

Лабораторная работа

Настройка основных параметров коммутатора

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
S1	VLAN 1	192.168.1.253	255.255.255.0
S2	VLAN 1	192.168.1.254	255.255.255.0
PC1	Сетевая интерфейсная плата	192.168.1.1	255.255.255.0
PC2	Сетевая интерфейсная плата	192.168.1.2	255.255.255.0

Задачи

Часть 1. Проверка конфигурации по умолчанию на коммутаторе

Часть 2. Настройка основных параметров коммутатора S1

Часть 3. Настройка коммутатора S2

Часть 4. Настройка компьютеров

Часть 5. Настройка виртуального интерфейса коммутатора для возможности удаленной настройки

Общие сведения

В этой лабораторной необходимо настроить основные параметры конфигурации коммутатора, обеспечить безопасный доступ с помощью пароля к интерфейсу командной строки (CLI) и настроить сообщения для входящих в систему пользователей. Также требуется, настроить IP-адреса виртуальных интерфейсов на коммутаторах и сетевых интерфейсных плат на компьютерах. После завершения настройки необходимо выполнить проверку конфигурации, используя различные форматы команды **show**, а также команду **ping** для проверки соединений между устройствами.

Часть 1. Проверка конфигурации по умолчанию

Шаг 1. Переключитесь в привилегированный режим.

Привилегированный режим предоставляет доступ ко всем командам **IOS**. Т. к. многие команды привилегированного режима задают важные параметры работы устройств, для предотвращения несанкционированного доступа переключение в привилегированный режим должно быть защищено паролем.

Набор команд привилегированного режима включает в себя команды, доступные в пользовательском режиме, и множество дополнительных команд, а также команду **configure**, обеспечивающую доступ к режимам конфигурации.

а. Выберите коммутатор **S1** и перейдите на вкладку **CLI**. Нажмите на

клавиатуре **Ввод**.

b. Переключитесь в привилегированный режим:

```
Switch>enable
```

```
Switch#
```

Обратите внимание, что изменилось приглашение командной строки.

Шаг 2. Изучите текущую конфигурацию коммутатора.

a. Введите команду:

```
Switch#show running-config
```

Сколько интерфейсов **Fast Ethernet** у коммутатора?

24

Сколько интерфейсов **Gigabit Ethernet** у коммутатора?

2

Каковы возможные диапазоны номеров линий виртуального терминала **VTY (Virtual Teletype)**?

0m 0 до 15

b. Какой командой можно вывести текущее содержимое энергонезависимого ОЗУ (**NVRAM**)?

show start сокращенно или можно show startup-config

c. Введите эту команду. Почему коммутатор отобразил сообщение **startup-config is not present?**

Это сообщение появляется потому, что файл конфигурации еще не был сохранен из оперативной памяти (Running-config) в Startup-config.

Часть 2. Настройка основных параметров коммутатора

Шаг 1. Присвойте коммутатору имя.

Настройка параметров коммутатора требует переключения между режимами интерфейса командной строки. Обратите внимание, как изменяется приглашение командной строки при переключении режимов интерфейса командной строки.

```
Switch#configure terminal
Switch(config)#hostname S1
S1(config)# exit
S1#
```

Шаг 2. Настройте безопасный доступ по консольному подключению.

Для безопасного доступа по консольному подключению переключитесь в режим настройки линии и установите пароль **letmein** для доступа по консольному подключению.

```
S1#configure terminal
```

В окне командной строки введите следующие команды настройки.

```
S1(config)#line console 0
S1(config-line)#password letmein
S1(config-line)#login
S1(config-line)#exit
S1(config)#exit
S1#
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

В конце ввода нажмите на клавиатуре сочетание **CNTL/Z**.

Для чего необходима команда **login**?

чтобы коммутатор запрашивал пароль при подключении пользователя

Шаг 3. Убедитесь, что доступ по консольному подключению защищен.

Переключитесь из привилегированного режима и убедитесь, что доступ по консольному подключению защищен паролем.

```
S1#exit
```

```
S1 con0 is now available
Press RETURN to get started.
User Access Verification
```

```
Password:
```

```
S1>
```

Примечание. Если коммутатор не запрашивает ввод пароля при консольном подключении, значит, команда **login** не была введена в Шаге 2.

Шаг 4. Настройте безопасный доступ к привилегированному режиму.

Задайте пароль **c1\$c0** для доступа к привилегированному режиму.

Примечание. Символ **0** в **c1\$c0** — это цифра ноль, а не заглавная буква **O**.

```
S1>enable
S1#configure terminal
S1(config)#enable password c1$c0
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

Шаг 5. Убедитесь, что доступ к привилегированному режиму защищен.

a. Введите команду **exit** еще раз, чтобы переключиться из привилегированного режима.

b. Будет предложено ввести пароль для доступа к консольному подключению, который был задан в Шаге 2.

```
User Access Verification
Password:
```

c. Введите этот пароль, чтобы войти в пользовательский режим интерфейса командной строки.

d. Введите команду для переключения в привилегированный режим.

e. Введите пароль **c1\$c0**, который был установлен для ограничения доступа к привилегированному режиму.

```
Password:
S1#
```

f. Изучите содержимое файла текущей конфигурации:

```
S1#show running-config
```

Можно увидеть, что пароли для консольного подключения и привилегированного режима отображаются в виде простого текста. Это представляет потенциальную угрозу безопасности, если кто-то увидит их на вашем экране или получит доступ к файлам конфигурации, хранящимся в резервной копии.

