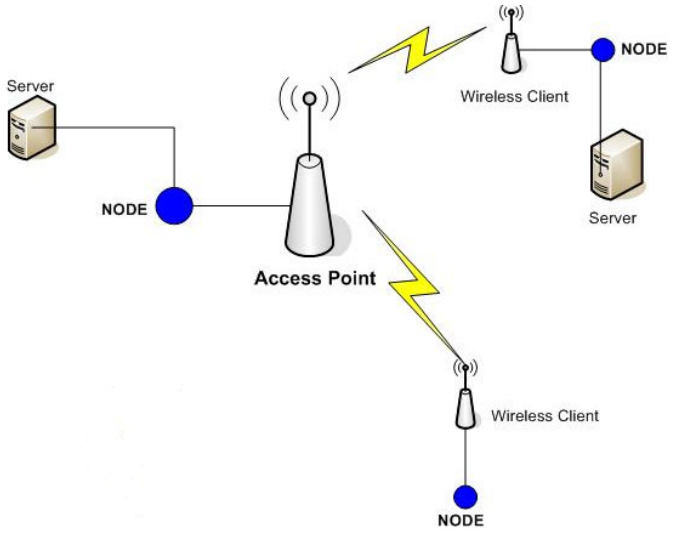
ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ
ΤΕΙ ΗΠΕΙΡΟΥ

ΤΜΗΜΑ ΤΗΛΕΠΛΗΡΟΦΟΡΙΚΗΣ& ΔΙΟΙΚΗΣΗΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ (Σ.Δ.Ο.)

ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ - WIFI
ΤΟ ΠΡΟΤΥΠΟ 802.11



Επιβλέπον καθηγητής: Κιτσαντάς Θωμάς

Σπουδάστρια: Ευαγγέλου Ελένη

ΑΡΤΑ 2006

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Η παρούσα εργασία έχει ως θέμα ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ-**WIFI.** Οπότε σκοπό έχει την αναφορά κάποιων πραγμάτων γύρω από τα ασύρματα δίκτυα και την ανάλυση του προτύπου 802.11, γνωστού και ως **WiFi** που αποτελεί το πρώτο πρότυπο για ασύρματη δικτύωση το οποίο αναπτύχθηκε. Εδώ να σημειώσουμε ότι τα ασύρματα τοπικά δίκτυα τα οποία είναι συμβατά με το πρότυπο IEEE 802.11 ονομάζονται και δίκτυα **Wi-Fi.**

Στο 1ο κεφάλαιο γίνεται μια γενική αναφορά στα ασύρματα δίκτυα. Εξηγούμε τι είναι τα ασύρματα δίκτυα, που μας χρειάζονται, καθώς και μια αναδρομή στην ιστορία τους. Στη συνέχεια μιλάμε για το βασικό εξοπλισμό ο οποίος χρησιμοποιείται στα ασύρματα δίκτυα και κλείνοντας το κεφάλαιο αναφερόμαστε στην ασφάλεια των ασύρματων δικτύων.

Στο 2ο κεφάλαιο μιλάμε για ασύρματες τεχνολογίες και πρότυπα ενώ κάνουμε εκτενέστερη αναφορά σε αυτά που θεωρούμε πιο σημαντικά, τα πρότυπα 802.11 και 802.16 και στο **Bluetooth** που αποτελεί τη βασικότερη τεχνολογία των ασύρματων δικτύων. Κλείνουμε το κεφάλαιο αναφερόμενοι σε μελλοντικά πρότυπα και τεχνολογίες.

Στο 3ο κεφάλαιο γίνεται ανάλυση του προτύπου 802.11 αφού είναι το κυρίαρχο πρότυπο στα ασύρματα **WLAN's** και όχι μόνο. Κάνουμε λοιπόν μία αναφορά στην ιστορία του προτύπου, τι είναι και που χρησιμοποιείται. Επίσης αναφερόμαστε αναλυτικά στην αρχιτεκτονική του.

Η εργασία αυτή κλείνει με το 4ο κεφάλαιο στο οποίο αναφέρουμε τα υποπρότυπα του προτύπου 802.11 που μας απασχόλησε σε όλες σχεδόν τις ενότητες της εργασίας, ενώ τη θέση επίλογου παίρνει η τελευταία παράγραφος που μιλάει για τις μελέτες νέων μεθόδων και προτύπων.

1 ΕΙΣΑΓΩΓΗ ΣΤΑ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

1.1 ΤΙ ΕΙΝΑΙ ΤΑ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ ΚΑΙ ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ ΣΕ ΑΥΤΑ

Το ασύρματο όριο δικτύωσης αναφέρεται στην τεχνολογία που καθιστά ικανούς δύο ή περισσότερους υπολογιστές (PC) να επικοινωνήσουν χρησιμοποιώντας κανονικά πρωτόκολλα δικτύωσης, αλλά χωρίς δικτυωτό καλώδιο. Με απλά λόγια τα ασύρματα δίκτυα (wireless networks) είναι δίκτυα στα οποία η πληροφορία δε μεταφέρεται μέσω καλωδίων, επιτρέποντας έτσι ευελιξία στο χρήστη για ανταλλαγή δεδομένων, ενώ χρησιμοποιούνται υπέρυθρα, υπεριώδη ή ράδιο κύματα για να συνδέσουν τα υπολογιστικά συστήματα στο δίκτυο. Η υπάρχουσα κατάσταση γενικά αναφέρεται σε ασύρματα LAN.
Αυτή η τεχνολογία (τροφοδοτείται από την εμφάνιση του cross-vendor industry και χρησιμοποιεί standards όπως IEEE 802.11) έχει παράγει ένα αριθμό από παρεχόμενες ασύρματες λύσεις που αναπτύσσονται σε πολιτισμούς με επιχειρήσεις και σχολεία τόσο καλά όσο έξυπνες εφαρμογές που είναι αδύνατες για τα ενσύρματα δίκτυα, τέτοιες όπως με αποθήκευση ή σημεία πώλησης με εξοπλισμό που τον κρατάς στο χέρι (handheld).
Η έννοια του ασύρματου δικτύου και ποιο συγκεκριμένα της ασύρματης επικοινωνίας δεν είναι νέα ιδέα. Ήδη από το 1901 ο Ιταλός φυσικός Γουλιέλμος Μαρκόνι επέδειξε στο κοινό έναν ασύρματο τηλέγραφο ανάμεσα στα πλοία και στη ξηρά. Ως κώδικα ο Μαρκόνι χρησιμοποίησε το κώδικα μορς (οι τελείες και οι παύλες είναι άλλωστε δυαδικό σύστημα). Τα σύγχρονα ψηφιακά ασύρματα έχουν βέβαια πολύ καλύτερη απόδοση, αλλά η βασική ιδέα είναι η ίδια.
Συνεχίζοντας την αναδρομή μετά τον Marconi, τα πρώτα ασύρματα δίκτυα που εμφανίστηκαν ήταν τα ραδιοδίκτυα δεδομένων (Data) τεχνολογίας TCP/IP. Οι πρώτες τεχνικές μεταγωγής πακέτων αναπτύχθηκαν γύρω στο 1964, ενώ ο όρος Packet" προτάθηκε από τον D. W. Davies του National Physical Laboratory της Μ. Βρετανίας. Οι έρευνες του εργαστηρίου αυτού οδήγησαν στο σημερινό διεθνές δημόσιο δίκτυο μεταγωγής πακέτων Χ.25, ενώ το ίδιο έτος ο οργανισμός ARPA (Advanced Research Projects Agency) των Η.Π.Α. άρχισε να χρηματοδοτεί τα προγράμματα που οδήγησαν στη δημιουργία του ARPAnet (πυρήνα του σημερινού Internet) το 1969.
Η τεχνολογία των ασυρμάτων δικτύων μετάδοσης πακέτων άρχισε να αναπτύσσεται στην δεκαετία 1970-1980, αν και η μεγάλη ανάπτυξή της συμπίπτει με την διάδοση των μικροϋπολογιστών στην δεκαετία 1980-1990. Εδώ αξίζει να

αναφέρουμε ότι το πρώτο ολοκληρωμένο ασύρματο LAN κατασκευάστηκε στο πανεπιστήμιο της Χαβάης στα πλαίσια ενός project που λέγονταν ***ALOHANET***. Λόγω των ιδιαίτερων χαρακτηριστικών του μέσου μεταδόσεως τα ασύρματα δίκτυα χρησιμοποιούν εξειδικευμένα πρωτόκολλα για το υποεπίπεδο πρόσβασης μέσου (Medium Access Control) και το επίπεδο σύνδεσης δεδομένων (Data Link Layer) και συχνά και για ανώτερα επίπεδα (π.χ. δρομολόγηση πακέτων).

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

Τα τελευταία χρόνια γίνονται σταθερά βήματα προόδου για την βελτίωση της ποιότητας των ασυρμάτων δικτύων με όλο και αυξανόμενες ταχύτητες και νέα πρότυπα από οργανισμούς και συμμαχίες γνωστών εταιρειών. Χαρακτηριστικά είναι τα παραδείγματα του **Bluetooth, GPRS (General Packet Radio Service)**, ενώ σε εξέλιξη βρίσκονται και άλλα δύο πρότυπα. Το ένα αναπτύσσεται στην Ευρώπη από το **ETSI (European Telecommunications Standard Institute)** και ονομάζεται **HIPERLAN (High – Performance European Radio LAN).** Το άλλο αναπτύσσεται από την **IEEE (Institute of Electrical and Electronics Engineers)** και ονομάζεται **802.11 WLAN.** Και τα δύο αυτά πρότυπα καλύπτουν τις προδιαγραφές για το φυσικό στρώμα και το υπόστρωμα MAC (**Medium Access Control**).

Περισσότερες λεπτομέρειες κυρίως για τα πρότυπα των ασύρματων δικτύων θα δούμε στη συνέχεια.

Ζώντας σε μια εποχή ραγδαίας τεχνολογικής προόδου όπου η διάδοση της πληροφορίας γίνεται με ασύλληπτη ταχύτητα θα ήταν μάλλον περιττό να κάνουμε μια εκτενή αναφορά στο κεντρικό ρόλο που παίζουν τα δίκτυα στην ανάπτυξη αυτή. Αρκεί να πούμε ότι στην εποχή μας η μετάδοση της πληροφορίας, η ανταλλαγή δεδομένων, η επικοινωνία βασίζεται αποκλειστικά στα δίκτυα (Internet, τηλεφωνία κλπ). Όμως γιατί στραφήκαμε στα ασύρματα δίκτυα; Τι παραπάνω μας προσφέρουν σε σχέση με τα ενσύρματα; Παρακάτω θα δούμε κάποια από τα πλεονεκτήματα των ασύρματων δικτύων που θα μας έπειθαν να τα προτιμήσουμε.

1.2 ΓΙΑΤΙ ΝΑ ΕΠΙΛΕΞΩ ΤΗΝ ΑΣΥΡΜΑΤΗ ΔΙΚΤΥΩΣΗ

1. Ευελιξία στην εγκατάσταση, στη συντήρηση και στη χρήση

Η εγκατάσταση ενός WLAN μπορεί να γίνει σε ελάχιστο χρόνο. Επιπλέον, είναι αρκετά εύκολη ως διαδικασία, αφού εδώ, σε αντίθεση με τα ενσύρματα δίκτυα, ούτε προβλήματα καλωδίωσης συναντάμε ούτε λαμβάνεται υπ' όψη η κτηριακή δομή.

2. Απαλλαγή από καλωδίωση

Η ασύρματη τεχνολογία επιτρέπει τη χρήση του δικτύου σε χώρους που η τοποθέτηση καλωδίων είναι ανεπιθύμητη ή ακόμα πολύ δύσκολο να πραγματοποιηθεί.
Π.χ. σε κάποιο περιορισμένο χώρο γραφείου, σε διατηρητέα κτίρια ή ακόμα και εκεί που κάποιο φυσικό όριο δεν επιτρέπει την τοποθέτηση καλωδίων.

3. Δυνατότητα πρόσβασης σε real-time

Το κατεξοχήν πλεονέκτημα που παρέχει ένα ασύρματο δίκτυο στους χρήστες του είναι η δυνατότητα πρόσβασης, σε πραγματικό χρόνο, σε βάσεις δεδομένων, ακόμη και αν εκείνοι βρίσκονται εν κινήσει. Μάλιστα, η προσβασιμότητα από παντού των δικτυακών πόρων μιας εταιρείας ή επιχείρησης, για παράδειγμα, διευκολύνει το έργο των υπαλλήλων, εκείνοι με τη σειρά τους αποδίδουν καλύτερα και έτσι αυξάνεται η παραγωγικότητα.

Επιπλέον, επιτρέπεται σε χρήστες κινητών ή φορητών συσκευών να έχουν πρόσβαση σε real-time πληροφορία από όπου και αν βρίσκονται μέσα στο δίκτυο.

4. Μειωμένο κόστος χρήσης

Ενώ το αρχικό κόστος για το hardware που θα υποστηρίξει ένα ασύρματο τοπικό δίκτυο είναι μεγαλύτερο από αυτό ενός ενσύρματου δικτύου, τα συνολικά έξοδα εγκατάστασης, καθώς και το κόστος χρήσης, είναι σημαντικά μικρότερα. Μακροπρόθεσμα τα οφέλη είναι ακόμη μεγαλύτερα για περιπτώσεις δυναμικών χώρων εργασίας, οι οποίες απαιτούν συχνές μετακινήσεις και αλλαγές, καθώς το κόστος του προϋπάρχοντος ασύρματου δικτύου θα είναι αμελητέο.

5. Δυνατότητα επέκτασης, plug &play

Τα ασύρματα δίκτυα μπορούν να υποστηρίξουν μια μεγάλη ποικιλία από τοπολογίες προκειμένου να ανταποκριθούν στις

ανάγκες συγκεκριμένων εφαρμογών. Οι τοπολογίες αυτές μπορούν εύκολα να αλλάξουν και περιλαμβάνουν από απλά ισότιμα δίκτυα κατάλληλα για μικρό αριθμό χρηστών, έως πλήρως εκτεταμένα δίκτυα με δυνατότητες περιαγωγής (roaming) που μπορούν να υποστηρίξουν χιλιάδες χρήστες σε μεγάλες αποστάσεις.

6. Δυνατότητα σύνδεσης με άλλο δίκτυο

Τα ασύρματα δίκτυα προσφέρουν διασύνδεση τοπικών δικτύων μεταξύ τους, όπως των καταστημάτων της επιχείρησης ή των εργαστηρίων ενός σχολικού εργαστηριακού κέντρου, επιτρέποντας τα ακόλουθα:

- Επικοινωνία των υπολογιστών συνολικά και ανεξάρτητα από την τοποθεσία
- Φωνητική επικοινωνία μεταξύ των δικτύων χωρίς κόστος
- Μείωση των τηλεπικοινωνιακών εξόδων με το μοίρασμα μιας σύνδεσης με το Διαδίκτυο προς όλα τα υποδίκτυα
- Επισκόπηση χώρων χρησιμοποιώντας Ασύρματες Κάμερες

Επιπλέον, ένα ασύρματο δίκτυο μπορεί να συνδεθεί και με κάποιο ενσύρματο δίκτυο. Για να το κάνετε αυτό θα χρειαστείτε κάποιο είδος γέφυρας μεταξύ του ασύρματου και του ενσύρματου δικτύου. Αυτό μπορεί να πραγματοποιηθεί είτε με ένα σημείο σύνδεσης υλικού ή με ένα σημείο σύνδεσης λογισμικού. Τα σημεία σύνδεσης υλικού είναι διαθέσιμα με πολλούς τύπους επαφών δικτύου, όπως ο Ethernet ή Token Ring, αλλά συνήθως χρειάζονται έξτρα υλικό αν οι απαιτήσεις του δικτύου αλλάξουν. Αν οι απαιτήσεις του δικτύου είναι περισσότερες απ' το απλώς να διασυνδέσεις ένα ενσύρματο δίκτυο σε ένα μικρό ασύρματο δίκτυο τότε το σημείο σύνδεσης λογισμικού ίσως να είναι η καλύτερη λύση. (Αν υπάρχει μικρό δίκτυο η καλύτερη λύση είναι η ασύρματη).

Το σημείο σύνδεσης λογισμικού δεν περιορίζει τον τύπο ή τον αριθμό των επαφών δικτύου που χρησιμοποιούνται. Επίσης μπορεί να επιτρέψει σημαντική ελαστικότητα στο να προσφέρει πρόσβαση σε διαφορετικούς τύπους δικτύου, όπως διαφορετικοί τύποι Ethernet, ασύρματα ή Token Ring δίκτυα. Τέτοιες συνδέσεις περιορίζονται μόνο από τον αριθμό των θυρίδων ή των επαφών του υπολογιστή που χρησιμοποιείται για αυτή την εργασία.

Πέρα απ' αυτό τα σημεία πρόσβασης λογισμικού μπορεί να περιλαμβάνουν επιπρόσθετα χαρακτηριστικά όπως πρόσβαση στο internet, web caching ή content filtering παρέχοντας σημαντικά οφέλη σε χρήστες και διαχειριστές.

7. Relocate

Ένα ασύρματο δίκτυο μπορεί εύκολα να αλλάξει την τοποθεσία στην οποία βρίσκεται (relocate), αφού οι συσκευές που είναι ασύρματα συνδεδεμένες μπορούν να μεταφέρονται πιο εύκολα (flexibility-roaming).

8. Περισσότερος χρόνος

Μπορούμε εύκολα να φανταστούμε, το χρόνο που κερδίζει κάποιος αν ακόμα και στην καφετέρια (εφόσον το επιτρέπει η κάλυψη του ασύρματου δικτύου) έχει τη δυνατότητα να διαβάσει το ηλεκτρονικό του ταχυδρομείο.

9. Εύκολο internet

Με τα ασύρματα δίκτυα είναι εξαιρετικά ευέλικτο να μοιράζεσαι μια σύνδεση στο internet ή και άλλους πόρους.

10. Αβλαβής ακτινοβολία

Ο εξοπλισμός που χρησιμοποιείται είναι εντελώς ακίνδυνος για τον ανθρώπινο οργανισμό. Η ακτινοβολία είναι μη ιονίζουσα και τα επίπεδα ακτινοβολίας είναι πολύ πιο χαμηλά από τα επιτρεπτά για τον ανθρώπινο οργανισμό όρια. Αρκεί να αναφέρουμε ότι μια ασύρματη κάρτα δικτύου (802.11b) ακτινοβολεί ισχύ 50 - 100 mwatt, ενώ ένα κινητό τηλέφωνο φτάνει και τα 2000 mwatt.

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

1.3 ΕΙΔΗ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ ΚΑΙ ΑΠΟ ΤΙ ΑΠΟΤΕΛΕΙΤΑΙ ΤΟ ΚΑΘΕΝΑ

Υπάρχουν 2 είδη ασύρματων δικτύων :

Α. Ένα ad-hoc ή peer-to-peer ασύρματο δίκτυο αποτελείται από ένα αριθμό από PC καθένα από τα οποία εφοδιάζεται με μία ασύρματη κάρτα επαφής. Το κάθε PC μπορεί να επικοινωνήσει άμεσα με όλα τα PCs που υπάρχουν στο δίκτυο. Μπορούν με αυτό τον τρόπο να διαχειριστούν τα

ίδια αρχεία και εκτυπωτές, αλλά να μην έχουν την ικανότητα να έχουν πρόσβαση σε ενσύρματες LAN πηγές, εκτός αν ένας Η/Υ λειτουργεί σαν γέφυρα στο ενσύρματο LAN χρησιμοποιώντας ειδικό λογισμικό. Αυτό ονομάζεται **“bridging”**.

Σχήμα **1: Ad-hoc or peer to peer** (Η/Υ με Η/Υ)
Κάθε Η/Υ με ασύρματη επαφή μπορεί να επικοινωνεί απευθείας με όλους τους άλλους.

Β. Ένα ασύρματο δίκτυο μπορεί επίσης να χρησιμοποιήσει ένα σημείο πρόσβασης ή ένα σταθμό βάσης. Σε αυτό τον τύπο δικτύου το σημείο πρόσβασης λειτουργεί σαν ένας κόμβος (**hub**) που προσφέρει σύνδεση σε όλους τους ασύρματους Η/Υ. Μπορεί να συνδέσει (ή **“bridge”**) το ασύρματο **LAN** σε ένα ενσύρματο **LAN** προσφέροντας ασύρματη σύνδεση σε πηγές **LAN** όπως **servers** αρχείων ή υπάρχουσα σύνδεση στο **internet**.

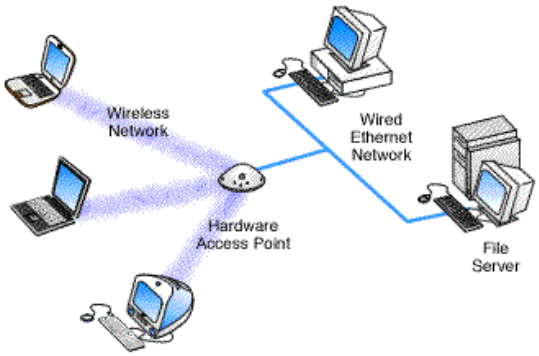
Υπάρχουν 2 τύποι σημείων εισόδου:

i. Αφοσιωμένα σημεία πρόσβασης υλικού (**HAP**) όπως **Lucent’s WaveLAN, Apple’s Airport Base Station** ή **WebGear’s AviatorPRO**. (Βλέπε εικ. 2). Σημεία πρόσβασης υλικού προσφέρουν εμπεριστατωμένη υποστήριξη, στα περισσότερα ασύρματα χαρακτηριστικά, αλλά ελέγξτε τις απαιτήσεις προσεκτικά.

