**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**федеральное государственное бюджетное образовательное учреждение высшего образования**

**«Российский экономический университет имени Г.В. Плеханова»**

**Московский приборостроительный техникум**

**Лабораторная работа №6**

по учебной практике

УП.01.02 Средства мониторинга и анализа в локальных сетях

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*индекс по УП и наименование практики*

Профессионального модуля ПМ.01«Выполнение работ по проектированию

сетевой инфраструктуры»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*индекс по УП и наименование профессионального модуля*

Специальность 09.02.06 Сетевое и системное администрирование

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*код и наименование специальности*

Студент Карпов Артем Владимирович

*(фамилия, имя, отчество)*

Группа СА50-1-22

Руководитель по практической подготовке от техникума

Кульчинская Нелли Андреевна

*(фамилия, имя, отчество)*

«\_\_\_\_» \_\_\_\_\_\_\_\_\_ 2024 года

1. Скачал dump и открыл

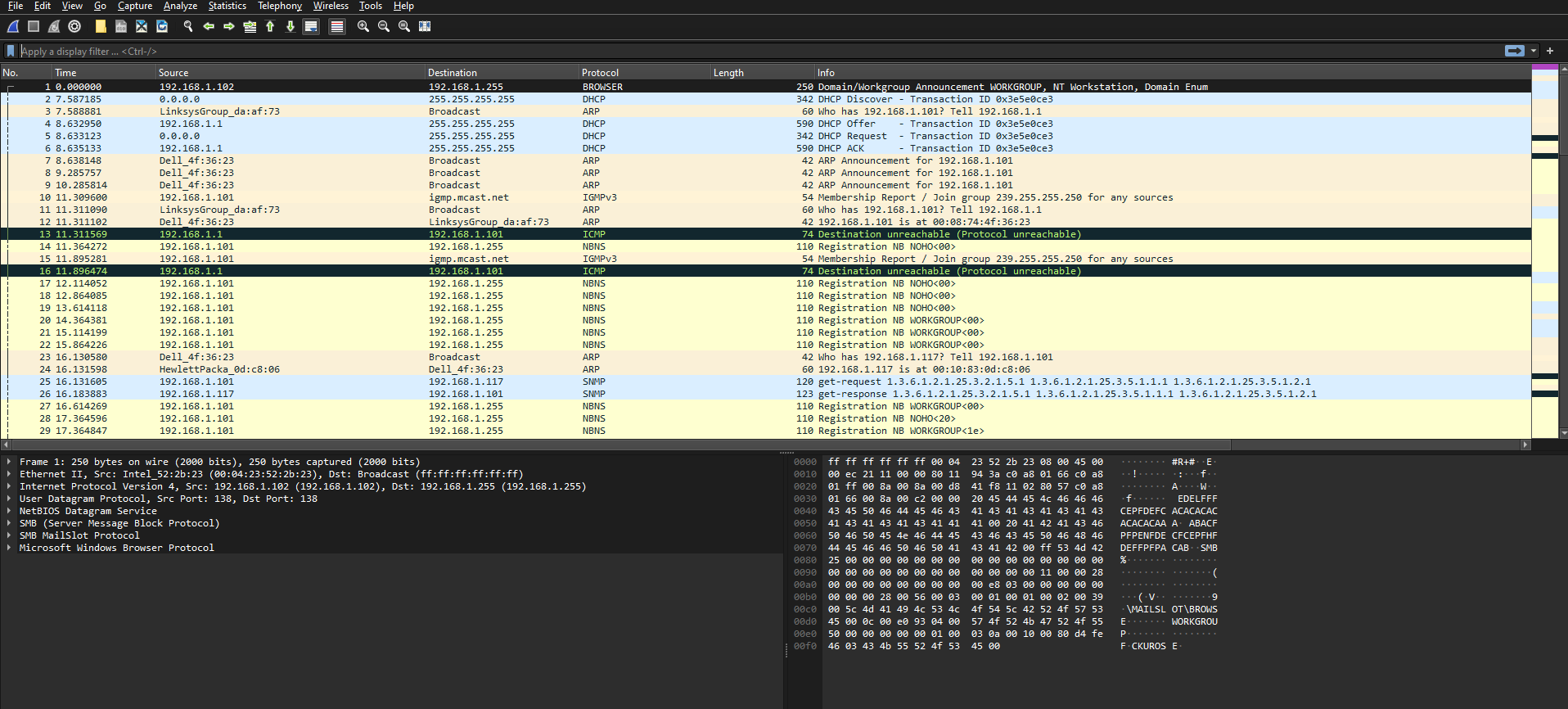


Рис. 1 – файл

1. Проведите анализ трафика протокола DHCP, **a)** определите какое устройство запрашивает IP адрес, **b)** определите тип операционной системы устройства. **c)** Найдите в дампе какая дейтаграмма соответствует поиску сервера, найдите в этом сегменте поле option (55), перечислети какую информацию запрашивает клиент. **d)** Обратите внимание есть ли у клиента IP адрес? **e)** На какой IP адрес исходит запрос? **f)** Обратите внимание на MAC адрес есть ли у клиента MAC адрес? **g)** На какой MAC адрес исходит запрос? **h)** Что это за MAC адрес и IP адрес такие (как назвываються)?

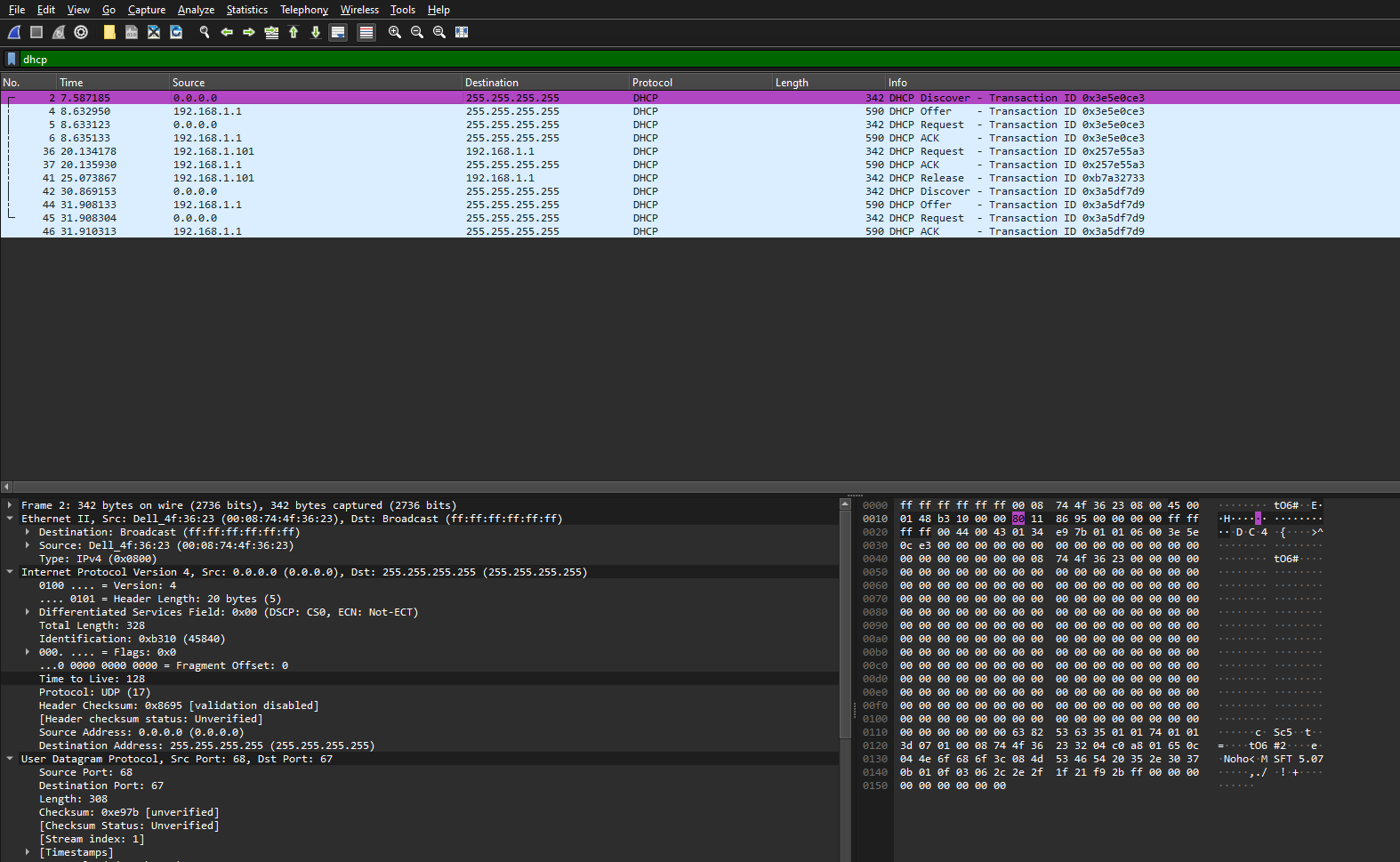
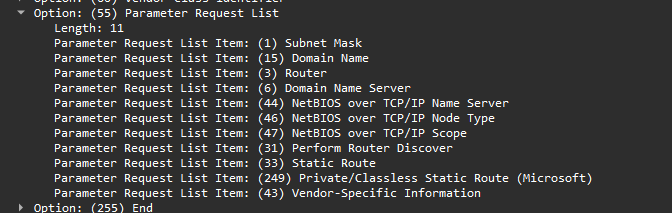


