**Федеральное государственное автономное образовательное учреждение**

**высшего образования**   
**"Национальный исследовательский университет**   
**"Высшая школа экономики"**

Московский институт электроники и математики

им. А. Н. Тихонова НИУ ВШЭ

Департамент компьютерной инженерии

Лабораторная работа №8

по теме:

«11.4.1.2 Packet Tracer – Skills Integration;11.4.3.6 Packet Tracer – Troubleshooting Connectivity Issues; Appendix Packet Tracer – Configuring an Integrated Router; Appendix Packet Tracer – Subneting Scenario;»

По дисциплине

«Вычислительные системы и компьютерные сети»

|  |  |
| --- | --- |
| **Группа:** | **БИВ203** |
| **Студент:** | **Камаров Лазизбек** |

**Москва 2022**

**Оглавление**

[11.4.1.2 3](#_Toc120143366)

[Решение 11.4.1.2 5](#_Toc120143367)

[11.4.3.6 13](#_Toc120143368)

[Решение 11.4.3.6 16](#_Toc120143369)

[Appendix Router 16](#_Toc120143370)

[Решение Appendix Router 18](#_Toc120143371)

[Appendix Scenario 18](#_Toc120143372)

[Решение Appendix Scenario 21](#_Toc120143373)

# 11.4.1.2

**Таблица адресации**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Устройство** | **Интерфейс** | **IPv4-адрес** | **Маска подсети** | **Шлюз по умолчанию** |
| **IPv6-адрес/префикс** | **Локальный адрес канала IPv6** |
| R1 | G0/0 |  |  | — |
| 2001:DB8:2::1/64 | FE80::1 | — |
| G0/1 |  |  | — |
| 2001:DB8:ACAD:1::1/64 | FE80::1 | — |
| G0/2 |  |  | — |
| 2001:DB8:ACAD:2::1/64 | FE80::1 | — |
| S0/0/1 | 172.16.1.2 | 255.255.255.252 | — |
| 2001:DB8:2::1/64 | FE80::1 | — |
| Central | S0/0/0 | 209.165.200.226 | 255.255.255.252 | — |
| 2001:DB8:1::1/64 | FE80::2 | — |
| S0/0/1 | 172.16.1.1 | 255.255.255.252 | — |
| 2001:DB8:2::2/64 | FE80::2 | — |
| S1 | VLAN 1 |  |  |  |
| S2 | VLAN 1 |  |  |  |
| S3 | VLAN 1 |  |  |  |
| Staff | NIC |  |  |  |
| 2001:DB8:ACAD::2/64 | FE80::2 | FE80::1 |
| Sales | NIC |  |  |  |
| 2001:DB8:ACAD:1::2/64 | FE80::2 | FE80::1 |
| IT | NIC |  |  |  |
| 2001:DB8:ACAD:2::2/64 | FE80::2 | FE80::1 |
| Web | NIC | 64.100.0.3 | 255.255.255.248 | 64.100.0.1 |
| 2001:DB8:CAFE::3/64 | FE80::2 | FE80::1 |

**Сценарий/общие сведения**

Центральный маршрутизатор Central, кластер ISP и веб-сервер Web полностью настроены. Ваша задача — создать новую схему адресации по протоколу IPv4, включающую четыре подсети, используя адрес 192.168.0.0/24. ИТ-отделу (IT) требуется 25 узлов. Отделу продаж (Sales) требуется 50 узлов. Подсеть для остальных сотрудников (Staff) должна быть рассчитана на 100 узлов. В будущем планируется добавление гостевой подсети (Guest), включающей в себя 25 узлов. Вам также нужно задать основные параметры безопасности и настроить интерфейс R1. Кроме того, вы должны настроить виртуальный интерфейс коммутатора (SVI) и задать основные параметры безопасности на коммутаторах S1, S2 и S3.

**Требования**

**IPv4-адресация**

         Создайте подсети в соответствии с требованиями узла, используя адрес 192.168.0.0/24.

         Staff: 100 узлов

         Sales: 50 узлов

         IT: 25 узлов

         Сеть Guest, которая будет добавлена позже: 25 узлов

         Запишите назначенные IPv4-адреса в таблицу адресации.

         Запишите подсеть для сети Guest:

**Настройка компьютера**

         Настройте компьютеры Staff, Sales и IT, используя назначенный IPv4-адрес, маску подсети и шлюз по умолчанию в соответствии с вашей схемой адресации.

         Назначьте адреса одноадресной рассылки IPv6 и локального канала, шлюз по умолчанию для сетей Staff, Sales и IT согласно таблице адресации.

**Настройка маршрутизатора R1**

         Настройте имя устройства в соответствии с таблицей адресации.

         Отключите поиск DNS.

         Назначьте **Ciscoenpa55** в качестве зашифрованного пароля доступа к привилегированному режиму EXEC.

         Назначьте **Ciscoconpa55** в качестве пароля консоли и включите вход по паролю.

         Установите минимальную длину 10 символов для всех паролей.

         Зашифруйте все открытые пароли.

         Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству. Обязательно включите в текст баннера слово **Warning (Предупреждение)**.

         Настройте все интерфейсы Gigabit Ethernet.

         Настройте IPv4-адреса в соответствии с вашей схемой адресации.

         Настройте IPv6-адреса в соответствии с таблицей адресации.

         Настройте SSH на R1:

         Укажите имя домена **CCNA-lab.com**

         Сгенерируйте **1024**-разрядный ключ RSA.

         Настройте линии VTY для доступа по протоколу SSH.

         Используйте локальные профили пользователей для аутентификации.

         Создайте пользователя **Admin1** с **15-м** уровнем привилегированного доступа и зашифрованным паролем **Admin1pa55**.

         Настройте закрытие линии связи через пять минут неактивности для консоли и линий VTY.

         Заблокируйте на три минуты всех, кто, выполнив четыре попытки в течение двух минут, не смог войти в систему.

**Настройка коммутаторов**

         Настройте имя устройства в соответствии с таблицей адресации.

         Присвойте виртуальному интерфейсу коммутатора (SVI) IPv4-адрес и маску подсети в соответствии с вашей схемой адресации.

         Настройте шлюз по умолчанию.

         Отключите поиск DNS.

         Назначьте **Ciscoenpa55** в качестве зашифрованного пароля доступа к привилегированному режиму EXEC.

         Назначьте **Ciscoconpa55** в качестве пароля консоли и включите вход по паролю.

         Настройте закрытие линии связи через пять минут неактивности для консоли и линий VTY.

         Зашифруйте все открытые пароли.

**Проверка подключения**

         Откройте веб-браузер на компьютерах Staff, Sales и IT и перейдите на сайт **www.cisco.pka**.

         Откройте веб-браузер на компьютерах Staff, Sales и IT и перейдите на сайт **www.cisco6.pka**.

         Команда ping должна успешно отправляться со всех компьютеров на все устройства.

# Решение 11.4.1.2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Устройство** | **Интерфейс** | **IPv4-адрес** | **Маска подсети** | **Шлюз по умолчанию** |
| **IPv6-адрес/префикс** | **Локальный адрес канала IPv6** |
| R1 | G0/0 | **192.168.0.1** | **255.255.255.128** | — |
| 2001:DB8:2::1/64 | FE80::1 | — |
| G0/1 | **192.168.0.129** | **255.255.255.192** | — |
| 2001:DB8:ACAD:1::1/64 | FE80::1 | — |
| G0/2 | **192.168.0.193** | **255.255.255.224** | — |
| 2001:DB8:ACAD:2::1/64 | FE80::1 | — |
| S0/0/1 | 172.16.1.2 | 255.255.255.252 | — |
| 2001:DB8:2::1/64 | FE80::1 | — |
| Central | S0/0/0 | 209.165.200.226 | 255.255.255.252 | — |
| 2001:DB8:1::1/64 | FE80::2 | — |
| S0/0/1 | 172.16.1.1 | 255.255.255.252 | — |
| 2001:DB8:2::2/64 | FE80::2 | — |
| S1 | VLAN 1 | **192.168.0.2** | **255.255.255.128** | **192.168.0.1** |
| S2 | VLAN 1 | **192.168.0.130** | **255.255.255.192** | **192.168.0.129** |
| S3 | VLAN 1 | **192.168.0.194** | **255.255.255.224** | **192.168.0.193** |
| Staff | NIC | **192.168.0.3** | **255.255.255.128** | **192.168.0.1** |
| 2001:DB8:ACAD::2/64 | FE80::2 | FE80::1 |
| Sales | NIC | **192.168.0.131** | **255.255.255.192** | **192.168.0.129** |
| 2001:DB8:ACAD:1::2/64 | FE80::2 | FE80::1 |
| IT | NIC | **192.168.0.195** | **255.255.255.224** | **192.168.0.193** |
| 2001:DB8:ACAD:2::2/64 | FE80::2 | FE80::1 |
| Web | NIC | 64.100.0.3 | 255.255.255.248 | 64.100.0.1 |
| 2001:DB8:CAFE::3/64 | FE80::2 | FE80::1 |

