Δίκτυα Υπολογιστών ΙΙ

(Ασκήσεις Πράξης)

Ανάλυση Πρωτοκόλλων

Τομέας Τηλεπικοινωνιών και Δικτύων

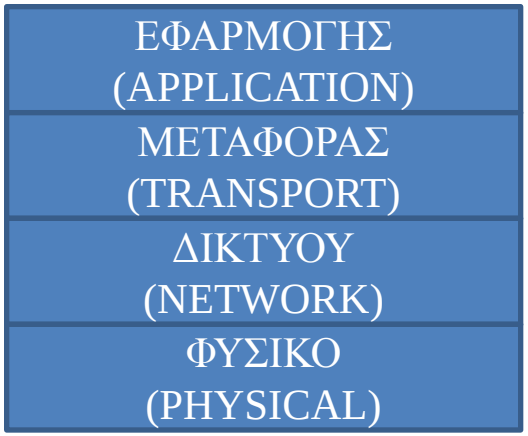
Δρ. Αναστάσιος Πολίτης
Καθηγητής Εφαρμογών
anpol@teiser.gr

Ανάλυση Πακέτων σε Δίκτυα IP

- Είναι η διαδικασία καταγραφής και ανάλυσης των πλαισίων (frame) που μεταδίδονται σε ένα δίκτυο τεχνολογίας IP.
- Πού χρησιμεύει:
  - Ανάλυση δικτυακών προβλημάτων.
  - Εντοπισμός εισβολών.
  - Εντοπισμός κακής χρήσης από χρήστες εντός του δικτύου.
  - Συλλογή δικτυακών στατιστικών.
- Πως επιτυγχάνεται:
  - με ειδικό λογισμικό (software) ή υλικό (hardware).
    - `wireshark` (GUI)
    - `tcpdump` (Command Line)
  - το λογισμικό αναλύει τα πεδία των επικεφαλίδων και των δεδομένων από τα οποία αποτελείται το καταγεγραμμένο πλαίσιο.

Επίπεδα TCP/IP

• Το TCP/IP είναι μια συλλογή από επικοινωνιακά πρωτόκολλα τα οποία ανήκουν σε διαφορετικά επίπεδα.



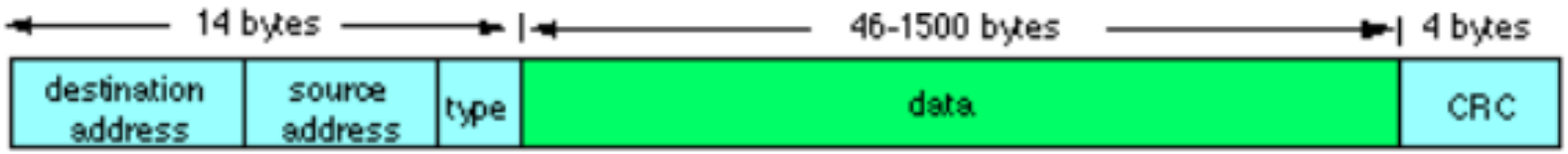
FTP, HTTP, DNS

TCP, UDP

IP, ICMP, ARP

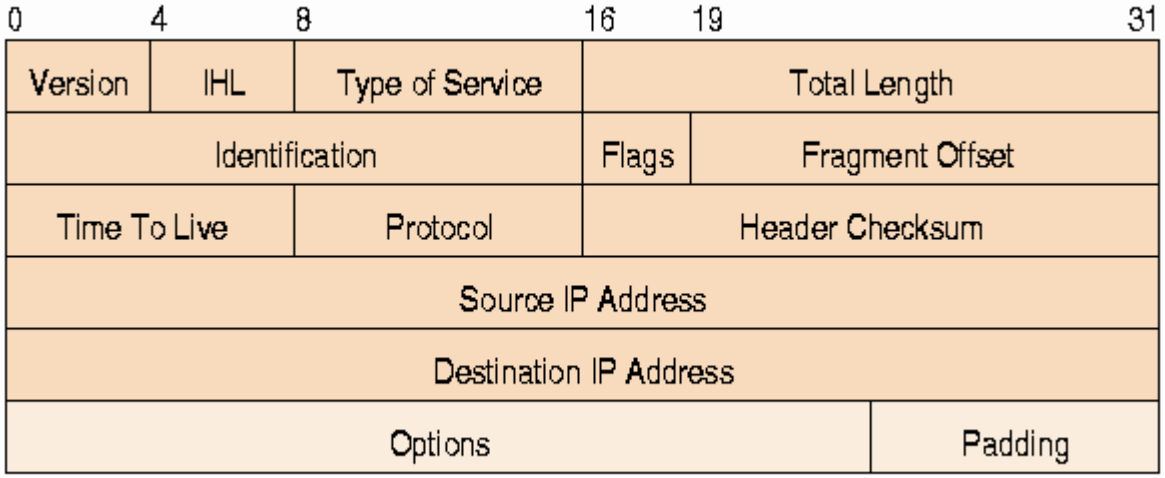
Ethernet, Token Ring

Μορφή Πλαισίου Ethernet



- MAC Διευθύνσεις:
  - Μοναδική ταυτότητα που αποδίδεται σε κάθε δικτυακή διεπαφή (interface) για επικοινωνία στο φυσικό επίπεδο. (48-bit)
  - Βρίσκονται στο hardware της κάρτας δικτύου και δεν μπορούν να αλλάξουν.
  - Γράφονται σε δεκαεξαδική μορφή.
  - Τα 24 MSB προσδιορίζουν τον κατασκευαστή και τα 24 LSB την κάρτα δικτύου.
- Type:
  - 2-byte μέγεθος.
  - Προσδιορίζει ποιό πρωτόκολλο επιπέδου δικτύου έχει ενθυλακωθεί από το Ethernet.
  - 0x0800 – IPv4
  - 0x86dd – IPv6
  - 0x0806 – ARP

Μορφή IP Επικεφαλίδας



- Αποτελείται από λέξεις (words) των 32-bit.
- Αποτελείται από ένα σταθερό και ένα μεταβλητό τμήμα
  - Από το πεδίο *Version* εώς το πεδίο *Destination IP Address*.
- Αποτελείται από πεδία (fields) διαφορετικών μεγεθών.
- Το συνολικό μέγεθος της πρέπει να είναι ακαίρεο πολλαπλάσιο των 32-bit
  - Εάν το μεταβλητό μήκος είναι μικρότερο από μια ή περισσότερες 32-bit λέξεις, προστίθενται επιπλέον bits *(Padding)*.

