ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΚΡΗΤΗΣ
ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ ΕΠΙΛΟΓΗΣ
ΤΕΧΝΟΛΟΓΙΑ ΙΑΤΡΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

"Μελέτη, ανάλυση, υλοποίηση και αξιολόγηση Ασύρματου Ευρυζωνικού Δικτύου Πρόσβασης (Wireless Broadband Access Network) για τη μεταφορά ιατρικών δεδομένων."

Εισηγητής: Δρ.Ε.Πάλλης

Σπουδαστές: Κων/νος Πομποδάκης
Εμμ.Κατσανεβάκη

Ηράκλειο Μάιος 2004

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ…….....σελ.7

ΚΕΦΑΛΑΙΟ 1ο
-1.1 ΤΗΛΕΪΑΤΡΙΚΗ ……σελ.8
1.1.1 Τηλεακτινολογία.....σελ.10
1.1.2 Τηλεκαρδιολογία……σελ.11
1.1.3 Τηλεπαθολογία……....σελ.11
1.1.4 Τηλεδερματολογία……..σελ.11
1.1.5 Τηλεοφθαλμολογία……σελ.12
1.1.6 Τηλεχειρουργική……σελ.13
1.1.7 Τηλεεκπαίδευση……..σελ.12
1.2 ΥΠΗΡΕΣΙΕΣ ΑΜΕΣΗΣ ΒΟΗΘΕΙΑΣ-ΕΠΕΙΓΟΥΣΑ ΙΑΤΡΙΚΗ σελ.14
1.2.1Ιατρικός Εξοπλισμός κατάλληλος για εφαρμογές Τηλεϊατρικής……σελ.15
1.2.2 Ποιότητα ιατρικών στοιχείων……...σελ.17
1.3 ΕΝΔΟΝΟΣΟΚΟΜΙΑΚΑ ΣΥΣΤΗΜΑΤΑ……...σελ.17
1.3.1 Αυτοματοποιημένα συστήματα νοσοκομείου……...σελ.18

ΚΕΦΑΛΑΙΟ 2ο
2.1 ΠΡΟΤΥΠΑ ΓΙΑ ΗΛΕΚΤΡΟΝΙΚΗ ΑΝΤΑΛΛΑΓΗ ΙΑΤΡΙΚΩΝ ΔΕΔΟΜΕΝΩΝ……σελ.19
2.1.1 Οργανισμοί δημοσίευσης προτύπων……σελ.19
2.1.2 ITU-T προδιαγραφές……..σελ.20
2.1.3 Προδιαγραφές για ήχο……σελ.21
2.1.4 Προδιαγραφές για εικόνα……...σελ.21
2.1.5 HL7……..σελ.21
2.1.6 Χαρακτηριστικά μεγέθη ιατρικών δεδομένων-απαιτήσεις ιατρικών εφαρμογών.....σελ.22

ΚΕΦΑΛΑΙΟ 3ο
3.1 ΕΙΣΑΓΩΓΗ ΣΤΑ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ……..σελ.24

3.2 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΑΣΥΡΜΑΤΗΣ ΔΙΚΤΥΩΣΗΣ.....σελ.25
3.2.1 Κινητικότητα (mobility)……σελ.25
3.2.2 Ταχύτητα και ευελιξία εγκατάστασης…….....σελ.25
3.2.3 Επεκτασιμότητα……..σελ.26
3.2.4 Διασύνδεση……..σελ.26
3.2.5 Συμβατότητα……...σελ.26
3.2.6 Μειωμένο κόστος.....σελ.27
3.2.7 Νομαδική πρόσβαση……...σελ.27

ΚΕΦΑΛΑΙΟ 4ο
4.1 WLANs, ΤΕΧΝΟΛΟΓΙΕΣ ΔΙΑΔΟΣΗΣ……..σελ.28
4.1.1 Φάσμα και Οργανισμοί Πρότυποποίησης……σελ.28

4.2 ΤΕΧΝΟΛΟΓΙΕΣ WLAN……..σελ.29
4.2.1 Το πρότυπο IEEE 802.11……...σελ.29
4.2.2 High Performance Radio LAN (HIPERLAN)……σελ.30

4.2.3 Home RF…… σελ.32
4.2.4 Τεχνολογία Bluetooth……σελ.34
4.3 LMDS……..σελ.36
4.3.1 Αρχιτεκτονική δικτύου LMDS……..σελ.37
4.3.2 Οφέλη……...σελ.37
4.3.3 Παράδειγμα χρήσης LMDS……...σελ.38
4.4 MMDS…….....σελ.38

ΚΕΦΑΛΑΙΟ 5ο

5.1 IEEE 802.11 WLAN……..σελ.41
5.1.1 Αρχική προσπάθεια……σελ.41
5.1.2 Βασική διαμόρφωση……σελ.41
5.1.3 Point-to-multipoint……...σελ.41
5.1.4 Point-to-point……σελ.42
5.1.5 Επιλογή συχνότητας……σελ.43
5.1.6 Περιβάλλον……σελ.43
5.1.7 Αναγνώριση κίνησης από το 802.11……...σελ.43
5.2 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ IEEE 802.11……σελ.44
5.2.1 Δικτύωση ειδικού σκοπού (ad-hoc networking)……....σελ.44
5.2.2 Κυψελωτή Αρχιτεκτονική……...σελ.45
5.3 ΦΥΣΙΚΟ ΣΤΡΩΜΑ 802.11……σελ.48
5.3.1 Η αρχιτεκτονική του φυσικού στρώματος……....σελ.48
5.3.2 Λειτουργίες του φυσικού στρώματος (Physical Layer Operations)σελ.49
5.3.2α Ανίχνευση φέροντος……σελ.50
5.3.2β Λειτουργία μετάδοσης……σελ.50
5.3.2γ Λειτουργία λήψης……σελ.50
5.4 ΤΟ ΦΥΣΙΚΟ ΣΤΡΩΜΑ ΤΟΥ 802.11 ΜΕ ΧΡΗΣΗ ΤΗΣ ΤΕΧΝΙΚΗΣ SPREAD SPECTRUM.....σελ.51
5.4.1 Εξάπλωση σήματος, στην περιοχή των συχνοτήτων με χρήση της τεχνικής spread spectrum.....σελ.51
5.4.2 Το υπόστρωμα PMD FHSS……..σελ.52
5.5 FREQUENCY –HOPPING SPREAD SPECTRUM (τεχνική διαμόρφωσης με μεταπήδηση συχνοτήτων)……σελ.52
5.5.1 Κατανομή συχνότητας του 802.11……...σελ.53
5.5.2 Η λειτουργία διαμόρφωσης συχνότητας FHSS……σελ.54
5.6 DIRECT SEQUENCE SPREAD SPECTRUM (DSSS)……...σελ.56
5.6.1 DSSS με χρήση BPSK διαμόρφωσης……..σελ.59
5.6.2 Υποστήριξη πολλών χρηστών……..σελ.59
5.6.3 Οι βελτιώσεις στο φυσικό επίπεδο που εισάγει το πρότυπο 802.11b….σελ.59
5.7 MAC LAYER……σελ.60
5.7.1 Υποστήριξη για δεδομένα που εξαρτώνται άμεσα από το χρόνο…....σελ.62
5.7.2 Διαχείριση ισχύος……..σελ.63
5.8 OPERATION……σελ.63
5.8.1 Active Scanning……σελ.63
5.8.2 Passive Scanning……σελ.63
5.8.3 Authentication και Association……....σελ.64
5.9 ROAMING……σελ.59
5.9.1 Comparison With Cellular……...σελ.65
5.9.2 Operation……...σελ.66
5.9.3 Basic Access Method……σελ.66

5.9.4 Minimizing Collisions……σελ.66
5.10 FRAME TYPES……...σελ.68

ΚΕΦΑΛΑΙΟ 6ο

6.1 ΚΑΤΗΓΟΡΙΕΣ WLAN 802.11…….σελ.73
6.1.1 802.11a……σελ.73
6.1.2 802.11d……σελ.73
6.1.3 802.11g……σελ.73
6.1.4 802.11h ……...σελ.73
6.1.5 802.11i……σελ.74
6.1.6 802.11e……σελ.74
6.1.7 802.11x……σελ.74

ΚΕΦΑΛΑΙΟ 7ο

7.1 ΑΣΦΑΛΕΙΑ WLAN……σελ.75
7.1.1 Υποκλοπή……...σελ.75
7.1.2 Αξιοπιστία μεταφοράς…….....σελ.75
7.1.3 Υποδομή……σελ.76
7.1.4 Άρνηση εξυπηρέτησης……..σελ.76
7.2 ΜΕΘΟΔΟΙ ΑΣΦΑΛΕΙΑΣ ΤΟΥ 802.11…….σελ.77
7.2.1 SSID (Service set identifier)……..σελ.77
7.2.2 MAC Address Filtering……σελ.77
7.2.3 WEP - Based Security……σελ.78
7.3 ΚΡΥΠΤΟΓΡΑΦΙΑ, ΓΕΝΙΚΑ……..σελ.78
7.4 ΤΟ ΠΡΩΤΟΚΟΛΛΟ WEP ΤΟΥ 802.11……σελ.80
7.4.1 Authentication……σελ.81
7.4.2 RC4……σελ.83
7.4.3 Δίκτυα με υψηλές απαιτήσεις ασφάλειας……....σελ.83
7.4.4 Ασύρματη ασφάλεια με χρήση της τεχνικής VPN (Virtual Privet Network)……..σελ.83
7.5 ΑΔΥΝΑΜΙΕΣ – ΤΡΩΤΑ ΣΗΜΕΙΑ……σελ.85

ΚΕΦΑΛΑΙΟ 8ο

8.1 ΔΟΜΙΚΑ ΣΤΟΙΧΕΙΑ WLAN……..σελ.87
8.1.1 Συσκευές χρηστών……σελ.87
8.1.2 Ασύρματες τοπικές γέφυρες (Wireless Local Bridges)…...σελ.87
8.1.3 Ασύρματες κάρτες δικτύου,-Network interface card (NIC).σελ.87
8.1.4 Κεραίες……....σελ.88

ΚΕΦΑΛΑΙΟ 9ο

9.1 ΣΧΕΔΙΑΣΜΟΣ ΚΑΙ ΥΛΟΠΟΙΗΣΗ ΔΙΚΤΥΟΥ……...σελ.89
9.2 Ο ΔΡΟΜΟΛΟΓΗΤΗΣ NAT……σελ.90
9.3 ΤΟ ΠΡΩΤΟΚΟΛΛΟ DHCP……σελ.92
9.3.1 Συνοπτική περιγραφή λειτουργίας του DHCP……....σελ.93
9.4 ΔΙΚΤΥΑΚΕΣ ΣΥΣΚΕΥΕΣ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΗΘΗΚΑΝ……σελ.93
9.5 ΑΠΟΤΕΛΕΣΜΑΤΑ ΜΕΤΡΗΣΕΩΝ……...σελ.95
9.6 Συμπεράσματα – Προτάσεις……...σελ.108
Λεξικό όρων-συντομογραφίες……..σελ112

ΠΕΡΙΕΧΟΜΕΝΑ ΣΧΗΜΑΤΩΝ & ΠΙΝΑΚΩΝ

Σχήμα 1: Παραδείγματα πιθανών εφαρμογών και ευρύτερης χρήσης
Σχήμα 2: Παράδειγμα ασύρματης δικτύωσης γειτονικών κτιριακών συγκροτημάτων

Σχήμα 3: Εφαρμογή Τηλεϊατρικής

Σχήμα 4: Πιθανή αρχιτεκτονική εφαρμογής WLAN, σε ιατρικό περιβάλλον.

Σχήμα 5: Μπλοκ διάγραμμα ενός ασύρματου συστήματος Τηλεϊατρικής

Πίνακας 6 : ITU-T προδιαγραφές
Πίνακας 7: Κατηγορίες Video συμπίεσης MPEG-2 format

Σχήμα 8: Το ηλεκτρομαγνητικό φάσμα

Σχήμα 9:Μπάντα των ISM

Σχήμα 10: Τα επίπεδα που καλύπτονται από το πρότυπο 802.11

Σχήμα 11: Τα επίπεδα του HIPERLAN, συσχετιζόμενα με τα αντίστοιχα του OSI

Πίνακας 12: Πρότυπα HIPERLAN

Πίνακας 13: Τεχνολογίες WLAN- Συγκριτικά στοιχεία

Σχήμα 14 : Προέλευση SWAP

Σχήμα 15: Χαρακτηριστική οργάνωση σύνδεσης Bluetooth

Σχήμα 16: Αρχιτεκτονική Blouetooth

Σχήμα 17: LMDS System

Σχήμα 18: LMDS System

Σχήμα 19 : Σύστημα MMDS

Σχήμα 20: Σύστημα MMDS

Σχήμα 21: Δίκτυο Point-to-point

Σχήμα 22: α) Ασύρματο δίκτυο το οποίο υποστηρίζει LAN extension και νομαδική πρόσβαση. β)Ad Hoc Wireless LAN

Σχήμα 23 : Extended Service Set

Σχήμα 24: Κυψέλη ασύρματου LAN (BSS)

Σχήμα 25 : Εκτεταμένη Μονάδα Υπηρεσιών Extended Service Set (ESS)

Σχήμα 26: ESS (Distribution System που ενσωματώνει δυο BSS)

Σχήμα 27: Επίπεδα 802.11

Σχήμα 28: Η αρχιτεκτονική του υποστρώματος MAC και του φυσικού στρώματος όπως αυτή καθορίζεται από το 802.11

Σχήμα 29: Τεχνική Spread Spectrum

Σχήμα 30: Εξάπλωση σήματος, στην περιοχή των συχνοτήτων με χρήση της τεχνικής spread spectrum.
Σχήμα 31: Μοντέλο ενός συστήματος Spread Spectrum

Πίνακας 32:Κατανομή συχνοτήτων και επιτρεπόμενα επίπεδα ισχύος

Σχήμα 33: Κατανομή των Καναλιών FHSS στο φάσμα συχνοτήτων.

Σχήμα 34: Ακολουθία μεταπήδησης συχνότητας σε συνάρτηση με το χρόνο

Σχήμα 35: Η διαμόρφωση GFSK

Σχήμα 36: Frame Format

Σχήμα 37: Διαμόρφωση και αποδιαμόρφωση με τεχνική DSSS

Σχήμα 38: Σχηματική αναπαράσταση ενός DSSS πομπού

Σχήμα 39: Αναπαράσταση ενός bit από μια ακολουθία θετικών και αρνητικών μονάδων

Σχήμα 40: Μετάδοση δεδομένων με χρήση της τεχνικής DBPSK

Σχήμα 41: Διασύνδεση backbone network με BSS

Σχήμα 42: Επικαλυπτόμενες κυψέλες

Σχήμα 43: Διαδικασία ανίχνευσης και σύνδεσης

Σχήμα 44: Παράδειγμα Roaming
Σχήμα 45: Network Allocation Vvector-δείκτης παραχώρησης δικτύου (NAV)

Σχήμα 46: Φαινόμενο κρυμμένου σταθμού

Σχήμα 47: MAC Data Format

Πίνακας 48: Πιθανές ακολουθίες Type και Subtype subfield

Σχήμα 49: Διαδικασία τεμαχισμού των πλαισίων

Σχήμα 50: Λειτουργία Roaming

Σχήμα 51: Κρυπτογράφηση απλού κειμένου

Σχήμα 52: Συμμετρική Κρυπτογραφία με shared key

Σχήμα 53: WEP, encryption

Σχήμα 54: WEP decryption

Σχήμα 55: WEP data frames

Σχήμα 56: shared key authentication

Σχήμα 57: Ασφάλεια VPN του 802.11

Σχήμα 58: Μετάφραση διευθύνσεων Δικτύου NAT-Network Address Translation

Σχήμα 59: 1η πρόταση υλοποίησης WLAN

Σχήμα 60: 2η πρόταση υλοποίησης WLAN

Εικόνα 61: Ψηφιακό οπτικό παράθυρο ψηφιακής αγγειογραφίας σε σμίκρυνση

Σχήμα 62: Σταθμός τηλεμετρίας

Σχήμα 63: Παράδειγμα ασύρματης δικτύωσης κλινικής 2 ορόφων

Σχήμα 64: Πρόταση για τη χρήση της κατηγορίας 802.11 σε Νοσοκομειακό περιβάλλον

ΕΙΣΑΓΩΓΗ

Η δικτύωση των υπολογιστών στα επιχειρησιακά περιβάλλοντα αποτελεί πλέον υπόθεση καθημερινής ρουτίνας, τα δε οφέλη της είναι πολύπλευρα και αναγνωρισμένα, ακόμα και για περιβάλλοντα πολύ μικρών εταιριών πόσο μάλλον δε, σε εκπαιδευτικά ή νοσοκομειακά ιδρύματα.

Η κοινωνία της πληροφορίας είναι πλέον πραγματικότητα και η κύρια πηγή άντλησης δεδομένων είναι το διαδίκτυο. Αυτή και μόνο η δυνατότητα, της πρόσβασης στο Διαδίκτυο, αποτελεί πρωτογενή ανάγκη κάθε εργαζόμενου – φοιτητή –επιστήμονα – ερευνητή.

Εδώ και χρόνια η δικτύωση με συμβατικές ενσύρματες τεχνολογίες, σε νοσοκομειακά περιβάλλοντα, δίνει λύσεις που αφορούν πάρα πολλούς τομείς δραστηριοτήτων, του νοσοκομειακού-ιατρικού προσωπικού, όπως: λογιστικές εφαρμογές, αρχειοθέτηση, βάσεις δεδομένων, έλεγχος αποθηκών -φαρμακείων-αναλωσίμων, αποστολή εργαστηριακών εξετάσεων, έλεγχος προσωπικού-επικοινωνία, ενδοεπικοινωνία, εκπαιδευτικούς σκοπούς, στατιστικές μελέτες, τηλεϊατρικές εφαρμογές.

Η εγκατάσταση ενός επιχειρησιακού δικτύου είναι πια απλή υπόθεση, η οποία ωστόσο πρέπει να γίνει με προσεκτικά βήματα τόσο κατά την επιλογή εξοπλισμού όσο και κατά τη σχεδίαση της τοπολογίας του δικτύου

Ασύρματα δίκτυα υπάρχουν εδώ και αρκετά χρόνια από διάφορους κατασκευαστές, αλλά η ταχύτητα που προσέφεραν (1,5Mbps) ήταν μικρή και δεν υπήρχε συμβατότητα μεταξύ τους.

Την τελευταία δεκαετία πολλά είναι τα πρότυπα που διεκδικούν ένα κομμάτι της αγοράς. Bluetooth, HiperLAN, HomeRF, 802.11a, 802.11b, 802.11g

Ένας από τους σημαντικότερους παράγοντες που βοήθησε στο γεγονός της συνεχόμενης ανάπτυξης της ασύρματης δικτύωσης, ήταν η συνεχής βελτίωση-στα πολύ μεγάλης κλίμακας ολοκλήρωσης- ηλεκτρονικά κυκλώματα, τα γνωστά VLSI (Very Large Scale Integration), τα οποία οδήγησαν σε μείωση του μεγέθους, της κατανάλωσης ισχύος και του κόστους των κυκλωμάτων υψηλών συχνοτήτων (RF-Radio Frequency). Επίσης, οι νέες τεχνικές ψηφιακής επεξεργασίας σημάτων (DSP), οι βελτιωμένες κεραίες (smart antennas) και οι αλγόριθμοι κωδικοποίησης για διόρθωση λαθών (error correction), συνέβαλαν επίσης στην ασύρματη «επανάσταση»

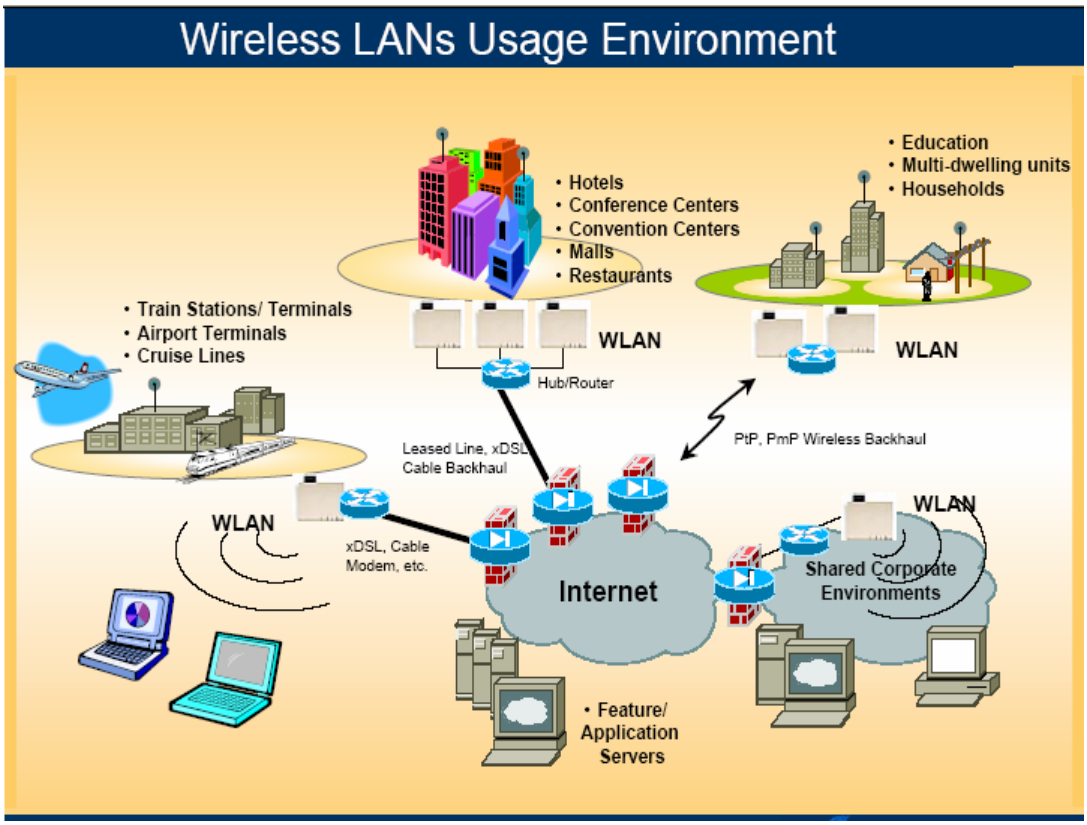
Η διείσδυση των τεχνολογιών αιχμής στον Ιατρικό κόσμο καταρρίπτει τα αντικειμενικά εμπόδια του παρελθόντος, που δημιουργούν η απόσταση και ο χρόνος, ενώ παράλληλα προσφέρει τα απαραίτητα εργαλεία και μεθόδους για την παροχή αναβαθμισμένων υπηρεσιών πρωτοβάθμιας φροντίδας υγείας. Αξίζει να σημειωθεί ότι οι υπηρεσίες αυτής της μορφής είναι καινοτόμες όχι μόνο για την Ελλάδα και την Ευρώπη , αλλά για όλο τον υπόλοιπο κόσμο. Είναι ένα ιδιαίτερα χρήσιμο εφόδιο τόσο για τους πολίτες όσο και για τους επιστήμονες διότι τους επιτρέπει την άσκηση της ιατρικής με τρόπους που συναρτώνται με τις σύγχρονες απαιτήσεις της κοινωνίας όπως της αυξημένης κινητικότητας των πολιτών, των απαιτήσεων για την ισότιμη πρόσβαση σε υπηρεσίες ποιότητας κ.α.

Η παρούσα εργασία διαπραγματεύεται τον τομέα της ασύρματης δικτύωσης γενικότερα, με σκοπό την επιλογή της καταλληλότερης τεχνολογίας και τον τρόπο, (σχεδιασμός και υλοποίηση), με τον οποίο, τα πλεονεκτήματά της μπορούν να ενσωματωθούν στο νοσοκομειακό περιβάλλον. Η μεθοδολογία σχεδιασμού και υλοποίησης, φαίνεται στα σχήματα 59,60. Σύμφωνα με αυτά τα σχήματα

ΚΕΦΑΛΑΙΟ 1^{ο}

1.1 ΤΗΛΕΪΑΤΡΙΚΗ

Η παροχή εξειδικευμένης Ιατρικής γνώσης με τη μορφή διάγνωσης ή συμβουλευτικής μέσω της χρήσης τηλεματικών συστημάτων. Στην κλασσική της μορφή κλινικά στοιχεία (π.χ. ακτινογραφίες, καρδιογραφήματα, κλπ) μεταδίδονται σε ψηφιακή μορφή μέσω δικτύου από τον "μη εξειδικευμένο" ιατρό σε Κάποιο "εξειδικευμένο ιατρό" ο οποίος αφού τα εξετάσει στον υπολογιστή του, προχωράει στη διάγνωση της εξέτασης την οποία επιστρέφει στο "μη ειδικευμένο ιατρό" μαζί με οδηγίες. Η μετάδοση μπορεί να γίνεται τοπικά (εντός ενός νοσοκομείου) αλλά και απομακρυσμένα (π.χ. μεταξύ κέντρων υγείας και νοσοκομείων). Παρότι είναι δυνατή η μετάδοση ενός μεγάλου αριθμού εξετάσεων, οι Περισσότερες εφαρμογές τηλεδιάγνωσης, επί του παρόντος, περιορίζονται στη μετάδοση ακτινολογικών εικόνων, καρδιογραφημάτων, εικόνων μικροσκοπίου, βιοχημικών και διαφόρων άλλων εργαστηριακών εξετάσεων κ.λ.π.



Σχήμα 1: Παραδείγματα πιθανών εφαρμογών και ευρύτερης χρήσης WLAN

Ο κοινός παρονομαστής όλων αυτών των εφαρμογών είναι ότι για την υλοποίησή τους απαιτείται, όλα τα δεδομένα τα οποία λαμβάνονται υπόψη, αξιολογούνται και συνεπώς διακινούνται να είναι σε ψηφιακή μορφή. Άρα, ανεξάρτητα από το είδος της εφαρμογής, ο βασικός εξοπλισμός που είναι απαραίτητος για την υλοποίηση μίας τηλεϊατρικής εφαρμογής συνοψίζεται σε:

A) Μια Ιατρική συσκευή που συλλέγει τα ιατρικά δεδομένα (π.χ. Βιοχημικός αναλυτής, Ακτινολογικό, ηλεκτροκαρδιογράφος, μικροσκόπιο, κλπ.)

B) Συσκευή ψηφιοποίησης της Ιατρικής πληροφορίας (σε περίπτωση που τα δεδομένα που παράγει ο βιοϊατρικός εξοπλισμός είναι σε αναλογική μορφή). Παράδειγμα τέτοιων συσκευών είναι οι ψηφιοποιητές ακτινογραφιών ή X-Ray

Scanners ,αναλογική κάμερα-frame grabber η και κατάλληλων προδιαγραφών ψηφιακές κάμερες υψηλής ανάλυσης ψηφιακός καρδιογράφος, κλπ)

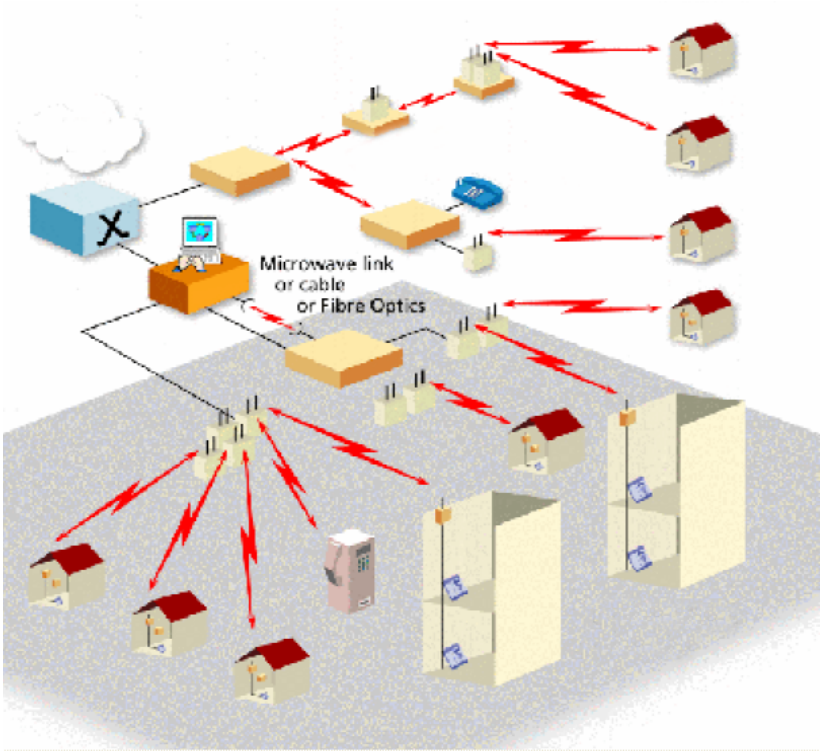
Γ) Ο εξοπλισμός για τη μετάδοση των ψηφιακών δεδομένων μέσω ενσύρματης ή ασύρματης ζεύξης

Δ) Διάταξη υπολογιστικών συστημάτων απεικόνισης και αξιοποίησης των δεδομένων που λαμβάνονται από τον τελικό αποδέκτη και κατάλληλο λογισμικό(Software).

Η Τηλεϊατρική μπορεί να κάνει χρήση της τηλεπικοινωνιακής υποδομής που υφίσταται σε κάθε γεωγραφική περιοχή στην οποία αναπτύσσεται, αλλά ανάλογα με τις προδιαγραφές των υπηρεσιών που πρόκειται να προσφερθούν είναι δυνατό να δημιουργηθούν και δίκτυα αποκλειστικής χρήσεως.

Η Τηλεϊατρική απαιτεί την ύπαρξη συνδέσεων μεταξύ των σημείων που πρέπει να επικοινωνούν, με τις εξής δυνατότητες:

- φωνητική επικοινωνία
- αποστολή και λήψη ιατρικών δεδομένων
- αποστολή και λήψη ιατρικών σημάτων και εικόνων
- πρόσβαση σε πηγές πληροφοριών και βάσεις δεδομένων
- πρόσβαση σε υπηρεσίες ηλεκτρονικού ταχυδρομείου



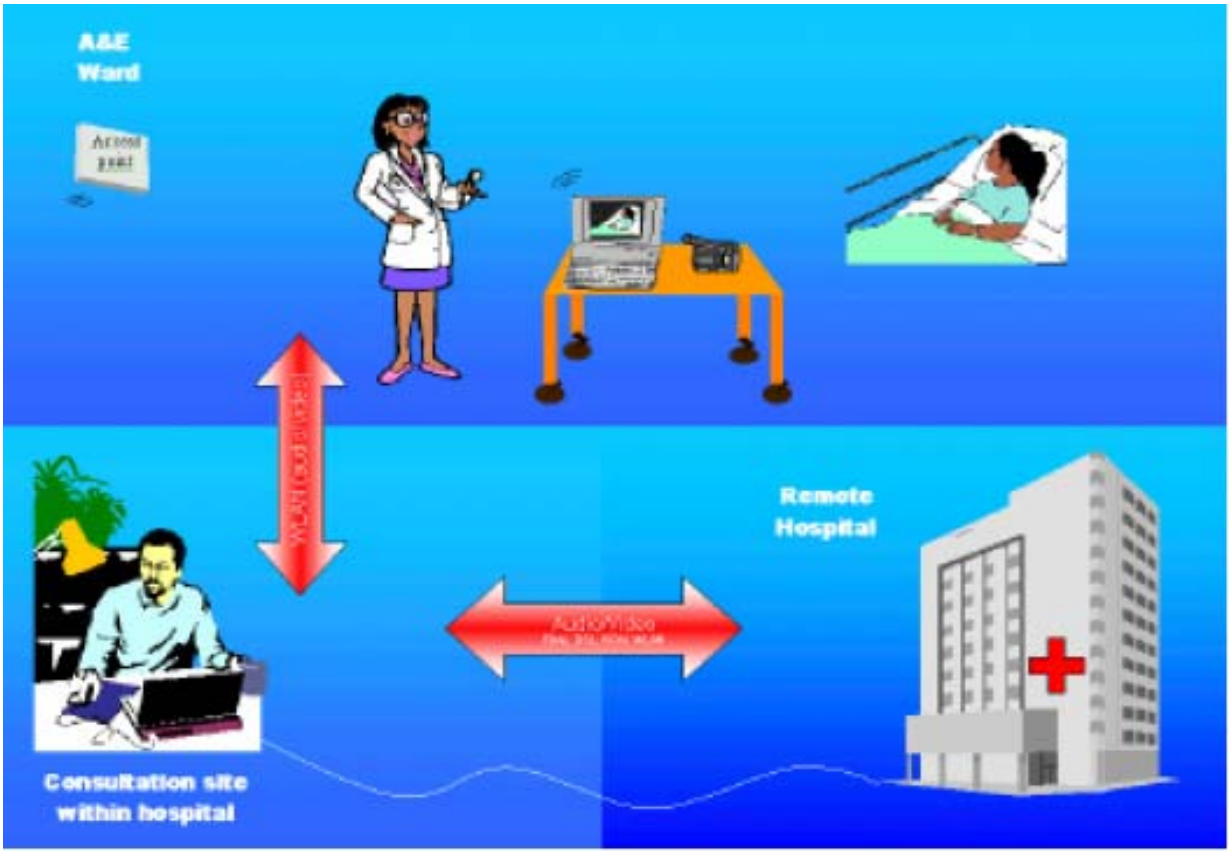
Σχήμα 2: Παράδειγμα ασύρματης δικτύωσης γειτονικών κτιριακών συγκροτημάτων.

Ανάλογα με τις συγκεκριμένες εφαρμογές και τις προσφερόμενες υπηρεσίες καθορίζονται οι απαιτήσεις και οι προδιαγραφές ως προς το επικοινωνιακό μέρος. Σε πολλές εφαρμογές, η φωνητική επικοινωνία είναι εκείνη η οποία καλύπτει το μεγαλύτερο χρονικό διάστημα της συνδέσεως. Μέσω όμως του δικτύου αυτού μπορούν να καλυφθούν και οι υπόλοιπες απαιτήσεις, με ορισμένους βέβαια περιορισμούς που σχετίζονται κυρίως με τις ταχύτητες μεταφοράς και την ακεραιότητα των πληροφοριών.

Η Τηλεϊατρική δεν ενδιαφέρεται ουσιαστικά για τον τεχνικό τρόπο μεταφοράς των πληροφοριών, αλλά κατά το σχεδιασμό συγκεκριμένων υπηρεσιών Τηλεϊατρικής, πρέπει να εξασφαλίζεται η τήρηση ειδικών προδιαγραφών που αφορούν:

- το χρόνο αποκαταστάσεως της συνδέσεως
- τη ταχύτητα μεταφοράς των πληροφοριών
- την ακεραιότητα των μεταφερόμενων στοιχείων
- τον αριθμό των ταυτόχρονων συνδέσεων
- τις διαδικασίες και τις εξουσιοδοτήσεις προσβάσεως και χρήσεως
- τις δαπάνες επικοινωνίας (ως συναρτήσεως του αποτελέσματος)
- την αξιοπιστία του δικτύου

Είναι προφανές ότι επιβάλλονται ειδικότερες προδιαγραφές στη περίπτωση διασυνδέσεων μεταξύ χωρών. Για τους λόγους αυτούς η Επιτροπή της Ευρωπαϊκής Ενώσεως, αλλά και άλλοι ευρωπαϊκοί και διεθνείς οργανισμοί, πρωταγωνιστούν στη καθιέρωση προτύπων.



Σχήμα 3: Εφαρμογή Τηλεϊατρικής

1.1.1 Τηλεακτινολογία

Μετάδοση ακτινολογικών εικόνων από ένα σημείο σε άλλο για γνωμάτευση ή απλά για συμβουλευτικούς σκοπούς μέσω υπολογιστή, χρησιμοποιώντας κατάλληλο δικτυακό εξοπλισμό ενσύρματης ή ασύρματης ζεύξης. Λόγω του γεγονότος ότι η μετάδοση αφορά ψηφιακή πληροφορία, απαιτείται η σύλληψη της εικόνας σε ψηφιακή μορφή.

Σε περιπτώσεις που το απεικονιστικό μηχάνημα δεν διαθέτει ψηφιακή έξοδο (πράγμα που συμβαίνει στα περισσότερα ακτινολογικά μηχανήματα και απεικονιστικές συσκευές υπερήχων, και σε αρκετούς αξονικούς και μαγνητικούς τομογράφους), είναι αναγκαία η ψηφιοποίηση της εικόνας χρησιμοποιώντας είτε

ψηφιοποιητές ακτινολογικού φιλμ (X-Ray Scanners), είτε Frame Grabbers συνδεδεμένους απευθείας στην έξοδο Composite Video της απεικονιστικής διάταξης.

Η Πρώτη λύση χρησιμοποιείται συνήθως για την ψηφιοποίηση ακτινογραφιών ενώ η δεύτερη για την ψηφιοποίηση εικόνων αξονικού και μαγνητικού τομογράφου, υπερήχων, και πυρηνικής Ιατρικής.

Η ψηφιοποίηση ακτινολογικών φιλμ μπορεί να γίνει είτε μέσω συστήματος διαφανοσκόπειου-Video Camera είτε μέσω Film Scanners. Στην πρώτη περίπτωση το φιλμ φωτίζεται μέσω του διαφανοσκοπείου και η εικόνα ψηφιοποιείται μέσω μίας υψηλής ευκρίνειας Video Camera. Η τεχνική αυτή, παρότι οικονομική, παρουσιάζει αρκετά μειονεκτήματα με βασικότερα αυτό της ανομοιόμορφης φωτεινότητας, της δυσκολίας στην χρήση (τοποθέτηση του φιλμ και ανάκτηση της πληροφορίας).

Τα τελευταία χρόνια τα συστήματα τηλεακτινολογίας διαθέτουν film Scanners και εξειδικευμένες συσκευές ψηφιοποίησης ακτινολογικών φιλμ. Οι συσκευές αυτές χρησιμοποιούν είτε την τεχνολογία CCD είτε την τεχνολογία LASER..

Πλεονεκτήματά τους είναι η αυτοματοποίηση της διαδικασίας ψηφιοποίησης, και η υψηλή ποιότητα και πιστότητα ψηφιοποίησης. Μειονέκτημα το υψηλό κόστος τους παρότι οι τιμές τους ολοένα μειώνονται.

1.1.2 Τηλεκαρδιολογία

Η πιο συνηθισμένη εφαρμογή τηλεκαρδιολογίας αφορά στη μετάδοση για διαγνωστικούς σκοπούς ηλεκτροκαρδιογραφημάτων (ΗΚΓ). Στην πιο συνηθισμένη μορφή της, η εφαρμογή απαιτεί την χρήση ενός ψηφιακού καρδιογράφου για την ανάκτηση, σε ψηφιακή μορφή, του καρδιογραφήματος, ενός τηλεπικοινωνιακού δικτύου και ενός υπολογιστικού σταθμού για την αποθήκευση και απεικόνιση του ΗΚΓ.

1.1.3 Τηλεπαθολογία

Η τηλεπαθολογία διακρίνεται σε στατική και δυναμική. Στην περίπτωση της στατικής τηλεπαθολογίας, μία ή περισσότερες ακίνητες (στατικές) εικόνες συλλέγονται, αποθηκεύονται προσωρινά, και στη συνέχεια μεταδίδονται off-line για διάγνωση. Στη δυναμική τηλεπαθολογία επιτυγχάνεται η σε πραγματικό χρόνο (Real Time) μετάδοση κινούμενων εικόνων σε συνδυασμό με τον εξ' αποστάσεως μηχανικό έλεγχο του μικροσκοπίου. Και στις δύο περιπτώσεις ο τυπικός εξοπλισμός περιλαμβάνει μία υψηλής ευκρίνειας κάμερα συνδεδεμένη σε ένα μικροσκόπιο, ένα υπολογιστικό σταθμό ψηφιοποίησης, κωδικοποίησης, και μετάδοσης εικόνας ,και σύστημα απεικόνισης και αποθήκευσής στην πλευρά του ειδικευμένου ιατρού. Είναι σαφές ότι τα κρίσιμα χαρακτηριστικά είναι η διακριτική ικανότητα συστήματος ψηφιοποίησης και απεικόνισης των δεδομένων και το εύρος ζώνης του τηλεπικοινωνιακού δικτύου για την περίπτωση της δυναμικής εφαρμογής.

1.1.4 Τηλεδερματολογία

Επί της αρχής, σι εφαρμογές τηλεδερματολογίας είναι απλές. Ο ασθενής με το δερματολογικό πρόβλημα βρίσκεται στην κλινική Α (που συνήθως στελεχώνεται από ένα γενικό ιατρό) και ο ειδικευμένος δερματολόγος βρίσκεται στην κλινική Β. Δερματολογικές εικόνες, ιστορικό του ασθενούς, εργαστηριακές αναλύσεις, και

οτιδήποτε άλλο σχετικό δεδομένο μεταδίδεται ηλεκτρονικά από το Α στο Β, όπου ο δερματολόγος αξιολογεί τα κλινικά δεδομένα, προβαίνει σε διάγνωση, και καθορίζει τις περαιτέρω πράξεις. Παρότι επί του παρόντος δεν υπάρχουν στοιχειοθετημένες στατιστικά μελέτες που να επιδεικνύουν τα ποσοστά δερματολογικών περιστατικών που μπορούν να διαγνωστούν μέσω τηλεϊατρικής, είναι γενικά αποδεκτό ότι το ποσοστό αυτό είναι σημαντικό. Αυτό είναι πολύ σημαντικό καθώς τα δερματολογικά περιστατικά είναι πολύ συνηθισμένα (7-20%) αλλά παρόλα αυτά συνήθως αντιμετωπίζονται ελλιπώς και δεν παραπέμπονται σε ειδικευμένους δερματολόγους.

Η εμπειρία έχει δείξει ότι η ανάκτηση, αποθήκευση και μετάδοση σε μη πραγματικό χρόνο δερματολογικών εικόνων είναι απόλυτα ικανή να επιτρέψει σε δερματολόγους την διάγνωση και διαχείριση σημαντικού αριθμού δερματολογικών περιστατικών. Για τον σκοπό αυτό, απαιτούμενος εξοπλισμός τηλεδερματολογίας αποτελείται από μια διάταξη ανάκτησης ακίνητων εικόνων υψηλής ανάλυσης, και μία διάταξη μετάδοσης ψηφιακών δεδομένων. Το κομμάτι της μετάδοσης ψηφιακών δεδομένων είναι παρόμοιο με αυτό των εφαρμογών τηλεακτινολογίας - μετάδοση ακίνητων ψηφιακών εικόνων.

Για την ανάκτηση ψηφιακών δερματολογικών εικόνων, δύο είναι οι πιο συνηθισμένοι τρόποι:

1. Μέσω μίας αναλογικής βιντεοκάμερας συνδεμένης με ένα σύστημα ψηφιακής ανάκτησης στατικών εικόνων (frame grabber)
2. Ανάκτηση μέσω ψηφιακών φωτογραφικών συσκευών (digital cameras) και εν συνεχεία μεταφορά στο σύστημα τηλεμετάδοσης.

Εκτός από την ανάκτηση και μετάδοση σε μη πραγματικό χρόνο, είναι δυνατή και η αλληλεπιδραστική τηλεδερματολογία (interactive Teledermatology) η οποία στην ουσία είναι εφαρμογή τηλεσυνδιάσκεψης - ο δερματολόγος μέσω της κάμερας μπορεί και βλέπει σε πραγματικό χρόνο την δερματική ανωμαλία και μπορεί να κατευθύνει την εξέταση / διάγνωση. Παρότι η Τεχνική αυτή έχει το πλεονέκτημα της άμεσης επαφής ειδικευμένου ιατρού / ασθενούς, έχει μεγαλύτερες δικτυακές απαιτήσεις (που αφορούν το εύρος ζώνης) μεγαλύτερο κόστος , μεγαλύτερο χρόνο επαφής και σε πολλές “απλές” περιπτώσεις δεν έχει ουσιαστικά πλεονεκτήματα.

1.1.5 Τηλεοφθαλμολογία

Οι εφαρμογές τηλεοφθαλμολογίας έχουν σαν στόχο να επιτρέπουν την πρόσβαση σε εξειδικευμένους οφθαλμίατρους αλλά και οφθαλμολογικά μηχανήματα ανά πάσα στιγμή και από οποιοδήποτε μέρος. Όπως και στις περισσότερες εφαρμογές τηλεϊατρικής τα συστατικά στοιχεία ενός συστήματος τηλεοφθαλμολογίας είναι το σύστημα ανάκτησης και ψηφιοποίησης εικόνας και το σύστημα μετάδοσης ψηφιακών εικόνων.

Στις περισσότερες εφαρμογές τηλεοφθαλμολογίας η εφαρμογή απαιτεί μετάδοση ακίνητων (στατικών) οφθαλμολογικών εικόνων. Έτσι λοιπόν, το σύστημα μετάδοσης εικόνων είναι παρόμοιο με αυτό της τηλεακτινολογίας. Αναφορικά με την ανάκτηση εικόνων τηλεοφθαλμολογίας, η πιο συνηθισμένη εφαρμογή είναι η χρήση CCD κάμερας τοποθετημένης εμπρός από μια ακτινοσκοπική αγγειογραφική συσκευή, ένα οφθαλμολογικό μικροσκόπιο, ή την ψηφιοποίηση slides οφθαλμολογικών εικόνων. Τα τελευταία χρόνια χρησιμοποιούνται ψηφιακές φωτογραφικές συσκευές Digital Cameras συνδεμένες σε οφθαλμολογικά εξεταστήρια (Slit-lamps) επιτρέποντας έτσι την ανάκτηση οφθαλμολογικών εικόνων υψηλής διακριτικής ικανότητας. Επιπλέον είναι δυνατή η ψηφιοποίηση εικόνων από Οφθαλμοσκόπιο Laser (Scanning Laser Ophthalmoscope) για την εξέταση

ανωμαλιών του αμφιβληστροειδούς. Σε κάθε περίπτωση, οι διαγνωστικές εικόνες ψηφιοποιούνται , αποθηκεύονται και σε ύστερο χρόνο μεταδίδονται στον εξειδικευμένο οφθαλμίατρο για γνωμάτευση και παροχή περαιτέρω οδηγιών.

1.1.6 Τηλεχειρουργική

Η τηλεχειρουργική είναι ένας Τομέας της τηλεϊατρικής που αναπτύχθηκε τα τελευταία χρόνια και παρουσιάζει μεγάλο ενδιαφέρον. Το βασικό έρεισμα στην ανάπτυξη της τηλεχειρουργικής είναι η ανάγκη μετάδοσης και διάχυσης των εξειδικευμένων χειρουργικών τεχνικών και γνώσεων διευκολύνοντας την αρτιότερη και αποτελεσματικότερη εκπαίδευση και διάδοση των λαπαροσκοπικών χειρουργικών διαδικασιών. Ένας σημαντικός αριθμός κατασκευαστών λαπαροσκοπικών συσκευών είναι εφοδιασμένος με δυνατότητες αμφίδρομης μετάδοσης κινούμενης εικόνας και ήχου, επιτρέποντας έτσι την σύνδεση χειρουργείων με εκπαιδευτικές ή έμπειρες χειρουργικές εγκαταστάσεις.

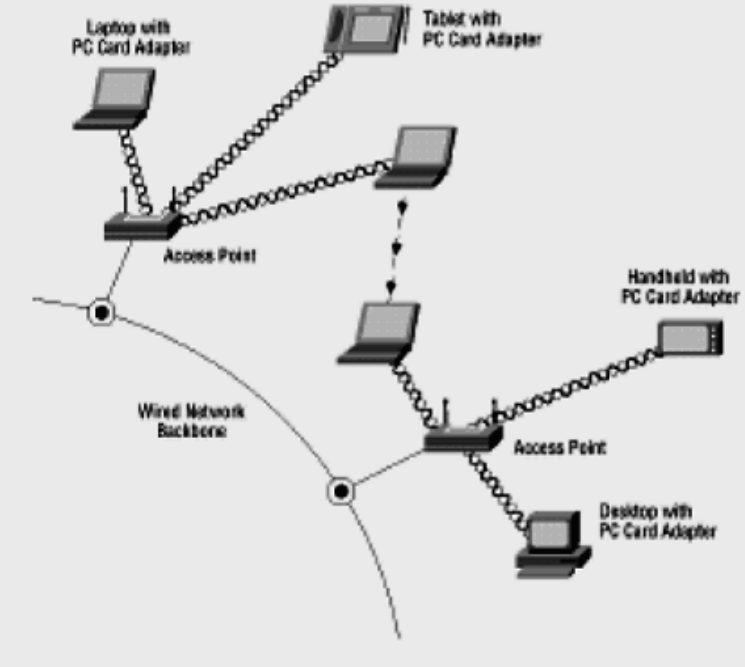
Σήμερα η τηλεχειρουργική μπορεί να θεωρηθεί σαν την αμφίδρομη μετάδοση εικόνας και ήχου επιτρέποντας την επικοινωνία μεταξύ χειρουργών (μικρής εμπειρίας) στα χειρουργεία και χειρουργών (με μεγάλη εμπειρία) σε απομακρυσμένες περιοχές. Η χρήση ρομποτικών συσκευών επιτρέπει στους απομακρυσμένους χειρουργούς να συμμετέχουν ενεργά στην χειρουργική διαδικασία. Είναι αυτονόητο ότι πέρα από τις αυξημένες τηλεπικοινωνιακές υποδομές που η εφαρμογή αυτή απαιτεί, απαιτείται και πολύ εξειδικευμένο λογισμικό υλικό ώστε να είναι εφικτή η προσομοίωση, στον απομακρυσμένο σταθμό, της καταστάσεως που επικρατεί στο χειρουργείο. Για τον σκοπό αυτό συνήθως απαιτούνται συστήματα εικονικής πραγματικότητας (Virtual Reality) που επιτρέπουν στους απομακρυσμένους χειρουργούς να έχουν μια πραγματική εικόνα της όλης διαδικασίας.

1.1.7 Τηλεεκπαίδευση

Η εξέλιξη των τηλεπικοινωνιακών και πληροφορικών συστημάτων τα τελευταία χρόνια κατέστησε δυνατή και με σχετικά χαμηλό κόστος την δυνατότητα τηλεσυνδιάσκεψης μεταξύ 2 ή περισσότερων προσώπων. Η ιατρική ήταν από τους πρώτους τομείς που αξιοποίησαν την δυνατότητα αυτή για την παροχή εξειδικευμένων υπηρεσιών υγείας. Έτσι λοιπόν είναι αρκετά σύνηθες σήμερα σε περιπτώσεις που απαιτείται η έμπειρη γνώμη ενός ή περισσότερων ιατρών αυτή να λαμβάνεται σε πραγματικό χρόνο μέσω υπηρεσιών τηλεσυνδιάσκεψης. Στην ιδανική περίπτωση είναι δυνατή η τηλεκαθοδήγηση της εξέτασης μέσο τηλεσυνδιάσκεψης αφού ο έμπειρος ιατρός μπορεί να βλέπει το ασθενή κατά την διάρκεια της εξέτασης και ταυτόχρονα να καθοδηγεί τον θεράποντα ιατρό. Σε άλλες περιπτώσεις είναι δυνατή η σύσταση ιατρικών συμβουλίων μέσω τηλεσυνδιάσκεψης χωρίς την ανάγκη μετακίνησης των εξειδικευμένων ιατρών που μπορεί να βρίσκονται σε διαφορετικές χώρες του κόσμου.

Παραλλαγή της παραπάνω περίπτωσης είναι και η περίπτωση της τηλεεκπαίδευσης μέσω υπηρεσιών τηλεσυνδιάσκεψης όπου μία ομάδα ιατρών / φοιτητών μπορεί να εκπαιδεύεται σε συγκεκριμένες ιατρικές διαδικασίες / τεχνικές χωρίς κατ ανάγκη να βρίσκονται στο χώρο που εκτελείται η ιατρική διαδικασία. Βέβαια η εξέλιξη των τεχνολογιών εικονικής πραγματικότητας έχει δημιουργήσει πολλαπλές δυνατότητες στην τηλεεκπαίδευση αφού τώρα πια η μέχρι πρότινος

“παθητική” εκπαίδευση μετατρέπεται σε “ενεργητική” με την εικονική συμμετοχή των εκπαιδευομένων.



Σχήμα 4: Πιθανή αρχιτεκτονική εφαρμογής WLAN, σε ιατρικό περιβάλλον.

1.2 ΥΠΗΡΕΣΙΕΣ ΑΜΕΣΗΣ ΒΟΗΘΕΙΑΣ - ΕΠΕΙΓΟΥΣΑ ΙΑΤΡΙΚΗ

Στον Ελλαδικό χώρο σήμερα, σι υπηρεσίες άμεσης βοήθειας παρέχονται από το Εθνικό Κέντρο Άμεσης Βοήθειας (Ε.Κ.Α.Β.). Οι υπηρεσίες αυτές συνίστανται τόσο στην παροχή άμεσης βοήθειας για την προσωρινή ιατρική αντιμετώπιση του προβλήματος, όσο και στην κατά το δυνατόν υποστηριγμένη μεταφορά των ασθενών σε οργανωμένο χώρο επείγουσας ιατρικής όπως είναι οι σταθμοί πρώτων βοηθειών, τα εξωτερικά ιατρεία επειγόντων περιστατικών (Τ.Ε.Π.), οι μονάδες εντατικής θεραπείας (Μ.Ε.Θ.), τα χειρουργεία, οι χώροι 24ωρης νοσηλείας, κ.λ.π.

Από το χαρακτήρα της Πρώτης φροντίδας, οι υπηρεσίες άμεσης βοήθειας αποτελούν αντικείμενο της επείγουσας ιατρικής. Τα Προβλήματα επείγουσας ιατρικής στη χώρα μας εντείνονται από τη γεωγραφική ανομοιομορφία της Ελλάδας (ορεινά χωριά, μεγάλος αριθμός νησιών) και από την ανομοιόμορφη πληθυσμιακή κατανομή.

Η ποιότητα της περίθαλψης πρώτης φροντίδας του ασθενούς, κατά τη διαδικασία της διακομιδής του σε χώρο επείγουσας ιατρικής, εξαρτάται κυρίως από την σύμφωνα με το ιατρικό ιστορικό αρχική αντιμετώπιση του περιστατικού και τις πρωτοβουλίες που λαμβάνει το προσωπικό του διακομιστικού σταθμού. Στην πλειονότητα των περιστατικών, η αντιμετώπιση αυτή αφορά εξειδικευμένης μορφής περίθαλψη. Σε ορισμένα περιστατικά, η αντιμετώπιση αυτή αφορά σύνθετης μορφής περίθαλψη και επιβάλλεται η συνεργασία περισσοτέρων της μιας ιατρικών ειδικοτήτων. Βεβαίως, σε κάθε περίπτωση, είναι αναγκαία η γνώση του ιατρικού ιστορικού του ασθενούς Κατά τη διαδικασία της παροχής Πρώτης βοήθειας.

Όμως, όπως είναι γνωστό, οι ιατρικού περιεχομένου πληροφορίες βρίσκονται διασκορπισμένες σε διάφορες μορφές όπως επί παραδείγματι σε έντυπα, βιβλιοθήκες, αρχεία συνοικιακών ιατρών, αρχεία κλινικών, αρχεία Νοσοκομείων κ.λ.π. Επίσης, το Ιστορικό υγείας ενός πολίτη εξαρτάται από την χρονική περίοδο και το φορέα υγείας

που αντιμετώπισε το πρόβλημά του. Δυστυχώς, με την πάροδο του χρόνου και κυρίως από την έλλειψη βοηθητικών χώρων (είναι σύνηθες φαινόμενο η έλλειψη αποθηκευτικών χώρων στα Νοσοκομεία) τα αρχεία αυτά καταστρέφονται, με αποτέλεσμα το νοσηλευτικό σύστημα σήμερα καθόλου ή σπανίως να χρησιμοποιεί το ιστορικό υγείας του πολίτη. Έτσι, στο σύνολο των περιπτώσεων, το ιστορικό γίνεται εκάστοτε γνωστό μόνο από τη μαρτυρία και τη δήλωση του πολίτη. Είναι προφανές ότι η εφαρμογή συγχρόνων τεχνολογιών στην ιατρική και ειδικότερα η τηλεϊατρική μπορεί να επιλύσει αυτά τα προβλήματα.

