Гвоздков И.В.
Хорошенко С.В

ИНФОКОММУНИКАЦИОННЫЕ СИСТЕМЫ И СЕТИ

ЛАБОРАТОРНЫЙ ПРАКТИКУМ

САНКТ-ПЕТЕРБУРГ
2016

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

Федеральное государственное образовательное бюджетное
учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ
им. проф. М. А. БОНЧ-БРУЕВИЧА»

Гвоздков И.В.
Хорошенко С.В

ИНФОКОММУНИКАЦИОННЫЕ СИСТЕМЫ И СЕТИ

ЛАБОРАТОРНЫЙ ПРАКТИКУМ

СПб ГУТ)))

САНКТ-ПЕТЕРБУРГ
2016

УДК 621.391.24(77)
ББК 3287я73
И20

Рецензент

Рекомендовано к печати
Редакционно-издательским советом СПбГУТ

Гвоздков И.В. Хорошенко С.В

И 20 Инфокоммуникационные системы и сети : лабораторный практикум / Гвоздков И.В. Хорошенко С.В – СПб. : СПбГУТ, 2016. – 48с

Написаны в соответствии с рабочими учебными программами дисциплины «Инфокоммуникационные системы и сети».

Данный курс лабораторных работ посвящен практическому изучению, настройке и работе с сетевым оборудованием локальных сетей.

Предназначен для студентов обучающихся по направлению подготовки 09.03.02 «Информационные системы и технологии»

УДК 621.391.24(77)
ББК 3287я73

СОДЕРЖАНИЕ

Лабораторная работа 1

УСТАНОВКА СЕАНСА КОНСОЛИ С ПОМОЩЬЮ ПРОГРАММЫ TERA TERM

1.1. Цель работы

Получение доступа к коммутатору Cisco через последовательный порт консоли
Отображение и настройка основных параметров устройства

1.1.1. Задачи

Часть 1. Получение доступа к коммутатору Cisco через последовательный порт консоли

1. Подключитесь к коммутатору Cisco с помощью последовательного консольного кабеля.
2. Установите сеанс консоли с помощью эмулятора терминала, например программы Tera Term.

Часть 2. Отображение и настройка основных параметров устройства

1. Отобразите настройки устройства с помощью команды **show.**
2. Настройка часов на коммутаторе.

1.1.2. Исходные данные/

Различные модели маршрутизаторов и коммутаторов Cisco используются во всех типах сетей. Управление этими устройствами осуществляется через локальное консольное подключение или удалённое подключение. Практически все устройства Cisco оснащены последовательным портом консоли, который можно использовать для подключения.

В ходе выполнения лабораторной работы вы узнаете, как получить доступ к устройству Cisco через прямое локальное подключение к порту консоли, пользуясь программой эмуляции терминала Tera Term, а также научитесь настраивать последовательный порт для консольного подключения Tera Term. Подключившись к устройству Cisco через консоль, вы сможете вывести на экран или изменить его настройки. В этой лабораторной работе необходимо только отобразить параметры и настроить часы.

1.1.3. Необходимые ресурсы

a. 1 маршрутизатор (серия Cisco 1941 и 1 коммутатор (серия Cisco 2960
b. 1 ПК (Windows 7, с программой эмулятора терминала, например Tera Term)
c. Для настройки коммутатора или маршрутизатора через порт консоли RJ-45 необходим консольный кабель (DB-9 для RJ-45).

Получение доступа к коммутатору Cisco через последовательный порт консоли

Подключить ПК к коммутатору Cisco можно с помощью инверсного

консольного кабеля. Такое подключение обеспечивает доступ к интерфейсу командной строки (CLI), а также позволяет просматривать и изменять настройки коммутатора.

1.2. Часть 1 Получение доступа к коммутатору Cisco через последовательный порт консоли

1.2.1. Подключите коммутатор Cisco к компьютеру с помощью инверсного консольного кабеля как показано на рис.1.

a. Вставьте инверсный консольный кабель в порт консоли RJ-45 коммутатора.
b. Другой конец кабеля подключите к последовательному COM-порту компьютера.
c. Включите коммутатор Cisco и компьютер.

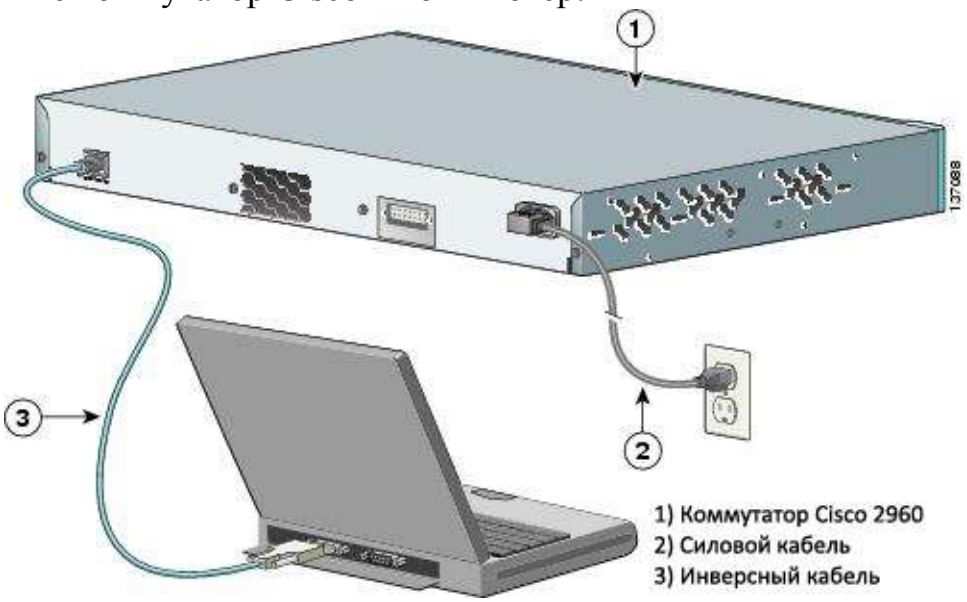

Рис.1 Подключение коммутатору Cisco через последовательный порт консоли

1.2.2. Настройте программу Tera Term для установки консольной сессии с коммутатором.

Tera Term - это программа эмуляции терминала. Она обеспечивает доступ к выходным данным терминала коммутатора и позволяет настраивать коммутатор.

a. Чтобы открыть программу Tera Term, нажмите кнопку **Пуск** на панели задач ОС **Windows**. На вкладке **Все программы** найдите **Tera Term**.
Примечание. Если программа Tera Term не установлена, её можно загрузить по следующему адресу, выбрав **Tera Term**:
http://logmett.com/index.php?/download/free-downloads.html
В диалоговом окне «Новое подключение» установите переключатель в

значении **Последовательный**. Проверьте, правильно ли указан COM-порт, и нажмите кнопку **OK**, чтобы продолжить. Рис.2

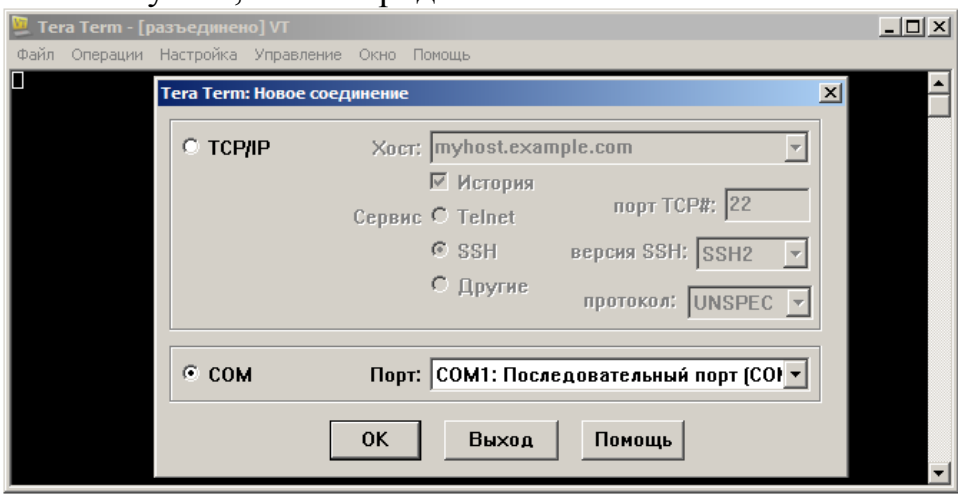

Рис.2 Программа эмуляции терминала Tera Term

b. В меню **Настройка** программы Tera Term выберите **Последовательный порт**, чтобы проверить настройки последовательного подключения. Параметры порта консоли по умолчанию: 9600 бод, 8 бит данных, без контроля по чётности, 1 стоповый бит, без управления потоком. Настройки Tera Term по умолчанию совпадают с настройками порта консоли для связи с коммутатором Cisco IOS. Рис.3

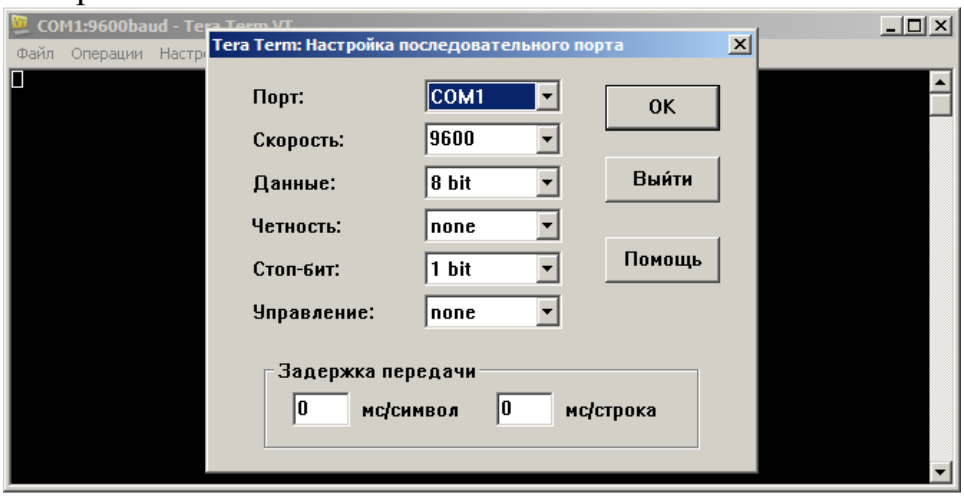

Рис.3 Настройка программы Tera Term

c. Отобразятся выходные данные терминала. Теперь можно настроить коммутатор Cisco. В приведённом ниже примере показаны выходные данные коммутатора, отображаемые в терминале во время загрузки устройства. Рис.4

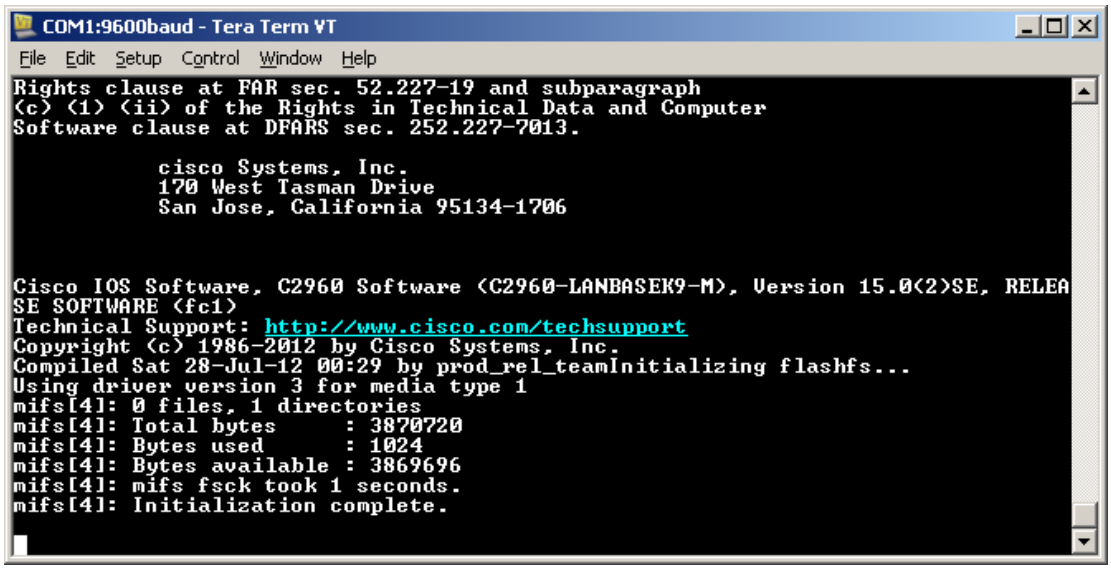

Рис.4 Выходные данные коммутатора

1.3. Часть 2 Отображение и настройка основных параметров устройства

В этом разделе вы познакомитесь с пользовательским и привилегированным режимами, определите версию межсетевой операционной системы (IOS), отобразите настройки часов и выполните настройку часов коммутатора.

Отобразите версию коммутатора IOS.

a. После запуска коммутатора появится указанное ниже сообщение. Введите **n**, чтобы продолжить**.**

   Would you like to enter the initial configuration dialog? [yes/no]: **n**

   Примечание. Если указанное выше сообщение не отображается, попросите преподавателя восстановить на коммутаторе начальную конфигурацию.

b. В пользовательском режиме отобразите версию IOS своего коммутатора.

   Switch> **show version**

1.4. Выполните настройку часов.

Изучая сетевые технологии, вы поймёте, какую важную роль играют правильные настройки времени на коммутаторе Cisco в процессе поиска и устранения неисправностей. Перечисленные ниже действия позволяют вручную настроить внутренние часы коммутатора.

a. Отобразите текущие настройки часов.

   Switch> **show clock**

   *00:30:05.261 UTC Mon Mar 1 2016

b. Настройки часов изменяются в привилегированном режиме. Войдите в привилегированный режим, набрав команду **enable** в командной строке пользовательского режима.
   Switch> **enable**
c. Выполните настройку часов. Вопросительный знак («?») открывает справку и позволяет определить необходимые настройки текущего времени, даты и года. Нажмите клавишу ВВОД, чтобы завершить настройку часов.
   Switch# **clock set ?**
     hh:mm:ss Current Time
   Switch# **clock set 15:08:00 ?**
     <1-31> Day of the month
     MONTH   Month of the year
   Switch# **clock set 15:08:00 Oct 26 ?**
     <1993-2035> Year
   Switch# **clock set 15:08:00 Oct 26 2016**
   Switch#
   *Oct 26 15:08:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 00:31:43 UTC Mon Mar 1 1993 to 15:08:00 UTC Fri Oct 26 2016, configured from console by console.
d. Введите команду **show clock** и проверьте, обновлены ли настройки часов.
   Switch# **show clock**
   15:08:07.205 UTC Fri Oct 26 2016

Лабораторная работа 2

СОЗДАНИЕ ПРОСТОЙ СЕТИ

2.1. Цель работы

Настройка топологии сети (только Ethernet). Рис 5.

Настройка узлов ПК. Настройка и проверка основных параметров коммутатора в соответствии с таблицей 1.

2.1.1 Топология

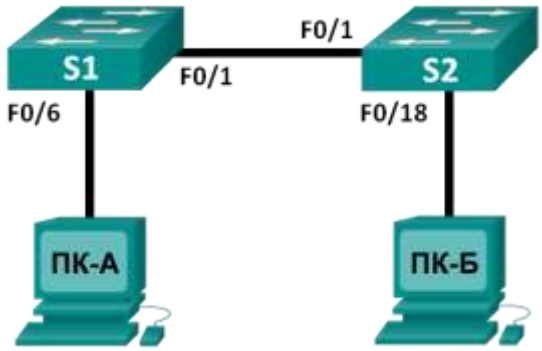

Рис 5 Топология сети

Таблица 1 Таблица адресации

Устройство	**Интерфейс**	**IP-адрес**	**Маска подсети**	**Шлюз по умолчанию**
S1	VLAN 1	Недоступно	Недоступно	Недоступно
S2	VLAN 1	Недоступно	Недоступно	Недоступно
ПК-А	Сетевой адаптер	192.168.1.10	255.255.255.0	Недоступно
ПК-Б	Сетевой адаптер	192.168.1.11	255.255.255.0	Недоступно

2.1.2 Задачи

Часть 1 Настройка топологии сети (только Ethernet)

1. Укажите, какие кабели и порты должны использоваться в сети.
2. Проложите кабели между устройствами.

Часть 2 Настройка узлов ПК

1. Настройте на узлах статический IP-адрес на интерфейсах, которые подключены к локальной сети.
2. Проверьте связь между компьютерами с помощью утилиты **ping**.

Часть 3 Настройка и проверка основных параметров коммутатора

1. Настройте имя узла, локальные пароли и баннер входа в систему для

каждого коммутатора.
2. Сохраните текущие конфигурации.
3. Отобразите текущую конфигурацию коммутатора.
4. Отобразите версию IOS текущего коммутатора.
5. Отобразите статус интерфейсов.

2.1.3 Исходные данные/

Сети состоят из трёх основных компонентов: узлов, коммутаторов и маршрутизаторов. В этой лабораторной работе вам предстоит построить простую сеть с двумя узлами и двумя коммутаторами и настроить основные параметры, включая имя узла, локальные пароли и баннер входа в систему. С помощью команды **show** отобразите текущую конфигурацию, версию IOS и состояние интерфейса. С помощью команды **copy** сохраните конфигурации устройств.

