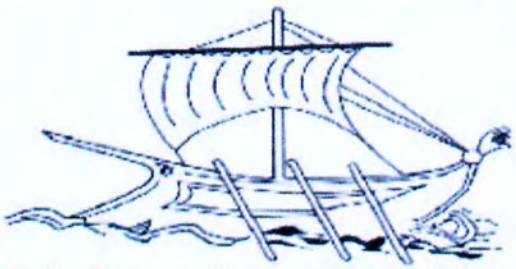


Τεχνολογικό Εκπαιδευτικό Ίδρυμα
Τ.Ε.Ι. ΠΕΙΡΑΙΑ

Πτυχιακή Εργασία

Θέμα: Το Ασύρματο Δίκτυο του Τμήματος Αυτοματισμού

Πειραιάς 2012

Καθηγητής: Ιωάννης Αγγελόπουλος

Σπουδαστές: Βασιλική Σπάνια

Κωνσταντίνος Λώτσος

Πίνακας περιεχομένων

Σπουδαστές: Βασιλική Σπάνια - Κωνσταντίνος Λώτσος

1 ΕΙΣΑΓΩΓΗ

1.1 Η ΑΡΧΙΚΗ ΙΔΕΑ

Οι ολοένα αυξανόμενες ανάγκες για επικοινωνία στις μέρες μας, κάνουν την χρήση του διαδικτύου ένα απαραίτητο αγαθό. Καθημερινά, εκατομμύρια άνθρωποι ανά τον κόσμο, αναζητούν πληροφορίες, ενημερώνονται, ανταλλάσουν emails και αρχεία, μιλούν με τα VoIP τηλέφωνα τους, και άλλα πολλά. Η αρχική λοιπόν ιδέα για την παρούσα πτυχιακή εργασία ήταν όλες αυτές οι πολύτιμες δυνατότητες που μας προσφέρει το διαδίκτυο ήταν δύσκολα προσβάσιμες από τους χώρους του ΤΕΙ. Έτσι σκεφτήκαμε να φτιάξουμε ένα ασύρματο δίκτυο οπού θα έλυνε το πρόβλημα αυτό και θα παρείχε την δυνατότητα σε όλους τους χώρους του κτιρίου μας να χρησιμοποιούμε το διαδίκτυο.

Επίσης η ραγδαία αύξηση των φορητών συσκευών με δυνατότητες ασύρματης δικτύωσης όπως είναι τα laptops, τα netbooks, τα smartphones, tablets, έκαναν ολοένα και περισσότερο την ανάγκη για πρόσβαση των φοιτητών αλλά και των καθηγητών στο διαδίκτυο επιτακτικότερη.

Εικόνα 1-1

Βασικός στόχος του όλου εγχειρήματος ήταν η ασφάλεια του ασύρματου δικτύου και κατ' επέκταση η ασφάλεια του δικτύου του ΤΕΙ. Για τον λόγο αυτό αναπτύξαμε μια ιστοσελίδα Captive Portal σε συνδυασμό με Radius Server, μέσα από την οποία θα μπορεί ο καθένας να συνδέεται στο δίκτυο με τον προσωπικό του κωδικό, «επώνυμα». Στο κομμάτι αυτό ευχαριστούμε για την βοήθεια του τον κ. Νικόλαο Αλαφοδήμο ο οποίος διατηρεί τον server με τα registrations.

Σε όλη την προσπάθεια καθοριστικό ρόλο έπαιξε η βοήθεια και η στήριξη του καθηγητή μας, του τμήματος Αυτοματισμού, κύριου Ιωάννη Αγγελόπουλου, ο οποίος από την αρχή βοήθησε την προσπάθεια αυτή, δίνοντας μας τις κατάλληλες κατευθύνσεις ως προς την μελέτη καθώς και την υλοποίηση του εγχειρήματος μας. Με την σειρά μας, τον ευχαριστούμε θερμά για την πολύτιμη βοήθεια του.

1.2 ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΔΙΚΤΥΩΣΗ

1.2.1 Μεταφορά δεδομένων

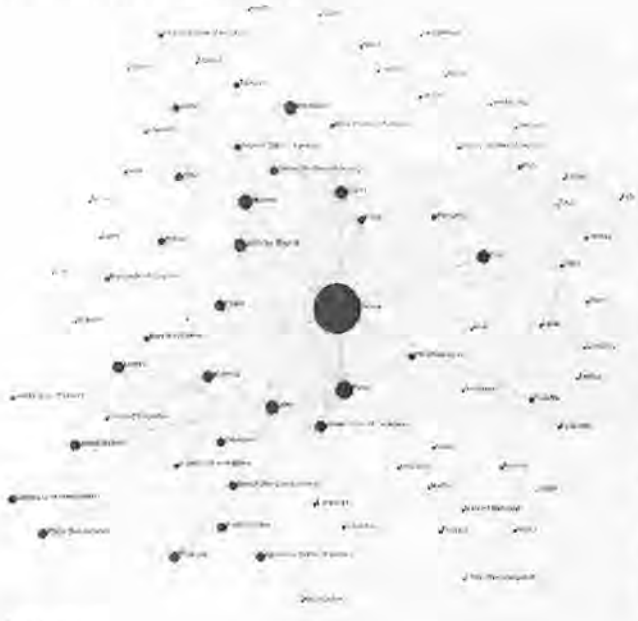
Τα δίκτυα δεδομένων εξαπλώνονται με ιλιγγιώδεις ρυθμούς και έχουν προ πολλού γίνει εργαλείο μελέτης, εργασίας και διασκέδασης που επηρεάζει όλους τους τομείς της ανθρώπινης δραστηριότητας. Η επικοινωνία δεδομένων έναντι της κλασσικής επικοινωνίας όπου η ανταλλασσόμενη πληροφορία ήταν κυρίως σε μορφή φωνής έφτασε στις μέρες μας να ξεπεράσει την κίνηση φωνής ενώ συνεχίζει να αυξάνει αλματωδώς.

Ένα δίκτυο επικοινωνιών σχηματίζεται με την διασύνδεση ενός συνόλου υπολογιστών εις τρόπον ώστε να μπορούν να ανταλλάσσουν πληροφορίες. Η επικοινωνία των υπολογιστών επιτυγχάνεται με την ανταλλαγή μηνυμάτων ειδικής φόρμας ακολουθώντας ειδικούς κανόνες (πρωτόκολλα) ώστε να μπορούν να τα ερμηνεύουν όλοι οι υπολογιστές που διαθέτουν τις αντίστοιχες προβλέψεις υπό μορφή υλικού (π.χ. κάρτας δικτύου) και λογισμικού (π.χ. πρωτόκολλο TCP/IP). Η απλούστερη μορφή δικτύου λαμβάνει χώρα όταν οι υπολογιστές συνδέονται ανά δύο απ' ευθείας με μια τηλεπικοινωνιακή ζεύξη σημείου προς σημείο. Όμως εκτός από πολύ απλές περιπτώσεις αυτό δεν είναι και τόσο χρήσιμη λύση διότι δεν είναι γενικεύσιμη. Οι υπολογιστές μπορεί να βρίσκονται πολύ μακριά ο ένας από τον άλλο, ώστε να μην δικαιολογείται το κόστος της απ' ευθείας σύνδεσης. Επίσης, εάν ακολουθήσουμε αυτή τη λογική θα πρέπει να ξεκινά από την κάθε συσκευή ένα πλήθος τέτοιων ζεύξεων ίσων με όλα τα πιθανά σημεία ανταπόκρισης. Δηλαδή αν δούμε την αντίστοιχη περίπτωση τηλεφωνίας, για να μπορεί να συνδεθεί το τηλέφωνο μας σε οποιαδήποτε άλλη τηλεφωνική συσκευή στη γη θα έπρεπε να ξεκινάνε από το σπίτι μας εκατομμύρια γραμμές που δεν θα υπήρχε χώρος να τοποθετηθούν, αλλά και θα χρειαζόντουσαν ώρες να βρεθεί η γραμμή του κάθε ανταποκριτή. Το πρόβλημα αυτό έλυσαν τα δίκτυα και η τεχνική της μεταγωγής (switching).

Ωστόσο η πιο κατάλληλη μέθοδος μεταγωγής για τα δεδομένα δεν συμπίπτει με τη μέθοδο που παραδοσιακά ακολουθήθηκε στην τηλεφωνία. Έτσι ο σχεδιασμός ενός δικτύου υπολογιστών, έχει πολλά κοινά σημεία αλλά και σημαντικές διαφορές με το σχεδιασμό του τηλεφωνικού δικτύου. Η επικοινωνία μεταξύ υπολογιστών έχει μερικές χαρακτηριστικές ιδιότητες που είναι ουσιωδώς διαφορετικές από εκείνες της τηλεφωνικής μετάδοσης. Όταν δύο άνθρωποι συνομιλούν, τα χάσματα στη συνομιλία διαρκούν λίγο οπότε η τηλεπικοινωνιακή κίνηση που προκύπτει είναι σχεδόν σταθερού ρυθμού. Ενίοτε μάλιστα οι γύρω ήχοι που περιγράφουν μία "ατμόσφαιρα" πρέπει να μεταφερθούν (π.χ. μετάδοση αθλητικού γεγονότος) οπότε απαιτείται συνεχής μετάδοση σταθερού ρυθμού. Επίσης η φωνή είναι μία υπηρεσία πραγματικού χρόνου που δεν ανέχεται καθυστέρηση. Αντίθετα όταν επικοινωνούν υπολογιστές η ακριβής στιγμή άφιξης της πληροφορίας δεν έχει κρίσιμη σημασία, ενώ τα χάσματα είναι ο κανόνας, όχι η εξαίρεση. Μια σειρά δεδομένων, π.χ. μεταφορά ενός αρχείου μπορεί να ακολουθηθεί από σιωπή πολλών λεπτών που ο χειριστής μελετά κάποιο μενού ή φτιάχνει τον καφέ του. Η μεταφορά από υπολογιστή σε υπολογιστή χρειάζεται διακοπτόμενη χρήση ενός κατά κανόνα μεγάλου εύρους ζώνης καναλιού. Το απαιτούμενο εύρος ποικίλει φυσικά πάρα πολύ αλλά γενικώς είναι εκνευριστικό να υπάρχει μεγάλη αναμονή μετά την αίτηση κάποιας εξυπηρέτησης. Έτσι ενώ δημιουργούνται στιγμιαία απαιτήσεις για υψηλό εύρος ζώνης, δεν υπάρχει καλή χρησιμοποίηση του καναλιού κατά το πλείστο του χρόνου. Επίσης η κίνηση υπολογιστών δεν ανέχεται σφάλματα ούτε ελάχιστων δυαδικών ψηφίων ενώ η φωνή δεν χάνει την κατανοησιμότητά της ακόμη και μετά την αλλοίωση πολλών ψηφίων.

Για την επικοινωνία υπολογιστών δημιουργήθηκαν δίκτυα δεδομένων στα οποία η χρήση των καναλιών είναι σε στατιστική βάση ενώ η πληροφορία είναι οργανωμένη σε ενότητες αποκαλούμενες πακέτα γι' αυτό και αποκαλούνται δίκτυα πακέτων (packet networks). Ο λόγος είναι ότι τα πακέτα περιέχουν τη διεύθυνση προορισμού πράγμα που δεν μπορεί να γίνει με την αναλογική φωνή και ως εκ τούτου μπορούν να αναγνωρίζονται ακόμη και όταν ανακατεύονται πακέτα πολλών χρηστών στο ίδιο κανάλι (πολύπλεξη). Αυτή η ιδιότητα επιτρέπει να μεταδίδονται από το ίδιο κανάλι μία το πακέτο ενός χρήστη και μία αυτό ενός άλλου κάνοντας αποδοτικότερη χρήση των ακριβών πόρων του δικτύου και ρίχνοντας σημαντικά το κόστος επικοινωνίας. Έτσι, δεν δεσμεύονται κυκλώματα είτε υπάρχει κίνηση είτε όχι, αλλά χρησιμοποιούνται κατ' απαίτηση (on demand). Στους κόμβους ενός τέτοιου δικτύου χρησιμοποιείται μία ουσιωδώς διαφορετική τεχνική μεταγωγής για την δρομολόγηση των πακέτων που αποκαλείται μεταγωγή πακέτων. (Η επιτυχία των δικτύων πακέτων είναι τέτοια που τείνουν όλες οι υπηρεσίες ακόμη και της ζώσης φωνής να διαβιβάζονται μέσω της τεχνικής πακέτων αν και υπάρχουν κάποιοι περιορισμοί που δεν επιτρέπουν την επίτευξη της ίδιας ποιότητας. Ωστόσο οι εξελίξεις δείχνουν ότι στο μέλλον η πακετοποίηση της φωνής θα επεκταθεί και θα κυριαρχήσει στα δίκτυα ενοποιημένων υπηρεσιών χάρις στην μικτή τεχνική του ATM αλλά και στο Διαδίκτυο (voice over IP).

1.2.2 Έλεγχος σφαλμάτων



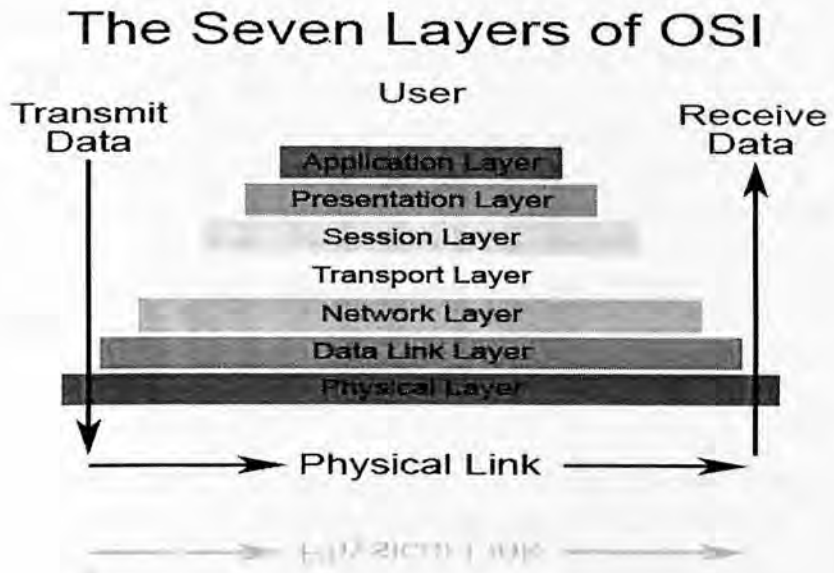
Εικόνα 1-2

Σε ένα τέλειο κύκλωμα μετάδοσης, το σήμα που εισέρχεται στο ένα άκρο είναι πανομοιότυπο με εκείνο που εξέρχεται από το άλλο. Αλλά στον πραγματικό κόσμο υπάρχει σχεδόν πάντα κάποιο είδος θορύβου, ο οποίος μπορεί να παρεμβληθεί στο αρχικό καθαρό σήμα μας. Ως θόρυβος ορίζεται οτιδήποτε μπορεί να προστεθεί στο αρχικό σήμα, θα μπορούσε να προκληθεί από κεραυνό, παρεμβολή από άλλο κανάλι επικοινωνίας, ή σκόνη σε μια ηλεκτρική επαφή σε κάποιο σημείο του κυκλώματος. Ανεξάρτητα από την πηγή, ο θόρυβος στο κανάλι μπορεί να διακόψει τη ροή των δεδομένων. Σε

ένα σύγχρονο σύστημα επικοινωνίας, αυτά τα bit ρέουν μέσω του κυκλώματος υπερβολικά γρήγορα — εκατομμύρια κάθε δευτερόλεπτο — άρα ένα χτύπημα θορύβου ακόμη και για κλάσμα του δευτερολέπτου μπορεί να εξαλείψει αρκετά bit ώστε να μετατρέψει τα δεδομένα σας σε ψηφιακές ασυναρτησίες.

Επομένως, στο ρεύμα των δεδομένων σας πρέπει να συμπεριλάβετε μια διαδικασία που ονομάζεται έλεγχος σφαλμάτων (error checking). Ο έλεγχος σφαλμάτων επιτυγχάνεται με την προσθήκη κάποιου είδους τυπικών πληροφοριών σε κάθε byte. Σε ένα απλό δίκτυο δεδομένων υπολογιστών, οι πληροφορίες χειραψίας (handshaking information), που περιγράφονται στην επόμενη ενότητα, ονομάζονται *bit ισοτιμίας* (parity bit), το οποίο πληροφορεί τη συσκευή που λαμβάνει κάθε byte αν το άθροισμα των μονάδων και των μηδενικών μέσα στο byte είναι άρτιο ή περιττό. Αν η συσκευή λήψης διαπιστώσει ότι το bit ισοτιμίας δεν είναι αυτό που ανέμενε, δίνει εντολή στον πομπό να στείλει ξανά το ίδιο byte. Αυτή η τιμή ονομάζεται άθροισμα ελέγχου (checksum). Τα πιο σύνθετα δίκτυα, μεταξύ των οποίων και τα ασύρματα συστήματα, περιλαμβάνουν πρόσθετα δεδομένα χειραψίας για τον έλεγχο σφαλμάτων σε κάθε ακολουθία δεδομένων.

1.2.3 Η στρωμάτωση OSI



Εικόνα 1-3 - Η στρωμάτωση OSI

1.2.3.1 Επίπεδο 7: Εφαρμογών

Το *επίπεδο εφαρμογών* παρέχει στον χρήστη έναν τρόπο να προσπελάσει μέσω μιας εφαρμογής τις πληροφορίες ενός δικτύου. Αυτό το επίπεδο είναι η κύρια διασύνδεση του χρήστη με την εφαρμογή και, συνεπώς, με το δίκτυο. Στο επίπεδο αυτό γίνεται η διαχείριση των κατανεμημένων εφαρμογών, η αποστολή του ηλεκτρονικού ταχυδρομείου κλπ. Παραδείγματα πρωτοκόλλων επιπέδου εφαρμογών αποτελούν τα Telnet, FTP, SMTP και http.

1.2.3.2 Επίπεδο 6: Παρουσίασης

Το *επίπεδο παρουσίασης* μετασχηματίζει τα δεδομένα σε τυπική μορφή που την αναμένει το επίπεδο εφαρμογών. Στο επίπεδο αυτό τα δεδομένα υφίστανται κρυπτογράφηση, συμπίεση, κωδικοποίηση MIME και όποια άλλη διαμόρφωση απαιτεί η μορφή δεδομένων ή ο σχεδιαστής του πρωτοκόλλου. Παραδείγματα αποτελούν η μετατροπή αρχείων από κώδικα EBCDIC σε κώδικα ASCII και η μετατροπή της δομής των δεδομένων σε μορφή XML ή αντίστροφα (π.χ. από XML σε έγγραφο τύπου DOC).

1.2.3.3 Επίπεδο 5: Συνόδου

Το *επίπεδο συνόδου* ελέγχει τις συνόδους (δηλαδή τις ανταλλαγές δεδομένων) μεταξύ δύο υπολογιστών, του Α και του Β. Ξεκινά, διαχειρίζεται και τερματίζει τη σύνδεση μεταξύ μιας τοπικής και μιας απομακρυσμένης εφαρμογής. Αντιμετωπίζει λειτουργίες FDX (full duplex, οι Α και Β μιλούν ταυτόχρονα από δύο κανάλια) ή HDX (half-duplex, μιλάει ο Α και μετά απαντάει ο Β από το ένα διαθέσιμο κανάλι), ενώ υποστηρίζει διαδικασίες αποθήκευσης κατάστασης (αγγλ. checkpoint), αναβολής (αγγλ. adjournment), τερματισμού (αγγλ. termination) και επανεκκίνησης (αγγλ. restart). Αυτό το επίπεδο είναι υπεύθυνο για το ομαλό κλείσιμο της συνόδου (που είναι ιδιότητα του TCP) και επίσης για την *αποθήκευση* και *ανάκτηση κατάστασης*, λειτουργίες οι οποίες δεν χρησιμοποιούνται στην στοίβα πρωτοκόλλων του Διαδικτύου.

1.2.3.4 Επίπεδο 4: Μεταφοράς

Το *επίπεδο μεταφοράς* διεκπεραιώνει τη μεταφορά των δεδομένων από χρήστη σε χρήστη, απαλλάσσοντας έτσι τα ανώτερα επίπεδα από κάθε φροντίδα να προσφέρουν αξιόπιστη μεταφορά δεδομένων από το ένα άκρο της επικοινωνίας στο άλλο. Το επίπεδο μεταφοράς ελέγχει την αξιοπιστία ενός χρησιμοποιούμενου καναλιού με έλεγχο ροής (αγγλ. flow control), κατάτμηση και αποτμηματοποίηση (αγγλ. segmentation / desegmentation), καθώς και έλεγχο σφαλμάτων (αγγλ. error control). Ορισμένα πρωτόκολλα καταγράφουν καταστάσεις και συνδέσεις, οπότε κρατούν λογαριασμό των πακέτων και

επανεκπέμπουν αυτά που δεν παρελήφθησαν σωστά. Τα διάφορα πρωτόκολλα μορφοποιούν διαφορετικά τα εκπεμπόμενα πακέτα πληροφοριών, αλλά τα προς αποστολή δεδομένα παραλαμβάνονται αρχικά από τα ανώτερα επίπεδα.

Το συνηθέστερο παράδειγμα πρωτοκόλλου μεταφοράς είναι το TCP (αγγλ. Transmission Control Protocol, πρωτόκολλο ελέγχου μετάδοσης). Άλλα πρωτόκολλα μεταφοράς είναι τα UDP (αγγλ. User Datagram Protocol, πρωτόκολλο για ασυνδεσμική αποστολή δεδομένων, SCTP (αγγλ. Stream Control Transmission Protocol, πρωτόκολλο ελέγχου της ροής μετάδοσης), κλπ.

1.2.3.5 Επίπεδο 3: Δικτύου

Το *επίπεδο δικτύου* παρέχει τα λειτουργικά και διαδικαστικά μέσα για τη μεταφορά στοιχειοσειρών δεδομένων μεταβλητού μήκους από μια προέλευση σε έναν προορισμό, μέσα από ένα ή περισσότερα ενδιάμεσα δίκτυα, ενώ διατηρεί την ποιότητα εξυπηρέτησης που απαιτεί το επίπεδο μεταφοράς. Το επίπεδο δικτύου εκτελεί λειτουργίες δρομολόγησης, με πιθανές κατατμήσεις / αποτμηματοποίηση, και αναφέρει σφάλματα σχετικά με την παράδοση των πακέτων. Οι δρομολογητές (αγγλ. restart) λειτουργούν στο επίπεδο αυτό· διακινώντας δεδομένα σε διασυνδεδεμένα δίκτυα έκαναν το Διαδίκτυο πραγματικότητα. Υπάρχουν και δικτυακοί διακόπτες που σχετίζονται με τις διευθύνσεις (IP). Εδώ υπάρχει μια λογική οργάνωση και τις τιμές των διευθύνσεων τις καθορίζει ιεραρχικά ο τεχνικός των επικοινωνιών. Το πλέον αναγνωρίσιμο παράδειγμα πρωτοκόλλου δικτύου είναι το Πρωτόκολλο Διαδικτύου (αγγλ. Internet Protocol, IP).

1.2.3.6 Επίπεδο 2: Ζεύξης Δεδομένων

Το *επίπεδο ζεύξης* δεδομένων παρέχει τα λειτουργικά και διαδικαστικά μέσα για τη μεταφορά δεδομένων από μια συσκευή ενός τοπικού δικτύου σε άλλη, αλλά και για την ανίχνευση και διόρθωση σφαλμάτων που συμβαίνουν στο φυσικό επίπεδο. Οι μη ιεραρχημένες διευθύνσεις των συσκευών εδώ είναι οι φυσικές (π.χ. MAC διευθύνσεις), δηλαδή είναι προκαθορισμένες και αποθηκευμένες στις κάρτες δικτύου των επικοινωνούντων κόμβων από το εργοστάσιο.

Το πιο γνωστό πρότυπο αυτού του επιπέδου είναι το Telnet, για τοπικά δίκτυα. Άλλα παραδείγματα πρωτοκόλλων ζεύξης δεδομένων αποτελούν τα:

- HDLC και ADCCP, για συνδέσεις από-σημείο-σε-σημείο (αγγλ. half-a-half).
- 802.11, για ασύρματα τοπικά δίκτυα.

Στα τοπικά δίκτυα της οικογένειας πρωτοκόλλων IEEE 802, και σε κάποια άλλα όπως το FDDI, αυτό το επίπεδο μπορεί να διαιρεθεί σε δύο μικρότερα:

- Ένα επίπεδο ελέγχου πρόσβασης στο κοινό μέσο, το επίπεδο MAC (αγγλ. On Access Control, Έλεγχος Πρόσβασης Μέσου)
- Ένα ανώτερο επίπεδο ελέγχου λογικών συνδέσεων, το υποεπίπεδο LLC (αγγλ. Logical Link Control, Έλεγχος Λογικών Ζεύξεων), όπου επικρατεί καθολικά το πρωτόκολλο IEEE 802.2 ανεξάρτητα από το υποκείμενο πρωτόκολλο MAC ή φυσικού επιπέδου.

Στο επίπεδο αυτό λειτουργούν οι δικτυακές *γέφυρες* (αγγλ. bridge) και οι δικτυακοί διακόπτες (αγγλ. switch). Η συνδεσιμότητα παρέχεται μόνο για κόμβους που συνδέονται στο ίδιο κοινό μέσο (τοπικό δίκτυο ή σύνδεση από-σημείο-σε-σημείο).

1.2.3.7 Επίπεδο 1: Φυσικό

Το *φυσικό επίπεδο* ορίζει όλες τις ηλεκτρικές και φυσικές προδιαγραφές της επικοινωνίας. Σ' αυτές περιλαμβάνονται οι σχηματισμοί των ακίδων, οι επιτρεπτές τάσεις, οι προδιαγραφές των καλωδίων κλπ. Συσκευές φυσικού επιπέδου είναι οι διανεμητές (αγγλ. hub), οι επαναλήπτες (αγγλ. repeater), οι κάρτες δικτύου (αγγλ. NIC), οι προσαρμοστές (αγγλ. adaptor) διαύλου (αγγλ. bus). Οι κυριότερες λειτουργίες και υπηρεσίες του φυσικού επιπέδου είναι:

- Έναρξη και τερματισμός της ηλεκτρικής σύνδεσης μιας επικοινωνιακής συσκευής.
- Συμμετοχή σε διαδικασίες όπου οι επικοινωνιακές συσκευές εξυπηρετούν αποτελεσματικά πολλούς χρήστες (πολυπλεξία). Επιλύονται προβλήματα προτεραιότητας πρόσβασης και ελέγχου ροής δεδομένων.
- Διαμόρφωση και αποδιαμόρφωση των ψηφιακών δεδομένων κατά τη μετάδοση από συσκευή σε συσκευή. Για παράδειγμα, τα ψηφιακά ηλεκτρικά σήματα μπορεί να ταξιδέψουν ως αναλογικά σε χάλκινο καλώδιο, μετά σε οπτική ίνα, μετά να μεταδοθούν από ραδιοζεύξη ή δορυφορικά, να φθάσουν πάλι αναλογικά σε χάλκινο καλώδιο και να γίνουν ψηφιακά στον παραλήπτη.