Рис. 2 – dump трафика

1. Ip адрес запрашивает компьютер
2. Тип ОС windows
3. Что запрашивает PC

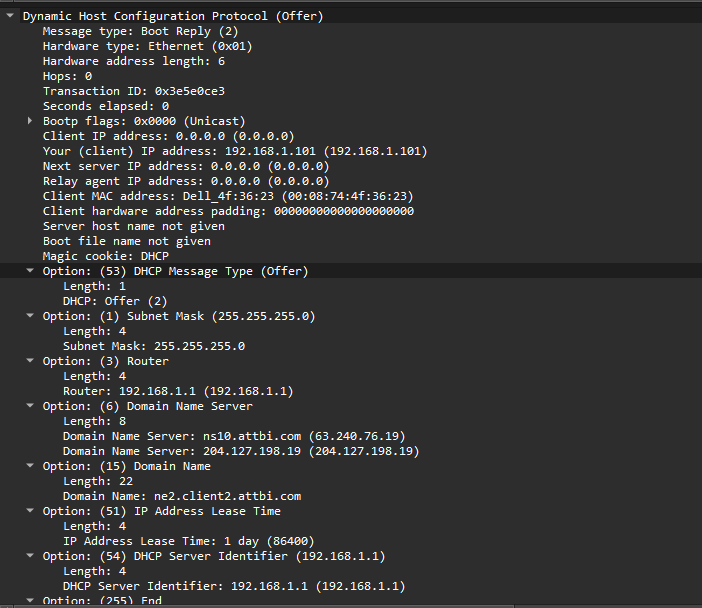


1. IP адреса у клиента пока нету, поэтому в роле него выступает 0.0.0.0
2. Запрос происходит на все устройства в сети: 255.255.255.255
3. У клиента есть MAC-адрес так как он является физическим: 00:08:74:4f:36:23
4. Запрос происходит широковещательным сообщением broadcast ff:ff:ff:ff:ff:ff
5. broadcast – шировешательное сообщение ff:ff:ff:ff:ff:ff

ip – исходный ip адрес 0.0.0.0

1. **a)** Найдите дейтаграмму в которой сервер предлагает сетевую настройки клиенту. **b)** Какой IP адрес сервер предлагает клиенту? **c)** Какую маску? **d)** В качестве шлюза сервер какой IP адрес предлагает клиенту? **e)** Какие параметры DNS сервера предлагает клиенту? **f)** Найдите информацию про dhcp option 15, какое значение оно имеет в данном пакете? **g)** Какое время аренды предлагает сервер в конфигурации? **h)** Кто являеться DHCP сервером в сети?

a)



b) Сервер предлагает клиенту адрес IPv4: 192.168.1.101

c) Предлагает маску: 255.255.255.0 (24)

d) В качестве шлюза он предлагает: 192.168.1.1

e) В качестве DNS выступают 2 адреса: 63.240.76.19, 204.127.198.19

Domain-name: ne2.client2.attbi.com

f) Имеет значение 22



g) Время аренды 1 день



1. DHCP сервером является роутер
2. Нашел дейтаграмму в dump соответствующую запросу клиента

DHCPREQUEST — Это сообщение используется как для получения IP-адреса, так и для продления его аренды.