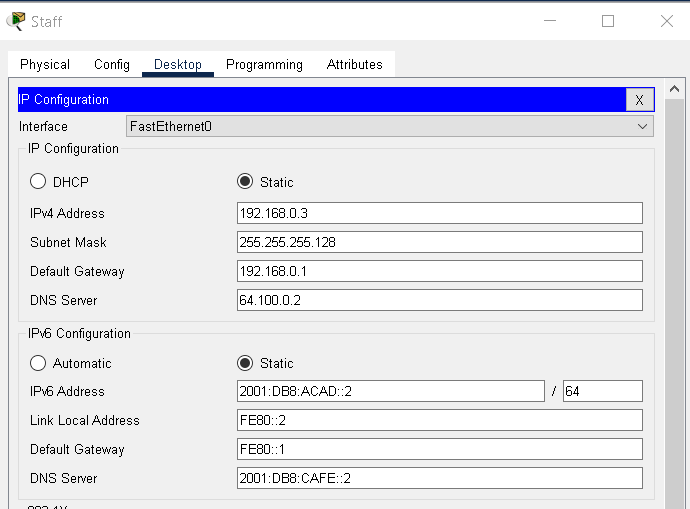
**IPv4 адресация**

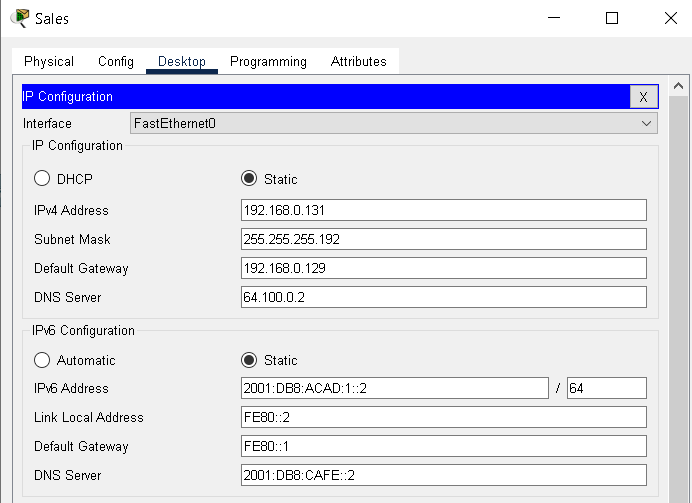
Рассчитаем на сайте[**http://vlsmcalc.com**](http://vlsmcalc.com)

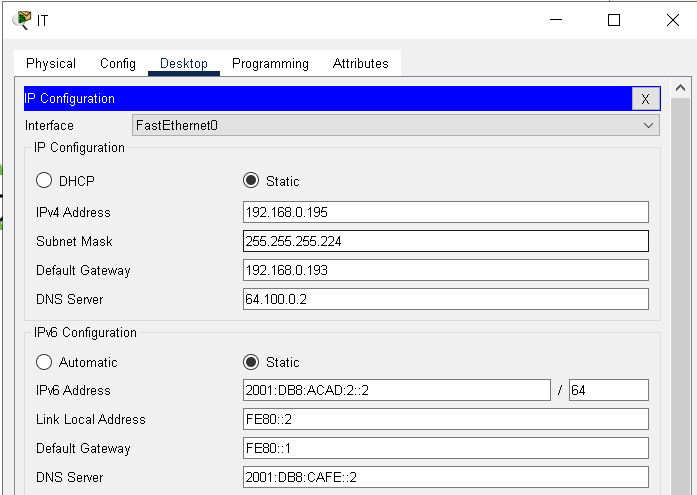
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Staff | NIC | **192.168.0.3** | **255.255.255.128** | **192.168.0.1** |
| 2001:DB8:ACAD::2/64 | FE80::2 | FE80::1 |
| Sales | NIC | **192.168.0.131** | **255.255.255.192** | **192.168.0.129** |
| 2001:DB8:ACAD:1::2/64 | FE80::2 | FE80::1 |
| IT | NIC | **192.168.0.195** | **255.255.255.224** | **192.168.0.193** |
| 2001:DB8:ACAD:2::2/64 | FE80::2 | FE80::1 |

