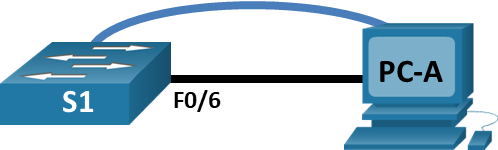


**Базовая настройка коммутатора**

# Топология



# Таблица адресации

|  |  |  |
| --- | --- | --- |
| **Устройство** | **Интерфейс** | **IP-адрес / префикс** |
| S1\_ФАМИЛИЯ  *S1*  *S1* | VLAN X  *VLAN 99*  *VLAN 99* | 192.168.1.X+2 /24 |
| 2001:db8:acad::2 /64 |
| fe80::2 |
| PC-A  *PC-A* | NIC  *NIC* | 192.168.1.X+10 /24 |
| 2001:db8:acad::3 /64 |
| fe80::3 |
| *PC-A* | *NIC* |  |

# Задачи

**Часть 1. Проверка конфигурации коммутатора по умолчанию Часть 2. Создание сети и настройка основных параметров устройства**

* Настройте базовые параметры коммутатора.
* Настройте IP-адрес для ПК.

**Часть 3. Проверка сетевых подключений**

* Отобразите конфигурацию устройства.
* Протестируйте сквозное соединение, отправив эхо-запрос.
* Протестируйте возможности удаленного управления с помощью Telnet.

**Часть 4. Управление таблицей MAC-адресов**

* Запишите MAC-адрес узла.
* Определите МАС-адреса, полученные коммутатором.
* Перечислите параметры команды **show mac address-table**.
* Назначьте статический MAC-адрес.

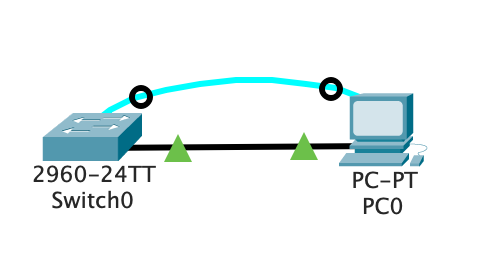
*Закройте окно настройки.*

# Необходимые ресурсы

* 1 коммутатор (Cisco 2960 с ПО Cisco IOS версии 15.2(2) с образом lanbasek9 или аналогичная модель)
* 1 ПК (под управлением Windows с программой эмуляции терминала, например, Tera Term)
* 1 консольный кабель для настройки устройства на базе Cisco IOS через консольный порт.
* 1 кабель Ethernet, как показано в топологии.

# Часть 1. Создание сети и проверка настроек коммутатора по умолчанию

В первой части лабораторной работы вам предстоит настроить топологию сети и проверить настройку коммутатора по умолчанию.



**Шаг 1. Создайте сеть согласно топологии.**

1. Подсоедините консольный кабель, как показано в топологии. На данном этапе не подключайте кабель Ethernet компьютера PC-A.
2. Установите консольное подключение к коммутатору с компьютера PC-A с помощью Tera Term или другой программы эмуляции терминала.

Вопрос:

Почему нужно использовать консольное подключение для первоначальной настройки коммутатора? Почему нельзя подключиться к коммутатору через Telnet или SSH?

**Шаг 2. Проверьте настройки коммутатора по умолчанию.**

На данном этапе вам нужно проверить такие параметры коммутатора по умолчанию, как текущие настройки коммутатора, данные IOS, свойства интерфейса, сведения о VLAN и флеш-память.

Все команды IOS коммутатора можно выполнять из привилегированного режима. Доступ к привилегированному режиму нужно ограничить с помощью пароля, чтобы предотвратить неавторизованное использование устройства — через этот режим можно получить прямой доступ к режиму глобальной конфигурации и командам, используемым для настройки рабочих параметров. Пароли можно будет настроить чуть позже.

1. Предположим, что коммутатор не имеет файла конфигурации, сохраненного в энергонезависимой памяти (NVRAM). Консольное подключение к коммутатору с помощью Tera Term или другой программы эмуляции терминала предоставит доступ к командной строке пользовательского режима EXEC в виде Switch>. Войдите в привилегированный режим EXEC.

*Откройте окно конфигурации*

Обратите внимание, что измененная в конфигурации строка будет отражать привилегированный режим EXEC.

1. Изучите текущий файл running configuration.

