

ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΣ ΔΙΚΤΥΩΝ

ΔΙΑΛΕΞΗ 2

ΔΙΔΑΣΚΩΝ: ΑΝΑΡΓΥΡΟΣ ΣΙΔΕΡΗΣ

`<sideris@epp.teiher.gr>`

`<https://eclass2.teicrete.gr/courses/TP182/>`

ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΠΟΛΥΜΕΣΩΝ
ΤΕΙ ΚΡΗΤΗΣ



ΠΡΩΤΟΚΟΛΛΟ ΔΙΑΔΙΚΤΥΟΥ (INTERNET PROTOCOL-IP)



Γενικά (1)

- Προτυποποίηση το Σεπτέμβρη του 1981 (RFC 791).
- Σκοπός:
 - Υπηρεσίες διαλειτουργικότητας μεταξύ δικτύων με διαφορετικές τεχνολογίες διασύνδεσης.
- Παρέχει:
 - Έλεγχο για αλλοίωση επικεφαλίδας.
 - Υποτυπώδη έλεγχο συμφόρησης.

Γενικά (2)

- Δεν παρέχει:
 - Έλεγχο ρυθμού ροής.
 - Έλεγχο πολλαπλών αντίγραφων των πακέτων.
 - Έλεγχο για ορθή σειρά παράδοσης των πακέτων.
- Λειτουργίες:
 - Διευθυνσιοδότηση
 - Κατακερματισμό/Επανασυναρμολόγηση πακέτων
- Πύλες (Gateways)
 - Δρομολόγηση



IP Επικεφαλίδα (1)

```

0          1          2          3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version|  IHL  |Type of Service|          Total Length        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Identification          |Flags|      Fragment Offset  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time to Live |    Protocol   |           Header Checksum   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source Address                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination Address                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

```

Πηγή: <http://www.networksorcery.com/enp/rfc/rfc791.txt>

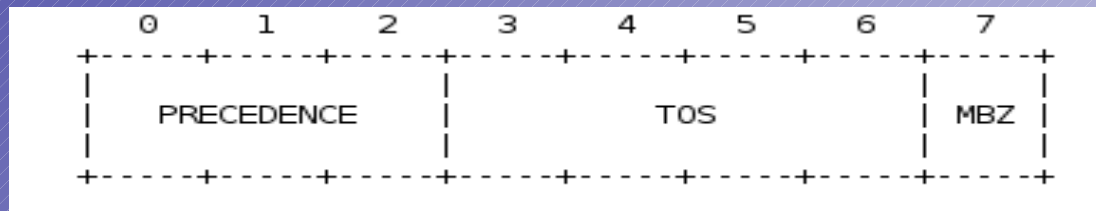


IP Επικεφαλίδα (2)

- **Version (4 bits)**: Η έκδοση του πρωτοκόλλου. Σε αυτή τη διάλεξη περιγράφουμε την έκδοση 4.
- **IHL (4 bits)**: Δίνει το μήκος της επικεφαλίδας σε λέξεις των 32 bit. Το ελάχιστο είναι 5.
- **TOS (8 bits-RFC 1349)**: χρησιμοποιείται για τον καθορισμό της ποιότητας υπηρεσίας των πακέτων μιας ροής.
 - Τα πρώτα 3 bit καθορίζουν την προτεραιότητα του πακέτου.
 - Τα επόμενα 4 bit καθορίζουν το τύπο της υπηρεσίας.
 - Το τελευταίο bit δεσμευμένο για πειραματικούς λόγους (συνήθως είναι 0).

IP Επικεφαλίδα (3)

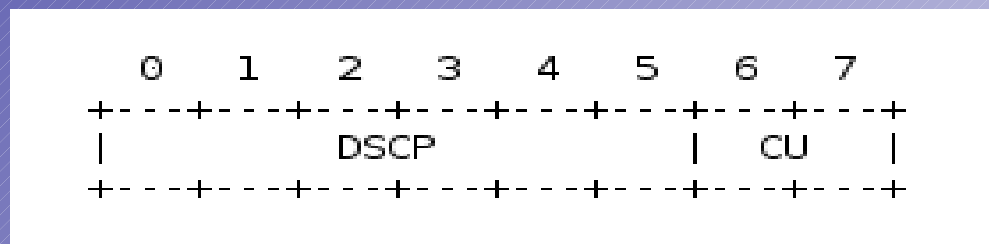
TOS τιμή	Σημασία
1000	Ελαχιστοποίηση καθυστέρησης
0100	Μεγιστοποίηση του ρυθμού μετάδοσης
0010	Μεγιστοποίηση της αξιοπιστίας
0001	Ελαχιστοποίηση κόστους
0000	Τυπική υπηρεσία



Πηγή: <http://tools.ietf.org/html/rfc1349>

IP Επικεφαλίδα (4)