Для Guest подсеть 192.168.0.224/27

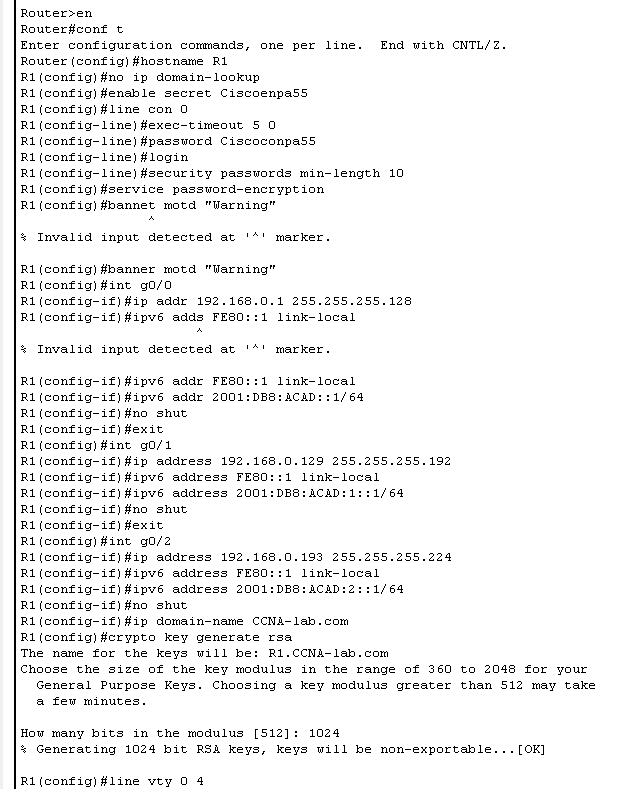
**Настройка компьютера**

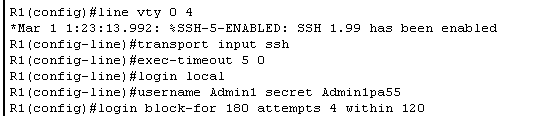
****

****

****

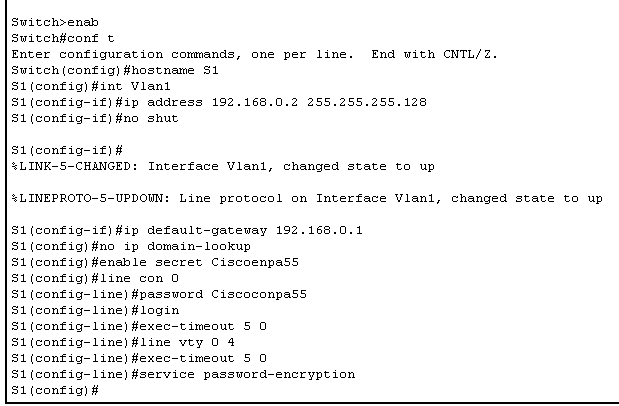
**Настройка R1**

****

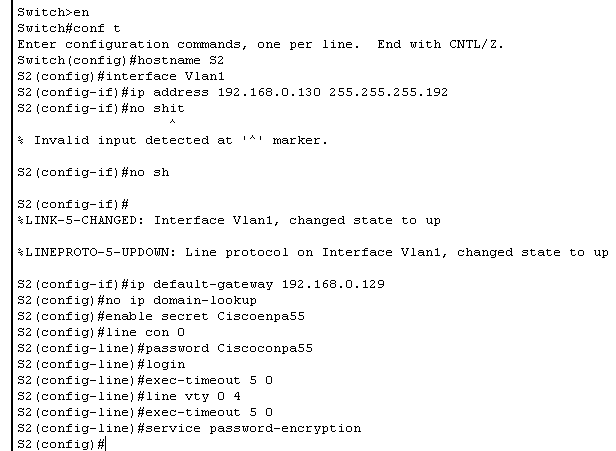
****

**Настройка коммутаторов**

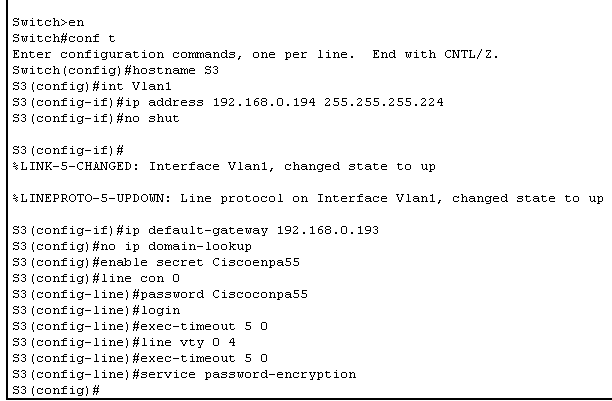
**S1**

****

**S2**

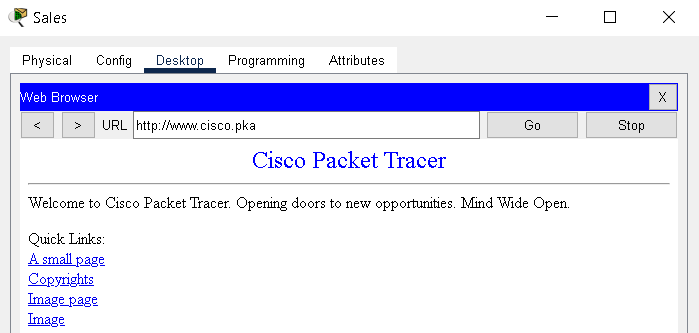
****

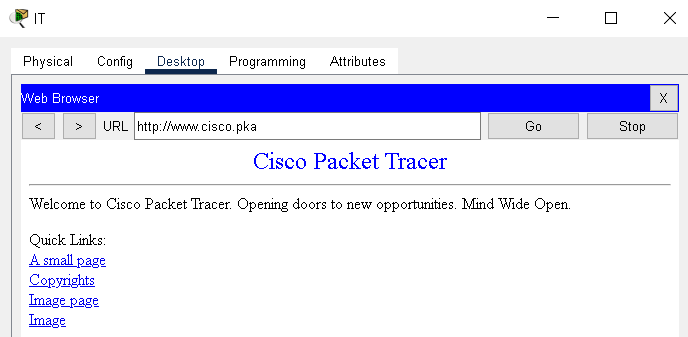
**S3**

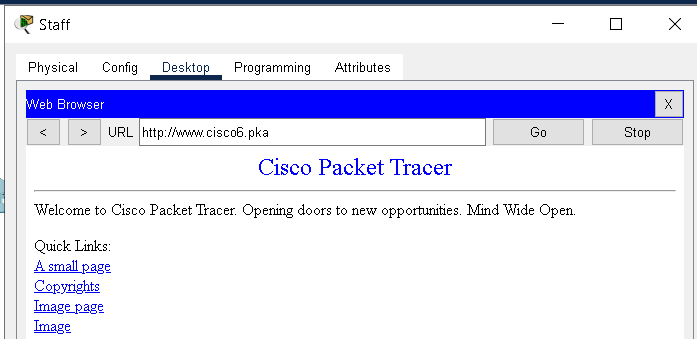
****

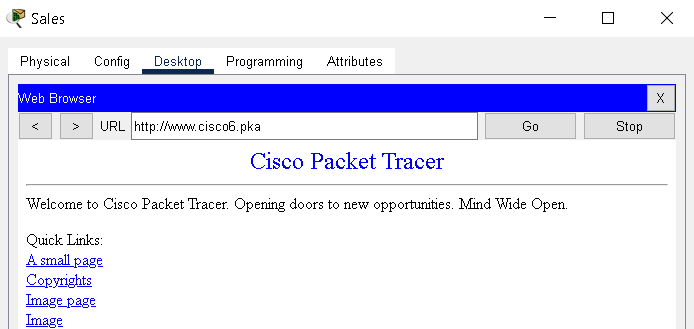
**Проверка подключения**

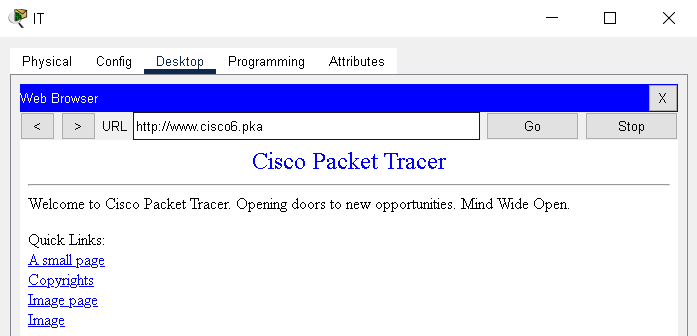
****

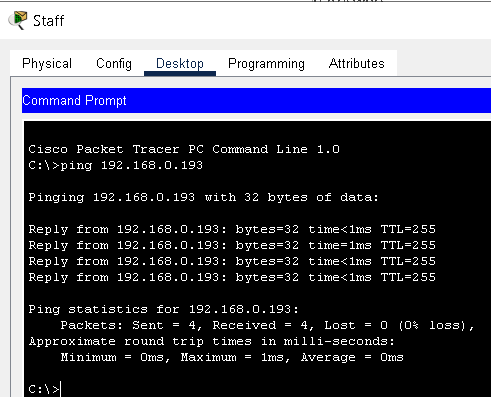
****

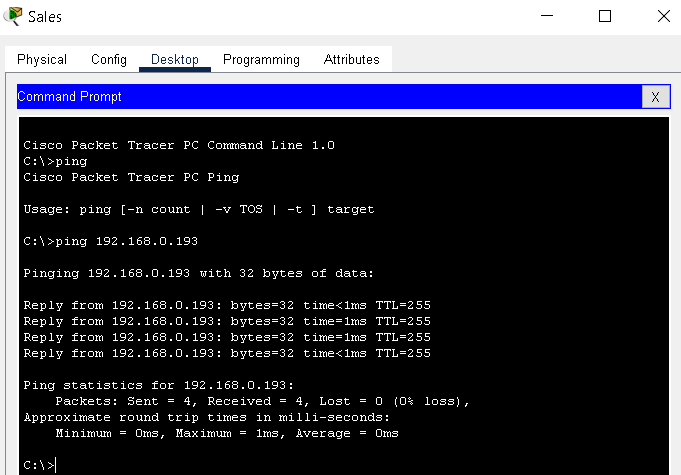
****

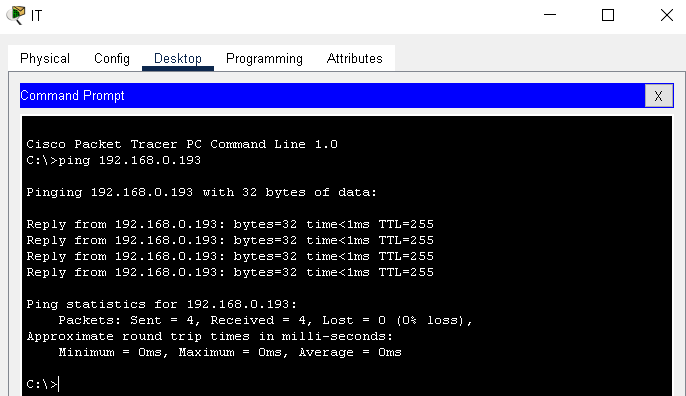
****

****

****

****

****

****

# 11.4.3.6

**Таблица адресации**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Устройство** | **Интерфейс** | **IP-адрес** | **Маска подсети** | **Шлюз по умолчанию** |
| R1 | G0/0 | 172.16.1.1 | 255.255.255.0 | — |
| G0/1 | 172.16.2.1 | 255.255.255.0 | — |
| S0/0/0 | 209.165.200.226 | 255.255.255.252 | — |
| R2 | G0/0 | 209.165.201.1 | 255.255.255.224 | — |
| S0/0/0 (DCE) | 209.165.200.225 | 255.255.255.252 | — |
| ПК-01 | Сетевой адаптер | 172.16.1.3 | 255.255.255.0 | 172.16.1.1 |
| ПК-02 | Сетевой адаптер | 172.16.1.4 | 255.255.255.0 | 172.16.1.1 |
| PC-A | NIC | 172.16.2.3 | 255.255.255.0 | 172.16.2.1 |
| PC-B | NIC | 172.16.2.4 | 255.255.255.0 | 172.16.2.1 |
| Web | NIC | 209.165.201.2 | 255.255.255.224 | 209.165.201.1 |
| DNS1 | Сетевой адаптер | 209.165.201.3 | 255.255.255.224 | 209.165.201.1 |
| DNS2 | Сетевой адаптер | 209.165.201.4 | 255.255.255.224 | 209.165.201.1 |

**Задачи**

Цель данного упражнения в программе Packet Tracer — найти неисправности подключения и по возможности устранить их. Если проблемы с подключением устранить не удается, подробно задокументируйте их для дальнейшей эскалации.

**Общие сведения/сценарий**

Пользователи сообщают, что после недавней модернизации, в рамках которой был добавлен второй сервер DNS, не удается подключиться к веб-серверу www.cisco.pka. Вы должны определить причину и попытаться устранить неполадки. Подробно задокументируйте неполадки и способы решения проблемы. У вас нет доступа к устройствам в облаке и к серверу www.cisco.pka. При необходимости эскалируйте проблему.

Доступ к маршрутизатору R1 возможен только по протоколу SSH с использованием имени пользователя **Admin01** и пароля **cisco12345**.

**Шаг 1. Определите неполадки подключения узла PC-01 к веб-серверу.**

А.     На узле PC-01 откройте приглашение ко вводу команды. Введите команду **ipconfig**, чтобы узнать, какие IP-адрес и шлюз по умолчанию назначены узлу PC-01. При необходимости исправьте заданные значения.

Б.    Устранив проблемы с IP-адресами на узле PC-01, отправьте ping-запрос на шлюз по умолчанию, на веб-сервер и на другие компьютеры. Успешно ли выполнена проверка связи? Запись результатов.

Ping-запрос на шлюз по умолчанию (172.16.1.1). Ping-запрос на веб-сервер (209.165.201.2).

Ping-запрос на PC-02. Ping-запрос на PC-A. Ping-запрос на PC-B.

В.     На узле PC-01 попробуйте подключиться к веб-серверу через браузер. Введите URL-адрес www.cisco.pka, а затем укажите IP-адрес 209.165.201.2. Запись результатов.

Доступен ли сервер www.cisco.pka с узла PC-01? Доступен ли он при вводе IP-адреса веб-сервера?

Г.    Задокументируйте неполадки и способы решения проблемы. По возможности устраните неполадки.

**Шаг 2. Определите неполадки подключения узла PC-02 к веб-серверу.**

А.     На узле PC-02 откройте приглашение ко вводу команды. Введите команду **ipconfig**, чтобы узнать, какие IP-адрес и шлюз по умолчанию назначены узлу. При необходимости исправьте заданные значения.

Б.    Устранив проблемы с IP-адресами на узле PC-02, отправьте ping-запрос на шлюз по умолчанию, на веб-сервер и на другие компьютеры. Успешно ли выполнена проверка связи? Запись результатов.

Ping-запрос на шлюз по умолчанию (172.16.1.1). Ping-запрос на веб-сервер (209.165.201.2).

Ping-запрос на PC-01. Ping-запрос на PC-A. Ping-запрос на PC-B.

В.     Используя браузер на узле PC-02, попробуйте подключиться к веб-серверу www.cisco.pka. Запись результатов.

Доступен ли сервер www.cisco.pka с узла PC-01? Доступен ли он при вводе IP-адреса веб-сервера?

Г.    Задокументируйте неполадки и способы решения проблемы. По возможности устраните неполадки.

**Шаг 3. Определите неполадки подключения узла PC-A к веб-серверу.**

А.     На узле PC-A откройте приглашение ко вводу команды. Введите команду **ipconfig**, чтобы узнать, какие IP-адрес и шлюз по умолчанию назначены узлу. При необходимости исправьте заданные значения.

Б.    Устранив проблемы с IP-адресами на узле PC-A, отправьте ping-запрос на шлюз по умолчанию, на веб-сервер и на другие компьютеры. Успешно ли выполнена проверка связи? Запись результатов.

Ping-запрос на шлюз по умолчанию (172.16.2.1). Ping-запрос на веб-сервер (209.165.201.2).

Ping-запрос на PC-B. Ping-запрос на PC-01. Ping-запрос на PC-02.

