Μανώλης Κιαγιάς

Δίκτυα Υπολογιστών

Το Ανεπίσημο Βοήθημα

Για τους Τομείς Πληροφορικής και Ηλεκτρονικής της Γ΄ Τάξης των ΕΠΑ.Λ.

Προσαρμοσμένο στην Ύλη των Πανελλαδικών Εξετάσεων 2017

Χανιά, 2017

Δίκτυα Υπολογιστών – Το Ανεπίσημο Βοήθημα

Μανώλης Κιαγιάς, MSc

01/03/2017

Κάθε γνήσιο αντίτυπο φέρει την υπογραφή του συγγραφέα:

1η Έκδοση - Αναθεώρηση: 02 – Χανιά, 08/04/2017

[Αριθμός αντιτύπου: (Web Edition)]

Με την κατανόηση ότι:

Αποποίηση – Οποιεσδήποτε από τις παραπάνω συνθήκες μπορούν να παρακαμφθούν αν πάρετε την άδεια του δημιουργού ή κατόχου των πνευματικών δικαιωμάτων.

Άλλα Δικαιώματα – Σε καμιά περίπτωση τα ακόλουθα δικαιώματα σας, δεν επηρεάζονται από την Άδεια:

- Η δίκαιη χρήση και αντιμετώπιση του έργου
- Τα ηθικά δικαιώματα του συγγραφέα
- Τα ενδεχόμενα επί του έργου δικαιώματα τρίτων προσώπων, σχετικά με τη χρήση του έργου, όπως για παράδειγμα η δημοσιότητα ή ιδιωτικότητα

Σημείωση – Για κάθε επαναχρησιμοποίηση ή διανομή, πρέπει να καταστήσετε σαφείς στους άλλους τους όρους της άδειας αυτού του Έργου. Ο καλύτερος τρόπος να το πράξετε αυτό, είναι να δημιουργήσετε ένα σύνδεσμο με το διαδικτυακό τόπο της παρούσας άδειας:

`http://creativecommons.org/licenses/by-nc-sa/3.0/gr/`

Το βιβλίο αυτό στοιχειοθετήθηκε σε XeLaTeX. Ο πηγαίος κώδικας του είναι διαθέσιμος στις δικτυακές τοποθεσίες που αναφέρονται παρακάτω και μέσω GitHub.

Επισκεφθείτε το δικτυακό τόπο του μαθήματος και κατεβάστε την τελευταία έκδοση του βιβλίου και διορθώσεις:

`http://diktia.chania-lug.gr`

Ή κατεβάστε απευθείας το PDF από την τοποθεσία:

`http://www.freebsdworld.gr/diktia/diktia2016.pdf`

(Κενή Σελίδα)

Το βιβλίο αυτό αφιερώνεται στους μαθητές μου Αλέξη Μπαλαμπανίδη, Γιώργο Πόπα και Γιώργο Πρίφτη που άντεξαν εμένα και τα δίκτυα!

> “Ο μόνος αληθινός νόμος είναι εκείνος που οδηγεί στην ελευθερία”, είπε ο Ιωνάθαν· “Δεν υπάρχει άλλος.”
>
> *“Ο Γλάρος Ιωνάθαν Λίβινγκστον”, Richard Bach*

(Κενή Σελίδα)

Εισαγωγή στο Νέο Βοήθημα

Καλώς ήλθατε στην πρώτη έκδοση του νέου “ανεπίσημου” βοηθήματος για το μάθημα “Δίκτυα Υπολογιστών” το οποίο διδάσκεται ως Πανελλαδικά εξεταζόμενο στην Γ’ Τάξη των Επαγγελματικών Λυκείων. Το βιβλίο αυτό καλύπτει την εξεταζόμενη ύλη όπως ανακοινώθηκε από το Υπουργείο Παιδείας για το σχολικό έτος 2016-2017 σύμφωνα με το νέο σχολικό βιβλίο και το πρόγραμμα σπουδών. Το νέο ανεπίσημο βοήθημα, με απλοποιημένη αλλά άρτια τεχνικά γλώσσα, ευελπιστεί να καλύψει τις ατέλειες του σχολικού εγχειριδίου και να βοηθήσει τους αποφασισμένους μαθητές να πετύχουν στις εξετάσεις. Η επιτυχία των δύο αρχικών βοηθημάτων για το ΤΕΕ και το ΕΠΑΛ, μας οδηγεί να πιστεύουμε ότι ο στόχος αυτός είναι εφικτός.

Η έκδοση αυτή κυκλοφορεί ως “ελεύθερη” με βάση την άδεια Creative Commons που μπορείτε να διαβάσετε στις πρώτες σελίδες του βιβλίου.

Πρόλογος της Πρώτης Έκδοσης (2004)

> Προλογίζει ο Αντώνης Αθανασάκης, καθηγητής στον Τομέα Οικονομίας, συνάδελφος του συγγραφέα στο ΤΕΕ Κισάμου.

Κάθε απόπειρα αγωγής καταλήγει σε σχέση μεταξύ προσώπων. Η διδασκαλία, δεν είναι ενέργεια κατά την οποία επικοινωνούν μόνο οι εγκέφαλοι, αλλά πορεία προσωπικής επικοινωνίας και αμοιβαίας προσπάθειας.

Το εγώ που δεν έχει απέναντί του κανένα συγκεκριμένο εσύ, αλλά είναι περιστοιχισμένο από μια πληθώρα “περιεχομένων”, δεν είναι διόλου παρόν και η στιγμή του είναι στερημένη από παρουσία. Μια παρουσία όμως δεν είναι κάτι που ξεφεύγει και γλιστράει αλλά είναι εκείνο που κατοικεί απέναντί μας και περιμένει την συνάντηση.

Αν η πραγματική συνάντηση είναι η πορεία, κατά την οποία ένας άνθρωπος αγγίζει έναν άλλον άνθρωπο στον πυρήνα του, τότε οι μαθητές του Μανώλη είχαν φέτος μια τρομερή ευκαιρία.

Το μόνο που χρειάζονται είναι την ικανότητα για ανταπόκριση. Γιατί η ελευθερία μέσα στην αγωγή, είναι το να μπεις σε δεσμό. Το αντίθετο του εξαναγκασμού, σύμφωνα με τον Buter δεν είναι η ελευθερία, αλλά ο δεσμός. Δεν θα μπορούσαμε χωρίς ελευθερία, αλλά από μόνη της δεν είναι χρησιμοποιήσιμη.

Περιεχόμενα

Κατάλογος σχημάτων

Κεφάλαιο 1

Βασικές Έννοιες Αρχιτεκτονικής και Διασύνδεσης Δικτύων

1.2.2 Το Μοντέλο Δικτύωσης TCP/IP

Το ARPANET είναι ο πρόγονος του σημερινού Internet.

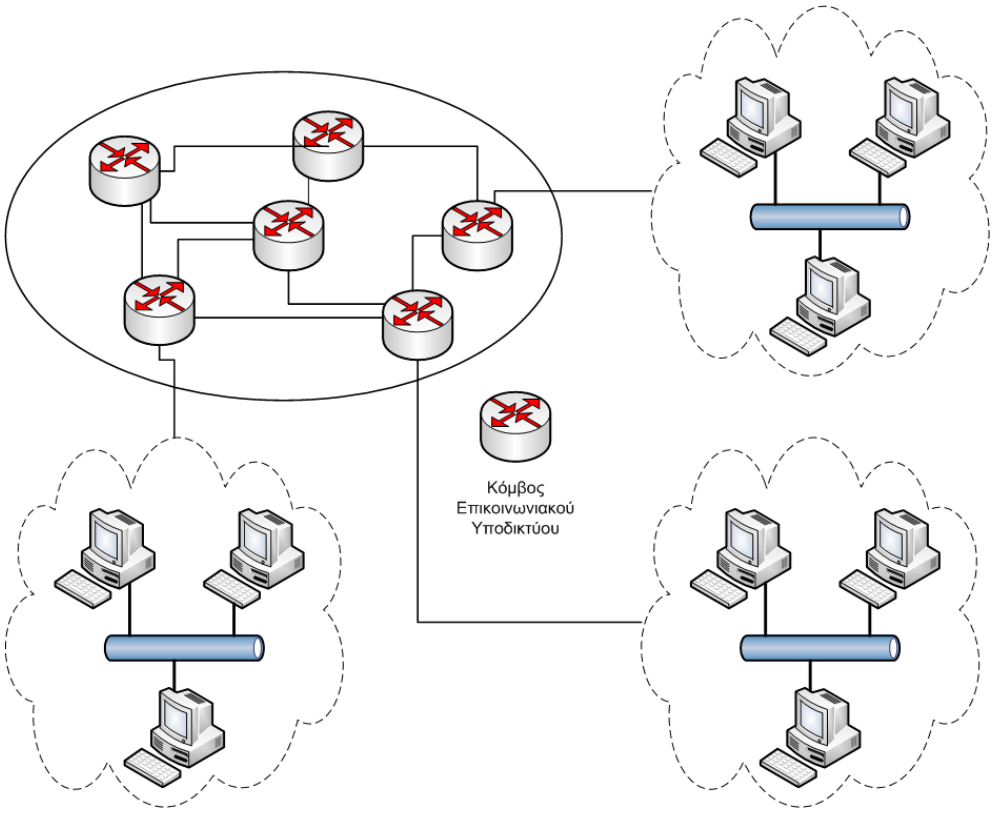
Τι σημαίνει ARPANET;

Είναι τα αρχικά των λέξεων Advanced Research Projects Agency Network. Το ARPA είναι μια υπηρεσία του υπουργείου Άμυνας των ΗΠΑ που ασχολείται – όπως λέει και το όνομα του – με προχωρημένα ερευνητικά προγράμματα. Ένα από αυτά ήταν και η δημιουργία ενός δικτύου με πολλά από τα χαρακτηριστικά του σημερινού Internet, το οποίο ονομάστηκε ARPANET.

Το δίκτυο αυτό χρηματοδοτήθηκε κατά κύριο λόγο από το υπουργείο Άμυνας των ΗΠΑ στα τέλη της δεκαετίας του 60. Κύριος στόχος του ήταν η διασύνδεση μεταξύ τους πολλών διαφορετικών συστημάτων και δικτύων με διαφανή τρόπο και δυνατότητα να παραμένει σε λειτουργία ακόμα και αν μεγάλα τμήματα του έβγαιναν εκτός λειτουργίας. Το ARPANET είναι από τα πρώτα δίκτυα που χρησιμοποίησε μεταγωγή πακέτων.

Τι είναι η μεταγωγή πακέτων; Τι είναι μεταγωγή γενικά;

Η λέξη μεταγωγή προέρχεται από το ρήμα “μετάγω” που σημαίνει μεταφέρω ή μετακινώ. Ένα δίκτυο που περιγράφεται ως μεταγωγής πακέτων μεταδίδει την χρήσιμη



Σχήμα 1.1: *Δίκτυο Μεταγωγής Πακέτων*

πληροφορία αφού πρώτα την κόψει σε μικρότερα κομμάτια (πακέτα) καθένα από τα οποία περνάει από μια σειρά ενδιάμεσων σταθμών (κόμβων) μέχρι να φτάσει στον προορισμό του, όπως φαίνεται στο σχήμα 1.1.

Το ενδιαφέρον εδώ είναι ότι οι ενδιάμεσοι σταθμοί είναι συνδεδεμένοι μεταξύ τους με πολλούς τρόπους (υπάρχουν περισσότερες από μία διαδρομές για να πάμε από ένα σημείο Α σε ένα Β). Εκτός από την μεταγωγή πακέτων, υπάρχει και η μεταγωγή κυκλώματος η οποία χρησιμοποιείται για τις τηλεφωνικές συνομιλίες στο κλασικό τηλεφωνικό δίκτυο.

Στη μεταγωγή κυκλώματος ο αποστολέας και ο παραλήπτης συνδέονται απευθείας με μια γραμμή (αγωγό), τυπικά μόνο για όση διάρκεια κρατάει η επικοινωνία. Για παράδειγμα, όταν παίρνουμε ένα τηλέφωνο το τηλεφωνικό κέντρο συνδέει απευθείας (με φυσικό κύκλωμα) την τηλεφωνική μας συσκευή με αυτή που καλούμε. Δεν υπάρχουν ενδιάμεσοι σταθμοί και η επικοινωνία ξεκινά με την εγκαθίδρυση της σύνδεσης (όταν ο συνομιλητής μας σηκώσει το ακουστικό!) Στο τέλος της συνομιλίας μας το τηλεφωνικό κέντρο αποσυνδέει το κύκλωμα το οποίο μπορεί να

χρησιμοποιηθεί για άλλη σύνδεση.

Προφανώς στη μεταγωγή κυκλώματος κάθε σύνδεση μπορεί να χρησιμοποιηθεί μόνο για μια συνομιλία, ενώ στη μεταγωγή πακέτων οι ενδιάμεσοι κόμβοι μπορούν να δρομολογούν πακέτα που προέρχονται από διαφορετικούς αποστολείς και κατευθύνονται σε διαφορετικούς παραλήπτες. Όπως θα δούμε παρακάτω, το πακέτο περιέχει τις πληροφορίες που χρειάζεται ο κόμβος για να το στείλει (δρομολογήσει) στον προορισμό του.

Για την λειτουργία του ARPANET επιλέχθηκε το 1983 η οικογένεια πρωτοκόλλων TCP/IP και το δίκτυο σταδιακά εξελίχθηκε στο Internet που γνωρίζουμε σήμερα.

Το TCP/IP είναι μια οικογένεια πρωτοκόλλων, με τα δύο βασικότερα, το TCP και το IP να δίνουν και το κύριο όνομα του. Το TCP/IP χρησιμοποιεί *διαστρωματωμένη αρχιτεκτονική*, χωρίζεται δηλ. σε επίπεδα (στρώματα) με τρόπο αντίστοιχο με αυτόν που προτείνεται από το πρότυπο OSI, αλλά χρησιμοποιεί μόνο τέσσερα (4) επίπεδα αντί για επτά (7). Υπάρχει σε γενικές γραμμές μια (όχι απόλυτη) αντιστοιχία των επιπέδων του TCP/IP με αυτά του OSI, που φαίνεται στο σχήμα 1.2.

Σχήμα 1.2: *Μοντέλα Δικτύωσης OSI και TCP/IP*

Τα τρία ανώτερα επίπεδα του TCP/IP περιγράφονται με λεπτομέρεια και διαθέτουν

αντίστοιχα πρωτόκολλα. Το τέταρτο επίπεδο (κάτω από το επίπεδο διαδικτύου) δεν καθορίζεται από το TCP/IP. Απλά το πρωτόκολλο υποδεικνύει ότι το επίπεδο αυτό θα πρέπει να περιέχει λειτουργίες κατάλληλες για την αποστολή πακέτων IP στο φυσικό μέσο του δικτύου. Οι λεπτομέρειες αφήνονται στον κατασκευαστή του εκάστοτε τύπου δικτύου (Ethernet, Token Ring κλπ).

Τα επίπεδα στο TCP/IP είναι:

- **Εφαρμογής** – Αντιστοιχεί στα επίπεδα Εφαρμογής, Παρουσίασης και Συνόδου του OSI
- **Μεταφοράς** – Αντιστοιχεί στο επίπεδο Μεταφοράς του OSI
- **Διαδικτύου** – Αντιστοιχεί στο επίπεδο Δικτύου του OSI
- **Ζεύξης ή Πρόσβασης Δικτύου** – Αντιστοιχεί στα επίπεδα Φυσικό και Ζεύξης Δεδομένων του OSI

Όπως αναφέραμε ήδη το TCP/IP είναι μια οικογένεια πρωτοκόλλων και παίρνει το όνομα του από τα δύο πιο σημαντικά πρωτόκολλα που περιέχει. Η δομή και λειτουργία του περιγράφεται στα έγγραφα RFC1122 και RFC1123.

Τι είναι τα έγγραφα RFC;

Τα RFC ή *Request For Comments* είναι έγγραφα που συντάσσονται από μηχανικούς και επιστήμονες της πληροφορικής οι οποίοι ασχολούνται με την ανάπτυξη του TCP/IP και του Internet γενικότερα. Σε αυτά περιγράφονται αλλαγές, επισημάνσεις, νέες δυνατότητες ή διορθώσεις. Τα έγγραφα αυτά κατατίθενται στον οργανισμό IETF (Internet Engineering Task Force) όπου ακολουθεί σχολιασμός και συζήτηση. Κάποιες από τις αλλαγές που προτείνονται τελικά ενσωματώνονται σε επόμενες εκδόσεις του πρωτοκόλλου.

Η ιδέα του RFC ξεκίνησε το 1969 από την ανάγκη εξέλιξης του ARPANET. Τα πρώτα RFC δακτυλογραφούνταν και κυκλοφορούσαν προς σχολιασμό από τα μέλη που ανέπτυσσαν το ARPANET. Ο τίτλος “αναζήτηση σχολίων” βοηθούσε να γίνεται εποικοδομητική συζήτηση (δεν θεωρούνταν ότι τα έγγραφα αυτά περιγράφουν μια τελική λύση, ή ότι η γνώμη του συγγραφέα είναι πιο σημαντική από των υπολοίπων). Σήμερα τα RFC είναι πιο επίσημα έγγραφα με τυποποιημένη μορφή, ενώ ο ρόλος που είχαν τα αρχικά αυτά RFC τώρα γίνεται μέσω των εγγράφων *Internet Drafts*.

Το RFC1122 προδιαγράφει τέσσερα (4) επίπεδα-στρώματα για το TCP/IP. Πολλές φορές στη βιβλιογραφία χρησιμοποιούνται 4+1 στρώματα. Στο στρώμα *Διεπαφής Δικτύου* χρησιμοποιούνται τα δύο αντίστοιχα του προτύπου OSI.

1. **Επίπεδο Πρόσβασης (Διεπαφής) Δικτύου** (Network Access ή Link Layer) – Όπως αναφέραμε, το TCP/IP δεν αναφέρεται με λεπτομέρεια στις λειτουργίες αυτού του επιπέδου. Το επίπεδο πρόσβασης δικτύου πρέπει να παρέχει λειτουργίες τέτοιες ώστε να μπορεί να στέλνει πακέτα IP στο δίκτυο χρησιμοποιώντας κάποιο πρωτόκολλο. Στη θέση αυτού του επιπέδου συνήθως αναφέρονται και χρησιμοποιούνται τα δύο αντίστοιχα επίπεδα του OSI:

   - **Φυσικό**
   - **Ζεύξης Δεδομένων**

2. **Επίπεδο Διαδικτύου** (Internet Layer) – Σε γενικές γραμμές ισχύει ότι και στο επίπεδο δικτύου του OSI. Μια σημαντική διαφορά είναι ότι στο OSI ορίζονται τόσο υπηρεσίες με σύνδεση όσο και χωρίς σύνδεση. Στο TCP/IP, το **βασικό πρωτόκολλο του επιπέδου Διαδικτύου είναι το IP** το οποίο προσφέρει μόνο *υπηρεσίες χωρίς σύνδεση*. Αυτό σημαίνει ότι τα πακέτα IP δρομολογούνται ανεξάρτητα το ένα από το άλλο μέσα στο δίκτυο και η παράδοση τους στο επίπεδο Διαδικτύου του παραλήπτη δεν είναι σίγουρα αξιόπιστη. Τα πακέτα μπορεί να φτάσουν με διαφορετική σειρά, με λάθη, ή το ίδιο πακέτο παραπάνω από μια φορές. Τα προβλήματα αυτά πρέπει να διορθωθούν σε ανώτερα επίπεδα.

3. **Επίπεδο Μεταφοράς** (Transport Layer) – Σε γενικές γραμμές ισχύει ότι και στο επίπεδο μεταφοράς του OSI. Στο επίπεδο αυτό παρέχονται υπηρεσίες τόσο **προσανατολισμένες στη σύνδεση (connection oriented)** όσο και **χωρίς σύνδεση (connectionless)**.

   Οι υπηρεσίες με σύνδεση υποστηρίζονται από το **πρωτόκολλο ελέγχου μετάδοσης TCP (Transmission Control Protocol)**. Για να πραγματοποιηθούν, πρέπει να γίνει μια αρχική επικοινωνία αποστολέα – παραλήπτη και να συμφωνηθεί ο τρόπος μεταφοράς των δεδομένων. Αποκαθίσταται έτσι μια λογική σύνδεση για όση ώρα κρατάει η μετάδοση. Οι συνδέσεις αυτές χαρακτηρίζονται από **αξιοπιστία** καθώς διαθέτουν δυνατότητα ελέγχου δεδομένων και διόρθωσης σφαλμάτων ενώ τα μηνύματα έχουν αρίθμηση προκειμένου να γίνει επανασύνθεση τους με τη σωστή σειρά.

   Οι υπηρεσίες χωρίς σύνδεση (ασυνδεσμικές) υποστηρίζονται από το **πρωτόκολλο αυτοδύναμων πακέτων χρήστη UDP (User Datagram Protocol)**. Δεν παρέχουν αξιοπιστία ούτε υπάρχει η έννοια της λογικής σύνδεσης. Είναι όμως απλούστερες, χωρίς καθυστερήσεις και μπορούν να χρησιμοποιηθούν και από συσκευές χωρίς ιδιαίτερη υπολογιστική ισχύ.

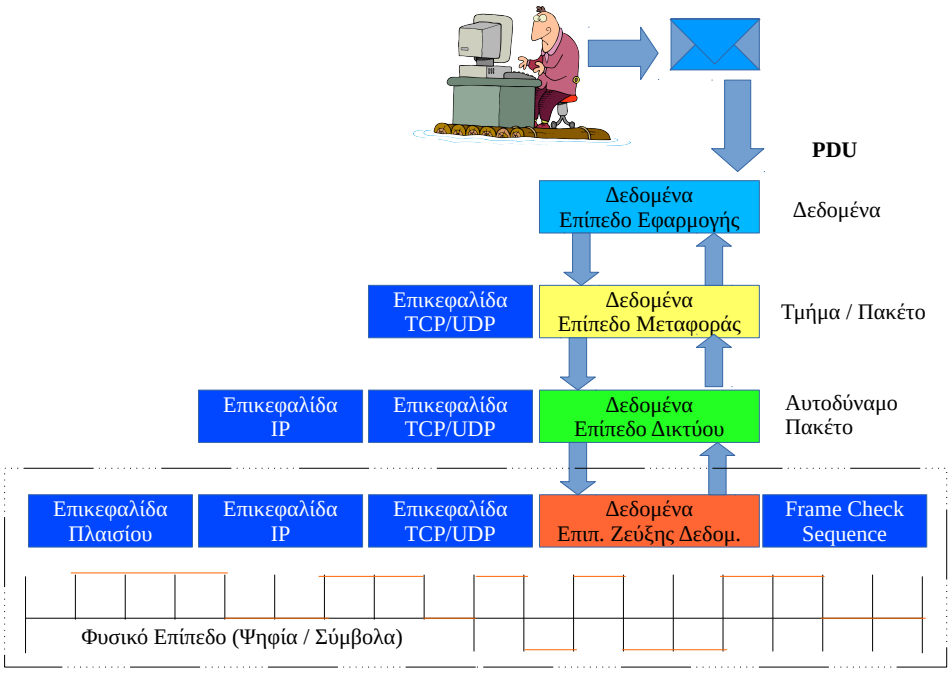
4. **Επίπεδο Εφαρμογής** (Application Layer) – Περιλαμβάνει πρωτόκολλα που αναφέρονται σε υπηρεσίες τελικού χρήστη: Το HTTP για τη μεταφορά ιστο-

σελίδων, το FTP για τη μεταφορά αρχείων, το TELNET για απομακρυσμένη σύνδεση τερματικού, τα SMTP/POP3/IMAP για ηλεκτρονικό ταχυδρομείο και πολλά ακόμα.

1.3 Ενθυλάκωση

Τι σημαίνει ενθυλάκωση;

Προέρχεται από το ρήμα ενθυλακώνω που σημαίνει “βάζω σε θύλακα (τσέπη)”. Εδώ χρησιμοποιείται για να εξηγήσει πως κάθε επίπεδο προσθέτει τις δικές του πληροφορίες (με τη μορφή επικεφαλίδας) στα δεδομένα που έχει λάβει από το πιο πάνω επίπεδο. Ο αντίστοιχος αγγλικός όρος είναι *encapsulation*.



Σχήμα 1.3: *Ενθυλάκωση (encapsulation)*

Όπως έχουμε ήδη εξηγήσει στο πρότυπο OSI, σε μια επικοινωνία μεταξύ των κόμβων Α και Β, το κάθε επίπεδο του Α φαίνεται να επικοινωνεί απευθείας με το αντίστοιχο (ομότιμο) επίπεδο του Β. Έτσι για παράδειγμα το επίπεδο εφαρμογής του

Α φαίνεται να επικοινωνεί απευθείας με το επίπεδο εφαρμογής του Β. Θυμηθείτε την εργαστηριακή επίδειξη του πρωτοκόλλου SMTP, που είναι ένα από τα κλασικά πρωτόκολλα στο επίπεδο εφαρμογής. Καθώς το επίπεδο εφαρμογής είναι το υψηλότερο, οι εντολές που χρησιμοποιεί είναι αρκετά κατανοητές από τον άνθρωπο και είδαμε ότι μπορούμε να τις δώσουμε από το τερματικό. Κατά τη διάρκεια της επικοινωνίας μας με τον SMTP δίναμε μόνο εντολές που είχαν να κάνουν με την αποστολή ενός μηνύματος ταχυδρομείου σε μια αντίστοιχη διεύθυνση ηλεκτρονικού ταχυδρομείου: δεν ασχοληθήκαμε καθόλου με λεπτομέρειες όπως τη διεύθυνση IP του εξυπηρετητή, ή τον τρόπο αποστολής των πακέτων από τον ένα υπολογιστή στο άλλο. Όλα αυτά δεν απασχολούν το πρωτόκολλο εφαρμογής γιατί εξυπηρετούνται από πρωτόκολλα σε χαμηλότερα επίπεδα. Αν και η επίδειξη έγινε ανάμεσα σε δύο μηχανήματα του εργαστηρίου, ακόμα και αν γινόταν μεταξύ ενός τοπικού και ενός απομακρυσμένου μηχανήματος, δεν θα άλλαζε σε κάτι όσο αφορά τις δικές μας εντολές. Το πρωτόκολλο εφαρμογής της μιας μεριάς φαίνεται να επικοινωνεί απευθείας με το πρωτόκολλο εφαρμογής της άλλης.

Ωστόσο η πραγματικότητα είναι διαφορετική: αν και το πρωτόκολλο εφαρμογής νομίζει το ίδιο ότι μιλάει απευθείας με το ομότιμο του στην άλλη πλευρά, στην πραγματικότητα τα δεδομένα που παράγει προωθούνται στα παρακάτω, κατώτερα επίπεδα. Σε κάθε επίπεδο προστίθεται στα δεδομένα του προηγούμενου μια νέα επικεφαλίδα.

Τι είναι η επικεφαλίδα;

Φανταστείτε ότι θέλετε να στείλετε ένα γράμμα (κανονικό, όχι email). Τα περιεχόμενα του γράμματος είναι τα δεδομένα σας. Το βάζετε σε ένα φάκελο. Αυτός είναι ο θύλακας (μόλις κάνατε μια ενθυλάκωση!) Πάνω στο φάκελο γράφετε τη διεύθυνση σας και τη διεύθυνση παραλήπτη. Αυτή είναι η επικεφαλίδα του πρωτοκόλλου εφαρμογής. Το ρίχνετε στο ταχυδρομείο και από κει και πέρα δεν ξέρετε με ποιο τρόπο θα πάει. Όσο αφορά εσάς, το γράμμα σας απλά θα πάει στο ίδιο επίπεδο στην άλλη μεριά (τον παραλήπτη).

Έστω ότι το γράμμα σας πηγαίνει από Χανιά στην Θεσσαλονίκη. Στο ταχυδρομείο, όλα τα γράμματα που κατευθύνονται προς Θεσσαλονίκη θα μπουν σε ένα μεγάλο σάκο με ένδειξη “Θεσσαλονίκη”. Το ταχυδρομείο έκανε ακόμα μια ενθυλάκωση: πήρε το γράμμα σας και το περιέκλεισε σε ένα άλλο “φάκελο” προσθέτοντας τη δική του επικεφαλίδα. Ο σάκος θα πάει στην αεροπορική εταιρεία όπου θα μπει σε ένα κοντέινερ μαζί με άλλα δέματα και αποσκευές και θα κολληθεί ένα bar code που αντιστοιχεί στο αεροδρόμιο Θεσσαλονίκης. Ακόμα μια ενθυλάκωση.

Καθώς φαντάζεστε, στην πλευρά του παραλήπτη υπάρχει η αντίστροφη διαδικασία, όπου διαδοχικά αφαιρούνται οι επικεφαλίδες και ακολουθείται μια διαδικασία πα-

ράδοσης μέχρι τον τελικό παραλήπτη. Τίποτα όμως από αυτή τη διαδικασία δεν είναι γνωστή (και ούτε ενδιαφέρει) τον παραλήπτη ή αποστολέα (επίπεδο εφαρμογής).

Στο TCP/IP έχουμε ακριβώς την ίδια διαδικασία, καθώς και αυτό είναι ένα διαστρωματωμένο πρωτόκολλο: το κάθε επίπεδο δημιουργεί μια επικεφαλίδα που περιέχει πληροφορίες απαραίτητες για το αντίστοιχο επίπεδο της άλλης μεριάς. Π.χ. σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου, το επίπεδο εφαρμογής θα βάλει τις διευθύνσεις email παραλήπτη και αποστολέα. Στην πραγματικότητα βέβαια το μήνυμα δεν θα πάει απευθείας αλλά θα περάσει διαδοχικά από τα επίπεδα μεταφοράς, δικτύου και διεπαφής δικτύου. Σε καθένα από αυτά τα επίπεδα θα προστεθεί η αντίστοιχη επικεφαλίδα που είναι απαραίτητη ώστε το επίπεδο να επικοινωνεί με το αντίστοιχο της άλλης μεριάς. Η επικεφαλίδα περιέχει ουσιαστικά πληροφορίες ελέγχου για να μπορεί να γίνει σωστά η ανασύνθεση των δεδομένων στην άλλη μεριά (τα δεδομένα μπορεί να μεταφέρονται σε μικρά κομμάτια). Σε κάποια επίπεδα (όπως στο 2ο του OSI) προστίθενται και πληροφορίες στο τέλος που έχουν να κάνουν με διόρθωση και έλεγχο σφαλμάτων μετάδοσης στο φυσικό μέσο. Η προσθήκη σαν περίβλημα των πληροφοριών ελέγχου με τη μορφή της επικεφαλίδας είναι η ενθυλάκωση.

Σε κάθε επίπεδο στο TCP/IP η μορφή των δεδομένων που προκύπτει μετά την ενθυλάκωση έχει συγκεκριμένη ονομασία (αν και πολλές φορές παρασυρόμαστε και λέμε παντού τη λέξη “πακέτο”). Η μορφή γενικά ονομάζεται **PDU, Protocol Data Unit** ή **Βασική Μονάδα Πληροφορίας Πρωτοκόλλου**. Στο TCP/IP έχουμε τα παρακάτω PDU:

- **Επίπεδο Εφαρμογής:** *Δεδομένα*
- **Επίπεδο Μεταφοράς:** *Τμήμα (Segment) στο TCP ή Πακέτο (Packet) στο UDP*
- **Επίπεδο Δικτύου:** *Αυτοδύναμο Πακέτο IP (IP Datagram)*
- **Επίπεδο Διεπαφής Δικτύου:** *Πλαίσιο (Frame) (για δίκτυα Ethernet, στο υποεπίπεδο ζεύξης δεδομένων* και *Δυαδικά ψηφία - σύμβολα (Bits / Symbols) στο φυσικό υποεπίπεδο*)

Έχουμε ήδη αναφέρει ότι το TCP/IP δεν ορίζει ακριβώς τι γίνεται στο κατώτερο επίπεδο. Η μόνη απαίτηση εδώ είναι να μπορεί να μεταφέρει με κάποιο τρόπο τα αυτοδύναμα πακέτα IP που δημιουργούνται, στο φυσικό μέσο. Ένα αυτοδύναμο πακέτο IP από το επίπεδο διαδικτύου τοποθετείται μέσα (ενθυλακώνεται) σε ένα πλαίσιο (frame) που δημιουργείται στο επίπεδο ζεύξης δεδομένων. Το πλαίσιο έχει την δική του επικεφαλίδα καθώς και κάποιες πληροφορίες ελέγχου στο τέλος (Frame Check Sequence, ακολουθία ελέγχου πλαισίου ή FCS). Με απλά λόγια, ένα “πακέτο” ανώτερου επιπέδου τοποθετείται εξ’ολοκλήρου (ενθυλακώνεται) μέσα σε ένα “πακέτο” του αμέσως κατώτερου επιπέδου. Η διαδικασία αυτή γίνεται τυπικά από το πρό-

γραμμα οδήγησης (driver) της κάρτας δικτύου.

Οι πληροφορίες ελέγχου που προστίθενται κατά τη διαδικασία ελέγχου είναι κυρίως *διευθύνσεις, χαρακτήρες ελέγχου σφαλμάτων ή άλλοι χαρακτήρες ελέγχου και συγχρονισμού*. Στο φυσικό πλέον επίπεδο τα μηδέν και ένα (δυαδικά ψηφία) που απαρτίζουν το πλαίσιο μετατρέπονται σε κατάλληλα ηλεκτρικά σήματα για να μεταδοθούν μέσα από το φυσικό μέσο. Η διαδικασία αυτή γίνεται από το υλικό (hardware) της κάρτας δικτύου. Στη λήψη δεδομένων γίνεται η ακριβώς αντίστροφη διαδικασία, με τα δεδομένα να κινούνται προς τα ανώτερα επίπεδα όπου αφαιρούνται διαδοχικά οι επικεφαλίδες, μέχρι να φτάσουμε στο επίπεδο εφαρμογής.

Κεφάλαιο 2

Τοπικά Δίκτυα – Επίπεδο Πρόσβασης Δικτύου TCP/IP

2.1 Φυσικό Επίπεδο - Επίπεδο Σύνδεσης (Ζεύξης) Δεδομένων (Μοντέλο OSI)

Το χαμηλότερο επίπεδο στο OSI, όπως έχουμε ήδη αναφέρει, είναι το *φυσικό*. Το επίπεδο αυτό είναι υπεύθυνο για τη μετάδοση των bits μέσα από το ενσύρματο ή ασύρματο τηλεπικοινωνιακό κανάλι. Το φυσικό επίπεδο καθορίζει τα ηλεκτρικά και μηχανικά χαρακτηριστικά της σύνδεσης του σταθμού με το μέσο μετάδοσης.

Τα μηχανικά χαρακτηριστικά καθορίζουν λεπτομέρειες όπως το είδος του συνδέτη (βύσματος) του δικτύου, τις διαστάσεις του, τις ανοχές, το πλήθος των ακροδεκτών, τον τρόπο με τον οποίο ασφαλίζει πάνω στο δικτυακό εξοπλισμό κλπ. Τα *ηλεκτρικά χαρακτηριστικά* καθορίζουν τον τρόπο με τον οποίο αναπαρίστανται τα bit 0 και 1 στο φυσικό μέσο (π.χ. τα επίπεδο τάσης σε ένα ενσύρματο δίκτυο που αναπαριστούν σε ηλεκτρικό σήμα τα 0 και 1). Στο φυσικό επίπεδο επίσης καθορίζεται αν η μετάδοση μπορεί να γίνει μόνο προς μια μεριά (half duplex) ή και προς τις δύο (full duplex) ταυτόχρονα. Το φυσικό επίπεδο δεν ενδιαφέρεται αν αυτό που μεταφέρει είναι bytes (8bits) ή χαρακτήρες ASCII των 7bits.

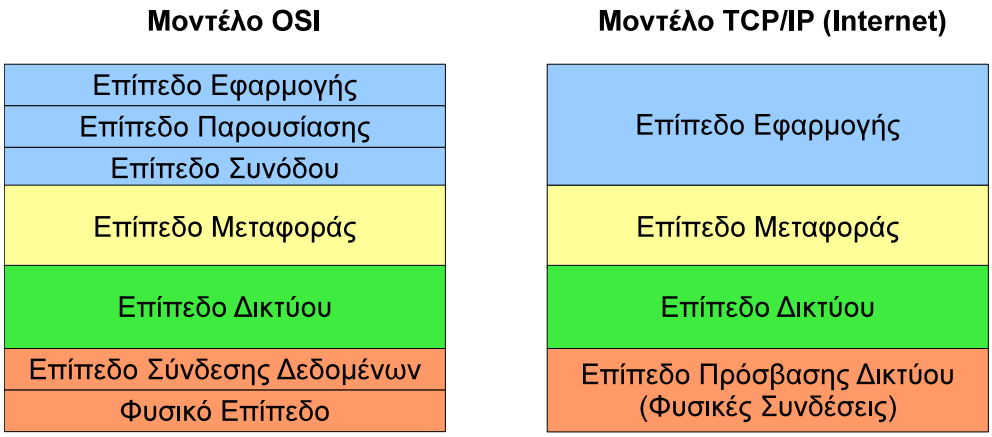
Τι είναι το ASCII; Υπάρχει 7bit ASCII;

Το ASCII είναι ίσως από τα πλέον παλιά, κοινά αποδεκτά πρότυπα των υπολογιστών. Προέρχεται από τα αρχικά των λέξεων American Standard Code for Information Interchange και είναι ένας κώδικας που αντιστοιχεί κάθε γράμμα του λατινικού αλ-

φαβήτου σε ένα αριθμό. Έτσι για παράδειγμα το Α αντιστοιχεί στο 65, το Β στο 66 κ.ο.κ. Εκτός από τα γράμματα κωδικοποιούνται αντίστοιχα τα ψηφία από 0 ως 9 και διάφορα σύμβολα. Για παράδειγμα το θαυμαστικό (!) είναι το 33, τα εισαγωγικά το 34 και το κενό διάστημα το 32. Οι χαρακτήρες από 0-31 δεν χρησιμοποιούνται για κανονικά γράμματα ή σύμβολα αλλά περιέχουν χαρακτήρες ελέγχου. Αυτοί όταν εκτυπώνονται εκτελούν κάποια ειδική λειτουργία ανάλογα με το τερματικό που χρησιμοποιείται. Π.χ. ο χαρακτήρας 7 στέλνει ηχητικό σήμα στο μεγαφωνάκι του τερματικού (ονομάζεται BEL(L) για ιστορικούς λόγους, που θα σας αναφέρω στο μάθημα!). Άλλοι ειδικοί χαρακτήρες μπορεί π.χ. να μετακινούν το δρομέα πάνω στην οθόνη κ.λ.π.

Αν χρησιμοποιήσουμε 7bit για το ASCII, μπορούμε να έχουμε ως 128 χαρακτήρες. Στις περισσότερες περιπτώσεις χρησιμοποιούμε 8bit ASCII (256 χαρακτήρες) που είναι απαραίτητο για να βάλουμε επιπλέον αλφάβητο εκτός από το λατινικό.

Φυσικά στις μέρες μας τίποτα από τα δύο δεν αρκεί, καθώς στο Internet χρειαζόμαστε ταυτόχρονα πολύ περισσότερους χαρακτήρες από ότι προσφέρει το ASCII. Η ανάγκη αυτή καλύπτεται με τεχνολογίες όπως το unicode.



Σχήμα 2.1: *Μοντέλα OSI και TCP/IP*

Ακριβώς πάνω από το φυσικό επίπεδο του OSI, βρίσκεται το *επίπεδο σύνδεσης (ζεύξης) δεδομένων - Data Link Layer*. Το επίπεδο αυτό έχει σκοπό να κάνει αξιόπιστη τη φυσική γραμμή σύνδεσης μεταξύ δύο σταθμών. Το επίπεδο αυτό λαμβάνει τα δεδομένα του από το πιο πάνω επίπεδο (επίπεδο δικτύου) με τη μορφή πακέτων. Από αυτά τα πακέτα δημιουργεί πλαίσια δεδομένων. Το επίπεδο σύνδεσης δεδομένων:

- Δημιουργεί πλαίσια δεδομένων από τα πακέτα που λαμβάνει. Σε κάθε πλαίσιο

προσθέτει κατάλληλη επικεφαλίδα (header) και ουρά (trailer)

- Ανιχνεύει τα σφάλματα μετάδοσης και είτε τα διορθώνει είτε ζητά την επανεκπομπή τους
- Ελέγχει πότε μπορεί να δεσμεύσει το φυσικό μέσο ώστε να ξεκινήσει την αποστολή των πλαισίων χωρίς κίνδυνο σύγκρουσης με άλλο σταθμό
- Μεταβάλλει την ροή των πλαισίων ανάλογα με τους ρυθμούς που μπορεί να δεχθεί ο παραλήπτης

Όπως έχουμε ήδη αναφέρει, το κατώτερο επίπεδο στο TCP/IP είναι το πρόσβασης δικτύου το οποίο αντιστοιχεί στα δύο επίπεδα του OSI που περιγράψαμε παραπάνω (σχήμα 2.1). Το επίπεδο πρόσβασης δικτύου παρέχει την πρόσβαση στο φυσικό μέσο στο οποίο η πληροφορία μεταδίδεται με μορφή πακέτων και αντιπροσωπεύει το χαμηλότερο επίπεδο λειτουργικότητας που απαιτείται από ένα δίκτυο. Το επίπεδο αυτό περιλαμβάνει όλα τα στοιχεία των φυσικών συνδέσεων (καλώδια, αναμεταδότες, κάρτες δικτύου, πρωτόκολλα πρόσβασης τοπικών δικτύων) και προσφέρει τις υπηρεσίες του στο επίπεδο δικτύου. Το TCP/IP δεν καθορίζει τον ακριβή τρόπο λειτουργίας του επιπέδου αυτού, αφού απλά προδιαγράφει ότι πρέπει να είναι ικανό να μεταδίδει με κάποιο τρόπο τα δεδομένα που λαμβάνει σε μορφή πακέτων από το επίπεδο δικτύου. Στο επίπεδο αυτό μπορούν να χρησιμοποιούνται διαφορετικές τεχνολογίες και οι λεπτομέρειες τους καθορίζονται από τους κατασκευαστές των δικτύων και των αντίστοιχων συσκευών.

2.2 Η Πρόσβαση στο Μέσο

Σε ένα δίκτυο, το μέσο μεταφοράς (καλώδιο, οπτική ίνα κλπ) είναι κοινό για όλους τους υπολογιστές που συνδέονται σε αυτό. Προκειμένου να εξασφαλιστεί η ομαλή μετάδοση των δεδομένων, θα πρέπει κάθε φορά να μεταδίδει μόνο ένας υπολογιστής. Αν δυο υπολογιστές αποκτήσουν ταυτόχρονα πρόσβαση για μετάδοση στο μέσο, τα πακέτα τους θα συγκρουστούν με αποτέλεσμα την καταστροφή τους. Καμιά από τις δύο μεταδόσεις δεν θα φτάσει στο προορισμό της. Για να έχουμε επιτυχή μετάδοση πρέπει να τηρούνται οι παρακάτω προϋποθέσεις:

- Εισαγωγή των δεδομένων στο μέσο μετάδοσης χωρίς να υπάρχει σύγκρουση με άλλα δεδομένα.
- Ο παραλήπτης να λάβει τα δεδομένα γνωρίζοντας ότι αυτά δεν έχουν καταστραφεί σε σύγκρουση δεδομένων (data collision) κατά τη μετάδοση.

Για να επιτευχθούν τα παραπάνω, σε κάθε δίκτυο υπάρχει μια σειρά από κανόνες με βάση τους οποίους γίνεται η εισαγωγή των δεδομένων στο μέσο μετάδοσης. Οι κανόνες αυτοί αποτελούν τη *μέθοδο προσπέλασης (access method)*. Είναι σημαντικό οι κανόνες αυτοί να είναι κοινοί για όλους τους υπολογιστές ενός συγκεκριμένου δικτύου. Αν κάποιοι υπολογιστές χρησιμοποιούν διαφορετικούς, το δίκτυο θα αποτύχει γιατί κάποιες μέθοδοι προσπέλασης θα κυριαρχήσουν στο καλώδιο. Σε γενικές γραμμές σκοπός των μεθόδων προσπέλασης είναι να εμποδίσουν την ταυτόχρονη εισαγωγή δεδομένων στο μέσο πρόσβασης. Εξασφαλίζοντας ότι μόνο ένας υπολογιστής μεταδίδει δεδομένα κάθε φορά, οι μέθοδοι προσπέλασης κρατούν οργανωμένες τις διαδικασίες αποστολής και λήψης δεδομένων δικτύου.

Υπάρχουν γενικά τρεις τρόποι για την αποφυγή ταυτόχρονης χρήσης του μέσου μετάδοσης:

- Μέθοδοι **Carrier Sense Multiple Access, CSMA** (Πολλαπλής πρόσβασης με ακρόαση φέροντος)
  - Με **Ανίχνευση Σύγκρουσης** (Collision Detection), CSMA/CD
  - Με **Αποφυγή Σύγκρουσης** (Collision Avoidance), CSMA/CA
- Μέθοδος με **Κουπόνι Διέλευσης** (Token Passing) που δίνει δυνατότητα μεμονωμένης αποστολής δεδομένων
- Μέθοδος **Απαίτησης Προτεραιότητας**

Τι είναι το CSMA και το CSMA/CD; (εκτός εξεταστέας ύλης)

Η τεχνική πολλαπλής πρόσβασης με ανίχνευση φέροντος ουσιαστικά σημαίνει ότι πριν αρχίσει η μετάδοση, γίνεται πρώτα ανίχνευση της γραμμής για να διαπιστωθεί αν γίνεται ήδη μετάδοση από κάποιο άλλο υπολογιστή. Το “φέρον” είναι ένα σήμα που υπάρχει στη γραμμή όσο γίνεται οποιαδήποτε μετάδοση. Δεν είναι απαραίτητο για τον υπολογιστή που επιθυμεί να μεταδώσει να προσπαθήσει να διαβάσει τα δεδομένα της γραμμής για να διαπιστώσει αν είναι σε χρήση. Η ανίχνευση του φέροντος είναι μια σχετικά απλή διαδικασία που μπορεί να γίνει ήδη από τα κυκλώματα της κάρτας δικτύου.

Ο υπολογιστής που πρόκειται να μεταδώσει, αν διαπιστώσει την ύπαρξη φέροντος θα περιμένει μέχρι το τέλος της μετάδοσης για να ξεκινήσει. Προσέξτε ότι έτσι αποφεύγεται μόνο το ένα είδος σύγκρουσης!

Αν έχουμε δύο υπολογιστές σε αναμονή για μετάδοση, είναι πιθανόν να ξεκινήσουν και οι δυο ταυτόχρονα με το που θα ελευθερωθεί η γραμμή. Στην περίπτωση αυτή θα έχουμε πάλι σύγκρουση. Εδώ μπορεί να αναλάβει η Ανίχνευση Σύγκρουσης (Collision Detection). Και σε αυτήν την περίπτωση, ένα κύκλωμα στην κάρτα

δικτύου μπορεί να αντιληφθεί ότι στη γραμμή γίνονται παραπάνω από μια μεταδόσεις (άρα έχουμε σύγκρουση). Ένας απλός τρόπος βασίζεται στο γεγονός ότι η ισχύς του σήματος στη γραμμή είναι μεγαλύτερη με δύο μεταδόσεις από ότι με μια. Έτσι γνωρίζουμε ότι τα δεδομένα καταστράφηκαν και σταματάμε τη μετάδοση, κερδίζοντας χρόνο.

Τι είναι το Κουπόνι Διέλευσης;

Είναι ένας διαφορετικός τρόπος να σκεφτούμε την πολλαπλή πρόσβαση: Μέσα στο δίκτυο κυκλοφορεί, από κόμβο σε κόμβο, ένα ειδικό πακέτο (κουπόνι) το οποίο χρησιμοποιείται ως φορέας μεταφοράς δεδομένων. Ο κόμβος που επιθυμεί να μεταδώσει, θα αποσύρει το κουπόνι από το δίκτυο, θα βάλει σε αυτό τα δεδομένα του και θα το ξαναστείλει. Ο παραλήπτης θα πάρει το κουπόνι, θα διαβάσει τα δεδομένα και θα το αφήσει ξανά "άδειο" στο δίκτυο. Το κουπόνι μπορεί έπειτα να το πάρει άλλος κόμβος κ.ο.κ.

Πρότυπα Τοπικών Δικτύων

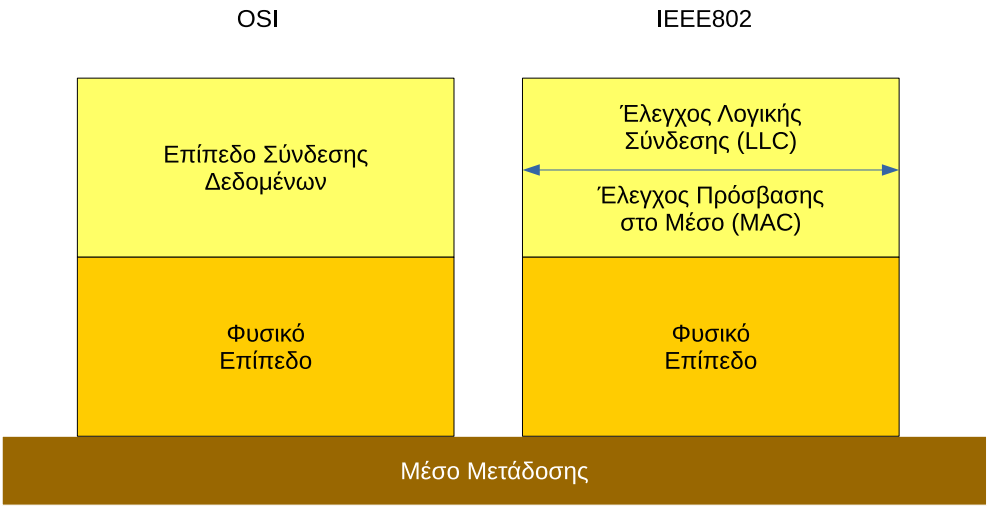
Οι σημαντικότερες τοπολογίες τοπικών δικτύων καθώς και τα πρωτόκολλα που θα χρησιμοποιούνταν από τους σταθμούς εργασίας, αναπτύχθηκαν αρχικά από διάφορες εταιρείες. Ωστόσο διαφορετικοί κατασκευαστές χρησιμοποιούσαν διαφορετικά, δικά του ο καθένας, πρωτόκολλα με αποτέλεσμα να μην είναι συνήθως δυνατή η επικοινωνία υπολογιστών διαφορετικών κατασκευαστών. Η αρχή της τυποποίησης έγινε όταν το *Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών* (IEEE, Institute of Electrical and Electronic Engineers) και η *Ευρωπαϊκή Ένωση Κατασκευαστών Υπολογιστών* (European Computer Manufacturing Association, ECMA) συμφώνησαν να ακολουθήσουν το πρότυπο OSI.

Στο OSI, η ανταλλαγή μηνυμάτων και η επικοινωνία των σταθμών εργασίας αναλύεται σε επτά επίπεδα. Τα δύο κατώτερα είναι το *επίπεδο σύνδεσης δεδομένων* και το *φυσικό επίπεδο*. Σε αυτά καθορίζεται ο τύπος του δικτύου και το πρωτόκολλο επικοινωνίας. Η υλοποίηση των δύο επιπέδων γίνεται με συνδυασμό υλικού και λογισμικού.

Για την δημιουργία του προτύπου, το IEEE δημιούργησε μια επιτροπή γνωστή ως 802 με έργο τον καθορισμό προτύπων για τα τοπικά (LAN) και τα μητροπολιτικά (MAN) δίκτυα.

Τι είναι τα Μητροπολιτικά Δίκτυα; (Metropolitan Area Network, MAN)

Τα μητροπολιτικά δίκτυα καλύπτουν αποστάσεις και γεωγραφικές περιοχές μεγαλύτερες από τα τοπικά δίκτυα αλλά γενικά μικρότερες από αυτές που καλύπτει ένα δίκτυο ευρείας περιοχής.Ένα τοπικό δίκτυο καλύπτει συνήθως τις ανάγκες ενός κτηρίου ή συμπλέγματος κτηρίων, ενώ ένα ευρείας περιοχής μπορεί να ενώνει μεταξύ τους πόλεις ή ακόμα και ηπείρους. Ένα μητροπολιτικό δίκτυο συνήθως έχει μέγεθος τέτοιο ώστε να καλύπτει μια πόλη.



Σχήμα 2.2: *Σχέση Μοντέλων Αναφοράς OSI και IEEE802*

Η επιτροπή 802 χωρίσθηκε σε έξι (6) μικρότερες υποεπιτροπές. Κάθε μια από αυτές ασχολήθηκε με την ανάπτυξη επιμέρους προτύπων για τους διαφορετικούς τύπους δικτύων. Αργότερα δημιουργήθηκαν ακόμα περισσότερες υποεπιτροπές (π.χ. για τα πρότυπα των ασύρματων δικτύων). Τα αποτελέσματα κάθε υποεπιτροπής είναι γνωστά με την ονομασία IEEE 802.x όπου x ο αριθμός της υποεπιτροπής. Για παράδειγμα, η υποεπιτροπή 3 σχεδίασε το πρότυπο IEEE 802.3 στο οποίο βασίζεται το Ethernet που θα εξετάσουμε σε επόμενη ενότητα.

Με βάση το έργο της επιτροπής 802, το δεύτερο επίπεδο του OSI χωρίσθηκε σε δύο υπο-επίπεδα (σχήμα 2.2): το υπο-επίπεδο *Ελέγχου Λογικής Σύνδεσης της Γραμμής* (Logical Line Control, LLC) που περιγράφεται στο IEEE802.2 και το υπο-επίπεδο *Ελέγχου Πρόσβασης στο Μέσο* (Media Access Control, MAC) που περιγράφεται στα IEEE 802.3, IEEE 802.4 και IEEE 802.5.

2.2.1 Έλεγχος Λογικής Σύνδεσης (LLC – IEEE 802.2)

Το υπο-επίπεδο ελέγχου λογικής σύνδεσης είναι το ανώτερο του επιπέδου σύνδεσης δεδομένων και αποτελεί το συνδετικό κρίκο μεταξύ των ανώτερου επιπέδου (επίπεδο δικτύου) και του υπο-επιπέδου ελέγχου πρόσβασης στο μέσο. Κύριος σκοπός του LLC είναι η παροχή υπηρεσιών στο επίπεδο δικτύου το οποίο υποστηρίζεται από τα *"Σημεία Πρόσβασης για Εξυπηρέτηση" (SAPs – Service Access Points)* που παρέχει το LLC. Το LLC με τη σειρά του δέχεται υπηρεσίες από το υπο-επίπεδο MAC.

Τι είναι τα Service Access Points;

Μπορείτε να φανταστείτε τα SAPs σαν τα σημεία διεπαφής των επιπέδων. Για παράδειγμα, γνωρίζουμε ότι το TCP/IP δεν καθορίζει ακριβώς τις λειτουργίες του Επιπέδου Πρόσβασης Δικτύου. Όμως το επίπεδο Δικτύου, που βρίσκεται ακριβώς από πάνω, χρειάζεται να δώσει τις πληροφορίες του (πακέτα IP) σε αυτό το επίπεδο με κάποιο τυποποιημένο τρόπο (και ανεξάρτητα από το είδος του φυσικού δικτύου που ακολουθεί). Για το σκοπό αυτό, το υπο-επίπεδο LLC παρέχει μια τυποποιημένη διεπαφή για την επικοινωνία του με το επίπεδο δικτύου. Η διεπαφή αυτή παρέχει συγκεκριμένες υπηρεσίες και τρόπους επικοινωνίας ώστε να είναι δυνατή η επικοινωνία των επιπέδων. Διαφορετικά, για κάθε διαφορετικό τύπο δικτύου θα έπρεπε να ξαναγράφουμε κάποιες λειτουργίες που ανήκουν στο επίπεδο δικτύου.

Το υπο-επίπεδο LLC μπορεί να παρέχει τις παρακάτω υπηρεσίες:

- **Υπηρεσία Χωρίς Επιβεβαίωση και Χωρίς Σύνδεση** – Unacknowledged Connectionless Service: Στην περίπτωση αυτή, ένα σταθμός εργασίας στέλνει πλαίσια (στο επίπεδο σύνδεσης δεδομένων, δεν έχουμε πλέον πακέτα αλλά πλαίσια, όπως θα δούμε στο Ethernet) στο σταθμό προορισμού χωρίς να περιμένει επιβεβαίωση λήψης. Πριν την έναρξη της επικοινωνίας δεν γίνεται καμιά συνεννόηση μεταξύ των σταθμών και ούτε υπάρχει διαδικασία τερματισμού σύνδεσης μετά το τέλος της μετάδοσης. Αν τα δεδομένα (π.χ. λόγω θορύβου) αλλοιωθούν ή χαθούν δεν γίνεται κάποια προσπάθεια επανάκτησης των αντίστοιχων πλαισίων. Καθώς δεν υπάρχει διαδικασία έναρξης σύνδεσης, η υπηρεσία αυτή παρέχει τη μικρότερη καθυστέρηση στην επικοινωνία και χρησιμοποιείται κυρίως για μεταδόσεις όπου το φυσικό μέσο παρουσιάζει μικρό ποσοστό λαθών και όπου η επανάκτηση λανθασμένων δεδομένων μπορεί να γίνει από ανώτερα επίπεδα.
- **Υπηρεσία με Επιβεβαίωση Λήψης Χωρίς Σύνδεση** – Acknowledged Connectionless Service: Όπως και στην προηγούμενη υπηρεσία, δεν εγκα-

θίσταται σύνδεση πριν την έναρξη της μετάδοσης των δεδομένων. Για κάθε πλαίσιο όμως, ο παραλήπτης στέλνει ένα αντίστοιχο πλαίσιο επιβεβαίωσης λήψης. Η υπηρεσία αυτή εφαρμόζεται κυρίως σε συνδέσεις σημείου προς σημείου (point to point).

- **Υπηρεσία με Σύνδεση** – Connection Oriented Service: Πρόκειται για την πιο πολύπλοκη υπηρεσία που παρέχεται από το υπο-επίπεδο LLC. Για την έναρξη της επικοινωνίας, ο σταθμός εργασίας πρέπει να επικοινωνήσει με το σταθμό προορισμού και να εγκαταστήσει με αυτόν ένα *νοητό κύκλωμα*. Η διαδικασία αυτή ουσιαστικά σημαίνει την εύρεση μιας συγκεκριμένης διαδρομής μέσω ενδιάμεσων κόμβων την οποία και θα ακολουθήσουν όλα τα πλαίσια μέχρι να φτάσουν στο προορισμό τους. Κατά τη διάρκεια της μετάδοσης γίνεται επίσης επιβεβαίωση λήψης κάθε πλαισίου καθώς και έλεγχος ροής των δεδομένων (ο έλεγχος ροής εξασφαλίζει ότι ο αποστολέας κάθε φορά θα στέλνει όσα δεδομένα είναι έτοιμος να δεχθεί ο παραλήπτης ώστε να αποφευχθούν φαινόμενα υπερχείλισης). Ο έλεγχος ροής αναφέρεται στο επίπεδο δικτύου.

  Η διαδικασία εγκατάστασης νοητού κυκλώματος περιλαμβάνει τρία στάδια:

  – **Την εγκατάσταση σύνδεσης:** Οι δύο σταθμοί δημιουργούν το νοητό κύκλωμα και ανταλλάσσουν κάποιες αρχικές τιμές για μεταβλητές και μετρητές που χρειάζονται για να παρακολουθήσουν τη μετάδοση των πλαισίων (παράδειγμα: συμφωνούν για πόση ώρα θα περιμένει ο αποστολέας μια επιβεβαίωση πλαισίου μέχρι να θεωρήσει ότι χάθηκε για να το μεταδώσει ξανά)

  – **Τη μεταφορά δεδομένων:** Μεταδίδονται τα πλαίσια και επιβεβαιώνεται η λήψη τους

  – **Το τερματισμό της σύνδεσης:** Στη φάση αυτή ελευθερώνονται οι μεταβλητές και μετρητές, αποδεσμεύεται το φυσικό μέσο (τερματίζεται το νοητό κύκλωμα) και γενικά σταματά η χρήση οποιουδήποτε μέσου χρησιμοποιήθηκε για την επίτευξη της επικοινωνίας

2.4 Δίκτυα ETHERNET (10/100/1000Mbps)

Το γνωστό μας πρότυπο Ethernet βασίζεται στις προδιαγραφές IEEE 802.3 αλλά καθώς εξελίσσεται έχουν δημιουργηθεί διάφορες παραλλαγές του.

Η κωδικοποίηση των βασικών προτύπων γίνεται με την παρακάτω ονοματοδοσία:

X Base/Broadband Y

Όπου:

- Το **X** είναι η ταχύτητα μετάδοσης των δεδομένων σε Mbps
- Το **Base** υποδηλώνει μετάδοση **Βασικής Ζώνης** ένω το **Broad** μετάδοση **Ευρείας Ζώνης** (τύπος σηματοδοσίας)
- Το **Y** υποδηλώνει το **μέγιστο μήκος** του **τμήματος (segment)**

Τι είναι η σηματοδοσία βασικής και τι η ευρείας ζώνης;

Όταν έχουμε να μεταδώσουμε ένα σήμα (είτε αναλογικό είτε ψηφιακό) μέσα από κάποιο φυσικό μέσο, υπάρχουν διάφορες πιθανότητες:

- Το φυσικό μέσο να μπορεί να μεταδώσει το σήμα όπως είναι αυτούσιο: Για παράδειγμα, το ηλεκτρικό σήμα (αναλογικό) μιας τηλεφωνικής συνομιλίας μπορεί να μεταδοθεί μέσα από τη γραμμή του τηλεφώνου χωρίς να χρειάζεται καμιά αλλαγή σε αυτό. Σε αυτή την περίπτωση έχουμε **μετάδοση βασικής ζώνης**.
- Αντίθετα, αν θέλουμε για παράδειγμα να μεταδώσουμε μουσική μέσω ραδιοκυμάτων (σκεφτείτε το ραδιόφωνο), δεν μπορούμε να μεταδώσουμε απευθείας το ηλεκτρικό σήμα που αντιστοιχεί στον ήχο στον αέρα. Αντίθετα, πρέπει να χρησιμοποιήσουμε μια συχνότητα που είναι κατάλληλη για εκπομπή (σκεφτείτε όταν συντονίζετε το ραδιόφωνο σε ένα σταθμό) και πάνω σε αυτή να “φορτώσουμε” τα δεδομένα μας (τη μουσική). Αυτή είναι μια διαδικασία γνωστή ως διαμόρφωση: ουσιαστικά έχουμε μετατρέψει την αρχική μορφή των δεδομένων μας με τρόπο κατάλληλο για τη μετάδοση από το φυσικό μέσο. Αυτή είναι μια **μετάδοση ευρείας ζώνης**.

