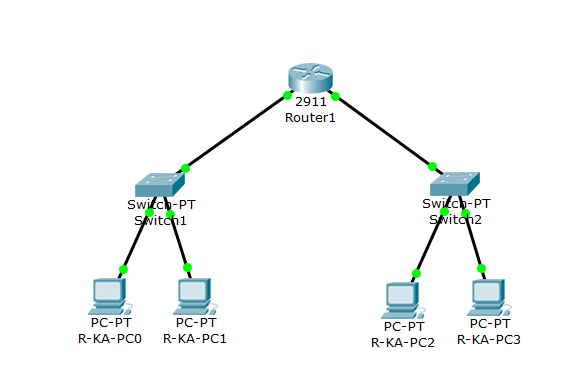
**Отчёт**

Для выполнения работы была использована программа Cisco Packet Tracer Student (6.2 version).

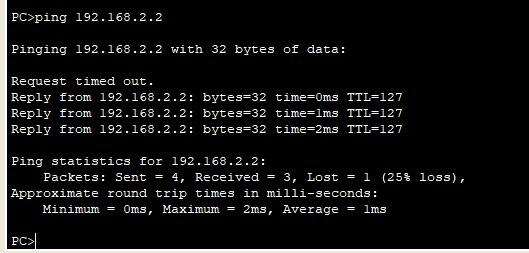
**Часть 1. Построение модели сети:**

Настроенная сеть с изменёнными названиями и описаниями:

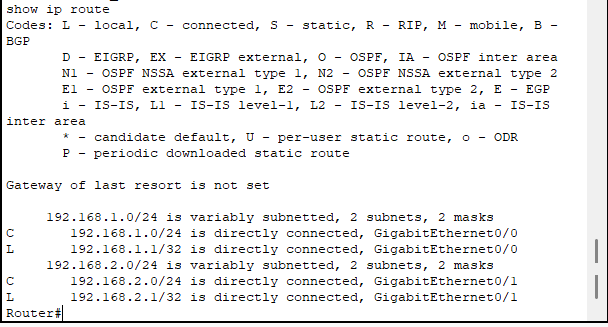
****

**Док-ва работоспособности:**

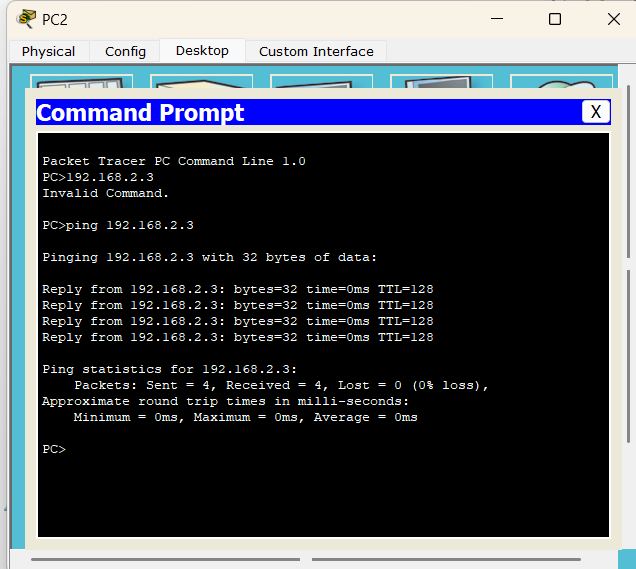
**Связь пк1 с пк2 (левая и правая подсети)**



