

Сетевые технологии

Лабораторная работа №3

Элсаиед Адел

19 января 2026

Российский университет дружбы народов, Москва, Россия

Цель и задачи работы

Цель лабораторной работы

Изучение кадров Ethernet и анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP с использованием Wireshark.

Ход выполнения работы

Вывод параметров подключения (ipconfig /all)

- Определены параметры интерфейса Wi-Fi
- Зафиксированы DHCP/DNS и срок аренды
- Получены IPv4/IPv6 адреса, маска, шлюз по умолчанию

```
Адаптер беспроводной локальной сети Беспроводная сеть:
```

```
DNS-суффикс подключения . . . . . : 
Описание . . . . . : Intel(R) Wi-Fi 6E AX211 160MHz
Физический адрес . . . . . : F8-FE-5E-6F-7B-EC
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . . . : fe80::da3b:4057:9ef4:1e28%7(Основной)
IPv4-адрес . . . . . : 192.168.1.69(Основной)
Маска подсети . . . . . : 255.255.255.0
Аренда получена. . . . . : 19 января 2026 г. 11:23:48
Срок аренды истекает. . . . . : 20 января 2026 г. 11:23:46
Основной шлюз. . . . . : 192.168.1.1
DHCP-сервер. . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 133758558
DUID клиента DHCPv6 . . . . . : 00-01-00-01-30-47-94-1A-10-FF-E0-21-D6-B4
DNS-серверы. . . . . : 192.168.1.1
NetBIOS через TCP/IP. . . . . : Включен
```

Основные параметры сети

- IPv4-адрес: **192.168.1.69**
- Маска: **255.255.255.0**
- Шлюз по умолчанию: **192.168.1.1**
- DNS/DHCP: **192.168.1.1**
- MAC (Wi-Fi): **F8-FE-5E-6F-7B-EC**

Проверка доступности шлюза (ping)

- Выполнен ping 192.168.1.1
- Потерь пакетов нет, задержка < 1 мс
- Связность в локальном сегменте подтверждена

```
PS C:\Users\Adel\Documents> ping 192.168.1.1

Обмен пакетами с 192.168.1.1 по с 32 байтами данных:
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время=1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время=1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=64

Статистика Ping для 192.168.1.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
              (0% потеря)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 1 мсек, Среднее = 0 мсек
PS C:\Users\Adel\Documents>
```

Рис. 2: ping 192.168.1.1

Структура MAC-адреса

Пример: F8-FE-5E-6F-7B-EC - OUI (производитель): F8-FE-5E (первые 24 бита) - NIC (интерфейс): 6F-7B-EC (последние 24 бита)

Определение типа по первому октету F8 = 11111000: - I/G (bit0) = 0 → unicast - U/L (bit1) = 0
→ **globally administered**

Фильтрация трафика и ICMP Echo Request

- ICMP Echo Request к шлюзу:
 - Ethernet II
 - Длина кадра: 74 bytes
 - Src MAC: f8:fe:5e:6f:7b:ec
 - Dst MAC: c8:7f:54:78:b6:f2

No.	Time	Source	Destination	Protocol	Length Info
26	6.485226	a2:1f:8e:51:22:03	Broadcast	ARP	42 Who has 192.168.1.1? Tell 192.168.1.1
40	11.743931	ASUSTekCOMPU_78:b6:...	Intel_6f:7b:ec	ARP	46 Who has 192.168.1.69? Tell 192.168.1.69
41	11.743962	Intel_6f:7b:ec	ASUSTekCOMPU_78:b6:...	ARP	42 192.168.1.69 is at f8:fe:5e:6f:7b:ec
→	239 24.146270	192.168.1.69	192.168.1.1	ICMP	74 Echo (ping) request id=0x0001, seq=1
←	240 24.147153	192.168.1.1	192.168.1.69	ICMP	78 Echo (ping) reply id=0x0001, seq=1
247	25.157390	192.168.1.69	192.168.1.1	ICMP	74 Echo (ping) request id=0x0001, seq=2
248	25.158336	192.168.1.1	192.168.1.69	ICMP	78 Echo (ping) reply id=0x0001, seq=2
251	26.170340	192.168.1.69	192.168.1.1	ICMP	74 Echo (ping) request id=0x0001, seq=3
252	26.171444	192.168.1.1	192.168.1.69	ICMP	78 Echo (ping) reply id=0x0001, seq=3
260	27.184725	192.168.1.69	192.168.1.1	ICMP	74 Echo (ping) request id=0x0001, seq=4
261	27.185433	192.168.1.1	192.168.1.69	ICMP	78 Echo (ping) reply id=0x0001, seq=4
558	58.078856	ASUSTekCOMPU_78:b6:...	Intel_6f:7b:ec	ARP	46 Who has 192.168.1.69? Tell 192.168.1.69
559	58.078888	Intel_6f:7b:ec	ASUSTekCOMPU_78:b6:...	ARP	42 192.168.1.69 is at f8:fe:5e:6f:7b:ec
597	66.592141	a2:1f:8e:51:22:03	Broadcast	ARP	42 Who has 192.168.1.1? Tell 192.168.1.1
906	105.949471	ASUSTekCOMPU_78:b6:...	Intel_6f:7b:ec	ARP	46 Who has 192.168.1.69? Tell 192.168.1.69
907	105.949501	Intel_6f:7b:ec	ASUSTekCOMPU_78:b6:...	ARP	42 192.168.1.69 is at f8:fe:5e:6f:7b:ec

