

Базовая настройка коммутатора

Топология

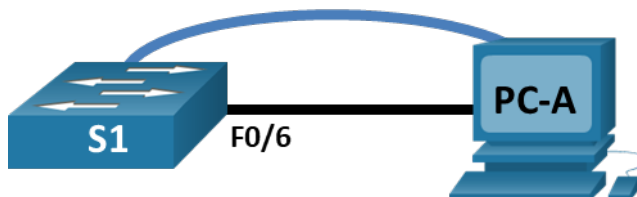


Таблица адресации

| Устройство | Интерфейс | IP-адрес / префикс |
|------------|-----------|----------------------|
| S1_ФАМИЛИЯ | VLAN X | 192.168.1.X+2 /24 |
| | | 2001:db8:acad::2 /64 |
| | | fe80::2 |
| PC-A | NIC | 192.168.1.X+10 /24 |
| | | 2001:db8:acad::3 /64 |
| | | fe80::3 |

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

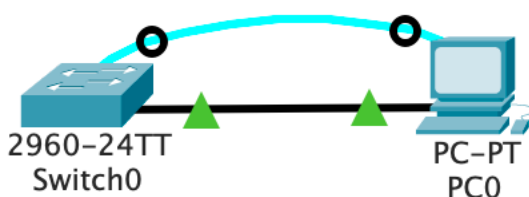
- Запишите MAC-адрес узла.
- Определите MAC-адреса, полученные коммутатором.
- Перечислите параметры команды **show mac address-table**.
- Назначьте статический MAC-адрес.

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.

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

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.

- 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.

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

- Изучите текущий файл running configuration.

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

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

- d. Изучите характеристики SVI для VLAN 1.

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

- e. Изучите сведения о версии ОС Cisco IOS на коммутаторе.

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

- f. 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

- g. 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

- h. 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.

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.

- a. 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. #
```

- b. 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.

```
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int vlan 6
S1(config-if)#ip address 192.168.1.8 255.255.255.0
S1(config-if)#no shutdown
... ..
```

- c. 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.

```
S1(config-if)#int range f0/1-24
S1(config-if-range)#sw ac vlan 6
% Access VLAN does not exist. Creating vlan 6
S1(config-if-range)#
%LINK-5-CHANGED: Interface Vlan6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan6, changed state to up
```

- d. Чтобы убедиться, что все порты находятся в сети VLAN X, выполните команду **show vlan brief**.

```
show vlan br
```

| VLAN | Name | Status | Ports |
|------|--------------------|--------|---|
| 1 | default | active | |
| 6 | VLAN0006 | active | Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2 |
| 1002 | fddi-default | active | |
| 1003 | token-ring-default | active | |
| 1004 | fddinet-default | active | |
| 1005 | trnet-default | active | |

```
S1#
```

- e. 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.

```
S1(config)#ip default 192.168.1.1
```

- f. 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.

```
S1(config)#line con 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#logging sync
S1(config-line)#
```

- g. Настройте каналы виртуального соединения для удаленного управления (vty), чтобы коммутатор разрешил доступ через Telnet. Если не настроить пароль VTY, будет невозможно подключиться к

```
S1(config-line)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#logging sync
```

коммутатору по протоколу Telnet.

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

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.

IP Configuration

☐ DHCP ☒ Static

| | |
|-----------------|---------------|
| IPv4 Address | 192.168.1.16 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.1.1 |
| DNS Server | 0.0.0.0 |

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.

- а. 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

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

- а. В командной строке компьютера PC-A с помощью утилиты ping проверьте связь сначала с адресом

PC-A.

```
C:\>ping 192.168.1.16

Pinging 192.168.1.16 with 32 bytes of data:

Reply from 192.168.1.16: bytes=32 time=14ms TTL=128
Reply from 192.168.1.16: bytes=32 time=16ms TTL=128
Reply from 192.168.1.16: bytes=32 time<1ms TTL=128
Reply from 192.168.1.16: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.16:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 16ms, Average = 7ms
```

- b. Из командной строки компьютера PC-A отправьте эхо-запрос на административный адрес интерфейса SVI коммутатора S1_ФАМИЛИЯ.

```
C:\>ping 192.168.1.8

Pinging 192.168.1.8 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.8: bytes=32 time<1ms TTL=255
Reply from 192.168.1.8: bytes=32 time<1ms TTL=255
Reply from 192.168.1.8: bytes=32 time=2ms TTL=255

Ping statistics for 192.168.1.8:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

Поскольку компьютеру PC-A нужно преобразовать MAC-адрес коммутатора S1_ФАМИЛИЯ с помощью ARP, время ожидания передачи первого пакета может истечь. Если эхо-запрос не удастся, 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.

