

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

Топология

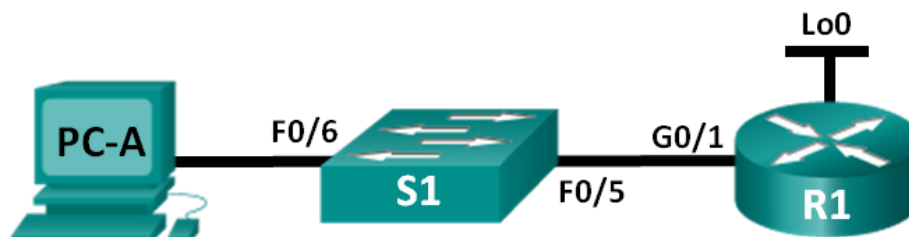


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	—
	Lo0	209.165.200.225	255.255.255.224	—
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Задачи

Часть 1. Настройка топологии и инициализация устройств

Часть 2. Настройка устройств и проверка подключения

Часть 3. Сбор сведений о сетевых устройствах

Общие сведения/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, версиям 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 сеть, выполните настройку устройств, добавьте некоторые основные средства защиты, а затем создадите документацию для полученной конфигурации, выполняя на маршрутизаторе, коммутаторе и компьютере различные команды для сбора требуемой информации.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интегрированными сервисами Cisco 1941 (ISR) под управлением Cisco IOS версии 15.2(4) M3 (образ universalk9). Также используются коммутаторы Cisco Catalyst 2960 с операционной системой Cisco IOS версии 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах. Точные идентификаторы интерфейсов см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что у всех маршрутизаторов и коммутаторов была удалена начальная конфигурация. Если вы не уверены, обратитесь к инструктору.

Необходимые ресурсы

- 1 маршрутизатор (Cisco 1941 с операционной системой Cisco IOS 15.2(4)M3 (универсальный образ) или аналогичная модель)
- 1 коммутатор (Cisco 2960 с ПО Cisco IOS версии 15.0(2) с образом lanbasek9 или аналогичная модель)
- 1 ПК (под управлением Windows 7 или 8 с программой эмуляции терминала, например, Tera Term)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты
- 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: Создайте сеть согласно топологии.

- а. Подключите устройства, показанные в топологии, и кабели соответствующим образом.
- б. Включите все устройства в топологии.

Шаг 2: Выполните инициализацию 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.

Шаг 1: Настройте IPv4-адрес на компьютере.

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

Шаг 2: Настройте маршрутизатор.

- а. Подключитесь к коммутатору с помощью консоли и войдите в привилегированный режим EXEC.
- б. Установите на маршрутизаторе правильное время и дату.
- в. Войдите в режим глобальной настройки.
 - 1) На основе топологии и таблицы адресации присвойте маршрутизатору имя устройства.

- 2) Отключите поиск DNS.
 - 3) Создайте баннер сообщения дня (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 включите доступ к консоли по паролю.
 - 6) Зашифруйте открытые пароли.
 - 7) Для доступа по протоколу SSH создайте имя домена **cisco.com**.
 - 8) Для доступа по протоколу SSH создайте пользователя **admin** с секретным паролем **cisco**.
 - 9) Создайте ключ RSA. Установите число бит **1024**.
- d. Настройте доступ к линии VTY.
- 1) Используйте локальную базу данных для аутентификации по протоколу SSH.
 - 2) Включите доступ к устройству только по SSH.
- e. Вернитесь в режим глобальной настройки.
- 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 текущую конфигурацию в файл загрузочной конфигурации.

Шаг 3: Настройте коммутатор.

