



ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Δίκτυα Υπολογιστών

Αναφορά 3ης Εργαστηριακής Άσκησης

**Ραπτόπουλος Πέτρος (ει19145)
Ομάδα 3**

Άσκηση 1: Ο πίνακας ARP

Χρησιμοποιώντας εντολές φλοιού σε terminal του ubuntu βρίσκουμε τις πληροφορίες που ζητούνται:

1.1) Εντολή για προβολή περιεχομένων του πίνακα ARP: **arp** ή **arp -a**

1.2) Εντολή για διαγραφή περιεχομένων του πίνακα ARP: **arp -d**

```
SYNOPSIS
arp [-vn] [-H type] [-t if] [-ae] [hostname]
arp [-v] [-t if] -d hostname [pub]
arp [-v] [-t type] [-t if] -s hostname hw_addr [temp]
arp [-v] [-H type] [-t if] -s hostname hw_addr [netmask nn] pub
arp [-v] [-H type] [-t if] -Ds hostname ifname [netmask nn] pub
arp [-vnD] [-H type] [-t if] -f [filename]

DESCRIPTION
Arp manipulates or displays the kernel's IPv4 network neighbour cache. It can add entries to the table, delete one or display the current content.

ARP stands for Address Resolution Protocol, which is used to find the media access control address of a network neighbour for a given IPv4 Address.

MODES
arp with no mode specifier will print the current content of the table. It is possible to limit the number of entries printed, by specifying an hardware address type, interface name or host address.

arp -d address will delete a ARP table entry. Root or netadmin privilege is required to do this. The entry is found by IP address. If a hostname is given, it will be resolved before looking up the entry in the ARP table.

arp -s address hw_addr is used to set up a new table entry. The format of the hw_addr parameter is dependent on the hardware class, but for most classes one can assume that the usual presentation can be used. For the Ethernet class, this is 6 bytes in hexadecimal, separated by colons. When adding proxy arp entries (that is those with the publish flag set) a netmask may be specified to proxy arp for entire subnets. This is not good practice, but is supported by older kernels because it can be useful. If the temp flag is not supplied entries will be permanent stored into the ARP cache. To simplify setting up entries for one of your own network interfaces, you can use the arp -Ds address ifname form, in that case the hardware address is taken from the interface with the specified name.

OPTIONS
-v, --verbose
    Tell the user what is going on by being verbose.

-n, --numeric
    Shows numerical addresses instead of trying to determine symbolic host, port or user names.

-H type, --hw-type type, -t type
    When setting or reading the ARP cache, this optional parameter tells arp which class of entries it should check for. The default value of this parameter is ether (i.e. hardware code 0x01 for IEEE 802.3 10Mbps Ethernet). Other values might include network technologies such as ARCnet (arcnet), PRONET (pronet), AX.25 (ax25) and NET/ROM (netrom).

-a
    Use alternate BSD style output format (with no fixed columns).

-e
    Use default Linux style output format (with fixed columns).

-D, --use-device
    Instead of a hw_addr, the given argument is the name of an interface. arp will use the MAC address of that interface for the table entry. This is usually the best option to set up a proxy ARP entry to yourself.

-t If, --device If
    Selects an interface. When dumping the ARP cache only entries matching the specified interface will be printed. When setting a permanent or temp ARP entry this interface will be associated with the entry; if this option is not used, the kernel will guess based on the routing table. For pub entries the specified interface is the interface on which ARP requests will be answered.
    NOTE: This has to be different from the interface to which the IP datagrams will be routed. NOTE: As of kernel 2.2.0 it is no longer possible to set an ARP entry for an entire subnet. Linux instead does automatic proxy arp when a route exists and it is forwarding. See arp(7) for details. Also the dontpub option which is available for delete and set operations cannot be used with

Manual page arp(8) line 6/95 69% (press h for help or q to quit)
```

1.3) Διεύθυνση IPv4 της προκαθορισμένης πύλης: **147.102.200.200**

Διεύθυνση IPv4 του εξυπηρετητή DNS: **147.102.224.243**

```
petrosrapto@petrosraptoAssistant:~$ systemd-resolve --status | grep Current
Current Scopes: none
Current Scopes: none
Current Scopes: DNS
Current DNS Server: 147.102.224.243
```

```
petrosrapto@petrosraptoAssistant:~$ arp -a
? (147.102.202.160) at <incomplete> on wlp1s0
gateway (147.102.200.200) at 08:ec:f5:d0:d9:1d [ether] on wlp1s0
? (147.102.203.254) at 00:50:56:b5:aa:aa [ether] on wlp1s0
```

1.4) Περιεχόμενα πίνακα ARP του υπολογιστή μας:

```
petrosrapto@petrosraptoAssistant:~$ arp -a
? (147.102.203.191) at ec:be:f5:e9:4a [ether] on wlp1s0
? (147.102.202.160) at <incomplete> on wlp1s0
gateway (147.102.200.200) at 08:ec:f5:d0:d9:1d [ether] on wlp1s0
? (147.102.203.254) at 00:50:56:b5:aa:aa [ether] on wlp1s0
```

1.5) Υπάρχει η διεύθυνση IPv4 της προκαθορισμένης πύλης στον πίνακα ARP;; Ναι

Υπάρχει η διεύθυνση IPv4 του εξυπηρετητή DNS στον πίνακα ARP;; Όχι

Σημείωση: Στον παραπάνω πίνακα περιέχονται οι διευθύνσεις MAC και IPv4 των υπολογιστών με τους οποίους έχει επικοινωνήσει πρόσφατα ο δικός μας.