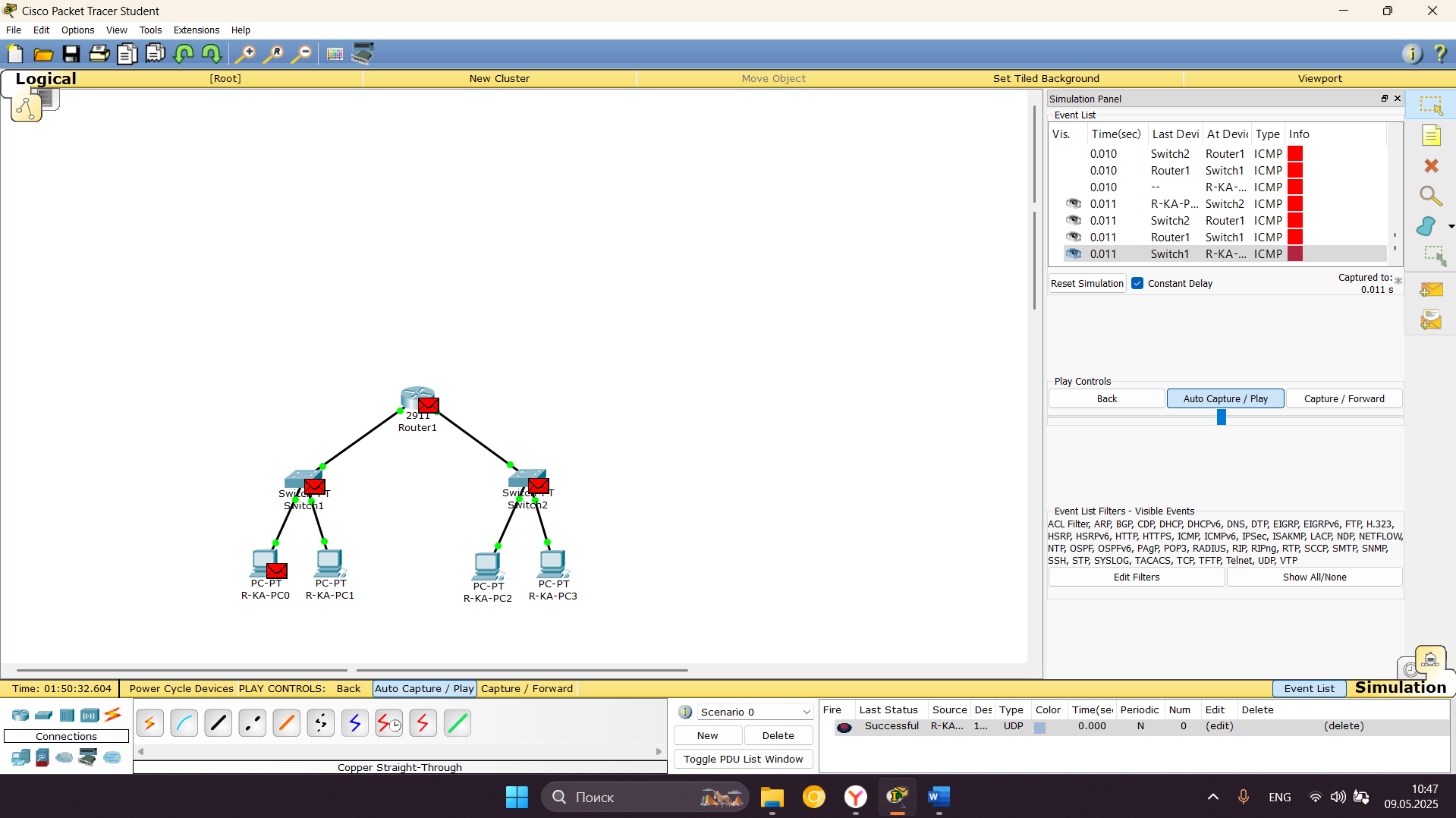
