Практическая работа по дисциплине  
“Сети и телекоммуникации”

№14

Выполнил:

Студент группы 606-12  
Демьянцев В.В.

# Задание “17.8.2”

| **Устройство** | **Интерфейс** | **IP адрес/префикс** | **Шлюз по умолчанию** |
| --- | --- | --- | --- |
| R1 | G0/0 | *192.168.0.1/25* | — |
|  |  | 2001:db8:acad።1/64 | *—* |
|  |  | fe80::1 | *—* |
|  | G0/1 | *192.168.0.129/26* | — |
|  |  | 2001:db8:acad:1።1/64 | *—* |
|  |  | fe80::1 | *—* |
|  | G0/2 | *192.168.0.192/27* | — |
|  |  | 2001:db8:acad:2።1/64 | *—* |
|  |  | fe80::1 | *—* |
|  | S0/0/1 | 172.16.1.2 /30 | — |
|  |  | 2001:db8:2::1/64 | *—* |
|  |  | fe80::1 | *—* |
| Central | S0/0/0 | 209.165.200.226 /30 | — |
|  |  | 2001:db8:1::1/64 | *—* |
|  |  | fe80::2 | *—* |
|  | S0/0/1 | 172.16.1.1/30 | — |
|  |  | 2001:db8:2።2/64 | *—* |
|  |  | fe80::2 | *—* |
| S1 | VLAN 1 | *192.168.0.2/25* | *192.168.0.1* |
| S2 | VLAN 1 | *192.168.0.130/26* | *192.168.0.129* |
| S3 | VLAN 1 | *192.168.0.194/27* | *192.168.0.193* |
| Staff | NIC | *192.168.0.3/25* | *192.168.0.1* |
|  |  | 2001:db8:acad።2/64 | fe80::1 |
|  |  | fe80::2 |  |
| Sales | NIC | *192.168.0.131/26* | *192.168.0.129* |
|  |  | 2001:db8:acad:1።2/64 | fe80::1 |
|  |  | fe80::2 |  |
| IT | NIC | *192.168.0.195/27* | *192.168.0.193* |
|  |  | 2001:db8:acad:2።2/64 | fe80::1 |
|  |  | fe80::2 |  |
| Web | NIC | 64.100.0.3 /29 | 64.100.0.1 |
|  |  | 2001:db8:cafe።3/64 | fe80::1 |
|  |  | fe80::2 |  |

# Общие сведения и сценарий

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 настроите интерфейс SVI и базовые параметры безопасности на коммутаторах S1, S2 и S3.

# Инструкции

**IPv4-адресация**

·          Создайте подсети в соответствии с требованиями хостов.

* + Staff: 100 узлов
  + Sales: 50 узлов
  + IT: 25 узлов
  + Guest сеть, которая будет добавлена позже: 25узлов

·          Запишите назначенные IPv4-адреса в таблицу адресации.

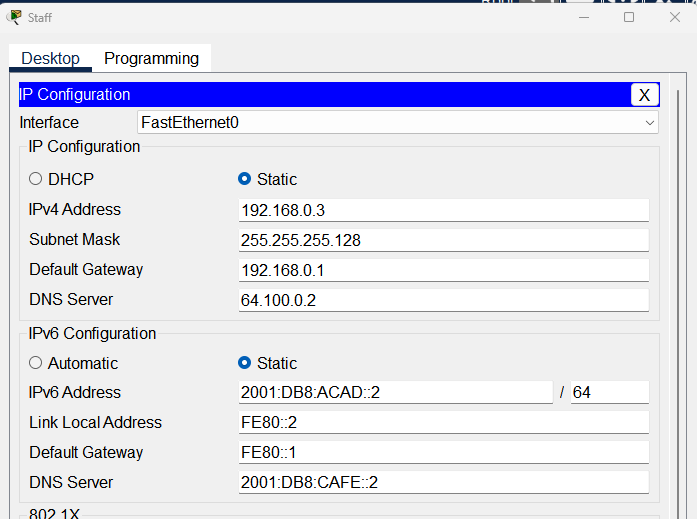
·          Запишите подсеть для сети Guest:

