

Лабораторная №3

Сетевые технологии - Комягин А.Н.

Российский университет дружбы народов, Москва, Россия

Цель

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

MAC-адресация

С помощью команды `ipconfig` определить основные параметры сетевого соединения.

```
Адаптер беспроводной локальной сети Беспроводная сеть:  
    DNS-суффикс подключения . . . . . :  
    Локальный IPv6-адрес канала . . . : fe80::28f2:9ef4:cafe:7d81%6  
    IPv4-адрес. . . . . : 192.168.0.138  
    Маска подсети . . . . . : 255.255.255.0  
    Основной шлюз. . . . . : 192.168.0.1
```

Рис. 1: `ipconfig`

Анализ кадров канального уровня в Wireshark

Захватить и проанализировать пакеты ARP и ICMP в части кадров канального уровня (Ethernet II).

Для генерации трафика была выполнена команда `ping 192.168.0.1` (ping основного шлюза). В Wireshark был применен фильтр **arp or icmp**.

На скриншоте ниже виден обмен ICMP-пакетами (эхо-запросы и эхо-ответы).

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|------------|------------------------|------------------------|----------|--------|--|
| 128 | 48.215607 | Intel_60:d8:d0 | TpLinkTechno_59:88:... | ARP | 42 | 192.168.0.138 is at 2c:6d:c1:60:d8:d0 |
| 165 | 74.200409 | TpLinkTechno_59:88:... | Intel_60:d8:d0 | ARP | 42 | Who has 192.168.0.138? Tell 192.168.0.1 |
| 166 | 74.200443 | Intel_60:d8:d0 | TpLinkTechno_59:88:... | ARP | 42 | 192.168.0.138 is at 2c:6d:c1:60:d8:d0 |
| 1564 | 100.182044 | TpLinkTechno_59:88:... | Intel_60:d8:d0 | ARP | 42 | Who has 192.168.0.138? Tell 192.168.0.1 |
| 1565 | 100.182074 | Intel_60:d8:d0 | TpLinkTechno_59:88:... | ARP | 42 | 192.168.0.138 is at 2c:6d:c1:60:d8:d0 |
| 1892 | 126.167161 | TpLinkTechno_59:88:... | Intel_60:d8:d0 | ARP | 42 | Who has 192.168.0.138? Tell 192.168.0.1 |
| 1893 | 126.167186 | Intel_60:d8:d0 | TpLinkTechno_59:88:... | ARP | 42 | 192.168.0.138 is at 2c:6d:c1:60:d8:d0 |
| 2026 | 153.208776 | TpLinkTechno_59:88:... | Intel_60:d8:d0 | ARP | 42 | Who has 192.168.0.138? Tell 192.168.0.1 |
| 2027 | 153.208811 | Intel_60:d8:d0 | TpLinkTechno_59:88:... | ARP | 42 | 192.168.0.138 is at 2c:6d:c1:60:d8:d0 |
| 2356 | 189.511051 | 192.168.0.138 | 192.168.0.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=1/2356, ttl=128 (reply in 2357) |
| 2357 | 189.513303 | 192.168.0.1 | 192.168.0.138 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=1/2356, ttl=64 (request in 2356) |
| 2358 | 190.529203 | 192.168.0.138 | 192.168.0.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 2359) |
| 2359 | 190.532317 | 192.168.0.1 | 192.168.0.138 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (request in 2358) |
| 2360 | 191.545940 | 192.168.0.138 | 192.168.0.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 2361) |
| 2361 | 191.547621 | 192.168.0.1 | 192.168.0.138 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (request in 2360) |
| 2362 | 192.562435 | 192.168.0.138 | 192.168.0.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 2363) |
| 2363 | 192.563908 | 192.168.0.1 | 192.168.0.138 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request in 2362) |
| 2392 | 201.607307 | TpLinkTechno_59:88:... | Intel_60:d8:d0 | ARP | 42 | Who has 192.168.0.138? Tell 192.168.0.1 |
| 2393 | 201.607365 | Intel_60:d8:d0 | TpLinkTechno_59:88:... | ARP | 42 | 192.168.0.138 is at 2c:6d:c1:60:d8:d0 |

Frame 2356: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{00000000-0000-0000-0000-000000000000} (0.0.0.0)

Ethernet II, Src: Intel_60:d8:d0 (2c:6d:c1:60:d8:d0), Dst: TpLinkTechno_59:88:0b (28:ee:52:59:88:0b)

Internet Protocol Version 4, Src: 192.168.0.138, Dst: 192.168.0.1

Internet Control Message Protocol

28 ee 52 59 88 0b 2c 6d c1 60 d8 d0 08 00 45 00

00 3c 1e 50 00 00 80 01 00 00 c0 a8 00 8a c0 a8

00 01 08 00 dd 5a 00 01 00 01 61 62 63 64 65 66

67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76

77 61 62 63 64 65 66 67 68 69

(...)

Рис. 2: ICMP 2356

| | | | | | | | |
|---|------|------------|------------------------|------------------------|------|--|--|
| → | 2356 | 189.511851 | 192.168.0.138 | 192.168.0.1 | ICMP | 74 Echo (ping) request | id=0x0001, seq=1/256, ttl=128 (reply in 2357) |
| ← | 2357 | 189.511303 | 192.168.0.1 | 192.168.0.138 | ICMP | 74 Echo (ping) reply | id=0x0001, seq=1/256, ttl=64 (request in 2356) |
| | 2358 | 190.529203 | 192.168.0.138 | 192.168.0.1 | ICMP | 74 Echo (ping) request | id=0x0001, seq=2/512, ttl=128 (reply in 2359) |
| | 2359 | 190.532317 | 192.168.0.1 | 192.168.0.138 | ICMP | 74 Echo (ping) reply | id=0x0001, seq=2/512, ttl=64 (request in 2358) |
| | 2360 | 191.545940 | 192.168.0.138 | 192.168.0.1 | ICMP | 74 Echo (ping) request | id=0x0001, seq=3/768, ttl=128 (reply in 2361) |
| | 2361 | 191.547621 | 192.168.0.1 | 192.168.0.138 | ICMP | 74 Echo (ping) reply | id=0x0001, seq=3/768, ttl=64 (request in 2360) |
| | 2362 | 192.562435 | 192.168.0.138 | 192.168.0.1 | ICMP | 74 Echo (ping) request | id=0x0001, seq=4/1024, ttl=128 (reply in 2363) |
| | 2363 | 192.563908 | 192.168.0.1 | 192.168.0.138 | ICMP | 74 Echo (ping) reply | id=0x0001, seq=4/1024, ttl=64 (request in 2362) |
| | 2392 | 201.607307 | TpLinkTechno_59:88:... | Intel_60:d8:d0 | ARP | 42 Who has 192.168.0.138? Tell 192.168.0.1 | |
| | 2393 | 201.607365 | Intel_60:d8:d0 | TpLinkTechno_59:88:... | ARP | 42 192.168.0.138 is at 2c:6d:c1:60:d8:d0 | |
| 4 | | | | | | | |
| ↳ Frame 2357: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{00000000-0000-0000-0000-000000000000} | | | | | | | |
| ↳ Ethernet II, Src: TpLinkTechno_59:88:0b (28:ae:52:59:88:0b), Dst: Intel_60:d8:d0 (2c:6d:c1:60:d8:d0) | | | | | | | |
| ↳ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.138 | | | | | | | |
| ↳ Internet Control Message Protocol | | | | | | | |
| | | | | | | 0000 | 2c 6d c1 60 d8 d0 28 ae 52 59 88 0b 00 00 45 00 ,m (RY E |
| | | | | | | 0010 | 00 3c 38 47 00 00 40 01 c0 9e c0 a8 00 01 c0 a8 <8G @ |
| | | | | | | 0020 | 00 8a 00 00 55 5a 00 01 00 01 61 62 63 64 65 66 ...UZ...abcdef |
| | | | | | | 0030 | 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklm opqrstuv |
| | | | | | | 0040 | 77 61 62 63 64 65 66 67 68 69 wabcdefg hi |

Рис. 3: ICMP 2357

Анализ ARP-трафика

arp or icmp

Список пакетов Фильтр отображения Введите фильтр отображения ...

