

Homework 02 Frolov Ivan

Как запустить

```
sudo java -jar target/IvanFrolov-1.0-SNAPSHOT-jar-with-dependencies.jar
```

Определяем Local IP, Router IP, Local MAC, Router MAC

--Первое--

```
admin@MacBook-Pro IvanFrolov % ipconfig getifaddr en0  
192.168.0.113
```

--Второе--

```
admin@MacBook-Pro IvanFrolov % netstat -nr | grep default  
default      link#22          UCSg           utun4  
default      192.168.0.1       UGScIg         en0  
default      link#24          UCSIg          bridge100  
default
```

--Третье--

```
admin@MacBook-Pro IvanFrolov % ifconfig en0 | grep ether  
ether ba:a9:89:78:af:b0
```

--Четвертое--

```
admin@MacBook-Pro IvanFrolov % arp -a  
? (169.254.169.254) at (incomplete) on en0 [ethernet]  
? (192.168.0.1) at c4:6e:1f:8:e7:16 on en0 ifscope [ethernet]
```

Все это кладем в `config.properties`

File structure

App - основное приложение

ArpScanner - сканирует ARP пакеты в локальной сети в течение какого-то промежутка времени

ArpSender - отправляет ARP запрос роутеру

Config - вспомогательный класс, который загружает конфигурации из config.properties

При запуске приложения меню выглядит так:

```
--- Приложение для управления ARP пакетами ---
Commands: 1 (Захват все ARP пакетов),
          2 (Найти MAC адрес роутера),
          3 (Статистика),
          exit
```

Enter command: █

Далее про каждую команду более подробно

Команда 1: захват ARP пакетов

Вывод захваченных ARP-пакетов в реальном времени (интерпретация полей).

```
admin@MacBook-Pro IvanFrolov % sudo java -jar target/IvanFrolov-1.0-SNAPSHOT-jar-with-dependencies.jar
--- Приложение для управления ARP пакетами ---
Commands: 1 (Захват все ARP пакетов),
          2 (Найти MAC адрес роутера),
          3 (Статистика),
          exit

Enter command: 1
Enter duration (sec): 10
SLF4J: Failed to load class "org.slf4j.impl.StaticLoggerBinder".
SLF4J: Defaulting to no-operation (NOP) logger implementation
SLF4J: See http://www.slf4j.org/codes.html#StaticLoggerBinder for further details.
WARNING: A restricted method in java.lang.System has been called
WARNING: java.lang.System::load has been called by com.sun.jna.Native in an unnamed module (file:/Users/admin/Desktop/Computer%20Networks/hw2/IvanFrolov/target/IvanFrolov-1.0-SNAPSHOT-jar-with-dependencies.jar)
WARNING: Use --enable-native-access=ALL-UNNAMED to avoid a warning for callers in this module
WARNING: Restricted methods will be blocked in a future release unless native access is enabled

Запуск захвата на 10 сек...
[ARP Header (28 bytes)]
  Hardware type: 1 (Ethernet (10Mb))
  Protocol type: 0x0800 (IPv4)
  Hardware address length: 6 [bytes]
  Protocol address length: 4 [bytes]
  Operation: 1 (REQUEST)
  Source hardware address: aa:29:48:0d:17:73
  Source protocol address: /192.168.0.103
  Destination hardware address: 00:00:00:00:00:00
  Destination protocol address: /192.168.0.100

[ARP Header (28 bytes)]
  Hardware type: 1 (Ethernet (10Mb))
  Protocol type: 0x0800 (IPv4)
  Hardware address length: 6 [bytes]
  Protocol address length: 4 [bytes]
  Operation: 1 (REQUEST)
  Source hardware address: aa:29:48:0d:17:73
  Source protocol address: /192.168.0.103
  Destination hardware address: 00:00:00:00:00:00
  Destination protocol address: /192.168.0.114

[ARP Header (28 bytes)]
  Hardware type: 1 (Ethernet (10Mb))
  Protocol type: 0x0800 (IPv4)
  Hardware address length: 6 [bytes]
```

Запуск захвата на 10 сек...

[ARP Header (28 bytes)]

Hardware type: 1 (Ethernet (10Mb))

Protocol type: 0x0800 (IPv4)

Hardware address length: 6 [bytes]

Protocol address length: 4 [bytes]

Operation: 1 (REQUEST)

Source hardware address: aa:29:48:0d:17:73

Source protocol address: /192.168.0.103

Destination hardware address: 00:00:00:00:00:00

Destination protocol address: /192.168.0.114

Hardware type: 1 (Ethernet) - пакет передается в сети Ethernet.