Τι είναι το Τμήμα Ethernet; (Ethernet Segment)

Σύμφωνα με τις προδιαγραφές του Ethernet, ένα τμήμα περιέχει το ομοαξονικό καλώδιο που χρησιμοποιείται ως φυσικό μέσο και τους υπολογιστές που βρίσκονται πάνω σε αυτό. Όταν φτάσουμε στο μέγιστο μήκος τμήματος, αν χρειάζεται να μεγαλώσουμε περισσότερο το δίκτυο χρησιμοποιούμε *αναμεταδότες* (repeaters), ενώνοντας μεταξύ τους περισσότερα τμήματα. Υπάρχουν συγκεκριμένοι κανόνες και περιορισμοί στο πόσα τμήματα και αναμεταδότες μπορούν να συνδεθούν (δείτε τον κανόνα 5-4-3 στην Wikipedia αν ενδιαφέρεστε για λεπτομέρειες). Γιατί όμως δεν μπορούμε να μεγαλώσουμε απλά το καλώδιο;

Μπορούμε να σκεφτούμε δύο βασικούς λόγους:

- Ανάλογα με τον τύπο του καλωδίου, οι απώλειες μετά από μια απόσταση μπορεί να είναι τέτοιες που (σε συνδυασμό και με το θόρυβο) να οδηγούν σε ανα-

ξιόπιστη μετάδοση

- Όταν γίνεται μια σύγκρουση στο δίκτυο, από μια απόσταση και μετά είναι πιθανόν οι σταθμοί να μη λαμβάνουν έγκαιρα το σήμα σύγκρουσης και να συνεχίζουν να μεταδίδουν

Στον πίνακα 2.1 αναφέρονται βασικά πρότυπα του IEEE 802.3 και τα χαρακτηριστικά τους.

Τύπος Δικτύου	**Μέσο Μετάδοσης**	**Μέθοδος Σηματοδοσίας**	**Ρυθμός Δεδομένων**	**Μέγιστο Μήκος Τμήματος**	**Τοπολογία**
10Base5	Ομοαξονικό 50 Ohm Thick	Βασικής Ζώνης	10 Mbps	500 m	Αρτηρίας
10Base2	Ομοαξονικό 50 Ohm Thin (RG-58)	Βασικής Ζώνης	10 Mbps	185 m	Αρτηρίας
1Base5	Αθωράκιστο συνεστραμμένο (UTP)	Βασικής Ζώνης	1 Mbps	250 m	Αστέρα
10BaseT	Αθωράκιστο συνεστραμμένο (UTP)	Βασικής Ζώνης	10 Mbps	100 m	Αστέρα
10Broad36	Ομοαξονικό 75 Ohm	Ευρείας Ζώνης	10 Mbps	3600 m	Αρτηρίας

Πίνακας 2.1: *Βασικά πρότυπα του IEEE 802.3 και τα χαρακτηριστικά τους*

Το πρότυπο Ethernet II είναι παρόμοιο με το 10Base5.

Εκτός από τις βασικές εκδόσεις Ethernet που αναφέρονται στον πίνακα, υπάρχουν και εκδόσεις για άλλα μέσα μετάδοσης, π.χ. για οπτική ίνα. Αυτά αναφέρονται με κωδικοποίηση 10Base-F (Fiber Ethernet).

Το πρότυπο *10Base-F* βασίζεται στην προδιαγραφή *FOIRL, Fiber Optic InterRepeater Link* η οποία δημιουργήθηκε για τη σύνδεση επαναληπτών (repeaters) μεταξύ τους με οπτικές ίνες. Συνήθως χρησιμοποιείται διπλή πολύτροπη οπτική ίνα 62.5/125 μm σε συνδυασμό με υπέρυθρο φως από LEDs. Η πιο συνηθισμένη παραλλαγή του προτύπου 10Base-F είναι η 10Base-FL που χρησιμοποιείται στη διασύνδεση κυρίως επαναληπτών σε απόσταση ως 2Km.

Πως μεταφέρουν πληροφορία οι οπτικές ίνες; Τι είναι οι πολύτροπες και τι οι μονότροπες οπτικές ίνες;

Οι οπτικές ίνες είναι ένα μέσο μετάδοσης φτιαγμένο να μεταδίδει φως αντί για ηλεκτρικό σήμα. Ουσιαστικά το φως εισέρχεται στο ένα άκρο της ίνας και μετά από διαδοχικές ανακλάσεις (φανταστείτε την ίνα σαν μια σειρά από μικρούς καθρέφτες) εξέρχεται από την άλλη μεριά. Οι οπτικές ίνες είναι κατάλληλες για μετάδοση ψηφιακών δεδομένων καθώς μπορούμε εύκολα να φτιάξουμε ένα κύκλωμα το οποίο να αναβοσβήνει με ταχύ ρυθμό το φώς στη μια άκρη, συμβολίζοντας έτσι τα δυαδικά 0 και 1.

Οι πολύτροπες οπτικές ίνες είναι γενικά μεγαλύτερης διαμέτρου από τις μονότροπες. Ονομάζονται πολύτροπες επειδή το φως μπορεί να διαδοθεί μέσα σε αυτές με διάφορους τρόπους. Αυτό τις κάνει φτηνότερες στην κατασκευή αλλά περιορίζει το μέγιστο μήκος τους ή την ταχύτητα μετάδοσης που μπορούν να επιτύχουν. Στις πολύτροπες ίνες χρησιμοποιούμε συνήθως φως από LEDs (φωτοεκπέμπουσες διόδους) οι οποίες είναι αρκετά φτηνές.

Οι μονότροπες ίνες είναι αρκετά μικρότερης διαμέτρου (τυπικά κάτω από 10 μικρόμετρα (μm)) και σε αυτές το φως μπορεί να διαδοθεί με ένα και μοναδικό τρόπο. Για το λόγο αυτό δεν μπορεί να χρησιμοποιηθεί κοινό φως από LED αλλά από LASER το οποίο έχει και μεγαλύτερο κόστος. Όμως οι ίνες αυτές προσφέρουν πολύ μεγαλύτερες ταχύτητες και αποστάσεις σε σχέση με τις πολύτροπες.

Η οπτική ίνα χρησιμοποιείται συνήθως για να συνδέσουμε μεταξύ τους σημεία που απέχουν αρκετά (μέχρι 2Km) και όταν υπάρχει αυξημένος ηλεκτρομαγνητικός θόρυβος (π.χ. σε βιομηχανικό περιβάλλον και εγκαταστάσεις όπου υπάρχουν ηλεκτρικοί κινητήρες ή δημιουργούνται σπινθήρες κλπ). Η οπτική ίνα έχει τα μειονεκτήματα του αυξημένου κόστους και της δυσκολίας χειρισμού (δεν μπορούμε να τη λυγίσουμε όπως ένα καλώδιο, είναι αρκετά πιο δύσκολο να την κολλήσουμε όταν κόψει, απαιτεί ειδικά βύσματα κλπ.)

Ethernet Υψηλών Ταχυτήτων

Στα πλαίσια των συνεχών βελτιώσεων και νέων εκδόσεων του Ethernet, δημιουργήθηκαν δύο νέα πρότυπα, το IEEE 802.3u (Fast Ethernet) και το IEEE 802.3z (Gigabit Ethernet). Το Fast Ethernet προσφέρει ταχύτητα 100Mbps ενώ το Gigabit, 1000 Mbps.

Για τη δημιουργία του Fast Ethernet, εκτός από το δεκαπλασιασμό της ταχύτητας

από τα 10 στα 100Mbps, δόθηκε προσοχή ώστε να μη διαταραχθεί κατά το δυνατόν η υπάρχουσα καλωδιακή υποδομή. Καθώς το πιο συνηθισμένο (εμπορικά) μέχρι τότε πρότυπο Ethernet ήταν το 10Base-T, το Fast Ethernet σχεδιάσθηκε να χρησιμοποιεί επίσης τον ίδιο τύπο καλωδίου, δηλ. συνεστραμμένων ζευγών. Το απλό 10Base-T μπορεί να χρησιμοποιήσει καλώδιο κατηγορίας 3 (Cat3) ενώ το Fast Ethernet στην πλέον διαδεδομένη εκδοχή του (100Base-TX) χρειάζεται κατηγορίας 5 (Cat5).

Τα επιμέρους πρότυπα του Fast Ethernet είναι:

- **100Base-TX:** Είναι το πιο διαδεδομένο στις μέρες μας πρότυπο. Χρησιμοποιεί καλώδιο UTP (αθωράκιστο) κατηγορίας 5 ή STP (θωρακισμένο). Η ταχύτητα φτάνει τα 100Mbps και η μετάδοση είναι Full Duplex δηλ. και προς τις δύο κατευθύνσεις (αμφίδρομη). Από τα τέσσερα (4) ζεύγη καλωδίων που διαθέτει το μέσο, χρησιμοποιούνται μόνο τα δύο (2). Το ένα ζεύγος χρησιμοποιείται για την αποστολή δεδομένων και το άλλο για τη λήψη. Για λόγους χρονισμού, στα δύο ζεύγη υπάρχει συνεχή μετάδοση συμβόλων, ακόμα και όταν δεν υπάρχουν δεδομένα προς μετάδοση (μεταδίδονται ειδικά σύμβολα σε αυτή την περίπτωση). Η απόσταση του τμήματος μπορεί να φτάσει τα 100 μέτρα. Τα δύο ζεύγη που δεν χρησιμοποιούνται συνήθως τερματίζονται (ώστε να μη λαμβάνουν θόρυβο από το περιβάλλον).

- **100Base-T4:** Σε αυτή την παραλλαγή του Ethernet, χρησιμοποιούνται και τα τέσσερα (4) ζεύγη καλωδίων. Αυτό αποτελεί μειονέκτημα σε παλιότερες εγκαταστάσεις όπου ενδεχομένως το εγκατεστημένο καλώδιο να μη διαθέτει πάνω από δύο ζεύγη. Το φυσικό μέσο είναι UTP κατηγορίας 3 και άνω. Η μέγιστη απόσταση τμήματος είναι και πάλι τα 100 μέτρα. Στα ζεύγη υπάρχει σήμα μόνο όταν υπάρχουν δεδομένα προς μετάδοση. Τα τρία ζεύγη χρησιμοποιούνται για μετάδοση δεδομένων, ενώ το τέταρτο για αναγνώριση (λήψη) των συγκρούσεων. Το πρότυπο 100Base-T4 δεν χρησιμοποιεί χωριστά κανάλια για την εκπομπή και τη λήψη, έτσι δεν είναι δυνατή η αμφίδρομη μετάδοση δεδομένων.

- **100Base-FX:** Το πρότυπο αυτό χρησιμοποιεί διπλή πολύτροπη (62.5/125μm) ή μονότροπη οπτική ίνα. Το μήκος τμήματος φτάνει τα 412 μέτρα σε περίπτωση πολύτροπης ίνας και μονόδρομης (half duplex) επικοινωνίας και τα δύο (2) χιλιόμετρα σε Full duplex. Με χρήση μονότροπης ίνας, η μέγιστη απόσταση τμήματος μπορεί να φτάσει τα 25 χιλιόμετρα.

Όνομα	Μέσο Μετάδοσης	Μέγιστο Μήκος Τμήματος	Χαρακτηριστικά
1000Base-SX	Οπτική Ίνα	550 m	Πολύτροπη (50μm)
1000Base-LX	Οπτική Ίνα	5000 m	Μονότροπη (9μm)
1000Base-CX	Χάλκινο καλώδιο 2 ζεύγη STP (Θωρακισμένο - συνεστραμμένο)	25 m	STP
1000Base-T	Χάλκινο καλώδιο 4 ζεύγη STP (Αθωράκιστο - συνεστραμμένο)	100 m	Cat5 UTP

Πίνακας 2.2: *Βασικά πρότυπα του IEEE 802.3z και τα χαρακτηριστικά τους*

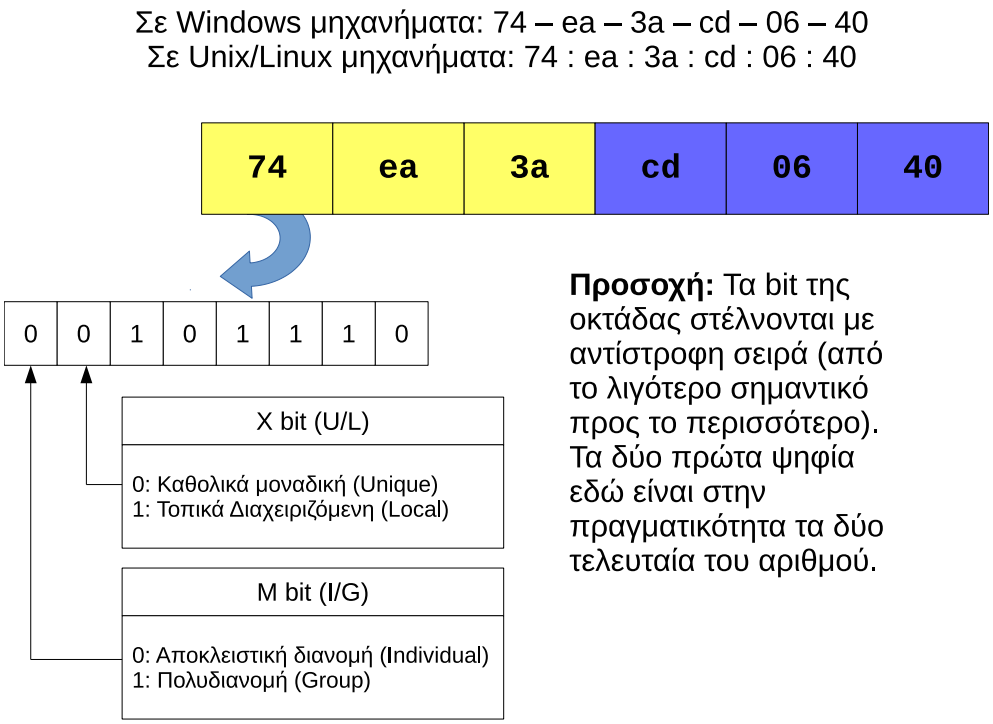
Gigabit Ethernet

Το πρότυπο IEEE 802.3z ή Gigabit Ethernet (πίνακας 2.2), είναι το νεώτερο πρότυπο στην κατηγορία 802.3 και προσφέρει ταχύτητες 1000 Mbps (1 Gigabit). Χρησιμοποιεί καλώδιο τουλάχιστον κατηγορίας 5e (Cat5e από το enhanced, ενισχυμένο). Διαθέτει επίσης πρότυπα για λειτουργία μέσω οπτικής ίνας. Με χρήση πολύτροπης οπτικής ίνας 62.5μm στο πρότυπο 1000Base-SX το μέγιστο μήκος τμήματος φτάνει τα 275 μέτρα ενώ με ίνα 50μm φτάνει τα 550 μέτρα. Με μονότροπη ίνα των 9μm μπορεί να φτάσει τα 5Km.

Από όλες τις παραλλαγές του Gigabit Ethernet, η πιο συχνά χρησιμοποιούμενη είναι η 1000Base-T καθώς χρησιμοποιεί ουσιαστικά το ίδιο καλώδιο (Cat5) με το Fast Ethernet το οποίο υπάρχει ήδη σε πολλά εγκατεστημένα δίκτυα. Εκτός από το Gigabit Ethernet έχουν αναπτυχθεί και εκδόσεις με ταχύτητες 10 Gigabits, 40 Gigabits και 100 Gigabits (αναφέρονται ως 10Gb, 40Gb, 100Gb) ενώ βρίσκονται υπό ανάπτυξη δίκτυα ταχύτητας 400Gb.

2.4.2 Διευθύνσεις Ελέγχου Πρόσβασης στο Μέσο (MAC) – Δομή Πλαισίου Ethernet

Όπως ξέρουμε ήδη, σε ένα δίκτυο Ethernet κάθε κόμβος έχει μια *φυσική διεύθυνση* (MAC address) ή *διεύθυνση υλικού* (Hardware Address) με την οποία αναγνωρίζεται με μοναδικό τρόπο σε όλο το δίκτυο. Η διεύθυνση αυτή αναφέρεται και ως διεύθυνσης προσπέλασης στο μέσο (Media Access Control, MAC) και είναι ένας δυαδικός αριθμός μεγέθους 48 bit ή έξι οκτάδων (bytes). Γράφεται ως δεκαεξαδικός αριθμός



Σχήμα 2.3: *Δομή Διεύθυνσης MAC στο Ethernet*

χωρισμένος ανά οκτάδα με παύλες (όταν τον βλέπουμε στα Windows) ή με άνω-κάτω τελείες σε συστήματα Unix/Linux. Ένα παράδειγμα είναι η διεύθυνση:

74:ea:3a:cd:06:40

(Σημείωση: τα γράμματα μπορεί να είναι μικρά ή κεφαλαία – δεν υπάρχει διαφορά)

Γιατί τόσο πολύ δεκαεξαδικό στους υπολογιστές;

Η επιλογή του δεκαεξαδικού συστήματος για τις φυσικές διευθύνσεις (και όχι μόνο) στην αρχή φαίνεται κάπως παράξενη. Εξάλλου οι άνθρωποι έχουμε συνηθίσει στο δεκαδικό και οι υπολογιστές λειτουργούν εσωτερικά στο δυαδικό. Για ποιο λόγο να εισάγουμε ακόμα ένα αριθμητικό σύστημα στην πληροφορική; Ο λόγος είναι πολύ απλός: πολλές φορές θέλουμε να δούμε γρήγορα τα επιμέρους bits ενός αριθμού. Αν τον έχουμε στο δυαδικό, είναι εύκολο. Αν όμως είναι στο δεκαδικό θα πρέπει να τον μετατρέψουμε πρώτα στο δυαδικό. Η διαδικασία δεν είναι δύσκολη αλλά δεν είναι και στιγμιαία. Το δεκαεξαδικό όμως έχει μια άμεση σύνδεση με το δυαδικό: αν έχουμε τον αριθμό στο δεκαεξαδικό μπορούμε με τη βοήθεια ενός πίνακα να δούμε αμέσως το δυαδικό του αντίστοιχο. Η μετατροπή από δυαδικό σε δεκαεξαδικό και

αντίστροφα δεν απαιτεί καμιά πράξη!

Παρακάτω μπορείτε να δείτε πως αντιστοιχίζονται τα δεκαεξαδικά ψηφία στο δυαδικό. Ουσιαστικά πρόκειται για μια αρίθμηση με τέσσερα bit στο δυαδικό (και υπάρχει εύκολος τρόπος να θυμάστε τον πίνακα, ψάξτε το!)

Δεκαεξαδικό	**Δυαδικό**	**Δεκαεξαδικό**	**Δυαδικό**
0	0000	8	1000
1	0001	9	1001
2	0010	A	1010
3	0011	B	1011
4	0100	C	1100
5	0101	D	1101
6	0110	E	1110
7	0111	F	1111

Για να το χρησιμοποιήσουμε, έχοντας ένα δεκαεξαδικό αριθμό, απλά κοιτάμε ένα – ένα τα ψηφία του και γράφουμε την αντίστοιχη δυαδική απεικόνιση. Π.χ. για τον αριθμό 74 του παραδείγματος που ακολουθεί, σύμφωνα με τον πίνακα:

7 = 0111
4 = 0100

Για να ξεχωρίζουμε τους δεκαεξαδικούς από αριθμούς άλλων συστημάτων, γράφουμε συχνά πριν τα ψηφία τους το πρόθεμα “0x”. Αντίστοιχα, στους δυαδικούς γράφουμε το “0b”. Έτσι:

0x74 = 0b01110100

Και αντίστροφα βέβαια, αν μας δώσουν ένα αριθμό στο δυαδικό:

0b11101010

Απλά τον χωρίζουμε σε δύο τμήματα των 4 bit και γράφουμε τα αντίστοιχα δεκαεξαδικά σύμφωνα με τον πίνακα:

0b1110 = 0xE
0b1010 = 0xA

Άρα 0b11101010 = 0xEA.

Η φυσική διεύθυνση (MAC address) είναι χαρακτηριστικό κάθε κάρτας δικτύου. Σε πολλές περιπτώσεις ο κατασκευαστής αναγράφει τη φυσική διεύθυνση πάνω στη κάρτα (συνήθως αυτοκόλλητο, δείτε τη φώτο 2.7). Αν η κάρτα είναι εγκατεστημένη

σε ένα υπολογιστή, μπορούμε συνήθως να διαβάσουμε τη φυσική διεύθυνση από το λειτουργικό.

Διαβάζοντας μια MAC διεύθυνση

Στα Windows ανοίγουμε τη γραμμή εντολών (command prompt) και πληκτρολογούμε:

```
ipconfig /all
```

Η φυσική διεύθυνση αναφέρεται ως ‘’Physical Address”:

```
Physical Address. . . . . . . . .: F8-CA-B8-1C-24-96
```

Σε μηχανήματα Unix/Linux χρησιμοποιούμε από το τερματικό την εντολή ifconfig (χωρίς άλλες παραμέτρους). Στις πιο καινούριες διανομές προτιμάμε την εντολή ip:

```
ip addr show
```

Η γραμμή που μας ενδιαφέρει μοιάζει με την παρακάτω:

```
link/ether F8:CA:BB:1C:24:96
```

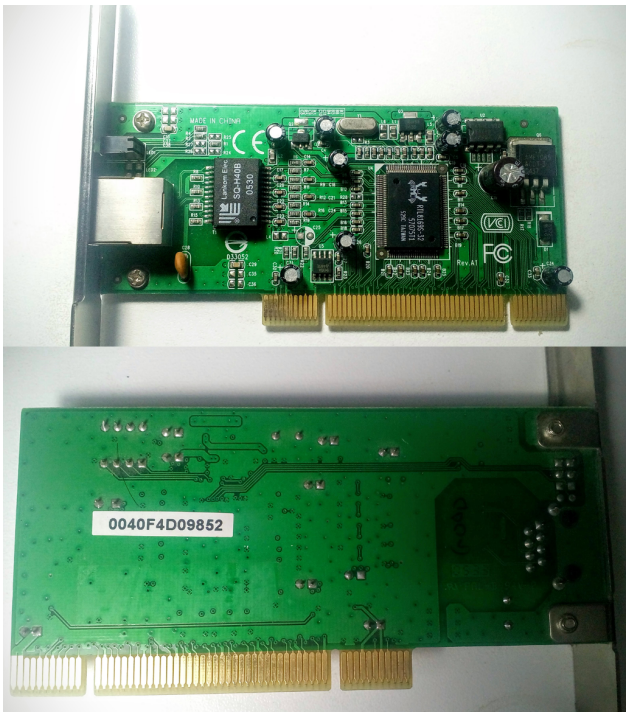
Οι φυσικές διευθύνσεις είναι συνολικού μεγέθους 48bit (6 bytes) και αποτελούνται από δύο μέρη των 24 bit. Το πρώτο μέρος, η *Μοναδική Ταυτότητα του Οργανισμού, (OUI - Organizational Unique Identifier) χορηγείται από το IEEE (το Ινστιτούτο Ηλεκτρολόγων - Ηλεκτρονικών Μηχανικών* και διατίθεται αποκλειστικά στον κατασκευαστή του υλικού. Το δεύτερο μέρος το προσδιορίζει με δική του ευθύνη ο κατασκευαστής του υλικού. Δείτε και το σχήμα 2.3.

Στο Ethernet αποστέλλεται πρώτα το πιο *σημαντικό byte (MSB, Most Significant Byte)* δηλ. το πρώτο από τα έξι που αποτελούν την φυσική διεύθυνση. Ωστόσο από το κάθε byte αποστέλλεται πρώτο το *λιγότερο σημαντικό ψηφίο, LSB Least significant bit*. Σε επίπεδο bit, η αποστολή χαρακτηρίζεται ως *Little Endian*.

Τι είναι το Endianness;

Όπως είναι γνωστό, η οργάνωση της μνήμης σε ένα υπολογιστή είναι σε bytes. Ωστόσο ένα byte μπορεί να έχει τιμές από 0 ως 255 και έτσι από μόνο του μπορεί να αντιπροσωπεύσει μόνο αυτές τις μικρές ακέραιες τιμές.

Ωστόσο, οι υπολογιστές συνήθως ασχολούνται και με αρκετά μεγαλύτερους αριθμούς καθώς και με αριθμούς που περιέχουν ψηφία μετά την υποδιαστολή (αποκα-



Σχήμα 2.4: *Κάρτα Δικτύου Ethernet με αυτοκόλλητο που δείχνει MAC address*

λούνται αριθμοί κινητής υποδιαστολής). Είναι προφανές ότι για μεγαλύτερους αριθμούς η αναπαράσταση θα γίνεται με περισσότερα από ένα bytes.

Όταν για παράδειγμα ένας αριθμός χρειάζεται δύο συνεχόμενα bytes στη μνήμη για να αναπαρασταθεί, ποιο από τα δύο θα είναι το πιο σημαντικό; Αν το σύστημα μας τοποθετεί το πιο σημαντικό byte πρώτα και μετά το λιγότερο σημαντικό, τότε χαρακτηρίζεται ως *Big Endian*. Διαφορετικά χαρακτηρίζεται ως *Little Endian*. Όταν ρωτάμε το endianness ενός συστήματος περιμένουμε μια απάντηση όπως Big Endian ή Little Endian.

Κατά αντιστοιχία με την αποθήκευση δεδομένων, endianness υπάρχει και στις μεταδόσεις δεδομένων. Όταν έχουμε να στείλουμε πολλά bytes σειριακά, ποιο στέλνουμε πρώτο και ποιο τελευταίο; Το Ethernet στέλνει πρώτα το περισσότερο σημαντικό byte. Αναλύοντας όμως το byte στα δυαδικά ψηφία που το αποτελούν (bits), το Ethernet στέλνει το λιγότερο σημαντικό ψηφίο του byte πρώτο. **Σε επίπεδο bit, το Ethernet είναι Little Endian.**

Το έντυπο σχολικό βιβλίο εδώ γράφει σε *επίπεδο byte* **που είναι λάθος**. Έχει ωστόσο διορθωθεί στα παροράματα που κυκλοφόρησε επίσημα το Υπουργείο Παιδείας.

Τα δύο πρώτα bit που μεταδίδονται (προσοχή: που αντιστοιχούν στην πραγματικότητα στα δύο λιγότερο σημαντικά ψηφία του πλέον σημαντικού byte της διεύθυνσης) έχουν ειδική σημασία:

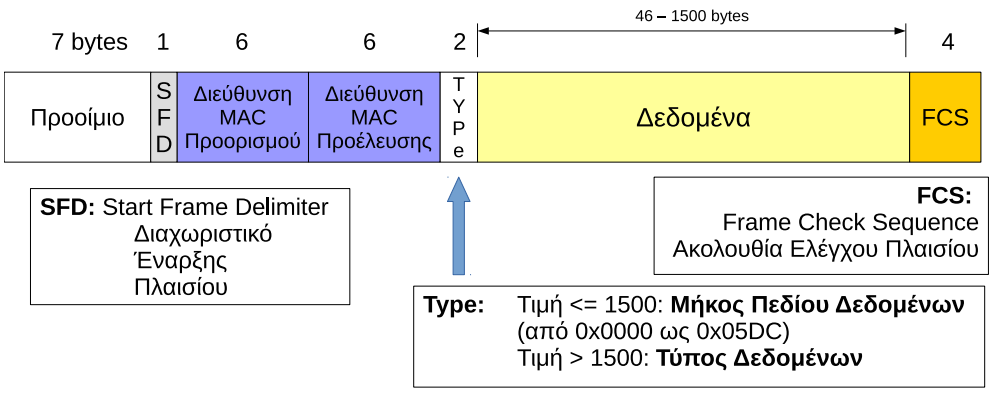
- Το πρώτο (b0) είναι το **M bit ή I/G (Individual Group**. Αν έχει τιμή 1 σημαίνει ότι η διεύθυνση αφορά πολλούς αποδέκτες, πρόκειται δηλ. για διεύθυνση *πολυδιανομής (multicasting)*. Άν έχει τιμή 0, αφορά ένα μοναδικό αποδέκτη
- Το δεύτερο (b1) είναι το **X bit ή U/L (Universal - Local)**. Όταν είναι 1 σημαίνει ότι η διεύθυνση είναι τοπικά διαχειριζόμενη (είναι εγγυημένα μοναδική μόνο στο συγκεκριμένο δίκτυο που βρίσκεται το υλικό) ενώ αν είναι 0 η διεύθυνση είναι καθολικά μοναδική (δεν υπάρχει σε κανένα άλλο υλικό πουθενά στο κόσμο)

Ειδική περίπτωση είναι η διεύθυνση όπου όλα τα ψηφία έχουν την τιμή 1, δηλ. φυσική διεύθυνση FF:FF:FF:FF:FF:FF. Πρόκειται για *διεύθυνση εκπομπής*. Ένα πλαίσιο με αυτή τη διεύθυνση προορισμού λαμβάνεται από όλα τα μηχανήματα που βρίσκονται στο ίδιο τοπικό δίκτυο. Αν στο δίκτυο υπάρχει μεταγωγέας (switch), το πλαίσιο αυτό εκπέμπεται σε όλες τις θύρες του.

Ποια είναι μια βασική διαφορά του Switch από το Hub;

Το hub πάντοτε αναπαράγει όλα τα πλαίσια που λαμβάνει σε όλες τις θύρες του. Το switch γνωρίζει ποια κάρτα δικτύου είναι συνδεδεμένη σε ποια θύρα (από τη φυσική της διεύθυνση) και έτσι μεταδίδει τα αντίστοιχα πλαίσια μόνο στη συγκεκριμένη πόρτα. Έτσι το hub ουσιαστικά λειτουργεί αποκλειστικά στο φυσικό επίπεδο, ενώ το switch στο ζεύξης δικτύου.

Θα εξετάσουμε τώρα τη δομή του πλαισίου Ethernet (δείτε το σχήμα 2.5).



Σχήμα 2.5: *Δομή Πλαισίου Ethernet*

Μπορούμε να διακρίνουμε τα παρακάτω:

- Το **Προοίμιο** (Preamble). Για να συγχρονιστεί ο δέκτης με τον πομπό στέλνεται μια εναλλαγή ψηφίων 0 και 1 (αντιστοιχεί στον δεκαεξαδικό αριθμό 0x55, δείτε και τον πίνακα του δεκαεξαδικού παραπάνω). Στέλνονται επτά (7) τέτοιες οκτάδες. Στο τέλος στέλνεται μια οκτάδα 0xD5 που αποτέλει το σήμα για την έναρξη του πλαισίου και ονομάζεται **SFD** (Start Frame Delimiter).

- Ακολουθούν οι **Διευθύνσεις MAC Προορισμού και Προέλευσης** με κάθε μια να καταλαμβάνει χώρο 6 bytes. Πρώτα μεταδίδεται η διεύθυνση προορισμού ώστε να ειδοποιηθεί έγκαιρα ο παραλήπτης και έπειτα μεταδίδεται η διεύθυνση του αποστολέα.

- Το πεδίο **Τύπος/Μήκος Δεδομένων** προσδιορίζει το είδος των δεδομένων που μεταφέρει το πλαίσιο ή πιο πρωτόκολλο ανώτερου επιπέδου τα έχει δημιουργήσει, αν η τιμή του είναι μεγαλύτερη από 1500. Αν η τιμή του είναι μικρότερη ή ίση με 1500 (0x5DC) τότε δηλώνει το μήκος των δεδομένων που μεταφέρει. Το πεδίο έχει μήκος 2 bytes.

- Ακολουθούν τα **Δεδομένα (Data)** τα οποία μπορεί να είναι από 46 ως 1500 οκτάδες.

- Το πλαίσιο τελειώνει με το πεδίο **Ακολουθίας Ελέγχου Πλαισίου** ή FCS (Frame Check Sequence). Το πεδίο αυτό έχει μέγεθος 4 bytes και περιέχει πληροφορίες σύμφωνα με τις οποίες ο παραλήπτης μπορεί να ελέγξει αν το πλαίσιο έχει μεταδοθεί σωστά ή περιέχει σφάλματα. Για το σκοπό αυτό χρησιμοποιείται ο αλγόριθμος CRC32.

Με το τέλος του πλαισίου ακολουθεί μια παύση μεγέθους 96 bit που ονομάζεται *IPG ή InterPacket Gap* και είναι απαραίτητη προκειμένου τα κυκλώματα του δέκτη να επεξεργαστούν το προηγούμενο πλαίσιο και να ετοιμαστούν για τη λήψη του επόμενου.

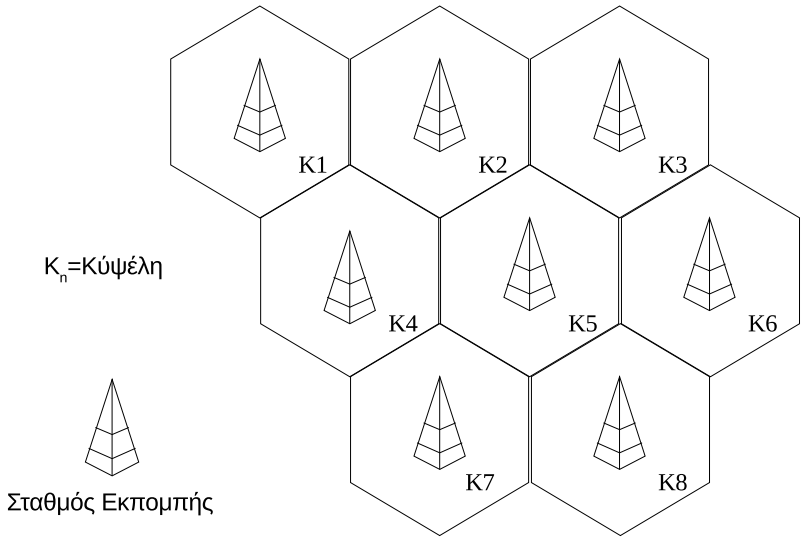
Το μέγιστο μήκος ωφέλιμων δεδομένων ορίζεται από το πρότυπο ως 1500 bytes και ονομάζεται *Μέγιστη Μονάδα Εκπομπής ή MTU (Maximum Transfer Unit)*. Η ελάχιστη ποσότητα δεδομένων που μπορεί να μεταφερθεί είναι 46 bytes. Μαζί με την επικεφαλίδα, το ελάχιστο επιτρεπτό μέγεθος πλαισίου είναι 64 οκτάδες (46 bytes δεδομένα και 18 επικεφαλίδα. Η επικεφαλίδα περιέχει τις δύο φυσικές διευθύνσεις (12 bytes), το πεδίο τύπος / μήκος δεδομένων (2 bytes) και το FCS (4 bytes)). Αν θέλουμε να στείλουμε μικρότερο πλαίσιο, τότε συμπληρώνουμε με μηδενικά (zero padding) ώστε να φτάσουμε το ελάχιστο μήκος.

2.5 Ασύρματα Δίκτυα

Σε ένα ασύρματο δίκτυο, αντί για καλώδιο το μέσο διάδοσης είναι ο αέρας (ή και το κενό). Για τη μετάδοση χρησιμοποιούνται οπτικά σήματα, υπέρυθρες, ή (συνηθέστερα) ραδιοκύματα.

Τα ασύρματα δίκτυα με τη μεγαλύτερη εξάπλωση σήμερα είναι τα κυψελοειδή: πολλά από τα ασύρματα συστήματα αποτελούν εξειδίκευση ή γενίκευση των κυψελοειδών δικτύων. Κάθε δίκτυο καλύπτει μια περιοχή που ονομάζεται *κυψέλη* χρησιμοποιώντας ένα *σταθμό βάσης* και πολλούς ασύρματους *χρήστες – δέκτες*.

Κάθε κυψέλη καλύπτει με σήμα μια περίπου εξαγωνική ή κυκλική περιοχή. Πολλές κυψέλες μαζί καλύπτουν ασύρματα μεγάλες εκτάσεις, όπως φαίνεται στο σχήμα 2.6.



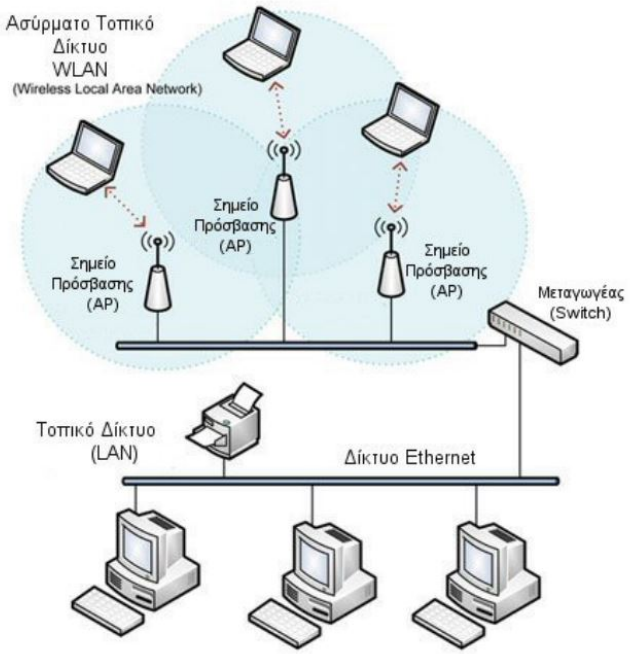
Σχήμα 2.6: *Δίκτυο με Κυψέλες*

Προϋπόθεση για τη σύνδεση των συσκευών μεταξύ τους είναι να έχουν εξοπλιστεί με κατάλληλο υλικό διεπαφής (π.χ. ασύρματες κάρτες δικτύου) που να επιτρέπει τη σύνδεση τους μέσω ασύρματης τεχνολογίας.

Ένα καθημερινό παράδειγμα δικτύου με κυψέλες

Ένα είδος ασύρματου δικτύου που χρησιμοποιεί κυψέλες είναι και το σύστημα κινητής τηλεφωνίας (GSM). Κάθε φορητή συσκευή (κινητό τηλέφωνο) είναι εφοδιασμένη με τον κατάλληλο πομποδέκτη και κυκλώματα που αφορούν τη ψηφιοποίηση των δεδομένων φωνής. Ο πάροχος της υπηρεσίας διαθέτει κυψέλες που γεωγραφικά καλύπτουν ολόκληρη τη χώρα. Καθώς το κινητό τηλέφωνο μετακινείται, συνδέεται κάθε φορά στην πιο κοντινή/ισχυρή κυψέλη χωρίς ο χρήστης να αντιλαμβάνεται τη μετάβαση από τη μια κυψέλη στην άλλη.

Τα **ασύρματα τοπικά δίκτυα** ή WLAN (Wireless Local Area Network) επιτρέπουν σε ένα χρήστη κινητής συσκευής όπως ένας φορητός υπολογιστής, tablet ή smartphone να συνδέονται σε ένα τοπικό δίκτυο μέσω ασύρματης σύνδεσης ραδιοκυμάτων υψηλής συχνότητας.



Σχήμα 2.7: *Ασύρματο τοπικό δίκτυο συνδεόμενο με ενσύρματο δίκτυο*

Στο σχήμα 2.7 φαίνεται ένα τέτοιο δίκτυο που αποτελείται από τρία σημεία πρόσβασης (APs, Access Points) τα οποία σχηματίζουν ένα τοπικό ασύρματο δίκτυο και επιτρέπουν σε φορητές συσκευές που βρίσκονται στην εμβέλεια τους να συνδεθούν σε αυτά. Τα σημεία πρόσβασης συνδέονται μεταξύ τους και με το υπόλοιπο

δίκτυο μέσω ενός μεταγωγέα (switch). Με αυτό το τρόπο δίνεται η δυνατότητα επέκτασης του τοπικού δικτύου και παροχής υπηρεσιών σε μεγαλύτερο αριθμό συσκευών.

Κεφάλαιο 3

Επίπεδο Δικτύου – Δικτύωση

3.1 Διευθυνσιοδότηση Internet Protocol Έκδοση 4 (IPv4)

Το επίπεδο Δικτύου (Network) στο OSI ή το επίπεδο Διαδικτύου (Internet) στο TCP/IP:

- Παρέχει τη *λογική διευθυνσιοδότηση* για όλα τα διασυνδεδεμένα μεταξύ τους δίκτυα.
- Φροντίζει για την εύρεση της κατάλληλης *διαδρομής* και παράδοσης του πακέτου στον τελικό κόμβο σε μια διαδικασία που ονομάζεται *δρομολόγηση* (routing).

Στη διαδικασία της δρομολόγησης, το πακέτο μπορεί να διασπαστεί σε πολλά μικρότερα κομμάτια (fragments). Το βασικό πρωτόκολλο σε αυτό το επίπεδο είναι το *Πρωτόκολλο Διαδικτύου ή IP (Internet Protocol)* το οποίο δημιουργεί *αυτοδύναμα πακέτα* γνωστά ως *datagrams (data+telegram)*. Καθώς είναι αυτοδύναμα, κάθε πακέτο μιας επικοινωνίας μπορεί να ακολουθήσει διαφορετική διαδρομή μέχρι τον παραλήπτη, με αποτέλεσμα να φτάσουν με διαφορετική σειρά. Κάποια επίσης μπορεί να μη παραδοθούν. Ωστόσο το επίπεδο Διαδικτύου είναι υπεύθυνο να τα ξαναβάλει στη σωστή σειρά και να ενημερώσει για πακέτα που δεν έφτασαν στον προορισμό τους ή αλλοιώθηκαν.

Στο επίπεδο Διαδικτύου λειτουργεί επίσης το *Πρωτόκολλο Μηνυμάτων Ελέγχου Διαδικτύου ή ICMP (Internet Control Message Protocol)* και το *Πρωτόκολλο Διαχείρισης Ομάδων Διαδικτύου ή IGMP (Internet Group Management Protocol* τα οποία χρησιμοποιούνται κυρίως από δικτυακές συσκευές και λογισμικό συστημάτων και

όχι τόσο από τελικούς χρήστες. Το ICMP χρησιμοποιείται για την αναφορά σφαλμάτων, μετάδοση ερωτημάτων και αναμετάδοση (relaying) διαγνωστικών μηνυμάτων. Εξαίρεση αποτελούν οι εντολές ping και traceroute.

Τι είναι οι εντολές ping και traceroute;

Οι δύο αυτές εντολές χρησιμοποιούν το πρωτόκολλο ICMP και μπορούν να χρησιμοποιηθούν σαν εργαλεία χρήστη (υπάρχουν εγκατεστημένες στα περισσότερα λειτουργικά συστήματα, μεταξύ άλλων στο Linux/UNIX και στα Windows). Η εντολή ping στέλνει πακέτα ICMP (για την ακρίβεια τύπου Echo Request) σε ένα παραλήπτη της επιλογής μας με σκοπό να δούμε αν υπάρχει δυνατότητα επικοινωνίας αποστολέα – παραλήπτη. Ο παραλήπτης παραλαμβάνει το πακέτο και το επιστρέφει σε μας. Με την εκτέλεση της εντολής θα δούμε επίσης πόσα πακέτα στάλθηκαν, πόσα παραλήφθηκαν καθώς και το χρόνο που χρειάζεται για την απάντηση.

Για παράδειγμα, μπορούμε να ελέγξουμε αν ο υπολογιστής με διεύθυνση 192.168.0.42 είναι διαθέσιμος στο τοπικό μας δίκτυο:

```
[16:26:28][sonic@pegasus:~]$ ping 192.168.0.42
PING 192.168.0.42 (192.168.0.42): 56 data bytes
64 bytes from 192.168.0.42: icmp_seq=0 ttl=64 time=0.447 ms
64 bytes from 192.168.0.42: icmp_seq=1 ttl=64 time=0.461 ms
64 bytes from 192.168.0.42: icmp_seq=2 ttl=64 time=0.284 ms
^C
--- 192.168.0.42 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.284/0.397/0.461/0.080 ms
```

Η εντολή *traceroute* (σε κάποια λειτουργικά *tracert*) χρησιμοποιείται για να μας δείξει από πόσους ενδιάμεσους κόμβους (hops) θα περάσουν τα πακέτα μας μέχρι να φτάσουν στον κόμβο προορισμού. Περισσότερες λεπτομέρειες θα δούμε σε επόμενη ενότητα. Για παράδειγμα, μπορούμε να δούμε πόσα hops χρειαζόμαστε από το τοπικό δίκτυο μέχρι τον υπολογιστή που παρέχει την δικτυακή τοποθεσία www.freebsdworld.gr μπορούμε να γράψουμε:

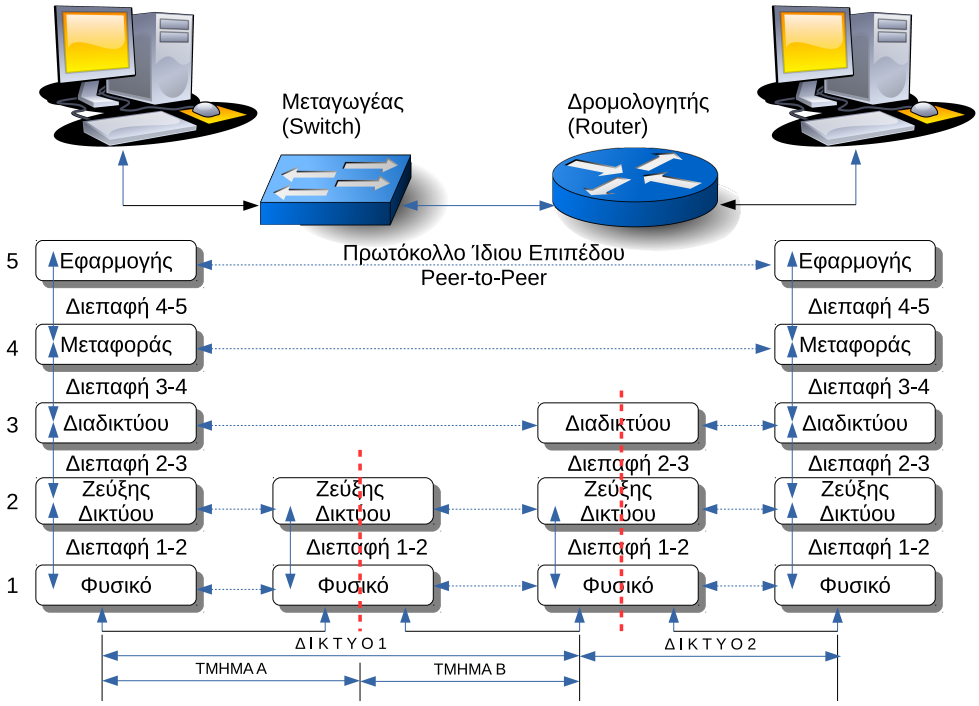
```
[16:43:33][sonic@pegasus:~]$ traceroute www.freebsdworld.gr
traceroute to freebsdworld.gr (193.183.99.68), 64 hops max,
40 byte packets

 1  router (192.168.0.250)  0.983 ms  0.614 ms  0.893 ms
 2  80.107.108.106 (80.107.108.106)  7.632 ms  7.701 ms  7.665 ms
 3  79.128.227.213 (79.128.227.213)  11.944 ms  11.210 ms
    79.128.226.245 (79.128.226.245)  11.790 ms
 4  gig5-0-5-gsr03.ath.OTEGlobe.gr (62.75.3.17)  11.356 ms
    62.75.3.157 (62.75.3.157)  11.321 ms  11.767 ms
```

```
 5  * * *
 6  212.162.19.109.ear2.Frankfurt1.Level3.net (212.162.19.109)
    48.464 ms  48.998 ms  49.037 ms
 7  ae-122-3508.bar2.Milan1.Level3.net (4.69.159.126)  57.132 ms
    ae-121-3507.bar2.Milan1.Level3.net (4.69.159.122)  56.833 ms
    57.746 ms
 8  212.73.241.130 (212.73.241.130)  57.867 ms  57.592 ms  64.055 ms
 9  217.171.38.134 (217.171.38.134)  57.439 ms  58.278 ms  58.169 ms
10  zms.gudgenet.com (193.183.99.68)  57.137 ms  57.998 ms  57.391 ms
```

Μέχρι τον προορισμό περνάμε από 9 ενδιάμεσους κόμβους, ενώ βλέπουμε ότι πηγαίνουμε σε ένα προορισμό στο Μιλάνο μέσω…Φρανκφούρτης!

Το IGMP χρησιμοποιείται για την ομαδοποίηση υπολογιστών και αποστολή ταυτόχρονα μηνυμάτων σε όλους τους υπολογιστές της ομάδας (streaming). Σε ένα υπολογιστή με TCP/IP, η υλοποίηση του ICMP είναι υποχρεωτική ενώ του IGMP προαιρετική.



Σχήμα 3.1: *Δίκτυο και Διαδίκτυο*

Το πακέτο IP φτάνει ουσιαστικά χωρίς αλλαγές (αυτούσιο) από τον υπολογιστή του αποστολέα στον υπολογιστή προορισμού. Οι ενδιάμεσοι κόμβοι κάνουν μόνο μικρές αλλαγές στην επικεφαλίδα του πακέτου για διαχειριστικούς λόγους. Σε όλα τα

ενδιάμεσα δίκτυα το πακέτο μπορεί να ενθυλακώνεται και να αποθυλακώνεται σε πλαίσια του 2ου επιπέδου, αλλά τα πλαίσια αυτά ισχύουν κάθε φορά μόνο για το συγκεκριμένο κομμάτι του δικτύου.

Για να το καταλάβουμε καλύτερα, ας δούμε το σχήμα 3.1. Ας θεωρήσουμε ότι το ΔΙΚΤΥΟ 1 και ΔΙΚΤΥΟ 2 είναι δύο δίκτυα Ethernet τα οποία ειναι συνδεδεμένα μεταξύ τους με το δρομολογητή που φαίνεται. Στο ΔΙΚΤΥΟ 1, ο υπολογιστής συνδέεται μέσω ενός μεταγωγέα (Switch). Ο μεταγωγέας όπως ξέρουμε δουλεύει στο επίπεδο ζεύξης δεδομένων (μπορεί δηλ. να δει τις φυσικές διευθύνσεις για να αποφασίσει σε ποια θύρα θα στείλει ένα πλαίσιο) αλλά δεν γνωρίζει τις λογικές διευθύνσεις (διευθύνσεις IP). Ο υπολογιστής παράγει κάποια πακέτα IP τα οποία ενθυλακώνονται σε πλαίσια Ethernet και μεταδίδονται μέσω του μεταγωγέα στο δρομολογητή.

Στο δρομολογητή, τα πλαίσια αποθυλακώνονται και ενθυλακώνονται ξανά σε νέα πλαίσια αυτή τη φορά για το ΔΙΚΤΥΟ 2. Το πακέτο IP σε όλη τη διαδρομή παρέμεινε ουσιαστικά το ίδιο, όμως αποθυλακώθηκε και ενθυλακώθηκε σε διαφορετικά πλαίσια.

Οι γραμμές μετάδοσης (γνωστές και ως ζεύξεις, κυκλώματα ή κανάλια) και οι συσκευές μεταγωγής – δρομολογητές που επιτρέπουν σε δύο ακραίους υπολογιστές να επικοινωνήσουν μεταξύ τους ονομάζονται *επικοινωνιακό υποδίκτυο*. Στα δίκτυα τεχνολογίας TCP/IP το επικοινωνιακό υποδίκτυο χρειάζεται να παρέχει λειτουργικότητα μέχρι το επίπεδο Διαδικτύου (ή το 3ο επίπεδο του OSI).

Γιατί;

Γιατί οι δρομολογητές που χρησιμοποιούνται κατά κύριο λόγο ως ενδιάμεσοι κόμβοι πρέπει να μπορούν να δουν τη λογική διεύθυνση προορισμού (διεύθυνση IP) προκειμένου να εκτελέσουν τη δρομολόγηση (να επιλέξουν δηλ. τη διαδρομή που θα στείλουν τα πακέτα). Η πληροφορία αυτή είναι διαθέσιμη μόνο στο επίπεδο Διαδικτύου, έτσι το επικοινωνιακό υποδίκτυο στο TCP/IP πρέπει να παρέχει λειτουργικότητα μέχρι τουλάχιστον αυτό το επίπεδο.

Δύο ή περισσότερα ανεξάρτητα δίκτυα διασυνδεδεμένα μεταξύ τους ώστε να λειτουργούν ως ένα μεγάλο δίκτυο συνθέτουν ένα *διαδίκτυο* (ή *internet* με μικρό i).

Σε ένα δίκτυο υπολογιστών, για να μπορέσει η πληροφορία να φτάσει στον υπολογιστή προορισμού με τη μορφή πακέτου δεδομένων, θα πρέπει οι υπολογιστές να *προσδιορίζονται με μοναδικό τρόπο* με κάποιο σχήμα διευθυνσιοδότησης, όπως οι κατοικίες σε μια πόλη προσδιορίζονται από τον αριθμό, την οδό και το ταχυδρομικό κώδικα. Αυτή η διευθυνσιοδότηση γίνεται μέσω των λογικών διευθύνσεων IP που

θα εξετάσουμε παρακάτω.

3.1.1 Διευθύνσεις IPv4

Οι υπολογιστές που συμμετέχουν σε ένα δίκτυο τεχνολογίας TCP/IP αναγνωρίζονται με ένα μοναδικό τρόπο, από ένα 32μπιτο (στην έκδοση 4 του πρωτοκόλλου IP, IPv4) δυαδικό αριθμό, την *διεύθυνση IP*.

Για παράδειγμα, ένας τέτοιος αριθμός είναι ο:

11000000 10101000 00000001 00010010

Τον παραπάνω αριθμό τον έχουμε ομαδοποιήσει σε 4 ομάδες των 8 bit τις οποίες αν μετατρέψουμε στους αντίστοιχους δεκαδικούς αριθμούς θα πάρουμε τους:

192 168 1 18

Ένας υπολογιστής στην πραγματικότητα μπορεί να έχει *περισσότερες από μία διευθύνσεις*. Για παράδειγμα:

- Μπορεί να διαθέτει περισσότερες από μία κάρτες δικτύου. Σε κάθε κάρτα δικτύου αντιστοιχίζεται τουλάχιστον μια διεύθυνση IP. Επίσης μπορούμε να αντιστοιχίσουμε πολλαπλές διευθύνσεις IP σε μια κάρτα.
- Μπορεί να είναι συνδεδεμένος ταυτόχρονα σε περισσότερα από ένα δίκτυα. Η σύνδεση μπορεί να γίνεται μέσω μιας κάρτας ή πολλών. Διαφορετικά δίκτυα χρησιμοποιούν διαφορετικές περιοχές/κλάσεις διευθύνσεων (θα δούμε παρακάτω) άρα ο υπολογιστής πρέπει να έχει μια διεύθυνση κατάλληλη για κάθε δίκτυο. Ένας υπολογιστής που έχει το ρόλο δρομολογητή έχει μια κάρτα δικτύου για κάθε διαφορετικό δίκτυο στο οποίο είναι συνδεδεμένος και προωθεί πακέτα από το ένα δίκτυο στο άλλο με βάση συγκεκριμένους κανόνες.

Μια διεύθυνση IP που προσδιορίζει μια συγκεκριμένη δικτυακή διασύνδεση (ένα υπολογιστή, μια συγκεκριμένη κάρτα δικτύου) χαρακτηρίζεται ως *αποκλειστικής διανομής (unicast)*. Όπως θα δούμε, υπάρχουν διευθύνσεις *multicast* που προορίζονται για πολυδιανομή (αποστολή των ίδιων πακέτων σε πολλούς παραλήπτες).

Τρόπος Γραφής μιας Διεύθυνσης IPv4

Επειδή είναι δύσκολο για τον άνθρωπο να απομνημονεύει δυαδικούς αριθμούς μεγέθους 32 bit, συνηθίζεται να αναγράφουμε τις διευθύνσεις IP στη δεκαδική τους

μορφή. Για το σκοπό αυτό:

- Χωρίζουμε τα δυαδικά ψηφία σε οκτάδες. Δημιουργούνται έτσι τέσσερα τμήματα του ενός byte το καθένα
- Μετατρέπουμε τους αριθμούς στους δεκαδικούς αντίστοιχους
- Γράφουμε τους αριθμούς χωρισμένους μεταξύ τους με τελείες

Ο αριθμός του προηγούμενου παραδείγματος:

$11000000_2 = 192_{10}$
$10101000_2 = 168_{10}$
$00000001_2 = 1_{10}$
$00010010_2 = 18_{10}$

γράφεται τελικά ως 192.168.1.18

Σύμφωνα με τον παραπάνω τρόπο γραφής, για να είναι έγκυρη μια διεύθυνση IP, θα πρέπει:

- Να αποτελείται από *τέσσερις δεκαδικούς αριθμούς* που να χωρίζονται μεταξύ τους με τελείες
- Κάθε αριθμός να είναι *μεταξύ του μηδενός (0) και του 255*. Με 8 bit (1 byte) ο ελάχιστος αριθμός που μπορούμε να γράψουμε είναι το 0 και ο μέγιστος το 2^8-1=255

Παραδείγματα διευθύνσεων IP:

Α/Α	Διεύθυνση	Σωστή/Λάθος	Αιτιολογία
1	192.168.1.12	Σωστή	
2	10.0.0.12.3	Λάθος	Περισσότερα από 4 τμήματα
3	172.16.257.3	Λάθος	Ένα τμήμα είναι μεγαλύτερο από 255
4	10.146.0.1	Σωστή	
5	194.219.227.3		
6	127.270.0.1		

Για να μάθετε να μετατρέπετε αριθμούς από το ένα σύστημα στο άλλο, δείτε τα παρακάτω παραδείγματα.

Μετατροπή Δυαδικού σε Δεκαδικό

Σε όλα τα συστήματα αρίθμησης, η θέση ενός ψηφίου δίνει το βάρος του. Για παράδειγμα, στο δεκαδικό σύστημα, το δεξιότερο ψηφίο ενός αριθμού αντιπροσωπεύει

τις μονάδες, το επόμενο τις δεκάδες, μετά τις εκατοντάδες κ.ο.κ. Γενικά θεωρώντας ότι το δεξιότερο ψηφίο αντιστοιχεί στη θέση μηδέν, η αξία του είναι:

ψηφίο X $10^{\text{θέση}}$

Όλα τα υπόλοιπα αριθμητικά συστήματα (και μπορούμε να φτιάξουμε όσα θέλουμε!) βασίζονται στην ίδια λογική, αλλάζει όμως η βάση. Έτσι π.χ. στο δυαδικό, το δεξιότερο (λιγότερο σημαντικό) ψηφίο αντιπροσωπεύει τις μονάδες, το επόμενο τις δυάδες, μετά τις τετράδες, οκτάδες κλπ. και γενικά μπορούμε να πούμε ότι η αξία ενός ψηφίου υπολογίζεται ως

ψηφίο X $2^{\text{θέση}}$

Στο δυαδικό βέβαια η μετατροπή είναι πολύ εύκολη καθώς τα ψηφία μπορεί να είναι μόνο 0 και 1 οπότε η μόνη πράξη που πρέπει να κάνουμε ουσιαστικά είναι η πρόσθεση (και λίγες δυνάμεις του 2).

Καθώς για τα συγκεκριμένα προβλήματα μας ενδιαφέρει να μετατρέπουμε αριθμούς από το 0 ως το 255, ξέρουμε ότι θα χρειαζόμαστε 8 bit. Φτιάχνουμε τον παρακάτω πίνακα με δυνάμεις από το 2^0 ως 2^7 και γράφουμε μέσα σε αυτό το δυαδικό αριθμό που θέλουμε να μετατρέψουμε:

Αξία Ψηφίου:	128	64	32	16	8	4	2	1
Ψηφίο:	**1**	**1**	**0**	**1**	**0**	**0**	**1**	**1**
Θέση Ψηφίου:	$\mathbf{b_7}$	$\mathbf{b_6}$	$\mathbf{b_5}$	$\mathbf{b_4}$	$\mathbf{b_3}$	$\mathbf{b_2}$	$\mathbf{b_1}$	$\mathbf{b_0}$

Αθροίζουμε τώρα όλες τις στήλες στις οποίες έχουμε άσους:

128+64+16+2+1=211. Δηλαδή:

$11010011_2 = 211_{10}$

Μετατροπή Δεκαδικού Αριθμού σε Δυαδικό

Για αυτή τη μετατροπή, δείχνουμε ένα απλό τρόπο χωρίς διαιρέσεις (τον κλασικό τρόπο μετατροπής που ήδη ξέρετε). Καθώς για το μάθημα δεν χρειαζόμαστε ποτέ αριθμούς μεγαλύτερους από 255, ξέρουμε ότι θα έχουμε πάντα το πολύ οκτώ ψηφία.

Το έντυπο βιβλίο έχει σαν παράδειγμα τον αριθμό 207, **αλλά βγάζει λάθος αποτέλεσμα(!)** γιατί έχουν κάνει λάθος στις πράξεις…(υπάρχει διόρθωση στα παροράματα)

Για να μετατρέψουμε το 207:

1. Ελέγχουμε αν αφαιρείται το 128 από το 207. Το αποτέλεσμα είναι 79. Σημειώνουμε **1** στο αντίστοιχο κουτάκι.
2. Ελέγχουμε τώρα το υπόλοιπο 79 με την αμέσως χαμηλότερη δύναμη του 2, το 64. 79-64=15. Γράφουμε και πάλι **1** στο αντίστοιχο κουτάκι.
3. Ελέγχουμε τώρα το 15 με την αμέσως χαμηλότερη δύναμη του 2, το 32. Επειδή το 32 δεν αφαιρείται από το 15, γράφουμε **0** στο αντίστοιχο κουτάκι.
4. Ελέγχουμε το 15 με την αμέσως χαμηλότερη δύναμη του 2, το 16. Επειδή το 16 δεν αφαιρείται από το 15, γράφουμε **0** στο αντίστοιχο κουτάκι.
5. Ελέγχουμε το 15 με την αμέσως χαμηλότερη δύναμη του 2, το 8. 15-8=7 οπότε γράφουμε **1** στο αντίστοιχο κουτάκι.
6. Ελέγχουμε το 7 με την αμέσως χαμηλότερη δύναμη του 2, το 4. 7-4=3 οπότε γράφουμε **1** στο αντίστοιχο κουτάκι.
7. Ελέγχουμε το 3 με την αμέσως χαμηλότερη δύναμη του 2, το 2. 3-2=1 οπότε γράφουμε **1** στο αντίστοιχο κουτάκι.
8. Τέλος, ελέγχουμε το 1 με την χαμηλότερη δύναμη του 2, το 1. 1-1=0 οπότε γράφουμε **1** στο αντίστοιχο κουτάκι.

Το τελικό αποτέλεσμα είναι ο δυαδικός αριθμός 11001111.

Αξία Ψηφίου:	128	64	32	16	8	4	2	1
Ψηφίο:	**1**	**1**	**0**	**0**	**1**	**1**	**1**	**1**
Θέση Ψηφίου:	$\mathbf{b_7}$	$\mathbf{b_6}$	$\mathbf{b_5}$	$\mathbf{b_4}$	$\mathbf{b_3}$	$\mathbf{b_2}$	$\mathbf{b_1}$	$\mathbf{b_0}$

Αποτέλεσμα: $207_{10} = 11001111_2$

Υποδείξεις για τις Μετατροπές

Όταν ένας αριθμός αποτελείται μόνο από δεξιά προς τα αριστερά συνεχόμενους άσους, αντί να κάνουμε τις πράξεις για να βρούμε το δεκαδικό αριθμό, απλά κοιτάμε την επόμενη αξία από τον πρώτο (αριστερότερο) άσο. Η τιμή που ψάχνουμε είναι αυτή η αξία μείον ένα.