Опции: Обычные и многобайтовые Чувствительность к регистру Назад Множественные случаи

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|------------|-----------------------|-----------------------|----------|--------|--|
| 81 | 20.204288 | TpLinkTechno_59:88:0b | Intel_60:d8:d0 | ARP | 42 | Who has 192.168.0.138? Tell 192.168.0.1 |
| 82 | 20.294315 | Intel_60:d8:d0 | TpLinkTechno_59:88:0b | ARP | 42 | 192.168.0.138 is at 2c:6d:c1:60:d8:d0 |
| 127 | 48.215575 | TpLinkTechno_59:88:0b | Intel_60:d8:d0 | ARP | 42 | Who has 192.168.0.138? Tell 192.168.0.1 |
| 128 | 48.215607 | Intel_60:d8:d0 | TpLinkTechno_59:88:0b | ARP | 42 | 192.168.0.138 is at 2c:6d:c1:60:d8:d0 |
| 165 | 74.200409 | TpLinkTechno_59:88:0b | Intel_60:d8:d0 | ARP | 42 | Who has 192.168.0.138? Tell 192.168.0.1 |
| 166 | 74.200443 | Intel_60:d8:d0 | TpLinkTechno_59:88:0b | ARP | 42 | 192.168.0.138 is at 2c:6d:c1:60:d8:d0 |
| 1564 | 100.182944 | TpLinkTechno_59:88:0b | Intel_60:d8:d0 | ARP | 42 | Who has 192.168.0.138? Tell 192.168.0.1 |
| 1565 | 100.182974 | Intel_60:d8:d0 | TpLinkTechno_59:88:0b | ARP | 42 | 192.168.0.138 is at 2c:6d:c1:60:d8:d0 |
| 1892 | 126.167161 | TpLinkTechno_59:88:0b | Intel_60:d8:d0 | ARP | 42 | Who has 192.168.0.138? Tell 192.168.0.1 |
| 1893 | 126.167186 | Intel_60:d8:d0 | TpLinkTechno_59:88:0b | ARP | 42 | 192.168.0.138 is at 2c:6d:c1:60:d8:d0 |
| 2026 | 153.208776 | TpLinkTechno_59:88:0b | Intel_60:d8:d0 | ARP | 42 | Who has 192.168.0.138? Tell 192.168.0.1 |
| 2027 | 153.208811 | Intel_60:d8:d0 | TpLinkTechno_59:88:0b | ARP | 42 | 192.168.0.138 is at 2c:6d:c1:60:d8:d0 |
| 2356 | 189.511851 | 192.168.0.138 | 192.168.0.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 2357) |
| 2357 | 189.513303 | 192.168.0.1 | 192.168.0.138 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in 2356) |
| 2358 | 190.529203 | 192.168.0.138 | 192.168.0.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 2359) |
| 2359 | 190.532317 | 192.168.0.1 | 192.168.0.138 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (request in 2358) |
| 2360 | 191.545940 | 192.168.0.138 | 192.168.0.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 2361) |
| 2361 | 191.547621 | 192.168.0.1 | 192.168.0.138 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (request in 2360) |
| 2362 | 192.562435 | 192.168.0.138 | 192.168.0.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 2363) |
| 2363 | 192.563908 | 192.168.0.1 | 192.168.0.138 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request in 2362) |
| 2392 | 201.607307 | TpLinkTechno_59:88:0b | Intel_60:d8:d0 | ARP | 42 | Who has 192.168.0.138? Tell 192.168.0.1 |
| 2393 | 201.607365 | Intel_60:d8:d0 | TpLinkTechno_59:88:0b | ARP | 42 | 192.168.0.138 is at 2c:6d:c1:60:d8:d0 |

4

Frame 81: Packet, 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{...} [Ethernet II, Src: TpLinkTechno_59:88:0b (28:ee:52:59:88:0b), Dst: Intel_60:d8:d0 (2c:6d:c1:60:d8:d0)]

Destination: Intel_60:d8:d0 (2c:6d:c1:60:d8:d0)

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

...0. = IG bit: Individual address (unicast)

Source: TpLinkTechno_59:88:0b (28:ee:52:59:88:0b)

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

...0. = IG bit: Individual address (unicast)

Type: ARP (0x0006)

[Stream index: 0]

Address Resolution Protocol (request)

0000 2c 6d c1 60 d8 d0 28 ee 52 59 88 0b 08 06 00 01 RY

0010 08 00 06 04 00 01 28 ee 52 59 88 0b c0 a8 00 01 RY

0020 00 00 00 00 00 00 c0 a8 00 0a

Рис. 4: ARP 81

Анализ ARP-трафика

arp or icmp

Список пакетов Фильтр отображения Введите фильтр отображения ...

Опции: Обычные и многобайтовые Чувствительность к регистру Назад Множественные случаи

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|------------|-----------------------|-----------------------|----------|--------|--|
| 81 | 20.204288 | TpLinkTechno_59:88:0b | Intel_60:d8:d0 | ARP | 42 | Who has 192.168.0.138? Tell 192.168.0.1 |
| 82 | 20.294315 | Intel_60:d8:d0 | TpLinkTechno_59:88:0b | ARP | 42 | 192.168.0.138 is at 2c:6d:c1:60:d8:d0 |
| 127 | 48.215575 | TpLinkTechno_59:88:0b | Intel_60:d8:d0 | ARP | 42 | Who has 192.168.0.138? Tell 192.168.0.1 |
| 128 | 48.215607 | Intel_60:d8:d0 | TpLinkTechno_59:88:0b | ARP | 42 | 192.168.0.138 is at 2c:6d:c1:60:d8:d0 |
| 165 | 74.200409 | TpLinkTechno_59:88:0b | Intel_60:d8:d0 | ARP | 42 | Who has 192.168.0.138? Tell 192.168.0.1 |
| 166 | 74.200443 | Intel_60:d8:d0 | TpLinkTechno_59:88:0b | ARP | 42 | 192.168.0.138 is at 2c:6d:c1:60:d8:d0 |
| 1564 | 100.182944 | TpLinkTechno_59:88:0b | Intel_60:d8:d0 | ARP | 42 | Who has 192.168.0.138? Tell 192.168.0.1 |
| 1565 | 100.182974 | Intel_60:d8:d0 | TpLinkTechno_59:88:0b | ARP | 42 | 192.168.0.138 is at 2c:6d:c1:60:d8:d0 |
| 1892 | 126.167161 | TpLinkTechno_59:88:0b | Intel_60:d8:d0 | ARP | 42 | Who has 192.168.0.138? Tell 192.168.0.1 |
| 1893 | 126.167186 | Intel_60:d8:d0 | TpLinkTechno_59:88:0b | ARP | 42 | 192.168.0.138 is at 2c:6d:c1:60:d8:d0 |
| 2026 | 153.208776 | TpLinkTechno_59:88:0b | Intel_60:d8:d0 | ARP | 42 | Who has 192.168.0.138? Tell 192.168.0.1 |
| 2027 | 153.208811 | Intel_60:d8:d0 | TpLinkTechno_59:88:0b | ARP | 42 | 192.168.0.138 is at 2c:6d:c1:60:d8:d0 |
| 2356 | 189.511851 | 192.168.0.138 | 192.168.0.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 2357) |
| 2357 | 189.513303 | 192.168.0.1 | 192.168.0.138 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in 2356) |
| 2358 | 190.529203 | 192.168.0.138 | 192.168.0.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 2359) |
| 2359 | 190.532317 | 192.168.0.1 | 192.168.0.138 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (request in 2358) |
| 2360 | 191.545940 | 192.168.0.138 | 192.168.0.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 2361) |
| 2361 | 191.547621 | 192.168.0.1 | 192.168.0.138 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (request in 2360) |
| 2362 | 192.562435 | 192.168.0.138 | 192.168.0.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 2363) |
| 2363 | 192.563908 | 192.168.0.1 | 192.168.0.138 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request in 2362) |
| 2392 | 201.607307 | TpLinkTechno_59:88:0b | Intel_60:d8:d0 | ARP | 42 | Who has 192.168.0.138? Tell 192.168.0.1 |
| 2393 | 201.607365 | Intel_60:d8:d0 | TpLinkTechno_59:88:0b | ARP | 42 | 192.168.0.138 is at 2c:6d:c1:60:d8:d0 |

