Лабораторная работа. Использование интерфейса командной строки (CLI) для сбора сведений о сетевых устройствах

Топология

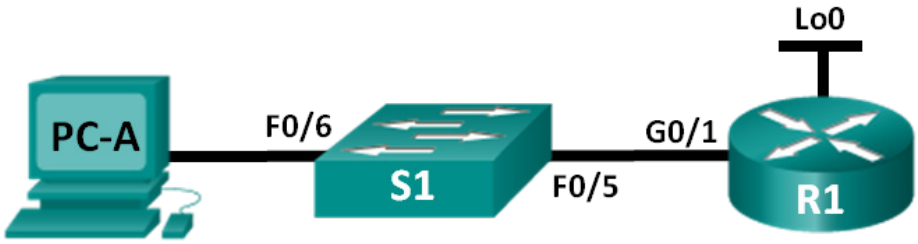


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	Недоступно
	Lo0	209.165.200.225	255.255.255.224	Недоступно
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
ПК-A	Сетевой адаптер	192.168.1.3	255.255.255.0	192.168.1.1

Задачи

Часть 1: настройте топологию и инициализацию устройств

- Настройте оборудование в соответствии с топологией сети.
- Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Часть 2: настройте параметры устройств и проверьте надёжность подключения

- Присвойте статический IP-адрес маршрутизатору PC-A NIC.
- Настройте базовые параметры на маршрутизаторе R1.
- Выполните базовую настройку коммутатора S1.
- Проверьте подключение к сети.

Часть 3: соберите сведения о сетевых устройствах

- Соберите информацию на R1 с помощью команд IOS CLI.
- Соберите информацию на S1 с помощью команд IOS CLI.
- Соберите информацию на PC-A с помощью команды CLI.

Исходные данные/сценарий

Одна из наиболее важных задач, выполняемых специалистами в области вычислительных сетей, состоит в документировании работы сети. Наличие документации, относящейся к IP-адресам, номерам моделей, версиями IOS, используемым портам и результатам проверки безопасности, имеет большое значение при поиске и устранении неполадок в работе сети.

В этой лабораторной работе вы построите небольшую вычислительную сеть, выполните настройку устройств, добавите некоторые основные средства защиты, а затем создадите документацию для полученной конфигурации, выполняя на маршрутизаторе, коммутаторе и ПК различные команды для сбора требуемой информации.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблице сводной информации об интерфейсах маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не имеют загрузочной конфигурации. Если вы не уверены в этом, обратитесь к преподавателю.

Необходимые ресурсы:

- 1 маршрутизатор (Cisco 1941 с универсальным образом M3 версии CISCO IOS 15.2(4) или аналогичный)
- 1 коммутатор (серия Cisco 2960, с программным обеспечением Cisco IOS версии 15.0(2), образ lanbasek9 или аналогичный)
- 1 ПК (под управлением Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Настройка топологии и инициализация устройств

В первой части лабораторной работы вам предстоит создать топологию сети, при необходимости удалить все настройки и настроить основные параметры для маршрутизатора и коммутатора.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

a. Подключите устройства, как показано в топологии, и подсоедините необходимые кабели.

b. Включите все устройства в топологии.

Шаг 2: Выполните запуск и перезагрузку маршрутизатора и коммутатора.

Часть 2: Настройка устройств и проверка подключения

Во второй части лабораторной работы вам предстоит создать топологию сети и настроить основные параметры для маршрутизатора и коммутатора. Имена и адреса устройств можно найти в топологии и таблице адресации в начале этой лабораторной работы.

Примечание. В приложении A приведены сведения о конфигурации для выполнения шагов в части 2. Постарайтесь выполнить часть 2, не пользуясь приложением.

Шаг 1: Настройте IPv4-адрес на ПК.

На основе таблицы адресации настройте адрес IPv4, маску подсети и адрес шлюза по умолчанию для PC-A.

Шаг 2: Настройте маршрутизатор.

Если возникли трудности при выполнении шага 2, обратитесь к приложению A.

a. Подключите консоль к маршрутизатору и войдите в привилегированный режим EXEC.

b. Установите на маршрутизаторе правильные время и дату.

c. Войдите в режим глобальной конфигурации.

   1) На основе топологии и таблицы адресации присвойте маршрутизатору имя устройства.

   2) Отключите поиск DNS.

   3) Создайте баннер MOTD с предупреждением о запрете несанкционированного доступа к устройству.

   4) Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.