- Το TOS πεδίο έχει αντικατασταθεί από το πεδίο διαφοροποιημένων υπηρεσιών (DS field-RFC 2474).
- Τα πρώτα 6 από τα 8 bit χρησιμοποιούνται για τη κατηγοριοποίηση του πακέτου.
- Τα τελευταία 2 bit δεν χρησιμοποιούνται.
 - Πόσες διαφορετικές κατηγοριοποιήσεις υπηρεσιών έχουμε τώρα;



Πηγή:

<http://tools.ietf.org/html/rfc2474>



IP Επικεφαλίδα (5)

- **Total length (16 bits):** Το συνολικό μέγεθος του IP πακέτου.
 - Ποιό είναι το μέγιστο μέγεθος;
- **Identification (16 bits):** Ο αριθμός αυτό χρησιμοποιείται για να αναγνωριστούν τα τμήματα ενός κατακερματισμένου πακέτου.
- **Flags (3 bits):**
 - **Reserved (1 bit).**
 - **DF (1 bit):** Εάν έχει την τιμή 1 απαγορεύει το τεμάχισμα του πακέτου.
 - **MF (1 bit):** Με τη τιμή ίσον με 1 δηλώνει ότι ακολουθούν και άλλα τεμάχια αυτού του πακέτου.



IP Επικεφαλίδα (6)

- **Fragment offset (13 bits):** Δηλώνει την θέση τμήματος στο αρχικό πακέτο.
- **Time to Live-TTL (8 bits):** Προσδιορίζει από πόσους ενδιαμέσους κόμβους μπορεί να περάσει ένα πακέτο πριν απορριφθεί.
 - Πόσοι κόμβοι είναι αυτοί;
 - Γιατί χρησιμοποιείται;
- **Protocol (8 bits):** Δηλώνει το πρωτόκολλο που τρέχει στο ανώτερο στρώμα (στρώμα μεταφοράς).
- **Header Checksum (16 bits):** Χρησιμοποιείται για να ελέγξει για τυχόν αλλοιώσεις κατά τη μετάδοση της IP επικεφαλίδας.
 - Κάθε πότε και γιατί γίνεται έλεγχος/υπολογισμός του checksum;



IP Επικεφαλίδα (7)

- **Source Address (32 bits):** Η διεύθυνση του αποστολέα.
- **Destination Address (32 bits):** Η διεύθυνση του παραλήπτη.
- **Options (μεταβλητό μέγεθος):** Επιπλέον παράμετροι μπορούν να δηλωθούν εδώ όπως για την καταγραφή διαδρομής, χρονοσφραγίδα κ.τ.λ. Το πεδίο αυτό πρέπει να είναι πολλαπλάσιο των 32 bit (Padding εάν όχι).
- Μετά και αυτό το πεδίο ακολουθούν τα δεδομένα (payload).
 - Εάν η επικεφαλίδα έχει μέγεθος 20 bytes (no options) πόσο είναι το μέγιστο payload;

Κατακερματισμός (1)

(RFC 791)