4

Frame 81: Packet, 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{...} (Ethernet II, Src: TpLinkTechno_59:88:0b (28:ee:52:59:88:0b), Dst: Intel_60:d8:d0 (2c:6d:c1:60:d8:d0))

Destination: Intel_60:d8:d0 (2c:6d:c1:60:d8:d0)

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

...0. = IG bit: Individual address (unicast)

Source: TpLinkTechno_59:88:0b (28:ee:52:59:88:0b)

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

...0. = IG bit: Individual address (unicast)

Type: ARP (0x0806)

[Stream Index: 0]

Address Resolution Protocol (request)

0000 2c 6d c1 60 d8 d0 28 ee 52 59 88 0b 08 06 00 01 RY

0010 08 00 06 04 00 01 28 ee 52 59 88 0b c0 a8 00 01 RY

0020 00 00 00 00 00 00 c0 a8 00 0a

Рис. 5: ARP 82

Анализ протоколов транспортного уровня

HTTP GET Request (пакет №152)

```
Capture Length: 557 bytes (4456 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocol in frame: ethertype:ip:tcp:http]
Character encoding: ASCII (0)
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
* Ethernet II, Src: Intel_60:d8:d0 (2c:6d:c1:60:d8:d0), Dst: TpLinkTechno_59:88:0b (28:ee:52:59:88:0b)
  Destination: TpLinkTechno_59:88:0b (28:ee:52:59:88:0b)
    ....0. .... = IG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  * Source: Intel_60:d8:d0 (2c:6d:c1:60:d8:d0)
    ....0. .... = IG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  [Stream index: 0]
  * Internet Protocol Version 4, Src: 192.168.0.138, Dst: 188.184.67.127
    0100 .... = Version: 4
    ....0101 = Header Length: 20 bytes (5)
    * Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total length: 543
      Identification: 0x03ce (37838)
    * 010. .... = Flags: 0x2, Don't fragment
      ...0 0000 0000 = Fragment Offset: 0
      Time to live: 128
      Protocol: TCP (6)
      Header checksum: 0x0000 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 192.168.0.138
      Destination Address: 188.184.67.127
      [Stream index: 7]
      * Transmission Control Protocol, Src Port: 54323, Dst Port: 80, Seq: 414614161, Len: 503
        0000 28 ee 52 59 88 0b 2c 6d c1 60 d8 d0 08 00 45 00 ( RY...E.
        0010 02 1f 93 ce 48 00 00 06 00 00 c0 a8 00 8a bc b8 ...@...
        0020 43 7f f4 99 00 50 12 48 3f c0 06 8b 38 68 50 1b C...P.W?..8BP
        0030 80 ff c3 7b 00 0a 47 45 54 20 2f 68 70 70 65 72 {...}.GT./hyper
        0040 74 65 78 74 2f 57 57 57 2f 54 68 65 50 72 6f 6a text/www/TheProj
        0050 65 63 74 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e ect.html HTTP/1.
        0060 31 8d 0a 48 6f 73 74 3a 20 69 6e 66 6f 2e 63 65 1 Host: info.ce
        0070 72 6e 2e 63 68 0d 0a 43 6f 6e 6e 63 74 69 6f en.ch - connectio
        0080 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 n: keep-alive. U
        0090 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d pgrade-I nsecure-
        00a0 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 Requests : 1 Use
        00b0 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6e 6c 61 r-Agent: Mozilla
        00c0 2f 35 2a 30 20 28 5f 69 6e 6d 6f 77 73 20 4e 54 /5.0 (Windows NT
        00d0 20 31 30 2a 30 3b 20 5f 69 6e 36 3a 3b 20 78 36 10.0; Win64; x6
        00e0 34 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 4) AppleWebKit/5
        00f0 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 37.36 (KHTML, li
        0100 6b 65 20 47 65 63 6b 6f 29 28 43 68 72 6f 6d 65 ka Gecko ) Chrome
        0110 2f 31 33 38 2a 30 2e 30 2e 30 20 59 61 42 72 6f /118.0.0.0 YaBro
        0120 77 73 65 72 2f 32 35 2a 38 2a 30 2a 30 20 53 61 user/25.8.0.0 Sa
        0130 66 61 72 69 2f 35 33 37 2e 33 36 0d 0a 41 63 63 fari/537.36 Acc
        0140 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 opt: text/html,a
        0150 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c plication/xhtml
        0160 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6a /xml,application
        0170 2f 78 6d 6c 3b 71 3d 30 2e 30 2c 69 6d 61 67 65 /xml;q=0.9,image
        0180 2f 61 76 69 66 2c 69 6d 61 67 65 2f 77 65 62 70 /avif,image/webp
        0190 2c 69 6d 61 67 65 2f 61 70 6e 67 2c 2a 2f 2a 3b ,image/png,*/*;
        01a0 71 3d 30 2a 38 2c 61 70 70 6c 69 63 61 74 69 6f q=0.8,application
        01b0 6e 2f 73 69 67 6e 65 64 2d 65 78 63 68 61 6e 67 n/signed-exchang
        01c0 65 3b 76 3d 63 3b 71 3d 30 2a 37 0d 0a 52 65 e;q=h3;q=0.7 Re
        01d0 66 65 72 65 72 3a 20 68 74 74 70 3a 2f 2f 69 6e ferer: http://in
        01e0 66 6f 2e 63 65 72 6e 2e 63 68 2f 0d 0a 41 63 63 fo.cern.ch/ Acc
        01f0 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a ept-Enconding: g
        0200 69 70 2c 20 64 65 66 6c 63 74 65 0d 0a 41 63 63 ip, deflate Acc
        0210 68 30 3d 3d 61 63 6e 63 2e 63 6e 6e 3b 3b 3b 3b
```

HTTP 200 OK Response (пакет №191)