В данной лабораторной работе вам нужно применить к компьютерам IP-адресацию и обеспечить соединение между этими двумя устройствами. Для проверки подключения используйте утилиту **ping.**

2.1.4 Необходимые ресурсы

- 2 коммутатора (Cisco 2960, ПО CISCO IOS версии 15.0(2), образ lanbasek9 или аналогичный)
- 2 ПК (Windows 7, Vista и XP с программой эмуляции терминала, например Tera Term)
- Консольные кабели для настройки устройств CISCO IOS через консольные порты
- Кабели Ethernet в соответствии с топологией

2.2. Часть 1 Настройка топологии сети (только Ethernet)

В части 1 необходимо проложить кабели между устройствами в соответствии с топологией сети.

Шаг 1: Включите устройства.

Включите все устройства в топологии. Коммутаторы не имеют кнопок включения и включаются при подключении шнура питания.

Шаг 2: Соедините два коммутатора.

Подключите один конец кабеля Ethernet к разъёму F0/1 на коммутаторе S1, а другой - к разъёму F0/1 на коммутаторе S2. Лампочки разъёмов F0/1 на обоих коммутаторах загорятся жёлтым, а потом зелёным цветом. Это означает, что коммутаторы подключены правильно.

Шаг 3: Подсоедините компьютеры к соответствующим коммутаторам.

a. Подключите один конец второго кабеля Ethernet к порту сетевого адаптера

ПК-А. Другой конец кабеля подключите к разъёму F0/6 на коммутаторе S1. После подключения ПК к коммутатору лампочка разъёма F0/6 загорится сначала жёлтым, а затем зелёным цветом, означающим, что ПК-А подключён правильно.

b. Подключите один конец последнего кабеля Ethernet к порту сетевого адаптера ПК-Б. Подключите другой конец кабеля к разъёму F0/18 на коммутаторе S2. После подключения ПК к коммутатору лампочка разъёма F0/18 загорится сначала жёлтым, а затем зелёным цветом, означающим, что ПК-Б подключён правильно.

Шаг 4: Осмотрите сетевые соединения.

После подведения кабелей к сетевым устройствам тщательно проверьте соединения, чтобы впоследствии сократить время поиска и устранить неполадки с сетевым подключением.

2.3. Часть 2 Настройка узлов ПК

Шаг 1: Настройте статический IP-адрес на компьютерах.

a. В ОС **Windows** нажмите кнопку **Пуск** и зайдите в **Панель управления**.

b. В разделе «Сеть и Интернет» нажмите на ссылку **Просмотр состояния сети и задач**.

Примечание. Если в Панели управления отображается список значков, нажмите на раскрывающееся меню **Просмотр:** и выберите параметр **Категория**.

c. В левой части окна «Центр управления сетями и общим доступом» нажмите на ссылку **Изменение параметров адаптера**.

d. В окне «Сетевые подключения» отображаются доступные интерфейсы ПК. Нажмите правой кнопкой мыши на значок **Подключение по локальной сети** и выберите пункт **Свойства**.

e. Выберите опцию **Протокол Интернета версии 4 (TCP/IPv4)** и нажмите кнопку **Свойства**.

Примечание. Чтобы открыть окно «Свойства», можно также дважды нажать кнопкой мыши на **Протокол Интернета версии 4 (TCP/IPv4)**.

f. Чтобы настроить IP-адрес, маску подсети и шлюз по умолчанию вручную, установите переключатель **Использовать следующий IP-адрес**.

Примечание. В рассмотренном выше примере введены IP-адрес и маска подсети для ПК-А. Шлюз по умолчанию не указан, поскольку к сети не подключён ни один маршрутизатор. В таблице 1 адресации указаны данные IP-адреса для ПК-Б.

g. Указав все данные IP, нажмите кнопку **OK**. Нажмите кнопку **OK** в окне «Свойства подключения по локальной сети», чтобы присвоить IP-адрес адаптеру локальной сети.
h. Повторите перечисленные выше действия, чтобы ввести данные IP-адреса для ПК-Б.

Шаг 2: Проверьте настройки и соединение ПК.

Для проверки настроек и соединения ПК используйте окно командной строки **(cmd.exe).**

a. На ПК-Анажмите кнопку **Пуск**, введите **cmd** в строке **Найти программы и файлы и** нажмите клавишу ВВОД.
b. В окне cmd.exe можно вводить команды сразу в компьютер и тут же просматривать их результаты. Проверьте настройки ПК с помощью команды **ipconfig /all**. Эта команда отображает имя ПК и сведения об IPv4-адресе.
c. Введите **ping 192.168.1.11** и нажмите клавишу ВВОД.
   Успешно ли выполнен эхо-запрос с помощью команды ping?
   Если нет, попытайтесь найти и устранить неполадку.
   Примечание. Если вы не получили ответ от ПК-Б, попробуйте отправить эхо-запрос с помощью команды ping на ПК-Б ещё раз. Если ответа от ПК-Б по-прежнему нет, попробуйте отправить эхо-запрос с помощью команды ping с ПК-Б на ПК-А. Если ответ от удалённого ПК не поступает, обратитесь за помощью к преподавателю.

2.4. Настройка и проверка основных параметров коммутатора

Шаг 1: Подключитесь к коммутатору через консоль.

С помощью программы Tera Term установите консольное подключение ПК-А к коммутатору.

Шаг 2: Войдите в привилегированный режим.

Привилегированный режим даёт доступ ко всем командам коммутатора. К привилегированному набору команд относятся те, которые содержатся в пользовательском режиме, а также команда **configure**, при помощи которой выполняется доступ к остальным командным режимам. Перейдите в привилегированный режим, введя команду **enable**.

```
Switch>enable
Switch#
```

Приглашение в командной строке изменится с **Switch >** на **Switch #**, что указывает на привилегированный режим.

Шаг 3: Войдите в режим конфигурации.

Для входа в режим конфигурации используйте команду **configuration terminal**.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

Switch (config) |

Приглашение в командной строке изменится в соответствии с режимом глобальной конфигурации.

Шаг 4: Присвойте коммутатору имя.

С помощью команды **hostname**измените имя коммутатора на **S1**.

Switch(config)# **hostname S1**

S1(config)#

Шаг 5: Запретите нежелательные поиски в DNS.

Отключите поиск в DNS, чтобы предотвратить попытки коммутатора преобразовывать введённые команды таким образом, как будто они являются именами узлов.

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

S1(config)#

Шаг 6: Введите локальные пароли.

Для предотвращения несанкционированного доступа к коммутатору необходимо настроить пароли.

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

S1(config)# **line con 0**

S1(config-line)# **password cisco**

S1(config-line)# **login**

S1(config-line)# **exit**

S1(config)#

Шаг 7: Введите сообщение дня (MOTD).

Баннер входа в систему, называемый также сообщением дня (MOTD), предупреждает о том, что любые попытки несанкционированного доступа к коммутатору запрещены.

Для использования команды **banner motd**необходимы разграничители, чтобы можно было распознать содержимое баннерного сообщения. Разграничительным символом может быть любой символ, которого нет в данном сообщении. По этой причине часто используются такие символы, как **#**.

S1(config)# **banner motd #**

Enter TEXT message.End with the character '#'.

Unauthorized access is strictly prohibited and prosecuted to the full extent of the law. #

S1(config)# **exit**

S1#

Шаг 8: Сохраните конфигурацию.

С помощью команды **copy** сохраните текущую конфигурацию в файл загрузочной конфигурации, который хранится в энергонезависимой памяти(NVRAM).

S1# **copy running-config startup-config**

Шаг 9: Отобразите текущую конфигурацию.

Команда **show running-config** отображает всю текущую конфигурацию постранично. Для пролистывания страниц используйте клавишу ПРОБЕЛ. Команды, выполненные в пунктах 1–8, выделены ниже.

S1# **show running-config**

Шаг 10: Отобразите версию IOS и другие необходимые данные коммутатора.

С помощью команды**show version**отобразите версию IOS коммутатора, а также другую полезную информацию. Здесь для пролистывания отображаемыхданных также используется клавиша ПРОБЕЛ.

S1# **show version**

Шаг 11: Отобразите состояние подключённых интерфейсов коммутатора.

Для проверки состояния подключённых интерфейсов используйте команду **show ip interface brief**. Для пролистывания списка используйте клавишу ПРОБЕЛ.

S1# **show ip interface brief**

Шаг 12: Повторите шаги 1–12 для настройки коммутатора S2.

В данном случае необходимо изменить имя узла на S2.

Приложение к лабораторной работе 2. Инициализация и перезагрузка коммутатора

Шаг 1: Подключитесь к коммутатору.

Подключите консоль к коммутатору и войдите в привилегированный режим.

Switch>**enable**

Switch#

Шаг 2: Определите, были ли созданы виртуальные локальные сети (VLAN).

Воспользуйтесь командой **show flash**, чтобы определить, были ли созданы сети VLAN на коммутаторе.

Switch# **show flash**

Шаг 3: Удалите файл виртуальной локальной сети (VLAN).

a. Если файл **vlan.dat** обнаружен во флеш-памяти, удалите этот файл.

Switch# **delete vlan.dat**

Delete filename [vlan.dat]?

Будет предложено проверить имя файла. На данном этапе можно изменить имя файла или нажать клавишу ВВОД, если имя введено верно.

b. При запросе удаления этого файла нажмите клавишу ВВОД, чтобы подтвердить удаление. (Чтобы отменить удаление, нажмите любую другую кнопку.)

Delete flash:/vlan.dat? [confirm]

Switch#

Шаг 4: Удалите файл загрузочной конфигурации.

Введите команду **erase startup-config**, чтобы удалить файл загрузочной конфигурации из NVRAM. При необходимости удаления файла конфигурации нажмите клавишу ВВОД, чтобы подтвердить удаление. (Чтобы отменить операцию, нажмите любую другую кнопку.)

Switch# **erase startup-config**

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

Switch#

Шаг 5: Перезагрузить коммутатор.

Перезагрузите коммутатор, чтобы удалить из памяти всю информацию о предыдущей конфигурации. При необходимости перезагрузки коммутатора нажмите клавишу ВВОД, чтобы продолжить перезагрузку. (Чтобы отменить перезагрузку, нажмите любую другую клавишу.)

Switch# **reload**

Proceed with reload? [confirm]

Примечание. Возможно, появится запрос о сохранении текущей конфигурации перед перезагрузкой коммутатора. Введите **no**и нажмите клавишу ВВОД.

System configuration has been modified. Save? [yes/no]: **no**

Шаг 6: Пропустите диалоговое окно начальной конфигурации.

После перезагрузки коммутатора появится запрос о входе в диалоговое окно начальной конфигурации. Введите **no** в окне запроса и нажмите клавишу ВВОД.

Would you like to enter the initial configuration dialog? [yes/no]: **no**

Switch>

Лабораторная работа 3

НАСТРОЙКА АДРЕСА УПРАВЛЕНИЯ КОММУТАТОРОМ

3.1. Цель работы

Настройка основных параметров сетевого устройства. Рис 6. Проверка и тестирование подключения к сети в соответствии с таблицей 2.

3.1.1 Топология

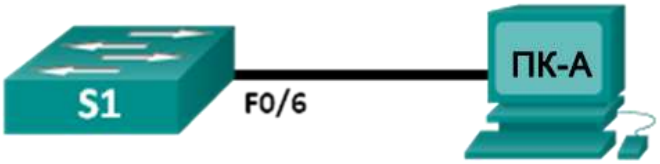

Рис 6 Топология сети

Таблица 2 Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
S1	VLAN 1	192.168.1.2	255.255.255.0	Недоступно
ПК-А	Сетевой адаптер	192.168.1.10	255.255.255.0	Недоступно

3.1.2 Задачи

Часть 1. Настройка основных параметров сетевого устройства

1. Создайте сеть в соответствии с изображенной на схеме топологией.
2. Настройте основные параметры коммутатора, включая имя узла, адрес управления и доступ по протоколу Telnet.
3. Настройте IP-адрес ПК.

Часть 2. Проверка и тестирование подключения ксети

4. Отобразите конфигурацию устройства.
5. Проверьте сквозное подключение с помощью эхо-запроса с помощью команды ping.
6. Проверьте возможность удалённого управления по протоколу Telnet.
7. Сохраните файл текущей конфигурации коммутатора.

3.1.3 Исходные данные

Коммутаторы Cisco имеют особый интерфейс, который называется виртуальным интерфейсом коммутатора (SVI). На SVI интерфейсе можно сконфигурировать IP-адрес, который обычно называют адресом управления. Он позволяет получить удалённый доступ к коммутатору для отображения и настройки параметров.

В ходе лабораторной работы вам необходимо создать простую сеть, используя

кабель локальной сети Ethernet и получить доступ к коммутатору Cisco, используя консоль и методы удалённого доступа. Вы настроите основные параметры коммутатора и IP-адресацию, а также продемонстрируете использование IP-адреса управления для удалённого доступа к коммутатору. Топология состоит из одного коммутатора и одного узла, использующего только порты Ethernet и консоли.

3.1.4 Необходимые ресурсы

- 1 коммутатор (серия Cisco 2960, с программным обеспечением Cisco IOS версии 15.0(2), образ lanbasek9 или аналогичный)
- 1 ПК (Windows 7, Vista или XP с программой эмулятора терминала, например Tera Term)
- Консольные кабели для настройки устройств CISCO IOS через консольные порты
- Кабели Ethernet в соответствии с топологией

3.2. Часть 1 Настройка основных параметров сетевого устройства

В части 1 вы должны настроить сеть и основные параметры, такие как IP-адреса интерфейсов и доступ к устройствам.

Подключите кабели.

a. Создайте сеть в соответствии с изображенной на схеме топологией.
b. Создайте консольное подключение к коммутатору на ПК-А.

Настройте основные параметры коммутатора.

На этом этапе вам необходимо настроить основные параметры коммутатора (такие как имя узла) и IP-адрес для SVI. Назначение IP-адреса на коммутаторе это лишь первый шаг. Как сетевому администратору, вам следует выбрать способ управления коммутатором. Два наиболее распространённых метода управления - это Telnet и SSH, однако протокол Telnet не очень надёжен. Вся информация, передаваемая между двумя устройствами, отправляется в виде простого текста. Анализатор пакетов может легко перехватить, а также прочесть пароли и другие важные данные.

a. Если в энергонезависимой памяти (NVRAM) коммутатора нет сохранённых файлов конфигурации, воспользовавшись командой Switch>, вы перейдете в пользовательский режим. Войдите в привилегированный режим.
   Switch> **enable**
   Switch#
b. Проверьте чистый файл конфигурации с помощью команды привилегированного режима **show running-config.** Если файл конфигурации был ранее сохранён, его нужно удалить. В зависимости от модели коммутатора и версии IOS конфигурация может выглядеть по-разному. При этом настроенных ранее паролей или IP-адреса на коммутаторе быть не должно. Если ваш коммутатор не имеет конфигурации по умолчанию,

обратитесь за помощью к преподавателю.

c. Войдите в режим глобальной конфигурации и назначьте имя узла коммутатора.
   Switch# **configure terminal**
   Switch(config)# **hostname S1**
   S1(config)#
d. Настройте пароль доступа к коммутатору.
   S1(config)# **enable secret class**
   S1(config)#
e. Запретите нежелательные поиски в службе доменных имен (DNS).
   S1(config)# **no ip domain-lookup**
   S1(config)#
f. Настройте сообщение дня (MOTD), которое будет отображаться перед входом в систему.
   S1(config)# **banner motd #**
   Enter Text message. End with the character '#'.
   Unauthorized access is strictly prohibited. #
g. Проверьте настройки доступа, переключаясь между режимами.
   S1(config)# **exit**
   S1#
   S1# **exit**
   Unauthorized access is strictly prohibited.
   S1>
h. Вернитесь из пользовательского режима в привилегированный.
   S1> **enable**
   Password: **class**
   S1#
   Примечание. Пароль не будет отображаться на экране в процессе ввода.
i. Войдите в режим глобальной конфигурации и настройте IP-адрес SVI для разрешения удалённого управления коммутатором.
   S1# **config t**
   S1#(config)# **interface vlan 1**
   S1(config-if)# **ip address 192.168.1.2 255.255.255.0**
   S1(config-if)# **no shut**
   S1(config-if)# **exit**
   S1(config)#
j. Ограничьте доступ к порту консоли. Конфигурация по умолчанию не требует пароля при консольных подключениях.
   S1(config)# **line con 0**
   S1(config-line)# **password cisco**

S1(config-line)# **login**
S1(config-line)# **exit**
S1(config)#

k. Настройте канал виртуального соединения для удалённого управления (VTY), чтобы к коммутатору можно было подключаться по протоколу Telnet. Если вы не укажете пароль VTY, то не сможете подключаться к коммутатору по протоколу Telnet.

S1(config)# **line vty 0 4**
S1(config-line)# **password cisco**
S1(config-line)# **login**
S1(config-line)# **end**
S1#
*Mar 1 00:06:11.590: %SYS-5-CONFIG_I: Configured from console by console

Настройте IP-адрес ПК-A.

a. Назначьте IP-адрес и маску подсети для ПК, как показано таблица 2. Процедура присвоения IP-адреса на ПК под управлением ОС Windows 7 описана ниже.

Нажмите **кнопку Пуск** > **Панель управления**.
Нажмите **кнопку Просмотр:** > **Категория**.
Выберите **вариант Просмотр состояния сети и задач** > **Изменение параметров адаптера**.
Нажмите правой кнопкой мыши на вариант **Подключение к локальной сети** и выберите пункт **Свойства**.
Выберите вариант **Протокол Интернета версии 4 (TCP/IPv4)**, далее щёлкните пункт Свойства > **OK**.
Установите переключатель **Использовать следующий IP-адрес и** введите IP-адрес и маску подсети.

