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»

ОТЧЁТ

По лабораторной работе №2

по дисциплине «Сети и Телекоммуникации»

Вариант 4

«Работа с утилитами ping, traceroute.

Работа с анализаторами протоколов tcpdump и wireshark»

ПРОВЕРИЛ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Гай В.Е.

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Зайкин А.М.

17-В-1

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

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

Нижний Новгород

2020

**Цель работы:**

**1.** 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 генератором пакетов PackETН.

**2.** Изучить структуру IP-пакета, TCP-сегмента и UDP-датаграммы. Получить практические навыки в вычислении контрольной суммы заголовка IP-пакета.

**Порядок выполнения лабораторной работы:**

**Часть 1.**

**ARP** — протокол в компьютерных сетях, предназначенный для определения MAC-адреса по IP-адресу другого компьютера. Необходимо составить кадр для широковещательного запроса хостом А и кадр ARP-ответа хостом В хосту А.

Хост А (отправитель) – ноутбук, с адресом IP=198.168.0.101 и MAC= B0:35:9F:9E:F5:D9

Хост B (приемник) – смартфон с адресом IP=198.168.0.100 и MAC= A8:3E:0E:4B:B3:81

ETHERTYPE в сети Ethernet= 08 06

HTYPE — код протокола передачи данных. Для Ethernet = 00 01

PTYPE — код сетевого протокола. Для IPv4 = 08 00

HLEN — длина физического адреса в байтах = 06

PLEN — длина логического адреса в байтах = 04

OPCODE — код операции отправителя. Для запроса 00 01

Зная все данные, мы можем составить ARP-запрос.

**Запрос**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | B0 | 35 | 9F | 9E | F5 | D9 | 08 | 06 | 00 | 01 |
| PTYPE | | HLEN | PLEN | OP CODE | | Source MAC | | | | | | Source IP | | | |
| 08 | 00 | 06 | 04 | 00 | 01 | B0 | 35 | 9F | 9E | F5 | D9 | C0 | A8 | 00 | 65 |
| Destination MAC | | | | | | Destination IP | | | |  | | | | | |
| 00 | 00 | 00 | 00 | 00 | 00 | C0 | A8 | 00 | 64 |

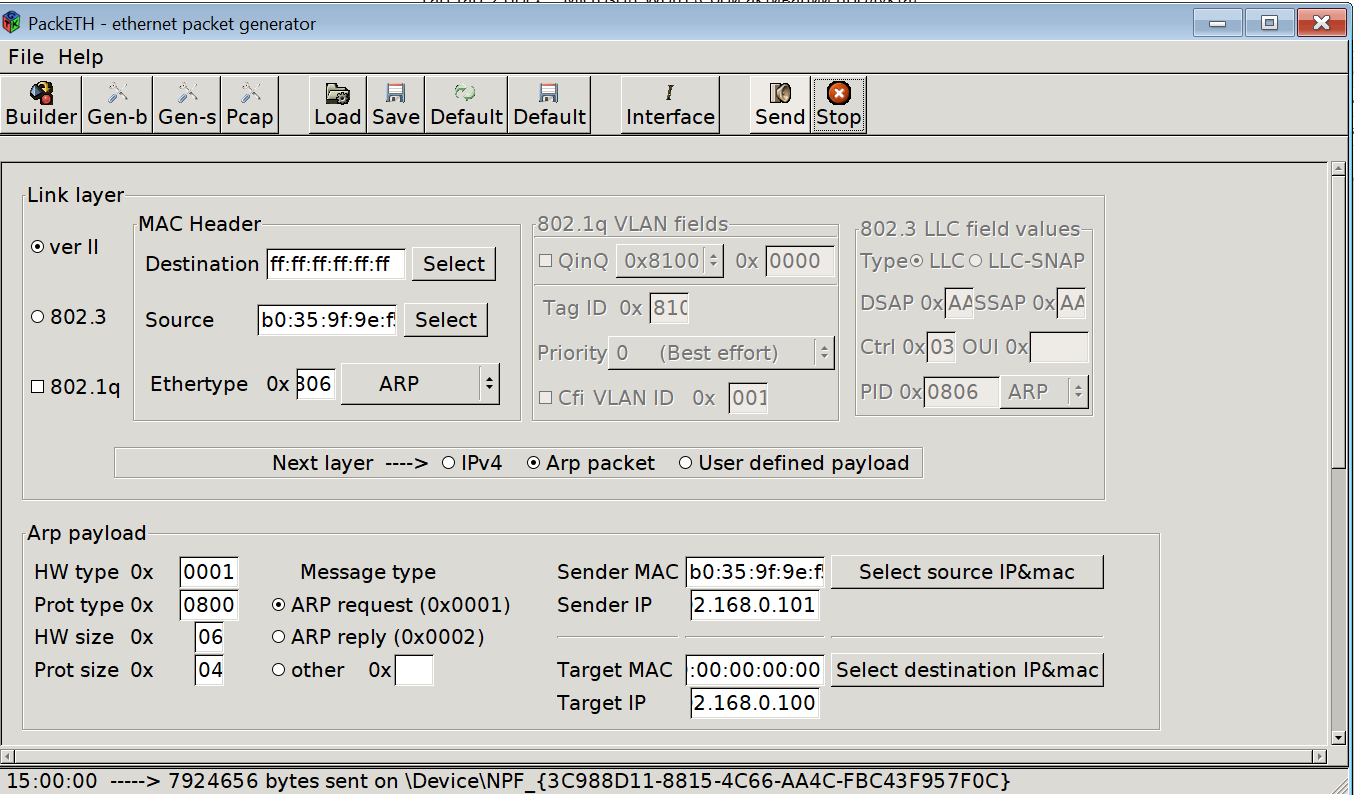
**Ответ**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| Destination MAC | | | | | | Source MAC | | | | | | ETHER TYPE | | HTYPE | |
| B0 | 35 | 9F | 9E | F5 | D9 | A8 | 3E | 0E | 4B | B3 | 81 | 08 | 06 | 00 | 01 |
| PTYPE | | HLEN | PLEN | OP CODE | | Source MAC | | | | | | Source IP | | | |
| 08 | 00 | 06 | 04 | 00 | 02 | A8 | 3E | 0E | 4B | B3 | 81 | C8 | A8 | 00 | 64 |
| Destination MAC | | | | | | Destination IP | | | |  | | | | | |
| B0 | 35 | 9F | 9E | F5 | D9 | C0 | A8 | 00 | 65 |

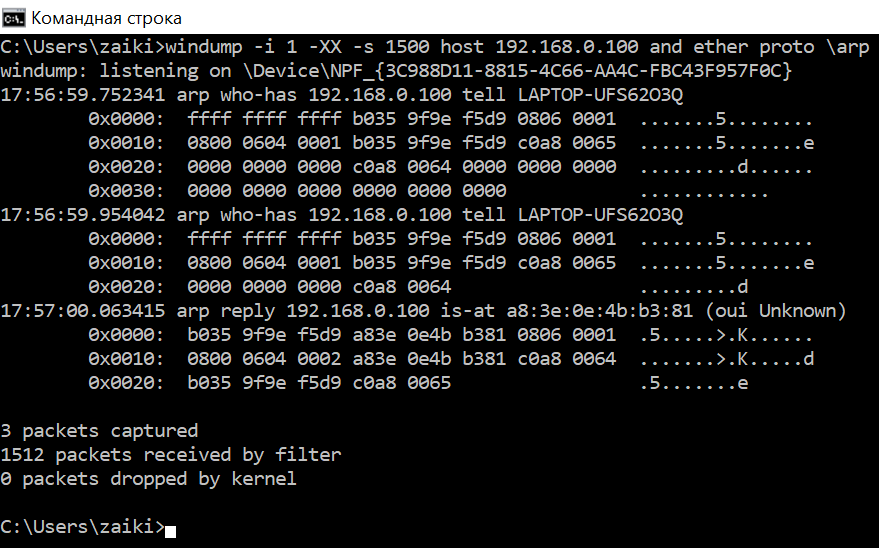
Начинаем захват пакетов при помощи windump

windump -i 1 -XX -s 1500 host 192.168.0.100 and ether proto \arp

Формирование кадра ARP-запроса с помощью утилиты PackETH и отправка его в сеть.



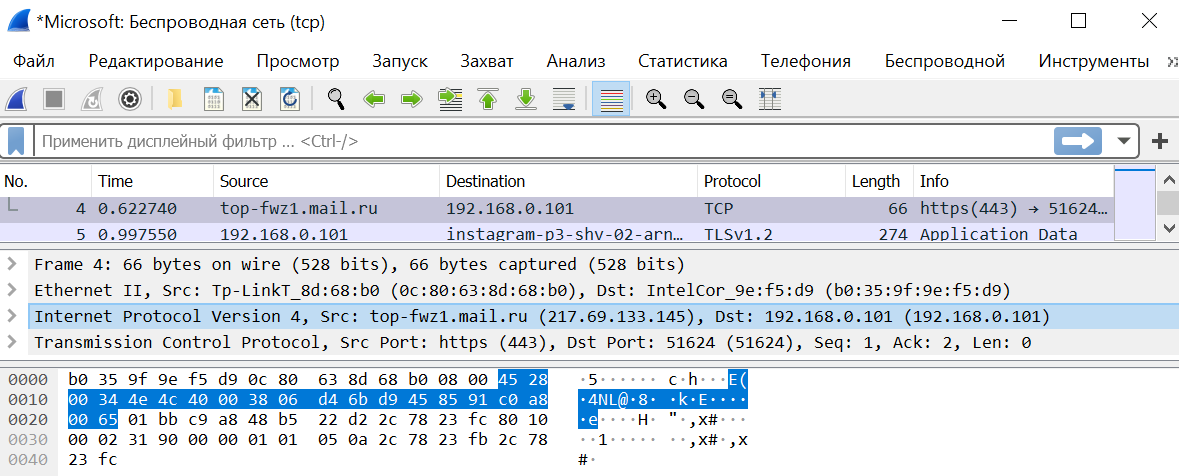
Получен кадр ARP-ответа, соответствующий посланному запросу.



Как видно из перехваченных пакетов, кадры ARP совпадают с подготовленным примером.

**Часть 2.**

Перехватим с помощью программы WireShark несколько пакетов, используя фильтр TCP, и выберем один случайный. Разобьем кадр на поля:

****

**Разбор TCP-пакета:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| Заголовок Ethernet кадра | | | | | | | | | | | | | | IP | |
| Destination MAC | | | | | | Source MAC | | | | | | ETHER TYPE  =Ethernet | | V=4  HL=5 | Type of Ser. |
| B0 | 35 | 9F | 9E | F5 | D9 | 0C | 80 | 63 | 8D | 68 | B0 | 08 | 00 | 45 | 28 |
| IP | | | | | | | | | | | | | | | |
| Total Length | | ID | | Flags=dont fragment | | TTL | Prot=TCP | Header  checksum | | Source IP | | | | Destination IP | |
| 00 | 34 | 4E | 4C | 40 | 00 | 38 | 06 | D4 | 6B | D9 | 45 | 85 | 91 | C0 | A8 |
| IP | | TCP | | | | | | | | | | | | | |
| Destination IP | | Source port | | Destination port | | Sequence number | | | | Aknowledgement number | | | | Hlength (4 bit)+Flags (12 bit) | |
| 00 | 65 | 01 | BB | C9 | A8 | 48 | B5 | 22 | D2 | 2C | 78 | 23 | FC | 80 | 10 |
| TCP | | | | | | | | | | | | | | | |
| Window size | | Checksum | | Urgent point | | Options ( 1b NOP +1b NOP+ 10b Timestamps | | | | | | | | | |
| 00 | 02 | 31 | 90 | 00 | 00 | 01 | 01 | 05 | 0A | 2C | 78 | 23 | FB | 2C | 78 |
| TCP | |  | | | | | | | | | | | | | |
|  | |
| 23 | FC |  | | | | | | | | | | | | | |

**Рассчет контрольной суммы заголовка IP-пакета:**

Для этого нужно сложить все слова (2 байта) в заголовке, за исключением контрольной суммы. Полученное число (если его длина будет больше 1 байта) разбить на 2 слова и сложить их. Результат перевести в двоичный код и побитово проинвертировать. В итоге должна получиться контрольная сумма заголовка TCP-сегмента.

4528 + 0034 + 4E4C + 4000 + 3806 + D46B + D945 + 8591 + C0A8 + 0065 = 3 2B91  
2B91 + 0003 = 2B94 h = 0010 1011 1001 0100 b  
! 0010 1011 1001 0100 b + 1101 0100 0110 1011b = **D46B h**

Вычисленное значение совпадает с контрольной суммой в пакете.

**Рассчет контрольной суммы TCP-сегмента:**

Для расчета TCP нужно подобным образом сложить заголовок (без поля checksum), данные и псевдозаголовок. Псевдозаголовок включает в себя данные IP: Hlength (20), Protocol (6), Source IP(D9458591) и Destination IP (C0A80065)

Заголовок:

01 BB + C9 A8 + 48 B5 + 22 D2 + 2C 78 + 23 FC + 80 10 + 00 02 + 0000 + 00 00 + 01 01 + 05 0A + 2C 78 + 23 FB + 2C 78 + 23 FC = 2 AE62

Псевдозаголовок:

D945 + 8591 + C0A8 + 0065 + 0006 + 0020 = 2 2009

Итого:

2 AE62 + 2 2009 = 4 CE6B‬  
0004 + CE6B‬ = CE6F = ! 1100 1110 0110 1111 b   
! 1100 1110 0110 1111 b = 0011 0001 1001 0000 b = **3190 h**

Вычисленное значение совпадает с контрольной суммой в пакете.

**Вывод:**В ходе выполнения 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 генератором пакетов PackETH.Так же было получено базовые представление об вычислении контрольной суммы в IP-пакетах.