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|----------------|----------------|----------|--------|--|
| 152 | 8.107977 | 192.168.0.138 | 188.184.67.127 | HTTP | 557 | GET /hypertext/World/TheProject.html HTTP/1.1 |
| 153 | 8.109087 | 192.168.0.138 | 192.168.0.137 | HTTP | 104 | HTTP/1.1 200 OK (text/html) |
| 191 | 12.986558 | 192.168.0.138 | 188.184.67.127 | HTTP | 588 | GET /hypertext/World/Bibliography.html HTTP/1.1 |
| 196 | 12.989581 | 188.184.67.127 | 192.168.0.138 | HTTP | 1471 | HTTP/1.1 200 OK (text/html) |
| 252 | 20.001620 | 192.168.0.138 | 188.184.67.127 | HTTP | 687 | GET /hypertext/World/Administration/Mailing/Overview.html HTTP/1.1 |
| 256 | 20.063923 | 188.184.67.127 | 192.168.0.138 | HTTP | 414 | HTTP/1.1 404 Not Found (text/html) |

| | |
|--|--|
| <div>Capture Length: 1044 bytes (8352 bits)</div> <div>[Frame is marked: False]</div> <div>[Frame is ignored: False]</div> <div>[Protocols in frame: ethertype:ip:tcp:ht:ip:data-text-lines]</div> <div>Character encoding: ASCII (0)</div> <div>[Coloring Rule Name: HTTP]</div> <div>[Coloring Rule String: http tcp.port == 80 http2]</div> <div>Ethernet II, Src: TplinkTechno_59:88:0b (28:ee:52:59:88:0b), Dst: Intel_60:d8:d0 (2c:6d:c1:60:d8:d0)<ul style="list-style-type: none">Destination: Intel_60:d8:d0 (2c:6d:c1:60:d8:d0)<ul style="list-style-type: none">.....0. = IG bit: Globally unique address (factory default).....0. = IG bit: Individual address (unicast)Source: TplinkTechno_59:88:0b (28:ee:52:59:88:0b)<ul style="list-style-type: none">.....0. = IG bit: Globally unique address (factory default).....0. = IG bit: Individual address (unicast)Type: IPv4 (0x0000)<ul style="list-style-type: none">[Stream index: 0]</div> <div>Internet Protocol Version 4, Src: 188.184.67.127, Dst: 192.168.0.138<ul style="list-style-type: none">0100 = Version: 4....0101 = Header Length: 20 bytes (5)Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)Total Length: 1030Identification: 0x84a4 (35402)010. = Flags: 0x2, Don't Fragment...0 0000 0000 0000 = Fragment Offset: 0Time to Live: 47Protocol: TCP (6)Header Checksum: 0xfc3d [validation disabled][Header checksum status: Unverified]Source Address: 188.184.67.127Destination Address: 192.168.0.138[Stream index: 1]</div> <div>Transmission Control Protocol, Src Port: 80, Dst Port: 64153, Seq: 1461, Ack: 504, Len: 390<ul style="list-style-type: none">[2 Reasonable TCP segments (2890 bytes): #154(1460), #155(999)]</div> | <div>0010 04 06 0a 4a 40 00 2f 06 fc 3d bc b8 43 7f c0 a8 ...30-/-...C-...</div> <div>0020 00 8a 00 50 fa 99 06 8b 3e 1c 12 48 41 c6 50 18 ...P....S:NA.P...</div> <div>0030 00 f9 d2 ca 00 00 41 0a 4e 41 4d 45 3d 33 35 20 ...A NAME=35</div> <div>0040 40 52 45 46 3d 22 53 74 61 74 75 73 2a 68 74 6d HREF="Status.htm</div> <div>0050 6c 21 33 35 22 3e 56 69 6f 6e 61 3c 2f 41 3e 20 [035">V] olac/A/</div> <div>0060 2c 20 20 3c 41 0a 4e 41 4d 45 3d 32 36 20 48 52 , <A NAME=26 HR</div> <div>0070 45 46 3d 22 4a 65 58 54 2f 57 6f 72 6c 64 57 69 EF="Next /WorldI</div> <div>0080 64 65 57 65 62 2a 68 74 6d 6c 22 3a 4a 65 58 54 dweb.ht ml">Next</div> <div>0090 53 74 65 70 3c 2f 41 3e 0a 2c 20 3c 41 0a 4e 41 Step/A/ , <A NA</div> <div>00a0 4d 45 3d 32 35 20 48 52 45 46 3d 22 44 61 65 6d ME=25 HR EF="Dann</div> <div>00b0 6f 6e 2f 4f 76 65 72 76 69 65 77 2a 68 74 6d 6c on/Overw ieu.html</div> <div>00c0 22 3a 53 65 72 76 65 72 73 3c 2f 41 3e 20 2c 20 ">Server s ,</div> <div>00d0 3c 41 0a 4e 41 4d 45 3d 35 31 20 48 52 45 46 3d <A NAME=51 HREF=</div> <div>00e0 22 54 6f 6f 6c 73 2f 4f 76 65 72 76 69 65 77 2a "Title/O verview.</div> <div>00f0 68 74 6d 6c 22 3a 54 6f 6f 6c 73 3c 2f 41 3e 20 html">To ols</div> <div>0100 2c 3c 41 0a 4e 41 4d 45 3d 35 31 20 48 52 45 46 <A NAME =53 HREF</div> <div>0110 3d 22 4d 61 69 6c 52 6f 62 6f 74 2f 4f 76 65 72 ="Maillo bot/Over</div> <div>0120 76 69 65 77 2a 68 74 6d 6c 22 3a 20 4d 61 69 6c view.htm l"> Mail</div> <div>0130 20 72 6f 62 6f 74 3c 2f 41 3e 20 3c 41 0a 4e robots</ A> ,<A N</div> <div>0140 41 4d 45 3d 35 32 20 48 52 45 46 3d 22 53 74 61 AME=52 H REF="Sta</div> <div>0150 74 75 73 2e 68 74 6d 6c 23 35 37 22 3e 0a 4c 69 tus.html #57"> Li</div> <div>0160 62 72 61 72 79 3c 2f 41 3e 20 29 0a 3c 44 54 3a brary<A> >) <DT></div> <div>0170 3c 41 0a 4e 41 4d 45 3d 34 37 20 48 52 45 46 3d <A NAME= 47 HREF=</div> <div>0180 22 54 65 63 68 6e 69 63 61 6c 2a 68 74 6d 6c 22 "Technic al.html"</div> <div>0190 3e 54 65 63 68 6e 69 63 61 6c 3c 2f 41 3e 0a 3c >Technic al <</div> <div>01a0 44 44 3a 20 44 65 74 61 69 6c 73 20 6f 66 20 70 DD: Data ils of p</div> <div>01b0 72 6f 74 6f 63 6f 6c 73 2c 20 66 6f 72 6d 61 74 rotocols , format</div> <div>01c0 73 2c 0a 70 72 6f 67 72 61 6d 20 69 6a 7a 65 72 s, prop ag inter</div> <div>01d0 22 54 65 63 68 6e 69 63 61 6c 2a 68 74 6d 6c 22 nals etc. <DT><A</div> <div>01e0 4e 41 4d 45 3d 34 30 20 48 52 45 46 3d 22 42 69 NAME=40 HREF="Bi</div> <div>01f0 62 6c 69 6f 67 72 61 70 68 79 2e 68 74 6d 6c 22 blograp hy.html"</div> <div>0200 3a 42 69 62 6c 69 6f 67 72 61 70 68 79 3c 2f 41 >Bibliog raphy</A</div> <div>0210 3e 0a 3c 44 4a 3e 20 50 61 70 65 72 20 6f 63 > <DD> P aper doc</div> <div>0220 75 6d 65 6e 74 61 74 69 6f 6e 0a 6f 6a 20 57 unstat on on M</div> |
|--|--|

DNS Standard Query (пакет №63)