Έχει διαπιστωθεί η ανάγκη διασύνδεσης σε ενοποιημένο τηλεπικοινωνιακό δίκτυο των κεντρικών νοσοκομειακών μονάδων με περιφερειακά νοσοκομεία, κέντρα υγείας, σταθμούς πρώτων βοηθειών, αγροτικά ιατρεία κ.λ.π., σε συνδυασμό με την υποστήριξη των διακομιστικών σταθμών επειγόντων περιστατικών (Ε.Κ.Α.Β., ασθενοφόρα κ.λ.π.) για τη λήψη βέλτιστης απόφασης σε σύντομο χρονικό διάστημα με χρήση ηλεκτρονικών υπολογιστών. Επίσης, έχει διαπιστωθεί η ανάγκη καταγραφής του ιατρικού ιστορικού όλων των Ελλήνων πολιτών (υποχρεωτική κάρτα υγείας με τον αντίστοιχο κωδικό αριθμό του πολίτη), ώστε κατά τη διάρκεια της διακομιδής του σε οργανωμένο χώρο επείγουσας Ιατρικής να δίνεται η δυνατότητα παροχής σημαντικής και ουσιαστικής βοήθειας για τη μετέπειτα εξέλιξη της υγείας του από το Προσωπικό του διακομιστικού σταθμού. Με τον τρόπο αυτό μπορεί να δοθεί η δυνατότητα συνεργασίας με τη μονάδα που θα υποδεχθεί τον ασθενή (Νοσοκομείο κ.λ.π.), ώστε να είναι κατάλληλα προετοιμασμένη για την άμεση αντιμετώπιση του περιστατικού, ή στη χειρότερη περίπτωση να έχει προετοιμαστεί η αναγκαία τεχνική υποστήριξη, χωρίς απώλεια πολύτιμου χρόνου (π.χ. εξετάσεις για ομάδα αίματος, επάρκεια σε φιάλες αίματος, απινιδωτής σε ετοιμότητα, ηλεκτροκαρδιογράφημα, προετοιμασμένος αξονικός τομογράφος ή τραυματολογικό μηχάνημα, προετοιμασία για χειρουργική επέμβαση κ.λ.π).

Μέχρι σήμερα, υπάρχουν αρκετές περιπτώσεις απώλειας συνανθρώπων μας από την καθυστερημένη παροχή ουσιαστικής πρώτης φροντίδας, όπως αποκαλύπτεται από τα περιστατικά θανάτων κατά τη διάρκεια της διακομιδής ασθενών από ακριτικές περιοχές και μικρά νησιά σε οργανωμένα νοσοκομειακά κέντρα, που έρχονται στο φως της δημοσιότητας. Δεδομένου ότι η αξία της ανθρώπινης ζωής δεν είναι δυνατόν να κοστολογηθεί, μπορεί κανείς να οδηγηθεί στη διαπίστωση της αναγκαιότητας εφαρμογής της διαδικτύωσης και της τηλεϊατρικής για την υποστήριξη διακομιστικών σταθμών σε εθνική κλίμακα.

1.2.1 Ιατρικός Εξοπλισμός κατάλληλος για εφαρμογές Τηλεϊατρικής

Μεταξύ των στοιχείων που πρέπει να επεξεργαστεί ο γιατρός προκειμένου να καταλήξει σε συμπεράσματα σχετικά με τη κατάσταση της υγείας ενός ατόμου είναι και τα αποτελέσματα εργαστηριακών και διαγνωστικών χειρισμών.

Οι συνήθεις αλλά απαραίτητες και επαρκείς εργαστηριακές βιοχημικές και αιματολογικές αναλύσεις απαιτούν εργαστηριακό εξοπλισμό και εξειδικευμένο προσωπικό και δεν αποτελούν μέρος των καθηκόντων του ιατρικού προσωπικού.

Τα διαγνωστικά μέσα που διατίθενται σήμερα περιλαμβάνουν και ένα μεγάλο φάσμα τεχνικών και μεθόδων, που παρέχουν τα αποτελέσματα των εξετάσεων με τη μορφή σημάτων και εικόνων. Τα πάσης φύσεως ακτινολογικά μηχανήματα, είναι συσκευές με μεγάλη συχνότητα χρήσεως και βρίσκονται εγκατεστημένα σε όλα τα νοσοκομεία, σε μεγάλο αριθμό πρωτοβαθμίων ιατρικών μονάδων όπως είναι τα Κέντρα Υγείας, αλλά και σε μεγάλο αριθμό ιδιωτικών ακτινολογικών εργαστηρίων.

Εικόνες παράγουν και διάφορα άλλα διαγνωστικά μηχανήματα σε αναλογική ή ψηφιακή μορφή. Οι λόγοι της παραγωγής των εικόνων σε φιλμ είναι η ευχρηστία των, ο χρόνος ζωής των και η ποιότητά των, ενώ των ψηφιακών είναι η άμεση δυνατότητα επεξεργασίας με υπολογιστή, η αποθήκευσή τους σε ηλεκτρονικά μέσα και κατά συνέπεια η εύκολη αναζήτησή τους και η και αποστολή τους σε άλλα σημεία ενός δικτύου. Μεγάλες εταιρείες κατασκευής εξοπλισμού όσο και μεγάλες νοσοκομειακές μονάδες του εξωτερικού έχουν ήδη αρχίσει να υιοθετούν την ηλεκτρονική παραγωγή, αποθήκευση και διακίνηση εικόνων (συστήματα PACS-Picture Archiving and Communication Systems).

Οι διαγνωστικές τεχνικές που χρησιμοποιούνται σε ευρεία κλίμακα σήμερα και παράγουν ασπρόμαυρες ή έγχρωμες εικόνες με τεχνητά χρώματα, είναι:

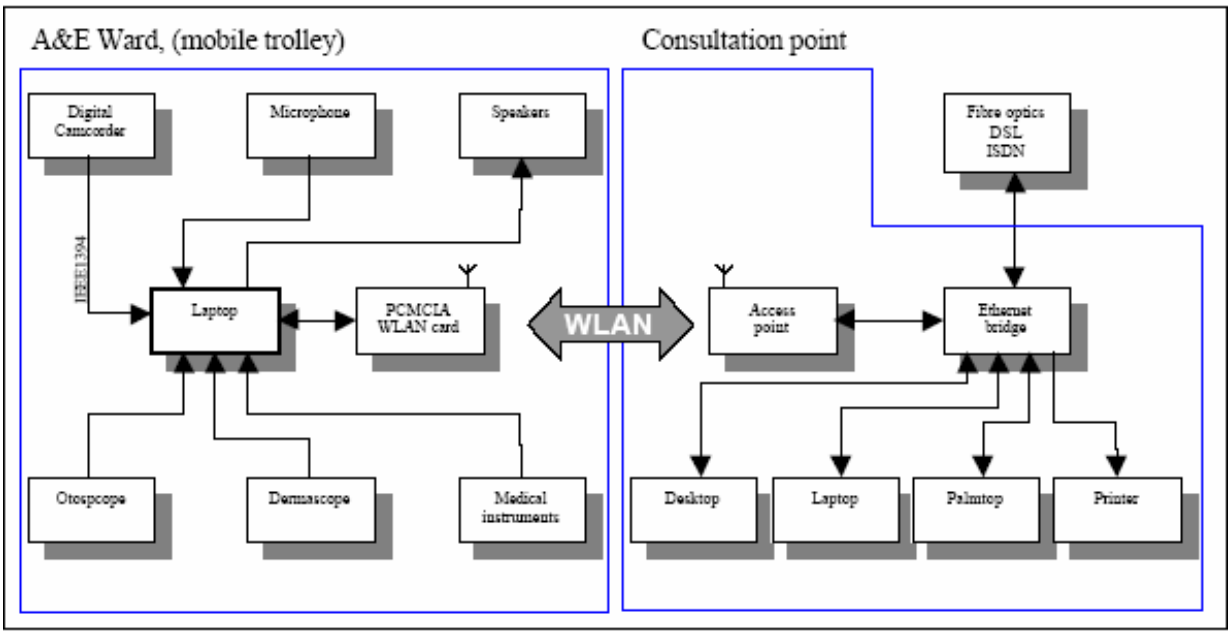
- η Αξονική Τομογραφία (CT)
- η Μαγνητική Τομογραφία (MRI)
- η τομογραφία εκπεμπόμενων φωτονίων (SPECT)
- η χρήση υπερήχων (US)
- η καταγραφή εκπομπής ακτινοβολίας γ (γ-camera)
- οι αγγειογραφικές
- οι ενδοσκοπικές με χρήση βίντεο
- η τομογραφία με εκπομπή ποζιτρονίων (PET, η οποία όμως δεν υπάρχει ακόμη στην Ελλάδα)

Ήδη από το 1994 κατασκευάστηκαν και λειτουργούν ακτινογραφικά μηχανήματα (Computer Radiology) χωρίς τη παραγωγή φιλμ. Η εικόνα είναι προϊόν της ηλεκτρονικής αναγνώσεως του αποτελέσματος της εξετάσεως ('εικόνας'), από ειδική επαναχρησιμοποιούμενη στην ακτινοβολία ειδική κασέτα. Οι ψηφιακές αυτές εικόνες επιτρέπουν περαιτέρω χειρισμό των με υπολογιστή, ενώ είναι δυνατή και η παραγωγή σκληρών αντιγράφων δηλ. σε φιλμ ή χαρτί.

Οι συσκευές που προαναφέρθηκαν είναι γενικά μεγάλης αξίας και βρίσκονται εγκαταστημένες, με εξαίρεση των συσκευών υπερήχων, σε τριτοβάθμια νοσοκομεία και ιδιωτικά διαγνωστικά κέντρα. Κατά συνέπεια η ανταλλαγή εικόνων που προέρχονται από τις προαναφερθείσες συσκευές, μεταξύ ιατρών σε διαφορετικές ιατρικές μονάδες, (ανεξάρτητα από τη μεταξύ τους απόσταση και το μέγεθος των ανταλλασσόμενων ιατρικών στοιχείων), αφορά κυρίως τη δευτεροβάθμιο και τριτοβάθμιο φροντίδα υγείας ή τα τυχόν ιδιωτικά δίκτυα και τις υπηρεσίες Τηλεϊατρικής που σχετίζονται με αυτές.

Υπάρχουν ακόμα και μια σειρά αναλύσεων ή εξετάσεων που έχουν την ανάγκη χρήσεως εγχρώμων εικόνων. Μεταξύ αυτών συγκαταλέγονται οι ιστολογικές και κυτταρολογικές εξετάσεις, οι εξετάσεις που αφορούν δερματολογικά περιστατικά και οι ενδοσκοπήσεις. Χρήση εγχρώμων εικόνων γίνεται επίσης στην ψυχιατρική και την ιατροδικαστική.

Μια άλλη τέλος κατηγορία είναι εκείνη που περιλαμβάνει μηχανήματα μετατροπής των σημάτων (ηλεκτρικά, ακουστικά, μηχανικά και που προέρχονται από τη λειτουργία οργάνων του σώματος, σε ηλεκτρικά αναλογικά ή ψηφιακά σήματα, που τελικώς παρουσιάζονται στον ιατρό σε διάφορα τελικά μέσα, όπως χαρτί, φιλμ, οθόνες κλπ. Κατά συνέπεια υπάρχει στις ιατρικές μονάδες πληθώρα εξοπλισμού, ο οποίος μπορεί άμεσα ή με την προσθήκη πρόσθετων ηλεκτρονικών κυκλωμάτων και κατά περίπτωση πρόσθετου εξοπλισμού, να αξιοποιηθεί για την παροχή υπηρεσιών Τηλεϊατρικής. Η ταχύτητα εξελίξεως της τεχνολογίας είναι σήμερα τέτοια, ώστε είναι απαραίτητο πλέον κατά τις περιπτώσεις αντικαταστάσεως ιατρικού εξοπλισμού, να λαμβάνεται πρόνοια για την επιλογή συσκευών, οι οποίες μπορούν να συνδεθούν με υπολογιστές και έχουν δυνατότητες συνδέσεώς τους σε δίκτυα.



Σχήμα 5: Μπλοκ διάγραμμα ενός ασύρματου συστήματος Τηλεϊατρικής

1.2.2 Ποιότητα ιατρικών στοιχείων

Κατά τις εφαρμογές της Τηλεϊατρικής και ιδιαίτερα κατά την οργάνωση και παροχή Τηλεϊατρικών υπηρεσιών είναι απαραίτητο να εξασφαλίζεται η ποιότητα των ιατρικών δεδομένων, τουλάχιστον στα επίπεδα που εξασφαλίζεται στις μεγάλες ιατρικές μονάδες.

Διεθνώς, φαίνεται να υπάρχει συμφωνία μεταξύ των ιατρών ότι ψηφιακές εικόνες με τουλάχιστον 1000X1000 στοιχεία και 256 επίπεδα της κλίμακας του γκρι, επιτρέπουν την διάγνωση εικόνων αξονικού και μαγνητικού τομογράφου, εξίσου καλά με εκείνη που επιτυγχάνεται από το φιλμ. Οι εικόνες υπερήχων έχουν συνήθως μικρότερο αριθμό στοιχείων (πχ. 512X512). Σε όλες τις περιπτώσεις είναι επιθυμητό μεγαλύτερο εύρος επιπέδων του γκρι (πχ. 4096 ή και 16384), παρόλο ότι ο οφθαλμός αδυνατεί να διακρίνει περισσότερα από 120 - 150 επίπεδα.

Σχετικά με τη διαγνωστική δυνατότητα επί ψηφιακών εικόνων, οι οποίες προέρχονται από ψηφιοποίηση ακτινογραφιών, οι απόψεις διίστανται και άλλοι ερευνητές ομιλούν για την ανάγκη ψηφιακών εικόνων με 2000X2000 στοιχεία και άλλοι για 4000X4000 στοιχεία, προκειμένου να γίνει διάγνωση με την ίδια ακρίβεια που γίνεται από το πρωτότυπο φιλμ [3]. Ωστόσο αυτό δεν σημαίνει ότι δεν είναι δυνατή η διάγνωση από ψηφιακές εικόνες με 1000X1000 στοιχεία. Το πρόβλημα βεβαίως που ανακύπτει είναι ο χρόνος αποστολής των εικόνων μέσα από τα εγκαταστημένα τηλεπικοινωνιακά δίκτυα.

1.3 ΕΝΔΟΝΟΣΟΚΟΜΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

0 βιοϊατρικός εξοπλισμός ενός σύγχρονου νοσοκομείου αποτελείται από ένα πλήθος ετερογενών συσκευών σι οποίες μπορούν να ταξινομηθούν σε γενικές κατηγορίες, ανάλογα με τη λειτουργία τους. Τα δεδομένα που παράγονται από κάθε κατηγορία παρουσιάζουν ένα μεγάλο βαθμό ανομοιομορφίας (εικόνες, κυματομορφές, αριθμητικά δεδομένα, κλπ.). Οι συσκευές που ανήκουν σε κάθε κατηγορία μπορούν να συνδεθούν μεταξύ τους με δίκτυο, αποτελώντας έτσι ξεχωριστά συστήματα συλλογής και αποθήκευσης ενός τύπου δεδομένων.

1.3.1 Αυτοματοποιημένα συστήματα νοσοκομείου

Τα συστήματα συλλογής και επεξεργασίας δεδομένων είναι τα παρακάτω:
Picture Archiving and Communication System(PACS): Είναι ένα σύστημα που παρέχει τη δυνατότητα συλλογής εικόνων (από CT, MRI ψηφιακος αγγειογράφους, συσκευές υπερήχων) αποθήκευσης και ανάκτησής τους και συμπεριλαμβάνει συσκευές απεικόνισης και διαχείρισης εικόνων, συνδεδεμένες με συσκευές αποθήκευσης.

Pharmacy Information System(PIS): Το σύστημα αυτό αυτοματοποιεί τις διαδικασίες φαρμακείου ενός νοσοκομείου (επεξεργασία συνταγών, συντήρηση της βάσης δεδομένων των φαρμάκων, παρακολούθησης της χρήσης τους, κλπ.).

Material Management Information System (MMIS): Χρησιμοποιείται για τη διαχείριση και τον έλεγχο όλων των διαδικασιών που αφορούν την προμήθεια υλικών (αγορά, λήψη, ταξινόμηση, απογραφή, κλπ.).

Anesthesia Information Management System(AIMS): Το σύστημα αυτό συλλέγει δεδομένα από πολυάριθμες πηγές σχετικά με την παρακολούθηση των διαδικασιών στα τμήματα αναισθησιολογίας, Παρέχει τη δυνατότητα ανάλυσης των δεδομένων αυτών και παράγει διάφορους τύπους αναφορών.

Laboratory Information System (LIS): Χρησιμοποιείται για τη συλλογή πληροφοριών από ένα πλήθος συσκευών (Clinical Chemistry Analyzers,Blood Culture Analyzers, κλπ.), για την αποθήκευση κλινικών δεδομένων, την επαλήθευση της ακρίβειας των εξετάσεων, τη βαθμονόμηση των Οργάνων και τη δημιουργία (και την ενημέρωση) αρχείων ασθενών.

Radiology Information System,(RIS): Είναι ένα σύστημα που συλλέγει και αποθηκεύει δεδομένα από ακτινολογικές συσκευές.

Hospital Information System (HIS): Είναι το κεντρικό σύστημα ενός νοσοκομείου, που συλλέγει δεδομένα από το σύνολο των συστημάτων και επιτρέπει την πρόσβαση σε όλες τις επιμέρους διαδικασίες, παρέχοντας τη δυνατότητα για συνολική διαχείριση του νοσοκομείου.

Η δικτύωση των συσκευών μίας κατηγορίας, όταν δεν υπακούουν σε κάποιο Standard, απαιτεί συνήθως την ύπαρξη ειδικών interfaces (hardware –software) και μετατροπείς πρωτοκόλλων. Το πρόβλημα της δικτύωσης μεταξύ των συσκευών διαφορετικών προμηθευτών αντιμετωπίζεται με την εφαρμογή επικοινωνιακών Standards (π.χ. για συστήματα PACS χρησιμοποιείται το DICOM 3.0), που εξασφαλίζουν ανταλλαγή δεδομένων μεταξύ διαφορετικών τύπων συσκευών. Επίσης, η ανάγκη δικτύωσης όλων των συστημάτων που συνιστούν το HIS, απαιτεί την ύπαρξη ενός Standard (για την ανταλλαγή δεδομένων μεταξύ των ετερογενών αυτών συστημάτων. Ένα τέτοιο standard είναι το Electronic Data Interchange Health Level 7 (HL7) που παρέχει υπηρεσίες ανταλλαγής κλινικών δεδομένων μεταξύ όλων των ετερογενών συστημάτων του νοσοκομείου, καθώς επίσης και λειτουργίες όπως καταχώρηση ασθενών, Admission /discharge/transfer(ADT), κλπ.
Πληροφοριακά συστήματα εργαστηρίου:

Το 1988 δημοσιεύτηκαν από το U.S.Department of Health and Human Services Clinical Laboratory Improvement Act (CLIA) οδηγίες που αφορούν τη σύνδεση ιατρικών συσκευών εργαστηρίου με συστήματα LIS και / ή HIS.

ΚΕΦΑΛΑΙΟ 2ο

2.1 ΠΡΟΤΥΠΑ ΓΙΑ ΗΛΕΚΤΡΟΝΙΚΗ ΑΝΤΑΛΛΑΓΗ ΙΑΤΡΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Οι εφαρμογές για να μπορέσουν να λειτουργήσουν αποδοτικά, αλλά και να διευρυνθούν θα πρέπει να υποστηρίζουν κάποια συγκεκριμένα πρότυπα. Υπάρχει ένα μεγάλος αριθμός συνεχώς αναπτυσσόμενων προδιαγραφών (standards), που σχεδιάστηκαν για να εξασφαλίσουν την διαλειτουργικότητα και την ποιότητα των υπηρεσιών μεταξύ των διαφορετικών εφαρμογών τηλεϊατρικής. Στη συνέχεια θα παρουσιαστούν επικυρωμένες προδιαγραφές για τις τηλεπικοινωνίες, τις ψηφιακές εικόνες, το βίντεο και τον ήχο, δίνοντας μεγαλύτερη έμφαση στις εφαρμογές που υποστηρίζουν διάγνωση από απόσταση.

Η σημαντικότητα όλων των παραπάνω προδιαγραφών διαφαίνεται στη μακροχρόνια και ευρείας κλίμακας διάδοση της τηλεϊατρικής. Η διαλειτουργικότητα είναι ένα από τα πιο κρίσιμα τμήματα στις εφαρμογές τηλεϊατρικής. Αν, για παράδειγμα, ένα νοσοκομείο έχει σύστημα βιντεοσυνδιάσκεψης που χρησιμοποιεί προδιαγραφές ISDN H.320, θα πρέπει να μπορεί να επικοινωνεί με κάποιο άλλο σύστημα video που χρησιμοποιεί τις ίδιες προδιαγραφές, ανεξάρτητα αν προέρχονται από διαφορετικό κατασκευαστή. Αν από την άλλη, η μονάδα υγείας έχει ένα σύστημα που χρησιμοποιεί έναν ιδιόκτητο ή εκτός προδιαγραφών αλγόριθμο, τότε θα πρέπει οπωσδήποτε και οι άλλες μονάδες που επικοινωνούν μαζί της να έχουν το ίδιο ακριβώς σύστημα.

Η Τηλεϊατρική μπορεί να χρησιμοποιήσει ποικίλα γήινα και δορυφορικά μέσα μετάδοσης. Το μέσο που χρησιμοποιείται είναι σημαντικό, επειδή το εύρος ζώνης (bandwidth) του ή ο ρυθμός μετάδοσης (bit rate) καθορίζει τον τύπο της τεχνολογίας που μπορεί να χρησιμοποιηθεί και την ποιότητα της παρεχόμενης υπηρεσίας. Συστήματα στενού - εύρους ζώνης, όπως είναι οι κοινές τηλεφωνικές γραμμές είναι φθηνά, αλλά στερούνται τη χωρητικότητα για κίνηση video 25-30 πλαίσια στο δευτερόλεπτο. Μπορούν όμως να μεταδώσουν ψηφιακό βίντεο σε χαμηλότερα πλαίσια στο δευτερόλεπτο, στατικές εικόνες, φωνή, κείμενο ή δεδομένα. Καμία τεχνολογία ή εύρος ζώνης δεν είναι κατάλληλο για όλους τους σκοπούς της τηλεϊατρικής. Αντιθέτως, οι χωρητικότητες και οι δυνατότητες κάθε συστήματος πρέπει να καθοριστούν από τις ανάγκες των χρηστών, συνυπολογίζοντας την υποδομή εγκατάστασης και τα τρέχοντα κόστη.

2.1.1 Οργανισμοί δημοσίευσης προτύπων

Η ανταλλαγή ηλεκτρικών ιατρικών δεδομένων και άλλων ιατρικών πληροφοριών στηρίζεται σε πρότυπα που έχουν δημοσιεύσει δημόσιοι και ιδιωτικοί οργανισμοί. Οι σημαντικότεροι από αυτούς είναι οι ακόλουθοι:

• ACR American College of Radiology
• CAP American College of Pathologists
• CEN TC251 που αποτελείται από τις ακόλουθες ομάδες:
  1) WGI: Information Models
  2) WGII: Terminology and Knowledge Bases
  3) WGIII: Security, Safety and Quality
  4) WGIV: Technology for Interoperability
• HL7 Health Level Seven
• IEEE Institute of Electrical and Electronic Engineers
• IFCC International Federation of Clinical Chemistry and Laboratory Medicine

• ISO/IEC JTCI/SC32 JTC1 είναι η πρώτη και μοναδική Joint Technical Committee of ISO και IEC, και διαπραγματεύεται με την τεχνολογία της πληροφορικής. SC32 είναι η υποεπιτροπή του JTC1 και διαπραγματεύεται τη διαχείριση και την ανταλλαγή δεδομένων.
• ISO TC 215 Healthcare informatics
• IUBMB International Union of Biochemistry and Molecular Biology
• IUPAC International Union of Pure and Applied Chemistry
• NLM US National Library of Medicine
• WHO World Health Organization
(www.diffuse.org/medical.html)

2.1.2 ITU-T προδιαγραφές

Η International Telecommunication Union (ITU), επισήμως γνωστή ως, η Consultative Committee for International Telegraph and Telephony (CCITT), που εδρεύει στην Γενεύη της Ελβετίας, είναι ένας διεθνής οργανισμός μέσω του οποίου κυβερνήσεις και ιδιωτικοί φορείς συντονίζουν τα δίκτυα και τις υπηρεσίες των παγκόσμιων τηλεπικοινωνιών. Οι ITU- T προδιαγραφές απευθύνονται στη μεταφορά και συμπίεση video, ήχου και δεδομένων. Οι προδιαγραφές, με ιδιαίτερη αναφορά στην τηλεϊατρική παρατίθενται στον ακόλουθο πίνακα:

	H.320	H.321	H.322	H323	H324	H.324/C	H.310
Network Types	Narrowband switched -digital, ISDN	Broadband ISDN, ATM, LAN	Guaranteed bandwidth packet-switched networks	Non-guaranteed bandwidth packet-switched networks	PSTN or POTS, the analog phone system	Mobile	Broadband ISDN, ATM, LAN
Video Codecs	H.261 H.263	H.261 H.263	H.261 H.263	H.262 H.263	H.262 H.263	H.262 H.263	MPEG-2 (H.262) H.261
Audio Codecs	G.711 G.722 G.728	G.711 G.722 G.728	G.711 G.722 G.728	G.711 G.722 G.723 G.728 G.729	G.723	G.723	MPEG-2 G.711 G.722 G.728
Multi-plexing	H.221	H.221	H.221	H.225.0	H.223	H.223A	H.222.0 H.222.1(MPEG)
Control	H.230 H.242	H.242	H.242 H.230	H.245	H.245	H.245	H.245
Multi-point	H.231 H.243	H.231 H.243	H.231 H.243	H.323	-	-	-
Data	T.120	T.120	T.120	T.120	T.120	T.120	T.120
Comm IF	I.400	AAL I.363 AJM I.361 PHY I.400	I.400,TCP/IP	TCP/IP	V.34 Modem	Mobile Radio	AA1 I.363 AJM I.361 PHY I.400

Πίνακας 6 : ITU-T προδιαγραφές

Μία σημαντική προειδοποίηση ωστόσο είναι ότι, ακόμα και όταν τα συστήματα βιντεοσυνδιάσκεψης συμμορφώνονται με τις ITU –T προδιαγραφές, αυτό που κυρίως καταφέρνουν είναι να εγγυηθούν μόνο συνεκτικότητα και επικοινωνία, γιατί η ποιότητα της βιντεοσυνδιάσκεψης εξαρτάται από μία πληθώρα άλλων παραγόντων.

Τα κυριότερα μέσα μετάδοσης για βιντεοσυνδιασκέψεις είναι:

1. ISDN
2. LAN/ETHERNET
3. ATM
4. PSTN
5. ADSL
6. WIRELESS LAN (802.11 a, b, g)

2.1.3 Προδιαγραφές για ήχο

Υπάρχουν τρεις κύριοι τύποι συμπίεσης ήχου που χρησιμοποιούνται στη βιντεοσυνδιάσκεψη. G.728 Χρησιμοποιεί το ελάχιστο εύρος ζώνης, συμπιέζοντας το σήμα όσο το δυνατόν περισσότερο, αλλά δεν μεταφέρει μεγάλη πιστότητα, γιατί η βαριά συμπίεση έχει σαν συνέπεια την απώλεια μερικών υψηλών και χαμηλών ηχητικών συχνοτήτων, όταν λαμβάνεται τελικά ο ήχος. Είναι αξιόπιστο για μερικές χρήσεις όπου απαιτείται αναγνώριση ήχου, αλλά όχι μεγάλης πιστότητας. G.711 Επίσης γνωστό και ως PCM ή Pulse Code Modulation. Ο πιο διαδεδομένος αλγόριθμος συμπίεσης, χρησιμοποιείται γενικά στην ψηφιακή τηλεφωνία. Βέβαια παρόλο το σχετικά ικανοποιητικό εύρος ζώνης που απαιτεί δεν μεταφέρει αρκετή πιστότητα. G.722 Έχει τρείς αποδόσεις, από τις οποίες πιο γνωστή είναι η τρίτη, η οποία δίνει απόκριση στις υψηλότερες συχνότητες(7kHz) που σημαίνει μεγάλη πιστότητα και καταλαμβάνει εύρος ζώνης μικρότερο από του G.711. Το εύρος ζώνης του G.722, που συνήθως χρησιμοποιείται στη βιντεοσυνδιάσκεψη είναι το καλύτερο.

2.1.4 Προδιαγραφές για εικόνα

Το 1985, το American College of Radiology (ACR) και ο National Electrical Manufacturers Association (NEMA) δημοσίευσαν ένα πρότυπο, που διηύθυνε τη μορφή δεδομένων και τη μετάδοση δεδομένων για ψηφιακές ιατρικές φωτογραφίες. Μία διορθωμένη έκδοση του προτύπου δημοσιεύτηκε το 1988. Και στις δύο εκδόσεις η μετάδοση δεδομένων οριζόταν για συνδέσεις από σημείο σε σημείο, περιβάλλον δικτύου δεν είχε ληφθεί υπόψη. ACR και NEMA ολοκλήρωσαν πρόσφατα την Τρίτη έκδοση του προτύπου που μετονομάστηκε σε DICOM v3.0 Το DICOM σημαίνει Digital Imaging and Communications in Medicine. Το ν.3.0 αναφέρεται στο ότι υπάρχουν δύο προηγούμενες εκδόσεις του προτύπου. Το DICOM αποτελεί το βιομηχανικό πρότυπο για τη *μεταφορά ιατρικών εικόνων* καθώς και άλλου είδους ιατρικής πληροφορίας μεταξύ απεικονιστικών και διαγνωστικών συστημάτων διαφορετικών κατασκευαστών, υπολογιστικών συστημάτων διαχείρισης ιατρικής πληροφορίας, ανεξάρτητων σταθμών εργασίας κ.ά.

Οι ACR/NEMA δημοσίευσαν τα πρώτα 10 από τα δεκατρία κεφάλαια του προτύπου DICAM για τη μετάδοση εικόνας. CEN, ο ευρωπαϊκός οργανισμός αντίστοιχος του ANSI, υιοθέτησε κι αυτός το DICOM.
(www.gmet.net/Lecturers/Technology/telehealthstandards.htm)

2.1.5 HL7

Ο HL7 ιδρύθηκε το 1987 με σκοπό να αναπτύξει πρότυπα για την ηλεκτρονική ανταλλαγή ιατρικών, οικονομικών και διαχειριστικών πληροφοριών

μεταξύ ανεξάρτητων υπολογιστικών συστημάτων προσανατολισμένων στην υγεία, όπως πληροφοριακά συστήματα νοσοκομείων, συστήματα κλινικών εργαστηρίων, συστήματα επιχειρήσεων και συστήματα φαρμακείων. Στα τελευταία τέσσερα χρόνια, τα μέλη του οργανισμού τριπλασιάστηκαν σε πάνω από 1500 νοσοκομεία, βιομηχανίες ιατρικής φροντίδας και μεμονωμένους ιδιώτες, περιλαμβανόμενους σχεδόν όλους τους γνωστούς κατασκευαστές αλλά και συμβούλους ιατρικής φροντίδας. Το πρότυπο HL7 υποστηρίζεται σήμερα από τους περισσότερους κατασκευαστές και χρησιμοποιείται στην πλειοψηφία του στα νοσοκομεία της Αμερικής. Επίσης χρησιμοποιείται στην Αυστραλία, Αυστρία, Γερμανία, Ολλανδία, Ισραήλ, Ιαπωνία, Νέα Ζηλανδία και Ηνωμένο Βασίλειο.

2.1.6 Χαρακτηριστικά μεγέθη ιατρικών δεδομένων-Δικτυακές απαιτήσεις ιατρικών εφαρμογών.

Παραθέτουμε κάποια ενδεικτικά στοιχεία που αφορούν ψηφιακά δεδομένα που παρέχουν τα πλέον σύγχρονα ιατρικά διαγνωστικά μηχανήματα που λειτουργούν στο ελληνικό σύστημα υγείας .

Οι εικόνες που παρέχει η ψηφιακή αξονική τομογραφία (CT)συνήθως έχουν μέγιστη ανάλυση 512X512 εικονοστοιχείων και βάθος χρώματος 8 ή 12 bit και μεγέθους 500 Kbyte. Παρόμοια είναι και τα δεδομένα των εξετάσεων των ψηφιακών μαγνητικών τομογράφων (MRI) με αναλύσεις 256 X 256 X 12 bit = 150 Kbytes, 512 X 512 X12 bit = 500 Kbytes με αποτέλεσμα μια εξέταση μαγνητικής τομογραφίας εγκεφάλου που αποτελείται από 100 περίπου λήψεις να έχει μέγεθος 1,5 Mbytes (για τα σύγχρονα δικτυακά δεδομένα, πολύ μικρό). Χαμηλότερα είναι τα χαρακτηριστικά της υπερηχογραφίας και των απεικονίσεων γ-κάμερας 256 X 256 X 16 bit.

Τα ψηφιακά δεδομένα που έχουν προκύψει από ψηφιοποίηση παραδοσιακών εξετάσεων αποτυπωμένων σε film και αναλογικό video, σίγουρα έχουν υψηλότερα χαρακτηριστικά αφού οι περιορισμοί πλέον δεν αφορούν τα κατασκευαστικές προδιαγραφές των ιατρικών διαγνωστικών συσκευών-μηχανημάτων αλλά τους ψηφιοποιητές (scanners) και τις κάρτες σύλληψης –ψηφιοποίησης video (Video acquisition Pc Cards) που καθαρά ανήκουν στην κατηγορία των Η/Υ και οι επιδώσεις τους τελευταία έχουν φτάσει σε απίστευτα υψηλά επίπεδα, υπερκαλύπτοντας τις ιατρικές απαιτήσεις. Έτσι μια ψηφιοποιημένη ακτινογραφία για παράδειγμα μπορεί να έχει ανάλυση έως και 2000 X 2000 pixels και μέγεθος 48 Mbytes (συμπιεσμένη 10 Mbytes).Οι οργανισμοί δημοσίευσης προτύπων βέβαια κάνουν προσπάθειες στον τομέα των αλγορίθμων συμπίεσης ούτως ώστε τα μεγέθη αυτά να περιοριστούν σε επίπεδα 2-5 Mbytes διατηρώντας την ιατρική διαγνωστική πληροφορία ακέραια.

Η κατηγορία τώρα των ιατρικών εφαρμογών που βασίζεται σε πραγματικού χρόνου μεταφορά και αναπαραγωγή Video (video Streaming) χρησιμοποιεί format συμπίεσης MPEG-4, MPEG-2 (εφαρμογές υψηλότερων απαιτήσεων) και περισσότερο βέβαια αλγόριθμους συμπίεσης προτύπου DICOM εξειδικευμένους για την κατηγορία αυτή, με ελαφρώς χαμηλότερες απαιτήσεις .

Στο σχεδιασμό ενός δικτύου και την επιλογή των δικτυακών συσκευών – πρωτοκόλλων επικοινωνίας κλπ. λαμβάνουμε περισσότερο υπόψη μας τις εφαρμογές για τις οποίες προορίζεται με τις υψηλότερες δικτυακές απαιτήσεις, μαζί βέβαια εξετάζονται διάφορες άλλες παράμετροι που μπορούν να αποτελέσουν περιορισμούς στην υλοποίηση, πως το κόστος, την ευκολία εγκατάστασης, την επεκτασιμότητα και συνυπολογίζοντας βέβαια τον παράγοντα της εξέλιξης της ιατρικής τεχνολογίας για πιθανές μελλοντικές εφαρμογές. Ακολουθούν κάποια χαρακτηριστικά μεγέθη της

κατηγορίας MPEG-2 που λόγω υψηλών απαιτήσεων θέτουν το 'ύψος' του πήχη στην εν λόγο εργασία.

- High-**Resolution** 1920x1152 and up to 80 MBITs/s (High **Definition** TV - HDTV)
- High-**Resolution** 1440x1440 and up to 60 MBITs/s (HDTV)
- Main-**Resolution** 720x576 and up to 15MBITs/s (digital TV and DVD-Video)
- Low-**Resolution** 352x288 and up to 4MBITs/s (S-VHS, SIF)

Level	Max. frame, width, pixels	Max. frame, height, lines	Max. frame, rate, Hz	Max. bit rate, Mbit/s	Buffer size, bits
Low	352	288	30	4	475136
Main	720	576	30	15	1835008
High-1440	1440	1152	60	60	7340032
High	1920	1152	60	80	9781248

Πίνακας 7: Κατηγορίες Video συμπίεσης MPEG-2 format

ΚΕΦΑΛΑΙΟ 3^{ο}

3.1 ΕΙΣΑΓΩΓΗ ΣΤΑ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

Ασύρματο τοπικό δίκτυο (WLAN) είναι ένα σύστημα επικοινωνίας δια μέσω ηλεκτρομαγνητικών κυμάτων μεταξύ σταθερών ή κινητών χρηστών και επιτρέπει τη μεταξύ τους διασύνδεση και μεταφορά δεδομένων

Τα ασύρματα δίκτυα και γενικότερα οι ασύρματες συνδέσεις αποτελούν μία ιδιαίτερα ευέλικτη λύση, ως επέκταση των ενσύρματων δικτύων ή ακόμα ως εναλλακτική λύση για υλοποίηση ολοκληρωμένων δικτύων.

Ασύρματα δίκτυα υπάρχουν εδώ και αρκετά χρόνια από διάφορους κατασκευαστές, αλλά η ταχύτητα που προσέφεραν (1,5Mbps) ήταν μικρή και δεν υπήρχε συμβατότητα μεταξύ τους.

Ο χώρος της ασύρματης επικοινωνίας και των προτύπων, τα οποία την καθορίζουν, βρίσκονται συνεχώς σε εξέλιξη. Οι μεγαλύτερες εταιρίες έχουν χωριστεί σε ομάδες και αναπτύσσουν ανταγωνιστικές τεχνολογίες με σκοπό την κυριαρχία σε μια αγορά που εκτινάσσεται στα ύψη από μέρα σε μέρα.

Επίσης, ένας αριθμός από καινούργιες συσκευές και προϊόντα ασύρματης επικοινωνίας που βασίζονται σε τεχνολογίες όπως spread-spectrum ραδιοφωνικά κύματα, υπέρυθρες ακτίνες, κυψελοειδείς και δορυφορικές επικοινωνίες, είναι πλέον διαθέσιμα.

Τα πρώτα ασύρματα δίκτυα που εμφανίστηκαν ήταν τα ραδιοδίκτυα δεδομένων (Data) τεχνολογίας TCP/IP. Οι πρώτες τεχνικές μεταγωγής πακέτων αναπτύχθηκαν γύρω στο 1964, ενώ ο όρος «Packet» προτάθηκε από τον D. W. Davies του National Physical Laboratory της Μεγ. Βρετανίας. Οι έρευνες του εργαστηρίου αυτού οδήγησαν στο σημερινό διεθνές δημόσιο δίκτυο μεταγωγής πακέτων X.25. Το X25 αποτέλεσε ένα πρωτόκολλο της ITU για δίκτυα WAN, το οποίο καθορίζει πως συνδέονται οι συσκευές του χρήστη και του δικτύου. Είναι ανεξάρτητο από τον τύπο των συστημάτων τα οποία είναι συνδεδεμένα στο δίκτυο. Το X.25 χρησιμοποιείται κυρίως στα δίκτυα μεταγωγής πακέτου κοινών φορέων, όπως είναι οι τηλεπικοινωνιακές εταιρίες. Οι συνδρομητές χρεώνονται ανάλογα με τη χρήση του δικτύου.

Η τεχνολογία των ασυρμάτων δικτύων μετάδοσης πακέτων άρχισε να αναπτύσσεται στην δεκαετία 1970-1980, αν και η μεγάλη ανάπτυξή της συμπίπτει με την διάδοση των μικροϋπολογιστών στην δεκαετία 1980-1990. Λόγω των ιδιαίτερων χαρακτηριστικών του μέσου μεταδόσεως τα ασύρματα δίκτυα χρησιμοποιούν εξειδικευμένα πρωτόκολλα για το υποεπίπεδο πρόσβασης μέσου (Medium Access Control) και το επίπεδο σύνδεσης δεδομένων (Data Link Layer) και συχνά και για ανώτερα επίπεδα (π.χ. δρομολόγηση πακέτων).

Σήμερα είναι διαθέσιμος ένας αριθμός από καινούργιες συσκευές και προϊόντα ασύρματης επικοινωνίας που βασίζονται σε νέές τεχνολογίες και νέα πρότυπα. Τα τελευταία χρόνια οι κινητοί υπολογιστές (notebook, laptop, palmtop) που ενσωματώνουν τεχνολογία ασύρματης πρόσβασης, είναι διαθέσιμοι και ελκυστικοί για το ευρύ κοινό, αφού έχουν πλέον συγκρίσιμο κόστος, υπολογιστική ισχύ και ποιότητα υπηρεσιών με τους σταθερούς υπολογιστές. Όλα αυτά έχουν σαν αποτέλεσμα την έρευνα για την ανάπτυξη προτύπων για την υποστήριξη των ασύρματων επικοινωνιών.

Την τελευταία δεκαετία πολλά είναι τα πρότυπα που διεκδικούν ένα κομμάτι της αγοράς. Bluetooth, HiperLAN, HomeRF, 802.11a, 802.11b, 802.11g είναι κάποια από τα πολυδιαφημιζόμενα ονόματα προτύπων.

Σε επόμενα κεφάλαια, θα περιγράψουμε αναλυτικότερα τα πρότυπα 802.11 και πως αυτά καθίστανται τα καταλληλότερα πρότυπα ασύρματων δικτύων για τη μεταφορά ιατρικών δεδομένων. Λιγότερο αναλυτικά θα γνωρίσουμε τους υπόλοιπους τύπους προτύπων που αναφέραμε.

3.2 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΑΣΥΡΜΑΤΗΣ ΔΙΚΤΥΩΣΗΣ

3.2.1 Κινητικότητα (mobility):

Τα WLAN δίνουν τη δυνατότητα σε χρήστες οι οποίοι είναι εν κινήσει (σε μεταφορικά μέσα, αεροδρόμια, συσκέψεις, εξυπηρέτηση πελατών), να έχουν πρόσβαση σε πληροφορίες όταν και όπου τις χρειάζονται. Σε αντίθεση με τα ενσύρματα δίκτυα που δεν παρέχουν αυτή κινητικότητα. Αξίζει να αναφερθούν κάποιες Αμερικανικές έρευνες, ενδεικτικές της 'αναγκαιότητας' πλέον, της κινητικότητας των WLAN:

Από το 70% των επιχειρηματιών που ταξιδεύουν και φέρουν lap-top, το 68% εξέφρασε ενδιαφέρον στην ασύρματη πρόσβαση Διαδικτύου στα ξενοδοχεία, στα αεροπλάνα και στους αερολιμένες (Src: McKinsey/Arezone, 2000)

93% των επιχειρηματιών, ενδιαφέρονται για την χρησιμοποίηση μιας ασύρματης υπηρεσίας του τοπικού LAN στους αερολιμένες, 60% στα café ή εστιατόρια (Src: BWCS, 2001)

Όταν αυτό είναι δυνατόν, το 97% των Αμερικανών ταξιδιωτών επιλέγουν ένα άλλο αερολιμένα ή ξενοδοχείο όταν δεν υπάρχει διαθέσιμο WLAN (Src: Boingo, 2001).

3.2.2 Ταχύτητα και ευελιξία εγκατάστασης:

Η εγκατάσταση ενός WLAN εξαλείφει την ανάγκη της χρήσης των καλωδίων η οποία απαιτεί συνήθως μελέτη, χρόνο και αρκετό κόστος λόγω των απαιτούμενων τροποποιήσεων των κτιριακών εγκαταστάσεων, όπου δεν έχει προβλεφθεί. Η ασύρματη τεχνολογία επιτρέπει την υλοποίηση δικτύων η οποία υπό άλλες συνθήκες θα ήταν αδύνατη.

Μακροπρόθεσμα, η εγκατάσταση, η αναβάθμιση και το κόστος συντήρησης των συστημάτων WLAN, αποτελούν μια οικονομικότερη λύση

Υπάρχουν και μερικά περιβάλλοντα στα οποία τα ασύρματα τοπικά δίκτυα αποτελούν καλύτερη λύση από ένα δίκτυο με καλώδιο. Στην κατηγορία αυτή ανήκουν:

- Περιβάλλοντα μεγάλων εκτάσεων, όπως οι χώροι παραγωγής ενός εργοστασίου ή μιας αποθήκης.
- Πολύ παλιά κτίρια, στα οποία είτε απαγορεύεται η οποιαδήποτε τροποποίηση των κτιριακών εγκαταστάσεων, είτε η καλωδίωση είναι ανεπαρκής ή ανύπαρκτη
- Μικρά γραφεία, όπου η εγκατάσταση και η συντήρηση ενός ενσύρματου δικτύου είναι αντιοικονομική

3.2.3 Επεκτασιμότητα

Αποτελεί μια από τις συχνότερα παρουσιαζόμενες ανάγκες των ήδη εγκατεστημένων τοπικών ενσύρματων δικτύων, καθώς οι απαιτήσεις δικτύωσης ολοένα αυξάνονται. Η ενσύρματη επέκταση των LANs, είναι μια διαδικασία ιδιαίτερα δύσκολη και όχι πάντα εφικτή, αφού συχνά προϋποθέτει αλλαγές της κτιριακής υποδομής και επεμβάσεις εντός του χώρου εργασίας.

Τα ασύρματα μέσα προσπερνούν τα παραπάνω προβλήματα, δίνοντας μια ευέλικτη λύση.

3.2.4 Διασύνδεση

Μια άλλη συνιστώσα της επεκτασιμότητας, είναι και η διασύνδεση δυο ή παραπάνω αυτόνομων τοπικών δικτύων που βρίσκονται σε διαφορετικούς χώρους (διαφορετικά κτιριακά συγκροτήματα γειτονικά ή απομακρυσμένα, εντός των ορίων μιας πόλης, των προαστίων της κ.λ.π)

Για παράδειγμα αν είναι δύσκολο να ενώσουμε δύο δίκτυα σε δύο διαφορετικά κτίρια με μια οπτική ίνα (λόγω εδάφους, κόστους, αδειών κ.τ.λ.) συμφέρει να χρησιμοποιήσουμε ασύρματες μεθόδους ,δεδομένου ότι το ασύρματο μέσο μπορεί να φθάσει σε θέσεις που το καλώδιο δεν μπορεί.

Στην περίπτωση αυτή, χρησιμοποιείται μια ασύρματη σύνδεση από σημείο-σε- σημείο (wireless point-to-point link) μεταξύ των δύο κτιρίων. Οι συσκευές που συνήθως διασυνδέονται είναι γέφυρες ή δρομολογητές.

3.2.5 Συμβατότητα

Τα WLAN μπορούν να υλοποιηθούν, σε μια ποικιλία από τύπους για να ικανοποιήσουν τις ανάγκες συγκεκριμένων εγκαταστάσεων και εφαρμογών. Οι διαμορφώσεις αλλάζουν εύκολα και επεκτείνονται από μικρά δίκτυα κατάλληλα για έναν μικρό αριθμό χρηστών μέχρι πλήρως ανεπτυγμένα δίκτυα που καλύπτουν εκατοντάδες χρήστες.

Η εξέλιξη στον τομέα της ασύρματης δικτύωσης, ο σχεδιασμός και η υλοποίηση καινούργιων προτύπων δίνει έμφαση στην ενσωμάτωση-συμβατότητα προϋπαρχόντων τεχνολογιών.

Επίσης λόγω της ευρείας ανταπόκρισης στην αγορά, οι κατασκευαστές ενσωματώνουν ασύρματη επικοινωνία σε ολοένα και περισσότερες περιφερικές συσκευές (Palmtops, PDA, Laptops, Barcode readers, Δικτυακοί εκτυπωτές, Digital Scanners, Wireless Cameras, κλπ) και εξειδικευμένες για ιατρική χρήση συσκευές. Ακόμα τελευταία έχουν κυκλοφορήσει wireless modules, ολοκληρωμένες ασύρματες κάρτες που επιτρέπουν τη δικτύωση οποιονδήποτε ψηφιακών συσκευών εξειδικευμένων και μη.

3.2.6 Μειωμένο κόστος

Ενώ η αρχική επένδυση που απαιτείται για τον εξοπλισμό και την εγκατάσταση ενός WLAN μπορεί σε μερικές περιπτώσεις να είναι υψηλότερη από το αντίστοιχο κόστος για μια ενσύρματη δικτύωση, το συνολικό κόστος λειτουργίας μπορεί να είναι σημαντικά χαμηλότερο, καθώς τα μακροπρόθεσμα κέρδη είναι πολύ

μεγαλύτερα σε δυναμικά περιβάλλοντα όπου απαιτούνται πολύ συχνές μετακινήσεις και αλλαγές.

Ακόμα, το κόστος συντήρησης και τροποποίησης στα ενσύρματα δίκτυα είναι πολλαπλάσιο από αυτό των ασυρμάτων.

3.2.7 Νομαδική πρόσβαση

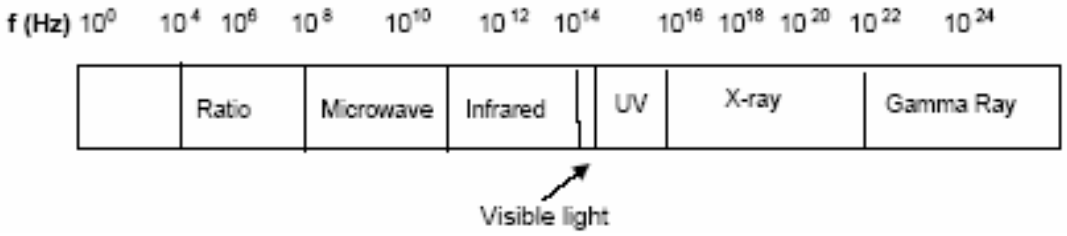
Η νομαδική πρόσβαση είναι χρήσιμη σε χώρους όπως μια επιχείρηση, ή μια πανεπιστημιούπολη, όπου τα κτίρια βρίσκονται συγκεντρωμένα ανά ομάδες. Στις περιπτώσεις αυτές, οι χρήστες μπορούν να μετακινούνται μέσα στο χώρο της επιχείρησης ή του πανεπιστημίου και με τους φορητούς υπολογιστές τους να προσπελαύνουν αρχεία των servers και των υπολογιστών που βρίσκονται συνδεδεμένοι σε κάποιο τοπικό δίκτυο.

Πάνω στη νομαδική πρόσβαση επιχειρήσεων, βασίζεται ένα πολύ μεγάλο κομμάτι της διαφημιστικής καμπάνιας μεγάλων εταιριών ασυρμάτων δικτύων, όπου από έρευνές τους έχει προκύψει ότι τα οφέλη κάθε επιχείρησης που οι εργαζόμενοί της κάνουν χρήση της ασύρματης δικτύωσης μέσω laptops, είναι πολύπλευρα. Μια πρόσφατη μελέτη που πραγματοποιήθηκε από τη NOP World—Technology για την Cisco Systems δείχνει ότι μπορεί έτσι κάποιος να αυξήσει μια έως δύο ώρες ημερησίως την παραγωγικότητα, ανά εργαζόμενο, κάνοντας χρήση ασύρματης σύνδεσης. Σήμερα, 45 εκατομμύρια επαγγελματίες εργάζονται ‘εν κινήσει’.

ΚΕΦΑΛΑΙΟ 4^{Ο}

4.1 WLANs, ΤΕΧΝΟΛΟΓΙΕΣ ΔΙΑΔΟΣΗΣ

Στις ασύρματες ζεύξεις χρησιμοποιούνται διάφορες τεχνολογίες που μπορούν να κατηγοριοποιηθούν ανάλογα με την τεχνική μετάδοσης δεδομένων που χρησιμοποιούν, όπως η **τεχνολογία ραδιοσυχνοτήτων** (radio frequency - **RF**), η **τεχνολογία υπερύθρων** (Infrared -**IR**) και η **τεχνολογία μικροκυμάτων** (microwave - **MW**).



Σχήμα 8: Το ηλεκτρομαγνητικό φάσμα.

Προκειμένου να αποφευχθεί το χάος, από τη χρήση των συχνοτήτων, υπάρχουν εθνικοί και διεθνείς οργανισμοί που αποφασίζουν ποιος θα χρησιμοποιήσει ποιες συχνότητες. Στην Αμερική υπάρχει η FCC και παγκοσμίως, όπως προαναφέραμε σε προηγούμενο κεφάλαιο, η ITU-R.

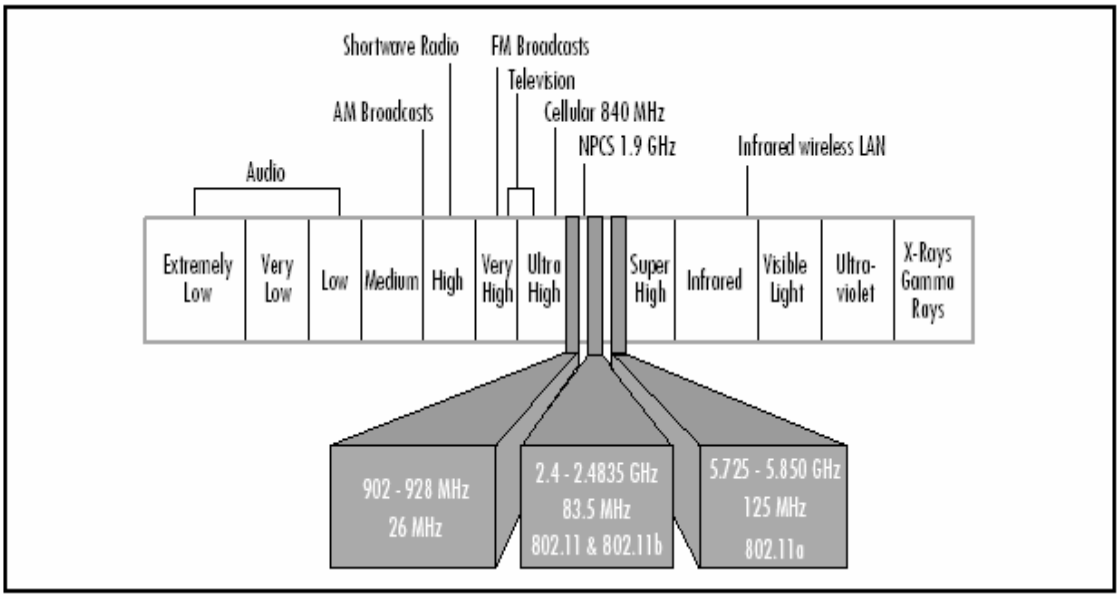
4.1.1 Φάσμα και Οργανισμοί Πρότυποποίησης

Η κατασκευή όλων των τεχνολογιών WLAN στηρίχτηκε στην κοινή χρήση του φάσματος συχνοτήτων ISM (Instrumentation, Scientific, and Medical), όπου έχει εξουσιοδοτηθεί από το 1985, από τον οργανισμό FCC, (Federal Communications Commission, Η.Π.Α) ο οποίος καθορίζει το εύρος συχνοτήτων που θα χρησιμοποιείται για κάθε τηλεπικοινωνιακή εφαρμογή.