Frame 239: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{3A 0000 c
Ethernet II, Src: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec), Dst: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2) 0010 e
Destination: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2) 0020 e
0 = 16 bit: Globally unique address (factory default) 0030 e

ICMP Echo Reply

- ICMP Echo Reply от шлюза:
 - Длина кадра: 78 bytes
 - Ethernet II (фиксируется 802.1Q VLAN в деталях)
 - Src MAC: c8:7f:54:78:b6:f2
 - Dst MAC: f8:fe:5e:6f:7b:ec

No.	Time	Source	Destination	Protocol	Length Info
40	11.743931	ASUSTekCOMPU_78:b6:...	Intel_6f:7b:ec	ARP	46 Who has 192.168.1.69? Tell 192.168.1.69
41	11.743962	Intel_6f:7b:ec	ASUSTekCOMPU_78:b6:...	ARP	42 192.168.1.69 is at f8:fe:5e:6f:7b:e
→ 239	24.146270	192.168.1.69	192.168.1.1	ICMP	74 Echo (ping) request id=0x0001, seq=1
← 240	24.147153	192.168.1.1	192.168.1.69	ICMP	78 Echo (ping) reply id=0x0001, seq=1
247	25.157390	192.168.1.69	192.168.1.1	ICMP	74 Echo (ping) request id=0x0001, seq=2
248	25.158336	192.168.1.1	192.168.1.69	ICMP	78 Echo (ping) reply id=0x0001, seq=2
251	26.170340	192.168.1.69	192.168.1.1	ICMP	74 Echo (ping) request id=0x0001, seq=3
252	26.171444	192.168.1.1	192.168.1.69	ICMP	78 Echo (ping) reply id=0x0001, seq=3
260	27.184725	192.168.1.69	192.168.1.1	ICMP	74 Echo (ping) request id=0x0001, seq=4
261	27.185433	192.168.1.1	192.168.1.69	ICMP	78 Echo (ping) reply id=0x0001, seq=4
558	58.078856	ASUSTekCOMPU_78:b6:...	Intel_6f:7b:ec	ARP	46 Who has 192.168.1.69? Tell 192.168.1.69
559	58.078888	Intel_6f:7b:ec	ASUSTekCOMPU_78:b6:...	ARP	42 192.168.1.69 is at f8:fe:5e:6f:7b:e
597	66.592141	a2:1f:8e:51:22:03	Broadcast	ARP	42 Who has 192.168.1.1? Tell 192.168.1.1
906	105.949471	ASUSTekCOMPU_78:b6:...	Intel_6f:7b:ec	ARP	46 Who has 192.168.1.69? Tell 192.168.1.69
907	105.949501	Intel_6f:7b:ec	ASUSTekCOMPU_78:b6:...	ARP	42 192.168.1.69 is at f8:fe:5e:6f:7b:e
993	126.700352	a2:1f:8e:51:22:03	Broadcast	ARP	42 Who has 192.168.1.1? Tell 192.168.1.1

```
Frame 240: Packet, 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{3A 0000
Ethernet II, Src: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2), Dst: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec) 0010
  Destination: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec)
    .... ..0. .... .... .... = LG bit: Globally unique address (factory default) 0020
    .... ..0. .... .... .... = LG bit: Globally unique address (factory default) 0030
    .... ..0. .... .... .... = LG bit: Globally unique address (factory default) 0040
```

