-Ethernet1/0/9)# switchport mode trunk

Switch(config)# interface Ethernet1/0/10
Switch(Config-If-Ethernet1/0/10)# switchport access vlan 5

Возможные проблемы и способы их устранения

1. **Порт назначения входит в агрегированный канал (LACP/LAG).** Необходимо вывести порт из группы агрегации либо изменить конфигурацию группы.
2. **Недостаточная пропускная способность порта назначения.** Если суммарный трафик источников превышает возможности порта назначения, возможны потери пакетов. Рекомендуется:
   - уменьшить количество зеркалируемых портов;
   - зеркалировать трафик только в одном направлении (rx или tx);
   - использовать порт с большей пропускной способностью.
3. **RSPAN VLAN совпадает с Native VLAN.** Это может привести к некорректной передаче трафика. Следует изменить Native VLAN на транковых портах.
4. **Ошибки из-за увеличенного размера кадра.** При использовании RSPAN к кадру добавляется дополнительный VLAN-тег, что увеличивает его размер. В этом случае необходимо увеличить значение MTU:

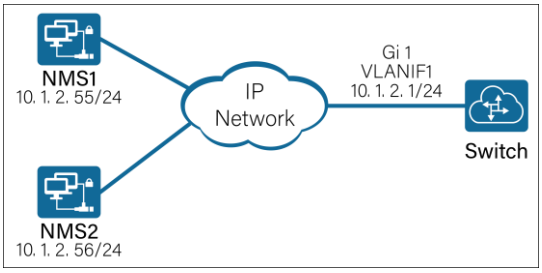
Switch(config)# system mtu 1504
Switch(config)# system mtu jumbo 9000

В данном разделе была выполнена настройка удалённого зеркалирования трафика с использованием RSPAN. Создан специализированный VLAN для передачи зеркалируемых данных, настроены транковые соединения между коммутаторами и определена сессия мониторинга. Рассмотрены два варианта конфигурации — с фиксированным портом назначения и с использованием отражающего порта. В результате обеспечена возможность централизованного анализа сетевого трафика через всю сеть без необходимости физического подключения к каждому коммутатору, что значительно упрощает администрирование и диагностику сети.

3.32 Настройка протокола простого сетевого управления (SNMP)

В данном примере в существующей сети системы управления NMS1 и NMS2 осуществляют централизованный мониторинг сетевых устройств по протоколу SNMPv1. В связи с расширением инфраструктуры был добавлен новый коммутатор, который также необходимо интегрировать в систему мониторинга. Настройка SNMP позволяет централизованно контролировать

состояние устройства, получать статистику интерфейсов и системные параметры, оперативно получать уведомления о сбоях (Trap-сообщения), ускорить диагностику и устранение неисправностей.



Этапы настройки:

Шаг 1. Настройка IP-интерфейса управления. Назначьте IP-адрес интерфейсу VLAN, через который будет осуществляться взаимодействие с системой управления:

```
Switch(config)# interface vlan 1
Switch(config-if-vlan1)# ip address 10.1.2.1 255.255.255.0
Switch(config-if-vlan1)# exit
```

Шаг 2. Настройка прав доступа и включение SNMP.

Включите службу SNMP и задайте имя сообщества с правами чтения и записи:

```
Switch(config)# snmp-server enable
Switch(config)# snmp-server community rw 0 1234
```

Отключите функцию securityip (если используется ограничение по IP-адресам):

```
Switch(config)# snmp-server securityip disable
```

Шаг 3. Настройка отправки Trap-сообщений на NMS. Укажите IP-адрес станции управления, которая будет получать уведомления:

```
Switch(config)# snmp-server host 10.1.2.56 traps
```

Шаг 4. Настройка станции управления. На стороне NMS необходимо:

- добавить новый коммутатор по IP-адресу 10.1.2.1;
- указать версию протокола SNMPv1;
- задать имя сообщества (в данном примере — 1234).

Шаг 5. Проверка результата настройки. Проверьте состояние SNMP-службы:

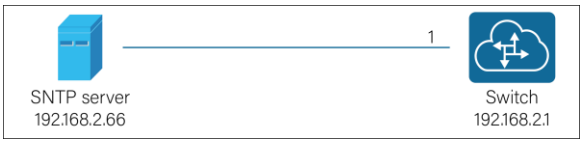
```
Switch(config)# show snmp status
```

В выводе должно отображаться состояние SNMP — Enabled, информация о настроенных сообществах, адрес получателя Trap-сообщений.

```
System Name : Switch
System Contact :
System Location : Default
Trap disable
RMON enable
Community Information:
        Community string: 1234
        Community access: Read-Write
        Community read view name: v1defaultviewname
        Community write view name: v1defaultviewname
V1/V2c Trap Host Information:
        Trap-rec-address: 10.1.2.56
        Host Version:V1
        Community string: traps
V3 Trap Host Information:
Security IP is Disabled.
```

После выполнения настройки новый коммутатор интегрирован в существующую систему мониторинга. Станция управления получает доступ к статистике устройства и может принимать уведомления о событиях, что обеспечивает централизованный контроль и оперативное реагирование на возможные неисправности.

3.33 Настройка упрощённого протокола синхронизации времени (SNTP)



Для корректной работы журналов событий, механизмов аутентификации и мониторинга коммутатор должен иметь точное системное время. В данной конфигурации синхронизация выполняется с использованием протокола SNTP, при этом сервер времени доступен в сети.

Этапы настройки:

Шаг 1. Указание адреса SNTP-сервера и исходящего интерфейса. Необходимо задать IP-адрес SNTP-сервера и указать интерфейс, через который будет выполняться синхронизация:

```
Switch(config)# sntp server 192.168.2.66 source vlan 1
```

Шаг 2. Настройка VLAN-интерфейса. Назначьте IP-адрес интерфейсу VLAN, который используется для связи с сервером времени:

```
Switch(config)# interface vlan 1
Switch(config-if-vlan1)# ip address 192.168.2.1 255.255.255.0
Switch(config-if-vlan1)# exit
```

Шаг 3. Настройка часового пояса. Установите корректный часовой пояс:

```
Switch(config)# clock timezone Krasnoyarsl add 7
```

Шаг 4. Проверка результатов настройки. Проверьте состояние SNTP и факт получения времени от сервера:

```
Switch(config)# show sntp
```

Пример вывода:

```
server address      version      last receive
192.168.2.66        1            20
```

Параметр **last receive** показывает время (в секундах) с момента последнего успешного получения ответа от SNTP-сервера.

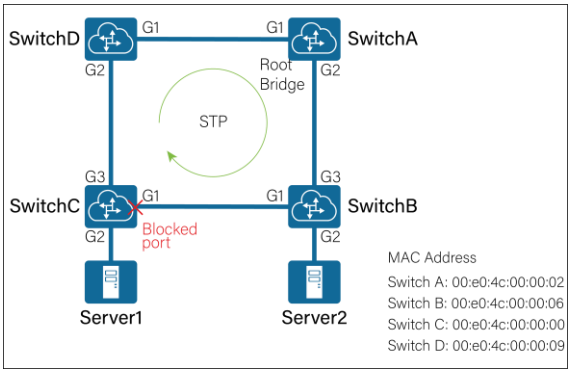
После выполнения настройки коммутатор автоматически синхронизирует системное время с указанным SNTP-сервером. Это обеспечивает корректную работу журналов событий, механизмов безопасности и систем мониторинга, а также упрощает анализ сетевых инцидентов.

3.34 Настройка алгоритма обнаружения петель (STP)

3.34.1 Настройка стандартного STP

В сложных сетях для повышения отказоустойчивости часто используются несколько физических каналов связи между коммутаторами. Один из каналов работает как основной, а остальные используются как резервные. Такая схема приводит к образованию кольцевой топологии.

Наличие петель в сети второго уровня может привести к широковещательным штормам, многократной передаче одних и тех же кадров и переполнению таблиц MAC-адресов. Для предотвращения подобных ситуаций применяется протокол STP (Spanning Tree Protocol).



Протокол STP автоматически обнаруживает избыточные соединения между коммутаторами и переводит часть портов в состояние блокировки. В результате физическая кольцевая топология преобразуется в логическую древовидную структуру без петель.
На приведенной схеме коммутаторы A, B, C и D образуют сеть с резервными каналами. После включения STP устройства обмениваются BPDU-сообщениями и определяют роли портов, один из которых блокируется для устранения петли.

Этапы настройки:

Шаг 1. Включение STP на коммутаторах и определение режима его работы:

```
SwitchA(config)# spanning-tree
SwitchA(config)# spanning-tree mode stp
```

Аналогичная настройка выполняется на остальных коммутаторах сети.

Шаг 2. Настройка корневого коммутатора. Чтобы коммутатор **SwitchA** был выбран корневым мостом (Root Bridge), необходимо установить более низкий приоритет:

```
SwitchA(config)# spanning-tree priority 4096
```

Коммутатор с наименьшим значением приоритета автоматически выбирается в качестве корневого.

