Гвоздков И.В.
Хорошенко С.В

СЕТЕВЫЕ ВЫСОКОПРОИЗВОДИТЕЛЬНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

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

СЕТЕВЫЕ ВЫСОКОПРОИЗВОДИТЕЛЬНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

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 Сетевые высокопроизводительные информационные технологии : лабораторный практикум / Гвоздков И.В. Хорошенко С.В – СПб. : СПбГУТ, 2016. – 48с

Написаны в соответствии с рабочими учебными программами дисциплины «Сетевые высокопроизводительные информационные технологии».

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

Настройка базовых параметров маршрутизатора с помощью интерфейса командной строки (CLI) системы Cisco IOS

1.1. Цель работы

Получение доступа к коммутатору и маршрутизатору 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. Подключите кабели к оборудованию в соответствии с топологией сети.
2. Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Часть 2. Настройка устройств и проверка подключения

1. Настройте статическую информацию IPv4 на интерфейсах ПК.
2. Настройте базовые параметры маршрутизатора.
3. Проверьте подключение к сети.
4. Настройте на маршрутизаторе протокол SSH.

Часть 3. Отображение сведений о маршрутизаторе

1. Загрузите из маршрутизатора данные об аппаратном и программном обеспечении.
2. Интерпретируйте выходные данные загрузочной конфигурации.
3. Интерпретируйте выходные данные таблицы маршрутизации.
4. Проверьте состояние интерфейсов.

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.

Это комплексная лабораторная работа, нацеленная на повторение ранее изученных команд IOS для маршрутизатора. В первой и второй частях вам предстоит подключить кабели к оборудованию и выполнить базовую настройку конфигураций и параметров IPv4-интерфейса на маршрутизаторе.

В третьей части вам нужно будет настроить удаленное подключение к маршрутизатору с помощью протокола SSH, а также использовать команды IOS для получения от устройства данных, необходимых для того, чтобы ответить на вопросы о маршрутизаторе.

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).
d. Кабели Ethernet, расположенные в соответствии с топологией.

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 и маршрутизатора.

1.2. Часть 1 Настройка топологии и инициализация устройств

1.2.1. Создайте сеть согласно топологии как показано на рис.1.

e. Подключите устройства, как показано в топологии, и подсоедините необходимые кабели.
f. Включите все устройства в топологии

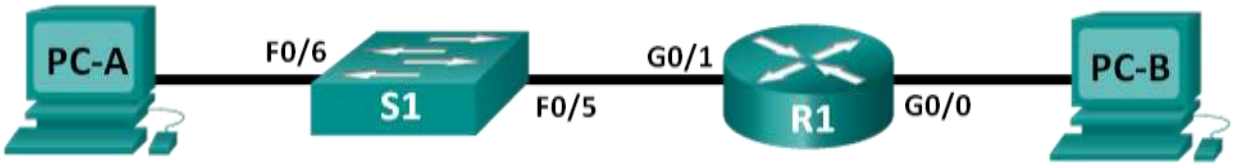

Рис.1 Топология

Таблица 1 Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	192.168.0.1	255.255.255.0	—
	G0/1	192.168.1.1	255.255.255.0	—
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

1.3. Часть 2 Настройка устройств и проверка подключения

1.3.1. Создайте сеть согласно топологии как показано на рис.1.

a. Настройте на компьютере PC-A IP-адрес, маску подсети и параметры основного шлюза.

b. Настройте на компьютере PC-B IP-адрес, маску подсети и параметры основного шлюза.

1.3.2. Создайте сеть согласно топологии как показано на рис.1.

a. Подключитесь к маршрутизатору с помощью консоли и активируйте привилегированный режим EXEC.

Router> **enable**
Router#

b. Войдите в режим глобальной конфигурации маршрутизатора.

Router# **config terminal**
Router(config)#

c. Назначьте маршрутизатору имя устройства.

Router(config)# **hostname R1**

d. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

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

e. Установите минимальную длину 10 символов для всех паролей.

R1(config)# **security passwords min-length 10**

Укажите способы усиления защиты паролей, кроме установки минимальной длины.

f. Назначьте **cisco12345** в качестве зашифрованного пароля привилегированного режима.

R1(config)# **enable secret cisco12345**

g. В качестве пароля консоли назначьте **ciscoconpass**, установите лимит времени, активируйте вход в систему и добавьте команду **logging synchronous**. Команда **logging synchronous** позволяет синхронизировать выходные данные отладки и программного обеспечения Cisco IOS, а также запрещает этим сообщениям прерывать ввод команд с клавиатуры.

R1(config)# **line con 0**
R1(config-line)# **password ciscoconpass**
R1(config-line)# **exec-timeout 5 0**
R1(config-line)# **login**
R1(config-line)# **logging synchronous**
R1(config-line)# **exit**
R1(config)#

Что представляют цифры **5** и **0** для команды **exec-timeout**?_____

h. В качестве пароля vty назначьте **ciscovtypass**, установите лимит времени, активируйте вход в систему и добавьте команду **logging synchronous**.

```
R1(config)# line vty 0 4
R1(config-line)# password ciscovtypass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
R1(config-line)# logging synchronous
R1(config-line)# exit
R1(config)#
```

i. Зашифруйте открытые пароли.

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

j. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.

```
R1(config)# banner motd #Unauthorized access prohibited!#
```

k. Настройте IP-адрес и описание интерфейса. Активируйте оба интерфейса на маршрутизаторе.

```
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 shutdown
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 shutdown
R1(config-if)# exit
R1(config)# exit
R1#
```

l. Настройте часы на маршрутизаторе.

```
R1# clock set 17:00:00 18 Feb 2019
```

m. Из командной строки компьютера PC-B отправьте эхо-запрос на компьютер PC-A.

n. Из командной строки компьютера PC с помощью команды **telnet 192.168.1.1**

o. Затем нажмите **Enter**, чтобы подключиться к маршрутизатору.Удаленный доступ был настроен успешно? Почему использование протокола Telnet считается угрозой безопасности?

1.3.3. Настройте маршрутизатор для доступа по протоколу SSH.

a. Активируйте подключения SSH и создайте пользователя в локальной базе данных маршрутизатора.

R1# **configure terminal**
R1(config)# **ip domain-name CCNA-lab.com**
R1(config)# **username admin privilege 15 secret adminpass1**
R1(config)# **line vty 0 4**
R1(config-line)# **transport input ssh**
R1(config-line)# **login local**
R1(config-line)# **exit**
R1(config)# **crypto key generate rsa modulus 1024**
R1(config)# **exit**

b. Установите SSH-подключение к R1.

c. Из командной строки компьютера PC с помощью команды **SSH –l admin 192.168.1.1**

d. затем нажмите Enter, чтобы подключиться к маршрутизатору.Удаленный доступ был настроен успешно? Почему использование протокола SSH считается безопасным?

c. Отобразите загрузочную конфигурацию.

d. Выполните команду show startup-config на маршрутизаторе, чтобы ответить на следующие вопросы.

e. Как пароли представлены в выходных данных?

f. Используйте show startup-config | begin vty.

g. Что происходит в результате выполнения этой команды?

h. Шаг 4: Отобразите таблицу маршрутизации на маршрутизаторе.

i. Выполните команду show ip route на маршрутизаторе, чтобы ответить на следующие вопросы.

j. Какой код используется в таблице маршрутизации для обозначения сети с прямым подключением?

k. Сколько записей маршрутов закодированы с символом «C» в таблице маршрутизации?

l. Отобразите на маршрутизаторе сводный список интерфейсов. Выполните команду show ip interface brief на маршрутизаторе

Лабораторная работа 2

НАСТРОЙКА СТАТИЧЕСКИХ МАРШРУТОВ И МАРШРУТОВ IPV4 ПО УМОЛЧАНИЮ

2.1. Цель работы

Настройка топологии сети (только Ethernet). Рис 5.

Настройка статических маршрутов и маршрутов IPv4 по умолчанию в соответствии с таблицей 1.

2.1.1 Топология

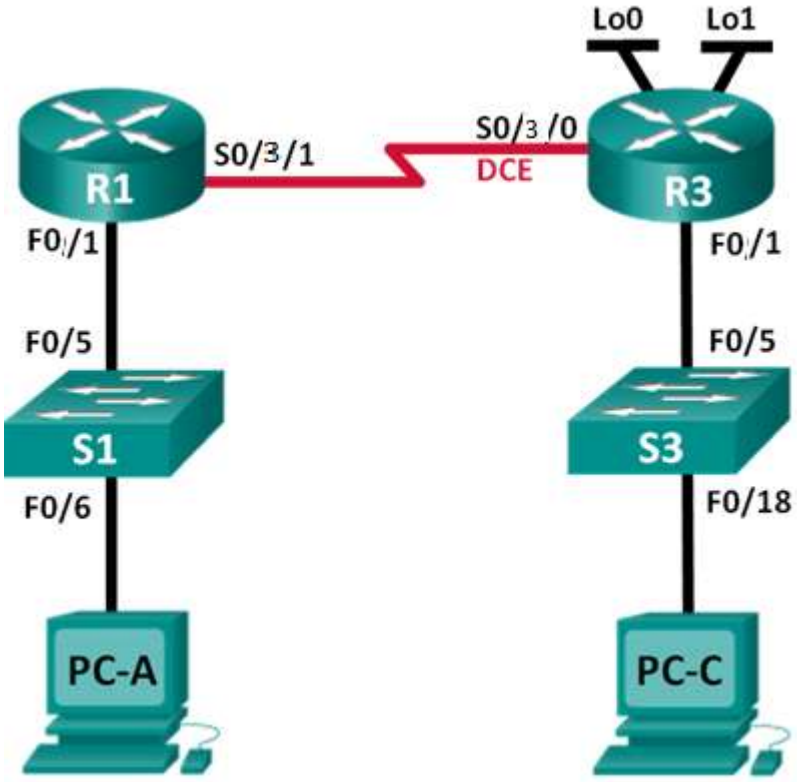

Рис 5 Топология сети

Таблица 1 Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.0.1	255.255.255.0	—
	S0/0/1	10.1.1.1	255.255.255.252	—
R3	G0/1	192.168.1.1	255.255.255.0	—
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	—
	Lo0	209.165.200.225	255.255.255.224	—
	Lo1	198.133.219.1	255.255.255.0	—
PC-A	NIC	192.168.0.10	255.255.255.0	192.168.0.1
PC-C	NIC	192.168.1.10	255.255.255.0	192.168.1.1

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 Конфигурация основных параметров устройств и проверка соединения

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 статических маршрутов

1. Настройка рекурсивного статического маршрута.
2. Настройка статического маршрута с прямым подключением.

Часть 4 Настройка и проверка маршрута по умолчанию

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 и последовательные кабели согласно топологии

2.2. Часть 1 Настройка топологии сети (только Ethernet)

Шаг 1: Настройте интерфейсы ПК.

Шаг 2: Настройте базовые параметры на маршрутизаторах.

Задайте устройствам имена в соответствии с топологией и таблицей адресации.

2.3. Часть 2 Настройка базовых параметров устройств и проверка подключения

Шаг 1: Настройте IP-параметры на маршрутизаторах.

a. Настройте IP-адреса на интерфейсах маршрутизаторов R1 и R3 в соответствии с таблицей адресации.

b. Подключение S0/3/0 — это подключение DCE, которое требует выполнения команды <0>clock rate<1>. Настройка интерфейса S0/3/0 маршрутизатора R3 отображена ниже.

```
R3(config)# interface s0/3/0
R3(config-if)# ip address 10.1.1.2 255.255.255.252
R3(config-if)# clock rate 128000
R3(config-if)# no shutdown
```

Шаг 2: Проверьте подключение в локальных сетях.

a. Проверьте связность, отправив эхо-запросы с каждого ПК на соответствующие шлюзы по умолчанию.

Успешно ли проходит эхо-запрос с узла PC-A на шлюз по умолчанию? _____

Успешно ли проходит эхо-запрос с узла PC-C на шлюз по умолчанию? _____

b. Проверьте связность, отправив эхо-запросы между маршрутизаторами с прямым подключением.

Успешно ли проходит эхо-запрос с маршрутизатора R1 на интерфейс S0/3/0 маршрутизатора R3?

Если на какой-либо из этих вопросов был дан ответ **нет**, найдите и устраните неполадки в конфигурации.

c. Проверьте связность между устройствами без прямого подключения.

Успешно ли проходит эхо-запрос с PC-A на PC-C? _____

Успешно ли отправляется эхо-запрос от узла PC-A на интерфейс Lo0? _____

Успешно ли проходит эхо-запрос с PC-A на Lo1? _____

Успешно ли выполнены эхо-запросы? Поясните свой ответ.

Шаг 3: Сбор информации.

a. С помощью команды **show ip interface brief** проверьте состояние интерфейсов на маршрутизаторе R1.

Сколько интерфейсов активировано на маршрутизаторе R1? _____

b. Проверьте состояние интерфейсов на маршрутизаторе R3.

Сколько интерфейсов активировано на маршрутизаторе R3? _____

c. Просмотрите таблицу маршрутизации на маршрутизаторе R1 с помощью команды **show ip route**.

Какие сети содержатся в таблице адресации, приведенной в данной лабораторной работе, но отсутствуют в таблице маршрутизации R1?

d. Просмотрите таблицу маршрутизации на маршрутизаторе R3.