   5) Назначьте **cisco** в качестве пароля консоли и активируйте использование имени для входа при получении доступа к консоли.

   6) Зашифруйте все открытые пароли.

   7) Для доступа с использованием SSH создайте имя домена **cisco.com**.

   8) Для доступа с использованием SSH создайте пользователя **admin** с секретным паролем **cisco**.

   9) Создайте ключ RSA. Для числа битов используйте значение **512**.

d. Настройте доступ к каналу vty.

   1) Для аутентификации при использовании SSH настройте локальную базу данных.

   2) Активируйте SSH только для доступа с использованием имени для входа.

e. Вернитесь в режим глобальной конфигурации.

   1) Создайте интерфейс Loopback 0 и присвойте IP-адрес на основе таблицы адресации.

   2) Настройте и активируйте интерфейс G0/1 на маршрутизаторе.

   3) Настройте описания интерфейсов для G0/1 и L0.

   4) Сохраните файл текущей конфигурации в файле загрузочной конфигурации.

Шаг 3: Настройте коммутатор.

Если возникли трудности при выполнении шага 3, обратитесь к приложению A.

a. Подключите консоль к коммутатору и войдите в привилегированный режим EXEC.

b. Установите на коммутаторе правильные время и дату.

c. Войдите в режим глобальной конфигурации.

   1) На основе топологии и таблицы адресации присвойте коммутатору имя устройства.

   2) Отключите поиск DNS.

   3) Создайте баннер MOTD с предупреждением о запрете несанкционированного доступа к устройству.

   4) Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.

5) Зашифруйте все открытые пароли.
6) Для доступа с использованием SSH создайте имя домена **cisco.com**.
7) Для доступа с использованием SSH создайте пользователя **admin** с секретным паролем **cisco**.
8) Создайте ключ RSA. Для числа битов используйте значение **512**.
9) На основе топологии и таблицы адресации создайте и активируйте на коммутаторе IP-адрес.
10) Установите на коммутаторе шлюз по умолчанию.
11) Назначьте **cisco** в качестве пароля консоли и активируйте использование имени для входа при получении доступа к консоли.

d. Настройте доступ к каналу vty.
1) Для аутентификации при использовании SSH настройте локальную базу данных.
2) Активируйте SSH только для доступа с использованием имени для входа.
3) Войдите в соответствующий режим для настройки описаний интерфейсов для F0/5 и F0/6.
4) Сохраните файл текущей конфигурации в файле загрузочной конфигурации.

Шаг 4: Проверьте подключение к сети.

a. Из командной строки на компьютере PC-A выполните команду ping для IP-адреса коммутатора S1 в сети VLAN 1. Если команды ping дали неудовлетворительный результат, отыщите ошибки в физических и логических настройках и выполните требуемые исправления.

b. Из командной строки на компьютере PC-A выполните команду ping для IP-адреса шлюза по умолчанию на маршрутизаторе R1. Если команды ping дали неудовлетворительный результат, отыщите ошибки в физических и логических настройках и выполните требуемые исправления.

c. Из командной строки на компьютере PC-A выполните команду ping для IP-адреса интерфейса закольцовывания на маршрутизаторе R1. Если команды ping дали неудовлетворительный результат, отыщите ошибки в физических и логических настройках и выполните требуемые исправления.

d. Снова подключите консоль к коммутатору и выполните команду ping для IP-адреса шлюза G0/1 на маршрутизаторе R1. Если команды ping дали неудовлетворительный результат, отыщите ошибки в физических и логических настройках и выполните требуемые исправления.

Часть 3: Сбор сведений о сетевых устройствах

В части 3 вы будете использовать различные команды для сбора сведений о сетевых устройствах и некоторых рабочих характеристик. Документация со сведениями о вычислительной сети является очень важной составляющей управления сетью. Важно документировать как физическую, так и логическую топологию, а также проверять модели платформ и версии IOS сетевых устройств. Специалистам по вычислительным сетям важно знать соответствующие команды для сбора сведений о сети.

Шаг 1: Соберите информацию на R1 с помощью команд IOS.

Одним из важнейших основных действий является сбор сведений о физическом устройстве наряду со сведениями об операционной системе.

a. Примените соответствующую команду для выявления следующих данных.

Модель маршрутизатора:

Версия IOS:

Всего ОЗУ:

Всего ОЗУ:

Всего флэш-памяти: _____

Файл-образ IOS:

Реестр конфигурации:

Технологический пакет:

Какая команда используется для сбора информации?

b. Для отображения сводки с важными сведениями об интерфейсах маршрутизаторов используйте соответствующую команду. Ниже запишите команду и полученные результаты.