Шаг 3. Настройка стоимости портов. Для управления выбором оптимального пути можно изменить стоимость интерфейсов. Пример настройки для порта Ethernet 1/0/1 на коммутаторе SwitchA:

```
SwitchA(config)# interface ethernet 1/0/1
SwitchA(config-if- ethernet1/0/1)# spanning-tree cost 20000
```

Аналогично настраиваются:

- порты **1 и 2** на коммутаторах **A** и **D**
- порты **1 и 3** на коммутаторе **B**
- порт **3** на коммутаторе **D**

Шаг 4. Настройка стоимости порта на коммутаторе C. Для корректного выбора корневого порта увеличивается стоимость интерфейса:

```
SwitchC(config)# interface ethernet 1/0/1
SwitchC(config-if- ethernet1/0/1)# spanning-tree cost 30000
```

В результате порт **3** станет **Root Port,** порт **1** будет переведен в состояние **Blocking.**

Шаг 5. Отключение STP на пользовательских портах. Порты, подключенные к конечным устройствам (например, серверам), можно исключить из участия в STP:

SwitchB(config)# interface ethernet 1/0/2
SwitchB(config-if- ethernet1/0/2)# no spanning-tree

SwitchC(config)# interface ethernet 1/0/2
SwitchC(config-if- ethernet1/0/2)# no spanning-tree

Шаг 6: Проверка результатов настройки:

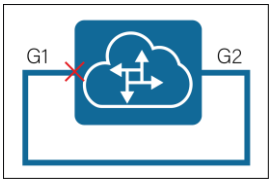
SwitchA(config)# show spanning-tree

```
********** Process 0 **********
        -- STP Bridge Config Info --

Standard        :   IEEE 802.1d
Bridge MAC      :   00:e0:4c:00:00:02
Bridge Times :   Max Age 20, Hello Time 2, Forward Delay 15
Force Version:   1

############################################################
Self Bridge Id    : 4096.00:e0:4c:00:00:02
Root Id           : this switch
Ext.RootPathCost : 0
Root Port ID      0

  PortName        ID        ExtRPC   State Role     DsgBridge          DsgPort
------------------------  ------------------------
Ethernet1/0/1   128.001     20000    FWD   DSGN   4096.00e04c000002 128.001
Ethernet1/0/2   128.002     20000    FWD   DSGN   4096.00e04c000002 128.001
```

Команда отображает корневой коммутатор сети, роли портов (Root, Designated, Blocking), стоимость путей до корневого моста:

После выполнения указанных настроек протокол STP автоматически обнаруживает избыточные соединения между коммутаторами и блокирует один из портов, предотвращая образование петель в сети. Это позволяет сформировать логическую древовидную топологию, обеспечивающую стабильную передачу данных. Использование STP повышает надежность сети и предотвращает возникновение широковещательных штормов.

3.34.2 Настройка защиты от внутренней петли



Иногда петля может возникнуть внутри одного коммутатора, например при случайном соединении двух его портов между собой. Такая ситуация называется внутренней петлей (self-loop).
Если на коммутаторе включен STP, протокол обнаружит петлю и заблокирует один из портов, разрывая цикл.

Этапы настройки:

Шаг 1. Включение STP:

SwitchA(config)# spanning-tree
SwitchA(config)# spanning-tree mode stp

Шаг 2. Проверка состояния STP:

SwitchA(config)# show spanning-tree

Шаг 3. Изменение приоритета порта. Для управления выбором активного порта можно изменить его приоритет:

SwitchA(config)# interface ethernet 1/0/1
SwitchA(config-if-ethernet1/0/1)# spanning-tree port-priority 240

Шаг 4. Проверка результата настройки:

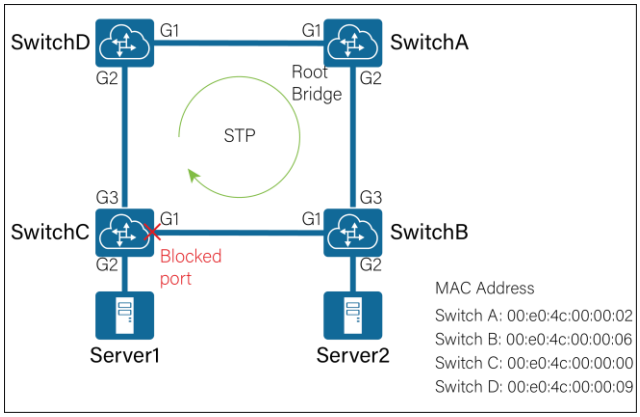
SwitchA(config)# show spanning-tree

После настройки один из портов будет переведен в состояние **Blocking** и станет резервным.

После настройки протокол STP способен обнаруживать внутренние петли, возникающие при ошибочном соединении портов одного коммутатора. Один из портов автоматически переводится в состояние блокировки, что предотвращает циркуляцию кадров в сети. Это обеспечивает корректную работу коммутатора и защищает сеть от перегрузки.

3.34.3 Настройка RTSP

RSTP (Rapid Spanning Tree Protocol) является усовершенствованной версией STP. Основное отличие заключается в более быстрой сходимости сети после изменения топологии. RSTP использует улучшенный алгоритм обработки портов и позволяет значительно сократить время восстановления сети.



Этапы настройки:

Шаг 1. Включение RSTP:

```
SwitchA(config)# spanning-tree
SwitchA(config)# spanning-tree mode rstp
```

Настройка выполняется на всех коммутаторах сети.

Шаг 2. Настройка корневого моста:

```
SwitchA(config)# spanning-tree priority 4096
```

Коммутатор с наименьшим значением приоритета автоматически выбирается в качестве корневого.

Шаг 3. Настройка стоимости интерфейса:

```
SwitchC(config)# interface ethernet 1
SwitchC(config-if-ethernet1/0/1)# spanning-tree cost 30000
```

Шаг 4. Настройка стоимости остальных портов:

```
SwitchA(config)# interface ethernet 1/0/1
SwitchA(config-if- ethernet1/0/1)# spanning-tree cost 20000
```

Шаг 5. Включение функции **PortFast**. Функция **PortFast** позволяет порту сразу перейти в состояние Forwarding:

```
SwitchB(config-if- ethernet1/0/2)# spanning-tree portfast
```

Шаг 6. Настройка механизмов защиты.

Root Guard позволяет корневому коммутатору не потерять свою роль при появлении в сети нового коммутатора:

```
SwitchA(config)# interface ethernet1/0/1-2
```

SwitchA(config-if-port-range)# spanning-tree rootguard

Loop Guard для защиты от петель для корневого и альтернативного портов коммутатора C:
SwitchC(config)# interface range ethernet1/0/1,3
SwitchC(config-if-port-range)# spanning-tree loopguard

Шаг 7. Настройка BPDU-защиты:

SwitchB(config)# interface ethernet1/0/2
SwitchB(config-if- ethernet1/0/2)# spanning-tree portfast bpduguard recovery 60

SwitchC(config)# interface ethernet1/0/2
SwitchC(config-if- ethernet1/0/2)# spanning-tree portfast bpdufilter

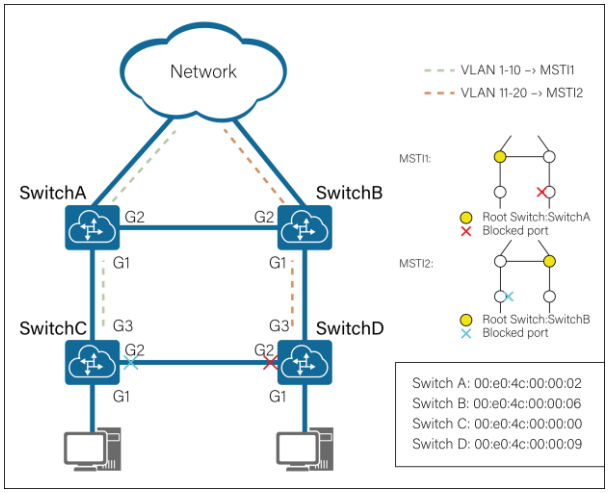
Шаг 8. Проверка результатов настройки:

SwitchA(config)# show spanning-tree

Команда позволяет проверить роли портов, стоимость путей и выбранный корневой коммутатор.

После выполнения настройки протокол RSTP обеспечивает более быстрое восстановление сети при изменении топологии по сравнению со стандартным STP. Дополнительные механизмы защиты, такие как PortFast, Root Guard, Loop Guard и BPDU Guard, повышают стабильность и безопасность сети. Это позволяет минимизировать время простоя и повысить надежность работы сетевой инфраструктуры.

3.34.4 Настройка MSTP



MSTP (Multiple Spanning Tree Protocol) позволяет создавать несколько экземпляров STP и распределять между ними различные VLAN. Это позволяет эффективно балансировать трафик в сети. В рассматриваемом примере: VLAN 1–10 используются в MSTI 1 и VLAN 11–20 используются в MSTI 2.

Этапы настройки:

Шаг 1. Создание VLAN и настройка trunk-портов:

SwitchA(config)# vlan 1-20
SwitchA(config)# interface ethernet 1/0/1-2
SwitchA(config-if-port-range)# switchport mode trunk
SwitchA(config-if-port-range)# switchport trunk allowed vlan add 1-20

Настройка коммутаторов **C** и **D** выполняется аналогично:
SwitchC(config)# interface ethernet 1/0/2-3
SwitchC(config-if-port-range)# switchport mode trunk
SwitchC(config-if-port-range)# switchport trunk allowed vlan add 1-20

Шаг 2. Включение MSTP:

SwitchA(config)# spanning-tree
SwitchA(config)# spanning-tree mode mstp

Настройка выполняется на всех коммутаторах сети.

Шаг 3. Настройка MST-региона:

SwitchA(config)# spanning-tree mst configuration
SwitchA(config-mstp-region)# name RG1
SwitchA(config-mstp-region)# instance 1 vlan 2-10
SwitchA(config-mstp-region)# instance 2 vlan 11-20

Настройка выполняется на всех коммутаторах сети.

Проверка результата настройки:

SwitchD(config-mstp-region)# show spanning-tree mst config Name RG1

Revision0
Instance Vlans Mapped
00 21-4094
01 1-10
02 11-20

Шаг 4. Настройка корневых коммутаторов.