Σε διεθνές επίπεδο η Διεθνής Τηλεπικοινωνιακή Ένωση (ITU, International Telecommunication Union), με κύριο όργανό της την CCITT (Consultative Committee for International Telephone and Telegraph) τυποποίησε τα modems για μετάδοση φωνής. Επιπλέον το IEEE (Institute of Electrical and Electronics Engineers, Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών μηχανικών) και ο ISO (International Standards Organization, Διεθνής Οργανισμός Τυποποίησης) διατύπωσαν πρότυπα για LAN, ενώ το ATM (Asynchronous Transfer Mode) Forum προώθησε την ολοκλήρωση ποικίλων υπηρεσιών σε υψηλής ταχύτητας LANs ή WANs.

Όσον αφορά την τυποποίηση της μετάδοσης στα WLAN, το 1990 ο IEEE όρισε την ομάδα εργασίας 802.11, που θα συνέθετε τα πρότυπα για χρήση στη "Βιομηχανική, Επιστημονική και Ιατρική ζώνη" (Indusrial, Scientific, and Medical Band). να αναπτύξει ένα παγκόσμιο πρότυπο για τις ασύρματες συσκευές και δίκτυα, που λειτουργούν στα 2.4GHz στα 1 και 2 Mbps. Αυτό που έκαναν τα πρότυπα,

Στον Ευρωπαϊκό χώρο το αντίστοιχο της FCC είναι η CEPT (Conference Europeen des Administrations des Postes et des Telegraphes). Η επιτροπή αυτή έχει ορίσει το πρότυπο HIPERLAN, στο οποίο υπόκεινται όλες οι ελεύθερες συχνότητες.



Σχήμα 9:Μπάντα των ISM

Οι μπάντες ISM(Industrial Scientific and Medical) μπορούν να χρησιμοποιηθούν χωρίς άδεια. Στο σχήμα μπορούμε να δούμε αναλυτικά το ραδιοφωνικό φάσμα και τις ελεύθερες περιοχές του.

4.2 ΤΕΧΝΟΛΟΓΙΕΣ WLAN

Ένα πρωτόκολλο επικοινωνίας, είναι ένα σύνολο κανόνων οι οποίοι καθορίζουν τον τρόπο δια- σύνδεσης των συστημάτων που επικοινωνούν, καθώς και τον τρόπο πρόσβασης των κόμβων στο μέσο μετάδοσης

4.2.1 Το πρότυπο IEEE 802.11

Το πρότυπο αυτό ανέπτυξε τις προδιαγραφές του Φυσικού Επιπέδου (PHY) και του Επιπέδου Προσπέλασης Μέσου (MAC) για την ασύρματη επικοινωνία σταθερών, φορητών και κινητών σταθμών σ' ένα WLAN. Συγκεκριμένα περιγράφει το πως μία συσκευή, που ακολουθεί το IEEE 802.11 , θα λειτουργήσει σε ένα δίκτυο με υποδομή και σε ένα πολλαπλά επικαλυπτόμενο (multiple overlapping) WLAN, καθώς επίσης τις διαδικασίες του MAC επιπέδου και τις απαιτήσεις πιστοποίησης μιας τέτοιας συσκευής.

Το IEEE 802.11 έχει σαν στόχο να αναπτύξει τις προδιαγραφές του επιπέδου MAC, το οποίο είναι ανεξάρτητο του φυσικού επιπέδου. Οι τεχνικές μετάδοσης στο φυσικό (PHY) επίπεδο και οι αντίστοιχοι ρυθμοί δεδομένων είναι:

- Frequency Hopping Spread Spectrum με 1 Mbps.
- Direct Sequence Spread Spectrum με 1 ή 2 Mbps.
- Infrared (Υπέρυθρες) με 1 ή 2 Mbps.

Το πρότυπο 802.11 ορίζει τρία διαφορετικά φυσικά επίπεδα (PHY). Η ύπαρξη περισσότερων από ένα επιλογών για το φυσικό επίπεδο επιτρέπει στους σχεδιαστές συστημάτων να επιλέγουν κάθε φορά την τεχνολογία εκείνη, η οποία ταιριάζει καλύτερα με το κόστος, την απόδοση και το προφίλ των λειτουργιών μιας συγκεκριμένης εφαρμογής.

Ειδικότερα, το πρότυπο προσδιορίζει ένα οπτικό PHY που χρησιμοποιεί υπέρυθρες ακτίνες για τη μετάδοση δεδομένων και δύο ΦΕ ραδιοσυχνότητας (RF-based), τα οποία λειτουργούν στην περιοχή συχνοτήτων των 2,4 GHz (από 2,4 - 2,4835 GHz) του ISM.

Στο παρακάτω σχήμα απεικονίζονται τα επίπεδα που καλύπτονται από το πρότυπο.

<table>
<tr><td>802.2</td><td colspan="2">Υπο-επίπεδο Ελέγχου Λογικών Καναλιών (LLC sublayer)</td><td rowspan="2">Επίπεδο Σύνδεσης Δεδομένων</td></tr>
<tr><td>802.11</td><td colspan="2">Υπο-επίπεδο Προσπέλασης Μέσου (MAC sublayer)</td></tr>
<tr><td>Υπέρυθρο ΦΕ</td><td>Direct Sequence ΦΕ</td><td>FH (Frequency Hop) ΦΕ</td><td>Φυσικό Επίπεδο</td></tr>
</table>

Σχήμα 10: Τα επίπεδα που καλύπτονται από το πρότυπο 802.11.
Διακρίνονται οι τρεις διαφορετικές τεχνολογίες του Φυσικού Επιπέδου που υποστηρίζει το πρότυπο.

Οι δύο διαφορετικές τεχνολογίες PHY ραδιοσυχνότητας που απεικονίζονται στο παραπάνω σχήμα, ανήκουν στην κατηγορία των τεχνικών *διασποράς φάσματος (spread spectrum techniques)*. Οι τεχνολογίες διασποράς φάσματος που προσδιορίζει το 802.11 για τα δύο PHY ραδιοσυχνότητας είναι η τεχνική διασποράς φάσματος άμεσης ακολουθίας *(Direct Sequence Spread Spectrum - DSSS)* και η τεχνική διασποράς φάσματος αναπήδησης συχνότητας *(Frequency Hopping Spread Spectrum – FHSS)*

Το μικρό εύρος κάλυψης που έχει το υπέρυθρο PHY το καθιστά κατάλληλο μόνο για εφαρμογές κλειστού χώρου, όπως ένα μικρό γραφείο, ένα δωμάτιο, κλπ. Αντίθετα, οι άλλοι δύο τύποι PHY μπορούν να χρησιμοποιηθούν σε εφαρμογές όπου υπάρχει η ανάγκη κάλυψης μεγάλων περιοχών (ανοικτών ή κλειστών), όπως είναι ένα νοσοκομείο, μια πανεπιστημιούπολη, τα κτίρια μιας επιχείρησης, κλπ.

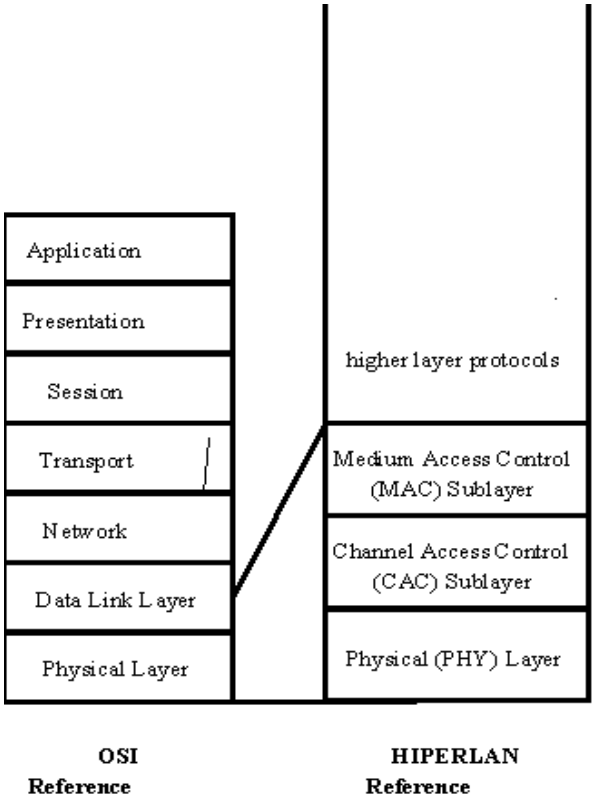
4.2.2 High Performance Radio LAN (HIPERLAN)

Ο αντίστοιχος ευρωπαϊκός οργανισμός του FCC στις ΗΠΑ, Conference Europeen des Administrations des Posts et des Telegraphes (CEPT), διένειμε 150 MHz καθαρού ηλεκτρομαγνητικού φάσματος στα 5.1 GHz, για υψηλής αξίας δεδομένων ασύρματα LANs. Το ευρωπαϊκό ινστιτούτο προτύπων για τηλεπικοινωνίες (European Telecommunications Standards Institute, ETSI), ανάθεσε σε μία υποομάδα τεχνικών, να ορίσουν τα πρότυπα σε αυτές τις ζώνες. Ο τωρινός σχεδιασμός είναι για πέντε κανάλια, το καθένα περίπου 23.5 Mb/s (HIPERLAN Standard 1996). Η μετάδοση σε αυτές τις ζώνες είναι ελεύθερη, αλλά υπόκειται στους περιορισμούς του ηλεκτρομαγνητικού φάσματος.

Το HIPERLAN περιορίζεται στα δύο χαμηλότερα επίπεδα του OSI (Open Systems Interconnect), το φυσικό επίπεδο και το επίπεδο σύνδεσης δεδομένων. Ειδικότερα, το μοντέλο αναφοράς αποτελείται από το υπο-επίπεδο ελέγχου προσπέλασης του μέσου (MAC), το υπο-επίπεδο ελέγχου προσπέλασης του καναλιού (CAC), και το φυσικό επίπεδο.

Το ινστιτούτο ETSI-RES10 έχει ορίσει το HIPERLAN ως ένα **ασύρματο δίκτυο LAN που επιτρέπει σταθερή ζεύξη κινούμενων σταθμών, με χαμηλό όριο**

ταχύτητας 1-2 m/s. Σε μια μετάδοση ισχύος 1W, ένα δίκτυο HIPERLAN παρέχει μία ακτίνα λήψης 50m μέσα σε εσωτερικό χώρο περίπου.



Σχήμα 11: Τα επίπεδα του HIPERLAN, συσχετιζόμενα με τα αντίστοιχα του OSI

Το HiperLAN υπάρχει σε δύο εκδόσεις, τη HiperLAN Type 1 που τυποποιήθηκε το 1996 και υποστηρίζει ταχύτητες μέχρι 24Mbps και τη HiperLAN Type 2, η ανάπτυξη της οποίας δεν έχει ακόμη ολοκληρωθεί και που θα υποστηρίζει ταχύτητες μέχρι 54Mbps. Αμφότερες οι εκδόσεις του HiperLAN χρησιμοποιούν τη συχνότητα των 5GHz, η οποία στην Αμερική και στην Ιαπωνία είναι ελεύθερη και στην Ευρώπη έχει επισήμως παραχωρηθεί για χρήση από τα ασύρματα δίκτυα, με αποτέλεσμα αφενός μεν να μη δημιουργούνται προβλήματα με τα δίκτυα που τρέχουν στα 2,4GHz και αφετέρου οι συσκευές HiperLAN να μπορούν να χρησιμοποιηθούν σε οποιοδήποτε μέρος του κόσμου χωρίς τροποποιήσεις.

HIPERLAN I: Χρησιμοποιεί μια παραλλαγή του CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), που στηρίζεται στο χρόνο ζωής του πακέτου, την προτεραιότητα των πακέτων και τις αναμεταδόσεις στο επίπεδο MAC (Μέσο ελέγχου πρόσβασης).

HIPERLAN II: Χρησιμοποιεί την τεχνική διαμόρφωσης OFDM (Ορθογώνιος πολυπλέκτης διαίρεσης συχνότητας), ενώ υποστηρίζει διάφορους ρυθμούς μετάδοσης 6,9,12,18,27,36 και 54 Mbps. Είναι ένα σύστημα ασυρμάτου ATM (Τρόπος ασύγχρονης μεταφοράς), ενώ το πρωτόκολλο που χρησιμοποιείται στο υπόστρωμα MAC στηρίζεται σε μια διαφοροποιημένη λειτουργία της τεχνικής TDMA (Time Division Multiple Access).

	HIPERLAN 1	HIPERLAN 2	HIPERLAN 3	HIPERLAN 4
Application	wireless LAN	access to ATM fixed networks	wireless local loop	point-to-point wireless ATM connections
Frequency	5.1-5.3GHz			17.2-17.3GHz
Topology	decentralized ad-hoc/infrastructure	cellular, centralized	point-to-multipoint	point-to-point
Antenna	omni-directional		directional	
Range	50 m	50-100 m	5000 m	150 m
QoS	statistical	ATM traffic classes (VBR, CBR, ABR, UBR)		
Mobility	<10m/s		stationary	
Interface	conventional LAN	ATM networks		
Data rate	23.5 Mbit/s	>20 Mbit/s		155 Mbit/s
Power conservation	yes		not necessary	

Πίνακας 12: Πρότυπα HIPERLAN

Μια άλλη ιδιαιτερότητα του HiperLAN είναι επίσης το ad hoc roaming, η δυνατότητα δηλαδή της αυτόματης προώθησης των δεδομένων από access point σε access point σε περίπτωση που ο δέκτης δεν βρίσκεται στο βεληνεκές του πομπό. Εκτός από αυτό, η υπεροχή στην ταχύτητα και η δυνατότητα QoS (Quality Of Service, Ποιότητα Υπηρεσιών) που μόνο το HiperLAN έχει από τα πρότυπα ασύρματης δικτύωσης. Με το QoS μπορούν τα πακέτα δεδομένων να κατηγοριοποιούνται και να αποκτούν διαφορετική σειρά προτεραιότητας ανάλογα με το είδος τους. Έτσι, τα πακέτα που αφορούν ένα video π.χ., μπορεί να έχουν μεγαλύτερη προτεραιότητα κατά τη μεταφορά, με αποτέλεσμα την πιο ομαλή εμφάνισή του. Το HiperLAN2, σε αντίθεση με όλα τα υπόλοιπα πρότυπα, είναι συμβατό με μια τεράστια ποικιλία δικτύων γιατί, εκτός από το να συνδέεται με δίκτυα Ethernet, έχει τη δυνατότητα και για μεταφορά πακέτων IP, Firewire, ATM, UMTS κ.ά.

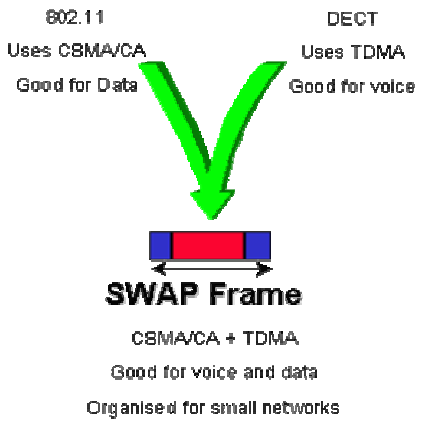
Τα ETSI project BRAN (ραδιοδίκτυα ευρυζωνικής πρόσβασης) αναπτύσσουν μια νέα γενεά προτύπων που θα υποστηρίξει και τα ασύγχρονα δεδομένα και τις υπηρεσίες στις οποίες ο χρόνος μετάδοσης είναι κρίσιμος (π.χ. η φωνή και το βίντεο), για να επιτύχουν μια αποδεκτή ποιότητα της υπηρεσίας (QoS). Ένα από αυτά τα πρότυπα είναι το High PErformance Radio Local Area Network type 2 (HIPERLAN/2) που θα υποστηρίζει μετάδοση multimedia εφαρμογών μεταξύ διαφορετικών ευρυζωνικών κεντρικών δικτύων και κινητών τερματικών.

4.2.3 Home RF

Τον Μάρτιο του 1998 η ομάδα εργασίας HomeRF ανέπτυξε μια ενιαία προδιαγραφή, το κοινό ασύρματο πρωτόκολλο εφαρμογής SWAP (Shared Wireless Access Protocol). Η συχνότητα λειτουργίας είναι τα 2.4 GHz. Το πρότυπο HomeRF 2.0 για τις ασύρματες μεταδόσεις χρησιμοποιεί στο φυσικό στρώμα την τεχνική FHSS, (την τεχνική αναπήδησης συχνότητας Frequency Hopping) και υποστηρίζει ταχύτητες διαμεταγωγής των δεδομένων που ανέρχονται στα 10Mbit/s και χρησιμοποιείται για την ασύρματη ενδοεπικοινωνία μεταξύ των ηλεκτρικών συσκευών, όπως ηλεκτρονικοί υπολογιστές, ασύρματα τηλέφωνα DECT, PDAs, ενώ χρησιμοποιείται και από ορισμένες συσκευές ήχου και εικόνας.

Το SWAP χρησιμοποιεί στο υπόστρωμα MAC ένα πρωτόκολλο, το οποίο συνδυάζει χαρακτηριστικά και λειτουργίες από το DECT και το 802.11.

Το HomeRF μπορεί πλέον να εφαρμοστεί εκτός από τις Η.Π.Α και σε προϊόντα που προορίζονται για την Ευρωπαϊκή αγορά. Αυτό προήλθε ύστερα από την αλλαγή των κανόνων που θέσπισε ο ETSI (European Telecommunications Standards Institute) που αφορούν τη διαχείριση της συχνότητας των 2,4GHz. Ο Ευρωπαϊκός όμιλος HomeRF ιδρύθηκε στα τέλη του 2001.



Σχήμα 13 : Προέλευση SWAP

<u>Υπόστρωμα MAC του HomeRF</u>

Το MAC του SWAP παρέχει τα ακόλουθα χαρακτηριστικά γνωρίσματα:

- Καλή υποστήριξη για τη φωνή και στοιχεία με τη χρησιμοποίηση και TDMA (Time Division Multiple Access) και των μηχανισμών πρόσβασης CSMA/ CA (Carrier Sense Multiple Access with Collision Avoidance)
- Υποστήριξη για 4 υψηλής ποιότητας συνδέσεις φωνής.
- Υψηλό ρυθμό απόδοσης δεδομένων 1.6Mbps.
- Ασφάλεια δεδομένων.
- Διαχείριση δύναμης για τους ισόχρονους και ασύγχρονους κόμβους.
- 24 bit Network ID.

Πίνακας 14: Τεχνολογίες WLAN- Συγκριτικά στοιχεία

Συγκριτικός πίνακας τεχνολογιών	Bluetooth	HomeRF	IEEE802.11	IEEE802.11b	IEEE802.11a	HiperLAN1	HiperLAN2
Ταχύτητα	1Mbps	2Mbps	2Mbps	11Mbps	54Mbps	24Mbps	54Mbps
Εμβέλεια	10μ	50μ	100μ	100μ	100μ	50μ	30-150μ
Συχνότητα	2,4GHz	2,4GHz	2,4GHz	2,4GHz	5GHz	5GHz	5GHz
Διασύνδεση	Καμία	Ethernet	Ethernet	Ethernet	Ethernet	Ethernet	Ethernet, ATM,IP, UMTS, Firewire, PPP
Κατάσταση	Διαθέσιμο	Διαθέσιμο	Διαθέσιμο	Διαθέσιμο	Διαθέσιμο	Διαθέσιμο	Διαθέσιμο
Υποστηρικτέ	Ericsson, IBM, Toshiba, Intel, Nokia, Motorola	Proxim, Intel,HP, 3COM, Motorola		Cisco, Lucent, 3Com, Apple, Compaq, Zoom, Dell, Nokia		ETSI, Proxim, HP, Xircom, IBM, Nokia	ETSI,HP, Xircom, IBM,TI, Dell Ericsson, Nokia, Proxim

4.2.4 Τεχνολογία Bluetooth

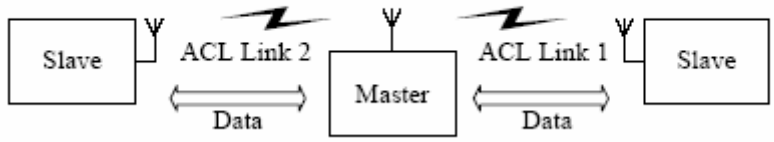
Το πρότυπο Bluetooth που δημιουργήθηκε από τις Ericsson, IBM, Toshiba, Intel, Nokia και Motorola και υποστηρίζεται και από άλλες πολλές εταιρίες, είναι το de facto πρότυπο περιορισμένου φάσματος ασύρματης τεχνολογίας με σκοπό να συνδέσει ποικίλες ηλεκτρονικές συσκευές, (κινητά, PDA, PC, εκτυπωτές, fax, modem, πληκτρολόγια κ.τ.λ.) με χαμηλή κατανάλωση (0,01W) και χαμηλό κόστος. Τα δίκτυα αυτά ονομάζονται PAN (Personal Area Networks, Δίκτυα Προσωπικού Χώρου) γιατί σε αντίθεση με τα LAN, ο χώρος ο οποίος καλύπτεται είναι πολύ λίγα μέτρα. Τα PAN έχουν ουσιαστικά σχεδιαστεί με σκοπό να επιτρέπουν την αντικατάσταση των καλωδίων και των υπέρυθρων συνδέσεων .

Το Bluetooth λειτουργεί στη βιομηχανική επιστημονική ζώνη συχνότητας ιατρικής (ISM) 2.4GHz. Χάρη στην frequency hopping τεχνική, το Bluetooth έχει ως σκοπό θεωρητικά να είναι άνοσο στις παρεμβάσεις στην ανωτέρω ζώνη συχνότητας, επιτυγχάνοντας ένα συνολικό, ακατέργαστο εύρος ζώνης 1Mbit/s μέσα στην

χαρακτηριστική απόσταση των 10m (για Power Class 2 και 3 Bluetooth συσκευές) μέχρι 100m (για Power Class 1 συσκευές).

Η ταχύτητα μεταφοράς δεδομένων είναι μέχρι 1Mbps ενώ είναι δυνατή και η ταυτόχρονη μεταφορά ήχου. Το Bluetooth υποστηρίζει τόσο άμεση επικοινωνία ανάμεσα σε δύο συσκευές (point to point) όσο και επικοινωνία πολλών συσκευών με ένα access point (point to multipoint). Η χωρητικότητά του είναι 8 συσκευές ανά δίκτυο αλλά η μέθοδος εναλλαγής συχνοτήτων (1600 εναλλαγές ανά δευτερόλεπτο σε 79 κανάλια) επιτρέπει σε περισσότερα από 1 δίκτυα να συνυπάρχουν στον ίδιο χώρο. Η ελάχιστη απόσταση ανάμεσα στον πομπό και το δέκτη είναι 10 εκατοστά και η μέγιστη 100 μέτρα. Από πλευράς ασφάλειας, αν και το Bluetooth δεν παρέχει ιδιαίτερα υψηλό επίπεδο, η μικρή του εμβέλεια περιορίζει τον κίνδυνο.

Το παρακάτω σχήμα απεικονίζει μια τυπική μορφή διασύνδεσης μεταξύ τριών συσκευών Bluetooth. Η μία από αυτές αποτελεί τον Master της σύνδεσης, ενώ οι άλλες δύο καλούνται Slaves. Κάθε Master μπορεί να συνδεθεί με μέχρι επτά Slaves μέσω ασύγχρονων (Asynchronous Connection-Less, ACL) συνδέσεων τύπου μεταγωγής πακέτου, αποτελώντας μια τοπολογία piconet. Οι ACL συνδέσεις μπορούν να είναι και τύπου σημείο -σε-πολλαπλά σημεία (point– to- multipoint) με δυνατότητα ταυτόχρονης εκπομπής από τον Master προς όλους τους Slaves (broadcasting), ενώ παρέχουν πραγματικές ταχύτητες μετάδοσης μέχρι και 721kbps. Η ορθότητα της μετάδοσης εξασφαλίζεται μέσω ενός μηχανισμού επαναμετάδοσης των χαμένων πακέτων, ο οποίος όμως μειώνει δραματικά το μετρούμενο ρυθμό μετάδοσης των δεδομένων, ειδικά σε περιβάλλοντα όπου υπάρχει ηλεκτρομαγνητική παρεμβολή στην περιοχή των 2.4GHz.

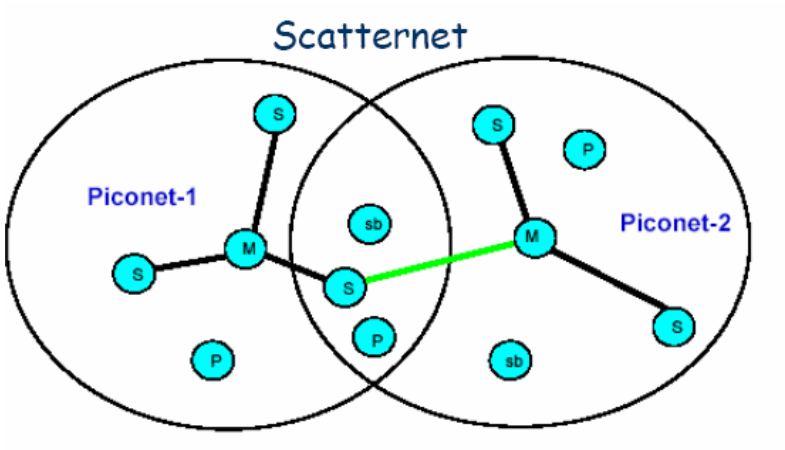


Σχήμα 15: Χαρακτηριστική οργάνωση σύνδεσης Bluetooth

Κατά τη διάρκεια μιας σύνδεσης ACL, δύο κατηγορίες πακέτων μπορούν να χρησιμοποιηθούν: Το Data-Medium rate (DM) packets και το Data-High rate (DH) packets. Η διαφορά τους είναι ότι τα τελευταία δεν περιλαμβάνουν Forward Error Correction (FEC) πληροφορίες. Υπάρχουν τρία DM και τρεις τύποι πακέτων DH που καλούνται DM1, DM3, DM5 και DH1, DH3, DH5 αντίστοιχα. Ένα DM3 πακέτο είναι ένα εκτεταμένο DM1 πακέτο. Ενώ ένα DM1 πακέτο στέλνεται κατά τη διάρκεια μιας ενιαίας μετάδοσης slot, 3 DM υιοθετούν το χρόνο τρία slots κ.λ.π.... Το ίδιο πράγμα αντιπροσωπεύει όλο τον άλλο τύπο πακέτων ACL. Υπάρχει επίσης ένα άλλο πακέτο ACL αποκαλούμενο τύπος AUX1, το οποίο δεν αναμεταδίδεται ποτέ.

Η προδιαγραφή Bluetooth επιτρέπει την ασύρματη επικοινωνία συσκευών μέσω σύγχρονων συνδέσεων (Synchronous Connection- Oriented, SCO), οι οποίες αποτελούν σημείο – σε - σημείο συνδέσεις μεταξύ ενός Master κι ενός Slave.

Κάθε Master συσκευή μπορεί να αποκαταστήσει ταυτόχρονα μέχρι τρεις το πολύ SCO συνδέσεις. Οι SCO συνδέσεις είναι κατάλληλες για την εξυπηρέτηση χρονικά κρίσιμων εφαρμογών και εγγυώνται σταθερό ρυθμό μετάδοσης ίσο προς 64kbit/s.



M: master
S: slave
Sb: stand by
P: parket/hold

Σχήμα 16: Αρχιτεκτονική Blouetooth

4.3 LMDS

Είναι ένα ευρυζωνικό (25-31 GHz), ασύρματο point-to-multipoint σύστημα επικοινωνίας που λειτουργεί σε συχνότητες πάνω από 20 GHz, (αναλόγως τη χώρα χορήγησης αδειών), που μπορεί να χρησιμοποιηθεί για την αμφίδρομη (διπλής κατεύθυνσης) παροχή ψηφιακής φωνής-δεδομένων-video-Internet-τηλεοπτικές υπηρεσίες.

Local: Τα χαρακτηριστικά του ύψους αυτού της συχνότητας που χρησιμοποιείται (GHz), δηλαδή του εύρους ζώνης LMDS περιορίζουν την ακτίνα κάλυψης σε μια κυψέλη, ακτίνας περίπου 5Km. (Κυψελωτή αρχιτεκτονική).

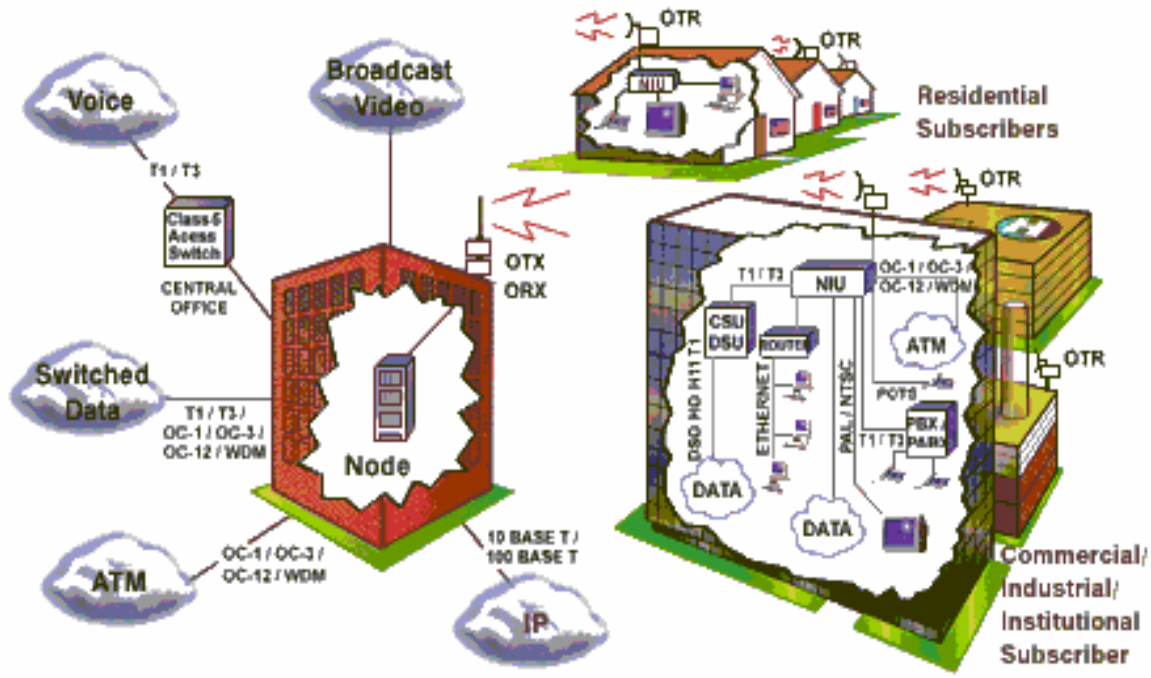
Multipoint: Δείχνει ότι τα σήματα διαβιβάζονται με μια point-to-multipoint (ένα προς πολλά), Broadcast μέθοδο. Το ασύρματο μονοπάτι της επιστροφής από τον απλό χρήστη (συνδρομητή) στον κεντρικό σταθμό είναι μια point-to-point εκπομπή.

Distribution: Αναφέρεται στη διανομή του σήματος, το οποίο μπορεί να αποτελείται από ταυτόχρονη εκπομπή φωνής, δεδομένων, Internet, video κλπ.

Service: Υπονοεί τη φύση της σχέσης μεταξύ διακομιστή και πελάτη (Server-Client), που είναι εξολοκλήρου εξαρτώμενες από την επιλογή του διακομιστή.

Η κυψελωτή αρχιτεκτονική είναι απαραίτητη για την ευρύτερη κάλυψη μιας περιοχής, π.χ. μιας πόλης, από τη στιγμή από τη στιγμή που για την ασύρματη επικοινωνία αυτού του είδους απαιτείται οπτική επαφή πομπού-δέκτη, εν αντιθέσει άλλων ασυρμάτων δικτύων χαμηλότερων συχνοτήτων, π.χ. κινητή τηλεφωνία όπου το σήμα είναι δυνατόν να διαπεράσει φυσικά εμπόδια όπως κτήρια κ.α.

Ταυτόχρονα μέσω ανακλαστήρων και επαναληπτών είναι δυνατή η επίτευξη ισχυρού-ικανού σήματος στις περιοχές των σκιών και η επίτευξη μεγαλύτερης κάλυψης.



Σχήμα 17: LMDS System

4.3.1 Αρχιτεκτονική δικτύου LMDS

Ένα LMDS σύστημα αποτελείται από:

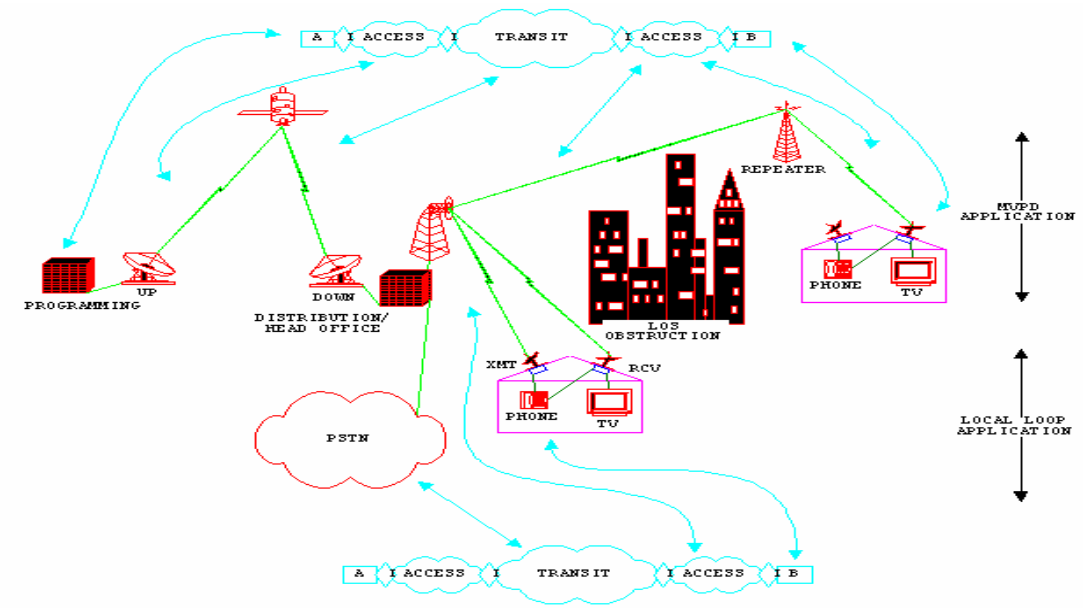
1) Υποσταθμό διανομής σήματος (κεντρικούς) ή NOC δηλ. Network Operate Center των οποίων η υποδομή και η λειτουργία μπορεί να βασίζεται στη λήψη των διαφόρων υπηρεσιών που πρέπει να διανεμηθούν στην κυψέλη, από ένα σύστημα οπτικών ινών Sonet τύπου ή δορυφορική τροφοδοσία.
2) Ένα δικτυακό κέντρο το οποίο θα επεξεργάζεται τα δεδομένα και θα χειρίζεται το πρωτόκολλο επικοινωνίας τις τεχνικές ασύρματης πρόσβασης όπως για παράδειγμα τεχνικές CDMA-FHSS-TSSS για τον έλεγχο ροής δεδομένων και την ασφάλεια της επικοινωνίας.
3) Τον εξοπλισμό των πομποδεκτών (κεραία) του σταθμού τοποθετημένο στο κατάλληλο σημείο ώστε να εξασφαλίζει καλύτερη οπτική επικοινωνία στους δέκτες
4) και φυσικά τον εξοπλισμό των πελατών-συνδρομητών, Receiver-Decoder-Modulator- up και down Converter-Antenna.

4.3.2 Οφέλη:

Χαμηλό κόστος: δεδομένου ότι ένα μέρος του δικτυακού εξοπλισμού π.χ εξοπλισμός χρηστών (πελατών) δεν υφίσταται έως ότου ενεργοποιηθούν οι συνδρομές τους.

Εύκολη χωροθετική και γρήγορη υλοποίηση: εφ' όσον αποφεύγονται οι εγκαταστάσεις καλωδιώσεων, που είναι η πιο δύσκολη υλοποιήσιμη διαδικασία.

Ευκολία και ταχύτητα επέκτασης και αποφυγή πολλών περιορισμών στην επεκτασιμότητα του δικτύου. Οικονομική συντήρηση και λειτουργικό κόστος.



Σχήμα 18: LMDS System

4.3.3 Παράδειγμα χρήσης LMDS

Χρησιμοποιώντας μόνο το εύρος ζώνης των 850MHz ενός LMDS συστήματος, μαζί με ένα σχέδιο διαμόρφωσης όπως η χρησιμοποίηση οριζόντιων και κάθετων πολωμένων τομέων, θα μπορούσε να συμπεριληφθεί σε αυτό ο αριθμός των 100T1 γραμμών (1,544Mbps)

Μια χαρακτηριστική εμπορική χρήση των LMDS μπορεί να παρέχει μια σύνδεση που να λαμβάνει δεδομένα με ταχύτητα 51,84-155,52 Mbps και μια σύνδεση επιστροφής T1 (1,544 Mbps).

Αυτή η δυναμική παρέχει τη δυνατότητα να παρασχεθεί η συσκευασία υπηρεσιών:

- πλήρης δικτυακή υπηρεσία
- Internet, με πολύ μεγάλη ταχύτητα πρόσβασης
- υπηρεσίες Video- φωνής (πραγματικού χρόνου)
- DAVIC Digital Audio-Video-Council

1GHz του φάσματος LMDS μπορεί να παρέχει έως 288 κανάλια ψηφιακής ποιοτικής τηλεόρασης

Παρέχει δυνατότητα για:

- πλήρη δικτυακή υπηρεσία
- ψηφιακή τηλεόραση-ραδιόφωνο
- DAVIC (τηλεσυνδιάσκεψη)
- Εργασία στο σπίτι
- Τηλεϊατρική

4.4 MMDS

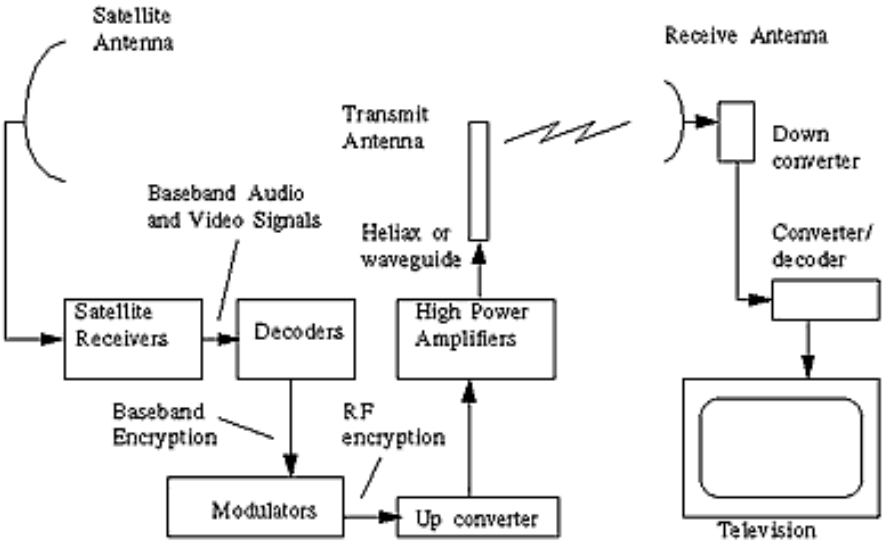
Το Multichannel Multipoin Distribution Service (MMDS), αναφερόμενο επίσης ως *microwave multipoint distribution service,* αντιπροσωπεύει μια ασύρματη ευρυζωνική τεχνολογία. Το MMDS λειτουργεί στα 2.5- 2.7 GHz frequency spectrum,

χαμηλότερα από τα 28-31 GHz που χρησιμοποιεί το LMDS. Μπορεί να υποστηρίξει ρυθμό δεδομένων εως και 10Mbps.

Στις Η.Π.Α ο FCC έχει σχεδιάσει 100 MHz από το παρακείμενο εύρος ζώνης που αρχίζει από τα 5.8 GHz στην ISM band, για ευρείας ζώνης ασύρματης πρόσβασης, χωρίς την ανάγκη χορήγησης άδειας. Επειδή δεν υπάρχει ανάγκη να χορηγηθεί άδεια, ελαχιστοποιείται ο χρόνος και το κόστος που θα απαιτούνταν για την παροχή της ευρυζωνικής πρόσβασης.

Χρησιμοποιείται για τη μετάδοση τηλεοπτικών υπηρεσιών και για τα TV σήματα με εύρος ζώνης 6MHz, μόνο 33 κανάλια μπορούν να συμπεριληφθούν σε ένα σύστημα MMDS.

Υψηλότερες περιοχές συχνότητας δεν επιλέγονται για το λόγο της εξασθένισης του σήματος από φυσικά εμπόδια (κτίρια κ.α)
Η χαρακτηριστική οργάνωση ενός συστήματος MMDS εμφανίζεται στο σχήμα.



Σχήμα 19 : Σύστημα MMDS

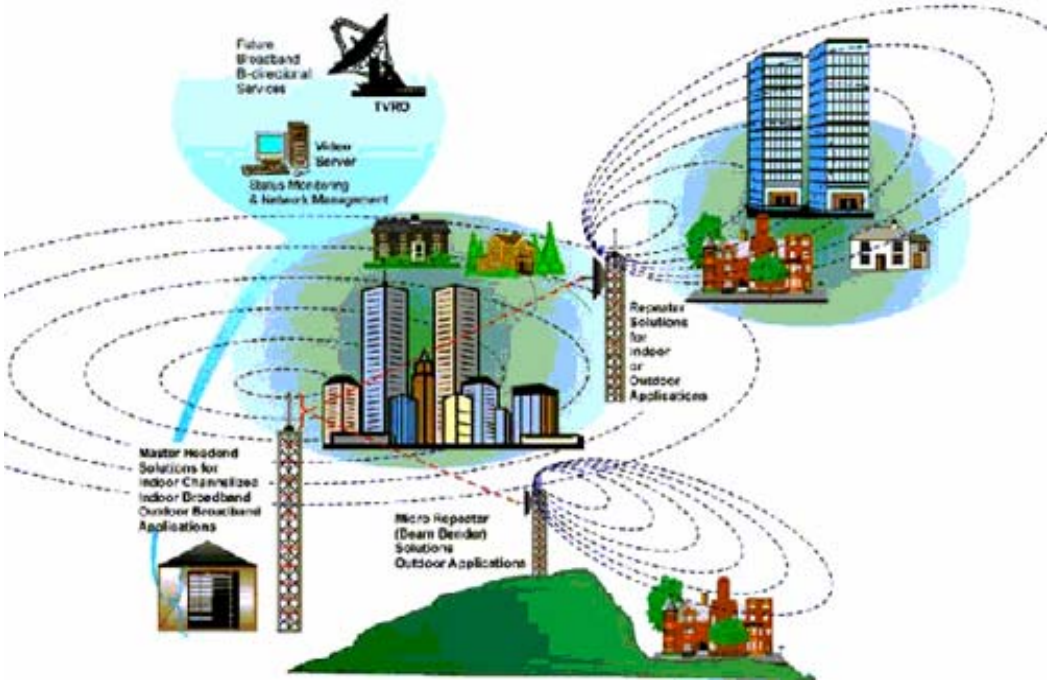
Η τυπική συνδεσμολογία ενός συστήματος MMDS αποτελείται από την συσκευή κεφαλής (συσκευή λήψης δορυφορικών σημάτων , ραδιοπομπό , άλλη συσκευή broadcast , κεραία λήψης, ενισχυτές υψηλής ισχύος) και από την συσκευή λήψης σε κάθε θέση του συνδρομητή (κεραία , διάταξη μετατροπής συχνότητας, και διάταξη set top.

Τα σήματα για εκπομπή MMDS πηγάζουν από μια ποικιλία πηγών ,όπως καλωδιακές πηγές. Τα δορυφορικά , επίγεια και καλωδιακά προγράμματα που παραδίδονται , πρόσθετα σε τοπικές υπηρεσίες ευρείας ζώνης , περιλαμβάνουν το υλικό που παραδίδεται σε άλλα MMDS .Όλες οι δορυφορικά παραδιδόμενες μορφές βασικής ζώνης επαναδιαμορφώνονται και στην συνέχεια μεταφέρονται στις μικροκυματικές συχνότητες.

Τα επίγεια παραδιδόμενα σήματα συνήθως διαβιβάζονται από ένα ετερόδυνο επεξεργαστή πριν γίνει μετατροπή στις επιθυμητές συχνότητες MMDS. Αναμεταδοτικοί σταθμοί μπορούν να χρησιμοποιηθούν για να επανακατευθύνουν τα σήματα MMDS σε άλλες περιοχές.

Η ακτίνα μιας κεραίας MMDS μπορεί να φθάσει σε 35 μίλια ενώ η ισχύς εκπομπής συνήθως είναι 1 έως 100 Watt που είναι κάτω από την ισχύ εκπομπής τηλεοπτικών σημάτων στην περιοχή VHF UHF. Η εκπομπή γίνεται με πάνελ μικρού μεγέθους (παρόμοια με αυτά της εκπομπής κινητής τηλεφωνίας) ή με κάτοπτρα

δορυφορικού τύπου αν πρόκειται για εκπομπή στενής δέσμης και μακρινής απόστασης (link), δίνοντας έτσι την δυνατότητα να προστατευθεί οπτικά το περιβάλλον παραδοσιακών οικισμών. Τα συστήματα μπορούν με την απαιτούμενη μελέτη να καλύψουν και περισσότερες από μια πόλη, χωριό ή οικισμό. Ένα από τα άλλα του πλεονεκτήματα είναι η αποφυγή της εκσκαφής των δρόμων, που απαιτείται για τα κλασσικά καλωδιακά δίκτυα, και φυσικά η πόντιση ειδικών καλωδίων και η τοποθέτηση ειδικών ενισχυτών.



Σχήμα 20: Σύστημα MMDS

Ένα σύστημα MMDS έχει κυψελωτή αρχιτεκτονική και η κάλυψη που παρέχει μια κυψέλη είναι μεγαλύτερη από αυτή της LMDS αναλόγως της ισχύος που επιλέγεται.

Μια ορθογώνια κεραία παραβολική διαμορφωμένη ρυθμίζεται για να λάβει κάθετα ή οριζόντια πολωμένα σήματα, (ή και τα δύο), στις εγκαταστάσεις κάθε τελικού χρήστη. Τα σήματα μικροκυμάτων περνούν έπειτα μέσω ενός down-converter που μετατρέπει τις συχνότητες σημάτων στο πρότυπο καλώδιο VHF ή τις UHF συχνότητες καναλιών. Τα σήματα TV μπορούν στη συνέχεια να περάσουν άμεσα σε ένα σύνολο TV ή έναν set-top converter.

ΚΕΦΑΛΑΙΟ 5°

5.1 IEEE 802.11 WLAN

Ο στόχος και οι προσπάθειες του ιδρύματος IEEE στον τομέα των ασύρματων LANs έως το 1990 όταν συστάθηκαν οι πρώτες ομάδες εργασίας ήταν η δημιουργία σφαιρικών προτύπων για ασύρματα LANs που λειτουργούν στη ζώνη συχνοτήτων των 2.4-GHz, που δεν απαιτεί αδειοδότηση για ταχύτητες μετάδοσης 1 έως 2 Gbps περίπου.

5.1.1 Αρχική προσπάθεια

Η αρχική προσπάθεια του IEEE στον τομέα ασύρματου LANs οδήγησε στις προδιαγραφές για το φυσικό στρώμα και το στρώμα ελέγχου πρόσβασης μέσων (MAC) που θα επέτρεπε στους κατασκευαστές των ασύρματων συσκευών τοπικών LAN να κατασκευάσουν τον εξοπλισμό. Στο φυσικό στρώμα, το IEEE καθόρισε τη διαμόρφωση και τα χαρακτηριστικά εκπομπής για δύο μεθόδους RF και μια **IR μέθοδο μετάδοσης** (υπέρυθρη περιοχή συχνοτήτων). Οι δύο μέθοδοι RF που υποστηρίζονται από τα πρότυπα περιλαμβάνουν την **τεχνική Frequensy Hopping Spread Spectrum (FHSS)** και τη **τεχνική Direct Sequence Spread Spectrum (DSSS)**.

Η αρχική προσπάθεια της ομάδας εργασίας του IEEE 802.11αποτελεί τώρα το πρότυπο 802,11a Standard και μπορεί να θεωρηθεί ότι αντιπροσωπεύει την πρώτη γενεά της τυποποίησης για τα ασύρματα δίκτυα LAN.

Υπό το prodject 802.11b υλοποιήθηκαν αρχικά δύο πρότυπα με ταχύτητες μετάδοσης στα 5,5 και 11 Mbps αντίστοιχα. Λόγω της ομοιότητας μεταξύ των δύο προτύπων, συνήθως αναφέρονται συλλογικά ως 802.11b πρότυπο.

Σαν αποτέλεσμα λοιπόν της υπάρχουσας ,εφαρμοσμένης τεχνολογίας καθώς και της αδιάκοπης εξέλιξής της ,οι ρυθμοί μετάδοσης που έχουν επιτευχθεί κυμαίνονται από τα 2 Mbps που υποστήριζε το αρχικό Standard του 802.11$^{\alpha}$,στα 5,5-11-22 Mbps του 802.11 b ,τα 54 Mbps του 802.11 g και αγγίζοντας τελευταία τα 108 Mbps του 802.11 Super g , υλοποιώντας βέβαια διάφορες τεχνικές διαμόρφωσης.

5.1.2 Βασική διαμόρφωση

Σύμφωνα με το 802.11, οι σταθμοί μπορούν να λειτουργήσουν με δύο διαμορφώσεις. Κατ' αρχάς, οι σταθμοί μπορούν να επικοινωνήσουν άμεσα ο ένας με τον άλλον. Ο IEEE αναφέρεται σε αυτό ως **Independent Configuration** και μπορεί να θεωρηθεί παρόμοιο με μια Point to Point επικοινωνία . Η δεύτερη μέθοδος διαμόρφωσης που υποστηρίζεται από το IEEE 802.11 πρότυπο αναφέρεται ως **Infrastructure__Configuration**. Σύμφωνα με τη μέθοδο αυτή, οι σταθμοί επικοινωνούν με ένα ή περισσότερα σημεία πρόσβασης, τα οποία συνδέονται με το ενσύρματο τοπικό δίκτυο LAN.

5.1.3 Point-to-multipoint

Το κύριο παράδειγμα point to multipoint επικοινωνίας αποτελεί η broadcast μετάδοση. Είναι ταυτόχρονη επικοινωνία περισσότερων από δύο κόμβων. Τα δίκτυα εκπομπής διαθέτουν ένα και μοναδικό κανάλι επικοινωνίας, το οποίο μοιράζονται όλοι οι κόμβοι που είναι συνδεδεμένοι στο δίκτυο. Αποτέλεσμα αυτής της σύνδεσης,

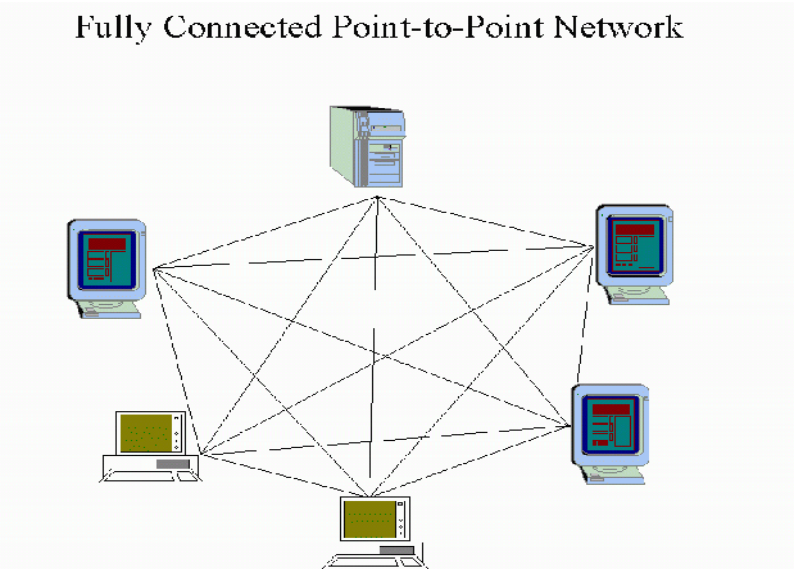
είναι ότι το κάθε μήνυμα που αποστέλλεται σε κάποιο σταθμό, παραλαμβάνεται από όλους ανεξαρτήτως τους χρήστες που βρίσκονται συνδεδεμένοι στο δίκτυο. Για το λόγο αυτό ο σύνδεσμος αυτής της μορφής, λέγεται και (point to multipoint connection) επικοινωνία ενός προς πολλούς. Το μήνυμα που στέλνεται από ένα κόμβο σε ένα άλλο, είναι εφοδιασμένο με τη διεύθυνση του παραλήπτη, και λαμβάνεται από όλους τους κόμβους που είναι συνδεδεμένοι στο δίκτυο. Όταν ένας κόμβος δεχθεί το μήνυμα, ελέγχει τη διεύθυνση του παραλήπτη. Αν η διεύθυνσή του ταυτίζεται με τη διεύθυνση του παραλήπτη, τότε παραλαμβάνει το μήνυμα, διαφορετικά το αγνοεί.

Παραδείγματα δικτύων point to multipoint εκπομπής είναι τα δίκτυα του ραδιοφώνου και της τηλεόρασης, ενώ περιοριζόμενοι στην περίπτωση των δικτύων υπολογιστών, τέτοια δίκτυα είναι για παράδειγμα αυτά που κάνουν χρήση της τεχνολογίας LMDS.

5.1.4 Point-to-point

Το βασικό χαρακτηριστικό της σύνδεσης από point to point connection είναι η σύνδεση μόνο δύο σταθμών κάθε φορά.

Πρόκειται για την απλούστερη μορφή επικοινωνίας μεταξύ δύο σταθμών, που επιτυγχάνεται με απευθείας σύνδεσή τους με κάποια γραμμή επικοινωνίας. Όταν δύο κόμβοι δεν επικοινωνούν με απευθείας σύνδεση, έχουν τη δυνατότητα να επικοινωνήσουν μέσω κάποιων άλλων κόμβων, με αποτέλεσμα η επικοινωνία να γίνεται τμηματικά. Φυσικά δεν είναι απαραίτητο η επικοινωνία δύο κόμβων να γίνεται πάντα μέσω των ίδιων γραμμών μετάδοσης, αφού είναι δυνατόν να αλλάξει η διαδρομή για διάφορους λόγους. Στο πλαίσιο αυτό, έχουν αναπτυχθεί ειδικές τεχνικές για τον έλεγχο και τον καθορισμό της δρομολόγησης των δεδομένων από τον αποστολέα στον παραλήπτη. Γνωστά δίκτυα με συνδέσεις από σημείο σε σημείο, είναι τα δίκτυα δεδομένων ευρείας περιοχής, το διαδίκτυο (peer to peer), καθώς και άλλα τηλεπικοινωνιακά δίκτυα, όπως για παράδειγμα το τηλεφωνικό δίκτυο κλπ. Από τις γνωστές τοπολογίες δικτύων που έχουν μελετηθεί, η τοπολογία αστέρα και η τοπολογία δέντρου, είναι παραδείγματα τοπολογιών που λειτουργούν με σύνδεση point to point.