3.3. Часть 2 Проверка и тестирование подключения сети

Теперь нужно проверить и зафиксировать конфигурацию коммутатора, протестировав сквозное подключение между ПК-A и коммутатором S1, а также возможность удалённого управления коммутатором.

Шаг 1: Отобразите конфигурацию коммутатора S1.

a. Воспользовавшись программой Tera Term на ПК, вернитесь к консольному подключению, чтобы отобразить и проверить конфигурацию коммутатора с помощью команды **show**. Ниже представлен пример конфигурации. Внесённые вами настройки выделены жёлтым цветом. Другие параметры конфигурации предусмотрены в IOS по умолчанию.

S1# **show run**

b. Проверьте состояние интерфейса управления SVI. Интерфейс VLAN 1 должен находиться в состоянии «up/up» и иметь назначенный IP-адрес.

Обратите внимание на то, что порт коммутатора F0/6 также должен функционировать, так как к нему подключён ПК-А. Поскольку все порты коммутатора по умолчанию входят в сеть VLAN 1, вы можете обмениваться данными с коммутатором по IP-адресу, который настроили для сети VLAN1.

S1# **show ip interface brief**

Проверьте сквозное подключение.

Откройте диалоговое окно (cmd.exe) на ПК-А. Для этого нажмите кнопку **Пуск** и введите команду **cmd** в поле **Найти программы и файлы.** Проверьте IP-адрес ПК-А с помощью команды **ipconfig /all**. Эта команда отображает имя ПК и сведения об IPv4-адресе. Отправьте эхо-запрос с помощью команды ping на собственный адрес ПК-А и адрес управления коммутатором S1.

a. Сначала отправьте эхо-запрос с помощью команды ping на адрес ПК-А.

   C:\Users\NetAcad> **ping 192.168.1.10**

   На экране должны появиться показанные ниже данные.

b. Отправьте эхо-запрос с помощью команды ping на адрес управления SVI коммутатора S1.

   C:\Users\NetAcad> **ping 192.168.1.2**

   На экране должны появиться данные. Если эхо-запрос с помощью команды ping выполнить не удалось, попробуйте найти ошибку в основных параметрах устройства. При необходимости проверьте кабели и IP-адресацию.

Проверьте удалённое управление коммутатором S1.

Сейчас вам предстоит получить удалённый доступ к коммутатору S1 по протоколу Telnet, используя адрес управления SVI. В данной лабораторной работе ПК-А и коммутатор S1 находятся рядом. В производственной сети коммутатор может находиться в коммутационном шкафу на последнем этаже, а компьютер - на первом. Telnet не является безопасным протоколом, однако в данной лабораторной работе для проверки удалённого доступа вы будете использовать его. Вся информация по протоколу Telnet, включая пароли и команды, отправляется в иде простого текста.

Примечание. Изначально ОС Windows 7 не поддерживает Telnet. Протокол должен быть активирован администратором. Для установки клиента Telnet откройте окно командной строки и введите **pkgmgr /iu: "TelnetClient"**.

C:\Users\NetAcad> **pkgmgr /iu:”TelnetClient”**

a. Для подключения к коммутатору S1 через адрес управления SVI в открытом окне командной строки на ПК-А введите команду Telnet. Пароль: **cisco.**

   C:\Users\NetAcad> **telnet 192.168.1.2**

b. Указав пароль **cisco**, вы сможете перейти в командную строку пользовательского режима. При появлении приглашения введите **enable.** Введите пароль **class,** чтобы войти в привилегированный режим и выполнить

команду **show run.**

Сохраните файл конфигурации.

a. Открыв сеанс Telnet, введите в командную строку **copy run start.**
   S1# **copy run start**
   Destination filename [startup-config]? **[Enter]**
   Building configuration ..
   S1#
b. Введите **quit**, чтобы завершить сеанс Telnet. После этого вы вернётесь в командную строку Windows 7.

Лабораторная работа 4

ИЗГОТОВЛЕНИЕ КРОССОВОГО КАБЕЛЯ ETHERNET

4.1. Цель работы

Анализ стандартов и схемы подключения кабелей Ethernet. Изготовление кроссового кабеля Ethernet. Проверка кроссового кабеля Ethernet в соответствии с топологией рис. 5 и таблицей 3.

4.1.1. Топология

Рис 7 Топология сети

Таблица 3 Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
ПК-А	Сетевой адаптер	192.168.10.1	255.255.255.0	Недоступно
ПК-Б	Сетевой адаптер	192.168.10.2	255.255.255.0	Недоступно

4.1.2. Задачи

Часть 1. Анализ стандартов и схемы подключения кабелей Ethernet

1. Проанализируйте таблицы для кабеля Ethernet стандарта TIA/EIA 568-A.
2. Проанализируйте таблицы для кабеля Ethernet стандарта TIA/EIA 568-B.

Часть 2. Изготовление кроссового кабеля Ethernet

1. Изготовьте и обработайте разъём кабеля TIA/EIA 568-A.
2. Изготовьте и обработайте разъём кабеля TIA/EIA 568-B.

Часть 3. Проверка кроссового кабеля Ethernet

1. Протестируйте кроссовый кабель Ethernet с помощью устройства для проверки кабелей.
2. Соедините два ПК с помощью кроссового кабеля Ethernet.

4.1.3. Исходные данные/

В лабораторной работе вы должны будете изготовить и обработать кроссовый кабель Ethernet, а также проверить его, соединив два ПК и отправив между ними эхо-запрос с помощью команды ping. Для начала вы проанализируете стандарты 568-A и 568-B Ассоциации телекоммуникационной промышленности и Ассоциации электронной промышленности (TIA/EIA) и их

применение к кабелям Ethernet. Затем вы изготовите и проверите кроссовый кабель Ethernet. И наконец, вы используете изготовленный кабель для соединения двух ПК и проверите связь посредством эхо-запросов с помощью команды ping.

4.1.4. Необходимые ресурсы

- Один отрезок кабеля категории 5 или 5e Кабель длиной 0,6–0,9 м
- Два разъёма RJ-45
- Обжимной инструмент для разъёмов RJ-45
- Кусачки
- Клещи для снятия изоляции
- Устройство для проверки кабелей Ethernet (необязательно).
- Два ПК (Windows 7, Vista или XP)

4.2. Часть 1 Анализ стандартов и схемы подключения кабелей Ethernet

Стандарты TIA/EIA определяют правила использования неэкранированных витых пар в локальных средах. Стандарты TIA/EIA 568-A и 568-B обусловливают коммерческие кабельные стандарты для локальных сетей; они широко применяются в разводке локальных сетей для организаций и, кроме прочего, определяют цвет каждого кабеля для разных контактов.

В кроссовом кабеле вторая и третья пары разъёма RJ-45 на одном конце кабеля переворачиваются на другом конце, что меняет местами пары отправки и приёма. На одном конце кабеля используется схема подключения кабеля со стандартом 568-A, а на другом - со стандартом 568-B. Кроссовые кабели обычно используются для подключения концентраторов к концентраторам или коммутаторов к коммутаторам, но могут применяться и для создания простой сети из двух узлов.

Примечание. Поскольку современные сетевые устройства имеют функцию автоматического определения скорости передачи данных, прямой кабель может использоваться даже для подключения аналогичных устройств. Благодаря автоматическому определению скорости, интерфейсы контролируют правильность соединения канальных пар отправления и получения. Если они соединены неверно, интерфейсы обращают один конец соединения в противоположную сторону. Функция автоматического определения скорости передачи данных также выравнивает скорость интерфейсов по самому медленному. Например, при подключении интерфейса маршрутизатора Gigabit Ethernet (1000 Мбит/с) к интерфейсу коммутатора Fast Ethernet (100 Мбит/с), соединение использует Fast Ethernet.

На коммутаторе Cisco 2960 автоматическое определение скорости передачи

данных по умолчанию включено, поэтому соединение двух коммутаторов 2960 осуществляется с помощью либо кроссового, либо прямого кабеля. С некоторыми старыми коммутаторами это не работает и приходится использовать именно кроссовый кабель.

Интерфейсы Gigabit Ethernet маршрутизатора Cisco 1941 обладают функцией автоматического определения скорости передачи данных, поэтому для прямого подключения ПК к интерфейсу маршрутизатора (в обход коммутатора) можно использовать прямой кабель. С некоторыми старыми маршрутизаторами это не работает и приходится использовать именно кроссовый кабель.

Как правило, при прямом подключении двух узлов рекомендуется использовать кроссовый кабель.

Приведённая ниже таблица 4 демонстрирует цветовую схему и расположение выводов, а также работу четырёх пар проводов, предусмотренных стандартом 568-A.

Примечание. В локальных сетях на основе стандарта 100Base-T (100 Мбит/с) используются только две пары из четырёх. **568-A 10/100/1000Base-TX Ethernet**

Таблица 4 Цветовая схема и расположение выводов, работа четырёх пар проводов, предусмотренных стандартом 568-A.

Номер разводки	Номер пары	Цвет провода	10Base-T Signal 100Base-TX Signal	1000Base-T Signal
1	2	Белый/зелёный	Передача	BI_DA+
2	2	Зелёный	Передача	BI_DA-
3	3	Белый/оранжевый	Приём	BI_DB+
4	1	Синий	Не используется	BI_DC+
5	1	Белый/синий	Не используется	BI_DC-
6	3	Оранжевый	Приём	BI_DB-
7	4	Белый/коричневый	Не используется	BI_DD+
8	4	Коричневый	Не используется	BI_DD-

Приведённая ниже таблица 5 демонстрирует цветовую схему и расположение выводов для стандарта 568-B.**568-B 10/100/1000-BaseTX Ethernet**

Таблица 5 Цветовая схема и расположение выводов, работа четырёх пар проводов, предусмотренных стандартом 568-A.

Номер разводки	Номер пары	Цвет провода	10Base-T Signal 100Base-TX Signal	1000Base-T Signal
1	2	Белый/оранжевый	Передача	BI_DA+
2	2	Оранжевый	Передача	BI_DA-
3	3	Белый/зелёный	Приём	BI_DB+
4	1	Синий	Не используется	BI_DC+
5	1	Белый/синий	Не используется	BI_DC-
6	3	Зелёный	Приём	BI_DB-
7	4	Белый/коричневый	Не используется	BI_DD+
8	4	Коричневый	Не используется	BI_DD-

4.3. Часть 2 Изготовление кроссового кабеля Ethernet

На кроссовом кабеле вторая и третья пары проводов в разъёме RJ-45 на одном конце обращены в обратную сторону (см. таблицы 4, 5). На одном конце кабеля используется схема подключения кабеля со стандартом 568-A, а на другом - со стандартом 568-B.

Изготовьте и обработайте разъём кабеля TIA/EIA 568-A.

a. Определите необходимую длину кабеля. (Преподаватель подскажет, какой длины кабель вам нужно сделать.)
b. Отрежьте кусок кабеля нужной длины и с помощью клещей для снятия изоляции очистите от оболочки оба конца кабеля на 3 см.
c. В месте срезания оболочки плотно сожмите все четыре пары витых кабелей. Поменяйте пары кабелей местами в порядке, соответствующем стандарту проводного подключения 568-A. При необходимости обращайтесь к таблицам 4, 5. Постарайтесь не повредить витые пары кабеля; их целостность обеспечивает отсутствие помех.
d. Большим и указательным пальцами сплющите, выпрямите и выровняйте провода.
e. Убедитесь в том, что провода кабеля расположены в правильном порядке, соответствующем стандарту 568-A. С помощью кусачек обрежьте четыре пары в прямую линию до длины 1,25–1,9 см.
f. На конце кабеля установите разъём RJ-45, выступ которого должен быть направлен вниз. Плотно вставьте провода в разъём RJ-45. Все провода должны быть видны в конце разъёма на соответствующих местах. Если провода не достигают конца разъёма, извлеките кабель, поменяйте расположение проводов соответствующим образом и вставьте провода обратно в разъём RJ-45.
g. Если всё сделано правильно, вставьте разъём RJ-45 с кабелем в обжимной

инструмент. Сожмите кабель в инструменте достаточно сильно, так чтобы контакты на разъёме RJ-45 прошли через изоляцию проводов, закрывая таким образом проводной канал.

Изготовьте и обработайте разъём кабеля TIA/EIA 568-B.

Повторите шаги a–g, используя цветовую схему таблица 5 проводки 568-B, для другого конца.

4.4. Часть 3 Проверка кроссового кабеля Ethernet

Проверьте кабель.

Многие кабельные тестеры проверяют длину и расположение проводов. Если кабельный тестер имеет функцию проверки схемы проводов, он проверяет, к каким контактам на одном конце кабеля подключены контакты на другом его конце.

Если преподаватель располагает кабельным тестером, проверьте работоспособность кроссового кабеля. Если кабель не прошел проверку, спросите у преподавателя, нужно ли вам поменять расположение контактов и заново проверить кабель.

Соедините два ПК с помощью сетевого адаптера и кроссового кабеля Ethernet.

a. Вместе с партнёром по лабораторной работе настройте свой ПК с одним из IP-адресов, указанных втаблице адресации. Например, если вы работаете на **ПК-А**, вам нужно указать IP-адрес **192.168.10.1** с **24-битной маской подсети.** IP-адрес вашего партнера **192.168.10.2**. Адрес шлюза по умолчанию можно оставить пустым.
b. Используя изготовленный вами кроссовый кабель, соедините два ПК через сетевые адаптеры.
c. Из командной строки ПК-А отправьте эхо-запрос с помощью команды ping на IP-адрес ПК-Б.

Примечание. Для прохождения эхо-запросов с помощью команды ping брандмауэр Windows можно на время отключить. В этом случае снова включите брандмауэр по завершении лабораторной работы.

d. Повторите процедуру и отправьте эхо-запрос с помощью команды ping с ПК-А на ПК-Б.

Если проблем с IP-адресацией и брандмауэром нет, при правильном подключении кабелей эхо-запросы с помощью команды ping должны пройти успешно.

Лабораторная работа 5

ИСПОЛЬЗОВАНИЕ ИНТЕРФЕЙСА КОМАНДНОЙ СТРОКИ IOS С ТАБЛИЦАМИ MAC-АДРЕСОВ КОММУТАТОРА

5.1Цель работы

Создание и настройка сети. Изучение таблицы MAC-адресов коммутатора в соответствии с топологией рис. 8 и таблицей 6..

5.1.1. Топология

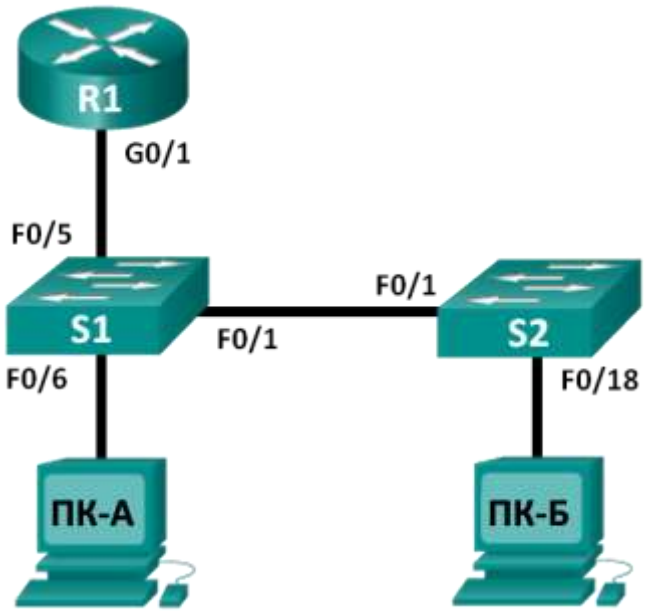

Рис 8 Топология сети

Таблица 6 Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	Недоступно
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S2	VLAN 1	192.168.1.12	255.255.255.0	192.168.1.1
ПК-А	Сетевой адаптер	192.168.1.3	255.255.255.0	192.168.1.1
ПК-Б	Сетевой адаптер	192.168.1.2	255.255.255.0	192.168.1.1

5.1.2. Задачи

Часть 1. Создание и настройка сети

1. Подключите сеть в соответствии со схемой топологии.
2. Настройте сетевые устройства в соответствии с таблицей адресации.

Часть 2. Изучение таблицы MAC-адресов коммутатора

С помощью команды **show** понаблюдайте за процессом создания таблицы MAC-адресов коммутатора.

5.1.3. Исходные данные

Коммутатор локальной сети на уровне 2 предназначен для доставки кадров Ethernet всем узловым устройствам в локальной сети. Коммутатор записывает MAC-адреса узлов, отображаемые в сети, и сопоставляет их с собственными портами коммутаторов Ethernet. Этот процесс называется созданием таблицы MAC-адресов. Получив кадр от ПК, коммутатор изучает MAC-адреса источника и назначения кадра. MAC-адрес источника регистрируется и сопоставляется с портом коммутатора, от которого он был получен. Также в таблице MAC-адресов находится MAC-адрес назначения. Если MAC-адрес назначения известен, кадр пересылается с MAC-адреса соответствующего порта коммутатора. Если MAC-адрес неизвестен, то кадр отправляется по широковещательной рассылке со всех портов коммутатора, кроме того, от которого он был получен. Важно видеть и понимать работу коммутатора и то, как он осуществляет передачу данных по сети. Функционал коммутаторов особенно полезен для сетевых администраторов, которые обеспечивают безопасную и стабильную сетевую коммуникацию.

