ΤΕΙ ΑΝΑΤΟΛΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ ΚΑΙ ΘΡΑΚΗΣ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΙΚΤΥΑ ΙΙ

ΚΩΝ/ΝΟΣ ΡΑΝΤΟΣ
krantos@teikav.edu.gr

Θεματικές ενότητες

- Εισαγωγή στο TCP/IP
- IP διευθυνσιοδότηση.
- Πρωτόκολλο IP
- Υποδίκτυα
- Δρομολόγηση (Γενικά και IP), Αλγόριθμοι δρομολόγησης.
- Πρωτόκολλα TCP/UDP
- Διευθυνσιοδότηση (IPv4, IPv6)
- Πρωτόκολλα του TCP/IP (ICMP, ARP, RARP)

ΔΙΚΤΥΑ ΙΙ

Εισαγωγή στο TCP/IP

Η δημιουργία του Internet

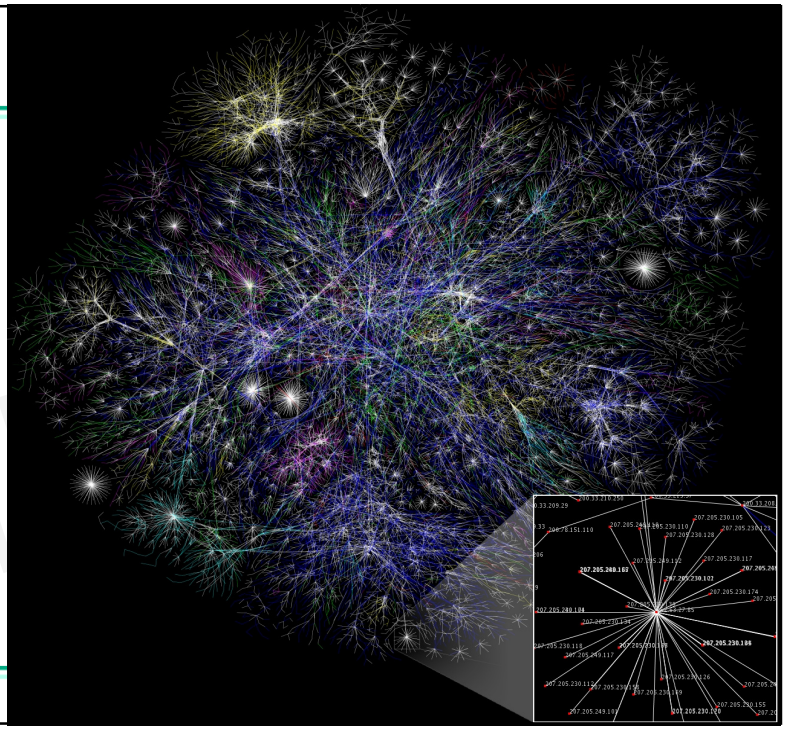
- Ξεκίνησε ως πειραματικό δίκτυο για στρατιωτικούς σκοπούς και τη σύνδεση των πανεπιστημίων για ερευνητικούς σκοπούς.
- Έτσι δημιουργήθηκε ένα πρότυπο δίκτυο μεταγωγής πακέτων
- Αρχικά ονομάστηκε ARPANET από τον φορέα που το δημιούργησε και ο οποίος ήταν το ARPA (Advanced Research Projects Agency) που ήταν ο πρόγονος του DARPA (Defense Advanced Research Projects Agency).
- ARPA: στρατιωτική υπηρεσία υπεύθυνη για τη χρηματοδότηση πανεπιστημίων και ερευνητικών κέντρων για στρατιωτικούς σκοπούς.

Η δημιουργία του Internet

- Δεν υπάρχει ένα μοναδικό δίκτυο που να ονομάζεται Internet.
  - Ο όρος αναφέρεται περισσότερο σε ένα σύνολο υποδικτύων συνδεδεμένα μεταξύ τους.
  - Όλα χρησιμοποιούν το TCP/IP πρωτόκολλο.
- Σήμερα υπάρχουν περίπου 2 δις χρήστες του διαδικτύου (με συνολικό πληθυσμό 6,8 δις)
  - Το 2000 οι χρήστες ήταν μόλις 361.000.
- Ρυθμός αύξησης των χρηστών 2000-2010: 444%
- Στη χώρα μας υπάρχουν περίπου 5 εκ. χρήστες με πληθυσμό σχεδόν 11 εκ.

Αναπαράσταση των μονοπατιών του διαδικτύου

Πηγή: The opte Project



Πρότυπα στο Internet

- Η χρήση προτύπων είναι επιτακτική για την ορθή και εύρυθμη λειτουργία του διαδικτύου καθώς εξασφαλίζει την απαραίτητη διαλειτουργικότητα μεταξύ των δικτυακών συστημάτων σε επίπεδο διακίνησης δεδομένων.
  - Θα υπήρχε το Internet αν δεν υπήρχαν τα πρότυπα;

    ή
  - Θα μπορούσαμε να έχουμε έναν αγώνα ποδοσφαίρου χωρίς κανόνες;

Πρότυπα στο Internet

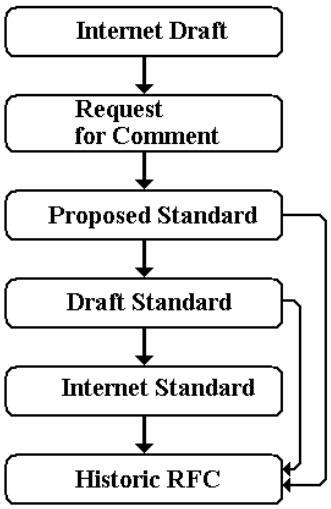
- Η οργάνωση και η χρήση νέων προτύπων για το Internet ελέγχεται από το Internet Architecture Board (IAB).
- Το IAB είναι ένας οργανισμός που συντονίζει άλλες ομάδες έργου (task forces) μεταξύ των οποίων είναι και το Internet Engineering Task Force (IETF).
- Το IETF ελέγχει τη δημιουργία νέων προτύπων και την υιοθεσία νέων τεχνολογιών μέσα από έναν αριθμό ομάδων εργασίας, κάθε μία εκ των οποίων ασχολείται με ένα συγκεκριμένο τομέα των τεχνολογιών που χρησιμοποιούνται στο Internet.

Πρότυπα στο Internet

- Η δημιουργία ενός νέου προτύπου απαιτεί την ακολουθία μιας συγκεκριμένης διαδικασίας.

  http://www.ietf.org/rfc.html

- Το RFC 5000 περιλαμβάνει την τρέχουσα λίστα από πρότυπα του Internet και RFCs



Δικτυακές συσκευές

- Οι συσκευές που μας επιτρέπουν τη δημιουργία δικτύων και την πρόσβαση στο δίκτυο είναι:
  - Hubs
  - Switches
  - Bridges
  - Routers
  - Gateways

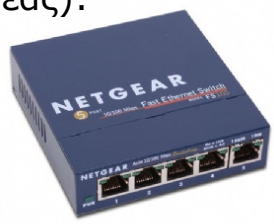
Δικτυακές συσκευές

- Hub (Ομφαλός):

  - συσκευή πολλών θυρών η οποία συνδέει δικτυακές συσκευές μεταξύ τους.
    - Έχει το χαρακτηριστικό ότι τα δεδομένα που φθάνουν σε μια από τις θύρες προωθούνται προς όλες τις άλλες θύρες (δηλαδή το hub δε κάνει κανέναν έλεγχο διευθύνσεων).
    - Χρησιμοποιείται σε τοπικό επίπεδο για πολύ μικρά δίκτυα

Δικτυακές συσκευές

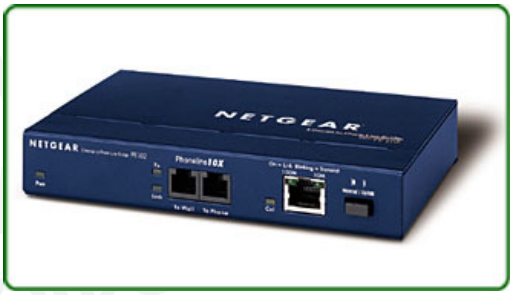
- Switch (Μεταγωγέας):



  - συσκευή πολλών θυρών η οποία συνδέει άλλες δικτυακές συσκευές (συμπεριλαμβανομένων άλλων switches και hubs) μεταξύ τους.
    - στέλνουν τα δεδομένα μόνο στη γραμμή στην οποία είναι συνδεδεμένος ο προορισμός μειώνοντας έτσι την κίνηση
    - χρησιμοποιεί MAC διευθύνσεις

Δικτυακές συσκευές

- Bridge (Γέφυρα):



  - συνδέει διαφορετικά τμήματα δικτύου ή διαφορετικές τεχνολογίες δημιουργώντας ένα μεγαλύτερο δίκτυο ενώ ελέγχει παράλληλα την κίνηση μεταξύ τους.

Δικτυακές συσκευές

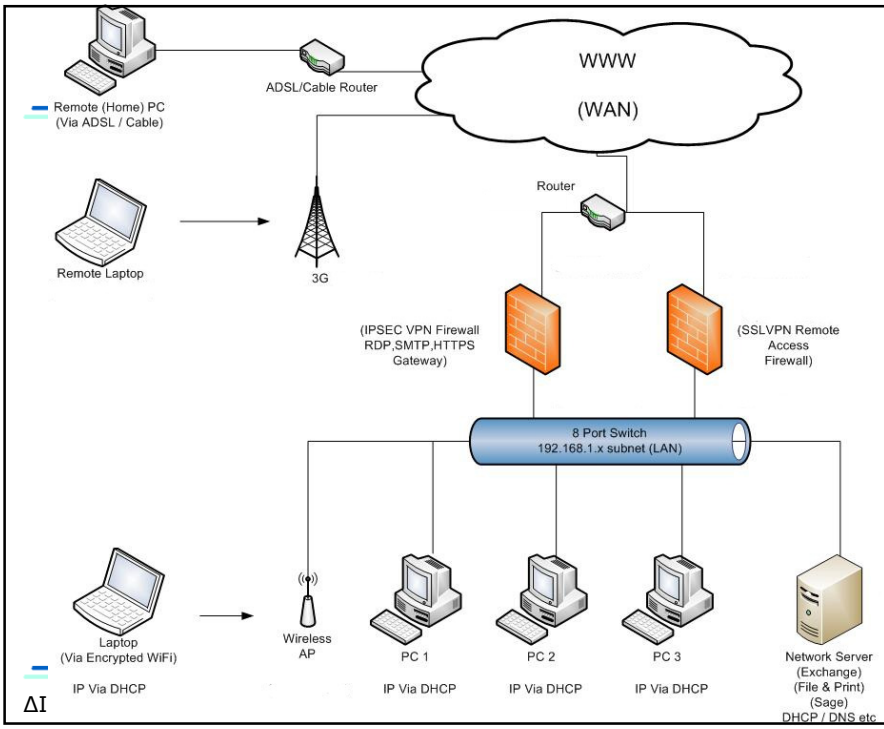
- Router (Δρομολογητής):

  - οριοθετεί και συνδέει δίκτυα μεταξύ τους και δρομολογεί πακέτα βρίσκοντας το μονοπάτι που οδηγεί στον προορισμό.
    - Η δρομολόγηση γίνεται βάσει πινάκων ή αλγορίθμων δρομολόγησης.

Δικτυακές συσκευές

- Gateway (Πύλη):

  - ενώνει δύο διαφορετικά δίκτυα μεταξύ τους επιτρέποντας έτσι τη χρήση διαφορετικών τεχνολογιών (πρωτοκόλλων).
  - μπορεί να έχει και τη μορφή λογισμικού
  - π.χ. Residential gateway



Εισαγωγή στο TCP/IP

- Πρόκειται για το σύνολο των πρωτοκόλλων που χρησιμοποιούνται στο Internet
- Αποτελεί το **de facto πρότυπο** για τα περισσότερα δίκτυα.
- Το όνομα του προέρχεται από τα:
  - **TCP** (Transmission Control Protocol): ένα από τα πρωτόκολλα του επιπέδου μεταφοράς του TCP/IP και
  - **IP** (Internet Protocol): το πρωτόκολλο του Internet επιπέδου του TCP/IP.
- Δε συγκρούεται με το OSI μοντέλο αφού τα δύο αναπτύχθηκαν παράλληλα. Αντιθέτως το TCP/IP συνεισέφερε στη δημιουργία του OSI και αντίστροφα.

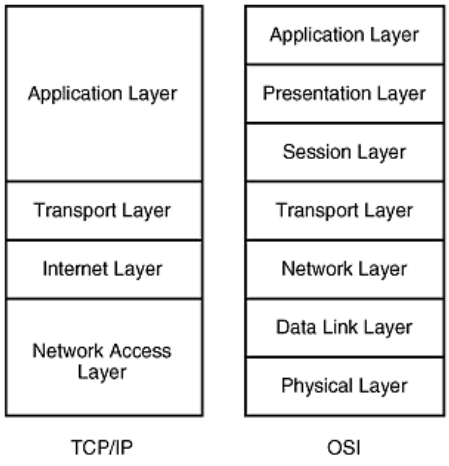
Το μοντέλο αναφοράς TCP/IP

- Αποτελείται από 4 στρώματα:
  - **Εφαρμογής (Application)**: Μήνυμα ή Ακολουθία Bytes, Message ή Stream
  - **Μεταφοράς (Transport)**: Πακέτο
  - **Διαδικτύου (Internet)**: Δεδομενογράφημα
  - **Πρόσβασης στο δίκτυο (Network Access Layer)**: Πλαίσιο

OSI

- Στρώματα OSI:
  - Εφαρμογής (Application): Η επικοινωνία με το χρήστη – όλες οι δικτυακές εφαρμογές.
  - Παρουσίασης (Presentation): Μετατρέπει τα δικτυακά δεδομένα σε συγκεκριμένο φορμά ανάλογα με την εφαρμογή.
  - Συνόδου (Session): Δημιουργεί συνδέσεις μεταξύ δικτυακών συσκευών και συγχρονίζει την ανταλλαγή των δεδομένων μεταξύ ανώτερων και κατώτερων επιπέδων.
  - Μεταφοράς (Transport): Μετάδοση από άκρη σε άκρη, ακεραιότητα δεδομένων, πολυπλεξία, και έλεγχος ροής.
  - Δικτύου (Network): Υπηρεσίες διαδικτύωσης, δρομολόγηση, διευθυνσιοδότηση.
  - Ζεύξης Δεδομένων (Data Link): Ορίζει τον τρόπο με τον οποίο γίνεται η προσπέλαση του δικτύου, διορθώνει λάθη μετάδοσης δεδομένων.
  - Φυσικό (Physical): Μεταφέρει δεδομένα

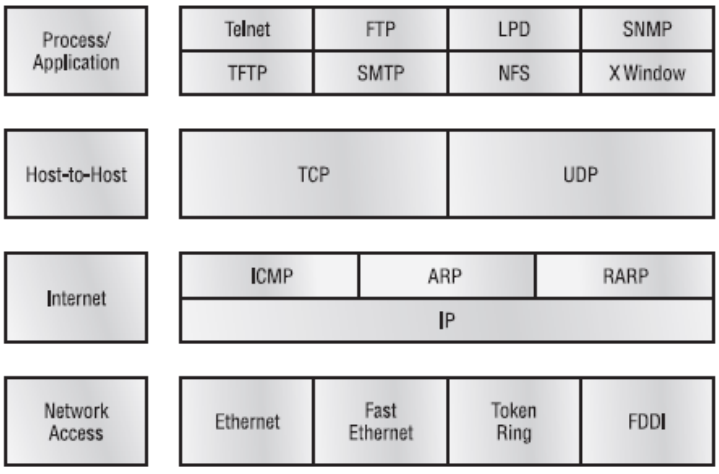
Αντιστοιχία μεταξύ OSI και TCP/IP



TCP/IP σε σύγκριση με το OSI

- Παρόλο που δεν είναι ένα επισήμως διεθνώς αναγνωρισμένο πρότυπο:
  - Έχει δοκιμαστεί και είναι πολύ αποδοτικό.
  - Έχει ένα άρτια οργανωμένο τμήμα διαχείρισης που το υποστηρίζει.
  - Το χρησιμοποιούν πολλές εφαρμογές.
- Παρουσιάζει όμως τα εξής μειονεκτήματα:
  - Το μοντέλο δεν είναι γενικό και επομένως δε μπορεί να χρησιμοποιηθεί για να περιγράψει άλλα πρωτόκολλα (π.χ. Bluetooth).
  - Ο αριθμός των στρωμάτων διαφέρει στη βιβλιογραφία.

Πρωτόκολλα του TCP/IP

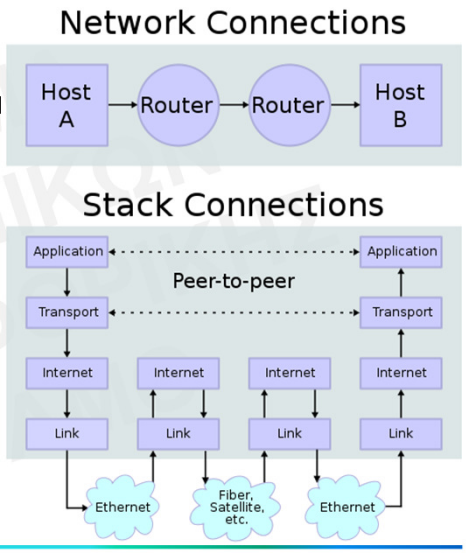


Στρώματα TCP/IP: εφαρμογής

- Περιλαμβάνει όλες τις γνωστές εφαρμογές που χρησιμοποιούνται ευρέως:
  - Μεταφοράς ιστοσελίδων (HTTP)
  - Απομακρυσμένο τερματικό (Telnet)
  - Μεταφοράς αρχείων (FTP)
  - Ηλεκτρονικό ταχυδρομείο (SMTP, IMAP, POP)
  - Μεταφοράς νέων (NNTP)
  - Υπηρεσίες ευρετηρίου (LDAP)

Στρώματα TCP/IP: εφαρμογής

- Αλληλεπιδρά με το επίπεδο μεταφοράς για να στείλει ή να παραλάβει δεδομένα.
- Κάθε εφαρμογή επιλέγει τον τρόπο με τον οποίο θα μεταφερθούν τα δεδομένα και προετοιμάζει τα δεδομένα ανάλογα για να τα προωθήσει προς το επόμενο επίπεδο.
- Η αντίστροφη διαδικασία λαμβάνει χώρα κατά την παραλαβή δεδομένων.



Στρώμα Μεταφοράς

- Εξασφαλίζει την επικοινωνία μεταξύ δύο εφαρμογών.
- Καθορίζει τη ροή των πληροφοριών.
- Χωρίζει τα δεδομένα σε μικρότερα κομμάτια (πακέτα) και προωθεί το κάθε πακέτο μαζί με μια διεύθυνση προορισμού στο επόμενο στρώμα.
- Μπορεί να δεχτεί ταυτόχρονα δεδομένα από πολλές εφαρμογές τα οποία πρέπει να προωθήσει στο επόμενο στρώμα. Για αυτό το λόγο προσθέτει πληροφορίες στο πακέτο για την εφαρμογή στην οποία ανήκουν τα δεδομένα, καθώς και ένα άθροισμα ελέγχου που χρησιμοποιείται για τον έλεγχο της ακεραιότητας του πακέτου.

Στρώμα Μεταφοράς

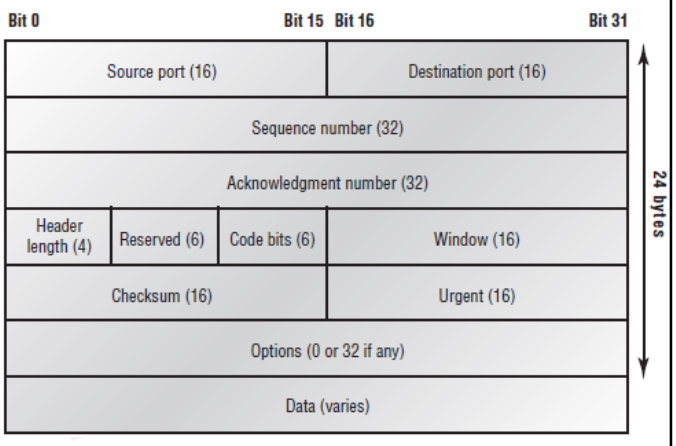
- Δύο πρωτόκολλα:
  - Πρωτόκολλο ελέγχου μετάδοσης TCP (Transmission Control Protocol):
    - Είναι ένα **αξιόπιστο και με σύνδεση** πρωτόκολλο: διαβεβαιώνει ότι τα πακέτα παραλαμβάνονται από τον παραλήπτη. Εάν κάποιο πακέτο χαθεί κατά τη διάρκεια της μετάδοσης του το TCP έχει τη δυνατότητα να τα ξαναστείλει.
    - **Τεμαχίζει τα δεδομένα** σε πακέτα τα οποία επανασυνδέονται στον παραλήπτη.
    - Χειρίζεται επίσης τον **έλεγχο ροής** των δεδομένων, την **ακολουθία των μηνυμάτων** (έτσι ώστε να υπάρχει σιγουριά ότι όλα τα πακέτα έχουν παραληφθεί)
    - Φροντίζει για την **ανεύρεση και διόρθωση λαθών**.

Στρώμα Μεταφοράς

- TCP (Transmission Control Protocol):
  - Με σύνδεση: Χρήση ενός είδους χειραψίας μεταξύ των δύο συστημάτων πριν την αποστολή δεδομένων.
  - Μετά τη χειραψία δημιουργείται μια εικονική σύνδεση που επιτρέπει την περαιτέρω αποστολή δεδομένων.
  - Λόγω των χαρακτηριστικών του χρησιμοποιείται από εφαρμογές όπου επιβάλλεται η αξιοπιστία. Π.χ. Email, FTP.

Στρώμα Μεταφοράς

- TCP πακέτο:
  - Θύρα αφετηρίας (16bit)
  - Θύρα προορισμού (16bit)
  - Αύξων αριθμός
  - Αριθμός επαλήθευσης
  - Κάποια άλλα πεδία (άλλα προαιρετικά και άλλα υποχρεωτικά)
  - Δεδομένα

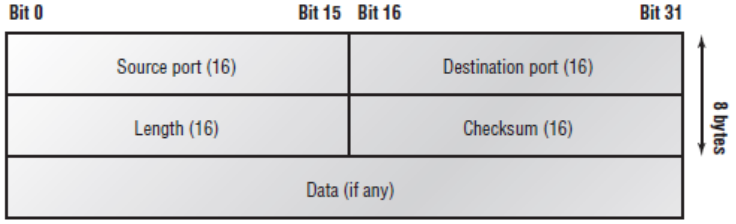


Στρώμα Μεταφοράς

- UDP (User Datagram Protocol):
  - Είναι ένα **μη αξιόπιστο, χωρίς σύνδεση** πρωτόκολλο. Δεν υπάρχει έλεγχος ροής και συμφόρησης όπως στο TCP, αρίθμηση των πακέτων και ο παραλήπτης δεν επαληθεύει την παραλαβή κάθε πακέτου.
  - Το μέγεθος του datagram μπορεί να φθάσει εως 64kbytes αλλά στην πράξη περιορίζονται στα 1500bytes.

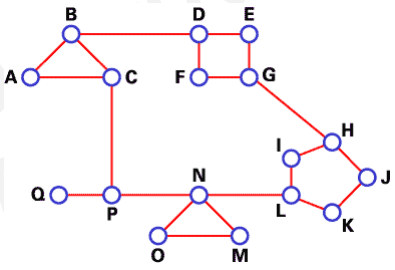
Στρώμα Μεταφοράς

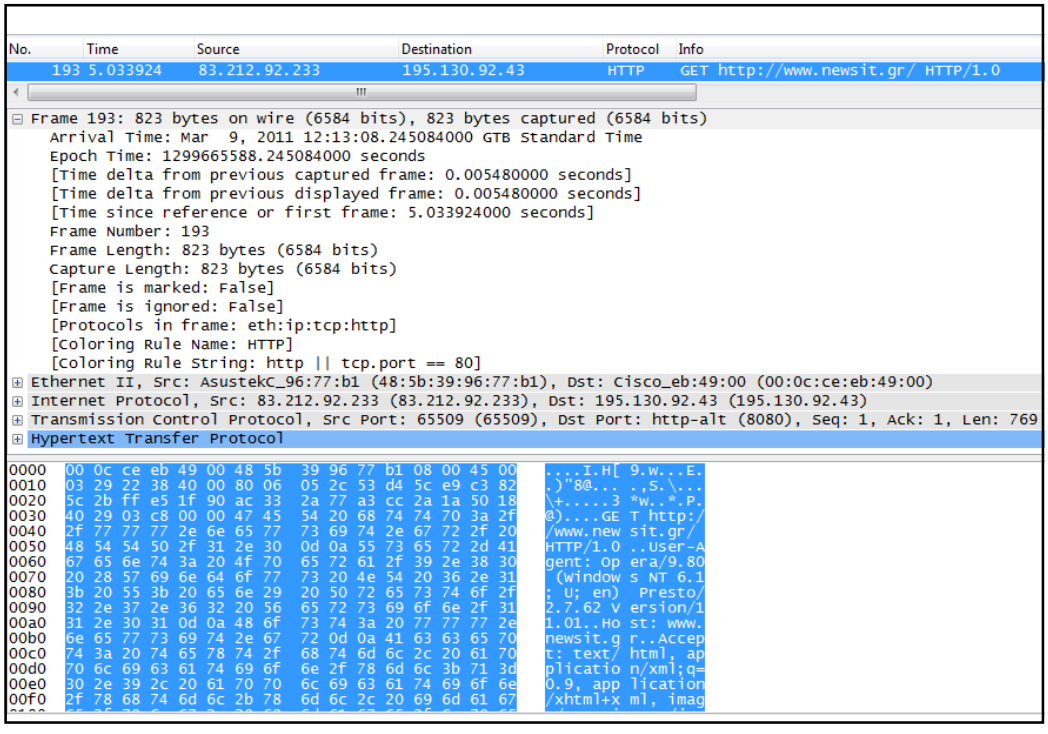
- UDP (User Datagram Protocol):
  - Χρησιμοποιείται κυρίως από εφαρμογές που τους ενδιαφέρει περισσότερο η ταχύτητα μετάδοσης παρά η αξιοπιστία, π.χ. Streaming Video (μετάδοση εικόνας), ήχος.
  - Αποτελείται από: Θύρα αφετηρίας (16bits), Θύρα προορισμού (16bits), Μήκος (16bits), Άθροισμα ελέγχου (16bits), Δεδομένα

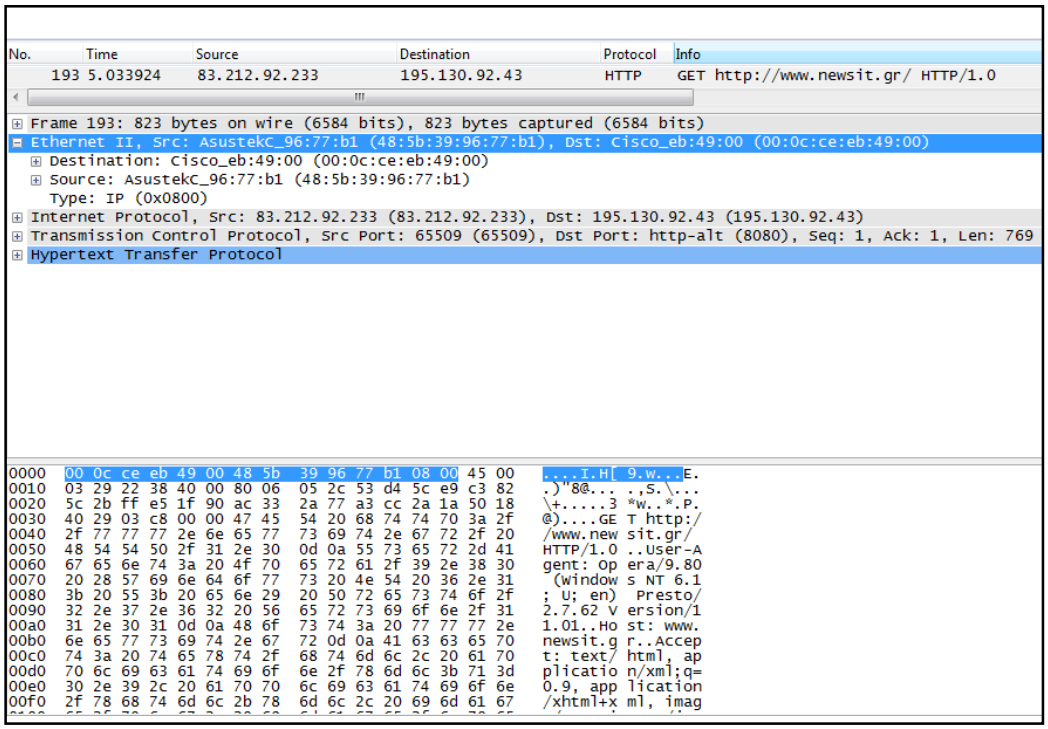


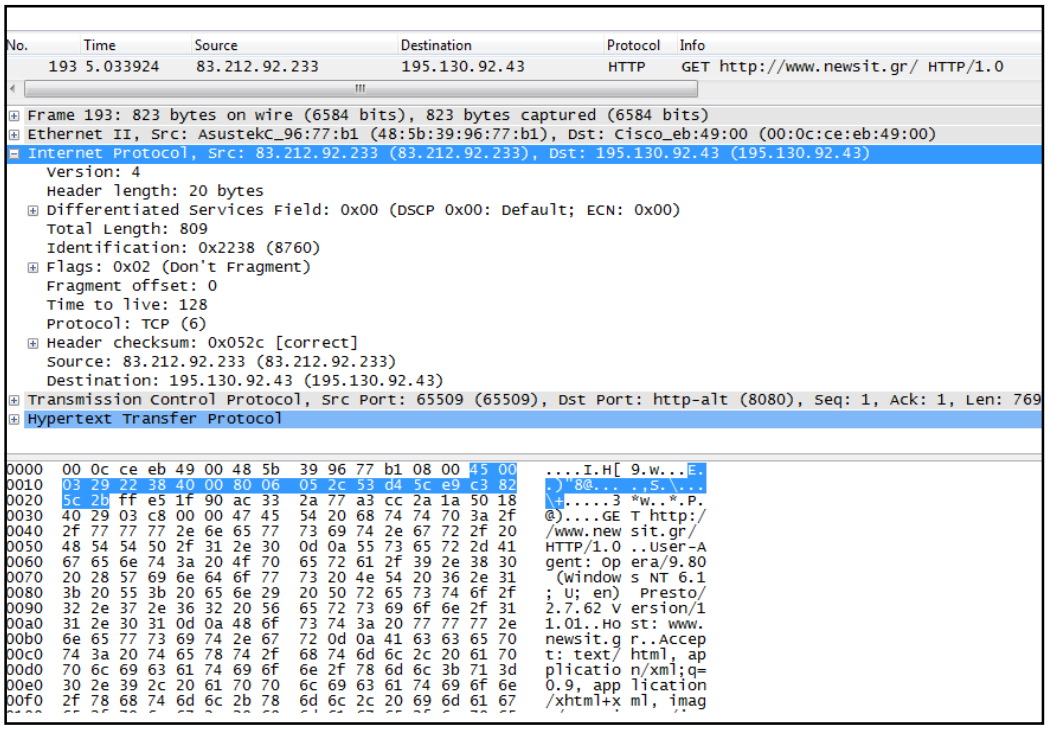
Στρώμα Διαδικτύου

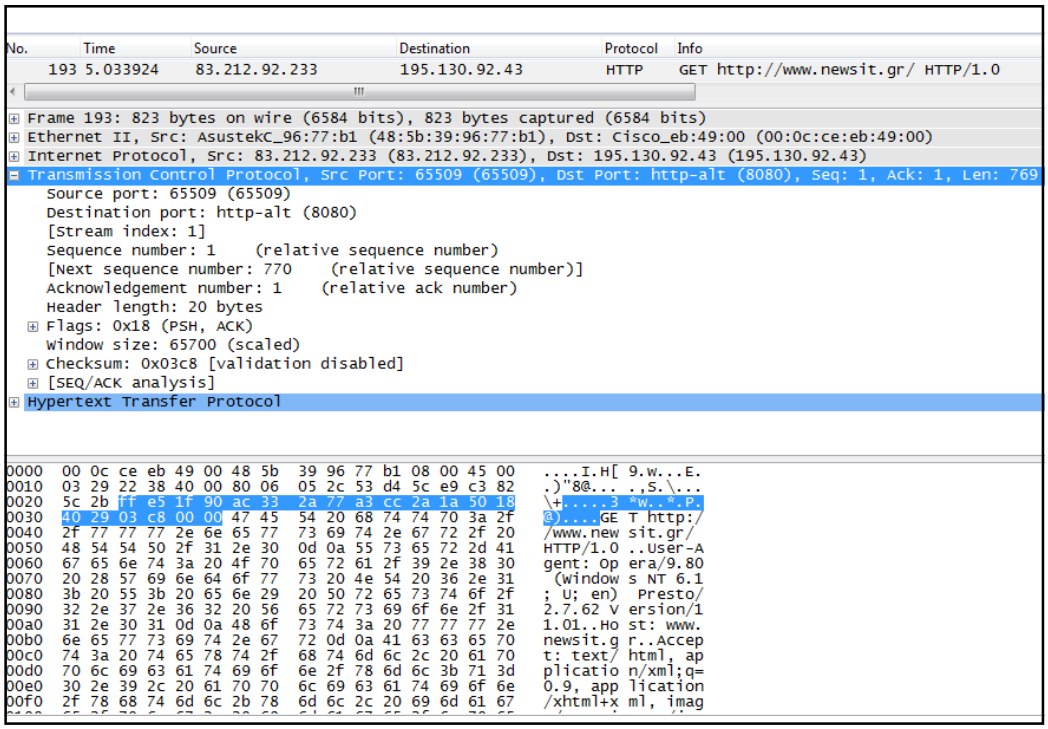
- Χρησιμοποιείται για τη **δρομολόγηση των πακέτων** τα οποία μπορεί να φθάσουν με οποιαδήποτε σειρά. Είναι δουλειά των ανώτερων στρωμάτων να τα βάλουν στη σωστή σειρά εάν αυτό απαιτείται όταν αυτά φθάσουν στον προορισμό τους.
- Χρησιμοποιεί **τεχνικές μεταγωγής πακέτων** για τη μεταφορά των δεδομένων όπου φυσικά δε χρειάζεται δημιουργία σύνδεσης για τη μεταφορά των πακέτων αλλά κάθε πακέτο δρομολογείται ξεχωριστά και μπορεί να ακολουθήσει διαφορετική διαδρομή.