1.6) Αδειάζουμε τον πίνακα ARP και εκτελούμε την εντολή ping χρησιμοποιώντας κάποια διεύθυνση IPv4 του 1.4:

```
petrosrapto@petrosraptoAssistant:~$ sudo ip -s -s neigh flush all
[sudo] password for petrosrapto:
147.102.203.191 dev wlp1s0 lladdr ec:be:f5:e9:4a used 842/902/842 probes 0 STALE
147.102.202.160 dev wlp1s0 used 999/1290/995 probes 6 FAILED
147.102.200.200 dev wlp1s0 lladdr 08:ec:f5:d0:d9:1d ref 1 used 150/6/147 probes 1 REACHABLE
147.102.203.254 dev wlp1s0 lladdr 00:50:56:b5:aa:aa ref 1 used 22/17/17 probes 1 REACHABLE
*** Round 1, deleting 4 entries ***
*** Flush is complete after 1 round ***
petrosrapto@petrosraptoAssistant:~$ arp -a
petrosrapto@petrosraptoAssistant:~$ man ping
petrosrapto@petrosraptoAssistant:~$ ping 147.102.203.254
PING 147.102.203.254 (147.102.203.254) 56(84) bytes of data.
64 bytes from 147.102.203.254: icmp_seq=1 ttl=64 time=2.48 ms
64 bytes from 147.102.203.254: icmp_seq=2 ttl=64 time=2.31 ms
64 bytes from 147.102.203.254: icmp_seq=3 ttl=64 time=2.44 ms
64 bytes from 147.102.203.254: icmp_seq=4 ttl=64 time=2.43 ms
64 bytes from 147.102.203.254: icmp_seq=5 ttl=64 time=3.00 ms
64 bytes from 147.102.203.254: icmp_seq=6 ttl=64 time=2.29 ms
64 bytes from 147.102.203.254: icmp_seq=7 ttl=64 time=2.25 ms
64 bytes from 147.102.203.254: icmp_seq=8 ttl=64 time=40.3 ms
64 bytes from 147.102.203.254: icmp_seq=9 ttl=64 time=5.20 ms
64 bytes from 147.102.203.254: icmp_seq=10 ttl=64 time=2.13 ms
64 bytes from 147.102.203.254: icmp_seq=11 ttl=64 time=2.30 ms
64 bytes from 147.102.203.254: icmp_seq=12 ttl=64 time=1.37 ms
64 bytes from 147.102.203.254: icmp_seq=13 ttl=64 time=4.58 ms
64 bytes from 147.102.203.254: icmp_seq=14 ttl=64 time=2.63 ms
64 bytes from 147.102.203.254: icmp_seq=15 ttl=64 time=2.30 ms
64 bytes from 147.102.203.254: icmp_seq=16 ttl=64 time=0.943 ms
64 bytes from 147.102.203.254: icmp_seq=17 ttl=64 time=4.14 ms
64 bytes from 147.102.203.254: icmp_seq=18 ttl=64 time=2.74 ms
64 bytes from 147.102.203.254: icmp_seq=19 ttl=64 time=4.13 ms
64 bytes from 147.102.203.254: icmp_seq=20 ttl=64 time=2.31 ms
64 bytes from 147.102.203.254: icmp_seq=21 ttl=64 time=2.98 ms
64 bytes from 147.102.203.254: icmp_seq=22 ttl=64 time=3.44 ms
^C
-- 147.102.203.254 ping statistics --
22 packets transmitted, 22 received, 0% packet loss, time 21031ms
rtt min/avg/max/mdev = 0.943/4.484/40.288/7.873 ms
```

1.7) Βλέπουμε πάλι τον πίνακα ARP του υπολογιστή μας.
Παρατηρούμε ότι η διεύθυνση που χρησιμοποιήθηκε στο ερώτημα 1.6 ξαναεμφανίζεται στον πίνακα ARP.

```
petrosrapto@petrosraptoAssistant:~$ arp -a
gateway (147.102.200.200) at 08:ec:f5:d0:d9:1d [ether] on wlp1s0
? (147.102.203.254) at 00:50:56:b5:aa:aa [ether] on wlp1s0
```

Οστόσο παρατηρούμε ότι ξαναεμφανίζεται το default gateway, το οποίο σύμφωνα με τη θεωρία δεν θα έπρεπε να συμβαίνει. Εφόσον η διεύθυνση 147.102.203.254

υπάρχει στον πίνακα ARP του υπολογιστή μας, ανήκει στο ίδιο υποδίκτυο και η επικοινωνία μας με την εν λόγω διεύθυνση δεν προϋποθέτει την διαμεσολάβηση του δρομολογητή. Ίσως διεργασίες ανεξάρτητες της ping που τρέχουν στο παρασκήνιο προκαλούν την επανεμφάνιση της διεύθυνσης του default gateway στον πίνακα ARP.

Εκτελούμε την εντολή sudo systemctl-resolve --flush-caches, αδειάζουμε τον πίνακα ARP και επισκεπτόμαστε την ιστοσελίδα <http://edu-dy.cn.ntua.gr/lab3>:

```
petrosrapto@petrosraptoAssistant:~$ sudo systemctl-resolve --flush-caches
petrosrapto@petrosraptoAssistant:~$ sudo ip -s -s neigh flush all
147.102.200.200 dev wlp1s0 lladdr 08:ec:f5:d0:d9:1d ref 1 used 17/6/17 probes 4 REACHABLE

*** Round 1, deleting 1 entries ***
*** Flush is complete after 1 round ***
petrosrapto@petrosraptoAssistant:~$ arp -a
petrosrapto@petrosraptoAssistant:~$ arp -a
gateway (147.102.200.200) at 08:ec:f5:d0:d9:1d [ether] on wlp1s0
```

Σημείωση: Ανάμεσα από τις δύο εντολές arp -a έγινε η επίσκεψη στην ιστοσελίδα.

1.8) Ποιες από τις διευθύνσεις IPv4 του ερωτήματος 1.3 καταχωρήθηκαν στον πίνακα ARP;; **Καταχωρήθηκε αποκλειστικά η διεύθυνση του default gateway.** Σύμφωνα με τη θεωρία, εάν πελάτης και εξυπηρετητής βρίσκονται σε διαφορετικά υποδίκτυα, η επικοινωνία στο στρώμα IP γίνεται μέσω της πύλης που υποδεικνύει ο πίνακας δρομολόγησης (στην περίπτωσή μας το default gateway).

1.9) Έχει καταχωρηθεί η διεύθυνση IPv4 του edu-dy.cn.ntua.gr στον πίνακα ARP;; **'Οχι.** Όπως είπαμε και στον προηγούμενο ερώτημα η εν λόγω διεύθυνση IP βρίσκεται εκτός τοπικού δικτύου. Συνεπώς η επικοινωνία γίνεται μέσω του δρομολογητή (default gateway) για το στρώμα ζεύχης πρωτοκόλλου ethernet.

Άσκηση 2: Το πλαίσιο Ethernet

Αδειάζουμε την προσωρινή μνήμη (cache) του πλοηγού μας, αδειάζουμε τον πίνακα ARP, αρχίζουμε την καταγραφή, επισκεπτόμαστε την ιστοσελίδα <http://edu-dy.cn.ntua.gr/lab3> και σταματάμε την καταγραφή μόλις φορτώσει η σελίδα. Ακόμη απενεργοποιούμε την επιλογή Resolve Physical Address και εφαρμόζουμε φίλτρο απεικόνισης ip or ipn6 or arp:

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Ip or ipv6 or arp

No.	Time	Source	Destination	Protocol	Length Info
15	2.065483160	142.251.209.36	147.102.203.117	UDP	162 443 → 40658 Len=120
16	2.090997399	147.102.203.117		UDP	75 40658 → 443 Len=33
17	2.148068726	ec:be:5f:8e:e9:4a	99:78:41:15:16:66	ARP	60 Who has 147.102.203.117? Tell 147.102.203.191
18	2.148090618	99:78:41:15:16:66	ec:be:5f:8e:e9:4a	ARP	42 147.102.203.117 is at 99:78:41:15:16:66
19	3.110906823	142.166.221.38	147.102.203.117	TCP	66 56951 → 40906 [SYN] Seq=0 Win=65535 Len=0 MSS=1398 WS=256 SAC...
20	6.242963083	147.102.203.117	35.224.179.84	TCP	74 33344 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
21	6.243815579	35.224.179.84	147.102.203.117	TCP	74 80 → 33344 [SYN, ACK] Seq=1 Ack=1 Win=64768 Len=0 MSS=1420 SA...
22	6.453893405	147.102.203.117	35.224.179.84	TCP	66 33344 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4213539267...
23	6.453893405	147.102.203.117	35.224.179.84	TCP	153 GET / HTTP/1.1
24	6.661438929	35.224.179.84	147.102.203.117	HTTP	60 33344 [ACK] Seq=1 Ack=88 Win=65024 Len=0 TSval=6479999027...
25	6.662010279	35.224.179.84	147.102.203.117	HTTP	214 HTTP/1.1 204 No Content
26	6.662010375	147.102.203.117	35.224.179.84	TCP	66 33344 → 80 [ACK] Seq=88 Ack=149 Win=64128 Len=0 TSval=4213539...
27	6.662010375	35.224.179.84	147.102.203.117	TCP	66 89 → 33344 [FIN, ACK] Seq=149 Ack=88 Win=65024 Len=0 TSval=64...
28	6.662104038	147.102.203.117	35.224.179.84	TCP	66 33344 → 80 [FIN, ACK] Seq=88 Ack=150 Win=64128 Len=0 TSval=42...
29	6.870536809	35.224.179.84	147.102.203.117	TCP	66 89 → 33344 [ACK] Seq=150 Ack=89 Win=65024 Len=0 TSval=6479992...
30	9.235249427	0.0.0.0	255.255.255.255	DHCP	349 DHCP Request - Transaction ID 0xe0arf9540
31	9.238862897	147.102.203.254	147.102.203.117	DHCP	342 DHCP ACK - Transaction ID 0xe0arf9540
32	9.238862897	147.102.203.117	255.255.255.254	TCP	378 Destination unreachable (Port unreachable)
33	9.699557848	89.248.163.181	147.102.203.117	TCP	54 50314 → 5662 [SYN] Seq=0 Win=1024 Len=0
Frame 23: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface wlp1s0, id 0					
Ethernet II, Src: 08:ec:f5:d0:d9:1d (08:ec:f5:d0:d9:1d), Dst: 147.102.203.117 (147.102.203.117)					
Destination: 147.102.203.117 (147.102.203.117)					
Source: 08:ec:f5:d0:d9:1d (08:ec:f5:d0:d9:1d)					
Type: IPv4 (0x0800)					
Internet Protocol Version 4, Src: 147.102.203.117, Dst: 35.224.179.84					
0100 08 ec f5 d0 d9 1d 90 78 41 15 16 66 08 09 45 00 x A- f- E					
0020 90 8b 75 49 49 00 49 06 98 1c 93 66 cb 75 23 e0 f- #					
0020 aa 54 82 49 00 50 03 29 e9 5d 8d 34 32 23 80 18 T @ P 1-2#					
0030 01 f6 06 04 00 00 01 01 08 0a fb 25 81 c3 26 9f % &					
0040 ad 5d 45 b4 20 29 48 54 54 50 2f 31 2e 31]GET / HTTP/1.1					
0050 0d 0a 48 6f 73 74 3a 29 63 6f 6e 6e 65 63 74 69 Host: connecti					
0060 76 69 74 79 2d 63 65 63 6b 2e 75 62 75 6e 74 vity-che ck.ubuntu					
0070 75 2e 63 6f 6d 6d 41 63 63 65 74 70 74 3a 29 u.com -A ccept: *					
0080 2f 2a 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 29 /* Conn ectio					
0090 63 6c fd 73 65 0d 0a 0d 0a close . . .					

2.2) Έχει καταγραφεί το προοίμιο και γιατί: **'Όχι, το προοίμιο δεν ανήκει στο πλαίσιο Ethernet και συνεπώς δεν καταγράφεται.**

Η χρησιμότητα του προοιμίου είναι η επίτευξη συγχρονισμού μεταξύ πομπού και δέκτη.

2.3) Καταγράφεται το CRC;: **'Όχι.** To Wireshark καταγράφει δεδομένα τα οποία καταγράφει η βιβλιοθήκη libpcap, τα δικαιώματα της οποίας περιορίζονται από το λειτουργικό σύστημα. Τα περισσότερα

λειτουργικά συστήματα δεν υποστηρίζουν καταγραφή του CRC.

- 2.4) Τιμή του πεδίου Type της επικεφαλίδας Ethernet για πακέτα IPv4: **0x0800** (φαίνεται παραπάνω)
- 2.5) Τιμή του πεδίου Type της επικεφαλίδας Ethernet για πακέτα ARP: **0x0806** (σύμφωνα με την 2η Εργ. Άσκηση)
- 2.6) Τιμή του πεδίου Type της επικεφαλίδας Ethernet για πακέτα IPv6: Δεν καταγράφηκαν πακέτα IPv6 αλλά σύμφωνα με το διαδίκτυο η τιμή είναι **0x86DD**.

Βρίσκουμε και επιλέγουμε, όπως φαίνεται παραπάνω, το πλαίσιο Ethernet που περιέχει το πρώτο μήνυμα HTTP GET προς το edu-dy.cn.ntua.gr. Σύμφωνα με την παραπάνω εικόνα:

2.7) Διεύθυνση MAC πηγής του πλαισίου: **90:78:41:15:16:66**

2.8) Διεύθυνση MAC προορισμού του πλαισίου: **08:ec:f5:do:d9:1d**

2.9) Είναι η παραπάνω διεύθυνση MAC αυτή του edu-dy.cn.ntua.gr;: **'Οχι**

2.10) Σε ποια συσκευή ανήκει και γιατί;: **Παρατηρούμε ότι η διεύθυνση αυτή ανήκει στον δρομολογητή (default gateway) σύμφωνα με το ερώτημα 1.3. Αυτό συμβαίνει διότι η διεύθυνση IP της σελίδας ανήκει σε διαφορετικό υποδίκτυο από αυτό του υπολογιστή μας και έτσι τα πακέτα δρομολογούνται στο default gateway μέσω του τοπικού μας δικτύου ώστε να καταλήξουν εν τέλει στην ζητούμενη διεύθυνση IP.**

2.11) Μήκος του πλαισίου σε byte: **153**

2.12) Byte του πλαισίου Ethernet που προηγούνται του χαρακτήρα ASCII "G" της λέξης GET: **66**

Όπως φαίνεται στην παραπάνω εικόνα επιλέγουμε στο πεδίο δεδομένων τη λέξη GET ώστε να υπογραμμιστούν τα κατάλληλα bytes του πλαισίου. Κάνουμε τη μέτρηση αό την αρχή του πλαισίου.

