

# Δίκτυα Υπολογιστών II

(Ασκήσεις Πράξης)

## *Ανάλυση Πρωτοκόλλων*

*Τομέας Τηλεπικοινωνιών και Δικτύων*

Δρ. Αναστάσιος Πολίτης  
Καθηγητής Εφαρμογών  
anpol@teiser.gr

- 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.

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

ΕΦΑΡΜΟΓΗΣ (APPLICATION)	FTP, HTTP, DNS
ΜΕΤΑΦΟΡΑΣ (TRANSPORT)	TCP, UDP
ΔΙΚΤΥΟΥ (NETWORK)	IP, <b>ICMP</b> , ARP
ΦΥΣΙΚΟ (PHYSICAL)	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

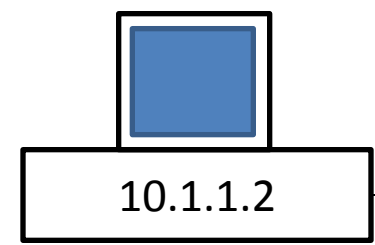
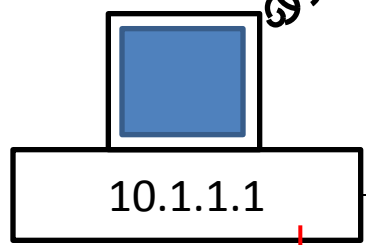
0	4	8	16	19	31
Version	IHL	Type of Service	Total Length		
Identification			Flags	Fragment Offset	
Time To Live		Protocol	Header Checksum		
Source IP Address					
Destination IP Address					
Options				Padding	

- Αποτελείται από λέξεις (words) των 32-bit.
- Αποτελείται από ένα σταθερό και ένα μεταβλητό τμήμα
  - Από το πεδίο *Version* έως 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*).

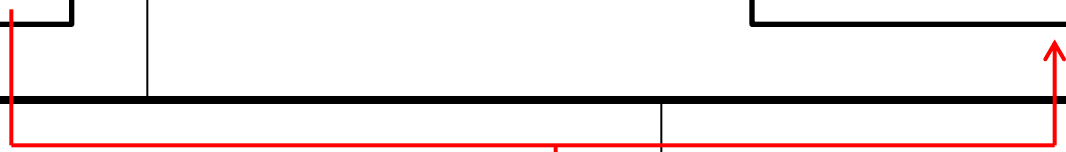
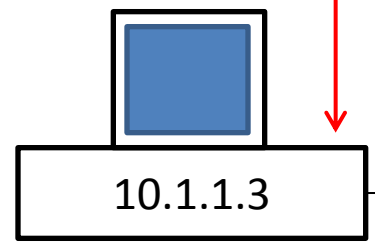