Protocol type: 0x0800 (IPv4) - ARP преобразует адреса для протокола IPv4.

Hardware address length: 6 - длина MAC (6 байт)

Protocol address length: 4: - длина IP (4 байт)

Operation: 1 (REQUEST) - в данном случае это запрос

Source hardware address (aa:29:48:0d:17:73) - MAC адрес отправителя

Source protocol address (192.168.0.103) - IP адрес отправителя

Destination hardware address (00:00:00:00:00:00) - заполнено нулями, так как отправитель не знает MAC адреса

Destination protocol address (192.168.0.114) - IP устройства, MAC которого мы ищем

В Wireshark все это выглядит примерно так

No.	Time	Source	Destination	Protocol	Length	Info
5588	769.016528	aa:29:48:0d:17:73	Broadcast	ARP	42	Who has 192.168.0.104? Tell 192.168.0.103
5589	770.037289	aa:29:48:0d:17:73	Broadcast	ARP	42	Who has 192.168.0.112? Tell 192.168.0.103
5590	770.037291	aa:29:48:0d:17:73	Broadcast	ARP	42	Who has 192.168.0.109? Tell 192.168.0.103
5591	770.037292	aa:29:48:0d:17:73	Broadcast	ARP	42	Who has 192.168.0.107? Tell 192.168.0.103
5592	770.037293	aa:29:48:0d:17:73	Broadcast	ARP	42	Who has 192.168.0.102? Tell 192.168.0.103
5593	770.037962	aa:29:48:0d:17:73	Broadcast	ARP	42	Who has 192.168.0.112? Tell 192.168.0.103
5594	773.006192	aa:29:48:0d:17:73	Broadcast	ARP	42	Who has 192.168.0.112? Tell 192.168.0.103
5595	773.006540	aa:29:48:0d:17:73	Broadcast	ARP	42	Who has 192.168.0.106? Tell 192.168.0.103
5596	773.006542	aa:29:48:0d:17:73	Broadcast	ARP	42	Who has 192.168.0.114? Tell 192.168.0.103
5597	773.006543	aa:29:48:0d:17:73	Broadcast	ARP	42	Who has 192.168.0.106? Tell 192.168.0.103
5598	773.006544	aa:29:48:0d:17:73	Broadcast	ARP	42	Who has 192.168.0.114? Tell 192.168.0.103
5599	773.006839	aa:29:48:0d:17:73	Broadcast	ARP	42	Who has 192.168.0.113? Tell 192.168.0.103
5600	773.006891	ba:a9:89:78:af:b0	aa:29:48:0d:17:73	ARP	42	192.168.0.113 is at ba:a9:89:78:af:b0
5601	773.007101	aa:29:48:0d:17:73	Broadcast	ARP	42	Who has 192.168.0.106? Tell 192.168.0.103
5602	773.007220	aa:29:48:0d:17:73	Broadcast	ARP	42	Who has 192.168.0.101? Tell 192.168.0.103
5603	773.0086743	ba:a9:89:78:af:b0	Broadcast	ARP	60	Who has 192.168.0.17 Tell 192.168.0.113

Команда 2: выяснить MAC адрес роутера

Для этого отправляем ARP запрос на IP адрес роутера в локальной сети

Выполнение команды в терминале:

Enter command: 2
Используется интерфейс: en0 (null)
ARP Request sent to 192.168.0.1

Запрос в Wireshark:

```

5602 773.007220 aa:29:48:0d:17:73 Broadcast ARP 42 Who has 192.168.0.1? Tell 192.168.0.103
5603 773.086743 ba:a9:89:78:af:b0 Broadcast ARP 60 Who has 192.168.0.1? Tell 192.168.0.113
5604 773.111338 TpLinkTechno_08:e7:16 ba:a9:89:78:af:b0 ARP 42 192.168.0.1 is at c4:6e:1f:08:e7:16
5605 774.030777 aa:29:48:0d:17:73 Broadcast ARP 42 Who has 192.168.0.114? Tell 192.168.0.103
5606 774.031598 aa:29:48:0d:17:73 Broadcast ARP 42 Who has 192.168.0.106? Tell 192.168.0.103
5607 774.031599 aa:29:48:0d:17:73 Broadcast ARP 42 Who has 192.168.0.116? Tell 192.168.0.103
5608 774.031600 aa:29:48:0d:17:73 Broadcast ARP 42 Who has 192.168.0.113? Tell 192.168.0.103
5609 774.031600 aa:29:48:0d:17:73 Broadcast ARP 42 Who has 192.168.0.114? Tell 192.168.0.103

> Frame 5603: Packet, 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface er
> Ethernet II, Src: ba:a9:89:78:af:b0 (ba:a9:89:78:af:b0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
< Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: ba:a9:89:78:af:b0 (ba:a9:89:78:af:b0)
  Sender IP address: 192.168.0.113
  Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
  Target IP address: 192.168.0.1