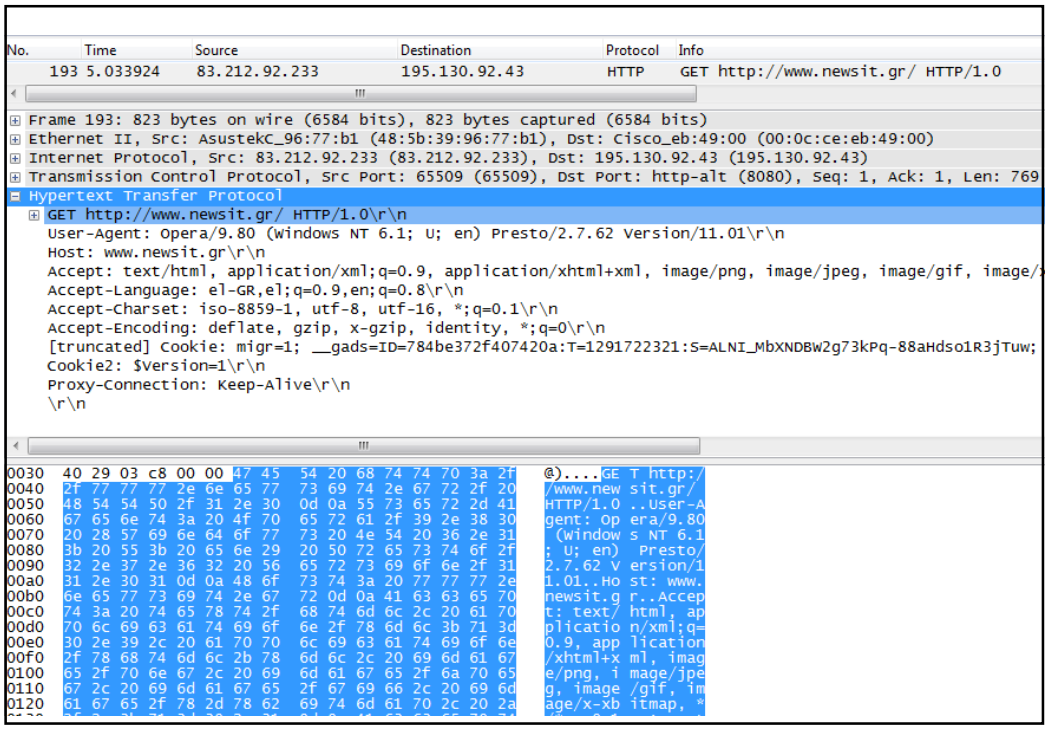





No. Time Source Destination Protocol Info
193 5.033924 83.212.92.233 195.130.92.43 HTTP GET http://www.newsit.gr/ HTTP/1.0
Frame 193: 823 bytes on wire (6584 bits), 823 bytes captured (6584 bits)
Ethernet II, Src: AsustekC_96:77:b1 (48:5b:39:96:77:b1), Dst: Cisco_eb:49:00 (00:0c:ce:eb:49:00)
Destination: Cisco_eb:49:00 (00:0c:ce:eb:49:00)
Source: AsustekC_96:77:b1 (48:5b:39:96:77:b1)
Type: IP (0x0800)
Internet Protocol, Src: 83.212.92.233 (83.212.92.233), Dst: 195.130.92.43 (195.130.92.43)
Transmission Control Protocol, Src Port: 65509 (65509), Dst Port: http-alt (8080), Seq: 1, Ack: 1, Len: 769
Hypertext Transfer Protocol
0000 00 0c ce eb 49 00 48 5b 39 96 77 b1 08 00 45 00 ....I.H[9.w...E.
0010 03 29 22 38 40 00 80 06 05 2c 53 d4 5c e9 c3 82 .)"8@... .,S.\...
0020 5c 2b ff e5 1f 90 ac 33 2a 77 a3 cc 2a 1a 50 18 \+.....3 *w..*.P.
0030 40 29 03 c8 00 00 47 45 54 20 68 74 74 70 3a 2f @)....GE T http:/
0040 2f 77 77 77 2e 6e 65 77 73 69 74 2e 67 72 2f 20 /www.new sit.gr/
0050 48 54 54 50 2f 31 2e 30 0d 0a 55 73 65 72 2d 41 HTTP/1.0 ..User-A
0060 67 65 6e 74 3a 20 4f 70 65 72 61 2f 39 2e 38 30 gent: Op era/9.80
0070 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 36 2e 31 (Window s NT 6.1
0080 3b 20 55 3b 20 65 6e 29 20 50 72 65 73 74 6f 2f ; U; en) Presto/
0090 32 2e 37 2e 36 32 20 56 65 72 73 69 6f 6e 2f 31 2.7.62 V ersion/1
00a0 31 2e 30 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 1.01..Ho st: www.
00b0 6e 65 77 73 69 74 2e 67 72 0d 0a 41 63 63 65 70 newsit.g r..Accep
00c0 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 20 61 70 t: text/ html, ap
00d0 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d plicatio n/xml;q=
00e0 30 2e 39 2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 0.9, app lication
00f0 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 20 69 6d 61 67 /xhtml+x ml, imag

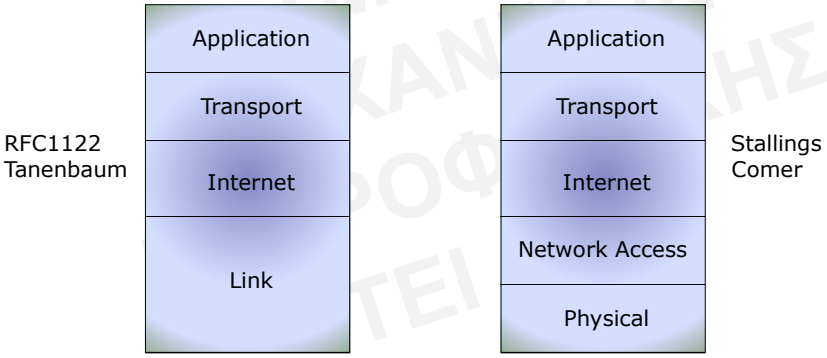

No. Time Source Destination Protocol Info
193 5.033924 83.212.92.233 195.130.92.43 HTTP GET http://www.newsit.gr/ HTTP/1.0
Frame 193: 823 bytes on wire (6584 bits), 823 bytes captured (6584 bits)
Ethernet II, Src: AsustekC_96:77:b1 (48:5b:39:96:77:b1), Dst: Cisco_eb:49:00 (00:0c:ce:eb:49:00)
Internet Protocol, Src: 83.212.92.233 (83.212.92.233), Dst: 195.130.92.43 (195.130.92.43)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
Total Length: 809
Identification: 0x2238 (8760)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x052c [correct]
Source: 83.212.92.233 (83.212.92.233)
Destination: 195.130.92.43 (195.130.92.43)
Transmission Control Protocol, Src Port: 65509 (65509), Dst Port: http-alt (8080), Seq: 1, Ack: 1, Len: 769
Hypertext Transfer Protocol
0000 00 0c ce eb 49 00 48 5b 39 96 77 b1 08 00 45 00 ....I.H[9.w...E.
0010 03 29 22 38 40 00 80 06 05 2c 53 d4 5c e9 c3 82 .)"8@... .,S.\...
0020 5c 2b ff e5 1f 90 ac 33 2a 77 a3 cc 2a 1a 50 18 \+.....3 *w..*.P.
0030 40 29 03 c8 00 00 47 45 54 20 68 74 74 70 3a 2f @)....GE T http:/
0040 2f 77 77 77 2e 6e 65 77 73 69 74 2e 67 72 2f 20 /www.new sit.gr/
0050 48 54 54 50 2f 31 2e 30 0d 0a 55 73 65 72 2d 41 HTTP/1.0 ..User-A
0060 67 65 6e 74 3a 20 4f 70 65 72 61 2f 39 2e 38 30 gent: Op era/9.80
0070 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 36 2e 31 (Window s NT 6.1
0080 3b 20 55 3b 20 65 6e 29 20 50 72 65 73 74 6f 2f ; U; en) Presto/
0090 32 2e 37 2e 36 32 20 56 65 72 73 69 6f 6e 2f 31 2.7.62 V ersion/1
00a0 31 2e 30 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 1.01..Ho st: www.
00b0 6e 65 77 73 69 74 2e 67 72 0d 0a 41 63 63 65 70 newsit.g r..Accep
00c0 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 20 61 70 t: text/ html, ap
00d0 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d plicatio n/xml;q=
00e0 30 2e 39 2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 0.9, app lication
00f0 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 20 69 6d 61 67 /xhtml+x ml, imag


No. Time Source Destination Protocol Info
193 5.033924 83.212.92.233 195.130.92.43 HTTP GET http://www.newsit.gr/ HTTP/1.0
Frame 193: 823 bytes on wire (6584 bits), 823 bytes captured (6584 bits)
Ethernet II, Src: AsustekC_96:77:b1 (48:5b:39:96:77:b1), Dst: Cisco_eb:49:00 (00:0c:ce:eb:49:00)
Internet Protocol, Src: 83.212.92.233 (83.212.92.233), Dst: 195.130.92.43 (195.130.92.43)
Transmission Control Protocol, Src Port: 65509 (65509), Dst Port: http-alt (8080), Seq: 1, Ack: 1, Len: 769
Source port: 65509 (65509)
Destination port: http-alt (8080)
[Stream index: 1]
Sequence number: 1 (relative sequence number)
[Next sequence number: 770 (relative sequence number)]
Acknowledgement number: 1 (relative ack number)
Header length: 20 bytes
Flags: 0x18 (PSH, ACK)
Window size: 65700 (scaled)
Checksum: 0x03c8 [validation disabled]
[SEQ/ACK analysis]
Hypertext Transfer Protocol
0000 00 0c ce eb 49 00 48 5b 39 96 77 b1 08 00 45 00 ....I.H[9.w...E.
0010 03 29 22 38 40 00 80 06 05 2c 53 d4 5c e9 c3 82 .)"8@... .,S.\...
0020 5c 2b ff e5 1f 90 ac 33 2a 77 a3 cc 2a 1a 50 18 \+.....3 *w..*.P.
0030 40 29 03 c8 00 00 47 45 54 20 68 74 74 70 3a 2f @)....GE T http:/
0040 2f 77 77 77 2e 6e 65 77 73 69 74 2e 67 72 2f 20 /www.new sit.gr/
0050 48 54 54 50 2f 31 2e 30 0d 0a 55 73 65 72 2d 41 HTTP/1.0 ..User-A
0060 67 65 6e 74 3a 20 4f 70 65 72 61 2f 39 2e 38 30 gent: Op era/9.80
0070 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 36 2e 31 (window s NT 6.1
0080 3b 20 55 3b 20 65 6e 29 20 50 72 65 73 74 6f 2f ; U; en) Presto/
0090 32 2e 37 2e 36 32 20 56 65 72 73 69 6f 6e 2f 31 2.7.62 V ersion/1
00a0 31 2e 30 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 1.01..Ho st: www.
00b0 6e 65 77 73 69 74 2e 67 72 0d 0a 41 63 63 65 70 newsit.g r..Accep
00c0 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 20 61 70 t: text/ html, ap
00d0 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d plicatio n/xml;q=
00e0 30 2e 39 2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 0.9, app lication
00f0 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 20 69 6d 61 67 /xhtml+x ml, imag


No. Time Source Destination Protocol Info
193 5.033924 83.212.92.233 195.130.92.43 HTTP GET http://www.newsit.gr/ HTTP/1.0
Frame 193: 823 bytes on wire (6584 bits), 823 bytes captured (6584 bits)
Ethernet II, Src: AsustekC_96:77:b1 (48:5b:39:96:77:b1), Dst: Cisco_eb:49:00 (00:0c:ce:eb:49:00)
Internet Protocol, Src: 83.212.92.233 (83.212.92.233), Dst: 195.130.92.43 (195.130.92.43)
Transmission Control Protocol, Src Port: 65509 (65509), Dst Port: http-alt (8080), Seq: 1, Ack: 1, Len: 769
Hypertext Transfer Protocol
GET http://www.newsit.gr/ HTTP/1.0\r\n
User-Agent: Opera/9.80 (Windows NT 6.1; U; en) Presto/2.7.62 Version/11.01\r\n
Host: www.newsit.gr\r\n
Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/
Accept-Language: el-GR,el;q=0.9,en;q=0.8\r\n
Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1\r\n
Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0\r\n
[truncated] Cookie: migr=1; __gads=ID=784be372f407420a:T=1291722321:S=ALNI_MbXNDBW2g73kPq-88aHdso1R3jTuw;
Cookie2: $Version=1\r\n
Proxy-Connection: Keep-Alive\r\n
\r\n
0030 40 29 03 c8 00 00 47 45 54 20 68 74 74 70 3a 2f @)....GE T http:/
0040 2f 77 77 77 2e 6e 65 77 73 69 74 2e 67 72 2f 20 /www.new sit.gr/
0050 48 54 54 50 2f 31 2e 30 0d 0a 55 73 65 72 2d 41 HTTP/1.0 ..User-A
0060 67 65 6e 74 3a 20 4f 70 65 72 61 2f 39 2e 38 30 gent: Op era/9.80
0070 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 36 2e 31 (window s NT 6.1
0080 3b 20 55 3b 20 65 6e 29 20 50 72 65 73 74 6f 2f ; U; en) Presto/
0090 32 2e 37 2e 36 32 20 56 65 72 73 69 6f 6e 2f 31 2.7.62 V ersion/1
00a0 31 2e 30 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 1.01..Ho st: www.
00b0 6e 65 77 73 69 74 2e 67 72 0d 0a 41 63 63 65 70 newsit.g r..Accep
00c0 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 20 61 70 t: text/ html, ap
00d0 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d plicatio n/xml;q=
00e0 30 2e 39 2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 0.9, app lication
00f0 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 20 69 6d 61 67 /xhtml+x ml, imag
0100 65 2f 70 6e 67 2c 20 69 6d 61 67 65 2f 6a 70 65 e/png, i mage/jpe
0110 67 2c 20 69 6d 61 67 65 2f 67 69 66 2c 20 69 6d g, image /gif, im
0120 61 67 65 2f 78 2d 78 62 69 74 6d 61 70 2c 20 2a age/x-xb itmap, *

Στρώμα Πρόσβασης στο δίκτυο

- Είναι το στρώμα που έχει προκαλέσει πολλές αντιδράσεις αναφορικά με τον αριθμό των υποστρωμάτων από τα οποία αποτελείται.



ΔΙΚΤΥΑ ΙΙ

IP διευθυνσιοδότηση

Το σύστημα διευθυνσιοδότησης IP

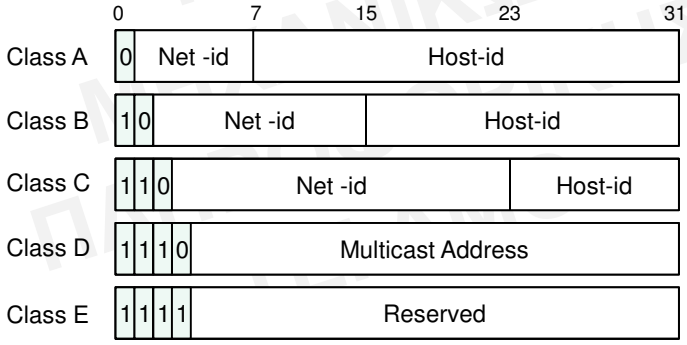
- Απαραίτητο στοιχείο για τη δρομολόγηση σε ένα δίκτυο αποτελεί η ύπαρξη διευθύνσεων οι οποίες θα ορίζουν μοναδικά κάποιο σταθμό.
- Οι MAC διευθύνσεις είναι μοναδικές στον κόσμο αλλά
  - Δεν έχουν συγκεκριμένη δομή,
  - Δε δίνουν πληροφορίες στα πρωτόκολλα δρομολόγησης.
- Για αυτό το λόγο το TCP/IP χρησιμοποιεί IP διευθύνσεις οι οποίες είναι **ιεραρχημένες**.
- Κάθε δικτυακή συσκευή έχει μια IP διεύθυνση η οποία αποτελείται από 32bits για το IPv4 (128bits για το IPv6).

Το σύστημα διευθυνσιοδότησης IPv4

- 3 κλάσεις: δεδομένης κάποιας IP διεύθυνσης, η κλάση της μπορεί να καθοριστεί από τα 3 πρώτα bits.
- Η αναπαράσταση είναι της μορφής x.x.x.x (x=byte)
- Τρεις κλάσεις:
  - Class A: **Το πρώτο bit έχει την τιμή: 0** (1.0.0.0 εως 127.255.255.255)
  - Class B: **Τα δύο πρώτα bits έχουν την τιμή: 10** (128.0.0.0 εως 191.255.255.255)
  - Class C: **Τα τρία πρώτα bits έχουν την τιμή: 110** (192.0.0.0 εως 223.255.255.255)
  - Class D: Χρησιμοποιείται για multicasting (1110)
  - Class E: Δεσμευμένες για μελλοντική χρήση (1111)

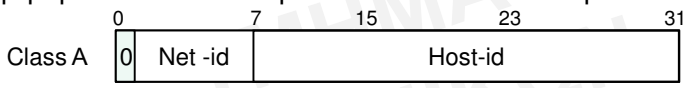
Το σύστημα διευθυνσιοδότησης IPv4

- Οι διευθύνσεις αποτελούνται από
  - ένα τμήμα δικτύου το οποίο αναγνωρίζει το δίκτυο στο οποίο είναι συνδεδεμένος ο σταθμός
  - ένα τμήμα σταθμού (host) το οποίο αναγνωρίζει μοναδικά τον κάθε σταθμό στο συγκεκριμένο δίκτυο.

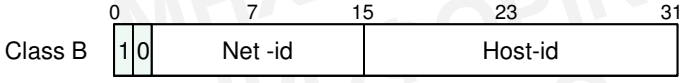


Το σύστημα διευθυνσιοδότησης IPv4

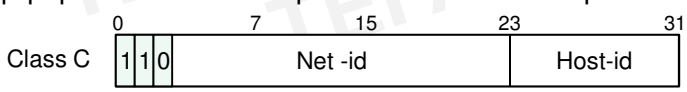
- Class A: 2^7 δίκτυα, με περισσότερους από 2^{16}(65,536) hosts χρησιμοποιούν 7 bits για το netid και 24bits για το hostid.



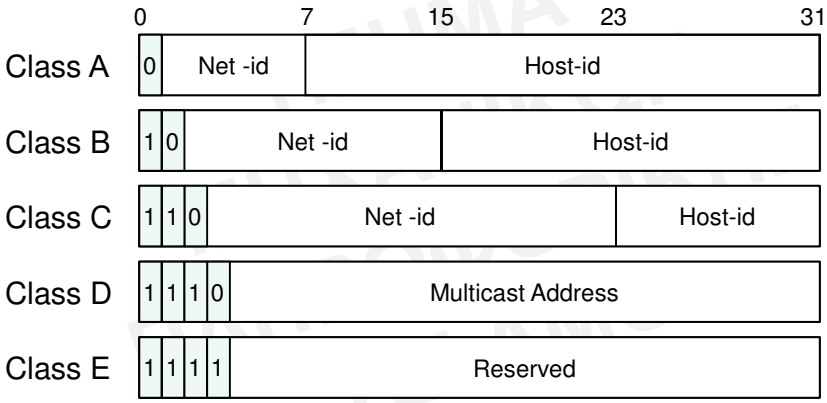
- Class B: 2^{14} δίκτυα, με 2^8(256) εως 2^{16}(65,536) hosts χρησιμοποιούν 14 bits για το netid και 16bits για το hostid.



- Class C: 2^{21} δίκτυα, με λιγότερους από 2^8(256) hosts χρησιμοποιούν 21 bits για το netid και 8bits για το hostid.



Το σύστημα διευθυνσιοδότησης IPv4



Δεσμευμένες διευθύνσεις

- Συσκευές που έχουν περισσότερες από μια φυσικές συνδέσεις έχουν απαραίτητα πολλαπλές IP διευθύνσεις.
- Ειδικές διευθύνσεις:
  - **Όλα 0**: εννοεί αυτόν τον host σε αυτό το δίκτυο.
  - **Netid 0**: κάποιον host σε αυτό το δίκτυο.
  - **Hostid 0**: αυτόν το host σε κάποιο δίκτυο.
  - **Όλα 1**: Εκπομπή στο τοπικό δίκτυο (broadcasting)
  - **Hostid 1**: Εκπομπή σε μακρινό δίκτυο. Η διεύθυνση καθορίζεται από το Netid.
  - **Netid 127**: Βρόχος επιστροφής (loopback).
- Γενικά,

  ένα πεδίο που αποτελείται μόνο από 1 σημαίνει "όλα", ενώ

  ένα πεδίο που αποτελείται μόνο από 0 σημαίνει "αυτό".

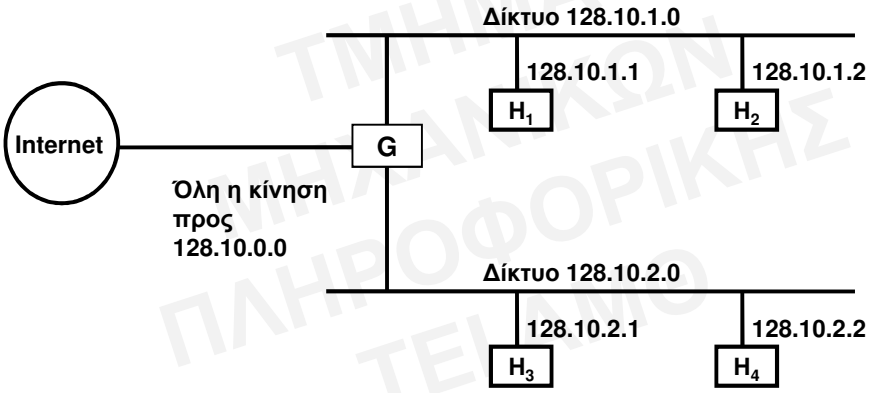
Το πρόβλημα

- Κάθε φυσικό δίκτυο έχει μία μοναδική διεύθυνση δικτύου.
- Η διεύθυνση κάθε host μέσα σε ένα φυσικό δίκτυο έχει ως προτασσόμενη τη δικτυακή διεύθυνση.
- Πολλές είναι οι περιπτώσεις όπου απαιτείται η δημιουργία ενός ξεχωριστού δικτύου ή η διάσπαση του υπάρχοντος.
  - Ωστόσο δεν υπάρχει διαθεσιμότητα πρόσθετης δικτυακής διεύθυνσης.
  - Π.χ. Έχουμε στη διάθεση μας μια διεύθυνση κλάσης C και ένα δίκτυο που αποτελείται από 78 δικτυακές συσκευές και θέλουμε να δημιουργήσουμε ακόμη ένα με 20 συσκευές.

Τι είναι υποδίκτυο

- Πρόκειται για μια τεχνική όπου **μια διεύθυνση δικτύου μπορεί να χρησιμοποιηθεί για τον λογικό διαχωρισμό ενός δικτύου.**
- Ο διαχωρισμός αυτός δεν είναι ορατός στους εξωτερικούς χρήστες επιτρέποντας έτσι την απόκρυψη κάποιων λεπτομερειών όσον αφορά την τοπολογία του δικτύου.
- Το διαχωρισμένο δίκτυο συμπεριφέρεται ως ένα και μοναδικό.
- Αποτελεί πρότυπο και είναι ένα βασικό μέρος της IP διευθυνσιοδότησης.

Υποδίκτυα



Υποδίκτυα

- Η πύλη G δέχεται όλη την κίνηση για το δίκτυο 128.10.0.0 και επιλέγει ένα φυσικό δίκτυο βάσει του τρίτου byte της διεύθυνσης.
- Η προσθήκη υποδικτύων απλά αλλάζει ελάχιστα τη μετάφραση των διευθύνσεων:
  - Αντί να χωρίζουμε τις 32bit διευθύνσεις σε τμήμα δικτύου και τμήμα host τις χωρίζουμε σε τμήμα δικτύου και ένα τμήμα το οποίο προσδιορίζει το υποδίκτυο και τον host.
  - **Σκοπός είναι η βέλτιστη χρήση των διαθέσιμων διευθύνσεων και κατανομή ενός εύρους σε περισσότερα του ενός φυσικά δίκτυα**

Υποδίκτυα

- Η μετάφραση της διεύθυνσης του δικτύου παραμένει η ίδια για όλους τους δρομολογητές εκτός από τον τοπικό που πρέπει να επιλέξει ανάμεσα στα δύο φυσικά δίκτυα.
- Η IP διεύθυνση χωρίζεται πλέον σε τρία τμήματα:

Υποδίκτυα

- Το αποτέλεσμα είναι μια ιεραρχημένη διευθυνσιοδότηση που οδηγεί σε μια ιεραρχημένη δρομολόγηση:
  - Αρχική δρομολόγηση σύμφωνα με το τμήμα δικτύου.
  - Δρομολόγηση σύμφωνα με το τμήμα της διεύθυνσης του υποδικτύου.
  - Δρομολόγηση (τοπικά) στον host σύμφωνα με τη συνολική διεύθυνση.

Πλεονεκτήματα υποδικτύων

- Μειωμένη κίνηση στο δίκτυο:
  - Οι δρομολογητές ορίζουν broadcast domains καθώς διατηρούν πακέτα εντός του τοπικού δικτύου και επιτρέπουν να περάσουν μόνο αυτά που προορίζονται για διαφορετικό δίκτυο. Όσο μικρότερο το domain τόσο λιγότερη κίνηση στα επιμέρους τμήματα του δικτύου.
- Βελτιστοποιημένη απόδοση δικτύου
  - Ως αποτέλεσμα της μειωμένης κίνησης
- Απλοποίηση στη διαχείριση
  - Μεγαλύτερη ευκολία στον εντοπισμό προβλημάτων
- Ανάπτυξη δικτύου σε μεγαλύτερες αποστάσεις

Υποδίκτυα

- Πως επιλέγουμε το τμήμα διεύθυνσης φυσικού δικτύου:
  - Εξαρτάται από τις απαιτήσεις μας για τον αριθμό υποδικτύων και hosts που θα έχει το κάθε υποδίκτυο.
  - Ανάλογα με τις απαιτήσεις μας πρέπει να επιλέξουμε τον αριθμό των bits, από το host τμήμα της διεύθυνσης, που θα αντιπροσωπεύσουν τα υποδίκτυα και τον αριθμό των bits που θα αντιπροσωπεύσουν τους hosts σε καθένα από αυτά τα δίκτυα.
  - Το πρότυπο TCP/IP μας δίνει αυτή τη δυνατότητα.