Какие сети содержатся в таблице адресации, приведенной в данной лабораторной работе, но отсутствуют в таблице маршрутизации R3?

Почему в таблицах маршрутизации каждого из маршрутизаторов содержатся не все сети?

2.4. Часть 3 Настройка статических маршрутов

В третьей части лабораторной работы вам предстоит разными способами реализовывать статические и маршруты по умолчанию, подтвердить, что маршруты были добавлены в таблицы маршрутизации маршрутизаторов R1 и R3, а также проверить подключение с использованием внесенных маршрутов.

Примечание. В данной лабораторной работе содержится минимальный набор команд, необходимых для настройки статической маршрутизации. Список требуемых команд приведен в Приложении A.

Настройка рекурсивного статического маршрута.

При использовании рекурсивного статического маршрута указывается IP-адрес следующего перехода. Поскольку задается только IP-адрес следующего перехода, перед пересылкой пакетов маршрутизатор должен несколько раз выполнить поиск в таблице маршрутизации. Для настройки рекурсивных статических маршрутов используйте следующий синтаксис:

```
Router(config)# ip route сетевой_адрес маска_подсети ip-адрес
```

a. На маршрутизаторе R1 настройте статический маршрут к сети 192.168.1.0, используя IP-адрес последовательного интерфейса Serial 0/3/0 маршрутизатора R3 в качестве адреса следующего перехода. Ниже напишите команду, которую вы использовали.

b. Проверьте наличие новой записи статического маршрута в таблице маршрутизации.

Как новый маршрут отображается в таблице маршрутизации?

Успешно ли проходит эхо-запрос с узла PC-A на узел PC-C? _____

Эти запросы не будут успешными. Если рекурсивный статический маршрут настроен правильно, ping-запрос дойдет до компьютера PC-C. Затем PC-C отправит ответ на запрос обратно компьютеру PC-A. Однако этот ответ будет отброшен маршрутизатором R3, потому что в его таблице маршрутизации нет обратного маршрута в сеть 192.168.0.0.

Шаг 1: Настройка статического маршрута с прямым подключением.

При использовании статического маршрута с прямым подключением указывается выходной интерфейс (параметр *exit-interface*), что позволяет маршрутизатору принять решение о пересылке за один поиск. Статический маршрут с прямым подключением обычно используется с последовательным

интерфейсом для соединения типа точка-точка. Для настройки статических маршрутов с прямым подключением с указанным выходным интерфейсом используйте следующий синтаксис:

```
Router(config)# ip route адрес-сети маска-подсети выходной-интерфейс
```

a. На маршрутизаторе R3 настройте статический маршрут к сети 192.168.0.0, используя интерфейс S0/3/0 в качестве выходного. Ниже напишите команду, которую вы использовали.

b. Проверьте наличие новой записи статического маршрута в таблице маршрутизации.

   Как новый маршрут отображается в таблице маршрутизации?

c. Успешно ли проходит эхо-запрос с узла PC-A на узел PC-C? _____

   Отправка эхо-запроса должна быть успешна.

Шаг 2: Настройте статический маршрут.

a. На маршрутизаторе R1 настройте статический маршрут к сети 198.133.219.0, указывая один из параметров настройки статического маршрута, предлагаемых на предыдущих шагах. Ниже напишите команду, которую вы использовали.

b. На маршрутизаторе R1 настройте статический маршрут к сети 209.165.200.224 маршрутизатора R3, задав другой параметр конфигурации статического маршрута из предлагаемых на предыдущих шагах. Ниже напишите команду, которую вы использовали.

c. Проверьте наличие новой записи статического маршрута в таблице маршрутизации.

   Как новый маршрут отображается в таблице маршрутизации?

d. Успешно ли проходит эхо-запрос с узла PC-A на адреса маршрутизатора R1 198.133.219.1? Отправка эхо-запроса должна быть успешна.

Шаг 3: Удалите статические маршруты для loopback-адресов.

a. На маршрутизаторе R1 используйте команду **no**, чтобы удалить статические маршруты для двух петлевых адресов из таблицы маршрутизации. В специально отведенном месте напишите команды, которые вы использовали.

b. Просмотрите таблицу маршрутизации, чтобы убедиться в успешном удалении маршрутов.

   Сколько маршрутов сети указано в таблице маршрутизации маршрутизатора R1? _____

   Настроен ли шлюз «последней надежды»? _____

Часть 4: Настройка и проверка маршрута по умолчанию

В четвертой части необходимо реализовать маршрут по умолчанию, проверить добавление маршрута в таблицу маршрутизации и проверить подключение, использующее внесенный маршрут.

Маршрут по умолчанию определяет шлюз, на который маршрутизатор отправляет все IP-пакеты, для которых у него нет заимствованного или статического маршрута. Статический маршрут по умолчанию — это статический маршрут, IP-адрес назначения и маска подсети которого равны 0.0.0.0. Обычно его называют маршрутом «четырех нолей».

В маршруте по умолчанию можно указать либо IP-адрес следующего перехода, либо выходной интерфейс. Для настройки статических маршрутов по умолчанию используйте следующий синтаксис:

```
Router(config)# ip route 0.0.0.0 0.0.0.0 {ip-адрес или выходной_интерфейс}
```

a. На маршрутизаторе R1 настройте маршрут по умолчанию, используя выходной интерфейс S0/0/1. Ниже напишите команду, которую вы использовали.

b. Проверьте наличие новой записи статического маршрута в таблице маршрутизации.

Как новый маршрут отображается в таблице маршрутизации?

Какой шлюз является шлюзом «последней надежды»?

c. Успешно ли проходит эхо-запрос с узла PC-A на адрес 209.165.200.225? _____

d. Успешно ли проходит эхо-запрос с узла PC-A на адрес 198.133.219.1? _____

Эхо-запросы должны быть обработаны успешно.

Вопросы для повторения

Новая сеть 192.168.3.0/24 подключена к интерфейсу G0/0 маршрутизатора R1. Какие команды можно использовать для настройки статического маршрута к этой сети от маршрутизатора R3?

Существует ли преимущество в настройке статического маршрута с прямым подключением по сравнению с настройкой рекурсивного статического маршрута?

Почему так важно настроить маршрут по умолчанию на маршрутизаторе?

Приложение A: команды настройки для частей 2, 3 и 4

Команды содержатся в приложении A только для справки. Приложение не содержит все команды, необходимые для выполнения данной лабораторной работы.

Базовые параметры устройств

Настройка параметров IP на маршрутизаторе.

```
R3(config)# interface s0/0/0
R3(config-if)# ip address 10.1.1.2 255.255.255.252
R3(config-if)# clock rate 128000
R3(config-if)# no shutdown
```

Настройка статического маршрута

Настройка рекурсивного статического маршрута.

```
R1(config)# ip route 192.168.1.0 255.255.255.0 10.1.1.2
```

Настройка статического маршрута с прямым подключением.

```
R3(config)# ip route 192.168.0.0 255.255.255.0 s0/0/0
```

Удаление статического маршрута.

```
R1(config)# no ip route 209.165.200.224 255.255.255.224 serial0/0/1
```

или

```
R1(config)# no ip route 209.165.200.224 255.255.255.224 10.1.1.2
```

или

```
R1(config)# no ip route 209.165.200.224 255.255.255.224
```

Настройка маршрута по умолчанию

```
R1(config)# ip route 0.0.0.0 0.0.0.0 s0/0/1
```

Лабораторная работа 3

НАСТРОЙКА ОСНОВНЫХ ПАРАМЕТРОВ ПРОТОКОЛА RIPV2

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

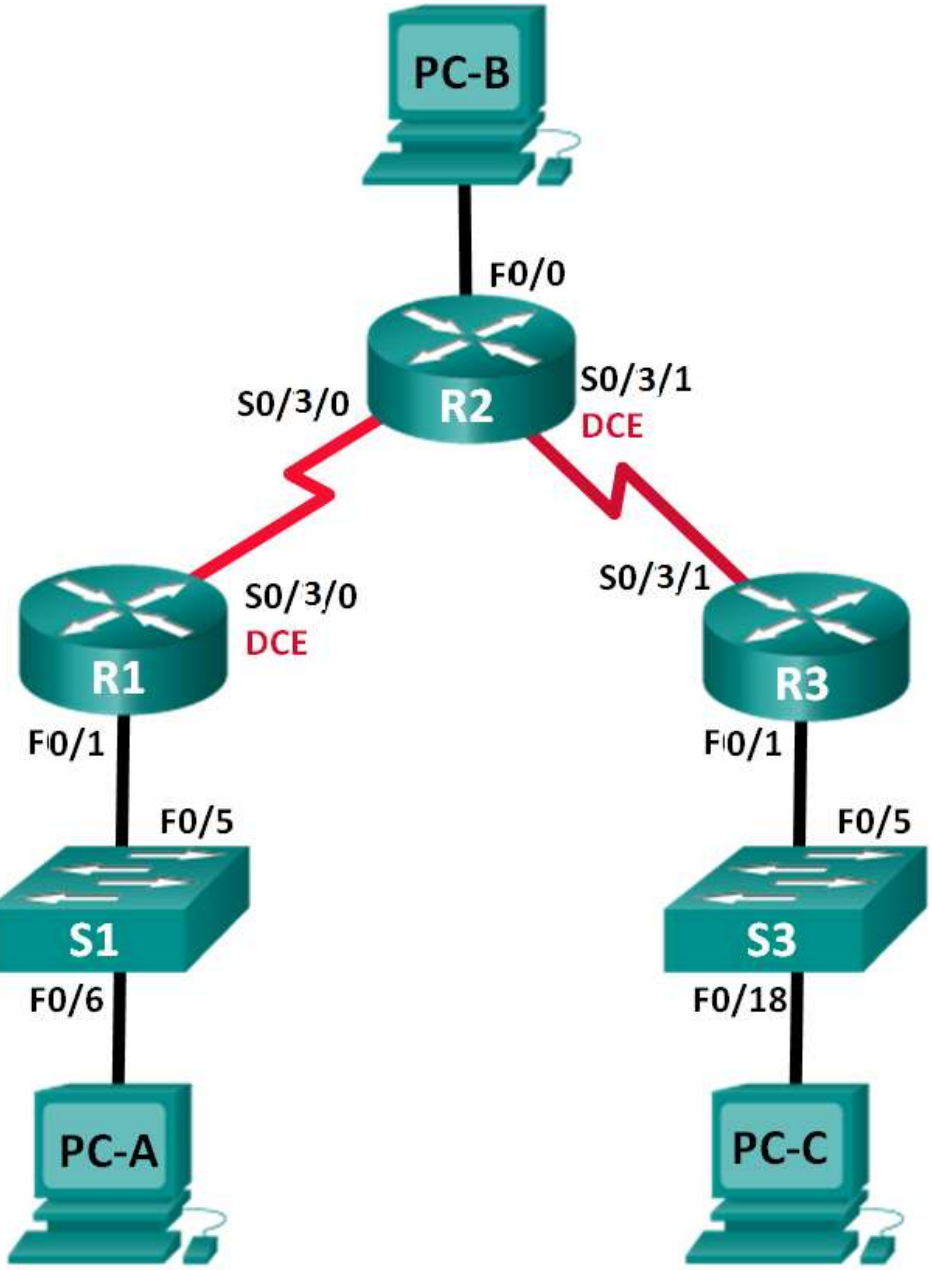

Рис 6 Топология сети

Таблица 2 Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	F0/1	172.30.10.1	255.255.255.0	—
	S0/3/0 (DCE)	10.1.1.1	255.255.255.252	—
R2	F0/0	209.165.201.1	255.255.255.0	—
	S0/3/0	10.1.1.2	255.255.255.252	—
	S0/3/1 (DCE)	10.2.2.2	255.255.255.252	—
R3	F0/1	172.30.30.1	255.255.255.0	—
	S0/3/1	10.2.2.1	255.255.255.252	—
S1	—	VLAN 1	—	—
S3	—	VLAN 1	—	—
PC-A	NIC	172.30.10.3	255.255.255.0	172.30.10.1
PC-B	NIC	209.165.201.2	255.255.255.0	209.165.201.1
PC-C	NIC	172.30.30.3	255.255.255.0	172.30.30.1

Задачи

Часть 1. Создание сети и настройка основных параметров устройства

Часть 2. Настройка и проверка маршрутизации RIPv2

1. Настройте на маршрутизаторах протокол RIPv2 и проверьте его работоспособность.
2. Настройте пассивный интерфейс.
3. Изучите таблицы маршрутизации.
4. Отключите автоматическое объединение.
5. Настройте маршрут по умолчанию.
6. Проверьте наличие сквозного соединения.

Общие сведения/сценарий

Протокол RIP версии 2 (RIPv2) используется для маршрутизации IPv4-адресов в небольших сетях. RIPv2 — это бесклассовый протокол маршрутизации на базе векторов расстояния, определенный в RFC 1723. Поскольку RIPv2 является бесклассовым протоколом маршрутизации, маски подсетей включены в обновления маршрутизации. По умолчанию протокол RIPv2 автоматически суммирует сети на границах сети. После отключения функции автоматического суммирования протокол RIPv2 прекращает суммирование сетей по их классовому адресу на пограничных маршрутизаторах.

В лабораторной работе необходимо настроить топологию сети с использованием маршрутизации RIPv2, отключить автоматическое суммирование, указать маршрут по умолчанию и использовать команды CLI для отображения и проверки сведений о маршрутизации RIP.