Коммутаторы используются для соединения компьютеров в сети и передачи данных между ними. Коммутаторы отправляют кадры Ethernet на узловые устройства, установленные по MAC-адресам сетевых адаптеров.

В части 1 вам нужно построить топологию, состоящую из маршрутизатора и двух коммутаторов, соединённых каналом. В части 2 вам предстоит отправить эхо-запросы с помощью команды ping на различные устройства и посмотреть, как два коммутатора строят свои таблицы MAC-адресов.

5.1.4. Необходимые ресурсы

1 маршрутизатор (Cisco 1941 с универсальным образом M3 версии CISCO IOS 15.2(4) или аналогичным)

2 коммутатора (Cisco 2960, ПО CISCO IOS версии 15.0(2), образ lanbasek9 или аналогичный)

2 ПК (Windows 7, Vista и XP с программой эмуляции терминала, например Tera Term)

Консольные кабели для настройки устройств CISCO IOS через консольные порты

Кабели Ethernet в соответствии с топологией

Примечание. Интерфейсы Fast Ethernet на коммутаторах Cisco 2960 определяют тип подключения автоматически, поэтому между коммутаторами S1 и S2 можно использовать прямой кабель Ethernet. При использовании коммутатора Cisco другой модели может потребоваться кроссовый кабель Ethernet.

5.2 Часть 1: Создание и настройка сети

Шаг 1: Подключите сеть в соответствии с топологией.

Шаг 2: Настройте узловые ПК.

Шаг 3: При необходимости включите и перезагрузите маршрутизаторы и коммутаторы.

Шаг 4: Настройте основные параметры для каждого коммутатора.

a. Задайте имя устройства, как показано на топологической схеме.
b. Настройте IP-адрес и шлюз по умолчанию, как указано в таблице адресации.
c. Назначьте **cisco** в качестве паролей консоли и виртуального терминала.
d. Назначьте **class** в качестве пароля привилегированного режима.

Шаг 5: Настройте основные параметры для маршрутизатора.

a. Отключите поиск DNS.
b. Настройте IP-адрес для маршрутизатора, как указано в таблице адресации.
c. Задайте имя устройства, как показано на топологической схеме.
d. Назначьте **cisco** в качестве паролей консоли и виртуального терминала.
e. Назначьте **class** в качестве пароля привилегированного режима.

5.3 Часть 2: Изучение таблицы MAC-адресов коммутатора

Как только между сетевыми устройствами начинается передача данных, коммутатор выясняет MAC-адреса и строит таблицу.

Шаг 1: Запишите MAC-адреса сетевых устройств.

Откройте командную строку на ПК-А и ПК-Б и введите команду **ipconfig /all**. Найдите физические адреса адаптера Ethernet.MAC-адрес ПК-А и MAC-адрес ПК-Б:

Подключитесь к маршрутизатору R1 через консоль и введите команду **show interface G0/1**. Назовите адрес оборудования.

MAC-адрес маршрутизатора R1 Gigabit Ethernet 0/1:

Подключитесь к коммутаторам S1 и S2 через консоль и введите команду **show interface F0/1** на каждом коммутаторе. Найдите адреса оборудования во второй строке выходных данных команды (или встроенный адрес [bia]).

MAC-адрес коммутатора S1 Fast Ethernet 0/1

MAC-адрес коммутатора S2 Fast Ethernet 0/1:

Шаг 2: Отображение таблицы MAC-адресов коммутатора

Подключитесь к коммутатору S2 через консоль и просмотрите таблицу MAC-адресов до и после тестирования сетевой связи посредством эхо-запросов с помощью команды ping.

f. Подключитесь к коммутатору S2 через консоль и войдите в привилегированный режим.
g. В привилегированном режиме введите команду **show mac address-table и** нажмите клавишу ВВОД.

S2# **show mac address-table**

Даже если сетевая коммуникация в сети не происходила (не использовался эхо-запрос с помощью команды ping), коммутатор может узнать MAC-адреса при подключении к ПК и другим коммутаторам.

Записаны ли в таблице MAC-адресов какие-то MAC-адреса?

Какие MAC-адреса записаны в таблице? С какими портами коммутатора они сопоставлены и каким устройствам принадлежат? Игнорируйте MAC-адреса, сопоставленные с центральным процессором.

Если вы не записали MAC-адреса сетевых устройств в шаге 1, как можно определить, каким устройствам принадлежат MAC-адреса, используя только выходные данные команды **show mac address-table**? Работает ли это решение в любой ситуации?

Шаг 3: Очистите таблицу MAC-адресов коммутатора S2 и снова отобразите таблицу MAC-адресов.

a. В привилегированном режиме введите команду **clear mac address-table dynamic**и нажмите клавишу ВВОД.

   S2# **clear mac address-table dynamic**

b. Сразу введите команду **show mac address-table** еще раз. Указаны ли в таблице MAC-адресов адреса для VLAN 1? Указаны ли другие MAC-адреса?

   Через 10 секунд введите команду **show mac address-table и** нажмите клавишу ВВОД. Появились ли в таблице MAC-адресов новые адреса?

Шаг 4: С ПК-Б отправьте эхо-запросы с помощью команды ping на устройства в сети и просмотрите таблицу MAC-адресов коммутатора.

a. В ПК-Б откройте командную строку и введите команду **arp-a.** Не считая адресов многоадресной рассылки и широковещательных адресов, сколько пар адресов устройств IP и MAC было получено протоколом ARP?

b. Из командной строки ПК-Б отправьте эхо-запрос с помощью команды ping на маршрутизатор (шлюз) R1, ПК-А, а также коммутаторы S1 и S2. От всех ли устройств получены отклики? Если нет, проверьте кабели и конфигурации IP.

c. Через консольное соединение на коммутаторе S2 введите команду **show mac address-table**. Добавил ли коммутатор в таблицу MAC-адресов дополнительные MAC-адреса? Если да, то какие адреса и устройства?

   В ПК-Б откройте командную строку и снова введите команду **arp-a.** Появились ли в ARP-кэше ПК-Б дополнительные записи для всех сетевых устройств, на которые были отправлены эхо-запросы с помощью команды ping?

Лабораторная работа 6

СОЗДАНИЕ СЕТИ, СОСТОЯЩЕЙ ИЗ КОММУТАТОРА И МАРШРУТИЗАТОРА

6.1. Цель работы

Настройка топологии и инициализация устройств. Настройка параметров устройств и проверка надёжности подключения в соответствии с топологией рис. 9 и таблицей 7. Отображение сведений об устройствеподключения к сети.

6.1.1 Топология

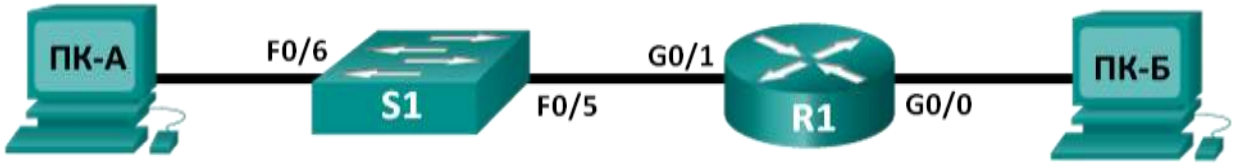

Рис 9 Топология сети

Таблица 7 Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	192.168.0.1	255.255.255.0	Недоступно
	G0/1	192.168.1.1	255.255.255.0	Недоступно
S1	VLAN 1	Недоступно	Недоступно	Недоступно
ПК-А	Сетевой адаптер	192.168.1.3	255.255.255.0	192.168.1.1
ПК-Б	Сетевой адаптер	192.168.0.3	255.255.255.0	192.168.0.1

6.1.2Задачи

Часть 1. Настройка топологии и инициализация устройств

1. Настройте оборудование в соответствии с топологией сети.
2. Выполните инициализацию и перезапуск маршрутизатора и коммутатора.

Часть 2. Настройка параметров устройств и проверка надёжности подключения

1. Назначьте интерфейсам ПК статическую информацию IP-адреса.
2. Настройте маршрутизатор.
3. Проверьте подключение к сети.

Часть 3. Отображение сведений об устройстве

1. Соберите с сетевых устройств данные об аппаратном и программном обеспечении.
2. Интерпретируйте выходные данные из таблицы маршрутизации.
3. Выведите на маршрутизатор сведения об интерфейсе.
4. Выведите на маршрутизатор и коммутатор сводный список интерфейсов.

6.1.3 Исходные данные

Это комплексная лабораторная работа, предназначенная для повторения изученных ранее команд IOS. В ходе лабораторной работы вам нужно будет соединить оборудование в соответствии со схемой топологии и настроить устройства согласно таблице адресации. Сохранённую конфигурацию нужно будет проверить, выполнив тестирование сетевого соединения.

Чтобы получить с устройств информацию и ответить на вопросы о сетевом оборудовании, после настройки устройств и проверки подключения к сети вам нужно будет выполнить различные команды IOS.

Эта лабораторная работа содержит минимум инструкций по выполнению команд, необходимых для настройки маршрутизатора. Список требуемых команд приведён в приложении к лабораторной работе. Проверьте свои знания и попробуйте настроить устройства, не пользуясь приложениями.

6.1.4 Необходимые ресурсы

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

6.2 Часть 1: Настройка топологии и инициализация устройств

Шаг 1: Создайте сеть в соответствии с изображенной на схеме топологией.

a. Соедините устройства в соответствии со схемой топологии, при необходимости используя кабели.
b. Подключите все устройства в топологии.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Если на маршрутизаторе и коммутаторе есть сохранённые файлы конфигурации, инициализируйте и перезагрузите эти устройства с начальными настройками. Инструкции по инициализации и перезагрузке этих устройств приводятся в приложении к лабораторной работе.

6.3 Часть 2: Настройка устройств и проверка подключения

В части вам нужно настроить топологию сети и основные параметры, такие как IP-адреса интерфейсов, доступ к устройствам и пароли. Имена устройств

иадресные данные можно найти в таблице 7.

6.3.1.Цель работы

Настройка топологии и инициализация устройств. Настройка параметров устройств и проверка надёжности подключения. Отображение сведений об устройствеподключения к сети.

6.3.2 Топология и таблица адресации в начале лабораторной работы.

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

Шаг 1: Назначьте интерфейсам ПК статическую информацию IP-адреса.

a. Настройте на ПК-А IP-адрес, маску подсети и параметры шлюза по умолчанию.
b. Настройте на ПК-Б IP-адрес, маску подсети и параметры шлюза по умолчанию.
c. Протестируйте ПК-Б, отправив на ПК-А запрос из окна командной строки. Почему эхо-запросы с помощью команды ping не прошли?

Шаг 2: Настройте маршрутизатор.

a. Подключите консоль к маршрутизатору и активируйте привилегированный режим.
b. Войдите в режим конфигурации.
c. Назначьте маршрутизатору имя устройства.
d. Отключите поиск в DNS, чтобы предотвратить попытки маршрутизатора преобразовывать неверно введённые команды таким образом, как будто они являются именами узлов.
e. Назначьте **class** в качестве пароля привилегированного режима.
f. Назначьте **cisco** в качестве пароля консоли и включите вход по паролю.
g. Назначьте **cisco** в качестве пароля виртуального терминала и включите вход по паролю.
h. Зашифруйте пароли, хранящиеся в открытом виде.
i. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.
j. Настройте и активируйте на маршрутизаторе оба интерфейса.
k. Для каждого интерфейса введите описание, указав, какое устройство к нему подключено.
l. Сохраните текущую конфигурацию в файл загрузочной конфигурации.
m. Настройте на маршрутизаторе время.

Примечание. Вопросительный знак (**?**) позволяет открыть справку с правильной последовательностью параметров, необходимых для выполнения этой команды.

n. Протестируйте ПК-Б, отправив на ПК-А запрос из окна командной строки. Успешно ли выполнен эхо-запрос с помощью команды ping? Почему?

6.4 Часть 3: Отображение сведений об устройстве

В части 3 вы воспользуетесь командами **show** для получения данных с маршрутизатора и коммутатора.

Шаг 1: Соберите с сетевых устройств данные об аппаратном и программном обеспечении.

a. С помощью команды **show version** ответьте на приведённые ниже вопросы о маршрутизаторе.
   Назовите имя образа IOS, который используется маршрутизатором.
   Каким объёмом DRAM обладает маршрутизатор?
   Каким объёмом NVRAM обладает маршрутизатор?
   Каким объёмом флеш-памяти обладает маршрутизатор?

b. С помощью команды **show version** ответьте на приведённые ниже вопросы о коммутаторе.
   Назовите имя образа IOS, который используется коммутатором.
   Каким объёмом оперативной динамической памяти (DRAM) обладает коммутатор?
   Каким объёмом энергонезависимой памяти (NVRAM) обладает коммутатор?
   Назовите номер модели коммутатора.

Шаг 2: Отобразите таблицу маршрутизации на маршрутизаторе.

С помощью команды **show ip route** на маршрутизаторе ответьте на заданные ниже вопросы.

Какой код используется в таблице маршрутизации для обозначения сети, подключённой напрямую?

Сколько записей маршрутизации отмечены кодом C в таблице маршрутизации?

Какие типы интерфейсов связаны с маршрутами с кодом C?

Шаг 3: Выведите на маршрутизатор сведения об интерфейсе.

С помощью команды **show interface g0/1** ответьте на заданные ниже вопросы.

Опишите состояние готовности интерфейса G0/1.

Назовите MAC-адрес интерфейса G0/1.

Каким образом отображается интернет-адрес в команде?

Шаг 4: Выведите на маршрутизатор и коммутатор сводный список интерфейсов.

Для проверки конфигурации интерфейса можно использовать несколько команд. Одна из наиболее удобных **show ip interface brief**. Выходные данные команды содержат общий список интерфейсов устройства с указанием статуса каждого

интерфейса.

a. Введите команду **show ip interface brief** на маршрутизаторе.
   R1# **show ip interface brief**
b. Введите команду **show ip interface brief** на коммутаторе.
   Switch# **show ip interface brief**

Приложение А к лабораторной работе 6. Сведения о конфигурации для выполнения шагов в части 2

Шаг 1: Настройте интерфейсы ПК.

a. Настройте на ПК-А IP-адрес, маску подсети и параметры шлюза по умолчанию.
b. Настройте на ПК-Б IP-адрес, маску подсети и параметры шлюза по умолчанию.
c. Протестируйте ПК-Б, отправив на ПК-А запрос из окна командной строки.

Шаг 2: Настройте маршрутизатор.

a. Подключите консоль к маршрутизатору и активируйте привилегированный режим.
   Router>**enable**
   Router#
b. Войдите в режим конфигурации.
   Router# **conf t**
   Enter configuration commands, one per line. End with CNTL/Z.
   Router(config)#
c. Назначьте маршрутизатору имя устройства.
   Router(config)# **hostname R1**
d. Отключите поиск в DNS, чтобы предотвратить попытки маршрутизатора преобразовывать неверно введённые команды таким образом, как будто они являются именами узлов.
   R1(config)# **no ip domain-lookup**
e. Назначьте **class** в качестве пароля привилегированного режима.
   R1(config)# **enable secret class**
f. Назначьте **cisco** в качестве пароля консоли и включите вход по паролю.
   R1(config)# **line con 0**
   R1(config-line)# **password cisco**
   R1(config-line)# **login**
   R1(config-line)# **exit**
   R1(config)#
g. Назначьте **cisco** в качестве пароля виртуального терминала и включите вход по паролю.
   R1(config)# **line vty 0 4**

R1(config-line)# **password cisco**
R1(config-line)# **login**
R1(config-line)# **exit**
R1(config)#

h. Зашифруйте пароли, хранящиеся в открытом виде.
R1(config)# **service password-encryption**

i. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.
R1(config)# **banner motd #**
Enter TEXT message. End with the character '#'.
Unauthorized access prohibited!
#
R1(config)#

j. Настройте и активируйте на маршрутизаторе оба интерфейса.
R1(config)# **int g0/0**
R1(config-if)# **description Connection to PC-B.**
R1(config-if)# **ip address 192.168.0.1 255.255.255.0**
R1(config-if)# **no shut**
R1(config-if)#
*Nov 29 23:49:44.195: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to down
*Nov 29 23:49:47.863: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Nov 29 23:49:48.863: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
R1(config-if)# **int g0/1**
R1(config-if)# **description Connection to S1.**
R1(config-if)# **ip address 192.168.1.1 255.255.255.0**
R1(config-if)# **no shut**
R1(config-if)# **exit**
R1(config)#**exit**

k. Сохраните текущую конфигурацию в файл загрузочной конфигурации.
R1# **copy running-config startup-config**

l. Настройте на маршрутизаторе время.
R1# **clock set 17:00:00 29 Nov 2012**

m. Протестируйте ПК-Б, отправив на ПК-А запрос из окна командной строки.

Приложение Б к лабораторной работе 6. Инициализация и перезагрузка маршрутизатора и коммутатора

Часть 1: Инициализация и перезагрузка маршрутизатора

Шаг 1: Подключитесь к маршрутизатору.

Подключите консоль к маршрутизатору и войдите в привилегированный режим с помощью команды **enable**.

Router>**enable**

Router#

Шаг 2: Удалите файл загрузочной конфигурации из NVRAM.

Введите команду **erase startup-config**, чтобы удалить загрузочную конфигурацию из энергонезависимого ОЗУ (NVRAM).

Router# **erase startup-config**

Шаг 3: Перезагрузите маршрутизатор.

Запустите команду **reload**, чтобы удалить из памяти предыдущую конфигурацию. По запросу перезагрузки нажмите клавишу ВВОД, чтобы подтвердить перезагрузку. Чтобы прервать перезагрузку, нажмите любую клавишу.

