

Лабораторная работа №3

Сетевые технологии

Андреева Софья Владимировна

Содержание

1 Цель работы	4
2 Выполнение лабораторной работы	5
3 Анализ кадров канального уровня в Wireshark	11
4 Анализ протоколов транспортного уровня в Wireshark	18
5 Анализ handshake протокола TCP в Wireshark	22
6 Вывод	24

Список иллюстраций

2.1	Вывод ipconfig	6
2.2	all	7
2.3	displaydns	9
2.4	Выполнение работы	10
3.1	Выполнение работы	11
3.2	Выполнение работы	11
3.3	Выполнение работы	12
3.4	Выполнение работы	12
3.5	Выполнение работы	12
3.6	Выполнение работы	14
3.7	Выполнение работы	14
3.8	Выполнение работы	15
3.9	Выполнение работы	17
3.10	Выполнение работы	17
4.1	Выполнение работы	18
4.2	Выполнение работы	19
4.3	Выполнение работы	20
4.4	Выполнение работы	21
5.1	Выполнение работы	23
5.2	Выполнение работы	23

1 Цель работы

Изучение посредством Wireshark кадров Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP

2 Выполнение лабораторной работы

Команда ipconfig без параметров выводит базовую информацию о конфигурации IP для всех активных сетевых адаптеров.

Активные сетевые адAPTERы: 1. Адаптер Ethernet Ethernet 2: Локальный IPv6-адрес канала: fe80::6f0c:e354:78f5:8579%4 Это link-local адрес IPv6, автоматически сгенерированный для коммуникации в пределах локальной сети %4 указывает на идентификатор зоны (интерфейс) IPv4-адрес: 192.168.56.1 Частный IP-адрес из диапазона, зарезервированного для сетей класса С Маска подсети: 255.255.255.0 Определяет, что в сети может быть до 254 узлов (192.168.56.1-192.168.56.254) Основной шлюз: не указан. Это характерно для адаптеров, используемых в виртуальных средах (например, VirtualBox Host-Only Network)

2. Адаптер беспроводной локальной сети Беспроводная сеть: Локальный IPv6-адрес канала: fe80::f984:20b8:5632:7cb7%16 Автоматически сгенерированный IPv6 адрес для локальной связи IPv4-адрес: 172.16.70.152 Частный IP-адрес из диапазона 172.16.0.0-172.31.255.255 (класс В) Маска подсети: 255.255.254.0 Нестандартная маска, позволяющая использовать 510 адресов в подсети (172.16.70.0-172.16.71.255) Основной шлюз: 172.16.70.1 Маршрутизатор, через который осуществляется выход в интернет

Три адаптера неактивны - это могут быть виртуальные адаптеры VPN или дополнительные сетевые интерфейсы

Рис. 2.1: Вывод ipconfig

Команда ipconfig /all

Выводит полную информацию о конфигурации всех сетевых адаптеров компьютера. В данном случае отображены следующие адAPTERы

```
PS C:\Users\799668> ipconfig /all

Настройка протокола IP для Windows

Имя компьютера . . . . . : LAPTOP-D0UFRT0J
Основной DNS-суффикс . . . . . :
Тип узла . . . . . : Гибридный
IP-маршрутизация включена . . . . . : Нет
WINS-прокси включен . . . . . : Нет

Адаптер Ethernet Ethernet 2:

DNS-суффикс подключения . . . . . :
Описание . . . . . : VirtualBox Host-Only Ethernet Adapter
Физический адрес . . . . . : 0A-00-27-00-00-04
DHCP включен . . . . . : Нет
Автонастройка включена . . . . . : Да
Локальный IPv6-адрес канала . . . . . : fe80::6f0c:3547:78f5:8579%4(Основной)
IPv4-адрес . . . . . : 192.168.56.1(Основной)
Маска подсети . . . . . : 255.255.255.0
Основной шлюз . . . . . :
IAID DHCPv6 . . . . . : 654966823
DUID клиента DHCPv6 . . . . . : 00-01-00-01-2B-9A-39-C4-C4-75-AB-5D-A6-9C
NetBios через TCP/IP . . . . . : Включен

Адаптер беспроводной локальной сети Подключение по локальной сети* 1:

Состояние среды . . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Физический адрес . . . . . : C4-75-AB-5D-A6-9D
DHCP включен . . . . . : Да
Автонастройка включена . . . . . : Да

Адаптер беспроводной локальной сети Подключение по локальной сети* 2:

Состояние среды . . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
```

