Национальный исследовательский университет ИТМО

Факультет программной инженерии и компьютерной техники

Учебно-исследовательская работа №3

по дисципение Сети ЭВМ и телекоммуникации

Анализ трафика компьютерных сетей утилитой Wireshark

Студент: Саржевский Иван

Группа: P3302

г. Санкт-Петербург

2020 г.

Содержание

1 Цель

Цель работы – изучить структуру протокольных блоков данных, анализируя реальный трафик на компьютере студента с помощью бесплатно распространяемой утилиты `Wireshark`.

2 Утилита `ping`

Для анализа трафика, создаваемого утилитой `ping` был выбран сайт **`www.ias.ru`**.

```
Frame 5: 1042 bytes on wire (8336 bits), 1042 bytes captured (8336 bits) on interface wlp4s0, id 0
Ethernet II, Src: Chongqin_64:e6:c5 (c0:b5:d7:64:e6:c5), Dst: Tp-LinkT_3d:06:ae (cc:32:e5:3d:06:ae)
Internet Protocol Version 4, Src: 192.168.0.105, Dst: 81.195.71.197
Internet Control Message Protocol
```

Рис. 1: Заголовки протоколов для команды `ping`.

На рисунке 1 изображены заголовки различных протоколов, используемых при передаче запроса.

2.1 Фрейм

```
Interface id: 0 (wlp4s0)
Encapsulation type: Ethernet (1)
Arrival Time: Apr 12, 2020 22:23:51.094101026 MSK
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1586719431.094101026 seconds
[Time delta from previous captured frame: 0.000253948 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.036999160 seconds]
Frame Number: 5
Frame Length: 1042 bytes (8336 bits)
Capture Length: 1042 bytes (8336 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:icmp:data]
[Coloring Rule Name: ICMP]
[Coloring Rule String: icmp || icmpv6]
```

Рис. 2: Информация о фрейме команды `ping`.

Структура, представленная на рисунке 2, описывает метаданные Wireshark для этого запроса - его порядковый номер среди всех записанных, время прибытия, размер, протокол и цвет выделения в интерфейсе.

2.2 Ethernet II

Ethernet II - протокол канального уровня, т.е. описывает передачу данных в рамках локальной сети. Типичная структура кадра Ethernet II представлена в таблице 1.

<table>
<tr><td colspan="5">Кадр Ethernet II
(от 64-х до 1528-ти байт)</td></tr>
<tr><td colspan="3">MAC-заголовок
(14 байт)</td><td>Данные
(от 46-ти до 1500 байт)</td><td>–</td></tr>
<tr><td>MAC получателя
(6 байт)</td><td>MAC отправителя
(6 байт)</td><td>Тип протокола
(2 байта)</td><td>Данные</td><td>CRC
(4 байта)</td></tr>
</table>

Таблица 1: Структура кадра Ethernet II.

В данном случае получателем выступает роутер, а отправителем - рабочая машина, их MAC-адреса записаны в кадр, тип протокола - `IPv4`, что можно увидеть на рисунке 3.

```
Destination: Tp-LinkT_3d:06:ae (cc:32:e5:3d:06:ae)
   Address: Tp-LinkT_3d:06:ae (cc:32:e5:3d:06:ae)
   .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
   .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Source: Chongqin_64:e6:c5 (c0:b5:d7:64:e6:c5)
   Address: Chongqin_64:e6:c5 (c0:b5:d7:64:e6:c5)
   .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
   .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
```

Рис. 3: Кадр Ethernet II для `ping`