Παράδειγμα Καταγεγραμμένου Πλαισίου

• Ο αναλυτής εμφανίζει το πλαίσιο στην δεκαεξαδική του μορφή (hex) και την μετάφραση των bytes σε κώδικα ASCII.

• *Ethernet header*

```
00 24 17 22 bc 76 00 25  22 b5 78 97 08 00 45 00   .$."·v·%  "·x···E·
00 3c 99 ca 00 00 80 01  1c 62 c0 a8 01 46 c0 a8   ·<·····  ·b···F··
01 fe 08 00 49 5c 02 00  02 00 61 62 63 64 65 66   ····I\··  ··abcdef
67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

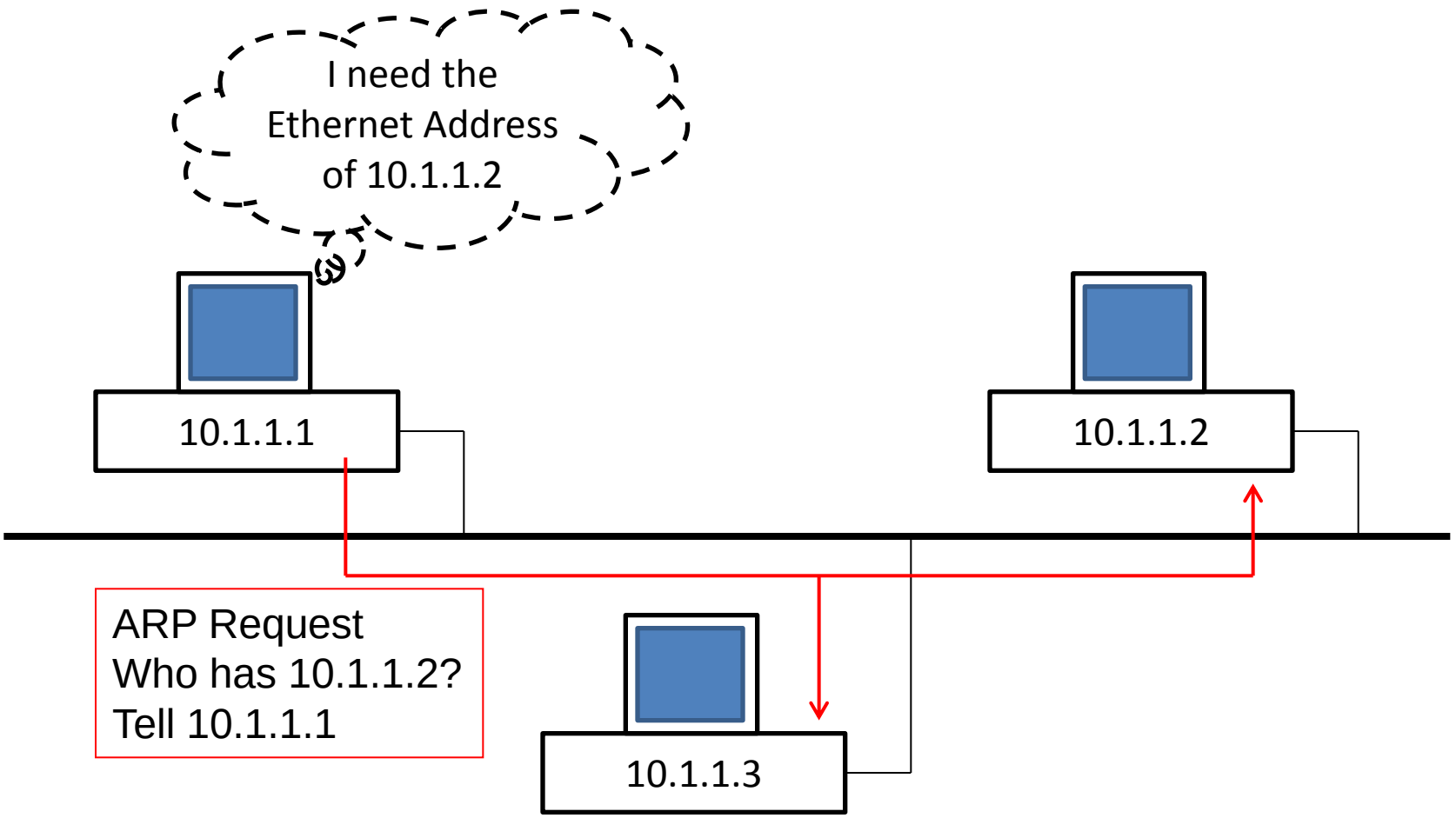
• *IP header*

```
00 24 17 22 bc 76 00 25  22 b5 78 97 08 00 45 00   .$."·v·%  "·x···E·
00 3c 99 ca 00 00 80 01  1c 62 c0 a8 01 46 c0 a8   ·<·····  ·b···F··
01 fe 08 00 49 5c 02 00  02 00 61 62 63 64 65 66   ····I\··  ··abcdef
67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