Вопросы:

Сколько интерфейсов FastEthernet имеется на коммутаторе 2960? - 24

Сколько интерфейсов Gigabit Ethernet имеется на коммутаторе 2960? - 2

Каков диапазон значений, отображаемых в vty-линиях? 0-15

1. Изучите файл загрузочной конфигурации (startup configuration), который содержится в энергонезависимом ОЗУ (NVRAM).

Вопрос:

1. Изучите характеристики SVI для VLAN 1.

Какие выходные данные вы видите? - no ip address, shutdown

1. Изучите сведения о версии ОС Cisco IOS на коммутаторе.

Вопросы:

Под управлением какой версии ОС Cisco IOS работает коммутатор? - C2960-LANBASE-M

Как называется файл образа системы? - c2960-lanbase-mz.122-25.FX.bin

Какой базовый MAC-адрес назначен коммутатору? - 0030.F2DE.EC13

1. Изучите свойства по умолчанию интерфейса FastEthernet, который используется компьютером PC-

A.

Интерфейс включен или выключен? - Включен

Что нужно сделать, чтобы включить интерфейс? -

Какой MAC-адрес у интерфейса? - 00E0.F797.B7EE

Какие настройки скорости и дуплекса заданы в интерфейсе? - Auto

1. Изучите параметры сети VLAN по умолчанию на коммутаторе.

Какое имя присвоено сети VLAN 1 по умолчанию? - default

Какие порты расположены в сети VLAN 1? - все

Активна ли сеть VLAN 1? - да

К какому типу сетей VLAN принадлежит VLAN по умолчанию? - enet

1. Изучите флеш-память.

Выполните одну из следующих команд, чтобы изучить содержимое флеш-каталога.

Switch# **show flash** Switch# **dir flash:**

В конце имени файла указано расширение, например, .bin. Каталоги не имеют расширения файла.

Вопрос:

Какое имя присвоено образу Cisco IOS? - c2960-lanbase-mz.122-25.FX.bin

# Часть 2. Настройка базовых параметров сетевых устройств

Во второй части необходимо будет настроить основные параметры коммутатора и компьютера.

**Шаг 1. Настройте базовые параметры коммутатора.**

1. В режиме глобальной конфигурации скопируйте следующие базовые параметры конфигурации и вставьте их в файл на коммутаторе S1\_ФАМИЛИЯ.

no ip domain-lookup hostname S1\_ФАМИЛИЯ service password-encryption enable secret class banner motd #

Unauthorized access is strictly prohibited. #

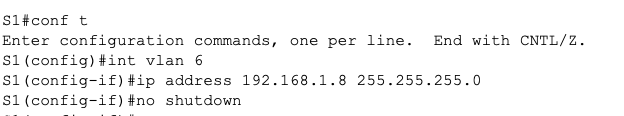
1. Назначьте IP-адрес интерфейсу SVI на коммутаторе. Благодаря этому вы получите возможность удаленного управления коммутатором.

Прежде чем вы сможете управлять коммутатором S1\_ФАМИЛИЯ удаленно с компьютера PC-A, коммутатору нужно назначить IP-адрес. Согласно конфигурации по умолчанию коммутатором можно управлять через VLAN 1. Однако в базовой конфигурации коммутатора не рекомендуется назначать VLAN 1 в качестве административной VLAN.

Для административных целей используйте VLAN X, где X – номер студента в журнале. Выбор VLAN X является случайным, поэтому вы не обязаны использовать VLAN X всегда.

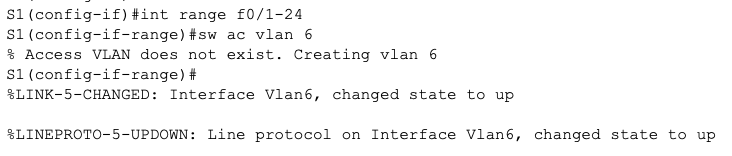
Итак, для начала создайте на коммутаторе новую VLAN X. Затем настройте IP-адрес коммутатора на 192.168.1.X+2 с маской подсети 255.255.255.0 на внутреннем виртуальном интерфейсе (SVI) VLAN X. IPv6-адрес также можно настроить на интерфейсе SVI. Настройте IPv6-адреса для маршрутизаторов в соответствии с таблицей адресации.

