Национальный исследовательский университет информационных технологий,
механики и оптики
Кафедра вычислительной техники
Сети ЭВМ и телекоммуникации

Лабораторная работа №3
«Аналииз структуры сетевого трафика с помощью программ Wireshark и Ostinato»
Вариант 5

Студентка:
Куклина М., P3301
Преподаватель:
Шинкарук Д.Н.

Санкт-Петербург, 2017

Цели работы

1. Исследование структуры сетевых пакетов с помощью анализатора трафика Wireshark.
2. Исследование структуры сетевых пакетов с помощью генератора пакетов Ostinato.

Часть 1. Исследование структуры сетевых пакетов с помощью анализатора трафика Wireshark

Протокол IP

Конечный узел: mk.ru.

Анализ трафика производился на операционной системе Linux, на котрой аналогом требуемой в задании утилиты tracert служить команда `traceroute -icmp`.

Структура первого пакета.

```
IP header
----------
Version:         4
IHL:             5
DSCP:            0
ECN:             0
Total length:    60
Identification:  0x2c80
Flags:           0x00
Fragment offset: 0
TTL:             1
Protocol:        1
Header Checksum: 0x49eb
Source IP:       192.168.1.26
Destination IP:  92.242.36.162
```

Из заголовка следует, что:

- исходный адрес хоста: 192.168.1.26 – адрес компьютера в локальной сети, с которого отправился пакет;
- протокол верхнего уровня определяется полем IP-заголовка «Protocols», которое имеет значение 1, обозначающее протокол ICMP в соответствии с RFC-790 ;
- размер заголовка IP определяется полем «Internet Header Length», значение в котором равно 5 DWORD'ам или 20 байтам;
- размер пакета, включающий заголовок и данные, определяется полем «Total Length», следовательно, данные занимают 40 байт;

- поле «TTL» равняется 1, что означает максимальное количество узлов на пути следования пакета; в данном случае ровно на первом узле пакет уничтожится и в ответ от текущего узле придёт ICMP Time Exceeded с информацией об узле;
- поле «Identification» идентифицирует отдельный пакет и используется при фрагемнтации (фрагменты с одинаковыми ID собираются в один пакет, порядок фрагментов определяется полем «Fragment offset», а наличие фрагметов – полем «Flags»).

Фрагментация пакетов

Конечный узел: wireshark.com
При запуске команды анализатор трафика выдаёт следующие результаты.

```
IP header 1                        IP header 2
-----------                        -----------
Version:         4                 Version:      4
IHL:             5                 IHL:          5
DSCP:            0                 DSCP:         0
ECN:             0                 ECN:          0
Total length:    1500              Total length: 548
Identification:  0x0d6b            ID:           0x0d6b
Flags:           0x01              Flags:        0x00
Fragment offset: 0                 Frag. off:    1480
TTL:             64                TTL:          64
Protocol:        1                 Protocol:     1
Header Checksum: 0x43c5            Checksum:     0x66c4
Source IP:       192.168.1.26      Source IP:    192.168.1.26
Destination IP:  172.110.10.86     Dest. IP:     172.110.10.86
```

Из этих двух последовательно пойманных пакета видно, что:

- имеет место фрагментация пакетов;
- первый пакет является фрагементом, чему свидетельствуют значение поля «Flags» (0x01 – More fragments), второй пакет является конечным (0x00 для флагов и не нулевое значение поля «Fragment offset»);
- из всего указанного следует, что пакета всего два.

Протокол ICMP

Конечный узел: wireshark.com

Часть 1. Исследование с помощью команды ping

После запуска команды анализатор трафика выдал следующие результаты.

```
IP header                          IP header
---------                          ---------
Version:         4                 Version:       4
IHL:             5                 IHL:           5
Total Length:    84                Total Length:  84
ID:              0x5afb            ID:            0x5afb
Frag.off.:       0                 Frag.off.:     0
TTL:             64                TTL:           40
Protocol:        1                 Protocol:      1
Checksum:        0x6727            Checksum:      0x66a1
Source IP:       192.168.1.26      Source IP:     172.110.10.86
Destination IP:  172.110.10.86     Dest. IP:      192.168.1.26

ICMP Echo Request                  ICMP Echo Reply
-----------------                  ---------------
Type:       8                      Type:      0
Code:       0                      Code:      0
Checksum:   0x3848                 Checksum:  0x4048
ID:         0x09b5                 ID:        0x09b5
Seq. num.:  1                      Seq. num:  1
```

1. Программа захватила 20 пакетов: ping отправил 10 ICMP Echo Request и на каждый получил ICMP Echo Reply.
2. IP адрес источника: 192.168.1.26; IP адресанта: 104.25.218.21.
3. Анализ первого пакета. Тип пакета ICMP определяется полями «Type» и «Code»; в данном случае (8,0) определяют Echo Request. Поля «ID» и «Sequence number» одинаковы в двух пакетах и служат для опеределения соответствия пары запрос-ответ. Также ID не меняется при всей ping-сессии для ей идентификации. Значение seq инкрементируется с каждым отправленым ICMP Echo Request. Поля «Type» и «Code» занимают 1 байт каждое; «Cheksum», «Identifier» и «Sequence number» – 2 байта.
4. Анализ второго пакета. Всё отличие от первого пакета обнаруживается в поле «Type», которое в паре с полем «Code» определяют Echo Reply.

Часть 2. Исследование с помощью команды traceroute

```
IP header
---------
```

```
Version:        4
IHL:            5
Total length:   60
ID:             0x3995
Flags:          0x00
Frag. off:      0
TTL:            1
Protocol:       1
Checksum:       0x07a6
Source:         192.168.1.26
Dest:           172.110.10.86

ICMP Echo Request
-----------------
Type:    8
Code:    0
Cheksum: 0x07a6
ID:      0x1536
Seq.num: 1

IP header
---------
Version:        4
IHL:            5
Total length:   88
ID:             0xa1f7
Flags:          0x00
Frag. off:      0
TTL:            64
Protocol:       1
Checksum:       0x07a6
Source:         192.168.1.1
Dest:           192.168.1.26

ICMP Time Exceeded
------------------
Type:    11
Code:    0
Cheksum: 0x0f4ff
+ Unused
+ Old IP header and 64 bits of datagram.

IP header
```

```
---------
Version:        4
IHL:            5
Total length:   60
ID:             0xaa64
Flags:          0x00
Frag. off:      0
TTL:            49
Protocol:       1
Checksum:       0x66b6
Source:         172.110.10.86
Dest:           192.168.1.26

ICMP Echo Reply
---------------
Type:    0
Code:    0
Cheksum: 0x7519
ID:      5430
Seq.num: 43
```

Часть 2. Исследование структуры сетевых пакетов с помощью генератора пакетов Ostinato

Вывод

1. Описать алгоритмы traceroute, объяснить, почему он отсылает три пакета 2. Каждый узел согласно RFC-1122 должен реализовывать ICMP Echo Server.