ARP request

- ARP используется для сопоставления IP \leftrightarrow MAC в сегменте L2
 - Рассмотрен ARP request:
 - Ethernet II + ARP (0x0806)
 - Длина кадра: 46 bytes
 - Отображается 802.1Q VLAN (0x8100)

源 IP	目的 IP	源端口	目的端口	协议	序列号	时间戳	数据包内容
40	11.743931	ASUSTekCOMPU_78:b6:...	Intel_6f:7b:ec	ARP	46	Who has 192.168.1.69? Tell 192.168.	
41	11.743962	Intel_6f:7b:ec	ASUSTekCOMPU_78:b6:...	ARP	42	192.168.1.69 is at f8:fe:5e:6f:7b:e	
239	24.146270	192.168.1.69	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=1	
240	24.147153	192.168.1.1	192.168.1.69	ICMP	78	Echo (ping) reply id=0x0001, seq=1	
247	25.157390	192.168.1.69	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=1	
248	25.158336	192.168.1.1	192.168.1.69	ICMP	78	Echo (ping) reply id=0x0001, seq=1	
251	26.170340	192.168.1.69	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=1	
252	26.171444	192.168.1.1	192.168.1.69	ICMP	78	Echo (ping) reply id=0x0001, seq=1	
260	27.184725	192.168.1.69	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=1	
261	27.185433	192.168.1.1	192.168.1.69	ICMP	78	Echo (ping) reply id=0x0001, seq=1	
558	58.078856	ASUSTekCOMPU_78:b6:...	Intel_6f:7b:ec	ARP	46	Who has 192.168.1.69? Tell 192.168.	
559	58.078888	Intel_6f:7b:ec	ASUSTekCOMPU_78:b6:...	ARP	42	192.168.1.69 is at f8:fe:5e:6f:7b:e	
597	66.592141	a2:1f:8e:51:22:03	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1	
906	105.949471	ASUSTekCOMPU_78:b6:...	Intel_6f:7b:ec	ARP	46	Who has 192.168.1.69? Tell 192.168.	
907	105.949501	Intel_6f:7b:ec	ASUSTekCOMPU_78:b6:...	ARP	42	192.168.1.69 is at f8:fe:5e:6f:7b:e	

```
▶ Frame 40: Packet, 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface \Device\NPF_{3AB 0000
▼ Ethernet II, Src: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2), Dst: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec) 0010
  ▼ Destination: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec) 0020
    .... ..0. .... .... .... = LG bit: Globally unique address (factory default)
    .... ..0. .... .... .... = IG bit: Individual address (unicast)
```

Ping по доменному имени и ARP reply

- Выполнен ping www.yandex.ru

```
PS C:\Users\Adel\Documents> ping www.yandex.ru

Обмен пакетами с www.yandex.ru [77.88.55.88] с 32 байтами данных:
Ответ от 77.88.55.88: число байт=32 время=10мс TTL=53
Ответ от 77.88.55.88: число байт=32 время=10мс TTL=53
Ответ от 77.88.55.88: число байт=32 время=10мс TTL=53
Ответ от 77.88.55.88: число байт=32 время=9мс TTL=53

Статистика Ping для 77.88.55.88:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
              (0% потеря)
Приблизительное время приема-передачи в мс:
    Минимальное = 9мсек, Максимальное = 10 мсек, Среднее = 9 мсек
```

Рис. 6: ping www.yandex.ru

Ping по доменному имени и ARP reply

- Имя разрешено в 77.88.55.88
- ARP reply подтверждает сопоставление IP устройства и его MAC

No.	Time	Source	Destination	Protocol	Length Info
37	7.660993	ASUSTekCOMPU_78:b6:f2	Intel_6f:7b:ec	ARP	46 Who has 192.168.1.69? Tell 192.168.1.69
38	7.661021	Intel_6f:7b:ec	ASUSTekCOMPU_78:b6:f2	ARP	42 192.168.1.69 is at f8:fe:5e:6f:7b:ec
60	13.586320	192.168.1.69	77.88.55.88	ICMP	74 Echo (ping) request id=0x0001, seq=1
61	13.596571	77.88.55.88	192.168.1.69	ICMP	78 Echo (ping) reply id=0x0001, seq=1
62	14.591521	192.168.1.69	77.88.55.88	ICMP	74 Echo (ping) request id=0x0001, seq=1
63	14.602207	77.88.55.88	192.168.1.69	ICMP	78 Echo (ping) reply id=0x0001, seq=1
69	15.604749	192.168.1.69	77.88.55.88	ICMP	74 Echo (ping) request id=0x0001, seq=1
70	15.614817	77.88.55.88	192.168.1.69	ICMP	78 Echo (ping) reply id=0x0001, seq=1
86	16.617226	192.168.1.69	77.88.55.88	ICMP	74 Echo (ping) request id=0x0001, seq=1
87	16.627143	77.88.55.88	192.168.1.69	ICMP	78 Echo (ping) reply id=0x0001, seq=1