Πως δημιουργούμε υποδίκτυα

- Βήματα:
  1. Προσδιορισμός του αριθμού των διαφορετικών δικτύων
     - Ένα για κάθε υποδίκτυο
     - Ένα για κάθε σύνδεση σε WAN
  2. Προσδιορισμός του αριθμού των hosts ανά υποδίκτυο
     - Ένα για κάθε host
     - Ένα για κάθε interface του router
  3. Βασιζόμενοι στα παραπάνω
     - Επιλέγουμε τη μάσκα υποδικτύου
     - Αναθέτουμε σε κάθε υποδίκτυο μια διεύθυνση υποδικτύου
     - Καθορίζουμε το εύρος διευθύνσεων των hosts για κάθε υποδίκτυο

Πως δημιουργούμε υποδίκτυα

- Κάθε δικτυακή συσκευή πρέπει να γνωρίζει ποιο τμήμα της διεύθυνσης του host χρησιμοποιείται ως διεύθυνση υποδικτύου:
  - Ο μηχανισμός είναι η **μάσκα υποδικτύου**
  - Η 32-bit μάσκα αποτελείται από 1 και 0, όπου
    - η τιμή 1 υποδηλώνει ότι αυτό το τμήμα της διεύθυνσης χρησιμοποιείται για το δίκτυο ή τη διεύθυνση υποδικτύου
    - η τιμή 0 υποδηλώνει ότι αυτό το τμήμα αποτελεί τη διεύθυνση του host
- Δεν απαιτούν όλα τα δίκτυα μάσκες υποδικτύου

Μάσκα υποδικτύου

- Π.χ.: Η 32-bit μάσκα

  11111111 11111111 11111111 00000000

  δηλώνει ότι τα τρία πρώτα bytes αντιπροσωπεύουν το δίκτυο και το τέταρτο τον host.
- Η δρομολόγηση γίνεται χρησιμοποιώντας BOOLEAN AND της διεύθυνσης που έχουμε με τη μάσκα υποδικτύου για να απαλλαγούμε από τη διεύθυνση του host και να πάρουμε τη διεύθυνση του δικτύου.
- Οι εξ ορισμού μάσκες για τις τρεις κλάσεις είναι:

  Class A: 255.0.0.0

  Class B: 255.255.0.0

  Class C: 255.255.255.0

Υποδίκτυα κλάσης C

- Τα διαθέσιμα bits για τον ορισμό των υποδικτύων είναι 8.
- Πιθανές μάσκες υποδικτύου

  255.255.255.128 ή /25

  255.255.255.192 ή /26

  255.255.255.224 ή /27

  255.255.255.240 ή /28

  255.255.255.248 ή /29

  255.255.255.252 ή /30

Υποδίκτυα κλάσης C

- Αριθμός υποδικτύων = 2^x , όπου x ο αριθμός των 1 στη μάσκα
- Αριθμός hosts = 2^y-2 , όπου y ο αριθμός των 0
- Broadcast address: "Επόμενο subnet" – 1
- Διευθύνσεις hosts: Οι αριθμοί μεταξύ των subnets παραλείποντας τα «όλα 0» και «όλα 1»

Class C: Παράδειγμα 1

- Ένα δίκτυο έχει διεύθυνση 192.168.10.0 και χρησιμοποιεί τη μάσκα 255.255.255.192
  - Αριθμός υποδικτύων: $2^2 = 4$
  - Αριθμός hosts ανά υποδίκτυο: 2^6-2 = 62
  - Υποδίκτυα: 0, 64, 128, 192
  - Broadcast address για κάθε υποδίκτυο: 63, 127, 191, 255
  - Διευθύνσεις host για κάθε υποδίκτυο: 1-62, 65-126, 129-190, 193-254

Class C: Παράδειγμα 2

- Ένα δίκτυο έχει διεύθυνση 192.168.10.0 και χρησιμοποιεί τη μάσκα 255.255.255.224
  - Αριθμός υποδικτύων:;
  - Αριθμός hosts ανά υποδίκτυο: ;
  - Υποδίκτυα: ;
  - Broadcast address για κάθε υποδίκτυο: ;
  - Διευθύνσεις host για κάθε υποδίκτυο: ;

Class C: Παράδειγμα 2

- Ένα δίκτυο έχει διεύθυνση 192.168.10.0 και χρησιμοποιεί τη μάσκα 255.255.255.224
  - Αριθμός υποδικτύων: $2^3 = 8$
  - Αριθμός hosts ανά υποδίκτυο: $2^5-2 = 30$
  - Υποδίκτυα: 192.168.10.0, 192.168.10.32, .64, .96, .128, .160, .192, .224
  - Broadcast address για κάθε υποδίκτυο: 31, 63, 95, 127, 159, 191, 223, 255
  - Διευθύνσεις host για κάθε υποδίκτυο: 1-30, 33-62, 65-94, 97-126, 129-158, 161-190, 193-222, 225-254

Class C: Παράδειγμα 3

- Ποιες από τις διευθύνσεις: 192.168.10.41, 192.168.10.131 και 192.168.10.154 ανήκουν στο ίδιο υποδίκτυο όταν η μάσκα υποδικτύου είναι 255.255.255.128;
- Όταν η μάσκα υποδικτύου είναι 255.255.255.224;
- Οι διευθύνσεις 192.168.10.32 και 192.168.15.42 ανήκουν στο ίδιο υποδίκτυο όταν η μάσκα είναι 255.255.255.18;

Υποδίκτυα κλάσης Β

- Τα διαθέσιμα bits για τον ορισμό των υποδικτύων είναι 16.
- Πιθανές μάσκες υποδικτύου

255.255.128.0	ή	/17	255.255.255.0	ή	/24
255.255.192.0	ή	/18	255.255.255.128	ή	/25
255.255.224.0	ή	/19	255.255.255.192	ή	/26
255.255.240.0	ή	/20	255.255.255.224	ή	/27
255.255.248.0	ή	/21	255.255.255.240	ή	/28
255.255.252.0	ή	/22	255.255.255.248	ή	/29
255.255.254.0	ή	/23	255.255.255.252	ή	/30

Class B: Παράδειγμα 1

- Ένα δίκτυο έχει διεύθυνση 154.12.0.0 και χρησιμοποιεί τη μάσκα 255.255.192.0
  - Αριθμός υποδικτύων: ;
  - Αριθμός hosts ανά υποδίκτυο: ;
  - Υποδίκτυα: ;
  - Broadcast address για κάθε υποδίκτυο: ;
  - Διευθύνσεις host για κάθε υποδίκτυο: ;

Class B: Παράδειγμα 1

- Ένα δίκτυο έχει διεύθυνση 154.12.0.0 και χρησιμοποιεί τη μάσκα 255.255.192.0
  - Αριθμός υποδικτύων: $2^2 = 4$
  - Αριθμός hosts ανά υποδίκτυο: $2^{14}-2 = 16382$
  - Υποδίκτυα: 0.0, 64.0, 128.0, 192.0
  - Broadcast address για κάθε υποδίκτυο: 63.255, 127.255, 191.255, 255.255
  - Διευθύνσεις host για κάθε υποδίκτυο:
    0.1-63.254,
    64.1-127.254,
    128.1-191.254,
    192.1-255.254

Class B: Παράδειγμα 2

- Ένα δίκτυο έχει διεύθυνση 154.12.0.0 και χρησιμοποιεί τη μάσκα 255.255.240.0
  - Αριθμός υποδικτύων: ;
  - Αριθμός hosts ανά υποδίκτυο: ;
  - Υποδίκτυα: ;
  - Broadcast address για κάθε υποδίκτυο: ;
  - Διευθύνσεις host για κάθε υποδίκτυο: ;

Class B: Παράδειγμα 2

- Ένα δίκτυο έχει διεύθυνση 154.12.0.0 και χρησιμοποιεί τη μάσκα 255.255.240.0
  - Αριθμός υποδικτύων: $2^4 = 16$
  - Αριθμός hosts ανά υποδίκτυο: $2^{12}-2 = 4094$
  - Υποδίκτυα: 0.0, 16.0, 32.0, 48.0, 64.0, ……, 240.0
  - Broadcast address για κάθε υποδίκτυο: 15.255, 31.255, 47.255, 63.255,…
  - Διευθύνσεις host για κάθε υποδίκτυο:
    0.1-15.254,
    16.1-31.254,
    32.1-47.254,
    48.1-63.254,
    …

Class B: Παράδειγμα 3

- Ένα δίκτυο έχει διεύθυνση 154.12.0.0 και χρησιμοποιεί τη μάσκα 255.255.255.192
  - Αριθμός υποδικτύων: ;
  - Αριθμός hosts ανά υποδίκτυο: ;
  - Υποδίκτυα: ;
  - Broadcast address για κάθε υποδίκτυο: ;
  - Διευθύνσεις host για κάθε υποδίκτυο: ;

Class B: Παράδειγμα 3

- Ένα δίκτυο έχει διεύθυνση 154.12.0.0 και χρησιμοποιεί τη μάσκα 255.255.255.192
  - Αριθμός υποδικτύων: $2^{10} = 1024$
  - Αριθμός hosts ανά υποδίκτυο: $2^6-2 = 62$
  - Υποδίκτυα: 0.0, 0.64, 0.128, 0.192, 1.0, 1.64, 1.128, 1.192…
  - Broadcast address για κάθε υποδίκτυο: 0.63, 0.127, 0.191, 0.255, 1.63, 1.127, 1.191, 1.255…
  - Διευθύνσεις host για κάθε υποδίκτυο:
    0.1-0.62,
    0.65-0.126,
    0.129-0.190,
    0.193-0.254,
    1.1-1.62
    …

Υποδίκτυα κλάσης Α

- Τα διαθέσιμα bits για τον ορισμό των υποδικτύων είναι 24.
- Πιθανές μάσκες υποδικτύου

255.128.0.0	(/9)	255.255.240.0	(/20)
255.192.0.0	(/10)	255.255.248.0	(/21)
255.224.0.0	(/11)	255.255.252.0	(/22)
255.240.0.0	(/12)	255.255.254.0	(/23)
255.248.0.0	(/13)	255.255.255.0	(/24)
255.252.0.0	(/14)	255.255.255.128	(/25)
255.254.0.0	(/15)	255.255.255.192	(/26)
255.255.0.0	(/16)	255.255.255.224	(/27)
255.255.128.0	(/17)	255.255.255.240	(/28)
255.255.192.0	(/18)	255.255.255.248	(/29)
255.255.224.0	(/19)	255.255.255.252	(/30)

Ασκήσεις υποδικτύων

- Έστω ότι οι ρυθμίσεις της κάρτας δικτύου είναι:

  Network address: 192.168.15.35
  Subnet mask: 255.255.255.248

  - Ποια είναι η διεύθυνση του δικτύου;
  - Ποια είναι η διεύθυνση του πρώτου host στο υποδίκτυο;
  - Ποια είναι η διεύθυνση του τελευταίου host στο υποδίκτυο;
  - Ποια είναι η broadcast διεύθυνση;
  - Ποιο είναι το επόμενο υποδίκτυο;

Μεθοδολογία εύρεσης στοιχείων

1. Γράφουμε το byte που "σπάει" η μάσκα σε δυαδική μορφή:

   35 = 00100011

2. Γράφουμε το byte της μάσκας που μας ενδιαφέρει σε δυαδικό:

   248 = 11111000

3. Διαχωρίζουμε τα σημαντικά bits από τη διεύθυνση

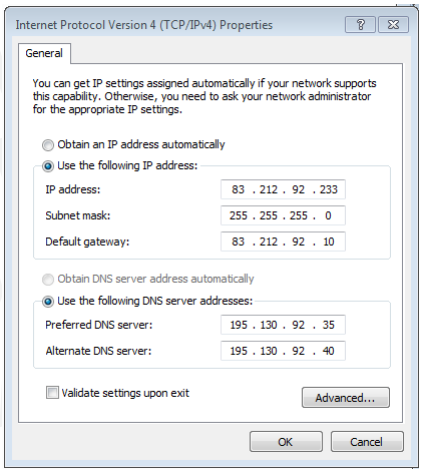
   00100|011
   11111|000

4. Οι απαντήσεις βασίζονται στα σημαντικά bits

Διεύθυνση δικτύου:	00100000
Διεύθυνση πρώτου host στο υποδίκτυο:	00100001
Διεύθυνση τελευταίου host στο υποδίκτυο:	00100110
Διεύθυνση broadcast:	00100111
Επόμενο υποδίκτυο:	00101000

Ασκήσεις υποδικτύων

- Έστω ότι οι ρυθμίσεις της κάρτας δικτύου είναι:
  - Ποια είναι η διεύθυνση του δικτύου;
  - Ποια είναι η διεύθυνση του πρώτου host στο υποδίκτυο;
  - Ποια είναι η διεύθυνση του τελευταίου host στο υποδίκτυο;
  - Ποια είναι η broadcast διεύθυνση;
  - Ποιο είναι το επόμενο υποδίκτυο;
  - Η διεύθυνση του DNS ανήκει στο ίδιο υποδίκτυο;



Απάντηση

1. Δίκτυο:

   212.92.233 = 11010100.01011100.11101001

2. Μάσκα:

   255.255.0 = 11111111.11111111.00000000

3. Διαχωρίζουμε τα σημαντικά bits από τη διεύθυνση

   11010100.01011100|.11101001
   11111111.11111111|.00000000

4. Οι απαντήσεις βασίζονται στα σημαντικά bits

Διεύθυνση δικτύου:	11010100.01011100.00000000
Διεύθυνση πρώτου host στο υποδίκτυο:	11010100.01011100.00000001
Διεύθυνση τελευταίου host στο υποδίκτυο:	11010100.01011100.11111110
Διεύθυνση broadcast:	11010100.01011100.11111111
Επόμενο υποδίκτυο:	11010100.01011101.00000000

Ασκήσεις υποδικτύων

- Ποιες είναι οι διευθύνσεις hosts που περιλαμβάνονται στις διευθύνσεις:
  - 195.12.32.192/26
  - 195.12.32.192/27
  - 195.12.32.192/28
  - 192.15.36.160/27
  - 192.15.36.160/28
  - 83.17.128.0/18

Ασκήσεις υποδικτύων

- Έστω ότι έχουμε στη διάθεση μας τη διεύθυνση 178.46.0.0. Με αυτή θέλουμε να καλύψουμε 19 φυσικά δίκτυα κάθε ένα από τα οποία δε περιέχει περισσότερους από 2046 hosts. Ορίστε μια μάσκα υποδικτύου που θα έκανε αυτό το διαχωρισμό.

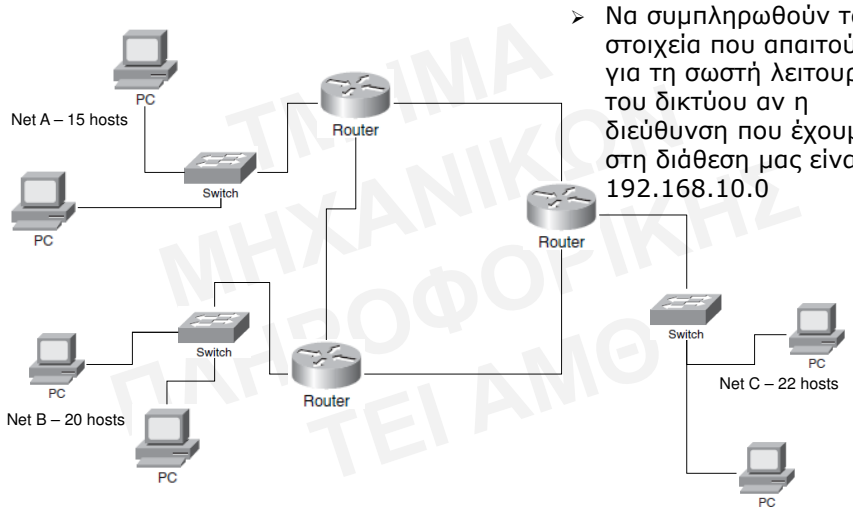
- Θεωρήστε ένα σταθερό τμήμα υποδικτύου ενός δικτύου κατηγορίας Β το οποίο θα πρέπει να έχει τουλάχιστον 176 υποδίκτυα. Μέχρι πόσους hosts μπορεί να έχει το κάθε δίκτυο;

Ασκήσεις υποδικτύων

- Έστω ότι θέλουμε να χρησιμοποιήσουμε τη διεύθυνση 192.168.10.0 για να καλύψουμε τα παρακάτω δίκτυα:
  - A: 20 hosts
  - B: 2 hosts
  - D: 30 hosts
  - E: 12 hosts
  - F: 30 hosts

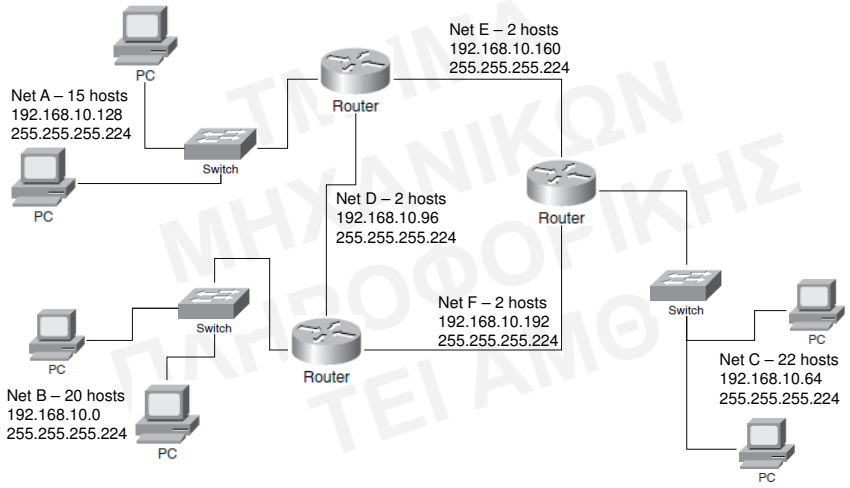
  Ποια είναι η μάσκα υποδικτύου που πρέπει να χρησιμοποιήσουμε;

Ασκήσεις υποδικτύων



- Να συμπληρωθούν τα στοιχεία που απαιτούνται για τη σωστή λειτουργία του δικτύου αν η διεύθυνση που έχουμε στη διάθεση μας είναι η 192.168.10.0

Ασκήσεις υποδικτύων



Variable Length Subnet Mask

- Η αυξημένη σπατάλη διευθύνσεων ως αποτέλεσμα χρήσης συγκεκριμένης μάσκας οδήγησε στη χρήση της τεχνικής Variable Length Subnet Mask η οποία επιτρέπει τη χρήση διαφορετικών subnet masks για τα επιμέρους υποδίκτυα.
  - Στην περίπτωση αυτή επιλέγουμε για το κάθε δίκτυο μια διαφορετική μάσκα τέτοια ώστε να ικανοποιεί τις ανάγκες του συγκεκριμένου δικτύου και να έχουμε τη μικρότερη δυνατή σπατάλη διευθύνσεων.
  - Ιδιαίτερη προσοχή θα πρέπει να δοθεί ώστε με τον καταμερισμό των διευθύνσεων και τη χρήση των διαφορετικών μασκών να μην υπάρχει επικάλυψη διευθύνσεων μεταξύ των επιμέρους δικτύων.

Ασκήσεις υποδικτύων

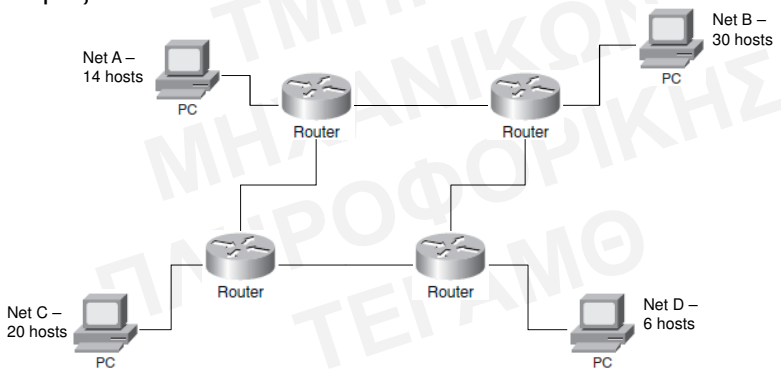
- Ένας οργανισμός έχει στη διάθεση του τη διεύθυνση 200.17.5.0 και θέλει να δημιουργήσει υποδίκτυα για πέντε τμήματα με τους ακόλουθους hosts:
  - A 82 hosts
  - B 55 hosts
  - C 30 hosts
  - D 10 hosts
  - E 8 hosts
  - Δώστε πιθανές διευθύνσεις δικτύων και το εύρος των hosts για κάθε υποδίκτυο

Ασκήσεις υποδικτύων

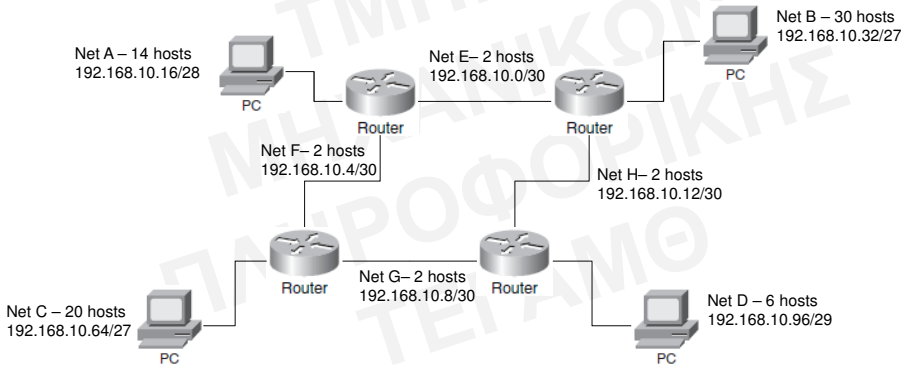
- Λύση: Επειδή αν χρησιμοποιήσουμε δύο bits για το υποδίκτυο τότε το κάθε ένα από τα τέσσερα υποδίκτυα θα μπορούσε να έχει μέχρι 63 hosts απαιτείται μια άλλη διαμόρφωση. Έτσι μπορούμε να δημιουργήσουμε αρχικά 2 υποδίκτυα με μάσκα υποδικτύου το 255.255.255.128 (χρησιμοποιούμε μόνο ένα bit) (ένα υποδίκτυο για το Α και ένα για τα άλλα τρία) και μετά, για τα τρία άλλα υποδίκτυα να χρησιμοποιήσουμε τρία bits για τη μάσκα υποδικτύου δίνοντας έτσι τη δυνατότητα να δημιουργήσουμε άλλα 3 υποδίκτυα του **δευτέρου υποδικτύου**.
- Εάν το Β είχε 35 hosts τότε θα έπρεπε πάλι να χωρίσουμε το δεύτερο υποδίκτυο σε 2 άλλα υποδίκτυα (χρησιμοποιώντας ακόμα 1 bit), ένα για το Β και ένα για τα C και D και μετά ακόμα 1 bit για να δημιουργήσουμε 2 υποδίκτυα, ένα για το C και ένα για το D.

Variable Length Subnet Mask

- Έστω το δίκτυο με διαθέσιμη διεύθυνση 192.168.10.0. Να οριστούν οι μάσκες, οι διευθύνσεις δικτύου και το διαθέσιμο εύρος διευθύνσεων.

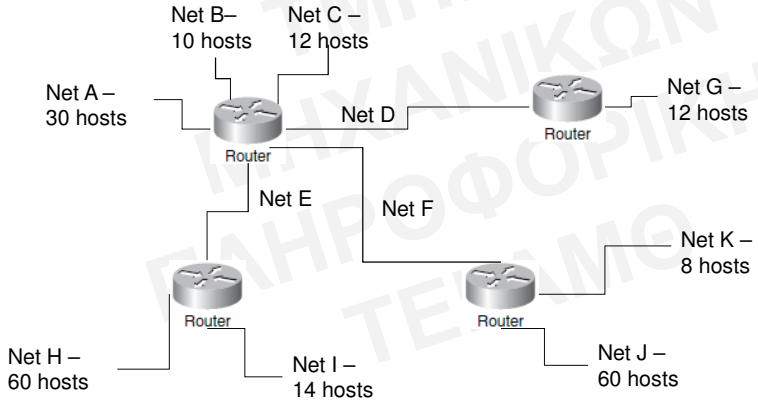


Variable Length Subnet Mask



Variable Length Subnet Mask

- Έστω το δίκτυο με διαθέσιμη διεύθυνση 192.168.10.0/24. Να οριστούν οι μάσκες, οι διευθύνσεις δικτύου και το διαθέσιμο εύρος διευθύνσεων.



ΔΙΚΤΥΑ ΙΙ

Πρωτόκολλο IP

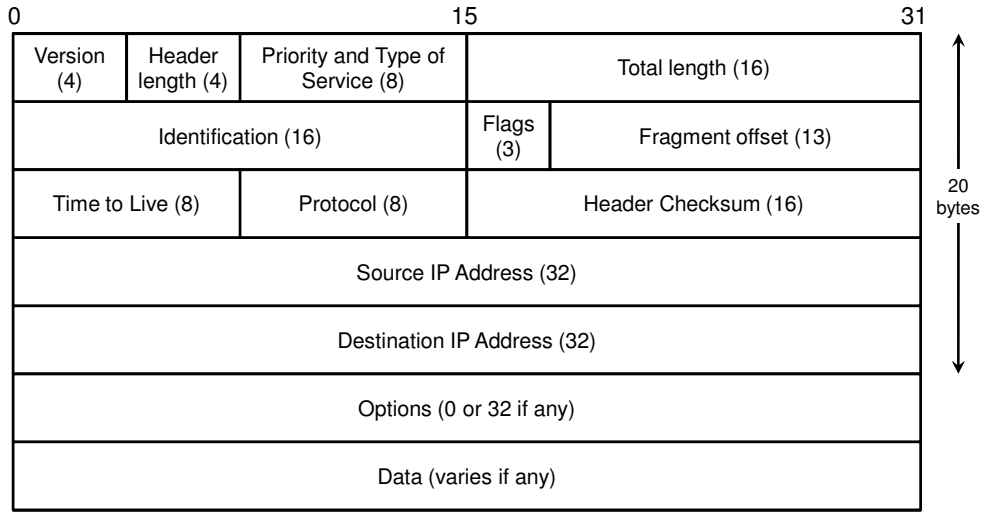
Στρώμα Διαδικτύου IP

- Το πρωτόκολλο διαδικτύου (Internet Protocol) είναι ένα **αναξιόπιστο** και **χωρίς σύνδεση** πρωτόκολλο του στρώματος διαδικτύου.
  - Δεδομενογραφήματα στέλνονται χωρίς την δημιουργία σύνδεσης
  - Δεδομενογραφήματα μπορεί να χαθούν ή να απορριφθούν λόγω λαθών, ή συμφόρησης στο δίκτυο (best effort delivery)
    - Ο έλεγχος της αξιοπιστίας στη μετάδοση γίνεται από ανώτερα στρώματα

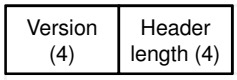
Στρώμα Διαδικτύου IP

- Ορίζει τη δομή των δεδομένων που μεταφέρονται υπό τη μορφή δεδομενογραφημάτων (πακέτων).
- Φροντίζει για τη **δρομολόγηση** τους από τον αποστολέα στον παραλήπτη.
- **Δεδομενογράφημα.** Αποτελείται από επικεφαλίδα (προκαθορισμένου μήκους 20 bytes + προαιρετικό τμήμα μεταβλητού μήκους) και δεδομένα.

Επικεφαλίδα IPv4

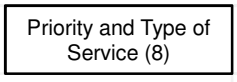


Επικεφαλίδα IPv4



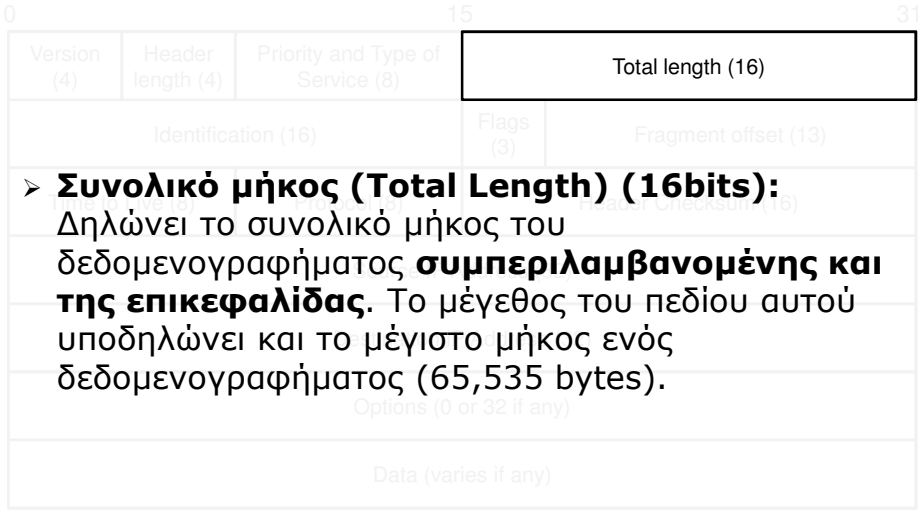
- **Έκδοση (Version) (4 bits)**: Μας πληροφορεί για την έκδοση στην οποία ανήκει το δεδομενογράφημα. Πιθανές εκδόσεις είναι οι 4 και 6.
- **Πεδίο μήκους επικεφαλίδας (Header Length Field) (4 bits)**: Μας πληροφορεί για το μέγεθος της επικεφαλίδας σε λέξεις των 32-bits.

Επικεφαλίδα IPv4



- **Πεδίο τύπου υπηρεσίας (Service Type) (8bits):** Αφορούν στην επιθυμητή ποιότητα της υπηρεσίας. Ο αλγόριθμος δρομολόγησης πρέπει να επιλέξει το κατάλληλο μέσο μετάδοσης βασισμένος σε αυτές τις πληροφορίες. Αποτελείται από τα πεδία:
  - `Bits 0-2: Precedence.`
  - `Bit 3: 0 = Normal Delay, 1 = Low Delay.`
  - `Bits 4: 0 = Normal Throughput, 1 = High Throughput.`
  - `Bits 5: 0 = Normal Reliability, 1 = High Reliability.`
  - `Bit 6-7: Reserved for Future Use.`

Επικεφαλίδα IPv4



- **Συνολικό μήκος (Total Length) (16bits):** Δηλώνει το συνολικό μήκος του δεδομενογραφήματος **συμπεριλαμβανομένης και της επικεφαλίδας**. Το μέγεθος του πεδίου αυτού υποδηλώνει και το μέγιστο μήκος ενός δεδομενογραφήματος (65,535 bytes).

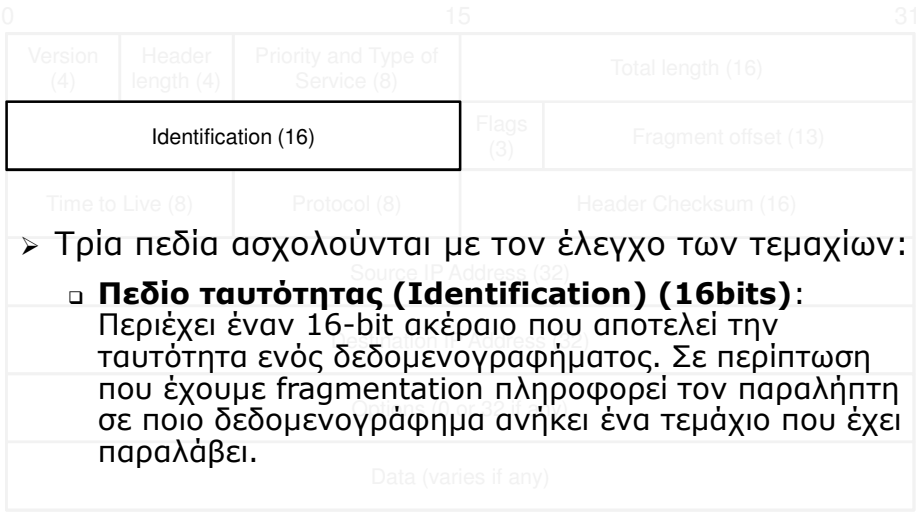
Μέγιστη μονάδα μεταφοράς (MTU)

- **Μέγιστη Μονάδα Μεταφοράς (Maximum Transfer Unit, MTU):** Κάθε τεχνολογία μεταγωγής πακέτων θέτει ένα ανώτατο όριο στο μέγεθος των δεδομένων που μπορεί να μεταδώσει με ένα πλαίσιο χρησιμοποιώντας κάποιο φυσικό δίκτυο. Π.χ. Ethernet (1500bytes), FDDI (περίπου 4470bytes). Τα MTU μεγέθη όμως μπορεί να είναι αρκετά μικρά (π.χ. 127bytes στο IEEE802.15.4 περί WPAN).
- Η χρήση μικρών δεδομενογραφημάτων (με μέγεθος μικρότερο από το μικρότερο πιθανό MTU κατά μήκος της διαδρομής) θα είχε ως αποτέλεσμα να μη χρησιμοποιούνται σωστά τα δίκτυα με μεγάλο MTU.
- Η χρήση μεγάλων δεδομενογραφημάτων σημαίνει ότι αυτά δε θα μπορούν πάντα να μπουν σε ένα και μόνο πλαίσιο.

Μέγιστη μονάδα μεταφοράς (MTU)

- **Λύση**: το TCP/IP επιλέγει ένα αρχικό μέγεθος δεδομενογραφήματος και το οποίο μπορεί να διαιρέσει σε μικρότερα κομμάτια (τεμάχια, fragments) όταν αυτό πρέπει να περάσει από δίκτυα με μικρό MTU. Η διαδικασία αυτή ονομάζεται **fragmentation**.
  - Το μέγεθος του κάθε τεμαχίου επιλέγεται έτσι ώστε αυτό να χωράει σε ένα απλό πλαίσιο.
  - Κάθε τεμάχιο έχει μια επικεφαλίδα που είναι σχεδόν ίδια με την αρχική επικεφαλίδα.
  - Η επανασύνδεση των τεμαχίων γίνεται στον τελικό προορισμό.