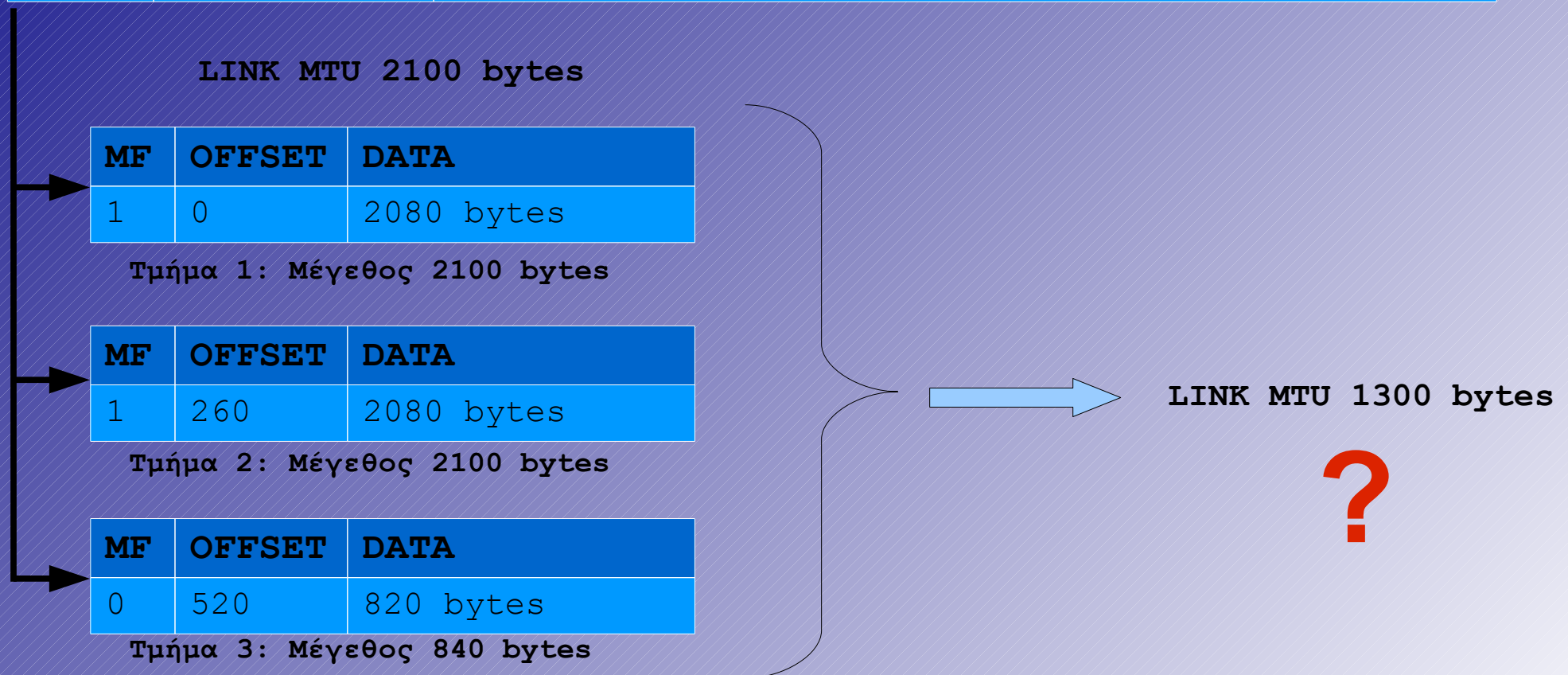
- Ενεργοποιείται όταν το MTU (Maximum Transmission Unit) της ζεύξης (link-L2) είναι μικρότερο του μεγέθους ενός IP πακέτου (L3).
- Το ελάχιστο MTU που υποστηρίζουν όλοι οι δρομολογητές είναι 576 bytes.
- Ο κατακερματισμός προκαλεί επιπλέον φόρτο στο δίκτυο (Γιατί).
- Υπάρχει η τεχνική MTU discovery:
 - Στέλνουμε πακέτα με το DF πεδίο ενεργοποιημένο.
 - Εάν κάποια ζεύξη ενός δρομολογητή δεν το υποστηρίζει θα μας γυρίσει ένα μήνυμα "Destination Unreachable - Fragmentation Needed".
 - Μειώνουμε το μέγεθος του IP πακέτου και επαναλαμβάνουμε μέχρι να μην παίρνουμε αυτό το μήνυμα



Κατακερματισμός (2) (RFC 791)

IP πακέτο 5000 bytes (20 bytes OH)

MF	OFFSET	DATA
0	0	4980 bytes



Ανασύνθεση κατακερματισμένων IP πακέτων (RFC 815)

- Ανασύνθεση των κατακερματισμένων πακέτων από τους τελικούς παραλήπτες.
- Βασικές λειτουργίες:
 - Αναγνώριση τμημάτων πακέτων:
 - Έλεγχος πεδίου MF.
 - Έλεγχος πεδίου Fragment Offset.
 - Ταυτοποίηση τμημάτων:
 - Πεδία protocol, identification, source/destination address.
 - Χρήση προσωρινής μνήμης για αποθήκευση.
 - Χρήση χρονοδιακόπτη.
 - Γιατί;



Διευθυνσιοδότηση (1)

- Διευθύνσεις μεγέθους 32 bits.
 - Χωρίζονται σε 4 ομάδες των 8 bit.
 - Εύρος τιμών ανά ομάδα (octet):
 - $2^8=256$ άρα από 0-255.
 - Κάθε IP διεύθυνση χωρίζεται σε δικτυακό (network) μέρος και μέρος υπολογιστή (host).
 - Το μέρος δικτύου αξιοποιείται από τους δρομολογητές για τις ανάγκες της προώθησης πακέτων μεταξύ διαφορετικών δικτύων.
 - Το μέρος του υπολογιστή ταυτοποιεί τον υπολογιστή μέσα σε ένα δίκτυο.
 - Μέχρι το 1993 διαχωρισμός δικτύων με το σύστημα των κλάσεων.
 - Από το 1993 και μετά διαχωρισμός δικτύων βάση του **Classless Interdomain Routing-CIDR (RFC 4632)**.



Διευθυνσιοδότηση (2)

Σύστημα Τάξεων

Τάξη	1 ^ο Octet	Default Subnet mask	Αριθ. δικτύων	Αριθ. Υπολογιστών
A	0xxxxxxx	255.0.0.0	$2^7=128$	$2^{24}-2=16777214$
B	10xxxxxx	255.255.0.0	$2^{14}=16384$	$2^{16}-2=65534$
C	110xxxxx	255.255.255.0	$2^{23}=2097152$	$2^8-2=254$
D	1110xxxx	Χρησιμοποιείται για πολλαπλή διανομή (multicast)		
E	1111xxxx	Δεσμευμένη για πειραματικούς λόγους.		