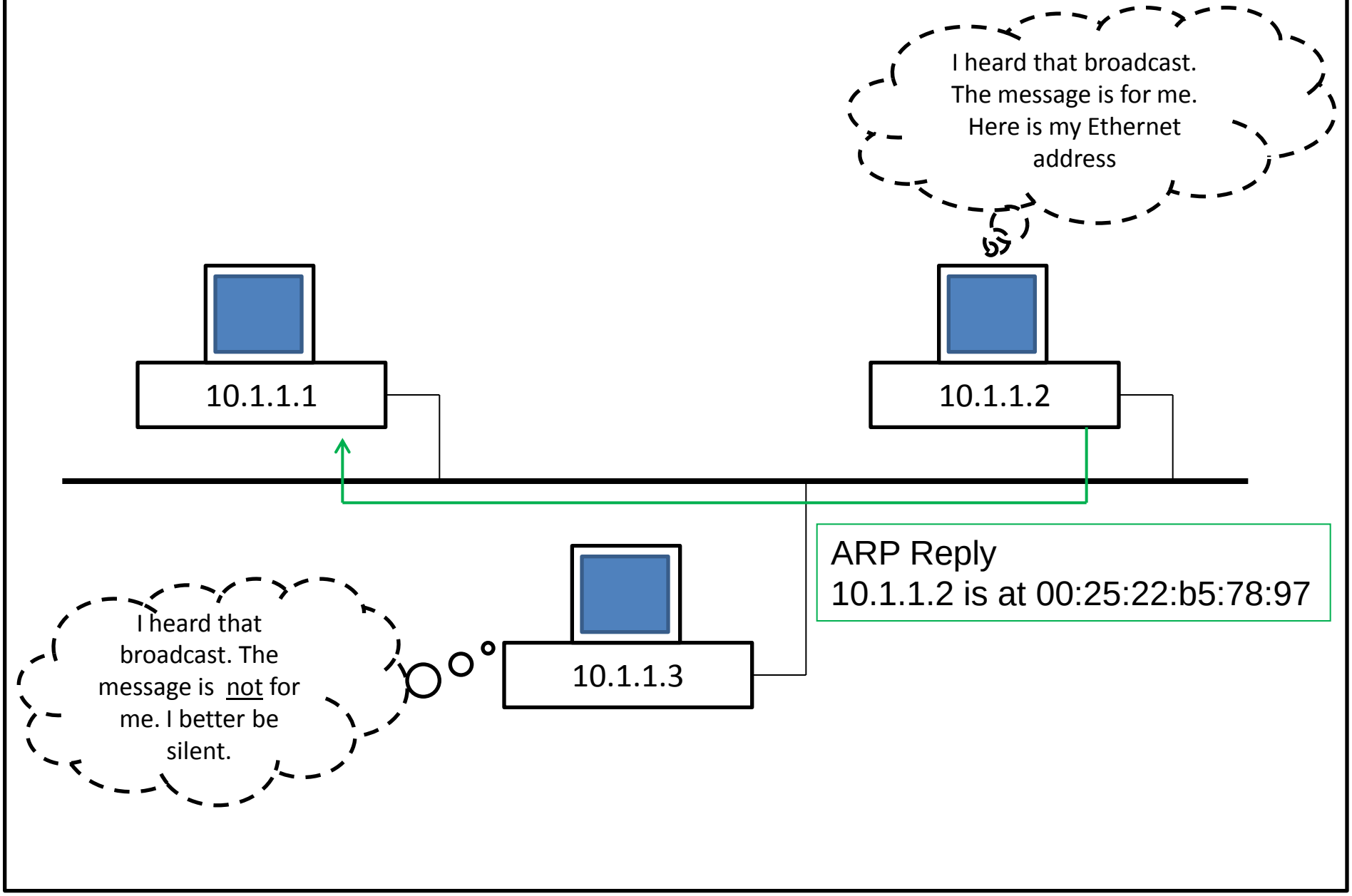
• *ARP header*

```
ff ff ff ff ff ff 00 24  17 22 bc 76 08 06 00 01   ·······$ ·"·v····
08 00 06 04 00 01 00 24  17 22 bc 76 c0 a8 01 fe   ·······$ ·"·v····
00 00 00 00 00 00 c0 a8  01 46 00 00 00 00 00 00   ·····F··  ··F·····
00 00 00 00 00 00 00 00  00 00 00 00               ·····F··  ····
```

