Отчёт по лабораторной работе №3

Сетевые технологии

Бызова Мария Олеговна

Содержание

# 1. Цель работы

Целью данной работы является изучение посредством Wireshark кадров Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP.

# 2. Выполнение лабораторной работы

## 2.1 MAC-адресация

С помощью команды ipconfig выведем информацию о текущем сетевом соединении ([рис. 1](#fig-001)).

|  |
| --- |
| Рисунок 1: Вывод информации о текущем сетевом соединении. |

Анализ вывода команды ipconfig показывает текущую конфигурацию сетевых интерфейсов системы. Адаптер “Ethernet 2” имеет статическую или автоматически назначенную конфигурацию в частной сети 192.168.56.0/24, о чём свидетельствует IPv4-адрес 192.168.56.1 с маской подсети 255.255.255.0; наличие адреса .1 может указывать на то, что данный компьютер выполняет роль шлюза или сервера (например, для виртуальной машины), при этом основной шлюз для этого интерфейса не задан, что ограничивает маршрутизацию за пределы локальной подсети. Основным активным сетевым подключением является “Беспроводная сеть”, которое успешно получило параметры от сети учреждения “rudn.ru” через DHCP: назначен IPv4-адрес 192.168.214.191 с маской подсети 255.255.224.0 (что соответствует сети 192.168.192.0/19) и основным шлюзом 192.168.192.1, что обеспечивает полноценный доступ в сеть и интернет. Остальные интерфейсы, включая основные проводные адаптеры “Ethernet” и “Подключение по локальной сети”, адаптеры виртуальных сетей (OpenVPN Connect DCO Adapter) и временные беспроводные профили, находятся в состоянии “Среда передачи недоступна”, что означает отсутствие физического подключения к сети или отключение адаптера на данный момент.

Теперь используем разные опции команды ([рис. 2](#fig-002) - [рис. 3](#fig-003)).

|  |
| --- |
| Рисунок 2: Отображение полной конфигурации TCP/IP для всех адаптеров. |

Анализ расширенного вывода команды ipconfig позволяет детализировать конфигурацию сетевых интерфейсов. Общая информация о системе указывает, что узел с именем DESKTOP-UR4UATB не состоит в домене (отсутствует основной DNS-суффикс), использует гибридный тип узла, что предполагает использование как локального файла hosts, так и DNS-сервера, при этом IP-маршрутизация отключена, а порядок просмотра DNS суффиксов настроен на домен rudn.ru. Основным и единственным активным интерфейсом, обеспечивающим сетевое подключение, является физический беспроводной адаптер “Беспроводная сеть” (Intel(R) Wi-Fi 6 AX201), который успешно получил через DHCP в сети университета rudn.ru IPv4-адрес 192.168.214.191/19 (маска 255.255.224.0) с основным шлюзом 192.168.192.1 и DNS-серверами 192.168.80.63 и 37.18.92.6; срок аренды адреса действителен. Виртуальный адаптер “Ethernet 2” (VirtualBox Host-Only) имеет статически назначенный адрес 192.168.56.1/24, выполняя роль хоста для виртуальных машин в изолированной сети, без доступа вовне (шлюз не указан), и использует для IPv6 специальные DNS-серверы fec0::ffff.

Остальные интерфейсы неактивны в данный момент. Физический проводной адаптер “Ethernet” (Intel(R) Ethernet Connection I219-LM) и адаптер Bluetooth ожидают подключения, о чём свидетельствует состояние “Среда передачи недоступна”. Сетевое программное обеспечение представлено виртуальными адаптерами: “OpenVPN Connect DCO Adapter” и два адаптера “TAP-Windows” и “OpenVPN Connect DCO”, которые не инициализированы (отсутствует среда передачи или физический адрес), что типично для неподключенного VPN-клиента. Дополнительно присутствуют два виртуальных адаптера “Microsoft Wi-Fi Direct Virtual Adapter”, созданные для прямой беспроводной связи, которые также не задействованы. Таким образом, работоспособное сетевое подключение осуществляется исключительно через беспроводной интерфейс в корпоративной сети университета.