Настройка максимального приоритета равным 4096 на общем корневом коммутаторе A для MST0:
SwitchA(config)# spanning-tree mst 0 priority 4096

Настройка приоритета моста в **instance 1** коммутаторе A равным 4096, а приоритет моста в **instance 2** коммутатора B равным 4096. Таким образом, коммутатор A станет корнем региона для MSTI1, а коммутатор B – корнем региона для MSTI2:

SwitchA(config)# spanning-tree mst 1 priority 4096
SwitchB(config)# spanning-tree mst 2 priority 4096

Шаг 5. Настройка стоимости портов:

SwitchC(config)# interface ethernet1/0/2
SwitchC(config-if-ethernet1/0/2)# spanning-tree mst 2 cost 30000

SwitchD(config)# interface ethernet1/0/2
SwitchD(config-if-ethernet1/0/2)# spanning-tree mst 1 cost 30000

Шаг 6. Настройка edge-порта:

SwitchC(config)# interface ethernet1/0/1
SwitchC(config-if-ethernet1/0/1)# spanning-tree portfast

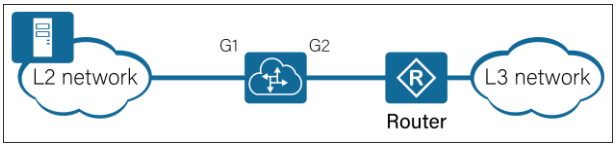
Шаг 7. Проверка результата настройки:

SwitchA(config)# show spanning-tree

В результате все коммутаторы объединяются в регион RG1, MSTI 1 обслуживает VLAN 1–10, MSTI 2 обслуживает VLAN 11–20, MSTI 0 (CIST) управляет общей топологией сети. Это позволяет обеспечить балансировку нагрузки и эффективное использование резервных каналов связи.

После выполнения настройки MSTP сеть разделяется на несколько экземпляров spanning-tree, каждый из которых обслуживает определенные группы VLAN. Это позволяет эффективно распределять трафик между различными каналами связи и использовать резервные линии для балансировки нагрузки. В результате повышается производительность и отказоустойчивость сети.

3.35 Настройка ограничения пакетов в сети (Storm-Control)



Как показано на рисунке справа, коммутатор **A** используется как точка подключения сети второго уровня к маршрутизатору третьего уровня. В таких сетях существует риск возникновения широковещательных штормов или избыточной передачи многоадресных и неизвестных одноадресных кадров. Подобные ситуации могут привести к перегрузке сети и снижению производительности устройств.
Для предотвращения таких проблем на коммутаторе применяется функция **Storm Control**, которая позволяет ограничить скорость передачи определенных типов трафика. Ограничения могут быть установлены для широковещательных (broadcast), многоадресных (multicast) и неизвестных одноадресных (unknown unicast) пакетов.

Этапы настройки:

Шаг 1. Выбор единицы измерения для Storm Control. В качестве единицы измерения для ограничения трафика используется килобит в секунду (kbps):

```
Switch(config)# storm-control kbps
```

Шаг 2. Настройка ограничений для различных типов трафика.

Настройка ограничения скорости для широковещательного, многоадресного и неизвестного одноадресного трафика на интерфейсе Ethernet 1/0/1:

```
Switch(config)# interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# storm-control broadcast 64
Switch(config-if-ethernet1/0/1)# storm-control multicast 128
Switch(config-if-ethernet1/0/1)# storm-control unicast 192
```

В данном примере устанавливаются следующие ограничения: широковещательный трафик — **64 кбит/с,** многоадресный трафик — **128 кбит/с,** неизвестный одноадресный трафик — **192 кбит/с.**

Шаг 3. Проверка результатов настройки.

Для проверки работы функции Storm Control можно сгенерировать соответствующие типы трафика и проверить скорость их передачи через коммутатор.

Пример проверки:

- при отправке широковещательного трафика со скоростью **100 Мбит/с** через порт 1 скорость его приема на других портах будет ограничена значением **64 кбит/с**;

- при отправке неизвестного многоадресного трафика со скоростью **100 Мбит/с** скорость приема составит **128 кбит/с**;
- при отправке неизвестного одноадресного трафика со скоростью **100 Мбит/с** скорость приема будет ограничена значением **192 кбит/с**.

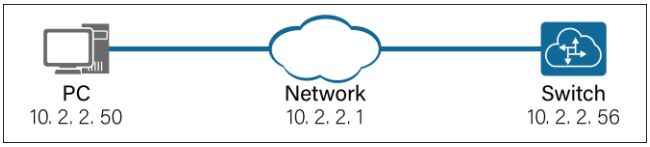
После выполнения настройки функция Storm Control ограничивает скорость передачи широковещательного, многоадресного и неизвестного одноадресного трафика на заданных портах. Это позволяет предотвратить возникновение широковещательных штормов и снизить вероятность перегрузки сети. В результате повышается стабильность и надежность работы сетевой инфраструктуры.

3.36 Отладка системы коммутатора

Для диагностики состояния сети и выявления возможных проблем на коммутаторах используются различные инструменты отладки. Наиболее распространёнными являются проверка доступности узлов сети, анализ маршрута прохождения пакетов и ведение системных журналов. Эти функции позволяют администраторам быстро обнаруживать неисправности, анализировать работу сети и фиксировать события, происходящие на оборудовании.

3.36.1 Проверка доступности узла (Ping/Traceroute)

Как показано на рисунке справа, необходимо проверить доступность удалённого хоста и определить путь прохождения пакетов до него. Для этого используются команды **ping** и **traceroute**.



Этапы настройки:

Шаг 1. Настройка IP-адреса интерфейса управления:

```
Switch(config)# interface vlan 1
Switch(config-if-vlan1)# ip address 10.2.2.56 255.255.255.0
```

Шаг 2. Проверка доступности и маршрута до узла. После настройки IP-адреса можно проверить доступность удалённого узла и определить маршрут прохождения пакетов:

```
Switch# ping 10.2.2.50
Switch# traceroute 10.2.2.50
```

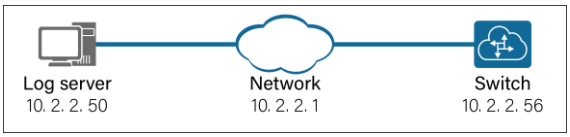
Команда **ping** используется для проверки доступности удалённого узла, а команда **traceroute** позволяет определить последовательность сетевых устройств, через которые проходит пакет до точки назначения.

Результат работы команд показан на рисунке ниже:

```
Type ^c to abort.
Sending 5 56-byte ICMP Echos to 10.2.2.50, timeout is 2 seconds.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

Type ^c to abort.
Traceroute to host 10.2.2.50, maxhops is 30, timeout is 2000ms.
 1     0ms       10.2.2.50
Traceroute completed.
```

После выполнения проверки администратор может убедиться в доступности удалённого устройства и определить путь прохождения пакетов в сети. Использование команд **ping** и **traceroute** позволяет быстро выявлять проблемы связи и диагностировать возможные сбои в сетевой инфраструктуре.

3.36.2 Настройка журналов



Система журналирования позволяет фиксировать события, происходящие на сетевом оборудовании, и передавать их на удалённый сервер для дальнейшего анализа. Это упрощает диагностику неисправностей и обеспечивает централизованное хранение информации о работе устройств. В данном примере управляющий интерфейс коммутатора имеет IPv4-адрес **10.2.2.56**, а удалённый сервер журналов — **10.2.2.50**. Необходимо настроить отправку логов на сервер с использованием хранилища **local1**.

Этапы настройки:

Шаг 1. Настройка IP-адреса интерфейса управления:

```
Switch(config)# interface vlan 1
Switch(config-if-vlan1)# ip address 10.2.2.56 255.255.255.0
```

Шаг 2. Настройка отправки журналов на удалённый сервер. Укажите IP-адрес сервера журналов и уровень логирования:

```
Switch(config)# logging 10.2.2.50 facility local1 level debugging
```

Шаг 3. Включение аудита выполненных команд. Для фиксации всех выполняемых команд включите журналирование действий администратора:

```
Switch(config)#logging executed-commands enable
```

Шаг 4. Проверка результатов настройки:

```
Switch(config)# show logging executed-commands state
```

Пример вывода:
Logging executed command state is enable

После выполнения настройки коммутатор будет отправлять системные журналы на удалённый сервер логирования. Это позволяет централизованно хранить информацию о событиях

сети и действиях администратора, что значительно упрощает анализ ошибок и диагностику неисправностей.

3.37 Настройка удаленного доступа Telnet/SSH

Удалённое управление сетевыми устройствами позволяет администраторам настраивать и контролировать работу оборудования без физического доступа к нему. На коммутаторах для этой цели могут использоваться протоколы Telnet и SSH.
Telnet обеспечивает удалённый доступ к командной строке устройства, однако передаёт данные в незашифрованном виде. Протокол SSH (Secure Shell) является более безопасной альтернативой, поскольку использует шифрование при передаче данных.

Настройка Telnet

Как показано на рисунке справа, два коммутатора соединены по сети. Администратору необходимо выполнить удалённое подключение к коммутатору **B** с коммутатора **A**.

Этапы настройки:

Шаг 1. Включение функции Telnet на коммутаторе B:

SwitchB(config)# enable service telnet-server

Шаг 2. Настройка IP-адресов интерфейсов управления. Для обеспечения связи между устройствами необходимо настроить IP-адреса на интерфейсах управления VLAN.

Настройка на коммутаторе **A**:
SwitchA(config)# interface vlan 1
SwitchA(config-if-vlan1)# ip address 10.2.2.56 255.255.255.0
SwitchA(config-if-vlan1)# exit

Настройка на коммутаторе **B**:
SwitchB(config)# interface vlan 1
SwitchB(config-if-vlan1)# ip address 10.2.2.57 255.255.255.0
SwitchB(config-if-vlan1)# exit

Шаг 3. Проверка результатов настройки.

Попробуйте установить Telnet-соединение с коммутатора **A** к коммутатору **B**:
SwitchA# telnet 10.2.2.57 23

Если настройка выполнена корректно, будет установлено удалённое соединение с командной строкой коммутатора **B**:

```
Connecting Host 10.2.2.57 Port 23...
Service port is 23
Connected to 10.2.2.57
login: admin
password:*****
router>
```

После выполнения настройки администратор может подключаться к коммутатору **B** удалённо с помощью протокола Telnet. Это позволяет выполнять конфигурацию и диагностику оборудования через сеть без необходимости физического доступа к устройству.

Настройка подключения SSH

В отличие от Telnet, протокол **SSH** обеспечивает защищённое удалённое подключение, используя шифрование передаваемых данных. В данном примере необходимо обеспечить доступ к коммутатору с компьютера **PC2** через SSH.