Οι παράλληλοι δίαυλοι SCSI λειτουργούν στο επίπεδο αυτό. Επίσης τα επίπεδα 1 και 2 αφορούν οι προδιαγραφές των πρωτοκόλλων Ethernet, Token Ring, FDDI (αγγλ. Fiber Distributed Data Interface, Διασύνδεση Κατανεμημένων Δεδομένων με Οπτικές Ίνες) και IEEE 802.11.

Η στρωμάτωση που προτείνει η αρχιτεκτονική OSI έχει σκοπό την ανάλυση του πολύπλοκου έργου της μελέτης και σχεδίασης των δικτύων τηλεπικοινωνιών σε μικρότερες επί μέρους ενότητες οι οποίες είναι ευκολότερο να μελετηθούν και περιορίζονται σε μικρό εύρος γνωστικών αντικειμένων. Είναι περισσότερο μία λογική κατάτμηση με βάση τον

διαχωρισμό λειτουργιών και πρωτοκόλλων και θα την ακολουθήσουμε στη οργάνωση της ύλης, εξετάζοντας τα στρώματα από κάτω προς τα επάνω. Ωστόσο είναι χρήσιμο πριν την λεπτομερή εξέταση των πρωτοκόλλων ανά στρώμα, να δούμε και τις συνιστώσες ενός τηλεπικοινωνιακού δικτύου από μια άλλη σκοπιά διακρίνοντας κάποια υποσυστήματα ανεξαρτήτως του πόσα στρώματα υλοποιούνται μέσα σε αυτά. Θα δοθεί παράλληλα η ευκαιρία εξοικείωσης και με τους βασικούς τηλεπικοινωνιακούς και συσκευές. Μία πολύ απλοποιημένη αλλά τυπική άποψη ενός δικτύου φαίνεται στο σχήμα 1-1 που θα μπορούσαμε να την θεωρήσουμε το «δάσος» των τηλεπικοινωνιών σε αντίθεση με τα επί μέρους «δένδρα» τα οποία θα μελετήσουμε στην συνέχεια με σκοπό να κατανοήσουμε σε βάθος όσα λαμβάνουν χώρα στο δίκτυο. Την γενική αυτή εικόνα είναι καλό να την φέρνουμε πάντα στο νου μας όταν μελετούμε επί μέρους πρωτόκολλα για να αντιλαμβανόμεθα το συνολικό αποτέλεσμα και την χωροθέτηση της επενέργειας των λειτουργιών και των πρωτοκόλλων του κάθε δικτύου.

Ένα λοιπόν επικοινωνιακό σύστημα αποτελείται από τα εξής κύρια στοιχεία:

- Τερματικές συσκευές (terminal equipment) π.χ. τηλέφωνα, τερματικά χαρακτήρων, υπολογιστές κτλ.

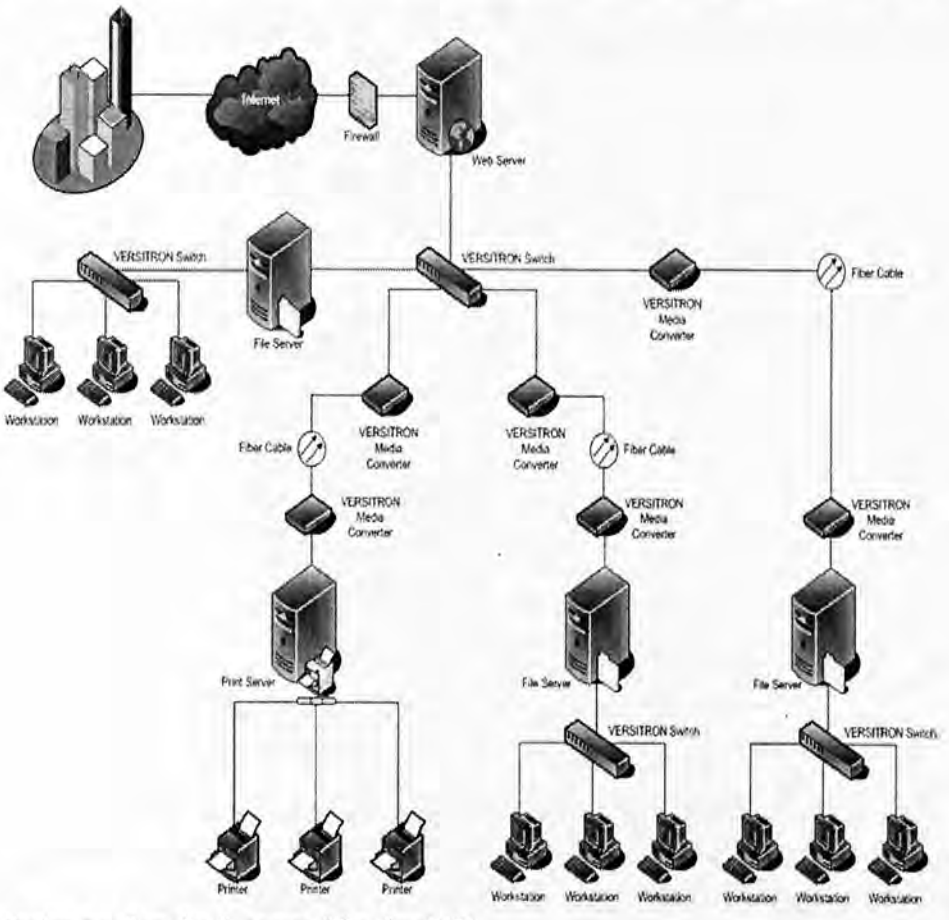
- Ζεύξεις (links). Οι ζεύξεις παρέχουν κανάλια επικοινωνίας βασισμένα σε ενσύρματα ή ασύρματα, οπτικά ή ηλεκτρικά μέσα. Ενώνουν κόμβους μεταξύ τους καθώς και τερματικά προς στους κόμβους. Στα δύο άκρα μιας ζεύξης βρίσκονται οι τερματιστές της γραμμής που περιέχουν τους πομποδέκτες που αποστέλλουν / λαμβάνουν το σήμα στη γραμμή. Η ζεύξη λοιπόν αποτελείται από δύο τερματιστές και το μέσο μεταφοράς (σύρμα, οπτική ίνα, ή και απλά αέρα στην περίπτωση της ασύρματης ή της δορυφορικής ζεύξης).

- Κόμβους (nodes) δηλ. μεταγωγείς (switches) ή δρομολογητές (routers) τηλεφωνικά κέντρα (telephone exchanges). Είναι τα σημεία όπου επιλέγεται η διαδρομή του πακέτου.

2 ΕΝΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

2.1 ΙΣΤΟΡΙΑ ΕΝΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

Τα ενσύρματα δίκτυα υπολογιστών, εδώ και πολλά χρόνια έχουν ίσως το



Εικόνα 2-1 - Τοπολογία τοπικού δικτύου LAN

μεγαλύτερο μερίδιο στην "πίτα" των δικτύων. Από το πρώτο μεγάλο δίκτυο, το τηλεφωνικό, μέχρι και στις μέρες μας, η σύνδεση υπολογιστών με χρήση καλωδίων είναι η πιο διαδεδομένη. Υπάρχουν πολλοί λόγοι για τους οποίους οι μηχανικοί δικτύων χρησιμοποιούν τα ενσύρματα δίκτυα. Ο πιο σημαντικός λόγος είναι φυσικά το κόστος. Για μικρής και μεσαίας κλίμακας δίκτυα, το καλώδιο είναι η πιο ελκυστική λύση. Το κόστος κατασκευής, προμήθειας, εγκατάστασης και συντήρησης είναι πολύ μικρό, ενώ είναι αρκετά αξιόπιστο, γρήγορο και ασφαλές.

Ενδεικτικά, αναφέρουμε μερικούς τύπους καλωδίων που χρησιμοποιούνται:

Συνεστραμμένου ζεύγους (STP/UTP -- θωρακισμένο και μη, αντίστοιχα)

Category 1 (1 MHz)

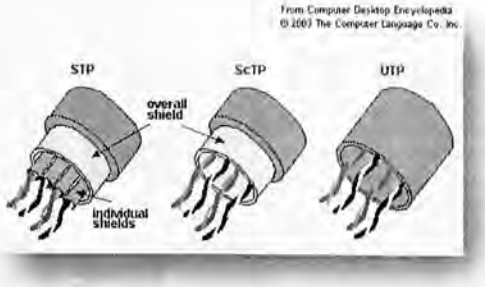
Category 2 (4MHz)

Category 3 (16MHz)

Category 4 (20 MHz)

Category 5 (100MHz)

Category 6 (250MHz)



Εικόνα 2-2 - Τύποι καλωδίων δικτύου

Category 7 (έως και 600MHz μέσα από καλώδιο 100Ohm)

Ομοαξονικό καλώδιο

Hard Line

Tri axial

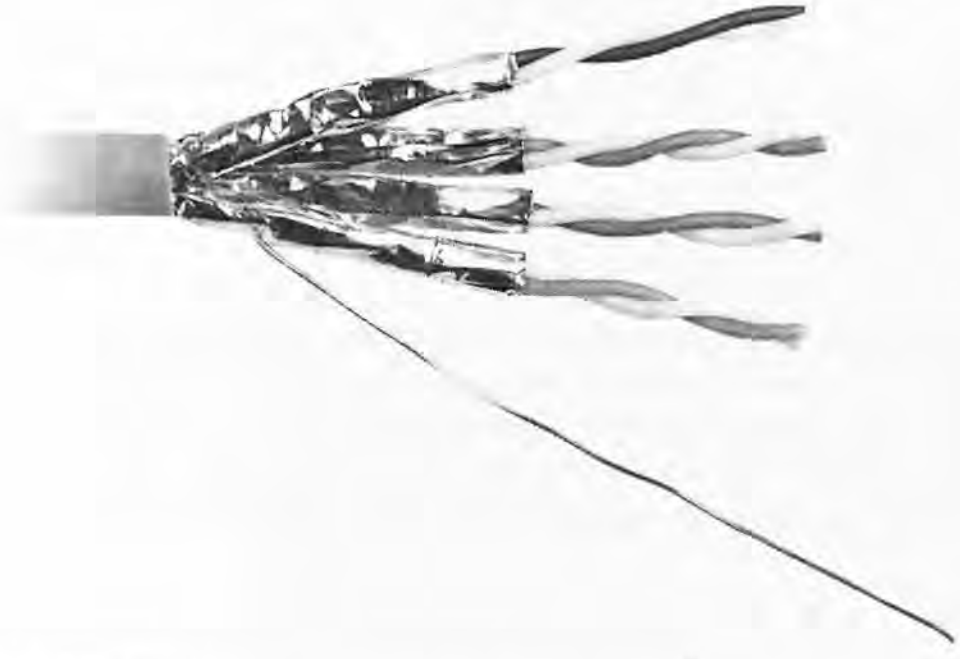
Twin axial

Bi axial

Semi rigid

Αρχικά, όταν ξεκίνησαν να αναπτύσσονται τα δίκτυα υπολογιστών, και κυρίως για μικρές αποστάσεις, χρησιμοποιούσαμε αρκετά το ομοαξονικό καλώδιο. Γρήγορα όμως, παρατήθηκε ότι δεν προσέφερε μεγάλες ταχύτητες και μετάδοση σε μεγάλες αποστάσεις. Πλέον χρησιμοποιείται, επί το πλείστον, το καλώδιο συνεστραμμένου ζεύγους. Για καθημερινή χρήση (απλά δίκτυα), χρησιμοποιούμε το UTP, το οποίο είναι φθηνό, και αρκετά αξιόπιστο, ενώ για μεγαλύτερες απαιτήσεις χρησιμοποιείται το STP, το οποίο είναι μεν αρκετά ακριβότερο, αλλά παρέχει μεγαλύτερη αξιοπιστία. Σ' αυτό το σημείο, να σημειωθεί, ότι η θωράκιση στην καλωδίωση είναι απαραίτητη προκειμένου να προστατέψουμε τα δεδομένα που μεταφέρουμε μέσα από το καλώδιο από ηλεκτρομαγνητικές παρεμβολές, είτε αυτές προέρχονται από το ίδιο το καλώδιο, είτε από το περιβάλλον (για παράδειγμα κρουστικός θόρυβος). Το

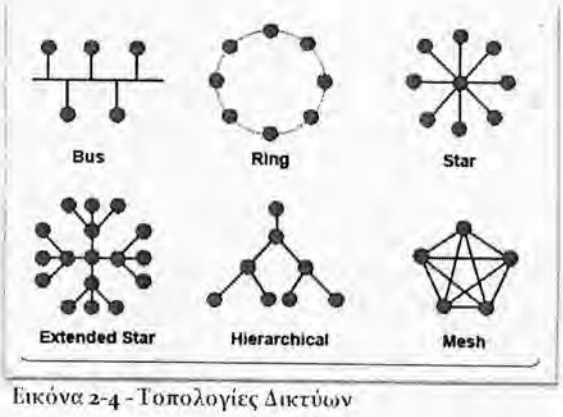
γεγονός ότι τα καλώδια του UTP/STP είναι συνεστραμμένα, είναι ένα πρώτο βήμα για την προστασία από ηλεκτρομαγνητική παρεμβολή (κάθε καλώδιο από κάθε ζεύγος δημιουργεί αντίστροφο μαγνητικό πεδίο από το ταίρι του, με σκοπό να ακυρώνει το ένα το πεδίο του άλλου), αλλά σε μεγάλες ταχύτητες μετάδοσης (για παράδειγμα στο Cat5e ή στο Cat6) όπου οι ρυθμοί μετάδοσης είναι της τάξης των Gbps, αυτή η προστασία δεν είναι αρκετή.



Εικόνα 2-3 - Καλώδιο **SFTP**

Η καλυπτόμενη απόσταση είναι ένα βασικό κριτήριο που επηρεάζει τον τρόπο σχεδίασης των δικτύων. Λόγω αυτού του χαρακτήρα των πρωτοκόλλων, η απόσταση έχει καταστεί ένας παράγοντας που χαρακτηρίζει την τεχνολογία των δικτύων. Έχουμε τρεις χαρακτηριστικές «χονδρικά» αποστάσεις που οριοθετούν τρεις τεχνολογίες δικτύων: Για αποστάσεις ολίγων μέτρων έως δύο-τριών χιλιομέτρων έχουμε τα Δίκτυα Τοπικής Περιοχής (LAN - Local Area Networks), από λίγα χιλιόμετρα μέχρι 100km έχουμε τα μητροπολιτικά Δίκτυα (MAN - Metropolitan Area Networks) και από εκεί μέχρι την άλλη άκρη του πλανήτη (ακόμα και μέσω δορυφόρων) έχουμε τα Δίκτυα Ευρείας Περιοχής (WAN - Wide Area Networks). Τα κυριότερα πρότυπα Τοπικών Δικτύων είναι τα δίκτυα Ethernet, Token ring, token bus, μητροπολιτικών τα FDDI, DQDB, και ευρείας περιοχής τα Internet SNA, DECNET, TYMNET, κλπ.

2.2 ΠΡΩΤΟΚΟΛΛΑ ΕΝΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ



Εικόνα 2-4 - Τοπολογίες Δικτύων

Με το χρόνο η ανάγκη υιοθέτησης βιομηχανικών προτύπων (standards) έγινε επιτακτική. Μια από τις πρώτες προσπάθειες δημιουργίας προτύπων για Τοπικά Δίκτυα (Τ.Δ.) έγινε από την επιτροπή 802 του Αμερικανικού Ινστιτούτου Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (IEEE). Ο σκοπός ήταν να καθοριστεί μια οικογένεια από πρότυπα Τ.Δ. τα οποία θα αφορούν ειδικά την ενδοδιασύνδεση, την διαχείριση δικτύων και τα επίπεδα 1 και 2 του OSI (φυσικό επίπεδο και επίπεδο δεδομένων). Η επιτροπή IEEE 802 είναι οργανωμένη σε υπο-επιτροπές κάθε μία των οποίων είναι αρμόδια να προτείνει πρότυπα για κάθε τεχνολογία δικτύου. Έχουν κυκλοφορήσει τα εξής πρότυπα:

Η Σειρά Προτύπων 802.Χ της IEEE για Τοπικά Δίκτυα

- 802.1: Προσαρμογή Υψηλού Επιπέδου (High Level Interface)

- 802. 2 Έλεγχος Λογικής Ζεύξης (Logical Link Control)

- 802.3: Δίκτυα CSMA/CD (παραλλαγή του Ethernet)

Το πρωτόκολλο 802.3 αναφέρεται σε γραμμική τοπολογία χρησιμοποιώντας ομοαξονικό καλώδιο με ταχύτητες δεδομένων 10 Mb/s. Στην αρτηρία (bus) του Ethernet μπορούν να συνδεθούν μέχρι και 1000 συσκευές με μέγιστη απόσταση μεταξύ τους μέχρι 2500 μέτρα. Η 802.3 χρησιμοποιεί την μέθοδο πολλαπλής πρόσβασης με αισθητήρα φέροντος και ανίχνευση συγκρούσεων (Carrier Sense Multiple Access with Collision Detection: CSMA/CD). Το πρωτόκολλο αυτό δεν χρησιμοποιείται σε περιβάλλον πραγματικού χρόνου όπου απαιτείται σίγουρη μεταφορά μηνύματος και ελεγχόμενος χρόνος μεταφοράς.

- 802.4: Αρτηρία Σκυτάλης (Token Bus)

Το πρωτόκολλο αυτό αφορά γραμμική τοπολογία χρησιμοποιώντας ομοαξονικό καλώδιο σαν μέσο μεταφοράς και επιτρέπει σηματοδότηση για φωνή και εικόνα με ταχύτητες 1 Mb/s, 5 Mb/s και 10 Mb/s. Επίσης, έχει την ικανότητα να διακρίνει διάφορες προτεραιότητες στη μετάδοση δεδομένων. Στην περίπτωση αυτή, αναγνώριση συγκρούσεων δεν είναι απαραίτητη διότι μόνο ένα τερματικό εκπέμπει πακέτα κάθε φορά μέχρι να εξαντληθεί το απόθεμα πακέτων ή να εξαντληθεί ο χρόνος κράτησης της σκυτάλης.

- 802.5: Δακτύλιος Σκυτάλης (Token Ring)

Η 802.5 προσδιορίζει τοπολογίες δακτυλίου σκυτάλης για χρήση σε ποικίλα μέσα μεταφοράς με ταχύτητες 1 Mb/s και 4 Mb/s. Η τοπολογία του δακτυλίου απλοποιεί την διάταξη μεταφοράς της σκυτάλης και καταργεί το πεδίο διεύθυνσης. Ένα μειονέκτημα του δακτυλίου είναι ότι εάν το μέσο διάδοσης κάπου κοπεί το δίκτυο παύει να λειτουργεί. Η 802.5 διακρίνει οκτώ προτεραιότητες υπηρεσιών.

- 802.6: Μητροπολιτικά Δίκτυα (DQDB).

- 802.7: Τεχνική Συμβουλευτική Ομάδα Ευρείας Ζώνης

- 802.8: Τεχνική Συμβουλευτική Ομάδα Οπτοηλεκτρονικών

- 802.9: Δίκτυα ενοποιημένων δεδομένων και φωνής

- 802.10: Διαλειτουργική Ασφάλεια Τοπικών Δικτύων

- 802.11: Ασύρματα Τοπικά Δίκτυα

- 802.12: Τοπικά Δίκτυα Προτεραιότητος Ζήτησης

- 802.14: Τοπικά Δίκτυα Καλωδιακής Τηλεόρασης

2.3 ΠΡΟΤΟΚΟΛΛΑ ΕΝΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ ΣΗΜΕΡΑ

Το Ethernet είναι αναμφισβήτητα, το συνηθέστερα χρησιμοποιούμενο πρωτόκολλο ενσύρματης τοπικής δικτύωσης υπολογιστών. Αναπτύχθηκε από την εταιρεία Xerox κατά τη δεκαετία του '70 και έγινε δημοφιλές αφότου η Digital Equipment Corporation και η Intel, από κοινού με τη Xerox,

προχώρησαν στην προτυποποίησή του το 1980. Το 1985 το Ethernet έγινε αποδεκτό επίσημα από τον οργανισμό IEEE ως το πρότυπο 802.3 για ενσύρματα τοπικά δίκτυα (LAN).

Το αρχικό Ethernet επέτρεπε ονομαστικούς ρυθμούς μετάδοσης δεδομένων της τάξης των 3 Mbps, μέσω ενός ομοαξονικού καλωδίου στο οποίο συνδέονταν οι επιμέρους υπολογιστές του δικτύου (σύνδεση token ring). Τη διασύνδεση αναλάμβανε μία κάρτα δικτύου Ethernet προσαρτημένη σε κάθε κόμβο, με κάθε κάρτα να χαρακτηρίζεται από μία μοναδική, εργοστασιακή 48-bit διεύθυνση MAC. Σήμερα, η σύνδεση token ring έχει εγκαταλειφθεί ολοκληρωτικά και οι επιμέρους υπολογιστές του δικτύου συνδέονται ο καθένας σε ανεξάρτητη θύρα ενός router ή διανομέα (hub). Έχουν εμφανιστεί νεότερες εκδόσεις του Ethernet οι οποίες χρησιμοποιούν είτε κοινά καλώδια χαλκού με αθωράκιστα (καλώδια UTP) ή θωρακισμένα (καλώδια STP) συνεστραμμένα ζεύγη αγωγών ή οπτικές ίνες.

Αναλυτικότερα, οι κυριότερες μορφές που συναντάμε σήμερα το Ethernet είναι οι παρακάτω:

Ethernet (10MBps), όπου για τις συνδέσεις με χαλκό χρησιμοποιείται το πρότυπο 10BASE-T και για τις οπτικές ίνες το πρότυπο 10BASE-F(L). Η σύνδεση χαλκού είναι συμβατή με αυτή του Fast Ethernet.

Fast Ethernet (100 Mbps), όπου για τις συνδέσεις με χαλκό έχει επικρατήσει το πρότυπο 100BASE-TX έναντι των ουσιαστικά εγκαταλελειμμένων 100BASE-T2, 100BASE-T4. Το 100BASE-TX χρησιμοποιεί καλώδια UTP κατηγορίας 5e (CAT-5e) με 2 ζεύγη αγωγών (ένα για αποστολή και ένα για λήψη δεδομένων), σε μήκη μέχρι 100μ. Πρακτικά, χρησιμοποιούνται καλώδια 4 ζευγών, ώστε να είναι δυνατή η σύνδεση με ή η αναβάθμιση σε Gigabit Ethernet (1000BASE-TX). Το αντίστοιχο πρότυπο για τις οπτικές ίνες είναι το 100BASE-FX. Επιπλέον, είναι δυνατή η αυτόματη ανίχνευση κυκλώματος 10BASE-T στην άλλη πλευρά του καλωδίου και η εν συνεχεία υποβάθμιση της ταχύτητας στα 10Mbps (λειτουργία auto-negotiation).

Gigabit Ethernet (1 Gbps), όπου για τις συνδέσεις με χαλκό έχει επικρατήσει το πρότυπο 1000BASE-T. Το 1000BASE-T χρησιμοποιεί καλώδια UTP κατηγορίας 5e (CAT-5e) με 4 ζεύγη αγωγών. Κάθε ζεύγος μεταφέρει δεδομένα προς τις δύο κατευθύνσεις ταυτόχρονα, ώστε να επιτυγχάνεται η μέγιστη δυνατή ταχύτητα μετάδοσης δεομένων προς κάθε κατεύθυνση. Ο τρόπος σύνδεσης των ζευγών είναι τέτοιος που επιτρέπει σε μια κάρτα Gigabit

Ethernet να μπορεί να ανιχνεύσει την ύπαρξη κυκλώματος Fast Ethernet στην άλλη άκρη του καλωδίου και να αλλάξει αυτόματα το πρωτόκολλό της σε 100BASE-TX (λειτουργία auto-negotiation). Το αντίστοιχο πρότυπο για τις οπτικές ίνες είναι τα 1000BASE-FX.

10Gigabit Ethernet (10Gbps). Οι προδιαγραφές που ορίζει το Ethernet αφορούν το φυσικό επίπεδο και το υποεπίπεδο MAC του μοντέλου αναφοράς OSI. Στη μεγάλη πλειονότητα των περιπτώσεων μαζί με το Ethernet χρησιμοποιείται, στο υποεπίπεδο LLC, το πρωτόκολλο IEEE 802.2. Για τον έλεγχο πρόσβασης στο κοινό μέσο το Ethernet αξιοποιεί τον αλγόριθμο CSMA/CD (Carrier Sense Multiple Access with Collision Detection), στις περιπτώσεις όπου επιτρέπεται μόνο half-duplex σύνδεση.

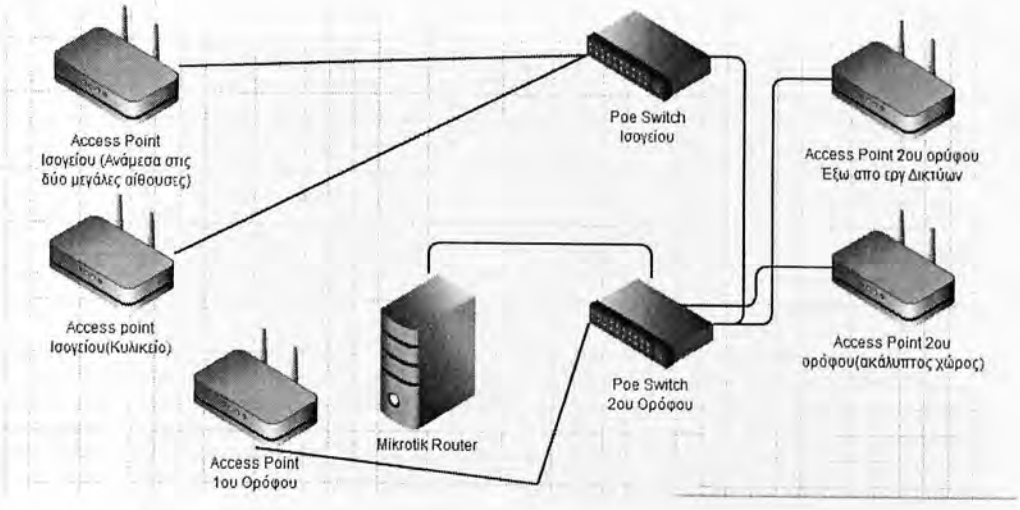
Πρακτικά, το Ethernet χρησιμοποιεί τη μέθοδο μετάδοσης δεδομένων σε μορφή πακέτων (packet switching) μέγιστου μεγέθους (Maximum Transmission Unit, MTU) 1500 bytes και ελάχιστου 46 bytes. Για το σκοπό αυτό, δεδομένα με μήκος μεγαλύτερο των 1500 bytes κατατέμνονται σε πακέτα των 46-1500 bytes (το λεγόμενο payload) τα οποία αποστέλλονται διαδοχικά στη γραμμή επικοινωνίας. Αν το payload έχει μήκος μικρότερο των 46 bytes, προστίθενται επιπλέον κενά bytes ώστε αυτό να αποκτήσει το επιθυμητό ελάχιστο μήκος. Επιπλέον του payload, προστίθενται πληροφορίες όπως ο σειριακός αριθμός της κάρτας Ethernet, οι φυσικές διευθύνσεις (MAC addresses) αποστολέα και παραλήπτη, το μήκος του payload, καθώς και δεδομένα για έλεγχο σφαλμάτων κατά τη μετάδοση.