Διευθυνσιοδότηση (3)

- CIDR
 - Οι διευθύνσεις αναγράφονται μαζί με το subnet mask τους.
 - 10.0.2.3/24
 - /24=11111111.11111111.11111111.00000000
 - Το subnet mask είναι πια μεταβλητού μήκους.
 - Πιο ευέλικτος τρόπος οργάνωσης και διαχείρισης δικτύων.
 - Δηλαδή;
- Διευθύνσεις ιδιωτικών δικτύων (ψεύτικες IP):
 - 10.0.0.0/8
 - 172.16.0.0/12
 - 192.168.0.0/16

Διευθυνσιοδότηση (4)

- Παράδειγμα εύρεσης μέρους δικτύου και υπολογιστή:

- 11.5.4.130/26:

00001011.00000101.00000100.10**000010** (Μέρος υπολογ.)

AND 11111111.11111111.11111111.11000000

00001011.00000101.00000100.10000000 (Μέρος δικτύου)

- Σε δεκαδικό το δικτυακό μέρος είναι 11.5.4.128.

- Άν το αφαιρέσουμε από το αρχικό IP παίρνουμε πάλι το μέρος υπολογιστή:

11.5.4.130

- 11.5.4.128

0.0.0.2 (Μέρος υπολογ.)

Υποδίκτυα (1)

- Δίκτυο:
 - 13.13.0.0/16
- Να το "σπάσουμε" σε 4 υποδίκτυα
- Βήματα:
 - Υπολογίζουμε το νέο subnet mask.
 - Ποιός είναι ο ελάχιστος αριθμός εκείνος που εάν τον υψώσουμε σαν εκθέτη στο 2 θα μας καλύψει τον αριθμό των νέων υποδικτύων;
 - Προσθέτουμε αυτό τον αριθμό στο αρχικό αριθμό άσων του subnet mask, $16+2=18$.
 - Άρα το νέο mask είναι /18. (Οι νέοι άσσοι είναι στο 3 octet)
 - Πόσα μηδενικά είναι στο octet που έχει το τελευταίο 1 στο νέο subnet; (Ονομάστε το αριθμό αυτό κ).

Υποδίκτυα (2)

- Τα νέα υποδίκτυα προκύπτουν με επαναληπτική πρόσθεση του αριθμού 2^k (εδώ $k=6$) ξεκινώντας από το πρώτο υποδίκτυο.

Υποδίκτυο	Εύρος Διευθύνσεων	Broadcast
13.13.0.0/18	13.13.0.1-13.13.63.254	13.13.63.255
13.13.64.0/18	13.13.64.1-13.13.127.254	13.13.127.255
13.13.128.0/18	13.13.128.1-13.13.191.254	13.13.191.255
13.13.192.0/18	13.13.192.1-13.13.255.254	13.13.255.255

Δρομολόγηση (1)