Необходимые ресурсы

1. 3 маршрутизатора (Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (универсальный образ) или аналогичная модель).
2. 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель).
3. 3 ПК (Windows 7, Vista или XP с программой эмуляции терминала, например, Tera Term).
4. Консольные кабели для настройки устройств Cisco IOS через консольные порты.
5. кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Создание сети и настройка основных параметров устройства

В части 1 вам предстоит создать топологию сети и настроить основные параметры.

Шаг 1: Создайте сеть согласно топологии.

Шаг 2: Настройте основные параметры на каждом маршрутизаторе и коммутаторе.

a. Отключите поиск DNS.

b. Настройте имена устройств в соответствии с топологией.

c. Назначьте IP-адреса всем интерфейсам в соответствии с таблицей адресации.

d. Для каждого интерфейса настройте описание с IP-адресом.

e. Установите значение тактовой частоты для последовательного интерфейса DCE.

Шаг 3: Настройте IP-адресацию на компьютере.

Сведения об IP-адресах компьютеров можно посмотреть в таблице адресации.

Шаг 4: Проверка связи.

На данный момент компьютеры не могут отправлять друг другу эхо-запросы.

a. Каждая рабочая станция должна иметь возможность проводить эхо-тестирование присоединенного маршрутизатора. При неудачном выполнении эхо-запросов выполните поиск и устранение неполадок.

b. Маршрутизаторы должны успешно отправлять эхо-запросы друг другу. При неудачном выполнении эхо-запросов выполните поиск и устранение неполадок.

Часть 2: Настройка и проверка маршрутизации RIPv2

В части 2 необходимо будет настроить маршрутизацию RIPv2 на всех маршрутизаторах в сети, а затем убедиться, что таблицы маршрутизации обновляются правильно. После проверки RIPv2 вам предстоит отключить автоматическое суммирование, настроить маршрут по умолчанию и проверить сквозное соединение.

Шаг 1: Настройте маршрутизацию по протоколу RIPv2.

a. Настройте протокол RIPv2 на маршрутизаторе R1 в качестве протокола маршрутизации и проинформируйте об этом соответствующие подключенные сети.

```
R1# config t
R1(config)# router rip
```

```
R1(config-router)# version 2
R1(config-router)# passive-interface f0/1
R1(config-router)# network 172.30.0.0
R1(config-router)# network 10.0.0.0
```

Команда **passive-interface** прекращает отправку обновлений маршрутизации из указанного интерфейса. Данный процесс предотвращает нежелательную отправку маршрутизирующей информации в локальную сеть. Тем не менее, сеть, к которой относится указанный интерфейс, по-прежнему объявляется в обновлениях маршрутизации, которые отправляются из других интерфейсов.

b. Настройте протокол RIPv2 на маршрутизаторе R3 и воспользуйтесь командой **network**, чтобы добавить соответствующие сети и предотвратить обновления маршрутизации в интерфейсе локальной сети.

c. Настройте протокол RIPv2 на маршрутизаторе R2 и воспользуйтесь командой network, чтобы добавить соответствующие подключенные сети. Не объявляйте сеть 209.165.201.0.

Шаг 2: Проверьте текущее состояние сети.

a. Состояние двух последовательных каналов можно легко проверить с помощью команды **show ip interface brief** на маршрутизаторе R2.

b. Проверьте наличие подключения между компьютерами.

Успешно ли отправляется эхо-запрос от узла PC-A на PC-B? _____Почему?

Успешно ли проходит эхо-запрос с PC-A на PC-C? _____Почему?

Успешно ли проходит эхо-запрос с узла PC-C на PC-B? _____Почему?

Успешно ли проходит эхо-запрос с узла PC-C на PC-A? _____Почему?

c. Убедитесь в том, что протокол RIPv2 активирован на маршрутизаторах.

Чтобы проверить это, можно воспользоваться командами **debug ip rip**, **show ip protocols** и **show run**.

Какие сведения подтверждают работу RIPv2 при выполнении команды **debug ip rip** на маршрутизаторе R2?

Изучив выходные данные отладки, в командной строке привилегированного режима выполните команду **undebug all**.

Какие сведения подтверждают работу RIPv2 при выполнении команды **show run** на маршрутизаторе R3?

d. Отключите автоматическое суммирование маршрутов.

Локальные сети, подключенные к маршрутизаторам R1 и R3, состоят из «разорванных» сетей. Маршрутизатор R2 отображает в таблице маршрутизации два пути к сети 172.30.0.0/16, имеющие одинаковую стоимость. Маршрутизатор R2 отображает только адрес главной классовой сети 172.30.0.0, но не отображает подсети этой сети.

```
R2# show ip route
```

Маршрутизатор R1 отображает только собственную подсеть для сети 172.30.10.0/24. В таблице маршрутизации R1 нет маршрута для подсети 172.30.30.0/24 маршрутизатора R3.

```
R1# show ip route
```

Маршрутизатор R3 отображает только собственную подсеть для сети 172.30.30.0/24. В таблице маршрутизации R3 нет маршрута для подсетей 172.30.10.0/24 маршрутизатора R1.

```
R3# show ip route
```

Чтобы определить маршруты, полученные в обновлениях RIP от маршрутизатора R3, используйте команду **debug ip rip** на маршрутизаторе R2. Укажите их далее.

Маршрутизатор R3 не передает какие-либо подсети 172.30.0.0, только суммарный маршрут 172.30.0.0/16, включая маску подсети. Поэтому таблицы маршрутизации на R1 и R2 не отображают подсети 172.30.0.0 на R3.

Шаг 3: Отключите автоматическое объединение.

a. Для отключения автоматического суммирования в RIPv2 используется команда **no auto-summary**. Отключите автоматическое суммирование на всех маршрутизаторах. Маршрутизаторы больше не суммируют маршруты на границах главной классовой сети. Маршрутизатор R1 приведен здесь в качестве примера.

```
R1(config)# router rip
R1(config-router)# no auto-summary
```

b. Чтобы очистить таблицу маршрутизации, используйте команду **clear ip route ***.

```
R1(config-router)# end
R1# clear ip route *
```

c. Изучите таблицы маршрутизации. Не забывайте, что после очистки таблиц маршрутизации потребуется некоторое время для выравнивания их содержимого.

Подсети LAN, подключенные к маршрутизаторам R1 и R3, должны быть включены во все три таблицы маршрутизации.

```
R2# show ip route
R1# show ip route
R3# show ip route
```

d. Чтобы проверить обновления RIP, на маршрутизаторе R2 используйте команду **debug ip rip**.

```
R2# debug ip rip
```

Через 60 секунд выполните команду **no debug ip rip**.

Какие маршруты содержатся в обновлениях RIP, принятых от R3?

Включены ли маски подсети в обновления маршрутизации? _____

Шаг 4: Настройка и перераспределение маршрута по умолчанию для доступа к Интернету

a. На маршрутизаторе R2 создайте статический маршрут к сети 0.0.0.0 0.0.0.0 с помощью команды **ip route**. В результате весь трафик с неизвестным адресом назначения будет пересылаться на компьютер PC-B с адресом 209.165.201.2, моделируя Интернет путем настройки шлюза «последней надежды» на маршрутизаторе R2.

```
R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.2
```

b. Маршрутизатор R2 объявит маршрут для других маршрутизаторов, если команда **default-information originate** будет добавлена в его конфигурацию RIP.

```
R2(config)# router rip
R2(config-router)# default-information originate
```

Шаг 5: Проверка конфигурации маршрутизации

a. Просмотрите таблицу маршрутизации маршрутизатора R1.

```
R1# show ip route
<Данные опущены>
Gateway of last resort is 10.1.1.2 to network 0.0.0.0
```

```
R*    0.0.0.0/0 [120/1] via 10.1.1.2, 00:00:13, Serial0/0/0
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.1/32 is directly connected, Serial0/0/0
R        10.2.2.0/30 [120/1] via 10.1.1.2, 0:00:13, Serial0/0/0
      172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
C        172.30.10.0/24 is directly connected, GigabitEthernet0/1
L        172.30.10.1/32 is directly connected, GigabitEthernet0/1
R        172.30.30.0/24 [120/2] via 10.1.1.2, 0:00:13, Serial0/0/0
```

Как на основании таблицы маршрутизации можно определить, что сеть, разбитая на подсети и используемая маршрутизаторами R1 и R3, имеет путь для интернет-трафика?

b. Просмотрите таблицу маршрутизации на R2.

Каким образом путь для интернет-трафика появился в таблице маршрутизации маршрутизатора R2?

Шаг 6: Проверьте подключение.

a. Смоделируйте отправку трафика в Интернет, отправив эхо-запросы от узла PC-A и PC-C в сеть 209.165.201.2.

Успешно ли выполнена проверка связи? _____

b. Убедитесь в том, что узлы в разбитой на подсети сети могут достичь друг друга. Для этого выполните эхо-запрос между узлами PC-A и PC-C.

Успешно ли выполнена проверка связи? _____

Вопросы для повторения

1. Зачем может потребоваться выключение автоматического суммирования при работе RIPv2?
2. Каким образом маршрутизаторы R1 и R3 получили информацию о пути в Интернет?

Лабораторная работа 4

КОНФИГУРАЦИЯ VLAN И МАГИСТРАЛЬНЫХ КАНАЛОВ

Топология

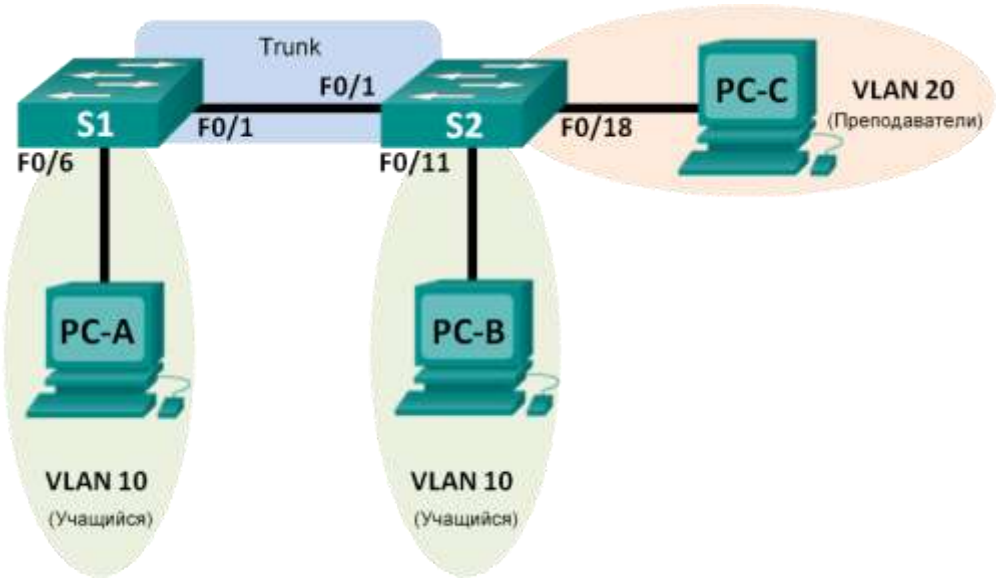

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
S1	VLAN 1	192.168.1.11	255.255.255.0	—
S2	VLAN 1	192.168.1.12	255.255.255.0	—
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.10.4	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.20.3	255.255.255.0	192.168.20.1

Задачи

Часть 1. Создание сети и настройка основных параметров устройства

Часть 2. Создание виртуальных локальных сетей и назначение портов коммутатора

Часть 3. Поддержка назначения портов VLAN и базы данных VLAN

Часть 4. Настройка магистрального канала стандарта 802.1Q между коммутаторами

Часть 5. Удаление базы данных VLAN

Общие сведения/сценарий

В целях повышения производительности сети большие широковещательные домены 2-го уровня делят на домены меньшего размера. Для этого современные коммутаторы используют виртуальные локальные сети (VLAN). Также сети VLAN можно использовать для определения узлов, между которыми возможен обмен данными, что позволяет повысить уровень безопасности. Сети VLAN облегчают процесс проектирования сети, обеспечивающей помощь в достижении целей организации.

Транковые каналы сети VLAN используются для распространения сетей VLAN по различным устройствам. Транковые каналы разрешают передачу трафика из множества сетей VLAN через один канал, не нанося вред идентификации и сегментации сети VLAN.

В этой лабораторной работе вам предстоит создать сети VLAN на обоих коммутаторах в топологии, назначить сети VLAN в порты доступа на коммутаторе, проверить корректность работы сетей VLAN, а затем создать магистральный канал сети VLAN между двумя коммутаторами, чтобы узлы в пределах одной сети VLAN могли обмениваться данными по транку вне зависимости от того, к какому коммутатору подключен узел.

Необходимые ресурсы

2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель).

3 ПК (Windows 7, Vista или XP с программой эмуляции терминала, например, Tera Term).

Консольные кабели для настройки устройств Cisco IOS через консольные порты.

Кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Создание сети и настройка основных параметров устройства

В первой части лабораторной работы вам предстоит создать топологию сети и настроить базовые параметры для узлов ПК и коммутаторов.

Шаг 1: Создайте сеть согласно топологии.

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

Шаг 2: Настройте базовые параметры каждого коммутатора.

a. Подключитесь к коммутатору с помощью консоли и перейдите в режим глобального конфигурирования.

b. Настройте имена хостов в соответствии с топологией.

c. Настройте на коммутаторе IP-адрес, указанный в таблице адресации для сети VLAN 1.