Παράδειγμα:

Αξία Ψηφίου:	128	64	32	16	8	4	2	1
Ψηφίο:	**0**	**0**	**0**	**1**	**1**	**1**	**1**	**1**
Θέση Ψηφίου:	$\mathbf{b_7}$	$\mathbf{b_6}$	$\mathbf{b_5}$	$\mathbf{b_4}$	$\mathbf{b_3}$	$\mathbf{b_2}$	$\mathbf{b_1}$	$\mathbf{b_0}$

Αποτέλεσμα: $00011111_2 = 31_{10}$

Μπορείτε επίσης σε αυτή τη περίπτωση να κάνετε απλά την πράξη $2^{\text{πλήθος-άσων}}$-1. Δηλαδή 2^5-1 = 32 - 1 = 31.

Όταν έχουμε περισσότερους άσους από μηδενικά, μπορούμε αντί να αθροίζουμε τις αξίες των άσων, να αφαιρέσουμε τις αξίες των μηδενικών από το 255 που είναι ο μέγιστος αριθμός που μπορούμε να γράψουμε με 8 ψηφία.

Παράδειγμα:

Αξία Ψηφίου:	128	64	32	16	8	4	2	1
Ψηφίο:	**1**	**1**	**0**	**1**	**0**	**1**	**1**	**1**
Θέση Ψηφίου:	**b_7**	**b_6**	**b_5**	**b_4**	**b_3**	**b_2**	**b_1**	**b_0**

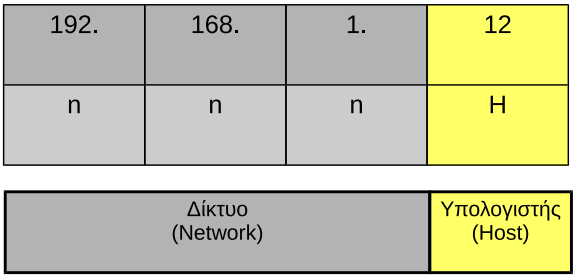
Αποτέλεσμα: 255 - 32 - 8 = 215

Τέλος, παρατηρήστε ότι όλες οι δυνάμεις του 2 είναι ζυγοί αριθμοί, εκτός από το 2^0=1. **Οπότε όποιος αριθμός στο δυαδικό τελειώνει σε 1, είναι περιττός (μονός) ενώ όποιος τελειώνει σε 0 είναι άρτιος (ζυγός)**. Έτσι μπορείτε να κάνετε μια πρώτη γρήγορη επαλήθευση των πράξεων σας.

3.1.2 Κλάσεις (Τάξεις) Δικτύων – Διευθύνσεων

Μια διεύθυνση δικτύου αποτελείται πάντα από δύο τμήματα: το πρώτο τμήμα *αναγνωρίζει το δίκτυο* στο οποίο ανήκει ο υπολογιστής (Network ID ή πρόθεμα - prefix) και το δεύτερο μέρος αναγνωρίζει τον υπολογιστή (Host ID ή επίθεμα - suffix) μέσα στο συγκεκριμένο δίκτυο. Αν θέλουμε να κάνουμε μια αντιστοίχιση με την καθημερινότητα, το τμήμα δικτύου δείχνει την οδό στην οποία βρίσκεται μια κατοικία ενώ το τμήμα υπολογιστή είναι ο αριθμός της πάνω στην οδό.

Για παράδειγμα, στην διεύθυνση 192.168.1.12, το τμήμα δικτύου είναι το 192.168.1 και δείχνει στο δίκτυο 192.168.1.0 ενώ το τμήμα υπολογιστή είναι το 12, που προσδιορίζει ένα συγκεκριμένο υπολογιστή πάνω σε αυτό το δίκτυο.



Τα δύο αυτά τμήματα δεν καταλαμβάνουν το ίδιο μήκος: διαφοροποιούνται ανάλογα με το μέγεθος του δικτύου και το πλήθος των υπολογιστών που θέλουμε να

συνδέσουμε σε αυτό. Στο παράδειγμα μας, το τμήμα υπολογιστή χρησιμοποιεί μόνο την τελευταία οκτάδα (το τελευταίο byte) της διεύθυνσης. Με 8 bit μπορούμε να γράψουμε μέχρι 2^8=256 διαφορετικές διευθύνσεις, άρα στο δίκτυο 192.168.1.0 μπορούμε να συνδέσουμε μέχρι 256 διαφορετικούς υπολογιστές (στην πραγματικότητα 254, καθώς η τιμή 0 προσδιορίζει τη *διεύθυνση δικτύου* και το 255 την *διεύθυνση εκπομπής* του δικτύου και δεν μπορούν να χρησιμοποιηθούν για κανονικές διευθύνσεις μηχανημάτων).

Αν θέλουμε το δίκτυο να έχει περισσότερους από 254 υπολογιστές, θα πρέπει να δώσουμε στο τμήμα υπολογιστή ακόμα μια οκτάδα. Τότε το δίκτυο θα μπορεί να έχει μέχρι 2^{16}=65536 υπολογιστές (στην πραγματικότητα, 65536 - 2 = 65534 όπως και πριν). Για ακόμα μεγαλύτερα δίκτυα μπορούμε να δώσουμε ακόμα μια οκτάδα στο τμήμα υπολογιστή, φτάνοντας έτσι τα 24 bit για το τμήμα υπολογιστή. Όσο αυξάνουμε το ένα τμήμα της διεύθυνσης IP, ανάλογα μειώνεται το άλλο και συνολικά η διεύθυνση παραμένει πάντα 32 bit.

Με τον παραπάνω τρόπο ορίζουμε *τάξεις ή κλάσεις* δικτύων ανάλογα με το μέγεθος που μας εξυπηρετεί: ουσιαστικά μπορούμε να φτιάξουμε λίγα δίκτυα με μεγάλο αριθμό υπολογιστών (όταν δώσουμε τρεις οκτάδες στο τμήμα υπολογιστή), περισσότερα δίκτυα με ενδιάμεσο αριθμό υπολογιστών (όταν δώσουμε δύο οκτάδες στο τμήμα υπολογιστή) ή πολλά δίκτυα με λίγους υπολογιστές (όταν δώσουμε μια οκτάδα στο τμήμα υπολογιστή). Ο πίνακας στο σχήμα 3.2 δείχνει αυτούς τους συνδυασμούς.

Τάξη	Διεύθυνση IP – 4 οκτάδες				Δίκτυα	Υπολογιστές
A	0 | n (7 bit)	H	H	H	2^7=128	2^{24}- 2 = 16777214
	Δίκτυο	Υπολογιστής				
B	10 | n (6 bit)	n (8 bit)	H	H	2^{14}=16384	2^{16}- 2 = 65534
	Δίκτυο		Υπολογιστής			
C	110 | n (5 bit)	n (8 bit)	n (8 bit)	H	2^{21}=2097152	2^8- 2 = 254
	Δίκτυο			Υπολογιστής		

n = Network (Δίκτυο) H = Host (Υπολογιστής)

Σχήμα 3.2: *Κλάσεις/Τάξεις Διευθύνσεων IPv4*

Συνολικά οι τάξεις δικτύων που μας ενδιαφέρουν είναι τρεις και χαρακτηρίζονται με τα γράμματα A,B,C. Προσέξτε ότι ανάλογα με την κλάση ορίζεται κάποιο ή κάποια ψηφία στην πρώτη οκτάδα που έχουν συγκεκριμένη τιμή. Έτσι:

- **Για Δίκτυα Τάξης Α:** Το πρώτο ψηφίο της πρώτης οκτάδας **έχει την τιμή 0**. Έτσι η πρώτη οκτάδα παίρνει τιμές από 00000000 μέχρι 01111111 δηλ. από 0

Τάξη	1η Οκτάδα	Δυαδικό		Δεκαδικό		Παρατηρήσεις
		Από	Έως	Από	Έως	
A	0xxx xxxx	0000 0000	0111 1111	0	127	x: 0 ή 1
B	10xx xxxx	1000 0000	1011 1111	128	191	
C	110x xxxx	1100 0000	1101 1111	192	223	
D	1110 xxxx	1100 0000	1110 1111	224	239	Multicast (Πολυδιανομή)
E	1111 0xxx	1111 0000	1111 1111	240	255	Δεσμευμένες

Πίνακας 3.1: Προσδιορισμός Κλάσης/Τάξης Διευθύνσεων

ως 127.

- **Για Δίκτυα Τάξης B:** Τα δύο πρώτα ψηφία της πρώτης οκτάδας **έχουν την τιμή 10**. Έτσι η πρώτη οκτάδα παίρνει τιμές από 10000000 μέχρι 10111111 δηλ. από 128 ως 191.

- **Για Δίκτυα Τάξης C:** Τα τρία πρώτα ψηφία της πρώτης οκτάδας **έχουν την τιμή 110**. Έτσι η πρώτη οκτάδα παίρνει τιμές από 11000000 μέχρι 11011111 δήλ. από 192 ως 223.

Εκτός από τις A,B,C που χρησιμοποιούνται για κανονική διευθυνσιοδότηση σε δίκτυα υπάρχουν και οι τάξεις D (διευθύνσεις που χρησιμοποιούνται για πολυδιανομή - multicasting) και E (δεσμευμένες) οι οποίες όμως είναι ειδικού σκοπού και δεν χρησιμοποιούνται ως διευθύνσεις σε υπολογιστές δικτύων. Ο πίνακας 3.1 συνοψίζει τις τάξεις διευθύνσεων και τα χαρακτηριστικά τους.

Κοιτάζοντας μόνο τη τιμή της πρώτης οκτάδας, μπορούμε άμεσα να προσδιορίσουμε σε ποια κλάση ανήκει το δίκτυο:

- Από 1 - 127: Δίκτυο τάξης A

- Από 128 - 191: Δίκτυο τάξης B

- Από 192 - 223: Δίκτυο τάξης C

- Τιμές από 224 και άνω είναι ειδικού σκοπού (όχι για απόδοση διεύθυνσης δικτύου σε υπολογιστή)

Εννοείται ότι αν μας δίνουν τη διεύθυνση στο δυαδικό, κοιτάζουμε την τιμή των πρώτων ψηφίων της πρώτης οκτάδας! Ο παρακάτω πίνακας δίνει παραδείγματα διευθύνσεων και τάξεων που ανήκουν:

Διεύθυνση IP	Τάξη	Αιτιολογία
192.168.1.12	C	Το 192 ανήκει στο διάστημα 192…223
10.146.0.1	A	Το 10 ανήκει στο διάστημα 0…127
172.16.32.253	B	Το 172 ανήκει στο διάστημα 128…191
127.0.0.1	A	Το 127 ανήκει στο διάστημα 1…127
194.219.227.1	C	Το 194 ανήκει στο διάστημα 192…223

Διαχείριση και Απόδοση Διευθύνσεων IP

Οι διευθύνσεις IP είναι μοναδικές στον κόσμο: Ανά πάσα στιγμή δεν είναι δυνατόν δύο υπολογιστές με άμεση σύνδεση στο Internet να έχουν την ίδια διεύθυνση IP. Η διαχείριση των διευθύνσεων γίνεται από ένα κεντρικό φορέα, τον *IANA/ICANN* (Internet Assigned Numbers Authority και Internet Corporation for Assigned Names and Numbers). Ο φορέας αυτός μεταβιβάζει αρμοδιότητες διαχείρισης σε περιφερειακούς καταχωρητές (RIR – Regional Internet Registry) και μέσω αυτών σε τοπικούς ή εθνικούς καταχωρητές (LIR – Local Internet Registry ή NIR – National Internet Registry). Για την Ευρώπη, Μέση Ανατολή και Κεντρική Ασία περιφερειακός καταχωρητής Internet είναι το RIPE NCC.

Οι τελικοί απλοί (οικιακοί) χρήστες καθώς και εταιρικοί χρήστες απευθύνονται στον πάροχο υπηρεσιών Διαδικτύου (ISP, Internet Service Provider) ο οποίος παρέχει υπηρεσίες πρόσβασης στο Διαδίκτυο και αποδίδει κάθε φορά σε αυτούς τις απαιτούμενες διευθύνσεις IP. Η απόδοση μπορεί να γίνεται δυναμικά (π.χ. αν κλείσουμε τον οικιακό μας δρομολογητή ADSL και τον ξανανοίξουμε, θα πάρουμε μια διαφορετική IP διεύθυνση) ή στατικά (να παίρνουμε κάθε φορά την ίδια σταθερή IP). Οι IPSs συνήθως είναι και τοπικοί καταχωρητές.

Ιδιωτικές Διευθύνσεις IP

Σύμφωνα με όσα γράψαμε παραπάνω, φαίνεται ότι είναι απαραίτητο πριν φτιάξουμε ένα δίκτυο (ακόμα και για δική μας χρήση) να έχουμε ζητήσει να μας διατεθούν διευθύνσεις IP από κάποιο πάροχο. Ωστόσο αυτό δεν είναι αλήθεια: τα περισσότερα τοπικά δίκτυα υπολογιστών μπορούν να χρησιμοποιούν την τεχνολογία IP αλλά δεν είναι άμεσα συνδεδεμένα στο Internet.

Για παράδειγμα:

Στο σπίτι σας πιθανότητα διαθέτετε μια σύνδεση ADSL και συνδέεστε με ένα ή περισσότερους υπολογιστές μέσω Ethernet ή WiFi σε ένα δρομολογητή που σας έχει προμηθεύσει ο παροχέας σας. Ο δρομολογητής αυτός αποστέλλει και όλες τις

απαραίτητες ρυθμίσεις δικτύου στο μηχάνημα σας (μέσω του πρωτοκόλλου DHCP που θα δούμε σε επόμενη ενότητα) και έτσι δεν χρειάζεται να τις κάνετε εσείς. Αν δείτε τη διεύθυνση IP του μηχανήματος σας, θα διαπιστώσετε ότι είναι της μορφής 192.168.0.X ή 192.168.1.X όπου το X αναφέρεται στο τμήμα υπολογιστή.

Οι διευθύνσεις αυτές δεν είναι μοναδικές: όλοι οι οικιακοί δρομολογητές χρησιμοποιούν τις ίδιες ρυθμίσεις. Πως όμως συνδέεστε στο Internet χωρίς μοναδική IP; Στην πραγματικότητα αυτή η διεύθυνση είναι γνωστή μόνο στο δικό σας τοπικό δίκτυο. Ο δρομολογητής διαθέτει δική του διαφορετική (και μοναδική) διεύθυνση με την οποία είναι συνδεδεμένος στο Internet. Η διεύθυνση αυτή αποδίδεται δυναμικά (συνήθως) από τον παροχέα και μπορεί να αλλάζει ανά τακτά διαστήματα (αλλάζει επίσης αν κλείσετε το router και το ξανανοίξετε). Όταν επικοινωνείτε με το Internet, ο δρομολογητής αλλάζει τη δική σας εσωτερική διεύθυνση με τη δική του πριν στείλει τα πακέτα σας. Εσωτερικά κρατάει ένα πίνακα αντιστοιχιών ώστε όταν λάβει απάντηση να αλλάξει την διεύθυνση προορισμού ξανά με τη δική σας εσωτερική IP. Η τεχνική αυτή ονομάζεται *NAT (Network Address Translation)* και μας επιτρέπει να συνδέσουμε ένα πλήθος υπολογιστών στο διαδίκτυο ενώ χρησιμοποιούμε μόνο μια δεσμευμένη διεύθυνση IP. Η σύνδεση εδώ δεν είναι άμεση: κανένα από αυτά τα μηχανήματα δεν φαίνεται απευθείας μέσω Internet. Μόνο ο δρομολογητής είναι άμεσα ορατός.

Για το σκοπό αυτό έχουν προβλεφθεί περιοχές διευθύνσεων και των τριών τάξεων που μπορούν να χρησιμοποιηθούν αυθαίρετα και χωρίς κανένα συντονισμό με κάποια από τις αρχές διαχείρισης διευθύνσεων. Να σημειωθεί εδώ ότι όλοι οι δρομολογητές της αγοράς είναι από πριν ρυθμισμένοι να αναγνωρίζουν τις περιοχές αυτές και ποτέ δεν δρομολογούν αυτές τις διευθύνσεις στο Internet. Οι περιοχές αυτές περιγράφονται στο έγγραφο RFC1918 - Address Allocation for Private Internets και φαίνονται στον παρακάτω πίνακα:

Τάξη	**Από**	**Εώς**	**Μορφή CIDR**
A	10.0.0.0	10.255.255.255	10.0.0.0/8
B	172.16.0.0	172.31.255.255	172.16.0.0/12
C	192.168.0.0	192.168.255.255	192.168.0.0/16

Σημείωση: Για τη μορφή CIDR θα μιλήσουμε σε επόμενη ενότητα.

Για την υλοποίηση ενός ιδιωτικού δικτύου επιλέγονται διευθύνσεις μόνο από τον παραπάνω πίνακα, ανάλογα με το μέγεθος του δικτύου που θα υλοποιηθεί. Για το τοπικό οικιακό ή μικρό δίκτυο επιλέγονται συνήθως διευθύνσεις από την τάξη C, έτσι συχνά βλέπουμε IP όπως 192.168.0.1 κλπ.

3.1.3 Σπατάλη Διευθύνσεων IP

Έχουμε δει ότι ένα δίκτυο κλάσης C μπορεί να δεχθεί μέχρι 254 διαφορετικούς υπολογιστές. Φανταστείτε μια εταιρεία που χρειάζεται να συνδέσει 55 υπολογιστές στο Internet. Θα πρέπει να ζητήσει να της παραχωρηθεί μια περιοχή διευθύνσεων τάξης C. Όμως θα χρησιμοποιήσει μόνο 55 διευθύνσεις. Οι υπόλοιπες 199 θα παραμείνουν δεσμευμένες και ανεκμετάλλευτες. Αν βέβαια αργότερα η εταιρεία μεγαλώσει θα μπορέσει να χρησιμοποιήσει και τις υπόλοιπες διευθύνσεις που της έχουν παραχωρηθεί χωρίς να ζητήσει νέα περιοχή.

Τι γίνεται όμως αν μια εταιρεία χρειάζεται να συνδέσει 300 μηχανήματα; Αν ζητήσει μια περιοχή τάξης B θα της αποδοθούν 65534 διευθύνσεις από τις οποίες θα χρησιμοποιήσει μόνο 300. *Οι υπόλοιπες 65234 θα παραμείνουν δεσμευμένες και ανεκμετάλλευτες*.

Ένας τέτοιος τρόπος διαμοιρασμού διευθύνσεων οδηγεί γρήγορα στην εξάντληση των διαθέσιμων διευθύνσεων IP (ειδικά της τάξης B). Πέρα από τη *σπατάλη και εξάντληση των διευθύνσεων* ο τρόπος αυτός οδηγεί και σε *δυσχέρειες στη δρομολόγηση των πακέτων δεδομένων και στη διαχείριση των πινάκων δρομολόγησης*.

Σήμερα γενικά δεν χρησιμοποιούμε το σύστημα με τις τάξεις διευθύνσεων: αντί για αυτό κάθε διεύθυνση IP συνοδεύεται από ένα ακόμα αριθμό τη *μάσκα δικτύου* με την οποία επιτυγχάνουμε τη λεγόμενη *αταξική δρομολόγηση* (CIDR – Classless Internet Domain Routing). Η αταξική δρομολόγηση περιγράφεται στα RFC1519 και RFC4632.

3.1.4 Μάσκα Δικτύου

Για να αποφύγουμε τη σπατάλη διευθύνσεων, μαζί με τη διεύθυνση IP χρησιμοποιούμε ακόμα ένα αριθμό, μεγέθους 32 bit την *μάσκα δικτύου (network mask)*. Η μάσκα διευκρινίζει ποια ψηφία της διεύθυνσης ανήκουν στο αναγνωριστικό δικτύου (network ID) και ποια στο αναγνωριστικό υπολογιστή (host id) μέσα στο συγκεκριμένο δίκτυο.

Με τον παραπάνω τρόπο:

- Όπου η μάσκα έχει άσους (1) το αντίστοιχο ψηφίο της διεύθυνσης IP ανήκει στο αναγνωριστικό δικτύου.
- Όπου η μάσκα έχει μηδενικά (0) το αντίστοιχο ψηφίο της διεύθυνσης IP ανήκει στο αναγνωριστικό υπολογιστή.

Να σημειώσουμε εδώ ότι δεν είναι δυνατόν να **αναμειγνύονται μεταξύ τους οι άσοι και τα μηδενικά**. Η μάσκα ξεκινάει πάντα σαν μια σειρά από άσους και καταλήγει σε μηδενικά. Δεν μπορεί ένας άσος στα αριστερά του να έχει ένα μηδενικό, και ένα μηδέν στα δεξιά του ένα άσο.

Για παράδειγμα, η παρακάτω μάσκα δικτύου είναι σωστή:

11111111 11111111 11111111 00000000

ενώ η επόμενη είναι **λάθος:**

11111111 11110111 11111111 00000000

Η παραπάνω απαίτηση περιγράφεται στο έγγραφο RFC1812 σελ.22. Ένα παράδειγμα διεύθυνσης δικτύου με μάσκα φαίνεται παρακάτω:

(δεκαδική μορφή)	192.	168.	1.	18.
Διεύθυνση IP:	1100 0000	1010 1000	0000 0001	0001 0010
Μάσκα:	1111 1111	1111 1111	1111 1111	0000 0000
(δεκαδική μορφή)	255.	255.	255.	0

Η *διεύθυνση δικτύου* στην οποία ανήκει ο υπολογιστής μπορεί να βρεθεί με την πράξη του *λογικού ΚΑΙ (AND)* μεταξύ των ψηφίων της διεύθυνσης IP και της μάσκας δικτύου.

Τι είναι το λογικό ΚΑΙ;

Είναι η λογική πράξη η οποία δίνει την τιμή ΑΛΗΘΗΣ (ή 1) μόνο όταν και οι δύο τιμές έχουν τιμή ΑΛΗΘΗΣ. Διαφορετικά, δίνει τιμή ΨΕΥΔΗΣ ή 0. Προσέξτε ότι οι λογικές πράξεις δεν είναι ίδιες με τις αντίστοιχες αριθμητικές! Ωστόσο μπορούμε να βρούμε το αποτέλεσμα του λογικού ΚΑΙ απλά πολλαπλασιάζοντας μεταξύ τους τα δυαδικά ψηφία.

Στο προηγούμενο παράδειγμα μας, υπολογίζουμε την διεύθυνση δικτύου με τον τρόπο που φαίνεται παρακάτω:

Διεύθυνση IP:	1100 0000	1010 1000	0000 0001	0001 0010	192.168.1.18
Μάσκα:	1111 1111	1111 1111	1111 1111	0000 0000	255.255.255.0
Διεύθυνση Δικτύου:	1100 0000	1010 1000	0000 0001	0000 0000	192.168.1.0

Προκαθορισμένες Μάσκες Δικτύων Τάξης A,B,C

Από τη περιγραφή που δώσαμε για τη μάσκα δικτύου, μπορούμε να υπολογίσουμε τις μάσκες για τις τρεις προκαθορισμένες κλάσεις δικτύων A,B,C που έχουμε δει. Γνωρίζουμε ότι για την κλάση A, χρησιμοποιούνται 8 ψηφία στο τμήμα δικτύου, για την κλάση B, 16 ψηφία και για την C, 24 ψηφία. Αυτός ο αριθμός των ψηφίων θα αντιπροσωπεύεται από άσους (1) στην αντίστοιχη μάσκα:

Τάξη	1η Οκτάδα	Δεκαδικό		Μάσκα		Παρατηρήσεις
		Από	Εώς	Δεκαδική	CIDR	
A	0xxx xxxx	0	127	255.0.0.0	/8	x: 0 ή 1
B	10xx xxxx	128	191	255.255.0.0	/16	
C	110x xxxx	192	223	255.255.255.0	/24	

Όπως έχουμε πει, σε μια μάσκα δικτύου δεν μπορεί να αναμειγνύονται οι άσοι και τα μηδενικά. Αν μετρήσουμε όλους τους άσους στη μάσκα, μπορούμε αντί να τη γράψουμε στη κλασική της δεκαδική μορφή, να χρησιμοποιήσουμε τη μορφή CIDR: βάζουμε μια κάθετο (/) μετά τη διεύθυνση IP και τον αριθμό των άσων της μάσκας. Π.χ. σε ένα δίκτυο κλάσης C, η μάσκα είναι 255.255.255.0 δηλ. 24 άσοι και 8 μηδενικά. Αυτή η μάσκα σε μορφή CIDR γράφεται ως /24. Έτσι, για τη διεύθυνση 192.168.0.16 θα γράφαμε 192.168.0.16/24. Η μορφή CIDR είναι γνωστή επίσης ως *πρόθεμα ή prefix*.

3.1.5 Ειδικές Διευθύνσεις

Εκτός από τις κανονικές διευθύνσεις IP που προορίζονται για συγκεκριμένους υπολογιστές (ονομάζονται διευθύνσεις *αποκλειστικής διανομής ή unicast*) υπάρχουν και κάποιες ειδικές κατηγορίες διευθύνσεων.

- **Διεύθυνση Δικτύου:** Προσδιορίζει το δίκτυο στο οποίο ανήκει μια διεύθυνση. Για να βρούμε τη διεύθυνση δικτύου, χρειαζόμαστε μια διεύθυνση IP που να ανήκει στο δίκτυο και τη μάσκα. Η διεύθυνση δικτύου είναι ίδια με τη διεύθυνση IP στο κομμάτι που αντιστοιχεί στο τμήμα δικτύου (εκεί δηλαδή που τα αντίστοιχα ψηφία της μάσκας είναι άσοι) ενώ στο τμήμα του υπολογιστή έχει μηδενικά. Δείτε την προηγούμενη ενότητα για τον υπολογισμό της διεύθυνσης δικτύου καθώς και τον Οδηγό Ασκήσεων Υποδικτύωσης.
- **Διεύθυνση Εκπομπής:** Αφορά όλους τους υπολογιστές που βρίσκονται στο ίδιο δίκτυο. Όταν ένα πακέτο έχει διεύθυνση προορισμού τη διεύθυνση εκπομπής λαμβάνεται από όλους τους υπολογιστές που βρίσκονται στο ίδιο δίκτυο ή υποδίκτυο (όπως προσδιορίζεται από την αντίστοιχη μάσκα). Για να βρούμε

τη διεύθυνση εκπομπής ξεκινάμε πάντα από τη *διεύθυνση δικτύου* και *θέτουμε σε "1" όλα τα ψηφία που ανήκουν στο τμήμα υπολογιστή*. Για παράδειγμα, στη διεύθυνση 192.168.1.18 με μάσκα 255.255.255.0, η διεύθυνση δικτύου είναι 192.168.1.0. Σε αυτή τη διεύθυνση θέτουμε σε "1" τα ψηφία της τελευταίας οκτάδας (που σύμφωνα με τη μάσκα αντιστοιχούν στο τμήμα υπολογιστή) και έχουμε το 192.168.0.255. *Προσέξτε ότι σε μάσκες που δεν έχουν μόνο τις προφανείς τιμές 0 και 255 θα πρέπει να κάνουμε την επεξεργασία ψηφίο προς ψηφίο και προσεκτικά!* Δείτε επίσης και τον Οδηγό Ασκήσεων Υποδικτύωσης.

- **Διεύθυνση Πολυδιανομής:** Πρόκειται για διευθύνσεις κλάσης D οι οποίες προσδιορίζουν μια ομάδα υπολογιστών/κόμβων. Για παράδειγμα, οι δρομολογητές του υποδικτύου ακούνε στη διεύθυνση 224.0.0.2. Η υλοποίηση των τεχνικών πολυδιανομής περιγράφεται στο RFC1112 και στην σελίδα της IANA υπάρχει επίσημη λίστα αυτών των διευθύνσεων και η χρήση τους.

- **Διεύθυνση Επανατροφοδότησης ή Ανατροφοδότησης:** Γνωστή επίσης και με τις ονομασίες *Loopback ή Local Loopback*. Πρόκειται για διευθύνσεις που ανήκουν στο δίκτυο 127.0.0.0/8 και συνήθως 127.0.0.0/32. Χρησιμοποιούνται για να κάνει ένας υπολογιστής δίκτυο με τον εαυτό του. Τα πακέτα που στέλνονται με προορισμό μια τέτοια διεύθυνση (συνήθως το 127.0.0.1 αλλά και οποιαδήποτε άλλη του 127.0.0.0/8) δεν φεύγουν ποτέ από τον υπολογιστή ούτε προωθούνται σε κάποια διεπαφή δικτύου. Απλά επιστρέφουν στον ίδιο υπολογιστή που τα έστειλε.

  Η διεύθυνση αυτή λειτουργεί ακόμα και σε υπολογιστές που δεν είναι συνδεδεμένοι σε κάποιο δίκτυο, ακόμα και σε αυτούς που δεν διαθέτουν καν κάρτα δικτύου. Ο λόγος είναι ότι διάφορες υπηρεσίες μέσα σε ένα υπολογιστή μπορεί να επικοινωνούν μεταξύ τους μέσω δικτύου και είναι άσκοπο (και ενδεχομένως και επικίνδυνο από άποψη ασφάλειας) τα πακέτα τους να προωθούνται στο κανονικό φυσικό δίκτυο και πίσω στον ίδιο τον υπολογιστή. Με τη χρήση του Loopback Address μπορούν οι υπηρεσίες αυτές να λειτουργούν ακόμα και χωρίς να υπάρχει πραγματική δικτυακή σύνδεση.

- **Διεύθυνση Limited Source 0.0.0.0/8:** Συναντάται μόνο ως *διεύθυνση προέλευσης (source)* και δηλώνει πακέτα που προέρχονται από υπολογιστές του ίδιου δικτύου στο οποίο ανήκει και ο υπολογιστής που τα παραλαμβάνει. Αν τα πακέτα προέρχονται από διευθύνσεις τύπου 0.0.0.0/32, προέρχονται από τον ίδιο τον υπολογιστή που τα παραλαμβάνει.

- **Διευθύνσεις Link Local 169.254.0.0/16:** Γνωστές και ως διευθύνσεις APIPA (Automatic Private IP Addressing). Για ευκολία στη διαχείριση, σε πολλά δίκτυα TCP/IP οι παράμετροι του δικτύου (διεύθυνση IP και άλλες ρυθμίσεις) δεν γίνονται χειροκίνητα σε κάθε μηχάνημα: υπάρχει ένας διακομιστής DHCP

(θα δούμε σε επόμενη ενότητα) που στέλνει αυτές τις ρυθμίσεις αυτόματα σε κάθε μηχάνημα που συνδέεται. Σε περίπτωση που ένα μηχάνημα έχει ρυθμιστεί να λαμβάνει αυτόματα ρυθμίσεις αλλά ο διακομιστής DHCP δεν ανταποκρίνεται (π.χ. λόγω βλάβης), τότε θα πάρει μια τυχαία διεύθυνση από την περιοχή 169.254.0.0/16. Για αυτές τις διευθύνσεις θα βρείτε λεπτομέρειες στο RFC3927.

- **Άλλες Ειδικές Διευθύνσεις IP:** Περιγράφονται στο RFC3330 (Special-Use IPv4 Addresses).

Ο παρακάτω πίνακας συνοψίζει μερικές από τις παραπάνω κατηγορίες με παραδείγματα:

Διεύθυνση	**Ερμηνεία**	**Παράδειγμα**
Αποκλειστικής Διανομής (unicast)	Προσδιορίζει ένα υπολογιστή (host) (μια διασύνδεση)	192.168.1.3 Ο υπολογιστής 192.168.1.3
Πολυδιανομής (multicast)	Προσδιορίζει ομάδα (group) υπολογιστών	224.0.0.2 Δρομολογητές του δικτύου (κλάση D)
Εκπομπής ή Ακρόασης broadcast	προσδιορίζει όλους τους υπολογιστές ενός δικτύου ή υποδικτύου	192.168.1.255 όλοι οι υπολογιστές του 192.168.1.0/24
Επανατροφοδότησης Loopback	Αναφέρεται στον ίδιο υπολογιστή	127.0.0.1 το ίδιο το μηχάνημα
Link Local	Διεύθυνση APIPA	169.254.54.21

3.1.6 Υποδικτύωση

Σε αρκετές περιπτώσεις είναι επιθυμητό να χωρίσουμε ένα δίκτυο σε μικρότερα *υποδίκτυα*:

- **Οικονομία διευθύνσεων IP:** Όπως έχουμε δει, χρησιμοποιώντας τις τυποποιημένες κλάσεις δικτύων υπάρχει μεγάλη σπατάλη διευθύνσεων: Μια εταιρεία που χρειάζεται 2000 υπολογιστές δεν χρειάζεται τις πάνω από 65 χιλιάδες διευθύνσεις ενός δικτύου κλάσης B. Οι διευθύνσεις που περισσεύουν πάνε χαμένες. Με την υποδικτύωση μπορούμε να μοιράσουμε ένα δίκτυο κλάσης B σε 32 υποδίκτυα των 2048 διευθύνσεων και να τις κατανείμουμε σε πολλαπλές εταιρίες.

- **Διαχειριστικοί λόγοι:** Μια εταιρεία μπορεί να διαθέτει λιγότερα από 254 μηχανήματα (ένα δίκτυο κλάσης C δηλαδή) αλλά σε διαφορετικούς χώρους ώστε

να εξυπηρετούν διαφορετικούς σκοπούς. Π.χ. κάποια μηχανήματα στο λογιστήριο, άλλα στο γραφείο κίνησης, στην αποθήκη κλπ. Αντί όλα αυτά τα μηχανήματα να είναι συνδεδεμένα σε ένα δίκτυο, μπορούμε να το χωρίσουμε σε υποδίκτυα ένα για κάθε τμήμα. Το κάθε υποδίκτυο μπορεί αν χρειάζεται να επικοινωνεί με τα άλλα μέσω δρομολογητών (όπως θα δούμε παρακάτω) και ταυτόχρονα δεν αυξάνεται η άσκοπη κίνηση στο δίκτυο όταν οι υπολογιστές ενός τμήματος επικοινωνούν μόνο με άλλους στο ίδιο τμήμα.

Για να εκτελέσουμε την υποδικτύωση, θα ακολουθήσουμε τα παρακάτω βήματα:

- Το ζητούμενο μας μπορεί να είναι να χωρίσουμε το δίκτυο σε *n πλήθος υποδικτύων* ή σε *m πλήθος υπολογιστών*. Από τους αριθμούς αυτούς θα υπολογίσουμε μια *νέα μάσκα δικτύου*
- Θα υπολογίσουμε τις *περιοχές διευθύνσεων* και τις διευθύνσεις υποδικτύου και εκπομπής για κάθε υποδίκτυο. Θα βρούμε την αρχική και τελική διεύθυνση IP που μπορούν να χρησιμοποιηθούν στους υπολογιστές που συνδέονται στο υποδίκτυο

Σημείωση: Όταν δίνουμε bits από το τμήμα υπολογιστή στο τμήμα δικτύου, έχουμε **υποδικτύωση**. Όταν δίνουμε bits από το τμήμα δικτύου στο τμήμα υπολογιστή έχουμε **υπερδικτύωση** (θα τη δούμε στην επόμενη ενότητα).

Για παραδείγματα και μεθοδολογία ασκήσεων δείτε και τον Οδηγό Ασκήσεων Υποδικτύωσης.

Παράδειγμα 1

Δίνεται η διεύθυνση δικτύου 192.168.3.0/24 (μάσκα 255.255.255.0).

- Να χωριστεί το δίκτυο σε τουλάχιστον έξι υποδίκτυα
- Να δοθούν οι περιοχές διευθύνσεων κάθε υποδικτύου
- Να δοθούν οι διευθύνσεις υποδικτύου και εκπομπής για κάθε υποδίκτυο
- Πόσους υπολογιστές μπορεί να έχει το κάθε υποδίκτυο;

Παρατηρήσεις για όλες τις ασκήσεις υποδικτύωσης:

- Θα πρέπει να ξέρουμε να μετατρέπουμε δυαδικό σε δεκαδικό και αντίστροφα

- Τα δεδομένα μπορεί να μας δίνονται σε δυαδικό ή (συνήθως) σε δεκαδικό. Για να κάνουμε υποδικτύωση θα πρέπει να μετατρέψουμε τα δεδομένα μας σε δυαδικό
- Σε κάθε υποδίκτυο, η πρώτη διεύθυνση που βρίσκουμε είναι η *διεύθυνση υποδικτύου* και η τελευταία η *διεύθυνση εκπομπής* για το συγκεκριμένο υποδίκτυο
- Σε κάθε υποδίκτυο "χάνουμε" δύο διευθύνσεις IP (την δικτύου και την εκπομπής). Π.χ. σε ένα υποδίκτυο με 16 διευθύνσεις, μόνο οι 14 είναι διαθέσιμες για IP υπολογιστών
- Τα διαθέσιμα υποδίκτυα ή IP διευθύνσεις που προκύπτουν είναι πάντοτε δυνάμεις του δύο. Αν μας πουν να χωρίσουμε το δίκτυο σε 6 υποδίκτυα, θα το χωρίσουμε στην πραγματικότητα σε 8. Γιαυτό άλλωστε και η εκφώνηση περιέχει τη λέξη "τουλάχιστον"

Για να απαριθμήσουμε 6 υποδίκτυα, θα χρειαστούμε στην πραγματικότητα να δώσουμε τρία επιπλέον bit στο τμήμα δικτύου. Με δύο bit μπορούμε να απαριθμήσουμε μέχρι 4 υποδίκτυα (2^2=4) ενώ με 3 bit, 8 υποδίκτυα (2^3=8). Τελικά θα έχουμε 8 υποδίκτυα και όχι 6 (είναι σκόπιμο να θυμάστε ή να μπορείτε να υπολογίσετε γρήγορα τις δυνάμεις του 2 μέχρι το 2^8=256).

Τα τρία έξτρα bit που θα δώσουμε στο τμήμα δικτύου, θα φαίνονται στη νέα μάσκα δικτύου ως "1". Το πρώτο πράγμα που πρέπει να υπολογίσουμε είναι η νέα μάσκα δικτύου:

Διεύθυνση Δικτύου	192	168	3	0
Παλιά Μάσκα Δικτύου	255	255	255	0
	11111111	11111111	11111111	00000000
Νέα Μάσκα Υποδικτύου	11111111	11111111	11111111	111 00000
	255	255	255	224

Η νέα μάσκα δικτύου είναι 255.255.255.224 και σε μορφή CIDR, μπορούμε να γράψουμε 192.168.3.0/27. Οι διευθύνσεις των υπολογιστών είναι της μορφής

<Network_ID>, <Subnet_ID >, <Host_ID>

με το τμήμα δικτύου (Network_ID) να καταλαμβάνει 24 bits, το τμήμα υποδικτύου (Subnet_ID) να καταλαμβάνει 3 bits και το τμήμα υπολογιστή (Host_ID) να καταλαμβάνει τα υπόλοιπα 5 bits.

Είναι προφανές ότι με 5 bits στο τμήμα υπολογιστή μπορούμε να έχουμε σε κάθε υποδίκτυο συνολικά 2^5=32 διευθύνσεις IP. Από αυτές η πρώτη είναι πάντα η διεύθυνση δικτύου και η τελευταία η διεύθυνση εκπομπής του υποδικτύου. Άρα συνο-

λικά σε κάθε υποδίκτυο θα έχουμε 30 διευθύνσεις IP που μπορούν να αποδοθούν σε υπολογιστές.

Σε σχέση με ένα δίκτυο κλάσης C, το οποίο μπορεί να έχει συνολικά 254 υπολογιστές, εδώ έχουμε λιγότερους γιατί χάνουμε δυο διευθύνσεις ανά υποδίκτυο. Έχουμε 8 υποδίκτυα με 30 διαθέσιμες IP, άρα συνολικά 240 διαθέσιμες IP. Η απώλεια αυτή είναι μικρή σε σχέση με τα οφέλη που αποκομίζουμε από την υποδικτύωση.

Για να γράψουμε τον πίνακα με τις περιοχές διευθύνσεων των υποδικτύων πιο εύκολα, παρατηρούμε τα παρακάτω:

- Στις οκτάδες που η μάσκα παραμένει 255 (11111111_2) δεν υπάρχει κάποια αλλαγή σε σχέση με προηγουμένως. Οι υπολογισμοί μας στο συγκεκριμένο παράδειγμα αφορούν μόνο την τέταρτη οκτάδα
- Υπάρχουν οκτώ υποδίκτυα που αντιστοιχούν στα αναγνωριστικά υποδικτύων από 0 ως 7 δηλ. από 000_2 ως 111_2
- Για κάθε υποδίκτυο θα πρέπει να πάρουμε όλες τις πιθανές τιμές στο τμήμα υπολογιστή δηλ. από 00000_2 ως 11111_2
- Σε κάθε υποδίκτυο, η πρώτη διεύθυνση είναι η διεύθυνση υποδικτύου και η τελευταία η εκπομπής. **Δεν χρειάζεται να κάνουμε έξτρα υπολογισμούς**
- Όπως φαίνεται στο παράδειγμα, όταν η μάσκα δεν έχει τις “προφανείς” τιμές 0 ή 255, οι διευθύνσεις δικτύου/εκπομπής επίσης δεν είναι προφανείς και χρειάζονται υπολογισμό από το δυαδικό. Δώστε προσοχή στις πράξεις!

Ο πίνακας είναι ο παρακάτω:

Α/Α	1η οκτάδα	2η οκτάδα	3η οκτάδα	4η οκτάδα		Διευθύνσεις
0	11000000	10101000	00000011	000	00000	192.168.3.0
	11000000	10101000	00000011		11111	192.168.3.31
1	11000000	10101000	00000011	001	00000	192.168.3.32
	11000000	10101000	00000011		11111	192.168.3.63
2	11000000	10101000	00000011	010	00000	192.168.3.64
	11000000	10101000	00000011		11111	192.168.3.95
3	11000000	10101000	00000011	011	00000	192.168.3.96
	11000000	10101000	00000011		11111	192.168.3.127
4	11000000	10101000	00000011	100	00000	192.168.3.128
	11000000	10101000	00000011		11111	192.168.3.159
5	11000000	10101000	00000011	101	00000	192.168.3.160
	11000000	10101000	00000011		11111	192.168.3.191
6	11000000	10101000	00000011	110	00000	192.168.3.192
	11000000	10101000	00000011		11111	192.168.3.223
7	11000000	10101000	00000011	111	00000	192.168.3.224
	11000000	10101000	00000011		11111	192.168.3.255

Στη στήλη A/A φαίνεται ο αύξοντας αριθμός του υποδικτύου (είναι ο αριθμός που αντιστοιχεί στο Subnet_ID αλλά στο δεκαδικό). Οι υπολογιστές του κάθε υποδικτύου έχουν κοινές ολόκληρες τις τρεις πρώτες οκτάδες (το Network_ID όπου η μάσκα έχει τιμή 255) και τα τρία πρώτα ψηφία της τέταρτης οκτάδας (που ανήκουν στο Subnet_ID).

Η πρώτη διεύθυνση του πρώτου υποδικτύου είναι 192.168.3.0 και αποτελεί τη διεύθυνση δικτύου για το υποδίκτυο αυτό. Αντίστοιχα η τελευταία διεύθυνση, 192.168.3.31, αποτελεί την διεύθυνση εκπομπής του υποδικτύου. Το ίδιο ισχύει και για τα υπόλοιπα υποδίκτυα. Σε κάθε υποδίκτυο υπάρχουν 32 διευθύνσεις, αλλά για υπολογιστές μπορούμε να χρησιμοποιήσουμε 30 (χάνουμε δύο εξαιτίας των διευθύνσεων δικτύου/εκπομπής).

Παράδειγμα 2

Δίνεται η διεύθυνση δικτύου 192.168.17.0/24 (μάσκα 255.255.255.0).

- Να χωριστεί το δίκτυο σε υποδίκτυα τουλάχιστον 50 υπολογιστών
- Να δοθούν οι περιοχές διευθύνσεων του κάθε υποδικτύου
- Να δοθούν οι διευθύνσεις υποδικτύου και εκπομπής κάθε υποδικτύου
- Πόσα υποδίκτυα μπορεί να έχει το συγκεκριμένο δίκτυο;

Εργαζόμαστε με τον ίδιο τρόπο όπως προηγουμένως, μόνο που αυτή τη φορά ξεκινάμε με το πλήθος των υπολογιστών. Για να έχουμε 50 υπολογιστές, χρειαζόμαστε 6 bit στο τμήμα υπολογιστή. 2^5=32 οπότε τα 5 bit δεν επαρκούν, ενώ 2^6=64 οπότε στην πραγματικότητα το κάθε υποδίκτυο μας θα έχει 64 διευθύνσεις. Όπως και προηγουμένως, οι διευθύνσεις είναι πάντοτε δύναμη του 2, οπότε δεν μπορούμε να φτιάξουμε υποδίκτυα για 50 υπολογιστές αλλά για περισσότερους.

Από αυτές τις 64 διευθύνσεις κάθε υποδικτύου η πρώτη θα είναι διεύθυνση δικτύου και η τελευταία εκπομπής, άρα για μηχανήματα κάθε υποδίκτυο θα διαθέτει 62 διευθύνσεις. Έχοντας δώσει 6 bit στο τμήμα υπολογιστή, μένουν 2 bit από την τέταρτη οκτάδα για το τμήμα υποδικτύου, οπότε θα έχουμε συνολικά 2^2=4 υποδίκτυα. Συνολικά μπορούμε σε όλα μαζί τα υποδίκτυα να συνδέσουμε 4 X 62 = 248 υπολογιστές, χάνουμε δηλ. 6 διευθύνσεις σε σχέση με την κανονική κλάση C. Σε σχέση με το προηγούμενο παράδειγμα, χάνουμε λιγότερες διευθύνσεις *γιατί έχουμε λιγότερα υποδίκτυα*.

Θα υπολογίσουμε τώρα τη νέα μάσκα δικτύου:

Διεύθυνση Δικτύου	192	168	17	0
Παλιά Μάσκα Δικτύου	255	255	255	0
	11111111	11111111	11111111	00000000
Νέα Μάσκα Υποδικτύου	11111111	11111111	11111111	11000000
	255	255	255	192

Η νέα μάσκα είναι 255.255.255.192 και σε μορφή CIDR μπορούμε να γράψουμε το δίκτυο 192.168.17.0/26. Οι διευθύνσεις των υπολογιστών είναι της μορφής

<Network_id<, <Subnet_ID>, <Host_ID>

όπου το Network_ID είναι 24 bit, το Subnet_ID είναι 2 bit και τα υπόλοιπα 6 bit ανήκουν στο Host_ID. Ο πίνακας διευθύνσεων προκύπτει ακριβώς με τον ίδιο τρόπο του προηγούμενου παραδείγματος. Οι υπολογιστές του κάθε υποδικτύου έχουν κοινές τις τρεις πρωτές οκτάδες (όπου η μάσκα έχει τιμή 255) και τα δυο πρώτα ψηφία της τέταρτης οκτάδας.

A/A	1η οκτάδα	2η οκτάδα	3η οκτάδα	4η οκτάδα		Διευθύνσεις
0	11000000	10101000	00010001	00	000000	192.168.17.0
	11000000	10101000	00010001		111111	192.168.17.63
1	11000000	10101000	00010001	01	000000	192.168.17.64
	11000000	10101000	00010001		111111	192.168.17.127
2	11000000	10101000	00010001	10	000000	192.168.17.128
	11000000	10101000	00010001		111111	192.168.17.191
3	11000000	10101000	00010001	11	000000	192.168.17.192
	11000000	10101000	00010001		111111	192.168.17.255

Εννοείται ότι σε κάθε υποδίκτυο από τα παραπάνω η πρώτη διεύθυνση που υπολογίσαμε είναι η διεύθυνση δικτύου, ενώ η τελευταία η εκπομπής του συγκεκριμένου υποδικτύου.

Παράδειγμα 3

Το παράδειγμα αυτό είναι αντίστοιχο με την “Δραστηριότητα 3η” του βιβλίου και αφορά υποδικτύωση σε δίκτυο κλάσης Β.

Δίνεται η διεύθυνση δικτύου 134.55.0.0/16 (μάσκα 255.255.0.0, κλάσης Β)

- Να χωριστεί το δίκτυο σε υποδίκτυα των 4000 υπολογιστών τουλάχιστον
- Να υπολογιστεί η νέα μάσκα υποδικτύου
- Να δοθούν οι περιοχές διευθύνσεων για τα τέσσερα πρώτα υποδίκτυα
- Να δοθούν οι διευθύνσεις δικτύου και εκπομπής για τα τέσσερα πρώτα υποδίκτυα

- Πόσα συνολικά υποδίκτυα έχει το συγκεκριμένο δίκτυο και πόσους υπολογιστές μπορούμε πραγματικά να συνδέσουμε σε κάθε υποδίκτυο;

- Πόσες διευθύνσεις χάνουμε συνολικά λόγω της υποδικτύωσης σε σχέση με το κανονικό δίκτυο κλάσης B;

Τη δεδομένη στιγμή, το δίκτυο διαθέτει 16 bit για το τμήμα δικτύου και 16 για το τμήμα υπολογιστή, δηλ. 65536 διευθύνσεις (65534 μηχανήματα). Για να έχουμε 4000 μηχανήματα, χρειαζόμαστε 12 bit γιατί 2^{12}=4096. Θα δώσουμε τα επιπλέον 4 bit από το τμήμα υπολογιστή, στο τμήμα δικτύου. Άρα:

- Με 4 bit στο τμήμα υποδικτύου μπορούμε να έχουμε συνολικά 2^4=16 υποδίκτυα

- Με 12 bit στο τμήμα υπολογιστή, θα έχουμε συνολικά 4096 διευθύνσεις σε κάθε υποδίκτυο. Από αυτές θα μπορέσουμε να δώσουμε 4096-2=4094 σε μηχανήματα

- Συνολικά χάνουμε 16 X 2 = 32 διευθύνσεις λόγω της υποδικτύωσης. Αντί για 65534 μηχανήματα, θα μπορούμε να συνδέσουμε 65504 (πολύ μικρή απώλεια σε σχέση με τα οφέλη της υποδικτύωσης)

Έχουμε απαντήσει ήδη στα δύο τελευταία ερωτήματα της άσκησης, κάνοντας μόνο τις απαραίτητες πράξεις με τα bit. Μπορούμε τώρα εύκολα να υπολογίσουμε τη νέα μάσκα υποδικτύου:

Διεύθυνση Δικτύου	134	55	0	0
Παλιά Μάσκα Δικτύου	255	255	0	0
	11111111	11111111	00000000	00000000
Νέα Μάσκα Υποδικτύου	11111111	11111111	1111 0000	00000000
	255	255	240	0

Έτσι η νέα μάσκα είναι 255.255.240.0 και σε μορφή CIDR μπορούμε να γράψουμε τη διεύθυνση δικτύου ως 134.55.0.0/20. Οι διευθύνσεις των υπολογιστών είναι πλέον της μορφής <Network_ID>, <Subnet_ID>, <Host_ID> όπου το Network_ID είναι 16 bit, το Subnet_ID είναι 4 bit και το Host_ID 12 bit.

Οι περιοχές διευθύνσεων για τα τέσσερα πρώτα υποδίκτυα, μπορούν να υπολογιστούν εύκολα και φαίνονται στον παρακάτω πίνακα. Οι υπολογιστές του κάθε υποδικτύου έχουν κοινές τις δύο πρώτες οκτάδες (το Network_ID, όπου η μάσκα έχει τιμή 255) και τα τέσσερα πρώτα ψηφία της τρίτης οκτάδας που αποτελούν το Subnet_ID.

A/A	1η οκτάδα	2η οκτάδα	3η οκτάδα		4η οκτάδα	Διευθύνσεις
0	10000110	00110111	0000	0000	00000000	134.55.0.0
	10000110	00110111		1111	11111111	134.55.15.255
1	10000110	00110111	0001	0000	00000000	134.55.16.0
	10000110	00110111		1111	11111111	134.55.31.255
2	10000110	00110111	0010	0000	00000000	134.55.32.0
	10000110	00110111		1111	11111111	134.55.47.255
3	10000110	00110111	0011	0000	00000000	134.55.48.0
	10000110	00110111		1111	11111111	134.55.63.255

Σε κάθε υποδίκτυο, η πρώτη διεύθυνση είναι η διεύθυνση δικτύου και η τελευταία η διεύθυνση εκπομπής. Έτσι π.χ. για το υποδίκτυο με A/A 0, η διεύθυνση δικτύου είναι 134.55.0.0 και η εκπομπής 134.55.15.255. Προσέξτε ότι οι 4096 διευθύνσεις προκύπτουν από συνδυασμό τιμών των δύο τελευταίων οκτάδων (δεν είναι απλά μια πρόσθεση όπως ίσως κάνατε στην κλάση C).

3.1.7 Αταξική Δρομολόγηση (CIDR), Υπερδικτύωση και Μάσκες Μεταβλητού Μήκους

Με τη χρήση μάσκας δικτύου, τα τμήματα δικτύου και υπολογιστή καθορίζονται πλέον από αυτή, άρα οι τυποποιημένες κλάσεις παύουν να έχουν σημασία. Μπορούμε δηλ. να έχουμε διευθύνσεις όπως την παρακάτω:

IP: 10.14.28.10 Mask: 255.255.255.0

Σύμφωνα με αυτά που ξέρουμε από τις κλάσεις, η παραπάνω διεύθυνση θα άνηκε σε ένα δίκτυο κλάσης A αν δεν υπήρχε η μάσκα. Όμως με τη συγκεκριμένη μάσκα, η διεύθυνση πλέον φαίνεται να αντιστοιχεί σε κλάση C. Στην πραγματικότητα, με τη χρήση της μάσκας δεν υπάρχουν πλέον κλάσεις και μπορούμε να έχουμε δίκτυα που δεν ανήκουν σε καμιά τυποποιημένη κλάση (σε αυτά η μάσκα περιέχει και τιμές διαφορετικές από 0 και 255).

Με αυτό τον τρόπο διευκολύνεται η διαδικασία της δρομολόγησης και της διαχείρισης των πινάκων δρομολόγησης από τους δρομολογητές (routers) IPv4. Όλος ο χώρος διευθύνσεων αντιμετωπίζεται ως ενιαίος και χωρίς κλάσεις από τα πρωτόκολλα δρομολόγησης. Η δρομολόγηση αυτή ονομάζεται *αταξική* ή *CIDR (Classless Internet Domain Routing)*.

Για παράδειγμα, σε μια εταιρεία με ανάγκες 1000 υπολογιστών, δεν θα δώσουμε πλέον ένα δίκτυο κλάσης B (με απώλεια των υπόλοιπων 64534 διευθύνσεων) αλλά τέσσερα συνεχόμενα δίκτυα κλάσης C. Τα δίκτυα αυτά ωστόσο θα τα αντιμετωπίζουμε ως ένα ενιαίο χώρο.

Στην προηγούμενη ενότητα, δίναμε ψηφία από το αναγνωριστικό του υπολογιστή στο αναγνωριστικό του δικτύου. Αυτό το ονομάσαμε **υποδικτύωση**. Εδώ θα δώσουμε ψηφία από το αναγνωριστικό δικτύου στο αναγνωριστικό του υπολογιστή και θα έχουμε **υπερδικτύωση**.

Στην υποδικτύωση, χωρίζουμε ένα μεγαλύτερο δίκτυο σε μικρότερα κομμάτια. Στην υπερδικτύωση φτιάχνουμε ένα μεγαλύτερο δίκτυο ενώνοντας μικρότερα. Στο παράδειγμα μας θα ενώσουμε τέσσερα δίκτυα που κανονικά θα χαρακτηρίζονταν ως κλάσης C για ένα μεγαλύτερο δίκτυο που θα διαθέτει 1024 διευθύνσεις, θα μπορεί δηλ. να συνδέσει 1022 μηχανήματα.

Για να βάλουμε 1000 μηχανήματα, θα χρειαστούμε 10 bit στο τμήμα υπολογιστή, αφού 2^{10}=1024. Άρα τα υπόλοιπα 22 bit θα αποτελέσουν το τμήμα δικτύου. Έχουμε δώσει δηλ. δύο παραπάνω bit στο τμήμα υπολογιστή σε σχέση με την τυποποιημένη κλάση C. Η νέα μας μάσκα θα είναι:

11111111.11111111.11111100.00000000 ή 255.255.252.0

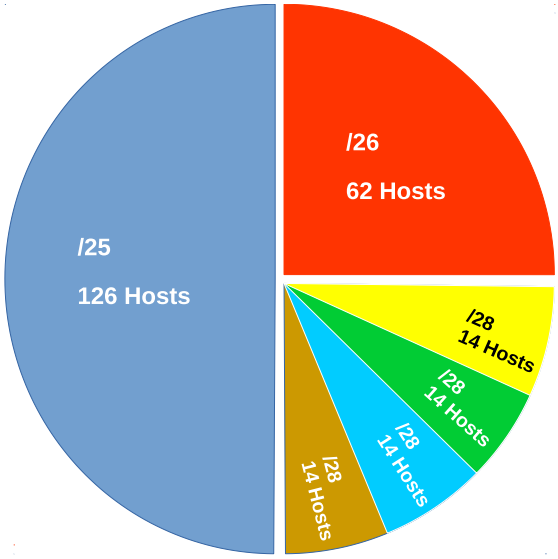
Θεωρώντας π.χ. το δίκτυο 194.75.128.0/22, θα έχουμε τις παρακάτω διευθύνσεις:

Α/Α	1η οκτάδα	2η οκτάδα	3η οκτάδα		4η οκτάδα	Διευθύνσεις
ΔΥ	11000010	01001011	100000	00	00000000	194.75.128.0
	11000010	01001011		11	11111111	194.75.131.255

Σημείωση: Το παράδειγμα του βιβλίου χρησιμοποιεί διεύθυνση τύπου 192.X.X.X η οποία καθώς ξέρουμε χρησιμοποιείται για ιδιωτικά δίκτυα και δεν θα μας δίνονταν ποτέ ως περιοχή διευθύνσεων από IANA/ICANN.

Δεν τίθεται εδώ θέμα υποδικτύωσης. Το δίκτυο είναι ενιαίο και είναι το 194.75.128.0/22. Η διεύθυνση δικτύου είναι 194.75.128.0 (το τμήμα υπολογιστή – Host_ID – έχει όλα τα ψηφία μηδέν) και η διεύθυνση εκπομπής 194.75.131.255 (το τμήμα υπολογιστή έχει όλα τα ψηφία ένα. Όπως και προηγουμένως, είναι αντίστοιχα η πρώτη και τελευταία διεύθυνση σε αυτές που υπολογίσαμε).

Στην περίπτωση της υποδικτύωσης που εξετάσαμε στην προηγούμενη ενότητα, έχουμε επιπλέον και τη δυνατότητα να μοιράσουμε ένα υποδίκτυο σε περισσότερα. Για παράδειγμα φανταστείτε ένα δίκτυο 192.168.0.0/24 δηλ. με 256 διευθύνσεις (254 υπολογιστές). Μπορούμε να το χωρίσουμε σε δύο υποδίκτυα με πρόθεμα /25 και 128 διευθύνσεις το καθένα (126 υπολογιστές). Από τα υποδίκτυα αυτά μπορούμε να επιλέξουμε να χωρίσουμε το ένα σε δύο επιπλέον υποδίκτυα με πρόθεμα /26 και 64 διευθύνσεις (62 υπολογιστές) κ.ο.κ. (δείτε το σχήμα 3.3). Καθώς έχουμε πολλαπλά υποδίκτυα που προκύπτουν από τον περαιτέρω διαχωρισμό άλλων υποδικτύων



Σχήμα 3.3: *Υποδικτύωση με VLSM*

(δηλ. υποδικτύωση υποδικτύων), οι μάσκες που χρησιμοποιούμε έχουν μεταξύ τους διαφορετικό μήκος και ονομάζονται *VLSM, Variable Length Subnet Masking, Μεταβλητού Μήκους Μάσκες Υποδικτύωσης*.

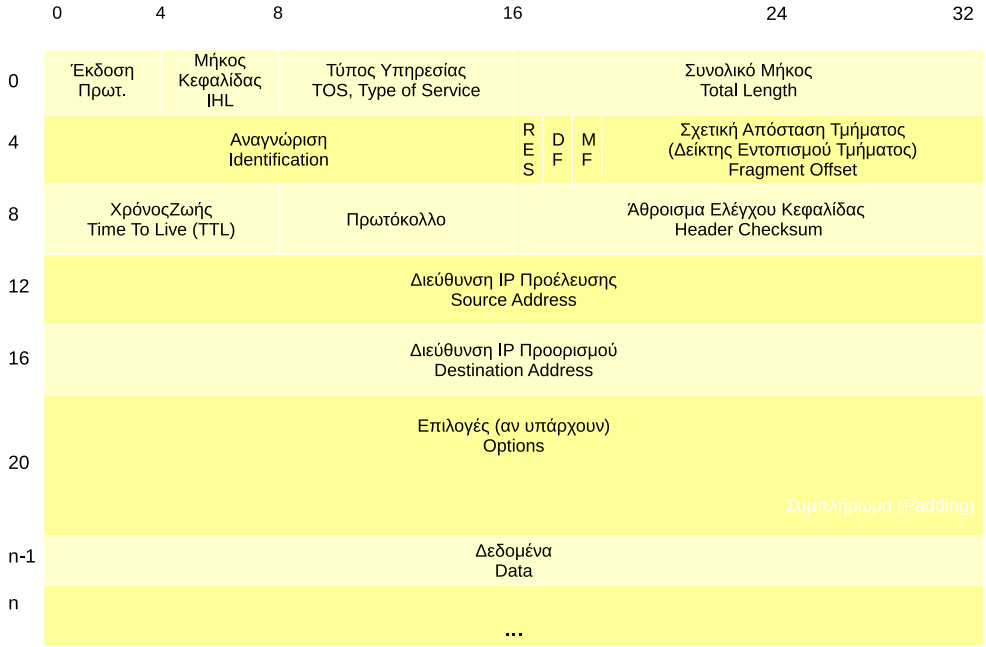
3.2 Το Αυτοδύναμο Πακέτο IP (Datagram) – Δομή Πακέτου

Το *πρωτόκολλο διαδικτύου (Internet Protocol – IP)* ενθυλακώνει τα πακέτα δεδομένων που του προωθούνται από το ανώτερο επίπεδο (μεταφοράς) σε *αυτοδύναμα πακέτα (datagrams)*. Τυπικά, το επίπεδο μεταφοράς προωθεί είτε τμήματα TCP (TCP Segments) είτε αυτοδύναμα πακέτα UDP (UDP Datagrams) – θα τα εξετάσουμε σε επόμενο κεφάλαιο. Το IP προσθέτει στη δική του επικεφαλίδα πεδία που περιέχουν όλες τις απαραίτητες διαχειριστικές πληροφορίες ώστε να γίνει δυνατή η εύρεση του προορισμού και η επιτυχής δρομολόγηση του πακέτου από τα πρωτόκολλα δρομολόγησης.

Τα πιο σημαντικά πεδία είναι η *Διεύθυνση IP Προέλευσης (Source IP)* και η *Διεύθυνση IP Προορισμού (Destination IP)* με μήκος 32 bit η κάθε μία (στην έκδοση IPv4).

Μπορείτε να δείτε την δομή του πρωτοκόλλου IP στο σχήμα 3.4. Θα αναλύσουμε

τα σημαντικότερα πεδία:



Σχήμα 3.4: *Δομή Αυτοδύναμου Πακέτου IP*

- **Έκδοση Πρωτοκόλλου:** Το πεδίο αυτό έχει μέγεθος 4 bit και δηλώνει την έκδοση του πρωτοκόλλου IP που χρησιμοποιείται. Έχει τις τιμές 4 για IPv4 και 6 για IPv6. Αν χρησιμοποιείται IPv6, η επικεφαλίδα έχει ελάχιστο μήκος 40 bytes.
- **Μήκος Επικεφαλίδας:** Το πεδίο αυτό είναι μήκους 4 bit και εκφράζει το μήκος της επικεφαλίδας σε λέξεις των 32 bit. Έτσι αν έχει τιμή 5, η επικεφαλίδα είναι 32X5=160 bit και άρα 160/8=20 bytes. Μπορείτε επίσης να πολλαπλασιάσετε την τιμή του πεδίου αυτού με το 4 για να βρείτε απευθείας το μήκος της επικεφαλίδας σε bytes.