В.     Используя браузер на узле PC-A, попробуйте подключиться к веб-серверу www.cisco.pka. Запишите результаты.

Доступен ли сервер www.cisco.pka с узла PC-A? Доступен ли он при вводе IP-адреса веб-сервера?

Г.    Задокументируйте неполадки и способы решения проблемы. По возможности устраните неполадки.

**Шаг 4. Определите неполадки подключения узла PC-B к веб-серверу.**

А.     На узле PC-B откройте приглашение ко вводу команды. Введите команду **ipconfig**, чтобы узнать, какие IP-адрес и шлюз по умолчанию назначены узлу. При необходимости исправьте заданные значения.

Б.    Устранив проблемы с IP-адресами на узле PC-B, отправьте ping-запрос на шлюз по умолчанию, на веб-сервер и на другие компьютеры. Успешно ли выполнена проверка связи? Запись результатов.

Ping-запрос на шлюз по умолчанию (172.16.2.1). Ping-запрос на веб-сервер (209.165.201.2).

Ping-запрос на PC-A. Ping-запрос на PC-01. Ping-запрос на PC-02.

В.     Попробуйте подключиться к веб-серверу www.cisco.pka через браузер. Запись результатов.

Доступен ли сервер www.cisco.pka с узла PC-B? Доступен ли он при вводе IP-адреса веб-сервера?

Г.    Задокументируйте неполадки и способы решения проблемы. По возможности устраните неполадки.

**Шаг 5. Проверьте подключение.**

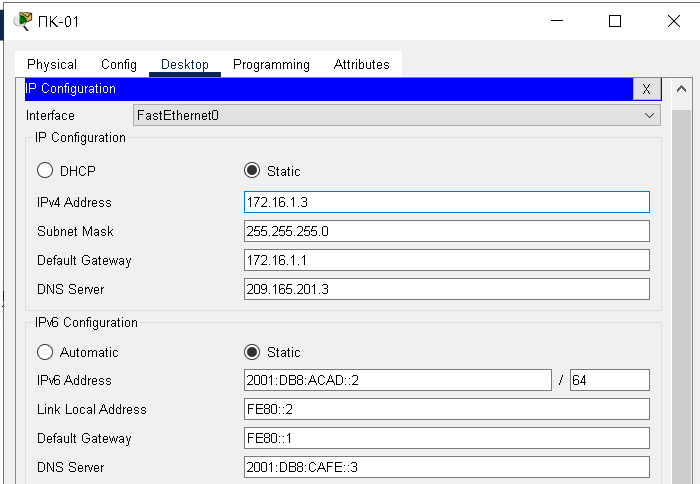
Убедитесь, что веб-сервер www.cisco.pka доступен на всех компьютерах.

Упражнение должно быть выполнено на 100 %. Если это не так, щелкните **Проверить результаты**, чтобы посмотреть, какие требуемые компоненты еще не завершены.

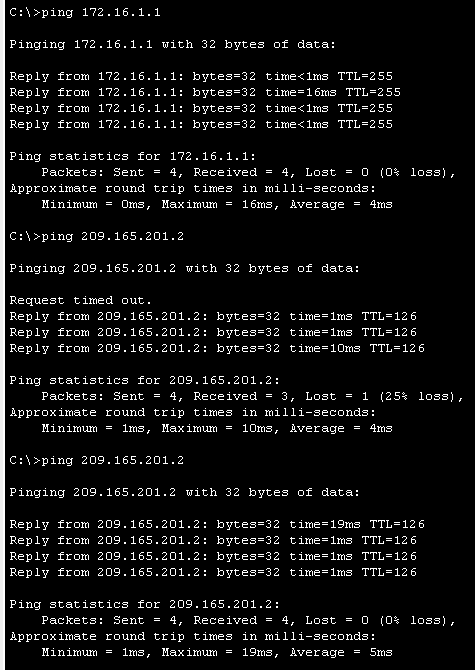
# Решение 11.4.3.6

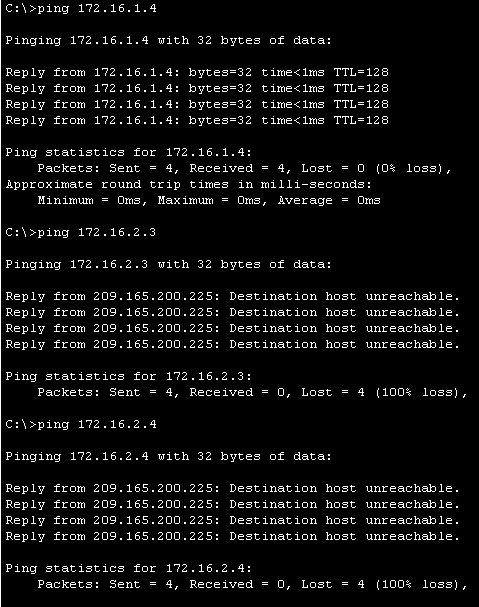
Шаг 1.А)

Неправильный IPv4,поменяли его на правильный



Шаг 1.Б)





Шаг 1.В)



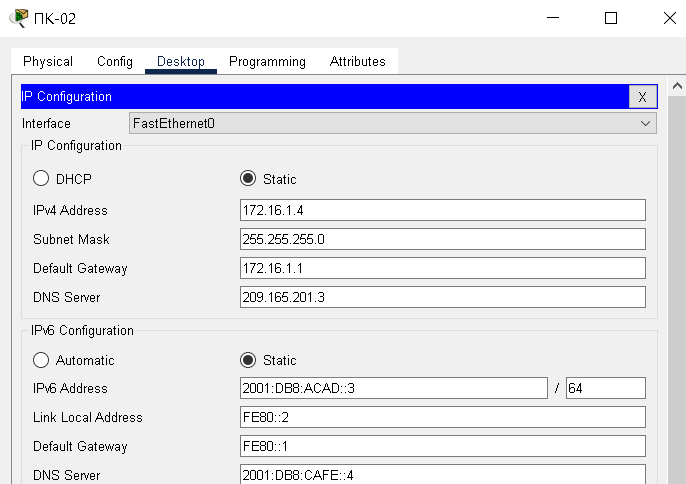


Шаг 1.Г)

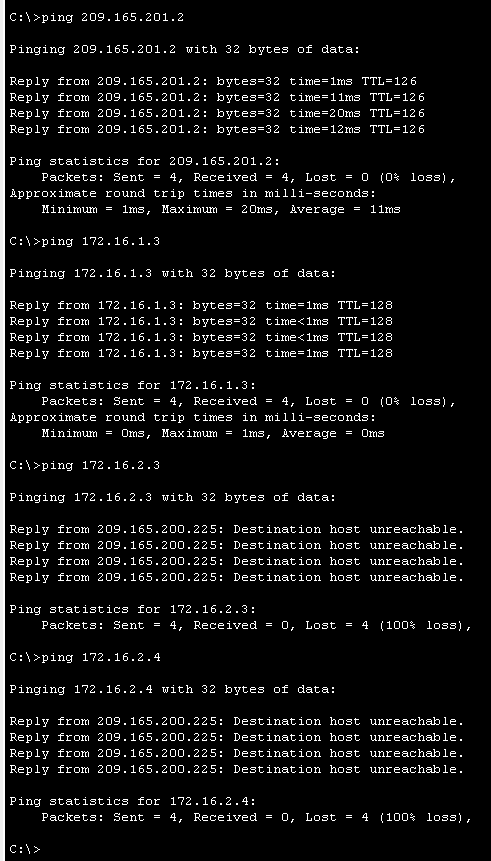
Неправильно настроен IP-адрес на ПК-01. Чтобы устранить проблему, IP-адрес изменен с 172.168.1.3 на 172.16.1.3 см. Шаг 1.А. PC-01 не может успешно выполнить пинг компьютеров в сети 172.16.2.0/24.

Шаг 2.А)

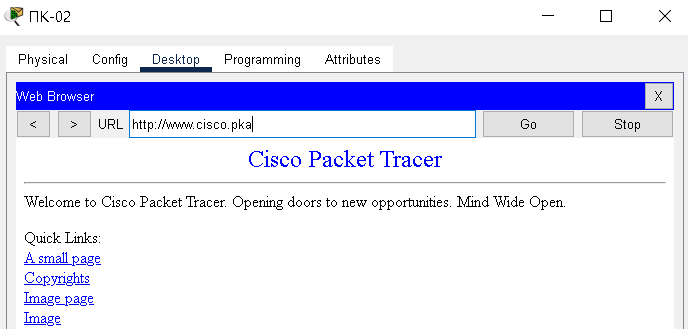
Шлюз по умолчанию неверен, измените адрес шлюза по умолчанию на 172.16.1.1:

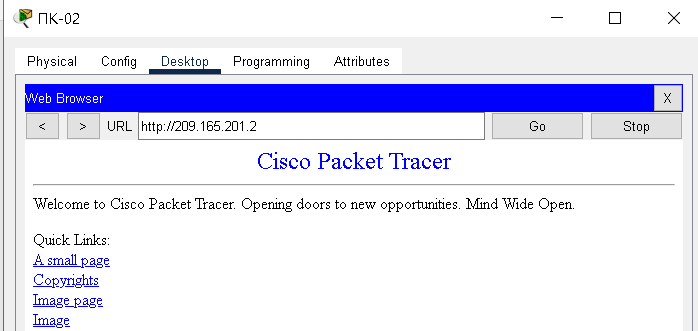


Шаг 2.Б)



Шаг 2.В)