Шаг 3: Настройте узлы ПК.

Адреса ПК можно посмотреть в таблице адресации.

Шаг 4: Проверка связи.

Проверьте способность компьютеров обмениваться эхо-запросами.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра.

Успешно ли выполняется эхо-запрос от узла PC-A на узел PC-B? _____

Успешно ли выполняется эхо-запрос от узла ПК A на узел ПК C? _____

Успешно ли выполняется эхо-запрос от узла PC-A на коммутатор S1? _____

Успешно ли выполняется эхо-запрос от узла PC-B на узел PC-C? _____

Успешно ли выполняется эхо-запрос от узла PC-B на коммутатор S2? _____

Успешно ли выполняется эхо-запрос от узла PC-C на коммутатор S2? _____

Успешно ли выполняется эхо-запрос от коммутатора S1 на коммутатор S2? _____

Часть 2: Создание сетей VLAN и назначение портов коммутатора

Во второй части лабораторной работы вам необходимо создать сети VLAN для учащихся, преподавателей и руководства на обоих коммутаторах. Затем вам нужно назначить сети VLAN соответствующему интерфейсу. Для проверки параметров конфигурации используйте команду **show vlan**.

Шаг 1: Создайте сети VLAN на коммутаторах.

a. Создайте сети VLAN на коммутаторе S1.

```
S1(config)# vlan 10
S1(config-vlan)# name Student
S1(config-vlan)# vlan 20
S1(config-vlan)# name Faculty
S1(config-vlan)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# end
```

b. Создайте такую же сеть VLAN на коммутаторе S2.

c. Выполните команду **show vlan**, чтобы просмотреть список сетей VLAN на коммутаторе S1.

```
S1# show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gi0/1, Gi0/2
10   Student                           active
20   Faculty                           active
99   Management                        active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

Какой является VLAN по умолчанию? _____

Какие порты назначены для сети VLAN по умолчанию?

Шаг 2: Назначьте сети VLAN соответствующим интерфейсам коммутатора.

a. Назначьте сети VLAN интерфейсам на коммутаторе S1.

1) Назначьте узел PC-A сети VLAN для учащихся.

```
S1(config)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
```

2) Переместите IP-адрес коммутатора сети VLAN 99.

```
S1(config)# interface vlan 1
S1(config-if)# no ip address
S1(config-if)# interface vlan 99
S1(config-if)# ip address 192.168.1.11 255.255.255.0
S1(config-if)# end
```

b. Выполните команду **show vlan brief** и убедитесь, что сети VLAN назначены правильным интерфейсам.

```
S1# show vlan brief
```

c. Выполните команду **show ip interfaces brief**.

В каком состоянии находится сеть VLAN 99? Почему?

d. Используйте топологию, чтобы назначить сети VLAN соответствующим портам коммутатора S2.

e. Удалите IP-адрес для сети VLAN 1 на коммутаторе S2.

f. Настройте IP-адрес для сети VLAN 99 на коммутаторе S2 в соответствии с таблицей адресации.

g. Выполните команду **show vlan brief**, чтобы убедиться, что сети VLAN назначены правильным интерфейсам.

```
S2# show vlan brief
```

Успешно ли выполняется эхо-запрос от узла PC-A на узел PC-B? Почему?

Успешно ли выполняется эхо-запрос от коммутатора S1 на коммутатор S2? Почему?

Часть 3: Поддержка назначения портов VLAN и базы данных VLAN

В третьей части лабораторной работы вам предстоит изменить назначения сети VLAN портам и удалить сети VLAN из базы данных VLAN.

Шаг 1: Назначьте сеть VLAN нескольким интерфейсам.

a. На коммутаторе S1 назначьте интерфейсы F0/11 – 24 сети VLAN 10.

```
S1(config)# interface range f0/11-24
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 10
S1(config-if-range)# end
```

b. Чтобы проверить настройку VLAN, выполните команду **show vlan brief**.

c. Заново назначьте порты F0/11 и F0/21 сети VLAN 20.

d. Убедитесь, что назначения сети VLAN настроены верно.

Шаг 2: Удалите назначение VLAN из интерфейса.

a. Используйте команду **no switchport access vlan**, чтобы удалить назначение сети VLAN 10 для F0/24.

```
S1(config)# interface f0/24
S1(config-if)# no switchport access vlan
S1(config-if)# end
```

b. Убедитесь, что это изменение сети VLAN вступило в силу.

С какой сетью VLAN теперь связан порт F0/24?

Шаг 3: Удалите идентификатор VLAN из базы данных VLAN.

a. Добавьте сеть VLAN 30 в интерфейс F0/24, не вводя команду сети VLAN.

```
S1(config)# interface f0/24
S1(config-if)# switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
```

b. Убедитесь, что новая сеть VLAN отображается в таблице VLAN.

```
S1# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Gi0/1, Gi0/2
10   Student                           active    Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/22, Fa0/23
20   Faculty                           active    Fa0/11, Fa0/21
30   VLAN0030                          active    Fa0/24
99   Management                        active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

Какое имя присвоено сети VLAN 30 по умолчанию?

c. Используйте команду **vlan 30**, чтобы удалить сеть VLAN 30 из базы данных VLAN.

```
S1(config)# no vlan 30
S1(config)# end
```

d. Выполните команду **show vlan brief**. Порт F0/24 было назначен сети VLAN 30.

Какой сети VLAN назначен порт F0/24 после удаления сети VLAN 30? Что происходит с трафиком, предназначенным для узла, подключенного к F0/24?

```
S1# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Gi0/1, Gi0/2
```

```
10   Student                          active    Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/22, Fa0/23
20   Faculty                          active    Fa0/11, Fa0/21
99   Management                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

e. Выполните команду **no switchport access vlan** на интерфейсе F0/24.

f. Выполните команду **show vlan brief**, чтобы определить назначение сети VLAN для F0/24. Какой сети VLAN назначен порт F0/24?

Примечание. Прежде чем удалять сеть VLAN из базы данных, рекомендуется переназначить все порты, назначенные для этой сети VLAN.

Почему перед удалением сети VLAN из базы данных рекомендуется назначить порт другой сети VLAN?

Часть 4: Конфигурация магистрального канала стандарта 802.1Q между коммутаторами

В четвертой части лабораторной работы вам необходимо настроить интерфейс F0/1 для использования протокола динамического создания магистрального канала (DTP), чтобы он мог согласовываться с магистральным режимом. После выполнения и проверки настройки вам нужно будет отключить DTP на интерфейсе F0/1 и вручную настроить его в качестве магистрального канала.

Шаг 1: Для создания магистральной связи на порте F0/1 используйте протокол DTP.

По умолчанию протокол DTP на порте коммутатора 2960 настроен на динамический автоматический режим. Благодаря этому интерфейс может преобразовать канал в магистральный канал, если соседний интерфейс настроен на магистральный или динамический рекомендуемый режим.

a. Настройте порт F0/1 на коммутаторе S1 для согласования магистрального режима.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode dynamic desirable
```

b. На коммутаторах S1 и S2 выполните команду **show vlan brief**. Интерфейс F0/1 больше не назначен сети VLAN 1. Транковые интерфейсы не указаны в таблице VLAN.

```
S1# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/24, Gi0/1, Gi0/2
10   Student                          active    Fa0/6, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/22, Fa0/23
20   Faculty                          active    Fa0/11, Fa0/21
99   Management                       active
1002 fddi-default                     act/unsup
```

```
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

c. Для просмотра магистральных интерфейсов выполните команду **show interfaces trunk**. Обратите внимание, что на коммутаторе S1 настроен рекомендуемый режим, а на S2 настроен автоматический режим.

```
S1# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       desirable        802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99

S2# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       auto             802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99
```

Примечание. По умолчанию доступ в магистральный канал разрешен для всех сетей VLAN. С помощью команды **switchport trunk** вы можете определить, какие сети VLAN имеют доступ к магистральному каналу.

Убедитесь в том, что трафик сети VLAN проходит через магистральный интерфейс F0/1.

Успешно ли выполняется эхо-запрос от коммутатора S1 на коммутатор S2? _____

Успешно ли выполняется эхо-запрос от узла PC-A на узел PC-B? _____

Успешно ли выполняется эхо-запрос от узла ПК A на узел ПК C? _____

Успешно ли выполняется эхо-запрос от узла PC-B на узел PC-C? _____

Успешно ли выполняется эхо-запрос от узла PC-A на коммутатор S1? _____

Успешно ли выполняется эхо-запрос от узла PC-B на коммутатор S2? _____

Успешно ли выполняется эхо-запрос от узла PC-C на коммутатор S2? _____

Если на один из этих вопросов вы ответили отрицательно, ниже объясните причины такого результата.

Шаг 2: Вручную настройте магистральный интерфейс F0/1.

Команда **switchport mode trunk** позволяет вручную настроить порт в качестве магистрального канала. Эту команду следует выполнять на обоих концах канала.

a. Измените режим порта коммутатора на интерфейсе F0/1, чтобы принудительно создать магистральную связь. Не забудьте сделать это на обоих коммутаторах.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
```

b. Для просмотра магистрального режима выполните команду **show interfaces trunk**. Обратите внимание, что режим изменен с **desirable** (рекомендуемый) на **on** (вкл.).

```
S2# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99
```

Почему вместо использования протокола DTP рекомендуется вручную настраивать интерфейс на магистральный режим?

Вопросы для повторения

Что нужно для того, чтобы узлы в сети VLAN 10 могли обмениваться данными с узлами в сети VLAN 20?

В чем заключаются основные преимущества, которые получает организация при использовании сетей VLAN?

Лабораторная работа 5

НАСТРОЙКА МАРШРУТИЗАЦИИ МЕЖДУ СЕТЯМИ VLAN

Топология

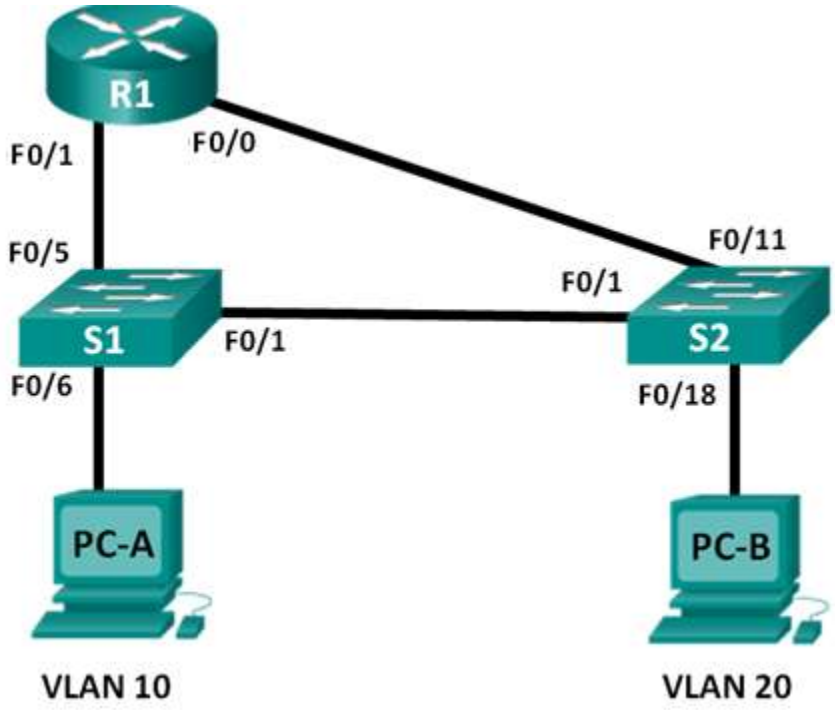

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	F0/0	192.168.20.1	255.255.255.0	—
	F0/1	192.168.10.1	255.255.255.0	—
S1	VLAN 10	192.168.10.11	255.255.255.0	192.168.10.1
S2	VLAN 10	192.168.10.12	255.255.255.0	192.168.10.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.20.3	255.255.255.0	192.168.20.1

Задачи

Часть 1. Создание сети и настройка основных параметров устройства

Часть 2. Настройка коммутаторов с сетями VLAN и магистральной связью

Часть 3. Проверка магистральной связи, сетей VLAN, маршрутизации и подключения

Общие сведения/сценарий

Устаревшие методы маршрутизации между сетями VLAN редко используются в современных сетях; однако, прежде чем переходить к маршрутизации между VLAN методом router-on-a-stick (ROS) или к настройке коммутации 3-го уровня, рекомендуется ознакомиться с этим типом маршрутизации и получить навыки его настройки. Кроме того, вы можете столкнуться с интерфейсной маршрутизацией между VLAN в организациях с очень маленькими сетями. Простота в использовании — это одно из преимуществ маршрутизации между VLAN с использованием устаревшего метода.

В этой лабораторной работе необходимо настроить один маршрутизатор с двумя коммутаторами, подключенными через интерфейсы маршрутизатора Ethernet. На коммутаторах будут настроены две отдельные сети VLAN, и вам будет необходимо настроить маршрутизацию между этими VLAN.

Необходимые ресурсы

1 маршрутизатор (Cisco 1941 с операционной системой Cisco IOS 15.2(4)M3 (универсальный образ) или аналогичная модель).

2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель).

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

Консольные кабели для настройки устройств Cisco IOS через консольные порты.

Кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Создание сети и настройка основных параметров устройства

В первой части лабораторной работы вы настроите топологию сети и при необходимости удалите все конфигурации.

Шаг 1: Создайте сеть согласно топологии.

Шаг 2: Настройте базовые параметры для маршрутизатора R1.

d. Подключитесь к маршрутизатору R1 с помощью консоли и перейдите в режим глобальной настройки.

e. Настройте адресацию на интерфейсах F0/0 и F0/1 и включите оба интерфейса.

Шаг 3: Настройте основные параметры обоих коммутаторов.

a. Подключитесь к коммутатору с помощью консоли и перейдите в режим глобальной конфигурации.

Шаг 4: Настройте базовые параметры на компьютерах PC-A и PC-B.

На компьютерах PC-A и PC-B настройте IP-адреса и адрес шлюза по умолчанию в соответствии с таблицей адресации.

Часть 2: Настройте коммутаторы для работы с сетями VLAN и создания магистральных каналов

Во второй части лабораторной работы вы будете настраивать коммутаторы для сетей VLAN и магистральных каналов.

Шаг 1: Настройте сети VLAN на коммутаторе S1.

a. Создайте сеть VLAN 10 на коммутаторе S1. Назначьте **Student** в качестве имени сети VLAN.

b. Создайте виртуальную локальную сеть VLAN 20. Назначьте **Faculty-Admin** в качестве имени сети VLAN.

c. Настройте F0/1 в качестве магистрального порта.

d. Назначьте порты F0/5 и F0/6 сети VLAN 10 и настройте оба порта в качестве портов доступа.

e. Назначьте IP-адрес сети VLAN 10 и активируйте его. См. таблицу адресации.

f. Настройте шлюз по умолчанию в соответствии с таблицей адресации.

Коммутатор S1

```
S1(config)# vlan 10
S1(config-vlan)# name Student
S1(config-vlan)# exit
S1(config)# vlan 20
S1(config-vlan)# name Faculty-Admin
S1(config-vlan)# exit
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# interface range f0/5 – 6
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 10
S1(config-if-range)# interface vlan 10
S1(config-if)# ip address 192.168.10.11 255.255.255.0
S1(config-if)# no shut
S1(config-if)# exit
S1(config)# ip default-gateway 192.168.10.1
```

Шаг 2: Настройте сети VLAN на коммутаторе S2.

a. Создайте сеть VLAN 10 на коммутаторе S2. Назначьте **Student** в качестве имени сети VLAN.

b. Создайте виртуальную локальную сеть VLAN 20. Назначьте **Faculty-Admin** в качестве имени сети VLAN.

c. Настройте F0/1 в качестве магистрального порта.

d. Назначьте порты F0/11 и F0/18 сети VLAN 20 и настройте оба порта в качестве портов доступа.

e. Назначьте IP-адрес сети VLAN 10 и активируйте его. См. таблицу адресации.

f. Настройте шлюз по умолчанию в соответствии с таблицей адресации.

Коммутатор S2

```
S2(config)# vlan 10
S2(config-vlan)# name Student
S2(config-vlan)# exit
```

```
S2(config)# vlan 20
S2(config-vlan)# name Faculty-Admin
S2(config-vlan)# exit
S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
S2(config-if)# interface f0/11
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 20
S2(config-if)# interface f0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 20
S2(config-if-range)# interface vlan 10
S2(config-if)#ip address 192.168.10.12 255.255.255.0
S2(config-if)# no shut
S2(config-if)# exit
S2(config)# ip default-gateway 192.168.10.1
```

Часть 3: Проверка магистральной связи, сетей VLAN, маршрутизации и подключения

Шаг 1: Проверьте таблицу маршрутизации маршрутизатора R1.

a. На маршрутизаторе R1 выполните команду **show ip route**. Какие маршруты указаны в маршрутизаторе R1?

b. На коммутаторах S1 и S2 выполните команду **show interface trunk**. Настроен ли порт F0/1 на обоих коммутаторах на магистральную связь? _____

c. На коммутаторах S1 и S2 выполните команду **show vlan brief**. Убедитесь, что сети VLAN 10 и 20 активны и что соответствующие порты в коммутаторах находятся в соответствующих VLAN. Почему порт F0/1 не отображается в составе в какой-либо из активных VLAN?

d. От компьютера PC-A в сети VLAN 10 отправьте эхо-запрос на компьютер PC-B в сети VLAN 20. Если маршрутизация VLAN работает правильно, эхо-запросы между сетями 192.168.10.0 и 192.168.20.0 должны проходить успешно.

e. Проверьте наличие подключения между всеми устройствами. Эхо-запросы должны успешно проходить между всеми устройствами. Если эхо-запросы не проходят, исправьте неполадки.

Вопросы для повторения

В чем заключается преимущество использования устаревшего метода маршрутизации между VLAN?

Лабораторная работа 6

НАСТРОЙКА И ПРОВЕРКА СТАНДАРТНЫХ СПИСКОВ КОНТРОЛЯ ДОСТУПА ДЛЯ IPV4

Топология

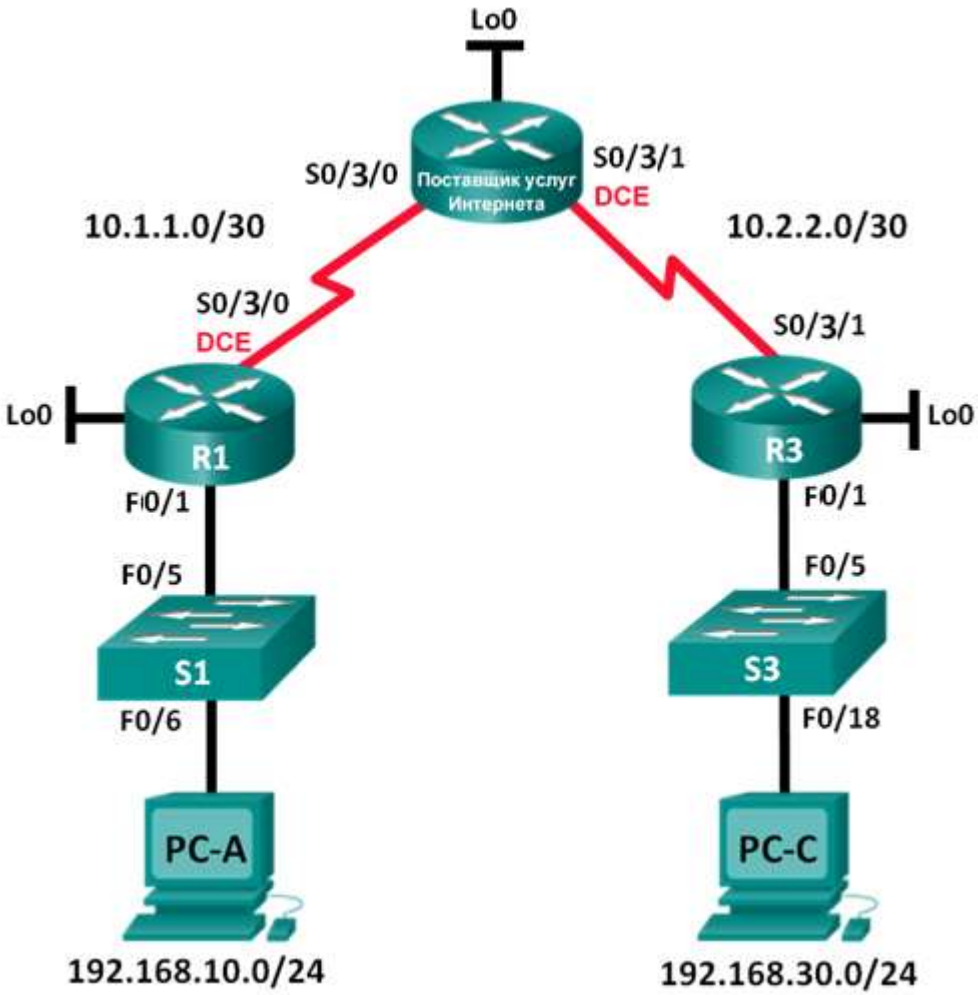

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	F0/1	192.168.10.1	255.255.255.0	—
	Lo0	192.168.20.1	255.255.255.0	—
	S0/3/0 (DCE)	10.1.1.1	255.255.255.252	—
ISP	S0/3/0	10.1.1.2	255.255.255.252	—
	S0/3/1 (DCE)	10.2.2.2	255.255.255.252	—
	Lo0	209.165.200.225	255.255.255.224	—
R3	F0/1	192.168.30.1	255.255.255.0	—
	Lo0	192.168.40.1	255.255.255.0	—
	S0/3/1	10.2.2.1	255.255.255.252	—
S1	VLAN 1	192.168.10.11	255.255.255.0	192.168.10.1
S3	VLAN 1	192.168.30.11	255.255.255.0	192.168.30.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.30.3	255.255.255.0	192.168.30.1

Задачи

Часть 1. Настройка топологии и инициализация устройств

Настройте оборудование в соответствии с топологией сети.

Часть 2. Настройка устройств и проверка подключения

Назначьте компьютерам статический IP-адрес.

Настройте маршрутизацию RIP на R1, ISP и R3.

Проверьте наличие подключения между всеми устройствами.

Часть 3. Настройка и проверка стандартных нумерованных списков ACL и стандартных именованных ACL-списков

Настройте, примените и проверьте работу нумерованных стандартных ACL-списков.

Настройте, примените и проверьте работу стандартных именованных ACL-списков.

Общие сведения/сценарий

Обеспечение сетевой безопасности является важным аспектом при разработке и управлении IP-сетями. Ценным навыком является умение применять соответствующие правила для фильтрации пакетов на основе установленной политики безопасности.

В данной лабораторной работе вы настроите правила фильтрации для двух офисов, представленных маршрутизаторами R1 и R3. Руководство определило некоторые правила в рамках политики безопасности для сетей LAN, расположенных на маршрутизаторах R1 и R3, которые вы должны реализовать. На маршрутизаторе ISP, расположенном между R1 и R3, ACL-списки не будут использоваться. У вас не будет прав административного доступа к маршрутизатору ISP, поскольку вы можете управлять только собственным оборудованием.

Необходимые ресурсы

3 маршрутизатора (Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (универсальный образ) или аналогичная модель).

2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель).

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

Консольные кабели для настройки устройств Cisco IOS через консольные порты.

Кабели Ethernet и последовательные кабели согласно топологии.

Часть 1: Настройка топологии и инициализация устройств

Шаг 1: Создайте сеть согласно топологии.

Часть 2: Настройка устройств и проверка подключения

Во второй части вам предстоит настроить базовые параметры маршрутизаторов, коммутаторов и компьютеров. Имена и адреса устройств указаны в топологии и таблице адресации.

Шаг 1: Настройте IP-адреса на PC-A и PC-C.

Шаг 2: Настройте базовые параметры маршрутизаторов.

a. Подключитесь к маршрутизатору с помощью консоли и перейдите в режим глобальной настройки.

b. Присвойте имена устройствам в соответствии с топологией.

c. Создайте интерфейсы loopback на каждом маршрутизаторе в соответствии с таблицей адресации.

d. Настройте IP-адреса интерфейсов в соответствии с топологией и таблицей адресации.

e. Установите тактовую частоту на **128000** для всех последовательных интерфейсов DCE.

f. Разрешите доступ по Telnet.

Шаг 3: Настройка базовых параметров на коммутаторах (дополнительно).

a. Подключитесь к коммутатору с помощью консоли и перейдите в режим глобального конфигурирования.

b. Присвойте имена устройствам в соответствии с топологией.

c. Назначьте административный IP-адрес интерфейса в соответствии с таблицами топологии и адресации.

d. Настройка шлюза по умолчанию.

e. Разрешите доступ по Telnet.

Шаг 4: Настройте маршрутизацию RIP на маршрутизаторах R1, ISP и R3.

a. Настройте протокол RIP версии 2 и анонсируйте все сети на маршрутизаторах R1, ISP и R3. Конфигурация OSPF для R1 и ISP приведена в справочных целях.

```
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# network 192.168.10.0
```

```
R1(config-router)# network 192.168.20.0
R1(config-router)# network 10.1.1.0

ISP(config)# router rip
ISP(config-router)# version 2
ISP(config-router)# network 209.165.200.224
ISP(config-router)# network 10.1.1.0
ISP(config-router)# network 10.2.2.0

R3(config)# router rip
R3(config-router)# version 2
R3(config-router)# network 192.168.30.0
R3(config-router)# network 10.2.2.0
```

b. После настройки RIP на маршрутизаторах R1, ISP и R3 убедитесь, что все маршрутизаторы имеют заполненные таблицы маршрутизации со всеми сетями. В случае необходимости выполните поиск и устранение неполадок.

Шаг 5: Проверьте наличие подключения между всеми устройствами.

Примечание. Соединение важно проверять **перед** настройкой и применением списков доступа! Удостовериться в правильной работе сети необходимо до начала фильтрации трафика.

a. От узла PC-A отправьте эхо-запрос на PC-C и интерфейс loopback маршрутизатора R3. Успешно ли выполнены эхо-запросы? _____

b. От маршрутизатора R1 отправьте эхо-запрос на PC-C и loopback-интерфейс на маршрутизаторе R3. Успешно ли выполнены эхо-запросы? _____

c. От узла PC-C отправьте эхо-запрос на PC-A и интерфейс loopback маршрутизатора R1. Успешно ли выполнены эхо-запросы? _____

d. От маршрутизатора R3 отправьте эхо-запрос на PC-A и интерфейс loopback маршрутизатора R1. Успешно ли выполнены эхо-запросы? _____

Часть 3: Настройка и проверка стандартных нумерованных ACL-списков и стандартных именованных ACL-списков

Шаг 1: Настройка стандартного именованного ACL-списка.