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|------------|---------------|---------------|----------|--------|--|
| 17 | 0.409716 | 192.168.0.1 | 192.168.0.138 | DNS | 416 | Standard query response 0xb75f A suggest.dzen.ru A 87.250.254.106 NS a.dns.rpn.net NS d.dns.rpn.net NS e.dns |
| 19 | 0.454014 | 192.168.0.1 | 192.168.0.138 | DNS | 432 | Standard query response 0xb89c A dzen.ru A 185.180.200.2 A 83.222.28.15 A 5.61.23.39 NS b.dns.rpn.net NS f.dns |
| 63 | 0.878113 | 192.168.0.138 | 192.168.0.1 | DNS | 81 | Standard query 0xc0c0 A api.brower.yandex.ru |
| 64 | 0.893825 | 192.168.0.1 | 192.168.0.138 | DNS | 248 | Standard query response 0xc0c0 A api.brower.yandex.ru A 213.180.193.234 NS ns4.yandex.ru NS ns3.yandex.ru A 8 |
| 383 | 49.910510 | 192.168.0.138 | 192.168.0.1 | DNS | 83 | Standard query 0xb0bf A www.msftconnecttest.com |
| 384 | 49.914620 | 192.168.0.1 | 192.168.0.138 | DNS | 535 | Standard query response 0xb0bf A www.msftconnecttest.com CNAME ncsl-geo.trafficmanager.net CNAME www.msftncsl. |
| 479 | 100.210107 | 192.168.0.138 | 192.168.0.1 | DNS | 82 | Standard query 0xfc1a A api.brower.yandex.net |
| 480 | 100.213556 | 192.168.0.1 | 192.168.0.138 | DNS | 246 | Standard query response 0xfc2a A api.brower.yandex.net A 213.180.193.234 NS ns3.yandex.ru NS ns4.yandex.ru A |
| 490 | 114.201929 | 192.168.0.138 | 192.168.0.1 | DNS | 73 | Standard query 0x0707 A dns.coms.one |
| 491 | 114.207407 | 192.168.0.1 | 192.168.0.138 | DNS | 422 | Standard query response 0x0707 A dns.coms.one A 83.220.160.155 A 212.109.195.93 NS vin.ns.cloudflare.com NS 1 |
| 1754 | 225.377574 | 192.168.0.138 | 192.168.0.1 | DNS | 69 | Standard query 0x7f1f A yandex.ru |
| 1755 | 225.383902 | 192.168.0.1 | 192.168.0.138 | DNS | 256 | Standard query response 0x7f1f A yandex.ru A 77.88.44.55 A 77.88.55.88 A 5.255.255.77 NS ns2.yandex.ru NS ns1. |
| 2016 | 434.809096 | 192.168.0.138 | 192.168.0.1 | DNS | 73 | Standard query 0x7db4 A dns.coms.one |

| | | | |
|--|------|---|---------------------|
| ↳ Ethernet II, Src: Intel_60:d8:d0 (2c:6d:c1:60:d8:d0), Dst: TplinkTechno_59:88:0b (28:ee:52:59:88:0b) | 0000 | 28 ee 52 59 88 0b 2c 6d c1 60 d8 d0 00 00 45 00 | (RY , e E : |
| ↳ Destination: TplinkTechno_59:88:0b (28:ee:52:59:88:0b) | 0010 | 00 43 1e 83 00 00 00 11 00 00 00 a8 00 8a c0 a8 | :C..... .xax.. |
|0..... = IG bit: Globally unique address (factory default) | 0020 | 00 01 c7 17 00 55 00 2f 82 1e c0 c0 01 00 00 01 | ...5 / |
|0..... = IG bit: Individual address (unicast) | 0030 | 00 00 00 00 00 00 03 61 70 05 07 62 72 6f 77 73 | a pi brows |
| ↳ Source: Intel_60:d8:d0 (2c:6d:c1:60:d8:d0) | 0040 | 55 72 00 79 61 6e 64 65 78 92 72 75 80 00 01 00 | er yande x ru |
|0..... = IG bit: Globally unique address (factory default) | 0050 | 01 | |
|0..... = IG bit: Individual address (unicast) | | | |
| Type: IPv4 (0x0800) | | | |
| [Stream index: 0] | | | |
| ↳ Internet Protocol Version 4, Src: 192.168.0.138, Dst: 192.168.0.1 | | | |
| 0100 = Version: 4 | | | |
|0101 = Header length: 20 bytes (5) | | | |
| ↳ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) | | | |
| Total Length: 67 | | | |
| Identification: 0x1e83 (7811) | | | |
| ↳ 000 = 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: 192.168.0.138 | | | |
| Destination Address: 192.168.0.1 | | | |
| [Stream index: 1] | | | |
| ↳ User Datagram Protocol, Src Port: 50967, Dst Port: 53 | | | |
| ↳ Domain Name System (query) | | | |

DNS Standard Query Response (пакет №64)

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|------------|---------------|---------------|----------|--------|--|
| 17 | 0.049716 | 192.168.0.1 | 192.168.0.138 | DNS | 416 | Standard query response 0xbf5f a suggest.dzen.ru A 87.250.254.186 NS a.dns.rign.net NS d.dns.rign.net NS e.dns.rign.net NS f.dns.rign.net |
| 19 | 0.054014 | 192.168.0.1 | 192.168.0.138 | DNS | 432 | Standard query response 0xb38e a dzen.ru A 185.180.200.2 A 83.222.28.15 A 5.61.23.39 NS b.dns.rign.net NS f.dns.rign.net NS e.dns.rign.net |
| 63 | 0.878113 | 192.168.0.138 | 192.168.0.1 | DNS | 81 | Standard query 0xb0b0 a api.brouser.yandex.ru |
| 64 | 0.893825 | 192.168.0.1 | 192.168.0.138 | DNS | 248 | Standard query response 0xb0b0 a api.brouser.yandex.ru A 213.180.193.234 NS ns4.yandex.ru NS ns3.yandex.ru A 87.250.250.1 A 77.88.21.1 |
| 383 | 49.910510 | 192.168.0.138 | 192.168.0.1 | DNS | 83 | Standard query 0xb6bf a www.sftconnecttest.com |
| 384 | 49.914620 | 192.168.0.1 | 192.168.0.138 | DNS | 535 | Standard query response 0xb6bf a www.sftconnecttest.com CNAME ncsl-geo.trafficmanager.net CNAME www.sftncsl.com.edgesuite.net CNAME |
| 479 | 108.210187 | 192.168.0.138 | 192.168.0.1 | DNS | 82 | Standard query 0xf02a a api.brouser.yandex.net |
| 480 | 108.215296 | 192.168.0.1 | 192.168.0.138 | DNS | 246 | Standard query response 0xf02a a api.brouser.yandex.net A 213.180.193.234 NS ns3.yandex.ru NS ns4.yandex.ru A 77.88.21.1 A 87.250.251 |
| 490 | 114.181929 | 192.168.0.138 | 192.168.0.1 | DNS | 73 | Standard query 0xb070 a dns.coms.one |
| 491 | 114.187487 | 192.168.0.1 | 192.168.0.138 | DNS | 422 | Standard query response 0xb070 a dns.coms.one A 83.220.169.155 A 212.109.195.93 NS vin.ns.cloudflare.com NS liv.ns.cloudflare.com A |
| 1754 | 225.377574 | 192.168.0.138 | 192.168.0.1 | DNS | 60 | Standard query 0xb71f a yandex.ru |
| 1755 | 225.383982 | 192.168.0.1 | 192.168.0.138 | DNS | 256 | Standard query response 0xb71f a yandex.ru A 77.88.44.55 A 77.88.55.88 A 5.255.255.77 NS ns2.yandex.ru NS ns1.yandex.ru A 93.158.134. |
| 2816 | 434.809096 | 192.168.0.138 | 192.168.0.1 | DNS | 73 | Standard query 0xb7d4 a dns.coms.one |