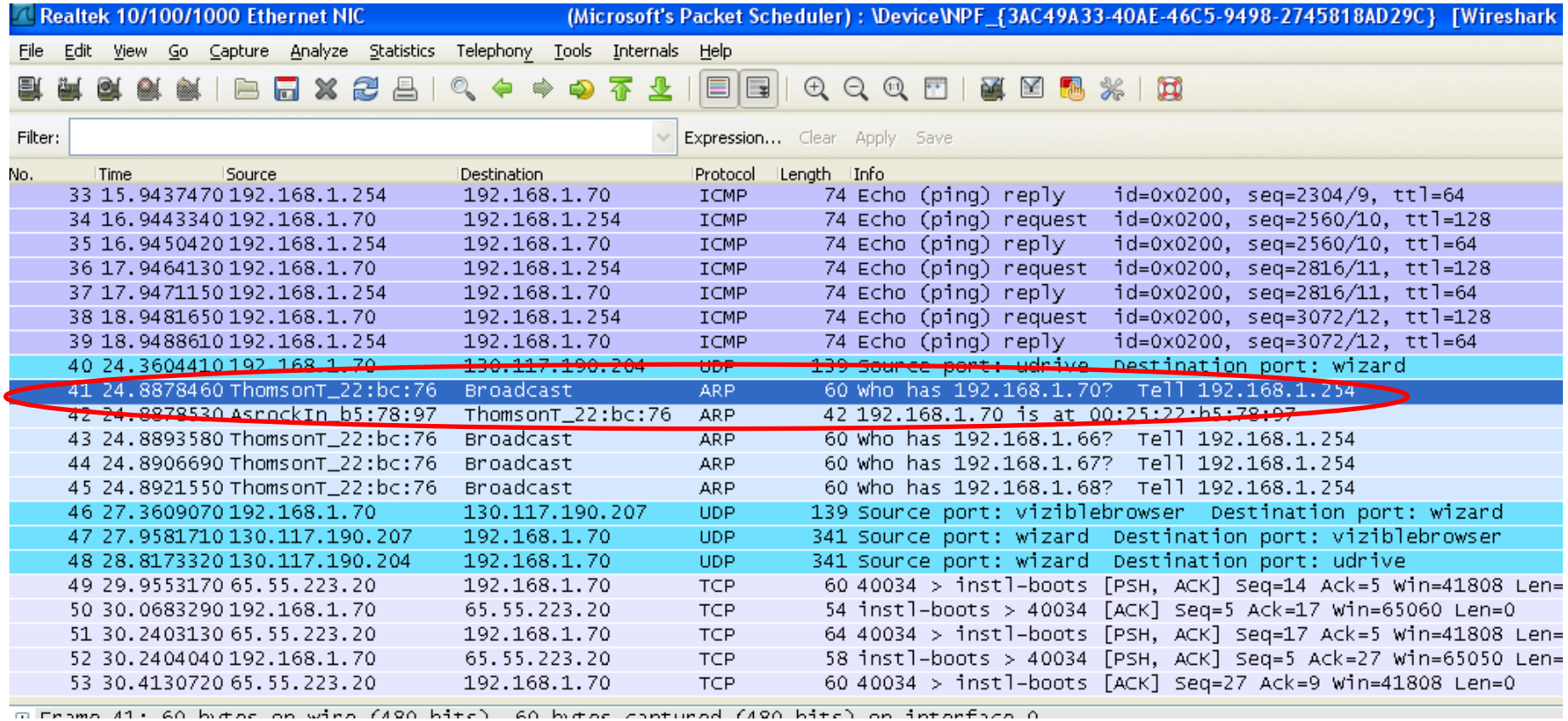
Address Resolution Protocol



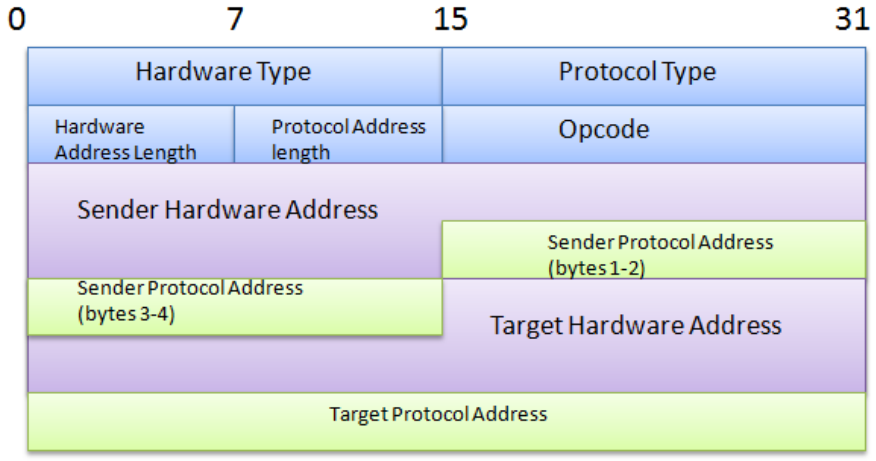
Address Resolution Protocol



Καταγραφή Πακέτων ARP



Μορφή Επικεφαλίδας ARP



- **Hardware Type:** Προσδιορίζει τον τύπο του δικτύου. 1 για το Ethernet.
- **Protocol Type:** Προσδιορίζει το πρωτόκολλο για το οποίο ζητήθηκε η διαδικασία του ARP. 0x0800 για το IPv4.
- **HW addr length:** Μέγεθος της hardware address. 6 για Ethernet.
- **Proto addr length:** Μέγεθος της διεύθυνσης του πρωτοκόλλου για το οποίο ζητήθηκε η ARP. 4 για το IPv4.
- **Opcode:** Τύπος του ARP μηνύματος. 1 για request, 2 για reply.
- **Source hardware address:** Η hardware address του αποστολέα αυτού του ARP μηνύματος.
- **Source protocol address:** Η διεύθυνση (IP) του αποστολέα.
- **Destination hardware address:** Η hardware address του παραλήπτη.
- **Destination protocol address:** Η διεύθυνση (IP) του παραλήπτη.

Ανάλυση Επικεφαλίδας ARP

ARP Request

```
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: ThomsonT_22:bc:76 (00:24:17:22:bc:76)
    Sender IP address: 192.168.1.254 (192.168.1.254)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.70 (192.168.1.70)
```

ARP Reply

```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: AsrockIn_b5:78:97 (00:25:22:b5:78:97)
    Sender IP address: 192.168.1.70 (192.168.1.70)
    Target MAC address: ThomsonT_22:bc:76 (00:24:17:22:bc:76)
    Target IP address: 192.168.1.254 (192.168.1.254)
```

Εφαρμογές ARP

• **Εφαρμογή Ι:** Δίνεται η παρακάτω δεκαεξαδική μορφή ενός καταγεγραμμένου Ethernet frame. Να βρεθούν:

```
00 24 17 22 bc 76 00 25  22 b5 78 97 08 06 00 01   .$."v.%  ".x.....
08 00 06 04 00 02 00 25  22 b5 78 97 c0 a8 01 46   .......%  ".x....F
00 24 17 22 bc 76 c0 a8  01 fe                     .$."v...  ..
```

1. Η MAC διεύθυνση του αποστολέα.
2. Η MAC διεύθυνση του παραλήπτη.
3. Το πρωτόκολλο επιπέδου δικτύου.

• **Εφαρμογή ΙΙ:** Δίνεται η παρακάτω δεκαεξαδική μορφή ενός καταγεγραμμένου Ethernet frame το οποίο ενθυλακώνει ένα ARP μήνυμα.

```
ff ff ff ff ff ff 00 24  17 22 bc 76 08 06 00 01   .......$ ."v.....
08 00 06 04 00 01 00 24  17 22 bc 76 c0 a8 01 fe   .......$ ."v.....
00 00 00 00 00 00 c0 a8  01 46 00 00 00 00 00 00   ........ .F......
00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

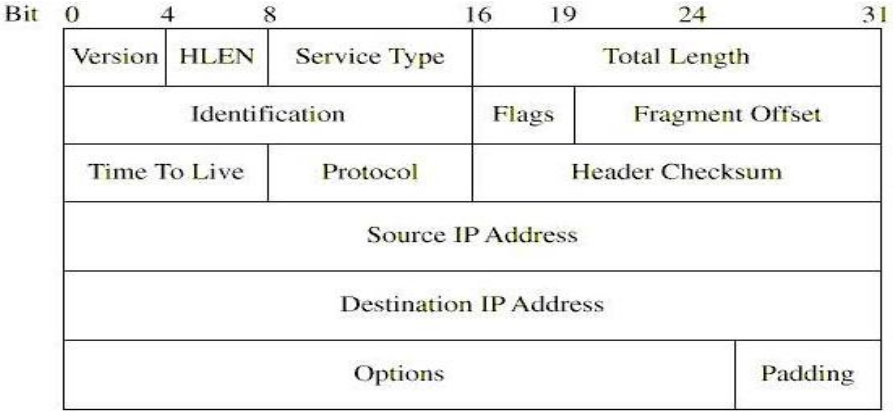
1. Να βρεθεί ο τύπος του ARP μηνύματος (με δύο τρόπους).
2. Η IP διεύθυνση του αποστολέα του μηνύματος αυτού.
3. Η IP διεύθυνση του παραλήπτη του μηνύματος αυτού.

Εφαρμογές IP

• **Εφαρμογή Ι:** Δίνεται η παρακάτω δεκαεξαδική μορφή ενός καταγεγραμμένου Ethernet frame καθώς και η μορφή του IP header. Να βρεθούν:

1. Οι MAC διευθύνσεις αποστολέα και παραλήπτη.
2. Η έκδοση του IP πρωτοκόλλου που χρησιμοποιείται.
3. Το μέγεθος των επιλογών (Options) που περιλαμβάνει ο IP header.
4. Ο αριθμός των αλμάτων (hops) που επιτρέπεται να διασχίσει το IP datagram.
5. Το πρωτόκολλο του επιπέδου μεταφορά που χρησιμοποιείται.