Рис. 2.2: all

На основании вывода команды ipconfig /all определены следующие MAC-адреса сетевых интерфейсов:

- ## 1. Адаптер Ethernet Ethernet 2 (VirtualBox Host-Only Ethernet Adapter):

MAC-адрес: 0A-00-27-00-00-04

- ## 2. Адаптер беспроводной локальной сети Беспроводная сеть:

MAC-адрес: C4-75-AB-5D-A6-9D

Структура MAC-адреса: MAC-адрес состоит из 6 байтов (48 битов), представленных в шестнадцатеричной системе:

Первые 3 байта (24 бита): OUI (Organizationally Unique Identifier) - идентификатор производителя

Последние 3 байта (24 бита): Уникальный идентификатор сетевого интерфейса

Анализ конкретных MAC-адресов: 1. Адаптер Ethernet Ethernet 2: 0A-00-27-00-00-04

OUI (производитель): 0A-00-27

Зарегистрирован за Oracle Corporation

Используется для виртуальных адаптеров VirtualBox

Идентификатор интерфейса: 00-00-04

Уникальный номер, назначенный производителем для данного сетевого интерфейса

Анализ типа адреса:

Первый байт: 0A в шестнадцатеричной = 00001010 в двоичной системе

Младший бит первого байта: 0 Индивидуальный (Unicast) адрес

Второй младший бит: 1 Локально администрируемый адрес

2. Адаптер беспроводной сети: C4-75-AB-5D-A6-9D

OUI (производитель): C4-75-AB

Зарегистрирован за Microsoft Corporation

Идентификатор интерфейса: 5D-A6-9D

Уникальный номер сетевого адаптера

Анализ типа адреса:

Первый байт: C4 в шестнадцатеричной = 11000100 в двоичной системе

Младший бит первого байта: 0 Индивидуальный (Unicast) адрес

Второй младший бит: 0 Глобально администрируемый адрес

Команда ipconfig /displaydns

Отображает содержимое DNS-кэша. В данном случае в кэше находятся записи для домена mc.yandex.ru: А-записи: 87.250.251.119, 87.250.250.119, 77.88.21.119 — IP-адреса серверов Яндекса. Дополнительные записи: ns1.yandex.ru и ns2.yandex.ru — DNS-серверы Яндекса. Это означает, что компьютер недавно обращался к сервисам Яндекса, и DNS-записи сохранены в кэше для ускорения последующих запросов.

```
PS C:\Users\79968> ipconfig /displaydns

Настройка протокола IP для Windows

mc.yandex.ru
-----
Имя записи. . . . . : mc.YANDEX.ru
Тип записи. . . . . : 1
Срок жизни. . . . . : 265
Длина данных. . . . . : 4
Раздел. . . . . : Ответ
А-запись (узла) . . . . : 87.250.251.119

Имя записи. . . . . : mc.YANDEX.ru
Тип записи. . . . . : 1
Срок жизни. . . . . : 265
Длина данных. . . . . : 4
Раздел. . . . . : Ответ
А-запись (узла) . . . . : 87.250.250.119

Имя записи. . . . . : mc.YANDEX.ru
Тип записи. . . . . : 1
Срок жизни. . . . . : 265
Длина данных. . . . . : 4
Раздел. . . . . : Ответ
А-запись (узла) . . . . : 77.88.21.119

Имя записи. . . . . : ns2.YANDEX.ru
Тип записи. . . . . : 1
Срок жизни. . . . . : 265
Длина данных. . . . . : 4
Раздел. . . . . : Дополнительно
А-запись (узла) . . . . : 93.158.134.1

Имя записи. . . . . : ns1.YANDEX.ru
Тип записи. . . . . : 1
```

Рис. 2.3: displaydns

Команда ipconfig /showclassid

Отображает все идентификаторы классов DHCP, разрешенные для указанного сетевого адаптера. В данном случае для адаптера “Беспроводная сеть” обнаружены следующие классы DHCPv4.

1. Default Routing and Remote Access Class

Этот класс предназначен для клиентов удаленного доступа (Remote Access).