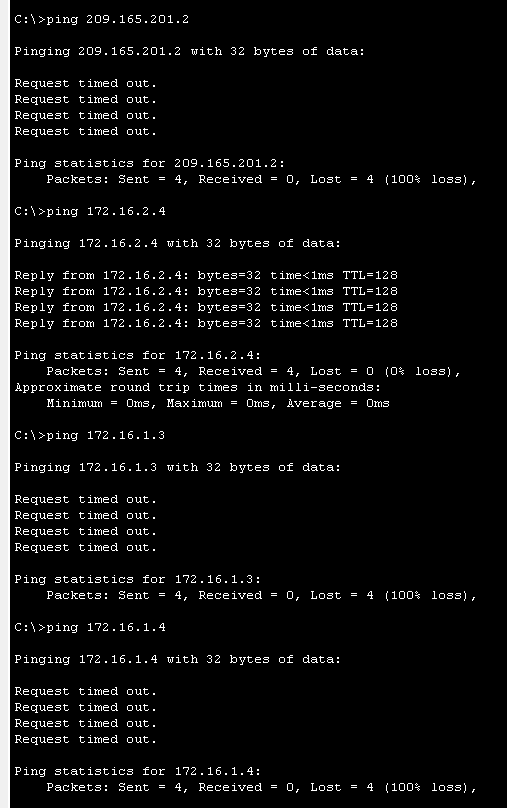




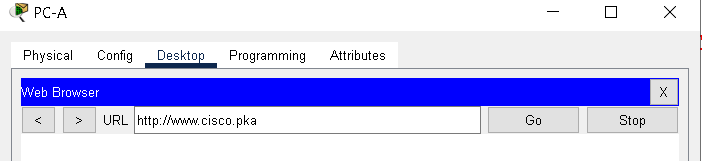
Шаг 2.Г)

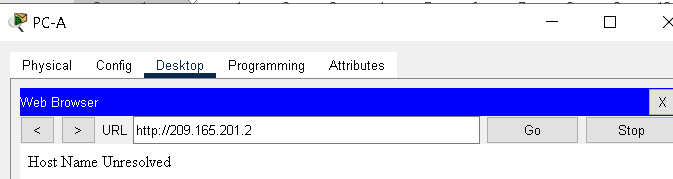
PC-02 может получить доступ к веб-серверу, используя IP-адрес после исправления шлюза по умолчанию. Шлюз по умолчанию должен быть настроен как 172.16.1.1 на ПК-02. PC-02 не удается успешно выполнить пинг компьютеров в сети 172.16.2.0/24.

Шаг 3.Б)



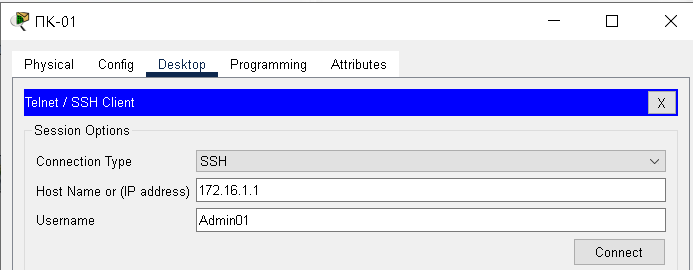
Шаг 3.В)

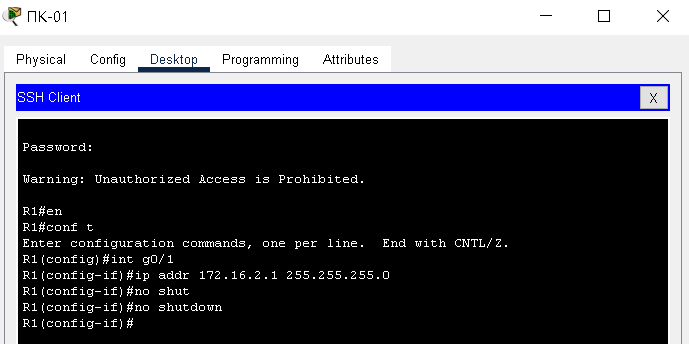




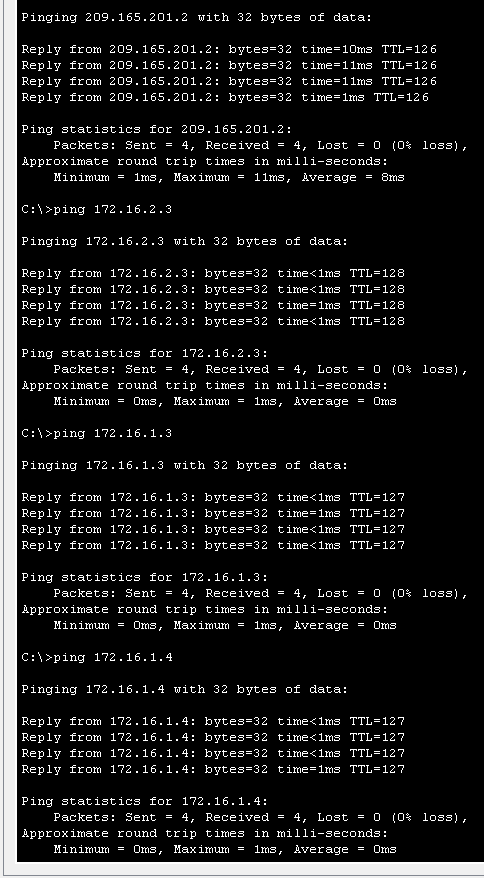
Шаг 3.Г)

ПК-А может получить доступ только к локальной сети. Интерфейс G0/1 на маршрутизаторе R1 неправильно настроен.Нужно IP-адрес на интерфейсе G0/1. Получить доступ к маршрутизатору R1 с помощью SSH с ПК-01 или ПК-02, чтобы изменить IP-адрес с 172.16.3.1 на 172.16.2.1.

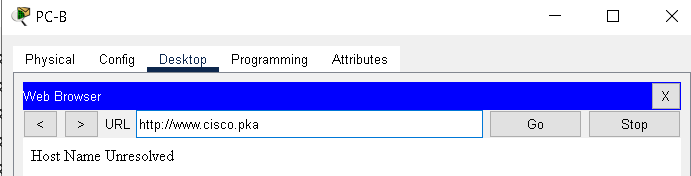


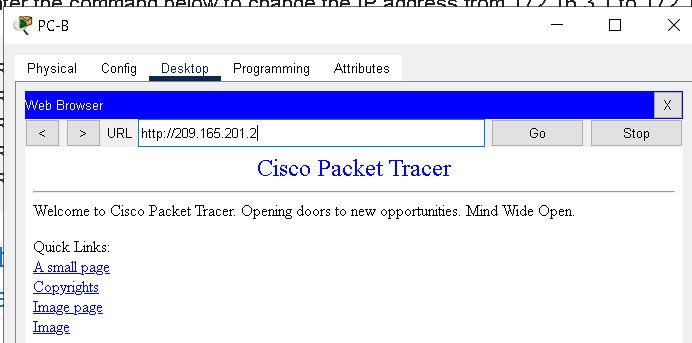


Шаг 4.Б)



Шаг 4.В)





Шаг 4.Г)

PC-B может получить доступ к веб-серверу, используя только IP-адрес. PC-B также настроен с правильным адресом сервера DNS-2. Это указывает на то, что сервер DNS-2, возможно, неправильно настроен. Чтобы временно устранить эту проблему, адрес DNS-сервера можно настроить на использование 209.165.200.3. Проблема с сервером DNS-2 должна быть устранена, поскольку у нас нету прав, мы этого сделать не можем.

# Appendix Router

**Задачи**

**Часть 1. Подключение к интегрированному маршрутизатору**

**Часть 2. Активация беспроводного подключения**

**Часть 3. Настройка и проверка доступа к беспроводным клиентам**

**Общие сведения**

В этом упражнении необходимо настроить интегрированный маршрутизатор, обеспечивающий удаленный доступ к беспроводным клиентам и подключение с защитой WPA.

**Часть 1.    Подключение к интегрированному маршрутизатору**

**Шаг 1.    Настройте и проверьте подключение к интегрированному маршрутизатору.**

А.    Подключите узел Host-A к порту Ethernet 1 интегрированного маршрутизатора (IR) с помощью соответствующего кабеля.

Б.   Дождитесь, когда индикатор связи загорится зеленым светом. На узле Host-A запустите командную строку и выполните команду **ipconfig**, чтобы проверить информацию об IP-адресе узла.

В.    С помощью команды ping **ping 192.168.0.1** проверьте, имеет ли узел **Host-A** доступ к шлюзу по умолчанию.

**Шаг 2.    Запустите веб-браузер и перейдите к графическому интерфейсу пользователя IR.**

А.    На узле Host-A запустите веб-браузер и перейдите к графическому интерфейсу пользователя для настройки интегрированного маршрутизатора. В поле URL-адреса укажите адрес шлюза по умолчанию для узла Host-A.

Б.   Введите **admin** в полях имени пользователя и пароля.

**Часть 2.    Активация беспроводного подключения**

**Шаг 1.    Настройте параметры подключения интегрированного маршрутизатора к Интернету.**

В этом сценарии нет подключения к Интернету, но несмотря на это, вам потребуется настроить параметры интерфейса для выхода в Интернет. В раскрывающемся списке **Internet Connection Type** (Тип подключения к Интернету) выберите **Static IP** (Статический IP-адрес). Затем введите следующие данные IP-адреса:

        IP-адрес в Интернете — **198.133.219.1**

        Маска подсети — **255.255.255.0**

        Шлюз по умолчанию — **198.133.219.254**

        DNS 1 — **198.133.219.10**

**Шаг 2.    Настройте параметры внутренней сети.**

Прокрутите страницу вниз до раздела **Network Setup** (Настройка сети) и задайте следующие параметры:

        IP-адрес — **172.31.1.1**

        Маска подсети — **255.255.255.224**

        Начальный IP-адрес — для последнего октета введите значение **5**.

        Максимальное количество пользователей — **25**

**Примечание.** Чтобы изменения в диапазоне IP-адресов пула DHCP вступили в силу, нажмите кнопку **Save Settings** (Сохранить параметры).

**Шаг 3.    Сохраните настройки и повторно подключитесь к интегрированному маршрутизатору.**

А.    Прокрутите страницу вниз до конца и нажмите кнопку **Save Settings** (Сохранить параметры).При переходе между вкладками без сохранения измененные параметры будут потеряны.