Примечание. Запишите только те интерфейсы, у которых есть IP-адреса.

c. Примените соответствующую команду для отображения таблицы маршрутизации. Ниже запишите команду и полученные результаты.

d. Какую команду следует использовать для отображения таблицы сопоставления адресов уровня 2 и уровня 3 на маршрутизаторе? Ниже запишите команду и полученные результаты.

e. Какую команду следует использовать для просмотра подробных сведений обо всех интерфейсах на маршрутизаторе или о конкретном интерфейсе? Ниже запишите команду.

f. Существует очень мощный протокол Cisco, работающий на уровне 2 модели OSI. Этот протокол облегчит получение схемы физических соединений устройств Cisco, а также определение номеров моделей и даже версий IOS и адресов IP. Какую команду или команды следует использовать на маршрутизаторе R1 для поиска информации о коммутаторе S1 для заполнения следующей таблицы?

Идентификатор устройства	Локальный интерфейс	Возможность настройки	Номер модели	Идентификатор удаленного порта	IP-адрес	Версия IOS

g. Простейшая проверка сетевых устройств осуществляется с помощью попытки подключиться к ним с использованием протокола telnet. Следует помнить, что Telnet не является безопасным протоколом. В большинстве случаев его не следует активировать. С помощью клиента Telnet, например Tera Term или PuTTY, попытайтесь посредством telnet подключиться к R1 с использованием IP-адреса шлюза по умолчанию. Полученные результаты запишите ниже.

h. С компьютера PC-A выполните проверку правильности работы SSH. Используя клиент SSH, например Tera Term или PuTTY, подключитесь посредством SSH к маршрутизатору R1 с компьютера PC-A. В случае получения сообщения с предупреждением об отличающемся ключе нажмите кнопку **Continue** («Продолжить»). Подключитесь с использованием соответствующего имени пользователя и пароля, созданных в части 2. Успешно ли был обработан эхо-запрос?

Различные пароли, настраиваемые на маршрутизаторе, должны быть надёжными и защищёными в максимально возможной степени.

Примечание. Пароли, используемые для нашей лабораторной работы (**cisco**и **class**) не соответствуют общепринятым требованиям для надёжных паролей. Эти пароли используются просто для удобства выполнения лабораторных работ. По умолчанию пароль консоли и все пароли канала vty явно отображаются в вашем файле конфигурации.

i. Убедитесь в том, что все ваши пароли в файле конфигурации зашифрованы. Ниже запишите команду и полученные результаты.

Команда:

Пароль консоли зашифрован?

Пароль SSH зашифрован?

Шаг 2: Соберите информацию на S1 с помощью команд IOS.

Многие из команд, используемых на маршрутизаторе R1, можно применять также на коммутаторе. Однако между некоторыми из этих команд существуют определённые различия.

a. Примените соответствующую команду для выявления следующих данных.

Модель коммутатора:

Версия IOS:

Всего RAM:

Файл-образ IOS:

Какая команда используется для сбора информации?

b. Для отображения сводки с важными сведениями об интерфейсах коммутаторов используйте соответствующую команду. Ниже запишите команду и полученные результаты.

Примечание. Укажите только активные интерфейсы.

c. Примените соответствующую команду для отображения таблицы MAC-адресов коммутатора. В отведённом ниже месте запишите только MAC-адреса динамического типа.

d. Убедитесь в том, что на коммутаторе S1 отключён доступ к VTY по Telnet. С помощью клиента Telnet, например Tera Term или PuTTY, попытайтесь посредством telnet подключиться к S1 с использованием адреса 192.168.1.11. Полученные результаты запишите ниже.

e. С компьютера PC-A выполните проверку правильности работы SSH. Используя клиент SSH, например Tera Term или PuTTY, подключитесь посредством SSH к коммутатору S1 с компьютера PC-A. В случае получения сообщения с предупреждением об отличающемся ключе нажмите кнопку **Continue** («Продолжить»). Подключитесь с использованием соответствующего имени пользователя и пароля. Успешно ли был обработан эхо-запрос?

f. Заполните идущую ниже таблицу сведениями о маршрутизаторе R1, используя для этого соответствующую команду или команды, применяемые на коммутаторе S1.