Шаг 6. Установите зашифрованный пароль для доступа к привилегированному режиму.

С помощью команды **enable secret** замените пароль для доступа к привилегированному режиму новым зашифрованным паролем **itsasecret**.

```
S1#config t
S1(config)#enable secret itsasecret
S1(config)#exit
S1#
```

Примечание. Если в коммутаторе установлены оба пароля для доступа к привилегированному режиму, для переключения в этот режим нужно ввести зашифрованный пароль, который был задан командой

enable secret.

Шаг 7. Убедитесь в том, что зашифрованный пароль добавлен в файл конфигурации.

Введите команду **show running-config**, чтобы убедиться, что новый зашифрованный пароль, заданный командой **enable secret** добавлен в файл конфигурации.

Примечание. Команду **show running-config** можно сократить до **S1#show run**

Как отображается зашифрованный пароль, заданный командой **enable secret**? Почему?

Пароль представлен в виде хеш-строки: 5 \$1\$mERr\$ILwq/b7kc.7X/ejA4Aosn0
enable secret использует алгоритм одностороннего хеширования. Это сделано для обеспечения безопасности. Цифра 5 перед хешем указывает на тип используемого алгоритма шифрования.

Шаг 8. Зашифруйте пароли на доступ к консольному подключению и привилегированному режиму.

В шаге 7 было видно, что пароль, заданный командой **enable secret** зашифрован, а пароли, заданные командами **enable** и **console** хранятся в виде простого текста. Зашифруйте эти пароли:

```
S1#config t
S1(config)#service password-encryption
S1(config)#exit
```

Если после этого изменить на коммутаторе пароли на доступ к консольному подключению и привилегированному режиму, они будут храниться в файле конфигурации в виде простого текста или в зашифрованном виде? Дайте пояснение.

Если после ввода команды **service password-encryption** изменить пароли, они будут храниться в файле конфигурации в зашифрованном виде. Команда **service password-encryption** запускает процесс шифрования для всех текущих и будущих паролей, которые изначально хранятся в виде текста

Шаг 9. Настройте баннер MOTD (сообщения дня).

В системе команд **Cisco IOS** есть команда, позволяющая настроить сообщение (сообщением дня или баннером **MOTD (Message Of The Day)**), которое будут видеть пользователи, получающие доступ к интерфейсу командной строки на устройстве. Текст баннера заключится в двойные кавычки или используется разделитель, отличный от любого символа в строке **MOTD**.

```
S1#config t
S1(config)#banner motd "This is a secure system.
Authorized Access Only!" (Authorized access only.
Violators will be prosecuted to the full extent of
the law.)
S1(config)# exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

Когда будет отображаться баннер **MOTD**?

При каждой попытке входа в систему через интерфейс командной строки до ввода пароля

Почему на всех устройствах обязательно должен быть баннер **MOTD**?

В юридических целях – для официального предупреждения о том, что доступ разрешен только авторизованным пользователям, что важно при преследовании нарушителей по закону

Шаг 10. Проверьте файл конфигурации и сохраните в NVRAM.

a. Проверьте правильность текущей конфигурации с помощью команды **show run**.

b. Сохраните файл конфигурации.

Базовая настройка коммутатора завершена. Сделайте резервную копию файла конфигурации в **NVRAM** и убедитесь, что внесенные изменения сохраняются при перезагрузке системы или отключении питания.

```
S1#copy running-config startup-config
Destination filename [startup-config]?[Enter]
Building configuration...
[OK]
```

Какая самая короткая версия команды **copy running-config startup-config**?

copy run start

c. Изучите содержимое файла загрузочной конфигурации.

Какая команда отображает содержимое **NVRAM**?

sh start

Все ли выполненные настройки были записаны в файл загрузочной конфигурации?

Да, все настройки (имя хоста MagomedovMS1, пароли, баннер и настройки шифрования) теперь записаны в файл загрузочной конфигурации.

Часть 3. Настройка коммутатора S2

a. Настройте коммутатор S2, используя параметры:

Имя устройства: S2

Пароль для доступа к консольному подключению: letmein

Пароль для доступа к привилегированному режиму: c1\$c0,
зашифрованный пароль для доступа к привилегированному режиму:
itsasecret.

Баннер: (см. коммутатор S1).

b. Зашифруйте все пароли.

c. Проверьте правильность конфигурации.

d. Сохраните файл конфигурации, чтобы предотвратить его потерю в случае отключения питания коммутатора.

Часть 4. Настройка компьютеров

Настройте IP-адреса для сетевых интерфейсных плат компьютеров PC1 и PC2.

Шаг 1. Настройте IP-адреса для компьютеров.

- Выделите компьютер PC1 и выберите вкладку Desktop.
- Выберите значок IP Configuration (Настройка IP-адресов). В Таблице адресации (см. выше) можно увидеть, что интерфейсной плате компьютера PC1 присвоен IP-адрес 192.168.1.1 и маска подсети 255.255.255.0. Установите эти значения для компьютера PC1 в окне IP Configuration. Закройте окно IP Configuration.
- Повторите шаги 1а и 1б для компьютера PC2.

Шаг 2. Проверьте связь между оконечными устройствами (компьютерами PC1 и PC2).

- Выделите компьютер PC1. На вкладке Desktop выберите значок Command Prompt (Командная строка).
- В окне командной строки введите команду ping с IP-адресом компьютера PC2 и нажмите на клавиатуре ВВОД.