Σχήμα 21: Δίκτυο Point-to-point

Στις περιπτώσεις κατά τις οποίες τα ασύρματα τοπικά δίκτυα χρησιμοποιούν συνδέσεις από σημείο σε σημείο, η επικοινωνία πραγματοποιείται είτε μεταξύ δύο σταθερών σημείων, είτε μεταξύ δύο σημείων, από τα οποία το ένα ή και τα δύο, βρίσκονται σε κίνηση. Επικοινωνίες αυτής της μορφής, αφορούν κυρίως τα ραδιοκύματα ή τα μικροκύματα τα οποία χρησιμοποιούνται ευρύτατα στην επικοινωνία μεγάλων αποστάσεων. Νεότερες εφαρμογές στηρίζονται τόσο στα επίγεια συστήματα οπτικών κυμάτων (laser) με οπτική επαφή, όσο και στα επίγεια συστήματα μικροκυμάτων.

Μικροκύματα χρησιμοποιούνται και σε ορισμένες εφαρμογές της ασύρματης δικτύωσης μικρής εμβέλειας, όπως είναι το άνοιγμα θυρίδων ή θυρών ασφαλείας, τα συστήματα ασφαλείας, τα συστήματα ενεργοποίησης ηλεκτρονικών συσκευών, οι βομβητές, κλπ.

5.1.5 Επιλογή συχνότητας

Το 802.11 αναπτύχθηκε βασισμένο να ικανοποιεί μια σειρά απαιτήσεων . Μια απαίτηση ήταν να αναπτυχθεί ένας έλεγχος πρόσβασης στο μέσο μετάδοσης (MAC) και ένα φυσικό στρώμα (PHY), κατάλληλα για την υλοποίηση ασύρματης ζεύξης για φορητούς , σταθερούς , και μετακινούμενους σταθμούς εργασίας μέσα σε μια τοπική περιοχή. Μια δεύτερη απαίτηση ήταν να παρασχεθεί η ασύρματη σύνδεση σε αυτοματοποιημένους σταθμούς και μηχανήματα (συσκευές), ή τους σταθμούς που απαιτούν 'ειδικά' γρήγορη επίτευξη ζεύξης –επικοινωνίας. Μια τρίτη απαίτηση που έπαιξε πρωταρχικό ρόλο στην επιλογή της συχνότητας των 2.4 GHz , ήταν η ανάγκη να καθιερωθούν πρότυπα που θα μπορούσαν να χρησιμοποιηθούν σε σφαιρική βάση (παγκόσμια κλίμακα) .

Η χρήση της ζώνης 2.4-GHz αντιπροσωπεύει μια ζώνη συχνότητας (**ISM**) που δεν απαιτεί αδειοδότηση και διατηρείται για τη βιομηχανική, επιστημονική, και ιατρική χρήση σε παγκόσμια κλίμακα, με κάποια διαφοροποίηση όσον αφορά στα επιτρεπόμενα επίπεδα ισχύος στις διάφορες χώρες. Στην πραγματικότητα, για ακριβώς τον ίδιο λόγο, το δίκτυο HomeRF χρησιμοποιεί επίσης τη ζώνη συχνότητας των 2.4-GHz.

5.1.6 Περιβάλλον

Αν και κάποιος φαντάζεται το ασύρματο τοπικό LAN σαν μια τεχνολογία επικοινωνίας για χρήση περιορισμένη μέσα σε ένα κτήριο, το 802.11 δεν είναι περιορισμένο σε εφαρμογές εσωτερικού μόνο χώρου. Εκτός από την πιθανή χρήση του σε καταστήματα, νοσοκομεία, τα κτίρια γραφείων-επιχειρήσεων, και οι κατοικίες, μπορεί επίσης να χρησιμοποιηθεί σε υπαίθριες περιοχές όπως τα μέρη χώρων στάθμευσης και τις πανεπιστημιουπόλεις, αεροδρόμια και να επεκταθεί καλύπτοντας την έκταση ολόκληρων πόλεων.

Για να γίνει εφικτή ευρύτερη κάλυψη μεγάλων περιοχών και επικοινωνία σταθμών η και τοπικών δικτύων σε μεγάλες αποστάσεις υιοθετήθηκε ένα μοντέλο που αποτελείται από δύο διαφορετικές περιοχές υπηρεσιών (service area). Μια βασική περιοχή υπηρεσιών **Basic Service Area (BSA)** και μια εκτεταμένη περιοχή υπηρεσιών **Extended Service Area**. **(ESA).**

Η βασική περιοχή υπηρεσιών αντιπροσωπεύει μια περιοχή στην οποία κάθε σταθμός μπορεί να επικοινωνήσει με οποιοδήποτε άλλο σταθμό σε εκείνη την περιοχή, σε σύγκριση με την εκτεταμένη περιοχή υπηρεσιών που αντιπροσωπεύει μια

περιοχή υπηρεσιών στην οποία κάθε σταθμός μπορεί να επικοινωνήσει με οποιοδήποτε άλλο σταθμό μέσω μιας συσκευής επέκτασης της περιοχής κάλυψης που η λειτουργία της μπορεί να παρομοιαστεί μ'αυτή ενός επαναλήπτη (repeater).

5.1.7 Αναγνώριση κίνησης από το 802.11

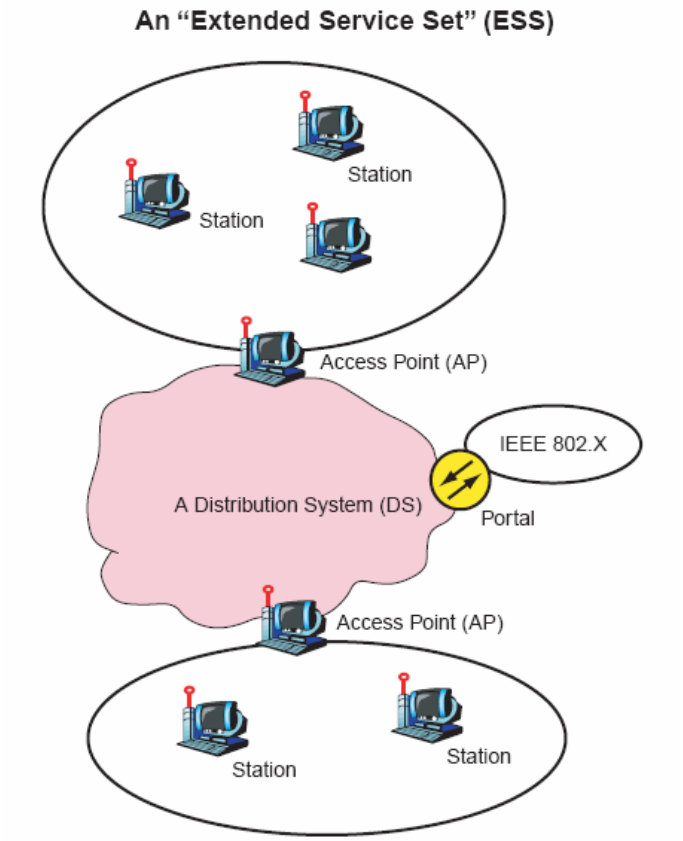
Το 802.11 αναγνωρίζει τους παρακάτω τύπους κίνησης:

Απουσία μετακίνησης: Ο τύπος αυτός αναφέρεται σε σταθμούς που δεν μετακινούνται και σε αυτούς που μετακινούνται μέσα σε ένα τοπικό BSS.

BSS μετακίνηση: Ο τύπος αυτός αναφέρεται σε σταθμούς που μετακινούνται από ένα BSS σε ένα άλλο BSS μέσα στο ίδιο ESS.

ESS μετακίνηση: Αυτός ο τύπος μετακίνησης αναφέρεται σε σταθμούς που μετακινούνται από ένα BSS σε ένα άλλο BSS το οποίο ανήκει σε διαφορετικό ESS.

Αξίζει να αναφέρουμε ότι το 802.11 ενώ υποστηρίζει ξεκάθαρα τους δύο πρώτους τύπους μετακίνησης, δεν εγγυάται την διατήρηση της σύνδεσης κατά την μετακίνηση σε διαφορετικό ESS.



Σχήμα 23 : Extended Service Set

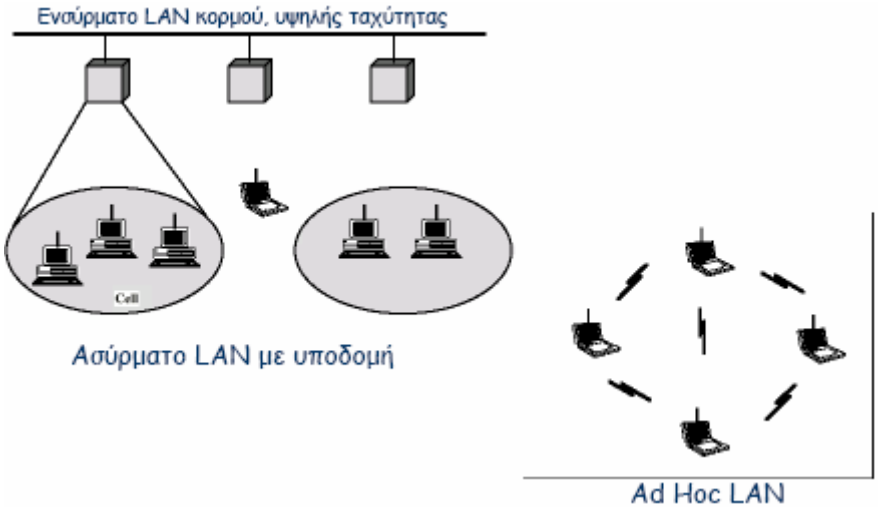
5.2 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ IEEE 802.11

5.2.1 Δικτύωση ειδικού σκοπού (ad-hoc networking)

Μία χρήση των ασύρματων δικτύων είναι εκείνη της δικτύωσης ειδικού σκοπού ή αλλιώς της Ad-Hoc Networking. Στην περίπτωση αυτή δεν υπάρχει κάποιος κεντρικός υπολογιστής που να διαχειρίζεται το δίκτυο, αλλά απλά οι υπολογιστές είναι συνδεδεμένοι ο ένας με τον άλλο. Δίκτυα τέτοιου είδους συνήθως

εγκαθίστανται προσωρινά και έχουν ως σκοπό την εξυπηρέτηση μιας άμεσης ανάγκης. Για παράδειγμα, μπορούμε να σκεφτούμε την περίπτωση όπου μια ομάδα υπαλλήλων συνδέουν τους φορητούς υπολογιστές τους, ώστε να εξυπηρετηθούν οι ανάγκες μιας on-line σύσκεψης ή παρουσίασης, όπου σε έναν υπολογιστή θα γίνεται η παρουσίαση και οι υπόλοιποι θα μπορούν να την παρακολουθούν από τους προσωπικούς τους υπολογιστές.

Στο παρακάτω σχήμα απεικονίζονται ένα ασύρματο δίκτυο ειδικού σκοπού (Ad Hoc Wireless LAN) και ένα ασύρματο δίκτυο το οποίο υποστηρίζει LAN extension και νομαδική πρόσβαση.

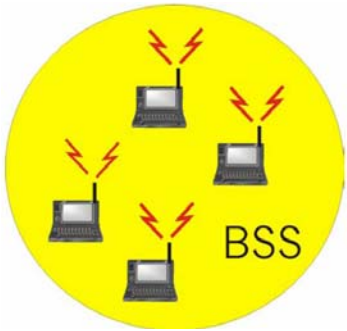


Σχήμα 22: α) Ασύρματο δίκτυο το οποίο υποστηρίζει LAN extension και νομαδική πρόσβαση. β)Ad Hoc Wireless LAN

5.2.2 Κυψελωτή Αρχιτεκτονική

Η αρχιτεκτονική στην οποία βασίστηκε το IEEE 802.11 LAN μοιάζει με την αρχιτεκτονική της κυψελωτής τηλεφωνίας , παρόλο που εντοπίζονται κάποιες, διαφορές.

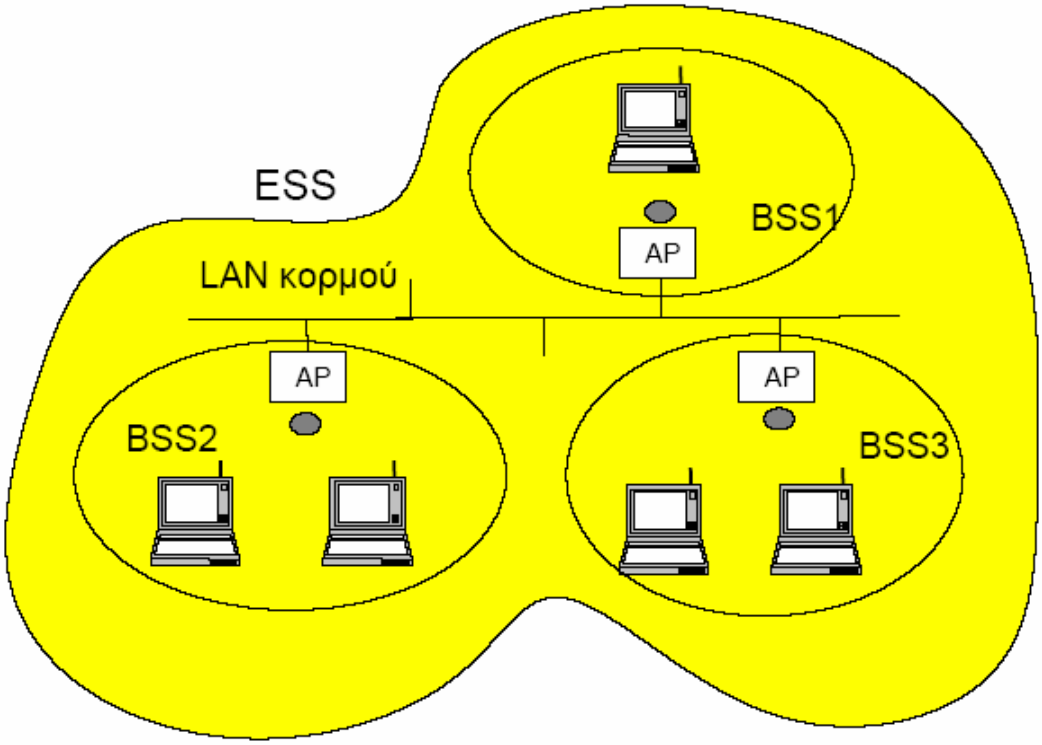
Cells and Sets: Το 802.11 ασύρματο LAN υποδιαιρείται σε κυψέλες, με κάθε κυψέλη αναφερόμενη, σύμφωνα με την ονοματολογία του 802.11, ως Βασική Μονάδα Υπηρεσιών Basic Service Set (BSS).



Σχήμα 24: Κυψέλη ασύρματου LAN (BSS)

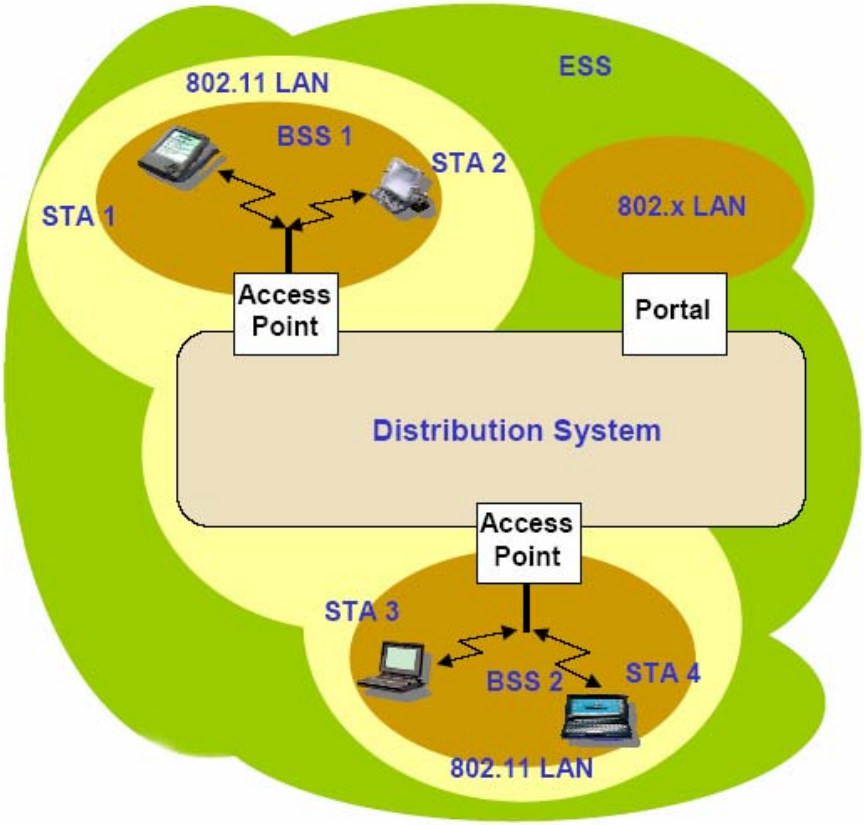
Κάθε **BSS** ελέγχεται από έναν Βασικό Σταθμό ο οποίος ονομάζεται **Access Point (AP)** (Σημείο-Σταθμός Πρόσβασης). Επειδή η εμβέλεια εκπομπής ενός ενιαίου AP μπορεί να είναι ανεπαρκής να καλύψει τις απαιτήσεις δικτύωσης μιας οργάνωσης, διάφορα APs μπορούν να συνδεθούν μεταξύ τους σε ένα κοινό **Backbone**. Όταν το WLAN υλοποιείται με αυτή τη μορφή, η τυποποιημένη ορολογία του 802.11 το καταγράφει σαν **Distribution System (DS).**

Ανεξάρτητα από το αν, το ασύρματο τοπικό LAN, αποτελείται ένα ή περισσότερα **BSS**, τα **APs** τους, και το **DS** τους, στα ανώτερα στρώματα του προτύπου αναφοράς, αντιμετωπίζονται σαν ένα ενιαίο IEEE 802 δίκτυο. Στην τυποποιημένη ορολογία του 802.11, στα ανώτερα στρώματα του προτύπου αναφοράς **OSI** στο σύνολό της αυτή η δομή αναφέρεται ως **Εκτεταμένη Μονάδα Υπηρεσιών Extended Service Set (ESS).**



Σχήμα 25 : Εκτεταμένη Μονάδα Υπηρεσιών Extended Service Set (ESS)

Τα δεδομένα μετακινούνται μεταξύ ενός BSS και του **DS** μόνο μέσω του **AP**, ενώ το **DS** υποστηρίζει τους τύπους κίνησης του 802.11 παρέχοντας υπηρεσίες ικανές να ελέγχουν την αντιστοίχηση (mapping) της διεύθυνσης στον προορισμό για κάθε σταθμό που μετακινείται.



Σχήμα 26: ESS (Distribution System που ενσωματώνει δυο BSS)

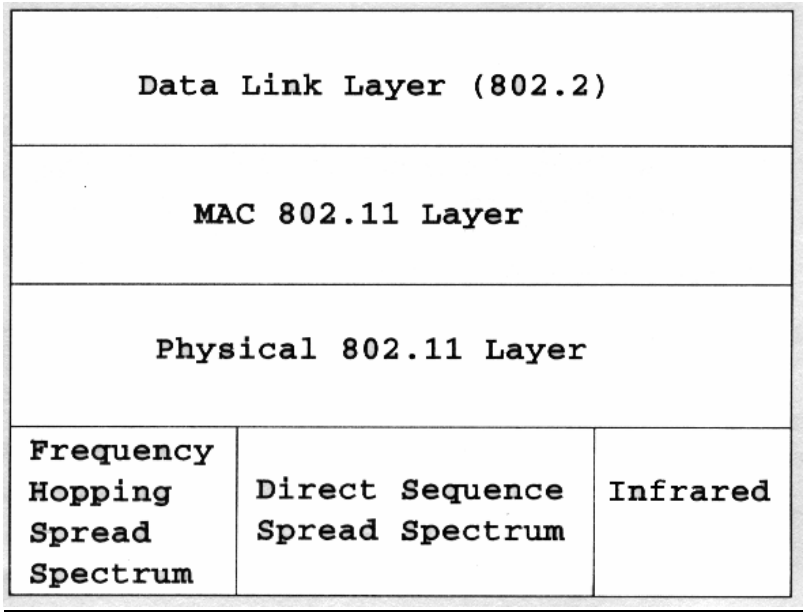
Η κεντρική ιδέα της συγκεκριμένης τοπολογίας, είναι ότι ένα δίκτυο **ESS** εμφανίζεται το ίδιο σε ένα επίπεδο **LLC** όπως και ένα δίκτυο **BSS**. Οι σταθμοί μέσα στο ίδιο **ESS** μπορούν να μετακινούνται από ένα **BSS** σε ένα άλλο διαφανώς ως προς το **LLC**.

PORTALS: ένα ακόμα σημαντικό δομικό στοιχείο ενός IEEE 802.11 LAN αποτελούν οι λεγόμενες πύλες. Η πύλη μπορεί να θεωρηθεί ότι αντιπροσωπεύει μια γέφυρα επειδή παρέχει την ικανότητα διασύνδεσης μεταξύ ενός τοπικού 802.11 και ενός άλλου τοπικού 802.11 WLAN ή ακόμη με άλλα δίκτυα που δεν ανήκουν στη οικογένεια 802.11. Η πύλη είναι το λογικό σημείο μέσω του οποίου τα MSDUs από ένα τοπικό δίκτυο διαφορετικό του 802.11 εισέρχονται στο DS του 802.11. Το Standard του 802.11 δεν περιορίζει τη σύνθεση του DS. Για τον λόγο αυτό μπορεί να είναι συμβατό με άλλα δίκτυα που είτε ανήκουν είτε όχι στην οικογένεια 802. π.χ. Για την ενοποίηση της αρχιτεκτονικής του 802.11 με ένα παραδοσιακό ενσύρματο τοπικό δίκτυο χρησιμοποιείται μια πύλη (portal). Οι περισσότεροι κατασκευαστές υλοποιούν τα PORTALS και τα APs ως ενιαία φυσική οντότητα ενσωματώνοντας τα σε μια κοινή συσκευή. Πιο συγκεκριμένα τα AP που κυκλοφορούν σαν πιο κοινές συσκευές ασύρματης δικτύωσης 802.11 b-g-super g ενσωματώνουν τις λειτουργικές υπηρεσίες των portals.

5.3 ΦΥΣΙΚΟ ΣΤΡΩΜΑ 802.11

Το πρωτόκολλο 802.11 καλύπτει το φυσικό και το MAC στρώμα. Όπως αναφέρθηκε εν συντομία νωρίτερα, αντί ενός φυσικού στρώματος, το πρότυπο 802.11 υποστηρίζει τρία. Αυτά περιλαμβάνουν το φυσικό στρώμα που υλοποιεί την τεχνολογία Frequency Hopping Spread Spectrum, αυτό που υλοποιεί την Direct Sequence Spread Spectrum ,και εκείνο που κάνει χρήση της τεχνολογίας του φάσματος των υπερύθρων (Infrared).

Η λειτουργία και των δύο μεθόδων RF (FHSS-DSSS) περιορίζεται στη ζώνη συχνοτήτων των 2.4GHz και χαρακτηριστικά καταλαμβάνει 83MHz του εύρους ζώνης από τα 2.400 έως τα 2.483 GHz.Τα χαρακτηριστικά αυτά της ζώνης των μικροκυμάτων , ενώ πιστοποιούνται και υιοθετούνται σε πάνω από 40 χώρες , μπορεί να διαφοροποιούνται ως προς τα επιτρεπόμενα επίπεδα ισχύος εκπομπής .



Σχήμα 27: Επίπεδα 802.11

Παραδείγματος χάριν, η επιτροπή Federal Communications Commission (FCC) στις ΗΠΑ έχει θεσπίσει ανώτερο περιοριστικό όριο εκπεμπόμενης ισχύος ,το 1 Watt, στην Ευρώπη επιτρέπονται 10 mW ανά 1 MHz, ενώ στην Ιαπωνία, περιορίζεται σε 10mW.Επιπλέον, υπάρχουν διαφορές στην κατανομή ορισμένων συχνοτήτων για το φυσικό στρώμα RF, μεταξύ χωρών που για παράδειγμα προ-καταλαμβάνουν συχνότητες του φάσματος του 802.11 που χρησιμοποιούνται από ομότιμο εξοπλισμό κρατικών υπηρεσιών ή μεγάλων πολυεθνικών εταιριών.

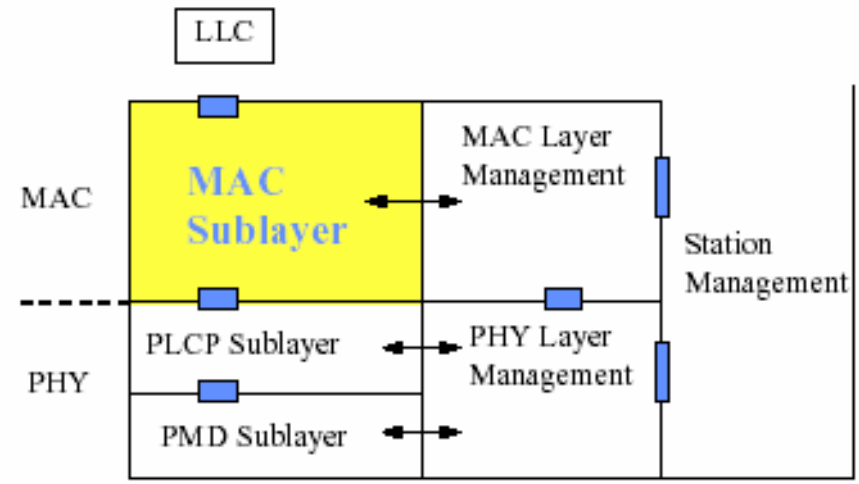
5.3.1 Η αρχιτεκτονική του φυσικού στρώματος

Η αρχιτεκτονική του φυσικού στρώματος αποτελείται από τα τρία επόμενα στοιχεία (components) για κάθε σταθμό:

- **PLM** (Physical Layer Management): Η συνιστώσα αυτή λειτουργεί σε συνεργασία με το υπόστρωμα διαχείρισης MAC και εκτελεί λειτουργίες διαχείρισης για το φυσικό στρώμα.

- **PLCP** (Physical Layer Convergence Procedure) υπόστρωμα: Το υπόστρωμα MAC επικοινωνεί με το PLCP μέσω στοιχείων υπηρεσίας (service primitives) με τη βοήθεια των SAPs (Service Access Points) του φυσικού στρώματος. Όταν το υπόστρωμα MAC δώσει εντολή, το PLCP ετοιμάζει τα **MPDUs** για μετάδοση. Το PLCP προσαρτίζει πεδία (PREAMBLE-HEADER κλπ) στο MPDU που περιέχουν πληροφορίες που χρειάζονται οι πομποί και οι δέκτες του φυσικού στρώματος. Το 802.11 αναφέρεται σε αυτό το σύνθετο πλαίσιο ως PPDU (PLCP Protocol Data Unit). Η δομή του **PPDU** πλαισίου παρέχεται για ασύγχρονη μεταφορά των MPDUs μεταξύ των σταθμών.
- **PMD** (Physical Medium Dependent) υπόστρωμα: Κάτω από την καθοδήγηση του PLCP, το PMD παρέχει την ουσιαστική μετάδοση και λήψη των οντοτήτων του φυσικού στρώματος μέσω του ασύρματου μέσου. Για την παροχή αυτής της υπηρεσίας, το PMD διασυνδέεται άμεσα με το ασύρματο μέσο (δηλαδή τον αέρα) και παρέχει διαμόρφωση και αποδιαμόρφωση των πλαισίων που μεταδίδονται. Τα PLCP και PMD επικοινωνούν μέσω των 'primitives' για τον έλεγχο των λειτουργιών μετάδοσης και λήψης.

Η συσχέτιση των παραπάνω στοιχείων τόσο μεταξύ τους όσο και με το υποστρώμα MAC απεικονίζεται στο επόμενο σχήμα.



Σχήμα 28: Η αρχιτεκτονική του υποστρώματος MAC και του φυσικού στρώματος όπως αυτή καθορίζεται από το 802.11.

5.3.2 Λειτουργίες του φυσικού στρώματος (Physical Layer Operations)

Για την εκτέλεση των λειτουργιών του υποστρώματος PLCP, το 802.11 καθορίζει την χρήση των μηχανών κατάστασης (state machines). Κάθε μηχανή κατάστασης εκτελεί μία από τις παρακάτω λειτουργίες:

α) Ανίχνευση φέροντος: Η λειτουργία αυτή αφορά τον καθορισμό της κατάστασης του μέσου

β) Μετάδοση: Η λειτουργία αυτή αναφέρεται στην αποστολή των διαδοχικών bytes ενός πλαισίου δεδομένων.

γ) Λήψη: Η λειτουργία αυτή αναφέρεται στην λήψη διαδοχικών bytes ενός πλαισίου δεδομένων.

Παρακάτω αναφέρονται εκτενέστερα αυτές οι λειτουργίες.

5.3.2α Ανίχνευση φέροντος

Το φυσικό επίπεδο υλοποιεί την λειτουργία της ανίχνευσης φέροντος (**carrier sense**) κατευθύνοντας το PMD να ελέγξει αν το μέσο είναι απασχολημένο ή ελεύθερο. Το PLCP εκτελεί τις παρακάτω λειτουργίες όταν ο σταθμός δεν βρίσκεται σε διαδικασία μετάδοσης ή λήψης ενός πλαισίου:

- Ανίχνευση των εισερχόμενων σημάτων: Το PLCP μέσα στον σταθμό θα ανιχνεύει διαρκώς το μέσο. Όταν το μέσο γίνει απασχολημένο, το PLCP θα διαβάσει τα πεδία 'preamble' και 'header' του πλαισίου PLCP και θα επιχειρήσει συγχρονισμό του δέκτη στον ρυθμό μετάδοσης του σήματος.
- Καθορισμός ελεύθερου καναλιού (CCA: Clear Channel Assessment): Με τη λειτουργία αυτή καθορίζεται αν το μέσο είναι απασχολημένο ή όχι. Ο πιο συνηθισμένος τρόπος λειτουργίας του CCA είναι η μέτρηση, από το PMD, της ενέργειας στο μέσο. Ο καθορισμός του μέσου προκύπτει ανάλογα με το αν η μετρούμενη τιμή ξεπερνάει ένα συγκεκριμένο όριο, το οποίο αναφέρεται ως κατώφλι ανίχνευσης ενέργειας (ED: Energy Detection).

5.3.2β Λειτουργία μετάδοσης

Το PLCP θα αλλάξει το PMD σε κατάσταση μετάδοσης μετά την λήψη του κατάλληλου 'service primitive' (PHY-TXSTART.request) από το επίπεδο MAC. Το επίπεδο MAC στέλνει τον αριθμό των bytes (0-4095) και τις οδηγίες για τον ρυθμό μετάδοσης μαζί με την παραπάνω αίτηση (request). Το PMD ανταποκρίνεται στέλνοντας το 'preamble' του πλαισίου στην κεραία μέσα σε 20 μs.

Ο πομπός στέλνει τα 'preamble' και 'header' με ρυθμό 1 Mbps. Αφού σταλεί το 'preamble' ο πομπός αλλάζει τον ρυθμό μετάδοσης σε αυτόν που καθορίζεται από το 'header'. Μετά την ολοκλήρωση της μετάδοσης, το PLCP στέλνει το κατάλληλο 'primitive' στο επίπεδο MAC, κλείνει τον πομπό και αλλάζει το κυκλωματικό (circuitry) του PMD σε κατάσταση λήψης.

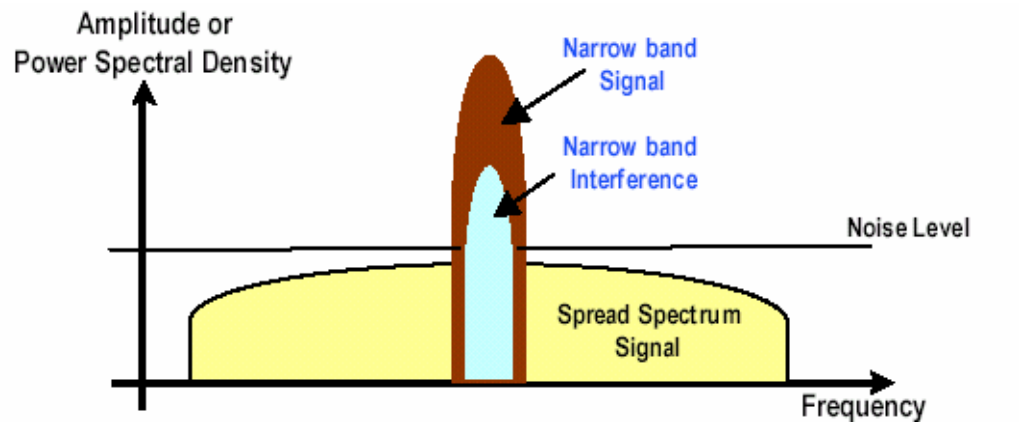
5.3.2γ Λειτουργία λήψης

Αν ο καθορισμός του ελεύθερου καναλιού (CCA) ανακαλύψει ότι το μέσο είναι απασχολημένο και ανιχνεύσει ένα έγκυρο 'preamble' ενός εισερχόμενου πλαισίου τότε το PLCP θα ελέγξει την επικεφαλίδα (header) του πλαισίου. Το PMD θα υποδείξει ότι το μέσο είναι απασχολημένο όταν ανιχνεύσει ένα σήμα με ισχύ μεγαλύτερη από 85 dBm. Αν το PLCP καθορίσει ότι η επικεφαλίδα είναι χωρίς λάθη θα στείλει το κατάλληλο 'primitive' (PHY-RXSTART.indicate) στο επίπεδο MAC για να ειδοποιήσει για την επικείμενη λήψη ενός πλαισίου. Μαζί με αυτήν την ειδοποίηση το PLCP στέλνει τις πληροφορίες που βρίσκει στην επικεφαλίδα του πλαισίου (όπως ο αριθμός των bytes και ο ρυθμός μετάδοσης).

Το PLCP θέτει σε λειτουργία έναν μετρητή byte βασιζόμενο στην τιμή του πεδίου 'PSDU Length Word' που βρίσκεται στην επικεφαλίδα. Με την βοήθεια του μετρητή αυτού, το PLCP γνωρίζει πότε λαμβάνει χώρα το τέλος του πλαισίου. Καθώς το PLCP λαμβάνει τα δεδομένα, στέλνει τα bytes του PSDU στο επίπεδο MAC με τα κατάλληλα primitives.

5.4 ΤΟ ΦΥΣΙΚΟ ΣΤΡΩΜΑ ΤΟΥ 802.11 ΜΕ ΧΡΗΣΗ ΤΗΣ ΤΕΧΝΙΚΗΣ SPREAD SPECTRUM

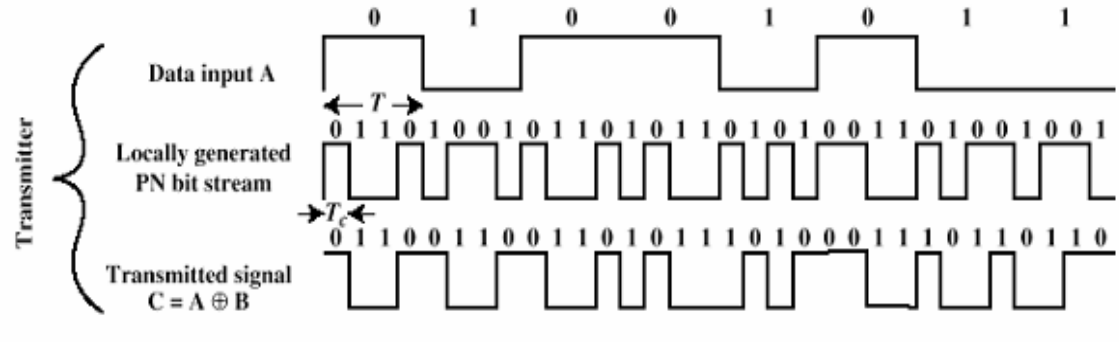
Το 802.11 καθορίζει δύο διαφορετικά φυσικά στρώματα τα οποία στηρίζονται στην τεχνική διαμόρφωσης που καλείται 'εξάπλωση φάσματος' (**SS**: **Spread Spectrum**). Η τεχνική αυτή 'εξαπλώνει' την ισχύ του σήματος σε μια ευρεία μπάντα συχνοτήτων, της φαίνεται στο σχήμα .Η διαδικασία αυτή κάνει το σήμα λιγότερο ευάλωτο στον θόρυβο και της παρεμβολές από της μεταδόσεις οι οποίες χρησιμοποιούν συνήθως ένα μικρό εύρος συχνοτήτων. Έτσι, η πιθανή προκύπτουσα παρεμβολή με το εξαπλωμένο σήμα θα οδηγεί σε λιγότερα λάθη κατά την αποδιαμόρφωση του σήματος από τον δέκτη.



Σχήμα 29: Τεχνική Spread Spectrum

5.4.1 Εξάπλωση σήματος, στην περιοχή των συχνοτήτων με χρήση της τεχνικής spread spectrum.

Η Spread Spectrum τεχνική έγκειται στο να "πολλαπλασιάζουμε" το σήμα εισόδου A με ένα σήμα B με περίοδο Tc << T. Το σήμα B έχει επομένως πολύ μεγαλύτερο εύρος φάσματος από το A, και το προκύπτον σήμα από τον πολλαπλασιασμό των A και B, το οποίο θα μεταδοθεί τελικά πάνω από το κανάλι έχει επίσης ευρύ, επίπεδο φάσμα. Το σήμα B είναι ένα ψευδοτυχαίο σήμα, το οποίο εκτός από τον αποστολέα πρέπει να γνωρίζει και ο δέκτης για να επανακτήσει το αρχικό σήμα.

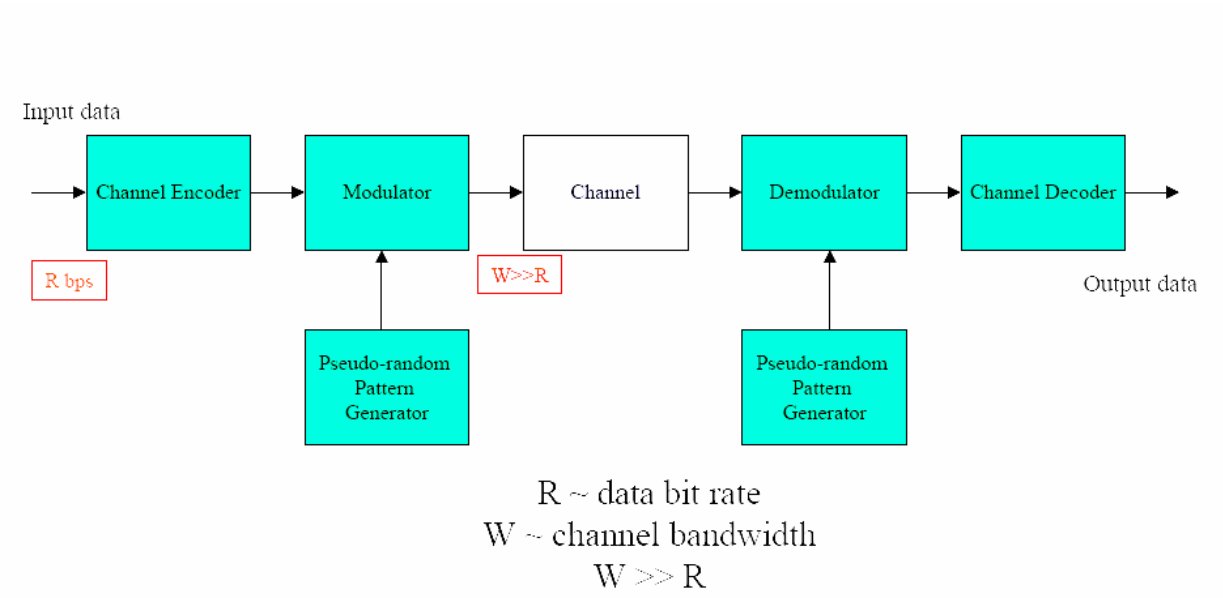


Σχήμα 30: Εξάπλωση σήματος, στην περιοχή των συχνοτήτων με χρήση της τεχνικής spread spectrum.

Η τεχνική αυτή χρησιμοποιήθηκε αρχικά για στρατιωτικούς σκοπούς, όπου η ασφάλεια των επικοινωνιών είναι πολύ σημαντική. Το σήμα που μεταδίδεται τελικά πάνω στο κανάλι (το οποίο μπορεί να ακούσει ο οποιοσδήποτε αν το κανάλι είναι π.χ. ο αέρας) είναι πολύ δύσκολο να υποκλαπεί, γιατί:

1. για την αποκωδικοποίηση και επανάκτηση του αρχικού σήματος πρέπει να αντιληφθεί αρχικά ο υποκλοπέας ότι γίνεται μετάδοση (γιατί λόγω του ευρέως φάσματος μετάδοσης η ισχύς σε κάθε συχνότητα είναι χαμηλή κι άρα εύκολα μπορεί ο υποκλοπέας να το θεωρήσει απλώς θόρυβο)
2. πρέπει επίσης ο υποκλοπέας να γνωρίζει το ψευδοτυχαίο σήμα B.

Το σήμα δύσκολα μπορεί επίσης να υποστεί παρεμβολές (jamming), γιατί λόγω του ευρέως φάσματος η παρεμβολή θα απαιτούσε πομπό εξαιρετικά υψηλής ισχύος ώστε να δημιουργήσει παρεμβολές σε όλες τις συχνότητες.



Σχήμα 31: Μοντέλο ενός συστήματος Spread Spectrum

5.4.2 Το υπόστρωμα PMD FHSS

Το υπόστρωμα PMD (Physical Medium Dependent) εκτελεί την πραγματική μετάδοση και λήψη των PPDUs υπό την καθοδήγηση του PLCP. Για να εκτελέσει αυτήν την λειτουργία το FHSS PMD συνδέεται απευθείας με το ασύρματο μέσο και παρέχει την διαμόρφωση και αποδιαμόρφωση των πλαισίων που μεταδίδονται μέσω της τεχνικής FHSS.

Το PMD μεταφράζει την δυαδική αναπαράσταση των PPDUs σε ένα ραδιοσήμα ικανό για μετάδοση. Το FHSS PMD εκτελεί αυτές τις λειτουργίες μέσω της λειτουργίας μεταπήδησης συχνότητας (frequency hopping) και της τεχνικής διαμόρφωσης που ονομάζεται **FSK** (Frequency Shift Keying). Η επόμενη παράγραφος εξηγεί το FHSS PMD.

5.5 FREQUENCY –HOPPING SPREAD SPECTRUM (τεχνική διαμόρφωσης με μεταπήδηση συχνοτήτων)

Σύμφωνα με το πρότυπο **802.11** οι επικοινωνίες που κάνουν χρήση της τεχνικής διαμόρφωσης FHSS αντιπροσωπεύουν ένα από τα τρία φυσικά στρώματα

που υποστηρίζονται από το standard . Το IEEE 802.11 FHSS φυσικό στρώμα χρησιμοποιεί 79 nonoverlapping (μη επικαλυπτόμενα) κανάλια συχνότητας, με κάθε κανάλι να χρησιμοποιεί (καλύπτει) το φάσμα του ενός 1- MHz. Αυτό επιτρέπει μέχρι 26 colocated networks (παράλληλα δίκτυα) να λειτουργήσουν, γεγονός το οποίο μπορεί να παρέχει εύλογα υψηλό throughput..

5.5.1 Κατανομή συχνότητας του 802.11

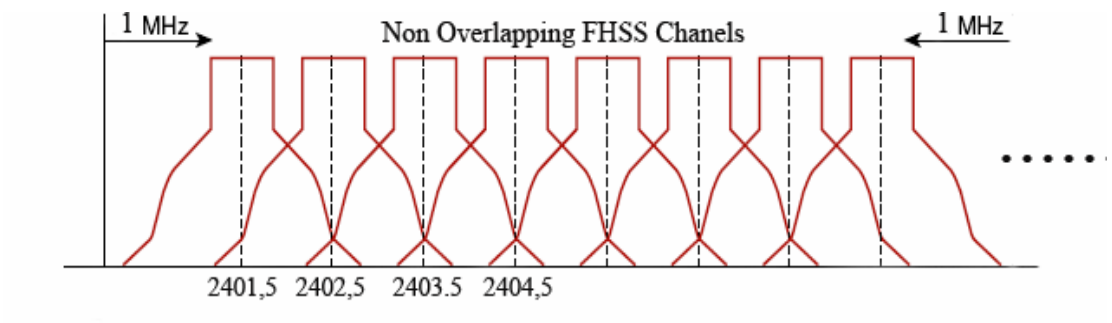
Αν και το πρότυπο 802.11 οριοθετεί τη χρήση 79 nonoverlapping (μη επικαλυπτόμενων) καναλιών συχνότητας, ο πραγματικός αριθμός καναλιών το ύψος της συχνότητάς τους και το ύψος της ισχύος εκπομπής τους ,καθορίζεται από την αρμόδια ρυθμιστική αρχή ανάθεσης της χρήσης συχνοτήτων κάθε χώρας.

Στον επόμενο πίνακα (31) παρουσιάζονται οι κατανομές συχνοτήτων ,ο αριθμός των επιτρεπόμενων καναλιών και των επιτρεπόμενων επιπέδων της ισχύος τους καθώς και του μεγίστου επιτρεπόμενου επίπεδου εκπομπής συνολικής ισχύος.

Geographic Area	Frequency Band (MHz)	Hopping Channels	Maximum Transmit Power
North America	2400–2483.5	At lease 75; 79 used	1 W
Europe	2400–2483.5	At least 20; 79 used	100 mW
Japan	2471–2497	At least 10; 23 used	10 mW/MHz

Πίνακας 32: Κατανομή συχνοτήτων και επιτρεπόμενα επίπεδα ισχύος

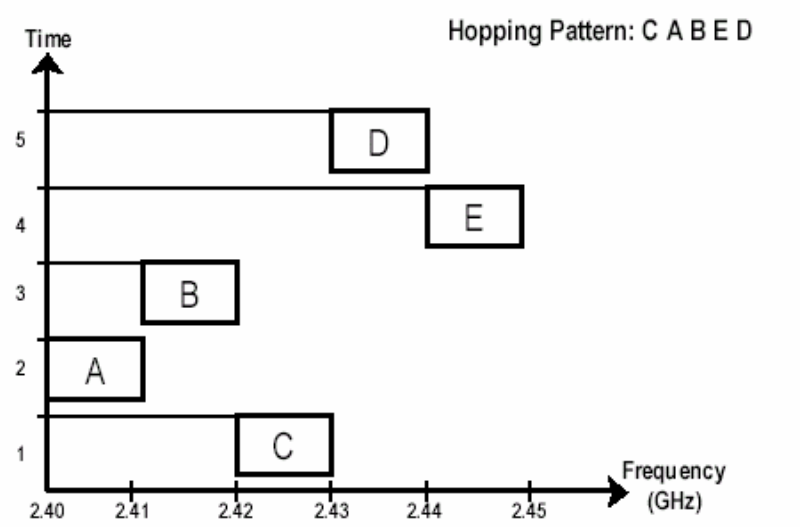
Το 802.11 καθορίζει έναν αριθμό καναλιών (79 για την Β. Αμερική και για τις περισσότερες χώρες της Ευρώπης) που ισοκατανέμονται στην μπάντα ISM στην συχνότητα των 2.4 GHz. Κάθε κανάλι έχει εύρος 1 MHz, κατά συνέπεια η κεντρική συχνότητα λειτουργίας (όσον αφορά τις ΗΠΑ) για το πρώτο κανάλι είναι τα 2.402 GHz, για το δεύτερο τα 2.403 GHz κ.ο.κ.



Σχήμα 33: Κατανομή των Καναλιών FHSS στο φάσμα συχνοτήτων.

Το PMD που στηρίζεται στο FHSS μεταδίδει τα δεδομένα μεταπηδώντας από κανάλι σε κανάλι σύμφωνα με μια συγκεκριμένη ψευδο-τυχαία ακολουθία μεταπήδησης (hopping pattern) η οποία κατανέμει ομοιόμορφα το σήμα κατά μήκος της μπάντας συχνοτήτων. Από την στιγμή που η ακολουθία μεταπήδησης τεθεί σε ένα

AP, οι σταθμοί αυτόματα συγχρονίζονται στην σωστή ακολουθία. Το 802.11 Standard καθορίζει έναν συγκεκριμένο αριθμό ακολουθιών, ώστε να αποφεύγεται η παρατεταμένη παρεμβολή μεταξύ των ακολουθιών αυτών. Μια τέτοια ακολουθία φαίνεται στο επόμενο σχήμα.



Σχήμα 34: Ακολουθία μεταπήδησης συχνότητας σε συνάρτηση με το χρόνο

Για κάθε βήμα μεταπήδησης (hop) στην ακολουθία μεταπήδησης ο πομπός μεταδίδει σε μια συγκεκριμένη κεντρική συχνότητα λειτουργίας για ένα συγκεκριμένο χρονικό διάστημα το οποίο καλείται 'dwell time'. Ο ρυθμός μεταπήδησης (hop rate) είναι ρυθμιζόμενος, παρ' όλα αυτά υπάρχει ένας ελάχιστος ρυθμός που καθορίζεται από τους αρμόδιους οργανισμούς κάθε χώρας (π.χ. στις Ηνωμένες Πολιτείες ο ελάχιστος ρυθμός είναι 2.5 hops/sec ο οποίος αντιστοιχεί σε ένα μέγιστο 'dwell time' ίσο με 400 ms). Επιπρόσθετα, η ελάχιστη απόσταση μεταπήδησης (hop distance) στην συχνότητα είναι 6 MHz για την Β. Αμερική και για το μεγαλύτερο μέρος της Ευρώπης και 5 MHZ για την Ιαπωνία.

Εάν ο αριθμός των χρησιμοποιούμενων συχνοτήτων μεταπήδησης είναι 79, ένας ψευδοτυχαίος αριθμός από 0 έως 78 χρησιμοποιείται για να επιλέξει την επόμενη συχνότητα μεταπήδησης .Αυτός ο τυχαίος αριθμός προκύπτει από έναν αλγόριθμο-(γεννήτρια) ψευδοτυχαίων αριθμών. Ο αριθμός αυτός μεταπήδησης εκπέμπεται μέσα στο κάθε frame έτσι ώστε οι δέκτες να γνωρίζουν την επόμενη συχνότητα μεταπήδησης για την συνέχεια λήψης των τεμαχισμένων δεδομένων.

5.5.2 Η λειτουργία διαμόρφωσης συχνότητας FHSS

Η διαμόρφωση σύμφωνα με το IEEE 802.11 Frequency Shift (FSK) standard, χρησιμοποιείται για FHSS, λόγω του χαμηλού κόστους του εξοπλισμού και της σχετικά απλής του λειτουργίας . Δύο εκδόσεις FSK είναι γνωστές, από τις οποίες χαρακτηριστικότερη είναι η *gaussian-shaped FSK* (GFSK).

Η ιδέα του GFSK είναι να μεταβάλει τη συχνότητα του φέροντος ώστε να αναπαριστά διαφορετικά δυαδικά σύμβολα.

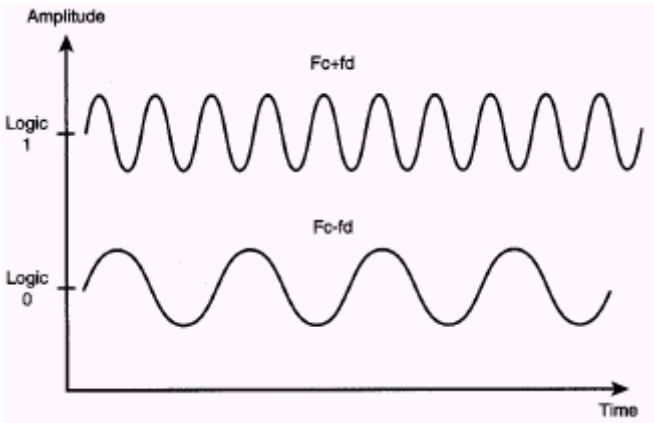
Η είσοδος στον GFSK διαμορφωτή είναι 0 ή 1 όπως αυτά προέρχονται από το PLCP. Ο διαμορφωτής μεταδίδει τα δυαδικά δεδομένα μεταβάλλοντας τη συχνότητα μετάδοσης λίγο πάνω ή λίγο κάτω από την κεντρική συχνότητα λειτουργίας (Fc) για

κάθε βήμα μεταπήδησης. Για να εκτελεστεί αυτήν την λειτουργία, χρησιμοποιούνται οι παρακάτω κανόνες:

- Συχνότητα μετάδοσης: Fc + fd, για την μετάδοση του bit 1
- Συχνότητα μετάδοσης: Fc – fd, για την μετάδοση του bit 0

Στις παραπάνω εξισώσεις, Fc είναι η κεντρική συχνότητα λειτουργίας (operating center frequency) για το συγκεκριμένο hop και fd είναι το μέγεθος της απόκλισης στη συχνότητα. Το 802.11 Standard εξηγεί τον τρόπο με τον οποίο υπολογίζονται οι ακριβείς τιμές για το fd, ενώ η ονομαστική τιμή είναι 160 KHz.

Στο επόμενο σχήμα φαίνεται η αντιστοίχηση των διαφορετικών συχνοτήτων μετάδοσης στα λογικά 1 και 0.



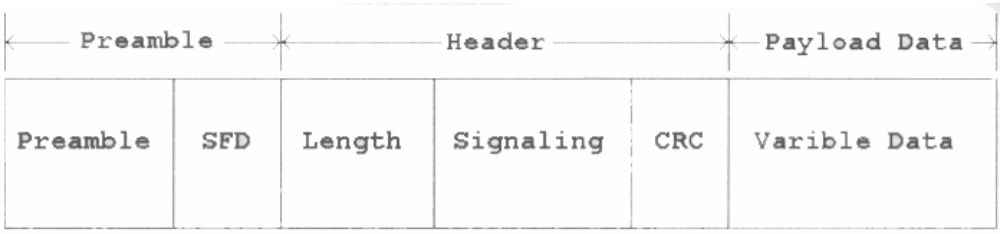
Σχήμα 35: Η διαμόρφωση GFSK χρησιμοποιεί 2 δυνατές συχνότητες για κάθε hop ώστε να δηλώνει αν ένα bit δεδομένων είναι 1 ή 0.

FRAME FORMAT: Στο φυσικό στρώμα, FHSS διαβιβάζει τα δεδομένα χρησιμοποιώντας ένα προκαθορισμένο frame format. Το σχήμα επεξηγεί το τυπικό FHSS 802.11 Frame Format , που αποτελείται από τρία διακριτά μέρη. Preamble (πρόλογος), Header (επικεφαλίδα) και Payload Data (Variable Data).

Το **Preamble** αποτελείται από μια ακολουθία 80 bit και χρησιμοποιείται για την ανίχνευση ενός σήματος ,to resolve antenna diversity.Η SFD περιέχει τέσσερα ευδιάκριτα τετράμπιτα paterns που επιτρέπουν στα αποτελέσματα όλων των πιθανών διαμορφώσεων GFSK να πιστοποιηθούν.

Η **FHSS Frame Header** αποτελείται από τρεις τομείς .Length Field, Signaling Field και Cyclic Redundancy Check -κυκλικός έλεγχος πλεονασμού - (CRC), με συνολικό μήκος 32 bits.

Τέλος το τμήμα των **Payload Data** (ωφέλιμα δεδομένα) έχει μέγιστο μήκος 4095 bytes.



Σχήμα 36: Frame Format

Μερικά από τα **πλεονεκτήματα** που προσφέρει η τεχνολογία FHSS είναι:

1. Ένας υποψήφιος υποκλοπέας πρέπει να γνωρίζει τη σειρά εναλλαγής των συχνοτήτων.
2. Οι παρεμβολές (jamming) είναι δύσκολες γιατί πρέπει να δημιουργηθούν παρεμβολές σε όλο το φάσμα των χρησιμοποιούμενων συχνοτήτων και άρα χρειάζεται πολύ μεγάλη ισχύς. Αν η παρεμβολή γίνει σε περιορισμένες μόνο συχνότητες θα δημιουργηθούν λίγα μόνο λάθη τα οποία θα είναι δυνατόν να ανιχνευτούν με κάποιο μηχανισμό ανίχνευσης / διόρθωσης λαθών.
3. Μπορούν να υποστηριχτούν πολλοί χρήστες, ο καθένας με διαφορετική σειρά εναλλαγής συχνοτήτων.

Μειονέκτημα:

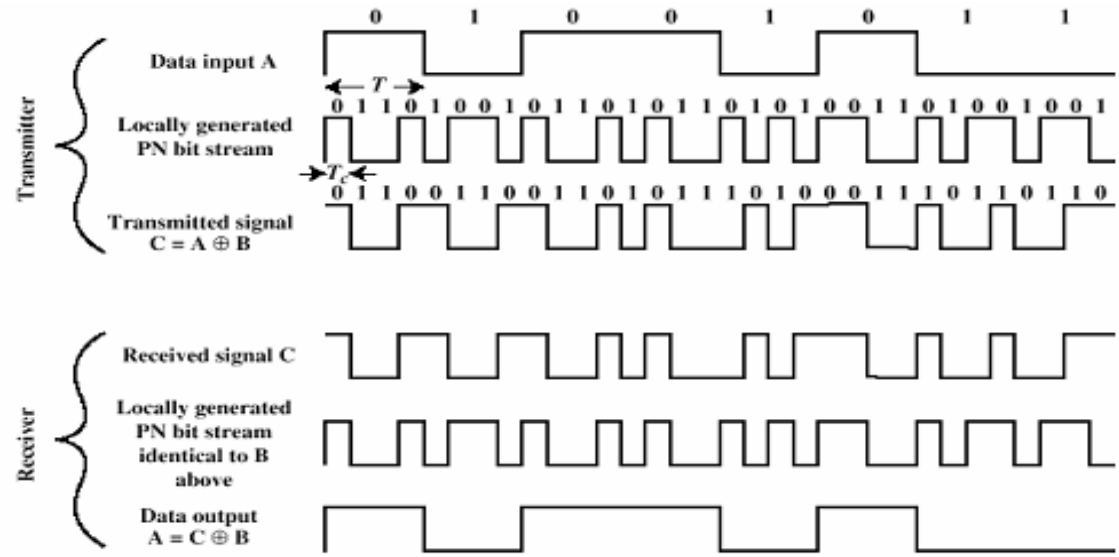
Χρησιμοποιείται k φορές μεγαλύτερο εύρος φάσματος συχνοτήτων (όπου k ο αριθμός των εναλλασσόμενων συχνοτήτων). Το μειονέκτημα αυτό ουσιαστικά αναιρείται εφόσον μπορούν να εξυπηρετηθούν k χρήστες στο ίδιο εύρος φάσματος.

Αν 2 διαφορετικοί χρήστες συμπέσουν τυχαία σε κάποια συχνότητα ο καθένας αντιλαμβάνεται τη μετάδοση του άλλου σαν jamming(παρεμβολή) και άρα όπως και το jamming μπορεί να διορθωθεί στον αποδέκτη με μηχανισμούς διόρθωσης λαθών.

5.6 DIRECT SEQUENCE SPREAD SPECTRUM (DSSS)

Αν θεωρήσουμε ότι τα bits μεταδίδονται ως 0 και 1, το προκύπτον σήμα που θα μεταδοθεί πάνω από το κανάλι προκύπτει ως το **αποκλειστικό OR (XOR)** του αρχικού σήματος A και της ψευδοτυχαίας ακολουθίας από 0 και 1, B. Δηλαδή **C=A⊕B**.

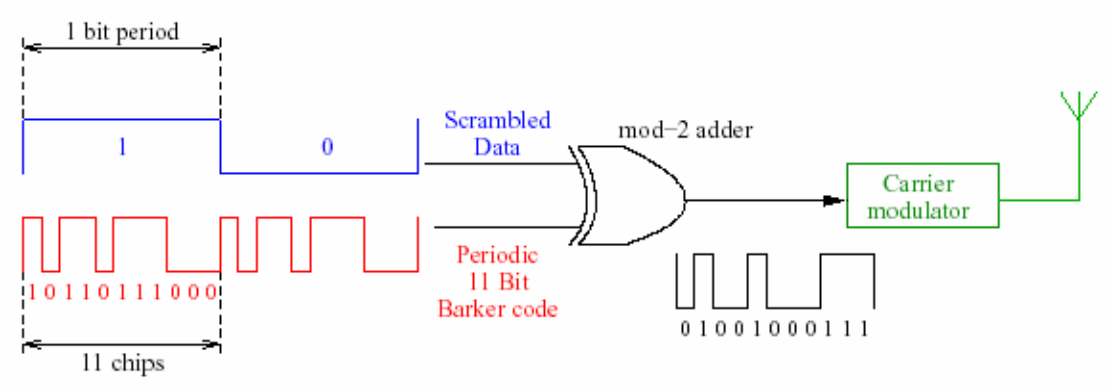
Η ανάκτηση του αρχικού σήματος A στον δέκτη θα γίνει υπολογίζοντας το XOR των C και B, δηλαδή A=C⊕B. Ο δέκτης είναι λοιπόν απαραίτητο να γνωρίζει την ψευδοτυχαία ακολουθία B για να ανακτήσει το αρχικό σήμα A. Αυτή η διαδικασία περιγράφεται στο παρακάτω σχήμα..



Σχήμα 37: Διαμόρφωση και αποδιαμόρφωση με τεχνική DSSS

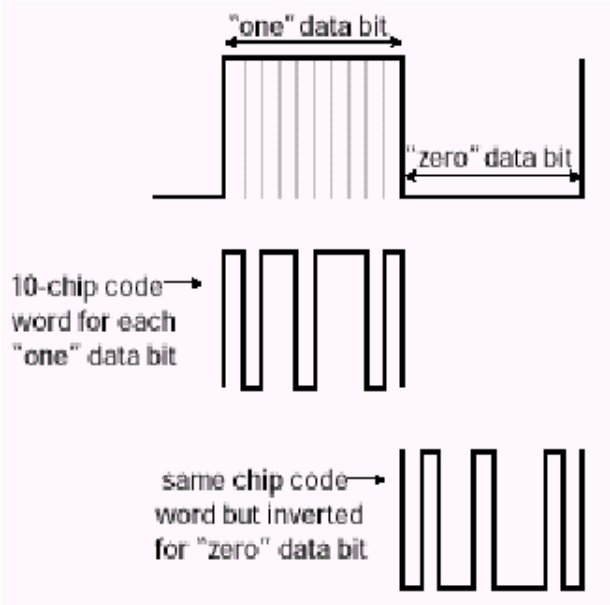
Η περίοδος Tc του ψευδοτυχαίου σήματος B ονομάζεται και **chip** και είναι γενικά T=k*Tc, όπου T η περίοδος του αρχικού σήματος A και το k είναι μία μεγάλη τιμή, π.χ. 128. Το k=128 θα σήμαινε ότι θα υπήρχαν 2^{128} δυνατές ακολουθίες που θα μπορούσαν να χρησιμοποιηθούν σαν B. Αν ο δέκτης χρησιμοποιήσει κάποια άλλη ακολουθία και όχι τη B για την αποκωδικοποίηση, το σήμα που θα παράγει θα έχει πάλι ευρύ φάσμα και δεν θα αντιστοιχεί στο αρχικό A.

Η κεντρική ιδέα της τεχνικής DSSS είναι, αρχικά, να εξαπλωθεί ψηφιακά το μη διαμορφωμένο PPDU της βασικής ζώνης (baseband) πράγμα που σημαίνει ότι γίνεται εφαρμογή της τεχνολογίας Spread Spectrum και έπειτα να διαμορφωθούν τα εξαπλωμένα δεδομένα σε μια συγκεκριμένη συχνότητα. Το σχήμα δείχνει τα στοιχεία που αποτελούν έναν DSSS πομπό.



Σχήμα 38: Σχηματική αναπαράσταση ενός DSSS πομπού.

Ο πομπός εξαπλώνει το PPDU συνδυάζοντας το PPDU ('Scrambled Data) με έναν Pseudo-Noise (PN) κώδικα (ο οποίος συχνά αναφέρεται ως **chip code** ή spreading sequence, ενώ στο σχήμα αναφέρεται ως 'Periodic 11 Bit Barker code') με την βοήθεια ενός modulo-2 αθροιστή (mod-2 adder). Η PN ακολουθία (PN sequence) αποτελείται από μία ακολουθία θετικών και αρνητικών '1'. Μία τέτοια ακολουθία δίνεται στο επόμενο σχήμα.



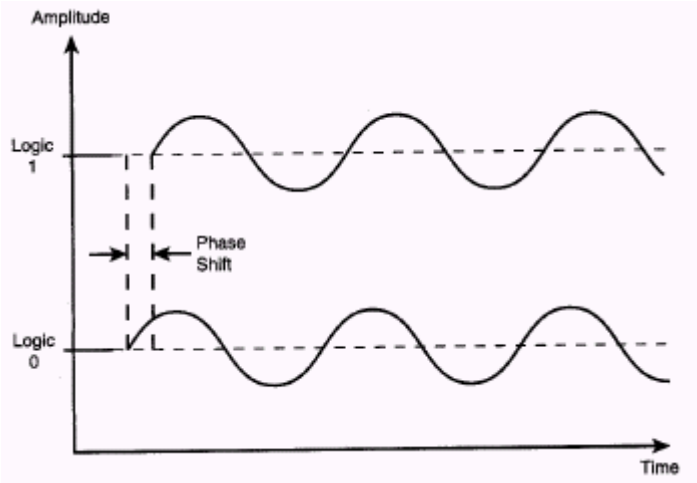
Σχήμα 39: Αναπαράσταση ενός bit από μια ακολουθία θετικών και αρνητικών μονάδων (1)

Ο κώδικας που χρησιμοποιείται στο 802.11 DSSS αναφέρεται στη βιβλιογραφία ως **11-chip Barker sequence** και δίνεται παρακάτω, με το bit που βρίσκεται πιο αριστερά να εφαρμόζεται πρώτο στο PPDU.

+1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1

Η έξοδος του mod-2 αθροιστή είναι ένα DSSS σήμα με υψηλότερο ρυθμό σηματοδοσίας από αυτόν του αρχικού σήματος. Ένα PPDU με ρυθμό 1 Mbps στην είσοδο θα καταλήξει σε ένα εξαπλωμένο σήμα με ρυθμό 11 Mbps στην έξοδο του αθροιστή. Στη συνέχεια, ο διαμορφωτής ('Carrier modulator') μεταφράζει το σήμα της βασικής ζώνης σε ένα αναλογικό σήμα στην συχνότητα λειτουργίας της μετάδοσης του επιλεγμένου καναλιού. Αν και η 'spreading sequence' είναι η ίδια για όλους τους χρήστες, υπάρχει η ελευθερία επιλογής οποιουδήποτε καναλιού συχνότητας, ώστε να υποστηρίζεται η ταυτόχρονη μετάδοση.

Το επόμενο σχήμα δείχνει πως ο διαμορφωτής μεταδίδει τα δεδομένα μεταβάλλοντας τη φάση του φέροντος.



Σχήμα 40: Μετάδοση δεδομένων με χρήση της τεχνικής DBPSK.

Πλεονεκτήματα της μεθόδου:

1. Παρέχει ασφάλεια (δεν υποκλέπτεται εύκολα), επειδή απαιτείται γνώση της ψευδοτυχαίας ακολουθίας που χρησιμοποίησε ο πομπός.
2. Για να υποστεί παρεμβολές (jamming) χρειάζεται πομπό μεγάλης ισχύος, εφόσον αυτός που θέλει να δημιουργήσει την παρεμβολή πρέπει να παρεμβληθεί σε όλες τις συχνότητες του ευρέως φάσματος.
3. Το εύρος φάσματος τελικά δεν καταναλώνεται άσκοπα σε σχέση με τεχνικές στενού φάσματος (όπως π.χ. FDMA), γιατί το ίδιο εύρος φάσματος μπορεί να χρησιμοποιηθεί από περισσότερους του ενός χρήστες. Κάθε χρήστης χρησιμοποιεί διαφορετική ψευδοτυχαία ακολουθία, και άρα ένας δέκτης μπορεί να ανακτήσει το σήμα που τον ενδιαφέρει "πολλαπλασιάζοντας" το σήμα που μεταδίδει το κανάλι με την κατάλληλη ακολουθία. Στο παραγόμενο σήμα θα ξεχωρίσει το σήμα που τον ενδιαφέρει και τα υπόλοιπα σήματα θα μοιάζουν με χαμηλής ισχύος θόρυβο.

Μειονεκτήματα:

1. Εφόσον έχουμε ρυθμό μετάδοσης k φορές μεγαλύτερο, τα ηλεκτρονικά συστήματα πρέπει να δουλεύουν k φορές πιο γρήγορα, άρα θα είναι πιο ακριβά και δύσκολα να κατασκευαστούν. Τα τελευταία βέβαια χρόνια με την

πρόοδο στην τεχνολογία των ηλεκτρονικών το πρόβλημα αυτό έχει σε μεγάλο βαθμό ξεπεραστεί.

5.6.1 DSSS με χρήση BPSK διαμόρφωσης

Το σήμα που προκύπτει από τον "πολλαπλασιασμό" του αρχικού σήματος με την ψευδοτυχαία ακολουθία προτού μεταδοθεί πάνω από το κανάλι μπορεί να διαμορφωθεί με BPSK, ή με κάποιο άλλο είδος διαμόρφωσης. Στην περίπτωση που χρησιμοποιείται BPSK το σήμα που μεταδίδεται είναι το

$$s(t) = A\, d(t)\, c(t) \cos(2\pi f_c t)$$

όπου A είναι το πλάτος του σήματος,
f_c η κεντρική συχνότητα του φάσματος
d(t) η διακριτή συνάρτηση [-1,1]
και το c(t) παίρνει τις τιμές {-1, 1} ανάλογα με το μεταδιδόμενο bit.
Ο αποδέκτης αρκεί να πολλαπλασιάσει το σήμα που λαμβάνει με c(t) για να ανακτήσει το αρχικό σήμα.

5.6.2 Υποστήριξη πολλών χρηστών

Στην περίπτωση που έχουμε στο ίδιο κανάλι N χρήστες, πρέπει να διαλέξουμε N ψευδοτυχαίες ακολουθίες που θα χρησιμοποιηθούν, από ένα σύνολο 2^{128} αν $T=128T_c$ (γενικά 2^k).Επιθυμητό είναι οι ακολουθίες που θα επιλεχτούν να είναι όσο το δυνατόν λιγότερο correlated (συσχετισμένες), ει δυνατόν να είναι ορθογώνιες, ώστε κάθε χρήστης να αποκωδικοποιεί μόνο το δικό του σήμα.
Γενικά σε ένα ασύρματο περιβάλλον εκτός από το κυρίως σήμα ο αποδέκτης λαμβάνει και ανακλάσεις του σήματος που διανύουν διαφορετικές αποστάσεις και φτάνουν με χρονική διαφορά από το κυρίως σήμα. Επομένως ο δέκτης λαμβάνει πολύ περισσότερα από N σήματα. Οι ψευδοτυχαίες ακολουθίες πρέπει να είναι ορθογώνιες όχι μόνο μεταξύ τους, αλλά η κάθε μία πρέπει να είναι επίσης ορθογώνια σε σχέση με τις χρονικές μετατοπίσεις του εαυτού της και τις χρονικές μετατοπίσεις των υπολοίπων ακολουθιών.

5.6.3 Οι βελτιώσεις στο φυσικό επίπεδο που εισάγει το πρότυπο 802.11b

Η πιο σημαντική συνεισφορά του 802.11b στα ασύρματα δίκτυα ήταν η τυποποίηση την υποστήριξη δύο νέων ταχυτήτων 5,5Mbps - 11Mbps σε φυσικό επίπεδο. Για να το επιτύχει αυτό, έπρεπε να επιλεγεί η τεχνική DSSS ως η μόνη που θα χρησιμοποιούνταν στο πρότυπο, εφόσον το hopping -όπως σημειώθηκε παραπάνω-δεν μπορεί να υποστηρίξει μεγαλύτερες ταχύτητες χωρίς να παραβιάζει τους κανονισμού της FCC. Έτσι τα 802.11b συστήματα μπορούν να συλλειτουργούν με αυτά που λειτουργούν σε 1 και 2 Mbps χρησιμοποιώντας την DSSS τεχνική, αλλά όχι με τα αντίστοιχα που χρησιμοποιούν FHSS.

Για να υποστηριχθούν περιβάλλοντα με πολύ θόρυβο ή που καταλαμβάνουν μεγάλη έκταση, το 802.11b WLAN χρησιμοποιεί δυναμική μετατόπιση του ρυθμού μετάδοσης, επιτρέποντας οι ρυθμοί μετάδοσης δεδομένων να προσαρμόζονται αυτόματα για να ανταποκριθούν στις αλλαγές του ραδιοκαναλιού. Ιδανικά οι χρήστες συνδέονται στα 11Mbps, όμως όταν οι συσκευές μετακινούνται πέρα από την βέλτιστη απόσταση για λειτουργία στα 11Mbps, (ή υπάρχουν μη αμελητέες

παρεμβολές) τότε οι συσκευές θα μεταδίδουν στα 5,5 ή ακόμη και στο 1 Mbps. Όμοια, αν η συσκευή μετακινηθεί πάλι μέσα στην ακτίνα για μετάδοση σε υψηλότερη μετάδοση η σύνδεση θα επιταχυνθεί ξανά. Αυτός ο μηχανισμός ανήκει στο φυσικό επίπεδο και είναι διαφανείς προς το χρήστη και την στοίβα των πρωτοκόλλων ανώτερων επιπέδων.

Χρησιμοποιώντας την τεχνική του hopping συχνότητας, η ζώνη των 2,4GHz διαιρείται σε υποκανάλια των 75MHz. Ο πομπός και ο δέκτης συμφωνούν σε ένα hopping pattern και τα δεδομένα στέλνονται σε μια ακολουθία από αυτά τα υποκανάλια. Κάθε συζήτηση μέσα στο 802.11 δίκτυο, συμβαίνει με χρήση διαφορετικού pattern τα οποία είναι έτσι σχεδιασμένα να ελαχιστοποιούν την πιθανότητα δύο πομποί να χρησιμοποιούν το ίδιο υποκανάλι ταυτόχρονα. Οι τεχνικές FHSS επιτρέπουν μια σχετικά απλή σχεδίαση του ραδιόπομποδεκτη, αλλά περιορίζεται σε ταχύτητες όχι υψηλότερες από 2 Mbps. Αυτός ο περιορισμός απορρέει καταρχήν από τους κανονισμούς της FCC που περιορίζουν το εύρος ζώνης του υποκαναλιού στο 1 MHz. Αυτοί οι κανονισμοί αναγκάζουν τα συστήματα FHSS να επεκτείνουν την χρήση τους σε όλη την ζώνη των 2,4MHz, πράγμα που σημαίνει πρέπει να γίνεται hopping συχνά δηλαδή μεγάλη επιβάρυνση λόγω hopping.

Σε αντίθεση με το FHSS, η ενική DSSS διαιρεί την ζώνη των 2,4GHz σε 14 κανάλια. Στην Αμερική, μόνο 11 κανάλια διατίθενται. Για να συνυπάρχουν πολλαπλά κανάλια στην ίδια τοποθεσία , πρέπει αυτά να διαφέρουν κατά 25 MHz για να αποφευχθούν οι παρεμβολές. Αυτό σημαίνει ότι το πολύ 3 κανάλια μπορούν να συνυπαρχουν στην ίδια τοποθεσία. Τα δεδομένα στέλνονται δια μέσου ενός από αυτά τα κανάλια χωρίς hopping σε άλλα κανάλια. Για να μειωθεί ο θόρυβος σε κάποιο κανάλι, χρησιμοποιείται μια τεχνική που ονομάζεται "chipping". Κάθε bit από τα δεδομένα του χρήστη μετατρέπεται σε μια σειρά από πλεονάζοντα pattern τα οποία ονομάζονται "chip". Ο πλεονασμός που αποκτιέται τελικά από κάθε chip σε συνδυασμό με την μετάδοση του σήματος στο κανάλι επιτρέπει την χρήση κώδικα για τον έλεγχο και την διόρθωση των λαθών: ακόμη και αν μέρος του σήματος έχει καταστραφεί, μπορεί να ανακτηθεί πάλι σε πολλές περιπτώσεις, πράγμα που μειώνει την ανάγκη για επαναμεταδόσεις

5.7 MAC LAYER

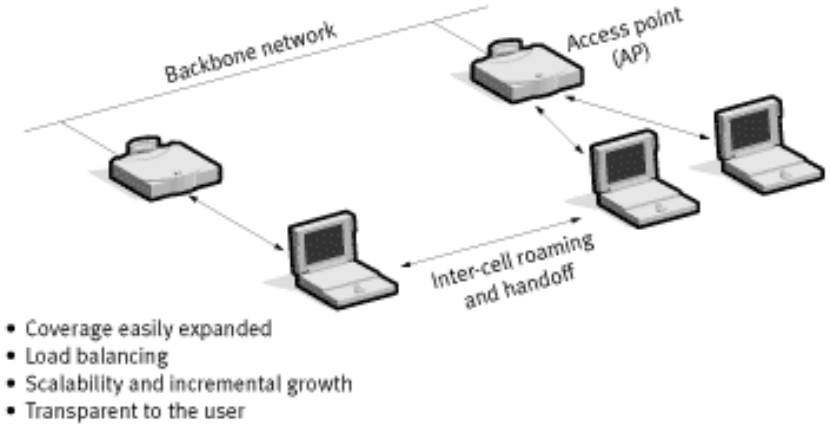
Η δομή του MAC layer του 802.11 είναι κατά τέτοιο τρόπο διαμορφωμένη ούτος ώστε να υποστηρίζει πολλαπλά φυσικά στρώματα (3). Αν και η αρχική λειτουργία του MAC layer είναι να ελέγχει την πρόσβαση στο φυσικό μέσο, αυτό το στρώμα είναι επίσης αρμόδιο και για άλλες λειτουργίες. Αυτές οι πρόσθετες λειτουργίες περιλαμβάνουν τον fragmentation, encryption, power management, synchronization (τεμαχισμό, κρυπτογράφηση, διαχείριση ισχύος και συγχρονισμό). Επιπλέον, το MAC layer είναι υπεύθυνο για τη λειτουργία περιαγωγής όπου υπάρχουν περισσότερα από ένα AP.

Το επίπεδο σύνδεσης δεδομένων του 802.11 αποτελείται από δύο υποστρώματα: Το στρώμα Logical Link Control (LLC) και το Media Access Control(MAC). Το 802.11 χρησιμοποιεί το ίδιο 802.2 LLC και την διευθυνσιοδότηση 48-bit όπως όλα τα υπόλοιπα LANs, επιτρέποντας πολύ απλή γεφύρωση μεταξύ ασύρματου και ενσύρματου IEEE-συμβατού δικτύου, με την διαφορά ότι η MAC διεύθυνση είναι διαφορετική στα WLANs.

Το 802.11 MAC είναι πολύ όμοιο στη σύλληψη με το 802.3, στο ότι έχει σχεδιαστεί για να υποστηρίζει πολλαπλούς χρήστες, σε ένα κοινό μέσο αναγκάζοντας

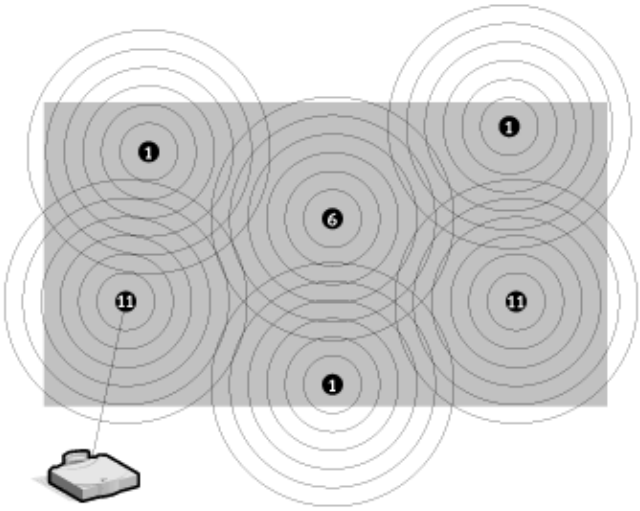
τον πομπό να ακροασθεί το μέσο πριν μεταδώσει. Για τα 802.3 Ethernet LANs, το Carrier Sense Multiple Access with Collision Detection (CSMA/CD) πρωτόκολλο καθορίζει πώς ένας σταθμός αποκτά πρόσβαση στο μέσο και πώς ανιχνεύονται και μεταχειρίζονται οι συγκρούσεις που συμβαίνουν όταν 2 ή περισσότερες συσκευές προσπαθήσουν να μεταδώσουν ταυτόχρονα κατά μήκος του LAN. Σ'ενα 802.11 WLAN, η ανίχνευση των συγκρούσεων δεν είναι εφικτή λόγω του προβλήματος που είναι γνωστό ως το "πρόβλημα near/far": για να ανιχνευτεί μία σύγκρουση, ο σταθμός πρέπει να μπορεί να μεταδίδει και να αφουγκράται την ίδια στιγμή, αλλά τα ραδιοσυστήματα δεν παρέχουν αυτή την δυνατότητα. Για να αντιμετωπιστεί αυτή η διαφορά, το 802.11 χρησιμοποιεί ένα ελαφρώς διαφορετικό πρωτόκολλο, γνωστό ως Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) ή την Distributed Coordination Function (DCF). Το CSMA/CA προσπαθεί να αποφύγει τις συγκρούσεις χρησιμοποιώντας ειδικά πακέτα acknowledgment (ACK), το οποίο σημαίνει ότι ένα ACK πακέτο στέλνεται από τον σταθμό-δέκτη για να επιβεβαιώσει ότι το πακέτο δεδομένων έχει φτάσει ανέπαφο στον προορισμό του.

Το 802.11 MAC επίπεδο είναι υπεύθυνο για το πως ένας σταθμός συσχετίζεται με ένα σημείο πρόσβασης. Όταν ένας τέτοιος πελάτης μπει στην εμβέλεια ενός ή περισσότερων σημείων πρόσβασης διαλέγει ένα AP για να συσχετιστεί μαζί του, δηλαδή να μπει σε ένα σύνολο βασικής υπηρεσίας, βασιζόμενος στην ισχύ του σήματος και τα ποσοστά λαθών στα πακέτα που παρατηρεί. Μόλις γίνει δεκτός από το σημείο πρόσβασης, ο πελάτης συγχρονίζεται στη ραδιοσυχνότητα του καναλιού του AP. Περιοδικά εξετάζει όλα τα 802.11 κανάλια για να αποφανθεί αν υπάρχει κάποιο σημείο πρόσβασης που θα του παρείχε καλύτερη απόδοση. Αν διαπιστώσει κάτι τέτοιο, επανασυσχετίζεται με το νέο AP, συγχρονίζοντας το ραδιοπομπό του στο ραδιοκανάλι του νέου σημείου πρόσβασης.



Σχήμα 41: Διασύνδεση backbone network με BSS

Επανασυσχέτιση συνήθως συμβαίνει διότι ο ασύρματος σταθμός έχει αλλάξει φυσική θέση μακρύτερα από το αρχικό σημείο πρόσβασης, προκαλώντας αποδυνάμωση του λαμβανόμενου σήματος. Σε άλλες περιπτώσεις, επανασυσχέτιση συμβαίνει λόγω μίας αλλαγής στα χαρακτηριστικά ραδιομετάδοσης του κτιρίου, ή ακόμη και απλά από υψηλή δικτυακή κυκλοφορία στο αρχικό AP. Στην τελευταία περίπτωση αυτή η λειτουργία είναι γνωστή σαν " load balancing" -- ισορρόπηση φορτίου, αφού η πρωταρχική του λειτουργία είναι να κατανέμει το συνολικό φορτίο του WLAN πιο αποδοτικά μεταξύ της υπάρχουσας υποδομής σε ασύρματο εξοπλισμό.



Σχήμα 42: Επικαλυπτόμενες κυψέλες

Αυτή η διαδικασία δυναμικής συσχέτισης και επανασυσχέτισης με AP επιτρέπει στους διαχειριστές του δικτύου να διαμορφώσουν WLANs με πολύ ευρεία κάλυψη δημιουργώντας μία σειρά από επικαλυπτόμενες κυψέλες που ακολουθούν το 802.11b, σε όλη την έκταση ενός κτιρίου ή μίας ολόκληρης περιοχής. Για να το επιτύχει αυτό ο τεχνικός πρέπει να εκμεταλλευτεί την "επαναχρησιμοποίηση καναλιού", φροντίζοντας να εγκαταστήσει κάθε σημείο πρόσβασης σε ένα 802.11 DSSS κανάλι το οποίο δεν επικαλύπτεται με ένα άλλο τέτοιο κανάλι που χρησιμοποιεί γειτονικό σημείο πρόσβασης (σχήμα 42). Όπως σημειώθηκε παραπάνω, ενώ υπάρχουν 14 μερικώς επικαλυπτόμενα κανάλια που ορίζονται από το 802.11 DSSS, υπάρχουν μόλις 3 κανάλια αμιγώς ανεξάρτητα, και αυτά είναι τα καλύτερα για να χρησιμοποιηθούν για κάλυψη πολλών κυψέλων. Εάν ένα σημείο πρόσβασης είναι μέσα στην εμβέλεια ενός άλλου σημείου πρόσβασης και έχουν τεθεί ώστε να χρησιμοποιούν το ίδιο ή μερικώς επικαλυπτόμενα κανάλια, τότε μπορεί να προκαλούν κάποιες παρεμβολές το ένα στο άλλο και επομένως να επέρχεται μείωση του bandwidth στην περιοχή της επικάλυψης.

5.7.1 Υποστήριξη για δεδομένα που εξαρτώνται άμεσα από το χρόνο

Τα δεδομένα που είναι ευαίσθητα στο χρόνο όπως η φωνή και το video υποστηρίζονται από το επίπεδο του MAC του προτύπου 802.11b με την λειτουργία συντονισμού σημείου *Point Coordination Function (PCF)*. Σε αντίθεση με το DFC, όπου ο έλεγχος κατανέμεται σε όλους τους σταθμούς, στην PCF λειτουργία ένα απλό σημείο πρόσβασης ελέγχει την πρόσβαση στο μέσο. Εάν ένα BSS έχει τεθεί να λειτουργεί σε PCF mode, το σύστημα κάποιο μέρος του χρόνου λειτουργεί σε PCF mode και κάποιο άλλο σε DCF (CSMA/CA) mode. Κατά την διάρκεια του χρόνου που το σύστημα βρίσκεται σε PCF mode, το σημείο πρόσβασης "ρωτάει" διαδοχικά κάθε σταθμό αν έχει δεδομένα για αποστολή μετά από δοσμένο χρονικό διάστημα. Κανένας σταθμός δεν επιτρέπεται να μεταδώσει δεδομένα αν δεν έχει πρώτα ερωτηθεί, και οι σταθμοί λαμβάνουν δεδομένα από το σημείο πρόσβασης μόνο όταν εξεταστούν . Εφόσον το PCF καθορίζει την σειρά μετάδοσης με προκαθορισμένο τρόπο, μια μέγιστη καθυστέρηση μπορεί να εγγυηθεί. Ένα μειονέκτημα του PCF αποτελεί το ότι δεν είναι ιδιαίτερα ευέλικτο από την άποψη ότι ένα μόνο σημείο

πρέπει να έχει έλεγχο της πρόσβασης στο μέσο και μα "ρωτάει" κάθε σταθμό πράγμα που είναι αναποτελεσματικό σε μεγάλα δίκτυα.

5.7.2 Διαχείριση ισχύος

Πέρα από τον έλεγχο πρόσβασης στο μέσο, το 802.11 HR MAC υποστηρίζει συντήρηση ισχύος για να παρατείνει την ζωή της μπαταρίας των φορητών συσκευών. Το στάνταρτ υποστηρίζει δύο τρόπους χρήσεις της ενέργειας που καλούνται Continuous Aware Mode και Power Save Polling Mode. Στην πρώτη ο ραδιοπομπός είναι συνέχεια σε λειτουργία και καταναλώνει ενέργεια, ενώ στην δεύτερη ο ραδιοπομπός ανοιγοκλείνει και το σημείο πρόσβασης βάζει σε μία ουρά τα δεδομένα που προορίζονται για αυτό. Ο ραδιοπομπός του σταθμού-πελάτη περιοδικά τίθεται σε λειτουργία με σκοπό να παραλάβει τακτά καθοδηγητικά σήματα από το σημείο πρόσβασης. Τα σήματα -οδηγοί περιλαμβάνουν πληροφορίες που αφορούν τους σταθμούς που έχουν κυκλοφορία που απευθύνεται σε αυτούς. Επομένως με την λήψη ενός τέτοιου σήματος ο σταθμός αφυπνίζεται για να λάβει τα δεδομένα , και μετά να επιστρέψει στην προηγούμενη κατάσταση.

5.8 OPERATION

Οι δύο βασικές λειτουργίες του ασύρματου τοπικού LAN: η μέθοδος με την οποία ένας σταθμός εισέρχεται και συνδέεται σε ένα BSS και η περίπτωση στην οποία έχουμε τη μετακίνηση ενός σταθμού από ένα BSS σε ένα άλλο.

Joining an Existing Cell: Υπάρχουν δυο περιπτώσεις που ένας σταθμός χρειάζεται να επιδιώξει πρόσβαση σε ένα υπάρχον basic service set (BSS).
1. Τη στιγμή που ο σταθμός ενεργοποιείται (powered up) από κατάσταση sleep mode
2. Όταν μπαίνει σε μια περιοχή BSS.

Για κάθε κατάσταση, ο σταθμός πρέπει να λάβει τις πληροφορίες συγχρονισμού. Κανονικά, αυτές οι πληροφορίες λαμβάνονται από ένα AP, εντούτοις, μπορούν επίσης να ληφθούν από άλλους σταθμούς μέσα στο BSS. Το τελευταίο αναφέρεται ως *ad-hoc mode of operation*. Για κάθε μια η κατάσταση, ο σταθμός θα αποκτήσει το συγχρονισμό μέσω, είτε ενεργούς, είτε παθητικής ανίχνευσης. Μόλις ολοκληρωθεί αυτό, ο σταθμός θα πρέπει έπειτα να περάσει από μια διαδικασία επικύρωση ταυτότητας (authentication).

5.8.1 Active Scanning

Η ενεργός ανίχνευση απαιτεί από έναν σταθμό να εντοπίσει ένα σημείο πρόσβασης ώστε να μπορεί να λάβει τις πληροφορίες συγχρονισμού. Για να ολοκληρώσει αυτόν τον στόχο, ο σταθμός θα διαβιβάσει τον έλεγχο request frames και θα περιμένει ένα πακέτο απάντησης ελέγχου, που διαβιβάζεται από το AP.

5.8.2 Passive Scanning

Μια άλλη μέθοδος με την οποία ένας σταθμός μπορεί να λάβει πληροφορίες συγχρονισμού είναι δια μέσου της παθητικής ανίχνευσης (passive scanning). Αν

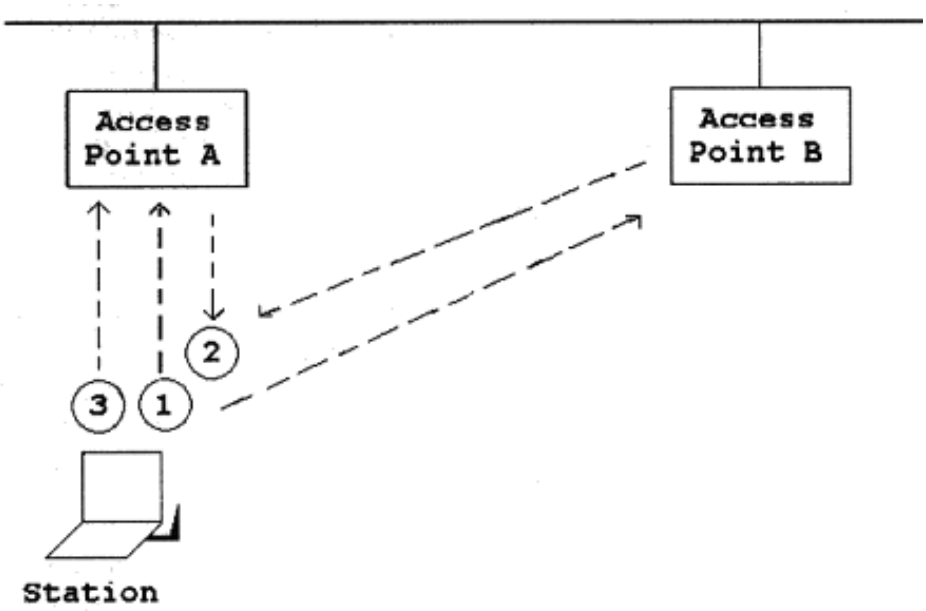
υποθέσουμε ότι ένας σταθμός είναι μέσα σε μια κατάλληλη απόσταση από ένα AP, μπορεί να λάβει ένα πλαίσιο αναγνωριστικών σημάτων που διαβιβάζεται περιοδικά από κάθε ένα AP. Επειδή το πλαίσιο αναγνωριστικών σημάτων περιέχει πληροφορίες συγχρονισμού, η δυνατότητα να λάβει τα πλαίσια αναγνώρισης παρέχει σε έναν σταθμό τις πληροφορίες συγχρονισμού που χρειάζεται. Η μέθοδος που θα χρησιμοποιηθεί από έναν σταθμό, active ή passive scanning, θα εξαρτηθεί από δύο παράγοντες, από την κατανάλωση ισχύος του σταθμού και την απόδοσή του.

5.8.3 Authentication και Association.

Μόλις ένας σταθμός, εντοπίσει ένα AP και λάβει πληροφορίες συγχρονισμού, πρέπει να ανταλλάξει πληροφορίες επικύρωσης (authentication). Αυτή η ανταλλαγή, των πληροφοριών πραγματοποιείται μεταξύ του AP και του σταθμού, κατά τη διάρκεια της οποίας κάθε συσκευή λαμβάνει γνώση ενός δεδομένου κωδικού πρόσβασης.

Μετά την επικύρωση του σταθμού, η διαδικασία σύνδεσης αρχίζει. Κατά τη διαδικασία σύνδεσης, οι πληροφορίες για το σταθμό και η δυνατότητες υποστήριξης-συμβατότητας του BSS ανταλλάσσονται. Αυτό επιτρέπει σε μια ομάδα APs να λάβει πληροφορίες σχετικά με την τρέχουσα θέση ενός σταθμού. Μόλις ολοκληρωθεί η διαδικασία σύνδεσης, ο σταθμός γίνεται ικανός να διαβιβάσει και να λάβει frames.

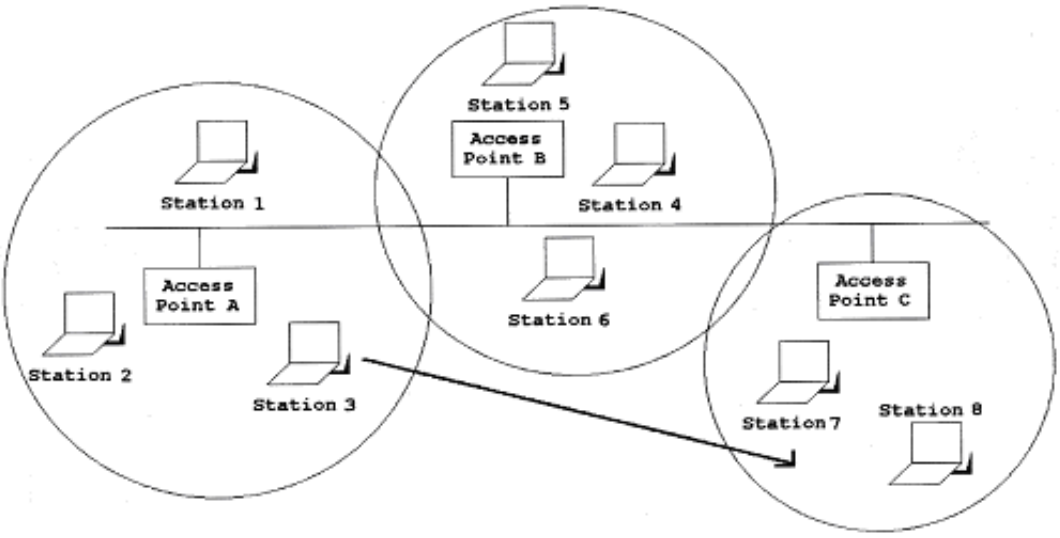
Το παρακάτω σχήμα επεξηγεί τη σειρά των βημάτων στην ενεργό διαδικασία ανίχνευσης και ένωσης που απαιτείται πριν από έναν σταθμό όντας σε θέση να ανταλλάξει τις πληροφορίες. Σημειώστε ότι αν και δύο σημεία πρόσβασης παρουσιάζονται, ένας σταθμός θα μπορούσε να εξετάσει περισσότερα από δύο πλαίσια απάντησης ελέγχου, για να επιλέξει ένα AP.



Σχήμα 43: Διαδικασία ανίχνευσης και ένωσης

5.9 ROAMING

Κάθε σταθμός στο IEEE 802.11 ασύρματου LAN συνδέεται με ένα συγκεκριμένο σημείο πρόσβασης. Όταν ένας σταθμός κινείται από μια κυψέλη (BSS) σε άλλη χωρίς απώλεια σύνδεσης, είναι σε κατάσταση περιαγωγής (Roaming).
Η παρακάτω εικόνα επεξηγεί ένα παράδειγμα roaming. Σε αυτό το παράδειγμα, το ασύρματο LAN η υποδομή αποτελείται από τρία AP και οκτώ σταθμούς. Σταθμοί 1, 2, και 3 συνδέονται με AP B, οι σταθμοί 7 και 8 συνδέεται με το σημείο πρόσβασης C. Σε αυτό το παράδειγμα, ο σταθμός 3 πραγματοποιεί roaming με την κίνησή του από τον τομέα της κάλυψης του σημείου πρόσβασης A στον τομέα της κάλυψης του σημείου πρόσβασης C.



Σχήμα 44: Παράδειγμα Roaming

5.9.1 Comparison With Cellular.

Αν και το roaming στο ασύρματο LAN περιβάλλον είναι παρόμοιο με το roaming σε ένα κυψελοειδές περιβάλλον, υπάρχουν δύο βασικές διαφορές. Πρώτον, το IEEE 802.11 standard υποστηρίζει τη μετάδοση πακέτων που έχουν διεύθυνση προορισμού, sequence, και fragment identification. Αυτό διευκολύνει το LAN roaming επειδή η μετάβαση αναμένεται να συμβεί με σχετικά πολύ μικρές ταχύτητες συγκριτικά με το raoming της κινητής κυψελωτής τηλεφωνίας, όπως για παράδειγμα είναι πολύ συχνές οι μεταβάσεις που ο σταθμός βρίσκεται μέσα σε ένα κινούμενο όχημα με πολύ μεγάλη ταχύτητα. Δεύτερον, ενώ ένα προσωρινό χάσμα-διακοπή στη μετάδοση μπορεί να μην έχει επιπτώσεις σε μια φωνητική συνομιλία, η επίδρασή του μπορεί να είναι εντονότερη στο ασύρματο LAN. Αυτό γίνεται επειδή η ανικανότητα να παραληφθεί ένα πακέτο θα προκαλέσει τον αποστολέα σταθμό να εκτελέσει εκ νέου μια αναμετάδοση . Αυτό αρχίζει χαρακτηριστικά από ένα ανώτερο layer του πρωτόκολλο που θέτει έναν timer πριν από κάθε μετάδοση. Εάν το χρονόμετρο λήξει χωρίς ο αποστολέας σταθμός να λάβει ACK, θα επανεκπέμψει το πακέτο. Επειδή η σε πραγματικό χρόνο φωνή χάνεται απλά και δεν αναμεταδίδεται, αυτό σημαίνει ότι μια προσωρινή αποσύνδεση μπορεί να έχει επιπτώσεις στο ασύρματο LAN περισσότερες από ένα κυψελοειδές τηλεφωνικό δίκτυο οφειλόμενος στις αναμεταδόσεις που περιγράφονται παραπάνω.

5.9.2 Operation

Κατά τη διαδικασία του roaming, ένας σταθμός που απομακρύνεται από το σημείο πρόσβασής του θα αντιλαμβάνεται ότι η σύνδεσή του με το AP γίνεται ανεπαρκής. Ο σταθμός θα χρησιμοποιήσει έπειτα τη λειτουργία ανίχνευσής του για να εντοπίσει ένα άλλο AP, ή θα μπορούσε να χρησιμοποιήσει τις πληροφορίες από μια προηγούμενη ανίχνευση για να επιλέξει ένα άλλο AP. Μόλις βρεθεί ένα νέο AP, ο σταθμός θα διαβιβάσει μια αίτηση επανασύνδεσης (reassociation request) στο AP. Εάν ο σταθμός λάβει απάντηση επανασύνδεσης (reassociation response), ο σταθμός έχει ένα νέο AP και έχει μπει στη διαδικασία roaming επιτυχώς.

Για να παραγάγει ένα reassociation response, το AP πρέπει να δηλώσει επανασύνδεση στο σύστημα διανομής (DS). Το DS κάνει αναπροσαρμογές στις πληροφορίες του και κοινοποιεί ότι το παλαιό AP δεν συνδέεται πλέον με το σταθμό. Εάν ο σταθμός δεν λάβει reassociation response, θα ανιχνεύσει για ένα άλλο AP.

5.9.3 Basic Access Method

Το πρότυπο IEEE 802.11 χρησιμοποιεί μια παραλλαγή του πρωτοκόλλου Carrier Sense Multiple Access με Collision Avoidance (CSMA/CA) για να παρέχει τη δυνατότητα ασύρματης πρόσβασης. Το πρωτόκολλο CSMA/CA επιτυγχάνει την αποφυγή συγκρούσεων αντί της ανίχνευσης μιας σύγκρουσης, που επιτυγχάνει το πρωτόκολλο CSMA/CD που χρησιμοποιείται από το πρότυπο IEEE 802.3 (Ethernet).

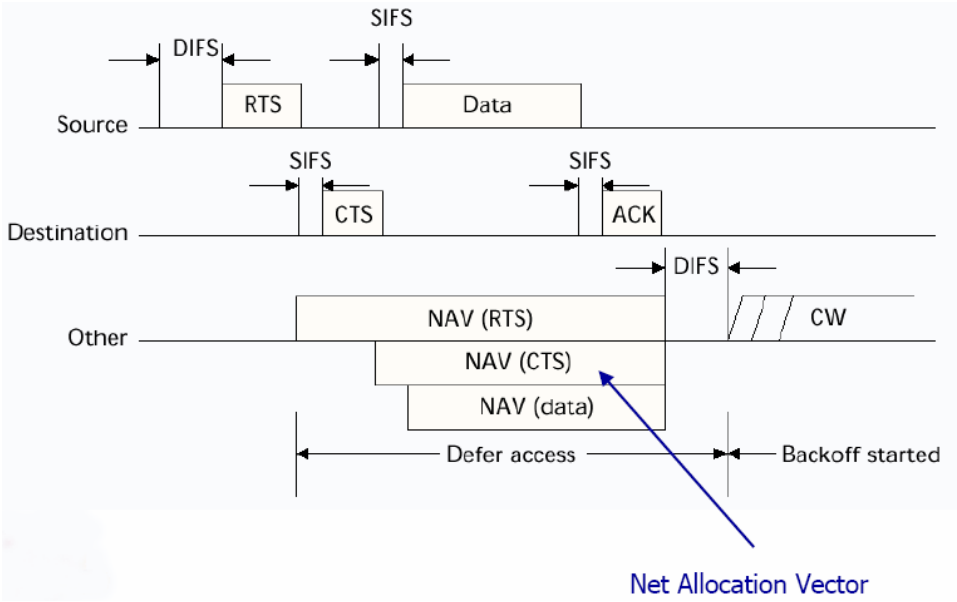
Η διαφοροποίηση του CSMA/CA protocol έγκειται στο γεγονός ότι ο σταθμός που θέλει να εκπέμψει, ακροάζεται το μέσο. Εάν το μέσο είναι απασχολημένο, ο σταθμός θα αναβάλει τη μετάδοσή του. Εάν το μέσο είναι διαθέσιμο για έναν καθορισμένο χρόνο, (αναφέρεται ως *distributed interframe space* (DIFS)), ο σταθμός μπορεί να εκπέμψει. Επειδή είναι δυνατό ένας άλλος σταθμός να θέλει να μεταδώσει περίπου στον ίδιο χρόνο, ο δέκτης θα ελέγξει το CRC από τα λαμβανόμενα πακέτα και διαβιβάζει ένα acknowledgment που ενημερώνει τον αποστολέα του ότι καμία σύγκρουση δεν εμφανίστηκε. Διαφορετικά, εάν ο αποστολέας δεν λάβει acknowledgment, θα διαβιβάζει μέχρι να λάβει acknowledgment ή θα εκπέμψει διαδοχικά το ίδιο πακέτο για ένα προκαθορισμένο αριθμό επαναλήψεων. Σχετικά με τα παραπάνω, εάν ο αποστολέας δεν λαμβάνει ένα acknowledgment μετά από έναν σταθερό αριθμό δοκιμών, θα εγκαταλείψει την προσπάθειά του, και το υψηλότερο στρώμα του πρωτοκόλλου θα ορίσει τον τρόπο με τον οποίο το πρόβλημα θα αντιμετωπιστεί.

Αυτού του είδους της μεθόδου πρόσβασης στο φυσικό μέσο του IEEE 802.11 προτύπου distributed coordination function (DCF), το οποίο μπορεί να θεωρηθεί ότι αντιπροσωπεύει μια μέθοδο CSMA/CA. Ο λόγος επιλογής αυτής της μεθόδου πρόσβασης στη θέση του CSMA/CD είναι ότι το CSMA/CD δεν είναι πρακτικό σε ασύρματο περιβάλλον. Και αυτό γιατί η εφαρμογή της μεθόδου CSMA/CD θα απαιτούσε ένα full-duplex RF ή IR ζευγάρι καναλιών το οποίο θα ήταν πολύ δαπανηρό. Επιπλέον, αντίθετα από τα ασύρματα LAN, όπου όλοι οι σταθμοί μπορούν να «ακούσουν» πότε συμβαίνει collision, σε ασύρματο περιβάλλον αυτό δεν συμβαίνει πάντα.

5.9.4 Minimizing Collisions

Επειδή είναι πιθανό, δυο σταθμοί ταυτόχρονα να μην αντιλαμβάνονται δραστηριότητα εκπομπής και συνεπώς να υποθέσουν ότι το φυσικό μέσο είναι

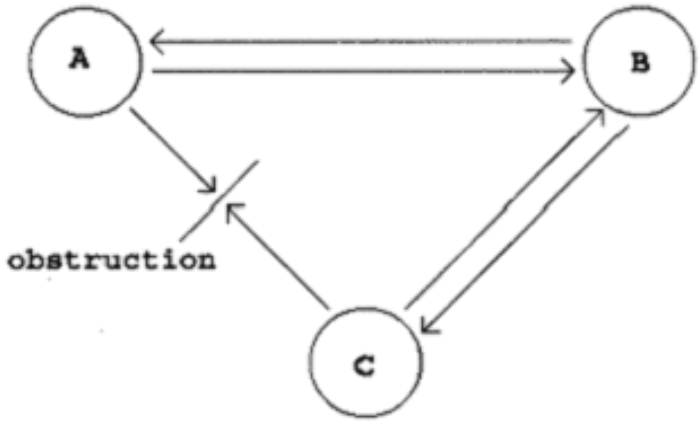
ελεύθερο και ότι μπορούν να εκπέμψουν, αποτέλεσμα είναι η ταυτόχρονη εκπομπή και των δύο και συνεπώς να συμβαίνει collision. Για να μειώσει τη πιθανότητα collision η μέθοδος CSMA/CA που υιοθετείται από το 802.11 χρησιμοποιεί μια τεχνική αναφερόμενη ως *virtual carrier sense* (VCS). Σύμφωνα με το VCS ένας σταθμός που θέλει να εκπέμψει ένα πακέτο, πρώτα θα εκπέμψει ένα request-to-send (RTS) packet. Το RTS packet είναι ένα σχετικά μικρό πακέτο έλεγχου που περιλαμβάνει τη διεύθυνση προέλευσης και προορισμού και τη διάρκεια της εκπομπής που θα επακολουθήσει. Η διάρκεια καθορίζεται από το μέγεθος του πακέτου και τον απαιτούμενο χρόνο αποστολής του acknowledgment του δέκτη. Ο δέκτης θα απαντήσει στο RTS πακέτο με ένα clear-to-send (CTS) control packet. Το CTS πακέτο θα υποδεικνύει την ίδια ακριβώς πληροφορία διάρκειας που εμπεριείχε και το RTS packet. Κάθε σταθμός που δέχεται τα πακέτα αυτά ή ένα από τα δυο πακέτα ή και τα δυο θα ρυθμίσει τον δείκτη virtual carrier sense indicator στη διάρκεια της εκπομπής. Ο VCS indicator καλείται ως *network allocation vector-δείκτης παραχώρησης δικτύου* (NAV) σύμφωνα με την ορολογία του IEEE 802.11 και λειτουργεί σαν μηχανισμός ενημέρωσης όλων των άλλων σταθμών του δικτύου να αναβάλλουν ή να καθυστερήσουν για λίγο την εκπομπή τους. Αν το CTS δεν ληφθεί σε προκαθορισμένο χρονικό διάστημα, ο αποστολέας σταθμός θα υποθέσει ότι έχει συμβεί κάποιο Collision και θα επαναλάβει την όλη διαδικασία, ξεκινώντας με την εκ νέου αποστολή ενός RTS πακέτου.



Σχήμα 45: Network Allocation Vvector-δείκτης παραχώρησης δικτύου (NAV)

Εάν το CTS frame ληφθεί από τον αποστολέα και το frame των δεδομένων σταλεί, ο δέκτης θα επιστρέψει ένα acknowledgement (ACK) packet για την επιβεβαίωση της επιτυχούς διαδικασίας.

Η χρήση των πακέτων RTS και CTS μειώνει τις πιθανότητες να συμβούν collisions τα οποία θα οφείλονται στο φαινόμενο του 'κρυμμένου σταθμού'(Σχήμα 46), εδώ το φαινόμενο του κρυμμένου κόμβου παραπέμπει σε ένα σταθμό ενός service set που δεν μπορεί να αντιληφθεί την μετάδοση ενός άλλου σταθμού και έτσι αποτυγχάνει να αναγνωρίσει ότι το φυσικό μέσο είναι κατειλημμένο.



Σχήμα 46: Φαινόμενο κρυμμένου σταθμού

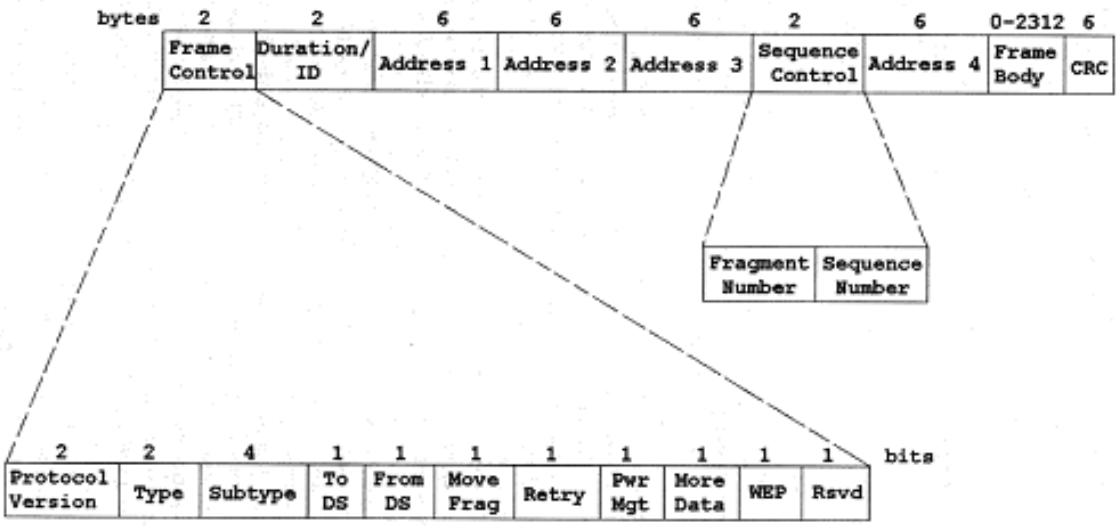
5.10 FRAME TYPES

Το MAC layer υποστηρίζει τρις διαφορετικούς τύπους από frames:

Data frames, τα οποία χρησιμοποιούνται για τη μετάδοση δεδομένων μεταξύ των σταθμών

Control frames, τα οποία χρειάζονται στον έλεγχο πρόσβασης στο μέσο.

Και management frames, τα οποία χρησιμεύουν στην ανταλλαγή πληροφορίας management, μεταξύ των σταθμών στο δεύτερο στρώμα αλλά δεν διαβιβάζεται στα ανώτερα επίπεδα.



Σχήμα 47: MAC Data Format

MAC DATA το σχήμα απεικονίζει το format ενός MAC data frame χρησιμοποιούμενο στη μετάδοση δεδομένων μεταξύ των σταθμών. Όπως θα διαπιστώσουμε στη συνέχεια, τμήματα αυτού του frame, χρησιμοποιούνται και σε άλλους τύπους πλαισίων (frames). το πλαίσιο στο σύνολό του αποτελείται από μια ακολουθία bits μεγίστου μήκους 2312bytes. Κατά συνέπεια αυτό παρέχει τη δυνατότητα να μπορεί μεταφερθεί ένα πλαίσιο Ethernet μεγίστου μήκους. Σημειώνουμε ότι το μέγιστο μήκος ενός πλαισίου Ethernet είναι 1500bits. Λόγω του ότι ένα λάθος στη σειρά μετάδοσης των bits μιας RF ζεύξης είναι πιθανότερο από ότι σε ένα ενσύρματο δίκτυο, η πιθανότητα αλλοίωσης ενός MAC data frame 802.11

αυξάνει όσο μεγαλύτερο είναι το μήκος των bit της πληροφορίας που περικλείει. Για να αντισταθμίσει αυτή την κατάσταση το MAC layer υιοθετεί ένα μηχανισμό τεμαχισμού (Fragmentation) και επανασυναρμολόγησης.

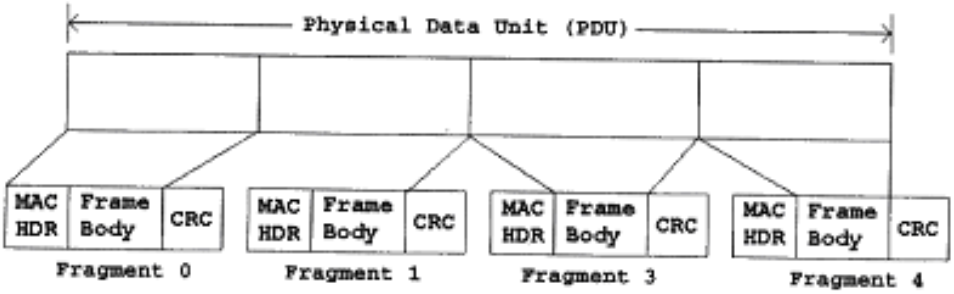
Control Field. Το Control field αποτελείται από 11 fields, από τα οποία τα 8 είναι fieldsτου ενός 1-bit , που ορίζουν ότι την ενεργοποίηση ή απενεργοποίηση μιας ιδιαίτερης ιδιότητας ή συνάρτησης.

1. Protocol Version Subfield. Τα 2-bit του Protocol Version subfieldπαρέχουν ένα μηχανισμό προσδιορισμού της έκδοσης του IEEE 802.11 προτύπου.
2. Type and Subtype Subfields. Αποτελούνται από 6 bits που προσδιορίζουν το πλαίσιο. Το Type subfield μπορεί να προσδιορίσει, μέχρι τέσσερις διαφορετικούς τύπους πλαισίων παρόλο που μέχρι σήμερα έχουν οριοθετηθεί μόνο τρεις. Τα άλλα 4 bits του Subtype subfield identifies προσδιορίζουν ένα συγκεκριμένο τύπο πλαισίου της κατηγορίας Type. Ο παρακάτω πίνακας απεικονίζει τις πιθανές ακολουθίες Type και Subtype subfield και τι κάθε μια αντιπροσωπεύει.

Type Value b3 b2	Type Description	Subtype Value b7 b6 b5 b4	Subtype Description
00	Management	0007	Association request
00	Management	0001	Association response
00	Management	0010	Association request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110-0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101-1111	Reserved
01	Control	0000-0001	Reserved
01	Control	1010	PS poll
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	ACK
01	Control	1110	CF end
01	Control	1111	CF end + CF-ACK
10	Data	0000	Data
10	Data	0001	Data + CF-ACK
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-ACK + CF-Poll
10	Data	0100	Null function (no data)
10	Data	0101	CF-ACK (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-ACK + CF-Poll (no data)
10	Data	1000-1111	Reserved
10	Data	0000-1111	Reserved

Πίνακας 48: Πιθανές ακολουθίες Type και Subtype subfield

3. DS Subfield: Αυτό το field του 1byte παίρνει την τιμή ένα, όταν το πλαίσιο προορίζεται σε ένα AP, μέσο του οποίου πρέπει να προωθηθεί στο ευρύτερο distribution system.
4. FromDS Subfield: Η τιμή και αυτού του τομέα, παίρνει την τιμή 1 όταν ένα πλαίσιο έχει προέρθει από το distribution system.
5. More Fragments Subfield: Είναι ένα ακόμα subfield του 1-bit του οποίου η τιμή γίνεται 1, όταν περισσότερα fragments που ανήκουν στο ίδιο fragment, όταν πρόκειται να ακολουθήσουν το ίδιο fragment. Δηλαδή, στην περίπτωση αυτή ένα πλαίσιο έχει υποστεί fragmentation με αποτέλεσμα να έχουμε διαδοχική μετάδοση των fragments του πλαισίου, αυτή η ιδιότητα είναι απαραίτητη στο resuscitation των fragments στο αρχικό πλαίσιο. Το σχήμα 49 απεικονίζει το frame fragmentation process (διαδικασία τεμαχισμού των πλαισίων) fragments.



Σχήμα 49: Διαδικασία τεμαχισμού των πλαισίων

Το fragmentation transmission process σύμφωνα με το πρότυπο IEEE 802.11 βασίζεται σε ένα απλό αλγόριθμο send-and-wait. Ο αλγόριθμος της ορίζει ότι ο σταθμός που μεταδίδει δεν μπορεί να στείλει ένα νέο fragment έως ότου λάβει ACK που αντιστοιχεί στο προηγούμενο segment ή αποφασίζει ότι το fragment αναμεταδόθηκε ένα προκαθορισμένο αριθμό επαναλήψεων και μεταδίδει ολόκληρο το πλαίσιο.

6. Retry Subfield: Subfield του 1-bit που υποδεικνύει ότι το συγκεκριμένο frame αποτελεί την αναμετάδοση του προηγούμενου fragment του οποίου η λήψη δεν ολοκληρώθηκε επιτυχώς. Ο αποδέκτης σταθμός χρησιμοποιεί αυτό το πεδίο για να εντοπίσει διπλές μεταδόσεις που μπορούν να συμβούν σε περίπτωση που ένα ACK χαθεί.
7. Power Management Subfield: Οι 802.11 σταθμοί είναι δυνατό να βρίσκονται σε δυο καταστάσεις λειτουργίας, σε κατάσταση power save (ανενεργός) ή active (ενεργός). Της ενεργός σταθμός αφού ολοκληρώσει τη μετάδοση της πλαισίου μπορεί να εισέλθει σε κατάσταση power save (ανενεργός). Μέσο του πεδίου Power_Management της σταθμός δηλώνει την κατάσταση λειτουργίας στην οποία βρίσκεται. Η πληροφορία αυτή είναι απαραίτητη στο AP το οποίο ενημερώνει συνεχώς ένα αρχείο των σταθμών που βρίσκονται σε κατάσταση power save. Το AP διατηρεί αποθηκεύοντας προσωρινά σε ένα buffer του, πακέτα διευθυνσιοδοτημένα σε τέτοιους σταθμούς, έως ότου ζητήσουν πακέτα εκπέμποντας ένα polling request ή αλλάξουν κατάσταση λειτουργίας.
   Μια άλλη τεχνική για τη μετάδοση πακέτων αποθηκευμένων προσωρινά στο AP της ένα σταθμό ο οποίος βρίσκεται σε κατάσταση power save επιτυγχάνεται μέσο της χρήσης πακέτων επισήμανσης beacon frames. Το AP

θα διαβιβάσει περιοδικά beacon frames που αφορούν σταθμούς που βρίσκονται σε κατάσταση power save mode. Οι σταθμοί αυτοί θα εξέλθουν από την κατάσταση αυτή δεχόμενοι τα beacon frames και με αυτό τον τρόπο πληροφορούνται ότι υπάρχουν κάποια πλαίσια αποθηκευμένα στο AP που περιμένουν να παραδοθούν. Οι σταθμοί εν συνεχεία θα παραμείνουν σε κατάσταση active και θα στείλουν ένα polling message στο AP της να διευθετήσουν αυτή την παράδοση.

8. More Data Subfield: Της το όνομά του υποδηλώνει, το More Data subfield δείχνει ότι περισσότερα πλαίσια ακολουθούν το εν λόγο πλαίσιο. Το συγκεκριμένο bit γίνεται 1 από το AP υποδεικνύοντας ότι υπάρχουν αποθηκευμένα περισσότερα πλαίσια που αφορούν αυτό το σταθμό. Ο σταθμός στη συνέχεια θα αποφασίσει αν θα πρέπει να αλλάξει την κατάστασή του σε active.
9. Web Subfield: Το πεδίο αυτό ορίζει ότι το εν λόγο πλαίσιο είναι κρυπτογραφημένο σύμφωνα με τον Web αλγόριθμο.
10. Order Subfield: Το τελευταίο αυτό subfield του frame control

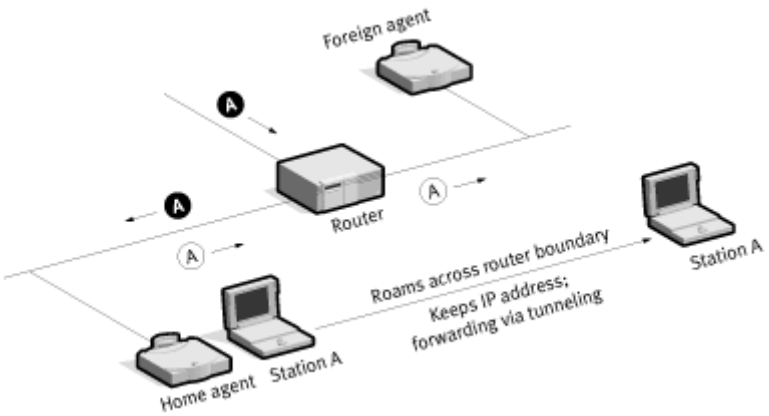
Duration/ID Field: η έννοια αυτού του πεδίου, εξαρτάται από τον τύπο του πλαισίου, σε ένα power save poll massage το πεδίο αυτό υποδηλώνει την ταυτότητα του σταθμού. Σε όλους της της τύπους πλαισίων δηλώνει την τιμή της διάρκειας η οποία αντιπροσωπεύει το χρόνο σε μsec που απαιτείται για τη μετάδοση του πλαισίου και το μεσοδιάστημα ως το επόμενο frame.

Address Fields: Είναι 4 fields τα οποία περιλαμβάνουν 4 διευθύνσεις σχετικά με τα distribution systems αποστολής και προορισμού και με της σταθμούς μετάδοσης και λήψης του πλαισίου, καθώς και των BSS στα οποία ανήκουν.
Α) Address 1: εάν έχει την τιμή 1, τότε περιλαμβάνει τη διεύθυνση του AP. Της μπορεί να περιέχει την διεύθυνση προορισμού (DA), την basic service set ID (BSSID) ή τη διεύθυνση recipient (RA).
Β) Address 2: Πάντα χρησιμοποιείται για την ταυτοποίηση του αποστολέα σταθμού.
Γ) Address 3: Μπορεί να περιλαμβάνει την διεύθυνση του αποστολέα (SA) ή τη διεύθυνση προορισμού (DA).
Δ) Address 4: Η διεύθυνση αυτή εμπλέκεται στην περίπτωση όπου ένα δεύτερο distribution system συμμετέχει και η μετάδοση συμβαίνει από ένα AP σε ένα άλλο. Αφορά τη διεύθυνση του πρώτου DS.

Εργαλεία διαχείρισης

Εφόσον ένα ασύρματο τοπικό δίκτυο που ακολουθεί το πρότυπο 802.11b, διαφέρει από τα κλασικά καλωδιωμένα LAN μόνο στα επίπεδα 1 και 2 του μοντέλου OSI, είναι αναμενόμενο το ίδιο τουλάχιστον επίπεδο διαχειρησιμότητας για τα προϊόντα αυτά , της συναντάται στα προϊόντα δικτύου για τα ενσύρματα δίκτυα. Τα προϊόντα αυτά λοιπόν, υποστηρίζουν το SNMP version 2, άρα μπορούν να διαχειρισθούν της και οι ενσύρματες δικτυακές συσκευές χρησιμοποιώντας της εφαρμογές και με της κατάλληλες MIBs να ελεγχθούν επιμέρους λειτουργίες του ασύρματου εξοπλισμού.

Εκτός από το SNMP, είναι χρήσιμο να υπάρχει η δυνατότητα για configuration και probing των AP's μέσω εύχρηστων Web περιβάλλοντος. Επιπλέον το κόστος της διαχείρισης μειώνεται αν υπάρχει η δυνατότητα για διαχείριση των συσκευών αυτών κατά ομάδες.



Σχήμα 50: Λειτουργία Roaming

ΚΕΦΑΛΑΙΟ 6°

6.1 ΚΑΤΗΓΟΡΙΕΣ WLAN 802.11

6.1.1 802.11a

Το πρότυπο 802.11a του IEEE, δημοσιεύτηκε το 1999, αλλά οι πρώτες συσκευές κυκλοφόρησαν στην αγορά τέλος του 2001.

Αποδίδει μέγιστο ρυθμό μετάδοσης 54Mbps, χρησιμοποιώντας οκτώ μη επικαλυπτόμενα κανάλια στο εύρος ζώνης των 5GHz, πετυχαίνοντας σχετικά υψηλές δικτυακές ικανότητες, έχοντας τη δυνατότητα χρήσης κυψελωτής αρχιτεκτονικής με ελάχιστες παρεμβολές μεταξύ γειτονικών κυψελών. Λειτουργώντας στην περιοχή των 5GHz που δεν χρήζει αδειοδότησης, πλεονεκτεί στο γεγονός ότι αποφεύγει παρεμβολές από συσκευές που λειτουργούν στα 2.4GHz , όπως φούρνοι μικροκυμάτων, ασύρματα τηλέφωνα και συσκευές Bluetooth.

Μειονέκτημα του είναι η μη συμβατότητά του με το 802.11b, γεγονός όμως που αποβαίνει θετικό στο πρόβλημα των παρεμβολών.

6.1.2 802.11d

Το πρότυπο 802.11d αποτελεί μια παραλλαγή του 802.11b, με το οποίο είναι σχεδόν ταυτόσημα. Ο σκοπός κατοχύρωσής του από τον IEEE, ταυτίζεται με την αναγκαιότητα μικρών διαφοροποιήσεων του προτύπου 802.11b σύμφωνα με τη νομοθεσία και τους περιορισμούς κάθε χώρας. Δηλαδή υλοποιεί στην ουσία το πρότυπο 802.11b με μικρές τροποποιήσεις αναλόγως τη χώρα. Ο λόγος που δεν είναι ευρέως διαδεδομένο είναι ότι οι κατασκευαστές ασύρματου εξοπλισμού αποφεύγουν την παραγωγή προϊόντων με συγκεκριμένες διαφοροποιήσεις, αναλόγως τη χώρα.

6.1.3 802.11g

Έκανε την εμφάνισή του πρόσφατα, στα μέσα του 2003. Συμβατό με το 802.11b, το πρότυπο αυτό παρέχει τη δυνατότητα ρυθμού μετάδοσης θεωρητικά έως 54Mbps , όπως το 802.11a. Λειτουργεί στη μπάντα συχνοτήτων των 2.4GHz χρησιμοποιώντας όμως διαφορετική τεχνολογία RF ώστε να αυξάνει σημαντικά το ρυθμό μετάδοσης. Το υπόστρωμα MAC ενσωματώνει ένα μηχανισμό υποστήριξης διαφορετικών ρυθμών μετάδοσης, επιλέγοντας ανάμεσα στα 1, 2 , 5.5 και 11Mbps του b ανεβαίνοντας έως τα 22 Mbps τουλάχιστον, στην πράξη. Η επιλογή του Bit Rate από το υπόστρωμα MAC , έχει να κάνει με την παρουσία ή όχι στο BSS, συσκευής 802.11b, με την απόσταση μεταξύ των συσκευών, με το ύψος του αριθμού σφαλμάτων μετάδοσης, τυχόν παρεμβολές κλπ. Το πλεονέκτημα της συμβατότητάς του με το προϋπάρχον b, αποτέλεσε το λόγο της άμεσης προώθησής του στην αγορά και όπως προβλέπεται σύντομα θα το αντικαταστήσει.

6.1.4 802.11h (Dynamic Frequency Selection Transmit Power Control)

Ενισχύει το υπόστρωμα MAC και το φυσικό στρώμα του 802.11a που λειτουργεί στα 5GHz με σκοπό να προσθέσει επιπλέον κανάλια για εσωτερικού-εξωτερικού χώρου λειτουργία (indoor-outdoor), τα οποία δεν θα έχουν περιορισμούς αδειοδότησης στην Ευρώπη. Για να το πετύχει αυτό διαθέτει ένα μηχανισμό διαχείρισης της εκπεμπόμενης ισχύος και του χρησιμοποιούμενου φάσματος, ο

οποίος παρακολουθεί και καταγράφει την ισχύ κάθε καναλιού. 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

Δεν έχει ακόμα τυποποιηθεί .

6.1.5 802.11i

Ενισχύει τους μηχανισμούς ασφαλείας και πιστοποίησης (authentication), σε επίπεδο MAC.

Θα προσπαθήσει να αντικαταστήσει το WEP και την υποστήριξή του σε συσκευές, αρχικά με την δημιουργία ανώτερου πρωτοκόλλου ασφαλείας συμβατό με το WEP.

Δεν έχει ακόμα τυποποιηθεί .

6.1.6 802.11e

Η ομάδα αυτή προσανατολίζεται στην εισαγωγή λειτουργιών Quality of Service με εισαγωγή προτεραιοτήτων στα πακέτα των 802.11 δικτύων, για μεταδώσεις που περιλαμβάνουν εφαρμογές audio και video , video conferencing, media stream distribution, υψηλές απαιτήσεις ασφαλείας, κινητή και νομαδική πρόσβαση. Η πραγματοποίηση αυτού του στόχου θα απαιτήσει συνεννόηση μεταξύ σταθμών πελατών και Access Points, αλλά και από τον διαχειριστή του δικτύου.

Με το QoS μπορούν τα πακέτα δεδομένων να κατηγοριοποιούνται και να αποκτούν διαφορετική σειρά προτεραιότητας ανάλογα με το είδος τους. Έτσι, τα πακέτα που αφορούν ένα video π.χ., μπορεί να έχουν μεγαλύτερη προτεραιότητα κατά τη μεταφορά, με αποτέλεσμα την πιο ομαλή εμφάνισή του.

Δεν έχει ακόμα τυποποιηθεί .

6.1.7 802.11x

Στόχος του είναι η ανάπτυξη ενός πρωτοκόλλου Inter-Access Point Protocol (IAPP) το οποίο θα παρέχει τις απαραίτητες δυνατότητες για να επιτευχθεί η διαλειτουργικότητα (συνεργασία) μεταξύ συσκευών διαφόρων κατασκευαστών μέσω ενός Distribution System που θα υποστηρίζει IEEE 802.11Wireless LAN Links.

Δεν έχει ακόμα τυποποιηθεί .

ΚΕΦΑΛΑΙΟ 7^{ο}

7.1 ΑΣΦΑΛΕΙΑ WLAN

Όσο οι συσκευές Wi-Fi εισέβαλλαν σε όλο και περισσότερα δίκτυα, τόσο οι χρήστες τους έβλεπαν πιο σοβαρά το ζήτημα της ασφάλειας των δεδομένων που διακινούσαν μέσω αυτών. Αναρίθμητες μελέτες, τόσο από κοινούς χρήστες, όσο και από την επιστημονική κοινότητα, βοήθησαν στο να ξεσκεπαστούν πολλές θεμελιώδεις ατέλειες στο μοντέλο ασφάλειας του πρωτοκόλλου. Θα προσπαθήσουμε να δώσουμε μια γενική εικόνα της όλης κατάστασης, προτείνοντας τελικά κάποιες λύσεις.

Στο πεδίο των κοινών LAN έχουμε να κάνουμε με τα ίδια προβλήματα ασφάλειας τα οποία παρουσιάζονται στα περιβάλλοντα των συμβατικών LAN. Στην περίπτωσή μας όμως υπάρχουν κάποια ζητήματα ασφάλειας τα οποία βαρύνουν περισσότερο όταν χρησιμοποιούμε την ασύρματη οδό. Τα γνωστότερα τρωτά σημεία είναι τα εξής:

7.1.1 Υποκλοπή

Η υποκλοπή είναι πολύ πιο εύκολη στις ασύρματες τηλεπικοινωνίες. Όταν κάποιος στέλνει ένα μήνυμα, οποιοσδήποτε εφοδιασμένος με ένα δέκτη, στο πεδίο του πομπού, μπορεί να υποκλέψει το μήνυμα. Ο αποστολέας καθώς και ο παραλήπτης του μηνύματος δεν είναι δυνατό να γνωρίζουν αν υπήρξε υποκλοπή ή όχι γι' αυτό η παρεμβολή αυτή είναι απολύτως μη εντοπίσημη. Η ζώνη της συχνότητας και η ισχύς του πομποδέκτη, έχει τεράστια επιρροή στην έκταση της υποκλοπής. Όταν χρησιμοποιούμε συχνότητές των 2 ή των 5MHz και ισχύ πομποδέκτη πάνω από 1W, όπως συμβαίνει στα σύγχρονα LAN, όλη η κίνηση του δικτύου μπορεί να καταγραφεί από κάποιον τρίτο, έξω από το κτίριο στο οποίο λειτουργεί το δίκτυο εφόσον δεν υπάρχει κάποιο ηλεκτρομαγνητικό κέλυφος προστασίας. Έτσι δεν μπορούμε να είμαστε σίγουροι ότι τα δεδομένα του δικτύου μας παραμένουν εντός κτιρίου.

Το γεγονός ότι τα ασύρματα δίκτυα παρακολουθούνται ευκολότερα έχει σαν αποτέλεσμα να σπαταλείται πολύ χρήμα προς την κατεύθυνση της «θωράκισης» των πληροφοριών μας.

7.1.2 Αξιοπιστία μεταφοράς

Όταν ένα μέρος του δικτύου της επιχείρησης είναι ασύρματο, λειτουργεί σαν πύλη για τον επίδοξο υποκλοπέα. Στα συμβατικά δίκτυα μπορούμε να ακολουθήσουμε το καλώδιο από το τερματικό μας ως τον κόμβο του δακτυλίου και να ανακαλύψουμε έτσι με ποιόν επικοινωνούμε. Στα ασύρματα δίκτυα όμως δεν υπάρχει αυτή η δυνατότητα. Έτσι οι μηχανισμοί πιστοποίησης είναι το κρισιμότερο τμήμα της ασφάλειας των δικτύων αυτών. Σε κάθε περίπτωση και τα δύο μέρη της ασύρματης επικοινωνίας θα πρέπει να είναι σε θέση να πιστοποιούν την ταυτότητα του συνομιλητή τους. Τα ασύρματα LAN μπορούν να χρησιμοποιηθούν σαν η βάση για να χτυπηθεί η αξιοπιστία της μεταφοράς. Αν ο επιτιθέμενος ξεγελάσει το ασύρματο δίκτυό μας έτσι ώστε να εμπιστευθεί τον σταθμό τον οποίο αυτός ελέγχει τότε θα έχουμε έναν εχθρικό κόμβο ο οποίος θα έχει περάσει όλα τα firewalls του δικτύου της εταιρίας μας και από εκεί και πέρα θα είναι πολύ δύσκολο να αποφύγουμε εχθρικές δραστηριότητες. Αυτού του είδους η επίθεση μπορεί να γίνει έξω από το δικό μας χώρο με εξοπλισμό συμβατό με τον δικό μας. Ο μόνος τρόπος αποφυγής

τέτοιων φαινομένων είναι ένας πραγματικά ισχυρός μηχανισμός πιστοποίησης αυτών που συναλλάσσονται με το δίκτυο. Ο προσδιορισμός των επιθέσεων θα πρέπει να βασιστεί στις ανεπιτυχείς προσπάθειες σύνδεσης στο δίκτυο, αν και στην πραγματικότητα είναι πολύ δύσκολο να διαπιστωθεί αν υπήρξε εξωτερική επίθεση λόγο του γεγονότος ότι και υπό κανονικές συνθήκες υπάρχουν παρεμβολές στο δίκτυο εξ' αιτίας του υψηλού BER της συχνότητας αλλά και άλλων παρεμβολών από σταθμούς που ανήκουν σε άλλα ασύρματα δίκτυα.

Ένα άλλο είδος επίθεσης, ειδικά στα ασύρματα δίκτυα, είναι να ξεγελαστούν οι σταθμοί ώστε να εμπιστευθούν μια βάση η οποία δεν ανήκει στο συγκεκριμένο δίκτυο και ελέγχετε βεβαίως από αυτόν που προσπαθεί να εισβάλει στο δίκτυο.

7.1.3 Υποδομή

Οι επιθέσεις στην υποδομή βασίζονται σε κάποιες αδυναμίες του συστήματος, τα λάθη στο λογισμικό, ανεπάρκεια του υλικού κ.α. Αυτού του είδους τα φαινόμενα απαντώνται και στα ασύρματα δίκτυα επίσης. Η προστασία όμως ενάντια στις επιθέσεις αυτού του είδους είναι σχεδόν αδύνατη. Δυστυχώς μαθαίνεις την αδυναμία του συστήματος όταν πια εκδηλωθεί το πρόβλημα. Το μόνο λοιπόν που μπορούμε να κάνουμε είναι να προσπαθούμε να μειώσουμε τις επιπτώσεις των προβλημάτων που θα εμφανιστούν αργά ή γρήγορα.

7.1.4 Άρνηση εξυπηρέτησης

Η ασύρματη τηλεπικοινωνία από τη φύση της είναι περισσότερο ευάλωτη, για το λόγο αυτό τα ασύρματα δίκτυα είναι πιο τρωτά σε επιθέσεις που σχετίζονται με την άρνηση εξυπηρέτησης. Αν ο «εχθρός» έχει αρκετά ισχυρό πομποδέκτη μπορεί να δημιουργήσει μια τέτοια παρεμβολή που να εμποδίζει την ομαλή λειτουργία του δικτύου. Αυτού του είδους η επίθεση μπορεί για παράδειγμα να γίνει είτε από ένα βάν παρκαρισμένο έξω από το κτίριό είτε από ένα απλό διαμέρισμα λίγα μέτρα μακρύτερα. Ο εξοπλισμός που απαιτείται γι' αυτού του είδους την επίθεση είναι αρκετά προσιτός, μπορεί να αγοραστεί από οποιοδήποτε κατάστημα ηλεκτρονικών ειδών σε αρκετά χαμηλές τιμές και δεν χρειάζεται ιδιαίτερες γνώσεις για τον χειρισμό του.

Αντιθέτως η προστασία από αυτού του είδους την δολιοφθορά, είναι δύσκολα κατορθωτή και οικονομικά απρόσιτη. Η μόνη αξιόπιστη λύση είναι να βρίσκεται το ασύρματο δίκτυό συνεχώς υπό την σκέπη ενός αόρατου κλουβιού αλλά αυτό είναι δυνατό σε πολύ λίγες περιπτώσεις. Το θετικό στην όλη υπόθεση είναι ότι είναι σχετικά εύκολο για τις αρχές να εντοπίσουν από που προέρχεται η παρεμβολή, έτσι ο «εχθρός» έχει περιορισμένο χρόνο στη διάθεσή του μέχρις ότου εντοπιστεί. Από την άλλη μεριά τα ασύρματα δίκτυα δεν είναι τόσο ευάλωτα σε άλλου είδους επεμβάσεις οι οποίες απαντώνται κυρίως στα συμβατικά δίκτυα. Για παράδειγμα ένας σταθερός κόμβος ενός LAN μπορεί εύκολα να απομονωθεί από το υπόλοιπο δίκτυο με ένα απλό κόψιμο του καλωδίου, πράγμα που δε μπορεί να γίνει σε ασύρματο περιβάλλον. Επίσης σε περιπτώσεις διακοπής ρεύματος τα συμβατικά δίκτυα είναι εντελώς άχρηστα, τα ασύρματα όμως δίκτυα είναι σε θέση να λειτουργήσουν με lap-top ή με άλλου είδους τερματικά που λειτουργούν με επαναφορτιζόμενες μπαταρίες.

7.2 ΜΕΘΟΔΟΙ ΑΣΦΑΛΕΙΑΣ ΤΟΥ 802.11

Τρεις γνωστές μέθοδοι εφαρμόζονται στο 802.11 για να εξασφαλισθεί η πρόσβαση σε ένα AP . Αυτές οι βασικές μέθοδοι είναι ευρέως διαθέσιμες και είναι ικανοποιητικές:

- Service set identifier (SSID)
- Media Access Control (MAC) address filtering
- Wired Equivalent Privacy (WEP)

Η κάθε μια μπορεί να εφαρμοστεί ξεχωριστά αλλά ο συνδυασμός και των τριών μαζί, παρέχει μια πιο ολοκληρωμένη και ασφαλή λύση .
Παρακάτω θα προσπαθήσουμε να αναλύσουμε τις τρεις αυτές μεθόδους.

7.2.1 SSID (Service set identifier)

Ο έλεγχος πρόσβασης στο δίκτυο μπορεί να εφαρμοσθεί χρησιμοποιώντας το SSID ενός AP ή περισσότερων. Μέσω της ταυτοποίησης SSID παρέχεται η δυνατότητα τμηματοποίησης (segment) ενός ασύρματου δικτύου ή περισσοτέρων που χρησιμοποιούν ένα ή περισσότερα APs. Κάθε AP είναι προγραμματισμένο με ένα SSID αντιστοίχως σε ένα συγκεκριμένο ασύρματο δίκτυο. Για να έχουν πρόσβαση σε αυτό το δίκτυο, οι χρήστες πρέπει να συμμορφωθούν με το σωστό SSID. Ένα κτήριο μιας επιχείρησης μπορεί να τμηματοποιηθεί σε περισσότερα δίκτυα, ανά όροφο ή τμήμα. Χαρακτηριστικά, ένας χρήστης μπορεί να έχει πολλαπλά SSIDs όταν απαιτεί πρόσβαση στο δίκτυο από ποικίλες διαφορετικές θέσεις.

Επειδή ένας χρήστης πρέπει να παρουσιάσει το σωστό SSID για να έχει πρόσβαση στο AP, η χρήση του SSID ως απλού κωδικού πρόσβασης παρέχει ένα μέτρο ασφάλειας. Εντούτοις, αυτή η ελάχιστη ασφάλεια υποχωρεί εάν το AP εκπέμπει "broadcast" το SSID του. Όταν αυτό το χαρακτηριστικό γνώρισμα broadcast επιτρέπεται, οποιοσδήποτε χρήστης που δεν κατέχει ένα συγκεκριμένο SSID λαμβάνει το SSID και έχει πρόσβαση στο AP. Επιπλέον, επειδή οι χρήστες αποθηκεύουν στα συστήματά τους το SSID τους, μπορεί να γίνει γνωστό και κατά συνέπεια, εύκολα προσβάσιμο.

7.2.2 MAC Address Filtering

Ενώ ένα AP ή μια ομάδα APs μπορεί να προσδιοριστεί από ένα SSID, ένας υπολογιστής ή οποιαδήποτε δικτυακή συσκευή ενός χρήστη μπορεί να προσδιοριστεί από τη μοναδική διεύθυνση της MAC 802.11 κάρτας δικτύου του. Η MAC διεύθυνση είναι ένας μοναδικός δεκαεξαδικός αριθμός, που είναι «γραμμένος» στο υλικό κάθε δικτυακής συσκευής. Για να αυξήσει την ασφάλεια ενός 802.11 δικτύου, κάθε AP μπορεί να προγραμματιστεί με έναν κατάλογο διευθύνσεων των MAC Addresses των υπολογιστών των χρηστών και των δικτυακών συσκευών γενικότερα, που έχουν άδεια πρόσβασης στο AP. Εάν ενός χρήστη η διεύθυνση της MAC δεν συμπεριλαμβάνεται σε αυτόν τον κατάλογο, ο χρήστης δεν έχει την άδεια να συνδεθεί με το AP.

Η διεύθυνση της MAC που φιλτράρεται (μαζί με τα SSIDs), παρέχει βελτιωμένη ασφάλεια, αλλά είναι καταλληλότερη στα μικρά δίκτυα όπου ο κατάλογος αποδεκτών της MAC μπορεί να ρυθμιστεί αποτελεσματικά.

Κάθε AP πρέπει να προγραμματιστεί χειροκίνητα (manually) με έναν κατάλογο διευθύνσεων των MAC, και ο κατάλογος πρέπει να ενημερώνεται. Στην πράξη, ο αριθμός διευθύνσεων των MAC που φιλτράρονται είναι πιθανό να είναι

λιγότερο από 255 χρήστες. Επιπλέον, οι διευθύνσεις MAC μπορούν να αλλοιωθούν και να εξαπατηθούν από έναν άλλο χρήστη για να κερδίσει την αναρμόδια πρόσβαση στο δίκτυο.

Κάποιος εκτός λίστας, με αρκετά δικαιώματα σε ένα unix-like λειτουργικό σύστημα, μπορεί με διάφορους τρόπους να αλλάξει την MAC διεύθυνση που παρουσιάζει στο δίκτυο, έτσι ώστε να μπορέσει να χρησιμοποιήσει μια MAC που να είναι αποδεκτή από το AP. Τέτοιες επιθέσεις ονομάζονται mac spoofing attacks. Χρησιμοποιώντας εξειδικευμένο «ανιχνευτικό» λογισμικό (network sniffer), που πολλές φορές είναι δωρεάν, μπορεί με μια απλή WiFi κάρτα και ένα laptop να φτιάξει μια λίστα με τις MAC διευθύνσεις που βλέπει ότι συνδέονται επιτυχώς στο Access Point-στόχο. Έτσι, αλλάζοντας την MAC διεύθυνσή του σε οποιαδήποτε από αυτές, έχει την δυνατότητα να συνδεθεί επιτυχώς στο δίκτυο, χωρίς κανείς να μπορεί να καταλάβει την διαφορά.

7.2.3 WEP - Based Security

Η κρυπτογράφηση (encryption) και Authentication (ταυτοποίηση) είναι ένα από τα πρώτιστα ζητήματα που εξετάζονται όταν αναπτύσσεται ένα ασύρματο δίκτυο. Ο στόχος της προσθήκης αυτών των γνωρισμάτων ασφαλείας είναι να γίνει η μεταφορά και η λήψη δεδομένων σε ένα ασύρματο δίκτυο, τόσο ασφαλής όσο και σε ένα ενσύρματο δίκτυο.

Τα 802.11 b,g κ.λ.π, πρότυπα του IEEE για να πετύχουν αυτό το στόχο παρέχουν ένα μηχανισμό που κρυπτογραφεί την κυκλοφορία και επικυρώνει τους κόμβους μέσω του Wired Equivalent Privacy (WEP) protocol.

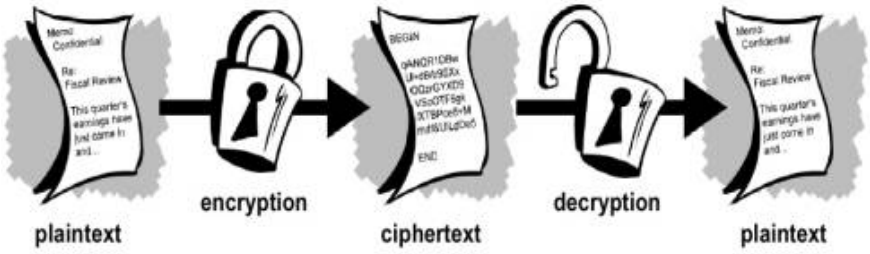
Η επιτροπή IEEE, για λόγους ασφάλειας και πιστοποίησης (authentication) χρηστών, όρισε το WEP (wired equivalent privacy), με σκοπό την ενθυλάκωση των πακέτων των δεδομένων για την επίτευξη ασφάλειας παρόμοιας με ένα ενσύρματο δίκτυο.

Η υλοποίηση του WEP σε εμπορικές συσκευές άργησε να υποστηριχτεί από όλους τους κατασκευαστές. Το WEP ήταν η πρώτη σοβαρή προσπάθεια υπέρ της αύξησης της ασύρματης ασφάλειας. Δυστυχώς, ο σχεδιασμός του προτύπου, συνέπεσε χρονικά με την τάση της κυβέρνησης των ΗΠΑ κατά της δημόσιας χρήσης συστημάτων ισχυρής κρυπτογράφησης, που σημαίνει μεγάλο μήκος κλειδιού. Έτσι το μήκος κλειδιού που υποστηρίζει το WEP, περιορίστηκε στα 40 ψηφία. Επιπλέον, ένα τέτοιο μήκος κλειδιού θα καθιστούσε το WEP ευκολότερο να υλοποιηθεί, καθώς η κατασκευή των MAC πλαισίων από το τότε υλικό ήταν ήδη μια διαδικασία που απαιτούσε μεγάλη υπολογιστική ισχύ, πόσο μάλλον η ενθυλάκωση τους με WEP. Η εισαγωγή μιας δυνατής κρυπτογράφησης θα επιβάρυνε ακόμη περισσότερο τις επιδόσεις των συσκευών. Καθώς όλοι είχαν πλέον καταλάβει ποσό τρωτό είναι ένα ανοιχτό δίκτυο, βιάστηκαν να υιοθετήσουν το πρότυπο αυτό.

7.3 ΚΡΥΠΤΟΓΡΑΦΙΑ, ΓΕΝΙΚΑ:

Η κρυπτογραφία (**encryption**) είναι 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**).

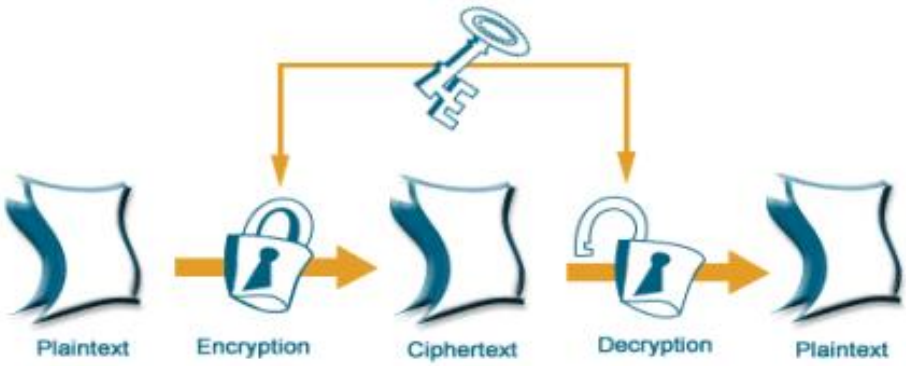


Σχήμα 51: Κρυπτογράφηση απλού κειμένου

Αποκρυπτογράφηση (**decryption**) 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 αυτή μπορούν να ανακτήσουν το περιεχόμενο του αρχικού μηνύματος.

Ο αλγόριθμος κρυπτογράφησης είναι μια μαθηματική συνάρτηση που χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση πληροφοριών. Όσο αυξάνει ο βαθμός πολυπλοκότητας του αλγορίθμου, τόσο μειώνεται η πιθανότητα να τον διαβάλλει 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.

Στη συμμετρική κρυπτογραφία, χρησιμοποιείται το ίδιο κλειδί τόσο για την κρυπτογράφηση, όσο και για την αποκρυπτογράφηση. Επομένως, το κλειδί αυτό πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη και, άρα, απαιτείται ασφαλές μέσο για τη μετάδοσή του, για παράδειγμα μία προσωπική συνάντηση κατά την οποία θα συμφωνηθεί το κλειδί που θα χρησιμοποιείται. Αν κάτι τέτοιο δεν είναι εφικτό, η συμμετρική κρυπτογραφία είναι αναποτελεσματική.

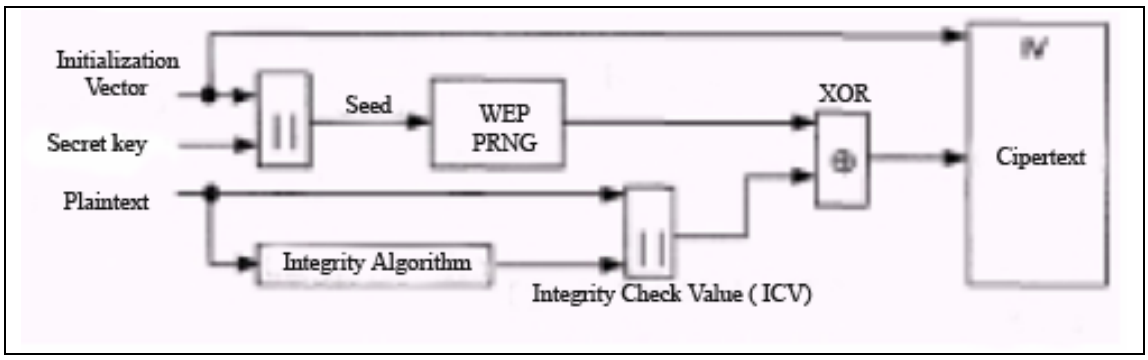


Σχήμα 52: Συμμετρική Κρυπτογραφία με shared key

7.4 ΤΟ ΠΡΩΤΟΚΟΛΛΟ WEP ΤΟΥ 802.11

Το πρωτόκολλο WEP επιλέχθηκε με τα ακόλουθα κριτήρια:
• **Reasonably strong**. Να ικανοποιεί τις ανάγκες του χρήστη.
• **Αυτοσυγχρονιζόμενο**.
• **Computationally efficient**. Ο αλγόριθμος WEP μπορεί να εφαρμοστεί με hardware ή software. Εξαρτάται από τις απαιτήσεις της εφαρμογής
• **Optional**. Είναι μια επιλογή που δεν απαιτεί σύστημα συμβατό με το 802.11

Χρησιμοποιείται το ίδιο κλειδί για κωδικοποίηση και αποκωδικοποίηση των δεδομένων. Ο αλγόριθμος κρυπτογράφησης του WEP λειτουργεί ως εξής:



Σχήμα 53: WEP, encryption

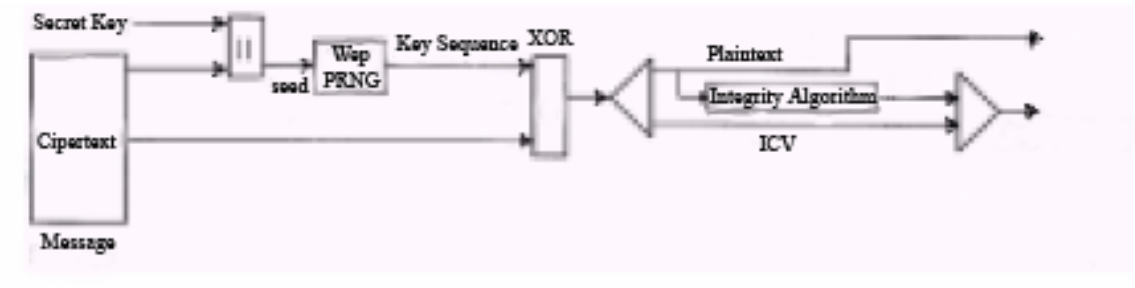
Δυο διαδικασίες εφαρμόζονται στο plaintext. Η μια κρυπτογραφεί τα δεδομένα και η άλλη προστατεύει ενάντια στην όποια αναρμόδια τροποποίηση.

Το μυστικό key (40-bits) συνδέεται αλυσιδωτά με διάνυσμα αρχικοποίησης IV (Initialization Vector, 24-bits) με αποτέλεσμα ένα 64-bit key. Το δημιουργούμενο key τοποθετείται σε μια ψευδοτυχαία γεννήτρια αριθμών (PRNG). Η PRNG (RC4) δίνει μια ψευδοτυχαία ακολουθία βασισμένη στο αρχικά εισερχόμενο key. Η απορρέων ακολουθία χρησιμοποιείται στην κρυπτογράφηση (encrypt) των data δια μέσω μιας XOR. Αυτό έχει ως αποτέλεσμα την κρυπτογράφηση μιας ακολουθίας bytes ίσου μήκους ως προς τον αριθμό των bytes των δεδομένων που πρέπει να μεταδοθούν.

Για να προστατευθεί ενάντια στην αναρμόδια τροποποίηση στοιχείων ένας αλγόριθμος ακεραιότητας CRC-32 λειτουργεί στο plaintext και παράγει το ICV. Το κρυπτογράφημα ολοκληρώνεται ως εξής.

- Υπολογίζεται το ICV χρησιμοποιώντας CRC-32 στο message plaintext
- Συνδέει το ICV στο plaintext.
- Επιλέγει ένα τυχαίο IV και το συνδέει στο secret key
- Εισάγει το secret key και το IV στο RC4 για να παραχθεί μια ψευδοτυχαία key sequence.
- Κρυπτογραφεί το plaintext+ICV μέσω μιας XOR με μια ψευδοτυχαία key sequence μέσω του RC4 για να γίνει η κρυπτογράφηση.
- Στέλνει το IV στον παραλήπτη τοποθετώντας το στην αρχή του ciphertext.

Το IV, το plaintext, και το ICV αποτελούν τα δεδομένα του πλαισίου δεδομένων (data frame)που αποστέλλεται .

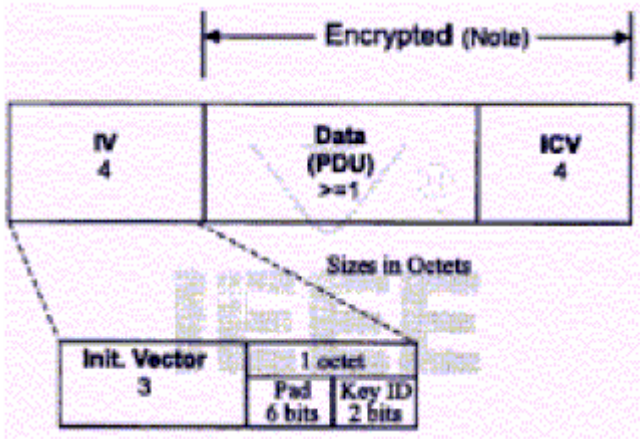


Σχήμα 54: WEP decryption

Στην αποκωδικοποίηση το IV του εισερχόμενου μηνύματος χρησιμοποιείται για να δημιουργήσει την key sequence απαραίτητη για την αποκρυπτογράφηση του εισερχόμενου μηνύματος.

Συνδυάζοντας το ciphertext (κρυπτογράφημα) με το Proper key, αποδίδεται το πρωτότυπο plaintext και ICV. Η αποκρυπτογράφηση ελέγχεται από την εκτέλεση του ελέγχου ακεραιότητας του αλγόριθμου στο επικαλυμμένο plaintext και συγκρίνει το εξερχόμενο ICV με το ICV που μεταφέρεται με το μήνυμα. Αν δεν είναι ίσα, το λαμβανόμενο μήνυμα είναι λανθασμένο και στέλνεται μια αναφορά του σφάλματος στο MAC Management και πίσω στον αποστέλον σταθμό. Κινητές μονάδες με λανθασμένα μηνύματα δεν πιστοποιούνται

Το ίδιο shared key χρησιμοποιείται για encrypt/decrypt. Τα data frames επίσης χρησιμοποιούνται για πιστοποιήσουν το station.



Σχήμα 55: WEP data frames

7.4.1 Authentication

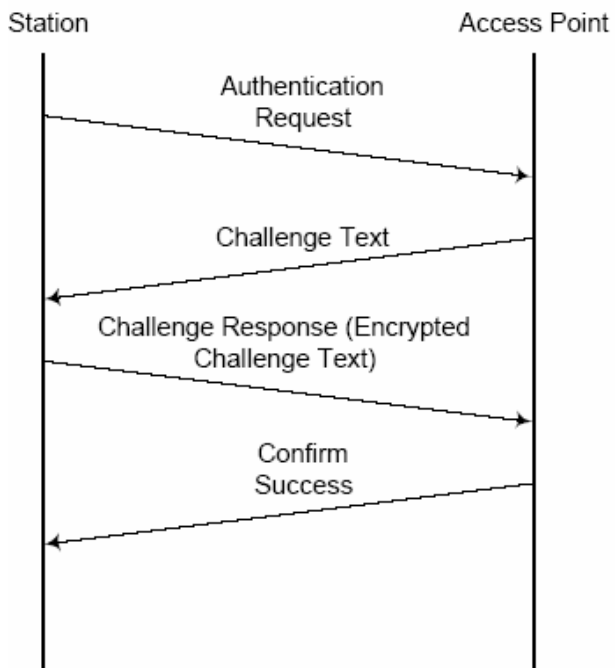
Υπάρχουν δυο τύποι Authentication στο 802.11:

- Open system authentication. Αυτή είναι η προεπιλεγμένη κατάσταση λειτουργίας ενός συστήματος που δε χρησιμοποιεί Authentication

- Shared key authentication: Όπου χρησιμοποιείται ένα shared secret key για να πιστοποιεί τον σταθμό στο AP.

Το *Open system authentication* σημαίνει ότι σταθμός μπορεί να συνδεθεί με οποιοδήποτε AP και να ακούσει όλα τα data που στέλνει. Αυτό συνήθως υλοποιείται όταν το ζητούμενο είναι η ευκολία χρήσης του δικτύου και ο network administrator δε θέλει να ασχολείται καθόλου με την ασφάλεια .

Η *shared key authentication* προσέγγιση, εξασφαλίζει ένα καλύτερο βαθμό authentication απ' ότι η προσέγγιση του Open system . Ένας σταθμός που χρησιμοποιεί shared key authentication πρέπει να εφαρμόζει WEP. Η παρακάτω εικόνα διευκρινίζει το χειρισμό του shared key authentication:



Σχήμα 56: shared key authentication

Ο καθορισμός και η τροποποίηση του secret shared key που χρησιμοποιεί κάθε σταθμός MIB, είναι διαθέσιμα μόνο στο MAC coordinator (συντονιστή). Το πρότυπο 802.11 δεν καθορίζει πως θα διανέμονται τα keys σε κάθε station.

Η διαδικασία είναι η ακόλουθη:

1. Ο αιτών σταθμός στέλνει ένα Authentication frame στο AP.
2. Όταν το AP λάβει ένα Authentication frame τότε αποκρίνεται με ένα άλλο Authentication frame που περιλαμβάνει 128 bytes random challenge text δημιουργούμενο από το WEP σε μια πρότυπη φόρμα.
3. Ο αιτών σταθμός τότε θα αντιγράψει το challenge text σε ένα Authentication frame, κρυπτογραφημένο με ένα shared key και τότε στέλνει το frame στο ανταποκριτή σταθμό.
4. Ο παραλήπτης AP θα αποκωδικοποιήσει την τιμή του challenge text χρησιμοποιώντας το ίδιο shared key και συγκρίνοντάς το με το challenge text που έστειλε νωρίτερα. Αν ταιριάζει ο ανταποκριτής station θα απαντήσει με Authentication. Αν όχι ο ανταποκριτής σταθμός θα στείλει αρνητική Authentication.

Η WEP PRNG (RC4) είναι καθοριστική συνιστώσα της WEP διαδικασίας, δεδομένου ότι είναι η χρησιμοποιούμενη μηχανή κρυπτογράφησης.

Το IV επεκτείνει το χρήσιμο χρόνο ζωής του shared key και παρέχει τη δυνατότητα αυτό-συγχρονισμού του αλγόριθμου.

Το Secret key παραμένει σταθερό όσο το IV αλλάζει περιοδικά. Ένα νέο IV αποτέλεσμα σε κάθε νέο key sequence, έτσι υπάρχει μια προς μια ανταποκρίσεις

μεταξύ του IV και του output. Το IV μπορεί να αλλάζει τόσο συχνά όσο και κάθε μήνυμα και από τη στιγμή που μεταδίδεται μαζί με το μήνυμα, ο παραλήπτης μπορεί πάντα να αποκρυπτογραφεί κάθε μήνυμα.

Ένας υποκλοπέας (eavesdropper) μπορεί αμέσως να προσδιορίσει τμήματα της βασικής ακολουθίας (key sequence) δημιουργούμενη από τη μηχανή κρυπτογράφησης Key, IV αν το ίδιο ζεύγος (Key, IV) χρησιμοποιείται για διαδοχικά μηνύματα . Τότε ο βαθμός της Privacy μειώνεται. Αλλάζοντας το IV μετά από κάθε μήνυμα μπορεί εύκολα να εξασφαλισθεί η αποτελεσματικότητα του WEP.

7.4.2 RC4

Η RC4 αναπτύχθηκε το 1987 από τον Ron Rivest για την RSA Data Security. Η RC4 είναι μια stream cipher που παίρνει ένα οποιουδήποτε μήκους Key και παράγει μια σειρά ψευδοτυχαίων bits τα οποία μαζί με το plaintext, δια μέσου μιας XOR, παράγουν το cipher text και το αντίστροφο.

Η RC4 είναι διαδεδομένη στο SSL Internet Protocol και σε πολλά άλλα κρυπτογραφικά προϊόντα. Τα προνόμια της χρήσης της RC4 είναι τα ακόλουθα:

.

- Η keystream είναι ανεξάρτητη του plaintext
- Η κωδικοποίηση και αποκωδικοποίηση είναι γρήγορη, περίπου 10 φορές γρηγορότερη από τη DES.
- Η RC4 είναι η πιο εύκολη για τους προγραμματιστές και μπορούν εύκολα να την περάσουν στο λογισμικό.
- Η RSADSI αξιώνει ότι η RC4 αμύνεται σε διαφορικές και γραμμικές cryptoanalysis.

7.4.3 Δίκτυα με υψηλές απαιτήσεις ασφάλειας

Για τα δίκτυα με υψηλές απαιτήσεις ασφάλειας, το VPN ή οι βασισμένες στο πρότυπο 802.11i λύσεις προτιμούνται. Αυτές οι λύσεις είναι επίσης προτιμητέες για τα μεγάλα δίκτυα, στα οποία το διοικητικό φορτίο της διατήρησης των διευθύνσεων της MAC σε κάθε AP καθιστά αυτήν την προσέγγιση μη πρακτική.

Το σημείο στο οποίο ο αριθμός ασύρματων χρηστών γίνεται ανεξέλεγκτος ποικίλλει ανάλογα με τη δυνατότητα της οργάνωσης να διαχειριστεί το δίκτυο, την επιλογή των μεθόδων ασφάλειας (SSID, WEP, και της MAC address filtering), και την ανοχή του για τον κίνδυνο. Εάν το MAC address filtering χρησιμοποιείται σε ένα ασύρματο δίκτυο, το σταθερό ανώτερο όριο καθιερώνεται από το μέγιστο αριθμό διευθύνσεων της MAC που μπορεί να προγραμματιστεί σε κάθε AP που χρησιμοποιείται σε μια εγκατάσταση. Αυτό το ανώτερο όριο ποικίλλει, αλλά το πρακτικό πρόβλημα της χειροκίνητης καταχώρησης και τις έγκυρες διευθύνσεις της MAC σε κάθε AP σε ένα δίκτυο περιορίζει τη χρήση του MAC address filtering στα μικρότερα δίκτυα.

7.4.4 Ασύρματη ασφάλεια με χρήση της τεχνικής VPN (Virtual Privet Network)

Οι λύση που παρέχει το VPN αναπτύσσεται ευρέως για να παρέχει στους απομακρυσμένους χρήστες την ασφαλή πρόσβαση σε ένα δίκτυο μέσω του Internet.

Σε αυτήν την απομακρυσμένη πρόσβαση, το VPN παρέχει ένα ασφαλές, «μονοπάτι» κατά τη χρήση ενός αναξιόπιστου δίκτυο —σε αυτήν την περίπτωση, του Διαδικτύου. Διάφορα πρωτόκολλα, συμπεριλαμβανομένου του Point-to-Point Tunneling Protocol (PPTP) και του Layer 2 Tunneling Protocol (L2TP), χρησιμοποιούνται από κοινού με τις πρότυπες, λύσεις πιστοποίησης ταυτότητας.

Η ίδια τεχνολογία VPN μπορεί επίσης να χρησιμοποιηθεί για την ασφαλή ασύρματη πρόσβαση. Σε αυτό το σενάριο, το "untrusted" δίκτυο είναι το ασύρματο δίκτυο. Τα APs διαμορφώνονται για την ανοικτή πρόσβαση χωρίς την κρυπτογράφηση WEP, αλλά η ασύρματη πρόσβαση απομονώνεται από το δίκτυο από τον κεντρικό υπολογιστή VPN. Το APs μπορεί να συνδεθεί μέσω του εικονικού τοπικού LAN (VLAN) 1 ή του τοπικού LAN που επεκτείνονται στην αποστρατικοποιημένη ζώνη (DMZ) 2 και συνδέονται με τον κεντρικό υπολογιστή VPN. (Το APs πρέπει ακόμα να διαμορφωθεί στον κλειστό τρόπο με SSIDs για την κατάτμηση δικτύων.) Η πιστοποίηση ταυτότητας και η πλήρης κρυπτογράφηση πέρα από το ασύρματο δίκτυο παρέχονται μέσω των κεντρικών υπολογιστών VPN που ενεργούν επίσης ως αντιπυρικές ζώνες/πύλες στο εσωτερικό ιδιωτικό δίκτυο. Αντίθετα από τις προσεγγίσεις φιλτραρίσματος διευθύνσεων πλήκτρων WEP και της MAC, η VPN λύση είναι εξελικτική σε έναν πολύ μεγάλο αριθμό χρηστών.

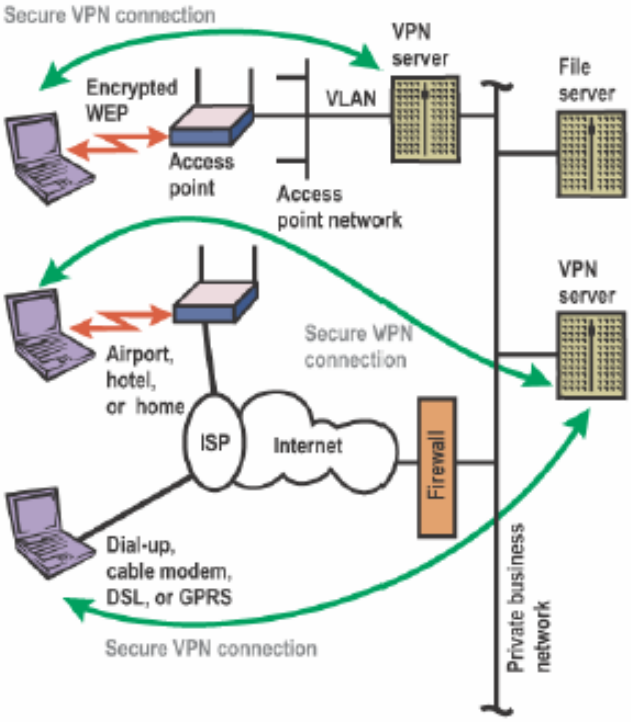


Figure 2. 802.11 VPN Wireless Security

Σχήμα 57: Ασφάλεια VPN του 802.11

Οι απομακρυσμένοι χρήστες μπορούν να χρησιμοποιήσουν μια από τις επιλογές, Digital Subscriber Line (DSL) ή κυψελοειδή στοιχεία (όπως General Packet Radio Service [GPRS]) η σύνδεση στο Διαδίκτυο και εγκαθιστά έπειτα μια σύνδεση VPN στο ιδιωτικό δίκτυο.

Η προσέγγιση VPN έχει διάφορα πλεονεκτήματα:

- Η χρησιμοποίησή του σε πολλά επιχειρηματικά δίκτυα, ήδη.
- Εξελικτικό σε έναν μεγάλο αριθμό 802.11 χρηστών.

• Χαμηλές απαιτήσεις διοίκησης για 802.11 APs και χρήστες. Οι κεντρικοί υπολογιστές VPN μπορούν να αντιμετωπιστούν κεντρικά.
• Η κυκλοφορία στο εσωτερικό δίκτυο είναι απομονωμένη έως ότου εκτελείται η πιστοποίηση ταυτότητας VPN.
• Το WEP και η διαχείριση καταλόγων αποδεκτών της MAC δεν απαιτούνται λόγω των μέτρων ασφάλειας που δημιουργούνται από το ίδιο το VPN κανάλι.
• Εξετάζει τη γενική εξ' αποστάσεως πρόσβαση με ένα συνεπές ενδιάμεσο με τον χρήστη στις διαφορετικές θέσεις όπως στο σπίτι, ση εργασία, και σε έναν αερολιμένα.
Ένα μειονέκτημα στις παρούσες λύσεις VPN είναι η έλλειψη υποστήριξης για multicasting, το οποίο είναι μια τεχνική που χρησιμοποιείται για να παραδώσει τα στοιχεία αποτελεσματικά στον πραγματικό χρόνο από μια πηγή σε πολλούς χρήστες πέρα από ένα δίκτυο. Το Multicasting είναι χρήσιμο για τις ηχητικές και τηλεοπτικές εφαρμογές ροής όπως οι συνεντεύξεις τύπου και οι κλάσεις κατάρτισης.

7.5 ΑΔΥΝΑΜΙΕΣ – ΤΡΩΤΑ ΣΗΜΕΙΑ

Δύο επιστημονικές εργασίες , από ομάδες του πανεπιστημίου του Berkeley και του Maryland, έμελλαν να ταράξουν τα νερά για το πρότυπο, και να καταστήσουν εμφανή τα τρωτά του σημεία. Η εργασία της ομάδας του Berkeley καταδεικνύει τις αδυναμίες του προτύπου λόγω της συνεχούς επαναχρησιμοποίησης κλειδιών, ενώ η εργασία του Maryland θίγει της αδυναμίες στους μηχανισμούς πρόσβασης, ακόμη και αυτούς που λειτουργούν με βάση το WEP. Άλλες εργασίες που ακολούθησαν πρότειναν τρόπους για την τοποθέτηση πλαστών πακέτων στην κίνηση του δικτύου, με αποκορύφωμα το άρθρο ενός μέλους της ομάδας 802.11 που μιλούσε για το WEP σαν «ανασφαλές για οποιοδήποτε μήκος κλειδιού» («WEP: unsafe at any key length»).

Όλες οι προηγούμενες εργασίες βασίζονταν σε σχεδιαστικές ατέλειες του προτύπου για να προτείνουν την ύπαρξη κενών ασφάλειας. Ο ίδιος ο αλγόριθμος κρυπτογράφησης(RC4 της RCA), παρόλα αυτά, θεωρούνταν επαρκής και δεν είχε δεχθεί αμφισβήτηση. Τότε οι Scott Fluhrer, Itsik Mantin, και Adi Shamir, ανακάλυψαν ένα ελάττωμα του αλγόριθμου χρονοδρομολόγησης κλειδιών που καθιστούσε κάποια κλειδιά «αδύναμα». Ένας εισβολέας, θα μπορούσε να βρει το μυστικό κλειδί WEP, απλά συλλέγοντας αρκετά αδύναμα κλειδιά. Δεν δημοσίευσαν ωστόσο κάποια υλοποίηση των ευρημάτων τους. Δυστυχώς ή ευτυχώς, ακολούθησαν πολλοί που το έκαναν. Πάμπολλα προγράμματα ανοιχτού λογισμικού, όπως το AirSnort έχουν την δυνατότητα να σπάσουν την κρυπτογράφηση WEP σε δευτερόλεπτα, δεδομένης μιας συλλογής αδύναμων κλειδιών του δικτύου – στόχος.

Η πραγματικότητα είναι ακόμη πιο οδυνηρή. Πολλές έρευνες σε περιοχές με μεγάλη πυκνότητα Wi-Fi δικτύων έχουν δείξει ότι μόνο ένα πολύ μικρό ποσοστό Access Points που ανιχνεύτηκαν, έχουν πράγματι το WEP ενεργοποιημένο.

Το μεγαλύτερο ποσοστό των εταιρικών δικτύων, είναι ορθάνοιχτο σε «επισκέπτες». Μάλιστα η μη νόμιμη πρόσβαση σε ασύρματα δίκτυα είναι τόσο εκτεταμένη, που υπάρχουν web sites στα οποία συγκεντρώνονται οι συντεταγμένες ανοιχτών εταιρικών και μη δικτύων (για παράδειγμα συντεταγμένες μητροπολιτικών δικτύων, που δημιουργήθηκαν σε πολλές Ελληνικές πόλεις τον τελευταίο καιρό). Τέτοιες ομάδες χρηστών χρησιμοποιούν προγράμματα όπως το netstumbler για να ανακαλύπτουν όλα τα ασύρματα δίκτυα εντός της εμβέλειας της κεραίας του φορητού τους υπολογιστή, αλλά και να βλέπουν χρήσιμες πληροφορίες όπως το SSID του Access Point, αν έχει ενεργοποιημένο το WEP, αλλά και την ποιότητα της εκπομπής της κεραίας – στόχου. Μια βόλτα με αυτοκίνητο στους εμπορικούς δρόμους της Νέας

Υόρκης, έχοντας ένα φορητό υπολογιστή, μια φτηνή Wi-Fi κάρτα και μια ακόμα φθηνότερη κεραία, μπορεί να αποδείξει την ύπαρξη τρυπών στα περισσότερα ασύρματα εταιρικά δίκτυα. Πολλοί έχουν αναγάγει την δραστηριότητα αυτή σε «σπορ», εν ονόματι wardriving, επωφελούμενοι κυρίως από την δωρεάν broadband σύνδεση στο διαδίκτυο που μπορεί να «προσφέρει» ένα απροστάτευτο δίκτυο.

Αυτό το είδος επίθεσης είναι μόνο μία από τις μεθόδους πρόκλησης κατάρρευσης σε ένα ασύρματο δίκτυο. Ένας αρκετά έξυπνος και δύσκολα αντιμετωπίσιμος τρόπος επίθεσης, είναι η ηθελημένη εκπομπή ψευδών πακέτων «αποσύνδεσης χρήστη»(disassociation/deauthentication packets) προς το Access Point. Εφόσον ο εισβολέας συλλέξει τις MAC διευθύνσεις των σταθμών πελατών μιας κυψέλης, μπορεί να απλά να στείλει πολλά πακέτα αποσύνδεσης για κάθε μια MAC-πελάτη. Το AP απλά δεν θα καταλάβει ότι τα πακέτα αυτά είναι κακόβουλα, και θα αποσυνδέσει όσους σταθμούς του ζητηθούν, προκαλώντας έτσι την κατάρρευση του δικτύου.

Όλα τα παραπάνω συνηγορούν ότι η προτυποποίηση της ασύρματης ασφάλειας, είναι μια εργασία σε εξέλιξη. Νέα πρότυπα μελετούνται, όπως το 802.11i, που υπόσχονται μια καλύτερη λύση από το WEP. Πολλοί χρησιμοποιούν λύσεις λογισμικού που κρυπτογραφούν την κίνηση δεδομένων σε υψηλότερο δικτυακό επίπεδο, όπως το IPsec, το ssl κτλ.

ΚΕΦΑΛΑΙΟ 8^{ο}

8.1 ΔΟΜΙΚΑ ΣΤΟΙΧΕΙΑ WLAN

Ένα ασύρματο τοπικό δίκτυο αποτελείται από διάφορα δομικά στοιχεία, τα οποία είναι απαραίτητα για την ορθή μετάδοση, λήψη και επεξεργασία του σήματος από το χρήστη και κατ' επέκταση απαραίτητα για την σωστή λειτουργία του δικτύου.

Στα στοιχεία αυτά περιλαμβάνονται το κατάλληλο λογισμικό (software), που επιτρέπει τη λειτουργία του δικτύου και το υλικό εξοπλισμού (hardware), (δηλ κόμβους επικοινωνίας, συσκευές διασύνδεσης).

8.1.1 Συσκευές χρηστών

Περιλαμβάνουν τις συσκευές εκείνες που είναι απαραίτητες για τη διασύνδεση του δικτύου με τους χρήστες. Κάποιες από αυτές τις συσκευές που χρησιμοποιούνται στα ασύρματα δίκτυα είναι και οι παρακάτω:

Laptop, Palmtop, Personal Digital Assistants (PDAs), Handheld PCs, printers, scanners.

8.1.2 Ασύρματες τοπικές γέφυρες (Wireless Local Bridges)

Οι γέφυρες χωρίζονται σε δύο είδη, σε *Local Bridges* που συνδέουν τοπικά δίκτυα κοντινών αποστάσεων και *Remote Bridges* οι οποίες συνδέουν δίκτυα που χωρίζονται από αποστάσεις μεγαλύτερες από αυτές που μπορούν να υποστηρίξουν τα πρωτόκολλα τοπικών δικτύων

Οι γέφυρες ανεξάρτητα από το αν υποστηρίζουν ενσύρματα ή ασύρματα δίκτυα, έχουν τις εξής χρήσεις:

- Η αύξηση του μήκους του δικτύου προς μια επιθυμητή κατεύθυνση.
- Παρέχει την ικανότητα στο δίκτυο να δεχθεί αυξημένο αριθμό χρηστών.
- Μείωση της υπερφόρτωσης του δικτύου.
- Να διαιρεθεί το υπερφορτωμένο δίκτυο σε δυο χωριστά δίκτυα κάνοντάς τα πιο αποδοτικά.
- Σύνδεση ενσύρματου-ασύρματου δικτύου.

Οι γέφυρες λειτουργούν στο υπόστρωμα MAC όπου παρακολουθούν την κυκλοφορία και ελέγχει τις διευθύνσεις προέλευσης και προορισμού κάθε πακέτου. Καθώς συλλέγει πληροφορίες δημιουργεί πίνακα δρομολόγησης. Κατόπιν προωθεί τα πακέτα ως ακολούθως: Αν ο προορισμός δεν υπάρχει στον πίνακα δρομολόγησης η γέφυρα προωθεί τα πακέτα σε όλα τα τμήματα, αν ο προορισμός υπάρχει στον πίνακα δρομολόγησης η γέφυρα προωθεί τα πακέτα στο συγκεκριμένο τμήμα.

8.1.3 Ασύρματες κάρτες δικτύου,-Network interface card (NIC)

Ένα PC ή ένας τερματικός σταθμός χρησιμοποιεί μια ασύρματη κάρτα δικτύου NIC, για να συνδεθεί με το ασύρματο δίκτυο και να πραγματοποιηθεί η μετάδοση ψηφιακών σημάτων μεταξύ των AP. Κατά την διαδικασία αυτή γίνεται η ενίσχυση και η διαμόρφωση του σήματος.

Οι ασύρματες κάρτες δικτύων συνδέονται με το τερματικό του χρήστη δια μέσου ενός διαύλου υπολογιστή όπως είναι οι ISA και PCMCIA (Industry Standard

Architecture , Personal Computer Memory Card Association), ή μέσω μιας RS-232 σειριακής ή παράλληλης θήρας.

Η διασύνδεση της ασύρματης κάρτας με τη συσκευή του χρήστη συμπεριλαμβάνει και ένα οδηγό λογισμικού (software driver) που συνδέει το λογισμικό του NOC στην κάρτα. Οι οδηγοί λογισμικού χρησιμοποιούν κάποια standards, τα κυριότερα από αυτά είναι:

- NDIS (Network Driver Interface Specification)
- ODI (Open Datalink Interface)
- PDS (Packet Driver Specification)

8.1.4 Κεραίες

Μια κεραία εκπέμπει το διαμορφωμένο σήμα μέσω του αέρα έτσι ώστε οι ασύρματοι χρήστες να μπορούν να το λάβουν .

Για τη μετάδοση του σήματος χρησιμοποιούνται δύο είδη κεραιών οι πολυκατευθυντικές (omnidirectional) και οι μονοκατευθυντικές (directional). Οι πρώτες διοχετεύουν την ισχύ προς κάθε κατεύθυνση, ενώ οι δεύτερες συγκεντρώνουν το μεγαλύτερο μέρος τους προς μια κατεύθυνση. Το μοντέλο διάδοσης μιας κεραίας καθορίζει και την περιοχή κάλυψης της κεραίας.

Οι κεραίες διακρίνονται σε πολλά είδη και μεγέθη και χαρακτηρίζονται από τις παρακάτω παραμέτρους:

- Propagation partner – Μοντέλο διάδοσης
- Gain - Ευαισθησία
- Transmit power – Ισχύς μετάδοσης
- Bandwidth – Εύρος ζώνης

ΚΕΦΑΛΑΙΟ 9^{ο}

9.1 ΣΧΕΔΙΑΣΜΟΣ ΚΑΙ ΥΛΟΠΟΙΗΣΗ ΔΙΚΤΥΟΥ

Ένα από τα πρώτα προβλήματα που συναντήσαμε κατά τη μελέτη και σχεδίαση του ασύρματου τοπικού δικτύου του εργαστηρίου ήταν ο πολύ περιορισμένος αριθμός διευθύνσεων IP που οι διαχειριστές δικτύου του ιδρύματος μπορούσαν να μας διαθέσουν. Σημειωτέον ότι η αρχική κατανομή των διευθύνσεων IP και η μελέτη καλωδιώσεων της εγκατάστασης, είχε γίνει σε παρελθόντα χρόνο σύμφωνα με τις ανάγκες της εποχής εκείνης, γεγονός που εύλογα οδηγεί στο συμπέρασμα ότι για τα σημερινά δεδομένα και τις δικτυακές απαιτήσεις ενός σύγχρονου εργαστηρίου, κρίνονται σχεδόν ανεπαρκείς.

Για να μπορέσει ένα δίκτυο υπολογιστών να συνδεθεί στο Internet πρέπει να έχει ο κάθε υπολογιστής τη δική του IP διεύθυνση. Η IP address είναι ένας αριθμός που χαρακτηρίζει μοναδικά παγκοσμίως έναν υπολογιστή. Υπάρχουν όμως και εσωτερικά δίκτυα τα οποία δεν συνδέονται άμεσα στο Internet, αλλά χρειάζονται να έχουν κάποιες IP. Για να καλυφθεί η συγκεκριμένη ανάγκη έχουν δημιουργηθεί κάποιες IP που ονομάζονται "ψεύτικες". Οι "ψεύτικες" διευθύνσεις μπορούν να χρησιμοποιούνται σε όλα τα υποδίκτυα που δεν συνδέονται άμεσα με το Internet. Το μειονέκτημα αυτών των IP είναι ότι δεν δρομολογούνται και κατά συνέπεια όποιος τις χρησιμοποιεί δεν μπορεί να συνδεθεί με το Internet (παρά μόνο με χρήση της υπηρεσίας NAT που θα δούμε παρακάτω). Αυτές οι διευθύνσεις είναι:

10.0.0.0 έως 10.255.255.255
172.0.0.0 έως 172.0.255.255
192.168.0.0 έως 192.168.255.255

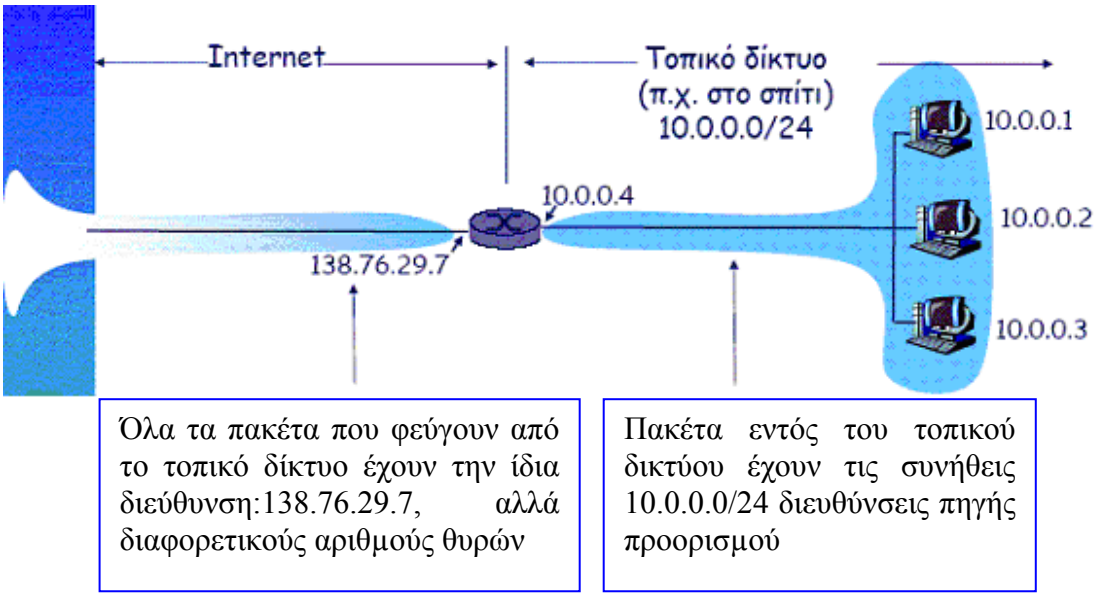
Υπάρχουν πολλές περιπτώσεις όπου πρέπει να συνδεθεί ένα ολόκληρο εσωτερικό δίκτυο υπολογιστών με το Internet, χωρίς όμως να μπορούμε να έχουμε όσες IP διευθύνσεις μας χρειάζονται (π.χ. 20 Η/Υ και 4 IP διευθύνσεις).

Υπάρχουν επίσης περιπτώσεις όπου θέλουμε να κάνουμε οικονομία στη χρήση των IP. Έτσι για παράδειγμα παρότι έχουμε πολλούς Η/Υ, θέλουμε να χρησιμοποιήσουμε συνολικά λίγες IP. Το παραπάνω πρόβλημα αντιμετωπίζεται με χρήση της υπηρεσίας NAT.

Η υπηρεσία NAT για να λειτουργήσει χρειάζεται να της καθοριστεί από το διαχειριστή του δικτύου ποιο είναι το **εσωτερικό υποδίκτυο** που θέλουμε να συνδέσουμε και ποιο είναι το **εξωτερικό δίκτυο,** δηλαδή το Internet.

Η υπηρεσία NAT δίνει τη δυνατότητα μία IP του εξωτερικού δικτύου να αντιστοιχεί σε ένα ή περισσότερα μηχανήματα του εσωτερικού δικτύου.

Η συνήθης τακτική ορίζει πως αν έχουμε έναν **server** στο εσωτερικό μας δίκτυο, ο οποίος θέλουμε να είναι άμεσα ορατός από το Internet, του αντιστοιχούμε μια IP του εξωτερικού δικτύου. Για τους υπολογιστές που χρησιμοποιούνται απλά σαν σταθμοί εργασίας δεσμεύουμε μια μόνο IP του εξωτερικού δικτύου για όλους τους σταθμούς εργασίας. Η συγκεκριμένη IP ονομάζεται **overload IP**.



Όλα τα πακέτα που φεύγουν από το τοπικό δίκτυο έχουν την ίδια διεύθυνση:138.76.29.7, αλλά διαφορετικούς αριθμούς θυρών

Πακέτα εντός του τοπικού δικτύου έχουν τις συνήθεις 10.0.0.0/24 διευθύνσεις πηγής προορισμού

Σχήμα 58: Μετάφραση διευθύνσεων Δικτύου NAT-Network Address Translation

9.2 Ο ΔΡΟΜΟΛΟΓΗΤΗΣ NAT

Εξερχόμενα πακέτα: Αντικαθιστά την διεύθυνση IP πηγής και τον αριθμό θύρας κάθε εξερχόμενου πακέτου με τη διεύθυνση IP του NAT και ένα νέο αριθμό θύρας -οι μακρινοί host απαντούν χρησιμοποιώντας την διεύθυνση IP του NAT ως διεύθυνση προορισμού.

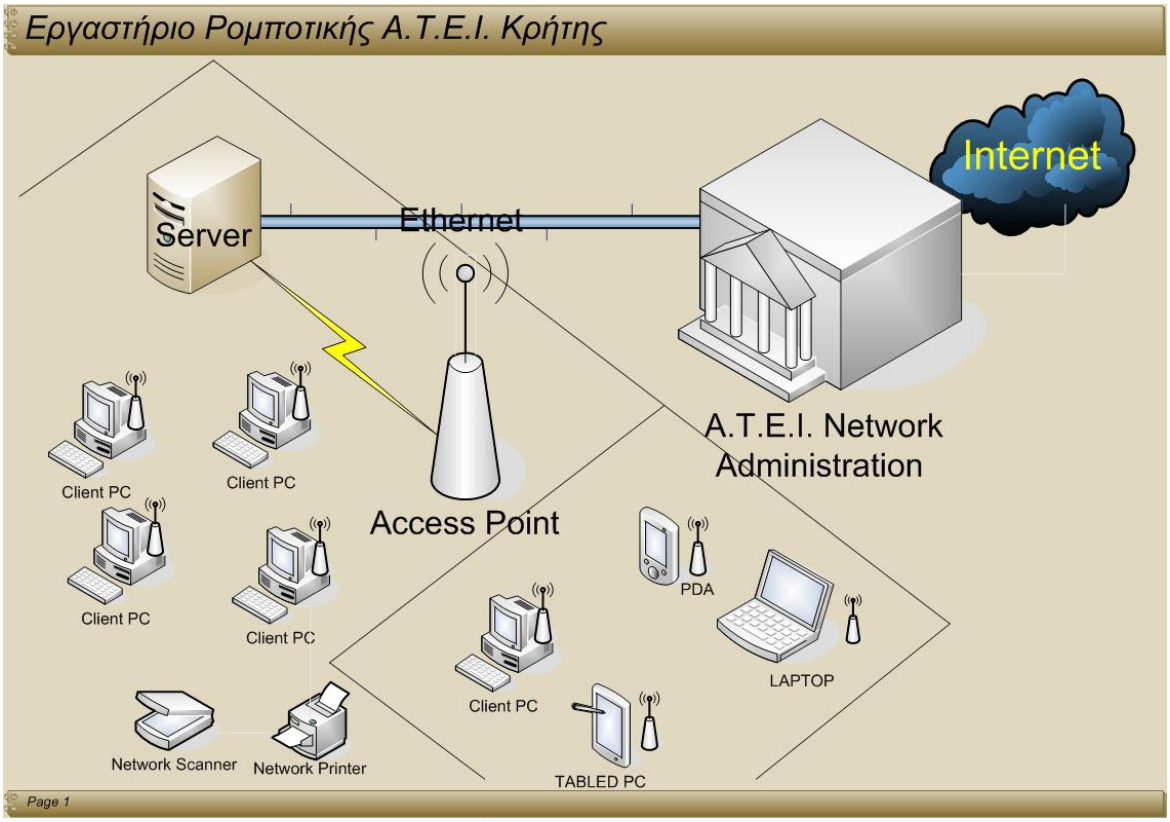
Πίνακας μετατροπής: Διατηρεί πίνακα με τις αντιστοιχίες για κάθε μετατρεπόμενο ζεύγος

Εισερχόμενα πακέτα: Αντικαθιστά τη διεύθυνση IP NAT και τον αριθμό θύρας των πεδίων προρισμού κάθε εισερχόμενου πακέτου με τον αντίστοιχο συνδυασμό διεύθυνσης IP πηγής και αριθμού θύρας που διατηρεί στον πίνακά του.

Σύμφωνα λοιπόν με τα παραπάνω μια πιθανή αρχιτεκτονική που θα μπορούσαμε να υλοποιήσουμε στο τοπικό μας ασύρματο LAN, σύμφωνα με τις ανάγκες μας και τους δεδομένους περιορισμούς, θα ήταν η εξής:

Θα χρησιμοποιούσαμε έναν Server ο οποίος θα αναλάμβανε να δεσμεύσει ένα ήδη υπάρχον IP για να μπορεί το WLAN μας να έχει πρόσβαση στο διαδίκτυο , και επίσης να διαμοιράσει ψεύτικες IP addresses στους υπόλοιπους ασύρματους σταθμούς του δικτύου μας, εφαρμόζοντας τις παραπάνω υπηρεσίες. Δηλαδή με τον τρόπο αυτόν ο κάθε σταθμός του εσωτερικού υποδικτύου μας, θα έχει ένα ξεχωριστό και μοναδικό για το υποδίκτυο IP και συνεπώς θα υπάρχει η δυνατότητα να διαμοιράσουμε Internet σε όλους τους σταθμούς. Παράλληλα για το Internet και για οποιοδήποτε εξωτερικό δίκτυο, σε όλους τους σταθμούς του WLAN θα αντιστοιχεί η IP address του Server, δηλαδή αυτό που σε κοινή ορολογία λέμε ότι, όλοι οι σταθμοί του εσωτερικού μας υποδικτύου, θα 'φαίνονται΄ στο εξωτερικό δίκτυο και κατ' επέκταση και στο Internet με το ίδιο IP, αυτό του Server.

Ο Server εν συνεχεία, θα συνδεόταν το Access Point που θα αναλάμβανε να εκπέμψει τα πακέτα, εφοδιασμένα ήδη με διευθύνσεις δρομολόγησης στο ασύρματο μέσο. (σχήμα 59).



Σχήμα 59: 1η πρόταση υλοποίησης WLAN

Η παραπάνω λύση είναι ευρέως αποδεκτή και συναντάται πολύ συχνά σε υποδίκτυα ενσύρματου περιβάλλοντος, όπου βέβαια το ρόλο του access point τον έχει ένα Hub ή καλύτερα ένα Switch. Όμως στην συγκεκριμένη περίπτωση παρουσιάζει κάποια μειονεκτήματα:

Απαραίτητη προϋπόθεση είναι η δέσμευση ενός σταθμού εργασίας, ο οποίος θα διαμορφωθεί ανάλογα και θα λειτουργήσει ως **Server**.

Επίσης, θα υπήρχε η ανάγκη της παρουσίας ενός ατόμου που θα εκτελεί το ρόλο του **System Administrator**, δηλαδή να διαχειρίζεται και να συντηρεί το Server και κατ' επέκταση το δίκτυο. Να παραχωρεί καινούριες IP σε προσωρινούς χρήστες και δικτυακές συσκευές και να κάνει τις απαραίτητες ρυθμίσεις σε περιπτώσεις τροποποιήσεων του δικτύου, γεγονός που σύμφωνα με τις σύγχρονες ανάγκες, συμβαίνει πολύ συχνά. Επισημαίνουμε ότι όλοι οι σταθμοί εργασίας και η πρόσβασή τους στο διαδίκτυο, εξαρτώνται άμεσα από την ορθή λειτουργία του Server.

Τα παραπάνω δεδομένα μας οδήγησαν σε μια έρευνα αγοράς για δικτυακές συσκευές ασύρματης δικτύωσης που υλοποιούν το πρωτόκολλο DHCP (Dynamic Host Configuration Protocol) Server. Θεωρήσαμε ότι ιδανικότερη και οικονομικότερη λύση για την ασύρματη επέκταση ενός υποδικτύου εργαστηριακής κλίμακας, θα ήταν μια συσκευή Access Point που ενσωματώνει Router, και μπορεί να λειτουργήσει σύμφωνα με το πρωτόκολλο DHCP. Δηλαδή, υλοποιεί με hardware τη λειτουργία του δρομολογητή και το πρωτόκολλο DHCP. Πρόσφατα στην αγορά κυκλοφορεί πληθώρα συσκευών που υλοποιούν τις παραπάνω απαιτήσεις και μάλιστα με πολύ χαμηλό κόστος, της τάξης των 100-500€.

9.3 ΤΟ ΠΡΩΤΟΚΟΛΛΟ DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)

Το Dynamic Host Control Protocol (DHCP), είναι ένα τυποποιημένο ανοικτό πρωτόκολλο που δημιουργήθηκε από την ανάγκη απλοποίησης της διαχείρισης δικτύων βασισμένων σε TCP/IP Protocol.

Κάθε Host υπολογιστής ο οποίος που συνδέετε σε ένα δίκτυο TCP/IP πρέπει να καταχωρηθεί με ένα μοναδικό IP Address. Εκτός από το πρόβλημα διαθεσιμότητας ελεύθερων IP Addresses που αναφέρθηκε παραπάνω η καταχώρηση των IP καθώς και μια σειρά άλλων παραμέτρων πρέπει να γίνεται από κάποιο διαχειριστή manually. Ένας DHCP Server αναλαμβάνει να διαχειριστεί τα παραπάνω θέματα από μόνος του χωρίς την παρουσία Διαχειριστή Δικτύου.

Εν συντομία αναλαμβάνει την παροδική απόδοση διευθύνσεων IP σε όλους τους σταθμούς χρηστών, συγκεκριμένης χρονικής διάρκειας, που ονομάζεται lease period. Δηλαδή ανιχνεύει και εντοπίζει όλους τους χρήστες, ανά τακτά χρονικά διαστήματα και τους αποδίδει διευθύνσεις IP με έναν 'ευφυή' τρόπο. Οι διευθύνσεις αυτές όπως είναι αναμενόμενο ανήκουν στην κατηγορία των 'ψεύτικων' ενώ, εκτός δικτύου αντιπροσωπεύονται από την ίδια IP, αυτή του Access Point και του αντίστοιχου Port, όπως ακριβώς συμβαίνει και στην υπηρεσία NAT.

Η επαναλαμβανόμενη ανίχνευση δικτυακών σταθμών και απόδοση διευθύνσεων IP, πραγματοποιείται για να δίνει τη δυνατότητα στο σύστημα να επαναχρησιμοποιεί τυχόν διευθύνσεις IP που είχαν αποδοθεί σε σταθμούς που έχουν αποσυνδεθεί από το δίκτυο.

Το μοντέλο συστήματος που χρησιμοποιεί το DHCP Server, χαρακτηρίζεται από μια αυτονομία λειτουργίας όντας ικανό να διαχειριστεί αυτοματοποιημένα όλα τα παραπάνω ζητήματα και η χρήση του είναι επιτυχώς εφαρμόσιμη σε δίκτυα με μεγάλο αριθμό χρηστών και επίσης σταθμούς κινητούς (palmtops, laptops)που συχνά αποσυνδέονται και επανασυνδέονται.

- Η διεύθυνση που εκχωρείται από τον διαχειριστή καταγράφεται σε αρχείο ή παραμέτρους του λειτουργικού συστήματος ή λαμβάνεται δυναμικά μέσω του DHCP.
- Μέσω του DHCP κάποιοι host μπορούν να μοιράζονται μια ομάδα διευθύνσεων IP
- Οι διευθύνσεις μπορούν να ξαναχρησιμοποιηθούν αφού δίδονται στον host όταν εισέρχεται στο δίκτυο και διατηρούνται μόνο όσο είναι συνδεδεμένος
- Μπορεί να υποστηριχθεί κινητικότητα των host

9.3.1 Συνοπτική περιγραφή λειτουργίας του DHCP

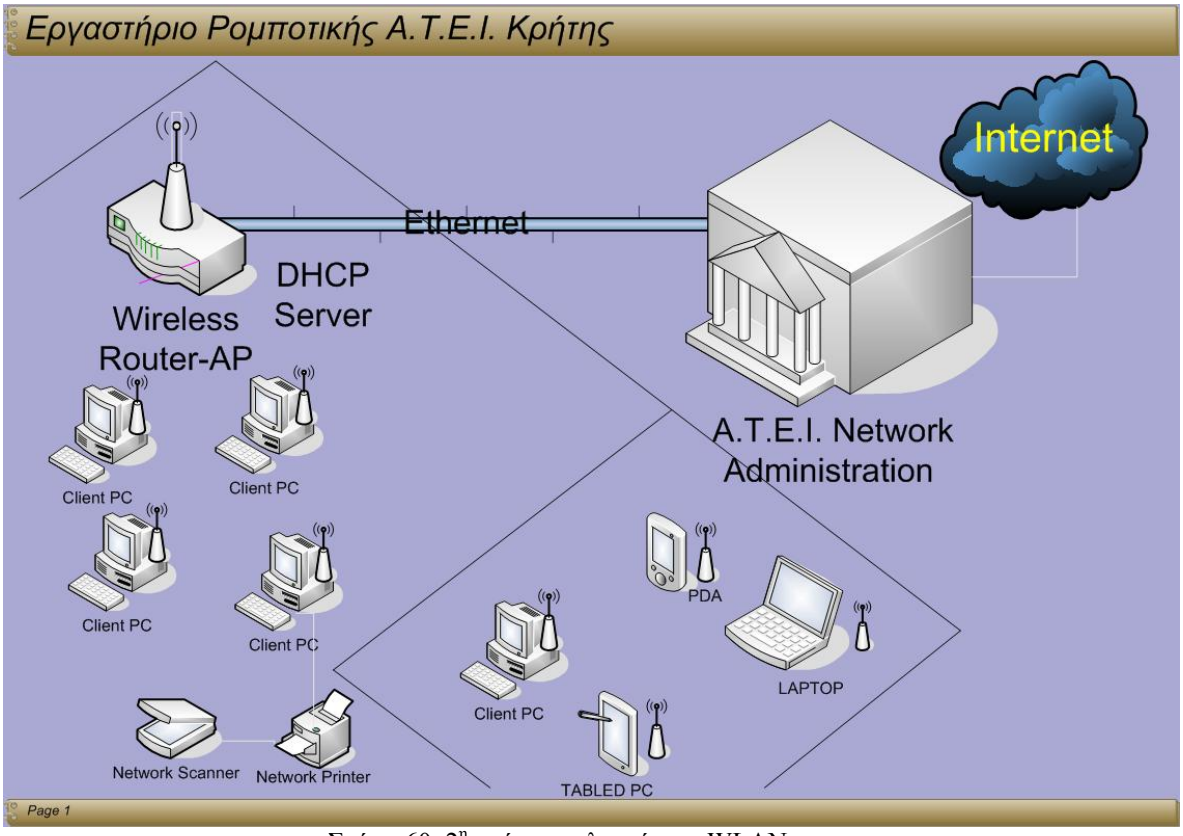
- Μόλις ο host εκκινήσει εκπέμπει ένα μήνυμα discover
- Ο εξυπηρετητής DHCP απαντά με το μήνυμα offers που ορίζει διευθύνσεις IP
- Ο host επιλέγει μία και εκπέμπει μια αίτηση request προς τον εξυπηρετητή
- Όλοι οι άλλοι εξυπηρετητές αποχωρούν και ο επιλεχθείς εξυπηρετητής στέλνει ack
- Όταν ο host τελειώσει στέλνει ένα release
- Η διεύθυνση IP παραχωρείται με δάνειο για συγκεκριμένο χρονικό διάστημα
- Ο host πρέπει να το ανανεώσει με μήνυμα lease εάν ο χρόνος λήξει

9.4 ΔΙΚΤΥΑΚΕΣ ΣΥΣΚΕΥΕΣ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΗΘΗΚΑΝ

Οι δικτυακές συσκευές που τελικά επιλέξαμε για να υλοποιήσουμε το δίκτυό μας είναι η εξής:

- Το Basic Service Set θα αποτελούνταν από τέσσερις Desktop Wireless σταθμούς έναν mobile υπολογιστή καθώς και έναν Palmtop Η/Υ που ενσωματώνει δυνατότητα Wi-Fi 802.11b. Επίσης συνυπολογίσαμε την ανάγκη περιοδικής διασύνδεσης κάποιων επιπλέον φορητών υπολογιστών που κατά διαστήματα χρησιμοποιεί το προσωπικό του εργαστηρίου καθώς και εξωτερικοί επισκέπτες-συνεργάτες . Ταυτόχρονα την ανάγκη διασύνδεσης κάποιων ρομποτικών συσκευών που ενσωματώνουν δυνατότητες ασύρματης δικτύωσης 802.11b και που μελλοντικά υπάρχει η δυνατότητα να αγοραστούν για τις ανάγκες του εργαστηρίου.
- Για το ρόλο του DHCP server χρησιμοποιήσαμε ένα Wireless 802.11g (54Mbps) ACCESS POINT –ROUTER της εταιρίας BELKIN κόστους της τάξης των 170 €, της περίοδο του 10-2003 που έγινε η αγορά.
  Η συγκεκριμένη συσκευή ενσωματώνει λειτουργίες :
  α) NAT IP Address Sharing
  β) Ενσωματωμένο 4-Port 10/100 Ethernet SWITCH
  γ) MAC Address Filtering
  δ) Built-In Dynamic Host Configuration Protocol (DHCP)
  ε) SPI Firewall
  στ) Λειτουργία VPN Pass-Through
  ζ) 64-128 bit WEP encryption
  η) Web Based Advanced User Interface
- Για την δικτύωση των Client Υπολογιστών επιλέξαμε 4 κάρτες Wireless 802.11g (54Mbps) PCI για τους Desktop Η/Υ και μια PCMCIA Cardbus κατάλληλη για

ένα Φορητό Η/Υ, της ίδιας εταιρίας για μέγιστη δυνατή συμβατότητα-συνεργασία.



Σχήμα 60: 2η πρόταση υλοποίησης WLAN

Αξίζει να σημειωθεί ότι η διαδικασία της υλοποίησης πραγματοποιήθηκε χωρίς ιδιαίτερη δυσκολία και σε πολύ σύντομο χρονικό διάστημα, γεγονός που μας εντυπωσίασε ιδιαίτερα.

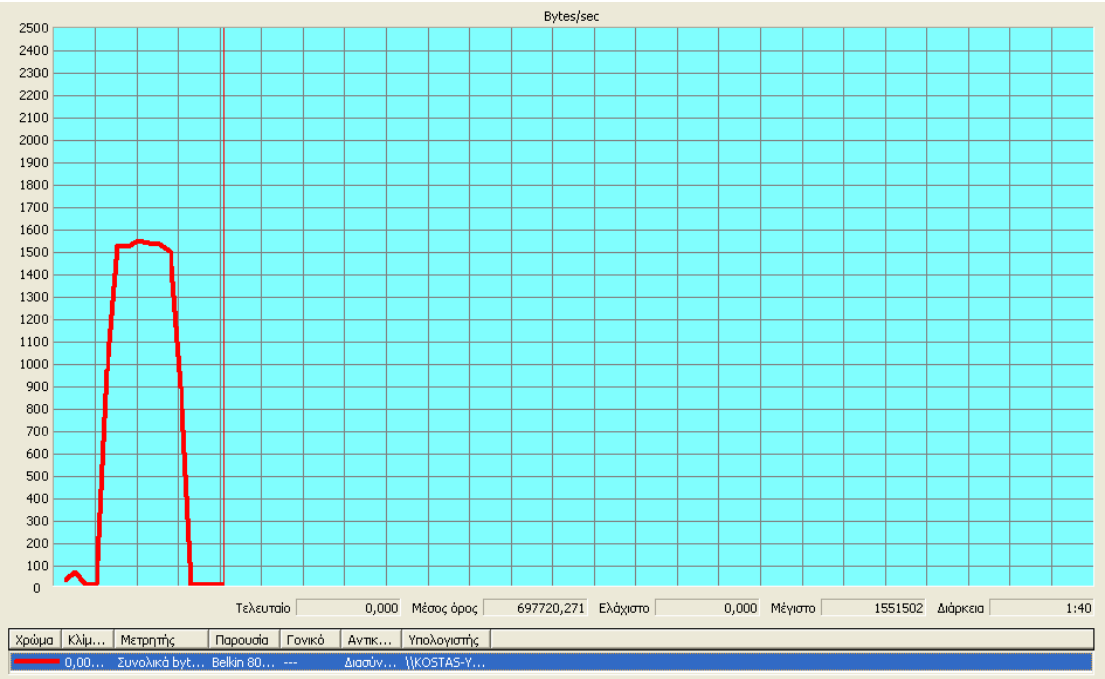
Πριν να μπούμε στη διαδικασία των μετρήσεων θεωρήσαμε σωστό να διαθέσουμε ένα εύλογο χρονικό διάστημα, όπου το δίκτυο θα βρισκόταν σε αδιάκοπη λειτουργία προκειμένου να εντοπίσουμε πιθανές τροποποιήσεις στην οργάνωση και ρύθμισή του, που θα προέκυπταν από ανάγκες τις οποίες αρχικά δεν είχαμε υπολογίσει.

Επίσης η συνεχής λειτουργία αυτή θα μας επέτρεπε να διαπιστώσουμε τη σταθερότητα του συστήματος και να εντοπίσουμε πιθανά μειονεκτήματα.

9.5 ΑΠΟΤΕΛΕΣΜΑΤΑ ΜΕΤΡΗΣΕΩΝ

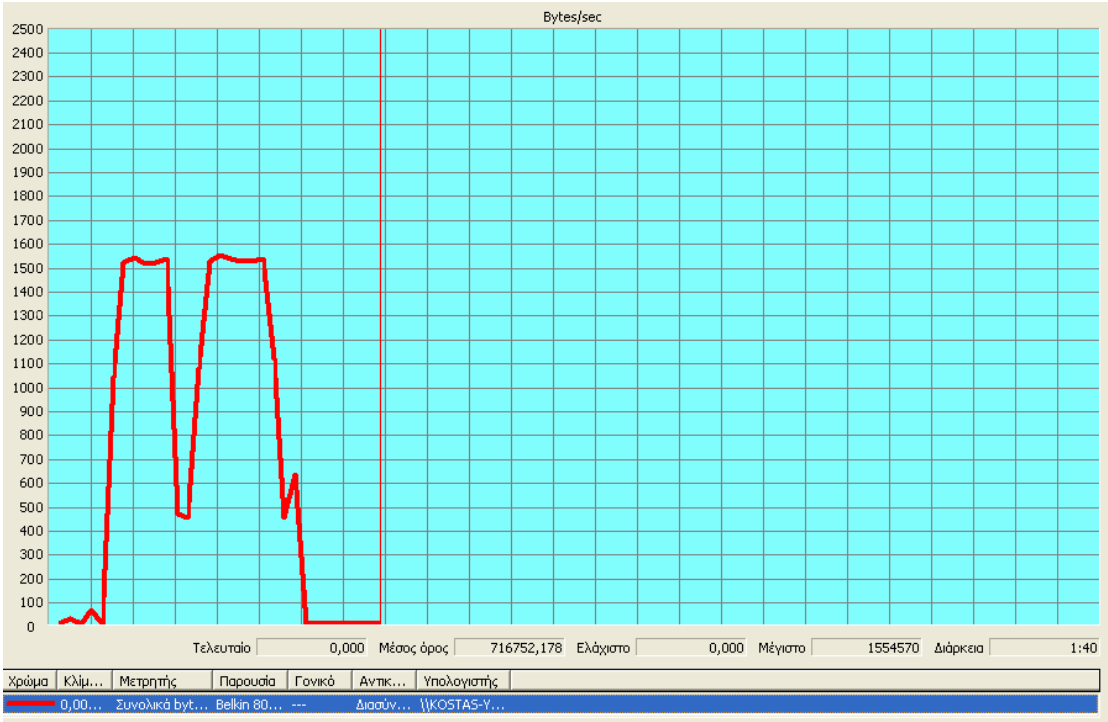
Αρχικά έγινε καταγραφή του throughput του ασύρματου μέσου, κατά τη μεταφορά πέντε αρχείων 10, 20, 30, 40, 50 MByte αντίστοιχα, από έναν τυχαίο σταθμό εργασίας σε έναν άλλο, ενώ οι υπόλοιποι σταθμοί έκαναν χαμηλή έως καθόλου χρήση του δικτύου. Οι αποστάσεις και των δυο σταθμών από το AP ήταν 5 m περίπου, χωρίς να μεσολαβούν φυσικά εμπόδια στον ενδιάμεσο χώρο (δηλαδή υπήρχε οπτική επαφή). Στις γραφικές παραστάσεις που προέκυψαν μελετήθηκαν, το μέγιστο- ελάχιστο bit rate, η συνέχεια του ρυθμού μετάδοσης, το throughput του δικτύου, ελήφθησαν μέσες τιμές και υπολογίστηκε επίσης ο απαιτούμενος χρόνος μεταφοράς των αρχείων σε κάθε περίπτωση.

1. Μεταφερόμενο αρχείο μεγέθους, 10Mbytes



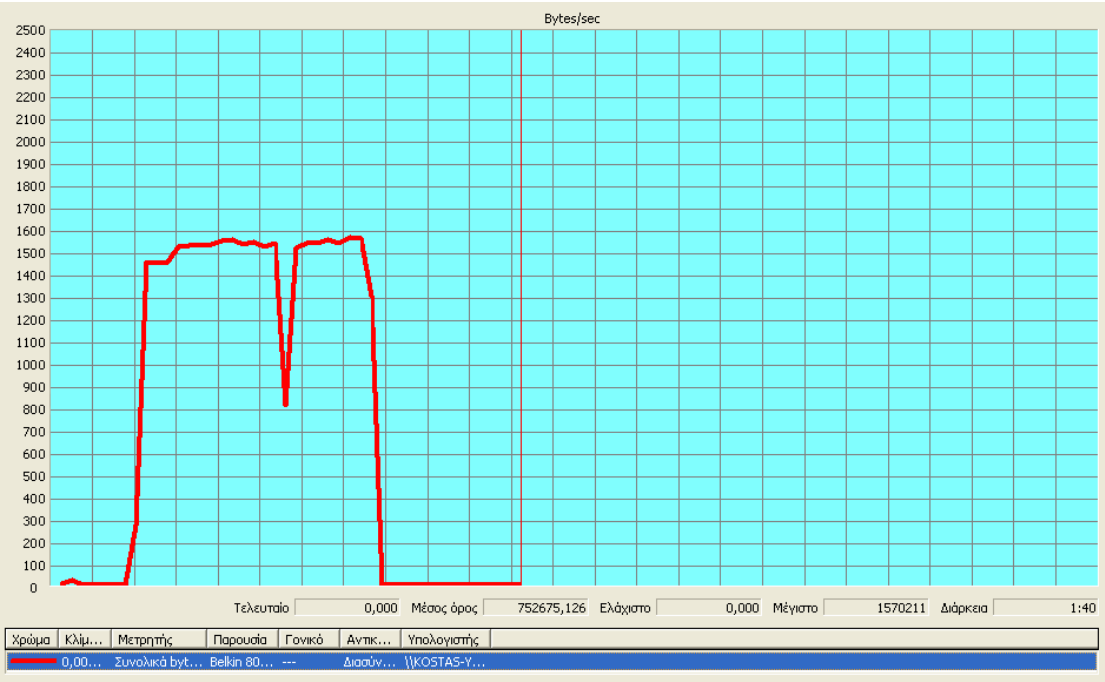
Μέγιστο bit rate 1,55MByte/sec=12,4Mbps, καλή συνέχεια μετάδοσης, χωρίς διακοπές και διακυμάνσεις της τάξης των 0,5Mbps. Ο χρόνος που απαιτήθηκε για τη μεταφορά, όπως προκύπτει από την καταγραφή είναι περίπου 9sec, συνεπώς το throughput, υπολογίζεται στα 11,1 Mbps.

2. Μεταφερόμενο αρχείο μεγέθους, 20Mbytes



Μέγιστο bit rate 1,55MByte/sec=12,4Mbps σχετικά καλή συνέχεια μετάδοσης, με περιορισμένες διακυμάνσεις, της τάξης όμως των 8Mbps, γεγονός που στην περίπτωση που η μεταφορά αφορούσε real time video streaming, πιθανόν να δημιουργούσε πρόβλημα (framing) σε περίπτωση που το λογισμικό αναπαραγωγής δεν διέθετε μηχανισμό buffering. Ο χρόνος που απαιτήθηκε για τη μεταφορά, όπως προκύπτει από την καταγραφή είναι περίπου 17sec, συνεπώς το throughput, υπολογίζεται στα 11.7 Mbps.

3. Μεταφερόμενο αρχείο μεγέθους, 30Mbytes



Μέγιστο bit rate 1,57MByte/sec=12,56Mbps, σχετικά καλή συνέχεια μετάδοσης, με περιορισμένες διακυμάνσεις, της τάξης των 6Mbps. Ο χρόνος που απαιτήθηκε για τη μεταφορά, όπως προκύπτει από την καταγραφή είναι περίπου 25sec, συνεπώς το throughput, υπολογίζεται στα 12Mbps.

4. Μεταφερόμενο αρχείο μεγέθους, 40Mbytes

Μέγιστο bit rate 1,6 MByte/sec= 12,8Mbps, σχετικά καλή συνέχεια μετάδοσης, με περιορισμένες διακυμάνσεις, της τάξης των 8Mbps. Ο χρόνος που απαιτήθηκε για τη μεταφορά, όπως προκύπτει από την καταγραφή είναι περίπου 33sec, συνεπώς το throughput, υπολογίζεται στα 12,1Mbps.

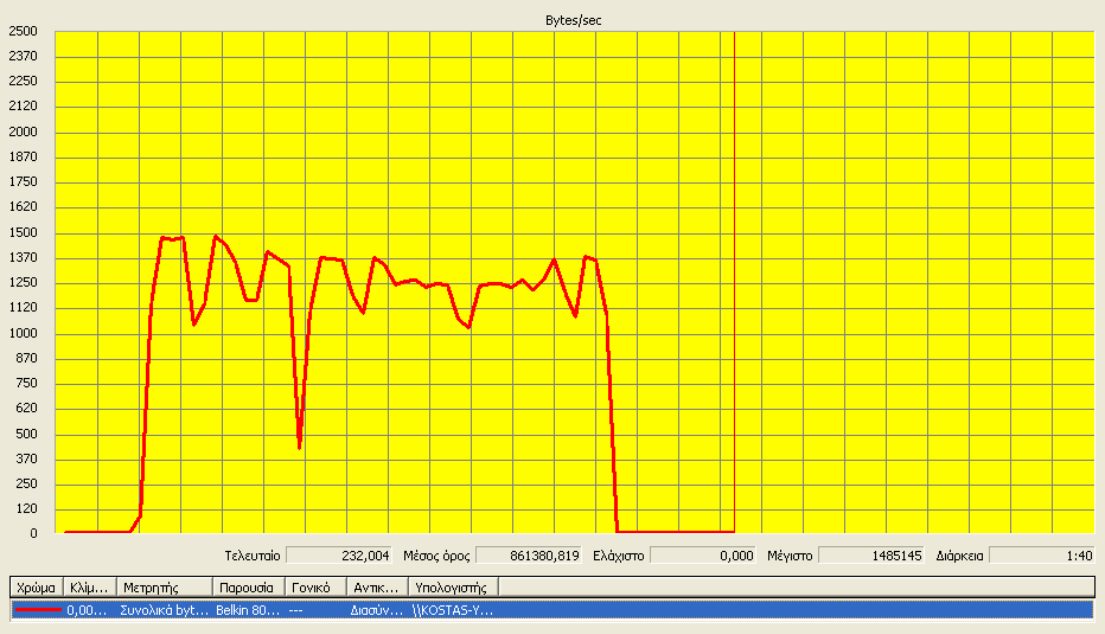
5. Μεταφερόμενο αρχείο μεγέθους, 50Mbytes

Μέγιστο bit rate 1,54MByte/sec=12,32Mbps, σχετικά καλή συνέχεια μετάδοσης, με περιορισμένες διακυμάνσεις, της τάξης των 5Mbps. Ο χρόνος που απαιτήθηκε για τη μεταφορά, όπως προκύπτει από την καταγραφή είναι περίπου 24sec, συνεπώς το throughput, υπολογίζεται στα 12.5Mbps.

Όπως παρατηρήσαμε στις παραπάνω καταγραφές, διαπιστώνονται διακυμάνσεις του bit rate , στιγμιαίες πτώσεις, διάρκειας κλασμάτων του δευτερολέπτου και επανάκαμψη στα μέγιστα της απόδοσης. Δεδομένου ότι κατά τη διάρκεια της μεταφοράς του αρχείου δεν υπήρξαν εξωτερικές παρεμβολές, π.χ διάβαση κάποιου ατόμου στον ενδιάμεσο χώρο σταθμού AP, δεδομένου επίσης ότι οι σταθμοί είναι σταθεροί οι διακυμάνσεις αυτές μπορούν να εξηγηθούν ως σφάλματα μετάδοσης του φυσικού στρώματος, που μπορεί για παράδειγμα να είναι μια μη ολοκληρωμένη παραλαβή ενός πακέτου, παράληψη αποστολής κάποιου ACK κ.λ.π . Το MAC layer αντιλήφθηκε το σφάλμα μετάδοσης που προκάλεσε την πτώση του ρυθμού μετάδοσης και δρομολόγησε τις κατάλληλες ενέργειες διόρθωσής του και συνέχισης της εκπομπής στο μέγιστο δυνατό επίπεδο.

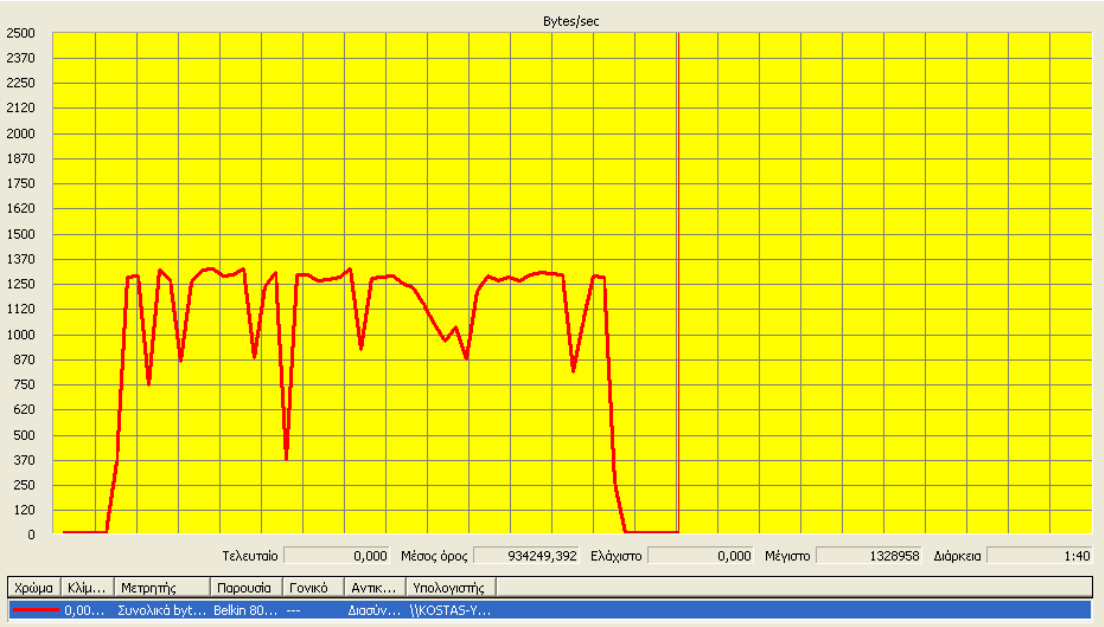
Ακολουθούν **μετρήσεις οι οποίες πραγματοποιήθηκαν με φορητό Η/Υ**, προκειμένου να επιτύχουμε διαφοροποιήσεις στην παράμετρο της απόστασης και παρεμβολές φυσικών εμποδίων (τοίχων), για να διαπιστωθεί η συμπεριφορά του δικτύου υπό τις εκάστοτε συνθήκες.

1. Μεταφορά αρχείου 50MBytes από το φορητό Η/Υ, σε έναν σταθερό σταθμό εργασίας, ο οποίος έχει οπτική επαφή με το AP και απόσταση 5m. Η απόσταση του φορητού Η/Υ από το AP είναι 2m και παρεμβάλλεται 1 τοίχος.



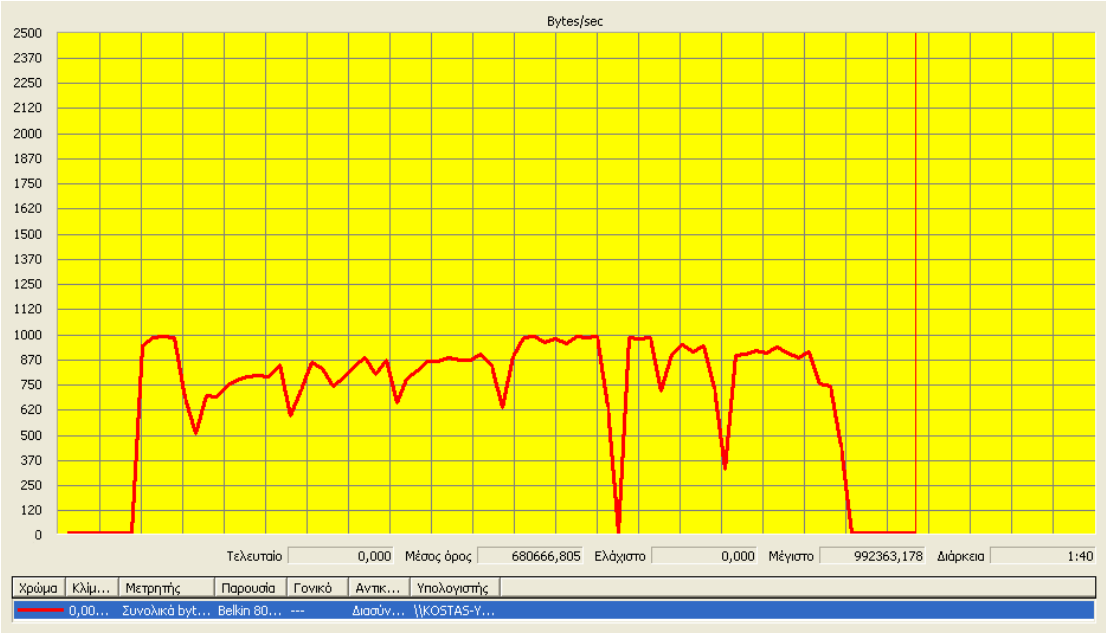
Μέγιστο bit rate 1,4851MByte/sec=11,9Mbps, σχετικά μέτρια συνέχεια μετάδοσης, χωρίς διακοπές με αρκετές διακυμάνσεις της τάξης των 7,2Mbps. Ο χρόνος που απαιτήθηκε για τη μεταφορά, όπως προκύπτει από την καταγραφή είναι περίπου 46sec, συνεπώς το throughput, υπολογίζεται στα 10,6 Mbps. Συγκριτικά με την προηγούμενη αντίστοιχη μέτρηση όπου η απόσταση του δεύτερου σταθμού από το AP ήταν μεγαλύτερη ,χωρίς όμως την μεσολάβηση της μεσοτοιχίας , διαπιστώνεται μείωση του throughput και κατά συνέπεια αύξηση του χρόνου αποστολής του αρχείου.

2. Μεταφορά αρχείου 50MBytes από το φορητό Η/Υ, σε έναν σταθερό σταθμό εργασίας, ο οποίος έχει οπτική επαφή με το AP και απόσταση 5m. Η απόσταση του φορητού Η/Υ από το AP είναι 10m και παρεμβάλλονται 2 τοίχοι.



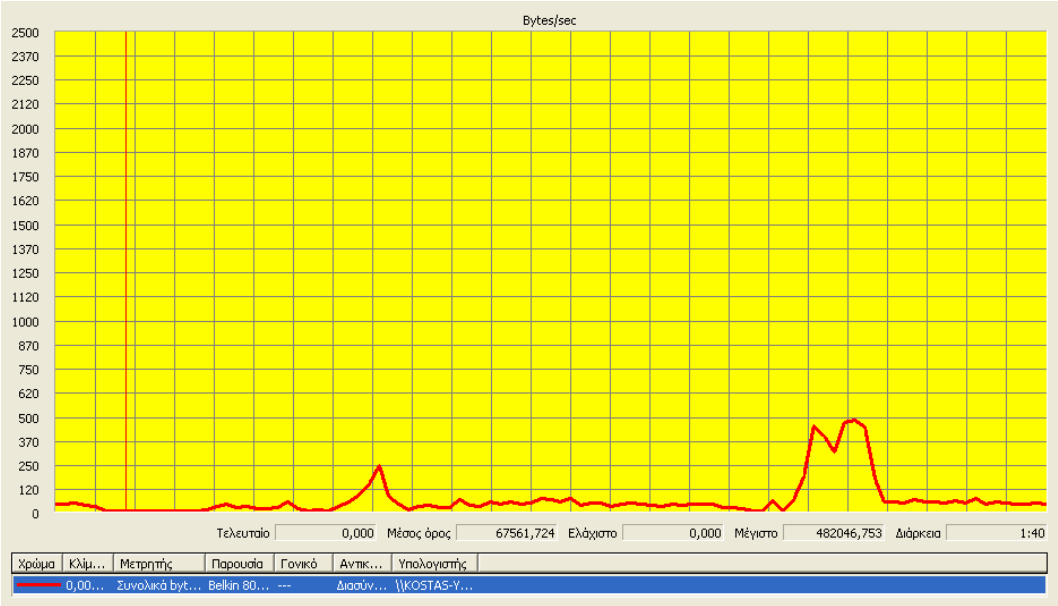
Μέγιστο bit rate 1,33MByte/sec=10,64Mbps, σχετικά μέτρια συνέχεια μετάδοσης, χωρίς διακοπές με πολλές διακυμάνσεις της τάξης των 8Mbps. Ο χρόνος που απαιτήθηκε για τη μεταφορά, όπως προκύπτει από την καταγραφή είναι περίπου 52sec, συνεπώς το throughput, υπολογίζεται στα 9,6Mbps. Η δεύτερη μεσοτοιχία και η αύξηση της απόστασης κατά 8m, προκάλεσε μείωση του throughput κατά μια μόνο μονάδα.

3. Μεταφορά αρχείου 50MBytes από το φορητό Η/Υ, σε έναν σταθερό σταθμό εργασίας, ο οποίος έχει οπτική επαφή με το AP και απόσταση 5m. Η απόσταση του φορητού Η/Υ από το AP είναι 30m και παρεμβάλλονται 3 τοίχοι.



Μέγιστο bit rate 9,920MByte/sec=7,936Mbps, μέτρια συνέχεια μετάδοσης, με μια διακοπή και πολλές διακυμάνσεις της τάξης των 8Mbps. Ο χρόνος που απαιτήθηκε για τη μεταφορά, όπως προκύπτει από την καταγραφή είναι περίπου 68sec, συνεπώς το throughput, υπολογίζεται στα 7,3Mbps. Η τρίτη μεσοτοιχία και η περαιτέρω αύξηση της απόστασης κατά 20m, πλέων προκαλεί αισθητή μείωση του throughput παρ' όλα αυτά όμως το δίκτυό μας εξακολουθεί να αποδίδει σε πολύ καλά επίπεδα.

4. Μεταφορά αρχείου 50MBytes από το φορητό Η/Υ, σε έναν σταθερό σταθμό εργασίας, ο οποίος έχει οπτική επαφή με το ΑΡ και απόσταση 5m. Η απόσταση του φορητού Η/Υ από το ΑΡ είναι 40m και παρεμβάλλονται 4 τοίχοι.



Στην παραπάνω καταγραφή, είναι άσκοπο να αναφερθούμε σε αριθμητικά αποτελέσματα, διότι όπως διαπιστώνουμε ο ρυθμός μετάδοσης έχει πέσει σε πολύ χαμηλά όρια, πολύ κάτω από 1 Mbyte/sec. Η επικοινωνία βέβαια διατηρήθηκε οριακά και κάποια στιγμή η μεταφορά του αρχείου ολοκληρώθηκε. Πρέπει όμως να σημειωθεί ότι στο γεγονός αυτό συνέβαλλαν δύο εξωτερικοί παράγοντες. Ο ένας ήταν ότι στην τελευταία μεσοτοιχία ήταν προσαρμοσμένοι μεταλλικοί φοριαμοί γεγονός που εξηγεί την μεγάλη απορρόφηση της ισχύος του μικροκυματικού σήματος. Ο δεύτερος παράγοντας ήταν η απότομη αύξηση των επιπέδων απολαβής θορύβου που παρατηρήθηκε εκτός της τέταρτης μεσοτοιχίας. Συγκεκριμένα η απολαβή ωφέλιμου σήματος κυμαίνονταν στα -75dB περίπου, ενώ το επίπεδο θορύβου υψηλότερο, στα -79 dB. Η παρεμβολή αυτή εξηγείται από το γεγονός ότι στο συγκεκριμένο σημείο βρισκόμασταν πολύ κοντά σε εξωτερική κεραία 802.11b μεγάλης εμβέλειας που χρησιμοποιείται για ασύρματες ζεύξεις μεγάλων αποστάσεων.

Το συγκεκριμένο δίκτυο υλοποιήθηκε στο Α.Τ.Ε.Ι. Κρήτης για να εξυπηρετεί τις ανάγκες του εργαστηρίου Αυτοματισμών-Ρομποτικής. Η παρούσα εργασία όμως, έχει στόχο την πειραματική διαπίστωση της συμπεριφοράς του, σε περιβάλλον νοσοκομείου και του χώρου υγείας γενικότερα ,προκειμένου να συμπεράνουμε κατά πόσο μπορεί να υλοποιηθεί σε ένα τέτοιο χώρο και να καλύψει τις ανάγκες του. Θεωρήσαμε σκόπιμο λοιπόν να πειραματιστούμε όσον αφορά τη χρήση του στη μεταφορά σύγχρονων ψηφιακών ιατρικών δεδομένων.

Συγκεκριμένα θα μας ενδιέφεραν οι ‘ιατρικές εφαρμογές’ με τις υψηλότερες δικτυακές απαιτήσεις όσον αφορά το εύρος ζώνης τον ρυθμό μετάδοσης κλπ. Όπως για παράδειγμα η πραγματικού χρόνου μετάδοση-αποστολή ιατρικών εξετάσεων που

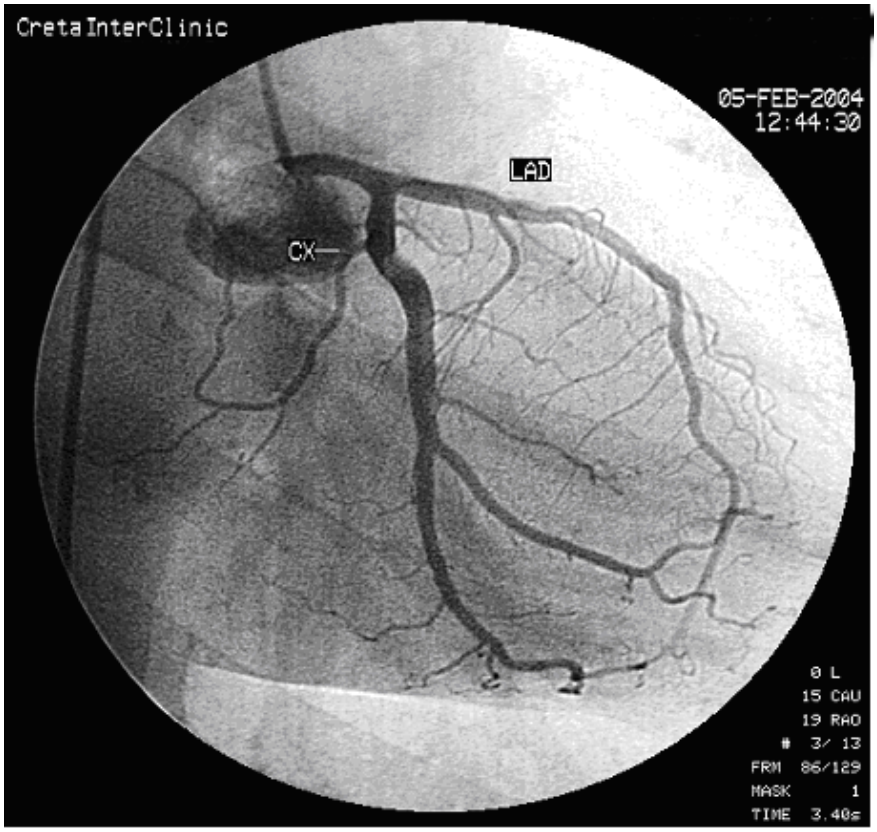
τα αποτελέσματά τους έχουν τη μορφή διαδοχικών ψηφιακών εικόνων υψηλής ανάλυσης , Real Time Video υψηλής ανάλυσης που τα πιο σύγχρονα μηχανήματα μπορούν να παρέχουν. Στην κατηγορία αυτή εντάσσονται τα ψηφιακά ακτινοσκοπικά-ακτινολογικά μηχανήματα τελευταίας τεχνολογίας (π.χ. Ψηφιακή Αγγειογράφια), η ψηφιακή αξονική τομογραφία γενικότερα (CT,MRI…….), οι εξετάσεις γ-κάμερας, κάποια μηχανήματα οφθαλμιατρικών εξετάσεων τελευταίας τεχνολογίας κλπ.

Στην περίπτωση που η κατηγορία αυτή της ασύρματης δικτύωσης είχε ικανοποιητική συμπεριφορά καλύπτοντας τις υψηλές δικτυακές απαιτήσεις αυτών των εφαρμογών , σίγουρα δεν θα υπήρχαν προβλήματα και περιορισμοί στην επιλογή αυτής της δικτυακής κατηγορίας στο ιατρικό περιβάλλον, από εφαρμογές τύπου ιατρικών βάσεων δεδομένων (πχ. Ιατρικός φάκελος Ασθενή), εφαρμογές διαχείρισης και πρόσβασης-διανομής, γνώσης, ιατρικής πληροφορίας, άμεσης πρόσβασης σε αποτελέσματα διαγνωστικών εργαστηριακών εξετάσεων πχ. Αιματολογικών-Βιοχημικών αναλυτών, δυνατότητα πρόσβασης στο διαδίκτυο με πολύ ικανοποιητικές ταχύτητες κλπ.

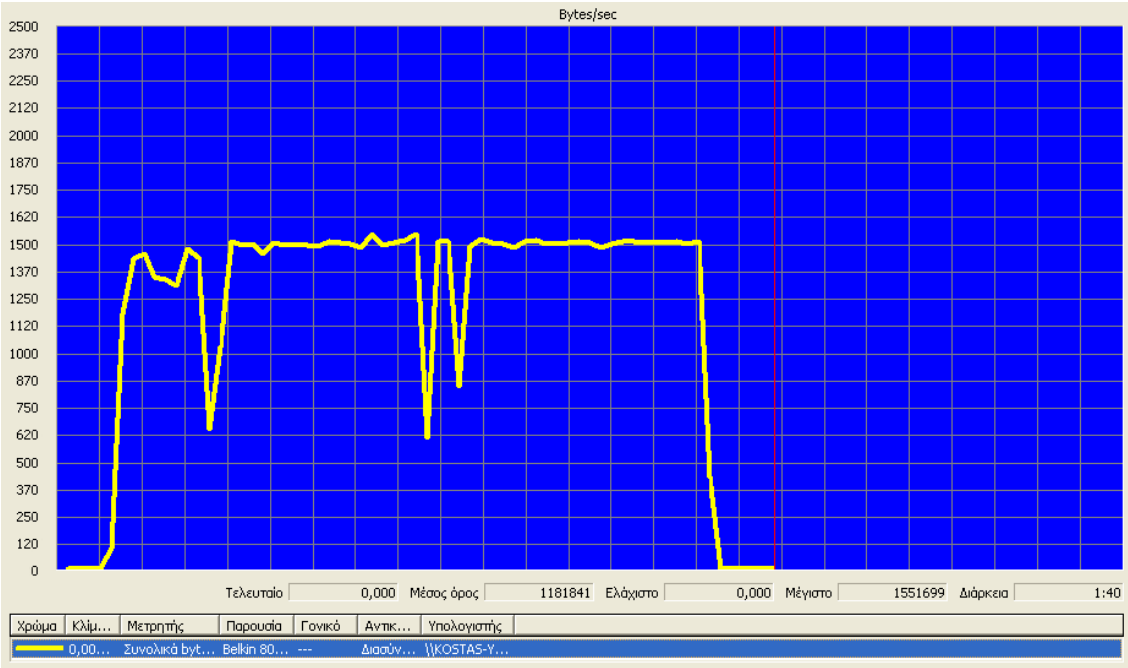
Επιλέξαμε λοιπόν σύμφωνα με τα παραπάνω κριτήρια κάποιες από αυτές και πραγματοποιήσαμε μετρήσεις θεωρώντας μια υπόθεση εργασίας όπου ένα διαγνωστικό μηχάνημα πραγματοποιεί μια εξέταση και ο δικτυακός σταθμός με τον οποίο είναι συνδεδεμένο, την μεταδίδει on line σε κάποιο άλλο απομακρυσμένο σταθμό του δικτύου. Ο γιατρός στον δεύτερο σταθμό με τη χρήση κατάλληλου λογισμικού παρακολουθεί σε πραγματικό χρόνο την εξέλιξη της εξέτασης.

Στην πλειοψηφία των επιλογών μας το δίκτυο ανταποκρίθηκε θετικά ,με την έννοια ότι το throughput του, επαρκεί για την πραγματικού χρόνου μεταφορά των εξετάσεων αυτών, σε μερικές περιπτώσεις οριακά σε άλλες ικανοποιητικά αφήνοντας κάποιο ποσοστό του εύρους ζώνης ελεύθερο για ταυτόχρονη χρήση από άλλες εφαρμογές. Αυτό που διαπιστώθηκε όμως ήταν ότι στο σύνολο σχεδόν των εφαρμογών αυτής της κατηγορίας συνέβαινε το εξής. Λόγω των υψηλών απαιτήσεων, κατά την real time μετάδοση της εξέτασης καταλαμβανόταν το μεγαλύτερο ποσοστό του επιτρεπόμενου throughput, δηλαδή το channel utilization έφτανε σε ποσοστά μεγαλύτερα του 60-70% απ' ότι δηλαδή διαφαίνεται ξεκάθαρα ότι υπάρχει περιορισμός σε μια μόνο real time μετάδοση εξέτασης κάθε φορά, που παρά ταύτα μπορεί να είναι broadband μετάδοση (ένα προς πολλά). Το γεγονός αυτό αποτελεί ένα σοβαρό μειονέκτημα καθώς στην αξιολόγηση μιας κατηγορίας δικτύου που πρόκειται να υλοποιηθεί σε νοσοκομειακό περιβάλλον ,θα πρέπει να ληφθούν υπόψη οι απαιτήσεις που δημιουργεί η παραπάνω από μία ταυτόχρονη μετάδοση παρόμοιων εξετάσεων υψηλών απαιτήσεων, που μέχρι σήμερα βέβαια δεν αποτελούν σύνηθες φαινόμενο, αλλά που σύντομα με την εξέλιξη της ιατρικής τεχνολογίας, θα προκύψουν.

Ενδεικτικά παραθέτουμε τα αποτελέσματα μιας καταγραφής που αφορά την πραγματικού χρόνου μετάδοση τμήματος μιας ψηφιακής αγγειογραφίας από έναν σταθμό με οπτική επαφή με το σημείο πρόσβασης και απόσταση 5 περίπου μέτρων , σε έναν άλλο με τα ίδια χαρακτηριστικά. Η λήψη της εξέτασης αυτής έγινε από ψηφιακό αγγειογράφο τελευταίας τεχνολογίας του ιατρικού κέντρου CretaInterClinic και είχε τα εξής αρκετά υψηλά χαρακτηριστικά και προδιαγραφές . Ανάλυση 1008x 1042 pixels βάθος χρώματος 32 bit, 22 πλαίσια/δευτερόλεπτο , ρυθμό αναπαραγωγής δεδομένων 1,978 Mbytes/sec= 15,82Mbps και διάρκεια 37 sec. Το μέγεθος της στο δίσκο ήταν 73,2 Mbytes.



Εικόνα 61: Ψηφιακό οπτικό παράθυρο ψηφιακής αγγειογραφίας σε σμίκρυνση.



Όπως διαπιστώνεται στην παραπάνω καταγραφή το μέγιστο του ρυθμού μετάδοσης που το δίκτυο επιτυγχάνει είναι 1,551 Mbytes/sec=12,48Mbps.Οι απαιτήσεις όμως της εφαρμογής κυμαίνονται σε υψηλότερο επίπεδο 1,978 Mbytes/sec. Η διάρκεια της μετάδοσης όπως υπολογίζεται από το γράφημα είναι 57

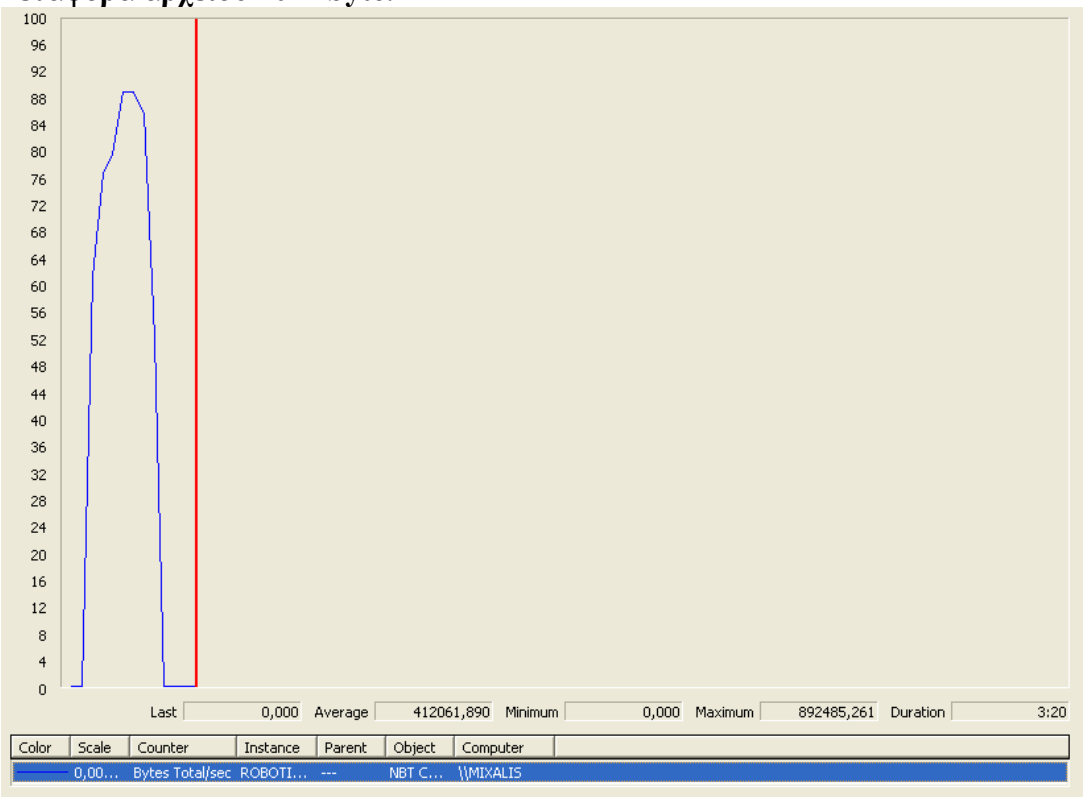
δευτερόλεπτα εμφανώς μεγαλύτερη από τη φυσιολογική διάρκεια της εξέτασης που ήταν 37 δευτερόλεπτα. Διαπιστώνεται αρκετή χρονική καθυστέρηση στη μετάδοση. Το δίκτυο δεν ανταποκρίνεται στις πολύ υψηλές απαιτήσεις αυτής της εφαρμογής.

Το αποτέλεσμα στην πραγματικού χρόνου αναπαραγωγή της εξέτασης στο δεύτερο σταθμό ήταν προβληματικό. Παρουσίασε πολλές διακοπές , έντονο framing και σε καμία περίπτωση δεν ήταν ικανοποιητικό. Βέβαια βελτιώθηκε εμφανώς μειώνοντας το βάθος χρώματος από τα 32 bit σε χαμηλότερα επίπεδα και σίγουρα μειώνοντας την ανάλυση και αυξάνοντας το ποσοστό συμπίεσης γεγονός που έχει ως αποτέλεσμα την απώλεια κάποιου βαθμού ιατρικής διαγνωστικής πληροφορίας .Κυμάνθηκε όμως πάντα σε οριακά εξαντλώντας παράλληλα όλους τους διαθέσιμους δικτυακούς πόρους .

Η μελέτη μας επικεντρώθηκε στην κατηγορία 802.11g , για τον απλούστατο λόγο ότι αποτελεί εξέλιξη του προτύπου 802.11b (που σίγουρα είναι πιο ευρέως διαδεδομένο) και επιτυγχάνει ρυθμούς μετάδοσης πολύ μεγαλύτερους .Συνεπώς η σκέψη μας εύλογα ήταν να εκμεταλλευτούμε τις μέγιστες δυνατότητες που η υπάρχουσα τεχνολογία της κατεύθυνσης αυτής μας παρέχει και παράλληλα το γεγονός ότι μεταξύ των δύο προτύπων υπάρχει συμβατότητα.

Για του λόγου του αληθές παραθέτουμε κάποιες μετρήσεις και της κατηγορίας 802.11 b που έγιναν χρησιμοποιώντας δικτυακές συσκευές τελευταίας κυκλοφορίας και αρκετά υψηλού κόστους.

Μεταφορά αρχείου 10 Mbyte.



Μεταφορά αρχείου 30 Mbyte.

Μεταφορά αρχείου 50 Mbyte.

Στις παραπάνω μετρήσεις οι συνθήκες πραγματοποίησης των καταγραφών ήταν πολύ καλές. Η επικοινωνία μεταξύ των δικτυακών συσκευών ήταν σχεδόν βέλτιστη με αποτέλεσμα να επιτυγχάνεται το μέγιστο δυνατό throughput το οποίο κατά μέσο όρο κυμάνθηκε γύρο στα 6,76 Mbytes/sec= 5,4 Mbps. Διαπιστώνεται λοιπόν αρκετά χαμηλότερος ωφέλιμος μέσος ρυθμός μετάδοσης γεγονός που σε αρκετές ιατρικές δικτυακές εφαρμογές θα αποτελούσε περιορισμό.

9.6 Συμπεράσματα - Προτάσεις

Τα αποτελέσματα των μετρήσεων στο σύνολό τους , χωρίς καμία αμφιβολία επικροτούν την επιλογή του προτύπου 802.11g έναντι του 802.11 b.

Οι δυνατότητες του 802.11g για εφαρμογές τύπου ιατρικών βάσεων δεδομένων (πχ. Ιατρικός φάκελος Ασθενή), εφαρμογές όπως φωνητική επικοινωνία video-συνδιάσκεψη , αποστολή και λήψη μη πραγματικού χρόνου video σε πολύ ικανοποιητικούς χρόνους δίχως περιορισμούς στην ανάλυση, αποστολή και λήψη ιατρικών δεδομένων αποστολή και λήψη ιατρικών σημάτων και εικόνων ,διαχείρισης και πρόσβασης-διανομής, ιατρικής πληροφορίας, άμεσης πρόσβασης σε αποτελέσματα διαγνωστικών εργαστηριακών εξετάσεων πχ. Αιματολογικών-Βιοχημικών αναλυτών, δυνατότητα διασύνδεσης-ελέγχου από απόσταση ιατρικών μηχανημάτων, δυνατότητα πρόσβασης στο διαδίκτυο , σίγουρα επαρκούν.

Οι τεχνολογικές δυνατότητες τύπου DHCP server ,υπηρεσίας NAT που οι σύγχρονες ασύρματες δικτυακές συσκευές της κατηγορίας αυτής ενσωματώνουν, αποτελούν μεγάλο πλεονέκτημα στη διαχείριση και εξυπηρέτηση μεγάλου αριθμού χρηστών (και μάλιστα μη σταθερών χρηστών).Η ταχύτητα και ευελιξία εγκατάστασης η άμεση επεκτασιμότητα η δυνατότητα κινητικότητας (mobility- roaming), η συμβατότητα μεταξύ των διαφόρων κατηγοριών του προτύπου 802.11 , η μεγάλη σταθερότητα και το χαμηλό κόστος , καθιστούν την κατηγορία αυτή της ασύρματης δικτύωσης μια από τις πιο αξιόλογες προτάσεις για το ιατρικό περιβάλλον. Ιδανική σε περιπτώσεις όπου υπάρχει ανάγκη επέκτασης ενός ήδη προϋπάρχοντος ενσύρματου δικτύου, όπου εύκολα αντιμετωπίζονται προβλήματα διευθυνσεοδότησης IP και συνυπολογίζεται η δυσκολία τοποθέτησης νέων καλωδιώσεων σε ήδη διαμορφωμένο και εν λειτουργία περιβάλλον.

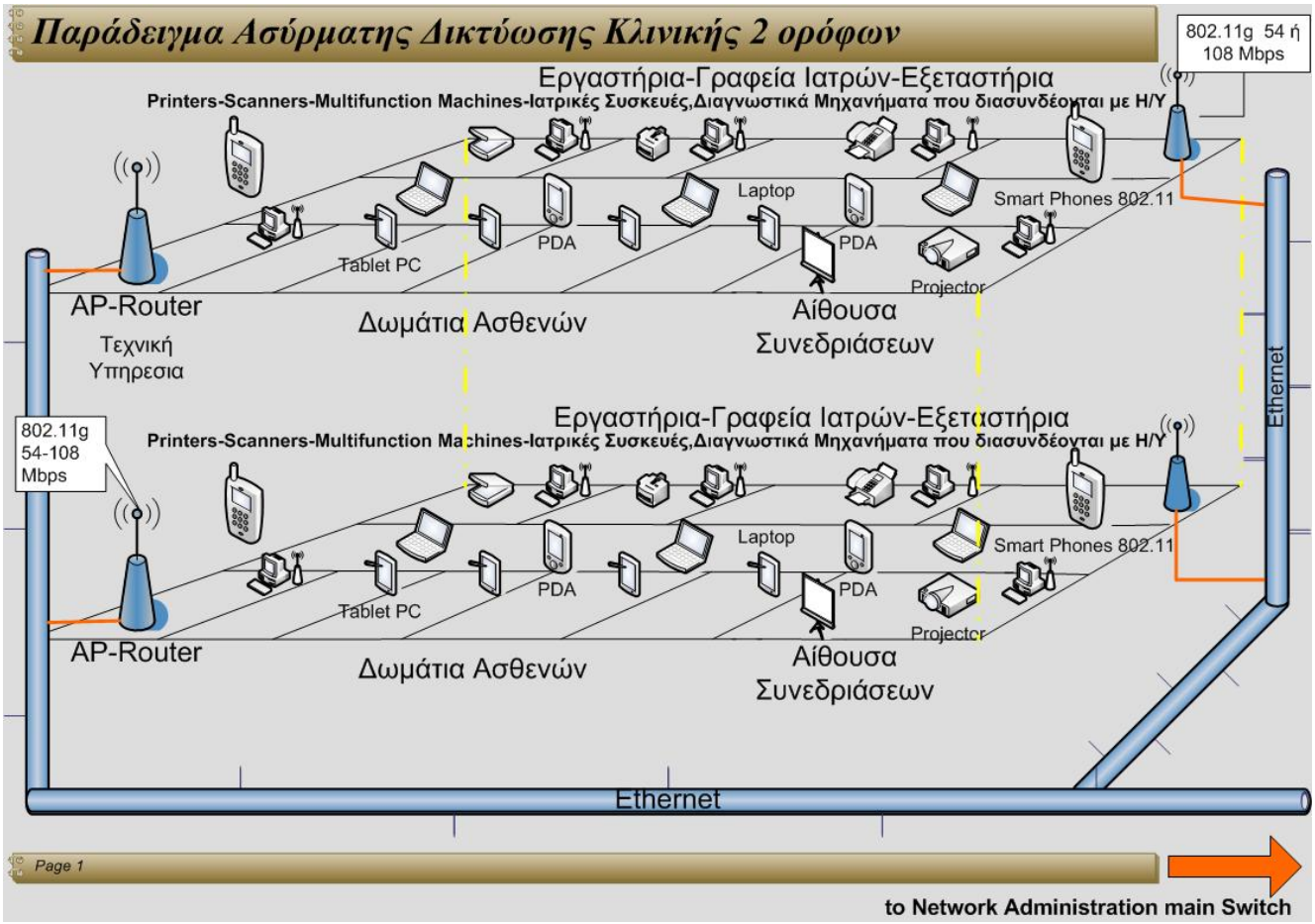
Περιορισμοί και μειονεκτήματα εντοπίζονται, όπως αναφέρθηκε και παραπάνω όταν το δίκτυο προορίζεται για ορισμένες εφαρμογές που απαιτούν πραγματικού χρόνου μεταφορά και αναπαραγωγή υψηλών προδιαγραφών Video, για τις οποίες όμως η κατηγορία του 802.11 ήδη έχει προγραμματισμένες προτάσεις για το προσεχές μέλλον κάποιες από τις οποίες , όπως το 802.11g 108 Mbps ,έχουν ήδη κυκλοφορήσει. Σημειώνεται δε ότι αντίστοιχοι ρυθμοί μεταφοράς δεδομένων επιτυγχάνονται και από τα τυπικά κατά κόρον διαδεδομένα Ethernet 10-100.

Πέρα από την ιδανική λύση που κατά την άποψή μας αποτελεί σε περιπτώσεις όπου παρουσιάζεται ανάγκη επέκτασης του ήδη προεγκατεστημένου και εν λειτουργία δικτύου ενός νοσοκομείου, όταν πρόκειται να γίνει αρχικός σχεδιασμός και εκ θεμελίων εγκατάσταση , μπορεί βεβαίως και κρίνουμε σκόπιμο να χρησιμοποιηθεί , με τον τρόπο που θα περιγράψουμε παρακάτω, αλλά δεν θα ήταν ιδανική επιλογή να αποτελέσει τον βασικό κορμό(network Backbone).Η σκοπιμότητα αυτή αφορά κυρίως τη δυνατότητα της Mobility-Roaming και της ευρείας πρόσβασης από οπουδήποτε εντός του χώρου του νοσοκομείου.

Θα μπορούσε λοιπόν ο σχεδιασμός μας να περιλάμβανε ένα δικτυακό βασικό κορμό (network Backbone) ενός ενσύρματου Ethernet υψηλών ταχυτήτων (άνω των 100Mbps) και ασύρματα υποδίκτυα καταλλήλως διανεμημένα ώστε να υπάρξει η μέγιστη δυνατή κάλυψη του χώρου. Συγκεκριμένα θα μπορούσε να σχεδιαστεί ένας βασικός κορμός πού από το κεντρικό fast Ethernet Switch του Network Administrator να επεκταθεί με καλωδίωση σε όλές τις επιμέρους κτιριακές εγκαταστάσεις .

Σχήμα 62

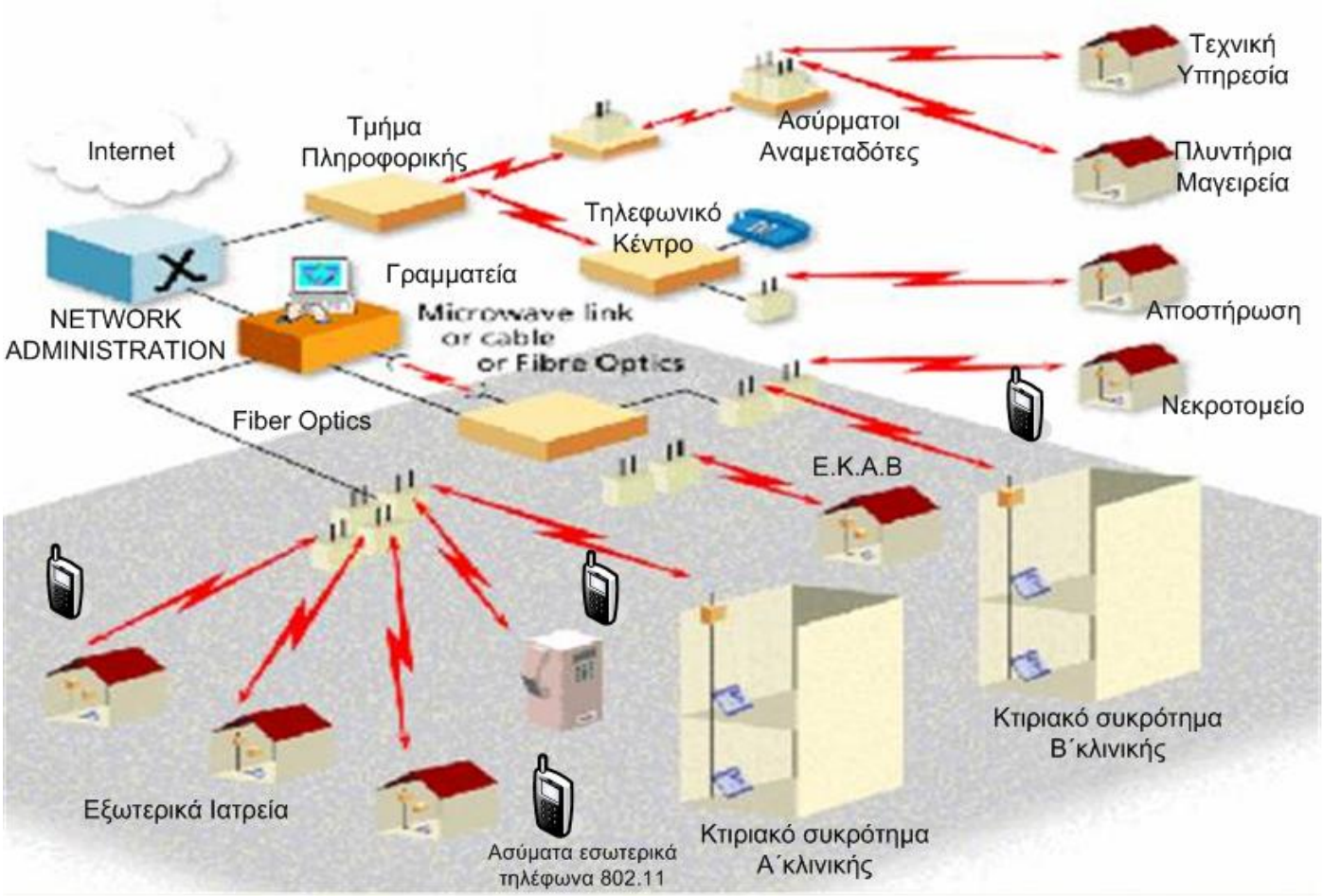
Με μια επιμελή χωροταξική μελέτη τα κτίρια –όροφοι των διαφόρων κλινικών ,τα εργαστήρια ,τα εξεταστήρια , τα χειρουργεία ,τα γραφεία των ιατρών και του προσωπικού όλων των ειδικοτήτων ,οι αποθήκες ,οι χώροι του τεχνικό προσωπικού κλπ , θα μπορούσαν να διαιρεθούν σε περιοχές κάλυψης -κυψέλες κάλυψης των σημείων πρόσβασης . Επειδή η ζώνη κάλυψης κάθε κυψέλης εξαρτάται από ισχύ εκπομπής και τη θέση κάθε σημείου πρόσβασης αλλά επίσης και από το πώς είναι δομημένο το περιβάλλον στο οποίο θα τοποθετηθεί (λόγω απορρόφησης – εξασθένισης της ισχύος του σήματος) η μελέτη θα πρέπει να γίνει προσεκτικά ,ίσως να χρειαστεί και κάποιος πειραματισμός , ούτως ώστε η διανομή των σημείων πρόσβασης να αποδώσει βέλτιστο αποτέλεσμα όσον αφορά την επίτευξη της μέγιστης και ομοιόμορφης κατανομής σήματος.



Σχήμα 63:

Ο αριθμός των κλάδων των δικτυακών καλωδιώσεων υψηλών ταχυτήτων , που μπορεί για παράδειγμα να αποτελούν οπτικές ίνες ,θα είναι περιορισμένος αναλόγως του αριθμού των Access Points που θα χρησιμοποιηθούν, στα οποία θα καταλήγουν. Επίσης με καλωδιώσεις θα μπορούσαν να έχουν πρόσβαση στο δίκτυο χώροι που για κατασκευαστικούς λόγους δεν μπορούν να καλυφθούν ασύρματα. Τέτοιοι χώροι για παράδειγμα είναι χώροι που έχουν σχεδιαστεί να φιλοξενούν ακτινολογικά μηχανήματα, γ-κάμερα, παρασκευαστήρια, χώρους χορήγησης και αποθήκες ραδιοφαρμάκων, γραμμικό επιταχυντή και συνεπώς για λόγους περιορισμού ακτινοβολίας έχουν θωρακιστεί με υλικά που ταυτόχρονα δεν επιτρέπουν την διάδοση ηλεκτρομαγνητικού σήματος.

Ασύρματος εξοπλισμός της κατηγορίας αυτής μπορεί επίσης να χρησιμοποιηθεί για ασύρματες ζεύξεις γειτονικών κτιριακών δομών του ίδιου νοσοκομειακού συγκροτήματος, αλλά και διαφορετικών νοσοκομείων εντός των ορίων μιας πόλης, όπου για ευνόητους λόγους δεν μπορούν να χρησιμοποιηθούν ενσύρματα μέσα. Η κατηγορία του 802.11 παρέχει αξιόλογο εξοπλισμό μεγάλης εμβέλειας, πχ. της τάξης των 50 Km, με ισχύ εκπομπής που φθάνει από 1 έως και 10 Watt. Μια τέτοια εφαρμογή ως γέφυρας μεταξύ νοσοκομειακών υποδομών παρέχει την δυνατότητα άμεσης ανταλλαγής δεδομένων στον ιατρικό χώρο, της κλίμακας μιας πόλης και σίγουρα θα ευνοήσει τη δημιουργία ενιαίων-κοινών βάσεων δεδομένων, γεγονός που αποτελεί μελλοντικό στόχο.



Σχήμα 64: Πρόταση για τη χρήση της κατηγορίας 802.11 σε Νοσοκομειακό περιβάλλον

ΛΕΞΙΚΟ ΟΡΩΝ-ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

AAA: Authentication and Authorization
AP: Access Point- Σημείο Πρόσβασης, σταθμός βάσης
ACK: Acknowledgment
ATM: Asynchronous Transfer Mode
Ad-hoc: Υλοποίηση Επικοινωνίας Σε Ένα Ασύρματο Δίκτυο χωρίς τη χρήση Σημείου Πρόσβασης.

Bandwidth: Εύρος Ζώνης

BSS: Basic Service Set-Βασικό Σύνολο Υπηρεσιών, κελί στην κυψελοειδή αρχιτεκτονική.
BSSID: Basic Service Set ID
BSA: Basic Service Area

CEPT: Conférence Européenne des administrations des Postes et des Télécommunications
CCA: Clear Channel Assessment
CSMA/CA: Carrier Sense Multiple Access με Collision Avoidance
CSMA/CD: Carrier Sense Multiple Access με Collision Detection

CTS: (Clear To Send): Αποστολή Δεκτή (πακέτων). Ακολουθεί το RTS

CDMA: Code Division Multiple Access
CCD:

DSSS: Direct Sequence Spread Spectrum- Τεχνική Διασποράς Φάσματος Άμεσης Ακολουθίας
Decryption: Αποκρυπτογράφηση
DS: Distribution System
DLC: Data Link Control
DIFS: Distributed Interframe Space- Κατανεμημένο δια-πλαισιακό διάστημα
DCF: Distributed Coordination Function
DSL: Digital Subscriber Line
DHCP: Dynamic Host Configuration Protocol
DECT: Digital Enhanced Cordless Telecommunications: Πανευρωπαϊκό πρότυπο επικοινωνίας μικρής εμβέλειας για ασύρματα τηλέφωνα

ESS: Extended Service Set-Εκτεταμένο Σύνολο Υπηρεσιών
Encryption: Κρυπτογράφηση
ETSI: European Telecommunications Standards Institute
EIFS: Extended Interframe Space - Εκτεταμένο δια-πλαισιακό διάστημα

ESA: Extended Service Area.

FHSS: Frequency Hopping Spread Spectrum - Τεχνική Διασποράς Φάσματος Αναπήδησης Συχνότητας
FCC: Federal Communication Commission
FDMA:
Firewalls:

GHz: Billion (Giga) cycles per second
GFSK: Gaussian Frequency Shift Key
GPRS: General Packet Radio Service
GFSK: Gaussian Frequency Shift Keying

HiPerLAN: High Performance wireless LAN

IEEE: Institute of Electrical and Electronics Engineers - Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών μηχανικών
ITU: International Telecommunication Union
IAPP:
ISO: International Standards Organization - Διεθνής Οργανισμός Τυποποίησης
ISM Band: Industrial, Scientific and Medical- Βιομηχανική, Επιστημονική και Ιατρική ζώνη
IR: Infrared
IP: Internet Protocol
Infrastructure: Υλοποίηση επικοινωνίας σε ένα ασύρματο δίκτυο, το οποίο διαθέτει ένα τουλάχιστον Σημείο Πρόσβασης που είναι συνδεδεμένο με ενσύρματο τοπικό δίκτυο.

LAN: Local Area Network
LLC: Logical Link Control
LMDS: Local Multipoint Distribution Service
MAC: Medium Access Control
Mbps: Megabit per second
MW: Microwave-Μικροκύματα
MSDU:
MMDS: Multichannel Multipoint Distribution Service

MIB : **Management Information Base**

NAV: Network Allocation Vector -Δείκτης Παραχώρησης Δικτύου
NIC: Network Interface Card
NAT:

OSI: Open Systems Interconnection
OFDM: Ορθογώνιος Πολυπλέκτης Διαίρεσης Συχνότητας

PCMCIA: Personal Computer Memory Card Interface Association
PDA: Personal Digital Assistant
PDU: Protocol Data Unit
PHY: Physical Layer
PRNG: Pseudo Random Number Generator-Ψευδοτυχαία Γεννήτρια Αριθμών
PIFS: Point Coordination Interframe Space - Δια-πλαισιακό διάστημα συντονισμού σημείου
PLM: Physical Layer Management
PLCP: Physical Layer Convergence Procedure
PMD: Physical Medium Dependent

QoS: Quality of Service

RF: Radio Frequency
Roaming: Περιαγωγή
RTS: Request To Send-Αίτηση Για Αποστολή Πακέτου

SDU: Service Data Unit
SWAP: Shared Wireless Access Protocol
SIFS: Short Interframe Space - Δια-πλαισιακό διάστημα μικρής διάρκειας
SSID: Service set identifier

TCP: Transport Control Protocol
Throughput:
TDMA: Time Division Multiple Access

WEP: Wired Equivalent Privacy- Πρωτόκολλο κρυπτογράφησης και πιστοποίησης των χρηστών
WAP: Wireless Application Protocol
Wi-Fi: Wireless Fidelity-ασύρματη πιστότητα
WLAN: Wireless Local Area Network- Ασύρματο τοπικό δίκτυο
WECA:

ΠΗΓΕΣ

www.wi-fi.org

www.cisco.com

www.80211-planet.com

http://www.wirelessethernet.org

http:// www.bluetooth.com

http:// www.hiperlan.com

http:// www.homerf.org

http://www.dell.com/r&d

http:// www.dias.aueb.gr/~gcp/wireless/notes/

http://www.sttsgroup.gr/mmds_right.htm.

http:// www.users.otenet.gr/~smylo/myseve02.htm

http:// www.noc.auth.gr/services/manuals/cryptography/#asym

http://www.cs.aueb.gr/courses/epl3600/ekpaid/ekp.htm#Simeiwseis

http://www.iec.org/online/tutorials/lmds/topic01.html

«Overview of IEEE 802.11b Security»: Sultan Weatherspoon, Network. Communications Group, Intel Corporation. Intel Technology Journal Q2, 2000.

«A Study of Wireless Compressed Digital-audio Transmission»: Andreas Floros, Marios Koutroubas, Nicolas-Alexander Tatlas and John Mourjopoulos.

«Εισαγωγή στα Ασύρματα Δίκτυα»: Δρ.Ε.Μ.Πάλλης. Έκδοση, Α.Τ.Ε.Ι Κρήτης.

«Data Over Wireless Networks Bluetooth, WAP & Wireless LANs» Gill Held Εκδόσεις, Osborne 2001.

«Wireless Broadband, Networks Handbook, 3G, LMDS & Wireless Internet» John R. Vacca. Εκδόσεις Osborne 2001.

«Wireless Access Networks» Martin P. Clark. Εκδόσεις, Wiley 2000.

«Mobilizing the Small- and Medium-sized Business» Cisco 2003.

«Encyclopedia Of Networking» (Second Edition) Werner Feibel. Εκδόσεις Network Press 1995.

«Secure Authentication, Access Control, and Data Privacy on Wireless LANs»White Paper, January 2002, Funk Software, Inc.

«IEEE 802.11 Procedures Dave Halasz and Nancy Cam-Winget »December 2002 Cisco Systems, Inc.

«Ο Ρόλος των Ασυρμάτων Τοπικών Δικτύων στις Κινητές Επικοινωνίες Τέταρτης Γενιάς - Προοπτικές, Προβλήματα και Λύσεις» Δρ. Νίκος Πασσάς Πανεπιστήμιο Αθηνών 2003.

«Operational Parameters of a Medical Wireless LAN: Security, Range and Interference issues» Konstantinos A. Banitsas, Sapal Tachakra, Robert S. H. Istepanian.

«Cisco, "*Wireless LAN Security*"», white paper, 2002.

«Technological and Economical Challenges of Public WLAN» Anand R. Prasad AAlborg University.

118