Ip адреса у клиента еще нет, в роли него пока выступает 0.0.0.0

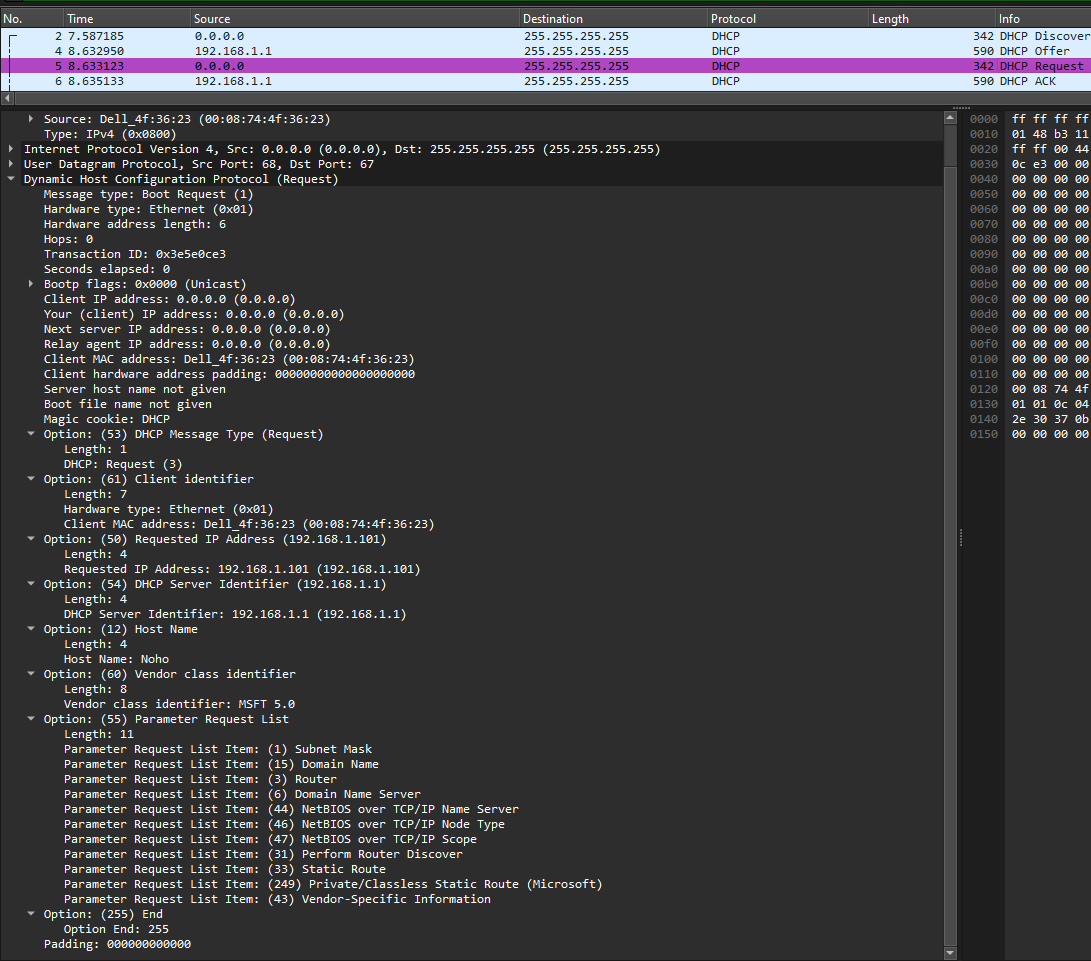


Рис. 3 – дейтограмма, соответствующая запросу

1. Нашел дейтаграмму, соответствующую подтверждению

DHCPACK - Когда клиент получает сообщение DHCPACK, он регистрирует информацию и выполняет поиск ARP для назначенного адреса. Если ответа на ARP нет, клиент знает, что адрес IPv4 действителен и начинает использовать его как свой собственный.

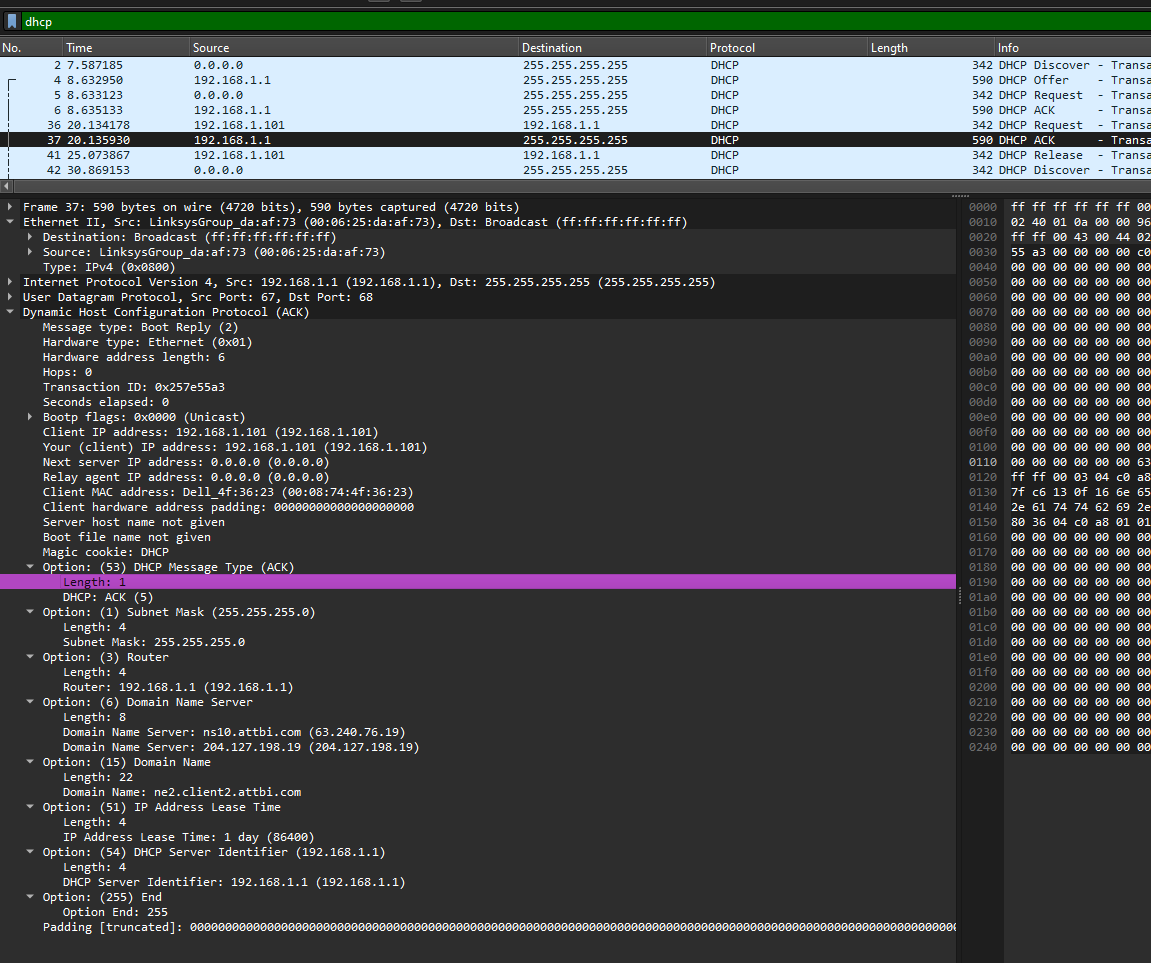


Рис. 4 - DHCPACK

1. DHCP Release:

Назначение: DHCP release - это процесс, с помощью которого клиент освобождает IP-адрес, который был ему назначен DHCP-сервером. Это может произойти при выключении клиента или когда пользователь вручную освобождает IP-адрес (например, с помощью команды в операционной системе).

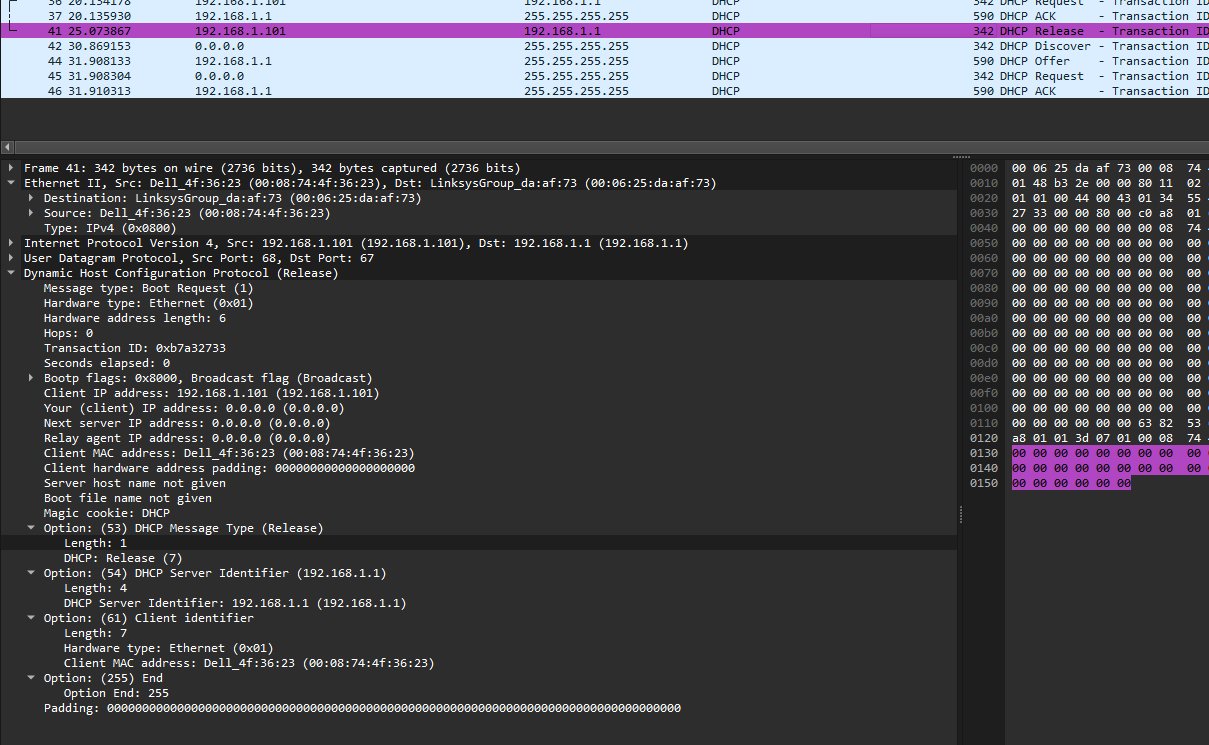


Рис. 5 – DHCP-relese

Контрольные вопросы:

1. Протокол DHCP (Dynamic Host Configuration Protocol):

- Краткое определение: DHCP – это сетевой протокол, который используется для автоматического назначения IP-адресов устройствам в сети, а также для настройки других сетевых параметров, таких как маска подсети, шлюз по умолчанию и DNS-серверы. Это упрощает процесс конфигурации сетевых устройств и помогает администраторам сети управлять назначением IP-адресов без необходимости вручную настраивать каждое устройство.

- DORA – это аббревиатура, обозначающая четыре основные стадии взаимодействия между клиентом и сервером в процессе назначения IP-адреса:

- Discover - Открытие. Клиент посылает широковещательный запрос (DHCP Discover) для поиска доступных DHCP-серверов.

- Offer - Предложение. DHCP-серверы отвечают на запрос клиента, посылая предложение (DHCP Offer), которое содержит IP-адрес, предлагаемый клиенту, и другие параметры конфигурации.

- Request - Запрос. Клиент выбирает одно из предложений и отправляет запрос (DHCP Request) на сервер, указывая, что он принимает предложенный IP-адрес (и, возможно, другие параметры).

- Acknowledge - Подтверждение. Сервер подтверждает запрос (DHCP Acknowledge) и окончательно назначает IP-адрес клиенту. После этого клиент может использовать назначенный IP-адрес для связи в сети.

Каждая из этих дейтаграмм выполняет уникальную роль в процессе автоматического назначения IP-адреса, обеспечивая гладкое взаимодействие между клиентом и сервером.

2. APIPA (Automatic Private IP Addressing):

- Определение: APIPA – это механизм, используемый операционными системами Windows для автоматического назначения себе частного IP-адреса из диапазона 169.254.0.1 до 169.254.255.254, когда DHCP-сервер недоступен и не может назначить IP-адрес. Это позволяет устройствам в локальной сети общаться друг с другом, даже если они не могут получить конфигурацию от DHCP-сервера.

- Как работает: Если при включении устройства DHCP-сервер не отвечает на запросы Discover, операционная система автоматически присваивает себе IP-адрес из указанного диапазона APIPA. Это обеспечивает базовую сетевую функциональность и позволяет устройствам находить друг друга и обмениваться данными в пределах одного сегмента сети, но не позволяет им получить доступ к внешним сетям или Интернету, так как для этого требуется шлюз, который обычно назначается DHCP-сервером.