2.4 ΤΟ ETHERNET ΤΟΥ ΤΕΙ ΠΕΙΡΑΙΑ

Για την υλοποίηση του ασύρματου δικτύου, όπως ήταν φυσικό, χρησιμοποιήσαμε το τοπικό δίκτυο (Ethernet) του ΤΕΙ Πειραιά.

Το τοπικό δίκτυο στο κτίριο μας παρέχει στο κάθε «μπριζάκι» Fast Ethernet (100 Mbps), στο οποίο συνδέσαμε τον δρομολογητή μας στον οποίο δώσαμε την IP: [redacted]. Το δίκτυο αυτό, σύμφωνα με δοκιμές που πραγματοποιήσαμε είδαμε ότι συνδέεται με την IP: [redacted] Public IP και πράγματι, βγαίνει στο διαδίκτυο με ταχύτητα 100Mbps, επίσης είναι συνδεδεμένη η συγκεκριμένη διεύθυνση με το [redacted] reverse dns. Κατά την διαδικασία της εγκατάστασης της καλωδίωσης των access points θα πρέπει να σημειώσουμε, ότι δεν πραγματοποιήσαμε απολύτως καμία αλλαγή ή

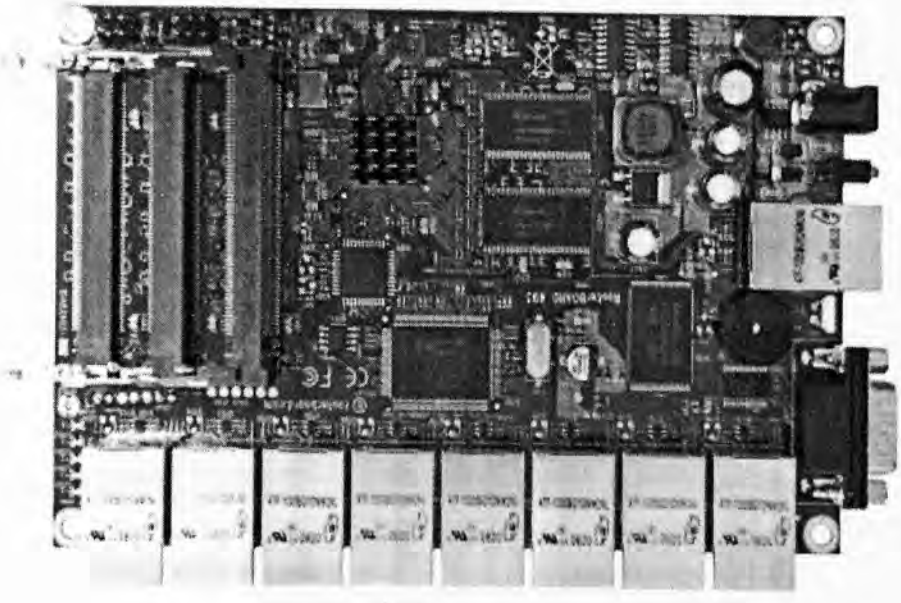
τροποποίηση, ούτε και χρησιμοποιήσαμε μέρος του υπάρχοντος δικτύου του κτιρίου. Αντιθέτως εγκαταστήσαμε νέα καλώδια, με την βοήθεια και την καθοδήγηση των τεχνικών υπηρεσιών του ιδρύματος, σύμφωνα με τις προδιαγραφές που μας υπέδειξαν. Η χρήση τους, γίνεται μόνο για τις λειτουργείς του ασύρματου δικτύου.



Εικόνα 2-5 - Τοπολογία ασύρματου δικτύου Τμήματος Αυτοματισμού

2.5 ΤΟ ETHERNET ΤΟΥ ΑΣΥΡΜΑΤΟΥ ΔΙΚΤΥΟΥ.

2.5.1 Mikrotik Router



Εικόνα 2-6 - Ο κεντρικός **Router** του δικτύου

CPU	Atheros AR7161 680MHz
Memory	128MB DDR onboard memory
Data storage	64MB onboard NAND memory chip
Ethernet	9 x 10/100 Mbit/s Fast Ethernet ports with Auto-MDI/X
miniPCI	Three miniPCI slots
Extras	Reset switch, Beeper
Serial port	One DB9 RS232C asynchronous serial port
LEDs	Power, NAND activity, 5 user LEDs
Power options	Power over Ethernet: 10..28V DC (except power over datalines)Power jack: 10..28V DC
Dimensions	105mm x 160mm
Weight	189 grams
Power	3W without extension cards, maximum – 16 W

consumption	
Operating System	MikroTik RouterOS v4, Level5 license

Την καρδιά του ασύρματου δικτύου, αποτελεί ο Mikrotik Router, ο οποίος έχει εγκατασταθεί σε ένα RouterBoard 493AH και έχει στην διάθεση του εννέα Ethernet Ports, εκ των οποίων η μία, με δυνατότητα Power Over Ethernet(POE) καθώς και τρεις miniPCI θύρες οι οποίες μπορούν να συνδεθούν με αντίστοιχες συσκευές.

Στην περίπτωση μας, χρησιμοποιήσαμε τα τέσσερα από τα εννέα Ethernet Ports, όπως φαίνονται παρακάτω.

name="2_Tei LAN" type="ether" mtu=1500 l2mtu=1522
address=[redacted]
Το interface αυτό χρησιμοποιείται για την σύνδεση του router με το δίκτυο του ΤΕΙ.

name="3_AP_LAN" type="ether" mtu=1500 l2mtu=1522
address=[redacted]
Το interface αυτό χρησιμοποιείται για την σύνδεση του router με το δίκτυο των Access Points.

name="4_SERVER" type="ether" mtu=1500 l2mtu=1522
address=[redacted]
Το interface αυτό χρησιμοποιείται για την σύνδεση του router με το δίκτυο του server που λειτουργεί.

name="5_NS5-AWMN" type="ether" mtu=1500 l2mtu=1522
address=[redacted]
Το interface αυτό χρησιμοποιείται για την σύνδεση του router με το δίκτυο του AWMN (Athens Wireless Metropolitan Network) στο οποίο υπάρχει πρόσβαση.

2.5.2 PoE Switches

Για να μην γίνει πολύπλοκη η εγκατάσταση και κατά συνέπεια η συντήρηση του δικτύου, για την τροφοδοσία των Access Points προτιμήθηκε η λύση της PoE τροφοδοσίας τους μέσω των ανάλογων switch.

Εικόνα 2-7 - Τα **Power Over Ethernet switches** του δικτύου

2.5.3 Access Points

Εικόνα 2-8 – Access Point TP-Link TL-WR543G

Για την κάλυψη όλων των χώρων του κτιρίου, τοποθετήθηκαν επτά Access Points, για τα οποία εγκαταστάθηκαν νέα καλώδια UTP Cat5e στους εξής χώρους.

Δύο τοποθετήθηκαν στο ισόγειο. Το ένα τοποθετήθηκε στον διάδρομο, ανάμεσα από τις δύο μεγάλες αίθουσες, με σκοπό την κάλυψη τους. Το δεύτερο Access Point του ισογείου τοποθετήθηκε στον χώρο του κυλικείου.

Ένα Access Point τοποθετήθηκε στον πρώτο όροφο και περίπου στο σημείο που βρισκόμαστε μόλις ανέβουμε τις σκάλες. Το Access Point αυτό έχει σκοπό να καλύψει τον

ακάλυπτο χώρο του πρώτου ορόφου, καθώς και τα κενά που μένουν στον δεύτερο όροφο αλλά και στο ισόγειο στο συγκεκριμένο σημείο.

Δύο ακόμα Access Point τοποθετήθηκαν στον δεύτερο όροφο. Το ένα βρίσκεται, στον ακάλυπτο, στο αντίστοιχο ακάλυπτο σημείο, πάνω ακριβώς από τον χώρο του κυλικείου. Το δεύτερο βρίσκεται έξω από το εργαστήριο των δικτύων, με σκοπό να καλύψει τα κενά του δευτέρου ορόφου αλλά και του πρώτο στο συγκεκριμένο σημείο.

Εικόνα 2-9 - Nanostation 5 M5

Το έκτο Access Point, είναι εξωτερικού χώρου και βρίσκεται στον χώρο της ταράτσας και καλύπτει τον προαύλιο χώρο, έξω από το κτίριο καθώς και τους εξωτερικούς χώρους του μεγάλου κυλικείου. Σε μετρήσεις που πραγματοποιήσαμε, είδαμε ότι το συγκεκριμένο Access Point, καλύπτει και ένα μέρος της νέας βιβλιοθήκης, στον δεύτερο όροφο, στο αναγνωστήριο.

Τέλος, έχει τοποθετηθεί και ένα Access Point το οποίο μας επιτρέπει την σύνδεση με το AWMN (Athens Wireless Metropolitan Network).

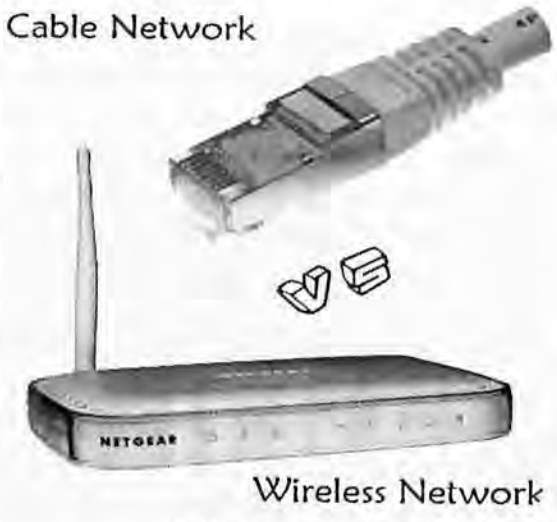
Για τα δύο Access Point που έχουν τοποθετηθεί στην ταράτσα, έχει τοποθετηθεί ειδικού τύπου καλώδιο FTP με προδιαγραφές για εξωτερικό χώρο, ώστε να αντέξει τις καιρικές συνθήκες.

2.5.4 Σύγκριση LAN – WALN

Σε σχέση με τα ενσύρματα τοπικά δίκτυα (Local Area Networks - LANs) τα WLANs παρουσιάζουν πλεονεκτήματα αλλά και αρκετούς περιορισμούς, που προσδιορίζουν σε μεγάλο βαθμό τον τρόπο χρήσης τους. Στη συνέχεια αναφέρονται τα βασικότερα πλεονεκτήματά τους:

- *Κινητικότητα (Mobility) χρηστών:* Το προφανέστερο πλεονέκτημα που προσφέρει ένα WLAN. Για να το εκμεταλλευτεί ο χρήστης πρέπει φυσικά να διαθέτει το αντίστοιχο κινητό τερματικό

- *Ευκολία και ταχύτητα εγκατάστασης:* Σε αντίθεση με τα ενσύρματα δίκτυα δεν απαιτούνται μεγάλες παρεμβάσεις στην περιοχή λειτουργίας, όπως είναι η εγκατάσταση καλωδιώσεων.



Εικόνα 2-10 - Σύγκριση LAN - WALN

- *Ευελιξία και επεκτασιμότητα:* Τα ασύρματα δίκτυα μπορούν να επεκταθούν εύκολα, εφόσον το μέσο μετάδοσης που χρησιμοποιούν είναι παντού διαθέσιμο. Επίσης μπορούν να προσαρμοστούν σε διάφορες ανάγκες των χρηστών τους, ανάλογα με την περίσταση.

- *Κόστος:* Σε μερικές περιπτώσεις η λύση του WLAN είναι φτηνότερη από το παραδοσιακό LAN. Μία τέτοια περίπτωση είναι η χρήση ασύρματου εξοπλισμού για μία ζεύξη σημείο - προς - σημείο (point - to - point) ανάμεσα σε δύο κτίρια, αντί της μίσθωσης κάποιας μόνιμης γραμμής. Όσο η τεχνολογία αυτή εξελίσσεται, εμφανίζονται νέα προϊόντα που προσφέρουν καλύτερες επιδόσεις με μικρότερο κόστος.

Φυσικά υπάρχουν και διάφοροι περιορισμοί στην εγκατάσταση και λειτουργία των ασυρμάτων δικτύων που δεν συναντώνται στα ενσύρματα. Οι βασικότεροι περιορισμοί είναι οι εξής:

- *Κατανάλωση ισχύος:* Για να εκμεταλλευτούν οι χρήστες την κινητικότητα που τους προσφέρει το ασύρματο δίκτυο πρέπει να χρησιμοποιούν κινητούς σταθμούς (mobile stations). Αυτοί λειτουργούν με μπαταρίες και ο σχεδιασμός του δικτύου πρέπει να τους επιτρέπει όσο το δυνατόν μεγαλύτερη αυτονομία.

- *Διέλευση:* Ιδανικά η διέλευση των ασύρματων δικτύων θα έπρεπε να είναι περίπου ίση με τη διέλευση των ενσύρματων. Αυτό δε συμβαίνει στην πράξη, λόγω περιορισμών που επιβάλλει η ασύρματη μετάδοση. Αν και έχει παρατηρηθεί αρκετά μεγάλη αύξηση των ρυθμών μετάδοσης, η διαφορά είναι ακόμα μεγάλη. Το πρωτόκολλο πρόσβασης στο μέσο του ασυρμάτου δικτύου πρέπει να φροντίζει για την επίτευξη μέγιστης διέλευσης στο δίκτυο.

- *Παρεμβολές και αξιοπιστία:* Όπως σε κάθε ασύρματη μορφή μετάδοσης, έτσι και στην περίπτωση των ασυρμάτων δικτύων τίθενται τα ζητήματα των παρεμβολών και της αξιοπιστίας. Παρεμβολές μπορεί να προέρχονται από τους ίδιους τους σταθμούς του δικτύου στην προσπάθειά τους να μεταδώσουν ταυτόχρονα. Επίσης μπορεί να προέρχονται από άλλες συσκευές που χρησιμοποιούν το ίδιο φασματικό εύρος, ιδίως στην περίπτωση χρήσης ελεύθερων φασματικών μπάντων όπως η ISM. Τέλος, πηγή παρεμβολών είναι το φαινόμενο των διαλείψεων πολλαπλών διαδρομών. Τα παραπάνω πρέπει να αντιμετωπιστούν με χρήση κατάλληλων τεχνικών διαμόρφωσης, κωδικοποίησης και διόρθωσης λαθών.

- *Ασφάλεια επικοινωνιών:* Δεδομένα που κυκλοφορούν σε ένα ασύρματο δίκτυο είναι εύκολο να υποκλαπούν από οποιονδήποτε, αρκεί να διαθέτει τον κατάλληλο δέκτη και πρόσβαση στην περιοχή κάλυψης του δικτύου. Γι' αυτόν το λόγο πρέπει να χρησιμοποιείται κάποια μέθοδος κρυπτογράφησης των εκπεμπόμενων δεδομένων, κάτι που αυξάνει το κόστος και μειώνει την επίδοση του τελικού συστήματος.

- *Υποστήριξη κινητικότητας:* Το ασύρματο δίκτυο πρέπει να υποστηρίζει την διαπομπή και τη δρομολόγηση της κίνησης σε κινούμενους χρήστες. Αυτό προσθέτει πολυπλοκότητα στη σχεδίασή του.

- *Κατανομή συχνοτήτων:* Πρέπει να βρεθούν οι φασματικές περιοχές στις οποίες θα λειτουργούν τα διάφορα ασύρματα δίκτυα. Αυτό μπορεί να είναι αρκετά δύσκολο, ιδίως όταν στη διαδικασία εμπλέκονται ρυθμιστικές αρχές διαφόρων χωρών.

- *Ασφάλεια χρηστών:* Η ασφάλεια των χρηστών κατά τη χρήση κάθε είδους ασύρματων συσκευών είναι ένα θέμα που μελετάται διαρκώς. Στα ασύρματα δίκτυα ένας από τους λόγους περιορισμού της εκπεμπόμενης ισχύος είναι η προστασία των χρηστών.

3 ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

3.1 ΙΣΤΟΡΙΑ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

Τα ασύρματα τοπικά δίκτυα (Wireless Local Networks – WLANs) είναι μία σχετικά νέα μορφή τοπικών δικτύων, που επιτρέπει στους χρήστες να συνδέονται και να ανταλλάσσουν πληροφορία, χωρίς να δεσμεύονται από την ύπαρξη κατάλληλης καλωδίωσης. Η προσφορά κινητικότητας στους χρήστες είναι το κύριο χαρακτηριστικό που διαφοροποιεί τα ασύρματα από τα ενσύρματα δίκτυα. Οι πρώτες προσπάθειες για τη δημιουργία ενός WLAN έγιναν στα τέλη της δεκαετίας του 1970 από τον Fritz R. Gfeller στα IBM Ruschlikon Laboratories στην Ελβετία. Χρησιμοποιήθηκε η τεχνολογία των υπέρυθρων ακτινών (Infrared – IR), αλλά το σχέδιο εγκαταλείφθηκε, διότι δεν ήταν εφικτή η επίτευξη του επιθυμητού ρυθμού μετάδοσης 1 Mbps μέσα σε μια λογική περιοχή κάλυψης. Στη συνέχεια έγιναν κι άλλες απόπειρες με χρήση ραδιοκυμάτων στα 900 MHz (Ferrert, HP Palo Alto Research Laboratories, 1980) και λίγο αργότερα στα 1,73 GHz (Motorola), αλλά απέτυχαν λόγω της πολυπλοκότητας των σχεδίων και της αδυναμίας εξασφάλισης μόνιμης άδειας χρήσης φάσματος από την FCC (Federal Communications Commission).

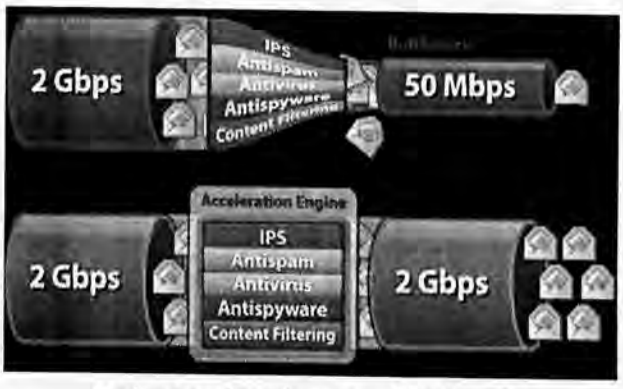
Τα τελευταία χρόνια η κατάσταση στο χώρο των ασυρμάτων δικτύων είναι πολύ διαφορετική. Υπάρχει ένας αριθμός ασυρμάτων δικτύων που λειτουργούν στις ISM (Industrial, Scientific, Medical) μπάντες. Τέτοια δίκτυα

είναι το FreePort και το WaveLAN. Το FreePort παρέχει ένα ασύρματο Ethernet (IEEE 802.3) και λειτουργεί στις ζώνες 2400 – 2483 MHz για εκπομπή και 5725 – 5850 MHz για λήψη. Το WaveLAN παρέχει άμεση επικοινωνία (peer – to – peer) και λειτουργεί στη ζώνη 902 – 928 MHz στις ΗΠΑ και στη ζώνη 2400 – 2480 MHz σε άλλες 39 χώρες. Υπάρχει επίσης και το σύστημα Altair, που χρησιμοποιεί το πρωτόκολλο Ethernet (IEEE802.3) και λειτουργεί στην μικροκυματική περιοχή συχνοτήτων των 18 GHz.

3.2 ΑΡΧΗ ΛΕΙΤΟΥΡΓΙΑΣ ΤΩΝ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

3.2.1 Η μεταφορά δεδομένων

Η μεταφορά δεδομένων μέσω ασύρματου δικτύου περιλαμβάνει τρία ξεχωριστά στοιχεία: τα ραδιοσήματα, τη μορφή των δεδομένων, και τη δομή του δικτύου. Καθένα από αυτά τα στοιχεία είναι ανεξάρτητο από τα άλλα δύο, άρα πρέπει να ορίσετε και τα τρία όταν επινοείτε ένα καινούργιο δίκτυο. Στο μοντέλο αναφοράς OSI, το ραδιοσήμα λειτουργεί στο φυσικό επίπεδο, και η μορφή των δεδομένων ελέγχει πολλά από τα υψηλότερα επίπεδα. Η δομή του δικτύου περιλαμβάνει τους ασύρματους προσαρμογείς διασύνδεσης δικτύου (network interface adapters) και τους σταθμούς βάσης (base stations) που στέλνουν και λαμβάνουν τα ραδιοσήματα. Στα ασύρματα δίκτυα, οι προσαρμογείς διασύνδεσης δικτύου σε κάθε υπολογιστή και σταθμό βάσης μετατρέπουν τα ψηφιακά δεδομένα σε ραδιοσήματα, τα οποία και μεταδίδουν σε άλλες συσκευές του ίδιου δικτύου, και λαμβάνουν και μετατρέπουν ξανά τα εισερχόμενα ραδιοσήματα από άλλα στοιχεία του δικτύου σε ψηφιακά δεδομένα.



Εικόνα 3-1 – Απεικόνιση του "Bottleneck"

Κάθε μία από τις ευρυζωνικές ασύρματες υπηρεσίες δεδομένων κάνει χρήση ενός διαφορετικού συνδυασμού από ραδιοσήματα, μορφές δεδομένων, και δομών δικτύου. Θα περιγράψουμε κάθε τύπο ασύρματου δικτύου δεδομένων με περισσότερες λεπτομέρειες αργότερα σε αυτό το κεφάλαιο, αλλά πρώτα είναι πολύ χρήσιμο να κατανοήσουμε μερικές γενικές αρχές.

3.2.2 Ραδιοκύματα

Οι βασικοί φυσικοί νόμοι που καθιστούν εφικτά τα ραδιοκύματα είναι γνωστοί ως εξισώσεις του Maxwell και καθορίστηκαν από τον James Clark Maxwell το 1864. Χωρίς να υπεισέλθουμε στα μαθηματικά, οι εξισώσεις του Maxwell δείχνουν ότι ένα μεταβαλλόμενο μαγνητικό πεδίο παράγει ηλεκτρικό πεδίο, και ένα μεταβαλλόμενο ηλεκτρικό πεδίο παράγει ένα μαγνητικό πεδίο. Όταν το εναλλασσόμενο ρεύμα (AC) κινείται μέσω ενός σύρματος ή άλλου φυσικού αγωγού, ένα μέρος της ενέργειας διαφεύγει στον περιβάλλοντα χώρο ως εναλλασσόμενο μαγνητικό πεδίο. Το συγκεκριμένο μαγνητικό πεδίο δημιουργεί ένα εναλλασσόμενο ηλεκτρικό πεδίο στο χώρο, το οποίο με τη σειρά του δημιουργεί ένα ακόμη μαγνητικό πεδίο και ούτω καθεξής, μέχρι να διακοπεί το αρχικό ρεύμα.

Αυτή η μεταβατική μορφή ενέργειας μεταξύ ηλεκτρικής και μαγνητικής ενέργειας ονομάζεται ηλεκτρομαγνητική ακτινοβολία ή ραδιοκύματα (radio waves). Τα ραδιοκύματα ορίζονται ως η ακτινοβολία της ηλεκτρομαγνητικής ενέργειας μέσα στο χώρο. Μια συσκευή που παράγει ραδιοκύματα ονομάζεται πομπός (transmitter), και η συμπληρωματική συσκευή που ανιχνεύει ραδιοκύματα στον αέρα και τα μετατρέπει σε κάποια άλλη μορφή ενέργειας ονομάζεται δέκτης (receiver). Τόσο οι πομποί όσο και οι δέκτες χρησιμοποιούν συσκευές με ειδικό σχήμα που ονομάζονται κεραίες (antennas) για να εστιάσουν το ραδιοσήμα σε μια συγκεκριμένη κατεύθυνση, ή μοτίβο (pattern), και για να αυξήσουν την ποσότητα της πραγματικής ακτινοβολίας (από κάποιο πομπό) ή της ευαισθησίας (σε κάποιο δέκτη).

Αν ρυθμίσουμε το ρυθμό με τον οποίο το εναλλασσόμενο ρεύμα ρέει από κάθε πομπό μέσω της κεραίας προς τα έξω στο χώρο (τη συχνότητα — frequency), και ρυθμίσουμε το δέκτη ώστε να λειτουργεί μόνο στη συγκεκριμένη συχνότητα, είναι δυνατή η αποστολή και η λήψη πολλών διαφορετικών σημάτων, το καθένα σε διαφορετική συχνότητα, τα οποία δεν παρεμβάλλονται μεταξύ τους. Το συνολικό εύρος των συχνοτήτων είναι γνωστό ως *ραδιοφάσμα* (radio spectrum). Ένα μικρότερο τμήμα του ραδιοφάσματος ονομάζεται συχνά *ζώνη* (band).

Οι ραδιοσυχνότητες, καθώς και άλλα σήματα AC εκφράζονται σε κύκλους ανα δευτερόλεπτο, ή *χερτζ* (hertz, Hz), από το όνομα του Heinrich Hertz, του πρώτου πειραματιστή που εξέπεμψε και έλαβε ραδιοκύματα. Ο κύκλος είναι η απόσταση από μία κορυφή (peak) ενός σήματος AC μέχρι την κορυφή του επόμενου σήματος. Τα ραδιοσήματα λειτουργούν γενικά σε συχνότητες χιλιάδων, εκατομμυρίων, ή δισεκατομμυρίων hertz (kilohertz ή KHz, megahertz ή MHz, και gigahertz ή GHz, αντίστοιχα).