Επικεφαλίδα IPv4



- Τρία πεδία ασχολούνται με τον έλεγχο των τεμαχίων:
  - **Πεδίο ταυτότητας (Identification) (16bits)**: Περιέχει έναν 16-bit ακέραιο που αποτελεί την ταυτότητα ενός δεδομενογραφήματος. Σε περίπτωση που έχουμε fragmentation πληροφορεί τον παραλήπτη σε ποιο δεδομενογράφημα ανήκει ένα τεμάχιο που έχει παραλάβει.

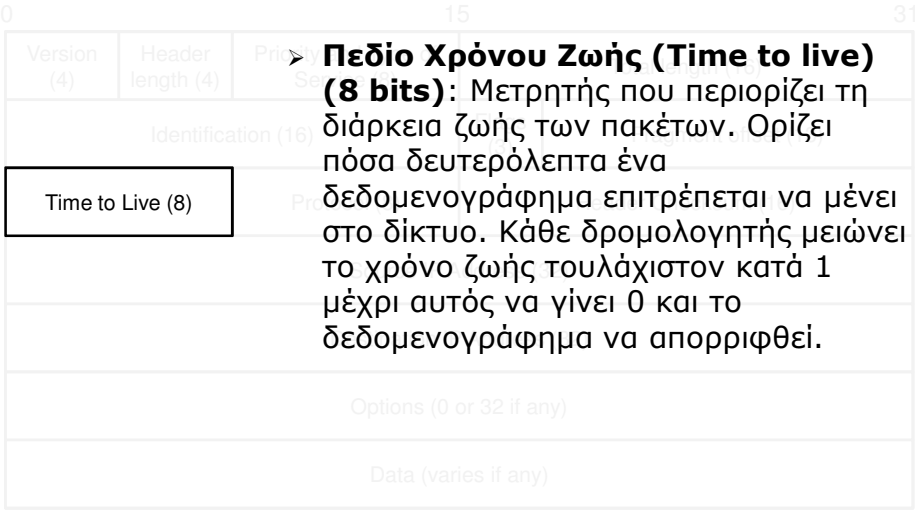
Επικεφαλίδα IPv4

- Τρία πεδία ασχολούνται με τον έλεγχο των τεμαχίων:
  - **Flags :**
    - **Bit 0: 0**
    - **Bit 1: 0=May fragment, 1=Don't fragment**
    - **Bit 2: 0=Last Fragment, 1=More Fragments**

Επικεφαλίδα IPv4

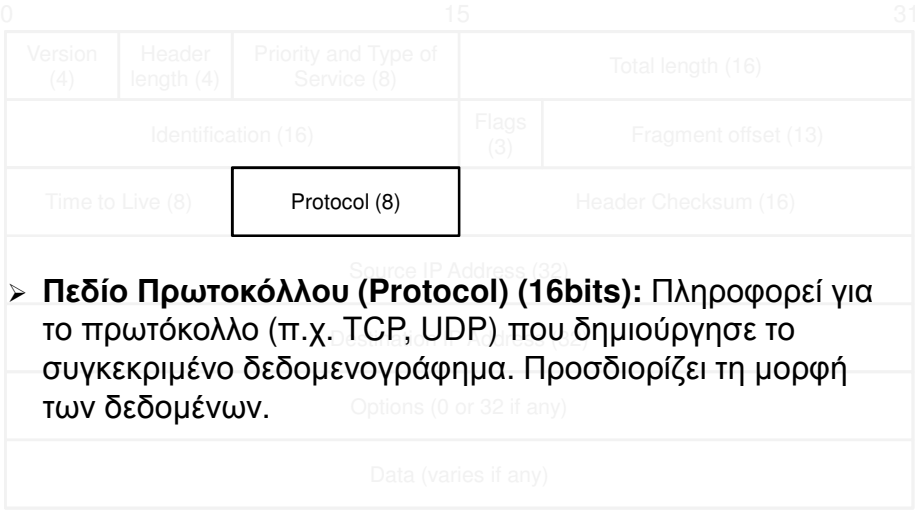
- Τρία πεδία ασχολούνται με τον έλεγχο των τεμαχίων:
  - **Πεδίο Θέσης Τεμαχίου (Fragment Offset) (13bits):** Πληροφορεί για τη θέση αυτού του τεμαχίου στο δεδομενογράφημα. Μετράται σε μονάδες των 8bytes. Το offset του πρώτου τεμαχίου είναι 0.

Επικεφαλίδα IPv4



- **Πεδίο Χρόνου Ζωής (Time to live) (8 bits)**: Μετρητής που περιορίζει τη διάρκεια ζωής των πακέτων. Ορίζει πόσα δευτερόλεπτα ένα δεδομενογράφημα επιτρέπεται να μένει στο δίκτυο. Κάθε δρομολογητής μειώνει το χρόνο ζωής τουλάχιστον κατά 1 μέχρι αυτός να γίνει 0 και το δεδομενογράφημα να απορριφθεί.

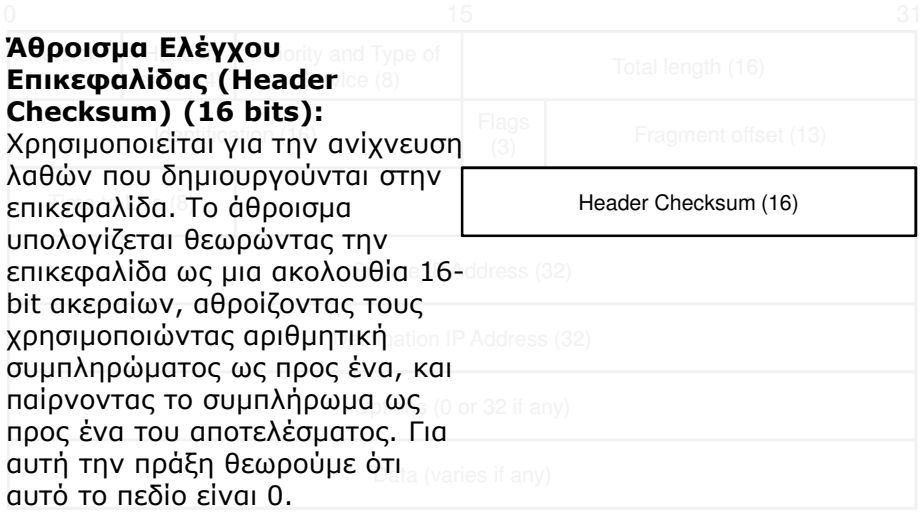
Επικεφαλίδα IPv4



- **Πεδίο Πρωτοκόλλου (Protocol) (16bits):** Πληροφορεί για το πρωτόκολλο (π.χ. TCP, UDP) που δημιούργησε το συγκεκριμένο δεδομενογράφημα. Προσδιορίζει τη μορφή των δεδομένων.

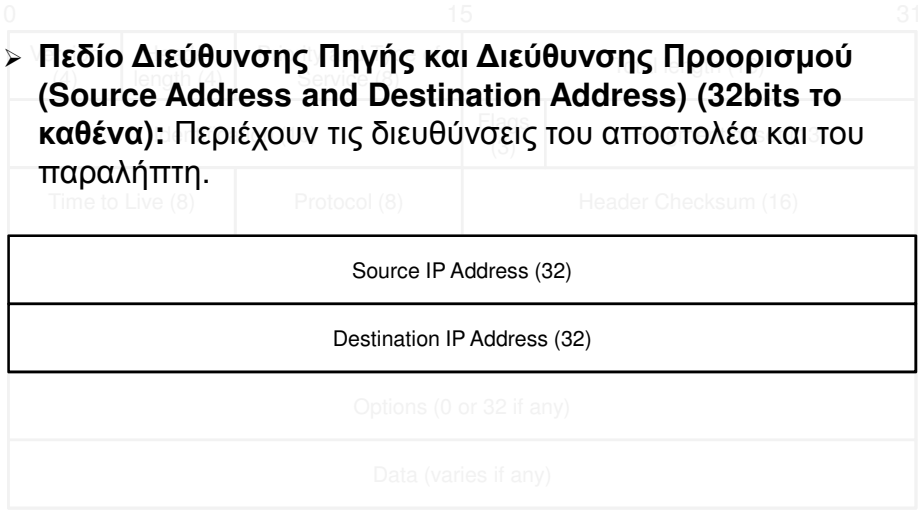
Επικεφαλίδα IPv4

- **Άθροισμα Ελέγχου Επικεφαλίδας (Header Checksum) (16 bits):** Χρησιμοποιείται για την ανίχνευση λαθών που δημιουργούνται στην επικεφαλίδα. Το άθροισμα υπολογίζεται θεωρώντας την επικεφαλίδα ως μια ακολουθία 16-bit ακεραίων, αθροίζοντας τους χρησιμοποιώντας αριθμητική συμπληρώματος ως προς ένα, και παίρνοντας το συμπλήρωμα ως προς ένα του αποτελέσματος. Για αυτή την πράξη θεωρούμε ότι αυτό το πεδίο είναι 0.



Επικεφαλίδα IPv4

- **Πεδίο Διεύθυνσης Πηγής και Διεύθυνσης Προορισμού (Source Address and Destination Address) (32bits το καθένα):** Περιέχουν τις διευθύνσεις του αποστολέα και του παραλήπτη.



Frame 1 (1506 bytes on wire, 1506 bytes captured)
Ethernet II, Src: Intracom_26:ac:be (00:05:59:26:ac:be), Dst: IntelCor_35:6f:69 (00:1f:3c:35:6f:69)
Internet Protocol, Src: 94.75.220.129 (94.75.220.129), Dst: 192.168.2.3 (192.168.2.3)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..0. = ECN-Capable Transport (ECT): 0 ECN: Explicit Congestion Notification
    ....0 = ECN-CE: 0
  Total Length: 1492
  Identification: 0x708f (28815)
  Flags: 0x02 (Don't Fragment)
    0.. = Reserved bit: Not Set
    .1. = Don't fragment: Set
    ..0 = More fragments: Not Set
  Fragment offset: 0
  Time to live: 114
  Protocol: TCP (0x06)
  Header checksum: 0x951c [correct]
    [Good: True]
    [Bad : False]
  Source: 94.75.220.129 (94.75.220.129)
  Destination: 192.168.2.3 (192.168.2.3)
Transmission Control Protocol, Src Port: http (80), Dst Port: 50513 (50513), Seq: 1, Ack: 1, Len: 1452
Hypertext Transfer Protocol

IP captured packet

ΔΙΚΤΥΑ ΙΙ

Πρωτόκολλο NAT
IPv6

NAT protocol

- Το πρωτόκολλο **NAT (Network Address Translation)** αποτελεί έναν τρόπο αντιμετώπισης του προβλήματος έλλειψης διευθύνσεων στο IPv4:
  - Η βασική ιδέα είναι ότι όλοι οι σταθμοί που μπορεί να επικοινωνήσουν μεταξύ τους μέσω Internet δε χρειάζεται να έχουν μοναδικές διευθύνσεις παγκοσμίως.
  - Σε ένα σταθμό μπορεί να δοθεί μια **ιδιωτική διεύθυνση** η οποία **δεν είναι μοναδική παγκοσμίως**, αλλά είναι **μοναδική μέσα σε ένα περιορισμένο δίκτυο** (όπως είναι π.χ. το τοπικό δίκτυο μιας εταιρίας).

NAT protocol

- Όσο ένας σταθμός με ιδιωτική διεύθυνση επικοινωνεί με άλλους σταθμούς μέσα στο ίδιο τοπικό δίκτυο μια τέτοια διεύθυνση επαρκεί.
- Εάν θα πρέπει να επικοινωνήσει με κάποιο σταθμό έξω από τα όρια αυτού του δικτύου, τότε η επικοινωνία γίνεται με τη χρήση του NAT, το οποίο **αναλαμβάνει τη μετάφραση της τοπικά μοναδικής διεύθυνσης σε μια παγκοσμίως μοναδική διεύθυνση**.
- Από τη στιγμή που είναι πιθανό πως μόλις ένας μικρός αριθμός από τους σταθμούς αυτού του περιορισμένου δικτύου θα θέλουν να επικοινωνήσουν ταυτόχρονα με κάποιους σταθμούς έξω από τα όρια αυτού του δικτύου, ένας μικρός μόνο αριθμός παγκοσμίως μοναδικών διευθύνσεων επαρκεί.

NAT protocol

- Έτσι οι απαιτήσεις σε μοναδικές διευθύνσεις μειώνονται σημαντικά. Επιπλέον ο φορέας που κάνει χρήση ιδιωτικών διευθύνσεων έχει πλήρη ευελιξία όσον αφορά τη διευθυνσιοδότηση μέσα στο δικό του δίκτυο.

- Οι παρακάτω διευθύνσεις έχουν οριστεί ως ιδιωτικές.
  - 10.0.0.0 – 10.255.255.255 (10.0.0.0/8)
  - 172.16.0.0 – 172.31.255.255 (172.16.0.0/12)
  - 192.168.0.0 – 192.168.255.255 (192.168.0.0/16)

NAT protocol

– Π.χ. Το πρωτόκολλο NAT (το οποίο τρέχει σε μια πύλη) λαμβάνει εξερχόμενα IP πακέτα από κάποιο σταθμό που είναι μέσα στο δίκτυο της εταιρίας και μεταφράζει την IP διεύθυνση πηγής (172.17.1.5) σε μια παγκοσμίως μοναδική διεύθυνση (165.69.210.246). Όταν τα πακέτα έρχονται με διεύθυνση προορισμού την 165.69.210.246 το πρωτόκολλο NAT είναι υπεύθυνο ώστε να μεταφράσει πάλι τη διεύθυνση αυτή στην τοπικά μοναδική διεύθυνση.

NAT protocol

- Μειονεκτήματα του πρωτοκόλλου NAT
  - Το βασικό μειονέκτημα του πρωτοκόλλου NAT είναι ότι δεν είναι σύμφωνο με τη βασική αρχή του IP μοντέλου όπου όλοι οι κόμβοι πρέπει να έχουν μοναδικές διευθύνσεις παγκοσμίως.
  - Σε αυτή την αρχή βασίζονται πολλά άλλα πρωτόκολλα και εφαρμογές. Για παράδειγμα, πρωτόκολλα ή εφαρμογές μπορεί να απαιτούν από τον κόμβο για τις ανάγκες της επικοινωνίας να διαθέτει μια σταθερή IP.

Ο δρόμος προς το IPv6

- Τον Φεβρουάριο του 2011, ο διεθνής μη κερδοσκοπικός Οργανισμός ICANN (Internet Corporation for Assigned Names and Numbers) που εποπτεύει την απόδοση και κατανομή των διαδικτυακών διευθύνσεων σε παγκόσμιο επίπεδο, στο Μαϊάμι των ΗΠΑ, παραχώρησε και τα τελευταία πέντε διαθέσιμα πακέτα διευθύνσεων IPv4.
- Οι τελευταίες διευθύνσεις IPv4 που εκχώρησε η ICANN διανεμήθηκαν στους τελευταίους δικαιούχους από τους Περιφερειακούς Καταχωρητές Διαδικτύου (RIR).

IPv6

- Στόχοι της δημιουργίας του IPv6 (RFC 2460):
  - Μεγαλύτερο εύρος διευθύνσεων.
  - Γρηγορότερη επεξεργασία των πακέτων από τους δρομολογητές (Για αυτό το λόγο έχουν αφαιρεθεί κάποια από τα πεδία που βρίσκονται στο IPv4).
  - Έμφαση στην ασφάλεια.
  - Μεγαλύτερη προσοχή στον τύπο της υπηρεσίας, ειδικά για δεδομένα πραγματικού χρόνου (real-time services).

IPv6

- Στόχοι της δημιουργίας του IPv6:
  - Περισσότερη ευελιξία με τη χρήση πολλών προαιρετικών επικεφαλίδων οι οποίες προσφέρουν λειτουργικότητα η οποία δεν υπάρχει σε παλαιότερες εκδόσεις του IP (η διαφορετική μορφή επικεφαλίδας βέβαια έχει ως αποτέλεσμα να μην υπάρχει συμβατότητα με παλαιότερες εκδόσεις).
  - Επιτρέπει την εξέλιξη του πρωτοκόλλου έτσι ώστε να μπορεί να προσαρμοστεί σε νέες τεχνολογίες.

IPv6 Διευθύνσεις

- Αποτελούνται από 128 bits.
  - Οι διαθέσιμες διευθύνσεις είναι ~$3,4 \times 10^{38}$

    ή

    340.282.366.920.938.463.463.374.607.431.768.211.456
- Δε χωρίζονται σε κλάσεις όπως οι διευθύνσεις στο IPv4.
- Ο τρόπος με τον οποίο συμβολίζονται οι διευθύνσεις είναι με το διαμερισμό της διεύθυνσης σε 8 16-bit τμήματα.
- Π.χ.
  2001:0ba0:01e0:d001:0000:0000:d0f0:0010

IPv6 Διευθύνσεις

- Τμήματα διευθυνσης:

Π.χ. 2001 : 0db8 : 3c4d : 0015 : 0000 : 0000 : abcd : ef12

| global prefix | subnet | Interface ID |

- Το global prefix δίνεται από τον ISP ή από κάποιο Regional Internet Registry. Οι τιμές των Subnet και Interface ID ελέγχονται από τον κάτοχο της διεύθυνσης.
- Για την διευκόλυνση στην ανάγνωση μιας IPv6 τα blocks από 0 (είτε στην αρχή είτε στο ενδιάμεσο) μπορούν να παραλειφθούν:
  - Π.χ. 2001 : 0db8 : 3c4d : 0015 : 0 : 0 : abcd : ef12

    2001 : 0db8 : 3c4d : 0015 : : abcd : ef12
- Localhost: : : 1

IPv6 – IPv4 Διευθύνσεις

- Στο IPv4 έχουμε τις **unicast, broadcast** και **multicast** διευθύνσεις.
- Στο IPv6 έχουμε τις **unicast, multicast** και **anycast** διευθύνσεις.
  - Οι broadcast διευθύνσεις αντικαθίστανται από τις multicast.

IPv6 – Unicast διευθύνσεις

- **Global unicast addresses**: Συμβατικές μοναδικές διευθύνσεις όπως και στο IPv4.
- **Link-local addresses**: Παρόμοιες με τις ιδιωτικές διευθύνσεις στο IPv4. Χρησιμοποιούνται μόνο σε ένα τοπικό δίκτυο (ή τμήμα αυτού), κυρίως για τη δημιουργία προσωρινών δικτύων (π.χ. Conference).
- **Unique local addresses**: Ίδιες με τις link-local μόνο που θα πρέπει να είναι μοναδικές μέσα σε ένα δίκτυο έτσι ώστε η σύνδεση δύο υποδικτύων να μη δημιουργεί πρόβλημα επικάλυψης διευθύνσεων.
- **Special addresses**: Loopback addresses και διευθύνσεις που χρησιμοποιούνται για μετάβαση από ένα IPv4 δίκτυο σε ένα IPv6.

Link στο IPv6

- **Το Link στο IPv6 ορίζεται ως εξής (RFC 4862):**

  μια διασύνδεση κατά την οποία οι κόμβοι επικοινωνούν χρησιμοποιώντας μόνο το επίπεδο ζεύξης δεδομένων. Παραδείγματα αποτελούν το Ethernet; PPP links; X.25, Frame Relay, ή ATM δίκτυα; καθώς και σήραγγες (tunnels) σε επίπεδο δικτύου (ή σε υψηλότερο).

IPv6 – Unicast διευθύνσεις

- **Η γενική μορφή των unicast διευθύνσεων είναι η ακόλουθη:**

bits	>=48	<=16	64
πεδίο	routing prefix	subnet id	interface identifier

O 64-bit interface identifier

- δημιουργείται αυτόματα από τη MAC διεύθυνση του interface με τη χρήση του τροποποιημένου EUI-64 format
- δίνεται από έναν DHCPv6 server
- δημιουργείται αυτόματα (τυχαία), ή
- δίνεται από τον διαχειριστή

Modified EUI-64

- Μια MAC διεύθυνση για να χρησιμοποιηθεί ως link local IPv6 διεύθυνση μετατρέπεται σε EUI-64:
  - με την προσθήκη του FF:FE στο μέσο της MAC διεύθυνσης, και
  - με την αντιστροφή της τιμής του bit Universal/Local (το 7ο σημαντικότερο bit) έτσι ώστε η τιμή 1 να σημαίνει καθολική διεύθυνση
- Παράδειγμα:
  - Η MAC διεύθυνση

    00:1C:BF:2F:C8:19 μετατρέπεται σε

    02:1C:BF:**FF:FE**:2F:C8:19

Multicast

- Πακέτα που στέλνονται σε μια multicast διεύθυνση διανέμονται σε όλες τις διευθύνσεις της ομάδας.
- Παρέχει έναν τρόπο broadcasting μόνο που τα δεδομένα θα τα παραλάβουν μόνο οι κόμβοι που είναι μέλος μιας ομάδας.
- Έτσι αποφεύγεται η άσκοπη διακίνηση δεδομένων σε κόμβους που δε θα έπρεπε να τα πάρουν (όπως με το broadcasting στο IPv4).

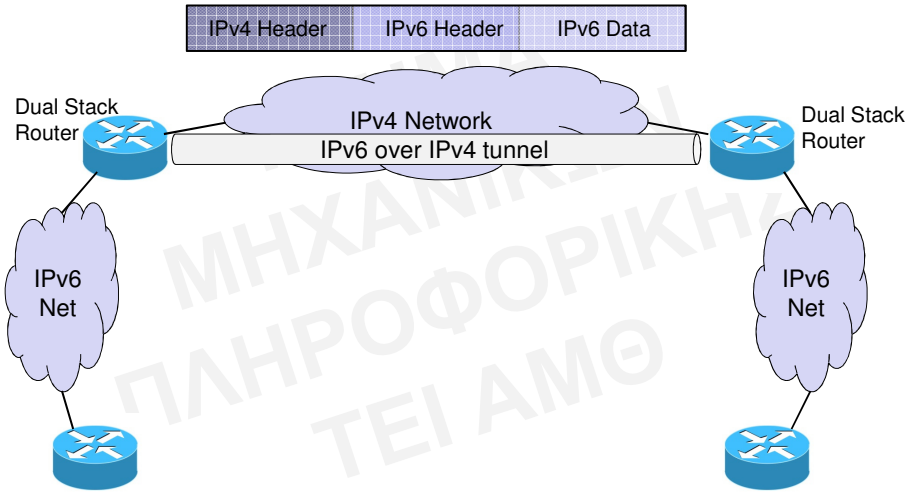
Anycast

- Πρόκειται για μοναδική διεύθυνση που δίνεται σε πολλούς κόμβους.
- **Ένα πακέτο που στέλνεται προς μια anycast διεύθυνση λαμβάνεται από τον πρώτο διαθέσιμο κόμβο στο μονοπάτι**.
  - Με αυτόν τον τρόπο διευκολύνεται το load balancing και παρέχεται ένα αυτόματο failover.

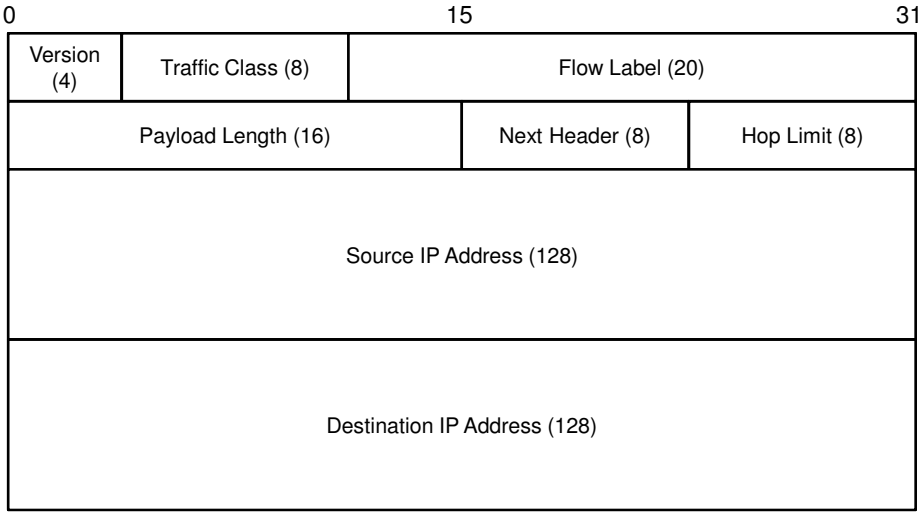
Μετάβαση στις IPv6 διευθύνσεις

- Συνύπαρξη IPv4 και IPv6:
  - Διπλή στοίβα (dual stack): Ο κάθε κόμβος υποστηρίζει και τις δύο εκδόσεις και αποφασίζει βάσει του πεδίου έκδοσης ποια θα χρησιμοποιήσει.
  - Σήραγγα (tunneling): Η μέθοδος αυτή χρησιμοποιείται για να αποσταλεί ένα πακέτο IPv6 μέσω ενός δικτύου που υποστηρίζει μόνο IPv4 ή ενός πακέτου IPv4 μέσω IPv6.

IPv6 over IPv4 Tunneling



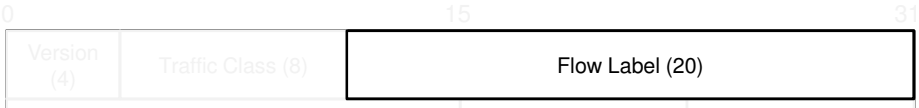
Επικεφαλίδα IPv6



Επικεφαλίδα IPv6

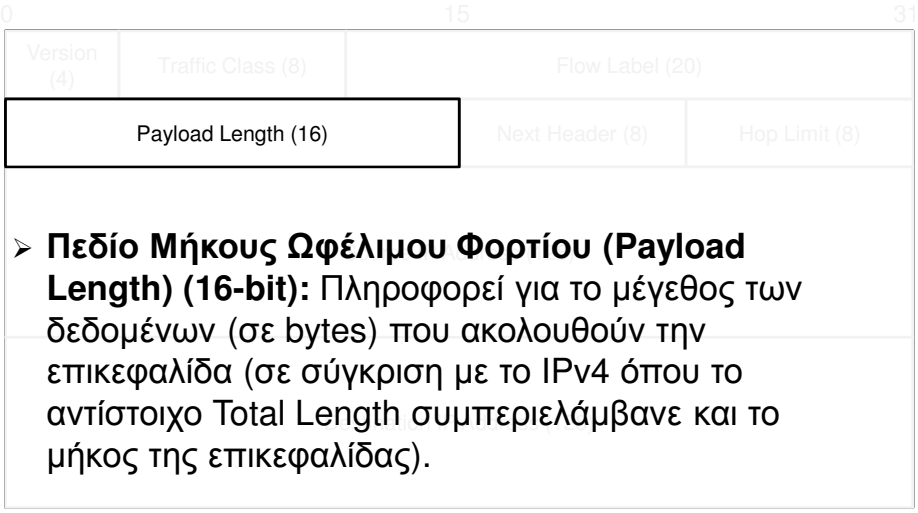
- **Πεδίο Έκδοσης (Version) 4bits**: Δηλώνει την έκδοση (6).
- **Πεδίο Κλάση Κίνησης (Traffic Class) 8bits**: χρησιμοποιείται για τη διάκριση των πακέτων σε αυτά των οποίων η ροή των πηγών τους μπορεί να ελεγχθεί και σε αυτά που δε μπορεί. Οι τιμές 0 εως 7 χρησιμοποιούνται για πηγές οι οποίες μπορούν να επιβραδυνθούν σε περίπτωση συμφόρησης. Οι τιμές από 8 εως 15 είναι για κίνηση πραγματικού χρόνου με σταθερό ρυθμό αποστολής ακόμη και αν τα πακέτα χάνονται (π.χ. ήχος, βίντεο). Αντικαθιστά το πεδίο Type of Service του IPv4.

Επικεφαλίδα IPv6



- **Πεδίο Ετικέτας Ροής (Flow Label) (20 bits):** Επιτρέπει στον αποστολέα και τον παραλήπτη να δημιουργήσουν μια ψευδο-σύνδεση με ιδιαίτερες ιδιότητες και απαιτήσεις. Η ετικέτα χρησιμοποιείται για να αναγνωρίσει τα πακέτα που αποτελούν μέρος μιας συγκεκριμένης ροής.

Επικεφαλίδα IPv6

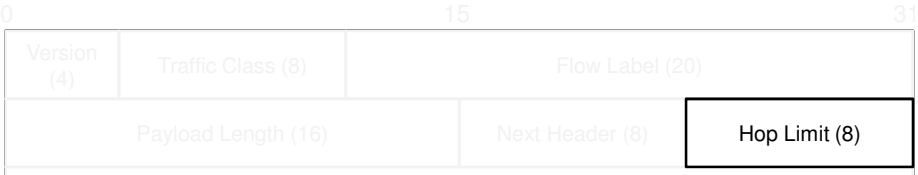


- **Πεδίο Μήκους Ωφέλιμου Φορτίου (Payload Length) (16-bit):** Πληροφορεί για το μέγεθος των δεδομένων (σε bytes) που ακολουθούν την επικεφαλίδα (σε σύγκριση με το IPv4 όπου το αντίστοιχο Total Length συμπεριελάμβανε και το μήκος της επικεφαλίδας).

Επικεφαλίδα IPv6

- **Πεδίο Επόμενης Επικεφαλίδας (Next Header) (8 bits):** Το IPv6 χρησιμοποιεί την έννοια των επικεφαλίδων επέκτασης (είναι παρόμοιες με τις προαιρετικές επικεφαλίδες που χρησιμοποιεί το IPv4) για να μεταφέρει πρόσθετες πληροφορίες. Χρησιμοποιούνται για να υποστηρίξουν λειτουργίες όπως **fragmentation, δρομολόγηση πηγής, και αυθεντικοποίηση**. Το πεδίο αυτό δηλώνει την ταυτότητα της επόμενης επικεφαλίδας**.**

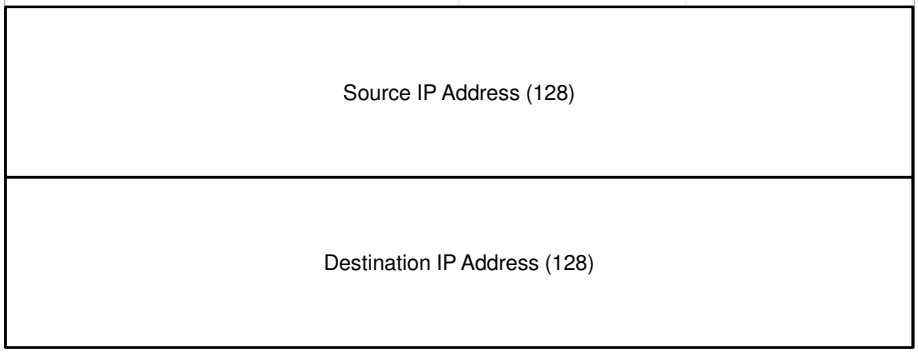
Επικεφαλίδα IPv6



- **Πεδίο Ορίου Βημάτων (Hop Limit) (8bits):** Αντικαθιστά το πεδίο Time-To-Live του IPv4. Σε αντίθεση με το IPv4 που μεταφράζει το πεδίο time-to-live ως ένα συνδυασμό βημάτων και μέγιστου χρόνου, το IPv6 μετράει μόνο βήματα και καθορίζει το μέγιστο αριθμό βημάτων που μπορεί να κάνει ένα δεδομενογράφημα πριν να απορριφθεί.

Επικεφαλίδα IPv6

- **Πεδία Διεύθυνσης Πηγής (Source Address) και Διεύθυνσης Προορισμού (Destination Address) (128bits η καθεμία):** Πληροφορεί για τις διευθύνσεις.