▼ Ethernet II, Src: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec), Dst: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2) 0000 0010 0020
 ▼ Destination: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
 ▼ Source: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
 Type: ARP (0x0806)
 [Stream index: 0]
▼ Address Resolution Protocol (reply)
 Hardware type: Ethernet (1)
 Protocol type: IPv4 (0x0800)

ICMP к внешнему узлу: роль шлюза

- ICMP Echo Request на 77.88.55.88
- На канальном уровне кадр адресован **MAC шлюза**, т.к. цель вне подсети

No.	Time	Source	Destination	Protocol	Length	Info
37	7.660993	ASUSTekCOMPU_78:b6:...	Intel_6f:7b:ec	ARP	46	Who has 192.168.1.69? Tell 192.168.1.69
38	7.661021	Intel_6f:7b:ec	ASUSTekCOMPU_78:b6:...	ARP	42	192.168.1.69 is at f8:fe:5e:6f:7b:ec
→ 60	13.586320	192.168.1.69	77.88.55.88	ICMP	74	Echo (ping) request id=0x0001, seq=1
← 61	13.596571	77.88.55.88	192.168.1.69	ICMP	78	Echo (ping) reply id=0x0001, seq=1
62	14.591521	192.168.1.69	77.88.55.88	ICMP	74	Echo (ping) request id=0x0001, seq=2

.....0.... = IG bit: Individual address (unicast)
Source: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec)
.....0.... = LG bit: Globally unique address (factory default)
.....0.... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
[Stream index: 0]
Internet Protocol Version 4, Src: 192.168.1.69, Dst: 77.88.55.88
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 60
Identification: 0x3edd (16093)
000. = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.69
Destination Address: 77.88.55.88
[Stream index: 12]
Internet Control Message Protocol
Type: Echo (ping) request (8)
Code: 0
Checksum: 0x44EC [correct]

ICMP к внешнему узлу: роль шлюза

- Echo Reply приходит в локальную сеть от MAC шлюза

No.	Time	Source	Destination	Protocol	Length Info	
→	60 13.586320	192.168.1.69	77.88.55.88	ICMP	74 Echo (ping) request id=0x0001, seq=0	
←	61 13.596571	77.88.55.88	192.168.1.69	ICMP	78 Echo (ping) reply id=0x0001, seq=0	
	62 14.591521	192.168.1.69	77.88.55.88	ICMP	74 Echo (ping) request id=0x0001, seq=1	
	63 14.602207	77.88.55.88	192.168.1.69	ICMP	78 Echo (ping) reply id=0x0001, seq=1	
	69 15.604749	192.168.1.69	77.88.55.88	ICMP	74 Echo (ping) request id=0x0001, seq=2	

Frame 61: Packet, 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{3...}

Ethernet II, Src: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2), Dst: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec)

 Destination: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec)

 0. = LG bit: Globally unique address (factory default)

 0. = IG bit: Individual address (unicast)

 Source: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2)

 0. = LG bit: Globally unique address (factory default)

 0. = IG bit: Individual address (unicast)

 Type: 802.1Q Virtual LAN (0x8100)

 [Stream index: 0]

 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 0

 Internet Protocol Version 4, Src: 77.88.55.88, Dst: 192.168.1.69

 0100 = Version: 4

 0101 = Header Length: 20 bytes (5)

 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

 Total Length: 60

 Identification: 0x3edd (16093)

 Flags: 0x0

 ...0 0000 0000 0000 = Fragment Offset: 0

 Time to Live: 53

 Protocol: ICMP (1)

 Header Checksum: 0x0047 [validation disabled]

 [Header checksum status: Unverified]

 Source Address: 77.88.55.88

 Destination Address: 192.168.1.69

 [Stream index: 12]

 Internet Control Message Protocol

 Type: Echo (ping) reply (0)

 [Stream index: 13]