```
Packet Tracer PC Command Line 1.0  
PC>ping 192.168.1.2
```

- Выберите компьютер PC2. На вкладке Desktop выберите значок Command Prompt.
- В окне командной строки введите команду ping с IP-адресом компьютера PC1 и нажмите на клавиатуре ВВОД.

```
Packet Tracer PC Command Line 1.0  
PC>ping 192.168.1.1
```

Есть ли связь между оконечными устройствами?

связь между оконечными устройствами установлена успешно 0% потерь

Шаг 3. Проверьте связь с коммутаторами.

- Выделите компьютер PC1. На вкладке Desktop выберите значок Command Prompt.
- В окне командной строки введите команду ping с IP-адресом виртуального интерфейса коммутатора S1 и нажмите клавишу ВВОД.

```
Packet Tracer PC Command Line 1.0  
PC>ping 192.168.1.253
```

Есть ли связь с виртуальным интерфейсом коммутатора S1?

Объясните полученный результат.

Нет, устойчивая связь отсутствует первый пакет получил ответ «Request timed out» а последующие пакеты показали наличие связи. Однако для полноценной работы интерфейса управления требуется его предварительная настройка

Часть 5. Настройка интерфейса управления коммутатором

Настройте IP-адреса виртуальных интерфейсов коммутаторов S1 и S2.

Шаг 1. Настройте IP-адрес виртуального интерфейса коммутатора S1.

Коммутаторы являются **plug-and-play** устройствами. Т. е. их **необязательно настраивать для работы**. Коммутаторы пересылают данные между портами с использованием MAC-адресов.

Почему необходимо настраивать IP-адрес?

IP-адрес на коммутаторе надо настраивать для возможности удаленного управления устройством по сети. Без этого адреса невозможно подключиться к коммутатору для его настройки.

Чтобы настроить IP-адрес виртуального интерфейса на коммутаторе S1, используйте следующие команды.

```
S1#configure terminal
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.1.253 255.255.255.0
S1(config-if)#no shutdown
%LINEPROTO-5-UPDOWN: Line protocol on Interface
Vlan1, changed state to up
S1(config-if)#
S1(config-if)#exit
S1#
```

Введите построчно команды настройки. В конце нажмите на клавиатуре **CNTL/Z**.

Зачем необходима команда **no shutdown**?

Команда **no shutdown** необходима для того, чтобы перевести интерфейс в активное состояние.

Шаг 2. Настройте IP-адрес виртуального интерфейса коммутатора S2.

Используя данные из Таблицы адресации, настройте IP-адрес виртуального интерфейса коммутатора S2.

Шаг 3. Проверьте настройки IP-адресов виртуальных интерфейсов на коммутаторах S1 и S2.

Команда **show ip interface brief** выводит сведения о состоянии всех портов и интерфейсов (а также об IP-адресе) коммутатора. Можно также использовать команду **show running-config**.

Шаг 4. Сохраните настройки коммутаторов S1 и S2 в NVRAM.

Какая команда сохраняет файл конфигурации из RAM в NVRAM?

copy running-config startup-config

Шаг 5. Проверьте соединение.

Соединение можно проверить с помощью команды **ping**. Очень важно, чтобы соединения были между всеми устройствами сети. В случае

неудачи необходимо устранить проблему. Проверьте связь между оконечными (компьютеры PC1 и PC2) и промежуточными устройствами (коммутаторы S1 и S2).

- a. Выделите компьютер PC1 и выберите вкладку Desktop.
- b. Выберите значок Command Prompt.
- c. Используя команду ping, проверьте связь с компьютером PC2.
- d. Используя команду ping, проверьте связь с виртуальным интерфейсом коммутатора S1.
- e. Используя команду ping, проверьте связь с виртуальным интерфейсом коммутатора S2.

Примечание. Аналогичные команды ping используйте и в интерфейсе командной строки на компьютере PC2.

Все проверки должны быть пройдены успешно. Если результат первой проверки 80 %, повторите попытку. Результат должен быть 100 %. Позже вы узнаете, почему первая проверка иногда завершается неудачно. Если связь с устройствами отсутствует, проверьте конфигурацию на наличие ошибок.

Примечание. В окне PT Activity нажмите кнопку Check Results, чтобы увидеть результаты выполненной работы.