Fragment extension

- **Επικεφαλίδα επέκτασης τεμαχίου (Fragment Extension Header) (8 bytes):** Πληροφορεί για τυχόν τεμαχισμό ενός δεδομενογραφήματος.
  - Στο IPv6 όμως ο τεμαχισμός αφήνεται εξ'ολοκλήρου στην πηγή του δεδομενογραφήματος (σε αντίθεση με το IPv4 το οποίο απαιτεί κάθε δρομολογητής να τεμαχίσει κάθε δεδομενογράφημα που είναι πολύ μεγάλο για το MTU του δικτύου που θα ταξιδέψει)
  - Η πηγή θα πρέπει να χρησιμοποιήσει την **τεχνική της Ανακάλυψης MTU του Μονοπατιού (MTU Path Discovery)** για να βρει το μικρότερο MTU κατά μήκος της διαδρομής για τον παραλήπτη. Επομένως ο τεμαχισμός στο IPv6 είναι από άκρη σε άκρη και δεν εμπλέκονται καθόλου οι ενδιάμεσοι δρομολογητές.

Fragment extension

- **Επικεφαλίδα επέκτασης τεμαχίου (Fragment Extension Header) (8 bytes):** Περιέχει σχεδόν τις ίδιες πληροφορίες που συναντάμε και στο IPv4 όπως είναι το πεδίο ταυτότητας, το πεδίο more fragments, και το πεδίο θέσης τεμαχίου.
- **Επιπτώσεις της χρήσης της τεχνικής (MTU Path Discovery):**
  - \+ Αφαιρεί πολλή από την επιπλέον δουλειά που έχουν να κάνουν οι δρομολογητές όταν τεμαχίζουν ένα δεδομενογράφημα.
  - – Αλλάζει μια βασική ιδιότητα του Internet όπου ένα μονοπάτι παράδοσης ενός δεδομενογραφήματος μπορεί να αλλάξει κατά την πορεία. Με τόσο εύκολα λόγω της χρήσης του MTU του μονοπατιού. το IPv6 τα μονοπάτια δε μπορούν να αλλάξουν

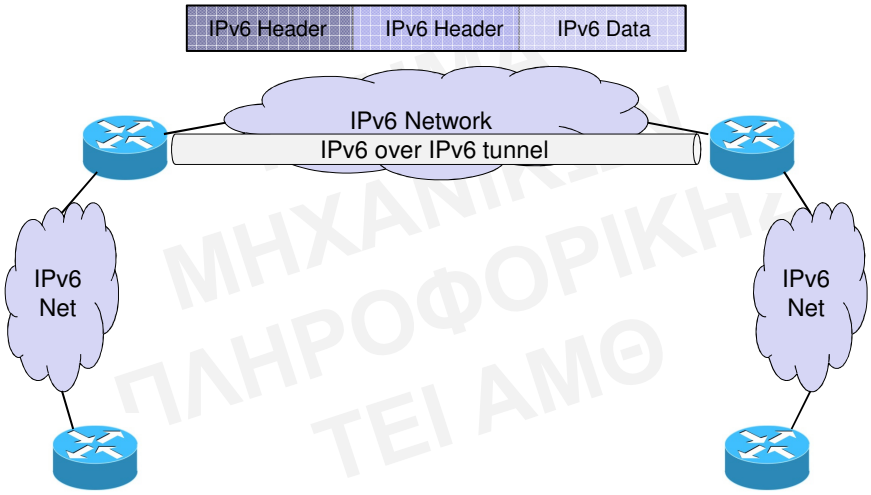
MTU Path Discovery

- **Πως αντιμετωπίζεται το πρόβλημα που προκύπτει από τη χρήση του MTU Path Discovery:** Το IPv6 επιτρέπει σε ενδιάμεσους δρομολογητές να χρησιμοποιήσουν τη μέθοδο της σήραγγας (tunnelling) για να περάσουν IPv6 δεδομενογραφήματα χρησιμοποιώντας IPv6.
- Εάν ένας δρομολογητής θέλει να τεμαχίσει ένα δεδομενογράφημα δεν εισάγει μια νέα επικεφαλίδα τεμαχίου, ούτε αλλάζει τα πεδία της βασικής επικεφαλίδας.

IPv6 Tunneling

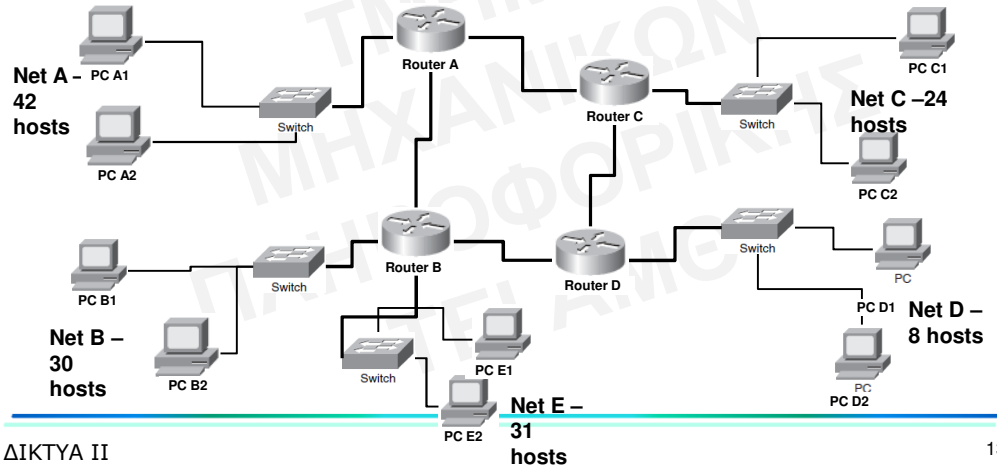
- Ο δρομολογητής δημιουργεί ένα νέο δεδομενογράφημα για να μεταφέρει το αρχικό ως δεδομένα στο νέο με την τεχνική της ενθυλάκωσης (encapsulation).
- Κατόπιν διαιρεί το νέο δεδομενογράφημα σε τεμάχια όπου αντιγράφει τη βασική επικεφαλίδα και εισάγει μια επικεφαλίδα επέκτασης σε κάθε ένα από αυτά.

IPv6 over IPv6 Tunneling



ΑΣΚΗΣΕΙΣ

- Να συμπληρωθούν τα στοιχεία που απαιτούνται για τη σωστή λειτουργία του δικτύου αν η διεύθυνση που έχουμε στη διάθεση μας είναι η 195.152.8.0/24. Να δοθούν διευθύνσεις στις δικτυακές συσκευές που απεικονίζονται. Οι δρομολογητές υποστηρίζουν VLSM.



ΔΙΚΤΥΑ ΙΙ

Δρομολόγηση & Αλγόριθμοι
Δρομολόγηση διανύσματος αποστάσεων

Δρομολόγηση

- Είναι η τεχνική που επιτρέπει την εύρεση ενός μονοπατιού και την προώθηση μέσω αυτού των δεδομένων που στέλνονται από τον αποστολέα στον παραλήπτη. Βέβαια το ζήτημα δεν είναι μόνο να βρεθεί ένα μονοπάτι αλλά και το καλύτερο.
  - Ποιο είναι το «καλύτερο» μονοπάτι;
- Κάθε δρομολογητής συνδέεται σε δύο ή περισσότερα φυσικά δίκτυα και προωθεί δεδομένα που έρχονται από τη μια σύνδεση προς κάποια άλλη.
- Αποτελεί την κύρια λειτουργία του επιπέδου δικτύου.

Δρομολόγηση

- Γίνεται από τους δρομολογητές βάσει του αλγορίθμου δρομολόγησης και των πληροφοριών δρομολόγησης.
  - **Πληροφορίες δρομολόγησης**: Πληροφορίες που αφορούν την τοπολογία και την κατάσταση (π.χ. καθυστερήσεις) του δικτύου.
  - **Αλγόριθμος δρομολόγησης**: Ο αλγόριθμος που χρησιμοποιείται για τη λήψη αποφάσεων για τη δρομολόγηση ενός πακέτου (ή δεδομενογραφήματος) βάσει των πληροφοριών δρομολόγησης.

Δρομολόγηση

- Κάθε δρομολογητής διατηρεί πληροφορίες, τυπικά σε ένα **πίνακα,** όσον αφορά το ποια διαδρομή πρέπει να ακολουθήσει το πακέτο που πρέπει να δρομολογήσει.
- Οι hosts διατηρούν μόνο δύο διαδρομές στους πίνακες δρομολόγησης:
  - τη διαδρομή για το τοπικό δίκτυο και
  - μια διαδρομή για έναν δρομολογητή που συνδέεται σε αυτό το δίκτυο
- Οι hosts στέλνουν όλα τα δεδομένα που δε προορίζονται στο τοπικό δίκτυο στον τοπικό δρομολογητή.

Δρομολόγηση

- Δρομολόγηση μπορούμε να έχουμε:
  - Μεταξύ ακραίου συστήματος (host) και δρομολογητή
  - Μεταξύ δρομολογητών.

Δρομολόγηση

- Ιδιότητες ενός αλγορίθμου δρομολόγησης:
  - **Ορθότητα** όσον αφορά τις αποφάσεις.
  - **Απλότητα** έτσι ώστε να υπάρχει αποδοτικότητα από τους δρομολογητές
  - **Ανθεκτικότητα** σε αλλαγές της τοπολογίας και της κίνησης
  - **Σταθερότητα** όσον αφορά την απόδοση του κάτω από οποιεσδήποτε συνθήκες (όχι όμως και των αποφάσεων του)
  - **Δικαιοσύνη**: δε μπορεί ο αλγόριθμος να στέλνει όλα τα πακέτα μόνο από μια γραμμή.
  - **Βελτιστοποίηση**: στην παράδοση των δεδομένων.

Δρομολόγηση

- Δύο κατηγορίες αλγορίθμων:
  - **Μη προσαρμοστικοί (Non-adaptive) – Παρέχουν στατική δρομολόγηση**
  - **Προσαρμοστικοί (Adaptive) – Παρέχουν δυναμική δρομολόγηση**

Non-adaptive

- Οι πληροφορίες δρομολόγησης λαμβάνονται υπόψη μόνο κατά τον αρχικό υπολογισμό και κατά τις αναθεωρήσεις (π.χ. λόγω αλλαγής της τοπολογίας, παρατήρησης μεγάλης καθυστέρησης κ.α.).
- Η υλοποίηση τους γίνεται συνήθως με τη χρήση πινάκων.

Adaptive

- Οι αποφάσεις παίρνονται δυναμικά βάσει των πληροφοριών που υπάρχουν για το δίκτυο την εκάστοτε χρονική στιγμή (τοπολογία, καθυστερήσεις). Διαφέρουν ως προς:
  - Την **προέλευση των πληροφοριών** (μόνο από τους γειτονικούς δρομολογητές, ή από όλους τους δρομολογητές σε ένα μονοπάτι)
  - Το **κάθε πότε αλλάζουν διαδρομή** (κάθε x sec, όταν αλλάζει η τοπολογία, βάσει καθυστερήσεων)
  - Το **κριτήριο βελτιστοποίησης** (απόσταση, αριθμός βημάτων, χρόνος μετάδοσης).

Στατική και δυναμική δρομολόγηση

- Στατική δρομολόγηση:
  - \+ Απλότητα
  - \+ Μικρό πρόσθετο φόρτο εργασίας για το δίκτυο.
  - – Μη ελαστική (αν υπάρξει κάπου μια βλάβη ενός δρομολογητή και δεν έχει δοθεί εναλλακτική διαδρομή τότε η δρομολόγηση θα είναι αδύνατη)
- Δυναμική δρομολόγηση:
  - \+ Αυτόματη λύση των προβλημάτων δρομολόγησης.
  - \+ Χρήση της τυπικά καλύτερης λύσης.
  - – Πρόσθετο φόρτο εργασίας για το δίκτυο.

Βελτιστοποίηση της δρομολόγησης

- Βελτιστοποίηση ως προς τι;
  - Το χρόνο καθυστέρησης;
  - Το σύνολο των πακέτων που μπορούν να εξυπηρετηθούν;
  - Τον αριθμό των βημάτων;
    Δεν είναι απαραίτητο ότι μειώνει και την καθυστέρηση
- Η μείωση του αριθμού των βημάτων φαίνεται να είναι η καλύτερη λύση.
- **Αρχή της βελτιστοποίησης**: Αν ο δρομολογητής *J* βρίσκεται πάνω στη βέλτιστη διαδρομή από το δρομολογητή *I* προς τον δρομολογητή *K*, τότε η βέλτιστη διαδρομή από τον *J* προς τον *K* επίσης βρίσκεται κατά μήκος της ίδιας διαδρομής.

Δρομολόγηση συντομότερης διαδρομής (shortest path)

- Χρησιμοποιεί τη θεωρία γράφων για να υπολογίσει τη συντομότερη διαδρομή μεταξύ δύο δρομολογητών. Ο κάθε κόμβος του γράφου τυπικά αναπαριστά έναν δρομολογητή.
- Αλγόριθμος Dijkstra. Χρησιμοποιείται κυρίως από συστήματα που κάνουν χρήση στατικής δρομολόγησης.
- Κριτήρια για τη συντομότερη διαδρομή:
  - Αριθμός των δρομολογητών που μεσολαβούν.
  - Γεωγραφική απόσταση.
  - Μέσος χρόνος καθυστέρησης.
  - Εύρος ζώνης.

Αλγόριθμος Dijkstra

- Σε κάθε κόμβο ανατίθεται μια μη αρνητική τιμή, που ονομάζεται **βάρος**, το άθροισμα των οποίων για όλους τους ενδιάμεσους κόμβους στο μονοπάτι καθορίζει και την αποτελεσματικότητα του μονοπατιού.
- Το βάρος μπορεί να προσδιορίζει απόσταση, καθυστέρηση ή και άλλα κριτήρια.
- Ο υπολογισμός μπορεί να γίνει και με τη χρήση συντελεστών βάρους για κάθε ένα από τα κριτήρια.

Δρομολόγηση βασισμένη στη ροή (flow based routing)

- Αν γνωρίζουμε την τοπολογία του δικτύου, τη χωρητικότητα και τη μέση ροή μιας δεδομένης γραμμής, μπορούμε να υπολογίσουμε τη μέση καθυστέρηση πακέτου στη γραμμή αυτή και κατ' επέκταση να βρούμε την ελάχιστη μέση καθυστέρηση για μια διαδρομή.
- Χρησιμοποιείται κυρίως από συστήματα που κάνουν χρήση στατικής δρομολόγησης.
- Κριτήρια δρομολόγησης: τοπολογία και ροή ή φορτίο στη γραμμή.

Επιλεκτική πλημμύρα (selective flooding)

- Οι δρομολογητές στέλνουν κάθε πακέτο σε όλες τις γραμμές οι οποίες κατευθύνονται προς το τελικό προορισμό.
  - Έχει το κόστος ότι γεμίζει το δίκτυο με πολλά ίδια πακέτα.
  - Το αποτέλεσμα είναι η χρήση και της συντομότερης διαδρομής (με μια μικρή επιβάρυνση που προκαλείται από την ύπαρξη πολλών ίδιων πακέτων μέσα στο δίκτυο).
- Χρησιμοποιείται από συστήματα στατικής δρομολόγησης.

Δρομολόγηση Διανύσματος Αποστάσεων (Distance Vector Routing)

- Κάθε δρομολογητής διατηρεί έναν πίνακα (διάνυσμα) που **δίνει τη βέλτιστη γνωστή απόσταση**, ή χρόνο που αντιστοιχεί σε κάθε προορισμό, καθώς **και το επόμενο βήμα** που πρέπει να χρησιμοποιηθεί.
- Εκμεταλλεύεται το γεγονός ότι ο κάθε δρομολογητής γνωρίζει πληροφορίες για τους γείτονες του.
- **Η ενημέρωση των πινάκων γίνεται με την ανταλλαγή πληροφοριών μεταξύ των γειτόνων και μόνο**.
- Οι δρομολογητές δε γνωρίζουν το πλήρες μονοπάτι για τον προορισμό.

Δρομολόγηση Διανύσματος Αποστάσεων (Distance Vector Routing)

- Ας υποθέσουμε ότι ο δρομολογητής μετρά βήματα μέχρι να φθάσει στο επιθυμητό δίκτυο. Πχ.

Προορισμός	Απόσταση	Επόμενο Βήμα
Κόμβος A	1	A
Κόμβος B	2	C
Κόμβος C	1	C
Κόμβος D	3	C

- Περιοδικά, ο κάθε δρομολογητής στέλνει μια αναφορά (ένα αντίγραφο του πίνακα δρομολόγησης) σε όλους τους γειτονικούς δρομολογητές (σε αυτούς με τους οποίους υπάρχει απευθείας σύνδεση).

Δρομολόγηση Διανύσματος Αποστάσεων (Distance Vector Routing)

- Όταν μία αναφορά φθάσει στο δρομολογητή *B* από τον *A*, ο *B* θα προσαρμόσει τον πίνακα του αν
  - ο Α ξέρει μία συντομότερη διαδρομή για κάποιο προορισμό, ή
  - ο Α έχει έναν προορισμό που ο Β δεν έχει στον πίνακα του, ή
  - ο Β δρομολογεί σε έναν προορισμό μέσω του Α και η απόσταση που δηλώνει ο Α έχει αλλάξει

Δρομολόγηση Διανύσματος Αποστάσεων (Distance Vector Routing)

- Π.χ. αν ο πίνακας που έχει ο Β είναι ο ακόλουθος:

Προορισμός	Απόσταση	Δρομολόγηση
Κόμβος A	1	A
Κόμβος D	1	D
Κόμβος C	8	D
Κόμβος H	2	A
Κόμβος E	7	D
Κόμβος F	3	D

και οι πληροφορίες που παίρνει από τον Α είναι οι ακόλουθες:

Προορισμός	Απόσταση
Κόμβος B	1
Κόμβος C	3
Κόμβος H	7
Κόμβος E	7
Κόμβος G	4

Δρομολόγηση Διανύσματος Αποστάσεων (Distance Vector Routing)

- Ο πίνακας του Β θα διαμορφωθεί ως ακολούθως:

Προορισμός	Απόσταση	Δρομολόγηση
Κόμβος A	1	A
Κόμβος D	1	D
Κόμβος C	4	A
Κόμβος H	8	A
Κόμβος E	7	D
Κόμβος F	3	D
Κόμβος G	5	A

Δρομολόγηση Διανύσματος Αποστάσεων (Distance Vector Routing)

- Προβλήματα: Συγκλίνει ο αλγόριθμος προς τη σωστή απάντηση? Δύο περιπτώσεις:
  - Όταν έχουμε πληροφορίες για έναν δρομολογητή
  - Όταν δεν έχουμε επειδή πιθανώς αυτός να βρίσκεται εκτός λειτουργίας.

Δρομολόγηση Διανύσματος Αποστάσεων (Distance Vector Routing)

- **Πρώτη περίπτωση**: Έστω το δίκτυο

- Έστω ότι ο Α είναι αρχικά εκτός λειτουργίας
  - όλοι οι υπόλοιποι κόμβοι θα έχουν καταχωρήσει το άπειρο ως τον απαιτούμενο αριθμό βημάτων για τον Α
- Όταν ο Α επανατεθεί σε λειτουργία οι υπόλοιποι κόμβοι θα ενημερωθούν μετά από 4 ανταλλαγές πινάκων.

Δρομολόγηση Διανύσματος Αποστάσεων (Distance Vector Routing)

- **Δεύτερη περίπτωση**: Θεωρούμε ότι όλοι οι κόμβοι είναι σε λειτουργία οπότε οι κόμβοι B, C, D και E θα έχουν καταχωρήσει τις τιμές 1, 2, 3 και 4 αντίστοιχα ως το μήκος των βημάτων που απαιτούνται για να φθάσουν στον A. Τι θα γίνει αν ο A τεθεί ξαφνικά εκτός λειτουργίας;

Count to infinity

- Ο B δεν ακούει από τον A οπότε και καταχωρεί το άπειρο.
- **Λαμβάνει ωστόσο από τον C την πληροφορία ότι υπάρχει μια διαδρομή για τον A που έχει μήκος 2 βήματα**.
- Ο B αλλάζει την καταχώρηση του σε 3 και ως επόμενο βήμα θα βάλει τον C.
- Στην επόμενη ανταλλαγή **ο C θα δει ότι ο B άλλαξε** την καταχώρηση σε 3 επομένως θα κάνει και αυτός την αντίστοιχη αλλαγή σε 4.
- Αν συνεχιστεί αυτή η αλλαγή πληροφοριών είναι προφανές ότι το μέτρημα θα συνεχιστεί μέχρι το άπειρο (για αυτό και το πρόβλημα ονομάζεται **μέτρημα προς το άπειρο**).

Ενημέρωση χωρισμένου ορίζοντα

- Αποτρέπει τη δημιουργία βρόχων όταν για τη δρομολόγηση χρησιμοποιείται ο αλγόριθμος διανύσματος αποστάσεων:
  - **Ο δρομολογητής δε μεταδίδει πληροφορίες δρομολόγησης στον κόμβο μέσω του οποίου γίνεται η δρομολόγηση.**
  - Π.χ. όταν ο Α τεθεί εκτός λειτουργίας,
    - ο Β θα ενημερώσει ότι ο Α δεν είναι διαθέσιμος
    - **ο C δε θα στείλει πίσω στον Β πληροφορίες για τον Α**.
    - ο Β αντιλαμβάνεται ότι δεν υπάρχει γείτονας που να μπορεί να φθάσει προς τον Α
    - στην επόμενη ανταλλαγή και ο C. Έτσι η πληροφορία για τον Α διαδίδεται πολύ πιο γρήγορα.

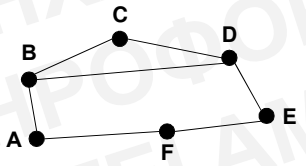
Ασκήσεις

- Οι πληροφορίες που έχει ο παρακάτω πίνακας είναι σωστές;

Προορισμός	Απόσταση	Δρομολόγηση
Κόμβος Α	1	Α
Κόμβος C	8	Α
Κόμβος D	2	C
Κόμβος E	7	F
Κόμβος F	3	D

Ασκήσεις

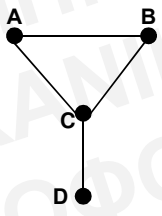
- Υποθέστε ότι στο παρακάτω υποδίκτυο όλοι οι κόμβοι είναι σε λειτουργία εκτός από τον Α. Περιγράψτε τα βήματα που θα ακολουθήσει ο αλγόριθμος δρομολόγησης διανύσματος αποστάσεων δίνοντας ταυτόχρονα τις τιμές που θα καταχωρηθούν στους πίνακες πριν τεθεί ο Α σε λειτουργία και μετά την ενεργοποίηση του. Υποθέτουμε ότι ο αλγόριθμος μετρά βήματα. Αν υπάρχει άμεση σύνδεση μεταξύ δύο κόμβων τότε το βήμα είναι 1.



- Εξετάστε αν θα αντιμετωπίσουμε το πρόβλημα του Μετρήματος προς το Άπειρο αν ο Α τεθεί εκτός λειτουργίας.

Ασκήσεις

- Στο παρακάτω υποδίκτυο βρίσκει εφαρμογή η λύση του χωρισμένου ορίζοντα αν ο D βγει εκτός λειτουργίας;



ΔΙΚΤΥΑ ΙΙ

Δρομολόγηση Κατάστασης Ζεύξεων

Δρομολόγηση διανύσματος αποστάσεων

- Η δρομολόγηση διανύσματος αποστάσεων αντιδρά αργά σε αλλαγές του δικτύου και απαιτεί ανταλλαγή μεγάλων μηνυμάτων.
- Τα μηνύματα ενημέρωσης της δρομολόγησης περιέχουν μια εγγραφή για κάθε πιθανό δίκτυο.
  - Μέγεθος μηνυμάτων ανάλογο του συνολικού αριθμού των δικτύων σε ένα διαδίκτυο
  - Σημαντικός ο όγκος των δεδομένων που ανταλλάσσονται
- Η εναλλακτική λύση είναι η **δρομολόγηση κατάστασης ζεύξεων (link state routing)**

Δρομολόγηση Κατάστασης Ζεύξεων (Link State Routing)

- **Πέντε βήματα** όπου ο κάθε δρομολογητής :
  - **ανακαλύπτει τους γείτονες του** μαθαίνοντας ταυτόχρονα τις διευθύνσεις δικτύου τους,
  - υπολογίζει την **καθυστέρηση ή το κόστος** για κάθε γείτονα,
  - κατασκευάζει ένα πακέτο που **πληροφορεί** αυτά που έχει μάθει,
  - στέλνει το πακέτο σε **όλους τους άλλους δρομολογητές**,
  - **υπολογίζει τη συντομότερη διαδρομή** προς κάθε άλλο δρομολογητή (ένας τρόπος είναι η χρήση του αλγορίθμου του Dijkstra).

Δρομολόγηση Κατάστασης Ζεύξεων – Βήματα

- **Μαθαίνοντας για τους γείτονες**:
  - Αποστολή πακέτων HELLO
  - Οι παραλήπτες ανταποκρίνονται δίνοντας στοιχεία για την ταυτότητα τους.
- **Μέτρηση τους κόστους γραμμής:**
  - Αποστολή ECHO πακέτων προς τους γειτονικούς δρομολογητές
    - Εάν ληφθεί υπόψη και το φορτίο ο υπολογισμός ξεκινά από τη στιγμή που το πακέτο μπει στην ουρά.
    - Ειδάλλως, ο υπολογισμός ξεκινά από τη στιγμή που το πακέτο φτάσει στην αρχή της ουράς.

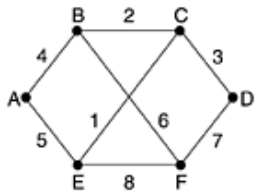
Υπολογισμός κόστους

- Θα πρέπει να συμπεριληφθούν οι καθυστερήσεις στον υπολογισμό του κόστους μιας γραμμής;

Δρομολόγηση Κατάστασης Ζεύξεων – Βήματα

- **Κατασκευή των πακέτων κατάστασης ζεύξεων**:
  - Ο κάθε δρομολογητής ετοιμάζει ένα πακέτο με όλες τις πληροφορίες:
    - ταυτότητα αποστολέα,
    - αύξοντα αριθμό,
    - ηλικία, και
    - λίστα με τους γείτονες καθώς και την καθυστέρηση προς κάθε έναν από αυτούς.
  - Τα πακέτα τυπικά κατασκευάζονται σε τακτά χρονικά διαστήματα ή όταν υπάρχει κάποια σημαντική αλλαγή.

Δρομολόγηση Κατάστασης Ζεύξεων – Πίνακες



(a)

Link State Packets

A	B	C	D	E	F
Seq.	Seq.	Seq.	Seq.	Seq.	Seq.
Age	Age	Age	Age	Age	Age
B 4	A 4	B 2	C 3	A 5	B 6
E 5	C 2	D 3	F 7	C 1	D 7
	F 6	E 1		F 8	E 8

(b)

Δρομολόγηση Κατάστασης Ζεύξεων – Βήματα

- **Διανομή των πακέτων κατάστασης ζεύξεων**:
  - Χρησιμοποιείται η τεχνική της πλημμύρας.
  - **Για να ελεγχθεί η πλημμύρα χρησιμοποιούνται αύξοντες αριθμοί**. Έτσι μπορεί ένας παραλήπτης να γνωρίζει αν έχει ήδη λάβει ένα πακέτο.

Δρομολόγηση Κατάστασης Ζεύξεων – Βήματα

- **Διανομή των πακέτων κατάστασης ζεύξεων.** Τροποποιήσεις που μπορούν να γίνουν για να βελτιωθεί ο αλγόριθμος είναι οι ακόλουθες:
  - Τα πακέτα πριν να δρομολογηθούν περιμένουν στο δρομολογητή για ένα μικρό χρονικό διάστημα. Όταν έρθει κάποιο πακέτο από την ίδια πηγή συγκρίνονται οι αύξοντες αριθμοί και γίνονται οι απαραίτητες τροποποιήσεις.
  - Γίνεται επαλήθευση όλων των πακέτων που φθάνουν στις γραμμές.

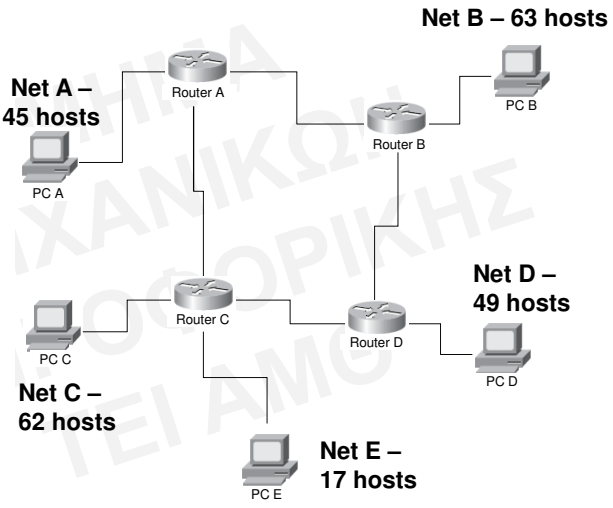
Δρομολόγηση Κατάστασης Ζεύξεων – Βήματα

- **Υπολογισμός των καινούργιων διαδρομών:** Με την συγκέντρωση των πακέτων ο δρομολογητής χρησιμοποιεί τον αλγόριθμο του Dijkstra για τον υπολογισμό των συντομότερων διαδρομών για όλες τις πιθανές κατευθύνσεις.
  - Προϋποθέτει την κατασκευή του αντίστοιχου γράφου.

Συνοπτικά

- **Δρομολόγηση διανύσματος αποστάσεων – Distance Vector Routing:** Προσδιορίζει την κατεύθυνση και την απόσταση προς οποιοδήποτε προορισμό στο διαδίκτυο (προσοχή στην έννοια του διαδικτύου)
- **Δρομολόγηση Κατάστασης Ζεύξεων – Link State Routing (γνωστό και ως Shortest Path First)**: Δημιουργεί την ακριβή τοπολογία του διαδικτύου, ή του τμήματος στο οποίο υπάγεται ο δρομολογητής

Έστω ότι η διεύθυνση που έχει ο διαχειριστής του δικτύου στη διάθεση του είναι η 111.2.24.0/23. Να δώσετε διευθύνσεις στα δίκτυα, τους hosts και τους routers που απεικονίζονται στο σχήμα. Λάβετε υπόψη ότι οι δρομολογητές υποστηρίζουν μάσκες μεταβλητού μεγέθους. Στον αριθμό των hosts συμπεριλαμβάνονται και οι συνδέσεις των δρομολογητών.



ΔΙΚΤΥΑ ΙΙ

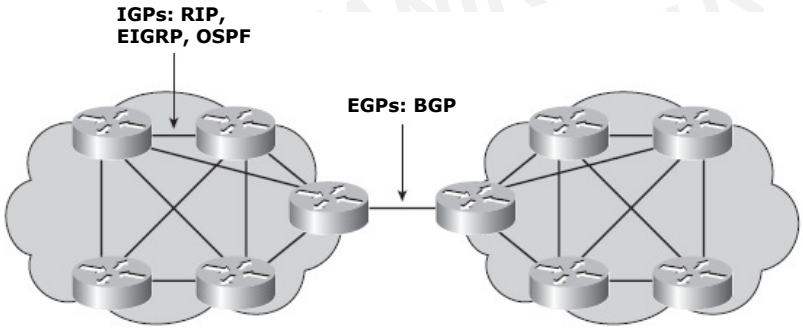
Δρομολόγηση στο TCP/IP

Δρομολόγηση στο TCP/IP

- **Αυτόνομο σύστημα**: το σύνολο δικτύων και δρομολογητών σε μια περιοχή:
  - Τυπικά ελέγχονται από μια αρχή διαχείρισης
  - Με κοινή πολιτική δρομολόγησης
- Το INTERNET αποτελεί μια συλλογή από αυτόνομα συστήματα.
- Η επιλογή των μηχανισμών δρομολόγησης μέσα σε ένα αυτόνομο σύστημα είναι ελεύθερη.
  - Ένας ή περισσότεροι δρομολογητές είναι υπεύθυνοι για τη μετάδοση των πληροφοριών πέραν των ορίων του συστήματος.