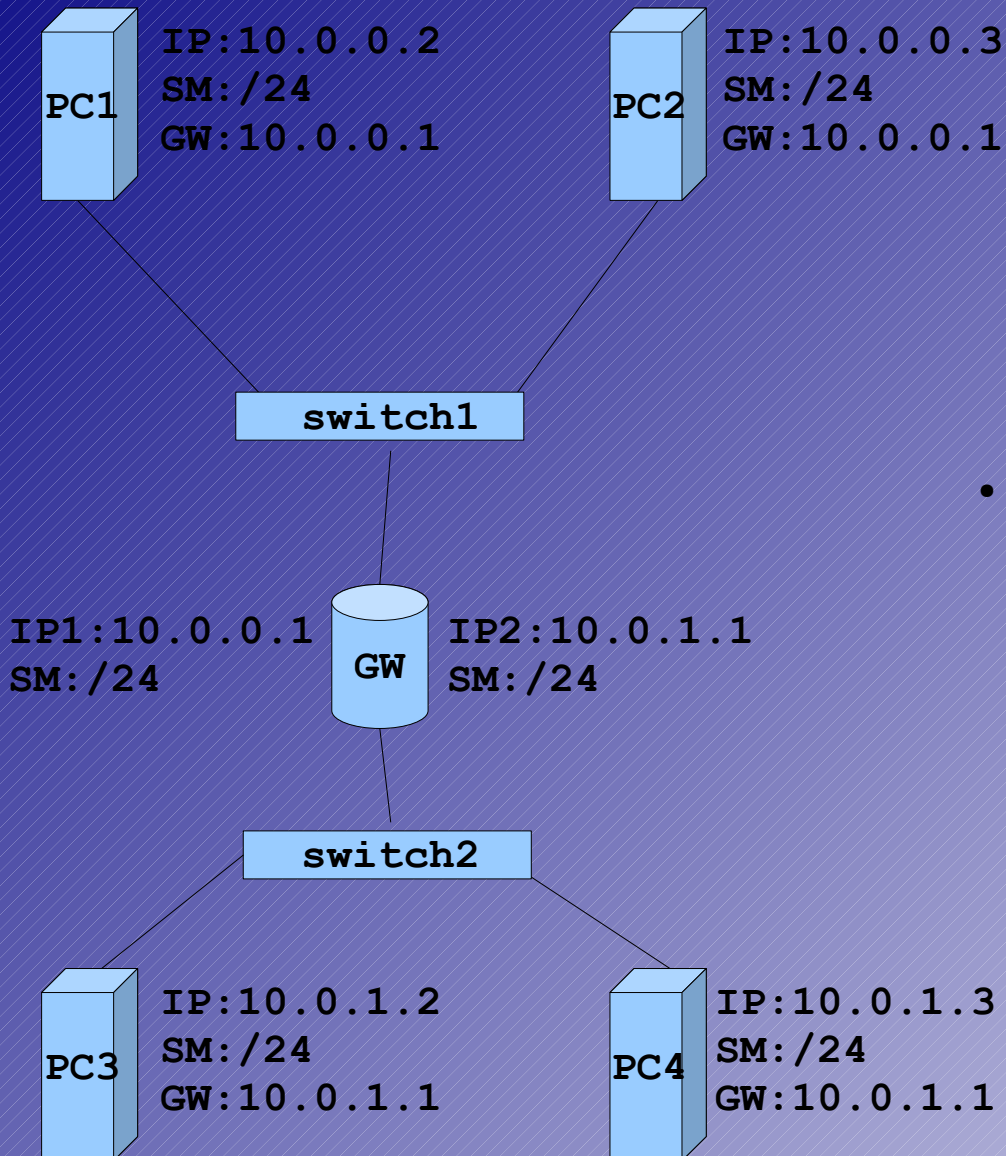
- Τι είναι;
 - Η διαδικασία παράδοσης ενός IP πακέτου.
 - Γίνεται βάση του μέρους δικτύου μιας IP διεύθυνσης και ενός πίνακα δρομολόγησης.

```
lilith ~ # ip route show
10.0.0.0/24 dev wlan0 proto kernel scope link src 10.0.0.242
127.0.0.0/8 dev lo scope link
default via 10.0.0.1 dev wlan0
```

- Δύο κατηγορίες:
 - Άμεση παράδοση.
 - Έμμεση παράδοση.



Δρομολόγηση (2)



- Άμεση παράδοση (PC1->PC2):
 - Το PC1 ελέγχει εάν ο παραλήπτης είναι στο ίδιο δίκτυο. (Είναι;)
 - Το PC1 μαθαίνει το MAC του παραλήπτη. (Πώς;)
 - Το PC1 ενθυλακώνει το IP πακέτο σε ένα Ethernet πλαίσιο και το αποστέλλει.
- Έμμεση παράδοση (PC1->PC4):
 - Το PC1 ελέγχει εάν ο παραλήπτης είναι στο ίδιο δίκτυο. (Είναι;)
 - Συμβουλευείται το πίνακα δρομολόγησης για να μάθει τον επόμενο κόμβο-σταθμό.
 - Το PC1 ενθυλακώνει το IP πακέτο σε ένα Ethernet πλαίσιο με MAC παραλήπτη τη MAC του επόμενου κόμβου και το αποστέλλει.
 - Ο GW επαναλαμβάνει τη διαδικασία.
 - Της άμεσης ή έμμεσης παράδοσης;

Internet Control Message Protocol ICMP



ICMP (RFC 792)

- Προτυποποιήθηκε Σεπτέμβρη του 1981 (RFC 792) .
- Προσφέρει μηχανισμούς ελέγχου και αναφοράς σφαλμάτων κατά την μετάδοση πακέτων IP.
- Τα ICMP πακέτα ενθυλακώνονται στο πεδίο δεδομένων των IP πακέτων.
- Στη ICMP επικεφαλίδα υπάρχουν τα πεδία τύπος και κωδικός.
 - Βάση των δύο αυτών πεδίων προσδιορίζεται και το είδος του ICMP μηνύματος.