Этапы настройки:

Шаг 1. Включение функции SSH. Активируйте SSH-сервер на коммутаторе и задайте время ожидания сеанса:

```
Switch(config)# ssh-server enable
Please waiting a few minutes for the host rsa key-pair to be created
ssh is enabled successfully
```

После включения SSH задайте время ожидания сеанса (120 минут):

```
Switch(config)# ssh-server timeout 120
```

Шаг 2. Проверка результата настройки.

Для подключения можно использовать командную строку операционной системы или специализированный SSH-клиент. Пример подключения из командной строки:

```
ssh username@10.2.2.56
```

После успешной аутентификации пользователь получит доступ к интерфейсу командной строки коммутатора.

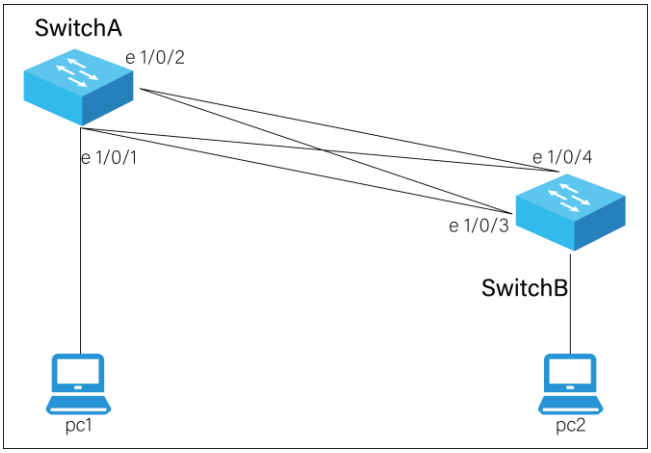
После выполнения настройки пользователи могут безопасно управлять коммутатором через протокол SSH. Использование шифрования обеспечивает защиту передаваемых данных и повышает уровень безопасности при удалённом администрировании сетевого оборудования.

3.38 Настройка протокола обнаружения однонаправленных связей (ULDP)

В сетях второго уровня иногда могут возникать однонаправленные каналы связи, при которых одно из устройств может передавать данные, но не может их принимать. Такая ситуация может возникать из-за повреждения кабеля, неисправности интерфейса или ошибок в работе оборудования. Однонаправленные соединения особенно опасны для протоколов управления топологией сети, например STP, так как могут привести к образованию петель и нарушению работы сети.

Для обнаружения подобных проблем используется протокол **ULDP (Unidirectional Link Detection Protocol)**. Он позволяет автоматически выявлять однонаправленные соединения между коммутаторами и принимать защитные меры, например отключать соответствующий порт.

Как показано на рисунке справае, необходимо настроить коммутаторы таким образом, чтобы при обнаружении однонаправленного соединения соответствующий интерфейс автоматически переводился в нерабочее состояние.



Этапы настройки:

Шаг 1. Включение ULDP. Сначала необходимо включить функцию ULDP в глобальном режиме, а затем активировать её на соответствующих интерфейсах.

Настройка на коммутаторе SwitchA:
SwitchA(config)# uldp enable
SwitchA(config)# interface ethernet 1/0/1
SwitchA(config-if-ethernet1/0/1)# uldp enable
SwitchA(config-if-ethernet1/0/1)# exit
SwitchA(config)# interface ethernet 1/0/2
SwitchA(config-if-ethernet1/0/2)# uldp enable

Настройка на коммутаторе SwitchB:
SwitchB(config)# uldp enable
SwitchB(config)# interface ethernet 1/0/3
SwitchB(config-if-ethernet1/0/3)# uldp enable
SwitchB(config-if-ethernet1/0/3)# exit
SwitchB(config)# interface ethernet 1/0/4
SwitchB(config-if-ethernet1/0/4)# uldp enable

После включения протокола коммутаторы начинают обмениваться служебными сообщениями для проверки двусторонней доступности соединения.

Шаг 2. Проверка результатов настройки:

SwitchA(config)# show uldp

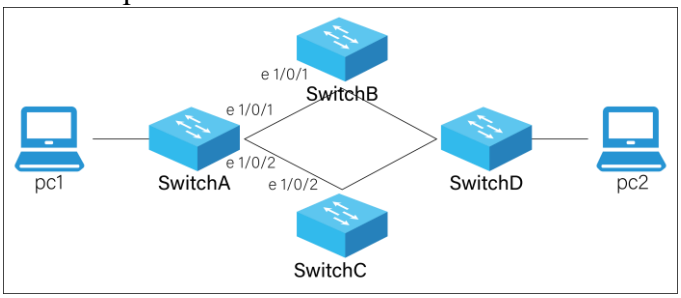
```
enable
uldp hello interval is                10
uldp shut down mode is                AUTO
uldp global work mode is              NORMAL
the total number of the port is       2

-------------------------------------------------------------------------------
  PortName      PhyLink   LineProto   WorkMode        PortState   NeighborNum
-------------------------------------------------------------------------------
  Ethernet1/0/1 UP        UP          NORMAL          INACTIVE    1
  Ethernet1/0/2 UP        UP          NORMAL          INACTIVE    1
-------------------------------------------------------------------------------
```

На рисунке справа показано, команда отображает информацию о состоянии протокола и интерфейсах, на которых он включен:

После выполнения настройки протокол ULDP позволяет обнаруживать однонаправленные соединения между коммутаторами и автоматически принимать меры для предотвращения нарушений работы сети. Это повышает надежность сетевой инфраструктуры и предотвращает возможные проблемы, связанные с образованием петель и некорректной работой протоколов второго уровня.

3.39 Настройка защиты Uplink-портов (ULPP)

В сетях второго уровня для обеспечения отказоустойчивости часто используются несколько восходящих каналов связи (uplink) к различным коммутаторам. Однако при отсутствии механизмов защиты такая топология может привести к образованию петель в сети.



На приведенной схеме справа коммутатор **A** имеет два аплинка, подключенных к коммутаторам **B** и **C**. Если в сети не используются механизмы предотвращения петель, такая структура может сформировать кольцевую топологию. Для предотвращения подобных ситуаций применяется протокол **ULPP (Uplink Loop Protection Protocol)**.

ULPP позволяет обнаруживать петли между восходящими каналами и автоматически отключать проблемный порт. Это обеспечивает стабильную работу сети и предотвращает возникновение широковещательных штормов.

Этапы настройки:

Шаг 1. Настройка протокола ULPP на коммутаторе A.

Сначала необходимо настроить VLAN и создать защищённый экземпляр MSTP, который будет использоваться протоколом ULPP:
SwitchA(config)# vlan 10
SwitchA(config-vlan10)# switchport interface ethernet 1/0/1-2
SwitchA(config-vlan10)# exit

Создание экземпляра MSTP:
SwitchA(config)# spanning-tree mst configuration
Create a protected instance
SwitchA(config-mstp-region)# instance 1 vlan 10
SwitchA(config-mstp-region)# exit

Создание группы ULPP:
SwitchA(config)# ulpp group 1
Create ulpp group
SwitchA(ulpp-group-1)# protect vlan-reference-instance 1
SwitchA(ulpp-group-1)# control vlan 10
SwitchA(ulpp-group-1)# exit

Назначение ролей интерфейсам:
SwitchA(config)# interface ethernet 1/0/1
SwitchA(config-if-ethernet1/0/1)# ulpp group 1 master
SwitchA(config-if-ethernet1/0/1)# exit

SwitchA(config)# interface ethernet 1/0/2
SwitchA(config-if-ethernet1/0/2)# ulpp group 1 slave
SwitchA(config-if-ethernet1/0/2)# exit

В данной конфигурации один из аплинков назначается **master**, а второй — **slave**, что позволяет ULPP контролировать состояние соединений.

Шаг 2. Настройка приема ULPP flush-пакетов на коммутаторе B.

На коммутаторе **B** необходимо включить обработку специальных ULPP-пакетов, которые используются для очистки таблиц MAC-адресов и ARP:
SwitchB(config)# vlan 10
SwitchB(config-vlan10)# switchport interface ethernet 1/0/1
SwitchB(config-vlan10)# exit

SwitchB(config)# interface ethernet 1/0/1
SwitchB(config-if-ethernet1/0/1)# ulpp flush enable mac
SwitchB(config-if-ethernet1/0/1)# ulpp flush enable arp
SwitchB(config-if-ethernet1/0/1)# ulpp control vlan 10

Шаг 3. Настройка приема ULPP flush-пакетов на коммутаторе C.

Аналогичная настройка выполняется на коммутаторе **C**:

```
SwitchC(config)# vlan 10
SwitchC(config-vlan10)# switchport interface ethernet 1/0/2
SwitchC(config-vlan10)# exit

SwitchC(config)# interface ethernet 1/0/2
SwitchC(config-if-ethernet1/0/2)# ulpp flush enable mac
SwitchC(config-if-ethernet1/0/2)# ulpp flush enable arp
SwitchC(config-if-ethernet1/0/2)# ulpp control vlan 10
```

Шаг 4. Проверка результата настройки:

```
switch(config)# show ulpp group 1
```

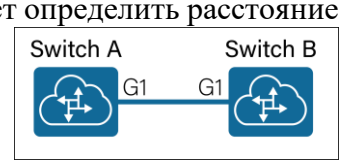
Команда отображает информацию о группе ULPP, состоянии интерфейсов и параметрах защиты, как показано на рисунке справа:

```
ULPP group 1 information:
Description:
Preemption mode: OFF
Preemption delay: 30s
Control VLAN: 10
Flush packet: MAC ARP
Protected VLAN: Reference Instance 1
Member              Role        State          Track-cfm-level
--------------------------------------------------------------------------------
Ethernet1/0/1       MASTER      STANDBY        -
Ethernet1/0/2       SLAVE       FORWARDING     -
--------------------------------------------------------------------------------
```

После выполнения настройки протокол ULPP контролирует состояние восходящих каналов и предотвращает образование петель в сети. При обнаружении петли один из аплинков может быть автоматически отключён, что обеспечивает стабильную работу сети и повышает её отказоустойчивость.