| | |
|---|--|
| <div>Ethernet II, Src: TplinkTechno 58:08:06 (28:0e:52:59:08:06), Dst: Intel_60:d8:d0 (2c:6d:c1:60:d8:d0)</div> <div>= Destination: Intel_60:d8:d0 (2c:6d:c1:60:d8:d0)</div> <div>....0..... = 16 bit: Globally unique address (factory default)</div> <div>....0..... = 16 bit: Individual address (unicast)</div> <div>= Source: TplinkTechno 58:08:06 (28:0e:52:59:08:06)</div> <div>....0..... = 16 bit: Globally unique address (factory default)</div> <div>....0..... = 16 bit: Individual address (unicast)</div> <div>Type: IPv4 (0x0000)</div> <div>[Stream index: 0]</div> <div>= Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.138</div> <div>0100 = Version: 4</div> <div>....0011 = Header Length: 20 bytes (5)</div> <div>> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)</div> <div>Total Length: 234</div> <div>Identification: 0xa136 (41278)</div> <div>> 0000 = Flags: 0x0</div> <div>...0 0000 0000 0000 = Fragment Offset: 0</div> <div>Time to live: 62</div> <div>Protocol: UDP (17)</div> <div>Header Checksum: 0x58f1 [validation disabled]</div> <div>[Header checksum status: Unverified]</div> <div>Source Address: 192.168.0.1</div> <div>Destination Address: 192.168.0.138</div> <div>[Stream index: 1]</div> <div>> User Datagram Protocol, Src Port: 53, Dst Port: 50667</div> <div>> Domain Name System (response)</div> | <div>0000 2c 6d c1 60 d8 d0 28 0e 52 59 08 06 08 00 45 00 ..p... (R... E...</div> <div>0010 00 0a a1 36 00 00 3e 11 38 f1 c0 a0 00 01 c0 a0 ...<...> X.....</div> <div>0020 00 8a 00 35 c7 17 00 d6 b7 74 c0 c0 81 80 00 01 ...5.....</div> <div>0030 00 01 00 82 00 84 03 61 70 69 67 62 72 6f 77 73 ... a p1.brows</div> <div>0040 65 72 06 79 a1 6e a4 65 78 02 72 75 00 00 01 00 er.yande x.ru</div> <div>0050 01 03 61 70 69 67 62 72 6f 77 73 65 72 06 59 41 ...api.br ouser-VA</div> <div>0060 4e 44 45 58 c0 1f 00 01 00 01 00 00 07 00 04 MEX.....</div> <div>0070 45 84 c1 a0 c0 2b 00 02 00 01 00 04 08 00 06</div> <div>0080 05 6e 73 34 c0 3b c0 2b 00 02 00 01 00 04 86 ns4.....</div> <div>0090 00 06 03 6e 73 33 c0 10 03 6e 73 33 c0 13 00 01 ...ns3.....ns3.3</div> <div>00a0 00 01 00 05 2e 16 00 04 57 fa 01 03 6e 73 14ns4</div> <div>00b0 c0 33 00 01 00 01 00 05 2e 16 00 04 4d 15 01MX</div> <div>00c0 c0 6e 00 1c 00 01 00 00 04 5a 00 10 2a 62 06 b82.....</div> <div>00d0 00 00 00 00 00 00 00 00 00 00 10 01 c0 82 00 1c</div> <div>00e0 00 01 00 00 04 5a 00 10 2a 02 06 b8 00 00 012.....</div> <div>00f0 00 00 00 00 00 01 00 01 2a 02 06 b8 00 00 01</div> |
|---|--|

Проанализировать информацию по протоколу QUIC.

Был захвачен трафик к современному веб-ресурсу, использующему протокол QUIC.

Описание: QUIC (Quick UDP Internet Connections) — это транспортный протокол, работающий поверх UDP. Он обеспечивает шифрование по умолчанию и более быстрое установление соединения.

На скриншотах виден обмен пакетами Initial и Handshake, которые служат для установления защищенного соединения между клиентом 192.168.0.138 и сервером 142.250.74.131.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|----------------|----------------|----------|--------|---|
| 540 | 44.361926 | 192.168.0.138 | 142.250.74.131 | QUIC | 1292 | Initial, DCID=fc65e30ab7b01fb7, PKN: 1, PING, PADDING, PING, CRYPTO, CRYPTO, PADDING, PING, CRYPTO, PING, PADDING |
| 541 | 44.362014 | 192.168.0.138 | 142.250.74.131 | QUIC | 1292 | Initial, DCID=fc65e30ab7b01fb7, PKN: 2, CRYPTO, PADDING, PING, PADDING, CRYPTO, CRYPTO, PING |
| 545 | 44.383661 | 142.250.74.131 | 192.168.0.138 | QUIC | 82 | Initial, SCID=fc65e30ab7b01fb7, PKN: 1, ACK |
| 550 | 44.385609 | 142.250.74.131 | 192.168.0.138 | QUIC | 1292 | Initial, SCID=fc65e30ab7b01fb7, PKN: 2, ACK, PADDING |
| 551 | 44.385609 | 142.250.74.131 | 192.168.0.138 | QUIC | 1292 | Initial, SCID=fc65e30ab7b01fb7, PKN: 3, CRYPTO, PADDING |
| 552 | 44.385609 | 142.250.74.131 | 192.168.0.138 | QUIC | 1292 | Initial, SCID=fc65e30ab7b01fb7, PKN: 4, CRYPTO, PADDING |
| 553 | 44.386216 | 192.168.0.138 | 142.250.74.131 | QUIC | 1292 | Initial, DCID=fc65e30ab7b01fb7, PKN: 3, ACK, PADDING |
| 554 | 44.393634 | 142.250.74.131 | 192.168.0.138 | QUIC | 1292 | Handshake, SCID=fc65e30ab7b01fb7 |
| 555 | 44.393634 | 142.250.74.131 | 192.168.0.138 | QUIC | 1292 | Handshake, SCID=fc65e30ab7b01fb7 |
| 556 | 44.393634 | 142.250.74.131 | 192.168.0.138 | QUIC | 1292 | Handshake, SCID=fc65e30ab7b01fb7 |
| 557 | 44.393925 | 192.168.0.138 | 142.250.74.131 | QUIC | 81 | Handshake, DCID=fc65e30ab7b01fb7 |
| 559 | 44.401315 | 192.168.0.138 | 142.250.74.131 | QUIC | 82 | Handshake, DCID=fc65e30ab7b01fb7 |
| 562 | 44.409890 | 142.250.74.131 | 192.168.0.138 | QUIC | 234 | Protected Payload (XPO) |