```
00 80 48 1d 02 25 00 0b  cd 88 dd 3b 08 00 45 00   ..H..%.. ...;..E.
05 dc 06 9d 20 00 80 01  8d 30 c0 a8 00 01 c0 a8   .... ... .0......
00 02 08 00 c2 e6 02 00  13 00 61 62 63 64 65 66   ........ ..abcdef
67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
77 61 62 63 64 65 66 67  68 69 6a 6b 6c 6d 6e 6f   wabcdefg hijklmno
70 71 72 73 74 75 76 77  61 62 63 64 65 66 67 68   pqrstuvw abcdefgh
69 6a 6b 6c 6d 6e 6f 70  71 72 73 74 75 76 77 61   ijklmnop qrstuvwa
```

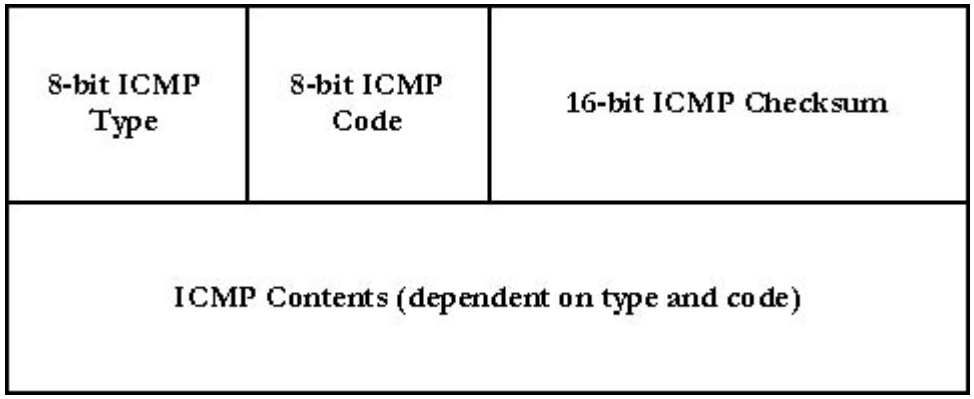


Internet Control Message Protocol

- Πρωτόκολλο για την μετάδοση μηνυμάτων ελέγχου μεταξύ δικτυακών κόμβων.
- Χρησιμοποιείται όταν παρουσιάζονται προβληματικές καταστάσεις, αλλά και από συγκεκριμένες εφαρμογές (ping και traceroute).
- Τα μηνύματα ICMP χωρίζονται σε:
  - Τύπους (Type)
    - Κωδικούς για κάθε τύπο (Code)

Type	Code	Description
0	0	Echo Reply
8	0	Echo Request
3	0	Network unreachable
3	1	Host unreachable
3	4	Fragmentation needed but don’t fragment bit is set
11	0	TTL equals 0 during transit

Μορφή Επικεφαλίδας ICMP



• Το μέγεθος της επικεφαλίδας είναι μεταβλητό και ανάλογο με τον Τύπο και Κωδικό του ICMP μηνύματος.

• Για το echo request και echo reply που παράγονται από τις εφαρμογές ping και traceroute το μέγεθος της επικεφαλίδας είναι 8 bytes.

Καταγραφή ICMP μηνυμάτων

- Ping

Realtek 10/100/1000 Ethernet NIC (Microsoft's Packet Scheduler) : \Device\NPF_{3AC49A33-40AE-46C5-9498-2745818AD29C} [Wiresh

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ip.proto==ICMP Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
24	12.7034670	192.168.1.70	155.207.1.12	ICMP	74	Echo (ping) request id=0x0200, seq=9728/38, ttl=128
25	12.7529930	155.207.1.12	192.168.1.70	ICMP	74	Echo (ping) reply id=0x0200, seq=9728/38, ttl=54
28	13.7069800	192.168.1.70	155.207.1.12	ICMP	74	Echo (ping) request id=0x0200, seq=9984/39, ttl=128
29	13.7563780	155.207.1.12	192.168.1.70	ICMP	74	Echo (ping) reply id=0x0200, seq=9984/39, ttl=54
30	14.7096550	192.168.1.70	155.207.1.12	ICMP	74	Echo (ping) request id=0x0200, seq=10240/40, ttl=128
31	14.7594450	155.207.1.12	192.168.1.70	ICMP	74	Echo (ping) reply id=0x0200, seq=10240/40, ttl=54
32	15.7130150	192.168.1.70	155.207.1.12	ICMP	74	Echo (ping) request id=0x0200, seq=10496/41, ttl=128
33	15.7634140	155.207.1.12	192.168.1.70	ICMP	74	Echo (ping) reply id=0x0200, seq=10496/41, ttl=54

- Traceroute

Capturing from Realtek 10/100/1000 Ethernet NIC (Microsoft's Packet Scheduler) : \Device\NPF_{3AC49A33-40AE-46C5-9498-2745818AD2

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ip.proto==ICMP Expression... Clear Apply Save

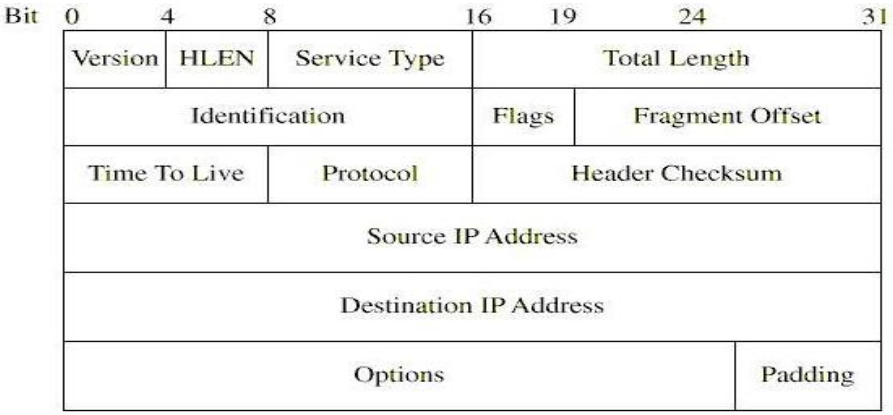
