Санкт-Петербургский Политехнический Университет Петра Великого Институт компьютерных наук и технологий Кафедра компьютерных систем и программных технологий

Защита информации

Отчет по лабораторной работе №1 Исследование сетевого трафика

Работу выполнил: Раскин Андрей Группа: 43501/3 Преподаватель: Новопашенный Андрей Гелиевич

1 Цель работы

Закрепление навыков работы в программе WireShark и знаний о некоторых сетевых протоколах.

2 Программа работы

При помощи анализатора сетевого трафика WireShark продемонстрировать в сети:

- 1. Работу утилиты ping
- 2. Работу утилиты tracert
- 3. Работу ІСМР-протокола в следующих ситуациях:

Отправка фрагментированного ping'a,

Получение ошибки 3.1 (Destination host unreachable)

- 4. Работу АРР-протокола (запрос и ответ);
- 5. Работу протокола ТСР в следующих ситуациях:

Установка соединения,

Разрыв соединения,

Попытка соединения на отсутствующий порт

3 Конфигурация компьютера в сети

1

```
C:\WINDOWS\system32\cmd.exe
:\Documents and Settings\Student.AIVTS9>telnet ya.ru 5g5ff
connecting To ya.ru...Could not open connection to the host, on port 5g5ff: Conn
::\Documents and Settings\Student.AIVTS9>ipconfig
Windows IP Configuration
Ethernet adapter UMware Network Adapter UMnet8:
         Connection-specific DMS Suffix IP Address. .
        IP Address. . .
Subnet Mask . .
Default Gateway
Ethernet adapter UMware Network Adapter UMnet1:
         Connection-specific DNS Suffix
IP Address.
Ethernet adapter VirtualBox Host-Only Network:
         Connection-specific DNS Suffix
IP Address
Ethernet adapter tapO:
        Media State . . . . . . . . : Media disconnected
Ethernet adapter Local Area Connection 3:
        C:\Documents and Settings\Student.AIUTS9>_
```

Рис. 1: Конфигурация сети

4 Ход работы

4.1 Работы утилиты ping

Ping — утилита для проверки целостности и качества соединений в сетях на основе TCP/IP, а также обиходное наименование самого запроса. Утилита отправляет запросы (ICMP Echo-Request) протокола ICMP указанному узлу сети и фиксирует поступающие ответы (ICMP Echo-Reply). По умолчанию производится 4 попытки отправки запроса.

```
### Frame 175 (74 bytes on wire, 74 bytes captured)

Arrival Time: Feb 13, 2017 10:47:49,961051000

[Time delta from previous displayed frame: 0.003757000 seconds]

[Time delta from previous displayed frame: 8.046081000 seconds]

[Time since reference or first frame: 8.046081000 seconds]

Frame Number: 175

Frame Length: 74 bytes

capture Length: 74 bytes

[Frame 1s marked: False]

[Protocols in frame: ethip:icmp:data]

[Coloring Rule Name: ICMP]

[Coloring Rule Name: ICMP]

[Coloring Rule String: icmp]

### Ethernet II, Src: AsustekC_40:0b:7c (00:1a:92:40:0b:7c), Dst: CameoCom_6e:7b:52 (00:40:f4:6e:7b:52)

### Internet Protocol, Src: 10.1.15.10 (10.1.15.10), Dst: 74.125.232.226 (74.125.232.226)

**Version: 4**

*## Header length: 20 bytes

### Offerentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)

**Total Length: 60

*## Idength: 60

*## Idength: 60

*## Idength: 10 tyle: 128

*## Protocol: ICMP (0xx1)

### Header checksum: 0xcc54 [correct]

**Source: 10.1.15.10 (10.1.15.10)

*## Destination: 74.125.232.226 (74.125.232.226)

### Internet Control Message Protocol
```