Στη συνέχεια επιλέγουμε το πλαίσιο Ethernet που περιέχει την απάντηση στο προηγούμενο μήνυμα HTTP:

2.13) Διεύθυνση MAC αποστολέα πλαισίου:

08:ec:f5:do:d9:1d

2.14) Είναι η παραπάνω διεύθυνση MAC αυτή του edu-dy.cn.ntua.gr;: **'Οχι**

2.15) Σε ποια συσκευή ανήκει:

Στον δρομολογητή (default gateway)

2.16) Διεύθυνση MAC παραλήπτη πλαισίου:

90:78:41:15:16:66

2.17) Σε ποιον υπολογιστή ανήκει:

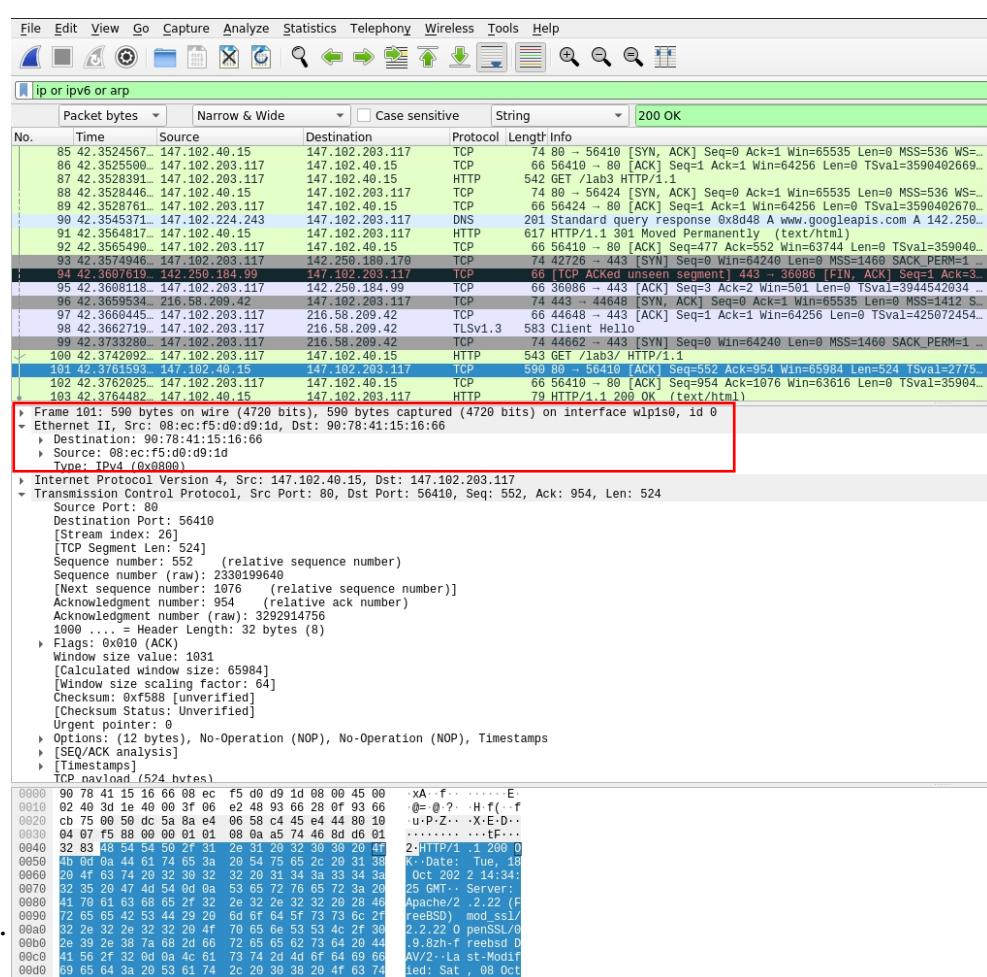
Στην κάρτα δικτύου του υπολογιστή μας

2.18) Μήκος του πλαισίου σε byte: **590**

2.19) Byte του πλαισίου Ethernet που προηγούνται του χαρακτήρα ASCII "O" της λέξης OK: **79**

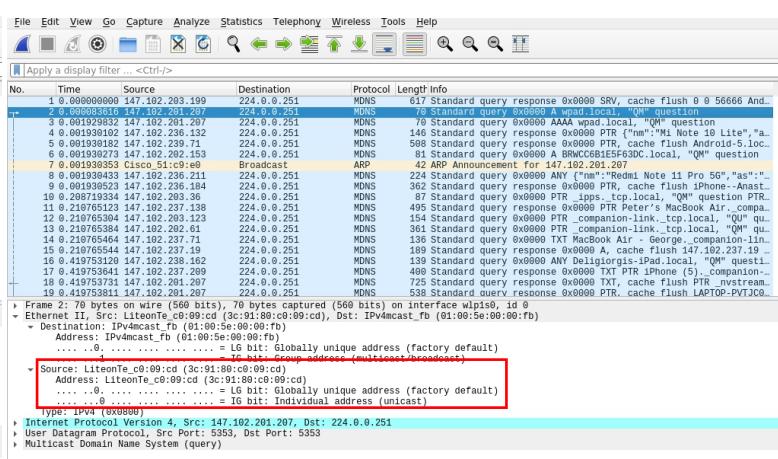
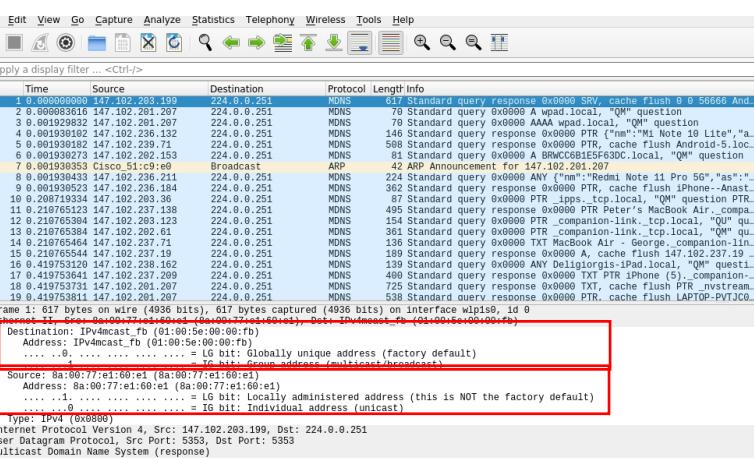
Όπως φαίνεται στην διπλανή εικόνα επιλέγουμε στο πεδίο δεδομένων τη λέξη OK ώστε να υπογραμμιστούν τα κατάλληλα bytes του πλαισίου.

Κάνουμε τη μέτρηση από τη αρχή πλαισίου.



Άσκηση 3: Περισσότερα για τα πλαίσια Ethernet

Ξεκινάμε μια νέα καταγραφή Wireshark με φίλτρο σύλληψης *ether multicast* ώστε να καταγράφονται μόνο πλαίσια που απευθύνονται σε πολλαπλούς προορισμούς. Επισκεπτόμαστε την ιστοθέση <http://edu-dy.cn.ntua.gr/lab3.pcap> και κατεβάζουμε το αρχείο lab3.pcap. Περιμένουμε λίγα δευτερόλεπτα και σταματάμε την καταγραφή:



No.	Time	Source	Destination	Protocol	Length/Info
1	0:00:00:00:00.000	147.192.283.199	ff:ff:ff:ff:ff:ff	NDNS	63 Standard query response 0x0000 SRV, cache flush 0.8 56666 And...
2	8.089883616.147.192.283.199	224.8.0.251	NDNS	78 Standard query response 0x0000 AAA wpad.local, "QM" question	
3	8.0812929832.147.192.283.207	224.8.0.251	NDNS	70 Standard query response 0x0000 AAA wpad.local, "QM" question	
4	8.0811939182.147.192.236.132	224.8.0.251	NDNS	146 Standard query response 0x0000 PTR {"nm": "Mi Note 10 Lite", "a...	
5	8.0811939182.147.192.236.132	224.8.0.251	NDNS	89 Standard query response 0x0000 PTR {"nm": "Mi Note 10 Lite", "a...	
6	8.0811939273.147.192.283.153	224.8.0.251	NDNS	81 Standard query response 0x0000 A BRWC8B1E5F63DC.local, "QM" question	
7	8.0811939353.Cisco_S1:c9:e9	Broadcast	ARP	42 ARP Announcement for 147.192.283.207	
8	8.0811939433.147.192.236.211	224.8.0.251	NDNS	224 Standard query response 0x0000 ANY {"nm": "Redmi Note 11 Pro 5G", "a...	
9	8.0811939522.147.192.236.184	224.8.0.251	NDNS	362 Standard query response 0x0000 PTR {"nm": "Redmi Note 11 Pro 5G", "a...	
10	8.0811939522.147.192.236.184	224.8.0.251	NDNS	363 Standard query response 0x0000 PTR {"nm": "Redmi Note 11 Pro 5G", "a...	
11	8.2187655213.147.192.237.138	224.8.0.251	NDNS	495 Standard query response 0x0000 PTR Peter's MacBook Air.compa...	
12	8.2187655308.147.192.283.123	224.8.0.251	NDNS	154 Standard query response 0x0000 PTR _companion-link._tcp.local, "QM" qu...	
13	8.2187655308.147.192.282.651	224.8.0.251	NDNS	361 Standard query response 0x0000 PTR _companion-link._tcp.local, "QM" qu...	
14	8.2187655308.147.192.282.651	224.8.0.251	NDNS	362 Standard query response 0x0000 TXT _companion-link._tcp.local, "QM" qu...	
15	8.2187655308.147.192.282.651	224.8.0.251	NDNS	363 Standard query response 0x0000 TXT _companion-link._tcp.local, "QM" qu...	
16	8.419753120.147.192.238.162	224.8.0.251	NDNS	139 Standard query response 0x0000 ANY Deligiorgis-iPad.local, "QM" questi...	
17	8.419753641.147.192.237.209	224.8.0.251	NDNS	400 Standard query response 0x0000 TXT PTR iPhone (5).compan...	
18	8.419753731.147.192.283.207	224.8.0.251	NDNS	725 Standard query response 0x0000 TXT cache flush PTR _nstream...	
19	8.419753731.147.192.283.207	224.8.0.251	NDNS	538 Standard query response 0x0000 PTR cache flush LAPTOP-PVTJC0...	

3.1) Είδος (ομαδικές ή ατομικές, τοπικές ή μοναδικές) διευθύνσεων MAC πηγής των πλαισίων Ethernet:

Έχουμε σε κάθε περίπτωση ατομικές διευθύνσεις (**LSB του Byte ο είναι 0**) και κατά περιπτώσεις τοπικές (**2nd LSB του Byte ο είναι 1**) / παγκόσμιες διευθύνσεις (**2nd LSB του Byte ο είναι 0**).

3.2) Είδος (ομαδικές ή ατομικές, τοπικές ή μοναδικές) διευθύνσεων MAC προορισμού των πλαισίων Ethernet:

Έχουμε σε κάθε περίπτωση ομαδικές διευθύνσεις (**LSB του Byte ο είναι 1**) και κατά περιπτώσεις τοπικές (**2nd LSB του Byte ο είναι 1**) / παγκόσμιες διευθύνσεις (**2nd LSB του Byte ο είναι 0**).

3.3) Θέση στο πρώτο byte που εμφανίζεται το πρώτο bit της διεύθυνσης MAC και θέση του επομένου του:

Σύμφωνα με τη θεωρία, ενώ τα bytes του πλαισίου μεταδίδονται με τη σειρά (από τα αριστερά προς τα δεξιά), τα bits του εκάστοτε byte φθάνουν “ανεστραμμένα”. Δηλαδή για κάθε byte πρώτα μεταδίδεται το λιγότερο σημαντικό bit (LSB) και τελευταίο το περισσότερο σημαντικό bit (MSB). Αν πρώτο == MSB τότε εμφανίζεται στην θέση 8 == LSB του byte 0. Αντίστοιχα το επόμενο bit θα βρίσκεται στη θέση 7.

3.4) Διεύθυνση MAC για τα πλαίσια εκπομπής (broadcast): **ff:ff:ff:ff:ff:ff**

3.5) Εφαρμόζουμε το φίλτρο απεικόνισης llc. Εμφανίζονται πλαίσια με πρωτόκολλο STP στρώματος δικτύου. Επίσης παρατηρούμε ότι στο στρώμα ζεύχης έχουμε IEEE 802.3 Ethernet.

3.6) Τι δηλώνει το πεδίο μετά τις διευθύνσεις MAC στα πλαίσια IEEE 802.3:: Μήκος δεδομένων (πεδίο Length)

3.7) Πώς ξεχωρίζουν τα πλαίσια IEEE 802.3 από τα Ethernet II:: Σε αντίθεση με το IEEE 802.3, το Ethernet II έχει πεδίο Type και όχι Length. Κατά σύμβαση το μέγιστο μήκος των πλαισίων είναι περίπου 1518 bytes. Προκειμένου να

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

llc

No.	Time	Source	Destination	Protocol	Length	Info
11	1.150926	Cisco_1b:ef:97	Spanning-tree-(for-... STP	60	RST. Root = 12288/38/7c:ad:4f:42:cc:e0 Cost = 102 Port = 0x...	
27	3.151038	Cisco_1b:ef:97	Spanning-tree-(for-... STP	60	RST. Root = 12288/38/7c:ad:4f:42:cc:e0 Cost = 102 Port = 0x...	
39	5.153592	Cisco_1b:ef:97	Spanning-tree-(for-... STP	60	RST. Root = 12288/38/7c:ad:4f:42:cc:e0 Cost = 102 Port = 0x...	
56	7.153744	Cisco_1b:ef:97	Spanning-tree-(for-... STP	60	RST. Root = 12288/38/7c:ad:4f:42:cc:e0 Cost = 102 Port = 0x...	
71	9.153861	Cisco_1b:ef:97	Spanning-tree-(for-... STP	60	RST. Root = 12288/38/7c:ad:4f:42:cc:e0 Cost = 102 Port = 0x...	