Router# **reload**

Примечание. Возможно, появится запрос о сохранении текущей конфигурации перед перезагрузкой маршрутизатора. Чтобы ответить, введите **no** и нажмите клавишу ВВОД.

System configuration has been modified. Save? [yes/no]: **no**

Шаг 4: Пропустите диалоговое окно начальной конфигурации.

После перезагрузки маршрутизатора появится запрос о входе в диалоговое окно начальной конфигурации. Введите **no**и нажмите клавишу ВВОД.

Would you like to enter the initial configuration dialog? [yes/no]:**no**

Шаг 5: Завершите программу автоустановки.

Программа предложит прекратить процесс автоустановки. Ответьте **yes** и нажмите клавишу ВВОД.

Would you like to terminate autoinstall? [yes]:**yes**

Router>

Часть 2: Инициализация и перезагрузка коммутатора

Шаг 1: Подключитесь к коммутатору.

Подключите консоль к коммутатору и войдите в привилегированный режим.

Switch>**enable**

Switch#

Шаг 2: Определите, были ли созданы виртуальные локальные сети (VLAN).

Воспользуйтесь командой **show flash**, чтобы определить, были ли созданы сети VLAN на коммутаторе.

Switch# **show flash**

Шаг 3: Удалите файл виртуальной локальной сети (VLAN).

a. Если файл **vlan.dat**обнаружен во флеш-памяти, удалите этот файл.
   Switch# **delete vlan.dat**
   Будет предложено проверить имя файла. На данном этапе можно изменить имя файла или нажать клавишу ВВОД, если имя введено верно.
b. При запросе удаления этого файла нажмите клавишу ВВОД, чтобы подтвердить удаление. (Чтобы отменить удаление, нажмите любую другую кнопку.)
   Delete flash:/vlan.dat? [confirm]
   Switch#

Шаг 4: Удалите файл загрузочной конфигурации.

Введите команду **erase startup-config**, чтобы удалить файл загрузочной конфигурации из NVRAM. При необходимости удаления файла конфигурации нажмите клавишу ВВОД, чтобы подтвердить удаление. (Чтобы отменить операцию, нажмите любую другую кнопку.)

Switch# **erase startup-config**

Шаг 5: Перезагрузить коммутатор.

Перезагрузите коммутатор, чтобы удалить из памяти всю информацию о предыдущей конфигурации. При необходимости перезагрузки коммутатора нажмите клавишу ВВОД, чтобы продолжить перезагрузку. (Чтобы отменить перезагрузку, нажмите любую другую клавишу.)

Switch# **reload**
Proceed with reload? [confirm]

Примечание. Возможно, появится запрос о сохранении текущей конфигурации перед перезагрузкой коммутатора. Введите **no** и нажмите клавишу ВВОД.

System configuration has been modified. Save? [yes/no]: **no**

Шаг 6: Пропустите диалоговое окно начальной конфигурации.

После перезагрузки коммутатора появится запрос о входе в диалоговое окно начальной конфигурации. Введите **no** в окне запроса и нажмите клавишу ВВОД.

Would you like to enter the initial configuration dialog? [yes/no]: **no**
Switch>

Лабораторная работа 7

НАСТРОЙКА IPV6-АДРЕСОВ НА СЕТЕВЫХ УСТРОЙСТВАХ

7.1. Цель работы

Настройка топологии и конфигурация основных параметров маршрутизатора и коммутатора в соответствии с топологией рис. 10 и таблицей 8. Ручная настройка IPv6-адресов. Проверка сквозного подключения.

7.1.1 Топология

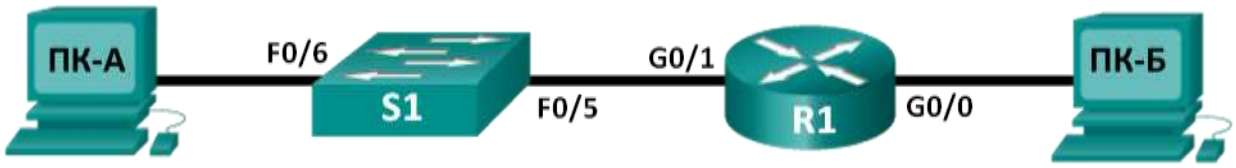

Рис 10 Топология сети

Таблица 8 Таблица адресации

Устройство	Интерфейс	IPv6-адрес	Длина префикса	Шлюз по умолчанию
R1	G0/0	2001:DB8:ACAD:A::1	64	Недоступно
	G0/1	2001:DB8:ACAD:1::1	64	Недоступно
S1	VLAN 1	2001:DB8:ACAD:1::B	64	Недоступно
ПК-А	Сетевой адаптер	2001:DB8:ACAD:1::3	64	FE80::1
ПК-Б	Сетевой адаптер	2001:DB8:ACAD:A::3	64	FE80::1

7.1.2 Задачи

Часть 1. Настройка топологии и конфигурация основных параметров маршрутизатора и коммутатора

Часть 2. Ручная настройка IPv6-адресов

Часть 3. Проверка сквозного подключения

7.1.3 Исходные данные/

Знание особенностей групп многоадресной рассылки протокола Интернета версии 6 (IPv6) пригодится при назначении IPv6-адресов вручную. Понимание того, как назначается многоадресная группа для всех маршрутизаторов и как контролируется назначение адресов для многоадресной группы запрошенных узлов, поможет избежать некоторых проблем маршрутизации IPv6 и обеспечить использование наиболее эффективных методов.

В ходе лабораторной работы вы настроите IPv6-адреса для узлов и интерфейсов устройств и выясните, как назначить маршрутизатору многоадресную группу для всех маршрутизаторов. Для отображения IPv6-адресов одноадресной

передачи и многоадресной рассылки используются команды **show**. Проверить сквозное подключение позволяют команды **ping** и **traceroute**.

7.1.4 Необходимые ресурсы

– 1 маршрутизатор (серия Cisco 1941 с программным обеспечением Cisco IOS версии 15.2(4)M3, универсальный или совместимый образ)

– 1 коммутатор (серия Cisco 2960, с программным обеспечением Cisco IOS версии 15.0(2), образ lanbasek9 или аналогичный)

– Два ПК (Windows 7 с эмулятором терминала, например Tera Term)

– Консольные кабели для настройки устройств Cisco IOS через консольные порты

– Кабели Ethernet в соответствии с топологией

Примечание. Интерфейсы Gigabit Ethernet на маршрутизаторах Cisco 1941 определяют скорость автоматически, поэтому для подключения маршрутизатора к ПК-Б можно использовать прямой кабель Ethernet. При использовании другой модели маршрутизатора Cisco может возникнуть необходимость использовать кроссовый кабель Ethernet.

7.2 Часть 1: Настройка топологии и конфигурация основных параметров маршрутизатора и коммутатора

Шаг 1: Создайте сеть в соответствии с изображенной на схеме топологией.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Шаг 3: Убедитесь в том, что интерфейсы ПК настроены на использование протокола IPv6.

Убедитесь в том, что протокол IPv6 активирован на обоих компьютерах. Для этого проверьте, установлен ли флажок **Протокол Интернета версии 6 (TCP/IPv6)** в окне «Свойства подключения по локальной сети».

Шаг 4: Настройте маршрутизатор.

a. Подключите консоль к маршрутизатору и активируйте привилегированный режим.
b. Назначьте маршрутизатору имя устройства.
c. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверного преобразования введённых команд так, как если бы они были узлами.
d. Назначьте **class** в качестве пароля привилегированного режима.
e. Назначьте **cisco** в качестве пароля консоли и включите вход по паролю.
f. Назначьте **cisco** в качестве пароля виртуального терминала и включите вход по паролю.
g. Зашифруйте пароли, хранящиеся в открытом виде.

h. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.
i. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Шаг 5: Настройте коммутатор.

a. Подключите консоль к коммутатору и активируйте привилегированный режим.
b. Назначьте имя коммутатору.
c. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверного преобразования введённых команд так, как если бы они были узлами.
d. Назначьте **class** в качестве пароля привилегированного режима.
e. Назначьте **cisco** в качестве пароля консоли и включите вход по паролю.
f. Назначьте **cisco** в качестве пароля виртуального терминала и включите вход по паролю.
g. Зашифруйте пароли, хранящиеся в открытом виде.
h. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.
i. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

7.3 Часть 2: Ручная настройка IPv6-адресов

Шаг 1: Присвойте IPv6-адреса Ethernet-интерфейсам на маршрутизаторе R1.

a. Назначьте глобальные IPv6-адреса одноадресной передачи из таблицы маршрутизации каждому из двух Ethernet-интерфейсов маршрутизатора R1.

```
R1(config)# interface g0/0
R1(config-if)# ipv6 address 2001:db8:acad:a::1/64
R1(config-if)# no shutdown
R1(config-if)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# end
R1#
```

b. Введите команду **show ipv6 interface brief**, чтобы проверить, назначен ли каждому интерфейсу действительный IPv6-адрес одноадресной передачи.

```
R1# show ipv6 interface brief
Em0/0                  [administratively down/down]
    unassigned
GigabitEthernet0/0     [up/up]
    FE80::D68C:B5FF:FECE:A0C0
    2001:DB8:ACAD:A::1
GigabitEthernet0/1     [up/up]
```

FE80::D68C:B5FF:FECE:A0C1
2001:DB8:ACAD:1::1
Serial0/0/0 [administratively down/down]
unassigned
Serial0/0/1 [administratively down/down]
unassigned
R1#

c. Введите команду **show ipv6 interface g0/0**. Обратите внимание на то, что в интерфейсе содержатся две многоадресные группы запрошенных узлов, поскольку идентификатор интерфейса локального канала (FE80) IPv6-адреса не был настроен в соответствии с идентификатором интерфейса IPv6-адреса одноадресной передачи вручную.
Примечание. Отображаемый локальный адрес канала основан на адресации EUI-64, которая автоматически использует для создания 128-битного локального IPv6-адреса канала MAC-адрес интерфейса.
R1# **show ipv6 interface g0/0**

d. Чтобы локальный адрес канала соответствовал адресу одноадресной передачи в интерфейсе, вручную введите локальные адреса каналов для каждого из двух Ethernet-интерфейсов маршрутизатора R1.
R1# **config t**
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# interface g0/0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# interface g0/1
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# end
R1#
Примечание. Каждый интерфейс маршрутизатора находится в отдельной сети. Пакеты с локальным адресом канала никогда не покидают локальную сеть, а значит, для обоих интерфейсов можно указывать один и тот же локальный адрес канала.

e. Еще раз введите команду **show ipv6interface g0/0**. Обратите внимание на то, что локальный адрес канала изменился на **FE80::1** и осталась только одна многоадресная группа запрошенных узлов.
R1# **show ipv6 interface g0/0**

Шаг 2: Активируйте IPv6-маршрутизацию на маршрутизаторе R1.

a. В окне командной строки компьютера ПК-Б введите команду **ipconfig**, чтобы получить данные IPv6-адреса, присвоенного интерфейсу компьютера.
Присвоен ли IPv6-адрес одноадресной передачи сетевому адаптеру ПК-Б?

b. Активируйте IPv6-маршрутизацию на маршрутизаторе R1 с помощью команды **IPv6 unicast-routing**.
   R1 # **configure terminal**
   R1(config)# **ipv6 unicast-routing**
   R1(config)# **exit**
   R1#
   *Dec 17 18:29:07.415: %SYS-5-CONFIG_I: Configured from console by console

c. Введите команду **show ipv6 interface g0/0**, чтобы узнать, какие многоадресные группы присвоены интерфейсу G0/0. Обратите внимание на то, что теперь в списке групп для интерфейса G0/0 отображается многоадресная группа всех маршрутизаторов (FF02::2).
   Примечание. Это позволит компьютерам получать IP-адреса и данные основного шлюза автоматически с помощью функции SLAAC (Автоконфигурация без сохранения состояния адреса).
   R1# **show ipv6 interface g0/0**
d. Теперь, когда маршрутизатор R1 входит в многоадресную группу всех маршрутизаторов, ещё раз введите команду **ipconfig** на компьютере ПК-Б. Изучите данные IPv6-адреса.
   Почему компьютер ПК-Б получил глобальный префикс маршрутизации и идентификатор подсети, который вы настроили на маршрутизаторе R1?

Шаг 3: Назначьте IPv6-адреса интерфейсу управления (SVI) на коммутаторе S1.

a. Назначьте полученный IPv6-адрес интерфейсу управления (VLAN 1) на коммутаторе S1. Также назначьте этому интерфейсу локальный адрес канала. Синтаксис команды IPv6 точно такой же, как и на маршрутизаторе.
b. Проверьте правильность назначения IPv6-адресов интерфейсу управления с помощью команды **show ipv6 interface vlan1**.

Шаг 4: Назначьте компьютерам статические IPv6-адреса.

a. На компьютереПК-А откройте окно «Свойства подключения по локальной сети». Выберите **Протокол Интернета версии 6 (TCP/IPv6)** и нажмите кнопку **Свойства**.
b. Установите переключатель **Использовать следующий IPv6-адрес**. Пользуясь таблицей адресации, укажите следующие параметры: **IPv6-адрес**, **Длина префикса подсети** и **Основной шлюз**. Нажмите **OK**.
c. Нажмите кнопку **Закрыть**, чтобы закрыть окно свойств подключения по локальной сети.
d. Повторите шаги с 4a по 4c, чтобы указать статический IPv6-адрес на компьютере ПК-Б. Правильный IPv6-адрес можно найти в таблице адресации.
e. Введите команду **ipconfig** в окне командной строки на компьютере ПК-Б,

чтобы проверить данные IPv6-адреса.

7.4 Часть 3: Проверка сквозного подключения

a. На компьютере ПК-Авведите эхо-запрос **FE80::1**. Это локальный адрес канала, назначенный интерфейсу G0/1 на маршрутизаторе R1.
   Примечание. Для проверки подключения вместо локального адреса канала можно использовать глобальный адрес одноадресной передачи.
b. Отправьте эхо-запрос с помощью команды ping в интерфейс управления коммутатора S1 с компьютера ПК-А.
c. Введите команду **tracert** на ПК-А, чтобы проверить наличие сквозного подключения к компьютеру ПК-Б.
d. С компьютера ПК-Б отправьте эхо-запрос с помощью команды ping на компьютер ПК-А.

Лабораторная работа 8

ТЕСТИРОВАНИЕ СЕТЕВОГО ПОДКЛЮЧЕНИЯ С ПОМОЩЬЮ КОМАНД «PING» И «TRACEROUTE»

8.1. Цель работы

Создание и настройка сети в соответствии с топологией рис. 11 и таблицей 9. Тестирование основной сети с помощью команды «ping». Тестирование основной сети с помощью команд tracert и traceroute. Поиск и устранение неисправностей в топологии

8.1.1 Топология

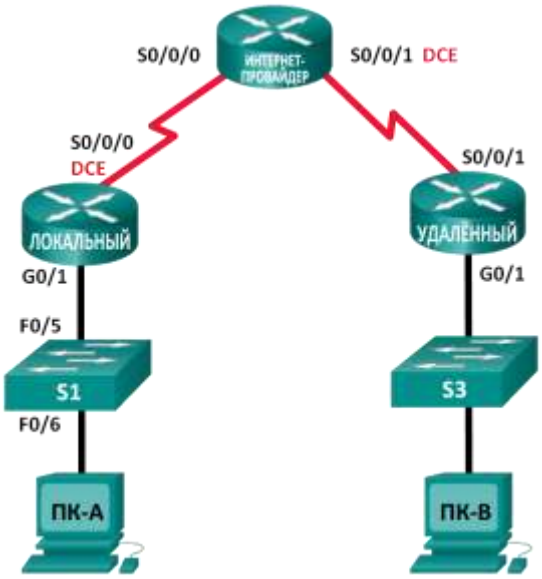

Рис 11 Топология сети

Таблица 9 Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
LOCAL	G0/1	192.168.1.1	255.255.255.0	Недоступно
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Недоступно
ISP	S0/0/0	10.1.1.2	255.255.255.252	Недоступно
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Недоступно
REMOTE	G0/1	192.168.3.1	255.255.255.0	Недоступно
	S0/0/1	10.2.2.1	255.255.255.252	Недоступно
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.3.11	255.255.255.0	192.168.3.1
ПК-А	Сетевой адаптер	192.168.1.3	255.255.255.0	192.168.1.1
ПК-В	Сетевой адаптер	192.168.3.3	255.255.255.0	192.168.3.1

8.1.2 Задачи

Часть 1. Создание и настройка сети

1. Подключите кабели.
2. Настройте компьютеры.
3. Настройте маршрутизаторы.
4. Настройте коммутаторы.

Часть 2. Тестирование основной сети с помощью команды «ping»

1. Отправьте эхо-запрос с помощью команды ping с компьютера.
2. Отправьте эхо-запрос с помощью команды ping с устройств Cisco.

Часть 3. Тестирование основной сети с помощью команд tracert и traceroute

1. Введите команду «tracert» на компьютере.
2. Введите команду «traceroute» на устройствах Cisco.

Часть 4. Поиск и устранение неисправностей в топологии

8.1.3 Исходные данные

Команды «ping» и «traceroute» незаменимы при проверке подключения к сетям TCP/IP. Ping - это утилита администрирования сетей, которая используется для проверки доступности устройств в IP-сети. Кроме того, она определяет время прохождения сигнала для сообщений, отправленных с узла источника на компьютер назначения. Утилита ping доступна в ОС Windows, Unix-подобных операционных системах (OS) и операционной системе сетевого взаимодействия Cisco (IOS).