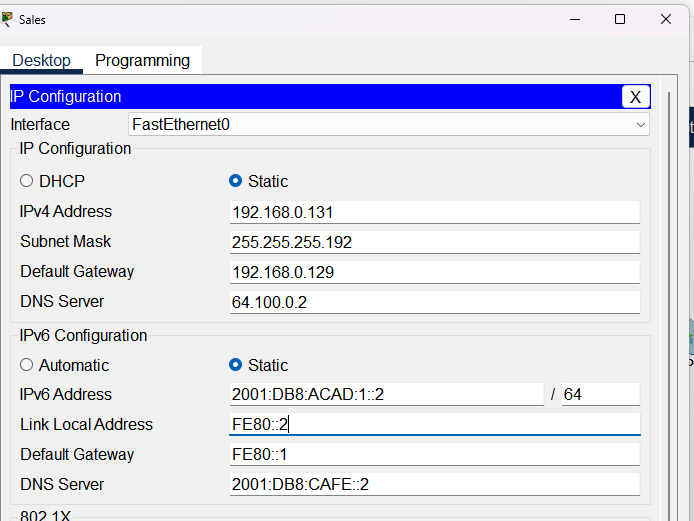
|  |  |  |  |
| --- | --- | --- | --- |
| 192.168.0.0/24 | Network Address | Subnet Mask | Broadcast Address |
| Staff: 100 узлов | 192.168.0.0 | 255.255.255.128 | 192.168.0.127 |
| Sales: 50 узлов | 192.168.0.128 | 255.255.255.192 | 192.168.0.191 |
| IT: 25 узлов | 192.168.0.191 | 255.255.255.224 | 192.168.0.223 |
| Guest: 25узлов | 192.168.0.224 | 255.255.255.224 | 192.168.0.255 |

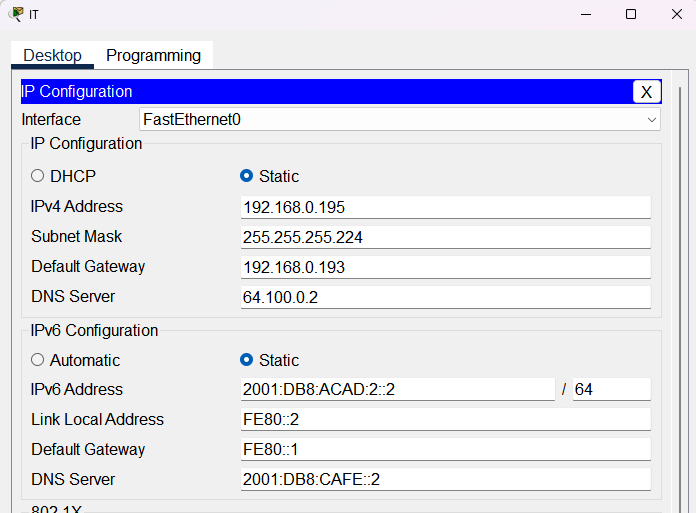
**Настройка компьютера**

·          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.



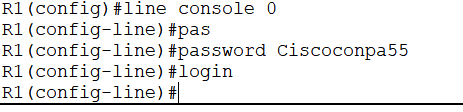
·          Отключите DNS-поиск.



·          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.

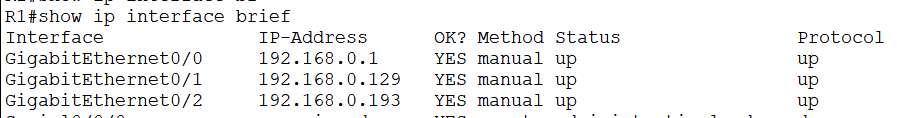


·          Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.