Frame 11: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{C2D8904D-AE9B-4BE9-B2AF-94E2B331D0B8}, id 0

- IEEE 802.3 Ethernet
 - > Destination: Spanning-tree-(for-bridges)_00 (01:80:c2:00:00:00)
 - > Source: Cisco_1b:ef:97 (cc:7f:76:1b:ef:97)
 - Length: 39
 - Padding: 0000000000000000
- Logical-Link Control
 - > DSAP: Spanning Tree BPDU (0x42)
 - > SSAP: Spanning Tree BPDU (0x42)
 - > Control field: U, func=UI (0x03)
- Spanning Tree Protocol
 - Protocol Identifier: Spanning Tree Protocol (0x0000)
 - Protocol Version Identifier: Rapid Spanning Tree (2)
 - BPDU Type: Rapid/Multiple Spanning Tree (0x02)
 - > BPDU flags: 0x3c, Forwarding, Learning, Port Role: Designated
 - > Root Identifier: 12288 / 38 / 7c:ad:4f:42:cc:e0
 - Root Path Cost: 102
 - > Bridge Identifier: 32768 / 38 / cc:7f:76:1b:ef:80
 - Port identifier: 0x8017
 - Message Age: 2
 - Max Age: 20
 - Hello Time: 2
 - Forward Delay: 15
 - Version 1 Length: 0

0000	01	80	c2	00	00	00	cc	7f	76	1b	ef	97	00	27	42	42	.	.	v	.	'BB
0010	03	00	00	02	02	3c	30	26	7c	ad	4f	42	cc	e0	00	00	.	.	<0&		OB ..
0020	00	66	80	26	2c	7f	76	1b	ef	80	80	17	02	00	14	00	f &	.	v
0030	02	00	0f	00	00	00	00	00	00	00	00	00	00	00	00	00

μπορούν αυτά τα δύο πρωτόκολλα να συνυπάρξουν έχει ορισθεί ότι το πεδίο Type θα παίρνει τιμές πάνω από 1536 (ΟΧΟ6ΟΟ). Συνεπώς, για να ξεχωρίσουμε ποιο από τα δύο πρωτόκολλα ακολουθεί ένα πλαίσιο, αρκεί να ελέγχουμε τα 2 bytes που ακολουθούν των διευθύνσεων και αν είναι κάτω από (ΟΧΟ6ΟΟ) πρόκειται για IEEE 802.3, ενώ αν είναι πάνω από (ΟΧΟ6ΟΟ) πρόκειται για Ethernet II.

3.8) Μέγεθος επικεφαλίδας LLC στα πλαίσια IEEE 802.3: 3 bytes

Πεδία που περιλαμβάνει η επικεφαλίδα LLC στα πλαίσια IEEE 802.3: **DSAP, SSAP, Control Field**

3.9) Δεδομένα ποιου πρωτοκόλλου μεταφέρουν τα πλαίσια IEEE 802.3 που παρατηρήσαμε; Spanning Tree Protocol

Μέγεθος των δεδομένων αυτών: **36 bytes**

3.10) Μέγεθος παραγεμίσματος (padding): 7 bytes

Γιατί υπάρχει; Το πρότυπο IEEE 802.3 ορίζει ότι το ελάχιστο μήκος πλαισίου Ethernet είναι 64 byte.

Ένα έγκυρο πλαίσιο, από τη διεύθυνση προορισμού μέχρι το άθροισμα ελέγχου, έχει μήκος τουλάχιστον 64 byte, με τα μικρότερου μήκους πλαίσια να είναι συνήθως αποτέλεσμα συγκρούσεων. Εάν το πακέτο που ενθυλακώνεται στο πλαίσιο είναι μικρότερο από 64 byte, τότε θα παραγεμισθεί με μηδενικά (pad) μέχρι το ελάχιστο μήκος των 64 byte. Στην περίπτωσή μας παρατηρούμε ότι έχουμε μέγεθος πλαισίου 60 bytes (δεν υπολογίζονται τα 4 bytes του CRC). Συνεπώς προστέθηκαν τα bytes του padding ώστε το πλαίσιο να φτάσει το ελάχιστο επιτρεπόμενο μήκος.

Άσκηση 4: Περισσότερα για τα πακέτα ARP

Ξεκινάμε μια νέα καταγραφή Wireshark χωρίς φίλτρο σύλληψης, αδειάζουμε τον πίνακα ARP και εκτελούμε την εντολή ping με διεύθυνση αυτή του default gateway. Διακόπτουμε την εκτέλεση της εντολής και σταματάμε την καταγραφή. Ελέγχουμε τον πίνακα ARP και βεβαιωνόμαστε ότι η διεύθυνση που χρησιμοποιήσαμε προστέθηκε.

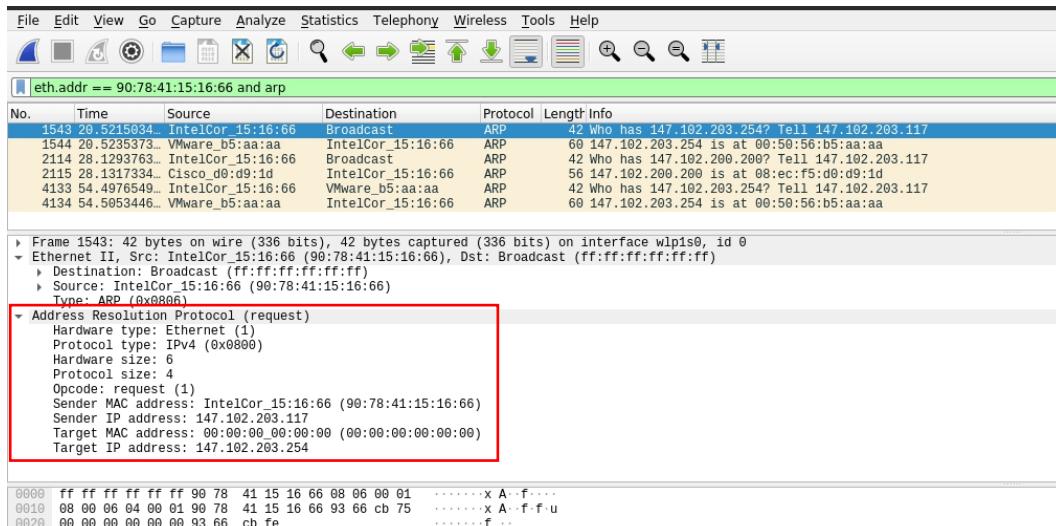
Εφαρμόζουμε φίλτρο απεικόνισης `eth.addr == 90:78:41:15:16:66` (διεύθυνση MAC του υπολογιστή μας).

4.1) Αποτέλεσμα εφαρμογής φίλτρου: Εμφανίζονται πλαίσια που απευθύνονται/παράγονται από τον υπολογιστή μας.

Δηλαδή στην επικεφαλίδα Ethernet υπάρχει η διεύθυνση 90:78:41:15:16:66 είτε στο destination είτε στο source addr.

Προσθέτουμε στο προηγούμενο φίλτρο απεικόνισης την έκφραση *and arp*.

4.2) Αποτέλεσμα εφαρμογής δεύτερου φίλτρου: **Εμφανίζονται πλαίσια που απευθύνονται/παράγονται από τον υπολογιστή μας με πρωτόκολλο στρώματος δικτύου ARP.** Δηλαδή στην επικεφαλίδα Ethernet υπάρχει η διεύθυνση 90:78:41:15:16:66 είτε στο destination είτε στο source address ενώ στο type υπάρχει ο κωδικός 0x0806 (για ARP).