Стандартные ACL-списки фильтруют трафик, исходя только из адреса источника. Согласно принятой рекомендации стандартные ACL-списки следует настраивать и применять как можно ближе к назначению. Для первого списка доступа создайте стандартный нумерованный ACL-список, который пропускает трафик от всех узлов в сети 192.168.10.0/24 и всех узлов в сети 192.168.20.0/24 ко всем узлам в сети 192.168.30.0/24. Согласно политике безопасности в конце всех ACL-списков должна содержаться запрещающая запись контроля доступа **deny any** (ACE), которую также называют оператором ACL-списка.

Какую шаблонную маску вы будете использовать, чтобы разрешить всем узлам из сети 192.168.10.0/24 доступ к сети 192.168.30.0/24?

Следуя практическим рекомендациям Cisco, на каком маршрутизаторе вы разместите ACL-список?

На каком интерфейсе вы разместите этот список? В каком направлении вы его примените?

a. Настройте ACL-список на маршрутизаторе R3. В качестве номера списка доступа используйте 1.

```
R3(config)# access-list 1 remark Allow R1 LANs Access
R3(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R3(config)# access-list 1 permit 192.168.20.0 0.0.0.255
R3(config)# access-list 1 deny any
```

b. Примените ACL-список к подходящему интерфейсу в нужном направлении.

```
R3(config)# interface F0/1
R3(config-if)# ip access-group 1 out
```

c. Проверьте нумерованный ACL-список.

Использование команды **show** поможет вам при проверке синтаксиса и размещении списков ACL в вашем маршрутизаторе.

Какую команду вы будете использовать для просмотра полного списка доступа 1 со всеми записями ACE?

Какую команду вы будете использовать, чтобы просмотреть, где и в каком направлении был применен список доступа?

1) На маршрутизаторе R3 выполните команду **show access-lists 1**.

```
R3# show access-list 1
Standard IP access list 1
    10 permit 192.168.10.0, wildcard bits 0.0.0.255
    20 permit 192.168.20.0, wildcard bits 0.0.0.255
    30 deny   any
```

2) На маршрутизаторе R3 выполните команду **show ip interface f0/1**.

```
R3# show ip interface f0/1
FastEthernet0/1 is up, line protocol is up
  Internet address is 192.168.30.1/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is 1
  Inbound access list is not set
  Выходные данные опущены
```

3) Проверьте, пропускает ли ACL-список трафик из сети 192.168.10.0/24 в сеть 192.168.30.0/24. Из командной строки узла PC-A отправьте эхо-запрос на IP-адрес PC-C. Успешно ли выполнена проверка связи? _____

4) Проверьте, пропускает ли ACL-список трафик из сети 192.168.20.0/24 в сеть 192.168.30.0/24. Вам нужно выполнить расширенный эхо-запрос и использовать loopback-адрес 0 на маршрутизаторе R1 в качестве источника. Отправьте эхо-запрос на IP-адрес узла PC-C. Успешно ли выполнена проверка связи? _____

```
R1# ping
Protocol [ip]:
Target IP address: 192.168.30.3
Repeat count [5]:
```

```
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.20.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.3, timeout is 2 seconds:
Packet sent with a source address of 192.168.20.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
```

d. Из командной строки маршрутизатора R1 снова отправьте эхо-запрос на IP-адрес узла PC-C.

```
R1# ping 192.168.30.3
```

Успешно ли выполнен эхо-запрос? Поясните свой ответ.

Шаг 2: Настройте стандартный именованный ACL-список.

Создайте стандартный именованный ACL-список, который соответствует следующему правилу: список должен разрешать доступ для трафика со всех узлов из сети 192.168.40.0/24 ко всем узлам в сети 192.168.10.0/24. Кроме того, доступ в сеть 192.168.10.0/24 должен быть разрешен только для узла PC-C. Этот список доступа должен быть назван BRANCH-OFFICE-POLICY.

Следуя практическим рекомендациям Cisco, на каком маршрутизаторе вы разместите ACL-список?

На каком интерфейсе вы разместите этот список? В каком направлении вы его примените?

a. Создайте стандартный ACL-список под именем BRANCH-OFFICE-POLICY на маршрутизаторе R1.

```
R1(config)# ip access-list standard BRANCH-OFFICE-POLICY
R1(config-std-nacl)# permit host 192.168.30.3
R1(config-std-nacl)# permit 192.168.40.0 0.0.0.255
R1(config-std-nacl)# end
R1#
*Feb 15 15:56:55.707: %SYS-5-CONFIG_I: Configured from console by console
```

Взгляните на первую запись ACE в списке доступа и ответьте, можно ли записать это иначе?

b. Примените ACL-список к подходящему интерфейсу в нужном направлении.

```
R1# config t
R1(config)# interface f0/1
R1(config-if)# ip access-group BRANCH-OFFICE-POLICY out
```

c. Проверьте именованный ACL-список.

1) На R1 выполните команду **show access-lists.**

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
    10 permit 192.168.30.3
```

```
        20 permit 192.168.40.0, wildcard bits 0.0.0.255
```

Существуют ли различия между ACL-списком на маршрутизаторе R1 и ACL-списком на маршрутизаторе R3? Если да, в чем они заключаются?

2) На маршрутизаторе R1 выполните команду **show ip interface g0/1**.

```
R1# show ip interface f0/1
fasttEthernet0/1 is up, line protocol is up
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is BRANCH-OFFICE-POLICY
  Inbound access list is not set
<Данные опущены>
```

3) Проверьте работу ACL-списка. Из командной строки узла PC-C отправьте эхо-запрос на IP-адрес узла PC-A. Успешно ли выполнена проверка связи? _____

4) Проверьте ACL-список, чтобы удостовериться, что доступ к сети 192.168.10.0/24 настроен только на узле PC-C. Вам нужно выполнить расширенный эхо-запрос и использовать адрес G0/1 на маршрутизаторе R3 в качестве источника. Отправьте эхо-запрос на IP-адрес компьютера PC-A. Успешно ли выполнена проверка связи? _____

5) Проверьте, пропускает ли ACL-список трафик из сети 192.168.40.0/24 в сеть 192.168.10.0/24. Вам нужно выполнить расширенный эхо-запрос и использовать loopback-адрес 0 на маршрутизаторе R3 в качестве источника. Отправьте эхо-запрос на IP-адрес компьютера PC-A. Успешно ли выполнена проверка связи? _____

Вопросы для повторения

Как вы видите, стандартные ACL-списки достаточно эффективны и полезны. Почему вам может понадобиться использовать расширенные списки ACL?

В большинстве случаев при использовании именованного ACL-списка требуется введение большего количества строк, нежели при использовании нумерованного ACL-списка. Почему вы бы предпочли использовать именованный ACL-список, а не нумерованный?

Лабораторная работа 7

БАЗОВАЯ НАСТРОЙКА DHCPV4 НА МАРШРУТИЗАТОРЕ

Топология

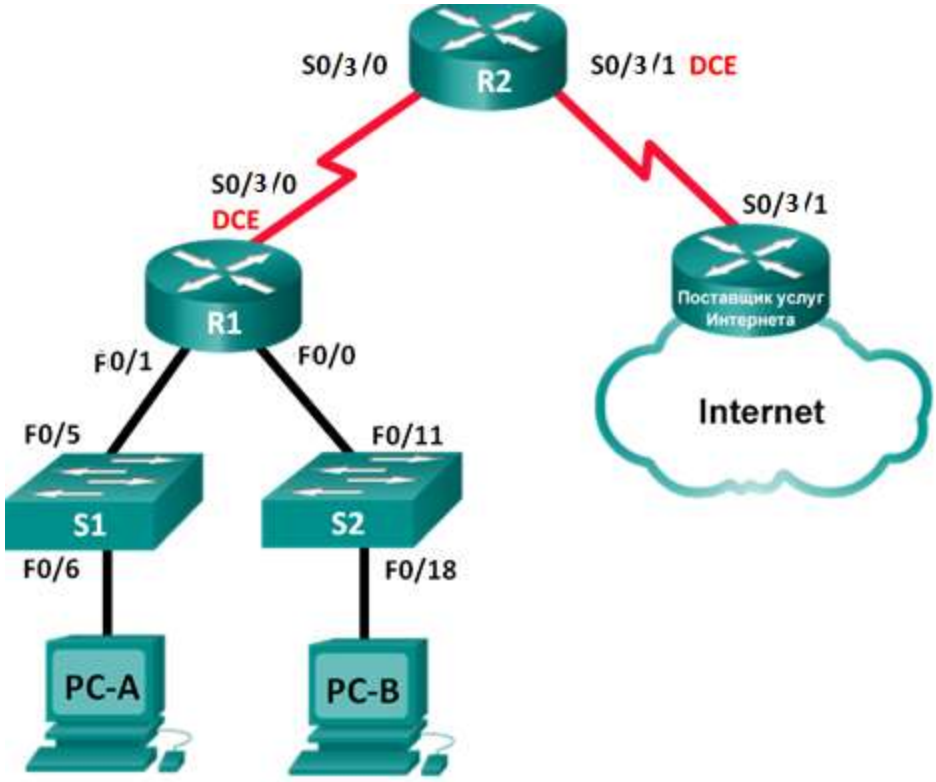

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	F0/0	192.168.0.1	255.255.255.0	—
	F0/1	192.168.1.1	255.255.255.0	—
	S0/3/0 (DCE)	192.168.2.253	255.255.255.252	—
R2	S0/3/0	192.168.2.254	255.255.255.252	—
	S0/3/1 (DCE)	209.165.200.226	255.255.255.224	—
ISP	S0/3/1	209.165.200.225	255.255.255.224	—
PC-A	Сетевой адаптер	DHCP	DHCP	DHCP
PC-B	Сетевой адаптер	DHCP	DHCP	DHCP

Задачи

Часть 1. Создание сети и настройка основных параметров устройства

Часть 2. Выполнение настройки DHCPv4-сервера и агента-ретранслятора DHCP

Общие сведения/сценарий

Протокол динамической конфигурации сетевого узла (DHCP) — сетевой протокол, позволяющий сетевым администраторам управлять и автоматизировать назначение IP-адресов. Без использования DHCP администратору необходимо вручную назначать и настраивать IP-адреса, предпочтительные DNS-серверы и шлюзы по умолчанию. По мере увеличения сети и перемещении устройств из одной внутренней сети в другую это становится административной проблемой.

В предложенном сценарии размеры компании увеличились, и сетевые администраторы больше не имеют возможности назначать IP-адреса для устройств вручную. Ваша задача заключается в настройке маршрутизатора R2 для назначения IPv4-адресов в двух разных подсетях, подключенных к маршрутизатору R1.

Примечание. В данной лабораторной работе содержится минимальный набор команд, необходимых для настройки DHCP.

Необходимые ресурсы

3 маршрутизатора (Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (универсальный образ) или аналогичная модель).

2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель).

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

Консольные кабели для настройки устройств Cisco IOS через консольные порты.

Кабели Ethernet и последовательные кабели согласно топологии.

Часть 1: Создание сети и настройка основных параметров устройства

В первой части лабораторной работы вам предстоит создать топологию сети и настроить основные параметры на маршрутизаторах и коммутаторах, такие как пароли и IP-адреса. Также вам предстоит настроить параметры IP для компьютеров в приведенной топологии.

Шаг 1: Создайте сеть согласно топологии.

a. Настройте имена хостов в соответствии с топологией.

b. Настройте на маршрутизаторе IPv4-адреса в соответствии с топологией.

c. Для последовательных интерфейсов DCE установите тактовую частоту 128000.

Шаг 2: Настройте на маршрутизаторах динамическую маршрутизацию, статическую маршрутизацию и маршрутизацию по умолчанию.

a. Настройте протокол RIPv2 на маршрутизаторе R1.

```
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# network 192.168.0.0
R1(config-router)# network 192.168.1.0
R1(config-router)# network 192.168.2.252
R1(config-router)# no auto-summary
```

b. Настройте протокол RIPv2 и маршрут по умолчанию к ISP на маршрутизаторе R2.

```
R2(config)# router rip
R1(config-router)# version 2
R2(config-router)# network 192.168.2.252
R2(config-router)# default-information originate
R2(config-router)# exit
R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.225
```

c. Настройте суммарный статический маршрут на ISP для доступа к сетям маршрутизаторов R1 и R2.

