Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Вятский государственный университет»

Колледж ВятГУ

**ОТЧЕТ**

**ПО ЛАБОРАТОРНОЙ РАБОТЕ №7**

**«Разрешение адресов по протоколу ARP. ARP-спуфинг»**

**«Компьютерные сети»**

Выполнил: студент учебной группы

ИСПк-202-52-00

Радыгин А.К.

Преподаватель:

Жилова Ю.А.

Киров

2024

**Цель работы** – ознакомиться с механизмом работы протокола ARP; научиться формировать и отправлять пользовательские пакеты; ознакомиться с журналом работы сетевого устройства в эмуляторе; научиться проводить сетевую атаку вида ARP-спуфинг.

**Результаты выполнения задания**

**Задание 1**

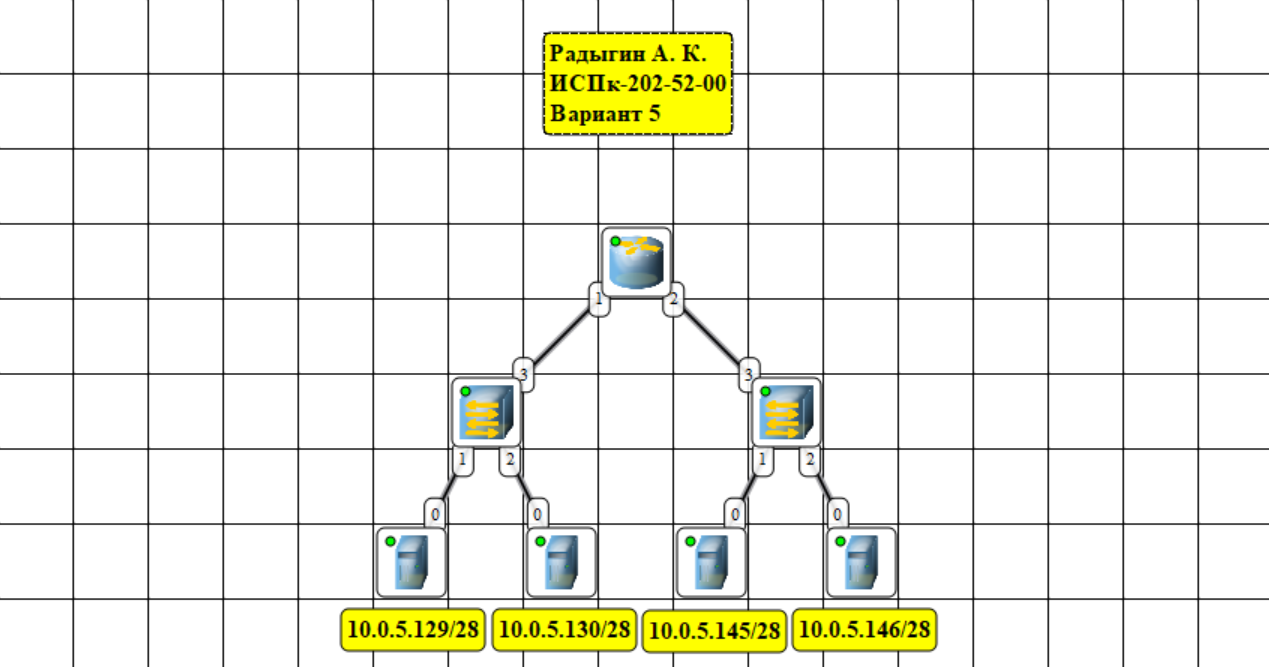


Рис. 1 – результат настройки сети

Сеть 10.0.5.128/27 была разбита на две подсети: 10.0.5.128/28 и 10.0.5.144/28, адреса, назначенные узлам, представлены на рисунке. Для каждого узла был указан основной шлюз и включена маршрутизация, в настройках маршрутизатора так же были указаны шлюзы обеих подсетей и была включена маршрутизация.

