Εργαστηριακή Άσκηση 3
Επικοινωνία στο τοπικό δίκτυο
(πλαίσιο Ethernet και πρωτόκολλο ARP)

ΟΝΟΜΑΤΕΠΩΝΥΜΟ: ΚΟΥΣΤΕΝΗΣ ΧΡΙΣΤΟΣ (03120227)

ΟΜΑΔΑ: 3

ΌΝΟΜΑ PC/ΛΣ: LAPTOP-TK5Q3T95 / WINDOWS 11

ΗΜΕΡΟΜΗΝΙΑ: 17/10/2023

ΔΙΕΥΘΥΝΣΗ IP: 192.168.1.14

ΔΙΕΥΘΥΝΣΗ MAC: B4-B5-B6-79-4B-09

1.1 Με ποια εντολή μπορείτε να δείτε τα περιεχόμενα του πίνακα ARP;

Η εντολή **arp -a** στο CLI των Windows.

1.2 Με ποια εντολή μπορείτε να διαγράψετε τα περιεχόμενα του πίνακα ARP;

Η εντολή **arp -d** στο CLI των Windows.

1.3 Σημειώστε τις διευθύνσεις IPv4 της προκαθορισμένης πύλης και των εξυπηρετητών DNS του υπολογιστή σας καθώς και την εντολή ή εντολές φλοιού με τις οποίες τις βρήκατε.

CLI <- **ipconfig /all**

IPv4 Address : 192.168.1.1

DNS Server : 8.8.8.8

1.4 Καταγράψτε το περιεχόμενο του πίνακα ARP του υπολογιστή σας.

```
Interface: 192.168.1.14 --- 0x16
  Internet Address      Physical Address      Type
  192.168.1.1           58-76-ac-4a-62-a0     dynamic
  192.168.1.24          00-12-15-51-9c-06     dynamic
  192.168.1.51          60-a4-4c-ae-c2-58     dynamic
  192.168.1.90          5c-c5-63-33-6e-a3     dynamic
  192.168.1.103         30-de-4b-46-c1-93     dynamic
  192.168.1.190         5c-c5-63-3e-5d-ff     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

1.5 Ο πίνακας περιέχει τις διευθύνσεις MAC και IPv4 των υπολογιστών με τους οποίους έχει επικοινωνήσει πρόσφατα ο δικός σας. Υπάρχουν οι διευθύνσεις της προκαθορισμένης πύλης και/ή των εξυπηρετητών DNS σε αυτόν;

Υπάρχει μόνο η διεύθυνση του Default Getaway(192.168.1.1).

1.6 Αδειάστε τον πίνακα ARP και εκτελέστε την εντολή ping <A.B.C.D>, όπου <A.B.C.D> κάποια διεύθυνση IPv4 της ερώτησης 1.4, πλην της προκαθορισμένης πύλης ή εξυπηρετητή DNS. Εάν δεν λάβετε απάντηση, επαναλάβετε με κάποια άλλη διεύθυνση μέχρι να λάβετε απάντηση. Καταγράψτε τη διεύθυνση που χρησιμοποιήσατε.

- ✓ Εκτελούμε **arp -d** για να αδείασουμε τον πίνακα ARP.

```
Interface: 192.168.1.14 --- 0x16
  Internet Address      Physical Address      Type
  224.0.0.22            01-00-5e-00-00-16     static
```

- ✓ Εκτελούμε **ping 192.168.1.190** και λαμβάνουμε απάντηση 4 πακέτων(default πλήθος στα Windows).

1.7 Δείτε πάλι και καταγράψτε τον πίνακα ARP του υπολογιστή σας. Τι παρατηρείτε;

```
Interface: 192.168.1.14 --- 0x16
  Internet Address      Physical Address      Type
  192.168.1.1           58-76-ac-4a-62-a0     dynamic
  192.168.1.24          00-12-15-51-9c-06     dynamic
  192.168.1.90          5c-c5-63-33-6e-a3     dynamic
  192.168.1.103         30-de-4b-46-c1-93     dynamic
  192.168.1.190         5c-c5-63-3e-5d-ff     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

Παρατηρώ ότι ξαναεμφανίστηκε στο arp table η διεύθυνση IPv4 στην οποία έκανα ping μαζί τη διεύθυνση του default getaway καθώς και κάποιες άλλες διευθύνσεις που προϋπήρχαν στο arp table πριν τον καθαρισμό του και μετά από κάποια δευτερόλεπτα ξαναγίνεται populate το arp table του υπολογιστή μας επιστρέφοντας στην αρχική του κατάσταση.