Ο απλούστερος τύπος ραδιοεπικοινωνίας χρησιμοποιεί ένα συνεχές σήμα το οποίο ο χειριστής του πομπού διακόπτει για να το διαιρέσει σε αποδεκτές

αλληλουχίες σημάτων μεγάλης και μικρής διάρκειας (τελείες και παύλες) που αντιστοιχούν σε διαφορετικά γράμματα και άλλους χαρακτήρες. Το σύνολο αυτών των αλληλουχιών που χρησιμοποιήθηκε περισσότερο ήταν ο κώδικας Μορς, ο οποίος πήρε το όνομα του από τον εφευρέτη του τηλεγράφου, τον Samuel G. B. Morse, όπου χρησιμοποιήθηκε για πρώτη φορά αυτός ο κώδικας.

Για τη μετάδοση ομιλίας, μουσικής, και άλλων ήχων μέσω ραδιοκυμάτων, ο πομπός μεταβάλλει ή *διαμορφώνει* (modulates) το σήμα AC (το φέρον σήμα — carrier) είτε συνδυάζοντας ένα ηχητικό σήμα με το φέρον, (αυτό ονομάζεται *διαμόρφωση πλάτους* — amplitude modulation, AM), ή διαμορφώνοντας τη συχνότητα μέσα σε μικρό εύρος, (αυτό ονομάζεται *διαμόρφωση συχνότητας* — frequency modulation, FM). Ο δέκτης AM ή FM περιλαμβάνει ένα συμπληρωματικό κύκλωμα που διαχωρίζει το φέρον σήμα από το σήμα διαμόρφωσης (modulating signal).

Επειδή δύο ή περισσότερα ραδιοσήματα που χρησιμοποιούν την ίδια συχνότητα συχνά παρεμβάλλονται μεταξύ τους, οι κυβερνητικές ρυθμιστικές αρχές και οι διεθνείς οργανισμοί, όπως η Διεθνής Ένωση Τηλεπικοινωνιών (International Telecommunication Union — ITU), έχουν δεσμεύσει ορισμένες συχνότητες για συγκεκριμένους τύπους διαμόρφωσης, και χορηγούν αποκλειστικές άδειες σε διαφορετικούς χρήστες. Για παράδειγμα, ένας ραδιοφωνικός σταθμός FM μπορεί να έχει άδεια λειτουργίας στα 92,1 MHz σε ορισμένη γεωγραφική τοποθεσία. Δεν επιτρέπεται σε κανέναν άλλο να χρησιμοποιεί τη συγκεκριμένη συχνότητα αρκετά κοντά ώστε να παρεμβληθεί στο συγκεκριμένο σήμα. Από την άλλη πλευρά, κάποιες υπηρεσίες ραδιοκυμάτων δεν απαιτούν άδεια χρήσης. Οι περισσότερες απαλλασσόμενες από άδεια χρήσης υπηρεσίες είναι είτε περιορισμένες σε πολύ μικρές αποστάσεις, είτε σε συγκεκριμένες ζώνες συχνοτήτων (frequency bands), είτε και στα. δύο.

Οι διαμορφώσεις AM και FM είναι αναλογικές μέθοδοι, επειδή το σήμα που εξέρχεται από το δέκτη (receiver) αποτελεί αντίγραφο του σήματος που εισήλθε στον πομπό (transmitter). Όταν στέλνουμε δεδομένα υπολογιστών μέσω συνδέσμου ραδιοκυμάτων, αυτά είναι ψηφιακά επειδή το περιεχόμενο έχει μετατραπεί από κείμενο, κώδικα υπολογιστή, ήχο, εικόνες, ή άλλες πληροφορίες σε μονάδες και μηδενικά πριν από τη μετάδοση του, και μετατρέπεται ξανά στην αρχική του μορφή μετά από τη λήψη του. Τα ψηφιακά ραδιοκύματα μπορούν να χρησιμοποιούν οποιαδήποτε από αρκετές διαφορετικές μεθόδους διαμόρφωσης: οι μονάδες και τα μηδενικά μπορούν να είναι δύο διαφορετικοί ηχητικοί τόνοι, δύο διαφορετικές ραδιοσυχνότητες, χρονισμένες διακοπές του φέροντος σήματος, ή κάποιος συνδυασμός αυτών και άλλων τεχνικών.

3.2.3 Ασύρματα δίκτυα δεδομένων

Κάθε τύπος ασύρματου δικτύου δεδομένων λειτουργεί σε συγκεκριμένο σύνολο ραδιοσυχνοτήτων. Για παράδειγμα, τα περισσότερα δίκτυα Wi-Fi λειτουργούν σε μια ειδική ζώνη ραδιοσυχνοτήτων γύρω στα 2,4 GHz, η οποία έχει δεσμευτεί στα περισσότερα μέρη του κόσμου για απαλλασσόμενες από άδεια χρήσης ραδιοϋπηρεσίες εξάπλωσης φάσματος από σημείο σε σημείο (point-to-point spread spectrum radio services). Άλλα συστήματα Wi-Fi κάνουν χρήση διαφορετικής απαλλασσόμενης από άδεια χρήσης ζώνης γύρω στα 5 GHz.

3.2.3.1 Υπηρεσίες ραδιοκυμάτων απαλλασσόμενες από άδεια χρήσης

Απαλλασσόμενες από άδεια χρήσης σημαίνει ότι όλοι όσοι χρησιμοποιούν εξοπλισμό που συμμορφώνεται με τις τεχνικές απαιτήσεις μπορούν να στείλουν και να λάβουν ραδιοσήματα σε αυτές τις συχνότητες χωρίς άδεια χρήσης ραδιοσταθμού. Σε αντίθεση με τις περισσότερες υπηρεσίες ραδιοκυμάτων (μεταξύ των οποίων και άλλες ευρυζω-νικές ασύρματες υπηρεσίες), οι οποίες απαιτούν άδειες χρήσης που παρέχουν αποκλειστική χρήση της συγκεκριμένης συχνότητας σε συγκεκριμένο τύπο υπηρεσίας και σε έναν ή περισσότερους συγκεκριμένους χρήστες, οι απαλλασσόμενες από άδεια χρήσης υπηρεσίες είναι δωρεάν για όλους, όπου οι πάντες έχουν ισοδύναμες αξιώσεις στα ίδια κύματα, Θεωρητικά, η τεχνολογία των ραδιοκυμάτων εξάπλωσης φάσματος κάνει εφικτή τη συνύπαρξη πολλών χρηστών (μέχρι ένα σημείο) χωρίς σημαντικές παρεμβολές.

3.2.3.2 Από σημείο σε σημείο

Μια υπηρεσία ραδιοκυμάτων από σημείο σε σημείο (point-to-point) χειρίζεται ένα κανάλι επικοινωνίας που μεταφέρει πληροφορίες από έναν πομπό σε ένα μόνο δέκτη. Στο δίκτυο μας, χρησιμοποιήσαμε την συγκεκριμένη τεχνολογία, για την ζεύξη, με το awmn. Το αντίθετο της υπηρεσίας από σημείο σε σημείο είναι η υπηρεσία εκπομπής (broadcast) όπως οι ραδιοφωνικοί ή τηλεοπτικοί σταθμοί, η οποία στέλνει το ίδιο σήμα σε πολλούς παραλήπτες ταυτόχρονα.

3.2.3.3 Εξάπλωση φάσματος

Η εξάπλωση φάσματος (spread spectrum) αποτελεί μια οικογένεια μεθόδων για τη μετάδοση ενός ραδιοσήματος με τη χρήση ενός σχετικά

μεγάλου εύρους τμήματος του ραδιοφάσματος. Τα ασύρματα δίκτυα Ethernet χρησιμοποιούν αρκετά διαφορετικά συστήματα ραδιομετάδοσης εξάπλωσης φάσματος, τα οποία ονομάζονται εξάπλωση φάσματος με συνεχή αλλαγή συχνότητας (frequency-hopping spread spectrum — FHSS), εξάπλωση φάσματος με άμεση ακολουθία (direct-sequence spread spectrum — DSSS), και ορθογωνική πολύπλεξη με διαίρεση συχνότητας (orthogonal frequency division multiplexing — OFDM). Κάποια παλαιότερα δίκτυα δεδομένων κάνουν χρήση του πιο αργού συστήματος FHSS, αλλά τα πρώτα δίκτυα Wi-Fi χρησιμοποίησαν το σύστημα DSSS και τα πιο πρόσφατα συστήματα χρησιμοποιούν το σύστημα OFDM. Στον Πίνακα 2.1 φαίνονται όλα τα πρότυπα Wi-Fi και ο τύπος διαμόρφωσης εξάπλωσης φάσματος που χρησιμοποιούν.

Τύπος Wi-Fi	Συχνότητα	Διαμόρφωση
802.11a	5 GHz	OFDM
802.11b	2,4 GHz	DSSS
802.11g	2,4 GHz	OFDM

Πρότυπα Wi-Fi και τύπος διαμόρφωσης

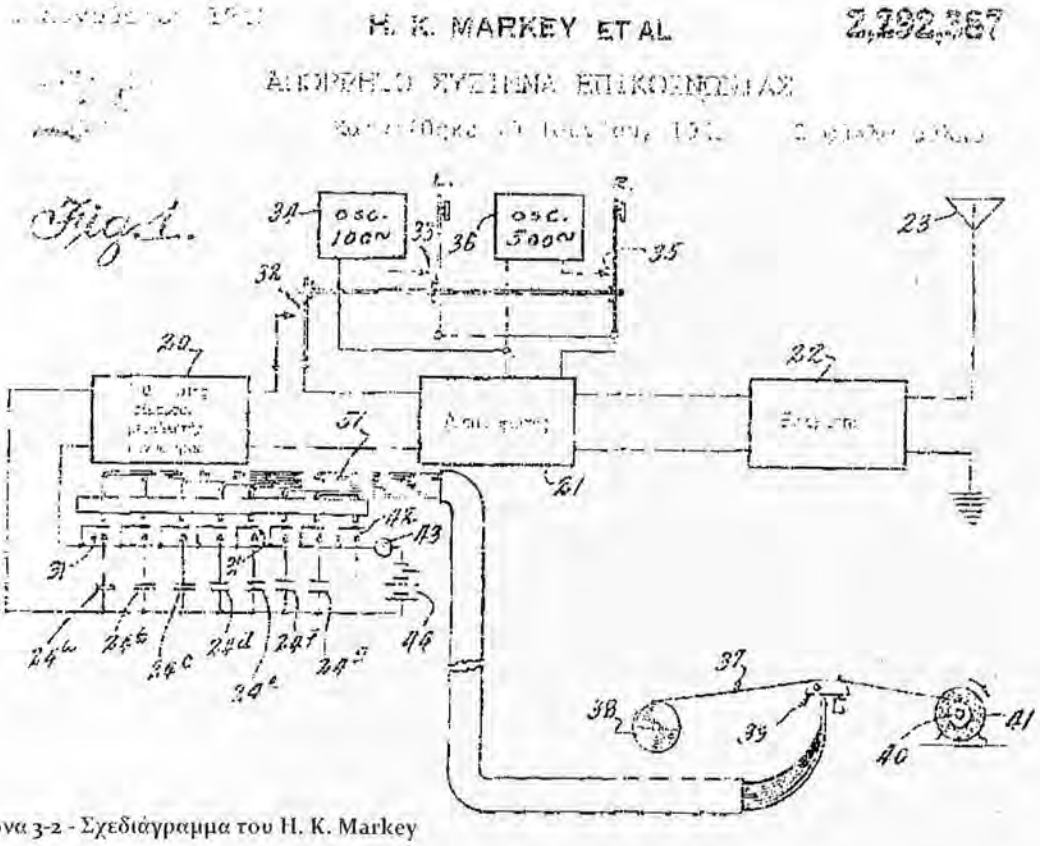
Τα ραδιοκύματα εξάπλωσης φάσματος προσφέρουν μερικά σημαντικά πλεονεκτήματα σε σχέση με τους υπόλοιπους τύπους ραδιοσημάτων, οι οποίοι χρησιμοποιούν ένα μόνο στενό κανάλι. Η εξάπλωση φάσματος είναι εξαιρετικά αποδοτική, οπότε οι ραδιοπομποί μπορούν να λειτουργήσουν με πολύ χαμηλή ισχύ. Επειδή τα σήματα λειτουργούν σε σχετικά ευρεία ζώνη συχνοτήτων, είναι λιγότερα ευαίσθητα σε παρεμβολές από άλλα ραδιοσήματα και ηλεκτρικό θόρυβο, γεγονός που σημαίνει ότι μπορούν συχνά να διέρχονται από περιβάλλοντα όπου η λήψη και η κατανόηση ενός συμβατικού σήματος στενής ζώνης (narrow-band) θα ήταν αδύνατες. Και επειδή το σήμα εξάπλωσης φάσματος με συνεχή αλλαγή συχνότητας μετατοπίζεται σε περισσότερα από ένα κανάλια, μπορεί να είναι εξαιρετικά δύσκολο για κάποιο μη εξουσιοδοτημένο ακροατή να συλλάβει και να αποκωδικοποιήσει τα περιεχόμενα ενός σήματος.

Η τεχνολογία εξάπλωσης φάσματος έχει ενδιαφέρουσα ιστορία. Επινοήθηκε από την ηθοποιό Hedy Lamarr και τον πρωτοποριακό Αμερικανό συνθέτη George Antheil ως ένα «απόρρητο σύστημα επικοινωνίας» για το σύστημα κατεύθυνσης ραδιο-ελεγχόμενων τορπιλών, το οποίο δε θα ήταν ευάλωτο στις εχθρικές παρεμβολές. Προτού έρθει στο Χόλυγουντ, η Lamarr είχε παντρευτεί με έναν έμπορο όπλων στην Αυστρία, όπου έμαθε για τα

προβλήματα των συστημάτων κατεύθυνσης των τορπιλών σε βραδινές συγκεντρώσεις φαγητού με τους πελάτες του συζύγου της. Χρόνια αργότερα, λίγο πριν οι Ηνωμένες Πολιτείες μπουν στο Δεύτερο Παγκόσμιο Πόλεμο, διατύπωσε την έννοια της αλλαγής των ραδιοσυχνοτήτων για την αντίσταση στις παρεμβολές. Οι Τάιμς της Νέας Υόρκης ανέφεραν το 1941 ότι η «ολοκαίνουργια» εφεύρεση της ήταν ζωτική για την εθνική άμυνα, αλλά η κυβέρνηση δεν αποκάλυπτε λεπτομέρειες.

Ο Antheil αποδείχθηκε το ιδανικό άτομο για να εφαρμόσει αυτή την ιδέα στην πράξη. Η πιο γνωστή σύνθεση του ήταν μια εξτραβαγκάντσα που ονομάζεται Ballet Mechanique (Μηχανική Μπαλέτου), μια σύνθεση για δεκάξι πιανόλες, δύο έλικες αεροπλάνου, τέσσερα ξυλόφωνα, τέσσερις γρανκάσες, και μία σειρήνα. Χρησιμοποίησε στη σχεδίαση του το ίδιο είδους μηχανισμού που είχε χρησιμοποιήσει παλαιότερα για να συγχρονίσει τις πιανόλες ώστε να αλλάζουν τις ραδιοσυχνότητες σε μια μετάδοση εξάπλωσης φάσματος. Το αρχικό σύστημα χαρτοταινιών διέθετε 88 διαφορετικά κανάλια ραδιοκυμάτων, ένα για καθένα από τα 88 πλήκτρα του πιάνου.

Θεωρητικά, η ίδια μέθοδος θα μπορούσε να χρησιμοποιηθεί για επικοινωνία φωνής και δεδομένων, καθώς επίσης και για τα συστήματα κατεύθυνσης των τορπιλών, αλλά την περίοδο των λυχνιών κενού, των χαρτοταινιών, και του μηχανικού συγχρονισμού, ολόκληρη η διαδικασία ήταν υπερβολικά πολύπλοκη για να κατασκευαστεί και να χρησιμοποιηθεί πραγματικά.



Εικόνα 3-2 - Σχεδιάγραμμα του H. K. Markey

Η Hedy Lamarr και ο George Antheil έλαβαν αυτό το δίπλωμα ευρεσιτεχνίας το 1942 για την εφεύρεση που έγινε η βάση για τη ραδιοεπικοινωνία εξάπλωσης φάσματος. Εδώ, της απονέμεται με το επώνυμο του συζύγου της, του H. K. Markey. (solid-state electronics) είχαν αντικαταστήσει τις λυχνίες κενού και τα ρολά χαρτιού των πιάνων, και η τεχνολογία χρησιμοποιούνταν στα πλοία του Ναυτικού των Η.Π.Α. για ασφαλή επικοινωνία κατά τη διάρκεια της κρίσης των πυραύλων στην Κούβα. Σήμερα, οι ασύρματοι εξάπλωσης φάσματος χρησιμοποιούνται στο Σύστημα Δορυφορικών Επικοινωνιών Milstar (Milstar Satellite Communications Systems) της Διοίκησης Διαστήματος (Space Command) της Αεροπορίας των Η.Π.Α, σε ψηφιακά κινητά τηλέφωνα, και σε ασύρματα δίκτυα δεδομένων.

3.2.3.4 Εξάπλωση φάσματος με συνεχή αλλαγή συχνότητας

Το αρχικό σχέδιο των Lamarr και Antheil για τα ραδιοκύματα εξάπλωσης φάσματος χρησιμοποιούσε ένα σύστημα συνεχούς αλλαγής συχνότητας (frequency-hopping system — FHSS). Όπως δείχνει το όνομα, η τεχνολογία FHSS διαιρεί το ραδιοσήμα σε μικρά τμήματα και αλλάζει από τη μια συχνότητα στην άλλη πολλές φορές το δευτερόλεπτο καθώς μεταδίδει αυτά τα τμήματα. Ο πομπός και ο δέκτης εγκαθιστούν ένα συγχρονισμένο μοτίβο

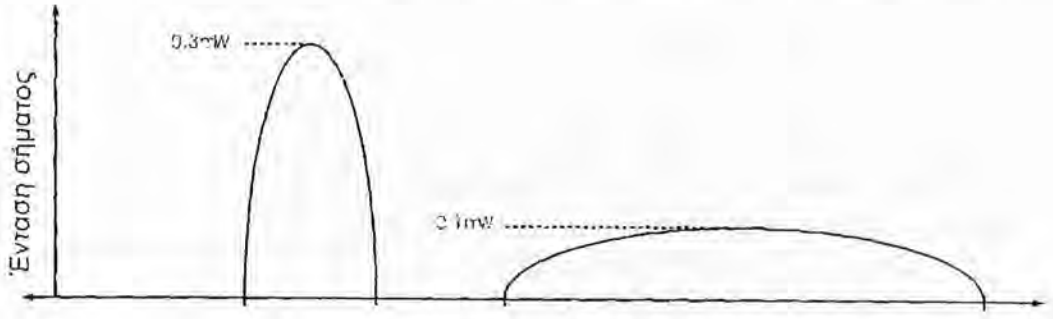
συνεχούς αλλαγής, το οποίο ρυθμίζει την ακολουθία με την οποία θα χρησιμοποιήσουν τα διαφορετικά υποκανάλια.

Τα συστήματα FHSS αντιμετωπίζουν επιτυχώς τις παρεμβολές από άλλους χρήστες με τη χρήση ενός στενού φέροντος σήματος (narrow carrier signal) που αλλάζει συχνότητα πολλές φορές το δευτερόλεπτο. Επιπλέον ζεύγη πομπού και δέκτη μπορούν να χρησιμοποιήσουν ταυτόχρονα διαφορετικά μοτίβα συνεχούς αλλαγής στο ίδιο σύνολο υποκαναλιών. Σε οποιαδήποτε χρονική στιγμή, κάθε μετάδοση χρησιμοποιεί πιθανόν διαφορετικό υποκανάλι, οπότε δεν υπάρχει παρεμβολή μεταξύ των σημάτων. Όταν σημειωθεί μια σύγκρουση, το σύστημα στέλνει ξανά το ίδιο πακέτο μέχρι ο δέκτης να λάβει ένα καθαρό αντίγραφο και να επιστρέψει μια επιβεβαίωση στο σταθμό μετάδοσης.

Για μερικές παλαιότερες ασύρματες υπηρεσίες δεδομένων με πρωτόκολλο 802.11, η απαλλασσόμενη από άδεια χρήσης ζώνη των 2,4 MHz διαιρείται σε 75 υποκανάλια, καθένα από τα οποία έχει εύρος 1 MHz. Επειδή κάθε αλλαγή συχνότητας προσθέτει επιβάρυνση στο ρεύμα των δεδομένων, οι μεταδόσεις FHSS είναι σχετικά αργές.

3.2.3.5 Εξάπλωση φάσματος με άμεση ακολουθία

Η τεχνολογία εξάπλωσης φάσματος με άμεση ακολουθία (direct-sequence spread spectrum, DSSS) που ελέγχει τα δίκτυα τύπου 802.1 1b, χρησιμοποιεί μια ακολουθία Barker (Barker sequence) 11 τεμαχίων (chips) για να εξαπλώσει το ραδιοσήμα μέσω ενός καναλιού με εύρος 22 MHz, χωρίς αλλαγή συχνοτήτων. Κάθε σύνδεσμος DSSS χρησιμοποιεί ένα μόνο κανάλι χωρίς καμία αλλαγή συχνότητας. Όπως φαίνεται στην Εικόνα 2.5, μια μετάδοση DSSS χρησιμοποιεί περισσότερο εύρος ζώνης (bandwidth), αλλά λιγότερη ισχύ από ένα συμβατικό σήμα. Το ψηφιακό σήμα στο αριστερό μέρος είναι μια συμβατική μετάδοση, στην οποία η ισχύς έχει συγκεντρωθεί σε περιορισμένο εύρος ζώνης. Το σήμα DSSS στο δεξιό μέρος χρησιμοποιεί την ίδια ποσότητα ισχύος, αλλά εξαπλώνει αυτή την ισχύ σε ευρύτερη ζώνη ραδιοσυχνοτήτων. Προφανώς, το κανάλι DSSS των 22 MHZ έχει πολύ μεγαλύτερο εύρος από τα κανάλια του 1 MHz που χρησιμοποιούνται στα συστήματα FHSS.



Εικόνα 3-3 - Ένα συμβατικό σήμα (αριστερά) χρησιμοποιεί μικρό εύρος ζώνης ραδιοσυχνοτήτων. Ένα σήμα DSSS (δεξιά) χρησιμοποιεί μεγαλύτερο εύρος ζώνης αλλά λιγότερο ισχυρό σήμα.

Οι πομποί DSSS διαχωρίζουν κάθε bit στο αρχικό ρεύμα δεδομένων σε μια σειρά από πλεονάζοντα μοτίβα bit, τα οποία ονομάζονται τεμάχια (chips), και τους μεταδίδουν σε κάποιο δέκτη που επανασυναρμολογεί (reassembles) τα τεμάχια σε ρεύμα δεδομένων πανομοιότυπο με το αρχικό. Επειδή οι περισσότερες παρεμβολές είναι πιθανόν να καταλαμβάνουν στενότερο εύρος ζώνης από κάποιο σήμα DSSS, και επειδή κάθε bit διαιρείται σε αρκετά τεμάχια, ο δέκτης μπορεί συνήθως να αναγνωρίσει το θόρυβο καινά τον απορρίψει πριν από την αποκωδικοποίηση του σήματος.

Όπως και τα υπόλοιπα πρωτόκολλα δικτύωσης, οι ασύρματοι σύνδεσμοι DSSS ανταλλάσσουν μηνύματα χειραψίας μέσα σε κάθε πακέτο δεδομένων για να επιβεβαιώσουν ότι ο δέκτης μπορεί να κατανοήσει κάθε πακέτο. Για παράδειγμα, ο τυπικός ρυθμός μετάδοσης δεδομένων σε ένα δίκτυο Wi-Fi 802.11b και διαμόρφωσης DSSS είναι ίσος με 11 Mbps, αλλά όταν η ποιότητα του σήματος δεν υποστηρίζει τη συγκεκριμένη ταχύτητα, ο πομπός και ο δέκτης χρησιμοποιούν μια διαδικασία που ονομάζεται δυναμική μεταβολή ρυθμού μετάδοσης (dynamic rate shifting) για να μειώσουν την ταχύτητα σε 5,5 Mbps. Η ταχύτητα μπορεί να μειωθεί επειδή κάποια πηγή ηλεκτρικού θορύβου κοντά στο δέκτη παρεμβάλλεται στο σήμα, ή επειδή ο πομπός και ο δέκτης βρίσκονται σε μεγάλη απόσταση μεταξύ τους για να υποστηρίξουν τη λειτουργία στη μέγιστη ταχύτητα. Αν η ταχύτητα των 5,5 Mbps εξακολουθεί να είναι πολύ μεγάλη για το σύνδεσμο, μειώνεται ξανά σε 2 Mbps ή ακόμη και σε 1 Mbps.

3.2.3.6 Ορθογωνική πολύπλεξη με διαίρεση συχνότητας.

Η διαμόρφωση ορθογωνικής πολύπλεξης με διαίρεση συχνότητας (orthogonal frequency division multiplexing modulation — OFDM), που χρησιμοποιείται στα δίκτυα Wi-Fi 802.11a, είναι πολύ πιο πολύπλοκη από την τεχνολογία DSSS. Το φυσικό επίπεδο διαιρεί το ρεύμα των δεδομένοι σε 52 παράλληλα ρεύματα bit, καθένα από τα οποία χρησιμοποιεί διαφορετική ραδιοσυχνότητα που ονομάζεται υπο-φέρον σήμα (subcar-rier). Τέσσερα από

τα υπο-φέροντα σήματα μεταφέρουν πιλοτικά δεδομένα (pilot data) που παρέχουν πληροφορίες αναφοράς σχετικά με τα υπόλοιπα 48 υποφέροντα σήματα, με σκοπό τη μείωση της απώλειας του σήματος λόγω ραδιοπαρεμβολών ή μετατόπισης φάσης (phase shift). Επειδή τα δεδομένα διαιρούνται σε 48 ξεχωριστά ρεύματα που κινούνται παράλληλα μέσω διαφορετικών υποφερόντων σημάτων, η συνολική ταχύτητα μετάδοσης είναι πολύ μεγαλύτερη από την ταχύτητα των δεδομένων μέσω ενός καναλιού.

Οι συχνότητες των υπο-φερόντων σημάτων σε ένα σήμα OFDM επικαλύπτονται, με την κορυφή (peak) της κυματομορφής (waveform) κάθε υπο-φέροντος σήματος να ταυτίζεται με τη γραμμή βάσης (baseline) των επικαλυπτόμενων σημάτων. Αυτό ονομάζεται ορθογωνική διαίρεση συχνότητας (orthogonal frequency division). Το πρότυπο 802.1 Ia ορίζει ένα σύνολο οκτώ καναλιών δεδομένων που έχουν εύρος 20 MHz. Καθένα από αυτά τα κανάλια διαιρείται σε 52 υπο-φέροντα σήματα των 300 KHz.

Όταν ένας ραδιοδέκτης Wi-Fi ανιχνεύει κάποιο σήμα 802.1 Ia, συναρμολογεί τα παράλληλα ρεύματα bit σε ένα ρεύμα δεδομένων υψηλών ταχυτήτων και χρησιμοποιεί τα πιλοτικά δεδομένα για να ελέγξει την ακρίβεια (accuracy) του σήματος. Σε ιδανικές συνθήκες, τα δίκτυα τύπου 802.11a μπορούν να μεταφέρουν δεδομένα με ταχύτητα 54 Mbps αλλά, όπως και στη διαμόρφωση DSSS, ο πομπός και ο δέκτης OFDM μειώνουν αυτόματα την ταχύτητα των δεδομένων όταν ο μέγιστος ρυθμός μετάδοσης δεν είναι εφικτός λόγω παρεμβολών, αδυνάμων σημάτων, η άλλων ατμοσφαιρικών συνθηκών που απέχουν από το ιδανικό.

Η πιο πρόσφατη προδιαγραφή 802.11g σχεδιάστηκε για να συνδυάζει τα καλύτερα χαρακτηριστικά του τύπου 802.11b (μεγαλύτερη εμβέλεια σήματος) και του τύπου 802.11a (μεγαλύτερη ταχύτητα). Για να επιτευχθεί αυτός ο αντικειμενικός στόχος, χρησιμοποιεί διαμόρφωση OFDM στη ζώνη συχνοτήτων 2,4 GHz.

3.2.3.7 Η σημασία της τεχνολογίας ραδιοκυμάτων

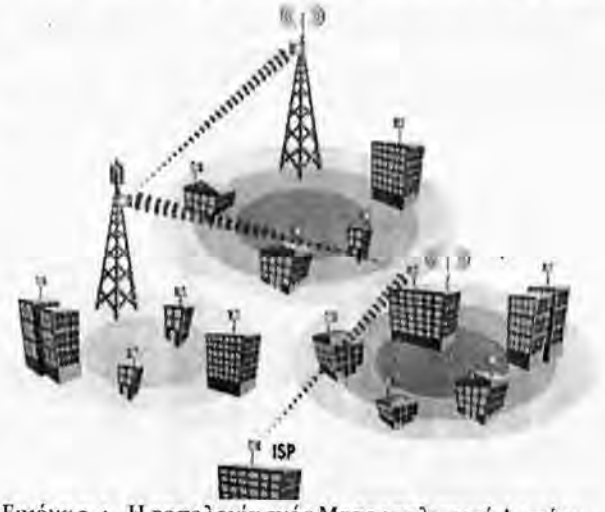
Ο μεγάλος συγγραφέας επιστημονικής φαντασίας, Arthur C. Clarke παρατήρησε κάποτε ότι *«Κάθε αρκετά προχωρημένη τεχνολογία δεν μπορεί να διακριθεί από τη μαγεία».* Για τους περισσότερους από εμάς, η τεχνολογία που ελέγχει τα ραδιοκύματα εξάπλωσης φάσματος υψηλών ταχυτήτων θα μπορούσε κάλλιστα να αποτελεί κάποια μορφή μαγείας, επειδή δε χρειάζεται να κατανοήσουμε αυτά που συμβαίνουν μέσα στον πομπό και στο δέκτη· είναι σχεδόν αόρατα όταν συνδέουμε κάποιον υπολογιστή με το Διαδίκτυο. Όπως είπαμε προηγουμένως σε αυτό το κεφάλαιο, δεν είναι απαραίτητο να κατανοήσετε τις τεχνικές λεπτομέρειες σχετικά με τον τρόπο που ένας πομπός

Wi-Fi διαιρεί τα δεδομένα σε πολύ μικρά κομμάτια και τα επανασυναρμολογεί σε δεδομένα, εκτός αν είστε σχεδιαστές ραδιοκυκλωμάτων.

Αλλά όταν ξέρετε ότι υπάρχει ένα καλά ορισμένο σύνολο κανόνων και μεθόδων που καθιστούν τη σύνδεση λειτουργική (ακόμη και αν δε γνωρίζετε όλες τις λεπτομέρειες), έχετε τον έλεγχο. Ξέρετε ότι δεν πρόκειται για μαγεία και, αν το σκεφθείτε, ενδέχεται να γνωρίζετε ακόμη κάποιες από τις σωστές ερωτήσεις που πρέπει να γίνουν όταν το σύστημα δε λειτουργεί σωστά. Αν η γνώση είναι δύναμη, τότε η γνώση για την τεχνολογία που χρησιμοποιείτε κάθε μέρα είναι η δύναμη να ελέγχετε τη συγκεκριμένη τεχνολογία αντί απλώς να τη χρησιμοποιείτε.

3.3 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΤΗΣ ΑΣΥΡΜΑΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ

Η ασύρματη ευρυζωνική τεχνολογία παρέχει στις φορητές συσκευές πρόσβαση στο Διαδίκτυο, πέρα από το γεγονός ότι δίνει τη δυνατότητα στους χειριστές των δικτύων να επεκτείνουν τα δίκτυα τους πέρα από την εμβέλεια των ενσύρματων συνδέσεων τους. Για το σκοπό μας, τα αμφίδρομα ραδιοκύματα αποτελούν την πιο λογική προσέγγιση για την ασύρματη ευρυζωνική τεχνολογία, αλλά είναι επίσης δυνατές και άλλες μέθοδοι (όπως το υπέρυθρο φως ή τα ορατά σήματα). Η σύνδεση του υπολογιστή μας με το Διαδίκτυο (ή με κάποιο τοπικό δίκτυο) μέσω ραδιοκυμάτων προσφέρει αρκετά πλεονεκτήματα σε σύγκριση με την ενσύρματη σύνδεση του.



Εικόνα 3-4 - Η τοπολογία ενός Μητροπολιτικού Δικτύου

Πρώτον, η ασύρματη τεχνολογία παρέχει κατάλληλη πρόσβαση για τους φορητούς υπολογιστές, δεν είναι απαραίτητο να βρείτε καλώδια ή πρίζες δεδομένων δικτύου. Δεύτερον, επιτρέπει στους χρήστες να συνδεθούν σε περισσότερες από μία τοποθεσίες, καθώς επίσης και να διατηρήσουν μια σύνδεση ενώ μετακινούνται από το ένα σημείο στο άλλο. Για τους δια-

χειριστές δικτύου, μια ασύρματη σύνδεση καθιστά εφικτή τη διανομή της πρόσβασης σε κάποιο δίκτυο χωρίς την ανάγκη να τοποθετήσουν καλώδια ή να ανοίξουν τρύπες στους τοίχους.

Στην πράξη, η πρόσβαση χωρίς καλώδια σημαίνει ότι ο ιδιοκτήτης ενός φορητού υπολογιστή ή άλλης φορητής συσκευής μπορεί να μπει σε μια τάξη διδασκαλίας, μια καφετέρια, ή κάποια βιβλιοθήκη και να συνδεθεί στο Διαδίκτυο απλώς ανάβοντας τον υπολογιστή και εκτελώντας κάποιο πρόγραμμα επικοινωνίας. Ανάλογα με τον τύπο του ασύρματου δικτύου που χρησιμοποιούμε, ενδέχεται να είμαστε επίσης σε θέση να διατηρήσουμε την ίδια σύνδεση σε κινούμενο όχημα.

Όταν εγκαθιστάτε το δικό σας δίκτυο, συχνά είναι ευκολότερο να χρησιμοποιήσετε συνδέσεις Wi-Fi για να επεκτείνετε το δίκτυο σας και τη σύνδεση σας με το Διαδίκτυο σε άλλα δωμάτια, επειδή τα ενσύρματα συστήματα απαιτούν την ύπαρξη φυσικής διαδρομής των καλωδίων ανάμεσα στο δρομολογητή δικτύου (network router) ή το μεταγωγό (switch) και κάθε υπολογιστή. Αυτό σημαίνει σχεδόν πάντα ότι πρέπει να ανοίξετε τρύπες στους τοίχους σας για συζευκτήρες δεδομένων και να τοποθετήσετε καλώδια μέσα στους τοίχους και κάτω από τα πατώματα, εκτός αν μπορείτε να δρομολογήσετε τα καλώδια αυτά μέσω ψευδοροφής ή άλλου υπάρχοντος καναλιού. Τα ραδιοσήματα που περνούν μέσα από αυτούς τους ίδιους τοίχους συχνά είναι πιο καθαρή και εύκολη λύση.

3.4 ΑΣΥΡΜΑΤΕΣ ΥΠΗΡΕΣΙΕΣ ΔΕΔΟΜΕΝΩΝ

Επειδή τα ραδιοσήματα κινούνται μέσω του αέρα, μπορεί να διαμορφώσετε μια σύνδεση δικτύου σε οποιοδήποτε σημείο μέσα στην εμβέλεια του πομπού του σταθμού βάσης (base station) του δικτύου· δεν είναι απαραίτητη η χρήση τηλεφωνικής γραμμής, καλωδίου τηλεόρασης, ή κάποιας άλλης αποκλειστικής καλωδίωσης για τη σύνδεση του υπολογιστή σας με το δίκτυο. Απλώς ανάβετε τον ασύρματο προσαρμογέα του υπολογιστή και ο οποίος, εντοπίζει το σήμα του δικτύου. Επομένως, η ασύρματη σύνδεση δικτύου είναι συχνά πολύ πιο κατάλληλη από την ενσύρματη.

Αυτό δε σημαίνει ότι η ασύρματη τεχνολογία είναι πάντα η καλύτερη επιλογή. Τα ενσύρματα δίκτυα είναι συνήθως πιο ασφαλή από τα ασύρματα, επειδή είναι πολύ πιο δύσκολο για μη εξουσιοδοτημένα άτομα που κρυφακούν, καθώς και για άλλους αδιάκριτους χρήστες, να παρακολουθήσουν τα δεδομένα καθώς αυτά κινούνται μέσω του δικτύου. Ακόμα, οι ενσύρματες συνδέσεις δεν απαιτούν τόσο πολλές σύνθετες διαπραγματεύσεις μεταξύ αποστολέα και παραλήπτη όσο αφορά τα πρωτόκολλα και τα λοιπά. Σε ένα

περιβάλλον όπου ο υπολογιστής μας δε μετακινείται ποτέ από το γραφείο μας και δεν υπάρχουν φυσικά εμπόδια ανάμεσα στον υπολογιστή και το access point στο δίκτυο, συχνά είναι πιο εύκολη η εγκατάσταση ενός καλωδίου δεδομένων, utp, μεταξύ του υπολογιστή και κάποιου μόντεμ.

Έτσι, έχουμε πλέον μια ομάδα πομπών και δεκτών ραδιοκυμάτων που λειτουργούν όλοι στις ίδιες συχνότητες και με το ίδιο είδος διαμόρφωσης. (Η διαμόρφωση είναι η μέθοδος που χρησιμοποιεί μια συσκευή ασύρματης επικοινωνίας για να προσθέσει κάποιο είδος περιεχομένου, όπως φωνή ή ψηφιακά δεδομένα, σε ένα ραδιοκύμα.) Το επόμενο βήμα είναι η αποστολή κάποιων δεδομένων δικτύου μέσω αυτών των συσκευών ασύρματης επικοινωνίας. Είναι διαθέσιμα πολλά διαφορετικά ασύρματα συστήματα και υπηρεσίες δεδομένων για τη σύνδεση υπολογιστών και άλλων συσκευών με τοπικά δίκτυα και το Διαδίκτυο, όπως τα. Wi-Fi, WiMAX, και ένας μικρός αριθμός υπηρεσιών που βασίζονται στις τελευταίες γενιές της τεχνολογίας κυψελωτής κινητής τηλεφωνίας.

3.4.1 WiFi

Το Ίδρυμα Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (Institute of Electrical and Electronic Engineers — IEEE) έχει δημιουργήσει ένα σύνολο προτύπων και προδιαγραφών για τα ασύρματα δίκτυα, με τον τίτλο IEEE 802.11, που ορίζουν τις μορφές και τις δομές των σημάτων σχετικά μικρής εμβέλειας τα οποία παρέχουν υπηρεσία Wi-Fi. Το αρχικό πρότυπο 802.1 1 (χωρίς κάποιο γράμμα στο τέλος) ανακοινώθηκε το 1997. Καλύπτει αρκετούς τύπους ασύρματων μέσων: δύο είδη μεταδόσεων ραδιοκυμάτων και δίκτυα που χρησιμοποιούν υπέρυθρο φως. Το πρότυπο 802.11b παρέχει επιπλέον προδιαγραφές για ασύρματα δίκτυα Ethernet. Ένα σχετικό έγγραφο, το IEEE 802.11a, περιγράφει ασύρματα δίκτυα που λειτουργούν με μεγαλύτερες ταχύτητες σε διαφορετικές ραδιοσυχνότητες. Υπάρχουν επίσης και άλλα

πρότυπα δικτύωσης ραδιοκυμάτων της κατηγορίας 802.11 με άλλα γράμματα (στο τέλος) που είναι διαθέσιμα ή πρόκειται να κυκλοφορήσουν.

Οι προδιαγραφές με τη μεγαλύτερη χρήση σήμερα είναι οι 802.11a, 802.11b, και 802.11 g. Είναι τα ντε φάκτο πρότυπα που χρησιμοποιούνται σε όλα σχεδόν τα ασύρματα Ethernet LAN τα οποία είναι πιθανό να συναντήσετε σε γραφεία και δημόσιους χοίρους και στα περισσότερα οικιακά δίκτυα. Αξίζει τον κόπο να παρακολουθούμε την πρόοδο των υπόλοιπων προτύπων αλλά, προς το παρόν, τα 802.1 la και 802.11g είναι εκείνα που θα χρησιμοποιήσετε για ασύρματα δίκτυα μικρής εμβέλειας, ιδιαίτερα αν υπολογίζετε να συνδεθείτε σε δίκτυα στα οποία δεν ελέγχετε οι ίδιοι όλο το υλικό. Μία ή δύο φορές το χρόνο, ο Συνασπισμός Wi-Fi (Wi-Fi Alliance) διεξάγει ένα «διαγωνισμό διαλειτουργικότητας», όπου οι μηχανικοί πολλών κατασκευαστών υλικού επαληθεύουν ότι το υλικό τους επικοινωνεί σωστά με εξοπλισμό από άλλους προμηθευτές. Ο δικτυακός εξοπλισμός που διαθέτει το λογότυπο Wi-Fi έχει πιστοποιηθεί από το Συνασπισμό Wi-Fi ότι πληροί τα σχετικά πρότυπα και ότι περνάει με επιτυχία τις δοκιμές διαλειτουργικότητας. Το Wi-Fi προοριζόταν αρχικά ως ασύρματη επέκταση ενός ενσύρματου LAN, άρα οι αποστάσεις μεταξύ των σταθμών βάσης Wi-Fi και των υπολογιστών που επικοινωνούν μέσω αυτών περιορίζονται σε περίπου 35 μέτρα σε εσωτερικούς χώρους ή μέχρι 100 μέτρα σε εξωτερικούς, με την προϋπόθεση ότι δεν υπάρχουν εμπόδια ανάμεσα στο σημείο πρόσβασης και τον υπολογιστή. Όταν θα είναι διαθέσιμος ο εξοπλισμός 802.11n, θα υποστηρίζει συνδέσεις μεταξύ υπολογιστών και σταθμών βάσης, τουλάχιστον στις ίδιες αποστάσεις μεταξύ τους με αυτές των παλαιοτέρων εκδόσεων Wi-Fi. Υπάρχουν τρόποι επέκτασης της εμβέλειας των σημάτων Wi-Fi, αλλά αυτές οι τεχνικές απαιτούν ειδικό εξοπλισμό και προσεκτική εγκατάσταση.

Επειδή τα περισσότερα σήματα Wi-Fi έχουν τόσο περιορισμένη εμβέλεια, πρέπει να βρίσκετε ένα νέο σημείο πρόσβασης ή θερμό σημείο (hot spot) και να εγκαθιστάτε μια νέα σύνδεση κάθε φορά που μετακινείτε τον υπολογιστή σας σε νέα θέση. Και επειδή τα σημεία πρόσβασης Wi-Fi δεν επιτρέπουν σε αγνώστους να συνδεθούν μέσω αυτών, ίσως πρέπει να δημιουργήσετε ξεχωριστό λογαριασμό για κάθε θέση.

Τα δίκτυα Wi-Fi που περιγράφονται, ακολουθούν τα πρότυπα 802.1 la, b, και g, αλλά μεγάλο κομμάτι των ίδιων πληροφοριών θα ισχύει και στα νέα δίκτυα 802.1 In όταν αυτά θα είναι διαθέσιμα.

3.4.1.1 Μητροπολιτικές υπηρεσίες Wi-Fi

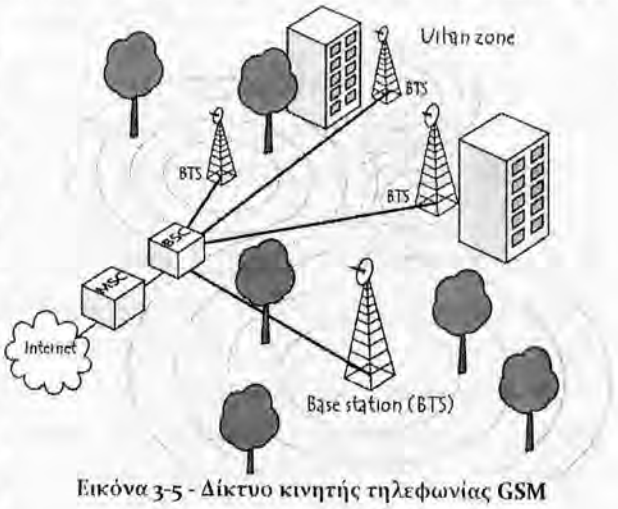
Σε κάποιες μητροπολιτικές περιοχές, όπως είναι η Αθήνα, εγκαθίσταται μεγάλος αριθμός από διασυνδεδεμένους σταθμούς βάσης Wi-Fi, από δημόσιες υπηρεσίες ή από ιδιωτικές επιχειρήσεις, ακόμα και από ιδιώτες που κάνουν το

χόμπι τους, για την παροχή ασύρματης υπηρεσίας σε μια ολόκληρη περιοχή ή σε επιλεγμένες γειτονιές, ως οικονομική εναλλακτική λύση στις καλωδιακές (cable) και τις τηλεφωνικές (DSL) υπηρεσίες. Οι σταθμοί βάσης γι' αυτές τις υπηρεσίες εγκαθίστανται συχνά σε κολώνες των επιχειρήσεων κοινής ωφέλειας (ΔΕΗ. ΟΤΕ) ή σε στέγες σπιτιών.

Τα ίδια δίκτυα ενδέχεται επίσης να παρέχουν μια ποικιλία ειδικών υπηρεσιών δεδομένων στην τοπική αυτοδιοίκηση και σε μεγάλους συνδρομητές. Για παράδειγμα, οι τοπικές επιχειρήσεις κοινής ωφέλειας για το φυσικό αέριο, το ηλεκτρικό ρεύμα, και το νερό θα μπορούσαν να προσθέσουν μικρούς προσαρμογείς Wi-Fi στους μετρητές τους και να χρησιμοποιούν το σύστημα για να στέλνουν μετρήσεις μία φορά το μήνα. Και τα αστικά λεωφορεία θα μπορούσαν να διαθέτουν πομποδέκτες που αναφέρουν τη θέση τους σε ένα κεντρικό σύστημα παρακολούθησης, όπως το σύστημα της πόλης του Σηάτλ. Δεν είναι ακόμη σαφές αν αυτές οι αστικές υπηρεσίες Wi-Fi θα μπορέσουν να ξεπεράσουν τα πιθανά προβλήματα παρεμβολών και τον ανταγωνισμό από τις άλλες ασύρματες εναλλακτικές λύσεις για δεδομένα, ή αν θα προσελκύσουν αρκετούς πελάτες ώστε να παραμείνουν βιώσιμες. Αλλά αν το καταφέρουν, κάθε υπολογιστής μέσα στην περιοχή κάλυψης, ο οποίος διαθέτει προσαρμογέα Wi-Fi, θα πρέπει να εντοπίζει το σήμα και να αποκτάει πρόσβαση σε μια ευρυζωνική σύνδεση με το Διαδίκτυο.

3.4.2 Ασύρματες υπηρεσίες κυψελωτής κινητής τηλεφωνίας

Αρκετές ευρυζωνικές ασύρματες υπηρεσίες δεδομένων είναι επεκτάσεις της τεχνολογίας της κυψελωτής κινητής τηλεφωνίας. Μπορεί να τις δείτε να περιγράφονται ως υπηρεσίες 3G (third generation — τρίτης γενιάς), επειδή βασίζονται στην τρίτη γενιά τεχνολογίας της κινητής τηλεφωνίας. Αν χρησιμοποιείτε κινητό τηλέφωνο για περισσότερα από ένα ή δύο χρόνια, θα θυμάστε ίσως ότι τα πρώτα τηλέφωνα είχαν δυνατότητα μόνο για φωνητικές κλήσεις αλλά, με κάθε καινούργια γενιά, οι φορείς της κινητής τηλεφωνίας πρόσφεραν περισσότερες και καλύτερες δυνατότητες. Το μεγάλο πλεονέκτημα της κινητής ευρυζωνικής υπηρεσίας για τα άτομα που χρησιμοποιούν τους υπολογιστές τους μακριά από το σπίτι ή το γραφείο είναι ότι καλύπτει πολύ μεγαλύτερη περιοχή από οποιονδήποτε



Εικόνα 3-5 - Δίκτυο κινητής τηλεφωνίας GSM

σταθμό βάσης Wi-Fi μπορείτε να συνδέσετε τον υπολογιστή σας στο Διαδίκτυο χωρίς την ανάγκη εύρεσης νέου hot spot και τη χρήση διαφορετικού λογαριασμού πρόσβασης.

4 ΤΟ ΑΣΥΡΜΑΤΟ ΜΗΤΡΟΠΟΛΙΤΙΚΟ ΔΙΚΤΥΟ ΑΘΗΝΩΝ

4.1 Η ΙΣΤΟΡΙΑ ΤΟΥ AWMN

Απο το 2000 και έπειτα, οι ανάγκες για την δικτύωση μεταξύ των υπολογιστών άρχισαν να γίνονται επιτακτικές. Όλο και περισσότεροι οικιακοί χρήστες είχαν την ανάγκη να μπορούν να ανταλλάσουν γρήγορα αρχεία και να επικοινωνούν οι υπολογιστές τους με σχετική ευκολία. Κάτι τέτοιο ήταν απαγορευτικό για εκείνη την εποχή, και ιδιαίτερα στους οικιακούς χρήστες, καθότι οι ISDN γραμμές που προσέφερε ο ΟΤΕ μετέφεραν το πολύ 128kbps και τα μισθωμένα κυκλώματα κόστιζαν εκατοντάδες και ίσως και χιλιάδες ευρώ μηνιαίως.

Ορισμένοι, λοιπόν, βρήκαν την λύση των ασύρματων δικτύων, προσιτή στην τιμή, και πολύ ταχύτερη από κάθε άλλη εμπορική, δημόσια υπηρεσία τηλεπικοινωνίας. Ξεκίνησαν λοιπόν να φτιάχνουν μικρά τοπικά ασύρματα δίκτυα ενώνοντας 2 – 3 κόμβους μεταξύ τους, με ασύρματες ζεύξεις στην συχνότητα των 2,4Ghz μέσω του πρωτοκόλλου 802.11b το οποίο θεωρητικά προσέφερε ταχύτητες 11Mbps περίπου δηλαδή 85 φορές γρηγορότερα από μία ISDN χρησιμοποιώντας και τα δύο κανάλια της. Φυσικά δεν ήταν το ίδιο διότι με τις ασύρματες αυτές ζεύξεις ενώνονταν μερικές δεκάδες άτομα και δεν είχαν την δυνατότητα να επικοινωνούν με αυτές τις ταχύτητες με όλο το διαδίκτυο, αλλά αυτό που είχαν καταφέρει μέχρι στιγμής ήταν ένα τεράστιο βήμα προς αυτό που ονομάζουμε σήμερα awmn.

Με την πάροδο του χρόνου, όλο και περισσότεροι μάθαιναν γι' αυτό το ασύρματο δίκτυο, με αποτέλεσμα να μεγαλώνει μέρα με την μέρα, και όσο οι

τεχνολογίες ευρυζωνικότητας δεν εξελίσσονταν, το awmn επεκτεινόταν από ταράτσα σε ταράτσα, σε όλη την Αθήνα, καθώς επίσης και σε πόλεις της περιφέρειας, όπως η Θεσσαλονίκη, η Λαμία, η Πάτρα, η Κατερίνη και πολλές ακόμα. Άρχισε πια να γίνεται πιο μαζικό και ταυτόχρονα πιο ενδιαφέρον, αφού πλέον, είχαν αναπτυχθεί νέα πρωτόκολλα ασύρματων ζεύξεων (802.11a και 802.11g) τα οποία παρείχαν μεγαλύτερες ταχύτητες και την δυνατότητα να υλοποιούνται ζεύξεις μεταξύ σημείων που απείχαν μερικά χιλιόμετρα.

Ο ρυθμός ανάπτυξης του awmn άρχισε να μικραίνει περίπου το 2008, οπού άρχισε ο να αναπτύσσεται η τεχνολογία DSL η οποία παρείχε πολύ μεγαλύτερους ρυθμούς μετάδοσης δεδομένων από τις προηγούμενες τεχνολογίες (μέχρι 8Mbps και στην συνέχεια μέχρι 24Mbps) με αποτέλεσμα να μικραίνει το ενδιαφέρον για την αναζήτηση γρηγορότερης σύνδεσης. Το awmn λοιπόν θα λέγαμε ότι έχει ωριμάσει και αυτήν την περίοδο αναπτύσσεται με μικρότερους ρυθμούς, παρέχοντας στους χρήστες του, υπηρεσίες μετάδοσης 300+Mbps και παραμένει σίγουρα ένα πάρα πολύ καλό «σχολείο» και μια αστείρευτη πηγή γνώσεων και εμπειριών στον χώρο των δικτύων και των τηλεπικοινωνιών γενικότερα.

4.2 ΤΟ WIND (Wireless Nodes Database)

4.2.1 Τι είναι το WIND

Μία από τις σημαντικότερες λειτουργίες ενός Ασύρματου Κοινοτικού Δικτύου, είναι η δυναμική καταγραφή και απεικόνιση των κόμβων του. Όποιος θέλει να συνδεθεί και να συμμετάσχει στο δίκτυο θα πρέπει να δηλώσει την θέση του στο WiND Wireless Nodes Database) Πρόκειται για μια web-based βάση κόμβων, που απεικονίζει γεωγραφικά πάνω σε χάρτες (geolocation), τους κόμβους ενός ασύρματου δικτύου, παρέχοντας χρήσιμες πληροφορίες για κάθε ένα κόμβο ξεχωριστά καθώς και τις μεταξύ τους συνδέσεις. Η κατανόηση του περιβάλλοντος της εφαρμογής είναι ιδιαίτερα σημαντική, καθώς θα σας επιτρέψει να εντοπίσετε εύκολα τα πιθανά σημεία σύνδεσής σας στο δίκτυο.

Ο πηγαίος κώδικας του WiND είναι υπό GNU GPL και ως εκ' τούτου είναι διαθέσιμος για οποιονδήποτε θέλει να συμμετάσχει στην ανάπτυξη του ή/και να τον χρησιμοποιήσει. Κάθε ένας Ασύρματος Κόμβος Δικτύου, έχει την δυνατότητα να χρησιμοποιήσει το WiND για την γεωγραφική αναπαράσταση των κόμβων του. Στην Ελλάδα, ήδη, χρησιμοποιείται πέρα του AWMN από την συντριπτική πλειοψηφία των Α.Κ.Δ. (πάνω από 20) και έχει εκδηλωθεί ενδιαφέρον για χρήση του και σε άλλες ασύρματες κοινότητες στο εξωτερικό.

4.2.2 Η ιστορία του wind

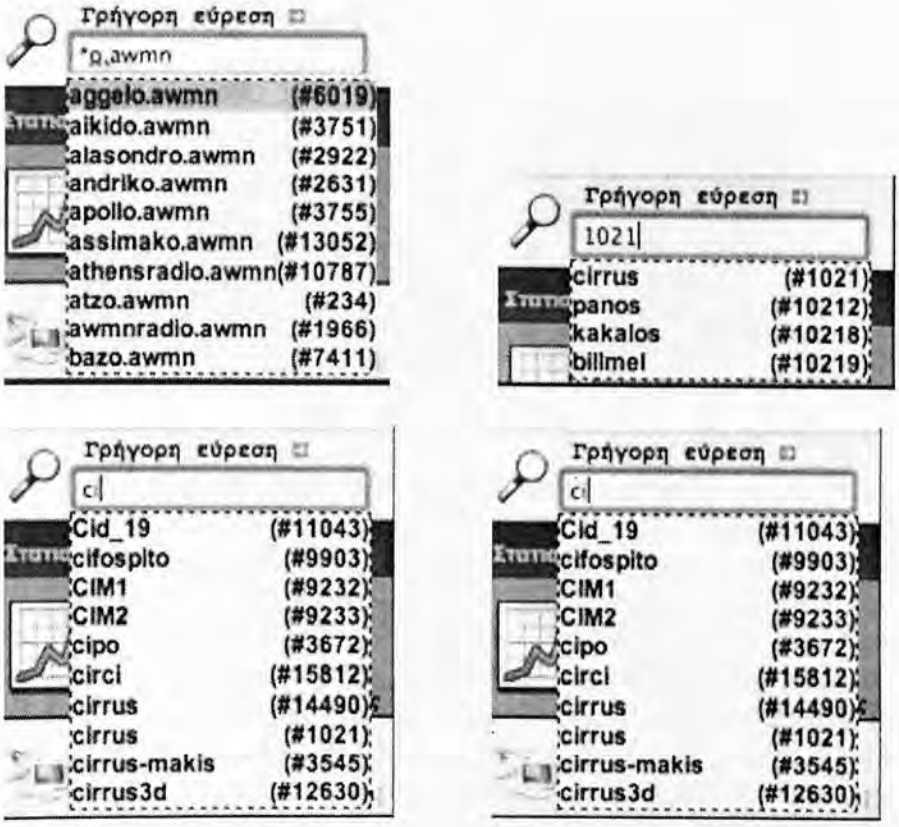
Το WiND αναπτύχθηκε από μέλη του AWMN σε μια προσπάθεια να αντικαταστήσουν την NodeDB. Η NodeDB είναι μια γεωγραφική βάση η οποία ξεκίνησε ως προσπάθεια χαρτογράφησης του Sydney Wireless αλλά γρήγορα εξελίχθηκε σε μια υπηρεσία γεωγραφικής καταγραφής αρκετών ασύρματων δικτύων σε όλο τον κόσμο. Δυστυχώς η ανάπτυξη στο project της NodeDB ήταν αρκετά αργή, αφού από επιλογή του Αυστραλού developer και ιδρυτή της NodeDB, παρέμεινε project κλειστού κώδικά, με αποτέλεσμα να μην καλύπτει επαρκώς τις ανάγκες των ταχύτατα αναπτυσσομένων δικτύων όπως το "δικό μας" (ελληνικό γαρ) AWMN. Ειδικά δε στην περίπτωση του τελευταίου οι ανάγκες που δεν κάλυπτε η NodeDB ήταν αρκετές και χρησιμοποιήθηκαν διάφορα μεμονωμένα εργαλεία κάτι που όπως αποδείχτηκε δεν ήταν πρακτικό. Την λύση ήρθε να δώσει το WiND όπου φτιάχτηκε απο την αρχή για να καλύψει τις ανάγκες των ΑΚΔ. Ας δούμε όμως αναλυτικά τις δυνατότητες και τα ιδιαίτερα χαρακτηριστικά του.

4.2.3 Τα χαρακτηριστικά του wind

Όπως προαναφέρθηκε, η κατανόηση των δυνατοτήτων και του περιβάλλοντος της εφαρμογής είναι ιδιαίτερα σημαντική. Ακολουθεί μια λίστα με τα σημαντικότερα χαρακτηριστικά του WiND.

Πολυγλωσσική υποστήριξη: Το περιβάλλον της εφαρμογής εμφανίζεται στα Ελληνικά και στα Αγγλικά.

Γρήγορη αναζήτηση κόμβων: Αναζήτηση μπορεί να γίνει βάση του ονόματος του κόμβου, του κωδικού nodeID ή ακόμα και του IP υποδίκτυου που χρησιμοποιεί.



Εικόνα 4-1 - Screenshots από το wind.awmn.net

Αναζήτηση: Αναζήτηση μπορεί να γίνει επίσης μέσω του μενού "Κόμβοι Δικτύου". Η αναζήτηση μπορεί να γίνει βάση διαφόρων κριτηρίων όπως ο Αριθμός Κόμβου nodeID, το Όνομα του Κόμβου, Δήμος/Κοινότητα, Νομαρχία, Ενεργές Διασυνδέσεις, Ενεργοί Πελάτες, AP κοκ.

Στατιστικά: Στο αριστερό πλαίσιο της εφαρμογής υπάρχουν τα συγκεντρωτικά στατιστικά της βάσης. Περιλαμβάνουν τους συνδεδεμένους κόμβους έναντι αυτών που έχουν δηλώσει απλώς το στίγμα, το σύνολο

των κόμβων κορμού (Backbone), τις διασυνδέσεις (p2p links), τα Access Points και τις δηλωμένες υπηρεσίες.

Υποστήριξη Google Maps: Από τα πιο εντυπωσιακά χαρακτηριστικά του WiND είναι η γεωγραφική απεικόνιση των κόμβων του ασύρματου δικτύου πάνω σε χάρτες του google. [Εικ. 2]. Οι χάρτες μπορεί να είναι οδικοί (map), δορυφορικοί (satellite), εδαφικοί (terrain) ή συνδυασμός (hybrid) με αρκετά επίπεδα zoom για να εστιάσετε ακριβώς στην περιοχή που θέλετε.

Εικόνα 4-2 - Screenshots από το wind.awmn.net

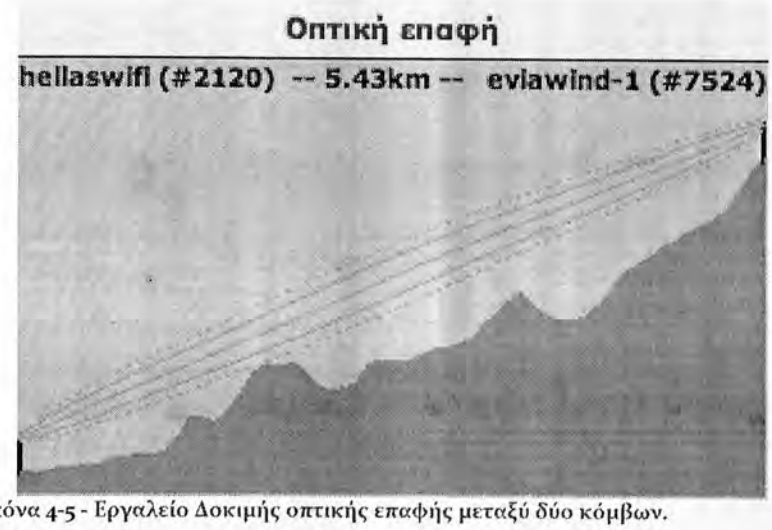
Οι κόμβοι εμφανίζονται πάνω στον χάρτη σύμφωνα με τις γεωγραφικές συντεταγμένες τους και με διαφορετικό χρώμα ανάλογα με το είδος του κόμβου που αναπαριστούν. Υπάρχουν τεσσάρων ειδών διαφορετικά αναπαράσταση των κόμβων πάνω στον χάρτη: σύμβολα για την α) Ο κόμβος "Backbone" (ή κόμβος κορμού ΒΒ) με πάνω από δύο αποκλειστικές συνδέσεις και αδιάλειπτη λειτουργία. Κάθε ένας BackBone κόμβος συνδέεται με άλλους BackBone συνθέτοντας το δίκτυο κορμού. β) Ο κόμβος "Access Point" (ή σημείο πρόσβασης ΑΡ) που συνδέεται ή μπορεί να αποτελεί μέρος του δικτύου κορμού (συνήθως είναι και ΒΒ κόμβος) και επιτρέπει την σύνδεση στο Δίκτυο, τερματικών κόμβων "Πελατών". γ) Ο κόμβος "Πελάτης" (ή τερματικός κόμβος Client) ο οποίος συνδέεται σε έναν κόμβο Access Point και δεν είναι απαραίτητη η αδιάλειπτη λειτουργία του. δ) Στην τέταρτη κατηγορία ανήκουν όλοι οι ασύνδετοι κόμβοι. "Ασύνδετοι" κόμβοι είναι όσοι έχουν εκδηλώσει την πρόθεσή τους να συνδεθούν στο δίκτυο και δεν έχουν συνδεθεί ακόμα. Είναι ιδιαίτερα σημαντική η καταχώριση αυτών επειδή αποτελούν τους μελλοντικούς πιθανούς κόμβους του δικτύου. Πέρα από τους κόμβους πάνω στους χάρτες εμφανίζονται και οι συνδέσεις τους. Με πράσινο φαίνονται οι συνδέσεις Backbone, με μπλε οι συνδέσεις κόμβων "Πελατών" και με κόκκινο οι συνδέσεις οι οποίες έχουν δηλωθεί ως ανενεργές.

Εικόνα 4-3 - **Screenshot** από το **wind.awmn.net(Google Maps)**

Υποστήριξη Google Earth: Για ακόμα καλύτερη απεικόνιση δίνεται η δυνατότητα εξαγωγής των στοιχείων όλων των κόμβων που είναι δηλωμένων σε αρχείο .kml κάτι που επιτρέπει το άνοιγμα του χάρτη μέσω της εφαρμογής google earth αρκεί να είναι εγκατεστημένη τοπικά στον Η/Υ. Η εξαγωγή του αρχείου γίνεται με ένα κλικ στον σύνδεσμο "Google Earth" που εμφανίζεται πάνω αριστερά στον χάρτη. Στην παρακάτω εικόνα εμφανίζεται μια όψη, με προοπτική, των κόμβων του WiND Ευβοίας, μέσω του Google Earth.

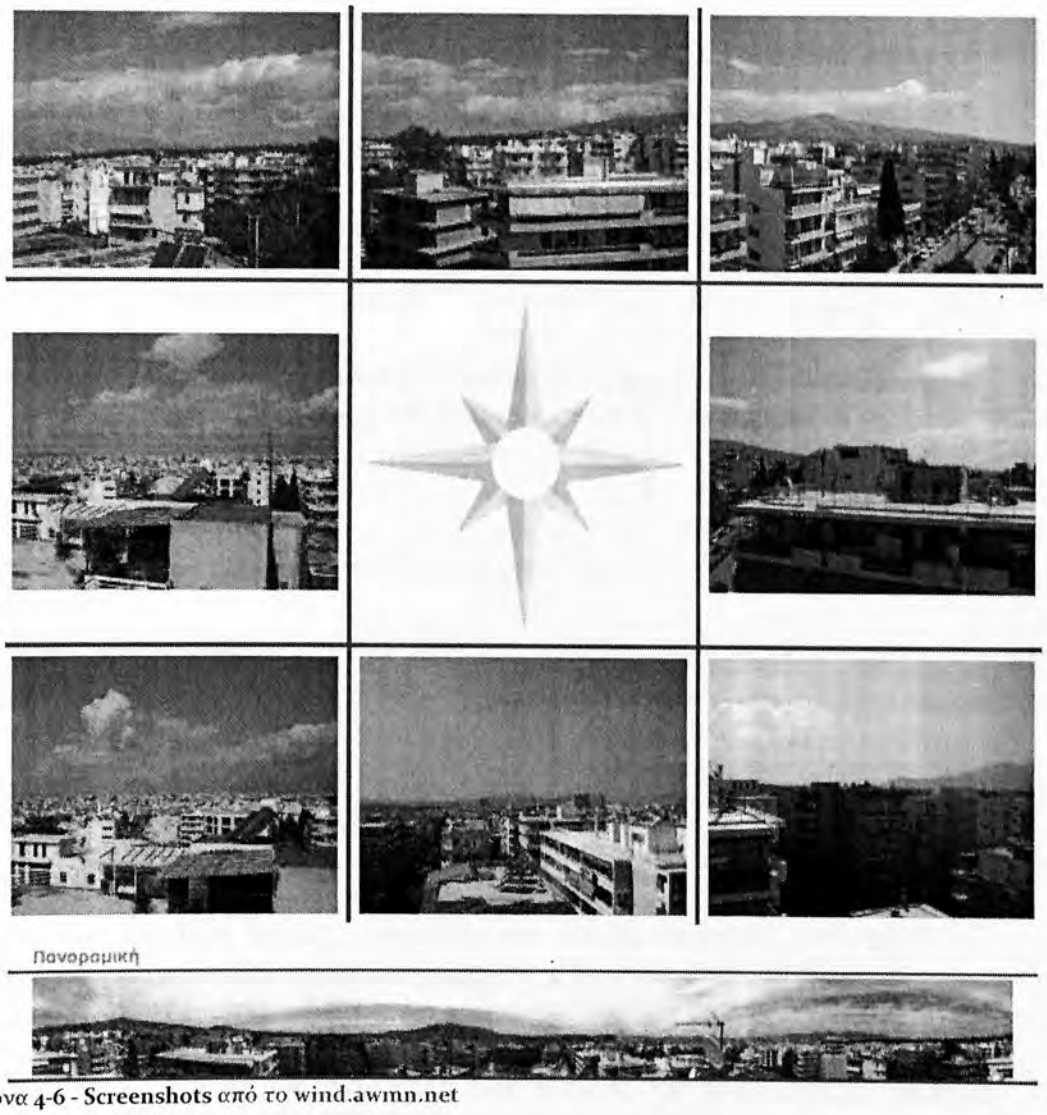
Εικόνα 4-4 - Screenshot από το wind.awmn.net

Υψομετρικό διάγραμμα σημείων: Το WiND πέρα από το γεωγραφικό μήκος και πλάτος περιέχει και υψομετρικές πληροφορίες για τα σημεία στους χάρτες. Με αυτό τον τρόπο επιτρέπει το έλεγχο για οπτική επαφή μεταξύ δύο σημείων και υπολογίζεται η μεταξύ τους απόσταση. Ο έλεγχος οπτικής επαφής μεταξύ δύο σημείων μπορεί να γίνει μέσω ειδικού παραθύρου όπου επιλέγονται τα δύο άκρα που μας ενδιαφέρουν να ελέγξουμε (σύνδεσμος "Οπτική επαφή με άλλους κόμβους"). Το αποτέλεσμα της οπτικής μπορεί να είναι όπως το παρακάτω παράδειγμα.



Εικόνα 4-5 - Εργαλείο Δοκιμής οπτικής επαφής μεταξύ δύο κόμβων.

Φωτογραφική Οπτική Κόμβου: Προαιρετικά η οπτική του κόμβου μπορεί να δοθεί με μια σειρά από φωτογραφίες που ανεβάζει ο χρήστης στην καρτέλα του κόμβου του κάτι που είναι ιδιαίτερα χρήσιμο για έλεγχο της οπτικής σε αστικές περιοχές που υπάρχουν κτήρια ή άλλα τεχνητά εμπόδια πέρα της υψομετρικής διαφοράς. Συνολικά στο κάτω μέρος της καρτέλας του κόμβου διακρίνονται 8 θέσεις για φωτογραφίες, μία για κάθε σημείο του ορίζοντα (Δ, ΒΔ, Β, ΒΑ, Α, ΝΑ, Ν, ΝΔ) και άλλη μια θέση που δίνει την δυνατότητα να συμπεριληφθεί στην οπτική του κόμβου μια πανοραμική φωτογραφία.



Εικόνα 4-6 - **Screenshots** από το wind.awmn.net

4.2.4 WiND Development Team

- Nikolaos "Winner" Nikalexis <winner [@] cube.gr> - Main Developer
- Konstantinos "vinilios" Papadimitriou <vinilios [@] cube.gr> - Basic Templates & Graphics
- Christos "nikpet" Petsas <nikpet [@] dtps.unipi.gr> - Alpha/Beta? testing
- Petros "Ernest0x" Moisiadis <ernest0x [@] dtps.unipi.gr> - BIND updater script
- Faidon "paravoid" Liambotis <faidon [@] cube.gr> - Spiritual leader
- John "cirrus" Kolovos <cirrus [@] awmn.net> - Developer

Special thanks

- Modulus SA for kindly hosting the project

http://wind.cube.gr/

(Η επίσημη σελίδα του project WiND)

4.3 ΟΙ ΥΠΗΡΕΣΙΕΣ ΤΟΥ AWMN

Το awmn πολλές φορές, ονομάζεται και «μικρό internet» αυτό συμβαίνει διότι παρέχονται πολλές υπηρεσίες από τα μέλη του δικτύου όπως ακριβώς συμβαίνει και στο internet, στο awmn όμως υπάρχει η διαφορά ότι ο καθένας μπορεί πολύ εύκολα να ¨ανεβάσει¨ μια υπηρεσία στο δίκτυο και να την δοκιμάσουν άμεσα τα υπόλοιπα μέλη του δικτύου. Θα ήταν αρκετά δύσκολο να καταγράψει κανείς το τι υπηρεσία προσφέρει ο καθένας, ωστόσο, μέσα στο wind υπάρχει σχετική καταχώρηση οπού ο καθένας μπορεί να δει τις υπηρεσίες που προσφέρονται στο δίκτυο. Μερικές από αυτές είναι οι παρακάτω:

4.3.1 Διακομιστές Ιστού

Ένας Διακομιστής Ιστού είναι το λογισμικό που είναι υπεύθυνο για την αποδοχή αιτημάτων HTTP από πελάτες, γνωστά και ως φυλλομετρητές Ιστού, και να στέλνουν απαντήσεις HTTP μαζί με προαιρετικά περιεχόμενα δεδομένων, τα οποία συνήθως είναι Ιστοσελίδες όπως αρχεία HTML και συνδεδεμένα αντικείμενα (εικόνες, κλπ.). Ο Apache είναι ο πιο διαδεδομένος Διακομιστής Ιστού σε συστήματα Linux. Οι Διακομιστές Ιστού χρησιμοποιούνται για να υπηρετούν Σελίδες Ιστού που ζητούνται από πελάτες υπολογιστές. Οι πελάτες τυπικά ζητούν και βλέπουν Σελίδες Ιστού

χρησιμοποιώντας εφαρμογές Φυλλομετρητών Ιστού όπως οι Firefox, Opera, ή Mozilla. Το πιο κοινό πρωτόκολλο που χρησιμοποιείτε για τη μεταφορά ιστοσελίδων είναι το Πρωτόκολλο Μεταφοράς Υπερκειμένου (Hyper Text Transfer Protocol (HTTP)). Πρωτόκολλα όπως το HTTP πάνω από το Στρώμα Ασφαλούς Υποδοχής (Secure Sockets Layer (HTTPS)), και το Πρωτόκολλο Μεταφοράς Αρχείων (File Transfer Protocol (FTP)), ένα πρωτόκολλο για την αποστολή και λήψη αρχείων, υποστηρίζονται επίσης. Οι Διακομιστές Ιστού Apache συχνά χρησιμοποιούνται σε συνδυασμό με τη μηχανή βάσης δεδομένων MySQL, τη γλώσσα σεναρίου Προεπεξεργαστή Υπερκειμένου (PHP), και άλλες δημοφιλείς γλώσσες σεναρίου όπως οι Python και Perl. Αυτή η σύνθεση ονομάζεται LAMP (Linux, Apache, MySQL and Perl/Python/PHP) και σχηματίζει μια ισχυρή και αυτοδύναμε πλατφόρμα για την ανάπτυξη εφαρμογών βασισμένες στον Ιστό.

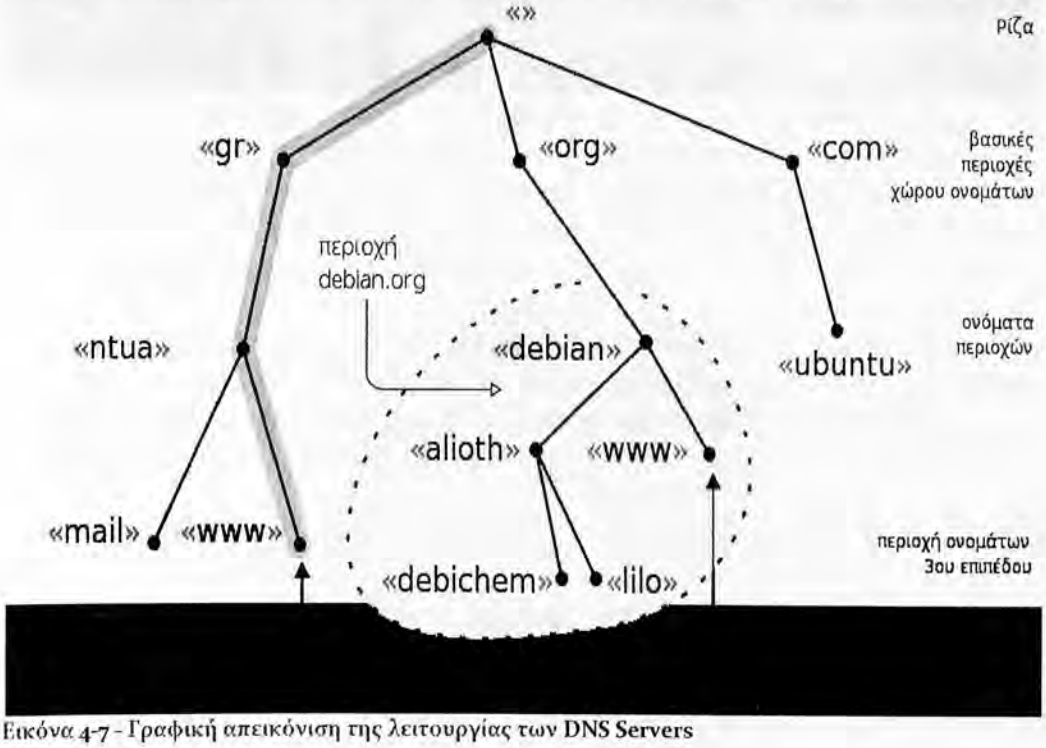
4.3.2 DNS Servers

Το σύστημα DNS προέκυψε επειδή στους ανθρώπους ονόματα σημαίνουν περισσότερα από αριθμητικές διευθύνσεις αλλά στην συνέχεια το σύστημα DNS απέκτησε και άλλες χρήσεις εξίσου σημαντικές. Μια πολύ σημαντική υπηρεσία στο awmn είναι οι dns servers, ο λόγος είναι ότι ο κάθε dns server θα πρέπει να έχει ρυθμιστεί έτσι ώστε να κάνει resolve τους dns του awmn αλλά ταυτόχρονα θα πρέπει να μπορεί να κάνει resolve και τους dns του internet, αυτό εξυπηρετεί ώστε ο κάθε κόμβος να χρησιμοποιεί ένα dns server για όλα.

Ο χώρος ονομάτων τομέων (Domain Name Space) του DNS είναι δομημένος ιεραρχικά σε δενδρική δομή, με τα ονόματα να φέρουν πληροφορία που αντανακλά τη θέση τους στη δομή αυτή. Ο χώρος ονομάτων DNS ενός ιδιωτικού δικτύου, όπως το awmn, μπορεί να διαφέρει με τον χώρο ονομάτων DNS του Διαδικτύου ή κάποιου άλλου διαδικτύου. Η αντιστοίχιση ονομάτων με αριθμητικές διευθύνσεις προέκυψε επειδή οι αριθμητικές διευθύνσεις IP δεν είναι εύχρηστες από τους ανθρώπους. Οι άνθρωποι αποδίδουν σημασία και θυμούνται ευκολότερα ονόματα.

Οι χώροι ή περιοχές ή τομείς (domains) χωρίζονται σε επίπεδα, και κάθε επίπεδο συχνά περιέχει κατώτερα επίπεδα, για παράδειγμα ένας τομέας πρώτου επιπέδου μπορεί να περιέχει ιεραρχικά τομείς δεύτερου επιπέδου κτλ. Η αλλαγή επιπέδου των ονομάτων χώρου είναι πολλές φορές ισοδύναμη με αλλαγή ζώνης DNS (DNS zone). Χρησιμοποιώντας την ορολογία που χρησιμοποιείται στην δενδρική δομή η ζώνη DNS είναι ένας κόμβος και ένα όνομα χώρου είναι ένα φύλλο. Όλες οι ζώνες DNS είναι και ονόματα χώρου αλλά το αντίστροφο δεν ισχύει πάντα. Στην πράξη οι ζώνες DNS είναι τα φυσικά αρχεία που βρίσκονται σε εξυπηρετητές DNS και περιέχουν τις αντιστοιχίσεις ονομάτων και διευθύνσεων ή άλλων ονομάτων ως εγγραφές

DNS (DNS records ή resource records). Δηλαδή οι ζώνες DNS είναι απλές βάσεις δεδομένων και οι εγγραφές DNS είναι τα δεδομένα.



Εικόνα 4-7 - Γραφική απεικόνιση της λειτουργίας των DNS Servers

Πχ. μια ζώνη DNS είναι η ζώνη ietf.org που περιέχει όλες τις εγγραφές DNS για το όνομα χώρου του ietf.org. Για διαχειριστικούς και λογιστικούς λόγους ο διαχειριστής της ζώνης ietf.org δημιούργησε τη ζώνη tools.ietf.org και έδωσε το δικαίωμα της διαχείρισης των εγγραφών DNS στον χώρο ονομάτων tools.ietf.org σε κάποιον άλλο διαχειριστή συστημάτων. Άλλη μια ζώνη DNS είναι η ζώνη com. Ο Διαχειριστής της ζώνης com δημιούργησε τη ζώνη example.com και έδωσε τον έλεγχο της στον IANA. Τώρα ο IANA ελέγχει όλες τις εγγραφές DNS για τον χώρο ονομάτων example.com.

4.3.3 FTP Servers

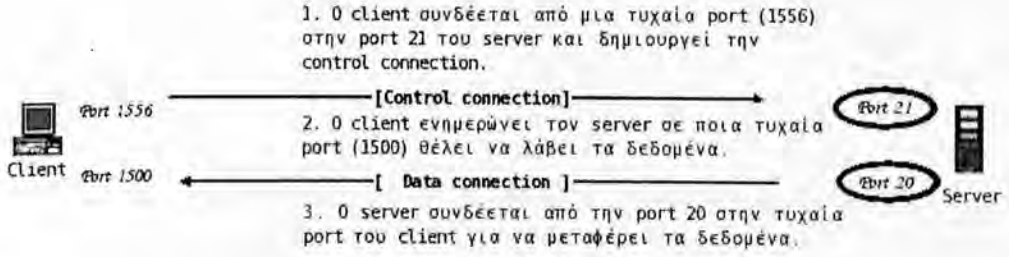
Το File Transfer Protocol (FTP), (ελληνικά: Πρωτόκολλο Μεταφοράς Αρχείων) είναι ένα ευρέως χρησιμοποιούμενο πρωτόκολλο σε δίκτυα τα οποία υποστηρίζουν το πρωτόκολλο TCP/IP (δίκτυα όπως internet ή intranet). Είναι από τα πρώτα πρωτόκολλα που χρησιμοποιήθηκαν στο awmn αφού όπως έχουμε αναφέρει παραπάνω η πρώτη ανάγκη που οδήγησε στην δημιουργία του ήταν η μεταφορά αρχείων. Ο υπολογιστής που τρέχει εφαρμογή FTP client μόλις συνδεθεί με τον server μπορεί να εκτελέσει ένα πλήθος διεργασιών όπως ανέβασμα αρχείων στον server, κατέβασμα αρχείων από τον server, μετονομασία ή διαγραφή αρχείων από τον server κ.ο.κ. Το

πρωτόκολλο είναι ένα ανοιχτό πρότυπο. Είναι δυνατό κάθε υπολογιστής που είναι συνδεδεμένος σε ένα δίκτυο, να διαχειρίζεται αρχεία σε ένα άλλο υπολογιστή του δικτύου, ακόμη και εάν ο δεύτερος διαθέτει διαφορετικό λειτουργικό σύστημα.

Αρχικά ο FTP server ανοίγει την θύρα (port) 21 περιμένοντας έναν FTP client να συνδεθεί. Στη συνέχεια ο client ξεκινά μια νέα σύνδεση από μια τυχαία θύρα προς την θύρα 21 του server. Μόλις γίνει η σύνδεση παραμένει ανοιχτή για όλη τη διάρκεια της συνόδου FTP. Η συγκεκριμένη σύνδεση ονομάζεται σύνδεση ελέγχου (control connection).

Έπεται η δημιουργία της σύνδεσης δεδομένων (data connection), της σύνδεσης με την οποία μεταφέρονται τα δεδομένα. Υπάρχουν δύο τρόποι για να δημιουργηθεί, με χρήση της ενεργητικής λειτουργίας (active mode) ή με χρήση της παθητικής λειτουργίας (passive mode).

Active mode

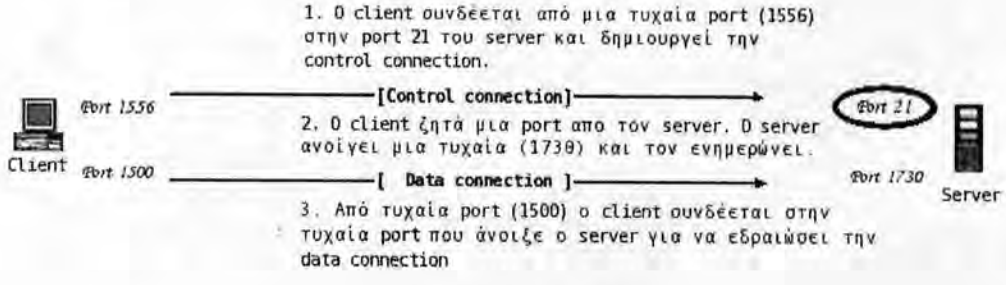


Active mode

Εικόνα 4-8 - **FTP Handshake(Active Mode)**

Στην ενεργητική λειτουργία (active mode) ο FTP client διαλέγει μια τυχαία θύρα στην οποία δέχεται τα δεδομένα της σύνδεσης. Ο client στέλνει τον αριθμό της θύρας, στην οποία επιθυμεί να "ακούει" (listen) για εισερχόμενες συνδέσεις. Ο FTP server δημιουργεί μια σύνδεση από την θύρα 20 στην ανοιχτή θύρα του client για τη μεταφορά των δεδομένων. Οποιαδήποτε πληροφορία ζητήσει ο client, ανταλλάσσεται με βάση αυτή τη σύνδεση, που βασίζεται στο TCP. Όταν η μεταφορά ολοκληρωθεί ο server κλείνει τη σύνδεση αποστέλλοντας ένα πακέτο FIN, όπως σε κάθε σύνδεση βασισμένη στο TCP. Κάθε φορά που ο client ζητάει δεδομένα, δημιουργείται κατά παρόμοιο τρόπο μια σύνδεση δεδομένων και η διαδικασία επαναλαμβάνεται.

Passive mode



Passive mode

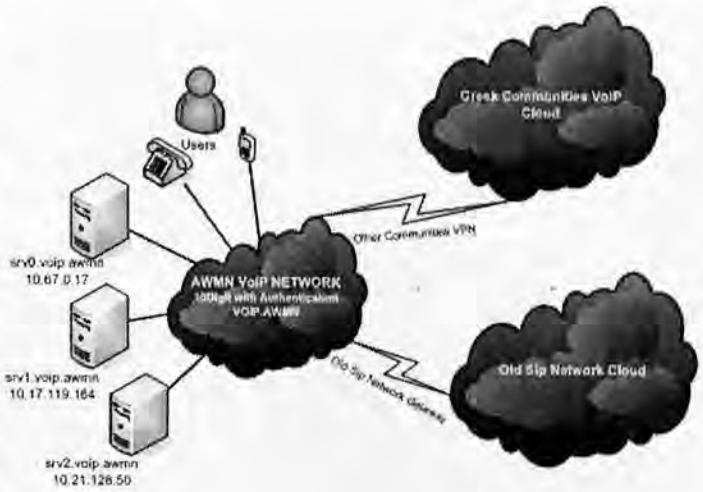
Εικόνα 4-9 - FTP Handshake(Passive Mode)

Στην παθητική λειτουργία (passive mode) ο client ζητά από τον server να διαλέξει μια τυχαία θύρα, στην οποία θα "ακούει" (listen) για την σύνδεση δεδομένων (data connection). Ο server ενημερώνει τον client για την θύρα την οποία έχει διαλέξει και ο client συνδέεται σε αυτή για τη μεταφορά των δεδομένων. Η μεταφορά ολοκληρώνεται όπως και στην ενεργητική λειτουργία (active mode), αφού η σύνδεση δεδομένων βασίζεται στο TCP.

4.3.4 VoIP Servers

Οι υπηρεσίες τηλεφωνίας έχουν αποκτήσει πολλούς υποστηρικτές τα τελευταία χρόνια. Ένας από αυτούς και μάλιστα φανατικούς είναι το awmn. Στην αρχή με την χρήση του H.323 πρωτοκόλλου και έπειτα με το SIP, πολλοί κόμβοι φιλοξενούν VoIP Servers και παρέχουν υπηρεσίες τηλεφωνίας στα υπόλοιπα μέλη. Το Voice over IP ή VoIP ή τηλεφωνία μέσω διαδικτύου ή σωστότερα ΦεΔΠ δηλαδή "Φωνή επί διαδικτυακού πρωτοκόλλου", χαρακτηρίζει μια ομάδα πρωτοκόλλων-τεχνολογιών (H.323, SIP), η οποία προσφέρει φωνητική συνομιλία σε πραγματικό χρόνο με πολύ καλή ποιότητα πλέον και στην ουσία χωρίς κόστος. Οι συνομιλίες αυτές παραδοσιακά γίνονταν αποκλειστικά μέσω PC που ήταν συνδεδεμένο με το Διαδίκτυο (Internet) και διέθετε μικρόφωνο, ακουστικά και το κατάλληλο λογισμικό. Η κλήση κατέληγε σε ένα άλλο, ανάλογα εξοπλισμένο, PC χωρίς να υπάρχει κάποια επιπλέον χρέωση, εκτός από αυτή της πρόσβασης στο Διαδίκτυο, αφού στη συγκεκριμένη επικοινωνία δεν μεσολαβεί κάποιος παραδοσιακός φορέας τηλεπικοινωνιών (π.χ. ΟΤΕ) παρά μόνο το Διαδίκτυο.

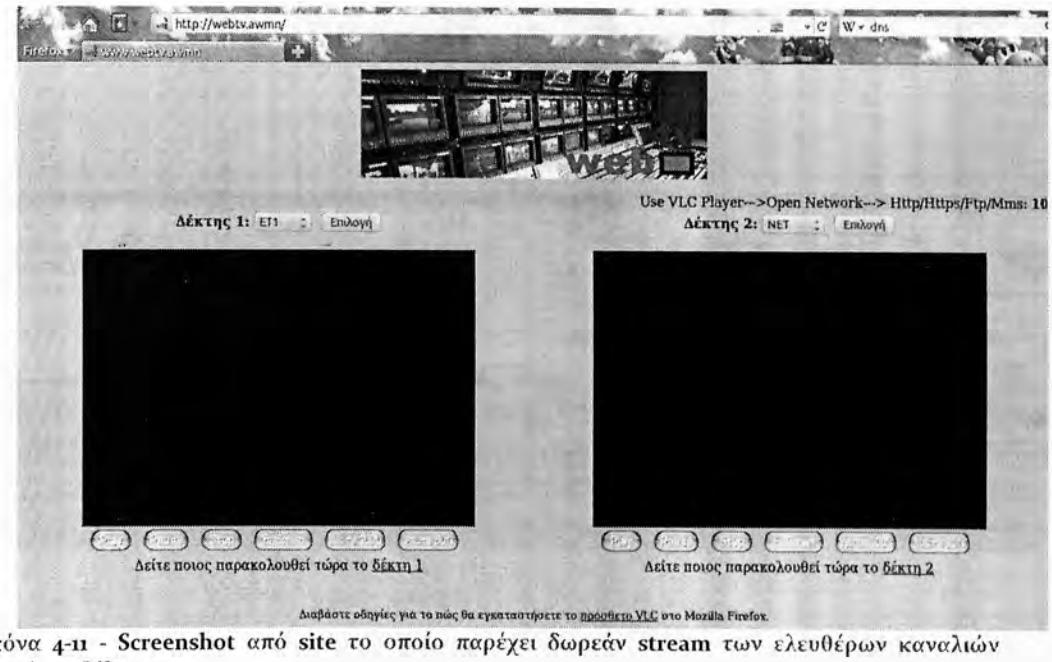
Τον τελευταίο καιρό έχουν εμφανιστεί οι λεγόμενοι εναλλακτικοί (ιντερνετικοί) τηλεπικοινωνιακοί φορείς, οι οποίοι προσφέρουν προώθηση των κλήσεων VoIP σε σταθερά δίκτυα τηλεπικοινωνιών σε εξαιρετικά χαμηλό κόστος, αλλά όχι το αντίστροφο. Μερικοί εξ αυτών έχουν παρουσιάσει και ειδικές τηλεφωνικές συσκευές USB VoIP, οι οποίες συνεργάζονται με το αντίστοιχο λογισμικό στον Η/Υ και καθιστούν τις κλήσεις μέσω Διαδικτύου σαφώς πιο λειτουργικές. Σήμερα υπάρχει πληθώρα εφαρμογών, συμπεριλαμβανομένων των Asterisk servers, οι οποίες προσφέρουν τηλεφωνία μέσω διαδικτύου. Το πιο ευρέως διαδεδομένο από τα παραπάνω είναι το Asterisk, το οποίο είναι δωρεάν λογισμικό και διέπεται από τους όρους χρήσης του GNU. Τα τηλεφωνικά κέντρα αυτά αναλαμβάνουν να μετατρέψουν την τηλεφωνία σε μια τηλεφωνία χωρίς κόστος χρήσης.



Εικόνα 4-10 - Τοπολογία VoIP δικτύου στο AWMN

4.3.5 Audio & Video Streaming

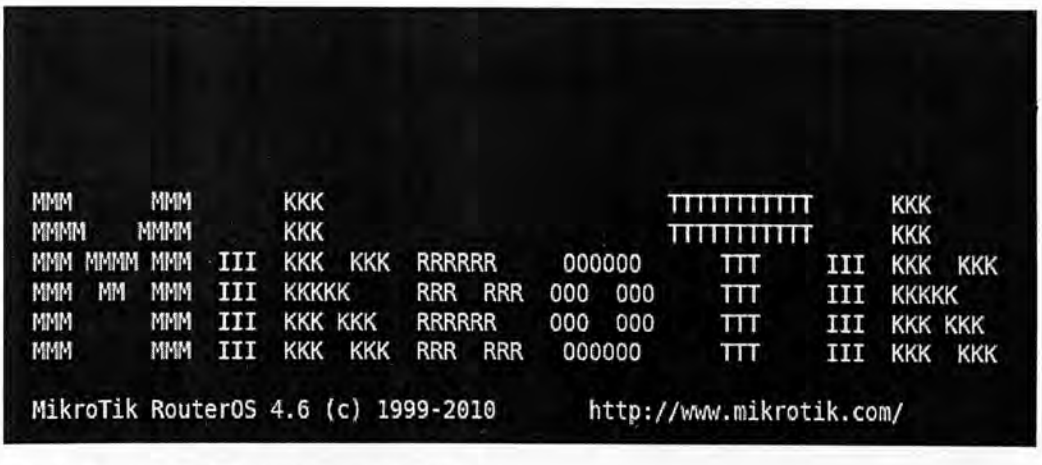
Το streaming είναι μια υπηρεσία που λόγω των υψηλών ρυθμών μετάδοσης, βρήκε πρόσφορο έδαφος στο awmn. Μέσω streaming δίνεται η δυνατότητα να πραγματοποιείται real-time μία μετάδοση ήχου και εικόνας μέσω του δικτύου. Υπάρχουν λοιπόν υπηρεσίες που αναμεταδίδουν τα Ελληνικά κανάλια της τηλεόρασης και μπορεί κάποιος να τα παρακολουθεί από τον υπολογιστή του, χωρίς την χρήση τηλεόρασης.



Εικόνα 4-11 - **Screenshot** από **site** το οποίο παρέχει δωρεάν **stream** των ελευθέρων καναλιών εθνικής εμβέλειας

Υπάρχουν επίσης και αντίστοιχες υπηρεσίες που κάνουν sreaming ραδιόφωνα κλπ.

5 ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΗ ΚΕΝΤΡΙΚΟΥ ROUTER



Εικόνα 5-1 - Η αρχική σελίδα του router μέσω ssh

5.1 Interfaces

Παρακάτω βλέπουμε την λίστα με τα εννέα διαθέσιμα Interfaces του κεντρικού router.

$interface print detail

Flags: D - dynamic, X - disabled, R - running, S - slave
0 X name="ether1" type="ether" mtu=1500

1 R name="2_Tei LAN" type="ether" mtu=1500 l2mtu=1522

2 R name="3_AP_LAN" type="ether" mtu=1500 l2mtu=1522

3 R name="4_SERVER" type="ether" mtu=1500 l2mtu=1522

4 R name="5_NS5-AWMN" type="ether" mtu=1500 l2mtu=1522

5 name="6_Test" type="ether" mtu=1500 l2mtu=1522

6 X name="ether7" type="ether" mtu=1500

7 X name="ether8" type="ether" mtu=1500

8 X name="ether9" type="ether" mtu=1500

9 X name="wlan1" type="wlan" mtu=1500

Επίσης, τα Ethernet Interfaces μπορούν να προβληθούν και με την παρακάτω, πιο αναλυτική μορφή (έχουν καλυφθεί οι MAC-Addresses)

$interface Ethernet print detail

Flags: X - disabled, R - running, S - slave
0 X name="ether1" mtu=1500 mac-address=[redacted] arp=enabled auto-negotiation=yes full-duplex=yes speed=100Mbps

1 R name="2_Tei LAN" mtu=1500 l2mtu=1522 mac-address=[redacted] arp=enabled auto-negotiation=yes full-duplex=yes speed=100Mbps master-port=none
bandwidth=unlimited/unlimited switch=switch1

2 R name="3_AP_LAN" mtu=1500 l2mtu=1522 mac-address=[redacted] arp=enabled auto-negotiation=yes full-duplex=yes speed=100Mbps master-port=none
bandwidth=unlimited/unlimited switch=switch1

3 R name="4_SERVER" mtu=1500 l2mtu=1522 mac-address=[redacted] arp=enabled auto-negotiation=yes full-duplex=yes speed=100Mbps master-port=none
bandwidth=unlimited/unlimited switch=switch1

4 R name="5_NS5-AWMN" mtu=1500 l2mtu=1522 mac-address=[redacted] arp=enabled auto-negotiation=yes full-duplex=yes speed=100Mbps master-port=none
bandwidth=unlimited/unlimited switch=switch1

5 name="6_Test" mtu=1500 l2mtu=1522 mac-address=[redacted] arp=enabled auto-negotiation=yes full-duplex=yes speed=100Mbps master-port=none
bandwidth=unlimited/unlimited switch=switch1

6 X name="ether7" mtu=1500 mac-address=[redacted] arp=enabled auto-negotiation=yes full-duplex=yes speed=100Mbps master-port=none
bandwidth=unlimited/unlimited switch=switch1

7 X name="ether8" mtu=1500 mac-address=[redacted]
arp=enabled auto-negotiation=yes full-duplex=yes speed=100Mbps master-port=none
bandwidth=unlimited/unlimited switch=switch1

8 X name="ether9" mtu=1500 mac-address=[redacted]

5.2 Διευθύνσεις IP (έχουν υποκρυφθεί)

$ip address print detail

Flags: X - disabled, I - invalid, D - dynamic
0 ;;; AP IP
address=[redacted]network=[redacted]
broadcast=[redacted]interface=3_AP_LAN actual-interface=3_AP_LAN

1 ;;; LAN IP
address=[redacted]network=[redacted]
broadcast=[redacted] interface=2_Tei LAN actual-interface=2_Tei LAN

2 ;;; Nanostation 5
address=[redacted] network=[redacted]
broadcast=[redacted] interface=5_NS5-AWMN actual-interface=5_NS5-AWMN

3 ;;; Server IF
address=[redacted] network=[redacted]
broadcast=[redacted] interface=4_SERVER actual-interface=4_SERVER

4 address=[redacted]network=[redacted]
broadcast=[redacted]interface=2_Tei LAN actual-interface=2_Tei LAN

5.3 ROUTES

$ip route print detail

Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme, B - blackhole, U - unreachable, P - prohibit

0 A S ;;; added by setup
dst-address=0.0.0.0/0 pref-src=[redacted] gateway=[redacted] gateway-status=[redacted] reachable 2_Tei LAN check-gateway=ping distance=1
scope=255 target-scope=10

1 A S dst-address=[redacted] gateway=[redacted] gateway-status=[redacted] reachable 5_NS5-AWMN check-gateway=ping distance=1 scope=30 target-scope=10

2 ADC dst-address=[redacted] pref-src=[redacted] gateway=5_NS5-AWMN gateway-status=5_NS5-AWMN reachable distance=0 scope=10

3 ADC dst-address=172[redacted] pref-src=[redacted] gateway=2_Tei LAN gateway-status=2_Tei LAN reachable distance=0 scope=10

4 ADC dst-address=[redacted] pref-src=[redacted] gateway=4_SERVER gateway-status=4_SERVER reachable distance=0 scope=10

5 ADC dst-address=[redacted] pref-src=[redacted] gateway=3_AP_LAN gateway-status=3_AP_LAN reachable distance=0 scope=10

Επειδή ο router διαχειρίζεται δύο local ip και κατ' επέκταση, δύο public ip έχουμε φτιάξει ένα τα παρακάτω rules για να μπορούμε να κάνουμε netmap τις δύο αυτές διευθύνσεις.

$ip firewall mangle print

Flags: X - disabled, I - invalid, D - dynamic
0 ;;; autonet-group Gateway
chain=prerouting action=mark-routing new-routing-mark=autonet-group passthrough=no src-address=[redacted]

1 ;;; autocom-group Gateway
chain=prerouting action=mark-routing new-routing-mark=autocom-group passthrough=no src-address=[redacted]

2 ;;; autocom-group Gateway
chain=prerouting action=mark-routing new-routing-mark=vpn-group passthrough=no src-address=[redacted]

5.4 PACKET PROCCESING

5.4.1 NAT

Για τις ανάγκες του Hotspot και για την διασφάλιση της ασφάλειας, έχουμε φτιάξει το παρακάτω NAT.

$ip firewall nat print detail

Flags: X - disabled, I - invalid, D - dynamic
0 ;;; masquerade hotspot network for AWMN
chain=srcnat action=masquerade src-address=[redacted] dst-address=10.0.0.0/8 out-interface=5_NS5-AWMN

1 ;;; masquerade server network for AWMN
chain=srcnat action=masquerade src-address=[redacted] dst-address=10.0.0.0/8 out-interface=5_NS5-AWMN

2 ;;; masquerade VPN network for AWMN

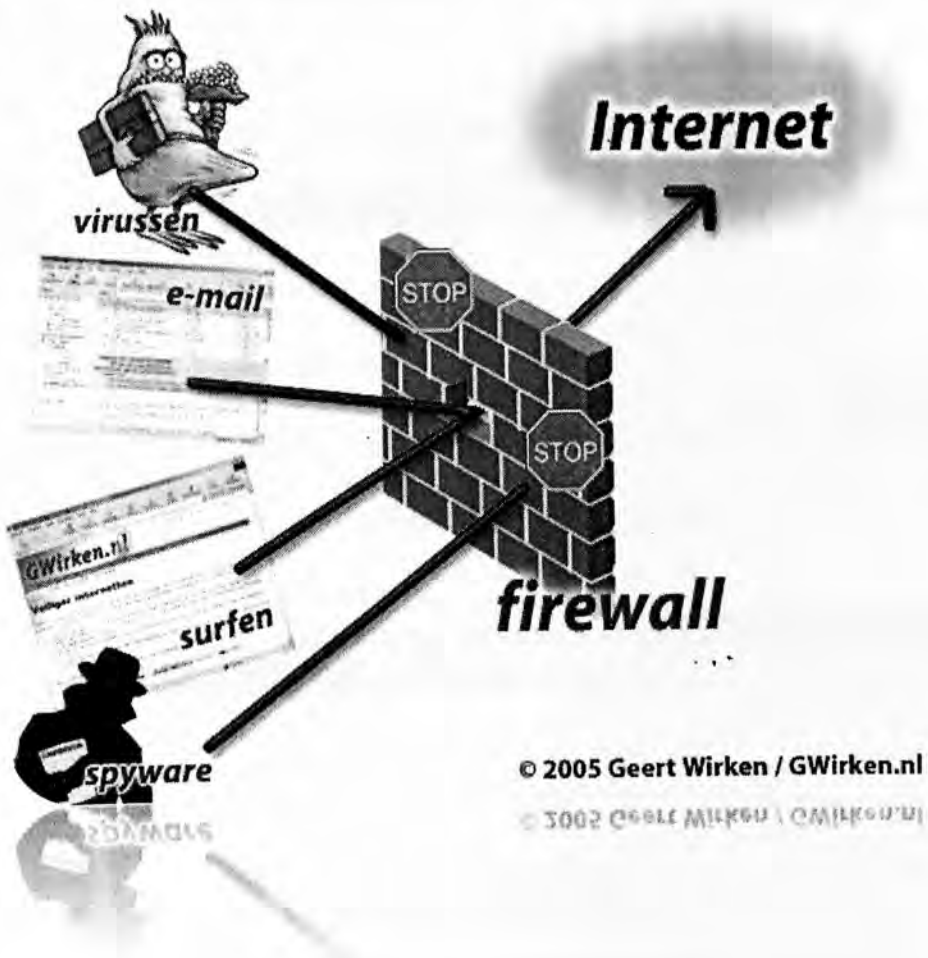
chain=srcnat action=masquerade src-address=[redacted] dst-address=10.0.0.0/8 out-interface=5_NS5-AWMN

3 ;;; masquerade hotspot network
chain=srcnat action=netmap to-addresses=[redacted] src-address=[redacted] out-interface=2_Tei LAN

4 ;;; masquerade server network
chain=srcnat action=netmap to-addresses=[redacted] src-address=[redacted] out-interface=2_Tei LAN

5 ;;; place hotspot rules here
chain=unused-hs-chain action=passthrough

5.4.2 Firewall



$filter print detail

Flags: X - disabled, I - invalid, D - dynamic

1 X ;;; place hotspot rules here
chain=unused-hs-chain action=passthrough

Για λόγους ασφαλείας, καταγράφουμε σε Address List την src και την dst ip κάθε πακέτου που έρχεται από το hotspot και πάει προς κάποια εσωτερική ip του δικτύου του ΤΕΙ. Με αυτόν τον τρόπο διασφαλίζεται ότι κανένας δεν μπορεί να έχει πρόσβαση προς το δίκτυο του ΤΕΙ και ταυτόχρονα, καταγράφουμε αυτούς που προσπαθούν.

1 ;;; Address SRC list for Atempters
chain=forward action=add-src-to-address-list src-address=[redacted] dst-address=[redacted] address-list=Atempts to TeiLan
address-list-timeout=0s

2 ;;; Address DST list for Atempters
chain=forward action=add-dst-to-address-list src-address=[redacted] dst-address=[redacted] address-list=Atempts to TeiLan
address-list-timeout=0s

3 ;;; Block TeiLan from AP
chain=forward action=accept src-address=[redacted] dst-address=[redacted] src-address-list=Atempts to TeiLan

Στα προηγούμενα rules καταγράφουμε, και στο επόμενο κάνουμε drop τα πακέτα.

4 ;;; Block TeiLan from AP
chain=forward action=drop src-address=[redacted] dst-address=[redacted] src-address-list=Atempts to TeiLan

Στα επόμενα 3 roules υλοποιείται η εξής λειτουργία.

Υπάρχει μία μέθοδος hacking που ονομάζεται bruteforce attack. Αυτή δεν είναι τίποτε άλλο απο το να δοκιμάζει ο εισβολέας κλειδιά, μέχρι κάποια στιγμή

αφού έχει κάνει όλους τους δυνατούς συνδυασμούς, να καταφέρει να μπει στο σύστημα μας. Στα 3 παρακάτω rules λοιπόν, εάν προσπαθήσει κάποιος να μας κάνει bruteforce, στον τρίτο λάθος κωδικό που δοκιμάζει μέσα σε τρία λεπτά, κάνουμε ban την ip του, και ότι πακέτο και να μας στέλνει, γίνεται drop και έτσι δεν μπορεί να δοκιμάσει άλλους κωδικούς, για τις επόμενες 3 ημέρες, μέχρι να λήξει το ban time.

5 ;;; Dynamic Ban for Bruteforce FTP Attack
chain=input action=drop protocol=tcp src-address-list=ftp_blacklist dst-port=21

6 chain=output action=accept protocol=tcp content=530 Login incorrect dst-limit=1/1m,2,dst-address/1m

7 chain=output action=add-dst-to-address-list protocol=tcp address-list=ftp_blacklist address-list-timeout=3d content=530 Login incorrect

Αντίστοιχη υλοποίηση, έχει γίνει και για το bruteforce για την πόρτα που χρησιμοποιούμε για το configuration του router.

Εδώ κάνουμε το ίδιο σχεδόν με το παραπάνω rule άλλα για το winbox, το configuration tool του mikrotik. Εδώ η διαδικασία γίνεται σε τρία επίπεδα, με την μόνη διαφορά, ότι εδώ, ακόμα και αν είναι επιτυχής η σύνδεση, αν γίνει 3 φορές μέσα σε 3 λεπτά, να το κάνει και πάλι ban καθώς επίσης να κρατάει και ένα ιστορικό με τις ip που συνδέθηκαν στο router. Με αυτόν τον τρόπο ελαχιστοποιείται ο κίνδυνος να hackάρει κάποιος το router μας και να αποκτήσει πρόσβαση στην παραμετροποίηση του.

8 ;;; Drop winbox bruteforce
chain=input action=drop protocol=tcp src-address-list=wb_blacklist dst-port=[redacted]

9 ;;; Winbox bruteforce blacklisting
chain=input action=add-src-to-address-list connection-state=new protocol=tcp src-address-list=wb_stage3 address-list=wb_blacklist
address-list-timeout=1w3d dst-port=[redacted]

10 ;;; Winbox brute force the third state
chain=input action=add-src-to-address-list connection-state=new protocol=tcp src-address-list=wb_stage2 address-list=wb_stage3 address-list-timeout=1m
dst-port=[redacted]

11 ;;; Winbox brute forcers the second state

chain=input action=add-src-to-address-list connection-state=new protocol=tcp src-address-list=wb_stage1 address-list=wb_stage2 address-list-timeout=1m
dst-port=[redacted]

12 ;;; Winbox bruteforcers the first state
chain=input action=add-src-to-address-list connection-state=new protocol=tcp address-list=wb_stage1 address-list-timeout=1m dst-port=[redacted]

13 ;;; GENERAL WINBOX FROM BRUTEFORCE PROTECTION Winbox Bruteforce Safe List
chain=input action=add-src-to-address-list connection-state=new protocol=tcp address-list=safe address-list-timeout=0s dst-port=[redacted]

Εδώ μπλοκάρουμε κάποια ενδεχόμενη επίθεση, ερχόμενη απο το awmn η οποία προσπαθεί να βγει στο internet.

14 ;;; Drop awmn to internet
chain=forward action=drop in-interface=5_NS5-AWMN out-interface=2_Tei LAN

5.4.3 Hotspot

Παρακάτω φαίνεται το setup του hotspot με το hotspot tool του mikrotik.

ip hotspot print detail
Flags: X - disabled, I - invalid, S - HTTPS
0 name="hotspot1" interface=3_AP_LAN address-pool=Pool for AP profile=default idle-timeout=5m keepalive-timeout=none addresses-per-mac=2
proxy-status="running"

5.4.4 Hotspot Profiles

$ip hotspot profile print detail

Flags: * - default
0 * name="default" hotspot-address=[redacted] dns-name="" html-directory=hotspot rate-limit="" http-proxy=[redacted] smtp-server=[redacted] login-by=http-pap
split-user-domain=no use-radius=yes radius-accounting=yes radius-interim-update=received nas-port-type=Ethernet radius-default-domain=""

radius-location-id="" radius-location-name="" radius-mac-format=XX:XX:XX:XX:XX:XX

Επειδή στο δίκτυο του Hotspot έχουμε συσκευές που δεν θέλουμε να κάνουνε login αλλά να μπαίνουνε ελεύθερα (πχ: Access Points), έχουμε σετάρει τα παρακάτω rules και τα κάνουμε ban. Αυτό είναι ασφαλές διότι τα αναγνωρίζουμε – ταυτοποιούμε απο ip και απο mac-address (ip-binding).

$ip hotspot ip-binding print detail

Flags: X - disabled, P - bypassed, B - blocked
0 P ;;; Acess Point 1 (Isogeio Aithouses Anamesa)
mac-address=[redacted] address=[redacted] server=hotspot1 type=bypassed

1 P ;;; Acess Point 2 (Isogeio Kylikeio)
mac-address=[redacted] address=[redacted] server=hotspot1 type=bypassed

2 P ;;; Acess Point 3 (1os Orofos)
mac-address=[redacted] address=[redacted] server=hotspot1 type=bypassed

3 P ;;; NanoStation 2 (Proavlio-Mpasketes)
mac-address=[redacted] address=[redacted] server=hotspot1 type=bypassed

4 P ;;; Acess Point 4 (2os Akalyptos Xoros)
mac-address=00[redacted] address=[redacted] server=hotspot1 type=bypassed

5 P ;;; Acess Point 5 (2os Eksw apo erg diktya)
mac-address=[redacted] address=[redacted] server=hotspot1 type=bypassed

6 P ;;; NanoStation 5
mac-address=[redacted] address=[redacted] server=hotspot1 type=bypassed

5.4.5 Dhcp Server

$dhcp-server print detail

Flags: X - disabled, I - invalid
0 name="AP dhcp" interface=3_AP_LAN lease-time=1d address-pool=Pool for AP bootp-support=static authoritative=after-2sec-delay

1 name="Server DHCP" interface=4_SERVER lease-time=3d address-pool=dhcp_local_server bootp-support=static authoritative=after-2sec-delay

5.4.6 IP Pools

$pool print detail

0 name="Pool for AP" ranges=[redacted]

1 name="dhcp_local_server" ranges=[redacted]

5.4.7 Radius Server για την ταυτοποίηση των χρηστών

$radius print detail

Flags: X - disabled
0 service=hotspot called-id="" domain="" address=[redacted] secret="****" authentication-port=[redacted] accounting-port=[redacted] timeout=[redacted]
accounting-backup=no realm=""

5.5 NETWATCH

Επειδή τα συστήματα πληροφορικής συνήθως πεθαίνουν λόγω έλλειψης συντήρησης, και επειδή στην δικά μας περίπτωση δεν θα θέλαμε να συμβεί αυτό, έχουμε φτιάξει ένα σύστημα ειδοποιήσεων με e-mail καθώς επίσης και logging, για να εποπτεύουμε κάποια κρίσιμα σημεία του δικτύου. Οι έλεγχοι αυτοί φαίνονται παρακάτω.

$netwatch print detail

Flags: X - disabled

Κάνουμε έναν έλεγχο στον κεντρικό router του ΤΕΙ για να γράφουμε σε log πότε είναι up και πότε down.

```
 0 X ;;; Gateway teipir
     host=[redacted] timeout=1s interval=5s since=jan/01/2002
03:00:04 status=unknown up-script=:log warning "GATEWAY is UP"
     down-script=:log error "GATEWAY is DOWN"
```

Κάνουμε έναν έλεγχο στο google.gr θεωρώντας ότι είναι ένα site με πολύ καλό redatancy, για να γράφουμε σε log εάν βλέπουμε internet μετά τον κεντρικό router του ΤΕΙ.

```
 1 X ;;; Google.gr
     host=74.125.77.104 timeout=10s interval=10s since=jan/01/2002
03:00:04 status=unknown up-script=:log warning "Google.gr is UP"
     down-script=:log error "Google.gr is DOWN"
```

Για να μπορέσουμε με κάποιο τρόπο να εποπτεύσουμε την φυσική ασφάλεια των συσκευών που έχουμε τοποθετήσει(Access Points, switches κλπ) έχουμε φτιάξει τα παρακάτω roules που κάνουν ping κάθε 10s όλες αυτές τις συσκευές, στην περίπτωση που δεν απαντήσει κάποια, τότε στέλνουν mail και ενημερώνουν για αυτήν την απουσία, καθώς επίσης το σημείο που βρίσκεται αυτή η συσκευή και την ώρα – ημερομηνία που αντιλήφθηκε ο router την απουσία. Με αυτόν τον τρόπο, μπορούμε να ξέρουμε εάν όλα είναι στην θέση τους, καθώς επίσης και μία ένδειξη ότι δουλεύουν σωστά.

```
 2 X ;;; Acess Point 1 (Isogeio Aithouses Anamesa)
     host=[redacted]timeout=1m interval=10s since=jan/01/2002
03:00:04 status=unknown up-script=:log warning "AP1 is UP"\r\n\r\n
```

down-script=\r\n:log error "AP1 is DOWN"\r\n\r\n /tool e-mail send tls=yes to="[redacted]m" subject= "A HOST IS DOWN" body= ("Afto einai ena

aftomatopoihmeno e-mail pou sas pliroforei oti to Access Point pou vrisketai sto Isogeio anamesa stis dyo megales aithouses einai DOWN. Apo

tis ".\ ([/system clock get date]).\ " kai wra ".\ ([/system clock get time]))\r\n\r\n

3 X ;;; Yahoo.com
host=87.248.122.122 timeout=1s interval=10s since=jan/01/2002 03:00:04 status=unknown up-script=:global yahoo "up" down-script=:global yahoo "down"

4 ;;; Hol.gr
host=195.97.21.22 timeout=300ms interval=1m since=aug/11/2011 22:48:00 status=up up-script=:global hol "up" down-script=:global hol "down"

5 X ;;; Google.com
host=209.85.135.104 timeout=300ms interval=1m since=jan/01/2002 03:00:04 status=up up-script=:global google "down"
down-script=:global google "down"

6 X ;;; SERVER
host=[redacted] timeout=1s interval=1s since=jan/01/2002 03:00:04 status=up up-script=:log warning "SERVER is UP"
down-script=:log error "SERVERr is DOWN"\r\n\r\n/tool e-mail send tls=yes to="[redacted]" subject= "A HOST IS DOWN" body= ("Afto einai ena

aftomatopoihmeno e-mail pou sas pliroforei oti o SERVER ([redacted]) einai DOWN. Apo tis ".\ ([/system clock get date]).\ " kai wra

".\ ([/system clock get time]))

7 X ;;; Acess Point 2 (Isogeio Kylikeio)
host=[redacted]timeout=1m interval=10s since=jan/01/2002 03:00:04 status=up up-script=:log warning "AP2 is UP"
down-script=:log error "AP2 is DOWN"\r\n\r\n/tool e-mail send tls=yes to="[redacted]" subject= "A HOST IS DOWN" body= ("Afto einai ena

aftomatopoihmeno e-mail pou sas pliroforei oti to Access Point pou vrisketai sto Isogeio ston xwro tou kylikeiou einai DOWN. Apo tis ".\

([/system clock get date]).\ " kai wra ".\ ([/system clock get time]))

8 X ;;; Acess Point 4 (2os Akalyptos Xoros)
host=[redacted] timeout=1m interval=10s since=jan/01/2002 03:00:04 status=up up-script=:log warning "AP4 is UP"
down-script=:log error "AP4 is DOWN"\r\n\r\n/tool e-mail send tls=yes to="[redacted]" subject= "A HOST IS DOWN" body= ("Afto einai ena
aftomatopoihmeno e-mail pou sas pliroforei oti to Access Point pou vrisketai ston deftero orofo, ston akalypto xwro einai DOWN. Apo tis ".\
([/system clock get date]).\ " kai wra ".\ ([/system clock get time]))

9 X ;;; NanoStation 2
host=[redacted] timeout=1m interval=10s since=jan/01/2002 03:00:04 status=up up-script=:log warning "NanoStation2 is UP"
down-script=:log error "NanoStation2 is DOWN"\r\n\r\n/tool e-mail send tls=yes to="[redacted]" subject= "A HOST IS DOWN" body= ("Afto einai ena
aftomatopoihmeno e-mail pou sas pliroforei oti to Access Point pou vrisketai sthn taratsa (NanoStation 2) einai DOWN. Apo tis ".\ ([/system
clock get date]).\ " kai wra ".\ ([/system clock get time]))

10 X ;;; Acess Point 3 (1os Orofos)
host=[redacted] timeout=1m interval=10s since=jan/01/2002 03:00:04 status=up up-script=:log warning "AP3 is UP"
down-script=:log error "AP3 is DOWN"\r\n\r\n/tool e-mail send tls=yes to="[redacted]" subject= "A HOST IS DOWN" body= ("Afto einai ena
aftomatopoihmeno e-mail pou sas pliroforei oti to Access Point pou vrisketai ston prwto orofo einai DOWN. Apo tis ".\ ([/system clock get
date]).\ " kai wra ".\ ([/system clock get time]))

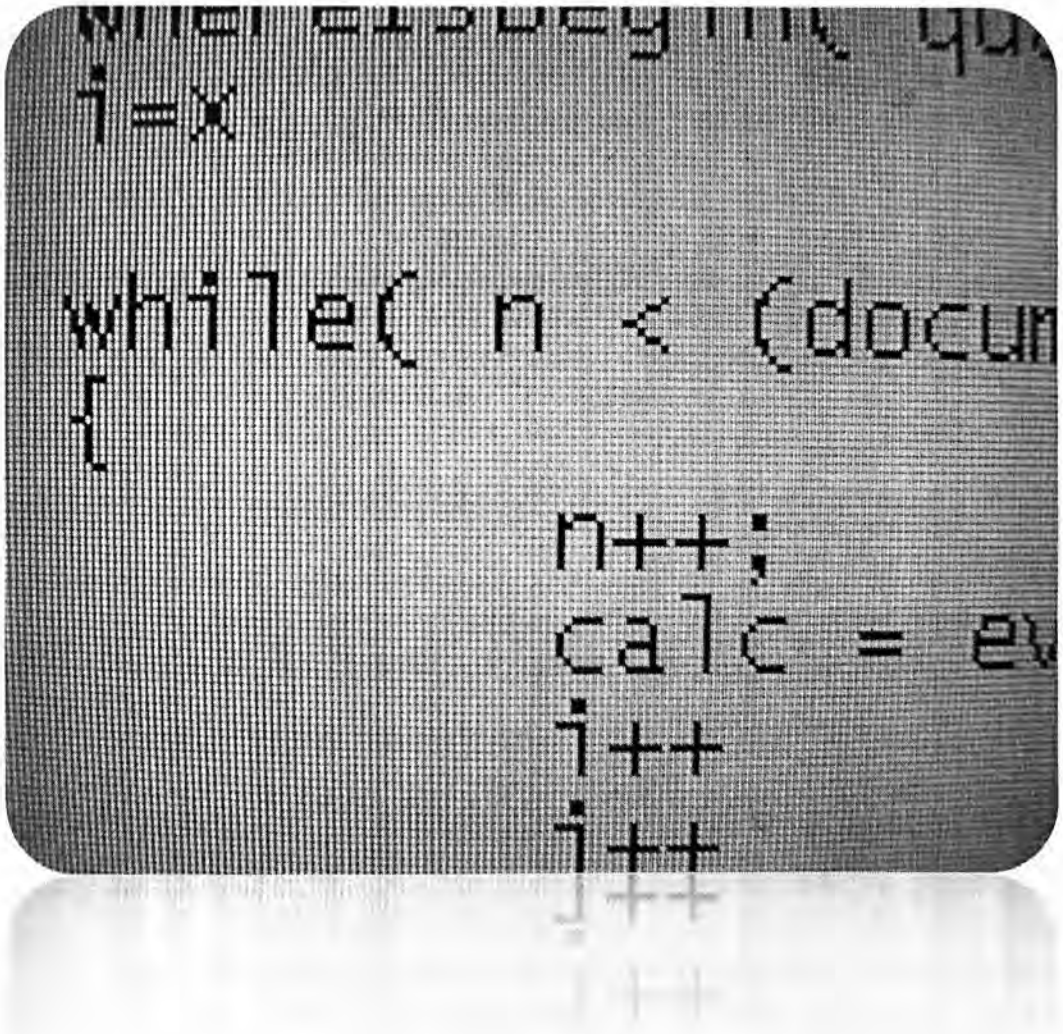
11 X ;;; Acess Point 5 (2os Eksw apo erg diktya)
host=[redacted]timeout=1m interval=10s since=jan/01/2002 03:00:04 status=up up-script=:log warning "AP5 is UP"
down-script=:log error "AP5 is DOWN"\r\n\r\n/tool e-mail send tls=yes to="[redacted]" subject= "A HOST IS DOWN" body= ("Afto einai ena
aftomatopoihmeno e-mail pou sas pliroforei oti to Access Point pou vrisketai ston deftero orofo, eksw apo to ergasthrio twn diktywn einai
DOWN. Apo tis ".\ ([/system clock get date]).\ " kai wra ".\ ([/system clock get time]))

12 ;;; NanoStation 5

host=[redacted]timeout=1m interval=10s since=aug/05/2011 01:50:20 status=up up-script=:log warning "NanoStation5 is UP"
down-script=:log error "NanoStation5 is DOWN"\r\n\r\n/tool e-mail send tls=yes to="[redacted]" subject= "A HOST IS DOWN" body= ("Afto einai ena
aftomatopoihmeno e-mail pou sas pliroforei oti to Access Point pou vrisketai sthn taratsa (NanoStation 5) einai DOWN. Apo tis ".\ ([/system clock get date]).\ " kai wra ".\ ([/system clock get time]))

13 ;;; AWMN Gateway&Change DNS Script
host=[redacted]timeout=1s interval=1m since=aug/11/2011 16:39:03 status=up
up-script=ip dns set servers=[redacted]\r\n:log warning "AWMN is up"
down-script=ip dns set servers=[redacted]\r\n:log error "AWMN is down"

5.5.1 Scripting



Επειδή ορισμένες εργασίες πρέπει να γίνονται ανα τακτά χρονικά διαστήματα, όπως πχ: το backup και επειδή θέλαμε να κάνουμε το όλο σύστημα όσο το δυνατόν πιο αυτόνομο γίνεται, φτιάξαμε μερικά script να κάνουν ορισμένες εργασίες, αντί για εμάς.

5.5.1.1 Καθημερινό BackUp και αποστολή με mail

Με το παρακάτω script, ο router παίρνει καθημερινά backup το configuration file με όλα τα settings και τα αποστέλλει σε ένα προκαθορισμένο λογαριασμό e-mail. Με αυτόν τον τρόπο μπορούμε ανα πάσα στιγμή που

παρουσιαστεί είτε hardware είτε software πρόβλημα στο σύστημα μας, να το επαναφέρουμε μέσα σε λίγα λεπτά σε κάποια επιθυμητή ημερομηνία, που λειτουργούσε σωστά. Το όφελος, είναι ότι έχουμε ελάχιστο downtime και ευελιξία στο configuration.

```
   name="Backup_Email_Script"                                    owner="admin"
policy=ftp,read,write,policy,test,winbox,sensitive    last-started=aug/13/2011
00:00:00 run-count=141
        source=
          /file remove [find type=backup]
          :log info "backup beginning now"
          :global backupfile ([/system identity get name] . "-" . [/system clock
get time])
          /system backup save name=$backupfile
          :log info "backup pausing for 10s"
          :delay 1s
          :log info "backup being emailed"
          /tool e-mail send tls=yes to="[redacted]
subject=([/system identity get name] . \
          "  Backup") from=auto.freespot09@gmail.com file=$backupfile
body=("Afto einai ena aftomatopoihmeno e-mail pou stelnei to backup file
kathe mera me mail>
          :log info "backup finished"
```

5.5.1.2 UPS Script

Το παρακάτω script, έχει σκοπό, να αντλεί δεδομένα από το ups, να μας ενημερώνει μέσω e-mail στην περίπτωση που κάτι «δεν πάει καλά» και να προστατεύει τον router από απότομες διακοπές της τροφοδοσίας, που μπορούν να βλάψουν τον router.

```
   name="ups-powermonitor"                                       owner="admin"
policy=ftp,read,write,policy,test,winbox run-count=0 source=


          :local smtp.gmail.com [:resolve mailserver];
          :local mailfrom "[redacted]";
          :local mailto "[redacted]";
          :local upsName "ups1";

          #
          #
          #
```

```
:global flagonbatt;
:global flagbattlow;

:local battalarm 15;
:local battok 40;

:local curonbatt;
:local curcharge;

:local sysname [/system identity get name];
:local datetime "$[/system clock get date] $[/system clock get time]";

# First run? If so, we need to initialize the global flags
:if ([:typeof $flagonbatt]="nothing") do={:set flagonbatt 0}
:if ([:typeof $flagbattlow]="nothing") do={:set flagbattlow 0}

:set curonbatt false;
:set curcharge 100;
/system ups monitor [/system ups find name=$upsName] once do={
  :set curonbatt $"on-battery"; :set curcharge $"battery-charge";
}

:if (($curonbatt) && ($flagonbatt=0)) do={
  :set flagonbatt 1;
  /tool e-mail send from=$mailfrom  to=$mailto server=$mailserver
subject="$sysname: Power failure!" \
    body="$sysname  is on battery since $datetime";
  :log info "Power-Fail: EMail sent to $mailto";
}

:if ((!$curonbatt) && ($flagonbatt=1)) do={
  :set flagonbatt 0;
  /tool e-mail send from=$mailfrom  to=$mailto server=$mailserver
subject="$sysname: Power is back" \
    body="$sysname is back on power since $datetime";
  :log info "Power-Restore: Email sent to $mailto";
}

:if (($curcharge <= $battalarm) && ($flagbattlow=0)) do={
  :set flagbattlow 1;
  /tool e-mail send from=$mailfrom  to=$mailto server=$mailserver
subject="$sysname: Low battery!" \
    body="$sysname battery is at $curcharge %! $datetime";
  :log info "Batt-Low: Email sent to $mailto";
```

```
}

:if (($curcharge >= $battok) && ($flagbattlow=1)) do={
 :set flagbattlow 0;
 /tool e-mail send from=$mailfrom  to=$mailto server=$mailserver
subject="$sysname: Battery recharged" \
  body="$sysname Battery recharged to $curcharge% $datetime";
 :log info "Batt-Recharged: Email sent to $mailto";
}
```

5.5.1.3 Auto Update & Upgrade Script

Το παρακάτω script, διμηουργήθικε με σκοπό να κρατάει πάντα τον router ενημερωμένο, και να τρέχει πάντα με την τελευταία stable έκδοση του λειτουργικού τους συστήματος, RouterOS. Αυτό προστατεύει το σύστημα μας από αδυναμίες, που ανακαλύπτονται στο software και κατ' επέκταση, αυξάνει την ασφάλεια, μιας και καλύπτει αμέσως τις «τρύπες» που ανακαλύπτονται.

```
##############################################################################
# download and upgrade
##############################################################################

# newest version
:local lMajor;
:local lMinor;

# current version
:local vMajor;
:local vMinor;

:local myVer [/system resource get version];

:for i from=0 to=([:len $myVer] - 1) do={
   :if ( [:pick $myVer $i] = ".") do={
         :set vMajor [:tonum [:pick $myVer 0 $i]];
         :set vMinor [:tonum [:pick $myVer ($i + 1) [:len $myVer]]] ;
   }
}

:if ($vMajor < 3) do={
   :log warning "RouterOS version too old ($vMajor.$vMinor), update
script not compatible";
```

```
    } else={

    #       detect platform (architecture-name is not available in older 3.x
versions)
        :local platform [/system resource get architecture-name];


    #     fetch latest version
        /tool      fetch      address="172.16.0.1"      src-path="latestVer.txt"
user="admin" password="" mode=ftp;
        :local lVer [/file get latestVer.txt content];


      :for i from=0 to=([:len $lVer] - 1) do={
            :if ( [:pick $lVer $i] = ".") do={
                  :set lMajor [:tonum [:pick $lVer 0 $i]];
                  :set lMinor [:tonum [:pick $lVer ($i + 1) [:len $lVer]]] ;
            }
      }

      :if (($vMajor = $lMajor) && ($vMinor < $lMinor)) do={
            :local pckgName "routeros-$platform-$lMajor.$lMinor.npk";
            /tool      fetch      address=[:resolve      "www.mikrotik.com"]
host="www.mikrotik.com" mode=http src-path="download/$pckgName";
            /system reboot;
      } else={
            :log info "Upgrade_script: already latest version";
        }
  }
```

6 Βιβλιογραφία

- Ιωάννης Αγγελόπουλος, « Δίκτυα Υπολογιστών – Σημειώσεις»
- Ιωάννης Αγγελόπουλος, « Διαδικτυακά Προτόκολλα– Σημειώσεις»
- Andrew S. Tanenbaum, « Δίκτυα Υπολογιστών – Εκδόσεις Κλειδάριθμος»
- Larry L. Peterson & Bruce S. Davie, « Δίκτυα Υπολογιστών, Μια προσέγγιση από την πλευρά των συστημάτων – Εκδόσεις Κλειδάριθμος»
- John Ross, «Εισαγωγή στην ασύρματη δικτύωση – Εκδόσεις Κλειδάριθμος»
- Nicopolitidis, Obaidat, Papadimitriou, Pomportsis, «Ασύρματα δίκτυα – Εκδόσεις Κλειδάριθμος»
- Διαδικτυακή Εγκυκλοπαίδεια «http://www.wikipedia.org/»
- Διαδικτυακός τόπος «http://www.w3schools.com/»
- Διαδικτυακός τόπος «http://wiki.mikrotik.com/wiki/Main_Page»
- Διαδικτυακός τόπος «http://www.tp-link.com/en/support/»
- Διαδικτυακός τόπος «http://routerboard.com/»
- Διαδικτυακός τόπος «http://www.cisco.com/en/US/docs/wireless/»
- Διαδικτυακός τόπος «http://www.wind.awmn.net/»
- Διαδικτυακός τόπος «http://www.awmn.net/»