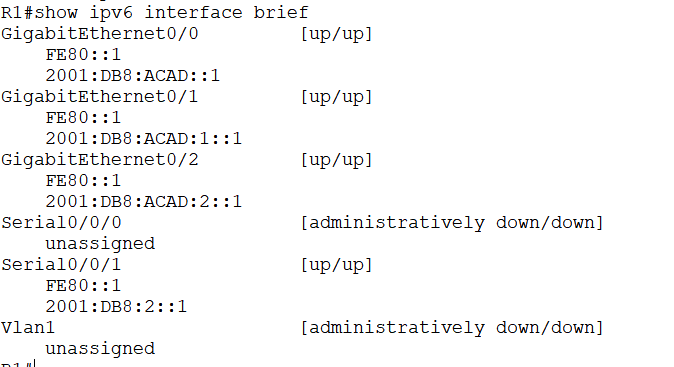


·          Настройте все интерфейсы Gigabit Ethernet.

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



* Настройте IPv6-адреса в соответствии с таблицей адресации.

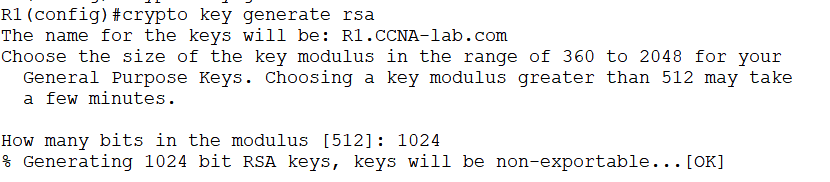


·          Настройте SSH на R1:

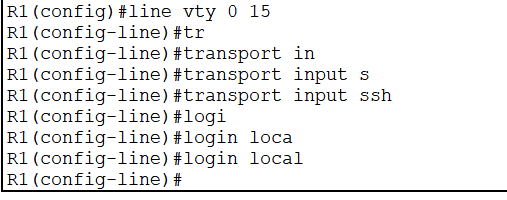
* Укажите имя домена **CCNA-lab.com**



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



* Настройте линии VTY для доступа по протоколу SSH.

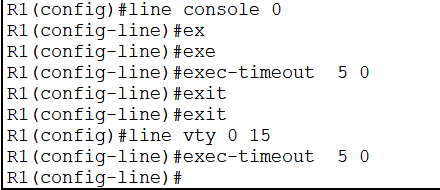


o    Используйте локальные профили пользователей для аутентификации.

* 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.  


**Конфигурация коммутатора**

·          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 DNS-поиск.

·          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.