No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.1.70	155.207.1.12	ICMP	106	Echo (ping) request id=0x0200, seq=10752/42, ttl=1
2	0.09802300	192.168.1.254	192.168.1.70	ICMP	86	Time-to-live exceeded (Time to live exceeded in transit)
3	0.10247000	192.168.1.70	155.207.1.12	ICMP	106	Echo (ping) request id=0x0200, seq=11008/43, ttl=1
4	0.19834200	192.168.1.254	192.168.1.70	ICMP	86	Time-to-live exceeded (Time to live exceeded in transit)
5	0.20277900	192.168.1.70	155.207.1.12	ICMP	106	Echo (ping) request id=0x0200, seq=11264/44, ttl=1
6	0.29801400	192.168.1.254	192.168.1.70	ICMP	86	Time-to-live exceeded (Time to live exceeded in transit)
9	1.19954300	192.168.1.70	155.207.1.12	ICMP	106	Echo (ping) request id=0x0200, seq=11520/45, ttl=2
10	1.23518500	213.16.246.17	192.168.1.70	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
11	1.23971300	192.168.1.70	155.207.1.12	ICMP	106	Echo (ping) request id=0x0200, seq=11776/46, ttl=2
12	1.27558200	213.16.246.17	192.168.1.70	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
13	1.28004900	192.168.1.70	155.207.1.12	ICMP	106	Echo (ping) request id=0x0200, seq=12032/47, ttl=2
14	1.31573900	213.16.246.17	192.168.1.70	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
15	2.28196800	192.168.1.70	155.207.1.12	ICMP	106	Echo (ping) request id=0x0200, seq=12288/48, ttl=3
16	2.31713100	194.219.41.190	192.168.1.70	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
17	2.32149000	192.168.1.70	155.207.1.12	ICMP	106	Echo (ping) request id=0x0200, seq=12544/49, ttl=3
18	2.35682700	194.219.41.190	192.168.1.70	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
19	2.36005700	192.168.1.70	155.207.1.12	ICMP	106	Echo (ping) request id=0x0200, seq=12800/50, ttl=3
20	2.39537200	194.219.41.190	192.168.1.70	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
26	3.35629300	192.168.1.70	155.207.1.12	ICMP	106	Echo (ping) request id=0x0200, seq=13056/51, ttl=4
27	3.40100600	212.251.94.17	192.168.1.70	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
28	3.40551600	192.168.1.70	155.207.1.12	ICMP	106	Echo (ping) request id=0x0200, seq=13312/52, ttl=4

Εφαρμογές ICMP

• **Εφαρμογή Ι:** Δίνεται η παρακάτω δεκαεξαδική μορφή ενός καταγεγραμμένου Ethernet frame το οποίο ενθυλακώνει ένα ICMP μήνυμα. Να βρεθεί:

1. Ο τύπος του ICMP μηνύματος.
2. Μέγεθος των δεδομένων που ενθυλακώνονται από το ICMP.

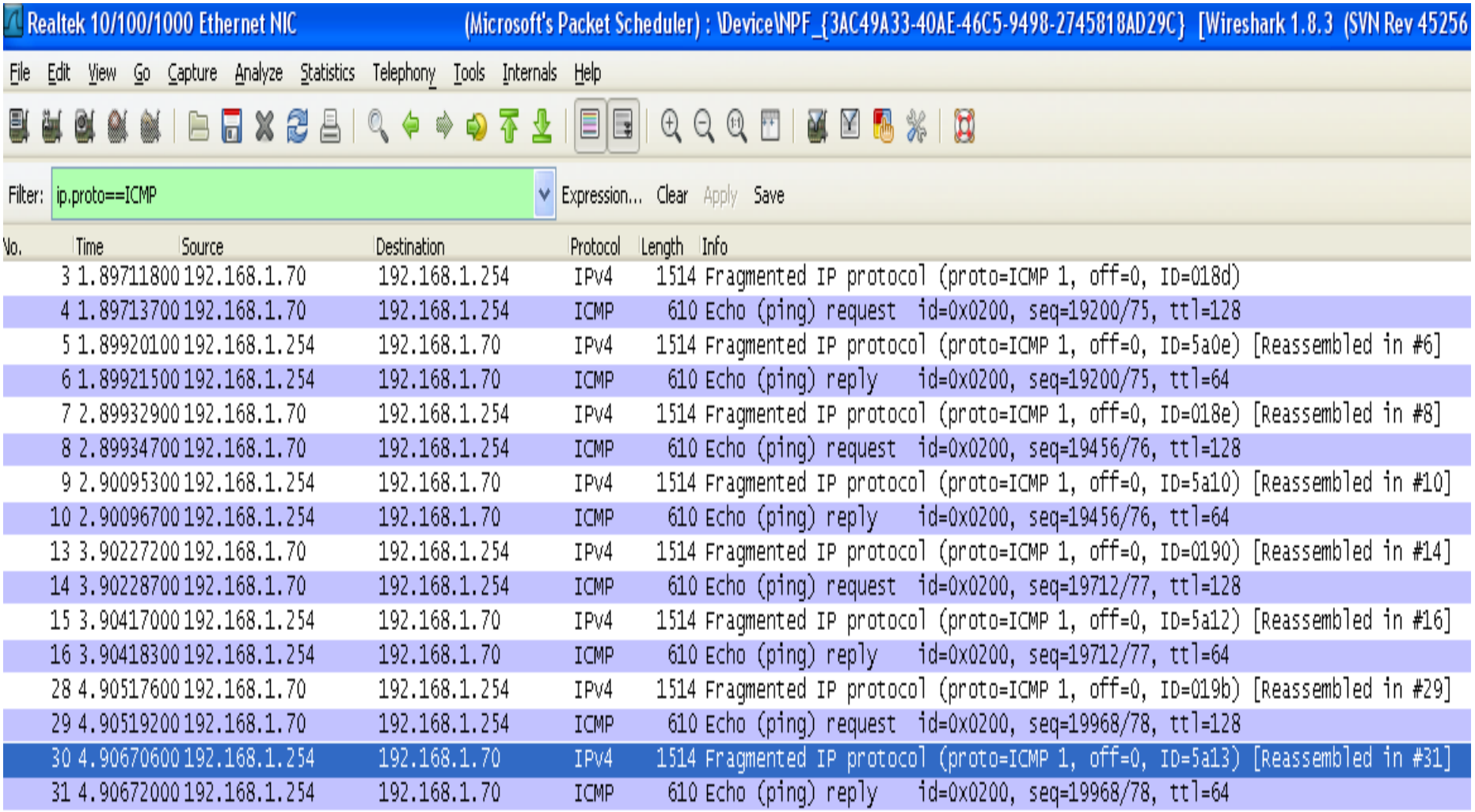
```
00 24 17 22 bc 76 00 25  22 b5 78 97 08 00 45 00   .$."·v·% "·x···E·
00 3c 1c d1 00 00 80 01  99 5b c0 a8 01 46 c0 a8   ·<······ ·[···F··
01 fe 08 00 fc 5b 02 00  4f 00 61 62 63 64 65 66   ·····[·· O·abcdef
67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```