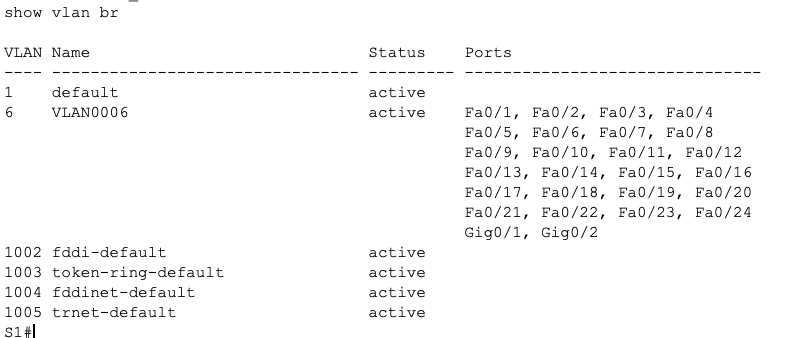
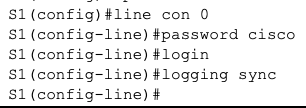
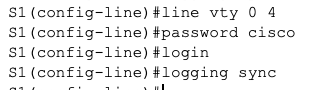
Обратите внимание, что интерфейс VLAN X выключен, несмотря на то что вы ввели команду **no shutdown**. В настоящее время интерфейс выключен, поскольку сети VLAN X не назначены порты коммутатора.



1. Ассоциируйте все пользовательские порты с VLAN X.

Чтобы установить подключение между узлом и коммутатором, порты, используемые узлом, должны находиться в той же VLAN, что и коммутатор. Обратите внимание, что в выходных данных выше интерфейс VLAN 1 выключен, поскольку ни один из портов не назначен сети VLAN 1. Через несколько секунд VLAN X включится, потому что как минимум один активный порт (F0/6, к которому подключен компьютер PC-A) назначен сети VLAN X.



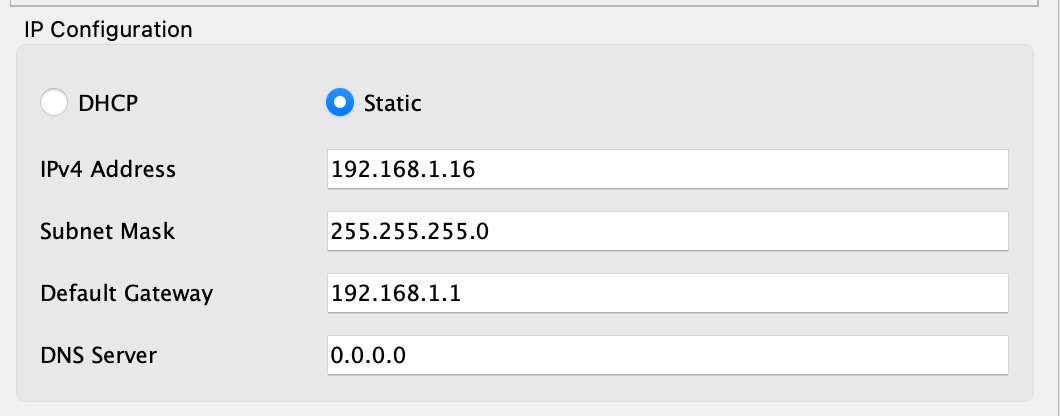
1. Чтобы убедиться, что все порты находятся в сети VLAN X, выполните команду **show vlan brief**. 
2. Настройте шлюз по умолчанию для коммутатора S1\_ФАМИЛИЯ. Если не настроен ни один шлюз по умолчанию, коммутатором нельзя управлять из удаленной сети, на пути к которой имеется более одного маршрутизатора. Хотя в этом упражнении не учитывается внешний IP-шлюз, представьте, что впоследствии вы подключите LAN к маршрутизатору для обеспечения внешнего доступа. При условии, что интерфейс LAN маршрутизатора равен 192.168.1.1, настройте шлюз по умолчанию для коммутатора. 
3. Доступ через порт консоли также следует ограничить с помощью пароля. Используйте **cisco** в качестве пароля для входа в консоль в этом задании. Конфигурация по умолчанию разрешает все консольные подключения без пароля. Чтобы консольные сообщения не прерывали выполнение команд, используйте параметр **logging synchronous** в режиме конфигурации консоли. 
4. Настройте каналы виртуального соединения для удаленного управления (vty), чтобы коммутатор разрешил доступ через Telnet. Если не настроить пароль VTY, будет невозможно подключиться к коммутатору по протоколу Telnet. 

