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:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Хрусталева М. О.

(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 | | 64 | 5a | | 04 | 93 | 55 | | 0e | 08 | 06 | 00 | 01 |
| PTYPE | | | | HLEN | | | | | | PLEN | | | OP CODE | | | | | Source MAC | | | | | | | | Source IP | | | |
| 08 | 00 | | | 06 | | | | | | 04 | | | 00 | | | | 01 | 64 | 5a | | 04 | 93 | 55 | | 0e | c0 | a8 | 58 | 0a |
| Destination MAC | | | | | | | | | | | | | | | | | | Destination IP | | | | | | | |
| 00 | 00 | | | | 00 | | | 00 | | | 00 | | | 00 | | | | c0 | | a8 | | 58 | | 0d | |

|  |
| --- |
| https://sun9-3.userapi.com/c854320/v854320767/212864/zn1dMAJK3kw.jpg |

**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 | |
| 64 | | 5a | | | | 04 | | | | 93 | | 55 | | | | 0e | |  |  | |  |  |  | |  | 08 | 06 | 00 | 01 |
| PTYPE | | | | HLEN | | | | | | PLEN | | | OP CODE | | | | | Source MAC | | | | | | | | Source IP | | | |
| 08 | 00 | | | 06 | | | | | | 04 | | | 00 | | | | 02 |  |  | |  |  |  | |  | c0 | a8 | 58 | 0d |
| Destination MAC | | | | | | | | | | | | | | | | | | Destination IP | | | | | | | |
| 64 | 5a | | | | 04 | | | 93 | | | 55 | | | 0e | | | | c0 | | a8 | | 58 | | 0a | |

|  |
| --- |
| https://sun9-24.userapi.com/c854320/v854320767/21286e/t929UXOPcBs.jpg |

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).

|  |
| --- |
| https://sun9-16.userapi.com/c854320/v854320767/212893/lyr1tedlnR0.jpg |
| https://sun9-23.userapi.com/c854320/v854320767/21289d/v57bajEYWPQ.jpg |
| https://sun9-39.userapi.com/c854320/v854320767/21288c/udBWK-JLa7M.jpg |

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

*Команда:*

*sudo packit -m inject -t ARP -c 1 -A 1 -y 192.168.88.13 -Y 3c:fa:43:e3:40:45*

*-x 192.168.88.10 -X 64:5A:04:93:55:0E -E 3c:fa:43:e3:40:45 -i wlp2s0*

|  |
| --- |
| https://sun9-70.userapi.com/c856520/v856520583/1437e3/qZbdViEr4b8.jpg |

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

|  |
| --- |
| https://sun9-28.userapi.com/c856520/v856520583/1437da/SkiCliiJbKY.jpg |

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.

|  |
| --- |
| https://sun9-22.userapi.com/c856520/v856520583/143679/6vkPIaIfPvw.jpg |
| https://sun9-30.userapi.com/c856520/v856520583/143683/ZcQ3zQVpl9w.jpg |

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

|  |
| --- |
| https://sun9-60.userapi.com/c856520/v856520583/1436d7/7kxtb9o5CJo.jpg |

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. Захваченный пакет

|  |
| --- |
| https://sun9-38.userapi.com/c857532/v857532221/1bda59/i0uP1lzqYPY.jpg |

1. Согласно материалам из рекомендованных источников ”разбить” заданный кадр на поля.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Заголовок Ethernet кадра | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | IP | | | | | | | | | | | | | | | | | | | | | | | |
| MAC получателя | | | | | | | | | | | | | | | | | | | | | | MAC отправителя | | | | | | | | | | | | | | | | | | | | | TYPE | | | | | | | | VERSION | | | | | | | IHL | | | | | Differentiated Services Code Point | | | | | | | ECN | | | | |
| 4c | 5e | | | | 0c | | | 0c | | | | | | 0b | | | 71 | | | | | 64 | | | | 5a | | 04 | | | 93 | | | 55 | | | | 0e | | | | | 08 | | | | 00 | | | | 45 | | | | | | | | | | | | 00 | | | | | | | | | | | |
| IP | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TOTAL LENGTH | | | | | | | | | | IDENTIFICATION | | | | | | | | | FLAGS | | | | | | | | TTL | | | | | | PROTOCOL | | | | | | | HEADER CHECKSUM | | | | | | | | | | | | | | | | SOURCE | | | | | | | | | | | | | | | | | | |
| 00 | | | | 3c | | | | | | 09 | | | | | 96 | | | | 40 | | | | | 00 | | | 40 | | | | | | 06 | | | | | | | 9f | | | | | | | | | 90 | | | | | | | c0 | | | | | a8 | | | | | 58 | | | | | 0a | | | |
| IP | | | | | | | | | | | | | | | | | | | | | | | TCP | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DESTINATION | | | | | | | | | | | | SRC PORT | | | | | | | | | | | DEST PORT | | | | | | | | | | | | | | SEGMENT NUMBER | | | | | | | | | | | | | | | | Acknowledgment NUMBER | | | | | | | | | | | | | | | HLEN(1010 ….),  FLAGS | | | | | | |
| 23 | | de | | | | 55 | | | 05 | | | d4 | | | | | | e8 | | | | | 00 | | | | | | | 50 | | | | | | | e9 | | | | | 8e | | | | 48 | | | | a9 | | | 00 | | | | 00 | | | 00 | | | | 00 | | | | a0 | | | | | 02 | |
| TCP | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| WINDOW SIZE | | | | | | | CHECKSUM | | | | | | URGENT POINTER | | | | | | | | OPTIONS | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| fa | | | f0 | | | | 82 | | | | 86 | | 00 | | | 00 | | | | | Max Segment Size | | | | | | | | | | | | | | | SACK Permitted | | | | | | | | Timestamps | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | 02 | | | | | 04 | | | | 05 | | | b4 | | | 04 | | | | | | 02 | | | | 08 | | | 0a | | | | 86 | | | 9a | | | | aa | | | d8 | | | 00 | | | | 00 | | | 00 | | 00 |
| TCP | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| OPTIONS | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| No-Operation | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | Window scale | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 01 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | 03 | | | | | | | | | | | | | | | 03 | | | | | | | | | | | | | 07 | | | | | | | |