| | |
|--|--|
| Character encoding: ASCII (0) | 0010 04 fe 01 f4 40 00 80 11 00 00 E0 a8 00 8a 8a fa ...@... .. |
| [Coloring Rule Name: UDP] | 0020 4a 83 45 ce 01 b5 04 ea 0f ab c0 00 00 00 01 00 J..... |
| [Coloring Rule String: udp] | 0030 fc 65 c3 0a b7 b0 1f b7 00 00 4a 00 d0 57 b5 67D Mg |
| Ethernet II, Src: Intel_60:d8:d0 (2c:6d:c1:60:d8:d0), Dst: TplinkTechno_59:88:0b (28:ee:52:59:88:0b) | 0040 50 da da 78 ca 49 55 fd dc bc f7 7c 82 9f 04 35 P...IU... 5 |
| Destination: TplinkTechno_59:88:0b (28:ee:52:59:88:0b) | 0050 1b b8 e9 90 75 0e ca 7f b9 24 fa 9b 11 6c 9c 0c ...u...\$ 1- |
| Source: Intel_60:d8:d0 (2c:6d:c1:60:d8:d0) | 0060 84 ae 39 5e 5a 17 74 f4 e7 6c 55 ec 5c fa 7a e8 ...9 Z t... U \ t |
| Type: IPv4 (0x0800) | 0070 67 ab 24 a0 ec a8 db 52 6f fd 91 ff 9f 5a 16 5c KA R o... \ ^ |
| Stream index: 0 | 0080 e1 61 e2 eb 75 a2 22 04 97 f8 4e 2a 91 5f c6 1b a u *... f... ^ |
| Internet Protocol Version 4, Src: 192.168.0.138, Dst: 142.250.74.131 | 0090 6b e1 02 79 89 64 64 32 c2 d9 a6 30 3b a9 b0 11 k y d d2 0... ^ |
| Version: 4 | 00a0 68 18 b1 8a 47 a9 de 39 0b 1c f5 0e 22 78 64 2b m G 9 ...ad |
| Header length: 20 bytes (5) | 00b0 9e 09 96 f5 1f 52 87 c0 2c b8 f2 db dd 35 e4 1c I...R...5 |
| Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) | 00c0 45 0d 46 81 76 47 c2 74 f6 8c fe 1e 96 20 df 86 E F G...5 |
| Total length: 1278 | 00d0 49 e1 11 42 4a 91 e8 46 ab 1d 00 ab cd 7f b4 08 I...F... .. |
| Identification: 0x01f4 (500) | 00e0 aa e8 47 4d c3 63 54 21 1f b3 08 f9 7c ae cb b7 a0 G...F... |
| Flags: 0x02, Don't fragment | 00f0 50 32 70 df 00 6f 5a ef bf 0f 70 15 b1 86 21 04 2p...o2...x 1 |
| Fragment offset: 0 | 0100 3c 60 ed 90 c0 8f bc 1e f8 b2 aa 97 30 fa 15 00 C... ..0 |
| Time to live: 128 | 0110 c5 74 81 8d 09 9b 0f d1 0e 46 b8 08 ed 13 cc 17 t... ..F... .. |
| Header checksum: 0x0000 [validation disabled] | 0120 e3 5c eb 72 0a 47 33 33 c8 99 3a 6f 3b 0a d2 4a V...G33...o; 0 |
| Source address: 192.168.0.138 | 0130 07 cb 03 b8 f0 fe a5 56 ac 66 8f 34 0b 6c 48 a0 ...V...f 4 1h |
| Destination address: 142.250.74.131 | 0140 c2 54 f7 3c 50 27 70 9e 9c 17 1f 24 93 25 ff 7f T...x...5 8 |
| | 0150 30 f9 68 ba de 8b 6f 09 b3 92 69 59 5f 81 53 05 o...h...o...y...5 |
| | 0160 4a da 13 b7 ee db 9e 09 a0 16 e6 a0 0e 65 73 25 J... ..i... ..esK |
| | 0170 07 cb 03 b8 f0 fe a5 56 ac 66 8f 34 0b 6c 48 a0 ...V...f 4 1h |
| | 0180 2b c8 70 1b 15 d2 4c a3 0b 04 c3 ea a8 d3 82 c9 ...L...K...4 1h |
| | 0190 c3 61 04 ff 72 5a ec bf 50 06 07 2b 1b a0 55 4a a...Z...]+ +U |
| | 01a0 b9 90 0f 52 e2 58 1b dc c7 f9 f0 fe a2 7c 9c dd ...R...X... |
| | 01b0 c9 92 54 54 fc 68 a0 48 0e dc cf 2f 65 fe 89 82 ...T...h.../e... |

Анализ handshake протокола TCP

С помощью Wireshark проанализировать handshake протокола TCP.

Было инициировано соединение с веб-сервером, трафик был отфильтрован по `tcp.port == 80`. Были проанализированы первые три пакета, составляющие трёхступенчатое рукопожатие.

Шаг 1: SYN (пакет №143)

Клиент (192.168.0.138) отправляет серверу (188.184.67.127) сегмент с установленным флагом SYN (Synchronize). Это запрос на установку соединения.

| tcp.port == 80 | | | | | |
|----------------|-----------|----------------|----------------|----------|---|
| No. | Time | Source | Destination | Protocol | Length Info |
| 142 | 26.862027 | 192.168.0.138 | 188.184.67.127 | TCP | 66 49174 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM |
| 143 | 26.862247 | 192.168.0.138 | 188.184.67.127 | TCP | 66 49175 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM |
| 146 | 26.918116 | 188.184.67.127 | 192.168.0.138 | TCP | 66 80 → 49174 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1460 SACK_PERM WS=128 |
| 147 | 26.918264 | 192.168.0.138 | 188.184.67.127 | TCP | 54 49174 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0 |
| 148 | 26.918371 | 188.184.67.127 | 192.168.0.138 | TCP | 66 80 → 49175 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1460 SACK_PERM WS=128 |
| 149 | 26.918413 | 192.168.0.138 | 188.184.67.127 | TCP | 54 49175 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0 |
| 265 | 58.702230 | 188.184.67.127 | 192.168.0.138 | TCP | 66 [TCP Retransmission] 80 → 49175 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1460 SACK_PERM WS=128 |
| 266 | 58.702320 | 192.168.0.138 | 188.184.67.127 | TCP | 66 [TCP Dup ACK 149#1] 49175 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0 SLE=0 SRE=1 |
| 267 | 58.702757 | 188.184.67.127 | 192.168.0.138 | TCP | 66 [TCP Retransmission] 80 → 49174 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1460 SACK_PERM WS=128 |
| 268 | 58.702792 | 192.168.0.138 | 188.184.67.127 | TCP | 66 [TCP Dup ACK 147#1] 49174 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0 SLE=0 SRE=1 |

| | | | | |
|---|------|-------------------------|-------------------------|----------------|
|0..... - IG bit: Individual address (unicast) | 0000 | 28 ee 52 59 88 0b 2c 6d | c1 60 d8 d0 08 00 45 00 | (.RY...m.....E |
| Source: Intel_60:d8:d0 (2c:6d:c1:60:d8:d0) | 0010 | 00 34 94 02 40 00 80 06 | 00 00 c0 a8 00 8a bc b8 | 4 @..... |
|0..... - IG bit: Globally unique address (factory default) | 0020 | 43 7f c0 17 00 50 7e e0 | 36 bf 0f 00 00 00 80 02 | C...P...6..... |
|0..... - IG bit: Individual address (unicast) | 0030 | ff ff c1 90 00 00 02 04 | 05 b4 01 03 03 08 01 01 | |
| Type: IPv4 (0x0000) | 0040 | 04 02 | | |
| [Stream index: 0] | | | | |
| Internet Protocol Version 4, Src: 192.168.0.138, Dst: 188.184.67.127 | | | | |
| Transmission Control Protocol, Src Port: 49175, Dst Port: 80, Seq: 0, Len: 0 | | | | |
| Source Port: 49175 | | | | |
| Destination Port: 80 | | | | |
| [Stream index: 23] | | | | |
| [Stream Packet Number: 1] | | | | |
| [Conversation completeness: Incomplete, ESTABLISHED (7)] | | | | |
| [TCP Segment Len: 0] | | | | |
| Sequence Number: 0 (relative sequence number) | | | | |
| Sequence Number (raw): 2128623119 | | | | |
| [Next Sequence Number: 1 (relative sequence number)] | | | | |
| Acknowledgment Number: 0 | | | | |
| Acknowledgment number (raw): 0 | | | | |
| 1000 = Header Length: 32 bytes (8) | | | | |
| Flags: 0x002 (SYN) | | | | |
| Window: 65535 | | | | |
| [Calculated window size: 65535] | | | | |
| Checksum: 0xc190 [unverified] | | | | |
| [Checksum Status: Unverified] | | | | |
| Urgent Pointer: 0 | | | | |
| Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No | | | | |
| [Timestamps] | | | | |
| [Client Contiguous Streams: 1] | | | | |

Шаг 2: SYN, ACK (пакет №146)

Сервер отвечает сегментом с двумя флагами: SYN (он также предлагает синхронизировать номер последовательности) и ACK (Acknowledgment - подтверждает получение первого пакета от клиента).