Вопрос:

Для чего нужна команда **login**? Не забудьте ввести данную команду в нужных режимах конфигурации.

***Введите ваш ответ здесь.***

**Шаг 2. Настройте IP-адрес на компьютере PC-A.**

Назначьте компьютеру IP-адрес и маску подсети в соответствии с таблицей адресации. Здесь описана сокращенная версия данной операции. Для рассматриваемой топологии не требуется шлюз по умолчанию. Однако вы можете ввести адрес **192.168.1.1** и **fe80::1**, чтобы смоделировать маршрутизатор, подключенный к коммутатору S1\_ФАМИЛИЯ. 

# Часть 3. Проверка сетевых подключений

В третьей части лабораторной работы вам предстоит проверить и задокументировать конфигурацию коммутатора, протестировать сквозное соединение между компьютером PC-A и коммутатором S1\_ФАМИЛИЯ, а также протестировать возможность удаленного управления коммутатором.

**Шаг 1. Отобразите конфигурацию коммутатора.**

Используйте консольное подключение на компьютере PC-A для отображения и проверки конфигурации коммутатора. Введите соответствующую команду, чтобы отобразить всю текущую конфигурацию. Для пролистывания используйте клавишу пробела.

a. Проверьте параметры административной VLAN X с помощью команды **show interface**.

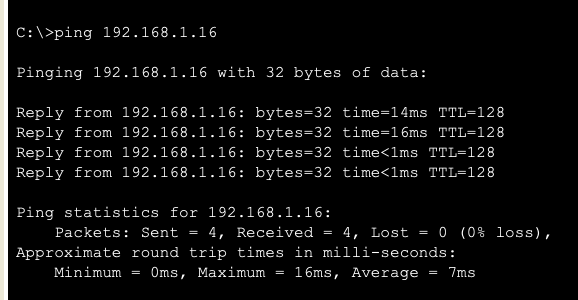
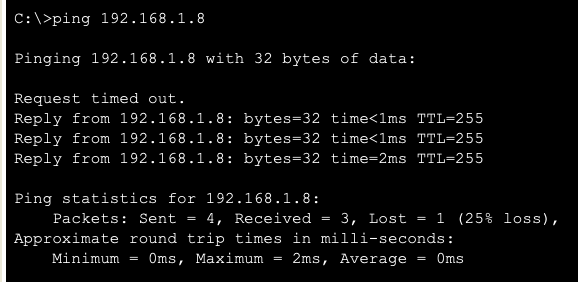
Какова полоса пропускания этого интерфейса? - 100000 Kbit

В каком состоянии находится VLAN X? - Up

В каком состоянии находится канальный протокол? - Up

*Закройте окно настройки.*

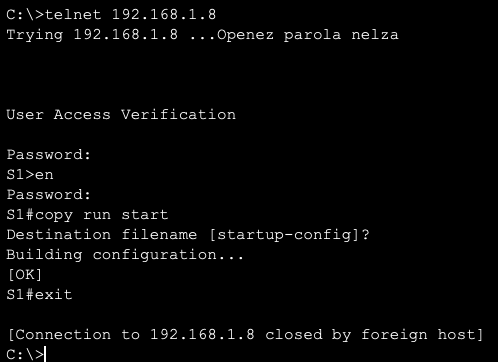
**Шаг 2. Протестируйте сквозное соединение, отправив эхо-запрос.**

1. В командной строке компьютера PC-A с помощью утилиты ping проверьте связь сначала с адресом PC-A. 
2. Из командной строки компьютера PC-A отправьте эхо-запрос на административный адрес интерфейса SVI коммутатора S1\_ФАМИЛИЯ. 

Поскольку компьютеру PC-A нужно преобразовать МАС-адрес коммутатора S1\_ФАМИЛИЯ с помощью ARP, время ожидания передачи первого пакета может истечь. Если эхо-запрос не удается, найдите и устраните неполадки базовых настроек устройства. Проверьте как физические кабели, так и логическую адресацию.