3.40 Настройка виртуального тестирования кабеля (VCT)

Функция **VCT (Virtual Cable Test)** предназначена для диагностики состояния сетевого кабеля, подключенного к порту коммутатора. Технология основана на методе рефлектометрии во временной области (TDR). При передаче по кабелю импульсного сигнала часть энергии может отражаться обратно, если сигнал достигает конца кабеля или места повреждения. Анализируя время прохождения сигнала и момент его возврата, коммутатор может определить расстояние до возможного повреждения или разрыва кабеля.



На приведённой справа схеме необходимо проверить состояние сетевого кабеля между коммутаторами A и B с помощью функции VCT:

Этапы настройки:

Шаг 1. Отключение сетевого кабеля. Сначала необходимо отсоединить сетевой кабель от порта 1 коммутатора B.

Шаг 2. Запуск VCT на коммутаторе A. После отключения кабеля выполните диагностику на соответствующем интерфейсе коммутатора **A**:

```
SwitchA# virtual-cable-test interface ethernet 1/0/1
```

Команда выполняет проверку состояния кабеля и отображает информацию о возможных повреждениях, длине кабеля и состоянии каждой пары проводников:

```
Interface Ethernet1/0/1:
------------------------------------------------
Cable pairs       Cable status       Length (meters)
------------      ------------       ---------------
(1, 2)            open                          1
(3, 6)            open                          1
(4, 5)            open                          1
(7, 8)            open                          1
As can be seen from the above information, the link of Switch A is disconnected, and the fault
point is 1 meter away from the port.
```

Шаг 3. Подключение сетевого кабеля. Подключите сетевой кабель обратно к порту 1 коммутатора B.

Шаг 4. Повторное выполнение тестирования. После восстановления соединения повторно выполните проверку кабеля:

SwitchA# virtual-cable-test interface ethernet 1/0/1

```
Interface Ethernet1/0/1:
-------------------------------------------------

Cable pairs       Cable status      Length (meters)
------------      ------------      ---------------
(1, 2)            well                        13
(3, 6)            well                        13
(4, 5)            well                        13
(7, 8)            well                        13

As can be seen from the above information, the link of Switch A works normally.
```

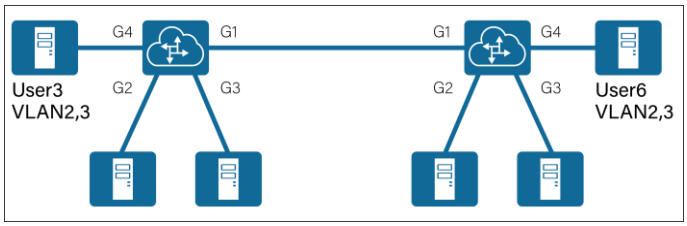
Результат работы команды представлен на рисунке справа:

Функция VCT позволяет выполнять диагностику сетевого кабеля непосредственно с коммутатора без использования дополнительных измерительных приборов. Это упрощает поиск повреждений кабеля, определение его длины и выявление возможных проблем соединения, что значительно ускоряет процесс обслуживания сетевой инфраструктуры.

3.41 Виртуальные локальные сети VLAN

Виртуальные локальные сети **VLAN (Virtual Local Area Network)** позволяют логически разделять сеть второго уровня на несколько изолированных сегментов. Это обеспечивает повышение безопасности сети, уменьшение широковещательного трафика и более гибкое управление доступом пользователей к сетевым ресурсам.
С помощью VLAN администратор может объединять устройства в логические группы независимо от их физического расположения. Устройства внутри одного VLAN могут напрямую обмениваться данными, тогда как связь между различными VLAN требует использования маршрутизации третьего уровня.

3.41.1 Настройка VLAN



Как показано на рисунке справа, в датацентре к двум коммутаторам подключено несколько пользователей. При этом пользователи, использующие одинаковые сетевые сервисы, могут подключаться через разные коммутаторы. Например: **User1 и User3** используют сервис **1, User2** использует сервис **2, User4 и User5** используют сервис **2, User6** использует сервисы **1 и 2.** Чтобы обеспечить безопасность сети и предотвратить широковещательные штормы, необходимо разделить пользователей по различным VLAN. Пользователи одного сервиса должны находиться в одном VLAN и иметь возможность обмениваться данными между собой, а пользователи разных сервисов не должны иметь прямого доступа друг к другу на втором уровне.

Этапы настройки:

Шаг 1. Создание VLAN и назначение портов. Создайте VLAN 2 и VLAN 3 на коммутаторе A, а затем назначьте соответствующие порты для пользователей.

Switch(config)# vlan 2-3

Назначение портов пользователей:
Switch(config)# interface ethernet 1/0/2

Switch(config-if-ethernet1/0/2)# switchport access vlan 2

Switch(config-if-ethernet1/0/2)# interface ethernet 1/0/3
Switch(config-if-ethernet1/0/3)# switchport access vlan 3

Порт, к которому подключён **User3**, настраивается как **гибридный (hybrid)** для доступа сразу к двум VLAN:
Switch(config-if-ethernet1/0/3)#interface ethernet 1/0/4
Switch(config-if-ethernet1/0/4)# switchport mode hybrid
Switch(config-if-ethernet1/0/4)# switchport hybrid allowed vlan 2-3 untag

Настройка коммутатора **B** выполняется аналогично.

Шаг 2. Настройка trunk-соединения между коммутаторами. Для передачи трафика нескольких VLAN между коммутаторами необходимо настроить магистральный порт (trunk):

Switch(config-if-ethernet1/0/4)# interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# switchport mode trunk
Switch(config-if-ethernet1/0/1)# switchport trunk allowed vlan add 2-3

Trunk-порт позволяет передавать трафик нескольких VLAN между коммутаторами.

Шаг 3. Проверка результата настройки:

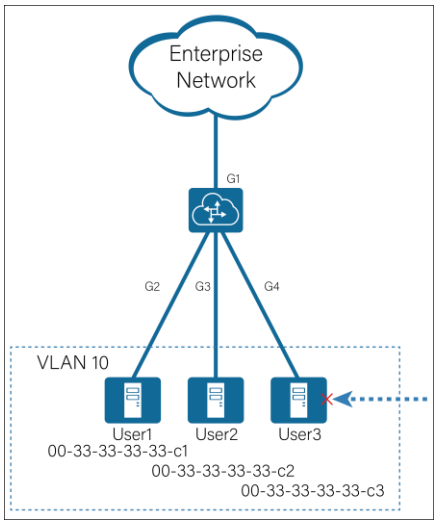
Switch(config)# show switchport interface ethernet 1/0/1

Пример вывода:
Ethernet1/0/1
Type :Universal
Mode :Trunk
Port VID :1
Trunk allowed Vlan: 1-4094

После выполнения настройки пользователи распределяются по различным VLAN в зависимости от используемых сервисов. Это позволяет изолировать сетевой трафик различных групп пользователей и повысить безопасность сети. Связь между коммутаторами осуществляется через trunk-порт, который передает трафик нескольких VLAN.

3.41.2 Настройка MAC-VLAN

В некоторых корпоративных сетях необходимо ограничить доступ к сети только для определённых пользователей. Одним из способов реализации такой политики является использование **MAC-VLAN**, при котором принадлежность устройства к VLAN определяется его **MAC-адресом**.
Как показано на рисунке справа, пользователи **User1**, **User2** и **User3** принадлежат конфиденциальному отделу компании. Только эти пользователи должны иметь возможность подключаться к сети через коммутатор. Если к порту будет подключено другое устройство с неизвестным MAC-адресом, доступ к сети предоставлен не будет.
Для реализации данной задачи выполняется привязка MAC-адресов пользователей к определённому VLAN.



Этапы настройки:

Шаг 1. Создание VLAN. Создайте VLAN, который будет использоваться для пользователей конфиденциального отдела:

Switch(config)# vlan 10

Шаг 2. Настройка портов.

Настройте порты коммутатора в режиме **hybrid** и добавьте их в VLAN 10:
Switch(config)# interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# switchport mode hybrid
Switch(config-if-ethernet1/0/1)# switchport hybrid native vlan 10
Switch(config-if-ethernet1/0/1)# switchport hybrid allowed vlan 10 tag

Настройка портов пользователей:
Switch(config-if-ethernet1/0/1)# interface ethernet 1/0/2-4
Switch(config-if-port-range)# switchport mode hybrid
Switch(config-if-port-range)# switchport hybrid allowed vlan 10 untag

Шаг 3. Привязка MAC-адресов к VLAN.

Настройте соответствие MAC-адресов пользователей VLAN 10:
Switch(config)# mac-vlan vlan 10
Switch(config)# mac-vlan mac 00-33-33-33-33-c1 ff-ff-ff-ff-ff-ff vlan 10 priority 1
Switch(config)# mac-vlan mac 00-33-33-33-33-c2 ff-ff-ff-ff-ff-ff vlan 10 priority 2
Switch(config)# mac-vlan mac 00-33-33-33-33-c3 ff-ff-ff-ff-ff-ff vlan 10 priority 3

В данной конфигурации MAC-адреса трёх пользователей привязываются к VLAN 10.

Шаг 4. Проверка результата настроек:

Switch(config)# show mac-vlan

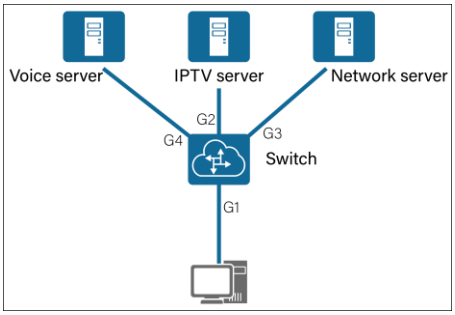
Результат выполнения команды представлен на рисунке справа:

Mac-Address	Mac-Mask	VLAN_ID	Priority
00-33-33-33-33-c1	ff-ff-ff-ff-ff-ff	10	1
00-33-33-33-33-c2	ff-ff-ff-ff-ff-ff	10	2
00-33-33-33-33-c3	ff-ff-ff-ff-ff-ff	10	3

После выполнения настройки устройства автоматически распределяются по VLAN на основе их MAC-адресов. Это позволяет ограничить доступ к сети только для авторизованных пользователей и повысить уровень информационной безопасности внутри организации.

