МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

Кафедра вычислительные системы и технологии

Отчет

по лабораторной работе № 2

по дисциплине

Сети и телекоммуникации

«Изучение протокола ARP. Получение навыков работы с генераторами пакетов.

Вычисление контрольной суммы в IP-пакетах»

РУКОВОДИТЕЛЬ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Гай В.Е. (подпись) (фамилия, и.,о.)

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Меженин М.Д.

(подпись) (фамилия, и.,о.)

17-АС

(шифр группы)

Работа защищена «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_

С оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Нижний Новгород, 2020

**Цель**:

* Получить практические навыки в составлении кадра для широковещательной передачи ARP-запроса хостом А и кадра ARP-ответа хостом В хосту А. Получение базовых навыков по работе с генераторами пакетов PackETH.
* Получить практические навыки в вычислении контрольной суммы заголовка IP-пакета.

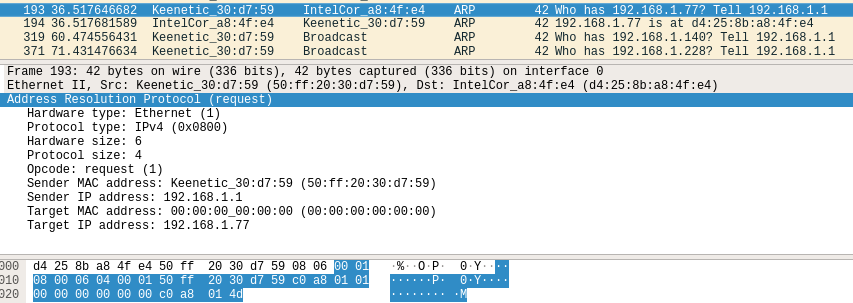
**Ход работы**

**Часть 1**

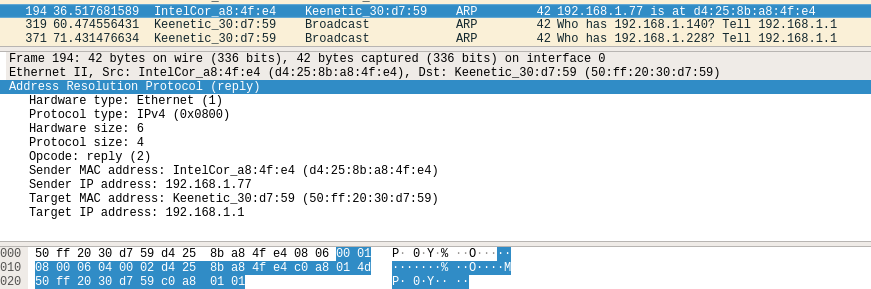
1. Подготовить и записать в 16-теричном виде пример кадра для широковещательной передачи ARP-запроса хостом А и кадра ARP-ответа хостом В хосту А. В кадре ARPответа поля для МАС-адреса хоста В не заполнять. (Хост А - это ПК, за которым работает бригада студентов. IP-адрес хоста В выбирается студентом по схеме ЛВС лаб.521). IP-адрес хоста A можно узнать с помощью команд ifconfig и ip addr show.

**Кадр широковещательной передачи ARP-запроса хостом A хосту B**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | | | 2 | | | | 3 | | 4 | | | 5 | | | 6 | | | 7 | 8 | | 9 | 10 | 11 | | 12 | 13 | 14 | 15 | 16 |
| Destination MAC | | | | | | | | | | | | | | | | | | Source MAC | | | | | | | | ETHER TYPE | | HTYPE | |
| ff | | ff | | | | ff | | | | ff | | ff | | | | ff | | 50 | ff | | 20 | 30 | d7 | | 59 | 08 | 06 | 00 | 01 |
| PTYPE | | | | HLEN | | | | | | PLEN | | | OP CODE | | | | | Source MAC | | | | | | | | Source IP | | | |
| 08 | 00 | | | 06 | | | | | | 04 | | | 00 | | | | 01 | 50 | ff | | 20 | 30 | d7 | | 59 | c0 | a8 | 01 | 01 |
| Destination MAC | | | | | | | | | | | | | | | | | | Destination IP | | | | | | | |  |  |  |  |
| 00 | 00 | | | | 00 | | | 00 | | | 00 | | | 00 | | | | c0 | | a8 | | 01 | | 4d | |  |  |  |  |

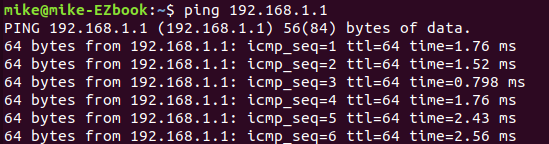


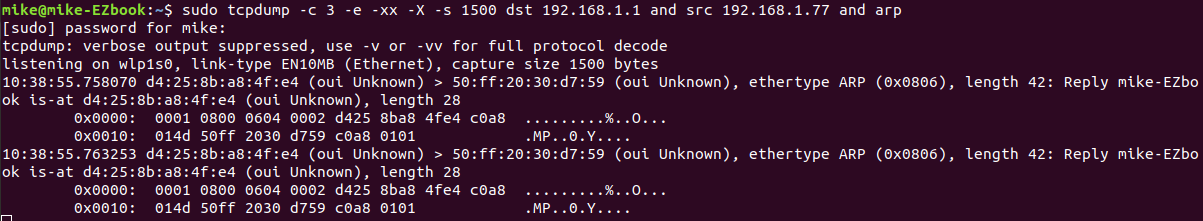
**Кадр широковещательной передачи ARP-ответа хостом B хосту A**



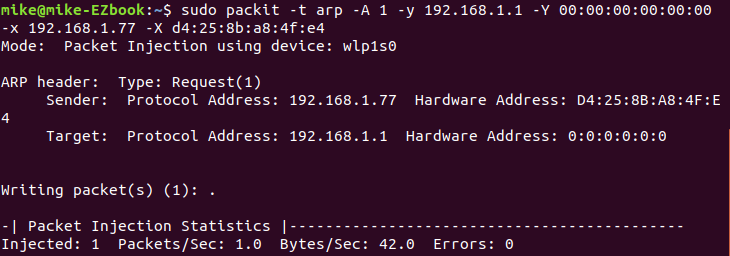
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | | | 2 | | | | 3 | | 4 | | | 5 | | | 6 | | | 7 | 8 | | 9 | 10 | 11 | | 12 | 13 | 14 | 15 | 16 |
| Destination MAC | | | | | | | | | | | | | | | | | | Source MAC | | | | | | | | ETHER TYPE | | HTYPE | |
| 50 | | ff | | | | 20 | | | | 30 | | d7 | | | | 59 | |  |  | |  |  |  | |  | 08 | 06 | 00 | 01 |
| PTYPE | | | | HLEN | | | | | | PLEN | | | OP CODE | | | | | Source MAC | | | | | | | | Source IP | | | |
| 08 | 00 | | | 06 | | | | | | 04 | | | 00 | | | | 02 |  |  | |  |  |  | |  | c0 | a8 | 01 | 4d |
| Destination MAC | | | | | | | | | | | | | | | | | | Destination IP | | | | | | | |  |  |  |  |
| 50 | ff | | | | 20 | | | 30 | | | d7 | | | 59 | | | | c0 | | a8 | | 01 | | 01 | |  |  |  |  |

1. Начать захват пакетов при помощи любого из изученных анализаторов протоколов. Захват проводить по фильтру (IP-адреса источника и получателя, протокол ARP; для tcpdump дополнительно указать размер пакета 1500 байт, а также флаг отображения пакета (включая заголовок кадра Ethernet) в 16-теричном и ASCII виде).

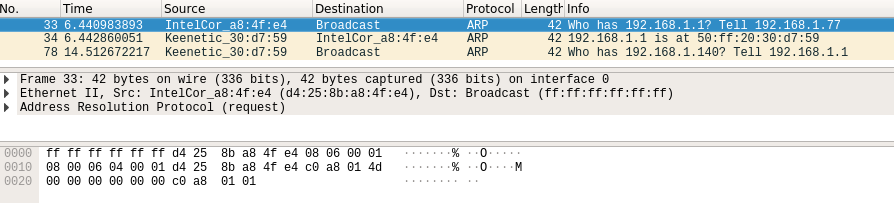




1. Сформировать кадр ARP-запроса с помощью утилиты packit и отправить его в сеть. Команду сохранить для отчета.



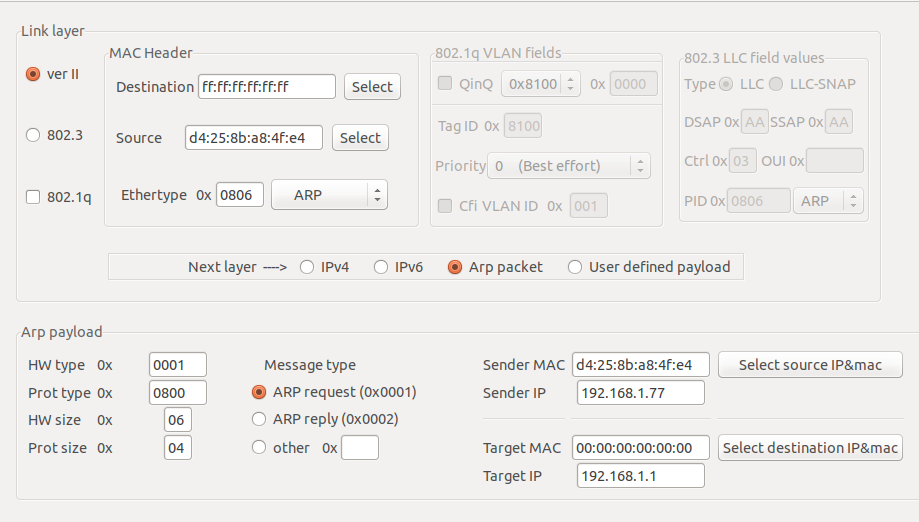
1. Убедиться, что был получен кадр ARP-ответа, соответствующий посланному запросу. Захваченные пакеты сохранить для отчета.



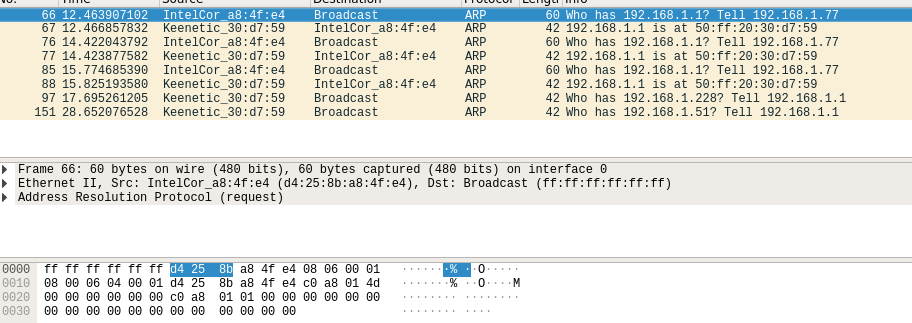
1. Сравнить полученный ARP-ответ с подготовленным в первом пункте примером.

Полученный ARP-ответ совпадает с ARP-ответом из 1 пункта.

1. Сформировать кадр ARP-запроса с помощью утилиты PackETH и отправить его в сеть.



Убедиться, что был получен кадр ARP-ответа, соответствующий посланному запросу. Захваченные пакеты сохранить для отчета.



1. Сравнить полученный ARP-ответ с подготовленным в первом пункте примером.

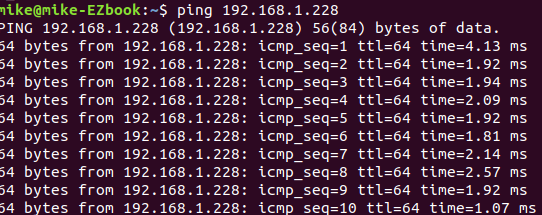
Полученный ARP-ответ совпадает с ARP-ответом из 1 пункта.

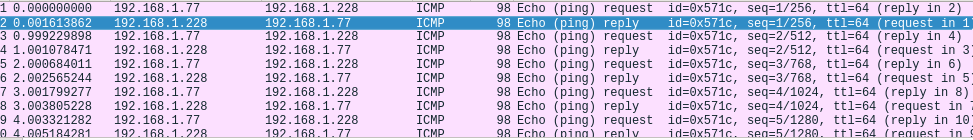
**Часть 2**

**Ход работы:**

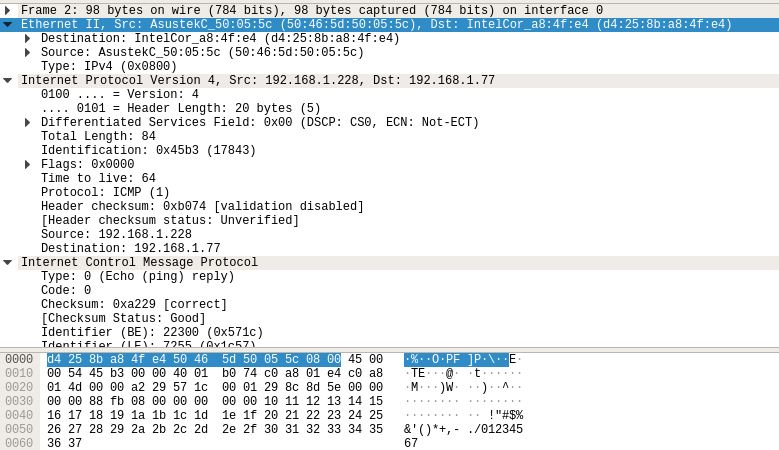
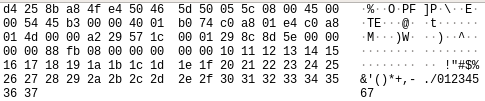
1) IP

Произведем отправку пакетов:

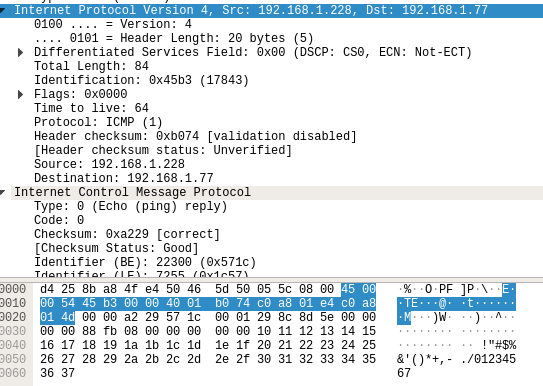


Анализируем второй пакет

Первые 14 байтов отведены под следующие значения:



Далее идёт непосредственно заголовок пакета, и мы можем наблюдать:



4 – версия; IPv4

5 – IHL (InternetHeaderLength); длина IP-заголовка, 5 блоков длиной 4 байта каждый

0054 – длина пакета (Total Length); 60 октетов, включая заголовок и данные

45b3 - идентификатор (Identification) пакета; значение, назначаемое отправителем пакета и предназначенное для определения корректной последовательности фрагментов при сборке пакета

0000 – смещение фрагмента (Fragmentoffset); определяет позицию фрагмента в потоке данных, количество восьмибайтовых блоков

40 – время жизни (Timetolive); число маршрутизаторов, которые может пройти этот пакет

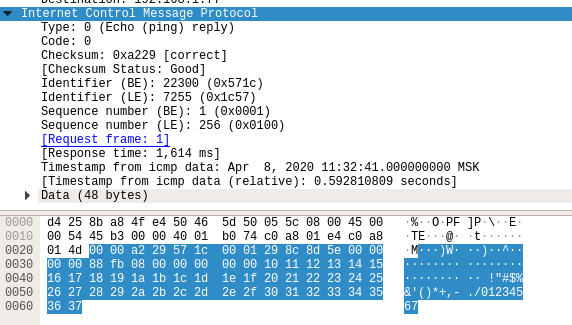
01 – протокол (Protocol); идентификатор, который указывает, данные какого протокола содержит пакет, 1- ICMP

b0 44 - контрольная сумма заголовка (Header Checksum)

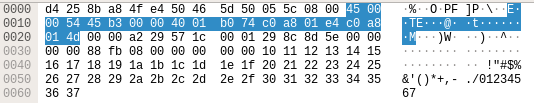
c0a8b1e4 – адрес отправителя (Source); 192.168.1.228

c0a8014d – адрес получателя (Destination); 192.168.1.77

Последующие байты – это поле данных.



Для вычисления контрольной суммы необходимо просуммировать все двухбайтовые слова из заголовка без учёта значения контрольной суммы.



4500 + 0054 + 45b3 + 0000 + 4001 + b074 + c0a8 + 01e4 + c0a8 + 014d = 2FFFD

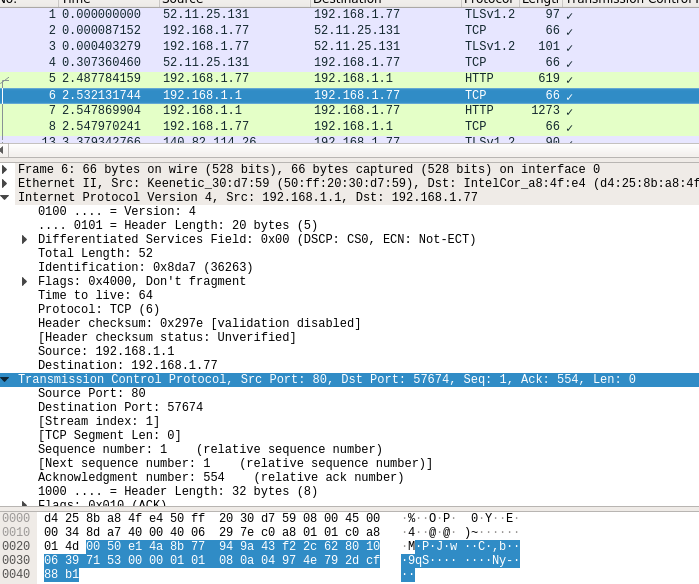
Переводим полученное число в двоичную систему счисления и побитово инвертируем его:

2FFFD16= 001011111111111111012

0010. 1111. 1111. 1111. 1101. = 1101. 0000. 0000. 0000. 0010.

1101. 0000. 0000. 0000. 0010. = D0002

2) TCP



Src IP: c0 a8 01 01  
Dst IP: c0 a8 01 4d  
Zero: 00 (const)  
Proto: 06   
TCP\_Len: 0042

TCP\_Len скадывается из: длина TCP Header, длина доп. опций, длина полезных данных.

Считаем сумму псевдозаголовка

C0A8 + 0101 + с0a8 + 014d+ 0000 + 0600 + 0042 = 189e0

Считаем сумму TCP-заголовка с зануленной суммой

0050 + e14a + 8b77 + 949a + 43f2 + 2c62 + 8010 + 0639 + 7153 + 0000 + 0101 + 080a + 0497 + 4e79 + 2dcf + 88b1 = 47C36

47C36 + 189e0 = 60616

0006 + 0616 = 061с

Находим двоичное поразрядное дополнение:

061с = 0000 0110 0001 1100

**CSTCP =** F9E3

**Выводы**

В ходе лабораторной работы были получены практические навыки в составлении кадра для широковещательной передачи ARP-запроса хостом А и кадра ARP-ответа хостом В хосту А, получены базовые навыки по работе с генераторами пакетов PackETH и packit, получены практические навыки в вычислении контрольных суммы заголовка IP-пакета и TCP сегмента.