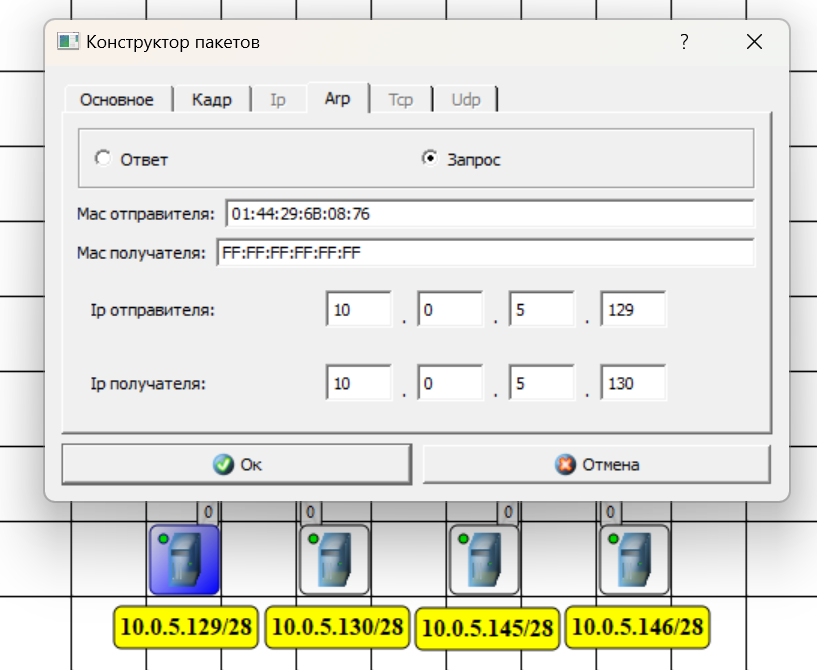


Рис. 2 – параметры в конструкторе пакетов

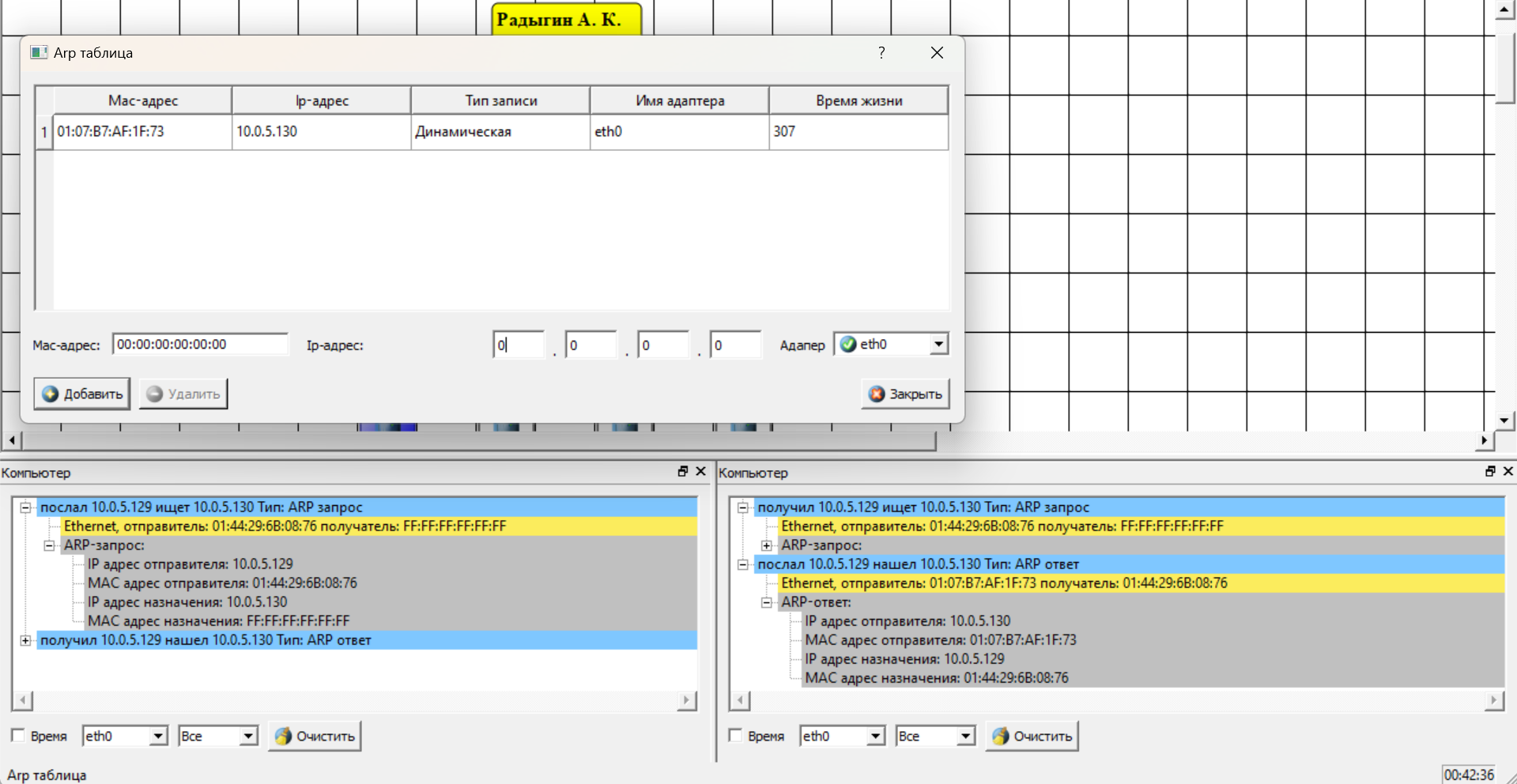


Рис. 3 – результат выполнения ARP-запроса

При поиске MAC-адреса узла 2 ARP-запрос был отправлен узлом 1 на коммутатор, который широковещательно переслал его маршрутизатору и узлу 2. Маршрутизатор не нашёл в своей таблице сети узла с искомым адресом, потому не стал предпринимать никаких действий; узел 2, узнавший свой IP, отправил ARP-ответ обратно на коммутатор; коммутатор передал ответ с искомым MAC-адресом узлу 1.