Κατακερματισμός IP πακέτων

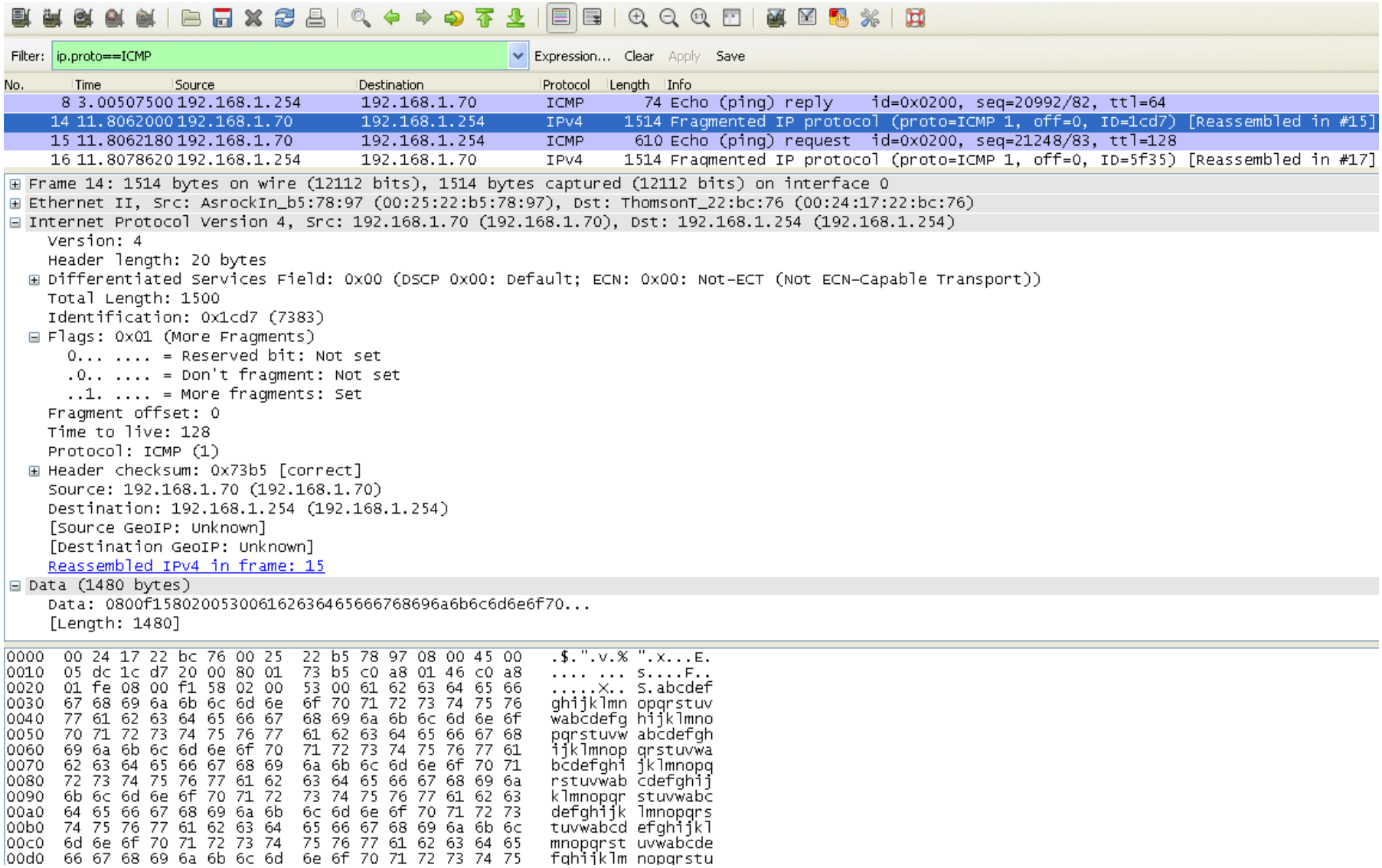
- Σε δίκτυα όπου το συνολικό μέγεθος του παραγόμενου πλαισίου (headers και data) ξεπερνούν το MTU, λαμβάνει χώρα ο κατακερματισμός.