Δρομολόγηση στο TCP/IP

- Δύο δρομολογητές που ανταλλάσουν πληροφορίες λέγονται **εξωτερικοί γείτονες** εάν ανήκουν σε δύο διαφορετικά αυτόνομα συστήματα, και **εσωτερικοί γείτονες** εάν ανήκουν στο ίδιο αυτόνομο σύστημα.



Δρομολόγηση στο TCP/IP

- **Interior Gateway Protocols**: Χρησιμοποιούνται για την ανταλλαγή πληροφοριών δρομολόγησης εντός ενός αυτόνομου συστήματος
  - Routing Information Protocol (RIPv1, RIPv2)
  - Enhanced Interior Gateway Routing Protocol (EIGRP)
  - Open Shortest Path First (OSPF)
- **Exterior Gateway Protocols**: Χρησιμοποιούνται για να συνδέσουν αυτόνομα συστήματα
  - Border Gateway Protocol (BGPv4)
- **Η αρίθμηση των Αυτόνομων Συστημάτων αποτελεί αρμοδιότητα της IANA (Internet Assigned Numbers Authority – www.iana.org)**

Δρομολόγηση μεταξύ Αυτόνομων Συστημάτων

- **Πρωτόκολλο συνοριακών πυλών (Border Gateway Protocol – BGP)**
- Ανήκει σε μια κλάση πρωτοκόλλων **διανύσματος αποστάσεων** όπου όμως ο κάθε δρομολογητής δε καταχωρεί μόνο το κόστος για κάποιο προορισμό αλλά και τις λεπτομέρειες της δρομολόγησης για αυτόν τον προορισμό (**path vector routing**).
- Λαμβάνεται υπόψη η **πολιτική δρομολόγησης**.
  - Μπορεί κάποιο αυτόνομο σύστημα να μην επιθυμεί να αποτελεί έναν ενδιάμεσο σταθμό δρομολόγησης ακόμη και αν αυτή θα ήταν η συντομότερη διαδρομή μεταξύ δύο κόμβων.

Πρωτόκολλο Εξωτερικών Πυλών

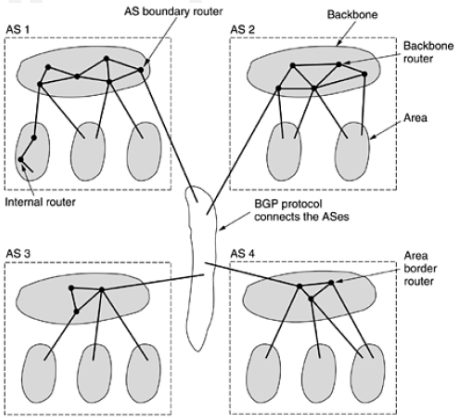
- Για τους σκοπούς του BGP χρησιμοποιούνται τρεις κατηγορίες δικτύων:
  - **Δίκτυα κλώνοι (stub networks)**: έχουν μόνο μια σύνδεση προς το υπόλοιπο δίκτυο (προς τα υπόλοιπα αυτόνομα συστήματα). Δρομολόγηση δε γίνεται ποτέ μέσω αυτών των δικτύων γιατί δε μπορούν να δρομολογήσουν διερχόμενη κίνηση.
  - **Πολλαπλώς συνδεδεμένα δίκτυα (multiconnected networks)**: Αυτά μπορούν να διαβιβάσουν πακέτα αλλά απλά το αρνούνται.
  - **Διαβιβαστικά δίκτυα (transit networks)**: Χρησιμοποιούνται για τη δρομολόγηση πακέτων άλλων αυτόνομων συστημάτων, πιθανώς με κάποιους περιορισμούς.

BGP

- Κατά την ανταλλαγή πληροφοριών οι δρομολογητές δε στέλνουν προς τους γείτονες τους το υπολογιζόμενο κόστος αλλά την **ακριβή διαδρομή** που χρησιμοποιεί.
- Από τις επιλογές που του προσφέρουν οι γείτονες του επιλέγει εκείνη με το **μικρότερο κόστος** εκτός και αν υπάρχει κάποιος περιορισμός.
- **Δεν αντιμετωπίζει το πρόβλημα μετρήματος προς το άπειρο** λόγω της πληροφόρησης για την ακριβή διαδρομή όταν ανταλλάσσουν πληροφορίες.
- Οι δρομολογητές που χρησιμοποιούν BGP επικοινωνούν χρησιμοποιώντας συνδέσεις TCP το οποίο εξασφαλίζει αξιοπιστία.

BGP

- Ο διαχειριστής του αυτόνομου συστήματος επιλέγει τουλάχιστον έναν κόμβο ο οποίος θα αποτελεί τον **εκπρόσωπο** των κόμβων για ολόκληρο το AS. Αυτοί οι εκπρόσωποι ανταλλάσουν πληροφορίες με άλλους εκπροσώπους σε άλλα αυτόνομα συστήματα.



BGP

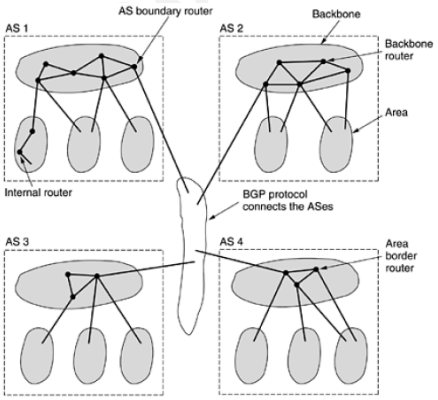
- Πως το BGP μας βοηθά στην επέκταση του Internet;
  - Ο αριθμός των κόμβων που λαμβάνουν μέρος στο BGP περιορίζεται στον αριθμό των αυτόνομων συστημάτων, ο οποίος είναι πολύ μικρότερος από τον πραγματικό αριθμό των δικτύων.
  - Η αναζήτηση μιας διαδρομής είναι στην ουσία μια αναζήτηση για την πύλη (δρομολογητή) που συνδέει το αυτόνομο σύστημα με άλλο αυτόνομο σύστημα. Ο περιορισμένος αριθμός των συνοριακών δρομολογητών καθιστά τη διαδικασία εφικτή.
  - Με αυτόν τον τρόπο η πολυπλοκότητα της δρομολόγησης μεταξύ ASs είναι παράγοντας του αριθμού των ASs ενώ η πολυπλοκότητα της δρομολόγησης εντός του AS είναι της τάξης του αριθμού των δικτύων που υπάρχουν μέσα σε αυτό το AS.

Interior Gateway Protocol – OSPF

- Βασίζεται στο πρωτόκολλο **κατάστασης ζεύξεων**:
  - Περιλαμβάνει **δρομολόγηση ανάλογα με τον τύπο της υπηρεσίας** χρησιμοποιώντας πολλαπλούς γράφους ανάλογα με την καθυστέρηση, διέλευση, αξιοπιστία.
  - Παρέχει **ισορρόπηση του φορτίου**

Interior Gateway Protocol – OSPF

- Επιτρέπει το διαχωρισμό ενός AS σε μικρότερα υποσύνολα που ονομάζονται **περιοχές (areas)**. Γνώση της τοπολογίας μιας περιοχής από μια άλλη δεν είναι απαραίτητη.
  - Κάθε AS έχει μια περιοχή **σπονδυλικής στήλης (backbone)** (περιοχή 0) στην οποία είναι συνδεδεμένες όλες οι περιοχές.
    - Η μετάβαση από μια περιοχή σε μια άλλη είναι δυνατή μέσω του backbone.
    - Κάθε δρομολογητής που είναι συνδεδεμένος με δύο ή περισσότερες περιοχές αποτελεί μέρος του backbone.



Interior Gateway Protocol – OSPF

- **Μέσα σε μια περιοχή κάθε δρομολογητής έχει την ίδια βάση δεδομένων των καταστάσεων ζεύξης και τρέχει τον ίδιο αλγόριθμο συντομότερης διαδρομής**.
  - Υπολογίζει τη διαδρομή από τον εαυτό του προς κάθε άλλο δρομολογητή της περιοχής συμπεριλαμβανομένου και του δρομολογητή που είναι συνδεμένος με τον σκελετό.
  - Ένας δρομολογητής που είναι συνδεμένος με δύο περιοχές χρειάζεται τις πληροφορίες και των δύο περιοχών και πρέπει να τρέξει τον αλγόριθμο της συντομότερης διαδρομής ξεχωριστά για κάθε μία.

Interior Gateway Protocol – OSPF

- Οι ανταλλαγές μεταξύ δρομολογητών πρέπει να είναι **αυθεντικοποιημένες**.
- Επιτρέπει στους διαχειριστές να περιγράψουν μια **εικονική τοπολογία** δικτύου η οποία αφαιρεί τις λεπτομέρειες των φυσικών συνδέσεων μέσα στο δίκτυο.
- Λαμβάνει υπόψη τις ανάγκες δικτύων πολλαπλής προσπέλασης με τη χρήση ενός **εκλεγμένου δρομολογητή** (designated router) ο οποίος στέλνει μηνύματα κατάστασης ζεύξεων εκ μέρους όλων των δρομολογητών που είναι συνδεδεμένοι στο δίκτυο.
- Ο εκλεγμένος δρομολογητής που ονομάζεται και **συνορεύων δρομολογητής** χρησιμοποιείται για να αποφεύγεται η ανταλλαγή πληροφοριών μεταξύ όλων των δρομολογητών.

Interior Gateway Protocol – OSPF

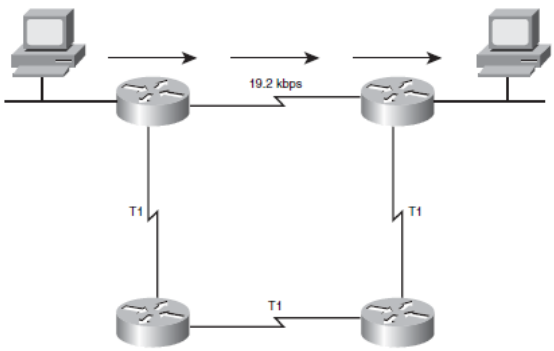
- Εξαιτίας του διαχωρισμού που κάνει το OSPF σε περιοχές διαχωρίζει και τους δρομολογητές σε τέσσερις κατηγορίες:
  - Οι **εσωτερικοί δρομολογητές** βρίσκονται σε μια περιοχή.
  - Οι **συνοριακοί δρομολογητές** συνδέουν δύο ή περισσότερες περιοχές.
  - Οι **δρομολογητές κορμού** βρίσκονται στην σπονδυλική στήλη.
  - Οι **ακραίοι δρομολογητές** συνδέουν δύο διαφορετικά αυτόνομα συστήματα.
- Κατά την κανονική λειτουργία μπορεί να χρειασθούν τρία είδη διαδρομών:
  - Εντός μιας περιοχής
  - Μεταξύ περιοχών
  - Μεταξύ AS.

Interior Gateway Protocol – OSPF

- Συνοπτική περιγραφή δρομολόγησης:
  - Ενημέρωση δρομολογητών περιοχής για τιμές κόστους και γείτονες με τη μέθοδο της πλημμύρας.
  - Ο κάθε δρομολογητής συνθέτει γράφο που απεικονίζει την περιοχή του (ή τις περιοχές για την περίπτωση που έχουμε κάποιο συνοριακό δρομολογητή). Το ίδιο ισχύει και για το σκελετό.
  - Οι δρομολογητές κορμού δέχονται πληροφορίες από τους συνοριακούς δρομολογητές ώστε να υπολογίσουν τη βέλτιστη διαδρομή προς οποιοδήποτε άλλο δρομολογητή.
  - Οι πληροφορίες αυτές περνάνε και στους συνοριακούς δρομολογητές οι οποίοι τις προωθούν σε όλους τους δρομολογητές των περιοχών τους.
  - Έτσι κάποιος δρομολογητής μιας περιοχής μπορεί να επιλέξει το δρομολογητή με τη συντομότερη διαδρομή.

Interior Gateway Protocol – RIP

- Routing Information Protocol – RIP: Είναι πρωτόκολλο διανύσματος αποστάσεων:
  - Ως απόσταση χρησιμοποιείται ο αριθμός των βημάτων
  - Το μονοπάτι που επιλέγεται είναι αυτό με τα λιγότερα βήματα.
  - Ωστόσο ενδέχεται να μην είναι και το συντομότερο



ΔΙΚΤΥΑ ΙΙ

Classless Routing

Classless Interdomain Routing

- Πρόκειται για μια τεχνική που αντιμετωπίζει δύο σημαντικά προβλήματα:
  - Την **ανάπτυξη των πινάκων δρομολόγησης** στους δρομολογητές της σπονδυλικής στήλης του Internet (οι οποίοι πρέπει να διατηρούν εγγραφές για όλα τα δίκτυα παγκοσμίως).
  - Την **εξάντληση των διευθύνσεων στο IPv4**. Το πρόβλημα αυτό προκύπτει από το γεγονός ότι χρειάζεται να αναθέτουμε διευθύνσεις σε τμήματα τριών διαφορετικών μεγεθών (των κλάσεων A,B και C). Έτσι, ένα δίκτυο με 2 μόνο υπολογιστές χρειάζεται μια διεύθυνση κλάσης C. Το πρόβλημα αυτό αντιμετωπίζεται εν μέρει με τη χρήση υποδικτύων.

CIDR

- Δίκτυα κλάσης C που αποκτούν πάνω από 255 hosts αναγκαστικά θα καταφύγουν στη χρήση μιας δεύτερης διεύθυνσης κλάσης C ή στη χρήση μιας διεύθυνσης κλάσης B.
- **Η χρήση πολλών διευθύνσεων κλάσης C για την κάλυψη του ίδιου δικτύου δημιουργεί μεγάλο πρόβλημα στους δρομολογητές οι οποίοι θα πρέπει να αποθηκεύσουν πολύ περισσότερες πληροφορίες για το ίδιο δίκτυο.**
- Π.χ., εάν ένα δίκτυο χρειαζόταν 16 διευθύνσεις κλάσης C τότε θα έπρεπε σε κάθε δρομολογητή της σπονδυλικής στήλης να υπάρχουν 16 εγγραφές για αυτό το δίκτυο. Εάν χρησιμοποιούσαμε μια διεύθυνση κλάσης B τότε θα χρησιμοποιούνταν μόνο οι 16x255 = 4080 από τις 65,536 διαθέσιμες διευθύνσεις host.

CIDR

- Το **Classless InterDomain Routing – CIDR** (ή **supernetting**) προσπαθεί να εξισορροπήσει την επιθυμία για ελαχιστοποίηση των διαδρομών τις οποίες πρέπει να γνωρίζει ένας δρομολογητής για ένα δίκτυο και την ανάγκη για σωστή διαχείριση των διευθύνσεων.
- **Επιτρέπει να χρησιμοποιήσουμε μια μόνο εγγραφή σε έναν πίνακα δρομολόγησης για να μας πληροφορήσει για τον τρόπο με τον οποίο θα προσπελάσουμε πολλά διαφορετικά δίκτυα.**
  - **Σπάει τα αυστηρά όρια που υπάρχουν μεταξύ των διευθύνσεων διαφορετικής κλάσης**.
  - Οι δρομολογητές δε δρομολογούν βάσει των κλάσεων αλλά βάσει των αριθμών bits που αντιπροσωπεύουν τη διεύθυνση δικτύου.

Classful, Classless και Routing Protocols

- Classful Routing:
  - Τα RIPv1 και IGRP δεν υποστηρίζουν subnetting (π.χ. VLSM) ή supernetting – CIDR.
- Classless Routing:
  - Τα RIPv2, EIGRP και OSPF, BGP-4 υποστηρίζουν subnetting (π.χ. VLSM) και supernetting – CIDR.

CIDR

- Έστω ότι έχουμε ένα δίκτυο το οποίο χρειάζεται 16 διευθύνσεις κλάσης C. Αντί να δοθούν 16 τυχαίες διευθύνσεις σε αυτό το δίκτυο, μπορούν να δοθούν 16 συνεχείς διευθύνσεις κλάσης C.
- Έστω οι διευθύνσεις 192.4.16.0 εως 192.4.31.0. Τα πρώτα 20 bits είναι όλα τα ίδια. Με αυτόν τον τρόπο έχουμε καταφέρει να "δημιουργήσουμε" έναν αριθμό δικτύου ο οποίος βρίσκεται μεταξύ ενός αριθμού κλάσης B και ενός αριθμού κλάσης C.
- Με άλλα λόγια, καταφέρνουμε να καλύψουμε ένα δίκτυο χρησιμοποιώντας πολλές διευθύνσεις κλάσης C χωρίς να χρησιμοποιούμε διεύθυνση κλάσης B και παράλληλα να χρησιμοποιήσουμε μια μόνο εγγραφή για τους πίνακες δρομολόγησης.

CIDR

- Για να μπορέσει να δουλέψει αυτό το σχήμα θα πρέπει να δίνονται μπλοκς από διευθύνσεις κλάσης C οι οποίες μοιράζονται ένα κοινό πρόθεμα. **Κάθε μπλοκ διευθύνσεων θα πρέπει να περιέχει έναν αριθμό από δίκτυα κλάσης C ο οποίος να είναι δύναμη του 2.**
- Οι δρομολογητές θα πρέπει να μπορούν να χειρίζονται διευθύνσεις που δεν ανήκουν σε μια συγκεκριμένη κλάση.

Δρομολόγηση σύμφωνα με το CIDR

- Όταν κάνουμε χρήση του CIDR δεν εξετάζουμε μόνο τη διεύθυνση του δικτύου για να τη συγκρίνουμε με κάποια εγγραφή στον πίνακα δρομολόγησης.
- **Ενδέχεται στον πίνακα δρομολόγησης να υπάρχουν προθέματα τα οποία αλληλεπικαλύπτονται, με την έννοια ότι κάποιες διευθύνσεις μπορεί να ταιριάζουν σε περισσότερα από ένα προθέματα.**
- Π.χ. στον πίνακα δρομολόγησης ενός δρομολογητή μπορεί να βρούμε τόσο το 171.69.0.0/16 όσο και το 171.69.10.0/24. Σε μια τέτοια περίπτωση το πακέτο με διεύθυνση προορισμού το 171.69.10.5 ταιριάζει και στα δύο προθέματα.

Δρομολόγηση σύμφωνα με το CIDR

- Ο κανόνας δρομολόγησης σε αυτήν την περίπτωση βασίζεται στην αρχή του **"μεγαλύτερου προθέματος" (longest prefix)**.
  - Έτσι η διεύθυνση 171.69.10.5 θα δρομολογηθεί σύμφωνα με την εγγραφή για το πρόθεμα 171.69.10.0/24.
  - Η διεύθυνση 171.69.20.5 ταιριάζει μόνο στο 171.69.0.0/16 και έτσι αυτή η εγγραφή θα χρησιμοποιηθεί για τη δρομολόγηση του.

ΑΣΚΗΣΕΙΣ

- Έστω ότι ένας δρομολογητής χρησιμοποιεί πρωτόκολλο που υποστηρίζει classless routing και χρησιμοποιεί τον παρακάτω πίνακα δρομολόγησης. Περιγράψτε τι θα κάνει ο δρομολογητής με ένα πακέτο που στέλνεται σε κάθε μια από τις διευθύνσεις:
  - 136.79.55.65
  - 136.79.55.137
  - 176.79.45.40
  - 176.79.45.194
  - 193.5.12.130
  - 193.5.12.225

Δίκτυο	Επόμενος κόμβος
136.79.55.0/25	R0
136.79.55.128/26	R1
176.79.45.128/26	R2
193.5.12.192/27	R3
Default	R4

ΑΣΚΗΣΕΙΣ

- Έστω ότι θέλουμε να αναθέσουμε μια διεύθυνση δικτύου σε ένα δίκτυο που αποτελείται από 400 hosts.
  - Πόσες διευθύνσεις hosts σπαταλούνται εάν χρησιμοποιήσουμε μια διεύθυνση κλάσης Β για να καλύψουμε αυτές τις διευθύνσεις?
  - Έστω ότι ο πάροχος υπηρεσιών αυτού του δικτύου έχει στη διάθεση του τις διευθύνσεις από 207.21.51.0 έως και 207.21.60.0. Δώστε κάποιες διευθύνσεις που θα μπορούσαν να χρησιμοποιηθούν για αυτό το σκοπό και με ποιο τρόπο.

ΑΣΚΗΣΕΙΣ

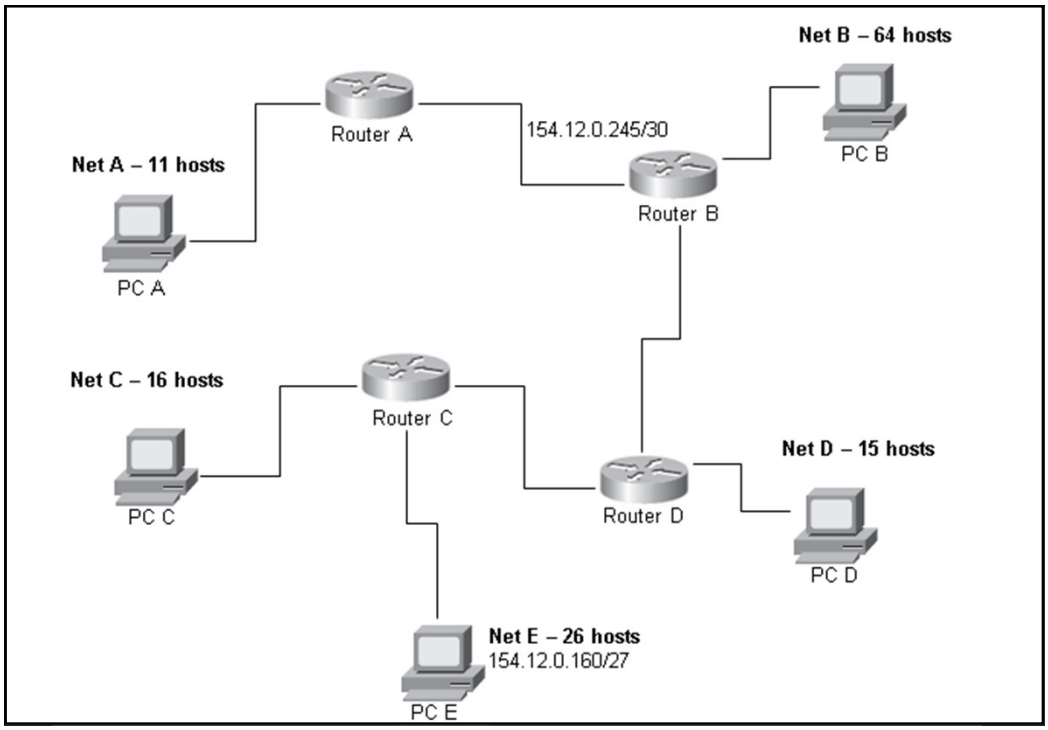
- Έστω ότι θέλουμε να διευθυνσιοδοτήσουμε έναν οργανισμό με 1400 hosts και έχουμε στη διάθεση μας τις διευθύνσεις 192.12.7.0-192.12.23.255.
  - Ορίστε τις διευθύνσεις που θα χρησιμοποιήσετε έτσι ώστε να διευκολυνθεί η λειτουργία των δρομολογητών στο μέγιστο δυνατό.
  - Αν από τους 1400 hosts είχαν ανάγκη πρόσβασης στο διαδίκτυο μόνο οι 400 θα άλλαζε τίποτα στην επιλογή σας?
  - Για τις διευθύνσεις που έχετε επιλέξει ορίστε τις διευθύνσεις δικτύων και τις μάσκες υποδικτύων ώστε να καλυφθούν 16 υποδίκτυα.

ΑΣΚΗΣΕΙΣ

- Έστω ότι θέλουμε να διευθυνσιοδοτήσουμε έναν οργανισμό με 1300 hosts και έχουμε στη διάθεση μας τις διευθύνσεις 192.12.160.0/20.
  - Ορίστε τις διευθύνσεις που θα χρησιμοποιήσετε έτσι ώστε να διευκολυνθεί η λειτουργία των δρομολογητών στο μέγιστο δυνατό.
- Δρομολογητής χρησιμοποιώντας το CIDR πρωτόκολλο δρομολογεί τις διευθύνσεις που περιλαμβάνει η εγγραφή 180.128.0.0/12 από μια γραμμή Α και θέλει να αρχίσει να δρομολογεί τις διευθύνσεις 180.131.0.0 – 180.136.255.255 καθώς και τις διευθύνσεις 180.142.0.0 – 180.146.255.255 από μια γραμμή Β. Ποιες είναι οι καλύτερες δυνατές αλλαγές που θα πρέπει να κάνει ο δρομολογητής στις εγγραφές του πίνακα του έτσι ώστε να πετύχει το επιθυμητό αποτέλεσμα με το μικρότερο δυνατό κόστος;

ΑΣΚΗΣΕΙΣ

- Έστω ότι ο διαχειριστής των δικτύων που απεικονίζονται στο σχήμα έχει στη διάθεση του τη διεύθυνση 154.12.0.0/24. Αν υποθέσουμε ότι οι τιμές του Net E και του Router B (στο interface του με τον router A) είναι σωστές, να συμπληρωθούν οι τιμές που λείπουν για τα δίκτυα, τους hosts, και τους routers. Λάβετε υπόψη ότι οι δρομολογητές υποστηρίζουν μάσκες μεταβλητού μεγέθους. Στον αριθμό των hosts συμπεριλαμβάνονται και οι συνδέσεις των δρομολογητών



ΑΣΚΗΣΕΙΣ

- Δρομολογητής χρησιμοποιώντας το CIDR πρωτόκολλο δρομολογεί τις διευθύνσεις που περιλαμβάνει η εγγραφή 145.224.0.0/12 από μια γραμμή Α και θέλει να αρχίσει να δρομολογεί τις διευθύνσεις 145.220.0.0 – 145.226.255.255 καθώς και τις διευθύνσεις 145.230.0.0 – 145.242.255.255 από μια γραμμή Β. Ποιες είναι οι καλύτερες δυνατές αλλαγές που θα πρέπει να κάνει ο δρομολογητής στις εγγραφές του πίνακα του έτσι ώστε να πετύχει το επιθυμητό αποτέλεσμα με το μικρότερο δυνατό κόστος;

ΔΙΚΤΥΑ ΙΙ

Πρωτόκολλα επιπέδου μεταφοράς
User Datagram Protocol
Transmission Control Protocol

User Datagram Protocol – UDP

- **Μηχανισμός αποστολής δεδομενογραφημάτων**
- Μαζί με το TCP αποτελούν τα βασικά πρωτόκολλα του επιπέδου μεταφοράς.
- Δίνει έμφαση στην απόδοση παρά στην αξιοπιστία.
- **Χρησιμοποιεί θύρες (ports)** για να προσδιορίσει τις υπηρεσίες τις οποίες αφορούν τα δεδομένα.
  - Μηχανισμός αναγνώρισης υπηρεσιών
  - 16-bit αριθμός (η αρίθμηση ελέγχεται από την IANA)
    - 0-1023: για συγκεκριμένες γνωστές υπηρεσίες
    - 1024-49151: για υπηρεσίες ελεγχόμενες από την IANA
    - 49152-65535: διαθέσιμες για κάθε σκοπό

Ports

- **7: echo**
- **21: FTP**
- **22: SSH**
- **23: Telnet**
- **25: SMTP**
- **80: WWW – Http**
- **110: POP3**
- **143: IMAP**
- **119: Network News Transfer Protocol**
- **443: https**

...http://www.iana.org/assignments/port-numbers

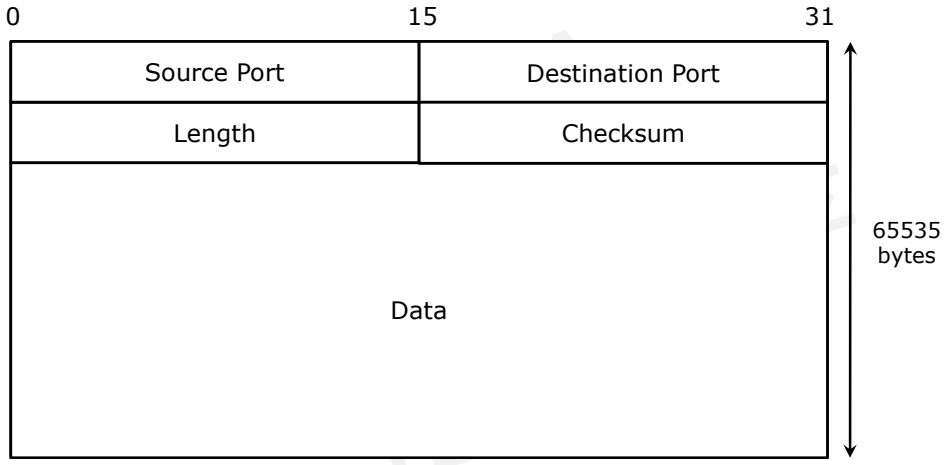
UDP

- Χρησιμοποιεί το IP πρωτόκολλο για να μεταφέρει τα μηνύματα.
- Χαρακτηριστικά:
  - **Μη αξιόπιστη και χωρίς σύνδεση** υπηρεσία.
  - **Δε χρησιμοποιεί επαληθεύσεις**
  - **Δε βάζει στη σωστή σειρά τα μηνύματα** που παραλαμβάνει.
  - **Δε δίνει πληροφορίες για τον έλεγχο του ρυθμού ροής** των δεδομένων.
- Ως αποτέλεσμα :
  - Μηνύματα μπορεί να χαθούν ή να φτάσουν ελλιπή.
  - Να φθάσουν με λάθος σειρά.
  - Να φθάνουν στον παραλήπτη γρηγορότερα από ότι αυτός μπορεί να τα επεξεργαστεί.

UDP

- Δομή δεδομενογραφήματος:
  - Αποτελείται από μια επικεφαλίδα (4 πεδία των 16bits το καθένα) και τα δεδομένα.
  - Η επικεφαλίδα περιλαμβάνει:
    - **Θύρα πηγής**: Είναι προαιρετική. Εάν δεν υπάρχει πρέπει να είναι 0 (σημαίνει ότι ο αποστολέας δε περιμένει απάντηση).
    - **Θύρα προορισμού**
    - **Μήκος μηνύματος**: Περιλαμβάνει τα 8 bytes της επικεφαλίδας και τα δεδομένα
    - **Άθροισμα ελέγχου**. Προαιρετικό για το IPv4, υποχρεωτικό για το IPv6. Όταν δε χρησιμοποιείται έχει τη τιμή 0.

UDP



Transmission Control Protocol – TCP

- Αποτελεί το άλλο βασικό πρωτόκολλο του επιπέδου μεταφοράς.
- Γιατί χρειαζόμαστε αξιόπιστη μεταφορά;
  - Απαιτείται από τις εφαρμογές
  - Να καλύψουμε την έλλειψη αξιοπιστίας σε χαμηλότερα επίπεδα.
  - **Πακέτα μπορεί να χαθούν ή να καταστραφούν** όταν υπάρχουν σφάλματα στη μετάδοση, όταν το υλικό αποτυγχάνει, ή όταν τα δίκτυα υπερφορτώνονται.
  - Τα δίκτυα που κάνουν δυναμική δρομολόγηση πακέτων μπορεί να τα παραδώσουν με **λάθος σειρά**, μετά από αρκετή **χρονική καθυστέρηση**, ή να τα παραδώσουν **διπλά**.