**Шаг 3. Проверьте удаленное управление коммутатором S1\_ФАМИЛИЯ.**

После этого используйте удаленный доступ к устройству с помощью Telnet. В этой лабораторной работе устройства PC-A и S1\_ФАМИЛИЯ расположены рядом. В производственной сети коммутатор может находиться в коммутационном шкафу на последнем этаже, в то время как административный компьютер находится на первом этаже. На данном этапе вам предстоит использовать Telnet для удаленного доступа к коммутатору S1\_ФАМИЛИЯ через его административный адрес SVI. Telnet — это не безопасный протокол, но вы можете использовать его для проверки удаленного доступа. В случае с Telnet вся информация, включая пароли и команды, отправляется через сеанс в незашифрованном виде. В последующих лабораторных работах вы будете использовать протокол SSH для удаленного доступа к сетевым устройствам.

1. Откройте Tera Term или другую программу эмуляции терминала с возможностью Telnet.
2. Выберите сервер Telnet и укажите адрес управления SVI для подключения к S1\_ФАМИЛИЯ. Пароль: **cisco**.
3. После ввода пароля **cisco** вы окажетесь в командной строке пользовательского режима. Войдите в привилегированный режим EXEC, используя пароль **class**.
4. Сохраните конфигурацию.
5. Чтобы завершить сеанс Telnet, введите **exit**. 

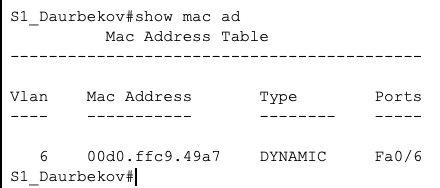
# Часть 4. Управление таблицей MAC-адресов

В четвертой части необходимо определить MAC-адрес, полученный коммутатором, настроить статический MAC-адрес для одного из интерфейсов коммутатора, а затем удалить статический MACадрес из конфигурации интерфейса.

**Шаг 1. Запишите MAC-адрес узла.**

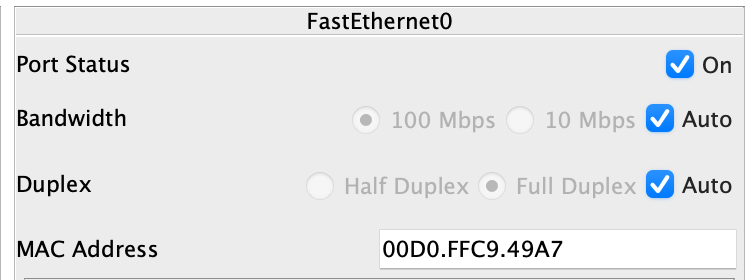
В командной строке компьютера PC-A выполните команду для отображения сетевой конфигурации, чтобы определить и записать адреса 2-го уровня (физические) сетевой интерфейсной платы. **Шаг 2. Определите МАС-адреса, полученные коммутатором.**

*Откройте окно конфигурации*

Отобразите МАС-адреса с помощью команды **show mac address-table**. 

Сколько динамических адресов присутствует? - 1

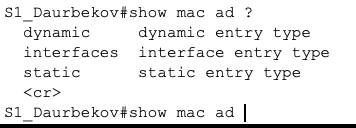
Сколько МАС-адресов имеется в общей сложности? - 1

Совпадает ли динамический MAC-адрес с МАС-адресом компьютера PC-A? - Да 

**Шаг 3. Перечислите параметры команды show mac address-table.**

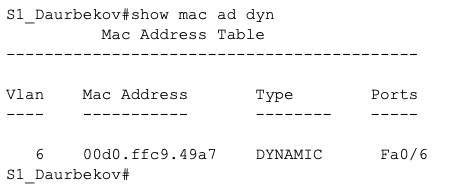
1. Отобразите параметры таблицы МАС-адресов.

S1\_ФАМИЛИЯ# **show mac address-table ?**



Вопрос:

Сколько параметров доступно для команды **show mac address-table**? - 3

1. Введите команду **show mac address-table dynamic**, чтобы отобразить только те МАС-адреса, которые были получены динамически. 

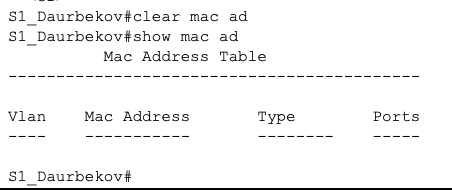
Сколько динамических адресов присутствует? - 1

1. Просмотрите запись MAC-адреса для компьютера PC-A. Формат MAC-адреса для команды:

xxxx.xxxx.xxxx.