Traceroute - это утилита сетевой диагностики, отображающая маршрут и измеряющая задержки при передаче пакетов в IP-сетях. Утилита tracert доступна в ОС Windows, а в Unix-подобных операционных системах (OS) и в Cisco IOS используется её аналог - утилита traceroute.

В этой лабораторной работе рассматриваются команды **ping** и **traceroute** и изучаются параметры командной строки, позволяющие изменять их поведение. Для изучения команд в лабораторной работе используются компьютеры и устройства Cisco. На маршрутизаторах Cisco в качестве протокола маршрутизации будет использоваться усовершенствованный протокол внутренней маршрутизации между шлюзами (EIGRP). В лабораторной работе даются необходимые конфигурации для устройств Cisco.

8.1.4 Необходимые ресурсы

– 3 маршрутизатора (Cisco 1941 под управлением системы Cisco IOS версии 15.2(4)M3, универсальный образ или аналогичный)

– 2 коммутатора (Cisco 2960, ПО CISCO IOS версии 15.0(2), образ lanbasek9 или аналогичный)

– 2 ПК (Windows 7, Vista и XP с программой эмуляции терминала, например

Tera Term)

– Консольные кабели для настройки устройств Cisco IOS через консольные порты

– Кабели Ethernet и последовательные кабели, как показано в топологии

–

8.2 Часть 1: Создание и настройка сети

В части 1 вам необходимо создать сеть в топологии и настроить компьютеры и устройства Cisco. Для справки приводятся загрузочные конфигурации маршрутизаторов и коммутаторов. В этой топологии для распределения пакетов между сетями используется протокол EIGRP.

Шаг 1: Создайте сеть в соответствии с изображенной на схеме топологией.

Шаг 2: Удалите настройки на маршрутизаторах и коммутаторах и перезагрузите устройства.

Шаг 3: Настройте IP-адреса и шлюзы по умолчанию для компьютеров в соответствии с таблицей адресации.

Шаг 4: Настройте маршрутизаторы LOCAL (Локальный), ISP (Интернет-провайдер) и REMOTE (Удалённый), используя приведённые ниже загрузочные конфигурации.

Скопируйте и вставьте в окно командной строки режима общих настроек параметры конфигурации для каждого устройства. Сохраните конфигурацию в файл загрузочной конфигурации startup-config.

Загрузочная конфигурация для маршрутизатора LOCAL:

```
hostname LOCAL
no ip domain-lookup
interface s0/0/0
ip address 10.1.1.1 255.255.255.252
 clock rate 56000
 no shutdown
interface g0/1
 ip add 192.168.1.1 255.255.255.0
 no shutdown
router eigrp 1
 network 10.1.1.0 0.0.0.3
 network 192.168.1.0 0.0.0.255
 no auto-summary
```

Загрузочная конфигурация для маршрутизатора ISP:

```
hostname ISP
no ip domain-lookup
interface s0/0/0
 ip address 10.1.1.2 255.255.255.252
```

```
 no shutdown
interface s0/0/1
 ip add 10.2.2.2 255.255.255.252
 clock rate 56000
 no shutdown
router eigrp 1
 network 10.1.1.0 0.0.0.3
 network 10.2.2.0 0.0.0.3
 no auto-summary
end
```

Загрузочная конфигурация для маршрутизатора REMOTE:

```
hostname REMOTE
no ip domain-lookup
interface s0/0/1
 ip address 10.2.2.1 255.255.255.252
 no shutdown
interface g0/1
 ip add 192.168.3.1 255.255.255.0
 no shutdown
router eigrp 1
 network 10.2.2.0 0.0.0.3
 network 192.168.3.0 0.0.0.255
 no auto-summary
end
```

Шаг 5: Настройте загрузочную конфигурацию на коммутаторах S1 и S3.

Загрузочная конфигурация для маршрутизатора S1:

```
hostname S1
no ip domain-lookup
interface vlan 1
 ip add 192.168.1.11 255.255.255.0
 no shutdown
 exit
ip default-gateway 192.168.1.1
end
```

Загрузочная конфигурация для маршрутизатора S3:

```
hostname S3
no ip domain-lookup
interface vlan 1
 ip add 192.168.3.11 255.255.255.0
 no shutdown
```

exit
ip default-gateway 192.168.3.1
end

Шаг 6: Настройте таблицу IP-узлов на маршрутизаторе LOCAL.

Таблица IP-узлов позволяет вместо IP-адреса использовать для подключения удалённого устройства имя узла. Таблица узлов обеспечивает разрешение имён для устройств с перечисленными ниже конфигурациями. Скопируйте и вставьте указанные ниже конфигурации для маршрутизатора LOCAL. Они позволят вводить команды **ping** и **traceroute** на маршрутизаторе LOCAL, используя имена узлов.

ip host REMOTE 10.2.2.1 192.168.3.1
ip host ISP 10.1.1.2 10.2.2.2
ip host LOCAL 192.168.1.1 10.1.1.1
ip host PC-C 192.168.3.3
ip host PC-A 192.168.1.3
ip host S1 192.168.1.11
ip host S3 192.168.3.11
end

8.3 Часть 2: Тестирование основной сети с помощью команды ping

В части 2 лабораторной работы необходимо проверить сквозное подключение с помощью команды **ping**. Утилита ping отправляет пакеты протокола управляющих сообщений в Интернете (ICMP) на целевой узел, а затем ожидает ответа ICMP. Утилита фиксирует как время прохождения сигнала туда и обратно, так и потери пакетов.

Вы проанализируете результаты выполнения команды **ping** и другие параметры утилиты, доступные на компьютерах под управлением Windows и устройствах Cisco.

Шаг 1: Проверьте сетевое подключение из сети LOCAL, используя компьютер ПК-А.

Все эхо-запросы с помощью команды ping с ПК-А на другие устройства в топологии должны быть успешными. Если это не так, проверьте топологию и подключение кабелей, а также настройки устройств Cisco и компьютеров.

a. Отправьте эхо-запрос с помощью команды ping с ПК-А на шлюз по умолчанию (интерфейс GigabitEthernet 0/1 маршрутизатора LOCAL).

C:\Users\User1>**ping 192.168.1.1**

В этом примере отправлено четыре (4) запроса ICMP по 32 байта каждый, а ответы получены менее чем через одну миллисекунду без потерь пакетов. Время передачи и получения ответов растёт по мере увеличения количества устройств, которые обрабатывают запросы и ответы ICMP в процессе их передачи к месту назначения и обратно.

b. Отправьте с компьютера ПК-А эхо-запросы с помощью команды ping на адреса, указанные в приведённой ниже таблице 10 , и запишите среднее время прохождения сигнала и существования (TTL).

Таблица 10

Назначение	Среднее время прохождения сигнала (мс)	TTL
192.168.1.1 (LOCAL)		
192.168.1.11 (S1)		
10.1.1.1 (LOCAL)		
10.1.1.2 (ISP)		
10.2.2.2 (ISP)		
10.2.2.1 (REMOTE)		
192.168.3.1 (REMOTE)		
192.168.3.11 (S3)		
192.168.3.3 (PC-C)		

Обратите внимание на среднее время прохождения сигнала при отправке запроса на адрес 192.168.3.3 (ПК-В). Время увеличилось, поскольку до того, как ПК-А получил ответ от ПК-В, запросы ICMP обрабатывались тремя маршрутизаторами.

C:\Users\User1>**ping 192.168.3.3**

Шаг 2: Отправьте расширенные команды ping с компьютера.

Используемая по умолчанию команда **ping** отправляет четыре запроса по 32 байта каждый. Ответ на каждый запрос ожидается в течение 4000 мс (4 с), после чего отображается сообщение Request timed out (Время запроса превышено). Для устранения неполадок в сети параметры команды **ping** можно настроить более точно.

a. В командной строке введите команду **ping** и нажмите клавишу ВВОД.

C:\Users\User1>**ping**

b. Используя параметр **–t**, отправьте эхо-запрос с помощью команды ping на компьютер ПК-В, чтобы проверить его доступность.

C:\Users\User1>**ping –t 192.168.3.3**

Чтобы проиллюстрировать результаты запроса в случае недоступности узла, отсоедините кабель между маршрутизатором REMOTE и коммутатором S3 или отключите интерфейс GigabitEthernet 0/1 на маршрутизаторе REMOTE.

Пока сеть функционирует нормально, с помощью команды **ping** можно определить, поступает ли ответ от узла назначения и через какое время. В случае проблем с сетевым подключением команда **ping** выдаёт сообщение об ошибке.

c. Перед тем, как перейти к следующему шагу, снова подключите Ethernet-кабель или активируйте интерфейс GigabitEthernet на маршрутизаторе

REMOTE (с помощью команды **no shutdown**). Через 30 секунд эхо-запрос с помощью команды ping снова должен быть успешным.

d. Чтобы остановить команду ping, нажмите клавиши **Ctrl**+**C**.

Шаг 3: Проверьте сетевое подключение из сети LOCAL, используя устройства Cisco.

Команду **ping** можно использовать и на устройствах Cisco. В этом шаге рассматривается выполнение команды **ping** на маршрутизаторе LOCAL и коммутаторе S1.

a. С маршрутизатора LOCAL отправьте эхо-запрос с помощью команды ping на компьютер ПК-B в сети REMOTE, используя IP-адрес 192.168.3.3.

LOCAL# **ping 192.168.3.3**

Восклицательный знак (!) показывает, что эхо-запрос с помощью команды ping с маршрутизатора LOCAL на ПК-B прошёл успешно. Сигнал проходит туда и обратно в среднем за 64 мс без потерь пакетов, о чём свидетельствует выполнение всех запросов.

b. Поскольку на маршрутизаторе LOCAL настроена таблица локальных узлов, эхо-запрос с помощью команды ping на ПК-B в сети REMOTE можно отправить, используя имя узла для маршрутизатора LOCAL.

LOCAL# **ping PC-C**

c. Для команды **ping** доступны дополнительные параметры. В командной строке введите команду **ping и** нажмите клавишу ВВОД. Введите **192.168.3.3** или **PC-C** (ПК-B) в поле Target IP address (Целевой IP-адрес). Нажмите клавишу ВВОД, чтобы принять значение по умолчанию для других параметров.

```
LOCAL# ping
Protocol [ip]:
Target IP address: PC-C
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/63/64 ms
```

d. Если в сети возникают проблемы, можно отправить расширенный эхо-запрос с помощью команды ping. Отправьте команду **ping** на адрес 192.168.3.3 с числом повторов 500. Затем отсоедините кабель между маршрутизатором REMOTE и коммутатором S3 или отключите интерфейс GigabitEthernet 0/1 на маршрутизаторе REMOTE.

Когда вместо восклицательных знаков (!) появятся буква U и точки (.), снова подключите Ethernet-кабель или активируйте интерфейс GigabitEthernet на маршрутизаторе REMOTE. Через 30 секунд эхо-запрос с помощью команды ping снова должен быть успешным. Нажмите клавиши **Ctrl**+**Shift**+**6**, чтобы остановить команду **ping**.

```
LOCAL# ping
Protocol [ip]:
Target IP address: 192.168.3.3
Repeat count [5]: 500
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 500, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
Success rate is 95 percent (479/500), round-trip min/avg/max = 60/63/72 ms
```

Буква U в результатах выполнения команды означает, что узел назначения не может быть достигнут. Маршрутизатор LOCAL получил протокольный блок данных (PDU) с ошибкой. Каждая точка (.) в полученных результатах означает, что в процессе ожидания ответа от ПК-B время эхо-запроса с помощью команды ping истекло. В этом примере за время моделирования сбоев в сети были потеряны 5 % пакетов.

Примечание. Такие же результаты позволит получить следующая команда:

```
LOCAL# ping 192.168.3.3 repeat 500
```

или

```
LOCAL# ping PC-C repeat 500
```

e. Кроме того, для проверки сетевого подключения можно использовать коммутатор. В этом примере коммутатор S1 отправляет эхо-запрос с помощью команды ping на коммутатор S3 в сети REMOTE.

```
S1# ping 192.168.3.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 67/67/68 ms
```

Команда **ping** чрезвычайно полезна при поиске и устранении неполадок сетевого подключения. Однако, если запрос не проходит, узнать место возникновения проблемы с помощью этой команды нельзя. Отобразить информацию о маршруте и задержках в сети позволяет команда **tracert** (или **traceroute**).

8.4 Часть 3 Тестирование основной сети с помощью команд tracert и

traceroute

Команды для отслеживания маршрутов доступны на компьютерах и сетевых устройствах. На компьютере под управлением ОС Windows команда **tracert** отслеживает путь к узлу назначения, используя сообщения ICMP. Команда **traceroute** отслеживает маршруты к узлам назначения на устройствах Cisco и компьютерах под управлением Unix-подобных операционных систем, используя датаграммы UDP.

В части 3 вы изучите команды traceroute и определите путь, который проходит пакет до узла назначения. На компьютерах под управлением Windows вы будете использовать команду **tracert**, а на устройствах Cisco - команду **traceroute**. Вы также рассмотрите параметры, доступные для точной настройки результатов traceroute.

Шаг 1: Отправьте команду tracert с компьютера ПК-А на компьютер ПК-В.

В командной строке введите **tracert 192.168.3.3**.

```
C:\Users\User1>tracert 192.168.3.3
Tracing route to PC-C [192.168.3.3]
Over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms    192.168.1.1
  2    24 ms    24 ms    24 ms    10.1.1.2
  3    48 ms    48 ms    48 ms    10.2.2.1
  4    59 ms    59 ms    59 ms    PC-C [192.168.3.3]

Trace complete.
```

Согласно результатам выполнения команды tracert, от ПК-А до ПК-В данные прошли следующий путь: ПК-А - маршрутизатор LOCAL - маршрутизатор ISP - маршрутизатор REMOTE - ПК-В. Маршрут к узлу назначения ПК-В прошёл через три маршрутизатора.

Шаг 2: Изучите дополнительные параметры команды tracert.

a. В командной строке введите команду **tracert** и нажмите клавишу ВВОД.

```
C:\Users\User1>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
   -d                 Do not resolve addresses to hostnames.
   -h maximum_hops    Maximum number of hops to search for target.
   -j host-list       Loose source route along host-list (IPv4-only).
   -w timeout         Wait timeout milliseconds for each reply.
```

-R Trace round-trip path (IPv6-only).
-S srcaddr Source address to use (IPv6-only).
-4 Force using IPv4.
-6 Force using IPv6.

b. Используйте параметр **-d**. Обратите внимание на то, что IP-адрес 192.168.3.3 не определяется как ПК-B.

C:\Users\User1>**tracert –d 192.168.3.3**
Tracing route to 192.168.3.3over a maximum of 30 hops:

1	<1 ms	<1 ms	<1 ms	192.168.1.1
2	24 ms	24 ms	24 ms	10.1.1.2
3	48 ms	48 ms	48 ms	10.2.2.1
4	59 ms	59 ms	59 ms	192.168.3.3

Trace complete.

Шаг 3: Отправьте команду traceroute с маршрутизатора LOCAL на ПК-B.

a. В командной строке маршрутизатора LOCAL введите **traceroute 192.168.3.3** или **traceroute PC-C**. Имена узлов будут определены, поскольку на маршрутизаторе LOCAL настроена таблица локальных IP-узлов.

LOCAL# **traceroute 192.168.3.3**
Type escape sequence to abort.
Tracing the route to PC-C (192.168.3.3)
VRF info: (vrf in name/id, vrf out name/id)
1 ISP (10.1.1.2) 16 msec 16 msec 16 msec
2 REMOTE (10.2.2.1) 28 msec 32 msec 28 msec
3 PC-C (192.168.3.3) 32 msec 28 msec 32 msec

LOCAL# **traceroute PC-C**
Type escape sequence to abort.
Tracing the route to PC-C (192.168.3.3)
VRF info: (vrf in name/id, vrf out name/id)
1 ISP (10.1.1.2) 16 msec 16 msec 16 msec
2 REMOTE (10.2.2.1) 28 msec 32 msec 28 msec
3 PC-C (192.168.3.3) 32 msec 32 msec 28 msec

Шаг 4: Отправьте команду traceroute с коммутатора S1 на ПК-B.

b. На коммутаторе S1 введите **traceroute 192.168.3.3**. В результатах выполнения программы traceroute имена узлов не отображаются, поскольку на этом коммутаторе таблица локальных IP-узлов не настроена.

S1# **traceroute 192.168.3.3**
Type escape sequence to abort.

Tracing the route to 192.168.3.3
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.1.1 1007 msec 0 msec 0 msec
2 10.1.1.2 17 msec 17 msec 16 msec
3 10.2.2.1 34 msec 33 msec 26 msec
4 192.168.3.3 33 msec 34 msec 33 msec

Команда **traceroute** имеет дополнительные параметры. Чтобы их посмотреть, после ввода команды **traceroute в** командной строке введите знак вопроса **?** или просто нажмите клавишу ВВОД.

8.5 Часть 4: Поиск и устранение неисправностей в топологии

Шаг 1: Удалите неисправности в топологии на маршрутизаторе REMOTE.

Шаг 2: Перезагрузите маршрутизатор REMOTE.

Шаг 3: Скопируйте и вставьте в маршрутизатор REMOTE указанную ниже конфигурацию.

```
hostname REMOTE
no ip domain-lookup
interface s0/0/1
 ip address 10.2.2.1 255.255.255.252
 no shutdown
interface g0/1
 ip add 192.168.8.1 255.255.255.0
 no shutdown
router eigrp 1
 network 10.2.2.0 0.0.0.3
 network 192.168.3.0 0.0.0.255
 no auto-summary
end
```

Шаг 4: Из сети LOCAL отправьте команды ping и tracert или traceroute, чтобы найти и устранить проблемы в сети REMOTE.

a. На компьютере ПК-А введите команды **ping** и **tracert**.