Рис. 2: ІСМР эхо запрос

```
□ Frame 176 (74 bytes on wire, 74 bytes captured)
Arrival Time: Feb 13, 2017 10:47:49.971183000

[Time delta from previous captured frame: 0.01032000 seconds]

[Time delta from previous displayed frame: 0.01032000 seconds]

[Time since reference or first frame: 8.056213000 seconds]

Frame Number: 176

Frame Length: 74 bytes

Capture Length: 74 bytes

[Frame is marked: False]

[Protocols in frame: ethich:cimp:data]

[Coloring Rule Name: ICMP]

[Coloring Rule Name: ICMP]

[Coloring Rule Name: ICMP]

[Sthernet II, Src: Cameocom_Ge:7b:52 (00:40:f4:6e:7b:52), Dst: Asustekc_40:0b:7c (00:1a:92:40:0b:7c)

□ Internet Protocol, Src: 74.125.232.226 (74.125.232.226), Dst: 10.1.15.10 (10.1.15.10)

Version: 4

Header length: 20 bytes

□ Offernentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)

Total Length: 60

Identification: 0xdb14 (56084)

□ Flags: 0x00

Fragment offset: 0

Time to live: 53

Protocol: ICMP (0x01)

□ Header checksum: 0x5e42 [correct]

Source: 74.125.232.226 (74.125.232.226)

Destination: 10.1.15.10 (10.1.15.10)

□ Internet Control Message Protocol
```

Рис. 3: ІСМР эхо ответ

Kак видно, в поле Destination указан IP-адрес google.com, поле Source показывает IP-адрес текущего компьютера.

4.2 Работа утилиты tracert

В основе работы данной утилиты лежит протокол icmp. Команда TRACERT определяет путь до точки назначения с помощью посылки в точку назначения эхо-сообщений протокола Control Message Protocol (ICMP) с постоянным увеличением значений срока жизни (Time to Live, TTL). Попробуем пронаблюдать трассировку маршрута пакетов до узла spbstu.ru при помощи протокола ICMP и утилиты tracert.

Первый пакет трассировки маршрута отправляется с TTL равным 1. Это значит, что на первом же маршрутизаторе пакет будет уничтожен и нам придет сообщение об ошибке.

В сообщении об ошибке указан тип ICMP-пакета — 11.0, что означает, что время жизни пакета истекло. Сообщение пришло от маршрутизатора сети, который имеет адрес 192.168.1.1. Аналогично продолжается трассировка маршрута дальше с постепенным инкрементом параметра TTL. Таким образом составляется примерный маршрут прохождения IP-пакета до узла с адресом spbstu.ru.

```
C:\Users\Georgiy\tracert spbstu.ru

Tpaccupobka маршрута к spbstu.ru [195.209.230.198]

c максимальным числом прыжков 30:

1 13 ms 5 ms 6 ms 192.168.1.1
2 6 ns 6 ms 14 ms 192.168.25.2
3 6 ns 4 ms 7 ns ip-1.47.255.92.net.unnet.ru [92.255.47.1]
4 3 ms 30 ms 5 ms 92.255.2.23
5 7 ms 6 ns 4 ms ip-51.97.104.89.net.unnet.ru [89.104.97.51]
6 3 ns 3 ms 3 ms 5 h116-1-gw.spb.runnet.ru [194.190.255.291]
7 78 ns 123 ms 5 ms stu.spb.runnet.ru [194.85.36.238]
8 4 ns 4 ms 6 ms 195.209.230.198]
9 4 ns 3 ms 4 ms cnd.spbstu.ru [195.209.230.198]
```