S1\_ФАМИЛИЯ# **show mac address-table address <PC-A MAC here>** \*Не работает\*

**Шаг 4. Назначьте статический MAC-адрес.**

1. Очистите таблицу MAC-адресов. Чтобы удалить существующие МАС-адреса, в исполнительском режиме EXEC используйте команду **clear mac address-table dynamic**.
2. Убедитесь, что таблица МАС-адресов очищена, введите команду для просмотра таблицы MACадресов. 

Вопрос:

Сколько статических MAC-адресов присутствует сейчас в таблице? - 0

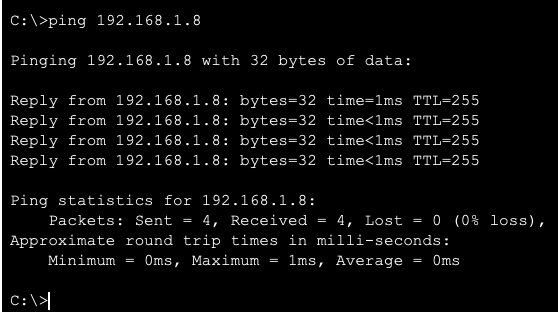
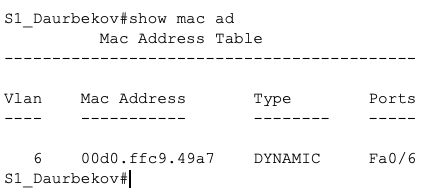
Сколько динамических адресов присутствует? - 0

1. Снова изучите таблицу МАС-адресов.

Скорее всего, приложение, работающее на вашем ПК, уже отправило кадр из сетевого адаптера на коммутатор S1\_ФАМИЛИЯ. Снова просмотрите таблицу МАС-адресов и выясните, был ли МАСадрес компьютера PC-A повторно получен коммутатором S1\_ФАМИЛИЯ.Вопросы:

Сколько динамических адресов присутствует? - 1

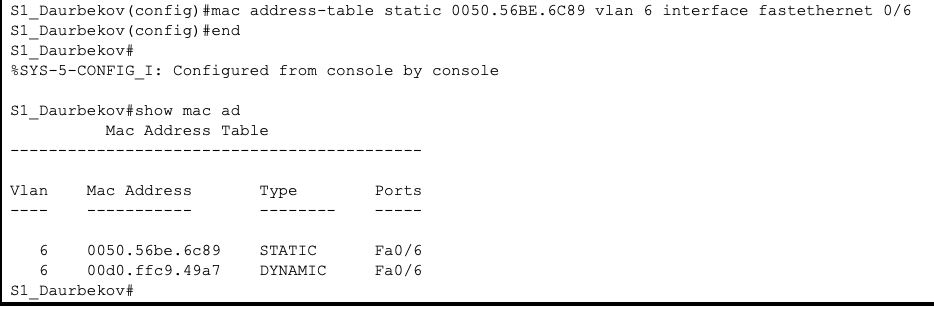
Почему это значение изменилось с предыдущего раза? – Из-за эхо запроса

Если коммутатор S1\_ФАМИЛИЯ еще не получил повторно MAC-адрес для PC-A, отправьте эхозапрос на IP-адрес VLAN X коммутатора от PC-A, а затем снова выполните команду для просмотра таблицы MAC-адресов.  

1. Назначьте статический MAC-адрес. Чтобы определить, к каким портам может подключиться узел, можно создать статическое сопоставление узлового МАС-адреса с портом.

Настройте статический MAC-адрес на интерфейсе F0/6, используя адрес, записанный для PC-A в части 4, на шаге 1. MAC-адрес 0050.56BE.6C89 используется только в качестве примера. Необходимо использовать MAC-адрес компьютера PC-A, который **отличается** от указанного здесь в качестве примера.