Προσέξτε ότι στις ασκήσεις άλλες φορές δίνεται το μήκος της επικεφαλίδας σε bytes (π.χ. 20 bytes) και άλλες **η τιμή του πεδίου "μήκος επικεφαλίδας"** οπότε πρέπει να πολλαπλασιάσουμε με το 4 για να βρούμε τα bytes της επικεφαλίδας.

Το ελάχιστο μήκος επικεφαλίδας είναι 5 λέξεις των 32 bit ή 20 bytes και το μέγιστο 15 λέξεις ή 60 bytes (4X15).

- **Τύπος Υπηρεσίας:** Το πεδίο αυτό έχει μήκος 8 bit και περιγράφει τον επιθυμητό χειρισμό του πακέτου από κάθε κόμβο που θα περάσει. Μπορεί να δίνεται προτεραιότητα στην ταχύτητα, εάν δηλ. επιτρέπεται να καθυστερήσει ή όχι, στην αξιοπιστία ή στο ρυθμό διακίνησης (throughput). Με νεώτερη αναθεώρηση, το RFC2474 αλλάζει τη σημασία του συγκεκριμένου πεδίου ώστε να υποστηρίζει ένα σύνολο διαφοροποιημένων υπηρεσιών που ονομάζει *Differentiated Services Code Point - DSCP (6 bit)*. Τα υπόλοιπα 2 bit χαρακτηρίζονται από το RFC3168 ως ρητή ειδοποίηση συμφόρησης, *Explicit Congestion Notification, ECN*. Οι αλλαγές αυτές έγιναν με σκοπό να υποστηρίξουν νέες υπηρεσίες με ιδιαίτερες απαιτήσεις όπως η μεταφορά φωνής μέσω VoIP. Για να είναι εφικτό αυτό, πρέπει οι υπηρεσίες να υποστηρίζονται και από το υπόλοιπο δίκτυο.

- **Συνολικό Μήκος:** Το πεδίο αυτό έχει μέγεθος 16 bit και δηλώνει το συνολικό μήκος (επικεφαλίδα και δεδομένα) του πακέτου σε bytes. Η ελάχιστη τιμή που μπορεί να πάρει είναι 20 (αντιπροσωπεύει ένα πακέτο με μόνο το βασικό, σταθερό τμήμα της επικεφαλίδας χωρίς καθόλου δεδομένα) και η μέγιστη 65535 (τιμή που αντιστοιχεί σε 16 άσους). Αυτό σημαίνει ότι το *μέγιστο μέγεθος του αυτοδύναμου πακέτου IP* στο IPv4 είναι 65535 bytes (πρακτικά, 64 Kbyte).

- **Αναγνώριση:** Καθώς το πακέτο IP κινείται προς τον προορισμό του, ενδέχεται να περάσει από αρκετά ενδιάμεσα δίκτυα.Το μέγιστο μήκος δεδομένων που μπορεί να μεταδοθεί σε ένα πλαίσιο από το επίπεδο ζεύξης δεδομένων ενός δικτύου, είναι γνωστό με την ονομασία *MTU, Maximum Transfer Unit*. Έτσι, για παράδειγμα το Ethernet έχει MTU 1500 bytes (κάθε πλαίσιο Ethernet μπορεί να μεταδώσει μέχρι 1500 bytes δεδομένων). Διαφορετικοί τύποι δικτύων έχουν άλλο MTU. Ένα πακέτο IP ενδέχεται να έχει μέγεθος τέτοιο που να μην μπορεί να μεταδοθεί από ένα ενδιάμεσο δίκτυο χωρίς να διασπαστεί περισσότερο.

  Στην περίπτωση αυτή, αν το πακέτο επιτρέπεται να διασπαστεί, θα χωριστεί σε τμήματα που ονομάζονται *fragments*. Η διαδικασία είναι γνωστή ως *διάσπαση ή κατάτμηση (IP Fragmentation)*. Όταν τα τμήματα φτάσουν στο προορισμό τους θα πρέπει να επανασυνδεθούν για να σχηματίσουν ξανά το αρχικό πακέτο IP. Καθώς στον παραλήπτη μπορεί να φτάνουν τμήματα από πακέτα IP που προέρχονται από διαφορετικές επικοινωνίες, το πεδίο *Αναγνώριση* περιέχει ένα αριθμό που χρησιμοποιείται για να αναγνωριστούν ποια τμήματα ανήκουν σε κάθε πακέτο: όλα τα τμήματα που προέρχονται από τη διάσπαση ενός συγκεκριμένου πακέτου έχουν τον ίδιο αριθμό αναγνώρισης στην επικεφαλίδα τους.

- **Σχετική Θέση Τμήματος ή Δείκτης Εντοπισμού Τμήματος:** Και αυτό το πεδίο (όπως και η Αναγνώριση) χρησιμοποιείται στην περίπτωση που έχουμε

διάσπαση. Χρησιμοποιείται για να μπουν ξανά τα fragments στη σωστή σειρά στον υπολογιστή προορισμού. Το πεδίο έχει μέγεθος 13 bits και ο αριθμός που περιέχει εκφράζει την απόσταση του τμήματος από το πρώτο σε οκτάδες (8x) byte. Η σχετική θέση τμήματος είναι πάντοτε μηδέν στο πρώτο τμήμα. Στα επόμενα τμήματα, την υπολογίζουμε διαιρώντας τα καθαρά δεδομένα (χωρίς επικεφαλίδα) που έχουν μεταδοθεί μέχρι εκείνη τη στιγμή με το οκτώ.

Για παράδειγμα, αν διασπάσουμε ένα πακέτο συνολικού μήκους 1500 bytes σε δίκτυο με MTU 500 bytes:

- Τα δεδομένα του αρχικού πακέτου είναι 1500 bytes - 20 bytes επικεφαλίδα = 1480 bytes.
- Το πρώτο τμήμα θα έχει Σχετική Θέση Τμήματος μηδέν και συνολικό μήκος 500 bytes. Από αυτά, τα 20 είναι επικεφαλίδα. Συνολικά θα μεταδώσουμε 480 bytes καθαρών δεδομένων.
- Το δεύτερο τμήμα θα έχει Σχετική Θέση Τμήματος 480/8 = 60 (τα δεδομένα που μεταδώσαμε στο πρώτο fragment δια οκτώ) και θα είναι επίσης 500 bytes συνολικό μήκος. Θα περιέχει επίσης 480 bytes δεδομένων.
- Το τρίτο τμήμα θα έχει Σχετική Θέση Τμήματος 960/8 = 120 (ή 2X60) και συνολικό μήκος 500 bytes. Θα περιέχει 480 bytes δεδομένων.
- Για το τέταρτο και τελευταίο τμήμα έχουν μείνει 40 bytes δεδομένων, αφού έχουμε ήδη μεταδώσει 3X480=1440 bytes. Το συνολικό μήκος είναι 60 bytes και η Σχετική Θέση Τμήματος είναι 1440/8=180 (ή 3X60).

Το σχολικό βιβλίο γράφει τον παρακάτω τύπο για τον υπολογισμό της σχετικής θέσης τμήματος:

Fragment_offset = n * INT((MTU - IHL * 4) / 8)

όπου το n συμβολίζει τον αριθμό του fragment (μηδέν για το πρώτο fragment) και το IHL το πεδίο “μήκος επικεφαλίδας” (με τιμή 5 για επικεφαλίδα 20 bytes). Πρακτικά, ο τύπος σημαίνει τα παρακάτω:

- Το πρώτο fragment έχει σχετική θέση τμήματος μηδέν (για n=0).
- Για το δεύτερο fragment (n=1), η σχετική θέση τμήματος είναι τα καθαρά δεδομένα (χωρίς επικεφαλίδα) που μεταδώσαμε στο πρώτο fragment δια οκτώ.
- Για τα επόμενα fragment, η σχετική θέση τμήματος είναι πολλαπλάσιο αυτής που υπολογίσαμε στο δεύτερο τμήμα (Για n>=2).

  - Αν στη σχετική θέση τμήματος δεν προκύπτει ακέραια τιμή, αποκόπτουμε τα δεκαδικά. Σε αυτή την περίπτωση όμως **θα πρέπει να υπολογίσουμε ξανά τα δεδομένα που μεταδόθηκαν, καθώς δεν είναι αυτά που υποθέσαμε αρχικά**. Θα δούμε σχετικό παράδειγμα στο τέλος της ενότητας.

Δεν χρειάζεται στην πραγματικότητα να μάθετε ή να αποστηθίσετε τον τύπο!

- **Το πεδίο DF:** Το πεδίο αυτό έχει μέγεθος 1 bit και είναι στην πραγματικότητα μια σημαία που δείχνει αν το πακέτο επιτρέπεται ή όχι να διασπαστεί *(DF: Don't Fragment, Απαγόρευση Διάσπασης)*. Αν για κάποιο λόγο το αυτοδύναμο πακέτο δεν πρέπει να διασπαστεί, το πεδίο αυτό θα έχει τιμή 1. Έτσι κατά τη δρομολόγηση του πακέτου θα επιλεχθεί διαδρομή τέτοια ώστε να μη χρειάζεται διάσπαση, ή, αν αυτό είναι αδύνατο, το πακέτο θα απορριφθεί (και ενδεχομένως να ειδοποιηθεί ο αποστολέας για αυτό το γεγονός). Στην έκδοση IPv6 η διάσπαση του πακέτου διενεργείται μόνο από τον υπολογιστή προέλευσης με βάση το μικρότερο MTU της διαδρομής (Path MTU, PMTU) και όχι από τους ενδιάμεσους δρομολογητές.

- **Το πεδίο MF:** Όταν ένα αυτοδύναμο πακέτο διασπαστεί σε τμήματα, αυτά φτάνουν με τυχαία σειρά στον παραλήπτη. Είναι πολύ εύκολο για τον παραλήπτη να βρει ποιο είναι το πρώτο fragment (είναι αυτό που έχει σχετική θέση τμήματος μηδέν). Από τη σχετική θέση τμήματος μπορούν επίσης να μπουν όλα τα επόμενα τμήματα στη σωστή σειρά αλλά δεν μπορούμε να γνωρίζουμε ποιο είναι το τελευταίο. Για αυτό το σκοπό χρησιμοποιείται η σημαία MF *(More Fragments, Περισσότερα Τμήματα)*. Σε όλα τα τμήματα έχει τιμή 1, εκτός από το τελευταίο που έχει τιμή μηδέν, σηματοδοτώντας έτσι το τέλος των τμημάτων του συγκεκριμένου αυτοδύναμου πακέτου.

- **Το πεδίο Χρόνος ζωής (TTL, Time To Live):** Το πεδίο αυτό έχει μήκος 8 bit. Ξεκινά από τον αποστολέα με μια αρχική τιμή (συνήθως 64) και μειώνεται κατά 1 σε κάθε δρομολογητή από τον οποίο διέρχεται το πακέτο. Όταν η τιμή του πεδίου γίνει μηδέν, το πακέτο καταστρέφεται και επιστρέφεται στον αποστολέα διαγνωστικό μήνυμα σφάλματος υπέρβασης χρόνου ζωής (time exceeded). Κάθε φορά που το πακέτο διέρχεται από ένα δρομολογητή, λέμε ότι έχουμε μια *αναπήδηση (hop)*. Το πεδίο αυτό μπορεί να χαρακτηριστεί ως ανάστροφος μετρητής αναπηδήσεων (αφού μειώνεται σε κάθε αναπήδηση). Λειτουργεί ως όριο απόρριψης ενός πακέτου όταν αυτό έχει καθυστερήσει, έχει χαθεί στη διαδρομή, έχει λάθος διεύθυνση παραλήπτη ή για κάποιο άλλο λόγο περιφέρεται άσκοπα στο δίκτυο χωρίς να μπορεί να παραδοθεί. Χωρίς αυτό το πεδίο, σύντομα το Internet θα πλημμύριζε από προβληματικά πακέτα που δεν θα μπορούσαν να παραδοθούν και θα σταματούσε να λειτουργεί!

Το πεδίο αυτό χρησιμοποιείται επίσης με έξυπνο τρόπο στην εντολή **traceroute ή tracert**. Πρόκειται για μια διαγνωστική εντολή που μας επιτρέπει να δούμε την διαδρομή που ακολουθούν τα πακέτα μέχρι ένα προορισμό. Ένα παράδειγμα εκτέλεσης της φαίνεται παρακάτω:

```
[09:15:17][sonic@pegasus:~]$ traceroute freebsdworld.gr
traceroute to freebsdworld.gr (193.183.99.68), 64 hops max, 40 byte packets
 1  router (192.168.0.250)  0.632 ms  0.879 ms  0.710 ms
 2  80.107.108.106 (80.107.108.106)  6.730 ms  8.669 ms  10.213 ms
 3  79.128.226.245 (79.128.226.245)  11.123 ms  11.170 ms
    79.128.227.213 (79.128.227.213)  11.505 ms
 4  62.75.3.157 (62.75.3.157)  12.009 ms
    kolasr02-hu-0-8-0-0.ath.OTEGlobe.gr (62.75.3.17)  11.596 ms
    kolasr02-hu-0-1-0-0.ath.OTEGlobe.gr (62.75.3.137)  11.286 ms
 5  62.75.4.162 (62.75.4.162)  58.291 ms  57.891 ms
    62.75.4.114 (62.75.4.114)  58.056 ms
 6  xe-7-1-1.edge5.London1.Level3.net (195.50.118.169)  58.150 ms  57.645 ms
    xe-7-3-0.edge5.London1.Level3.net (212.187.138.117)  57.233 ms
 7  ae-122-3508.bar2.Milan1.Level3.net (4.69.159.126)  77.716 ms  78.636 ms
    ae-120-3506.bar2.Milan1.Level3.net (4.69.159.118)  79.893 ms
 8  212.73.241.130 (212.73.241.130)  78.258 ms  78.423 ms  78.586 ms
 9  217.171.38.134 (217.171.38.134)  78.732 ms  78.130 ms  79.205 ms
10  zms.gudgenet.com (193.183.99.68)  79.799 ms  79.910 ms  79.773 ms
```

Η εντολή δουλεύει ως εξής: Αρχικά στέλνει ένα πακέτο προς τον προορισμό που έχουμε επιλέξει με TTL 1. Το πακέτο αυτό καταστρέφεται στον πρώτο δρομολογητή ο οποίος μας επιστρέφει διαγνωστικές πληροφορίες που εμφανίζονται από την traceroute. Έπειτα στέλνεται άλλο πακέτο με TTL 2 το οποίο καταστρέφεται στο δεύτερο δρομολογητή κ.ο.κ. Αυξάνοντας συνέχεια το TTL μπορούμε να ανιχνεύσουμε όλη τη διαδρομή που ακολουθεί το πακέτο μέχρι τον προορισμό.

- **Το πεδίο Πρωτόκολλο:** Το πεδίο αυτό έχει μήκος 8 bit. Περιέχει μια αριθμητική τιμή που δηλώνει από ποιο πρωτόκολλο του αμέσως ανώτερου επιπέδου (μεταφοράς) προέρχονται τα δεδομένα που μεταφέρει το συγκεκριμένο IP πακέτο. Έτσι, πληροφορείται το πρωτόκολλο IP στον παραλήπτη προκειμένου να παραδώσει τα δεδομένα στο αντίστοιχο πρωτόκολλο του επιπέδου μεταφοράς. Για παράδειγμα, αν η τιμή είναι 6 τα δεδομένα προέρχονται από το TCP, ενώ αν είναι 17 από το UDP. Καθώς φαντάζεστε υπάρχουν πολλά περισσότερα πρωτόκολλα στο επίπεδο μεταφοράς εκτός από τα δύο βασικά (TCP, UDP). Μπορείτε να δείτε μια λίστα των πιθανών τιμών και αντίστοιχων πρωτοκόλλων για αυτό το πεδίο στο σχετικό λήμμα της Wikipedia. Ακόμα μπορείτε να δείτε τα περιεχόμενα του αρχείου /etc/protocols σε οποιοδήποτε υπολογιστή UNIX/Linux ή το αρχείο C:\Windows\System32\drivers\etc\protocols σε υπολογιστή Windows.

- **Το πεδίο Άθροισμα Ελέγχου Επικεφαλίδας (Header Checksum):** Πρόκειται για ένα πεδίο μήκους 16 bit. Το πεδίο διασφαλίζει την ακεραιότητα δε-

δομένων της επικεφαλίδας, αποθηκεύοντας ένα άθροισμα ελέγχου που προκύπτει από όλα τα υπόλοιπα πεδία της (το ίδιο το πεδίο δεν συμμετέχει στο άθροισμα, θεωρώντας ότι περιέχει τιμή μηδέν). Το άθροισμα ελέγχου αναφέρεται μόνο στην επικεφαλίδα και όχι στα δεδομένα. Καθώς το πακέτο περνάει από διάφορους δρομολογητές, κάποια πεδία της επικεφαλίδας αλλάζουν, έτσι θεωρείται αναγκαία η ύπαρξη πεδίου ελέγχου για να αποφευχθούν λάθη.

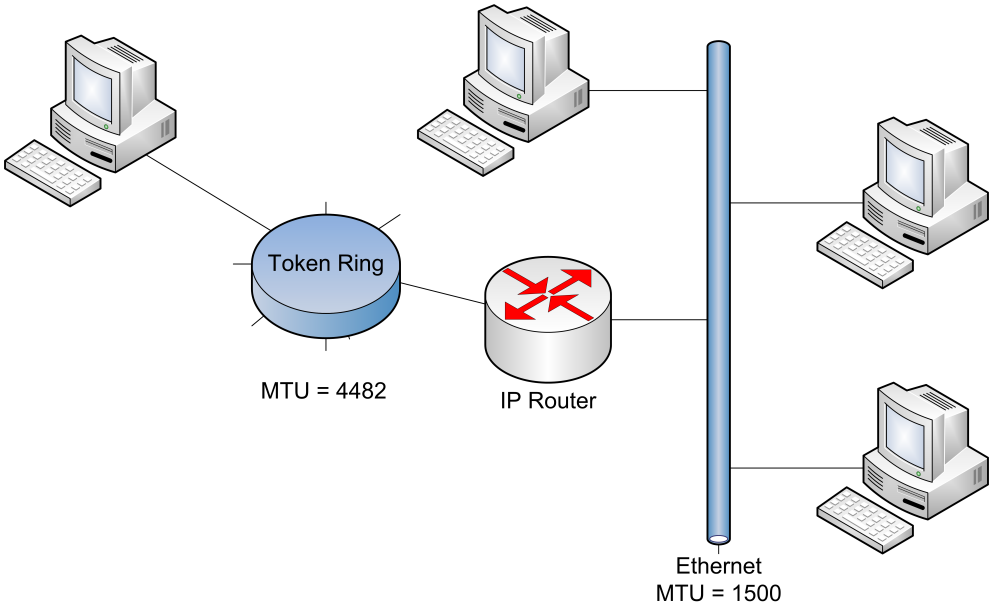
- **Το πεδίο Επιλογές (Options):** Είναι προαιρετικό και όταν χρησιμοποιείται, προφανώς η επικεφαλίδα μας είναι μεγαλύτερη από τη βασική των 20 bytes. Χρησιμοποιείται για ειδικές λειτουργίες, όχι όμως συχνά. Αν χρειάζεται, μαζί με τις Επιλογές, χρησιμοποιείται και το πεδίο **Συμπλήρωμα (padding)** το οποίο συμπληρώνει το πεδίο με μηδενικά ώστε η επικεφαλίδα να είναι πάντοτε ακέραιο πολλαπλάσιο των 32 bit.

Παράδειγμα Κατάτμησης Αυτοδύναμου Πακέτου IP

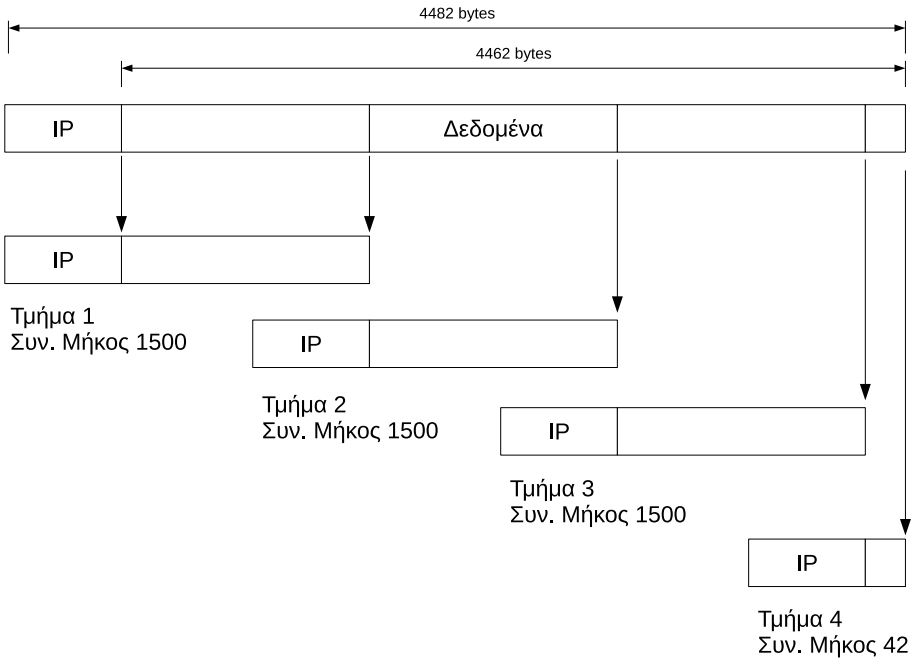
Έστω ότι έχουμε ένα αυτοδύναμο πακέτο IP το οποίο προέρχεται από ένα δίκτυο Token Ring (δακτυλίου με κουπόνι πρόσβασης) και πρόκειται να παραδοθεί σε ένα υπολογιστή προορισμού ο οποίος βρίσκεται σε δίκτυο Ethernet (σχήμα 3.5).Τα δύο αυτά δίκτυα ενώνονται μεταξύ τους με ένα δρομολογητή IP. Το δίκτυο δακτυλίου έχει MTU = 4482 bytes, δηλ. το πλαίσιο του (επίπεδο 2) μπορεί να μεταφέρει 4482 bytes δεδομένων, ενώ στο Ethernet γνωρίζουμε ότι το MTU = 1500 bytes. Είναι φανερό ότι ένα πακέτο IP του Token Ring δεν μπορεί να μεταδοθεί χωρίς να υποστεί κατάτμηση. Η δημιουργία των τμημάτων γίνεται στο δρομολογητή, εφόσον βέβαια το πεδίο DF έχει τιμή μηδέν. Θα περιγράψουμε εδώ τη διαδικασία διάσπασης.

- Το αρχικό πακέτο IP στο Token Ring έχει συνολικό μέγεθος 4482 bytes. Η επικεφαλίδα του είναι 20 bytes και περιέχει 4462 bytes δεδομένων.
- Για να περάσει από το Ethernet θα πρέπει να διασπαστεί σε κομμάτια όχι μεγαλύτερα των 1500 bytes μαζί με την επικεφαλίδα. Κάθε τέτοιο κομμάτι θα περιέχει 1480 bytes δεδομένων.
- Η Σχετική Θέση Τμήματος για το πρώτο τμήμα είναι μηδέν. Υπολογίζουμε τη Σχετική Θέση Τμήματος για το δεύτερο τμήμα διαιρώντας τα καθαρά δεδομένα του πρώτου με το οκτώ. 1480/8=185. Από τη διαίρεση προκύπτει ακέραιος αριθμός. **Επειδή δεν προκύπτουν δεκαδικά, τα τμήματα (εκτός από το τελευταίο) θα περιέχουν 1480 bytes δεδομένων όπως υποθέσαμε αρχικά.**

Πόσα τμήματα θα έχουμε; Στα πρώτα τρία τμήματα μεταδίδουμε 1480 bytes δεδομένων και απομένουν 22 bytes ακόμα για το τελευταίο, τέταρτο τμήμα. Το συνολικό



Σχήμα 3.5: *Δίκτυα με Διαφορετικό MTU*



Σχήμα 3.6: *Κατάτμηση Αυτοδύναμου Πακέτου IPv4*

μέγεθος για καθένα από τα τρία πρώτα τμήματα είναι 1500 bytes ενώ του τέταρτου 42 bytes. Η κατάτμηση φαίνεται στο σχήμα 3.6. Το πεδίο “Σχετική Θέση Τμήμα-

τος" είναι μηδέν για το πρώτο τμήμα, 185 για το δεύτερο, 2X185=370 για το τρίτο, 3X185=555 για το τέταρτο τμήμα. Το πεδίο MF έχει τιμή 1 για όλα τα τμήματα εκτός του τελευταίου που έχει τιμή μηδέν.

Το σχολικό βιβλίο εφαρμόζει και πάλι τον τύπο, που δεν χρειάζεται να μάθετε!

Όλα τα τμήματα του αρχικού πακέτου έχουν τον ίδιο αριθμό στο πεδίο "Αναγνώριση". Ο παραλήπτης χρησιμοποιεί τα πεδία MF και Σχετική Θέση Τμήματος για να βάλει τα τμήματα στη σωστή σειρά και να συναρμολογήσει ξανά το αρχικό αυτοδύναμο IP πακέτο. Τα τμήματα μπορεί να φτάσουν στον παραλήπτη με οποιαδήποτε σειρά. Παρακάτω δίνουμε τον πίνακα με τα πεδία για το κάθε τμήμα:

	1ο Τμήμα	2ο Τμήμα	3ο Τμήμα	4ο Τμήμα
Πεδίο Μήκος Επικεφαλίδας (Λέξεις των 32 bit)	5	5	5	5
Συνολικό Μήκος (Bytes)	1500	1500	1500	42
Μήκος Δεδομένων (Bytes)	1480	1480	1480	22
Αναγνώριση	0x2b41	0x2b41	0x2b41	0x2b41
DF (Σημαία)	0	0	0	0
MF (Σημαία)	1	1	1	0
Σχετική Θέση Τμήματος (Οκτάδες Byte)	0	185	370	555

Παράδειγμα Κατάτμησης Αυτοδύναμου Πακέτου IP #2

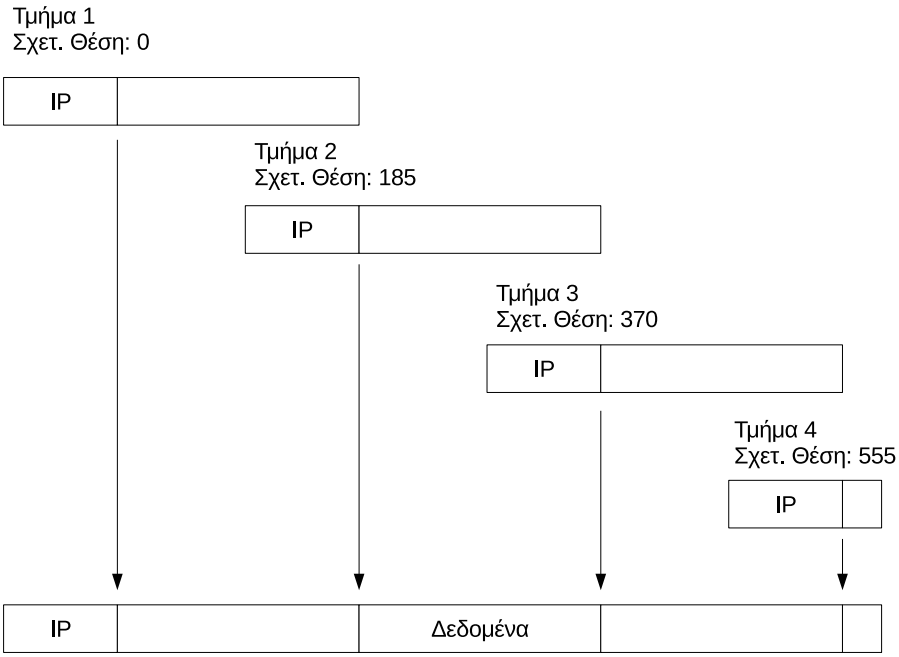
Στο παράδειγμα αυτό θα δούμε τι συμβαίνει αν κατά τον υπολογισμό της Σχετικής Θέσης Τμήματος προκύψει αριθμός με δεκαδικά ψηφία.

Ένα αυτοδύναμο πακέτο με συνολικό μέγεθος 2400 bytes, DF=0 και Αναγνώριση 0x2a28 πρόκειται να διέλθει από δίκτυο το οποίο υποστηρίζει πακέτα συνολικού μεγέθους 1000 bytes (σχήμα 3.8).

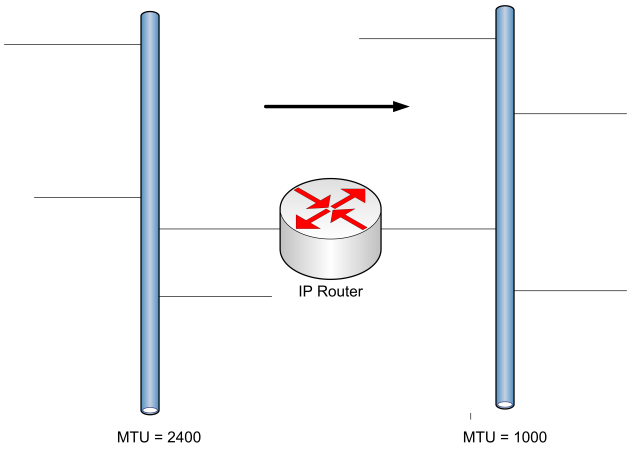
1. Θα γίνει κατάτμηση του πακέτου;
2. Αν ναι, δώστε τον πίνακα με τις τιμές των πεδίων Μήκος Επικεφαλίδας, Συνολικό Μήκος, Αναγνώριση, DF, MF και Σχετική Θέση Τμήματος (Offset)

Στο πρώτο ερώτημα, η απάντηση είναι ναι, γιατί το πακέτο έχει DF=0 άρα η κατάτμηση επιτρέπεται.

Για το δεύτερο ερώτημα, ξέρουμε ότι το δίκτυο προορισμού υποστηρίζει πακέτα συνολικού μήκους 1000 bytes. Υποθέτουμε λοιπόν ότι το πακέτο μας θα γίνει τμήματα



Σχήμα 3.7: *Επανασύνθεση Πακέτου Από Τμήματα*



Σχήμα 3.8: *Δίκτυα με Διαφορετικό MTU*

των 1000 bytes συνολικά. Το κάθε τμήμα όμως έχει 20 bytes επικεφαλίδα, άρα το μήκος δεδομένων του κάθε τμήματος θα είναι:

$$1000 - 20 = 980 \text{ bytes}$$

Η Σχετική Θέση Τμήματος για το πρώτο τμήμα είναι μηδέν. Για το δεύτερο τμήμα

θα είναι:

$$980 / 8 = 122.5$$

Όμως η Σχετική Θέση Τμήματος δεν μπορεί να έχει δεκαδικά καθώς το μήκος δεδομένων του τμήματος διαιρείται πάντα ακριβώς με το οκτώ! Αποκόπτοντας τα δεκαδικά, προκύπτει ότι η Σχετική Θέση Τμήματος για το δεύτερο τμήμα θα είναι 122.

Αυτό όμως σημαίνει ότι δεν μεταδώσαμε τελικά 980 bytes δεδομένων στο πρώτο τμήμα, **αλλά 122 X 8 = 976 bytes**. Όλα τα τμήματα μας θα έχουν αυτό το μήκος δεδομένων – εκτός ενδεχομένως από το τελευταίο που θα είναι μικρότερο. Μπορούμε τώρα να φτιάξουμε τον πίνακα με τις τιμές των πεδίων του προβλήματος:

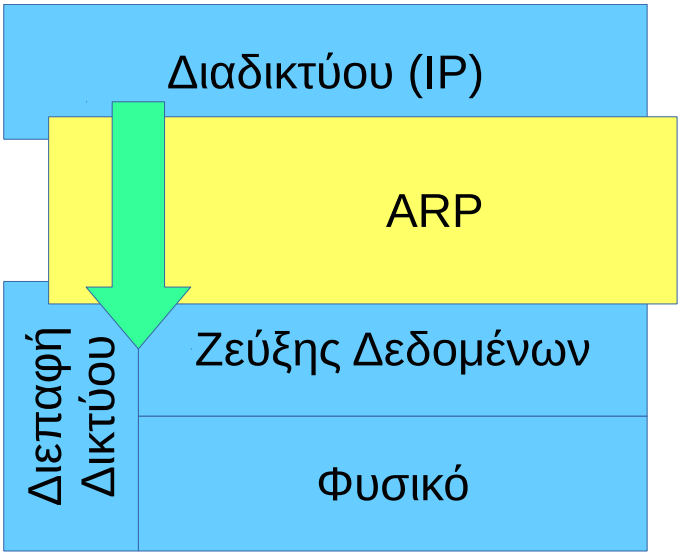
	1ο Τμήμα	2ο Τμήμα	3ο Τμήμα
Πεδίο Μήκος Επικεφαλίδας (Λέξεις των 32 bit)	5	5	5
Συνολικό Μήκος (Bytes)	996	996	448
Μήκος Δεδομένων (Bytes)	976	976	428
Αναγνώριση	0x2a28	0x2a28	0x2a28
DF (Σημαία)	0	0	0
MF (Σημαία)	1	1	0
Σχετική Θέση Τμήματος (Οκτάδες Byte)	0	122	244

Για επιπλέον παραδείγματα, κατεβάστε επίσης τη Συνοπτική Μεθοδολογία Ασκήσεων IP Fragmentation.

3.3 Πρωτόκολλα Ανεύρεσης και Απόδοσης Διευθύνσεων, Address Resolution Protocol (ARP) και Dynamic Host Configuration Protocol (DHCP)

Όπως έχουμε δει μέχρι τώρα, το κάθε επίπεδο παραλαμβάνει τα δεδομένα από το αμέσως ανώτερο επίπεδο και προσθέτει σε αυτά τις δικές του διαχειριστικές πληροφορίες (τη δική του επικεφαλίδα) σε μια διαδικασία που έχουμε ονομάσει ενθυλάκωση. Σε κάθε επίπεδο τα δεδομένα περιέχουν όλες τις πληροφορίες και τις επικεφαλίδες των προηγούμενων επιπέδων ενώ προστίθεται και μια καινούρια. Σε κάποια επίπεδα επίσης μπορεί να γίνεται κατακερματισμός των δεδομένων σε μικρότερα κομμάτια (στο επίπεδο μεταφοράς αυτό το κάνει το TCP και στο επίπεδο δικτύου

το IP). Σε κάθε επίπεδο επίσης η μονάδα δεδομένων έχει διαφορετικό όνομα: στο επίπεδο μεταφοράς, στο πρωτόκολλο TCP έχουμε τμήματα (segments), στο επίπεδο δικτύου με το πρωτόκολλο IP έχουμε πακέτα (packets) και στο επίπεδο ζεύξης δεδομένων (για δίκτυο Ethernet) έχουμε πλαίσια (frames).



Σχήμα 3.9: *Το Πρωτόκολλο ARP*

Στο επίπεδο δικτύου προστίθενται οι λογικές διευθύνσεις (διευθύνσεις IP) και δημιουργούνται αυτοδύναμα πακέτα. Τα πακέτα αυτά θα πρέπει να προωθηθούν στο επίπεδο ζεύξης δεδομένων για να αποσταλούν στο φυσικό μέσο και να παραδοθούν. Το πρόβλημα είναι ότι το επίπεδο ζεύξης δεδομένων δεν γνωρίζει τίποτα για τις λογικές διευθύνσεις του επιπέδου δικτύου: γνωρίζει μόνο τις δικές του φυσικές (MAC) διευθύνσεις. Για να μπορέσει να παραδώσει τα δεδομένα, θα πρέπει να δημιουργήσει πλαίσια στα οποία οι επικεφαλίδες να περιέχουν τις φυσικές διευθύνσεις αποστολέα και παραλήπτη (θυμηθείτε το πλαίσιο Ethernet που είδαμε στο κεφάλαιο 2).

θα πρέπει με κάποιο τρόπο να μετατραπούν οι λογικές διευθύνσεις σε φυσικές. Τη μετατροπή αυτή την κάνει το *πρωτόκολλο ARP*, το οποίο δρα σα συνδετικός κρίκος (σχήμα 3.9) μεταξύ του επιπέδου δικτύου και του επιπέδου ζεύξης δεδομένων.

Σε ποιο επίπεδο είναι το πρωτόκολλο ARP;

Το σχήμα του βιβλίου σας δείχνει το ARP ανάμεσα στα επίπεδα δικτύου και ζεύξης δεδομένων. Στο OSI συχνά αναφέρεται ως πρωτόκολλο επιπέδου 3 (Δικτύου) το οποίο ενθυλακώνεται σε πρωτόκολλα επιπέδου 2 (τα ερωτήματα και οι απαντήσεις ARP γίνονται μέσω πλαισίων). Ωστόσο το ARP δεν έχει σχεδιαστεί με βάση

το μοντέλο OSI (το Ethernet προϋπάρχει του OSI) και έτσι η παραπάνω ταξινόμηση είναι κάπως αυθαίρετη. Είναι πιο σωστό να το θεωρήσουμε ως λειτουργία που βρίσκεται ενδιάμεσα στα δύο επίπεδα (cross layer function). Στο μοντέλο TCP/IP, τα χαρακτηριστικά του ARP το κατατάσσουν στο επίπεδο ζεύξης δεδομένων.

Το *ARP, Πρωτόκολλο Ανάλυσης Διευθύνσεων, Address Resolution Protocol* αναλαμβάνει να απαντήσει σε ερωτήματα του τύπου "Ποια είναι η φυσική (MAC) διεύθυνση του υπολογιστή με τη συγκεκριμένη διεύθυνση IP;"

Για να επιτελέσει το σκοπό του, το πρωτόκολλο ARP χρησιμοποιεί το *ερώτημα ARP (ARP request)* με το οποίο απευθύνεται στο τοπικό δίκτυο Ethernet. Το ερώτημα αυτό γίνεται με ένα πλαίσιο εκπομπής: θυμηθείτε από το Ethernet ότι η φυσική διεύθυνση εκπομπής είναι άσοι και στα 48 ψηφία, ή στο δεκαεξαδικό FF:FF:FF:FF:FF:FF. Με αυτή τη διεύθυνση παραλήπτη, το ερώτημα θα ληφθεί από όλους τους κόμβους.

Κάθε κόμβος συγκρίνει την ζητούμενη IP με τη δική του και αν δεν συμπίπτει, απλά θα αγνοήσει το ερώτημα. Ο κόμβος όμως που διαθέτει τη συγκεκριμένη IP θα διαμορφώσει μια κατάλληλη *απάντηση ARP (ARP Reply)* και θα την αποστείλει στον κόμβο που έκανε την ερώτηση.

Επειδή είναι χρονοβόρο (και προκαλεί και αυξημένη κίνηση στο δίκτυο) να γίνεται συνέχεια η ίδια ερώτηση σε κάθε μετάδοση, κάθε κόμβος αποθηκεύει τις απαντήσεις που λαμβάνει προσωρινά στην τοπική μνήμη, σε ένα πίνακα που ονομάζεται *ARP Cache*. Πριν ένας κόμβος υποβάλλει ερώτημα στο δίκτυο, ελέγχει πρώτα από όλα τον τοπικό του πίνακα και αν υπάρχει αντίστοιχη καταχώριση την χρησιμοποιεί. Πρέπει να σημειώσουμε ότι κάθε κόμβος έχει δικό του πίνακα ARP με τις απαντήσεις στα ερωτήματα που έχει υποβάλλει ο ίδιος μέχρι στιγμής. Αν ένας κόμβος έχει περισσότερες από μια κάρτες δικτύου (για παράδειγμα αν είναι συνδεδεμένος με περισσότερα από ένα δίκτυα), υπάρχει ένας πίνακας ARP για κάθε κάρτα δικτύου.

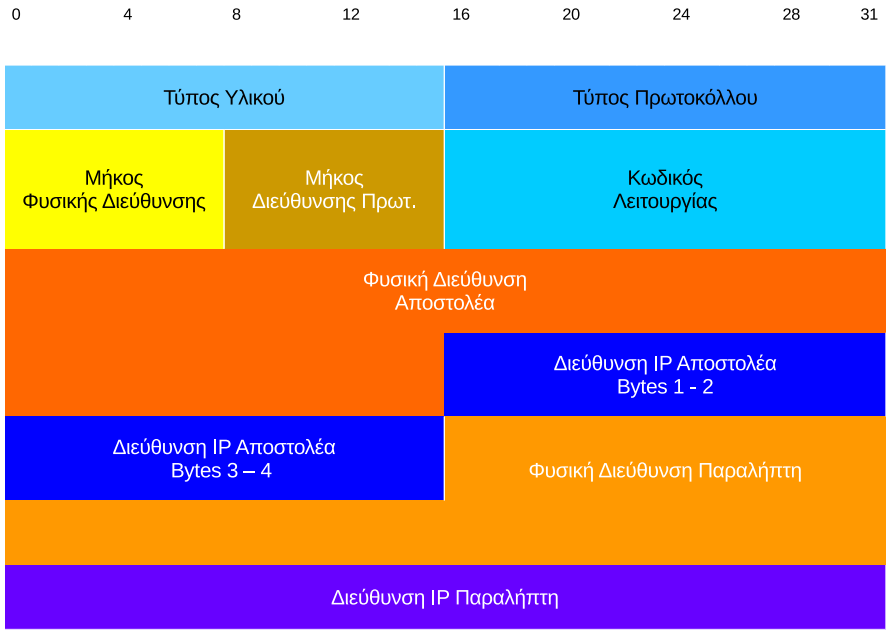
```
[14:05:29][sonic@pegasus:~]$ arp -a
? (192.168.0.106) at 8c:3a:e3:83:6d:77 on bge0 expires in 910 seconds [ethernet]
? (192.168.0.107) at ac:b5:7d:8e:14:8d on bge0 expires in 1079 seconds [ethernet]
pegasus.chania-lug.gr (192.168.0.3) at 1c:98:ec:0f:61:8c on bge0 permanent [ethernet]
? (192.168.0.101) at 78:0c:b8:a3:58:31 on bge0 expires in 1177 seconds [ethernet]
? (192.168.0.103) at a0:91:69:a5:92:b5 on bge0 expires in 1059 seconds [ethernet]
router.chania-lug.gr (192.168.0.250) at 78:96:82:45:eb:22 on bge0 expires in 1197 sec
? (192.168.0.112) at 00:21:29:e1:82:74 on bge0 expires in 953 seconds [ethernet]
```

Σχήμα 3.10: *Εκτέλεση εντολής arp σε ένα UNIX σύστημα*

Οι καταχωρίσεις στον πίνακα ARP είναι μπορεί να είναι *στατικές ή δυναμικές*. Οι δυναμικές καταχωρίσεις είναι προσωρινές: μετά από κάποιο χρονικό διάστημα (από

μερικά δευτερόλεπτα ως λίγα λεπτά συνήθως, το διάστημα μπορεί να ρυθμιστεί από το διαχειριστή του δικτύου) οι καταχωρίσεις λήγουν και το αντίστοιχο ερώτημα πρέπει να γίνει εκ νέου. Αντίθετα οι στατικές καταχωρίσεις έχουν μόνιμη ισχύ και δε λήγουν (παράδειγμα στατικής καταχώρισης είναι αυτή που αντιστοιχεί στην κάρτα δικτύου του ίδιου του μηχανήματος). Στο σχήμα 3.10 βλέπουμε τον πίνακα ARP σε ένα μηχάνημα UNIX (FreeBSD). Η ένδειξη “expires” δείχνει σε πόσα δευτερόλεπτα λήγει κάθε καταχώριση του πίνακα. Μετά τη λήξη, θα πρέπει να δημιουργηθεί ξανά ερώτημα ARP για τη συγκεκριμένη διεύθυνση. Η μόνιμη (permanent) καταχώριση στον πίνακα αντιστοιχεί στο ίδιο το μηχάνημα που εκτελεί την εντολή.

Το πακέτο ARP που αντιστοιχεί στο ερώτημα ενθυλακώνεται σε ένα πλαίσιο Ethernet και έχει τη μορφή που φαίνεται στο σχήμα 3.11.



Σχήμα 3.11: *Δομή Πακέτου ARP (για Ethernet)*

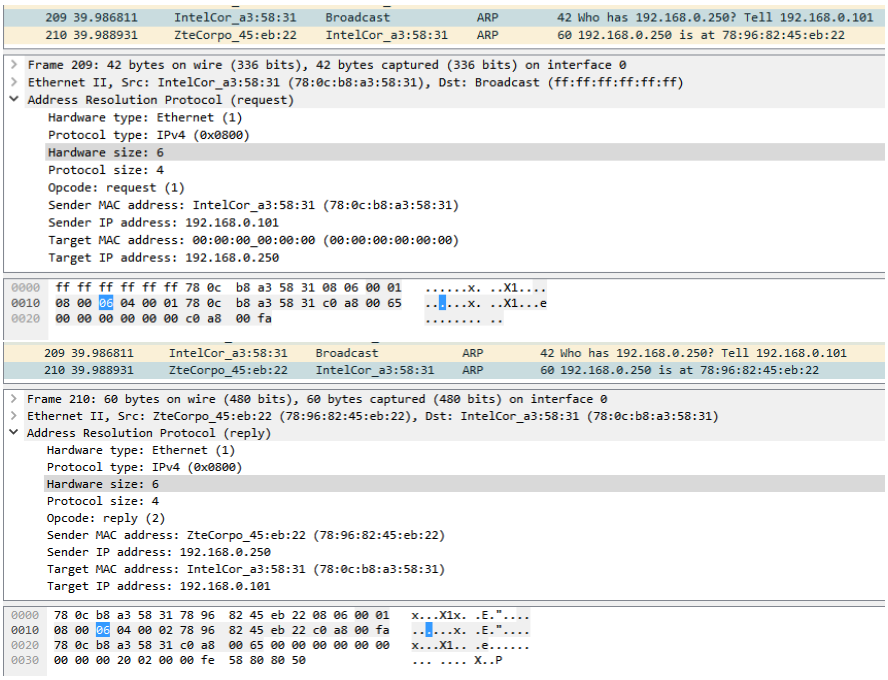
Τα πεδία είναι τα παρακάτω:

- **Τύπος Υλικού:** Έχει την τιμή 1 για δίκτυο Ethernet
- **Τύπος Πρωτοκόλλου:** Έχει την τιμή 0x800 (2048) για το IP
- **Μήκος Φυσικής Διεύθυνσης:** Έχει την τιμή 6 για φυσική διεύθυνση Ethernet (έξι bytes)
- **Μήκος Διεύθυνσης Πρωτοκόλλου:** Έχει την τιμή 4 για το πρωτόκολλο IPv4 (τέσσερα bytes)

- **Κωδικός Λειτουργίας:** Έχει την τιμή 1 για arp request και την τιμή 2 για arp reply

Ακολουθούν οι φυσικές και λογικές διευθύνσεις με τον τρόπο που φαίνεται στο σχήμα (**Προσοχή:** στο σχήμα του βιβλίου αναγράφεται λανθασμένα η σειρά των bytes της διεύθυνσης πρωτοκόλλου παραλήπτη. Τα δεδομένα τοποθετούνται μέσα στο πλαίσιο ακριβώς όπως θα διαβάζαμε εμείς τη διεύθυνση, κάτι που φαίνεται και στο πρόγραμμα Wireshark).

Στο σχήμα 3.12 φαίνεται το πακέτο arp με κωδικό λειτουργίας 1 (arp request) που αναζητεί τη φυσική διεύθυνση για τον κόμβο με IP 192.168.0.250. Βλέπουμε επίσης και την αντίστοιχη απάντηση (arp reply, με κωδικό λειτουργίας 2).

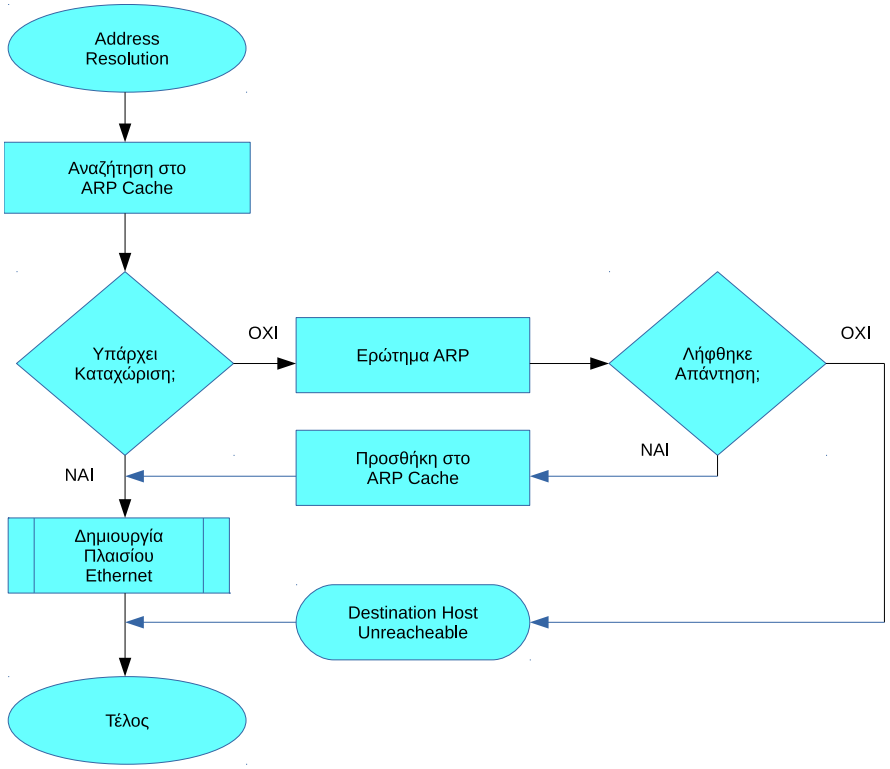


Σχήμα 3.12: *Ερώτημα και Απάντηση ARP*

Αν σε μια αναζήτηση φυσικής διεύθυνσης δεν βρεθεί απάντηση στον πίνακα ARP και ούτε δοθεί απάντηση στο ερώτημα ARP, αυτό μπορεί να σημαίνει ότι ο συγκεκριμένος υπολογιστής δεν υπάρχει, είναι σβηστός, ή έχει κάποιο πρόβλημα που τον εμποδίζει να επικοινωνήσει με το δίκτυο. Στην περίπτωση αυτή επιστρέφεται στην εφαρμογή διαγνωστικό μήνυμα που δηλώνει την αδυναμία πρόσβασης. Χαρακτηριστικό παράδειγμα είναι η χρήση της εντολής *ping* σε ανύπαρκτο υπολογιστή:

```
From 10.146.0.110 icmp_seq=3 Destination Host Unreachable
```

Τα βήματα που ακολουθούνται για την αποστολή ενός πακέτου IP, είναι τα παρακάτω (φαίνονται και στο διάγραμμα ροής στο σχήμα 3.13):



Σχήμα 3.13: *Διάγραμμα Ροής για Ανάλυση Διευθύνσεων ARP*

- Το αυτοδύναμο IP πακέτο εισέρχεται στην ουρά αναμονής για μετάδοση
- Γίνεται αναζήτηση στον πίνακα ARP για να διαπιστωθεί αν υπάρχει καταχώριση για τη συγκεκριμένη IP
- Αν υπάρχει καταχώριση, το πακέτο IP βγαίνει από την ουρά αναμονής, δημιουργείται το αντίστοιχο πλαίσιο Ethernet με βάση την καταχώριση και αποστέλλεται στο δίκτυο
- Αν δεν υπάρχει καταχώριση δημιουργείται το κατάλληλο ερώτημα ARP και αποστέλλεται στη διεύθυνση εκπομπής του Ethernet (FF:FF:FF:FF:FF:FF)
- Αν ληφθεί ARP απάντηση, καταχωρείται στον πίνακα ARP, το πακέτο IP εξέρχεται από την αναμονή, δημιουργείται το αντίστοιχο πλαίσιο Ethernet και αποστέλλεται στο δίκτυο
- Αν δεν ληφθεί ARP απάντηση, ο υπολογιστής μπορεί να μην υπάρχει ή να μην είναι ενεργός. Επιστρέφεται στον αποστολέα διαγνωστικό μήνυμα λάθους

Το πρωτόκολλο ARP περιγράφεται στο RFC826.

Εκτός από το πρωτόκολλο ARP, υπάρχει και το πρωτόκολλο *RARP (Reverse Address Resolution Protocol)*. Το RARP έχει σκοπό να απλοποιήσει την εγκατάσταση ενός δικτύου: όταν προστίθεται ένας υπολογιστής σε ένα δίκτυο, ο διαχειριστής θα πρέπει να του αποδώσει μια διεύθυνση IP που να συμφωνεί με τις ρυθμίσεις του δικτύου. Ωστόσο θα πρέπει να φροντίσει η διεύθυνση αυτή να είναι μοναδική στο δίκτυο διαφορετικά θα υπάρχει σύγκρουση με κάποιο άλλο υπολογιστή. Σε πολλές περιπτώσεις, είναι προτιμότερο να αποκτά ο υπολογιστής διεύθυνση αυτόματα. Αυτό επιτυγχάνεται με το πρωτόκολλο RARP: στην εκκίνηση, ο υπολογιστής στέλνει ένα κατάλληλα διαμορφωμένο μήνυμα στο δίκτυο και ένας *εξυπηρετητής RARP* αναλαμβάνει να του στείλει κατάλληλη διεύθυνση IP για να χρησιμοποιήσει. Με αυτό τον τρόπο αποφεύγεται η ταλαιπωρία των χειροκίνητων ρυθμίσεων και εξασφαλίζεται ότι δεν θα υπάρχουν συγκρούσεις, αφού ο εξυπηρετητής RARP γνωρίζει ποιες διευθύνσεις έχουν αποδοθεί ήδη και ποιες είναι διαθέσιμες. Το πρωτόκολλο RARP περιγράφεται στο RFC903.

Στις μέρες μας όμως, το RARP χρησιμοποιείται σπάνια, καθώς εκτός από τη διεύθυνση θέλουμε πλέον να στέλνουμε και αρκετές επιπλέον ρυθμίσεις, όπως τη μάσκα δικτύου, την προεπιλεγμένη πύλη, τους διακομιστές DNS κλπ τα οποία το RARP δεν τα καλύπτει. Αντί για το RARP, χρησιμοποιούνται τα πιο σύγχρονα πρωτόκολλα *BOOTP (Bootstrap protocol, πρωτόκολλο εκκίνησης)* και *DHCP, Dynamic Host Configuration Protocol, πρωτόκολλο δυναμικής απόδοσης ρυθμίσεων*.

Το BOOTP προορίζεται κυρίως για χρήση σε υπολογιστές που εκκινούν αποκλειστικά από το δίκτυο και δεν διαθέτουν δικό τους σκληρό δίσκο. Το DHCP είναι πιο ευέλικτο και μπορεί να εξυπηρετήσει τόσο πελάτες BOOTP όσο και μηχανήματα που εκκινούν τοπικά αλλά χρειάζεται να ανακτήσουν τις υπόλοιπες ρυθμίσεις τους από το δίκτυο. Τα δύο αυτά πρωτόκολλο υλοποιούνται στο επίπεδο εφαρμογής, σε αντίθεση με τα ARP/RARP που βρίσκονται στα επίπεδα 2 και 3 του OSI. Είναι εφαρμογές που ακολουθούν το μοντέλο *Πελάτη – Εξυπηρετητή*.

3.3.2 Το Πρωτόκολλο Δυναμικής Διευθέτησης Υπολογιστή DHCP

Το DHCP λειτουργεί με παρόμοιο τρόπο με το BOOTP και επεκτείνει τη λειτουργία του. Πρόκειται για πρωτόκολλο που χρησιμοποιεί το μοντέλο *πελάτη – εξυπηρετητή* και εκτελείται στο επίπεδο εφαρμογής. Το DHCP χρησιμοποιεί πακέτα UDP και έχει καθορισμένες θύρες τόσο για τον εξυπηρετητή (θύρα 67) όσο και για τον πελάτη (θύρα 68).

Το DHCP μας επιτρέπει να στείλουμε σε ένα μόνο μήνυμα ένα πλήθος ρυθμίσεων και όχι μόνο μια διεύθυνση όπως το RARP. Τυπικά στέλνουμε ρυθμίσεις όπως τη

διεύθυνση, τη μάσκα δικτύου, την προεπιλεγμένη πύλη (δρομολογητή) και έναν ή περισσότερους εξυπηρετητές DNS. Το DHCP καθορίζει τρεις τύπους εκχώρησης διευθύνσεων:

- **Τη μη αυτόματη (ή χειροκίνητη) ρύθμιση (manual configuration):** Στην περίπτωση αυτή ο διαχειριστής ορίζει συγκεκριμένες διευθύνσεις που θα πάρουν συγκεκριμένοι υπολογιστές και ο εξυπηρετητής απλά στέλνει πάντα τις ίδιες αυτές ρυθμίσεις στα συγκεκριμένα μηχανήματα
- **Την αυτόματη ρύθμιση (automatic configuration):** Σε αυτή ο εξυπηρετητής DHCP στέλνει μια μόνιμη διεύθυνση σε ένα υπολογιστή ο οποίος συνδέεται για πρώτη φορά
- **Τη δυναμική ρύθμιση (dynamic configuration):** Σε αυτή ο εξυπηρετητής DHCP δανείζει (μισθώνει) μια διεύθυνση σε ένα υπολογιστή για κάποιο περιορισμένο χρονικό διάστημα

Η δυναμική ρύθμιση είναι η πιο συχνά χρησιμοποιούμενη.

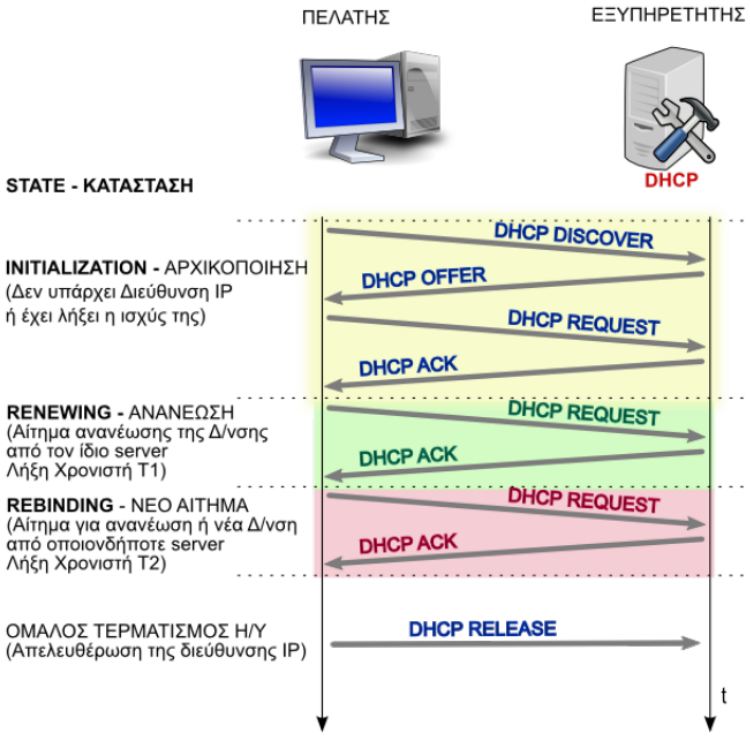
Ποια η διαφορά μεταξύ αυτόματης και μη αυτόματης ρύθμισης; Αφού και οι δυο στέλνουν μόνιμες διευθύνσεις.

Στην αυτόματη ρύθμιση, αποδίδεται στον υπολογιστή μια μόνιμη διεύθυνση από μια λίστα διαθέσιμων διευθύνσεων που διατηρεί ο εξυπηρετητής. Στη χειροκίνητη ρύθμιση, η μόνιμη διεύθυνση επιλέγεται απευθείας από τον διαχειριστή. Είναι σημαντικό για ορισμένα κρίσιμα μηχανήματα σε ένα δίκτυο να έχουν πάντοτε την ίδια και γνωστή σε μας διεύθυνση, ώστε να μπορούμε να συνδεθούμε σε αυτά χρησιμοποιώντας το IP τους ακόμα και όταν για κάποιο λόγο δεν λειτουργούν υπηρεσίες ονομάτων όπως το DNS που θα δούμε παρακάτω.

Πλεονεκτήματα του DHCP: Βασικό πλεονέκτημα του DHCP από τη σκοπιά των απλών (μη-τεχνικών) χρηστών είναι η απλούστευση στη σύνδεση σε ένα δίκτυο. Οι περισσότεροι χρήστες δεν κατανοούν την τεχνική πολυπλοκότητα της σύνδεσης σε ένα δίκτυο και το DHCP τους δίνει τη δυνατότητα να συνδεθούν εύκολα σε αυτό. Ταυτόχρονα διευκολύνεται και η εργασία του διαχειριστή που δεν χρειάζεται πλέον να κάνει σε κάθε μηχάνημα χωριστά ρυθμίσεις, αλλά μπορεί να τις διαχειρίζεται κεντρικά και να συντηρεί ευκολότερα το δίκτυο.

Εκτός από τις ρυθμίσεις που αναφέραμε παραπάνω, το πρωτόκολλο DHCP μπορεί να στείλει στον υπολογιστή ή σε κάθε του δικτυακή σύνδεση ρυθμίσεις για το επίπεδο ζεύξης δεδομένων, για το πρωτόκολλο TCP (επίπεδο μεταφοράς), καθώς και για υπηρεσίες (επίπεδο εφαρμογής) όπως για παράδειγμα διακομιστές χρόνου (NTP,

χρησιμοποιούνται για την αυτόματη ρύθμιση της ώρας στους υπολογιστές), διακομιστές αλληλογραφίας κλπ. Οι ρυθμίσεις αυτές περιγράφονται στο RFC2132 και τα συμπληρωματικά του.



Σχήμα 3.14: *Η Λειτουργία του DHCP*

Ένας υπολογιστής – πελάτης που έχει ρυθμιστεί να χρησιμοποιεί την υπηρεσία DHCP, αμέσως μετά την εκκίνηση του, εκτελεί τα παρακάτω βήματα (σχήμα 3.14):

- Δημιουργεί ένα αυτοδύναμο πακέτο **UDP DHCPDISCOVER** από τη θύρα 68 στην θύρα προορισμού 67. Όλη η επικοινωνία του πρωτοκόλλου DHCP (εφαρμογής) ενθυλακώνεται σε πρωτόκολλο UDP (μεταφοράς).
- Το πακέτο UDP το ενθυλακώνει σε πακέτο IP στο επίπεδο δικτύου. Δεδομένου ότι ο υπολογιστής μας δεν διαθέτει διεύθυνση δικτύου, χρησιμοποιείται ως διεύθυνση αποστολέα η ειδική διεύθυνση 0.0.0.0. Ο υπολογιστής δεν γνωρίζει την διεύθυνση IP του εξυπηρετητή DHCP, οπότε ως διεύθυνση παραλήπτη χρησιμοποιείται η διεύθυνση εκπομπής 255.255.255.255.
- Το παραπάνω πακέτο IP ενθυλακώνεται σε ένα πλαίσιο στο επίπεδο ζεύξης δεδομένων. Η φυσική διεύθυνση προέλευσης (48 bit) είναι η πραγματική του αποστολέα. Καθώς δεν γνωρίζουμε τη φυσική διεύθυνση του εξυπηρετητή

DHCP, χρησιμοποιείται η διεύθυνση εκπομπής FF:FF:FF:FF:FF:FF. Το πλαίσιο στέλνεται στο τοπικό δίκτυο.