1.8 Ποιες από τις διευθύνσεις IPv4 που προσδιορίσατε στο ερώτημα 1.3 έχουν τώρα καταχωρηθεί στον πίνακα ARP και γιατί; [Υπενθύμιση: Εάν πελάτης και εξυπηρετητής βρίσκονται σε διαφορετικά υποδίκτυα, η επικοινωνία στο στρώμα IP γίνεται μέσω της πύλης που υποδεικνύει ο πίνακας δρομολόγησης.]

Η διεύθυνση του default gateaway 192.168.1.1

1.9 Έχει καταχωρηθεί η διεύθυνση IPv4 του edu-dy.cn.ntua.gr στον πίνακα ARP και γιατί;

Όχι, δεν έχει καταχωρηθεί γιατί η επικοινωνία του υπολογιστή μας με ξένα υποδίκτυα γίνεται μέσω δρομολογητή που έχει τη διεύθυνση 192.168.1.1 του default getaway

2. Το πλαίσιο Ethernet

2.1 Ποια από τα πεδία του πλαισίου Ethernet καταγράφει το Wireshark; [Υπόδειξη: συμβουλευθείτε την ιστοσελίδα https://en.wikipedia.org/wiki/Ethernet_frame για να δείτε τα πεδία του πλαισίου Ethernet και τα ονόματά τους.]

Για το πλαίσιο Ethernet το Wireshark καταγράφει τα εξής πεδία :

- Source
- Destination
- Type

2.2 Έχει καταγραφεί το προοίμιο; Γιατί;

Όχι, γιατί το προοίμιο χρείαζεται μόνο για τον συγχρονισμό δέκτη και αποστολέα.

2.3 Τι συμβαίνει με το CRC; [Υπόδειξη: Αναζητήστε FCS – Frame Check Sequence στην ιστοσελίδα https://www.wireshark.org/faq.html.]

Τα περισσότερα ΛΣ δεν υποστηρίζουν την καταγραφή του FCS τμήματος του Ethernet frame.

2.4 Ποια είναι η τιμή του πεδίου Type της επικεφαλίδας Ethernet για πακέτα IPv4;
Type : 0800_{16}

2.5 Ποια είναι η τιμή του πεδίου Type για πακέτα ARP;
Type : 0806_{16}

2.6 Εάν καταγράφηκαν, ποια είναι η τιμή του πεδίου Type για πακέτα IPv6;
Type : $86DD_{16}$

2.7 Ποια είναι η διεύθυνση MAC πηγής του πλαισίου;
Source: b4:b5:b6:79:4b:09

2.8 Ποια είναι η διεύθυνση MAC προορισμού του πλαισίου;
Destination: 58:76:ac:4a:62:a0

2.9 Είναι η παραπάνω διεύθυνση MAC αυτή του edu-dy.cn.ntua.gr;
Όχι, δεν είναι.

2.10 Εάν όχι, σε ποια συσκευή ανήκει και γιατί;
Όπως φαίνεται από το ARP table είναι η MAC διεύθυνση του δρομολογητή του τοπικού μας δικτύου που ανήκει στο Default gateaway αφού για πρόσβαση σε ξένα υποδίκτυα χρησιμοποιείται ο δρομολογητής για την επίλυση MAC διευθύνσεων.

Internet Address	Physical Address	Type
192.168.1.1	58-76-ac-4a-62-a0	dynamic

2.11 Ποιο είναι το μήκος του πλαισίου σε byte;
Frame size : 379 bytes.

2.12 Πόσα byte του πλαισίου Ethernet προηγούνται του χαρακτήρα ASCII “G” της λέξης GET;[Υπόδειξη: Για ευκολία με δεξί κλικ στο παράθυρο με τα περιεχόμενα ακυρώστε το Allow hover highlighting.]
379(Total frame size) – 325(Payload size) = 54 bytes προήγουνται του byte που αντιστοιχεί στον ASCII χαρακτήρα “G” του “GET”.

