

# Cisco Packet Tracer. Отработка комплексных практических навыков

Таблица адресации

Устройство	Интерфейс	IP адрес/префикс	Шлюз по умолчанию
R1	G0/0	192.168.0.1/25	—
	G0/0	2001:db8:acad::1/64	—
	G0/0	fe80::1	—
	G0/1	192.168.0.129/26	—
		2001:db8:acad:1::1/64	—
		fe80::1	—
	G0/2	192.168.0.193/27	—
		2001:db8:acad:2::1/64	—
		fe80::1	—
	S0/0/1	172.16.1.2 /30	—
	S0/0/1	2001:db8:2::1/64	—
		fe80::1	—
Central	S0/0/0	209.165.200.226 /30	—
Центральный офис	S0/0/0	2001:db8:1::1/64	—
Центральный офис		fe80::2	—
Центральный офис		172.16.1.1/30	—
Центральный офис	S0/0/1	2001:db8:2::2/64	—
Центральный офис		fe80::2	—
S1	VLAN 1	192.168.0.2/25	пусто
S2	VLAN 1	192.168.0.130/26	пусто
S3	VLAN 1	192.168.0.194/27	пусто
Staff	NIC	192.168.0.126	192.168.0.1
Staff		2001:db8:acad::2/64	fe80::1
Staff		fe80::2	
Sales	NIC	192.168.0.190/26	192.168.0.129
Sales		2001:db8:acad:1::2/64	fe80::1
Sales		fe80::2	
IT	NIC	192.168.0.222/27	192.168.0.193
IT		2001:db8:acad:2::2/64	fe80::1
IT		fe80::2	
Web	NIC	64.100.0.3 /29	64.100.0.1
Web		2001:db8:cafe::3/64	fe80::1
Web		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.

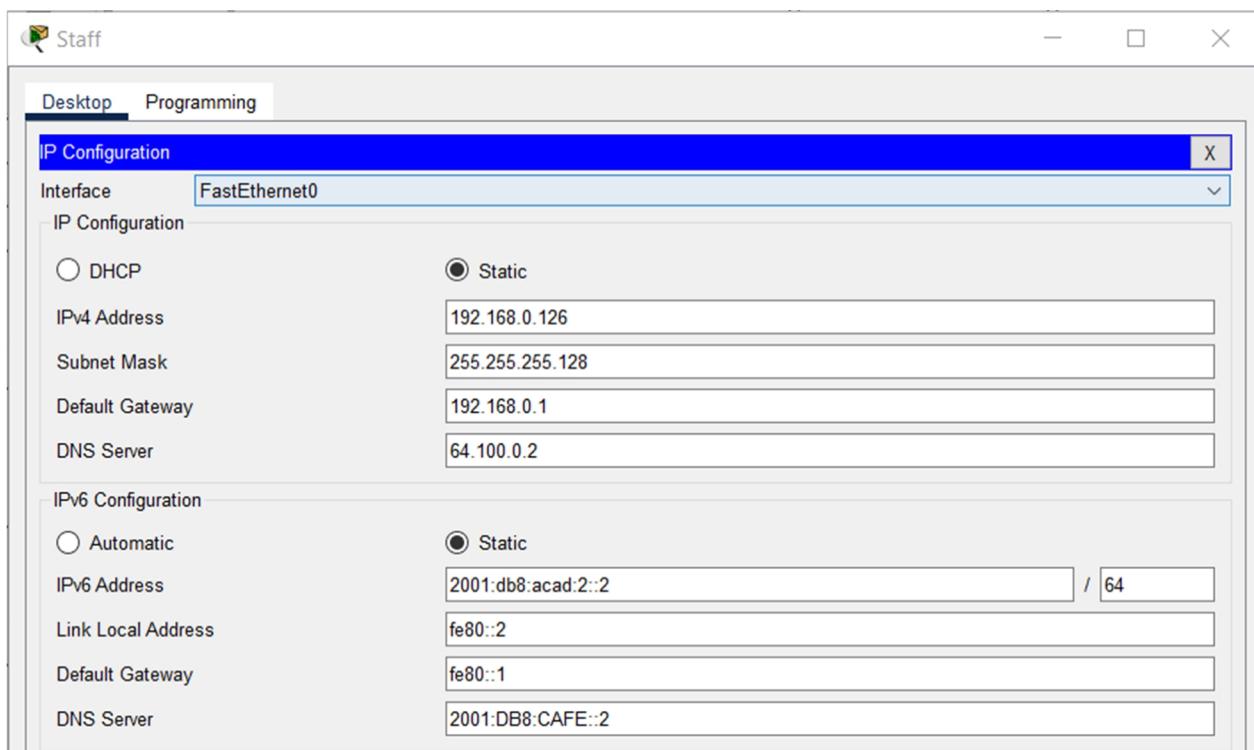
## Инструкции

### IPv4-адресация

- Создайте подсети в соответствии с требованиями хостов.
  - Staff: 100 узлов
  - Sales: 50 узлов
  - IT: 25 узлов
  - Guest сеть, которая будет добавлена позже: 25 узлов
- Запишите назначенные IPv4-адреса в таблицу адресации.
- Запишите подсеть для сети Guest: 192.168.0.224/27

### 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.





### Sales

Desktop Programming

**IP Configuration**

Interface **FastEthernet0**

IP Configuration

<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.0.190
Subnet Mask	255.255.255.192
Default Gateway	192.168.0.129
DNS Server	64.100.0.2

IPv6 Configuration

<input type="radio"/> Automatic	<input checked="" type="radio"/> Static
IPv6 Address	2001:db8:acad:1::2 / 64
Link Local Address	fe80::2
Default Gateway	fe80::1
DNS Server	2001:DB8:CAFE::2



### IT

Desktop Programming

**IP Configuration**

Interface **FastEthernet0**

IP Configuration

<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.0.222
Subnet Mask	255.255.255.224
Default Gateway	192.168.0.193
DNS Server	64.100.0.2

IPv6 Configuration

<input type="radio"/> Automatic	<input checked="" type="radio"/> Static
IPv6 Address	2001:db8:acad:2::2 / 64
Link Local Address	fe80::2
Default Gateway	fe80::1
DNS Server	2001:DB8:CAFE::2

### Настройка маршрутизатора R1

- Настройте имя устройства в соответствии с таблицей адресации.
- Отключите DNS-поиск.
- Назначьте **Ciscoenpr455** в качестве зашифрованного пароля доступа к привилегированному режиму EXEC.
- Назначьте **Ciscoconpr455** 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.