Рис. 4: Результат трассировки маршрута в консоли

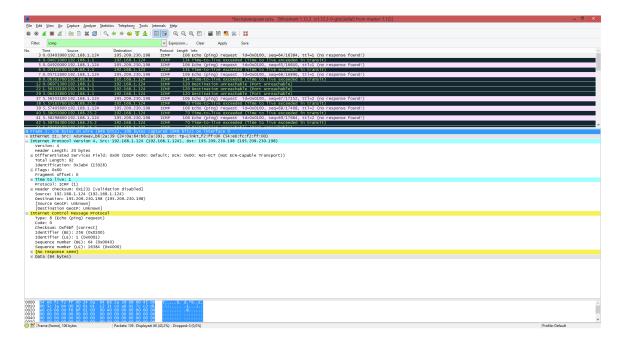


Рис. 5: Первый пакет трассировки маршрута

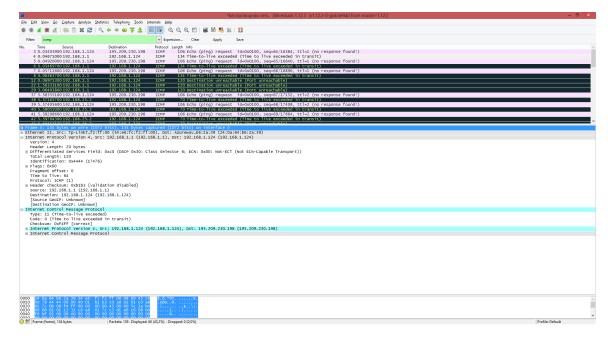


Рис. 6: Ответ на первый пакет трассировки

4.3 Протокол ІСМР

4.3.1 Фрагментированный ping

Попробуем отослать фрагментированный ping-запрос. Данный вид запроса использует ICMP-протокол. Для фрагментации пакета необходимо указать его размер, превышающий MTU (maximum transmission

unit) - максимальный размер полезного блока данных одного пакета, который может быть передан протоколом без фрагментации. Для протокола Ethernet обычно это чуть больше 1500 байт. Для фрагментации пакета на 3 части укажем размер — 4000 байт.

```
E Frame 4855 (1514 bytes on wire, 1514 bytes captured)

Arrival Time: Feb 13, 2017 11:24:25,286832000
[Time delta from previous captured frame: 0.763102000 seconds]
[Time delta from previous displayed frame: 17.167839000 seconds]
[Time since reference or first frame: 71.872501000 seconds]
Frame Number: 4855
Frame Length: 1514 bytes

Capture Length: 1514 bytes

[Frame is marked: False]
[Protocols in frame: eth:ip:icmp:data]
[Coloring Rule Name: ICMP]
[Coloring Rule String: icmp]
[Eclorert II, Src: 02:ifficei:11:bi4:33 (02:ff:ei:11:bi4:33), Dst: Asustekc_40:0b:7c (00:1a:92:40:0b:7c)

■ Internet Protocol, Src: 10.1.15.11 (10.1.15.11), Dst: 10.1.15.10 (10.1.15.10)

version: 4

Header length: 20 bytes

■ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)

Total Length: 1500

Identification: 0x02cb (715)

■ Flags: 0x02 (More Fragments)
Fragment offset: 0

Time to live: 128

Protocol: ICMP (0x01)

■ Header checksum: 0xe03f [correct]
Source: 10.1.15.11 (10.1.15.11)
```

Рис. 7: Ответ на первый пакет трассировки

О фрагментированности пакета свидетельствуют флаги пакета IP (0х01 – имеются еще фрагменты). О том, что это первый пакет из фрагментированных, свидетельствует нулевое смещение фрагмента. При этом во всех трех IP пакетах содержится ICMP-пакет с одним и тем же идентификатором.

4.3.2 Несуществующий хост

Попробуем пронаблюдать ошибку типа 3.1 (целевой узел недостижим). Для этого отправим ping-запрос на адрес, которого не существует. В пакете можно наблюдать типичный ping-запрос (ICMP-пакет типа 8.0).

```
⊞ Ethernet II, Src: AsustekC_40:0b:7c (00:1a:92:40:0b:7c), Dst: CameoCom_6e:7b:52 (00:40:f4:6e:7b:52)

⊟ Internet Protocol, Src: 10.1.15.10 (10.1.15.10), Dst: 10.1.15.1 (10.1.15.1)

     Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
     Total Length: 148
     Identification: 0x19ef (6639)
  ⊞ Flags: 0x00
     Fragment offset: 1480
Time to live: 128
  Protocol: ICMP (0x01)

Header checksum: 0xedb4 [correct]
     Source: 10.1.15.10 (10.1.15.10)
Destination: 10.1.15.1 (10.1.15.1)

⊞ [IP Fragments (1608 bytes): #5032(1480), #5033(128)]

□ Internet Control Message Protocol

     Type: 8 (Echo (ping) request)
Code: 0 ()
     Checksum: 0x2150 [correct]
     Identifier: 0x0600
     Sequence number: 7168 (0x1c00)
  ⊕ Data (1600 bytes)
       00 40 f4 6e 7b 52 00 1a
00 94 19 ef 00 b9 80 01
0f 01 61 62 63 64 65 66
6f 70 71 73 73 74 75 76
                                                                                                                                                                                                                      *
                                         92 40 0b 7c 08 00 45 00
ed b4 0a 01 0f 0a 0a 01
67 68 69 6a 6b 6c 6d 6e
                                                                              ..abcdef ghijklmn
Frame (162 bytes) Reassembled IPv4 (1608 bytes)
```

