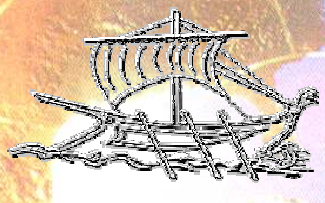


ΤΕΙ ΚΡΗΤΗΣ (ΠΑΡΑΡΤΗΜΑ ΧΑΝΙΩΝ)
ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΝΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΜΕΛΕΤΗ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΕΙΣΗΓΗΤΗΣ : *ΑΝΤΩΝΙΔΑΚΗΣ ΜΑΝΩΛΗΣ*

ΣΠΟΥΔΑΣΤΗΣ :*ΚΑΤΣΑΟΥΝΟΣ ΒΑΣΙΛΗΣ*

- ΑΚΑΔΗΜΑΙΚΟ ΕΤΟΣ-
- 2006/2007-

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ:

ΜΕΛΕΤΗ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΕΙΣΗΓΗΤΗΣ: ΑΝΤΩΝΙΔΑΚΗΣ ΜΑΝΩΛΗΣ

ΣΠΟΥΔΑΣΤΗΣ: ΚΑΤΣΑΟΥΝΟΣ ΒΑΣΙΛΗΣ

ΤΕΙ ΚΡΗΤΗΣ (ΠΑΡΑΡΤΗΜΑ ΧΑΝΙΩΝ)
ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΝΙΚΗΣ

ΑΚΑΔΗΜΑΙΚΟ ΕΤΟΣ 2006 - 2007

Abstract

In this project we will describe you the network evolution from the plain networks until the most sophisticated as the wireless networks. Especially we will analyze the IEEE 802.11 family protocols, the wireless network categories (technologies), main features and the coupling methods for each category.

One of the most important feature is the security in the data transfer. So we will see the IEEE 802.11 methods, that make the wireless net secure and safe such as firewall and encryption. Also their advantages and disadvantages, algorithms, examples and effects.

At last we will describe the wireless network implementations and the hardware of industry systems.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ

ΚΕΦΑΛΑΙΟ 2

ΠΡΩΤΟΚΟΛΛΑ & ΚΑΤΗΓΟΡΙΕΣ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

ΚΕΦΑΛΑΙΟ 4

ΕΦΑΡΜΟΓΕΣ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

ΚΕΦΑΛΑΙΟ 5

ΕΠΙΠΡΟΣΘΕΤΑ-ΕΠΙΛΟΓΕΣ

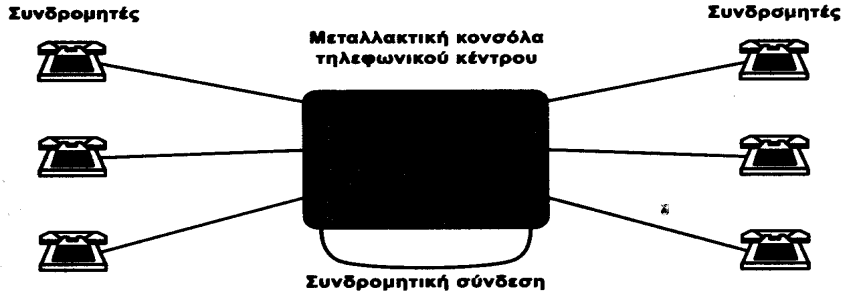
ΚΕΦΑΛΑΙΟ 1 ο

ΕΙΣΑΓΩΓΗ

Ως σκαλοπατι στη καταννοηση των ασυρματων δικτυων υπολογιστων ειναι αναγκαια μια αναφορα στην ιστορια,την εξελιξη και τα χαρακτηριστικα των δικτυων γενικα. Στη συνεχεια θα δουμε την αντιστοιχη πορεια των ασυρματων δικτυων καθως και χαρακτηριστικα που διεπουν την ασυρματη μεταδοση.

1.1) Η Ανάγκη των δικτύων

'Οταν ο Γκράχαμ Μπελ (Graham Bell) έθεσε για πρώτη φορά σε πρακτική εφαρμογή το τηλέφωνο, συνομιλούσε με ένα φίλο του μέσω δυο τηλεφωνικών συσκευών και μιας γραμμής. 'Οταν και άλλοι του ζήτησαν να έχουν και αυτοί το ίδιο προνόμιο, ο Bell για κάθε τέτοια σύνδεση διέθετε από δύο τηλεφωνικές συσκευές και από μια γραμμή. 'Ετσι ο ίδιος που μπορούσε να μιλήσει με όλους, είχε στο σπίτι του τόσες συσκευές όσες και οι συνδέσεις, ενώ παράλληλα ο ίδιος αριθμός γραμμών ξεκινούσε από εκεί με προορισμό τους φίλους του . 'Οσο ο αριθμός των χρηστών μεγάλωνε τόσο μεγάλωνε και ο αριθμός των συσκευών και των γραμμών. Η αύξηση ήταν τέτοια ώστε σε λίγο χρονικό διάστημα φάνηκε ότι η κατάσταση αυτή δεν ήταν δυνατόν να συνεχιστεί, καθώς από κάποιο σημείο και μετά το πρόβλημα της πληθώρας θα ήταν άλυτο.Τότε λοιπόν προέκυψε η ανάγκη του Δικτύου. Η λύση του προβλήματος πέρασε από τότε πολλά στάδια. Δημιουργήθηκαν τα πρώτα τηλεφωνικά κέντρα, στα οποία ο κάθε συνδρομητής συνδεόταν ακτινωτά με μια αφιερωμένη γραμμή και μια συσκευή, όπως φαινεται στο ***σχήμα 1*** παρακάτω. Πολλοί θα θυμούνται ακόμα τις τηλεφωνήτριες χειρίστριες των κέντρων, όπου ως καλοί τροχονόμοι συνέδεαν την γραμμή του καλούντος συνδρομητή με την γραμμή του καλούμενου με την βοήθεια βυσμάτων. Ειδικές γεννήτριες ρεύματος (μανιατό) ενσωματωμένες στις τηλεφωνικές συσκευές επέτρεπαν τις κλήσεις προς το κέντρο. Αυτή ήταν και η πρώτη μορφή δικτύου επικοινωνιών φωνής. Στη συνέχεια η τεχνολογία των τηλεφωνικών κέντρων προόδευσε με την ανάπτυξη των



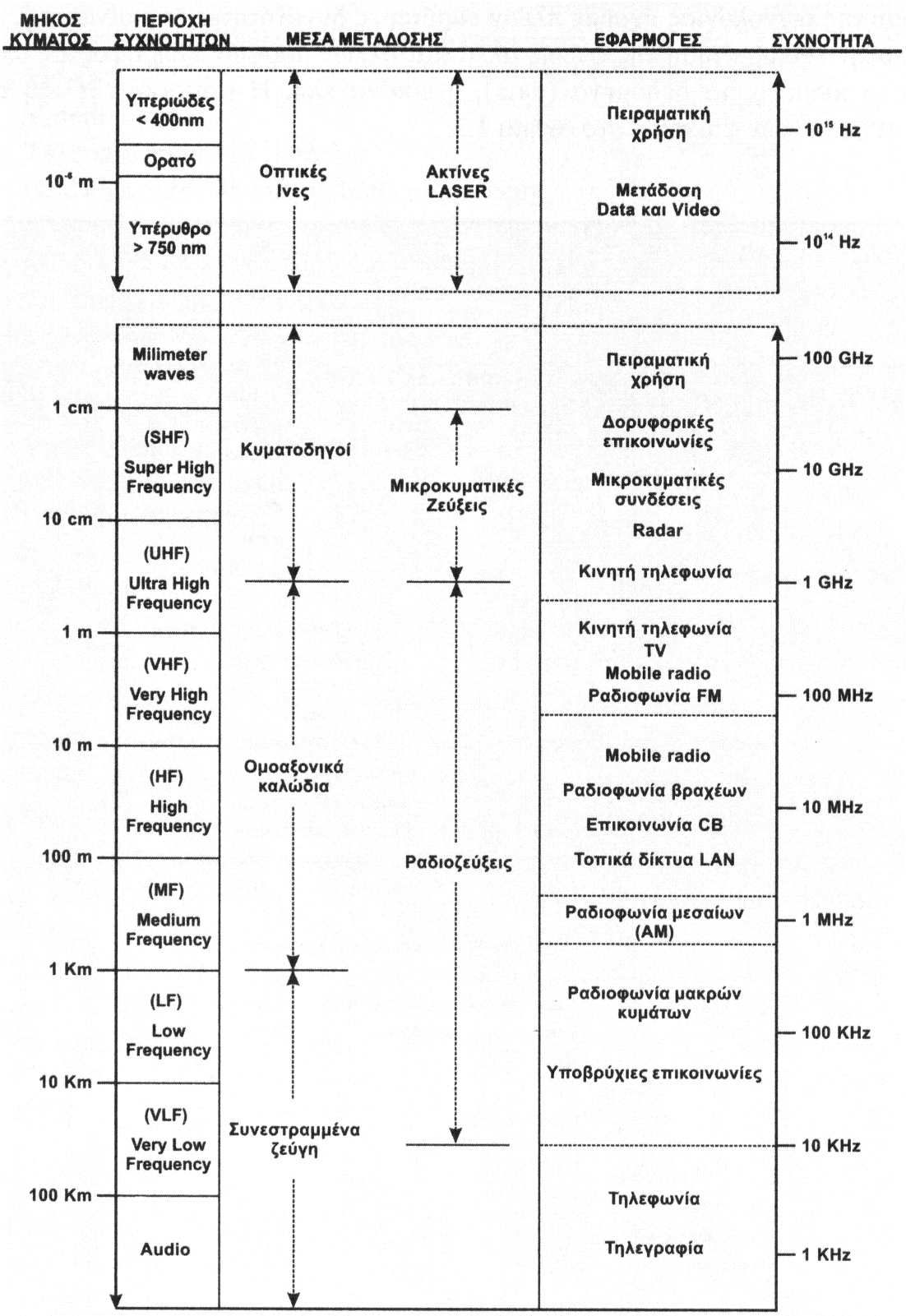
Σχημα 1

ηλεκτρομηχανικών τηλεφωνικών κέντρων και τη χρήση της αυτόματης επιλογής.
Ακολούθησε η ανάπτυξη των ηλεκτρονικών κέντρων, για να καταλήξουμε στη σημερινή χρήση υπολογιστικών συστημάτων και ψηφιακών τεχνικών.
Παρόμοια σχεδόν ιστορία ακολουθείται και στα δίκτυα Data. Στην αρχή ένας τερματικος σταθμός (Data Terminal Equipment) συνδέεται με έναν άλλο τέτοιο σταθμό χρησιμοποιώντας το κοινό τηλεφωνικό δίκτυο ή τις μόνιμες αφιερωμένες (dedicated) γραμμές. Στη συνέχεια η ανάγκη πολλαπλών συνδέσεων των τερματικών σταθμών, οδήγησε στη δημιουργία και εκμετάλλευση ποικίλων δικτύων data. Τα σύγχρονα δίκτυα είναι τέτοια που δεν χρειάζονται πολλαπλές αφιερωμένες συνδέσεις μεταξύ των συνδρομητών . Ο κάθε συνδρομητής συνδέεται μόνο με μια γραμμή με το πλησιέστερο τηλεπικοινωνιακό κέντρο.

Προκειμένου να υλοποιηθεί μια τέτοια σύνδεση, ο συνδρομητής με τα πρώτα data που αποστέλλει,ενημερώνει το δίκτυο στο οποίο ανήκει για την ταυτότητα του επιθυμητού ανταποκριτή τερματικού σταθμού. Προς αυτή τη κατεύθυνση δημιουργήθηκαν ιδιωτικά και δημόσια δίκτυα data, παραδείγματα των οποίων αναφέρουμε το τηλεφωνικό, το δίκτυο telex, τα ασύρματα δίκτυα κινητής τηλεφωνίας, δίκτυα videotex, το ISDN και άλλα.

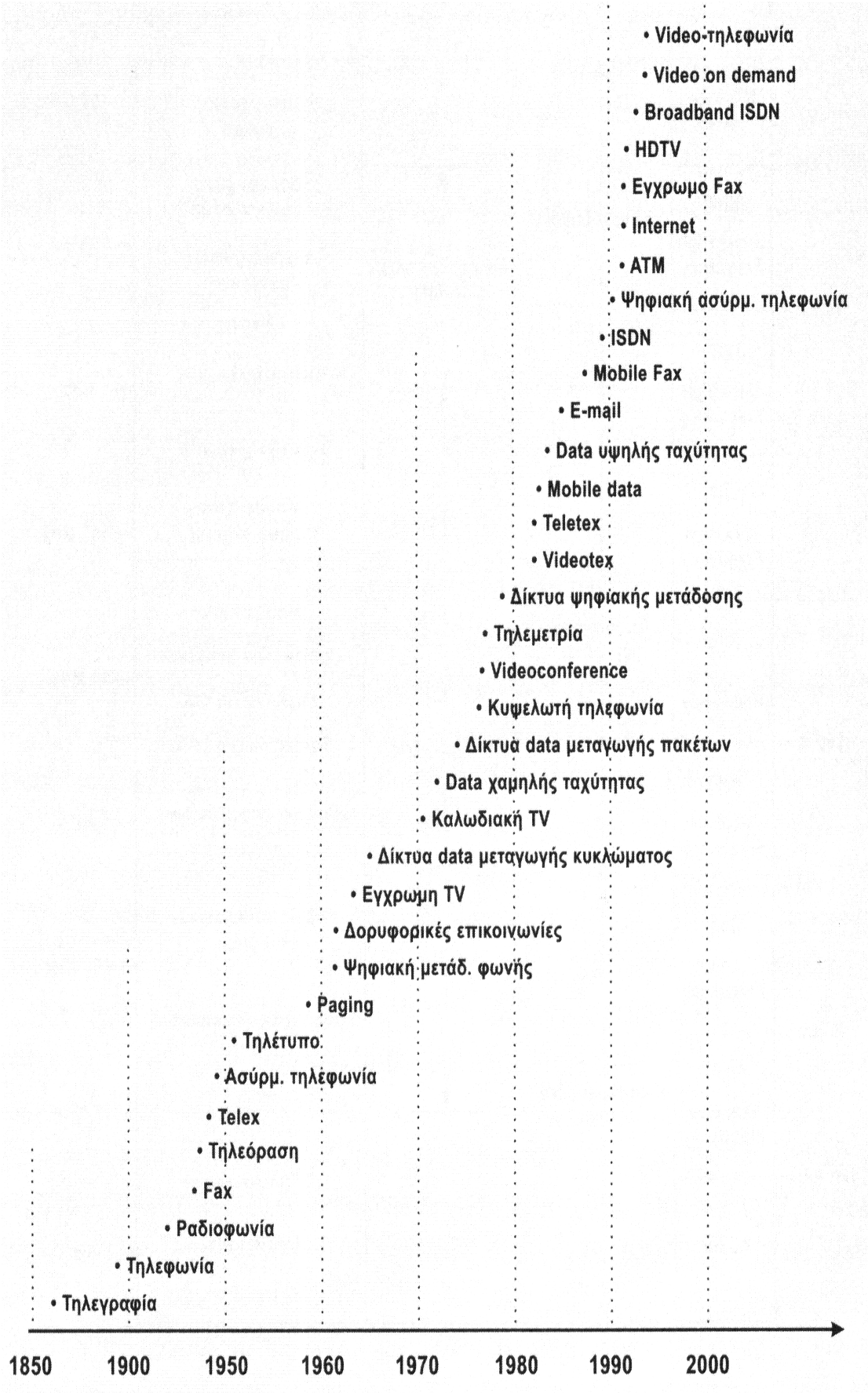
Η χρήση της ηλεκτρομαγνητικής ακτινοβολίας απο τον 19ο αιώνα ήταν ο βασικός μοχλός ανάπτυξης των Τηλεπικοινωνιών. Η συχνότητα του ηλεκτρομαγνητικού κύματος είναι ένα ιδιαίτερο χαρακτηριστικό και η κάθε εφαρμογή συνδέεται με τη χρήση ενός ορισμένου τμήματος του φάσματος συχνοτήτων. Το ***σχήμα 2*** παρουσιάζει την κατανομή των εφαρμογών στο φάσμα των συχνοτήτων .

Από τη στιγμή που η μικροηλεκτρονική με τα επιτεύγματά της εισήλθε στην περιοχή των τηλεπικοινωνιών, οι τελευταίες είχαν την ευκαιρία να αλλάξουν πρόσωπο και να ξεφύγουν από τις γνωστές κλασσικές εφαρμογές όπως είναι το τηλέφωνο και το τηλέτυπο.



Σχήμα 2

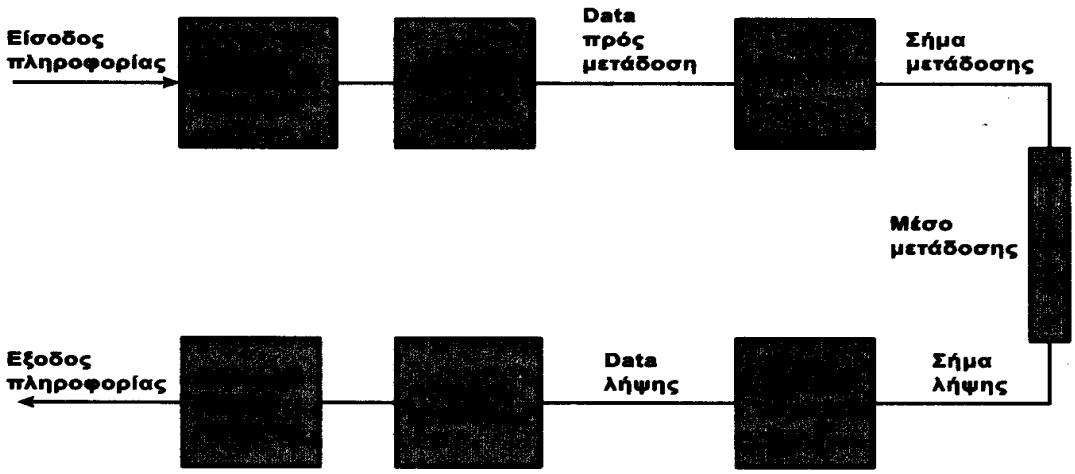
Η ιστορική εξέλιξη των Τηλεπικοινωνιών φαίνεται στο ***σχήμα 3*** που ακολουθεί.


• Video-τηλεφωνία
• Video on demand
• Broadband ISDN
• HDTV
• Εγχρωμο Fax
• Internet
• ATM
• Ψηφιακή ασύρμ. τηλεφωνία
• ISDN
• Mobile Fax
• E-mail
• Data υψηλής ταχύτητας
• Mobile data
• Teletex
• Videotex
• Δίκτυα ψηφιακής μετάδοσης
• Τηλεμετρία
• Videoconference
• Κυψελωτή τηλεφωνία
• Δίκτυα data μεταγωγής πακέτων
• Data χαμηλής ταχύτητας
• Καλωδιακή TV
• Δίκτυα data μεταγωγής κυκλώματος
• Εγχρωμη TV
• Δορυφορικές επικοινωνίες
• Ψηφιακή μετάδ. φωνής
• Paging
• Τηλέτυπο
• Ασύρμ. τηλεφωνία
• Telex
• Τηλεόραση
• Fax
• Ραδιοφωνία
• Τηλεφωνία
• Τηλεγραφία
1850
1900
1950
1960
1970
1980
1990
2000

Σχήμα 3

Νέες τεχνολογίες εισήλθαν πλέον στις τηλεπικοινωνίες, όπως η ψηφιακή
μετάδοση των σημάτων και η ψηφιακή μεταγωγή και επεξεργασία. Παράλληλα είχαμε τη βελτίωση των μέσων μετάδοσης, της υποδομής (οπτικές ίνες,δορυφορικές ζεύξεις, κλπ.) και των τεχνικών μετάδοσης (multiplexing, compression, κωδικοποιήσεις, διαμορφώσεις κλπ.). Σήμερα βρισκόμαστε στο αναπτυξιακό στάδιο ενός νέου επιστημονικού κλάδου που καλείται κατά σύζευξη των όρων Τηλεπικοινωνίες και Πληροφορική, Τηλεπληροφορική.
Ήδη σήμερα οι μεταδόσεις φωνής, data, εικόνας κλπ. φαίνεται να ολοκληρώνονται μέσω ψηφιακών δικτύων υψηλών ταχυτήτων που χρησιμοποιούν τεχνολογίες bandwidth on demand, για βέλτιστη εκμετάλλευση της χωρητικότητας των καναλιών και των επικοινωνιακών κόμβων με την χρήση τεχνικών όπως η A TM (AsynchronousTransfer Mode).

Το *Επικοινωνιακό μοντέλο* που παραθέτουμε ***σχήμα 4*** μας βοηθά να κατανοήσουμε ακόμα καλύτερα την έννοια "επικοινωνίες" δεδομένων.



Μοντέλο επικοινωνιών

Σχήμα 4

Αυτό το μοντέλο αναλύει και περιγράφει τα διάφορα στάδια από τα οποία θα
περάσει η πληροφορία. Βασικές λειτουργίες του μοντέλου είναι:

- Προετοιμασία της πληροφορίας προς αποστολή.
- Συγχρονισμός των διαφόρων συμμετεχόντων στοιχείων της μετάδοσης.
- Συντονισμός δηλαδή όλων των συσκευών και των λειτουργιών που επιτελούν.
- Προσδιορισμός του προορισμου της πληροφορίας.
- Δρομολόγηση της πληροφορίας.
- Έλεγχος ροής.

- Διαδικασίες λήψης.
- Αναγνώριση / διόρθωση σφαλμάτων.
- Ασφάλεια μεταδιδομένων data.
- Τακτοποίηση / παρουσίαση ληφθέντος μηνύματος.
- Διαχείριση συνομιλίας.

Το βασικό θέμα στον χώρο των επικοινωνιών είναι να ξεκαθαρισθεί από την αρχή ποια πληροφορία είναι αυτή που θέλουμε να μετακινήσουμε , Σημαντικό θέμα είναι επίσης τα μέσα μετάδοσης, ο δρόμος δηλαδή που χρησιμοποιεί η πληροφορία για την μετάδοσή της. Ενα άλλο κρίσιμο σημείο είναι οι τεχνικές μετάδοσης των δεδομένων, οι τρόποι διαμόρφωσης και η χρήση της ψηφιακής τεχνολογίας.

0 όρος ***Δίκτυο Υπολογιστών*** χαρακτηρίζει ένα σύνολο αυτόνομων υπολογιστών,οι οποίοι συνδέονται μεταξύ τους με κάποιο επικοινωνιακό μέσο. Τα δίκτυα διακρίνονται σε δύο κατηγορίες: Στα Τοπικά Δίκτυα ή LANs (Local Area Networks),
τα οποία χρησιμοποιούνται για κάλυψη μικρών περιοχών όπως το περιβάλλον ενός γραφείου, και στα Δημόσια Δίκτυα ή WANs (Wide Area Networks),τα Μητροπολιτικά Δίκτυα ή MANs (Metropolitan Area Networks) και το Ψηφιακό Δίκτυο ολοκληρωμένων γπηρεσιών ή ISDN (Integrated Services Digital Network). Τα δίκτυα αυτά καλύπτουν μεγάλες περιοχές όπως και τα Δημόσια Δίκτυα, αλλά παρέχουν υψηλές υπηρεσίες σε ό, τι αφορά την ταχύτητα και την αξιοπιστία.*Αξιζει εδώ να κανουμε μια ξεχωρηστη αναφορα στα τοπικα δικτυα* **:**

Τα τοπικά δίκτυα (local area networks), συνήθως αποκαλούμενα LAN, είναι ιδιωτικά δίκτυα εκτεινόμενα εντός ενός μοναδικού κτιρίου ή σε εγκαταστάσεις ακτίνας έως μερικά χιλιόμετρα. Χρησιμοποιούνται ευρύτατα για να συνδέουν προσωπικούς υπολογιστές και σταθμούς εργασίας σε γραφεία εταιρειών και σε εργοστάσια, με σκοπό την κοινή χρήση των μέσων (π.χ. των εκτυπωτών) και την ανταλλαγή πληροφοριών. Τα LAN διακρίνονται από τα άλλα είδη δικτύων με βάση τρία χαρακτηριστικά: 1ο το μέγεθος, 2ο την τεχνολογία μετάδοσης και 3ο την τοπολογία τους.

Τα LAN είναι περιορισμένου μεγέθους, που σημαίνει ότι ο χρόνος μετάδοσης στη χειρότερη περίπτωση είναι φραγμένος και γνωστός εκ των προτέρων. Η γνώση του ορίου αυτού επιτρέπει τη χρήση συγκεκριμένων τεχνικών που αλλιώς θα ήταν ανέφικτες. Επίσης, απλοποιεί τη διαχείριση του δικτύου. Τα LAN χρησιμοποιούν συχνά μια τεχνολογία μετάδοσης που αποτελείται από ένα απλό καλώδιο, στο οποίο έχουν συνδεθεί όλες οι μηχανές, όπως στις ομαδικές γραμμές που κάποτε χρησιμοποιούσαν οι τηλεφωνικές εταιρείες στις αγροτικές περιοχές.Τα παραδοσιακά LAN που λειτουργούν σε ταχύτητες των 10 έως 100 Mbps, παρουσιάζουν χαμηλή καθυστέρηση (δεκάδες μικροδευτερολέπτων) και εμφανίζουν πολύ λίγα λάθη. Τα νεώτερα LAN

μπορούν να λειτουργούν σε υψηλότερες ταχύτητες, έως και εκατοντάδες megabit ανά δευτερόλεπτο (Σήμερα έχουμε δυνατότητα μέχρι 1Gbps).

1.1.2) Οργανισμοί καθορισμού επικοινωνιακών προτύπων

Τα τελευταία χρόνια, η ανάγκη διασύνδεσης υπολογιστικών συστημάτων διάφορων κατασκευαστών οδήγησε στη μεγάλη ανάπτυξη επικοινωνιακού λογισμικού. Οι κατασκευαστές επικοινωνιακού υλικού και λογισμικού, για να αντεπεξέλθουν στις νέες ανάγκες, αποφάσισαν να δημιουργήσουν προϊόντα σύμφωνα με πρότυπα γενικής αποδοχής. 'Ετσι, δημιουργήθηκαν διεθνείς οργανισμοί για την ανάπτυξη, τον καθορισμό και την πρόβλεψη της υλοποίησης επικοινωνιακής τεχνολογίας. Πολλοί οργανισμοί ανά τον κόσμο έχουν αναμειχθεί στην ανάπτυξη επικοινωνιακών προτύπων, οι κυριότεροι από τους οποίους είναι:

- **International Standards Organization - ISO**

Τα μέλη του ISO είναι κυρίως αντιπρόσωποι κρατικών οργανισμών που ασχολούνται με τον καθορισμό προτύπων. Ο ISO έχει αναπτύξει πρότυπα που καλύπτουν μεγάλο τεχνολογικό φάσμα, μέρος του οποίου αποτελεί και η τεχνολογία των επικοινωνιών. Σε ό,τι αφορά τα δίκτυα, έχει προτείνει το μοντέλο αναφοράς OSI (Open Systems Interconnection), για διασύνδεση ανοικτών συστημάτων, που αποτελείται από 7 επίπεδα και έχει γίνει διεθνώς αποδεκτό.

- **Consultative Committee for International Telegraph and Telephone - CCITT**

Η CCITT είναι η Επιτροπή της Διεθνούς 'Ενωσης Τηλεπικοινωνιών. Τα μέλη της είναι αντιπρόσωποι κρατικών οργανισμών των χωρών που ανήκουν στα Ηνωμένα 'Εθνη Ο.Η.Ε.). Η CCITT ανέπτυξε πρότυπα, ώστε να είναι συμβατή η λειτουργία των τηλεπικοινωνιακών συστημάτων των χωρών - μελών.

- **American National Standards Institute (ANSI)**

Η ANSI είναι ο αντιπρόσωπος των Η.Π.Α. στον ISO. Η ANSI είναι μη κερδοσκοπικός και μη κρατικός οργανισμός, που αποτελείται από πολυάριθμους εμπορικούς οργανισμούς, κατασκευαστές και τηλεπικοινωνιακούς φορείς. Είναι ο κυριότερος φορέας ανάπτυξης προτύπων στις Η.Π.Α. Οι οργανισμοί - μέλη του που επηρεάζουν περισσότερο την ανάπτυξη των προτύπων είναι οι:

●***Electronics Industries Association (EIA):*** είναι μια εμπορική ένωση που έχει αναπτύξει πρότυπα για τα μέσα μετάδοσης που χρησιμοποιούνται στα δίκτυα.
●***Institute of Electrical and Electronics Engineers (IEEE):*** είναι μία επαγγελματική ένωση, η οποία ανέπτυξε πρότυπα για τα μέσα μετάδοσης και τα επικοινωνιακά πρωτόκολλα που χρησιμοποιούνται στα δίκτυα.

Το μελλον των δικτυων είναι ασυρματο!!

Η επανασταση που προμηνύεται, είναι η επέκταση των ψηφιακών ασύρματων επικοινωνιών υψηλών ταχυτήτων που θα αλλάξει την μορψή των δικτύων καθώς τα τερματικά σημεία του δικτύου δεν εξαρτώνται από το πού καταλήγει το καλώδιο, αλλά έχει την ελευθερία κίνησης που προσφέρει η ασύρματη επικοινωνία.
Παρακατω,ως κυριο θεμα της μελετης αυτης,θα δουμε τα χαρακτ ηριστικα την εξελιξη καθως και την δομη και υποδομη της νεας αυτης τεχνολογιας των ασυρματων δικτυων.

ΕΙΣΑΓΩΓΗ ΣΤΑ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

1.2) Τα ηλεκτρομαγνητικά κύματα

Τα ηλεκτρομαγνητικά κύματα (ακτινοβολία) είναι τα γνωστά σε όλους ραδιοκύματα που χρησιμοποιούνται στο ραδιόφωνο, στην τηλεόραση και σε άλλες
τεχνολογικές εφαρμογές της καθημερινής μας ζωής . Πρόκειται για ταλαντώσεις ηλεκτρικών και μαγνητικών πεδίων που διαδίδονται ως κύματα με την ταχύτητα του φωτός. Ποικίλες εφαρμογές τους βρίσκονται στην υπηρεσία του ανθρώπου για περισσότερο από 100 χρόνια, καθώς καθημερινά χρησιμοποιούνται για την λειτουργία οικιακών συσκευών (όπως για παράδειγμα ραδιόφωνο, τηλεόραση,φούρνος μικροκυμάτων), ασύρματων εφαρμογών καθώς και σε ιατρικές εφαρμογές κ.α. Επιπλέον χρησιμοποιούνται στα τηλεπικοινωνιακά συστήματα της Πυροσβεστικής, Αστυνομίας, των ασθενοφόρων αλλά και των ραντάρ. Οι πιο πρόσφατες εφαρμογές των ηλεκτρομαγνητικών κυμάτων πραγματοποιήθηκαν στις δεκαετίες του ΄80 και ’90, όταν έγινε η χρήση τους στην κινητή και δορυφορική επικοινωνία.Κάθε πηγή ηλεκτρομαγνητικών κυμάτων (π.χ. κεραίες ραδιοφωνίας,τηλεόρασης, κινητής τηλεφωνίας, ραντάρ) παράγει ηλεκτρομαγνητικό πεδίο που διαδίδεται στο χώρο (συχνά χρησιμοποιούμε τον όρο ηλεκτρομαγνητική ακτινοβολία). Τα ηλεκτρομαγνητικά πεδία (ΗΜΠ), υπάρχουν παντού στο περιβάλλον μας. Μπορεί να είναι φυσικής προέλευσης ή μπορεί να έχουν δημιουργηθεί από τον άνθρωπο. Το ηλεκτρικό ρεύμα δημιουργεί ΗΜΠ. Τα ΗΜΠ μπορεί να είναι ψηλής ή χαμηλής έντασης, συνεχή ή μικρής διάρκειας. Τα ηλεκτρικά πεδία δημιουργούνται λόγω διαφοράς ηλεκτρικής τάσης. Όσο πιο μεγάλη είναι η διαφορά, τόσο πιο δυνατό θα είναι το ηλεκτρικό πεδίο που προκύπτει. Η μονάδα μέτρησης των ηλεκτρικών πεδίων είναι βολτ ανά μέτρο (V/m). Τα μαγνητικά πεδία δημιουργούνται όταν υπάρχει ροή ηλεκτρικού ρεύματος. Όσο πιο ψηλή είναι η ένταση του ρεύματος τόσο πιο δυνατό θα είναι το μαγνητικό πεδίο. Όταν διακοπεί το ηλεκτρικό ρεύμα, το μαγνητικό πεδίο μηδενίζεται. Μια συσκευή όπως για παράδειγμα ο στεγνωτήρας μαλλιών, παράγει μαγνητικό πεδίο μόνο όταν το ηλεκτρικό ρεύμα τη θέτει σε λειτουργία. Η διακοπή του ρεύματος, εξαφανίζει άμεσα το μαγνητικό πεδίο.
Τα ΗΜΠ δημιουργούνται μεταξύ άλλων από τα ακόλουθα:
1. Ηλεκτροφόρα καλώδια ψηλής τάσης
2. Ηλεκτροφόρα καλώδια στις γειτονιές
3. Συστήματα γείωσης που προστατεύουν από κεραυνούς ή από ελαττωματικές
οικιακές συσκευές

4. Οικιακές συσκευές όπως φούρνοι μικροκυμάτων, στεγνωτήρες μαλλιών,
ηλεκτρικοί φούρνοι, ηλεκτρική θέρμανση,
5. Οθόνες ηλεκτρονικών υπολογιστών, ηλεκτρικά ρολόγια, ηλεκτρικές κουβέρτες
6. Κινητά τηλέφωνα, κεραίες σταθμών βάσης, ραντάρ, ραδιοφωνικοί και τηλεοπτικοί σταθμοί
7. Φυσικές πηγές
8. Ακτίνες Χ
9. Φως του ήλιου
10. Ακτίνες γάμα

1.2.2) Ιστορία των ασύρματων δικτύων

Τηλεπικοινωνία είναι η επικοινωνία μεταξύ ανθρώπων (ή και μηχανών) που βρίσκονται σε απόσταση μεταξύ τους και συνίσταται στη μετάδοση πληροφοριών που επιτυγχάνει ένας πομπός προς έναν δεκτή.
Από τα αρχαία χρόνια οι άνθρωποι έβρισκαν τρόπους να επικοινωνούν από απόσταση.
Ξεκινώντας από τους αγγελιοφόρους, δρομείς δηλαδή, που έκαναν τη μεταφορά προφορικών και γραπτών μηνυμάτων, περνώντας στις φρυκτωρίες που ήταν ένα σύστημα μεταβίβασης φωτεινών σημάτων με διαδοχικό άναμμα φωτιάς στις κορυφές βουνών και που χρησιμοποιήθηκαν για στρατιωτικούς κυρίως σκοπούς από την εποχή του τρωικού πόλεμου έως τους βυζαντινούς χρόνους από τους Ελληνες, που ήταν ο πρώτος οπτικός τηλέγραφος που αναφέρεται στην ιστορία, μέχρι τα ταχυδρομικά περιστέρια και τα τύμπανα των αφρικανικών φυλών και τα σήματα καπνού των ινδιάνων, φτάσαμε τελικά στο πρώτο πραγματικά ασύρματο τρόπο επικοινωνίας σύμφωνα με τον ορισμό που χρησιμοποιούμε και σημερα.
Ήταν ο ασύρματος του Μαρκόνι ο οποίος άρχισε να πειραματίζεται με τον ηλεκτρομαγνητισμό το 1894 και πέτυχε την πρώτη μετάδοση μηνύματος χωρίς την χρήση συρμάτων. Αυτή του η εφεύρεση χρησιμοποιήθηκε στα πλοία και χρησιμοποιούταν ακόμα και πριν από λίγα χρόνια. Συχνά δε τον ασυρματιστή του πλοίου τον αποκαλούσαν Μαρκόνι.
Τον περασμένο αιώνα έγινε ένα μεγάλο άλμα τις τηλεπικοινωνίες. Κι αυτό έγινε με τη χρήση δορυφόρων που επέτρεψε την εύκολη διασύνδεση απομακρυσμένων περιοχών της υδρογείου και κατήργησε την ανάγκη χρήσης συρμάτινων αγωγών τεράστιου μήκους η την χρήση πολλών και ισχυρών επίγειων αναμεταδοτών. Ο πρώτος τηλεπικοινωνιακός δορυφόρος εκτοξεύτηκε από τη nasa στις 12 Αυγούστου 1960.
Η ασύρματη επικοινωνία χρησιμοποιεί τα ηλεκτρομαγνητικά κύματα τα

οποία μεταδίδονται στη γήινη ατμόσφαιρα ή στο διάστημα.
Έτσι για παράδειγμα τα ραδιοκύματα (με συχνότητες από 3KHz μέχρι 300MHz), χρησιμοποιούνται στα ασύρματα τηλέφωνα, στην κινητή τηλεφωνία, στη ραδιοεπικοινωνία, τη ραδιοφωνική και τηλεοπτική μετάδοση.
Τα μικροκύματα (με συχνότητες από 300MHz μέχρι 300GHz)) χρησιμοποιούνται στη ραδιοφωνική και τηλεοπτική μετάδοση και σε διάφορες μικροκυματικες ζευξεις.
Ακόμα και υπέρυθρη ακτινοβολία χρησιμοποιείται για ψηφιακή επικοινωνία σε δίκτυα περιορισμένης γεωγραφικής εμβέλειας.

1.2.3) Ασυρματα τοπικα δικτυα

Με την δημιουργία των πρώτων δικτύων ηλεκτρονικών υπολογιστών, παράλληλα με τις μεθόδους που αναπτύχθηκαν για ενσύρματη σύνδεση των κόμβων, είχαμε και την προσπάθεια δημιουργίας ασύρματων τοπικών δικτύων που θα αποδέσμευε την επικοινωνία από τα ενσύρματα μεσα.Σημερα τα ασύρματα τοπικά δίκτυα υπολογιστών, υλοποιούνται βασισμένα στις προδιαγραφές που ορίζει η οικογένεια πρωτοκόλλων του IEEE 802.11 και που στην ουσία είναι τον πρότυπο ethernet και το csma/ca, δηλαδή το πρωτόκολλο πολλαπλής πρόσβασης με ανίχνευση φέροντος και αποφυγή συγκρούσεων. Ενδεικτικά αναφέρουμε το 802.11b που είναι τεχνολογία ασύρματης μετάδοσης που επιτρέπει ταχύτητες μέχρι 11Mbps και το 802.11g που είναι τεχνολογία ασύρματης μετάδοσης που επιτρέπει ταχύτητες μέχρι 54Mbps. Η κάρτα δικτύου που χρησιμοποιείται στην υλοποίηση, κάνοντας χρήση της ασύρματης τεχνολογίας επιτυγχάνει την ίδια δικτύωση με μια κλασσική κάρτα δικτύου, αλλά χωρίς καλώδια. Μια ειδική περίπτωση που μας ενδιαφέρει ιδιαίτερα, είναι το hotspot, το οποίο είναι το ασύρματο δίκτυο στο οποίο ο χρήστης μπορεί να έχει πρόσβαση στο internet.
Τα ασύρματα τοπικά δίκτυα επιτρέπουν στους σταθμούς εργασίας να συνδέονται μεταξύ τους χωρίς την ανάγκη εγκατάστασης καλωδιακών συστημάτων . 'Ενα τυπικό ασύρματο τοπικό δίκτυο αποτελείται από έναν ασύρματο transceiver που είναι συνδεδεμένος στον server καλωδιακά και ασύρματους πομποδέκτες στον κάθε σταθμό εργασίας.

Τα ασύρματα δίκτυα έχουν φέρει αλλαγή στον τρόπο επικοινωνίας των υπολογιστών, αλλά και των χρηστών τους. Με την αύξηση του αριθμού των συσκευών που αλληλεπιδρούν με τους υπολογιστές τα ασύρματα δίκτυα μπορούν να προσφέρουν λύσεις, οι οποίες θα βελτιώσουν την επικοινωνία και θα αυξήσουν την αποδοτικότητα π.χ. σε ένα εργασιακό χώρο όπως μια εταιρεία, μια τράπεζα αλλά και μια σχολική μονάδα ή σε ένα νοσοκομείο.
Με τη χρήση των ασύρματων δικτύων η επικοινωνία γίνεται πιο άμεση,

το δίκτυο παρέχει κάλυψη χωρίς περιορισμούς και η επέκταση του γίνεται πολύ πιο εύκολα και με αμελητέο κόστος.
Ο εξοπλισμός που χρησιμοποιείται είναι εντελώς ακίνδυνος για τον ανθρώπινο οργανισμό. Η ακτινοβολία είναι μη ιονίζουσα και τα επίπεδα ακτινοβολίας είναι πολύ πιο χαμηλά από τα επιτρεπτά για τον ανθρώπινο οργανισμό όρια. Αρκεί να αναφέρουμε ότι μια ασύρματη κάρτα δικτύου (802.11b) ακτινοβολεί ισχύ 50 - 100 mwatt, ενώ ένα κινητό τηλέφωνο φτάνει και τα 2000 mwatt.
Επιπλέον, τα ασύρματα δίκτυα προσφέρουν διασύνδεση τοπικών δικτύων μεταξύ τους, όπως των καταστημάτων της επιχείρησης ή των εργαστηρίων ενός σχολικού εργαστηριακού κέντρου, επιτρέποντας τα ακόλουθα:

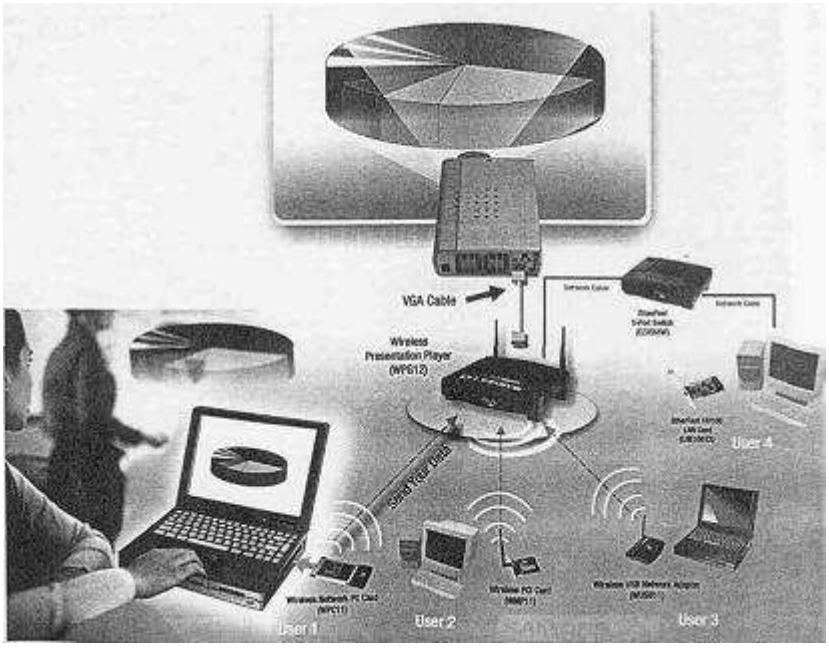
- Επικοινωνία των υπολογιστών συνολικά και ανεξάρτητα από την τοποθεσία.
- Φωνητική επικοινωνία μεταξύ των δικτύων χωρίς κόστος
- Μείωση των τηλεπικοινωνιακών εξόδων με το μοίρασμα μιας σύνδεσης με το Διαδίκτυο προς όλα τα υποδίκτυα.
- Ακόμα και επισκόπηση χωρών χρησιμοποιώντας ασύρματες κάμερες.

1.2.4)Χρήση ασύρματων τοπικών δικτύων

Ενδεικτικά, τα ασύρματα δίκτυα μπορούν να χρησιμοποιηθούν μέσα στο χώρο μιας επιχείρησης, μιας σχολικής μονάδας, μιας δημόσιας υπηρεσίας, κ.λ.π., για:

- Επικοινωνία των υπολογιστών χωρίς τη χρήση και το κόστος της δομημένης καλωδίωσης.
- Επέκταση του ήδη υπάρχοντος δικτύου με αμελητέο κόστος και υποδομή.
- Χρήση ασύρματης τηλεφωνίας μέσα από το ήδη υπάρχον ασύρματο δίκτυο.
- Επισκόπηση χωρών χρησιμοποιώντας ασύρματες κάμερες
- Ως hotspot. Το hotspot είναι ένα ασύρματο σημείο πρόσβασης στο internet. Στην πραγματικότητα, δεν είναι απλώς ένα σημείο, αλλά μια περιοχή η οποία καλύπτεται από συσκευές που επιτρέπουν και διαχειρίζονται την ασύρματη πρόσβαση των χρηστών στο internet. Ένα hotspot μπορεί να έχει εμβέλεια από μερικά μέτρα και να φτάσει ακόμη και το ένα χιλιόμετρο κάλυψης, αν αυτό είναι επιθυμητό. Ένας χρήστης, εκμεταλλευόμενος τις δυνατότητες που του παρέχει η ασύρματη σύνδεση του με το hotspot, είναι σε θέση να πραγματοποιήσει στον υπολογιστή του οποιαδήποτε εργασία έχει σχέση με το internet σαν να ήταν στο σπίτι του ή στο γραφείο του. Αυτό σημαίνει ότι ο χρήστης του hotspot μπορεί να το χρησιμοποιήσει για τις ακόλουθες εργασίες:

- Πλοήγηση στο Διαδίκτυο (web surfing)
- Ανταλλαγή αρχείων και online επικοινωνία μεταξύ των χρηστών
- Πρόσβαση σε εφαρμογές πολυμεσικού περιεχομένου (multimedia), για τη λήψη εικόνων, διαδραστικού βίντεο και μουσικής
- Λήψη ενημερωτικού ή εκπαιδευτικού περιεχομένου



1.2.5) Ασύρματα δίκτυα και Hot Spots

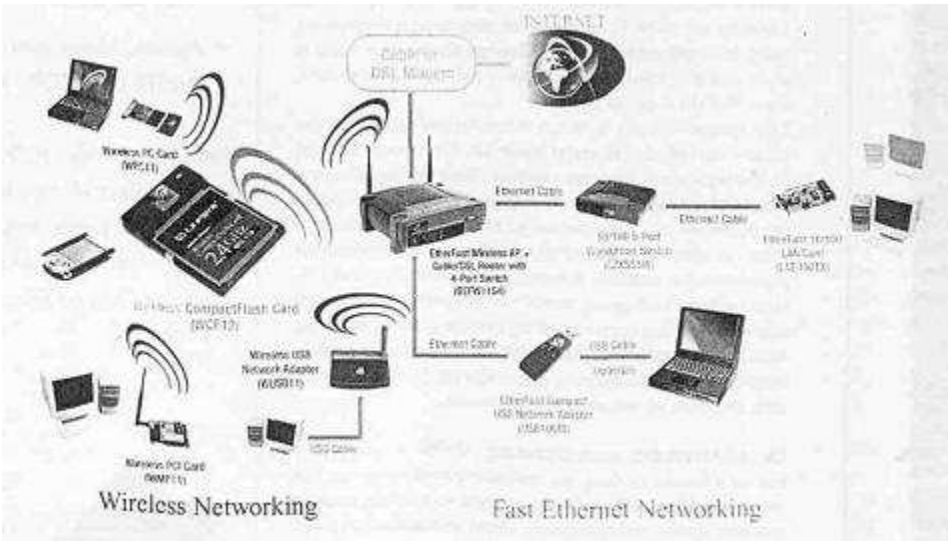
Μια τυπική διάταξη WLAN, μπορεί να περιλαμβάνει πλην των τερματικών σταθμών ένα ή περισσότερα σημεία πρόσβασης, τα οποία μπορεί να διασυνδέονται για να παρέχουν μεγαλύτερη κάλυψη. Υπάρχουν οι εξής αρχιτεκτονικές σύνδεσης:

- Η ανεξάρτητη διάταξη, στην οποία οι χρήστες συνδέονται απευθείας μεταξύ τους, χωρίς τη διαμεσολάβηση σημείων πρόσβασης (δίκτυο adhoc).
- Η ανεξάρτητη διάταξη με μεσολάβηση σημείου πρόσβασης, που λειτουργεί ως επαναλήπτης και διπλασιάζει πρακτικά την εμβέλεια του δικτύου.
- Δίκτυο σταθερής υποδομής με πολλαπλά, αλλά μεμονωμένα, σημεία πρόσβασης (περιοχές ασύρματης κάλυψης). Κάθε ασύρματο δίκτυο που περιλαμβάνει σημείο πρόσβασης, λέγεται συνήθως δίκτυο "infrastructure".

- Κυψελοειδές δίκτυο, με αλληλοεπικαλυπτόμενες κυψέλες, που παρέχουν δυνατότητα συνεχούς επικοινωνίας σε αρκετά μεγάλη περιοχή, κάτι σαν μικρογραφία του δικτύου της κινητής τηλεφωνίας.

Η εμβέλεια των ασύρματων καρτών και συσκευών εξαρτάται από πολλές παραμέτρους: από την ποιότητα κατασκευής του προϊόντος (κυρίως από τον πομποδέκτη που ενσωματώνουν), από την τεχνολογία μετάδοσης που χρησιμοποιείται, από τον περιβάλλοντα χώρο και από την ταχύτητα μετάδοσης των δεδομένων. Οποιαδήποτε στιγμή βρεθούν δύο ή περισσότεροι υπολογιστές στην ακτίνα δράσης των ασύρματων καρτών τους, αυτόματα συνθέτουν ένα ομότιμο δίκτυο (peer to peer). Αυτή είναι και η απλούστερη μορφή ενός ασύρματου δικτύου, η οποία εξυπηρετεί περιορισμένες ανάγκες και τη συναντάμε περισσότερο στα οικιακά δίκτυα ή σε μικρά δίκτυα στο γραφείο. Όλοι οι υπολογιστές σε ένα ομότιμο δίκτυο έχουν τα ίδια δικαιώματα και μοιράζονται εξίσου τους πόρους του δικτύου. Για την επικοινωνία πολλών ανεξάρτητων δικτύων, που θα συνδέονται μεταξύ τους ή για την επικοινωνία ενός ασύρματου δικτύου με ένα ενσύρματο, χρησιμοποιούνται τα λεγόμενα Access Points (Σημεία Πρόσβασης). Πρόκειται για ειδικές συσκευές, που διαθέτουν θύρα Ethernet και λειτουργούν κατά κάποιον τρόπο όπως τα hub, παρέχοντας όμως κάποιες επιπλέον δυνατότητες. Έχουν μεγαλύτερη ακτίνα δράσης από τις απλές ασύρματες κάρτες, επεκτείνοντας έτσι την εμβέλεια του ασύρματου δικτύου. Αυτό, με απλά λόγια σημαίνει ότι, αν δύο κόμβοι βρίσκονται έξω από την ακτίνα δράσης τους, είναι δυνατόν να επικοινωνήσουν μέσω του σημείου πρόσβασης. Επιπλέον, τα Access Points ελέγχουν την κίνηση του δικτύου, κατανέμουν ανάλογα με τον αριθμό των υπολογιστών το διαθέσιμο εύρος και φροντίζουν να κατευθύνουν τα πακέτα πληροφοριών. Για την εμβέλεια τους ισχύει ό,τι και για τις απλές ασύρματες κάρτες, ενώ ο αριθμός των κόμβων που μπορούν να "σηκώσουν" εξαρτάται από τον κατασκευαστή.

.



1.3) Ad hoc και Infrastructure Ασύρματα Δίκτυα

Στο IEEE 802.11 υπάρχουν 2 τρόποι για να σχηματιστεί ένα ασύρματο δίκτυο:
ad-hoc και infrastructure.

1.3.1) Infrastructure Ασύρματα Δίκτυα

Στα infrastructure δίκτυα υπάρχουν κάποια σταθερά σημεία πρόσβασης (access points-AP) μέσω των οποίων μπορούν οι διάφορες συσκευές να επικοινωνούν. Οι συσκευές έχουν ενσωματωμένους μηχανισμούς πρόσβασης στο ασύρματο μέσο μετάδοσης και επικοινωνούν με τα AP μέσω ραδιοκυμάτων. Τα AP μαζί με τις συσκευές που βρίσκονται στην δική τους κάλυψη, σχηματίζουν ένα βασικό σετ υπηρεσιών (Basic Service Set -BSS). Η σύνθεση των διαφόρων BSS, γίνεται μέσω των AP με ένα κατανεμημένο σύστημα και έτσι σχηματίζεται ένα δίκτυο. Οι συσκευές μπορούν να επιλέξουν ένα AP και να συσχετιστούν μαζί του. Τα AP παρέχουν συγχρονισμό μέσα στα BSS, υποστηρίζουν διαχείριση ενέργειας και μπορούν να ελέγχουν το μέσο πρόσβασης για υποστήριξη υπηρεσιών με χρονικούς περιορισμούς .

1.3.2) Ad hoc Ασύρματα Δίκτυα

Στα ad-hoc δίκτυα δεν υπάρχει κάποια συγκεκριμένη δομή στο δίκτυο Κάθε ασύρματος σταθμός έχει την δυνατότητα να επικοινωνήσει απευθείας με οποιονδήποτε άλλο σταθμό χωρίς να χρειάζεται να παρεμβληθεί στην επικοινωνία το access point. Έτσι μεταξύ των συσκευών μπορούν να δημιουργηθούν διάφορα BSS. Σε αυτή την περίπτωση, ένα BSS αποτελείται από συσκευές που λειτουργούν και εκπέμπουν στην ίδια συχνότητα. Υπάρχουν διάφοροι αλγόριθμοι για την διατήρηση τέτοιου είδους δικτύου

όπως για παράδειγμα αλγόριθμοι εκλογής προέδρου, όπου ένας κόμβος λειτουργεί σαν σταθμός βάση (base station) ή αφέντης και οι άλλοι σαν «σκλάβοι», αλγόριθμοι υπερχείλισης (flooding) και ευρείας μετάδοσης για επικοινωνία μεταξύ των κόμβων. Τα ad-hoc δίκτυα μπορούν να φανούν χρήσιμα, π.χ κατά την διάρκεια μια σύσκεψης οι συμμετέχοντες επικοινωνούν μεταξύ τους και ανταλλάσσουν αρχεία.

1.4) Χαρακτηριστικά ενός ασυρματου LAN

Η ζώνη των 2.4GHz γίνεται ολοένα και πιο δημοφιλής σήμερα. Ο λόγος γι' αυτό είναι ότι πρόκειται για ελεύθερη ζώνη και έχει κατάλληλα χαρακτηριστικά για μετάδοση σε μικρές αποστάσεις

Παρεμβολές

Τα ασύρματο LAN μπορεί να δεχτεί και να προκαλέσει παρεμβολλές σε άλλα 2.4GHz προϊόντα όπως μερικά ασύρματα τηλέφωνα ή φούρνοι μικροκυμάτων. Γενικά πάντως δεν έχει παρατηρηθεί να έχουν σημαντικό πρόβλημα με παρεμβολλές από φούρνους μικροκυμάτων. Μπορεί επίσης να δεχθεί παρεμβολλές από αρμονικές από συσκευές που εκπέμπουν σε υποπολαπλάσια της συχνότητας λειτουργίας. Το σημαντικότερο πρόβλημα παρεμβολλών πάντως προκύπτει από την κακή σχεδίαση ενός ασύρματου ραδικτύου (μεγάλύτερες ισχυς εκπομπής από το αναγκαίο, κακές και ακατάλληλες καραίες, λάθος επιλογή συχνοτήτων και τοποθεσίας, συσκευές με μικρή ευαισθησία κ.τ.λ)

Εμβέλεια

Η εμβέλεια ενός ασύρματου δικτύου σε περιβάλλον γραφείου μπορεί να είναι μερικές δεκάδες μέτρα. Τα ραδιοκύματα σε εσωτερικό χώρο λεχουν να διαπεράσουν τοίχους και οροφές οπότε υφίστανται σημαντική απόσβεση. Δηλαδή όταν ένα ραδιοκύμα προσπέσει σε ένα τοίχο ένα μέρος της ισχύος του θα απορροφηθεί από το υλικό του τοίχου και ένα κομμάτι μόνο θα μπορεί να τον διαδοθεί. Επίσης το σήμα θα ανακλαστεί στις περιβάλλουσες επιφάνειες με αποτέλεσμα στο δέκτη τελικά να φτάσουν ένας αριθμός από αντίγραφα του αρχικού σήματος, όλα με διαφορετικά πλάτη και φάσεις. Από την άθροιση τους μπορεί να προκύψει αλληλοαναίρεση και το τελικό σήμα να έχει πολύ μικρότερη ισχύ με αποτέλεσμα την υποβάθμιση της ποιότητας της ζευξης.
Σε περιβάλλον όπου υπάρχει κατευθείαν οπτική επαφή, σε εξωτερικό χώρο, η εμβέλεια είναι πολύ μεγαλύτερη, εξαρτάται από την ισχύ εκπομπής, την ευαισθησία του δέκτη, τις κεραίες, την απόσταση, την ευθυγράμμιση των κεραιών, το επίπεδο παρεμβολών και θορύβου. Πάντως αποστάσεις αρκετών χιλιομέτρων είναι δυνατό να επιτευχθούν με πολύ καλή ποιότητα ζεύξης.

Ρυθμός μετάδοσης
Η πραγματική διαπερατότητα του συστήματος εξαρτάται από ένα πλήθος παραγόντων όπως οι παράμετροι ραδιομετάδοσης (εμβέλεια, ανακλάσεις, απορρόφηση, σκέδαση) , όπως και από τον αριθμό των χρηστών. Για τις περισσότερες εφαρμογές το bandwidth είναι επαρκές.

Ποιότητα επικοινωνίας
Έχοντας πίσω τους μισό αιώνα σε εμπορικές και κυρίως σε στρατιωτικές εφαρμογές οι ασύρματες τεχνολογίες έχουν γίνει πολύ στιβαρές και αξιόπιστες. Έτσι μπορούν να περέχουν αξιόπιστες συνδέσεις και μάλιστα ίσως σε καλύτερο επίπεδο από ότι οι αντίστοιχες στην κινητή τηλεφωνία.

Συμβατότηταμε το υπάρχον δίκτυο
Τα περισσότερα WLAN έχουν προτυποποιημένο τρόπο σύνδεσης με τα υπάρχοντα ενσύρματα δίκτυα. Συστήματα διαχείρησης επιβλέπουν τους ασύρματους κόμβους οποώς και οποιοδήποτε αλλο στοιχείο δικτύου.

Διαλειτουργικότητα
Υπαρχουν οι εξής περιπτώσεις στις οποίες οι συσκευές δεν συνεργάζονται μεταξύ τους:
1)***Διαφορετικές τεχνολογίες***
Ένα ράδιο βασισμένο σε τεχνολογία FHSS δεν μπορεί να συνεργαστεί με κάποιο τεχνολογίας DSSS.

2)***Διαφορετικές συχνότητες***
Προφανώς συσκευές 802.11a στους 5.7GHz δεν μπορουν να δουλέψουν μαζί με συσκευές 802.11b/g που εργάζονται στους 2.4GHz.

3)***Διαφορετικές υλοποιήσεις***
Προϊόντα διαφορετικών κατασκευαστών μπορεί να μην συνεργάζονται ή να συνεργάζονται μερικώς μεταξύ τους. Για παράδειγμα υπάρχει ένας αριθμός προϊόντων βασισμένα σε chipsets της Texas Instruments τα οποία υποστηρίζουν ένα τρόπο μετάδοσης 22Mbps. Αυτός όμως ισχύει μόνο μεταξύ συσκευών της ίδιας εταιρίας. Για μία λύση του προβλήματος της δια λειτουργικότητας δημιουργήθηκε το Wifi πιστοποιητικό .

1.5) Εξοπλισμός

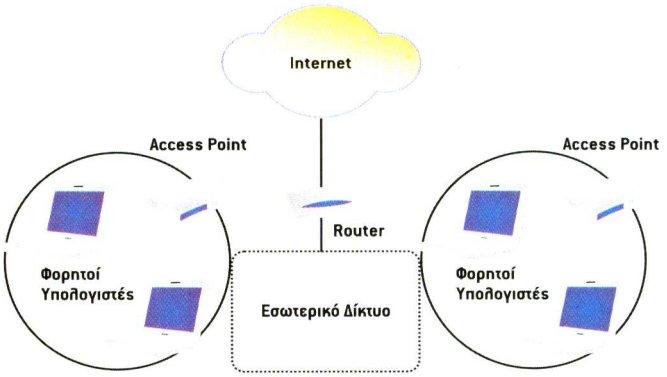
Η πρόσβαση στο ασύρματο δίκτυο είναι δυνατή από ένα σύνολο συσκευών συμβατών με τα κατάλληλα πρωτόκολλα επικοινωνίας, όπως φορητοί υπολογιστές (laptops), έξυπνες συσκευές χειρός (handheld pdas, τηλέφωνα κλπ), ασύρματες κάμερες και οθόνες τηλε-προβολής κ.α.
Η ευκολία με την οποία μπορεί κανείς να "στήσει" ένα ασύρματο τοπικό δίκτυο, ήταν ένας από τους βασικούς παράγοντες που συνέβαλαν στη ραγδαία εξάπλωση τους. Τα στοιχεία τα οποία χρειάζεται ένα WLAN για να λειτουργήσει, καθώς και για να συνδεθεί στο ευρύτερο δίκτυο, είναι:

- Προσαρμογείς: που λειτουργούν ως συνδετικά στοιχεία μεταξύ του τελικού εξοπλισμού του χρήστη και του σημείου ασύρματης πρόσβασης του δικτύου.
- Σημεία πρόσβασης: που είναι πομποδέκτες με μία ή δύο κεραίες. Συνδέονται με το ενσύρματο τοπικό δίκτυο (ή με την ευρυζωνική σύνδεση). Μέσω αυτών, επικοινωνεί ο προσαρμογέας του τελικού χρήστη με το υπόλοιπο δίκτυο.
- Γέφυρες: Παρέχουν την από σημείο σε σημείο ασύρματη σύνδεση μεταξύ δύο WLANs, όπως μεταξύ δύο ορόφων.
- Κόμβοι Διανομής: Συγκεντρώνουν και συνδέουν πολλαπλά σημεία ασύρματης πρόσβασης με το ενσύρματο ή ασύρματο δίκτυο κορμού.
- Κόμβοι κορμού: Διασυνδέουν τους κόμβους διανομής. Καλύπτουν πολλούς χρήστες, λόγω του μεγάλου αριθμού των σημείων πρόσβασης που είναι συνδεδεμένα μέσω των κόμβων διανομής με αυτά. Σχεδόν πάντα επικοινωνούν μεταξύ τους, με περισσότερες από μία συνδέσεις, για να μειωθούν περιπτώσεις απώλειας επαφής.

Με τον τρόπο αυτό, και χωρίς τη χρήση καλωδίων, επιτυγχάνεται η διασύνδεση όλων των υπολογιστικών συστημάτων του χώρου. Για την επέκταση του δικτύου απαιτείται απλά η εγκατάσταση ενός επιπλέον σημείου ασύρματης πρόσβασης.Ένα δίκτυο WLAN υλοποιείται ως εξής: Πολυκατευθυντικές κεραίες τοποθετούνται σε σημεία πρόσβασης ή σε κόμβους διανομής / κορμού, ενώ κατευθυντικές στους τελικούς χρήστες. Οι κεραίες αυτές είναι εξωτερικές και συνήθως βρίσκονται στις κορυφές κτιρίων στο κέντρο της περιοχής χρήσης. Ένας απλός χρήστης που θέλει μόνο να συνδεθεί, αλλά να μη διευκολύνει την ευρύτερη δικτύωση, χρειάζεται μία κατευθυντική κεραία. Με αυτή, μπορεί να εξασφαλίσει πρόσβαση από ένα σημείο πρόσβασης, ώστε να έχει σύνδεση στο τοπικό δίκτυο και ενδεχομένως και στο διαδίκτυο (αν το σημείο πρόσβασης παρέχει τέτοια δυνατότητα). Ένας πιο ενεργός χρήστης μπορεί να χρησιμοποιεί δύο κατευθυντικές κεραίες, ώστε να φροντίζει για τη συνέχιση του δικτύου ή και μια πολυκατευθυντική για να

λειτουργεί ο ίδιος σαν σημείο πρόσβασης άλλων χρηστών. Αν κάποιος κόμβος έχει πάνω από δύο κατευθυντικές κεραίες, μπορεί να διευκολύνει και την πολλαπλή δρομολόγηση. Με τον τρόπο αυτό μπορεί να δημιουργηθεί ένα δίκτυο που να καλύπτει μία πύλη. Τέλος, συνδέοντας ο χρήστης μία δική του γραμμή DSL με το WLAN, θα μπορούσε να γίνει "πύλη" για το Διαδίκτυο και να επιτρέπει την πρόσβαση γειτονικών χρηστών σε αυτό.

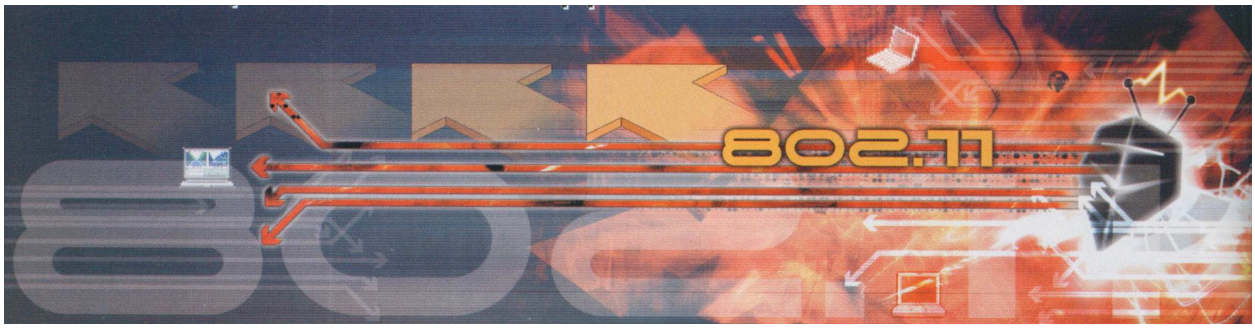
Ένα ασύρματο δίκτυο στην πράξη



Τα access points λειτουργούν ως συνδετικοί κρίκοι ανάμεσα στους υπολογιστές του ασύρματου δικτύου, ενώ χρησιμεύουν και για τη σύνδεσή τους με συμβατικά δίκτυα.

ΚΕΦΑΛΑΙΟ 2^{Ο}

ΠΡΩΤΟΚΟΛΛΑ & ΚΑΤΗΓΟΡΙΕΣ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ



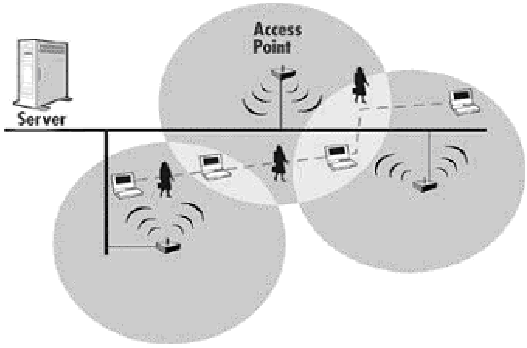
2.1) Το πρότυπο IEEE 802.11

Ένα ασύρματο τοπικό δίκτυο είναι αυτό στο οποίο ένας κινούμενος χρήστης μπορεί να συνδεθεί σε ένα τοπικό δίκτυο μέσω μια ασύρματης σύνδεσης. Το 1997 με την εισαγωγή του προτύπου 802.11, γινεται δυνατή η ασύρματη μεταφορά δεδομένων σε ταχύτητες μέχρι και 2Mbps.

Στα πέντε χρόνια που μεσολάβησαν το συγκεκριμένο πρωτόκολλο υπέστη πολλές αλλαγές και πλέον , με την εισαγωγή τριών νέων εκδόσεών του, αναμένεται να αποτελέσει μία άκρως ενδιαφέρουσα επιλογή για πολλές κατηγορίες χρηστών.Το πρότυπο IEEE 802.11 περιγράφει τις τεχνολογίες που χρησιμοποιούνται στα ασύρματα τοπικά δίκτυα.
Το 802.11 είναι μια οικογένεια προδιαγραφών για ασύρματα τοπικά δίκτυα που αναπτύχθηκαν από ομάδες εργασίας του ινστιτούτου ηλεκτρολόγων και ηλεκτρονικών μηχανικών, το γνωστό institute of electrical and electronics engineers (IEEE).
Όλα τα πρότυπα που περιλαμβάνει το 802.11, χρησιμοποιούν το πρωτόκολλο ethernet και μέθοδο πολλαπλής πρόσβασης με ανίχνευση φέροντος και αποφυγή συγκρούσεων, το carrier sense multiple access with collision avoidance (csma/ca). Η μέθοδος διαμόρφωσης που χρησιμοποιήθηκε αρχικά ήταν το κλείδωμα μεταλλαγής φάσης ή διαμόρφωση διακριτής φάσης, phase-shift keying (psk). Σε νεότερες προδιαγραφές όμως, χρησιμοποιούνται και άλλα σχήματα ψηφιακής διαμόρφωσης, όπως το complementary code keying (cck). Οι νεότερες μέθοδοι διαμόρφωσης παρέχουν μεγαλύτερους ρυθμούς μετάδοσης

δεδομένων.
Αυτή τη στιγμή υπάρχουν 4 πρότυπα στην οικογένεια 802.11: 802.11, 802.11a, 802.11b, 802.11g και μέχρι το τέλος του έτους αναμένεται να εγκριθούν τα 802.11i και 802.11e. Και τα 4 χρησιμοποιούν το πρωτόκολλο ethernet και μέθοδο πολλαπλής πρόσβασης με ανίχνευση φέροντος και αποφυγή συγκρούσεων, το carrier sense multiple access with collision avoidance (csma/ca).
IEEE 802.11:
Δημοσιεύθηκε το 1997 από την IEEE , μετά από επτά χρόνια μελέτης
Προβλέπει ρυθμούς μετάδοσης 1 και 2 Mbps
Υποστηρίζει ασύγχρονη, connectionless υπηρεσία
Στο φυσικό επίπεδο προβλέπει τεχνική FHSS ή DSSS σε ζώνες συχνοτήτων 915MHz , 2.4MHz , 5.2MHz ή υπέρυθρη μετάδοση στα 850nm ως 900nm
Υποστηρίζει δυνατότητες όπως προτεραιοποίηση της κίνησης, υποστήριξη εφαρμογών πραγματικού χρόνου και διαχείριση ισχύος συσκευής. Τα ασύρματα δίκτυα 802.11 αποτελούνται από τις κάτωθι τέσσερις βασικές μονάδες:

- Σημείο πρόσβασης (Access Point - AP): Το AP είναι η μονάδα που παίζει το ρόλο γέφυρας μεταξύ του ενσύρματου και του ασύρματου δικτύου, μετατρέποντας κατάλληλα τα πλαίσια που ανταλλάσσονται μεταξύ αυτών. Επιτελεί και πολλές άλλες λειτουργίες στο ασύρματο δίκτυο που θα αναφερθούν στη συνέχεια.
- Σύστημα διανομής (Distribution System): Το σύστημα διανομής ενώνει τα διάφορα AP του ίδιου δικτύου, επιτρέποντάς τους να ανταλλάσσουν πλαίσια. Το 802.11 δεν προσδιορίζει τον τρόπο που θα γίνεται αυτό.
- Ασύρματο μέσο μετάδοσης (Wireless Medium): Έχουν οριστεί διάφορα φυσικά στρώματα που χρησιμοποιούν είτε ραδιοσυχνότητες είτε υπέρυθρες ακτίνες για τη μετάδοση των πλαισίων μεταξύ των σταθμών του ασύρματου δικτύου.
- Σταθμοί (Stations): Οι σταθμοί που ανταλλάσσουν πληροφορία μέσω του ασυρμάτου δικτύου συνήθως είναι φορητές συσκευές (για παράδειγμα laptops ή PDAs) χωρίς όμως αυτό να είναι απαραίτητο.



2.1.1)ΥΠΗΡΕΣΙΕΣ ΤΟΥ IEEE 802.11

Η IEEE802.11 ορίζει υπηρεσίες που πρέπει να προσφέρονται, δεν ορίζει συγκεκριμένες υλοποιήσεις. Αφήνει έτσι τους κατασκευαστές να υλοποιήσουν με τον δικό οτυς τρόπο την κάθε υπηρεσία, αφήνοντας έτσι περιθώριο για κάτι πιο αποδωτικό.

Οι υπηρεσίες που περιγράφονται υλοποιούνται απο το MAC επίπεδο και μπορούν να χωριστούν σε δύο κατηγορίες:

Υπηρεσίες σταθμού (SS, Station Service)
Οι υπηρεσίες αυτές υλοποιούνται σε κάθε ασύρματο σταθμό.

a) Authentication
b) Deauthentication
c) Privacy
d) MSDU delivery

Υπηρεσίες συστήματος διανομής (DSS, Distribution System Service)
Οι υπηρεσίες αυτές υλοποιούνται μόνο στα AP, Access Point

a) Association
b) Disassociation
c) Distribution
d) Integration
e) Reassociation

Μπορεί να υποθέσει κανείς ότι η διαφορά ενός AP από έναν client είναι μόνο η υλοποίηση των υπηρεσίων της δεύτερης κατηγορίας. Οι υπηρεσίες αυτές υλοποιούνται με λογισμικό και όχι με επιπλεόν υλικό και έτσι η μεγάλη διαφορά κόστους που συνήθως υπάρχει ανάμεσα στις αντίστοιχες συσκευές δεν δικαιολογείται από την πλευρά του πραγματικού κόστους τους.

- ***Υπηρεσίες σταθμού***

Το 802.11 ορίζει έναν αριθμό από παρεχόμενες υπηρεσίες μεταξύ των σταθμών.

Security
Η λειτουργία της ασφάλειας είναι ευθύνη του MAC επιπέδου και περιλαμβάνει τον έλεγχο της πρόσβασης και τη λειτουργία της κωδικοποίησης και οι οποίες είναι γνωστές σαςν WEP, Wired Equivalent Privacy. Η ονομασία είναι αρκετά πομπώδης κα υπονοεί ότι καταφέρνει να εξασφάλίσει ισοδύναμο βαθμό ασφαλείας στο ασύρματο μέσο με αυτό του ενσύρματου.

Για τον έλεγχο της πρόσβασης κάθε AP προγραμματίζεται με ένα μοναδικό ESSID (WLAN Serviec Area ID). Κάθε σταθμός πρέπει να γνωρίζει το ESSID προκειμένου να συσχετιστεί με το AP. Αυτό έχει το νόημα ελέγχου αυθεντικότητας. Επίσης το AP έχει έναν πίνακα με MAC διευθύνσεις (Access Control List) , και οι σταθμοί προκειμένου να μπορούν να συνδεθούν πρέπει να έχουν την MAC τους στον πίνακα αυτό. Επίσης ο πίνακας αυτός μπορεί να περιέχει τις διευθύνσεις που αποκλείονται από την πρόσβαση.

Authentication
Ορίζονται διαδικασίες αυθεντικοποίησης ώστε να ελεγχθεί η πρόσβαση στο WLAN. Ο σκοπός της αυθεντικοποίησης είναι να παρέχει έλεγχο πρόσβασης όμοιο με αυτόν στα ενσύρματα LAN.

Παρέχει ένα μηχανισμό για ένα σταθμό να προσδιορίζει άλλον. Χωρίς απόδειξη της ταυτότητας του ένας σταθμός δεν επιτρέπεται να χρησιμοποιεί το WLAN. Όλοι οι 802.11 σταθμοί είτε είναι μέρος ενός ανεξάρτητου BSS ή ESS δικτύου πρέπει να χρησιμοποιήσουν την υπηρεσία αυτή πριν επικοινωνήσουν με άλλον σταθμό.
Ορίζονται δύο τύποι αυθεντικοποίησης:

Open system authentication
Είναι ο εξ' ορισμού τρόπος, είναι πολύ απλός και έχει δύο βήματα. Πρώτα ο σταθμός που θέλει να κάνει την αυθεντικοποίηση στέλενει ένα πλαίσιο αυθεντικοποίησης το οποίο περιέχει την ταυτότητα του. Ο άλλος σταθμός στέλνει πίσω ένα πλαίσιο που περιέχει την πληροφορία αναγνώρισης ή μη της ταυτότητας του αποστολέα.

Shared key authentication
Ο κάθε σταθμός έχει λάβει ένα κρυφό κλειδί, μέσω ενός καναλιού το οποίο είναι ανεξάρτητο του 802.11 δικτύου. Οι σταθμοί κάνουν αυθεντικοποίηση μέσω της κοινής γνώσης του κρυφού κλειδιού. Η υλοποίηση αυτή απαιτεί την κρυπτογράφηση μέσω αλγορίθμου WEP, Wired Equivalent Privacy.

De-authentication
Η υπηρεσία αυτή αφορά την απομάκρυνση ενός σταθμού που είχε προηγούμενα αυθεντικοποιηθεί από το δίκτυο. Για να αποκτήσει πάλι ο σταθμός πρόσβαση πρέπει να επαναληφθεί η διαδικασία αυθεντικοποίησης. Το μύνημα απο-αυθεντικοποίησης έχει το νόημα ειδοποίησης και δεν μπορεί να απορριφθεί. Το αντίστοιχο πλαίσιο μπορεί να σταλεί από ένα σταθμό ή από το AP.

Privacy
Το πρότυπο προτείνει για την κωδικοποίηση των δεδομένων τη χρήση κλειδιού μήκους 40-bit. Η υπηρεσία αυτή είναι προαιρετική. Ο

αλγόριθμος είναι ο RC4 PRNG από την RSA Data Security. Όλα τα δεδομένα που στέλνονται και λαμβάνονται μεταξύ του AP και των συσχετιζόμενων σταθμών του, έχουν κωδικοποιηθεί με αυτό το κλειδί. Επιπρόσθετα όταν ένας σταθμός προσπαθήσει να συσχετιστεί με ένα AP, το AP του στέλνει ένα κωδικοποιημένο πακέτο, ο σταθμός πρέπει κωδικοποιήσει την σωστή απάντηση χρησιμοποιώντας το κλειδί του, ώστε να κερδίσει πρόσβαση στο δίκτυο
Η υπηρεσία αυτή έχει σκοπό να παρέχει ένα ισοδύναμο επίπεδο προστασίας με αυτό που παρέχεται στα ενσύρματα δίκτυα, όπου η φυσική πρόσβαση είναι περιορισμένη. Παρέχει προστασία στα δεδομένα στο κομμάτι της διαδρομής τους στο ασύρματο μέσο. Δεν παρέχει πλήρη προστασία από άκρο σε άκρο μεταξύ εφαρμογών που λειτουργούν σε ένα μικτό δίκτυο. Στο ασύρματο δίκτυο όλοι ο σταθμοί καθώς και άλλες συσκευές μπορούν να αφουγκραστούν τα δεδομένα που ανταλλάσονται, και έτσι να θέσουν σημαντικά προβλήματα ασφαλείας στο δίκτυο. Το πρότυπο προσφέρει μία υπηρεσία η οποία αυξάνει την ασφάλεια του δικτύου και την κάνει παρόμοια με αυτή ενός ενσύρματου δικτύου. Έτσι κωδικοποιεί τα πακέτα δεδομένων καθώς και κάποια πακέτα διαχείρισης με ένα αλγόριθμο βασισμένο στον αλγόριθμο WEP, Wired Equivalent Privacy toy 802.11

Πέρα από τις υπηρεσίες ασφαλείας δευτέρου επιπέδου, μπορεί να χρησιμοποιηθούν και υπηρεσίες ανωτέρω επιπέδων για έλεγχο της πρόσβασης και κωδικοποίηση, όπως το IPsec ή κωδικοποίηση επιπέδου εφαρμογής. Αυτές οι τεχνολογίες ανωτέρων επιπέδων μπορεί να δημιουργήσουν ένα δίκτυο ασφαλές από άκρο σε άκρο, που να περιλαμβάνει ασύρματες και ενσύρματες τεχνολογίες.

Data Delivery Data
Παρόμοια με αυτή που παρέχεται από άλλα δίκτυα IEEE 802. Η υπηρεσία αυτή παρέχει αξιόπιστη μεταφορά των πακέτων δεδομένων από το MAC του ενός σταθμού στο MAC ενός άλλου, με ελάχιστα διπλότυπα και αναδιατάξεις. Ο όρος αξιόπιστη μεταφορά σημαίνει ότι θα ζητηθεί επανεκπομπή των πακέτων αν διαπιστωθεί ότι αυτά έχουν λάθη. Ο λόγος που δεν αφήνουμε στα ανώτερα επίπεδα να χειριστούν το θέμα αυτό είναι ότι ο ραδιοφορέας είναι μη αξιόπιστος φορέας μετάδοσης και πολλά λάθη συμβαίνουν, άρα πολλές επανεκπομπές θα χρειαστούν να γίνουν.

- ***Υπηρεσίες συστήματος διανομής***

Παρέχουν διάφορες λειτουργίες στο DS. Τυπικά αυτές παρέχονται από τα AP

Association
Υπηρεσία με την οποία δημιουργείται μία λογική σύνδεση μεταξή ενός ασύρματου σταθμού και ενός AP. Κάθε σταθμός σχετίζεται με ένα AP, πριν του επιτραπεί να στείλει δεδομένα μέσω του AP προς το DS. Η σύνδεση αυτή είναι απαραίτητη έτσι ώστε το DS να γνωρίζει που και πως θα παραδώσει δεδομένα στον ασύρματο σταθμό. Ο ασύρματος σταθμός επικαλείται την υπηρεσία αυτή μόνο μία φορά κατά την είσοδο του στο BSS. Κάθε σταθμός σχετίζεται με μόνο ένα AP και ένα AP μπορεί να σχετιστεί με πολλούς σταθμούς.

Disassociation
Υπηρεσία που σκοπό έχει να επιβάλλει σε σταθμό να εγκαταλείψει μία συσχέτιση με ένα AP ή για ένα σταθμό να ενημερώσει το AP ότι δεν χρειάζεται πλέον τις υπηρεσίες του DS. Όταν ένας σταθμός αποσυσχετιστεί, πρέπει να ξεκινήσει μία καινούργια συσχέτιση με ένα AP. Ένα AP μπορεί να αναγκάσει ένα ή περισσότερους σταθμούς να απομακρυνθούν, λόγω περιορισμένων πόρων ή γιατί το AP απομακρύνεται από το δίκτυο. Όταν ο σταθμός ενημερωθεί ότι δεν θα έχει πλέον τις υπηρεσίες ενός AP, μπορεί να επικαλεστεί την υπηρεσία αποσυσχέτισης ώστε να ειδοποιήσει το AP ότι η λογική σύνδεση μεταξύ τους δεν απαιτείται πλέον. Οι σταθμοί πρέπει να αποσυσχετίζονται όταν αφήνουν το δίκτυο. Η αποσυσχέτιση έχει τη μορφή ειδοποίησης και μπορεί να σταλεί από οποιοδήποτε από τα συσχετιζόμενα μέρη και κανένα από τα δύο δεν μπορεί να την αρνηθεί..

Re-association
Η επανασυσχέτιση επιτρέπει σε ένα σταθμό να αλλάξει τη τρέχουσα συσχέτιση του με ένα AP. Είναι παρόμοια υπηρεσία με τη συσχέτιση με τη διαφορά ότι περιέχει πληροφορία για το AP στο οποίο ο σταθμός ήταν πριν συσχετισμένος. Ένας σταθμός χρησιμοποιεί την υπηρεσία αυτή καθώς μετακινείται διαρκώς σε ένα ESS δίκτυο, χάνει την επαφή με το AP με το οποίο είχε συσχετιστεί και χρειάζεται να συσχετιστεί με κάποιο καινούργιο. Με την υπηρεσία αυτή. Στέλνοντας πληροφορία για το προηγούμενο AP με το οποίο είχε συσχετιστεί, το καινούργιο AP μπορεί να επικοινωνήσει με το προηγούμενο και να αποκτήσει τα πακέτα τα οποία μπορεί να έχουν παραμείνει εκεί προς παράδοση στον σταθμό. Η υπηρεσία επανασυσχέτισης αρχικοποιείτε πάντα από τον σταθμό

Distribution
Η διανομή είναι βασική υπηρεσία η οποία παρέχεται από έναν 802.11 σταθμό. Ο σταθμός χρησιμοποιεί την υπηρεσία κάθε φορά που στέλνει ένα MAC πλαίσιο προς το DS. Το DS αναλαμβάνει τη διανομή του χρησιμοποιώντας την πληροφορία που έχει αποκτήσει με τις υπηρεσίες συσχέτισης. Ο σταθμός πρέπει να έχει συσχετιστεί με ένα AP ώστε να γίνει η προώθηση των πλαισίων σωστά.

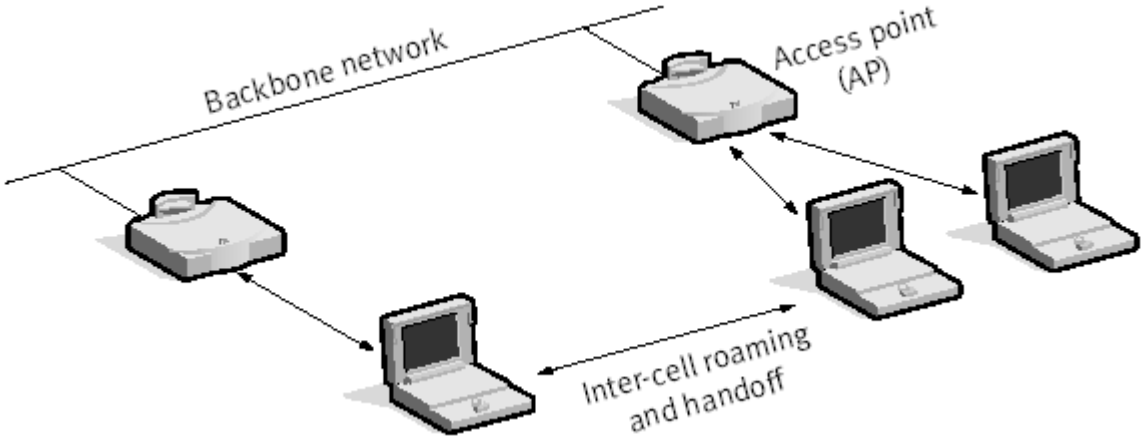
Integration
Η υπηρεσία αυτή συνδέει ένα δίκτυο 802.11 WLAN σε άλλα LANs ενσύρματα ή ασύρματα. Ένα portal είναι αυτό που υλοποιεί την υπηρεσία αυτή. Τυπικά βρίσκεται σε ένα AP, μπορεί όμως και να είναι τμήμα ενός διαφορετικού δικτύου. Η υπηρεσία αυτή μεταφράζει πλαίσιο 802.11 σε πλαίσια που μπορούν να μεταδοθούν σε άλλο δίκτυο και το ανάστροφο.

Roaming
Ο τρόπος με τον οποίο γίνεται η συσχέτιση ενός σταθμού με το AP είναι εργασία του MAC επιπέδου. Όταν ένας σταθμός βρεθεί εντός εμβέλειας ενός ή περισσοτέρων AP, διαλέγει εκείνο το AP το οποίο έχει καλύτερο σήμα ή μικρότερο αριθμό λαθών. Η διαδικασία αυτή λέγεται Joining a Basic Service Set . Όταν γίνει αποδεκτή η συσχέτιση από το AP, ο σταθμός συντονίζεται στο κανάλι εκπομπής του AP. Περιοδικά γίνεται ανίχνευσή των καναλιών και στην περίπτωση που βρεθεί κανάλι με καλύτερα χαρακτηριστικά, γίνεται επανασυσχέτιση με το καινούργιο AP και συντονισμός του σταθμού στην καινούρια συχνότητα. Η επανασυσχέτιση μπορεί να γίνει λόγω φυσικής μετακίνησης του σταθμού ή μπορεί να γίνει σαν αποτέλεσμα υψηλού φόρτου στο δίκτυο. Η λειτουργία αυτή γνωστή ως " load balancing " κατανέμει τον συνολικό φόρτο του WLAN με αποτελεσματικό τρόπο στην ασύρματη δομή του. Αυτός ο δυναμικός τροπος συσχέτισης επιτρέπει την διάρθρωση ενός WLAN με πολύ ευρεία κάλυψη απλώς δημιουργόντας μία σειρά από 802.11 κυψέλες. Για να πετύχει μια τέτοια σχεδίαση πρέπει οι κυψέλλες να σχεδιαστούν σωστά, δηλαδή να γίνει επιλογή της τοποθεσίας, της συχνότητας, των κεραιών.

Με χρήση των παραπάνω υπηρεσιών οι χρήστες (τα ανώτερα επίπεδα) μπορούν να απολαμβάνουν τις ακόλουθες δυνατότητες:

Mobility
Ενώ το πρότυπο περιγράφει πως ένας σταθμός συσχετίζεται σε ένα AP, δεν ορίζει πως τα AP ανιχνεύουν τους χρήστες, καθώς αυτοί περιάγονται. Αυτό μπορεί να γίνει είτε σε επίπεδο 2, μεταξύ δύο AP στο ίδιο υποδίκτυο, είτε σε επίπεδο 3, όταν ο χρήστης διασχίζει το σύνορο μεταξύ υποδικτύων.
Ο πρώτος τρόπος μπορεί να γίνει με πρωτόκολλα που έχουν δημιουργηθεί από τον κατασκευαστή και τα οποία μπορεί να είναι διαφορετικά και να ποικίλουν στην επίδοση τους. Αν το πρωτόκολλο δεν είναι αποτελεσματικό, υπάρχει πιθανότητα να χαθούν πακέτα καθώς ο χρήστης περιάγεται από AP σε AP. Η WECA και η IEEE δημιουργούν πρότυπα και σε αυτό το κομμάτι.
Ο δεύτερος τρόπος μπορεί να υλοποιηθεί με αντίστοιχα πρωτόκολλα, όπως το Mobile IP ή αλλιώς RFC2002. Σε αυτό κάθε χρήστης έχει

ορισμένο ένα AP, σαν "home agent". Όταν ένας σταθμός μπαίνει σε άλλη περιοχή, το νέο AP ρωτάει το σταθμό για τον "home agent". Στη συνέχεια εγκαθίσταται ένας μηχανισμός προώθησης πακέτων από το ένα AP στο άλλο, έτσι ώστε η IP του χρήστη να διατηρηθεί και ο χρήστης να λαμβάνει διαφανώς τα δεδομένα του. Το πρωτόκολλο αυτό δεν είναι ακόμα στην τελική του μορφή, οπότε οι κατασκευαστές μπορεί να παρέχουν τα δικά τους αντίστοιχα.
Τέλος μία ατελής αλλά αποτελεσματική λύση είναι το πρωτόκολλο DHCP , ώστε να ανατίθενται αυτόματα νέες διευθύνσεις στον χρήστη που περιάγεται στο δίκτυο.



2.2) Φυσικό επίπεδο (PHY Layer)

Το πρότυπο ***802.11*** ορίζει τρία διαφορετικά PHY επίπεδα.Η ύπαρξη περισσότερων από ένα επιπέδων κάνει την τεχνολογία περισσότερο ευέλικτη στα χέρια των σχεδιαστών συστημάτων. Το πρότυπο 802.11 προσδιορίζει ένα οπτικό PHY που
χρησιμοποιεί υπέρυθρες ακτίνες για μετάδοση με ταχύτητες 1 ή 2 Mbps και δύο PHY ραδιοσυχνότητας (RF-based), τα οποία λειτουργούν στην περιοχή συχνοτήτων των 2,4 GHz του ISM (Industrial, Scientific and Medical).
Τα δύο PHY επίπεδα ραδιοσυχνότητας ανήκουν στην κατηγορία των τεχνικών διασποράς φάσματος (spread spectrum techniques)
πιο αναλυτικα:

- ***Για την ασύρματη μετάδοση μεταξύ των σταθμών υπάρχουν τρεις τεχνικές:***

2.2.1) Υπέρυθρες (Infrared light). Αυτή η μέθοδος προσφέρει ένα μεγάλο εύρος ζώνης και μπορεί να εκπέμπει σήματα σε πολύ μεγάλες

ταχύτητες. Προϋπόθεση για αυτή την τεχνική είναι το ότι πομπός και δέκτης πρέπει να έχουν οπτική επαφή μεταξύ τους και να ευρίσκονται σε μικρές αποστάσεις 10-20 μέτρα. Τυπικές ταχύτητες με αυτή την τεχνική είναι 10 Mbps.

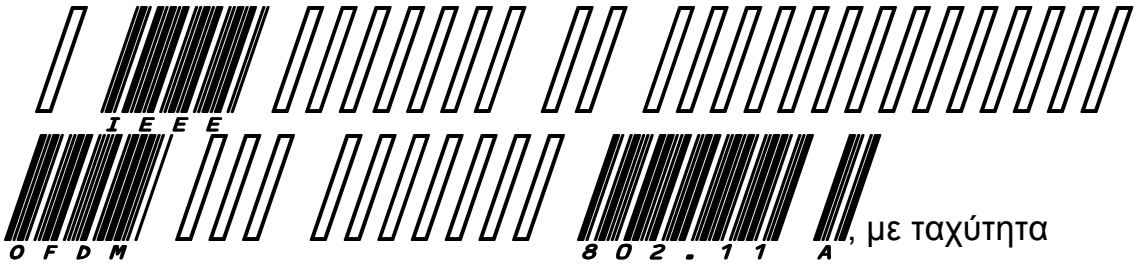
2.2.2) Ραδιοσυχνότητες στενής ζώνης ή απλής συχνότητας (Narrow-band radio). Πρόκειται για τεχνική παρόμοια με την εκπομπή ραδιοσταθμών . Ρυθμίζοντας σε μια συχνότητα πομπό και δέκτη και μη έχοντας την ανάγκη οπτικής επαφής, επιτυγχάνεται η επικοινωνία με τυπικές ταχύτητες γύρω στα 4.8 Mbps. Μειονέκτημα της τεχνικής αυτής είναι η λειτουργία σε μια απλή συχνότητα που κάνει την επικοινωνία ευαίσθητη σε παρεμβολές.

2.2.3) Κωδικοποίηση διασποράς φάσματος [Spread Spectrum]
Με αυτή την τεχνική εκπέπονται σήματα σε μια ευρεία ζώνη συχνοτήτων αποφεύγοντας τα προβλήματα της στενής ζώνης. Με έναν ειδικό κώδικα διαχέεται το σήμα στον αέρα και ο δέκτης χρησιμοποιεί τον ίδιο κώδικα για να το ανακτήσει. Τυπική ταχύτητα εδώ είναι τα 2-3 Mbps.
Η διασπορά φάσματος είναι η μέθοδος που χρησιμοποιείται για τη μετάδοση δεδομένων σε περισσότερες από μία συχνότητες. Μετά την επιτυχημένη εφαρμογή της, επί δεκαετίες, στις στρατηγικές επικοινωνίες της εποχής του Ψυχρού Πολέμου, "ξέπεσε" τώρα να χρησιμοποιείται στα ασύρματα τοπικα δίκτυα. Υπάρχουν δύο διαφορετικοί τύποι τεχνολογιών διασποράς φάσματος. Με αυτόν τον τύπο διαμόρφωσης, το σήμα είναι καλύτερα θωρακισμένο από το θόρυβο και τις παρεμβολές και επιτρέπει να μοιράζονται τις συχνότητες λειτουργίας της περιοχής 2,4GHz πολλοί χρήστες, με όσο το δυνατόν μικρότερες παρεμβολές από άλλους ή από συσκευές, όπως οι φούρνοι μικροκυμάτων που χρησιμοποιούν την ίδια συχνότητα λειτουργίας!

Η διασπορά ευθείας ακολουθίας ***(Direct Sequence Spread Spectrum, DSSS)*** και η διασπορά με αλλαγή συχνότητας ***(Frequency Hopping Spread Spectrum, FHSS)***. Η DSSS είναι μια τεχνολογία μετάδοσης φάσματος ευρείας ζώνης, η οποία χρησιμοποιεί ένα επιπλέον bit pattern για κάθε bit που μεταδίδεται. Αυτό το bit pattern, το οποίο έχει μεγαλύτερο ρυθμό (bitrate) από αυτόν των δεδομένων, καλείται chip ή chipping code. Όσο μεγαλύτερο μήκος ακολουθίας έχει το chip, τόσο μεγαλύτερη η πιθανότητα ανάκτησης των μεταδιδόμενων δεδομένων χωρίς σφάλμα. Η δυσμενής συνέπεια της χρησιμοποίησης μακρύτερων chip, είναι το ευρύτερο φάσμα που απαιτείται για τη μετάδοση. Ακόμα και αν κατά την αποστολή δεδομένων χαθούν κάποια bit, είναι δυνατόν να ανακτηθούν, χωρίς να είναι απαραίτητη η εκ νέου αποστολή τους, κάτι που θα επέφερε καθυστέρηση στη μεταφορά των δεδομένων και θα επιβάρυνε την κίνηση στο δίκτυο. Αν κάποιος δέκτης λάβει τα

σήματα χωρίς να είναι σε θέση να τα αποκωδικοποιήσει, θα τα "ερμηνεύσει" ως θόρυβο και θα τα αγνοήσει. Η FHSS χρησιμοποιεί ένα στενό φασματικά φέρον σήμα, το οποίο μεταβάλλει συνεχώς την κεντρική του συχνότητα, σύμφωνα με ένα συγκεκριμένο πρότυπο. Το σήμα εξαπλώνεται, καθώς λειτουργεί σε μια συχνότητα για σύντομη χρονική διάρκεια και έπειτα μεταπηδά σε μια άλλη. Ο αλγόριθμος για τη μεταπήδηση (hopping) της συχνότητας, είναι εκ των προτέρων γνωστός, τόσο στον πομπό όσο και στο δέκτη. Στην FHSS, το 802.11 καθορίζει 79 κανάλια και 78 διαφορετικούς τρόπους εναλλαγής των καναλιών. Εάν το σήμα ληφθεί από κάποιον μη εξουσιοδοτημένο δέκτη, ερμηνεύεται ως μικρής διάρκειας θόρυβος και αγνοείται. Το FHSS, λόγω της τεχνικής μεταπήδησης συχνότητας, έχει μεγαλύτερη ανοχή στις παρεμβολές απ' ότι το DSSS, ενώ επίσης αποφεύγει την ταυτόχρονη δέσμευση μεγάλου μέρους του φάσματος. Η μετάδοση σημάτων FHSS απαιτεί μικρότερη ισχύ από την DSSS.

2.3) ***Ορθογώνια πολυπλεξία συχνότητας (Orthogonal Frequency Division Multiplexing-OFDM)***



, με ταχύτητα μετάδοσης μέχρι 54Mbps. Η κωδικοποίηση OFDM, είναι μια μορφή διαμόρφωσης πολλών φερόντων σημάτων και διαφέρει από αυτήν της διασποράς φάσματος. Η τεχνική OFDM χωρίζει το σήμα σε πολλά μικρότερα υποσήματα, τα οποία και εκπέμπει σε διαφορετικές συχνότητες. Αυτό μειώνει τη διαφωνία (crosstalk) στις μεταδόσεις σημάτων, κάτι το οποίο καθιστά το OFDM πολύ χρήσιμο για τη μετάδοση υψίρρυθμων και ευρυζωνικών πληροφοριών. Επίσης, με τον τρόπο αυτό, η μετάδοση είναι πολύ ανθεκτική στις παρεμβολέςΗ ίδια διαμόρφωση χρησιμοποιείται στην τεχνολογία ADSL, που πετυχαίνει υψηλότατες ταχύτητες στα κοινά τηλεφωνικά δίκτυα, αλλά και στην επερχόμενη ψηφιακή τηλεόραση. Είναι μια τεχνολογία, που ενώ είχε αναλυθεί σε θεωρητικό επίπεδο εδώ και χρόνια, έκανε ξαφνικά, δυναμική εμφάνιση στη σκηνή των ψηφιακών επικοινωνιών και κατέλαβε εξ εφόδου όλες τις νέες εφαρμογές.

Η χρήση της OFDM , Orthogonal Frequency Division Multiplexing έχει σαν αποτέλεσμα την πιο αποτελεσματική χρήση του διαθέσιμου φάσματος.

2.4) Η οικογένεια του IEEE802.11

Η Στην οικογενεια του IEEE 802.11 ανοικουν τα παρακατω προτυπα:

1)**IEEE 802.11a**: Το πρότυπο αυτό υποστηρίζει μεγαλύτερους ρυθμούς μετάδοσης με διαμόρφωση OFDM απο 6 ως 54 Mbps , στην ζώνη των 5.7GHz. Η ομάδα της IEEE εγγυάται την συμβατότητα όλων τωνμερών εκτός του ραδιοφωνικού πομπού μιας συσκευής με τα άλλα πρωτόκολλα b,g.Έτσι ένας κατασκευαστής μπορεί να χρησιμοποιεί κοινό HW και διαφορετικούς εκπομπούς, για να παράγει συσκευές που θα είναι συμβατές με μια πλειάδα πρωτοκόλλων. Χρησιμοποιείται σε ασύρματα δίκτυα ATM.

2)**IEEE 802.11b**: Συνήθως το λέμε wi-fi και είναι συμβατό με το 802.11. Η μέθοδος διαμόρφωσης που χρησιμοποιήθηκε στο 802.11 ήταν το κλείδωμα μεταλλαγής φάσης ή διαμόρφωση διακριτής φάσης, phase-shift keying (psk). Η μέθοδος διαμόρφωσης που επιλέχθηκε για το 802.11b είναι γνωστή ως complementary code keying (cck) και παρέχει μεγαλύτερους ρυθμούς μετάδοσης δεδομένων.

3)**IEEE 802.11c** Λειτουργία γεφύρωσης (bridging) πλαισίων 802.11

4)**IEEE 802.11d** Επεκτάσεις στο πρότυπο ώστε να λειτουργεί σε επιπλέον ρυθμιστικά πλαίσια (άλλες ζώνες συχνοτήτων)

5)**IEEE 802.11e**: το πρώτο ασύρματο πρότυπο για οικιακό ή εταιρικό δικτυακό περιβάλλον. Παρέχει χαρακτηριστικά ποιότητας υπηρεσιών και υποστήριξη πολυμέσων στα υπάρχοντα ασύρματα πρότυπα IEEE 802.11a και IEEE 802.11b ενώ ταυτόχρονα είναι και συμβατό με αυτά. Η ποιότητα υπηρεσιών και υποστήριξη πολυμέσων είναι ένας κρίσιμος παράγοντας στα ασύρματα οικιακά δίκτυα που θέλουμε να παρέχουν φωνή, video και ήχο (video on demand, audio on demand, voice over ip, υψηλής ταχύτητας πρόσβαση στο internet). Το υποπρότυπο IEEE 802.16 e εισάγει και περιγράφει την έννοια της κινητικότητας των χρηστών από ένα base station σε άλλο. Στο υποπρότυπο αυτό ορίζεται ότι ένας κινητός χρήστης μπορεί να συνεχίσει να εξυπηρετείται από το δίκτυο ακόμα και αν κινείται με ταχύτητες οι οποίες προσεγγίζουν τα 120 Km / h . Ωστόσο η παραπάνω τιμή είναι ενδεικτική - πειραματική, καθώς μέχρι τη στιγμή αυτή δεν υπάρχει κάποιο διαθέσιμο προϊόν στην αγορά

συμβατό με το IEEE 802.16 e υποπρότυπο που να πιστοποιεί την προαναφερθείσα τιμή.

6)**IEEE 802.11f** Συνιστώμενη πρακτική για το πρωτόκολλο IAPP, Inter Access Point Protocol

7) **IEEE 802.11g**: εφαρμόζεται σε ασύρματα τοπικά δίκτυα και παρέχει ρυθμούς μετάδοσης άνω των 20mbps στη μπάντα των 2.4GHz. Αυτό είναι το πρότυπο που εγκρίθηκε πιο πρόσφατα και παρέχει ασύρματη μετάδοση σε σχετικά κοντινές αποστάσεις με ταχύτητες μέχρι και 54mbps συγκριτικά με τα 11mbps του πρότυπου 802.11b. Όπως και το 802.11b, το IEEE 802.11g λειτουργεί στη μπάντα των 2.4GHz οπότε είναι συμβατό με αυτό. Αρχικά για τον τρόπο διαμόρφωσης η εταιρία intersil πρότεινε την χρησιμοποίηση του OFDM (Orthogonal Frequency Division Multiplexing), μια μέθοδο που αναπτύχθηκε για το 802.11a. Αυτή η πρόταση βρήκε αντίπαλες πολλές εταιρίες, όπως η Texas Instruments, που πρότεινε την χρήση της δικής της τεχνολογίας PBCC (Packet Binary Convolution Coding) για το πρωτόκολλο. Τελικά η προτυποποίηση του πρωτοκόλλου 802.11g, έφερε και την λύση. Το πρωτόκολλο χρησιμοποιεί υποχρεωτικά όλους τους τρόπους κωδικοποίησης του 802.11b για εγγυημένη προς τα πίσω συμβατότητα. Επίσης υποχρεωτική είναι η υλοποίηση του OFDM σαν τρόπο κωδικοποίησης στο g πρωτόκολλο. Προαιρετικά μπορεί ο κάθε κατασκευαστής να υλοποιήσει και μια τροποποιημένη έκδοση του OFDM ή τον PBCC, αν επιθυμεί συσκευές με καλύτερες επιδόσεις.

8)**IEEE 802.11h** Εδώ γινεται προσπαθεια να εισάχθει στο 802.11a η δυνατότητα για καλύτερο
έλεγχο συγκρούσεων, καθώς και την λειτουργία Transmit Power Control(TPC) και Dynamic Frequency Selection ή DFS. Μια συσκευή θα επιλέγει αυτόματα την ελάχιστη αναγκαία ισχύ εκπομπής, πριν ξεκινήσει οποιαδήποτε ανταλλαγή δεδομένων. Επίσης θα επιλέγει αυτόματα σε ποια συχνότητα θα λειτουργήσει, αναλόγως την χρήση της κάθε συχνότητας στον περιβάλλοντα χώρο.

9)**IEEE 802.11i**: προσθέτει στο 802.11 πρότυπο ασύρματων τοπικών δικτύων, το πρωτόκολλο ασφάλειας advanced encryption standard (aes). Η ομάδα IEEE 802.11I είναι συνώνυμη της ασφάλειας. Θα προσπαθήσει να αντικαταστήσει το WEP και την υποστήριξή του σε συσκευές, αρχικά με την δημιουργία ανώτερου (;)πρωτοκόλλου ασφαλείας προς τα πίσω συμβατό με το WEP, και τελικά με την πλήρη κατάργησή του. Η αρχική προσέγγιση προσανατολίζεται στην αύξηση του μήκους κλειδιού, έτσι ώστε brute force επιθέσεις σε αυτόν να έχουν

απαγορευτικούς χρόνους επιτυχίας με την υπάρχουσα τεχνολογία. .υστυχώς και πάλι μπορούν να
χρησιμοποιηθούν σχεδιαστικές ατέλειες που θα καταστήσουν έναν τέτοιο αλγόριθμο ανασφαλή.

2.5) WAP (Wireless Application Protocol)

Γενικα:
Το Wireless Application Protocol (WAP) είναι ένα «ανοικτό» διεθνές πρότυπο για την ανάπτυξη εφαρμογών σε ασύρματο περιβάλλον, όπως για παράδειγμα η ασύρματη πρόσβαση στο Internet μέσω κινητού τηλεφώνου. Αρχικά, το WAP σχεδιάστηκε για να παρέχει υπηρεσίες ανάλογες με αυτές που προσφέρει μια εφαρμογή Web Browser, με ορισμένες απαραίτητες μετατροπές, ώστε να είναι εφικτή η εμφάνιση πληροφοριών σε ψηφιακές συσκευές με πολύ περιορισμένες δυνατότητες. Ωστόσο, τα πρώτα χρόνια μετά την υιοθέτησή του από τα δίκτυα κινητής τηλεφωνίας, το WAP σχολιάστηκε ιδιαίτερα για τους περιορισμούς τους, αλλά και για τον τρόπο με τον οποίο τα δίκτυα επέλεξαν να το προωθήσουν. Η νεότερη έκδοση του WAP (WAP 2.0) λύνει τα περισσότερα προβλήματα του παρελθόντος και παράλληλα προσφέρει πλήρη συμβατότητα με τις προδιαγραφές της XHTML, της γλώσσας που χρησιμοποιείται πλέον ευρέως για τη δημιουργία ιστοσελίδων στο Web. Είναι πολύ πιθανόν στο εγγύς μέλλον, το WAP να αντικατασταθεί ολοκληρωτικά από εφαρμογές, που επιτρέπουν στους χρήστες κινητών τηλεφώνων την πρόσβαση στο κανονικό Web Το WAP ή (Πρωτόκολλο Ασύρματων Εφαρμογών) σχεδιάστηκε αρχικά για να επιτρέψει στους χρήστες των κινητών τηλεφώνων να έχουν πρόσβαση, ανεξαρτήτως τόπου και χρόνου, σε διάφορες πληροφορίες που αντλούνται από ειδικά διαμορφωμένες «ιστοσελίδες». Πριν από το WAP η πρόσβαση σε online πληροφορίες από το κινητό τηλέφωνο μπορούσε να γίνει μόνο με την παράλληλη χρήση κάποιου ηλεκτρονικού υπολογιστή. Με το WAP όμως το «surfing» μπορεί να γίνει από την οθόνη οποιουδήποτε κινητού, ακόμη και αν η οθόνη του έχει περιορισμένες διαστάσεις. Φυσικά οι «ασύρματες ιστοσελίδες» δεν έχουν καμία ομοιότητα με τις ιστοσελίδες που οι χρήστες μπορούν να δουν μέσω του World Wide Web και των Η/Υ.

2.5.1) ΔΗΜΙΟΥΡΓΙΑ ΤΟΥ WAP

Εξαιτίας των τεχνικών τους περιορισμών και του μικρού τους μεγέθους τα περισσότερα κινητά τηλέφωνα της αγοράς τείνουν να έχουν «αδύναμους» επεξεργαστές, περιορισμένη μνήμη, μικρές και πολλές φορές μονόχρωμες οθόνες, καθώς και λίγα πλήκτρα για την εισαγωγή δεδομένων. Τα δίκτυα GSM προσέφεραν μεν τη δυνατότητα «ασύρματης» πρόσβασης, ωστόσο ο ρυθμός μεταφοράς δεδομένων (data rate) ήταν πολύ χαμηλός με αποτέλεσμα ακόμη και μια ιστοσελίδα

λίγων kilobytes να χρειάζεται αρκετή ώρα για να μεταφερθεί στον ενδιαφερόμενο. Το 1997 η αμερικανική Unwired Planet (που πλέον έχει μετονομαστεί σε Phone.com), καθώς και οι Ericsson, Motorola και Nokia, συνεργάστηκαν για την ανάπτυξη ενός προτύπου που θα έδινε στο Internet την ευκαιρία να διεισδύσει στο χώρο των κινητών τηλεφώνων και των υπολοίπων φορητών ψηφιακών συσκευών και παράλληλα να ξεπεραστούν τα όποια προβλήματα και οι περιορισμοί.

Το WAP προσδιόρισε ένα περιβάλλον εφαρμογών και πρωτοκόλλων δικτύου, το οποίο βασίζεται εν μέρει στην επέκταση των τεχνολογιών του Διαδικτύου, ενώ παράλληλα διασφαλίζει τη διαλειτουργικότητα, ώστε οι «κινητές συσκευές» ανεξαρτήτως κατασκευαστή και προδιαγραφών, να έχουν τη δυνατότητα πρόσβασης σε αυτό, την αποτελεσματικότητα, την αξιοπιστία και την ασφάλεια.

2.5.2) ΣΥΣΚΕΥΕΣ ΠΟΥ ΕΝΣΩΜΑΤΩΝΟΥΝ ΤΟ WAP

Σχεδόν όλα τα κινητά τηλέφωνα της αγοράς ενσωματώνουν πλέον το WAP, επιτρέποντας την ασύρματη ανάκτηση πληροφοριών και πολλές φορές λογοτύπων, μελωδιών κ.α. Μέρος των πρωτοκόλλων του WAP άλλωστε χρησιμοποιείται για τη μεταφορά των multimedia στοιχείων των MMS. Σύμφωνα με το WAP Forum, το WAP έχει χρησιμοποιηθεί επίσης σε PDAs, pagers, ασύρματα τηλέφωνα κ.α.WAP;

2.5.3) ΛΕΙΤΟΥΡΓΙΑ ΤΟΥ WAP

Το περιβάλλον του WAP είναι παρόμοιο με αυτό του World Wide Web. Το γεγονός αυτό προσφέρει αρκετά πλεονεκτήματα στους developers εφαρμογών WAP, αφού χρησιμοποιείται ένα σχετικά γνώριμο «προγραμματιστικό μοντέλο», δοκιμασμένη αρχιτεκτονική, καθώς και η δυνατότητα επέκτασης και εκμετάλλευσης των υπαρχόντων εργαλείων, όπως οι Web Servers ή γλώσσα XHTML/XML κ.α. Όπου ήταν δυνατό το WAP εκμεταλλεύεται τα ήδη γνώριμα πρότυπα.

Ο τύπος των δεδομένων και των εφαρμογών του WAP προσδιορίζεται μέσα σε ένα σύνολο γνωστών μορφότυπων που βασίζεται στα γνωστά πρότυπα του παγκόσμιου ιστού. Τα δεδομένα μεταφέρονται με τη χρήση ενός γνωστού συνόλου επικοινωνιακών πρωτοκόλλων που βασίζονται στα WWW πρωτόκολλα. Ο micro-browser στο κινητό τηλέφωνο συντονίζει τη διεπαφή συσκευής-χρήστη και είναι ανάλογος των γνωστών browsers για το World Wide Web.

Το WAP καθορίζει ένα σύνολο μηχανισμών, βάση των οποίων πραγματοποιείται η επικοινωνία μεταξύ των κινητών τηλεφώνων και των εξυπηρετητών (servers) του δικτύου. Μέσα σ’ αυτούς περιλαμβάνονται και οι παρακάτω:

- Βασικό μοντέλο διευθυνσιοδότησης: Χρησιμοποιείται ο μηχανισμός των URLs για να αναγνωριστεί το WAP περιεχόμενο στους servers.

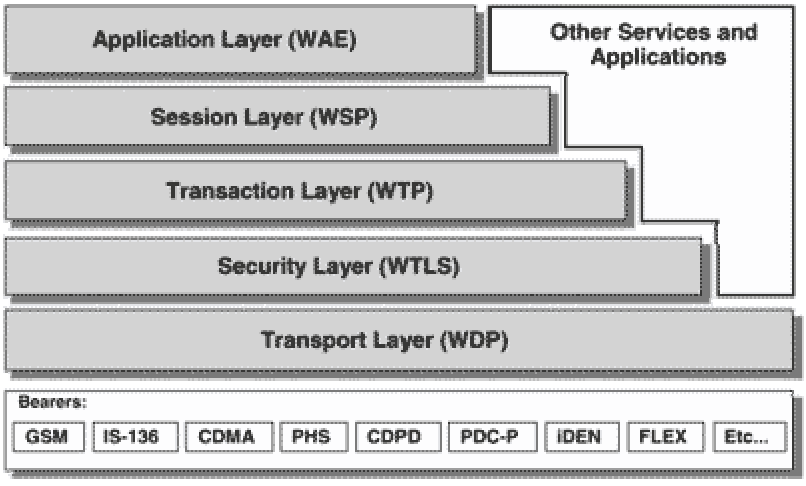
- Τύποι δεδομένων: Ο τύπος όλων των δεδομένων που μεταδίδονται μέσω του WAP είναι συμβατός με τους αντίστοιχους τύπους του παγκόσμιου ιστού.
- Βασικά μορφότυπα: Τα μορφότυπα του WAP είναι βασισμένα στην τεχνολογία του παγκόσμιου ιστού και περιλαμβάνουν σήμανση οθόνης, πληροφορίες ημερολογίου, αντικείμενα καρτών ηλεκτρονικού εμπορίου (electronic business card objects), εικόνες και γλώσσα script.
- Βασικά επικοινωνιακά πρωτόκολλα: Με τα επικοινωνιακά πρωτόκολλα του WAP επιτυγχάνεται η μεταφορά των αιτήσεων του browser της κινητής συσκευής στον web server.

Όλα τα παραπάνω έχουν βελτιστοποιηθεί για χρήση σε ασύρματες συσκευές χειρός, όπως τα κινητά τηλέφωνα.

Στο WAP χρησιμοποιείται η τεχνολογία «proxy» για να διασφαλιστεί η σωστή μεταφορά των πληροφοριών από το Web Server προς τη ψηφιακή συσκευή και αντίστροφα. Το WAP Proxy εμπεριέχει το δρομολογητή πρωτοκόλλου, ο οποίος μεταφράζει τις αιτήσεις που δίνονται από το WAP (WSP, WTP, WTLS και WDP) σε αιτήσεις πρωτοκόλλου WWW (HTTP και TCP/IP). Παράλληλα διαθέτει κωδικοποιητές και αποκωδικοποιητές περιεχομένου, που μετατρέπουν τις πληροφορίες με τέτοιον τρόπο, ώστε να μπορούν να απεικονιστούν σωστά στην οθόνη της ψηφιακής συσκευής.

2.5.4) Η ΑΡΧΙΤΕΚΤΟΝΙΚΗ WAP

Η αρχιτεκτονική του WAP παρέχει ένα βαθμωτό επεκτάσιμο περιβάλλον για την ανάπτυξη εφαρμογών που υλοποιούνται σε ψηφιακές συσκευές, όπως τα κινητά τηλέφωνα.



Πρώτο στη σειρά είναι το στρώμα του περιβάλλοντος εφαρμογής

(WAE), το οποίο συνδυάζει τις τεχνολογίες της κινητής τηλεφωνίας και του παγκοσμίου ιστού και περιλαμβάνει το micro-browser της συσκευής. Ακολουθεί το στρώμα του πρωτοκόλλου συνόδου (WSP), το στρώμα Transaction (WTP), το στρώμα ασφαλείας (WTLS), καθώς και το στρώμα μεταφοράς (WDP).

2.5.5) Τι είναι το WAP Push;

Το WAP Push «παρέχεται» από την έκδοση 1.2 του Πρωτοκόλλου και σχεδιάστηκε ώστε να επιτρέπει την «προώθηση» περιεχομένου από τους παροχείς υπηρεσιών απευθείας στις συσκευές των χρηστών. Ουσιαστικά, πρόκειται για ένα κωδικοποιημένο μήνυμα το οποίο περιλαμβάνει μια διεύθυνση (URL). Το κινητό, εφόσον έχει την απαραίτητη έγκριση από το χρήστη, αναλαμβάνει να συνδεθεί με τη διεύθυνση και να ανακτήσει το περιεχόμενο. Αυτό μπορεί να είναι κάποια πληροφορία, λογότυπο, μελωδία κ.ο.κ. Με τη χρήση του WAP Push οι πάροχοι περιεχομένου μπορούν πολύ πιο εύκολα να διαθέσουν υπηρεσίες προστιθέμενης αξίας στους πελάτες τους.

2.6) Τεχνολογιες Ασυρματων Δικτυων (***Κατηγοριες***)

2.6.1)WLAN(Wi-Fi)

Το Wi-Fi προέρχεται από τα αρχικά των “wireless fidelity” , «ψηφιακή πιστότητα» στα Ελληνικά και έχει επικρατήσει σαν όρος για το υψηλής συχνότητας ασύρματο τοπικό δίκτυο (WLAN). Βασικά αποτελεί ένα ασύρματο τρόπο διασύνδεσης μεταξύ ηλεκτρονικών συσκευών – το κομπιούτερ ή το στερεοφωνικό σας για παράδειγμα- ενώ δίνει την δυνατότητα σύνδεσης και με το Internet. Η μόνη προϋπόθεση είναι οι συσκευές που συνδέονται να είναι Wi-Fi ready δηλ. να έχουν δυνατότητα από τον κατασκευαστή Wi-Fi και επίσης να βρίσκεστε στην περιοχή κάλυψης του σήματος.
Είτε στο σπίτι σας είτε στο εργασιακό σας περιβάλλον στην ασύρματη εποχή, εάν έχετε έναν ή περισσότερους υπολογιστές, υπάρχουν πολλά καλά επιχειρήματα για να έχετε κάποιο ασύρματο δίκτυο:

1. Το Wi-Fi δεν είναι ακριβό: Εξοικονόμηση χρημάτων από την απαιτούμενη καλωδίωση στο σπίτι ή στο γραφείο, λιγότερα χρήματα σε συνδέσεις Internet, μοίρασμα της χρήσης περιφερειακών συσκευών όπως εκτυπωτές και σαρωτές και χρήση του υπολογιστή για άλλες εφαρμογές όπως διασκέδαση στο σπίτι ή κέντρο εφαρμογών πολυμέσων (home entertainment, multimedia centre).
2. Το Wi-Fi είναι ευέλικτο: Τώρα μπορείτε αν είναι καλή ημέρα και θέλετε να δουλέψετε στον μπαλκόνι ή στον κήπο με το laptop να το κάνετε. Χάρις το Wi-Fi δεν είστε πια καθηλωμένος με το καλώδιο σε ένα σημείο που σημαίνει ότι μπορείτε να δουλέψετε εκεί που θέλετε όταν θέλετε.
3. Το Wi-Fi είναι εύκολο στην εγκατάσταση: Στόχος αυτού του κειμένου είναι να δώσει την πληροφορία για το πώς θα εγκαταστήσετε το δικό σας Wi-Fi.

Το Wi-Fi διεύκολινει τα πραγματα επιτρέποντας μας να είμαστε online σχεδόν από παντού είτε στο σπίτι είτε έξω από αυτό. Τρία πράγματα θα πρέπει να θυμάστε για να αποκομίσετε τα περισσότερα οφέλη από το Wi-Fi

- Ευρυζωνική σύνδεση : Το Wi-Fi είναι ο καλύτερος τρόπος να μοιραστείτε μια γρήγορη μόνιμη σύνδεση.

- Wi-Fi broadband router: Μπορείτε να μοιράσετε την σύνδεση και τα περιφερειακά σας χωρίς να είναι απαραίτητο να έχετε υπολογιστή συνεχώς αναμμένο με αυτές τις συσκευές.
- Wi-Fi adapter δικτύου για κάθε PC: Αν το laptop σας έχει ενσωματωμένη τη δυνατότητα Wi-Fi όπως είναι σε αυτά με την τεχνολογία Intel Centrino τότε το έχετε ήδη.

Η πρόσβαση στο Wi-Fi είναι σίγουρη όταν έχετε τα παρακάτω:

- Σωστά εγκατεστημένο και ρυθμισμένο Wi-Fi adapter δικτύου στο laptop. Βεβαιωθείτε ότι πληρή ένα από τα στάνταρς.
- Καλά σχεδιασμένο ταξίδι. Ελέγξτε από πριν τις τοποθεσίες των hotspots όταν πρόκειται να ταξιδέψετε. Χρησιμοποιείστε τα hotspot locators.
- Πλήρως φορτισμένες μπαταρίες του laptop. Αν δεν είστε κοντά σε πρίζα ρεύματος θα αναγκαστείτε να χρησιμοποιείτε το laptop με την μπαταρία του.

Σχεδιάζοντας το δικό μας Wi-Fi

Είτε για το σπίτι είτε για το γραφείο η εγκατάσταση απαιτεί σωστό σχεδιασμό προκειμένου να αποφευχθούν περιττές σπατάλες.
Ο σχεδιασμός θα υποδείξει αν χρειάζεται εγκατάσταση περισσότερων του ενός access points και που θα πρέπει να μπουν. Το πλεονέκτημα είναι ότι θα πρέπει να ξεχάσετε το κόστος, την ενόχληση και τη σπατάλη του να καλωδιώσετε όλο το χώρο. Το Wi-Fi μπορεί να είναι έτοιμο σε πολύ λίγο χρόνο και όπως γνωρίζουμε ο χρόνος είναι χρήμα. Παρόλα αυτά πριν κάνετε οτιδήποτε σταθείτε για λίγο και σκεφτείτε πως θέλετε να χρησιμοποιήσετε το Wi-Fi.

- Επιλογή standard: Για να εξασφαλίσουμε τη σωστή λειτουργία του, χρησιμοποιουμε πάντα πιστοποιημένα προϊόντα Wi-Fi . Η επιλογή είναι μεταξύ 802.11b με 11 Mbps και 802.11b ή g με 11Mbps ή 54Mbps.
- Αγορά δρομολογητή (router): Ο απλός Wi-Fi router καλύπτει μια ελεύθερη απόσταση περίπου 90 μέτρα – απόσταση ικανοποιητική για την κάλυψη ενός μέσου σπιτιού. Αν ο χώρος είναι πολύ μεγάλος

τότε ίσως χρειαστούν παραπάνω από ένας. Επίσης παίζει ρόλο και η κατασκευή του χώρου (μεταλλικά χωρίσματα, πολύ χοντροί τοίχοι) δεδομένου ότι το Wi-Fi βασίζεται σε ραδιοσυχνότητες. Για να ξεπεραστεί ένα τέτοιο πρόβλημα θα χρειαστούν περισσότερα σημεία πρόσβασης (access points) προς ενίσχυση του σήματος. Με το πακέτο "ADSL in-a-box Plus", ο Router περιλαμβάνεται οπότε δεν χρειάζεται να αγοράσετε.

- Πρεπει οι συσκευές που θέλουμε να συνδέσουμε να είναι Wi-Fi ready: Η διασύνδεση μεταξύ του PC/Wirless router και των διάφορων ηλεκτρονικών συσκευών (CE) ίσως απαιτεί την αγορά υλικών, λογισμικού ή υπηρεσιών. Μερικές συσκευές (CE) μπορεί να μην συνεργάζονται με το PC ή το laptop. πριν αγοράσετε μια συσκευή βεβαιωθείτε για την συμβατότητα τους.
- Επιλογή του κατάλληλου χώρου: Τοποθετουμε τον router κοντά στην τηλεφωνική πρίζα έτσι ώστε να μπορεί να συνδεθεί στο ADSL. Αυτό πρέπει να βρίσκετε κάπου στο κέντρο του χώρου των υπολογιστών που χρησιμοποιούνται. Αποφευγουμε να βάζουμε τον router δίπλα από φούρνο μικροκυμάτων ή ασύρματο τηλέφωνο γιατί δεδομένου ότι εκπέμπουν στην ίδια συχνότητα (2.4GHz), μπορεί σε κάποιες περιπτώσεις να προκαλέσουν παρεμβολές.

Εγκατάσταση. Ο εύκολος τρόπος

Αφού έχουμε βρει την κατάλληλη θέση του router θα πρέπει να τον συνδέσουμε. Οι προρυθμίσεις του θα πρέπει να μας αφήσουν να συνδέσουμε σε αυτόν άμεσα τους υπολογιστές. Στη συνέχεια τον ρυθμίζουμε να συνδεθεί στον παροχέα Internet. Είναι ένα κλασικό παράδειγμα plug and play. Επίσης εύκολο είναι να προστεθούν υπολογιστές στο Wi-Fi. Δεν χρειάζεται να πάρετε καλώδια ή να βρείτε πόρτες Ethernet. Ενεργοποιήστε το WiFi στο PC σας και είστε στο ασύρματο δίκτυο.

Για να φτιάξετε το δικό σας ασύρματο δίκτυο το πιθανότερο είναι ότι πρέπει να αγοράσετε εξοπλισμό Wi-Fi για τους υπολογιστές που θέλετε να βγάλετε στον αέρα. Υπάρχει αρκετά μεγάλη ποικιλία τέτοιου εξοπλισμού. Μερικά από τα μεγάλα ονόματα του χώρου είναι και οι 3Com, Intel, Linksys, Netgear.

Αναλυτικότερα :

Wi-Fi Network adapter

Το πρώτο που χρειάζεστε είναι ένας Wi-Fi προσαρμογέας δικτύου. Είναι αυτός που επιτρέπει στον υπολογιστή σας να έχει πρόσβαση και να επικοινωνεί με το ασύρματο δίκτυο. Στην αγορά υπάρχουν διάφορα είδη Wi-Fi adapters όπως έναν απλό που συνδέεται σε υποδοχή του υπολογιστή ή κάποιος που είναι εσωτερικός του υπολογιστή.
Σε υπολογιστή γραφείου για παράδειγμα μπορείτε να προσαρμόσετε ή USB ή PCI Wi-Fi adapter.

- **USB (Universal Serial Bus)**

Οι περισσότεροι σύγχρονοι υπολογιστές έχουν αρκετές υποδοχές USB. Επιλέγουμε μια τέτοια υποδοχή του PC και συνδέουμε τον USB Wi-Fi adapter.

- **PCI (Peripheral Component Interconnect)**

Αυτού του είδους οι adaptors συνδέονται στην υποδοχή PCI της μητρικής του υπολογιστή. Προσαρμόζονται εσωτερικά στον υπολογιστή. Όταν αγοράζετε Wi-Fi adapter θα πρέπει να προσέξετε να υποστηρίζει τα διάφορα Wi-Fi standards. Οι περισσότεροι σήμερα υποστηρίζουν τουλάχιστον τα δύο πιο δημοφιλή. Με αυτόν τον τρόπο θα μπορείτε να τρέξετε σε υπάρχοντα δίκτυα ή να προσαρμόσετε αργότερα έναν καινούργιο router.

Ρυθμίστε το laptop :

Αν πήρατε πρόσφατα ένα laptop είναι σχεδόν σίγουρο ότι έχει ενσωματωμένη την ασύρματη πρόσβαση- συνήθως υπάρχει λογότυπο “Wi-Fi ready” σε αυτοκόλλητο. Τα laptops που έχουν το λογότυπο Intel Centrino για παράδειγμα έχουν ενσωματωμένη την ασύρματη δυνατότητα. Σε αυτές τις περιπτώσεις το laptop είναι έτοιμο και δεν χρειάζεται να αγοράσετε κάτι άλλο.
Αν το laptop δεν έχει αυτή τη δυνατότητα τοτε χρειάζετε ένας PC Card Wi-Fi adapter που απλά το βάζετε στην αντίστοιχη υποδοχή του. Μπορείτε επίσης να χρησιμοποιήσετε ένα USB Wi-Fi adapter που μπαίνει σε κάποια ελεύθερη υποδοχή USB. Όταν φυλάτε το laptop στη τσάντα του θα πρέπει να βγάζετε την κάρτα. Με κατάλληλη έρευνα αγοράς θα βρείτε αυτήν την κάρτα που σας ταιριάζει και οικονομικά.

Χρήση Wi-Fi router

Από τη στιγμή που ο υπολογιστής σας είναι Wi-Fi ready μπορεί να λειτουργεί είτε σαν Wi-Fi router είτε σαν σημείο πρόσβασης (Wireless Access Point) μοιράζοντας για παράδειγμα την σύνδεση του στο Internet. Κάτω από συγκεκριμένες συνθήκες αυτό μπορεί να σας εξοικονομήσει χρήματα αλλά σημαίνει ότι θα πρέπει να έχετε ανοιχτό τον υπολογιστή συνεχώς που πολλές φορές δεν είναι και πολύ καλό. Για το λόγο αυτό συνήθως είναι καλύτερο να αγοράσετε ξεχωριστά έναν Wi-Fi router. Είναι μικρές συσκευές (στο μέγεθος βιβλίου) που καθορίζουν σε ένα δίκτυο την κίνηση προς τη σωστή κατεύθυνση. Μπορεί να λειτουργεί και σαν σημείο πρόσβασης (Wireless Access Point) ενώνοντας ένα ενσύρματο δίκτυο σε ένα ασύρματο. Επίσης λειτουργεί σαν πύλη προς την ευρυζωνική σύνδεση στο Internet, επιτρέποντας να την μοιράσετε ασύρματα σε όλους τους υπολογιστές σας. Ενώστε τον router στην ADSL σύνδεση και μετά όλα τα PCs συνδέονται ασύρματα στον router φροντίζοντας για τη διακίνηση της πληροφορίας στη σωστή κατεύθυνση. Οι σωστοί routers περιλαμβάνουν firewalls για την προστασία του δικτύου από εξωτερικούς εισβολείς.

Το νέο πακέτο "ADSL in-a-box Plus", περιλαμβάνει ADSL Router της Linksys, με Wi-Fi, firewall και 4πορτο ethernet switch, διατίθεται σε δύο εκδόσεις, για τηλεφωνική γραμμή PSTN ή ISDN .

Roaming

Εάν έχουμε Wi-Fi στο σπίτι ή στο γραφείο και μπαίνουμε στο Internet με το laptop από εκεί, στην πραγματικότητα μπορουμε να κάνουμε roaming από παντού.

Όταν βρεθουμε με το laptop μας στην εμβέλεια κάποιου άλλου Hotspot και συνδεθουμε σε αυτό όπως και στο δικό μας τότε κάνουμε roaming. Αυτό είναι σίγουρα μια από τις πιο ελκυστικές πτυχές του Wi-Fi αν και το ασύρματο δίκτυο είναι ελκυστικό από μόνο του.

Σε αυτό το κείμενο χρησιμοποιούμε τον όρο Hotspot για δημόσια προσβάσιμους χώρους όπως καφετέριες, αεροδρόμια ή ακόμη και πλατείες που έχουν ασύρματη ευρυζωνική πρόσβαση αν και τεχνικά ένα hotspot υπάρχει σε κάθε μέρος με δυνατότητα Wi-Fi . Αυτού του είδους το roaming –το να ειμαστε οπουδήποτε και να μπορουμε να συνεχίζουμε τις online συνήθειες μας- είναι ιδανικό για να ελέγχουμε τα email μας, να πλοηγουμαστε στο Web ή να συνδεθουμε στο δίκτυο του

γραφείου για να αποκτήσουμε πρόσβαση σε ένα αρχείο που χρειάζομαστε σε μια off-site συνάντηση.
Με το Wi-Fi enabled laptop ή PDA μας αποκτάμε γρήγορη σύνδεση στο Internet χωρίς να χρειάζομαστε τηλεφωνικές πρίζες ή απελπιστικά αργές συνδέσεις, αποκτώντας την ίδια άμεση σύνδεση είτε στο γραφείο μας είτε στον άνετο καναπέ της καφετέριας.

Επέκταση της κάλυψης

Τα Wi-Fi access points συνήθως έχουν μια κάλυψη γύρω στα 90 μέτρα. Αυτή η κάλυψη περιορίζεται εάν υπάρχουν εμπόδια στη μετάδοση του σήματος όπως τοίχοι ή συσκευές που επηρεάζουν την μετάδοση γιατί λειτουργούν στην ίδια συχνότητα με το Wi-Fi όπως φούρνοι μικροκυμάτων ή ασύρματα τηλέφωνα. Για να ενισχυθεί το σήμα ή να επεκταθεί η κάλυψη του Wi-Fi πολλαπλασιάζουμε τα access points που μπορούν να συνδεθούν στο ίδιο ασύρματο δίκτυο για να έχουμε ευρύ και αδιάκοπο σήμα.

Wi Fi Hotspot

Το Wi-Fi hotspot δεν έχει καμία σχέση με σημείο θέρμανσης – είναι ένας δημόσιος χώρος που προσφέρει υψηλής ταχύτητας ασύρματη πρόσβαση στο Internet. Πού μπορουμε λοιπόν να βρουμε αυτές τις οάσεις της πρόσβασης στο Internet; Τα περισσότερα hotspots βρίσκονται σε χώρους συγκέντρωσης ανθρώπων όπου μπορούν να καθίσουν, όπως σε:

- Καφετέριες
- Fast food – εστιατόρια
- Pubs
- Χώρους αναχωρήσεων αεροδρομίων – σταθμών τρένων
- Ξενοδοχεία
- Σταθμούς εθνικών δρόμων
- Μέσα μεταφοράς (πλοία, αεροπλάνα κλπ)

Ένα δημόσια προσβάσιμο hotspot συνήθως έχει εύρος Wi-Fi μεγαλύτερο από ένα οικιακό. Συνήθως αυτό οφείλεται στο ότι υπάρχουν λιγότερα εμπόδια (τοίχοι κλπ) και στο ότι υπάρχουν περισσότερα access points. Πάντα όμως αν θέλουμε να έχουμε πολύ δυνατό σήμα θα πρέπει να βρίσκομαστε κοντά στο access point. Αυτό πρακτικά σημαίνει ότι πρέπει να βρίσκομαστε μέσα στην καφετέρια ή το

εστιατόριο απολαμβάνοντας τον καφέ ή το γεύμα μας και να πάρουμε τα επείγοντα emails μας.
Η πρόσβαση στα περισσότερα hotspots είναι επί πληρωμή. Ελεύθερη πρόσβαση μπορεί να παρέχεται από κλειστές μόνο ομάδες ή κοινότητες.
Στο μέλλον (όχι μακρινό) θα υπάρχει κάλυψη Wi-Fi στα περισσότερα δημόσια μέρη. Έτσι θα σταματήσει ο λήθαργος της φορητότητας και θα επεκταθεί παντού. Στον κόσμο υπάρχουν χιλιάδες hotspots.

Εκτός από να ψάχνετε για τα σήματα που προσδιορίζουν τα hotspots στους δημόσιους χώρους μπορείτε να τα αναζητήσετε στο Intel Hotspot Finder http://intel.jiwire.com/ ή στο Wi-Fi ZONE™ http://www.wi-fizone.org/zoneFinder.asp ή το http://www.forthnet.gr/hotspotlocator της FORTHnet.

Τρία πράγματα χρειάζομαστε για να αποκτήσουμε πρόσβαση σε ένα hotspot.

- Ένα laptop ή PDA με δυνατότητα Wi-Fi . Το laptop σας ίσως ήδη έχει αυτήν τη δυνατότητα. Αν όχι είναι πολύ απλό το να του βάλουμε μια κάρτα (Wi-Fi adapter). Έχουμε στην αρχή του κειμένου εξηγήσει πως γίνετε αυτό.
- Έναν Web Browser. κανένα πρόσθετο λογισμικό δεν χρειάζεται.
- Έναν τρόπο πληρωμής για τη χρήση του Wi-Fi hotspot . Επειδή σχεδόν όλα τα hotspots λειτουργούν εμπορικά, πληρώνουμε για τη χρήση τους. Όπως στα κινητά τηλέφωνα υπάρχει πληρωμή με προπληρωμένο χρόνο ή συνδρομες. Μπορουμε είτε να αγοράσουμε μια προπληρωμένη κάρτα στο hotspot και να ξύσουμε τον κωδικό για να αποκτήσουμε πρόσβαση είτε αν είμαστε τακτικός χρήστης να υπογράψουμε συνδρομή μεγαλύτερου χρονικού διαστήματος χωρίς άλλες ενοχλήσεις. Αυτό μπορεί να αποδειχθεί οικονομικότερο ανάλογα με τη χρήση. Επίσης υπάρχει η επιλογή αποστολής SMS από το κινητό μας όπου στέλνοντας τη συνθηματική λέξη λαμβάνουμε απάντηση με τον κωδικό πρόσβασης.

Δημιουργώντας τη σύνδεση Wi Fi

Η σύνδεση στο Wi-Fi έχει δύο μέρη:

- Το Wi-Fi hardware και το hotspot πρέπει να αναγνωρίσουν το ένα το άλλο έτσι ώστε το laptop να «μιλά» στο hotspot. Αυτό γίνεται αυτόματα στο Wi-Fi hardware όταν ανοίξει. Αν έχουμε Windows XP αυτόματα βρίσκει και προσπαθεί να συνδεθεί στο Wi-Fi Hotspot. Τα περισσότερα laptops δείχνουν ένα σήμα στην οθόνη ή κάπου αλλού στο σώμα τους όταν βρίσκονται στην εμβέλεια ενός Wi-Fi Hotspot. Αν έχουμε παλιότερη έκδοση των Windows μάλλον θα πρέπει να αλλάξουμε το όνομα του δικτύου (ή SSID) σε κάτι όπως για παράδειγμα FORTHnet στην περίπτωση που βρίσκομαστε σε FORTHnet HotSpot. Συνήθως υπάρχουν οδηγίες χρήσης σε φυλλάδια στα hotspots.
- Θα πρέπει να δώσουμε τα στοιχεία μας (username, password) και να ρυθμίσουμε το laptop σύμφωνα με τις οδηγίες του provider.Τις περισσότερες φορές απλά ανοίγουμε τον browser και μπαίνουμε αυτόματα στην σελίδα υποδοχής του παροχέα για να συμπληρώσουμε το username και το password. Μπορεί διαφορετικά hotspots να έχουν διαφορετικούς παρόχους αλλά κάθε ένα θα πρέπει να έχει σαφής και κατανοητές οδηγίες για τη σύνδεση. Το προσωπικό σε αυτά τα μέρη συνήθως δεν είναι τεχνικοί αλλά έχουν γραπτές οδηγίες ή τηλεφωνική τεχνική υποστήριξη.

Μια ευρυζωνική σύνδεση σε Wi-Fi hotspot μας επιτρέπει να κάνουμε αυτά που συνηθίζουμε στο γραφείο ή το σπίτι. Μπορουμε να έχουμε πρόσβαση σε οποιαδήποτε πηγή στο Internet ως επίσης σε οποιοδήποτε εταιρικό δίκτυο που επιτρέπει πρόσβαση στο Internet. Έτσι μπορουμε να σερφάρουμε στο Web, να ακούσουμε έναν ραδιοφωνικό σταθμό από το Internet , να «κατεβάσουμε» αρχεία από το γραφείο, να παίξουμε online games, να ανταλλάξουμε άμεσα μηνύματα (instant messages –IM) με φίλους και συνεργάτες.
Αν συνδεθουμε στο εταιρικό μας Internet μπορουμε επίσης να κατεβάσουμε email, σημαντικά αρχεία, τους τελευταίους τιμοκαταλόγους και παρουσιάσεις- με άλλα λόγια όλα τα πράγματα που θα κάναμε αν ήμασταν στο γραφείο.
Μπορεί να μπορουμε να λαμβάνουμε email αλλά δεν θα μπορουμε να στέλνουμε με το email πρόγραμμα μας- οι περισσότεροι ISPs δεν αποδέχονται mail που στέλνονται από λογαριασμούς άλλων ISPs.

Παρόλα αυτά οι περισσότεροι προσφέρουν τη δυνατότητα Web mail ώστε να έχεμε πρόσβαση στον email λογαριασμό μας από μακριά.

ΕΦΑΡΜΟΓΕΣ ΤΟΥ Wi Fi

Το Wi-Fi δεν είναι απλά η διασύνδεση υπολογιστών και Internet. Είναι βεβαία από τα πιο σημαντικά θέματα στην σημερινή εποχή της δικτύωσης αλλά αυτό είναι μόνο το ένα μέρος του. Από τα πιο βασικά πλεονεκτήματα της ασύρματης δικτύωσης είναι η κοινή χρήση.

- Κοινη χρηση Δίσκων, εκτυπωτών, σαρωτών και Internet υψηλής ταχύτητας.

- Παιγνίδια με πολλούς παίχτες μεταξύ υπολογιστών: Αν είστε οπαδός των video games (multi-player card games ή role-playing games) παίζοντας μέσω ασύρματου δικτύου ή ακόμη και στο Internet είναι σίγουρο ότι θα «κολλήσετε».
- Ακρόαση τραγουδιών σε οποιοδήποτε σημείο στο χώρο μας: Φορτώνουμε τα CD μας στον υπολογιστή μας και ακούμε ασύρματα στο στερεοφωνικό μας ή στο MP3 player.
- Δημιουργία σύνδεσης για κάποια συγκεκριμένη περίοδο όπως πχ σε εκθέσεις: Το Wi-Fi απλουστεύει τη δημιουργία τέτοιων δικτύων για χρήση από ομάδες εργασίας σε συγκεκριμένο project που βρίσκονται σε απομακρυσμένο σημείο.
- Περιαγωγή όπου τη θέλετε: Μπείνουμε στο δίκτυο με τον υπολογιστή μας από δημόσια Wi-Fi hotspots οπουδήποτε στον κόσμο χωρίς ούτε ένα καλώδιο.
- Επίβλεψη χώρων: Νέες ασύρματες κάμερες στο Wi-Fi μπορούν να μεταφέρουν ασύρματα εικόνα ιδιωτικά ή δημόσια στο Internet. Η παρακολούθηση χώρων ή η επίβλεψη παιδιών μπορεί να γίνει εύκολα καλώντας την ασύρματα δικτυωμένη κάμερα.
- Τηλεφωνία: Με κάποιες ασύρματες τηλεφωνικές συσκευές μπορουμε να απελευθερωθουμε από τη δέσμευση των τηλεφωνικών καλωδίων και να μπεουμε στην ψηφιακή εποχή εξοικονομώντας χρήματα χρησιμοποιώντας φθηνότερες τηλεφωνικές υπηρεσίες βασισμένες στο Internet.

- Κοινή χρήση σύνδεσης Internet:Ένας από τους πιο σημαντικούς λόγους ενδιαφέροντος για Wi-Fi για πάρα πολλούς είναι η επιθυμία κοινής χρήσης μιας υψηλής ταχύτητας (ευρυζωνικής) σύνδεσης με το

Internet. Μοιράζοντας μια ευρυζωνική σύνδεση μέσω του Wi-Fi σε όλους τους υπολογιστές μας, σε σχέση με μια απλή dial up, πετυχαινουμε πολύ καλύτερες ταχύτητες με μόνο μια συνδρομή.

Το Wi-Fi βοηθάει να διαμοιράσετουν πληροφορίες από το σπίτι ή το γραφείο.

Επικοινωνία με περιφερειακά

Η κοινή χρήση εκτυπωτών ήταν πάντοτε ένα πολύ καλό πλεονέκτημα της διασύνδεσης υπολογιστών. Για παράδειγμα, μεγάλες εταιρίες επενδύουν σε υψηλής ταχύτητας και δυνατότητας εκτυπωτών που τον μοιράζονται πολλοί υπάλληλοι. Κάποιες φορές σε ένα ολόκληρα τμήματα χρησιμοποιούν από κοινού εκτυπωτές, φωτοαντιγραφικά και μηχανές fax.

Όπως ακριβώς σε ένα κλασικό δίκτυο υπολογιστών με το Wi-Fi όλοι οι υπολογιστές μπορούν να επικοινωνούν με τα περιφερειακά (εκτυπωτές κλπ) αλλά με το επιπλέον πλεονέκτημα ότι δεν απαιτούνται καλωδιώσεις.

Μεταφορά αρχείων

Όλοι γνωρίζουμε τι είναι τα αρχεία των υπολογιστών. Αν για παράδειγμα χρησιμοποιείτε ένα πρόγραμμα επεξεργασίας κειμένου όπως το Microsoft Word για να γράψετε ένα κείμενο, μπορείτε να το αποθηκεύσετε ως ηλεκτρονικό αρχείο.

Ένα δίκτυο υπολογιστών, σας επιτρέπει να μοιραστείτε αυτά τα ηλεκτρονικά αρχεία μεταξύ δύο ή περισσοτέρων υπολογιστών. Αλλά αυτό ακριβώς είναι το λεπτό σημείο. Τι εννοούμε υπολογιστές. Για παράδειγμα τα σημερινά αυτοκίνητα έχουν τεράστιες υπολογιστικές και δικτυακές δυνατότητες. Το στερεοφωνικό σήμερα εξελίσσεται συνεχώς ώστε να λειτουργεί σαν υπολογιστής με αρχεία και πληροφορία προς κοινή χρήση.

Ο παλιός τρόπος μεταφοράς αρχείων μεταξύ υπολογιστών και υπολογιστικών συσκευών ήταν η αντιγραφή τους σε δισκέτα και η μεταφορά της δισκέτας στον άλλο υπολογιστή. Σήμερα με το Wi-Fi η αντιγραφή αρχείων γίνετε πολύ ευκολότερα χωρίς δισκέτες και καλώδια.

Αποδοτικότητα

Το Wi-Fi μπορεί να αυξήσει την αποδοτικότητα της επιχείρησης σας. Σκεφτείτε αν για παράδειγμα οι πωλητές σας μπορούσαν να έχουν πρόσβαση από τα δημόσια Wi-Fi Hotspots σε ένα κατάστημα καφέ ή σε κάποιο σταθμό βενζίνης, πόση παραπάνω αποδοτικότητα θα κερδίζατε. Ένας πωλητής θα μπορούσε να κάνει άλλο ένα τηλέφωνο την ημέρα αν μπορούσε να παίρνει τα email του σε μια στάση για καφέ αντί να πρέπει να γυρίσει στο γραφείο του.

Ακόμη αν το προσωπικό μπορεί να έχει πρόσβαση στο δίκτυο της επιχείρησης από το meeting room, θα μπορούσαν να παίρνουν αποφάσεις στη διάρκεια της συνάντησης αντί να σπαταλήσουν χρόνο στο να ενημερώσουν μετά τη συνάντηση τα δεδομένα τους.Τέλος, και επισκέπτες της επιχείρησης θα μπορούσαν ως μπόνους να έχουν πρόσβαση στα mails τους , στο Internet ή το δίκτυο της επιχείρησης ανάλογα με την πολιτική ασφάλειας που θα θέσετε.

Με το Wi-Fi οι άνθρωποι μπορούν να χρησιμοποιούν τους υπολογιστές-laptops τους κυριολεκτικά οπουδήποτε στο κτήριο. Παρέχοντας τους δυνατό σήμα μπορούν να δουλέψουν από την αποθήκη και τον διάδρομο έως στην ταράτσα. Τώρα μπορείτε να παίρνετε τα laptops στα meetings χωρίς να χρειάζεται να ψάχνετε τριγύρω για πρίζα δικτύου. Η τοπική καφετέρια ή το εστιατόριο μπορούν να γίνουν μέρη που μπορείτε να αξιοποιήσετε το χρόνο σας. Χάρις το Wi-Fi επίσης μπορείτε να εκμεταλλευτείτε τις δυνατότητες ενός PDA κάτι που ήταν πολύ δύσκολο με τα ενσύρματα δίκτυα. Εξάλλου αυτές οι συσκευές από τη φύση τους απαιτούν ασύρματη σύνδεση.

2.6.2)WiMAX (WMANS)

Προκειται για ένα νέο πρωτοκολλο σχεδιασμενο για τα MANS.
Το WiMAX ,γνωστο και ως ***802.16***,είναι μια νέα τεχνολογία, που θα πραγματοποιήσει την ευρυζωνική πρόσβαση του "τελευταίου μιλίου" - έκφραση που αναφέρεται στην τελική διασπορά των υπηρεσιών τηλεφωνίας και δεδομένων σε αστικά περιβάλλοντα- σε μια μεγαλύτερη γεωγραφική περιοχή από ότι το WLAN, παρέχοντας στους επιχειρησιακούς πελάτες ευρυζωνικές υπηρεσίες τύπου TI (1.544Mbps), ενώ στους απλούς χρήστες πρόσβαση ανάλογη του DSL. Με ακτίνα κάλυψης από 1,5 έως 9km, το WiMAX θα επιτρέψει μεγαλύτερη κινητικότητα στις εφαρμογές δεδομένων υψηλών ταχυτήτων. Το 2003 η IEEE υιοθέτησε το πρότυπο 802.16 γνωστό και σαν WiMAX, ώστε να ικανοποιήσει τις απαιτήσεις για ασύρματη πρόσβαση (με σταθερούς ρυθμούς) ευρείας ζώνης. Όπως συμβαίνει με

τα πρότυπα της σειράς 802 για ασύρματα τοπικά δίκτυα, έτσι και το 802.16 καθορίζει μια οικογένεια προτύπων με επιλογές για συγκεκριμένες ρυθμίσεις.

Το πρότυπο αυτό σχεδιάστηκε ώστε να λειτουργεί σε μια ευρεία μπάντα συχνοτήτων η οποία εκτείνεται από 2 ως 66 GHz. Υποστηρίζει ταχύτητες μετάδοσης ως και 72 Mbps στον αέρα ενώ η πραγματική ταχύτητα στο Ethernet υπολογίζεται στα 50 Mbps. Οι αποστάσεις που μπορεί να καλυφθούν ξεπερνούν τα 50 Km σε συνθήκες οπτικής επαφής. Μια σημαντική διαφορά του προτύπου IEEE 802.16 σε σχέση με το IEEE 802.11 είναι ότι το πρώτο μπορεί να χρησιμοποιηθεί και σε συνθήκες μη οπτικής επαφής φυσικά με ρυθμούς μετάδοσης πολύ χαμηλότερους των 50 Mbps.

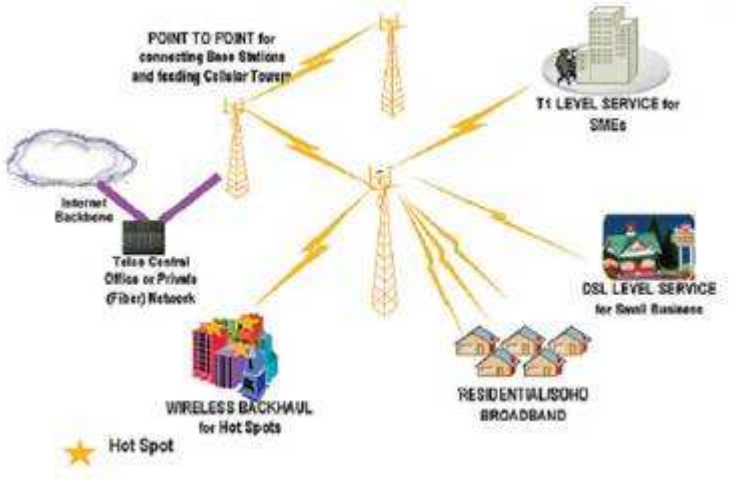
Το WiMAX σχεδιάστηκε κατά βάση ώστε να καλύπτει κυρίως Point-to-Multipoint (PTM) συνδέσεις χωρίς ωστόσο να αποκλείεται και η χρήση του για point to point συνδέσεις. Η διαμόρφωση η οποία χρησιμοποιείται ονομάζεται OFDM (Orthogonal Frequency Division Multiplexing). Πρόκειται για μια πολύ ανθεκτική διαμόρφωση σε ότι αφορά το φαινόμενο της πολυδιόδευσης ειδικότερα στις συχνότητες πάνω των 2 GHz όπου το πρότυπο χρησιμοποιεί.

Παραλλαγές του προτύπου, που στοχεύουν στους κινητούς χρήστες (802.16e) και στην παροχή QoS (802.16b) είναι ήδη σε εξέλιξη. Διάφοροι προμηθευτές chip, συμπεριλαμβανομένης και της Intel, εργάζονται στο 802.16a ενσωματωμένο πυρίτιο, και σε χαμηλού κόστους μονάδες συνδρομητών και αναμένεται στο τέλος του 2005 να είναι ευρέως διαθέσιμα σημεία πρόσβασης (Access Points - AP). Αρκετοί προμηθευτές που έχουν ασχοληθεί με εξοπλισμό για ευρείας ζώνης ασύρματη πρόσβαση, έχουν εκδηλώσει το ενδιαφέρον τους για το WiMAX και έτσι δραστηριοποιούνται στην κατασκευή προϊόντων συμβατών με το εν λόγω πρότυπο.

Λόγω των μεγάλων αποστάσεων που καλύπτει και ταυτόχρονα τους υψηλούς ρυθμούς μετάδοσης που μπορεί να παρέχει, το πρότυπο WiMAX βρίσκει πολλές εφαρμογές, λύνοντας σημαντικά προβλήματα που απασχολούσαν του τεχνικούς δικτύων σήμερα. Τρεις είναι οι βασικότερες χρήσεις του:

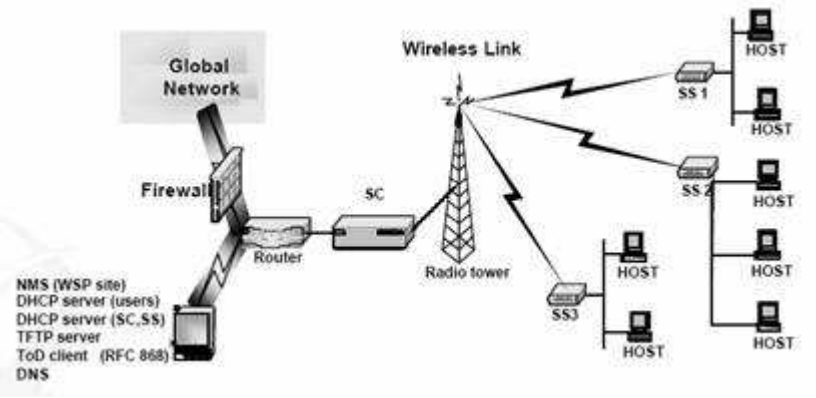
- Δίκτυο κορμού στα κυψελωτά συστήματα κινητής τηλεφωνίας. Η εισαγωγή του προτύπου αυτού αναμένεται να μειώσει σημαντικά το κόστος εξάπλωσης των δικτύων κινητής τηλεφωνίας μιας και αποτελεί μια οικονομικότερη πρόταση, αν συγκριθεί με την οπτική ίνα, για τις εταιρίες κινητής τηλεφωνίας. Εξασφαλίζει ταυτόχρονα αξιοπιστία και υψηλούς ρυθμούς μετάδοσης που απαιτούν τα δίκτυα κορμού των κινητών δικτύων επικοινωνιών.

- Broadband on Demand. Παρέχει υψηλούς ρυθμούς μετάδοσης κάνοντας εφικτή τη χρήση της τεχνολογίας για εφαρμογές πραγματικού χρόνου κάτι που με το πρότυπο IEEE 802.11 σε μεγάλες αποστάσεις δεν ήταν εφικτό.
- Παρέχει κάλυψη σε περιοχές που είναι αδύνατο τα καλυφθούν με χρήση χαλκού ή οπτικής ίνας. Μπορεί να χρησιμοποιηθεί σαν συμπλήρωμα δικτύων οπτικών ινών σε τμήματα του εδάφους στα οποία το κόστος εγκατάστασης και συντήρησης δικτύων οπτικών ινών είναι απαγορευτικό.



Οι ταχύτητες μετάδοσης του προτύπου εξαρτώνται από την εκάστοτε ψηφιακή διαμόρφωση που χρησιμοποιείται. Συνήθεις διαμορφώσεις είναι η 64 QAM η οποία μπορεί να εξασφαλίσει και τη μεγαλύτερη ταχύτητα μετάδοσης, η 16 QAM και η QPSK η οποία μπορεί να εξασφαλίσει μεγάλη κάλυψη του συστήματος.

Το πρότυπο IEEE 802.16 παρέχει υψηλού επιπέδου ποιότητα υπηρεσίας. Το επίπεδο MAC του προτύπου είναι σχεδιασμένο κατά τέτοιο τρόπο ώστε να παρέχει στους χρήστες, όταν οι ίδιοι το επιθυμούν, εγγυημένο ρυθμό μετάδοσης και ταυτόχρονα κίνηση best effort σε χρήστες που καλύπτονται από το ίδιο base station κάτι που το πρότυπο IEEE 802.11 δεν μπορούσε να εξασφαλίσει. Δηλαδή, αν υποθέσουμε ότι δύο χρήστες καλύπτονται από το ίδιο Base Station, είναι δυνατό ο ένας χρήστης να έχει εγγυημένη ποιότητα υπηρεσίας και ο δεύτερος χρήστης να δέχεται και να στέλνει απλή IP κίνηση best effort κάτι που με το πρότυπο 802.11 δεν ήταν δυνατό. Δηλαδή χρήστες που βρισκόταν στην κάλυψη ενός Access Point είχαν την ίδια ποιότητα υπηρεσίας.



Την ασφαλή μετάδοση των δεδομένων στο WiMAX αναλαμβάνει ο αλγόριθμος κρυπτογράφησης DES (Data Encryption Standard, Πρότυπο Κωδικοποίησης Δεδομένων) και συγκεκριμένα μια παραλλαγή του αλγορίθμου ο Triple DES. Το DES αναπτύχθηκε το 1970 από το Αμερικανικό Εθνικό Γραφείο Προτύπων. Η βασική ιδέα ήταν η ανάπτυξη ενός αλγόριθμου κρυπτογράφησης που θα μπορούσε να χρησιμοποιηθεί (και να βελτιωθεί) από διάφορες εταιρείες ή οργανισμούς. Το DES ανήκει στην οικογένεια των συμμετρικών αλγόριθμων και κάνει χρήση κλειδιών με μήκος 56 bit. Ο "κλασικός" αλγόριθμος DES είναι πλέον ξεπερασμένος, αφού με τη χρήση ενός σύγχρονου υπολογιστή μπορεί να παραβιαστεί σχετικά εύκολα. Στο μεταξύ, εφαρμόζοντας διάφορες τεχνικές επάνω στο DES, μπορούμε να αυξήσουμε σημαντικά την ασφάλειά του. Με τη μέθοδο Triple - DES, για παράδειγμα, το μήνυμα κωδικοποιείται τρεις φορές, με τρία διαφορετικά κλειδιά.

Όπως έχει ήδη αναφερθεί, στην αρχική του έκδοση το πρότυπο IEEE 802.16 λειτουργούσε στην ζώνη συχνοτήτων 10-66 GHz. Στις παραπάνω συχνότητες η επικοινωνία μεταξύ δύο σταθμών επιτυγχάνεται μόνο όταν οι σταθμοί αυτοί βρίσκονται σε συνθήκες οπτικής επαφής. Η παραπάνω διαδικασία περιγράφεται στο υποπρότυπο IEEE 802.11 c. Η ανάγκη για επικοινωνία μεταξύ σταθμών που δεν βρίσκονται σε οπτική επαφή ήταν το κίνητρο για τη δημιουργία του υποπροτύπου IEEE 802.16 a. Τον Ιανουάριο του 2003 το πρότυπο επεκτάθηκε ώστε να λειτουργεί και στις συχνότητες από 2-11 GHz όπου στις συχνότητες αυτές ήταν δυνατή η δημιουργία συνδέσεων χωρίς οπτική επαφή πομπού - δέκτη. Το υποπρότυπο το οποίο περιγράφει τη διαδικασία αυτή ονομάστηκε IEEE 802.16 a. Τα πρώτα προϊόντα WiMAX τα οποία σήμερα είναι διαθέσιμα στην αγορά ακολουθούν στην μεγαλύτερή τους πλειοψηφία το υποπρότυπο αυτό.

2.6.3)HiperLAN/1 και 2

Το HiperLAN (High Performance Radio LAN) είναι μια τεχνολογια που αναπτύχθηκε στις ευρωπαϊκές χώρες ως πρότυπο υψηλής ταχύτητας WLAN και είναι παρόμοιο με το αμερικάνικο πρότυπο IEEE 802.11. Υπάρχουν δύο τύποι προδιαγραφών, το HiperLAN/1 και το HiperLAN/2. Και τα δύο πρότυπα έχουν υιοθετηθεί από το ETSI. Το HiperLAN/1 αναπτύχθηκε το 1996 και προσφέρει ταχύτητες δεδομένων μέχρι 20Mbps στη ζώνη των SCHz του φάσματος ραδιοσυχνοτήτων, κυρίως σε ad-hoc δίκτυα και χωρίς να εγγυάται την ποιότητα υπηρεσιών. Το HiperLAN/2 προσφέρει ταχύτητες δεδομένων μέχρι 54Mbps στην ίδια ζώνη ραδιοσυχνοτήτων, καθώς και καλύτερη ποιότητα υπηρεσιών. Το φυσικό μέσο μετάδοσης είναι το ίδιο με αυτό του 802.11a και το ETSI συνεργάστηκε με το IEEE για την ανάπτυξη του. Δεδομένου ότι ο χαμηλότερος ρυθμός μετάδοσης του 802.11a περιορίζει τη χρήση του, ειδικά στις εφαρμογές πολυμέσων, η υψηλότερη ταχύτητα του HiperLAN, αν και είναι πιθανόν να κοστίζει περισσότερο, αποτελεί μια αποτελεσματική εναλλακτική τεχνολογία για ορισμένες εφαρμογές WLAN, ιδιαίτερα αυτές που περιλαμβάνουν μετάδοση τηλεοπτικών εικόνων. Το HiperLAN είναι βασισμένο στην τεχνολογία ασύγχρονης μεταφοράς (ATM) και προσφέρει καλύτερη ποιότητα υπηρεσιών από τις αντίστοιχες του 802.11.

2.6.4)Wi Wan(3G/UMTS)

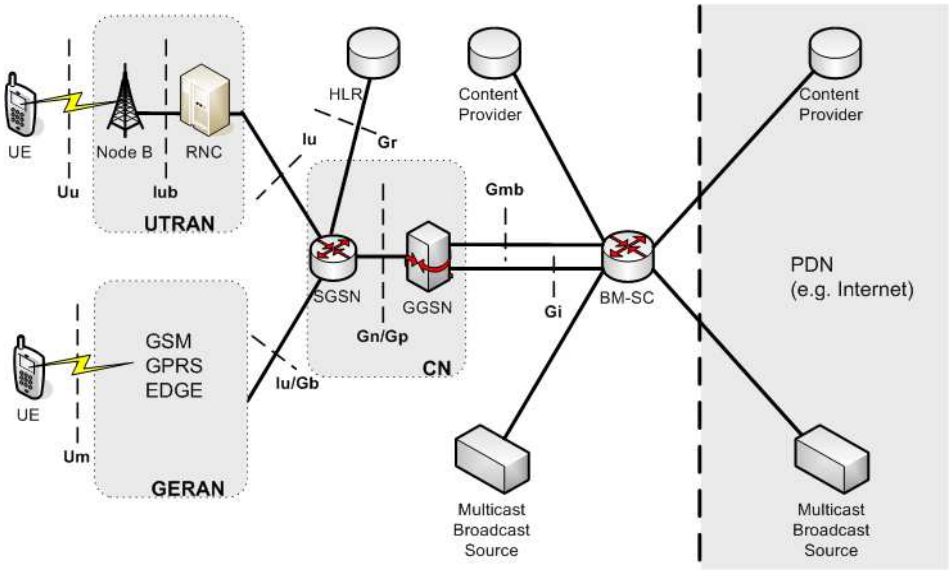
Ο όρος UMTS προέρχεται από τα αρχικά των λέξεων "Universal Mobile Telecommunications System" (Παγκόσμιο Σύστημα Κινητών Τηλεπικοινωνιών). Πρόκειται για την εξέλιξη σε σχέση με την χωρητικότητα, την ταχύτητα μετάδοσης των δεδομένων και την ύπαρξη νέων υπηρεσιών, των κινητών δικτύων δεύτερης γενιάς. Σήμερα, περισσότερα από εξήντα 3G/UMTS δίκτυα που χρησιμοποιούν την WCDMA τεχνολογία λειτουργούν σε 25 χώρες. Για την οργάνωση του όλου εγχειρήματος έχει θεσπιστεί ειδικός μη κερδοσκοπικός οργανισμός με την ονομασία Third Generation Partnership Project (3GPP) του οποίου μέλημα είναι η παρακολούθηση και η καθοδήγηση των εξελίξεων στην συγκεκριμένη τεχνολογική περιοχή.

Ανάμεσα στα πλεονεκτήματα των UMTS δικτύων ξεχωρίζουμε τους αυξημένους ρυθμούς μετάδοσης των δεδομένων και την ταυτόχρονη υποστήριξη μεγαλύτερου όγκου δεδομένων και φωνής. Πιο συγκεκριμένα, το UMTS δίκτυο στην αρχική του φάση, θεωρητικά προσφέρει ρυθμούς μετάδοσης δεδομένων έως και 384 kbps σε περιπτώσεις όπου παρατηρείται αυξημένη κινητικότητα του χρήστη.

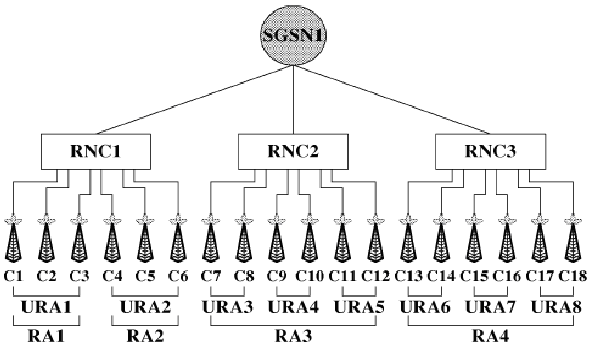
Αντίθετα, όταν ο χρήστης παραμένει ακίνητος οι ρυθμοί μετάδοσης αυξάνουν κατά πολύ φθάνοντας την τιμή των 2 Mbps.

Εκτιμάται ότι στο μέλλον θα υπάρξει περαιτέρω αύξηση των ρυθμών μετάδοσης δεδομένων. Ήδη, ο 3GPP έχει θέσει σαν standard δύο νέες τεχνολογίες. Πρόκειται για το High Speed Downlink Packet Access (HSDPA) και το High Speed Uplink Packet Access (HSUPA) αντίστοιχα. Οι συγκεκριμένες τεχνολογίες ουσιαστικά αποτελούν εξέλιξη του UMTS, αφού υπόσχονται ρυθμούς μετάδοσης των δεδομένων έως και 14,4 Mbps στο downlink και 5.8 Mbps στο uplink.

Στην συνέχεια παρουσιάζεται η αρχιτεκτονική ενός UMTS δικτύου καθώς και διάφορα άλλα σχετικά θέματα όπως η διαχείριση της κινητικότητας των χρηστών. Πιο συγκεκριμένα λοιπόν, ένα δίκτυο UTMS αποτελείται από δύο βασικές οντότητες: το δίκτυο κορμού (CN - core network) και το δίκτυο επίγειας ασύρματης πρόσβασης (UTRAN - UMTS terrestrial radio-access network). Το δίκτυο κορμού είναι υπεύθυνο για την δρομολόγηση των τηλεφωνημάτων καθώς και για τις συνδέσεις για μεταφορά δεδομένων με εξωτερικά δίκτυα. Αντίθετα, το UTRAN είναι υπεύθυνο για οτιδήποτε σχετίζεται με το ασύρματο μέρος του δικτύου. Το CN αποτελείται από δύο domain: α) circuit -switched (CS - μεταγωγή κυκλώματος), β) packet-switched (PS - μεταγωγή πακέτου). Το CS domain παρέχει πρόσβαση στο PSTN/ISDN , ενώ το PS domain παρέχει πρόσβαση στα IP δίκτυα. Στο εξής μας ενδιαφέρει το PS domain. Έτσι λοιπόν, το PS μέρος του UMTS δικτύου αποτελείται από δύο GPRS κόμβους υποστήριξης: τον gateway GPRS support node (GGSN) και τον serving GPRS support node (SGSN). Ο SGSN συνδέεται με τον SGSN μέσω της διεπαφής Gn και με το UTRAN μέσω της διεπαφής Iu. Το UTRAN αποτελείται από τον ελεγκτή ασύρματης πρόσβασης (RNC - radio network controller) και το Node B το οποίο αποτελεί την βάση που προσφέρει κάλυψη στο αντίστοιχο κελί. Το Node B συνδέεται με τον εξοπλισμό του χρήστη (user equipment - UE) μέσω της διεπαφής Uu (βασισμένο στην τεχνολογία W-CDMA) και με το RNC μέσω της διεπαφής Gi . Επιπλέον, υπάρχει και ένας άλλος κόμβος σχετιζόμενος με τις υπηρεσίες broadcast/multicast (BM-SC - broadcast/multicast service center), ο οποίος λειτουργεί σαν το σημείο εισόδου για την παραλαβή των δεδομένων για εσωτερικές πηγές. Τα παραπάνω παρουσιάζονται καλύτερα στο σχήμα που ακολουθεί:



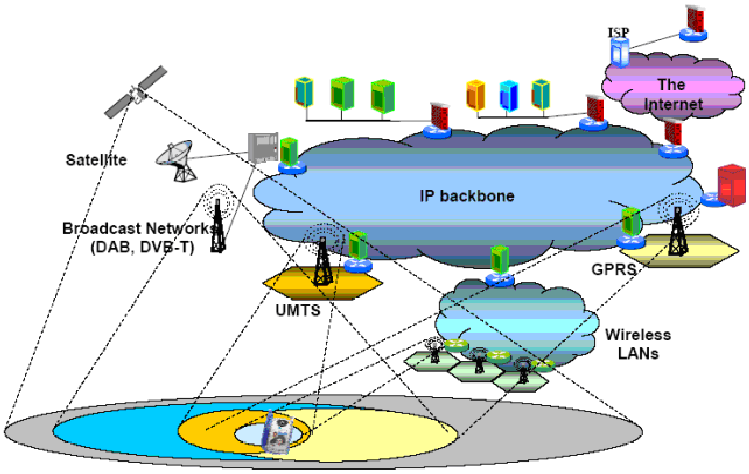
Προτού ένας χρήστης είναι σε θέση να ανταλλάξει δεδομένα με ένα εξωτερικό PDN (Public Data Network), πρέπει να εγκαθιδρύσει μία εικονική σύνδεση με αυτό το PDN. Από την στιγμή που ο συγκεκριμένος κινητός χρήστης γίνει γνωστός στο δίκτυο, τα πακέτα μεταφέρονται μεταξύ αυτού και του δικτύου, βασισμένα στο packet data protocol (PDP), το οποίο αποτελεί το πρωτόκολλο του επιπέδου δικτύου του UMTS. Ένα στιγμιότυπο του PDP ονομάζεται PDP context και περιέχει όλες τις παραμέτρους που χαρακτηρίζουν την σύνδεση με το εξωτερικό δίκτυο όπως τις διευθύνσεις αποστολέα και παραλήπτη καθώς και την ποιότητα της υπηρεσίας. Ένα PDP context εγκαθιδρύεται για όλες τις εφαρμογές που κατευθύνονται προς ή προέρχονται από μία IP διεύθυνση. Μία ενεργοποίηση ενός PDP context ουσιαστικά αποτελεί μία διαδικασία αίτησης - απάντησης μεταξύ του κινητού χρήστη (UE) και του GGSN. Μία επιτυχής PDP context ενεργοποίηση οδηγεί στην δημιουργία δύο GPRS tunneling protocol (GTP) συνόδων για τον εκάστοτε χρήστη. Η πρώτη GTP σύνοδος δημιουργείται μεταξύ του GGSN και του SGSN πάνω από την διεπαφή Gn, ενώ η δεύτερη δημιουργείται μεταξύ του SGSN και του RNC πάνω από την διεπαφή Iu. Τα IP πακέτα τα οποία προορίζονται για μία εφαρμογή, χρησιμοποιώντας συγκεκριμένα GTP contexts, προσαρτώνται σε αυτά και μέσω του PDP μεταφέρονται στο αντίστοιχο SGSN. Το SGSN ανακτά τα IP πακέτα, ζητά το κατάλληλο PDP context βασισμένο στο UE και στο PDP και προωθεί τα πακέτα στο κατάλληλο RNC. Παράλληλα, το RNC διατηρεί έναν φορέα ασύρματης πρόσβασης (RAB - radio access bearer). Αντίστοιχα με τα PDP context, ένα RAB context επιτρέπει στο RNC να ανακτήσει την ταυτότητα του αποστολέα που έχει συσχετιστεί με ένα GTP. Αφού πλέον, το RNC έχει ανακτήσει το πακέτο, το προωθεί στο κατάλληλο Node B. Τέλος, χρησιμοποιείται ένας tunnel endpoint identifier (TEID) στις διεπαφές Gn και Iu έτσι ώστε να μπορεί να αναγνωριστεί το τέλος του tunnel στον κόμβο που δέχεται τα πακέτα.



Στην συνέχεια, αναλύεται ο τρόπος με τον οποίο γίνεται η διαχείριση της κινητικότητας των UE (λεπτομέρειες παρουσιάζονται στο αντίστοιχο σχήμα). Έτσι λοιπόν, στο PS domain του UMTS, τα κελιά ομαδοποιούνται σε περιοχές δρομολόγησης (RAs - routing areas), ενώ τα κελιά σε μία περιοχή δρομολόγησης χωρίζονται περαιτέρω σε UTRAN registration areas (URAs). Επιπλέον, η διαχείριση της κινητικότητας (MM - mobility management) των κινητών χρηστών χαρακτηρίζεται από δύο μηχανές πεπερασμένων καταστάσεων: την μηχανή διαχείρισης της κινητικότητας (MM) και την radio resource control (RRC). Η μηχανή packet MM (PMM) του PS domain του UMTS εκτελείται μεταξύ του SGSN και του UE και είναι υπεύθυνη για τον έλεγχο στο επίπεδο του CN, ενώ η μηχανή RRC εκτελείται μεταξύ του UTRAN και του UE και είναι υπεύθυνη για τον σχετικό έλεγχο στο επίπεδο του UTRAN. Πιο συγκεκριμένα λοιπόν, αφότου ένα UE συνδεθεί στο PS domain, η μηχανή πεπερασμένων καταστάσεων PMM βρίσκεται σε μία από τις εξής δύο καταστάσεις: PMM idle ή PMM connected. Αντίστοιχα η μηχανή RRC μπορεί να βρίσκεται σε μία από τις εξής τρεις καταστάσεις: RRC idle, RRC cell - connected και RRC URA connected. Σημειώνεται ότι όταν δεν υπάρχει ροή δεδομένων μεταξύ του UE και του CN, το UE βρίσκεται στις καταστάσεις PMM idle και RRC idle αντίστοιχα. Στην περίπτωση αυτή το UTRAN δεν έχει καμία πληροφορία για το UE και το UE παρακολουθείται μόνο από το αντίστοιχο SGSN στο επίπεδο RA. Όταν ύστερα ξεκινήσει μία σύνδεση μεταξύ του UE και του SGSN, το UE μεταβαίνει στην κατάσταση PMM connected. Από την στιγμή που η σύνδεση στο PS λάβει χώρα, αυτόματα ξεκινά και μία RRC σύνδεση μεταξύ του UE και του αντίστοιχου RNC που το εξυπηρετεί. Σε αυτή την περίπτωση η RRC μηχανή για το συγκεκριμένο UE μεταβαίνει στην κατάσταση RRC cell - connected. Όταν κάτι τέτοιο συμβεί, το SGSN παρακολουθεί το UE με ακρίβεια μέσω του αντίστοιχου RNC που εξυπηρετεί το UE. Το συγκεκριμένο RNC είναι υπεύθυνο να παρακολουθεί το κελί όπου το UE βρίσκεται κάθε στιγμή. Σημειώνεται ότι τα πακέτα μπορούν να ληφθούν από το UE μόνο όταν βρίσκεται σε αυτή την κατάσταση. Στην PMM connected/RRC cell - connected κατάσταση, αν το UE δεν έχει μεταδώσει/λάβει πακέτα για ένα συγκεκριμένο χρονικό διάστημα, η RRC μηχανή μεταβαίνει στην κατάσταση RRC URA connected. Σε αυτή την

περίπτωση, η RCC σύνδεση διατηρείται ακόμη, ενώ το UE παρακολουθείται από το RNC που το εξυπηρετεί. Η συγκεκριμένη μετάβαση δεν επηρεάζει καθόλου την κατάσταση της PMM μηχανής για το συγκεκριμένο UE. Στην PMM connected / RRC URA connected κατάσταση, αν το UE μεταδώσει/λάβει ένα πακέτο, η RRC μηχανή μεταβαίνει πάλι στην κατάσταση RRC cell - connected. Αντίθετα, αν οι πόροι για τις συνδέσεις στο PS και RRC επίπεδο αποδεσμευτούν (για παράδειγμα όταν μία σύνοδος επικοινωνίας ολοκληρωθεί) ή αν κανένα πακέτο δεν έχει μεταδοθεί για ένα μεγάλο χρονικό διάστημα, η RRC μηχανή αρχικά μεταβαίνει στην RRC cell - connected κατάσταση και μετά στην RRC idle κατάσταση. Σε αυτή την περίπτωση, η PMM μηχανή αντίστοιχα μεταβαίνει στην PMM idle κατάσταση. Τέλος, όταν ένα UE δεν μπορεί να εντοπιστεί από το δίκτυο, η κατάστασή του χαρακτηρίζεται σαν PMM detached.

Η τεχνολογία εξελίσσεται διαρκώς και παρά το γεγονός ότι η τρίτη γενιά δεν είναι ακόμη σε πλήρη λειτουργία, η ακαδημαϊκή εξερεύνηση της 4G κινητής επικοινωνίας έχει ήδη ξεκινήσει. Καταρχήν η τρίτη γενιά ασφαλώς ήταν το βασικότερο βήμα για την επίτευξη των προσωπικών τηλεπικοινωνιών, αλλά ωστόσο δεν κατάφερε να τις κάνει πραγματικότητα.



Η τέταρτη γενιά θα προσεγγίσει περισσότερο τις προσωπικές επικοινωνίες παρέχοντας επικοινωνία οποιαδήποτε μορφής, σε κάθε χώρο και χρόνο, με οποιονδήποτε. Θα απαιτήσει επίσης καλή απόδοση επικοινωνίας, που θα αφορά κυρίως media παρά φωνή. Στις εφαρμογές τα τερματικά της τέταρτης γενιάς δε θα παρέχουν μόνο ομιλία ή εικόνα αλλά επιπλέον θα προειδοποιεί και θα ενημερώνει το χρήστη. Τα τερματικά μπορεί ακόμα να γίνουν μέρος του ανθρώπινου σώματος, ενημερώνοντας το χρήστη για την πίεσή του, τη θερμοκρασία του κ.α.

Αναμένεται νέα δημοσίευση του πρωτοκόλλου με ταχύτητα στα 10Mbps.

2.6.5) *Wi Pan (Personal)*

Περνώντας στο πεδίο των προσωπικών δικτύων (Personal Area Networks, εν
αντιθέσει με τα LANs), πρέπει να αναφερθούμε στο **Bluetooth**, ένα πρωτόκολλο με μεγάλη αποδοχή από τους μεγαλύτερους κατασκευαστές στον χώρο.Προκειται για το πρωτοκολλο ***802.15.*** Λειτουργεί και αυτό στους 2.4 μεγάκυκλους και έχει μέγιστη ταχύτητα το 1mbps. Έχει σκοπό την δημιουργία ενός δικτύου μικρής εμβέλειας γύρω από τον χρήστη του, το οποίο μπορεί να αλληλεπιδρά με αντίστοιχες Bluetooth-enabled συσκευές.
Το **HomeRF** ξεκίνησε από την HomeRF Working Group η οποία προσέφερε
στην αγορά μια ανοιχτή βιομηχανική προδιαγραφή με το όνομαSWAP(Shared
Access Wireless Protocol), με προορισμό την ασύρματη ψηφιακή επικοινωνία μεταξύηλεκτρονικών υπολογιστών και ηλεκτρονικών συσκευών στο οικιακό περιβάλλον.Υποστηρίζει διαμόρφωση Frequency Hopping spread spectrum με ταχύτητα του1Mbps.

2.6.6)LMDS και WLL

Το Local Multipoint Distribution System (LMDS), είναι η ευρυζωνική ασύρματη τεχνολογία, που χρησιμοποιείται για να μεταδώσει φωνή, δεδομένα/υπηρεσίες διαδικιύου και τηλεοπτικές υπηρεσίες στην περιοχή των 25CHz, καθώς και σε υψηλότερες συχνότητες. Ως αποτέλεσμα των χαρακτηριστικών διάδοσης του σήματος, σε αυτό το φάσμα, το LMDS χρησιμοποιεί μια κυψελοειδή δικτυακή αρχιτεκτονική, αν και οι παρεχόμενες υπηρεσίες είναι σταθερές και όχι κινητές. Το LMDS είναι ένα σύστημα απευθείας μικροκυματικής μετάδοσης από μια τοπική κεραία στο σπίτι ή την επιχείρηση, εντός της ακτίνας οπτικής επαφής, αποτελώντας έτσι μια λύση στο αποκαλούμενο "πρόβλημα του τελευταίου μιλίου", προσφέροντας οικονομικές υπηρεσίες ευρείας ζώνης στους τελικούς χρήστες. Το LMDS αποτελεί εναλλακτική λύση στην εγκατάσταση οπτικής ίνας για προσφορά ευρυζωνικών υπηρεσιών (η δυνατότητα αυτή δεν υφίσταται σήμερα στην Ελλάδα). Ανάλογα με την εφαρμογή, το LMDS παρέχει ταχύτητα μέχρι 1 ,SCbps προς το χρήστη (downstream) και 200Mbps από το χρήστη προς το δίκτυο (upstream), αν και ένας πιο ρεαλιστικός αριθμός είναι τα 38Mbps downstream. Το κόστος του LMDS θεωρείται πολύ χαμηλότερο από αυτό της εγκατάστασης οπτικών ινών ή της αναβάθμισης των συστημάτων καλωδιακής τηλεόρασης.

2.7) Χρήσεις

Κάθε τεχνολογία είναι σημαντική, για διαφορετικούς λόγους. Ενώ το WLAN είναι ιδανικό νια τις απομονωμένες περιοχές, τοW1MAX πρόσφερα ασύρματη κάλυψη σε μεγάλες αποστάσεις. Το LMDS από την άλλη πλευρά, προσφέρει πολύ υψηλούς ρυθμούς μετάδοσης, αλλά κυρίως σε σταθερούς προορισμούς, λόγω του σχετικά ογκώδους απαιτούμενου εξοπλισμού. Δεδομένου ότι η πληροφορική και οι επικοινωνίες συγκλίνουν σε ευρυ-ζωνικές ασύρματες πλατφόρμες και τεχνολογίες, η ανάγκη για αληθινή κινητικότητα θα γίνει επιτακτική/Οταν αυτό συμβεί, οι τεχνολογίες, η υποδομή, οι συσκευές και οι υπηρεσίες που θα επιτρέπουν στους χρήστες να μένουν συνδεμένοι, ακόμη και όταν αυτοί κινούνται σε οποιονδήποτε χώρο, θα πρέπει να είναι έτοιμες να λειτουργήσουν. Απώτερος σκοπός είναι η "πάντα καλύτερη δυνατή σύνδεση" του χρήστη (best connected), χρησιμοποιώντας τις προαναφερθείσες συμπληρωματικές ευρυζωνικές τεχνολογίες. Στην πραγματικότητα, η κινητικότητα που επιτρέπεται από την ασύρματη τεχνολογία, απαιτεί τη συμπληρωματικότατα των δικτύων και τη συνύπαρξη των τεχνολογιών - είτε αυτές είναι ενσύρματες είτε ασύρματες

2.8) ΠΡΟΒΛΗΜΑΤΑ ΣΤΑ ΑΣΥΡΜΑΤΑ LANS

Το πρόβλημα του «κρυμμένου σταθμού» (hidden node)

Στην παράγραφο αυτό θα ορίσουμε και θα περιγράψουμε ίσως ένα από τα μεγαλύτερα μειονεκτήματα του 802.11b, το πρόβλημα του κρυμμένου κόμβου, το οποίο είναι καθαρά εγγενές στο σχεδιασμό του πρωτοκόλλου και οφείλεται πιθανότατα στους ίδιους τους στόχους τους οποίους έθεσε η ομάδα εργασίας της IEEE για το WiFi σαν εναλλακτικό τρόπο δικτύωσης σε τοπικό επίπεδο. Είναι ένα πρόβλημα που εμφανίζεται μόνο σε infrastructure mode, όπως θα γίνει κατανοητό στις πιο κάτω γραμμές. Ας υποθέσουμε ότι έχουμε ένα κεντρικό Access Point και πολλούς clients σε διαφορετικές τοποθεσίες, έτσι ώστε όλοι οι clients να έχουν οπτική επαφή με το AP, αλλά όχι και καθένας με τον άλλο. Μιλάμε δηλαδή για μια αρκετά τυπική περίπτωση ενός π.χ., ενδοπανεπιστημιακού δικτύου.
Από τον ορισμό του το 802.11b προορίζονταν για ένα κλειστό περιβάλλον γραφείου. Σε αυτό το περιβάλλον, η επιτροπή της IEEE θεώρησε λογικό το ότι όλοι οι client κόμβοι που είναι συνδεδεμένοι σε ένα Access Point θα μπορούν «ακούν» το τι στέλνει ο γείτονάς τους.

Χωρίς δηλαδή στην πραγματικότητα να λαμβάνουν τα δεδομένα που εκπέμπει ο διπλανός client προς το AP, έχουν την πληροφορία ότι αυτή την στιγμή κάποιος χρησιμοποιεί το κανάλι, στέλνοντας δεδομένα.
Η κύρια μέθοδος αποφυγής συγκρούσεων στο 802.11 είναι το CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Η λειτουργία Carrier Sense πραγματοποιείται με παρακολούθηση του καναλιού πριν της έναρξη εκπομπής. Αν κάποιος άλλος client εκείνη την ώρα τύχει να εκπέμπει, τότε ο πρώτος περιμένει, έως ότου να βρεθεί στιγμή που το κανάλι να είναι ελεύθερο. Όπως καταλαβαίνουμε, για να επιτευχθεί ένα καλό ποσοστό συγχρονισμού, που θα εξασφαλίσει την εύρυθμη λειτουργία του δικτύου, πρέπει οι περισσότεροι client να βρίσκονται σε θέση να ακούν τις εκπομπές όλων των άλλων. Όταν δηλαδή ένας σταθμός ελέγχει το μέσο για να δει αν είναι σε χρήση, μπορεί εσφαλμένα να αποφασίσει ότι είναι ελεύθερο, μιας και δεν είναι σε θέση να λαμβάνει τις εκπομπές όλων των άλλων σταθμών του Access Point. Σε αυτήν την περίπτωση, το αποτέλεσμα θα είναι συνεχείς συγκρούσεις. Σε περίπτωση σύγκρουσης, το αποτέλεσμα είναι όμως δεν είναι τυχαίο,κάτι που αν συνέβαινε θα οδηγούσε ίσως σε ισορροπία. Συνήθως το Access Point τείνει να ευνοεί τον εκπομπό με το καλύτερο σήμα, καθώς λαμβάνει το σήμα του ασθενέστερου σαν θόρυβο και απορρίπτοντάς το. .εδομένων λοιπόν των συνθηκών,μια και μόνο συσκευή μπορεί να μονοπωλήσει ολόκληρο το εύρος ζώνης του AP.
Ευνοϊκές συνθήκες για την εμφάνιση προβλήματος κρυμμένου κόμβου δεν είναι όμως μόνο οι περιπτώσεις που υπάρχουν εμπόδια μεταξύ δύο ή περισσότερων σταθμών. Η επικοινωνία τύπου «όλοι ακούν όλους», μπορεί να είναι εφικτή μόνο όταν χρησιμοποιούμε μη κατευθυντικές(omni directional) κεραίες, οι οποίες εκπέμπουν κυκλικά το σήμα τους. Πολλές φορές όμως, η χρήση κατευθυντικών κεραιών(yagi, parabolic grid) υψηλού κέρδους σήματος, είναι μονόδρομος για να επιτευχθεί σύνδεσή. Κάτω από αυτές τις συνθήκες, μια και μόνο client συσκευή είναι δυνατόν να μονοπωλήσει όλο το εύρος ζώνης του Access Point,προκαλώντας έτσι τεράστια συμφόρηση στις διακινήσεις δεδομένων των υπόλοιπων κόμβων.
Η εισαγωγή του μηχανισμού RTS/CTS έδωσε κάποια ελπιδοφόρα μηνύματα στην κοινότητα χρηστών του 802.11b. Η υλοποίηση βέβαια του μηχανισμού αυτού δεν είναι υποχρεωτική, και υπάρχουν πάρα πολλές συσκευές που δεν το υποστηρίζουν. Τελικά όμως ο μηχανισμός αυτός αποτυγχάνει πλήρως να αμβλύνει το φαινόμενο του Hidden Node, εν μέρει λόγω συγκρούσεων στα ίδια τα πακέτα RTS (περνάνε μόνο τα RTS του δυνατότερου). Παρόλο τον σχεδιασμό του, με πακέτα μικρού μεγέθους και ως εκ τούτου μικρότερη πιθανότητα σύγκρουσης, αλλά και γρηγορότερη διόρθωση των συγκρούσεων, η πραγματική χρήση τους σε δίκτυα εξωτερικού χώρου δεν φαίνεται να έχει αποτέλεσμα.

Λύσεις υπάρχουν, και διαφέρουν σε προσέγγιση αλλά και κόστος. Υπάρχουν ειδικές συσκευές (ή firmware για συσκευές) οι οποίες εφαρμόζουν ένα είδος polling στο δίκτυο. Τέτοιες λύσεις έχουν θεωρικά αλλά και πρακτικά μεγάλη επιτυχία στην σωστή χρήση του εύρους ζώνης, αλλά έχουν μεγάλο κόστος, καθώς είναι παντελώς ασύμβατες με τα κλασσικά wifi προϊόντα, μιας και βγαίνουν εκτός του προτύπου. Λύσεις για bandwidth control σε υψηλότερο επίπεδο ερευνούνται, μα και πάλι δεν παρέχουν καμία εγγύηση για την εξάλειψη συγκρούσεων. Ίσως η καλύτερη λύση στο πρόβλημα έχει να προσφέρει η κοινότητα ανοιχτού κώδικα, και για την ακρίβεια, η ομάδα του Patras Wireless. Μια ελπιδοφόρος λύση είναι το πρωτόκολλο WiCCP(Wireless Central Coordination Protocol), το οποίο γράφτηκε και υλοποιήθηκε από δύο μέλη του PWN.Το πρωτόκολλο υλοποιείται σε δύο κομμάτια λογισμικού, ένα master και ένα client network driver. Το πρώτο μπαίνει σε έναν υπολογιστή με wired σύνδεση στο AP και το client κομμάτι στο network driver stack κάθε υπολογιστή-χρήστη του AP. Στο πρωτόκολλο υπάρχει η ιδέα του token. Ο master δίνει το token σε κάθε client για ένα συγκεκριμένο χρονικό περιθώριο (timeslice). Μόνο ένας client μπορεί να έχει το token κάθε φορά. Όταν ο client θέλει να στείλει κάποιο πακέτο, κοιτάει αν το master τμήμα(στο access point) του έχει δώσει το token. Αν ναι, τότε προχωρά στην αποστολή, που θα κρατήσει όσο χρόνο του αφήνει το token. Αν δεν το έχει, τότε ο driver κρατά τα πακέτα που στέλνει ο χρήστης σε προσωρινή ουρά, και περιμένει να ξαναπάρει το token, αδειάζοντας την ουρά. Στην ουσία δημιουργεί ένα είδος tokenring στο standard Ethernet που χρησιμοποιεί το δίκτυο, τελείως transparent στις εφαρμογές χρήστη. Έτσι εγγυημένα αποφεύγονται όλες οι συγκρούσεις, καθώς μόνο ένας μιλάει κάθε φορά στο Access Point. .είτε το patraswireless.net για περισσότερες πληροφορίες πάνω στο πρωτόκολλο, το οποίο ονομάζεται WiCCP(Wireless Central Coordinated Protocol), και βρίσκεται αισίως στην έκδοση 0.5. Η ανάπτυξη του driver γίνεται σε συνεργασία με άλλες μεγάλες ασύρματες κοινότητες, όπως το Perth Wireless της Αυστραλίας.

ΚΕΦΑΛΑΙΟ 3^{Ο}

ΑΣΦΑΛΕΙΑ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

3.1) *Γενικά περί ασφάλειας*

Δεν είναι δυνατό να υπάρξει 100% ασφαλές δίκτυο. Η πληροφορία πρέπει να είναι προσβάσιμη για να είναι χρήσιμη, όμως η ασφάλεια μειώνεται όσο πιο προσβάσιμη γίνεται η πληροφορία. Γι αυτό το λόγο η ισορροπία μεταξύ πρόσβασης και ασφάλειας βασίζεται στη πολιτική που ασκεί η διαχείριση του δικτύου. Η σωστή ασφάλεια χρειάζεται προσεκτικό σχεδιασμό έτσι ώστε η παράτυπη, χωρίς άδεια πρόσβαση να είναι δύσκολο να συμβεί και εύκολο να ανιχνευτεί.

Η ασφάλεια ενός δικτύου περιλαμβάνει ένα μεγάλο εύρος θεμάτων. Τέτοια θέματα περιέχουν τη προστασία του δικτύου και των σχετικών συσκευών, τη προστασία της πληροφορίας που αποθηκεύεται σε ένα σύστημα ή ταξιδεύει πάνω στο δίκτυο καθώς και τη προστασία εναντίων των χρηστών που δεν έχουν άδεια πρόσβασης.

Ένα ασφαλές δίκτυο σημαίνει ότι όλα τα συστήματα του δικτύου μπορούν να πραγματοποιήσουν τα εξής:

- Να αποτρέψουν τη πρόσβαση στη πληροφορία σε μη εξουσιοδοτημένους χρήστες
  Να αποτρέψουν τη φθορά πληροφορίας που απευθύνεται σε συστήματα ή χρήστες.
- Να αποτρέψουν τη μη εξουσιοδοτημένη αλλαγή στη πληροφορία που πραγματοποιείται από χρήστες ή εισβολείς.

  Γρήγορη επαναφορά του συστήματος σε σταθερή κατάσταση ύστερα από δυσλειτουργία του υλικού ή λογισμικού μέρους.

Μέρος λοιπόν των παραπάνω στόχων για ασφάλεια στο δίκτυο πραγματοποιείται μέσω μηχανισμών για τον έλεγχο της πρόσβασης στο δίκτυο. Τέτοιοι μηχανισμοί είναι, οι IP Filtering Firewalls, οι Application/Proxy Gateways και οι Access Lists(CiscoIOS). Αυτοί οι μηχανισμοί διαβαθμίζονται από πολύ απλούς σε αρκετά πολύπλοκους και οι βασικές αρχές λειτουργίας τους περιέχουν:

- Περιορισμούς στη παροχή πρόσβασης προς τα έξω ή προς τα έσω.

Μέσω των περιορισμών στη παροχή της πρόσβασης ουσιαστικά ελέγχεται σε ποιόν χρήστη ή host θα δοθεί παροχή χρήσης TCP υπηρεσίας όπως το TELNET ή το FTP.Αυτοί οι περιορισμοί τίθονται ανά χρήστη ή host.

- Φιλτράρισμα Πακέτων

Στο φιλτράρισμα πακέτων εξετάζονται τα datagrams που προορίζονται για κάποιο σύστημα. Το φιλτράρισμα πακέτων πραγματοποιείται με βάση το host. Το σύστημα πετάει τα datagrams που έχουν απορριφθεί από τους περιορισμούς. Αυτή η λογισμικού τύπου τεχνική φιλτράρει τα datagrams σύμφωνα με το πρωτόκολλο (TCP,UDP,IP,ICMP) ,τη διεύθυνση της προέλευσης και του προορισμού και τις UDP ή TCP πόρτες προορισμού.

3.2) Ασφάλεια ασυρμάτων δικτύων

Τα πλεονεκτήματα που προκύπτουν από τις τεχνολογίες WLAN είναι αναμφίβολα πολλά, με σημαντικότερο, στις περισσότερες περιπτώσεις, την ευελιξία που παρέχουν. Παρόλα αυτά, ο τρόπος με τον οποίο πραγματοποιείται η διακίνηση της πληροφορίας παρουσιάζει κάποιες αδυναμίες, κυρίως όσον αφορά στην ασφάλεια. Για να το θέσουμε με περισσότερη ειλικρίνεια, ΝΑΙ, υπάρχουν προβλήματα ασφαλείας στα ασύρματα δίκτυα και δικαίως ανησυχούν οι καχύποπτοι χρήστες! Στο πρότυπο 802.11 b, τα δεδομένα εκπέμπονται, όπως αναφέρθηκε, στη φασματική περιοχή των 2,4GHz, σε συχνότητες που μπορούν εύκολα να διαπεράσουν κάποια τυπική τοιχοποιία και μεταλλική κατασκευή. Το γεγονός ότι τα δεδομένα που διακινούνται ανά πάσα στιγμή στο δίκτυο, διαχέονται "ελεύθερα" στον περιβάλλοντα χώρο, επιτρέπει σε κάθε περαστικό, με ένα laptop να συνδεθεί στο δίκτυο και να το χρησιμοποιήσει με καλούς ή κακούς σκοπούς. Γενικά, οι "επιθέσει" που είναι πιθανόν να δεχτεί ένα ασύρματο δίκτυο, χωρίζονται σε δύο βασικούς τύπους. Ο πρώτος αποτελείται από επιθέσεις που έχουν βασικό σκοπό την υποκλοπή των πληροφοριών που διακινούνται. Στόχος των παραπάνω επιθέσεων είναι τις περισσότερες φορές τα εταιρικά δίκτυα, στα οποία ανταλλάσσονται αρκετά "ευαίσθητες", τόσο για την εταιρεία όσο και τους ανταγωνιστές της, πληροφορίες. Ο δεύτερος τύπος περιλαμβάνει επιθέσεις, με τις οποίες ένας "κακόβουλος" επισκέπτης προσπαθεί να αποκτήσει πρόσβαση και να χρησιμοποιήσει "προσωρινά" ένα ασύρματο δίκτυο. Δεδομένων των παραπάνω κινδύνων και έχοντας ως στόχο την αύξηση της ασφάλειας των ασύρματων δικτύων, το IEEE έχει ενσωματώσει στο πρότυπο 802.11 μεθόδους, που συντελούν στην αύξηση της ασφάλειας του ασυρμάτου δικτύου (Basic Industry Standard Security).

3.3) Η Προστασία του Firewall

Το Firewall είναι η μόνη ασπίδα προστασίας του εσωτερικού δικτύου από εξωτερικές απειλές. Η καλύτερη δυνατή προστασία που μπορούμε να πετύχουμε, ακόμα και εάν έχουμε υλοποιήσει άριστα την βέλτιστη πολιτική ασφαλείας, περιορίζεται στο βαθμό ασφάλειας που παρέχει το Firewall σε επιθέσεις εναντίον του ιδίου του Firewall. Για παράδειγμα εάν είναι δυνατό να συνδεθεί ο οποιοσδήποτε στο firewall με την υπηρεσία telnet τότε το δίκτυο που προστατεύει δεν είναι καθόλου ασφαλές. Για αυτό τον λόγο πρέπει να περιορίζονται στο ελάχιστο οι υπηρεσίες που παρέχει στο δίκτυο το ίδιο το firewall. Φυσικά η βέλτιστη επιλογή είναι να μην είναι ενεργή καμία υπηρεσία στο firewall. Το αρχείο που ελέγχει τους δαίμονες των υπηρεσιών, είναι το /etc/inetd.conf . Τέλος το Firewall δεν πρέπει να διασυνδέεται με το Internet πριν ολοκληρωθεί η ρύθμιση του, διότι είναι πιθανό να δεχτεί μια επίθεση πριν ολοκληρωθεί η ρύθμιση του.Ενας “firewall” υπολογιστής μπορεί να "ακουμπά" αμφότερα, το προστατευόμενο δίκτυο και το Internet. Το προστατευόμενο δίκτυο δεν μπορεί να προσεγγίσει το Internet, ούτε το Internet μπορεί να προσεγγίσει το προστατευόμενο δίκτυο. Για κάποιον που θέλει να επικοινωνήσει με το Internet μέσα από το προστατευόμενο δίκτυο, πρέπει να κάνει σύνδεση telnet στο firewall, και να χρησιμοποιήσει το Internet από εκεί. Η απλούστερη μορφή ενός firewall είναι ένα διπλό σπιτικό σύστημα (ένα σύστημα με δύο συνδέσεις δικτύου). ΕΑΝ ΜΠΟΡΕΙΤΕ ΝΑ ΕΜΠΙΣΤΕΥΤΗΤΕ ΟΛΟΥΣ ΤΟΥΣ ΧΡΗΣΤΕΣ ΣΑΣ μπορείτε απλά να στήσετε ένα Linux (μεταγλωττίστε το πυρήνα με IP Forwarding απενεργοποιημένο) και δώστε όλους τους λογαριασμούς πάνω του. Θα μπορούν να κάνουν σύνδεση στο σύστημα (login), telnet, FTP, να διαβάζουν e-mail, και να χρησιμοποιούν ό,τι έχετε εφοδιάσει. Με αυτό το στήσιμο, ο μόνος υπολογιστής στο προσωπικό σας δίκτυο που θα γνωρίζει τα πάντα σχετικά με τον έξω κόσμο είναι ο firewall. Το άλλο σύστημα στο προστατευόμενο δίκτυο σας, δεν χρειάζονται καν να ορίσετε το συνήθες δρομολόγιο (default route).

Το πρόβλημα με τους firewalls φίλτραρίσματος είναι ότι παρεμποδίζουν τη πρόσβαση στο δίκτυο από το Internet. Μόνο υπηρεσίες στα συστήματα που έχουν περάσει το φιλτράρισμα μπορεί να παρεχθεί πρόσβαση. Με τους διακομιστές εξουσιοδότησης οι χρήστες μπορούν να συνδεθούν (login) στο firewall, έχοντας πρόσβαση σε κάθε σύστημα μέσα στο προσωπικό σας δίκτυο, όπου έχουν πρόσβαση. Επίσης, νέοι τύποι από πελάτες δικτύων (network clients) και διακομιστών έρχονται σχεδόν κάθε μέρα. Όταν αυτό συμβεί θα πρέπει να βρείτε νέους τρόπους για να επιτρέψετε την ελεγχόμενη πρόσβαση πριν αυτές οι υπηρεσίες μπορούν να χρημοποιηθούν.

3.3.1) Τύποι των Firewalls

Υπάρχουν δύο τύποι firewalls

1. IP Firewalls Φιλτραρίσματος (filtering firewalls) - μπλοκάρουν τα πάντα αλλά σε επιλεγμένα κυκλοφοριακά δίκτυα.
2. Διακομιστές Εξουσιοδότησης (Proxy Servers) - αυτοί κάνουν τη δικτυακή σύνδεση για εσάς.

1.IP Firewalls Φιλτραρίσματος

Ο IP firewall φιλτραρίσματος δουλεύει σαν ισοσταθμιστής πακέτων. Έχει σχεδιαστεί για να ελέγχει τη ροή από πακέτα βασισμένα στη πηγαία (προορισμένη) πύλη και στις πληροφοριές που περιέχει κάθε πακέτο. Αυτός ο firewall είναι πολύ ασφαλής αλλά στερήται οποιασδήποτε είδους χρήσιμη εγγραφή συμβάντων. Μπορεί να μπλοκάρει το κόσμο από τη πρόσβαση στο προσωπικό σας δίκτυο αλλά δεν θα αναφέρει ποιός προσπέλασε το δημόσιο σύστημα ή ποιος το Internet από μέσα. Τα Firewalls φιλτραρίσματος είναι απόλυτα φίλτρα. Ακόμη και αν θέλετε να δώσετε πρόσβαση απ' έξω από τους προσωπικούς σας διακομιστές δεν μπορείτε να το κάνετε χωρίς να δώσετε στους πάντες πρόσβαση στους διακομιστές. Το Linux περιλαμβάνει το πακέτο φιλτραρίσματος στο πυρήνα από την έκδοση 1.3.χ

- ***Πλεονεκτήματα των IP Filtering Firewalls***

1. Εύκολη υλοποίηση, λόγο των ενσωματωμένων δυνατοτήτων φιλτραρίσματος πακέτων στους σημερινούς δρομολογητές.

2. Επίτευξη μεγάλων ταχυτήτων για περιπτώσεις απλών κανόνων φιλτραρίσματος.

3. Παρέχει προστασία χωρίς να δυσκολεύει την χρήση του δικτύου από τον χρήστη. (Transparent security)

- ***Μειονεκτήματα των IP Filtering Firewalls***

1. Επιτρέπουν την συλλογή χρήσιμης πληροφορίας για την μηχανή του χρήστη (π.χ. IP διεύθυνση), χρησιμοποιώντας packet sniffers.

2. Δεν είναι αρκετά ευέλικτα και γίνονται δύσχρηστα στις περιπτώσεις πολλών υποδικτύων (subnets) με διαφορετικά επίπεδα ασφάλειας

3. Δεν παρέχουν δυνατότητα αναγνώρισης του χρήστη και για αυτό δεν μπορούν να επιτρέψουν ή να απαγορεύσουν την πρόσβαση σε υπηρεσίες ανάλογα με το επίπεδο προνομίων του χρήστη.

4. Δεν παρέχει πληροφορίες σχετικά με την χρήση της κάθε υπηρεσίας (application logging)

2. Διακομιστές Εξουσιοδότησης

Οι διακομιστές εξουσιοδότησης επιτρέπουν την έμμεση πρόσβαση στο Internet μέσω του firewall. Καλλίτερο παράδειγμα πως δουλεύει είναι, ένα άτομο κάνει telnet σε ένα σύστημα και μετά άλλο telnet από εκεί προς κάπου αλλού. Μόνο με τους διακομιστές εξουσιοδότησης η λειτουργία είναι αυτόματη. Όταν συνδεθείτε σε ένα διακομιστή εξουσιοδότησης με το δικό σας πελατειακό λογισμικό (client software) ο διακομιστής ξεκινά το δικό του πελατειακό (εξουσιοδοτούμενο) λογισμικό και μεταβιβάζει τα δεδομένα σας. Επειδή οι διακομιστές εξουσιοδότησης αναπαράγουν όλες τις επικοινωνίες μπορούν να καταγράφουν ό,τι κάνουν. Το καλό με τους διακομιστές εξουσιοδότησης είναι ότι, είναι εντελώς ασφαλείς, όταν ρυθμιστούν σωστά. Δεν θα επιτρέψουν σε κάποιον να περάσει από μέσα τους. Δεν υπάρχουν άμεσα IP δρομολόγια.

Application/Proxy GateWays

Τα application gateways παρουσιάζονται σαν μια λύση που παρέχει ακόμη μεγαλύτερη ασφάλεια. Το εσωτερικό δίκτυο ουσιαστικά δεν έχει διασύνδεση με το υπόλοιπο Internet αφού τα proxies για κανένα λόγο δεν μπορούν να προωθήσουν IP πακέτα.

Ο χρήστης για να χρησιμοποιήσει κάποια υπηρεσία του δικτύου θα πρέπει να συνδεθεί πρώτα με το proxy. Το proxy στην συνέχεια θα πραγματοποιήσει εξακρίβωση της ταυτότητας τους (authentication) και εάν επιτρέπεται η χρήση της υπηρεσίας από τον χρήστη, θα πραγματοποιήσει την σύνδεση με την υπηρεσία και τον εξυπηρέτη που ζητήθηκε και θα προωθεί την πληροφορία από και προς τις δυο κατευθύνσεις. Όπως φαίνεται και στο Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε. η πληροφορία που μεταφέρει ένα proxy δεν έχει την μορφή IP πακέτων, αλλά πακέτα μιας ροής δεδομένων ανάμεσα στην εφαρμογή του χρήστη και τον απομακρυσμένο εξυπηρέτη.

Η λειτουργία του proxy σε επίπεδο εφαρμογής(Application), απαιτεί να γνωρίζει το πρωτόκολλο κάθε υπηρεσίας (ftp,http,finger,κ.λ.π.) που πρέπει να παρέχει για να συνομιλεί με την εφαρμογή του χρήστη και του

εξυπηρέτη. Η έλλειψη της απευθείας σύνδεσης με το Internet κάνει δυνατή την χρήση διευθύνσεων από τον χώρο διευθύνσεων για ιδιωτικά δίκτυα.

- ***Πλεονεκτήματα των Application Gateways***

1. Η έλλειψη της απευθείας σύνδεσης του προστατευόμενου δικτύου από το Internet, αποκρύπτει πληροφορίες για την δομή το δικτύου που θα μπορούσαν να φανούν χρήσιμες σε ένα επίδοξο εισβολέα.

2. Λόγο της πλήρης κατανόησης του πρωτοκόλλου μιας εφαρμογής που πρέπει να έχει ένας proxy μπορεί να παρέχει ασφάλεια σε επίπεδο εφαρμογής, ελέγχοντας το είδος των δεδομένων που μεταφέρονται.

3. Είναι δυνατή η συλλογή πληροφοριών μεγάλης λεπτομέρειας, σχετικά με την χρήση των επιμέρους εφαρμογών.

- ***Μειονεκτήματα των Application Gateways***

1. Απαιτούν ειδική ρύθμιση από την πλευρά των εφαρμογών του χρήστη, ώστε να χρησιμοποιούν το proxy.

2. Η διαδικασία εξακρίβωσης της ταυτότητας του χρήστη πρέπει να επαναλαμβάνετε για κάθε μια εφαρμογή που ξεκινάει.

3. Παρουσιάζει έλλειψη ευελιξίας προσαρμογής στις νέες υπηρεσίες που παρουσιάζονται. Για κάθε νέα υπηρεσία πρέπει να γραφεί το λογισμικό που θα την υποστηρίξει στο proxy, διαφορετικά δεν είναι δυνατή η χρησιμοποίηση της.

3.4) Encryption (Κρυπτογραφηση)

Σε νομικό και κοινωνικό επίπεδο, τίθεται ζήτημα προστασίας του απορρήτου σε όλες τις εκδοχές δικτυακής συναλλαγής (email, εμπορικές συναλλαγές, τραπεζικό και ιατρικό απόρρητο) και γενικότερα ζήτημα προστασίας προσωπικών δεδομένων του κάθε χρήστη του Internet.

Η κρυπτογράφηση έρχεται να εξασφαλίσει το απόρρητο των προσωπικών πληροφοριών. Πρόκειται για μια επιστήμη που βασίζεται στα μαθηματικά για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων. Οι μέθοδοι κρυπτογράφησης καθιστούν τα ευαίσθητα προσωπικά δεδομένα προσβάσιμα μόνο από όσους είναι κατάλληλα εξουσιοδοτημένοι. Εξασφαλίζουν έτσι το απόρρητο στις ψηφιακές επικοινωνίες αλλά και στην αποθήκευση ευαίσθητων πληροφοριών. Το αρχικό μήνυμα ονομάζεται απλό κείμενο (plaintext), ενώ το ακατάληπτο μήνυμα που προκύπτει από την κρυπτογράφηση του απλού κειμένου ονομάζεται κρυπτογράφημα (ciphertext).

Αποκρυπτογράφηση είναι η ανάκτηση του απλού κειμένου από το κρυπτογράφημα με την εφαρμογή αντίστροφου αλγορίθμου. Η κρυπτογραφημένη επικοινωνία είναι αποτελεσματική, όταν μόνο τα άτομα που συμμετέχουν σε αυτήν μπορούν να ανακτήσουν το περιεχόμενο του αρχικού μηνύματος. Η κρυπτογραφία δεν πρέπει να συγχέεται με την κρυπτανάλυση, που ορίζεται ως η επιστήμη για την ανάλυση και αποκωδικοποίηση κωδικοποιημένων πληροφοριών χωρίς τη χρήση του αντίστροφου αλγορίθμου κρυπτογράφησης.

Ο αλγόριθμος κρυπτογράφησης είναι μια μαθηματική συνάρτηση που χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση πληροφοριών. Όσο αυξάνεται ο βαθμός πολυπλοκότητας του αλγορίθμου, τόσο μειώνεται η πιθανότητα να τον προσπελάσει κάποιος. Ο αλγόριθμος κρυπτογράφησης λειτουργεί σε συνδυασμό με ένα κλειδί (key), για την κρυπτογράφηση του απλού κειμένου. Το ίδιο απλό κείμενο κωδικοποιείται σε διαφορετικά κρυπτογραφήματα όταν χρησιμοποιούνται διαφορετικά κλειδιά.

3.5) Μέθοδοι κρυπτογράφησης

Υπαρχουν δυο μεθοδοι κρυπτογραφησης:η συμμετρικη και η ασυμμετρη.Ποιο αναλυτικα:

3.5.1) Συμμετρική κρυπτογράφηση

Στη συμμετρική κρυπτογράφηση χρησιμοποιείται το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση. Το κλειδί αυτό θα πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη και, κατά συνέπεια, απαιτείται κάποιο ασφαλές μέσο για τη μετάδοσή του, όπως μια προσωπική συνάντηση, κατά την οποία θα συμφωνηθεί το κλειδί που θα χρησιμοποιείται. Αν κάτι τέτοιο δεν είναι εφικτό, η συμμετρική κρυπτογραφία είναι αναποτελεσματική.

Υπάρχουν αρκετοί αλγόριθμοι που ανήκουν στην κατηγορία αυτή, με πιο γνωστό τον Data Encryption Standard (DES), ο οποίος αναπτύχθηκε αρχικά από την IBM και υιοθετήθηκε το 1977 από την κυβέρνηση των Ηνωμένων Πολιτειών ως το επίσημο πρότυπο κρυπτογράφησης απόρρητων πληροφοριών.

Τα συστήματα συμμετρικής κρυπτογράφησης προϋποθέτουν την ύπαρξη ενός ασφαλούς καναλιού για την ανταλλαγή των μυστικών κλειδιών. Τέτοια συστήματα έχουν αναπτυχθεί και ήδη χρησιμοποιούνται, με πιο διαδεδομένο το σύστημα Kerberos, του MIT (Massachusetts Institute of Technology).

3.5.2) Ασύμμετρη κρυπτογράφηση

Στην ασύμμετρη κρυπτογράφηση, χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση: το δημόσιο (public) και το ιδιωτικό (private) κλειδί αντίστοιχα. Τα κλειδιά αυτά δημιουργούνται με τρόπο ώστε να έχουν τις εξής ιδιότητες:

Μήνυμα κρυπτογραφημένο με το δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί και αντίστροφα

Το ένα κλειδί δεν μπορεί να προκύψει από το άλλο με απλό τρόπο

Η βασική αυτή αρχή της κρυπτογραφίας δημόσιου κλειδιού διατυπώθηκε το 1976 από τους Diffie και Hellman, ενώ το 1977 οι Rivest, Shamir και Adleman, βασιζόμενοι σε αρχές της θεωρίας των πεπερασμένων πεδίων, δημιούργησαν το κρυπτοσύστημα RSA, την πρώτη υλοποίηση συστήματος κρυπτογραφίας δημόσιου κλειδιού.

Προκειμένου να επιτευχθεί η επικοινωνία με χρήση ασύμμετρης κρυπτογραφίας, ο κάθε χρήστης πρέπει να διαθέτει τα δικά του κλειδιά, ένα δημόσιο και ένα ιδιωτικό. Ο αποστολέας ενός μηνύματος πρέπει να γνωρίζει το δημόσιο κλειδί του παραλήπτη και να κρυπτογραφήσει το μήνυμα με αυτό. Ο παραλήπτης αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί.

Το δημόσιο κλειδί δεν αποτελεί μυστική πληροφορία, συνεπώς μπορεί να μεταδοθεί χωρίς την απαίτηση ύπαρξης ασφαλούς μέσου. Το

ιδιωτικό κλειδί χρησιμοποιείται μόνο από τον ιδιοκτήτη του και δεν μεταδίδεται ποτέ. Όταν ένα μήνυμα έχει κρυπτογραφηθεί με το δημόσιο κλειδί κάποιου χρήστη, μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό του κλειδί. Και επειδή μόνο ο ίδιος ο χρήστης γνωρίζει το ιδιωτικό του κλειδί, μόνο αυτός μπορεί να αποκρυπτογραφήσει τα μηνύματα που απευθύνονται σε αυτόν. Ούτε καν το δημόσιο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση δεν μπορεί να αποκωδικοποιήσει το μήνυμα, γι' αυτό και η γνώση του δημόσιου κλειδιού από τρίτους δεν αποτελεί πρόβλημα.

Η ασύμμετρη κρυπτογράφηση παρέχει μεγαλύτερη ασφάλεια από ό,τι η συμμετρική. Έχει όμως το μειονέκτημα ότι οι αλγόριθμοι που χρησιμοποιεί είναι πολύ βραδύτεροι από τους αντίστοιχους της συμμετρικής

3.5.3) Υποδομη δημοσιου κλειδιου και κρυπτογραφηση στη στη πραξη

Η Υποδομή Δημόσιου Κλειδιού
(Public Key Infrastructure PKI
αποτελεί ένα συνδυασμό λογισμικού, τεχνολογιών κρυπτογραφίας και υπηρεσιών, ο οποίος πιστοποιεί την εγκυρότητα του κάθε φυσικού προσώπου που εμπλέκεται σε μια συναλλαγή στο Διαδίκτυο, και παράλληλα προστατεύει την ασφάλεια της συναλλαγής.

Το PKI ενσωματώνει ψηφιακά πιστοποιητικά, κρυπτογραφία δημόσιου κλειδιού και αρχές πιστοποίησης σε ένα ασφαλές αρχιτεκτονικό σχήμα. Μια τυπική υλοποίηση του PKI περιλαμβάνει την παροχή ψηφιακών πιστοποιητικών σε χρήστες, εξυπηρετητές (servers) και λογισμικό χρηστών. Παράλληλα προσφέρει σειρά εργαλείων για τη διαχείριση, ανανέωση και ανάκληση των πιστοποιητικών.

Οι βασικές λειτουργίες/υπηρεσίες των Υποδομών Δημόσιου Κλειδιού είναι οι εξής:

Εμπιστευτικότητα (Confidentiality): Πρόκειται για την προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη πρόσβαση ή γνωστοποίησή τους. Η υπηρεσία αυτή υλοποιείται μέσω μηχανισμών ελέγχου

πρόσβασης στην περίπτωση αποθήκευσης δεδομένων και μέσω κωδικοποίησης κατά την αποστολή τους. Η Υποδομή Δημόσιου Κλειδιού παρέχει κωδικοποίηση, αφού οι μηχανισμοί ελέγχου πρόσβασης υλοποιούνται κατά βάση από το συνδυασμό μεθόδων πιστοποίησης (authentication) και εξουσιοδότησης (authorization).

Ακεραιότητα (Integrity): Είναι η προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη τροποποίηση ή αντικατάστασή τους. Παρέχεται από μηχανισμούς κρυπτογραφίας όπως οι ηλεκτρονικές υπογραφές.

Μη Άρνηση Αποδοχής (Non-Repudiation): Η Μη Άρνηση Αποδοχής συνδυάζει τις υπηρεσίες της Πιστοποίησης και της Ακεραιότητας. Ο αποστολέας δεδομένων δεν μπορεί να αρνηθεί ότι δημιούργησε και απέστειλε το μήνυμα. Η ασύμμετρη κρυπτογραφία παρέχει ηλεκτρονικές υπογραφές, κατά συνέπεια μόνο ο αποστολέας του μηνύματος θα μπορούσε να κατέχει τη συγκεκριμένη υπογραφή. Με αυτόν τον τρόπο, ο οποιοσδήποτε, και φυσικά ο παραλήπτης του μηνύματος, μπορεί να επιβεβαιώσει την ηλεκτρονική υπογραφή του αποστολέα.

Πιστοποίηση (Authentication): Πρόκειται για την επιβεβαίωση της ταυτότητας ενός ατόμου ή της πηγής αποστολής των πληροφοριών. Κάθε χρήστης που επιθυμεί να επιβεβαιώσει την ταυτότητα ενός άλλου προσώπου ή εξυπηρετητή με τον οποίο επικοινωνεί, βασίζεται στην πιστοποίηση. Οι παραδοσιακές μέθοδοι πιστοποίησης είναι οι εξής:

- Με κάποιον κωδικό που γνωρίζουμε, όπως το PIN μιας τραπεζικής κάρτας ή το password ενός λογαριασμού
- Με κάποιο αντικείμενο που έχουμε στην ιδιοκτησία μας, λόγου χάρη το κλειδί μιας πόρτας ή μια τραπεζική κάρτα
- Με δακτυλικά αποτυπώματα, φωνή κ.λπ.

Το πιστοποιητικό (certificate) είναι ο τρόπος με τον οποίο η Υποδομή Δημόσιου Κλειδιού μεταδίδει τις τιμές των δημόσιων κλειδιών ή πληροφορίες που σχετίζονται με αυτά, ή και τα δύο. Η εκδότρια αρχή των πιστοποιητικών ονομάζεται Αρχή Πιστοποίησης (Certificate Authority - CA). Οι Αρχές Πιστοποίησης διασφαλίζουν τη δημοσίευση και τη διανομή των δημόσιων κλειδιών και λαμβάνουν το δημόσιο κλειδί του ενδιαφερόμενου χρήστη. Εάν ο χρήστης ενεργεί στη συγκεκριμένη περίπτωση ως ιδιώτης, θα πρέπει να παραχωρήσει όλα τα απαραίτητα στοιχεία που αποδεικνύουν την ταυτότητά του. Σε αντίθετη περίπτωση, ο χρήστης θεωρείται ότι ενεργεί εκ μέρους κάποιας επιχείρησης, οπότε οφείλει να παραχωρήσει όλες τις νομικές πληροφορίες που απαιτούνται για την αξιοπιστία και τη νόμιμη λειτουργία της.

Ουσιαστικά ένα ψηφιακό πιστοποιητικό αποτελεί μια ψηφιακά

υπογεγραμμένη δήλωση από μια αρχή πιστοποίησης, η οποία:

1. Προσδιορίζει την αρχή πιστοποίησης που το εξέδωσε
2. Περιέχει το όνομα και κάποιες άλλες πληροφορίες του εγγεγραμμένου
3. Περιέχει το δημόσιο κλειδί του εγγεγραμμένου, το οποίο είναι ψηφιακά υπογεγραμμένο από την αρχή πιστοποίησης που το εξέδωσε

Για την πιστοποίηση της ταυτότητας των συναλλασσομένων χρησιμοποιούνται τα πιστοποιητικά ασφαλείας, που επιπλέον εγγυώνται και την ασφάλεια ενός δικτυακού τόπου. Υπάρχουν δύο είδη πιστοποιητικών:

- Τα προσωπικά πιστοποιητικά, τα οποία αποτελούν ένα είδος εγγύησης ότι ο χρήστης είναι αυτός που δηλώνει ότι είναι. Σε αυτά καταχωρούνται προσωπικές πληροφορίες, όπως όνομα χρήστη και κωδικός πρόσβασης. Στη συνέχεια, οι πληροφορίες αυτές αποθηκεύονται σε ένα πιστοποιητικό, το οποίο χρησιμοποιείται όταν στέλνονται προσωπικές πληροφορίες σε ένα διακομιστή ελέγχου ταυτότητας που απαιτεί πιστοποιητικό. Επίσης, ένα προσωπικό πιστοποιητικό επιτρέπει στο χρήστη να λαμβάνει κρυπτογραφημένα μηνύματα από τους υπόλοιπους χρήστες.
- Τα πιστοποιητικά δικτυακών τόπων, τα οποία περιέχουν πληροφορίες που πιστοποιούν ότι η συγκεκριμένη ιστοσελίδα είναι γνήσια και ασφαλής. Αυτό διασφαλίζει ότι κανένα άλλο site δεν μπορεί να παρουσιαστεί με την ταυτότητα της γνήσιας, ασφαλούς τοποθεσίας. Επίσης, τα πιστοποιητικά δικτυακών τόπων χρονολογούνται κατά την έκδοσή τους. Όταν προσπαθείτε να συνδεθείτε με το website ενός οργανισμού, το πρόγραμμα ανάγνωσης επαληθεύει τη διεύθυνση Internet που είναι αποθηκευμένη στο πιστοποιητικό και ελέγχει την ημερομηνία λήξης του. Εάν οι πληροφορίες αυτές δεν είναι έγκυρες ή εάν έχει παρέλθει η ημερομηνία λήξης, εμφανίζεται προειδοποιητικό μήνυμα (Warning).

Έχουν αναπτυχθεί ή βρίσκονται υπό κατασκευή διάφορα πρωτόκολλα ασφαλείας που κάνουν χρήση των παραπάνω τεχνικών, όπως το SSL (Secure Sockets Layer), της Netscape, και το SET (Secure Electronic Transactions), που αναπτύχθηκε από τη Visa και τη MasterCard. Από αυτά σήμερα χρησιμοποιείται το SSL. Αρκετές ιστοσελίδες είναι εξοπλισμένες με προγράμματα που χρησιμοποιούν το πρωτόκολλο αυτό, αποτρέποντας έτσι τα μη εξουσιοδοτημένα πρόσωπα από την πρόσβασή τους σε δεδομένα που αποστέλλονται από και προς αυτές τις ιστοσελίδες. Τέτοια sites ονομάζονται "ασφαλή".

Οι πιο γνωστοί φυλλομετρητές ιστοσελίδων (browsers) υποστηρίζουν το πρωτόκολλο SSL και την κρυπτογράφηση που προσφέρει, ενώ ενημερώνουν το χρήστη ότι βρίσκεται σε ασφαλή τοποθεσία και μπορεί να στέλνει πληροφορίες ακίνδυνα. Με το πρωτόκολλο αυτό οι επικοινωνίες πραγματοποιούνται σε κωδικοποιημένη μορφή και επιπλέον γίνεται έλεγχος της αυθεντικότητας της ιστοσελίδας.

Η διαδικασία μιας ασφαλούς επικοινωνίας έχει ως εξής:

- Ο φυλλομετρητής συνδέεται με τον ασφαλή δικτυακό τόπο.
- Ο δικτυακός τόπος δηλώνει την ταυτότητά του, η οποία ελέγχεται με τα πιστοποιητικά που εκδίδονται από υπηρεσίες πιστοποίησης.
- Η ασφαλής ιστοσελίδα και ο browser συμφωνούν στη χρήση συγκεκριμένου κλειδιού/αλγορίθμου που χρησιμοποιείται για την κρυπτογράφηση της υπόλοιπης επικοινωνίας.
- Τα δεδομένα που διακινούνται είναι κρυπτογραφημένα με το κλειδί/αλγόριθμο που συμφωνήθηκε στο προηγούμενο βήμα.

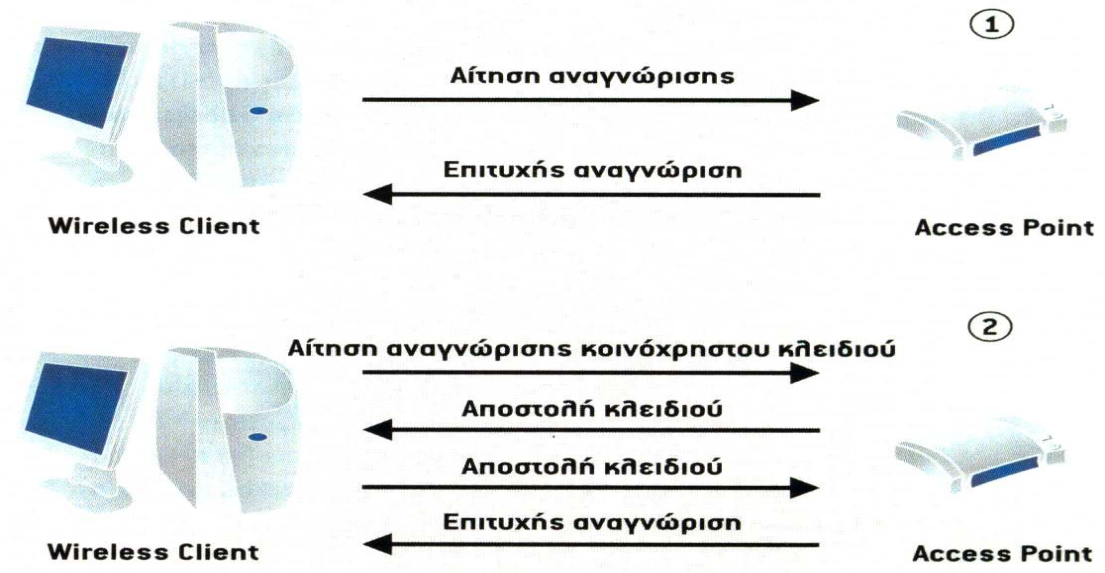
Η κρυπτογράφηση γίνεται με χρήση αλγορίθμου 40bit ή 128bit. Εάν έχει χρησιμοποιηθεί κρυπτογράφηση 40bit, τότε για να αποκρυπτογραφήσει κανείς τα δεδομένα που ανταλλάχθηκαν, θα πρέπει να δοκιμάσει περίπου 240 διαφορετικά κλειδιά, ενώ, εάν έχει χρησιμοποιηθεί κρυπτογράφηση 128bit, τότε θα πρέπει να δοκιμάσει περίπου 2.128 διαφορετικά κλειδιά. Με τη χρήση μεγάλης υπολογιστικής ισχύος, η αποκρυπτογράφηση του κλειδιού των 40bit μπορεί να επιτευχθεί σε μερικές ημέρες, ενώ η αποκρυπτογράφηση του κλειδιού των 128bit, με τα σημερινά δεδομένα, είναι πρακτικά αδύνατη. Θα πρέπει να σημειωθεί ότι απαγορεύεται από τη νομοθεσία των ΗΠΑ η εξαγωγή και χρήση προγραμμάτων που υποστηρίζουν κωδικοποίηση 128bit εκτός των Ηνωμένων Πολιτειών και του Καναδά.

Στο πλαίσιο των προσπαθειών που καταβάλλονται για την ανάπτυξη των ηλεκτρονικών συναλλαγών, έχει επιτραπεί η χρήση της τεχνολογίας SGC (Server Gated Cryptography) ή International Step-Up Encryption, που αποτελεί επέκταση του πρωτοκόλλου SSL, από πιστωτικά ιδρύματα και άλλων χωρών. Η επέκταση αυτή επιτρέπει στα πιστωτικά ιδρύματα, εφόσον διαθέτουν το κατάλληλο πιστοποιητικό, να επικοινωνούν με τους πελάτες τους με κωδικοποίηση 128bit

3.6) WEP (Wired Equivalent Privacy)

Η κρυπτογράφηση για τα ασύρματα δίκτυα γίνεται μέσω του WEP (Wired Equivalent Privacy). Το WEP μεταδίδει κρυπτογραφημένα τα

μηνύματα μέσω των ραδιοκυμάτων. Το WEP χρησιμοποιεί κρυπτογράφηση των 128-bit. Αυτό σημαίνει ότι μπορούμε να ορίσουμε ένα κλειδί μέχρι 13 χαρακτήρες. Μπορείτε να ορίσετε το κλειδί από το configuration του AP ή του router. Βέβαια είναι αυτονόητο να πούμε ότι αν η συσκευή σας υποστηρίζει 256-bit κρυπτογράφηση (26 χαρακτήρες) παρέχει σε σας μεγαλύτερη ασφάλεια. Παρόλα αυτά το WEP δεν είναι πλέον και τόσο ασφαλές. Υπάρχουν πολλά εργαλεία τα οποία μπορούν να παραβιάσουν την κρυπτογράφηση που σας παρέχει το WEP. Δύο τέτοια προγράμματα είναι τα Aircrack και Airsnort. Το WEP έχει ήδη παραβιαστεί καθώς με τον χείριστο τρόπο (brute force) χρειάζονται 256^6 πακέτα, ενώ για το WEP 128-bit με τον χείριστο τρόπο (brute force) απαιτούνται 256^32 πακέτα.
Έτσι η χρήση του WEP παρέχει μια ψευδαίσθηση ασφαλείας, που από μόνη της μπορεί να είναι επικίνδυνη. Αν κρυπτογραφήσουμε μια σύνδεση γίνεται πιο δύσκολο για ένα νέο κόμβο να συνδεθεί, και το key του καναλιού θα πρέπει να διανεμηθεί ή να γίνει public όπως και να έχει (άρα εφ' όσον θα έχει ο καθένας δικαίωμα να έχει το κλειδί, το link θ α μπορεί να αποκρυπτογραφηθεί από τον καθένα).
Αφετέρου δεν μπορούμε να εγγυηθούμε ότι τα δεδομένα δε θα δρομολογηθούν σε μη κρυπτογραφημένα links, ή ότι οι ιδιοκτήτες των nodes δεν κάνουν sniffing στα δεδομένα που δρομολογούν.



Στην εικονα 1 το WEP είναι απενεργοποιημενο ενώ στην εικονα 2 ενεργοποιημενο

3.7) WPA (Wi-Fi Protected Access).

Μια βελτίωση για το WEP είναι το Το WPA βελτιώνει το WEP σε δύο τομείς: Βελτιώνει την κρυπτογράφηση με το πρωτόκολλο TKIP (Temporal Key Integrity Protocol) και την αυθεντικότητα του χρήστη μέσω του EAP (extensible authentication protocol).

Οι *δυνατότητες ασφαλείας WPA περιγραφονται παρακατω:*

- ***Έλεγχος ταυτότητας WPA***

Απαιτείται έλεγχος ταυτότητας 802.1x στο πρότυπο WPA. Ο έλεγχος ταυτότητας 802.1x είναι προαιρετικός στο πρότυπο 802.11.

Για περιβάλλοντα που δεν διαθέτουν υποδομή RADIUS (Remote Authentication Dial-In User Service), το πρότυπο WPA υποστηρίζει τη χρήση κλειδιού προηγούμενης κοινής χρήσης. Για περιβάλλοντα με υποδομή RADIUS, υποστηρίζεται το πρωτόκολλο EAP (Extensible Authentication Protocol) και η υπηρεσία RADIUS.

- ***Διαχείριση κλειδιών WPA***

Με το πρότυπο 802.1x, η νέα αντιστοίχιση κλειδιών κρυπτογράφησης μοναδικής διανομής είναι προαιρετική. Επιπλέον, τα πρότυπα 802.11 και 802.1x δεν παρέχουν μηχανισμό αλλαγής του κλειδιού καθολικής κρυπτογράφησης που χρησιμοποιείται για κυκλοφορία πολλαπλής διανομής και ευρείας μετάδοσης. Με το πρότυπο WPA, απαιτείται νέα αντιστοίχιση κλειδιών κρυπτογράφησης μοναδικής διανομής και καθολικής κρυπτογράφησης. Για το κλειδί κρυπτογράφησης μοναδικής διανομής, το πρωτόκολλο TKIP (Temporal Key Integrity Protocol) αλλάζει το κλειδί για κάθε πλαίσιο και η αλλαγή συγχρονίζεται μεταξύ του προγράμματος-πελάτη ασύρματου δικτύου και του σημείου ασύρματης πρόσβασης. Για το κλειδί καθολικής κρυπτογράφησης, το πρότυπο WPA περιλαμβάνει μια υπηρεσία για το σημείο ασύρματης πρόσβασης, ώστε να κοινοποιηθεί το κλειδί που έχει αλλάξει στα συνδεδεμένα προγράμματα-πελάτες ασύρματου δικτύου.

- ***Πρωτόκολλο TKIP (Temporal Key Integrity Protocol)***

Για το πρότυπο 802.11, η κρυπτογράφηση WEP (Wired Equivalent Privacy) είναι προαιρετική. Για το πρότυπο WPA, απαιτείται η κρυπτογράφηση με τη χρήση του πρωτοκόλλου TKIP. Το πρωτόκολλο TKIP αντικαθιστά το πρότυπο WEP με έναν νέο αλγόριθμο κρυπτογράφησης, ο οποίος είναι ισχυρότερος από τον αλγόριθμο WEP αλλά χρησιμοποιεί τις υπηρεσίες υπολογισμού που εμφανίζονται στις

υπάρχουσες ασύρματες συσκευές για την εκτέλεση λειτουργιών κρυπτογράφησης. Το πρωτόκολλο TKIP εξασφαλίζει επίσης τα ακόλουθα:

- Την επαλήθευση της ρύθμισης παραμέτρων ασφαλείας μετά τον προσδιορισμό των κλειδιών κρυπτογράφησης.
- Τη συγχρονισμένη αλλαγή του κλειδιού κρυπτογράφησης μοναδικής διανομής για κάθε πλαίσιο.
- Τον προσδιορισμό μοναδικού κλειδιού έναρξης κρυπτογράφησης μοναδικής διανομής για κάθε έλεγχο ταυτότητας κλειδιού προηγούμενης κοινής χρήσης.

• ***Michael***

Με τα πρότυπα 802.11 και WEP, η ακεραιότητα δεδομένων παρέχεται από μια τιμή ελέγχου ακεραιότητας (integrity check value - ICV) που προσαρτάται σε φορτίο 802.11 και κρυπτογραφείται με το πρότυπο WEP. Ενώ η τιμή ICV είναι κρυπτογραφημένη, μπορείτε να χρησιμοποιήσετε κρυπτογραφική ανάλυση για να αλλάξετε bit στο κρυπτογραφημένο φορτίο και για να ενημερώσετε την κρυπτογραφημένη τιμή ICV, χωρίς να σας εντοπίσει ο παραλήπτης.

Με το πρότυπο WPA, μια μέθοδος που είναι γνωστή ως Michael καθορίζει έναν νέο αλγόριθμο που υπολογίζει έναν κώδικα ακεραιότητας μηνύματος (message integrity code - MIC) 8 byte, ο οποίος χρησιμοποιεί τις υπηρεσίες υπολογισμού που είναι διαθέσιμες σε υπάρχουσες ασύρματες συσκευές. Ο κώδικας MIC τοποθετείται μεταξύ του τμήματος δεδομένων του πλαισίου IEEE 802.11 και της τιμής ICV 4 byte. Το πεδίο MIC κρυπτογραφείται μαζί με τα δεδομένα πλαισίου και την τιμή ICV.

Η μέθοδος Michael παρέχει επίσης προστασία αναπαραγωγής. Χρησιμοποιείται ένας νέος μετρητής πλαισίου στο πλαίσιο IEEE 802.11 για την αποτροπή εισβολών αναπαραγωγής.

• ***Υποστήριξη AES***

Το πρότυπο WPA ορίζει τη χρήση του προτύπου AES (Advanced Encryption Standard) ως επιπλέον αντικατάσταση για την κρυπτογράφηση WEP. Επειδή ίσως να μην είναι δυνατή η προσθήκη υποστήριξης AES μέσα από ενημερωμένη έκδοση υλικολογισμικού σε υπάρχον ασύρματο εξοπλισμό, η υποστήριξη προτύπου AES είναι προαιρετική και εξαρτάται από την υποστήριξη που παρέχει ο προμηθευτής όσον αφορά προγράμματα οδήγησης.

3.8) WPA2

Το WPA2 είναι μια πιστοποίηση προϊόντος που είναι διαθέσιμη μέσω του Wi-Fi Alliance. Το WPA2 πιστοποιεί ότι ο ασύρματος εξοπλισμός είναι συμβατός με το πρότυπο IEEE 802.11i. Η πιστοποίηση προϊόντος WPA2 αντικαθιστά επίσημα το WEP (Wired Equivalent Privacy) και τις υπόλοιπες δυνατότητες ασφαλείας του αρχικού προτύπου IEEE 802.11. Ο στόχος της πιστοποίησης του WPA2 είναι να υποστηρίζει τις πρόσθετες υποχρεωτικές δυνατότητες ασφαλείας του προτύπου IEEE 802.11i οι οποίες δεν περιλαμβάνονται ακόμη σε προϊόντα που υποστηρίζουν WPA.

Η ενημερωμένη έκδοση του WPA2/WPS IE υποστηρίζει τις ακόλουθες δυνατότητες του WPA2:

- Το WPA2 Enterprise χρησιμοποιώντας τον έλεγχο ταυτότητας IEEE 802.1X και το WPA2 Personal που χρησιμοποιώντας ένα κλειδί προηγούμενης κοινής χρήσης (PSK).
- Τη δυνατότητα AES (Advanced Encryption Standard) χρησιμοποιώντας το Counter Mode-Cipher Block Chaining (CBC)-Message Authentication Code (MAC) Protocol (CCMP) το οποίο παρέχει εμπιστευτικότητα δεδομένων, έλεγχο ταυτότητας προέλευσης δεδομένων και ακεραιότητα δεδομένων για ασύρματα πλαίσια.
- Την προαιρετική χρήση της προσωρινής αποθήκευσης PMK (Pairwise Master Key) και της περιστασιακής προσωρινής αποθήκευσης PMK. Στην αποθήκευση PMK, οι υπολογιστές-πελάτες ασύρματου δικτύου και τα σημεία ασύρματης πρόσβασης κάνουν προσωρινή αποθήκευση των αποτελεσμάτων των ελέγχων ταυτότητας 802.1X. Επομένως, η πρόσβαση είναι πολύ ταχύτερη όταν ένας υπολογιστής-πελάτης ασύρματου δικτύου μετακινείται πίσω σε ένα σημείο ασύρματης πρόσβασης στο οποίο έχει γίνει ήδη έλεγχος ταυτότητας του υπολογιστή-πελάτη.
- Την προαιρετική χρήση του προκαταρκτικού ελέγχου ταυτότητας. Στον προκαταρκτικό έλεγχο ταυτότητας, ένας υπολογιστής-πελάτης ασύρματου δικτύου με WPA2 μπορεί να εκτελέσει έλεγχο ταυτότητας 802.1X με άλλα σημεία ασύρματης πρόσβασης που βρίσκονται μέσα στο εύρος του, όταν εξακολουθεί να είναι συνδεδεμένος στο τρέχον σημείο ασύρματης πρόσβασης

3.9) Αλλοι τροποι ασφαλειας

3.9.1)Αλλαγή SSID. Κάθε Access Point ή Router έχει ένα προκαθορισμένο SSID (Service Set Identifier). Όλα τα σημεία πρόσβασης σε ένα ασύρματο δίκτυο έχουν το ίδιο SSID και επιτρέπουν πρόσβαση στο δίκτυο μόνο στους ασύρματους κόμβους που το

διαθέτουν. Ο μηχανισμός αυτός, αν χρησιμοποιηθεί σωστά, παρέχει μία υποτυπώδη ασφάλεια στο δίκτυο, αφού απαιτείται η δήλωση στο λογισμικό της ασύρματης κάρτας του κωδικού SSIDH αλλαγή αυτή είναι αναγκαία ώστε να μη μπορεί ο καθένας να μπει μέσα στο δίκτυο (για να μπορέσει κάποιος να μπει στο δίκτυο είναι αναγκαίο να γνωρίζει το SSID). Αν αφήσουμε το προκαθορισμένο τότε είναι σχετικά εύκολο να βρει κάποιος αφού για τα προϊόντα των:Buffalo Technologies, Cisco, D-Link, Enterasys, Intermec, Lucent, and Proxim χρησημοποιήται ως προκαθορισμένο SSID το “any” ενώ μερικά άλλα είναι τα: "tsunami", "101", "RoamAbout Default Network Name", "Default SSID" και "Compaq". Όταν θα γίνει η αλλαγή καλό θα ήταν να χρησιμοποιήσουμε νούμερα & γράμματα μαζί και το όνομα να είναι όσο μεγαλύτερο μας επιτρέπεται. Επίσης σωστή κίνηση θα ήταν η αλλαγή του SSID να μην γίνει μια φορά αλλά ανά τακτά χρονικά διαστήματα. Επιπλέον πρέπει να ελέγξουμε αν η συσκευή μας έχει SSID boardcasting. Αν ναι τότε η απενεργοποίηση του είναι αναγκαία. Είναι μάλιστα εφικτό, ένας υπολογιστής να ρυθμιστεί με διαφορετικά SSID για την πρόσβαση σε διαφορετικά δίκτυα. Δυστυχώς, στα περισσότερα ασύρματα δίκτυα το SSID δεν αποτελεί δικλείδα ασφαλείας, άλλα ένα απλό αναγνωριστικό για την είσοδο στο δίκτυο. Εξάλλου, τα σημεία πρόσβασης μπορεί να είναι ρυθμισμένα να εκπέμπουν το SSID τους, συνεπώς οποιοσδήποτε πλησιάσει στην εμβέλεια τους, θα αποκτήσει πρόσβαση στο δίκτυο

3.9.2) MAC filtering. Ένας άλλος τρόπος για να ασφαλίσουμε κατά κάποιο τρόπο το δίκτυο μας είναι με ένα MAC filtering. Κάθε δικτυακή συσκευή έχει μια διεύθυνση. Αυτή η διεύθυνση αποτελείται από έξι δεκαεξαδικούς αριθμούς. Οι πρώτοι τρεις δεκαεξαδικοί αριθμοί είναι το ID του κατασκευαστή (manufacturers ID) και τα υπόλοιπα τρεις είναι ένας σειριακός αριθμός που έδωσε ο κατασκευαστής για καθεμία κάρτα. Ένα παράδειγμα διεύθυνσης MAC είναι αυτό: 00-53-45-00-00-00. Για να βρείτε μια MAC address σε windows πηγαίνετε σε γραμμή εντολών και γράψτε ipconfig /all και θα δείτε όλες τις διευθύνσεις MAC των δικτυακών σας συσκευών (αναφέρονται ως physical address ή φυσικές διευθύνσεις). Σε linux η εντολή είναι ifconfig. Κατόπιν πάμε στο configuration το AP η το router ώστε να βάλουμε τις MAC διευθύνσεις που θέλουμε να φιλτράρονται.Να προστέσω απλός ότι το MAC filtering δεν είναι κάτι το σπουδαίο ως προς την ασφάλεια. Αν κάποιος ξέρει μια MAC διεύθυνση μπορεί μέσα από τα windows χρησιμοποιόντας αυτό το πρόγραμμα και να αλλάξει την MAC διεύθυνση του. Σε linux: ifconfig ethx down hw ether 00:00:00:00:00:00 0.0.0.0 up .

3.10) Πολιτικές ασφάλειας

Το ποιο σημαντικό μέρος της ασφάλειας ενός δικτύου είναι η πολιτική που θα υλοποιηθεί μέσω των εργαλείων που υπάρχουν.Οι δύο βασικές τάσεις που υπάρχουν είναι:

- Ότι δεν απαγορεύεται ρητά, επιτρέπεται
- Ότι δεν επιτρέπεται, απαγορεύεται.

Οι πρώτη παρουσιάζει πολύ μεγαλύτερους κίνδυνους και απαιτεί πολύ μεγαλύτερη προσπάθεια για να διατηρείται η ασφάλεια του δικτύου σε υψηλά επίπεδα. Για αυτό το λόγο γενικά προτιμάται η δεύτερη πολιτική και είναι αυτή που θα παρουσιάσουμε στα παραδείγματα που θα ακολουθήσουν.

Στην πραγματικότητα μία πολιτική ασφάλειας πρέπει να είναι ιδιαίτερα μελετημένη, ούτε τελείως ανοιχτή (πολιτική 1), ούτε τελείως κλειστή (πολιτική 2), ώστε να μην αφαιρεί το σύνολο της λειτουργικότητας του από τους χρήστες.

Η πολιτική ασφάλειας ασύρματων δικτύων θα πρέπει να καλύπτει όλο τον ασύρματο εξοπλισμό, όπως σημεία πρόσβασης (access points), υπολογιστές με ασύρματες κάρτες, υπολογιστές παλάμης κ.λπ. που συνδέονται στο εταιρικό δίκτυο.

Συγκεκριμένα:

Όλα τα σημεία πρόσβασης (access points), σταθμοί βάσης (base stations), και ασύρματες κάρτες θα πρέπει να εγκρίνονται και να καταγράφονται από το Τμήμα Ασφάλειας της εταιρίας και να προέρχονται από κατασκευαστές που εγκρίνει το παραπάνω τμήμα.
Η σχεδίαση και υλοποίηση του δικτύου θα πρέπει να γίνεται προσεκτικά, έτσι ώστε να παρέχεται κάλυψη μόνο σε σημεία/περιοχές όπου χρειάζεται.

Όλες οι ασύρματες συσκευές θα πρέπει να λειτουργούν μέσω ενός VPN (Ιδεατό Ιδιωτικό Δίκτυο) για κρυπτογράφηση με προηγμένους μηχανισμούς ταυτοποίησης/αναγνωρισιμότητας.

ΚΕΦΑΛΑΙΟ 4^{Ο}

ΕΦΑΡΜΟΓΕΣ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

4.1) ΕΦΑΡΜΟΓΕΣ ΤΩΝ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

- ✓ Το πεδίο εφαρμογής των ασύρματων δικτύων είναι ιδιαίτερα ευρύ και, ουσιαστικό, περιέχει τόσο τις λειτουργίες που συναντώνται στα συμβατικά δίκτυα όσο και μία νέα γενιά εφαρμογών που προκύπτει από την απελευθέρωση από τα καλώδια. Το ασύρματο δίκτυο είναι ο φθηνότερος τρόπος για ευρυζωνικές υπηρεσίες. Αυτά που κάνουν οι χρήστες στο internet από το ασύρματο δίκτυο μπορούν να τα κάνουν καλύτερα. Δεν υπάρχει κάτι που να δουλεύει στο internet και να μη δουλεύει στο ασύρματο δίκτυο. Μερικές εφαρμογές είναι ανταλλαγή αρχείων, δικτυακά παιχνίδια (δράσης, στρατηγικής κ.τ.λ.), τηλεδιάσκεψη με όσους έχουν πρόσβαση, και πολλά άλλα. Για όσους επιμένουν να ενδιαφέρονται αποκλειστικά για το internet καλό είναι να ξέρουν πως υπάρχει η δυνατότητα να μοιράζουν μια DSL στα πρόσωπα που επιθυμούν (φίλους, συγγενείς κ.τ.λ.). Επίσης θα μπορούσατε να έχετε σύνδεση με τη παραπάνω DSL από τον φορητό σας ή το palm pc σας, προσαρμόζοντας σε αυτά (αν δεν υπάρχει ήδη) μια ασύρματη καρτούλα, σε οποιοδήποτε σημείο της πόλης όπου υπάρχει το σήμα κάποιου σημείου πρόσβασης. Πάντως το ασύρματο internet πιστεύω πως δεν θα αργήσει να φανεί.

Στη συνέχεια αναφέρουμε τις σημαντικότερες λειτουργίες και εφαρμογές των ασύρματων δικτύων.

- ✓ **Πρόσβαση στο Διαδίκτυο**. Ανεξάρτητα από το αν είναι φορητός ή επιτραπέζιος, κάθε υπολογιστής που εισέρχεται στο Δίκτυο μέσω του πρωτοκόλλου 802.11 γίνεται αυτόματα μέρος του απολαμβάνοντας τα ίδια ‘προνόμια’ με τα υπόλοιπα μέλη του. Κατ' αυτό τον τρόπο ο κάτοχός του μπορεί να αποκτήσει πρόσβαση στο Internet χωρίς να χρειάζεται να έχει modem ή κάποια άλλη κάρτα δικτύου.

- ✓ **Αυτόματος συγχρονισμός δεδομένων.** Ο χρήστης μπορεί να εισαγάγει ατοιχεία ατο notebook ή το PDA του και, μόλις πάει στο σπίτι ή στο γραφείο του, αυτά να ενημερωθούν αυτόματα με τον επιτραπέζιο υπολογιστή που διαθέτει. Κατ' αυτό τον τρόπο σε όλες τις συσκευές του χρήστη που παρέχουν υποστήριξη στο

πρωτόκολλο 802.11 και τα παράγωγά του περιλαμβάνονται οι τελευταίες εκδόσεις κάθε τύπου αρχείου.

- ✓ **Μεταφορά εικόνας και ήχου.** Η υποστήριξη ταχυτήτων μεγαλύτερων των 54Mbps καθιστά δυνατή την απρόσκοπτη μεταφορά εικόνας και ήχου, και μάλιστα με ιδιαίτερα υψηλή ποιότητα. Σε συνδυασμό με την εξάπλωση του broadband Internet (π.χ. ADSL), είναι δυνατή η προβολή αρχείων multimedia κορυφαίας ποιότητας σε κάθε υπολογιστή του κεντρικού δικτύου, ανεξάρτητα από το εάν αυτός είναι συνδεδεμένος σε αυτό ενσύρματα ή ασύρματα.

- ✓ **Διαχείριση επιμέρους συσκευών**. Καθώς τα ασύρματα δίκτυα θα εξαπλώνονται, θα ξεκινήσει η ενσωμάτωση καρτών δικτύου σε κάθε είδους υλοποίηση, όπως είναι οι οικιακές συσκευές ή τα παιχνίδια. Συγκεκριμένα, ενσωματώνοντας δυνατότητα ασύρματης δικτύωσης, οι εν λόγω συσκευές θα μπορούν να "συμμετέχουν" στο κεντρικό δίκτυο. Κατ' αυτό τον τρόπο θα είναι δυνατή η πλήρης διαχείρισή τους από οποιονδήποτε υπολογιστή του δικτύου.

Από όλα τα παραπανω και τη πληθώρα εφαρμογών των ασυρματων δικτυων ευκολα καταληγουμε ότι παρουσιαζουν τοσο ενδιαφερων εξάιτιας των χαρακτηριστικων τους αλλα και των πλεονεκτήματων που εχουν στη πραξη.

4.2) <u>ΠΛΕΟΝΕΚΤΗΜΑΤΑ & ΜΕΙΟΝΕΚΤΗΜΑΤΑ</u>

4.2.1)<u>Πλεονεκτηματα:</u>

• Ευκαμψία (Flexibility)
Με τα ραδιοκύματα ,οι διάφορες συσκευές του δικτύου μπορούν να επικοινωνούν
χωρίς άλλους περιορισμούς (τοίχους, πατώματα) και μπορούν να τοποθετηθούν παντού.
Γίνεται ακόμη πιο εύκολη η επικοινωνία μεταξύ κτιρίων.
• Προσχεδίαση (Planning)
Μόνο τα wireless ad-hoc δίκτυα επιτρέπουν την επικοινωνία χωρίς προηγούμενο
σχεδιασμό –οποιαδήποτε ασύρματο δίκτυο χρειάζεται σχεδιασμό για τις καλωδιώσεις.Στα WLANS, οι συσκευές μπορούν να επικοινωνούν, φτάνει να ακολουθούν το ίδιο πρότυπο και πρωτόκολλο, ενώ στα ενσύρματα δίκτυα, χρειάζονται επιπρόσθετα 5 σύρματα, ειδικές πρίζες, πιθανόν ακόμη και εσωτερικές συσκευές (π.χ switches) για να γίνει δυνατή η επικοινωνία.

• Σχεδιασμός (Design)
Μόνο τα WLANS επιτρέπουν το σχεδιασμό μικρών φορητών συσκευών που θα ενώνονται με το δίκτυο. Τα καλώδια περιορίζουν όχι μόνο τους χρήστες
αλλά και τους σχεδιαστές μικρών PDAs, notepads κτλ. Επιπλέον, η τρέχουσα
τεχνολογία δικτύων μπορεί να εφαρμοστεί χωρίς να είναι ορατή.
• Δύναμη (Robustness)
Τα wireless LANS μπορούν να αντέξουν και να επιβιώσουν από διάφορες
καταστροφές ,όπως σεισμούς. Τα παραδοσιακά LANS θα κατέρρεαν εντελώς.

4.2.2) Μειονεκτηματα:

• Ποιότητα Υπηρεσίας (Quality of Service)
Τα WLANS, τυπικά προσφέρουν χαμηλότερη ποιότητα υπηρεσίας από τα
ενσύρματα δίκτυα. Ο κύριος λόγος για αυτό, είναι το χαμηλό bandwidth που
οφείλεται σε περιορισμούς στην εκπομπή ραδιοκυμάτων και στα μεγαλύτερα
ποσοστά λαθών λόγω παρεμβολών.
• Ιδιοκτησιακές Λύσεις (Proprietary Solutions)
Λόγω της καθυστέρησης στις διαδικασίες προτυποποίησης, πολλές εταιρίες, έχουν βρει κάποιες ιδιοκτησιακές λύσεις και προσφέρουν προτυποποιημένες λειτουργίες με πολλές επιπρόσθετες υπηρεσίες.
• Περιορισμοί (Restrictions)
Όλα τα ασύρματα προϊόντα πρέπει να συμβιβάζονται με τους κρατικούς μηχανισμούς. Πολλές κυβερνήσεις και μη κυβερνητικά ιδρύματα, περιορίζουν
κάποιες συχνότητες για να αποφεύγονται οι παρεμβολές.
• Ασφάλεια και Προστασία δεδομένων (Safety and Security)
Η χρήση ραδιοκυμάτων για μετάδοση δεδομένων, μπορεί να δημιουργήσει παρεμβολές σε κάποια άλλα μηχανήματα, όπως για παράδειγμα σε μηχανήματα που χρησιμοποιούνται σε νοσοκομεία.
• Πρακτικα προβληματα
Οι τιμές των συχνοτήτων που χρησιμοποιούνται για την ασύρματη επικοινωνία των συσκευών καθιστούν εφικτή την ανταλλαγή δεδομένων ακόμα και όταν παρεμβάλλονται φυσικά εμπόδια (π.χ. τοίχοι ή έπιπλα). Βέβαια, προβλήματα δεν παύουν να υπάρχουν και, γενικά, της τοποθέτησης των access points πρέπει να προηγείται προσεκτική μελέτη του χώρου και της διαρρύθμισής του.

Αρχικά, αν στο χώρο που πρόκειται να γίνει η εγκατάσταση υπάρχουν μεταλλικά χωρίσματα μεγάλων διαστάσεων, τα access points πρέπει να τοποθετηθούν επάνω από αυτά. Παράλληλα, συσκευές όπως οι

φούρνοι μικροκυμάτων ή τα ασύρματα τηλέφωνα, οι οποίες χρησιμοποιούν τη συχνότητα των 2,4GHz, είναι δυνατό να προκαλέσουν παρεμβολές. Μάλιστα, καθώς το Bluetooth (εναλλακτικό πρότυπο ασύρματης επικοινωνίας) εξαπλώνεται, τα προβλήματα αναμένεται να αυξηθούν, καθώς και το συγκεκριμένο πρωτόκολλο λειτουργεί στα 2,4GHz. Τέλος, παρεμβολές ενδέχεται να παρουσιαστούν εξαιτίας επίπλων μεγάλων διαστάσεων, ακόμα και ενυδρείων.

Αξίζει να σημειωθεί ότι τα προβλήματα που περιγράφηκαν είναι σαφώς εντονότερα όταν επιλεγεί το πρωτόκολλο 802.11a, το οποίο χρησιμοποιεί τη συχνότητα των 5GHz για τη λειτουργία του. Στη συγκεκριμένη περίπτωση, και για να είναι δυνατή η επίτευξη ταχυτήτων κοντά στην ονομαστική τιμή των 54Mbps, ο χρήστης πρέπει να τοποθετήσει τα διαθέσιμα access points σε κοντινή απόσταση και να φροντίσει να απομακρύνει κάθε είδους συσκευή που θα μπορούσε να προκαλέσει οποιουδήποτε είδους παρεμβολή.

Όλα τα προαναφερομενα όμως δεν αναιρουν το γεγονος ότι υπαρχουν και καποια μειονεκτηματα με σημαντικες επιπτωσεις και κυριο θυμα δυστυχως τον ιδιο τον ανθρωπο.Παρακατω φαινεται ο τροπος με τον οποιο ένα ασυρματο δικτυο μπορει να είναι επιβλαβη για τον ανθρωπο:

Επιπτώσεις των ηλεκτρομαγνητικών πεδίων στον ανθρωπο

Τα ηλεκτρομαγνητικά κύματα μεταφέρονται από τα σωματίδια που ονομάζονται κβάντα. Στην ψηλή συχνότητα (και άρα στα μικρά μήκη κύματος) ηκβαντική ενέργεια είναι πολύ μεγάλη και αποτελεί μεταλλαξογόνο παράγοντα.
Όταν η μεταφερόμενη ενέργεια είναι μεγάλη, τότε σπάζουν οι δεσμοί μεταξύ των μορίων. Το γεγονός αυτό είναι ιδιαίτερα επικίνδυνο. Προκαλούνται αλλοιώσεις του γενετικού κώδικα του DNA. Το αποτέλεσμα είναι η πρόκληση καρκίνου και άλλων σοβαρών ασθενειών. Ευτυχώς δεν είναι όλα τα είδη ΗΜΠ που μπορούν να προκαλέσουν αλλοιώσεις στο DNA. Μόνο αυτά που χαρακτηρίζονται από ψηλή συχνότητα, μικρό μήκος κύματος και ψηλή ενέργεια μπορούν να προκαλέσουν βλάβες στο DNA. Η ακτινοβολία που έχει αυτή τη δυνατότητα ονομάζεται ιονίζουσαακτινοβολία. Η ηλεκτρομαγνητική ακτινοβολία στην οποία υποβαλλόμαστε συνήθωςκαι καθημερινά είναι η μη ιονίζουσα ακτινοβολία και δεν έχει τέτοιες δυνατότητεςκαι κινδύνους. Υπάρχει μόνο μια εξαίρεση στην καθημερινή ακτινοβολία που δεχόμαστε. Πρόκειται για την ιονίζουσα ακτινοβολία που προκαλείται από τις υπεριώδεις ακτίνες του ήλιου. Η έκθεση στο ηλιακό φως και κατά συνέπεια στιςυπεριώδεις ακτίνες, είναι αιτία καρκίνου του δέρματος (μελανώματος,ακανθοκυτταρικού και βασεοκυτταρικού

καρκινώματος) και άλλων αλλοιώσεων και ρυτίδων. Τα διάφορα είδη ηλεκτρομαγνητικής ακτινοβολίας και τα πεδία που προκύπτουν, έχουν διαφορετικές επιδράσεις στον ανθρώπινο οργανισμό.
Οι επιπτώσεις που προκαλούνται από την έκθεση στην ηλεκτρομαγνητική
ακτινοβολία εξαρτώνται κυρίως από δύο παράγοντες:

Τη Συχνότητα Εκπομπής: Για συχνότητες που ανήκουν στο ραδιοφάσμα (υπηρεσίες ραδιοφωνίας, τηλεόρασης, κινητής τηλεφωνίας), η εκπεμπόμενη ακτινοβολία ονομάζεται «μη ιονίζουσα», διότι δεν μπορεί να δημιουργήσει ιόντα μέσα στην ύλη, δηλαδή (με επιστημονικούς όρους) το φωτόνιό της δεν έχει αρκετή ενέργεια, ώστε να εκδιώξει ένα ηλεκτρόνιο από ένα άτομο της ύλης. Αντιθέτως, σε πολύ υψηλές συχνότητες (π.χ. ακτίνες Χ) η ακτινοβολία μπορεί να προκαλέσει ιονισμό, επομένως άμεση βλάβη στη βιολογική ύλη, και ονομάζεται «ιονίζουσα». Στις ραδιοσυχνότητες, έχει διαπιστωθεί ότι οι κύριες επιπτώσεις της ηλεκτρομαγνητικής ακτινοβολίας είναι θερμικές**.**
Την Ισχύ Εκπομπής**:** Υπάρχουν διάφορα μεγέθη που ποσοτικοποιούν την ηλεκτρομαγνητική ακτινοβολία, με το πιο ευρέως διαδεδομένο στις ραδιοσυχνότητες την Ένταση του ηλεκτρικού πεδίου (συμβολίζεται με Ε και μετριέται σε Βολτ ανά μέτρο).

Ως επιπροσθετη πληροφορια στη μελετη αυτή δε μπορουμε να παραλειψουμε τα υλικα που χρειαζονται για τη σύνδεση σε ένα ασύρματο δίκτυο ελεύθερης πρόσβασης ως απλός χρήστης.Παρακατω αναφερουμε ένα τετοιο παραδειγμα:

4.3) ΥΛΙΚΑ ΕΝΟΣ ΑΣΥΡΜΑΤΟΥ ΔΙΚΤΥΟΥ:

1. *Μία κατευθυντική κεραία.*
2. *Ένα καλώδιο RG-213 2 έως 3 μέτρα.*
3. *Δύο θηλυκά βύσματα τύπου N.*
4. *Ένα μετατροπέα ή pigtail από βύσμα τύπου N σε βύσμα της ασύρματης κάρτας που θα χρησιμοποιήσετε.*
5. *Μία ασύρματη κάρτα δικτύου.*
6. *Μία κάρτα LAN.*

7. *Ένα κουτί προστασίας της ασύρματης κάρτας.*
8. *Καλώδιο FTP ή UTP .*
9. *Ένα κλασικό ιστό κεραίας.*

Ανάλυση του κάθε αντικειμένου χωριστά:

Κατευθυντική Κεραία

1. Η κατευθυντική κεραία είναι ένας τύπος κεραίας που έχει την ικανότητα να εκπέμπει ηλεκτρομαγνητικά κύματα προς ένα συγκεκριμένο στόχο. Επίσης μπορεί να λαμβάνει κύματα από τον στόχο αυτό και να τα ενισχύει. Στη δική μας περίπτωση ο στόχος αυτός θα είναι ένα σημείο πρόσβασης (Access Point - AP). Οι συνηθέστερες κατευθυντικές κεραίες για ασύρματο δίκτυο είναι οι συρμάτινες παραβολικές. Καλό είναι το καλώδιο της κεραίας να καταλήγει σε αρσενικό βύσμα τύπου N για λόγους που θα εξηγηθούν αμέσως μετά. Η ενίσχυση που πετυχαίνουν λόγο της συγκέντρωσης των ηλεκτρομαγνητικών κυμάτων σε ένα σημείο (εστία) μετρείται σε dB. Κλασικές τιμές της ενίσχυσης μίας κεραίας είναι 15 έως 21 dB περίπου.

Καλώδιο RG213

2. Το καλώδιο RG213 (εμπορική ονομασία 213) μεταφέρει το σήμα από την κεραία προς την ασύρματη κάρτα. Είναι ένα παχύ καλώδιο με χοντρό πυρήνα και με ηλεκτρομαγνητική θωράκιση από χάλκινα σύρματα. Το κόστος του κυμαίνεται από 1.5 έως 2.5 ευρώ το μέτρο. Οι απώλειες σε σήμα είναι σημαντικές 4dB/m. Γι' αυτό το μήκος του περιορίζεται σε 10 μέτρα το πολύ. Υπάρχουν και άλλων τύπων καλώδια μικρότερων απωλειών όπως το LMR400 το οποίο είναι λεπτό και έχει απώλειες μόλις 0.5dB/m. Στα αρνητικά του είναι η πολύ υψηλή του τιμή που κυμαίνεται στα 7 ευρώ το μέτρο.

Καλώδιο RG213

Καλώδια LMR

Θηλυκά βύσματα τύπου Ν

3. Τα θυλικά βύσματα τύπου Ν τοποθετούνται στα άκρα του RG213, και συνεπώς θα πρέπει να είναι κατάλληλα για χονδρό καλώδιο. Αυτό είναι σημαντικό γιατί υπάρχουν στενά θηλυκά βύσματα τύπου Ν για λεπτό καλώδιο LMR400. Προτιμώ τα θηλυκά βύσματα γιατί είναι ποιο εύκολα στην τοποθέτηση στο RG213. Γι' αυτόν το λόγο το βύσμα της κεραίας πρέπει να είναι αρσενικό. Το κόστος του ενός βύσματος κυμαίνεται στα 2 ευρώ.

Μετατροπέας-Pigtail

4. Μετατροπέας ή pigtail όπως συνηθίζεται να λέγεται στο εμπόριο επειδή έτσι το βαπτίσαν οι αμερικάνοι (pigtail=γουρουνοουρά;!). Παρόλα αυτά θα συνεχίσω με τον ευρέως χρησιμοποιούμενο όρο pigtail. Το pigtail αποτελείται από ένα λεπτό καλώδιο χαμηλών απολειών σαν το LMR400. Στο ένα του άκρο έχει ένα βύσμα τύπου Ν που για την δική μας περίπτωση πρέπει να είναι αρσενικό αφού στο RG213 έχουν τοποθετηθεί θηλυκά βύσματα. Στο άλλο του άκρο υπάρχει ένα βύσμα το οποίο μπαίνει στην ασύρματη κάρτα που έχετε (το χρυσαφί στην εικόνα). Η δουλεία του είναι να συνδέσει το καλώδιο που έρχεται από την κεραία με την ασύρματη κάρτα. Υπάρχουν pigtail με αρσενικό ή

θηλυκό Ν τύπου βύσμα για διάφορες ασύρματες κάρτες.

Ασύρματη κάρτα δυκτύου

5. Η ασύρματη κάρτα είναι υπεύθυνη για την μετατροπή του ηλεκτρομαγνητικού κύματος σε ψηφιακό. Υπάρχουν τρία βασικά είδη ασύρματων καρτών. Οι εξωτερικές με σύνδεση LAN, οι εξωτερικές με σύνδεση USB και οι εσωτερικές PCI κάρτες. Η καλύτερη λύση είναι η εξωτερική κάρτα με σύνδεση LAN που τοποθετείται κοντά στην κεραία. Τα πλεονεκτήματα είναι τα εξής. Χρειάζονται λίγο καλώδιο RG213 για να συνδεθεί με την κεραία που σημαίνει λίγες απώλειες και μικρό κόστος καλωδίου. Ακόμα και να έχετε διαμέρισμα ρετιρέ το καλώδιο RG213 για να έρθει από την ταράτσα θα πρέπει να είναι αρκετά μεγάλο. Εκτός αν τοποθετήσετε την κεραία σας στο παράθυρο από το οποίο θα έχετε οπτική επαφή με κάποιο κόμβο(αυτό προϋποθέτει να μένετε ρετιρέ σε κάποια ιδιαίτερα ψηλή πολυκατοικία). Σε αυτή την εξαίρεση η φθηνότερη λύση είναι η εσωτερική PCI κάρτα. Το κόστος της εξωτερικής κάρτας είναι μεγαλύτερο από αυτό της εσωτερικής. Όμως αν προστεθεί το κόστος του καλωδίου, ακόμα και να χρησιμοποιήσετε το σχετικά φθηνό RG213 αντι του LMR, η λύση της εσωτερικής PCI κάρτας είναι ακριβότερη. Η ασύρματη κάρτα για να μπορεί να επικοινωνήσει με τις άλλες κάρτες θα πρέπει να έχει πάνω της το chipset Prism2 ή Prism2.5 και να λειτουργούν με το πρωτόκολλο 802.11b ή g. Με απλά λόγια θα πρέπει να αγοράσετε κάποια συγκεκριμένα μοντέλα κάποιων εταιριών. Τέτοιες πληροφορίες αγοράς θα βρείτε στην κοινότητα συζητήσεων. Το κόστος της εξωτερικής ασύρματης κάρτας με σύνδεση LAN κυμαίνεται στα 60 έως 300 το πολύ ευρώ. (Οι φθηνές κάρτες δεν υστερούν και πολύ από τις ακριβές. Χρειάζεται να κάνετε μία έρευνα αγοράς για να καταλάβετε ακριβώς τι συμβαίνει).

Εσωτερική PCI ασύρματη κάρτα - Εξωτερική LAN ασύρματη καρτα

Κάρτα LAN

6. Η κάρτα LAN είναι μία φθηνή PCI κάρτα ενσύρματου δικτύου και τοποθετείται στη μητρική σας. Το κόστος της κυμαίνεται στα 10-15 ευρώ.

Κουτί προστασίας

7. Το κουτί αυτό προστατεύει την εξωτερική ασύρματη κάρτα από τον ήλιο και την βροχή. Μπορεί να είναι ένα ηλεκτρολογικό κουτί το οποίο κοστίζει αρκετά 40-60 ευρώ ή να χρησιμοποιήσετε ένα αυτοσχέδιο όπως ένα τάπερ ή κάτι άλλο.

Καλώδιο FTP ή UTP

8. Το FTP καλώδιο είναι αρκετά φθηνό και μπορεί να έχει σημαντικά μεγαλύτερο μήκος από το RG213 χωρίς να έχει απώλειες. Αυτό οφείλεται στο ότι το FTP καλώδιο δεν μεταφέρει ηλεκτρομαγνητικά κύματα αλλά ψηφιακά όπως το καλώδιο του τηλεφώνου. Ο ρόλος του είναι να συνδέσει την LAN έξοδο της ασύρματης κάρτας με τη κάρτα LAN του υπολογιστή.

Ιστός κεραίας

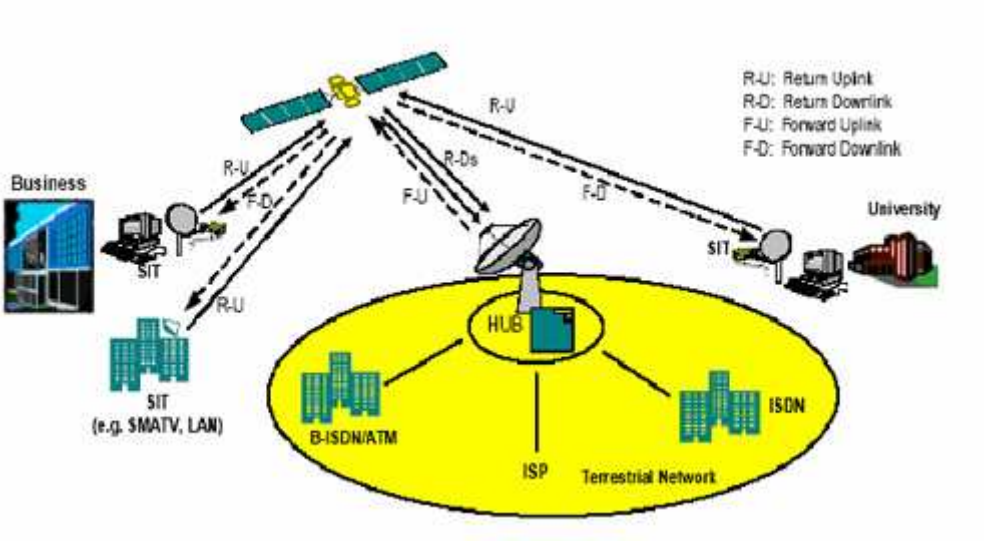
9. Ένας συνηθισμένος ιστός τηλεόρασης που το ύψος του, σύμφωνα με τον νόμο, δεν πρέπει να ξεπερνάει τα 4 μέτρα από την βάση του.

4.3.1) Παράδειγμα ασύρματης δικτυακής εγκατάστασης : Η εταιρία Χ

Η εταιρία Χ δραστηριοποιείται στον χώρο των web services. Σε κάθε όροφο του τετραώροφου κτιριακού της συγκροτήματος πρέπει να παρέχεται σύνδεση στο εταιρικό LAN στους υπαλλήλους, καθώς και διασύνδεση με το internet. Access Points στημένα σε κάθε όροφο, συνδεδεμένα στον ενσύρματο «κορμό» του εταιρικού δικτύου, θα δίνουν αυτή τη δυνατότητα στους υπαλλήλους. Οι εργαζόμενοι μπορούν είτε να εργάζονται στους σταθμούς εργασίας τους, είτε να κινούνται με φορητούς υπολογιστές ανά τους ορόφους χωρίς να χάνουν την σύνδεση με το δίκτυο. Ένα προφανές πρόβλημα, είναι ότι η επιχείρηση έχει κτίρια και στις δύο μεριές μιας λεωφόρου. Θα ξεπεράσουμε αυτό το εμπόδιο, εγκαθιστώντας μια ad hoc σύνδεση μεταξύ των δύο κτιρίων, χρησιμοποιώντας μια συσκευή σταθμό σε κάθε ταράτσα,εφοδιασμένη με κατευθυντικές yagi κεραίες μικρού σχετικά κέρδους, μιας και η απόσταση που πρέπει να καλυφθεί είναι μικρή. Η χρήση αυτού του τύπου κεραίας(ιδιαίτερα κατευθυντικής εκπομπής) γίνεται για δύο σημαντικούς λόγους.
Α) Χρειαζόμαστε ένα απόλυτα κατευθυντικό Link. .εν θέλουμε να συνδεθούμε η να παρέχουμε κάποια υπηρεσία σε κανέναν άλλον εκτός από το απέναντι κτίριο. Με αυτό το δεδομένο, οποιαδήποτε ποσότητα ενέργειας της εκπομπής μας γίνεται σε χώρο εκτός της απέναντι κεραίας, θεωρείται σπατάλη, καθώς επιζητούμε την μέγιστη ποιότητα σύνδεσης που μπορούμε να έχουμε με μία δεδομένη ισχύ. Η ισχύς της κεραίας πρέπει πάντα να κρατηθεί εντός νομικών ορίων.
Β) Κατευθυντική εκπομπή στην ελάχιστη δυνατή ισχύ, σε αυτή την περίπτωση,σημαίνει αυξημένη ασφάλεια. Ένας υποθετικός εισβολέας, για να μπορέσει να εκμεταλλευτεί όλα τα μειονεκτήματα ασφαλείας του 802.11 που,πρέπει αρχικά να έχει πρόσβαση στην ίδια την μικροκυματική εκπομπή της κεραίας μας. Σε ένα ιδανικά και απόλυτα κατευθυντικό link, κάποιος θα μπορούσε να υποκλέψει την πληροφορία που διακινείτο στον αέρα, μόνο αν ήταν πάνω στην νοητή ευθεία των δύο κεραιών. Εφόσον η πρόσβαση στις ταράτσες των κτιρίων είναι απαγορευμένη, είναι πολύ μικρή η πιθανότητα να καταφέρει κάποιος την κακοπροαίρετη λήψη πακέτων χωρίς να αποθαρρυνθεί από την κακή ποιότητα σήματος που θα έχει από παραδείγματος χάριν, τον δρόμο.

4.4)Αμφίδρομο Δορυφορικό Internet

Η τεχνολογία DVB-RCS προσφέρει αμφίδρομες ευρυζωνικές υπηρεσίες μετάδοσης φωνής, δεδομένων, εικόνας και video μέσω του δορυφόρου. Το δίκτυο, το οποίο συνίσταται από το δορυφόρο, τον Κομβικό Σταθμό Εδάφους (HUB) και τα τερματικά των χρηστών (σταθερών και κινητών), διατάσσεται σε τοπολογία αστέρα και απεικονίζεται στο ακόλουθο σχήμα:



Για τη μετάδοση της κίνησης υφίστανται δύο οδεύσεις οι οποίες είναι:

- το προωστικό κανάλι (forward channel) από τον Κεντρικό Δορυφορικό Σταθμό Εδάφους στο δορυφόρο και στη συνέχεια προς το τερματικό
- το κανάλι επιστροφής (return channel) από το τερματικό προς το δορυφόρο και ύστερα στον Κεντρικό Δορυφορικό Σταθμό Εδάφους

Το καινοτόμο σύστημα καναλιών επιστροφής διευκολύνει την αμφίδρομη επικοινωνία υψηλού ρυθμού μετάδοσης δεδομένων και δίνει πλέον τη δυνατότητα να χρησιμοποιηθεί για τη γρήγορη πρόσβαση στο Διαδίκτυο καθώς και για τις μεγάλες ανταλλαγές δεδομένων. Το σύστημα DVB-RCS το οποίο υποβλήθηκε στην τελική τυποποίηση από το ETSI το 2000, περιλαμβάνει το σύστημα δεδομένων DVB/MPEG-2 για την προωστική σύνδεση καθώς και το πρωτόκολλο πολλαπλής πρόσβασης MF-TDMA για τη σύνδεση επιστροφής. Πιο συγκεκριμένα, το φέρον μετάδοσης στην προωστική όδευση χρησιμοποιεί τη διαμόρφωση QPSK καθώς και συνδεμένους συνελικτικούς κώδικες Reed Solomon. Επιπλέον, μηνύματα σηματοδοσίας μεταφέρονται στα επιμέρους τερματικά που αφορούν λάθη συχνότητας και συγχρονισμού καθώς και την κατανομή του εύρους ζώνης (θυρίδες χρόνου και συχνότητας). Αυτά τα μηνύματα μεταφέρονται μέσω ενός ή

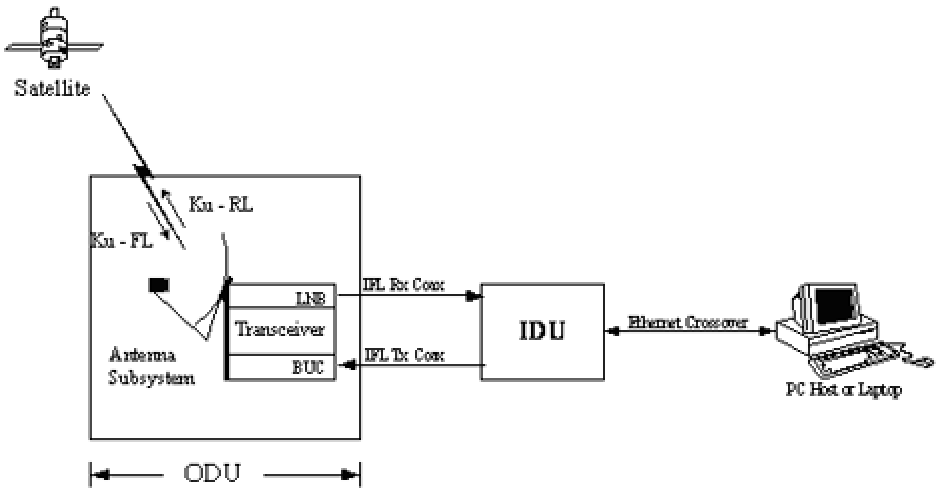
περισσοτέρων πολυπλεγμένων καναλιών ελέγχου του δικτύου. Επομένως, το κάθε δορυφορικό τερματικό για τη μετάδοσή του στο κανάλι επιστροφής δεν έχει σταθερή συχνότητα ούτε σταθερό εύρος φάσματος εκπομπής αλλά οι προαναφερθείσες παράμετροι καθορίζονται από τον Κεντρικό Δορυφορικό Σταθμό Εδάφους. Επομένως, τα τερματικά λαμβάνουν πίνακες με πληροφορίες για την εύρεση των καναλιών ελέγχου τους και είναι παρόμοιοι με τον πίνακα πληροφοριών δικτύου (NIT), πίνακα περιγραφής υπηρεσιών (SDT), και τον πίνακα πληροφοριών γεγονότος (EIT) στη μετάδοση DVB. Αναφορικά με την πορεία επιστροφής από τον επιμέρους χρήστη μέσω ενός δορυφορικού τερματικού, το τελευταίο λειτουργεί ως δρομολογητής-πολυπλέκτης για τις διάφορες πηγές δεδομένων, προς το διαδραστικό κεντρικό υπολογιστή στον Κεντρικό Δορυφορικό Σταθμό Εδάφους χρησιμοποιώντας ένα σχέδιο πολλαπλής πρόσβασης, MF-TDMA. Το MF-TDMA επιτρέπει σε μία ομάδα τερματικών να επικοινωνεί με τον κεντρικό κόμβο χρησιμοποιώντας συγκεκριμένες θυρίδες χρόνου/συχνότητας που απορρέουν από τη δυναμική ανάθεση εύρους ζώνης από τον κεντρικό σταθμό στα τερματικά με αποτέλεσμα το διαθέσιμο εύρος ζώνης να χρησιμοποιείται αποτελεσματικά.

Δορυφορικό Τερματικό (SIT)

Ο απαιτούμενος εξοπλισμός για τα άκρα του δικτύου περιγράφονται στην παράγραφο αυτή. Το δορυφορικό τερματικό αποτελείται τυπικά από τα παρακάτω στοιχεία

- - Εξωτερική μονάδα (ODU)
- - Εσωτερική μονάδα (IDU)

Η συνδεσμολογία του εξοπλισμού φαίνεται στο παρακάτω σχήμα



Η εξωτερική μονάδα αποτελείται από μία κεραία που μπορεί να λειτουργεί στην Ku μπάντα συχνοτήτων. Τα μεγέθη που μπορεί να υποστηρίξει το προτεινόμενο μοντέλο εκτείνονται από 0.96m ως 1.8m. Οι συχνότητες λήψης βρίσκονται στην μπάντα μεταξύ 10.95 ως 12.75GHz. Η λήψη πραγματοποιείται με την χρήση ενός LNB που λειτουργεί επίσης στην ίδια μπάντα συχνοτήτων. Η μονάδα αυτή διαθέτει διεπαφή L-band η οποία συνδέεται απευθείας στην εσωτερική μονάδα μέσω ομοαξονικού καλωδίου. Η μετάδοση πραγματοποιείται με τη χρήση ενός High Power Block Up Converter που λειτουργεί επίσης στην Ku μπάντα συχνοτήτων. Στις περισσότερες των περιπτώσεων μετάδοσης χρησιμοποιείται ένας 2-Watt ενισχυτής. Οι συχνότητες μετάδοσης βρίσκονται στην μπάντα 14 ως 14.5 GHz. Παρομοίως με τη λήψη η έξοδος του συστήματος μετάδοσης μέσω ομοαξονικού καλωδίου συνδέεται με την εσωτερική μονάδα.

ΚΕΦΑΛΑΙΟ 5 ο

ΕΠΙΠΡΟΣΘΕΤΑ-ΕΠΙΛΟΓΕΣ

Στο πεμπτο και τελευταιο κεφαλαιο της μελετης αυτης πανω στη δομη,τα χαρακτηρηστικα και το τροπο λειτουργιας των ασυρματων δικτυων θα παρουσιασουμε καποιες επιπροσθετες πληροφοριες

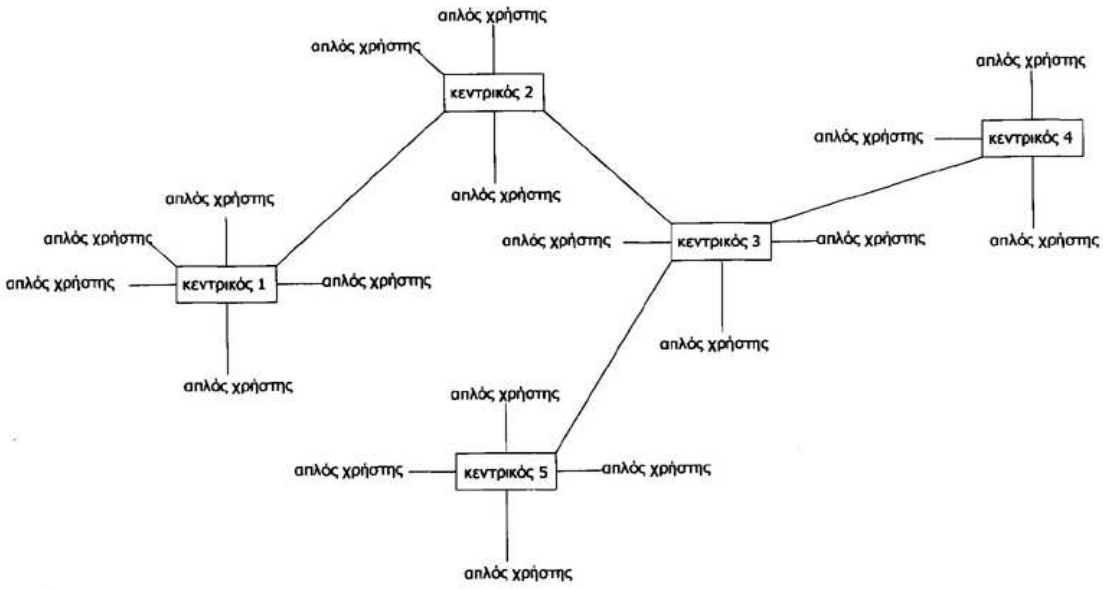
5.1) Τα Ασυρματα δικτυα υπολογιστων στην Ελλαδα σημερα

Είναι γεγονός πως η Ελλάδα υστερεί σημαντικά σε τεχνολογικό επίπεδο σε σχέση με αρκετές ευρωπαϊκές χώρες. Σε αυτό δεν αποτελούν εξαίρεση οι υψηλής ταχύτητας ψηφιακές συνδέσεις, οι οποίες αποτελούν στη χώρα μας προνόμιο λίγων. Τη στιγμή που σε άλλα κράτη έχουν συνδέσεις ADSL μεμικρό κόστος εμείς έχουμε μείνει στην εποχή του modem και της dial-up σύνδεσης για καθαρά εμπορικούς λόγους του ΟΤΕ και των ISP ενώ το κόστος της πολλά υποσχόμενης ISDN θεωρείται υψηλό για τον μέσο Έλληνα χρήστη. Για τον λόγο αυτό δημιουργήθηκαν σε διάφορες πόλεις της Ελλάδας ασύρματα δίκτυα τα οποία χαρακτηρίζονται από υψηλή ταχύτητα μετάδοσης δεδομένων η οποία είναι στην πράξη (1-6 Mbps).Το ασύρματο δίκτυο αυτή τη στιγμή δεν προσφέρει πρόσβαση στο διαδίκτυο χωρίς αυτό να σημαίνει πως στο μέλλον δεν θα συμβεί κάτι τέτοιο. Δεν έχει δημιουργηθεί από κάποια εταιρία αλλά από τα ίδια του τα μέλη που συμμετέχουν σε αυτό. Δηλαδή με τη συμμετοχή σου και το απλό στήσιμο του εξοπλισμού σου συμβάλεις στην επέκταση του δικτύου. Αρα δεν τίθεται θέμα πληρωμής για συνδρομή.

5.1.1) Πως δουλεύει αυτό το δίκτυο

Όπως σε όλα τα μεγάλα δίκτυα υπολογιστών υπάρχει ένας κεντρικός υπολογιστής στον οποίο συνδέονται οι υπόλοιποι. Ο κεντρικός με τη σειρά του επικοινωνεί με ένα ή πολλούς κεντρικούς και με την επανάληψη αυτού του μοτίβου δημιουργείται ένα δίκτυο.

Ένα ασύρματο δίκτυο που καλύπτει μία πόλη σαν τη Θεσσαλονίκη βασίζεται σε αυτή τη φιλοσοφία. Ορισμένοι είναι πρόθυμοι να ξοδέψουν παραπάνω χρήματα για τη κατασκευή ασύρματων κόμβων που λειτουργούν όλο το εικοσιτετράωρο για την εξυπηρέτηση των απλών χρηστών (χωρίς αυτά τα παιδιά δεν θα υπήρχε τίποτα). Ένα απλό διάγραμμα ενός υποτιθέμενου ασύρματου δικτύου.



Ο κεντρικός υπολογιστής 1 συνδέει κάποιους απλούς χρήστες δημιουργώντας ένα τοπικό δίκτυο. Ο ίδιος συνδέεται με ένα άλλο κεντρικό τον 2. Ο κεντρικός 2 φέρνει σε επαφή τον 1 και τον 3 καθώς και τους γύρω του απλούς χρήστες. Ο 3 συνδέει με τη σειρά του άμεσα τους 2, 4, και 5. Με τον τρόπο αυτό ο απλός χρήστης που επικοινωνεί με τον κεντρικό 1 μπορεί να ανταλλάξει πληροφορίες με τον απομακρυσμένο απλό χρήστη που επικοινωνεί με τον κεντρικό 4. Στο ασύρματο δίκτυο οι κεντρικοί υπολογιστές ονομάζονται σημεία πρόσβασης (Access Point σύντομα A.P.) και με αυτή τη φιλοσοφία μπορεί να καλύψει μία ολόκληρη πόλη.
Ο αριθμός μελών των ασύρματων δικτύων αυξάνεται συνεχώς στην Ελλάδα και σε αυτό τον τομέα πρωτοπορούμε στη κυριολεξία παγκοσμίως χωρίς τη βοήθεια του κράτους ή κάποιου άλλου φορέα παρά μόνο με το προσωπικό ενδιαφέρον των μελών.

5.2) Υφιστάμενο καθεστώς για τα ασύρματα τοπικά δίκτυα (WLAN) στην Ελλάδα

Ως Σταθερή Ασύρματη Πρόσβαση (ΣΑΠ), ορίζεται η εφαρμογή της ασύρματης πρόσβασης, στην οποία η τοποθεσία του τερματισμού του χρήστη και του σημείου πρόσβασης του δημόσιου τηλεπικοινωνιακού δικτύου, στο οποίο συνδέεται ο χρήστης, είναι σταθερά, με χρήση αποκλειστικά και μόνο ραδιοσυχνοτήτων, που έχουν εκχωρηθεί για το σκοπό αυτό. Δεδομένου του καθορισμού των ζωνών Σταθερής Ασύρματης Πρόσβασης με Υπουργική Απόφαση στα 3,6 και 26GHz και της χορήγησης των σχετικών αδειών με τη διαδικασία της δημοπρασίας το Δεκέμβριο του 2000, δεν έχει επιτραπεί μέχρι σήμερα η χρήση των 2,4GHz για την παροχή υπηρεσιών ΣΑΠ.

5.2.1) Περιοχή 2,4GHz

Δεν απαιτείται Εκχώρηση Ραδιοσυχνότητας για τη λειτουργία Σταθμών Ραδιοεπικοινωνιών, οι οποίοι πληρούν τις παρακάτω προϋποθέσεις

(απόφαση ΕΕΤΤ 254/72, ΦΕΚ 895/Β/1672002/άρθρο 5):
1. Εκπέμπουν και λαμβάνουν στην περιοχή ραδιοσυχνοτήτων 2.400 - 2.483,5 MHz (ISM band).
2. Χρησιμοποιούν τεχνολογία διασποράς φάσματος (Spread Spectrum).
3. Είναι πλήρως συμβατοί με το εναρμονισμένο πρότυπο EN 300 328 του ETSI.

Χρειάζεται ειδική άδεια για παροχή τηλεπικοινωνιακών υπηρεσιών, με τη χρήση αυτής της συχνότητας σε τρίτους. Στον Κάτοχο της Άδειας, δίδεται το δικαίωμα παροχής Δημόσιων Κινητών Τηλεπικοινωνιακών Υπηρεσιών Ασύρματων Τοπικών Δικτύων σε δημόσιους χώρους (hotspots), με χρήση ραδιοεξοπλισμού συμβατού με το πρότυπο EN 300 328 του ETSI, που χρησιμοποιεί ραδιοσυχνότητες που βρίσκονται στη ζώνη 2.400-2.483,5MHz. Ο κάτοχος της άδειας αποδέχεται ότι στους σταθμούς ραδιοεπικοινωνιών που εγκαθίστανται και οι οποίοι λειτουργούν στη ζώνη 2.400-2.483,5MHz για την παροχή Δημόσιων Κινητών Τηλεπικοινωνιακών Υπηρεσιών Ασύρματων Τοπικών Δικτύων, δεν παρέχεται προστασία από τυχόν παρεμβολές, ούτε επιτρέπεται οι σταθμοί αυτοί να προκαλούν επιζήμιες παρεμβολές σε άλλους σταθμούς ραδιοεπικοινωνίας. Τέλος, ο κάτοχος της Άδειας δεν επιτρέπεται να παρέχει υπηρεσίες Σταθερής Ασύρματης Πρόσβασης (δεν επιτρέπεται η ζεύξη σημείου προς σημείο) και δεν επιτρέπεται να αναπτύξει Δημόσιο Τηλεπικοινωνιακό Δίκτυο Κορμού, κάνοντας χρήση ραδιοσυχνοτήτων, που βρίσκονται στη ζώνη 2.400-2.483,5MHz.

5.2.2) Περιοχή 5GHz
Γενικά, για τις περιοχές 5.150-5.250, 5.250-5.350, 5.470-5.725MHz και 1 7,1 - 1 7,3GHz, (ΦΕΚ 979/Β11672003, παρ. 3/ιδ) επιτρέπεται χωρίς άδεια, η λειτουργία συσκευών μικρής εμβέλειας, οι οποίες είναι σύμφωνες με το Προεδρικό Διάταγμα 44/2002, τη Σύσταση ERC/REC 7003 και τα Πρότυπα EN 3008361, 2, 3 και 4, για την υλοποίηση τοπικών ασύρματων δικτύων με πρωτόκολλο HIPERLAN, σε εσωτερικούς μόνο χώρους. Η δημιουργία τέτοιων δικτύων σε εξωτερικούς χώρους, επιτρέπεται μόνο μετά από άδεια της ΕΕΤΤ, η οποία χορηγείται ύστερα από σύμφωνη γνώμη του Υπουργείου Εθνικής Αμύνης. Παρομοίως, με την περιοχή των 2,4GHz, δεν επιτρέπονται ζεύξεις σημείου προς σημείο. Δοθέντος του γεγονότος ότι η εγκατάσταση δικτύων σε εξωτερικούς χώρους απαιτεί τη σύμφωνη γνώμη του ΓΕΕΘΑ, καθίσταται πολύ δύσκολη έως αδύνατη, η χορήγηση αδειών για παροχή υπηρεσιών στο κοινό, λόγω του ότι θα πρέπει οι παροχείς να καθορίζουν εκ των προτέρων και με την αίτηση τους, τους χώρους στους οποίους επιθυμούν να εγκαταστήσουν δίκτυα για την παροχή υπηρεσιών.

5.3) Ελληνικές κοινότητες WiFi

Έχει και η Ελλάδα τις δικές της ασύρματες κοινότητες, που στήνουν το ανεξάρτητο δίκτυο τους, στηριγμένο στο WiFi, χωρίς να ενοχλούν κανένα, εξασφαλίζοντας φθηνή και απρόσκοπτη επικοινωνία. Τέτοια δίκτυα (community networks) υπάρχουν σε αρκετές ελληνικές πόλεις (Αθήνα, Θεσσαλονίκη, Πάτρα, Γιάννενα, Σέρρες, Ξάνθη, κ.ά) ενώ υπάρχει στα σκαριά η διαμόρφωση πανελλήνιου δικτύου. Στη χώρα μας, οι επίσημοι κόμβοι WiFi έχουν πλέον αυξηθώ κατά πολύ (κυρίως στα αστικά κέντρα), ενώ πληθαίνουν

τα hotspots σε ξενοδοχεία, infokαφετέριες και κάθε είδους επιχειρήσεις. Δυστυχώς, τα ελληνικά ασύρματα δίκτυα παραμένουν ακόμη στην πρώτη εποχή του WiFi, δηλαδή του τοπικού δικτύου, αλλά αυτό δεν μειώνει καθόλου το ενδιαφέρον.
Το **Ασύρματο Μητροπολιτικό Δίκτυο Αθηνών (AWMN)** είναι ένας μη κερδοσκοπικός σύλλογος, που καλύπτει τις περισσότερες περιοχές της Αθήνας (σύμφωνα με το αντίστοιχο site, 2257 κόμβοι τον Ιούλιο 2004) και συνεχώς επεκτείνεται. Είναι αξιοσημείωτη η ανάπτυξη ενός τέτοιου ασύρματου δικτύου σε τόσο μεγάλη γεωγραφική κλίμακα. Το Salonica Wireless Network (SWN), η ασυρμάτως δικτυωμένη κοινότητα της Θεσσαλονίκης, αυτοπροσδιορίζεται στην ιστοσελίδα της ως εξής: "7ο SWN είναι μια ομάδα ατόμων, η οποία επεκτείνεται μέρα με τη μέρα, που ασχολούνται με τη δημιουργία ενός νόμιμου, ψηφιακού, ασύρματου δικτύου υψηλών ταχυτήτων, ελεύθερης πρόσβασης, στην ευρύτερη περιοχή της Θεσσαλονίκης. Κύριος σκοπός είναι να δημιουργηθεί ένα αξιοπρεπές, ελεύθερο δίκτυο, με υψηλό bandwidth ανάμεσα στους κόμβους κάθε ενδιαφερόμενου, μέσω ενός κοινοτικού ασύρματου δικτύου. Το SWN δεν θέτει ως στόχο του αυτήν τη στιγμή την παροχή Ίντερνετ. Ως χρήσεις του τοπικού δικτύου που θέλει να στήσει, είναι η ανταλλαγή δεδομένων και αρχείων, το ηλεκτρονικό ταχυδρομείο, τα παιχνίδια, η ανταλλαγή υπηρεσιών, το voiceoverIP και η τηλεφωνία, η τηλεδιάσκεψη, το video streaming, οι συνομιλίες (chatting) και γενικά οποιαδήποτε λειτουργία μπορεί να αναπτυχθεί στο Ίντερνετ. Ας μην ξεχνάμε πως και το Ίντερνετ ξεκίνησε σαν τοπικό δίκτυο μεταξύ Πανεπιστημίων των ΗΠΑ, χωρίς να είναι βέβαιο το μέλλον του".
Το **Ακαδημαϊκό Ασύρματο Δίκτυο Ηρακλείου**, είναι άλλο ένα community network, που έχει δημιουργηθεί εξ ολοκλήρου από την ακαδημαϊκή κοινότητα του Πανεπιστημίου Ηρακλείου και παρουσιάζει σοβαρή ανάπτυξη. Στο Βόλο, το Πανεπιστήμιο Θεσσαλίας έχει υλοποιήσει ένα ασύρματο δίκτυο, το οποίο συνδέει ευρυζωνικά όλα τα σχολεία της περιοχής, στο πλαίσιο του Πανελλήνιου Σχολικού Δικτύου. Αξίζει να σημειωθεί ότι όλα τα Ασύρματα

Δίκτυα της Ελλάδας, δεν έχουν εμπορική διάσταση, αλλά αυστηρά συνεργατική. Με βάση το ισχύον κανονιστικό πλαίσιο, τα community networks εντάσσονται στο "καθεστώς ιδίας χρήσης", υπό την προϋπόθεση ότι δεν παρέχουν εμπορικές υπηρεσίες σε τρίτους, δεν κάνουν δηλαδή εμπορική εκμετάλλευση του δικτύου, αλλά χρήση μόνο από τα μέλη τους. Μια εικόνα της ελληνικής ασύρματης κοινωνίας μπορείτε να έχετε, εάν ψάξετε στο Διαδίκτυο με τους κωδικούς Hellas Wireless Network.
Οι κύριες εφαρμογές των ελληνικών WLAN εντοπίζονται στα εξής: Τη δημιουργία hotspots και επομένως την εξυπηρέτηση κινούμενων χρηστών εντός μικρών και συγκεκριμένων περιοχών. Τη δημιουργία ζεύξεων σημείου προς σημείο με συγκεκριμένη χρήση. Την αντικατάσταση του ενσύρματου δικτύου στο οικιακό ή το επιχειρηματικό περιβάλλον.
Με την υπ. αριθμ. 12197/344/25-02-2004 Κοινή Υπουργική Απόφαση των Υπουργών Οικονομίας & Οικονομικών και Μεταφορών & Επικοινωνιών, προκηρύχθηκε το Πρόγραμμα "Χρηματοδότηση Επιχειρήσεων για τη δημιουργία Σημείων Ασύρματης Ευρυζωνικής Πρόσβασης (WIRELESS HOTSPOTS)" στο πλαίσιο του Μέτρου 4.2 "Ανάπτυξη Υποδομών Δικτύων Τοπικής Πρόσβασης" του Επιχειρησιακού Προγράμματος Κοινωνία της

Πληροφορίας. Στο πρόγραμμα μπορούν να συμμετάσχουν επιχειρήσεις που επιθυμούν να αξιοποιήσουν τις τεχνολογίες των ασύρματων δικτύων, με σκοπό την παροχή δικτυακών ή διαδικτυακών υπηρεσιών προστιθέμενης αξίας, σε χρήστες που κινούνται στο χώρο κάλυψης τους επισκέπτες, φιλοξενούμενους και εργαζόμενους.

5.4) ΑΠΟΣΤΑΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

Από αυτά τα πειράματα μαζί με άλλα που έχουν γίνει πάνω σε ανθρώπινα ομοιώματα, μετρώντας την άνοδο της θερμοκρασίας που η ακτινοβολία προκαλούσε και συνυπολογίζοντας το Specific Absorption Rate (SAR)(μέτρο που έχει καθορίσει η FCC (Federal Communications Commission [24]) για το ποσοστό απορρόφησης της ακτινοβολίας από το σώμα) βρέθηκαν (όπως αναλύεται και στις διαφάνειες του κ. Νικήτα Γιαννάκου[10]) τα ακόλουθα μεγέθη για την ένταση του πεδίου σε σχέση με τα όρια του ανθρώπινου οργανισμού:
1 μέχρι 10 mW/cm2 Είναι επιτρεπτή η έκθεση λίγες ώρες κάθε 24ωρο
Πάνω από 10 mW/cm2 ΕΠΙΚΙΝΔΥΝΗ ΑΚΤΙΝΟΒΟΛΙΑ.
Το προσωπικό δεν πρέπει να εκτίθεται σε ακτινοβολία αυτού του μεγέθους.
Έργο «Προώθηση της ευρυζωνικής πρόσβασης Επιπτώσεις ασύρματωνδικτύων στους νομούς της Περιφέρειας Πελοποννήσου» επικοινωνιών στην δημόσια υγεία 29 Ιουνίου 2005 Σελίδα 15 © Πανεπιστήμιο Πελοποννήσου.
Αυτό πρακτικά σημαίνει ότι αν υπερβούμε το 1mW/cm2 η άνοδος της θερμοκρασίας θα μας προκαλέσει μη αντιστρεπτή μεταβολή στα κύτταρα μας.
Επίσης άλλες έρευνες, χρησιμοποιώντας τα δεδομένα από την FCC, έχουν καταλήξει ότι μπορούμε να υπολογίσουμε μια απόσταση ασφαλείας για κάθε πηγή σύμφωνα με τον παρακάτω τύπο :
Rmin = .N 10(G-L)/10 P
.4 π S
όπου
• G το κέρδος (gain) της κεραίας
• P η ισχύς εισόδου στην κεραία
• L απώλειες (dB) μεταξύ πομπού - κεραίας
• N αριθμός πομπών συνδεδεμένοι με την κεραία
• S μέγιστη επιτρεπόμενη πυκνότητα ισχύος (W/m2)
Υπολογίζοντας μάλιστα για κάποιες ενδεικτικές τιμές έχουμε
Ισχύς (W) Επικίνδυνη
Απόσταση (m)
Απόσταση
Ασφαλείας (m)
1 0.2 0.3
4 0.2 0.6
10 0.3 0.95

40 0.6 2.0
400 1.9 6.0
1000 3.0 9.5
έτσι σε πραγματικές συνθήκες, ανάλογα με την περίπτωση, υπολογίζουμε ότι
• Ένα WiFi τερματικό, όπου η EIRP περιορίζεται εκ του νόμου στα 100mW,
δηλαδή 0,1Watt έχει απόσταση ασφαλείας τα 10cm
• Ένα κινητό GSM εκπέμπει 1 με 2 Watt (όταν είναι μακριά από το σταθμό
βάσης του), άρα η απόσταση ασφαλείας είναι 30cm
• Μία κεραία κινητής τηλεφωνίας στη χειρότερη περίπτωση έχει 40Watt ισχύ, με κέρδος κεραίας 10db, άρα EIRP=400Watt, άρα η ελάχιστη απόσταση είναι 6 μέτρα
• Ένας πομπός ραδιοφώνου ή τηλεόρασης με ισχύ 30000Watt έχει ελάχιστη απόσταση 30μέτρα.
Εύκολα μπορούμε να διαπιστώσουμε πως η ισχύς εκπομπής καθώς και η απόσταση ασφαλείας των ασυρμάτων δικτύων είναι κατά πολύ μικρότερα αυτών των κινητών τηλεφώνων. Από τα παραδείγματα βλέπουμε πως μια κεραία ασυρμάτων δικτύων εκπέμπει στα 0,1Watt, ενώ μια κεραία κινητής τηλεφωνίας στα 40Watt, με αποστάσεις ασφαλείας 10cm στα ασύρματα και 6 μέτρα στα κινητά !
Έργο «Προώθηση της ευρυζωνικής πρόσβασης Επιπτώσεις ασύρματωνδικτύων στους νομούς της Περιφέρειας Πελοποννήσου» επικοινωνιών στην δημόσια υγεία 29 Ιουνίου 2005 Σελίδα 16 © Πανεπιστήμιο Πελοποννήσου.
Επιπρόσθετα, να σημειώσουμε ότι για μία απόσταση 1 μέτρου η ένταση πεδίου θα είναι 10000 φορές μικρότερη από το όριο ασφαλείας και για μία απόσταση 10 μέτρων θα είναι 1000000 φορές μικρότερη. Άρα καταλαβαίνουμε ότι σε μία απόσταση ενός μέτρου από την κεραία ασυρμάτων δικτύων η ένταση πεδίου είναι ελάχιστη !

5.5) ΑΝΑΚΕΦΑΛΑΙΩΣΗ-ΠΕΡΙΛΗΨΗ

Οι ασύρματες τεχνολογίες πρόσβασης χρησιμοποιούνται για να αντικαταστήσουν ή να επεκτείνουν ένα κοινό ενσύρματο δίκτυο (Ethernet) και επιτρέπουν στον κινητό χρήστη την ασύρματη μετάδοση και λήψη δεδομένων.

Τα Ασύρματα Τοπικά Δίκτυα (WLANs) ακολουθούν το πρότυπο IEEE 802.11, το πρώτο πρότυπο για ασύρματη δικτύωση το οποίο

αναπτύχθηκε. Τα ασύρματα τοπικά δίκτυα τα οποία είναι συμβατά με το πρότυπο IEEE 802.11 ονομάζονται και δίκτυα Wi - Fi.

Τα βασικά στοιχεία ενός δικτύου IEEE 802.11 είναι:

- Station (STA): Ένας προσωπικός υπολογιστής ή μια συσκευή με ασύρματη σύνδεση.

- Access Point (AP): Η γέφυρα μεταξύ του ασύρματου και του ενσύρματου LAN.

- Basic Service Set (BSS): Σύνολο από STAs τα οποία επικοινωνούν μέσω του ίδιου καναλιού στην ίδια περιοχή.

- Extended Service Set (ESS): Ένα σύνολο από BSSs και ενσύρματα LANs.

Όσον αφορά την αρχιτεκτονική - τοπολογία τους τα δίκτυα αυτά εμφανίζονται με δύο μορφές. Τη δομημένη (Infrastructure) και την τυχαία (Ad - hoc).

Τα πιο κοινά WLANs λειτουργούν στη μη αδειοδοτημένη περιοχή συχνοτήτων ISM (Industrial, Scientific and Medical) των 2,4 GHz και στην UNII (Unlicensed National Information Infrastructure) μπάντα των 5 GHz.

- Τα IEEE 802.11b WLANs λειτουργούν στη ζώνη 2,4 - 2.4835 GHz.

- Το πρότυπο IEEE 802.11a χρησιμοποιεί την περιοχή των 5 GHz UNII. Αυτή η περιοχή έχει εύρος 300 MHz και είναι χωρισμένη σε δύο υποπεριοχές. Η χαμηλότερη υποπεριοχή επεκτείνεται από 5,15 MHz ως 5,35 MHz. Η ανώτερη υποπεριοχή είναι από 5.725 MHz ως 5.825 MHz (η ΕΕΤΤ δεν έχει δώσει άδεια χρήσης της στην Ελλάδα).

Στο φυσικό επίπεδο προδιαγράφονται δύο τεχνικές διαμόρφωσης (Απλωμένου Φάσματος):

- FHSS (Frequency Hopping Spread Spectrum)

- DSSS (Direct Sequence Spread Spectrum)

Και στις δύο υποστηρίζονται ρυθμοί μετάδοσης 1 και 11Mbps στην ζώνη συχνοτήτων 2.4 - 2.4835GHz.

Στην ζώνη συχνοτήτων 5GHz η τεχνική η οποία χρησιμοποιείται είναι η Orthogonal Frequency Division Multiplexing (OFDM). Οι ρυθμοί μετάδοσης μπορούν να αγγίξουν τα 54Mbps

Με σκοπό τη βελτίωση και την εξέλιξη του προτύπου δημιουργήθηκαν κατά την διάρκεια των χρόνων, εξελίξεις του προτύπου που διαφορετικά ονομάζονται και υποπρότυπα. Τα πιο γνωστά από αυτά είναι:

- IEEE 802.11 a: Χρησιμοποιεί τη ζώνη των 5 GHz και OFDM . Ταχύτητα:<54M bps
- IEEE 802.11 b (Χρησιμοποιείται στην Ελλάδα): Χρησιμοποιεί τη ζώνη των 2.4 GHz και DSSS . Ταχύτητα:<11M bps
- IEEE 802.11 e: Παρέχει εγγυήσεις για ποιότητα υπηρεσίας
- IEEE 802.11f: Κινητικότητα των σταθμών μέσα σε ένα IP δίκτυο (Intra - network Handover)
- IEEE 802.11 g: Επεκτείνει το 802.11 b ώστε να προσεγγίζει ταχύτητες υψηλότερες από 11M bps
- IEEE 802.11 i: Πρότυπο το οποίο μελετά θέματα ασφάλειας στα WLANs
- IEEE 802.11 h: Η ομάδα αυτή θα προσπαθήσει να εισάγει στο 802.11 a την δυνατότητα για καλύτερο έλεγχο συγκρούσεων.Γνωστοτερα προτυπα είναι τα:WI-FI,WI-WAN,WI-MAN,PERSONAL,HiperLan1&2.

Το 2003 η IEEE υιοθέτησε το πρότυπο 802.16 γνωστό και σαν Wi - Max , ώστε να ικανοποιήσει τις απαιτήσεις για ασύρματη πρόσβαση (με σταθερούς ρυθμούς) ευρείας ζώνης. Όπως συμβαίνει με τα πρότυπα 802 για ασύρματα τοπικά δίκτυα LAN , έτσι και το 802.16 καθορίζει μια οικογένεια προτύπων.Λέγεται ότι το Wi - Max θα αποτελέσει το κατεξοχήν πρότυπο για ασύρματη δικτύωση στο μέλλον.

Firewall αποκαλείται το λογισμικό που ελέγχει ή και απαγορεύει την απομακρυσμένη πρόσβαση σε ένα υπολογιστή

Η κρυπτογράφηση εξασφαλίζει το απόρρητο των προσωπικών πληροφοριών. Πρόκειται για μια επιστήμη που βασίζεται στα μαθηματικά για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων. Η κρυπτογράφηση για τα ασύρματα δίκτυα γίνεται μέσω του WEP (Wired Equivalent Privacy).

Η πολιτική ασφάλειας ασύρματων δικτύων θα πρέπει να καλύπτει όλο τον ασύρματο εξοπλισμό, όπως σημεία πρόσβασης (access points), υπολογιστές με ασύρματες κάρτες, υπολογιστές παλάμης κ.λπ. που συνδέονται στο εταιρικό δίκτυο.Η επιρροη της Η/Μ ακτινοβολιας στον ανθρωπο από τα ασυρματα δικτυα είναι μηδαμηνη.

Μεχρι σημερα στην Ελλαδα δεν εχει επιτραπει η χρηση των 2,4GHz για σταθερη ασυρματη προσβαση.

Κυριοτερες ασυρματες κοινοτητες στην Ελλαδα είναι το Ασυρματο Μητροπολιτικο Δικτυο Αθηνων και το Ακαδιμαικο Ασυρματο Δικτυο Ηρακλειου.

Τα πλεονεκτηματα των ασυρματων δικτυων είναι πολλα και οι εφαρμογες τους επισης πολλες. Ειναι αναμφησβητητο γεγονος ότι το μελλον των δικτυων είναι ασυρματο!

ΠΑΡΑΡΤΗΜΑ

Ακρωνύμια

AP Access Point
BPSK Binary Phase Shift Keying
BSS Basic Service Set
CCK Complementary Code Keying
CRC Cyclic Redundancy Check
CSMA/CA Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD Carrier Sense Multiple Access with Collision Detection
CTS Clear to Send
DCF Distribution Coordination Function
DHCP Dynamic Host Configuration Protocol
DS Distribution system
DSSS direct sequence spread spectrum
ESS Extended Service Set
ETSI European Telecommunications Standards Institute
FCC Federal Communications Commission (USA)
FHSS Frequency Hopping Spread Spectrum
IBSS Independent Basic Service Set
IEEE Institute of Electrical and Electronics Engineers
IETF Internet Engineering Task Force IP Internet Protocol
IPSec Internet Protocol Security
ISA Integrated Services Architecture
ISM Industry, Scientific, and Medical
ISO International Organization for Standardization
LLC Logical Link Control
MAC Media Access Control
MIB Management information base
MKK Radio Equipment Inspection and Certification Institute (Japan)
NIC Network interface card
NOS Network operating system
PCF Point Coordination Function
PCI Peripheral Component Interconnect
PRNG Pseudo Random Number Generator
QPSK Quadrature Phase Shift Keying
RC4 Ron□s Code or Rivest□s Cipher
RTS Request to Send
SNMP Simple Network Management Protocol
TCP/IP Transmission Control Protocol/Internet Protocol
WECA Wireless Ethernet Compatibility Alliance
WEP Wired Equivalent Privacy
WLAN Wireless Local Area Network
WLANA Wireless LAN Alliance

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. B. Crow et al., "IEEE 802.11 Wireless Local Area Networks "– IEEE Communications Magazine-September 1997.
2. S. Mangold et al., "IEEE 802.11e Wireless LAN for Quality of Service" in Proc.
European Wireless '02, Florence, Italy, February 2002.
3. Banchs et al., "Providing Throughput Guarantees in IEEE 802.11e Wireless
LANS"- In. Proc. of the 18th International Teletraffic Congress (ITC-18), North Holland, 2003.
4. . Giuseppe Bianchi,"Performance Analysis of the IEEE 802.11 Distributed
Coordination Function," IEEE Journal on Selected Areas in Communications, vol
18, Mar.2000.
5. T.S. Ho and K.C. Chen, "Performance evaluation and enhancement of the
CSMA/CA MAC Protocol for 802.11 wireless LAN's", in Proceedings of IEEE
PIRMC, Tapei, Taiwan, Oct.1996.
6. Brian P. Crow, Indra Widjaja, Jeong Geun Kim, Prescott T. Sakai, "IEEE
802.11 Wireless Local Area Networks," IEEE Communications Magazine, September 1997.
7. Jangeun Jun et al., " Theoretical Maximum Throughput of IEEE 802.11 and its
Applications"
8. A.S. Tanenbaum, "Computer Networks", 4th ed. Prentice- Hall, 2002
9. "The Network Simulator –ns-2," http://www.isi.edu/nsnam/ns/, Online Link.
10. M. Ergen and P. Varaiya, "Throughput Formulation and WLAN Optimazation in
Mixed Data Rates for IEEE 802.11 DCF Modes".
11. M. Ergen, " IEEE 802.11 Tutorial ", http://www.eecs.berkeley.edu
12. M. Ergen, "I-WAN: Intelligent Wireless Local Area Networking", PhD. Thesis,
November 2004.
13. M. Ergen and P. Varaiya , "Throughput Analysis and Admission Control for
IEEE 802.11a"
14. Jie Hui and Mihail Devestikiotis "Performance Analysis of IEEE 802.11e EDCA
by a Unified Model "
48
15. Dali Xiao and Kang G.Shin,"Achieving Efficient Channel Utilization and
Weighted Fairness for Data Communication in IEEE 802.11WLAN under the

DCF", in Proc. of IWCQoS'2002, May 2002.
16. G. Bianchi,"Performance Analysis of the IEEE 802.11 Distributed Coordination
Function", IEEE J. Select, Areas Commun, 2000.
17. F. Cali et al., "Dynamic Tuning of the IEEE 802.11 Protocol to Achieve a
Theoretical Throughput Limit "in Proc. of INFOCOM '98, San Francisco, CA,
March 1998.
18. S. Choi et al., "IEEE 802.11e Contention –Based Channel Access (EDCF)
Performance Evaluation", in Proc. of IEEE ICC'03, 2003.
19. Stefan Mangold," Analysis of IEEE 802.11e and Application of Game Models for
Support Quality of Service in Co-existing Wireless Networks", PhD. Thesis, June
2003.
20. D.J Leith and P.Clifford, "Using the 802.11e EDCF to Achieve TCP Upload
Fairness over WLAN Links "
21. Vasilios A. Siris and Panagiotis Alafouzos, "Throughput Differentiation for TCP
Uplink Traffic in IEEE 802.11e Wireless LANs", in Proc. of IEEE LANMAN 2005.
22. Rafaelo Bruno, Marco Conti and Enrico Gregori, "Analytical Modeling of TCP
Clients in Wi-Fi Hot Spot Networks".
23. Mobile Communications – Jochen Schiller
24. www.computer.org/students/looking/summer97/ieee802.htm