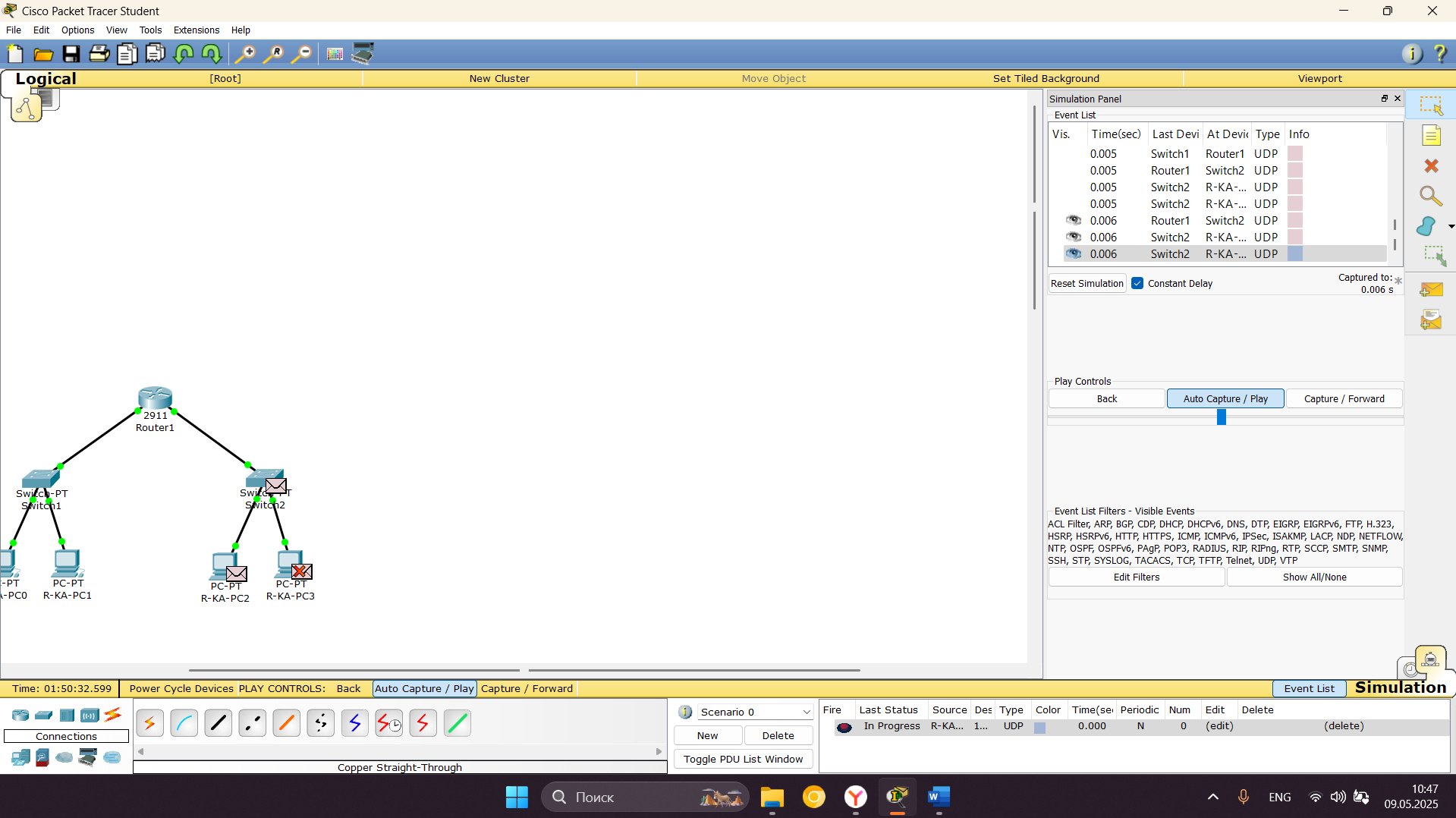
**Работа роутера:**