|  |
| --- |
| Рисунок 3: Отображение содержимого кэша сопоставителя DNS-клиента, включающее как записи, предварительно загруженные из локального файла Hosts, так и все недавно полученные записи ресурсов для запросов имен, разрешенных компьютером. |

Кэш DNS содержит записи, свидетельствующие о недавней сетевой активности системы. Преобладают домены, связанные с фоновой работой установленного программного обеспечения. Значительная часть записей принадлежит сервисам антивируса Касперского (ds.kaspersky.com, dc1-file.ksn.kaspersky-labs.com, dc1-st.ksn.kaspersky-labs.com), что указывает на его активное взаимодействие с облачной инфраструктурой для проверки угроз. Наличие записей Microsoft (array622.prod.do.dsp.mp.microsoft.com, login.live.com) характерно для работы операционной системы Windows, служб обновления и аутентификации. Домен edgedl.me.gvt1.com ассоциируется с загрузкой компонентов браузера Microsoft Edge. Специальная запись ipv4only.arpa используется для обнаружения поддержки IPv6. Все CNAME и A-записи имеют актуальный срок жизни, кэш функционирует нормально, отображая стандартную фоновую активность ОС.

|  |
| --- |
| Рисунок 4: Инициализация динамической регистрации вручную для DNS-имен и IP-адресов, настроенных на компьютере |

Команда ipconfig /registerdns была успешно выполнена. Данная команда инициирует принудительную отправку запросов на регистрацию и обновление всех DNS-записей (как A, так и PTR) для данного компьютера на настроенных DNS-серверах. Это стандартная процедура для динамического обновления информации о хосте в DNS-зоне, что может потребоваться после изменения IP-адреса или для устранения проблем с сетевым именем. Система указывает, что отчёт об ошибках, если они возникнут в процессе фоновой регистрации, будет доступен в оснастке «Просмотр событий» Windows через 15 минут.

|  |
| --- |
| Рисунок 5: Отображение идентификатора класса DHCP для указанного адаптера. |

Результат выполнения команды ipconfig /showclassid \* указывает на отсутствие на данном компьютере настроенных классов идентификатора DHCP (DHCP Class ID). Для большинства сетевых адаптеров, включая основные проводные (“Подключение по локальной сети”, “Ethernet”), беспроводные, Bluetooth и виртуальные (OpenVPN), система возвращает ошибку “Не удается найти указанный файл”, что стандартно означает, что для этих интерфейсов не задан пользовательский класс DHCP. Для адаптеров “Ethernet 2” (VirtualBox Host-Only) и “Беспроводная сеть” явно указано, что классы DHCPv4 не определены, что является ожидаемым поведением, поскольку эти идентификаторы обычно используются в корпоративных сетях для применения специальных политик и на персональных компьютерах, как правило, не настраиваются. Вывод подтверждает, что конфигурация сетевых интерфейсов использует стандартные параметры DHCP без специализированных идентификаторов классов.

Определим MAC-адреса сетевых интерфейсов на нашем компьютере с помощью команды GETMAC ([рис. 6](#fig-006)).

|  |
| --- |
| Рисунок 6: Определение MAC-адреса сетевых интерфейсов на нашем компьютере. |

Из вывода команды GETMAC и раздела сведений о сетевом подключении были идентифицированы следующие физические адреса:

00-93-37-00-28-DC – Основной беспроводной адаптер (Intel Wi-Fi 6 AX201).

00-93-37-00-28-E0 – Адаптер Bluetooth.

A0-36-BC-6B-61-DE – Проводной сетевой адаптер (Intel Ethernet).

0A-00-27-00-00-0D – Виртуальный адаптер VirtualBox (указан в предыдущих выводах как “Ethernet 2”).

00-FF-AD-94-98-8E – Виртуальный адаптер TAP-Windows для OpenVPN.

1. Анализ структуры MAC-адреса на примере 00-93-37-00-28-DC

MAC-адрес имеет длину 48 бит и записывается в шестнадцатеричном формате. Его структура регламентируется стандартом IEEE 802.

Первые 3 байта (OUI - Organizationally Unique Identifier): 00-93-37 Эта часть адреса уникально идентифицирует производителя сетевого оборудования. В данном случае код 00-93-37 принадлежит компании Intel Corporation.