TCP

- Ιδιότητες της υπηρεσίας αξιόπιστης μεταφοράς:
  - **Stream Orientation**: Η υπηρεσία παράδοσης συρμού στον προορισμό θα δώσει ακριβώς την ίδια ακολουθία δεδομένων τα οποία στέλνει ο αποστολέας.
  - **Virtual Circuit Connection**: Η δημιουργία εικονικού κυκλώματος μεταξύ αποστολέα και παραλήπτη παρέχει όλες τις ιδιότητες μιας αξιόπιστης επικοινωνίας.
  - **Μεταφορά με χρήση προσωρινού καταχωρητή (Buffered Transfer)**: Μπορεί να συγκεντρώνει αλλά και να τεμαχίζει δεδομένα των εφαρμογών έτσι ώστε να κάνει πιο αποτελεσματική χρήση του δικτύου.

TCP

- Ορίζει:
  - Τη **δομή** των **δεδομένων** και των **επαληθεύσεων**
  - Πως το λογισμικό **διαχωρίζει μεταξύ πολλαπλών υπηρεσιών** σε έναν συγκεκριμένο σταθμό.
  - Πως οι δύο οντότητες **αρχικοποιούν μια μεταφορά συρμού** και πως **συμφωνούν όταν έχει ολοκληρωθεί**.
- Δε κάνει καμιά παραδοχή όσον αφορά το υφιστάμενο σύστημα επικοινωνίας

Χαρακτηριστικά του TCP

- **Παροχή αξιοπιστίας**: Με την τεχνική της **θετικής επαλήθευσης με επαναμετάδοση**:
  - Η ορθή λήψη δεδομένων επιβεβαιώνεται με μια θετική επαλήθευση.
  - Η επαλήθευση είναι απαραίτητη για να προχωρήσει ο αποστολέας στα επόμενα δεδομένα.
  - Η έγκαιρη λήψη της επαλήθευσης ελέγχεται με χρονομετρητή. Με τη λήξη του γίνεται επαναποστολή των δεδομένων.
  - Για την αποφυγή αντιγράφων χρησιμοποιούνται αύξοντες αριθμοί τόσο στα πακέτα όσο και στις επαληθεύσεις.

Χαρακτηριστικά του TCP

- Για να γίνει καλύτερη χρήση της γραμμής μετάδοσης χρησιμοποιείται η **τεχνική του ολισθαίνοντος παραθύρου** όπου
  - ο αποστολέας μπορεί να μεταδώσει πολλά πακέτα πριν να πάρει μια επαλήθευση.
  - τα πακέτα που μπορεί να μεταδώσει ο αποστολέας σε μια χρονική στιγμή αποτελούν το **παράθυρο του αποστολέα**.
  - τα πακέτα που μπορεί να παραλάβει ο παραλήπτης αποτελούν το **παράθυρο του παραλήπτη**.
  - ο αριθμός των πακέτων τα οποία δε χρειάζεται να έχουν επαληθευτεί σε μια χρονική στιγμή περιορίζεται από το μέγεθος του παραθύρου.

TCP

- Χρησιμοποιεί θύρες για να δηλώσει τον απόλυτο προορισμό σε ένα σταθμό και την **έννοια της σύνδεσης** για να αναγνωρίζει κάποιο αντικείμενο σε ένα σταθμό αντί της θύρας.
  - Μια σύνδεση αναγνωρίζεται μοναδικά από ένα **ζεύγος τελικών σημείων**:
  - Τελικό σημείο: το **ζεύγος (IP, θύρα)**
- Έτσι μια συγκεκριμένη TCP θύρα μπορεί να μοιραστεί από πολλές συνδέσεις στον ίδιο σταθμό. Π.χ., μπορούμε να έχουμε ταυτόχρονα τις συνδέσεις

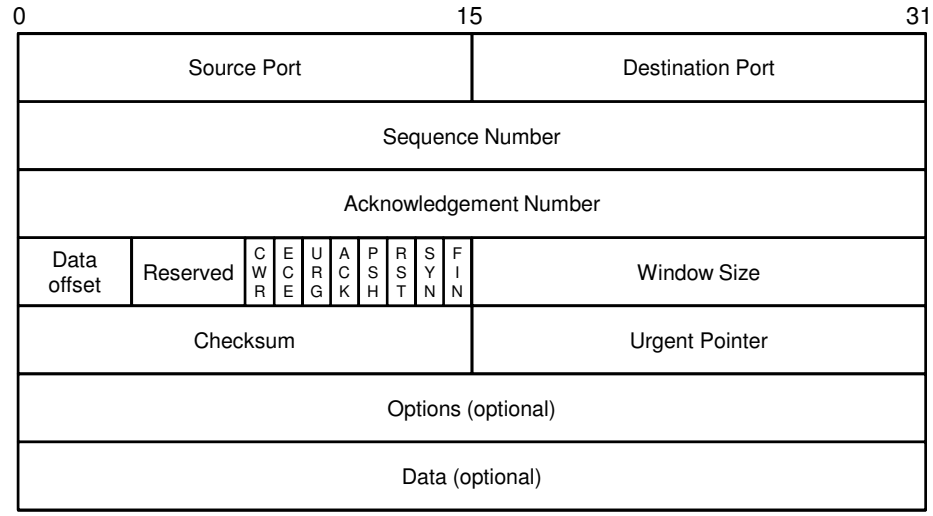
  (109.1.2.3, 1112), (224.1.2.3, 26) και

  (115.3.2.1, 2112), (224.1.2.3, 26)

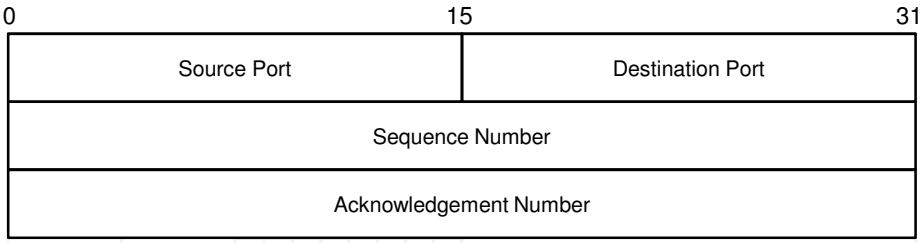
TCP

- Τα δύο τελικά σημεία θα πρέπει να συμφωνήσουν στη δημιουργία της σύνδεσης.
- Η μονάδα των δεδομένων που ανταλλάσσεται σε αυτό το επίπεδο ονομάζεται **segment** (τεμάχιο). Συνήθως κάθε τεμάχιο μεταφέρεται με ένα μόνο IP δεδομενογράφημα.

TCP



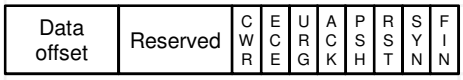
TCP



- Θύρες πηγής και προορισμού
- Αύξων αριθμός τεμαχίου (32 bits): δίνει τη θέση του πρώτου byte αυτού του τμήματος των δεδομένων στο συνολικό συρμό δεδομένων.
- Αριθμός επαλήθευσης (32 bits): ο αριθμός του **επόμενου byte** που περιμένει ο παραλήπτης. Επιβεβαιώνει την ορθή λήψη όλων των προηγούμενων.

TCP

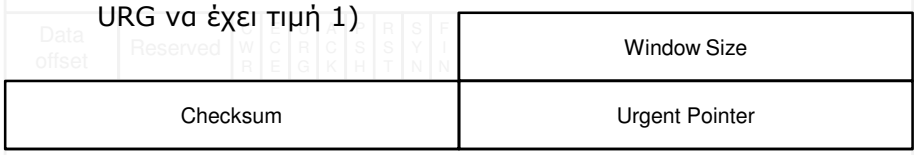
- Data offset: Μήκος της επικεφαλίδας τεμαχίου σε 32-bit words
- Code Bits (6 bits): Χρησιμοποιείται για να δηλώσει το περιεχόμενο και το σκοπό του τεμαχίου. Μπορεί να δηλώσει τα παρακάτω:
  - **CWR, ECE**: Χρησιμοποιούνται για τον έλεγχο της ροής σε περίπτωση που υπάρχει συμφόρηση και αν υποστηρίζεται από τους κόμβους



  - **URG**: Επείγον
  - **ACK**: Το πεδίο της επαλήθευσης είναι σημαντικό.
  - **PSH (PUSH)**: Αιτείται τη μεταφορά των δεδομένων ακόμα και αν δεν ζητούνται από τον παραλήπτη.
  - **RST**: Επανεκκινεί τη σύνδεση
  - **SYN**: Συγχρονίζει τους αύξοντες αριθμούς.
  - **FIN**: Ο αποστολέας δεν έχει άλλα δεδομένα να στείλει.

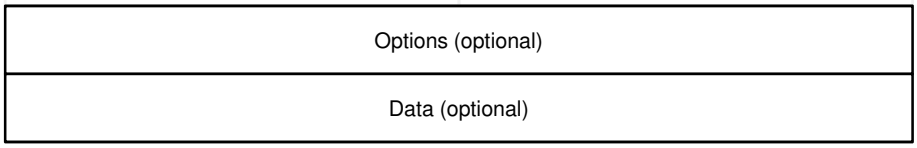
TCP

- **Window Size**: Δηλώνει το μέγεθος του προσωρινού καταχωρητή του παραλήπτη και κατ' επέκταση πόσα bytes μπορεί ο παραλήπτης να δεχτεί.
- **Checksum**: Άθροισμα ελέγχου επικεφαλίδας και δεδομένων
- **Urgent Pointer**: Προσδιορίζει σε ποιο σημείο (offset) αυτού του segment τελειώνουν τα urgent data (θα πρέπει η σημαία URG να έχει τιμή 1)



TCP

- **Options**: Μεταφέρουν διάφορες πληροφορίες είτε κατά την έναρξη της σύνδεσης είτε κατά τη διάρκεια της, μεταξύ των οποίων είναι το Maximum Segment Size και Window Scale



Maximum Segment Size

- Όλα τα τεμάχια που ανταλλάσσονται σε μια σύνδεση δεν είναι του ίδιου μεγέθους.
  - Ωστόσο, **οι δύο σταθμοί πρέπει να συμφωνήσουν στο μέγιστο μέγεθος ενός τεμαχίου.**
  - Χρησιμοποιούν το πεδίο OPTIONS για να δηλώσουν το μέγιστο μέγεθος τεμαχίου (maximum segment size ή MSS) το οποίο είναι διατεθειμένος ο σταθμός να δεχτεί.

TCP – MSS

- **Η σωστή επιλογή του MSS αποτελεί ένα σημαντικό παράγοντα για τη αποτελεσματική χρήση του δικτύου**.
  - Εάν οι δύο σταθμοί βρίσκονται στο ίδιο φυσικό δίκτυο το MSS επιλέγεται τέτοιο ώστε το IP δεδομενογράφημα που προκύπτει να ταιριάζει στο MTU του δικτύου.

    MSS = MTU - sizeof(TCPHDR) - sizeof(IPHDR)

  - Εάν βρίσκονται σε διαφορετικό φυσικό δίκτυο τότε θα προσπαθήσουν να βρούνε το ελάχιστο MTU στο μονοπάτι μεταξύ των σταθμών ή θα επιλέξουν ως MSS το 536 (το default μέγεθος ενός IP δεδομενογραφήματος).
- **Το μέγιστο μέγεθος του τεμαχίου παίζει ρόλο στη σωστή χρήση του δικτύου;**

TCP – MSS

- Η απόδοση ενός δικτύου μπορεί να είναι πολύ χαμηλή εάν επιλέξουμε ένα μικρό MSS ή αντίστοιχα ένα πολύ μεγάλο.
  - Εάν επιλέξουμε ένα πολύ μικρό MSS τότε ένα μεγάλο εύρος ζώνης του δικτύου καταναλώνεται για τη μεταφορά των bytes της επικεφαλίδας.
  - Εάν επιλέξουμε ένα μεγάλο MSS τότε θα έχουμε και μεγάλα IP δεδομενογραφήματα. Ενδέχεται κατά τη διακίνηση να απαιτηθεί τεμαχισμός (fragmentation). Τα τεμαχισμένα τμήματα (IP fragment) δε μπορούν να επαληθευτούν ή να επαναμεταδοθούν ανεξάρτητα από τα άλλα. Όλα τα τεμάχια του IP πρέπει να παραληφθούν ή αλλιώς το συνολικό δεδομενογράφημα πρέπει να επαναμεταδοθεί.

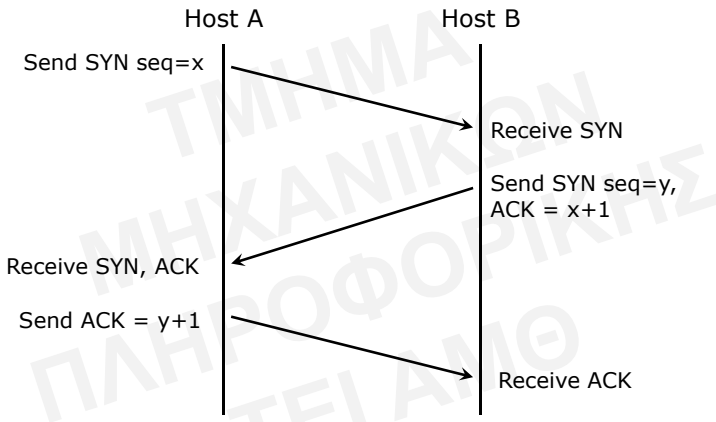
TCP – MSS

- Θεωρητικά, το ιδανικό MSS είναι αυτό το οποίο μας δίνει IP δεδομενογραφήματα τα οποία είναι τόσο μεγάλα ώστε να μη χρειάζεται ο τεμαχισμός τους οπουδήποτε κατά τη διαδρομή τους από την πηγή στον προορισμό.
- Στην πράξη η εύρεση του ιδανικού MSS είναι δύσκολη:
  - Οι περισσότερες υλοποιήσεις του TCP δε παρέχουν τέτοιο μηχανισμό.
  - Η δυναμική δρομολόγηση συνεπάγεται και εν δυνάμει αλλαγή του μονοπατιού.

TCP – Δημιουργία σύνδεσης

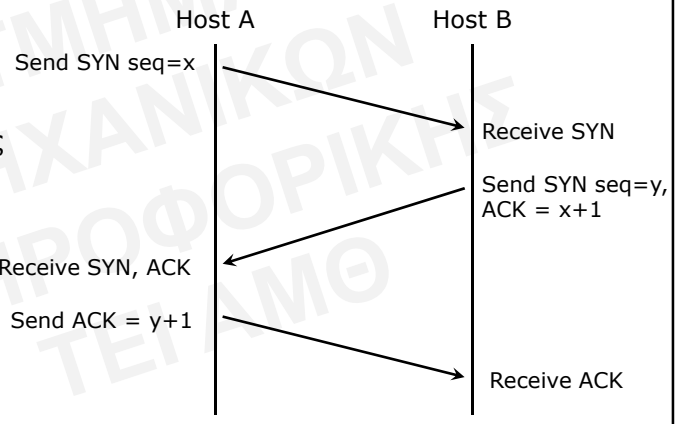
- Είναι μία **χειραψία (handshake) τριών βημάτων**.
  - Το πρώτο segment ονομάζεται **συγχρονισμού** (synchronisation): το SYN bit είναι 1. Δηλώνει την επιθυμία του αποστολέα να δημιουργήσει μια σύνδεση με τον παραλήπτη και την αίτηση συγχρονισμού των αυξόντων αριθμών.
  - Στην απάντηση το SYN και το ACK bits είναι 1. Δηλώνει ότι επαληθεύει το πρώτο SYN τεμάχιο και ότι επιθυμεί να συνεχίσει αυτή τη διαδικασία χειραψίας.
  - Το τελευταίο τεμάχιο είναι απλά μια επαλήθευση στο δεύτερο όπου δηλώνεται στον προορισμό ότι και τα δύο μέρη συμφωνούν ότι έχει δημιουργηθεί μια σύνδεση.

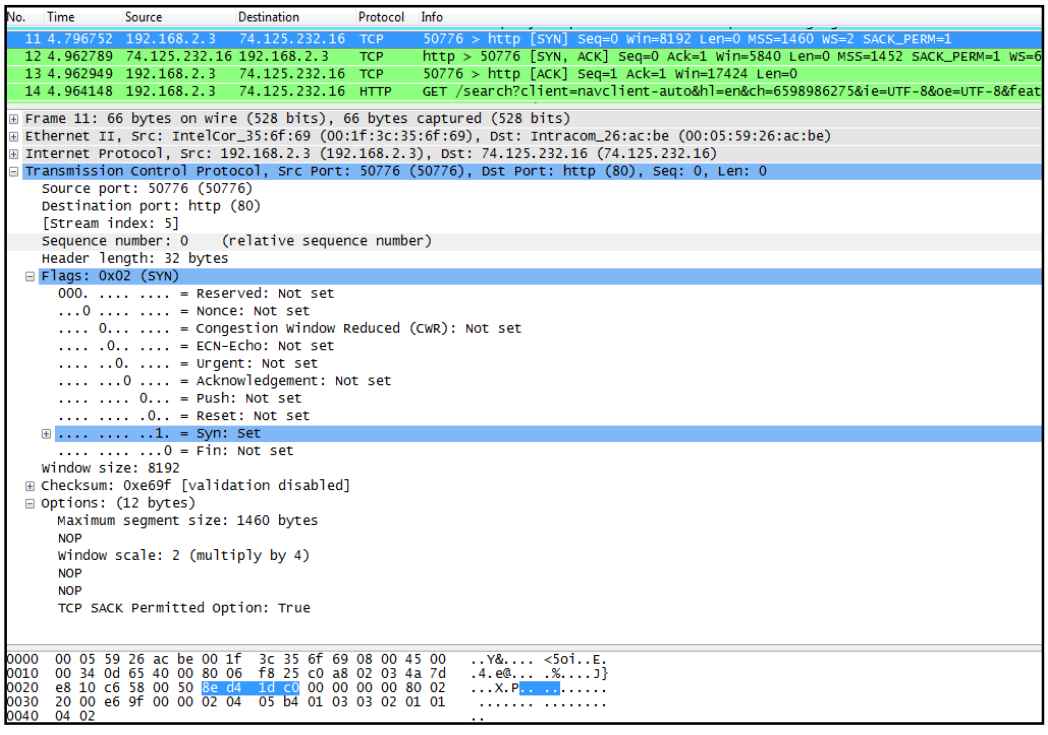
TCP – Δημιουργία σύνδεσης

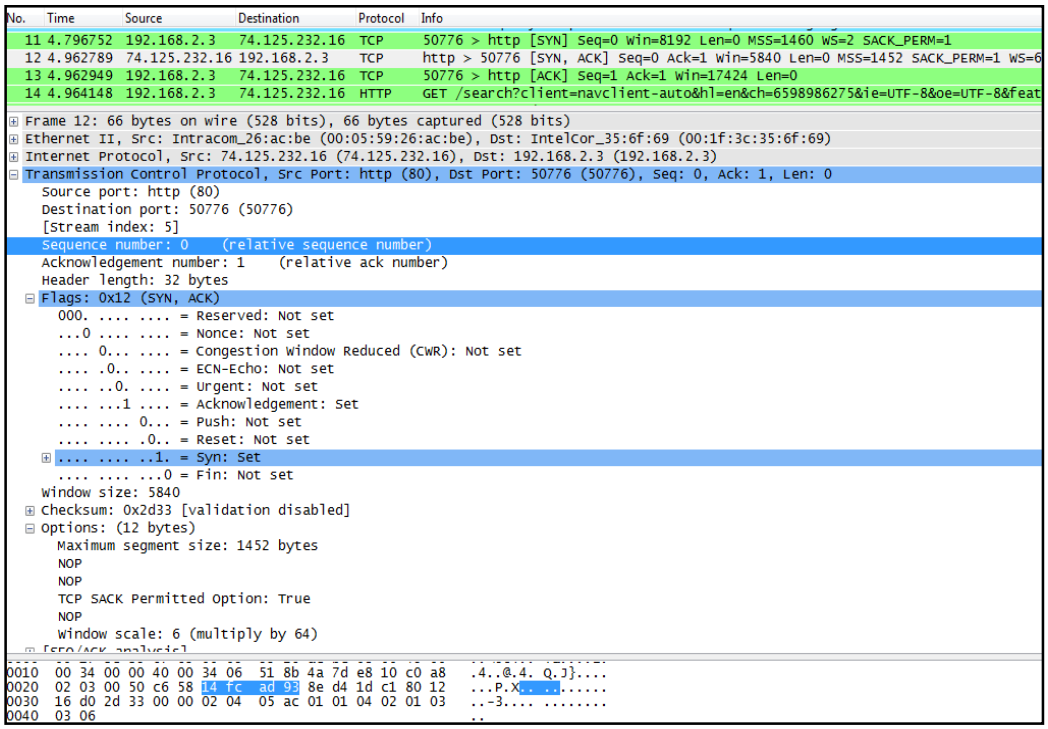


TCP

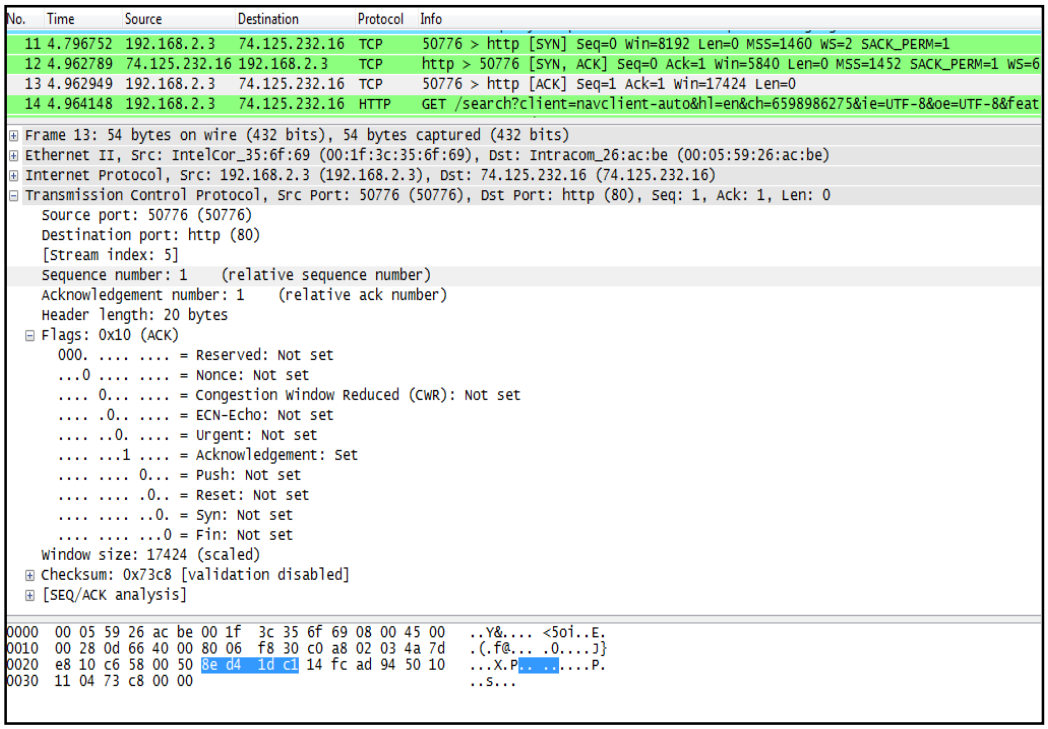
- **Αρχικοί αύξοντες αριθμοί:** τυχαίοι αριθμοί που χρησιμοποιούνται για την αναγνώριση των μεταδιδόμενων bytes.
  - Κάθε τεμάχιο έχει ένα πεδίο αύξοντα αριθμού και ένα πεδίο επαλήθευσης







```
No.  Time        Source          Destination     Protocol  Info
  11 4.796752  192.168.2.3     74.125.232.16   TCP       50776 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2 SACK_PERM=1
  12 4.962789  74.125.232.16   192.168.2.3     TCP       http > 50776 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1452 SACK_PERM=1 WS=6
  13 4.962949  192.168.2.3     74.125.232.16   TCP       50776 > http [ACK] Seq=1 Ack=1 Win=17424 Len=0
  14 4.964148  192.168.2.3     74.125.232.16   HTTP      GET /search?client=navclient-auto&hl=en&ch=6598986275&ie=UTF-8&oe=UTF-8&feat

⊞ Frame 12: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
⊞ Ethernet II, Src: Intracom_26:ac:be (00:05:59:26:ac:be), Dst: IntelCor_35:6f:69 (00:1f:3c:35:6f:69)
⊞ Internet Protocol, Src: 74.125.232.16 (74.125.232.16), Dst: 192.168.2.3 (192.168.2.3)
⊟ Transmission Control Protocol, Src Port: http (80), Dst Port: 50776 (50776), Seq: 0, Ack: 1, Len: 0
    Source port: http (80)
    Destination port: 50776 (50776)
    [Stream index: 5]
    Sequence number: 0    (relative sequence number)
    Acknowledgement number: 1    (relative ack number)
    Header length: 32 bytes
  ⊟ Flags: 0x12 (SYN, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgement: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    ⊞ .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
    Window size: 5840
  ⊞ Checksum: 0x2d33 [validation disabled]
  ⊟ Options: (12 bytes)
      Maximum segment size: 1452 bytes
      NOP
      NOP
      TCP SACK Permitted Option: True
      NOP
      Window scale: 6 (multiply by 64)
  ⊞ [SEQ/ACK analysis]

0010  00 34 00 00 40 00 34 06  51 8b 4a 7d e8 10 c0 a8   .4..@.4. Q.J}....
0020  02 03 00 50 c6 58 14 fc  ad 93 8e d4 1d c1 80 12   ...P.X.. ........
0030  16 d0 2d 33 00 00 02 04  05 ac 01 01 04 02 01 03   ..-3.... ........
0040  03 06                                             ..
```

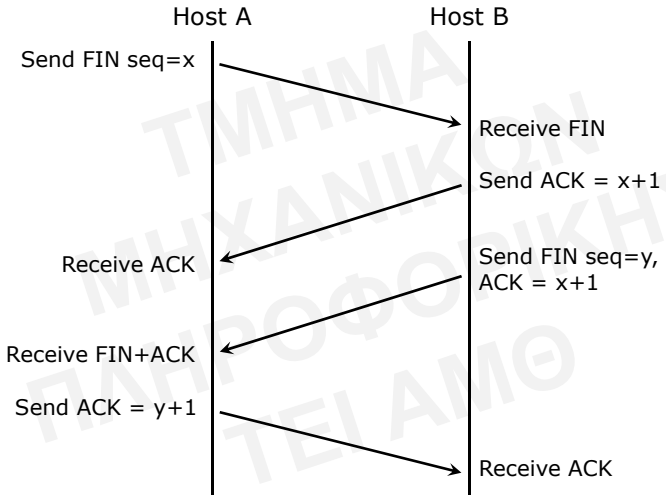


```
No.  Time        Source          Destination     Protocol  Info
  11 4.796752  192.168.2.3     74.125.232.16   TCP       50776 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2 SACK_PERM=1
  12 4.962789  74.125.232.16   192.168.2.3     TCP       http > 50776 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1452 SACK_PERM=1 WS=6
  13 4.962949  192.168.2.3     74.125.232.16   TCP       50776 > http [ACK] Seq=1 Ack=1 Win=17424 Len=0
  14 4.964148  192.168.2.3     74.125.232.16   HTTP      GET /search?client=navclient-auto&hl=en&ch=6598986275&ie=UTF-8&oe=UTF-8&feat

⊞ Frame 13: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
⊞ Ethernet II, Src: IntelCor_35:6f:69 (00:1f:3c:35:6f:69), Dst: Intracom_26:ac:be (00:05:59:26:ac:be)
⊞ Internet Protocol, Src: 192.168.2.3 (192.168.2.3), Dst: 74.125.232.16 (74.125.232.16)
⊟ Transmission Control Protocol, Src Port: 50776 (50776), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0
    Source port: 50776 (50776)
    Destination port: http (80)
    [Stream index: 5]
    Sequence number: 1    (relative sequence number)
    Acknowledgement number: 1    (relative ack number)
    Header length: 20 bytes
  ⊟ Flags: 0x10 (ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgement: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
    Window size: 17424 (scaled)
  ⊞ Checksum: 0x73c8 [validation disabled]
  ⊞ [SEQ/ACK analysis]

0000  00 05 59 26 ac be 00 1f  3c 35 6f 69 08 00 45 00   ..Y&.... <5oi..E.
0010  00 28 0d 66 40 00 80 06  f8 30 c0 a8 02 03 4a 7d   .(.f@... .0....J}
0020  e8 10 c6 58 00 50 8e d4  1d c1 14 fc ad 94 50 10   ...X.P.. ......P.
0030  11 04 73 c8 00 00                                 ..s...
```

TCP

- **Τερματισμός σύνδεσης:** Θεωρούμε ότι μια σύνδεση είναι ένα ζεύγος μονόδρομων συνδέσεων. Κάθε μια από αυτές τερματίζεται ανεξάρτητα από την άλλη.
- Για να τερματιστεί μια σύνδεση από τη μια πλευρά:
  - Η πλευρά αυτή θα στείλει ένα TCP segment με το bit FIN να είναι 1.
  - Μόλις λάβει την επαλήθευση μπορεί να τερματίσει τη σύνδεση.
  - **Η άλλη πλευρά μπορεί όμως να συνεχίσει να στέλνει δεδομένα**.
- Για να τερματιστεί η σύνδεση και από την άλλη πλευρά ακολουθείται η ίδια διαδικασία.

TCP – Τερματισμός σύνδεσης



TCP

- Υπάρχουν περιπτώσεις όπου τα δύο άκρα ενδέχεται να στείλουν τεμάχια FIN την ίδια χρονική στιγμή. Το καθένα από αυτά θα επαληθευτεί και έτσι θα τερματιστεί η σύνδεση.
- Δεν υπάρχει διαφορά αν ο τερματισμός σύνδεσης γίνεται ταυτόχρονα ή ακολουθιακά.

TCP

- **Πρόβλημα των δύο στρατών.** Τμήματα του ίδιου στρατού Α στρατοπεδεύουν εκατέρωθεν του στρατού Β. Για την επικοινωνία τους θα πρέπει να περάσουν μέσα από τον Β. Καθένα από τα τμήματα του Α ξεχωριστά δε μπορούν να νικήσουν τον Β αλλά μαζί μπορούν. Για αυτό πρέπει να συνεννοηθούν πότε θα επιτεθούν.
  - Το 1ο τμήμα του Α στέλνει ένα μήνυμα στο 2ο τμήμα λέγοντας ότι η επίθεση ξεκινά αύριο.
  - Το 2ο τμήμα το λαμβάνει και στέλνει επαλήθευση την οποία λαμβάνει το 1ο τμήμα.
  - Το 2ο τμήμα όμως δε ξέρει αν το 1ο πήρε την επαλήθευση και επομένως δε ξέρει αν θα πρέπει να επιτεθεί.
  - Ακόμη και αν το 1ο τμήμα στείλει μια επαλήθευση για την επαλήθευση το πρόβλημα θα συνεχίσει να υφίσταται.

TCP

- Το πρόβλημα των δύο στρατών έχει την εξής εφαρμογή κατά τον τερματισμό μιας σύνδεσης: **Αν καμιά πλευρά δεν είναι διατεθειμένη να αποσυνδεθεί μέχρι να πεισθεί ότι η άλλη πλευρά θα αποσυνδεθεί και αυτή, ο τερματισμός δε θα γίνει ποτέ.**
- Το TCP αντιμετωπίζει το πρόβλημα των δύο στρατών με τη χρήση **χρονομετρητών**:
  - Αν η απάντηση στο τεμάχιο FIN δε φθάσει σε χρόνο ίσο με το διπλάσιο του χρόνου ζωής των πακέτων η σύνδεση μπορεί να τερματιστεί. Η άλλη πλευρά, επειδή θα δει ότι κανένας δε την ακούει πια μπορεί και αυτή να απολέσει τη σύνδεση της.