# Address Resolution Protocol

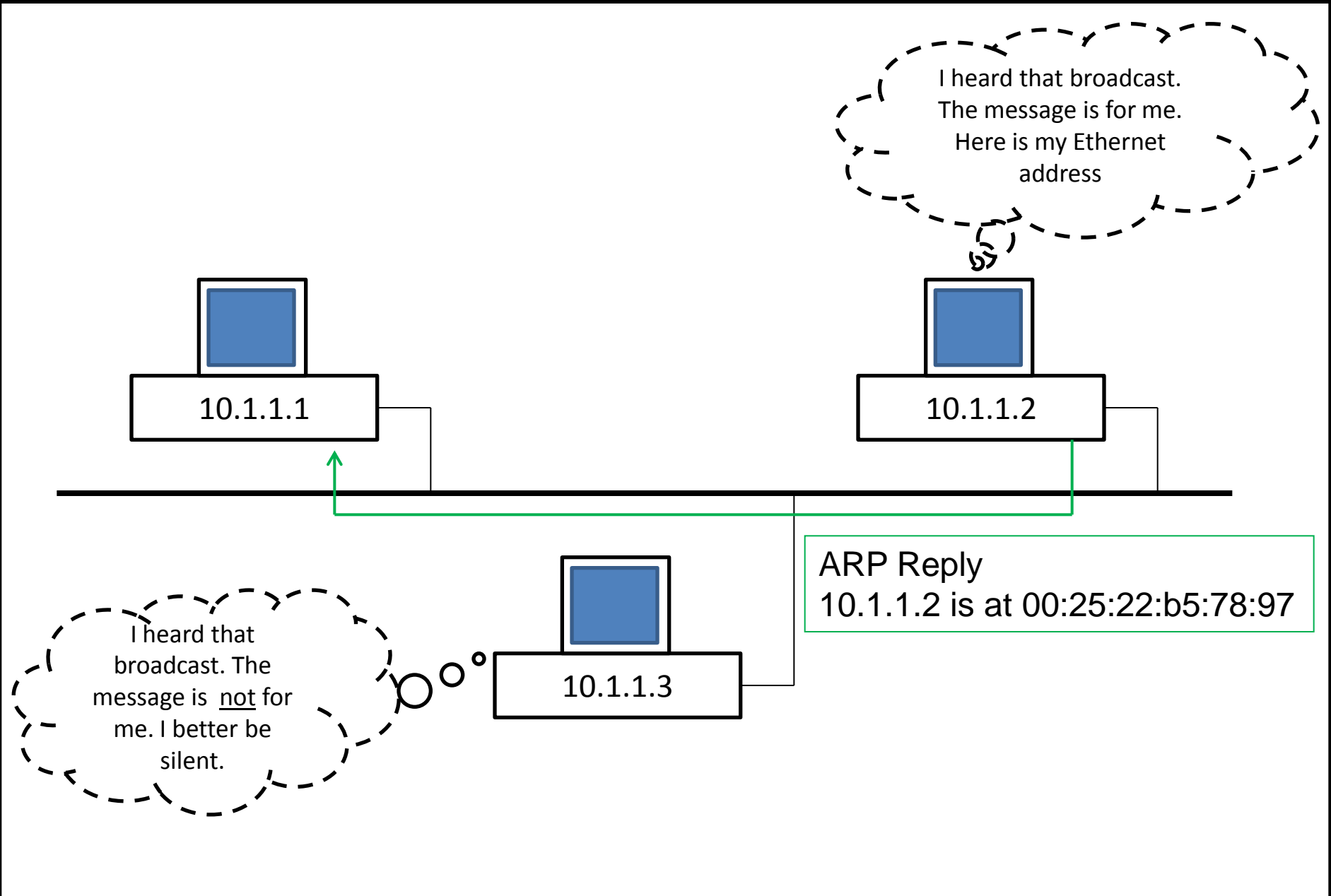
I need the Ethernet Address of 10.1.1.2



ARP Request  
Who has 10.1.1.2?  
Tell 10.1.1.1



# Address Resolution Protocol





# Καταγραφή Πακέτων ARP

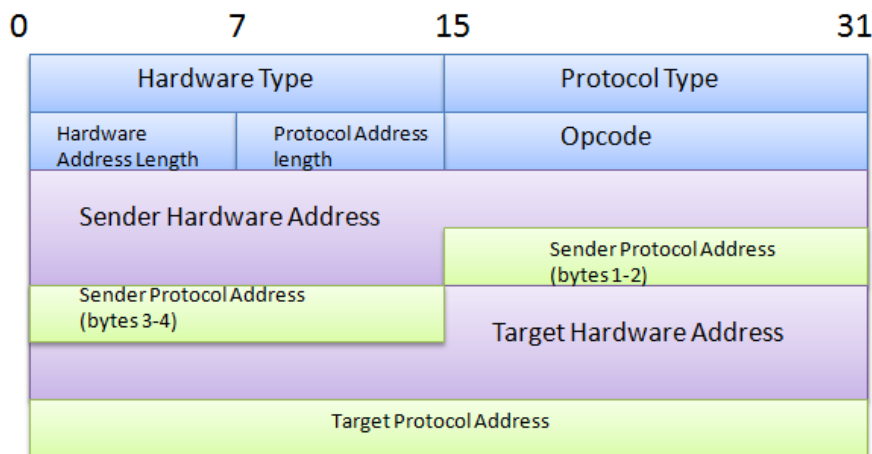
Realtek 10/100/1000 Ethernet NIC (Microsoft's Packet Scheduler) : \Device\NPF\_{3AC49A33-40AE-46C5-9498-2745818AD29C} [Wireshark]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
33	15.9437470	192.168.1.254	192.168.1.70	ICMP	74	Echo (ping) reply id=0x0200, seq=2304/9, ttl=64
34	16.9443340	192.168.1.70	192.168.1.254	ICMP	74	Echo (ping) request id=0x0200, seq=2560/10, ttl=128
35	16.9450420	192.168.1.254	192.168.1.70	ICMP	74	Echo (ping) reply id=0x0200, seq=2560/10, ttl=64
36	17.9464130	192.168.1.70	192.168.1.254	ICMP	74	Echo (ping) request id=0x0200, seq=2816/11, ttl=128
37	17.9471150	192.168.1.254	192.168.1.70	ICMP	74	Echo (ping) reply id=0x0200, seq=2816/11, ttl=64
38	18.9481650	192.168.1.70	192.168.1.254	ICMP	74	Echo (ping) request id=0x0200, seq=3072/12, ttl=128
39	18.9488610	192.168.1.254	192.168.1.70	ICMP	74	Echo (ping) reply id=0x0200, seq=3072/12, ttl=64
40	24.3604410	192.168.1.70	130.117.190.204	UDP	139	source port: udrive destination port: wizard
41	24.8878460	ThomsonT_22:bc:76	Broadcast	ARP	60	who has 192.168.1.70? Tell 192.168.1.254
42	24.8878530	AsrockIn_b5:78:97	ThomsonT_22:bc:76	ARP	42	192.168.1.70 is at 00:25:22:b5:78:97
43	24.8893580	ThomsonT_22:bc:76	Broadcast	ARP	60	who has 192.168.1.66? Tell 192.168.1.254
44	24.8906690	ThomsonT_22:bc:76	Broadcast	ARP	60	who has 192.168.1.67? Tell 192.168.1.254