Последние 3 байта (NIC - Network Interface Controller): 00-28-DC Эта часть адреса назначается производителем и уникально идентифицирует конкретный сетевой интерфейс (контроллер) в рамках продукции этого вендора.

1. Классификация MAC-адреса 00-93-37-00-28-DC

Индивидуальный (Unicast) или Групповой (Multicast): Определяется младшим битом самого первого байта адреса.

Первый байт: 00 (шестнадцатеричный) = 0000 0000 (двоичный).

Младший бит (самый правый бит в этом байте) равен 0.

Вывод: Адрес является индивидуальным (Unicast). Это означает, что кадры данных, отправленные на этот адрес, предназначены только для одного конкретного сетевого интерфейса.

Глобально администрируемый (Universally Administered) или Локально администрируемый (Locally Administered): Определяется вторым младшим битом самого первого байта адреса.

Первый байт: 00 (шестнадцатеричный) = 0000 0000 (двоичный).

Второй младший бит равен 0.

Вывод: Адрес является глобально администрируемым (UAA - Universally Administered Address). Это означает, что адрес был “прошит” производителем оборудования (Intel) и является уникальным в глобальном масштабе.

Итоговый вывод:

MAC-адрес 00-93-37-00-28-DC является индивидуальным (Unicast) и глобально администрируемым (UAA), постоянным адресом, назначенным производителем Intel для конкретного беспроводного сетевого адаптера этого компьютера.

## 2.2 Анализ кадров канального уровня в Wireshark

Установим на нашем устройстве Wireshark ([рис. 7](#fig-007)).

|  |
| --- |
| Рисунок 7: Установка на нашем устройстве Wireshark. |

Запустим Wireshark. Выберем активный на нашем устройстве сетевой интерфейс и убедимся, что начался процесс захвата трафика ([рис. 8](#fig-008)).

|  |
| --- |
| Рисунок 8: Запуск Wireshark. Выбор активного сетевого интерфейса. |

На нашем устройстве в консоли определим с помощью команды ipconfig IP-адрес устройства и шлюз по умолчанию ([рис. 9](#fig-009)).

|  |
| --- |
| Рисунок 9: Определение IP-адреса устройства и шлюза по умолчанию. |

На нашем устройстве в консоли с помощью команды ping пропингуем шлюз по умолчанию ([рис. 10](#fig-010)).

|  |
| --- |
| Рисунок 10: Пинг шлюза по умолчанию. |

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. 11](#fig-011)).

|  |
| --- |
| Рисунок 11: Остановка захвата трафика. Фильтр arp or icmp. |

Изучим эхо-запрос и эхо-ответ ICMP в программе Wireshark ([рис. 12](#fig-012) - [рис. 13](#fig-013)).

|  |
| --- |
| Рисунок 12: Кадр ICMP — эхо-запрос. |

|  |
| --- |
| Рисунок 13: Кадр ICMP — эхо-ответ. |

Эхо-запрос ICMP:

* Длина кадра: 74 байта
* Тип Ethernet: Ethernet II
* MAC-адрес источника: 00:93:37:00:28:46 (Intel)
* MAC-адрес получателя: 70:18:07:00:9c:0b (Cisco)
* Тип адресов: индивидуальные, глобально администрируемые

Эхо-ответ ICMP:

* Длина кадра: 74 байта
* Тип Ethernet: Ethernet II
* MAC-адрес источника: 70:18:07:00:9c:0b (Cisco)
* MAC-адрес получателя: 00:93:37:00:28:46 (Intel)
* Тип адресов: индивидуальные, глобально администрируемые

Изучим кадры данных протокола ARP и данные в полях заголовка Ethernet II ([рис. 14](#fig-014)).

|  |
| --- |
| Рисунок 14: Изучение кадров данных протокола ARP и данных в полях заголовка Ethernet II. |

ARP-пакет (Gratuitous ARP Reply):