Τύπος	Κωδικός	Περιγραφή
8	0	Echo request
0	0	Echo reply
11	0	time to live exceeded in transit
11	1	fragment reassembly time exceeded
3	0	net unreachable

Παραδείγματα (1)

```
irons : bash
File Edit View Scrollback Bookmarks Settings Help
lilith ~ # ping -c 1 193.92.9.1
PING 193.92.9.1 (193.92.9.1) 56(84) bytes of data.
64 bytes from 193.92.9.1: icmp_seq=1 ttl=254 time=1.75 ms

--- 193.92.9.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.750/1.750/1.750/0.000 ms
lilith ~ #
```

Terminal window showing a ping command execution. The window title is "irons : bash". The output shows a successful ping to 193.92.9.1 with a response time of 1.75 ms. The statistics show 1 packet transmitted and received with 0% packet loss. The terminal window is part of a desktop environment with other tabs visible at the bottom: "...ons : wpa_supplicant", "irons : python2.6", "irons : bash", and "irons : bash".

Παραδείγματα (2)

The image shows a Wireshark capture window titled "(Untitled) - Wireshark". The filter bar is set to "icmp". The packet list pane shows two packets:

No.	Time	Source	Destination	Protocol	Info
5	14.022323	10.0.0.242	193.92.9.1	ICMP	Echo (ping) request
6	14.023998	193.92.9.1	10.0.0.242	ICMP	Echo (ping) reply

The packet details pane for packet 5 shows:

- Ethernet II, Src: IntelCor_bc:78:ad (00:1c:bf:bc:78:ad), Dst: EdimaxTe_01:81:ef (00:0e:2e:01:81:ef)
- Internet Protocol, Src: 10.0.0.242 (10.0.0.242), Dst: 193.92.9.1 (193.92.9.1)
- Internet Control Message Protocol
 - Type: 8 (Echo (ping) request)
 - Code: 0 ()
 - Checksum: 0x55df [correct]
 - Identifier: 0x451d
 - Sequence number: 1 (0x0001)
 - Data (56 bytes)

The packet bytes pane shows the raw data for packet 5:

```
0020 09 01 08 00 55 df 45 1d 00 01 24 3a a3 4b aa 79  ..U.E. ..$.K.y
0030 00 00 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15  .....
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  ..!#$%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,-./012345
```

The status bar at the bottom indicates: Type (icmp.type), 1 byte | Packets: 34 Displayed: 2 Marked: 0 Dropped: 0 | Profile: Default

Παραδείγματα (3)

```
irons : bash
File Edit View Scrollback Bookmarks Settings Help
lilith ~ # ping -c 1 -s 1473 -M do 193.92.9.52
PING 193.92.9.52 (193.92.9.52) 1473(1501) bytes of data.
From 10.0.0.242 icmp_seq=1 Frag needed and DF set (mtu = 1500)
(00:2e:01:31:ef), Dst: IntelCor_bc:78:ad (00:1c:bf:bc:78:ad)
--- 193.92.9.52 ping statistics ---
0 packets transmitted, 0 received, +1 errors

lilith ~ # ping -c 1 -t 2 193.92.30.19
PING 193.92.30.19 (193.92.30.19) 56(84) bytes of data.
From 193.92.9.1 icmp_seq=1 Time to live exceeded

--- 193.92.30.19 ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms

lilith ~ #
```



Παραδείγματα (4)

The image shows a Wireshark capture of an ICMP Echo (ping) request and its response. The packet list pane shows two packets:

No.	Time	Source	Destination	Protocol	Info
52	25.966634	10.0.0.242	193.92.30.19	ICMP	Echo (ping) request
53	25.971053	193.92.9.1	10.0.0.242	ICMP	Time-to-live exceeded (Time to live exceeded in transit)

The packet details pane for packet 52 shows the following structure:

- Frame 52 (98 bytes on wire, 98 bytes captured)
- Ethernet II, Src: IntelCor_bc:78:ad (00:1c:bf:bc:78:ad), Dst: EdimaxTe_01:81:ef (00:0e:2e:01:81:ef)
- Internet Protocol, Src: 10.0.0.242 (10.0.0.242), Dst: 193.92.30.19 (193.92.30.19)
 - Version: 4
 - Header length: 20 bytes
 - Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
 - Total Length: 84
 - Identification: 0x0000 (0)
 - Flags: 0x02 (Don't Fragment)
 - Fragment offset: 0
 - Time to live: 2
 - [Expert Info (Note/Sequence): "Time To Live" only 2]
 - Protocol: ICMP (0x01)
 - Header checksum: 0x8e48 [correct]
 - Source: 10.0.0.242 (10.0.0.242)
 - Destination: 193.92.30.19 (193.92.30.19)
- Internet Control Message Protocol
 - Type: 8 (Echo (ping) request)
 - Code: 0 ()
 - Checksum: 0x816a [correct]
 - Identifier: 0x0308
 - Sequence number: 1 (0x0001)
 - Data (56 bytes)

The packet bytes pane shows the raw data for the first few bytes of the packet:

```
0010  00 54 00 00 40 00 02 01 8e 48 0a 00 00 f2 c1 5c  .T..@. .H....\  
0020  1e 13 08 00 81 6a 03 08 00 01 74 3e a3 4b 65 ff  ....j.. ..t>.Ke.  
0030  0b 00 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15  ..  
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  ..!"#$%
```



Παραδείγματα (5)

The image shows a Wireshark window titled "(Untitled) - Wireshark". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, and Help. The toolbar contains various icons for file operations, capture, and analysis. The filter bar shows "Filter: icmp" with buttons for "Expression...", "Clear", and "Apply".