- Αν υπάρχουν εξυπηρετητές DHCP ανταποκρίνονται ο καθένας με ένα πακέτο **DHCPOFFER** το οποίο απευθύνεται στη θύρα 68 και ενθυλακώνεται σε ένα πακέτο IP εκπομπής (255.255.255.255) το οποίο με τη σειρά του ενθυλακώνεται σε ένα πλαίσιο εκπομπής (FF:FF:FF:FF:FF:FF). Καθώς οι διακομιστές γνωρίζουν από το πακέτο DHCPDISCOVER τη φυσική διεύθυνση του αποστολέα, μπορούν να απαντήσουν με πλαίσιο που να απευθύνεται απευθείας σε αυτόν και όχι με πλαίσιο εκπομπής. Το πακέτο DHCPOFFER περιέχει όλες τις απαιτούμενες ρυθμίσεις δικτύου.
- Ο υπολογιστής – πελάτης επιλέγει τις ρυθμίσεις που επιθυμεί από ένα από τους εξυπηρετητές που απάντησαν (οι υπόλοιποι ενημερώνονται και αποσύρουν τις προσφορές τους) και το δηλώνει αποστέλλοντας ένα πακέτο **DHCPREQUEST** στο οποίο ζητά τις προσφερόμενες ρυθμίσεις.
- Ο εξυπηρετητής DHCP που προσέφερε τις ρυθμίσεις επιβεβαιώνει την προσφορά του με ένα πακέτο **DHCPACK** (επιβεβαίωσης).

Μετά τη λήψη της επιβεβαίωσης DHCPACK ο υπολογιστής πλέον λειτουργεί με τις ρυθμίσεις δικτύου που πήρε μέσω του πακέτου DHCPOFFER. Στην κατάσταση αυτή ο υπολογιστής ονομάζεται δεσμευμένος (BOUND). Στη συνηθισμένη δυναμική ρύθμιση, η διεύθυνση IP παραχωρείται στον υπολογιστή για συγκεκριμένο χρονικό διάστημα, χαρακτηρίζεται δε ως *μίσθωση*, *lease*. Το χρονικό αυτό διάστημα μπορεί να ρυθμιστεί από το διαχειριστή στις ρυθμίσεις του εξυπηρετητή DHCP.

Από τη στιγμή αυτή, αρχίζει η σχετική μέτρηση χρόνου: πριν λήξει ο χρόνος μίσθωσης, ο υπολογιστής θα προβεί σε ενέργειες για την ανανέωση ή παράταση της. Ο υπολογιστής κρατά δύο χρόνους:

- Το χρόνο T1 – τυπικά 0.5 * χρόνος μίσθωσης – μετά τον οποίο προσπαθεί να ανανεώσει τη μίσθωση από το διακομιστή ο οποίος έδωσε αρχικά τη διεύθυνση. Σε αυτή την περίπτωση λέμε ότι ο υπολογιστής βρίσκεται σε κατάσταση *RENEWING (ανανέωσης)*. Για την διαδικασία αυτή στέλνει εκ νέου πακέτο DHCPREQUEST - unicast δηλ. προς το συγκεκριμένο διακομιστή (δεν χρησιμοποιεί διεύθυνση εκπομπής).
- το χρόνο T2 – τυπικά 0.875 * χρόνος μίσθωσης – μετά τον οποίο αναζητά ανανέωση ή νέα διεύθυνση από οποιοδήποτε πλέον διακομιστή DHCP του δικτύου. Σε αυτή την περίπτωση ο υπολογιστής είναι σε κατάσταση *REBINDING*. Για τη διαδικασία αυτή στέλνει πακέτο DHCPREQUEST - broadcast χρησιμοποιεί δηλ. διεύθυνση εκπομπής.

Ο χρόνος T1 είναι προφανώς μικρότερος του T2.

Όταν ο υπολογιστής τερματίζει τη λειτουργία του ομαλά και πριν λήξει η μίσθωση της διεύθυνσης, ζητά την απελευθέρωση της (ώστε να μπορεί να δοθεί σε άλλον υπολογιστή αν υπάρχει ανάγκη) στέλνοντας πριν το τερματισμό ένα πακέτο **DHCPRELEASE** στο διακομιστή DHCP.

Στο πρωτόκολλο DHCP προβλέπονται ακόμα τα εξής μηνύματα:

- **DHCPNAK:** Από το διακομιστή προς τον πελάτη: Αν μετά από το DHCPREQUEST, ο διακομιστής δεν επιβαιώσει ως σωστές τις ρυθμίσεις που ζητά ο πελάτης, απαντά με ένα μήνυμα μη-επιβεβαίωσης DHCPNAK.
- **DHCPDECLINE:** Από τον πελάτη προς το διακομιστή: Αν μετά τη λήψη μιας προσφοράς μέσω DHCPOFFER ο πελάτης διαπιστώσει ότι οι ρυθμίσεις που του στάλθηκαν είναι σε σύγκρουση με άλλο υπολογιστή στο δίκτυο, απορρίπτει την προσφορά στέλνοντας ένα πακέτο DHCPDECLINE. Έπειτα ξεκινά τη διαδικασία από την αρχή στέλνοντας πακέτο DHCPDISCOVER.
- **DHCPINFORM:** Αν μετά την αρχική λήψη ρυθμίσεων μέσω DHCPOFFER ο πελάτης χρειάζεται επιπλέον ρυθμίσεις δικτύου, δεν μπορεί να χρησιμοποιήσει ξανά το πακέτο DHCPREQUEST. Στην περίπτωση αυτή τις ζητά με ένα αίτημα DHCPINFORM.

Η λειτουργία του DHCP υποστηρίζεται και από **Πράκτορες Αναμετάδοσης, DHCP Relay Agents**. Ένας υπολογιστής πελάτης που βρίσκεται σε διαφορετικό τμήμα ή φυσικό δίκτυο από αυτό που βρίσκεται ο διακομιστής DHCP δεν μπορεί να επικοινωνήσει απευθείας με αυτόν καθώς δεν διαθέτει διεύθυνση IP (οι φυσικές διευθύνσεις ισχύουν μόνο στο συγκεκριμένο τμήμα δικτύου και δεν μπορούν να δρομολογηθούν). Ένας υπολογιστής που βρίσκεται στο ίδιο φυσικό δίκτυο με τον πελάτη μπορεί να λειτουργήσει ως αναμεταδότης, προωθώντας τα μηνύματα του πελάτη προς το διακομιστή DHCP στο άλλο δίκτυο και επιστρέφοντας τις απαντήσεις του.

Το πρωτόκολλο DHCP προτάθηκε ως επέκταση του BOOTP, αρχικά στα RFC1531, RFC1541 τα οποία αντικαταστάθηκαν από το RFC2131. Σε αυτό και τα συμπληρωματικά του βρίσκονται όλες οι απαιτούμενες πληροφορίες για τη λειτουργία του.

3.4 Διευθύνσεις IP και Ονοματολογία

Όπως γνωρίζουμε, οι διευθύνσεις στο IPv4 είναι στην πραγματικότητα δυαδικοί αριθμοί των 32 bit. Ωστόσο σχεδόν πάντα τους χωρίζουμε σε οκτάδες ψηφίων και τους γράφουμε με δεκαδικούς αριθμούς χωρισμένους μεταξύ τους με τελείες, ώστε να τους θυμόμαστε πιο εύκολα. Αυτός ο τρόπος γραφής ονομάζεται *dotted decimal*.

Συγκρίνετε για παράδειγμα τη διεύθυνση:

`192.168.1.2`

με την αντίστοιχη δυαδική:

`11000000.10101000.00000001.00000010`

Όμως ακόμα και με την δεκαδική αναπαράσταση, είναι απίθανο για ένα άνθρωπο να απομνημονεύσει πάνω από μερικές διευθύνσεις. Αν και οι υπολογιστές δεν έχουν κανένα πρόβλημα στην αποθήκευση αριθμών, οι άνθρωποι τα πηγαίνουν καλύτερα με τα ονόματα: σπάνια θυμόμαστε για παράδειγμα τους αριθμούς τηλεφώνων όλων των φίλων μας. Τυπικά χρησιμοποιούμε το όνομα τους και αναζητούμε το τηλέφωνο τους σε ένα κατάλογο (σημειωματάριο, τις επαφές στο κινητό μας κλπ).

Αν και το πρωτόκολλο IP χρησιμοποιεί μόνο τις διευθύνσεις, για τη δική μας ευκολία χρειάζεται κάποιο σύστημα αντίστοιχο με τον τηλεφωνικό κατάλογο: να μπορούμε να αναφερθούμε σε ένα υπολογιστή με το όνομα του και με κάποιο τρόπο να αντιστοιχιστεί στην πραγματική διεύθυνση IP.

Στην αρχή της ανάπτυξης του Internet, το πλήθος των υπολογιστών ήταν πολύ μικρό και συνήθως οι ίδιοι οι "χρήστες" του Διαδικτύου ήταν και οι διαχειριστές των μηχανημάτων. Στα περισσότερα μηχανήματα δίνονταν απλώς ένα *μονολεκτικό όνομα*. Θα έπρεπε όμως με κάποιο τρόπο να υπάρχει μια λίστα που να αντιστοιχεί αυτά τα ονόματα σε διευθύνσεις. Με τη λίστα αυτή οι άνθρωποι θα μπορούσαν να χρησιμοποιούν τα ονόματα, ενώ τα πρωτόκολλα θα τη συμβουλεύονταν για να βρουν την αριθμητική διεύθυνση. Το ρόλο αυτής της λίστας ανέλαβε το αρχείο *hosts*.

Σημείωση: Το βιβλίο σας το αναφέρει ως HOSTS.TXT – ίσως για να τονίσει ότι πρόκειται για αρχείο κειμένου. Στην πραγματικότητα, δεν έχει την κατάληξη .TXT σε κανένα λειτουργικό σύστημα (ούτε στα Windows). Είναι όμως κοινό αρχείο κειμένου που μπορούμε να το ανοίξουμε με το Σημειωματάριο. Για να αλλάξουμε κάποια καταχώριση σε αυτό χρειάζονται δικαιώματα διαχειριστή.

Κάθε φορά που προστίθεται ένα υπολογιστής στο δίκτυο, πρέπει να προστεθεί η αντίστοιχη εγγραφή στο αρχείο αυτό, με μορφή:

<διεύθυνση IP> <όνομα υπολογιστή>

το πρόβλημα όμως είναι ότι αυτό το αρχείο θα πρέπει να υπάρχει – ενημερωμένο – σε κάθε υπολογιστή του δικτύου. Αρχικά, όταν το Internet αποτελούνταν από λίγα μηχανήματα, οι διαχειριστές αντάλλαζαν μεταξύ τους το αρχείο κάθε φορά που γίνονταν κάποια αλλαγή και εγκαθιστούσαν τη νέα έκδοση στα μηχανήματα που δια-

χειρίζονταν. Προφανώς μια τέτοια τακτική δεν μπορεί να λειτουργήσει όταν διαχειριζόμαστε ένα δίκτυο με περισσότερα από λίγες δεκάδες μηχανήματα.

Το αρχείο αυτό πάντως εξακολουθεί να υπάρχει μέχρι σήμερα, αν και η χρήση του είναι περιορισμένη.

```
# $FreeBSD: releng/11.0/etc/hosts 109997 2003-01-28 21:29:23Z dbaker $
#
# Host Database
#
# This file should contain the addresses and aliases for local hosts that
# share this file.  Replace 'my.domain' below with the domainname of your
# machine.
#
# In the presence of the domain name service or NIS, this file may
# not be consulted at all; see /etc/nsswitch.conf for the resolution order.
#
#
::1                     localhost localhost.my.domain
127.0.0.1               localhost localhost.my.domain
10.14.28.10             aquarius64 aquarius64.lab1.local
#
# Imaginary network.
#10.0.0.2               myname.my.domain myname
#10.0.0.3               myfriend.my.domain myfriend
#
# According to RFC 1918, you can use the following IP networks for
```

Σχήμα 3.15: *Απόσπασμα Αρχείου hosts σε Λειτουργικό UNIX (FreeBSD)*

Σημείωση: Ακόμα και σήμερα τα περισσότερα συστήματα είναι ρυθμισμένα πρώτα να συμβουλεύονται το αρχείο hosts και μετά τις υπόλοιπες υπηρεσίες ονομάτων (τυπικά το DNS). Έτσι μπορούμε να χρησιμοποιήσουμε αυτό το αρχείο για να αποκλείσουμε διευθύνσεις (blacklisting) στις οποίες δεν θέλουμε να συνδεθεί ο υπολογιστής μας. Αρκεί να προσθέσουμε μια γραμμή που να παραπέμπει το αντίστοιχο όνομα σε μια ψεύτικη διεύθυνση ή (συνήθως) στο localhost – 127.0.0.1

Στα Windows θα βρείτε το αρχείο αυτό στην τοποθεσία:

`%SystemRoot%\System32\drivers\etc\hosts`

(τυπικά το SystemRoot είναι συνήθως ο φάκελος C:\Windows). Σε μηχανήματα UNIX/Linux το αρχείο βρίσκεται στη θέση /etc/hosts. Μπορείτε να δείτε ένα υπόδειγμα αρχείου hosts στο σχήμα 3.15.

Καθώς ο αριθμός των διασυνδεδεμένων στο Internet υπολογιστών αυξάνονταν με ραγδαίο ρυθμό, έγινε γρήγορα φανερό ότι ούτε το αρχείο hosts ούτε ο επίπεδος χώρος ονομάτων (απλό όνομα υπολογιστή, χωρίς τομέα) θα μπορούσαν να αντεπεξέλθουν. Σχετικά νωρίς (1983) προτάθηκε και υλοποιήθηκε η *Υπηρεσία Ονομάτων Περιοχών ή DNS, Domain Name System*. Στο DNS, το σύστημα ονομάτων δεν

είναι επίπεδο αλλά *ιεραρχικά δομημένο και οργανωμένο σε περιοχές και υποπεριοχές σε διάφορα επίπεδα*. Στο κατώτερο επίπεδο, στο αριστερό μέρος βρίσκεται το όνομα του υπολογιστή. Η διαδικασία μετάφρασης – αντιστοίχισης των ονομάτων σε διευθύνσεις ονομάζεται *ανάλυση ονομάτων* (name resolve) και το κομμάτι του λογισμικού που εκτελεί αυτή τη διαδικασία *name resolver*.

Η μορφή ενός ονόματος στο DNS είναι:

υπολογιστής.υποπεριοχή_n. … .υποπεριοχή_1.περιοχή_TLD

όπου TLD = Top Level Domain (περιοχή ανώτατου επιπέδου).

για παράδειγμα στη διεύθυνση:

joshua.freebsdgr.org

Το **joshua** είναι το όνομα του υπολογιστή, το **.freebsdgr** είναι η υποπεριοχή και το **.org** είναι η περιοχή ανώτατου επιπέδου.

Το σύστημα DNS δουλεύει ως μια μεγάλη κατανεμημένη και ιεραρχικά δομημένη βάση δεδομένων. Τμήματα της βάσης βρίσκονται σε διάφορους εξυπηρετητές της υπηρεσίας, οι οποίοι είναι υπεύθυνοι να απαντούν σε ερωτήματα για συγκεκριμένες περιοχές και υποπεριοχές. Θα εξετάσουμε αναλυτικότερα το DNS στην ενότητα 6.1.

Μπορείτε να βρείτε περισσότερες πληροφορίες στα RFC882, RFC883, RFC1034 και RFC1035.

3.6 Δρομολόγηση

Το επίπεδο διαδικτύου στο TCP/IP εκτός από τη διευθυνσιοδότηση (που έχουμε δει), είναι επίσης επιφορτισμένο και με την δρομολόγηση των αυτοδύναμων πακέτων IP (IP datagrams) εξασφαλίζοντας την επικοινωνία μεταξύ των δύο ακραίων υπολογιστών του δικτύου (host to host) μέσα από το απαιτούμενο *επικοινωνιακό υποδίκτυο*.

Επικοινωνιακό υποδίκτυο είναι το σύνολο των κόμβων που παρέχουν υπηρεσίες προώθησης και δρομολόγησης πακέτων ανάμεσα σε δύο ακραίους υπολογιστές. Οι κόμβοι μπορεί να είναι κανονικοί υπολογιστές ή εξειδικευμένες δικτυακές συσκευές με δυνατότητα να λειτουργούν τουλάχιστον ως το επίπεδο διαδικτύου του TCP/IP.

Στην πραγματικότητα η δρομολόγηση έχει νόημα όταν ανάμεσα στους δύο υπολογιστές που επικοινωνούν μεσολαβεί τουλάχιστον ένας δρομολογητής. Αν οι υπολογιστές βρίσκονται πάνω στο ίδιο φυσικό μέσο (π.χ. σε ένα τμήμα Ethernet) η δρομολόγηση είναι άμεση (χωρίς να απαιτείται δρομολογητής). Επίσης σε αυτές τις περιπτώσεις μπορούν να χρησιμοποιηθούν και άλλες τεχνικές (μεταγωγή – switching, γεφύρωση – bridging) οι οποίες πραγματοποιούνται από το δεύτερο επίπεδο του OSI καθώς αναφέρονται στο ίδιο φυσικό δίκτυο.

Δρομολόγηση είναι το έργο της μετακίνησης (προώθησης, διεκπεραίωσης) της πληροφορίας από την αφετηρία στο προορισμό της μέσω του επικοινωνιακού υποδικτύου. Η δρομολόγηση στην πραγματικότητα περιλαμβάνει δύο διακριτές (διαφορετικές) δραστηριότητες:

- Τον *προσδιορισμό της καλύτερης διαδρομής* από την αφετηρία στον προορισμό
- Την *μεταφορά (προώθηση – IP forwarding)* των πακέτων στον προορισμό τους μέσω του Διαδικτύου

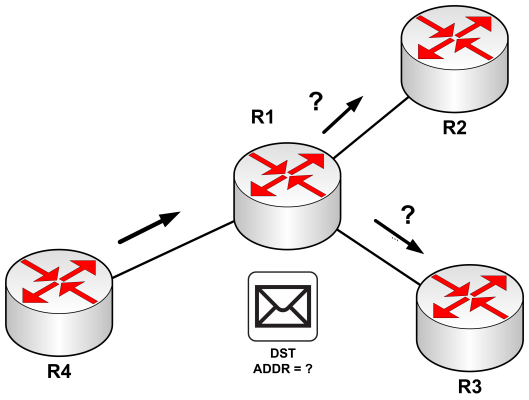
Η μεταφορά των πακέτων στην πραγματικότητα δεν είναι μια ιδιαίτερα δύσκολη διαδικασία. Η εύρεση όμως της καλύτερης διαδρομής αποτελεί σημαντικό και σύνθετο πρόβλημα το οποίο καλούνται να αντιμετωπίσουν τα *πρωτόκολλα δρομολόγησης*.

Ένα βασικό πρόβλημα στην εύρεση της καλύτερης διαδρομής είναι τα κριτήρια με τα οποία αποφασίζεται ότι μια διαδρομή είναι καλύτερη από κάποια άλλη. Είναι για παράδειγμα μια μικρότερη διαδρομή (με λιγότερους ενδιάμεσους σταθμούς – άλματα (hops) καλύτερη από μια μεγαλύτερη; Αυτό στην πραγματικότητα εξαρτάται και από την κίνηση που έχουν οι ενδιάμεσοι κόμβοι τη δεδομένη στιγμή αλλά και από τη χωρητικότητα των γραμμών που εξυπηρετούν τις διαδρομές αυτές. Για την εύρεση της καλύτερης διαδρομής, οι αλγόριθμοι δρομολόγησης χρησιμοποιούν μια σειρά από μετρήσιμα χαρακτηριστικά όπως:

- Το πλήθος των ενδιάμεσων κόμβων (αλμάτων) ανάμεσα στους δύο υπολογιστές
- Την δικτυακή κίνηση – καθυστέρηση που μπορεί να μετρηθεί σε μια συγκεκριμένη διαδρομή
- Το εύρος ζώνης / χωρητικότητα των ενδιάμεσων γραμμών κ.α.

Με τη βοήθεια των αλγόριθμων δρομολόγησης συντάσσονται οι *πίνακες δρομολόγησης* οι οποίοι περιέχουν πληροφορίες δρομολογίων. Οι πληροφορίες αυτές διαφέρουν ανάλογα με τον αλγόριθμο που χρησιμοποιείται κάθε φορά. Οι πίνακες περιέχουν μια ποικιλία πληροφοριών: η βασικότερη πληροφορία είναι οι *αντιστοιχίσεις προορισμού και επόμενου άλματος (next hop)* οι οποίες λένε στο δρομολογητή

σε ποια από τις διαθέσιμες δικτυακές διασυνδέσεις να προωθήσει ένα εισερχόμενο πακέτο ανάλογα με τον προορισμό του. Για να ληφθεί μια τέτοια απόφαση, ο δρομολογητής εξετάζει την διεύθυνση παραλήπτη του πακέτου από την επικεφαλίδα IP και προσπαθεί να την ταιριάξει με μια εγγραφή επόμενου άλματος στον πίνακα δρομολόγησης. Σκοπός είναι πάντα το πακέτο να προωθηθεί σε ένα επόμενο δρομολογητή ο οποίος να είναι ένα βήμα πιο κοντά στον προορισμό και η διαδικασία επαναλαμβάνεται μέχρι την τελική επίδοση του πακέτου στον παραλήπτη. Όταν βρεθεί η κατάλληλη διασύνδεση, το πακέτο προωθείται σε αυτή.



Σχήμα 3.16: *Προώθηση Πακέτων IP*

Πρέπει να διευκρινίσουμε ότι η διαδικασία αυτή επαναλαμβάνεται χωριστά για κάθε αυτοδύναμο πακέτο, ακόμα και αν όλα που λαμβάνονται αποτελούν τμήματα της ίδιας επικοινωνίας (σχήμα 3.16). Έτσι είναι δυνατόν IP πακέτα της ίδιας επικοινωνίας να ακολουθούν το καθένα διαφορετική διαδρομή σε άλλη χρονική στιγμή (με αποτέλεσμα βέβαια να λαμβάνονται και εκτός σειράς από τον παραλήπτη). Ένας δρομολογητής αποφασίζει μόνο για το επόμενο άλμα ενός πακέτου: *η πλήρης διαδρομή δεν είναι γνωστή από την αρχή της επικοινωνίας*.

Οι πίνακες δρομολόγησης περιέχουν και πληροφορίες οι οποίες περιέχουν το βαθμό προτίμησης μια διαδρομής (του επόμενου άλματος – next hop).

Για να επιτυγχάνεται η καλύτερη δυνατή δρομολόγηση, οι δρομολογητές ανταλλάσσουν μεταξύ τους μηνύματα και ενημερώνουν τους πίνακες δρομολόγησης τους. Τα μηνύματα μπορεί να περιέχουν ολόκληρους πίνακες δρομολόγησης ή μέρος αυτών. Από την ανάλυση των μηνυμάτων, ένας δρομολογητής μπορεί να σχηματίσει μια ξεκάθαρη εικόνα της τοπολογίας και της τρέχουσας κατάστασης των γραμμών και των συνδέσεων του Διαδικτύου. Από τις πληροφορίες αυτές είναι σε θέση να προσδιορίζει τις βέλτιστες διαδρομές προς τους διαφορετικούς προορισμούς του Διαδικτύου.

Το πρωτόκολλο IP χρησιμοποιεί αυτοδύναμα πακέτα (datagrams) και είναι σχεδιασμένο να λειτουργεί σε όλους τους τύπους υλικού δικτύου (Ethernet, Token Ring κλπ). Πρόκειται για ένα πρωτόκολλο λογικής *best effort delivery* δηλ. βέλτιστης προσπάθειας: κάνει ότι καλύτερο μπορεί για να επιδώσει το κάθε αυτοδύναμο πακέτο, δεν παρέχει όμως εγγυήσεις π.χ. για την ταχύτητα, την καθυστέρηση, τη σειρά επίδοσης κλπ. Δεν μπορεί να αντιμετωπίσει τα παρακάτω προβλήματα:

- Επανάληψη αυτοδύναμου πακέτου
- Επίδοση με καθυστέρηση ή εκτός σειράς
- Αλλοίωση δεδομένων
- Απώλεια αυτοδύναμου πακέτου

Για την αντιμετώπιση τέτοιων σφαλμάτων, είναι υπεύθυνα τα ανώτερα επίπεδα. Για παράδειγμα, μια επικοινωνία TCP (επίπεδο μεταφοράς) παρέχει αξιοπιστία παρά το γεγονός ότι στο επίπεδο διαδικτύου εξυπηρετείται από το πρωτόκολλο IP.

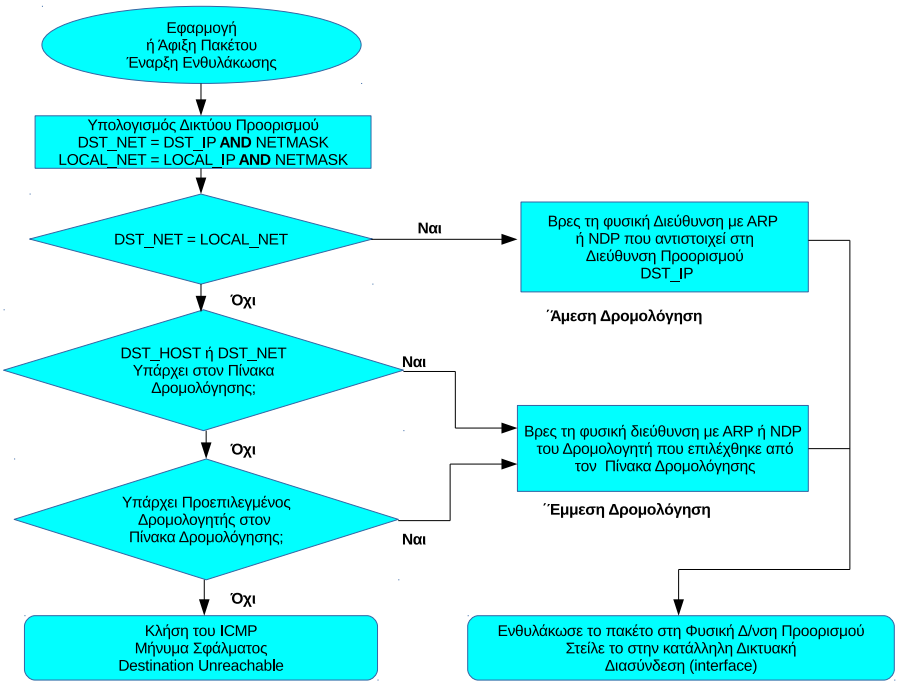
3.6.1 Άμεση – Έμμεση Δρομολόγηση

Η βασική αρχή της δρομολόγησης είναι απλή: Ο αποστολέας δημιουργεί τα αυτοδύναμα πακέτα IP και εξετάζει την διεύθυνση προορισμού: αν είναι τοπική, βρίσκεται δηλ. στο ίδιο δίκτυο με αυτόν, δεν έχει να κάνει κάτι το ιδιαίτερο: αρκεί να δώσει το πακέτο στο παρακάτω επίπεδο που θα φροντίσει για την αποστολή στο φυσικό μέσο.

Εάν η διεύθυνση προορισμού δεν είναι τοπική, ο αποστολέας αναζητά κατάλληλο δρομολογητή ο οποίος ελπίζει να βρίσκεται στη σωστή κατεύθυνση προς τον προορισμό και στέλνει τα πακέτα σε αυτόν. Ο δρομολογητής εκτελεί ουσιαστικά την ίδια διαδικασία και το στέλνει σε ένα άλλο δρομολογητή κ.ο.κ. μέχρι το πακέτο να φτάσει σε ένα δρομολογητή που βρίσκεται στο ίδιο φυσικό δίκτυο με τον υπολογιστή προορισμού. Εκεί παραδίδεται το πακέτο.

Με περισσότερες λεπτομέρειες, ακολουθείται η παρακάτω διαδικασία:

- Ο αποστολέας εκτελεί τη λογική πράξη **ΚΑΙ** μεταξύ της διεύθυνσης προορισμού και της μάσκας υποδικτύου. Προκύπτει έτσι η *Διεύθυνση Δικτύου Προορισμού*.
- Ο αποστολέας εξετάζει τη διεύθυνση δικτύου προορισμού: αν είναι στο ίδιο φυσικό δίκτυο με αυτόν, δεν χρειάζεται να κάνει κάτι το ιδιαίτερο: η δρομολόγηση είναι *άμεση*. Θα χρησιμοποιήσει το πρωτόκολλο ARP (ή NDP για IPv6) για να βρει τη φυσική διεύθυνση του υπολογιστή προορισμού και θα



Σχήμα 3.17: *Διαδικασία Δρομολόγησης Αυτοδύναμου Πακέτου*

παραδώσει το πακέτο στο παρακάτω επίπεδο για να γίνει ενθυλάκωση του σε πλαίσιο και αποστολή στο φυσικό μέσο.

- Αν η διεύθυνση δικτύου προορισμού δεν είναι ίδια με αυτή του αποστολέα, το πακέτο θα πρέπει να αποσταλεί σε ένα κατάλληλο δρομολογητή. Στην περίπτωση αυτή η δρομολόγηση είναι *έμμεση*. Ο αποστολέας θα συμβουλευτεί τον πίνακα δρομολόγησης αναζητώντας μια εγγραφή που να ταιριάζει στον υπολογιστή προορισμού (DST_HOST) ή στο δίκτυο προορισμού (DST_NET). Αν βρει αυτή την εγγραφή, θα χρησιμοποιήσει το πρωτόκολλο ARP για να βρει τη φυσική διεύθυνση του αντίστοιχου δρομολογητή. Στη συνέχεια θα παραδώσει το πακέτο στο παρακάτω επίπεδο για να γίνει ενθυλάκωση του σε πλαίσιο και αποστολή στο φυσικό μέσο. Σημειώστε ότι στην έμμεση δρομολόγηση το πακέτο έχει τη λογική διεύθυνση του τελικού παραλήπτη αλλά το πλαίσιο τη φυσική διεύθυνση του δρομολογητή που θα αναλάβει την δρομολόγηση.

- Αν ο πίνακας δρομολόγησης δεν περιέχει εγγραφή που να ταιριάζει με τη διεύθυνση του υπολογιστή προορισμού ή με τη διεύθυνση δικτύου του υπολογιστή προορισμού, ο αποστολέας θα αναζητήσει εγγραφή για *προεπιλεγμένο δρομολογητή*. Σε ένα δίκτυο, ο προεπιλεγμένος δρομολογητής αναλαμβάνει τη δρομολόγηση όλων των πακέτων για τα οποία δεν υπάρχει πιο συγκεκρι-

μένη καταχώριση στον πίνακα δρομολόγησης (το router με το οποίο συνδέεστε στο Internet είναι ο προεπιλεγμένος δρομολογητής για το οικιακό σας δίκτυο). Αν υπάρχει προεπιλεγμένος δρομολογητής, ο αποστολέας θα αναζητήσει τη φυσική του διεύθυνση μέσω του ARP και θα παραδώσει το πακέτο στο παρακάτω επίπεδο για να γίνει, όπως και προηγουμένως, ενθυλάκωση και αποστολή του στο φυσικό μέσο.

- Αν δεν βρεθεί καμιά κατάλληλη καταχώριση στον πίνακα και ούτε υπάρχει προεπιλεγμένος δρομολογητής, το πακέτο δεν είναι δυνατόν να παραδοθεί: η δρομολόγηση είναι αδύνατη. Ο αποστολέας θα ειδοποιηθεί μέσω του πρωτοκόλλου ICMP ότι ο προορισμός δεν είναι προσβάσιμος.

Η παραπάνω διαδικασία φαίνεται και ως διάγραμμα ροής στο σχήμα 3.17.

Κεφάλαιο 4

Επίπεδο Μεταφοράς

4.1 Πρωτόκολλα Προσανατολισμένα στη Σύνδεση – Χωρίς Σύνδεση

Οι δικτυακές εφαρμογές που είναι εγκαταστημένες στους κόμβους ενός δικτύου (υπολογιστές, έξυπνες συσκευές, smartphones κλπ) επικοινωνούν ανταλλάσσοντας μεταξύ τους μηνύματα δεδομένων. Το επίπεδο μεταφοράς παρέχει τις διαδικασίες που αναλαμβάνουν τη μεταφορά μηνυμάτων με διαφανή τρόπο από τις εφαρμογές που τα παράγουν.

Το επίπεδο μεταφοράς είναι υπεύθυνο για την επικοινωνία των δεδομένων που λαμβάνονται από το επίπεδο εφαρμογής του υπολογιστή αφετηρίας μέχρι το αντίστοιχο του προορισμού. Πρόκειται για μια επικοινωνία από *άκρο σε άκρο* (end to end). Το επίπεδο μεταφοράς δεν ενδιαφέρεται για το γεγονός ότι στην πραγματικότητα τα δεδομένα του προωθούνται μέσα από ένα πλήθος άλλων κόμβων με τη βοήθεια του πρωτοκόλλου IP (στο επίπεδο διαδικτύου). Όσο αφορά το επίπεδο μεταφοράς, η σύνδεση είναι μια ευθεία γραμμή μεταξύ αφετηρίας και προορισμού.

Υπάρχουν γενικά δύο τρόποι να ξεκινήσει μια επικοινωνία στο επίπεδο μεταφοράς:

- Ο κόμβος στην αφετηρία μπορεί να ξεκινήσει με την *εγκατάσταση σύνδεσης*: Θα επικοινωνήσει για αυτό το σκοπό με τον προορισμό και η μετάδοση των δεδομένων θα αρχίσει αφού καθοριστούν πρώτα οι παράμετροι της επικοινωνίας. Το πρόγραμμα στον υπολογιστή αφετηρίας επικοινωνεί και συνομιλεί με ένα παρόμοιο πρόγραμμα στον υπολογιστή προορισμού. Οι πληροφορίες της σύνδεσης αποθηκεύονται στις επικεφαλίδες του μηνύματος και στα μηνύματα

ελέγχου.

- Εναλλακτικά, ο κόμβος στην αφετηρία μπορεί απλά να ξεκινήσει να στέλνει δεδομένα προς τον προορισμό *χωρίς να γίνει από πριν εγκατάσταση σύνδεσης*.

Και στις δυο περιπτώσεις, τα δεδομένα που παράγονται στο επίπεδο μεταφοράς προωθούνται στην πραγματικότητα μέσα από το επίπεδο Διαδικτύου αφού ενθυλακωθούν μέσα σε πακέτα IP. Στη μεταφορά αυτή χρησιμοποιούνται πολλοί ενδιάμεσοι κόμβοι που εκτελούν υπηρεσίες δρομολόγησης (όπως είδαμε στο προηγούμενο κεφάλαιο).

Συνοπτικά, οι λειτουργίες που αναλαμβάνει το επίπεδο μεταφοράς είναι η εγκατάσταση και ο τερματισμός των συνδέσεων και ο έλεγχος ροής της πληροφορίας ώστε μια γρήγορη μηχανή να μην υπερφορτώνει μια αργή, καθώς και η επιβεβαίωση ότι η πληροφορία έφτασε πράγματι στον προορισμό της.

Τα δύο βασικά πρωτόκολλα στο επίπεδο μεταφοράς είναι το *TCP, Transmission Control Protocol* και το *UDP, User Datagram Protocol*. Το πρωτόκολλο TCP είναι *προσανατολισμένο στη σύνδεση (connection oriented)* ενώ το UDP *χωρίς σύνδεση (connectionless)*.

Τα πρωτόκολλα που είναι *προσανατολισμένα στη σύνδεση* πριν ξεκινήσουν τη μετάδοση των δεδομένων εγκαθιστούν μια σύνδεση από άκρο σε άκρο μεταξύ των κόμβων για να εξασφαλίσουν μια διαδρομή (νοητή σύνδεση) για τη μετάδοση των πακέτων. Όλα τα πακέτα μεταδίδονται μέσα από τήν ίδια νοητή σύνδεση. Αφού ξεκινήσει η μετάδοση, εξασφαλίζουν ότι τα δεδομένα θα φτάσουν στον παραλήπτη χωρίς σφάλματα. (Σημείωση: εδώ το βιβλίο χρησιμοποιεί τον όρο “πακέτα” με την ευρεία έννοια: στο επίπεδο μεταφοράς η μονάδα δεδομένων του TCP είναι το τμήμα – segment)

Αντίθετα στα πρωτόκολλα *χωρίς σύνδεση* η μετάδοση δεδομένων ξεκινά άμεσα χωρίς να έχει προηγηθεί επικοινωνία με τον παραλήπτη. Τα δεδομένα μεταδίδονται σε *αυτοδύναμα πακέτα* (datagrams) χωρίς την εγκατάσταση νοητής σύνδεσης. Τα πρωτόκολλα αυτά θεωρούνται αναξιόπιστα καθώς δεν εξασφαλίζουν ότι τα δεδομένα θα φτάσουν στο προορισμό τους.

Η πληροφορία που μεταφέρεται από άκρο σε άκρο στο επίπεδο μεταφοράς, οργανώνεται σε ακολουθία από ομάδες δεδομένων που ονομάζονται datagrams. Κάθε datagram μετράται σε octets δηλ. οκτάδες δεδομένων ή bytes και αντιμετωπίζεται απολύτως ανεξάρτητα από το δίκτυο.

Λάθος ορολογία του σχολικού βιβλίου στην προηγούμενη παράγραφο: Το TCP έχει *τμήματα (segments)* και όχι *datagrams*. Το UDP (πρωτόκολλο χωρίς σύνδεση)

έχει datagrams. Στο επίπεδο μεταφοράς, δεν υπάρχει η παραμικρή ιδέα για το ενδιάμεσο δίκτυο: η επικοινωνία θεωρείται ευθεία γραμμή. Στο επίπεδο Διαδικτύου, τα TCP segments και τα πακέτα UDP προφανώς ενθυλακώνονται σε IP datagrams και το καθένα αντιμετωπίζεται απολύτως ανεξάρτητα από το δίκτυο (μπορεί να ακολουθήσει διαφορετική διαδρομή, να διασπαστεί σε fragments κλπ).

Τι είναι τα octets; Αναφέρονται σε ομάδες δεδομένων των 8 bit, αυτό δηλαδή που σήμερα όλοι αποκαλούμε bytes. Ωστόσο το byte δεν ήταν πάντοτε 8 bit όπως σήμερα (ως byte ορίζεται το ελάχιστο πλήθος bit που αποθηκεύεται σε μια διεύθυνση μνήμης και παλιότερα – 1950 – δεν αντιστοιχούσε σε 8 bit). Για το σκοπό αυτό και προκειμένου να μην υπάρχει σύγχυση πολλές φορές στα δίκτυα χρησιμοποιείται ο όρος οκτάδα ή octet. Στις μέρες μας βέβαια μπορείτε να λέτε ελεύθερα byte!

4.1.1 Πρωτόκολλο TCP – Δομή Πακέτου

Προσοχή: Η αντίστοιχη ενότητα στο βιβλίο περιέχει διάφορα λάθη και ανακρίβειες, έχοντας ανακατέψει τις λειτουργίες των επιπέδων Μεταφοράς και Διαδικτύου. Σε αυτή την παράγραφο γράφουμε την πραγματικότητα, χρησιμοποιώντας το παράδειγμα του βιβλίου.

Παράδειγμα Σχολικού Βιβλίου: Έστω ότι θέλουμε να αποστείλουμε ένα μήνυμα μέσω ηλεκτρονικού ταχυδρομείου. Ο χρήστης θα γράψει το μήνυμα του στην αντίστοιχη εφαρμογή και θα συμπληρώσει την διεύθυνση ηλεκτρονικού ταχυδρομείου του παραλήπτη. Η διεύθυνση αυτή (μαζί με την αντίστοιχη του αποστολέα) αποτελούν μέρος της επικεφαλίδας που προστίθεται στο μήνυμα που δημιουργείται από το επίπεδο εφαρμογής.

Θυμηθείτε ότι το επίπεδο εφαρμογής, λειτουργεί με εντολές που είναι γενικά κατανοητές από τον άνθρωπο: τα προγράμματα σε αυτό το επίπεδο συνεννοούνται κατά βάση με εντολές στα αγγλικά που μπορούμε πολλές φορές να στείλουμε και χειροκίνητα. Για παράδειγμα μια συνομιλία με ένα διακομιστή ηλεκτρονικού ταχυδρομείου ξεκινά με το χαιρετισμό “helo” (ναι, είναι με ένα “l”) ή “ehlo”. Όλες αυτές οι εντολές και τα δεδομένα (κείμενο) του χρήστη πρέπει ωστόσο να μεταφερθούν μέσα από το επίπεδο μεταφοράς.

Το επίπεδο εφαρμογής δεν ενδιαφέρεται – και δεν γνωρίζει – τους περιορισμούς του φυσικού μέσου. Όσο αφορά ένα πρόγραμμα ταχυδρομείου, ο χρήστης μπορεί να γράψει και να στείλει όσο μεγάλο (ή μικρό) μήνυμα θέλει. Το πρόγραμμα φαίνεται

να επικοινωνεί απευθείας με το αντίστοιχο στην άλλη μεριά: οι λεπτομέρειες της πραγματικής επικοινωνίας κρύβονται στα παρακάτω επίπεδα.

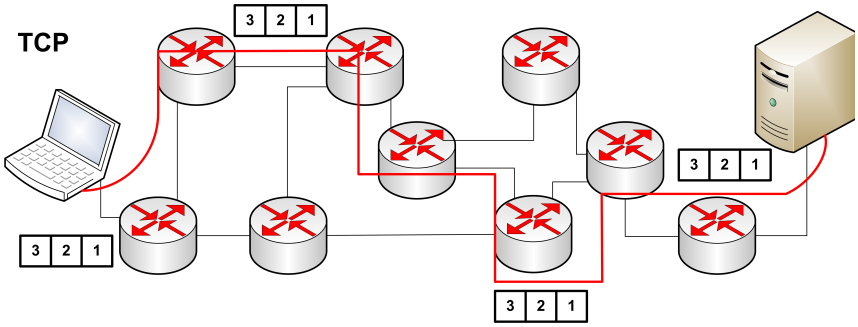
Ας υποθέσουμε λοιπόν ότι ο χρήστης έγραψε ένα μήνυμα μεγέθους 6000 octets (ή bytes, αν το προτιμάτε). Το επίπεδο μεταφοράς θα πρέπει να τα μεταφέρει μέσω του TCP, αφού πρώτα γίνει μια αρχική σύνδεση και συνεννόηση με τον παραλήπτη (το TCP είναι πρωτόκολλο με σύνδεση). Με ποιο τρόπο και για ποιο λόγο θα αποφασίσει το TCP να δημιουργήσει τη δική του μονάδα δεδομένων (τα τμήματα, ή segments) με κάποιο συγκεκριμένο μέγεθος; Θα μπορούσε να στείλει όλο το μήνυμα σε ένα τμήμα;

Σύμφωνα με αυτά που ξέρουμε η απάντηση είναι ναι: Το TCP μπορεί να δημιουργήσει ένα τμήμα των 6000 bytes: τα τμήματα του TCP ενθυλακώνονται πάντα σε αυτοδύναμα πακέτα IP, και αυτά με τη σειρά τους ενθυλακώνονται στην αντίστοιχη μονάδα δεδομένων του κατώτερου επίπεδου (π.χ. σε πλαίσια Ethernet). Στο επίπεδο Διαδικτύου, τα πακέτα IP μπορούν να υποστούν κατάτμηση (fragmentation) αν το μέγεθος τους είναι τέτοιο που δεν μπορούν να ενθυλακωθούν σε πλαίσια. Θα μπορούσε λοιπόν το TCP να αφήσει αυτή τη λειτουργία στο IP. Υπάρχει λόγος να μην το κάνει;

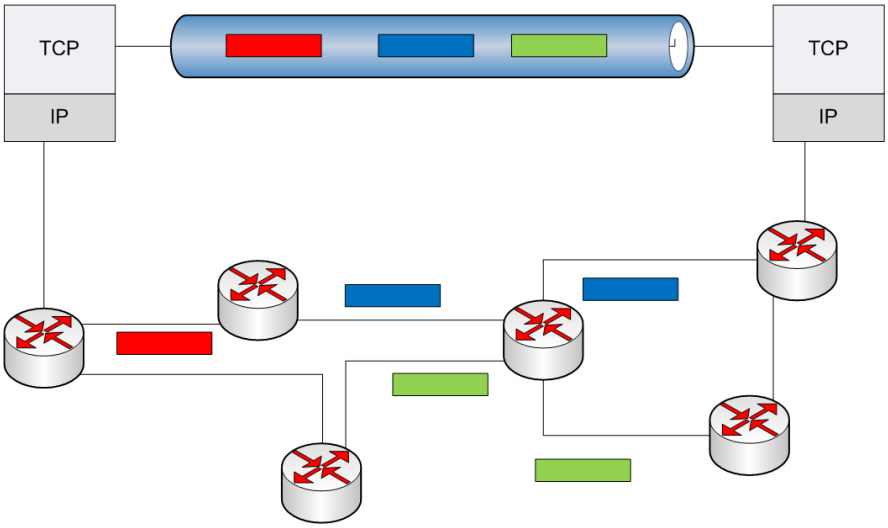
Ναι. Όταν τα αυτοδύναμα πακέτα IP διασπώνται σε fragments, η απόδοση μειώνεται. Το κάθε fragment έχει δική του επικεφαλίδα και άρα μεταφέρει λιγότερα χρήσιμα δεδομένα από ότι ένα μη-διασπασμένο αυτοδύναμο πακέτο. Επίσης αν ένα fragment χαθεί ή καταστραφεί, είναι πλέον αδύνατο να συναρμολογηθεί το αντίστοιχο αυτοδύναμο πακέτο IP. Όμως αυτό το πακέτο έχει μέσα του πολλά δεδομένα (ένα ολόκληρο “μεγάλου μεγέθους” τμήμα): το επίπεδο μεταφοράς θα χρειαστεί να ξαναστείλει όλο το τμήμα. Θυμηθείτε ότι το IP είναι πρωτόκολλο τύπου “best effort”: δεν παρέχει αξιοπιστία μετάδοσης και ούτε έχει κάποιο μηχανισμό να μεταδώσει ξανά fragment ή πακέτο IP που χάθηκε ή καταστράφηκε. Αυτό θα πρέπει να γίνει στο επίπεδο μεταφοράς.

Για να βελτιστοποιήσουμε την απόδοση, στην έναρξη της επικοινωνίας και οι δυο μεριές δηλώνουν το μέγιστο μέγεθος τμήματος που μπορούν να χρησιμοποιήσουν. Αυτό είναι γενικά γνωστό ως *Maximum Segment Size (MSS)*. Δεν γίνεται κάποια διαπραγμάτευση μεταξύ των δύο άκρων: είναι απλά μια δήλωση. Σε γενικές γραμμές, επιλέγεται μια τιμή τέτοια ώστε να μη χρειαστεί να γίνει IP fragmentation: μια τέτοια τιμή προφανώς είναι κοντά στη μέγιστη μονάδα μεταφοράς του φυσικού μέσου (MTU), αφού ληφθούν υπόψη και οι επικεφαλίδες που θα προστεθούν σε κάθε επίπεδο. Σημειώστε ότι δεν θα χρησιμοποιηθεί αναγκαστικά η τιμή MSS για όλα τα τμήματα: απλά είναι η μέγιστη δυνατή. Η πραγματική μπορεί να είναι μικρότερη και ρυθμίζεται και από άλλους παράγοντες όπως ο έλεγχος ροής (το πεδίο “παράθυρο”) και ο έλεγχος συμφόρησης.

Στο παράδειγμα μας, έστω ότι τελικά ανακαλύψαμε ότι μια κατάλληλη τιμή είναι τα 600 bytes. Τα αρχικά δεδομένα (6000 bytes) από το επίπεδο εφαρμογής θα γίνουν 10 τμήματα των 600 bytes στο επίπεδο μεταφοράς. Σε καθένα από αυτά τα 10 τμήματα θα προστεθεί (κατ'ελάχιστον) μια επικεφαλίδα 20 bytes για το TCP και μια ακόμα 20 bytes στο επίπεδο IP. Προφανώς το επίπεδο πρόσβασης δικτύου θα πρέπει να μπορεί να δημιουργήσει πλαίσια με μήκος δεδομένων τουλάχιστον 640 bytes.



Σχήμα 4.1: *Επικοινωνία TCP - ΛΑΘΟΣ*



Σχήμα 4.2: *Επικοινωνία TCP - ΣΩΣΤΗ*

Η εικόνα 4.1 στο βιβλίο σας είναι επίσης λάθος: ο συγγραφέας προσπαθεί να δείξει ότι υπάρχει ένα νοητό κύκλωμα στο TCP αλλά φτιάχνει μια συγκεκριμένη διαδρομή μέσα από δρομολογητές: οι δρομολογητές όμως δεν ασχολούνται με το επίπεδο μεταφοράς αλλά με το επίπεδο διαδικτύου. Όπως γνωρίζουμε το κάθε αυτοδύναμο IP πακέτο αντιμετωπίζεται χωριστά από τους δρομολογητές και πακέτα της ίδιας μετάδοσης μπορεί τελικά να ακολουθήσουν διαφορετικές διαδρομές μέσα από το

επικοινωνιακό υποδίκτυο. Η γραμμή που ενώνει εδώ τους κόμβους μέσα από μια συγκεκριμένη διαδρομή είναι άκυρη. Για ένα σωστό σχήμα δείτε την εικόνα 4.2 όπου φαίνεται καθαρά ότι όσο αφορά το TCP η επικοινωνία είναι μια ευθεία γραμμή (end to end) αλλά στην πραγματικότητα τα αυτοδύναμα πακέτα μπορεί να κινούνται από διαφορετικές διαδρομές.

Όταν τα τμήματα φτάσουν στο άλλο άκρο θα επανασυνδεθούν για να σχηματίσουν το αρχικό μήνυμα των 6000 οκτάδων. Καθώς στην πραγματικότητα τα τμήματα μεταφέρονται μέσω ενθυλάκωσης σε αυτοδύναμα πακέτα IP, είναι πιθανόν να φτάσουν με διαφορετική σειρά (κάθε IP πακέτο μπορεί να ακολουθήσει διαφορετική διαδρομή). Επίσης στην διαδρομή ενδεχομένως κάποια πακέτα IP να καταστραφούν: το πρωτόκολλο IP δεν παρέχει λειτουργίες αξιόπιστης μετάδοσης. Τα τμήματα που μεταφέρονται σε προβληματικά (ή χαμένα) πακέτα IP θα πρέπει να μεταδοθούν ξανά.

Ένα ακόμα πρόβλημα που προκύπτει και πρέπει να λυθεί από το πρωτόκολλο TCP, είναι ο διαχωρισμός των δεδομένων της κάθε σύνδεσης: ανά πάσα στιγμή ένας υπολογιστής – πελάτης μπορεί να είναι συνδεδεμένος με πολλαπλές συνδέσεις σε ένα εξυπηρετητή. Φανταστείτε για παράδειγμα ότι με τον υπολογιστή σας βλέπετε μια ιστοσελίδα από ένα εξυπηρετητή. Κάνετε κλικ σε ένα σύνδεσμο και αρχίζετε να κατεβάζετε κάποιο αρχείο από την ίδια ιστοσελίδα. Πως γνωρίζει ο φυλλομετρητής σας ποια δεδομένα ανήκουν στην ιστοσελίδα και ποια στο αρχείο που κατεβάζετε, αφού μάλιστα είναι από τον ίδιο εξυπηρετητή;

Σημειώστε ότι αυτό το πρόβλημα δεν υπάρχει όταν αναφερόμαστε σε διαφορετικούς εξυπηρετητές: εκεί είναι δυνατόν να γίνει ο διαχωρισμός ήδη από το πρωτόκολλο δικτύου με βάση τη διεύθυνση IP. Ας δούμε τώρα το ίδιο πρόβλημα από τη μεριά του εξυπηρετητή: είναι δυνατόν (και συμβαίνει συχνά) το ίδιο μηχάνημα να παρέχει πολλές υπηρεσίες. Π.χ. σε μια μικρή εταιρεία δεν είναι σπάνιο ένας εξυπηρετητής να διαθέτει ταυτόχρονα υπηρεσία ηλεκτρονικού ταχυδρομείου (email), ιστοσελίδων (web), μεταφοράς αρχείων (ftp) κ.α. Πως ο εξυπηρετητής διαχωρίζει ποια τμήματα TCP αναφέρονται σε κάθε υπηρεσία;

Όσο αφορά το TCP υπάρχει ένα είδος *πολυπλεξίας* δίνεται δηλ. η δυνατότητα πολλές διεργασίες μέσα στον ίδιο τερματικό κόμβο (host) να χρησιμοποιούν τις υπηρεσίες του πρωτοκόλλου *ταυτόχρονα*. Η δυνατότητα αυτή εξασφαλίζεται με τα πεδία *Θύρας Προέλευσης* και *Θύρας Προορισμού*. Όπως ακριβώς το πρωτόκολλο IP μας πηγαίνει μέχρι ένα συγκεκριμένο μηχάνημα χρησιμοποιώντας τη διεύθυνση IP, οι θύρες μας οδηγούν σε μια συγκεκριμένη εφαρμογή πελάτη ή εξυπηρετητή (συγκεκριμένη σύνδεση) όταν έχουμε πλέον φτάσει στον προορισμό μας.

Στη φάση της επανασύνθεσης του αρχικού μηνύματος, το TCP πρέπει να γνωρίζει ποια είναι η προέλευση (source) και ποιος ο προορισμός (destination) του μηνύμα-

τος. Το TCP εξασφαλίζει την *αξιοπιστία* της σύνδεσης με:

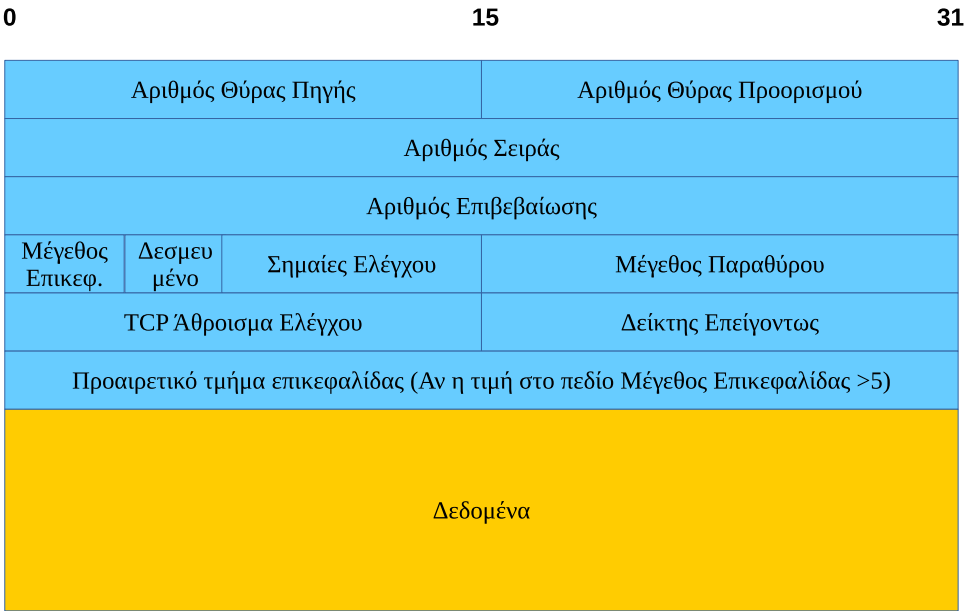
- Την εγκατάσταση νοητής σύνδεσης από την προέλευση στο προορισμό
- Τον τεμαχισμό των δεδομένων σε τμήματα κατάλληλα για το δίκτυο
- Την επιβεβαίωση στην παραλαβή των δεδομένων
- Την τοποθέτηση των τμημάτων στη σωστή σειρά κατά την παραλαβή (και την επαναμετάδοση τμημάτων που χάθηκαν ή καταστράφηκαν)

Σχήμα 4.3: *Τμήμα TCP*

Όλες οι πληροφορίες που είναι απαραίτητες για τον έλεγχο και την ανασύνθεση του αρχικού μηνύματος περιέχονται στην *επικεφαλίδα (header)* που δημιουργείται στο σχηματισμό του τμήματος. Η επικεφαλίδα είναι μια σειρά από οκτάδες που προστίθενται στην αρχή του τμήματος, πριν από τα πραγματικά δεδομένα (σχήμα 4.3).

Το ελάχιστο μέγεθος της επικεφαλίδας είναι 20 οκτάδες και το μέγιστο 60, αν υπάρχει το προαιρετικό τμήμα. Στο σχήμα 4.4 βλέπουμε τα πεδία της επικεφαλίδας του TCP που εξετάζουμε παρακάτω.

- **Αριθμός Θύρας Προέλευσης (Source Port number) και Αριθμός Θύρας Προορισμού (Destination Port Number):** Όπως αναφέραμε προηγουμένως, οι δύο αυτοί αριθμοί χρησιμεύουν στην ταυτοποίηση διαφορετικών συνομιλιών TCP. Για παράδειγμα ένα πρόγραμμα εξυπηρέτησης ηλεκτρονικού ταχυδρομείου χρησιμοποιεί (βάση προτύπου) τη θύρα TCP 25, ενώ ένα αντίστοιχο ιστοσελίδων τη θύρα 80. Αν οι δύο αυτές υπηρεσίες εκτελούνται στο ίδιο μηχάνημα, όλα τα τμήματα που λαμβάνονται με θύρα προορισμού 25 προωθούνται στο ηλεκτρονικό ταχυδρομείο ενώ αυτά με θύρα προορισμού 80 στο πρόγραμμα εξυπηρέτησης ιστοσελίδων. Αν ο ίδιος πελάτης (από την ίδια διεύθυνση IP) συνδεθεί ταυτόχρονα και στις δύο υπηρεσίες, τα τμήματα θα έχουν επίσης και διαφορετικές θύρες αποστολέα: έτσι και τα τμήματα – απαντήσεις από τον εξυπηρετητή θα μπορούν αντίστοιχα να διαχωριστούν στις αντίστοιχες εφαρμογές στον πελάτη. *Το παράδειγμα στο βιβλίο σας είναι λάθος:* Αν οι συνδέσεις προέρχονται από διαφορετικούς υπολογιστές δεν μπορούμε να τα ξεχωρίσουμε με βάση τη θύρα αποστολέα. Οι θύρες αποστολέα επιλέγονται τυχαία στους πελάτες και μπορεί διαφορετικά μηχανήματα να χρησιμοποιούν την ίδια θύρα αποστολέα. Όμως ο διαχωρισμός γίνεται πλέον μέσω της διεύθυνσης IP στο επίπεδο δικτύου. Όταν το πρόγραμμα εξυπηρέτησης απαντά



Σχήμα 4.4: *Πεδία Επικεφαλίδας TCP Τμήματος*

σε ένα πελάτη, προφανώς τα πεδία των θυρών αντιστρέφονται μεταξύ τους (η θύρα προέλευσης γίνεται αποστολής και η αποστολής προέλευσης). Τα πεδία αυτά έχουν μέγεθος 16 bit το καθένα, επιτρέποντας ένα μέγιστο 2^{16}=65536 θυρών.

- **Αριθμός Σειράς (Sequence Number):** Ο αριθμός αυτός χρησιμεύει ώστε ο παραλήπτης να τοποθετεί τα τμήματα στη σωστή σειρά καθώς ανασυνθέτει τα αρχικά δεδομένα. Τα τμήματα μπορεί να έχουν παραληφθεί με διαφορετική σειρά από τη σειρά αποστολής καθώς ταξιδεύουν μέσα στο δίκτυο ενθυλακωμένα σε αυτοδύναμα πακέτα IP. Το TCP αριθμεί τα τμήματα με βάση τα octets, έτσι αν κάθε τμήμα αποτελείται από 600 octets, το πρώτο έχει αριθμό σειράς 0, το δεύτερο 600, το τρίτο 1200 κλπ (Σημείωση: πρόκειται για μια απλούστευση του σχολικού βιβλίου, τα πράγματα δεν είναι ακριβώς έτσι. Η σωστότερη εξήγηση υπάρχει στο βιβλίο αλλά είναι εκτός ύλης). Το πεδίο αυτό έχει μέγεθος 32 bit.

- **Αριθμός Επιβεβαίωσης (Acknowledgement):** Ο αριθμός αυτός χρησιμοποιείται για να εξασφαλιστεί ότι κάθε τμήμα έχει φτάσει στον προορισμό του. Όταν ο παραλήπτης στο άλλο άκρο παραλάβει το τμήμα, στέλνει ένα νέο τμήμα επιβεβαίωσης (ACK) με συμπληρωμένο το πεδίο αυτό. Π.χ. ένα τμήμα επιβεβαίωσης με αριθμό επιβεβαίωσης 1201 σημαίνει ότι έχουν φτάσει όλα τα δεδομένα μέχρι και την οκτάδα 1200. Αν ο αποστολέας δεν παραλάβει

τμήμα επιβεβαίωσης μέσα σε ένα συγκεκριμένο χρονικό διάστημα, θεωρεί ότι το τμήμα έχει χαθεί και μεταδίδεται ξανά. Το πεδίο αυτό έχει μέγεθος 32 bit, όπως και ο αριθμός σειράς.

- **Μέγεθος Παραθύρου (Window):** Για να επιταχυνθεί η επικοινωνία το TCP δεν περιμένει παραλαβή της επιβεβαίωσης για να στείλει το επόμενο τμήμα. Όμως δεν είναι δυνατόν να αποστέλλονται συνεχώς δεδομένα γιατί ένας γρήγορος αποστολέας στο ένα άκρο μπορεί να ξεπεράσει την ταχύτητα με την οποία μπορεί να δεχθεί δεδομένα ένας πιο αργός παραλήπτης. Στο πεδίο Window το κάθε άκρο δηλώνει πόσα νέα δεδομένα μπορεί να απορροφήσει κάθε φορά, θέτοντας σε αυτό την τιμή των ελεύθερων οκτάδων του ενταμιευτή του (Ο ενταμιευτής ή buffer είναι ο προσωρινός χώρος όπου αποθηκεύονται τα τμήματα προκειμένου να επανασυνδεθούν και να προωθηθούν στο παραπάνω επίπεδο). Ένας παραλήπτης μπορεί να λαμβάνει δεδομένα πιο γρήγορα από ότι μπορεί να τα επεξεργαστεί με αποτέλεσμα ο διαθέσιμος χώρος στον ενταμιευτή να μειώνεται συνέχεια. Αν ο χώρος αυτός γεμίσει ο αποστολέας πρέπει προσωρινά να σταματήσει την αποστολή νέων δεδομένων διαφορετικά αυτά θα απορριφθούν. Ο παραλήπτης δηλώνει με το πεδίο Window ότι είναι έτοιμος να δεχτεί νέα δεδομένα. Το πεδίο αυτό έχει μέγεθος 16 bit.