45	24.8921550	ThomsonT_22:bc:76	Broadcast	ARP	60	who has 192.168.1.68? Tell 192.168.1.254
46	27.3609070	192.168.1.70	130.117.190.207	UDP	139	source port: vizablebrowser destination port: wizard
47	27.9581710	130.117.190.207	192.168.1.70	UDP	341	source port: wizard destination port: vizablebrowser
48	28.8173320	130.117.190.204	192.168.1.70	UDP	341	source port: wizard destination port: udrive
49	29.9553170	65.55.223.20	192.168.1.70	TCP	60	40034 > instl-boots [PSH, ACK] Seq=14 Ack=5 win=41808 Len=
50	30.0683290	192.168.1.70	65.55.223.20	TCP	54	instl-boots > 40034 [ACK] Seq=5 Ack=17 win=65060 Len=0
51	30.2403130	65.55.223.20	192.168.1.70	TCP	64	40034 > instl-boots [PSH, ACK] Seq=17 Ack=5 win=41808 Len=
52	30.2404040	192.168.1.70	65.55.223.20	TCP	58	instl-boots > 40034 [PSH, ACK] Seq=5 Ack=27 win=65050 Len=
53	30.4130720	65.55.223.20	192.168.1.70	TCP	60	40034 > instl-boots [ACK] Seq=27 Ack=9 win=41808 Len=0

Frame 41: 60 bytes on wire (480 bits) captured (480 bits) on interface 0



- **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.

## 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)
```

• **Εφαρμογή I:** 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 II:** 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 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.

• **Εφαρμογή I:** 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 qrstuvw
  
```

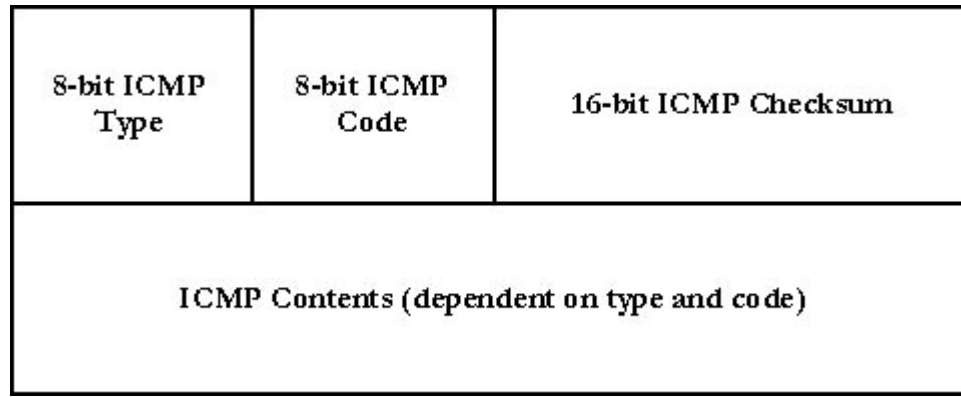
Bit	0	4	8	16	19	24	31
Version	HLEN		Service Type		Total Length		
Identification				Flags	Fragment Offset		
Time To Live		Protocol		Header Checksum			
Source IP Address							
Destination IP Address							
Options						Padding	