```
ISP(config)# ip route 192.168.0.0 255.255.252.0 209.165.200.226
```

d. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

Шаг 3: Выполните проверку сетевого соединения между маршрутизаторами.

При неудачных эхо-запросах между маршрутизаторами прежде чем переходить к следующему шагу исправьте возникшие ошибки. Используйте команды **show ip route** и **show ip interface brief**, чтобы определить возможные неполадки.

Шаг 4: Убедитесь, что ПК на узлах настроены для работы DHCP.

Часть 2: Настройка DHCPv4-сервера и агента-ретранслятора DHCP

Для того чтобы автоматически назначить адресную информацию в сети, вам необходимо настроить маршрутизатор R2 в качестве сервера DHCPv4, а маршрутизатор R1 в качестве агента-ретранслятора.

Шаг 1: Выполните настройку сервера DHCPv4 на маршрутизаторе R2.

На маршрутизаторе R2 необходимо создать пул DHCP-адресов для каждой локальной сети маршрутизатора R1. Используйте имя пула **R1G0** для интерфейса F0/0 LAN и **R1G1** для интерфейса F0/1 LAN. Также вам нужно исключить адреса, которые не будут назначаться из пула адресов. Исключать адреса рекомендуется в первую очередь, чтобы предотвратить их случайную аренду для других устройств.

Исключите первые девять адресов из каждой локальной сети маршрутизатора R1, начиная с .1. Все другие адреса должны быть доступны в пуле DHCP. Убедитесь, что каждый пул DHCP содержит шлюз по умолчанию, домен **ccna-lab.com**, сервер DNS (209.165.200.225), а срок аренды составляет два дня.

В строках ниже запишите команды, необходимые для настройки служб DHCP на маршрутизаторе R2, включая те, что требуются для исключения DHCP-адресов и создания пулов DHCP.

Команды настройки DHCP

Маршрутизатор R1

```
R1(config)# interface f0/0
R1(config-if)# ip helper-address 192.168.2.254
R1(config-if)# exit
R1(config-if)# interface f0/1
R1(config-if)# ip helper-address 192.168.2.254
```

Шаг 1: Настройте маршрутизатор R1 в качестве агента ретрансляции.

Настройте вспомогательные IP-адреса на маршрутизаторе R1, чтобы переслать все DHCP-запросы на сервер DHCP маршрутизатора R2.

Маршрутизатор M2

```
R2(config)# ip dhcp excluded-address 192.168.0.1 192.168.0.9
R2(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.9
R2(config)# ip dhcp pool R1G1
R2(dhcp-config)# network 192.168.1.0 255.255.255.0
R2(dhcp-config)# default-router 192.168.1.1
R2(dhcp-config)# dns-server 209.165.200.225
R2(dhcp-config)# domain-name ccna-lab.com
R2(dhcp-config)# lease 2
R2(dhcp-config)# exit
R2(config)# ip dhcp pool R1G0
R2(dhcp-config)# network 192.168.0.0 255.255.255.0
R2(dhcp-config)# default-router 192.168.0.1
R2(dhcp-config)# dns-server 209.165.200.225
R2(dhcp-config)# domain-name ccna-lab.com
R2(dhcp-config)# lease 2
```

На узлах PC-A или PC-B откройте командную строку и введите команду **ipconfig /all**. Получил ли какой-либо из узловых ПК IP-адрес от сервера DHCP?

Шаг 2: Проверьте работу служб DHCP и аренды адресов на маршрутизаторе R2.

a. На маршрутизаторе R2 выполните команду **show ip dhcp binding**, чтобы просмотреть список арендованных DHCP адресов.

b. На маршрутизаторе R2 выполните команду **show ip dhcp show statistics**, чтобы отобразить статистику пула DHCP и активность сообщений.

c. На маршрутизаторе R2 выполните команду **show ip dhcp pool**, чтобы просмотреть настройки пула DHCP.

d. На маршрутизаторе R2 выполните команду **show run | section dhcp**, чтобы просмотреть конфигурацию DHCP в текущей конфигурации.

e. На маршрутизаторе R1 выполните команду **show run interface** для интерфейсов G0/0 и G0/1, чтобы просмотреть настройки ретранслятора DHCP в текущей конфигурации.

Вопросы для повторения

Как вы думаете, в чем заключается преимущество использования агентов DHCP-ретрансляции вместо использования нескольких маршрутизаторов, работающих в качестве серверов DHCP?

Лабораторная работа 8

НАСТРОЙКА СТАТИЧЕСКОГО NAT

Топология

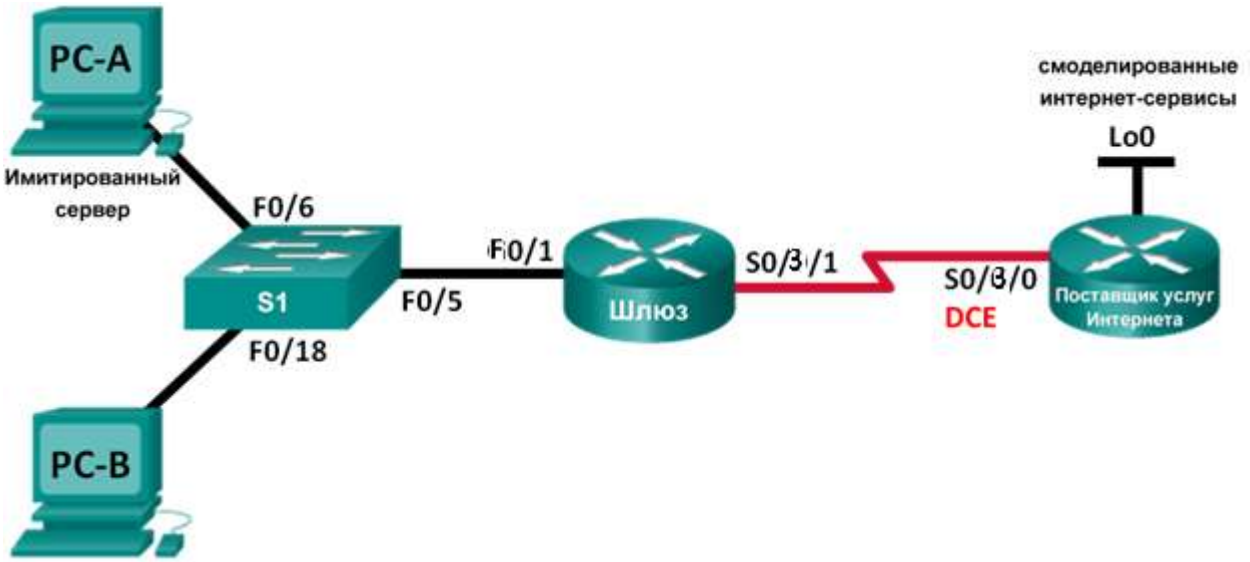

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
Шлюз	F0/1	192.168.1.1	255.255.255.0	—
	S0/3/1	209.165.201.18	255.255.255.252	—
ISP	S0/3/0 (DCE)	209.165.201.17	255.255.255.252	—
	Lo0	192.31.7.1	255.255.255.255	—
PC-A (смоделированный сервер)	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1

Задачи

Часть 1. Построение сети и проверка соединения

Часть 2. Настройка и проверка статического NAT

Общие сведения/сценарий

Преобразование (NAT) — это процесс, при котором сетевое устройство, например маршрутизатор Cisco, назначает публичный адрес узлам в пределах частной сети. NAT используют для сокращения количества публичных IP-адресов, используемых организацией, поскольку количество доступных публичных IPv4-адресов ограничено.

Согласно сценарию данной лабораторной работы интернет-провайдер выделил для компании пространство публичных IP-адресов 209.165.200.224/27. В результате компания получила 30 публичных IP-адресов. Адреса от 209.165.200.225 до 209.165.200.241 подлежат статическому распределению, а адреса от 209.165.200.242 до 209.165.200.254 — динамическому распределению. Статический маршрут используется на участке от интернет-провайдера до маршрутизатора, являющегося шлюзом, в то время как маршрут по умолчанию используется на участке от шлюза до маршрутизатора интернет-провайдера. Подключение интернет-провайдера к Интернету смоделировано loopback-адресом на маршрутизаторе интернет-провайдера.

Необходимые ресурсы

2 маршрутизатора (Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (универсальный образ) или аналогичная модель).

1 коммутатор (Cisco 2960 с ПО Cisco IOS версии 15.0(2) с образом lanbasek9 или аналогичная модель).

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

Консольные кабели для настройки устройств Cisco IOS через консольные порты.

Кабели Ethernet и последовательные кабели согласно топологии.

Часть 1: Построение сети и проверка связи

В первой части вам предстоит настроить топологию сети и выполнить базовую настройку, например, IP-адреса интерфейсов, статическую маршрутизацию, доступ к устройствам и пароли.

Шаг 1: Создайте сеть согласно топологии.

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

Шаг 2: Настройте узлы ПК.

a. Подключитесь к маршрутизатору с помощью консоли и перейдите в режим глобальной настройки.

b. Настройте имена хостов в соответствии с топологией.

Шаг 3: Для симуляции создайте веб-сервер на ISP.

a. Создайте локального пользователя с именем **webuser** с зашифрованным паролем **webpass**.

```
ISP(config)# username webuser privilege 15 secret webpass
```

b. Включите службу HTTP-сервера на маршрутизаторе ISP.

```
ISP(config)# ip http server
```

c. Настройте сервис HTTP таким образом, чтобы он использовал локальную базу данных пользователей.

```
ISP(config)# ip http authentication local
```

Шаг 4: Настройте статическую маршрутизацию.

a. Создайте статический маршрут на маршрутизаторе ISP до диапазона назначенных публичных сетевых адресов 209.165.200.224/27 маршрутизатора Gateway

```
ISP(config)# ip route 209.165.200.224 255.255.255.224 209.165.201.18
```

b. Создайте маршрут по умолчанию от маршрутизатора Gateway к маршрутизатору ISP.

```
Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

Шаг 5: Сохранение текущей конфигурации в качестве начальной.

Шаг 6: Проверьте подключение к сети.

a. С компьютеров отправьте эхо-запросы на интерфейс G0/1 маршрутизатора Gateway. Выполните отладку, если эхо-запрос не проходит.

b. Отобразите таблицы маршрутизации на обоих маршрутизаторах, чтобы убедиться, что статические маршруты содержатся в таблице маршрутизации и правильно настроены на обоих маршрутизаторах.

Часть 2: Настройка и проверка статического преобразования NAT

В статическом NAT используется сопоставление локальных и глобальных адресов по схеме «один к одному». Метод статического преобразования особенно полезен для веб-серверов или устройств, которые должны иметь постоянный адрес и быть доступными из Интернета.

Шаг 1: Настройте статическое сопоставление.

Статическая привязка должна быть настроена для преобразования маршрутизатором частного внутреннего адреса сервера 192.168.1.20 в публичный адрес 209.165.200.225 и обратно. Это позволит пользователю из Интернета получить доступ к компьютеру PC-A. Компьютер PC-A моделирует сервер или устройство с постоянным адресом, к которому можно получить доступ из Интернета.

```
Gateway(config)# ip nat inside source static 192.168.1.20 209.165.200.225
```

Шаг 2: Задайте интерфейсы.

Выполните на интерфейсах команды **ip nat inside** и **ip nat outside**.

```
Gateway(config)# interface f0/1
Gateway(config-if)# ip nat inside
Gateway(config-if)# interface s0/3/1
Gateway(config-if)# ip nat outside
```

Шаг 3: Протестируйте настройку.

a. Отобразите таблицу статических преобразований NAT с помощью команды **show ip nat translations**.

```
Gateway# show ip nat translations
Pro Inside global      Inside local         Outside local      Outside global
--- 209.165.200.225    192.168.1.20         ---                ---
```

Во что был преобразован внутренний адрес локального узла?

192.168.1.20 = _____

Кем назначен внутренний глобальный адрес?

Кем назначен внутренний локальный адрес?

b. На компьютере ПК A отправьте эхо-запрос на интерфейс Lo0 (192.31.7.1) маршрутизатора ISP. Если эхо-запрос не прошел, выполните отладку. На маршрутизаторе Gateway просмотрите таблицу NAT.

```
Gateway# show ip nat translations
Pro Inside global      Inside local         Outside local      Outside global
icmp 209.165.200.225:1 192.168.1.20:1       192.31.7.1:1       192.31.7.1:1
--- 209.165.200.225    192.168.1.20         ---                ---
```

Когда компьютер ПК A отправил ICMP-запрос (эхо-запрос) на адрес ISP 192.31.7.1, в таблицу была добавлена запись NAT, где ICMP указан в виде протокола.

Какой номер порта использовался в данном обмене пакетами ICMP? _____

c. С компьютера ПК A подключитесь по Telnet к интерфейсу Lo0 ISP и отобразите таблицу NAT.

```
Pro Inside global        Inside local       Outside local      Outside global
icmp 209.165.200.225:1   192.168.1.20:1     192.31.7.1:1       192.31.7.1:1
tcp 209.165.200.225:1034 192.168.1.20:1034  192.31.7.1:23      192.31.7.1:23
--- 209.165.200.225      192.168.1.20       ---                ---
```

Примечание. NAT для запроса ICMP может устареть, из-за чего он будет удален из таблицы NAT.

Какой протокол использовался для этого преобразования? _____

Укажите номера используемых портов.