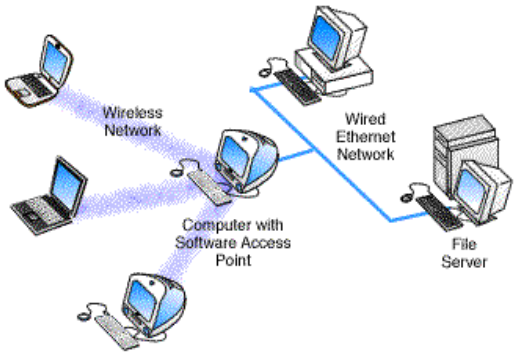
ii. Σημεία πρόσβασης λογισμικού τα οποία τρέχουν σε Η/Υ εξοπλισμένο με ασύρματη κάρτα επαφής όπως χρησιμοποιείται σε ένα **ad-hoc** ή **peer-to-peer** ασύρματο δίκτυο. (Βλέπε εικ. 3). Το **Vicomsoft InterGate** σειρά προγραμμάτων είναι δρομολογητές λογισμικού τα οποία μπορούν να χρησιμοποιηθούν σαν βασικά σημεία επαφής λογισμικού και περιλαμβάνουν χαρακτηριστικά τα οποία δεν βρίσκονται εύκολα σε λύσεις υλικού (όπως το **Direct PPPoE** ενίσχυση και εκτεταμένη ελαστικότητα στη διαμόρφωση), αλλά δε μπορεί να προσφέρουν μεγάλη ακτίνα ασύρματων

χαρακτηριστικών όπως υποστηρίζονται στο πρότυπο 802.11.

Με την κατάλληλη ενίσχυση δικτύωσης λογισμικού, χρήστες ενός ασύρματου LAN μπορούν να διαχειριστούν αρχεία και εκτυπωτές τα οποία βρίσκονται σε ενσύρματο LAN και αντίθετα. Οι λύσεις της Vicomsoft μπορούν να υποστηρίξουν μοίρασμα αρχείων χρησιμοποιώντας TCP/IP.



Σχήμα 2: Σημείο σύνδεσης υλικού – Hardware Access Point
Η/Υ ασύρματα συνδεδεμένοι χρησιμοποιώντας σημείο πρόσβασης υλικού.



Σχήμα 3: Σημείο σύνδεσης λογισμικού–Software Access Point
Η/Υ ασύρματα συνδεδεμένοι χρησιμοποιώντας σημείο πρόσβασης λογισμικού.

1.4 ΚΑΤΗΓΟΡΙΕΣ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

Με μια πρώτη προσέγγιση τα ασύρματα δίκτυα μπορούν να διαιρεθούν σε τρεις βασικές κατηγορίες :

I. Διασύνδεση συστήματος (System interconnection).
II. Ασύρματα LAN.
III. Ασύρματα WAN.

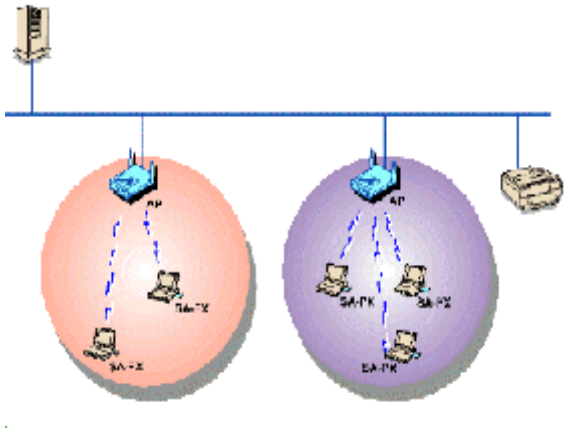
Η διασύνδεση συστήματος αναφέρεται στη διασύνδεση των εξαρτημάτων του υπολογιστή με τη χρήση ραδιοκυμάτων μικρής εμβέλειας. Έτσι ένας χρήστης που δυσκολεύεται να συνδέσει καλώδια μπορεί εύκολα να χρησιμοποιήσει ένα ασύρματο ποντίκι ή πληκτρολόγιο κ.α. Κατά συνέπεια μερικές εταιρίες αποφάσισαν να σχεδιάσουν ένα ασύρματο δίκτυο μικρής εμβέλειας το οποίο ονομάζεται ***'Bluetooth'*** για την σύνδεση των εξαρτημάτων αυτών χωρίς καλώδια. Να σημειώσουμε εδώ ότι το Bluetooth χρησιμοποιείται ευρέως στην κινητή τηλεφωνία (Σχήμα 4). Για το Bluetooth θα αναφέρουμε περισσότερα πράγματα στην συνέχεια.

Σχήμα 4: Bluetooth

Πριν προχωρήσουμε στα ασύρματα LAN, πρέπει να αναφέρουμε ότι μπορούμε πιθανώς να συναντήσουμε και μία ακόμα κατηγορία ασύρματων δικτύων τα PAN's (Personal area networks). Αυτά είναι δίκτυα που μπορούν να εγκατασταθούν σε κάποιο μικρό γραφείο ή στο σπίτι σε απόσταση 5-15 μέτρων. Μεταξύ των συσκευών του γραφείου πρέπει να υπάρχει οπτική επαφή. Δύο τεχνολογίες που χρησιμοποιούνται σε αυτού του τύπου τα συστήματα είναι η IrDA και το Bluetooth.
Το Bluetooth δεν απαιτεί οπτική επαφή. Για περισσότερες πληροφορίες για την IrDA επισκεφτείτε το site : ***www.irda.org***

Το επόμενο βήμα στην ασύρματη δικτύωση είναι τα ασύρματα LAN's (WLAN's). Αυτά είναι συστήματα στα οποία κάθε υπολογιστής έχει ένα ασύρματο modem και μια κεραία μέσω των οποίων μπορεί να επικοινωνεί με άλλα συστήματα. Το ασύρματο LAN με τη σειρά του μπορεί να συνδεθεί σε ένα ενσύρματο LAN ή να αποτελέσει βάση για ένα καινούργιο δίκτυο. Η βασική δομική μονάδα (building block) του WLAN είναι το κελί (cell). Το κελί είναι ουσιαστικά η περιοχή όπου η ασύρματη επικοινωνία λαμβάνει χώρα. Η περιοχή που

καλύπτει ένα κελί εξαρτάται από τη ισχύ διάδοσης του ραδιοκύματος και από κάποια φυσικά χαρακτηριστικά (ύπαρξη τοίχου...) που υπάρχουν στην περιοχή του δικτύου. Μπορούμε να φανταστούμε την περιοχή που καλύπτει το κελί ως κυκλική. Οι σταθμοί του δικτύου (PC's) μπορούν να μετακινούνται στο κελί χωρίς να χάνουν την επαφή με το δίκτυο. Η επικοινωνία μεταξύ των σταθμών μέσα στο κελί του ασύρματου δικτύου συντονίζονται από ένα σταθμό βάσης που ονομάζεται σημείο πρόσβασης (**access point**). Το **access point** μπορεί να συνδέσει πολλά κελιά ενός WLAN μεταξύ τους και μπορεί επίσης να συνδέσει τα κελιά του WLAN με ένα ενσύρματο **Ethernet LAN** μέσω καλωδίου σε μια έξοδο του **Ethernet LAN.** Ένα παράδειγμα μιας τοπολογίας όπου χρησιμοποιείται το πακέτο δικτύωσης BreezeNET PRO.11 φαίνεται στο παρακάτω σχήμα. Να σημειώσουμε εδώ ότι το συγκεκριμένο πακέτο χρησιμοποιεί το πρότυπο 802.11.



Σχήμα 5: WLAN

Πριν ολοκληρώσουμε την αναφορά μας στα WLAN πρέπει επίσης να σημειώσουμε ότι το access point (σημείο πρόσβασης) μπορεί να είναι hardware αλλά και κάποιο PC με κατάλληλο λογισμικό τα οποία αναλύσαμε προηγουμένως.

Το τρίτο είδος ασύρματου δικτύου (ασύρματα **WAN**) χρησιμοποιείται στα συστήματα ευρείας περιοχής. Το δίκτυο ραδιοκυμάτων που χρησιμοποιείται στα κυψελωτά (cellular) κινητά τηλέφωνα είναι παράδειγμα ασύρματου συστήματος με χαμηλό εύρος ζώνης. Αυτό το σύστημα βρίσκεται είδη στη τρίτη γενιά που καλύπτει ψηφιακά φωνή και δεδομένα. Κατά κάποιο τρόπο τα κυψελωτά ασύρματα δίκτυα είναι παρόμοια με τα WLAN's με τη διαφορά ότι οι αποστάσεις είναι πολύ μεγαλύτερες και ο ρυθμός μετάδοσης των bit πολύ χαμηλότερος. Τα WLAN's λειτουργούν σε ταχύτητες μέχρι περίπου 50 Mbps για αποστάσεις μερικών δεκάδων μέτρων. Τα κυψελωτά συστήματα λειτουργούν σε ταχύτητες κάτω από 1

Mbps αλλά η απόσταση μεταξύ του σταθμού βάσης και του υπολογιστή ή του τηλεφώνου μετριέται σε χιλιόμετρα αντί σε μέτρα.
Να σημειώσουμε εδώ ότι πολύ συχνά αναφέρεται και μια νέα κατηγορία ασύρματων δικτύων η οποία είναι ενδιάμεση των ασύρματων LAN και ασύρματων **WAN.** Αυτή η κατηγορία αναφέρεται ως ασύρματα MAN (Wireless Metropolitan Area Networks) και καλύπτει ένα μικρότερο εύρος ασύρματης δικτύωσης. Η σύγκριση του διαφορετικού εύρους των δύο δικτύων ασύρματων **WAN** και ασύρματων **MAN** φαίνεται στα δύο παρακάτω σχήματα.

Σχήμα 6: Ασύρματο MAN

Σχήμα 7: Ασύρματο WAN

1.5 ΕΞΟΠΛΙΣΜΟΣ ΑΣΥΡΜΑΤΟΥ ΔΙΚΤΥΟΥ

Στη παράγραφο αυτή αναφερόμαστε συνοπτικά σε όλες εκείνες τις μονάδες που συνθέτουν τον απαραίτητο ασύρματο

εξοπλισμό, για να μπορεί να γίνει εφικτή η πρόσβαση στο δίκτυο. Οι μονάδες αυτές είναι οι εξής:

1) **Κεραία**

Ένας απλοϊκός ορισμός της κεραίας αναφέρεται σε μια συσκευή που λαμβάνει και εκπέμπει σήματα. Το σχήμα και το μέγεθος της κεραίας έχουν να κάνουν σε μεγάλο ποσοστό, με τη συχνότητα του σήματος που λαμβάνει. Να διασαφηνίσουμε εδώ ότι η κεραία δε δίνει στον εκπομπό μεγαλύτερη ενέργεια. Ουσιαστικά η κεραία είναι μια κατευθυντική συσκευή η οποία δίνει το σχήμα κατεύθυνσης (directional pattern) για το σήμα που παράγει ο εκπομπός. Έτσι γνωρίζοντας αυτό το directional pattern, μπορεί να λάβει και καλύτερο σήμα από κάποιον άλλο εκπομπό.

Ο τύπος της κεραίας καθορίζει την μορφή ακτινοβολίας. Οι κεραίες διακρίνονται σε μη κατευθυντικές που είναι κατάλληλες για την κάλυψη των μεγάλων περιοχών, δικατευθυντικές που είναι κατάλληλες για την κάλυψη των διαδρόμων και μονοκατευθυντικές, που ενδείκνυνται για την σύνδεση μεταξύ κτιρίων (point-to-point). Αξίζει να αναφέρουμε εδώ τους βασικούς τύπους κεραιών :

Dipole: Χρησιμοποιείται για να καλύψει ένα διάδρομο, μία μεγάλη ή και μικρή περιοχή.

Vertical: Έχει κέρδος από 3-10 dBi. Είναι μη κατευθυντική σε οριζόντια κατεύθυνση. Είναι μεγαλύτερη από κάθε άλλη κεραία καθώς επίσης και ακριβότερη. Την χρησιμοποιούμε για να καλύψουμε μια περιοχή στην οποία υπάρχουν αρκετά κτίρια που θέλουμε να συνδεθούν ασύρματα.

Yagi: Είναι μια υψηλού κέρδους (12-18dBi) μονοκατευθυντική κεραία.

Parabolic: Έχει πολύ υψηλό κέρδος μέχρι και 24 dBi (very narrow beam widths). Χρησιμοποιείται στην περίπτωση που θέλουμε να συνδέσουμε δύο κτίρια. Μια τέτοια κεραία έχει εμβέλεια μέχρι και 20 miles. Και οι δύο πλευρές αυτής της ασύρματης σύνδεσης έχουν την ίδια κεραία, οι οποίες πρέπει και να σημαδεύονται σωστά. Παραβολική είναι και η κεραία τύπου grid.

Στο παρακάτω σχήμα φαίνονται παραδείγματα αυτών των τύπων κεραίας.

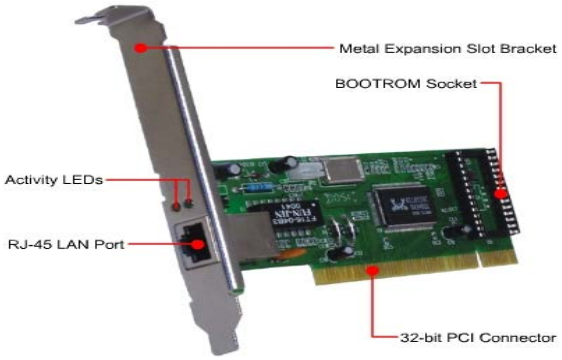
Vertical Grid Parabolic Yagi Dipole

Σχήμα 1: Τύποι κεραιών

Για να κάνουμε κατανοητή την ορολογία dBi να πούμε ότι όρος dBi υποδηλώνει το υποτιθέμενο κέρδος μίας ισοτροπικής κεραίας (υποθετική κεραία που ακτινοβολεί ενέργεια προς όλες τις κατευθύνσεις). Για παράδειγμα 0dBi είναι το κέρδος μίας υποθετικής κεραίας που ακτινοβολεί όλη την ισχύ της σε μία τέλεια ομοιόμορφη σφαιρική κατανομή. Κεραίες με τέτοια ακτινοβολία δεν υπάρχουν στην πραγματικότητα.

2) NIC

NIC ή διαφορετικά Network Interface Card, είναι το υλικό που ενσωματώνεται στην κεντρική μητρική κάρτα του υπολογιστή μας (motherboard) ή εισάγεται στο δίαυλο διασύνδεσης (bus) και έχει ως σκοπό τη σύνδεση του υπολογιστή μας με το υποσύστημα επικοινωνίας (καλωδίωση) του δικτύου μας. Κλασσικά παραδείγματα καρτών NIC's είναι αυτές που αποτελούν διεπαφή (interface) μεταξύ ενός υπολογιστή και ενός Ethernet LAN (Σχήμα 2) ή ενός FDDI δικτύου δακτυλίου.



Σχήμα 2: PCI Ethernet Network Interface Card

3) Καλώδιο RF

Σχήμα 3: Καλώδιο RF

Πρόκειται για το ένα από τα δύο καλώδια που απαιτούνται. Όταν η απόσταση της κεραίας από την κάρτα δικτύου είναι μεγαλύτερη από 50cm χρειάζεται ένα καλώδιο κεραίας που να συνδέει την υποδοχή της κεραίας με το pigtail (αναλύεται παρακάτω).

4) Connectors

Οι connectors είναι το υλικό που απαιτείται για την διασύνδεση αλλά και την προσαρμογή των επαφών (ακροδεκτών) της κάρτας δικτύου με το σύστημα καλωδίωσης. Στην περίπτωση μάλιστα εξωτερικής χρήσης οι connectors, πρέπει να είναι σωστά τοποθετημένοι, έτσι ώστε τα καλώδια να είναι απόλυτα στεγνά και προστατευμένα. Ένας connector φαίνεται στο παρακάτω σχήμα.

Σχήμα 4: MTRJ fiber optic network connector

5) UTP καλώδιο

Το UTP ή διαφορετικά unshielded twisted pair καλώδιο αποτελείται από δύο μη προστατευμένα καλώδια γυρισμένα το ένα γύρω από το άλλο. Αυτά τα καλώδια είναι τα πιο συχνά χρησιμοποιούμενα καλώδια, αφού είναι εύκολα στην εγκατάσταση και τα πιο οικονομικά. Επίσης χρησιμοποιούνται για την διασύνδεση των συσκευών Wireless to Ethernet Bridge ή USB που τοποθετούνται στην κεραία (όταν το σημείο σύνδεσης με την κεραία μας είναι μακριά από το Η/Υ).

Σχήμα 5: UTP cable

Το καλώδιο που φαίνεται στο παραπάνω σχήμα είναι UTP 5ης κατηγορίας με λίγο διαφορετική δομή από αυτή που περιγράψαμε και επιτυγχάνει ταχύτητες μεγαλύτερες των 100 million bits per second.

6) Pigtail καλώδιο

Το καλώδιο Pigtail είναι απλά ένα μικρό κομμάτι καλώδιο με connectors προσαρμογής για την ένωση του αποκλειστικού connector της κάρτας Wi-Fi με το καλώδιο της εξωτερικής κεραίας. Υπάρχουν αρκετοί τύποι αυτού του καλωδίου. ένας από αυτούς φαίνεται στο σχήμα που ακολουθεί.

Σχήμα 6: pigtail cable (type T47)

7) Γέφυρα-Bridge

Μια γέφυρα δικτύου (network bridge), αφηρημένα μπορούμε να πούμε ότι είναι μια συσκευή που συνδέει πολλαπλά τμήματα του δικτύου (network segments) μέσω του επιπέδου συνδέσμου μετάδοσης δεδομένων (data link layer). Όταν μιλάμε για network segments, μιλάμε για κομμάτια του δικτύου τα οποία χωρίζονται μεταξύ τους από κάποια δικτυακή συσκευή όπως hubs, switches, routers κ.α . Έτσι λοιπόν σε ένα δίκτυο υπολογιστών μια γέφυρα μπορεί να είναι ένας switch.
*Ο switch συνήθως χρησιμοποιείται για τοπολογία αστέρα.

Σχήμα 7: Linksys 10/100 Etherfast 8 Port Switch – EZXS88W

8) Δρομολογητής (Router)

Router ή δρομολογητή μπορούμε να θεωρήσουμε ένα ειδικού σκοπού υπολογιστή ο οποίος κατευθύνει(δρομολογεί) τα πακέτα δεδομένων στο δίκτυο. Οι δρομολογητές είναι συσκευές που μπορούν να ανιχνεύσουν εάν μέρος του δικτύου δεν λειτουργεί ή βρίσκεται σε συμφόρηση και να ανακατευθύνουν την πληροφορία.

Επίσης οι routers επιτρέπουν την διασύνδεση δικτύων με διαφορετικά πρωτόκολλα επικοινωνίας. Ο router είναι η μόνη συσκευή που ουσιαστικά βλέπει κάθε μήνυμα που αποστέλλεται και από τις δύο πλευρές του δικτύου. Έτσι μπορεί να διασφαλίσει ότι η πληροφορία θα φτάσει στον προορισμό της και απαγορεύει την πρόσβαση από το ένα δίκτυο στο άλλο, απαγορεύοντας μη αναγκαία πληροφορία να μεταφέρεται από δίκτυο σε δίκτυο. Οι routers συνδέουν πολλαπλά δίκτυα LAN και έχει πρόσβαση στις network addresses. Στο παρακάτω σχήμα φαίνεται ένας δρομολογητής της εταιρείας NETGEAR.

Σχήμα 8: NETGEAR RP114 Web Safe 4 Port Cable/DSL Network Route

1.6 ΑΣΥΡΜΑΤΗ ΑΣΦΑΛΕΙΑ

Είναι αρκετά εύκολος ο σχεδιασμός ενός ασύρματου δικτύου με χρήση VPN (virtual private network το οποίο διαθέτει μηχανισμούς ασφάλειας για δικαιούχους χρήστες και κρυπτογράφηση δεδομένων) και με χρήση firewall, ο οποίος υπόσχεται ένα αρκετά ασφαλές σύστημα. Ένας τέτοιος

σχεδιασμός μπορεί να προκύψει αν μερικές μηχανές είναι ασύρματες και χρησιμοποιούν ραδιοκυματικές επικοινωνίες, οι οποίες περνούν πάνω από firewall και από τις δύο κατευθύνσεις. Παρόλα αυτά η εμπειρία έχει δείξει ότι τέτοια δίκτυα είναι πολύ ευάλωτα σε επιθέσεις.
Μεγάλο μέρος του προβλήματος ασφάλειας μπορεί να αποδοθεί στους κατασκευαστές των access points οι οποίοι προσπαθούν να κάνουν τα προϊόντα τους όσο γίνεται πιο φιλικά στο χρήστη. Αυτή η απλότητα παραμερίζει τελείως το θέμα ασφάλειας και έτσι οποιοσδήποτε είναι εντός εμβέλειας μπορεί να αποσπάσει δεδομένα.

Ασφάλεια στο Bluetooth

Αν και το Bluetooth έχει αρκετά μικρή εμβέλεια η ασφάλεια παίζει πολύ σημαντικό ρόλο. «Φανταζόμαστε τι θα μπορούσε να συμβεί αν σε ένα γραφείο όπου όλα τα περιφερειακά των PC's ήταν ασύρματα Bluetooth και ένας ανταγωνιστής συνάδελφος προσπαθούσε να αποσπάσει τις πληροφορίες που γράφαμε μέσω του πληκτρολόγιου μας».
Το Bluetooth στην ασφάλεια είναι αρκετά αυστηρό. Παρακάτω συνοψίζονται κάποια βασικά σημεία της ασφάλειας του.

- Ο κάθε χρήστης έχει τη δυνατότητα να ορίσει ποιες υπηρεσίες θα είναι διαθέσιμες από την συσκευή του και σε ποιους.
- Κάθε συσκευή χαρακτηρίζεται από έναν κωδικό μήκους 48bit (δηλαδή μπορούν να γίνουν 2^{48} = 281.474.976.710.656 διαφορετικοί συνδυασμοί).
- Η πιστοποίηση της κάθε συσκευής που είναι συνδεδεμένη στο δίκτυο γίνεται με τυχαίο ανακάτεμα του παραπάνω μοναδικού κωδικού με τυχαίους αριθμούς που παράγονται κάθε φορά που γίνεται η σύνδεση της συσκευής του PicoNet.
- Επίσης τα δεδομένα, σε κάθε επικοινωνία, προτού μεταφερθούν κρυπτογραφούνται χρησιμοποιώντας το σύστημα της ασύμμετρης κρυπτογράφησης, ιδιωτικού – δημοσίου κλειδιού, μήκους 128bit το καθένα.