* Тип операции: Reply (2)
* Аппаратный тип: Ethernet (1)
* Протокольный тип: IPv4 (0x0800)
* Отправитель: MAC 14:13:33:f2:1d:cc, IP 192.168.201.226
* Получатель: MAC 14:13:33:f2:1d:cc, IP 192.168.201.226
* Назначение: объявление своего MAC-адреса в сети

Ethernet II заголовок:

* MAC назначения: ff:ff:ff:ff:ff:ff (широковещательный)
* MAC источника: 7c:0e:ce:63:c1:60 (Cisco)
* Тип: 0x0806 (ARP протокол)
* Тип адресов: широковещательный (destination), индивидуальный (source)

Начнём новый процесс захвата трафика в Wireshark. На нашем устройстве в консоли пропингуем по имени адрес ping vk.com ([рис. 15](#fig-015)).

|  |
| --- |
| Рисунок 15: Пингуем по имени адрес vk.com. |

В Wireshark остановим захват трафика. Изучим запросы и ответы протоколов ARP и ICMP ([рис. 16](#fig-016) - [рис. 17](#fig-017)).

|  |
| --- |
| Рисунок 16: Кадр ICMP — эхо-запрос. |

|  |
| --- |
| Рисунок 17: Кадр ICMP — эхо-ответ. |

ICMP запрос и ответ для vk.com:

* Запрос (39403):
  + MAC источника: 00:93:37:00:28:46 (Intel)
  + MAC получателя: 70:18:07:00:9c:0b (Cisco)
  + Тип адресов: индивидуальные, глобально администрируемые
* Ответ (39409):
  + MAC источника: 70:18:07:00:9c:0b (Cisco)
  + MAC получателя: 00:93:37:00:28:46 (Intel)
  + Тип адресов: индивидуальные, глобально администрируемые

ARP-пакеты: - MAC источника: 7c:0e:ce:63:c1:60 (Cisco) - MAC назначения: ff:ff:ff:ff:ff:ff (широковещательный) - Тип: Gratuitous ARP для объявления адресов в сети

## 2.3 Анализ протоколов транспортного уровня в Wireshark

Запустим Wireshark. Выберем активный на нашем устройстве сетевой интерфейс и убедимся, что начался процесс захвата трафика ([рис. 18](#fig-018)).

|  |
| --- |
| Рисунок 18: Запуск Wireshark. Выбор активного сетевого интерфейса. |

На устройстве в браузере перейдём на сайт, работающий по протоколу HTTP (http://httpbin.org/) и поперемещаемся по ссылкам и разделам сайта в браузере ([рис. 19](#fig-019)).

|  |
| --- |
| Рисунок 19: Открытие в браузере сайта |

В Wireshark в строке фильтра укажем http и проанализируем информацию по протоколу TCP в случае запросов и ответов ([рис. 20](#fig-020) - [рис. 21](#fig-021)).

|  |
| --- |
| Рисунок 20: Анализ информации по протоколу TCP |

|  |
| --- |
| Рисунок 21: Анализ информации по протоколу TCP |

HTTP запрос и ответ для httpbin.org:

* Запрос (42622):
  + MAC источника: 00:93:37:00:28:dc (Intel)
  + MAC получателя: 76:81:8d:19:ae:eb
  + IP источника: 10.193.235.206
  + IP назначения: 44.210.206.228
  + Порт источника: 50906
  + Порт назначения: 80
  + Метод: GET / HTTP/1.1
  + Тип адресов: индивидуальные, глобально администрируемые
* Ответ (43247):
  + MAC источника: 76:81:8d:19:ae:eb
  + MAC получателя: 00:93:37:00:28:dc (Intel)
  + IP источника: 44.210.206.228
  + IP назначения: 10.193.235.206
  + Порт источника: 80
  + Порт назначения: 50910
  + Статус: Continuation (передача данных)
  + Тип адресов: индивидуальные, глобально администрируемые

Дополнительная информация:

* Используется VLAN (802.1Q) с ID: 0
* Время между запросом и ответом: ~6.3 секунды
* Протоколы в кадрах: eth:ethertype::vlan:ethertype::ip::tcp::http::data

В Wireshark в строке фильтра укажем dns и проанализируем информацию по протоколу UDP в случае запросов и ответов ([рис. 22](#fig-022) - [рис. 23](#fig-023)).