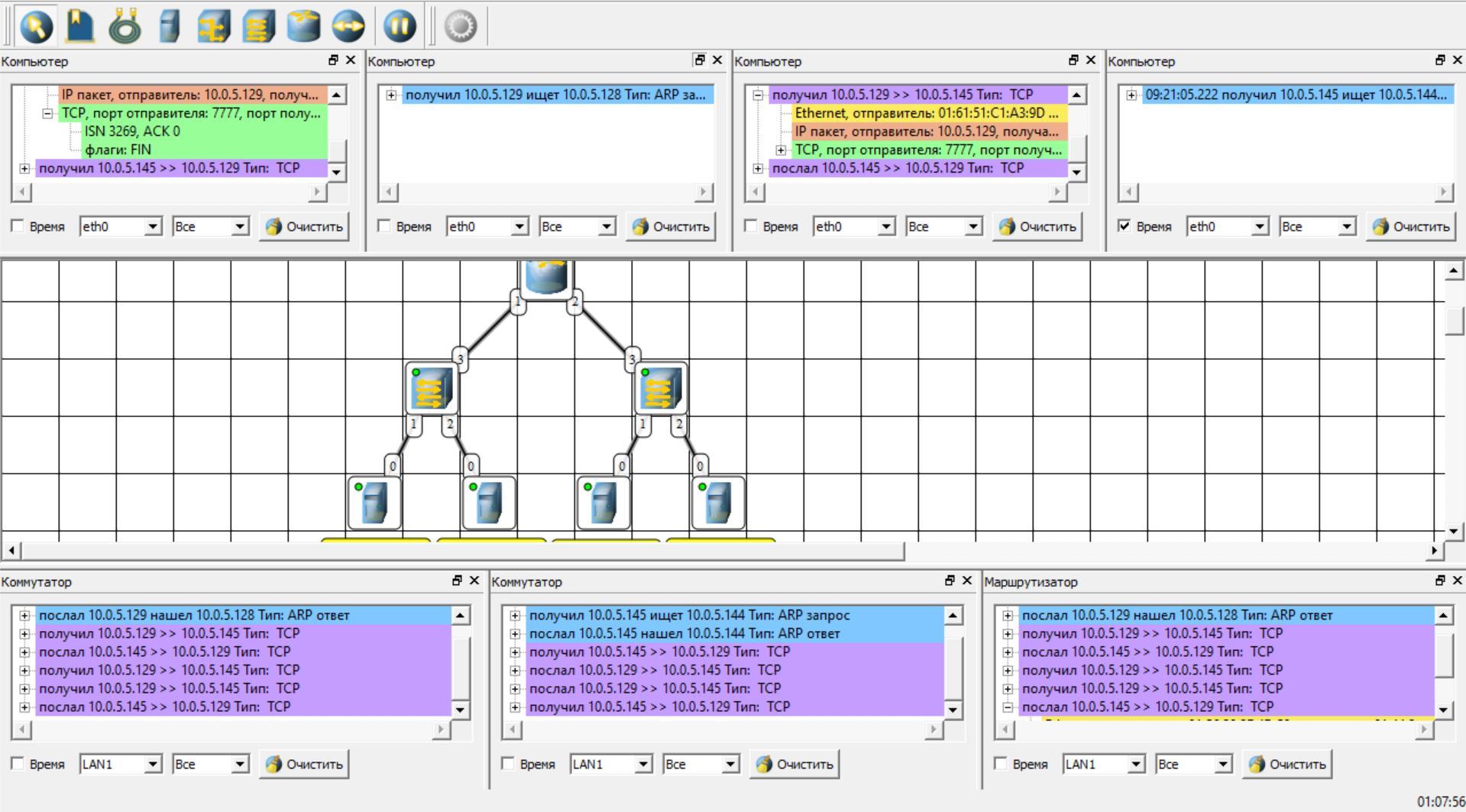


Рис. 4 – результат передачи TCP-пакета от узла 1 к узлу 3

На рисунке 4 сверху слева направо изображены журналы узлов 1, 2, 3 и 4 соответственно; снизу слева направо изображены журналы коммутаторов 1 и 2 и маршрутизатора соответственно.

Сначала узел 1 отправил ARP-запрос на коммутатор в своей подсети; коммутатор переслал этот запрос маршрутизатору и узлу 2, при чём последний на этом перестал участвовать в процессе, так как не увидел своего адреса и понял, что тут не при чём (его журнал можно наблюдать на второй таблице сверху). Маршрутизатор же приметил, что искомый узел находится во второй подсети, и потому перенаправил запрос на её коммутатор. Коммутатор так же широковещательно разослал запрос: узел 4 себя в нём не узнал и продолжил молчать, а узел 3 отправил ARP-ответ узлу 1 тем же путём, что дошёл до него запрос.

Наконец узнав адрес своего получателя, узел 1 отправил TCP-пакет объёмом 1 килобайт узлу 3. Этот пакет дошёл до узла 3 тем же путём, что и ARP-запрос, за исключением того, что на этот раз без широковещательных рассылок, так как все адреса уже известны. После получения пакета с информацией узел 3 отправил аналогичный пакет с подтверждением о получении узлу 1, который так же без лишних рассылок и пересылок дошёл до своего получателя.

Первая строчка TCP-пакета содержит ISN (Initial Sequence Number) – порядковый номер пакета и ACK (Acknowledgment Number) – номер подтверждения. Вторая строчка содержит флаг или флаги SYN, ACK, FIN в зависимости от своего состояния (с какой целью отправлен).