**Связь пк2 с пк3:**



**TCP запрос на 5 КБ успешно выполнен:**

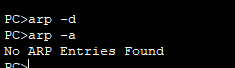


**Вывод:**

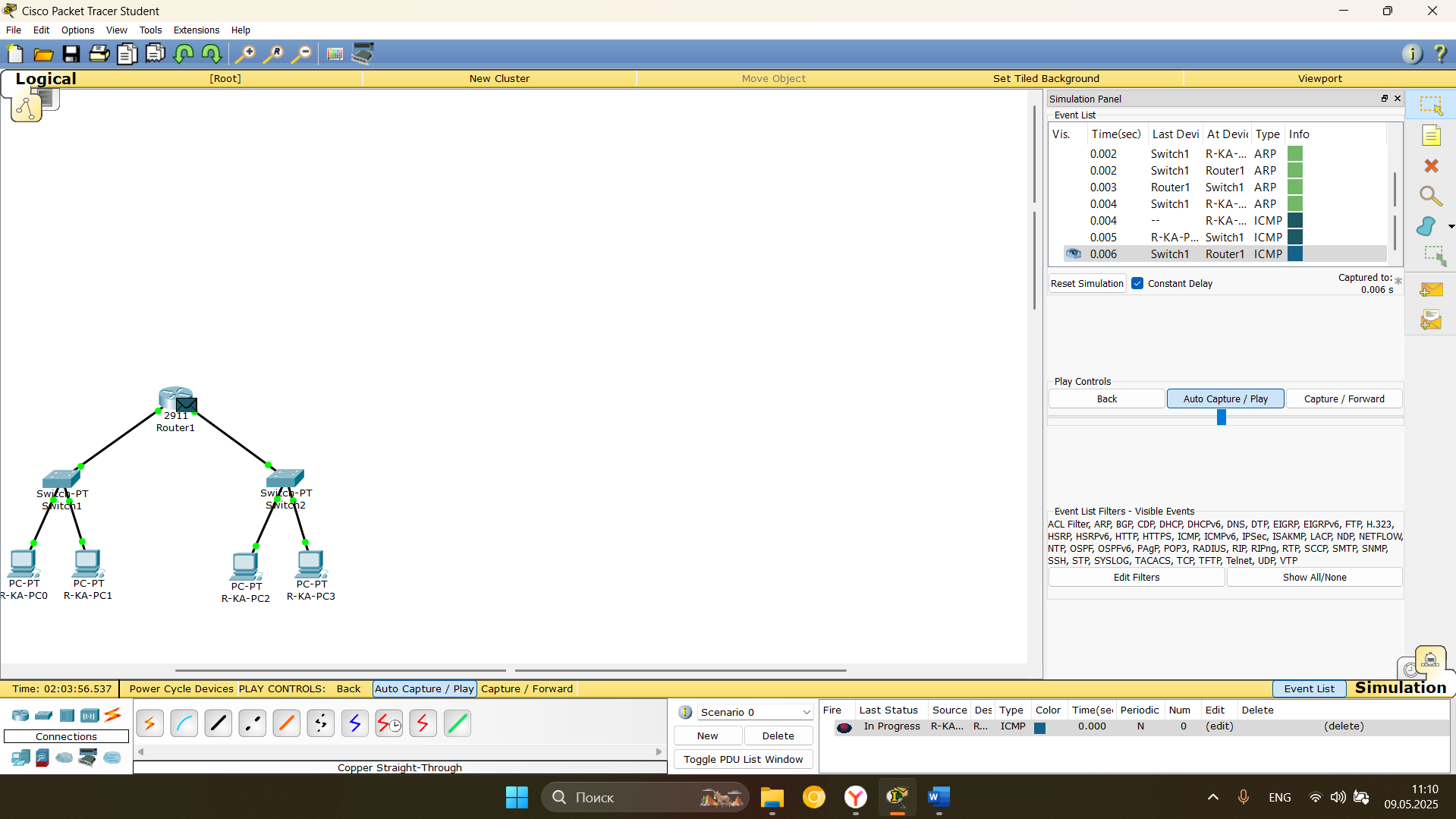
Сеть настроена успешно. Об этом говорят следующие факты: медные провода горят зелёным, значит подключено всё верно; скриншоты подтверждают информацию о том, что компьютеры связаны с роутером и коммутаторами. TCP запрос на 5КБ успешно выполнен через вкладку ADD Complex PDU.

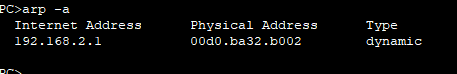
**Часть 2. Определение MAC-адреса с помощью ARP-запроса:**

**Проведена очистка arp на пк 1 и пк 2:**



**ARP запрос отправлен и записан в таблицу:**





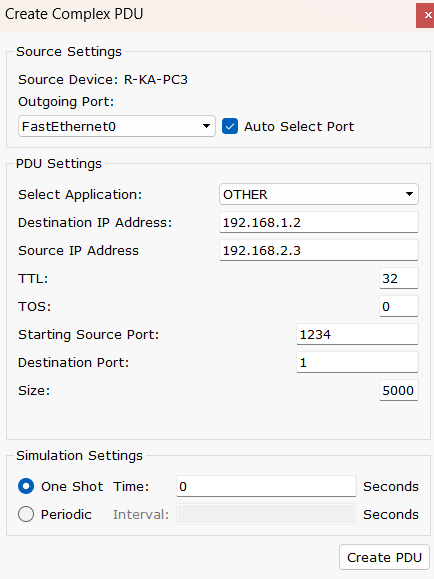
**Вывод:**

ARP запрос успешно дошёл до правой подсети (R-KA-PC1 to R-KA-PC2) на то есть док-во на скриншоте с консоли R-KA-PC2, тем самым мы узнали MAC address ПК (Physical Address).