TCP

- **Έλεγχος λαθών και ροής στο TCP**: Γίνεται με τη χρήση των μεθόδων του ολισθαίνοντος παραθύρου είτε με επιλεκτική επανάληψη είτε με οπισθοδρόμηση κατά Ν.
- **Τα παράθυρα του TCP δουλεύουν σε επίπεδο bytes και όχι σε segments.**
  - Το TCP χρησιμοποιεί **παράθυρα μεταβλητού μεγέθους** όπου ο παραλήπτης χρησιμοποιώντας το πεδίο WINDOW μπορεί να δηλώσει στον αποστολέα πόσα bytes δύναται να δεχτεί. Ο αποστολέας μπορεί να προσαρμόσει το παράθυρο του στις απαιτήσεις του παραλήπτη.
  - Τα παράθυρα μεταβλητού μεγέθους παρέχουν **έλεγχο ροής**. Σε εξαιρετικές περιπτώσεις ο παραλήπτης μπορεί να θέσει ως μέγεθος παραθύρου το 0 για να δηλώσει ότι δε μπορεί να δεχτεί άλλα δεδομένα.

Σύνδρομο του ανόητου παραθύρου (silly window syndrome)

- Είναι το αποτέλεσμα χρήσης πολύ μικρών παραθύρων:
  - Με τη συνεχή αποστολή δεδομένων ενδέχεται ο καταχωρητής του παραλήπτη να γεμίσει.
  - Ο παραλήπτης θα πρέπει να δηλώσει ότι ο καταχωρητής του έχει πλέον γεμίσει (μέγεθος παραθύρου 0).
  - Όταν ο παραλήπτης διαβάσει κάποια bytes (λίγα στον αριθμό) από τον καταχωρητή θα ελευθερωθεί μια θέση στον καταχωρητή και ο παραλήπτης θα ενημερώσει τον αποστολέα ότι υπάρχει χώρος για μερικά bytes.
  - Ο αποστολέας θα στείλει στον παραλήπτη ένα TCP τεμάχιο με τα λίγα bytes που μπορεί να στείλει.
  - Αυτό θα έχει ως αποτέλεσμα την αποστολή πολλών πολύ μικρών TCP τεμαχίων και κακή χρήση της γραμμής.
- Ο αποστολέας μπορεί να δημιουργήσει το ίδιο πρόβλημα στέλνοντας δεδομένα μόλις αυτά δημιουργούνται.

Σύνδρομο του ανόητου παραθύρου (silly window syndrome)

- Πως αποφεύγουμε το πρόβλημα:
  - **Στον παραλήπτη**: Θα πρέπει να δηλώσει στον αποστολέα κάποιο διαθέσιμο χώρο **μόνο όταν αυτός ξεπεράσει κάποιο συγκεκριμένο μέγεθος**.
    - Το TCP ορίζει αυτό το μέγεθος να είναι το ελάχιστο μεταξύ του μισού του καταχωρητή του παραλήπτη και του αριθμού των bytes που υπάρχουν στο μέγιστο τεμάχιο που μπορεί να χρησιμοποιηθεί.
  - **Στον αποστολέα**: Ο αποστολέας δε στέλνει δεδομένα μέχρι αυτά να συμπληρώσουν το μέγεθος του μέγιστου τεμαχίου.

Σύγκριση TCP και UDP

	TCP	UDP
Αξιοπιστία	Σιγουρεύει ότι τα τεμάχια φθάνουν στον προορισμό τους, επιστρέφει επαληθεύσεις (ACKs) όταν ένα τεμάχιο παραληφθεί.	Δεν επιστρέφει επαληθεύσεις (ACKs) και δε σιγουρεύει ότι ένα πακέτο έχει φθάσει στον προορισμό του.
Σύνδεση	Με σύνδεση: Χρησιμοποιεί το πρωτόκολλο χειραψίας και δημιουργεί μια εικονική σύνδεση μεταξύ αποστολέα και παραλήπτη.	Χωρίς σύνδεση.
Ακολουθία Πακέτων	Χρησιμοποιεί ακολουθία αριθμών μέσα στα τεμάχια για να σιγουρέψει ότι όλα θα παραλειφθούν.	Δεν χρησιμοποιεί αρίθμηση

Σύγκριση TCP και UDP

	TCP	UDP
Έλεγχος συμφόρησης	Ο παραλήπτης μπορεί να πληροφορήσει τον αποστολέα εάν δέχεται μεγάλο αριθμό πακέτων και να καθυστερήσει τη μετάδοση.	Δεν υπάρχει πληροφόρηση του αποστολέα.
Χρήση	Χρησιμοποιείται από εφαρμογές που απαιτούν αξιοπιστία όπως είναι το email και οι αιτήσεις DNS.	Χρησιμοποιείται όταν δεν απαιτείται αξιοπιστία όπως στο video streaming και στην εκπομπή κατάστασης
Ταχύτητα	Χρησιμοποιεί αρκετούς πόρους του συστήματος και είναι σχετικά αργό.	Χρησιμοποιεί λιγότερους πόρους και είναι πιο γρήγορο από το TCP.

ΑΣΚΗΣΕΙΣ

- Θέλετε να σχεδιάσετε ένα αξιόπιστο πρωτόκολλο επικοινωνίας το οποίο χρησιμοποιεί το πρωτόκολλο ολισθαίνοντος παραθύρου (όπως το TCP). Το πρωτόκολλο αυτό θα χρησιμοποιείται σε μια γραμμή των C=100Kbps. Η καθυστέρηση διάδοσης είναι P=50ms και ο μέγιστος χρόνος ζωής ενός τεμαχίου T=60seconds.
  - Πόσα bits θα πρέπει να χρησιμοποιήσετε για το Window και για το Sequence Number πεδία του επικεφαλίδας;

ΑΣΚΗΣΕΙΣ

- Ένας κόμβος χρησιμοποιεί το TCP και στέλνει παράθυρα των 65,535 byte μέσω διαύλου του 1Gbps που παρουσιάζει καθυστέρηση μιας κατεύθυνσης 10msec. Ποιά είναι η μέγιστη δυνατή διέλευση; Ποιά είναι η αποδοτικότητα της γραμμής?

ΑΣΚΗΣΕΙΣ

- Στο TCP πρωτόκολλο μπορούμε να έχουμε δύο συνδέσεις μεταξύ δύο σταθμών που να έχουν τις ίδιες θύρες πηγής και προορισμού;
- Τι θα γίνει αν οι δύο σταθμοί προσπαθήσουν να δημιουργήσουν ταυτόχρονα δύο συνδέσεις χρησιμοποιώντας τις ίδιες υποδοχές (η μία σύνδεση γίνεται από τον ένα κόμβο και η άλλη από τον άλλο);

ΑΣΚΗΣΕΙΣ

- Γιατί πρέπει να χρησιμοποιούμε τυχαίους αριθμούς στην εγκατάσταση μιας σύνδεσης;

ΑΣΚΗΣΕΙΣ

- Το μέγιστο μέγεθος του τεμαχίου παίζει ρόλο στη σωστή χρήση του δικτύου από πλευράς εκμετάλλευσης του διαθέσιμου εύρους ζώνης;

ΑΣΚΗΣΕΙΣ

- Χαμένες επαληθεύσεις στο TCP δεν απαιτούν απαραίτητα την επαναμετάδοση των τεμαχίων. Εξηγήστε γιατί.
- Εάν για την εγκατάσταση σύνδεσης χρησιμοποιούσαμε μια διμερή αντί της τριμερούς χειραψία, θα ήταν δυνατό να εγκαταστήσουμε μια σύνδεση;

ΑΣΚΗΣΕΙΣ

- Στο πρόβλημα των δύο στρατών αν ο ένας στρατός αντί για 2 μέρη αποτελούνταν από n θα λυνόταν το πρόβλημα; Υπάρχει πρωτόκολλο που να επιτρέπει σε αυτόν το στρατό να νικήσει;

ΑΣΚΗΣΕΙΣ

- Ποιό είναι το βασικό πλεονέκτημα της χρήσης θυρών αντί του αριθμού διεργασίας για να προσδιορίσουμε τον απόλυτο προορισμό σε μια συσκευή;

ΔΙΚΤΥΑ ΙΙ

DNS
ARP
RARP
ICMP
DHCP
FTP

DNS

- **Domain Name System**: Κατανεμημένη βάση δεδομένων που χρησιμοποιείται για την αντιστοίχιση IP διευθύνσεων – ονομάτων (εύκολα επεξεργάσιμων από τον άνθρωπο).
- Παραχωρεί σε σταθμούς τη δυνατότητα να επιλέξουν τα δικά τους ονόματα ανεξάρτητα από τις IP διευθύνσεις.
- Τα ονόματα που μπορούν να χρησιμοποιηθούν είναι ιεραρχημένα (για ευκολότερη επεξεργασία)
- Χρησιμοποιείται από εφαρμογές όπως ftp, email, http για να μπορούν να αποστέλλονται τα πακέτα στον προορισμό τους βάσει των IP διευθύνσεων.

Ονοματολογία

- Ονόματα έχουν τη μορφή x.y.z: κάποια τμήματα μπορεί να ελέγχονται από κάποια αρμόδια αρχή
  - Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων – ΕΕΤΤ
- Οι καταλήξεις είναι δύο τύπων:
  - Γενικές ή θεματικές (προσδιορίζουν τον τύπο του συγκεκριμένου site)
  - Περιοχών (προσδιορίζουν γεωγραφικά το χώρο στον οποίο βρίσκεται το site)
- Παραδείγματα γενικών καταλήξεων
  - .com Εμπορικές διευθύνσεις
  - .edu Εκπαιδευτικά ιδρύματα
  - .gov Κυβερνητικά sites
  - .mil Στρατιωτικά sites
  - .org Μη κερδοσκοπικοί οργανισμοί
  - .net Φορείς δικτύου

Ονοματολογία

- Τα ονόματα περιοχών περιλαμβάνουν τυπικά όλες τις χώρες οι οποίες κάνουν χρήση του δικτύου:
  - .gr Το site δραστηριοποιείται στην Ελλάδα ή διαθέτει περιεχόμενο που αφορά τη γεωγραφική περιοχή της Ελλάδας
  - .fr Γαλλία
  - .uk Ηνωμένο Βασίλειο
  - κ.λ.π.
- Λόγω της ιεράρχησης κάθε γεωγραφική περιοχή μπορεί να ορίσει και την ονοματολογία για άλλα επίπεδα.
  - Χρήση .edu ή .ac πριν το γεωγραφικό προσδιορισμό, π.χ.
    - www.teikav.edu.gr
    - www.rhul.ac.uk
  - Εμπορικά και κυβερνητικά sites κ.λ.π. Π.χ.
    - www.sony.co.uk
    - www.ypes.gov.gr

DNS Servers

- Οι **εξυπηρετητές DNS** είναι υπεύθυνοι για τη διατήρηση πινάκων με πλήθος έγκυρων εγγραφών με αντιστοιχίες IP διευθύνσεων – ονομάτων.
- Για μια συγκεκριμένη περιοχή μπορεί να υπάρχει ένας **πρωτεύον** καθώς και ένας **δευτερεύον** εξυπηρετητής. Ο δευτερεύον παίρνει όλες τις πληροφορίες του από τον πρωτεύον και χρησιμοποιείται για την περίπτωση που ο πρωτεύον δεν είναι διαθέσιμος (καθώς επίσης και για την κατανομή των ερωτήσεων)

DNS

- Κάθε κόμβος θα πρέπει να γνωρίζει τη **διεύθυνση του εξυπηρετητή DNS** στον οποίο πρέπει να καταφύγει για να γίνει η αντιστοίχιση του ονόματος προορισμού σε μια αποδεκτή διεύθυνση προορισμού.
- Ο εξυπηρετητής απαντά σε ερωτήσεις πελατών για διευθύνσεις βάσει ονομάτων καθώς και για ονόματα βάσει διευθύνσεων (Reverse DNS).

DNS

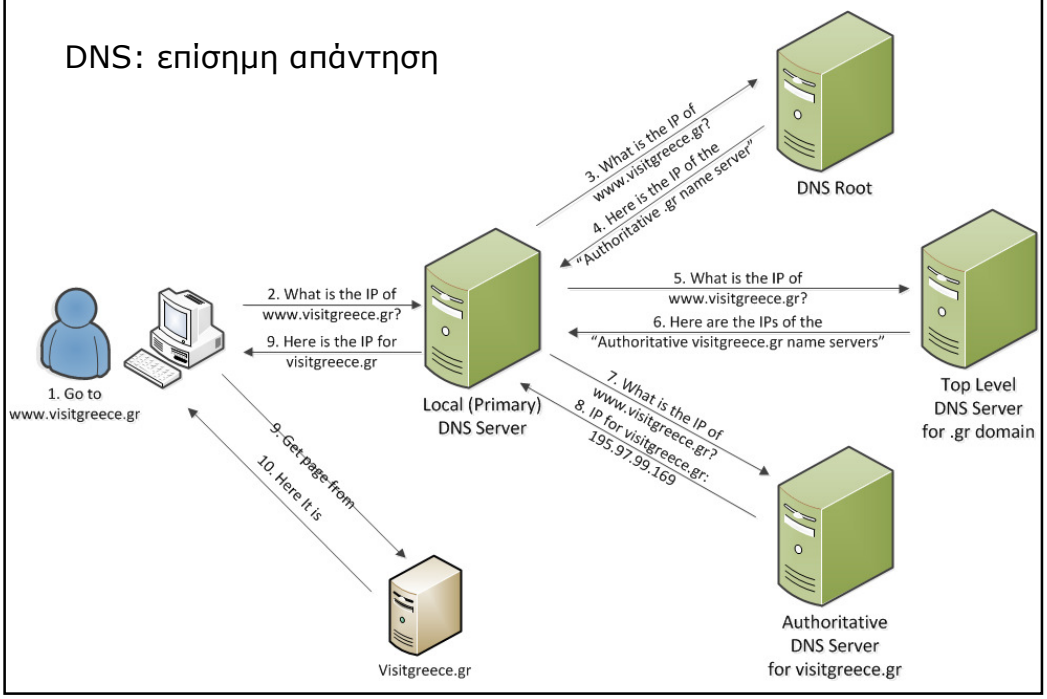
- Οι ερωτήσεις στον εξυπηρετητή μπορούν να γίνουν και από τον ίδιο τον χρήστη με τη χρήση της εντολής nslookup (χρήση κυρίως UDP στη θύρα 53).
- Π.χ.

```
$ nslookup www.ieee.org
Server:   philippos.teikav.edu.gr
Address:  195.130.92.35

Non-authoritative answer:
Name:     e1630.c.akamaiedge.net
Address:  95.100.182.198
Aliases:  www.ieee.org
          www.ieee.org.edgekey.net
```


Authoritative and non-authoritative answers

- Αν η απάντηση στο ερώτημα προέρχεται από τον εξυπηρετητή που είναι υπεύθυνος για τη διαχείριση αυτών των αντιστοιχιών τότε μιλάμε για **authoritative response (επίσημη απάντηση)** ενώ αν προέρχεται από κάποιον άλλο εξυπηρετητή που έχει απλά καταχωρημένη την αντιστοίχιση μιλάμε για **non-authoritative response (ανεπίσημη απάντηση)**.
- Σε περίπτωση που ο εξυπηρετητής δε γνωρίζει την απάντηση πρέπει να καταφύγει στον εξυπηρετητή που είναι υπεύθυνος για τη συγκεκριμένη περιοχή. Αν τη γνωρίζει από κάποιο προηγούμενο ερώτημα τότε μπορεί να δώσει μια ανεπίσημη απάντηση στον πελάτη.

DNS: επίσημη απάντηση



Address Resolution Protocol

- Ασχολείται με το πρόβλημα της παράδοσης ενός IP δεδομενογραφήματος στον απόλυτο προορισμό μέσα σε ένα τοπικό δίκτυο.
  - Δίνει τη φυσική διεύθυνση που αντιστοιχεί σε μια IP.
- Ένα δίκτυο μπορεί να χρησιμοποιεί δικό του σύστημα διευθυνσιοδότησης (πέραν του IP). Π.χ. ethernet.
  - Έτσι πρέπει οι IP διευθύνσεις να μεταφραστούν κατάλληλα.
  - Συνδυάζεται με ενθυλάκωση του IP δεδομενογραφήματος μέσα σε ένα πλαίσιο το οποίο περιέχει την κατάλληλη διεύθυνση έτσι ώστε να μπορέσει να σταλεί στον απόλυτο προορισμό.

Address Resolution Protocol

- Η αντιστοίχιση μεταξύ IP διευθύνσεων και φυσικών διευθύνσεων μπορεί να γίνει με τη χρήση πινάκων οι οποίοι ανανεώνονται αυτόματα.
- Το ARP **εκμεταλλεύεται τη λειτουργία της εκπομπής** που υποστηρίζουν τέτοια δίκτυα επιπέδου ζεύξης δεδομένων όπως είναι το Ethernet και το Token Ring.

Παράδειγμα

No.	Time	Source	Destination	Protocol	Info
406	10.190147	Cisco_eb:49:00	Broadcast	ARP	Who has 195.130.92.82? Tell 195.130.92.33

```
⊞ Frame 406: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
⊟ Ethernet II, Src: Cisco_eb:49:00 (00:0c:ce:eb:49:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Source: Cisco_eb:49:00 (00:0c:ce:eb:49:00)
    Type: ARP (0x0806)
    Trailer: 00000000000000000000000000000000000000
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    [Is gratuitous: False]
    Sender MAC address: Cisco_eb:49:00 (00:0c:ce:eb:49:00)
    Sender IP address: 195.130.92.33 (195.130.92.33)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 195.130.92.82 (195.130.92.82)
```

```
0000  ff ff ff ff ff ff 00 0c  ce eb 49 00 08 06 00 01   ........ ..I.....
0010  08 00 06 04 00 01 00 0c  ce eb 49 00 c3 82 5c 21   ........ ..I...\!
0020  00 00 00 00 00 00 c3 82  5c 52 00 00 00 00 00 00   ........ \R......
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

Address Resolution Protocol - Βήματα

- Εάν κάποιος σταθμός θέλει να στείλει ένα IP δεδομενογράφημα σε κάποιον άλλο σταθμό στο ίδιο δίκτυο, πρώτα ψάχνει στην ARP cache για την αντιστοίχιση.
- Εάν δεν υπάρχει η αντιστοίχιση αυτή στον πίνακα του τότε ο σταθμός στέλνει μια αίτηση ARP χρησιμοποιώντας εκπομπή. Η αίτηση αυτή περιέχει την IP διεύθυνση για την οποία γίνεται η ερώτηση.
- Όλοι οι σταθμοί λαμβάνουν την αίτηση, μόνο ο σταθμός στον οποίο απευθύνεται θα απαντήσει στην ερώτηση στέλνοντας πίσω στην πηγή τη φυσική του διεύθυνση.
- Η αίτηση περιλαμβάνει την IP διεύθυνση και τη φυσική διεύθυνση της πηγής έτσι ώστε όλοι οι παραλήπτες να καταχωρήσουν στους πίνακες τους και αυτά τα στοιχεία.

Reverse Address Resolution Protocol

- Επιστρέφει στον ενδιαφερόμενο την IP διεύθυνση που αντιστοιχεί σε μια φυσική διεύθυνση.
- Χρησιμοποιείται από τερματικά τα οποία δεν έχουν μέσα αποθήκευσης και επομένως δε μπορούν να διατηρήσουν πληροφορίες όπως IP διεύθυνση.
  - Για να μπορέσει κάποιο τέτοιο τερματικό (dummy terminal) να μάθει την IP διεύθυνση του μπορεί να χρησιμοποιήσει το RARP πρωτόκολλο.
  - Η φυσική διεύθυνση είναι γνωστή γιατί υπάρχει στη ROM της κάρτας δικτύου και επομένως δε χάνεται με την επανεκκίνηση του τερματικού.

Internet Control Message Protocol

- Είναι το πρωτόκολλο που χειρίζεται τα λάθη στις επικοινωνίες όπως όταν ο προορισμός δε μπορεί να επεξεργαστεί ένα IP δεδομενογράφημα, π.χ. ότι
  - το IP δεδομενογράφημα δε μπορεί να φθάσει στον προορισμό του (host unreachable),
  - η επανασύνδεση σε περίπτωση τεμαχισμού απέτυχε,
  - το TTL έγινε 0,
  - το άθροισμα ελέγχου της IP επικεφαλίδας είναι λανθασμένο.
- Μπορεί επίσης να χρησιμοποιηθεί και από **δρομολογητές** για να πληροφορήσει την πηγή ότι υπάρχει καλύτερη διαδρομή από αυτήν που έχει επιλεγεί.

Dynamic Host Configuration Protocol – DHCP

- Σε περιπτώσεις όπου ένα τερματικό δε φέρει κάποια μέσα αποθήκευσης ή βάσει απόφασης του διαχειριστή οι κόμβοι δεν έχουν σταθερές διευθύνσεις (γιατί δεν υπάρχει κάποιος σταθερός αριθμός τερματικών) οι υπολογιστές μπορούν να πάρουν μια διεύθυνση δυναμικά.
  - Ο διαχειριστής του δικτύου ορίζει ένα συγκεκριμένο εύρος διευθύνσεων το οποίο μπορούν να χρησιμοποιήσουν οι σταθμοί.
  - Κάποιος server αναλαμβάνει τη διαχείριση των διευθύνσεων.
  - Κάθε φορά που κάποιος σταθμός θέλει να κάνει χρήση του δικτύου ο server του δίνει μια προσωρινή διεύθυνση για να μπορεί ο σταθμός αυτός να επικοινωνήσει.

File Transfer Protocol

- Πρόκειται για ένα πρωτόκολλο το οποίο επιτρέπει τη μεταφορά αρχείων μεταξύ απομακρυσμένων κόμβων
- Τα κύρια χαρακτηριστικά του:
  - Είναι αξιόπιστο
  - Παρέχει στους χρήστες πολλές υπηρεσίες διαχείρισης αρχείων σε κάποιον απομακρυσμένο εξυπηρετητή.
  - Επιτρέπει στους χρήστες να ορίσουν τον τρόπο μεταφοράς των αρχείων (binary ή ascii)
  - Αυθεντικοποίηση χρηστών: Οι χρήστες πριν τη μεταφορά αρχείων πρέπει να δηλώσουν την ταυτότητα τους και να την αποδείξουν (με τη χρήση κάποιου password)
  - Επιτρέπει την ύπαρξη πολλαπλών ταυτόχρονων συνόδων από κάποιο πελάτη.

File Transfer Protocol

- Ένας πελάτης για να μεταφέρει αρχεία από και προς κάποιο server πρέπει να δημιουργήσει μια σύνδεση η οποία παίζει το ρόλο της **σύνδεσης ελέγχου**. Η μεταφορά των δεδομένων γίνεται χρησιμοποιώντας μια ξεχωριστή σύνδεση η οποία δημιουργείται κάθε φορά που έχουμε μεταφορά κάποιου αρχείου.
- Χρήση θυρών
  - Ο πελάτης πραγματοποιεί μια σύνδεση (ελέγχου της συνόδου) στη θύρα 21 του προορισμού.
  - Όταν πρέπει να γίνει μεταφορά αρχείου δημιουργείται μια νέα σύνδεση. Τι θύρες χρησιμοποιούν πελάτης και εξυπηρετητής για αυτή τη νέα σύνδεση;

File Transfer Protocol

- Προφανώς δε μπορούν να χρησιμοποιήσουν το ίδιο ζεύγος θυρών αφού αυτές χρησιμοποιούνται από τη σύνδεση ελέγχου. Για αυτό το λόγο:
  - Ο πελάτης χρησιμοποιεί μια ελεύθερη θύρα στο σταθμό του ενώ για τον εξυπηρετητή χρησιμοποιείται η θύρα 20 για τη μεταφορά αρχείων.

ΔΙΚΤΥΑ ΙΙ

Email

Email

- Δύο πρότυπα
  - RFC 822 and MIME
- Πως αποθηκεύονται, μεταφέρονται και διαβάζονται τα emails?
  - MUAs, MTAs
  - SMTP, POP3, IMAP

RFC 822

- Ένα e-mail είναι ένα μήνυμα το οποίο αποτελείται από μια ακολουθία ASCII χαρακτήρων η δομή του οποίου ορίζεται στο RFC 822.
- Αποτελείται από δύο τμήματα τα οποία **χωρίζονται με μια κενή γραμμή**:
  - **Επικεφαλίδα**: sender, recipient, date, subject, delivery path,…
  - **Δεδομένα (body)**
- Η χρήση του ASCII δημιουργεί προβλήματα όταν πρέπει να μεταφερθούν μη-ASCII δεδομένα, π.χ. δυαδικά αρχεία.

Παράδειγμα RFC 822 Μηνύματος

```
From: krantos@teikav.edu.gr
To:   noc@teikav.edu.gr
Cc:   library@teikav.edu.gr
Subject: RFC 822 example
Date: Tue, 16 Nov 2010 12:15:32

This is an RFC 822 email example.
```


Multipurpose Internet Mail Extensions – MIME

- Επεκτείνει τις δυνατότητες του RFC 822 ώστε να επιτρέψει σε κάποιο e-mail να μεταφέρει περιεχόμενο το οποίο δεν είναι αποκλειστικά ακολουθία ASCII χαρακτήρων, καθώς και μεγάλα μηνύματα.
- Χρησιμοποιεί επιπλέον πεδία επικεφαλίδας από ότι το RFC 822 για να ορίσει τη μορφή και το περιεχόμενο των επεκτάσεων (extensions).
- Υποστηρίζει διάφορα είδη περιεχομένου.
- Ορίζεται στα RFCs 2045-2049.

Επικεφαλίδες MIME

Ορίζει 5 νέα πεδία επικεφαλίδας:

- `MIME-Version`
- `Content-Type`
- `Content-Disposition`
- `Content-Transfer-Encoding`
- `Content-ID` – προαιρετικό
- `Content-Description` – προαιρετικό

`Content-Type`

- Ορίζει τον τύπο του περιεχομένου βάσει συγκεκριμένων κατηγοριών.
- Η εξ' ορισμού τιμή είναι η `text/plain`
- Η `Multipart/mixed`, υποδεικνύει ότι το σώμα του email περιέχει πολλαπλά τμήματα.
- Κάθε τμήμα μπορεί να είναι ένα ξεχωριστό MIME μήνυμα – επομένως μπορούν να σταλούν εμφωλιασμένα MIME μηνύματα.
- Τα διάφορα τμήματα χωρίζονται με μια ακολουθία χαρακτήρων (boundary string) το οποίο ορίζεται στο πεδίο `Content-Type`.

Content-Disposition

- Αφορά τον τρόπο με τον οποίο θα παρουσιαστούν κάποια δεδομένα.
  - `Inline`: Τα δεδομένα θα παρουσιαστούν ως μέρος το μηνύματος
  - `Attachment`: Η παρουσίαση των δεδομένων απαιτεί κάποια ενέργεια από τον χρήστη (και τυπικά τη σχετική εφαρμογή)
- Περιλαμβάνει πληροφορίες σχετικές με το αρχείο που μεταδίδεται όπως το όνομα και ημερομηνία δημιουργίας.

Content-Transfer-Encoding

- Τα RFC 822 e-mails μπορούν να περιέχουν μόνο ASCII χαρακτήρες.
- MIME μηνύματα μεταφέρουν αυθαίρετα δεδομένα.
- Το πεδίο `Content-Transfer-Encoding` field δείχνει πως τα δεδομένα κωδικοποιήθηκαν από απλά δεδομένα (raw data) σε ASCII.
- Μια συνηθισμένη κωδικοποίηση είναι η `base64` :
  - 24 bits (3 bytes) κωδικοποιούνται σε 4 ASCII χαρακτήρες.
  - Έχει ως αποτέλεσμα την επέκταση δεδομένων.

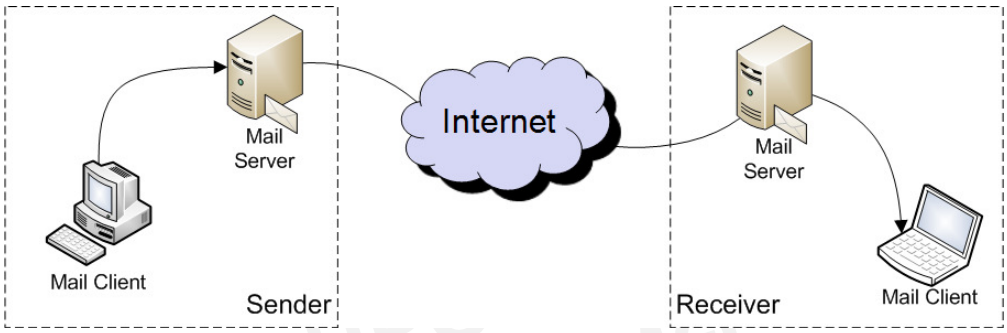
Παράδειγμα

```
Message-ID: <4CDCFD3E.2000903@teikav.edu.gr>
Date: Fri, 12 Nov 2010 10:39:26 +0200
From: Konstantinos Rantos <krantos@teikav.edu.gr>
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.12)
   Gecko/20101027 Lightning/1.0b2 Thunderbird/3.1.6
MIME-Version: 1.0
To: ioannis papadopoulos <papadopoulos@gmail.com>
Subject: Re: test
Content-Type: multipart/mixed;
 boundary="------------080009000908090002030108"

This is a multi-part message in MIME format.
```


Παράδειγμα

```
--------------080009000908090002030108
Content-Type: text/plain; charset=ISO-8859-7;
Content-Transfer-Encoding: 8bit

Γιάννη καλημέρα,

...

--------------080009000908090002030108
Content-Type: application/msword;
 name="test.doc"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
 filename="test.doc"

0M8R4KGxGuEAAAAAAAAAAAAAAAAAAAAAPgADAP7/CQAGAAAAAAAAAAAAAAABAAAAXgAAAAA
...
--------------080009000908090002030108--
```

Μετάδοση emails



- Mail Server: γνωστός και ως Mail Transfer Agent – MTA
- Mail Client: γνωστός και ως Mail User Agent – MUA

Δημιουργία και παράδοση

- Mail client: εφαρμογή που χρησιμοποιεί ο χρήστης π.χ. Microsoft Outlook ή Thunderbird.
  - Μεταφράζει το email σε ένα RFC 822 μήνυμα και συνδέεται με τον Mail Server.
  - Δίνει εντολή στον Mail Server χρησιμοποιώντας το **SMTP (Simple Mail Transfer Protocol)** πρωτόκολλο και στέλνει το RFC 822 μήνυμα.
  - SMTP: Ορίζεται στο RFC 821, και χρησιμοποιείται για MUA-MTA και MTA-MTA συνδιαλέξεις. Χρησιμοποιεί τη θύρα 25 του TCP. Οι νεότερες εκδόσεις του συστήματος υποβολής email χρησιμοποιούν τη θύρα 587.

Δημιουργία και παράδοση

- Ο Mail Server του αποστολέα δημιουργεί σύνδεση με τον Mail Server του παραλήπτη και χρησιμοποιεί το SMTP για να μεταφέρει το RFC 822 μήνυμα.
  - Στη διαδικασία της μεταφοράς μπορεί να εμπλακούν και ενδιάμεσοι Mail Servers.
- Ο Mail Server του παραλήπτη μπορεί να παραδώσει το μήνυμα στο Mail Client του παραλήπτη ή να αποθηκεύσει το μήνυμα τοπικά για την πρόσβαση σε αυτό από τον παραλήπτη σε κάποια στιγμή στο μέλλον.

Πρόσβαση στο e-mail

- Για την πρόσβαση στον mail server με τη χρήση κάποιου mail client:
  - POP=Post Office Protocol (RFC 1939, v3).
  - IMAP=Internet Message Access Protocol (RFC 2060, v4rev1).
  - Άλλα πρωτόκολλα...
- Πρόσβαση μέσω Web
  - Χρήσιμο για χρήστες που δε διαθέτουν κάποιο mail client