- **Άθροισμα Ελέγχου (TCP Checksum):** Το πεδίο αυτό περιέχει ένα άθροισμα ελέγχου όλων των οκτάδων του τμήματος (επικεφαλίδας και δεδομένων). Στον υπολογισμό του αθροίσματος ελέγχου θεωρείται ότι το συγκεκριμένο πεδίο έχει τιμή μηδέν. Ο παραλήπτης στο άλλο άκρο υπολογίζει ξανά το άθροισμα από την αρχή και το συγκρίνει με αυτό που παρέλαβε. Αν τα δυο αποτελέσματα δεν είναι ίδια, το τμήμα θεωρείται κατεστραμμένο και απορρίπτεται. Το πεδίο αυτό έχει μέγεθος 16 bit.

- **Μέγεθος Επικεφαλίδας (Data Offset):** Το πεδίο αυτό καθορίζει το μέγεθος της επικεφαλίδας σε λέξεις των 32bit. Για παράδειγμα αν η τιμή του πεδίου αυτού είναι 5, η επικεφαλίδα είναι 5X32 bit = 160 bit ή 20 bytes. (Μπορείτε απλά να πολλαπλασιάσετε αυτή τη τιμή με το 4 για να πάρετε τα bytes της επικεφαλίδας). Αν η επικεφαλίδα είναι μεγαλύτερη από 20 bytes (τιμή πεδίου μεγαλύτερη από 5) θα υπάρχουν επιπλέον επιλογές TCP στο *Προαιρετικό τμήμα επικεφαλίδας*. Αν τα δεδομένα του προαιρετικού τμήματος δεν είναι πολλαπλάσια των 32bit (ώστε να συμπληρώνουν όλη τη γραμμή της επικεφαλίδας), συμπληρώνονται με μηδενικά στο τέλος (padding). Το πεδίο “Μέγεθος Επικεφαλίδας” έχει μέγεθος 4 bit.

- **Οι σημαίες ελέγχου (flags)** είναι εννέα πεδία του ενός bit το καθένα και σηματοδοτούν διάφορες καταστάσεις που αφορούν το χειρισμό των συνδέσεων. Τα σημαντικότερα από αυτά είναι:

1. **URG, Urgent Pointer, Δείκτης Επείγοντος:** Το πεδίο αυτό χρησιμοποιείται για να πληροφορήσει το άλλο άκρο για κάτι σημαντικό, π.χ. να προχωρήσει επειγόντως στην επεξεργασία της συγκεκριμένης οκτάδας. Αυτό μπορεί να συμβαίνει π.χ. αν ο χρήστης ζητήσει τη διακοπής της επικοινωνίας στέλνοντας ένα χαρακτήρα ελέγχου (π.χ. πιέζοντας CTRL+C (διακοπή) σε μια μεταφορά αρχείου μέσω FTP σε ένα σύστημα UNIX)

2. **ACK, Acknowledgement, Επιβεβαίωση:** Όταν τίθεται τιμή 1 σε αυτό το πεδίο, σημαίνει ότι το συγκεκριμένο τμήμα περιέχει επιβεβαίωση δεδομένων. Ο παραλήπτης του τμήματος θα πρέπει να εξετάσει το πεδίο "Αριθμός Επιβεβαίωσης"

3. **PSH, Push, Προώθηση:** Το πεδίο αυτό ενημερώνει τον παραλήπτη ότι πρέπει να προωθήσει όσο το δυνατόν πιο γρήγορα τα περιεχόμενα του τμήματος στο επίπεδο εφαρμογής

4. **RST, Reset, Επανεκκίνηση:** Το πεδίο αυτό επισημαίνει επανεκκίνηση / καθαρισμό της σύνδεσης

5. **SYN, Synchronize, Συγχρονισμός:** Το πεδίο αυτό χρησιμεύει (μαζί με τον αριθμό σειράς) για το συγχρονισμό της εγκατάστασης μιας νέας σύνδεσης

6. **FIN, Finalize, Ολοκλήρωση:** Το πεδίο αυτό ενημερώνει ότι ο αποστολέας έχει ολοκληρώσει την αποστολή δεδομένων

Η δομή του τμήματος TCP περιέχει όλες τις πληροφορίες που απαιτούνται για την παροχή επικοινωνίας με σύνδεση:

- *Την εγκατάσταση σύνδεσης* με συμφωνημένες προδιαγραφές επικοινωνίας μεταξύ των δύο άκρων

- *Την αξιοπιστία* στη μετάδοση δεδομένων. Όποια τμήματα χαθούν ή καταστραφούν θα μεταδοθούν ξανά

- *Τον έλεγχο ροής δεδομένων* που επιτυγχάνεται με το πεδίο Window και έχει σκοπό να μην υπερφορτωθεί ένας αργός παραλήπτης από ένα γρήγορο αποστολέα

- *Τον έλεγχο συμφόρησης δεδομένων:* που εξασφαλίζει ότι ένα αργό κανάλι επικοινωνίας δεν θα πλημμυρίσει με δεδομένα με κίνδυνο κατάρρευσης

4.1.2 Πρωτόκολλο UDP – Δομή Πακέτου

Το πρωτόκολλο UDP, User Datagram Protocol, βρίσκεται επίσης στο επίπεδο μεταφοράς αλλά είναι ένα αρκετά απλούστερο πρωτόκολλο σε σχέση με το TCP. Το UDP χρησιμοποιεί αυτοδύναμα πακέτα για τη μεταφορά των δεδομένων του και είναι πρωτόκολλο χωρίς σύνδεση: η μετάδοση ξεκινά αμέσως χωρίς να υπάρχει από πριν συνεννόηση με την άλλη πλευρά.

Μερικές ακόμα σημαντικές διαφορές με το TCP είναι:

- Το UDP δεν μπορεί να τεμαχίσει δεδομένα. Αν επιθυμούμε κάτι τέτοιο θα πρέπει να το αναλάβει το επίπεδο εφαρμογής
- Το UDP δεν εξασφαλίζει αξιόπιστη μετάδοση δεδομένων. Τα πακέτα είναι αυτοδύναμα και δεν παρέχεται αναμετάδοση σε περίπτωση απώλειας ή καταστροφής πακέτων. Αν κάτι τέτοιο είναι επιθυμητό, θα πρέπει και πάλι να το αναλάβει το επίπεδο εφαρμογής

Από την άλλη, το UDP είναι αρκετά απλούστερο πρωτόκολλο. Η επικεφαλίδα του είναι μόνο 8 οκτάδες, άρα διαθέτει περισσότερο χώρο για να μεταφέρει χρήσιμα δεδομένα. Καθώς δεν χρειάζεται εγκατάσταση σύνδεσης η μετάδοση μπορεί να ξεκινήσει άμεσα. Η έλλειψη ελέγχων σημαίνει συνήθως μεγαλύτερη ταχύτητα μετάδοσης δεδομένων και δεν χρησιμοποιούνται πόροι του δικτύου για τη μετάδοση πληροφοριών που δεν αποτελούν πραγματικά δεδομένα χρήστη (όπως αναφέρει το σχολικό βιβλίο, λιγότερο overhead, λιγότερη επιβάρυνση δηλ. από δεδομένα ελέγχου κλπ).

Σχήμα 4.5: *Πεδία Επικεφαλίδας UDP Πακέτου*

Η επικεφαλίδα του UDP έχει μέγεθος 8 οκτάδων (σχήμα 4.5) και τα πεδία της είναι:

- **Αριθμοί Θύρας Προέλευσης και Προορισμού (Source / Destination Ports:** Με μέγεθος 16 bit το καθένα, εξυπηρετούν τον ίδιο ακριβώς σκοπό με τις θύρες του TCP
- **Μήκος Datagram (Length):** Το ελάχιστο μέγεθος είναι 8 bytes (μόνο η επικεφαλίδα δηλαδή) και το μέγιστο 65535 bytes (64 Kb) μαζί με την επικεφαλίδα. Το πεδίο αυτό έχει (προφανώς) μέγεθος 16 bit
- **Το Άθροισμα Ελέγχου (Checksum):** Προαιρετικό πεδίο μεγέθους 16 bit. Χρησιμεύει για επαλήθευση ορθότητας της επικεφαλίδας και των δεδομένων στον παραλήπτη και λειτουργεί παρόμοια με το αντίστοιχο πεδίο του TCP

Είναι προφανές ότι το πρωτόκολλο TCP χρησιμοποιείται όπου απαιτείται αξιόπιστη μεταφορά των δεδομένων ενώ το UDP σε εφαρμογές που δεν έχει τόση σημασία η πληρότητα της μεταφοράς των δεδομένων σε σχέση με την ταχύτητα που θα παραληφθούν.

Τέτοιες εφαρμογές είναι:

- Όσες μεταδίδουν εικόνα, βίντεο και ήχο σε πραγματικό χρόνο (ρόες – streams – δεδομένων). Για παράδειγμα εφαρμογές τηλεδιάσκεψης, εφαρμογές τηλεόρασης μέσω Διαδικτύου, τηλεφωνία μέσω IP (VoIP), Internet Radio κλπ. Στις περιπτώσεις αυτές μας ενδιαφέρει τα δεδομένα να φτάνουν στη σωστή χρονική στιγμή ενώ μερικές απώλειες δεν είναι σημαντικές αφού επηρεάζουν μόνο για λίγο την ποιότητα αναπαραγωγής.
- Εξυπηρετητές (servers) οι οποίοι απαντούν σε μικρά αιτήματα τεράστιου αριθμού από πελάτες όπως π.χ. σε δικτυακά online παιχνίδια. Οι συγκεκριμένοι εξυπηρετητές μπορούν να αντιμετωπίσουν έτσι αρκετά μεγαλύτερο φορτίο εργασίας από ότι αν χρησιμοποιούσαν TCP, καθώς το UDP πρωτόκολλο είναι αρκετά απλούστερο και δεν χρειάζεται να ανταλλάσσουν πληροφορίες ελέγχου και κατάστασης της σύνδεσης.

Όπως αναφέραμε ωστόσο, αν θέλουμε να έχουμε αξιοπιστία, κατατεμαχισμό δεδομένων ή έλεγχο ροής στο UDP, θα πρέπει να μεταφέρουμε αυτές τις ενέργειες στο επίπεδο εφαρμογής. Υπάρχει επίσης το πρόβλημα της δικτυακής συμφόρησης που προκύπτει όταν κάποιος αποστολέας UDP πλημμυρίσει το δίκτυο με πακέτα. Για το σκοπό αυτό οι δρομολογητές πρέπει να χρησιμοποιούν τεχνικές ελέγχουν ώστε να μπορούν να απορρίπτουν ή να αποθηκεύουν προσωρινά πακέτα IP που ενθυλακώνουν UDP πακέτα για να αποφεύγεται η κατάρρευση (Hint: Το πακέτο IP περιέχει πεδίο στην επικεφαλίδα που αναγράφει από ποιο πρωτόκολλο του επιπέδου μεταφοράς προέρχονται τα δεδομένα που μεταφέρει. Το σχολικό βιβλίο εδώ γράφει για άλλη μια φορά ότι οι δρομολογητές απορρίπτουν πακέτα UDP, που είναι, φυσικά, **λάθος**).

Κεφάλαιο 5

Επεκτείνοντας το Δίκτυο – Δίκτυα Ευρείας Περιοχής

Εισαγωγή στα Δίκτυα Ευρείας Περιοχής

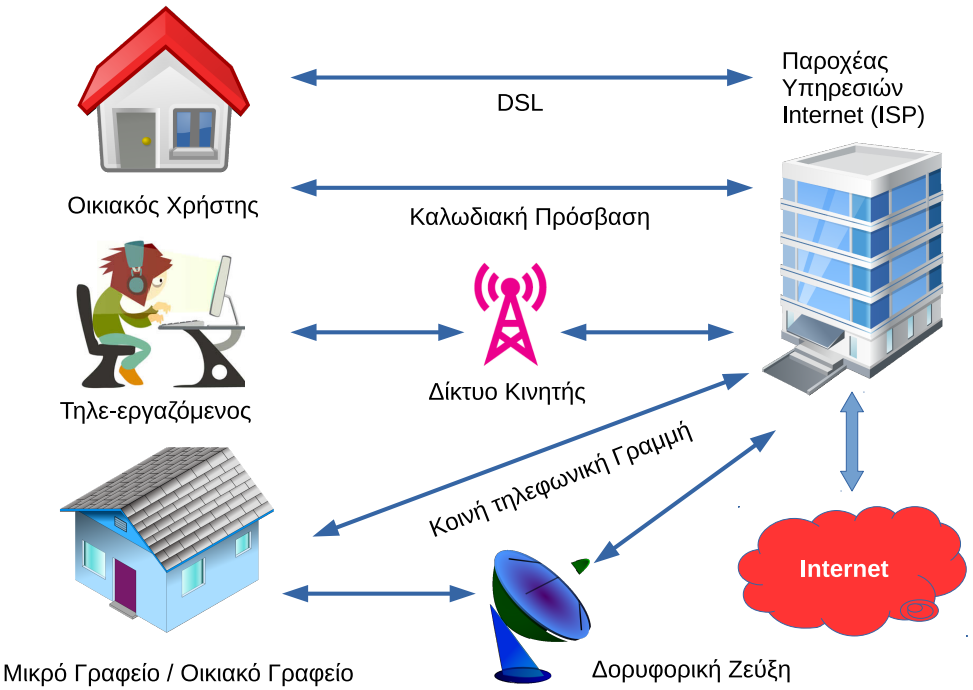
Τα τοπικά δίκτυα αποτελούν πολύ καλή λύση για επικοινωνία όταν η απόσταση που χρειάζεται να καλυφθεί είναι μικρή. Για μεγαλύτερες γεωγραφικές εκτάσεις, αναπτύσσονται τα δίκτυα ευρείας περιοχής (WAN, Wide Area Networks). Η επέκταση των τοπικών δικτύων σε δίκτυα ευρείας περιοχής επιτυγχάνεται χρησιμοποιώντας κατάλληλες γραμμές σύνδεσης και δικτυακά εξαρτήματα όπως modems, γέφυρες, δρομολογητές κ.α.

Για την ανάπτυξη γραμμών WAN μπορεί να χρησιμοποιούνται δίκτυα μεταγωγής (κυκλώματος ή πακέτου), δορυφορικές συνδέσεις, μικροκυματικές ζεύξεις, οπτικές ίνες ή σύστημα καλωδιακής τηλεόρασης.

Όσο αφορά το χρήστη, το δίκτυο ευρείας περιοχής φαίνεται να λειτουργεί με τον ίδιο ακριβώς τρόπο με το LAN. Αν το WAN έχει υλοποιηθεί με σωστές τεχνικές, δεν έχει καμιά διαφορά στη συμπεριφορά με το LAN (είναι όπως λέμε *διάφανο*).

Είναι αρκετά δύσκολο για μια εταιρεία να εγκαταστήσει και να διαχειριστεί τις δικές της γραμμές WAN. Συνήθως τις νοικιάζει από κάποιο τηλεπικοινωνιακό φορέα ο οποίος διαθέτει ήδη τις γραμμές και τον απαραίτητο εξοπλισμό. Οι τεχνολογίες που χρησιμοποιούνται στις υπηρεσίες δικτύων ευρείας περιοχής είναι:

- Επιλεγόμενες τηλεφωνικές γραμμές (κοινό τηλεφωνικό δίκτυο)
- Μόνιμες ή μισθωμένες γραμμές



Σχήμα 5.1: *Επιλογές Σύνδεσης σε WAN*

- Πρότυπο X.25
- Πρότυπο Frame Relay
- Γραμμές ISDN
- ATM (Asychronous Transfer Mode, Ασύγχρονος Τρόπος Μεταφοράς)
- Γραμμές xDSL
- Τεχνολογίες FTTH (Fiber To The Home, Οπτική Ίνα για Οικιακή Χρήση) και Metro Ethernet (Μητροπολιτικό δίκτυο βασισμένο σε τεχνολογία Ethernet)
- Ασύρματες και Δορυφορικές ζεύξεις

Από τις παραπάνω τεχνολογίες, η X.25 και Frame Relay έχουν ουσιαστικά ήδη καταργηθεί.

5.1 Εγκατεστημένο Τηλεφωνικό Δίκτυο

Η κανονική τηλεφωνική εγκατάσταση αποτελείται από ένα ζευγάρι χάλκινων καλωδίων που εγκαθίσταται από μια τηλεφωνική εταιρεία. Τα χάλκινα καλώδια που χρησιμοποιούνται στο τηλεφωνικό δίκτυο έχουν αρκετό εύρος ζώνης και μπορούν να μεταφέρουν αρκετά μεγαλύτερες συχνότητες από αυτές που χρησιμοποιούνται για τη μεταφορά φωνής. Στις συνδέσεις DSL αυτό το έξτρα εύρος ζώνης χρησιμοποιείται για να μεταφέρει πληροφορίες χωρίς να παρεμβάλλει τις επικοινωνίες φωνής που γίνονται ταυτόχρονα μέσα στην ίδια γραμμή.

Στην τηλεφωνική συνομιλία, οι συχνότητες που χρησιμοποιούνται είναι από 0 – 3400 Hz. Οι συχνότητες αυτές έχουν επιλεχθεί καθώς εκεί βρίσκεται η περιοχή ομιλίας της ανθρώπινης φωνής. Ο περιορισμός των συχνοτήτων επιτρέπει επίσης στην τηλεφωνική εταιρεία να πακετάρει πολλά καλώδια σε μικρό χώρο χωρίς να ανησυχεί για παρεμβολές (crosstalk) μεταξύ τους. Η περιοχή συχνοτήτων ομιλίας είναι πολύ μικρή σε σχέση για παράδειγμα με τις συχνότητες που μπορεί να αναπαράγει ένα στερεοφωνικό συγκρότημα (από 20 Hz – 200000 Hz). Τα τηλεφωνικά καλώδια έχουν τη δυνατότητα να μεταφέρουν και να χειρισθούν σήματα συχνότητας αρκετών εκατομμυρίων κύκλων (σήματα τάξης MHz). Τα σύγχρονα μηχανήματα στέλνουν ψηφιακά και όχι αναλογικά δεδομένα και μπορούν να χρησιμοποιήσουν με ασφάλεια πολύ μεγαλύτερο εύρος ζώνης της τηλεφωνικής γραμμής χωρίς πρόβλημα παρεμβολών.

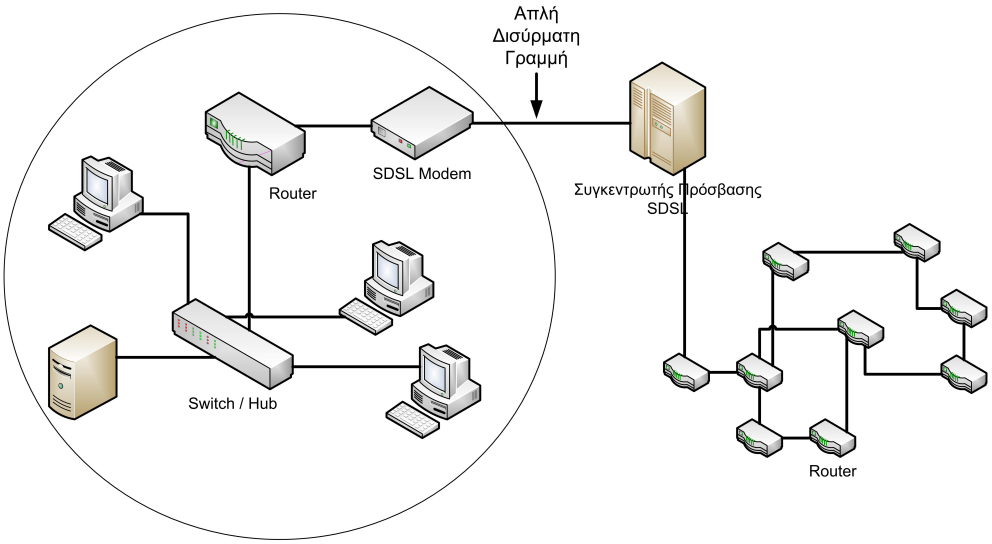
5.1.4 Τεχνολογίες Ψηφιακής Συνδρομητικής Γραμμής (xDSL)

Το ακρωνύμιο DSL προέρχεται από τις λέξεις *Digital Subscriber Line* και αποτελεί μια τεχνολογία που μετατρέπει την απλή τηλεφωνική γραμμή σε ένα δίαυλο μεταφοράς ψηφιακών δεδομένων υψηλής ταχύτητας και μεγάλου εύρους ζώνης με τη χρήση ειδικών modems που τοποθετούνται στα άκρα της γραμμής. Τα modems αυτά χρησιμοποιούν αισθητά μεγαλύτερες συχνότητες από αυτές που χρησιμοποιούνται για τη φωνή (όπως είδαμε στην προηγούμενη ενότητα η τηλεφωνική γραμμή μπορεί να τις μεταφέρει) και για το λόγο αυτό ονομάζονται και *broadband modems*. Κατά τα άλλα τα broadband modems λειτουργούν με τον ίδιο τρόπο λειτουργίας των κλασικών modems, μετατρέπουν δηλ. τη ροή ψηφιακού σήματος σε αναλογικό σήμα υψηλού ρυθμού (υψηλής συχνότητας). Η γραμμή μπορεί να μεταφέρει ταυτόχρονα χωρίς πρόβλημα τη φωνή και τα δεδομένα καθώς οι συχνότητες που χρησιμοποιούνται για τις δυο μεταδόσεις απέχουν αρκετά μεταξύ τους και μπορούν να ξεχωρίσουν εύκολα (αυτή τη δουλειά κάνει το φίλτρο ή ο διαχωριστής (splitter) που βάζουμε στην τηλεφωνική γραμμή).

Στη μετάδοση δεδομένων DSL χρησιμοποιούνται διάφορες τεχνολογίες διαμόρφωσης οι οποίες επιτυγχάνουν διαφορετικές ταχύτητες. Το διαθέσιμο εύρος ζώνης της γραμμής χωρίζεται σε τρία κανάλια:

- Ένα για τη μετάδοση φωνής
- Ένα για τη μετάδοση δεδομένων προς τα πάνω (από το συνδρομητή προς τον παροχέα), γνωστό ως *upstream*
- Ένα για τη μετάδοση δεδομένων προς τα κάτω (από τον παροχέα προς το συνδρομητή), γνωστό ως *downstream*

Οι επιδόσεις που επιτυγχάνονται διαφέρουν ανάλογα με το modem που θα συνδέσουμε. Με την τεχνολογία DSL επιτυγχάνονται ταχύτητες μέχρι 52 Mbps downstream και 12 Mbps upstream ενώ μεταδίδεται ταυτόχρονα και το αναλογικό σήμα φωνής.



Σχήμα 5.2: *Πρόσβαση Τοπικού Δικτύου σε Δίκτυο Ευρείας Περιοχής*

Οι παραλλαγές xDSL υποστηρίζουν *συμμετρική ή ασύμμετρη* μετάδοση δεδομένων. Στη συμμετρική μετάδοση η ταχύτητα είναι ίδια και προς τις δυο κατευθύνσεις (upstream και downstream) ενώ στην ασύμμετρη διαφορετικές (το upstream είναι μικρότερο). Κάθε παραλλαγή είναι κατάλληλη για συγκεκριμένη χρήση:

- Η ασύμμετρη μετάδοση είναι κατάλληλη για χρήση όπου απαιτείται κατά βάση μεγαλύτερη ταχύτητα downstream, δηλαδή προς το χρήστη (π.χ. για πρόσβαση σε ιστοσελίδες και κατέβασμα αρχείων)
- Η συμμετρική μετάδοση ενδείκνυται ως υποκατάστατο μισθωμένης γραμμής

E1 και όπου απαιτείται υψηλή ταχύτητα μετάδοσης και προς τις δύο κατευθύνσεις (π.χ. για τηλεδιάσκεψη)

Οι βασικές παραλλαγές xDSL είναι A(symmetric)DSL, S(ymmetric)DSL, H(igh bit rate)DSL και V(ery high bit rate)DSL.

Τεχνολογία	**Σημασία**	**Αριθμός Ζευγών**	**Ταχύτητα**	**Μέγιστη Απόσταση**
ADSL	Asymmetric DSL	1	8 Mbps Downstream 1,5 Mbps upstream	3 Km 6,6 – 7,5 Km
ADSL Lite		1	1 Mbps Downstream 384 Kbps upstream	
HDSL	High-bit-rate DSL	2 3	2 Mbps full duplex (E1) 1,5 Mbps full duplex (T1)	3,5 – 4,5 Km
SDSL	Single-line DSL	1	2 Mbps full duplex (E1) 1,5 Mbps full duplex (T1)	3 Km
VDSL	Very-high-bit-rate DSL	1	13 – 52 Mbps Downstream 1,5 – 12 Mbps upstream	0,3 – 1,4 Km

Πίνακας 5.1: *Τεχνολογίες x-DSL*

Η ADSL (Asymmetric Digital Subscriber Line) παρέχεται στους περισσότερους οικιακούς χρήστες στην Ελλάδα. Η τεχνολογία προσφέρει μεγάλες ταχύτητες δεδομένων (κατάλληλη για φωνή, δεδομένα, κινούμενη εικόνα, γραφικά) και ταυτόχρονα μετάδοση φωνής. Κύριο χαρακτηριστικό της τεχνολογίας είναι ότι η μετάδοση γίνεται με *ασύμμετρο τρόπο* με το ρυθμό λήψης (downstream) να φτάνει μέχρι 8 Mbps και αποστολής (upstream) μέχρι 1 Mbps. Το εύρος ζώνης αυτό παρέχεται εξ'ολοκλήρου στο χρήστη (δεν το μοιράζεται με άλλους χρήστες) και η σύνδεση είναι συνέχεια ενεργή (always on), σε αντίθεση με τις παλιού τύπου συνδέσεις όπου γίνεται κλήση για τη σύνδεση και στο τέλος της επικοινωνίας γίνεται αποσύνδεση. Η απόδοση της ADSL εξαρτάται σημαντικά από την απόσταση του χρήστη από τον τηλεπικοινωνιακό πάροχο (και από τη διατομή του καλωδίου που χρησιμοποιείται). Επιτυγχάνονται οι παρακάτω ταχύτητες:

- 1,5 MBps για απόσταση 5,5 Km
- 2,0 Mbps για απόσταση 4,9 Km
- 6,3 Mbps για απόσταση 3,6 Km
- 8.4 Mbps για απόσταση 2,7 Km

Υπάρχουν επίσης οι πιο εξελιγμένες εκδόσεις ADSL, η *ADSL2 και ADSL2+* που παρέχουν μεγαλύτερες ταχύτητες αξιοποιώντας με διαφορετικό τρόπο το εύρος ζώνης του καλωδίου. Η μέγιστη ταχύτητα στο ADSL2+ είναι τα 24 Mbps downstream και

1 Mbps upstream (ή σε περίπτωση που υλοποιεί το πρότυπο ITU G992.5 Annex M τα 24 MBps / 3,5 Mbps). Στην πράξη, σε αυτές τις ταχύτητες μπορούν να συνδεθούν πολλοί λίγοι χρήστες λόγω της απόστασης τους από το τηλεφωνικό κέντρο.

Όνομα Προτύπου	**Κοινή Ονομασία**	**Μέγιστος Ρυθμός Λήψης**	**Μέγιστος Ρυθμός Αποστολής**
ANSI T1.413-1998 Issue 2	ADSL	8 Mbit/s	1 Mbit/s
ITU G.992.1	ADSL (G.DMT)	8 Mbps	1 Mbps
ITU G.992.1 Annex A	ADSL over POTS	8 Mbps	1 Mbps
ITU G.992.1 Annex B	ADSL over ISDN	8 Mbps	1 Mbps
ITU G.992.2	ADSL Lite (G.Lite)	1,5 Mbps	0,5 Mbps
ITU G.992.3/4	ADSL2	12 Mbps	1 Mbps
ITU G.992.3/4 Annex J	ADSL2	12 Mbps	3,5 Mbps
ITU G.992.3/4 Annex L	RE-ADSL2	5 Mbit/s	0,8 Mbit/s
ITU G.992.5	ADSL2+	24 Mbit/s	1 Mbit/s
ITU G.992.5 Annex L	RE-ADSL2+	24 Mbit/s	1 Mbit/s
ITU G.992.5 Annex M	ADSL2+	24 Mbit/s	3,5 Mbit/s

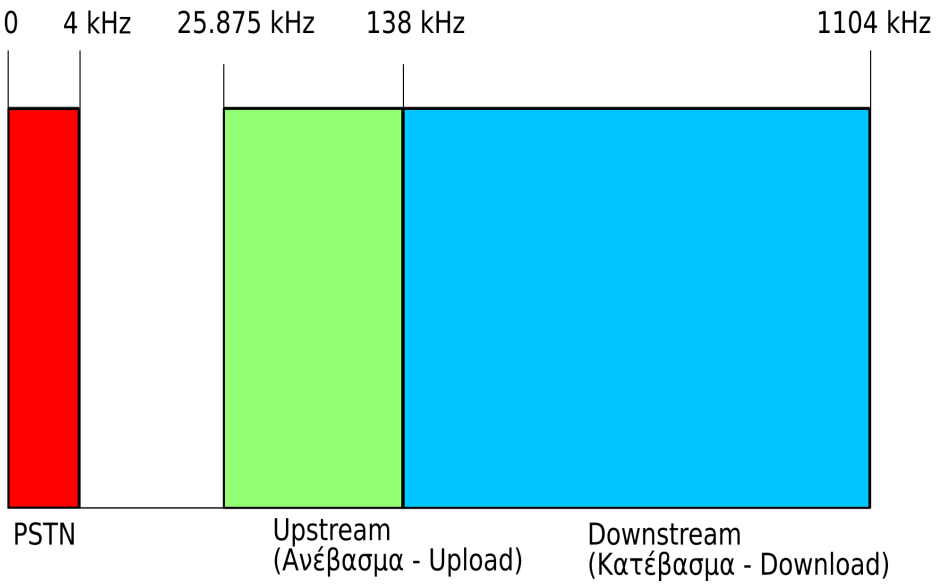
Πίνακας 5.2: *Πρότυπα ADSL*

Η υψηλή ταχύτητα της ADSL επιτυγχάνεται χάρη σε εξελιγμένους αλγορίθμους και ψηφιακή επεξεργασία σήματος (DSP, Digital Signal Processing) που συμπιέζουν σε μεγάλο βαθμό την πληροφορία που μεταδίδεται μέσα από τα τηλεφωνικά καλώδια καθώς και στη βελτίωση των μετασχηματιστών των αναλογικών φίλτρων και των μετατροπέων από αναλογικό σε ψηφιακό (ADC, Analog to Digital Converter).

Στη μετάδοση φωνής της απλής τηλεφωνικής σύνδεσης χρησιμοποιείται μόνο η περιοχή συχνοτήτων από 0 Hz – 4 KHz. Καθώς το καλώδιο μπορεί να μεταδώσει πολύ μεγαλύτερες συχνότητες, το επιπλέον εύρος ζώνης χρησιμοποιείται για τη μετάδοση δεδομένων. Οι συνηθισμένοι οικιακοί χρήστες χρησιμοποιούν τη γραμμή περισσότερο για κατέβασμα παρά για ανέβασμα δεδομένων, έτσι το μεγαλύτερο εύρος ζώνης της γραμμής διατίθεται στο κανάλι downstream παρά στο upstream.

Οι συχνότητες του καναλιού υποδιαιρούνται σε μικρότερες περιοχές των 4,3125 KHz που ονομάζονται bins. Τα modems τυπικά κατά την έναρξη της επικοινωνίας (training) ελέγχουν ξεχωριστά κάθε τέτοια περιοχή για να καθορίσουν ποιες από αυτές μπορούν να χρησιμοποιηθούν.

Η σύνδεση ADSL χρησιμοποιείται για τη μεταφορά δεδομένων από τον τελικό χρήστη μέχρι το τηλεφωνικό κέντρο της περιοχής. Στο τηλεφωνικό κέντρο διακλαδώνεται μέσω DSLAM και μεταβιβάζεται με γραμμές πολύ μεγαλύτερης ταχύτητας στον αντίστοιχο πάροχο υπηρεσιών Internet.



Σχήμα 5.3: *Κατανομή Συχνοτήτων ADSL σε Γραμμή PSTN*

Στο σχήμα 5.3 φαίνονται οι περιοχές συχνοτήτων που χρησιμοποιούνται σε μια τηλεφωνική γραμμή PSTN που μεταφέρει δεδομένα ADSL. Με κόκκινο χρώμα φαίνεται η περιοχή συχνοτήτων φωνής (από 0 – 4 KHz) με μπλε τα κανάλια για κατέβασμα (downstream) με και με πράσινο για ανέβασμα (upstream).

Οι τηλεφωνικές γραμμές μεγάλου μήκους προξενούν μεγάλη εξασθένιση στα σήματα υψηλών συχνοτήτων. Στην συχνότητα του 1 MHz (που αντιστοιχεί στις συχνότητες Downstream ADSL/ADSL2+) η εξασθένιση μπορεί να φτάσει και τα 90 db.

Πόσο μεγάλη εξασθένιση είναι τα 90 db;

Το decibel (db) δεν είναι από μόνο του μονάδα μέτρησης, αλλά χρησιμοποιείται για να συγκρίνουμε μεγέθη μεταξύ τους και λειτουργεί λογαριθμικά. Εξασθένιση 90 db σημαίνει ότι η ισχύς του σήματος μειώνεται κατά 10^9 (1 δις!) φορές.

Με τόσο μεγάλη εξασθένιση είναι προφανές ότι το κύκλωμα του ADSL modem

εκτελεί αρκετά πολύπλοκες λειτουργίες προκειμένου να εξασφαλίσει το απαραίτητο εύρος ζώνης. Για να δημιουργηθούν πολλαπλά κανάλια επικοινωνίας τα ADSL modems χωρίζουν το διαθέσιμο εύρος ζώνης της γραμμής με ένα από τους δύο παρακάτω τρόπους:

- Πολυπλεξία με διαίρεση συχνότητας (Frequency Division Multiplexing)
- Καταστολή της ηχούς (Echo Cancellation)

Τι είναι η πολυπλεξία στη συχνότητα; Η πολυπλεξία στη συχνότητα είναι μια τεχνική που χρησιμοποιείται μαζί με τη διαμόρφωση για να περάσουμε περισσότερες από μια επικοινωνίες ταυτόχρονα μέσα από το ίδιο φυσικό μέσο, χωρίς να παρεμβάλλονται μεταξύ τους. Το πιο απλό παράδειγμα καθημερινής χρήσης που μπορούμε να δώσουμε είναι το ραδιόφωνο: έχουμε ένα μοναδικό κοινό φυσικό μέσο (τον αέρα) αλλά μπορούμε μέσα από αυτό να μεταδώσουμε πολλαπλά σήματα ίδιων ουσιαστικά συχνοτήτων (λόγος, μουσική, τραγούδι). Πως το επιτυγχάνουμε; Δεν μεταδίδουμε απευθείας τις συχνότητες της μουσικής στον αέρα, αλλά χρησιμοποιούμε διαμόρφωση για να "φορτώσουμε" το μουσικό σήμα σε μια άλλη υψηλότερη συχνότητα (αυτή στην οποία συντονίζουμε το ραδιόφωνο). Οι συχνότητες αυτές (φέρουσες) απέχουν αρκετά μεταξύ τους ώστε να μπορούμε να τις ξεχωρίσουμε με το κατάλληλο κύκλωμα και να ανακτήσουμε την αρχική πληροφορία (μουσική).

Τι είναι η καταστολή της ηχούς; Όταν μεταδίδουμε ένα σήμα μέσα από μια γραμμή, δημιουργείται ηχώ. Καθώς το σήμα φτάνει στον αποδέκτη, ένα μέρος του ανακλάται στην άκρη της γραμμής και αρχίζει να επιστρέφει στον αποστολέα. Καθώς η ηχώ ταξιδεύει μέσα από την τηλεφωνική γραμμή παρεμβάλλει το κανονικό σήμα εξασθενώντας το. Αν πρόκειται για γραμμή που μεταφέρει μόνο ομιλία, η ηχώ προκαλεί χειροτέρευση της ποιότητας επικοινωνίας. Σε γραμμή που μεταφέρει και δεδομένα (όπως η DSL) η ηχώ μειώνει το διαθέσιμο εύρος ζώνης της γραμμής και προκαλεί επιπλέον εξασθένιση στο σήμα που μεταδίδεται. Για το σκοπό αυτό προσπαθούμε είτε να αποφύγουμε τη δημιουργία της, είτε να την καταστείλουμε αν έχει ήδη δημιουργηθεί. Στις γραμμές DSL αυτό γίνεται με ειδικά ηλεκτρονικά κυκλώματα καταστολής της ηχούς.

Παραλλαγές xDSL

- **HDSL:** High-bit-rate Digital Subscriber Line. Πρόκειται για συμμετρική παραλλαγή και προσφέρει τον ίδιο ρυθμό αποστολής και λήψης, μέχρι 2 Mbps. Η μέγιστη απόσταση των δύο άκρων δεν μπορεί να υπερβαίνει τα 3,5 km.

Επίσης απαιτεί την εγκατάσταση δυο τηλεφωνικών γραμμών (δύο ζεύγη συνεστραμμένων καλωδίων). Νεότερες εκδόσεις είναι το HDSL2 (2 Mbps με ένα ζεύγος καλωδίων) και το HDSL4 (ίδια ταχύτητα με το HDSL2 αλλά με δύο ζεύγη καλωδίων για καλύτερη αξιοπιστία).

- **SDSL:** Το SDSL (Single-line Digital Subscriber Line γνωστό και ως Symmetric Digital Subscriber Line) είναι τεχνολογία παρόμοια με το HDSL (συμμετρική) και με ίδιο ρυθμό μεταφοράς δεδομένων (μέχρι 2 Mbps) αλλά απαιτεί μόνο ένα συνεστραμμένο ζεύγος καλωδίων. Για αυτό το λόγο η μέγιστη απόσταση μεταξύ των δύο άκρων δεν μπορεί να ξεπερνά τα 3 Km.
- **VDSL:** Το VDSL (Very-high-data-rate Digital Subscriber Line) δίνει εντυπωσιακά μεγαλύτερες ταχύτητες που φτάνουν μέχρι τα 52 Mbps downstream και 12 Mbps upstream σε περιορισμένη όμως απόσταση μεταξύ των δύο άκρων. Ανάλογα με την υλοποίηση η απόσταση δεν μπορεί να ξεπερνά το 1,5 Km. Διάδοχος τεχνολογία είναι το VDSL2 με ταχύτητες πάνω από 200 Mbps σε πολύ μικρή απόσταση, 100 Mbps στα 500 μέτρα και 50 Mbps στο 1 χιλιόμετρο.

Κεφάλαιο 6

Επίπεδο Εφαρμογής

6.1 Σύστημα Ονοματολογίας DNS

Όπως είδαμε στην ενότητα 3.4 κάθε υπολογιστής που μετέχει σε ένα δίκτυο TCP/IP διαθέτει μια μοναδική διεύθυνση IP με την οποία μπορεί να αναγνωριστεί. Καθώς όμως οι άνθρωποι δεν είναι ιδιαίτερα καλοί στην απομνημόνευση αριθμών (και μάλιστα της μορφής που έχουν οι διευθύνσεις), προτιμούμε να αντιστοιχίζουμε ονόματα σε αυτές τις αριθμητικές διευθύνσεις.

Στη ενότητα 3.4 είδαμε ότι ένας τρόπος αντιστοίχισης ονομάτων σε διευθύνσεις είναι μέσω του αρχείου *hosts* το οποίο υπάρχει μέχρι και σήμερα ουσιαστικά σε όλα τα λειτουργικά συστήματα. Στο αρχείο αυτό – το οποίο είναι απλό κείμενο – υπάρχουν γραμμές της μορφής

<διεύθυνση IP> <όνομα υπολογιστή>

Για παράδειγμα, σε ένα μικρό δίκτυο ένα αρχείο hosts θα μπορούσε να περιέχει τα παρακάτω:

```
128.174.5.1                atlas
128.174.5.2                kronos
128.174.5.3                aris
```

Το σύστημα αυτό προφανώς μπορεί να λειτουργήσει σε μικρά μόνο δίκτυα, καθώς έχει σοβαρά μειονεκτήματα:

- Πρέπει να υπάρχει αντίγραφο του αρχείου σε κάθε μηχάνημα του δικτύου
- Όλα τα αντίγραφα πρέπει να ενημερώνονται κάθε φορά που γίνεται μια αλλαγή

- Αν το αρχείο έχει πάρα πολλές καταχωρίσεις, η αναζήτηση σε αυτό θα είναι αργή

Είναι προφανές ότι αν μιλάμε για ονομασίες μηχανημάτων (και τοποθεσιών) στο Διαδίκτυο, η λύση του αρχείου hosts είναι ανέφικτη:

- Το αρχείο hosts έχει επίπεδη μορφή: δεν διακρίνει υποχρεωτικά περιοχές ή υποδίκτυα. Οι υπολογιστές μπορεί να έχουν απλά ένα όνομα
- θα ήταν αδύνατο να έχουμε ενημερωμένα αντίγραφα σε όλους τους υπολογιστές του Διαδικτύου αλλά…
- …ακόμα και αν μπορούσαμε, το αρχείο θα ήταν τόσο μεγάλο που η αναζήτηση σε αυτό θα ήταν αδύνατη

Είναι φανερό ότι όσο αφορά το Internet χρειαζόμαστε ένα διαφορετικό τρόπο αντιμετώπισης του προβλήματος αντιστοίχισης ονομάτων σε διευθύνσεις και το αντίστροφο. Η λύση σε αυτό είναι το σύστημα DNS, που εκτελείται στο επίπεδο εφαρμογής και ακολουθεί το μοντέλο πελάτη – εξυπηρετητή.

Το σύστημα DNS προχωρά αρκετά παραπέρα από το αρχείο hosts:

- Επιτρέπει τον διαχωρισμό της ονοματολογίας σε περιοχές και υποπεριοχές αντί για την επίπεδη λογική του αρχείου hosts
- Καταχωρεί τα δεδομένα του σε μια κατανεμημένη βάση δεδομένων για γρήγορη αναζήτηση
- Κατανέμει το φορτίο εργασίας σε πάρα πολλούς υπολογιστές
- Ένα μηχάνημα – πελάτης (ο υπολογιστής π.χ. του τελικού χρήστη) δεν χρειάζεται να έχει καμιά διεύθυνση αποθηκευμένη, εκτός από το IP του υπολογιστή που εκτελεί την υπηρεσία DNS (και το οποίο μπορεί επίσης να αποστέλλεται αυτόματα μέσω της υπηρεσίας DHCP)

Πρέπει εδώ να τονίσουμε ότι το DNS λειτουργεί ως *κατανεμημένη* βάση δεδομένων: δεν υπάρχει ένας και μοναδικός υπολογιστής που να διαθέτει ολόκληρη τη βάση. Καθώς το DNS χωρίζει το Internet σε περιοχές και υποπεριοχές, διαφορετικοί εξυπηρετητές είναι υπεύθυνοι για κάθε μια από αυτές. Το σύστημα επιτρέπει ένα εξυπηρετητή να ρωτάει κάποιον άλλο προκειμένου να μάθει μια διεύθυνση που είναι έξω από την περιοχή ευθύνης του. Ένα σύστημα που δεν θα λειτουργούσε με κατανεμημένο τρόπο θα κατέρρεε πολύ γρήγορα, καθώς δεν υπάρχει υπολογιστής και γραμμή δικτύου που θα μπορούσε να αντέξει τόσο τεράστια κίνηση από ερωτήματα.

Σε γενικές γραμμές το σύστημα DNS (Domain Name System ή Σύστημα Ονομασίας Περιοχών) είναι μια κατανεμημένη βάση δεδομένων που περιλαμβάνει:

- Το *χώρο ονομάτων*
- Τους *εξυπηρετητές* μέσω των οποίων γίνεται διαθέσιμος ο χώρος ονομάτων
- Τους *αναλυτές (resolvers)* που θέτουν ερωτήματα στους εξυπηρετητές σχετικά με ονόματα και διευθύνσεις που περιέχονται στο χώρο ονομάτων

Από τα παραπάνω, ένα μηχάνημα – πελάτης χρειάζεται να διαθέτει μόνο τον αναλυτή (resolver).

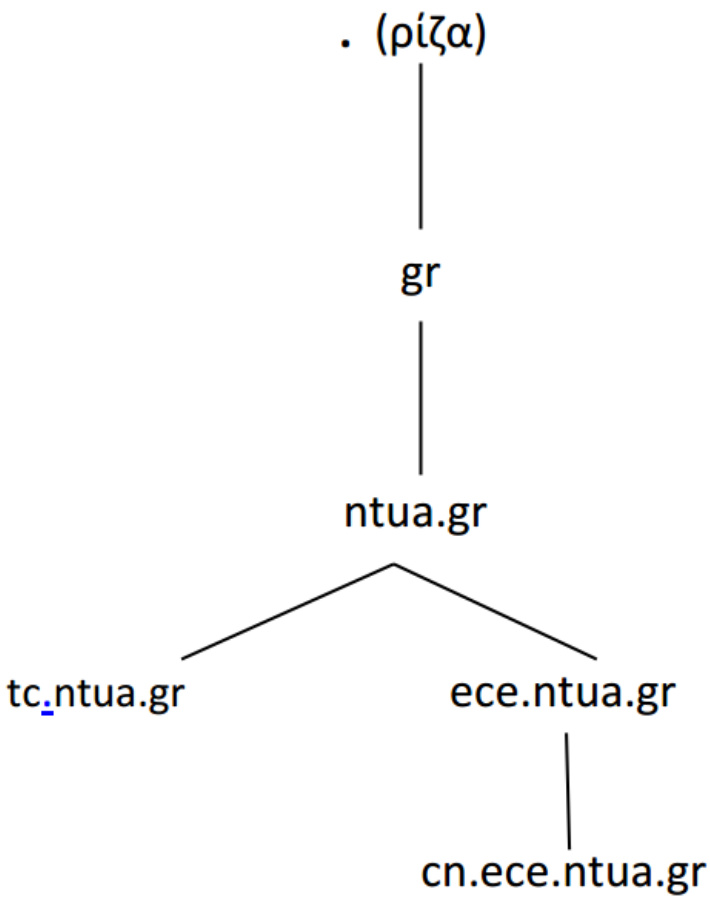
Το σύστημα DNS λειτουργεί στο επίπεδο εφαρμογής και εξυπηρετεί ουσιαστικά οποιαδήποτε συσκευή χρειάζεται να γνωρίζει την IP διεύθυνση που αντιστοιχεί σε ένα όνομα (ή το αντίθετο), περιλαμβανομένων τελικών υπολογιστών (hosts), δρομολογητών (routers) αλλά και εξυπηρετητών DNS μεταξύ τους. Το DNS είναι βασική υπηρεσία του Διαδικτύου και αναζητήσεις μπορεί να γίνονται από οποιοδήποτε μηχάνημα και υπηρεσία. Τυπικά οι αναλυτές στα μηχανήματα των χρηστών είναι ρυθμισμένοι να απευθύνουν ερωτήματα μόνο σε ένα ή δύο εξυπηρετητές DNS. Όταν ένας εξυπηρετητής DNS ερωτηθεί για ένα όνομα που δεν γνωρίζει (γιατί είναι έξω από τη ζώνη ευθύνης του), θα ρωτήσει άλλους εξυπηρετητές DNS προκειμένου να μάθει την απάντηση και να την επιστρέψει στον αναλυτή. Η απάντηση αυτή αποθηκεύεται προσωρινά προκειμένου να επιταχυνθεί η λειτουργία αν τεθεί ξανά η ίδια ερώτηση από άλλο μηχάνημα.

6.1.1 Χώρος Ονομάτων του DNS

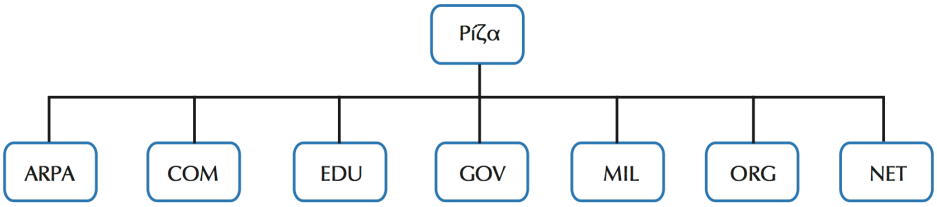
Το Διαδίκτυο χωρίζεται νοητά σε εκατοντάδες διαφορετικές περιοχές που ονομάζονται *domains*. Οι περιοχές χωρίζονται σε υποπεριοχές (subdomains) και αυτές σε άλλες κ.ο.κ. κάθε μια με ένα ή περισσότερους υπολογιστές (hosts).

Οι περιοχές μπορούν να αναπαρασταθούν με ένα δέντρο. Τα ονόματα σχηματίζουν μια ιεραρχία με τρόπο που να είναι μοναδικά και μπορούν να απομνημονευθούν σχετικά εύκολα. Για κάθε περιοχή ορίζεται κάποιος αρμόδιος ο οποίος διαχειρίζεται τον αντίστοιχο εξυπηρετητή DNS και μπορεί να προσθέσει ή να επεξεργαστεί υποπεριοχές (subdomains) και υπολογιστές (hosts). Κάθε κόμβος στο σύστημα DNS αναπαριστά ένα όνομα DNS (DNS Name). Κάθε κλαδί κάτω από ένα κόμβο είναι μια περιοχή DNS (DNS Domain) και μπορεί να περιέχει υποπεριοχές και υπολογιστές.

Στην κορυφή της ιεραρχίας του DNS είναι η ρίζα που συμβολίζεται με μια τελεία "." (σχήμα 6.1). Επίσημος διαχειριστής της ρίζας είναι η *IANA, Internet Assigned Numbers Authority*. Κάτω από τη ρίζα υπάρχουν οι περιοχές *ανώτατου επιπέδου (top level domains ή περιοχές βασικού επιπέδου ή βασικές περιοχές)*. Αρχικά (το 1988) υπήρχαν οι περιοχές που φαίνονται στο σχήμα 6.2.



Σχήμα 6.1: *Παράδειγμα Περιοχών DNS*



Σχήμα 6.2: *Περιοχές DNS 1ου Επιπέδου*

Οι καταλήξεις στο πρώτο επίπεδο δηλώνουν:

- **.arpa**: Ειδικοί οργανισμοί διαδικτύου
- **.com**: Εταιρίες (εμπορικές)

- **.edu**: Εκπαιδευτικά ιδρύματα, πανεπιστήμια κλπ
- **.gov**: Κυβερνητικοί οργανισμοί και υπηρεσίες
- **.mil**: Στρατιωτικοί οργανισμοί
- **.net**: Κέντρα διαχείρισης δικτύου
- **.org**: Μη κερδοσκοπικοί οργανισμοί και γενικά οτιδήποτε δεν μπορεί να κατηγοριοποιηθεί σε μια από τις παραπάνω κατηγορίες

Αργότερα προστέθηκαν περιοχές για κάθε χώρα (π.χ. .gr, .uk, .fr κλπ) και κάποιες επιπλέον περιοχές (όπως .biz, .post, .info κλπ.). Η διαχείριση τους (εκτός από την .int και .arpa) έχει εκχωρηθεί από την IANA σε άλλους οργανισμούς.

Κάτω από κάθε περιοχή πρώτου επιπέδου, υπάρχει δεύτερο επίπεδο που προσδιορίζει την εταιρία ή τον οργανισμό στον οποίο ανήκει το δίκτυο. Οι περιοχές αυτές ονομάζονται *2ου επιπέδου* και κάθε μια είναι μοναδική.

Όταν μια εταιρεία ή οργανισμός κατοχυρώνει ένα domain, αναλαμβάνει και τη διαχείριση του αντίστοιχου χώρου ονομάτων. Μπορεί να αναθέσει σε μια εταιρία παροχής υπηρεσιών Internet να συντηρεί την περιοχή ή μπορεί να διαθέτει δικούς της εξυπηρετητές DNS. Σε κάθε περίπτωση ο κάτοχος του χώρου θα πρέπει να διαθέτει τον εξοπλισμό ώστε να απαντά σε ερωτήματα σχετικά με τους υπολογιστές που ανήκουν στη περιοχή του καθώς και σε όποιες υποπεριοχές έχει δημιουργήσει ο ίδιος.

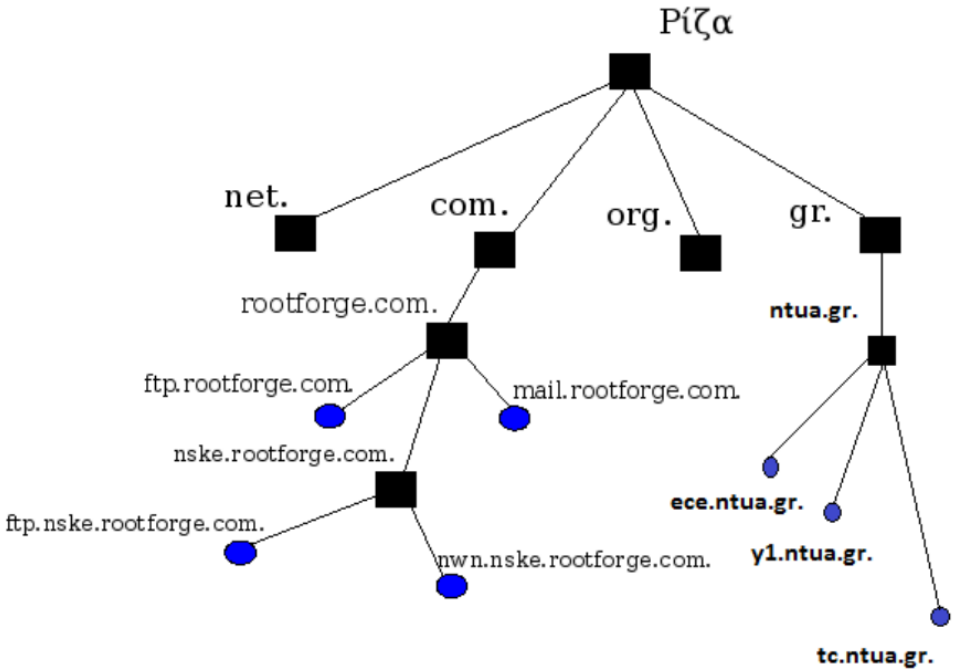
Στο σχήμα 6.3 φαίνεται μια τέτοια οργάνωση. Στην κορυφή του δέντρου βρίσκεται η ρίζα που τη διαχειρίζεται η IANA. Μια από τις βασικές περιοχές (1ου επιπέδου) είναι και η **.gr** για την οποία είναι υπεύθυνο το ΙΤΕ, Ίδρυμα Τεχνολογίας και Έρευνας. Στο δεύτερο επίπεδο συναντάμε την περιοχή **ntua.gr** η οποία ανήκει στο Εθνικό Μετσόβιο Πολυτεχνείο (ΕΜΠ). Το όνομα **y1.ntua.gr** προσδιορίζει τον υπολογιστή **y1** στο δίκτυο του ΕΜΠ.

Σε γενικές γραμμές, όταν βλέπουμε ένα πλήρες όνομα DNS, το πλέον αριστερό τμήμα προσδιορίζει τον υπολογιστή και το πλέον δεξιό την περιοχή βασικού επιπέδου. Για παράδειγμα, το παρακάτω είναι έγκυρο όνομα:

ektor.tc.ntua.gr

όπου:

- ektor: Είναι το όνομα του υπολογιστή
- .tc: Είναι το όνομα της περιοχής 3ου επιπέδου
- .ntua: Είναι το όνομα της περιοχής 2ου επιπέδου



Σχήμα 6.3: *Ιεραρχική Οργάνωση Χώρου DNS*

- .gr: Είναι το όνομα της περιοχής 1ου (βασικού) επιπέδου

Σημειώνουμε εδώ ότι μπορεί να υπάρχουν επίπεδα και πάνω από το 3ο, αλλά δεν τα συναντάμε συχνά, τουλάχιστον όχι σε εξυπηρετητές ιστοσελίδων. Δεν είναι όμως σπάνιο για μια επιχείρηση να έχει δομήσει το εσωτερικό της δίκτυο σε περισσότερα από τρία επίπεδα.

Ένα πιο συνηθισμένο παράδειγμα DNS για ένα υπολογιστή που εκτελεί χρέη εξυπηρετητή ιστοσελίδων είναι το παρακάτω:

Όταν συνδεθήκατε για να κατεβάσετε αυτό το βιβλίο, χρησιμοποιήσατε τη διεύθυνση:

www.freebsdworld.gr

- Για να συνδεθείτε, ο αναλυτής (resolver) στον υπολογιστή σας πρέπει να μάθει τη διεύθυνση IP της παραπάνω τοποθεσίας. Το ερώτημα τίθεται στον εξυπηρετητή DNS του παροχέα Internet που χρησιμοποιείτε.
- Ο DNS του παροχέα σας ρωτάει αρχικά τον εξυπηρετητή που είναι υπεύθυνος για την περιοχή ".gr". Ο εξυπηρετητής αυτός γνωρίζει μόνο ποιος εξυπηρετητής DNS είναι υπεύθυνος για την περιοχή 2ου επιπέδου "freebsdworld.gr"

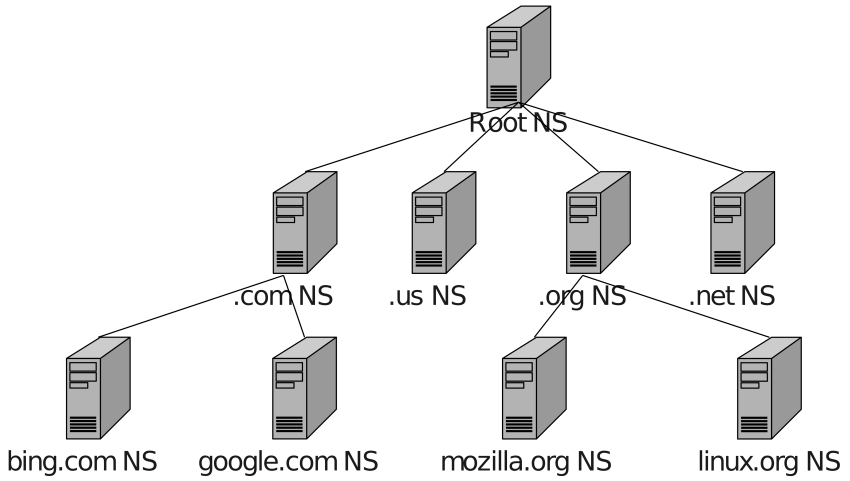
και τον παραπέμπει προς αυτόν.

- Ο εξυπηρετητής του παροχέα επικοινωνεί με τον εξυπηρετητή DNS που είναι υπεύθυνος για την περιοχή “freebsdworld.gr” για να μάθει τη διεύθυνση IP του μηχανήματος με όνομα “www”. Την απάντηση αυτή στέλνει στο δικό σας ερώτημα (και ταυτόχρονα την αποθηκεύει για μελλοντική χρήση).

Στην παραπάνω διεύθυνση, το “www” αποτελεί το όνομα του υπολογιστή που εκτελεί την υπηρεσία ιστοσελίδων (web server). Όπως φαίνεται και από το παράδειγμα μας, η βάση DNS είναι κατανεμημένη και διαφορετικοί υπολογιστές είναι υπεύθυνοι για τις αντίστοιχες περιοχές. Οι εξυπηρετητές DNS βρίσκονται σε διαφορετικά σημεία και συνεργάζονται μεταξύ τους για να απαντήσουν στα ερωτήματα.

6.1.2 Οργάνωση DNS

Η ιεραρχία του χώρου ονομάτων είναι αντίστοιχη με την ιεραρχία των εξυπηρετητών (σχήμα 6.4)



Σχήμα 6.4: *Ιεραρχία Εξυπηρετητών DNS*

Κάθε εξυπηρετητής είναι υπεύθυνος για ένα τμήμα του χώρου ονομάτων που ονομάζεται *ζώνη (zone)*.

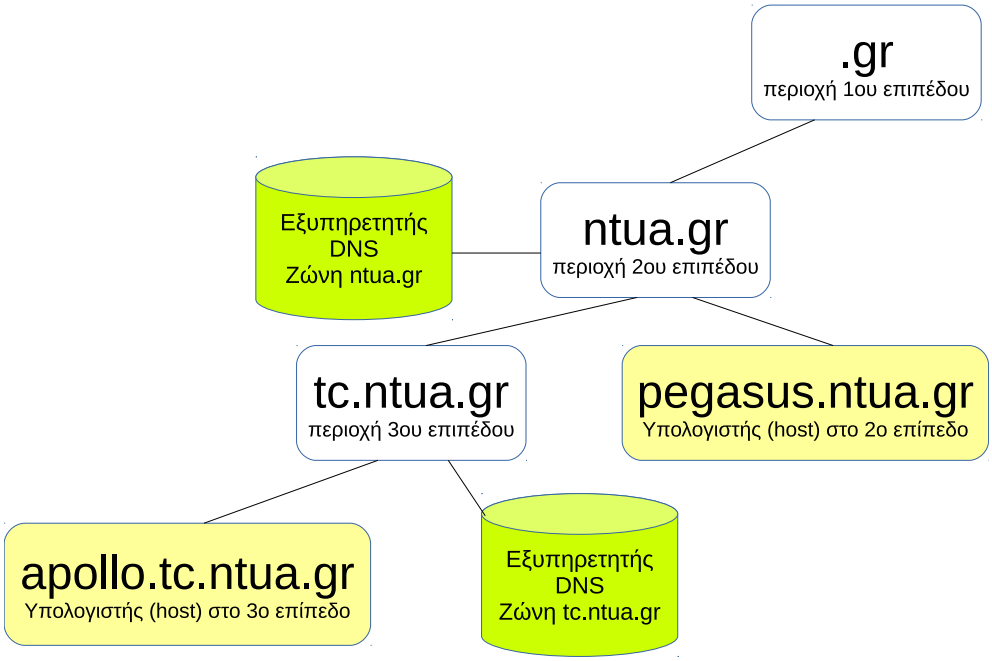
Μα αν ένας εξυπηρετητής είναι υπεύθυνος για μια περιοχή (domain) αυτό δεν σημαίνει ότι η ζώνη περιέχει όλα τα μηχανήματα της περιοχής; Ποια είναι η διαφορά μεταξύ ζώνης και περιοχής;

Η ζώνη περιέχεται σε ένα αρχείο μέσα στον εξυπηρετητή και περιέχει εγγραφές με διευθύνσεις και ονόματα. Αν έχουμε μια περιοχή που δεν περιέχει άλλες υποπεριοχές αλλά μόνο μηχανήματα, το αρχείο ζώνης μπορεί πράγματι να περιέχει όλα τα μηχανήματα της περιοχής. Για παράδειγμα η περιοχή freebsdworld.gr δεν περιέχει άλλες υποπεριοχές αλλά μόνο μηχανήματα (hosts). Δείτε παρακάτω ένα απόσπασμα της αντίστοιχης ζώνης:

```
ns1             IN      A       193.183.99.68
ns2             IN      A       46.19.141.199
equinox         IN      A       193.183.99.68
falcon          IN      A       46.19.141.199
```

(Οι εγγραφές τύπου “A” υποδηλώνουν μηχανήματα (hosts))

Ας πάρουμε όμως την περίπτωση μια περιοχή να περιέχει υποπεριοχές. Δείτε για παράδειγμα το σχήμα 6.5.