2.13 Ποια είναι η διεύθυνση MAC του αποστολέα;
Source: 58:76:ac:4a:62:a0

2.14 Είναι η παραπάνω διεύθυνση MAC αυτή του edu-dy.cn.ntua.gr;
Όχι, δεν είναι.

2.15 Σε ποια συσκευή πρέπει να ανήκει η διεύθυνση αυτή; Είναι η ίδια διεύθυνση με αυτήν της ερώτησης 2.10; Εάν όχι, τι συμβαίνει; [Υποδ. Δείτε RFC 3768: Virtual Router Redundancy Protocol παράγραφο 8.2 Host ARP Requests.]
Όπως απαντήθηκε στην 2.10 είναι η MAC διεύθυνση του δρομολογητή του τοπικού μας δικτύου που είναι υπεύθυνος για επιλύσεις των διευθύνσεων όταν συνδεόμαστε σε ξένο υποδίκτυο.

2.16 Ποια είναι η διεύθυνση MAC του παραλήπτη;
Destination: b4:b5:b6:79:4b:09

2.17 Σε ποιον υπολογιστή ανήκει;
Στον υπολογιστή που χρησιμοποιώ.

2.18 Ποιο είναι το μήκος του πλαισίου σε byte;
Frame size : 590 bytes.

2.19 Πόσα byte του πλαισίου Ethernet προηγούνται του χαρακτήρα ASCII "O" της λέξης OK;
590(Total frame size) - 536(Payload size) + 13(ο ζητούμενος χαρακτήρας είναι στο 14 byte) = 67 bytes προήγουνται του byte που αντιστοιχεί στον ASCII χαρακτήρα "O" του "OK".

3. Περισσότερα για τα πλαίσια Ethernet

3.1 Τι είδους (ομαδικές ή ατομικές, τοπικές ή μοναδικές) είναι οι διευθύνσεις MAC πηγής των πλαισίων Ethernet που καταγράψατε; [Υπόδειξη: Αναπτύξτε το περιεχόμενο του πεδίου διεύθυνσης πηγής των πλαισίων].
Ατομικές(LSB = 0) και παγκόσμιες/μοναδικές (LSB(byte0 >> 1)) εκτός από ένα πακέτο στο οποίο έχει LSB(byte0 >> 1) το οποίο δείχνει τοπική διεύθυνση.

3.2 Τι είδους (ομαδικές ή ατομικές, τοπικές ή μοναδικές) είναι διευθύνσεις MAC προορισμού των πλαισίων Ethernet που παρατηρείτε στην καταγραφή;
Όλες ομαδικές(LSB = 1) και είτε παγκόσμιες/μοναδικές (LSB(byte0 >> 1) = 0) είτε τοπικές(LSB(byte0 >> 1) = 1).

3.3 Σε ποια θέση στο πρώτο byte εμφανίζεται το πρώτο bit της διεύθυνσης MAC και σε ποια το επόμενό του;
Η μετάδοση γίνεται από LSB --> MSB για κάθε byte άρα το πρώτο bit εμφανίζεται στη $8^η$ θέση και το επόμενό του στην $7^η$ θέση του byte.

3.4 Ποια είναι η διεύθυνση MAC για τα πλαίσια εκπομπής (broadcast);
Destination MAC address για broadcast frames είναι η ff:ff:ff:ff:ff:ff.

3.5 Εφαρμόστε φίλτρο απεικόνισης llc. Τι είδους πλαίσια παραμένουν;
Κανένα στην καταγραφή του υπολογιστή μου, όμως στο lab3.pcap που καταγράψαμε παρατηρούμε ότι απομένουν μόνο τα STP αρχεία(IEEE 802.3 Ethernet).

3.6 Τι δηλώνει το πεδίο μετά τις διευθύνσεις MAC στα πλαίσια IEEE 802.3;
Το πεδίο Length που δηλώνει το πλήθος byte στο πεδίο δεδομένων.

