Университет ИТМО

**Лабораторная работа №3 по дисциплине**

**«Сети ЭВМ и телекоммуникации»**

Выполнил:

студент 3-го курса

группы 3125

Припадчев Артём

Санкт-Петербург

2015

**Часть 1. Исследование структуры сетевых пакетов**

**с помощью анализатора трафика Wireshark**

**Протокол IP**



**tracert www.pa.gov**

1) Мой IP-адрес: 192.160.0.104

2) Protocol: ICMP

3) Header length: 20 bytes

Total length - header length = 92 - 20 = 72 bytes

4) Time to live: 1 данное поле инкрементируется на следующих ICMP Echo request (с повторением одного значения несколько раз)

5) Identification: 0x2d28 (11560)

Идентификатор - значение, назначаемое отправителем пакета и предназначенное для определения корректной последовательности фрагментов при сборке пакета.

**Фрагментация пакетов**



**ping -l 1470 4tochka.esy.es**

1, 3) Фрагментация имеет место, на это указывает поле 2 IPv4 Fragments

2) В заголовке 3 бита флагов. Первый бит должен быть всегда равен нулю, второй бит DF (don't fragment) определяет возможность фрагментации пакета и трений бит MF (more fragments) показывает, не является ли этот пакет последним в цепочке пакетов.

**Вариант 5. ICMP**



**ping -n 10 4tochka.esy.es**

1) 20 пакетов, 10 запросов и 10 ответов

2) Мой ip 192.160.1.136. IP-адрес назначения: 31.170.165.244

3) Type: 8 Echo (ping) request Code: 0

Также содержит поля Checksum 2 байта, Identifier 2 байта, Sequence number 2 байта и поле Data 32 байта

4) Type: 0 Echo (ping) reply Code: 0

Также содержит поля Checksum 2 байта, Identifier 2 байта, Sequence number 2 байта и поле Data 32 байта



**tracert 4tochka.esy.es**

1) Мой IP 192.160.1.136 IP назначения: 31.170.165.244

2) Отличаются размером данных. Здесь Data занимает 64 байта.

3) Например, Time exceeded. Type - 11 (TTL exceeded). Code: 0 (в процессе передачи дейтаграммы поле TTL приняло значение 0).

ICMP Error содержит в общем случае Type, Code, Checksum, а дальше уже в зависимости от ошибки

**Часть 2. Исследование структуры сетевых пакетов**

**с помощью генератора пакетов Ostinato**

|  |  |
| --- | --- |
| **ARP** | **UDP** |
| C:\Users\Артём\Desktop\ARP.PNG | **C:\Users\Артём\Desktop\UDP.PNG** |





 **Sequential Streams** отличается от **Interleaved Streams** тем, что в первом случае сначала будут отправлены все пакеты первого протокола, а затем пакеты второго протокола. Во втором случае пакеты чередуются при передаче.

 В Wireshark протокол посылаемых пакетов определяется неправильно, т.к. пропущены некоторые уровни сетевой модели. UDP – это протокол 4 (транспортного) уровня, а ARP – 2 (канального).