**Задание 2**

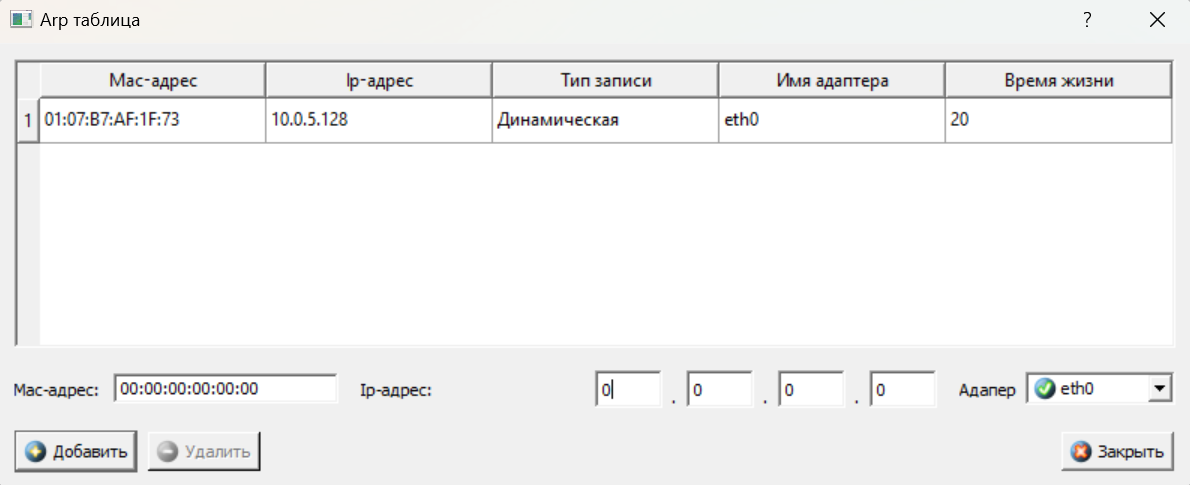


Рис. 5 – ARP-таблица узла 1после отправки ARP-ответа с узла 2

В ARP-таблице, представленной на рисунке 5, можно наблюдать, что mac-адрес узла 2 и IP-адрес основного шлюза теперь располагаются в одной записи. Похоже, кто-то выдаёт себя не за того, кем является на самом деле.