Идентификатор устройства	Локальный интерфейс	Возможность настройки	Номер модели	Идентификатор удаленного порта	IP-адрес	Версия IOS

g. Убедитесь в том, что все ваши пароли в файле конфигурации зашифрованы. Ниже запишите команду и полученные результаты.

Команда:

Пароль консоли зашифрован?

Шаг 3: Соберите сведения о компьютере PC-A.

С помощью различных команд служебных программ Windows вы сможете собрать сведения о PC-A.

a. В командной строке PC-A запустите на выполнение команду **ipconfig /all** и запишите ниже полученные результаты.

   Укажите IP-адрес PC-A.

   Укажите маску подсети PC-A.

   Укажите адрес шлюза по умолчанию для PC-A.

   Укажите MAC-адрес компьютера PC-A.

b. Выполните соответствующую команду для проверки связи стека протокола TCP/IP с сетевой интерфейсной платой. Какую команду вы использовали?

c. Проверьте интерфейс закольцовывания маршрутизатора R1, выполнив команду Ping из командной строки компьютера PC-A. Успешно ли выполнен эхо-запрос?

d. Выполните соответствующую команду на компьютере PC-A, чтобы получить список переходов по маршрутизаторам для пакетов, отправленных с PC-A на интерфейс закольцовывания маршрутизатора R1. Ниже запишите команду и полученный результат. Какую команду вы использовали?

e. Выполните соответствующую команду на компьютере PC-A, чтобы найти схему сопоставления адресов уровня 2 и уровня 3, используемую на вашей сетевой интерфейсной плате. Ниже запишите свои ответы. Запишите только ответы, относящиеся к сети 192.168.1.0/24. Какую команду вы использовали?

Вопросы на закрепление

Почему важно документировать сведения о сетевых устройствах?

Сводная таблица интерфейсов маршрутизатора

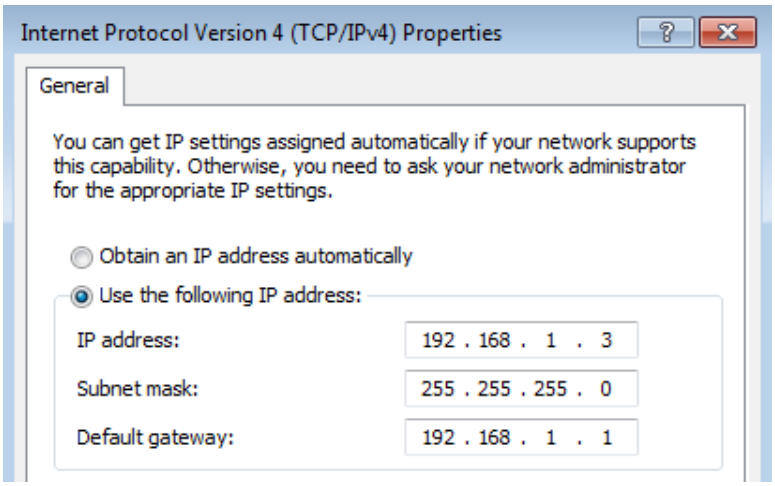
Сводка по интерфейсам маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet №1**	**Интерфейс Ethernet №2**	**Последовательный интерфейс №1**	**Последовательный интерфейс №2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы для определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех комбинаций настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В эту таблицу интерфейсов не включены какие-либо иные типы интерфейсов, даже если они присутствуют на каком-либо определённом маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.

Приложение A. Сведения о конфигурации для выполнения шагов в части 2

Шаг 1. Настройка IPv4-адреса на ПК.

В начале выполнения этой лабораторной работы выполните на основе таблицы адресации настройку адреса IPv4, маски подсети и адреса шлюза по умолчанию для PC-A.



Шаг 2. Настройка маршрутизатора.

a. Подключите консоль к маршрутизатору и войдите в привилегированный режим EXEC.

```
Router>enable
Router#
```

b. Установите на маршрутизаторе правильные время и дату.

```
Router# clock set 10:40:30 6 February 2013
Router#
```

c. Войдите в режим глобальной конфигурации.

```
Router# config t
Router(config)#
```

1) Назначьте маршрутизатору имя узла. В качестве инструкций используйте топологию и таблицу адресации.

```
Router(config)# hostname R1
R1(config)#
```

2) Отключите поиск DNS.

```
R1(config)# no ip domain-lookup
```

3) Создайте баннер MOTD с предупреждением о запрете несанкционированного доступа к устройству.

```
R1(config)# banner motd #Warning! Unauthorized Access is Prohibited!#
```