4.3) Πόσα πακέτα ARP ανταλλάχθηκαν κατά την εκτέλεση της εντολής ping:: 6 πακέτα

4.4) Ποιο πεδίο του πλαισίου Ethernet διαφοροποιεί τα πακέτα ARP από τα πακέτα IPv4: **Το πεδίο Type**

Επιλέγουμε ένα πακέτο ARP και βλέπουμε την πληροφορία που μεταφέρει στο παράθυρο με τις λεπτομέρειες.

4.5) Ονόματα και μήκος σε byte των πεδίων του πακέτου ARP:

- ◆ **Hardware Type-2 bytes**
- ◆ **Protocol Type-2 bytes**
- ◆ **Hardware Size-1 byte**
- ◆ **Protocol Size-1 byte**
- ◆ **Opcode-2 bytes**
- ◆ **Sender MAC address-6 bytes**
- ◆ **Sender IP address-4 bytes**
- ◆ **Target MAC address-6 bytes**
- ◆ **Target IP address-4 bytes**

4.6) Τιμή του πεδίου Hardware type: **0x0001**. Είδος υλικού κάρτας δικτύου που υποδεικνύει: **Ethernet**

4.7) Τιμή του πεδίου Protocol type: **0x0800**. Είδος πρωτοκόλλου που υποδεικνύει: **IPv4**

4.8) Σχέση της τιμής του πεδίου Protocol type με τα Ethertypes του Ethernet II: **Στο πεδίο Type του Ethernet έχουμε στη συγκεκριμένη περίπτωση 0x0806 (για πρωτόκολλο ARP) ενώ στο πεδίο Protocol Type του ARP 0x0800 (για πρωτόκολλο IPv4).** Η τιμή 0x0800 χρησιμοποιείται επίσης στο πεδίο type του Ethernet II για πρωτόκολλο IPv4.

4.9) Εξήγηση γιατί η τιμή του πεδίου Protocol size έχει την τιμή 4:

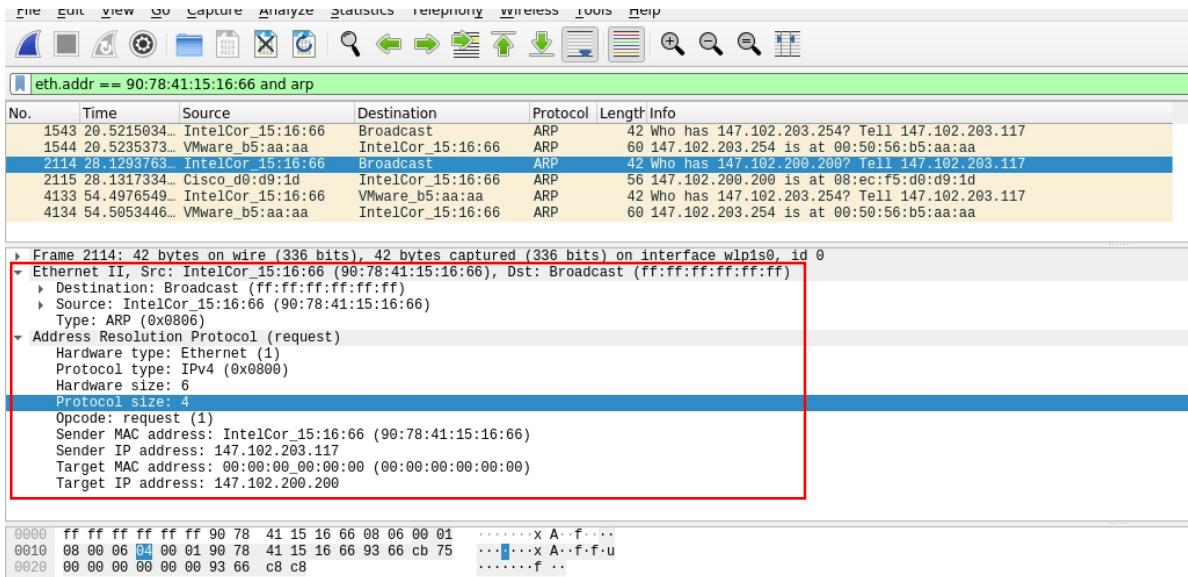
(Το συγκεκριμένο πακέτο ARP που παρατηρούμε είναι request.)

Στο πεδίο Protocol Size αναγράφεται το μήκος της διεύθυνσης (σε bytes) για την οποία ζητείται η MAC της.

Συνεπώς για τιμή 4, έχουμε 4 bytes διεύθυνση και άρα διεύθυνση IPv4.

4.10) Εξήγηση γιατί η τιμή του πεδίου Hardware size έχει την τιμή 6: Στο πεδίο Hardware Size αναγράφεται το μήκος της διεύθυνσης υλικού (σε bytes). Συνεπώς για τιμή 6, έχουμε 6 bytes διεύθυνση και άρα διεύθυνση MAC.

Με βάση την πληροφορία στη στήλη Info του παραθύρου με τη λίστα πακέτων επιλέγουμε το πακέτο ARP request που περιέχει την ερώτηση για το ποιος έχει τη διεύθυνση IPv4 που κάναμε ping (του default gateway).



**4.11) Σε ποιον ανήκει η διεύθυνση MAC αποστολέα του πλαισίου Ethernet που μεταφέρει το ARP request;:
Στην κάρτα δικτύου του υπολογιστή μας.**

4.12) Διεύθυνση MAC παραλήπτη που πλαισίου: ff:ff:ff:ff:ff:ff (γίνεται broadcast προς όλους τους κόμβους του LAN)

4.13) Συνολικό μέγεθος σε byte του πακέτου ARP request: 28 bytes

Συνολικό μέγεθος σε byte του πλαισίου Ethernet που το μεταφέρει: **42 bytes**

4.14) Bytes του πλαισίου Ethernet που προηγούνται του πεδίου opcode στο ARP request: 20 bytes

4.15) Τιμή του πεδίου opcode στο ARP request: 0x00001

4.16) Πεδίο του πακέτου ARP request που περιέχεται η διεύθυνση MAC του αποστολέα: Sender MAC address