Σχήμα 6.5: *Περιοχές και Ζώνες*

Υπάρχει εδώ η περιοχή **ntua.gr** (στο 2ο επίπεδο) και η **tc.ntua.gr** (στο 3ο επίπεδο). Σε κάθε επίπεδο υπάρχει από ένας υπολογιστής (host) και ένας εξυπηρετητής

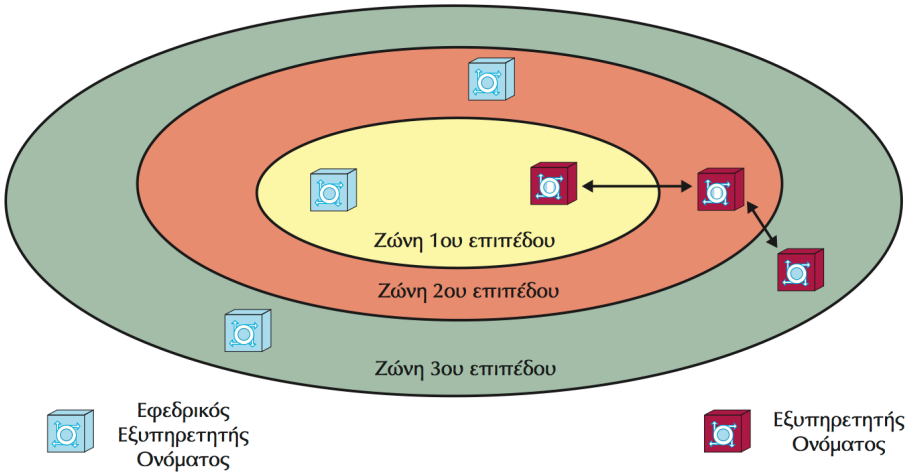
DNS.

Τι περιέχει η ζώνη **ntua.gr** στο DNS 2ου επιπέδου; Περιέχει μια εγγραφή για τον υπολογιστή **pegasus.ntua.gr** που είναι στο ίδιο επίπεδο, αλλά **δεν** περιέχει για τον **apollo.tc.ntua.gr** που είναι στο 3ο επίπεδο!

Αντί για αυτό, η ζώνη δευτέρου επιπέδου διαθέτει μια εγγραφή που δείχνει στην IP του εξυπηρετητή DNS 3ου επιπέδου και ορίζει ότι αυτός είναι υπεύθυνος για την υποπεριοχή **tc.ntua.gr**. Αν ο DNS 2ου επιπέδου δεχθεί ένα ερώτημα του τύπου "ποια είναι η διεύθυνση του υπολογιστή apollo.tc.ntua.gr" μπορεί:

- Είτε να ρωτήσει τον εξυπηρετητή DNS 3ου επιπέδου (τον οποίο γνωρίζει καθώς η διεύθυνση του περιέχεται στη δική του ζώνη)
- Είτε να παραπέμψει όποιον έθεσε το ερώτημα στον εξυπηρετητή DNS 3ου επιπέδου στέλνοντας του μια απάντηση του τύπου "υπεύθυνος για την υποπεριοχή είναι ο εξυπηρετητής DNS με IP x.x.x.x"

Είναι όμως φανερό από τα παραπάνω ότι η ζώνη που περιέχεται στον εξυπηρετητή DNS 2ου επιπέδου δεν περιέχει τις πληροφορίες όλης της περιοχής **ntua.gr**. Γενικά μια ζώνη περιέχει συνήθως πληροφορίες για ένα μόνο τμήμα ενός χώρου ονομάτων και τα υπόλοιπα τμήματα της περιοχής μπορεί να είναι αποθηκευμένα σε άλλες ζώνες και εξυπηρετητές.



Σχήμα 6.6: *Οργάνωση σε Ζώνες*

Τελικά, για να βρεθεί μια αντιστοίχιση μπορεί να χρειαστεί να ερωτηθούν αρκετοί εξυπηρετητές.

Για κάθε ζώνη πρέπει να υπάρχει ένας κύριος (primary) και ένας δευτερεύον (secondary) εξυπηρετητής. Ο δευτερεύων κρατάει αντίγραφα των δεδομένων του κύριου εξυπηρετητή. Η βάση δεδομένων μπορεί να ενημερωθεί δυναμικά προσθέτοντας, διαγράφοντας ή τροποποιώντας τις εγγραφές της. Για να προστεθεί ένα μηχάνημα (host) σε μια ζώνη ο διαχειριστής προσθέτει τις αντίστοιχες πληροφορίες (όνομα και διεύθυνση) στο αντίστοιχο αρχείο ζώνης. Ο δευτερεύων εξυπηρετητής συνήθως ενημερώνεται αυτόματα για την αλλαγή μέσω του κύριου.

Σχεδόν κάθε οργανισμός, εταιρεία, πανεπιστήμιο κλπ διαθέτει ένα τοπικό εξυπηρετητή ονομάτων που είναι γνωστός και ως *επιλεγμένος ή προεπιλεγμένος (default)* εξυπηρετητής. Ο εξυπηρετητής αυτός μπορεί να απαντήσει σε ερωτήματα για τα ονόματα και τις διευθύνσεις των μηχανημάτων του τοπικού (εσωτερικού) δικτύου (διαθέτει τις απαραίτητες ζώνες) αλλά απαντάει και για ερωτήματα που αναφέρονται σε υπολογιστές και διευθύνσεις εκτός της εταιρίας (στο Διαδίκτυο). Για το σκοπό αυτό ρωτά άλλους εξυπηρετητές και μπορεί αν χρειαστεί να φτάσει και μέχρι τους εξυπηρετητές ρίζας (Για λόγους απόδοσης μπορεί φυσικά να αποθηκεύει προσωρινά τα αποτελέσματα).

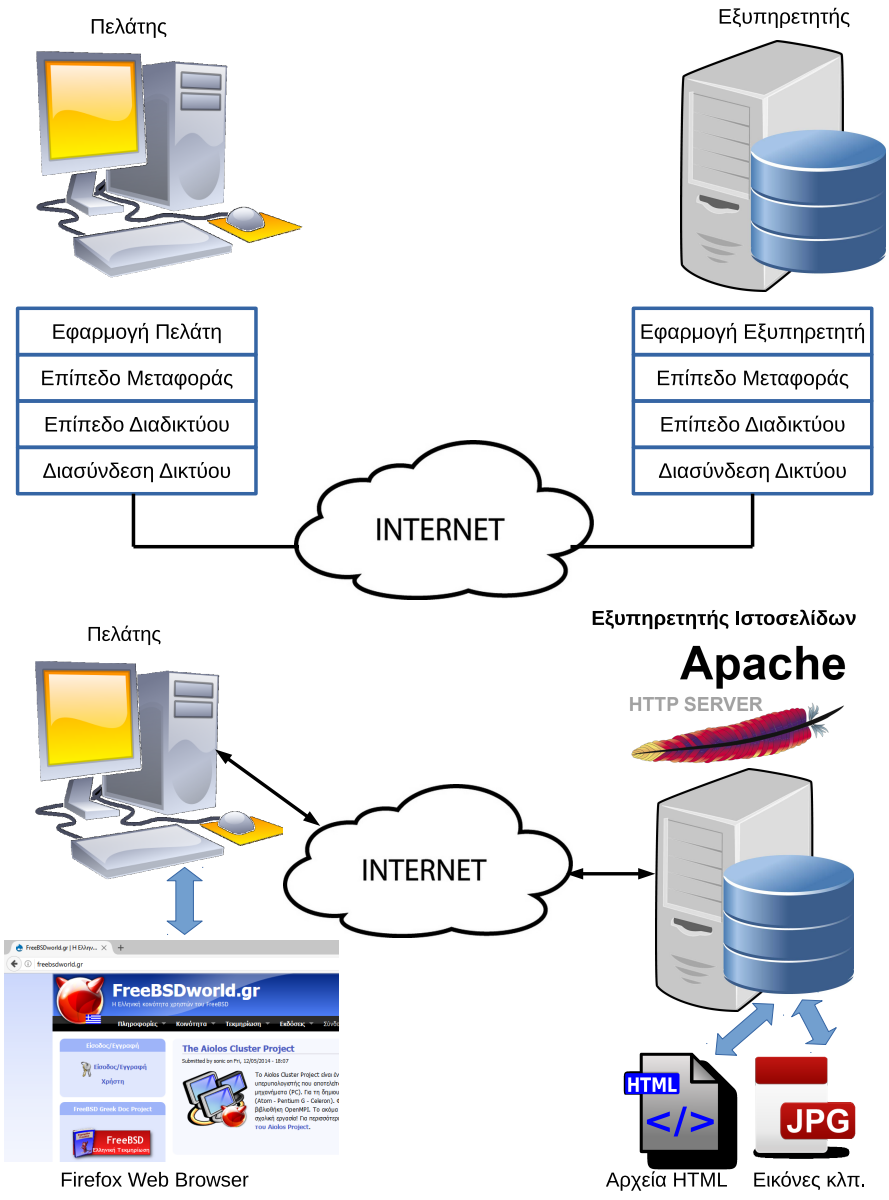
Το **πρωτόκολλο DNS** βρίσκεται στο επίπεδο εφαρμογής και χρησιμοποιεί το μοντέλο πελάτη – εξυπηρετητή. Ο πελάτης ονομάζεται *αναλυτής (resolver)*. Το πρωτόκολλο DNS υποστηρίζει τη μετατροπή ονομάτων σε διευθύνσεις και το ανάστροφο (ανάλυση ή resolution) καθώς και την ενημέρωση δεδομένων μεταξύ των εξυπηρετητών ονομάτων.

Η **ανάλυση ονομάτων (name resolution)** είναι η διαδικασία με την οποία αναλυτές και εξυπηρετητές DNS συνεργάζονται για να βρουν δεδομένα εντός του χώρου ονομάτων. Για την ανεύρεση δεδομένων οι εξυπηρετητές DNS χρειάζονται μόνο τις διευθύνσεις IP των εξυπηρετητών κορυφής (ρίζας). Οι εξυπηρετητές ρίζας γνωρίζουν όλες τις περιοχές ανωτάτου επιπέδου και μπορούν να υποδείξουν τους εξυπηρετητές περιοχών με τους οποίους μπορεί να γίνει επαφή.

6.2 Υπηρεσίες Διαδικτύου

Οι υπηρεσίες του Διαδικτύου και πολλές εφαρμογές λογισμικού στηρίζονται στο μοντέλο *Πελάτη – Εξυπηρετητή*. Στο μοντέλο αυτό ο Εξυπηρετητής οργανώνει και διαχειρίζεται το αρχείο δεδομένων ενώ δέχεται αιτήματα και απαντά στο πρόγραμμα Πελάτης. Το πρόγραμμα Πελάτης θέτει ερωτήματα στον εξυπηρετητή και αποκωδικοποιεί τις απαντήσεις του εξυπηρετητή.

Το μοντέλο Πελάτη – Εξυπηρετητή υλοποιείται με δύο ανεξάρτητα τμήματα λογισμικού:



Σχήμα 6.7: *Μοντέλο Πελάτη – Εξυπηρετητή στο TCP/IP και στην Υπηρεσία Ιστοσελίδων*

- Το πρόγραμμα του **Εξυπηρετητή (Server)** εγκαθίσταται σε ένα ή περισσότερους υπολογιστές. Ένας εξυπηρετητής μπορεί συνήθως να εξυπηρετήσει ταυτόχρονα εκατοντάδες ή και χιλιάδες Πελάτες

- Το πρόγραμμα του **Πελάτη (Client)** εγκαθίσταται σε πολλούς υπολογιστές

Για παράδειγμα ένας εξυπηρετητής ιστοσελίδων (σχήμα 6.7) μιας δικτυακής τοποθεσίας εκτελείται σε ένα μηχάνημα εξυπηρετητή. Ο εξυπηρετητής αυτός διαχειρίζεται τα αρχεία της ιστοσελίδας τα οποία τυπικά βρίσκονται αποθηκευμένα σε ένα κατάλογο (φάκελο) στο σύστημα αρχείων του εξυπηρετητή. Ο εξυπηρετητής ιστοσελίδων δέχεται συνδέσεις από πελάτες μέσω του πρωτοκόλλου TCP (στη θύρα 80). Οι πελάτες με αιτήματα τους ζητούν συγκεκριμένες σελίδες (αρχεία μορφής HTML) και τα στοιχεία τους (εικόνες κλπ) και ο εξυπηρετητής ανταποκρίνεται στέλνοντας απαντήσεις (κείμενο σε μορφή HTML κλπ). Ένας μόνο εξυπηρετητής μπορεί να ανταποκριθεί ταυτόχρονα σε χιλιάδες πελάτες (ανάλογα και με τη δυναμική του μηχανήματος και της γραμμής). Το πρόγραμμα πελάτης σε αυτή τη περίπτωση είναι ο φυλλομετρητής (browser) που εκτελείται στο μηχάνημα τελικού χρήστη.

6.2.1 Υπηρεσία Ηλεκτρονικού Ταχυδρομείου E-mail (POP3 – IMAP / SMTP)

Το ηλεκτρονικό ταχυδρομείο είναι ένα σύστημα για μετάδοση μηνυμάτων μεταξύ υπολογιστών. Στην αρχική του μορφή, το ηλεκτρονικό ταχυδρομείο είχε σχεδιαστεί για να μεταφέρει μηνύματα μόνο κειμένου, αργότερα όμως προστέθηκε η δυνατότητα για μεταφορά εικόνων, ήχου, βίντεο ακόμα και ιστοσελίδων, είτε μέσα στο ίδιο το μήνυμα είτε ως *επισυναπτόμενο αρχείο*. Ο χρήστης e-mail έχει τη δυνατότητα να στέλνει μηνύματα σε άλλους χρήστες της υπηρεσίας, άνετα γρήγορα και φθηνά. Το ηλεκτρονικό ταχυδρομείο μπορεί επίσης να στέλνει μηνύματα σε ομάδες χρηστών επιτρέποντας τη δημιουργία *λιστών διανομής ή mailing lists*. Όπως και στο συμβατικό ταχυδρομείο, κάθε χρήστης διαθέτει τη δική του διεύθυνση η οποία είναι γενικά της μορφής:

xxxxx@yyyyy.zzz

όπου

- **xxxxx** είναι το όνομα ή κάποιο ψευδώνυμο του χρήστη
- **yyyyy** είναι το όνομα της περιοχής της εταιρίας που παρέχει την υπηρεσία e-mail. Η εταιρία μπορεί να είναι η ίδια που παρέχει υπηρεσίες Internet στον πελάτη ή άλλη εταιρία που παρέχει e-mail επί πληρωμή ή δωρεάν. Η περιοχή μπορεί στην πραγματικότητα να περιέχει υποπεριοχές χωρισμένες με τελείες
- **zzz** είναι η κατάληξη που αντιστοιχεί στην περιοχή 1ου επιπέδου και συμβολίζει είτε το είδος της εταιρείας που παρέχει την υπηρεσία (.com, .edu, .org κλπ) είτε τη χώρα (.gr, .de, .fr κλπ)

Το ηλεκτρονικό ταχυδρομείο είναι μια υπηρεσία που χρησιμοποιεί το μοντέλο πε-

λάτη – εξυπηρετητή. Πελάτης είναι το πρόγραμμα που χρησιμοποιεί ο χρήστης για να γράψει, να λάβει και να στείλει e-mail (π.χ. Windows Live Mail, Outlook, Mozilla Thunderbird). Ο εξυπηρετητής e-mail (e-mail server) είναι μια δικτυακή υπηρεσία που εκτελείται σε υπολογιστή του παροχέα. Σε γενικές γραμμές:

Ο Πελάτης (client):

- Ξεκινάει την επαφή με τον εξυπηρετητή ταχυδρομείου
- Ζητά εξυπηρέτηση από τον εξυπηρετητή (π.χ. για να λάβει ή να στείλει mail)

Ο Εξυπηρετητής (server):

- Παρέχει στον πελάτη την εξυπηρέτηση που ζήτησε. Ο εξυπηρετητής είναι υπεύθυνος για να παραδώσει στον πελάτη τα μηνύματα που ήρθαν για αυτόν και να παραδώσει τα μηνύματα που στέλνει ο πελάτης στον εξυπηρετητή προορισμού προκειμένου να παραδοθούν στον πελάτη – παραλήπτη όταν τα ζητήσει.
- Κρατά σε ηλεκτρονική θυρίδα (mailbox) τα μηνύματα που δεν έχει ακόμα παραλάβει ο χρήστης. Σε άλλη αντίστοιχη θυρίδα (ουρά) κρατά τα μηνύματα που έχει παραλάβει από το χρήστη μέχρι να μπορέσει να τα αποστείλει στον προορισμό τους.

Τα πλεονεκτήματα του ηλεκτρονικού ταχυδρομείου είναι:

- Είναι πολύ γρήγορο (πρακτικά άμεσο)
- Ο χρήστης δεν χρειάζεται να παρακολουθεί τη μετάδοση του μηνύματος όπως π.χ. συμβαίνει με το φαξ
- Είναι πιο οικονομικό από το συμβατικό ταχυδρομείο
- Μπορούμε να στείλουμε εύκολα το ίδιο μήνυμα σε πολλούς χρήστες ταυτόχρονα

Ωστόσο υπάρχουν και μειονεκτήματα:

- Δεν υπάρχει απόλυτη εγγύηση ότι το μήνυμα έφτασε στο προορισμό του
- (Εκτός βιβλίου) Λαμβάνουμε μεγάλο αριθμό άσχετων / κακόβουλων μηνυμάτων, ιών κλπ – γνωστό και ως spam

Η μορφή των μηνυμάτων κειμένου ηλεκτρονικού ταχυδρομείου καθορίζεται από διεθνές πρότυπο. Ένα τέτοιο μήνυμα αποτελείται από:

- Την **επικεφαλίδα (header)**: Είναι ένα σύνολο γραμμών όπου κάθε γραμμή αποτελείται από μια λέξη – κλειδί, μια άνω-κάτω τελεία και μια τιμή. Για παράδειγμα:

```
From: sonic@thecompany.gr
To: mpampis@othercompany.gr
Reply-to: sonic@thecompany.gr
Subject: Testing Email
```

- Το **σώμα (body)** του μηνύματος: χωρίζεται από την επικεφαλίδα με μια κενή γραμμή. Το σώμα περιέχει το ASCII κείμενο του μηνύματος. Στην πραγματικότητα ακόμα και τα συνημμένα κωδικοποιούνται και μεταδίδονται με αντίστοιχη μορφή. Το τέλος του μηνύματος σηματοδοτείται από μια τελεία "." μόνη της σε μια γραμμή.

Τα βασικά πρωτόκολλα που χρησιμοποιούνται για τη διεκπεραίωση των διαδικασιών του ταχυδρομείου είναι τα **SMTP, POP3, IMAP** και βρίσκονται φυσικά στο επίπεδο εφαρμογής. Το SMTP είναι υπεύθυνο για την αποστολή ταχυδρομείου από το πελάτη προς τον εξυπηρετητή και μεταξύ εξυπηρετητών, ενώ τα άλλα δύο για τη λήψη μηνυμάτων από τον εξυπηρετητή στον πελάτη.

Με τι μοιάζει μια επικοινωνία SMTP;

Μπορούμε πράγματι να δούμε και να εκτελέσουμε μια επικοινωνία SMTP στέλνοντας μόνοι μας τις κατάλληλες εντολές, χωρίς να χρειαζόμαστε κάποιο πρόγραμμα ηλεκτρονικού ταχυδρομείου. Γενικά θα πρέπει να θυμάστε ότι στο επίπεδο εφαρμογής οι εντολές των πρωτοκόλλων είναι κατανοητές από τον άνθρωπο: πρόκειται για εντολές στα Αγγλικά, κατά βάση συντομεύσεις (συντμήσεις) λέξεων.

Στο παρακάτω παράδειγμα δείχνουμε πως θα ήταν η επικοινωνία ενός πελάτη με ένα εξυπηρετητή SMTP για την αποστολή ενός μηνύματος. Μπορούμε να εκτελέσουμε χειροκίνητα αυτή τη διαδικασία αν συνδεθούμε με ένα πρόγραμμα ικανό να στείλει ακολουθίες χαρακτήρων (εντολές) στη θύρα 25 (όπου βρίσκεται ο εξυπηρετητής SMTP). Στο παράδειγμα μας χρησιμοποιούμε το πρόγραμμα telnet για να συνδεθούμε σε ένα εξυπηρετητή SMTP που εκτελείται τοπικά σε ένα σύστημα UNIX:

```
$ telnet 127.0.0.1 25

Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 pegasus.chania-lug.gr ESMTP Sendmail 8.15.2/8.15.2;
    Thu, 23 Feb 2017 21:28:58 +0200 (EET)
```

Ο εξυπηρετητής μας απαντάει με το αναγνωριστικό του όπου μπορούμε να δούμε την έκδοση λογισμικού που εκτελεί, καθώς και την ημερομηνία / ώρα του συστή-

ματος. Για να ξεκινήσουμε την επικοινωνία, στέλνουμε την εντολή “helo” ή “ehlo” και το όνομα του συστήματος μας για αναγνώριση (και ναι, είναι με ένα “l” δεν είναι τυπογραφικό!). Προσέξτε ότι οι απαντήσεις του εξυπηρετητή ξεκινάνε με ένα αριθμό (π.χ. 250, 354 κλπ) και ακολουθεί επεξηγηματικό μήνυμα.

```
helo localhost
250 pegasus.chania-lug.gr Hello localhost [127.0.0.1],
    pleased to meet you
```

Ο εξυπηρετητής μας απαντάει με ένα μήνυμα καλωσορίσματος. Τώρα πρέπει να προχωρήσουμε στέλνοντας τα στοιχεία της επικεφαλίδας, και ακολούθως τα δεδομένα. Ξεκινάμε με την επικεφαλίδα:

```
mail from: sonic@chania-lug.gr
250 2.1.0 sonic@chania-lug.gr... Sender ok
```

Ο εξυπηρετητής επιβεβαιώνει ότι η διεύθυνση αποστολέα είναι δεκτή.

```
rcpt to: mpampis@freebsdworld.gr
250 2.1.5 mpampis@freebsdworld.gr... Recipient ok
```

Επιβεβαιώνεται επίσης η διεύθυνση παραλήπτη. Είμαστε έτοιμοι να στείλουμε το σώμα του email γράφοντας την εντολή “data” (στο παράδειγμα μας παραλείψαμε το θέμα):

```
data
354 Enter mail, end with ”.” on a line by itself
```

Ο εξυπηρετητής μας προτρέπει να γράψουμε το μήνυμα μας και να τελειώσουμε με μια τελεία “.” σε μια γραμμή από μόνη της.

```
Hello, this is a test mail
.
250 2.0.0 v1NJaK3Q095307 Message accepted for delivery
```

Ο εξυπηρετητής επιβεβαιώνει ότι δέχτηκε να παραδώσει το μήνυμα μας στον παραλήπτη. Σε αυτό το σημείο, μπορούμε να αποσυνδεθούμε από τον εξυπηρετητή.

```
quit
221 2.0.0 pegasus.chania-lug.gr closing connection
```

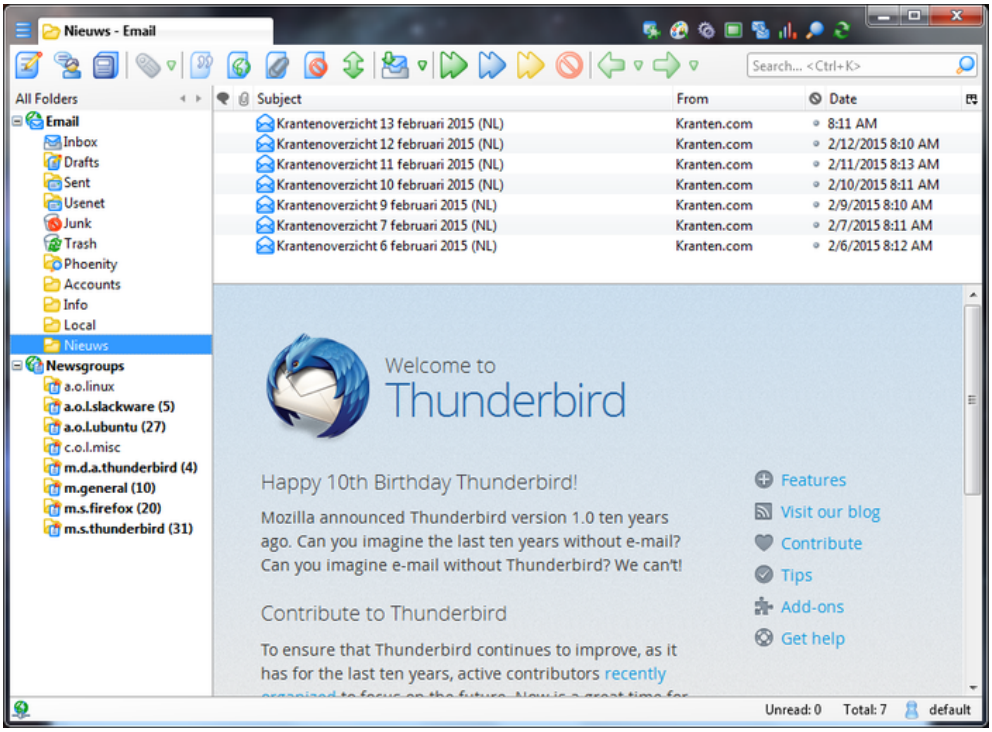
Στην πραγματικότητα κάθε φορά που στέλνετε ένα mail μέσω ενός προγράμματος όπως το Thunderbird, το πρόγραμμα στέλνει αυτές τις εντολές για εσάς. Όπως βλέπετε δεν υπάρχει κάτι το μυστηριώδες στις εντολές πρωτοκόλλων του επιπέδου εφαρμογής!

Πως ολοκληρώνεται η προηγούμενη επικοινωνία; Ο εξυπηρετητής που παρέλαβε το μήνυμα μας θα βρει (μέσω ερωτήματος στο DNS) ποιος είναι ο εξυπηρετητής ταχυδρομείου που είναι υπεύθυνος για την περιοχή που ανήκει ο παραλήπτης (στο παράδειγμα μας, θα ψάξει ποιος εξυπηρετητής ταχυδρομείου είναι υπεύθυνος για τον τομέα freebsdworld.gr π.χ. ο mail.freebsdworld.gr). Έπειτα θα επικοινωνήσει με τον εξυπηρετητή αυτό χρησιμοποιώντας πάλι το πρωτόκολλο SMTP και θα του παραδώσει το μήνυμα για το χρήστη mpampis. Ο παραλήπτης του μηνύματος θα συνδεθεί με το δικό του πρόγραμμα (π.χ. Thunderbird, σχήμα 6.8) και θα κατεβάσει το μήνυμα από το διακομιστή χρησιμοποιώντας το πρωτόκολλο POP3 ή IMAP.

- Το πρωτόκολλο **SMTP, Simple Mail Transfer Protocol** ή Πρωτόκολλο Μεταφοράς Απλών Μηνυμάτων χρησιμοποιείται όταν παραδίδεται ένα μήνυμα από ένα πελάτη προς ένα διακομιστή ηλεκτρονικού ταχυδρομείου προκειμένου να παραδοθεί σε ένα παραλήπτη. Χρησιμοποιείται επίσης και για την αποστολή μηνυμάτων μεταξύ εξυπηρετητών e-mail. Το SMTP παραδοσιακά χρησιμοποιεί τη θύρα 25 όπου τα μηνύματα μεταδίδονται χωρίς κρυπτογράφηση, ενώ οι σύγχρονες εκδοχές χρησιμοποιούν τη θύρα 465 για κρυπτογραφημένη επικοινωνία SSL ή την 587 για TLS.

- Το πρωτόκολλο **POP3, Post Office Protocol 3** ή πρωτόκολλο ταχυδρομικού γραφείου, χρησιμοποιείται στο πρόγραμμα – πελάτη (e-mail client) προκειμένου να συνδεθεί στον διακομιστή ταχυδρομείου και να κατεβάσει τα μηνύματα ηλεκτρονικού ταχυδρομείου στον τοπικό υπολογιστή. Το πρωτόκολλο αυτό είναι αρκετά απλό και δεν προσφέρει ιδιαίτερες δυνατότητες εκτός από τη λήψη. Μετά τη σύνδεση και την επαλήθευση στοιχείων κατεβάζει όλα τα μηνύματα από τον εξυπηρετητή στο τοπικό μηχάνημα, κατόπιν τα διαγράφει από τον εξυπηρετητή και αποσυνδέεται. Υπάρχει η δυνατότητα να παραμείνουν αντίγραφα των μηνυμάτων στο διακομιστή μέσω ρύθμισης στο e-mail client. Το POP3 χρησιμοποιεί τη θύρα 110 ενώ η παραλλαγή με κρυπτογράφηση χρησιμοποιεί την 995 (SSL).

- Το πρωτόκολλο **IMAP, Internet Message Access Protocol** ή πρωτόκολλο πρόσβασης ηλεκτρονικού ταχυδρομείου έχει αρκετά παρόμοια χαρακτηριστικά με το POP3 αλλά και πρόσθετες δυνατότητες. Πρόκειται επίσης για πρωτόκολλο που χρησιμοποιείται για να διαβάσει ο πελάτης τα μηνύματα από ένα διακομιστή ταχυδρομείου. Έχει σχεδιαστεί για να επιτρέπει στους χρήστες να διατηρούν τα mail τους στον διακομιστή, αντί να τα κατεβάζουν εξ'ολοκλήρου στον τοπικό τους υπολογιστή. Το IMAP απαιτεί περισσότερο χώρο στο δίσκο του κεντρικού υπολογιστή ταχυδρομείου (mail server) και περισσότερη υπολογιστική ισχύ (CPU) από το POP3 καθώς τα μηνύματα παραμένουν στο διακομιστή. Το IMAP χρησιμοποιεί τη θύρα TCP 143 ή την 993 για κρυπτογραφημένη επικοινωνία (SSL).



Σχήμα 6.8: *Το Πρόγραμμα Thunderbird (e-mail client)*

Ένας διαφορετικός τύπος ηλεκτρονικού ταχυδρομείου είναι το *Web mail* που χρησιμοποιεί το πρωτόκολλο HTTP για να ολοκληρωθεί η επικοινωνία και διαβάζεται μέσα από κάποιο browser (φυλλομετρητή). Αυτό το είδος ηλεκτρονικού ταχυδρομείου είναι μια υπηρεσία του Παγκόσμιου Ιστού (World Wide Web).

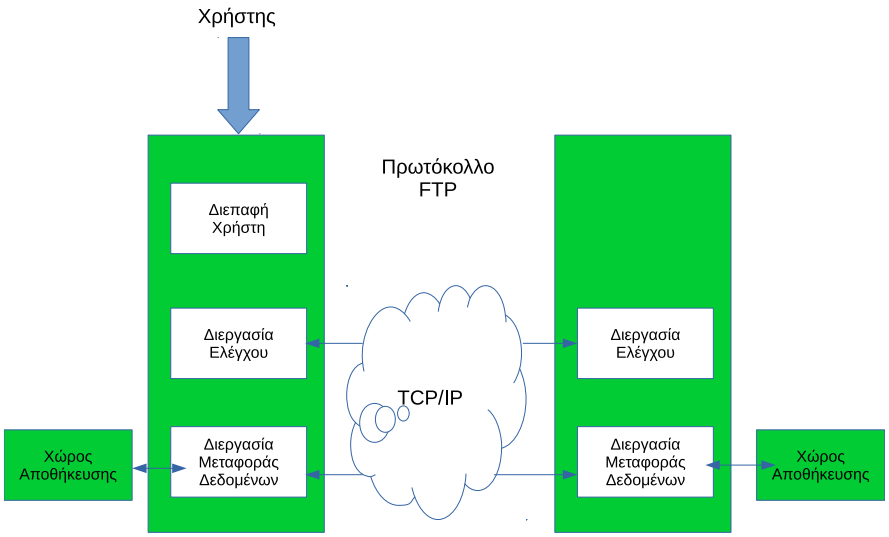
Για να μπορέσει ένας χρήστης να διαβάσει τα μηνύματα του, θα πρέπει να πιστοποιηθεί από τον εξυπηρετητή εισερχόμενης αλληλογραφίας (POP3 ή IMAP) χρησιμοποιώντας κατάλληλο όνομα χρήστη (User Id ή Login) και κωδικό (Password). Έτσι μπορεί να διαπιστωθεί ότι είναι πράγματι ο χρήστης στον οποίο αντιστοιχεί η ηλεκτρονική διεύθυνση που προσπαθεί να προσπελάσει.

6.2.2 Υπηρεσία Μεταφοράς Αρχείων (FTP, TFTP)

Και τα δύο αυτά πρωτόκολλα ασχολούνται με τη μεταφορά αρχείων μεταξύ δύο συστημάτων που συνδέονται σε ένα δίκτυο τεχνολογίας TCP/IP.

Το *FTP, File Transfer Protocol* ή Πρωτόκολλο Μεταφοράς Αρχείων χρησιμοποιείται για αποστολή / λήψη αρχείων από ένα απομακρυσμένο εξυπηρετητή. Το FTP

πραγματοποιεί δυο συνδέσεις μεταξύ του πελάτη και του εξυπηρετητή: στη μια μεταφέρονται εντολές και πληροφορίες ελέγχου και στην άλλη τα δεδομένα που πρόκειται να μεταφερθούν. Για να γίνει ταυτοποίηση του χρήστη που συνδέεται, γίνεται χρήση ονόματος (username) και κωδικού πρόσβασης (password). Με την ολοκλήρωση της διαδικασίας εισόδου, ο χρήστης μπορεί να επιλέξει και να μεταφέρει τα αρχεία που επιθυμεί. Το FTP μπορεί να χειριστεί τόσο αρχεία απλού κειμένου (text) όσο και δυαδικά (binary). Οι εντολές και τα δεδομένα ελέγχου μεταφέρονται μέσα από τη θύρα 21 που ενεργοποιείται κατά την έναρξη της σύνδεσης. Τα δεδομένα μεταφέρονται από τη θύρα 20.



Σχήμα 6.9: *Μοντέλο Λειτουργίας FTP*

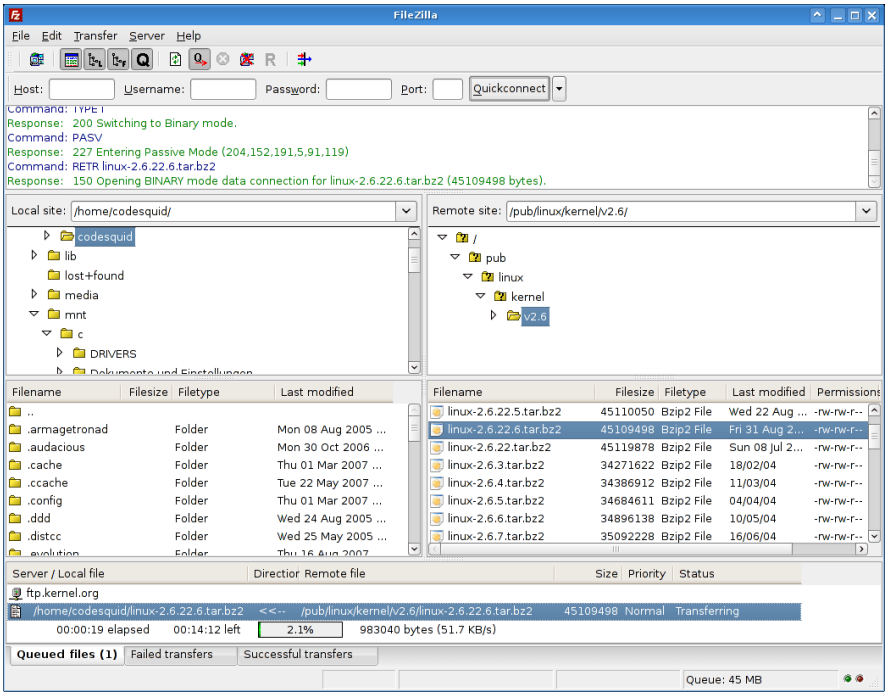
Τι μειονέκτημα έχει το FTP στις μέρες μας;

Το FTP (όπως και το mail) είναι από τα πλέον παλιά πρωτόκολλα εφαρμογής της τεχνολογίας TCP/IP. Την εποχή που φτιάχτηκε ο κόσμος ήταν αρκετά πιο “αθώος” από σήμερα. Το FTP μεταφέρει όλες τις πληροφορίες του χωρίς κανένα είδος κρυπτογράφησης. Ακόμα και το όνομα χρήστη και ο κωδικός πρόσβασης μεταφέρονται σαν απλό κείμενο μέσα από τις γραμμές του δικτύου. Αυτό φυσικά σημαίνει ότι στις μέρες μας οποιοσδήποτε θα μπορούσε να τα υποκλέψει. Για το λόγο αυτό σήμερα το FTP σπάνια χρησιμοποιείται με πραγματικούς κωδικούς πρόσβασης (έχει αντικατασταθεί για το σκοπό αυτό με άλλες ασφαλείς παραλλαγές). Σήμερα χρησιμοποιούμε περισσότερο το *ανώνυμο* FTP όπου συνδεόμαστε σε ένα εξυπηρετητή ουσιαστικά χωρίς να έχουμε λογαριασμό (ως επισκέπτες) αλλά και χωρίς να έχουμε δικαιώματα πέρα από το να κατεβάσουμε συγκεκριμένα αρχεία που έχει επιλέξει ο διαχειριστής. Αυτού του είδους ο εξυπηρετητής συχνά είναι ρυθμισμένος να επιτρέπει πρόσβαση

μόνο σε επισκέπτες και όχι σε αναγνωρισμένους χρήστες.

Με τι μοιάζουν οι εντολές του FTP;

Όπως φαντάζεστε, σπάνια χρησιμοποιούμε απευθείας τις εντολές για να συνδεθούμε σε ένα εξυπηρετητή FTP. Συνήθως χρησιμοποιούμε κάποιο πρόγραμμα πελάτη όπως το filezilla (σχήμα 6.10). Ωστόσο και οι εντολές του FTP είναι απλές, όπως είδαμε και στο SMTP. Βασικές εντολές είναι η **get** για να πάρουμε ένα αρχείο, η **put** για να στείλουμε αρχείο (αν έχουμε συνδεθεί με όνομα και κωδικό) και η **cd** για να μετακινηθούμε σε άλλο κατάλογο (φάκελο). Για να δούμε τα περιεχόμενα ενός καταλόγου χρησιμοποιούμε την **ls**. Όπως φαντάζεστε, ένα γραφικό πρόγραμμα – πελάτης απλά αναλαμβάνει να στείλει τις ίδιες αυτές εντολές για μας.



Σχήμα 6.10: *Πρόγραμμα Πελάτης FTP (Filezilla)*

Το πρωτόκολλο **TFTP, Trivial File Transfer Protocol** είναι μια πιο απλή εκδοχή του FTP. Μπορεί να μεταφέρει αρχεία μεταξύ πελάτη και εξυπηρετητή, αλλά δεν παρέχει έλεγχο ταυτότητας χρήστη και άλλες χρήσιμες λειτουργίες που διαθέτει το κανονικό FTP. Το TFTP χρησιμοποιεί UDP στο επίπεδο μεταφοράς, ενώ το FTP χρησιμοποιεί TCP. Ο παρακάτω πίνακας δείχνει τις διαφορές μεταξύ των δύο πρωτοκόλλων.

FTP (File Transfer Protocol)	TFTP (Trivial File Transfer Protocol)
Χρησιμοποιεί το TCP στο επίπεδο μεταφοράς	Χρησιμοποιεί το UDP στο επίπεδο μεταφοράς
Χρησιμοποιεί ισχυρές εντολές ελέγχου	Χρησιμοποιεί απλές εντολές ελέγχου
Στέλνει δεδομένα και εντολές από χωριστές συνδέσεις TCP	Δεν χρησιμοποιεί συνδέσεις γιατί το UDP είναι πρωτόκολλο χωρίς σύνδεση
Απαιτεί περισσότερη μνήμη και υπολογιστική ισχύ	Απαιτεί λιγότερη μνήμη και υπολογιστική ισχύ

6.2.3 Υπηρεσία Παγκόσμιου Ιστού WWW

Η πιο γνωστή και διαδεδομένη υπηρεσία του Διαδικτύου, είναι ο Παγκόσμιος Ιστός ή World Wide Web (www). Είναι τόσο διαδεδομένη που ο περισσότερος κόσμος τη συγχέει με την ίδια την έννοια του Διαδικτύου. Ωστόσο αυτό είναι λάθος: ο Παγκόσμιος Ιστός είναι απλά μια υπηρεσία που χρησιμοποιεί το Διαδίκτυο για να μεταφέρει τις πληροφορίες της. Ο Παγκόσμιος Ιστός είναι ένα είδος διαμορφωμένης πληροφορίας που χτίζεται πάνω από το Διαδίκτυο.

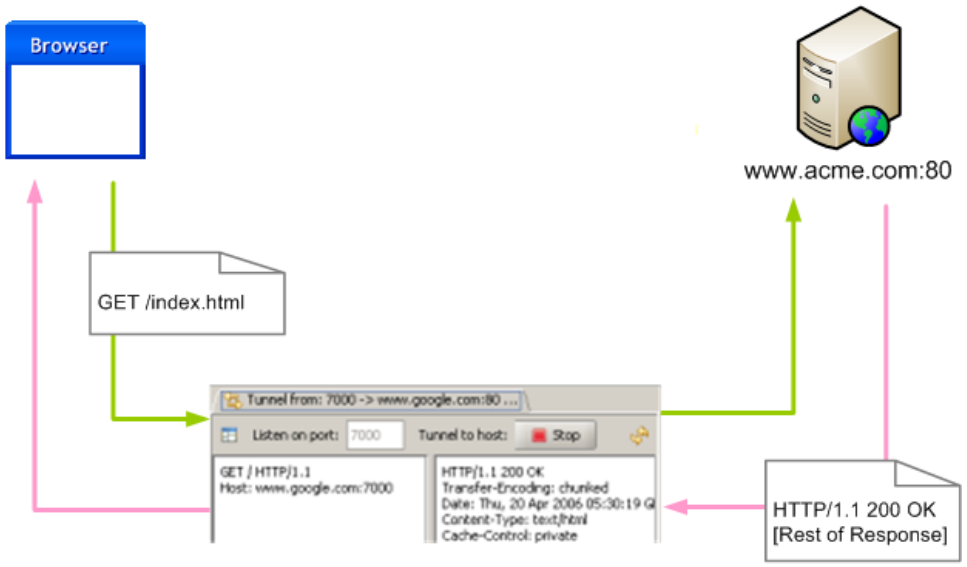
Ένα γνώρισμα του Παγκόσμιου Ιστού είναι η μη γραμμική οργάνωση της πληροφορίας του, όπως περίπου συμβαίνει σε ένα λεξικό: όταν ψάχνουμε μια λέξη δεν παίρνουμε το λεξικό από την αρχή, αλλά βρίσκουμε πρώτα το γράμμα και μετά μια κοντινή λέξη και ακολουθούμε τις λέξεις μέχρι τη σωστή.

Στον παγκόσμιο ιστό, ορίζονται οι έννοιες του *υπερκειμένου* και του *υπερμέσου*:

- **Υπερκείμενο (hypertext):** Είναι το κείμενο όπου η πληροφορία δεν είναι οργανωμένη με γραμμική μορφή, η αναζήτηση της δε γίνεται με κάποια συγκεκριμένη σειρά, αλλά με τυχαία, ακολουθώντας τους συνδέσμους που υπάρχουν στο σώμα του κειμένου.
- **Υπερμέσα (hypermedia):** Μια συλλογή πολυμεσικών στοιχείων (εικόνα, ήχος, βίντεο, κινούμενα σχέδια, animation) οργανωμένη με μη γραμμικό τρόπο.

Ο παγκόσμιος ιστός χρησιμοποιεί το πρωτόκολλο *HTTP (Hyper Text Transfer Protocol)* για να μεταφέρει δεδομένα. Όπως φαντάζεστε, όπως και τα υπόλοιπα πρωτόκολλα στο επίπεδο εφαρμογής, το HTTP διαθέτει κάποιες απλές εντολές στα Αγγλικά με τις οποίες ο πελάτης επικοινωνεί με τον εξυπηρετητή και ζητά στοιχεία.

Το ρόλο του εξυπηρετητή αναλαμβάνουν προγράμματα γνωστά ως *web servers*. Ένα από τα πλέον γνωστά είναι ο *Apache Web Server*. Οι πληροφορίες είναι οργανωμένες σε μορφή ιστοσελίδων (web pages) και κάθε μια αντιστοιχεί σε ένα αρχείο HTML



Σχήμα 6.11: *Επικοινωνία HTTP*

στο δίσκο του διακομιστή. Οι ιστοσελίδες είναι μια εφαρμογή υπερμέσων (περιέχουν εικόνες, κείμενο, video κλπ). Για να προσπελάσουμε μια ιστοσελίδα πρέπει να ξέρουμε τη διεύθυνση της, γνωστή και ως *URL*, *Uniform Resource Locator*. Το URL εκτός από το όνομα αρχείου, περιέχει και την πλήρη διαδρομή που χρειαζόμαστε για να εντοπίσουμε τη σελίδα (τον εξυπηρετητή και το φάκελο στον οποίο βρίσκεται το αρχείο).

Ας πάρουμε για παράδειγμα τη σελίδα **http://www.ntua.gr/info/studies.html**. Μπορούμε να την αναλύσουμε στα παρακάτω στοιχεία:

- **http:** Είναι το πρωτόκολλο της υπηρεσίας που ανήκει η ιστοσελίδα. Αν είναι “https” πρόκειται για ασφαλή σύνδεση http
- **www:** Δηλώνει ότι πρόκειται για σελίδα του ιστού. Μπορεί σε κάποιες περιπτώσεις να παραλείπεται
- **ntua.gr:** Είναι η διεύθυνση του εξυπηρετητή ιστοσελίδων. Το κομμάτι αυτό όπως μπορείτε να αναγνωρίσετε είναι μια περιοχή 2ου επιπέδου, που ουσιαστικά αναφέρεται στην διεύθυνση IP του εξυπηρετητή και αναλύεται μέσω DNS
- **/info/:** Αναφέρεται σε ένα φάκελο (κατάλογο ή directory) στο web server
- **studies.html:** Είναι το αρχείο που περιέχει την ιστοσελίδα που θέλουμε να προσπελάσουμε

Οι ιστοσελίδες περιέχουν *σημεία σύνδεσης ή hyperlinks* τα οποία μπορεί να είναι κείμενο, εικόνα κλπ. Ένα σημείο σύνδεσης μπορεί να παραπέμπει:

- Σε άλλο σημείο πάνω στην ίδια σελίδα (anchor)
- Σε άλλη ιστοσελίδα στον ίδιο εξυπηρετητή / site (εσωτερικός σύνδεσμος)
- Σε άλλη ιστοσελίδα άλλου εξυπηρετητή / διαφορετικού site οπουδήποτε στο Διαδίκτυο (εξωτερικός σύνδεσμος)

Η ίδια η ιστοσελίδα δεν ακολουθεί τις συμβάσεις των έντυπων βιβλίων (συγκεκριμένο μέγεθος για εκτύπωση σε χαρτί) αλλά μπορεί να έχει μεγαλύτερο μήκος και πλάτος από ότι εμφανίζεται στην οθόνη (εξάλλου, διαφορετικές οθόνες έχουν διαφορετική ανάλυση και ειδικά σε φορητές συσκευές υπάρχει μεγάλη διακύμανση).

Ένα σύνολο πληροφοριών που οργανώνεται σε μορφή ιστοσελίδων ονομάζεται *τοποθεσία (site)*.

Οι *Φυλλομετρητές (browsers)* είναι το πρόγραμμα πελάτης που χρησιμοποιεί ο χρήστης για να απευθύνει αιτήματα στο Web Server. Υπάρχουν πολλά προγράμματα φυλλομετρητών για διάφορα λειτουργικά συστήματα: Firefox, Chrome, Opera, Edge κλπ. Οι βασικές λειτουργίες που συναντάμε σε ένα πρόγραμμα φυλλομετρητή, είναι:

- Αποστέλλει αιτήματα / ερωτήματα στους εξυπηρετητές ιστοσελίδων χρησιμοποιώντας το πρωτόκολλο HTTP
- Σχεδιάζει την ιστοσελίδα σύμφωνα με τις πληροφορίες που του έστειλε ο εξυπηρετητής. Οι φυλλομετρητές διαθέτουν μια μηχανή απεικόνισης που ερμηνεύει τις εντολές της γλώσσας HTML και σχεδιάζει τη σελίδα στην οθόνη σύμφωνα με αυτές
- Τονίζει τα σημεία σύνδεσης όπου υπάρχουν, ώστε να είναι ευδιάκριτα και να εντοπίζονται εύκολα από το χρήστη πάνω στη σελίδα
- Δίνει τη δυνατότητα αποθήκευσης των ιστοσελίδων σε καταλόγους
- Κρατάει ιστορικό με τις διευθύνσεις των ιστοσελίδων που έχουμε επισκεφθεί

Με τους φυλλομετρητές έχουμε τη δυνατότητα να διαβάζουμε ιστοσελίδες του Διαδικτύου, οι οποίες είναι στη πραγματικότητα σελίδες υπερμέσων (μπορούν να περιέχουν φωτογραφίες, ήχο, animation κλπ). Για να διαβάσουμε μια ιστοσελίδα θα πρέπει να ξέρουμε το όνομα της, το φάκελο στον οποίο είναι αποθηκευμένη και τη διεύθυνση του web server (με λίγα λόγια το URL της). Στην πραγματικότητα τα πράγματα είναι πιο απλά: τυπικά δεν χρειάζεται να θυμόμαστε τίποτα περισσότερο από τη διεύθυνση του εξυπηρετητή. Οι εξυπηρετητές είναι ρυθμισμένοι όταν δεν ζητηθεί κάποια συγκεκριμένη ιστοσελίδα να δίνουν μια *αρχική προεπιλεγμένη*

σελίδα (default page). Συνήθως αντιστοιχεί στο αρχείο index.html ή index.htm ή default.html. Μέσα από τους συνδέσμους που υπάρχουν σε αυτή τη σελίδα μπορούμε να αναζητήσουμε τις πληροφορίες που θέλουμε αλλά και να πλοηγηθούμε στις υπόλοιπες σελίδες του site.

Κεφάλαιο 7

Διαχείριση Δικτύου

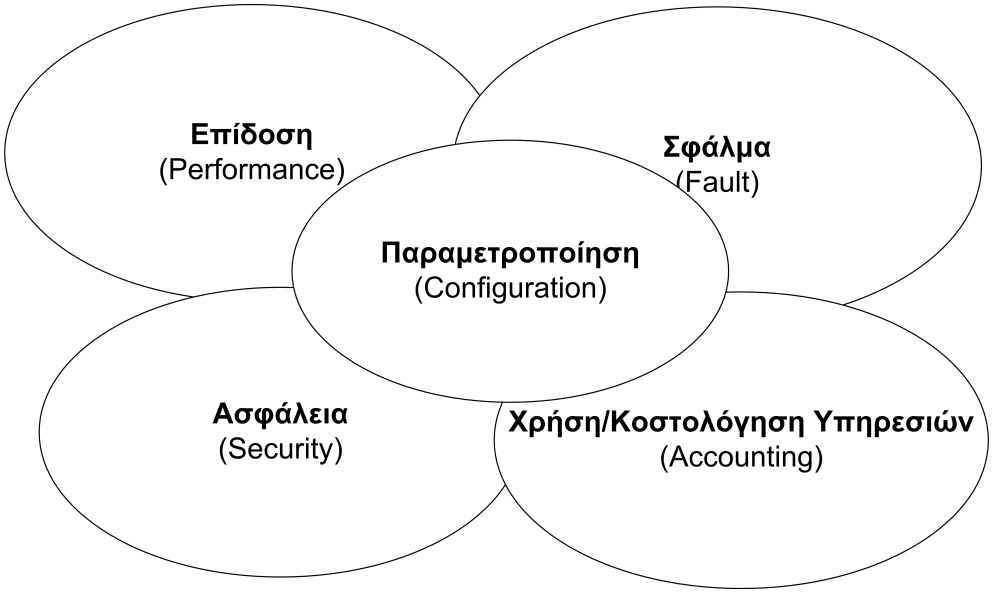
7.2 Περιοχές / Τομείς Διαχείρισης Δικτύου στο Μοντέλο OSI

Σε δίκτυα μεσαίου και μεγάλου μεγέθους είναι σχεδόν πάντοτε απαραίτητος ο σχεδιασμός και η εγκατάσταση ενός *Συστήματος Διαχείρισης Δικτύου, NMS (Network Management System)*. Ένα τέτοιο σύστημα αποτελείται από υλικό και λογισμικό που επιτρέπει στο διαχειριστή να επιβλέπει (και σε αρκετές περιπτώσεις να ρυθμίζει) τα στοιχεία που αποτελούν το δίκτυο και να ελέγχει για σημεία με προβληματική λειτουργία. Η διαχείριση γίνεται από κεντρικό σημείο, τυπικά από ένα υπολογιστή που έχει οριστεί ως υπολογιστής διαχείρισης (Manager Server).

Η Διαχείριση Δικτύου στο μοντέλο OSI χωρίζεται σε πέντε περιοχές, όπως φαίνεται στο σχήμα 7.1. Οι περιοχές αυτές είναι:

- Παραμετροποίηση (Configuration Management)
- Διαχείριση Σφαλμάτων (Fault Management)
- Διαχείριση Επιδόσεων (Performance Management)
- Διαχείριση Κόστους (Accounting Management)
- Διαχείριση Ασφάλειας (Security Management)

Το μοντέλο αυτό ονομάζεται και *FCAPS* από τα αρχικά των λέξεων *Fault Configuration Accounting Performance Security*. Παρακάτω θα εξηγήσουμε τις διαδικασίες αυτές.



Σχήμα 7.1: *Περιοχές Διαχείρισης του OSI*

7.2.1 Παραμετροποίηση

Η *Διαχείριση Παραμετροποίησης (Configuration Management, CM)* ασχολείται με την παρακολούθηση των παραμέτρων του δικτύου και των αλλαγών που συμβαίνουν σε αυτό.

Τα προβλήματα που παρουσιάζονται σε ένα δίκτυο είναι συχνά αποτέλεσμα των αλλαγών που κάνει ο διαχειριστής στις ρυθμίσεις του. Αυτή η περιοχή διαχείρισης είναι πολύ σημαντική γιατί παρακολουθεί και καταγράφει όλες αυτές τις αλλαγές.

Πότε γίνονται αλλαγές στις ρυθμίσεις;

Αλλαγές στις ρυθμίσεις μπορεί να γίνουν όταν:

- Ο διαχειριστής του δικτύου προσθέτει ή αφαιρεί υπολογιστές ή δικτυακό υλικό
- Ο διαχειριστής προσθέτει ή αφαιρεί εφαρμογές (λογισμικό)
- Ο διαχειριστής αλλάζει τις ρυθμίσεις μιας συσκευής την ώρα που αυτή είναι σε χρήση
- Γίνονται αυτόματες ενημερώσεις στο λογισμικό ή εγκατάσταση νέων εκδόσεων κλπ

- Γίνεται αναβάθμιση στα ενσωματωμένα προγράμματα (firmware) δικτυακών συσκευών (δρομολογητών, switch κλπ.)

Μια σωστή διαχείριση παραμετροποίησης περιλαμβάνει την καταγραφή όλων των παραπάνω (και ακόμα περισσότερων) αλλαγών. Η καταγραφή μπορεί φυσικά να γίνεται χειροκίνητα χωρίς χρήση λογισμικού, αλλά σε οποιοδήποτε μεγάλο δίκτυο αυτό γενικά είναι χρονοβόρο και οδηγεί σε σφάλματα. Συνήθως χρησιμοποιείται κατάλληλο λογισμικό διαχείρισης παραμέτρων όπως το CiscoWorks 2000 ή το Infosim.

Η διαχείριση παραμέτρων περιλαμβάνει τους παρακάτω στόχους:

- Τη συλλογή και αποθήκευση παραμέτρων των συσκευών του δικτύου, είτε τοπικά είτε από απόσταση (δεν είναι πάντα δυνατή η απομακρυσμένη διαχείριση μιας συσκευής: οι πιο απλές / φτηνές δικτυακές συσκευές δεν διαθέτουν περιβάλλον απομακρυσμένης διαχείρισης)
- Την απλοποίηση της παραμετροποίησης των συσκευών
- Την παρακολούθηση αλλαγών που συμβαίνουν στις παραμέτρους
- Τη διαμόρφωση νοητών κυκλωμάτων μέσα από δίκτυα χωρίς μεταγωγή (non-switched networks). Πρόκειται για το λεγόμενο *provisioning*: ο διαχειριστής βρίσκει διαδρομές και καθορίζει τα νοητά κυκλώματα που θα χρησιμοποιηθούν στην δικτυακή επικοινωνία
- Το σχεδιασμό και την πρόβλεψη μελλοντικών επεκτάσεων

Η διαχείριση παραμέτρων υλικού και λογισμικού αποτελείται από πέντε ξεχωριστές δράσεις:

Σημείωση: Τα παρακάτω σημεία είναι μετάφραση στο βιβλίο σας από το αντίστοιχο άρθρο της Wikipedia. Προσπαθήσαμε εδώ να κάνουμε καλύτερη μετάφραση γιατί δυστυχώς στο σχολικό βιβλίο δεν βγαίνει νόημα…

- **Σχεδιασμός και Διαχείριση Παραμέτρων:** Πρόκειται για ένα επίσημο έγγραφο που περιγράφει τους τομείς και τις παραμέτρους με τις οποίες ασχολείται η διαχείριση και περιλαμβάνει μεταξύ άλλων:
  - Το προσωπικό
  - Τις διαδικασίες εκπαίδευσης
  - Τα εργαλεία και τις διαδικασίες που πρέπει να ακολουθούνται

  - Τις μεθόδους ελέγχου κ.α.

- **Ταυτοποίηση Παραμετροποίησης:** Ορίζει τις βασικές προδιαγραφές και παραμέτρους του δικτύου (baseline) με βάση τις οποίες γίνεται κατόπιν η παρακολούθηση των αλλαγών σε αυτό

- **Έλεγχος Παραμετροποίησης:** Περιλαμβάνει την αξιολόγηση όλων των προτάσεων για αλλαγές ή βελτιώσεις πάνω στο δίκτυο. Κατά τον έλεγχο κάποιες αλλαγές μπορεί να εγκρίνονται και άλλες να απορρίπτονται

- **Κοστολόγηση Κατάστασης Παραμετροποίησης:** (Σημείωση: κανονικά δεν είναι κοστολόγηση, αλλά καταγραφή) Περιλαμβάνει την καταγραφή και αναφορά όλων των παραμέτρων του δικτύου (υλικού, λογισμικού, firmware κλπ) και των αποκλίσεων τους σε σχέση με τις αρχικές προδιαγραφές

- **Επαλήθευση και Αξιολόγηση Παραμετροποίησης:** Πρόκειται για μια ανεξάρτητη έκθεση αξιολόγησης του υλικού και του λογισμικού του δικτύου προκειμένου να διαπιστωθεί αν τηρεί συγκεκριμένες προδιαγραφές που απαιτούνται από κανονισμούς (π.χ. για στρατιωτική χρήση κλπ.)

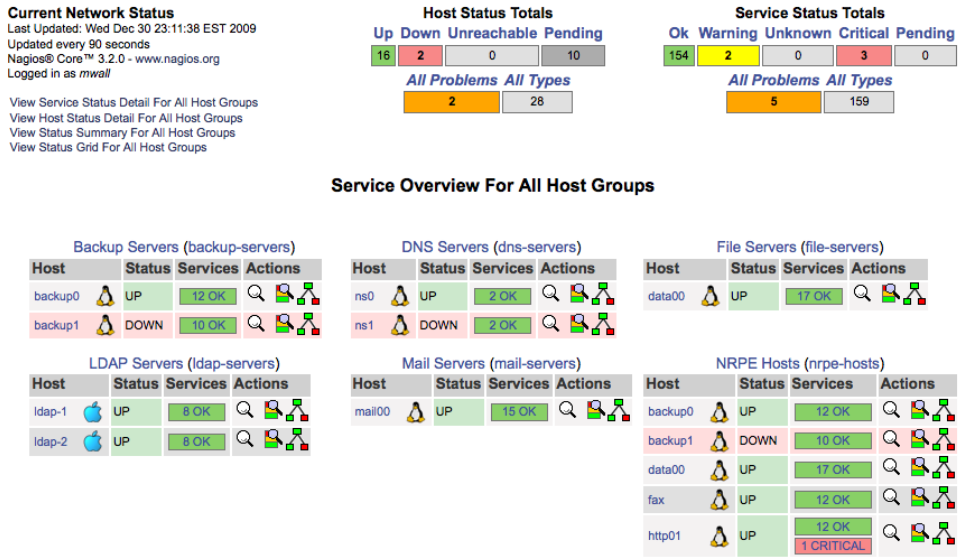
7.2.2 Διαχείριση Σφαλμάτων

Για να λειτουργεί σωστά το δίκτυο, θα πρέπει να φροντίζουμε να λειτουργούν σωστά τα επιμέρους στοιχεία του. Σε ένα δίκτυο μπορεί να συμβαίνουν τόσο βλάβες / σφάλματα όσο και λάθη.

Σημείωση: Το βιβλίο εδώ αναφέρει το “σφάλμα” ως συνώνυμο της “βλάβης”. Στην πραγματικότητα “σφάλμα” και “λάθος” είναι συνώνυμες λέξεις στα ελληνικά. Στην ξένη βιβλιογραφία η βλάβη αναφέρεται ως **fault** ενώ το λάθος ως **error** και είναι πράγματι διαφορετικές έννοιες όπως θα δείτε στους παρακάτω ορισμούς.

Βλάβη ή σφάλμα είναι μια μη φυσιολογική κατάσταση που απαιτεί την προσοχή του διαχειριστή και την άμεση διόρθωση του. Μια βλάβη συνεπάγεται μη σωστή λειτουργία ή μεγάλο αριθμό λαθών και προβλημάτων. Για παράδειγμα ένα καλώδιο δικτύου το οποίο δεν κάνει καλή επαφή μπορεί να προκαλεί διακοπές στο δίκτυο ή μεγάλο αριθμό από λανθασμένα bit.

Λάθος είναι ένα μεμονωμένο γεγονός το οποίο συνήθως δεν συνεπάγεται διακοπή της επικοινωνίας. Σε πολλές περιπτώσεις το δίκτυο μπορεί να διορθώνει αυτόματα λάθη που οφείλονται σε τυχαία γεγονότα (π.χ. παρεμβολή σε ένα καλώδιο δικτύου



Σχήμα 7.2: *Σύστημα Διαχείρισης Δικτύου (NMS)*

μπορεί να προκαλέσει τη λανθασμένη λήψη κάποιων bit) χρησιμοποιώντας μηχανισμούς ελέγχου που περιέχονται στα ίδια τα πρωτόκολλα (θυμηθείτε π.χ. ότι το TCP έχει άθροισμα ελέγχου και τη δυνατότητα να μεταδώσει ξανά τα χαλασμένα τμήματα).