HTTP поверх TCP: GET-запрос

Фильтр: http - TCP: Src Port 54457 → Dst Port 80 - Флаги: PSH, ACK - HTTP: GET
/hypertext/www/TheProject.html

No.	Time	Source	Destination	Protocol	Length/Info
364	19.881198	192.168.1.69	188.184.67.127	HTTP	527 GET /hypertext/www/TheProject
369	19.933786	188.184.67.127	192.168.1.69	HTTP	1044 HTTP/1.1 200 OK (text/html)
376	20.004187	192.168.1.69	188.184.67.127	HTTP	468 GET /favicon.ico HTTP/1.1
387	20.057021	188.184.67.127	192.168.1.69	HTTP	248 HTTP/1.1 200 OK (image/vnd

Frame 364: Packet, 527 bytes on wire (4216 bits), 527 bytes captured (4216 bits) on interface \Device\NPF
Ethernet II, Src: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec), Dst: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2)
Internet Protocol Version 4, Src: 192.168.1.69, Dst: 188.184.67.127
Transmission Control Protocol, Src Port: 54457, Dst Port: 80, Seq: 1, Ack: 1, Len: 473
Source Port: 54457
Destination Port: 80
[Stream index: 29]
[Stream Packet Number: 1]
[Conversation completeness: Incomplete (28)]
[TCP Segment Len: 473]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 3880720057
[Next Sequence Number: 474 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 187318726
0101 = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 513
[Calculated window size: 513]
[Window size scaling factor: -1 (unknown)]
Checksum: 0xc418 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[Client Contiguous Streams: 1]

HTTP ответ сервера

- HTTP/1.1 200 OK
- Content-Type: text/html
- Данные передаются несколькими сегментами (reassembly)

No.	Time	Source	Destination	Protocol	Length	Info
→ 364	19.881198	192.168.1.69	188.184.67.127	HTTP	527	GET /hypertext/WWW/TheProject.htm
+ 369	19.933786	188.184.67.127	192.168.1.69	HTTP	1044	HTTP/1.1 200 OK (text/html)
376	20.004187	192.168.1.69	188.184.67.127	HTTP	468	GET /favicon.ico HTTP/1.1
387	20.057021	188.184.67.127	192.168.1.69	HTTP	748	HTTP/1.1 200 OK /image/und_mic

Frame 369: Packet, 1044 bytes on wire (8352 bits), 1044 bytes captured (8352 bits) on interface \Device\N 000
Ethernet II, Src: ASUStekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2), Dst: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec) 001
Internet Protocol Version 4, Src: 188.184.67.127, Dst: 192.168.1.69 002
Transmission Control Protocol, Src Port: 80, Dst Port: 54457, Seq: 1461, Ack: 474, Len: 990 003
Source Port: 80 004
Destination Port: 54457 005
[Stream index: 29] 006
[Stream Packet Number: 4] 007
[Conversation completeness: Incomplete (28)] 008
[TCP Segment Len: 990] 009
Sequence Number: 1461 (relative sequence number) 00a
Sequence Number (raw): 187320186 00b
[Next Sequence Number: 2451 (relative sequence number)] 00c
Acknowledgment Number: 474 (relative ack number) 00d
Acknowledgment number (raw): 3880720530 00e
0101 = Header Length: 20 bytes (5) 00f
Flags: 0x018 (PSH, ACK) 010
Window: 501 011
[Calculated window size: 501] 012
[Window size scaling factor: -1 (unknown)] 013
Checksum: 0x3d23 [unverified] 014
[Checksum Status: Unverified] 015
Urgent Pointer: 0 016
017
018

DNS поверх UDP: запрос

Фильтр: dns - UDP: Src Port 55855 → Dst Port 53 - Src IP: 192.168.1.69 → Dst IP: 192.168.1.1 - Standard query (запрос A/HTTPS)

No.	Time	Source	Destination	Protocol	Length Info
48	4.826737	192.168.1.69	192.168.1.1	DNS	88 Standard query 0x822f HTTPS brows
49	4.826824	192.168.1.69	192.168.1.1	DNS	88 Standard query 0x2b0c A browser.t
52	4.848430	192.168.1.1	192.168.1.69	DNS	139 Standard query response 0x822f HT
53	4.848681	192.168.1.1	192.168.1.69	DNS	104 Standard query response 0x2b0c A
78	4.897774	192.168.1.69	192.168.1.1	DNS	82 Standard query 0x06b4 HTTPS stora
79	4.897869	192.168.1.69	192.168.1.1	DNS	82 Standard query 0x7cd0 A storage.a
80	4.930811	192.168.1.1	192.168.1.69	DNS	140 Standard query response 0x06b4 HT
81	4.930811	192.168.1.1	192.168.1.69	DNS	98 Standard query response 0x7cd0 A