3.41.3 VLAN на основе подсетей (Subnet-based VLAN)

В некоторых сетях требуется автоматически распределять сетевой трафик по различным VLAN в зависимости от IP-адреса источника. Такой механизм называется **VLAN на основе подсетей (Subnet-based VLAN)**.
Как показано на рисунке справа, коммутатор получает трафик от пользователей различных сервисов: интернет, IPTV, голосовая связь и другие. Для каждого сервиса используется своя IP-подсеть. Настроив соответствие между IP-под-



сетями и VLAN, коммутатор сможет автоматически определять принадлежность трафика к нужному VLAN и направлять его на соответствующий сервер.

Этапы настройки:

Шаг 1. Создание VLAN. Создайте VLAN для каждого типа сервиса:

Switch(config)# vlan 100,200,300

Шаг 2. Настройка соответствия подсетей VLAN.

Задайте правила, определяющие соответствие IP-подсетей определенным VLAN:
Switch(config)# subnet-vlan ip-address 192.168.1.2 mask 255.255.255.0 vlan 100 priority 1
Switch(config)# subnet-vlan ip-address 192.168.2.2 mask 255.255.255.0 vlan 200 priority 2
Switch(config)# subnet-vlan ip-address 192.168.3.2 mask 255.255.255.0 vlan 300 priority 3

В данной конфигурации:
- подсеть 192.168.1.0/24 сопоставляется с VLAN 100
- подсеть 192.168.2.0/24 сопоставляется с VLAN 200
- подсеть 192.168.3.0/24 сопоставляется с VLAN 300

Шаг 3. Настройка портов коммутатора.

Настройте порт, к которому подключаются пользователи, в режиме **hybrid** и разрешите передачу нескольких VLAN:
Switch(config)# interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# switchport mode hybrid
Switch(config-if-ethernet1/0/1)# switchport hybrid allowed vlan 100,200,300 untag

Настройте магистральные порты для передачи соответствующих VLAN к вышестоящим устройствам:
Switch(config-if-ethernet1/0/1)# interface ethernet 1/0/2
Switch(config-if-ethernet1/0/2)# switchport mode trunk
Switch(config-if-ethernet1/0/2)# switchport trunk allowed vlan add 100

Switch(config-if-ethernet1/0/2)# interface ethernet 1/0/3
Switch(config-if-ethernet1/0/3)# switchport mode trunk
Switch(config-if-ethernet1/0/3)# switchport trunk allowed vlan add 200

Switch(config-if-ethernet1/0/3)# interface ethernet 1/0/4
Switch(config-if-ethernet1/0/4)# switchport mode trunk
Switch(config-if-ethernet1/0/4)# switchport trunk allowed vlan add 300

Шаг 4. Проверка результата настройки:

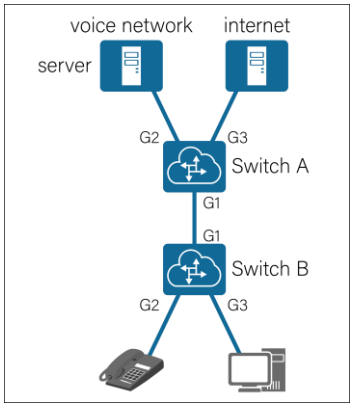
Switch(config)#show subnet-vlan

Результат выполнения команды показан на рисунке справа:

IP-Address	Mask	VLAN_ID	Priority
192.168.3.2	255.255.255.0	300	3
192.168.2.2	255.255.255.0	200	2
192.168.1.2	255.255.255.0	100	1

После выполнения настройки коммутатор автоматически определяет принадлежность трафика к соответствующему VLAN на основе IP-адреса источника. Это позволяет упростить управление сетью и автоматически разделять различные сервисы по отдельным VLAN.

3.41.4 VLAN на разных протоколах (Protocol-based VLAN)



В некоторых сетях требуется разделять трафик различных сетевых протоколов по отдельным VLAN. Такой подход называется **VLAN на основе протоколов (Protocol-based VLAN)**.
Как показано на рисунке справа, предприятие использует различные сетевые сервисы, такие как IPTV, VoIP и интернет. Для упрощения управления сетью администратор может распределить трафик разных протоколов по отдельным VLAN. В данном примере пользователи VLAN 100 используют протокол IPv4, пользователи VLAN 200 используют протокол IPv6. Разделение трафика по VLAN позволяет направлять его на соответствующие серверы и оптимизировать работу сети.

Этапы настройки:

Шаг 1. Создание VLAN.

Создайте VLAN для различных типов сервисов:
Switch(config)# vlan 100,200

В данном примере VLAN 100 используется для сервисов голосовой связи, VLAN 200 используется для сервисов передачи данных.

Шаг 2. Настройка соответствия протоколов VLAN.

Настройте соответствие между типом протокола и VLAN:
Switch(config)# protocol-vlan frametype ether2 ethertype 2048 vlan 100 priority 1
Switch(config)# protocol-vlan frametype ether2 ethertype 34525 vlan 200 priority 2

В данной конфигурации протокол IPv4 (ethertype 2048) сопоставляется с VLAN 100, протокол IPv6 (ethertype 34525) сопоставляется с VLAN 200.

Шаг 3. Настройка портов коммутатора.

Настройте пользовательский порт в режиме **hybrid** и добавьте его в соответствующие VLAN:
Switch(config)# interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# switchport mode hybrid
Switch(config-if-ethernet1/0/1)# switchport hybrid allowed vlan 100,200 untag

Настройте магистральные порты для передачи VLAN к другим устройствам сети:
Switch(config-if-ethernet1/0/1)# interface ethernet 1/0/2
Switch(config-if-ethernet1/0/2)# switchport mode trunk
Switch(config-if-ethernet1/0/2)# switchport trunk allowed vlan add 100

Switch(config-if-ethernet1/0/2)# interface ethernet 1/0/3
Switch(config-if-ethernet1/0/3)# switchport mode trunk
Switch(config-if-ethernet1/0/3)# switchport trunk allowed vlan add 200

Шаг 4: Проверка результата настройки:

Switch(config)# show protocol-vlan

Результат проверки команды показан на рисунке ниже:

Protocol_Type		VLAN_ID	Priority
---	---	---	
mode ethernetii etype 0x86dd		200	2
mode ethernetii etype 0x800		100	1

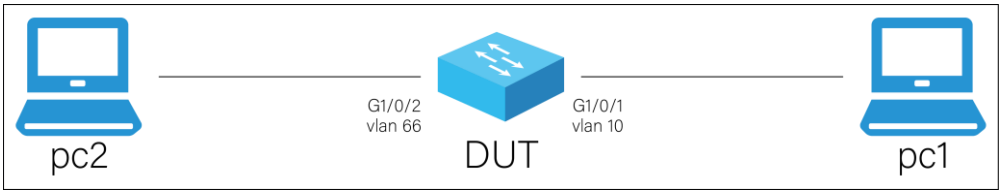
После выполнения настройки коммутатор автоматически распределяет сетевой трафик по VLAN в зависимости от используемого протокола. Это позволяет упростить управление сетью, разделить различные сервисы и повысить эффективность обработки сетевого трафика.

3.42 Настройка маршрутизации VLAN (VLAN Route)

Маршрутизация между VLAN используется для обеспечения обмена данными между различными виртуальными сетями. Поскольку устройства, находящиеся в разных VLAN, изолированы на втором уровне модели OSI, для их взаимодействия требуется маршрутизация третьего уровня. На коммутаторах уровня L3 данная задача может быть реализована с помощью **SVI (Switch Virtual Interface)** — виртуальных интерфейсов VLAN, которые выполняют функцию шлюза для устройств внутри соответствующих VLAN.

3.42.1 VLAN route внутри локальной сети

Как показано на рисунке ниже, **PC1** и **PC2** напрямую подключены к тестируемому устройству (**DUT**). Необходимо назначить статические IP-адреса на компьютерах и распределить порты коммутатора между **VLAN 10** и **VLAN 66**, чтобы обеспечить маршрутизацию между ними.



Этапы настройки:

Шаг 1: Создание VLAN и настройка SVI-интерфейсов.

Создайте VLAN и настройте виртуальные интерфейсы VLAN (SVI), которые будут выполнять роль шлюзов для соответствующих подсетей:
Switch(config)# vlan 10,66

Настройка интерфейса VLAN 10:
Switch (config)# interface vlan 10
Switch(config-if-vlan10)# ip address 10.10.10.1 255.255.255.0

Настройка интерфейса VLAN 66:
Switch (config)# interface vlan 66
Switch(config-if-vlan66)# ip address 10.10.66.1 255.255.255.0

Для просмотра текущей конфигурации используйте команду:
Switch(config)# show running-config

Шаг 2. Назначение портов VLAN.

Порт **Ethernet 1/0/1** добавляется в VLAN 10:
Switch(config)# interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# switchport access vlan 10

Порт **Ethernet 1/0/2** добавляется в VLAN 66:
Switch(config)# interface ethernet 1/0/2
Switch(config-if-ethernet1/0/1)# switchport access vlan 66

Шаг 3. Проверка результата настройки.
На конечных устройствах необходимо задать сетевые параметры. Например:
PC1:

- IP-адрес: 10.10.10.2
- Маска: 255.255.255.0
- Шлюз: 10.10.10.1

PC2:

- IP-адрес: 10.10.66.2
- Маска: 255.255.255.0
- Шлюз: 10.10.66.1

Функция **ip-routing** на коммутаторе включена по умолчанию.