# 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} [Wireshark]

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-46C5-9498-2745818AD29C}

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	0.0000000	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 I:** 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                      wabcdefghg hi
  
```

Bit	0	4	8	16	19	24	31	
	Version		HLEN		Service Type		Total Length	
	Identification				Flags		Fragment Offset	
	Time To Live			Protocol		Header Checksum		
	Source IP Address							
	Destination IP Address							
	Options						Padding	

- 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*

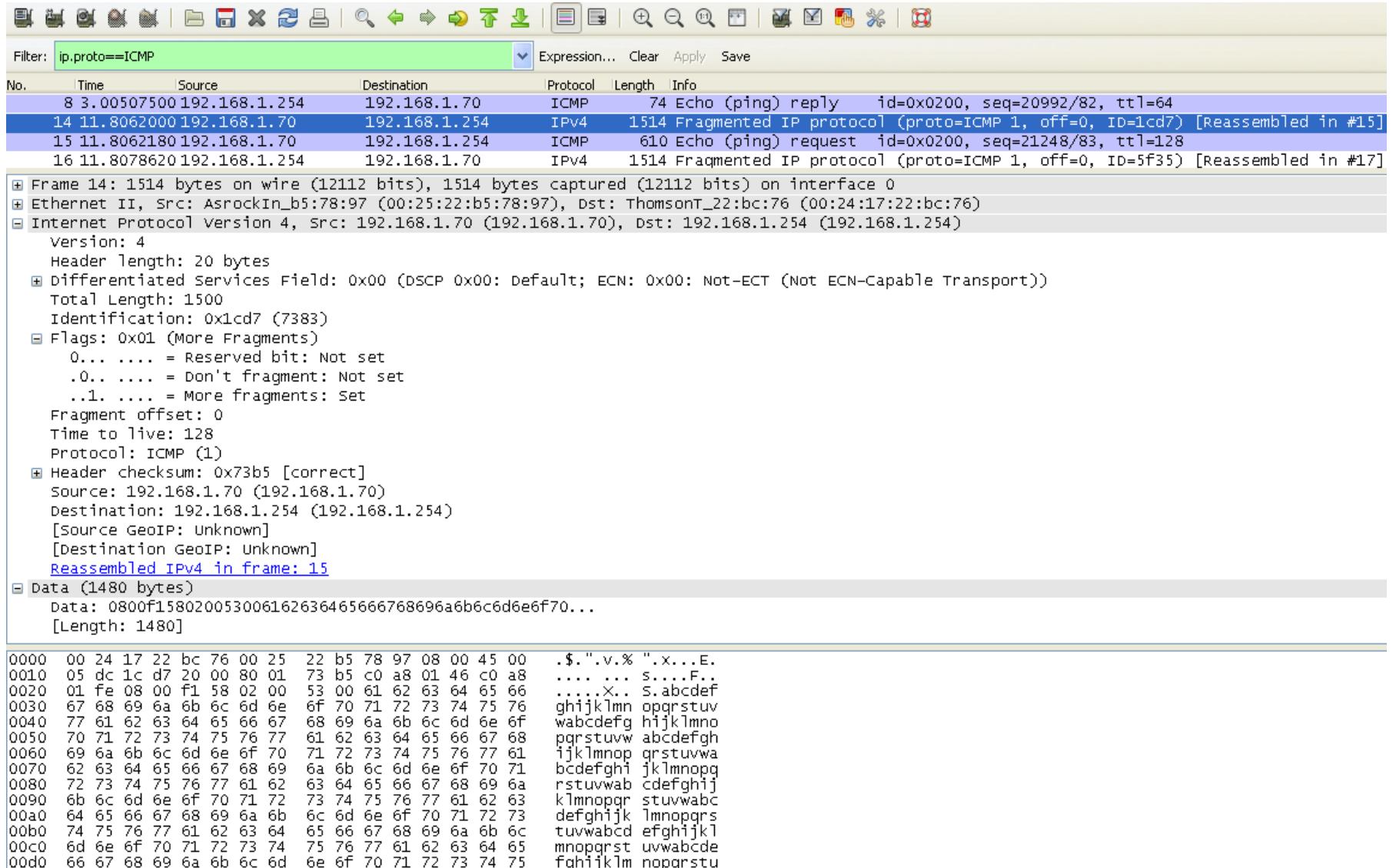
Realtek 10/100/1000 Ethernet NIC (Microsoft's Packet Scheduler) : \Device\NPF\_{3AC49A33-40AE-46C5-9498-2745818AD29C} [Wireshark 1.8.3 (SVN Rev 45256)]

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
3	1.89711800	192.168.1.70	192.168.1.254	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=018d)
4	1.89713700	192.168.1.70	192.168.1.254	ICMP	610	Echo (ping) request id=0x0200, seq=19200/75, ttl=128
5	1.89920100	192.168.1.254	192.168.1.70	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=5a0e) [Reassembled in #6]
6	1.89921500	192.168.1.254	192.168.1.70	ICMP	610	Echo (ping) reply id=0x0200, seq=19200/75, ttl=64
7	2.89932900	192.168.1.70	192.168.1.254	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=018e) [Reassembled in #8]
8	2.89934700	192.168.1.70	192.168.1.254	ICMP	610	Echo (ping) request id=0x0200, seq=19456/76, ttl=128
9	2.90095300	192.168.1.254	192.168.1.70	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=5a10) [Reassembled in #10]
10	2.90096700	192.168.1.254	192.168.1.70	ICMP	610	Echo (ping) reply id=0x0200, seq=19456/76, ttl=64