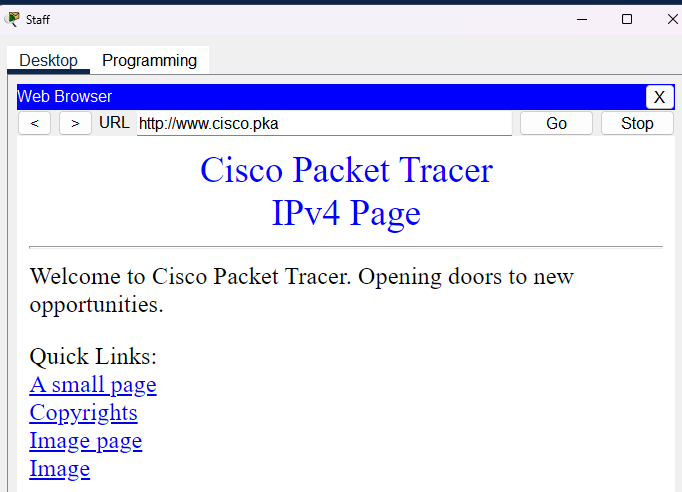


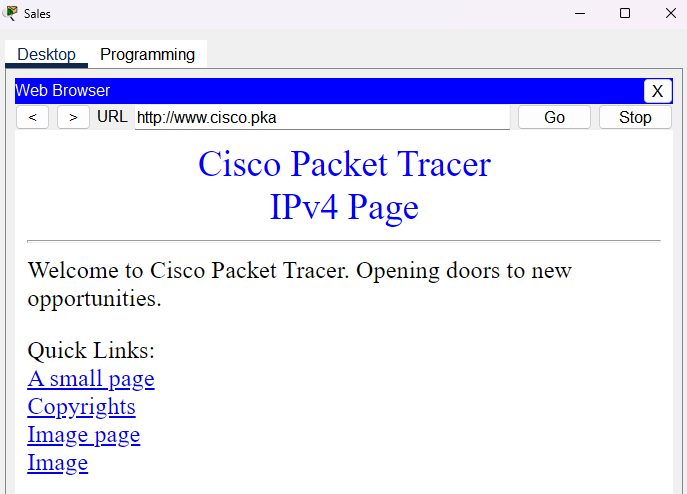


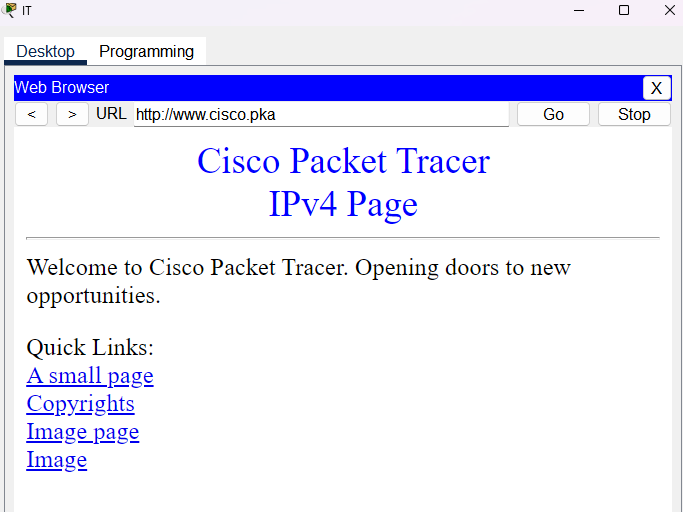


**Требования к возможности подключения**

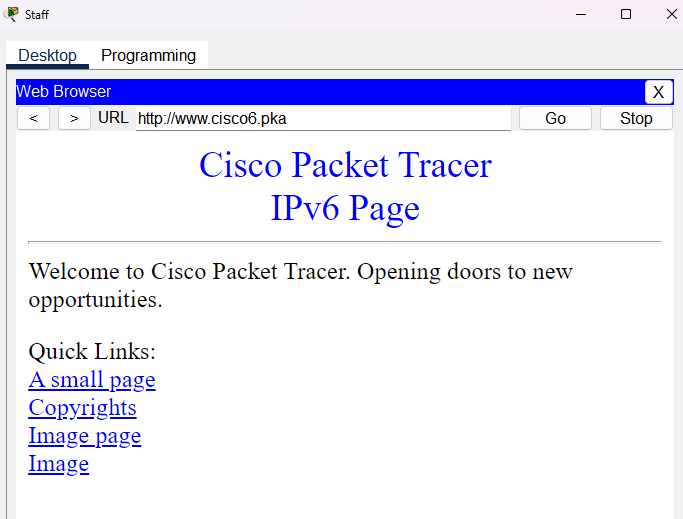
·          Откройте веб-браузер на компьютерах Staff, Sales и IT и перейдите на сайт [**www.cisco.pka**](http://www.cisco.pka)**.**