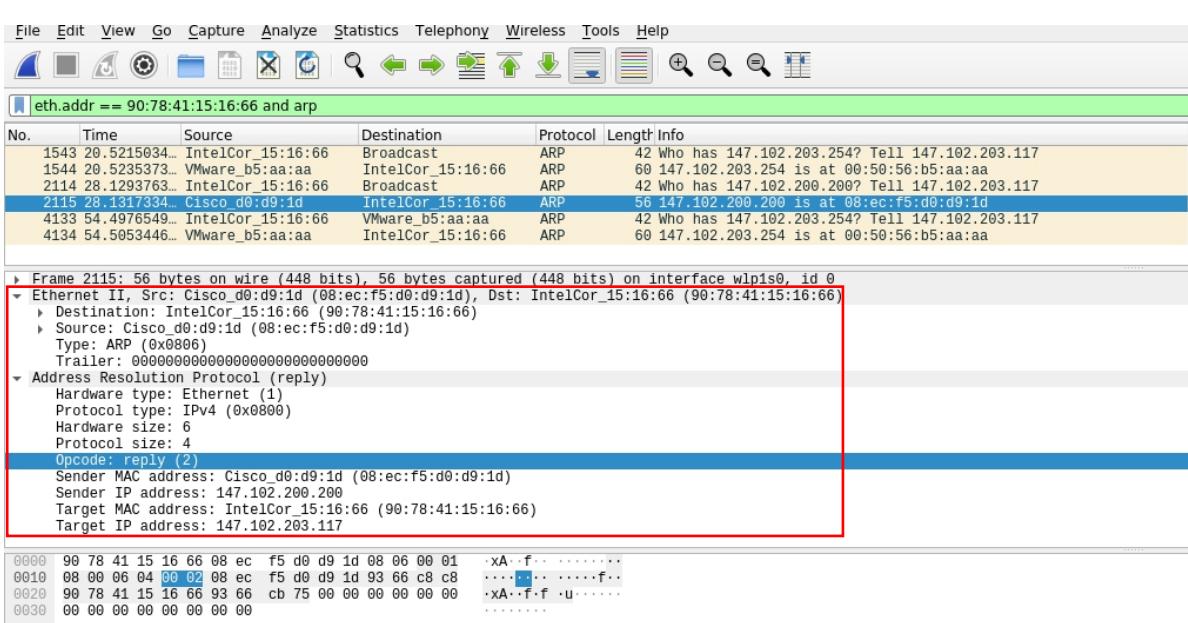
4.17) Πεδίο του πακέτου ARP request που περιέχεται η διεύθυνση IPv4 του αποστολέα: Sender IP address

4.18) Πεδίο του πακέτου ARP request που περιέχεται η διεύθυνση IPv4 του υπολογιστή του οποίου αναζητείται η διεύθυνση MAC: Target IP address

4.19) Υπάρχει στο πακέτο ARP request πεδίο για τη ζητούμενη διεύθυνση MAC;: Ναι το Target MAC address

Ποια τιμή περιέχει: **00:00:00:00:00:00**

Εντοπίζουμε το πακέτο ARP reply που αποτελεί απόκριση στο παραπάνω πακέτο ARP request.



**4.20) Σε ποιον ανήκει η διεύθυνση MAC αποστολέα του πλαισίου Ethernet που μεταφέρει το ARP reply;:
Στον δρομολογητή (default gateway)**

Σε ποιον ανήκει η διεύθυνση MAC παραλήπτη του πλαισίου Ethernet που μεταφέρει το ARP reply;:

Στην κάρτα δικτύου του υπολογιστή μας

4.21) Τιμή του πεδίου opcode στο ARP reply: 0x0002

Για τις παρακάτω ερωτήσεις θεωρούμε αποστολέα αυτόν που έκανε το ARP request και όχι αυτόν που έκανε reply.

4.22) Πεδίο του πακέτου ARP reply που περιέχεται η διεύθυνση IPv4 του αποστολέα; Target IP address

4.23) Πεδίο του πακέτου ARP reply που περιέχεται η διεύθυνση MAC του αποστολέα; Target MAC address

4.24) Πεδίο του πακέτου ARP reply που περιέχεται η διεύθυνση IPv4 του παραλήπτη; Sender IP address

4.25) Πεδίο του πακέτου ARP reply που περιέχεται η διεύθυνση MAC του υπολογιστή που έχει τη διεύθυνση IPv4 για την οποία έγινε η ερώτηση: Sender MAC address

4.26) Συνολικό μέγεθος σε byte του πακέτου ARP reply: 28 bytes

Συνολικό μέγεθος σε byte του πλαισίου Ethernet που το μεταφέρει: 56 bytes

4.27) Είναι ίδια με αυτά που προσδιορίσατε στην ερώτηση 4.13;: Το συνολικό μέγεθος σε byte του πακέτου ARP είναι το ίδιο. Το πλαίσιο του ARP reply είναι μεγαλύτερο από αυτό του request.

4.28) Πεδίο που υποδεικνύει το κατά πόσον πρόκειται για πακέτο ARP request ή ARP reply: Το πεδίο Opcode

4.29) Πώς εξηγείτε το διαφορετικό μήκος πλαισίων Ethernet για πακέτα ARP reply και ARP request;:

Σύμφωνα με την υπόδειξη, η βιβλιοθήκη pycap που χρησιμοποιεί το Wireshark συλλαμβάνει τα απερχόμενα πλαισία προτού μεταδοθούν. Συνεπώς για τα απερχόμενα πλαισία δεν καταγράφει τα μηδενικά που προστίθενται μετέπειτα στην διαδικασία μετάδοσης ώστε το πλαίσιο να φτάσει το ελάχιστο επιτρεπόμενο όριο μεγέθους. Αντίθετα για τα πλαισία που λαμβάνονται έχει γίνει ήδη η προσθήκη των μηδενικών και γίνεται έτσι αντιληπτή κατά την καταγραφή.

4.30) Άλλες διαφορές πλαισίων για πακέτα ARP request και ARP reply: Συνολικά:

-Η αίτηση ARP χρησιμοποιεί unicast address για το source και broadcast address για το destination.

Η απάντηση ARP χρησιμοποιεί unicast address για το source και unicast address για το destination.

-Η αίτηση ARP έχει κωδικό 0x0001 στο Opcode ενώ η απάντηση ARP έχει κωδικό 0x0002.

-Το πεδίο trailer (που είναι διαφορά λόγω του Wireshark και όχι γενικώς)

-Το πεδίο Target MAC της αίτησης ARP είναι μη έγκυρη unicast address. Αντίθετα συμβαίνει με την απάντηση ARP.

4.31) Τι θα συνέβαινε εάν ένας κακόβουλος υπολογιστής στο τοπικό δίκτυο απαντούσε σε όλα τα ARP request δίνοντας τη δική του διεύθυνση MAC;

Η τεχνική αυτή ονομάζεται **ARP spoofing/ARP cache poisoning/ARP poison routing**. Η απάντηση σε όλα τα ARP requests δίνοντας άλλη διεύθυνση MAC έχει σαν αποτέλεσμα στα ARP tables των hosts (συμπεριλαμβανομένου και του default gateway) να γίνει αντιστοίχιση των IP των hosts με τη MAC διεύθυνση του κακόβουλου υπολογιστή.

Έτσι τα πλαισία θα στέλνονται πλέον στη νέα διεύθυνση MAC (του κακόβουλου υπολογιστή) ενώ απευθύνονται στα IP των χρηστών. Έτσι ο κακόβουλος υπολογιστής παρεμβάλλεται στην επικοινωνία των χρηστών και έχει πλέον τη δυνατότητα να αλλάξει το περιεχόμενο των πλαισίων πριν σταλούν στο δίκτυο (man in the middle) ή ακόμα και να κάνει drop τα πλαισία (denial of service).

Σημείωση: Με την παραπάνω τεχνική έχουμε δύο ARP replies για ένα ARP request. Στα ARP tables γίνονται updates σύμφωνα με τα πιο πρόσφατα ληφθέντα ARP replies. Αρκεί λοιπόν το reply του κακόβουλου υπολογιστή να φθάσει στον εκάστοτε host μετά το reply του “αυθεντικού” χρήστη.