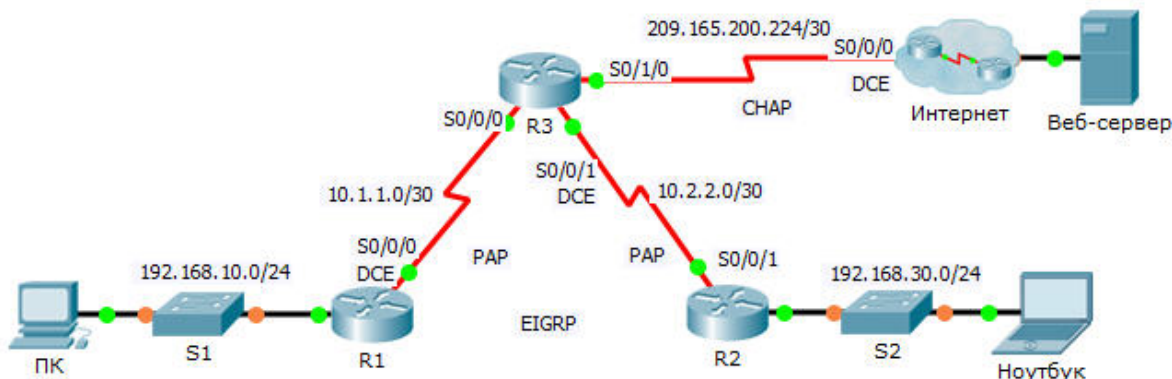


# Packet Tracer. Настройка аутентификации протоколов PAP и CHAP

## Топология



## Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	192.168.10.1	255.255.255.0	Недоступно
	S0/0/0	10.1.1.1	255.255.255.252	Недоступно
R2	G0/0	192.168.30.1	255.255.255.0	Недоступно
	S0/0/1	10.2.2.2	255.255.255.252	Недоступно
R3	S0/0/0	10.1.1.2	255.255.255.252	Недоступно
	S0/0/1	10.2.2.1	255.255.255.252	Недоступно
	S0/1/0	209.165.200.225	255.255.255.252	Недоступно
ISP	S0/0/0	209.165.200.226	255.255.255.252	Недоступно
	G0/0	209.165.200.1	255.255.255.252	Недоступно
Веб-сервер	Сетевой адаптер	209.165.200.2	255.255.255.252	209.165.200.1
ПК	Сетевой адаптер	192.168.10.10	255.255.255.0	192.168.10.1
Ноутбук	Сетевой адаптер	192.168.30.10	255.255.255.0	192.168.30.1

## Задачи

Часть 1. Проверка настроек маршрутизации

Часть 2. Настройка PPP в качестве метода инкапсуляции

Часть 3. Настройка аутентификации PPP

## Исходные данные

В рамках данного задания вам предстоит отработать настройку инкапсуляции PPP на последовательных каналах. Также вы сможете настроить аутентификацию PAP PPP и аутентификацию CHAP PPP.

## Часть 1: Проверьте настройки маршрутизации

### Шаг 1: Просмотрите текущие настройки на всех маршрутизаторах.

Рассматривая настройки маршрутизатора, обратите внимание на использование в топологии как статических, так и динамических маршрутов.

### Шаг 2: Проверьте связь между компьютерами и веб-сервером.

Отправьте эхо-запрос с ПК и Ноутбука на веб-сервер по адресу 209.165.200.2. Обе команды **ping** должны пройти успешно. Не забудьте выделить достаточно времени на схождение STP и EIGRP.

## Часть 2: Настройте PPP в качестве метода инкапсуляции

### Шаг 1: Настройте R1 на использование инкапсуляции PPP с R3.

На R1 введите следующие команды:

```
R1(config)# interface s0/0/0
R1(config-if)# encapsulation ppp
```

### Шаг 2: Настройте R2 на использование инкапсуляции PPP с R3.

Введите соответствующие команды на R2:

### Шаг 3: Настройте R3 на использование инкапсуляции PPP с R1, R2 и ISP.

Введите соответствующие команды на маршрутизаторе R3:

### Шаг 4: Настройте ISP на использование инкапсуляции PPP с R3.

a. Нажмите на облако **Интернет**, затем на ISP. Введите следующие команды:

```
Router(config)# interface s0/0/0
Router(config-if)# encapsulation ppp
```

b. Выйдите из облака **Интернет** путем нажатия кнопки **Back** (Назад) в левом верхнем углу или сочетания клавиш **Alt+СТРЕЛКА ВЛЕВО**.

### Шаг 5: Проверьте подключение к веб-серверу.

ПК и Ноутбук должны успешно отправлять эхо-запросы на веб-сервер по адресу 209.165.200.2. Возможно, понадобится подождать, пока заработают интерфейсы и EIGRP снова сойдётся.

## Часть 3: Настройте аутентификацию PPP

### Шаг 1: Настройте аутентификацию PAP PPP между R1 и R3.

Примечание. Чтобы обеспечить более надёжное шифрование пароля, вместо ключевого слова **password**, приведённого в учебных материалах, следует использовать ключевое слово **secret**.

a. На R1 введите следующие команды:

```
R1(config)# username R3 secret class
R1(config)# interface s0/0/0
R1(config-if)# ppp authentication pap
R1(config-if)# ppp pap sent-username R1 password cisco
```

- b. Введите следующие команды на маршрутизаторе **R3**:

```
R3(config)# username R1 secret cisco
R3(config)# interface s0/0/0
R3(config-if)# ppp authentication pap
R3(config-if)# ppp pap sent-username R3 password class
```

### Шаг 2: Настройте аутентификацию PAP PPP между R2 и R3.

Повторите шаг 1 для настройки аутентификации между маршрутизаторами **R2** и **R3**, при необходимости изменяя имена пользователей. Обратите внимание, что каждый пароль, отправленный на каждый последовательный порт, соответствует паролю, ожидаемому на противоположном маршрутизаторе.

### Шаг 3: Настройте аутентификацию PPP CHAP между маршрутизаторами R3 и ISP.

- a. Введите следующие команды на маршрутизаторе **ISP**. Имя узла отправляется в качестве имени пользователя:

```
Router(config)# hostname ISP
ISP(config)# username R3 secret cisco
ISP(config)# interface s0/0/0
ISP(config-if)# ppp authentication chap
```

- b. Введите следующие команды на маршрутизаторе **R3**: Для аутентификации CHAP пароли должны совпадать:

```
R3(config)# username ISP secret cisco
R3(config)# interface serial0/1/0
R3(config-if)# ppp authentication chap
```

### Шаг 4: Проверьте связь между компьютерами и веб-сервером.

Отправьте эхо-запрос с **ПК** и **Ноутбука** на веб-сервер по адресу 209.165.200.2. Обе команды **ping** должны пройти успешно. Не забудьте выделить достаточно времени на схождение STP и EIGRP.