↳ Source: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec) 0000
Type: IPv4 (0x0800) 0010
[Stream index: 0] 0020
▼ Internet Protocol Version 4, Src: 192.168.1.69, Dst: 192.168.1.1 0030
 0100 = Version: 4 0040
 0101 = Header Length: 20 bytes (5) 0050
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 68
 Identification: 0x81bd (33213)
 Flags: 0x0
 ...0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 128
 Protocol: UDP (17)
 Header Checksum: 0x0000 [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 192.168.1.69
 Destination Address: 192.168.1.1
 [Stream index: 8]
▼ User Datagram Protocol, Src Port: 55855, Dst Port: 53
 Source Port: 55855
 Destination Port: 53
 Length: 48

DNS поверх UDP: ответ

- Ответ от DNS-сервера 192.168.1.1
- Возвращается сопоставление имени с IP
- Фиксируется TTL и служебные признаки IP

No.	Time	Source	Destination	Protocol	Length	Info
48	4.826737	192.168.1.69	192.168.1.1	DNS	88	Standard query 0x822f HTTPS browser
49	4.826824	192.168.1.69	192.168.1.1	DNS	88	Standard query 0x2b0c A browser.tr
52	4.848430	192.168.1.1	192.168.1.69	DNS	139	Standard query response 0x822f HTTP
53	4.848681	192.168.1.1	192.168.1.69	DNS	104	Standard query response 0x2b0c A br
78	4.897774	192.168.1.69	192.168.1.1	DNS	82	Standard query 0x06b4 HTTPS storage
79	4.897869	192.168.1.69	192.168.1.1	DNS	82	Standard query 0x7cd0 A storage.ap
80	4.930811	192.168.1.1	192.168.1.69	DNS	140	Standard query response 0x06b4 HTTP
81	4.930811	192.168.1.1	192.168.1.69	DNS	98	Standard query response 0x7cd0 A st

Source: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2) Type: IPv4 (0x0800) [Stream index: 0]

Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.69

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 126
Identification: 0xd943 (55619)

010. = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: UDP (17)
Header Checksum: 0xdd94 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.1
Destination Address: 192.168.1.69
[Stream index: 8]

User Datagram Protocol, Src Port: 53, Dst Port: 55855

0000
0010
0020
0030
0040
0050
0060
0070
0080

QUIC поверх UDP: Initial

Фильтр: quic - UDP: Src Port 443 → Dst Port 50215 - QUIC: Long Header, Packet Type: Initial -
Используются Connection ID, передаётся криптографическая информация

No.	Time	Source	Destination	Protocol	Length Info
3570	486.615374	192.168.1.69	173.194.220.94	QUIC	121 0-RTT, DCID=ec4db1023fe2ebc3
3694	486.638934	173.194.220.94	192.168.1.69	QUIC	82 Initial, SCID=ec4db1023fe2ebc3
3712	486.639045	173.194.220.94	192.168.1.69	QUIC	1292 Initial, SCID=ec4db1023fe2ebc3
3725	486.644577	173.194.220.94	192.168.1.69	QUIC	1292 Initial, SCID=ec4db1023fe2ebc3
3726	486.644577	173.194.220.94	192.168.1.69	QUIC	341 Protected Payload (KP0)
3727	486.644577	173.194.220.94	192.168.1.69	QUIC	990 Protected Payload (KP0)
3786	486.644869	192.168.1.69	173.194.220.94	QUIC	120 Handshake, DCID=ec4db1023fe2ebc3
3787	486.644908	192.168.1.69	173.194.220.94	QUIC	73 Protected Payload (KP0), DCID=ec4db1023fe2ebc3

Internet Protocol Version 4, Src: 173.194.220.94, Dst: 192.168.1.69
User Datagram Protocol, Src Port: 443, Dst Port: 50215

Source Port: 443

Destination Port: 50215

Length: 1258

Checksum: 0x3e61 [unverified]

[Checksum Status: Unverified]

[Stream index: 70]

[Stream Packet Number: 6]

[Timestamps]

UDP payload (1250 bytes)

QUIC IETF

QUIC Connection information

[Packet Length: 1250]

1... = Header Form: Long Header (1)