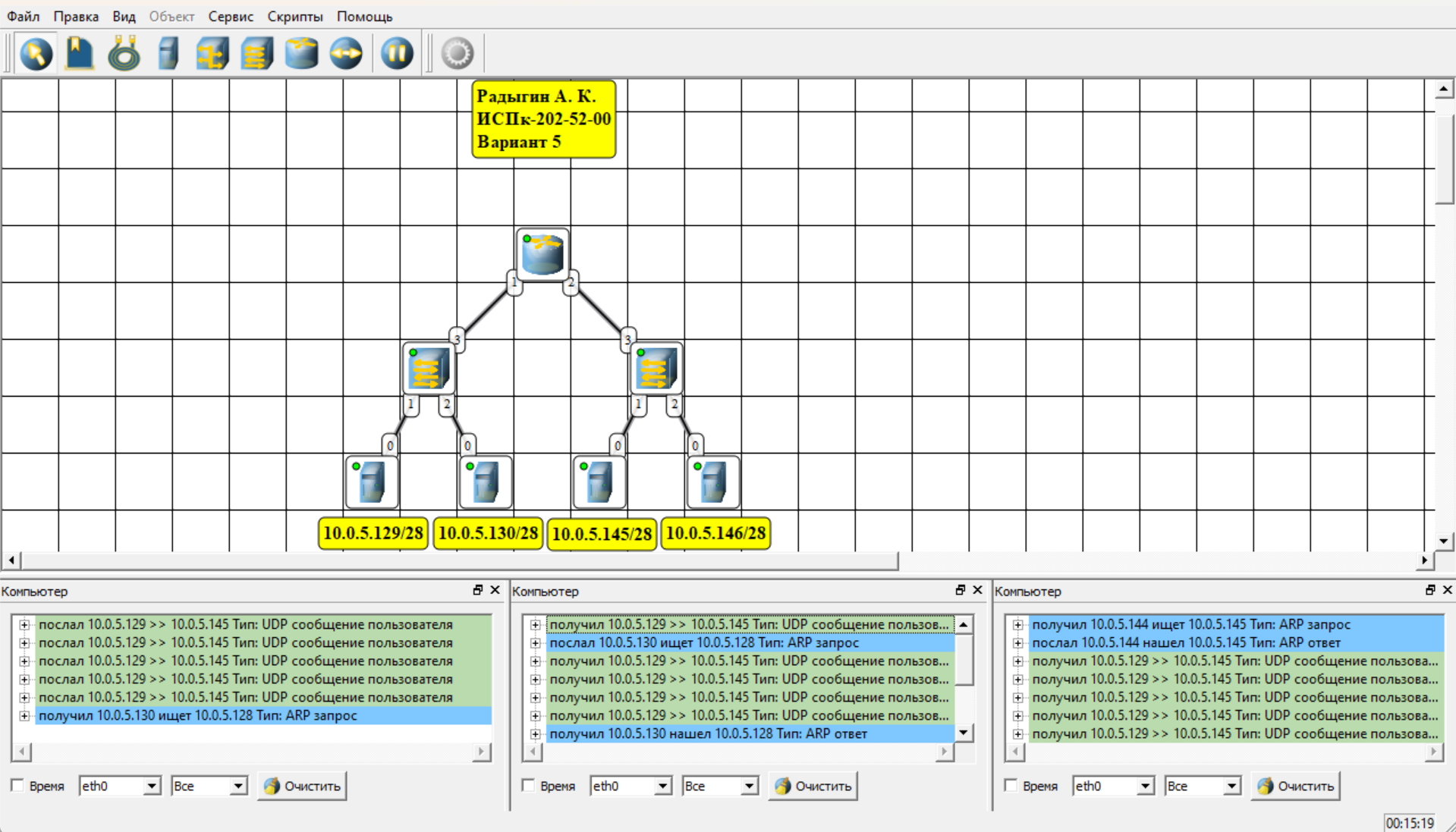


Рис. 6 – результат передачи пакетов от узла 1 к узлу 3

Как можно видеть на рисунке 6 (снизу представлены журналы для узлов 1, 2 и 3 соответственно), пакеты от узла 1 сначала передаются узлу 2, и только потом от последнего доставляются узлу 3.