Рис. 8: Ping-запрос

А вот ответом на указанный выше запрос будет ICMP-пакет типа 3.1, свидетельствующий об ошибке «целевой узел недостижим». При этом, в ответе, в качестве данных пакета отправляется заголовок того пакета, на который пришел ответ.

Рис. 9: ІСМР-ответ

4.4 ARP протокол

ARP-запрос выполняется по широковещательному адресу (ff:ff:ff:ff:ff:ff), для того, чтобы все узлы сети получили данный пакет. В пакете указывается его тип (поле Opcode) – запрос, а так же целевой IP-адрес для которого запрашивается MAC-адрес. MAC-адрес цели при этом обнулен.

```
⊟ Frame 575 (60 bytes on wire, 60 bytes captured)

    Arrival Time: Feb 13, 2017 11:03:17.131479000
    [Time delta from previous captured frame: 0.121888000 seconds]
    [Time delta from previous displayed frame: 0.367064000 seconds]
    [Time since reference or first frame: 5.185051000 seconds]
    Frame Number: 575
    Frame Length: 60 bytes
    Capture Length: 60 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
⊕ Ethernet II, Src: CameoCom_6e:7b:52 (00:40:f4:6e:7b:52), Dst: 48:5b:39:78:46:f0 (48:5b:39:78:46:f0)
■ Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    opcode: request (0x0001)
    Sender MAC address: CameoCom_6e:7b:52 (00:40:f4:6e:7b:52)
    Sender IP address: 10.1.15.1 (10.1.15.1)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.1.15.8 (10.1.15.8)
```

Рис. 10: Часть IP-пакета, содержащего ARP-запрос

ARP-ответ отсылается уже на тот адрес, с которого исходил ARP-запрос. В пакете указывается его тип (поле Opcode) – ответ, а так же заполненный MAC-адрес цели.

```
Frame 576 (60 bytes on wire, 60 bytes captured)
    Arrival Time: Feb 13, 2017 11:03:17.131530000
    [Time delta from previous captured frame: 0.000051000 seconds]
    [Time delta from previous displayed frame: 0.000051000 seconds]
    [Time since reference or first frame: 5.185102000 seconds]
    Frame Number: 576
    Frame Length: 60 bytes
    Capture Length: 60 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
⊕ Ethernet II, Src: 48:55:39:78:46:f0 (48:5b:39:78:46:f0), Dst: CameoCom_6e:7b:52 (00:40:f4:6e:7b:52)
■ Address Resolution Protocol (reply)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    opcode: reply (0x0002)
    Sender MAC address: 48:5b:39:78:46:f0 (48:5b:39:78:46:f0)
    Sender IP address: 10.1.15.8 (10.1.15.8)
    Target MAC address: CameoCom_6e:7b:52 (00:40:f4:6e:7b:52)
    Target IP address: 10.1.15.1 (10.1.15.1)
```

Рис. 11: Часть IP-пакета, содержащего ARP-ответ

4.5 ТСР-протокол

4.5.1 Установление соединения

Эта операция происходит следующим образом: Клиент, посылает серверу сегмент с номером последовательности и флагом SYN. Сервер получает сегмент, запоминает номер последовательности и

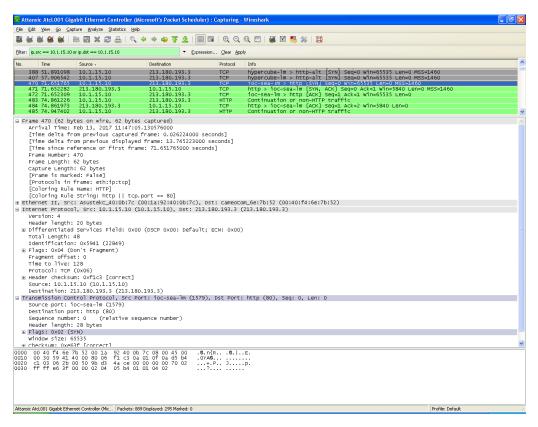


Рис. 12: TCP запрос на установление соединения SYN

посылает клиенту сегмент с номером последовательности и флагами SYN и ACK. Если клиент получает сегмент с флагом SYN, то он запоминает номер последовательности и посылает сегмент с флагом ACK.