Внутренний глобальный/локальный: _____

Внешний глобальный/локальный: _____

d. Поскольку статический NAT настроен для ПК A, убедитесь в успешном прохождении эхо-запроса от ISP до ПК A по публичному адресу через статический NAT (209.165.200.225).

e. На маршрутизаторе Gateway отобразите таблицу NAT, чтобы проверить преобразование.

```
Gateway# show ip nat translations
Pro Inside global       Inside local       Outside local      Outside global
icmp 209.165.200.225:12 192.168.1.20:12    209.165.201.17:12  209.165.201.17:12
--- 209.165.200.225     192.168.1.20       ---                ---
```

Обратите внимание, что внешний локальный и внешний глобальный адреса совпадают. Этот адрес — адрес источника в удаленной сети ISP. Для успешной отправки эхо-запроса от ISP, внутренний глобальный адрес статического NAT 209.165.200.225 был преобразован во внутренний локальный адрес компьютера ПК A (192.168.1.20).

f. Проверьте статистику NAT, выполнив команду **show ip nat statistics** на маршрутизаторе, являющемся шлюзом.

```
Gateway# show ip nat statistics
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Peak translations: 2, occurred 0:02:12 ago
Outside interfaces:
  Serial0/3/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 39  Misses: 0
CEF Translated packets: 39, CEF Punted packets: 0
Expired translations: 3
```

```
Dynamic mappings:

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Примечание. Показанный результат приведен исключительно в качестве примера. Полученные вами результаты могут не совпадать с ним.

Вопросы для повторения

Зачем нужно использовать NAT в сети?

В чем заключаются ограничения NAT?

Лабораторная работа 9

НАСТРОЙКА ПРЕОБРАЗОВАНИЯ АДРЕСА И НОМЕРА ПОРТА (PAT)

Топология

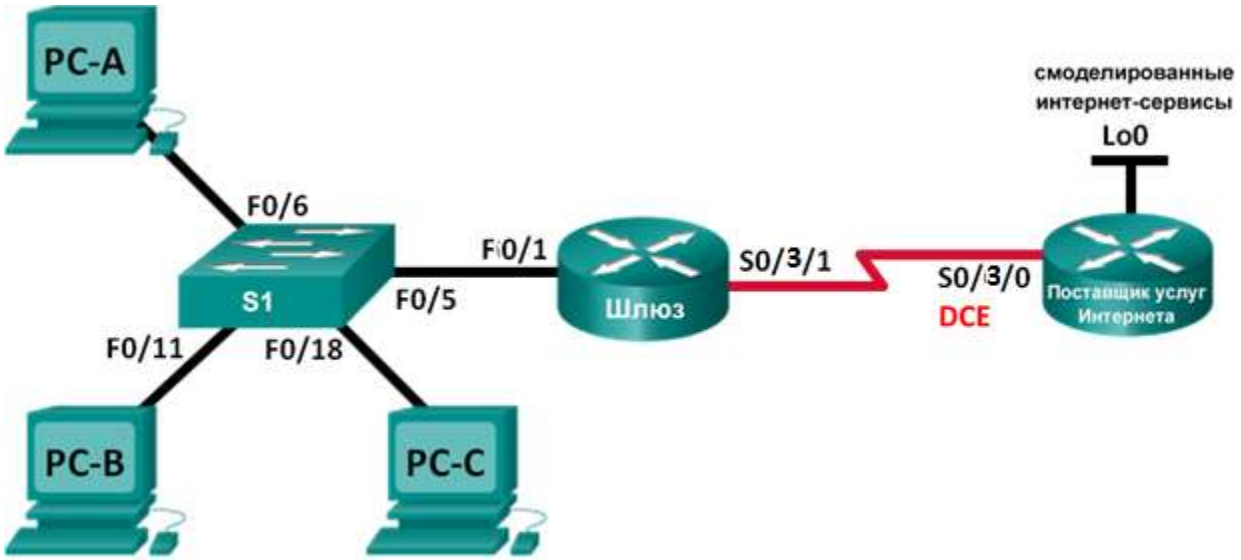

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
Шлюз	F0/1	192.168.1.1	255.255.255.0	—
	S0/3/1	209.165.201.18	255.255.255.252	—
ISP	S0/3/0 (DCE)	209.165.201.17	255.255.255.252	—
	Lo0	192.31.7.1	255.255.255.255	—
PC-A	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.22	255.255.255.0	192.168.1.1

Задачи

Часть 1. Построение сети и проверка соединения

Часть 2. Настройка и проверка пула NAT с перегрузкой

Часть 3. Настройка и проверка PAT

Общие сведения/сценарий

По сценарию первой части лабораторной работы интернет-провайдер выделил вашей компании диапазон публичных IP-адресов 209.165.200.224/29. Благодаря этому компания получила шесть публичных IP-адресов. Перегрузка пула динамического NAT использует пул IP-адресов по модели «множество к множеству». Маршрутизатор использует первый IP-адрес в пуле и назначает подключения с помощью IP-адреса и уникального номера порта. После достижения на маршрутизаторе максимального количества преобразований для одного IP-адреса (зависит от платформы и оборудования), используется следующий IP-адрес в пуле. Перегрузка пула NAT представляет собой вид преобразования адреса и номера порта (PAT), которое перегружает группу публичных IPv4-адресов.

Во второй части интернет-провайдер выделил вашей компании один IP-адрес, 209.165.201.18, для подключения маршрутизатора Gateway, являющегося шлюзом, к сети интернет-провайдера. Для преобразования нескольких внутренних адресов в один пригодный для использования публичный адрес используйте преобразование адресов портов (PAT). Вы выполните тестирование, отображение и проверку осуществления всех преобразований и проанализируете статистику NAT/PAT для контроля процесса.

Необходимые ресурсы

2 маршрутизатора (Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (универсальный образ) или аналогичная модель).

1 коммутатор (Cisco 2960 с ПО Cisco IOS версии 15.0(2) с образом lanbasek9 или аналогичная модель).

3 ПК (Windows 7, Vista или XP с программой эмуляции терминала, например, Tera Term).

Консольные кабели для настройки устройств Cisco IOS через консольные порты.

Кабели Ethernet и последовательные кабели согласно топологии.

Часть 1: Построение сети и проверка связи

В первой части вам предстоит настроить топологию сети и выполнить базовую настройку

Шаг 1: Создайте сеть согласно топологии.

Шаг 2: Настройте узлы ПК.

Настройте имена хостов в соответствии с топологией.

Шаг 3: Настройте статическую маршрутизацию.

a. Создайте статический маршрут от маршрутизатора ISP к маршрутизатору Gateway.

```
ISP(config)# ip route 209.165.200.224 255.255.255.248 209.165.201.18
```

b. Создайте маршрут по умолчанию от маршрутизатора Gateway к маршрутизатору ISP.

```
Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

Шаг 4: Проверьте подключение к сети.

a. С компьютеров отправьте эхо-запросы на интерфейс G0/1 маршрутизатора Gateway. Выполните отладку, если эхо-запрос не проходит.

b. Проверьте настройку статических маршрутов на обоих маршрутизаторах.

Часть 2: Настройка и проверка пула NAT с перегрузкой

Во второй части вам предстоит настроить Маршрутизатор Gateway, для преобразования IP-адреса из сети 192.168.1.0/24 в один из шести пригодных к использованию адресов в диапазоне 209.165.200.224/29.

Шаг 1: Создайте ACL, соответствующий диапазону частных IP-адресов локальной сети.

ACL-список 1 используется для разрешения преобразования сети 192.168.1.0/24.

```
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

Шаг 2: Определите пул пригодных к использованию публичных IP-адресов.

```
Gateway(config)# ip nat pool public_access 209.165.200.225 209.165.200.230
netmask 255.255.255.248
```

Шаг 3: Определите NAT из внутреннего списка адресов источника на пул внешних адресов.

```
Gateway(config)# ip nat inside source list 1 pool public_access overload
```

Шаг 4: Задайте интерфейсы.

Выполните на интерфейсах команды **ip nat inside** и **ip nat outside**.

```
Gateway(config)# interface f0/1
Gateway(config-if)# ip nat inside
Gateway(config-if)# interface s0/3/1
Gateway(config-if)# ip nat outside
```

Шаг 5: Проверьте настройку пула NAT с перегрузкой.

a. От каждого ПК отправьте эхо-запрос на адрес маршрутизатора интернет-провайдера — 192.31.7.1.

b. Просмотрите статистику NAT для маршрутизатора Gateway.

```
Gateway# show ip nat statistics
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Peak translations: 3, occurred 0:00:25 ago
Outside interfaces:
  Serial0/3/1
Inside interfaces:
  fastEthernet0/1
Hits: 24  Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 3
 pool public_access: netmask 255.255.255.248
        start 209.165.200.225 end 209.165.200.230
        type generic, total addresses 6, allocated 1 (16%), misses 0

Total doors: 0
```

```
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

c. Отобразите преобразования NAT на маршрутизаторе Gateway.

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.225:0 192.168.1.20:1     192.31.7.1:1       192.31.7.1:0
icmp 209.165.200.225:1 192.168.1.21:1     192.31.7.1:1       192.31.7.1:1
icmp 209.165.200.225:2 192.168.1.22:1     192.31.7.1:1       192.31.7.1:2
```

Примечание. В зависимости от времени, истекшего с момента отправки эхо-запросов с каждого ПК, вы можете не увидеть все три преобразования. Для преобразований ICMP характерны низкие значения времени ожидания.

Сколько внутренних локальных IP-адресов указано в примере выходных данных выше?

Сколько указано внутренних глобальных IP-адресов? _____

Сколько номеров портов используется в паре с внутренними глобальными адресами? _____

Что произойдет в результате отправки эхо-запроса на внутренний локальный адрес компьютера ПК A с маршрутизатора интернет-провайдера? Почему?

Часть 3: Настройка и проверка преобразования PAT

В третьей части вам предстоит настроить PAT, используя для определения внешних адресов интерфейс вместо пула адресов. Не все команды из части 2 будут использоваться в части 3.

Шаг 1: Очистите преобразования NAT и статистику на маршрутизаторе Gateway.

```
Gateway# clear ip nat translation *
Gateway# clear ip nat statistics
```

Шаг 2: Проверьте настройку NAT.

a. Убедитесь, что статистика стерта.

b. Убедитесь, что внешние и внутренние интерфейсы настроены для преобразований NAT.

c. Убедитесь, что ACL-список по-прежнему настроен для преобразований NAT.

Какую команду вы использовали для того, чтобы подтвердить результаты после выполнения шагов от a до c?

Шаг 3: Удалите пул пригодных к использованию публичных IP-адресов.

```
Gateway(config)# no ip nat pool public_access 209.165.200.225 209.165.200.230
netmask 255.255.255.248
```

Шаг 4: Удалите преобразование NAT с ACL в пул внешних адресов.

```
Gateway(config)# no ip nat inside source list 1 pool public_access overload
```

Шаг 5: Сопоставьте список источников с внешним интерфейсом.

```
Gateway(config)# ip nat inside source list 1 interface serial 0/3/1 overload
```

Шаг 6: Проверьте настройку PAT.

a. От каждого ПК отправьте эхо-запрос на адрес маршрутизатора интернет-провайдера — 192.31.7.1.

b. Просмотрите статистику NAT для маршрутизатора Gateway.

```
Gateway# show ip nat statistics
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Peak translations: 3, occurred 0:00:19 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 24  Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 2] access-list 1 interface Serial0/0/1 refcount 3

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

c. Отобразите преобразования NAT на маршрутизаторе Gateway.

```
Gateway# show ip nat translations
Pro Inside global      Inside local         Outside local      Outside global
icmp 209.165.201.18:3  192.168.1.20:1     192.31.7.1:1       192.31.7.1:3
icmp 209.165.201.18:1  192.168.1.21:1     192.31.7.1:1       192.31.7.1:1
icmp 209.165.201.18:4  192.168.1.22:1     192.31.7.1:1       192.31.7.1:4
```

Вопросы для повторения

В чем заключаются преимущества PAT?

Приложение

СБРОС КОММУТАТОРА CISCO 2960

1. Подключиться терминалом к консольному порту со скоростью 9600
2. Выключить свитч. Отсоединить кабель питания на 15 секунд, затем включить кабель обратно и зажать на передней панели свитча кнопку "Mode" пока светодиод System мигает зеленым. Продолжать нажимать кнопку "Mode" когда светодиод System загорелся янтарным. Когда светодиод престал гореть кнопку "Mode" можно отпустить.
3. Инициализируем файловую систему на флэше командой flash_init
4. Смотрим контент флэша с помощью команды dir flash:
5. Удаляем конфигурационный файл config.text командой delete flash:config.text
6. Загружаем IOS с помощью команды boot

СБРОС МАРШРУТИЗАТОРА CISCO

1. Подключитесь к устройству
2. Включите электропитание устройства. На экране консоли вы увидите процесс начала загрузки IOS;
3. В начальный момент загрузки устройства, желательно до момента распаковки с flesh-памяти операционной системы, вам следует послать устройству сигнал Break, нажав на клавиатуре одновременно две клавиши Ctrl+Break;
4. Устройство войдет в режим ROM Monitor, о чем будет свидетельствовать приглашение:

```
rommon 1>
```

5. В этом режиме установите значение конфигурационного регистра 0x2142, при котором устройство не будет использовать при загрузке конфиг, записанный во flesh-память:

```
rommon 1> confreg 0x2142
Yuo mast reset or power cycle for new config to take effect
rommon 2>
```

6. Перезагрузите устройство:

```
rommon 2> reset
rommon 3>
```

7. После перезагрузки вашего устройства Cisco на вопрос IOS о начальном конфигурировании вам следует ответить No:

```
Would you like to enter the initial configuration dialog? [yes/no]: No
Press RETURN to get started!
Router>
```

8. Теперь Cisco позволит войти в привилегированный режим без пароля:

```
Router> enable
Router#
```

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.