Б.   После нажатия кнопки **Save Settings** (Сохранить параметры) соединение будет разорвано, поскольку вы изменили IP-адрес маршрутизатора.

В.    Вернитесь в окно командной строки узла Host-A и выполните команду **ipconfig /renew**, чтобы обновить IP-адрес.

Г.   В веб-браузере узла Host-A повторно подключитесь к интегрированному маршрутизатору. Необходимо использовать новый адрес шлюза по умолчанию. Проверьте параметры **Internet Connection** (Подключение к Интернету) на вкладке **Status** (Состояние). Значения параметров должны совпадать с теми, которые были заданы на шаге 1 части 2. Если значения не совпадают, повторите шаги 1 и 2 части 2.

**Шаг 4.    Настройте беспроводное подключение для беспроводных устройств.**

А.    Откройте вкладку **Wireless** (Беспроводные сети) и изучите параметры в раскрывающемся списке **Network Mode** (Режим сети).

Когда следует выбрать параметр **Disable** (Откл.)?

Когда следует выбрать параметр **Mixed** (Смешанная)?

Б.   Выберите режим сети **Wireless-N Only** (Только беспроводная).

В.    Измените SSID на **MyHomeNetwork**.

Г.   Когда беспроводной клиент выполняет поиск беспроводных сетей поблизости, он обнаруживает все широковещательные рассылки SSID. Широковещательные рассылки SSID включены по умолчанию.

Если SSID точки доступа не рассылается в широковещательном режиме, как устройства смогут к ней подключиться?

Д.    Чтобы обеспечить наилучшую производительность сети с использованием беспроводной сети Wireless-N, установите диапазон частот **Wide-40MHz** (Широкий — 40 МГц).

Е.    Нажмите кнопку **Save Settings** (Сохранить параметры), а затем — кнопку **Continue** (Продолжить).

**Шаг 5.    В настройках защиты беспроводной сети включите обязательную аутентификацию для клиентов.**

А.    На вкладке **Wireless** (Беспроводные сети) щелкните параметр **Wireless Security** (Защита беспроводной сети).

Б.   Выберите для параметра **Security Mode** (Режим безопасности) значение **WPA2 Personal** (WPA2-личная).

В чем разница между режимами личной и корпоративной сети?

В.    Не изменяйте режим шифрования AES и введите парольную фразу **itsasecret**.

Г.    Нажмите кнопку **Save Settings** (Сохранить параметры), а затем — кнопку **Continue** (Продолжить).

**Шаг 6.    Измените пароль по умолчанию для доступа к настройкам интегрированного маршрутизатора.**

А.    Всегда изменяйте пароль по умолчанию. Откройте вкладку **Administration** (Администрирование) и измените пароль **Router Access** (Доступ к маршрутизатору) на **letmein**.

Б.    Нажмите кнопку **Save Settings** (Сохранить параметры). Введите имя пользователя **admin** и новый пароль.

**Часть 3.    Настройка и проверка доступа к беспроводным клиентам**

**Шаг 1.    Подключите ноутбук к беспроводной сети.**

А.    Щелкните **Laptop** (Ноутбук) и выберите **Desktop** > **PC Wireless** (Настольные системы > Беспроводное подключение ПК). Открывшееся окно — это графический интерфейс пользователя маршрутизатора для клиента.

Б.   Перейдите на вкладку **Connect** (Подключить) и при необходимости нажмите кнопку **Refresh** (Обновить). В списке доступных сетей в поле Wireless Network Name (Имя беспроводной сети) должна быть указана сеть **MyHomeNetwork**.

В.    Щелкните сеть **MyHomeNetwork** и нажмите кнопку **Connect** (Подключить).

Г.   Теперь вы должны увидеть сеть **MyHomeNetwork**. Щелкните эту сеть и нажмите кнопку **Connect** (Подключить).

Д.    В поле **Pre-shared Key** (Общий ключ) необходимо указать пароль, который вы задали на шаге 5 В в части 2. Введите пароль и нажмите кнопку **Connect** (Подключить).

Е.    Закройте интерфейс пользователя интегрированного маршрутизатора и щелкните элемент **Command Prompt** (Командная строка). Выполните команду **ipconfig**, чтобы убедиться, что узел **Laptop** получил IP-адрес.

**Шаг 2.    Проверьте подключение между узлами Laptop и Host-A.**

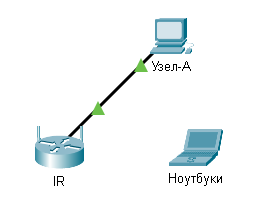
А.    Отправьте команду ping с узла Laptop для проверки связи с узлом IR.

Б.   Отправьте команду ping с узла Laptop для проверки связи с узлом Host-A.

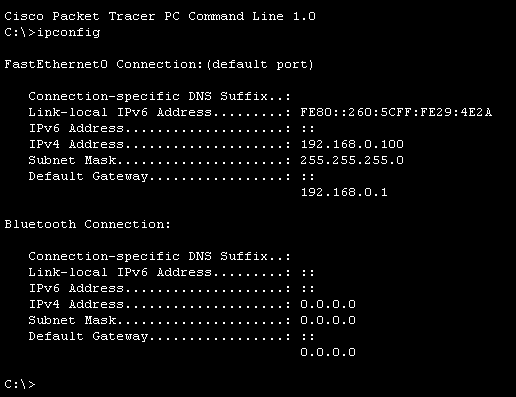
# Решение Appendix Router

**Часть 1**

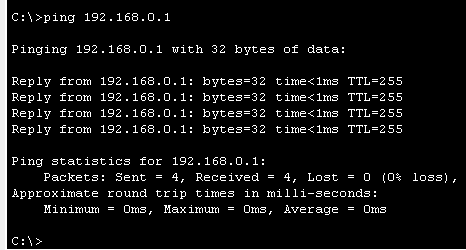
Шаг 1.А)



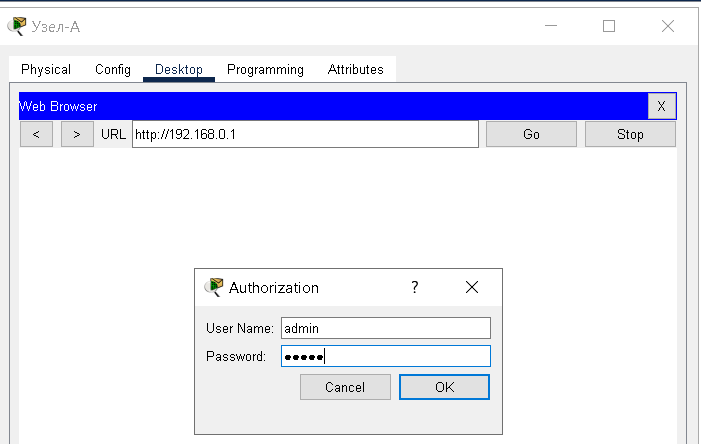
Шаг 1.Б)



Шаг 1.В)

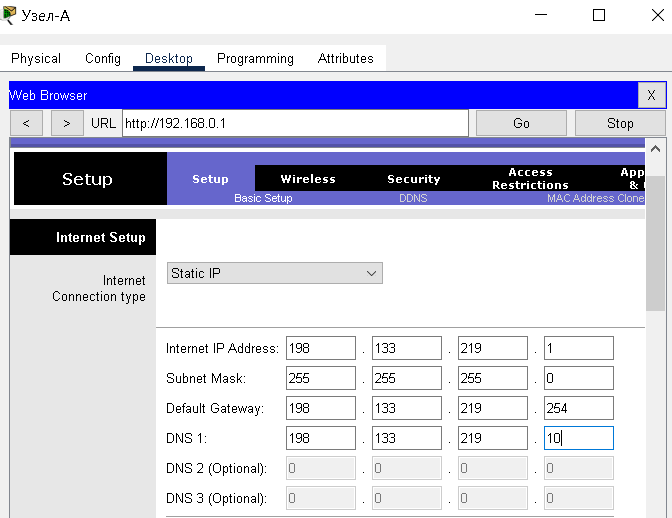


Шаг 2)

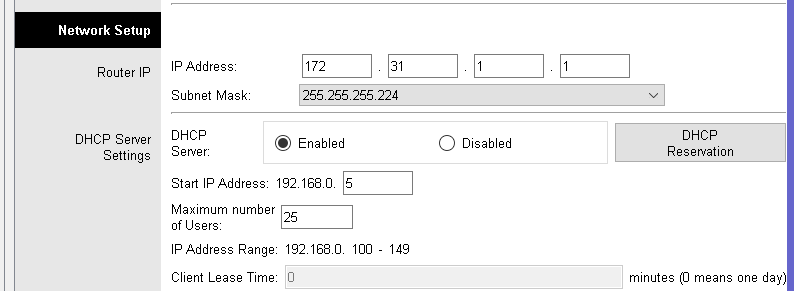


**Часть 2**

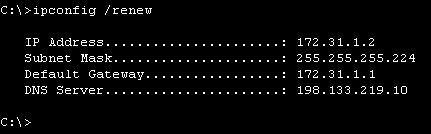
Шаг 1)



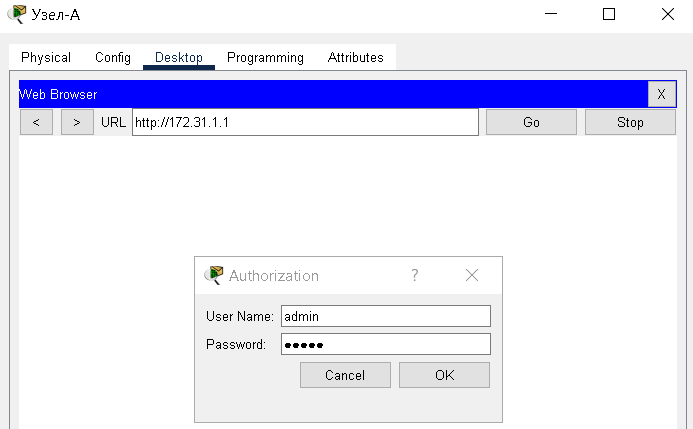
Шаг 2)



