

1) Ανίχνευση

Η ανίχνευση είχε διάρκεια 95.231486 sec

2) Πρωτόκολλα

| Επίπεδο Δεδομένων | Επίπεδο Δικτύου | Επίπεδο Μεταφοράς | Επίπεδο Εφαρμογών |
|----------------------|--------------------|----------------------|----------------------|
| ARP | ICMPv6 | TCP | HTTP |
| | | QUIC | DNS |
| | | | SSDP |
| | | | TLSv1.2 |

Protocol

▼ Frame

▼ Ethernet

▼ Internet Protocol Version 6

▼ User Datagram Protocol

QUIC IETF

Domain Name System

▼ Transmission Control Protocol

Transport Layer Security

Data

Internet Control Message Protocol v6

▼ Internet Protocol Version 4

▼ User Datagram Protocol

Simple Service Discovery Protocol

Domain Name System

▼ Transmission Control Protocol

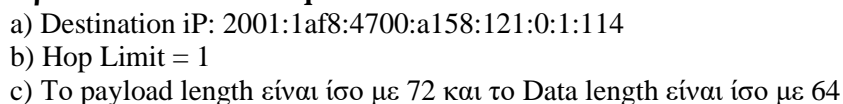
Transport Layer Security

Data

Address Resolution Protocol

Τα πρωτόκολλα DNS και SSDP χρησιμοποιούν το πρωτόκολλο QUIC. Ωστόσο το QUIC αποτελεί ένα multiplex stream transport πάνω στο πρωτόκολλο UDP (σύμφωνα με την Google).

Σημειώνουμε ωστόσο ότι δεν εμφανίζει κάτι καθώς το Wireshark έκανε capture το icmpv6, κάτι που σημαίνει ότι ο provider μου τρέχει όλο το δίκτυο σε IPv6.



```
Payload Length: 72
Next Header: ICMPv6 (58)
Hop Limit: 1
Source Address: 2a02:587:d25:6100:5045:af1d:cc3f:92e8
Destination Address: 2001:1af8:4700:a158:121:0:1:114
```

a) Destination iP: 2a02:587:d25:6100:5045:af1d:cc3f:92e8
b) Source iP: 2a00:1cb8:2000::69

```
Payload Length: 120
Next Header: ICMPv6 (58)
Hop Limit: 60
Source Address: 2a00:1cb8:2000::69
Destination Address: 2a02:587:d25:6100:5045:af1d:cc3f:92e8
```

7) **Source IP διευθύνσεις των πακέτων που μεταφέρουν ICMP Time Exceeded μηνύματα**

- 2a00:1cb8:2000::69
- 2a00:1cb8:1::1b6
- 2a03:2280:36::82
- 2a03:2280:36::68
- 2a03:2280:38::83
- 2001:1af8:4700:0:81:17:34:19
- 2a07:3b80:3::2
- 2001:1af8:4700:a03f::b

```
C:\Users\Μαρίνα Σαμ>tracert www.acm.org

Tracing route to www.acm.org [2001:1af8:4700:a158:121:0:1:114]
over a maximum of 30 hops:

 1      *          *          *          Request timed out.
 2      *          *          *          Request timed out.
 3      *          *          *          Request timed out.
 4      *          20 ms       *          2a00:1cb8:2000::69
 5      *          *          23 ms      2a00:1cb8:1::1b6
 6      *          *          *          Request timed out.
 7      492 ms     182 ms     254 ms  2a03:2280:36::82
 8      459 ms     817 ms     262 ms  2a03:2280:36::68
 9      211 ms     568 ms     812 ms  2a03:2280:38::83
10     642 ms     175 ms    1019 ms 2001:1af8:4700:0:81:17:34:19
11     583 ms     719 ms     708 ms 2a07:3b80:3::2
12     609 ms    1021 ms     201 ms 2001:1af8:4700:a03f::b
13     816 ms     817 ms     644 ms 2001:1af8:4700:a158:121:0:1:114

Trace complete.
```

Τα πρώτα Request Timed Outs είναι αρκετά συνηθισμένα σε ένα traceroute και μπορούμε να τα αγνοήσουμε. Σημαίνει ότι η συσκευή δεν ανταποκρίνεται σε ICMP Requests. Κατά τα άλλα, οι διευθύνσεις IP που βρήκαμε με το cmd είναι ίδιες με αυτές που βρήκε το WireShark, με εξαίρεση το τελευταίο IP source, το οποίο αναφέρεται στο τελευταίο Echo Reply.

| | | | | |
|---------------|------------------------|------------------------|--------|---|
| 239 91.750677 | 2001:1af8:4700:a158... | 2a02:587:d25:6100:5... | ICMPv6 | 126 Echo (ping) reply id=0x0001, seq=339, hop limit=52 (request in 238) |
|---------------|------------------------|------------------------|--------|---|