3.7 Πώς ξεχωρίζουν τα πλαίσια IEEE 802.3 από τα Ethernet II;
Στο Ethernet II στη θέση του Length που έχει μήκος από 0 μέχρι και 1500 bytes έχουμε το EtherType που έχει μήκος μεγαλύτερο των 1536 bytes. Επιπλέον, μετά το Length τα πλαίσια IEEE 802.3 περιέχουν μια επικεφαλίδα Logical Link Control (LLC), που καθορίζεται στο πρότυπο IEEE 802.2 (το άνω μέρος του στρώματος ζεύξης δεδομένων), ώστε να προσδιορίζεται το πρωτόκολλο ανωτέρου στρώματος που ενθυλακώνεται.

STP(Spanning Tree Protocol): The STP is a network protocol that builds a loop-free logical topology for Ethernet networks. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. In a LAN, redundant links are added to improve the network availability of LAN. But these redundant links may cause the frame to loop in the network for an infinite time until some action is taken, e.g, some links are taken down. To cope with the problem of frame looping, (STP) comes into play.

3.8 Τι μέγεθος έχει και ποια πεδία περιλαμβάνει η επικεφαλίδα LLC στα πλαίσια IEEE 802.3;
LLC size = 3 bytes και πεδία :

- DSAP
- SSAP
- Control field

1 byte each.

3.9 Δεδομένα ποιου πρωτοκόλλου μεταφέρουν τα πλαίσια IEEE 802.3 που παρατηρήσατε και τι μέγεθος έχουν αυτά;
Μεταφέρουν δεδομένα του STP πρωτοκόλλου μεγάθους 36 bytes.

3.10 Τι μέγεθος έχει το παραγέμισμα (padding) και γιατί υπάρχει;
Padding size : 7 bytes

Και η ύπαρξη του εξασφαλίζει το ελάχιστο απαιτούμενο μήκος πλαισίου Ethernet.

4. Περισσότερα για τα πακέτα ARP

4.1 Τι αποτέλεσμα έχει η εφαρμογή αυτού του φίλτρου;
Εμφανίζονται μόνο πακέτα που έχουν Source ή Destination MAC address αυτή της κάρτας δικτύου του υπολογιστή μου.

4.2 Κάντε κλικ στο τέλος του προηγούμενο φίλτρου, προσθέστε την έκφραση and arp και πατήστε το <Enter>. Τι αποτέλεσμα έχει η εφαρμογή του δεύτερου φίλτρου;
Εμφανίζονται μόνο πακέτα ARP που προφανώς ικανοποιούν και το προηγούμενο φίλτρο.

4.3 Πόσα πακέτα ARP ανταλλάχθηκαν κατά την εκτέλεση της εντολής ping;
2 πακέτα request και reply:

No.	Time	Source	Destination	Protocol	Info
33	0.000000	b4:b5:b6:79:4b:09	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.190? Tell 192.168.1.14
34	0.012831	5c:c5:63:3e:5d:ff	b4:b5:b6:79:4b:09	ARP	192.168.1.190 is at 5c:c5:63:3e:5d:ff
42	3.112441	b4:b5:b6:79:4b:09	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.1? Tell 192.168.1.14
43	0.008435	58:76:ac:4a:62:a0	b4:b5:b6:79:4b:09	ARP	192.168.1.1 is at 58:76:ac:4a:62:a0
52	1.890317	5c:c5:63:3e:5d:ff	b4:b5:b6:79:4b:09	ARP	Who has 192.168.1.14? Tell 192.168.1.190
53	0.000029	b4:b5:b6:79:4b:09	5c:c5:63:3e:5d:ff	ARP	192.168.1.14 is at b4:b5:b6:79:4b:09
72	3.784884	58:76:ac:4a:62:a0	b4:b5:b6:79:4b:09	ARP	Who has 192.168.1.14? Tell 192.168.1.1
73	0.000013	b4:b5:b6:79:4b:09	58:76:ac:4a:62:a0	ARP	192.168.1.14 is at b4:b5:b6:79:4b:09
170	6.184660	b4:b5:b6:79:4b:09	30:de:4b:46:c1:93	ARP	192.168.1.14 is at b4:b5:b6:79:4b:09

4.4 Τα πακέτα ARP δεν είναι πακέτα IPv4. Ποιο πεδίο του πλαισίου Ethernet τα διαφοροποιεί;
Το πεδίο Type:

- Για τα ARP πακέτα είναι Type: ARP (0x0806)
- Για τα IPv4 είναι Type: IPv4 (0x0800)

4.5 Καταγράψτε τα ονόματα και το μήκος σε byte των πεδίων του πακέτου ARP χρησιμοποιώντας ως υπόδειγμα το σχήμα στο τέλος του φυλλαδίου των απαντήσεων.