Шаг 3.В)



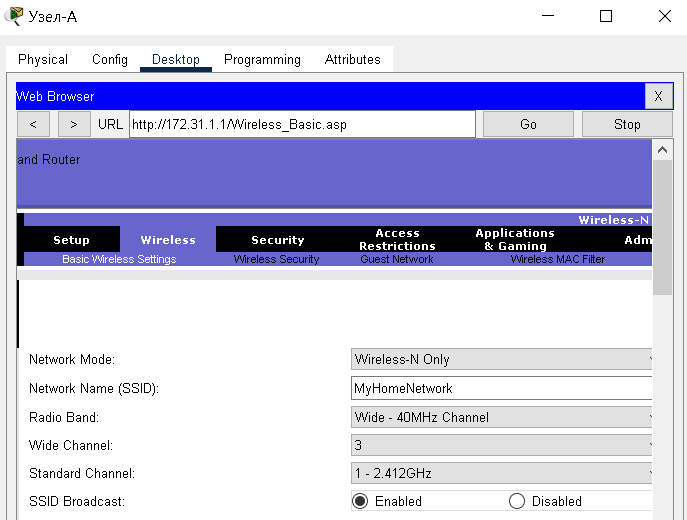
Шаг 3.Г)



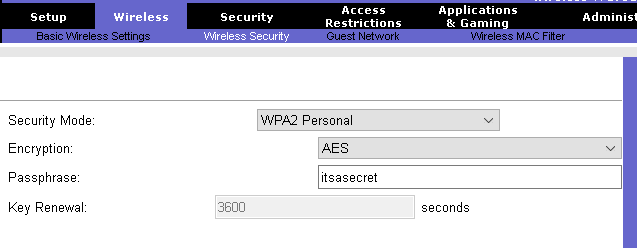
Шаг 4)

Когда у вас нет беспроводных устройств.

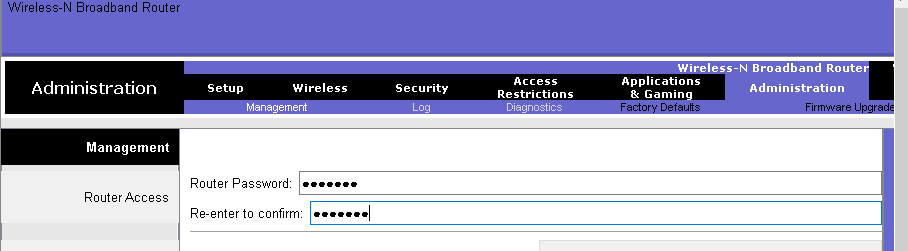
Если у вас есть беспроводные устройства, состоящие из B, G или N



Шаг 5)

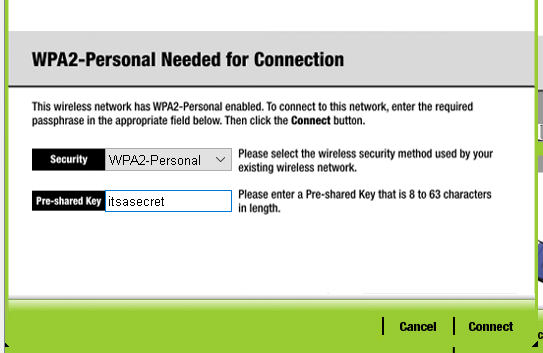


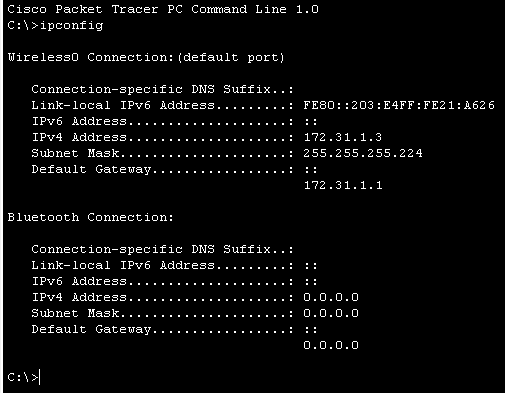
Шаг 6)



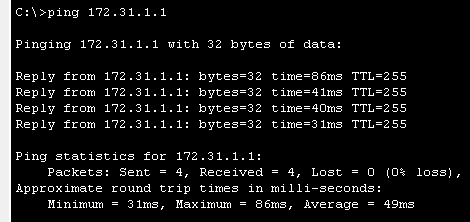
**Часть 3**

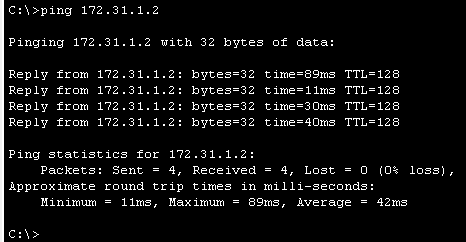
Шаг 1)





Шаг 2)





# Appendix Scenario

**Таблица адресации**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Устройство** | **интерфейс** | **IP-адрес** | **Subnet Mask (Маска подсети)** | **Основной шлюз** |
| R1 | G0/0 |  |  | — |
| S0/0/0 |  |  | — |
| R2 | G0/0 |  |  | — |
| S0/0/0 |  |  | — |
| S0/0/1 |  |  | — |
| R3 | G0/0 |  |  | — |
| S0/0/0 |  |  | — |
| S0/0/1 |  |  | — |
| R4 | G0/0 |  |  | — |
| S0/0/0 |  |  | — |
| S1 | VLAN 1 |  |  |  |
| S2 | VLAN 1 |  |  |  |
| S3 | VLAN 1 |  |  |  |
| S4 | VLAN 1 |  |  |  |
| PC1 | NIC |  |  |  |
| PC2 | NIC |  |  |  |
| PC3 | NIC |  |  |  |
| PC4 | NIC |  |  |  |

**Задачи**

**Часть 1. Разработка схемы IP-адресации**

**Часть 2. Назначение сетевым устройствам IP-адресов и проверка подключения**

**Сценарий**

В этом задании вам предоставляется сетевой адрес 172.31.1.0 /24 для подсети, и вы должны составить схему IP-адресации сети, изображенной в топологии. Требуемые адреса узла для каждого канала глобальной сети (WAN) и локальной сети (LAN) отмечены в топологии.

**Часть 1.    Разработка схемы IP-адресации**

**Шаг 1.    Разбейте сеть 172.31.1.0/24 на подсети, исходя из максимального количества узлов, необходимых для самой крупной подсети.**

А.    Сколько потребуется подсетей в соответствии с имеющейся топологией?

Б.   Сколько битов необходимо заимствовать для поддержки нескольких подсетей в таблице топологии?

В.    Сколько в результате этого создается подсетей?

Г.   Сколько при этом в каждой подсети будет доступно адресов узлов?

**Примечание**. Если ваш ответ — менее 14 узлов, необходимых для локальной сети (LAN) маршрутизатора R3, значит, вы зарезервировали слишком много бит.

Д.    Рассчитайте двоичное значение для первых пяти подсетей. Подсеть 0 уже показана.

Net 0: 172 . 31 . 1 . 0 0 0 0 0 0 0 0

Net 1: 172 . 31 . 1 . \_\_\_ \_\_\_ \_\_\_ \_\_\_ \_\_\_ \_\_\_ \_\_\_ \_\_\_

Net 2: 172 . 31 . 1 . \_\_\_ \_\_\_ \_\_\_ \_\_\_ \_\_\_ \_\_\_ \_\_\_ \_\_\_

Net 3: 172 . 31 . 1 . \_\_\_ \_\_\_ \_\_\_ \_\_\_ \_\_\_ \_\_\_ \_\_\_ \_\_\_

Net 4: 172 . 31 . 1 . \_\_\_ \_\_\_ \_\_\_ \_\_\_ \_\_\_ \_\_\_ \_\_\_ \_\_\_

Е.    Рассчитайте двоичное и десятичное значение новой маски подсети.

11111111.11111111.11111111. \_\_\_ \_\_\_ \_\_\_ \_\_\_ \_\_\_ \_\_\_ \_\_\_ \_\_\_

255 . 255 . 255 . \_\_\_\_\_\_

Ж.   Заполните **Таблицу подсетей**,перечислив все доступные подсети, первый и последний используемый адрес узла и широковещательный адрес. Первая подсеть уже введена за вас. Повторяйте эти действия до тех пор, пока все адреса не будут внесены в список.

**Примечание.** Возможно, потребуется заполнить не все строки.

**Таблица подсетей**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Номер подсети** | **IP-адрес подсети** | **Первый используемый IP-адрес узла** | **Последний используемый IP-адрес узла** | **Широковещательный адрес** |
| 0 | 172.31.1.0 | 172.31.1.1 | 172.31.1.14 | 172.31.1.15 |
| **1** |  |  |  |  |
| **2** |  |  |  |  |
| **3** |  |  |  |  |
| **4** |  |  |  |  |
| **5** |  |  |  |  |
| **6** |  |  |  |  |
| **7** |  |  |  |  |
| **8** |  |  |  |  |
| **9** |  |  |  |  |
| **10** |  |  |  |  |
| **11** |  |  |  |  |
| **12** |  |  |  |  |
| **13** |  |  |  |  |
| **14** |  |  |  |  |
| **15** |  |  |  |  |

**Шаг 2.    Назначьте подсети для сети, показанной в топологии.**

При назначении подсетей необходимо учитывать, что для отправки информации по сети потребуется маршрутизация.

А.    Назначьте подсеть 0 локальной сети (LAN) маршрутизатора R1.