4) Назначьте **class**в качестве зашифрованного пароля привилегированного режима EXEC.

```
R1(config)# enable secret class
```

5) Назначьте **cisco**в качестве пароля консоли и активируйте использование имени для входа при получении доступа к консоли.

```
R1(config)# line con 0
R1(config-line)# password cisco
R1(config-line)# login
```

6) Зашифруйте все открытые пароли.

```
R1(config)# service password-encryption
```

7) Для доступа с использованием SSH создайте имя домена **cisco.com**.

```
R1(config)# ip domain-name cisco.com
```

8) Для доступа с использованием SSH создайте пользователя **admin** с секретным паролем **cisco**.

```
R1(config)# username admin secret cisco
```

9) Создайте ключ RSA. Для числа битов используйте значение **512**.

```
R1(config)# crypto key generate rsa modulus 512
```

d. Настройте доступ к каналу vty.

1) Для аутентификации при использовании SSH настройте локальную базу данных.

```
R1(config)#line vty 0 4
R1(config-line)# login local
```

2) Активируйте SSH только для доступа с использованием имени для входа.

```
R1(config-line)# transport input ssh
```

e. Вернитесь в режим глобальной конфигурации.

```
R1(config-line)# exit
```

1) Создайте интерфейс Loopback 0 и присвойте IP-адрес на основе таблицы адресации.

```
R1(config)# interface loopback 0
R1(config-if)# ip address 209.165.200.225 255.255.255.224
```

2) Настройте и активируйте интерфейс G0/1 на маршрутизаторе.

```
R1(config-if)# int g0/1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shut
```

3) Настройте описания интерфейсов для G0/1 и L0.

```
R1(config-if)# description Connected to LAN
R1(config-if)# int lo0
R1(config-if)# description Emulate ISP Connection
```

4) Сохраните файл текущей конфигурации в файле загрузочной конфигурации.

```
R1(config-if)# end
R1# copy run start
```

Шаг 3. Настройка коммутатора.

a. Подключите консоль к коммутатору и войдите в привилегированный режим EXEC.

```
Switch>enable
Switch#
```

b. Установите на коммутаторе правильные время и дату.

```
Switch# clock set 10:52:30 6 February 2013
```

c. Войдите в режим глобальной конфигурации.

```
Switch# config t
```

1) На основе топологии и таблицы адресации присвойте коммутатору имя узла.

```
Switch(config)# hostname S1
```

2) Отключите поиск DNS.

```
S1(config)# no ip domain-lookup
```

3) Создайте баннер MOTD с предупреждением о запрете несанкционированного доступа к устройству.

```
S1(config)# banner motd #Warning! Unauthorized access is prohibited!#
```

4) Назначьте **class**в качестве зашифрованного пароля привилегированного режима EXEC.

```
S1(config)# enable secret class
```

5) Зашифруйте незашифрованные пароли.

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

6) Для доступа с использованием SSH создайте имя домена **cisco.com**.

```
S1(config)# ip domain-name cisco.com
```

7) Для доступа с использованием SSH создайте пользователя **admin** с секретным паролем **cisco**.

```
S1(config)# username admin secret cisco
```

8) Создайте ключ RSA. Для числа битов используйте значение **512**.

```
S1(config)# crypto key generate rsa modulus 512
```

9) На основе топологии и таблицы адресации создайте и активируйте на коммутаторе IP-адрес.

```
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.11 255.255.255.0
S1(config-if)# no shut
```

10) Установите на коммутаторе шлюз по умолчанию.

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

11) Назначьте **cisco** в качестве пароля консоли и активируйте использование имени для входа при получении доступа к консоли.

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

d. Настройте доступ к каналу vty.

1) Для аутентификации при использовании SSH настройте локальную базу данных.

```
S1(config-line)# line vty 0 15
S1(config-line)# login local
```

2) Активируйте SSH только для доступа с использованием имени для входа.

```
S1(config-line)# transport input ssh
```

3) Войдите в соответствующий режим для настройки описаний интерфейсов для F0/5 и F0/6.

```
S1(config-line)# int f0/5
S1(config-if)# description Connected to R1
S1(config-if)# int f0/6
S1(config-if)# description Connected to PC-A
```

4) Сохраните файл текущей конфигурации в файле загрузочной конфигурации.

```
S1(config-if)# end
S1# copy run start
```