- a. Подключитесь к коммутатору с помощью консоли и войдите в привилегированный режим EXEC.
 - b. Установите на коммутаторе правильные время и дату.
 - c. Войдите в режим глобальной настройки.
 - 1) На основе топологии и таблицы адресации присвойте коммутатору имя устройства.
 - 2) Отключите поиск DNS.
 - 3) Создайте баннер сообщения дня (MOTD) с предупреждением о запрете несанкционированного доступа к устройству.
 - 4) Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
 - 5) Зашифруйте открытые пароли.
 - 6) Для доступа по протоколу SSH создайте имя домена **cisco.com**.
 - 7) Для доступа по протоколу SSH создайте пользователя **admin** с секретным паролем **cisco**.
 - 8) Создайте ключ RSA. Установите число бит **1024**.
 - 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 включите доступ к консоли по паролю.
- d. Настройте доступ к линии VTY.
- 1) Используйте локальную базу данных для аутентификации по протоколу SSH.
 - 2) Активируйте SSH только для доступа по имени пользователя.
 - 3) Сохраните текущую конфигурацию в файл загрузочной конфигурации.

- е. Войдите в соответствующий режим для настройки описаний интерфейсов для F0/5 и F0/6.

Шаг 4: Проверьте подключение к сети.

- Из командной строки на компьютере PC-A отправьте команду ping на IP-адрес коммутатора S1 в сети VLAN 1. Если отправить команды ping не получилось, найдите ошибки в физических и логических конфигурациях и исправьте их.
- Из командной строки на компьютере PC-A отправьте команду ping на IP-адрес шлюза по умолчанию на маршрутизаторе R1. Если отправить команды ping не получилось, найдите ошибки в физических и логических конфигурациях и исправьте их.
- Из командной строки на компьютере PC-A отправьте команду ping на IP-адрес виртуального интерфейса loorback на маршрутизаторе R1. Если отправить команды ping не получилось, найдите ошибки в физических и логических конфигурациях и исправьте их.
- Снова подключите консоль к коммутатору и отправьте команду ping на IP-адрес G0/1 на маршрутизаторе R1. Если отправить команды ping не получилось, найдите ошибки в физических и логических конфигурациях и исправьте их.

Часть 3: Сбор сведений о сетевых устройствах

В третьей части вы будете использовать различные команды для сбора сведений о сетевых устройствах, а также отдельных характеристиках производительности. Документация со сведениями о 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: Выполните сбор информации на маршрутизаторе R1 с помощью команд IOS.

Одним из основных шагов является сбор сведений о физическом устройстве, а также об его операционной системе.

- а. Выполните соответствующую команду для получения следующей информации:

Модель маршрутизатора:

Версия IOS: 15.1(4)M4

Общий объем ОЗУ: 491520K/32768K

Общий объем NVRAM: 255K

Общий объем флэш-памяти: 249856K

Файл образа IOS: flash0:c1900-universalk9-mz.SPA.151-1.M4.bin

Регистр конфигурации: 0x2102

Технологический пакет: ipbaseek9

Какая команда использовалась для сбора информации?

`show version`

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

`show ip interface brief`

GigabitEthernet0/1 192.168.1.1 YES manual up up

Loopback0 209.165.200.225 YES manual up up

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

- с. Выполните соответствующую команду для отображения таблицы маршрутизации. Ниже запишите команду и полученные результаты.

show ip route

```

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, GigabitEthernet0/1
L    192.168.1.1/32 is directly connected, GigabitEthernet0/1
209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C    209.165.200.0/24 is directly connected, Loopback0
L    209.165.200.225/32 is directly connected, Loopback0

```

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

show arp

```

Internet 192.168.1.1      - 0030.F2AA.AC02 ARPA  GigabitEthernet0/1
Internet 192.168.1.3      17 0030.F223.32B9 ARPA  GigabitEthernet0/1
Internet 192.168.1.11     14 0009.7C63.D8A7 ARPA  GigabitEthernet0/1

```

- е. Какую команду следует использовать для просмотра подробных сведений обо всех интерфейсах на маршрутизаторе или о конкретном интерфейсе? Запишите команду ниже.

show interfaces

- ф. Компания Cisco разработала очень эффективный протокол, работающий на уровне 2 модели OSI. Этот протокол позволяет легко понять, как устройства Cisco подключены физически, а также определить номера моделей и даже версии IOS и IP-адресацию. Какую команду или команды следует использовать на маршрутизаторе R1 для получения информации о коммутаторе S1 для заполнения следующей таблицы? show cdp neighbors

Идентификатор устройства	Локальный интерфейс	Функциональные возможности	Номер модели	Идентификатор удаленного порта	IP-адрес	Версия IOS

- г. Простейшая проверка сетевых устройств осуществляется с помощью попытки подключиться к ним с использованием протокола telnet. Следует помнить, что Telnet — это незащищенный протокол. В большинстве случаев активировать его не следует. 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.