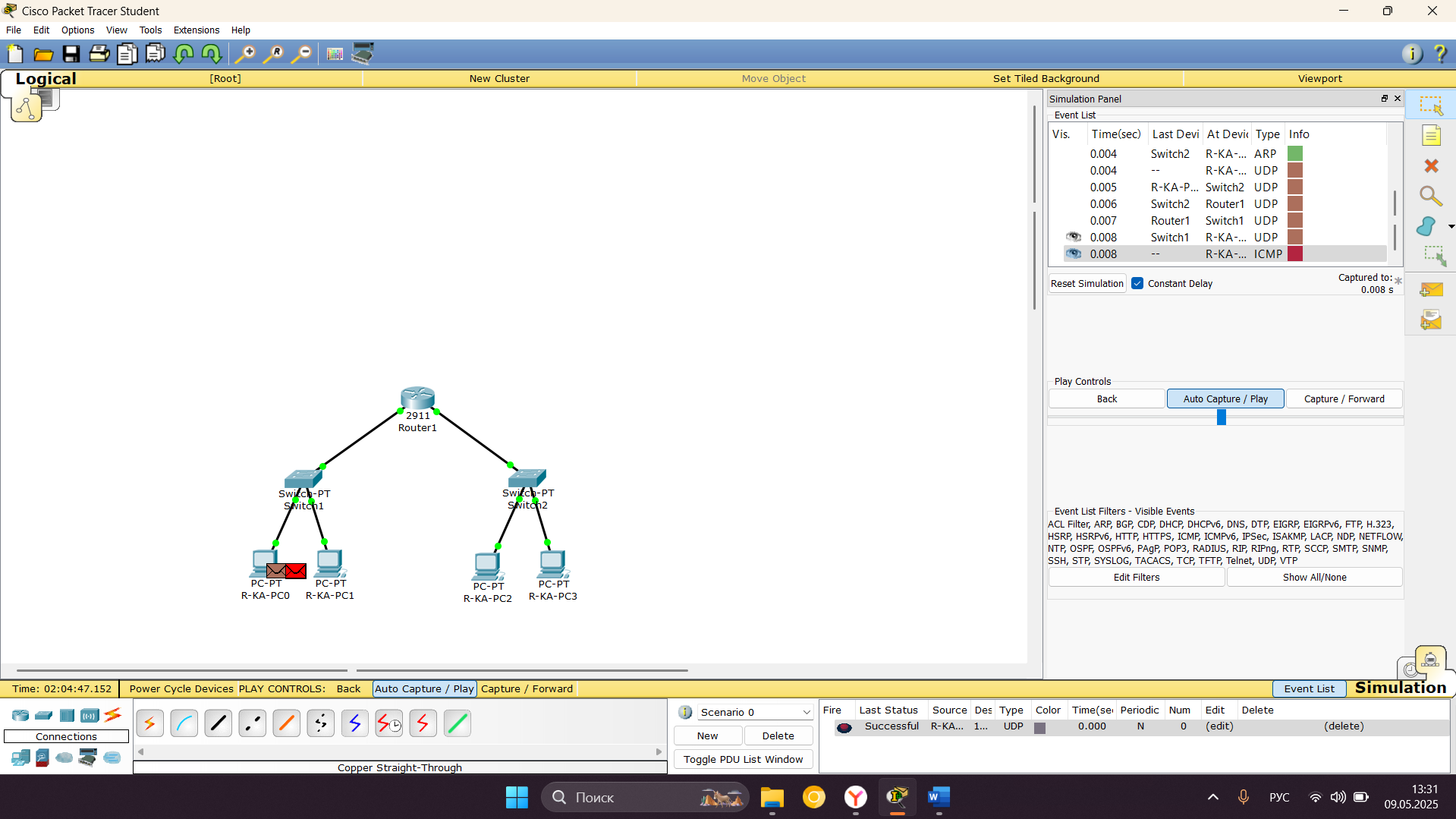
**Часть 3. Реализация атаки ARP-спуфинг:**

**Создание ложного ARP-ответа через Complex-PDU:**

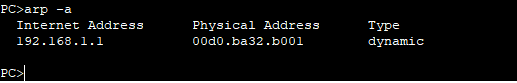
Передача пакетов 5KB (size 5000). APR = OTHER (т.к. отдельно APR в конверте нет)!



**Выводы:**

****

**Успешная замена MAC-Address:**

****

**Другой путь:**

Можно также было и выполнить через консоль командой:

arp -s 192.168.1.1 00d0.ba32.b001

Вывод остался таким же.