- Откройте Tera Term или другую программу эмуляции терминала с возможностью Telnet.
- Выберите сервер Telnet и укажите адрес управления SVI для подключения к S1_ФАМИЛИЯ. Пароль: **cisco**.
- После ввода пароля **cisco** вы окажетесь в командной строке пользовательского режима. Войдите в привилегированный режим EXEC, используя пароль **class**.
- Сохраните конфигурацию.

```
C:\>telnet 192.168.1.8
Trying 192.168.1.8 ...Openez parola nelza

User Access Verification

Password:
S1>en
Password:
S1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
S1#exit

[Connection to 192.168.1.8 closed by foreign host]
C:\>
```

- e. 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 MAC-адрес 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 MAC-адреса, полученные коммутатором.

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

```
S1_Daurbekov#show mac ad
Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
6       00d0.ffc9.49a7   DYNAMIC   Fa0/6
S1_Daurbekov#
```

Сколько динамических адресов присутствует? - 1

Сколько MAC-адресов имеется в общей сложности? - 1

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

| FastEthernet0 | |
|---------------|---|
| Port Status | <input checked="" type="checkbox"/> On |
| Bandwidth | <input type="radio"/> 100 Mbps <input type="radio"/> 10 Mbps <input checked="" type="checkbox"/> Auto |
| Duplex | <input type="radio"/> Half Duplex <input checked="" type="radio"/> Full Duplex <input checked="" type="checkbox"/> Auto |
| MAC Address | <input type="text" value="00D0.FFC9.49A7"/> |

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

а. Отобразите параметры таблицы MAC-адресов.

```
S1_ФАМИЛИЯ# show mac address-table ?
S1_Daurbekov#show mac ad ?
dynamic      dynamic entry type
interfaces   interface entry type
static       static entry type
<cr>
S1_Daurbekov#show mac ad |
```

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

- b. Введите команду **show mac address-table dynamic**, чтобы отобразить только те MAC-адреса,

```
S1_Daurbekov#show mac ad dyn
Mac Address Table
-----
Vlan    Mac Address      Type        Ports
----    -
6       00d0.ffc9.49a7   DYNAMIC     Fa0/6
```

которые были получены динамически. S1_Daurbekov#

Сколько динамических адресов присутствует? - 1

- c. 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.

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

```
S1_Daurbekov#clear mac ad
S1_Daurbekov#show mac ad
Mac Address Table
-----
Vlan    Mac Address      Type        Ports
----    -

```

MACадресов. S1_Daurbekov#

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

Сколько динамических адресов присутствует? - 0

- c. Снова изучите таблицу MAC-адресов.

Скорее всего, приложение, работающее на вашем ПК, уже отправило кадр из сетевого адаптера на коммутатор S1_ФАМИЛИЯ. Снова просмотрите таблицу MAC-адресов и выясните, был ли MACадрес 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

```
C:\>ping 192.168.1.8

Pinging 192.168.1.8 with 32 bytes of data:

Reply from 192.168.1.8: bytes=32 time=1ms TTL=255
Reply from 192.168.1.8: bytes=32 time<1ms TTL=255
Reply from 192.168.1.8: bytes=32 time<1ms TTL=255
Reply from 192.168.1.8: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

просмотра таблицы MAC-адресов.

```
S1_Daurbekov#show mac ad
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
6       00d0.ffc9.49a7   DYNAMIC Fa0/6
S1_Daurbekov#
```

- d. Назначьте статический MAC-адрес. Чтобы определить, к каким портам может подключиться узел, можно создать статическое сопоставление узлового MAC-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
```

- e. Выполните проверку записей в таблице MAC-адресов.

```
S1_Daurbekov(config)#mac address-table static 0050.56BE.6C89 vlan 6 interface fastethernet 0/6
S1_Daurbekov(config)#end
S1_Daurbekov#
%SYS-5-CONFIG_I: Configured from console by console

S1_Daurbekov#show mac ad
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
6       0050.56be.6c89   STATIC  Fa0/6
6       00d0.ffc9.49a7   DYNAMIC Fa0/6
S1_Daurbekov#
```

Сколько всего динамических адресов присутствует? - 1

Сколько статических адресов присутствует? - 1

- f. Удалите запись статического MAC. Перейдите в режим глобальной настройки и удалите команду.

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

```
S1_Daurbekov(config)#no mac address-table static 0050.56BE.6C89 vlan 6 interface fastethernet 0/6
S1_Daurbekov(config)#show mac ad
      ^
% Invalid input detected at '^' marker.

S1_Daurbekov(config)#exit
S1_Daurbekov#
%SYS-5-CONFIG_I: Configured from console by console

S1_Daurbekov#show mac ad
      Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
6       00d0.ffc9.49a7   DYNAMIC   Fa0/6
S1_Daurbekov#
```

- g. Убедитесь, что статический MAC-адрес был удален.

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

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 настройки 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.

1.