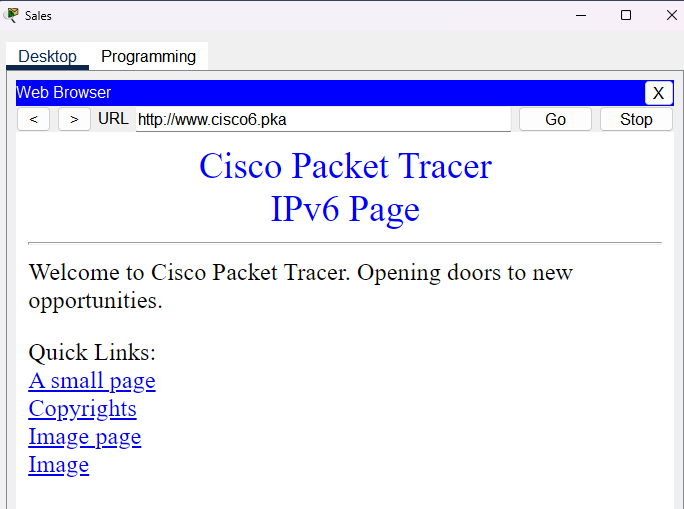


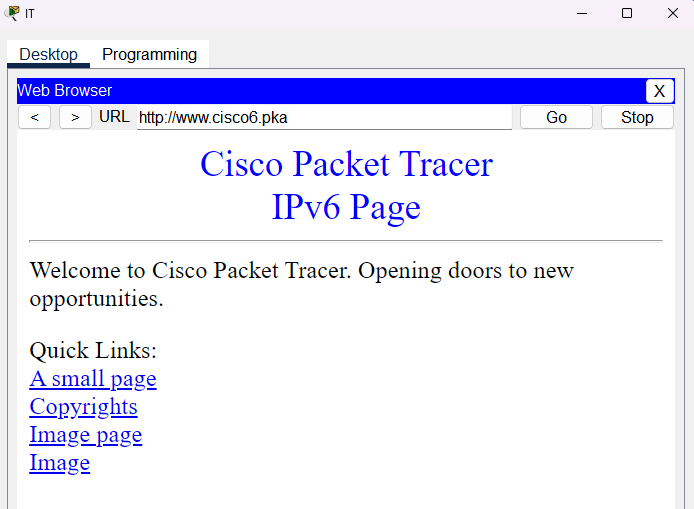




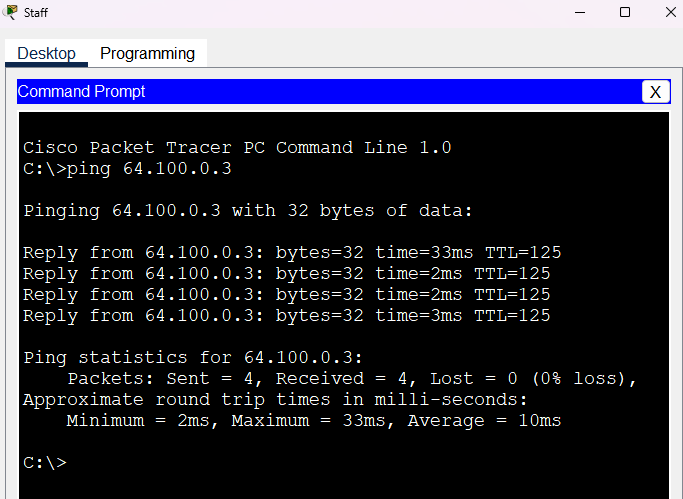
·          Откройте веб-браузер на компьютерах Staff, Sales и IT и перейдите на сайт [**www.cisco6.pka**](http://www.cisco6.pka)**.**