No.	Time	Source	Destination	Protocol	Info
52	25.966634	10.0.0.242	193.92.30.19	ICMP	Echo (ping) request
53	25.971053	193.92.9.1	10.0.0.242	ICMP	Time-to-live exceeded (Time to live exceeded in transit)

Below the packet list, the details pane for frame 53 is expanded, showing the following structure:

- Frame 53 (70 bytes on wire, 70 bytes captured)
- Ethernet II, Src: EdimaxTe_01:81:ef (00:0e:2e:01:81:ef), Dst: IntelCor_bc:78:ad (00:1c:bf:bc:78:ad)
- Internet Protocol, Src: 193.92.9.1 (193.92.9.1), Dst: 10.0.0.242 (10.0.0.242)
 - Version: 4
 - Header length: 20 bytes
 - Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6; ECN: 0x00)
 - Total Length: 56
 - Identification: 0xb823 (47139)
 - Flags: 0x00
 - Fragment offset: 0
 - Time to live: 254
 - Protocol: ICMP (0x01)
 - Header checksum: 0x2e92 [correct]
 - Source: 193.92.9.1 (193.92.9.1)
 - Destination: 10.0.0.242 (10.0.0.242)
- Internet Control Message Protocol
 - Type: 11 (Time-to-live exceeded)
 - Code: 0 (Time to live exceeded in transit)
 - Checksum: 0xe8b7 [correct]
 - Internet Protocol, Src: 10.0.0.242 (10.0.0.242), Dst: 193.92.30.19 (193.92.30.19)
 - Version: 4
 - Header length: 20 bytes
 - Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
 - Total Length: 84

At the bottom, the packet bytes pane shows hex and ASCII data for packets 0020, 0030, and 0040.

Bottom status bar: Type (icmp.type), 1 byte | Packets: 106 Displayed: 2 Marked: 0 Dropped: 0 | Profile: Default



User Datagram Protocol

UDP



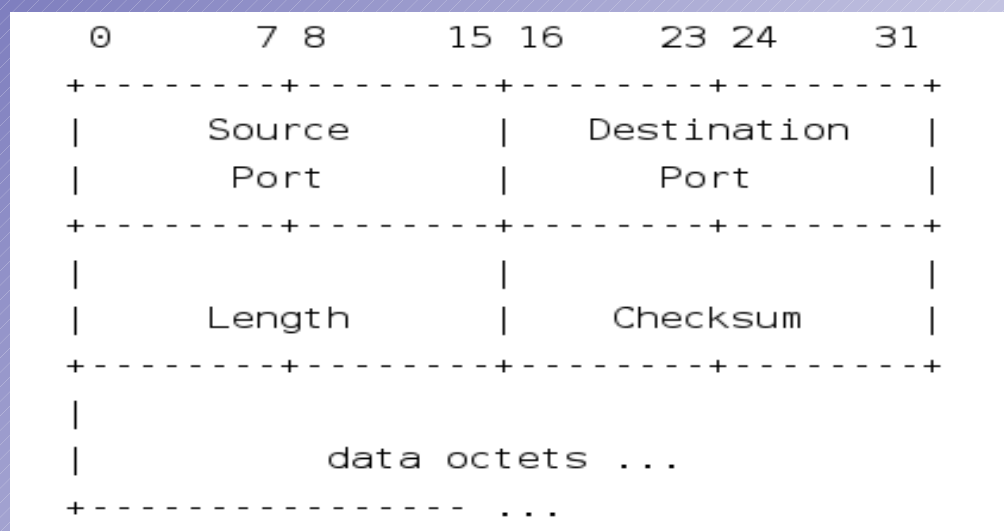
Γενικά (1)

- Προτυποποίηση το Αύγουστο του 1980 (RFC 768).
- Σκοπός:
 - Υπηρεσίες επικοινωνίας μεταξύ διεργασιών.
- Παρέχει:
 - Έλεγχο για αλλοίωση πακέτου.
 - Χρήση ψευτοεπικεφαλίδας.
 - IP:src/dst address,protocol,udp length
 - UDP: όλα τα πεδία.
- Δεν παρέχει:
 - Έλεγχο ρυθμού ροής, συμφόρησης και απώλειας πακέτων.
 - Έλεγχο πολλαπλών αντίγραφων των πακέτων.
 - Έλεγχο για ορθή σειρά παράδοσης των πακέτων.