13	3.90227200	192.168.1.70	192.168.1.254	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0190) [Reassembled in #14]
14	3.90228700	192.168.1.70	192.168.1.254	ICMP	610	Echo (ping) request id=0x0200, seq=19712/77, ttl=128
15	3.90417000	192.168.1.254	192.168.1.70	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=5a12) [Reassembled in #16]
16	3.90418300	192.168.1.254	192.168.1.70	ICMP	610	Echo (ping) reply id=0x0200, seq=19712/77, ttl=64
28	4.90517600	192.168.1.70	192.168.1.254	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=019b) [Reassembled in #29]
29	4.90519200	192.168.1.70	192.168.1.254	ICMP	610	Echo (ping) request id=0x0200, seq=19968/78, ttl=128
30	4.90670600	192.168.1.254	192.168.1.70	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=5a13) [Reassembled in #31]
31	4.90672000	192.168.1.254	192.168.1.70	ICMP	610	Echo (ping) reply id=0x0200, seq=19968/78, ttl=64

## • Fragment #1



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

No.	Time	Source	Destination	Protocol	Length	Info
8	3.00507500	192.168.1.254	192.168.1.70	ICMP	74	Echo (ping) reply id=0x0200, seq=20992/82, ttl=64
14	11.8062000	192.168.1.70	192.168.1.254	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=1cd7) [Reassembled in #15]
15	11.8062180	192.168.1.70	192.168.1.254	ICMP	610	Echo (ping) request id=0x0200, seq=21248/83, ttl=128
16	11.8078620	192.168.1.254	192.168.1.70	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=5f35) [Reassembled in #17]

+ Frame 14: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0  
 + Ethernet II, Src: AsrockIn\_b5:78:97 (00:25:22:b5:78:97), Dst: ThomsonT\_22:bc:76 (00:24:17:22:bc:76)  
 + Internet Protocol version 4, Src: 192.168.1.70 (192.168.1.70), Dst: 192.168.1.254 (192.168.1.254)