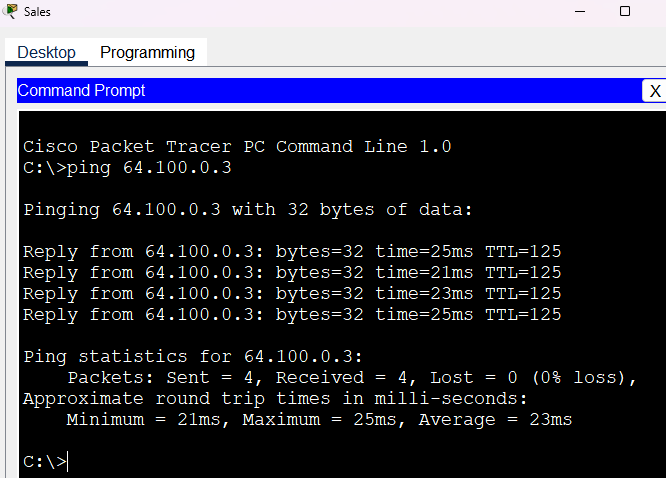


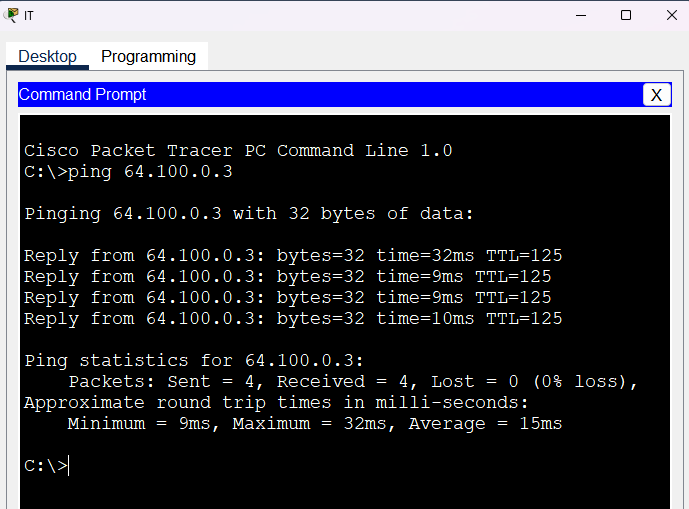


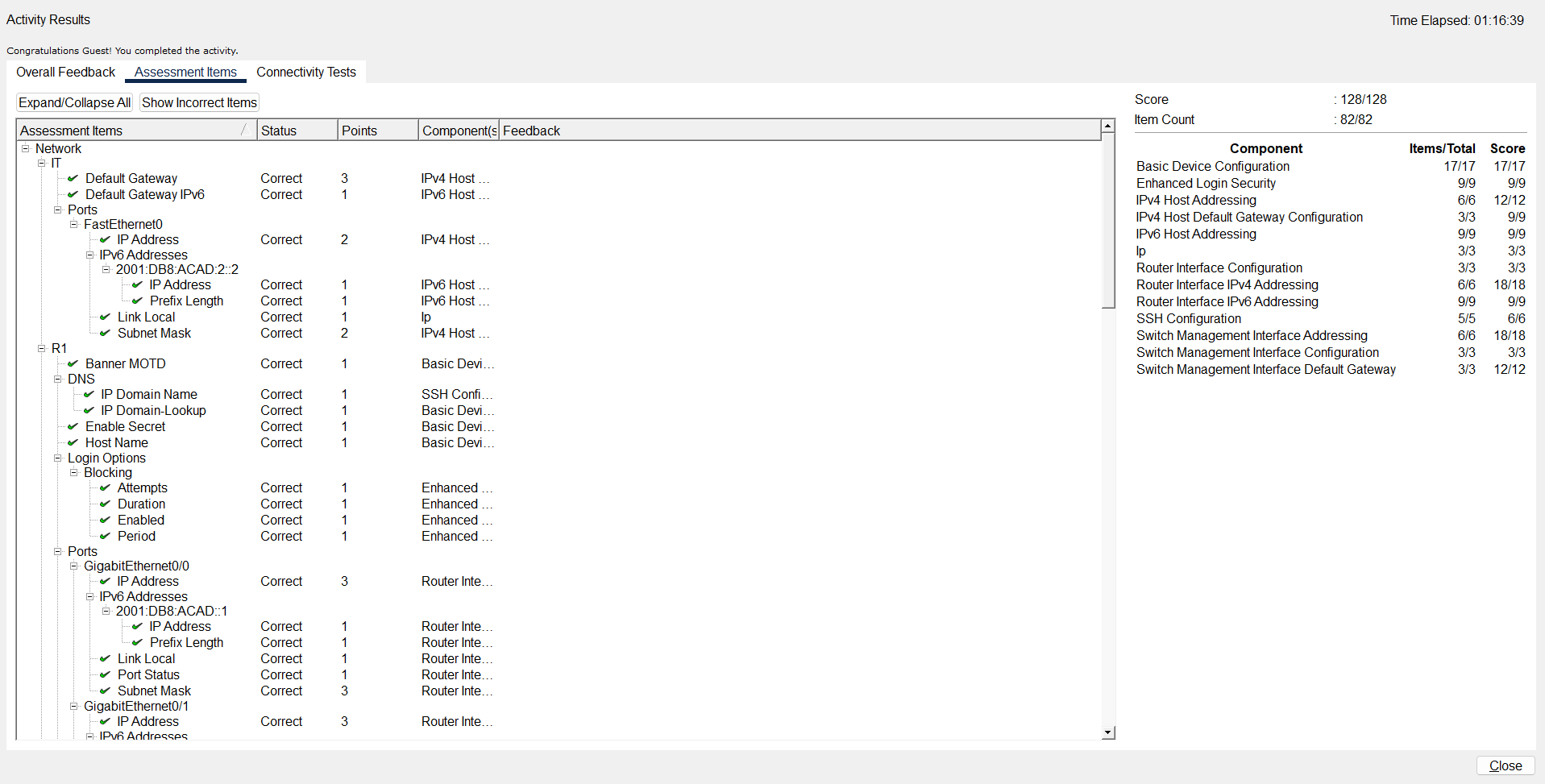


·          Команда ping должна успешно отправляться со всех компьютеров на все устройства.









# Задание “17.8.3”

# Таблица адресации

| **Устройство** | **Интерфейс** | **IP адрес/префикс** | **Шлюз по умолчанию** |
| --- | --- | --- | --- |
| R1 | G0/0 | 172.16.1.62 /26 | — |
|  |  | 2001:db8:cafe::1/64 | *—* |
|  |  | fe80::1 | *—* |
|  | G0/1 | 172.16.1.126 /26 | — |
|  |  | 2001:db8:cafe:1::1/64 | *—* |
|  |  | fe80::1 | *—* |
|  | G0/2 | 172.16.1.254 /25 | — |
|  |  | 2001:db8:cafe:2::1/64 | *—* |
|  |  | fe80::1 | *—* |
|  | S0/0/1 | 10.0.0.2 /30 | — |
|  |  | 2001:db8:2::1/64 | *—* |
|  |  | fe80::1 | *—* |
| Main | S0/0/0 | 209.165.200.226 /30 | — |
|  |  | 2001:db8:1::1/64 | *—* |
|  |  | fe80::2 | *—* |
|  | S0/0/1 | 10.0.0.1 /30 | — |
|  |  | 2001:db8:2::2/64 | *—* |
|  |  | fe80::2 | *—* |
| S1 | VLAN 1 | 172.16.1.61 /26 | 172.16.1.62 |
| S2 | VLAN 1 | 172.16.1.125 /26 | 172.16.1.126 |
| S3 | VLAN 1 | 172.16.1.253 /25 | 172.16.1.254 |
| IT | NIC | 172.16.1.1 /26 | 172.16.1.62 |
|  |  | 2001:db8:cafe::2/64 | fe80::1 |
|  |  | fe80::2 | *fe80::1* |
| Marketing | NIC | 172.16.1.65/26 | 172.16.1.126 |
|  |  | 2001:db8:cafe:1::2/64 | fe80::1 |
|  |  | fe80::2 | *fe80::1* |
| R&D | NIC | 172.16.1.129/25 | 172.16.1.254 |
|  |  | 2001:db8:cafe:2::2/64 | fe80::1 |
|  |  | fe80::2 | *fe80::1* |
| Web | NIC | 64.100.0.3/29 | 64.100.0.1 |
|  |  | 2001:db8:acad።3/64 | fe80::1 |
|  |  | fe80::2 | *fe0::1* |

# Общие сведения и сценарий

После обновления сети некоторые устройства необходимо настроить заново. Необходимо исправить конфигурации и убедиться, что все компьютеры имеют доступ к веб-серверу, R1 и коммутаторам. Кроме того, все ПК должны иметь доступ к R1 с помощью SSH. Необходимо проверить подключение как для IPv4, так и для IPv6, за исключением коммутаторов.

# Инструкции

На маршрутизаторе R1 и коммутаторах были выставлены следующие настройки:

· Пароль на привелегированый режим: **Ciscoenpa55**

Пароль консоли: **Ciscoconpa55**

· Имя пользователя и пароль администратора для SSH: **Admin1/Admin1pa55**



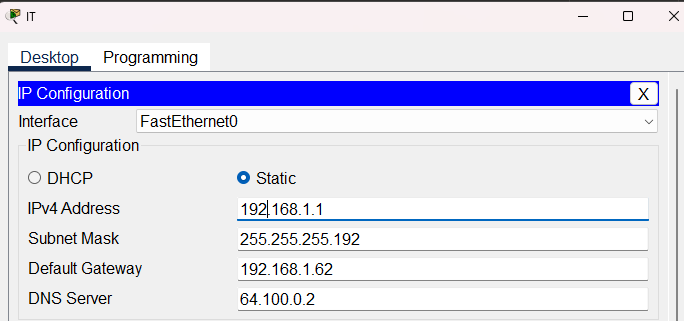
Требуемое количество узлов в подсети:

IT: 50 узлов

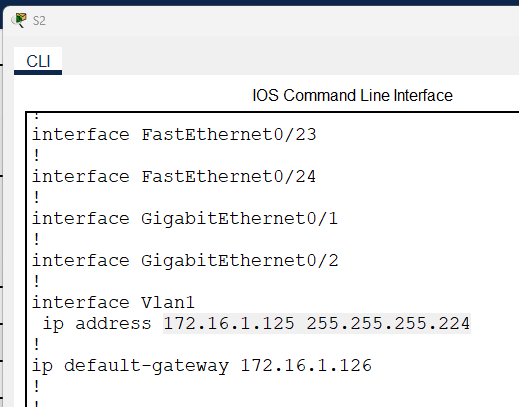
Marketing: 50 узлов

R&D: 100 узлов

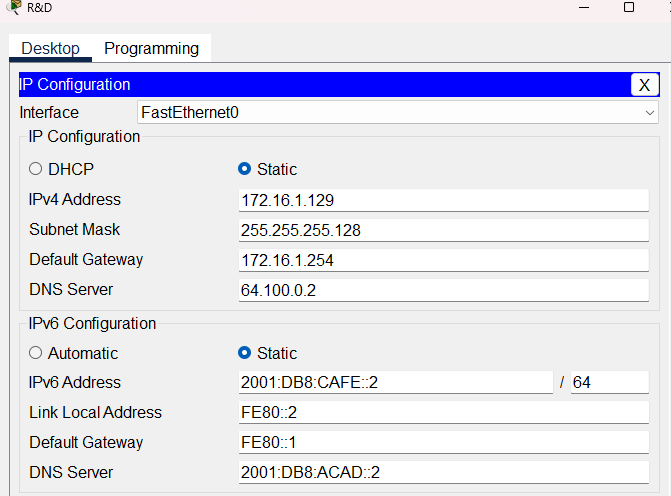
Если все проблемы конфигурации были устранены, все устройства должны иметь возможность пинговать друг друга и веб-сервер.



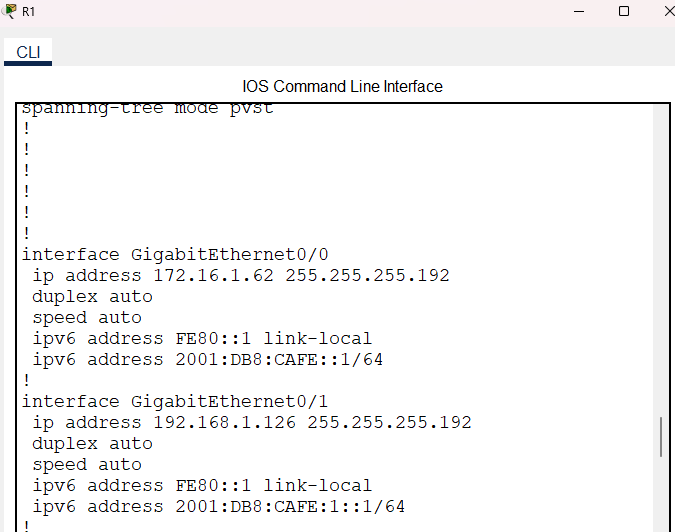
Ip и шлюз не тот что в таблице



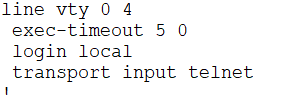
Неправильная маска



Неправильный ipv6



G0/1 неправильный ip



telnet, а должно быть ssh