|  |
| --- |
| Рисунок 22: Анализ информации по протоколу UDP. |

|  |
| --- |
| Рисунок 23: Анализ информации по протоколу UDP. |

DNS запрос и ответ для httpbin.org:

* Запрос (1573):
  + MAC источника: 00:93:37:00:28:dc (Intel)
  + MAC получателя: 70:18:37:00:9c:eb (Cisco)
  + IP источника: 192.168.214.191
  + IP назначения: 192.168.80.63
  + Порт источника: 62253
  + Порт назначения: 53
  + Тип: Standard query
  + Запрос: A-запрос для httpbin.org
  + Протокол: UDP
* Ответ (1575):
  + MAC источника: 70:18:37:00:9c:eb (Cisco)
  + MAC получателя: 00:93:37:00:28:dc (Intel)
  + IP источника: 192.168.80.63 (DNS-сервер)
  + IP назначения: 192.168.214.191
  + Порт источника: 53
  + Порт назначения: 62253
  + Тип: Standard query response
  + Ответ: A-запись для httpbin.org
  + Протокол: UDP

Характеристики DNS-трафика:

* Используется протокол UDP для быстрого разрешения имен
* Порт 53 - стандартный порт для DNS-сервиса
* Время между запросом и ответом: ~0.018 секунд
* Размер запроса: 71 байт
* Размер ответа: 167 байт
* Тип запроса: A-запрос (получение IPv4-адреса)

В Wireshark в строке фильтра укажем quic и проанализируем информацию по протоколу quic в случае запросов и ответов ([рис. 24](#fig-024) - [рис. 25](#fig-025)).

|  |
| --- |
| Рисунок 24: Анализ информации по протоколу QUIC. |

|  |
| --- |
| Рисунок 25: Анализ информации по протоколу QUIC. |

QUIC соединение для установки безопасного подключения:

* Инициирующие пакеты от клиента (58208, 58209):
  + MAC источника: 00:93:37:00:28:dc (Intel)
  + MAC получателя: 70:18:47:00:9c:db (Cisco)
  + IP источника: 192.168.214.191
  + IP назначения: 173.194.178.225
  + Порт источника: 57781
  + Порт назначения: 443
  + Тип: Initial packets
  + DCID: 6945764x144356c (Destination Connection ID)
  + Флаги: PRM (Packet Number)
  + Содержимое: PADDING, PTNG, CRYPTO (рукопожатие)
  + Длина: 1292 байта
* Ответ от сервера (58212):
  + MAC источника: 70:18:47:00:9c:db (Cisco)
  + MAC получателя: 00:93:37:00:28:dc (Intel)
  + IP источника: 173.194.178.225
  + IP назначения: 192.168.214.191
  + Порт источника: 443
  + Порт назначения: 57781
  + Тип: Initial packet
  + DCID: 6945764x144356c
  + Флаги: PRM: 3, ACK (подтверждение)
  + Длина: 82 байта

Характеристики QUIC-трафика:

* Протокол: QUIC поверх UDP
* Порт 443 - стандартный для HTTPS/QUIC
* Используется для быстрого установления безопасного соединения
* Время между запросом и ответом: ~0.002 секунд
* Поддержка мультиплексирования потоков

## 2.4 Анализ handshake протокола TCP в Wireshark

Запустим Wireshark. Выберем активный на нашем устройстве сетевой интерфейс и убедимся, что начался процесс захвата трафика ([рис. 26](#fig-026)).

|  |
| --- |
| Рисунок 26: Запуск Wireshark. Выбор активного сетевого интерфейса. |

На устройстве используем соединение по HTTP с сайтом для захвата в Wireshark пакетов TCP ([рис. 27](#fig-027)).

|  |
| --- |
| Рисунок 27: Использование соединения по HTTP с сайтом |

В Wireshark проанализируем handshake протокола TCP ([рис. 28](#fig-028) - [рис. 30](#fig-030)).

|  |
| --- |
| Рисунок 28: Анализ handshake протокола TCP. |

|  |
| --- |
| Рисунок 29: Анализ handshake протокола TCP. |

|  |
| --- |
| Рисунок 30: Анализ handshake протокола TCP. |

TCP handshake и установление соединения:

* SYN от клиента (2108):
  + Порт клиента: 55724 → Порт сервера: 80
  + Флаг: [SYN]
  + Seq=0, Win=64240
  + Параметры: MSS=1460, WS=256, SACK\_PERM
  + Назначение: инициация TCP-соединения
* SYN-ACK от сервера (2113):
  + Порт сервера: 80 → Порт клиента: 55724
  + Флаг: [SYN, ACK]
  + Seq=0, Ack=1, Win=26883
  + Параметры: MSS=1460, WS=256, SACK\_PERM
  + Назначение: подтверждение соединения и синхронизация
* ACK от клиента (2114):
  + Порт клиента: 55724 → Порт сервера: 80
  + Флаг: [ACK]
  + Seq=1, Ack=1, Win=131328
  + Назначение: подтверждение установления соединения

Параллельные соединения:

* Дополнительные порты: 55725, 55726
* Время установления: ~0.167 секунд между SYN и SYN-ACK
* Используется механизм SACK (Selective Acknowledgment)

Статистика потока TCP:

* Успешное трехстороннее рукопожатие (3-way handshake)
* Несколько подключений для параллельной загрузки
* Поддержка масштабирования окна (Window Scaling)

В Wireshark в меню «Статистика» выберем «График Потока» ([рис. 31](#fig-031)).

|  |
| --- |
| Рисунок 31: График потока. |

1. Начало установки соединения (Трехстороннее рукопожатие):

* SYN (55646 -> 443): Клиент (55646) отправляет пакет SYN серверу (443). Seq=0 указывает на начальный номер последовательности. Win=64240 указывает на размер окна приема клиента. MSS=1460 - максимальный размер сегмента, который клиент готов принять.
* SYN, ACK (55647 -> 443): Сервер (443) отвечает пакетом SYN, ACK. Seq=0 указывает на начальный номер последовательности сервера. Ack=1 подтверждает получение SYN от клиента (Ack=номер последовательности SYN клиента + 1). Win=42340 - размер окна приема сервера.
* ACK (55646 -> 443): Клиент отвечает пакетом ACK, подтверждая получение SYN, ACK от сервера. Seq=1 (начальный Seq клиента + 1). Ack=1 (начальный Seq сервера + 1). Win=131328. Соединение установлено.

1. Обмен данными:

* После установки соединения начинается обмен данными, о чем свидетельствуют пакеты “Application Data”. После них идут ACK пакеты.
* Seq (Sequence Number): Указывает на номер первого байта данных в пакете. После каждого отправленного пакета данных Seq увеличивается на размер отправленных данных.
* Ack (Acknowledgment Number): Указывает на следующий байт, который отправитель ожидает получить от получателя. Ack динамически обновляется на основе полученных данных. Он указывает на то, что все байты до значения Ack успешно получены.
* Win (Window Size): Указывает размер окна приема отправителя, т.е. сколько данных он готов принять в данный момент. Это значение может меняться в зависимости от загруженности сети и доступных ресурсов.

1. TLS Handshake:

После установки TCP соединения начинается TLS Handshake, о чем свидетельствуют пакеты “Client Hello” и “Server Hello”. Это согласование параметров шифрования и аутентификации для безопасной передачи данных.

1. TCP Retransmission:

Внизу графика присутствует пакет [TCP Retransmission]. Это означает, что один из пакетов не был доставлен вовремя или был поврежден, и TCP протокол выполнил повторную отправку этого пакета.

Ключевые изменения в значениях при установлении TCP-соединения:

* SYN: Установка начальных номеров последовательности (Seq) и объявление размера окна приема (Win).
* SYN, ACK: Подтверждение установки соединения и объявление начального номера последовательности сервера.
* ACK: Окончательное подтверждение установки соединения и начало обмена данными.
* Seq и Ack: Динамическое изменение номеров последовательности и подтверждений в зависимости от передачи данных.
* Win: Динамическое изменение размера окна приема в зависимости от доступных ресурсов.

# 3. Выводы

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