1. Рассчитать контрольную сумму заголовка IP-пакета. Вписать результат в соответствующее поле на бланке задания. Привести процесс расчета.

Контрольная сумма заголовка передаваемого пакета IPv4 рассчитывается по следующему алгоритму:

1. Заголовок разбивается на слова Wi по 16 бит(2 байта). При необходимости последнее слово заголовка дополняется нулями справа (биты заполнения), чтобы «выровнять» длину заголовка в битах кратно 16.

|  |  |
| --- | --- |
| W1 | 450016 |
| W2 | 003c16 |
| W3 | 099616 |
| W4 | 400016 |
| W5 | 400616 |
| W6 | 000016 |
| W7 | c0a816 |
| W8 | 580a16 |
| W9 | 23de16 |
| W10 | 550516 |

2.Значение поля контрольной суммы, которому соответствует слово W6, принимается равным нулю:

W6 = (0000)16

3. Полученные 16-битные слова Wi поэлементно суммируются между собой, как двоичные числа с переносом в старшие разряды:

450016 + 003c16=453C16

453C16 + 099616=4ED216

4ED216 + 400016=8ED216

8ED216 + 400616=CED816

CED816 + C0A816 =18F8016

18F8016 + 580A16 =1E78A16

1E78A16 + 23DE16 =20B6816

20B6816 + 550516 =2606D16

Ws=2606D16

4. В том случае, если результат сложения Ws в двоичном представлении превышает по длине 16 бит, он разбивается на два 16-битных слова, которые складываются между собой. Эту процедуру называют «круговым переносом», т. е, переполнение старшего разряда переносится в младший.

Ws=000216 + 606D16=606F16

5. Находится двоичное поразрядное дополнение результата сложения, которое и записывается в поле контрольной суммы:

CSIP = 9F9016

Контрольная сумма совпала с полученной контрольной суммой из пакета.

Проверка контрольной суммы при приеме IP-пакета производится по аналогичному алгоритму, отличаясь только тем, что в расчете участвует и контрольная сумма принятого IP-пакета. Если итоговое поразрядное двоичное дополнение полученной суммы равно 0, т. е. (()160000), то это говорит о корректности контрольной суммы.

450016 + 003c16 + 099616 + 400016  + 400616 +9F9016 + C0A816 + 580A16 + 23DE16 + 550516 =2FFFD16

Разбиваем результат сложения на 2(т.к он превышает 16 бит)

000216 +FFFD16=FFFF16

Находим поразрядное дополнение

FFFF16 FFFF16=000016

Вычисленная контрольная сумма 9F9016 корректна.

1. Рассчитать контрольную сумму TCP-сегмента. Вписать результат в соответствующее поле на бланке задания.

Src IP: c0 a8 58 0a  
Dst IP: 23 de 55 05  
Zero: 00 (const)  
Proto: 06   
TCP\_Len: 0040

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

Считаем сумму псевдозаголовка

C0A8 + 580A + 23DE + 5505 + 0000 + 0600 + 0040 = 197D5

Считаем сумму TCP-заголовка с зануленной суммой

|  |  |  |  |
| --- | --- | --- | --- |
| W1 | D4E8 | W11 | 0204 |
| W2 | 0050 | W12 | 05B4 |
| W3 | E98E | W13 | 0402 |
| W4 | 48A9 | W14 | 080A |
| W5 | 0000 | W15 | 86A9 |
| W6 | 0000 | W16 | AAD8 |
| W7 | A002 | W17 | 0000 |
| W8 | FA F0 | W18 | 0000 |
| W9 | 0000 | W19 | 0103 |
| W10 | 0000 | W20 | 0307 |
| ∑ | 4EBB0 |

4EBB0+ 197D5 =68385

0006 + 8385=838B

Находим двоичное поразрядное дополнение:

838B16 = 1000 0011 1000 01012

**CSTCP=7C7416**

Проверка:

C0A8+580A+23DE+5505+0000+0600+0040+ D4E8+0050+E98E+48A9+0000+0000+A002+FAF0+ 7C74+0000+0204+05B4+0402+080A+86A9+AAD8+0000+0000+0103+0307=6FFF9

0006+FFF9=FFFF16

Находим поразрядное дополнение

FFFF16 FFFF16=000016

**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.