```

Version: 4
Header length: 20 bytes
+ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
Total Length: 1500
Identification: 0x1cd7 (7383)
+ Flags: 0x01 (More Fragments)
  0... .... = Reserved bit: Not set
  .0.. .... = Don't fragment: Not set
  ..1. .... = More fragments: Set
Fragment offset: 0
Time to live: 128
Protocol: ICMP (1)
+ Header checksum: 0x73b5 [correct]
Source: 192.168.1.70 (192.168.1.70)
Destination: 192.168.1.254 (192.168.1.254)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Reassembled IPv4 in frame: 15
+ Data (1480 bytes)
  data: 0800f158020053006162636465666768696a6b6c6d6e6f70...
  [Length: 1480]
  
```

0000	00 24 17 22 bc 76 00 25 22 b5 78 97 08 00 45 00	.\$."v.% ".x...E.
0010	05 dc 1c d7 20 00 80 01 73 b5 c0 a8 01 46 c0 a8	.... .s....F..
0020	01 fe 08 00 f1 58 02 00 53 00 61 62 63 64 65 66	.....X.. s.abcdef
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
0040	77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f	wabcdefg hijklmno
0050	70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68	pqrstuvwxyz abcdefgh
0060	69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61	ijklmnop qrstuvw
0070	62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71	bcdefghi jklmnopq
0080	72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 6a	rstuvwab cdefghij
0090	6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63	klmnopqr stuvwabc
00a0	64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73	defghijk lmnopqrs
00b0	74 75 76 77 61 62 63 64 65 66 67 68 69 6a 6b 6c	tuvwxyzefghijkl
00c0	6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63 64 65	mopqrstu vwabcde
00d0	66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75	fghijklm nopqrstu

## • Fragment #2

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

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
15	11.8062180	192.168.1.70	192.168.1.254	ICMP	610	Echo (ping) request id=0x0200, seq=21248/83, ttl=128

- Frame 15: 610 bytes on wire (4880 bits), 610 bytes captured (4880 bits) on interface 0
- Ethernet II, Src: AsrockIn\_b5:78:97 (00:25:22:b5:78:97), Dst: ThomsonT\_22:bc:76 (00:24:17:22:bc:76)
- Internet Protocol Version 4, Src: 192.168.1.70 (192.168.1.70), Dst: 192.168.1.254 (192.168.1.254)
  - Version: 4
  - Header length: 20 bytes
  - Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  - Total Length: 596
  - Identification: 0x1cd7 (7383)
  - Flags: 0x00
    - 0... .... = Reserved bit: Not set
    - .0.. .... = Don't fragment: Not set
    - ..0. .... = More fragments: Not set
  - Fragment offset: 1480
  - Time to live: 128
  - Protocol: ICMP (1)
  - Header checksum: 0x9684 [correct]
  - Source: 192.168.1.70 (192.168.1.70)
  - Destination: 192.168.1.254 (192.168.1.254)
  - [Source GeoIP: Unknown]
  - [Destination GeoIP: Unknown]
  - [2 IPv4 Fragments (2056 bytes): #14(1480), #15(576)]
- Internet Control Message Protocol
  - Type: 8 (Echo (ping) request)
  - Code: 0
  - Checksum: 0xf158 [correct]
  - Identifier (BE): 512 (0x0200)
  - Identifier (LE): 2 (0x0002)
  - Sequence number (BE): 21248 (0x5300)
  - Sequence number (LE): 83 (0x0053)
  - [\[Response In: 17\]](#)
- Data (2048 bytes)
 

0000	00 24 17 22 bc 76 00 25 22 b5 78 97 08 00 45 00	.\$."v.% ".x...E.
0010	02 54 1c d7 00 b9 80 01 96 84 c0 a8 01 46 c0 a8	.T..... ..F..
0020	01 fe 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e	..abcdef ghijklmn
0030	6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67	opqrstuv wabcdefg
0040	68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77	hijklmno pqrstuvw

# Παράδειγμα

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

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

B) 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  wabcdefgh hijklmno
70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68  pqrstuvwxyz abcdefgh
69 6a                                           ij
  
```

IP Header

Bit	0	4	8	16	19	24	31
	Version	HLEN	Service Type	Total Length			
	Identification			Flags	Fragment Offset		
	Time To Live		Protocol	Header Checksum			
	Source IP Address						
	Destination IP Address						
	Options					Padding	

ICMP Header

8-bit ICMP Type	8-bit ICMP Code	16-bit ICMP Checksum
ICMP Contents (dependent on type and code)		