**Задание 3**

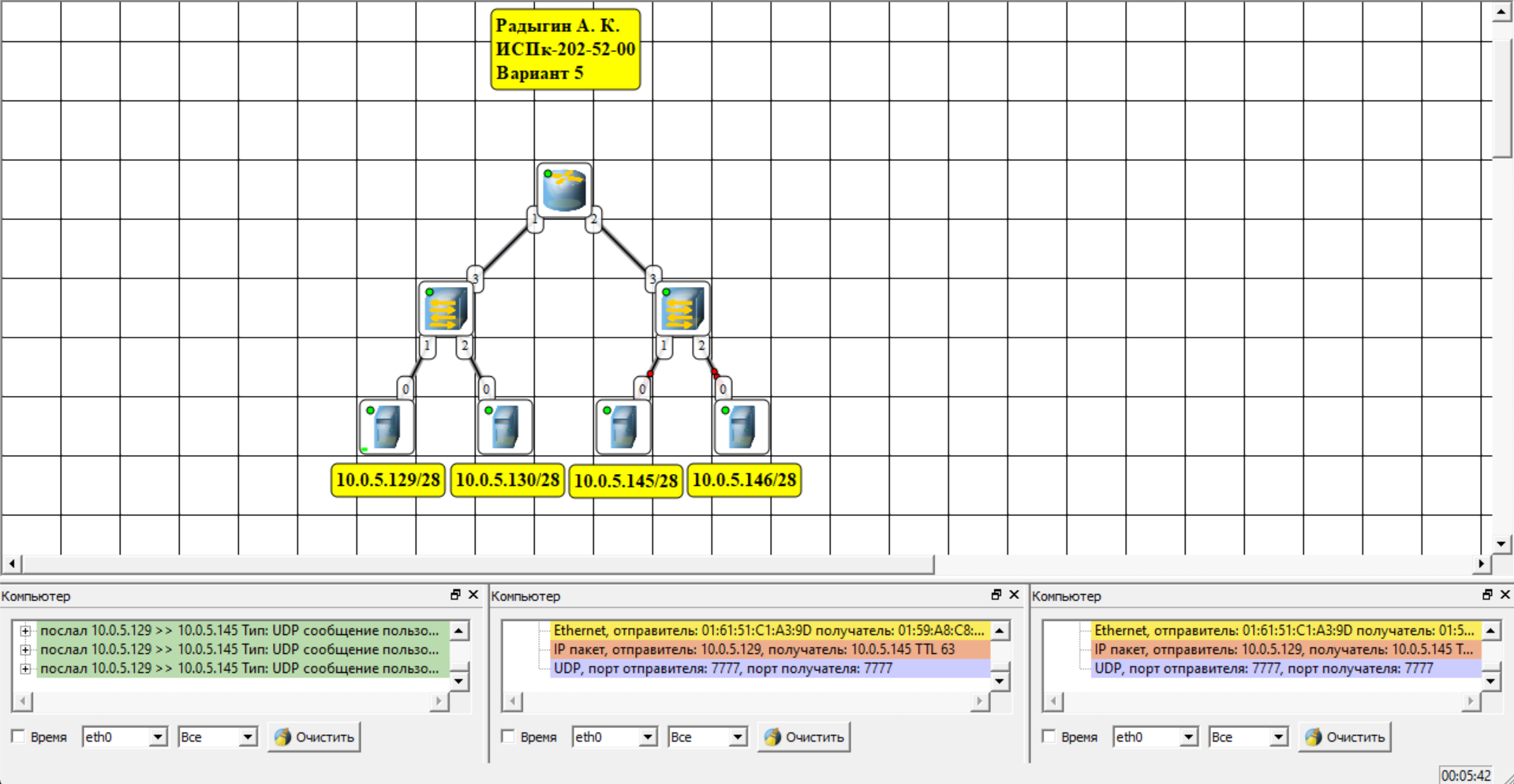


Рис. 7 – результат воспроизведения IP-спуфинга

Для реализации передачи пакетов, представленной на рисунке 7 (пакты были отправлены с узла 1 на узел 3, но несмотря на то, что во второй подсети используется коммутатор, а не концентратор, пакеты доходят и до узла 3, и до узла 4), узлу 4 был присвоен IP-адрес узла 3.

**Ответы на контрольные вопросы**

1. Протокол ARP (Address Resolution Protocol) используется для сопоставления IP-адресов с MAC-адресами в локальной сети. Когда устройство хочет отправить данные другому устройству в той же сети, оно использует ARP для определения MAC-адреса устройства-получателя.
2. Самопроизвольный ARP (или Gratuitous ARP) – это сообщение ARP, которое отправляется устройством без запроса от других устройств. Оно служит для обновления таблиц ARP у других устройств в сети и проверки наличия дублирующихся IP-адресов.
3. ARP-спуфинг – это атака, при которой злоумышленник посылает ложные сообщения ARP в сеть. Это позволяет ему связывать свой собственный MAC-адрес с IP-адресом другого устройства, что ведет к перенаправлению трафика через машину злоумышленника.
4. IP-спуффинг – это метод атаки, при котором злоумышленник фальсифицирует исходящий IP-пакет так, чтобы он выглядел как отправленный с другого IP-адреса. Основное отличие от ARP-спуффинга заключается в том, что IP-спуффинг изменяет информацию на уровне сетевого уровня модели OSI, тогда как ARP-спуффинг работает на канальном уровне.