WAP & ασφάλεια
Το WAP έχει μεγαλύτερη ασφάλεια έναντι του WEB και υλοποιείται με βάση τα πρωτόκολλα SSL (Secure Sockets Layer) και WTLS (Wireless Transport Layer Security).Η μεταφορά των δεδομένων στο WAP από τον WEB γίνεται με την μεσολάβηση ενός WAP Gateway.

Έτσι όταν γίνει μια αίτηση για μεταφορά δεδομένων από μια υπηρεσία του WEB προς ένα κινητό τηλέφωνο, τότε τα δεδομένα αποστέλλονται από τον WEB Server μέσω του Internet και κάνοντας χρήση του SSL, στον WAP Gateway. Μετά τα δεδομένα μέσω του δικτύου κινητής τηλεφωνίας και κάνοντας χρήση του WTLS μεταφέρονται στο κινητό τηλέφωνο. Στο κομμάτι αυτό κάναμε μια σύντομη αναφορά σε θέματα ασφάλειας και περιγράψαμε περιληπτικά την ασφάλεια σε Bluetooth και WAP.

2 ΑΣΥΡΜΑΤΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΚΑΙ ΠΡΟΤΥΠΑ

Σε αυτή τη παράγραφο γίνεται αναφορά και μια σύντομη αλλά περιεκτική περιγραφή στις πιο δημοφιλείς ασύρματες τεχνολογίες και πρότυπα. Σκοπός μας δεν είναι να αναφέρουμε οτιδήποτε έχει υπάρξει κατά καιρούς αλλά να δώσουμε το παλμό της τεχνολογίας σε αυτό το τομέα. Να τονίσουμε πλέον ότι τα πρότυπα και οι τεχνολογίες στις οποίες θα επικεντρωθούμε αναφέρονται κατά κύριο λόγο σε ασύρματα LAN's.

2.1 ΠΡΟΤΥΠΟ IEEE 802.11

Το πρότυπο IEEE 802.11 ή διαφορετικά Wi-Fi εισάγει ένα σύνολο από standards για ασύρματα LAN's (wireless local area networks) από την ομάδα 11 της IEEE 802. Η IEEE 802 είναι η επιτροπή που ασχολείται με LAN, MAN (metropolitan area network) standards. Εδώ πρέπει να αναφέρουμε ότι το Wi-Fi (Wireless Fidelity) είναι ένα εμπορικό όνομα για το πρότυπο 802.11 αλλά τις περισσότερες φορές θα το δούμε να ταυτίζεται με το 802.11b που αναλύεται παρακάτω. Τέλος να αναφέρουμε ότι το WiFi δεν χρησιμοποιείται μόνο για ασύρματα LAN αλλά και για πρόσβαση στο internet.
Η οικογένεια 802.11 περιλαμβάνει τρία βασικά πρωτόκολλα τα οποία έχουν τις κωδικοποιήσεις 802.11a, 802.11b και 802.11g. Η ασφάλεια αρχικά συμπεριλαμβανόταν σε αυτά τα πρότυπα αλλά τώρα είναι κομμάτι άλλων προτύπων της οικογένειας όπως το 802.11i. Άλλα standards της οικογένειας 802.11 (c-f, h-j, n) είναι συμπληρώματα υπηρεσιών ή διορθώσεις σε ήδη υπάρχοντα standards. Παραδόξως σε σχέση με το 802.11a, το 802.11b ήταν το πρώτο ευρέως αποδεκτό πρότυπο στην ασύρματη δικτύωση.
Παρακάτω ακολουθούν κάποιες πολύ βασικές πληροφορίες για τα περισσότερο δημοφιλή standards της οικογένειας 802.11.

I. 802.11legacy

Η πρώτη εκδοχή του IEEE 802.11 που ανακοινώθηκε το 1997 και καμιά φορά ονομάζεται και "802.1y" , καθορίζει δύο ρυθμούς μετάδοσης δεδομένων, αυτούς των 1 και 2 Mbps (Megabits per second). Αυτά μεταδίδονταν μέσω υπέρυθρων σημάτων σε συχνότητες των 2.4 GHz. Η χρησιμοποίηση υπέρυθρων (infrared) απορρίφθηκε στα πρότυπα που ακολούθησαν γιατί δε μπορούσε να

ανταγωνιστεί το ήδη πετυχημένο πρωτόκολλο IrDA και επίσης δεν είχε ουσιαστική εφαρμογή.

II. 802.11b

Το 802.11b ήταν αυτό που διαδέχτηκε το 802.11 legacy. Το 802.11b έχει εύρος 50 μέτρων περίπου. Αποτελείται από μια χαμηλής ισχύς (low gain) omni κεραία η οποία συνήθως χρησιμοποιείται στις 802.11b συσκευές. Αν μιλήσουμε για υψηλής ισχύος (high gain) εξωτερικές κεραίες τότε το πρωτόκολλο μπορεί να χρησιμοποιηθεί σημείο προς σημείο (point to point) για επικοινωνία εύρους μεγαλύτερου από 8 χιλιόμετρα. Το πρωτόκολλο 802.11b έχει ρυθμό μετάδοσης δεδομένων 11Mbps αλλά όμως σημαντικό ποσοστό του εύρους ζώνης (bandwidth) χρησιμοποιείται για προετοιμασία της επικοινωνίας (communications overhead). Στη πραγματικότητα ο ρυθμός μετάδοσης δεδομένων που επιτυγχάνεται είναι 5,5Mbps. Δραστικό ρόλο στην εξασθένηση του σήματος παίζουν το νερό το μεγάλος πάχος τοίχων, το μέταλλο και άλλα. Τέλος το 802.11b δουλεύει στο φάσμα συχνοτήτων των 2,4 GHz.

Διάφορες επεκτάσεις έχουν γίνει στο πρωτόκολλο 802.11b για να αυξηθεί ο ρυθμός μετάδοσης δεδομένων σε 22, 33, και 44 Mbit/s με αποτέλεσμα να μετονομασθεί σε 802.11b+. Αυτό το πρότυπο υποστηρίχθηκε από εταιρίες αλλά δεν υιοθετήθηκε από την IEEE.

III. 802.11a

Το 802.11a ανακοινώθηκε το 2001 αν και είχε επικυρωθεί ήδη από το 1999. Το πρωτόκολλο λειτουργεί σε συχνότητα των 5 GHz και με ρυθμό μετάδοσης δεδομένων στα 54 Mbit/s. Στη πραγματικότητα όμως ο ρυθμός μετάδοσης των δεδομένων που επιτυγχάνεται είναι περίπου 20 Mbit/s. Το πρωτόκολλο 802.11a δεν υιοθετήθηκε ευρέως όπως το 802.11b εξαιτίας προβλημάτων που δημιουργούσε η συχνότητα των 5 GHz όπως για παράδειγμα η κατανάλωση ενέργειας.

IV. 802.11g

Τον Ιούνιο του 2003 ένα άλλο πρότυπο επικυρώθηκε, το 802.11.g. Το πρωτόκολλο αυτό λειτουργεί επίσης σε συχνότητα 2,4 GHz αλλά ο ρυθμός μετάδοσης δεδομένων είναι στα 54 Mbit/s όπως το 802.11.a. Λόγω συχνότητας το 802.11.g είναι απόλυτα συμβατό με το 802.11.b, όμως κάποιες φορές η χρήση του 802.11.b σε ένα δίκτυο που χρησιμοποιεί το 802.11.g, κάνει το δίκτυο ποιο αργό.

Το πρωτόκολλο 802.11.g κέρδισε το καταναλωτικό κοινό από τον Ιανουάριο του 2003 πριν ακόμα εγκριθεί.

Αξίζει να αναφέρουμε ότι μία επέκταση του 802.11.g, η Super G έχει ολοκληρωθεί και υπόσχεται ταχύτητες μεγαλύτερες των 108 Mbit/s.

V. 802.11n

Τον Ιανουάριο του 2004 η IEEE ανακοίνωσε ότι θα δημιουργηθεί ένα νέο πρότυπο το οποίο θα αναφέρεται σε ασύρματα WAN. Η πραγματική του ταχύτητα θα είναι 100 Mbit/s περίπου δηλαδή 4-5 φορές μεγαλύτερη από τη πραγματική ταχύτητα του 802.11g και 50 φορές μεγαλύτερη από τη πραγματική ταχύτητα του 802.11b. Η διαδικασία προτυποποίησης αναμένεται να τελειώσει στα τέλη του 2006.

Το πρότυπο 802.11 θα αναλυθεί σε επόμενο κεφάλαιο. Εκεί θα δοθούν πληροφορίες σχετικά με την αρχιτεκτονική του, την ασφάλεια για διάφορα εμπορικά ζητήματα και γύρω από άλλα θέματα. Αυτό επειδή το 802.11 είναι το πιο δημοφιλές αυτή τη στιγμή σε ασύρματα LAN.
Παρακάτω παρουσιάζεται ένας πίνακας έτσι όπως έχει δοθεί από το IEEE και αναφέρει όλες τις επεκτάσεις του 802.11 καθώς και μια μικρή περιγραφή.

Πίνακας 1: **802.11**

- IEEE 802.11 - The original 2 Mbit/s, 2.4 GHz standard
- IEEE 802.11a - 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)
- IEEE 802.11b - Enhancements to 802.11 to support 5.5 and 11 Mbit/s (1999)
- IEEE 802.11d - New countries
- IEEE 802.11e- Enhancements: QoS, including packet bursting
- IEEE 802.11f - Inter-Access Point Protocol (IAPP)
- IEEE 802.11g - 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)
- IEEE 802.11h - 5 GHz spectrum, Dynamic Channel/Frequency Selection (DCS/DFS) and Transmit Power Control(TPC) for European compatibility
- IEEE 802.11i(ratified 24 June 2004) - Enhanced security
- IEEE 802.11j - Extensions for Japan
- IEEE 802.11n - Higher throughput improvements
- IEEE 802.11p - Adding wireless capabilities to mobile vehicles such as ambulances and passenger cars

2.2 ΤΟ ΠΡΟΤΥΠΟ IEEE 802.16

Το πρότυπο 802.16 ομοίως με το 802.11 αναπτύχθηκε από την ομάδα 16 της IEEE 802. Όπως αναφέραμε και προηγουμένως η IEEE 802 είναι η επιτροπή που ασχολείται με LAN, MAN (metropolitan area network) standards. Το 802.16 ειδικεύεται σε ευρυζωνική σημείου προς σημείο ασύρματη πρόσβαση (point-to-point broadband wireless access). Για να γίνουμε σε αυτό το σημείο περισσότερο κατανοητοί η τεχνολογία broadband wireless access (BWA), έχει ως στόχο να παρέχει ασύρματη πρόσβαση σε δίκτυα δεδομένων, με πολύ υψηλό ρυθμό μετάδοσης δεδομένων.
Το πρότυπο 802.16 είναι γνωστό και ως WiMAX που σημαίνει ***Worldwide Interoperability for Microwave Access.*** Παρόμοιες τεχνολογίες με το WiMAX είναι η BWA καθώς και η HIPERMAN η οποία είναι και η «Ευρωπαία» ανταγωνίστρια της.
Το WiMAX δεν συγκρούεται με το WiFi αλλά στη πραγματικότητα το συμπληρώνει. Το WiMAX είναι μια ασύρματη WAN (wide area network) τεχνολογία η οποία συνδέει τους σταθμούς βάσης (hotspots) του WiFi με το internet και έτσι αποτελεί μια επέκταση του. Να σημειώσουμε εδώ ότι το hotspot έχει την ίδια έννοια με το access point για το οποίο μιλήσαμε παραπάνω. Βασικό χαρακτηριστικό του 802.16 είναι ότι μπορεί να παρέχει ασύρματη σύνδεση σε ένα εύρος μεγαλύτερο από 50 χιλιόμετρα χωρίς να χρειάζεται άμεση οπτική επαφή με ένα σταθμό βάσης. Επίσης το πρότυπο 802.16 εξασφαλίζει ένα ρυθμό μετάδοσης δεδομένων ίσο με 54 Mbit/s.

<u>Προσδοκίες από το WiMAX:</u>
Το WiMAX στοχεύει στο να δώσει τη δυνατότητα σε εκατομμύρια ανθρώπους να έχουν πρόσβαση στο internet ασύρματα, γρήγορα αλλά και φθηνά. Για να καταλάβουμε καλύτερα ένας σταθμός βάσης WiMAX αναμένεται να παρέχει γρήγορες συνδέσεις στο internet σε σπίτια και εταιρείες σε ακτίνα μεγαλύτερη των 30 χιλιομέτρων. Ο σταθμοί βάσης αναμένεται να μετατρέψουν μια περιοχή σε WMAN (wireless metropolitan area) και έτσι να επιτρέπουν οποιαδήποτε ασύρματη κίνηση μέσα σε αυτήν όπως επικοινωνία laptops και PDA's. Εδώ όμως πρέπει να πούμε ότι πραγματικό

roaming σε ασύρματο ευρυζωνικό δίκτυο βασισμένο σε κελιά αναμένεται να εξυπηρετηθεί από ένα άλλο standard της IEEE το 802.20.

2.3 Bluetooth

Το Bluetooth είναι μια τεχνολογία η οποία καθιστά δυνατή τη μικρού εύρους (short range) ασύρματη σύνδεση μεταξύ desktop PC's και laptops, PDA's, κινητά τηλέφωνα, εκτυπωτές, πληκτρολόγια, ποντίκια καθώς και πολλά άλλα. Η συχνότητα του Bluetooth είναι 2,4GHz καθώς το εύρος ζώνης είναι στο 1 MHz. Τέλος η ταχύτητα μεταφοράς δεδομένων είναι μέχρι 1Mbps ενώ είναι δυνατή και η ταυτόχρονη μεταφορά ήχου. Μια χαρακτηριστική εικόνα που δείχνει το εύρος των εφαρμογών του Bluetooth φαίνεται παρακάτω.

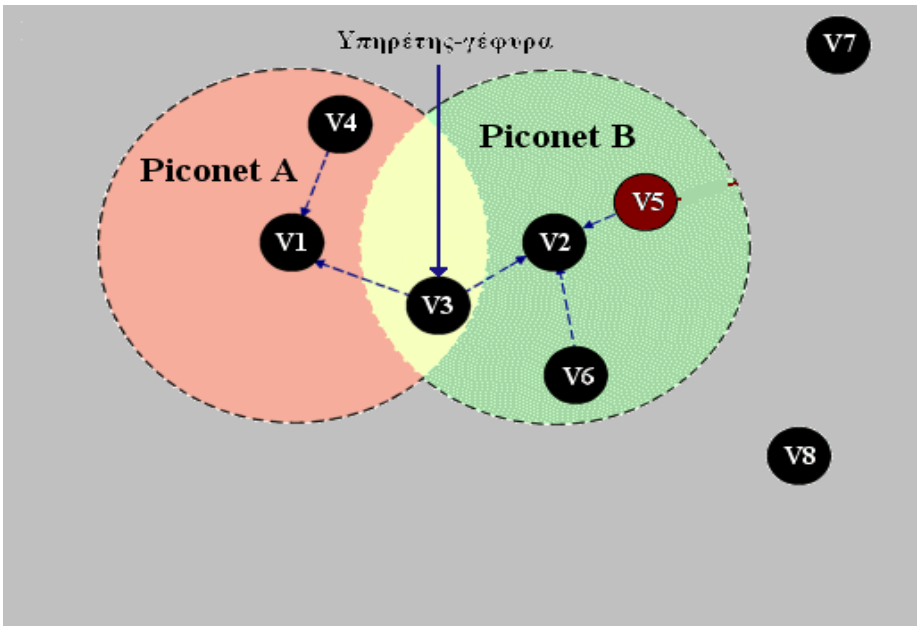
Σχήμα 1: Bluetooth applications

Ιστορικά στοιχεία.

Το 1994 η εταιρεία Ericsson έδειξε ενδιαφέρον για τη σύνδεση των κινητών τηλεφώνων σε άλλες συσκευές χωρίς καλώδια. Έτσι μαζί με άλλες εταιρίες (IBM Intel, Nokia, Toshiba) σχημάτισε τη SIG (Special Interest Group) που σημαίνει ουσιαστικά κοινοπραξία, για την ανάπτυξη ενός

προτύπου ασύρματης διασύνδεσης υπολογιστικών και επικοινωνιακών συσκευών και βοηθημάτων με χρήση ραδιοκυματικών πομποδεκτών μικρής εμβέλειας , χαμηλής ισχύος και χαμηλού κόστους. Το έργο ονομάστηκε **Bluetooth,** από τον Harald Blaatand το 2^{ο} (ή **Bluetooth) (940-**981), ένα βασιλιά των Βίκινγκ που ενοποίησε (κατέκτησε) τη Δανία και τη Νορβηγία χωρίς να χρησιμοποιήσει καλώδια.
Αν και η αρχική ιδέα ήταν να απαλλαγούμε από τα καλώδια ανάμεσα στις συσκευές, το έργο αυτό άρχισε σύντομα να εισβάλλει και στο χώρο των ασύρματων LAN. Αν και αυτή η κίνηση κάνει το πρότυπο ποιο χρήσιμο δημιουργεί κάποιο ανταγωνισμό με το πρότυπο 802.11. Για να χειροτερέψουν τα πράγματα τα δύο συστήματα παρεμβάλλονται ηλεκτρικά μεταξύ τους. Εδώ πρέπει να σημειωθεί ότι και η Hewlett-**Packard** παρουσίασε πριν από μερικά χρόνια ένα υπέρυθρο δίκτυο για σύνδεση περιφερειακών υπολογιστών χωρίς καλώδια, αλλά δε γνώρισε επιτυχία.
Η επιτροπή του **Bluetooth** δε πτωήθηκε από τις εξελίξεις και τον Ιούλιο του 1999 εξέδωσε μια προδιαγραφή 1500 σελίδων για την έκδοση 1.0 του συστήματος. Λίγο αργότερα η ομάδα προτύπων του IEEE που δούλευε πάνω σε WLAN, 802.15 υιοθέτησε ως βάση το έγγραφο του **Bluetooth** και άρχισε να το τροποποιεί. Αν και μπορεί να φαίνεται περίεργη η τυποποίηση ενός συστήματος που έχει ήδη πολύ λεπτομερείς προδιαγραφές και δεν έχει ασύμβατες υλοποιήσεις που να χρειάζεται να εναρμονιστούν, η ιστορία δείχνει ότι η ύπαρξη ενός ανοικτού προτύπου το οποίο διαχειρίζεται μια ουδέτερη αρχή όπως η IEEE συχνά προάγει τη χρήση μιας τεχνολογίας. Σήμερα αν και οι εκδόσεις της επιτροπής του **Bluetooth** και του IEEE δεν είναι πανομοιότυπες, υπάρχει ελπίδα ότι θα συγκλίνουν σε ένα μοναδικό πρότυπο.

Αρχιτεκτονική **B**luetooth.
Συνεχίζοντας θα αναφέρουμε κάποια βασικά σημεία της αρχιτεκτονικής του **B**luetooth. Η βασική μονάδα ενός συστήματος **B**luetooth είναι ένα μικροσκοπικό δίκτυο το ***piconet***. **Το piconet** αποτελείται από ένα κόμβο master και μέχρι επτά ενεργούς συνεργάτες (slaves), μέσα σε μια απόσταση 10 μέτρων. Πολλαπλά piconets μπορούν να συνυπάρξουν στο ίδιο μεγάλο δωμάτιο, ενώ μπορεί να είναι συνδεδεμένα μέσω ενός κόμβου γέφυρας. Ένα τέτοιο διασυνδεδεμένο σύνολο φαίνεται στο παρακάτω σχήμα και ονομάζεται διάσπαρτο δίκτυο (scatternet). Να πούμε ότι στο σχήμα 2 έχουμε δύο piconets το A και το B. Το piconet B αποτελείτε από έναν master v2 και τα v3, v5, v6 είναι slaves. Το v3 που είναι η γέφυρα υπηρέτης χρησιμοποιείται σαν router για τα δύο piconets. Τέλος τα v7, v8 είναι εκτός του εύρους του δικτύου.



Σχήμα 2: Scatternet

Εκτός από τους 7 ενεργούς κόμβους υπηρέτη του piconet μπορούν να υπάρχουν μέχρι και 255 σταθμευμένοι (parked) κόμβοι στο δίκτυο. Οι κόμβοι αυτοί είναι συσκευές τις οποίες ο master έχει φέρει σε κατάσταση χαμηλής ισχύος, έτσι ώστε να μειώσει την κατανάλωση των μπαταριών τους. Στην parked (η οποία συμβολίζεται στο σχήμα με καφέ χρώμα) κατάσταση η συσκευή δε μπορεί να κάνει τίποτε άλλο από το να αποκρίνεται σε ένα σήμα ενεργοποίησης ή σε ένα σήμα φάρου από τον master.
Η αιτία για τη σχεδίαση αρχιτεκτονικής master/slave είναι ότι οι σχεδιαστές ήθελαν να διευκολύνουν την υλοποίηση ολοκληρωμένων κυκλωμάτων Bluetooth με κόστος μικρότερο από 5$. Να συμπληρώσουμε επίσης ότι το piconet είναι ουσιαστικά ένα συγκεντρωτικό σύστημα TDM, με τον master να ελέγχει το ρολόι και να καθορίζει ποια συσκευή θα επικοινωνήσει σε ποια χρονική υποδοχή.

Εφαρμογές του Bluetooth.