Б.   Назначьте подсеть 1 локальной сети маршрутизатора R2.

В.   Назначьте подсеть 2 локальной сети маршрутизатора R3.

Г.   Назначьте подсеть 3 локальной сети маршрутизатора R4.

Д.   Назначьте подсеть 4 промежуточному каналу.

Е.   Назначьте подсеть 5 промежуточному каналу.

Ж.   Назначьте подсеть 6 промежуточному каналу.

**Шаг 3.    Задокументируйте схему адресации.**

Заполните **Таблицу адресации** в соответствии со следующими рекомендациями.

А.    Назначьте первые используемые IP-адреса маршрутизаторам для каждого из каналов локальной сети.

Б.   При назначении IP-адресов каналам глобальной сети (WAN) используйте следующий метод:

        Для канала WAN между маршрутизаторами R1 и R2 назначьте первый используемый IP-адрес маршрутизатору R1, а последний используемый IP-адрес — маршрутизатору R2.

        Для канала WAN между маршрутизаторами R2 и R3 назначьте первый используемый IP-адрес маршрутизатору R2, а последний используемый IP-адрес — маршрутизатору R3.

        Для канала WAN между маршрутизаторами R3 и R4 назначьте первый используемый IP-адрес маршрутизатору R3, а последний используемый IP-адрес — маршрутизатору R4.

В.    Второй из используемых IP-адресов назначьте коммутаторам.

Г.      Последний из используемых IP-адресов назначьте узлам.

**Часть 2.    Назначение сетевым устройствам IP-адресов и проверка подключения**

Основная часть параметров IP-адресации для данной сети уже настроена. Для завершения настройки адресации выполните следующие шаги.

**Шаг 1.    Настройте IP-адресацию на интерфейсах локальной сети маршрутизаторов R1 и R2.**

**Шаг 2.    Настройте IP-адресацию на коммутаторе S3, включая шлюз по умолчанию.**

**Шаг 3.    Настройте IP-адресацию на компьютере PC4, включая шлюз по умолчанию.**

**Шаг 4.     Проверьте подключение.**

Подключение можно проверить только между маршрутизаторами R1, R2, коммутатором S3 и компьютером PC4. При этом необходимо иметь возможность успешно отправить эхо-запрос на каждый IP-адрес, перечисленный в **таблице адресации**.

# Решение Appendix Scenario

**Часть 1**

Шаг 1.А)

7 подсетей потребуется

Шаг 1.Б)

4 бита

Шаг 1.В)

16 подсетей

Шаг 1.Г)

14 узлов

Шаг 1.Д)

Net 0: 172 . 31 . 1 . 0 0 0 0 0 0 0 0

Net 1: 172 . 31 . 1 . 0 0 0 1 0 0 0 0

Net 2: 172 . 31 . 1 . 0 0 1 0 0 0 0 0

Net 3: 172 . 31 . 1 . 0 0 1 1 0 0 0 0

Net 4: 172 . 31 . 1 . 0 1 0 0 0 0 0 0

Шаг 1.Е)

11111111.11111111.11111111. 1 1 1 1 0 0 0 0

255 . 255 . 255 . 240

Шаг 1.Ж)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Номер подсети** | **IP-адрес подсети** | **Первый используемый IP-адрес узла** | **Последний используемый IP-адрес узла** | **Широковещательный адрес** |
| 0 | 172.31.1.0 | 172.31.1.1 | 172.31.1.14 | 172.31.1.15 |
| **1** | 172.31.1.16 | 172.31.1.17 | 172.31.1.30 | 172.31.1.31 |
| **2** | 172.31.1.32 | 172.31.1.33 | 172.31.1.46 | 172.31.1.47 |
| **3** | 172.31.1.48 | 172.31.1.49 | 172.31.1.62 | 172.31.1.63 |
| **4** | 172.31.1.64 | 172.31.1.65 | 172.31.1.78 | 172.31.1.79 |
| **5** | 172.31.1.80 | 172.31.1.81 | 172.31.1.94 | 172.31.1.95 |
| **6** | 172.31.1.96 | 172.31.1.97 | 172.31.1.110 | 172.31.1.111 |
| **7** | 172.31.1.112 | 172.31.1.113 | 172.31.1.126 | 172.31.1.127 |
| **8** | 172.31.1.128 | 172.31.1.129 | 172.31.1.142 | 172.31.1.143 |
| **9** | 172.31.1.144 | 172.31.1.145 | 172.31.1.158 | 172.31.1.159 |
| **10** | 172.31.1.160 | 172.31.1.161 | 172.31.1.174 | 172.31.1.175 |
| **11** | 172.31.1.176 | 172.31.1.177 | 172.31.1.190 | 172.31.1.191 |
| **12** | 172.31.1.192 | 172.31.1.193 | 172.31.1.206 | 172.31.1.207 |
| **13** | 172.31.1.208 | 172.31.1.209 | 172.31.1.222 | 172.31.1.223 |
| **14** | 172.31.1.224 | 172.31.1.225 | 172.31.1.238 | 172.31.1.239 |
| **15** | 172.31.1.240 | 172.31.1.241 | 172.31.1.254 | 172.31.1.255 |

Шаг 2)

Подсеть 0 R1=172.31.1.0 /28

Подсеть 1 R2=172.31.1.16 /28

Подсеть 2 R3=172.31.1.32 /28

Подсеть 3 R4=172.31.1.48 /28

Подсеть 4 промежуточный=172.31.1.64 /28

Подсеть 5 промежуточный=172.31.1.80 /28

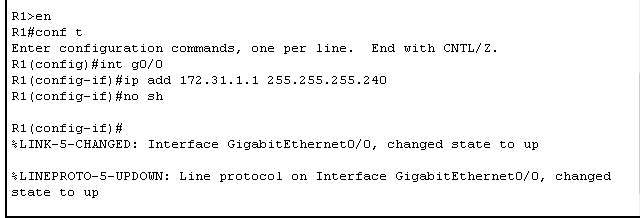
Подсеть 6 промежуточный=172.31.1.96 /28

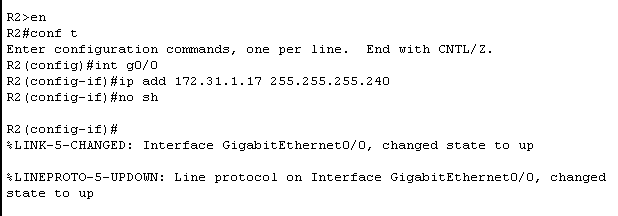
Шаг 3)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Устройство** | **интерфейс** | **IP-адрес** | **Subnet Mask (Маска подсети)** | **Основной шлюз** |
| R1 | G0/0 | 172.31.1.1 | 255.255.255.240 | — |
| S0/0/0 | 172.31.1.65 | 255.255.255.240 | — |
| R2 | G0/0 | 172.31.1.17 | 255.255.255.240 | — |
| S0/0/0 | 172.31.1.78 | 255.255.255.240 | — |
| S0/0/1 | 172.31.1.81 | 255.255.255.240 | — |
| R3 | G0/0 | 172.31.1.33 | 255.255.255.240 | — |
| S0/0/0 | 172.31.1.97 | 255.255.255.240 | — |
| S0/0/1 | 172.31.1.94 | 255.255.255.240 | — |
| R4 | G0/0 | 172.31.1.49 | 255.255.255.240 | — |
| S0/0/0 | 172.31.1.110 | 255.255.255.240 | — |
| S1 | VLAN 1 | 172.31.1.2 | 255.255.255.240 | 172.31.1.1 |
| S2 | VLAN 1 | 172.31.1.18 | 255.255.255.240 | 172.31.1.17 |
| S3 | VLAN 1 | 172.31.1.34 | 255.255.255.240 | 172.31.1.33 |
| S4 | VLAN 1 | 172.31.1.50 | 255.255.255.240 | 172.31.1.49 |
| PC1 | NIC | 172.31.1.14 | 255.255.255.240 | 172.31.1.1 |
| PC2 | NIC | 172.31.1.30 | 255.255.255.240 | 172.31.1.17 |
| PC3 | NIC | 172.31.1.46 | 255.255.255.240 | 172.31.1.33 |
| PC4 | NIC | 172.31.1.62 | 255.255.255.240 | 172.31.1.49 |

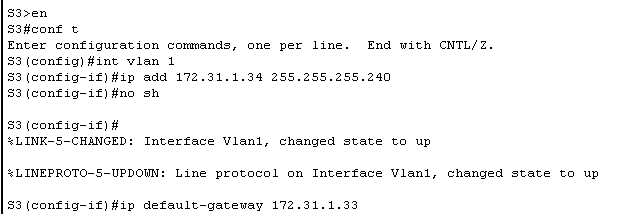
**Часть 2**

Шаг 1)

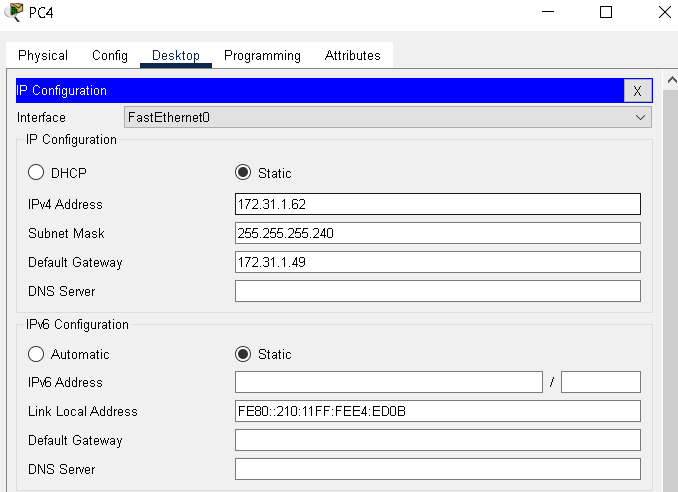




Шаг 2)



Шаг 3)



Шаг 4)