.1... = Fixed Bit: True

..00 = Packet Type: Initial (0)

[..... 00.. = Reserved: 0]

[..... ..00 = Packet Number Length: 1 bytes (0)]

Version: 1 (0x00000001)

Destination Connection ID Length: 0

Source Connection ID Length: 0

QUIC: Handshake

- QUIC Handshake фиксируется как отдельный тип пакета
- Часть нагрузки зашифрована (без ключей расшифровка невозможна)
- QUIC объединяет транспортные механизмы и защиту соединения

No.	Time	Source	Destination	Protocol	Length Info
3570	486.615374	192.168.1.69	173.194.220.94	QUIC	121 0-RTT, DCID=ec4db1023fe2ebc3
3694	486.638934	173.194.220.94	192.168.1.69	QUIC	82 Initial, SCID=ec4db1023fe2ebc3, PKN
3712	486.639045	173.194.220.94	192.168.1.69	QUIC	1292 Initial, SCID=ec4db1023fe2ebc3, PKN
3725	486.644577	173.194.220.94	192.168.1.69	QUIC	1292 Initial, SCID=ec4db1023fe2ebc3, PKN
3726	486.644577	173.194.220.94	192.168.1.69	QUIC	341 Protected Payload (KP0)
3727	486.644577	173.194.220.94	192.168.1.69	QUIC	990 Protected Payload (KP0)
3786	486.644869	192.168.1.69	173.194.220.94	QUIC	120 Handshake, DCID=ec4db1023fe2ebc3
3787	486.644908	192.168.1.69	173.194.220.94	QUIC	73 Protected Payload (KP0), DCID=ec4db1023fe2ebc3

Source: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
[Stream index: 0]
Internet Protocol Version 4, Src: 192.168.1.69, Dst: 173.194.220.94
User Datagram Protocol, Src Port: 50215, Dst Port: 443
Source Port: 50215
Destination Port: 443
Length: 86
Checksum: 0x4c76 [unverified]
[Checksum Status: Unverified]
[Stream index: 70]
[Stream Packet Number: 9]
[Timestamps]
UDP payload (78 bytes)
QUIC IETF
QUIC Connection information
[Packet Length: 78]

Установление TCP-соединения (3-way handshake)

Пример соединения к 188.184.67.127:80 - 1) SYN (клиент → сервер), Seq = 0 - 2) SYN, ACK (сервер → клиент), Ack = 1 - 3) ACK (клиент → сервер), Seq = 1, Ack = 1

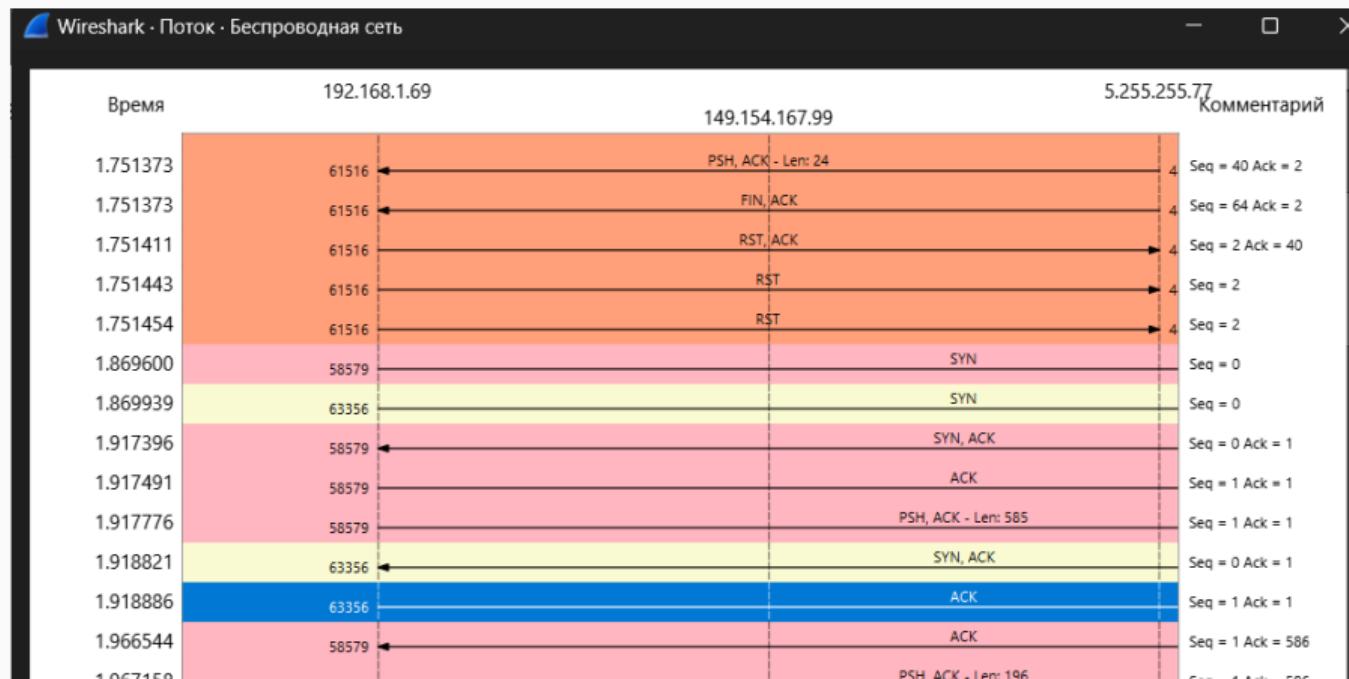
Далее передаются данные (PSH, ACK) и соединение закрывается (FIN, ACK). RST фиксирует принудительное завершение отдельных попыток.