Команду **tracert** можно использовать для проверки сквозного сетевого подключения. В данном случае результаты выполнения команды tracert показывают, что компьютер ПК-А достигает шлюза по умолчанию с адресом 192.168.1.1, но не может подключиться к ПК-В.

C:\Users\User1>**tracert 192.168.3.3**

Tracing route to 192.168.3.3 over a maximum of 30 hops
1 <1 ms <1 ms <1 ms 192.168.1.1
2 192.168.1.1 reports: Destination host unreachable.

Trace complete.

Один из способов обнаружения проблемы в сети - это эхо-запрос с помощью команды ping на каждый встречающийся в сети переход на пути к ПК-B. Сначала выясните, может ли компьютер ПК-A подключиться к интерфейсу Serial 0/0/1 маршрутизатора ISP с IP-адресом 10.2.2.2.

C:\Users\Utraser1>**ping 10.2.2.2**

Эхо-запрос с помощью команды ping к маршрутизатору ISP прошёл успешно. Следующий переход в сети - маршрутизатор REMOTE. Отправьте эхо-запрос с помощью команды ping на интерфейс Serial 0/0/1 маршрутизатора REMOTE с IP-адресом 10.2.2.1.

C:\Users\User1>**ping 10.2.2.1**

Компьютер ПК-A достигает маршрутизатора REMOTE. Судя по успешному прохождению эхо-запроса с помощью команды ping с компьютера ПК-A на маршрутизатор REMOTE, проблема с подключением связана с сетью 192.168.3.0/24. Отправьте эхо-запрос с помощью команды ping на шлюз ПК-B по умолчанию, в качестве которого выступает интерфейс GigabitEthernet 0/1 маршрутизатора REMOTE.

C:\Users\User1>**ping 192.168.3.1**

Как видно из результатов выполнения команды **ping**, компьютер ПК-A не может подключиться к интерфейсу GigabitEthernet 0/1 маршрутизатора REMOTE.

Чтобы проверить сетевое подключение, с компьютера ПК-A можно также отправить эхо-запрос с помощью команды ping на коммутатор S3 - для этого в командной строке введите **ping 192.168.3.11**. Поскольку ПК-A не может подключиться к интерфейсу GigabitEthernet 0/1 маршрутизатора REMOTE, эхо-запрос с помощью команды ping с ПК-A на коммутатор S3, скорее всего, не пройдёт, что и показывают приведённые ниже результаты.

C:\Users\User1>**ping 192.168.3.11**

Результаты выполнения команд tracert и ping говорят о том, что компьютер ПК-A подключается к маршрутизаторам LOCAL, ISP и REMOTE, но не может связаться с ПК-B, коммутатором S3 или шлюзом ПК-B по умолчанию.

b. Проверьте текущие параметры конфигурации маршрутизатора REMOTE с помощью команд **show**.

REMOTE# **show ip interface brief**

10.2.2.1 YES manual up up

REMOTE# **show run**

Результаты выполнения команд **show run** и **show ip interface brief** показывают, что интерфейс GigabitEthernet 0/1 функционирует нормально (up/up), но IP-адрес в нём указан неправильно.

c. Укажите правильный IP-адрес для интерфейса GigabitEthernet 0/1.

REMOTE# **configure terminal**
Enter configuration commands, one per line. End with CNTL/Z.
REMOTE(config)# **interface GigabitEthernet 0/1**
REMOTE(config-if)# **ip address 192.168.3.1 255.255.255.0**

d. Убедитесь в том, что компьютер ПК-A может отправлять команды ping и tracert на ПК-B.

C:\Users\User1>**ping 192.168.3.3**
Pinging 192.168.3.3 with 32 bytes of data:
Reply from 192.168.3.3: bytes=32 time=44ms TTL=125

Лабораторная работа 9

Разработка и внедрение схемы адресации разделённой на подсети IPv4-сети

9.1. Цель работы

Проверка сети и устранение неполадок. Настройка устройств с топологией рис. 12 и таблицей 11. Разработка схемы разделения сети на подсети

9.1.1 Топология

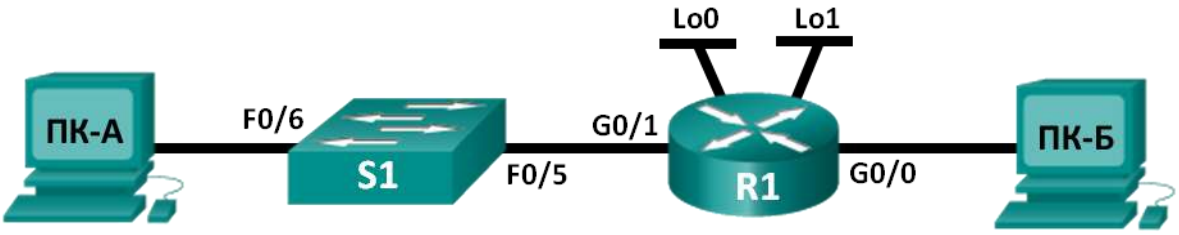

Рис 12 Топология сети

Таблица 11 Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0			Недоступно
	G0/1			Недоступно
	Lo0			Недоступно
	Lo1			Недоступно
S1	VLAN 1	Недоступно	Недоступно	Недоступно
ПК-А	Сетевой адаптер			
ПК-Б	Сетевой адаптер			

9.1.2 Задачи

Часть 1. Разработка схемы разделения сети на подсети

1. Создайте схему разделения на подсети, которая соответствует количеству подсетей и адресов узлов.
2. Заполните диаграмму, указав, где будут применяться IP-адреса узлов.

Часть 2. Настройка устройств

1. Назначьте компьютерам IP-адреса, маски подсети и шлюзы по умолчанию.
2. Настройте IP-адреса и маски подсети для интерфейсов Gigabit Ethernet маршрутизатора.
3. На маршрутизаторе создайте два логических интерфейса loopback и настройте для каждого из них IP-адрес и маску подсети.

Часть 3. Проверка сети и устранение неполадок

Проверьте подключение и устраните неполадки, используя команду ping.

9.1.3 Исходные данные/

В этой лабораторной работе вам нужно будет разделить сеть, начиная с адреса и маски одной сети, на несколько подсетей. При создании схемы подсети необходимо учитывать количество компьютеров каждой подсети и другие аспекты, например дальнейшее расширение узлов в сети.

После того как вы составите схему разделения на подсети и диаграмму сети и укажете IP-адреса узлов и интерфейсов, вам нужно будет настроить компьютеры и интерфейсы маршрутизаторов, включая логические интерфейсы loopback. Интерфейсы loopback создаются для моделирования дополнительных локальных сетей, подключённых к маршрутизатору R1.

После того как сетевые устройства и компьютеры будут настроены, вы проверите сетевые подключения с помощью команды **ping.**

Эта лабораторная работа содержит минимум инструкций по выполнению команд, необходимых для настройки маршрутизатора. Список требуемых команд приведён в приложении А. Проверьте свои знания и попробуйте настроить устройства, не пользуясь приложениями.

Необходимые ресурсы

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

Примечание. Интерфейсы Gigabit Ethernet на маршрутизаторах Cisco 1941 определяют скорость автоматически, поэтому для подключения маршрутизатора к ПК-Б можно использовать прямой кабель Ethernet. При использовании маршрутизатора Cisco другой модели может потребоваться кроссовый кабель Ethernet.

9.2 Часть 1: Разработка схемы разделения сети на подсети

Шаг 1: Создайте схему разделения на подсети, которая соответствует необходимому количеству подсетей и адресов узлов.

В этом сценарии вы выступаете в роли сетевого администратора, работающего в

небольшом филиале крупной компании. Вам необходимо создать несколько подсетей в пространстве сетевого адреса 192.168.0.0/24, выполнив следующие требования:

Первая подсеть - это сеть для сотрудников. Необходимо не меньше 25 IP-адресов узлов.

Вторая подсеть - сеть администрирования. Необходимо не меньше 10 IP-адресов узлов.

Третья и четвёртая подсети зарезервированы как виртуальные сети на интерфейсах виртуальных маршрутизаторов, loopback 0 и loopback 1. Интерфейсы виртуальных маршрутизаторов используются для моделирования локальных сетей, подключённых к маршрутизатору R1.

Вам также необходимы две дополнительные неиспользуемые подсети для дальнейшего расширения сети.

Примечание. Маски подсети переменной длины использоваться не будут. Все маски подсети для устройств будут иметь одинаковую длину.

Составить схему разделения на подсети, отвечающую указанным условиям, помогут приведённые ниже вопросы.

1) Сколько адресов узлов необходимо для самой крупной подсети?
2) Каково минимальное количество необходимых подсетей?
3) Сеть, которую необходимо разделить на подсети, имеет адрес 192.168.0.0/24. Как маска подсети /24 будет выглядеть в двоичном формате?
4) Маска подсети состоит из двух частей - сетевой и узловой. В двоичном формате они представлены в маске подсети единицами и нулями.
   Что в маске сети представляют единицы?
   Что в маске сети представляют нули?
5) Чтобы разделить сеть на подсети, биты из узловой части исходной маски сети заменяются битами подсети. Количество битов подсетей определяет количество подсетей. Если каждая из возможных масок подсети представлена в указанном двоичном формате, сколько подсетей и сколько узлов будет создано в каждом примере?

   Совет: помните, что количество битов узлов (во второй степени) определяет количество узлов для каждой подсети (минус 2), а количество битов подсетей (во второй степени) определяет количество подсетей. Биты подсетей (выделены полужирным шрифтом) - это биты, заимствованные за пределами исходной маски подсети /24. /24 - префиксная запись с косой чертой, которая соответствует десятичному представлению маски 255.255.255.0.

   (/25) 11111111.11111111.11111111.**1**0000000

Эквивалент десятичного представления маски подсети с разделением точками:

Количество подсетей? Количество узлов?

(/26) 11111111.11111111.11111111.11000000

Эквивалент десятичного представления маски подсети с разделением точками:

Количество подсетей? Количество узлов?

(/27) 11111111.11111111.11111111.11100000

Эквивалент десятичного представления маски подсети с разделением точками:

Количество подсетей? Количество узлов?

(/28) 11111111.11111111.11111111.11110000

Эквивалент десятичного представления маски подсети с разделением точками:

Количество подсетей? Количество узлов?

(/29) 11111111.11111111.11111111.11111000

Эквивалент десятичного представления маски подсети с разделением точками:

Количество подсетей? Количество узлов?

(/30) 11111111.11111111.11111111.11111100

Эквивалент десятичного представления маски подсети с разделением точками:

Количество подсетей? Количество узлов?

1) Учитывая ваши ответы, какие маски подсети соответствуют минимальному необходимому количеству адресов узлов?

2) Учитывая ваши ответы, какие маски подсети соответствуют минимальному необходимому количеству подсетей?

3) Учитывая ваши ответы, какая маска подсети соответствует минимальному необходимому количеству как узлов, так и подсетей?

4) Выяснив, какая маска подсети соответствует всем указанным требованиям к сети, вы определите каждую подсеть, начиная с исходного сетевого адреса. Ниже перечислите все подсети от первой до последнейи запишите их в таблицу12. Помните, что первая подсеть - 192.168.0.0 с новой полученной маской подсети.

Таблица 12 Таблица адресов.

Адрес подсети/Префикс	Маска подсети (десятичное представление с точками)

Шаг 2: Заполните таблицу, указав, где будут применяться IP-адреса узлов.

В приведённых ниже строках укажите IP-адреса и маски подсетей в виде префиксной записи с косой чертой. На маршрутизаторе укажите первый допустимый адрес в каждой подсети для каждого интерфейса - Gigabit Ethernet 0/0, Gigabit Ethernet 0/1, loopback 0 и loopback 1. Впишите IP-адрес для каждого компьютера (ПК-А и ПК-Б) Внесите эти данные в таблицу адресации 11.

9.3 Часть 2: Настройка устройств

В части 2 вам нужно настроить топологию сети и основные параметры на компьютерах и маршрутизаторе, такие как IP-адреса интерфейса Gigabit Ethernet и компьютеров, маски подсети и шлюзы по умолчанию. Имена устройств и IP-адреса указаны в таблице адресации.

Примечание. В приложении А лабораторной работе 9 приведены сведения о конфигурации для выполнения шагов в части 2. Постарайтесь выполнить задания в части 2, не пользуясь приложением А.

Шаг 1: Настройте маршрутизатор.

a. Войдите в привилегированный режим, а затем в режим глобальной конфигурации.
b. Укажите **R1** в качестве имени узла для маршрутизатора.
c. Укажите и активируйте IP-адреса и маски подсети для интерфейсов **G0/0** и **G0/1**.
d. Интерфейсы loopback создаются для моделирования дополнительных локальных сетей, подключённых к маршрутизатору R1. Укажите IP-адреса и маски подсети для интерфейсов loopback. Созданные интерфейсы loopback по умолчанию будут активны. (Чтобы создать адреса loopback, введите команду **interface loopback 0** в режиме глобальной конфигурации.)

   Примечание. При необходимости можно создать дополнительные адреса loopback для проверки в различных схемах адресации.
e. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Шаг 2: Настройте интерфейсы ПК.

f. Настройте на ПК-А IP-адрес, маску подсети и параметры шлюза по умолчанию.
g. Настройте на ПК-Б IP-адрес, маску подсети и параметры шлюза по умолчанию.

Часть 3: Проверка сети и устранение неполадок

В части 3 вы проверите подключение сети с помощью команды **ping**.

a. Проверьте, может ли ПК-А установить связь со своим шлюзом по умолчанию. На ПК-А откройте окно командной строки и отправьте эхо-запрос с помощью команды ping на IP-адрес интерфейса Gigabit Ethernet 0/1 маршрутизатора. Получен ли ответ?

b. Проверьте, может ли ПК-Б установить связь со своим шлюзом по умолчанию. На ПК-Б откройте окно командной строки и отправьте эхо-запрос с помощью команды ping на IP-адрес интерфейса Gigabit Ethernet 0/0 маршрутизатора. Получен ли ответ?
c. Проверьте, может ли ПК-А установить связь с ПК-Б. На ПК-А откройте окно командной строки и отправьте эхо-запрос с помощью команды ping на IP-адрес компьютера ПК-Б. Получен ли ответ?
d. Если вы ответили отрицательно на любой из заданных выше вопросов, вернитесь назад и проверьте введённые IP-адреса и маски подсети, а также убедитесь в том, что шлюзы по умолчанию ПК-А и ПК-Б правильно настроены.
e. Если все параметры указаны верно, но эхо-запросы с помощью команды ping по-прежнему не проходят, проверьте дополнительные факторы, которые могут блокировать сообщения по протоколу ICMP. На ПК-А и ПК-Б под управлением ОС Windows убедитесь в том, что межсетевой экран Windows для сетей типа «Домашняя», «Сеть предприятия» и «Общественная» отключён.
f. Попробуйте ввести заведомо неправильный адрес шлюза на ПК-А, указав значение 10.0.0.1. Что происходит при попытке отправить эхо-запрос с помощью команды ping с ПК-Б на ПК-А? Получен ли ответ?

Вопросы на закрепление

1. Разбиение одной крупной сети на несколько подсетей обеспечивает более высокую гибкость и безопасность сетевой архитектуры. Тем не менее, подумайте и назовите, какие недостатки могут возникнуть, если все подсети должны иметь одинаковые размеры? Как вы считаете, почему в качестве IP-адреса шлюза по умолчанию или маршрутизатора обычно используется первый пригодный IP-адрес в сети?Сводная таблица интерфейса маршрутизатора

Приложение к лабораторной работе 9. Сведения о конфигурации для выполнения шагов в части 2

Шаг 1: Настройте маршрутизатор.

a. Подключите консоль к маршрутизатору и активируйте привилегированный режим.
   Router>**enable**
   Router#
b. Войдите в режим конфигурации.
   Router# **conf t**
   Enter configuration commands, one per line. End with CNTL/Z.
   Router(config)#
c. Назначьте маршрутизатору имя устройства.

Router(config)# **hostname R1**
R1(config)#

d. Укажите и активируйте IP-адреса и маски подсети для интерфейсов **G0/0** и **G0/1**.

R1(config)# **interface g0/0**
R1(config-if)# **ip address <ip address><subnet mask>**
R1(config-if)# **no shutdown**
R1(config-if)# **interface g0/1**
R1(config-if)# **ip address <ip address><subnet mask>**
R1(config-if)# **no shutdown**

e. Интерфейсы loopback создаются для моделирования дополнительных локальных сетей, подключаемых к маршрутизатору R1. Укажите IP-адреса и маски подсети для интерфейсов loopback. Созданные интерфейсы loopback по умолчанию будут активны.

R1(config)# **interface loopback 0**
R1(config-if)# **ip address <ip address><subnet mask>**
R1(config-if)# **interface loopback 1**
R1(config-if)# **ip address <ip address><subnet mask>**
R1(config-if)# **end**

Шаг 2: Настройте интерфейсы ПК.

a. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

R1# **copy running-config startup-config**

b. Настройте на ПК-А IP-адрес, маску подсети и параметры шлюза по умолчанию.

c. Настройте на ПК-Б IP-адрес, маску подсети и параметры шлюза по умолчанию.