Используется для маршрутизации и управления удаленным доступом, позволя-

ет применять специальные настройки DHCP для VPN-клиентов и других удаленных подключений

2. Default Network Access Protection Class

Класс для клиентов с ограниченным доступом в рамках технологии Network Access Protection (NAP). NAP - технология безопасности, которая проверяет соответствие клиента политикам безопасности перед предоставлением полного доступа к сети. Клиенты, не прошедшие проверку, получают ограниченный доступ.

3. Default BOOTP Class

Класс для клиентов, использующих протокол BOOTP (Bootstrap Protocol)BOOTP - предшественник DHCP, используется для загрузки бездисковых рабочих станций и сетевых устройств. Современные системы обычно используют DHCP, но поддерживают обратную совместимость.

Наличие этих классов указывает на то, что: Система поддерживает удаленный доступ (VPN и другие технологии Remote Access). Реализованы механизмы безопасности через Network Access Protection. Обеспечена обратная совместимость с устаревшими протоколами (BOOTP). Сетевые политики могут дифференцировать клиентов по типам подключения

```
PS C:\Users\79968> ipconfig /showclassid "Беспроводная сеть"
Настройка протокола IP для Windows

Классы DHCPv4 для адаптера "Беспроводная сеть":

Имя ClassID DHCPv4 . . . . . : Default Routing and Remote Access Class
Описание ClassID DHCPv4 . . . . . : User class for remote access clients

Имя ClassID DHCPv4 . . . . . : Default Network Access Protection Class
Описание ClassID DHCPv4 . . . . . : Default special user class for Restricted Access clients

Имя ClassID DHCPv4 . . . . . : Default BOOTP Class
Описание ClassID DHCPv4 . . . . . : User class for BOOTP Clients
PS C:\Users\79968>
```

Рис. 2.4: Выполнение работы

3 Анализ кадров канального уровня в Wireshark

Запустим Wireshark. Выберем активный на нашем устройстве сетевой интерфейс и убедимся, что начался процесс захвата трафика

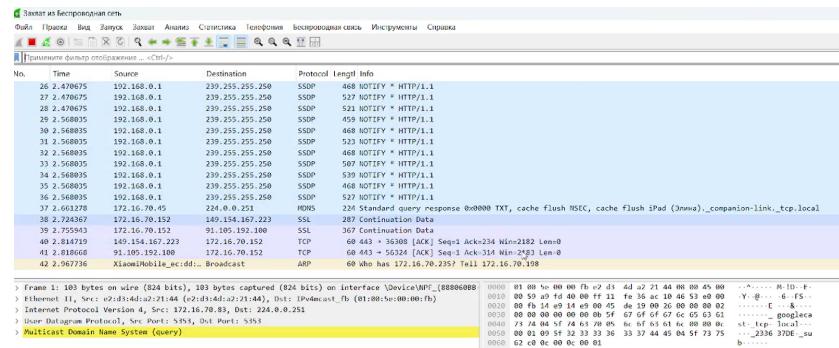


Рис. 3.1: Выполнение работы

На нашем устройстве в консоли определим с помощью команды ipconfig IP-адрес устройства и шлюз по умолчанию

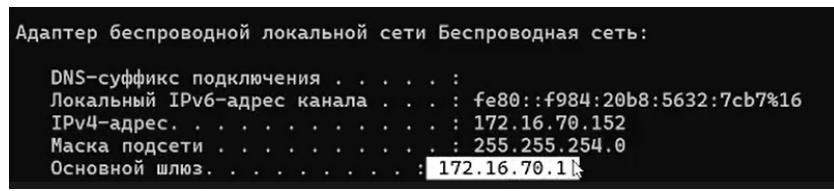


Рис. 3.2: Выполнение работы

На нашем устройстве в консоли с помощью команды `ping` пропингуем шлюз по умолчанию

```
C:\Users\79968>ping 172.16.70.1

Обмен пакетами с 172.16.70.1 по с 32 байтами данных:
Ответ от 172.16.70.1: число байт=32 время=1мс TTL=254
Ответ от 172.16.70.1: число байт=32 время=3мс TTL=254
Ответ от 172.16.70.1: число байт=32 время=2мс TTL=254
Ответ от 172.16.70.1: число байт=32 время=3мс TTL=254

Статистика Ping для 172.16.70.1:
Пакетов: отправлено = 4, получено = 4, потеряно = 0
(0% потеря)
Приблизительное время приема–передачи в мс:
Минимальное = 1мсек, Максимальное = 3 мсек, Среднее = 2 мсек

C:\Users\79968>
```

Рис. 3.3: Выполнение работы

В Wireshark остановим захват трафика. В строке фильтра пропишем фильтр arp or icmp и убедимся, что в списке пакетов отобразились только пакеты ARP или ICMP, в частности пакеты, которые были сгенерированы с помощью команды ping, отправленной с нашего устройства на шлюз по умолчанию.