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#enable secret Ciscoenpa55
R1(config)#line console 0
R1(config-line)#password Ciscoconpa55
R1(config-line)#login
R1(config-line)#exit
R1(config)#security password min-length 10
R1(config)#service password-encryption
R1(config)#banner motd "Some"
```

- Настройте все интерфейсы Gigabit Ethernet.
  - Настройте IPv4-адреса в соответствии с вашей схемой адресации.
  - Настройте IPv6-адреса в соответствии с таблицей адресации.

```
R1(config)#interface G0/0
R1(config-if)#ip address 192.168.0.1 255.255.255.128
R1(config-if)#ipv6 address 2001:db8:acad::1
% Incomplete command.
R1(config-if)#ipv6 address 2001:db8:acad::1/64
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#no shutdown

R1(config-if)#interface G0/1
R1(config-if)#ip address 192.168.0.129 255.255.255.192
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#no shutdown

R1(config-if)#interface G0/2
R1(config-if)#ip address 192.168.0.193 255.255.255.224
R1(config-if)#ipv6 address 2001:db8:acad:2::1/64
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#no shutdown

R1(config)#interface S0/0/1
R1(config-if)#ip address 172.16.1.2 255.255.255.252
R1(config-if)#ipv6 address 2001:db8:2::1/64
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#

```

- 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.

```
--> R1(config)#ip domain-name CCNA-lab.com
R1(config)#generate key rsa
^
% Invalid input detected at '^' marker.

R1(config)#crypto key generate rsa
The name for the keys will be: R1.CCNA-lab.com
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#vty 0 4
*Mar 1 8:46:58.143: %SSH-5-ENABLED: SSH 1.99 has been enabled
^
% Invalid input detected at '^' marker.

R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#exec-timeout 6
R1(config-line)#username Admin1 privilege 15 secret Adminlpa55
R1(config)#exec-timeout 5
^
% Invalid input detected at '^' marker.

R1(config)#line vty 0 4
R1(config-line)#exec-timeout 5
R1(config-line)#login block-for 180 attempts 4 within 120
R1(config)#
R1(config)#

```

### 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.

```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#interface VLAN1
S1(config-if)#ip address 192.168.0.2 255.255.255.128
S1(config-if)#ip default-gateway 192.168.0.1
S1(config)#ip no domain-name
^
% Invalid input detected at '^' marker.

S1(config)#no ip domain-lookup
S1(config)#enable secret Ciscoenpa55
S1(config)#line console 0
S1(config-line)#password Ciscoenpa55
S1(config-line)#login
S1(config-line)#exec 5
S1(config-line)#exit
S1(config)#line vty 0 4
S1(config-line)#exec 5
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#interface VLAN1
S1(config-if)#no shutdown

S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S1(config-if)#exit
S1(config)#vty 0 4
^
% Invalid input detected at '^' marker.

S1(config)#line vty 0 4
S1(config-line)#password Ciscoenpa55
S1(config-line)#login
S1(config-line)#

```

```
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#hostname S2
S2(config)#interface VLAN1
S2(config-if)#ip address 192.168.0.130 255.255.255.192
S2(config-if)#ip default-gateway 192.168.0.129
S2(config)#no ip domain-lookup
S2(config)#enable secret Ciscoenpa55
S2(config)#line console 0
S2(config-line)#password Ciscoenpa55
S2(config-line)#login
S2(config-line)#exec 5
S2(config-line)#exit
S2(config)#line vty 0 4
S2(config-line)#exec 5
S2(config-line)#exit
S2(config)#service password-encryption
S2(config)#interface VLAN1
S2(config-if)#no shutdown

S2(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S2(config-if)#exit
S2(config)#line vty 0 4
S2(config-line)#password Ciscoenpa55
S2(config-line)#login
S2(config-line)#

```

---

```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#interface VLAN1
S2(config-if)#ip address 192.168.0.193 255.255.255.224
S2(config-if)#ip address 192.168.0.131 255.255.255.224
S2(config-if)#ip default-gateway 192.168.0.193
S2(config)#interface VLAN1
S2(config-if)#no shutdown

S2(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S2(config-if)#exit
S2(config)#hostname S3
S3(config)#no ip domain-lookup
S3(config)#enable secret Ciscoenpa55
S3(config)#line console 0
S3(config-line)#password Ciscoenpa55
S3(config-line)#login
S3(config-line)#exec 5
S3(config-line)#exit
S3(config)#line vty 0 4
S3(config-line)#exec 5
S3(config-line)#exit
S3(config)#service password-encryption
S3(config)#interface VLAN1
S3(config-if)#ip address 192.168.0.194 255.255.255.224
S3(config-if)#exit
S3(config)#+
```

#### Требования к возможности подключения

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

#### Cisco Packet Tracer IPv4 Page

Welcome to Cisco Packet Tracer. Opening doors to new opportunities.

Quick Links:

[A small page](#)

[Copyrights](#)

[Image page](#)

[Image](#)

- 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.