Τα περισσότερα πρωτόκολλα δικτύου απλώς παρέχουν κανάλια ανάμεσα σε οντότητες που επικοινωνούν αφήνοντας τους σχεδιαστές των εφαρμογών να αποφασίσουν για ποιο σκοπό θέλουν να χρησιμοποιήσουν τα κανάλια αυτά. Αντίθετα όμως, οι προδιαγραφές της έκδοσης 1.1 του Bluetooth κατονομάζουν 13 συγκεκριμένες εφαρμογές οι οποίες θα υποστηρίζονται και παρέχουν διαφορετικές στοίβες πρωτοκόλλων για την καθεμία. Οι 13 αυτές εφαρμογές ονομάζονται προφίλ (profiles). Ο πίνακας 2 είναι profiles

table όπως ακριβώς το παρουσιάζει ο Tanenbaum στο βιβλίο του ***Computer Newtworks 4th Edition.***

Πίνακας 2: Bluetooth profiles

Name	**Description**
Generic access *	Procedures for link management
Service discovery *	Protocol for discovering offered service
Serial port	Replacement for a serial cable
Generic object exchange	Defines client-server relationships for object movement
LAN access	Protocol between a mobile computer and a fixed LAN
Dial-Up networking	Allows a mobile fax machine to talk to a mobile
Fax	Allows a mobile fax machine to talk to a mobile
Cordless telephony	Connects a handset and its local base station
Intercom	Digital walkie talkie
Headset	Allows hands-free voice communication
Object push	Provides a way to exchange simple objects
File transfer	Provides a more general file transfer facility
Synchronization	Permits a PDA to synchronize with another computer

Το προφίλ generic access δεν είναι πια πραγματική εφαρμογή, αλλά η βάση πάνω στην οποία χτίζονται οι πραγματικές εφαρμογές. Η βασική του δουλειά είναι να παρέχει μια μέθοδο εγκαθύδρισης και διατήρησης ασφαλών καναλιών ανάμεσα στον master και τους υπηρέτες του. Το προφίλ της Serial port εξομοιώνει τη παρουσία μιας σειριακής γραμμής ιδιαίτερα χρήσιμης για παλιές εφαρμογές. Συνεχίζοντας, το προφίλ Generic object exchange προδιαγράφει μια σχέση client-server για τη μεταφορά δεδομένων, ενώ τα τρία επόμενα προφίλ (LAN access, Dial-Up Networking, FAX) χρησιμοποιούνται για τη δικτύωση. Τέλος τα προφίλ (Cordless Telephony, Intercom, Headset) χρησιμοποιούνται για τηλεφωνία, ενώ τα (Object Push, File Transfer, Synchronization) για ανταλλαγή αντικειμένων ανάμεσα σε δυο ασύρματες συσκευές.

Ασφάλεια στο Bluetooth.
Το Bluetooth χρησιμοποιεί την **authentication** λογισμικού για να δημιουργήσει μια βάση δεδομένων άλλων "**trusted**" συσκευών. Ο χρήστης θα ενεργοποιήσει χαρακτηριστικά μια διαδικασία εγγραφής και στις δύο συσκευές Bluetooth και θα εισαγάγει έναν μικρό αριθμό **PINS** σε κάθε μια πρίν να μπορέσουν να επικοινωνήσουν οι δύο συσκευές Bluetooth.
Η κρυπτογράφηση, συμπεριλαμβανόμενης επίσης της εναέριας διεπαφής, μπορεί να παρέχει προστασία ενάντια στις υποκλοπές με τη χρησιμοποίηση ενός κλειδιού που προέρχεται από διαδικασίες επικύρωσης.

2.4 ΑΛΛΑ ΠΡΟΤΥΠΑ

Πέρα από τα πρότυπα που αναφέραμε παραπάνω (τα οποία είναι και ιδιαίτερα δημοφιλή) υπάρχουν και πολλά άλλα πρότυπα στα ασύρματα δίκτυα. Αξίζει να αναφέρουμε το **HIPERLAN,** το **HomeRF,** το **UWB (Ultra-wideband**) όπως και για την κινητή τηλεφωνία το **GSM,WAP** κ.τ.λ.

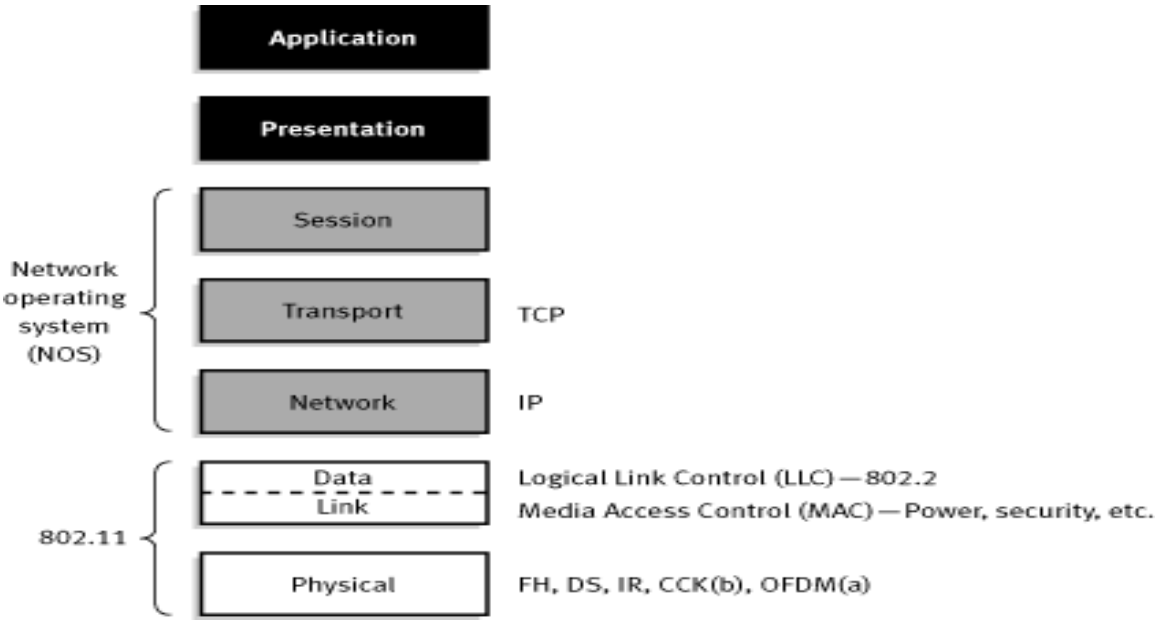
3 ΤΟ ΠΡΟΤΥΠΟ 802.11

Σχήμα 1: IEEE's 802.11 certification

Τον Ιούνιο του 1997, το Ινστιτούτο των Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών – Institute of Electrical and Electronic Engineers (IEEE) κατέληξε στο αρχικό πρότυπο για ασύρματα δίκτυα WLANs, IEEE 802.11. Αυτό το πρότυπο προδιάγραφε ως συχνότητα λειτουργίας τα 2,4 GHz, με ρυθμούς μετάδοσης δεδομένων 1 και 2 Mbps.
Αποτελεί το πρώτο πρότυπο για ασύρματη δικτύωση και ακολουθείται από τα περισσότερα ασύρματα δίκτυα μέχρι και σήμερα.

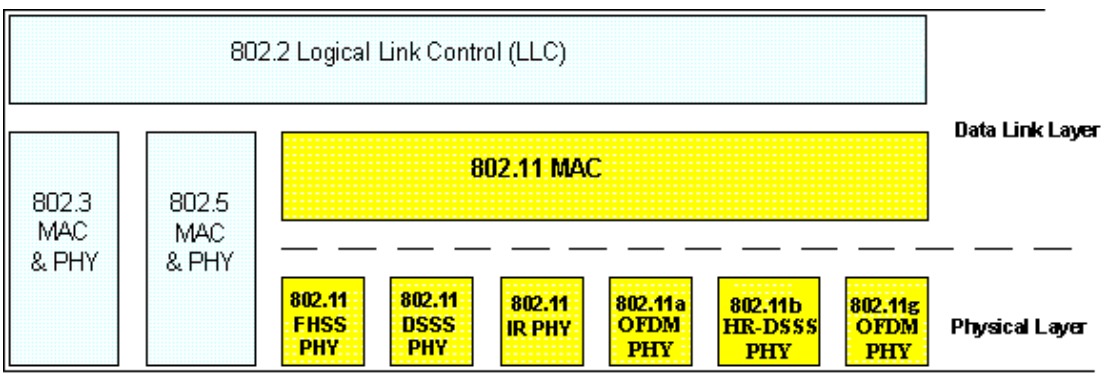
3.1 ΣΤΟΙΒΑ ΠΡΩΤΟΚΟΛΛΩΝ ΤΟΥ 802.11

Όπως όλα τα 802.x πρότυπα, έτσι και το 802.11 επικεντρώνεται στα δύο χαμηλότερα στρώματα του μοντέλου OSI (Open System Interconnection), δηλαδή στο φυσικό στρώμα (Physical Layer-PHY) και στο υπόστρωμα MAC (Medium Access Control-Ελέγχου προσπέλασης Μέσων) του στρώματος διασύνδεσης δεδομένων (Data Link Layer) όπως φαίνεται στο σχήμα 2.
Το υπόστρωμα MAC ορίζει πώς γίνεται η εκχώρηση του καναλιού, δηλαδή ποιος θα μεταδώσει στη συνέχεια. Το υπόστρωμα LLC(Logical Link Control-Έλεγχος Λογικού Συνδέσμου) του στρώματος Data Link βρίσκεται πάνω από το υπόστρωμα MAC, έχει υλοποιηθεί ως IEEE 802.2 και δουλειά του είναι να κρύβει τις διαφορές ανάμεσα στις διαφορετικές παραλλαγές του 802, έτσι ώστε να κάνει τις παραλλαγές αυτές "αόρατες" όσον αφορά το επίπεδο δικτύου.



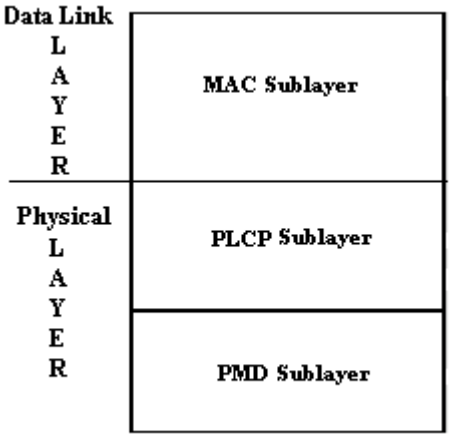
Σχήμα 2: Μοντέλο Αναφοράς OSI

Το πρότυπο του 1997 καθορίζει τρεις επιτρεπόμενες τεχνικές μετάδοσης για το φυσικό στρώμα (PHY). Η μέθοδος των υπέρυθρων χρησιμοποιεί σχεδόν την ίδια τεχνολογία με τα τηλεχειριστήρια των τηλεοράσεων. Οι άλλες δύο μέθοδοι χρησιμοποιούν ραδιοκύματα μικρής εμβέλειας χρησιμοποιώντας τεχνικές που ονομάζονται FHSS (Frequency Hopping Spread Spectrum) και DSSS (Direct Sequence Spread Spectrum). Και οι δύο χρησιμοποιούν ένα τμήμα του φάσματος στο οποίο δεν απαιτείται ειδική άδεια (τη ζώνη ISM στα 2,4 GHz). Το 1999 παρουσιάστηκαν δύο νέες τεχνικές για επίτευξη υψηλότερου εύρους ζώνης. Οι τεχνικές αυτές ονομάζονται OFDM (Orthogonal Frequency Division Multiplexing) και HR-DSSS (High Rate DSSS) και λειτουργούν μέχρι τα 54 Mbps και τα 11 Mbps αντίστοιχα. Το 2001 παρουσιάστηκε και μια δεύτερη τεχνική διαμόρφωσης OFDM, αλλά σε διαφορετική ζώνη συχνοτήτων από την πρώτη. Στο παρακάτω σχήμα φαίνεται η διαστρωμάτωση του προτύπου 802.11.



Σχήμα 3: Διαστρωμάτωση του προτύπου 802.11

Η φιλοσοφία που ακολουθεί το πρότυπο 802.11 είναι η ύπαρξη ενός μόνο MAC που όμως υποστηρίζει περισσότερα του ενός φυσικά στρώματα. Κάθε φυσικό στρώμα όπως φαίνεται στο σχήμα 4, χωρίζεται σε δύο υποστρώματα.
Το υπόστρωμα PLCP (Physical Layer Convergence Procedure) χρησιμεύει στην προσαρμογή των διαφόρων φυσικών στρωμάτων στο κοινό MAC. Το υπόστρωμα PMD (Physical Medium Dependent) περιέχει όλες τις λειτουργίες που απαιτούνται για τη μετάδοση της πληροφορίας από το εκάστοτε φυσικό στρώμα.

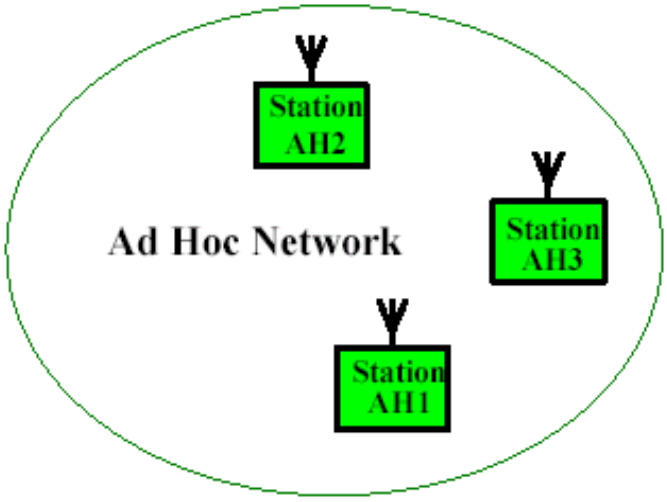


Σχήμα 4: Φυσικό Στρώμα προτύπου 802.11

3.2 ΤΟΠΟΛΟΓΙΑ

Υπάρχουν δύο βασικές τοπολογίες, βάσει των οποίων ορίζονται δύο είδη ασύρματων δικτύων. Πρόκειται για τα ανεξάρτητα δίκτυα (independent networks) και τα δίκτυα υποδομής (infrastructure networks).

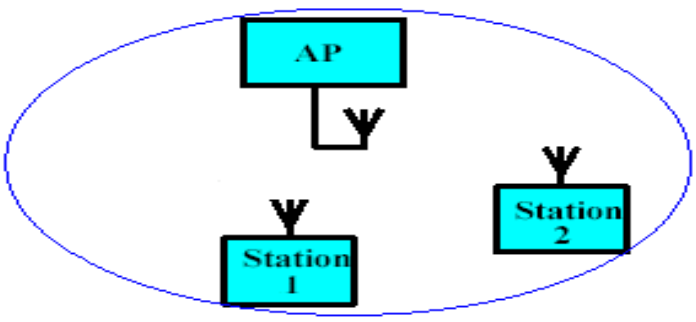
Ανεξάρτητα Δίκτυα
Το BSS (Basic Service Set - κυψέλη) αποτελείται από δύο ή περισσότερους ασύρματους κόμβους ή σταθμούς (STAs) και κάθε σταθμός επικοινωνεί απευθείας με όλους τους υπόλοιπους εφόσον βρίσκεται στην περιοχή ραδιοκάλυψής τους. Το BSS σε αυτή την περίπτωση αναφέρεται και ως IBSS (Independent Basic Service Set) ή ad-hoc BSS ή ad-hoc δίκτυο και είναι συνήθως προσωρινό, δηλαδή δημιουργείται για κάποιο σκοπό και στη συνέχεια διαλύεται. Πρόκειται για τον απλούστερο τύπο ασύρματου δικτύου.



Σχήμα 5: Τοπολογία IBSS

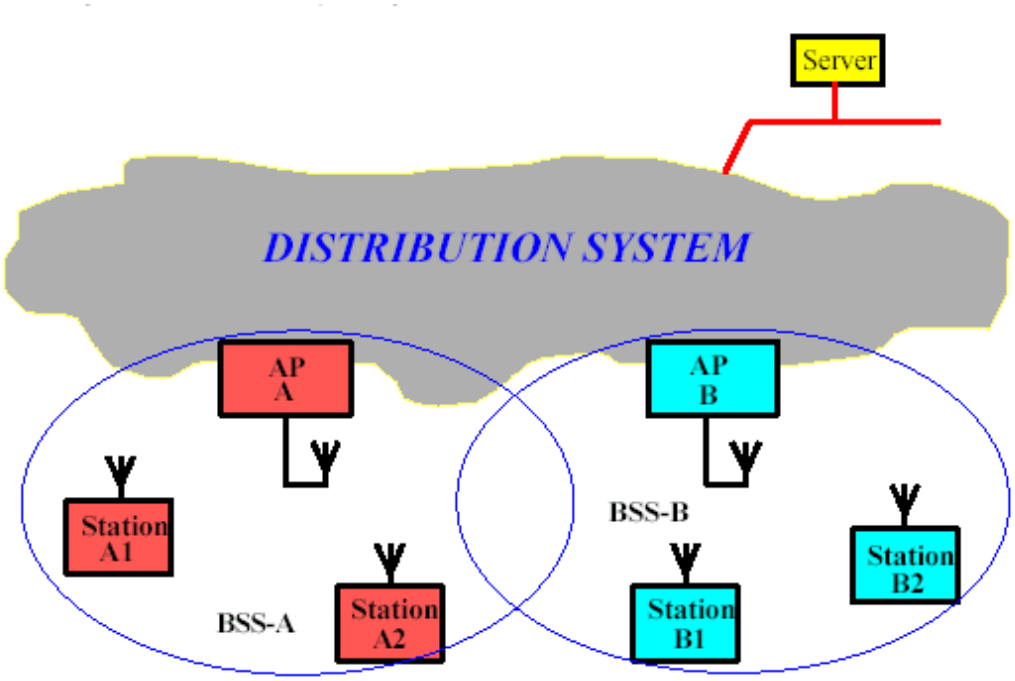
Δίκτυα Υποδομής

Το BSS περιλαμβάνει ένα AP (Access Point-σταθμός βάσης). Το AP είναι υπεύθυνο για τη σύνδεση του BSS με το ενσύρματο δίκτυο, την ανταλλαγή πλαισίων μεταξύ των σταθμών και για τον κεντρικό έλεγχο της λειτουργίας του BSS. Όταν ένας σταθμός θέλει να στείλει ένα πλαίσιο σε έναν άλλο σταθμό, δεν του το στέλνει απευθείας, αλλά το πλαίσιο αποστέλλεται πρώτα στο AP και αυτό με τη σειρά του το στέλνει στον τελικό προορισμό. Η BSA (Basic Service Area) είναι η περιοχή ραδιοκάλυψης του AP. Δηλαδή οι σταθμοί πρέπει να βρίσκονται στην περιοχή ραδιοκάλυψης του AP για να επικοινωνήσουν μεταξύ τους, χωρίς να παίζει ρόλο η μεταξύ τους απόσταση όπως στην περίπτωση του IBSS. Για να συμμετέχει ένας σταθμός στο BSS θα πρέπει να ακολουθήσει τη διαδικασία association (σύνδεσης) με τον AP. Η διαδικασία αυτή ξεκινάει με πρωτοβουλία του σταθμού και είναι απόφαση του AP αν ο σταθμός θα γίνει δεκτός στο BSS.



Σχήμα 6: Τοπολογία infrastructure BSS

Ένας αριθμός από BSSs μπορούν να συνδεθούν και να αποτελέσουν ένα ESS (Extended Service Set). Στο ESS τα APs των BSSs συνδέονται μέσω ενός ενσύρματου δικτύου κορμού, που ονομάζεται σύστημα διανομής (Distribution System-DS). Με αυτόν τον τρόπο είναι εφικτή η επικοινωνία μεταξύ σταθμών που ανήκουν σε διαφορετικά BSSs αλλά στο ίδιο ESS. Σε αυτή την περίπτωση πρέπει τα APs να επικοινωνούν στο στρώμα ζεύξης δεδομένων μέσω του δικτύου κορμού, επιτελώντας τη λειτουργία της γέφυρας για τους σταθμούς διαφορετικών BSSs. Το ESS τελειώνει όταν παρεμβληθεί μεταξύ των APs οντότητα δικτύου που να λειτουργεί σε υψηλότερο στρώμα, όπως είναι ο δρομολογητής (router).



Σχήμα 7: Τοπολογία infrastructure δύο BSS

Το 802.11 προσφέρει κινητικότητα σε ένα ESS, αρκεί το δίκτυο κορμού να είναι ένα απλό LAN(Local Area Network) ή και VLAN (Virtual LAN). Σε κάθε άλλη περίπτωση η σύνδεση θα χαθεί εκτός και αν χρησιμοποιείται κάποια άλλη τεχνολογία όπως το Mobile IP.

3.3 ΥΠΗΡΕΣΙΕΣ ΑΣΥΡΜΑΤΟΥ ΔΙΚΤΥΟΥ 802.11

Το πρότυπο 802.11 καθορίζει ότι κάθε ασύρματο LAN που ακολουθεί το πρότυπο πρέπει να παρέχει εννέα υπηρεσίες. Οι υπηρεσίες αυτές διαιρούνται σε δύο κατηγορίες: πέντε

υπηρεσίες διανομής που σχετίζονται με τη διαχείριση των μελών ενός BSS και την αλληλεπίδραση με σταθμούς εκτός BSS, και τέσσερις υπηρεσίες σταθμών που σχετίζονται με τις δραστηριότητες μέσα σε ένα BSS.

Υπηρεσίες διανομής

- Association (Συσχέτιση): Υπηρεσία συσχέτισης ενός σταθμού με το AP, προκειμένου να είναι σε θέση να δεχθεί και να στείλει πλαίσια μέσω του ασύρματου δικτύου. Τυπικά η υπηρεσία αυτή χρησιμοποιείται μόλις ένας σταθμός μετακινηθεί εντός της BSA του AP, οπότε και του ανακοινώνει την ταυτότητα και τις δυνατότητές του. Το AP μπορεί να δεχθεί ή και να απορρίψει το σταθμό. Αν τον αποδεχθεί θα πρέπει στη συνέχεια να γίνει authentication.
- Disassociation (Αποσυσχέτιση): Υπηρεσία αφαίρεσης ενός σταθμού ή του AP από το δίκτυο. Ένα AP μπορεί να την χρησιμοποιεί πριν απενεργοποιηθεί για λόγους συντήρησης. Το MAC του 802.11 μπορεί να χειριστεί και σταθμούς που εγκαταλείπουν το δίκτυο χωρίς να έχουν κάνει πρώτα χρήση της υπηρεσίας.
- Reassociation (Επανασυσχέτιση): Με τη συγκεκριμένη υπηρεσία ένας σταθμός μπορεί να αλλάξει AP. Είναι πολύ χρήσιμη για κινητούς σταθμούς που μετακινούνται από ένα BSS σε ένα άλλο.
- Distribution (Διανομή): Η υπηρεσία αυτή προσδιορίζει πώς θα δρομολογούνται τα πλαίσια που στέλνονται στο AP. Αν ο σταθμός-παραλήπτης βρίσκεται μέσα στο BSS τότε το πλαίσιο μπορεί να σταλθεί άμεσα από το AP, διαφορετικά θα πρέπει να σταλεί στο DS και από εκεί στο AP που σχετίζεται με τον παραλήπτη.
- Integration (Ενοποίηση): Υπηρεσία που παρέχεται από το DS. Όταν ένα πλαίσιο πρέπει να σταλεί μέσω ενός δικτύου που δεν είναι της μορφής 802.11 και χρησιμοποιεί διαφορετική μέθοδο διευθυνσιοδότησης ή μορφή πλαισίων, η υπηρεσία αυτή διαχειρίζεται τη μετατροπή από τη μορφή του 802.11 στη μορφή που απαιτείται από το δίκτυο προορισμού.