Для проверки конфигурации SVI используйте команду:
Switch(config)# show running-config

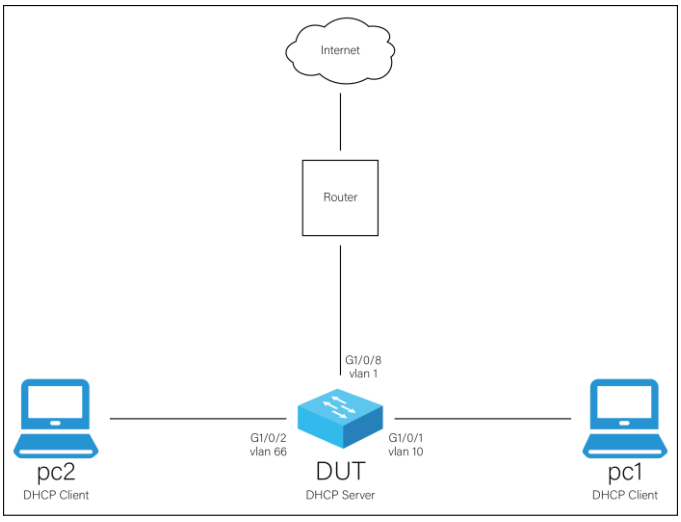
Результат работы программы показан на рисунке справа:

```
!
interface Vlan10
 ip address 10.10.10.1 255.255.255.0
!
interface Vlan66
 ip address 10.10.66.1 255.255.255.0
```

После выполнения настройки коммутатор уровня L3 выполняет маршрутизацию между VLAN 10 и VLAN 66 с использованием виртуальных интерфейсов SVI. Это позволяет устройствам из разных VLAN обмениваться данными через коммутатор.

3.42.2 VLAN route в сети Интернет

В данном сценарии тестируемое устройство (**DUT**) выполняет роль **DHCP-сервера**, который автоматически назначает IP-адреса клиентским устройствам. **PC1** и **PC2** получают сетевые параметры по DHCP. Коммутатор подключен к маршрутизатору, а маршрутизатор, в свою очередь, соединён с внешней сетью (Internet).



Этапы настройки:

Шаг 1. Включение DHCP-сервера:

Switch(config)# service dhcp

Шаг 2. Создание пулов DHCP-адресов. Создайте DHCP-пулы для VLAN 10 и VLAN 66 и настройте параметры сети.

Настройка DHCP для VLAN 10:
Switch(config)# ip dhcp pool VLAN10
Switch(dhcp-vlan10-config)# network-address 10.10.10.0 255.255.255.0
Switch(dhcp-vlan10-config)# default-router 10.10.10.1
Switch(dhcp-vlan10-config)# dns-server 8.8.8.8
Switch(dhcp-vlan10-config)# lease infinite
Switch(dhcp-vlan10-config)# max-lease-time infinite
Switch(dhcp-vlan10-config)# domain-name VLAN10
Switch(dhcp-vlan10-config)# exit

Настройка DHCP для VLAN 66:
Switch(config)# ip dhcp pool VLAN66
Switch(dhcp-vlan10-config)# network-address 10.10.66.0 255.255.255.0
Switch(dhcp-vlan10-config)# default-router 10.10.66.1
Switch(dhcp-vlan10-config)# dns-server 8.8.8.8
Switch(dhcp-vlan10-config)# lease infinite
Switch(dhcp-vlan10-config)# max-lease-time infinite
Switch(dhcp-vlan10-config)# domain-name VLAN66
Switch(dhcp-vlan10-config)# exit

Шаг 3. Настройка IP-адресов интерфейсов VLAN:

Switch(config)# interface vlan 1
Switch(config-if-vlan1)# ip address 192.168.20.60 255.255.255.0

Switch(config)# vlan10,66

Switch (config)# interface vlan 10
Switch(config-if-vlan10)# ip address 10.10.10.1 255.255.255.0

Switch (config)# interface vlan 66
Switch(config-if-vlan66)# ip address 10.10.66.1 255.255.255.0

Для корректной работы сети необходимо также настроить **статические или динамические маршруты** на коммутаторе и маршрутизаторе. Проверить текущую конфигурацию можно командой:

Switch(config)# show running-config

Шаг 4. Проверка результата настроек.

Для просмотра выданных DHCP-адресов используйте команду:
Switch(config)# show ip dhcp binding

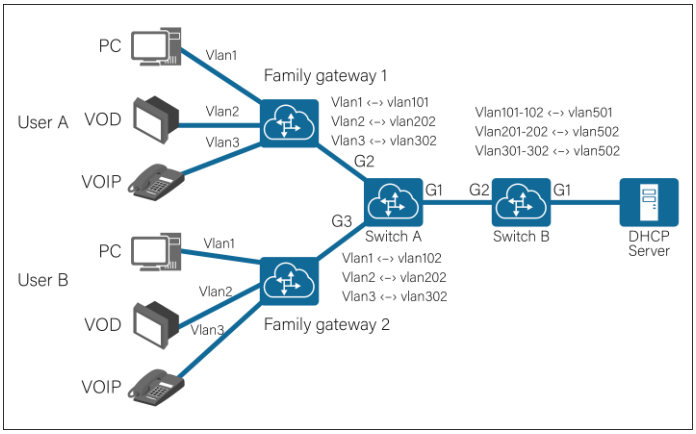
В выводе команды отображаются IP-адреса, назначенные подключённым устройствам:

```
Cloud-L3#show ip dhcp binding
Total dhcp binding items: 2, the matched: 2
IP address          Hardware address        Lease expiration        Type
10.10.10.2          00-E0-4C-21-00-34       Infinite                Automatic
10.10.66.2          F0-DE-F1-57-3B-C1       Infinite                Automatic
```

После выполнения настройки коммутатор выполняет функции DHCP-сервера и маршрутизатора между VLAN. Подключённые устройства автоматически получают сетевые параметры и

могут обмениваться данными как внутри локальной сети, так и с внешними сетями через маршрутизатор.

3.43 Настройка преобразования VLAN (VLAN Translation)



В сетях операторов связи часто используется механизм **VLAN Translation (преобразование VLAN)**. Он позволяет изменять VLAN ID при прохождении трафика через коммутатор. Это необходимо, когда на разных участках сети используются различные VLAN для одних и тех же сервисов. Как показано на рисунке справа, провайдер предоставляет домашним пользователям три вида услуг: **доступ в интернет (PC), видео по запросу (VoD), IP-телефонию (VoIP).**
Домашний шлюз пользователя разделяет услуги по VLAN: интернет — **VLAN 1,** видео — **VLAN 2,** телефония — **VLAN 3.** Однако на домовом коммутаторе необходимо разделить трафик разных пользователей для предотвращения конфликтов и повышения безопасности. Для этого каждому пользователю назначаются отдельные VLAN. На вышестоящем оборудовании трафик снова объединяется по типу сервиса: интернет → **VLAN 501,** видео → **VLAN 502,** телефония → **VLAN 503.**

Этапы настройки:

Шаг 1. Создание VLAN.

На **коммутаторе A**:
SwitchA(config)# vlan 1-3,101-102,201-202,301-302

На **коммутаторе B**:
SwitchB(config)# vlan 101-102,201-202,301-302,501-503

Шаг 2. Включение VLAN Translation и настройка правил преобразования. Включите функцию преобразования VLAN на соответствующих портах и задайте правила преобразования.

На **коммутаторе A.** Для первого пользователя:
SwitchA(config-if-ethernet1/0/2)# vlan-translation enable
SwitchA(config-if-ethernet1/0/2)# vlan-translation 1 to 101 in
SwitchA(config-if-ethernet1/0/2)# vlan-translation 2 to 201 in
SwitchA(config-if-ethernet1/0/2)# vlan-translation 3 to 301 in

На **коммутаторе A.** Для второго пользователя:
SwitchA(config-if-ethernet1/0/2)# interface ethernet 1/0/3
SwitchA(config-if-ethernet1/0/3)# vlan-translation enable
SwitchA(config-if-ethernet1/0/3)# vlan-translation 1 to 102 in
SwitchA(config-if-ethernet1/0/3)# vlan-translation 2 to 202 in
SwitchA(config-if-ethernet1/0/3)# vlan-translation 3 to 302 in

На **коммутаторе B**:
SwitchB(config)# interface ethernet 1/0/1
SwitchB(config-if-ethernet1/0/1)# vlan-translation enable

SwitchB(config-if-ethernet1/0/1)# vlan-translation 101 to 501 out
SwitchB(config-if-ethernet1/0/1)# vlan-translation 102 to 501 out
SwitchB(config-if-ethernet1/0/1)# vlan-translation 201 to 502 out
SwitchB(config-if-ethernet1/0/1)# vlan-translation 202 to 502 out
SwitchB(config-if-ethernet1/0/1)# vlan-translation 301 to 503 out
SwitchB(config-if-ethernet1/0/1)# vlan-translation 302 to 503 out

Шаг 3. Настройка типов портов и разрешенных VLAN. Настройте режимы портов и разрешите прохождение соответствующих VLAN:

На **коммутаторе A**:
SwitchA(config)# interface ethernet 1/0/2
SwitchA(config-if-ethernet1/0/2)# switchport mode hybrid
SwitchA(config-if-ethernet1/0/2)# switchport hybrid allowed vlan 1-3,101,201,301 tag

SwitchA(config-if-ethernet1/0/2)# interface ethernet 1/0/3
SwitchA(config-if-ethernet1/0/3)# switchport mode hybrid
SwitchA(config-if-ethernet1/0/3)# switchport hybrid allowed vlan 1-3,102,202,302 tag

Порт соединения между коммутаторами:
SwitchA(config-if-ethernet1/0/3)# interface ethernet 1/0/1
SwitchA(config-if-ethernet1/0/1)# switchport mode hybrid
SwitchA(config-if-ethernet1/0/1)# switchport hybrid allowed vlan 101-102,201-202,301-302 tag