ARP(request):

- ✓ ***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 Ποια είναι η τιμή του πεδίου Hardware type και τι είδος υλικού κάρτας δικτύου υποδεικνύει;

Η τιμή του είναι 1 και υποδεικνύει Ethernet.

4.7 Ποια είναι η τιμή του πεδίου Protocol type και ποιο πρωτόκολλο υποδεικνύει;

Είναι 0800_{16} και υποδεικνύει IPv4.

4.8 Πώς σχετίζεται η τιμή του πεδίου Protocol type με τα Ethertypes του Ethernet II;

Το Protocol type έχει τιμή 0800_{16}(IPv4) ενώ το Ethertype του Ethernet II τιμή 0806_{16}(ARP).

4.9 Εξηγήστε γιατί η τιμή του πεδίου Protocol size έχει την τιμή 4. [Υπόδειξη: Συμβουλευθείτε την ιστοσελίδα http://www.networksorcery.com/enp/default.htm επιλέγοντας το “IP protocol suite” από το αριστερό της μέρος και στη συνέχεια το πρωτόκολλο ARP στο δεξιό της μέρος. Επειδή εδώ και πολύ καιρό ιστοσελίδα δεν ανταποκρίνεται αναζητήστε την στο Internet Archive.]

Υποδηλώνει το μήκος σε bytes της IP διεύθυνσης που πρέπει να μεταφραστεί (IPv4), άρα 4.

4.10 Εξηγήστε γιατί η τιμή του πεδίου Hardware size έχει την τιμή 6.

Γιατί υποδηλώνει το μήκος σε bytes της MAC διεύθυνσης που ψάχνει να βρει, άρα 6 bytes.

4.11 Σε ποιον υπολογιστή ανήκει η διεύθυνση MAC αποστολέα του πλαισίου Ethernet που μεταφέρει το ARP request;

Στον υπολογιστή μου.

4.12 Ποια είναι η διεύθυνση MAC παραλήπτη που πλαισίου αυτού;

Destination: ff:ff:ff:ff:ff:ff (broadcast).

4.13 Ποιο είναι το συνολικό μέγεθος σε byte του πακέτου ARP request και ποιο του πλαισίου Ethernet που το μεταφέρει;

Total Ethernet frame size = 42 bytes.

ARP request size = 28 bytes.

4.14 Πόσα byte του πλαισίου Ethernet προηγούνται του πεδίου opcode στο ARP request;

20 bytes.

4.15 Ποια η τιμή του πεδίου opcode στο ARP request;
Opcode: 0001_{16} --> request.

4.16 Σε ποιο πεδίο του πακέτου ARP request περιέχεται η διεύθυνση MAC του αποστολέα;
Στο ***Sender MAC address***.

4.17 Σε ποιο πεδίο του πακέτου ARP request περιέχεται η διεύθυνση IPv4 του αποστολέα;
Στο ***Sender IP address***.

4.18 Σε ποιο πεδίο του πακέτου ARP request περιέχεται η ερώτηση, δηλαδή, η διεύθυνση IPv4 του υπολογιστή του οποίου αναζητείται η διεύθυνση MAC;
Στο ***Target IP address***.

4.19 Υπάρχει στο πακέτο ARP request πεδίο για τη ζητούμενη διεύθυνση MAC και ποια τιμή περιέχει;
Υπάρχει το πεδίο ***Target MAC address*** το οποίο περιέχει μηδενικά.

4.20 Σε ποιον υπολογιστή ανήκει η διεύθυνση MAC του αποστολέα και σε ποιον του παραλήπτη του πλαισίου Ethernet που μεταφέρει το ARP reply;
Η διεύθυνση MAC του αποστολέα ανήκει στον δρομολογητή μας που αντιστοιχεί στο default gateaway του δικτύου μας(192.168.1.1) και επιλύει διευθύνσεις MAC ξένων υποδικτύων.