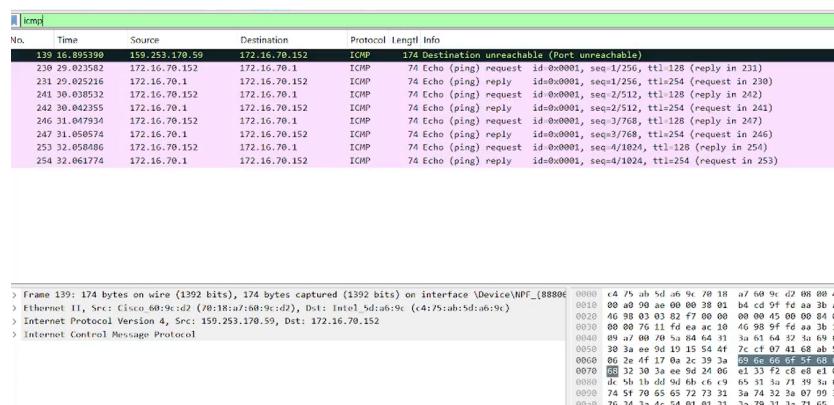


Рис. 3.4: Выполнение работы

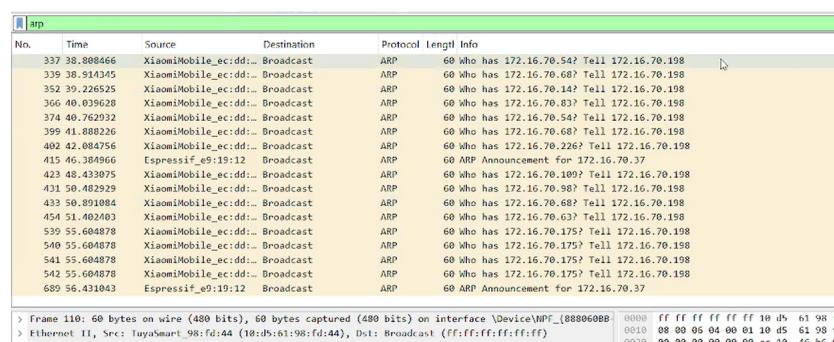


Рис. 3.5: Выполнение работы

Изучим эхо-запрос и эхо-ответ ICMP в программе Wireshark:

ICMP эхо-запрос (Echo Request)

Основные характеристики:

Длина кадра: 74 байта (592 бита)

Тип Ethernet кадра: Ethernet II

Инкапсуляция: Ethernet (1)

MAC-адреса:

Источник (Source): c4:75:ab:5d:a6:9c

Назначение (Destination): 70:18:a7:60:90:42

Анализ MAC-адресов:

Источник: c4:75:ab:5d:a6:9c

OUI: c4:75:ab - Microsoft Corporation

Идентификатор интерфейса: 5d:a6:9c

Тип адреса:

Первый байт с4 = 11000100 в двоичной системе

Младший бит = 0 Индивидуальный (Unicast)

Второй младший бит = 0 Глобально администрируемый

Назначение: 70:18:a7:60:90:42

OUI: 70:18:a7 - Cisco Systems

Тип адреса:

Первый байт 70 = 01110000 в двоичной системе

Младший бит = 0 Индивидуальный (Unicast)

Второй младший бит = 0 Глобально администрируемый

ICMP эхо-ответ (Echo Reply)

Основные характеристики:

Длина кадра: 74 байта (592 бита)

Тип Ethernet кадра: Ethernet II

Инкапсуляция: Ethernet (1)

Протоколы в кадре: eth:ethertype:ip:icmp:data

MAC-адреса:

Источник (Source): 70:18:a7:60:90:42 (Cisco Systems)

Назначение (Destination): c4:75:ab:5d:a6:9c (Microsoft Corporation)

Анализ MAC-адресов:

Источник: 70:18:a7:60:90:42

OUI: 70:18:a7 - Cisco Systems

Идентификатор интерфейса: 60:90:42

Тип адреса: Индивидуальный, глобально администрируемый

Назначение: c4:75:ab:5d:a6:9c

OUI: c4:75:ab - Microsoft Corporation

Тип адреса: Индивидуальный, глобально администрируемый

```
Frame 230: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{888060}
  Section number: 1
  > Interface id: 0 (\Device\NPF_{888060BB-39FF-4F4E-8915-42CE67278D30})
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 29, 2025 18:30:49.868914000 RTZ 2 (зима)
    UTC Arrival Time: Sep 29, 2025 15:30:49.868914000 UTC
    Epoch Arrival Time: 1759159849.868914000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.045772000 seconds]
    [Time delta from previous displayed frame: 12.128192000 seconds]
    [Time since reference or first frame: 29.023582000 seconds]
  Frame Number: 230
  Frame Length: 74 bytes (592 bits)
  Capture Length: 74 bytes (592 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
```

Рис. 3.6: Выполнение работы

```
Frame 231: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{888060}
  Section number: 1
  > Interface id: 0 (\Device\NPF_{888060BB-39FF-4F4E-8915-42CE67278D30})
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 29, 2025 18:30:49.870548000 RTZ 2 (зима)
    UTC Arrival Time: Sep 29, 2025 15:30:49.870548000 UTC
    Epoch Arrival Time: 1759159849.870548000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.001634000 seconds]
    [Time delta from previous displayed frame: 0.001634000 seconds]
    [Time since reference or first frame: 29.025216000 seconds]
  Frame Number: 231
  Frame Length: 74 bytes (592 bits)
  Capture Length: 74 bytes (592 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:etherType:ip:icmp:data]
  [Coloring Rule Name: ICMP]
```

Рис. 3.7: Выполнение работы

Изучим кадры данных протокола ARP. Изучим данные в полях заголовка Ethernet II.

Тип Ethernet кадра: Все ARP-запросы используют Ethernet II с типом 0x0806

MAC-адресация:

Источник: Всегда индивидуальный Unicast адрес запрашивающего устройства

Назначение: Всегда широковещательный адрес ff:ff:ff:ff:ff:ff

Структура сети:

Сеть использует подсеть 172.16.70.0/23 (маска 255.255.254.0)

Основной шлюз: 172.16.70.1

В сети присутствуют устройства различных производителей (Xiaomi и другие)

Назначение ARP-запросов:

Разрешение IP-адресов в MAC-адреса

Обновление ARP-кэшей устройств

Обнаружение новых устройств в сети

Производители устройств:

Xiaomi: OUI 2c:19:5c

Другие устройства: имеют различные OUI, соответствующие их производителям

Данный трафик характерен для нормально функционирующей Ethernet сети, где устройства активно общаются и разрешают адреса через ARP протокол.

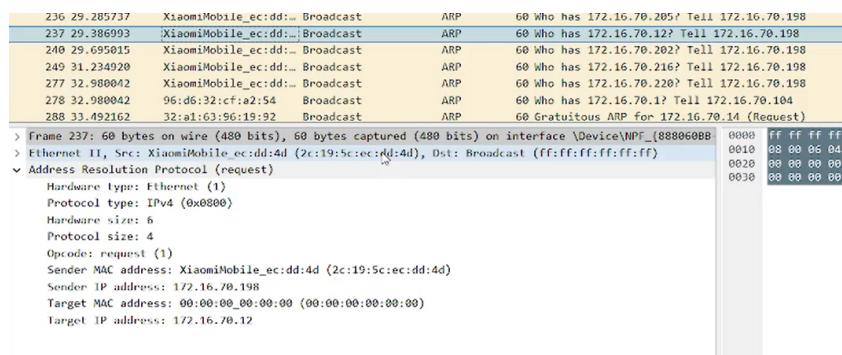


Рис. 3.8: Выполнение работы

Начнём новый процесс захвата трафика в Wireshark. На нашем устройстве в

консоли пропингуем по имени адрес ping www.yandex.com. В Wireshark остановим захват трафика. Изучим запросы и ответы протоколов ARP и ICMP:

Маршрутизация пакетов:

Запрос: Компьютер (172.16.70.152) → Маршрутизатор Cisco → Яндекс (77.88.44.55)

Ответ: Яндекс (77.88.44.55) → Маршрутизатор Cisco → Компьютер (172.16.70.152)

MAC-адресация:

Оба MAC-адреса являются индивидуальными (unicast) и глобально администрируемыми

В локальной сети коммуникация происходит между компьютером и маршрутизатором

NAT преобразование:

Маршрутизатор Cisco выполняет преобразование сетевых адресов (NAT)

Внешний сервер видит запрос от публичного IP маршрутизатора, а не от локального 172.16.70.152

ICMP протокол:

Используется для диагностики сети (ping)

Identifier и Sequence Number позволяют сопоставлять запросы и ответы

32 байта данных используются для проверки целостности передачи

Сетевая инфраструктура:

Локальная сеть: 172.16.70.0/23 (частный диапазон)

Маршрутизатор: Cisco Systems

Конечное устройство: Intel (вероятно, Wi-Fi адаптер)

Внешний сервер: Яндекс (77.88.44.55)

```
> Frame 7599: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{888060BE
> Ethernet II, Src: Intel_5d:a6:9c (c4:75:ab:5d:a6:9c), Dst: Cisco_60:9c:d2 (78:18:a7:60:9c:d2)
> Internet Protocol Version 4, Src: 172.16.70.152, Dst: 77.88.44.55
  ✓ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d50 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LF): 256 (0x0100)
    Sequence Number (BE): 11 (0x000b)
    Sequence Number (LF): 2816 (0x0b80)
    [Response frame: 7599]
    > Data (32 bytes)
```

Рис. 3.9: Выполнение работы

```
> Frame 7600: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{888060BE
  ✓ Ethernet II, Src: Cisco_60:9c:d2 (78:18:a7:60:9c:d2), Dst: Intel_5d:a6:9c (c4:75:ab:5d:a6:9c)
    ✓ Destination: Intel_5d:a6:9c (c4:75:ab:5d:a6:9c)
      .... ..0. .... .... .... = LG bit: Globally unique address (factory default)
      .... ..0. .... .... .... = IG bit: Individual address (unicast)
    ✓ Source: Cisco_60:9c:d2 (78:18:a7:60:9c:d2)
      .... ..0. .... .... .... = LG bit: Globally unique address (factory default)
      .... ..0. .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 4]
  > Internet Protocol Version 4, Src: 77.88.44.55, Dst: 172.16.70.152
  > Internet Control Message Protocol
```

Рис. 3.10: Выполнение работы

4 Анализ протоколов транспортного уровня в Wireshark

На устройстве в браузере перейдём на сайт, работающий по протоколу HTTP (<http://info.cern.ch/>) и поперемещаемся по ссылкам и разделам сайта в браузере. В Wireshark в строке фильтра укажите http и проанализируем информацию по протоколу TCP в случае запросов и ответов.

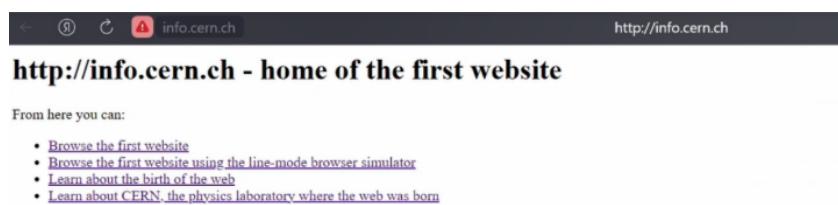


Рис. 4.1: Выполнение работы

1. Успешность соединения: Соединение установлено - трехстороннее рукопожатие завершено

Данные передаются в обоих направлениях

Подтверждения работают - Ack числа корректны

Окно переполнения = 249 - нормальное значение для управления потоком

2. Эффективность передачи: Клиент отправил 508 байт HTTP запроса

Сервер подтвердил получение и отправил 990 байт ответа

Используется PSH-флаг - ускоренная доставка данных приложению

Keep-alive соединение - возможность повторного использования

3. HTTP транзакция:

КЛИЕНТ (172.16.70.152:38569) СЕРВЕР (188.184.67.127:80) |— GET /hypertext/www/TheProject —>| |<— HTTP Response + данные (990 байт) ——|