Лабораторная работа 10

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СЕТЕВЫХ УСТРОЙСТВ

10.1. Цель работы

Настройка топологии и инициализация устройств. Настройка основных мер обеспечения безопасности на маршрутизаторе и коммутаторе в соответствии с топологией рис. 13 и таблицей 13.

10.1.1 Топология

Рис 13 Топология сети

Таблица 13 Таблица адресации

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

10.1.2 Задачи

Часть 1. Настройка основных параметров устройства

Часть 2. Настройка основных мер обеспечения безопасности на маршрутизаторе

Часть 3. Настройка основных мер обеспечения безопасности на коммутаторе

10.1.3 Исходные данные

Все сетевые устройства рекомендуется настраивать с использованием хотя бы минимального набора эффективных команд обеспечения безопасности. Это относится к устройствам конечных пользователей, серверам и сетевым устройствам, таким как маршрутизаторы и коммутаторы.

В ходе лабораторной работы вы должны будете настроить сетевые устройства в топологии таким образом, чтобы принимать SSH-сеансы для удалённого управления. Кроме того, вы настроите основные эффективные меры обеспечения безопасности через интерфейс командной строки IOS CLI. Затем вам необходимо будет протестировать меры обеспечения безопасности и убедиться в том, что они реализованы должным образом и работают без ошибок.

Примечание. Маршрутизаторы, используемые на практических занятиях CCNA, - Cisco 1941, ПО Cisco IOS версии 15.2(4)M3 (образ universalk9). Используемые коммутаторы: семейство коммутаторов Cisco Catalyst 2960 версии CISCO IOS 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии ПО Cisco IOS. В зависимости от модели и версии Cisco IOS выполняемые доступные команды и выводы могут отличаться от данных, полученных в ходе лабораторных работ. Точные идентификаторы интерфейсов указаны в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что информация, имеющаяся на маршрутизаторе и коммутаторе, удалена и они не содержат файлов загрузочной конфигурации. Если вы не уверены, что сможете это сделать, обратитесь к преподавателю.

10.1.4 Необходимые ресурсы

1 маршрутизатор (серия Cisco 1941 с программным обеспечением Cisco IOS версии 15.2(4)M3, универсальный или совместимый образ)

1 коммутатор (серия Cisco 2960, с программным обеспечением Cisco IOS версии 15.0(2), образ lanbasek9 или аналогичный)

1 ПК (Windows 7, Vista или XP с программой эмулятора терминала, например Tera Term)

Консольные кабели для настройки устройств Cisco IOS через консольные порты

Кабели Ethernet в соответствии с топологией

10.2 Часть 1: Основные настройки устройства

В части 1 потребуется настройка топологии сети и основных параметров, таких как IP-адреса интерфейсов, доступ к устройствам и пароли на маршрутизаторе.

Шаг 1: Создайте сеть в соответствии с изображенной на схеме топологией.

Подключайте отображаемые в топологии устройства, а также кабель по мере необходимости.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Шаг 3: Настройте маршрутизатор.

Справку по командам, необходимым для протокола SSH, см. в предыдущей лабораторной работе.

d. Подключите консоль к маршрутизатору и активируйте привилегированный режим.
e. Войдите в режим конфигурации.
f. Присвойте маршрутизатору имя R1.
g. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверного преобразования введённых команд так, как если бы они были узлами.
h. Назначьте **class** в качестве пароля привилегированного режима.

i. Назначьте **cisco** в качестве пароля консоли и включите вход по паролю.
j. Назначьте **cisco** в качестве пароля виртуального терминала и включите вход по паролю.
k. Зашифруйте пароли, хранящиеся в открытом виде.
l. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.
m. Настройте и активируйте интерфейс маршрутизатора G0/1 с помощью сведений, содержащихся в таблице адресации.
n. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Шаг 4: Настройте коммутатор.

o. Подключите консоль к коммутатору и активируйте привилегированный режим.
p. Войдите в режим конфигурации.
q. Присвойте коммутатору имя S1.
r. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверного преобразования введённых команд так, как если бы они были узлами.
s. Назначьте **class** в качестве пароля привилегированного режима.
t. Назначьте **cisco** в качестве пароля консоли и включите вход по паролю.
u. Назначьте **cisco** в качестве пароля виртуального терминала и включите вход по паролю.
v. Зашифруйте пароли, хранящиеся в открытом виде.
w. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.
x. Присвойте интерфейсу SVI, который используется по умолчанию, IP-адрес из таблицы адресации.
y. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

10.3 Часть 2: Настройка основных мер безопасности на маршрутизаторе

Шаг 1: Используйте надёжные пароли.

Администратор должен следить за тем, чтобы пароли отвечали стандартным рекомендациям по созданию надёжных паролей. Рекомендации могут включать сочетание в пароле букв, цифр и специальных символов и определять его минимальную длину.

Примечание. Согласно рекомендациям по обеспечению эффективной работы в производственной среде необходимо использовать надёжные пароли, такие как приводятся в этой лабораторной работе. Однако для простоты выполнения лабораторных работ в данном курсе используются пароли cisco и class.

a. Чтобы соблюсти рекомендации, измените зашифрованный пароль привилегированного режима.

   R1(config)# **enable secret Enablep@55**

b. Укажите, что пароль должен включать не менее десяти символов.
R1(config)# **security passwords min-length 10**

Шаг 2: Активируйте подключения SSH.

a. В качестве имени домена укажите **CCNA-lab.com**.
R1(config)# **ip domain-name CCNA-lab.com**
b. Создайте в базе данных локальных пользователей запись, которая будет использоваться при подключении к маршрутизатору через SSH. Пароль должен соответствовать стандартам надёжных паролей, а пользователь - иметь права доступа уровня администратора.
R1(config)# **username admin privilege 15 secret Admin15p@55**
c. Настройте транспортный ввод для vty-линий таким образом, чтобы они могли принимать подключения SSH, но не разрешайте подключения Telnet.
R1(config)# **line vty 0 4**
R1(config-line)# **transport input ssh**
d. Для проверки подлинности в vty-линиях должна использоваться база данных локальных пользователей.
R1(config-line)# **login local**
R1(config-line)# **exit**
e. Создайте ключ шифрования RSA с длиной 1024 бит.
R1(config)# **crypto key generate rsa modulus 1024**
The name for the keys will be: R1.CCNA-lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)

R1(config)#
*Jan 31 17:54:16.127: %SSH-5-ENABLED: SSH 1.99 has been enabled

Шаг 3: Обеспечьте защиту консоли и vty-линий.

a. Маршрутизатор можно настроить таким образом, чтобы он завершал сеанс подключения, неактивного в течение указанного времени. Если сетевой администратор вошёл в систему сетевого устройства, а потом был внезапно вызван в другое место, по истечении установленного времени эта команда автоматически завершит сеанс подключения. Приведённые ниже команды закрывают линию связи через пять минут неактивности.
R1(config)# **line console 0**
R1(config-line)# **exec-timeout 5 0**
R1(config-line)# **line vty 0 4**
R1(config-line)# **exec-timeout 5 0**
R1(config-line)# **exit**

R1(config)#

b. Указанная ниже команда препятствует входу в систему с использованием метода полного перебора. Маршрутизатор блокирует попытки входа в систему на 30 секунд, если в течение 120 секунд будет дважды введён неверный пароль. На этом таймере установлено низкое значение специально для выполнения данной лабораторной работы.

   R1(config)# **login block-for 30 attempts 2 within 120**

   Что означает **2 within 120** в приведённой выше команде?

   Что означает **block-for 30** в приведённой выше команде?

Шаг 4: Убедитесь, что все неиспользуемые порты отключены.

По умолчанию порты маршрутизатора отключены, однако рекомендуется лишний раз убедиться, что все неиспользуемые порты административно отключены. Для этого можно воспользоваться командой **show ip interface brief**. Все неиспользуемые порты, не отключенные административно, необходимо отключить с помощью команды **shutdown** в режиме конфигурации интерфейса.

R1# **show ip interface brief**

Шаг 5: Убедитесь, что все меры безопасности предприняты должным образом.

a. С помощью программы Tera Term подключитесь к R1 по протоколу Telnet.

   Принимает ли R1 подключение по протоколу Telnet?

   Поясните свой ответ.

b. С помощью программы Tera Term подключитесь к R1 по протоколу SSH.

   Принимает ли R1 подключение по протоколу SSH?

c. Намеренно укажите неверное имя пользователя и пароль, чтобы проверить, будет ли заблокирован доступ к системе после двух неудачных попыток.

   Что произошло после ввода неправильных данных для входа в систему во второй раз?

d. Из консольной сессии на маршрутизаторе отправьте команду **show login**, чтобы проверить состояние входа в систему. В приведённом ниже примере команда **show login** была отправлена в течение 30-секундной блокировки доступа к системе и показывает, что маршрутизатор находится в режиме «Quiet». Маршрутизатор не будет принимать попытки входа в систему в течение еще 14 секунд.

   R1# **show login**

   A default login delay of 1 second is applied.
   No Quiet-Mode access list has been configured.
   Router enabled to watch for login Attacks.
   If more than 2 login failures occur in 120 seconds or less,
   logins will be disabled for 30 seconds.

   Router presently in Quiet-Mode.

Will remain in Quiet-Mode for 14 seconds.
Denying logins from all sources.
R1#

e. По истечении 30 секунд повторите попытку подключения к R1 по протоколу SSH и войдите в систему, используя имя пользователя **admin** и пароль **Admin15p@55**.
Что отобразилось после успешного входа в систему?

f. Выберите привилегированный режим и укажите в качестве пароля **Enablep@55**.
Если вы неправильно укажете пароль, прервётся ли подключение по протоколу SSH после двух неудачных попыток в течение 120 секунд?
Поясните свой ответ.

g. Введите команду **show running-config** в строке привилегированного режима для просмотра установленных параметров безопасности.

10.4 Часть 3: Настройка основных мер безопасности на коммутаторе

Шаг 1: Выберите более надёжные пароли для коммутатора.

Чтобы соблюсти рекомендации по созданию надёжных паролей, измените зашифрованный пароль привилегированного режима.

S1(config)# **enable secret Enablep@55**

Примечание. Команда безопасности **password min-length** на коммутаторах модели 2960 не используется.

Шаг 2: Активируйте подключения SSH.

a. В качестве имени домена укажите **CCNA-lab.com**.
S1(config)# **ip domain-name CCNA-lab.com**

b. Создайте в базе данных локальных пользователей запись, которая будет использоваться при подключении к маршрутизатору через SSH. Пароль должен соответствовать стандартам надёжных паролей, а пользователь - иметь права доступа уровня администратора.
S1(config)# **username admin privilege 15 secret Admin15p@55**

c. Настройте транспортный ввод для vty-линий таким образом, чтобы они могли принимать подключения SSH, но не разрешайте подключения Telnet.
S1(config)# **line vty 0 15**
S1(config-line)# **transport input ssh**

d. Для проверки подлинности в vty-линиях должна использоваться база данных локальных пользователей.
S1(config-line)# **login local**
S1(config-line)# **exit**

e. Создайте ключ шифрования RSA с длиной 1024 бит.
S1(config)# **crypto key generate rsa modulus 1024**

Шаг 3: Обеспечьте защиту консоли и vty-линий.

a. Настройте коммутатор таким образом, чтобы он закрывал линию через десять минут отсутствия активности.

```
S1(config)# line console 0
S1(config-line)# exec-timeout 10 0
S1(config-line)# line vty 0 15
S1(config-line)# exec-timeout 10 0
S1(config-line)# exit
S1(config)#
```

b. Чтобы помешать попыткам входа в систему с использованием метода полного перебора, настройте коммутатор таким образом, чтобы он блокировал доступ к системе на 30 секунд после двух неудачных попыток входа за 120 секунд. На этом таймере установлено низкое значение специально для выполнения данной лабораторной работы.

```
S1(config)# login block-for 30 attempts 2 within 120
S1(config)# end
```

Шаг 4: Убедитесь, что все неиспользуемые порты отключены.

По умолчанию порты коммутатора включены. Отключите на коммутаторе все неиспользуемые порты.

a. Состояние портов коммутатора можно проверить с помощью команды **show ip interface brief**.

```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.11    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  down                  down
FastEthernet0/2        unassigned      YES unset  down                  down
FastEthernet0/3        unassigned      YES unset  down                  down
FastEthernet0/4        unassigned      YES unset  down                  down
FastEthernet0/5        unassigned      YES unset  up                    up
FastEthernet0/6        unassigned      YES unset  up                    up
FastEthernet0/7        unassigned      YES unset  down                  down
……
FastEthernet0/23       unassigned      YES unset  down                  down
FastEthernet0/24       unassigned      YES unset  down                  down
GigabitEthernet0/1     unassigned      YES unset  down                  down
GigabitEthernet0/2     unassigned      YES unset  down                  down
S1#
```

b. Чтобы отключить сразу несколько интерфейсов, воспользуйтесь командой **interface range**.

```
S1(config)# interface range f0/1–4 , f0/7-24 , g0/1-2
```

S1(config-if-range)# **shutdown**
S1(config-if-range)# **end**
S1#

c. Убедитесь, что все неактивные интерфейсы административно отключены.

S1# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	192.168.1.11	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	administratively down	down
FastEthernet0/2	unassigned	YES	unset	administratively down	down
FastEthernet0/3	unassigned	YES	unset	administratively down	down
FastEthernet0/4	unassigned	YES	unset	administratively down	down
FastEthernet0/5	unassigned	YES	unset	up	up
FastEthernet0/6	unassigned	YES	unset	up	up
FastEthernet0/7	unassigned	YES	unset	administratively down	down
……					
FastEthernet0/23	unassigned	YES	unset	administratively down	down
FastEthernet0/24	unassigned	YES	unset	administratively down	down
GigabitEthernet0/1	unassigned	YES	unset	administratively down	down
GigabitEthernet0/2	unassigned	YES	unset	administratively down	down

S1#

Шаг 5: Убедитесь, что все меры безопасности предприняты должным образом.

a. Убедитесь, что протокол Telnet на коммутаторе отключён.
b. Подключитесь к коммутатору по протоколу SSH и намеренно укажите неверное имя пользователя и пароль, чтобы проверить, будет ли заблокирован доступ к системе.
c. По истечении 30 секунд повторите попытку подключения к S1 по протоколу SSH и войдите в систему, используя имя пользователя **admin** и пароль **Admin15p@55**.

   Появился ли баннер после успешного входа в систему?
d. Выберите привилегированный режим, используя **Enablep@55** в качестве пароля.
e. Введите команду **show running-config** в строке привилегированного режима для просмотра установленных параметров безопасности.

Приложение

. Общие команды конфигурации устройств сети

Настройка IPv4-адреса на ПК.

В начале выполнения каждой лабораторной работы выполните на основе таблицы адресации настройку адреса IPv4, маски подсети и адреса шлюза по умолчанию для сетевых плат персоональных компютеров в соответствии с рис. 14.

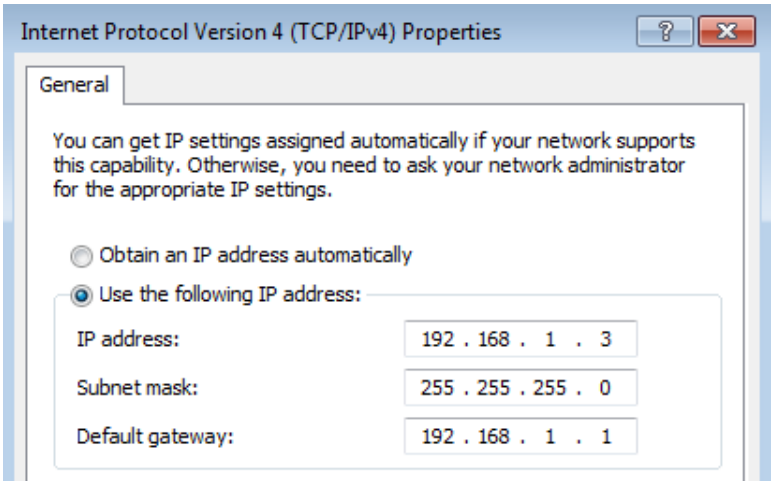

Рис. 14 Настройка IPv4-адреса на ПК

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 2016**

   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**

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 2016**

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**

СПИСОК ЛИТЕРАТУРЫ

1. Олифер, В. Г. Компьютерные сети : принципы, технологии, протоколы: учебник для вузов/ В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб.: Питер, 2010

2. Олифер В., Олифер Н.: "Компьютерные сети", Спб: Издательство "Питер", 2010.

3. Программа сетевой академии Cisco CCNA 1 и 2. Вспомогательное руководство, 3-издание, исправленное 1168 стр., с ил.; ISBN 978-5-8459-0842-1, 1-58713-150-1; формат 70x100/16; твердый переплетCD-ROM; серия Cisco Press; 2009, 1 кв.; Вильямс

4. Программа сетевой академии Cisco CCNA 3 и 4. Вспомогательное руководство944 стр., с ил.; ISBN 978-5-8459-1120-9, 1-58-713113-7; формат 70x100/16; твердый переплет CD-ROM; 2009, 2 кв.; Вильямс.

5. Полный справочник по Cisco1088 стр., с ил.; ISBN 5-8459-0589-3, 0-07-219280-1; формат 70x100/16; твердый переплет серия Полный справочник; 2009, 1 кв.; Вильямс.

6. Руководство по Cisco IOS Питер, Русская Редакция, 2009 г.Твердый переплет, 784 стр. ISBN 978-5-469-01413-3, 5-469-01413-4, 978-5-7502-0309-3 Тираж: 2000 экз.