Γενικά (2)

- Γρήγορο: μη εγκαθίδρυση σύνδεσης πριν την αποστολή δεδομένων.
- Εύκολη υλοποίηση
- Χρησιμοποιείται από εφαρμογές όπως:
 - Εφαρμογές μετάδοσης video και φωνής.
 - Γιατί;
 - DNS, DHCP, SNMP....



Πηγή: <http://tools.ietf.org/html/rfc768>



Παραδείγματα (1)

```
irons : iperf
File Edit View Scrollback Bookmarks Settings Help
lilith ~ # iperf -s -u
-----
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size: 112 KByte (default)
-----
[ 3] local 10.0.0.242 port 5001 connected with 10.0.0.1 port 18302
[ ID] Interval      Transfer    Bandwidth    Jitter    Lost/Total Datagrams
[ 3] 0.0-60.0 sec  7.50 MBytes 1.05 Mbits/sec 0.101 ms   1/ 5352 (0.019%)
#
```

```
10.0.0.1:
File Edit View Scrollback Bookmarks Settings Help
# iperf -c 10.0.0.242 -t 60 -u
-----
Client connecting to 10.0.0.242, UDP port 5001
Sending 1470 byte datagrams
UDP buffer size: 9.00 KByte (default)
-----
[ 3] local 10.0.0.1 port 18302 connected with 10.0.0.242 port 5001
[ 3] 0.0-60.0 sec  7.50 MBytes 1.05 Mbits/sec
[ 3] Sent 5351 datagrams
[ 3] Server Report:
[ 3] 0.0-60.0 sec  7.50 MBytes 1.05 Mbits/sec 0.100 ms   1/ 5352 (0.019%)
#
```

Παραδείγματα (2)

The image shows the Wireshark network traffic analysis interface. The title bar reads "(Untitled) - Wireshark". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, and Help. The toolbar contains various icons for file operations, capture, and analysis. The filter bar shows the filter "udp and ip.addr==10.0.0.1". The packet list pane displays several UDP packets from source 10.0.0.1 to destination 10.0.0.242. The packet details pane shows the structure of frame 5571, including Ethernet II, Internet Protocol (Version 4), and User Datagram Protocol (Source port: 18302, Destination port: complex-link). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Info
5569	94.036011	10.0.0.1	10.0.0.242	UDP	Source port: 18302 Destination port: complex-link
5570	94.047216	10.0.0.1	10.0.0.242	UDP	Source port: 18302 Destination port: complex-link
5571	94.058426	10.0.0.1	10.0.0.242	UDP	Source port: 18302 Destination port: complex-link
5572	94.069636	10.0.0.1	10.0.0.242	UDP	Source port: 18302 Destination port: complex-link
5577	94.081358	10.0.0.1	10.0.0.242	UDP	Source port: 18302 Destination port: complex-link

Frame 5571 (1512 bytes on wire, 1512 bytes captured)

- Ethernet II, Src: EdimaxTe_01:81:ef (00:0e:2e:01:81:ef), Dst: IntelCor_bc:78:ad (00:1c:bf:bc:78:ad)
- Internet Protocol, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.0.242 (10.0.0.242)
 - Version: 4
 - Header length: 20 bytes
 - Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
 - Total Length: 1498
 - Identification: 0x3282 (12930)
 - Flags: 0x00
 - Fragment offset: 0
 - Time to live: 64
 - Protocol: UDP (0x11)
 - Header checksum: 0x2d9f [correct]
 - Source: 10.0.0.1 (10.0.0.1)
 - Destination: 10.0.0.242 (10.0.0.242)
- User Datagram Protocol, Src Port: 18302 (18302), Dst Port: complex-link (5001)
 - Source port: 18302 (18302)
 - Destination port: complex-link (5001)
 - Length: 1478
 - Checksum: 0x1344 [validation disabled]
- Data (1470 bytes)

0000 00 1c bf bc 78 ad 00 0e 2e 01 81 ef 08 00 45 00E.
0010 05 da 32 82 00 00 40 11 2d 9f 0a 00 00 01 0a 00 ..2...@. -.....
0020 00 f2 47 7e 13 89 05 c6 13 44 00 00 14 e5 4b a3 ..G~.... .D...K.
0030 5e a1 00 05 76 c1 00 00 00 00 00 00 01 00 00 ^...v...

Frame (frame), 1512 bytes | Packets: 5591 Displayed: 5353 Marked: 0 Dropped: 0 | Profile: Default



ΒΙΒΛΙΟΓΡΑΦΙΑ

- "Δίκτυα Υπολογιστών", A.S. Tanenbaum, Εκδόσεις Παπασωτηρίου, 3η έκδοση.
- *The TCP/IP GUIDE* © 2003-2005 Charles M. Kozierek. All Rights Reserved.
<http://www.tcpiptide.com/free/index.htm>
- *RFCs*
 - <http://www.ietf.org/rfc.html>