Trying 192.168.1.1 ...Open

[Connection to 192.168.1.1 closed by foreign host]

- h. Выполните проверку правильности работы протокола SSH с компьютера PC-A. С помощью клиента SSH, например, Tera Term или PuTTY, попытайтесь посредством SSH подключиться к R1 с PC-A. Если вы увидите предупреждение безопасности о несоответствии ключа, нажмите Continue (Продолжить). Подключитесь с использованием соответствующего имени пользователя и пароля, созданных в части 2. Удалось ли выполнить подключение?

Да

Различные пароли, настраиваемые на маршрутизаторе, должны быть максимально надежными и защищенными.

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

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

Команда: `show running-config`

Пароль консоли зашифрован? Да

Пароль SSH зашифрован? Да

Шаг 2: Выполните сбор информации на коммутаторе S1 с помощью команд IOS.

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

- a. Выполните соответствующую команду для получения следующей информации:

Модель коммутатора: C2960

Версия IOS: 12.2(25r)FX

Общий объем NVRAM: 21039K

Файл образа IOS: Не отображается в Packet Tracer.

Какая команда использовалась для сбора информации?

`show version`

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

Примечание. Укажите только активные интерфейсы.

`show ip interface brief`

FastEthernet0/5	unassigned	YES manual up	up
FastEthernet0/6	unassigned	YES manual up	up
Vlan1	192.168.1.11	YES manual up	up

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

`show mac-address-table`

1	0030.f2aa.ac02	DYNAMIC	Fa0/5
---	----------------	---------	-------

- d. Убедитесь в том, что на коммутаторе S1 отключен 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.

[Connection to 192.168.1.1 closed by foreign host]

- e. Выполните проверку правильности работы протокола SSH с компьютера PC-A. С помощью клиента SSH, например, Tera Term или PuTTY, попытайтесь посредством SSH подключиться к S1 с PC-A. Если вы видите предупреждение безопасности о несоответствии ключа, нажмите Continue (Продолжить). Подключитесь с использованием соответствующего имени пользователя и пароля. Удалось ли выполнить подключение?

Да

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

Идентификатор устройства	Локальный интерфейс	Функциональные возможности	Номер модели	Идентификатор удаленного порта	IP-адрес	Версия IOS
S1	Gig 0/1	S	2960	Fas 0/5	.11	12.2(25)FX

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

Команда: `show running-config`

Пароль консоли зашифрован? Да

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.

192.168.1.3

Укажите маску подсети PC-A.

255.255.255.0

Укажите адрес шлюза по умолчанию для PC-A.

192.168.1.1

Укажите MAC-адрес PC-A.

0030.F223.32B9

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

`ping 127.0.0.1`

- c. Проверьте виртуальный интерфейс loopback R1, отправив команду `ping` из командной строки компьютера PC-A. Получилось отправить команду?

Да

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

```
tracert 209.165.200.225
```

```
1 1 ms 0 ms 12 ms 209.165.200.225
```

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

```
arp -a
```

```
192.168.1.1      0030.f2aa.ac02    dynamic
192.168.1.11    0009.7c63.d8a7    dynamic
```

Вопросы для повторения

Почему важно документировать сведения о сетевых устройствах?

Это упрощает нахождение и устранение возникающих проблем и позволяет быстро восстановить работоспособность сети.

Сводная таблица по интерфейсам маршрутизаторов

Сводная таблица 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 определить конфигурацию маршрутизатора, можно посмотреть на интерфейсы и установить тип маршрутизатора и количество его интерфейсов. Перечислить все комбинации конфигураций для каждого класса маршрутизаторов невозможно. Эта таблица содержит идентификаторы для возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов на устройстве. Другие типы интерфейсов в таблице не представлены, хотя они могут присутствовать в данном конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это официальное сокращение, которое можно использовать в командах Cisco IOS для обозначения интерфейса.				