4. Общий результат: TCP соединение между клиентом и сервером info.cern.ch функционирует корректно и эффективно. HTTP запрос успешно доставлен, сервер обработал его и вернул запрашиваемый ресурс. Сетевое соединение демонстрирует надежную доставку данных с правильным управлением потоком и подтверждением получения

```
> Frame 6522: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface \Device\NPF_{8886
> Ethernet II, Src: Intel_5d:a6:9c (4:75:ab:5d:a6:9c), Dst: Cisco_60:9c:d2 (70:18:a7:60:9c:d2)
> Internet Protocol Version 4, Src: 172.16.70.152, Dst: 188.184.67.127
> Transmission Control Protocol, Src Port: 38569, Dst Port: 80, Seq: 1, Ack: 1, Len: 508
└ Hypertext Transfer Protocol
    > GET /hypertext/www/TheProject.html HTTP/1.1\r\n
        Host: info.cern.ch\r\n
        Connection: keep-alive\r\n
        Upgrade-Insecure-Requests: 1\r\n
        User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/1
        Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
        Referer: http://info.cern.ch/\r\n
        Accept-Encoding: gzip, deflate\r\n
        Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7\r\n
    [Response in frame: 6528]
```

Рис. 4.2: Выполнение работы

В Wireshark в строке фильтра укажем dns и проанализируем информацию по протоколу UDP в случае запросов и ответов

Запрос: Клиент: 172.16.70.152:61538 DNS сервер: 37.18.92.5:53 Размер запроса: 62 байта - компактный запрос Ответ: Размер ответа: 503 байта - близко к лимиту UDP для DNS Содержит: Обычно A-записи, CNAME, NS записи и другую DNS информацию DNS over UDP демонстрирует оптимальное использование бессоединенного протокола для службы разрешения имен. Несмотря на отсутствие гарантий доставки на транспортном уровне, механизмы повторения на уровне приложения обеспечивают достаточную надежность при минимальных задержках.

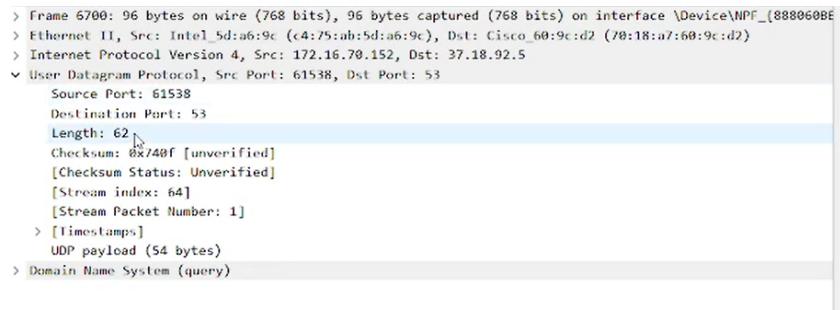


Рис. 4.3: Выполнение работы

Wireshark в строке фильтра укажем quic и проанализируем информацию по протоколу quic в случае запросов и ответов.

QUIC запрос

Ethernet II заголовок: Длина кадра: 74 байта (592 бита) MAC источника: c4:75:ab:5d:a6:9c - Intel Corporate (компьютер) MAC назначения: 70:18:a7:60:9c:d2 - Cisco Systems (маршрутизатор) Тип: 0x0800 - IPv4 IP заголовок: IP источника: 172.16.70.152 - локальный адрес компьютера IP назначения: 173.194.73.198 - сервер Google (видно по IP) UDP заголовок: Исходный порт: 49664 - эфемерный порт клиента Порт назначения: 443 - порт для QUIC (аналогично HTTPS) Длина: 40 байт Данные: 32 байта QUIC

QUIC ответ

MAC назначения: c4:75:ab:5d:a6:9c - Intel (компьютер) MAC источника: 70:18:a7:60:9c:d2 - Cisco (маршрутизатор) Тип адресов: Оба индивидуальные (unicast), глобально администрируемые IP источника: 173.194.73.198 - сервер Google IP назначения: 172.16.70.152 - клиент UDP заголовок: Источник: Порт 443 (QUIC сервер) Назначение: Порт 49664 (клиент) Длина: 33 байта Данные: QUIC payload

```
▼ Ethernet II, Src: Cisco_60:9c:d2 (70:18:a7:60:9c:d2), Dst: Intel_5d:a6:9c (c4:75:ab:5d:a6:9c)
  ▼ Destination: Intel_5d:a6:9c (c4:75:ab:5d:a6:9c)
    .... ..0. .... ..... .... = LG bit: Globally unique address (factory default)
    .... ..0. .... ..... .... = IG bit: Individual address (unicast)
  ▼ Source: Cisco_60:9c:d2 (70:18:a7:60:9c:d2)
    .... ..0. .... ..... .... = LG bit: Globally unique address (factory default)
    .... ..0. .... ..... .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x8000)
  [Stream index: 2]
> Internet Protocol Version 4, Src: 173.194.73.198, Dst: 172.16.70.152
  ▼ User Datagram Protocol, Src Port: 443, Dst Port: 49664
    Source Port: 443
    Destination Port: 49664
    Length: 33
    Checksum: 0x743e [unverified]
    [Checksum Status: Unverified]
    [Stream index: 41]
    [Stream Packet Number: 94]
```