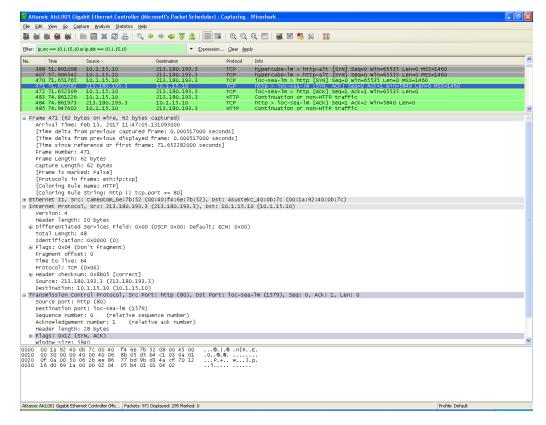


Рис. 13: Ответ сервера на установление ТСР-соединения

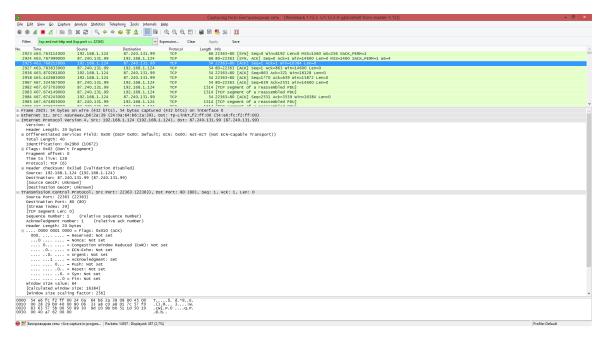


Рис. 14: Подтверждение от клиента о получении ответа

4.5.2 Разрыв соединения

При разрыве соединения сервер отсылает клиенту пакет с установленным флагом RST.

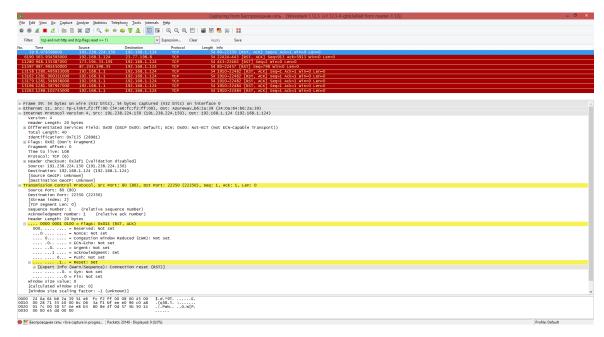


Рис. 15: Пример пакета с флагом RST

4.5.3 Установка соединения с отсутствующим портом

При попытке подключения к отсутствующему порту, не приходит ACK и RST, поэтому клиент находится в подвешенном состоянии и ожидает ответа.

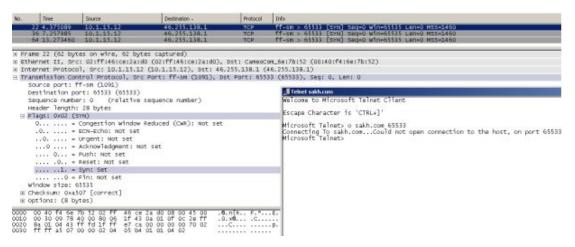


Рис. 16: Пример пакета с подвешенным состоянием

5 Выводы

В ходе работы были получены навыки работы в программе WireShark и закреплены знания о сетевых протоколах ARP, ICMP, TCP. Были рассмотрены:

- 1. работу утилит ping и tracert;
- 2. работа АРР-протокола;
- 3. работа протокола ICMP, включая такие типовые случаи, как: отправка фрагментированного пакета, возникновение ошибки 3.1, трассировка маршрута;
- 4. установка, разрыв и завершение ТСР соединения;