Εκτέλεση της εντολής ***ping www.auth.gr –l 2048***



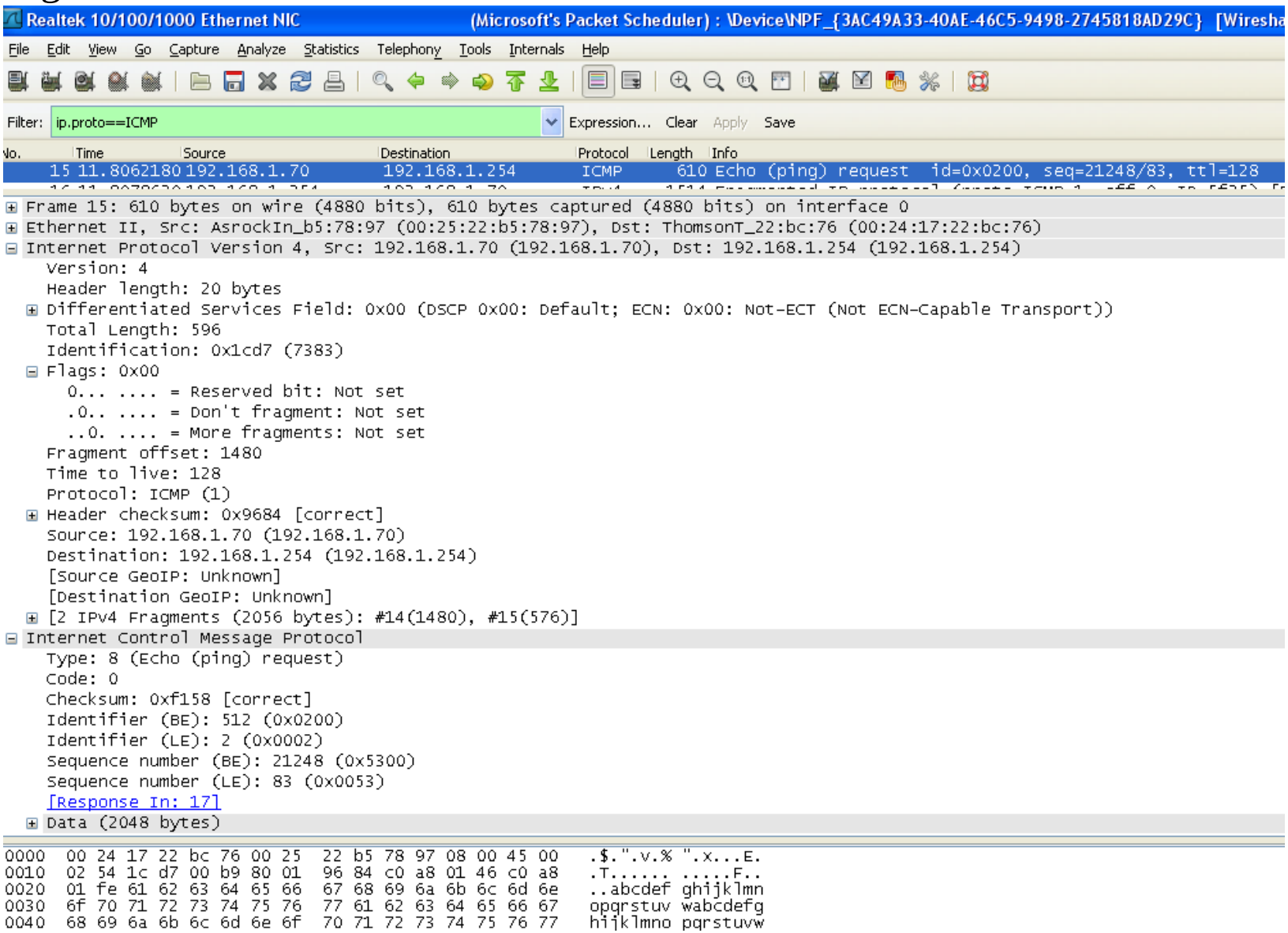
Ανάλυση Κατακερματισμένων IP πακέτων

- Fragment #1



Ανάλυση Κατακερματισμένων IP πακέτων

- Fragment #2



Παράδειγμα

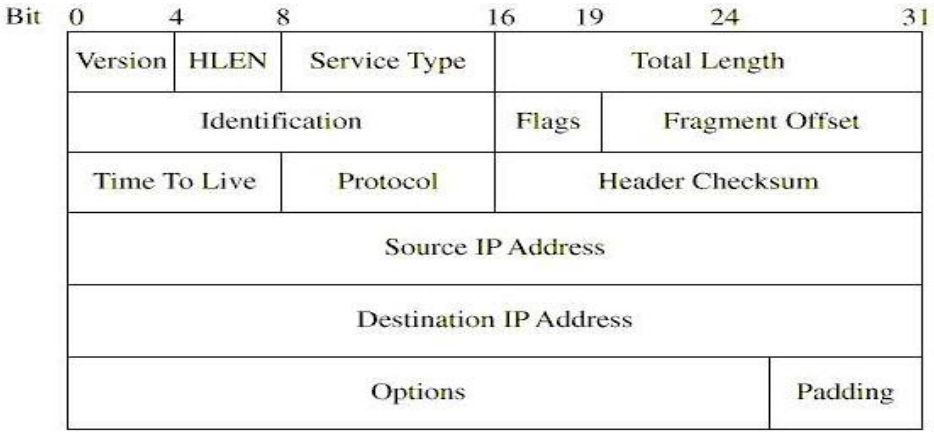
• Δίνεται η δεκαεξαδική μορφή του παρακάτω καταγεγραμμένου πλαισίου το οποίο παράχθηκε έπειτα από την εκτέλεση της εντολής ping.

Α) Πώς μπορούμε να αναγνωρίσουμε ότι το παρακάτω πλαίσιο ενθυλακώνει ένα κομμάτι ενός μεγαλύτερου κατακερματισμένου πακέτου;

Β) Ποιό είναι το μέγεθος των data που προσδιορίσαμε στην εντολή ping;

```
00 24 17 22 bc 76 00 25  22 b5 78 97 08 00 45 00   .$."·v·% "·x···E·
00 44 09 43 01 72 80 01  d1 3b c0 a8 01 45 9b cf   ·D·C·r·· ·;···E··
01 0c 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ··ijklmn opqrstuv
77 61 62 63 64 65 66 67  68 69 6a 6b 6c 6d 6e 6f   wabcdefg hijklmno
70 71 72 73 74 75 76 77  61 62 63 64 65 66 67 68   pqrstuvw abcdefgh
69 6a                                              ij
```

IP Header



ICMP Header