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|----------------|----------------|----------|--------|--|
| 142 | 26.062027 | 192.168.0.138 | 188.184.67.127 | TCP | 66 | 49174 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM |
| 143 | 26.062247 | 192.168.0.138 | 188.184.67.127 | TCP | 66 | 49175 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM |
| 146 | 26.910116 | 188.184.67.127 | 192.168.0.138 | TCP | 66 | 80 → 49174 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1460 SACK_PERM WS=128 |
| 147 | 26.910264 | 192.168.0.138 | 188.184.67.127 | TCP | 54 | 49174 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0 |
| 148 | 26.918371 | 188.184.67.127 | 192.168.0.138 | TCP | 66 | 80 → 49175 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1460 SACK_PERM WS=128 |
| 149 | 26.918413 | 192.168.0.138 | 188.184.67.127 | TCP | 54 | 49175 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0 |
| 265 | 58.702230 | 188.184.67.127 | 192.168.0.138 | TCP | 66 | [TCP Retransmission] 80 → 49175 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1460 SACK_PERM WS=128 |
| 266 | 58.702280 | 192.168.0.138 | 188.184.67.127 | TCP | 66 | [TCP Dup ACK 14941] 49175 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0 SLE=0 SRE=1 |
| 267 | 58.702757 | 188.184.67.127 | 192.168.0.138 | TCP | 66 | [TCP Retransmission] 80 → 49174 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1460 SACK_PERM WS=128 |
| 268 | 58.702792 | 192.168.0.138 | 188.184.67.127 | TCP | 66 | [TCP Dup ACK 14741] 49174 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0 SLE=0 SRE=1 |

| | | |
|--|--|-----------|
|0..... = IG bit: Individual address (unicast) | 0000 2c 6d c1 00 d8 d0 28 ee 52 59 08 0b 00 00 45 00 | 4 0 / 2 C |
| Source: Tplinktechno.59:08:0b (28ree52:59:08:0b) | 0010 00 34 00 00 40 00 2f 06 8a 5a bc b0 43 7f c0 a3 | P To F |
|0..... = IG bit: Globally unique address (factory default) | 0020 00 8a 00 50 c0 16 54 0f fe c5 46 60 b0 96 80 12 | xX |
|0..... = IG bit: Individual address (unicast) | 0030 7d 78 25 8c 00 00 02 04 95 b4 01 01 04 02 01 03 | |
| Type: IPv4 (0x0800) | 0040 03 07 | |
| [Stream index: 0] | | |
| Internet Protocol Version 4, Src: 188.184.67.127, Dst: 192.168.0.138 | | |
| Transmission Control Protocol, Src Port: 80, Dst Port: 49174, Seq: 0, Ack: 1, Len: 0 | | |
| Source Port: 80 | | |
| Destination Port: 49174 | | |
| [Stream index: 22] | | |
| [Stream Packet Number: 2] | | |
| [Conversation completeness: Incomplete, ESTABLISHED (7)] | | |
| [TCP Segment Len: 0] | | |
| Sequence Number: 0 (relative sequence number) | | |
| Sequence Number (raw): 1616625861 | | |
| [Next Sequence Number: 1 (relative sequence number)] | | |
| Acknowledgment Number: 1 (relative ack number) | | |
| Acknowledgment number (raw): 1180741782 | | |
| 1000 = Header Length: 32 bytes (0) | | |
| Flags: 0x012 (SYN, ACK) | | |
| Window: 32120 | | |
| [Calculated window size: 32120] | | |
| Checksum: 0x258c [unverified] | | |
| [Checksum Status: Unverified] | | |
| Urgent Pointer: 0 | | |
| Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, | | |
| [Timestamps] | | |
| [SEQ/ACK analysis] | | |

ACK (пакет №147)

Клиент отправляет серверу сегмент с флагом ACK, подтверждая получение пакета SYN, ACK от сервера. На этом рукопожатие завершается, и соединение считается установленным.

The image displays a Wireshark packet capture of a TCP connection. The top pane shows a list of packets, with packet 147 highlighted. The middle pane shows the packet details for the selected packet, and the bottom pane shows the raw packet data in hexadecimal and ASCII.

Packet List:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|----------------|----------------|----------|--------|--|
| 142 | 26.862027 | 192.168.0.138 | 188.184.67.127 | TCP | 66 | 49174 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM |
| 143 | 26.862247 | 192.168.0.138 | 188.184.67.127 | TCP | 66 | 49175 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM |
| 146 | 26.918116 | 188.184.67.127 | 192.168.0.138 | TCP | 66 | 80 → 49174 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1460 SACK_PERM WS=128 |
| 147 | 26.918264 | 192.168.0.138 | 188.184.67.127 | TCP | 54 | 49174 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0 |
| 148 | 26.918371 | 188.184.67.127 | 192.168.0.138 | TCP | 66 | 80 → 49175 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1460 SACK_PERM WS=128 |
| 149 | 26.918413 | 192.168.0.138 | 188.184.67.127 | TCP | 54 | 49175 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0 |
| 265 | 58.702220 | 188.184.67.127 | 192.168.0.138 | TCP | 66 | [TCP Retransmission] 80 → 49175 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1460 SACK_PERM WS=128 |
| 266 | 58.702320 | 192.168.0.138 | 188.184.67.127 | TCP | 66 | [TCP Dup ACK] 49175 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0 SLE=0 SRE=1 |
| 267 | 58.702757 | 188.184.67.127 | 192.168.0.138 | TCP | 66 | [TCP Retransmission] 80 → 49174 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1460 SACK_PERM WS=128 |
| 268 | 58.702792 | 192.168.0.138 | 188.184.67.127 | TCP | 66 | [TCP Dup ACK] 49174 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0 SLE=0 SRE=1 |

Packet Details:

- ...0 ...0 ...0 ...0 = IG bit: Individual address (unicast)
- Source: Intel_60:d8:d0 (2c:6d:c1:60:d8:d0)
- ...0 ...0 ...0 ...0 = IG bit: Globally unique address (factory default)
- ...0 ...0 ...0 ...0 = IG bit: Individual address (unicast)
- Type: IPv4 (0x0000)
- [Stream index: 0]
- Internet Protocol Version 4, Src: 192.168.0.138, Dst: 188.184.67.127
- Transmission Control Protocol, Src Port: 49174, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
 - Source Port: 49174
 - Destination Port: 80
 - [Stream index: 22]
 - [Stream Packet Number: 3]
 - [Conversation completeness: Incomplete, ESTABLISHED (7)]
 - [TCP Segment Len: 0]
 - Sequence Number: 1 (relative sequence number)
 - Sequence Number (raw): 1180741782
 - [Next Sequence Number: 1 (relative sequence number)]
 - Acknowledgment Number: 1 (relative ack number)
 - Acknowledgment number (raw): 1616025862
 - 0101 ... = Header Length: 20 bytes (5)
 - Flags: 0x010 (ACK)
 - Window: 255
 - [Calculated window size: 65280]
 - [Window size scaling factor: 256]
 - Checksum: 0xc184 [unverified]
 - [Checksum Status: Unverified]
 - Urgent Pointer: 0
 - [Timestamps]
 - [SEQ/ACK analysis]

Raw Data:

```
0000 28 ee 52 59 88 0b 2c 6d c1 60 d8 d0 00 00 45 00 (-HY...m.....E
0010 00 28 94 03 40 00 80 06 00 00 c0 a8 00 8a bc b8 ( @.....
0020 43 7f c0 16 00 50 40 60 b0 96 54 0f fe c6 50 10 C...P?..To..P
0030 00 ff c1 84 00 00
```

График Потока

Для визуализации обмена был построен график потока, на котором наглядно представлено всё ТСР-соединение, включая начальное трёхступенчатое рукопожатие и последующие повторные передачи (Retransmissions).

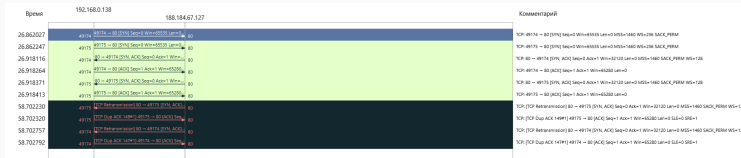


Рис. 6: График Потока

Выводы

В ходе работы изучение посредством Wireshark кадров Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP прошли успешно.