22 1.751454	192.168.1.69	5.255.255.77	TCP	54 61516 → 443 [RST] Seq=2 Win=0
32 1.869600	192.168.1.69	188.184.67.127	TCP	66 58579 → 80 [SYN] Seq=0 Win=642
33 1.869939	192.168.1.69	188.184.67.127	TCP	66 63356 → 80 [SYN] Seq=0 Win=642
34 1.917396	188.184.67.127	192.168.1.69	TCP	66 80 → 58579 [SYN, ACK] Seq=0 Ack=1
35 1.917491	192.168.1.69	188.184.67.127	TCP	54 58579 → 80 [ACK] Seq=1 Ack=1 Win=642
36 1.917776	192.168.1.69	188.184.67.127	HTTP	639 GET /hypertext/WWW/TheProject.html
37 1.918821	188.184.67.127	192.168.1.69	TCP	66 80 → 63356 [SYN, ACK] Seq=0 Ack=1
38 1.918886	192.168.1.69	188.184.67.127	TCP	54 63356 → 80 [ACK] Seq=1 Ack=1 Win=642
39 1.966544	188.184.67.127	192.168.1.69	TCP	54 80 → 58579 [ACK] Seq=1 Ack=586
40 1.967158	188.184.67.127	192.168.1.69	HTTP	250 HTTP/1.1 304 Not Modified
41 1.967158	188.184.67.127	192.168.1.69	TCP	54 80 → 58579 [FIN, ACK] Seq=197 Ack=586
42 1.967188	192.168.1.69	188.184.67.127	TCP	54 58579 → 80 [ACK] Seq=586 Ack=197
43 1.967343	192.168.1.69	188.184.67.127	TCP	54 58579 → 80 [FIN, ACK] Seq=586 Ack=197
48 1.988930	192.168.1.69	87.250.251.20	TCP	66 63242 → 443 [SYN] Seq=0 Win=642
49 2.010326	87.250.251.20	192.168.1.69	TCP	66 443 → 63242 [SYN, ACK] Seq=0 Ack=1
50 2.010376	192.168.1.69	87.250.251.20	TCP	54 63242 → 443 [ACK] Seq=1 Ack=1
51 2.010705	192.168.1.69	87.250.251.20	TLSv1.2	1984 Client Hello (SNI=browser.transport)
52 2.013386	192.168.1.69	149.154.167.99	TLSv1.2	203 Application Data

Рис. 16: TCP handshake в списке пакетов

График потока (Flow Graph)

- Наглядно отображены этапы SYN → SYN,ACK → ACK
- Видны направления обмена, рост Seq/Ack
- Отражены PSH/ACK при передаче данных и FIN/ACK при закрытии



Итоговые выводы

- Определены параметры сетевого подключения (IP/шлюз/DNS/MAC) и подтверждена связность с шлюзом.
- Проанализированы ARP и ICMP: показаны IP \leftrightarrow MAC соответствия и отличие L2-доставки в локальной сети и при выходе во внешние сети.
- Рассмотрены HTTP (TCP), DNS (UDP), QUIC (UDP): выявлены различия в доставке данных и служебных механизмах.
- На практике подтверждён механизм TCP handshake и интерпретация Seq/Ack по графику потока Wireshark.