Υπηρεσίες σταθμών

- Authentication (Πιστοποίηση Ταυτότητας): Επειδή οι ασύρματες μεταδόσεις είναι εύκολο να σταλούν ή να ληφθούν από μη εξουσιοδοτημένους σταθμούς, ο σταθμός θα πρέπει να πιστοποιήσει την ταυτότητα του πριν του επιτραπεί να στείλει δεδομένα. Μόλις γίνει το association, το AP στέλνει στον σταθμό ένα ειδικό πλαίσιο "πρόσκλησης" για να δει αν ο σταθμός γνωρίζει το μυστικό κλειδί (συνθηματικό) που του έχει εκχωρηθεί. Ο σταθμός αποδεικνύει ότι γνωρίζει

το μυστικό κλειδί κρυπτογραφώντας το πλαίσιο πρόσκλησης και στέλνοντάς το πίσω στο AP. Αν το αποτέλεσμα είναι ορθό, ο σταθμός εγγράφεται πλήρως στην κυψέλη.

- Deauthentication (Ακύρωση πιστοποίησης ταυτότητας): Τερματισμός μίας ισχύουσας κατάστασης authentication. Μετά την ακύρωση της πιστοποίησης, ο σταθμός δεν μπορεί πια να χρησιμοποιήσει το δίκτυο.
- Privacy (Προστασία Απορρήτου): Για να διατηρούνται εμπιστευτικές οι πληροφορίες που στέλνονται μέσω ενός ασύρματου LAN, θα πρέπει να κρυπτογραφούνται. Από το 802.11 έχει ορισθεί μία προαιρετική υπηρεσία κρυπτογράφησης των δεδομένων που ονομάζεται WEP (Wired Equivalent Privacy). Το WEP δεν προσφέρει σε καμία περίπτωση ασφαλή μεταφορά δεδομένων και ήδη μελετάται η αντικατάστασή του.
- MSDU (MAC Service Data Unit) *Delivery* (Παράδοση Πλαισίων MAC): Η υπηρεσία αυτή ασχολείται με την παράδοση πλαισίων MAC στον τελικό προορισμό τους.

3.4 ΦΥΣΙΚΟ ΣΤΡΩΜΑ ΤΟΥ 802.11

Στο φυσικό στρώμα προδιαγράφονται τρεις τεχνικές διαμόρφωσης:

- **Infrared (Υπέρυθρες Ακτίνες)** σε μήκη κύματος μεταξύ 850 και 950 nm με ρυθμούς μετάδοσης 1 και 2 Mbps.
- **Frequency Hopping Spread Spectrum-FHSS (Εξάπλωση Φάσματος με Συνεχή Αλλαγή Συχνότητας)** στην ISM μπάντα των 2,4 GHz με ρυθμούς μετάδοσης 1 και 2 Mbps.
- **Direct Sequence Spread Spectrum-DSSS (Εξάπλωση Φάσματος Άμεσης Ακολουθίας)** στην ISM μπάντα των 2,4 GHz με ρυθμούς μετάδοσης 1 και 2 Mbps.

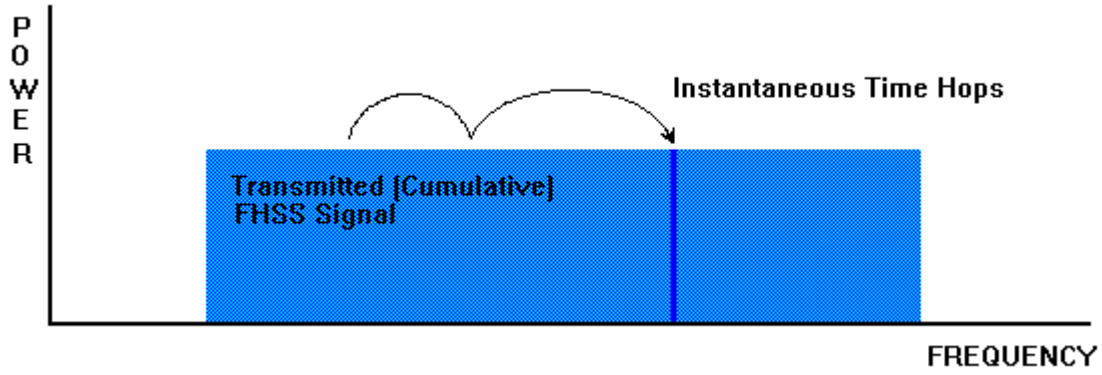
Infrared

Η τεχνική των υπέρυθρων ακτινών δεν χρησιμοποιείται ιδιαίτερα λόγω του χαμηλού εύρους ζώνης και του γεγονότος ότι το φως του ήλιου εξαφανίζει τα υπέρυθρα σήματα.
Η υπέρυθρη επιλογή χρησιμοποιεί διάχυτη (δηλαδή όχι σε ευθεία γραμμή) μετάδοση στα 0,85 ή στα 0,95 micron. Στα 1 Mbps χρησιμοποιείται μία μέθοδος κωδικοποίησης στην οποία κάθε ομάδα των 4 bit κωδικοποιείται ως μία

κωδικολέξη των 16 **bit** που περιέχει δεκαπέντε 0 και ένα 1, χρησιμοποιώντας τον **Gray code** (κώδικα **Gray**) ο οποίος έχει την ιδιότητα ότι ένα μικρό σφάλμα συγχρονισμού οδηγεί σε ένα σφάλμα του ενός **bit** στην έξοδο. Στα 2 **Mbps** η κωδικοποίηση παίρνει 2 **bit** και παράγει μία κωδικολέξη των **4 bit** όπου πάλι υπάρχει ένα μόνο 1, δηλαδή δίνει μία από τις κωδικολέξεις 0001, 0010, 0100, 1000. Τα υπέρυθρα σήματα δεν μπορούν να διαπεράσουν τους τοίχους, έτσι οι κυψέλες (**BSS**) που βρίσκονται σε ξεχωριστά δωμάτια είναι καλά απομονωμένες η μία από την άλλη.

Frequency Hopping Spread Spectrum-FHSS

Πρόκειται για τεχνική εξάπλωσης φάσματος. Η τεχνική **FHSS** βασίζεται στην ιδέα της αλλαγής της φέρουσας ενός σήματος μέσα σε ένα μεγάλο εύρος συχνοτήτων και σύμφωνα με μία συγκεκριμένη ψευδοτυχαία ακολουθία (**hopping pattern**). Χρησιμοποιείται μία γεννήτρια ψευδοτυχαίων (**PN**) αριθμών για την παραγωγή της ακολουθίας συχνοτήτων στις οποίες μεταβαίνουν διαδοχικά οι σταθμοί, όπως φαίνεται στο σχήμα 8.



Σχήμα **8:** Φάσμα FHSS

Όσο όλοι οι σταθμοί χρησιμοποιούν το ίδιο **seed** στη γεννήτρια ψευδοτυχαίων αριθμών και παραμένουν χρονικά συγχρονισμένοι, θα εκτελούν ταυτόχρονα τη μετάβαση στις ίδιες συχνότητες. Η χρονική διάρκεια στην οποία μένουμε στην ίδια συχνότητα, δηλαδή το **dwell time** (χρόνος παραμονής) είναι ρυθμιζόμενη παράμετρος, αλλά θα πρέπει να είναι μικρότερη από 400 **msec**. Η τυχαία ακολουθία της **FHSS** παρέχει κάποια περιορισμένη ασφάλεια, αφού ένας εισβολέας που δεν γνωρίζει την ακολουθία συχνοτήτων ή το χρόνο παραμονής δεν μπορεί να υποκλέψει τις μεταδόσεις.

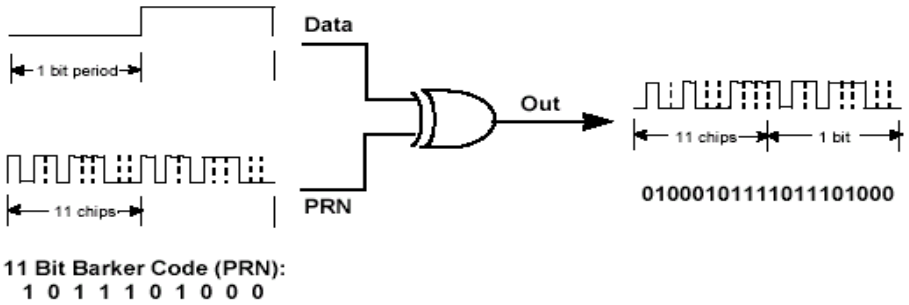
Σε μεγαλύτερες αποστάσεις μπορεί να δημιουργήσει πρόβλημα η εξασθένιση πολλαπλών διαδρομών, η τεχνική FHSS όμως παρέχει αρκετή αντοχή σε αυτό το φαινόμενο.
Ένα άλλο πλεονέκτημα είναι ότι είναι σχετικά ανθεκτική στις ραδιοκυματικές παρεμβολές, γεγονός που την κάνει δημοφιλή για συνδέσεις από κτίριο σε κτίριο.
Πλεονεκτήματα έναντι της εναλλακτικής DSSS είναι τα απλούστερα και φθηνότερα ηλεκτρονικά για την υλοποίηση των ανάλογων συσκευών, η χαμηλότερη κατανάλωση ενέργειας και η δυνατότητα συνύπαρξης πολλών τέτοιων δικτύων στην ίδια περιοχή χωρίς να επηρεάζεται η συνολική διέλευση.
Βασικό πλεονέκτημα είναι η δυνατότητα συνύπαρξης διαφορετικών ασυρμάτων δικτύων, αρκεί τα hopping patterns τους να είναι διαφορετικά, δηλαδή σε κάθε χρονική στιγμή κάθε σύστημα να μεταδίδει σε διαφορετική φέρουσα. Τότε τα hopping patterns ονομάζονται 'ορθογώνια' και η συνολική διέλευση μεγιστοποιείται.
Το κύριο μειονέκτημα της τεχνικής FHSS είναι το χαμηλό εύρος ζώνης της. Η FHSS χρησιμοποιεί κανάλια, το καθένα με εύρος 1 MHz, ξεκινώντας από το κάτω όριο της ζώνης ISM στα 2,4 GHz. Ο Πίνακας 3 παρουσιάζει τα κανάλια και τα hopping patterns που χρησιμοποιούνται σε διάφορες γεωγραφικές περιοχές.

Πίνακας 3: Διαθέσιμα κανάλια ανά περιοχή για το φυσικό στρώμα.

Περιοχή / Υπεύθυνη Αρχή	**Επιτρεπόμενα Κανάλια**	**Αριθμός hopping patterns / ομάδα**
ΗΠΑ / FCC – Καναδάς / IC	2 έως 79 (2,402 – 2,479 GHz)	26
Ευρώπη (εκτός Γαλλίας & Ισπανίας) / ETSI	2 έως 79 (2,402 – 2,479 GHz)	26
Γαλλία	48 έως 82 (2,448 – 2,482 GHz)	27
Ισπανία	47 έως 73 (2,447 – 2,473 GHz)	35
Ιαπωνία / MKK	73 έως 95 (2,473 – 2,495 GHz)	13

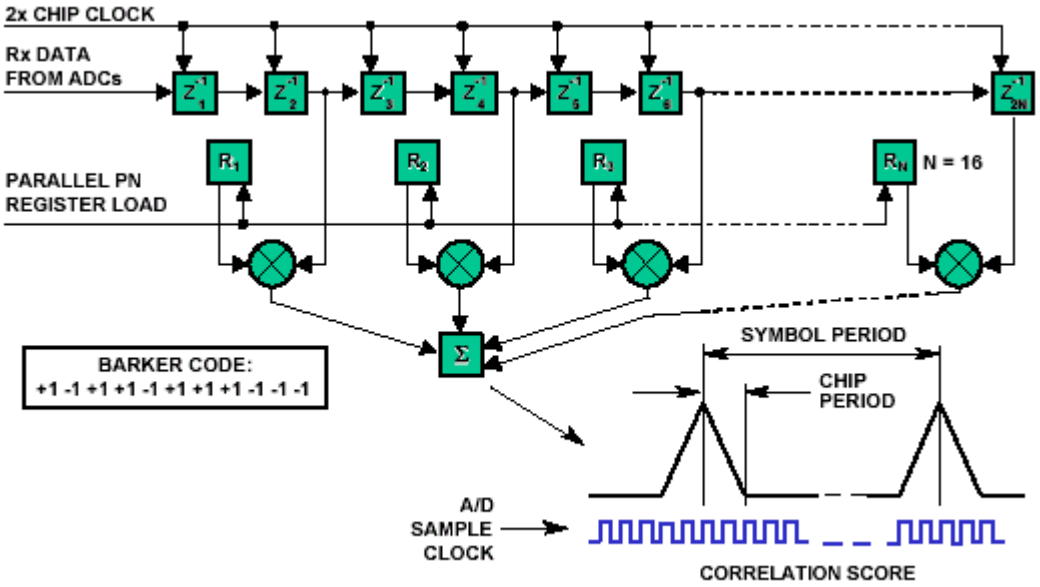
Direct Sequence Spread Spectrum-DSSS
Πρόκειται για τεχνική εξάπλωσης φάσματος. Η DSSS τεχνική είναι η πιο επιτυχημένη που έχει χρησιμοποιηθεί σε συνδυασμό με τα ασύρματα δίκτυα. Σε σχέση με την FHSS

τεχνική μετάδοσης απαιτεί περισσότερη ενέργεια για να επιτύχει παρόμοια διέλευση, όμως το μεγάλο πλεονέκτημά της είναι ότι μπορεί εύκολα να αναβαθμιστεί για την επίτευξη υψηλότερων ρυθμών μετάδοσης.
Η **DSSS** περιορίζεται και αυτή σε 1 ή 2 Mbps. Η τεχνική αυτή αντικαθιστά κάθε **bit** πληροφορίας με μία σειρά από **bits** που ονομάζεται **spreading code** (κώδικας εξάπλωσης).
Κάθε **bit** μεταδίδεται ως 11 θραύσματα (**chips**), χρησιμοποιώντας την ονομαζόμενη ακολουθία **Barker (Barker sequence**) η οποία είναι ο **spreading code**. Για την ακρίβεια, κάθε **bit** πληροφορίας συνδέεται μέσω μίας **XOR** με μία ψευδοτυχαία αριθμητική (**Pseudo-random Numerical** ή **PN**) ακολουθία όπως δείχνει το σχήμα 9. Το αποτέλεσμα είναι ένα ψηφιακό φέρον σήμα υψηλής ταχύτητας το οποίο διαμορφώνεται σε ένα κατά τη φάση φέρον σήμα χρησιμοποιώντας **Differential Phase Shift Keying-DPSK** (διαφορική μεταλλαγή ολίσθησης φάσης).



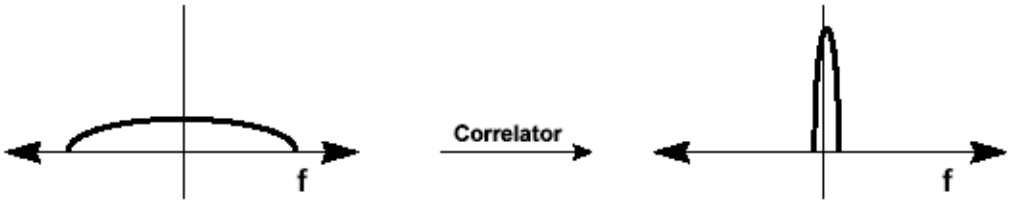
Σχήμα **9:** Ψηφιακή Διαμόρφωση Δεδομένων με μία **PN**

Ο δέκτης εκτελεί την αντίστροφη διαδικασία. Κατά τη λήψη του **DSSS** σήματος, χρησιμοποιεί ένα συσχετιστή (φίλτρο αντιστοίχησης) όπως φαίνεται στο σχήμα 10. Ο συσχετιστής αφαιρεί την **PN** ακολουθία και ανακτά το αρχικό σήμα.
Τα αποτελέσματα της χρησιμοποίησης **PN** ακολουθιών για την δημιουργία εξάπλωσης φάσματος φαίνονται στα σχήματα 11 και 12.
Όπως παρατηρούμε στο σχήμα 11 η ακολουθία **PN** διευρύνει το φάσμα του προς μετάδοση σήματος, μειώνοντας ταυτόχρονα το πλάτος του, δηλαδή απλώνει την ισχύ του σήματος σε πολύ μεγαλύτερο φασματικό εύρος. Βλέπουμε όμως ότι η συνολική ισχύς δεν μεταβάλλεται. Στο σχήμα 12 παρατηρούμε μετά τη λήψη του σήματος, το σήμα συσχετίζεται με την ίδια **PN** ακολουθία για να ανακτηθεί το αρχικό σήμα.
Ένα πλεονέκτημα της τεχνικής **DSSS** είναι η ανοχή σε παρεμβολές στενής ζώνης, καθώς και μεγαλύτερη ασφάλεια, εφόσον το "απλωμένο" σήμα μοιάζει σαν απλός θόρυβος σε πομπό που λαμβάνει μόνο σήμα στενής ζώνης.



Σχήμα 10: Συσχετιστής (φίλτρο αντιστοίχησης) κατά τη λήψη του DSSS σήματος

Σχήμα 11: Επίδραση της PN ακολουθίας στο μεταδιδόμενο σήμα



Σχήμα 12: Το λαμβανόμενο σήμα συσχετίζεται με την PN ακολουθία για την ανάκτηση του αρχικού σήματος.

Η DSSS χρησιμοποιεί 14 κανάλια, το καθένα με εύρος 5 MHz, ξεκινώντας από το κάτω όριο της ζώνης ISM στα 2,4 GHz.Ο Πίνακας 4 παρουσιάζει τα κανάλια που χρησιμοποιούνται σε διάφορες γεωγραφικές περιοχές.

Πίνακας 4: Διαθέσιμα κανάλια ανά περιοχή για το φυσικό στρώμα.

Περιοχή / Υπεύθυνη Αρχή	**Επιτρεπόμενα Κανάλια**
ΗΠΑ / FCC - Καναδάς / IC	1 έως 11 (2,412 - 2,462 GHz)
Ευρώπη (εκτός Γαλλίας & Ισπανίας) / ETSI	1 έως 13 (2,412 - 2,472 GHz)
Γαλλία	10 έως 13 (2,457 - 2,472 GHz)
Ισπανία	10 έως 11 (2,457 - 2,462 GHz)
Ιαπωνία / MKK	14 (2,484 GHz)

3.5 ΥΠΟΣΤΡΩΜΑ MAC ΤΟΥ 802.11

Το πρότυπο IEEE 802.11 καθορίζει ένα κοινό medium access control (MAC) υπόστρωμα, το οποίο παρέχει μία ποικιλία υπηρεσιών που υποστηρίζουν τη λειτουργία ασύρματων δικτύων – wireless LANs (WLANS) που βασίζονται στο 802.11. Γενικά, το υπόστρωμα MAC διαχειρίζεται και διατηρεί επικοινωνίες μεταξύ σταθμών που βασίζονται στο 802.11 με το να συντονίζει την πρόσβαση σε ένα κοινό radio κανάλι και χρησιμοποιώντας πρωτόκολλα που προάγουν τις επικοινωνίες σε ένα ασύρματο μέσον. Συχνά, αν το δούμε σαν τον εγκέφαλο του δικτύου, το υπόστρωμα 802.11 MAC χρησιμοποιεί ένα 802.11 φυσικό στρώμα (PHY), όπως το 802.11b ή το 802.11a, προκειμένου να εκτελέσει τις ενέργειες carrier sensing, μετάδοσης (transmit) και λήψης (receive) πλαισίων του 802.11.

3.5.1 ΠΡΟΣΒΑΣΗ ΣΤΟ ΜΕΣΟΝ

Προτού ξεκινήσει η μετάδοση πλαισίων, ένας σταθμός πρέπει πρώτα να αποκτήσει πρόσβαση στο μέσον, το οποίο είναι ένα κανάλι radio, κοινό για όλους τους σταθμούς. Το πρότυπο 802.11 ορίζει δύο μορφές πρόσβασης στο μέσον :

- Distributed Coordinated Function (DCF)
- Point Coordinated Function (PCF)

Το DCF είναι υποχρεωτικό και βασίζεται στο CSMA/CA (carrier sense multiple access with collision avoidance) πρωτόκολλο. Με το DCF, οι σταθμοί αγωνίζονται να διεκδικήσουν πρόσβαση και επιχειρούν να στείλουν πλαίσια όταν κανένας άλλος σταθμός δεν μεταδίδει. Αν ένας άλλος σταθμός στέλνει πλαίσια εκείνη τη στιγμή, οι σταθμοί διαθέτουν την ευγένεια και αναμένουν μέχρι να απελευθερωθεί το κανάλι.

Ως όρος προκειμένου να υπάρξει πρόσβαση στο μέσον, το υπόστρωμα MAC ελέγχει την τιμή που έχει ο Network Allocation Vector (NAV), ο οποίος είναι ένας καταμετρητής που εδρεύει σε κάθε σταθμό και που αντιπροσωπεύει το χρόνο που ο προηγούμενος σταθμός χρειάζεται για να στείλει ένα πλαίσιο. Το NAV πρέπει να είναι μηδέν προτού ένας σταθμός να επιχειρήσει να στείλει ένα πλαίσιο. Πριν τη μετάδοση ενός πλαισίου, ο σταθμός υπολογίζει το χρόνο που απαιτείται για να σταλεί το πλαίσιο λαμβάνοντας υπόψη το μήκος και το ρυθμό μετάδοσης του πλαισίου. Όταν οι σταθμοί λάβουν το πλαίσιο, εξετάζουν τη διάρκειά του και χρησιμοποιούν αυτή την τιμή ως βάση για τον καθορισμό των αντίστοιχων δικών τους NAV. Αυτή η διαδικασία καθιστά αποκλειστικό χρήστη του μέσου, το σταθμό που κάνει μετάδοση εκείνη τη στιγμή.

Ένα σπουδαίο χαρακτηριστικό του DCF είναι ένας χρονομετρητής τυχαίας τιμής που χρησιμοποιεί ένας σταθμός όταν αντιληφθεί ότι το μέσον είναι απασχολημένο. Αν το κανάλι είναι σε χρήση, τότε ο σταθμός πρέπει να περιμένει ένα τυχαίο χρονικό διάστημα προτού επιχειρήσει να αποκτήσει πρόσβαση στο μέσον ξανά. Αυτό εξασφαλίζει ότι πολλοί σταθμοί που επιθυμούν να κάνουν αποστολή δεδομένων, να μη μεταδίδουν ταυτόχρονα. Η τυχαία καθυστέρηση έχει ως αποτέλεσμα οι σταθμοί να περιμένουν διαφορετικά χρονικά διαστήματα και έτσι αποφεύγεται η ταυτόχρονη α) ανίχνευση του μέσου από όλους τους σταθμούς, β) ανεύρεση του καναλιού σε κατάσταση αδράνειας γ) μετάδοση και δ) σύγκρουση μεταξύ τους. Ο χρονομετρητής τυχαίας τιμής μειώνει σημαντικά των αριθμό των συγκρούσεων και αντίστοιχων αναμεταδόσεων, ειδικά όταν αυξάνεται ο αριθμός των ενεργών χρηστών του δικτύου.

Με radio-βασιζόμενα LANs, ένας σταθμός που είναι σε διαδικασία μετάδοσης δεδομένων δεν μπορεί ταυτόχρονα να ακούσει και τις συγκρούσεις, κυρίως διότι ο σταθμός δεν μπορεί να έχει σε λειτουργία το δέκτη του κατά τη διάρκεια που μεταδίδει το πλαίσιο. Ως εκ τούτου, ο σταθμός που λαμβάνει το πλαίσιο πρέπει να αποστείλει μία επιβεβαίωση – αναγνώριση (ACK) αν δεν εντοπίσει λάθη στο παραληφθέν πλαίσιο. Αν ο σταθμός αποστολής δεν λάβει την επιβεβαίωση ACK ύστερα από συγκεκριμένο χρονικό διάστημα, ο σταθμός αποστολής θα υποθέσει ότι υπήρξε μία σύγκρουση (ή RF παρεμβολή) και θα μεταδώσει ξανά το πλαίσιο.

Για την υποστήριξη χρονικά περιορισμένης παράδοσης πλαισίων δεδομένων, το πρότυπο 802.11 ορίζει προαιρετικά τον αλγόριθμο **Point Coordination Function (PCF)** σύμφωνα με τον οποίο το σημείο πρόσβασης (**access point**) παραχωρεί την πρόσβαση στο μέσον για ένα σταθμό, σφυγμομετρώντας (**polling**) το σταθμό κατά τη περίοδο χωρίς ανταγωνισμό (**contention free period**). Οι σταθμοί δεν μπορούν να μεταδώσουν πλαίσια μέχρι το **access point** να τους σφυγμομετρήσει. Το χρονικό διάστημα για κίνηση δεδομένων που έχουν βάση τον αλγόριθμο **PCF** (αν είναι ενεργοποιημένος) συμβαίνει εναλλάξ ανάμεσα σε περιόδους ανταγωνισμού **DCF**.

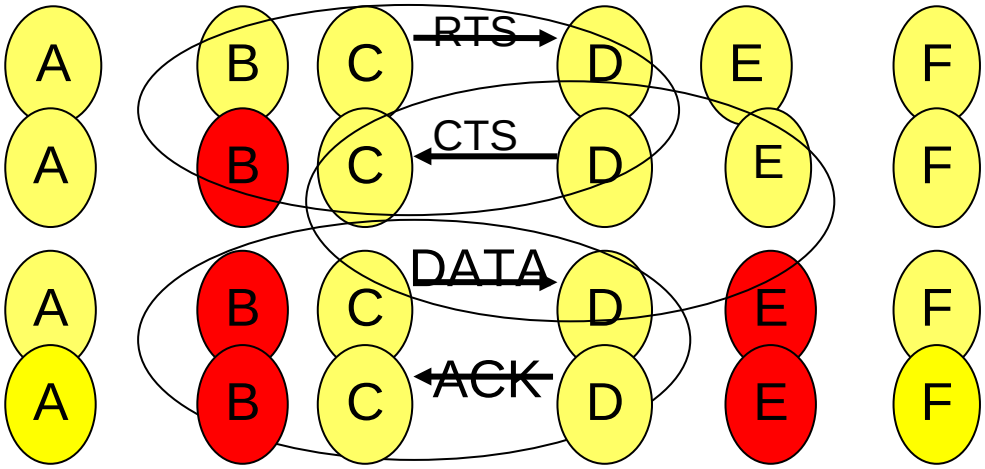
Το **access point** κάνει σφυγμομέτρηση των σταθμών σύμφωνα με μία λίστα σφυγμομέτρησης, κατόπιν εισέρχεται σε μία περίοδο ανταγωνισμού όπου οι σταθμοί χρησιμοποιούν τον αλγόριθμο **DCF**. Αυτή η διαδικασία επιτρέπει να υποστηρίζονται αμφότερες οι μέθοδοι λειτουργίας, σύγχρονη (π.χ. εφαρμογές **Video**) και ασύγχρονη (π.χ. εφαρμογές **e-mail** και **Web browsing**).

Για να εξασφαλιστεί ότι μία συγκεκριμένη ανταλλαγή πλαισίων θα γίνει χωρίς διακοπή λόγω μετάδοσης τρίτου σταθμού, το πρότυπο 802.11 υποστηρίζει το μηχανισμό **RTS/CTS**. Αυτός ο μηχανισμός διαφοροποιεί την διαδικασία αποστολής πλαισίου εισάγοντας δύο επιπλέον πλαίσια, τα **RTS (Ready To Send)** και **CTS (Clear To Send)**. Προστατεύοντας την ανταλλαγή πλαισίων, ο μηχανισμός **RTS/CTS** βελτιώνει 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 αποστολέας στέλνει αρχικά ένα πλαίσιο **RTS** στον παραλήπτη το οποίο δεν περιέχει δεδομένα. Αυτό το πλαίσιο έχει ως σκοπό 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**. Ο παραλήπτης λαμβάνοντας το **RTS** απαντάει 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.

Η παραπάνω διαδικασία γίνεται κατανοητή με το ακόλουθο παράδειγμα. Όσοι σταθμοί ακούν το πλαίσιο **CTS** παραμένουν σιωπηλοί για να μη δημιουργηθεί σύγκρουση κατά την μετάδοση του πλαισίου δεδομένων από τον σταθμό **C** στον σταθμό **D**. Επίσης σιωπηλοί παραμένουν και όσοι σταθμοί ακούν το πλαίσιο **RTS**, προκειμένου να μην δημιουργήσουν

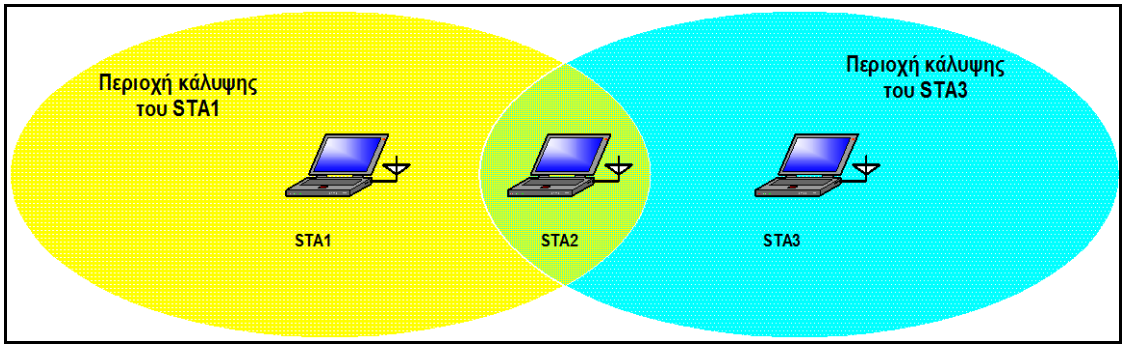
σύγκρουση κατά την μετάδοση της επιβεβαίωσης ACK από τον σταθμό D στον C. Το διάστημα στο οποίο οι σταθμοί παραμένουν σιωπηλοί περιλαμβάνεται σε ένα πεδίο RTS/CTS πλαισίων και εξαρτάται από την διάρκεια του πλαισίου πληροφορίας. Το πλαίσιο επιβεβαίωσης χρησιμοποιείται, διότι παρά την ύπαρξη του RTS/CTS μηχανισμού, υπάρχει πάντα η πιθανότητα λαθών λόγω του θορύβου του καναλιού καθώς επίσης και η πιθανότητα σύγκρουσης. Αν ένας σταθμός δεν λάβει πλαίσιο επιβεβαίωσης, αναμεταδίδει τότε το πλαίσιο.



Σχήμα 1: 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. 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.
Ο εν λόγω μηχανισμός αντιμετωπίζει αποτελεσματικά το πρόβλημα ύπαρξης κρυμμένου κόμβου (hidden node). Το πρόβλημα αυτό απεικονίζεται στο παρακάτω σχήμα.



Σχήμα 2: Πρόβλημα κρυμμένου κόμβου

Πρόβλημα κρυμμένου κόμβου
Όπως φαίνεται στο παραπάνω 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 οποίος δεν γνωρίζει την ύπαρξη του STA1, για τον ίδιο λόγο με την προηγούμενη περίπτωση. Ο STA2 βρίσκεται στην κοινή περιοχή κάλυψης των STA1 και STA3 και συνεπώς μπορεί να ανταλλάσσει πλαίσια και με τους δύο. Το πρόβλημα δημιουργείται στην περίπτωση που οι STA1 και STA3 επιχειρούν να επικοινωνήσουν με τον STA2 ταυτόχρονα. Το αποτέλεσμα είναι η δημιουργία συγκρούσεων και τα πλαίσια που έχουν σταλθεί χάνονται.
Τη λύση λοιπόν σ' αυτό το πρόβλημα έρχεται μας δώσει ο μηχανισμός RTS/CTS. Σύμφωνα μ' αυτόν, 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 (καθώς «ακούει»)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.

3.5.2 ΠΡΟΣΒΑΣΗ ΣΤΟ ΔΙΚΤΥΟ

Τα βασικά βήματα για να αποκτήσει ένας σταθμός πρόσβαση στο δίκτυο 802.11 είναι τα εξής:

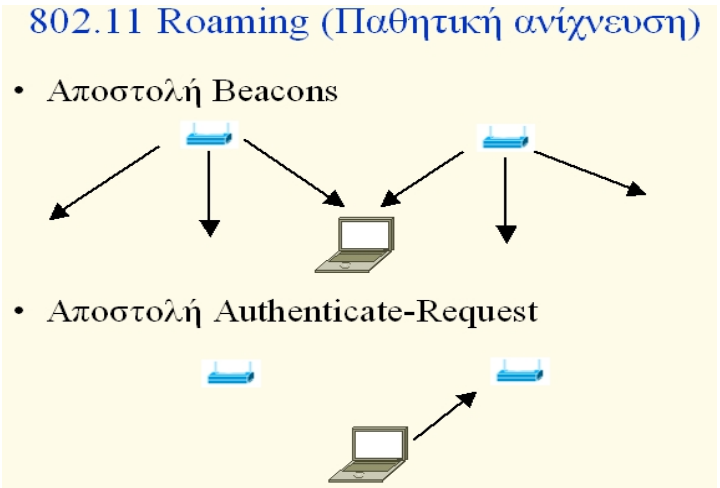
Roaming (Περιαγωγή)

Η διαδικασία της περιαγωγής (roaming), είναι η διαδικασία με την οποία μπορεί ένας σταθμός να μεταβαίνει από ένα BSS σε ένα άλλο διατηρώντας τη σύνδεση με το δίκτυο.

Το πρότυπο 802.11 δεν προσδιορίζει κάποια συγκεκριμένη διαδικασία περιαγωγής. Το μόνο που προσδιορίζει είναι τα βασικά εργαλεία για τη λειτουργία αυτή, τα οποία περιλαμβάνουν την παθητική (passive) και ενεργή (active) σάρωση, όπου μία radio NIC (network interface card) ψάχνει για σημεία πρόσβασης (access points). Το passive scanning είναι υποχρεωτικό όπου κάθε NIC σαρώνει τα κανάλια για να βρει το καλύτερο σημείο πρόσβασης (Access Point).

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.

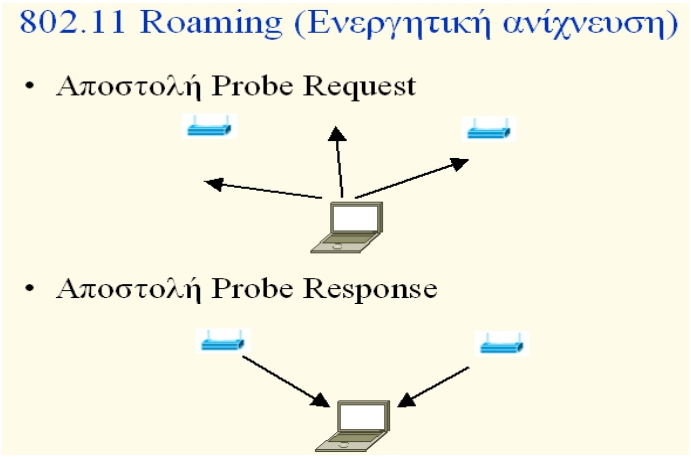
Η διαδικασία φαίνεται στο παρακάτω σχήμα.



Σχήμα 3: Παθητική ανίχνευση

Προαιρετικά το active scanning είναι παρόμοιο, εκτός του ότι η NIC ξεκινάει τη διαδικασία μεταδίδοντας ένα πλαίσιο ανίχνευσης (probe request frame), και όλα τα σημεία πρόσβασης (access points) εντός του βεληνεκούς απαντούν με απόκριση ανίχνευσης (probe response frame). Το active scanning δίνει τη δυνατότητα σε μία radio NIC να έχει άμεση απάντηση από τα access points, χωρίς να περιμένει τη μετάδοση ενός beacon πλαισίου. Ωστόσο, παραμένει το θέμα ότι το active scanning επιβάλλει πρόσθετο βάρος στο

δίκτυο λόγω της μετάδοσης πλαισίων **probe request** και αντίστοιχων πλαισίων **probe response.**
Η διαδικασία αυτή φαίνεται στο επόμενο σχήμα.



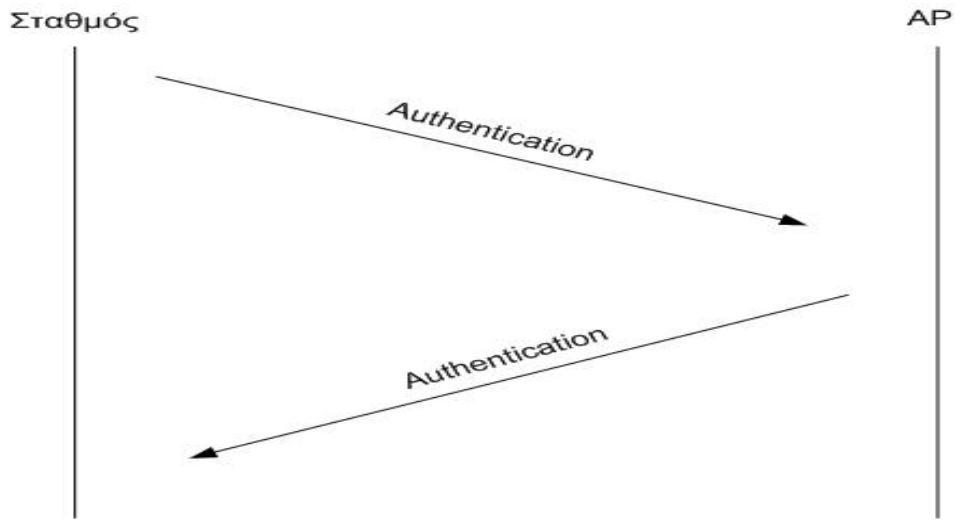
Σχήμα 4: Ενεργητική ανίχνευση

Όποιο τρόπο **scanning** κι αν ακολουθεί ο σταθμός, στο τέλος της διαδικασίας θα έχει αποκτήσει κάποιες βασικές πληροφορίες για τα διαθέσιμα δίκτυα.

Joining (Σύνδεση)
Όταν εντοπιστεί το δίκτυο ακολουθεί η διαδικασία του joining, χωρίς όμως ο κινητός σταθμός να αποκτήσει ακόμα πρόσβαση στο δίκτυο. Η διαδικασία του joining δεν δίνει σε έναν σταθμό πρόσβαση στο δίκτυο, απλώς είναι ένα απαραίτητο βήμα στη 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.

Authentication (Πιστοποίηση)
Authentication είναι η διαδικασία κατά την οποία αποδεικνύεται και πιστοποιείται η ταυτότητα. Η διαδικασία αυτή είναι εξαιρετικά σημαντική στη διατήρηση της ασφάλειας στα ασύρματα δίκτυα, εφόσον δεν υπάρχουν ουσιαστικά φυσικοί περιορισμοί για κάποιον που θέλει να αποκτήσει πρόσβαση σε ένα δίκτυο. Για την πιστοποίηση

πρέπει να ανταλλαχθούν οι κατάλληλες πληροφορίες και κλειδιά, όπως φαίνεται στο παρακάτω σχήμα.



Σχήμα 5: Διαδικασία Πιστοποίησης

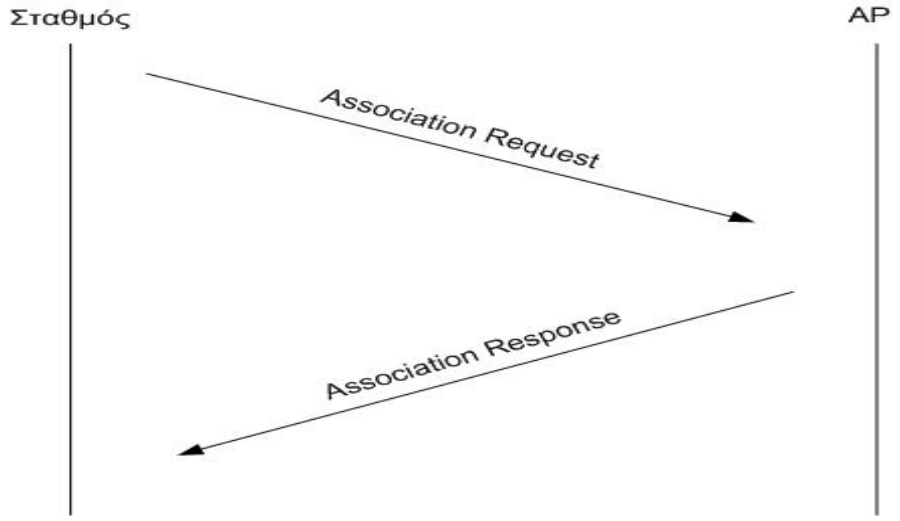
Το πρότυπο 802.11 προδιαγράφει δύο είδη διαδικασιών πιστοποίησης : **Open System Authentication** και **Shared Key Authentication**. Η διαδικασία **Open System Authentication** είναι υποχρεωτική και γίνεται σε δύο βήματα. Πρώτα, μία **radio NIC** ξεκινάει τη διαδικασία στέλνοντας ένα **authentication request** πλαίσιο στο σημείο πρόσβασης (**access point**). Το **access point** απαντάει με ένα **authentication response** πλαίσιο το οποίο περιέχει την έγκριση ή τη μη έγκριση μέσα στο Status Code Field που βρίσκεται στο σώμα του πλαισίου.
Η διαδικασία Shared Key Authentication είναι μία προαιρετική διαδικασία που γίνεται σε τέσσερα βήματα και που βασίζει την πιστοποίηση στο εάν η συσκευή που κάνει την πιστοποίηση έχει το σωστό **Wired Equivalent Privacy (WEP)** κλειδί. Υπενθυμίζεται ότι το πρότυπο 802.11 δεν θεωρεί υποχρεωτική την υποστήριξη του WEP, άρα αυτός ο τύπος πιστοποίησης μπορεί να μην είναι πάντα διαθέσιμος. Η **radio NIC** αποστέλλει ένα **Authentication Request** πλαίσιο στο σημείο πρόσβασης (**access point**). Κατόπιν, το **access point** τοποθετεί στο σώμα ενός απαντητικού (response) πλαισίου ένα κείμενο αμφισβήτησης (**challenge**) και το στέλνει στη **radio NIC**. Η **radio NIC** χρησιμοποιεί το δικό της **WEP** κλειδί για να κρυπτογραφήσει το κείμενο αμφισβήτησης και μετά το στέλνει πίσω στο **access point** με ένα άλλο πλαίσιο. Το **access point** αποκρυπτογραφεί το κείμενο αμφισβήτησης και το συγκρίνει με το αρχικό κείμενο. Αν τα κείμενα ισοδυναμούν τότε το **access point**

υποθέτει ότι η **radio NIC** έχει το σωστό **WEP** κλειδί. Το **access point** τελειώνει την ακολουθία στέλνοντας ένα πλαίσιο πιστοποίησης στη **radio NIC**, το οποίο περιέχει την έγκριση ή τη μη έγκριση.

Deauthentication (Ακύρωση Πιστοποίησης)
Προκειμένου ένας σταθμός (που είναι πιστοποιημένος στο δίκτυο) να εγκαταλείψει το δίκτυο, πρέπει να ακυρώσει την πιστοποίησή του. Μετά την ακύρωση της πιστοποίησης, ο σταθμός δεν έχει πλέον τη δυνατότητα να χρησιμοποιήσει το δίκτυο.

Association (Συσχέτιση)
Μόλις γίνει η πιστοποίηση, η radio **NIC** πρέπει να συσχετιστεί με το **access point** προτού αρχίσει την αποστολή πλαισίων δεδομένων (**data frames**). Η Συσχέτιση (**Association**) είναι αναγκαία προκειμένου να γίνει ο συγχρονισμός σπουδαίων πληροφοριών, όπως ο υποστηριζόμενος ρυθμός δεδομένων, ανάμεσα στο radio NIC και το access point. Η radio NIC ξεκινάει τη Συσχέτιση (Association) στέλνοντας ένα **Association Request Frame** που περιέχει στοιχεία ταυτότητας και υποστηριζόμενο ρυθμό δεδομένων. Το **access point** απαντάει στέλνοντας ένα **Association Response Frame** που περιέχει ένα **Association** Identification μαζί με άλλες πληροφορίες που αφορούν το access point. Μόλις η radio NIC και το access point ολοκληρώσουν τη διαδικασία του Association, τότε μπορούν να στείλουν πλαίσια δεδομένων το ένα στο άλλο.

Η διαδικασία φαίνεται στο παρακάτω σχήμα.



Σχήμα 6: Διαδικασία Συσχέτισης

3.6 ΕΞΟΙΚΟΝΟΜΗΣΗ ΕΝΕΡΓΕΙΑΣ ΣΤΟ 802.11

Τα ασύρματα δίκτυα (WLANs) βεβαίως και παρέχουν ελευθερία κινητικότητας αφού χρησιμοποιούμε τα Laptops μας και τα PDAs μας χωρίς τους περιορισμούς καλωδιώσεων δικτύου. Φυσικά, προκειμένου να διευκολύνουμε αυτό το πλεονέκτημα ακόμα περισσότερο, αποσυνδέουμε τις συσκευές μας από την ισχύ εναλλασσόμενου ρεύματος (AC Power) και τις λειτουργούμε με μπαταρίες. Ωστόσο, όπως όλοι μας γνωρίζουμε, οι κάρτες δικτύου 802.11 καταναλώνουν σημαντικές ποσότητες ενέργειας που εξαντλούν τις μπαταρίες των συσκευών πολύ γρήγορα.
Για να παρατείνουμε τη ζωή της μπαταρίας, το πρότυπο 802.11 καθορίζει ένα προαιρετικό Power Save Mode, το οποίο είναι διαθέσιμο σήμερα στις περισσότερες 802.11 κάρτες δικτύου – network interface cards (NICs). Οι τελικοί χρήστες μπορούν απλά να θέσουν σε λειτουργία (ON) ή εκτός λειτουργίας (OFF) το power save mode είτε μέσω του οδηγού της κάρτας δικτύου (card driver) είτε με κάποιο εργαλείο διαμόρφωσης.
Με το power save mode εκτός λειτουργίας, η 802.11 κάρτα δικτύου βρίσκεται συνήθως σε κατάσταση λήψης και ακρόασης πακέτων από το ασύρματο δίκτυο και μόνο περιστασιακά σε κατάσταση μετάδοσης όταν στέλνει πακέτα δεδομένων. Αυτή η περίπτωση απαιτεί η κάρτα δικτύου 802.11 να διατηρεί τα περισσότερα κυκλώματα σε εγρήγορση παρέχοντάς τους ηλεκτρική ισχύ και έτοιμα προς λειτουργία.
Όταν ενεργοποιήσουμε και θέσουμε σε λειτουργία το power save mode, η 802.11 κάρτα δικτύου δείχνει την επιθυμία της να εισέλθει σε κατάσταση ύπνου 'sleep' στο access point αλλάζοντας το power save bit από 0 σε 1 στο header κάθε πλαισίου 802.11. Το access point λαμβάνει αυτό το πλαίσιο και σημειώνει την ευχή του αντίστοιχου πελάτη να εισέλθει στην κατάσταση power save mode. Τότε το access point θα αρχίσει να αποθηκεύει πακέτα για τον πελάτη, ενώ η κάρτα δικτύου 802.11 του πελάτη βρίσκεται σε κατάσταση ύπνου. Αυτό είναι ανάλογο με το να πάρουμε ένα υπνάκο και να πούμε στο βοηθό μας να κρατήσει όλα τα μηνύματα που απευθύνονται σε μας.
Η κάρτα δικτύου 802.11 (NIC) του πελάτη (client) καταναλώνει πολύ λιγότερη ενέργεια κατά τη διάρκεια του 'ύπνου' όταν θέσει εκτός λειτουργίας σχεδόν όλα τα ηλεκτρικά κυκλώματα πλην ενός μόνο χρονικού κυκλώματος. Αυτός ο τρόπος λειτουργίας καθιστά την κάρτα δικτύου ικανή να καταναλώνει πολύ λίγη ενέργεια και περιοδικά να αφυπνίζεται (στον κατάλληλο χρόνο) προκειμένου να κάνει λήψη κανονικών μεταδόσεων beacon που προέρχονται από το access point. Αυτά τα beacons έχουν την πληροφορία που

καθορίζει αν οι σταθμοί που βρίσκονται σε κατάσταση ύπνου έχουν πακέτα αποθηκευμένα στο access point και αναμένουν την παράδοσή τους στους αντίστοιχους προορισμούς τους.
Όταν μία NIC που είναι σε κατάσταση 'ύπνου' ξυπνήσει και πληροφορηθεί από το beacon ότι υπάρχουν πακέτα που αναμένουν προς παραλαβή, η ράδιο NIC επικοινωνεί με το access point προκειμένου να τα ανακτήσει. Αμέσως μετά, η κάρτα δικτύου 802.11 μπορεί να επιστρέψει στην κατάσταση 'ύπνου' μέχρι την επόμενη αφύπνισή της για να ακούσει την επόμενη μετάδοση beacon.

Πρέπει να χρησιμοποιούμε το power save mode ?

Όταν πρέπει να αποφασίσουμε αν πρέπει να χρησιμοποιήσουμε το power save mode, πρέπει να έχουμε υπόψη τα παρακάτω:

- **Πραγματική εξοικονόμηση ενέργειας**
  Η πραγματική εξοικονόμηση ενέργειας για τη ζωή της μπαταρίας, όταν χρησιμοποιούμε το 802.11 power save mode, είναι πολύ δύσκολο να προσδιορισθεί, και υπάρχουν περιπτώσεις που δεν υπάρχει κανένα απολύτως πλεονέκτημα. Όταν η κάρτα δικτύου 802.11 μεταδίδει ή λαμβάνει, θα καταναλώσει κατά μέσο όρο περίπου 250 miliamps, ενώ το ρεύμα που καταναλώνει κατά τη κατάσταση 'ύπνου' μπορεί να είναι πολύ χαμηλό μέχρι και 30 miliamps. Επειδή η κοιμώμενη κάρτα δικτύου θα ξυπνάει περιοδικά, το συνολικό ρεύμα που καταναλώνεται θα κυμαίνεται κάπου μεταξύ 30 και 250 miliamps, το οποίο εξαρτάται από το κάθε πότε γίνεται η αφύπνιση (διαστήματα beacons).
  Αν εξαναγκάσουμε τη κάρτα δικτύου 802.11 να ξυπνάει συχνά προκειμένου να επεξεργαζόμαστε μεγαλύτερα επίπεδα κίνησης, τότε το συνολικό ρεύμα θα είναι πιο κοντά στις τιμές μετάδοσης / λήψης, ενδεχομένως περίπου 230 miliamps. Το αποτέλεσμα θα είναι ότι μάλλον δεν θα αντιληφθούμε κάποια σπουδαία εξοικονόμηση στη ζωή της μπαταρίας.

  Αν η ρύθμιση των χρόνων αφύπνισης επιτρέπει στη κάρτα δικτύου 802.11 να κοιμάται για μεγαλύτερες περιόδους, τότε το συνολικό ρεύμα που καταναλώνεται θα είναι πιο κοντά στη τιμή 'ύπνου', ίσως περίπου 100 miliamps. Το αποτέλεσμα θα είναι ότι η επιβάρυνση στη ζωή της μπαταρίας από τη κάρτα δικτύου 802.11 θα πέσει κατά 50 τοις εκατό ή και περισσότερο. Ωστόσο, αυτό δεν σημαίνει ότι η μπαταρία μας θα έχει διπλάσιο χρόνο ζωής, διότι και η συσκευή του χρήστη (laptop, PDA κλπ) καταναλώνει επίσης ενέργεια από τη μπαταρία. Οι βελτιώσεις της κάρτας δικτύου 802.11 απλώς μόνο συνεισφέρουν μερικώς στην επιμήκυνση της ζωής της μπαταρίας.

- **Μείωση της απόδοσης**
  Πρέπει να έχουμε υπόψη ότι προκειμένου να επιτύχουμε σημαντική εξοικονόμηση στη ζωή της μπαταρίας χρησιμοποιώντας power save mode, πρέπει να είμαστε και διατεθειμένοι να εργασθούμε με εξαιρετικά χαμηλή απόδοση. Ορισμένες εφαρμογές που απαιτούν συχνή επικοινωνία με τους πελάτες (clients), δεν θα λειτουργούν καλά αν έχουμε θέσει σε κατάσταση 'ON' το power save mode.

- **Υποστήριξη πακέτων Broadcast.**
  Τα περισσότερα access points είναι σχεδιασμένα να μην αποθηκεύουν πακέτα broadcast για πελάτες που είναι σε κατάσταση 'ύπνου'. Με αυτό τον τρόπο, αποφεύγουμε την ανάγκη για σχετικά μεγάλους χώρους αποθήκευσης (buffers), επειδή τα πακέτα broadcast εμφανίζονται πολύ συχνά στα περισσότερα δίκτυα. Αν τα πακέτα broadcast αποτελούν σημαντικό μέρος των ασύρματων εφαρμογών με τις οποίες εργαζόμαστε, τότε πρέπει να αποφεύγουμε τη χρήση του power save mode. Οι πελάτες μας (clients) μάλλον θα χάσουν σημαντικές πληροφορίες ενώ βρίσκονται σε κατάσταση 'ύπνου'.

Όλα τα παραπάνω είναι γενικές οδηγίες. Η αληθινή δοκιμή είναι η πραγματική πρακτική. Αν πιστεύουμε ότι το power save mode θα έχει σημαντική εξοικονόμηση στη ζωή της μπαταρίας, τότε αρχικά κάνουμε κάποιες πιλοτικές δοκιμές προκειμένου να εξασφαλίσουμε ότι πράγματι εξοικονομούμε ενέργεια και ζωή στη μπαταρία και τελικά ότι η πτώση της απόδοσης δεν επηρεάζει την λειτουργία των ασύρματων εφαρμογών μας.

4 ΥΠΟΠΡΟΤΥΠΑ ΤΟΥ 802.11

Οι αναθεωρήσεις του Πρότυπου 802.11
Από τότε που έγινε η επικύρωση του αρχικού προτύπου, η ομάδα εργασίας του IEEE 802.11 έκανε αρκετές αναθεωρήσεις μέσω διαφόρων ομάδων αναθεώρησης.

Η σημασία των γραμμάτων
Οι ομάδες αναθεώρησης εντός της ομάδας εργασίας του 802.11 έχουν ως αποστολή την ενίσχυση – εμπλουτισμό τμημάτων του προτύπου 802.11. Ένα ειδικό γράμμα του αλφαβήτου που αντιστοιχεί σε κάθε αναθεώρηση, όπως π.χ. 802.11a, 802.11b κλπ, αντιπροσωπεύει τις διάφορες ομάδες αναθεώρησης. Ως παράδειγμα μπορούμε να αναφέρουμε την ομάδα αναθεώρησης Β (δηλαδή 802.11b) που είναι υπεύθυνη για την αναβάθμιση του αρχικού πρότυπου 802.11 έτσι ώστε να συμπεριλάβει λειτουργία υψηλότερου ρυθμού μετάδοσης δεδομένων χρησιμοποιώντας DSSS στη μπάντα των 2,4 GHz.

Πίνακας 5: Τα πιο γνωστά υποπρότυπα του 802.11

- IEEE 802.11a: Χρησιμοποιεί τη ζώνη των 5 GHz και OFDM. Ταχύτητα μικρότερη από 54Mbps.
- IEEE 802.11b (Χρησιμοποιείται στην Ελλάδα): Χρησιμοποιεί τη ζώνη των 2.4 GHz και DSSS. Ταχύτητα μικρότερη από 11M bps
- IEEE 802.11e: Παρέχει εγγυήσεις για ποιότητα υπηρεσίας (Quality of Service - QoS).
- IEEE 802.11f: Κινητικότητα των σταθμών μέσα σε ένα IP δίκτυο (Intra - network Handover).
- IEEE 802.11g: Επεκτείνει το 802.11b ώστε να προσεγγίζει ταχύτητες που αγγίζουν τα 54Mbps.
- IEEE 802.11i: Πρότυπο το οποίο μελετά θέματα ασφάλειας στα WLANs.
- IEEE 802.11h: Η ομάδα αυτή θα προσπαθήσει να εισάγει στο 802.11a την δυνατότητα για καλύτερο έλεγχο συγκρούσεων.

4.1 802.11a-OFDM ΣΤΗ ΜΠΆΝΤΑ ΤΩΝ 5 GH_Z

Το 802.11a είναι ένα πρότυπο φυσικού επιπέδου (IEEE Std. 802.11a – 1999) που προδιαγράφει τη λειτουργία στη μπάντα

των 5 GHz χρησιμοποιώντας OFDM (Orthogonal Frequency Division Multiplexing / Ορθογωνική Πολυπλεξία Διαίρεσης Συχνότητας). Η βασική ιδέα πίσω από την OFDM είναι η διαίρεση ενός κύριου υψηλού ρυθμού σε πολλούς μικρότερους ρυθμούς και η χρήση αυτών για την αποστολή των δεδομένων ταυτόχρονα. Όλα τα «αργά» κανάλια πολυπλέκονται τελικά σε ένα «γρήγορο» κανάλι και μεταδίδονται. Με την ορθογωνοποίηση λύνεται το πρόβλημα της σπατάλης του εύρους ζώνης, προκειμένου να διαχωρίσουμε τα κανάλια μεταξύ τους. Το 802.11a υποστηρίζει ρυθμούς μετάδοσης δεδομένων που εκτείνονται από 6 έως 54 Mbps. Συσκευές και προϊόντα που στηρίζονται στο πρότυπο 802.11a άρχισαν να γίνονται διαθέσιμα προς το τέλος του έτους 2001.
Επειδή η λειτουργία γίνεται στη μπάντα των 5 GHz, το 802.11a προσφέρει καλύτερη συμπεριφορά στις παρεμβολές ράδιο συχνοτήτων από ότι άλλα φυσικά πρωτόκολλα (PHY) (π.χ. 802.11b και 802.11g) που χρησιμοποιούν συχνότητες στη μπάντα των 2,4 GHz. Με υψηλούς ρυθμούς μετάδοσης δεδομένων και σχετικά πολύ μικρές παρεμβολές, το 802.11a είναι κατάλληλο για την υποστήριξη εφαρμογών πολυμέσων και πυκνοκατοικημένα περιβάλλοντα χρηστών. Αυτό καθιστά το 802.11a μία εξαιρετική λύση μακράς διαρκείας για να ικανοποιηθούν τρέχουσες και μελλοντικές απαιτήσεις. Συστήνεται να ληφθεί σοβαρά υπόψη η ανάπτυξη του 802.11a, εκτός και αν οι περιστάσεις προτρέπουν τη χρήση ενός διαφορετικού φυσικού πρωτοκόλλου (PHY), όπως το 802.11b.

4.2 802.11b-ΥΨΗΛΟΣ ΡΥΘΜΟΣ ΜΕΤΑΔΟΣΗΣ DSSS ΣΤΗ ΜΠΑΝΤΑ ΤΩΝ 2,4GHz

Η ομάδα αναθεώρησης για το 802.11b ήταν υπεύθυνη για τον εμπλουτισμό του αρχικού 802.11 DSSS PHY έτσι ώστε εκτός από τους ρυθμούς μετάδοσης δεδομένων του 1 Mbps και 2 Mbps του αρχικού προτύπου, να συμπεριληφθούν και οι ρυθμοί μετάδοσης δεδομένων των 5,5 Mbps και 11 Mbps. Η εξέλιξη του IEEE Std 802.11b κατέληξε προς τα τέλη του έτους 1999. Το IEEE Std 802.11b, προκειμένου να παρέχει υψηλότερους ρυθμούς δεδομένων, χρησιμοποιεί Complementary Code Keying (CCK), μία τεχνική διαμόρφωσης που κάνει αποτελεσματική χρήση του ράδιο φάσματος.
Το 802.11b είναι το πιο διαδεδομένο στην αγορά ανεξάρτητα από το γεγονός ότι το 802.11a, προσφέρει υψηλότερους ρυθμούς μετάδοσης. Όταν η ποιότητα επικοινωνίας είναι φτωχή, το σύστημα μπορεί να ρίξει την ταχύτητα σε 5,5 Mb/s, 2 Mb/s ή 1 Mb/s προκειμένου να διατηρηθεί η σύνδεση μεταξύ των ασύρματων συσκευών.

Χρησιμοποιεί το ίδιο υπόστρωμα MAC όπως και τα άλλα πρότυπα, την τεχνική HR/DSSS (High Rate/ Direct Sequence Spread Spectrum) και την διαμόρφωση CCK (Complementary Code Keying - χρησιμοποιεί το πλήρες εύρος ζώνης συχνοτήτων κάθε υποκαναλιού για να διαμορφώσει τα σήματά του). Μπορεί να θεωρηθεί σαν επέκταση του αρχικού DSSS φυσικού στρώματος που ορίστηκε στο 802.11 και μάλιστα χρησιμοποιεί τα ίδια κανάλια με αυτό, πετυχαίνοντας αρκετά μεγαλύτερους ρυθμούς μετάδοσης.
Οι περισσότερες εγκαταστάσεις WLANs σήμερα είναι συμβατές με το IEEE Std 802.11b, που είναι επίσης η βάση για Wi-Fi πιστοποίηση από τη WECA (Wireless Ethernet Compatibility Alliance). Αυτά τα προϊόντα είναι διαθέσιμα εδώ και δύο χρόνια. Σε μερικές περιπτώσεις σήμερα, θα έπρεπε να αναπτύσσονται 802.11b δίκτυα προκειμένου να εκμεταλλευτούμε την ήδη εγκατεστημένη ευρεία βάση των εξοπλισμένων με το πρότυπο IEEE Std 802.11b χρηστών. Παραδείγματος χάριν, θα μπορούσαμε να χρησιμοποιήσουμε το 802.11b ως βάση για την ανάπτυξη δημόσιων WLANs για να μεγιστοποιήσουμε τον αριθμό των συνδρομητών.

4.3 802.11c-BRIDGE OPERATION PROCEDURES

Το 802.11c παρέχει τις απαραίτητες πληροφορίες προκειμένου να διασφαλιστούν οι κατάλληλες λειτουργίες γεφύρωσης (Bridge). Η μελέτη αυτή έχει ολοκληρωθεί και οι σχετικές διαδικασίες έχουν ενσωματωθεί στο πρότυπο 802.11c. Οι κατασκευαστές προϊόντων χρησιμοποιούν αυτό το πρότυπο όταν αναπτύσσουν σταθμούς πρόσβασης (access points). Δεν υπάρχει σχεδόν τίποτα σε αυτό το πρότυπο που να σχετίζεται με τις εγκαταστάσεις των WLANs.

4.4 802.11d-Global Harmonization (Συνολική Εναρμόνιση)

Όταν το 802.11 έγινε διαθέσιμο στην αρχή, μόνο μία χούφτα κανονιστικών πεδίων – περιοχών (USA, Ευρώπη και Ιαπωνία) διέθεταν κανονισμούς για τη λειτουργία 802.11 WLANs. Για να υπάρξει υποστήριξη και ευρεία υιοθέτηση του 802.11, η ομάδα αναθεώρησης 802.11d είχε μία συνεχώς αυξανόμενη υποχρέωση να καθορίσει απαιτήσεις φυσικού επιπέδου (PHY) που να ικανοποιούν κανονισμούς και σε άλλες τρίτες χώρες. Αυτό είναι εξαιρετικά σημαντικό για λειτουργία στις μπάντες των 5 Ghz επειδή η χρήση αυτών των συχνοτήτων διαφέρει πολύ από μία χώρα σε μία άλλη. Όπως και με το 802.11c, έτσι και το πρότυπο 802.11d ως επί το πλείστον

έχει εφαρμογή σε εταιρείες που αναπτύσσουν προϊόντα με βάση το πρότυπο 802.11.

4.5 802.11e-MAC ENHANCEMENTS FOR QoS (ΕΜΠΛΟΥΤΙΣΜΟΣ ΤΟΥ MAC ΓΙΑ ΠΟΙΟΤΗΤΑ ΥΠΗΡΕΣΙΩΝ)

Χωρίς ισχυρή ποιότητα υπηρεσιών - QoS (Quality of Service), η υπάρχουσα έκδοση του πρότυπου 802.11 δεν βελτιστοποιεί τη μετάδοση φωνής και εικόνας. Επί του παρόντος δεν υπάρχει κανένας αποτελεσματικός μηχανισμός που να καθορίζει την προτεραιότητα κίνησης εντός του 802.11. Ως εκ τούτου, η εργασία της ομάδας αναθεώρησης 802.11e, είναι να διυλίσει – καθαρίσει το 802.11 MAC (Medium Access Layer) για να βελτιωθεί το Quality of Service (QoS) προκειμένου να υπάρξει καλύτερη υποστήριξη στις εφαρμογές audio και video (όπως οι MPEG-2).
Επειδή το 802.11e είναι εντός των ορίων του MAC υποστρώματος, είναι κοινό και σε όλα τα φυσικά υποστρώματα του 802.11 και επομένως συμβατό προς τα πίσω με όλα τα υπάρχοντα 802.11 WLANs.

4.6 802.11f-INTR ACCESS POINT PROTOCOL

Το υπάρχον πρότυπο 802.11 δεν προδιαγράφει τις επικοινωνίες μεταξύ των Access Points και αυτό για να υποστηρίζονται οι χρήστες που περιπλανώνται από το ένα στο άλλο Access Point. Η ομάδα εργασίας του 802.11 εσκεμμένα δεν καθόρισε αυτό το στοιχείο για να υπάρχει ελαστικότητα όταν εργαζόμαστε με διαφορετικά συστήματα διανομής (δηλαδή, ενσύρματα backbones που διασυνδέουν Access Points.
Το πρόβλημα ωστόσο είναι ότι Access Points από διαφορετικούς κατασκευαστές μπορεί να μη έχουν διαλειτουργηκότητα όταν υποστηρίζουν περιαγωγή (roaming). Το 802.11f προδιαγράφει ένα Inter Access Point Protocol το οποίο παρέχει τις αναγκαίες πληροφορίες που χρειάζονται να ανταλλάξουν τα Access Points προκειμένου να υποστηριχθούν οι λειτουργίες των συστημάτων διανομής του προτύπου 802.11 (δηλαδή, περιαγωγή – roaming).
Εν απουσία του προτύπου 802.11f, θα πρέπει να χρησιμοποιείται ο ίδιος κατασκευαστής για τα Access Points έτσι ώστε να διασφαλίζεται η διαλειτουργηκότητα για τους περιπλανώμενους χρήστες. Σε ορισμένες περιπτώσεις μία ανάμιξη από Access Points διαφορετικών κατασκευαστών μπορεί να λειτουργήσει, ειδικά αν τα Access Points έχουν πιστοποίηση Wi-Fi. Η προσμέτρηση του προτύπου 802.11f στο σχεδιασμό των Access Points

ενδεχομένως να αυξήσει τις εναλλακτικές λύσεις και να προσθέσει μερικώς ασφάλεια διαλειτουργικότητας όταν πρόκειται να γίνει επιλογή για Access Points διαφορετικών κατασκευαστών.

4.7 802.11g-ΥΨΗΛΟΤΕΡΟΙ ΡΥΘΜΟΙ ΜΕΤΑΔΟΣΗΣ ΣΤΗΝ ΜΠΑΝΤΑ ΤΩΝ 2,4 GHz

Η αποστολή της ομάδας αναθεώρησης 802.11g ήταν να επεκτείνει το 802.11b και να αναπτύξει μία υψηλότερη ταχύτητα μετάδοσης (μέχρι 54 Mbps), ενώ η λειτουργία θα είναι εντός της μπάντας των 2,4 GHz. Το 802.11g υλοποιεί όλα τα υποχρεωτικά στοιχεία του προτύπου IEEE 802.11b PHY. Παραδείγματος χάριν, ένας 802.11b χρήστης είναι σε θέση να συσχετιστεί με ένα 802.11b access point και να λειτουργεί με ρυθμούς μετάδοσης δεδομένων μέχρι 11 Mbps. Νωρίς το έτος 2002, αποφασίστηκε το 802.11g να χρησιμοποιήσει OFDM αντί για DSSS ως βάση για την παροχή υψηλότερων ρυθμών μετάδοσης.
Ένα ζήτημα είναι ότι η παρουσία ενός 802.11b χρήστη σε ένα 802.11g δίκτυο απαιτεί τη χρήση RTS / CTS (request to send / clear-to-send), το οποίο δημιουργεί ουσιαστικό πρόβλημα και μειώνει σημαντικά την απόδοση για όλους τους 802.11b και 802.11g χρήστες. Το RTS / CTS εξασφαλίζει ότι ο σταθμός που κάνει την αποστολή, να μεταδίδει πρώτα ένα πλαίσιο RTS και να λαμβάνει ένα πλαίσιο CTS από το access point προτού στείλει δεδομένα. Ένας συνδυασμός από 802.11b και 802.11g χρήστες απαιτεί RTS / CTS προκειμένου να αποφευχθούν συγκρούσεις επειδή οι 802.11b σταθμοί δεν μπορούν να ακούσουν τους 802.11g σταθμούς χρησιμοποιώντας OFDM.
Η ομάδα αναθεώρησης IEEE 802.11g, στα μέσα του 2003 ολοκλήρωσε τις εργασίες της και εξέδωσε το πρότυπο 802.11g, το οποίο επεκτείνει το 802.11b, προσφέρει ρυθμούς μετάδοσης μέχρι 54 Mbps αλλά και συμβατότητα με το 802.11b. Χρησιμοποιεί και αυτό τη μπάντα των 2,4 GHz. Σε αντίθεση με το 802.11b χρησιμοποιεί την OFDM για να πετύχει τους επιθυμητούς ρυθμούς μετάδοσης.
Το πιο σημαντικό χαρακτηριστικό του 802.11g είναι η συμβατότητά του με το 802.11b. Το 802.11b ως γνωστό αποτελεί σήμερα το φυσικό στρώμα που υλοποιείται στα περισσότερα προϊόντα ασύρματης δικτύωσης. Το 802.11g λειτουργώντας ταυτόχρονα με το 802.11b μπορεί να το αντικαταστάσει σταδιακά εξολοκλήρου.

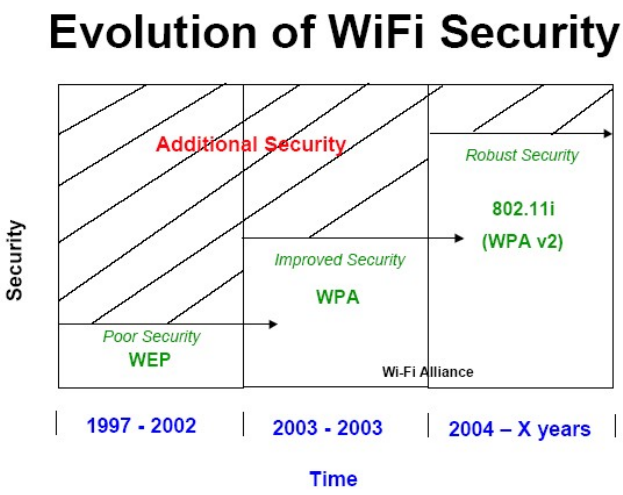
4.8 802.11h-SPECTRUM MANAGED 802.11a

Το 802.11h απευθύνεται και καλύπτει τις απαιτήσεις των Ευρωπαϊκών κανονισμών. Παρέχει Dynamic Channel Selection (DCS) – δυναμική επιλογή καναλιών και Transmit Power Control (TPC) – έλεγχο μετάδοσης ισχύος, για συσκευές που λειτουργούν στη μπάντα των 5 GHz (802.11a). Στην Ευρώπη υπάρχει εν δυνάμει πιθανότητα το 802.11a να έχει παρεμβολές με τις δορυφορικές επικοινωνίες. Με τη χρήση των DCS και TPC, το 802.11h θα αποφύγει τις παρεμβολές.
Προκειμένου να υλοποιήσει το DCS και TCP, το 802.11h αναπτύσσει πρακτικές που επηρεάζουν αμφότερα τα υποστρώματα MAC και PHY. Με το να συμπεριληφθούν το DCS και το TPC, το 802.11h θα μπορέσει να γίνει ο διάδοχος του 802.11a. Ευτυχώς, δεν υπάρχουν ζητήματα μη καλής διαλειτουργικότητας ανάμεσα σε υπάρχοντα 802.11a και 802.11h χρήστες και access points. Τα καλά νέα είναι ότι το 802.11h ενισχύει πωλήσεις 802.11a δικτύων στην Ευρώπη, πράγμα που ενδεχομένως να έχει ως αποτέλεσμα υψηλότερους όγκους πωλήσεων και χαμηλότερες τιμές.

4.9 802.11i-ΕΝΙΣΧΥΣΗ ΤΩΝ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ ΤΟΥ MAC ΓΙΑ ΕΝΙΣΧΥΜΕΝΗ ΑΣΦΑΛΕΙΑ

Το 802.11i εμπλουτίζει το υπόστρωμα MAC προκειμένου να αντιμετωπίσει τα ζητήματα ασφαλείας που σχετίζονται με το Wired Equivalent Privacy (WEP).
Οι αλγόριθμοι κρυπτογράφησης που χρησιμοποιούνται σήμερα, όπως ο WEP (Wired Equivalent Privacy), ο WPA (Wi-Fi Protected Access) και IP SEC παρουσιάζουν κάποια προβλήματα. Για παράδειγμα ο πρώτος εμφανίζει σημαντικά κενά ασφαλείας, ο WPA ενώ έρχεται να καλύψει τα κενά του WEP, στην πραγματικότητα δεν καλύπτει την ουσιαστική ασφάλεια στα ασύρματα τοπικά δίκτυα. Τέλος ο IP SEC εφαρμόζεται τοπικά σε κάθε χρήστη και καλύπτει Point-to-Point συνδέσεις.
Το υπάρχον πρότυπο 802.11 προδιαγράφει τη χρήση σχετικά αδύναμων, στατικών κρυπτογραφικών κλειδιών χωρίς καμία μορφή διαχείρισης της κατανομής των κλειδιών. Αυτό δίνει τη δυνατότητα σε hackers να αποκτήσουν πρόσβαση και να αποκρυπτογραφήσουν δεδομένα του ασύρματου δικτύου (WLAN) που έχουν κρυπτογραφηθεί με τον αλγόριθμο WEP. Η ομάδα αναθεώρησης του 802.11i θα προσπαθήσει να αντικαταστήσει το WEP και την υποστήριξή του σε συσκευές, αρχικά με την δημιουργία ανώτερου πρωτοκόλλου ασφάλειας προς τα πίσω συμβατό με το WEP, και τελικά με την πλήρη κατάργησή του. Το 802.11i θα ενσωματώσει το 802.1x και μεταγενέστερες

ισχυρότερες τεχνικές κρυπτογράφησης, όπως το AES (Advanced Encryption Standard). Η υλοποίηση του AES, ωστόσο, μπορεί να απαιτήσει νέο εξοπλισμό.
Στο παρακάτω σχήμα γίνεται μια αναδρομή στους διάφορους αλγορίθμους κρυπτογράφησης.



Σχήμα 1: Αλγόριθμοι Κρυπτογράφησης

4.10 802.11-Η ΕΠΟΜΕΝΗ ΓΕΝΙΑ

Εκτός από τις παραπάνω αναφερθείσες ομάδες αναθεώρησης, η ομάδα εργασίας του 802.11 μελετάει και νέες μεθόδους για να αυξηθεί η απόδοση και να γίνει καλύτερη χρήση του ράδιο φάσματος. Παραδείγματος χάριν, η ομάδα εργασίας σκέφτεται σοβαρά τη χρήση διαμόρφωσης ultrawideband ως ένα νέο μηχανισμό για την υποστήριξη εφαρμογών υψηλότερων ταχυτήτων και για τη μείωση της εν δυνάμει πιθανότητας RF παρεμβολών. Ωστόσο, θα περάσουν αρκετά χρόνια μέχρι να δούμε αυτά τα νεότερα και ταχύτερα πρότυπα.

ΕΠΙΛΟΓΟΣ

Όπως είδαμε από όλα τα προαναφερόμενα κεφάλαια της εργασίας τα ασύρματα δίκτυα είναι μία τεχνολογία που συνεχώς εξελίσσεται και δεν έχει κανένα λόγο να ζηλέψει κάτι από τα ενσύρματα δίκτυα.
Τα ασύρματα δίκτυα έχουν φέρει αλλαγή στον τρόπο επικοινωνίας των υπολογιστών, αλλά και των χρηστών τους. Με την αύξηση του αριθμού των συσκευών που αλληλεπιδρούν με τους υπολογιστές τα ασύρματα δίκτυα μπορούν να

προσφέρουν λύσεις, οι οποίες θα βελτιώσουν την επικοινωνία και θα αυξήσουν την αποδοτικότητα στον εργασιακό χώρο.
Ένα άλλο ενδιαφέρον σημείο στην περίπτωση των ασύρματων δικτύων είναι η συμβατότητα των διαφόρων συσκευών. Έτσι λοιπόν, έχει δημιουργηθεί ένας μη κερδοσκοπικός οργανισμός με την ονομασία Wi-Fi Alliance του οποίου μέλημα είναι ο έλεγχος της συμβατότητας Wi-Fi προϊόντων διαφορετικών κατασκευαστών. Για τον λόγο αυτό έχει υιοθετηθεί και το logo που παρουσιάζεται στο σχήμα που ακολουθεί, το οποίο γνωστοποιεί στον καταναλωτή ότι το προϊόν που σκοπεύει να αγοράσει είναι συμβατό με την Wi-Fi τεχνολογία και δεν θα συναντήσει προβλήματα σε περίπτωση που προσπαθήσει να συνδεθεί ασύρματα με συσκευές διαφορετικών κατασκευαστών από την δική του.

Σχήμα 2: Logo συμβατότητας με τεχνολογία Wi-Fi

Συνολικά, ανάμεσα στα πλεονέκτημα της W-LAN τεχνολογίας ξεχωρίζουμε την ευκολία υλοποίησης και το μικρό κόστος τόσο για τον σταθμό βάσης όσο και για τον χρήστη. Ενδεικτικά, τα Ασύρματα Δίκτυα θα μπορούσαν να χρησιμοποιηθούν μέσα στο χώρο της επιχείρησης για επικοινωνία των Υπολογιστών της Επιχείρησης χωρίς τη χρήση και το κόστος της δομημένης καλωδίωσης ή επέκταση του ήδη υπάρχοντος δικτύου με αμελητέο κόστος και υποδομή.
Θα μπορούσαμε να χρησιμοποιήσουμε ένα ασύρματο δίκτυο για να συνδέσουμε δύο LAN αφού τα ασύρματα δίκτυα προσφέρουν μία αποτελεσματική σε κόστος λύση σε χρήστες με δυσκολία στη φυσική εγκατάσταση. Η ασύρματη σύνδεση επιτρέπει στα δύο σημεία πρόσβασης να επικοινωνούν μεταξύ τους και να διασυνδέουν τα δύο LAN.
Εδώ θα πρέπει να σημειωθεί ότι όλα τα σημεία πρόσβασης υλικού δεν έχουν την ικανότητα να διασυνδεθούν απευθείας με ένα άλλο σημείο πρόσβασης υλικού και το αντικείμενο της διασύνδεσης LAN με ασύρματες συνδέσεις είναι μεγάλο και πολύπλοκο.
Δεν θα πρέπει να ξεχνάμε ότι τα ασύρματα δίκτυα, εκτός από τα οφέλη που προσφέρουν για χρήστες με υπολογιστές σταθερής θέσης, προσφέρουν σημαντικά οφέλη σε χρήστες laptop οι οποίοι κινούνται από περιοχή σε περιοχή μέσα στη μέρα. Σε αυτό το σημείο βλέπουμε τη διαφορά με ένα ενσύρματο δίκτυο αφού εξαιτίας των καλωδίων του δικτύου

ένα laptop δεν μπορεί να απομακρυνθεί από το χώρο του δικτύου και κατ' επέκταση να εκπροσωπήσει το σκοπό για τον οποίο δημιουργήθηκε.
Επιπρόσθετα μπορούμε πολύ εύκολα να χρησιμοποιήσουμε ένα ασύρματο LAN για να μοιραστούμε σύνδεση στο internet, αν λάβουμε υπόψη μας ότι οι ασύρματες κάρτες είναι ανάλογες με τις Ethernet και ότι ο άδειος χώρος είναι ανάλογος με καλώδια Ethernet.
Ένα ασύρματο δίκτυο μας επιτρέπει να χρησιμοποιήσουμε περισσότερους από ένα ασύρματα δικτυωμένους υπολογιστές με ένα μόνο σημείο πρόσβασης. Αυτό βέβαια εξαρτάται από τον κατασκευαστή, αφού σημεία πρόσβασης υλικού έχουν ένα συνιστάμενο όριο των 10 υπολογιστών ενώ άλλα, πιο ακριβά σημεία πρόσβασης μπορούν να καλύψουν μέχρι 100 ασύρματες συνδέσεις. Εκτός αυτού ένα ασύρματο δίκτυο μας επιτρέπει να έχουμε πάνω από ένα σημείο πρόσβασης, αφού πολλαπλά σημεία πρόσβασης μπορούν να συνδεθούν σε ενσύρματο LAN ή μερικές φορές σε ένα δεύτερο ασύρματο LAN αν το σημείο πρόσβασης το επιτρέπει αυτό.
Ένα σημαντικό χαρακτηριστικό είναι η δυνατότητα χρήσης "roaming", όπου ο χρήστης μπορεί να μετακινηθεί από μία περιοχή σε μία άλλη διάφανα ενώ το υλικό του ασύρματου δικτύου αυτόματα αλλάζει στο σημείο πρόσβασης με το καλύτερο σήμα. Όταν χρησιμοποιούμε πολλαπλά σημεία πρόσβασης, κάθε σημείο πρόσβασης της ασύρματης περιοχής πρέπει να είναι μέσα στα όρια της ασύρματης επικοινωνίας. Αυτό παρέχει seamless περιοχή για τους χρήστες στην οποία κινούνται και εδώ χρησιμοποιείται το "roaming".
Ανεξάρτητα από την αβλαβή ακτινοβολία την οποία προσφέρει ένα ασύρματο δίκτυο, μπορεί να μας παρέχει μία αρκετά μεγάλη ακτίνα στην οποία μπορούμε να κινούμαστε. Τα όρια της ακτίνας του εσωτερικού χώρου είναι 150 - 300 πόδια (1 foot = 0,3042 m) αλλά μπορεί να είναι μικρότερα αν η κατασκευή του κτιρίου παρεμβαίνει στη μετάδοση του σήματος. Το μειονέκτημα εδώ είναι ότι όταν λειτουργούμε στα όρια της ακτίνας η απόδοση μπορεί να μειωθεί, γιατί η ποιότητα της σύνδεσης φθείρεται και το σύστημα αντισταθμίζει αναλόγως. Υπάρχουν όμως τρόποι να επεκτείνουμε τη βασική επιχειρησιακή ακτίνα μίας ασύρματης επικοινωνίας χρησιμοποιώντας περισσότερα από ένα σημεία πρόσβασης ή χρησιμοποιώντας ένα ασύρματο σημείο επέκτασης.
Σημαντικό ρόλο στη σωστή λειτουργία των ασύρματων δικτύων αποτελούν τα πρωτόκολλα, οι αλγόριθμοι και οι μηχανισμοί οι οποίοι τρέχουν στα ασύρματα δίκτυα αφού φροντίζουν για τη σίγουρη και χωρίς λάθη αποστολή και λήψη των πλαισίων-πακέτων που αποστέλλονται από το ένα σημείο στο άλλο και βοηθάνε έτσι ώστε αυτά να μην χάνονται κατά τη μεταφορά τους.
Μία αδυναμία που θα μπορούσαμε να εντοπίσουμε στα ασύρματα δίκτυα θα μπορούσε να θεωρηθεί το θέμα της

ασφάλειας. Ασύρματες επικοινωνίες προφανώς έχουν θέματα ασφάλειας διότι ένας εισβολέας δεν χρειάζεται να έχει φυσική πρόσβαση σε ένα παραδοσιακά ενσύρματο δίκτυο για να έχει πρόσβαση σε αρχεία. Παρόλα αυτά οι ασύρματες επικοινωνίες του 802.11 δεν μπορούν να ληφθούν, πόσο μάλλον να αποκωδικοποιηθούν από απλούς σαρωτές ή δέκτες sort waves. Αυτό έχει οδηγήσει σε λάθος αντίληψη ότι οι ασύρματες επικοινωνίες δεν μπορούν να υποκλαπούν καθόλου. Παρόλα αυτά υποκλοπή είναι δυνατό να γίνει χρησιμοποιώντας ειδικό εξοπλισμό.

Για προστασία κατά κάποιου πιθανού ζητήματος ασφάλειας για ασύρματες επικοινωνίες 802.11 έχουν μία λειτουργία η οποία λέγεται WEP (Wired Equivalent Privacy), μία μορφή κωδικοποίησης η οποία παρέχει ασφάλεια σε σύγκριση με ένα παραδοσιακό ενσύρματο δίκτυο. Αν ένα ασύρματο δίκτυο έχει πληροφορίες οι οποίες πρέπει να είναι ασφαλείς, τότε το WEP (ασφάλεια ίση με το ενσύρματο) πρέπει να χρησιμοποιηθεί και διαβεβαιώνει ότι τα δεδομένα προστατεύονται σε επίπεδα παραδοσιακού ενσύρματου δικτύου.

Επίσης πρέπει να σημειωθεί ότι οι παραδοσιακές τεχνικές VPN θα δουλέψουν σε ασύρματα δίκτυα με τον ίδιο τρόπο όπως στα παραδοσιακά ενσύρματα.

Τέλος οι κάρτες δικτύου 802.11 καταναλώνουν σημαντικές ποσότητες ενέργειας με αποτέλεσμα να εξαντλούνται γρήγορα οι μπαταρίες. Αυτό όμως μπορεί να λυθεί με το Power Save Mode το οποίο βοηθάει στην παράταση ζωής της μπαταρίας. Έχει όμως και αυτό τις επιπτώσεις του αφού επηρεάζει ελάχιστα όμως την απόδοση.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Internet

http://www.online.gr

http://www.jaht.com

http://www.vicomsoft.com

http://www.wireless.eng.auth.gr

http://www.bluetooth.org

http://www.ieee.org

http://www.muniwireless.com/

http://www.protocols.com

http://www.wirelessman.org

Books

[1] Stallings, William, 2002 First Edition «Wireless Communications and Networks», Prentice Hall.

[2] Tanenbaum, Andrew S 2004 Fourth Edition. «Δίκτυα Υπολογιστών», Εκδόσεις «Κλειδάριθμος».

[3] Brenner P., "A Technical Tutorial on the IEEE 802.11 Protocol": BreezeCOM Wireless Communications (1997)

Standards

IEEE 802-2001, «IEEE Standard for Local and Metropolitan Area Networks:Overview and Architecture», 2001

IEEE 802.11b-1999/Cor 1-2001, «Part 11: Wireless LAN

Medium Access Control(MAC) and Physical Layer (PHY) Specifications/Amedment 2: Higher-SpeedPhysical Layer Extension in the 2,4 GHz Band - Corrigendum 1», 2001

IEEE 802.11g-2003, «Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications / Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band», 2003

IEEE 802.11h-2003, «Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications / Amendment 5: Spectrum and Transmit Power Management Extensions in the 5 GHz band in Europe», 2003