Υποσημείωση: Σε αυτή τη διεύθυνση έγινε ping πορηγουμένως.

Η διεύθυνση MAC του παραλήπτη αντιστοιχεί του πλαισίου Ethernet αντιστοιχεί στο υπολογιστή μας.

4.21 Ποια η τιμή του πεδίου opcode στο ARP reply;
Opcode: 0002_{16} (reply)

4.22 Σε ποιο πεδίο του πακέτου ARP reply περιέχεται η διεύθυνση IPv4 του αποστολέα;
Στο ***Sender IP address.***

4.23 Σε ποιο πεδίο του πακέτου ARP reply περιέχεται η διεύθυνση MAC του αποστολέα;
Στο ***Sender MAC address.***

4.24 Σε ποιο πεδίο του πακέτου ARP reply περιέχεται η διεύθυνση IPv4 του παραλήπτη;
Στο ***Target IP address***.

4.25 Σε ποιο πεδίο του πακέτου ARP reply περιέχεται η απάντηση, δηλαδή, η διεύθυνση MAC του υπολογιστή που έχει τη διεύθυνση IPv4 για την οποία έγινε η ερώτηση;
Στο ***Sender MAC address.***

4.26 Ποιο είναι το συνολικό μέγεθος σε byte του πακέτου ARP reply και ποιο του πλαισίου Ethernet που το μεταφέρει;
Total Ethernet frame size = 60 bytes.

ARP reply size = 28 bytes.

4.27 Είναι ίδια με αυτά που προσδιορίσατε στην ερώτηση 4.13;
Όχι το πλαίσιο Ethernet στο reply είναι μεγαλύτερο.

4.28 Όπως θα έχετε ήδη παρατηρήσει ότι η δομή των πακέτων ARP request/reply είναι η ίδια. Ποιο πεδίο υποδεικνύει το κατά πόσον πρόκειται για πακέτο ARP request ή ARP reply;

Το πεδίο ***opcode***(1 --> request, 2 --> reply)

4.29 Πώς εξηγείτε το διαφορετικό μήκος πλαισίων Ethernet για πακέτα ARP reply και ARP request; [Υπόδειξη: Η βιβλιοθήκη npcap που χρησιμοποιεί το Wireshark, όπως φαίνεται και στο σχετικό σχήμα της Εργαστηριακής Άσκησης 1, συλλαμβάνει τα απερχόμενα πλαίσια προτού μεταδοθούν.]

Προκύπτει λόγω του πεδίου Padding(που υπάρχει για την ικανοποιήση του ελαχίστο ορίου των 64 bytes) το οποίο η βιβλιοθήκη npcap δεν καταγράφει για τα request πακέτα, αφού προστίθεται σε αυτά μόλις μεταβούν στην κάρτα δικτύου, αλλά καταγράφει για τα reply.

4.30 Που αλλού διαφέρουν τα πλαίσια για πακέτα ARP request και ARP reply;

Συνολίκά οι διαφορές:

- Στο πεδίο Padding(μόνο στο reply),
- στο συνολικό μέγεθος του Ethernet frame(reply>request),
- στο πεδίο opcode(1 --> request, 2 --> reply) και
- στην κενή Target MAC address του request.

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

Το λεγόμενο ARP spoofing(poisoning). Θεωρείται ένα Man in the Middle attack το οποίο μπορεί να διατηράξει την επικοινωνία μεταξύ όλων των συσκευών ενός δικτύου.

Αν ο κακόβουλος υπολογιστής απαντήσει σε όλα τα arp requests τότε τόσο ο δέκτης όσο και ο πομπός στα διάφορα ζεύγη εποκοινωνίας εντός του δικτύου θα στέλνουν τα δεδομένα στον κακόβουλο υπολογιστή νομίζοντας ότι αυτός είναι ο σωστός παραλήπτης αφού στο ARP table τους θα έχει αντικατασταθεί η MAC αυτού με τα διάφορα IP addresses. Στη συνέχεια ο παραλήπτης-κακόβουλος υπολογιστής μπορεί είτε να τα ανακατευθύνει κατάλληλη έχοντας όμως πραγματοποιήσει υποκλοπή είτε να μην τα ανακατευθύνει διακόπτοντας την επικονωνίας εντελώς.