```

Ответ в Wireshark:

```

5603 773.086743 ba:a9:89:78:af:b0 Broadcast ARP 60 Who has 192.168.0.1? Tell 192.168.0.113
5604 773.111338 TpLinkTechno_08:e7:16 ba:a9:89:78:af:b0 ARP 42 192.168.0.1 is at c4:6e:1f:08:e7:16
5605 774.030777 aa:29:48:0d:17:73 Broadcast ARP 42 Who has 192.168.0.114? Tell 192.168.0.103
5606 774.031598 aa:29:48:0d:17:73 Broadcast ARP 42 Who has 192.168.0.106? Tell 192.168.0.103
5607 774.031599 aa:29:48:0d:17:73 Broadcast ARP 42 Who has 192.168.0.116? Tell 192.168.0.103
5608 774.031600 aa:29:48:0d:17:73 Broadcast ARP 42 Who has 192.168.0.113? Tell 192.168.0.103
5609 774.031600 aa:29:48:0d:17:73 Broadcast ARP 42 Who has 192.168.0.114? Tell 192.168.0.103
5610 774.031600 ba:a9:89:78:af:b0 ARP 42 192.168.0.113 is at ba:a9:89:78:af:b0

> Frame 5604: Packet, 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface er
> Ethernet II, Src: TpLinkTechno_08:e7:16 (c4:6e:1f:08:e7:16), Dst: ba:a9:89:78:af:b0 (ba:a9:89:78:af:b0)
< Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: TpLinkTechno_08:e7:16 (c4:6e:1f:08:e7:16)
  Sender IP address: 192.168.0.1
  Target MAC address: ba:a9:89:78:af:b0 (ba:a9:89:78:af:b0)
  Target IP address: 192.168.0.113

```

Ура! Вроде как MAC адрес роутера нашли и он совпадает с тем, который мы получили через `arp -a`

Команда 3: статистика

--- Статистика за период ---
1. Ethernet фреймов: 123
2. ARP пакетов: 70
3. Уникальных MAC адресов: 4
4. Широковещательных Ethernet: 69
5. Широковещательных ARP: 67
6. Gratuitous ARP: 3
7. ARP targeted pairs (replies): 3
8. Объем данных устройство–роутер (bytes): 18793

Примечание: промежуток времени был выбран 10 секунд

Ответы на вопросы:

- **Почему обнаружено именно столько уникальных MAC?** В локальной сети видны MAC-адреса всех активных устройств, общающихся в данный момент: сетевые интерфейсы роутера, другие компьютеры, смартфоны, IoT-устройства
- **Как рассчитывается объем данных в байтах?** Объем рассчитывается как сумма длин всех Ethernet-фреймов (L2). Он включает заголовок Ethernet, полезную нагрузку (IP/ARP) и Padding, если нагрузка меньше 46 байт

Контрольные вопросы

1. **Для каких целей нужны ARP targeted requests/responses? Какова их структура?**

Они используются для определение MAC адреса у определенного IP адреса. В запросе Target MAC обнулен, в ответе — заполнен.

Структура:

```
Запуск захвата на 10 сек...
[ARP Header (28 bytes)]
Hardware type: 1 (Ethernet (10Mb))
Protocol type: 0x0800 (IPv4)
Hardware address length: 6 [bytes]
Protocol address length: 4 [bytes]
Operation: 1 (REQUEST)
Source hardware address: aa:29:48:0d:17:73
Source protocol address: /192.168.0.103
Destination hardware address: 00:00:00:00:00:00
Destination protocol address: /192.168.0.114
```

2. **Gratuitous ARP:** Запрос, где Source IP = Target IP. Используется для объявления своего присутствия в сети и предотвращения конфликтов адресов.