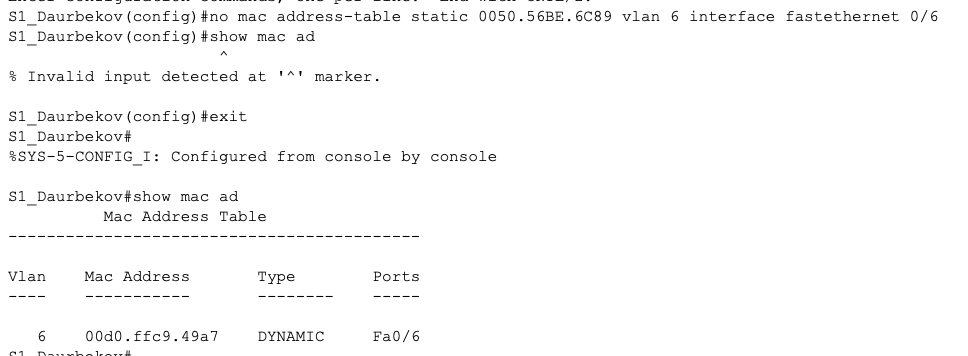
S1\_фамилия(config)# **mac address-table static 0050.56BE.6C89 vlan X interface fastethernet 0/6**

1. Выполните проверку записей в таблице MAC-адресов. 

Сколько всего динамических адресов присутствует? - 1

Сколько статических адресов присутствует? - 1

1. Удалите запись статического МАС. Перейдите в режим глобальной настройки и удалите команду.

Для этого укажите **no** перед строкой с командой. 

1. Убедитесь, что статический МАС-адрес был удален.

Сколько всего статических MAC-адресов содержится в таблице? - 0

*Закройте окно настройки.*

## Вопросы для защиты теоретической части (главы 1, 2)

**Зачем необходимо настраивать пароль VTY для коммутатора?**

Настройка пароля VTY для коммутатора важна по нескольким причинам:

1. Безопасность: Установка пароля на линии VTY помогает обеспечить безопасность вашей сети, предотвращая несанкционированный доступ к коммутатору через удаленное управление.

2. Аутентификация: По мере того как пользователи будут пытаться подключиться к коммутатору по Telnet или SSH через линии VTY, пароль будет использоваться для проверки подлинности пользователей.

3. Контроль доступа: Настройка пароля VTY позволяет контролировать, кто имеет право подключаться к коммутатору по удаленным средствам управления.

**Зачем нужно изменять VLAN 1 по умолчанию на сеть VLAN с другим номером?**

1. Безопасность: VLAN 1 по умолчанию часто используется для управления и имеет ряд уязвимостей, связанных с протоколами управления сетью. Изменение на другой VLAN с другим номером поможет уменьшить уязвимости и улучшить безопасность сети.

2. Изоляция устройств: Использование VLAN, отличного от VLAN 1, помогает разделить сетевой трафик на логические сегменты, что повышает безопасность и упрощает управление сетью.

3. Избегание конфликтов: Переключение с VLAN 1 на другой номер предотвращает возможные конфликты и проблемы, связанные с попытками наложения настройка на стандартный VLAN по умолчанию.

**. Что нужно сделать, чтобы пароли не отправлялись в незашифрованном виде?**

Для того чтобы пароли не отправлялись в незашифрованном виде, особенно в контексте сетевых устройств или приложений, следует принимать следующие меры:

1. Использование протоколов шифрования: Важно использовать защищенные протоколы, такие как SSH (Secure Shell) или HTTPS, для удаленного доступа к устройствам. Эти протоколы обеспечивают шифрование трафика, включая передачу паролей.

2. Хэширование паролей: Вместо хранения паролей в открытом виде, рекомендуется хэшировать их с помощью криптографических хэш-функций. Таким образом, даже если данные будут скомпрометированы, злоумышленники не смогут прочитать сами пароли.

3. \*\*Регулярная смена паролей\*\*: Важно регулярно менять пароли и следить за их сложностью, чтобы уменьшить вероятность компрометации учетных данных.

**Зачем нужно настраивать статический MAC-адрес на интерфейсе порта**

Настройка статического MAC-адреса на интерфейсе порта имеет несколько преимуществ и целей:

1. Безопасность сети: При наличии статического MAC-адреса на интерфейсе порта можно предотвратить атаки, связанные с подменой MAC-адресов (spoofing). Это поможет обеспечить дополнительный уровень безопасности для сетевых устройств.

2. Стабильность сети: Использование статического MAC-адреса на интерфейсе порта помогает сохранить постоянное соответствие между MAC-адресом и портом в сети, что способствует стабильной работе сети.

3. Идентификация устройства: Установление статического MAC-адреса на интерфейсе порта упрощает идентификацию конкретных устройств в сети и управление ими.

4. Предотвращение конфликтов с MAC-адресами: Использование статического MAC-адреса на интерфейсе порта помогает избежать возможных конфликтов с другими устройствами в сети.