Рис. 4.4: Выполнение работы

5 Анализ handshake протокола TCP в Wireshark

На устройстве используем соединение по HTTP с сайтом CERN для захвата в Wireshark пакетов TCP. В Wireshark проанализируем handshake протокола TCP
ISN сервера: 1066793423 - случайное начальное число ISN клиента: 3100681904
(вычисляется из Ack: 3100681905 - 1)

1. Корректность handshake: SYN-ACK корректно сформирован - флаги и номера верны ISN выбран случайно - защита от предсказуемости Ack Number = ISN_c + 1 - правильное подтверждение SYN
2. Безопасность: Случайные ISN - предотвращение предсказуемости последовательностей Расширенные опции TCP - современные возможности протокола
3. Производительность: Оптимальный размер заголовка - 32 байта с необходимыми опциями Подготовка к быстрой передаче - установка параметров окна
4. Сетевые характеристики: Сервис: CERN через HTTP - зашифрованная коммуникация Порт 443: Стандартный для защищенных веб-сервисов Стабильное соединение: Нет признаков проблем с сетью

```
Frame 34068: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{8880
Ethernet II, Src: Cisco 60:9c:d2 (78:18:a7:60:9c:d2), Dst: Intel 5d:a6:9c (4:75:ab:5d:a6:9c)
Internet Protocol Version 4, Src: 149.154.167.222, Dst: 172.16.70.152
Transmission Control Protocol, Src Port: 443, Dst Port: 53678, Seq: 0, Ack: 1, Len: 0
    Source Port: 443
    Destination Port: 53678
    [Stream index: 47]
    [Stream Packet Number: 2]
> [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 0      (relative sequence number)
    Sequence Number (raw): 1060/93423
    [Next Sequence Number: 1      (relative sequence number)]
    Acknowledgment Number: 1      (relative ack number)
    Acknowledgment number (raw): 3100681995
    1000 .... = Header length: 32 bytes (8)
▼ Flags: 0x012 (SYN, ACK)
    0000 .... .... = Reserved: Not set
```

Рис. 5.1: Выполнение работы

В Wireshark в меню «Статистика» выберем «График Потока»

Анализ TCP-записей в Wireshark показывает установление и поддержание сетевых соединений между клиентами и серверами.

Примеры : - TCP: 22854 – 443 [ACK] — подтверждение установления соединения с веб-сервером (порт 443) - Seq=1 Ack=1 Win=509 — начальные номера последовательностей и размер окна - Len=1 — передача 1 байта данных (keep-alive) - SLE=1 — использование Selective Acknowledgment - TLSv1.2: Application Data — зашифрованный трафик поверх TCP - Win=16385 — увеличенное окно для высокоскоростной передачи TLS-данных

Записи демонстрируют фазы TCP-коммуникации: handshake, передача данных, подтверждения и управление потоком через размеры окон.

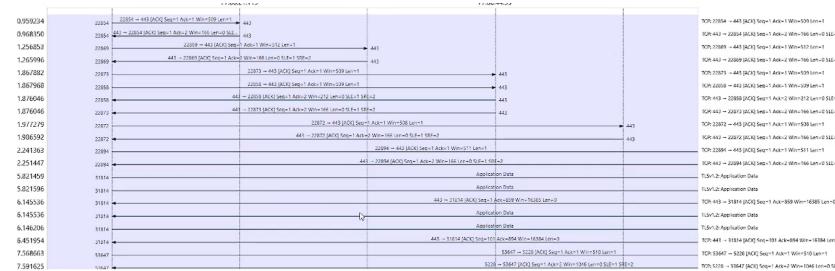


Рис. 5.2: Выполнение работы

6 Вывод

В ходе выполнения лабораторной работы мы изучили посредством Wireshark кадров Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP.