ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ

ΑΛΕΞΑΝΔΡΕΙΟ ΤΕΧΝΟΛΟΓΙΚΟ ΙΔΡΥΜΑ ΘΕΣΣΑΛΟΝΙΚΗΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΑΣΥΡΜΑΤΑ ΤΟΠΙΚΑ ΔΙΚΤΥΑ ΡΑΔΙΟΚΥΜΑΤΩΝ

ΔΗΜΗΤΡΙΟΥ Ε. ΜΑΥΡΟΜΑΤΗ

ΣΠΟΥΔΑΣΤΗ ΤΟΥ ΤΜΗΜΑΤΟΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΘΕΣΣΑΛΟΝΙΚΗ 2009

ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ

ΑΛΕΞΑΝΔΡΕΙΟ ΤΕΧΝΟΛΟΓΙΚΟ ΙΔΡΥΜΑ ΘΕΣΣΑΛΟΝΙΚΗΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΑΣΥΡΜΑΤΑ ΤΟΠΙΚΑ ΔΙΚΤΥΑ ΡΑΔΙΟΚΥΜΑΤΩΝ

ΔΗΜΗΤΡΙΟΥ Ε. ΜΑΥΡΟΜΑΤΗ

ΣΠΟΥΔΑΣΤΗ ΤΟΥ ΤΜΗΜΑΤΟΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΘΕΣΣΑΛΟΝΙΚΗ 2009

Περίληψη

Η παρούσα πτυχιακή εργασία έχει ως θέμα τα «Ασύρματα Τοπικά Δίκτυα Ραδιοκυμάτων». Το ενδιαφέρον μας εστιάζεται στο πρότυπο ασύρματης δικτύωσης IEEE 802.11. Αφού γίνει μια εισαγωγή στα ασύρματα δίκτυα και στα δομικά του στοιχεία, καθώς και στις προηγούμενες τεχνολογίες και τη μετάβαση που χρειαζόταν να γίνει από τα ενσύρματα στα ασύρματα αλλά και μια σύγκριση μεταξύ τους, έπειτα παρουσιάζονται τα πιο σημαντικά πρότυπα ασύρματων δικτύων , όπως HIPERLAN 1και 2, Bluetooth, HomeRF και αναλυτικότερα το πρότυπο IEEE 802.11 και τα υποπρότυπα 802.11a και 802.11b αλλά και η νέα τεχνολογία 802.16/WiMax .

Στην παρουσίαση κάθε προτύπου δίνουμε έμφαση στην ανάλυση των κύριων χαρακτηριστικών, του φάσματος εκπομπής, του εύρους ζώνης, των προδιαγραφών του φυσικού επιπέδου καθώς και του υποεπιπέδου ελέγχου πρόσβασης στο μέσο(MAC SubLayer), αλλά και κάποιες εφαρμογές που συναντάμε στην καθημερινή χρήση των συγκεκριμένων προτύπων ασύρματης δικτύωσης.

Μεγάλο βάρος της συγκεκριμένης εργασίας έχει πέσει στο υποεπίπεδο MAC του 802.11, όπου και αναλύονται διάφοροι μηχανισμοί που χρησιμοποιούνται από το συγκεκριμένο πρωτόκολλο. Αρχικά έχουμε τους μηχανισμούς πρόσβασης στο μέσο CSMA/CD και CSMA/CA, όπου με τον πρώτο απλά εντοπίζονται οι συγκρούσεις, ενώ με τον δεύτερο αποφεύγονται κιόλας. Στο 802.11 χρησιμοποιείται ο CSMA/CA, για τον οποίο έχουν προβλεφθεί δύο τρόποι λειτουργίας, ένας αποκεντρωμένος μέσω του αλγορίθμου DCF και ένας με κεντρικό έλεγχο μέσω του αλγορίθμου PCF που αποτελεί προέκταση του DCF. Υπάρχουν ακόμα και κάποιοι μηχανισμοί, όπως η θετική επιβεβαίωση (positive acknowledgment) κάθε πλαισίου και η ανταλλαγή πλαισίων RTS και CTS πριν τη μετάδοση κάποιου πλαισίου που χρησιμοποιούνται για να αποφευχθούν κάποια προβλήματα κακής ποιότητας της ασύρματης ζεύξης, όπως θόρυβος, παρεμβολές, πιθανότητα να βγει κάποιος κόμβος εκτός εμβέλειας δικτύου ακόμα και η ύπαρξη κρυμμένων κόμβων.

Summary

The present final work has as subject the “Wireless Local Networks of Radiowaves”. Our interest is focused in the model of wireless networking [IEEE] 802.11. After the import in the wireless networks and in his structural elements, as well as in the previous technologies and the passage that needed it becomes from wired in wireless but also a comparison from each other, then there is presented the most important models of wireless networks, as HIPERLAN 1 and 2, Bluetooth, HomeRF and more analytically the model IEEE 802.11 and the submodels 802.11a and 802.11b but also the new technology 802.16/WiMax.

In the presentation of each model we give accent in the analysis of main characteristics, the spectrum of emission, the breadth of area, specifications of natural level as well as the sub-level of control of access in means (MAC SubLayer), but also certain applications that we meet in the daily use of particular models of wireless networking.

Big weight of particular work has fallen in sub-level MAC the 802.11, where are also analyzed various mechanisms that are used by the particular protocol. Initially we have the mechanisms of access in the medium CSMA/CD and CSMA/CA, where with the first one are simply located the conflicts, while with the second they are avoided already. In the 802.11 is used the CSMA/CA, for that have been forecasted two ways of operation, one decentralized via the algorithm DCF and one with central control via algorithm PCF that it constitutes extension of DCF.

There also exist even certain mechanisms, as the positive confirmation (positive acknowledgment) for each frame and the exchange of frames RTS and CTS before the transmission of some frame that is used in order to avoid certain problems of bad quality of wireless junction, as noise, interjections, probability comes out some node except scope of network even the existence of hidden nodes.

Ευχαριστίες

Αρχικά, θα ήθελα να ευχαριστήσω τον Καθηγητή του Τμήματος Πληροφορικής του Α.Τ.Ε.Ι. Θεσσαλονίκης κ. Βασίλη Βίτσα για τη δυνατότητα που μου έδωσε να ασχοληθώ με ένα τόσο ενδιαφέρον θέμα καθώς και για την εμπιστοσύνη που μου έδειξε, καθώς και για τις πολύτιμες διορθώσεις και συμβουλές του.

Επιπλέον, θα ήθελα να ευχαριστήσω τον φίλο μου και καθηγητή Πληροφορικής και Μαθηματικών Γιώργο Μακρή για το χρόνο που διέθεσε και τη βοήθειά του στην περάτωση της διπλωματικής μου εργασίας.

Τέλος, ευχαριστώ θερμά τους γονείς μου, Λευτέρη και Μαίρη, και την αδερφή μου Χριστίνα για την αγάπη και την υποστήριξη τους.

Περιεχόμενα

1.Εισαγωγή

Ορισμός

Ασύρματο τοπικό δίκτυο (Wireless Local Area Network -WLAN) ονομάζεται ένα δίκτυο που επιτρέπει τη σύνδεση δύο η περισσότερων υπολογιστών μεταξύ τους χωρίς τη χρήση καλωδίων, πράγμα που τους δίνει τη δυνατότητα να κινούνται μέσα σε μια ευρεία περιοχή μένοντας συνδεδεμένη στο δίκτυο.

Τα WLAN δίκτυα είναι μεσαίου μεγέθους δίκτυα που βασίζονται σε ραδιοκύματα και οι μέθοδοι που χρησιμοποιεί είναι η Εξάπλωση Φάσματος και η Ορθογώνια Πολυπλέξη με Διαίρεση Συχνότητας(OFDM), έτσι ώστε να κάνει εφικτή την επικοινωνία ανάμεσα σε συσκευές που βρίσκονται σε μια περιοχή περιορισμένου εύρους.

1.1 Ασύρματα Τοπικά Δίκτυα

Η τεχνολογία βάση της οποίας έχουν σχεδιαστεί τα ασύρματα δίκτυα επιτρέπει σε ένα τερματικό, δηλαδή κάποιο υπολογιστή ή οποιαδήποτε άλλη συσκευή που χρησιμοποιεί την τεχνολογία των WLAN's, να επικοινωνεί με άλλα τερματικά χωρίς τη χρήση καλωδίων. Τα ασύρματα δίκτυα παρέχουν όλα τα προνόμια των ενσύρματων τοπικών δικτύων, αλλά είναι πιο ευέλικτα, αφού δεν θέτουν περιορισμούς στην επικοινωνία «βάση γεωγραφικής θέσης» και επιπλέον έχουν αποδεσμευτεί από ακριβό και δυσκίνητο εξοπλισμό. Η ακτίνα δράσης ενός τέτοιου δικτύου είναι αρκετά μέτρα, τα οποία επιτρέπουν τη διασύνδεση ενός κτιρίου ή μίας πανεπιστημιούπολης.

Το μέσο μετάδοσης των δεδομένων στην ασύρματη δικτύωση είναι η ραδιοσυχνότητες. Τα δεδομένα προς μετάδοση μεταφέρονται σε ένα κύμα, το οποίο ονομάζεται φέρον κύμα, μέσω της διαδικασίας της διαμόρφωσης.

Οι παγκόσμιοι οργανισμοί που ασχολούνται με τη δημιουργία προτύπων θέσπισαν κάποια πρότυπα λειτουργίας στα οποία βασίζονται τα σημερινά ασύρματα τοπικά και προσωπικά δίκτυα (WLANs και WPANs).Αυτό το έκαναν για να μπορέσουν να βρουν ένα τρόπο για να επιτευχθεί η διασύνδεση ασυρμάτων τοπικών δικτύων και ο κάθε χρήστης να έχει πρόσβαση τόσο σε ασύρματα όσο και σε ενσύρματα δίκτυα. Τέτοια είναι το IEEE 802.11x, το HIPERLAN I και II, το Bluetooth, το HOME RF, κ.α. ,τα οποία θα τα αναλύσουμε και σε επόμενα κεφάλαια.

Το πιο βασικό πρόβλημα κατά τη δημιουργία ενός ασύρματου δικτύου, είναι να μπορούν πολλοί χρήστες ταυτόχρονα να έχουν πρόσβαση στο δίκτυο. Λύση σε αυτό το πρόβλημα, δίνουν τεχνικές πολλαπλής πρόσβασης, όπως είναι η Time Division Multiple Access (TDMA- πολύπλεξη χρόνου), η Frequency Division Multiple Access (FDMA- πολύπλεξη συχνότητας), και Code Division Multiple Access (CDMA-πολύπλεξη με διαίρεση κωδίκων), ή συνδυασμός αυτών (π.χ. FDMA/TDMA).

Το πλέον χρησιμοποιημένο πρότυπο για τη δημιουργία ενός ασύρματου δικτύου είναι το IEEE 802.11 (Wireless Ethernet) το οποίο καλύπτει μόνο τα δύο κατώτερα στρώματα του μοντέλου OSI:

- το Medium Access Control (MAC)
- το Physical Layer (PHY)

1.2 Δομικά στοιχεία ενός ασύρματου δικτύου (WLAN)

Ένα ασύρματο τοπικό δίκτυο αποτελείται από διάφορα στοιχεία (components) τα οποία βοηθούν στην σωστή μετάδοση, λήψη και επεξεργασία του σήματος από τον χρήστη. Στα στοιχεία αυτά συμπεριλαμβάνονται τόσο το κατάλληλο λογισμικό (software) όσο και το ανάλογο υλικό εξοπλισμού (hardware).

1.2.1 Συσκευές χρηστών (End users devices)

Η ύπαρξη τρόπου διασύνδεσης ανάμεσα στις διάφορες εφαρμογές και υπηρεσίες με τους χρήστες που χρησιμοποιούν ένα δίκτυο, είτε είναι ενσύρματο, είτε ασύρματο, είναι απαραίτητη προϋπόθεση για την σωστή λειτουργία του δικτύου αυτού. Η διασύνδεση μεταξύ χρήστη και δικτύου επιτυγχάνεται με διάφορες συσκευές, τις συσκευές χρηστών(End Users Devices). Τέτοιες συσκευές που χρησιμοποιούνται σε ασύρματα δίκτυα είναι και οι επόμενες:

- Laptop computers
- Palmtop computers
- Handheld PCs and printers
- Personal Digital Assistants (PDAs)
- Handheld printers and scanners

1.2.2 Λογισμικό Δικτύου

Σε διάφορα μέρη ενός ασύρματου δικτύου βρίσκεται κατάλληλο λογισμικό, όπως ένα σύστημα διαχείρισης δικτύου, το οποίο παρέχει διάφορες υπηρεσίες, όπως μεταφορά δεδομένων, εκτύπωση κ.ά.

Πολλά τέτοια συστήματα στηρίζονται στην ύπαρξη ενός server, στον οποίο βρίσκονται οι βασικές συσκευές λογισμικού και οι βάσεις δεδομένων στις οποίες έχουν πρόσβαση οι διάφορες συσκευές τις οποίες ελέγχει ο χρήστης. Οι συσκευές αυτές διαθέτουν το δικό τους λογισμικό, το οποίο κατευθύνει τις εντολές του χρήστη στον server.

1.2.3 Ασύρματες κάρτες δικτύου (Wireless Network Interface Card)

Για να μπορέσει ένα ψηφιακό σήμα να διαμορφωθεί, να ενισχυθεί και να μεταδοθεί από ένα ασύρματο μέσο ενός υπολογιστή σε ένα άλλο, είναι απαραίτητες οι ασύρματες κάρτες δικτύου. Οι κάρτες αυτές, συνδέονται μέσω ενός διαύλου με τη συσκευή του χρήστη. Οι δίαυλοι που χρησιμοποιούνται για να επιτευχθεί αυτή η διασύνδεση είναι οι ISA (Industry Standard Architecture) και PCMCIA (Personal Computer Memory Card International Association), ενώ τελευταία μερικές εταιρίες παράγουν κάρτες οι οποίες συνδέονται με τον υπολογιστή μέσω μιας RS-232 σειριακής ή παράλληλης θύρας. Για την σύνδεση της ασύρματης κάρτας με τη συσκευή του χρήστη, απαιτείται ένας οδηγός λογισμικού (software driver), που συνδέει το λογισμικό του NOC στην κάρτα. Τα κυριότερα Standards για τους παραπάνω οδηγούς είναι τα εξής:

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

1.2.4 Ασύρματες Τοπικές Γέφυρες (Wireless Local Bridges)

Οι τοπικές γέφυρες συμβάλλουν στη διαμόρφωση ενός εκτενέστερου κ πιο λειτουργικού δικτύου, αφού μπορούν και συνδέουν πολλά LANs μεταξύ τους στο επίπεδο του υποστρώματος MAC,αποτελώντας ένα σημαντικό μέρος της τοπολογίας ενός δικτύου.

Οι γέφυρες χωρίζονται σε δύο είδη:

- **Local bridges :** Συνδέουν τοπικά δίκτυα που βρίσκονται σε κοντινή απόσταση
- **Remote bridges:** Συνδέουν δίκτυα που χωρίζονται από αποστάσεις μεγαλύτερες από αυτές που μπορούν να υποστηρίξουν τα πρωτόκολλα

των τοπικών δικτύων. Στην ορολογία των ασύρματων δικτύων οι γέφυρες αναφέρονται ως APs (Access Points), τα οποία είναι συσκευές απαραίτητες για τη διασύνδεση ενός WLAN με ένα ενσύρματο δίκτυο, αλλά και τη διασύνδεση πολλών WLAN μεταξύ τους.

1.2.5 Κεραίες (Antennas)

Η κεραία εκπέμπει το διαμορφωμένο σήμα μέσω του αέρα, ώστε αυτό να φτάσει στον προορισμό του. Γενικά, οι κεραίες διακρίνονται σε πολλά είδη και μεγέθη και χαρακτηρίζονται από τις παρακάτω παραμέτρους:

- Μοντέλο διάδοσης (propagation pattern)
- Ευαισθησία - Κέρδος (Gain)
- Ισχύς μετάδοσης (Transmit power)
- Εύρος ζώνης (Bandwidth)

Το μοντέλο διάδοσης μιας κεραίας καθορίζει την περιοχή κάλυψης (coverage area) της κεραίας. Για τη μετάδοση του σήματος στα WLAN χρησιμοποιούνται κυρίως δύο είδη κεραιών:

- **Πολυκατευθυντική (omnidirectional) κεραία:** μία τέτοια κεραία διοχετεύει την ισχύ της προς κάθε κατεύθυνση.
- **Μονοκατευθυντική (directional) κεραία**: αυτός ο τύπος κεραίας συγκεντρώνει το μεγαλύτερο μέρος της ισχύος της σε μία μόνο κατεύθυνση.

1.3 Λόγοι ανάπτυξης και χρησιμότητα WLAN- Εξάπλωση WLAN's

Σε αυτήν την ενότητα θα θέλαμε να παραθέσουμε κάποιους από τους πιο σημαντικούς λόγους για τους οποίους αναπτύχτηκαν αρχικά και στην συνέχεια εξαπλώθηκαν με αρκετά γρήγορο ρυθμό και μπήκαν ακόμα και στην καθημερινή μας ζωή.

Τα ασύρματα δίκτυα αν και προορίζονταν αρχικά για αντικατάσταση των ενσύρματων δικτύων ωστόσο είναι ένα συμπλήρωμα στα σταθερά δίκτυα, και όχι μια τεχνολογία αντικατάστασης. Κάτι παρόμοιο είχε γίνει και με τα κινητά τηλέφωνα, τα οποία συμπλήρωναν την τηλεφωνία σταθερών γραμμών. Εδώ τα ασύρματα δίκτυα συμπληρώνουν τα υπάρχοντα σταθερά τοπικά δίκτυα (LAN's) με την παροχή κινητικότητας στους χρήστες. Οι υπολογιστές πρέπει να έχουν πρόσβαση στα δεδομένα, δηλαδή στους εξυπηρετητές, αλλά η φυσική θέση των εξυπηρετητών δεν μας απασχολεί. Εφ' όσον δεν κινούνται οι κεντρικοί υπολογιστές, μπορούν να συνδεθούν στην ενσύρματη υποδομή. Στο άλλο όμως άκρο, τα ασύρματα δίκτυα πρέπει να σχεδιαστούν για να καλύψουν μεγάλες περιοχές προκειμένου να φιλοξενήσουν γρήγορα κινούμενους πελάτες.

Τα ασύρματα τοπικά δίκτυα μπορούν να χρησιμοποιηθούν μέσα στο χώρο μιας επιχείρησης, ενός εκπαιδευτικού οργανισμού, μιας δημόσιας υπηρεσίας κτλ, για την επικοινωνία των υπολογιστών χωρίς τη χρήση και το κόστος της δομημένης καλωδίωσης. Με τον τρόπο αυτό πετυχαίνουμε την επέκταση του ήδη υπάρχοντος δικτύου με αμελητέο κόστος και υποδομή. Επίσης μπορούμε να κάνουμε χρήση ασύρματης τηλεφωνίας για επικοινωνία μεταξύ χρηστών ή ακόμα ασύρματων καμερών για παρακολούθηση κτιρίων χρησιμοποιώντας το ήδη υπάρχον ασύρματο δίκτυο. Αυτό σημαίνει ότι οι χρήστες μπορούν να χρησιμοποιήσουν το ασύρματο δίκτυο για τις ακόλουθες εργασίες: Πλοήγηση στο Διαδίκτυο (web surfing), ανταλλαγή αρχείων και ζωντανή επικοινωνία μεταξύ των χρηστών, πρόσβαση σε εφαρμογές πολυμεσικού περιεχομένου (multimedia), για τη λήψη εικόνων, διαδραστικού βίντεο και μουσικής, λήψη ενημερωτικού ή εκπαιδευτικού περιεχομένου κτλ.

Τα ενσύρματα δίκτυα σήμερα προσφέρουν πολύ μεγαλύτερους ρυθμούς μετάδοσης, μεγαλύτερη ασφάλεια, αλλά και σχετική ευκολία εγκατάστασης, αφού τα περισσότερα κτήρια σήμερα διαθέτουν τη σχετική δομημένη καλωδίωση. Σε αντίθεση με τα ασύρματα δίκτυα που διαθέτουν πολύ μικρότερη ταχύτητα και αξιοπιστία, λόγω παρεμβολών και ασφάλειας δεδομένων στο ασύρματο μέσο.

Ένα από τα βασικά πλεονεκτήματα των ασύρματων δικτύων είναι η κινητικότητα. Τα ασύρματα δίκτυα υπολογιστών απελευθερώνουν τους χρήστες από το καλώδιο Ethernet και το γραφείο τους. Μπορούν πλέον να δουλεύουν οπουδήποτε και αν βρίσκονται, αρκεί να είναι εντός της περιοχής κάλυψης του σταθμού πρόσβασης που σήμερα έχουν τη δυνατότητα να καλύψουν μεγάλες εκτάσεις με την κατάλληλη υποδομή (κεραίες, σταθμούς πρόσβασης).

Ένα άλλο βασικό πλεονέκτημα είναι η ευελιξία που διαθέτουν. Τα ασύρματα δίκτυα προσαρμόζονται εύκολα, ανάλογα με τις κατά καιρούς απαιτήσεις των χρηστών κάτι που επιφέρει σημαντική εξοικονόμηση χρημάτων. Επίσης η προσθήκη νέων χρηστών είναι πολύ ανώδυνη ως αμελητέα εργασία αφού τις περισσότερες φορές δεν χρειάζεται να κάνουμε οτιδήποτε. Επιπλέον τα ασύρματα δίκτυα μειώνουν το κόστος διασύνδεσης χρηστών στο δίκτυο δεδομένων και διευκολύνουν την διαδικασία πρόσβασης.

Τέλος τα ασύρματα δίκτυα έχουν φέρει αλλαγή στον τρόπο επικοινωνίας των υπολογιστών, αλλά και των χρηστών τους. Με την αύξηση του αριθμού των συσκευών που αλληλεπιδρούν με τους υπολογιστές τα ασύρματα δίκτυα μπορούν να προσφέρουν λύσεις, οι οποίες βελτιώνουν την επικοινωνία και αυξάνουν την αποδοτικότητα π.χ. σε ένα εργασιακό χώρο όπως μια εταιρεία, μια τράπεζα αλλά και μια σχολική μονάδα ή σε ένα νοσοκομείο.

1.4 Αναγκαίες Προϋποθέσεις

Ένα ασύρματο δίκτυο θα πρέπει να πληροί ορισμένες αναγκαίες προϋποθέσεις, όπως της υψηλής χωρητικότητας, της ικανότητας κάλυψης μικρών αποστάσεων, της πλήρους συνδεσιμότητας και της δυνατότητας εκπομπής (broadcasting). Επιπρόσθετα, υπάρχουν και μερικές άλλες

προϋποθέσεις, που θα πρέπει να πληρούνται αποκλειστικά από τα ασύρματα τοπικά δίκτυα. Παρακάτω παραθέτουμε τις περισσότερο σημαντικές:

- **Αποδοτική χρήση του μέσου μετάδοσης:** Το πρωτόκολλο ελέγχου πρόσβασης στο μέσο(MAC), θα πρέπει να κάνει όσο το δυνατόν αποδοτικότερη χρήση του ασύρματου μέσου μετάδοσης, έτσι ώστε να μεγιστοποιείται η χωρητικότητα.
- **Αριθμός Κόμβων:** Τα ασύρματα δίκτυα θα πρέπει να μπορούν να υποστηρίζουν συνδέσεις σε τοπικό δίκτυο μέχρι και εκατοντάδων κόμβων διαμέσου πολλών κελιών.
- **Σύνδεση σε ραχοκοκαλιά τοπικού δικτύου:** Στις περισσότερες περιπτώσεις είναι απαραίτητο το ασύρματο δίκτυο να μπορεί να διασυνδεθεί με σταθμούς εργασίας που βρίσκονται σε κάποιο τοπικό δίκτυο «ραχοκοκαλιάς». Για δομημένα ασύρματα δίκτυα αυτό μπορεί εύκολα να επιτευχθεί με τη χρήση υπομονάδων ελέγχου, οι οποίες συνδέονται και στους δύο τύπους τοπικών δικτύων. Είναι επίσης πιθανό να πρέπει να προβλεφθεί και η περίπτωση εξυπηρέτησης «κινητών» χρηστών καθώς επίσης και περιπτώσεις Ad Hoc δικτύωσης.
- **Περιοχή Εξυπηρέτησης (Service area):** Ένα συνηθισμένο ασύρματο τοπικό δίκτυο θα πρέπει να μπορεί να εξυπηρετήσει χρήστες, που βρίσκονται σε διάμετρο από 100 μέχρι 300 μέτρα από τους κεντρικούς υπολογιστές.
- **Οικονομική κατανάλωση ενέργειας μπαταρίας:** Οι «κινητοί» χρήστες χρησιμοποιούν φορητούς υπολογιστές οι οποίοι χρειάζεται να έχουν μια αρκετά μεγάλη διάρκεια ζωής μπαταρίας. Αυτό υπονοεί ότι ένα πρωτόκολλο ελέγχου πρόσβασης στο διαμοιραζόμενο μέσο (MAC protocol), δε θα απαιτεί από τους κινητούς κόμβους να εποπτεύουν συνεχώς τα σημεία πρόσβασης στο μέσο, όπως συμβαίνει στα κλασσικά πρωτόκολλα MAC, έτσι ώστε να εξοικονομείται όσο το δυνατόν περισσότερη ενέργεια για περισσότερο ουσιαστικές λειτουργίες.

1.5 Προηγούμενες τεχνολογίες και μετάβαση στα ασύρματα δίκτυα

Η ιδέα της ψηφιακής ασύρματης τεχνολογίας δεν είναι καινούρια. Ο Ιταλός φυσικός Γουλιέλμος Μαρκόνι το 1901 επέδειξε στο κοινό έναν ασύρματο τηλέγραφο. Ο τηλέγραφος αυτός χρησιμοποιούσε κώδικα μορς κ επιτύγχανε επικοινωνία ανάμεσα στα πλοία και την ξηρά. Αυτό υπήρξε το εφαλτήριο για μία σειρά ανακαλύψεων, εφευρέσεων και ιδεών που οδήγησαν τα ασύρματα τοπικά δίκτυα όπως είναι στη σημερινή τους μορφή.

Η πρώτη δικτυακή επικοινωνία που αναπτύχθηκε παγκοσμίως ήταν το 1970 στο Πανεπιστήμιο της Χαβάη, με την επίβλεψη του Norman Abramson. Αυτή χρησιμοποιούσε ερασιτεχνικά ραδιόφωνα (ham-like) χαμηλού κόστους και ονομάστηκε ALOHAnet. Η αμφίδρομη τοπολογία αστέρα του συστήματος περιελάμβανε επτά υπολογιστές διασκορπισμένους σε τέσσερα νησιά, οι οποίοι επικοινωνούσαν με τον κεντρικό υπολογιστή στα νησί Oahu χωρίς τη χρήση τηλεφωνικών γραμμών.

Η πρώτη ουσιαστική παρουσίαση τοπικού ασύρματου δικτύου έγινε το 1979, όταν οι F.R Gfeller και U. Baspst δημοσίευσαν μία εργασία στα πρακτικά του IEEE. Το δίκτυο αυτό βρισκόταν σε πειραματικό στάδιο και χρησιμοποιούσε την υπέρυθρη ακτινοβολία για την επικοινωνία. Μέσα σε σύντομο χρονικό διάστημα όμως, το 1980, ο P. Ferrert υπέβαλε μία έκθεση σχετικά με μία πειραματική εφαρμογή για ασύρματη επικοινωνία μεταξύ τερματικών στο εθνικό συνέδριο τηλεπικοινωνιών του IEEE , που χρησιμοποιούσε την τεχνική της εξάπλωσης φάσματος(Spread Spectrum). Το 1984 στο Συμπόσιο για τα Δικτύων Υπολογιστών του IEEE δημοσιεύτηκε από τον Kaveh Pahlavan μία σύγκριση ανάμεσα στα συστήματα επικοινωνίας, που χρησιμοποιούν τις υπέρυθρες ακτινοβολίες και CDMA εξάπλωση φάσματος, για τα ασύρματα πληροφοριακά δίκτυα, η οποία αργότερα δημοσιεύτηκε στο Communication Society περιοδικό του IEEE.

Το Μάιο του 1985, οι προσπάθειες του Marcus οδήγησαν την FCC να ορίσει πειραματικές ISM ζώνες για εμπορική εφαρμογή της τεχνολογίας Εξάπλωσης Φάσματος (Spread Spectrum). Αργότερα, ο M. Kavehrad

δημοσίευσε μία έκθεση σχετικά με ένα πειραματικό ασύρματο PBX σύστημα, που χρησιμοποιούσε Πολλαπλή Πρόσβαση με Διαίρεση Κώδικα (CDMA). Αυτές οι προσπάθειες παρακίνησαν σημαντικές βιομηχανικές δραστηριότητες στην ανάπτυξη μιας νέας γενιάς ασύρματων τοπικών δικτύων και αυτό είχε ως συνέπεια με τη σειρά του, τον εμπλουτισμό και ανανέωση διαφόρων παλαιών συζητήσεων σχετικών με τη φορητή και κινητή βιομηχανία.

Η πρώτη γενιά των ασύρματων modems αναπτύχθηκε στις αρχές της δεκαετίας του ’80 από τους λεγόμενους “ amateur radio” χειριστές. Πρόσθεσαν ένα modem για την επικοινωνία μέσω μιας μπάντας συχνοτήτων φωνητικών δεδομένων , με συχνότητες δεδομένων κάτω από τα 9600 bps , σε ένα ήδη υπάρχον μικρής εμβέλειας σύστημα ραδιοφώνου. Η δεύτερη γενιά των ασύρματων modems αναπτύχθηκε αμέσως μετά από την ανακοίνωση της FCC σχετικά με τις πειραματικές ζώνες συχνοτήτων, η οποία επέτρεπε την μη-στρατιωτική χρήση της τεχνολογίας Εξάπλωσης Φάσματος. Αυτά τα modems παρείχαν συχνότητες της τάξης των εκατοντάδων kbps. Ενώ η τρίτη γενιά των ασύρματων modems στόχευσε στη συμβατότητα των υπαρχόντων τοπικών δικτύων με συχνότητες της τάξης των Mbps.

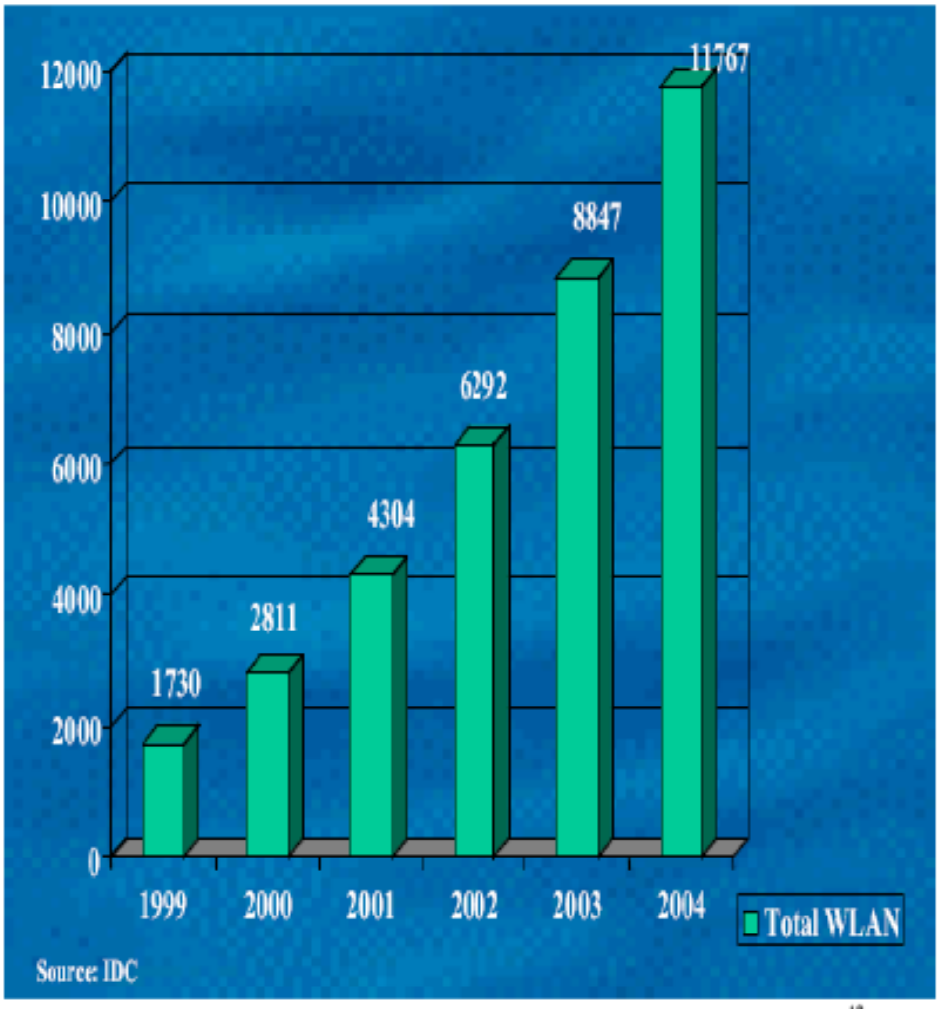
Το πρώτο από τα συνέδρια για ασύρματα τοπικά δίκτυα του IEEE(IEEE Workshop) πραγματοποιήθηκε το 1991. Εκείνη ακριβώς την περίοδο τα “πρόωρα” προϊόντα για τα ασύρματα τοπικά δίκτυα είχαν κάνει μόλις την εμφάνισή τους καθώς και η επιτροπή του IEEE 802.11 είχε μόλις αρχίσει της δραστηριότητες της για την ανάπτυξη προτύπου για τα ασύρματα τοπικά δίκτυα. Το πρώτο αυτό συνέδριο είχε εστίασε στην αξιολόγηση των εναλλακτικών τεχνολογιών. Μέχρι το 1996, η τεχνολογία είχε σχετικά ωριμάσει, είχε καθοριστεί μία ποικιλία εφαρμογών και είχαν κατανοηθεί πλήρως οι τεχνολογίες που επέτρεπαν αυτές τις εφαρμογές. Αυτή την εποχή, στην αγορά ήταν αναδυόμενα τα σύνολα των ολοκληρωμένων, που στόχευαν στην υλοποίηση και στις εφαρμογές των ασύρματων τοπικών δικτύων. Τα ασύρματα τοπικά δίκτυα είχαν εδραιωθεί πλέον στη καθημερινή ζωή και χρησιμοποιούνταν στα νοσοκομεία, στις πανεπιστημιουπόλεις, καθώς και στα διάφορα κτήρια με σκοπό την μαζική πρόσβαση και επικοινωνία. Ένα ακόμη γεγονός που αποδεικνύει την άνθιση των WLANs σε αυτή την περίοδο, είναι ότι το πρωτόκολλο του IEEE 802.11 και οι παραλλαγές του είχαν σημειώσει ραγδαία εξέλιξη.

Στις 21 Ιουλίου του 1999, πρωτοεμφανίστηκε το AirPort στην πόλη της Νέας Υόρκης από τον Steve Jobs, ένα ασύρματο τοπικό δίκτυο που βασίζεται στο πρωτόκολλο του IEEE 802.11b. Οι καταναλωτές το επιδοκίμασαν καθώς συνειδητοποίησαν την χρηστικότητα της μη ύπαρξης καλωδίων. Αυτή ήταν η πρώτη φορά που τα ασύρματα τοπικά δίκτυα έγιναν δημόσια διαθέσιμα στους ιδιώτες καταναλωτές για προσωπική χρήση. Πριν από τη δημοσίευση του AirPort, η ιδιωτική χρήση των WLANs ήταν πολύ ακριβή για τους καταναλωτές και αυτό είχε ως αποτέλεσμα την αποκλειστική τους χρήση σε εγκαταστάσεις μεγάλων εταιριών.

Σε αυτό συνέβαλε η ακριβή εγκατάσταση του υλικού που απαιτούνταν για ένα ασύρματο δίκτυο και χρησιμοποιήθηκε μόνο ως εναλλακτική λύση του ενσύρματου σε περιοχές που η καλωδίωση ήταν δύσκολη ή αδύνατη. Η ανάπτυξη των ασύρματων δικτύων ήταν ακόμα σε πρώιμη κατάσταση και περιελάμβανε πρωτόκολλα ιδιοκτησίας και προσαρμοσμένες λύσεις στην βιομηχανία. Στα τέλη όμως της δεκαετίας του 1990 αυτά αντικαταστάθηκαν από πρότυπα, κυρίως διαφόρων εκδόσεων του IEEE 802.11.

Στις μέρες μας, ο ρόλος των ασύρματων τοπικών δικτύων έχει εδραιωθεί στην καθημερινή μας ζωή. Έχει εξελιχθεί και εξακολουθεί να εξελίσσεται συνεχώς με ραγδαίους ρυθμούς. Στην εποχή μας πρωταγωνιστικό ρόλο παίζει η τεχνολογία WiMax, που βασίζεται στο πρότυπο 802.16.

Παρακάτω παρουσιάζεται ένα ραβδόγραμμα, ενδεικτικό της εξέλιξης αυτής.



Σχήμα 1.5 Εξέλιξη των WLAN

1.6 Πλεονεκτήματα-Μειονεκτήματα WLAN's σε σύγκριση με τα ενσύρματα LAN

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

- **Κινητικότητα (Mobility) χρηστών:** Το προφανέστερο πλεονέκτημα που προσφέρει ένα WLAN. Για να το εκμεταλλευτεί ο χρήστης πρέπει φυσικά να διαθέτει το αντίστοιχο κινητό τερματικό (για παράδειγμα laptop με κάρτα ασύρματης δικτύωσης). Αυτό σημαίνει ότι ο χρήστης μπορεί να κινηθεί στην εμβέλεια που προσφέρει το δίκτυο, χωρίς να αποσυνδεθεί από αυτό.

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

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

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

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

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

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

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

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

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

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

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

1.7 Εφαρμογές Των Ασυρμάτων Δικτύων

Όπως αναφέραμε και προηγουμένως κατά την αρχική περίοδο της ανάπτυξής τους τα ασύρματα δίκτυα προορίζονταν ως αντικαταστάτες των ενσύρματων. Αυτό σήμερα έχει αλλάξει. Τα ενσύρματα δίκτυα προσφέροντας πολύ μεγαλύτερους ρυθμούς μετάδοσης, μεγαλύτερη ασφάλεια αλλά και σχετική ευκολία εγκατάστασης (τα σύγχρονα κτίρια διαθέτουν σχεδόν πάντα τη σχετική καλωδίωση) δεν πρόκειται να αντικατασταθούν εξολοκλήρου. Τα ασύρματα δίκτυα έχουν σήμερα τέσσερις βασικές εφαρμογές.

- **Επέκταση των ενσύρματων LAN :** Τα ασύρματα δίκτυα χρησιμοποιούνται για τη διασύνδεση των χρηστών με το βασικό κορμό (backbone) του ενσύρματου δικτύου. Έτσι δεν απαιτείται η ύπαρξη καλωδίωσης μέχρι τον τελικό χρήστη, που μπορεί να είναι δύσκολο και οικονομικά ασύμφορο να εγκατασταθεί.

- **Διασύνδεση μεταξύ κτιρίων :** Είναι δυνατόν με την τεχνολογία των ασυρμάτων δικτύων να κατασκευαστούν ζεύξεις μεταξύ κτιρίων. Οι συσκευές που συνδέονται στα δύο άκρα της ζεύξης είναι συνήθως δρομολογητές (routers) ή γέφυρες (bridges).
- **Σποραδική πρόσβαση στο δίκτυο :** Ασύρματα δίκτυα μπορούν να εγκατασταθούν σε χώρους όπου κινούνται διάφοροι χρήστες ελεύθερα, όπως σε βιβλιοθήκες, εκπαιδευτικά ιδρύματα ή χώρους εργασίας, για να προσφέρουν πρόσβαση στο ενσύρματο δίκτυο του εκάστοτε οργανισμού. Σημαντικό θέμα σε αυτήν την περίπτωση είναι φυσικά η ασφάλεια των δεδομένων. Ακόμη είναι δυνατόν να εγκατασταθούν και σε σημεία υψηλής κίνησης, όπως αεροδρόμια, εμπορικά καταστήματα, συνεδριακά κέντρα, σημεία ψυχαγωγίας, ώστε να προσφέρουν ενημέρωση, διαφήμιση, ψυχαγωγία.
- **Δημιουργία Ad – Hoc δικτύων :** Τα δίκτυα ad – hoc είναι αποκεντρωμένα peer – to – peer δίκτυα, που συνήθως δημιουργούνται για να ικανοποιήσουν άμεσα μία συγκεκριμένη ανάγκη. Τέτοια δίκτυα μπορούν να χρησιμοποιηθούν για παράδειγμα σε συνεδριακούς χώρους ή σε αίθουσες διδασκαλίας, οπότε οι συμμετέχοντες μπορούν να ανταλλάσσουν δεδομένα μέσω του προσωρινού ασυρμάτου δικτύου, χωρίς να απαιτείται οποιαδήποτε εκ των προτέρων διαμόρφωση του χώρου.

2.Περιγραφή προτύπων ασύρματων δικτύων

2.1 Λεπτομερής περιγραφή του προτύπου 802.11

2.1.1 Το πρωτόκολλο 802.11

Όσο η εξέλιξη των ασύρματων δικτύων ήταν ακόμα σε αρχικό στάδιο ανάπτυξης, υπήρχε η ανάγκη δημιουργίας κάποιου προτύπου για τα ασύρματα δίκτυα, όπως κάτι ανάλογο είχε γίνει και με τα ενσύρματα δίκτυα. Έτσι η βιομηχανία αποφάσισε ότι η επιτροπή IEEE που είχε τυποποιήσει τα ενσύρματα LAN θα αναλάμβανε να σχεδιάσει και ένα πρότυπο για τα ασύρματα LAN- WLAN.Το πρότυπο στο οποίο κατέληξε ονομάστηκε 802.11 ή το πιο γνωστό με το εμπορικό όνομα WiFi. Το προτεινόμενο πρότυπο έπρεπε να λειτουργεί με δύο τρόπους:

1.Με παρουσία ενός σταθμού βάσης

2.Με απουσία ενός σταθμού βάσης

Στην πρώτη περίπτωση όλες οι επικοινωνίες πρέπει να περνούν από το σταθμό βάσης, ο οποίος ονομάζεται σημείο πρόσβασης στην ορολογία του 802.11. Στη δεύτερη περίπτωση οι υπολογιστές απλώς μεταδίδουν ο ένας στον άλλο. Αυτός ο τρόπος λειτουργίας ονομάζεται μερικές φορές και δικτύωση ad hoc.

Η πρώτη απόφαση ήταν η ευκολότερη: πως θα ονομαζόταν το πρότυπο. Όλα τα άλλα πρότυπα για LAN είχαν αριθμούς όπως 802.1, 802.2, 802.3, μέχρι 802.10, έτσι το πρότυπο για τα ασύρματα LAN βαφτίστηκε 802.11. Οι υπόλοιπες αποφάσεις ήταν δυσκολότερες.

Πιο συγκεκριμένα, μερικές από τις πολλές προκλήσεις που έπρεπε να αντιμετωπιστούν ήταν:

- Η ανεύρεση μιας κατάλληλης ζώνης συχνοτήτων. Η οποία να είναι κατά προτίμηση διαθέσιμη σε όλο τον κόσμο
- Η αντιμετώπιση της πεπερασμένης εμβέλειας των ραδιοκυμάτων
- Η εξασφάλιση των ιδιωτικών δεδομένων των χρηστών
- Η λήψη πρόνοιας για την περιορισμένη ζωή της μπαταρίας
- Η ανησυχία για την ανθρώπινη ασφάλεια(προκαλούν καρκίνο τα ραδιοκύματα;)
- Η κατανόηση του αντίκτυπου που θα είχε η μεταφερσιμότητα των υπολογιστών
- Η υλοποίηση ενός συστήματος με επαρκές εύρος ζώνης ώστε να είναι οικονομικά βιώσιμο.

Μετά από αρκετή εργασία η επιτροπή κατέληξε το 1997 σε ένα πρότυπο που αντιμετώπιζε αυτά και άλλα ζητήματα. Το ασύρματο LAN που περιγραφόταν λειτουργούσε είτε στο 1 Mbps είτε στα 2 Mbps. Σχεδόν αμέσως κάποιοι διαμαρτυρήθηκαν ότι ήταν πολύ αργό, έτσι ξεκίνησε η δουλειά για ταχύτερα πρότυπα. Αποτέλεσμα αυτής της δουλείας ήταν τα πρότυπα 802.11a, και το 802.11b. Στη συνέχεια ακολούθησαν και άλλες του προτύπου 802.11, τις οποίες και θα εξετάσουμε σε επόμενες παραγράφους.

2.1.2 Μετάδοση στο φυσικό επίπεδο του 802.11

Η ομάδα IEEE που σχεδίασε το 802.11 καθόρισε και πέντε τεχνικές μετάδοσης για το φυσικό επίπεδο. Σε κάθε μία από αυτές τις τεχνικές γίνετε δυνατή η μετάδοση ενός πλαισίου MAC από έναν σταθμό σε έναν άλλο. Οι τεχνικές αυτές διαφέρουν μεταξύ τους και στη χρησιμοποιούμενη τεχνολογία και στις ταχύτητες που επιτυγχάνουν. Αυτές οι τεχνικές επιγραμματικά είναι οι ακόλουθες:

- Με υπέρυθρες
- Με Εξάπλωση Φάσματος με Συνεχή Αλλαγή Συχνότητας (FHSS)
- Με Εξάπλωση Φάσματος Άμεσης Ακολουθίας (DSSS)

- Με Ορθογώνια Πολύπλεξη με Διαίρεση Συχνότητας (OFDM)
- Με Εξάπλωση Φάσματος Άμεσης Ακολουθίας Υψηλού Ρυθμού Μετάδοσης (HR-DSSS)

2.1.2.1 Με υπέρυθρες

Η υπέρυθρη επιλογή χρησιμοποιεί διάχυτη μετάδοση στα 0.85 ή 0.95 micron και επιτρέπονται δύο ταχύτητες: 1 Mbps και 2 Mbps. Τα υπέρυθρα σήματα όμως δεν μπορούν να διαπεράσουν τους τοίχους, έτσι οι κυψέλες που βρίσκονται σε διαφορετικά δωμάτια είναι καλά απομονωμένες η μία από την άλλη. Ωστόσο, λόγω του χαμηλού εύρους ζώνης και του γεγονότος ότι το φως του ήλιου εξαφανίζει τα υπέρυθρα σήματα, η επιλογή αυτή δεν είναι τόσο δημοφιλής.

2.1.2.2 Εξάπλωση Φάσματος με Συνεχή Αλλαγή Συχνότητας (FHSS)

Σε αυτήν την τεχνική χρησιμοποιείται μία γεννήτρια ψευδοτυχαίων αριθμών για την παραγωγή της ακολουθίας συχνοτήτων στις οποίες μεταβαίνουν διαδοχικά οι σταθμοί. Οι σταθμοί αυτοί θα πρέπει να μένουν στην ίδια συχνότητα για μια χρονική διάρκεια, η οποία είναι μία μεταβλητή παράμετρος και ρυθμίζεται ανάλογα με τον χρόνο παραμονής στον σταθμό που θα πρέπει να είναι μικρότερος από 400 msec. Με την τεχνική αυτή επιτυγχάνεται ένας δίκαιος τρόπος εκχώρησης του φάσματος καθώς επίσης και κάποια περιορισμένη ασφάλεια, αφού ένας εισβολέας που δεν γνωρίζει την ακολουθία συχνοτήτων ή το χρόνο παραμονής δεν μπορεί να υποκλέψει τις μεταδόσεις. Είναι επίσης ανθεκτική στις ραδιοκυματικές μεταβολές.

Κύρια μειονεκτήματα αυτής της τεχνικής είναι το χαμηλό εύρος ζώνης και ότι σε μεγάλες αποστάσεις μπορεί να δημιουργήσει πρόβλημα η εξασθένηση των πολλαπλών διαδρομών.

2.1.2.3 Εξάπλωση Φάσματος Άμεσης Ακολουθίας(DSSS)

Περιορίζεται στα 1 ή 2 Mbps. Κάθε bit μεταδίδεται ως 11 θραύσματα, χρησιμοποιώντας την ονομαζόμενη ακολουθία Baker. Χρησιμοποιεί διαμόρφωση μετατόπισης φάσης στο 1 Mbaud, με μετάδοση 1 bit ανά baud για λειτουργία στο 1 Mbps και 2 bit ανά baud για λειτουργία στο 2 Mbps. Επί χρόνια ήταν απαίτηση όλος ό εξοπλισμός της ασύρματης επικοινωνίας που λειτουργούσε στις ζώνες ISM στις Η.Π.Α, να χρησιμοποιεί αυτή τη τεχνική αλλά το 2002 αυτό καταργήθηκε.

2.1.2.4 Ορθογώνια Πολυπλέξη με Διαίρεση Συχνότητας(OFDM)

Σε αυτήν την τεχνική χρησιμοποιούνται 52 διαφορετικές συχνότητες, 48 για δεδομένα και 4 για συγχρονισμό. Αυτή η διαίρεση του φάσματος σε πολλές στενές ζώνες έχει κάποια βασικά πλεονεκτήματα σε σχέση με τη χρήση μίας μόνο ευρείας ζώνης, μερικά από τα οποία είναι η καλύτερη ανοχή σε παρεμβολές στενής ζώνης και η δυνατότητα χρήσης μη συνεχόμενων ζωνών. Στην OFDM χρησιμοποιείται ένας περίπλοκος μηχανισμός κωδικοποίησης ο οποίος βασίζεται σε διαμόρφωση μετατόπισης φάσης για ταχύτητες μέχρι τα 18 Mbps και σε QAM (ορθογωνική διαμόρφωση πλάτους Quadrature amplitude modulation) για τις μεγαλύτερες ταχύτητες. Η τεχνική αυτή έχει καλή αποδοτικότητα φάσματος και καλή αντοχή στην εξασθένηση των πολλαπλών μεταδόσεων.

2.1.2.5 Εξάπλωση Φάσματος Άμεσης Ακολουθίας Υψηλού Ρυθμού Μετάδοσης (HR-DSSS)

Χρησιμοποιεί 11 εκατομμύρια θραύσματα/sec για να επιτύχει ταχύτητα 11 Mbps στη ζώνη των 2.4 GHz. Ονομάζεται και 108.11b. Οι ρυθμοί μετάδοσης των δεδομένων που υποστηρίζονται από το 108.11b είναι 1, 2, 5.5 και 11 Mbps. Ο ρυθμός μετάδοσης δεδομένων μπορεί να προσαρμοστεί δυναμικά κατά τη λειτουργία του συστήματος, ώστε να επιτευχθεί η βέλτιστη

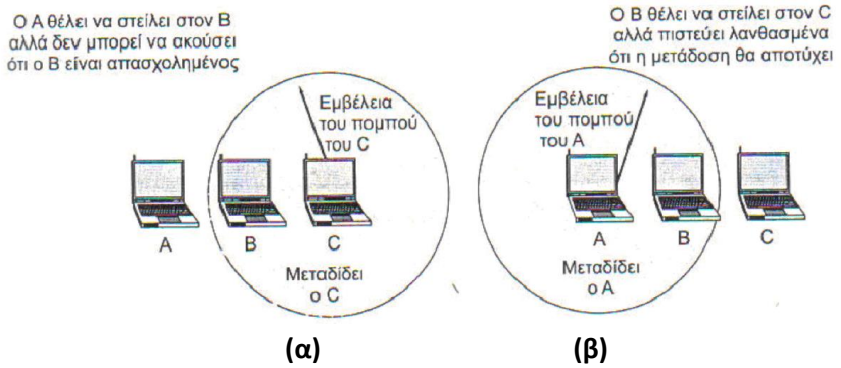
δυνατή ταχύτητα κάτω από τις τρέχουσες συνθήκες φορτίου και θορύβου. Στην πράξη η ταχύτητα του 802.11b είναι σχεδόν πάντα 11 Mbps.

2.1.3 Το πρωτόκολλο του υποεπιπέδου MAC 802.11

Σε αυτήν την ενότητα θα δώσουμε μια σύντομη περιγραφη του πρωτοκόλλου του MAC του 802.11 καθώς στο επόμενο κεφάλαιο θα μελετηθεί περισσότερο.

Το πρωτόκολλο του υποεπιπέδου του MAC του 802.11 έχει πολλές διαφορές από αυτό του Ethernet , λόγω της εγγενούς πολυπλοκότητας του ασύρματου περιβάλλοντος σε σύγκριση με ένα ενσύρματο. Υπάρχουν αρκετά προβλήματα που πρέπει να αντιμετωπιστούν.

Αρχικά, υπάρχει το πρόβλημα του κρυφού σταθμού. Αυτό δημιουργείται αφού όλοι οι σταθμοί δεν είναι εντός της εμβέλειας όλων των άλλων, οι μεταδόσεις που πραγματοποιούνται σε ένα τμήμα μιας κυψέλης μπορεί να μη λαμβάνονται σε άλλα σημεία στην ίδια κυψέλη. Στην εικόνα που φαίνεται παρακάτω όταν ένας σταθμός C μεταδίδει στο B, αν ο A ανιχνεύσει το κανάλι, δεν θα ακούσει τίποτα και θα συμπεράνει εσφαλμένα ότι μπορεί να αρχίσει να μεταδίδει στο B.



Σχήμα 2.1.3.1 (α) Το πρόβλημα του κρυφού σταθμού και

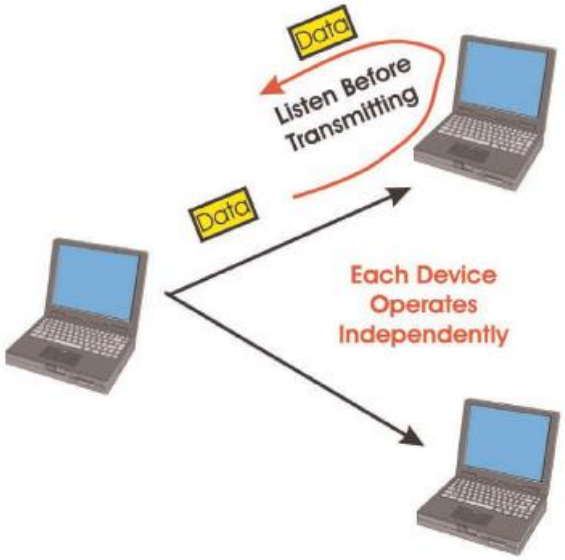
(β) Το πρόβλημα του εκτεθειμένου σταθμού

Επίσης υπάρχει το αντίστροφο πρόβλημα, το πρόβλημα του εκτεθειμένου σταθμού. Στο ανώτερο παράδειγμα-εικόνα ο Β θέλει να στείλει

στον C. Για το λόγο αυτό ακούει το κανάλι και αν ακούσει κάποια μετάδοση, βγάζει το συμπέρασμα λανθασμένα ότι δεν πρέπει να στείλει στο C, αν και ο A μεταδίδει σε κάποιον άλλο σταθμό που βρίσκεται εντός της εμβέλειας του, έστω D.

Για να αντιμετωπιστούν αυτά τα προβλήματα, το 802.11 υποστηρίζει δύο καταστάσεις λειτουργίας, την Κατανεμημένη Λειτουργία Συντονισμού (DCF) και την Σημειακή Λειτουργία Συντονισμού (PCF) που θα αναλυθούν και στο επόμενο κεφάλαιο.

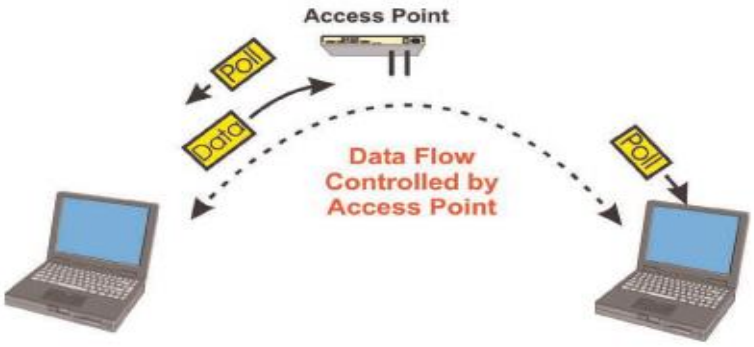
Όταν χρησιμοποιείται η DCF , το 802.11 χρησιμοποιεί το πρωτόκολλο CSMA/CA. Σύμφωνα με αυτό το, όταν ένας σταθμός θέλει να μεταδώσει, ανιχνεύει πρώτα το κανάλι και αν αυτό είναι αδρανές, τότε αρχίζει να μεταδίδει. Στη διάρκεια της μετάδοσης δεν ανιχνεύει ξανά το κανάλι, αλλά στέλνει ολόκληρο το πλαίσιο του, το οποίο μπορεί να καταστραφεί λόγω παρεμβολών στον παραλήπτη. Όταν το κανάλι είναι απασχολημένο, ο αποστολέας αναβάλλει τη μετάδοση μέχρι το κανάλι να γίνει αδρανές και τότε αρχίζει να μεταδίδει. Αν συμβεί μία σύγκρουση, οι σταθμοί που συγκρούστηκαν αναμένουν για τυχαίο χρονικό διάστημα και ξαναδοκιμάζουν αργότερα. Στην κατάσταση λειτουργίας του DCF δεν υπάρχει κεντρικός έλεγχος και οι σταθμοί ανταγωνίζονται για το κανάλι.



Σχήμα 2.1.3.2 η μέθοδος DFC

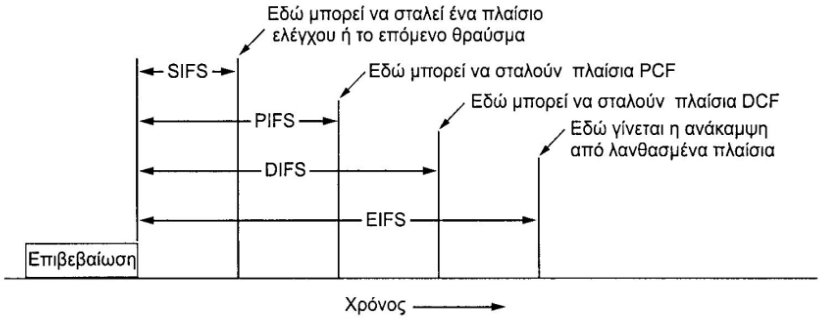
Η άλλη κατάσταση λειτουργίας είναι η PCF,σύμφωνα με την οποία ο σταθμός βάσης χρησιμοποιεί περιόδευση για τους άλλους σταθμούς, ρωτώντας τους αν έχουν κάποια πλαίσια προς αποστολή. Στην κατάσταση αυτής της λειτουργίας δεν συμβαίνουν ποτέ συγκρούσεις γιατί η σειρά

μετάδοσης ελέγχεται πλήρως από το σταθμό βάσης. Ο βασικός μηχανισμός είναι να εκπέμπει ο σταθμός βάσης περιοδικά ένα πλαίσιο φάρου, με συχνότητα από 10 έως 100 φορές ανά δευτερόλεπτο. Το πλαίσιο φάρου περιέχει παραμέτρους του συστήματος και προσκαλεί τους νέους σταθμούς να εγγραφούν στην υπηρεσία περιόδευσης. Με την εγγραφή του σταθμού στην υπηρεσία περιόδευσης για ένα συγκεκριμένο ρυθμό μετάδοσης, αυτός λαμβάνει ένα εγγυημένο ποσοστό του εύρουςζώνης. Αυτό έχει ως συνέπεια να υπάρχει εγγύηση στην ποιότητα των υπηρεσιών.



Σχήμα 2.1.3.3 Η μέθοδος PCF

Οι δύο αυτές καταστάσεις λειτουργίας, PCF και DCF, μπορούν να συνυπάρχουν μέσα σε μία κυψέλη. Αυτό αν και φαίνεται δύσκολο, επιτυγχάνεται χάρης σε μία μέθοδο επίτευξης αυτού του στόχου που παρέχεται από το πρωτόκολλο του 802.11. Σε αυτή τη μέθοδο καθορίζεται προσεκτικά το χρονικό διάστημα μεταξύ των πλαισίων. Αφού σταλθεί ένα πλαίσιο, πρέπει να περάσει ένα συγκεκριμένο διάστημα νεκρού χρόνου πριν να επιτραπεί σε οποιονδήποτε σταθμό να στείλει ένα άλλο πλαίσιο. Έχουν οριστεί τέσσερα διαφορετικά διαστήματα, το καθένα για κάποιο συγκεκριμένο σκοπό. Τα διαστήματα αυτά φαίνονται παρακάτω.



Σχήμα 2.1.3.4 Διαστήματα μεταξύ πλαισίων στο 802.11

Το μικρότερο διάστημα είναι το Βραχύ Διάστημα μεταξύ Πλαισίων (**SIFS**). Αυτό χρησιμοποιείται για να δώσει στα δύο άκρα μιας συνδιάλεξης την ευκαιρία να μεταδώσουν πρώτα. Οι περιπτώσεις που περιλαμβάνονται είναι να στέλνει ο παραλήπτης ένα μήνυμα CTS(πλαίσιο για την αποδοχή μιας αίτησης αποστολής δεδομένων) σε απάντηση ενός RTS(πλαίσιο για αίτηση άδειας με σκοπό την αποστολής δεδομένων), να στέλνει ο παραλήπτης μία επιβεβαίωση για ένα θραύσμα(τμήματα στα οποία κατακερματίζεται ένα πλαίσιο) ή ένα πλήρες πλαίσιο δεδομένων, και να στέλνει ο αποστολέας μιας ριπής θραυσμάτων το επόμενο θραύσμα χωρίς να χρειαστεί να στείλει ξανά ένα μήνυμα RTS.

Μετά το διάστημα αυτό υπάρχει πάντα ακριβώς ένας σταθμός ο οποίος έχει το δικαίωμα να απαντήσει. Αν δεν κάνει χρήση της ευκαιρίας αυτής και περάσει χρόνος ίσος με το Διάστημα PCF Μεταξύ Πλαισίων(**PIFS**), ο σταθμός βάσης μπορεί να στείλει ένα πλαίσιο φάρου ή ένα πλαίσιο περιόδευσης. Αυτός ο μηχανισμός επιτρέπει σε ένα σταθμό που στέλνει ένα πλαίσιο δεδομένων ή μία ακολουθία θραυσμάτων να ολοκληρώσει το πλαίσιο του χωρίς να μπει κανείς άλλος στη μέση, δίνει όμως επίσης στο σταθμό βάσης την ευκαιρία να καταλάβει το κανάλι μόλις τελειώσει ο προηγούμενος αποστολέας, χωρίς να χρειαστεί να ανταγωνιστεί με τους ανυπόμονους χρήστες.

Αν ο σταθμός βάσης δεν έχει τίποτα να πει και περάσει ο χρόνος ίσος με το Διάστημα DCF Μεταξύ Πλαισίων(**DIFS**), κάθε σταθμός μπορεί να προσπαθήσει να καταλάβει το κανάλι για να στείλει ένα νέο πλαίσιο. Ισχύουν οι συνηθισμένοι κανόνες ανταγωνισμού και μπορεί να χρειαστεί να εκτελεστεί δυαδική εκθετική οπισθοχώρηση αν παρουσιαστεί σύγκρουση.

Το τελευταίο χρονικό διάστημα, το Επεκτεταμένο Διάστημα Μεταξύ Πλαισίων(**EIFS**), χρησιμοποιείται μόνο από ένα σταθμό που μόλις έχει λάβει ένα λανθασμένο ή άγνωστο πλαίσιο και σκοπεύει να αναφέρει το πρόβλημα.

2.1.4 Υπηρεσίες

Το 802.11 πρότυπο καθορίζει ότι κάθε ασύρματο LAN που συμμορφώνεται με το πρότυπο πρέπει να παρέχει εννέα υπηρεσίες, οι οποίες διαιρούνται σε δύο κατηγορίες. Η πρώτη κατηγορία παρέχει πέντε υπηρεσίες

διανομής, οι οποίες σχετίζονται με τη διαχείριση των μελών μιας κυψέλης και την αλληλεπίδραση με σταθμούς εκτός κυψέλης. Αντιθέτως η δεύτερη κατηγορία παρέχει τέσσερις υπηρεσίες σταθμών, οι οποίες ασχολούνται με τις δραστηριότητες μέσα σε μία μόνο κυψέλη.

Οι πέντε υπηρεσίες διανομής παρέχονται από τους σταθμούς βάσης και ασχολούνται με τη δυνατότητα μετακίνησης των σταθμών καθώς αυτοί εισέρχονται και εγκαταλείπουν τις κυψέλες, συνδεόμενοι και αποσυνδεόμενοι από τους σταθμούς βάσης.

Οι υπηρεσίες αυτές είναι οι ακόλουθες:

1. **Συσχέτιση.** Είναι η κύρια υπηρεσία που χρησιμοποιείται από κινητούς σταθμούς ώστε να μπορέσουν να συνδεθούν με τους σταθμούς βάσης. Η συσχέτιση γίνετε μόλις ένας σταθμός μετακινηθεί εντός της εμβέλειας του σταθμού βάσης. Με την άφιξη του, ο σταθμός ανακοινώνει την ταυτότητα και τις δυνατότητές του. Οι δυνατότητες περιλαμβάνουν τους υποστηριζόμενους ρυθμούς μετάδοσης δεδομένων, την ανάγκη για υπηρεσίες PCF και τις απαιτήσεις διαχείρισης ισχύος. Ο σταθμός βάσης μπορεί να αποδεχτεί ή να απορρίψει τον κινητό σταθμό. Αν ο κινητός σταθμός γίνει αποδεκτός, θα πρέπει στη συνέχεια να πιστοποιήσει την ταυτότητά του.

2. **Αυτοσυσχέτιση.** Η υπηρεσία αυτή ουσιαστικά είναι ο τερματισμός της συσχέτισης, είτε από κάποιον σταθμό είτε από τον σταθμό βάσης. Ο σταθμός θα πρέπει να χρησιμοποιεί την υπηρεσία αυτή πριν απενεργοποιηθεί ή πριν φύγει από την κυψέλη, ενώ ο σταθμός βάσης μπορεί επίσης να τη χρησιμοποιήσει πριν απενεργοποιηθεί για λόγους συντήρησης.

3. **Επανασυσχέτιση.** Η υπηρεσία αυτή μπορεί να προσφέρει την άμεση αλλαγή του προτεινόμενου σταθμού βάσης. Αυτή η ιδιότητα βρίσκει εφαρμογή όταν έχουμε κινητούς σταθμούς που μετακινούνται από κυψέλη σε κυψέλη. Η σωστή εφαρμογή της

υπηρεσίας οδηγεί σε μηδενική απώλεια δεδομένων κατά τη μεταβίβαση.

4. **Διανομή.** Η υπηρεσία αυτή έχει δύο επιλογές να χρησιμοποιήσει για να προσδιορίσει πως θα δρομολογούνται τα πλαίσια που στέλνονται από το σταθμό βάσης. Αν ο προορισμός είναι τοπικός στο σταθμό βάσης, τα πλαίσια μπορούν να σταλούν άμεσα στην κυψέλη. Διαφορετικά, θα πρέπει να προωθηθούν μέσω του ενσύρματου δικτύου.
5. **Ενοποίηση.** Αυτή η υπηρεσία διαχειρίζεται τη μετατροπή ενός πλαισίου από μορφή 802.11 στη μορφή που απαιτείται από το δίκτυο προορισμού. Αυτό το φαινόμενο το συναντάμε όταν ένα πλαίσιο πρέπει να σταλεί μέσω ενός δικτύου δεν είναι της μορφής 802.11 και χρησιμοποιεί διαφορετική μέθοδο διευθυνσιοδότησης ή μορφής πλαισίων

Οι υπόλοιπες τέσσερις υπηρεσίες σταθμών είναι εσωτερικές στις κυψέλες και χρησιμοποιούνται αφού πραγματοποιηθεί η συσχέτιση .

Οι υπηρεσίες αυτές είναι οι ακόλουθες:

1. **Πιστοποίηση ταυτότητας**. Ο κάθε σταθμός θα πρέπει να πιστοποιήσει την ταυτότητα του πριν του επιτραπεί να στείλει τα δεδομένα και αυτό γιατί οι ασύρματες μεταδόσεις είναι εύκολο να σταλούν ή να ληφθούν από μη εξουσιοδοτημένους σταθμούς. Μόλις ένας κινητός σταθμός συνδεθεί με το σταθμό βάσης , ο σταθμός βάσης του στέλνει ένα ειδικό πλαίσιο «πρόσκλησης» για να δει αν ο κινητός σταθμός γνωρίζει το μυστικό κλειδί που του έχει εκχωρηθεί. Ο σταθμός αποδεικνύει ότι γνωρίζει το μυστικό κλειδί κρυπτογραφώντας το πλαίσιο πρόσκλησης και επιστρέφοντάς το στο σταθμό βάσης. Αν το αποτέλεσμα είναι ορθό, ο κινητός σταθμός εγγράφεται πλήρως στην κυψέλη.
2. **Ακύρωση πιστοποίηση ταυτότητας**. Η χρήση αυτής της υπηρεσίας οδηγεί στην ανικανότητα του σταθμού να χρησιμοποιήσει το δίκτυο που

ήταν συνδεδεμένος, δηλαδή είχε ήδη πιστοποιηθεί και πλέον θέλει να αγεκαταλείψει.

3. **Προστασία απορρήτου**. Η υπηρεσία αυτή διαχειρίζεται την κρυπτογράφηση και την αποκρυπτογράφηση, έτσι ώστε να διατηρούνται εμπιστευτικές οι πληροφορίες που στέλνονται μέσω ενός ασύρματου LAN. Ο αλγόριθμος κρυπτογράφησης που προσδιορίζεται είναι ο RC4, που εφευρέθηκε από τον Ronald Rivest του M.I.T.
4. **Παράδοση δεδομένων**. Τέλος, αφού η μετάδοση δεδομένων είναι ο σκοπός του δικτύου, το 802.11 είναι φυσικό να παρέχει μία μέθοδο μετάδοσης και λήψης δεδομένων. Επειδή το 802.11 ακολουθεί το μοντέλο Ethernet και η μετάδοση στο Ethernet δεν είναι εγγυημένα αξιόπιστη κατά 100%, ούτε η μετάδοση στο 802.11 είναι εγγυημένα αξιόπιστη. Τα ανώτερα επίπεδα θα πρέπει να ασχοληθούν με την ανίχνευση και την αποσφαλμάτωση.

2.1.5 Παραλλαγές

Οι παραλλαγές του 802.11 εμφανίζονται με ένα λατινικό γράμμα το οποίο προέρχεται από την ομάδα εργασίας (task group) που έκανε την αναθεώρηση του πρωτοκόλλου.

802.11c – Bridge Op Procedures

Το 802.11c παρέχει απαραίτητες πληροφορίες για να διασφαλιστεί η σωστή λειτουργία των bridges. Οι πληροφορίες που περιέχονται σε αυτό το πρωτόκολλο χρησιμοποιούνται κυρίως από τους κατασκευαστές σημείων πρόσβασης ώστε να εξασφαλίζεται η διαλειτουργικότητά τους με συσκευές άλλων κατασκευαστών.

802.11d – Global Harmonization

Το task group D έχει αναλάβει την εργασία να καθορίσει τις απαιτήσεις του φυσικού επιπέδου καθώς και να καταγράψει το νομικό πλαίσιο που ισχύει

για την χρησιμοποίηση ραδιοσυχνοτήτων σε διάφορες χώρες ώστε να μπορούν να κατασκευαστούν προϊόντα που θα λειτουργούν σε διάφορες γεωγραφικές περιοχές.

802.11e – MAC Enhancements for QoS

Χωρίς καλό QoS (Quality of Service) το αρχικό πρωτόκολλο 802.11 δεν βελτιστοποιεί την μετάδοση φωνής και video. Αυτό ακριβώς το μειονέκτημα έρχεται να καλύψει το task group E τροποποιώντας το υποεπίπεδο MAC και βελτιώνοντας το QoS του πρωτοκόλλου.

802.11f – Inter Access Point Protocol

Η αρχική ομάδα εργασίας του 802.11 σκοπίμως δεν προσδιορίζει την επικοινωνία μεταξύ σημείων πρόσβασης με σκοπό την υποστηρίξει της περιαγωγής των χρηστών από ένα σημείο πρόσβασης σε ένα άλλο. Η επιλογή αυτή δίνει ευελιξία όταν χρησιμοποιούνται διάφορα distribution system. Το πρόβλημα, όμως που ανακύπτει είναι ότι τα σημεία πρόσβασης από διαφορετικούς κατασκευαστές μπορεί να μην λειτουργούν ομαλά μεταξύ τους όταν υποστηρίζουν λειτουργίες περιαγωγής. Το 802.11f έρχεται ακριβώς σε αυτό το σημείο, να φτιάξει μια προδιαγραφή που θα παρέχει στα σημεία πρόσβασης της απαραίτητες πληροφορίες για να γίνει μια περιαγωγή με επιτυχία και να εξασφαλιστεί η ομαλή λειτουργία του συστήματος.

802.11g – Union of .11a and .11b

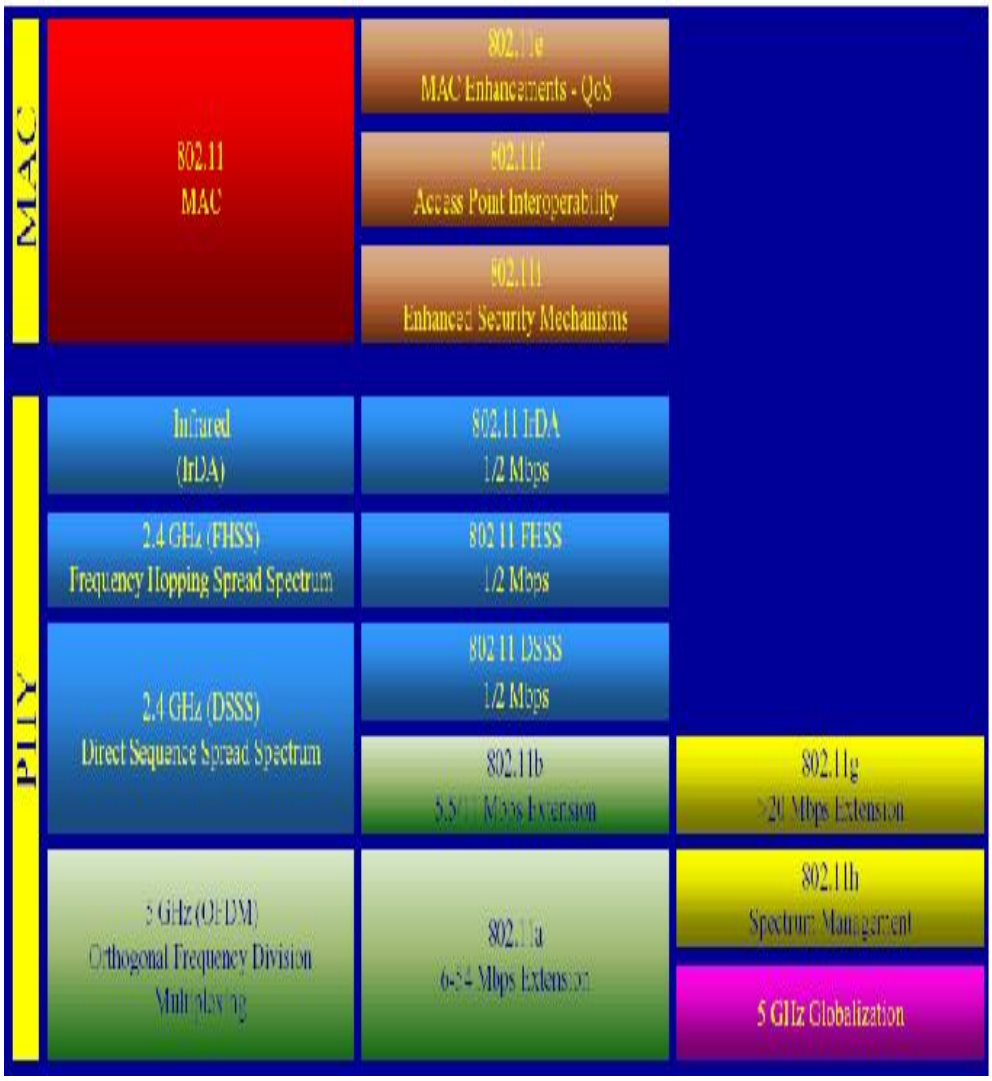
Η παραλλαγή αυτή του 802.11 έχει ως αντικείμενο εργασίας να προσφέρει ρυθμούς μετάδοσης της τάξης των 54Mbps, όπως και το 802.11a διατηρώντας όμως την συμβατότητα με το διαδεδομένο 802.11b. Λειτουργεί στην ISM ζώνη συχνοτήτων όπως το 802.11b αλλά χρησιμοποιεί διαμόρφωση OFDM όπως το 802.11a για να πετύχει υψηλούς ρυθμούς μετάδοσης. Χάριν συμβατότητας με το 802.11b υποστηρίζεται και η διαμόρφωση CCK.

802.11h – UNII for Europe

Η προδιαγραφή αυτή είναι συμπληρωματική του υποεπιπέδου MAC και συμμορφώνεται με τους ευρωπαϊκούς κανονισμούς για την χρήση της ζώνης συχνοτήτων στα 5GHz. Συγκεκριμένα οι ευρωπαϊκοί κανονισμοί απαιτούν για τις συσκευές που λειτουργούν σε αυτή την ζώνη συχνοτήτων να έχουν δυνατότητες ελέγχου εκπεμπόμενης ισχύος (Transmission Power Control) και δυναμικής επιλογής συχνότητας (Dynamic Frequency Selection).

802.11i – Enhanced Security

Η προδιαγραφή αυτή έρχεται να καλύψει πολλά από τα κενά σε θέματα ασφαλείας που βρέθηκαν στο πρωτόκολλο κρυπτογράφησης WEP του 802.11. Ο αλγόριθμος RC4 της RCA που χρησιμοποιείται αποδείχτηκε ανεπαρκής, με πολλά σφάλματα και παραλήψεις, κάνοντας τα ασύρματα δίκτυα εύκολο στόχο σε διάφορα είδη επιθέσεων. Με την νέα προδιαγραφή καθορίζονται πρωτόκολλα για τα κλειδιά κρυπτογράφησης όπως τα TKIP (Temporal Key Integrity Protocol) και AES (Advanced Encryption Standard).Στο παρακάτω σχήμα παρουσιάζονται μερικές από τις παραλλαγές του 802.11 σε σχέση με την λειτουργία τους και την θέση τους στο μοντέλο αναφοράς OSI.



Σχήμα 2.1.5 Παραλλαγές 802.11

2.2 Το πρωτόκολλο IEEE 802.11a

Το πρωτόκολλο 802.11a δημιουργήθηκε το 1999, όταν η IEEE διαπίστωσε ότι οι τηλεοπτικές, όπως και οι 'βαριές' εφαρμογές πολυμέσων θα απαιτούσαν ταχύτητες υψηλότερες από 11 Mb/s. Το πρωτόκολλο αυτό έχει βελτιστοποιηθεί για υψηλότερες αποδόσεις στα εσωτερικά περιβάλλοντα. Παρέχει ρυθμούς μετάδοσης δεδομένων μέχρι 54 Mb/s, ενώ χρησιμοποιεί την μπάντα των 5GHz. Ένας κατασκευαστής μάλιστα έχει δηλώσει ότι είναι σε

θέση να προχωρήσει το πρότυπο ώστε να υποστηρίζει ταχύτητες μέχρι 108 Mb/s, με κάποιες μικρές αλλαγές.

Το 802.11a βασίζεται στην τεχνική πολυπλεξίας OFDM (Orthogonal Frequency Division Multiplexing / Ορθογωνική Πολυπλεξία Διαίρεσης Συχνότητας). Η τεχνική της OFDM καταφέρνει να διαιρέσει τον κύριο υψηλό ρυθμό σε πολλούς μικρότερους ρυθμούς ώστε να τους χρησιμοποιήσει για να μπορεί να αποστέλλει τα δεδομένα ταυτόχρονα. Όλα τα «αργά» κανάλια πολυπλέκονται τελικά σε ένα «γρήγορο» κανάλι και μεταδίδονται. Το πλεονέκτημα αυτής της τεχνικής είναι ότι μπορεί να λύσει το πρόβλημα της σπατάλης του εύρους ζώνης, προκειμένου να διαχωρίσουμε τα κανάλια μεταξύ τους.

Τα χαμηλότερα 200 MHz υποδιαιρούνται σε οκτώ κανάλια 20 MHz το κάθε ένα (τα πρόσθετα 40 MHz χρησιμοποιούνται για το χωρισμό καναλιών) Κάθε κανάλι με τη σειρά του υποδιαιρείται σε 52 υποκανάλια, 300 KHz το κάθε ένα. Διαδοχικά υποκανάλια απέχουν μεταξύ τους 0,3125 MHz. Αυτά τα στενότερα κανάλια βελτιώνουν τη μεταφορά δεδομένων επειδή είναι λιγότερο ευαίσθητα στη διασπορά χρόνου και συχνότητας. Από τα 52 κανάλια, τα 48 χρησιμοποιούνται για δεδομένα και τα υπόλοιπα τέσσερα χρησιμοποιούνται για την ανίχνευση σφάλματος.

Κάθε κανάλι χρησιμοποιεί διαμόρφωση μετατόπισης φάσης (PSK). Το πρότυπο απαιτεί τα συμβατά συστήματα να υποστηρίζουν διαμόρφωση φάσης 90 μοιρών 2, 4 και 16 επιπέδων για κάθε κανάλι. Αυτά αντιστοιχούν σε ταχύτητες 6, 12, και 24 Mb/s αντίστοιχα.

Στις ΗΠΑ έχει κρατηθεί συγκεκριμένο τμήμα της μπάντας των 5 GHz (U-NII) για χρήση από ασύρματα δίκτυα 802.11a. Συνολικά είναι διαθέσιμα 12 κανάλια των 20 MHz.

Τα πρότυπα 802.11a και 802.11b πρέπει να είναι σε θέση να λειτουργήσουν παράλληλα στο τοπικό LAN δεδομένου ότι χρησιμοποιούν την ίδια MAC και λειτουργούν σε διαφορετικές περιοχές συχνότητας. Εντούτοις, οι διαφορές στη διάδοση μπορούν να κάνουν απαραίτητο τον επαναπροσδιορισμό των περιοχών κάλυψης τους.

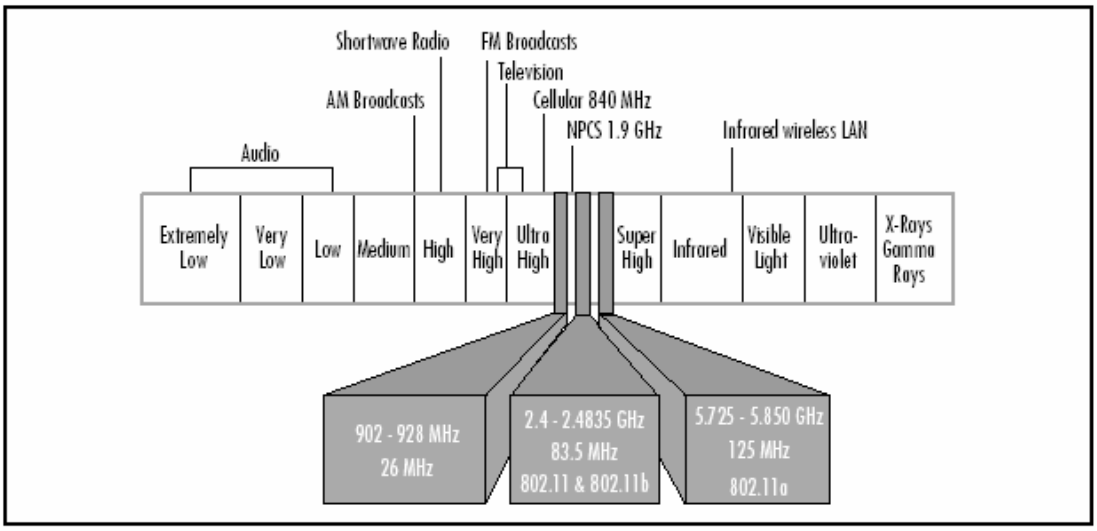
2.3 Το πρωτόκολλο IEEE 802.11b

2.3.1 Κύρια χαρακτηριστικά του πρωτοκόλλου

Το 802.11b είναι το πρώτο wireless πρωτόκολλο που κατάφερε να μπει τόσο δυναμικά στον χώρο της δικτύωσης, έναν χώρο που γνωρίζει ελάχιστες επαναστάσεις και αλλαγές. Το γράμμα b του πρωτοκόλλου 802.11b αποτελεί επέκταση και είναι ένας ορισμός του Media Access Control (MAC) Layer καθώς και τριών διαφορετικών και ασύμβατων Physical Layers στο υπάρχον δικτυακό μοντέλο του OSI. Η έγκριση του πρωτοκόλλου έγινε το στις 26 Ιουνίου του 1997 από την ομάδα 802 της IEEE, η οποία και θέτει το πλαίσιο για μια προτυποποιημένη ασύρματη επικοινωνία ευρείας ζώνης. Στις παρακάτω σελίδες δίνουμε μια περιγραφή του 802.11 πρωτοκόλλου, και επεκτείνουμε την έρευνά μας στις επεκτάσεις και τροποποιήσεις που προσέθεσε το 802.11b.

2.3.2 Φάσμα εκπομπής

Η μπάντα που χρησιμοποιεί το πρωτόκολλο για την μετάδοση των δεδομένων είναι αυτή των 2.4 GHz. Η Federal Communications Commission (FCC) είναι υπεύθυνη για την εκχώρηση μικρών περιοχών στο φάσμα των ραδιοσυχνοτήτων για να αποφεύγονται παρεμβολές από ραδιοφωνικά σήματα στις ΗΠΑ. Η χρήση οποιασδήποτε από της ζώνες που ορίζει η FCC, πρέπει να συνοδεύεται από ειδική άδεια. Η FCC παράλληλα χαρακτηρίζει ελεύθερα κάποια τμήματα του ραδιοφωνικού φάσματος. Αυτές οι μπάντες ονομάζονται ISM(Industrial Scientific and Medical) και μπορούν να χρησιμοποιηθούν χωρίς άδεια. Στο Σχήμα 2.3.2 μπορούμε να δούμε αναλυτικά το ραδιοφωνικό φάσμα και τις ελεύθερες περιοχές του.



Σχήμα 2.3.2 Οι ελεύθερες συχνότητες

Το 802.11(b) χρησιμοποιεί όπως βλέπουμε μια ελεύθερη ζώνη η οποία είναι πλήρως ελεύθερη για εκπομπή χαμηλής ισχύος. Όλα τα παραπάνω βέβαια, ισχύουν στις ΗΠΑ. Ευτυχώς και οι υπόλοιπες παρόμοιας ευθύνης οργανώσεις κάθε χώρας συμβαδίζουν, λιγότερο η περισσότερο με αυτά τα πρότυπα της FCC.

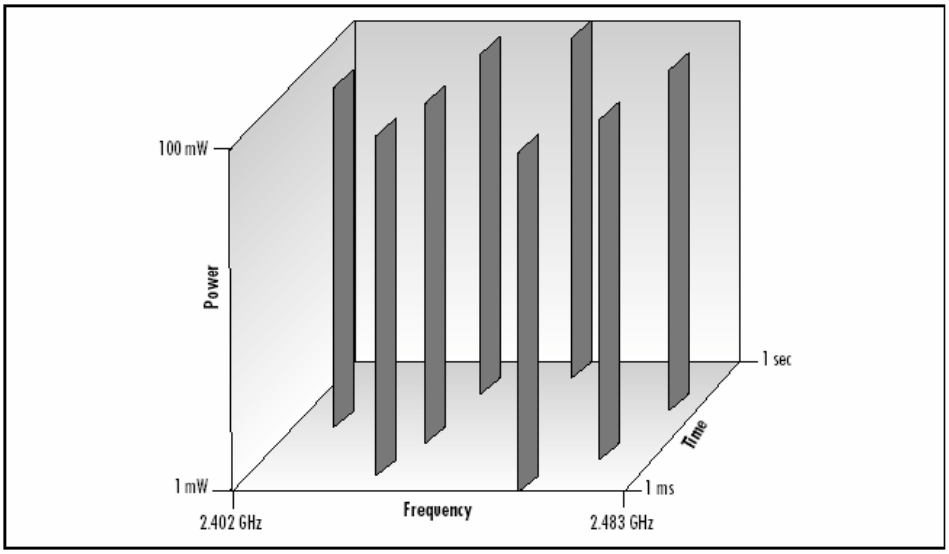
Δυστυχώς, το νομικό πλαίσιο που διέπει τις λεπτομέρειες χρήσης αυτής της μπάντας, εξαρτάται σε μεγάλο βαθμό από την νομοθεσία κάθε χώρας. Μεγάλα είναι τα νομικά κενά σε πολλές χώρες, όπως και στην Ελλάδα, που αφήνουν πολλά ερωτηματικά ως προς την μέγιστη νόμιμη εκπεμπόμενη ισχύ, την εμπορική ή όχι χρήση του ραδιοφωνικού φάσματος αυτού και πολλά άλλα. Η ισχύς που ορίζει το στάνταρτ στις εξόδους κεραίας των εμπορικών συσκευών είναι τα 0.2mw, το οποίο με τις μικρές εργοστασιακές κεραίες που συνοδεύουν τις συσκευές WiFi, δίνει στο 802.11b εμβέλεια της τάξεως των 300μ σε ανοιχτό χώρο. Λόγω της φύσης των μικροκυματικών συχνοτήτων, η εμβέλεια συσκευών WiFi μειώνεται αισθητά όταν μεταξύ τους παρεμβάλλονται τσιμέντινοι τοίχοι, δέντρα(και γενικώς αντικείμενα που περιέχουν νερό) ή μεταλλικές πόρτες. Μείωση της ποιότητας σύνδεσης, σημαίνει αρχικά μειωμένο throughput του δικτύου με υψηλά error rates, και στην χειρότερη περίπτωση αδυναμία σύνδεσης των συσκευών. Για τον ίδιο λόγο, μακρινές συνδέσεις (>300μ) επιτυγχάνονται μόνο σε καταστάσεις όπου η μία συσκευή έχει οπτική επαφή με την άλλη (Line of Site), ένας κανόνας που ευτυχώς δεν είναι τόσο αυστηρός(καταστάσεις near-LOS). Αντανακλάσεις του σήματος

μπορεί να επιτρέψουν σύνδεση χωρίς LOS. Βεβαίως, όπως είναι αναμενόμενο, για την επίτευξη ζεύξεων πολύ μεγάλων αποστάσεων, υπάρχει το φυσικό εμπόδιο της καμπυλότητας της γης. Ακόμη και αν καταφέρουμε δηλαδή να ενισχύσουμε την εκπομπή και την λήψη των 802.11 συσκευών μας, προσπαθώντας να καταστήσουμε δυνατή μια σύνδεση μεγάλης απόστασης, δεν είναι δυνατό να ξεπεράσουμε την δεδομένη μέγιστη απόσταση (~20μίλια), στην οποία η ίδια η γη εμποδίζει την οπτική επαφή.

2.3.3 Διαμόρφωση

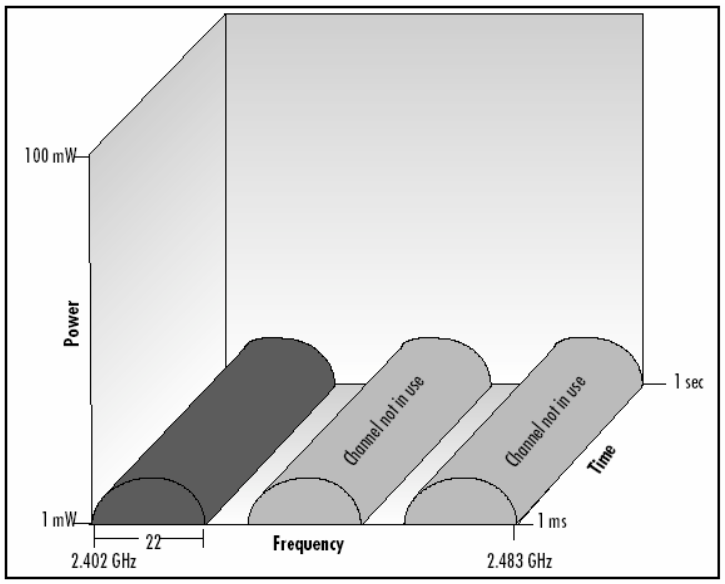
Στο αρχικό πρωτόκολλο 802.11, καθορίζονται δύο τρόποι κωδικοποίησης, ο FHSS (Frequency Hopping Spread Spectrum) και ο DSSS (Direct Sequence Spread Spectrum).

Στον FHSS η εκπομπή και η λήψη μοιράζονται σε 75 κανάλια του 1MHz και εναλλάσσονται συνεχώς σε ένα από αυτά τα κανάλια. Σε αυτή τη τεχνική ο εκπομπός στέλνει τα δεδομένα διαδοχικά σε μια ακολουθία από φαινομενικά τυχαίες συχνότητες (frequency hopping). Ο δέκτης ακολουθεί την ίδια ακολουθία εναλλαγής καναλιών συχνότητας με τον εκπομπό και λαμβάνει το μήνυμα. Η ακεραιότητα της λήψης του μηνύματος μπορεί να επιτευχθεί μόνο όταν είναι γνωστή η ακολουθία της εναλλαγής συχνοτήτων. Καθώς μόνον ο δέκτης γνωρίζει την σωστή ακολουθία, το μήνυμα είναι αναγνώσιμο μόνο από τον πραγματικό του παραλήπτη. Με αυτή την τεχνική, ηλεκτρομαγνητικές παρεμβολές στον χώρο της λήψης θα επηρεάσουν μόνο ένα τμήμα του μηνύματος, έχοντας ως αποτέλεσμα την ανάγκη για επανεκπομπή μόνο μικρού όγκου μηνυμάτων. Ο συγκεκριμένος τρόπος κωδικοποίησης μπορεί να δώσει ταχύτητες μεταφοράς δεδομένων έως και 2mbit. Ακολουθεί γράφημα που δείχνει την τεχνική FHSS συναρτήσει της ισχύος και του χρόνου.



Σχήμα 2.3.3.1 FSSS συναρτήσει ισχύος και χρόνου

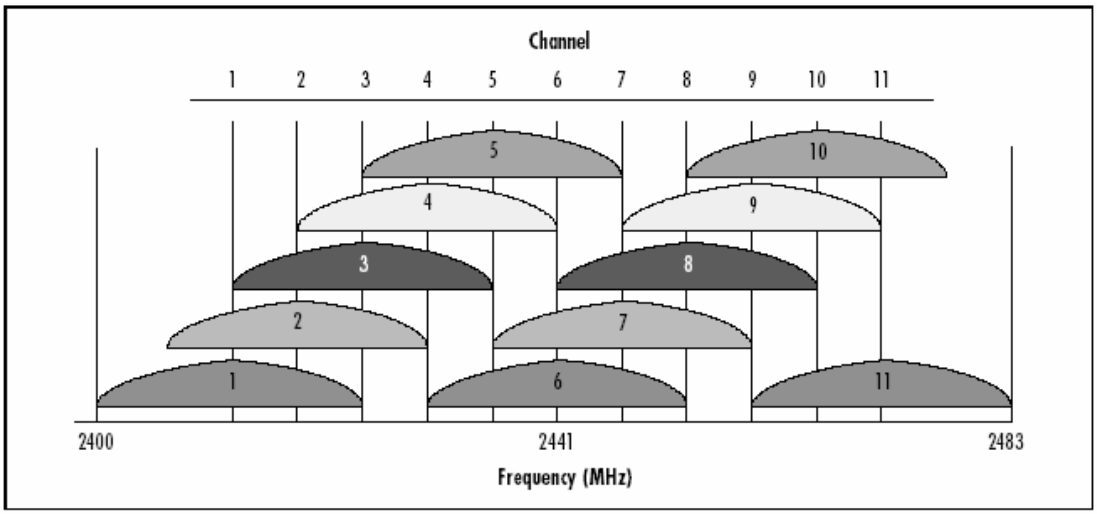
Στον DSSS το φάσμα χωρίζεται σε 14 μερικώς (ανά ~4) επικαλυπτόμενα κανάλια πλάτους 22 MHz και χρησιμοποιείται ένα κάθε φορά για επικοινωνία.



Σχήμα 2.3.3.2 DSSS συναρτήσει ισχύος και χρόνου

Ένας εκπομπός direct sequence επικοινωνεί στα δεδομένα, προσθέτοντας bits εφεδρείας που καλούνται chips. Σε κάθε bit πληροφορίας προστίθενται τουλάχιστον 10 chips. Αμέσως μετά τα τμήματα των δεδομένων στέλνονται σε όσες περισσότερες συχνότητες γίνεται, ταυτόχρονα, εντός του καναλιού. Η μέγιστη ταχύτητα φτάνει τα 11mbit. Στο ακόλουθο σχήμα

βλέπουμε την κατανομή των καναλιών στο φάσμα των 2.4GHz, καθώς και τον τρόπο με τον οποίο επικαλύπτονται.



Σχήμα 2.3.3.3 DSSS κανάλια

Ας δούμε όμως αναλυτικά ποια κανάλια λειτουργίας του 802.11 είναι ελεύθερα σε μερικές χώρες.

Κανάλι	Συχνότητα	ΗΠΑ	Ευρώπη	Ισπανία	Γαλλία	Ιαπωνία
1	2.412	X	X			
2	2.417	X	X			
3	2.422	X	X			
4	2.427	X	X			
5	2.432	X	X			
6	2.437	X	X			
7	2.442	X	X			
8	2.447	X	X			
9	2.452	X	X			
10	2.457	X	X	X	X	
11	2.462	X	X	X	X	
12	2.467		X		X	
13	2.472		X		X	
14	2.483					X

Σχήμα 2.3.3.4 Κανάλια σε μερικες χώρες

Τελικά με την έλευση του 802.11b το Σεπτέμβρη του 1999, η επιτροπή αποφάσισε να αφήσει στο πρότυπο μόνο την κωδικοποίηση DSSS, παρόλο που το FHSS αρχικά φαίνονταν σαν ευκολότερο αλλά και φθηνότερο στην

υλοποίηση του. Με αυτό τον τρόπο το 802.11b απέκτησε ένα από τα μεγαλύτερά του πλεονεκτήματα, την υψηλή διαμεταγωγή δεδομένων.

2.3.4 Εύρος Ζώνης

Όπως εξηγήσαμε και νωρίτερα το πρωτόκολλο IEEE 802.11b φτάνει τη μέγιστη ταχύτητα των 11 mbps, χάρη στην κωδικοποίηση DSSS που χρησιμοποιεί. Οι ασύρματες συνδέσεις είναι επιρρεπής σε σφάλματα μετάδοσης από τη φύση τους. Έτσι το overhead μετάδοσης πακέτων ελέγχου και διόρθωσης λαθών, μεταφράζεται σε πραγματική ταχύτητα μεταφοράς δεδομένων πολύ χαμηλότερη της ονομαστικής. Ακόμα λόγω του γεγονότος ότι όλες οι συσκευές WiFi έχουν ένα ραδιοφωνικό πομποδέκτη, η λειτουργία τους σαν δικτυακές συσκευές είναι σε half-duplex mode, πράγμα που επιτρέπει στον πομποδέκτη να μπορεί να ακούει το δίκτυο ή να στέλνει σε αυτό, αλλά όχι ταυτόχρονα. Έτσι το πραγματικό όριο για το bandwidth μιας 802.11b σύνδεσης διαμορφώνεται στα 5mbps.

Πολλές εταιρίες υπόσχονται ονομαστικές διπλάσιες ή και περισσότερο ταχύτητες. Τέτοια χαρακτηριστικά είναι εκτός του στάνταρ, και λειτουργούν μόνο μεταξύ των προϊόντων της ίδιας εταιρίας. Από την στιγμή που επιτευχθεί σύνδεση με μια άλλη συσκευή WiFi, τότε ισχύουν όλοι οι κανόνες ενός κοινού Ethernet δικτύου.

2.3.5 Μέθοδος πρόσβασης στο μέσο(Access Method)

Το 802.11 πρωτόκολλο για την πρόσβαση στο φυσικό μέσο υποστηρίζεται από δύο μεθόδους, το PCF (Point Coordination Function) και DCF (Distributed Coordination Function) με Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) σε αναλογία με το Ethernet που υλοποιεί το CSMA/CD (Collision Detection).

Το CSMA στο Ethernet λειτουργεί ως ακολούθως: όταν κάποιος επιθυμεί να στείλει δεδομένα, ελέγχει αν το κανάλι είναι κατειλημμένο από μια

άλλη μεταφορά δεδομένων. Αν είναι, τότε περιμένει ένα τυχαίο χρονικό περιθώριο(μικρό) σύμφωνα με τον αλγόριθμο exponential random backoff.

Ο τρόπος πρόσβασης αυτός δεν μπορεί να είναι αποδοτικός στο 802.11 για δύο λόγους:

1. Η υλοποίηση αυτής της μεθόδου θα απαιτούσε ραδιοφωνικούς εκπομπούς που θα είχαν την δυνατότητα Full – Duplex επικοινωνίας (αποστολή και λήψη ταυτόχρονα), κάτι το οποίο θα αύξανε το κόστος.

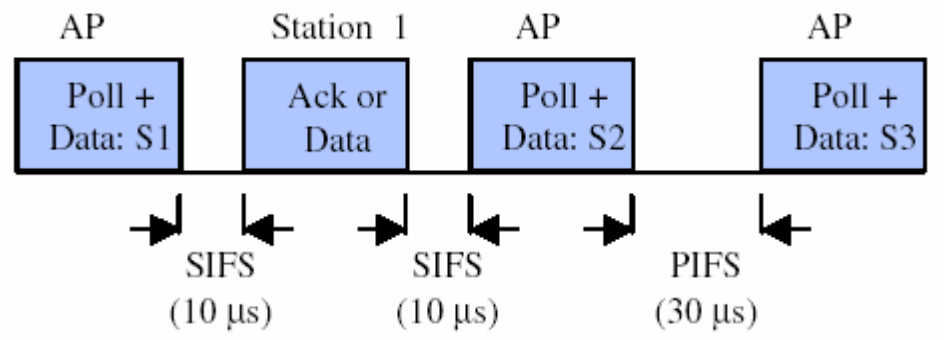
2. Σένα ασύρματο περιβάλλον δεν μπορούμε με ασφάλεια να υποθέσουμε ότι όλοι οι σταθμοί θα μπορούν να ακούν ο ένας τον άλλον. Ένας σταθμός που ελέγχει το μέσο και το βρίσκει ελεύθερο, δεν σημαίνει και ότι είναι ελεύθερο στην περιοχή του λήπτη.

Αναλυτικότερα το 802.11 ορίζει πέντε διαφορετικά χρονικά διαστήματα για συγχρονισμό στο MAC επίπεδο. Αυτά είναι τα εξής : το short interframe space (SIPS), το slot time, το priority interframe space (PIFS), το istributed interframe space (DIFS), και το extended interframe space (EIFS).

Το χρονικό διάστημα SIPS και το slot time θεωρούνται βασικά και καθορίζονται από το MAC. Τα υπόλοιπα διαστήματα καθορίζονται βάσει των παραπάνω διαστημάτων. Το SIPS είναι το μικρότερο όλων των χρονικών αυτών διαστημάτων, ακολουθούμενο από το slot time, το οποίο μπορεί να ερμηνευθεί σαν η μονάδα χρόνου για το MAC του 802.11, παρόλο που το πρωτόκολλο δεν βασίζεται σε αρχιτεκτονική με χρονικές «θυρίδες» (time slots). Ειδικά στο 802.11b, οι χρόνοι SIFS και slot είναι 20μs, χρόνος που επιλέχθηκε έτσι ώστε να δώσει ένα λογικό σε διάρκεια διάστημα για τις καθυστερήσεις διάδοσης και επεξεργασίας από τις συσκευές. Ο χρόνος PIFS ισούται με τον χρόνο SIFS επαυξημένο κατά ένα slot και ο DIFS κατά δύο slots. Ο χρόνος EIFS είναι μεγαλύτερος και από τους τέσσερις προηγούμενους, και χρησιμοποιείται για την επανεκπομπή πακέτων που ελήφθησαν λανθασμένα.

Το 802.11, όπως έχουμε πει και προηγουμένως, υποστηρίζει δύο τρόπους λειτουργίας : τον PCF και τον DCF. Με την πρώτη μέθοδο λειτουργίας, το κεντρικό AP της κυψέλης στέλνει μηνύματα στους σταθμούς πελάτες, τους ρωτάει δηλαδή στην ουσία για το αν έχει δεδομένα για αποστολή ή όχι (Polling). Αν ο σταθμός απαντήσει, μπορεί να στείλει την θετική του απάντηση (ACK) στο ίδιο πακέτο με τα δεδομένα προς αποστολή.

Αν δεν απαντήσει εντός του χρονικού ορίου SIFS, τότε το Access Point προχωρά στον επόμενο σταθμό.

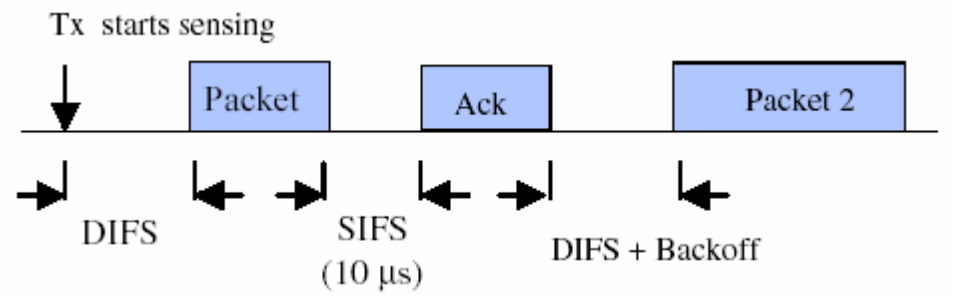


Σχήμα 2.3.5.1 Μέθοδος PCF στο 802.11b MAC

Η επιτροπή που ήταν υπεύθυνη για την προτυποποίηση του 802.11b όρισε πάρα πολύ αυστηρά τις απαιτήσεις χρονισμού SIFS και PIFS. Ένα ACK πακέτο, η απάντηση δηλαδή στην ερώτηση poll ενός σταθμού, πρέπει να φτάσει στο Access Point εντός του χρόνου SIFS, που είναι 10μs. Σε ένα ασύρματο δίκτυο που εκτείνεται σε μια ευρύτερη περιοχή (>1,5χλμ), ο round trip(χρόνος για να λάβει χώρα μια αίτηση-απάντηση) χρόνος ενός σήματος είναι 15μs. Είναι δηλαδή ολοφάνερο ότι το ACK πακέτο θα εκπεμφθεί κανονικά από τον σταθμό πελάτη, αλλά δεν θα διαβαστεί ποτέ από το Access Point λόγω έλλειψης σωστού χρονισμού. Έτσι η μέθοδος PCF δεν χρησιμοποιείται στις περισσότερες υλοποιήσεις του 802.11b, καθώς περιορίζει εμμέσως αλλά αυστηρώς την εμβέλεια ενός ασύρματου δικτύου.

Στην μέθοδο λειτουργίας DCF, το 802.11 χρησιμοποιεί έναν μηχανισμό Αποφυγής Συγκρούσεων μαζί με αναγνώριση βεβαίωσης λήψης των πακέτων που στέλνονται. Αν ο εκπομπός, κατά την έναρξη διαδικασία αποστολής, δει ότι το μέσο είναι ελεύθερο(κανείς δεν χρησιμοποιεί το κανάλι) για χρόνο ίσο με DIFS, τότε αρχίζει την εκπομπή. Αν δεν είναι ελεύθερο το κανάλι, συνεχίζει να το ελέγχει για να δει αν βρίσκεται σε κατάσταση busy ή idle. Αν βρεθεί το κανάλι ελεύθερο για χρόνο DIFS, τότε ξεκινά να μετράει το χρόνο χρήσης του σε μονάδες slot time, σύμφωνα με τον υπάρχον αλγόριθμο και συνεχίζει τον έλεγχο της κατάστασης του καναλιού. Στο τελευταίο βήμα, για κάθε slot time που ο εκπομπός βρίσκει ελεύθερο κανάλι, ο τυχαίος χρόνος αναμονής μειώνεται κατά ένα slot time. Όταν αυτός ο χρόνος μηδενιστεί, τότε και μόνο ο εκπομπός μπορεί να ξεκινήσει τη διαδικασία μετάδοσης των δεδομένων που

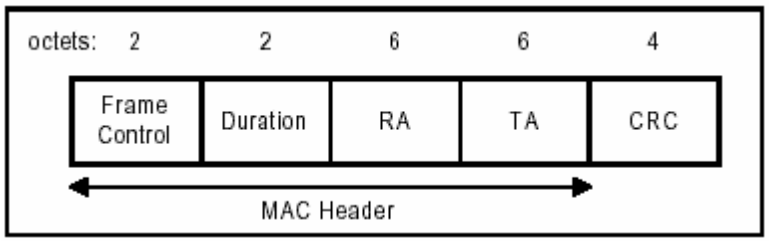
θέλει να στείλει. Με αυτή τη μέθοδο αποφεύγονται οι συγκρούσεις πακέτων διαφορετικών εκπομπών, αλλά και αποκλείεται η μονοπώληση του καναλιού από έναν και μόνο σταθμό που ίσως να προσπαθούσε συνεχείς εκπομπές.



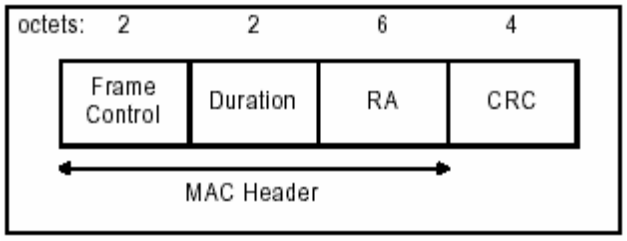
Σχήμα 2.3.5.2 Μέθοδος DCF στο 802.11b MAC

Ο δέκτης θα ελέγξει την «υπογραφή» CRC του πακέτου που πήρε, και αν την βρει έγκυρη, τότε στέλνει ένα πακέτο ACK στον αποστολέα. Αν ο αρχικός αποστολέας δεν πάρει ACK πακέτο, τότε συνεχίζει να επανεκπέμπει την πληροφορία ως που να λάβει ένα ACK ή να σταματήσει να προσπαθεί και να απορρίψει το αρχικό πακέτο.

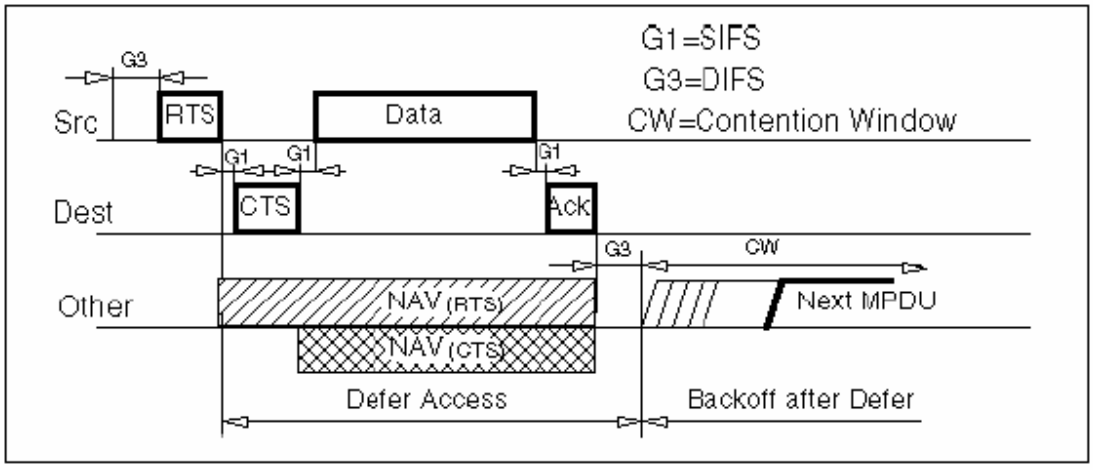
Η επιτροπή IEEE εισήγαγε έναν μηχανισμό Virtual Carrier Sense στο 802.11 για να αμβλύνει το φαινόμενο κατά το οποίο δύο σταθμοί δεν μπορούν να ακούσουν ο ένας τον άλλον και προκαλούνται συγκρούσεις. Ο μηχανισμός λέγεται CTS/RTS(clear to send/request to send) και θα μελετηθεί και στο επόμενο κεφάλαιο πιο διεξοδικά. Όταν ενεργοποιείται, κάθε client πριν ξεκινήσει την αποστολή δεδομένων, στέλνει ένα ειδικό πακέτο με πληροφορίες που έχουν σχέση με το χρόνο που θα πάρει η εκπομπή του. Αν το κανάλι είναι ελεύθερο, το AP στέλνει σαν απάντηση ένα πακέτο CTS. Ο client ξεκινά την εκπομπή του, αλλά και όλοι οι υπόλοιποι clients ακούν το CTS και αναβάλλουν τις δικές τους εκπομπές. Όλοι οι σταθμοί που ακούσουν το RTS και/ή το CTS, θέτουν το δείκτη Virtual Carrier Sense(που ονομάζεται NAV) για τον χρόνο που αναγράφει το πακέτο RTS, και χρησιμοποιούν την πληροφορία αυτή για να αποκτήσουν πρόσβαση στο μέσο. Μάλιστα, τα πακέτα RTS στέλνονται από client/AP, ανάλογα με κάποιο κατώφλι(RTS threshold). Αν το πακέτο που θα εκπεμφθεί, έχει μέγεθος μεγαλύτερο του κατωφλίου σε KB, τότε πριν το πακέτο αυτό, αποστέλλεται ένα RTS. Βλέπε τις παρακάτω εικόνες για την ακριβή μορφή των πακέτων RTS/CTS, αλλά και για την χρονική ακολουθία της διαδικασίας αποστολής ενός πακέτου δεδομένων.



Σχήμα 2.3.5.3 Το πλαίσιο RTS



Σχήμα 2.3.5.4 Το πλαίσιο CTS



Σχήμα 2.3.5.5 Η διαδικασία αποστολής των RTS-CTS

2.3.6 Πρότυπα συμβατότητας και πιστοποίηση προτύπου WiFi

Το εμπόριο έχει κατακλυστεί πλέον από προϊόντα εταιριών που υλοποιούν με κάποιο τρόπο κάποιο μέρος του πρωτοκόλλου 802.11b(Access Points, clients, routers, VoIP terminals, cameras κτλ). Την λύση στην ερώτηση «τι εγγύηση έχει ο καταναλωτής για την συμβατότητα λειτουργίας όλων των 802.11b συσκευών;» έρχεται να δώσει η WECA(Wireless Ethernet Compatibility Alliance). Πρόκειται για μια οργάνωση που εξετάζει και πιστοποιεί την συμβατότητα των 802.11 συσκευών. Πρόκειται για μια πολύ

σημαντική πρωτοβουλία, καθώς ένα wireless δίκτυο μπορεί να αποτελείται από συσκευές διαφορετικών εταιριών. Μια πιστοποιημένη από την weca συσκευή, έχει την εγγύηση ότι θα μπορεί να συνεργαστεί με άλλο ασύρματο ή όχι υλικό, που υποδεικνύεται από το πρωτόκολλο 802.11b για τον συγκεκριμένο τύπο συσκευής(π.χ. ένα Access Point πρέπει να μπορεί να συνδεθεί με οποιονδήποτε client, αλλά και να μπορεί να δεχτεί και μια Ethernet σύνδεση). Η WECA έχει θεσπίσει το Wireless Fidelity πρότυπο, και σε κάθε συσκευή που περνάει επιτυχώς όλες τις δοκιμές συμβατότητας, απονέμεται η «σφραγίδα συμβατότητας».

Σχήμα 2.3.6 WiFi trademark

Αυτή η σφραγίδα δίνει στους καταναλωτές την εγγύηση ότι, τα προϊόντα που την φέρουν, θα μπορούν να λειτουργούν μεταξύ τους. Παρόλα ταυτά, το wifi δεν είναι ένα τεχνολογικό στάνταρ. Είναι απλά μια εγγύηση συμβατότητας μεταξύ προϊόντων.

Βεβαίως τα πράγματα ποτέ δεν είναι τόσο απλά. Πολλές φορές ερχόμαστε αντιμέτωποι με προϊόντα που είτε απλά δεν μπορούν να συνεργαστούν, είτε η συνεργασία τους αυτή είναι προβληματική. Τέτοια προβλήματα τις περισσότερες φορές βρίσκονται στο υλικό των συσκευών, οπότε είναι απίθανο να λυθούν. Έτσι η προσωπική δοκιμή των προϊόντων πριν την αγορά, ή η έρευνα για παραδείγματα αποδεδειγμένης συνεργασίας ενδείκνυται πριν από μια σοβαρή επένδυση σε υλικό διαφορετικών κατασκευαστών.

2.3.7 Ασφάλεια δικτύων 802.11b

Με την πάροδο του χρόνου όσο οι συσκευές WiFi εισέβαλλαν όλο και περισσότερο στα δίκτυα, τόσο οι χρήστες έβλεπαν πιο σοβαρά το ζήτημα της ασφάλειας των δεδομένων που διακινούσαν μέσω αυτών. Μεγάλο μέρος της επιστημονικής κοινότητας, αλλά ακόμα και κοινοί χρήστες, βοήθησαν με

μελέτες, ώστε να αποκαλυφθούν πολλές σημαντικές ατέλειες που είχε το μοντέλο ασφάλειας του πρωτοκόλλου. Θα προσπαθήσουμε να δώσουμε μια γενική εικόνα της όλης κατάστασης, προτείνοντας τελικά κάποιες λύσεις.

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. Μια γρήγορη λύση για την υποκατάστασή του, ήταν η πιστοποίηση χρηστών μέσω λιστών επιτρεπόμενων MAC διευθύνσεων. Η MAC διεύθυνση είναι ένας μοναδικός δεκαεξαδικός αριθμός, που είναι «γραμμένος» στο υλικό κάθε δικτυακής συσκευής. Το Access Point κρατούσε μια λίστα με όλες τις διευθύνσεις MAC που ο διαχειριστής του δικτύου επέτρεπε να συνδεθούν. Αν η MAC μιας client συσκευής δεν ανήκε στη λίστα, αυτή η συσκευή δεν θα μπορούσε να συνδεθεί στο Access Point. Αυτή όμως είναι μια πολύ αδύναμη μέθοδος πιστοποίησης στοιχείων των σταθμών-πελατών, αφού κάποιος που χρησιμοποιεί unix λειτουργικό περιβάλλον, το οποίο παρέχει πολλά δικαιώματα, θα μπορούσε με διάφορους τρόπους να αλλάξει την διεύθυνση MAC 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.

Το WEP ήταν η πρώτη σοβαρή προσπάθεια υπέρ της αύξησης της ασύρματης ασφάλειας. Δυστυχώς, ο σχεδιασμός του προτύπου, συνέπεσε χρονικά με την φρενίτιδα 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.

Δύο επιστημονικές εργασίες όμως, 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), παρόλαυτα, 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 wifi 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». Η μη νόμιμη πρόσβαση σε ασύρματα δίκτυα είναι τόσο εκτεταμένη, αφού υπάρχουν web sites τα οποία μπορούν να εντοπίσουν συντεταγμένες ανοιχτών εταιρικών ασύρματων δικτύων. Ακόμα υπάρχουν ομάδες χρηστών που χρησιμοποιούν προγράμματα όπως το netstumbler για να εντοπίζουν 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 wifi 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», ενονόματι wardriving, επωφελούμενοι κυρίως από την δωρεάν broadband σύνδεση στο διαδίκτυο που μπορεί να «προσφέρει» ένα απροστάτευτο δίκτυο. Η επίθεση parking lot, συνεπάγεται την χρήση της εμβελείας ενός wifi δικτύου σε συνδυασμό με κάποια τρύπα ασφαλείας, για την εισβολή στο δίκτυο αυτό από έναν ασφαλή για τον εισβολέα χώρο, όπως ο εταιρικός χώρος πάρκιν. 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.

Συνοπτικό συμπέρασμα όλων των παραπάνω είναι ότι η προτυποποίηση της ασύρματης ασφάλειας θα είναι πάντα μια εργασία προς εξέλιξη. Νέα πρότυπα μελετούνται, όπως το 802.11i, που υπόσχονται μια καλύτερη λύση από το WEP. Βέβαια ένας τέτοιος στόχος φαίνεται εύκολος, δεδομένης της πλήρους και πέρα για πέρα αποτυχίας του WEP πρωτοκόλλου. Πολλοί χρησιμοποιούν λύσεις λογισμικού που κρυπτογραφούν την κίνηση δεδομένων σε υψηλότερο δικτυακό επίπεδο, όπως το IPsec, το ssl κτλ.

2.3.8 Εφαρμογές WiFi δικτύων στο σπίτι, το γραφείο, την βιομηχανία

Τα πάμπολλα πλεονεκτήματα του 802.11 το καθιστούν ιδανικό για εγκατάσταση είτε σαν ένα αυτόνομο δίκτυο, είτε σαν ένα δίκτυο που επεκτείνει τις δυνατότητες μιας ενσύρματης δικτυακής εγκατάστασης.

Δύο από τους βασικούς σχεδιαστικούς στόχους της ομάδας του 802.11 θέτουν ιδανική την χρήση του στη βιομηχανία. Αυτοί είναι το χαμηλό κόστος των συσκευών και η χαμηλή τους κατανάλωση. Συχνά στη βιομηχανία χρειάζεται η συνεχής παρακολούθηση ενός συνόλου από συσκευές που ελέγχουν την σωστή λειτουργία της εγκατάστασης και επικοινωνούν με έναν κεντρικό υπολογιστή που συλλέγει τις πληροφορίες. Ένα peer to peer (ομότιμο) δίκτυο από wifi-enabled αισθητήριων συσκευών (sensors) μπορεί να εγκατασταθεί για την παρακολούθηση συγκεκριμένων εργασιών. Ένα τέτοιο δίκτυο, μπορεί εύκολα να γίνει «έξυπνο». Οι συσκευές αυτές μπορούν να βρίσκουν εναλλακτικές διαδρομές για να επικοινωνούν με τον κεντρικό εξυπηρετητή, δίνοντας 100% uptime στο σύστημα. Επίσης λόγω της υψηλής διαμεταγωγής του πρωτοκόλλου μπορούν να διακινούν μεγάλους όγκους δεδομένων, πράγμα που εγγυάται την παρακολούθηση του συστήματος σε πραγματικό χρόνο. Βέβαια η ασύρματη επικοινωνία είναι από μόνη της το μεγαλύτερο πλεονέκτημα της τεχνολογίας, καθώς δεν χρειάζονται άλλες καλωδιώσεις στον ήδη επιβαρημένο χώρο της εγκατάστασης.

Στο γραφείο, το wifi γίνεται συνώνυμο της ευελιξίας. Οι εργαζόμενοι μπορούν ελεύθερα να κινούνται με φορητούς υπολογιστές στους εργασιακούς τους χώρους, χωρίς να χάνουν ούτε λεπτό την σύνδεσή τους στο εταιρικό δίκτυο και το διαδίκτυο. Με αυτόν τον τρόπο επιτυγχάνεται η αύξηση της παραγωγικότητας τους, καθώς μπορούν να συνεργάζονται ευκολότερα και να έχουν συνεχή πρόσβαση σε κρίσιμες πληροφορίες. Πολλά τοπικά δίκτυα σε κάθε κτίριο μπορούν εύκολα να συνενωθούν με Links μεγάλων αποστάσεων, αποδοτικά και κυρίως οικονομικά. Δεν πρέπει βεβαίως να ξεχνάμε τους

κινδύνους ασφάλειας που παρουσιάζονται, κινδύνους που θα αναλύσουμε στην αντίστοιχη παράγραφο.

Στο σπίτι, μια wifi enabled συσκευή, μπορεί να δώσει την δυνατότητα για περιήγηση στο διαδίκτυο, παρακολούθηση video, εσωτερική βιντεοδιάσκεψη, σε οποιοδήποτε σημείο του σπιτιού. Φυσικά το στήσιμο ενός τοπικού δικτύου μπορεί να γίνει χωρίς τον βραχνά των καλωδίων, hubs και λοιπών δικτυακών συσκευών, που δύσκολα χωρούν σε ένα σπίτι. Όλη ή υποδομή αντικαθιστάται από μόνο ένα ή περισσότερα κεντρικά Access Points.

2.3.9 802.11b Συνοπτικά

Στον παρακάτω πίνακα φαίνονται εν συντομία τα κυριότερα χαρακτηριστικά και τα πλεονεκτήματά τους στο πρότυπο 802.11b.

Χαρακτηριστικό	Πλεονεκτήματα
Χρήση συχνότητας 2.4GHz (ISM Band).	• Συσκευές 802.11b λειτουργούν σε παγκό-σμιο επίπεδο.
Υλοποίηση τεχνικών απλωμένου φάσματος για την κωδικοποίηση του σήματος.	• Σήμα λιγότερο ευάλωτο στο θόρυβο στενής ζώνης. • Λιγότερα λάθη κατά την αποδιαμόρφωση του σήματος και μικρότερο FER.
Ρυθμοί μετάδοσης της τάξης των 11Mbps.	• Ρυθμοί μετάδοσης ισάξιοι του Ethernet. • Ιδανικό για την επέκταση ενός ενσύρματου δικτύου.
Πρόσβαση στο ασύρματο μέσο με την τεχνι-κή Virtual Carrier Sense.	• Εξάλειψη του φαινομένου «Κρυμμένου Κόμβου»
Χρήση αλγορίθμου ασφαλείας WEP.	• Κρυπτογράφηση των δεδομένων με κλειδί των 128bit. • Δυνατότητα αυτοσυγχρονισμού για κάθε πακέτο με στέλνεται. • Μεγάλη αποδοτικότητα και δυνατότητα υλοποίησης τόσο σε software όσο και

	σε hardware . • Προστασία του δικτύου από μη εξουσιοδο-τημένη πρόσβαση. • Ασφάλεια και μυστικότητα για τα δεδομένα των χρηστών.
Ύπαρξη τεχνικών Διαχείρισης Ενέργειας (Power Management).	• 802.11b κατάλληλο για φορητές συσκευές και γενικά συσκευές που δουλεύουν με μπαταρίες.
Το 802.11b είναι φτηνό, αξιόπιστο και εύκολο στην εγκατάσταση.	• Κατάλληλο για μικρές επιχειρήσεις, γραφεία και οικιακή χρήση. • Απαιτεί πολύ λίγες γνώσεις και ελάχιστο χρόνο προκειμένου να το κάνει κανείς να λειτουργήσει.

2.4 High Perfomance Radio LAN(HIPERLAN)

Το HIPERLAN είναι ευρωπαϊκή απάντηση στα πρωτόκολλα IEEE802.11. Το ινστιτούτο ETSI European Telecommunications Standardization Institute έχει ορίσει το HIPERLAN ως ένα ασύρματο δίκτυο LAN που επιτρέπει σταθερή ζεύξη κινούμενων σταθμών. Δημιουργήθηκε στα πλαίσια μιας προσπάθειας του ινστιτούτου που ονομάζεται Ευρυζωνικό Δίκτυο Ραδιοπρόσβασης (Broadband Radio Access Network-BRAN).

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 οποία δημιουργήθηκε το 2000 και υποστηρίζει ταχύτητες μέχρι 54Mbps καθώς όπως προσφέρει υψηλές επιδόσεις σε περιβάλλοντα με

μεγάλη διασπορά χρόνου που μπορεί να οφείλεται σε πολλαπλές ανακλάσεις. Και οι δύο εκδόσεις του HIPERLAN χρησιμοποιούν τη συχνότητα των 5GHz, η οποία στην Αμερική και στην Ιαπωνία είναι ελεύθερη, ενώ στην Ευρώπη έχει επισήμως παραχωρηθεί για χρήση από τα ασύρματα δίκτυα. Αυτό έχει ως αποτέλεσμα αφενός να μη δημιουργηθούν 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.

Μια άλλη ιδιαιτερότητα του HiperLAN είναι όπως το ad hoc roaming, η δυνατότητα δηλαδή όπως αυτόματης προώθησης των δεδομένων από access point σε access point σε περίπτωση που ο δέκτης δεν βρίσκεται στο βεληνεκές του πομπού. Εκτός από αυτό, υπερέχει έναντι των άλλων πρωτοκόλλων ασύρματης δικτύωσης λόγω του γεγονότος ότι δίνει τη δυνατότητα QoS (Quality Of Service, Ποιότητα Υπηρεσιών). Με το QoS μπορούν τα πακέτα δεδομένων να κατηγοριοποιούνται και να αποκτούν διαφορετική σειρά προτεραιότητας ανάλογα με το είδος όπως. 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 HiperLAN υποστηρίζει τόσο μία δομημένη αρχιτεκτονική δικτύου που ενσωματώνει ένα σταθμό βάσης όσο και ad-hoc δίκτυα. Ακόμα έχει τη δυνατότητα υποστήριξης, πιστοποίησης και κρυπτογράφησης για να επιτυγχάνει μεγαλύτερη ασφάλεια. Με την διαδικασία πιστοποίησης τόσο το σημείο πρόσβασης όσο και το κινητό τερματικό μπορούν να πιστοποιήσουν το ένα το άλλο ώστε να διασφαλίσουν διαπιστευμένη πρόσβαση στο δίκτυο Το HiperLAN2, σε αντίθεση με όλα τα υπόλοιπα πρότυπα, είναι συμβατό με μια τεράστια ποικιλία δικτύων (Ethernet, ATM, 3G, IP κ.ά.) και η εμβέλεια του φτάνει τα150m.

Παρακάτω είναι μερικά από τα πλεονεκτήματα και μειονεκτήματα της χρήσης του ασύρματου δικτύου HiperLan :

Πλεονεκτήματα :

- Συγκριτικά μεγαλύτερη ταχύτητα μετάδοσης (54Mbps)
- Δυνατότητα ad-hoc roaming
- Δυνατότητα QoS

- Κατάλληλο για απαιτητικές σε bandwidth εφαρμογές

Μειονεκτήματα :

- Αρκετά πολύπλοκο πρωτόκολλο
- Μπορεί να δημιουργηθεί πρόβλημα συμβατότητας
- Χρησιμοποιείται μόνο στην Ευρώπη
- Δεν έχει όπως εμπορικές εφαρμογές

2.4.1 HiperLan 1

Το 1996, το ETSI προτυποποίησε το HIPERLAN 1 (High Performance Local Area Network) σαν σύστημα για WLANs, επιτρέποντας κινητικότητα χρήστη και υποστηρίζοντας ad hoc τοπολογίες και τοπολογίες με υποδομή. Το HIPERLAN 1 ήταν αρχικά ένα από τα τέσσερα HIPERLANs που είχαν οραματιστεί, καθώς το ETSI αποφάσισε να έχει διαφορετικά δίκτυα για διαφορετικούς σκοπούς. Το κύριο χαρακτηριστικό όλων των τεσσάρων δικτύων, είναι ο συνδυασμός τους με time-sensitive υπηρεσίες μεταφοράς δεδομένων. Σήμερα τα HIPERLAN 3 και 4 ονομάζονται HIPERACCESS και HIPERLINK αντίστοιχα.

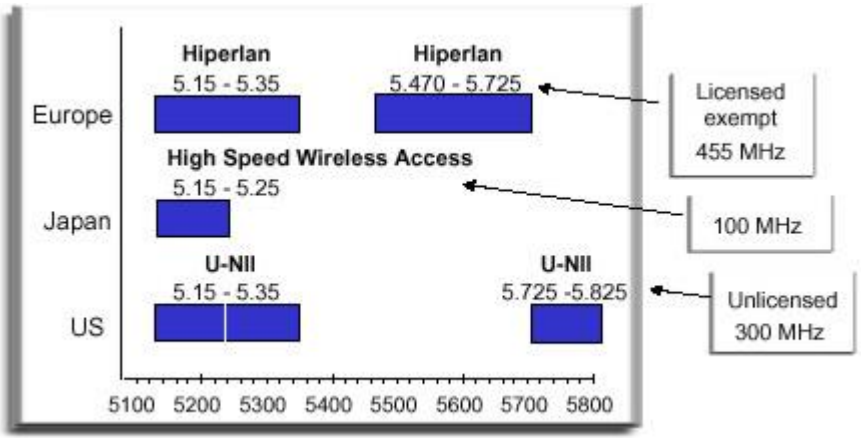
Το πρότυπο αυτό περιγράφει ένα ασύρματο τοπικό δίκτυο που περιέχει μηχανισμούς αναγνώρισης δικτύου, ανακάλυψης τοπολογίας, μεταβίβασης, κρυπτογράφησης δεδομένων, καθώς και μηχανισμούς διατήρησης ενέργειας. Ακόμα υποστηρίζει προτεραιότητα και διάρκεια ζωής για μεταφορά δεδομένων στα 23.5Mbps. Γενικά τα HIPERLANs λειτουργούν στα 5.1 – 5.3GHz σε ακτίνα 50μ σε κτίρια με ισχύ μετάδοσης 1W.

Ένα ιδιαίτερο χαρακτηριστικό που άλλα wireless δίκτυα δεν φαίνεται να προσφέρουν είναι η δυνατότητα που έχουν να προωθούν πακέτ σε διάφορους χρόνους. Αυτό είναι αρκετά χρήσιμο για τη διατήρηση της ενέργειας με τον εξής τρόπο: Μια συσκευή για παράδειγμα, μπορεί να ενεργοποιήσει ένα ειδικό wake-up μοτίβο. Αυτό το μοτίβο καθορίζει σε ποιά χρονική στιγμή η συσκευή είναι έτοιμη για παραλαβή δεδομένων, έτσι την υπόλοιπη ώρα η συσκευή

μπορεί να έχει κλειστό τον παραλήπτη της, εξοικονομώντας ενέργεια. Αυτές οι συσκευές ονομάζονται p-savers και χρειάζονται τους λεγόμενους p-supporters που περιέχουν τις πληροφορίες για το wake-up μοτίβο όλων των p-savers για τους οποίους είναι υπεύθυνοι. Ένας p-supporter στέλνει δεδομένα σε ένα p-saver μόνο όταν αυτός είναι «ξύπνιος».

2.4.2 HiperLan 2

Το HiperLAN/2 (High Performance Radio LAN type 2) αποτελεί ένα πρότυπο που αναπτύχθηκε και τυποποιήθηκε από το project BRAN (Broadband Radio Access Networks) του Ευρωπαϊκού ινστιτούτου τηλεπικοινωνιακών προτύπων (ETSI) για την ασύρματη δικτύωση κινητών τερματικών σε ευρυζωνικά δίκτυα. Υποστηρίζει την μετάδοση τόσο ασύγχρονων δεδομένων όσο και χρονικά εξαρτώμενων υπηρεσιών (πακέτα φωνής και video), οι οποίες έχουν ένα ανώτερο όριο στην καθυστέρηση μετάδοσης προκειμένου να πετύχουν ικανοποιητική ποιότητα υπηρεσιών



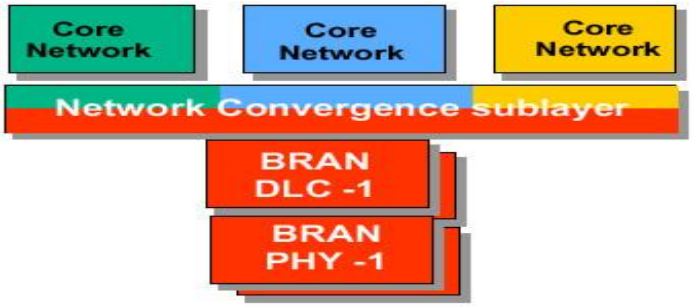
Σχήμα 2.4.2 U-NII Ζώνη Συχνοτήτων

Το 1999 ιδρύθηκε ένα διεθνές forum από τις Bosch, Dell, Ericsson, Nokia, Telia και Texas Instruments με σκοπό να προάγουν και να καταστήσουν το HiperLAN/2 ως παγκόσμιο πρότυπο για τα ασύρματα ευρυζωνικά δίκτυα στα 5GHz. Σκοπός του εγχειρήματος είναι να γίνει δυνατή

η χρήση διαλειτουργικών συσκευών, για την παροχή υψηλής ταχύτητας multimedia εφαρμογών και επικοινωνιών, μεταξύ διαφόρων δικτύων και κινητών τερματικών σε οικιακό, εταιρικό και δημόσιο περιβάλλον.

2.4.2.1 Τεχνικά Χαρακτηριστικά HiperLAN/2

Το πρωτόκολλο HiperLAN/2, μπορεί να χρησιμοποιηθεί σε μια ποικιλία δικτύων (Core Networks) και αυτό λόγω της ευέλικτης αρχιτεκτονικής που διαθέτει, η οποία καθορίστηκε από το project BRAN. Όπως φαίνεται και στο παρακάτω σχήμα αποτελείται από το Physical Layer, το Data Link Control Layer (DLC) και από ένα σύνολο υποεπιπέδων Network Convergence Sublayers, καθένα από τα οποία εξαρτάται από το δίκτυο που υλοποιείται στα ανώτερα στρώματα (Ethernet, ATM, UMTS).



Σχ. 0.4.2.1 Επίπεδα HiperLAN/2

2.4.2.2 Φυσικό Επίπεδο HiperLAN/2

Το project BRAN που εξέδωσε το πρότυπο για το HiperLAN/2 ήθελε τα δίκτυα που θα βασίζονται σε αυτό να μην απαιτούν άδεια για την λειτουργία τους ως προς την χρήση ραδιοσυχνοτήτων. Προκειμένου να αποφευχθεί η συνωστισμένη μπάντα ISM των 2.4GHz επιλέχτηκε μια ζώνη συχνοτήτων στα 5GHz, μεγάλο μέρος της οποίας βρίσκεται πάνω στην ζώνη U-NII (Unlicensed National Information Infrastructure) της Αμερικής.

Αυτό είχε ως συνέπεια να προκύψει ένα πρόβλημα κατά το οποίο μέρος του διαθέσιμου φάσματος είχε ήδη παραχωρηθεί σε άλλες εφαρμογές σε ορισμένες γεωγραφικές περιοχές. Αυτό είχε ως αποτέλεσμα την διάσπασή του σε μικρότερες ζώνες συχνοτήτων, όπως φαίνεται στο παραπάνω σχήμα, και την εξαίρεση μερικών από αυτών στις αντίστοιχες περιοχές. Για την Ευρώπη το διαθέσιμο φάσμα είναι 455MHz, χωρισμένο σε τρεις ζώνες όπως φαίνεται στον παρακάτω πίνακα.

Frequency band	RF Power limit	Comments
5.150 GHz – 5.250 GHz	200 mW mean EIRP	Indoor use only
5.250 GHz – 5.350 GHz	200 mW mean EIRP	Indoor use only and implementation of DFS and TPC.
5.470 GHz – 5.725 GHz	1 W mean EIRP	Indoor and outdoor use and implementation of DFS and TPC.

Σχήμα 2.4.2.2 Διάσπαση σε Ζώνες Συχνοτήτων της Μπάντας των 5GHz

Στο φάσμα αυτό υλοποιούνται 19 κανάλια εύρους 20MHz τα οποία μπορούν να μεταφέρουν 54Mbps το καθένα σε μέγιστη απόσταση 200m. Για την μετάδοση των δεδομένων χρησιμοποιείται διαμόρφωση OFDM με κάθε κανάλι να αποτελείται από 52 φέρουσες συχνότητες. Από αυτές 48 χρησιμοποιούνται για την μεταφορά δεδομένων και 4 για την μεταφορά σημάτων ελέγχου και συγχρονισμού. Κάθε φέρουσα συχνότητα ενός καναλιού διαμορφώνεται ξεχωριστά με μεθόδους όπως BPSK, QPSK, 16QAM, 64QAM και όλες μαζί εκπέμπονται προς τους δέκτες.

2.4.2.3 DLC Επίπεδο HiperLan 2

Το επίπεδο ελέγχου διασύνδεσης δεδομένων (DLC Layer) αποτελεί τον συνδετικό κρίκο ενός σημείου πρόσβασης και ενός κινητού τερματικού. Συγκροτείται από διάφορα υποεπίπεδα τόσο για την προσπέλαση του μέσου και την εκπομπή / λήψη δεδομένων όσο και για την διαχείριση της σύνδεσης σημείου πρόσβασης / κινητού τερματικού. Κάθε υποεπίπεδο συνοδεύεται και από ένα πρωτόκολλο το οποίο αναλαμβάνει μια λειτουργία.

- **Πρωτόκολλο MAC** – Με τη βοήθεια αυτού του πρωτοκόλλου επιτυγχάνεται ο έλεγχος της προσπέλασης στο μέσο και κατ' επέκταση της εκπομπής δεδομένων σε αυτό.
- **Πρωτόκολλο ER** – Αποτελεί το πρωτόκολλο ελέγχου λαθών (Error Control) του μέσου. Αναλαμβάνει να εντοπίσει πακέτα με λάθη, να ζητήσει την επανεκπομπή τους και να τα παραδώσει στην σωστή σειρά στο ανώτερο επίπεδο (Convergence Layer) ώστε να αυξηθεί η αξιοπιστία του ασύρματου μέσου.
- **Πρωτόκολλο RLC** – Η αρμοδιότητα του πρωτοκόλλου αυτού (Radio Link Control), είναι να αναλάβει την διαχείριση των οντοτήτων σηματοδοσίας που είναι απαραίτητες στο δίκτυο. Τέτοιες είναι οι οντότητες ελέγχου αντιστοίχησης (Association Control) οι οποίες αντιστοιχίζουν ένα κινητό τερματικό σε ένα σημείο πρόσβασης, οι οντότητες ελέγχου ασύρματων πόρων (Radio Resource Control) οι οποίες κάνουν μετρήσεις στην ποιότητα του σήματος για θέματα διαπομπής, εντοπισμού παρεμβολών και επιλογής συχνότητας λειτουργίας και οι οντότητες ελέγχου διασύνδεσης επιπέδων DLC (DLC Connection Control) που αναλαμβάνουν να εγκαθιστούν και να τερματίζουν συνδέσεις μεταξύ κινητών τερματικών και σημείων πρόσβασης.

2.4.2.4 Επίπεδο Convergence HiperLan 2

Το επίπεδο Convergence έχει ως λειτουργία να μεταφέρει τις υπηρεσίες που παρέχει το επίπεδο DLC στα ανώτερα επίπεδα του δικτύου (Core Network) αλλά ακόμα και να μετατρέπει τα πακέτα που έρχονται από τα ανώτερα επίπεδα με μεταβλητό ή σταθερό μέγεθος στο σταθερό μέγεθος που χρησιμοποιεί το επίπεδο DLC. Το δίκτυο που στήνεται πάνω από το επίπεδο αυτό, μπορεί να είναι είτε δίκτυο μεταγωγής πακέτου (packet based) όπως είναι τα δίκτυα Ethernet, PPP, Firewire, UMTS είτε δίκτυο κυψελωτής μορφής (cell based) όπως είναι τα δίκτυα ATM. Για κάθε περίπτωση δικτύου έχουμε και ένα αντίστοιχο επίπεδο convergence, που αναλαμβάνει να κάνει την

διασύνδεση με το επίπεδο DLC. Αν και μπορούμε να έχουμε πολλαπλά επίπεδα convergence, μόνο ένα μπορεί να είναι ενεργό κάθε φορά και επομένως ενός τύπου δικτύου να υποστηρίζεται από τα σημεία πρόσβασης και τα κινητά τερματικά.

2.4.2.5 Λειτουργία HiperLan 2

Το HiperLAN/2 ακολουθεί την τοπολογία των κυψελωτών δικτύων παρέχοντας ταυτόχρονα και την δυνατότητα δημιουργίας ad-hoc συνδέσεων. Στις ad-hoc συνδέσεις δύο ή περισσότερα κινητά τερματικά επικοινωνούν άμεσα μεταξύ τους για την ανταλλαγή πληροφοριών. Τέτοιες υλοποιήσεις συναντάμε συνήθως σε οικιακά δίκτυα όπου μια κυψέλη ουσιαστικά καλύπτει όλη την περιοχή εξυπηρέτησης.

Σε εταιρικά περιβάλλοντα και hot spots (ξενοδοχεία, αεροδρόμια, internet café, χώροι συνεδριάσεων) όπου η περιοχή που πρέπει να καλυφτεί είναι μεγαλύτερη από τον χώρο που μπορεί να εξυπηρετήσει ένα σημείο πρόσβασης, απαιτείται δίκτυο κυψελωτής μορφής με περισσότερα σημεία πρόσβασης συνδεδεμένα σε ένα σταθερό δίκτυο υψηλότερου επιπέδου. Σε αυτή την μορφή δικτύου έχουμε κεντρική διαχείριση των ραδιοδιαύλων από τα σημεία πρόσβασης και όλες οι επικοινωνίες των κινητών τερματικών γίνονται μέσω των σημείων πρόσβασης.

Σε ένα τέτοιο δίκτυο κυψελωτής μορφής, τα σημεία πρόσβασης έχουν επιλέξει τα κανάλια λειτουργίας τους σύμφωνα με τον αλγόριθμο DFS (Dynamic Frequency Selection) ώστε να μην υπάρχουν αλληλοπαρεμβολές. Μόλις ένα κινητό τερματικό, ζητήσει να συνδεθεί στο δίκτυο αρχίζει μια διαδικασία αντιστοίχησης (Association). Η διαδικασία αυτή περιλαμβάνει μετρήσεις τις ισχύος του σήματος που λαμβάνει το κινητό τερματικό από τα σημεία πρόσβασης και σύνδεση με το ισχυρότερο, εκχώρηση ενός αναγνωριστικού στο τερματικό (MAC ID), πιστοποίηση ταυτότητας (Authentication) τερματικού και σημείου πρόσβασης, επιλογή ή όχι κρυπτογράφησης και επιλογή επιπέδου convergence. Μετά την διαδικασία αυτή, το τερματικό είναι αντιστοιχισμένο με το συγκεκριμένο σημείο πρόσβασης και μπορεί να ανταλλάξει δεδομένα μόνο με αυτό. Ωστόσο το

τερματικό δεν είναι αναγκασμένο να παραμένει μονίμως συνδεδεμένο σε ένα σημείο πρόσβασης. Σε τακτά χρονικά διαστήματα γίνονται μετρήσεις του λαμβανόμενου σήματος από τα σημεία πρόσβασης. Έτσι, αν βρεθεί σημείο πρόσβασης με ισχυρότερο σήμα, τότε ξεκινάει μια διαδικασία διαπομπής (handover) η οποία περιλαμβάνει και την αντιστοίχηση του τερματικού στο νέο σημείο πρόσβασης.

2.4.2.6 Ασφάλεια HiperLan 2

Το HiperLAN 2 υποστηρίζει διαδικασίες πιστοποίησης ταυτότητας (authentication) και κρυπτογράφηση. Το authentication γίνεται κατά την διαδικασία της αντιστοίχησης του τερματικού με το σημείο πρόσβασης και έχει ως σκοπό αφενός την πρόσβαση στο δίκτυο μόνο των νόμιμων χρηστών και αφετέρου την εξακρίβωση ότι το δίκτυο που συνδέεται το τερματικό είναι αυτό που επιθυμεί. Ως προς την κρυπτογράφηση το HiperLAN 2 χρησιμοποιεί κλειδί των 56bit βασισμένο στο DES ή στο 3DES το οποίο δημιουργείται κατά την διαδικασία της αντιστοίχησης, με τον αλγόριθμο Diffie – Hellmann. Το κλειδί αυτό δεν είναι μόνιμο αλλά μπορεί να αλλάξει και κατά την διάρκεια μιας σύνδεσης αν ζητηθεί από το σημείο πρόσβασης.

2.4.2.7 HiperLAN/2 Συνοπτικά

Στον παρακάτω πίνακα φαίνονται εν συντομία τα κυριότερα χαρακτηριστικά και τα πλεονεκτήματά τους στο πρωτόκολλο HiperLAN/2.

Χαρακτηριστικό	Πλεονεκτήματα
Λειτουργία στη ζώνη συχνοτήτων των 5GHz.	• Δεν απαιτείται άδεια χρήσης. • Λιγότερος συνωστισμός απ' ότι στην ISM και επομένως λιγότερες παρεμβολές.

	• Λειτουργία σε παγκόσμιο επίπεδο με την διαίρεση του φάσματος σε ζώνες.
Χρήση διαμόρφωσης OFDM στο φυσικό επίπεδο του HiperLAN/2.	• Επιτυγχάνεται μετάδοση 54Mbps στο φυ-σικό επίπεδο και έως 25Mbps στο τρίτο επίπεδο. • Η υλοποίηση τέτοιου κυκλώματος διαμόρ-φωσης απαιτεί τις μισές πύλες από ένα κύκλωμα διαμόρφωσης μιας φέρουσας συχνότητας. • Μπορεί να διαχειριστεί μεγαλύτερη εξάπλωση χρονοκαθυστέρησης. • Δεν απαιτούνται πολύπλοκα ηλεκτρονικά κυκλώματα (equalizers).
Ύπαρξη αλγορίθμου δυναμικής επιλογής συχνότητας (DFS).	• Δεν απαιτείται σχεδιασμός δικτύου και κα-τανομή συχνοτήτων στα σημεία πρόσ-βασης. • Πολλά δίκτυα HiperLAN/2 μπορούν να μοιραστούν το ίδιο φάσμα χωρίς να πα-ρεμβάλει το ένα το άλλο. • Αλλαγή καναλιού σε περίπτωση εντοπι-σμού παρεμβολών.
Δυνατότητα χρήσης κεραιών τύπου sector.	• Μείωση των παρεμβολών.
Ύπαρξη πολλαπλών επιπέδων conver gence.	• Υποστήριξη πολλών ειδών δικτύων όπως Ethernet, PPP, Firewire, UMTS, ATM.
Λειτουργίες πιστοποίησης ταυτότητας και κρυπτογράφηση.	• Μόνο νόμιμοι χρήστες μπορούν να χρησιμοποιήσουν το δίκτυο. • Κάθε χρήστης ξέρει ότι συνδέεται στο δίκτυο που πραγματικά θέλει να συνδεθεί. • Τα δεδομένα που ταξιδεύουν στον αέρα είναι ασφαλή.
Διαδικασίες ελέγχου ισχύος και εξοικονόμη-σης ενέργειας (Power Saving).	• Ο έλεγχος της εκπεμπόμενης ισχύος του κινητού τερματικού απλοποιεί την σχεδία-ση του δέκτη του σημείο

	πρόσβασης (αποφεύγεται ο gain controller). • Ο έλεγχος της εκπεμπόμενης ισχύος των σημείων πρόσβασης μειώνει τις παρεμ-βολές σε άλλα συστήματα. • Οι μπαταρίες των φορητών συσκευών διαρκούν περισσότερο.
Υποστήριξη κινητικότητας του τερματικού (Mobility).	• Το τερματικό μπορεί να κινείται όχι μόνο στην περιοχή κάλυψης μιας κυψέλης αλλά ολόκληρου του δικτύου.

2.5 Ανταγωνιστικές Τεχνολογίες στις Ασύρματες Επικοινωνίες

Στην ενότητα αυτή θα μελετηθούν κάποιες ανταγωνιστικές τεχνολογίες στις ασύρματες επικοινωνίες. Οι κυριότερες εξ' αυτών είναι το Bluetooth και το HomeRF.

2.5.1 Bluetooth

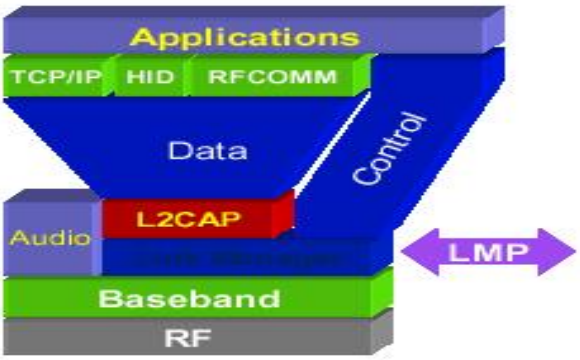
Η τεχνολογία Bluetooth δημιουργήθηκε από τις Ericsson, Nokia, Motorola, Intel, IBM, Toshiba και 3COM. Πρόκειται για μια τεχνολογία που έχει ως στόχο τα ασύρματα προσωπικά δίκτυα (WPAN) και ως σκοπό να αντικαταστήσει τα καλώδια διασύνδεσης στις φορητές συσκευές με ραδιοσυχνότητες. Η τεχνολογία Bluetooth είναι η μόνη αυτή την στιγμή που στοχεύει στην αντικατάσταση των καλωδίων με ραδιοκύματα και ως εκ τούτου

το πρωτόκολλο 802.15 που αναπτύσσεται από την IEEE για τα ασύρματα προσωπικά δίκτυα είναι βασισμένο σε αυτή.

Όταν μια συσκευή Bluetooth εντοπίσει στην εμβέλεια της μία άλλη συσκευή, τότε μπορεί να δημιουργηθεί ένα ομότιμο δίκτυο (ad hoc) για την ανταλλαγή πληροφοριών. Ένα δίκτυο Bluetooth(piconet) επιτρέπει μέχρι και οχτώ συσκευές να συνδεθούν με αυτό για την ανταλλαγή πληροφοριών.

2.5.1.1Τεχνικά Χαρακτηριστικά Bluetooth

Η τεχνολογία Bluetooth είναι δομημένη σε δύο πακέτα προδιαγραφών. Τις προδιαγραφές πυρήνα, οι οποίες περιγράφουν πώς η τεχνολογία λειτουργεί στα χαμηλότερα επίπεδα (έως και το επίπεδο Link Manager) και τις προδιαγραφές προφίλ χρήσης οι οποίες εστιάζουν στο πώς πρέπει να φτιαχτούν διαλειτουργικές συσκευές στηριζόμενες στις προδιαγραφές πυρήνα.



Σχήμα2.5.1.1 Επίπεδα Bluetooth

2.5.1.2 Προδιαγραφές Πυρήνα

Το Bluetooth φτιάχτηκε με σκοπό να λειτουργεί σε παγκόσμιο επίπεδο. Για το λόγο αυτό λειτουργεί στα 2.4GHz όπου βρίσκεται η ISM ζώνη συχνοτήτων. Η μπάντα ISM είναι μια ζώνη συχνοτήτων εύρους 83.5MHz η οποία είναι παγκοσμίως αναγνωρισμένη για χρήση χωρίς άδεια για

βιομηχανικούς, επιστημονικούς και ιατρικούς σκοπούς (Industrial, Scientific, Medicine). Η μετάδοση της πληροφορίας στο ασύρματο μέσο γίνεται με την τεχνική απλωμένου φάσματος με εναλλαγή συχνότητας (Frequency Hopping Spread Spectrum, FHSS). Το Bluetooth χωρίζει το φάσμα που του διατίθεται (2.402GHz – 2.48GHz) σε 79 κανάλια εύρους 1MHz και κάθε φορά που μεταδίδει ένα πακέτο δεδομένων αλλάζει συχνότητα σύμφωνα με ένα προσυμφωνημένο pattern μεταξύ πομπού και δέκτη. Έτσι αποφεύγονται οι παρεμβολές από άλλα σήματα και από θορύβους στενής ζώνης.

Στις προδιαγραφές του Bluetooth υπάρχουν τρεις κλάσεις συσκευών οι οποίες χαρακτηρίζονται από την εκπεμπόμενη ισχύ τους και φαίνονται στον παρακάτω πίνακα.

Power Class	Maximum Output Power (Pmax)	Nominal Output Power	Minimum Output Power[1)]	Power Control
1	100 mW (20 dBm)	N/A	1 mW (0 dBm)	Pmin<+4 dBm to Pmax Optional: Pmin[2)] to Pmax
2	2.5 mW (4 dBm)	1 mW (0 dBm)	0.25 mW (-6 dBm)	Optional: Pmin[2)] to Pmax
3	1 mW (0 dBm)	N/A	N/A	Optional: Pmin[2)] to Pmax

Σχήμα 2.5.1.2 Κλάσεις Ισχύος Bluetooth

Παρόλα αυτά η εκπεμπόμενη ισχύς ρυθμίζεται πάντα στην ελάχιστη που απαιτείται για την ζεύξη. Έτσι, αν ο δέκτης βρίσκεται σε απόσταση λίγων μέτρων, ο πομπός μειώνει την ισχύ του σήματος ώστε να ταιριάζει στην δεδομένη απόσταση. Με αυτό τον τρόπο επιτυγχάνεται ελαχιστοποίηση των παρεμβολών μεταξύ Bluetooth συσκευών αλλά και εξοικονόμηση ενέργειας στις μπαταρίες των φορητών συσκευών.

Η ακτίνα λειτουργίας του Bluetooth ξεκινάει από τα 10m για τις συσκευές κλάσης - 3 και φτάνει μέχρι τα 100m για αυτές που ανήκουν στην κλάση -1. Για την υλοποίηση WPAN χρησιμοποιούνται συσκευές κλάσης - 3 οπότε η ακτίνα δράσης τους περιορίζεται στα 10m. Αξίζει να σημειωθεί ότι δεν απαιτείται η οπτική επαφή του πομπού και του δέκτη για την επίτευξη της ζεύξης.

Η μέγιστη ταχύτητα μεταφοράς δεδομένων στο φυσικό επίπεδο είναι το 1Mbps. Το Bluetooth μοιράζει το εύρος ζώνης για να υποστηρίξει, ταυτόχρονα,

μεταφορά φωνής και δεδομένων. Υποστηρίζεται ένα ασύγχρονο κανάλι δεδομένων, έως και τρία σύγχρονα κανάλια φωνής, ή ένα κανάλι για ταυτόχρονη ασύγχρονη μεταφορά δεδομένων και σύγχρονη μεταφορά φωνής. Κάθε κανάλι φωνής υποστηρίζει 64Kbps σύγχρονης μετάδοσης, ενώ το κανάλι δεδομένων μπορεί να μεταφέρει συμμετρικά (προς κάθε κατεύθυνση) 432.6kbps ή ασύμμετρα 721Kbps / 57.6Kbps.

2.5.1.3 Εφαρμογές

Το Bluetooth επιτρέπει την κατάργηση όλων των καλωδίων τα οποία παλαιότερα ήταν απαραίτητα για τη «διασύνδεση» μεταξύ υπολογιστών, φορητών υπολογιστών χειρός, κινητών τηλεφώνων και άλλων ψηφιακών συσκευών, όπως ψηφιακές κάμερες, σαρωτές, εκτυπωτές, μικρόφωνα, ακουστικά, ραδιόφωνα κ.α. Το Bluetooth επιτρέπει την σύνδεση του κινητού με τον υπολογιστή, τη μεταφορά δεδομένων, όπως εικόνες, επαφές και σημειώσεις από κινητό προς κινητό, τη σύνδεση στο Internet κ.α. Όλα αυτά χωρίς καλώδια και πολύπλοκες ρυθμίσεις.

Οι εφαρμογές του λοιπόν είναι πολλαπλές:

- Ασύρματη δικτύωση μεταξύ επιτραπέζιου και φορητού υπολογιστή, σε έναν περιορισμένο χώρο με ελάχιστο διαθέσιμο εύρος ζώνης.
- Ασύρματη μεταφορά ψηφιακών αρχείων (εικόνες, mp3 κλπ) ανάμεσα σε κινητά τηλέφωνα και PDA.
- Ασύρματα περιφερειακά, όπως εκτυπωτές, ποντίκια και πληκτρολόγια, τα οποία επικοινωνούν με κάποιον επιτραπέζιο ή φορητό υπολογιστή.
- Ασύρματα ακουστικά για κινητά τηλέφωνα και Smartphone.
- Ασύρματη τηλεφωνία στο αυτοκίνητο: Το Bluetooth δίνει τη δυνατότητα σε χρήστες καταλλήλως εξοπλισμένων κινητών τηλεφώνων να χρησιμοποιούν κάποιες βασικές λειτουργίες τους με ασύρματα ακουστικά. Ανάλογο σύστημα υπάρχει ενσωματωμένο και σε κράνη οδηγών μοτοσικλέτας, επιτρέποντας τη συνομιλία κατά την οδήγηση.
- Ιατρικές εφαρμογές – δοκιμάζονται συσκευές από εταιρίες που παρέχουν ηλεκτρονικές συσκευές προχωρημένης ιατρικής.

- Ορισμένοι δέκτες GPS μεταφέρουν πληροφορίες NMEA μέσω Bluetooth.
- Απομακρυσμένος έλεγχος συσκευών, όπου έως την εμφάνιση του Bluetooth χρησιμοποιούνταν τεχνολογία υπέρυθρων ακτίνων.

2.5.1.4 Προδιαγραφές Προφίλ Χρήσης

Οι προδιαγραφές V1.0b του Bluetooth περιλαμβάνουν τα παρακάτω προφίλ τα οποία προσδιορίζουν και τις εφαρμογές που υποστηρίζει αυτή τη στιγμή το Bluetooth:

- **General Access** – Υπηρεσίες για την αναζήτηση άλλων συσκευών Bluetooth, διαχείριση του επιπέδου σύνδεσης (Link Management) και της ασφάλειας μεταξύ Bluetooth συσκευών.
- **Service Discovery** – Αναζήτηση των διαθέσιμων υπηρεσιών σε άλλες συσκευές Bluetooth.
- **Cordless Telephony** – Το προφίλ αυτό δίνει την δυνατότητα σε ένα κινητό τηλέφωνο να λειτουργεί σαν ασύρματο τηλέφωνο όταν βρεθεί στην εμβέλεια του σταθμού βάσης.
- **Intercom** – Το προφίλ αυτό δίνει την δυνατότητα σε δύο κινητά που διαθέτουν την τεχνολογία Bluetooth να επικοινωνούν μεταξύ τους χωρίς να γίνεται χρήση του δικτύου που ανήκουν αλλά της τεχνολογίας Bluetooth.
- **Serial Port** – Προσομοίωση σειριακής θύρας.
- **Headset** – Καθορισμός εκπομπής και λήψης δεδομένων φωνής πάνω από μια σύνδεση Bluetooth.
- **Dial-Up** Networking – Καθορισμός σύνδεσης μεταξύ ενός υπολογιστή και ενός κινητού τηλεφώνου.
- **Fax** – Προφίλ για την αποστολή και λήψη φαξ από υπολογιστή μέσω κινητού τηλεφώνου.
- **LAN Access** – Προφίλ για την δημιουργία ενός PAN χρησιμοποιώντας PPP πρωτόκολλο.

- **Generic Object Exchange (OBEX)** – Υπηρεσίες που χρησιμοποιούνται από άλλα προφίλ (File Transfer, Object Push, Synchronization).
- **Object Push** – Προφίλ για την αποστολή και λήψη επαγγελματικών καρτών και ραντεβού από μια συσκευή Bluetooth σε μια άλλη.
- **File Transfer** – Δημιουργία, διαγραφή, επισκόπηση, μεταφορά ενός συστήματος αρχείων και φακέλων από μια συσκευή Bluetooth σε μια άλλη.
- **Synchronization** – Το προφίλ αυτό δίνει την δυνατότητα συγχρονισμού δύο συσκευών Bluetooth την στιγμή που θα βρεθεί η μία στην εμβέλεια της άλλης.

2.5.1.5 Λειτουργία

Οι προδιαγραφές του Bluetooth καθορίζουν την «ασύρματη» τεχνολογία χαμηλού κόστους και χαμηλής ισχύος, που εξαλείφει τα καλώδια μεταξύ των κινητών συσκευών και επιτρέπει τη διασύνδεσή τους. Το Bluetooth λειτουργεί στο «αδέσμευτο» φάσμα συχνοτήτων των 2,4 GHz, ώστε οι συσκευές που το ενσωματώνουν να μπορούν να λειτουργήσουν απροβλημάτιστα σε οποιοδήποτε σημείο του πλανήτη. Για να περιοριστούν στο ελάχιστο οι παρεμβολές από παρεμφερείς συσκευές, το Bluetooth εκμεταλλεύεται την αμφίδρομη επικοινωνία και τη μέθοδο μετάδοσης με διασπορά φάσματος Frequency Hopping (έως και 1600 εναλλαγές συχνότητας ανά δευτερόλεπτο). Από φυσική άποψη επίσης το Bluetooth λειτουργεί περίπου στα 2.4 GHz, προδιαγράφει τρία επίπεδα ισχύος της εκπομπής από τα οποία εξαρτάται και η εμβέλεια επικοινωνίας (πάντα μικρότερη των 10 μέτρων σε PAN), ενώ η τακτική αλλαγή της συχνότητας εκπομπής λόγω της αξιοποίησης του FHSS καθορίζεται ψευδοτυχαία από έναν κεντρικό κόμβο, τον *Master*.

Το Bluetooth επιτρέπει τις απευθείας συνδέσεις από συσκευή προς συσκευή (point to point), καθώς και την ταυτόχρονη σύνδεση έως και 7 συσκευών με τη χρήση μιας μοναδικής συχνότητας. Τις προδιαγραφές της συγκεκριμένης τεχνολογίας ανέπτυξε και υποστηρίζει το Bluetooth Special Interest Group, ενώ η τελευταία «δημόσια» έκδοσή τους είναι η 1.1, η οποία

ενσωματώνεται πλέον στις περισσότερες συμβατές συσκευές μέσω κατάλληλων πομποδεκτών και καρτών δικτύου. Ένα πρόβλημα των προδιαγραφών του Bluetooth είναι ότι, λόγω της μετάδοσης στην ελεύθερη ζώνη συχνοτήτων των 2,4 GHz, οι συσκευές που το υποστηρίζουν αδυνατούν να χρησιμοποιήσουν ταυτόχρονα τα περισσότερα πρωτόκολλα της οικογένειας IEEE 802.11, καθώς τότε θα υπήρχαν σοβαρά προβλήματα παρεμβολών.

Οι βασικότερες προδιαγραφές του Bluetooth αφορούν το φυσικό επίπεδο και το υποεπίπεδο MAC, όπου έχουν δημιουργηθεί διαφορετικά πρωτόκολλα για διαφορετικές εφαρμογές και τα οποία ονομάζονται προφίλ. Το Bluetooth SIG έχει ήδη παρουσιάσει τέτοιες παραμετροποιημένες εκδοχές του προτύπου για διάφορες «αγορές» (π.χ. προφίλ ασύρματου τηλεφώνου, προφίλ πρόσβασης σε LAN, προφίλ εκτύπωσης, φωτογραφίας, αυτοκινήτου κλπ). Κάθε προφίλ περιλαμβάνει πρότυπα για όλα τα επίπεδα και προσφέρει λύσεις για τη διασύνδεση με διαφορετικά δίκτυα μεγαλύτερης κλίμακας.

2.5.1.6 Δομή

Η βασική δομική μονάδα ενός δικτύου Bluetooth είναι το **piconet**, στο οποίο όλοι οι κόμβοι που μετέχουν (μέχρι 7 συσκευές *Slaves*) μοιράζονται τον ίδιο κώδικα διασποράς και υπόκεινται στον έλεγχο ενός κοινού *Master*. Ο τελευταίος διαμοιράζει στους σταθμούς Slaves την πρόσβαση στο κοινό μέσο (τον ελεύθερο χώρο) με τη μέθοδο TDMA/TDD, όπου ο χρόνος διαμερίζεται σε αυστηρές χρονοθυρίδες, ο Master εκπέμπει στις περιττές και οι Slaves στις άρτιες (εναλλάξ), κάθε κόμβος που θέλει να εκπέμψει λαμβάνει περιοδικά από τον Master το δικαίωμα μετάδοσης σε 1, 3 ή 5 συνεχόμενες χρονοθυρίδες και κατά τη διάρκεια εκπομπής ενός πλαισίου δεν γίνεται εναλλαγή συχνότητας. Τα τερματικά μεταδίδουν μόνο στον Master, ο οποίος αποστέλλει στη συνέχεια τα πλαίσιά τους προς τον τελικό παραλήπτη, και διακρίνονται από μία παγκόσμια μοναδική 48-bit διεύθυνση. Δύο ή περισσότερα piconet μπορούν να βρίσκονται στον ίδιο χώρο, με τους κόμβους να μπορούν να συμμετέχουν

σε παραπάνω από ένα ταυτόχρονα, και να επικοινωνούν μεταξύ τους δημιουργώντας ένα μεγαλύτερης κλίμακας **scatternet**.

Υπάρχουν δύο τύποι συνδέσεων:

- **Σύγχρονες ή SCO.** Επιτρέπουν τη διέλευση χρονικά κρίσιμων πληροφοριών (συνήθως φωνής), κάθε κόμβος μπορεί να δεσμεύσει μόνο μέχρι μία χρονοθυρίδα, έχουν ρυθμό μετάδοσης δεδομένων 64 kbps, υλοποιούν συνδεσμοστρεφή επικοινωνία αυστηρά από σημείο σε σημείο, χρησιμοποιούν αλγορίθμους ανίχνευσης και διόρθωσης σφαλμάτων (FEC), ενώ δεν υπάρχουν επανεκπομπές ή επιβεβαιώσεις.
- **Ασύγχρονες ή ACL.** Τυπικά χρησιμοποιούνται για τη μετάδοση δεδομένων, κάθε κόμβος μπορεί να δεσμεύσει 1, 3 ή 5 χρονοθυρίδες για την εκπομπή ενός πλαισίου, είναι ασυνδεσμικές με έλεγχο ροής, έλεγχο σφαλμάτων (με αριθμούς ακολουθίας 1-bit και θετικές/αρνητικές επιβεβαιώσεις) και δυνατότητα πολυδιανομής, ενώ ο ρυθμός μετάδοσης μπορεί να ανέβει ως τα 724 kbps.

2.5.1.7 Διαδικασίες

Ένα piconet σχηματίζεται από έναν κόμβο που επιθυμεί να γίνει Master (διαδικασία Inquiry). Ο Master είναι υπεύθυνος για τις μεταβολές της δικτυακής τοπολογίας (εισαγωγές, αποχωρήσεις κόμβων και συντονισμός τους - διαδικασία Page). Η ακολουθία των ενεργειών είναι ως εξής: ο δυνάμει Master κόμβος εκκινεί τη διαδικασία ανίχνευσης πιθανών Slaves εκπέμποντας ένα μήνυμα Inquiry που περιέχει έναν κώδικα ονόματι *IAC*. Κάθε κόμβος που λαμβάνει ένα τέτοιο μήνυμα απαντά με πλαίσιο που περιέχει τη διεύθυνση του και πληροφορίες συγχρονισμού, ενώ στη συνέχεια αναμένει μήνυμα Page. Ο

Master λαμβάνει αυτά τα πλαίσια των Slaves, χρησιμοποιεί τις διευθύνσεις των τελευταίων για να υπολογίσει τον κώδικα διασποράς του Frequency Hopping και αποστέλλει στους Slaves που βρέθηκαν ένα μήνυμα Page που περιέχει έναν κώδικα *DAC*. Οι Slaves απαντούν με τον κώδικα IAC (ένα είδος πιστοποίησης) και ο κεντρικός Master τους στέλνει τον κώδικα διασποράς. Οι Slaves επιβεβαιώνουν τη λήψη, συνδέονται κι έτσι το piconet σχηματίστηκε. Οι συνδεδεμένοι κόμβοι μπορούν να είναι κάθε στιγμή είτε *Active* (συμμετέχουν ενεργά στο δίκτυο ανταλλάσσοντας δεδομένα), είτε *Sniff* (ακούν σε συγκεκριμένες χρονοθυρίδες), είτε *Hold* (όπου μπορούν να μεταφέρουν μόνο φωνή, με σύνδεση SCO, κι έχουν μειωμένη κατανάλωση ισχύος), είτε τέλος *Parked* (είναι μέλη του δικτύου αλλά δεν ακούν το κανάλι και δεν ανταλλάσσουν δεδομένα). Οι κόμβοι Active, Sniff και Hold αναγνωρίζονται από διευθύνσεις 3-bit (έως 7 ενεργοί Slaves), ενώ οι κόμβοι Parked από διευθύνσεις 8-bit (έως 256 ανενεργοί Slaves).

Υπάρχουν τέσσερις διαφορετικοί τύποι πλαισίων SCO και έξι τύποι ACL. Σε όλους όμως υπάρχει ένας κώδικας πρόσβασης, ο οποίος είναι είτε ο IAC, είτε ο DAC είτε ο CAC και σκοπεύει στο συγχρονισμό της εναλλαγής συχνοτήτων του FHSS μεταξύ του Master και των Slaves, μία κεφαλίδα υποεπιπέδου MAC με άθροισμα ελέγχου CRC και το ωφέλιμο φορτίο. Το τελευταίο ουσιαστικά είναι ένα πλαίσιο υποεπιπέδου LLC το οποίο μπορεί να έχει μια δική του κεφαλίδα, μεταφέρουσα στοιχεία για τη λογική σύνδεση του LLC στην οποία ανήκει το πλαίσιο και το μήκος του ωφέλιμου φορτίου, την πληροφορία προς μετάδοση και ίσως έναν κώδικα CRC ή/και FEC. Οι διαφορετικοί τύποι πλαισίων MAC του Bluetooth διαφοροποιούνται στο ωφέλιμο φορτίο: οι τύποι SCO είναι ο High Quality Voice 1, στον οποίον τα 2/3 του μήκους του ωφέλιμου φορτίου του πλαισίου είναι κώδικας FEC (με αποτέλεσμα μικρή απώλεια πλαισίων αλλά μειωμένο ρυθμό μετάδοσης δεδομένων) και τα υπόλοιπα πληροφορίες φωνής, ο High Quality Voice 2, στον οποίον το 1/3 του μήκους του ωφέλιμου φορτίου του πλαισίου είναι κώδικας FEC και τα υπόλοιπα πληροφορίες φωνής, ο High Quality Voice 3, στο ωφέλιμο φορτίο του οποίου υπάρχουν μόνο πληροφορίες φωνής, και ο Data-Voice, ο οποίος έχει κώδικα FEC ίσο με το 1/3 του συνολικού μήκους του πλαισίου, κώδικα CRC, την κεφαλίδα LLC που προαναφέρθηκε, πληροφορίες

φωνής και πληροφορίες δεδομένων. Οι τύποι ACL από την άλλη επίσης υποστηρίζουν διαφορετικούς ρυθμούς μετάδοσης και απώλειας πακέτων (όπου υψηλός ρυθμός μετάδοσης σημαίνει μικρό μήκος κώδικα FEC και άρα υψηλή απώλεια πακέτων), μεταφέρουν μόνο πληροφορίες δεδομένων και διακρίνονται σε Data Medium Rate 1,3 και 5, καθώς και Data High Rate 1,3 και 5.

2.5.1.8 Ασφάλεια Bluetooth

Σε ένα ασύρματο δίκτυο όπως το Bluetooth, όπου τα δεδομένα μεταφέρονται ελεύθερα στον αέρα και μπορούν να συλληφθούν από οποιονδήποτε βρεθεί στην εμβέλεια της συσκευής που εκπέμπει, η ασφάλεια είναι ένας πολύ σημαντικός παράγοντας και μπορεί να καθορίσει την επιτυχία ή όχι ενός πρωτοκόλλου. Η τεχνολογία Bluetooth έχει διάφορα επίπεδα και μηχανισμούς ασφαλείας για να εξασφαλίσει ότι τα δεδομένα που μεταδίδονται δεν μπορούν να υποκλαπούν. Για να το πετύχει αυτό χρησιμοποιεί τέσσερα βασικά κλειδιά για κρυπτογράφηση και για την εξακρίβωση των άλλων συσκευών Bluetooth. Πρόκειται για την φυσική διεύθυνση των 48bit κάθε συσκευής Bluetooth, για ένα τυχαίο αριθμό των 128bit που παράγεται για κάθε συναλλαγή μεταξύ δύο συσκευών Bluetooth, και για δύο μυστικά κλειδιά, το κλειδί για την εξακρίβωση της συσκευής από άλλες (authentication key) και το κλειδί κρυπτογράφησης (encryption key) τα οποία μπορούν να είναι από 8bit έως 128bit. Από αυτά τα τέσσερα βασικά κλειδιά παράγονται άλλα που χρησιμοποιούνται στις διάφορες συνδέσεις ad hoc μεταξύ συσκευών Bluetooth.

Το Bluetooth υποστηρίζει τρία διαφορετικά επίπεδα ασφαλείας:

- **Non-Security** – Η συσκευή δεν χρησιμοποιεί καμιά διαδικασία ασφαλείας.
- **Service Level Enforced Security** – Σε αυτό το επίπεδο η άδεια για την χρήση μιας συσκευής εξαρτάται από το είδος της υπηρεσίας που ζητάτε.

- **Link Level Enforced Security** – Αυτό το επίπεδο ασφαλείας απαιτεί διαδικασίες εξακρίβωσης προτού δοθεί η δυνατότητα χρήσης κάποιας υπηρεσίας της συσκευής.

2.5.1.9 Bluetooth Συνοπτικά

Στον παρακάτω πίνακα φαίνονται εν συντομία τα κυριότερα χαρακτηριστικά και τα πλεονεκτήματά τους στο πρωτόκολλο Bluetooth.

Χαρακτηριστικό	Πλεονεκτήματα
Χρήση συχνότητας 2.4GHz (ISM Band).	• Συσκευές Bluetooth λειτουργούν σε παγ-κόσμιο επίπεδο.
Υποστήριξη μέχρι 8 συσκευών από ένα piconet, όπου η μία δουλεύει σαν master και οι υπόλοιπες ως slave.	• Πολλαπλά piconets συνδέονται μεταξύ τους μέσω των συσκευών που δουλεύουν σαν master, αυξάνοντας έτσι τον αριθμό των συνδεδεμένων συσκευών.
Το Bluetooth θα κάνει δυνατή την ασύρ-ματη σύνδεση ενός φορητού και ενός κινη-τού τηλεφώνου.	• Απλοποίηση της σύνδεσης στο Internet ή στο εταιρικό δίκτυο εξαλείφοντας την ανάγ-κη καλωδίων.
Οι συσκευές Bluetooth μπορούν να επι-κοινωνούν σε εμβέλεια έως και 10m.	• Περιορίζοντας την εμβέλεια των συσκευών στα 10m, μειώνονται και οι απαιτήσεις των συσκευών σε ενέργεια, κάνοντας το Bluetooth πρακτικό για συσκευές που λειτουργούν με μπαταρία. • Τα 10m είναι αρκετά για WPAN, για τα οποία σχεδιάστηκε το Bluetooth. Περιορίζει έτσι τις παρεμβολές σε άλλες συνδέσεις Bluetooth και μειώνει το κόστος που θα χρειάζονταν ακριβά ηλεκτρονικά μεγάλης εμβέλειας.
Η εξακρίβωση και η κρυπτογράφηση με Public και Private κλειδιά είναι	• Παρέχεται υψηλού βαθμού ασφάλεια στην επικοινωνία μεταξύ Bluetooth

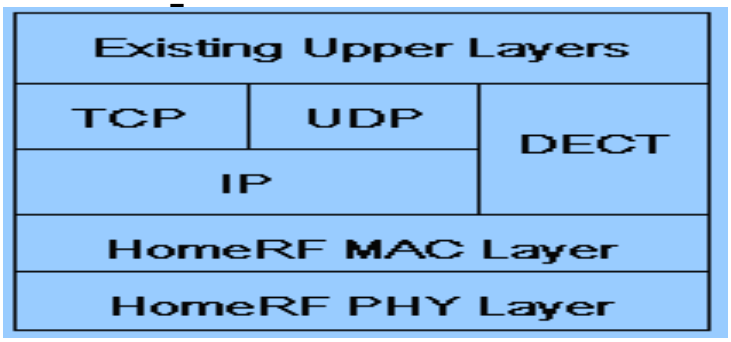
βασικά στοιχεία του προτύπου Bluetooth.	συσκευών.
Δεν απαιτείται οπτική επαφή μεταξύ των συσκευών Bluetooth για να γίνει μια σύνδεση.	• Παρέχεται μεγαλύτερη ευελιξία και ευκο-λία χρήσης σε αντίθεση με άλλες τεχνο-λογίες όπως το IrDA. • Είναι δυνατόν να γίνουν συνδέσεις ακόμα και όταν υπάρχουν εμπόδια στη μέση.
Πρόγραμμα απόκτησης του σήματος Bluetooth για τις συσκευές που συμμορ-φώνονται με τις προδιαγραφές του Bluetooth.	• Το πρόγραμμα αυτό θα παρέχει στην βιομηχανία και την αγορά ένα μηχανισμό για να αναγνωρίζει τις συσκευές που μπορούν να συνεργαστούν μεταξύ τους βάση του Bluetooth. • θα διασφαλιστεί η διάφανη λειτουργία μεταξύ των συσκευών που υποστηρίζουν το Bluetooth και θα είναι πιο εύκολή η χρήση των υπηρεσιών που υποστηρίζει από τον τελικό χρήστη.

2.5.2 HomeRF

Η ομάδα εργασίας που ασχολήθηκε με την δημιουργία του HomeRF ιδρύθηκε τον Μάρτιο του 1998 με σκοπό την δημιουργία ενός διεθνούς στάνταρ για την ασύρματη δικτύωση ενός σπιτιού. Λίγους μήνες αργότερα και με την συμμετοχή εταιριών από την βιομηχανία των προσωπικών υπολογιστών, του λογισμικού και των ημιαγωγών, αναπτύχθηκε το πρωτόκολλο SWAP (Shared Wireless Application Protocol) το οποίο απευθύνεται σε ένα ευρύ φάσμα διαλειτουργικών συσκευών. Από την ίδρυση της ομάδας εργασίας του HomeRF έως και σήμερα, πάνω από εκατό εταιρίες από τον κλάδο των υπολογιστών και του λογισμικού και σχεδόν όλοι οι μεγάλοι κατασκευαστές ημιαγωγών και ηλεκτρονικών γίνανε μέλη του HomeRF, με αποτέλεσμα μια μεγάλη ποικιλία συμβατών προϊόντων για την δικτύωση του σπιτιού να είναι διαθέσιμες στον τελικό καταναλωτή.

2.5.2.1 Τεχνικά Χαρακτηριστικά HomeRF

Η τεχνολογία HomeRF και το πρωτόκολλο SWAP επιδρούν στα δύο κατώτερα επίπεδα του μοντέλου αναφοράς OSI και συγκεκριμένα στο φυσικό επίπεδο και στο υποεπίπεδο ελέγχου προσπέλασης μέσου (MAC sublayer) όπως φαίνεται και στο διπλανό σχήμα. Στα πιο πάνω επίπεδα χρησιμοποιούνται τα γνωστά πρωτόκολλα IP (επίπεδο δικτύου) και TCP, UDP (επίπεδο μεταφοράς) για την μεταφορά δεδομένων και το DECT για την διασύνδεση του δημόσιου τηλεφωνικού δικτύου (PSTN) με τις συσκευές HomeRF και τη μεταφορά φωνής.



2.1 Επίπεδα HomeRF

2.5.2.2 Φυσικό Επίπεδο HomeRF

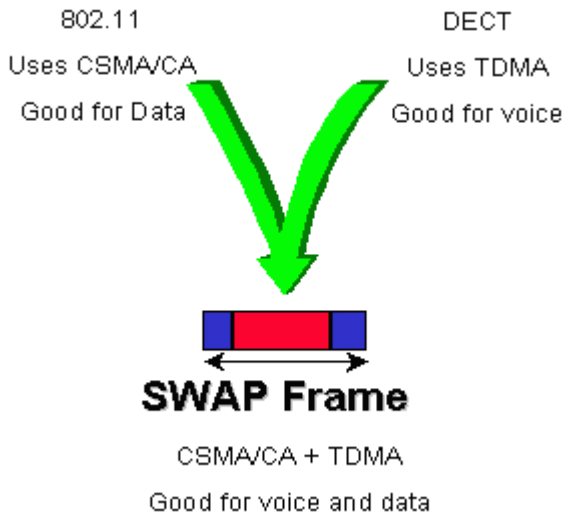
Το πρωτόκολλο SWAP υιοθέτησε τις προδιαγραφές του φυσικού επιπέδου του 802.11 για το φυσικό επίπεδο του HomeRF. Ωστόσο έγιναν αρκετές τροποποιήσεις σε αυτό, προκειμένου να μειωθεί το κόστος, να γίνει δυνατή η υλοποίηση σε ένα μόνο chip και παράλληλα να διατηρηθούν αξιόλογες επιδόσεις για οικιακή χρήση.

Για την ασύρματη μετάδοση των πληροφοριών (φωνής και δεδομένων) χρησιμοποιούνται δύο τεχνικές. Η διαμόρφωση FSK σταθερής περιβάλλουσας και τεχνικές απλωμένου φάσματος με εναλλαγή συχνότητας (FHSS με 50 hops/sec) για την μείωση των παρεμβολών από άλλες συσκευές. Οι ραδιοσυχνότητες που χρησιμοποιούνται βρίσκονται στην ζώνη συχνοτήτων ISM και συγκεκριμένα μεταξύ 2.4GHz και 2.4835GHz. Στο διαθέσιμο αυτό εύρος ζώνης υλοποιούνται 75 κανάλια του 1MHz με δυνατότητα μεταφοράς 1.6Mbps στην πρώτη έκδοση του HomeRF, έως και 10Mbps στην δεύτερη έκδοσή του, ενώ μέσα στο 2003 κατάφεραν να φτάσουν την ταχύτητα έως και 20Mbps. Η εμβέλεια του δικτύου είναι γύρω στα 50 μέτρα, απόσταση που θεωρείται αρκετά ικανοποιητική για να καλύψει τις ανάγκες ενός σπιτιού. Η μέγιστη εκπεμπόμενη ισχύς είναι τα 100mW (20dBm). Ακόμα έχει ληφθεί

μέριμνα και για τις φορητές συσκευές που λειτουργούν με μπαταρία, ώστε το chip του HomeRF να καταναλώνει περίπου 0dBm σε κατάσταση standby και γύρω στα 4dBm για την αποστολή πληροφοριών. Αξίζει να σημειωθεί ότι το HomeRF είναι ανθεκτικό και δεν επηρεάζεται από τις παρεμβολές. Αυτό επιτυγχάνεται αφού καταφέρνει να ανιχνεύσει την συγκεκριμένη συχνότητα που γίνεται η παρεμβολή και δίνοντας εντολή στον frequency hopper να μην χρησιμοποιεί το συγκεκριμένο κανάλι.

2.5.2.3 Υποεπίπεδο MAC HomeRF

Το υποεπίπεδο ελέγχου πρόσβασης του μέσου (MAC Sublayer) για το HomeRF, έχει βελτιστοποιηθεί για να γίνει πιο εύχρηστο για οικιακή χρήση, σχεδιαστεί ώστε να μεταφέρει φωνή και δεδομένα και ικανό να επικοινωνεί με το δημόσιο τηλεφωνικό δίκτυο μέσω του πρωτοκόλλου DECT. Το πρωτόκολλο SWAP συνδυάζει την αποδοτικότητα του CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance) και του TDMA (Time Division Multiple Access) για την μεταφορά δεδομένων και φωνής αντίστοιχα.



Σχ2.5.2.3 Πρωτόκολλο SWAP

Με αυτόν τον τρόπο επιτυγχάνονται ικανοποιητικά αποτελέσματα τόσο στη μετάδοση δεδομένων όπου χρησιμοποιείται ένα δοκιμασμένο και αξιόπιστο πρωτόκολλο όπως το CSMA/CA, όσο και στη μετάδοση φωνής όπου το TDMA εγγυάται την χωρίς καθυστέρηση μετάδοση έως και τεσσάρων

συνδέσεων υψηλής ποιότητας και δίνει την δυνατότητα σε συνεργασία με το DECT διαφόρων ευκολιών όπως αναγνώριση κλήσης, περιαγωγή από ένα Connection Point σε άλλο και ενδοεπικοινωνία μεταξύ δύο ασυρμάτων τηλεφώνων. Το υποεπίπεδο MAC επίσης προσφέρει διαχείριση ενέργειας στις φορητές συσκευές και ασφάλεια δεδομένων.

2.5.2.4 Πρωτόκολλο DECT

Το DECT (Digital Enhanced Cordless Telephony) αποτελεί τον διάδοχο του CT2 στα πρωτόκολλα για την ασύρματη τηλεφωνία. Λειτουργεί στην ζώνη συχνοτήτων μεταξύ 1.88GHz και 1.9GHz και υλοποιεί πολλαπλή πρόσβαση με διαίρεση συχνότητας και χρόνου (FDMA & TDMA), σε δέκα διαφορετικές συχνότητες εύρους 1MHz και 24 χρονοσχισμές με μέγιστη διαμεταγωγή 24kbps η καθεμία. Η μέγιστη εκπεμπόμενη ισχύς του DECT είναι τα 250mW (24dBm) και η εμβέλειά του ξεκινάει από τα 40m σε εσωτερικούς χώρους και φτάνει τα 350m στον ελεύθερο χώρο.

Το πρωτόκολλο DECT έχει σχεδιαστεί να είναι ευέλικτο ως προς την τοπολογία του δικτύου για να εξυπηρετήσει καλύτερα τις ανάγκες του χρήστη. Έτσι μπορεί να στηθεί ένα μονοκυψελικό δίκτυο με ένα σταθμό DECT και έως 8 ασύρματες συσκευές ή ένα πολυκυψελικό δίκτυο όπου οι ασύρματες συσκευές θα έχουν την δυνατότητα περιαγωγής από τον ένα σταθμό βάσης στον άλλο. Το δίκτυο μπορεί να ρυθμιστεί είτε ως «κλειστής ομάδας», όπου μόνο οι ασύρματες συσκευές που έχουν καταχωρηθεί στο δίκτυο μπορούν να το χρησιμοποιήσουν, είτε ως «ανοιχτό» και κάθε ασύρματη συσκευή DECT να μπορεί να χρησιμοποιεί τις υπηρεσίες του. Η δυναμική επιλογή καναλιών εξαλείφει την ανάγκη για κατανομή συχνοτήτων στους σταθμούς βάσεις κάνοντας έτσι πιο εύκολη την υλοποίηση ενός πολυκυψελικού συστήματος αλλά και την συνύπαρξη πολλών δικτύων DECT χωρίς παρεμβολές.

Για τις ανάγκες του HomeRF γίνανε ορισμένες μετατροπές στο πρωτόκολλο DECT. Η συχνότητα λειτουργίας του μεταφέρθηκε στην ζώνη ISM και η ισχύς του μειώθηκε στα 100mW (20dBm) για να συμμορφώνεται με τους κανονισμούς του FCC. Παράλληλα υλοποιήθηκε μηχανισμός εναλλαγής συχνότητας (FHSS) με 50hops/sec για την εξάλειψη θορύβου στενής ζώνης και τα κανάλια γίνανε 45 με εύρος 1.728MHz και μέγιστη διαμεταγωγή 1.152Mbps. Από αυτά τα δέκα χρησιμοποιούνται για τον έλεγχο ποιότητας μετάδοσης και τους μηχανισμούς διαπομπής και τα υπόλοιπα για μετάδοση δεδομένων.

2.5.2.5 Λειτουργία HomeRF

Στο HomeRF υποστηρίζονται ομότιμα προσωρινά δίκτυα (ad hoc) αλλά και δίκτυα διαχείρισης κεντρικού σημείου. Στα ομότιμα δίκτυα είναι δυνατή μόνο η μετάδοση δεδομένων και όλοι οι σταθμοί εργασίας είναι ίσοι. Η διαχείριση του δικτύου κατανέμεται και αυτή εξ' ίσου στους σταθμούς. Όταν όμως ζητείται μετάδοση φωνής όπου η καθυστέρηση μετάδοσης δυσχεραίνει την ποιότητα, τότε απαιτείται ένα σημείο σύνδεσης (Connection Point, CP) το οποίο θα αναλάβει την διαχείριση του δικτύου. Το σημείο σύνδεσης αποτελεί πύλη (gateway) των συσκευών HomeRF προς το δημόσιο τηλεφωνικό δίκτυο και είναι συνδεδεμένο συνήθως σε ένα PC και σπανιότερα αυτόνομο μηχάνημα.

Το πρωτόκολλο SWAP χρησιμοποιεί διευθύνσεις IP οπότε θεωρητικά μπορούν να συνδεθούν έως και 2^{48} συσκευές, αλλά οι περισσότεροι κατασκευαστές προϊόντων HomeRF συνιστούν ο μέγιστος αριθμός των συσκευών να μην ξεπερνάει τις δέκα. Οι συσκευές αυτές μπορεί να είναι ισόχρονες (Isochronous Clients) ή ασύγχρονες (Asynchronous Peers). Στις ισόχρονες συσκευές συγκαταλέγονται όλες εκείνες στις οποίες η καθυστέρηση στην μετάδοση παίζει σημαντικό ρόλο και υποβαθμίζει την ποιότητα επικοινωνίας. Τέτοιες είναι τα ασύρματα τηλέφωνα και handsets, τα οποία χρησιμοποιούν TDMA και είναι πάντα συνδεδεμένα με το σημείο σύνδεσης. Αυτό από την μεριά του, τους εξασφαλίζει συνεχώς διαθέσιμο εύρος ζώνης ώστε να περιοριστούν οι χρονικές καθυστερήσεις. Στις ασύγχρονες συσκευές

συμπεριλαμβάνονται όλες εκείνες που η καθυστέρηση στην μετάδοση δεν παίζει τόσο σημαντικό ρόλο. Τέτοιες συσκευές είναι οι υπολογιστές τα PDAs, οι εκτυπωτές και γενικά οι παραδοσιακές συσκευές δικτύωσης οι οποίες συνδέονται μέσω CSMA/CA. Το πρωτόκολλο SWAP λειτουργεί έξυπνα και συμπεριφέρεται σαν client/server στις συνδέσεις των ισόχρονων συσκευών με το σημείο σύνδεσης και σαν ομότιμο (peer to peer) στις συνδέσεις μεταξύ ασύγχρονων συσκευών.

2.5.2.6 Ασφάλεια HomeRF

Ένα από τα μεγαλύτερα ζήτημα που απασχολεί τους χρήστες των ασύρματων δικτύων είναι κατά πόσο είναι ασφαλή τα δεδομένα τους. Η ομάδα εργασίας του HomeRF, θέλοντας να κάνει το πρωτόκολλο SWAP όσο πιο ασφαλές αλλά και πιο διάφανο γίνεται προς τον τελικό χρήστη, όρισε τις εξής προδιαγραφές ασφαλείας:

- Κάθε δίκτυο HomeRF αποτελείται από το Network ID, ένα αριθμό από 24bit, ο οποίος είναι διαφορετικός για κάθε οικιακό δίκτυο. Αν σε ένα περιφερειακό δεν έχει οριστεί το σωστό Network ID τότε αυτό δεν θα μπορεί να συνεργαστεί με το υπόλοιπο δίκτυο.
- Τα δεδομένα στέλνονται κρυπτογραφημένα με ένα κλειδί των 56bit στο HomeRF 1.0 ενώ το HomeRF 2.0 θα ακολουθεί κρυπτογράφηση με κλειδί των 128bit. Ο αλγόριθμος κρυπτογράφησης, αν και πολύ πιο ισχυρός από τον αλγόριθμο A5 του GSM είναι ελαφρώς πιο δύσκολο να υλοποιηθεί στο hardware.

Τα παραπάνω μέτρα ασφαλείας, σε συνδυασμό με το γεγονός ότι χρησιμοποιούνται τεχνικές FHSS στο φυσικό επίπεδο και η εμβέλεια του δικτύου δεν ξεπερνάει τα 50m κάνουν το HomeRF ένα αρκετά ασφαλές δίκτυο.

2.5.2.7 HomeRF Συνοπτικά

Στον παρακάτω πίνακα φαίνονται εν συντομία τα κυριότερα χαρακτηριστικά και τα πλεονεκτήματά τους στο πρωτόκολλο HomeRF.

Χαρακτηριστικό	Πλεονεκτήματα
Το HomeRF είναι φτηνό, αξιόπιστο και εύκολο στην εγκατάσταση.	• Ιδανική λύση για την ασύρματη δικτύωση ενός σπιτιού. • Η λειτουργία του είναι διάφανη ως προς τον τελικό χρήστη.
Δημιουργία πρωτοκόλλου SWAP από την ομάδα εργασίας του HomeRF.	• Φτιάχτηκε από την αρχή με σκοπό να καλύψει τις ανάγκες δικτύωσης ενός σπιτιού. • Κατασκευή διαλειτουργικών συσκευών από πολλές εταιρίες. • Ασύρματη δικτύωση φωνής και δεδομένων κάτω από ένα κοινό interface. • Δημιουργία ενός προτύπου για τα ασύρματα ψηφιακά τηλέφωνα, που θα επιτρέπει την διαλειτουργικότητά τους.
Χρήση συχνότητας 2.4GHz (ISM)	• Συσκευές HomeRF λειτουργούν σε παγ-κόσμιο επίπεδο.
Το SWAP βασίζεται στα CSMA/CA και TDMA καθώς και στο DECT.	• Υποστηρίζεται η μετάδοση φωνής και δε-δομένων. • Η μετάδοση δεδομένων φτάνει στα 1.6Mbps(HomeRF 1.0), 10Mbps(HomeRF 2.0) και αναμένεται να φτάσει τα 20Mbps μέσα στο 2003. • Συνεργασία και διαλειτουργικότητα με το PSTN. • Παρέχεται η υποστήριξη 4 ταυτόχρονων συνδέσεων ομιλίας (8 στο HomeRF 2.0) και 8 ακουστικών. • Παροχή ευκολιών παρόμοιων με αυτές του PSTN, όπως αναγνώριση και εκτροπή κλήσης και ενδοεπικοινωνία.
Το HomeRF καταναλώνει πολύ λίγη	• Κατάλληλο για φορητές συσκευές που δουλεύουν με μπαταρία.

ενέργεια.	
24bit Network ID και κρυπτογράφηση.	• Μόνο εξουσιοδοτημένες συσκευές, που έχουν το Network ID μπορούν να χρησιμοποιήσουν τους πόρους του δικτύου. • Υψηλός βαθμός ασφάλειας στην επικοινωνία μεταξύ των συσκευών.

3. Υπόεπίπεδο Mac του 802.11

3.1 Εισαγωγή

Κάτω από τα standards της σειράς IEEE 802, το datalink επίπεδο του OSI μοντέλου, είναι υποδιαιρεμένο σε δυο υποεπίπεδα (sublayers): το Logical Link Control (LLC) και το Medium Access Control (MAC).

Το υποεπίπεδο Mac του 802.11 υποστηρίζει όλα τα στρώματα και προσφέρει υπηρεσίες αξιόπιστης μεταφοράς δεδομένων και πρόσβασης στο μέσο στα ανώτερα στρώματα. Αυτό ισχύει στην περίπτωση που το κανάλι δεν είναι απασχολημένο, οπότε ελέγχει την περίπτωση εμφάνισης κάποιου collision.Αν βρει collision ακολουθούνται κάποια βήματα που θα αναλυθούν παρακάτω.

Το MAC υποεπίπεδο είναι ένα interface μεταξύ δεδομένων χρήστη και φυσικής τοποθέτησης, και ανάκτησης δεδομένων στο δίκτυο. Ακόμα θα μπορούσαμε να πούμε ότι οι όποιες διαφοροποιήσεις του από τα αντίστοιχο MAC των ενσύρματων δικτύων οφείλονται περισσότερο στις ιδιαιτερότητες του ασύρματου μέσου μετάδοσης που χρησιμοποιείται στο φυσικό επίπεδο.

Σαν μηχανισμός πρόσβασης στο μέσο έχει επιλεχτεί ο CSMA (Carrier Sense Multiple Access). Υπάρχουν δύο υποκατηγορίες αυτού του μηχανισμού, η CSMA/CD (Collision Detection) και η CSMA/CA (Collision Avoidance). Με τη πρώτη απλά εντοπίζονται οι συγκρούσεις, ενώ με τη δεύτερη αποφεύγονται κιόλας. Στο συγκεκριμένο πρωτόκολλο επιλέχτηκε η CSMA/CA γιατί ο δέκτης είχε αδυναμία στο να αντιλαμβάνεται την κατάσταση του ασύρματου μέσου την χρονική στιγμή που μετέδιδε κάποια πληροφορία. Αυτό είχε ως συνέπεια όταν γινόταν κάποια σύγκρουση, δηλαδή όταν δύο ή περισσότεροι σταθμοί προσπαθούσαν να μεταδώσουν την ίδια ακριβώς χρονική στιγμή, αυτή να γίνετε αντιληπτή μόνο εκ του αποτελέσματος που είναι η μη παράδοση των πακέτων πληροφορίας.

Το Mac του 802.11 έχει δημιουργηθεί ώστε να προσφέρει κάποιους μηχανισμούς για να μπορέσει να ξεπεράσει κάποια προβλήματα που

αντιμετώπιζε. Τέτοια προβλήματα ήταν η κακή ποιότητα της ασύρματης ζεύξης λόγω θορύβου ή παρεμβολών, η πιθανότητα κάποιος κόμβος να βγει εκτός εμβέλειας δικτύου ακόμα και η ύπαρξη κρυμμένων κόμβων(hidden nodes), τα οποία δεν τα συναντούσαμε σε ενσύρματα δίκτυα. Οι μηχανισμοί που χρησιμοποιούνται για την καταπολέμηση αυτών των προβλημάτων είναι η θετική επιβεβαίωση(positive acknowledgment) κάθε πλαισίου και η ανταλλαγή πλαισίων RTS(Request To Send) και CTS(Clear To Send) πριν τη μετάδοση κάποιου πλαισίου.

3.2 Μέθοδοι Προσπέλασης Μέσου

Ο μηχανισμός πρόσβασης στο μέσο που χρησιμοποιείται από το 802.11 MAC είναι ο CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance). Έχουν προβλεφθεί δύο τρόποι λειτουργίας, ένας αποκεντρωμένος μέσω του αλγορίθμου DCF (Distributed Coordination Function) και ένας με κεντρικό έλεγχο μέσω του αλγορίθμου PCF (Point Coordination Function) που αποτελεί προέκταση του DCF. Ο αλγόριθμος PCF εκτελείται μόνο σε AP(Access Point), οπότε μπορεί να χρησιμοποιηθεί μόνο σε infrastructure δίκτυα. Μία τρίτη επιλογή προσφέρεται στο υποπρότυπο 802.11e, το οποίο συμπληρώνει το MAC υπόστρωμα του 802.11 και ορίζει έναν επιπλέον μηχανισμός ελέγχου πρόσβασης μέσω του αλγορίθμου HCF (Hybrid Coordination Function). Ο αλγόριθμος DCF είναι κατάλληλος για εξυπηρέτηση ασύγχρονης κίνησης, ενώ ο PCF είναι κατάλληλος για σύγχρονη κίνηση. Ο HCF εισάγει ένα σχήμα προτεραιοτήτων για να προσφέρει συγκεκριμένη ποιότητα υπηρεσίας (Quality of Service – QoS).

3.2.1 Πρόσβαση στο Μέσο με χρήση του Αλγορίθμου DCF

Στο κεφάλαιο αυτό παρουσιάζεται ο αλγόριθμος DCF. Με τη χρήση αυτού του αλγόριθμου επιτυγχάνεται η πρόσβαση στο μέσο, δίνοντας έμφαση στην αντιμετώπιση μιας αποτυχημένης προσπάθειας μετάδοσης. Σε

περίπτωση που περισσότεροι του ενός σταθμοί διεκδικούν τον έλεγχο του μέσου, εισάγεται η έννοια του παραθύρου ανταγωνισμού για να βρεθεί λύση.

3.2.1.1 Ο Αλγόριθμος DCF

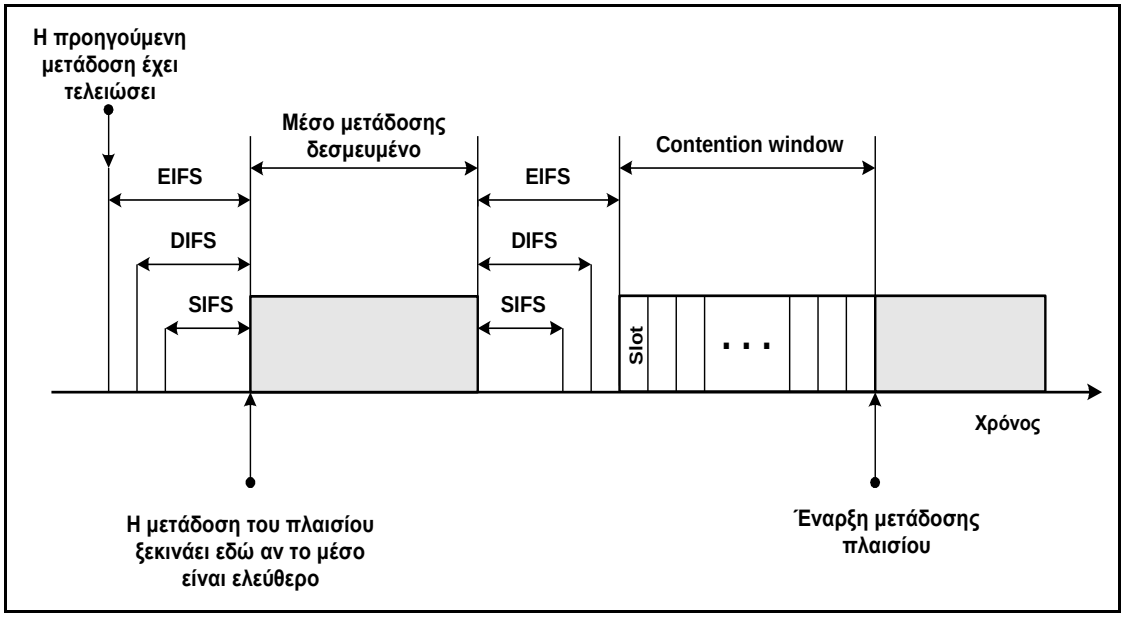
Ο αλγόριθμος DCF, όπως έχει ήδη αναφερθεί, είναι αποκεντρωμένος και έτσι μπορεί να χρησιμοποιηθεί σε κάθε είδους ασύρματο δίκτυο. Τα βασικά βήματα του, όπου πρέπει να ακολουθήσει κάθε σταθμός πριν εκπέμψει κάποιο πλαίσιο είναι τα εξής:

Αρχικά κάθε σταθμός, πριν επιχειρήσει να εκπέμψει, ελέγχει το μέσο μετάδοσης για να δει αν είναι διαθέσιμο. Ο έλεγχος γίνεται και σε φυσικό επίπεδο και μέσω εικονικής ανίχνευσης φέροντος.

Αν το μέσο μετάδοσης είναι δεσμευμένο τότε ο σταθμός συνεχίζει να ελέγχει το ασύρματο μέσο περιοδικά περιμένοντας να ελευθερωθεί. Αν το μέσο είναι διαθέσιμο ο σταθμός περιμένει ένα χρονικό διάστημα που εξαρτάται από το είδος του πλαισίου που θέλει να μεταδώσει (IFS) και ελέγχει ξανά το μέσο. Ο χρόνος αναμονής που χρησιμοποιείται συνήθως είναι ο DIFS. Στην περίπτωση που ο σταθμός θέλει να στείλει πλαίσιο CTS, πλαίσιο θετικής επιβεβαίωσης (ACK), ή τμήμα (fragment) μεγαλύτερου πλαισίου τότε ο χρόνος αναμονής είναι ο SIFS. Τέλος, στην περίπτωση που η μετάδοση του προηγούμενου πλαισίου περιείχε λάθη τότε ο χρόνος αναμονής είναι ο EIFS.

Αν πάλι το μέσο είναι ελεύθερο τότε ο σταθμός μεταδίδει το πλαίσιο που θέλει. Αν το μέσο είναι δεσμευμένο ο σταθμός περιμένει μέχρι το μέσο να μείνει ελεύθερο για IFS. Τότε ξεκινάει τη διαδικασία της δυαδικής εκθετικής υποχώρησης (binary exponential backoff) για να καθορίσει πόσο θα είναι το επιπλέον χρονικό διάστημα αναμονής. Αυτό γίνεται επιλέγοντας τυχαία μια σχισμή του παραθύρου ανταγωνισμού (contention window). Αφού περάσει και αυτό το τελευταίο χρονικό διάστημα, ο σταθμός μεταδίδει το πλαίσιο που θέλει.

Αν η μετάδοση είναι αποτυχημένη θεωρείται ότι έχει συμβεί σύγκρουση (collision). Τότε ο σταθμός επιλέγει πάλι τυχαία μια σχισμή του contention window, το οποίο όμως είναι μεγαλύτερο αυτή τη φορά, και επιχειρεί ξανά να μεταδώσει. Αυτή η διαδικασία επαναλαμβάνεται μέχρι να υπάρξει επιτυχής μετάδοση του πλαισίου ή να απορριφθεί το πλαίσιο.



Σχήμα 3.2.1.1: Διαδικασία πρόσβασης στο μέσο με χρήση του αλγορίθμου DCF

Πρόκειται για τον βασικό μηχανισμό ώστε να μπορέσει ένας σταθμός να αποκτήσει τον έλεγχο του μέσου. Υπάρχουν και άλλοι κανόνες που συμπληρώνουν τα παραπάνω και εξαρτώνται από την συγκεκριμένη κατάσταση ή από την κατάληξη της προηγούμενης μετάδοσης. Μερικοί τέτοιοι κανόνες παρατίθενται στη συνέχεια.

Κάθε μετάδοση πλαισίου θεωρείται επιτυχημένη μόνο αν ληφθεί σωστά και το αντίστοιχο πλαίσιο ACK. Όλα τα πλαίσια μονοεκπομπής (unicast) πρέπει να επιβεβαιώνονται από τον παραλήπτη. Αντίθετα, πλαίσια τύπου πολυεκπομπής (multicast) και ευρυεκπομπής (broadcast) δεν απαιτούν επιβεβαίωση. Είναι ευθύνη του αποστολέα να ξαναστείλει το πλαίσιο αν δεν ληφθεί η ανάλογη επιβεβαίωση. Κάθε αποτυχία αποστολής που οφείλεται είτε σε αδυναμία ελέγχου του μέσου είτε σε μη λήψη ACK αυξάνει έναν μετρητή (retry counter) που χρησιμεύει για τον προσδιορισμό του χρόνου μέχρι την επόμενη προσπάθεια αποστολής του πλαισίου.

Κάθε σταθμός που συμμετέχει στην ανταλλαγή πολλαπλών πλαισίων μπορεί να ανανεώνει το NAV μετά από κάθε λήψη πλαισίου. Έτσι ο έλεγχος του μέσου διατηρείται μέχρι να ολοκληρωθεί η ανταλλαγή. Η διατήρηση του ελέγχου μπορεί να εξασφαλιστεί επιπλέον με τη χρήση του SIFS στις περιπτώσεις που έχουν ήδη αναφερθεί.

Υπάρχουν συγκεκριμένα κατώφλια μεγέθους για τα πλαίσια. Κάθε πλαίσιο μεγαλύτερο από το κατώφλι RTS πρέπει να σταλεί χρησιμοποιώντας

το μηχανισμό RTS/CTS (που θα παρουσιαστεί στη συνέχεια). Κάθε πλαίσιο μεγαλύτερο από το κατώφλι κατακερματισμού (fragmentation threshold) διασπάται σε μικρότερα πλαίσια πριν σταλεί.

3.2.1.2Αντιμετώπιση αποτυχημένης προσπάθειας μετάδοσης

Όπως έχει ήδη αναφερθεί, ο εντοπισμός και η διόρθωση κάποιου λάθους κατά τη μετάδοση είναι ευθύνη του αποστολέα. Σε περίπτωση που η αποστολή ενός πλαισίου δεν ολοκληρωθεί κανονικά ο αποστολέας πρέπει να το ξαναστείλει. Για τον έλεγχο της διαδικασίας αυτής κάθε πλαίσιο έχει έναν μετρητή (retry counter) συσχετισμένο με αυτό. Κάθε φορά που το πλαίσιο αυτό επανεκπέμπεται ο retry counter που του αντιστοιχεί αυξάνεται κατά 1. Αν ο μετρητής ξεπεράσει κάποιο προκαθορισμένο όριο, το πλαίσιο απορρίπτεται και η απώλειά του αναφέρεται στα υψηλότερα στρώματα.

Κάθε σταθμός διακρίνει τα πλαίσια σε short και long. Ως short χαρακτηρίζονται τα πλαίσια που έχουν μήκος μικρότερο από το RTS threshold και ως long τα υπόλοιπα. Ο σταθμός διατηρεί και δύο αντίστοιχους μετρητές, τους short retry count και long retry count. Κάθε φορά που η μετάδοση ενός πλαισίου αποτυγχάνει ο αντίστοιχος μετρητής αυξάνεται. Οι μετρητές αυτοί μηδενίζονται σε συγκεκριμένες περιπτώσεις.

Για τον short retry count αυτές είναι :

- Λήψη CTS πλαισίου σε απάντηση ενός RTS.
- Λήψη πλαισίου ACK μετά από μη κατακερματισμένη μετάδοση πλαισίου.
- Λήψη broadcast ή multicast πλαισίου.
- Αντίστοιχα, ο long retry count μηδενίζεται στις ακόλουθες περιπτώσεις :
- Λήψη πλαισίου ACK για πλαίσιο μεγαλύτερο του RTS threshold.
- Λήψη broadcast ή multicast πλαισίου.

Σε περίπτωση κατακερματισμού ενός πλαισίου όλα τα fragments έχουν έναν μετρητή διάρκειας ζωής (lifetime counter). Αυτός ξεκινάει όταν μεταδοθεί το πρώτο fragment. Αν μέχρι να μηδενιστεί δεν έχει μεταδοθεί ολόκληρο το πλαίσιο, αυτό απορρίπτεται και δεν γίνεται προσπάθεια μετάδοσης των υπόλοιπων fragments του.

3.2.1.3 Παράθυρο Ανταγωνισμού

Σε προηγούμενη ενότητα ήδη έχει αναφερθεί η έννοια του παραθύρου ανταγωνισμού (contention window) και που χρησιμεύει. Το contention window χωρίζεται σε σχισμές (slots) που η διάρκειά τους είναι εξαρτώμενη από το φυσικό στρώμα. Κάθε σταθμός διαλέγει μια σχισμή και περιμένει τη σειρά του πριν επιχειρήσει να αποκτήσει πρόσβαση στο μέσο μετάδοσης. Η επιλογή γίνεται τυχαία, με χρήση μιας διαδικασίας που ονομάζεται δυαδική εκθετική υποχώρηση. Αν περισσότεροι του ενός σταθμοί διεκδικούν τον έλεγχο του μέσου, νικητής θα αναδειχθεί αυτός που θα επιλέξει την πρώτη σχισμή.

Κάθε σταθμός επιλέγει τη σχισμή του contention window μέσα από ένα εύρος τιμών που αυξάνεται όσο αποτυγχάνει η επιθυμητή μετάδοση πλαισίου. Υπενθυμίζεται ότι η μετάδοση θεωρείται αποτυχημένη αν δεν ληφθεί έγκαιρα επιβεβαίωση ή αν ο σταθμός δεν καταφέρει να πάρει τον έλεγχο του μέσου για να μεταδώσει το πλαίσιο. Το εύρος τιμών από το οποίο καλείται να επιλέξει τυχαία ο κάθε σταθμός είναι πάντα αριθμός κατά ένα μικρότερος από κάποια δύναμη του 2. Κάθε φορά που η μετάδοση αποτυγχάνει το εύρος υπολογίζεται ξανά με βάση την αμέσως επόμενη δύναμη του 2. Αυτό γίνεται μέχρι να φτάσει το εύρος μία μέγιστη τιμή, οπότε δεν μεγαλώνει άλλο. Το εύρος αυτό επανέρχεται στην ελάχιστη τιμή του μετά από επιτυχημένη μετάδοση ή από απόρριψη του προς μετάδοση πλαισίου. Κάθε φυσικό στρώμα χρησιμοποιεί δικές του παραμέτρους για την παραπάνω διαδικασία. Με αυτόν τον τρόπο εξασφαλίζεται η σταθερότητα της λειτουργίας του δικτύου, ακόμη και κάτω από καταστάσεις έντονης κίνησης.

3.2.2 Πρόσβαση στο Μέσο με χρήση του Αλγορίθμου PCF

Ο αλγόριθμος PCF είναι η εναλλακτική λύση στο πρόβλημα του ελέγχου της πρόσβασης στο μέσο. Η λειτουργία του μοιάζει αρκετά με σχήματα ελέγχου πρόσβασης με σκυτάλη (token based). Ο συγκεκριμένος αλγόριθμος δεν χρησιμοποιείται ιδιαίτερα στα προϊόντα που κυκλοφορούν στην αγορά, ενώ οι
κατασκευαστές δεν είναι υποχρεωμένοι να τον υποστηρίξουν, αφού αποτελεί προαιρετικό μέρος του προτύπου 802.11. Επιπλέον, εφόσον απαιτεί κεντρικό έλεγχο από κάποιο AP, μπορεί να χρησιμοποιηθεί μόνο σε infrastructure δίκτυα.

Σκοπός του PCF είναι να προσφέρει πρόσβαση στο μέσο χωρίς ανταγωνισμό μεταξύ των σταθμών (contention - free medium access). Υλοποιείται χρησιμοποιώντας την υποδομή του αλγορίθμου DCF και προσθέτοντας την επιπλέον λειτουργικότητα. Η χρήση του συνεπάγεται τη δημιουργία χρονικών περιόδων χωρίς ανταγωνισμό (contention - free periods), ενώ κατά τον υπόλοιπο χρόνο η πρόσβαση ελέγχεται κανονικά από τον DCF (contention periods). Υπάρχει δυνατότητα καθορισμού της σχέσης των δύο παραπάνω χρονικών περιόδων ανάλογα με τη χρήση του δικτύου. Αυτές οι περίοδοι επαναλαμβάνονται διαδοχικά, ενώ η διάρκειά τους κάθε φορά ονομάζεται contention - free repetition interval.

Κατά τη διάρκεια του contention - free period η διαδικασία πρόσβασης στο μέσο για τους σταθμούς ελέγχεται από το AP. Στην αρχή της περιόδου αυτής το AP στέλνει ένα πλαίσιο Beacon το οποίο περιέχει τη μέγιστη διάρκεια της contention – free period. Οι σταθμοί θέτουν το NAV σε αυτήν την τιμή αποτρέποντας την πρόσβαση μέσω του DCF γι’ αυτήν την περίοδο.

Όταν το AP πάρει τον έλεγχο του μέσου δίνει την άδεια σε κάθε σταθμό διαδοχικά να μεταδώσει στέλνοντάς του ένα polling πλαίσιο (CF – Poll). Τα polling πλαίσια πρέπει να επιβεβαιωθούν από τους σταθμούς. Αν κάποιος σταθμός δεν στείλει ACK αφού λάβει το polling πλαίσιο το AP προχωράει στον επόμενο σταθμό. Όλοι οι σταθμοί κατά τη διαδικασία του association με το AP μπαίνουν σε μία λίστα (polling list)

ώστε το AP να τους δίνει το δικαίωμα μετάδοσης κατά την contention - free period. Σημειώνεται ότι κάθε πλαίσιο polling δίνει στο σταθμό που το έλαβε δικαίωμα μετάδοσης ενός μόνο πλαισίου.

Για να διασφαλιστεί περισσότερο ότι ο έλεγχος του μέσου θα μείνει στο AP κατά την contention - free period, όλοι οι χρόνοι αναμονής που χρησιμοποιούνται είναι SIFS ή PIFS. Ο χρόνος αναμονής από το AP για να επιβεβαιωθεί το polling πλαίσιο που έστειλε είναι ίσος με τον PIFS ενώ όλοι οι υπόλοιποι χρόνοι αναμονής είναι ίσοι με SIFS.

Η διάρκεια της contention - free period πρέπει να είναι τουλάχιστον ίση με το χρόνο που απαιτείται να μεταδοθεί και να επιβεβαιωθεί ένα πλαίσιο μέγιστου μεγέθους. Σε περίπτωση που η contention period δεν τελειώσει όταν πρέπει να αρχίσει η contention - free period, η δεύτερη έχει μειωμένη διάρκεια. Το AP που τρέχει τον PCF μπορεί να διακόψει νωρίτερα την contention - free period για οποιοδήποτε λόγο. Τέλος, για να εκμεταλλεύονται οι σταθμοί όσο το δυνατόν περισσότερο την contention - free period είναι σύνηθες να συνδυάζουν σε ένα πλαίσιο επιβεβαιώσεις, polling και μεταφορά δεδομένων, οπότε προκύπτουν σύνθετα πλαίσια με πολλές λειτουργίες. Για παράδειγμα ένας σταθμός μπορεί να συνδυάσει τη μεταφορά δεδομένων με την επιβεβαίωση του πλαισίου polling σε ένα κοινό πλαίσιο και να το στείλει. Το AP που θα το λάβει μπορεί να στείλει σε κοινό πλαίσιο την επιβεβαίωση λήψης των δεδομένων στον αποστολέα και τα δεδομένα στον παραλήπτη.

3.2.3 Πρόσβαση στο Μέσο με χρήση του Αλγορίθμου HCF

Ο αλγόριθμος πρόσβασης HCF είναι ο νεότερος αλγόριθμος πρόσβασης που θα προστεθεί στο υπόστρωμα MAC όταν ολοκληρωθούν οι εργασίες της ομάδας 802.11e. Ονομάζεται και Enhanced DCF (EDCF) και σκοπός του είναι να προσφέρει πρόσβαση στο μέσο είτε με ανταγωνισμό είτε χωρίς ανταγωνισμό μεταξύ των σταθμών, προσφέροντας ταυτόχρονα έναν μηχανισμό προτεραιοτήτων. Χρησιμοποιεί στοιχεία από τους DCF και PCF και διατηρεί τη συμβατότητα με αυτούς.

Κατά τη λειτουργία του EDCF ορίζονται κάποιες κατηγορίες πρόσβασης (Access Categories – ACs) και οι αντίστοιχοι μηχανισμοί πρόσβασης. Κάθε AC αντιστοιχίζεται με ροές πληροφορίας συγκεκριμένης προτεραιότητας (για παράδειγμα βέλτιστης προσπάθειας, video, φωνής). Κάθε AC χρησιμοποιεί μία παραλλαγή του DCF για να αποκτήσει πρόσβαση στο μέσο. Υπάρχει διαφοροποίηση τόσο του contention window (CW), όσο και του IFS, που σε αυτήν την περίπτωση ονομάζεται arbitration IFS (AIFS), ανάλογα με την AC. Το AIFS είναι τουλάχιστον ίσο με DIFS. Επιπλέον, κάθε AC σε έναν σταθμό συμπεριφέρεται σαν εικονικός σταθμός (virtual station), προσπαθώντας να αποκτήσει πρόσβαση στο μέσο με τις δικές τις παραμέτρους. Οι συγκρούσεις εντός του ίδιου σταθμού διευθετούνται σαν τις κλασσικές συγκρούσεις στο ασύρματο μέσο.

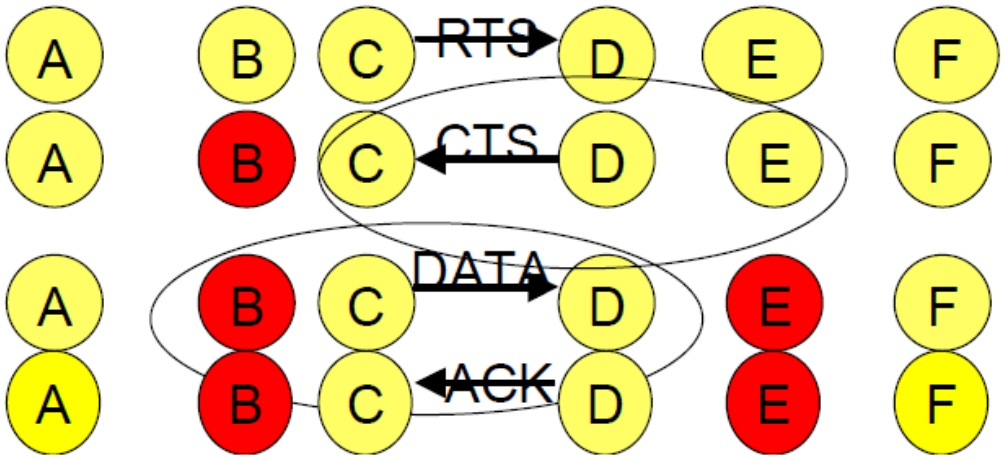
Για την κεντρικά ελεγχόμενη λειτουργία του αλγορίθμου χρειάζεται, όπως και στον PCF, ένα AP στο οποίο θα τρέχει ο αλγόριθμος ελέγχου HC (Hybrid Coordinator). Ο τελευταίος έχει πρόσβαση στο μέσο με μεγαλύτερη προτεραιότητα από τον EDCF και έχει την δυνατότητα να προσφέρει QoS χαρακτηριστικά στην κίνηση από και προς τους σταθμούς . Μπορεί να λειτουργεί και σε contention periods, σε αντίθεση με τον PCF

3.2.4 Request To Send / Clear To Send

Ο μηχανισμός αυτός χρησιμοποιείται για να διασφαλιστεί ότι μία συγκεκριμένη ανταλλαγή πλαισίων θα γίνει χωρίς διακοπή από μετάδοση τρίτου σταθμού το 802.11. Αυτός ο μηχανισμός διαφοροποιεί την διαδικασία αποστολής πλαισίου που είχε αναφερθεί σε προηγούμενη παράγραφο, εισάγοντας δύο επιπλέον πλαίσια, τα RTS (Ready To Send) και CTS (Clear To Send). Ο μηχανισμός αυτός εκτός ότι προστατεύει την ανταλλαγή πλαισίων, βελτιώνει κιόλας την απόδοση της χρήσης του ασύρματου δικτύου σε περιπτώσεις μεγάλου φόρτου εξαιτίας της ύπαρξης πολλών τερματικών και αντιμετωπίζει το πρόβλημα του κρυμμένου κόμβου. Αν όμως χρησιμοποιείται χωρίς λόγο, έχει το ακριβώς αντίθετο αποτέλεσμα, εφόσον προσθέτει επιπλέον φορτίο στο ασύρματο δίκτυο.

Ο κεντρικός στόχος του μηχανισμού είναι να στέλνει ο αποστολέας αρχικά ένα πλαίσιο RTS στον παραλήπτη που δεν περιέχει δεδομένα. Σκοπός του πλαισίου αυτού είναι να δεσμεύσει ο αποστολέας το μέσο μετάδοσης για όσο χρόνο υπολογίζει ότι θα διαρκέσει η αποστολή του πλαισίου δεδομένων και να το ανακοινώσει στους υπόλοιπους σταθμούς μέσω του μετρητή NAV στο πλαίσιο RTS. Αυτό που κάνει ο παραλήπτης αφού λάβει το RTS είναι να απαντήσει με ένα πλαίσιο CTS. Υπενθυμίζεται ότι η αποστολή πλαισίου CTS γίνεται με το συντομότερο χρόνο αναμονής SIFS. Τότε ο αποστολέας στέλνει το πλαίσιο δεδομένων και περιμένει την επιβεβαίωση ορθής λήψης του από τον παραλήπτη. Έτσι η διαδικασία αποστολής πλαισίου απαιτεί την ανταλλαγή τεσσάρων πλαισίων για να ολοκληρωθεί σωστά.

Για να γίνει αντιληπτή ακόμα καλύτερα η παραπάνω διαδικασία θα αναλύσουμε ένα παράδειγμα που απεικονίζεται κ με την παρακάτω εικόνα. Όλοι οι σταθμοί που θα ακούσουν το πλαίσιο CTS παραμένουν σιωπηλοί, ώστε να αποφευχθούν οι συγκρούσεις κατά την μετάδοση του πλαισίου δεδομένων από το σταθμό C στον D. Επιπλέον όσοι σταθμοί ακούσουν το πλαίσιο RTS παραμένουν σιωπηλοί, για να μην δημιουργήσουν σύγκρουση κατά την μετάδοση της επιβεβαίωσης ACK από τον σταθμό D στον C. Το διάστημα στο οποίο οι σταθμοί παραμένουν σιωπηλοί περιλαμβάνεται σε ένα πεδίο RTS/CTS πλαισίων και εξαρτάται από την διάρκεια του πλαισίου πληροφορίας. Το πλαίσιο επιβεβαίωσης χρησιμοποιείται, διότι παρά την ύπαρξη του RTS/CTS μηχανισμού, υπάρχει πάντα η πιθανότητα λαθών λόγω του θορύβου του καναλιού καθώς επίσης και η πιθανότητα σύγκρουσης. Αν ένας σταθμός δεν λάβει πλαίσιο επιβεβαίωσης, επαναμεταδίδει τότε το πλαίσιο.

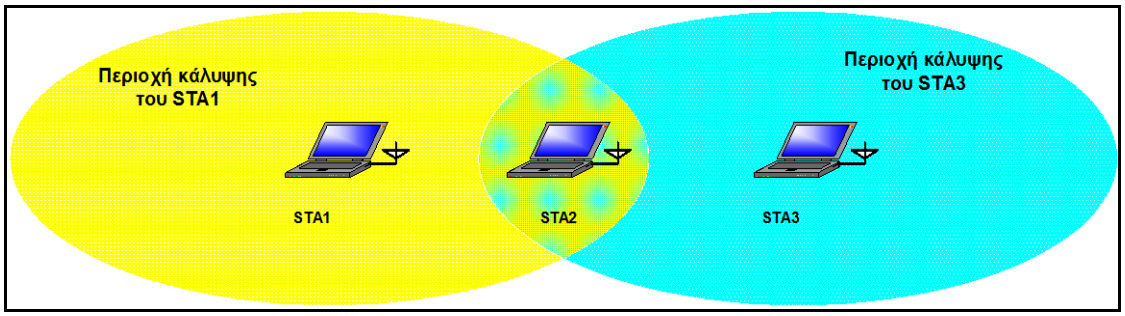


Σχήμα 3.2.4 Μηχανισμός RTS/CTS

Ο μηχανισμός αυτός ενεργοποιείται αυτόματα όταν το μέγεθος ενός πλαισίου είναι μεγαλύτερο από το RTS threshold για να διασφαλίσει την ομαλή αποστολή μεγάλων πλαισίων. Επίσης μπορεί να χρησιμοποιηθεί σε συνδυασμό με τον κατακερματισμό. Συνήθως τα κατώφλια RTS threshold και Fragmentation threshold τίθενται στην ίδια τιμή. Αυτό έχει σαν αποτέλεσμα όλα τα fragments ενός πλαισίου να μεταδίδονται με τη σειρά προστατευμένα από το μηχανισμό RTS/CTS. Σε αυτήν την περίπτωση το πλαίσιο RTS που στέλνει ο αποστολέας στην αρχή της διαδικασίας δεσμεύει το μέσο για όσο χρόνο απαιτεί η αποστολή και η επιβεβαίωση του πρώτου τμήματος του πλαισίου. Όταν ο αποστολέας πάρει το CTS αρχίζει να στέλνει διαδοχικά τα τμήματα περιμένοντας φυσικά κάθε φορά για το αντίστοιχο πλαίσιο ACK, του οποίου η αποστολή γίνεται με χρήση του χρόνου SIFS. Ο αποστολέας και ο παραλήπτης ανανεώνουν το NAV κατά τη διάρκεια της ανταλλαγής πλαισίων, εξασφαλίζοντας ότι θα διατηρήσουν τον έλεγχο του μέσου. Το μέσο αποδεσμεύεται με την λήψη από τον αποστολέα του τελευταίου πλαισίου ACK από τον παραλήπτη. Σημειώνεται εδώ ότι ένας άλλος τρόπος μετάδοσης των τμημάτων ενός πλαισίου είναι να δεσμεύσει ο αποστολέας το μέσο με χρήση του μετρητή NAV στο πρώτο τμήμα που θα στείλει.

3.2.5 Πρόβλημα ύπαρξης κρυφών και εκτεθειμένων σταθμών

Ο μηχανισμός RTS/CTS αντιμετωπίζει αποτελεσματικά το πρόβλημα ύπαρξης κρυμμένου κόμβου (hidden node). Το πρόβλημα αυτό φαίνεται στο παρακάτω σχήμα.



Σχήμα 3.2.5 Πρόβλημα κρυμμένου κόμβου

Όπως φαίνεται στο Σχήμα, ο σταθμός STA1 δεν γνωρίζει την ύπαρξη του STA3, εφόσον αυτός είναι έξω από την περιοχή κάλυψής του. Το ίδιο συμβαίνει και με τον STA3. Ο STA2 βρίσκεται στην κοινή περιοχή κάλυψης των STA1 και STA3 και μπορεί να ανταλλάσσει πλαίσια και με τους δύο. Το πρόβλημα προκύπτει όταν οι STA1 και STA3 επιχειρούν να επικοινωνήσουν με τον STA2 ταυτόχρονα. Τότε προκύπτουν συγκρούσεις και τα πλαίσια που έχουν εκπεμφθεί χάνονται.

Αν όμως χρησιμοποιηθεί ο μηχανισμός RTS/CTS ο κόμβος STA2 θα εκπέμψει ένα πλαίσιο CTS σε απάντηση του RTS που θα του έχει στείλει νωρίτερα ο STA1. Αυτό το πλαίσιο CTS θα το λάβει και ο STA3 και έτσι θα αποφύγει να μεταδώσει κι αυτός κάποιο πλαίσιο που θα προκαλούσε σύγκρουση. Τον ίδιο ρόλο παίζει και το πλαίσιο RTS που μεταδίδει ο STA1, δηλαδή ενημερώνει άλλους κρυφούς κόμβους που μπορεί να βρίσκονται γύρω του και δεν βλέπουν τον STA2.

3.2.6 Εκθετικός Αλγόριθμος Αποφυγής Συγκρούσεων

Η υποχώρηση είναι μια γνωστή μέθοδος για την επίλυση του προβλήματος της σύγκρουσης που μπορεί να παρουσιαστεί όταν δύο σταθμοί επιθυμούν ταυτόχρονη πρόσβαση στο μέσο. Η μέθοδος απαιτεί κάθε σταθμός να διαλέξει έναν τυχαίο αριθμό n μεταξύ του 0 και ενός δοσμένου αριθμού, και να περιμένει n αριθμό χρονικών σχισμών πριν επιχειρήσει την πρόσβαση στο μέσο, ελέγχοντας πάντα αν ένας διαφορετικός σταθμός απέκτησε πριν την πρόσβαση στο μέσο.

Η χρονική σχισμή ορίζεται με τέτοιο τρόπο που ο σταθμός να είναι πάντα σε θέση να αποφασίσει αν κάποιος άλλος σταθμός απέκτησε το μέσο στην αρχή της προηγούμενης σχισμής. Αυτό μειώνει την πιθανότητα σύγκρουσης στο μισό.

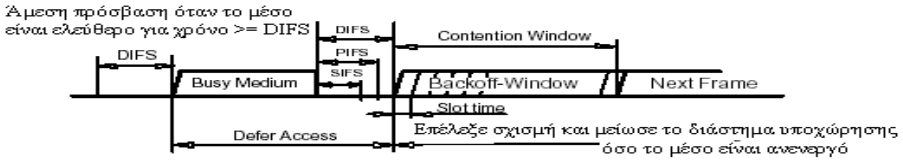
Εκθετική υποχώρηση σημαίνει ότι κάθε φορά που ο σταθμός επιλέγει μια σχισμή και συμβαίνει να συγκρούεται, θα αυξήσει τον μέγιστο αριθμό για την τυχαία επιλογή εκθετικά.

Το 802.11 στάνταρ ορίζει έναν αλγόριθμο εκθετικής υποχώρησης που πρέπει να εκτελεστεί στις εξής ακόλουθες περιπτώσεις:

- αν ο σταθμός «ακούσει» το μέσο πριν την πρώτη μετάδοση πακέτου και το μέσο είναι απασχολημένο
- μετά από κάθε αναμετάδοση
- μετά από μια επιτυχημένη μετάδοση

Η μόνη περίπτωση που ο μηχανισμός δεν χρησιμοποιείται είναι όταν ο σταθμός αποφασίσει να μεταδώσει ένα νέο πακέτο και το μέσο είναι ελεύθερο για περισσότερο από DIFS διάστημα.

Η σχηματική αναπαράσταση του μηχανισμού πρόσβασης φαίνεται ακολούθως:



Σχήμα 3.2.6 Σχηματική αναπαράσταση του μηχανισμού πρόσβασης

3.3 Τύποι Πλαισίων του Υποεπιπέδου του MAC

Στο υποεπίπεδο MAC του 802.11 ορίζονται οι παρακάτω τρεις τύποι πλαισίων :

- **Πλαίσια δεδομένων (Data) :** Χρησιμοποιούνται για την μετάδοση δεδομένων.
- **Πλαίσια ελέγχου (Control) :** Για τον έλεγχο του μέσου μετάδοσης.
- **Πλαίσια διαχείρισης (Management) :** Ανταλλαγή πληροφορίας διαχείρισης.

3.3.1 Πλαίσια Δεδομένων (Data)

Τα πλαίσια αυτά χρησιμεύουν για τη μεταφορά δεδομένων από ανώτερα επίπεδα του πρωτοκόλλου, αλλά επιτελούν κι άλλες λειτουργίες.

Παρακάτω παρατίθενται τα διάφορα πλαίσια αυτού του τύπου.

- ***Data*** : Το απλούστερο πλαίσιο του τύπου αυτού, μπορεί να χρησιμοποιηθεί και σε contention - free period και σε contention period. Το μόνο που κάνει είναι να μεταφέρει δεδομένα.
- ***Data + CF-Ack*** : Το πλαίσιο αυτό χρησιμοποιείται μόνο κατά την contention - free period. Μεταφέρει δεδομένα και ταυτόχρονα επιβεβαιώνει κάποιο πλαίσιο που έχει ήδη ληφθεί.
- ***Data + CF-Poll*** : Το πλαίσιο αυτό αποστέλλεται από το AP που τρέχει τον PCF αλγόριθμο κατά την contention - free period. Μεταφέρει δεδομένα προς έναν σταθμό και ζητάει από αυτόν να στείλει ότι πλαίσια έχει αποθηκεύσει προσωρινά.
- ***Data + CF-Ack + CF-Poll*** : Συνδυάζει τις λειτουργίες των δύο προηγούμενων πλαισίων, αποστέλλεται μόνο από το AP.

- *Null* : Το πλαίσιο αυτό δεν μεταφέρει δεδομένα. Αποστέλλεται από έναν σταθμό στο AP έχοντας το bit Power Management του πεδίου Frame Control ίσο με «1» για να δηλώσει στο AP ότι μπαίνει σε λειτουργία εξοικονόμησης ενέργειας. Το AP όταν λάβει τέτοιο πλαίσιο πρέπει να αποθηκεύει μελλοντικά πλαίσια προς το σταθμό αυτόν.
- *CF-Ack* : Ίδια λειτουργία με το Data + CF-Ack χωρίς να μεταφέρει δεδομένα.
- *CF-Poll* : Ίδια λειτουργία με το Data + CF-Poll χωρίς να μεταφέρει δεδομένα.
- *CF-Ack + CF-Poll* : Ίδια λειτουργία με το Data + CF-Ack +CF-Poll χωρίς να μεταφέρει δεδομένα.

3.3.2 Πλαίσια Ελέγχου (Control)

Τα πλαίσια του τύπου Control λειτουργούν βοηθητικά για την αξιόπιστη μεταφορά των Data πλαισίων και την πρόσβαση στο μέσο των σταθμών.

Υπάρχουν τα παρακάτω έξι διαφορετικά πλαίσια αυτού του τύπου :

- *Power Save Poll (PS-Poll)* : Το πλαίσιο αυτό αποστέλλεται από οποιοδήποτε σταθμό στο AP, όταν αυτός επανέλθει στην κανονική του λειτουργία μετά από περίοδο λειτουργίας εξοικονόμησης ενέργειας, για να ζητήσει να του αποσταλούν όσα πλαίσια προορίζονται για αυτόν και είναι προσωρινά αποθηκευμένα στο AP.
- *RTS* : Το πλαίσιο αυτό, όπως έχει ήδη αναφερθεί, είναι μέρος του μηχανισμού RTS/CTS για την απρόσκοπτη μεταφορά ενός ή περισσοτέρων πλαισίων. Ειδοποιεί τον σταθμό προορισμού αλλά και όσους άλλους το λάβουν ότι ζητάει άδεια να στείλει δεδομένα.
- *CTS* : Το έτερο πλαίσιο του μηχανισμού RTS/CTS. Δίνει την άδεια σε κάποιον σταθμό να στείλει δεδομένα, ενώ ειδοποιεί τους υπόλοιπους ότι επίκειται ανταλλαγή πλαισίων.

- *ACK* : Το πλαίσιο αυτό επιβεβαιώνει τη λήψη του αμέσως προηγούμενου πλαισίου. Η σωστή λήψη του είναι απαραίτητη για να θεωρήσει ο αποστολέας ότι το πλαίσιο που έστειλε παραδόθηκε κανονικά.
- *Contention Free End (CF-End)* : Το πλαίσιο αυτό αποστέλλεται από το AP που ελέγχει την πρόσβαση κατά μία contention - free period για να δηλώσει τη λήξη της.
- *CF-End + CF-Ack* : Σύνθετο πλαίσιο που δηλώνει τη λήξη της contention free period και επιβεβαιώνει τη λήψη του τελευταίου πλαισίου που είχε σταλεί.

3.3.3 Πλαίσια Διαχείρισης(Management)

Τα ασύρματα δίκτυα έχουν αυξημένες ανάγκες διαχείρισης σε σχέση με τα ενσύρματα. Στην συνέχεια θα παρουσιαστούν οι διάφοροι τύποι πλαισίων που επιτελούν τις απαραίτητες λειτουργίες. Η δομή των πλαισίων Management διαφέρει αρκετά από αυτή των πλαισίων Data, αφού χρησιμοποιούν διάφορα πεδία για διαφορετικό λόγο. Τέτοιο παράδειγμα είναι το πεδίο Data που χρησιμοποιείται από κάποια Management πλαίσια για να μεταφέρει επιπλέον πληροφορίες.

Παρακάτω παρατίθενται τα διάφορα πλαίσια αυτού του τύπου.

- *Association Request* : Το πλαίσιο αυτό στέλνεται από έναν σταθμό στο AP για να δηλώσει την πρόθεσή του να ξεκινήσει τη διαδικασία του association με το BSS αυτό. Το πλαίσιο περιέχει πληροφορίες όπως το SSID (Service Set ID), το είδος του δικτύου, τη χρήση ή όχι του αλγορίθμου WEP, τους υποστηριζόμενους από το σταθμό ρυθμούς μετάδοσης και άλλα.
- *Association Response* : Στέλνεται από το AP σε σταθμό ως απάντηση σε πλαίσιο Association Request. Δηλώνει αν ο σταθμός έγινε αποδεκτή η αίτηση του σταθμού και σε περίπτωση θετικής απάντησης περιέχει το AID.

- *Reassociation Request* : Το ίδιο με το Association Request, αποστέλλεται όταν ένας σταθμός κινείται μεταξύ διαφορετικών BSS εντός του ιδίου ESS ή αν χάσει προσωρινά τη σύνδεση στο BSS που βρίσκεται.
- *Reassociation Response* : Απάντηση στο πλαίσιο Reassociation Request.
- *Disassociation* : Το πλαίσιο αυτό αποστέλλεται από έναν σταθμό στο AP του BSS για να τερματίσει τη σχέση association με αυτό. Περιέχει έναν κωδικό που δηλώνει την αιτία του τερματισμού (Reason Code).
- *Probe Request* : Πλαίσιο που αποστέλλεται από έναν σταθμό που ψάχνει ασύρματα δίκτυα στην περιοχή του. Περιέχει το SSID του δικτύου που ψάχνει ο σταθμός και τους υποστηριζόμενους από αυτόν ρυθμούς μετάδοσης.
- *Probe Response* : Απάντηση σε πλαίσιο Probe Request. Περιέχει διάφορες παραμέτρους του δικτύου ώστε να μπορέσει ο σταθμός που το λαμβάνει να συνεχίσει τη διαδικασία ένταξης στο δίκτυο.
- *Authentication* : Πλαίσια που ανταλλάσσονται μεταξύ AP και ενδιαφερόμενου σταθμού για τη διαδικασία του authentication που προηγείται του association.
- *Deauthentication* : Αντίστοιχο του Disassociation, περιέχει και αυτό πεδίο Reason Code.
- *Beacon* : Το πλαίσιο αυτό εκπέμπεται περιοδικά από το AP και έχουν ήδη αναφερθεί κάποιες λειτουργίες που σχετίζονται με αυτό (δήλωση έναρξης contention free period). Κύριος ρόλος τους είναι η γνωστοποίηση της ύπαρξης του δικτύου στην περιοχή κάλυψής του. Περιέχει διάφορες παραμέτρους λειτουργίας του δικτύου.
- *IBSS Announcement Traffic Indication Message* : Αυτό το πλαίσιο συναντάται αποκλειστικά σε IBSS δίκτυα. Αποστέλλεται από οποιονδήποτε σταθμό έχει αποθηκευμένα πλαίσια που προορίζονται για άλλον σταθμό, ο οποίος λειτουργούσε σε κατάσταση εξοικονόμησης ενέργειας για να τον ειδοποιήσει. Ο παραλήπτης πρέπει να εκκινήσει τη διαδικασία παραλαβής των αποθηκευμένων πλαισίων.

3.4 Εξοικονόμηση ενέργειας

Έχουμε αναφέρει σε παραπάνω κεφάλαια ότι η ευελιξία και η ελευθερία κινητικότητας είναι από τα βασικότερα πλεονεκτήματα των ασύρματων δικτύων για τους χρήστες των κινητών συσκευών. Αυτό φυσικά επιτυγχάνεται με την έλλειψη καλωδίων και τους περιορισμούς που θα έθεταν αν υπηρχαν, όπως στα ενσύρματα δίκτυα. Έτσι η τροφοδοσία των συσκευών λογικά γίνετε με μπαταρία που θα έχει συγκεκριμένη διάρκεια ζωης. Όσο το δυνατόν μικρότερη κατανάλωση ισχύος γίνεται από τους σταθμούς τόσο περισσότερο θα επιμηκύνεται η διάρκεια ζωής της μπαταρίας και θα αυξάνεται η αυτονομία τους. Επίσης είναι γνωστό πως η μεγαλύτερη κατανάλωση ισχύος σε ασύρματα συστήματα προέρχεται από τους ενισχυτές που ενισχύουν το σήμα αμέσως πριν την εκπομπή ή μετά τη λήψη του.

Έχοντας σκεφτεί πολύ σοβαρά τα παραπάνω θέματα αυτοί που δημιούργησαν το 802.11, φρόντισαν να υπάρχει δυνατότητα ένας σταθμός να σταματήσει τη λειτουργία του πομποδέκτη του για κάποια περίοδο, που ονομάζεται sleeping period. Παράλληλα οι σταθμοί, συμπεριλαμβανομένων και των APs(Access Points), έχουν τη δυνατότητα της προσωρινής αποθήκευσης (buffering) των πλαισίων που προορίζονται για σταθμούς που έχουν εισέλθει σε sleeping period. Με αυτόν τον τρόπο οι σταθμοί μπορούν να «ξυπνούν» περιοδικά και να δέχονται τα πλαίσια που έχει αποθηκεύσει το AP ή να στέλνουν οι ίδιοι πλαίσια στο AP.

Ένας σταθμός που μόλις έχει ξυπνήσει μπορεί να ζητήσει από το AP να του στείλει όσα πλαίσια έχει αποθηκευμένα για αυτόν με την αποστολή ενός PS-Poll πλαισίου. Το AP όταν λάβει ένα τέτοιο πλαίσιο μπορεί είτε να αρχίσει να στέλνει αμέσως πλαίσια στον σταθμό, αν φυσικά υπάρχουν, ή να του στείλει άμεσα ένα πλαίσιο ACK και να στείλει αργότερα τα αποθηκευμένα πλαίσια. Ο σταθμός στη δεύτερη περίπτωση πρέπει να περιμένει μέχρι να του αποσταλούν τα πλαίσια χωρίς φυσικά να ξαναμπεί σε sleeping period.

Οι σταθμοί έχουν επίσης την υποχρέωση να ξυπνούν κατά περιόδους και να λαμβάνουν Beacon πλαίσια από το AP. Αυτά, πέραν των άλλων λειτουργιών που επιτελούν, έχουν ένα πεδίο που ονομάζεται TIM (Traffic Indication Map). Εκεί σημειώνεται κάθε σταθμός για τον οποίο το AP έχει αποθηκευμένα πλαίσια, τα οποία ο σταθμός μπορεί στη συνέχεια να τα ζητήσει με ένα PS-Poll πλαίσιο.

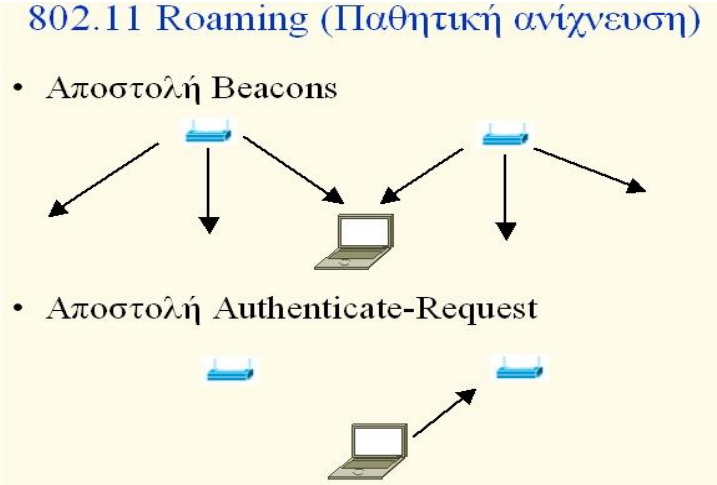
3.5 Διαδικασία Πρόσβασης στο Δίκτυο

Η διαδικασία πρόσβασης ενός σταθμού σε ένα δίκτυο απαιτεί την ολοκλήρωση κάποιον βημάτων. Κάθε σταθμός είναι εξοπλισμένος με μια NIC (network interface card) η οποία ψάχνει για διαθέσιμα σημεία πρόσβασης (APs-Access Points). Η διαδικασία αυτή καλείται scanning και είναι το πρώτο από τα βήματα που θα αναλύσουμε και παρακάτω.

3.5.1 Scanning

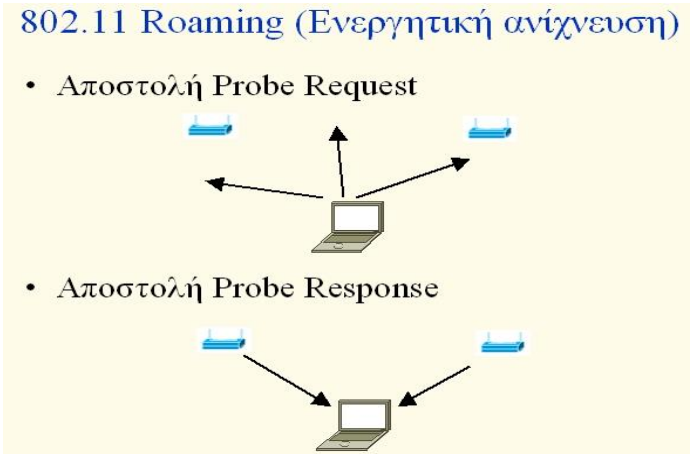
Κατά την διαδικασία του scanning ο σταθμός πρέπει πρώτα να εντοπίσει το δίκτυο στο οποίο θέλει να αποκτήσει πρόσβαση. Έτσι ξεκινάει να εντοπίσει όλα τα υπάρχοντα δίκτυα στην περιοχή που βρίσκεται. Η συγκεκριμένη διαδικασία έχει δύο παραλλαγές, το ενεργό (active scanning) και το παθητικό(passive scanning).

Κατά το passive scanning ο σταθμός δεν εκπέμπει τίποτα, εξοικονομώντας έτσι ενέργεια. Παρακολουθεί τα διαθέσιμα κανάλια ψάχνοντας για πλαίσια Beacon που δηλώνουν την ύπαρξη κάποιου δικτύου. Τα πλαίσια Beacon περιέχουν όλες τις απαραίτητες πληροφορίες για το BSS απ' όπου εκπέμπονται ώστε ο σταθμός να μπορεί να προχωρήσει στο επόμενο βήμα, δηλαδή στη διαδικασία του joining. Η διαδικασία φαίνεται στο παρακάτω σχήμα.



Σχήμα 3.5.1.1 : Παθητική ανίχνευση

Η δεύτερη παραλλαγή είναι το active scanning,μία παραλλαγή κατά την οποία ο σταθμός εκπέμπει περιοδικά σε όλα τα διαθέσιμα κανάλια πλαίσια Probe Request που περιέχουν και το SSID (ή network name) του δικτύου που ψάχνει. Για να εκπέμψει αυτό το πλαίσιο ο σταθμός πρέπει να αποκτήσει κανονικά πρόσβαση στο μέσο χρησιμοποιώντας τον αλγόριθμο DCF. Ο σταθμός έχει προβλεφθεί ώστε να καταλαβαίνει ο σταθμός πότε ένα κανάλι είναι ανενεργό. Σε κάθε BSS ένας σταθμός είναι υπεύθυνος για να απαντάει σε πλαίσια Probe Request. Σε infrastructure δίκτυα υπεύθυνο είναι το AP, ενώ σε IBSS υπεύθυνος είναι ο σταθμός που εξέπεμψε το τελευταίο πλαίσιο Beacon. Σε κάθε περίπτωση ο σταθμός που έστειλε το Probe Request θα λάβει ένα ή περισσότερα πλαίσια Probe Response αν υπάρχουν ασύρματα δίκτυα στην περιοχή του. Η διαδικασία αυτή φαίνεται στο παρακάτω σχήμα.



Σχήμα 3.5.1.2 : Ενεργητική Ανίχνευση

Οποιονδήποτε από τις δύο παραπάνω παραλλαγές και να ακολουθηθεί από τον σταθμό στο τέλος της διαδικασίας θα έχει αποκτήσει τις βασικές πληροφορίες που χρειάζεται για τα διαθέσιμα δίκτυα που υπάρχουν.

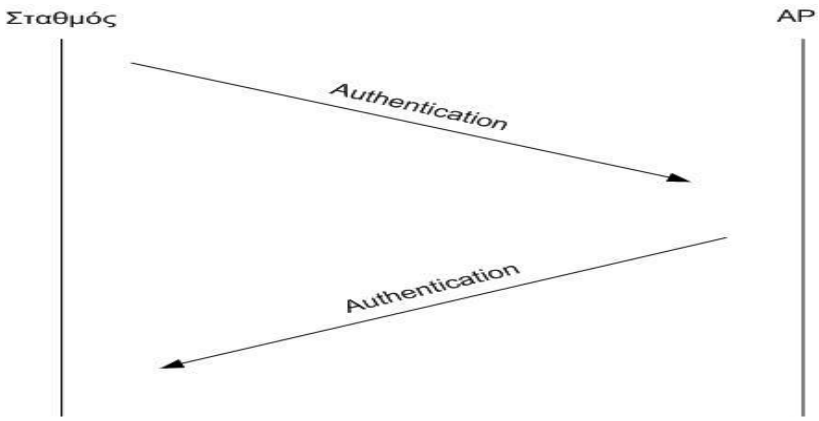
3.5.2 Joining

Η διαδικασία αυτή ξεκινάει με το που εντοπιστεί το δίκτυο, χωρίς όμως ο κινητός σταθμός να αποκτήσει πρόσβαση στο δίκτυο, κάτι που ισχύει σε όλες τις περιπτώσεις. Η χρησιμότητα αυτής της διαδικασίας είναι ότι είναι απαραίτητο βήμα για τη διαδικασία του association.

Ο σταθμός, έχοντας τις απαραίτητες πληροφορίες από το scanning, εξετάζει τις παραμέτρους κάθε BSS και αποφασίζει με ποιο από αυτά θα προχωρήσει τη διαδικασία του association. Για να επιλέξει ο σταθμός ένα BSS πρέπει φυσικά να μπορεί να λειτουργήσει με τις συγκεκριμένες παραμέτρους του BSS. Επιπλέον, κριτήρια όπως το επίπεδο ισχύος ή η ένταση του σήματος από κάθε BSS παίζουν ρόλο. Παρόλα αυτά δεν υπάρχει συγκεκριμένη διαδικασία επιλογής ενός δικτύου έναντι κάποιου άλλου. Η επιλογή γίνεται εσωτερικά στο σταθμό και εξαρτάται από τον εκάστοτε κατασκευαστή.

3.5.3 Authentication

Αφού ο σταθμός επιλέξει σε ποιο BSS θέλει να προσχωρήσει, κάτι που γίνετε μέσω της διαδικασίας του joining, ακολουθεί η συγκεκριμένη διαδικασία. Εδώ είναι αρκετά σημαντικό να διατηρηθεί η ασφάλεια στα ασύρματα δίκτυα, εφόσον δεν υπάρχουν φυσικοί περιορισμοί για κάποιον που θέλει να αποκτήσει πρόσβαση σε ένα δίκτυο. Έτσι για την πιστοποίηση πρέπει να ανταλλαχθούν οι κατάλληλες πληροφορίες και κλειδιά, όπως φαίνετε στο παρακάτω σχήμα.



Σχήμα 3.5.3 : Διαδικασία πιστοποίησης

Η διαδικασία αυτή έχει μεγαλύτερη σημασία σε infrastructure δίκτυα εφόσον το authentication είναι μονόδρομο και όχι αμφίδρομο. Αυτό σημαίνει ότι κάθε σταθμός που θέλει να αποκτήσει πρόσβαση στο δίκτυο πρέπει να πιστοποιήσει τον εαυτό του σε κάποιο AP, αλλά το AP δεν έχει καμιά υποχρέωση πιστοποίησης. Αυτό εξυπηρετεί τους διαχειριστές του δικτύου που θέλουν να πιστοποιούνται όλοι οι χρήστες που αποκτούν πρόσβαση στο δίκτυο αλλά δημιουργεί πιθανά προβλήματα ασφάλειας. Για παράδειγμα ένα AP μπορεί να στέλνει πλαίσια Beacon ενός δικτύου του οποίου δεν είναι μέρος για να υποκλέψει στοιχεία του authentication από το δίκτυο αυτό.

Υπάρχουν τα παρακάτω δύο είδη authentication :

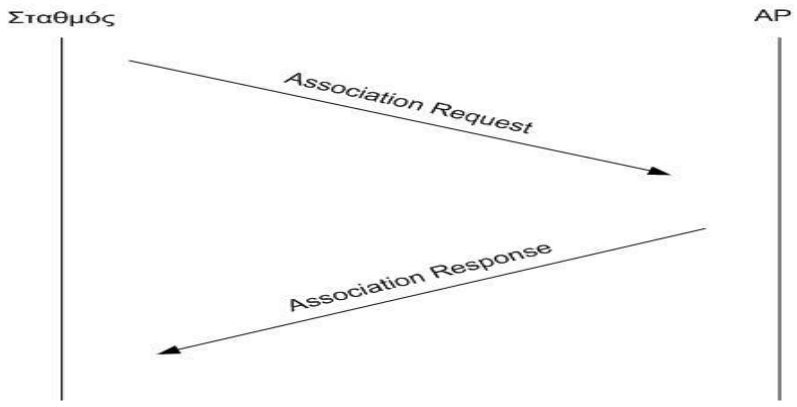
- **Open – System authentication :** Αυτό το είδος authentication είναι το μόνο που απαιτείται από το πρότυπο 802.11. Στην ουσία δεν πρόκειται για πραγματικό authentication, εφόσον το AP δέχεται την ταυτότητα του σταθμού χωρίς οποιαδήποτε διαδικασία πιστοποίησής της.
- **Shared – Key authentication :** Αυτός ο τύπος πιστοποίησης ταυτότητας χρησιμοποιεί τον αλγόριθμο κρυπτογράφησης WEP (Wired Equivalent Privacy), ο οποίος στοχεύει στην ασφάλεια κατά την μεταφορά δεδομένων μέχρι το AP (η αναλυτική περιγραφή του ξεφεύγει από το παρών σύγγραμμα). Υπενθυμίζεται ότι το πρότυπο 802.11 δεν θεωρεί υποχρεωτική την υποστήριξη του WEP, άρα αυτός ο τύπος πιστοποίησης μπορεί να μην είναι πάντα διαθέσιμος. Για να λειτουργήσει απαιτεί την ύπαρξη ενός μοιραζόμενου κλειδιού (shared key) από τους σταθμούς.

Η διαδικασία του authentication πρέπει οπωσδήποτε να ολοκληρωθεί με επιτυχία για να ακολουθήσει το association, αλλά δεν είναι υποχρεωτικό να ακολουθήσει το association αμέσως μετά. Οι σταθμοί μπορούν να ολοκληρώσουν το authentication με διάφορα AP έτσι ώστε όταν απαιτηθεί association με οποιοδήποτε από αυτά να γίνει χωρίς άλλη καθυστέρηση. Αυτό μπορεί να χρησιμεύσει στην περίπτωση διαπομπής, αν το AP έχει ήδη ολοκληρώσει το authentication με το καινούργιο AP πριν την διαπομπή. Αυτού του είδους το authentication ονομάζεται και preauthentication.

3.5.4 Assosiation

Η διαδικασία αυτή είναι το τελικό βήμα για να αποκτήσει ο σταθμός πρόσβαση στο δίκτυο. Το association απαιτεί την ανταλλαγή δύο πλαισίων μεταξύ σταθμού και AP.

Το πρώτο πλαίσιο το στέλνει ο σταθμός και είναι τύπου Association Request. Σε περίπτωση που δεν έχει προηγηθεί authentication το AP απαντά με ένα πλαίσιο Deauthentication. Σε περίπτωση που το authentication έχει γίνει κανονικά το AP αποφασίζει αν θα ολοκληρώσει ή όχι τη διαδικασία. Δεν υπάρχει ούτε εδώ κάποιος προβλεπόμενος από το 802.11 τρόπος απόφασης αλλά είναι θέμα της συγκεκριμένης υλοποίησης. Αν τελικά η αίτηση γίνει δεκτή, το AP απαντά με ένα πλαίσιο Association Response. Επίσης, γνωστοποιεί την ύπαρξη του σταθμού στο δικό του BSS στο σύστημα διανομής (Distribution System – DS) ώστε να δρομολογούνται σωστά πλαίσια που προορίζονται για τον σταθμό αυτόν. Η όλη διαδικασία φαίνεται στο παρακάτω σχήμα.



Σχήμα 3.5.4 : Διαδικασία Συσχέτισης

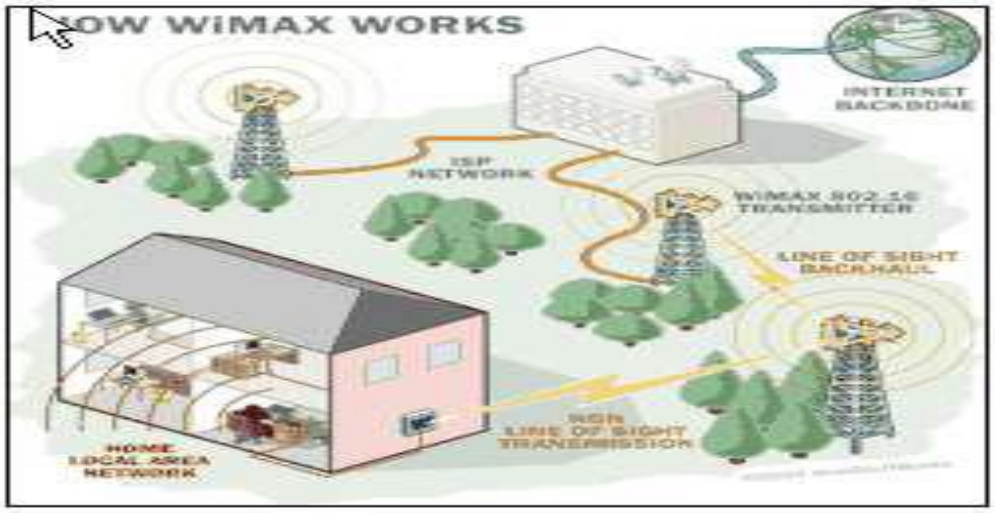
4 Νεα Τεχνολογία 802.16/ WiMax

4.1 Χαρακτηριστικά

Το 2003 η IEEE υιοθέτησε το πρότυπο 802.16, ευρέως γνωστό και σαν WiMax, ώστε να ικανοποιεί όλες τις απαιτήσεις για ασύρματη πρόσβαση ευρείας ζώνης με σταθερούς ρυθμούς. Όπως συμβαίνει με όλα τα πρότυπα της σειράς 802 για ασύρματα τοπικά δίκτυα, έτσι και το συγκεκριμένο πρότυπο καθορίζει μια οικογένεια προτύπων με επιλογές για συγκεκριμένες ρυθμίσεις.

Το WiMax είναι ένα αρκτικόλεξο που αντιπροσωπεύει το Worldwide Interoperability for Microwave Access, ένα σημάδι πιστοποίησης για τα προϊόντα που περνούν τις δοκιμές συμμόρφωσης και διαλειτουργικότητας για τα IEE 802.16 πρότυπα. Τα προϊόντα αυτά είναι σε θέση να δημιουργούν ασύρματες συνδέσεις μεταξύ τους για να επιτρέψουν τη μεταφορά των στοιχείων πακέτων διαδικτύου. Είναι παρόμοιο με το WiFi στην έννοια, αλλά έχει ορισμένες βελτιώσεις που στοχεύουν στη βελτίωση της απόδοσης και μπορεί να επιτρέψουν τη χρήση σε πολύ μεγαλύτερες αποστάσεις.

Το πώς λειτουργεί το WiMax μπορούμε να το αντιληφθούμε και από την παρακάτω εικόνα:



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

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

οποία είναι διαθέσιμα στην αγορά ακολουθούν στην μεγαλύτερή τους πλειοψηφία το υποπρότυπο αυτό.

Η ποιότητα υπηρεσίας πάνω από τέτοια δίκτυα γίνεται ένας πολύ καθοριστικός παράγοντας για την ποιότητα της επικοινωνίας, ειδικά όσο αυξάνεται η πολυπλοκότητα των εφαρμογών που διαδίδονται πάνω από ένα ασύρματο δίκτυο. Για παράδειγμα, η μετάδοση video σε πραγματικό χρόνο απαιτεί από το δίκτυο συνθήκες πολύ χαμηλής καθυστέρησης μετάδοσης. Για αυτό το λόγο, προκειμένου να ικανοποιηθεί η ανάγκη για ποιότητα υπηρεσίας ορίστηκε το υποπρότυπο **IEEE 802.16 d**.

Η ένωση των υπό-προτύπων IEEE 802.11 a, c, d όρισε το πρότυπο **IEEE 802.16-2004** το οποίο περιγράφει τη συνολική λειτουργικότητα των επιμέρους υπό-προτύπων που προαναφέρθηκαν για συχνότητες λειτουργίας 2-66 GHz. Υποστηρίζει ταχύτητες μετάδοσης ως και 72 Mbps στον αέρα ενώ η πραγματική ταχύτητα στο Ethernet υπολογίζεται στα 50 Mbps. Οι αποστάσεις που μπορεί να καλυφθούν ξεπερνούν τα 50 Km σε συνθήκες οπτικής επαφής. Μια σημαντική διαφορά του προτύπου IEEE 802.16 σε σχέση με το IEEE 802.11 είναι ότι το πρώτο μπορεί να χρησιμοποιηθεί και σε συνθήκες μη οπτικής επαφής φυσικά με ρυθμούς μετάδοσης πολύ χαμηλότερους των 50 Mbps.

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

Το πρότυπο IEEE 802.16-2004 ορίζει την επικοινωνία χρηστών οι οποίοι βρίσκονται μέσα σε ένα κελί το οποίο καλύπτεται από ένα base station . Όταν κάποιος χρήστης κινηθεί σε περιοχή που βρίσκεται εκτός περιοχής κάλυψης του base station η σύνδεση χάνεται. Το υποπρότυπο **IEEE 802.16 e** εισάγει και περιγράφει την έννοια της κινητικότητας των χρηστών από ένα base station σε άλλο. Στο υποπρότυπο αυτό ορίζεται ότι ένας κινητός χρήστης

μπορεί να συνεχίσει να εξυπηρετείται από το δίκτυο ακόμα και αν κινείται με ταχύτητες οι οποίες προσεγγίζουν τα 120 Km/h .

4.2 Ταχύτητες Μετάδοσης, Ποιότητα Υπηρεσίας και Ασφάλεια

Οι ταχύτητες μετάδοσης του προτύπου δεν είναι πάντα ίδιες, αλλά εξαρτώνται από την ψηφιακή διαμόρφωση που χρησιμοποιείται κάθε φορά ανάλογα με την περίπτωση. Οι πιο συνηθισμένες διαμορφώσεις είναι η 64 QAM η οποία μπορεί να εξασφαλίσει και τη μεγαλύτερη ταχύτητα μετάδοσης, η 16 QAM και η QPSK η οποία μπορεί να εξασφαλίσει μεγάλη κάλυψη του συστήματος.

Ένα σημαντικό στοιχείο του WiMax είναι ότι παρέχει ποιότητα υπηρεσίας υψηλού επιπέδου. Η σχεδίαση του MAC επιπέδου του έχει γίνει με τέτοιο τρόπο, ώστε να παρέχει στους χρήστες, όταν αυτοί το επιθυμούν, κίνηση Best Effort σε χρήστες που καλύπτονται από το ίδιο base station, κάτι που στο 802.11 δεν ίσχυε, αλλά ταυτόχρονα παρέχει και εγγυημένο ρυθμό μετάδοσης. Δηλαδή, αν υποθέσουμε ότι δύο χρήστες καλύπτονται από το ίδιο Base Station, είναι δυνατό ο ένας χρήστης να έχει εγγυημένη ποιότητα υπηρεσίας και ο δεύτερος χρήστης να δέχεται και να στέλνει απλή IP κίνηση best effort κάτι που με το πρότυπο 802.11 δεν ήταν δυνατό. Δηλαδή χρήστες που βρισκόταν στην κάλυψη ενός Access Point είχαν την ίδια ποιότητα υπηρεσίας.

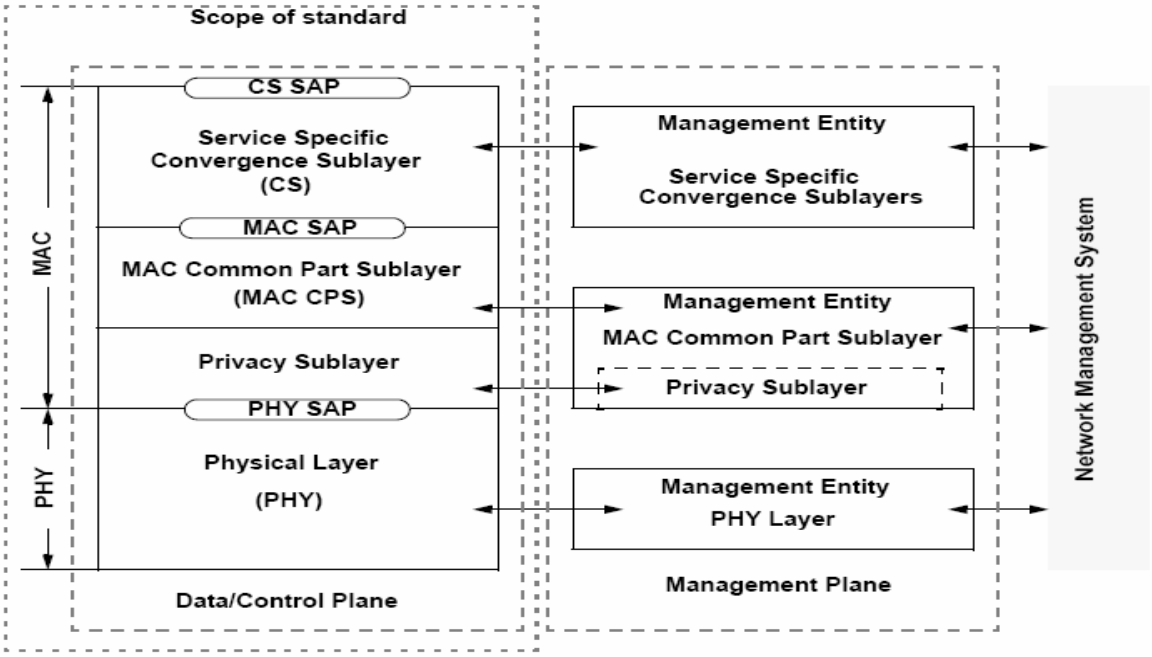
Ο αλγόριθμος κρυπτογράφησης DES (Data Encryption Standard, Πρότυπο Κωδικοποίησης Δεδομένων) και συγκεκριμένα μια παραλλαγή του αλγορίθμου ο Triple DES έχει αναλάβει την ασφαλή μετάδοση των δεδομένων στο WiMAX. Ο αλγόριθμος αυτός αναπτύχτηκε το 1970 από το Αμερικανικό Εθνικό Γραφείο Προτύπων. Δημιουργήθηκε με στόχο την ανάπτυξη ενός αλγόριθμου κρυπτογράφησης που θα μπορούσε να χρησιμοποιηθεί και να βελτιωθεί από διάφορες εταιρίες και οργανισμούς.Το DES ανήκει στην οικογένεια των συμμετρικών αλγόριθμων και κάνει χρήση κλειδιών με μήκος 56 bit. Ο "κλασικός" αλγόριθμος DES είναι πλέον ξεπερασμένος, αφού με τη χρήση ενός σύγχρονου υπολογιστή μπορεί να παραβιαστεί σχετικά εύκολα.

Στο μεταξύ, εφαρμόζοντας διάφορες τεχνικές επάνω στο DES, μπορούμε να αυξήσουμε σημαντικά την ασφάλειά του. Με τη μέθοδο Triple - DES, για παράδειγμα, το μήνυμα κωδικοποιείται τρεις φορές, με τρία διαφορετικά κλειδιά.

4.3 Αναλυτική Παρουσίαση του προτύπου IEEE 802.16

4.3.1 Το Φυσικό Επίπεδο

Το φυσικό επίπεδο του WiMax είναι υπεύθυνο για την μετάδοση της πληροφορίας, η οποία επιτυγχάνεται με τη χρήση της παραδοσιακής μετάδοσης ραδιοκυμάτων στενής ζώνης. Όπως φαίνεται και στο σχήμα παρακάτω, όπου απεικονίζεται η στοίβα του πρωτοκόλλου, οι υπηρεσίες του φυσικού επιπέδου παρέχονται στο MAC υποεπίπεδο μέσω του PHY SAP.



Σχήμα 4.3.1.1 Στοίβα πρωτοκόλλων του 802.16

Στο φυσικό επίπεδο η διαμόρφωση η οποία έχει υιοθετηθεί από το πρότυπο είναι το OFDM. Ένας από τους κυριότερους λόγους υιοθέτησης του OFDM ως του μοντέλο διαμόρφωσης για ένα ασύρματο τηλεπικοινωνιακό σύστημα είναι η μεγάλη αντοχή που επιδεικνύει σε περιβάλλοντα εξασθένησης σήματος και παρεμβολών. Σε συστήματα μονής φέρουσας ένας επίδοξος παρεμβολέας μπορεί να προκαλέσει ακόμα και την κατάρρευση ενός link, σε αντίθεση με τα συστήματα πολλών φερουσών, όπου ένα μικρό μόνο ποσοστό των φερουσών θα επηρεαστεί. Μία από τις προτεινόμενες λύσεις για βέλτιστη αντιμετώπιση του προβλήματος είναι η χρήση Κωδικοποίησης Διόρθωσης Σφάλματος (Error Correction Coding).

Σε ένα κλασικό σύστημα παράλληλης μετάδοσης δεδομένων η συνολικά διαθέσιμη μπάντα συχνοτήτων διαιρείται σε N μη επικαλυπρόμενα υποκάναλα συχνοτήτων. Κάθε υποκανάλι διαμορφώνεται και από διαφορετικό σύμβολο και ακολούθως τα N υποκανάλια πολυπλέκονται στο πεδίο των συχνοτήτων. Η ιδέα που εισήγαγε το OFDM ήταν πρωτοποριακή μιας και οδηγούσε στην εξοικονόμηση φάσματος. Πιο συγκεκριμένα, έκανε λόγο για χρήση επικαλυπτόμενων υποκαναλιών, που χαρακτηρίζονται από την κοινή ιδιότητα της μεταξύ τους ορθογωνιότητας γεγονός που οδηγεί στην αποφυγή ισοστάθμισης, την αντιμετώπιση θορύβου και εξασθένησης σήματος λόγω πολυδιόδευσης (multipath fading) καθώς και την πλήρη αξιοποίηση του διαθέσιμου φάσματος. Αυτό έχει ως αποτέλεσμα η διαφορά μεταξύ των συμβατών τεχνικών με μη επικαλυπτόμενα υποκανάλια και του OFDM να γέρνει υπέρ της δεύτερης, αφού καταφέρνει να εξοικονομήσει μέχρι και 50% από το εύρος φάσματος που θα χρησιμοποιούσε. Είναι όμως επιτακτική ανάγκη να εξασφαλίσουμε την όσο δυνατόν μικρότερη παρεμβολή μεταξύ των υποφερουσών.

Τα σπουδαιότερα πλεονεκτήματα της χρήσης του OFDM είναι συνοπτικά τα ακόλουθα :

- Το OFDM αντιμετωπίζει αποτελεσματικά το φαινόμενο της πολυδιόδευσης(multipath), ενώ η πολυπλοκότητα ενός OFDM συστήματος είναι κατά πολύ μικρότερη από ένα σύστημα μονής φέρουσας (SC) με χρήση ισοσταθμιστή, ο οποίος αναλαμβάνει και το έργο.
- Σε συστήματα όπου οι δίαυλοι μετάδοσης μεταβάλλονται πολύ αργά σε

σχέση με τη συχνότητα μετάδοσης των δεδομένων είναι εφικτή η αύξηση της χωρητικότητας με την ανάλογη προσαρμογή της συχνότητας δεδομένων ανά υποφέρουσα σε σχέση πάντα και με το λόγο σήματος προς το θόρυβο για το συγκεκριμένο κανάλι (SNR).

- Το OFDM είναι εξαιρετικά ανθεκτικό στην παρεμβολή στενού φάσματος διότι τέτοιου είδους παρεμβολή επηρεάζει μόνο ένα μικρό ποσοστό των υποφερουσών.

Τα συστήματα WiMAX συνδυάζουν τεχνολογίες και αλγόριθμους ώστε να επιτυγχάνουν απόδοση BER των 10 -9 (BER of 10 -9) με διαθεσιμότητα ζεύξης 99,999%.

Η αύξηση της φασματικής απόδοσης είναι ένας σημαντικός παράγοντας που επηρεάζει απ' ευθείας το αποτέλεσμα. Για το λόγο αυτό, τα συστήματα WiMAX προσφέρουν διπλής κατευθύνσεως προσαρμοστική διαμόρφωση (Adaptive Modulation) που τα προσαρμόζει ανάμεσα σε έξι τύπους διαμόρφωσης (από QPSK σε 64 QAM) με σκοπό να προσαρμόζει τη ποιότητα διαβάθμισης της ζεύξης ενώ προσφέρουν το μέγιστο ρυθμό μετάδοσης για δεδομένα σενάρια ανάπτυξης.

Στο σχήμα 4.3.1.2 απεικονίζονται οι τύποι διαμόρφωσης και κωδικοποίησης σε σχέση με τον ρυθμό μετάδοσης. Τέλος στο σχήμα 4.3.1.3 παρουσιάζονται συνοπτικά ορισμένα από τα χαρακτηριστικά και τα πλεονεκτήματα του φυσικού επιπέδου του προτύπου IEEE 802.16a.

Modulation	FEC Coding Rate	Uncoded Burst Rate (Mbps)	End to End Ethernet Throughput (Mbps)
BPSK	½	6	5.7
BPSK	¾	9	8.6
QPSK	½	12	11.4
QPSK	¾	18	17
16QAM	½	24	22.4
16QAM	¾	36	33
64QAM	2/3	48	43.2
64QAM	¾	54	48.1

Σχήμα 4.3.1.2 Τύποι διαμόρφωσης

Χαρακτηριστικά	Πλεονεκτήματα
Χρήση OFDM με 256 φέρουσες	Επικοινωνία LOS και NLOS
Χρήση προσαρμοστικής διαμόρφωσης και κωδίκων διόρθωσης σφαλμάτων	Αποτελεσματικές ζεύξεις με μέγιστο αριθμό bits/sec σε κάθε χρήστη
Υποστήριξη TDD και FDD	Ικανοποιεί τις συνθήκες διαχείρισης φάσματος κάθε χώρας
Μεταβλητό εύρος ζώνης καναλιού (3.5 MHz , 5MHz , 10MHz)	Δυνατότητα λειτουργίας σε πολλές ζώνες συχνοτήτων ανάλογα με τον κανονισμό κάθε χώρας
Υποστήριξη έξυπνων κεραιών	Εξασφαλίζεται υψηλό κέρδος ισχύος

Σχήμα 4.3.1.3 Χαρακτηριστικά και Πλεονεκτήματα του φυσικού επιπέδου

4.3.2 Υποεπίπεδο MAC

Το MAC του WiMAX παρέχει «νοημοσύνη» για το Φυσικό Στρώμα και εξασφαλίζει ένα πλήθος χαρακτηριστικών. Το πρωτόκολλο MAC του WiMAX σχεδιάστηκε για point-to-multipoint εφαρμογές ασύρματης ευρυζωνικής πρόσβασης. Είναι υπεύθυνο για τη δημιουργία υψηλών ρυθμών μετάδοσης τόσο προς τον σταθμό βάσης όσο και από τον σταθμό βάσης. Οι αλγόριθμοι πρόσβασης και κατανομής εύρους ζώνης, που χρησιμοποιούνται εξυπηρετούν εκατοντάδες τερματικά ανά κανάλι με συνέπεια πολλαπλοί τελικοί χρήστες να μοιράζονται αυτά τα τερματικά. Ακόμα το MAC επίπεδο του 802.16a στηρίζεται σε ένα πρωτόκολλο κράτησης/αιτήματος για την πρόσβαση στο μέσο και υποστηρίζει ξεχωριστά επίπεδα υπηρεσιών. Το πρότυπα 802.16a χρησιμοποιεί ένα slotted πρωτόκολλο TDMA σχεδιασμένο από το BTS να δεσμεύει χωρητικότητα για τους συνδρομητές σε μια point-to-multipoint τοπολογία δικτύου.

Τα συστήματα WiMax είναι σε θέση να μεταδίδουν όχι μόνο στοιχεία υψηλής ταχύτητας, αλλά και ευαίσθητες σε καθυστέρηση υπηρεσίες όπως η φωνή και το βίντεο ή η πρόσβαση σε βάσεις δεδομένων. Αυτό το καταφέρνουν αρχίζοντας με TDMA προσέγγιση με ευφυή προγραμματισμό. Το πρότυπο προσφέρει QoS επιπλέον από το μόνο καθορισμό προτεραιοτήτων, μια τεχνική που είναι πολύ περιορισμένη στην αποτελεσματικότητα της με φορτία κίνησης και με αυξανόμενο αριθμό συνδρομητών. Το στρώμα του MAC στα

επικυρωμένα με WiMAX συστήματα έχει ως σκοπό επίσης να εξετάζει το εχθρικό φυσικό περιβάλλον στρώματος PHY layer όπου η παρεμβολή, η γρήγορη εξασθένιση και άλλα φαινόμενα παρουσιάζονται σε λειτουργία σε εξωτερικούς χώρους.

Το πρωτόκολλο χρησιμοποιεί τις ροές δεδομένων TDM στο DL (downlink) και TDMA στο UL (uplink). Εξασφαλίζοντας πρόσβαση στο κανάλι απαλλαγμένη από συγκρούσεις δεδομένων, η 16a MAC βελτιώνει τη συνολική ρυθμό-απόδοση του συστήματος και την αποδοτικότητα του εύρους ζώνης. Η 16a MAC εξασφαλίζει επίσης την οριοθετημένη καθυστέρηση στα δεδομένα . Η τεχνική πρόσβασης TDM/TDMA εξασφαλίζει επίσης ευκολότερη υποστήριξη για υπηρεσίες multicast και broadcast.

Στο σχήμα 4.3.2 παρουσιάζονται μερικά από τα χαρακτηριστικά και τα πλεονεκτήματα του MAC του 802.16a.

Χαρακτηριστικά	**Πλεονεκτήματα**
TDM/TDMA Scheduled Uplink/Downlink frames	Αποτελεσματική χρησιμοποίηση φάσματος
Κλιμάκωση από 1 εώς εκατοντάδες συνδρομητές	Επιτρέπει εφαρμογές οικονομικά αποδοτικές υποστηρίζοντας αρκετούς συνδρομητές
Συνδεσοστραφής Connection – oriented	Qos ανά σύνδεση Γρηγορότερη δρομολόγηση και προώθηση πακετών
QoS υποστηρίζει UGS,ertPS,rtPS,nrtPS,BE	Μικρή καθυστέρηση για υπηρεσίες ευαίσθητες σε αυτή(TDM Voice,VoIP) Βέλτιστη μεταφορά για κυκλοφορία VBR(video) Καθορισμός προτεραιότητας δεδομένων
Automatic Retransmission request(ARG)	Βελτιώνει την απόδοση απ’ άκρο σε άκρο κρύβοντας απ’ τα πρωτόκολλα ανωτέρου στρώματος τα προκληθέντα λάθη στο στρώμα RF

Υποστήριξη προσαρμοστικής διαμόρφωσης και κωδικων διόρθωσης σφαλμάτων	Επιτρέπει υψηλότερους ρυθμούς μετάδοσης δεδομένων ανάλογα με τις συνθήκες του καναλιού βελτιώνοντας τη χωρητικότητα του συστήματος
Ασφάλεια και κρυπτογράφηση (Triple DES)	Προστατεύει τα δεδομένα του χρήστη
Automatic Power control	Δυνατότητα για δημιουργία, ελαχιστοποιώντας τη ομοδιαυλική παρεμβολή

Σχήμα 4.3.2 Χαρακτηριστικά MAC του 802.16a

4.4 Εφαρμογές

Ένα ασύρματο δίκτυο βασισμένο στην τεχνολογία WiMAX είναι κατασκευασμένο πάνω κάτω με τον ίδιο τρόπο όπως ένα παραδοσιακό κυψελωτό δίκτυο με στρατηγικά τοποθετημένους σταθμούς-βάσεις χρησιμοποιώντας την αρχιτεκτονική point-to-multipoint με σκοπό να παρέχει υπηρεσίες σε μία ακτίνα μερικών χιλιομέτρων. Το πόσο μεγάλη θα είναι αυτή η ακτίνα, εξαρτάται από τη συχνότητα, από την ισχύ εκπομπής, καθώς επίσης και από την ευαισθησία του δέκτη. Σε πυκνοκατοικημένες περιοχές η εμβέλεια θα περιορίζεται από την χωρητικότητα λόγω του περιορισμού στο διαθέσιμο φάσμα.

Οι σταθμοί βάσης συνδέονται συνήθως στο κεντρικό δίκτυο (core network),μέσω οπτικής ίνας ή μέσω point-to-multipoint μικροκυματικών ζεύξεων στους διαθέσιμους κόμβους ινών ή μέσω μισθωμένων γραμμών από τον πάροχο του ενσύρματου δικτύου. Η εμβέλεια και η ικανότητα NLOS καθιστούν την τεχνολογία εξίσου ελκυστική και οικονομική σε μια ευρεία γκάμα εφαρμογής τους σε λειτουργικά περιβάλλοντα. Η τεχνολογία αυτή είχε από την αρχή προβλεφθεί ώστε να παρέχει ασύρματη ευρυζωνική πρόσβαση μέσω του τελευταίου μιλίου (last mile) στο μητροπολιτικό δίκτυο (MAN), με επιδόσεις

ισάξιες ή και καλύτερες ακόμη από ένα παραδοσιακό ADSL ή τις μισθωμένες T1/E1 γραμμές υπηρεσιών.

Λόγω των μεγάλων αποστάσεων που καλύπτει και ταυτόχρονα των υψηλών ρυθμών μετάδοσης που μπορεί να παρέχει, το πρότυπο WiMax βρίσκει πολλές εφαρμογές, λύνοντας σημαντικά προβλήματα που απασχολούσαν του τεχνικούς δικτύων σήμερα.

Τρεις είναι οι βασικότερες χρήσεις του :

- **Δίκτυο κορμού στα κυψελωτά συστήματα κινητής τηλεφωνίας:** Το κόστος της εξάπλωσης των δικτύων κινητής τηλεφωνίας αναμένετε να μειωθεί σημαντικά
- **Broadband on Demand:** Παρέχει υψηλούς ρυθμούς μετάδοσης κάνοντας εφικτή τη χρήση της τεχνολογίας για εφαρμογές πραγματικού χρόνου
- **Παρέχει κάλυψη σε περιοχές που είναι αδύνατο να καλυφθούν με χρήση χαλκού ή οπτικής ίνας:** Μπορεί να χρησιμοποιηθεί σαν συμπλήρωμα δικτύων οπτικών ινών σε τμήματα του εδάφους στα οποία το κόστος εγκατάστασης και συντήρησης δικτύων οπτικών ινών είναι απαγορευτικό.

Οι τομείς αγοράς που θα μελετηθούν είναι οι παρακάτω;

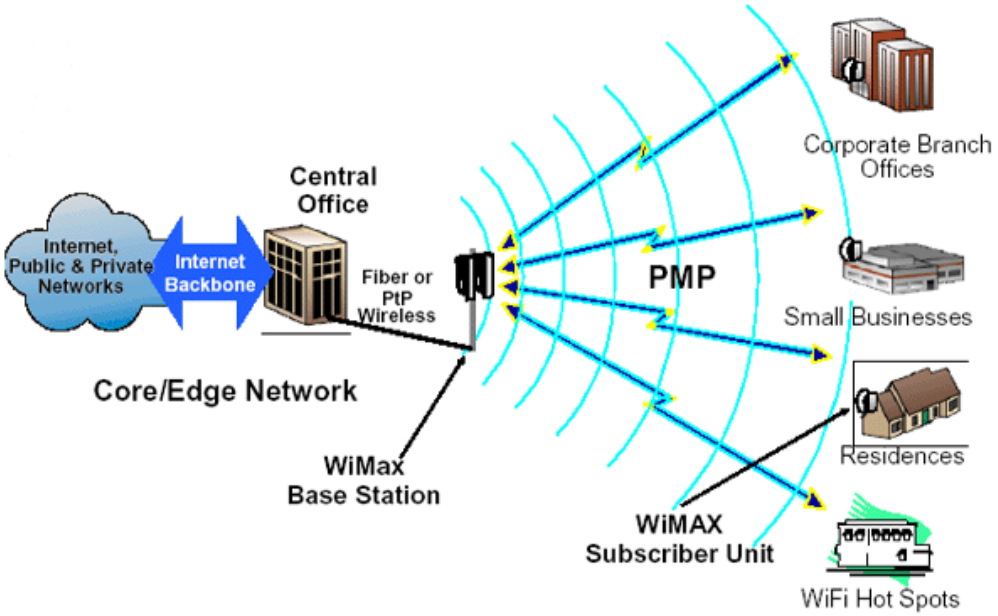
i. **Οικιακή και SOHO υψηλής ταχύτητας πρόσβαση στο Διαδίκτυο**: Σήμερα αυτός ο τομέας της αγοράς βασίζεται πρωτίστως στη διαθεσιμότητα του ADSL ή του καλωδίου. Σε μερικές περιοχές η διαθέσιμες υπηρεσίες μπορεί να μην ανταποκρίνονται στις προσδοκίες του αγοραστικού κοινού ως προς την απόδοση καθώς περιορίζονται σε χαμηλές dial-up συνδέσεις. Στις αναπτυσσόμενες χώρες υπάρχουν πολλές περιοχές όπου δεν υπάρχει με κανένα τρόπο σύνδεση στο Διαδίκτυο. Η ανάλυση θα δείξει ότι η τεχνολογία WiMAX καθιστά δυνατόν, ένας πάροχος να καλύψει αυτές τις περιοχές με καθόλου υπέρογκο κόστος και η εταιρεία του να είναι ιδιαίτερα επικερδής.

ii. **Μικρές και μεσαίου μεγέθους επιχειρήσεις**: Ο τομέας αυτός του αγοραστικού κοινού πολύ συχνά, εξυπηρετείται από χαμηλής ποιότητας υπηρεσίες, αν εξαιρέσουμε τις υψηλά ανταγωνιστικές αστικές περιοχές. Η τεχνολογία WiMAX μπορεί με υψηλό συντελεστή απόδοσης-κόστους να

ικανοποιήσει τις απαιτήσεις μιας μικρής ή μεσαίου μεγέθους επιχείρησης σε αραιοκατοικημένες περιοχές. Επίσης μπορεί να προσφέρει εξαιρετικά ανταγωνιστικές και οικονομικές λύσεις σε αστικές περιοχές με ADSL και μισθωμένες γραμμές υπηρεσιών.

iii. **WiFi Hot Spot Backhaul:** Παγκοσμίως, εγκαθίστανται WiFi hot spots με πολύ γοργό ρυθμό. Παρόλα αυτά, ένα από τα εμπόδια της επέκτασης του είναι η διαθεσιμότητα υψηλής χωρητικότητας, χαμηλού κόστους backhaul λύσεων. Αυτή η εφαρμογή μπορεί επίσης να καλυφθεί από την τεχνολογία WiMAX. Με την νομαδική ικανότητα, το WiMAX μπορεί να βοηθήσει στην κάλυψη των κενών από τα WiFi hot spots.

Η WiMAX αρχιτεκτονική και η εφαρμογές αναπαρίστανται στο παρακάτω σχήμα.



Σχήμα 4.2 Αρχιτεκτονική WiMAX

4.5 Πλεονεκτήματα - Μειονεκτήματα

Τα βασικά πλεονεκτήματα του WiMax σε σχέση με τα πρότυπα 802.11 (Wifi), περιλαμβάνουν τα ακόλουθα:

1. Υψηλότερες ταχύτητες πρόσβασης σε σχέση με το WiFi.
2. Σημαντικά υψηλότερη εμβέλεια από το WiFi.
3. Ένας ενιαίος κύριος σταθμός WiMAX μπορεί να εξυπηρετήσει εκατοντάδες χρήστες.
4. Τα τερματικά σημεία εγκαθίστανται εντός ημερών αντί των εβδομάδων που απαιτούνται για τις συνδεμένες με καλώδιο συνδέσεις.
5. Μπορεί να δουλέψει σε ορισμένες συχνότητες και χωρίς οπτική επαφή.

Το WiMax παρουσιάζει επίσης και μια σειρά από μειονεκτήματα στα οποία συμπεριλαμβάνονται τα ακόλουθα:

1. Η οπτική επαφή (LOS) απαιτείται για τις μεγάλης απόστασης (5-30 μίλια) συνδέσεις.
2. Οι δυνατές βροχές μπορούν να δημιουργήσουν προβλήματα στην ρυθμαπόδοση.

Άλλη ασύρματη ζεύξη στην περιοχή μπορεί να δημιουργήσει παρεμβολές και να προκαλέσει μια μείωση της ρυθμαπόδοσης.

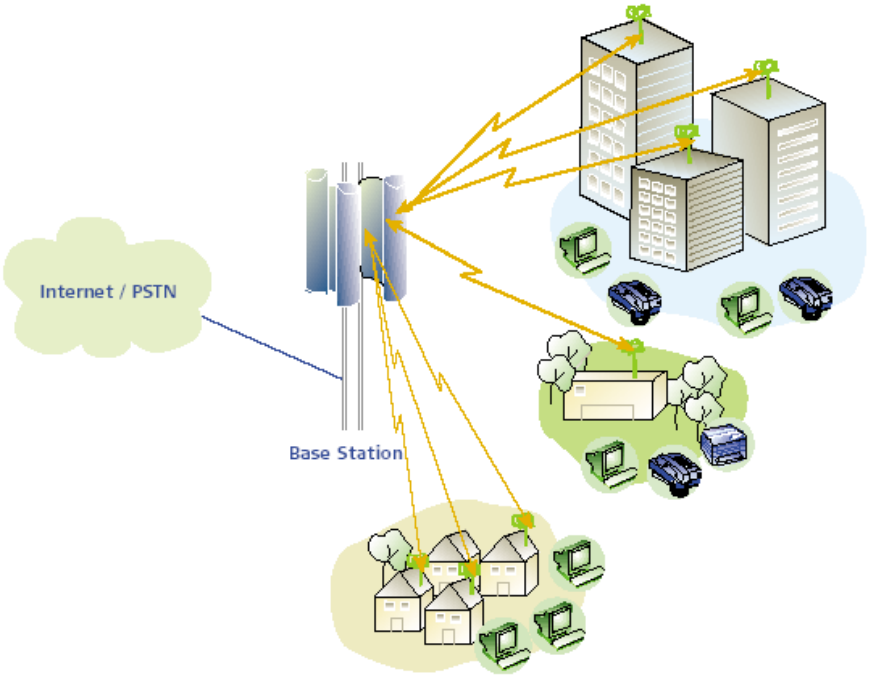
4.6 Παραλλαγές

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

- 802.16a

Το πρότυπο αυτό εγκρίθηκε τον Ιανουάριο του 2003.Λειτουργεί για οποιαδήποτε συχνότητα στο διαάστημα 2-11 GHz. Στις παραπάνω συχνότητες, η επικοινωνία NLOS (Non-Line of Sight) είναι πραγματικότητα με το πρότυπο αυτό, γεγονός που το καθιστά ως τη κατάλληλη τεχνολογία για εφαρμογές last-mile. Ο συνολικός ρυθμός δεδομένων φτάνει τα 100 Mb/s σε κάθε κανάλι επικοινωνίας των 20MHz. Οι τυπικές ακτίνες κυψελών είναι 1-2 μίλια.

Αποτελεί τη κατάλληλη backhaul τεχνολογία για να συνδέσει 802.11 wireless LANs (τοπικά δίκτυα υπό το πρότυπο τεχνολογίας 802.11) και commercial hotspots με το διαδίκτυο. Απευθύνεται κυρίως σε επιχειρήσεις, οικιακούς χρήστες, προωθώντας την ανάπτυξη των ευρυζωνικών υπηρεσιών ακόμα και σε περιοχές όπου η παραδοσιακή ενσύρματη επικοινωνία είναι μη διαθέσιμη. Η τυπική τοπολογία συστήματος 802.16 αποτελείται από ένα κεντρικό σταθμό βάσης στη κορυφή κτηρίου ή πύργου, που επικοινωνεί με κινητό συνδρομητή. Η ζεύξη είναι σημειακή-πολύ-σημειακή (a point-to-multipoint communication). Στο ακόλουθο σχήμα απεικονίζεται η τοπολογία αυτή.



Σχήμα 4.1 Σύνδεση point to multipoint

- 802.16b

Το πρότυπο IEEE 802.16b αναφέρεται σε συστήματα FWA με συχνότητες λειτουργίας (license-exempt applications) 5-6 GHz.

- 802.16c

Σκοπός η ανάπτυξη προφίλ συστημάτων με συχνότητα λειτουργίας 10-66 GHz και προδιαγραφών ασύρματης ευρυζωνικής πρόσβασης LOS (Line-of-sight). Μέγιστοι ρυθμοί δεδομένων σε αυτά, 70Mbits/s, με ακτίνα κάλυψης μέχρι 50km.

- 802.16d

Εγκρίθηκε στις 24 Ιουνίου 2004. Δημοσιεύεται με το τίτλο IEEE Standard 802.16-2004 αντικαθιστώντας τα πρότυπα IEEE 802.16-2001, 802.16c-2002 και 802.16a-2003. Στόχος του η ανάπτυξη προφίλ συστημάτων 802.16 ("Air Interface for Fixed Broadband Wireless Access Systems")

- IEEE 802.16e (Mobile Wireless MAN)

Το πρότυπο αυτό εγκρίθηκε στις 23 Σεπτεμβρίου 2004. Αποτελεί παραλλαγή του πρότυπου IEEE 802.16 ("Air Interface for Fixed Broadband Wireless Access Systems") όπως αυτό ορίζεται στα πρότυπα IEEE Standards 802.16a και 802.16c.Περιέχει τις προδιαγραφές των επιπέδων Physical, Medium Access Control για τη συνδυασμένη λειτουργία σταθερής και εν κινήσει ασύρματης ευρυζωνικής πρόσβασης σε αδειοδοτημένες μπάντες συχνοτήτων.

Παρέχει στους χρήστες τη δυνατότητα ασύρματης σύνδεσης με πάροχο υπηρεσιών διαδικτύου (Wireless Internet Service Provider), όταν ταξιδεύουν πέραν του γραφείου ή του σπιτιού τους ή σε άλλη πόλη που έχει διαφορετικό WISP. Αναπτύσσει δηλαδή νομαδικούς χρήστες. Η σύνδεση του κινητού

χρήστη είναι εφικτή για ταχύτητες από 75 μέχρι 93 μίλια την ώρα. Συμπληρώνει ή ανταγωνίζεται το πρότυπο IEEE 802.20, το οποίο αποτέλεσε αντικείμενο μελέτης και ανάπτυξης προγενέστερα του IEEE802.16e.

Ασύρματα Πρότυπα	**Ταχύτητα (Mbps)**	**Εμβέλεια**	**Συχνότητα**	**Διασύνδεση**	**Υποστηρίζεται**
Bluetooth	1Mbps	10m	2.4GHz	Καμία	Eriscon,IBM, Intel, Toshiba, Nokia, Motorola
HomeRF	2Mbps	50m	2.4GHz	Ethernet	Proxim, Intel, HP, 3COM, Motorola
IEEE802.11 **802.11b** **802.11a** **802.11g**	2Mbps 11Mbps 54Mbps 54Mbps	100m-2km	2.4GHz 2.4GHz 5GHz 2.4GHz	Ethernet	Cisco, Lucent, 3COM, Apple, Nokia, Compaq
Wi-max	70 Mbps	70Km	2-11 GHz		Red Line

Πίνακας 4.1: Σύγκριση Ασύρματων Τεχνολογιών

4.7 Σύγκριση Wi-Fi και WiMax

Οι δύο αυτές τεχνολογίες WiFi και WiMax έχουν δημιουργηθεί για να ικανοποιούν το καθένα και διαφορετικές εφαρμογές. Παρόλα αυτά συχνά γίνονται αντικείμενα σύγκρισης και αρκετές φορές σύγχυσης, αφού και οι δύο τεχνολογίες αρχίζουν με τα ίδια γράμματα IEEE, τα πρότυπα τους ξεκινάνε από 802. και επειδή και τα δύο αφορούν ασύρματες επικοινωνίες.

Μια σημαντική διαφορά του προτύπου WiMax σε σχέση με το WiFi είναι ότι το πρώτο μπορεί να χρησιμοποιηθεί και σε συνθήκες όπου δεν υπάρχει οπτική επαφή, ωστόσο με σημαντική μείωση στο ρυθμό μετάδοσης δεδομένων πολύ χαμηλότερο των 50 Mbps.

Επιπλέον το WiMax παρέχει υψηλότερου επιπέδου ποιότητα υπηρεσίας. Το επίπεδο MAC του προτύπου 802.16 έχει σχεδιαστεί με τέτοιο τρόπο, ώστε να παρέχει στους τελικούς χρήστες εγγυημένο ρυθμό μετάδοσης και συγχρόνως κίνηση best effort σε χρήστες που καλύπτονται από το ίδιο σταθμό βάσης, έπειτα από δική τους επιθυμία. Αυτό φυσικά δεν διασφαλίζεται και από το πρότυπο 802.11, όπως εξηγήσαμε και πιο πριν. Συμπερασματικά λοιπόν, όσοι χρήστες βρίσκονταν στην κάλυψη ενός Access Point είχαν την ίδια ποιότητα υπηρεσίας.

Το WiFi είναι μια τεχνολογία για τοπική δικτύωση και σχεδιάστηκε για να δώσει μια κινητικότητα σε ιδιωτικά ενσύρματα LAN ενώ το WiMAX σχεδιάστηκε για να παρέχει ευρυζωνική ασύρματη πρόσβαση (Broadband Wireless Access BWA). Αυτή είναι και η θεμελιώδης διαφορά μεταξύ των συγκεκριμένων προτύπων. Στόχος των υπηρεσιών BWA είναι η ασύρματη πρόσβαση στο internet χωρίς καλώδια και DSL τεχνολογίες. Έτσι, ενώ το WiFi υποστηρίζει εύρος μετάδοσης μερικών εκατοντάδων μέτρων, τα WiMAX συστήματα είναι σε θέση να υποστηρίξουν υπηρεσίες της τάξης των 10 χιλιομέτρων. Το παραπάνω στοιχείο αποτελεί και το επιχείρημα γιατί δεν είναι ακόμη τόσο διαδεδομένη η χρήση των συστημάτων WiMAX όσο αυτών που χρησιμοποιούν την τεχνολογία WiFi, αφού το WiFi στοχεύει στο χρήστη ενώ το WiMAX χρησιμοποιείται κυρίως για μεταφορά δεδομένων σε μακρινές αποστάσεις.

Μία άλλη σημαντική διαφορά είναι ότι το WiMax παρέχει συμμετρικό εύρος ζώνης για πολλά χιλιόμετρα και σειρά με την ισχυρότερη κρυπτογράφηση (3DES ή AES) και συγκεκριμένα με τη λιγότερη παρέμβαση. Σε αντίθεση με το WiFi που έχει κρυπτογράφηση WEP ή WPA και δεν μπορεί να υπάρχει μεγάλη παρέμβαση σε περιοχές όπως αυτές που παρέχουν πολλοί συνδεδεμένοι χρήστες.

Επίσης οι δυναμικές ζώνες του προτύπου IEEE 802.11 είναι backhauled στο ADSL, επομένως η πρόσβαση WiFi είναι τυπικά υποστηριζόμενη και έχει πολύ μικρές upload ταχύτητες μεταξύ του δρομολογητή και του Διαδικτύου.

Εκτός από αυτές τις διαφορές σχετικά με το εύρος μετάδοσης των δύο προτύπων, υπάρχουν αρκετές διαφορές στη ραδιοτεχνολογία που διακρίνουν τα δύο πρότυπα. Από τη μια πλευρά το WiMax αποτελείται από ένα πολύ μεγάλο εύρος πιθανών υλοποιήσεων για να μπορεί να παίξει το ρόλο του μεταφορέα σήματος σε ολόκληρο τον κόσμο και από την άλλη το WiFi περιγράφει 4ων τύπων ραδιοσυνδέσεις, οι οποίες δουλεύουν στις συχνότητες 2.4 ή 5 GHz στη μη νόμιμη περιοχή. Αυτό που είναι επίσης αξιόλογο να σημειωθεί, είναι ότι ενώ όλες οι υλοποιήσεις του WiFi χρησιμοποιούν μη νόμιμες συχνοτικές μπάντες, το WiMAX δουλεύει σε νόμιμες και μη, μπάντες συχνοτήτων.

Επίσης τα πρότυπα WiFi και WiMAX έχουν και μία σημαντική διαφορά στο εύρος ζώνης των καναλιών. Το WiFi καθορίζει ένα σταθερό εύρος ζώνης καναλιού που είναι 25MHz για το 802.11b και 20MHz για τα 802.11a και 802.11g. Αντίθετα στο WiMAX, το εύρος ζώνης του καναλιού είναι προσαρμοστικό και κυμαίνεται από το 1.25MHz μέχρι τα 20MHz .

Βιβλιογραφία(Ελληνική)

[1] «Εισαγωγή στα ασύρματα δίκτυα», *Δρ. Ε. Μ. ΠΑΛΛΗΣ*

[2] «Εισαγωγή στις Νέες Τεχνολογίες Επικοινωνιών", Πομπόρτσης Α., Εκδόσεις, Α. Τζιόλα Ε.

[3] «Διαχείριση Δικτύων Υπολογιστών» Μάγκλαρης Β., Χιώτης Τ., Καρούνος Θ., Σταματελόπουλος Φ., Εκδόσεις Ε.Μ.Π., 1994

[4] «Δίκτυα Δημόσιας Χρήσης και Διασύνδεση Δικτύων», Χρήστος Ι. Μπούρας , Έκδοση 2004

[5] «Δίκτυα Επικοινωνιών», Jean Walrand, 1997

[6] «Δίκτυα Κινητών και Προσωπικών Επικοινωνιών», Θεολόγου, Μ.Ε., Εκδόσεις Ε.Μ.Π., 2002

[7] «Δίκτυα Υπολογιστών Ι», ΓΙΩΡΓΟΣ ΦΟΥΣΚΑΣ, ΕΑΠ 2002

[8] «Δίκτυα Υψηλών Ταχυτήτων», Χρήστος Ι. Μπούρας, Έκδοση 2005

[9] «Μια μελέτη του κραταιού πρωτοκόλλου ασύρματης δικτύωσης», WiFi - 802.11b

Βιβλιογραφία(Αγγλική)

[1] «802.11 Wireless Networks – The Definitive Guide», Gast, S. Matthew, O'Reilly & Associates, 2002

[2] «Computer Networks, 4th edition», Tanenbaum, Andrew S., Prentice Hall, 2003

[3] «OFDM For Wireless Multimedia Communications», Van Nee, Richard, Prasad, Ramjee, Artech House, 2000

[4] «Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications», IEEE 802.11-1999, 1999

[5] «Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer Extension in the 2,4 GHz Band», IEEE 802.11b-1999, 1999

[6] «Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-Speed Physical Layer in the 5 GHz Band» IEEE 802.11a-1999, 1999

[7]«Principles Of Wireless Networks – A Unified Approach», Pahlavan, Kaveh, Krishnamurthy Prashant, Prentice Hall, 2002

[8]«QoS Enhancement in IEEE802.11 Wireless Local Area Networks», Gu, Daqing, Zhang, Jinyun, IEEE Communications Magazine, Ιούνιος 2003

[9] «Wireless Communications and Networks», Stallings, William, Prentice Hall, 2002

Δικτυακοί Τόποι

[1] http://www.bluetooth.org

[2] http://hiperlan2.com

[3] http://www.wikipedia.org

[4] http://www.wimaxforum.org/home/

[5] http://el.wikipedia.org/wiki/802.11

[6] http://el.wikipedia.org/wiki/WiMAX

[7] www.ieee802.org