SwitchB(config)# interface ethernet 1/0/2
SwitchB(config-if-ethernet1/0/2)# switchport mode hybrid
SwitchB(config-if-ethernet1/0/2)# switchport hybrid allowed vlan 101-102,201-202,301-302 tag

SwitchB(config-if-ethernet1/0/2)# interface ethernet 1/0/1
SwitchB(config-if-ethernet1/0/1)# switchport mode hybrid
SwitchB(config-if-ethernet1/0/1)# switchport hybrid allowed vlan 101-102,201-202,301-302,501-503 tag

Шаг 4. Проверка результата настройки:

Switch(config)# show vlan-translation

Пример результата выполнения команды:
vlan-translation is enable, miss drop is not set

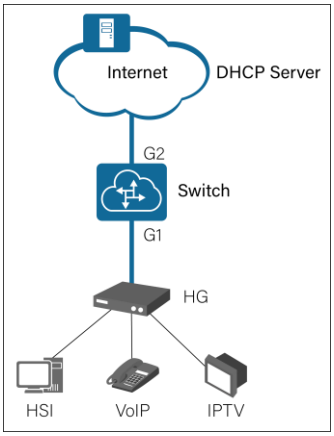
Interface Ethernet1/0/2:
vlan-translation 1 to 101 in
vlan-translation 2 to 201 in
vlan-translation 3 to 301 in

Interface Ethernet1/0/3:
vlan-translation 1 to 102 in
vlan-translation 2 to 202 in
vlan-translation 3 to 302 in

После выполнения настройки механизм **VLAN Translation** позволяет изменять VLAN-идентификаторы при прохождении трафика через коммутаторы. Это дает возможность разделять

трафик пользователей на уровне доступа и объединять его по типам сервисов на уровне агрегации сети. Такой подход повышает безопасность сети и позволяет эффективно использовать ресурсы VLAN.

3.44 Настройка голосового VLAN (Voice VLAN)



В сетях, где передаются различные типы трафика (HSI, IPTV, VoIP), особое внимание уделяется качеству голосовой связи. Для этого используется **Voice VLAN**, который позволяет выделить голосовой трафик в отдельную VLAN и задать для него повышенный приоритет. Как показано на рисунке справа, необходимо настроить голосовой VLAN для обеспечения стабильной и качественной передачи VoIP-трафика.

Этапы настройки:

Шаг 1. Создание голосового VLAN. Создайте VLAN, который будет использоваться для голосового трафика, и назначьте его как Voice VLAN:

```
Switch(config)# vlan 333
Switch(config-vlan)# exit
Switch(config)# voice vlan 333
```

Шаг 2. Настройка OUI (Organizationally Unique Identifier) для голосового трафика и определения голосовых устройств (например, IP-телефонов):

```
Switch(config)# voice-vlan mac 00:33:33:33:33:c1 ff:ff:ff:00:00:00 priority 1 name abc
```

Это позволяет коммутатору автоматически определять голосовой трафик по MAC-адресу и назначать ему соответствующий приоритет.

Шаг 3. Включение Voice VLAN на пользовательском порту:

```
Switch(config)# interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# switchport voice-vlan enable
```

Шаг 4. Настройка портов. Настройте порты в режиме **hybrid** и добавьте VLAN.

Порт для подключения IP-телефона (нетегированный трафик):

```
Switch(config-if-ethernet1/0/1)# switchport mode hybrid
Switch(config-if-ethernet1/0/1)# switchport hybrid allowed vlan 333 untag
```

Порт для передачи тегированного голосового трафика:

```
Switch(config-if-ethernet1/0/1)# interface ethernet 1/0/2
Switch(config-if-ethernet1/0/2)# switchport mode hybrid
Switch(config-if-ethernet1/0/2)# switchport hybrid allowed vlan 333 tag
```

Шаг 5. Проверка результата настройки:

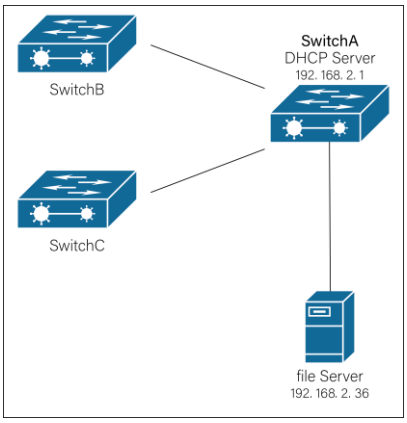
```
Switch(config)#show voice-vlan
```

Результат работы команды показан на рисунке ниже:

```
  Ethernet1/0/1(H)      Ethernet1/0/2(H)
  Ethernet1/0/3(A)      Ethernet1/0/4(A)
  Ethernet1/0/5(A)      Ethernet1/0/6(A)
  Ethernet1/0/7(A)      Ethernet1/0/8(A)
  Ethernet1/0/9(A)      Ethernet1/0/10(A)
Voice name              Mac-Address           Mask                  Priority
----------------------  --------------------  --------------------  --------
Siemens phone           00-01-E3-00-00-00     ff-ff-fff-00-00-00    0
Cisco phone             00-03-6B-00-00-00     fff-ff-ff-00-00-00    0
Avaya phone             00-04-0D-00-00-00     ff-ff-ff-00-00-00     0
Philips/NEC phone       00-60-B9-00-00-00     ff-ff-ff-00-00-00     0
Pingtel phone           00-D0-1E-00-00-00     ff-ff-ff-00-00-00     0
Polycom phone           00-E0-75-00-00-00     ff-ff-ff-00-00-00     0
3Com phone              00-E0-BB-00-00-00     ff-ff-ff-00-00-00     0
```

После выполнения настройки голосовой трафик автоматически выделяется в отдельный VLAN и получает повышенный приоритет. Это обеспечивает стабильное качество связи и минимизирует задержки и потери пакетов при передаче VoIP.

3.45 Автоматическая настройка сетевых устройств (ZTP)



ZTP (Zero Touch Provisioning) — это технология автоматической настройки сетевых устройств без участия администратора. Новые коммутаторы с «чистой» конфигурацией автоматически получают IP-адрес, загружают конфигурацию и обновления с сервера. Как показано на рисунке справа, коммутаторы **B** и **C** подключаются к коммутатору **A**, который выступает в роли DHCP-сервера и обеспечивает их автоматическую настройку:

Этапы настройки:

Шаг 1. Подготовка файла конфигурации. Создайте конфигурационный файл для новых устройств. Например, файл конфигурации: ***new.cfg,*** файл прошивки: ***new.img.*** Файл должен содержать все необходимые параметры для автоматической настройки коммутаторов.

Шаг 2. Настройка DHCP-сервера на коммутаторе A:

Включение DHCP:
Switch(config)# service dhcp

Создание диапазона адресов:
Switch(config)# ip dhcp pool 1

Настройка сети:
Switch(dhcp-1-config)# network-address 192.168.2.0 255.255.255.0

Указание загрузочного файла:
Switch(dhcp-1-config)# bootfile new.cfg:new.img

Указание TFTP-сервера для автоматического обновления и настройки новых устройств:
Switch(dhcp-1-config)# auto upgrade via tftp address 192.168.2.36

Указание сервера файлов:

Switch(dhcp-1-config)# next-server 192.168.2.36

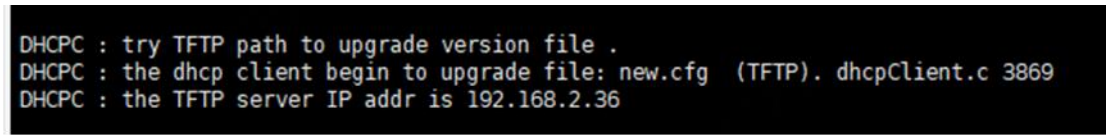
Шаг 3. Настройка файлового сервера. Настройте TFTP-сервер (или другой файловый сервер), на котором размещены файл конфигурации ***new.cfg*** и образ системы ***new.img.*** Убедитесь, что новые устройства имеют доступ к этому серверу по сети.

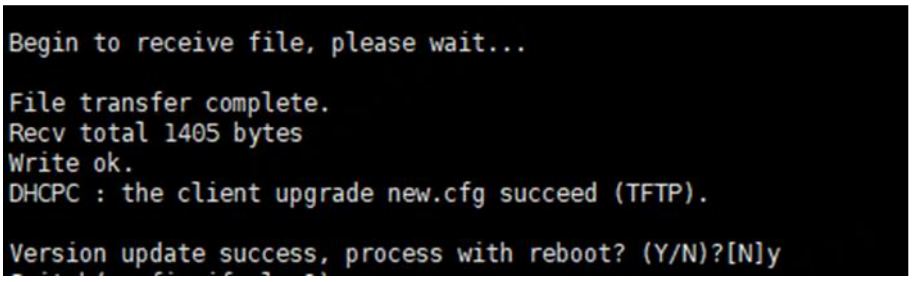
Шаг 4. Включение ZTP на коммутаторах. На новых коммутаторах включите автоматическое обновление через DHCP:

Switch(config)# interface vlan 1
Switch(config-if-vlan1)# ip dhcp-client upgrade enable
Switch(config-if-vlan1)# ip dhcp-client upgrade begin

Шаг 5. Проверка результата настройки.

После включения коммутаторов устройства получают IP-адрес от DHCP, подключаются к TFTP-серверу, загружают конфигурацию и ПО, автоматически применяют настройки. Результат процесса можно наблюдать в логах устройства или на рисунках ниже:





После настройки ZTP новые коммутаторы автоматически получают конфигурацию и обновления без ручного вмешательства. Это значительно ускоряет развертывание сети, снижает вероятность ошибок и упрощает администрирование большого количества устройств.

ipanda.pro

info@ipanda.pro

8-800-222-94-84

ТЕХ.ПОДДЕРЖКА:

ВК:

MAX:

САЙТ: