МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Кафедра «Вычислительные системы и технологии»

Лабораторная работа №2

по дисциплине: «Сети и телекоммуникации»

Выполнил:

Студент группы 17-В-1

Двитовская А.Н.

Проверил:

Гай В.Е.

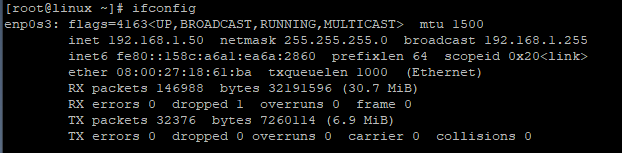
Нижний Новгород

2020 г.

Цель работы:

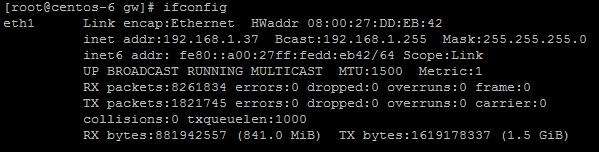
Получить практические навыки в составлении кадра для широковещательной передачи ARP-запроса хостом А и кадра ARP-ответа хостом В хосту А. Получение базовых навыков по работе с генератором пакетов PackETН. Изучить структуру IP-пакета, TCP-сегмента и UDP-датаграммы. Получить практические навыки в вычислении контрольной суммы заголовка IP-пакета.

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.



Получили адреса:

192.168.1.50 и 08:00:27:18:61:ba на машине А



Получили адреса:

192.168.1.37 и 08:00:27:DD:EB:42 на машине B

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| Destination MAC | | | | | | Source MAC | | | | | | ETHER TYPE | | HTYPE | |
| 08 | 00 | 27 | DD | EB | 42 | 08 | 00 | 27 | 18 | 61 | ba | 08 | 06 | 00 | 01 |
| PTYPE | | HLEN | PLEN | OP CODE | | Source MAC | | | | | | Source IP | | | |
| 08 | 00 | 06 | 04 | 00 | 01 | 08 | 00 | 27 | 18 | 61 | ba | C0 | A8 | 1 | 32 |
| Destination MAC | | | | | | Destination IP | | | |  | | | | | |
| 08 | 00 | 27 | DD | EB | 42 | C0 | A8 | 1 | 25 |

Начать захват пакетов при помощи любого из изученных анализаторов протоколов.

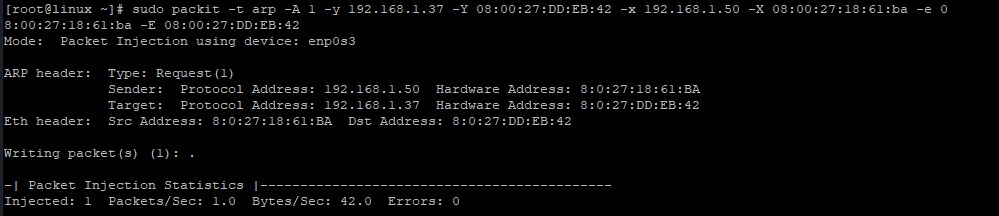
Захват проводить по фильтру (IP-адреса источника и получателя, протокол ARP; для

tcpdump дополнительно указать размер пакета 1500 байт, а также флаг отображения

пакета (включая заголовок кадра Ethernet) в 16-теричном и ASCII виде):

tcpdump -XX arp 'host 192.168.1.50 or host 192.168.1.37 and less 1500'

Сгенерируем ARP-запрос с помощью packit.



Где:

-t — тип пакета, -A — код операции (1 для запроса, 2 для ответа)

-y — логический адрес приемника, -Y — физический адрес приемника

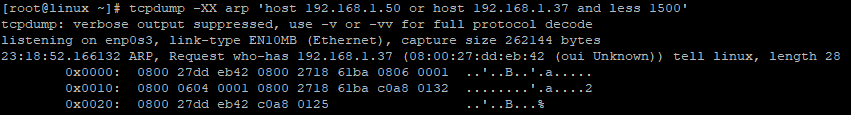
-x — логический адрес отправителя, -X — физический адрес отправителя

-e — адрес отправителя для ethernet, -E — адрес приемника для ethernet

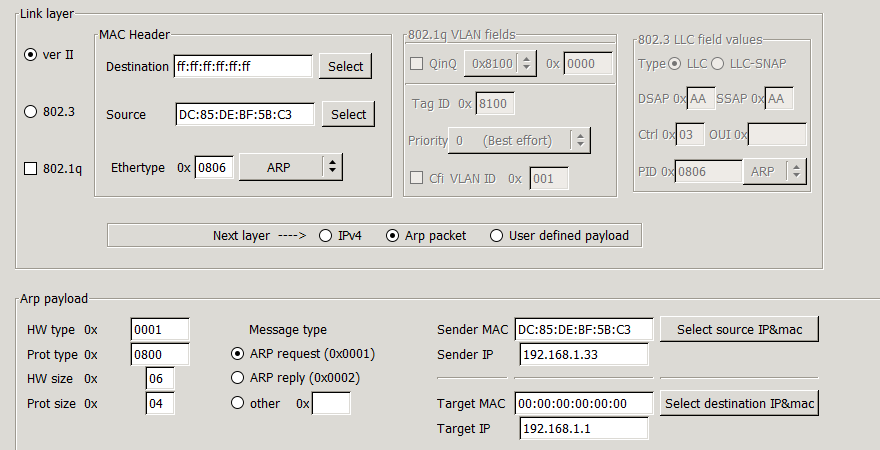
Теоретически составленный ответ (приемник и отправитель поменялись местами, OPCODE стал равен 00 02):

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| Destination MAC | | | | | | Source MAC | | | | | | ETHER TYPE | | HTYPE | |
| 08 | 00 | 27 | 18 | 61 | ba | 08 | 00 | 27 | DD | EB | 42 | 08 | 06 | 00 | 01 |
| PTYPE | | HLEN | PLEN | OP CODE | | Source MAC | | | | | | Source IP | | | |
| 08 | 00 | 06 | 04 | 00 | 02 | 08 | 00 | 27 | DD | EB | 42 | C0 | A8 | 1 | 25 |
| Destination MAC | | | | | | Destination IP | | | |  | | | | | |
| 08 | 00 | 27 | 18 | 61 | ba | C0 | A8 | 1 | 32 |

Был получен кадр пакета, соответствующий теоретическому примеру:



Кадр ARP-запроса с помощью утилиты PackETH:

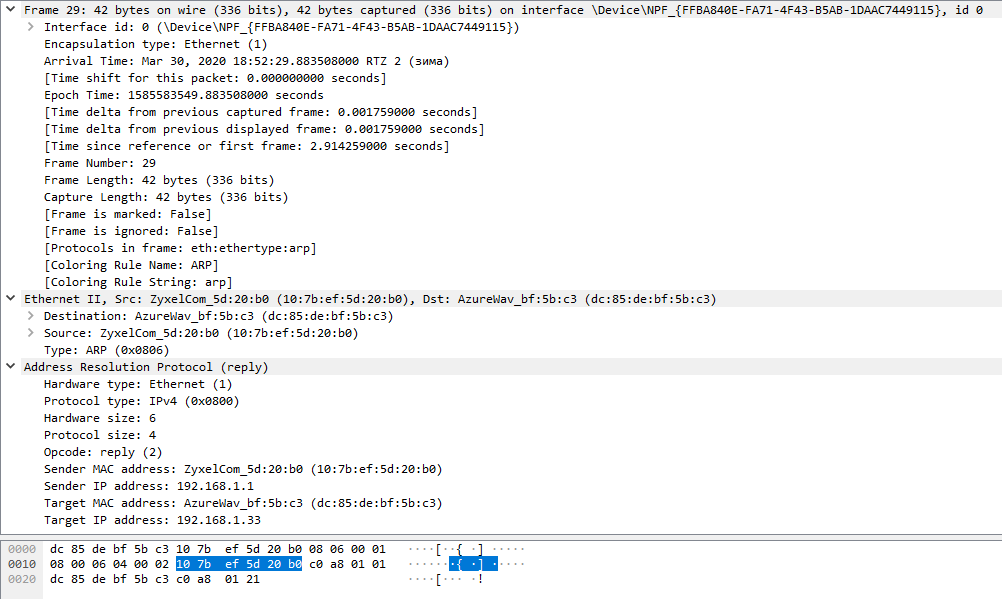


С помощью программ PackETH и Wireshark узнать МАС-адрес второго компьютера. Для этого загружаем программу PackETH и выставляем соответствующие параметры:

* Destination: ff:ff:ff:ff:ff:ff – для того, чтобы узнать МАС-адрес компьютера-получателя;
* Source – MAC-адрес компьютера-отправителя;
* Sender MAC - MAC-адрес компьютера-отправителя;
* Sender IP – IP компьютера-отправителя;
* Target MAC: 00:00:00:00:00:00 - для того, чтобы узнать МАС-адрес компьютера-получателя;
* Target IP - IP компьютера-получателя;
* необходимо выбрать Interface, иначе – ошибка при отправке.

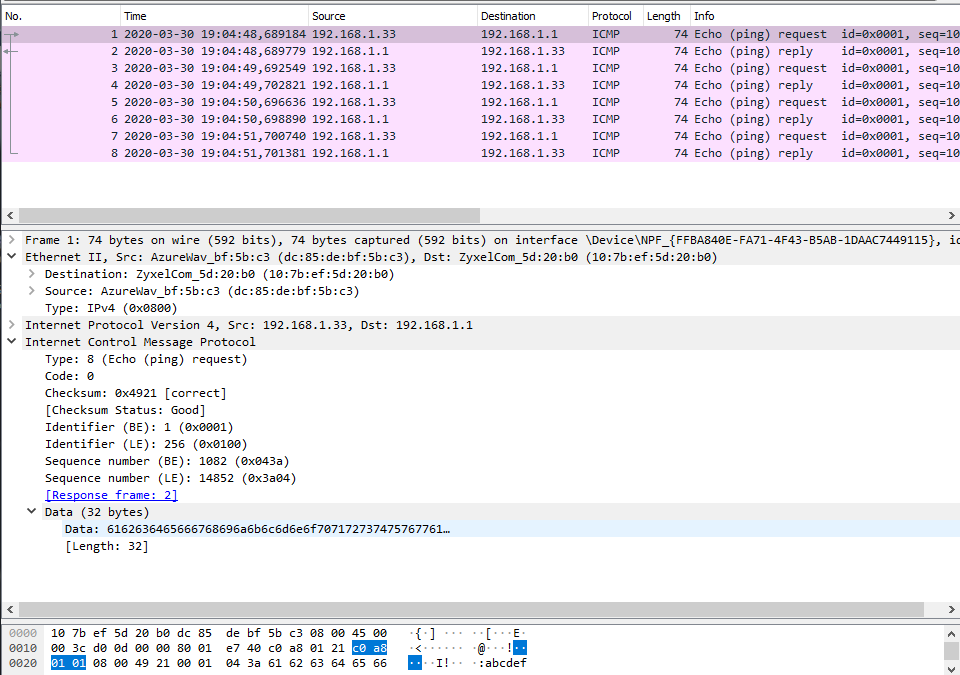
Открыв Wireshark можем наблюдать результат:

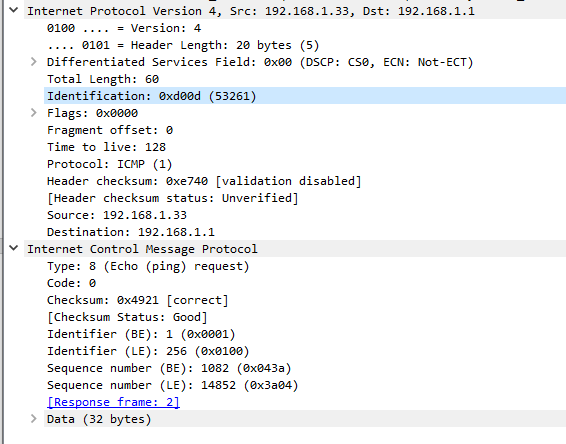




Часть 2.

В программе WireShark выставляем фильтр icmp. Воспользовавшись утилитой ping наблюдаем результат успешной отправки и получения пакетов:





4 – версия; IPv4

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

0x003С – длина пакета (Total Length); 60 октетов, включая заголовок и данные

0xd00d - идентификатор (Identification) пакета; значение, назначаемое отправителем пакета и предназначенное для определения корректной последовательности фрагментов при сборке пакета

0x0000 – смещение фрагмента (Fragment offset); определяет позицию фрагмента в потоке данных, количество восьмибайтовых блоков

0x80 – время жизни (Time to live); число маршрутизаторов, которые может пройти этот пакет, 128

0x01 – протокол (Protocol); идентификатор, который указывает, данные какого протокола содержит пакет, 1- ICMP

0xe740 - контрольная сумма заголовка (Header Checksum)

C0A80121 – адрес отправителя (Source); 192.168.1.33

C0A80101 – адрес получателя (Destination); 192.168.1.1

Для расчета контрольной суммы IP нужно сложить все слова (2 байта) в заголовке, за исключением контрольной суммы. Полученное число разбить на 2 слова и сложить их. Полученное число перевести в двоичный код и побитово проинвертировать. Полученное число в шестнадцатиричной записи — и есть контрольная сумма заголовка TCP-сегмента.

4500 + 003C + d00d + 0000 + 8001 + C0A8 + 0121 + C0A8 + 0101 = 318BC

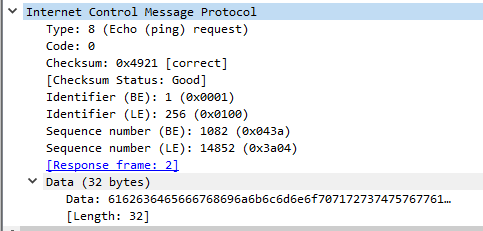
0x3+0x18BC = 18BF = 0001 1000 1011 1111

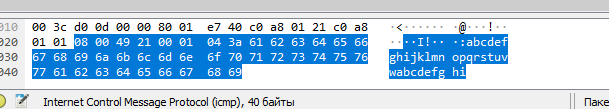
1110 0111 0100 0000 = 0xE740

0x3FFFC‬ = 0011 1111 1111 1111 1100

1100 0000 0000 0000 0011 = C 0003

Для расчета контрольной суммы ICMP сегмента нужно подобным образом сложить заголовок (без поля checksum) и данные.





0800+0001+043a+6162+6364+6566+6768+696a+6b6c+6d6e+6f70+7172+7374+7576+7761+6263+6465+6667+6869 = 0x6B6D8

0x6+0xB6D8 = 0xB6DE = 1011 0110 1101 1110

Инвертируем

0100 1001 0010 0001 = 0x4921

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. Также были получены базовые навыки по работе с генератором пакетов packit и были получены базовые представления об вычислении контрольной суммы в IP-пакетах.