Ο εντοπισμός ενός σφάλματος (βλάβης) μπορεί να γίνει έμμεσα, με την *παρατήρηση ενδείξεων* από την κίνηση και τη συμπεριφορά του δικτύου σε πραγματικό χρόνο (παρατηρούμε ότι μια σελίδα που κανονικά ανοίγει πολύ γρήγορα καθυστερεί υπερβολικά, ή ότι ένας κοινόχρηστος φάκελος στο δίκτυο δεν ανταποκρίνεται) είτε σε *μορφή συναγερμού (alarm)* εφόσον έχουμε εγκαταστήσει ένα Σύστημα Διαχείρισης Δικτύου (σχήμα 7.2).

Σε περίπτωση σφάλματος, υπάρχουν συγκεκριμένα βήματα που πρέπει να ακολουθήσουμε για την αντιμετώπιση του και γενικά ονομάζονται *Κύκλος Επεξεργασίας Διαχείρισης Σφαλμάτων, Fault Management Process Cycle*. Τα συνήθη βήματα είναι τα παρακάτω:

- **Να προσδιοριστεί το σφάλμα**, να βρεθεί δηλαδή τι είδους σφάλμα είναι και από που μπορεί να προέρχεται
- **Να εντοπιστεί το σφάλμα**, ώστε να ανακαλυφθεί σε πιο σημείο του δικτύου βρίσκεται
- **Να απομονωθεί το υπόλοιπο του δικτύου**, ώστε να λειτουργεί χωρίς να εμποδίζεται από το σφάλμα

- **Να αναδιαμορφωθεί το δίκτυο** ώστε να μπορεί να λειτουργεί όσο το δυνατόν καλύτερα για όσο υπάρχει ακόμα το σφάλμα
- **Να γίνει έλεγχος και ανάλυση των ενδείξεων** ώστε να κατανοηθεί καλύτερα η αιτία και να δοθεί μια καλύτερη εξήγηση της πηγής του σφάλματος
- **Να επισκευαστεί ή να αντικατασταθεί** το υλικό ή το λογισμικό που προκάλεσε τη βλάβη ώστε το δίκτυο να επανέλθει στην προηγούμενη του λειτουργική κατάσταση
- **Να παρακολουθηθεί το δίκτυο** από το διαχειριστή για ένα προκαθορισμένο χρονικό διάστημα ώστε να επιβεβαιωθεί η σωστή λειτουργία του και να είμαστε σίγουροι ότι το σφάλμα επιλύθηκε επιτυχώς

Η επίδραση που έχει ένα σφάλμα στο δίκτυο μπορεί να μετριαστεί αν έχουμε φροντίσει να υπάρχουν για παράδειγμα πολλαπλές (εναλλακτικές) διαδρομές που να ενώνουν δυο σημεία επικοινωνίας (αλλαγή διαδρομής). Όσο αφορά το δικτυακό υλικό, μπορούμε να διαθέτουμε πολλαπλές δικτυακές συσκευές για την ίδια εργασία ώστε να αναλαμβάνει κάποια άλλη το φορτίο του δικτύου σε περίπτωση βλάβης.

Για παράδειγμα, σε πολλούς εξυπηρετητές δικτύου χρησιμοποιούμε συστήματα mirror (καθρέπτη) στους σκληρούς δίσκους: τα δεδομένα μας αποθηκεύονται ταυτόχρονα σε περισσότερους από ένα δίσκους και το σύστημα μπορεί να συνεχίσει να λειτουργεί κανονικά ακόμα και μετά από απώλεια ενός ή περισσότερων δίσκων. Στην περίπτωση αυτή βέβαια ειδοποιείται ο διαχειριστής για να αντικαταστήσει το χαλασμένο δίσκο το συντομότερο δυνατόν.

7.2.3 Διαχείριση Επιδόσεων

Η *Διαχείριση Επιδόσεων* (Performance Management ή Capacity Management) διασφαλίζει ότι η απόδοση του δικτύου βρίσκεται σε αποδεκτά επίπεδα, αυτά δηλαδή για τα οποία σχεδιάστηκε.

Για το σκοπό αυτό, η διαχείριση επιδόσεων αξιολογεί κάποια μετρήσιμα χαρακτηριστικά απόδοσης όπως το χρόνο απόκρισης του δικτύου, την απώλεια πακέτων, τη χρήση των γραμμών επικοινωνίας, το βαθμό λαθών που συμβαίνουν κλπ. Οι πληροφορίες αυτές συλλέγονται σε ένα σύστημα διαχείρισης δικτύου (χρησιμοποιώντας πρωτόκολλα όπως το SNMP) με τους παρακάτω τρόπους:

- **Με συνεχή παρακολούθηση** και εκτίμηση της τρέχουσας κατάστασης από το διαχειριστή

- **Με ορισμό συναγερμών** στο σύστημα διαχείρισης δικτύου, το οποίο και θα μας ειδοποιήσει όταν τα επίπεδα απόδοσης μεταβληθούν σε σχέση με τα προκαθορισμένα και αποδεκτά

Με σωστά σχεδιασμένη στρατηγική συλλογής και ανάλυσης δεδομένων απόδοσης, ο διαχειριστής μπορεί:

- Να πιστοποιήσει την αποτελεσματικότητα και αξιοπιστία του δικτύου
- Να προβλέψει τα προβλήματα πριν εμφανιστούν
- Να επανασχεδιάσει το δίκτυο για ακόμα καλύτερες επιδόσεις
- Να προετοιμάσει το δίκτυο για μελλοντικές βελτιώσεις / επεκτάσεις

Για να εκτιμήσει καλύτερα την κατάσταση, ο διαχειριστής επιλέγει κάποιες παραμέτρους (πόρους) του δικτύου τους οποίους παρακολουθεί στενά.

7.2.4 Διαχείριση Κόστους

Η *Διαχείριση Κόστους* (Accounting Management ή Billing Management) ασχολείται με την παρακολούθηση πληροφοριών κόστους που σχετίζονται με τη χρήση των πόρων ενός δικτύου.

Βέβαια δεν παρέχουν όλα τα δίκτυα υπηρεσίες επί πληρωμή. Για παράδειγμα η τυπική χρήση ενός εταιρικού δικτύου δεν προκαλεί αύξηση του κόστους εκτός αν χρησιμοποιούνται υλικά που αναλώνονται (π.χ. εκτύπωση σε ένα δικτυακό εκτυπωτή) ή συνδέσεις δικτύου με ογκοχρέωση (π.χ. μισθωμένες γραμμές, δορυφορικές συνδέσεις). Στην περίπτωση αυτή προφανώς παρακολουθούνται μόνο οι συγκεκριμένες υπηρεσίες. Σε δίκτυα που δεν έχουν στόχο το κέρδος η έννοια αυτή αντικαθίσταται από την έννοια της Διοίκησης (Administration).

Ανάλογα με την περίπτωση, ο σκοπός της διαχείρισης κόστους είναι:

Για επιχειρήσεις με στόχο το κέρδος:

- **Ο υπολογισμός του σωστού ποσού χρέωσης** που προκύπτει από τις επί πληρωμή υπηρεσίες στους αντίστοιχους χρήστες (ή ομάδες χρηστών, ή οργανισμούς)

Για επιχειρήσεις χωρίς στόχο το κέρδος:

- **Δημιουργία κοστολόγησης (ή σωστότερα: καταγραφής) της χρήσης των πόρων** του δικτύου ανά χρήστη ή ανά τμήμα για να προσδιοριστούν καλύτερα λειτουργίες όπως η λήψη αντιγράφων ασφαλείας ή ο συγχρονισμός των δεδομένων

Η διαχείριση κόστους επίσης καλείται να αναγνωρίσει και να εντοπίσει χρήστες ή ομάδες χρηστών του δικτύου που:

- **Παραβιάζουν τα δικαιώματα πρόσβασης** και επιβαρύνουν το δίκτυο με άσκοπες λειτουργίες
- **Κάνουν μη αποτελεσματική χρήση του δικτύου**

Ο διαχειριστής είναι υπεύθυνος να αποφασίσει και να ορίσει τις παραμέτρους που θα παρακολουθούνται και θα καταγράφονται, τα χρονικά διαστήματα της καταγραφής καθώς και τον τρόπο υπολογισμού (αλγόριθμο) του κόστους. Αν δεν απαιτείται χρέωση, η συλλογή των δεδομένων θα χρησιμοποιηθεί για βελτιστοποίηση της απόδοσης.

7.2.5 Διαχείριση Ασφάλειας

Η *Διαχείριση Ασφαλείας* σε ένα δίκτυο αναφέρεται στη διαχείριση πληροφοριών που σχετίζονται με την ομαλή λειτουργία του δικτύου, την παρακολούθηση και έλεγχο πρόσβασης σε τμήματα του ή όλο το δίκτυο και στην ασφάλεια των δεδομένων που διακινούνται και αποθηκεύονται σε αυτό.

Για να ολοκληρωθεί το έργο της διαχείρισης ασφάλειας, πρέπει σε τακτά διαστήματα να συλλέγονται και να αναλύονται οι πληροφορίες που σχετίζονται με τους παραπάνω τομείς. Για το σκοπό αυτό χρησιμοποιούνται εργαλεία λογισμικού όπως:

- Πλατφόρμες συλλογής και ελέγχου δικτυακών δεδομένων (NMS Platforms)
- Εργαλεία κρυπτογράφησης (cryptography tools)
- Εργαλεία αυθεντικοποίησης (authentication tools) για τον έλεγχο πρόσβασης
- Συστήματα ελέγχου εισβολέων (intrusion detection systems)
- Τείχος προστασίας (firewall)
- Εφαρμογή πολιτικών ασφαλείας (security policies)
- Ημερολόγιο (αρχεία) καταγραφής (security logs) κ.α.

Καθένα από τα παραπάνω εργαλεία έχει διαφορετική εφαρμογή και στοχεύει να καλύψει επιμέρους ανάγκες ασφαλείας ενός δικτύου. Ένας διαχειριστής θα χρησιμοποιήσει περισσότερα από ένα εργαλεία για να εξασφαλίσει την ασφάλεια του δικτύου. Για το λόγο αυτό η διαχείριση ασφαλείας είναι μια αρκετά πολύπλοκη διαδικασία.

Για να είναι αποτελεσματική η διαχείριση ασφαλείας, θα πρέπει να προβλεφθούν οι πιθανές απειλές και τα σημεία κινδύνου ώστε να επιλεγούν τα σημεία που χρειάζονται μεγαλύτερη προσοχή και προστασία. Αφού γίνει αυτή η αναγνώριση, εγκαθίσταται και ρυθμίζεται το κατάλληλο λογισμικό. Μέσα από αυτό ο διαχειριστής παρακολουθεί και εντοπίζει πηγές κινδύνου και επιθέσεις στο δίκτυο στο συντομότερο χρονικό διάστημα.

7.3 Πρότυπα Διαχείρισης

Τα *βασικά συστατικά ή οντότητες* από τις οποίες αποτελείται ένα τυπικό Σύστημα Διαχείρισης Δικτύου είναι:

- **Ο Διαχειριστής Δικτύου** (Manager Server)
- **Ο Αντιπρόσωπος** (Agent)
- **Η Βάση Πληροφοριών Διαχείρισης** (Management Information Base, MIB)

Σημείωση: Επειδή από τα παραπάνω, ίσως δεν είναι προφανές, θα πρέπει να ξεκαθαρίσουμε:

Ο Διαχειριστής και ο Αντιπρόσωπος είναι προγράμματα που εκτελούνται σε μηχανήματα του δικτύου.

Συγκεκριμένα, ο διαχειριστής (πρόγραμμα) χρησιμοποιείται από τον διαχειριστή (άνθρωπο) προκειμένου να λάβει πληροφορίες για την κατάσταση του δικτύου. Ο διαχειριστής (πρόγραμμα) εκτελείται σε ένα υπολογιστή που είναι επιφορτισμένος με τη διαχείριση του δικτύου και συχνά ονομάζεται Manager Server.

Ο διαχειριστής (πρόγραμμα) συλλέγει δεδομένα επικοινωνώντας με τους αντιπροσώπους, που είναι αντίστοιχα προγράμματα που εκτελούνται σε κάθε τμήμα / συσκευή του δικτύου που διαθέτει δυνατότητα διαχείρισης. Προφανώς δεν είναι όλες οι συσκευές ή τα τμήματα του δικτύου κατάλληλα για την εκτέλεση προγραμμάτων αντιπροσώπου και άρα δεν είναι πάντα διαχειρίσιμα με κεντρικό τρόπο. Δεν μπορούμε να έχουμε αντιπρόσωπο να εκτελείται σε ένα…καλώδιο δικτύου. Επίσης φτηνές δικτυακές συσκευές δεν διαθέτουν συνήθως δυνατότητα διαχείρισης. Για παρά-

δειγμα ένας φτηνός μεταγωγέας δικτύου (switch) όπως αυτός που έχετε πιθανόν στο σχολικό εργαστήριο δεν είναι διαχειριζόμενος. Για να διαθέτει μια συσκευή τέτοια δυνατότητα χρειάζεται να έχει επεξεργαστή, μνήμη και το κατάλληλο πρόγραμμα από τον κατασκευαστή της (firmware). Το πρόγραμμα αυτό δρα ως αντιπρόσωπος (agent) και επιτρέπει την ανταλλαγή πληροφοριών με το διαχειριστή (πρόγραμμα) μέσω πρωτοκόλλων διαχείρισης (π.χ. SNMP). Όταν φτιάχνουμε ένα δίκτυο μεσαίου ή μεγάλου μεγέθους προσπαθούμε να χρησιμοποιούμε δικτυακές συσκευές με δυνατότητα διαχείρισης όπου είναι δυνατόν. Μερικές φορές ωστόσο το κόστος μπορεί να είναι απαγορευτικό.

Τα πιο γνωστά *Πρότυπα Διαχείρισης Δικτύου (Network Management, NM)* είναι:

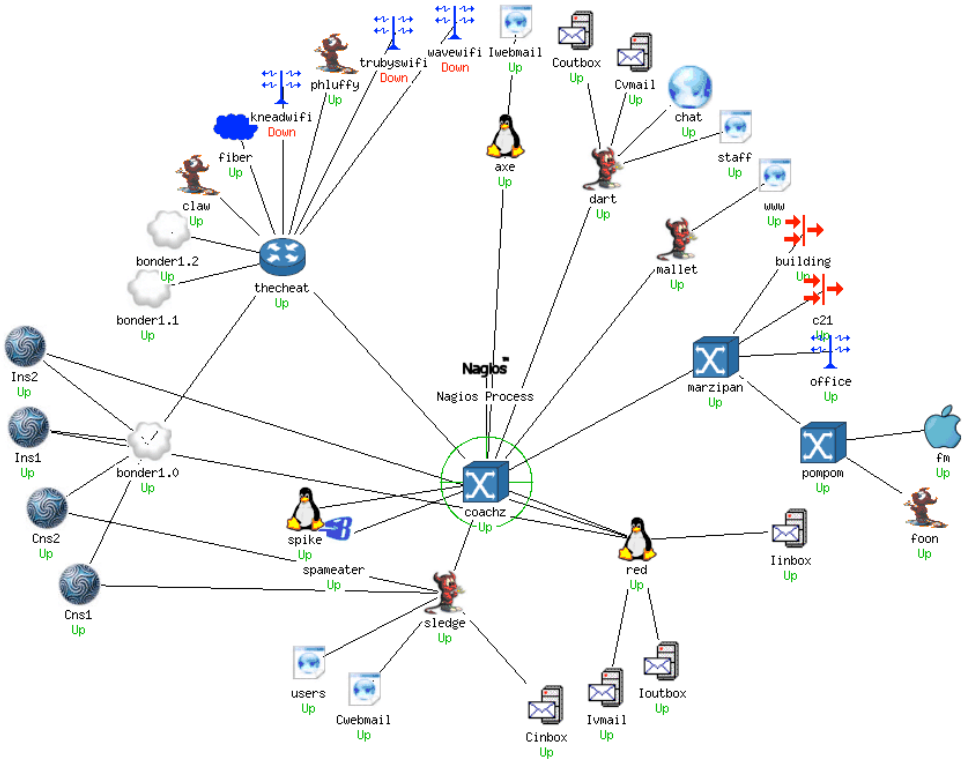
- Το **SNMP, Simple Network Management Protocol** του Διαδικτύου
- Το **CMIP, Common Management Information Protocol** του OSI

7.3.1 Βασικά Συστατικά Συστήματος Διαχείρισης (MS – MIB – AGENT)

Ο *Διαχειριστής Δικτύου (Manager Server)* είναι ένας ή περισσότεροι υπολογιστές που διαχειρίζεται τα στοιχεία του δικτύου που έχουν επιλεγεί για αυτό το σκοπό. Ο Manager Server εκτελεί κατάλληλο λογισμικό διαχειριστή το οποίο συχνά εμφανίζει στο διαχειριστή (άνθρωπο) το δίκτυο σε μορφή χάρτη (σχήμα 7.3) επιτρέποντας του να δει με μια ματιά την κατάσταση όλων των διαχειριζόμενων συσκευών.

Το λογισμικό πραγματοποιεί τις παρακάτω λειτουργίες:

- Αποστέλλει αιτήματα στους αντιπροσώπους που είναι εγκατεστημένοι στο δίκτυο
- Λαμβάνει απαντήσεις από τους αντιπροσώπους
- Ορίζει μεταβλητές παρακολούθησης στους αντιπροσώπους. Ουσιαστικά καθορίζει ποια είναι τα μεγέθη που θα μετρώνται. Για παράδειγμα, ο διαχειριστής μπορεί να ορίσει να μετρώνται τα πλαίσια ανα δευτερόλεπτο που διακινούνται σε μια θύρα Ethernet ενός switch. Για το σκοπό αυτό θα στείλει αντίστοιχη οδηγία στον αντιπρόσωπο που εκτελείται στο switch αυτό
- Παρακολουθεί τους συναγερμούς. Ειδοποιεί τον διαχειριστή (άνθρωπο) όταν οι παράμετροι λειτουργίας του δικτύου είναι εκτός των αποδεκτών ορίων



Σχήμα 7.3: *Δικτυακός Χάρτης*

(μπορεί να στείλει ειδοποιήσεις μέσω email, sms κλπ)

- Προσφέρει κατάλληλο περιβάλλον χρήστη (π.χ. δικτυακό χάρτη) για την καλύτερη παρακολούθηση των πληροφοριών του δικτύου από τον άνθρωπο

Ο *Αντιπρόσωπος Δικτύου* είναι το λογισμικό που εκτελείται σε κάθε δικτυακή συσκευή που είναι υπό διαχείριση.

Όπως αναφέραμε και πριν, δεν είναι όλες οι συσκευές δικτύου κατάλληλες για την εκτέλεση λογισμικού αντιπροσώπου. Οι φτηνές συσκευές συνήθως δεν έχουν δυνατότητες διαχείρισης και προσπαθούμε να τις αποφεύγουμε σε δίκτυα μεσαίου / μεγάλου μεγέθους.

Βασικές λειτουργίες του αντιπροσώπου είναι:

- Η συλλογή πληροφοριών από τα διαχειριζόμενα αντικείμενα του δικτύου
- Η διαμόρφωση παραμέτρων των διαχειριζόμενων αντικειμένων. Σε αρκετές

διαχειριζόμενες συσκευές είναι δυνατή η αλλαγή ρυθμίσεων με την αποστολή κατάλληλων εντολών από το Manager Server

- Η απάντηση στα αιτήματα των προγραμμάτων διαχείρισης δικτύου
- Η δημιουργία και αποστολή συναγερμών στους διαχειριστές

Η *Βάση Πληροφοριών Διαχείρισης ή MIB, Management Information Base* είναι ένα σχήμα αποθήκευσης πληροφοριών σε μορφή βάσης δεδομένων που χρησιμοποιείται για τη διαχείριση των αντικειμένων / οντοτήτων ενός δικτύου. Αντικείμενο θεωρείται εδώ κάθε συσκευή που είναι συνδεδεμένη στο δίκτυο (υπολογιστές, εκτυπωτές, δικτυακές συσκευές, δρομολογητές κλπ).

Η δομή της παραπάνω βάσης είναι ιεραρχική και μοιάζει με αντεστραμμένο δέντρο. Κάθε φύλλο είναι ένα διαχειριζόμενο αντικείμενο και αντιστοιχεί σε ένα πόρο του συστήματος. Η εισαγωγή πληροφοριών γίνεται μέσω μιας ακολουθίας αριθμών που προσδιορίζει με μοναδικό τρόπο ένα αντικείμενο (Ταυτοποίηση Αντικειμένου ή Object Identifier).

Οι MIBs συνήθως χρησιμοποιούν δομές πινάκων με πολλές μεταβλητές (πεδία). Οι πίνακες μπορεί να έχουν από μηδέν εγγραφές και άνω και ένα σύστημα διαχείρισης έχει πρόσβαση σε αυτούς για να εκτελέσει τυπικές λειτουργίες βάσεων δεδομένων: εισαγωγή δεδομένων, ανάκτηση (αναζήτηση), ανάκτηση επόμενης / προηγούμενης εγγραφής, ενημέρωση, διαγραφή κλπ.

Κεφάλαιο 8

Ασφάλεια Δικτύων

8.1 Βασικές Έννοιες Ασφάλειας Δεδομένων

Για να κατανοήσουμε την έννοια της ασφάλειας, θα πρέπει:

- Να σκεφτούμε τι σημαίνει για τον καθένα μας. Η ασφάλεια αντιμετωπίζεται διαφορετικά από ιδιώτες και από εταιρίες
- Να βρούμε ποιοι είναι αυτοί που προσπαθούν να την παραβιάσουν
- Να ανακαλύψουμε τις προθέσεις των εισβολέων και το πιθανό όφελος τους από μια επιτυχή παραβίαση

Όταν σκεφτόμαστε την ασφάλεια σε προσωπικό επίπεδο και σε σχέση με την τεχνολογία, το Διαδίκτυο και τους υπολογιστές, συνήθως σκεφτόμαστε υποκλοπή δεδομένων όπως τον αριθμό της πιστωτικής μας κάρτας ή τους κωδικούς του e-banking με σκοπό προφανώς το οικονομικό όφελος. Άνθρωποι που έχουν δημόσιο προφίλ (ηθοποιοί, τραγουδιστές, πολιτικοί κλπ) ή που ασχολούνται με τα κοινά μπορεί να έχουν στις συσκευές τους ευαίσθητα δεδομένα που πρέπει να παραμείνουν μυστικά. Τυχόν διαρροή τέτοιων πληροφοριών μπορεί να είναι επιζήμια για το ίδιο το άτομο ή τον οργανισμό στον οποίο εργάζεται. Ο μέσος άνθρωπος πάντως σε γενικές γραμμές είναι αδιάφορος για την ασφάλεια πέρα από τις πληροφορίες που μεταφέρει και αποθηκεύει σε υπολογιστικά συστήματα και που έχουν να κάνουν με ηλεκτρονικές συναλλαγές (η υποκλοπή των οποίων μπορεί να προκαλέσει απώλεια χρημάτων).

Μπορούμε να θεωρήσουμε ότι ασφάλεια γενικότερα είναι η προσπάθεια προστασίας από εξωτερικές επιβουλές (κακόβουλες ενέργειες) στις πληροφορίες και τα

συστήματα κατά τη λειτουργία τους ή κατά την επικοινωνία τους με άλλα συστήματα.

Κάθε πράγμα που θέλουμε να προστατεύσουμε αποτελεί για μας ένα *αγαθό* η απώλεια του οποίου μπορεί να μας προκαλέσει οικονομική ή άλλη ζημιά.

Αγαθό ή πόρος ενός υπολογιστικού / πληροφοριακούς συστήματος είναι κάθε αντικείμενο που ανήκει ή στηρίζει το σύστημα και το οποίο αξίζει να προστατευθεί.

Σε μια εταιρία, τα παραπάνω αγαθά μπορεί να ανήκουν τόσο στο υλικό όσο και στο λογισμικό του συστήματος και προφανώς περιέχουν επίσης τα δεδομένα (τα οποία πολλές φορές είναι αναντικατάστατα σε σχέση με όλα τα άλλα τμήματα):

Αγαθά είναι:

- Κτήρια, υπολογιστές, δικτυακός εξοπλισμός και υποδομή
- Έπιπλα, γραφεία κλπ.
- Αρχεία (ηλεκτρονικά και έντυπα), πληροφορίες σε συστήματα βάσεων δεδομένων κλπ.
- Λογισμικό εφαρμογών, λειτουργικά συστήματα κλπ.

Για να είναι αποτελεσματική η προστασία μας στις επιθέσεις, θα πρέπει αρχικά να κατανοούμε ποιοι αποτελούν την απειλή, ποια δικά μας δεδομένα τους είναι χρήσιμα και πως μπορούν να τα χρησιμοποιήσουν εναντίον μας. Για παράδειγμα ένα πολύ σημαντικό όπλο στην ασφάλεια δεδομένων αποτελεί η διαδικασία της κρυπτογράφησης. Η πρώτη ισχυρή κρυπτογράφηση έγινε από τους Γερμανούς κατά το δεύτερο παγκόσμιο πόλεμο: έπρεπε να μεταδίδουν μηνύματα προς τα υποβρύχια τους μέσω ασυρμάτου χωρίς να μπορεί να γίνει υποκλοπή από τους συμμάχους. Για το σκοπό αυτό έφτιαξαν τη μηχανή Enigma. Ωστόσο στην Αγγλία, οι σύμμαχοι ανακάλυψαν αδυναμίες τόσο στη μηχανή όσο και στη διαδικασία μετάδοσης μηνυμάτων και κατάφερναν να αποκωδικοποιούν τα μηνύματα σε καθημερινή βάση.

Από τα παραπάνω είναι προφανές ότι οι κυβερνήσεις είναι αυτές που διαθέτουν τον καλύτερο εξοπλισμό τόσο για να προστατεύσουν τα δεδομένα τους όσο και για να προβούν σε παραβιάσεις ασφαλείας εναντίον άλλων κρατών.

Μια εταιρεία ή οργανισμός με πολλούς εργαζόμενους και πελάτες συνήθως απευθύνεται σε συμβούλους ασφαλείας. Σε πολλές περιπτώσεις επιλέγεται μια λύση μεγάλου κόστους που προσπαθεί να δημιουργήσει τη μεγαλύτερη δυνατή ασφάλεια. Η πραγματικότητα όμως είναι ότι *δεν μπορεί ποτέ να υπάρξει απόλυτη ασφάλεια*, εκτός αν δεν έχουμε ευαίσθητα δεδομένα και δεν υπάρχουν μυστικά που πρέπει να μεταδοθούν. Σε ένα υπολογιστικό σύστημα η ασφάλεια είναι πάντα τόσο καλή όσο

είναι ο πιο αδύναμος κρίκος του, και αυτός αποδεικνύεται συχνά ότι είναι ο άνθρωπος.

Επίσης η μεγαλύτερη ασφάλεια κάνει συνήθως ένα σύστημα πιο δύσχρηστο: οι χρήστες καλούνται συνέχεια να εισάγουν κωδικούς και οι κινήσεις τους ελέγχονται τόσο συχνά που το σύστημα μπορεί να είναι δυσκίνητο. Αν και αρχικός σκοπός είναι η αύξηση της ασφάλειας, ένα δύσχρηστο σύστημα στην πραγματικότητα μειώνει την ασφάλεια: σύντομα οι χρήστες θα ψάξουν να βρουν τρόπους για να παρακάμψουν ή να συντομεύσουν τις διαδικασίες αντικαθιστώντας τις με άλλες, ανασφαλείς.

Τελικά η ασφάλεια βασίζεται πάντα σε μια ανάλυση αντιστάθμισης του κόστους και των ωφελημάτων που μπορούν να επιτευχθούν. Είναι ένας συμβιβασμός που στη μια μεριά έχει το κόστος της απώλειας ή διαρροής των δεδομένων και στην άλλη το κόστος προφύλαξης τους από διαφορετικές απειλές. Σε αντίθεση με τους ειδικούς ασφαλείας που προτείνουν λύσεις με το μέγιστο κόστος, η πραγματική ασφάλεια συνήθως αναγνωρίζει τις συνηθισμένες απειλές και προσπαθεί να λάβει τα απαραίτητα μέτρα για αυτές, ενώ μπορεί να αγνοεί απειλές που είναι σπάνιες ή απίθανες.

Για παράδειγμα, μια συνηθισμένη επίθεση σε μια τράπεζα μπορεί να έχεις ως αποτέλεσμα την υποκλοπή στοιχείων πελατών όπως τραπεζικοί λογαριασμοί και πιστωτικές κάρτες. Το σύστημα ασφαλείας της τράπεζας θα πρέπει να είναι προετοιμασμένο για τέτοιες επιθέσεις. Μέχρι τι επίπεδο όμως; Τι απώλεια έχει η τράπεζα από τη διαρροή μιας πιστωτικής κάρτας; Εκτός από την προφανή άμεση οικονομική ζημιά, υπάρχει και η έμμεση: οι πελάτες δεν έχουν πλέον εμπιστοσύνη στη τράπεζα. Απώλεια πελατών σημαίνει επίσης μελλοντική οικονομική απώλεια.

Γενικά είναι πιο εύκολο να υπολογίσουμε μια άμεση ζημιά (π.χ. από την καταστροφή ενός υλικού) από την έμμεση (απώλεια εμπιστοσύνης). Ένα άλλο κόστος μπορεί να είναι οι νομικές συνέπειες που προκύπτουν ως αποτέλεσμα της παραβίασης ασφάλειας. Τέλος, αν μια εταιρεία βασίζεται στην αδιάλειπτη παροχή υπηρεσιών μέσω Διαδικτύου και δεχθεί επίθεση άρνησης υπηρεσίας (DOS attack) η απώλεια χρημάτων (πέρα από τις νομικές συνέπειες) μπορεί να είναι ανυπολόγιστη. Σκεφτείτε για παράδειγμα μια εταιρεία όπως το Amazon: αν το site του Amazon σταματήσει ξαφνικά να είναι προσβάσιμο, θα χάνονται αρκετά εκατομμύρια πωλήσεων κάθε λεπτό.

8.2 Εμπιστευτικότητα – Ακεραιότητα – Διαθεσιμότητα – Αυθεντικότητα – Εγκυρότητα

Τα βασικά προβλήματα που πρέπει να επιλύσει κάποιος κατά την ανάλυση και το σχεδιασμό του επιπέδου ασφαλείας που θέλει να πετύχει είναι τέσσερα:

- **Εμπιστευτικότητα (confidentaliaty):** Αποτροπή της πρόσβασης σε ιδιωτικές πληροφορίες από άτομα που δεν έχουν εξουσιοδότηση.

  Για παράδειγμα, όταν κάνουμε μια ηλεκτρονική παραγγελία μέσω Διαδικτύου θέλουμε να εξασφαλίσουμε ότι ο αριθμός της πιστωτικής μας κάρτας δεν θα είναι ορατός παρά μόνο από το σύστημα που θα τελέσει τη συναλλαγή.

- **Αυθεντικοποίηση (authentication) ή πιστοποίηση ταυτότητας:** Η εξασφάλιση ότι η πληροφορία προέρχεται πραγματικότητα από αυτόν που νομίζουμε (ή που ισχυρίζεται) ότι τη μετέδωσε.

  Για παράδειγμα, να μπορούμε να διασφαλίσουμε ότι το άτομο που έστειλε τον αριθμό της πιστωτικής κάρτας είναι πράγματι ο κάτοχος της. Ή όταν κάποιος εισέρχεται σε ένα υπολογιστικό σύστημα ότι πράγματι είναι το πρόσωπο στο οποίο ανήκει ο αντίστοιχος λογαριασμός χρήστη.

- **Ακεραιότητα (integrity):** είναι η διασφάλιση ότι οι πληροφορίες δεν έχουν αλλοιωθεί και όλες οι αλλαγές που έχουν γίνει σε αυτές προέρχονται από εξουσιοδοτημένα άτομα.

  Για παράδειγμα, αν κάποιος τρίτος μπορούσε να υποκλέψει τη συναλλαγή πληρωμής μιας ηλεκτρονικής αγοράς, θα μπορούσε να κατευθύνει το χρηματικό ποσό στο δικό του λογαριασμό. Μια τέτοια αλλοίωση σημαίνει απώλεια ακεραιότητας των δεδομένων.

  Όταν αναφερόμαστε σε πληροφορίες, *εξουσιοδοτημένα άτομα* είναι προφανώς ο αρχικός δημιουργός της πληροφορίας και τα άτομα στα οποία αυτός έχει δώσει τα αντίστοιχα δικαιώματα πρόσβασης (μερικούς ή πλήρης).

- **Μη Άρνηση Ταυτότητας (non-repudiation):** Η μη-αποποίηση των ευθυνών εκ των υστέρων χρηστών που συμμετείχαν σε μια ηλεκτρονική επικοινωνία.

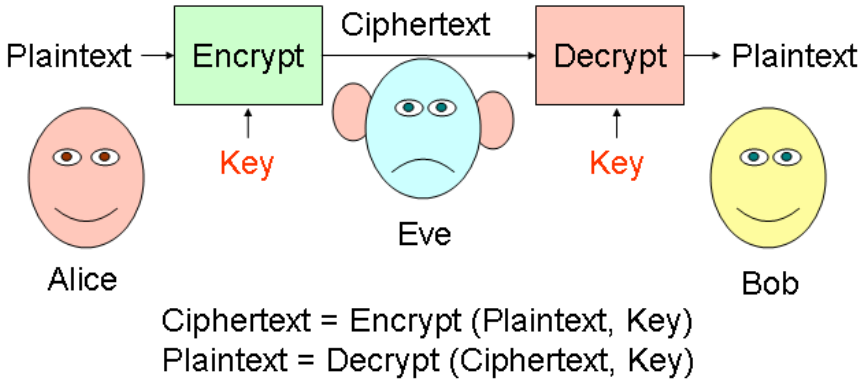
  Ουσιαστικά αυτό σημαίνει ότι μπορούμε να επιρρίψουμε με σιγουριά ευθύνες σε χρήστες για κινήσεις ή παραλήψεις που έκαναν κατά τη διάρκεια μιας επικοινωνίας αφού μπορούμε να είμαστε σίγουροι για τους συμμετέχοντες και το ρόλο του καθενός. Είναι σημαντικό οι συμμετέχοντες σε μια επικοινωνία που χειρίζεται εμπιστευτικές πληροφορίες, να μη μπορούν να αρνηθούν την εμπλοκή τους.

Ο συνδυασμός της Αυθεντικότητας (πιστοποίηση ταυτότητας) και της Ακεραιότητας (μη αλλοίωσης) των δεδομένων είναι γνωστός ως *Εγκυρότητα (validity)* των πληροφοριών.

Σε περιπτώσεις που είναι απαραίτητη η αδιάλειπτη παροχής πρόσβασης σε πληροφορίες από εξουσιοδοτημένους χρήστες, ορίζεται και η έννοια της *διαθεσιμότητας* των πληροφοριών. Για παράδειγμα αν μια εταιρεία που διαθέτει λογαριασμούς ηλεκτρονικού ταχυδρομείου δεν μπορεί να εξυπηρετήσει τους εξουσιοδοτημένους χρήστες της λόγω επίθεσης στο δίκτυο της, αυτό αποτελεί απώλεια διαθεσιμότητας.

Ασφάλεια των πληροφοριών είναι η επίτευξη του σχεδιαζόμενου επιπέδου διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των πληροφοριών.

Για την εξασφάλιση της εμπιστευτικότητας των πληροφοριών, η πιο συχνά χρησιμοποιούμενη τεχνική είναι η κρυπτογράφηση: Σκοπός της κρυπτογράφησης είναι η μετατροπή ενός αρχικού μηνύματος με τρόπο τέτοιο ώστε να μη μπορεί να διαβαστεί από οποιονδήποτε εκτός από τον τελικό παραλήπτη. Προφανώς ο παραλήπτης θα χρησιμοποιήσει την αντίστροφη τεχνική (αποκρυπτογράφηση) για να αποκαλύψει την αρχική πληροφορία. Όσο αφορά την ασφάλεια σε μια μετάδοση δεδομένων, θεωρούμε ότι πάντα υπάρχει κάποιος που προσπαθεί να υποκλέψει τις πληροφορίες που μεταδίδουμε και ότι έχει πιθανότητες να το πετύχει.

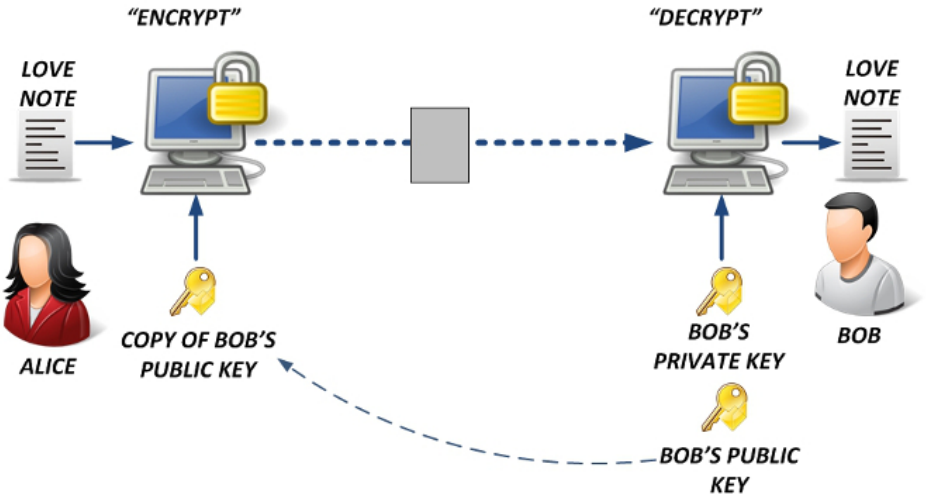


Σχήμα 8.1: *Κρυπτογραφημένη Επικοινωνία*

- **Κρυπτογράφηση** είναι η εφαρμογή μιας τεχνικής, συνήθως ένος μαθηματικού αλγόριθμου, μετατροπής της πληροφορίας από μορφή απλού κειμένου σε μορφή μη-αναγνωρίσιμη ώστε να μην είναι προσβάσιμη κατά τη μεταφορά

της από μη εξουσιοδοτημένα άτομα

- **Αποκρυπτογράφηση:** είναι μια τεχνική αντίστροφη της κρυπτογράφησης που εφαρμόζεται μόνο από εξουσιοδοτημένα άτομα σε κρυπτογραφημένη πληροφορία ώστε να επανέλθει στην αρχική μορφή απλού κειμένου
- **Κρυπτογράφημα (ή κρυπτόγραμμα, ciphertext)** είναι η μη-αναγνωρίσιμη μορφή που προκύπτει όταν υποστεί κρυπτογράφηση το αρχικό απλό κείμενο
- **Κλειδί (key)** είναι ένας κωδικός από ψηφιακά δεδομένα (μια σειρά από bytes ή ένα αρχείο π.χ.) το οποίο χρησιμοποιείται από τον αλγόριθμο κρυπτογράφησης / αποκρυπτογράφησης για την αντίστοιχη διαδικασία



Σχήμα 8.2: *Κρυπτογράφηση Δημόσιου Κλειδιού*

Υπάρχουν δυο βασικά είδη κρυπτογράφησης: στην *συμμετρική* κρυπτογράφηση χρησιμοποιείται το ίδιο κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση. Στην περίπτωση αυτή το κλειδί ονομάζεται και *μυστικό κλειδί (secret key)* καθώς όποιος το έχει μπορεί προφανώς να αποκρυπτογραφήσει το μήνυμα. Είναι σημαντικό σε αυτή την περίπτωση το κλειδί να μη διαρρεύσει και πρέπει επίσης να βρεθεί ασφαλής τρόπος για να δοθεί σε όλα τα ενδιαφερόμενα μέρη.

Αντίθετα στην *κρυπτογράφηση με δημόσιο κλειδί* (σχήμα 8.2) ή μη-συμμετρική κρυπτογράφηση, κάθε χρήστης διαθέτει δύο κλειδιά: ένα *δημόσιο κλειδί (public key)* και ένα *ιδιωτικό κλειδί (private key)*. Η ιδέα εδώ είναι ότι όλοι ανταλλάσσουν τα δημόσια κλειδιά τους ενώ κρατάνε τα ιδιωτικά ως μυστικά. Στη κρυπτογράφηση δημόσιου κλειδιού, ότι κλειδώνει με το δημόσιο κλειδί ξεκλειδώνει μόνο με το αντίστοιχο ιδιωτικό (τα κλειδιά δημιουργούνται ως ζεύγη). Έτσι αν ο χρήστης Α θέλει

να στείλει ένα ιδιωτικό μήνυμα στον Β, χρησιμοποιεί το δημόσιο κλειδί του Β για να το κρυπτογραφήσει. Το μήνυμα έπειτα μπορεί να αποκρυπτογραφηθεί μόνο από τον Β χρησιμοποιώντας το ιδιωτικό κλειδί του.

Παράρτημα Α΄

Μεθοδολογία Ασκήσεων Υποδικτύωσης

Α΄.1 Μεθοδολογία Ασκήσεων Υποδικτύωσης

Για να επιλύσουμε ασκήσεις υποδικτύωσης θα πρέπει:

- Να γνωρίζουμε μετατροπή από δυαδικό στο δεκαδικό και το ανάποδο (το βιβλίο και το βοήθημα περιγράφουν κάποιους εύκολους τρόπους).
- Να γνωρίζουμε τις δυνάμεις του δύο (όχι απαραίτητα απ'έξω βέβαια, αρκεί να γράψουμε το αντίστοιχο πινακάκι πριν ξεκινήσουμε).

Τα παραπάνω είναι απαραίτητα, καθώς για να δουλέψουμε με τις μάσκες στην υποδικτύωση θα πρέπει να έχουμε τις αντίστοιχες οκτάδες στο δυαδικό. Τα δεδομένα / ζητούμενα της άσκησης μπορεί να δίνονται / ζητούνται σε οποιοδήποτε από τα δύο συστήματα. Καλό θα είναι να εξασκηθείτε στις μετατροπές. Επίσης συνηθίστε να ελέγχετε το αποτέλεσμα μιας μετατροπής κάνοντας την αντίστροφα.

Χρήσιμο tip: Ένας αριθμός στο δυαδικό με το τελευταίο ψηφίο 0 είναι ζυγός, ενώ με 1 είναι μονός. Είναι η πιο γρήγορη αρχική επαλήθευση που μπορείτε να κάνετε.

Μάσκα Δικτύου και Διευθύνσεις Δικτύου / Εκπομπής

Η μάσκα δικτύου σε μια άσκηση μπορεί να δίνεται σε οποιαδήποτε από τις παρακάτω μορφές:

```
Δεκαδική: 255.255.240.0
Δυαδικό: 11111111 11111111 11110000 00000000
CIDR (πρόθεμα): /20
```

Όταν θέλουμε να εργαστούμε με τη μάσκα για να βρούμε διευθύνσεις δικτύου, εκπομπής ή να κάνουμε υποδικτύωση, πάντα θα πρέπει να τη φέρουμε στη δυαδική της μορφή.

Παράδειγμα 1

Δίνεται η διεύθυνση IP 192.168.3.124 με μάσκα 255.255.255.0. Να υπολογιστεί η Διεύθυνση Δικτύου και η Διεύθυνση Εκπομπής.

Απάντηση

Θα πρέπει να γράψουμε τη μάσκα και τη διεύθυνση IP στις αντίστοιχες δυαδικές μορφές κάνοντας τη μετατροπή. Για τη μάσκα είναι εύκολο να θυμάστε φυσικά ότι το 255 (που συναντάται πολύ συχνά) είναι απλά οκτώ άσοι: 11111111. Φτιάχνουμε το παρακάτω πινακάκι:

IP (Δεκαδικό):	192.	168.	3.	124
IP (Δυαδικό):	1100 0000	1010 1000	0000 0011	0111 1100
Μάσκα (Δυαδικό):	1111 1111	1111 1111	1111 1111	0000 0000
Διεύθυνση Δικτύου:	1100 0000	1010 1000	0000 0011	0000 0000
Διεύθ. Δικτύου (Δεκαδικό):	192.	168.	3.	0

Βοηθάει αν γράφουμε τους δυαδικούς χωρισμένους σε τετράδες ψηφίων ώστε να μη μπερδευόμαστε στο μέτρημα. Δεν είναι ωστόσο απαραίτητο.

Η διεύθυνση δικτύου προκύπτει από το λογικό “ΚΑΙ” της μάσκας και της διεύθυνσης IP.

Χρήσιμο tip: Όπου η μάσκα είναι 255 (ή 11111111), προκύπτει ακριβώς ο ίδιος αριθμός που αναγράφεται στην αντίστοιχη οκτάδα της διεύθυνσης IP. Όπου η μάσκα είναι μηδέν (ή 00000000) προκύπτει μηδέν στην αντίστοιχη οκτάδα. **Προσέξτε στις μάσκες δικτύου που έχουν άλλους αριθμούς: θα πρέπει να το κάνετε ανά ψηφίο.**

Για να υπολογίσουμε τη διεύθυνση εκπομπής, θα πρέπει να πάρουμε τη **διεύθυνση δικτύου που βρήκαμε πριν** και να βάλουμε 1 (ένα) σε όλα τα bit που ανήκουν στο τμήμα του υπολογιστή. Οπότε είναι σκόπιμο να γράψετε σε ένα πίνακα τη διεύθυνση δικτύου και τη μάσκα ξανά:

Διεύθυνση Δικτύου:	1100 0000	1010 1000	0000 0011	0000 0000
Μάσκα (Δυαδικό):	1111 1111	1111 1111	1111 1111	0000 0000
Διεύθυνση Εκπομπής:	1100 0000	1010 1000	0000 0011	1111 1111
Διεύθ. Εκπομπής (Δεκαδικό):	192.	168.	3.	255

Κάνουμε “1” όλα τα bit στη διεύθυνση δικτύου στα οποία τα αντίστοιχα ψηφία της μάσκας είναι μηδέν. Έπειτα μετατρέπουμε ξανά στο δεκαδικό και παίρνουμε τη διεύθυνση εκπομπής 192.168.3.255. Προσοχή, για να βρούμε τη διεύθυνση εκπομπής πρέπει να ξεκινήσουμε από τη **διεύθυνση δικτύου** και όχι την IP!

Όπως καταλαβαίνετε, η εύρεση της διεύθυνσης εκπομπής είναι πολύ εύκολη αν έχουμε μάσκα με τιμές μόνο 255 και 0. Αν ωστόσο η μάσκα που έχουμε αντιστοιχεί σε υποδικτύωση (ή υπερδικτύωση) θα πρέπει να κάνετε το παραπάνω προσεκτικά. Δείτε το παρακάτω παράδειγμα.

Παράδειγμα 2

Δίνεται η διεύθυνση IP 192.168.5.73/27. Να βρείτε τη διεύθυνση δικτύου και τη διεύθυνση εκπομπής.

Απάντηση

Στο συγκεκριμένο παράδειγμα μας δίνεται η μάσκα σε μορφή CIDR. Οπότε ξέρουμε ότι απλά θα γράψουμε 27 άσους. Μια τέτοια μάσκα δεν αντιστοιχεί σε μια τυποποιημένη κλάση (A,B,C). Έχουμε δώσει τρία παραπάνω bit στο τμήμα δικτύου και έτσι το τμήμα υπολογιστή διαθέτει μόνο 5 bit. Πρόκειται δηλ. για υποδικτύωση. Κάνουμε ξανά τον αντίστοιχο πίνακα:

IP (Δεκαδικό):	192.	168.	5.	73
IP (Δυαδικό):	1100 0000	1010 1000	0000 0101	0100 1001
Μάσκα (Δυαδικό):	1111 1111	1111 1111	1111 1111	1110 0000
Διεύθυνση Δικτύου:	1100 0000	1010 1000	0000 0101	0100 0000
Διεύθ. Δικτύου (Δεκαδικό):	192.	168.	5.	64

Δώστε προσοχή στην τελευταία οκτάδα!

Αντίστοιχα, (και με την ίδια προσοχή!) θα πρέπει να υπολογίσουμε τη διεύθυνση εκπομπής. Ξεκινάμε από τη **διεύθυνση δικτύου** που βρήκαμε πριν και με τη μάσκα που έχουμε:

Διεύθυνση Δικτύου:	1100 0000	1010 1000	0000 0101	0100 0000
Μάσκα (Δυαδικό):	1111 1111	1111 1111	1111 1111	1110 0000
Διεύθυνση Εκπομπής:	1100 0000	1010 1000	0000 0101	0101 1111
Διεύθ. Εκπομπής (Δεκαδικό):	192.	168.	5.	95

Η διεύθυνση εκπομπής προκύπτει όταν κάνουμε “1” τα ψηφία στη διεύθυνση δικτύου στα οποία τα αντίστοιχα ψηφία της μάσκας είναι “0”. Δηλ. κάνουμε “1” τα ψηφία που ανήκουν στο τμήμα υπολογιστή. Και βλέπετε ότι σε αυτή τη περίπτωση η απάντηση δεν είναι προφανής (όπως όταν έχουμε μόνο 255 και 0 στη μάσκα).

Για να επαληθεύετε τα αποτελέσματα σας μπορείτε πάντα να επισκεφθείτε μια από τις πολλές σελίδες στο διαδίκτυο που υπολογίζουν τις αντίστοιχες διευθύνσεις. Π.χ. για διευθύνσεις δικτύου και εκπομπής, δείτε:

http://www.remotemonitoringsystems.ca/broadcast.php

Ασκήσεις προς επίλυση

1. Να βρείτε τη διεύθυνση δικτύου και εκπομπής σε ένα δίκτυο όπου μια διεύθυνση IP είναι 10.14.28.55 και η μάσκα είναι 255.240.0.0. (Τα αποτελέσματα να εκφραστούν και στο δεκαδικό σύστημα).

2. Να βρείτε τη διεύθυνση δικτύου και εκπομπής σε ένα δίκτυο με IP 192.168.3.94 /26. (Τα αποτελέσματα να εκφραστούν και στο δεκαδικό σύστημα).

3. Να βρείτε τη διεύθυνση δικτύου και εκπομπής σε ένα δίκτυο με IP 192.168.230.20 και μάσκα 255.255.248.0. (Τα αποτελέσματα να εκφραστούν και στο δεκαδικό σύστημα).

Υποδικτύωση

Στην υποδικτύωση, δίνουμε κάποια ψηφία από το τμήμα υπολογιστή στο τμήμα δικτύου. Έτσι για παράδειγμα, ενώ στην κλάση C έχουμε 24 bit στο τμήμα δικτύου και 8 στο τμήμα υπολογιστή, με την υποδικτύωση μπορούμε να μειώσουμε το τμήμα υπολογιστή και να αυξήσουμε το τμήμα δικτύου. Για παράδειγμα, αν δώσουμε 27 bit στο τμήμα δικτύου (με τη βοήθεια πάντα της μάσκας) θα μας μείνουν μόνο 5 bit στο τμήμα υπολογιστή.

Χωρίζουμε ένα δίκτυο κλάσης C συνήθως για διαχειριστικούς λόγους: Δεν θέλουμε ένα δίκτυο με 254 μηχανήματα αλλά μερικά δίκτυα με λιγότερα (ένα για το λογιστήριο, ένα για την αποθήκη, ένα για τη μισθοδοσία κλπ). Χωρίζουμε ένα δίκτυο κλάσης B σε μικρότερα γιατί σχεδόν καμιά εταιρεία δεν θα χρησιμοποιήσει σε μια εγκατάσταση 65534 υπολογιστές: χωρίζοντας το σε μερικά κομμάτια π.χ. των 8000 υπολογιστών, μπορούμε να τα διαθέσουμε σε πολλές εταιρείες και να αποφύγουμε τη σπατάλη διευθύνσεων.

Χρήσιμο tip: Όταν δίνουμε bits από το τμήμα υπολογιστή στο τμήμα δικτύου, έχουμε υποδικτύωση. Όταν δίνουμε bits από το τμήμα δικτύου στο τμήμα υπολογιστή έχουμε υπερδικτύωση.

Παραδείγματα Υποδικτύωσης

Παράδειγμα 1

Δίνεται η διεύθυνση δικτύου 192.168.12.0/24.

1. Να χωριστεί το δίκτυο σε 5 τουλάχιστον υποδίκτυα, να δοθούν οι διευθύνσεις δικτύου και εκπομπής για κάθε υποδίκτυο
2. Πόσους υπολογιστές έχει το κάθε υποδίκτυο;

Απάντηση

Είναι εμφανές ότι έχουμε ένα δίκτυο κλάσης C με μάσκα 255.255.255.0. Αν το χωρίσουμε σε 5 υποδίκτυα, το κάνουμε μάλλον για διαχειριστικούς λόγους.

Θα πρέπει να πάρουμε κάποια bit από το τμήμα υπολογιστή και να τα δώσουμε στο τμήμα δικτύου. Αλλά πόσα;

Αντί για ένα δίκτυο, θέλουμε πλέον 5. Με 2 bit επιπλέον μπορούμε να φτιάξουμε 2^2=4 δίκτυα ενώ με 3 bit, 2^3=8. Προφανώς τα δύο bit είναι λίγα, ενώ τα τρία περισσεύουν. Ωστόσο δεν έχουμε ενδιάμεση επιλογή και θα χρησιμοποιήσουμε τρία bit. Άλλωστε για αυτό το λόγο και η άσκηση λέει **τουλάχιστον** 5 υποδίκτυα, και όχι ακριβώς 5! Αν μας δώσουν πλήθος υποδικτύων που είναι δύναμη του 2, θα μπορέσουμε να το κάνουμε ακριβώς.

Στο σημείο αυτό είναι χρήσιμο να έχουμε το παρακάτω πινακάκι δυνάμεων του 2. Αν δεν είστε εξοικειωμένοι με τις δυνάμεις του 2 τουλάχιστον μέχρι το 2^8 καλό θα είναι να το γράψετε πριν ξεκινήσετε την άσκηση για να το έχετε ως αναφορά:

Ψηφία n	**Πλήθος 2^n**
1	2
2	4
3	8
4	16
5	32
6	64
7	128
8	256

Και από τον πίνακα είναι εμφανές ότι για 5 υποδίκτυα χρειαζόμαστε 3 bit. Αυτά τα τρία bit θα πάρουν τιμή “1” στη μάσκα του δικτύου που θα φτιάξουμε!

Για να ξεκινήσουμε πρέπει να γράψουμε τη διεύθυνση δικτύου στο δυαδικό:

Διεύθυνση Δικτύου:	192.	168.	12.	0
Δ. Δικτύου (Δυαδικό):	1100 0000	1010 1000	0000 1100	0000 0000
Μάσκα (Δυαδικό):	1111 1111	1111 1111	1111 1111	1110 0000
Μάσκα (Δεκαδικό):	255.	255.	255	224

Δώσαμε τρία επιπλέον ψηφία από το τμήμα υπολογιστή στο τμήμα δικτύου, έτσι η νέα μάσκα είναι 255.255.255.224.

Μπορούμε τώρα να γράψουμε τα οκτώ υποδίκτυα που προκύπτουν (θυμηθείτε ότι περισσεύουν…)

Α/Α	**1η οκτάδα**	**2η οκτάδα**	**3η οκτάδα**	**4η οκτάδα**		**Διευθύνσεις**
0	1100 0000	1010 1000	0000 1100	000	00000	192.168.12.0
					11111	192.168.12.31
1	1100 0000	1010 1000	0000 1100	001	00000	192.168.12.32
					11111	192.168.12.63
2	1100 0000	1010 1000	0000 1100	010	00000	192.168.12.64
					11111	192.168.12.95
3	1100 0000	1010 1000	0000 1100	011	00000	192.168.12.96
					11111	192.168.12.127
4	1100 0000	1010 1000	0000 1100	100	00000	192.168.12.128
					11111	192.168.12.159
5	1100 0000	1010 1000	0000 1100	101	00000	192.168.12.160
					11111	192.168.12.191
6	1100 0000	1010 1000	0000 1100	110	00000	192.168.12.192
					11111	192.168.12.223
7	1100 0000	1010 1000	0000 1100	111	00000	192.168.12.224
					11111	192.168.12.255

Πως τα γράψαμε; Θυμηθείτε στις τρεις πρώτες οκτάδες δεν υπάρχει καμιά αλλαγή: ανήκουν εξ'ολοκλήρου στο δίκτυο. Στη τέταρτη οκτάδα ωστόσο, τα τρία πρώτα bit δείχνουν το δίκτυο και τα άλλα πέντε τον υπολογιστή. Οπότε για κάθε ένα από τους 8 συνδυασμούς των τριών πρώτων ψηφίων τα άλλα πέντε μπορούν να πάρουν όλες τις τιμές από 00000 μέχρι 11111.

Σε όλα αυτά τα υποδίκτυα, η πρώτη διεύθυνση που βρίσκουμε είναι η διεύθυνση δικτύου και η τελευταία η διεύθυνση εκπομπής! Μπορείτε αν θέλετε να το επαληθεύσετε με τη βοήθεια της μάσκας υποδικτύου.

Έτσι μπορούμε να δώσουμε τον παρακάτω πίνακα απαντήσεων:

A/A	Διεύθυνση Δικτύου	Διεύθυνση Εκπομπής	IP Από – Εώς	Πλήθος Υπολογιστών
0	192.168.12.0	192.168.12.31	192.168.12.1 192.168.12.30	30
1	192.168.12.32	192.168.12.63	192.168.12.33 192.168.12.62	30
2	192.168.12.64	192.168.12.95	192.168.12.65 192.168.12.94	30
3	192.168.12.96	192.168.12.127	192.168.12.97 192.168.12.126	30
4	192.168.12.128	192.168.12.159	192.168.12.129 192.168.12.158	30
5	192.168.12.160	192.168.12.191	192.168.12.161 192.168.12.190	30
6	192.168.12.192	192.168.12.223	192.168.12.193 192.168.12.222	30
7	192.168.12.224	192.168.12.255	192.168.12.225 192.168.12.254	30

Παράδειγμα 2

Ενώ στο πρώτο παράδειγμα μας ζήτησαν συγκεκριμένο αριθμό δικτύων, σε άλλη περίπτωση μπορεί να μας ζητήσουν να φτιάξουμε υποδίκτυα με συγκεκριμένο αριθμό μηχανημάτων. Για παράδειγμα:

Δίνεται η διεύθυνση δικτύου 192.168.14.0 με μάσκα 255.255.255.0 (δηλ /24). Να χωριστεί σε υποδίκτυα ώστε το καθένα από αυτά να έχει τουλάχιστον 14 μηχανήματα.

Απάντηση

Σκεφτόμαστε με τον ίδιο τρόπο όπως προηγουμένως, μόνο που τώρα υπολογίζουμε πόσα bit χρειαζόμαστε για τα μηχανήματα. Τα υπόλοιπα bit θα τα διαθέσουμε στο τμήμα δικτύου.

Για 14 μηχανήματα, χρειαζόμαστε 4 ψηφία, γιατί 2^4=16. Τα 3 ψηφία δεν αρκούν (2^3=8). Παρατηρήστε ότι με 4 ψηφία θα έχουμε **ακριβώς 14 μηχανήματα, γιατί χάνουμε δύο διευθύνσεις ανά υποδίκτυο (δικτύου και εκπομπής).**

Εδώ λοιπόν θα κρατήσουμε τα 4 τελευταία ψηφία της 4ης οκτάδας για το τμήμα υπολογιστή και θα δώσουμε τα άλλα 4 στο τμήμα υπολογιστή.

Θα έχουμε λοιπόν συνολικά 16 υποδίκτυα, με 14 μηχανήματα στο καθένα. Θα υπολογίσουμε αρχικά τη μάσκα δικτύου:

Διεύθυνση Δικτύου:	192.	168.	14.	0
Δ. Δικτύου (Δυαδικό):	1100 0000	1010 1000	0000 1110	0000 0000
Μάσκα (Δυαδικό):	1111 1111	1111 1111	1111 1111	1111 0000
Μάσκα (Δεκαδικό):	255.	255.	255	240

Α/Α	**1η οκτάδα**	**2η οκτάδα**	**3η οκτάδα**	**4η οκτάδα**		**Διευθύνσεις**
0	1100 0000	1010 1000	0000 1110	0000	0000	192.168.14.0
					1111	192.168.14.15
1	1100 0000	1010 1000	0000 1110	0001	0000	192.168.14.16
					1111	192.168.14.31
2	1100 0000	1010 1000	0000 1110	0010	0000	192.168.14.32
					1111	192.168.14.47
3	1100 0000	1010 1000	0000 1110	0011	0000	192.168.14.48
					1111	192.168.14.63
4	1100 0000	1010 1000	0000 1110	0100	0000	192.168.14.64
					1111	192.168.14.79
5	1100 0000	1010 1000	0000 1110	0101	0000	192.168.14.80
					1111	192.168.14.95
6	1100 0000	1010 1000	0000 1110	0110	0000	192.168.14.96
					1111	192.168.12.111
7	1100 0000	1010 1000	0000 1110	0111	0000	192.168.14.112
					1111	192.168.14.127

Και ακόμα 8 υποδίκτυα που δεν δείχνουμε για οικονομία χώρου (και χαρτιού)!

Όπως καταλαβαίνετε, σε καθένα από αυτά τα υποδίκτυα η πρώτη διεύθυνση είναι η **διεύθυνση δικτύου και η τελευταία η διεύθυνση εκπομπής.** Το κάθε υποδίκτυο συνδέει ακριβώς 14 υπολογιστές. Συνολικά έχουμε 16 X 14 = 224 υπολογιστές αντί για 254.

Μπορείτε να δείτε πάντα σε ένα αντίστοιχο web calculator αν έχετε κάνει τους σωστούς υπολογισμούς:

http://jodies.de/ipcalc

Προσπαθήστε τώρα να λύσετε τη δραστηριότητα 3η του βιβλίου (σελ. 81) χωρίς τη βοήθεια του site :D

Παράρτημα Β΄

Ορόσημα (Milestones)

Β΄.1 Ορόσημα στη Συγγραφή του Βοηθήματος

Ημερομηνία	Περιγραφή
12/09/2016	Δημιουργία του GitHuB Repository
02/10/2016	Δημιουργία του αρχικού σκελετού αρχείων LaTeX.
02/10/2016	Συγγραφή της πρώτης ενότητας (1.2.2)
09/10/2016	Ολοκλήρωση Κεφαλαίου 1
09/10/2016	Δημιουργία της Παρουσίασης διδασκαλίας
29/10/2016	Ολοκλήρωση Κεφαλαίου 2
29/01/2017	Ολοκλήρωση Κεφαλαίου 3
07/02/2017	Ολοκλήρωση Κεφαλαίου 4
08/02/2017	Προσθήκη Παραρτήματος: Μεθοδολογία Ασκήσεων Κεφ. 3
09/02/2017	Ολοκλήρωση όλων των εναπομείναντων εικόνων / σχημάτων
16/02/2017	Προσθήκη φωτογραφίας / αφιέρωσης
18/02/2017	Ολοκλήρωση Κεφαλαίου 8
19/02/2017	Προσθήκη Επίσημου Εξωφύλλου Έκδοσης (Σκίτσο)
19/02/2017	Ολοκλήρωση Κεφαλαίου 7
21/02/2017	Ολοκλήρωση Κεφαλαίου 5
23/02/2017	Προσθήκη του παρόντος Παραρτήματος
24/02/2017	Ολοκλήρωση κειμένου. Αναθεώρηση alpha1
27/02/2017	Αναθεώρηση beta1
01/03/2017	Επίσημη Κυκλοφορία 1.00